EPSON
EXCEED YOUR VISION

Příručka správce

NPD5668-00 CS

Obsah

Dodatek

Rozšířená nastavení zabezpečení pro podnik

Autorská práva

Ochranné známky

- ❏ EPSON® je registrovaná ochranná známka a EPSON EXCEED YOUR VISION nebo EXCEED YOUR VISION jsou ochranné známky společnosti 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.
- ❏ Obecná poznámka: Další zde použité názvy produktů slouží pouze k identifikačním účelům a mohou být ochrannými známkami příslušných vlastníků. Společnost Epson se vzdává všech práv na tyto značky.

O této příručce

Značky a symboly

> ⚠ ***Upozornění:***
>
> *Pokyny, které je nutno respektovat, aby nedošlo ke zranění.*

> ***Důležité:***
>
> *Pokyny, které je nutno respektovat, aby nedošlo k poškození vybavení.*

Poznámka:
Pokyny obsahující užitečné tipy a omezení pro používání skeneru.

Související informace

➡ Klepnutím na tuto ikonu budete přesměrováni na související informace.

Popisy používané v této příručce

❏ Snímky obrazovky ovladače skeneru a aplikace Epson Scan 2 (ovladač skeneru) pocházejí ze systému Windows 10 nebo OS X El Capitan. Obsah zobrazený na snímcích obrazovek se liší v závislosti na konkrétním modelu a situaci.

❏ Ilustrace v této příručce jsou pouze příklady. I když zde mohou existovat nepatrné rozdíly v závislosti na modelu, způsob provozu je stejný.

❏ Některé položky menu na LCD obrazovky se liší v závislosti na modelu a nastavení.

Odkazy na operační systémy

Windows

Termíny v této příručce, například „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“ a „Windows Server 2003“ odkazují na následující operační systémy. Kromě toho je použit termín „Windows“ jako odkaz na všechny verze.

❏ Operační systém Microsoft® Windows® 10

❏ Operační systém Microsoft® Windows® 8.1

❏ Operační systém Microsoft® Windows® 8

❏ Operační systém Microsoft® Windows® 7

❏ Operační systém Microsoft® Windows Vista®

❏ Operační systém Microsoft® Windows® XP

- ❏ Operační systém Microsoft® Windows® XP Professional x64 Edition
- ❏ Operační systém Microsoft® Windows Server® 2016
- ❏ Operační systém Microsoft® Windows Server® 2012 R2
- ❏ Operační systém Microsoft® Windows Server® 2012
- ❏ Operační systém Microsoft® Windows Server® 2008 R2
- ❏ Operační systém Microsoft® Windows Server® 2008
- ❏ Operační systém Microsoft® Windows Server® 2003 R2
- ❏ Operační systém Microsoft® Windows Server® 2003

Mac OS

V této příručce odkazuje termín „Mac OS“ na operační systémy „macOS Sierra“, „OS X El Capitan“, „OS X Yosemite“, „OS X Mavericks“, „OS X Mountain Lion“, „Mac OS X v10.7.x“ a „Mac OS X v10.6.8“.

Úvod

O příručce

Tato příručka je určena pro správce zařízení, který je odpovědný za připojení tiskárny nebo skeneru k síti. Příručka obsahuje informace o nastaveních, která je nutné udělat pro využívání všech funkcí.

Více informací o využití funkcí naleznete v dokumentu *Uživatelská příručka*.

Příprava

Popisuje úkoly správce, nastavení zařízení a software pro správu.

Připojení

Popisuje proces připojení zařízení k síti nebo telefonní lince. Také popisuje síťové prostředí, například používání portů pro zařízení, databáze DNS a server proxy.

Nastavení funkcí

Popisuje nastavení všech funkcí zařízení.

Základní nastavení zabezpečení

Popisuje nastavení pro každou funkci, jako je tisk, skenování a faxování.

Provozní nastavení a nastavení správy

Popisuje nutné procesy po zahájení používání zařízení, jako například kontrolu informací a správu.

Řešení potíží

Popisuje nastavení inicializace a řešení potíží se sítí.

Rozšířená nastavení zabezpečení pro podnik

Popisuje metodu nastavení, aby byla zvýšena úroveň zabezpečení zařízení, například certifikát certifikační autority, komunikace SSL/TLS a filtrování IPsec/IP.

V závislosti na modelu nemusí být některé funkce z této kapitoly podporované.

Definice termínů používaných v tomto průvodci

V tomto průvodci se používají následující termíny.

Správce

Osoba odpovědná za instalaci a nastavení zařízení nebo sítě v kanceláři nebo organizaci. V případě malých organizací může být jedna osoba odpovědná za zařízení i za síť. V případě velkých organizací jsou správci odpovědní za síť nebo zařízení ve skupině dané divize nebo oddělení, správci sítě jsou odpovědní za nastavení komunikace mimo organizaci, například internet.

Správce sítě

Osoba odpovědná za řízení síťové komunikace. Osoba, která konfiguruje směrovač, server proxy, server DNS a poštovní server a řídí tak komunikaci přes internet nebo síť.

Uživatel

Osoba, která používá zařízení, jako například tiskárnu nebo skener.

Web Config (webová stránka zařízení)

Jedná se o webový server, který je integrován do zařízení. Nazývá se Web Config. Kontrolovat a měnit stav zařízení můžete pomocí prohlížeče.

Nástroj

Obecný název pro software určený k nastavení nebo správě zařízení, jako například Epson Device Admin, EpsonNet Config, EpsonNet SetupManager atd.

Skenování stiskem tlačítka

Jedná se o obecný název pro skenování z ovládacího panelu zařízení.

ASCII (American Standard Code for Information Interchange)

Jeden ze standardních znakových kódů. Je definováno 128 znaků, včetně znaků abecedy (a–z, A–Z), arabských číslic (0–9), symbolů, prázdných znaků a řídicích znaků. Pokud se v tomto průvodci píše o „ASCII“, jedná se o znaky 0x20–0x7E (hex číslo) uvedené níže a nejsou zahrnuty řídicí znaky.

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	{	|	}	~	

* Znak mezery.

Unicode (UTF-8)

Mezinárodní standardní kód, pokrývající většinu globálních jazyků. Pokud se v tomto průvodci píše o „UTF-8“, jedná se o znaky kódování ve formátu UTF-8.

Příprava

Tato kapitola popisuje roli správce a proces přípravy před provedením nastavení.

Proces nastavení a správy skeneru

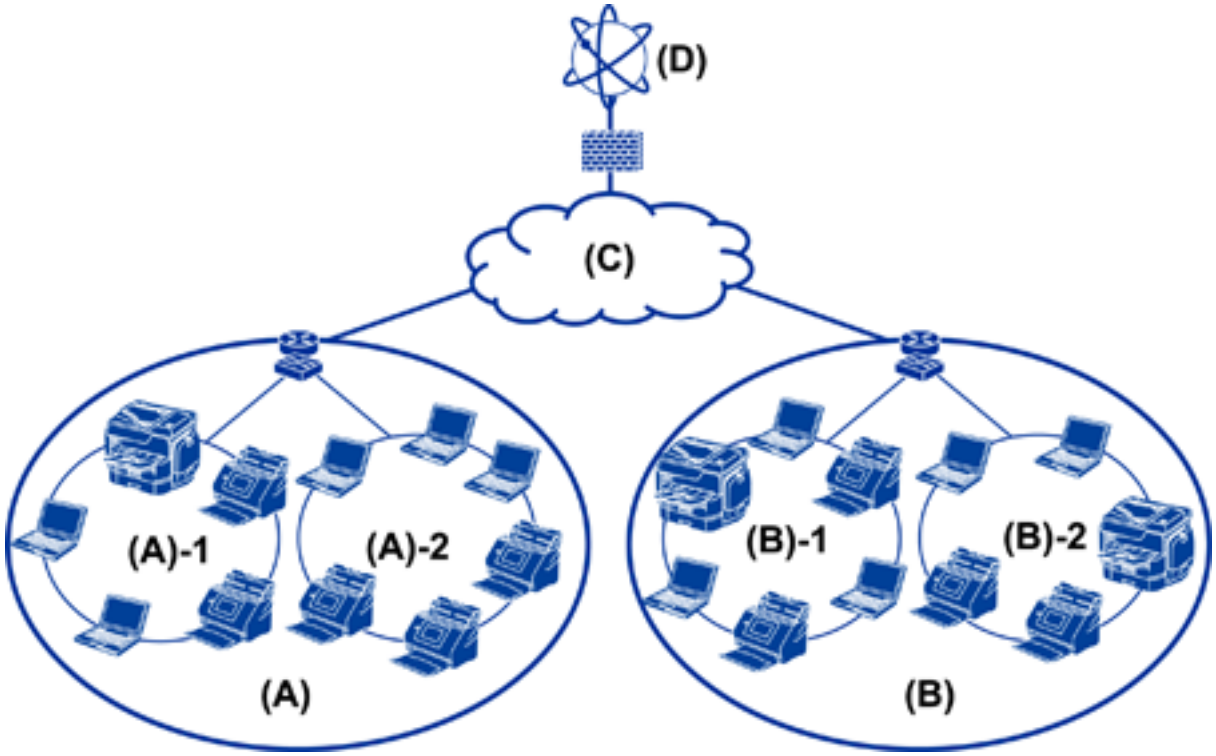
Správce provádí nastavení připojení k síti, počáteční nastavení a správu skeneru tak, aby bylo toto zařízení k dispozici uživatelům.

1. Příprava
   - ❏ Sběr informací o nastavení připojení
   - ❏ Rozhodnutí o metodě připojení
2. Připojení
   - ❏ Připojení k síti z ovládacího panelu skeneru
3. Nastavení funkcí
   - ❏ Nastavení ovladače skeneru
   - ❏ Další rozšířená nastavení
4. Nastavení zabezpečení
   - ❏ Nastavení správce
   - ❏ SSL/TLS
   - ❏ Řízení protokolu
   - ❏ Rozšířená nastavení zabezpečení (Volitelné)
5. Provoz a správa
   - ❏ Kontrola stavu zařízení
   - ❏ Manipulace v případě nouze
   - ❏ Zálohování nastavení zařízení

Související informace

➡ „Příprava“ na str. 10
➡ „Připojení“ na str. 15
➡ „Nastavení funkcí“ na str. 22
➡ „Základní nastavení zabezpečení“ na str. 32
➡ „Provozní nastavení a nastavení správy“ na str. 40

Příklad síťového prostředí



(A): Kancelář 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): Kancelář 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): Internet

Příklad nastavení připojení skeneru

V závislosti na způsobu použití skeneru můžete zvolit hlavně dva typy připojení. V případě obou připojení se skener připojí k síti pomocí počítače a rozbočovače.

❏ Připojení server/klient (Skener používá server Windows a správu úlohy.)

❏ Připojení Peer-to-Peer (přímé připojení klientským počítačem)

Související informace

➡ „Připojení server/klient“ na str. 12

➡ „Připojení Peer-to-Peer“ na str. 12

Připojení server/klient

Centralizujte správu skeneru a úlohy pomocí aplikace Document Capture Pro Server nainstalované na serveru. Centralizaci nejvíce využijete, pokud používáte ke skenování většího počtu dokumentů v určitém formátu více skenerů.

Související informace

➡ „Definice termínů používaných v tomto průvodci“ na str. 8

Připojení Peer-to-Peer

Použijte skener s ovladačem, například s aplikací Epson Scan 2 nainstalovanou na klientském počítači. Pokud nainstalujete aplikaci Document Capture Pro (Document Capture) do klientského počítače, budete moci spustit úlohy na jednotlivých klientských počítačích daného skeneru.

Související informace

➡ „Definice termínů používaných v tomto průvodci“ na str. 8

Příprava připojení k síti

Shromažďování informací o nastavení připojení

Pro připojení k síti je nutné mít adresu IP, adresu brány atd. Předem si zkontrolujte následující.

Divize	Položky	Poznámka
Metoda připojení zařízení	❏ Ethernet	Pro ethernetové připojení použijte kabel kategorie 5e nebo vyšší STP (Shielded Twisted Pair).
Informace o připojení k síti LAN	❏ Adresa IP ❏ Maska podsítě ❏ Výchozí brána	Pokud nastavíte adresu IP automaticky pomocí funkce směrovače DHCP, toto není vyžadováno.
Informace o serveru DNS	❏ Adresa IP pro primární DNS ❏ Adresa IP pro sekundární DNS	Pokud jako adresu IP používáte statickou adresu IP, proveďte konfiguraci serveru DNS. Proveďte konfiguraci v případě automatického přiřazení pomocí funkce DHCP a pokud server DNS nelze přiřadit automaticky.
Informace o serveru proxy	❏ Název serveru proxy ❏ Číslo portu	Proveďte konfiguraci, pokud používáte pro připojení k internetu server proxy a používáte službu Epson Connect nebo funkci automatických aktualizací firmwaru.

Specifikace skeneru

Informace ke specifikaci, zda skener podporuje standardní režim nebo režim připojení, naleznete v příručce *Uživatelská příručka*.

Používání čísla portu

Číslo portu, který skener používá, najdete v části „Dodatek“.

Související informace

➡ „Používání portu pro skener“ na str. 60

Typ přiřazení adresy IP

Existují dva typy přiřazení adresy IP skeneru.

Statická adresa IP:

Přiřazení předem stanovené unikátní adresy IP skeneru.

Adresa IP se nemění ani v případě vypnutí skeneru nebo směrovače, můžete tedy zařízení spravovat pomocí adresy IP.

Tento typ je vhodný pro sítě s větším množstvím spravovaných skenerů, jako v případě velkých kanceláří nebo škol.

Automatické přiřazení pomocí funkce DHCP:

Pokud komunikace mezi skenerem a směrovačem, který podporuje funkci DHCP, proběhne úspěšně, dojde k automatickému přiřazení správné adresy IP.

Pokud není vhodné změnit adresu IP u určitého zařízení, tuto adresu IP si předem rezervujte a později ji přiřaďte.

Server DNS a Server Proxy

Pokud používáte služby internetového připojení, proveďte konfiguraci serveru DNS. Pokud neprovedete konfiguraci, bude nutné pro získání přístupu zadat adresu IP, existuje totiž riziko selhání překladu adres.

Server proxy je umístěn na bráně mezi sítí a internetem, komunikuje s počítačem, skenerem a internetem (protější server) a při jejich vzájemné komunikaci zastupuje všechny strany. Protější server komunikuje pouze se serverem proxy. Proto není možné přečíst informace o skeneru, jako například adresu IP nebo číslo portu a je očekávána zvýšená míra zabezpečení.

Můžete zakázat přístup k určitým adresám URL pomocí funkce filtrování, server proxy je totiž schopen kontrolovat obsah komunikace.

Metoda nastavení síťového připojení

Nastavení adresy IP, masky podsítě a výchozí brány pro připojení skeneru proveďte podle následujících instrukcí.

Použití ovládacího panelu:

Proveďte konfiguraci nastavení pomocí ovládacího panelu skeneru pro každý skener. Po konfigurování nastavení připojení skeneru se připojte k síti.

Použití instalačního programu:

Pokud používáte instalační program, síť skeneru a klientský počítač se nastaví automaticky. Nastavení proveďte podle instrukcí instalačního programu, není nutné mít obsáhlé znalosti o síti.

Použití nástroje:

Můžete také použít nástroj z počítače správce. Můžete objevit skener a poté jej nastavit, nebo vytvořit soubor SYLK a provést dávková nastavení skenerů. Můžete provést nastavení u více skenerů, před tím ale všechny musí být fyzicky připojené ethernetovým kabelem. Proto se doporučuje v případě tohoto nastavení vytvořit síť Ethernet.

Související informace

➡ „Připojení k síti z ovládacího panelu“ na str. 15

➡ „Připojení k síti pomocí instalačního programu“ na str. 19

➡ „Přiřazení adresy IP pomocí programu EpsonNet Config“ na str. 56

Připojení

Tato kapitola popisuje prostředí nebo procesy spojené s připojením skeneru k síti.

Připojení k síti

Připojení k síti z ovládacího panelu

Připojte skener k síti pomocí ovládacího panelu skeneru.

Více informací o ovládacím panelu skeneru získáte v dokumentu *Uživatelská příručka*.

Přiřazování IP adres

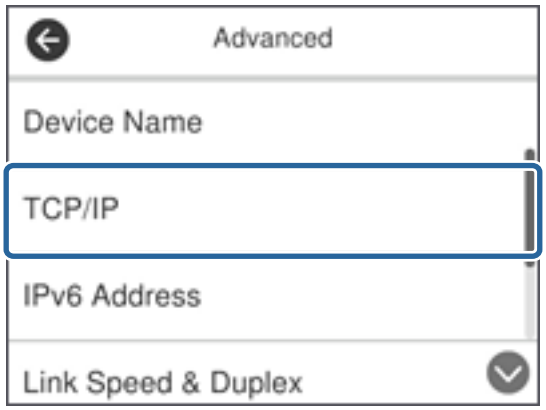
Můžete nastavit základní položky, například Adresa IP, Maska podsítě, a Výchozí brána.

1. Zapněte skener.
2. Potáhněte obrazovku směrem doleva na ovládacím panelu skeneru a poté klepněte na možnost **Nast.**.

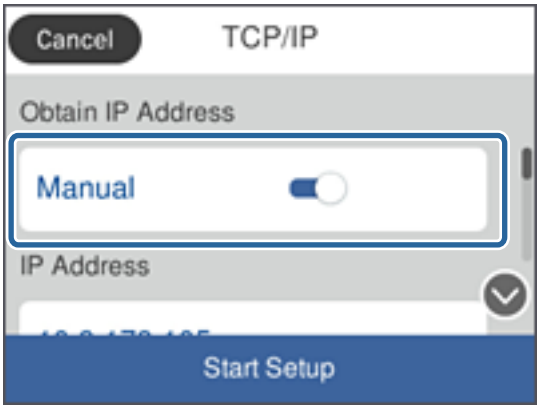
3. Klepněte na položku **Nastavení sítě** > **Změnit nastavení**.

   Pokud se položka nezobrazí, potáhněte obrazovku nahoru pro její zobrazení.

4. Klepněte na položku **TCP/IP**.

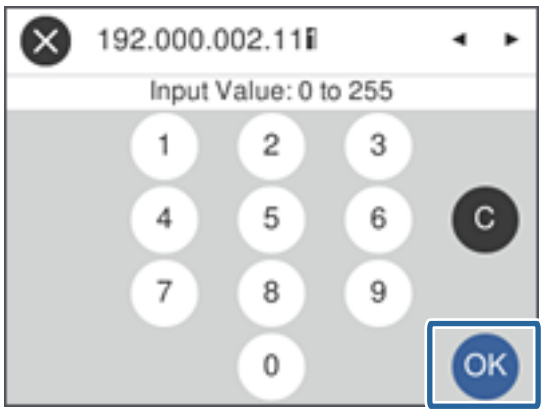


5. Vyberte **Ruční** pro **Získat adresu IP**.



Poznámka:
*Pokud provedete automatické nastavení adresy IP pomocí funkce DHCP na směrovači, vyberte možnost **Automaticky**. V tom případě se položky **Adresa IP**, **Maska podsítě**, a **Výchozí brána** v krocích 6 až 7 nastaví také automaticky, přejděte proto ke kroku 8.*

6. Klepněte na pole **Adresa IP**, zadejte adresu IP pomocí klávesnice, zobrazené na obrazovce, a poté klepněte na možnost **OK**.



Potvrďte hodnotu, která byla uvedena na předchozí obrazovce.

7. Nastavte položky **Maska podsítě** a **Výchozí brána**.

   Potvrďte hodnotu, která byla uvedena na předchozí obrazovce.

   Poznámka:
   *Pokud je kombinace Adresa IP, Maska podsítě a Výchozí brána nesprávná, položka **Zahájit instalaci** je neaktivní a nastavení nelze provést. Potvrďte, že v zadání není chyba.*

8. Klepněte na pole **Primární DNS** pro **Server DNS**, zadejte adresu IP pro primární server DNS pomocí klávesnice, zobrazené na obrazovce, a poté klepněte na možnost **OK**.

   Potvrďte hodnotu, která byla uvedena na předchozí obrazovce.

   Poznámka:
   *Pokud pro nastavení přiřazení adresy IP vyberete možnost **Automaticky**, můžete vybrat nastavení serveru DNS **Ruční** nebo **Automaticky**. Pokud nemůžete získat adresu serveru DNS automaticky, vyberte možnost **Ruční** a zadejte adresu serveru DNS. Poté zadejte adresu sekundárního serveru DNS přímo. Pokud vyberete možnost **Automaticky**, přejděte ke kroku 10.*

9. Klepněte na pole **Sekundární DNS**, zadejte adresu IP pro sekundární server DNS pomocí klávesnice, zobrazené na obrazovce, a poté klepněte na tlačítko **OK**.

   Potvrďte hodnotu, která byla uvedena na předchozí obrazovce.

10. Klepněte na položku **Zahájit instalaci**.

11. Klepněte na položku **Zavřít** na potvrzovací obrazovce.

    Pokud neklepnete na tlačítko **Zavřít** do uplynutí specifického časového intervalu, obrazovka se automaticky zavře.

Připojování k síti Ethernet

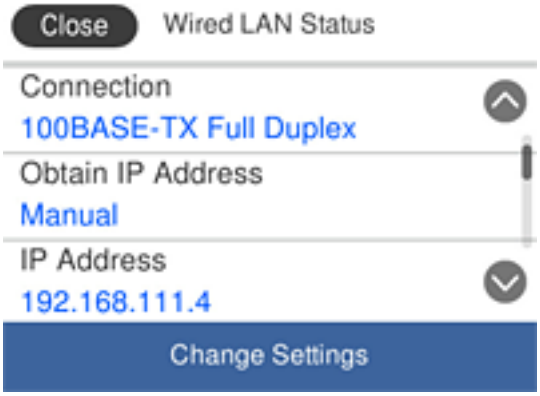
Připojte skener k síti pomocí ethernetového kabelu a zkontrolujte připojení.

1. Připojte skener k rozbočovači (přepínač L2) pomocí ethernetového kabelu.

   Ikona na domovské obrazovce se změní na  .

2. Klepněte na ikonu  na domovské obrazovce.

3. Přetočte obrazovku vzhůru nohama a ujistěte se, že připojení a adresa IP jsou správné.



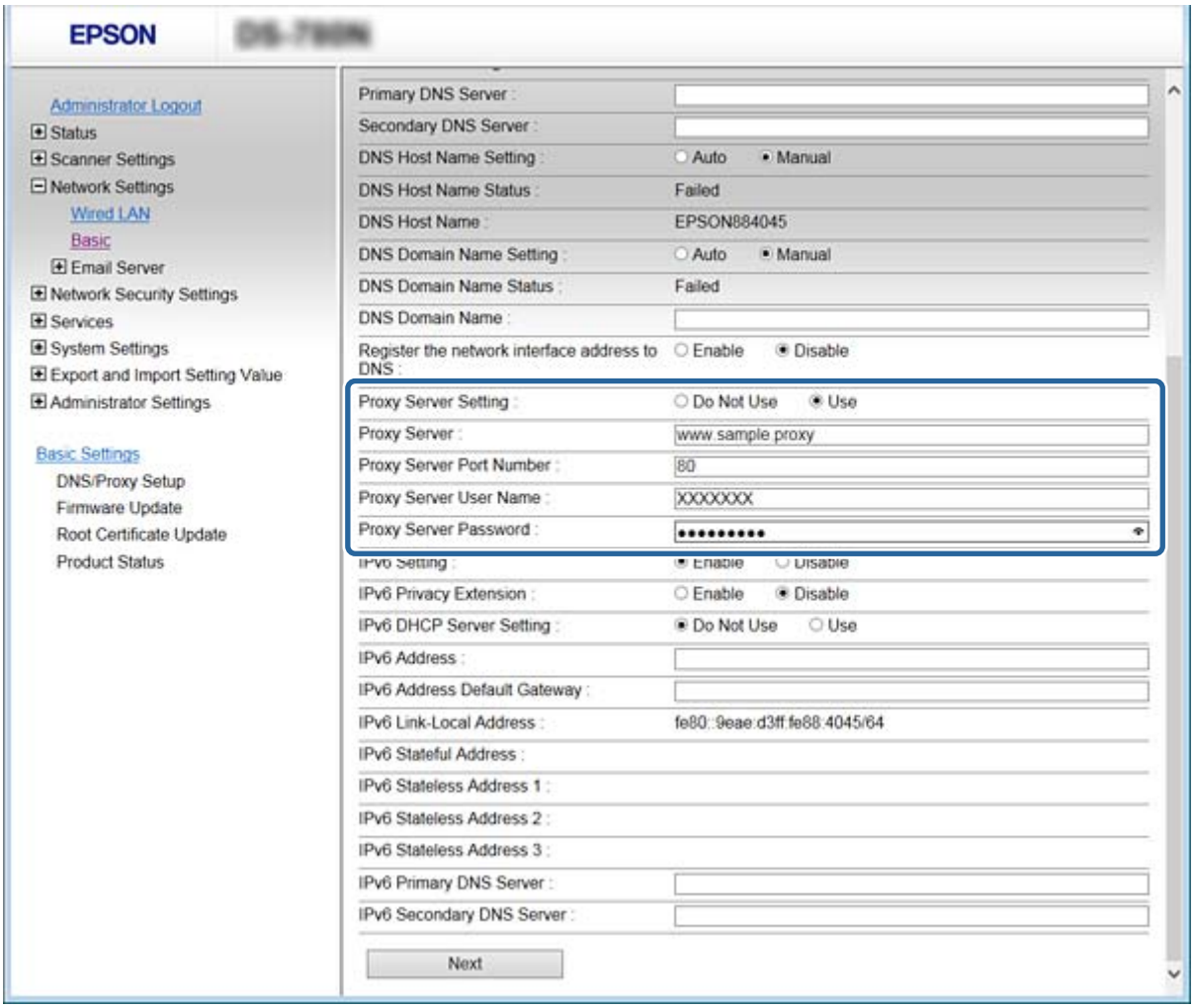
Nastavení serveru Proxy

Na panelu nelze nastavit server proxy. Konfiguraci proveďte pomocí aplikace Web Config.

1. Otevřete aplikaci Web Config a vyberte možnost **Network Settings** > **Basic**.
2. V nabídce **Proxy Server Setting** vyberte možnost **Use**.
3. V adrese IPv4 nebo formátu FQDN pod položkou **Server proxy** určete server proxy a poté zadejte v poli **Proxy Server Port Number** číslo portu.

   U serverů proxy, které vyžadují ověření, zadejte uživatelské jméno a heslo ověření serveru proxy.

4. Klikněte na tlačítko **Next**.



5. Potvrďte nastavení a poté klikněte na možnost **Nastavení**.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Připojení k síti pomocí instalačního programu

Pro připojení skeneru k počítači doporučujeme použít instalační program. Instalační program můžete spustit pomocí jedné z následujících metod.

❏ Nastavení z webu

Otevřete následující webovou stránku a pak zadejte název produktu. Přejděte na položku **Instalace** a pak proveďte nastavení.

http://epson.sn

❏ Nastavení pomocí softwarového disku (pouze pro modely, se kterými je dodáván softwarový disk, a pro uživatele, kteří mají počítač s diskovou jednotkou.)

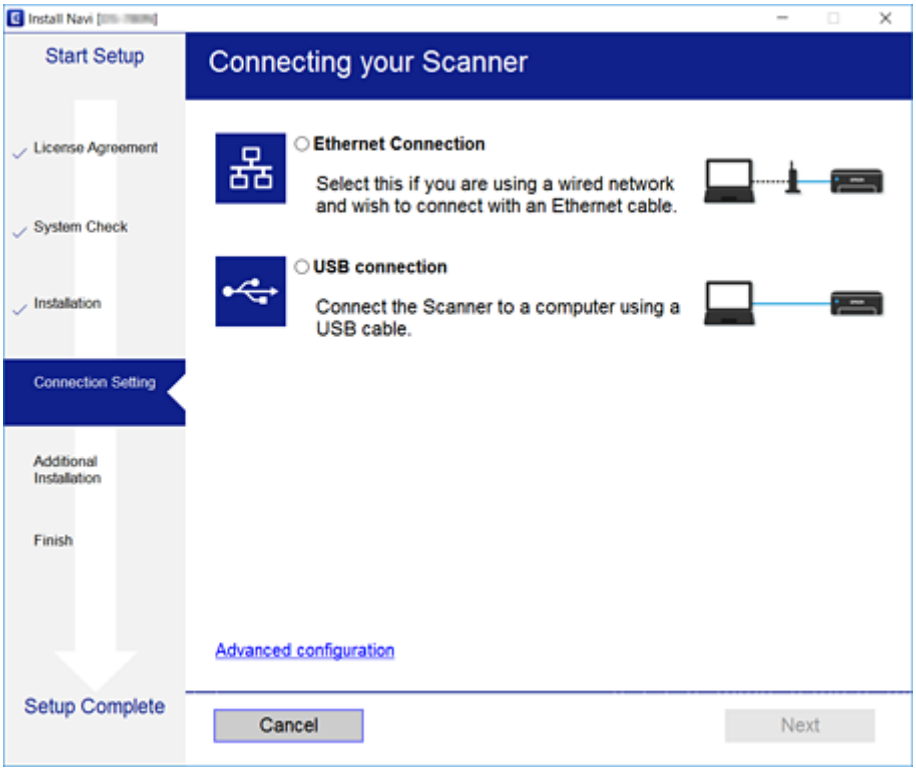
Vložte do počítače softwarový disk a postupujte podle pokynů na obrazovce.

Výběr metod připojení

Postupujte podle instrukcí na obrazovce až do zobrazení následující obrazovky, poté vyberte metodu připojení skeneru k počítači.

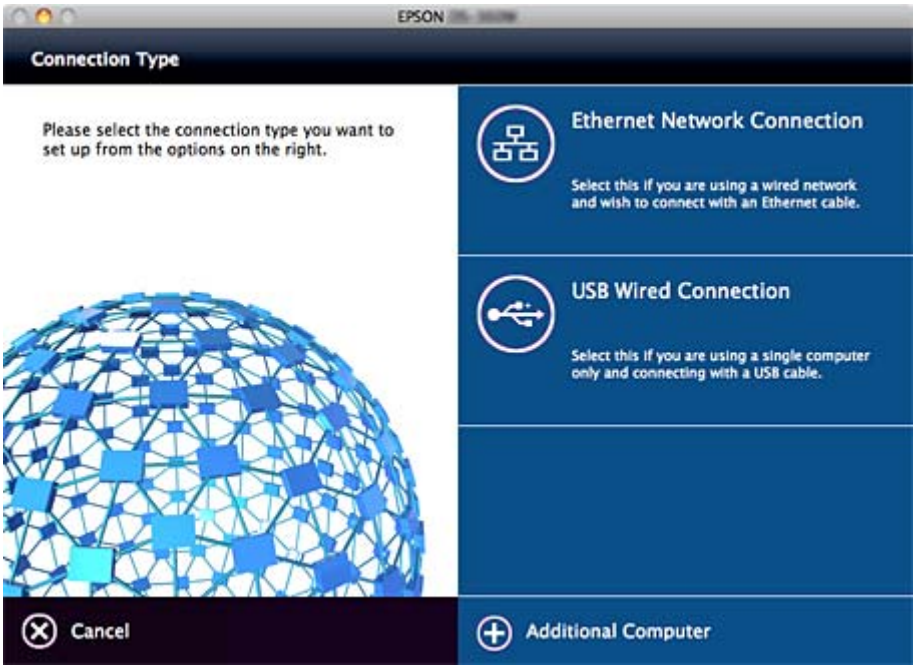
❏ Windows

Vyberte typ připojení a potom klikněte na tlačítko **Další**.



❏ Mac OS

Vyberte typ připojení.



Připojení

Postupujte podle pokynů na obrazovce. Potřebný software je nainstalován.

Nastavení funkcí

Tato kapitola popisuje první nastavení k používání pro každou z funkcí zařízení.

Software nastavení

V tomto tématu je popsán proces realizace nastavení ze správcovského počítače pomocí nástroje Web Config.

Web Config (webová stránka zařízení)

O aplikaci Web Config

Web Config je aplikace na bázi prohlížeče pro konfigurování nastavení skeneru.

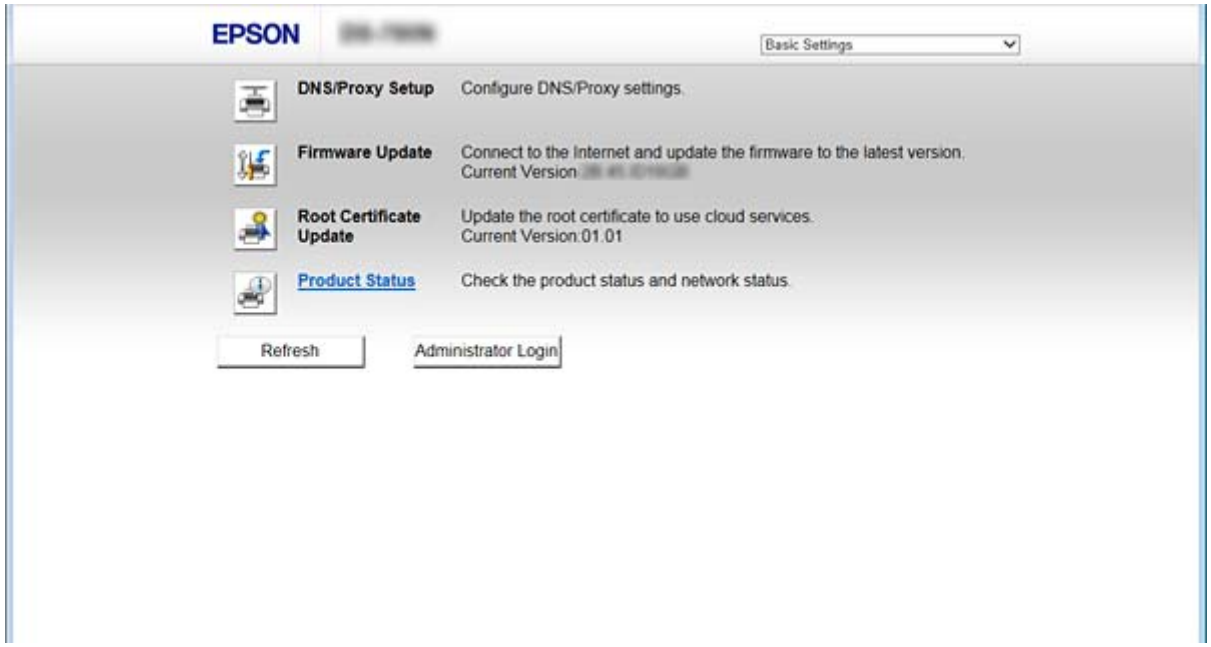
Aby bylo možné přistupovat k aplikaci Web Config, je nutné nejprve přiřadit skeneru adresu IP.

Poznámka:
Nastavení lze zamknout nakonfigurováním hesla správce pro skener.

K dispozici jsou dvě stránky nastavení (viz níže).

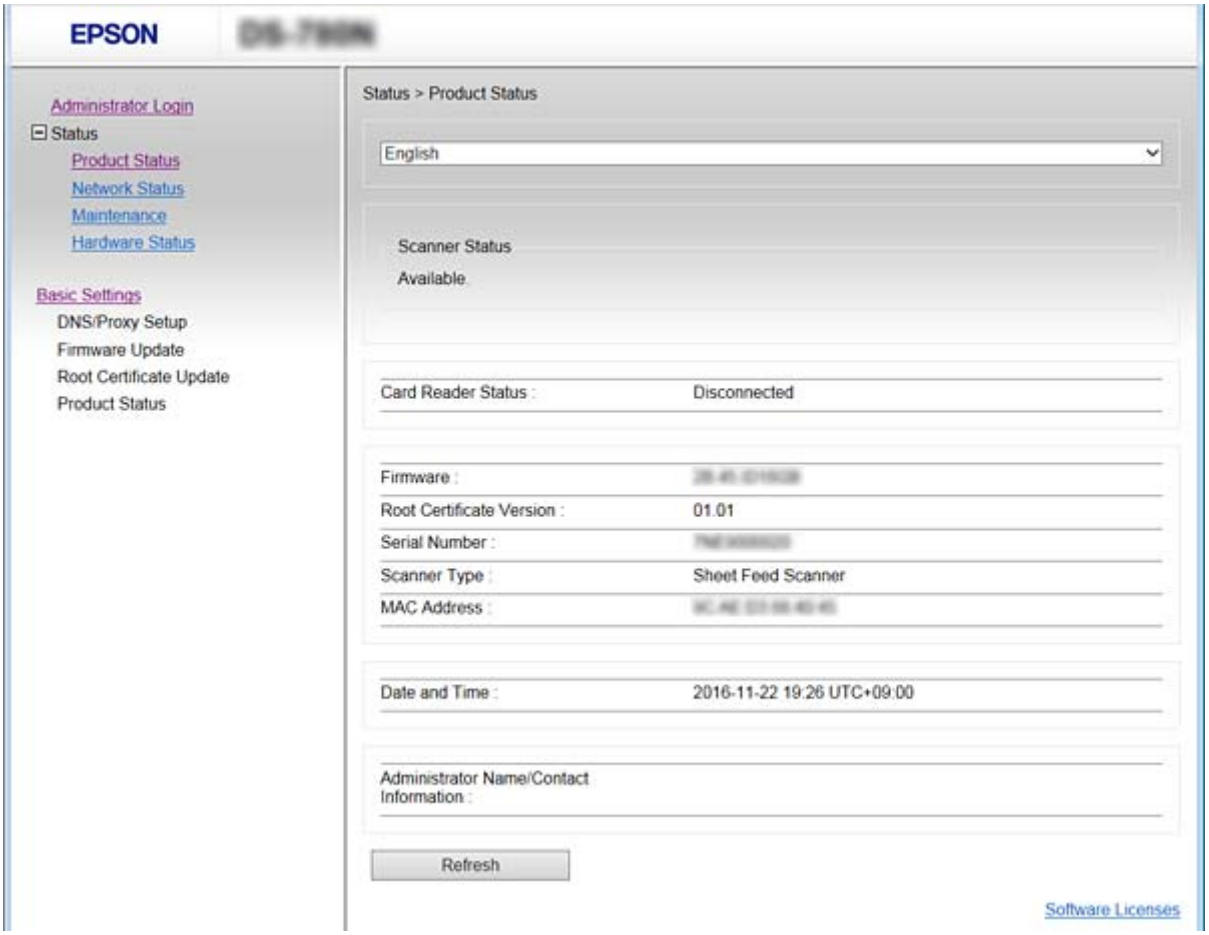
❏ **Basic Settings**

Můžete konfigurovat základní nastavení skeneru.



❏ **Advanced Settings**

Můžete konfigurovat upřesňující nastavení skeneru. Tato stránka je určena především pro správce.



Přístup k aplikaci Web Config

Zadejte adresu IP skeneru do webového prohlížeče. Musí být povolen jazyk JavaScript. Pokud přistupujete k aplikaci Web Config prostřednictvím HTTPS, zobrazí se v prohlížeči výstražná zpráva, jelikož je používán samopodpisovatelný certifikát uložený ve skeneru.

❏ Přístup prostřednictvím HTTPS

IPv4: https://<adresa IP skeneru> (bez < >)

IPv6: https://[adresa IP skeneru]/ (s [ ])

❏ Přístup prostřednictvím HTTP

IPv4: http://<adresa IP skeneru> (bez < >)

IPv6: http://[adresa IP skeneru]/ (s [ ])

Poznámka:

❏ *Příklady*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

https://[2001:db8::1000:1]/

http://[2001:db8::1000:1]/

❏ *Pokud je název skeneru zaregistrován na serveru DNS, můžete místo adresy IP skeneru použít název skeneru.*

Související informace

➡ „Komunikace SSL/TLS se skenerem“ na str. 63

➡ „O digitálním certifikátu“ na str. 63

Používání funkcí skenování

V závislosti na způsobu použití skeneru nainstalujte následující software a pomocí něj proveďte nastavení.

❏ **Skenování z počítače**

❏ Pomocí aplikace Web Config zkontrolujte platnost služby skenování v síti (platnost v době dodávky z továrny).

❏ Nainstalujte aplikaci Epson Scan 2 do počítače a nastavte adresu IP

❏ Pokud chcete skenovat pomocí úloh, nainstalujte aplikaci Document Capture Pro (Document Capture) a změňte nastavení úloh.

❏ **Skenování z provozního panelu**

❏ Při použití aplikace Document Capture Pro nebo Document Capture Pro Server:

Nainstalujte aplikaci Document Capture Pro nebo Document Capture Pro Server

Nastavení DCP (režim serveru nebo klienta).

❏ Při použití protokolu WSD:

Pomocí aplikace Web Config nebo provozního panelu (platnost v době dodávky z továrny) potvrďte platnost protokolu WSD

Doplňkové nastavení zařízení (počítač se systémem Windows).

Skenování z počítače

Nainstalujte software, zkontrolujte, zda je povolena služba skenování v síti, a skenujte z počítače přes síť.

Související informace

➡ „Software k instalaci“ na str. 25

➡ „Povolení síťového skenování“ na str. 25

Software k instalaci

❏ Epson Scan 2

Toto je ovladač skeneru. Pokud ovládáte zařízení z počítače, nainstalujte ovladač na každý klientský počítač. Pokud je nainstalována aplikace Document Capture Pro/Document Capture, můžete provádět operace přiřazené tlačítkům na zařízení.

Pomocí aplikace EpsonNet SetupManager můžete rozeslat ovladače tiskárny v balíčcích.

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

Aplikaci nainstalujte na klientský počítač. Pomocí provozního panelu počítače nebo skeneru můžete prostřednictvím sítě vyvolat a provést úlohy zaregistrované na počítači s nainstalovanou aplikací Document Capture Pro/Document Capture.

Můžete také skenovat z počítače prostřednictvím sítě. Pro skenování je vyžadována aplikace Epson Scan 2.

Související informace

➡ „EpsonNet SetupManager“ na str. 56

Nastavení adresy IP v aplikaci Epson Scan 2

Určete adresu IP skeneru, aby bylo možné jej použít v síti.

1. Pomocí nabídky **Start** > **Všechny programy** > **EPSON** > **Epson Scan 2** spusťte nástroj **Epson Scan 2 Utility**.

   Pokud je již zaregistrován jiný skener, přejděte ke kroku 2.

   Pokud zaregistrován není, přejděte ke kroku 4.

2. Klikněte na možnost ▼ na skeneru **Skener**.
3. Klikněte na položku **Nastavení**.
4. Klikněte na možnost **Povolit úpravy** a poté na položku **Přidat**.
5. V nabídce **Model** vyberte název modelu skeneru.
6. V nabídce **Adresa** pod položkou **Hledat síť** vyberte adresu IP skeneru, který chcete použít.

   Chcete-li aktualizovat seznam, klikněte na ikonu  a poté na ikonu  . Pokud nemůžete vyhledat adresu IP skeneru, vyberte možnost **Zadat adresu** a zadejte adresu IP.

7. Klikněte na položku **Přidat**.
8. Klikněte na tlačítko **OK**.

Povolení síťového skenování

Pokud skenujete z klientského počítače přes síť, můžete nastavit službu síťového skenování. Výchozí nastavení je povoleno.

1. Přistupte k aplikaci Web Config a vyberte **Services** > **Network Scan**.

2. Ujistěte se, že je v aplikaci **EPSON Scan** vybrána možnost **Enable scanning**.

   Výběrem dokončíte akci. Zavřete aplikaci Web Config.

   Pokud není tato možnost vybrána, vyberte ji a přejděte k dalšímu kroku.

3. Klikněte na tlačítko **Next**.

4. Klikněte na tlačítko **OK**.

   Připojení k síti je obnoveno, a poté jsou povolena nastavení.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Skenování pomocí ovládacího panelu

Funkce skenování do složky a do e-mailu pomocí ovládacího panelu skeneru a přenos naskenovaného snímku do e-mailu, složky apod. jsou obvykle provedeny zahájením úlohy z počítače.

Pokud chcete naskenované snímky přenést, nastavte úlohu pomocí aplikace Document Capture Pro Server nebo Document Capture Pro.

Detaily o nastavení a nastavení úlohy naleznete v dokumentaci nebo nápovědě k aplikaci Document Capture Pro Server nebo Document Capture Pro.

Související informace

➡ „Nastavení aplikace Document Capture Pro Server/Document Capture Pro“ na str. 26

➡ „Nastavení serverů a složek“ na str. 27

Software k instalaci do počítače

❏ **Document Capture Pro Server**

Jedná se o serverovou verzi aplikace Document Capture Pro. Aplikaci nainstalujte na server Windows. Server může centrálně spravovat více zařízení a úloh. A úlohy lze provádět současně na více skenerech.

Pomocí certifikované verze aplikace Document Capture Pro Server můžete spravovat úlohy a historii skenování, které jsou spojeny s určitými uživateli a skupinami.

Detaily o aplikaci Document Capture Pro Server vám poskytne místní kancelář společnosti Epson.

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

Stejně jako při skenování z počítače můžete na ovládacím panelu vyvolat úlohy zaregistrované v počítači a provést je. Provádění úloh počítače současně ve více skenerech není možné.

Nastavení aplikace Document Capture Pro Server/Document Capture Pro

Zařízení můžete nastavit pomocí funkce skenování na provozním panelu skeneru.

1. Otevřete aplikaci Web Config a vyberte možnost **Services** > **Document Capture Pro**.

2. Vyberte **Provozní režim**.

   ❏ Server Mode:

   Tuto možnost vyberte, pokud používáte aplikaci Document Capture Pro Server nebo Document Capture Pro pouze pro úlohy, které byly nastaveny na konkrétním počítači.

   ❏ Client Mode:

   Tuto možnost nastavte při výběru nastavení úlohy aplikace Document Capture Pro (Document Capture) nainstalované na jednotlivých klientských počítačích v síti bez určení počítače.

3. V závislosti na vybraném režimu nastavte následující položky.

   ❏ Server Mode:

   Pod položkou **Server Address** určete server, na kterém je aplikace Document Capture Pro Server nainstalovaná. Zadat můžete 2 až 252 znaků ve formátu IPv4, IPv6, názvu hostitele nebo formátu FQDN. V případě formátu FQDN lze použít písmena, číslice, znaky a pomlčky (kromě znaků na začátku a na konci) amerického formátu ASCII.

   ❏ Client Mode:

   Určete možnost **Group Settings**, aby bylo možné použít skupinu skenerů určenou v aplikaci Document Capture Pro (Document Capture).

4. Klikněte na položku **Nastavení**.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Nastavení serverů a složek

Aplikace Document Capture Pro a Document Capture Pro Server uloží naskenovaná data na server nebo do klientského počítače a poté pomocí funkce přenosu provede funkci skenování do složky nebo skenování do e-mailu.

K přenosu dat z počítače, kde je nainstalována aplikace Document Capture Pro nebo Document Capture Pro Server, do počítače nebo cloudové služby je nutné oprávnění a příslušné informace.

Využijte informace o požadovaných funkcích podle následujících požadavků.

Tyto funkce můžete nastavit pomocí aplikace Document Capture Pro nebo Document Capture Pro Server. Detaily o nastavení naleznete v dokumentaci nebo nápovědě k aplikaci Document Capture Pro Server nebo Document Capture Pro.

Název	Nastavení	Požadavek
Skenování do síťové složky (SMB)	Vytvořte a nastavte sdílení složky pro uložení	Účet uživatele s právy pro správu počítače, který vytváří složky pro uložení.
	Příjemce skenování do síťové složky (SMB)	Uživatelské jméno a heslo pro přihlášení do počítače se složkou pro uložení, a dále oprávnění k aktualizaci složky pro uložení.
Skenování do síťové složky (FTP)	Nastavení přihlášení na server FTP	Přihlašovací informace pro server FTP a oprávnění k aktualizaci složky pro uložení.

Název	Nastavení	Požadavek
Skenování do e-mailu	Nastavení poštovního serveru	Informace o nastavení poštovního serveru
Skenování do aplikace Document Capture Pro (pokud se používá aplikace Document Capture Pro Server)	Nastavení přihlášení ke cloudovým službám	Prostředí internetového připojení Registrace účtu cloudových služeb

Použití skenování WSD (pouze pro systém Windows)

Skenování WSD můžete použít, pokud je v počítači nainstalován systém Windows Vista nebo novější.

Pokud lze protokol WSD použít, zobrazí se na ovládacím panelu skeneru nabídka **Počítač (WSD)**.

1. Otevřete aplikaci Web Config a vyberte možnost **Services** > **Protocol**.
2. Zkontrolujte, zda je v nastavení **WSD Settings** zaškrtnuto políčko **Enable WSD**.
   Pokud zaškrtnuto je, úloha je dokončena a vy můžete zavřít aplikaci Web Config.
   Pokud zaškrtnuto není, zaškrtněte je a pokračujte k dalšímu kroku.
3. Klikněte na tlačítko **Next**.
4. Potvrďte nastavení a klikněte na možnost **Nastavení**.

Nastavení systému

Nastavení systému na ovládacím panelu

Nastavení jasu obrazovky

Můžete nastavit jas LCD obrazovky.

1. Klepněte na položku **Nast.** na domovské obrazovce.
2. Klepněte na položku **Obecná nastavení** > **Jas LCD**.
3. Klepnutím na ikonu nebo upravte jas.
   Zadat můžete číslice od 1 do 9.
4. Klepněte na tlačítko **OK**.

Nastavení zvuku

Můžete nastavit zvuky vydávané, pokud je panel v provozu nebo pokud se vyskytne chyba.

1. Klepněte na položku **Nast.** na domovské obrazovce.
2. Klepněte na položku **Obecná nastavení** > **Zvuk**.
3. Podle potřeby nastavte následující položky.
   - ❏ Zvuk vydávaný při provozu
     Nastavte hlasitost zvuku, který bude vydávat provozní panel, pokud jej používáte.
   - ❏ Zvuk, který bude vydán, pokud se vyskytne chyba
     Nastavte hlasitost zvuku, který bude vydán, pokud se vyskytne chyba.
4. Klepněte na tlačítko **OK**.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Detekce dvojitého vložení předlohy

Určete funkci, pomocí které detekujete, zda byl dokument ke skenování vložen dvakrát. Pokud se tak stalo, díky této funkci nebude spuštěno skenování.

Chcete-li skenovat předlohy, u kterých je určeno, že byly vloženy víckrát, například obálky nebo papíry s nálepkami, tuto funkci u nich vypněte.

Poznámka:
Nastavení můžete také provést v nástroji Web Config nebo v aplikaci Epson Scan 2.

1. Klepněte na položku **Nast.** na domovské obrazovce.
2. Klepněte na položku **Externí skenování - nastavení** > **Ultrazv. detekce dvojitého zavedení**.
3. Klepněte na možnost **Ultrazv. detekce dvojitého zavedení** a funkci zapněte nebo vypněte.
4. Klepněte na tlačítko **Zavřít**.

Nastavení nízkorychlostního režimu

Nastavte nízkorychlostní skenování, aby při skenování tenkých dokumentů, například proužků papíru, neuvízl papír.

1. Klepněte na položku **Nast.** na domovské obrazovce.
2. Klepněte na položku **Externí skenování - nastavení** > **Pomalu**.
3. Klepněte na možnost **Pomalu** a funkci zapněte nebo vypněte.
4. Klepněte na tlačítko **Zavřít**.

Nastavení systému pomocí aplikace Web Config

Nastavení úsporného režimu v době nečinnosti

Proveďte nastavení úsporného režimu pro období nečinnosti skeneru. Nastavte čas v závislosti na prostředí, ve kterém pracujete.

Poznámka:
Úsporný režim lze nastavit na ovládacím panelu skeneru.

1. Otevřete aplikaci Web Config a vyberte možnost **System Settings** > **Power Saving**.
2. Zadejte čas pro funkci **Sleep Timer** pro přepnutí do úsporného režimu v případě nečinnosti.

   Můžete nastavit až 240 minut po minutách.
3. Vyberte čas vypnutí v poli **Power Off Timer**.
4. Klikněte na tlačítko **OK**.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Nastavení ovládacího panelu

Můžete nastavit ovládací panel skeneru. Nastavení můžete provést následujícím způsobem.

1. Otevřete aplikaci Web Config a vyberte možnost **System Settings** > **Control Panel**.
2. Podle potřeby nastavte také následující položky.

   ❏ Language

   Na ovládacím panelu vyberte zobrazený jazyk.

   ❏ Panel Lock

   Pokud vyberete možnost **ON**, budete potřebovat heslo správce v případě provádění operací, které vyžadují oprávnění správce. Pokud není heslo správce nastaveno, je funkce uzamčení panelu zakázána.

   ❏ Operation Timeout

   Pokud vyberete možnost **ON**, budete při přihlášení jako správce po určité době nečinnosti automaticky odhlášeni a přesměrováni na úvodní obrazovku.

   Můžete nastavit rozpětí 10 sekund až 240 minut v sekundách.
3. Klikněte na tlačítko **OK**.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Nastavení omezení externího rozhraní

Můžete omezit připojení USB z počítače. Pomocí tohoto nastavení můžete omezit jiné skenování než skenování přes síť.

1. Otevřete aplikaci Web Config a vyberte možnost **System Settings** > **External Interface**.
2. Vyberte volbu **Enable** nebo **Disable**.

   Chcete-li omezit připojení, vyberte možnost **Disable**.
3. Klepněte na tlačítko **OK**.

Synchronizace data a času s časovým serverem

Pokud používáte certifikát certifikační agentury, můžete předejít problémům s časem.

1. Přistupte na aplikaci Web Config a vyberte **System Settings** > **Date and Time** > **Time Server**.
2. Vyberte **Use** pro **Use Time Server**.
3. Zadejte adresu časového serveru pro **Time Server Address**.

   Lze použít formát IPv4, IPv6 nebo FQDN. Zadejte 252 znaků nebo méně. Pokud toto nechcete specifikovat, ponechte pole prázdné.
4. Zadejte informace do pole **Update Interval (min)**.

   Můžete nastavit až 10 800 minut po minutách.
5. Klikněte na tlačítko **OK**.

   Poznámka:
   *Stav připojení můžete potvrdit s časovým serverem v části **Time Server Status**.*

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Základní nastavení zabezpečení

Tato kapitola popisuje základní nastavení zabezpečení, které nevyžaduje zvláštní prostředí.

Úvod k základním funkcím zabezpečení

Zde uvádíme základní funkce zabezpečení pro zařízení společnosti Epson.

Název funkce	Typ funkce	Co je třeba nastavit	Čemu je třeba zabránit
Nastavení hesla správce	Uzamkněte nastavení systému, například nastavení sítě nebo připojení USB, aby jej nemohl změnit nikdo kromě správce.	Heslo k zařízení nastavuje správce. Konfigurace nebo aktualizace jsou k dispozici v nástroji Web Config, na ovládacím panelu, v Epson Device Admin a v programu EpsonNet Config.	Zabraňte neoprávněnému čtení a změnám informací uložených v zařízení, jako je například ID, heslo, síťová nastavení a kontakty. Také se snažte co nejvíce omezit další bezpečnostní rizika, mezi které patří únik informací v síťovém prostředí nebo porušování zásad zabezpečení.
Komunikace SSL/TLS	Pokud se připojujete k severu Epson pomocí internetu a zařízení, například při komunikace počítače přes prohlížeč nebo při aktualizaci firmwaru, je obsah komunikace zašifrován komunikací SSL/TLS.	Získejte certifikát podepsaný certifikační autoritou a poté jej importujte do skeneru.	Odstranění identifikace zařízení, za pomoci certifikátu podepsaného certifikační autoritou, zabraňuje přisvojení totožnosti či neoprávněnému přístupu. Navíc je obsah komunikací SSL/TLS chráněn a zabraňuje úniku obsahu tiskových dat a informací o nastavení.
Řídicí protokoly	Řídicí protokoly slouží ke komunikaci mezi zařízeními a počítači a k povolení/zákazu funkcí.	Nastavte protokol nebo službu, které umožňují povolení nebo zákaz jednotlivých funkcí.	Snížení bezpečnostního rizika neoprávněného používání zrušením nepotřebných uživatelských funkcí.

Související informace

➡ „O aplikaci Web Config“ na str. 22
➡ „EpsonNet Config“ na str. 55
➡ „Epson Device Admin“ na str. 55
➡ „Konfigurování hesla správce“ na str. 32
➡ „Řídicí protokoly“ na str. 35

Konfigurování hesla správce

Pokud nastavíte heslo správce, žádní uživatelé s výjimkou správců nebudou moci měnit nastavení pro správu systému. Nastavit nebo změnit heslo správce můžete buď pomocí nástroje Web Config, přes ovládací panel skeneru

nebo pomocí softwaru (Epson Device Admin nebo EpsonNet Config). V případě použití softwaru si přečtěte dokumentaci k příslušnému softwaru.

Související informace

➡ „Konfigurace hesla správce z ovládacího panelu“ na str. 33
➡ „Konfigurace hesla správce pomocí nástroje Web Config“ na str. 33
➡ „EpsonNet Config“ na str. 55
➡ „Epson Device Admin“ na str. 55

Konfigurace hesla správce z ovládacího panelu

Pomocí ovládacího panelu skeneru můžete nastavit heslo správce.

1. Klepněte na položku **Nast.** na domovské obrazovce.
2. Klepněte na položku **Správa systému** > **Nastavení správce**.

   Pokud se položka nezobrazí, potáhněte obrazovku nahoru pro její zobrazení.
3. Klepněte na položku **Heslo správce** > **Registrovat**.
4. Zadejte nové heslo a poté klepněte na možnost **OK**.
5. Zadejte znovu heslo a poté klepněte na možnost **OK**.
6. Klepněte na položku **OK** na potvrzovací obrazovce.

   Zobrazí se obrazovka nastavení správce.
7. Klepněte na možnost **Nastavení zámku** a poté **OK** na potvrzovací obrazovce.

   Možnost Nastavení zámku je nastavena na **Zap.** a v případě použití uzamčené položky nabídky bude vyžadováno heslo správce.

Poznámka:

❏ *Pokud nastavíte možnost **Nast.** > **Obecná nastavení** > **Časový limit operace** na hodnotu **Zap.**, skener vás po určité době, kdy nebudete používat ovládací panel, odhlásí.*

❏ *Heslo správce můžete změnit nebo odstranit, pokud vyberete možnost **Změnit** nebo **Reset** na obrazovce **Heslo správce** a zadáte heslo správce.*

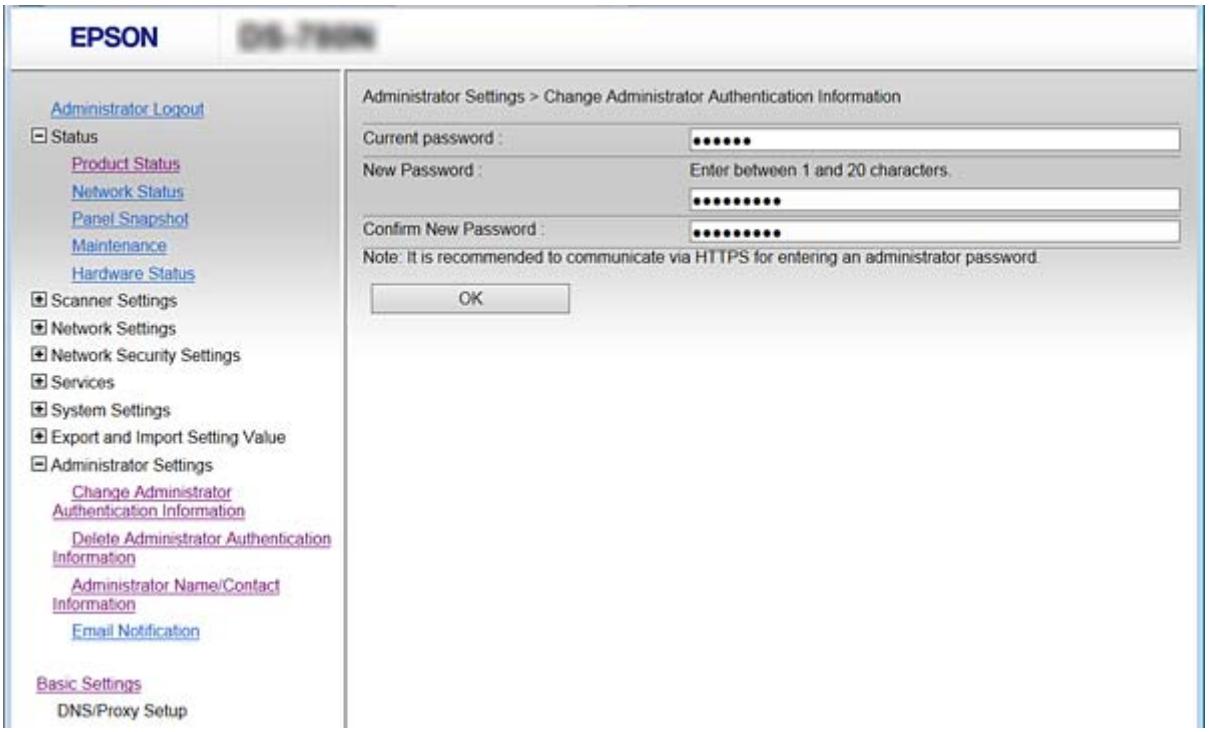
Konfigurace hesla správce pomocí nástroje Web Config

Heslo správce můžete nastavit pomocí aplikace Web Config.

1. Otevřete aplikaci Web Config a vyberte možnost **Administrator Settings** > **Change Administrator Authentication Information**.

2. Zadejte heslo do pole **New Password** a do pole **Confirm New Password**. V případě potřeby zadejte uživatelské jméno.

   Pokud chcete změnit heslo na nové, zadejte současné heslo.



3. Vyberte **OK**.

   Poznámka:

   ❏ *Pro nastavení nebo změnu uzamčených položek nabídky klikněte na možnost **Administrator Login** a zadejte heslo správce.*

   ❏ *Chcete-li odstranit heslo správce, klikněte na možnost **Administrator Settings** > **Delete Administrator Authentication Information** a zadejte heslo správce.*

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Položky k uzamčení pomocí hesla správce

Správci mají oprávnění pro nastavení a změny všech funkcí v zařízeních.

Pokud u zařízení nastavíte heslo správce, můžete jej uzamknout, takže nebudete moci změnit nastavení správy zařízení.

Následující položky může správce ovládat.

Položka	Popis
Nastavení skeneru	Nastavení detekce dvojitého vložení předlohy a nastavení nízkorychlostního režimu.
Nastavení ethernetového připojení	Slouží ke změně názvu zařízení a adresy IP, nastavení serveru DNS nebo serveru proxy a nastavení změn vzhledem k síťovým připojením.

Základní nastavení zabezpečení

Položka	Popis
Nastavení uživatelských služeb	Slouží k nastavení pro protokoly řízení komunikace, síťového skenování a služeb Document Capture Pro.
Nastavení poštovního serveru	Slouží k nastavení poštovního serveru, se kterým zařízení přímo komunikují.
Nastavení zabezpečení	Nastavení zabezpečení sítě, jako například komunikace SSL/TLS, filtrování IPsec/IP a IEEE802.1X.
Aktualizace kořenového certifikátu	Slouží k aktualizaci kořenových certifikátů vyžadovaných pro ověření Document Capture Pro Server a aktualizaci firmwaru z aplikace Web Config.
Aktualizace firmwaru	Kontrola a aktualizace firmwaru zařízení.
Čas, nastavení časovače	Čas přechodu do režimu spánku, automatické vypnutí, datum/čas, neprovozní časovač, další nastavení časovače.
Obnovení výchozích nastavení	Slouží k nastavení skeneru na přechod do továrního nastavení.
Nastavení správce	Nastavení zámku správce nebo hesla správce.
Nastavení certifikovaného zařízení	Nastavení ID zařízení pro ověření. Tuto možnost nastavte, pokud používáte skener na ověřovacím systému, který podporuje ověřovací zařízení.

Řídící protokoly

Můžete skenovat do různých umístění a pomocí různých protokolů. Síťové skenování můžete provést z neurčeného množství síťových počítačů. Povoleno je například skenování pomocí pouze do určených umístění a pomocí určených protokolů. Můžete snížit bezpečnostní rizika neoprávněného používání omezením skenování z konkrétních umístění nebo řízením dostupných funkcí.

Nakonfigurujte nastavení protokolů.

1. Otevřete aplikaci Web Config a vyberte možnost **Services** > **Protocol**.
2. Nakonfigurujte jednotlivé položky.
3. Klikněte na tlačítko **Next**.
4. Klikněte na tlačítko **OK**.

   Tato nastavení budou použita ve skeneru.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Protokoly, které lze povolit nebo zakázat“ na str. 36
➡ „Položky nastavení protokolu“ na str. 37

Protokoly, které lze povolit nebo zakázat

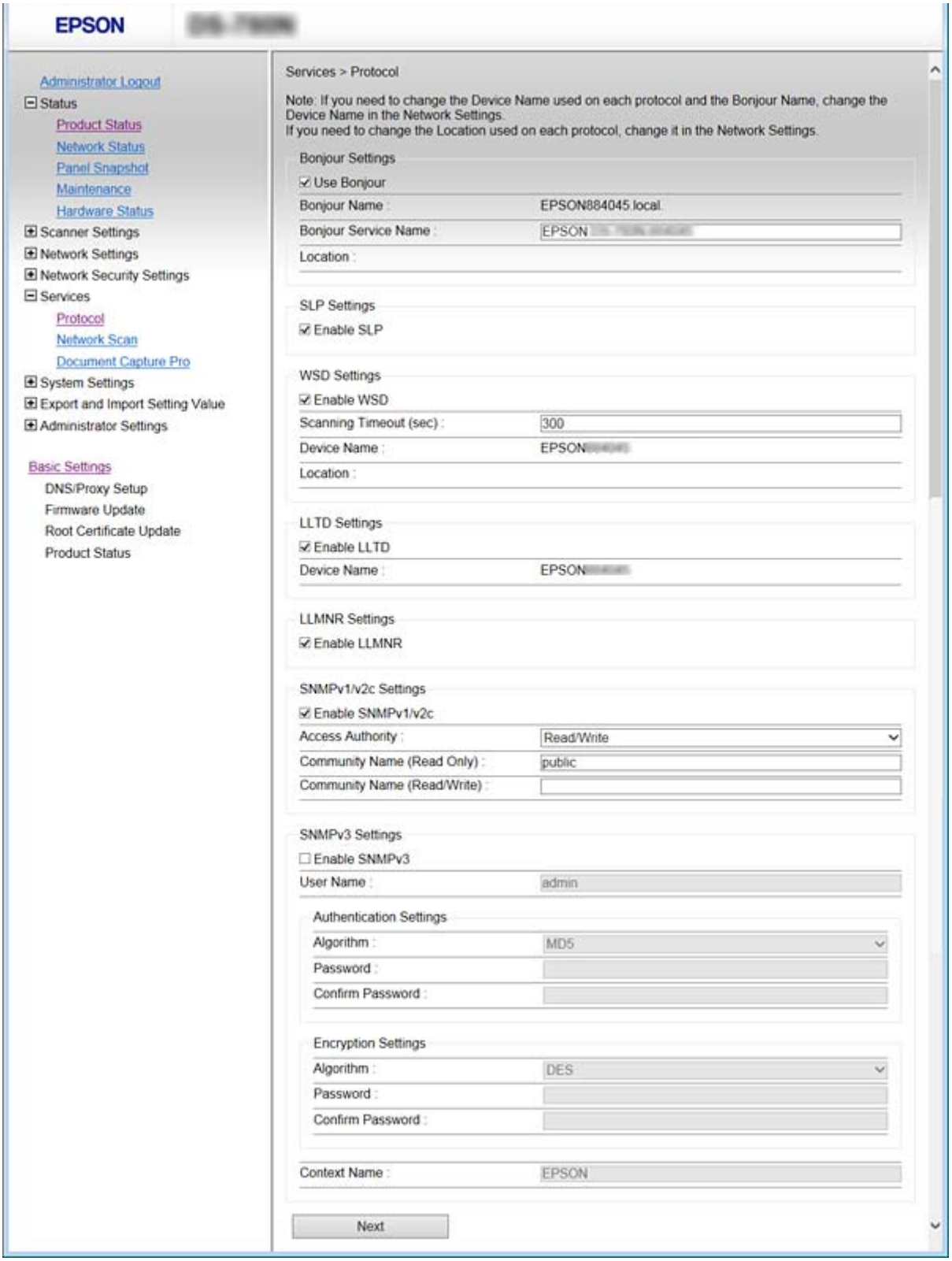
Protokol	Popis
Bonjour Settings	Můžete určit, zda se má používat protokol Bonjour. Služba Bonjour se používá k vyhledávání zařízení a k jiným úkonům.
SLP Settings	Můžete povolit nebo zakázat funkci SLP. Funkce SLP se používá v aplikaci Epson Scan 2 a k síťovému vyhledávání v aplikaci EpsonNet Config.
WSD Settings	Můžete povolit nebo zakázat funkci WSD. Když je tato funkce povolená, můžete přidávat zařízení WSD nebo skenovat z portu WSD.
LLTD Settings	Můžete povolit nebo zakázat funkci LLTD. Když je tato funkce povolena, je zobrazena na mapě sítě Windows.
LLMNR Settings	Můžete povolit nebo zakázat funkci LLMNR. Když je tato funkce povolena, můžete používat překlad adres IP bez systému NetBIOS, i když nelze používat DNS.
SNMPv1/v2c Settings	Můžete povolit nebo zakázat protokol SNMPv1/v2c. Slouží pro nastavení zařízení, sledování atd.
SNMPv3 Settings	Můžete povolit nebo zakázat protokol SNMPv3. Slouží pro nastavení šifrovaných zařízení, sledování atd.

Související informace

➡ „Řídící protokoly“ na str. 35

➡ „Položky nastavení protokolu“ na str. 37

Položky nastavení protokolu



Položky	Hodnota nastavení a popis
Bonjour Settings	

Základní nastavení zabezpečení

Položky	Hodnota nastavení a popis
Use Bonjour	Výběrem této položky můžete vyhledat nebo používat zařízení prostřednictvím služby Bonjour.
Bonjour Name	Zobrazí název Bonjour.
Bonjour Service Name	Můžete zobrazit a nastavit název služby Bonjour.
Location	Zobrazí název umístění Bonjour.
SLP Settings	
Enable SLP	Výběrem této položky povolíte funkci SLP. Používá se k vyhledání sítě v aplikacích Epson Scan 2 a EpsonNet Config.
WSD Settings	
Enable WSD	Výběrem této položky povolíte přidávání zařízení pomocí rozhraní WSD a tisk a skenování z portu WSD.
Scanning Timeout (sec)	Zadejte hodnotu časového limitu komunikace pro skenování WSD mezi 3 a 3 600 sekundami.
Device Name	Zobrazí název zařízení WSD.
Location	Zobrazí název umístění WSD.
LLTD Settings	
Enable LLTD	Výběrem této položky povolíte LLTD. Skener bude zobrazen na mapě sítě Windows.
Device Name	Zobrazí název zařízení LLTD.
LLMNR Settings	
Enable LLMNR	Výběrem této položky povolíte LLMNR. Můžete používat překlad adres IP bez systému NetBIOS, i když nelze používat DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	Výběrem této položky povolíte SNMPv1/v2c. Zobrazí se pouze skenery, které podporují protokol SNMPv3.
Access Authority	Pokud je povolen protokol SNMPv1/v2c, nastavte oprávnění k přístupu. Vyberte volbu **Read Only** nebo **Read/Write**.
Community Name (Read Only)	Zadejte 0 až 32 znaků ASCII (0x20 až 0x7E).
Community Name (Read/Write)	Zadejte 0 až 32 znaků ASCII (0x20 až 0x7E).
SNMPv3 Settings	
Enable SNMPv3	Pokud je toto pole zaškrtnuto, je povolen protokol SNMPv3.
User Name	Zadejte 1 až 32 znaků s použitím 1bajtových znaků.
Authentication Settings	
Algorithm	Vyberte algoritmus pro ověřování protokolu SNMPv3.

Základní nastavení zabezpečení

Položky	Hodnota nastavení a popis
Password	Zadejte heslo ověřování protokolu SNMPv3. Zadejte 8 až 32 znaků ve formátu ASCII (0x20–0x7E). Pokud toto nechcete specifikovat, ponechte pole prázdné.
Confirm Password	Zadejte heslo nakonfigurované pro potvrzení.
Encryption Settings	
Algorithm	Vyberte algoritmus ověřování protokolu SNMPv3.
Password	Zadejte heslo ověřování protokolu SNMPv3. Zadejte 8 až 32 znaků ve formátu ASCII (0x20–0x7E). Pokud toto nechcete specifikovat, ponechte pole prázdné.
Confirm Password	Zadejte heslo nakonfigurované pro potvrzení.
Context Name	Zadejte 32 znaků nebo méně v Unicode (UTF-8). Pokud toto nechcete specifikovat, ponechte pole prázdné. Počet znaků, které lze zadat, se liší v závislosti na jazyku.

Související informace

➡ „Řídící protokoly“ na str. 35

➡ „Protokoly, které lze povolit nebo zakázat“ na str. 36

Provozní nastavení a nastavení správy

Tato kapitola popisuje položky, které se týkají každodenních operací a správy zařízení.

Potvrzení informací o zařízení

Z nabídky **Status** pomocí nástroje Web Config můžete zkontrolovat následující informace o provozním zařízení.

❏ Product Status

Slouží ke kontrole jazyka, stavu, čísla produktu, adresy MAC atd.

❏ Network Status

Slouží ke kontrole informací o stavu připojení sítě, adrese IP, serveru DNS atd.

❏ Panel Snapshot

Slouží k zobrazení snímku obrazovky, který se zobrazí na ovládacím panelu zařízení.

❏ Maintenance

Slouží ke kontrole data zahájení, informací o skenování apod.

❏ Hardware Status

Slouží ke kontrole stavu skeneru.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Správa zařízení (Epson Device Admin)

Pomocí nástroje Epson Device Admin můžete spravovat a provozovat více zařízení. Nástroj Epson Device Admin vám umožňuje správu zařízení, umístěných na jiné síti. Níže uvádíme hlavní funkce správy.

Více informací o funkcích a používání softwaru najdete v dokumentaci nebo nápovědě k nástroji Epson Device Admin.

❏ Zjišťování zařízení

Můžete zjišťovat zařízení na síti a poté je registrovat do seznamu. Pokud jsou zařízení Epson, například tiskárny a skenery, připojena ke stejnému segmentu sítě jako počítač správce, můžete je najít i v případě, že jim nebyly přiřazeny adresy IP.

Můžete také vyhledávat zařízení připojená k počítačům na síti pomocí kabelů USB. Musíte však do počítače nainstalovat Epson Device USB Agent.

❏ Nastavení zařízení

Můžete vytvořit vzor, obsahující položky nastavení, jako je například síťové rozhraní a zdroj papíru, a aplikovat jej na ostatní zařízení jako sdílené nastavení. Pokud je zařízení připojené k síti, můžete mu přiřadit adresu IP, pokud se tak ještě nestalo.

❏ Sledování zařízení

Můžete pravidelně získávat podrobné informace a další informace o stavu zařízení na síti. Můžete také sledovat zařízení připojená k počítačům na síti pomocí kabelů USB a zařízení jiných společností, která byla registrována na seznamu zařízení. Pro sledování zařízení připojených pomocí kabelu USB musíte nainstalovat nástroj Epson Device USB Agent.

❏ Správa výstrah

Můžete sledovat výstrahy stavu zařízení a spotřebních dílů. Systém automaticky odesílá správci e-mailová upozornění v závislosti na nastavených podmínkách.

❏ Správa zpráv

Můžete vytvářet pravidelné zprávy, systém totiž shromažďuje informace o využití zařízení a spotřebních dílů. Tyto zprávy pak můžete uložit a odesílat e-mailem.

Související informace

➡ „Epson Device Admin“ na str. 55

Přijímání e-mailových oznámení když dojde k událostem

O e-mailových upozorněních

Tuto funkci můžete používat k příjmu výstrah prostřednictvím e-mailu, pokud nastane příslušná událost. Můžete registrovat až 5 e-mailových adres a vybrat, pro které události chcete přijmout upozornění.

Pro použití této funkce je nutné nakonfigurovat poštovní server.

Související informace

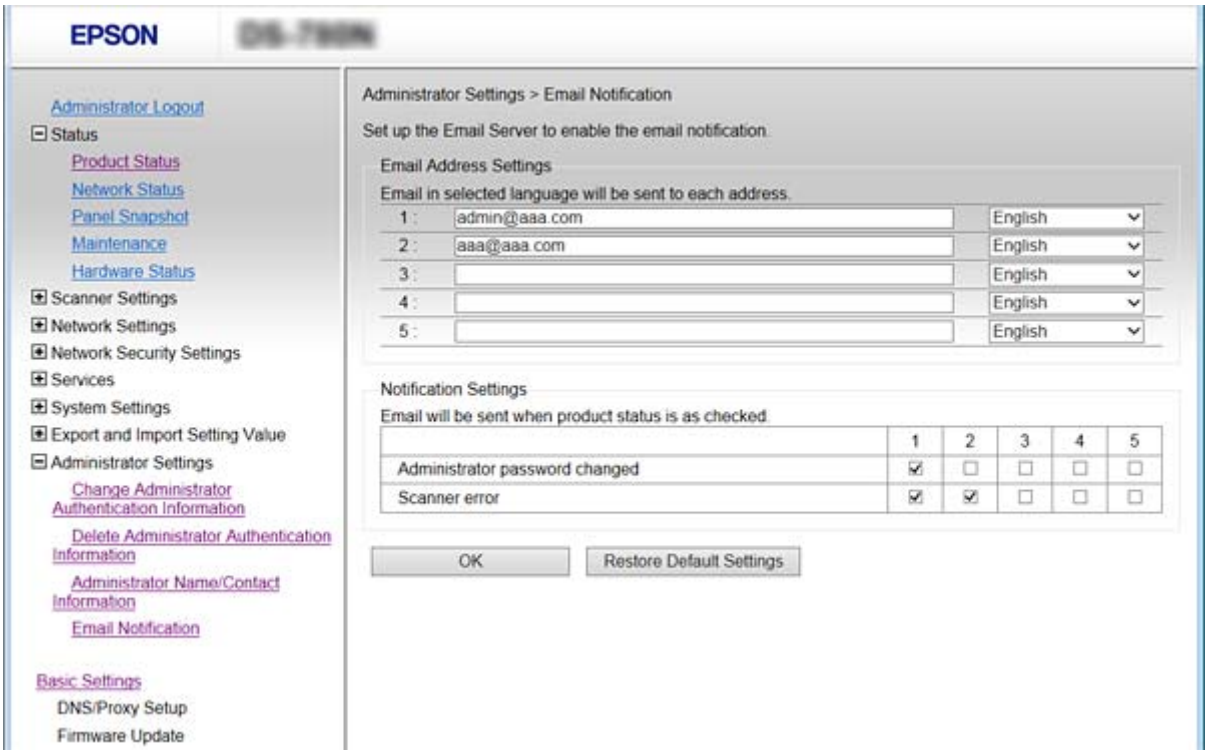
➡ „Konfigurování poštovního serveru“ na str. 42

Konfigurování e-mailových upozornění

Chcete-li používat tuto funkci, musíte nakonfigurovat poštovní server.

1. Přistupte na aplikaci Web Config a vyberte **Administrator Settings** > **Email Notification**.
2. Zadejte e-mailovou adresu, na kterou chcete přijímat e-mailová upozornění.
3. Vyberte jazyk pro e-mailová upozornění.

4. Zaškrtněte pole upozornění, která chcete přijímat.



5. Klepněte na tlačítko **OK**.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Konfigurování poštovního serveru“ na str. 42

Konfigurování poštovního serveru

Před konfigurováním ověřte následující.

❏ Skener je připojen k síti.

❏ Informace o poštovním serveru počítače.

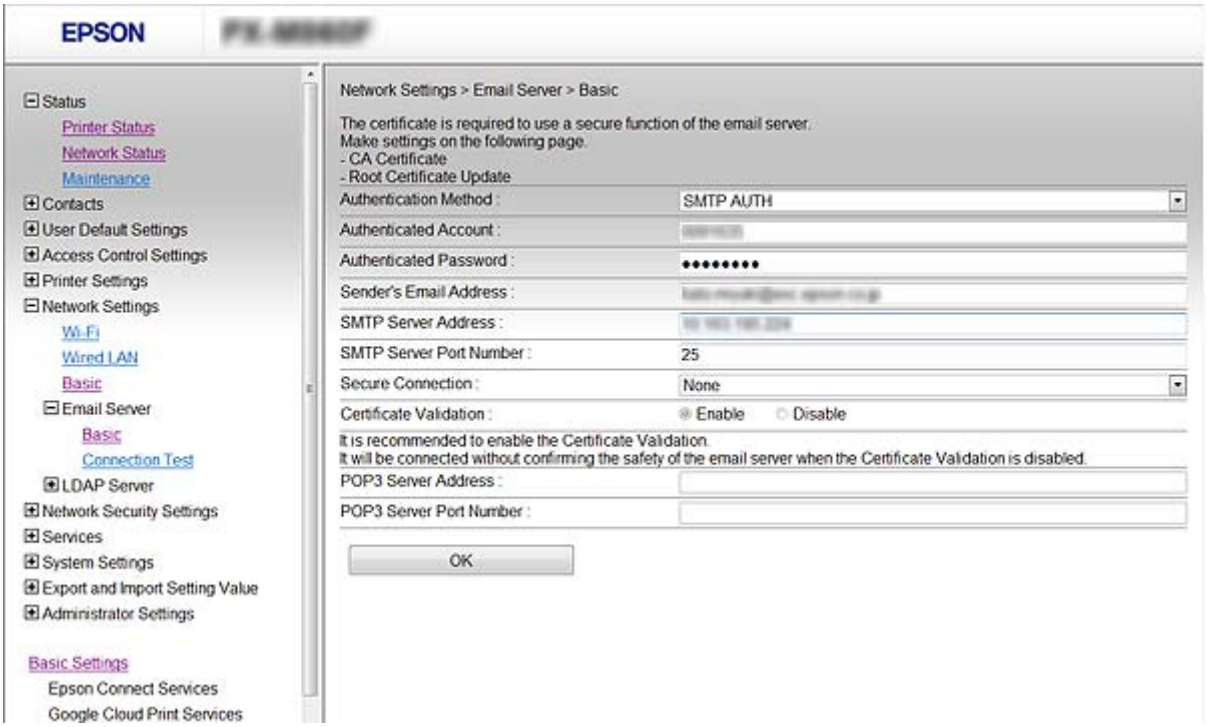
1. Přistupte na aplikaci Web Config a vyberte **Network Settings** > **Email Server** > **Basic**.
2. Zadejte hodnotu pro každou položku.
3. Vyberte volbu **OK**.

   Zobrazí se vybraná nastavení.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Položky nastavení poštovního serveru“ na str. 43

Položky nastavení poštovního serveru



Položky	Nastavení a vysvětlení	
Authentication Method	Určete metodu ověřování skeneru pro přístup k poštovnímu serveru.	
	Off	Ověřování je při komunikaci s poštovním serverem zakázané.
	SMTP AUTH	Vyžaduje, aby poštovní server podporoval ověřování SMTP.
	POP before SMTP	Při výběru této metody nakonfigurujte server POP3.
Authenticated Account	Vyberete-li **SMTP AUTH** nebo **POP before SMTP** jako **Authentication Method**, zadejte ověřovaný název účtu od 0 do 255 znaků ve formátu ASCII (0x20–0x7E).	
Authenticated Password	Vyberete-li **SMTP AUTH** nebo **POP before SMTP** jako **Authentication Method**, zadejte ověřené heslo v rozsahu 0 až 20 znaků s použitím znaků A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	Zadejte e-mailovou adresu odesilatele. Zadejte 0 až 255 znaků ve formátu ASCII (0x20–0x7E) vyjma znaků : ( ) < > [ ] ; ¥. Jako první znak nelze použít tečku „.“.	
SMTP Server Address	Zadejte 0 až 255 znaků s použitím znaků A–Z a–z 0–9 . - . Lze použít formát IPv4 nebo FQDN.	
SMTP Server Port Number	Zadejte číslo 1 až 65535.	

Položky	Nastavení a vysvětlení	
Secure Connection	Určete metodu zabezpečeného připojení poštovního serveru.	
	None	Vyberete-li **POP before SMTP** v **Authentication Method**, bude metoda připojení nastavena na **None**.
	SSL/TLS	Tato možnost je dostupná, když je položka **Authentication Method** nastavena na **Off** nebo **SMTP AUTH**.
	STARTTLS	Tato možnost je dostupná, když je položka **Authentication Method** nastavena na **Off** nebo **SMTP AUTH**.
Certificate Validation	Když je tato možnost povolena, certifikát je ověřen. Doporučujeme nastavit tuto možnost na **Enable**.	
POP3 Server Address	Vyberete-li **POP before SMTP** jako **Authentication Method**, zadejte adresu serveru POP3 v rozsahu 0 až 255 znaků s použitím znaků A–Z a–z 0–9 . - . Lze použít formát IPv4 nebo FQDN.	
POP3 Server Port Number	Vyberete-li volbu **POP before SMTP** jako **Authentication Method**, zadejte číslo v rozmezí hodnot 1 až 65535.	

Související informace

➡ „Konfigurování poštovního serveru“ na str. 42

Kontrola připojení k poštovnímu serveru

1. Přistupte na aplikaci Web Config a vyberte **Network Settings** > **Email Server** > **Connection Test**.
2. Vyberte volbu **Start**.

   Bude zahájen test připojení k poštovnímu serveru. Po zkoušce se zobrazí kontrolní hlášení.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Reference zkoušky připojení poštovního serveru“ na str. 44

Reference zkoušky připojení poštovního serveru

Zprávy	Vysvětlení
Connection test was successful.	Tato zpráva se zobrazí, když je připojení k serveru úspěšné.
SMTP server communication error. Check the following. - Network Settings	Tato zpráva se zobrazí v následujících případech ❏ Skener není připojen k síti ❏ Server SMTP je vypnutý ❏ Došlo k odpojení síťového připojení během komunikace ❏ Byla přijata neúplná data

Provozní nastavení a nastavení správy

Zprávy	Vysvětlení
POP3 server communication error. Check the following. - Network Settings	Tato zpráva se zobrazí v následujících případech ❏ Skener není připojen k síti ❏ Server POP3 je vypnutý ❏ Došlo k odpojení síťového připojení během komunikace ❏ Byla přijata neúplná data
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	Tato zpráva se zobrazí v následujících případech ❏ Připojení k serveru DNS se nezdařilo ❏ Překlad adres IP pro server SMTP se nezdařil
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	Tato zpráva se zobrazí v následujících případech ❏ Připojení k serveru DNS se nezdařilo ❏ Překlad adres IP pro server POP3 se nezdařil
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Tato zpráva se zobrazí v případě chyby ověření serveru SMTP.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	Tato zpráva se zobrazí v případě chyby ověření serveru POP3.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	Tato zpráva se zobrazí, když se pokusíte komunikovat pomocí nepodporovaných protokolů.
Connection to SMTP server failed. Change Secure Connection to None.	Tato zpráva se zobrazí, když dojde k neshodě protokolu SMTP mezi serverem a klientem nebo když server nepodporuje zabezpečené připojení (připojení SSL) protokolu SMTP.
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	Tato zpráva se zobrazí, když dojde k neshodě protokolu SMTP mezi serverem a klientem nebo když server požádá po použití připojení SSL/TLS pro zabezpečené připojení SMTP.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	Tato zpráva se zobrazí, když dojde k neshodě protokolu SMTP mezi serverem a klientem nebo když server požádá po použití připojení STARTTLS pro zabezpečené připojení SMTP.
The connection is untrusted. Check the following. - Date and Time	Tato zpráva se zobrazí, když není nastavení data a času skeneru správné nebo když vypršela platnost certifikátu.
The connection is untrusted. Check the following. - CA Certificate	Tato zpráva se zobrazí, když skener nemá kořenový certifikát odpovídající serveru nebo pokud nebyl naimportován žádný CA Certificate.
The connection is not secured.	Tato zpráva se zobrazí, když je získaný certifikát poškozený.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	Tato zpráva se zobrazí, když nastane neshoda metod ověření mezi serverem a klientem. Server podporuje SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	Tato zpráva se zobrazí, když nastane neshoda metod ověření mezi serverem a klientem. Server nepodporuje SMTP AUTH.

Zprávy	Vysvětlení
Sender's Email Address is incorrect. Change to the email address for your email service.	Tato zpráva se zobrazí, když je zadána nesprávná e-mailová adresa odesilatele.
Cannot access the product until processing is complete.	Tato zpráva se zobrazí, když je skener zaneprázdněný.

Související informace

➡ „Kontrola připojení k poštovnímu serveru“ na str. 44

Aktualizace firmwaru

Aktualizace firmwaru pomocí aplikace Web Config

Funkce aktualizuje firmware pomocí aplikace Web Config. Zařízení musí být připojeno k internetu.

1. Otevřete aplikaci Web Config a vyberte možnost **Basic Settings** > **Firmware Update**.
2. Klikněte na položku **Start**.

   Zahájí se potvrzení firmwaru, a pokud aktualizovaný firmware existuje, dojde k zobrazení informací o firmwaru.
3. Klikněte na možnost **Start** a postupujte podle instrukcí na obrazovce.

Poznámka:
Můžete také aktualizovat firmware pomocí nástroje Epson Device Admin. Informace o firmwaru můžete vizuálně ověřit na seznamu zařízení. To se hodí v případě, když potřebujete aktualizovat firmware u více zařízení. Další podrobnosti najdete v průvodci aplikace Epson Device Admin nebo v nápovědě.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Epson Device Admin“ na str. 55

Aktualizace firmwaru pomocí aplikace Epson Firmware Updater

Firmware k zařízení si můžete stáhnout na počítač z webu společnosti Epson. Poté připojte zařízení s počítačem pomocí kabelu USB a aktualizujte firmware. Pokud nemůžete provést aktualizaci přes síť, zkuste následující metodu.

1. Přejděte na web společnosti Epson a stáhněte si potřebný firmware.
2. Připojte počítač, který obsahuje stažený firmware k zařízení, pomocí kabelu USB.
3. Dvakrát klikněte na stažený soubor s příponou .exe.

   Spustí se aplikace Epson Firmware Updater.

4. Postupujte podle pokynů na obrazovce.

Záloha nastavení

Pomocí exportu položek nastavení aplikace Web Config můžete kopírovat položky do jiných skenerů.

Exportování nastavení

Můžete exportovat každé nastavení skeneru.

1. Přistupte na aplikaci Web Config a pak vyberte **Export and Import Setting Value** > **Export**.
2. Vyberte nastavení, které chcete exportovat.

   Vyberte nastavení, které chcete exportovat. Vyberete-li nadřazenou kategorii, je možné rovněž vybírat podkategorie. Nelze ovšem vybírat podkategorie, které způsobují chyby duplikováním v rámci stejné sítě (například adresy IP atd.).
3. Zadejte heslo pro zašifrování exportovaného souboru.

   K importování souboru je zapotřebí heslo. Pokud soubor nechcete šifrovat, ponechte toto pole prázdné.
4. Klepněte na tlačítko **Export**.

   Důležité:

   Chcete-li exportovat síťová nastavení skeneru, například název tiskárny a adresu IP, vyberte ***Enable to select the individual settings of device*** *a vyberte další položky. Pro náhradní skener použijte pouze vybrané hodnoty.*

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Importování nastavení

Můžete importovat exportovaný soubor Web Config do skeneru.

Důležité:

Při importování hodnot, které obsahují individuální údaje, například název skeneru nebo adresu IP, ověřte, zda stejná adresa IP neexistuje ve stejné síti. Pokud se adresa IP překrývá, skener tuto hodnotu nerespektuje.

1. Přistupte na aplikaci Web Config a pak vyberte **Export and Import Setting Value** > **Import**.
2. Vyberte exportovaný soubor a potom zadejte zašifrované heslo.
3. Klepněte na tlačítko **Next**.
4. Vyberte nastavení, která chcete importovat a potom klepněte na tlačítko **Next**.
5. Klepněte na tlačítko **OK**.

Provozní nastavení a nastavení správy

Tato nastavení budou použita ve skeneru.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Odstraňování problémů

Tipy pro odstraňování problémů

Další informace jsou k dispozici v následující příručce.

❏ Uživatelská příručka

Obsahuje pokyny pro používání skeneru, údržbu a odstraňování problémů.

Kontrola protokolu serveru a síťového zařízení

Pokud se objeví problémy s připojením k síti, můžete odhalit příčinu kontrolou protokolu poštovního serveru, serveru LDAP apod., případně kontrolou stavu pomocí síťového protokolu ze systémových protokolů zařízení, například směrovačů.

Inicializace síťového nastavení

Obnovení nastavení sítě z ovládacího panelu

Veškeré nastavení sítě můžete obnovit na výchozí hodnoty.

1. Klepněte na položku **Nast.** na domovské obrazovce.
2. Klepněte na položku **Správa systému** > **Obnovit výchozí nastavení** > **Nastavení sítě**.
3. Zkontrolujte zprávu a pak klepněte na položku **Ano**.
4. Jakmile se zobrazí zpráva o dokončení, klepněte na tlačítko **Zavřít**.

   Pokud neklepnete na tlačítko **Zavřít** do uplynutí specifického časového intervalu, obrazovka se automaticky zavře.

Kontrola komunikace mezi zařízeními a počítači

Kontrola připojení pomocí příkazu Ping — Windows

Pomocí příkazu Ping můžete zkontrolovat, zda je počítač připojený ke skeneru. Pomocí těchto kroků s příkazem Ping zkontrolujte připojení.

1. Zkontrolujte IP adresu skeneru pro připojení, které chcete zkontrolovat.

   Ke kontrole můžete použít Epson Scan 2.

2. Zobrazte obrazovku příkazového řádku počítače.
   - ❏ Windows 10

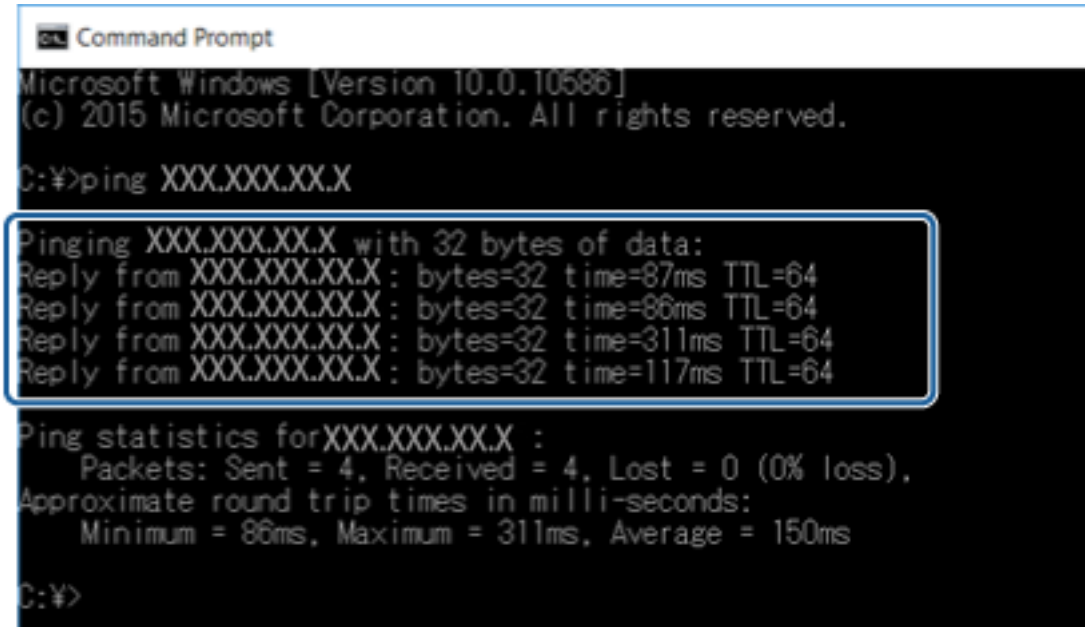
     Klikněte pravým tlačítkem na tlačítko Start nebo ho stiskněte a podržte, a pak vyberte **Příkazový řádek**.
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

     Zobrazte obrazovku aplikace a pak vyberte položku **Příkazový řádek**.
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 nebo novější

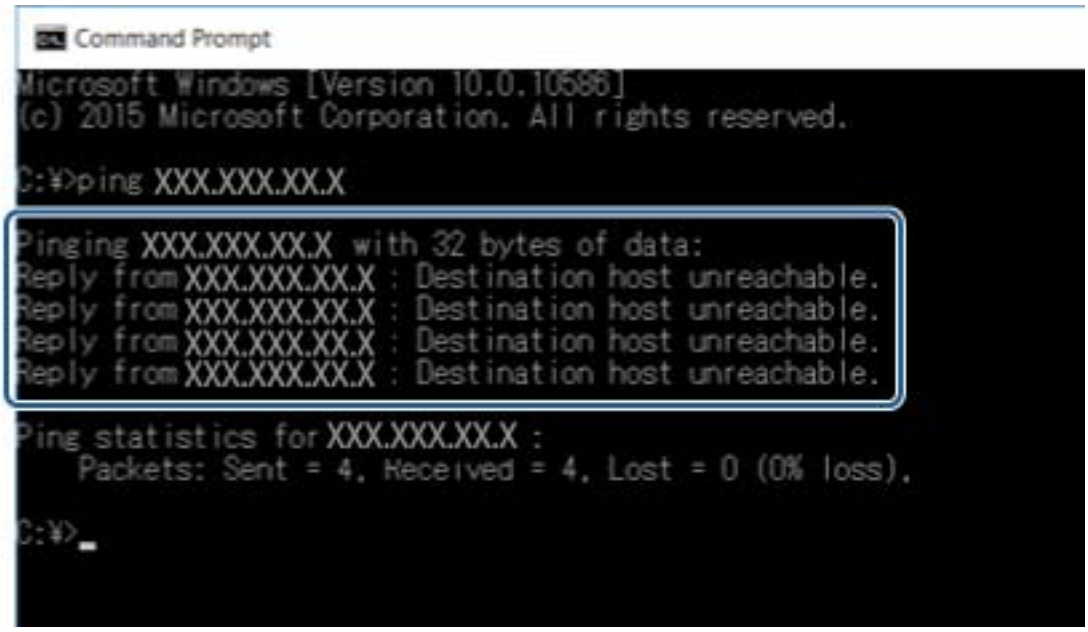
     Klikněte na tlačítko Start, vyberte položku **Všechny programy** nebo **Programy** > **Příslušenství** > **Příkazový řádek**.
3. Zadejte text „ping xxx.xxx.xxx.xxx“ a pak stiskněte klávesu Enter.

   Zadejte IP adresu skeneru pro xxx.xxx.xxx.xxx.
4. Zkontrolujte stav komunikace.

   Pokud skener a počítač komunikují, zobrazí se následující zpráva.



Pokud skener a počítač nekomunikují, zobrazí se následující zpráva.



Kontrola připojení pomocí příkazu Ping — systém Mac OS

Pomocí příkazu Ping můžete zkontrolovat, zda je počítač připojený ke skeneru. Pomocí těchto kroků s příkazem Ping zkontrolujte připojení.

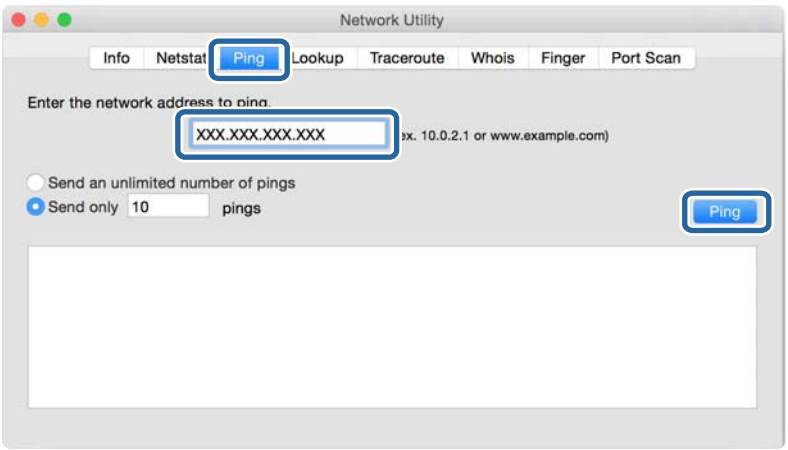
1. Zkontrolujte adresu IP skeneru pro požadované připojení.

   Ke kontrole můžete použít aplikaci Epson Scan 2.

2. Spusťte síťový nástroj.

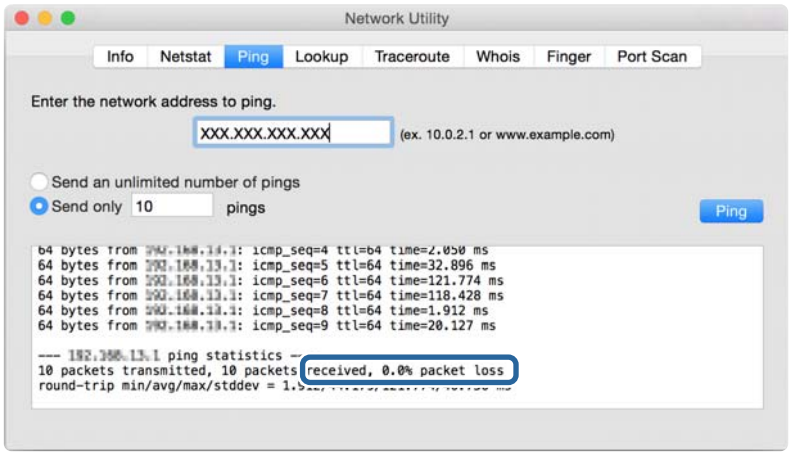
   Zadejte „Síťový nástroj“ do položky **Spotlight**.

3. Klikněte na kartu **Ping**, zadejte adresu IP, kterou jste zkontrolovali v kroku 1, a poté klikněte na položku **Ping**.

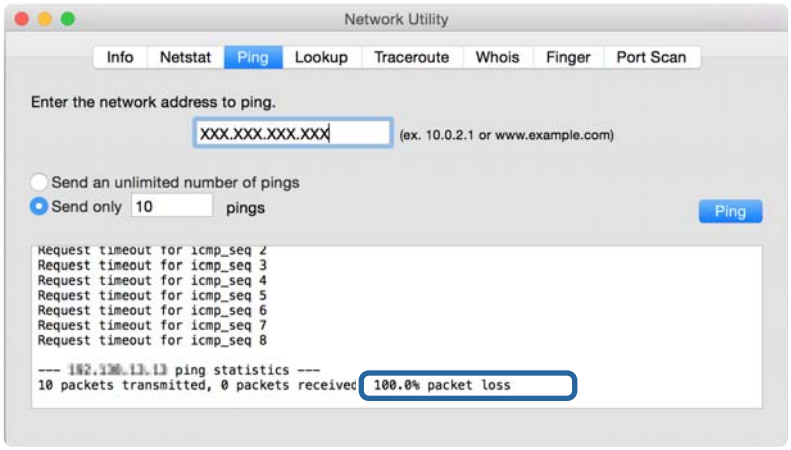


4. Zkontrolujte stav komunikace.

   Pokud skener a počítač komunikují, zobrazí se následující zpráva.



   Pokud skener a počítač nekomunikují, zobrazí se následující zpráva.



Problémy při používání síťového softwaru

Nelze získat přístup k aplikaci Web Config

Je správně nakonfigurována adresa IP skeneru?

Nakonfigurujte adresu IP pomocí aplikace Epson Device Admin nebo EpsonNet Config.

Podporuje váš prohlížeč hromadná šifrování pro možnost Encryption Strength pro protokol SSL/TLS?

Hromadná šifrování pro Encryption Strength pro SSL/TLS jsou následující. K aplikaci Web Config lze přistupovat pouze v prohlížeči, který podporuje následující hromadná šifrování. Zkontrolujte podporu šifrování svého prohlížeče.

- ❏ 80 bitů: AES256/AES128/3DES
- ❏ 112 bitů: AES256/AES128/3DES
- ❏ 128 bitů: AES256/AES128

❏ 192 bitů: AES256

❏ 256 bitů: AES256

Při přístupu k aplikaci Web Config pomocí komunikace SSL (https) se zobrazí zpráva „Zastaralý certifikát“.

Pokud je certifikát zastaralý, získejte jej znovu. Pokud se tato zpráva zobrazí před datem vypršení jeho platnosti, zkontrolujte, zda je správně nakonfigurováno datum skeneru.

Při přístupu k aplikaci Web Config pomocí komunikace SSL (https) se zobrazí zpráva „Název bezpečnostního certifikátu se neshoduje…“.

Adresa IP skeneru zadaná v poli **Common Name** pro vytvoření certifikátu podepsaného svým držitelem nebo pro nástroj CSR se neshoduje s adresou zadanou do prohlížeče. Znovu získejte a naimportujte certifikát nebo změňte název skeneru.

Pro přístup ke skeneru je využíván server proxy.

Používáte-li se skenerem server proxy, je třeba nakonfigurovat nastavení proxy prohlížeče.

❏ Windows:

Vyberte volbu **Ovládací panely** > **Síť a Internet** > **Možnosti Internetu** > **Připojení** > **Nastavení LAN** > **Server proxy** a potom nastavte, aby server proxy nepoužíval místní adresy.

❏ Mac OS:

Vyberte volbu **Předvolby systému** > **Síť** > **Pokročilé** > **Proxy** a potom zaregistrujte místní adresu pro **Vyřadit nastavení proxy pro tyto hostitele a domény**.

Příklad:

192.168.1.*: Místní adresa 192.168.1.XXX, maska podsítě 255.255.255.0

192.168.*.*: Místní adresa 192.168.XXX.XXX, maska podsítě 255.255.0.0

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

➡ „Přiřazování IP adres“ na str. 15

➡ „Přiřazení adresy IP pomocí programu EpsonNet Config“ na str. 56

V aplikaci EpsonNet Config se nezobrazuje název modelu a/nebo adresa IP

Byla vybrána možnost Blokovat, Storno nebo Vypnout při zobrazení obrazovky zabezpečení Windows nebo obrazovky brány firewall?

Pokud jste vybrali volbu **Blokovat**, **Storno** nebo **Vypnout**, v aplikaci EpsonNet Config nebo EpsonNet Setup se nezobrazí adresa IP a název modelu.

Chcete-li tento problém odstranit, zaregistrujte aplikaci EpsonNet Config jako výjimku v bráně firewall systému Windows a v komerčním bezpečnostním softwaru. Používáte-li antivirový nebo bezpečnostní program, ukončete jej a potom zkuste použít aplikaci EpsonNet Config.

Není nastavení časového intervalu chyby komunikace příliš krátké?

Spusťte aplikaci EpsonNet Config a vyberte volbu **Tools** > **Options** > **Timeout** a potom prodlužte časový interval nastavení **Communication Error**. Upozorňujeme vás, že v takovém případě může aplikace EpsonNet Config fungovat pomaleji.

Související informace

➡ „Spuštění aplikace EpsonNet Config — systém Windows“ na str. 56

➡ „Spuštění aplikace EpsonNet Config — systém Mac OS“ na str. 56

Dodatek

Úvod k síťovému softwaru

Následující část popisuje software, který zajišťuje konfiguraci a správu zařízení.

Epson Device Admin

Epson Device Admin je aplikace, která vám umožňuje instalovat zařízení na síti, a poté tato zařízení ovládat a konfigurovat. Můžete získávat podrobné informace o zařízení, jako například stav a spotřební díly, odesílat oznámení o výstrahách a vytvářet zprávy o využití zařízení. Můžete také vytvořit vzor, obsahující položky nastavení, a aplikovat jej na ostatní zařízení jako sdílené nastavení. Aplikaci Epson Device Admin můžete stáhnout z webu podpory Epson. Další informace viz dokumentace nebo nápověda k aplikaci Epson Device Admin.

Spuštění Epson Device Admin (pouze systém Windows)

Vyberte možnost **Všechny programy** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**.

Poznámka:
Pokud se zobrazí varování brány firewall, povolte přístup aplikaci Epson Device Admin.

EpsonNet Config

Aplikace EpsonNet Config umožňuje správci konfigurovat síťová nastavení skeneru, například přiřazení adresy IP a změnu režimu připojení. V operačním systému Windows je podporována funkce dávkového nastavení. Další informace viz dokumentace nebo nápověda k aplikaci EpsonNet Config.

Spuštění aplikace EpsonNet Config — systém Windows

Vyberte možnost **Všechny programy** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

Poznámka:
Pokud se zobrazí varování brány firewall, povolte aplikaci EpsonNet Config přístup.

Spuštění aplikace EpsonNet Config — systém Mac OS

Zvolte položku **Otevřít** > **Aplikace** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**.

EpsonNet SetupManager

Aplikace EpsonNet SetupManager slouží k vytvoření balíčku pro jednoduchou instalaci skeneru, například instalaci a konfiguraci ovladače skeneru a instalaci aplikace Document Capture Pro. Tato aplikace umožňuje správci vytvářet jedinečné softwarové balíčky a distribuovat je mezi skupinami.

Další informace naleznete na regionálních webových stránkách společnosti Epson.

Přiřazení adresy IP pomocí programu EpsonNet Config

Pomocí programu EpsonNet Config můžete přiřadit adresu IP ke skeneru. Program EpsonNet Config umožňuje přiřazení adresy IP ke skeneru, ke kterému ještě nebyla přiřazena, po připojení pomocí ethernetového kabelu.

Přiřazení adresy IP pomocí dávkových nastavení

Vytvoření souboru pro dávková nastavení

Pomocí adresy MAC a názvu modelu jako klíče můžete vytvořit nový soubor SYLK pro nastavení adresy IP.

1. Otevřete tabulkovou aplikaci (jako například Microsoft Excel) nebo textový editor.

2. Jako názvy položek nastavení zadejte do první řádky „Info_MACAddress“, „Info_ModelName“, a „TCPIP_IPAddress“.

   Zadejte položky nastavení pro následující textové řetězce. Pro rozlišení mezi velkým a malým písmem a dvoubajtovými/jednobajtovými znaky, pokud je odlišný jediný znak, položka nebude rozeznána.

   Zadejte název položky nastavení jak je popsáno níže, v opačném případě nástroj EpsonNet Config nebude moci rozpoznat položky nastavení.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. Zadejte adresu MAC, název modelu a adresu IP pro každé síťové rozhraní.

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

4. Zadejte název a uložte jako soubor SYLK (*.slk).

Dávková nastavení s využitím konfiguračního souboru

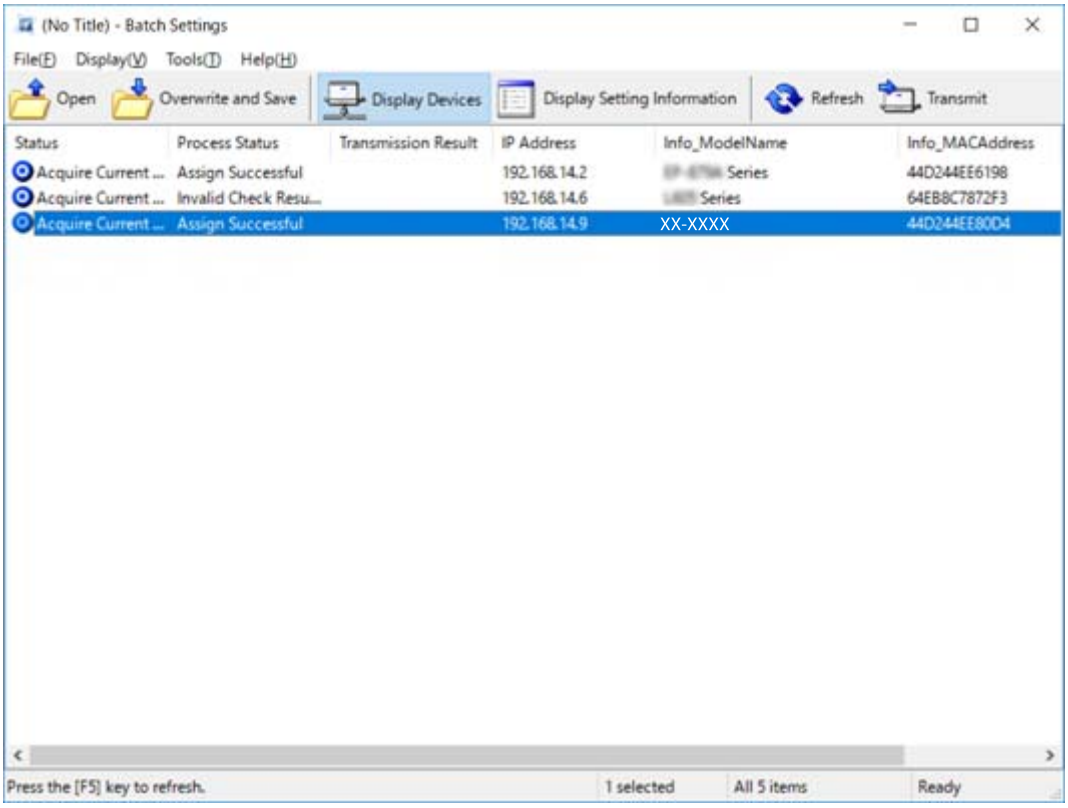
Přiřaďte adresy IP v konfiguračním souboru (soubor SYLK) najednou. Před přiřazením musíte vytvořit konfigurační soubor.

1. Připojte všechna zařízení k síti ethernetovými kabely.
2. Zapněte skener.
3. Spusťte aplikaci EpsonNet Config.

   Zobrazí se seznam skenerů na síti. Zobrazení seznamu může chvíli trvat.
4. Klikněte na položku **Tools** > **Batch Settings**.
5. Klikněte na položku **Open**.
6. Na obrazovce výběru souboru vyberte soubor SYLK (*.slk), který obsahuje potřebná nastavení, a poté klikněte na možnost **Open**.

7. Vyberte zařízení, u kterých chcete provést dávková nastavení, ve sloupci **Status** s nastavením **Unassigned**, a **Process Status** s nastavením **Assign Successful**.

   Pokud chcete vybrat více položek, stiskněte klávesu Ctrl nebo Shift a klikněte nebo pohybem myši proveďte výběr.



8. Klikněte na položku **Transmit**.

9. Pokud se zobrazí obrazovka pro zadání hesla, zadejte heslo a poté klikněte na možnost **OK**.

   Proveďte přenos nastavení.

   Poznámka:
   Informace jsou přenášeny do rozhraní sítě až do dokončení ukazatele průběhu. Nevypínejte zařízení ani bezdrátový adaptér, ani do zařízení neposílejte žádná data.

10. Na obrazovce **Transmitting Settings** klikněte na možnost **OK**.

11. Zkontrolujte vámi nastavený stav zařízení.

    V případě, že je v zařízení zobrazena ikona nebo , zkontrolujte obsah souboru nastavení nebo prověřte, zda restartování zařízení proběhlo v pořádku.

Ikona	Status	Process Status	Vysvětlení
	Setup Complete	Setup Successful	Nastavení bylo standardně dokončeno.
	Setup Complete	Rebooting	Pokud došlo k přenosu informací, je potřeba restartovat všechna zařízení a načíst nová nastavení. Proběhne kontrola schopnosti připojení zařízení po provedení restartu.
	Setup Complete	Reboot Failed	Nelze potvrdit zařízení po přenosu nastavení. Zkontrolujte, zda je zařízení zapnuté, a zda jeho restart proběhl normálně.
	Setup Complete	Searching	Hledání zařízení uvedeného v souboru nastavení.*
	Setup Complete	Search Failed	Nelze kontrolovat zařízení, která již byla nastavena. Zkontrolujte, zda je zařízení zapnuté, a zda jeho restart proběhl normálně.*

    * Pouze pokud se zobrazí informace o nastavení.

Související informace

➡ „Spuštění aplikace EpsonNet Config — systém Windows“ na str. 56
➡ „Spuštění aplikace EpsonNet Config — systém Mac OS“ na str. 56

Přiřazení adresy IP ke každému zařízení

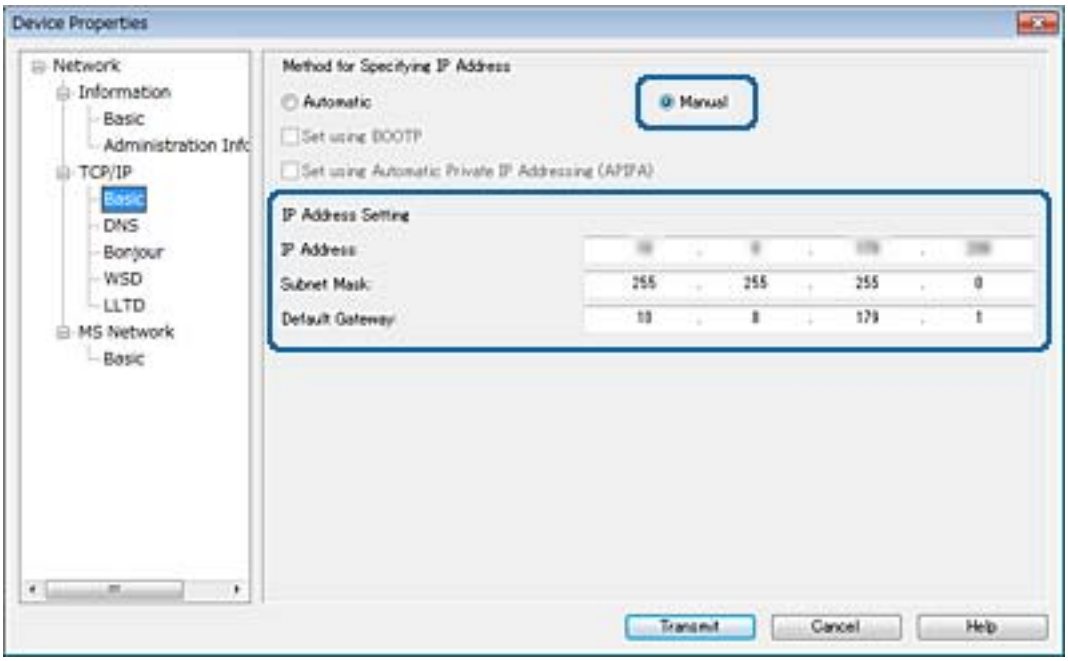
Adresu IP můžete přiřadit ke skeneru pomocí programu EpsonNet Config.

1. Zapněte skener.
2. Připojte skener k síti ethernetovým kabelem.
3. Spusťte aplikaci EpsonNet Config.

   Zobrazí se seznam skenerů na síti. Zobrazení seznamu může chvíli trvat.
4. Poklepejte na skener, ke kterému chcete provést přiřazení.

   Poznámka:
   Pokud jste připojili více skenerů stejného modelu, můžete provést identifikaci skeneru pomocí adresy MAC.
5. Vyberte možnost **Network** > **TCP/IP** > **Basic**.

6. Zadejte adresy pro **IP Address**, **Subnet Mask**, a **Default Gateway**.



Poznámka:
Zadejte statickou adresu, pokud chcete připojit skener k zabezpečené síti.

7. Klikněte na položku **Transmit**.

   Zobrazí se obrazovka s potvrzením přenosu informací.

8. Klikněte na tlačítko **OK**.

   Zobrazí se obrazovka dokončení přenosu.

   Poznámka:
   Informace jsou přeneseny do zařízení a poté se zobrazí zpráva, že byla úspěšně dokončena konfigurace. Nevypínejte zařízení, ani do zařízení neposílejte žádná data.

9. Klikněte na tlačítko **OK**.

Související informace

➡ „Spuštění aplikace EpsonNet Config — systém Windows“ na str. 56
➡ „Spuštění aplikace EpsonNet Config — systém Mac OS“ na str. 56

Používání portu pro skener

Skener používá následující port. Tyto porty by měl dle potřeby povolit a zpřístupnit správce sítě.

Dodatek

Odesílatel (Klient)	Používat	Příjemce (Server)	Protokol	Číslo portu
Skener	Odesílání e-mailů (e-mail s oznámením)	Server SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	Připojení přes protokol POP před protokolem SMTP (e-mail s oznámením)	Server POP	POP3 (TCP)	110
	Řízení WSD	Klientský počítač	WSD (TCP)	5357
	Prohledat počítač při nabízeném skenování z aplikace Document Capture Pro	Klientský počítač	Network Push Scan Discovery (Zjišťování nabízeného síťového skenování)	2968
	Sběr informací o úloze nabízeného skenování z Document Capture Pro	Klientský počítač	Network Push Scan (síťové skenování stiskem tlačítka)	2968
Klientský počítač	Vyhledejte skener z aplikace (například EpsonNet Config) a ovladače skeneru.	Skener	ENPC (UDP)	3289
	Shromážděte a nastavte informace MIB z aplikace (například EpsonNet Config) a ovladače skeneru.	Skener	SNMP (UDP)	161
	Vyhledávání skeneru WSD	Skener	WS-Discovery (UDP)	3702
	Předávání dat skenování z Document Capture Pro	Skener	Síťové skenování (TCP)	1865

Rozšířená nastavení zabezpečení pro podnik

V této části jsou popsány rozšířené funkce zabezpečení.

Nastavení zabezpečení a předcházení nebezpečí

Pokud je zařízení připojeno k síti, můžete k němu přistupovat ze vzdáleného umístění. Navíc toto zařízení může sdílet více lidí, což pomáhá zvýšit provozní efektivitu a pracovní komfort. Nicméně dochází ke zvýšení rizika ilegálního přístupu, používání a neoprávněného upravování dat. Pokud používáte zařízení v prostředí s přístupem na internet, riziko se ještě zvyšuje.

Zařízení Epson jsou vybavena různými bezpečnostními technologiemi, aby se předešlo těmto rizikům.

Nastavte zařízení dle podmínek okolí, které byly vytvořeny na základě informací o prostředí zákazníka.

Název	Typ funkce	Co je třeba nastavit	Čemu je třeba zabránit
Komunikace SSL/TLS	Komunikační cesta počítače a zařízení je šifrována pomocí komunikace SSL/TLS. Obsah komunikace přes prohlížeč je chráněn.	Nastavte certifikát certifikační autority pro server, což je certifikát podepsaný certifikační autoritou pro zařízení.	Zamezte úniku informací o nastavení a obsahu dat přenesených z počítače do skeneru. Přístup na server Epson na internetu ze zařízení lze také chránit aktualizací firmwaru atd.
Filtrování IPsec/IP	Můžete povolit oddělení a odříznutí dat od určitého klienta nebo určitého typu. Jelikož protokol IPsec chrání data pomocí jednotky paketu IP (šifrování a ověřování), můžete bezpečně komunikovat v rámci nezabezpečeného protokolu skenování.	Vytvořte základní zásady a individuální zásady pro nastavení klienta nebo typu dat, které získají přístup k zařízení.	Chraňte se před neoprávněným přístupem, úpravou dat a zachycením dat komunikace se zařízením.
SNMPv3	Jsou přidány funkce, jako například sledování připojených zařízení v síti, integrita dat protokolu SNMP k řízení, šifrování, ověření uživatele atd.	Povolte protokol SNMPv3 a poté nastavte metodu ověřování a šifrování.	Zajistěte změnu nastavení přes síť, zachování důvěrnosti u sledování stavu.
IEEE802.1X	Povoluje pouze uživatele, kteří jsou ověřeni pro ethernetové připojení. Umožňuje použití zařízení pouze povoleným uživatelům.	Nastavení ověření serveru RADIUS (ověřovací server).	Chraňte před neoprávněným přístupem a použitím zařízení.

Název	Typ funkce	Co je třeba nastavit	Čemu je třeba zabránit
Čtení průkazu	Zařízení můžete používat podržením průkazu nad připojeným ověřovaným zařízením. Můžete omezit získávání protokolů pro každého uživatele a zařízení, dále také možnost užívání zařízení a dostupných funkcí pro každého uživatele a skupinu.	Připojte ověřovací zařízení k zařízení a poté nastavte informace uživatele v ověřovacím systému.	Předejdete neoprávněnému použití a zneužití tohoto zařízení.

Související informace

➡ „Komunikace SSL/TLS se skenerem“ na str. 63
➡ „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 71
➡ „Používání protokolu SNMPv3“ na str. 82
➡ „Připojení skeneru k síti IEEE802.1X“ na str. 84

Nastavení funkce zabezpečení

Při nastavování filtrování IPsec/IP nebo IEEE802.1X se doporučuje přistoupit k aplikaci Web Config pomocí SSL/TLS a komunikovat informace o nastavení, redukuje se tím riziko zabezpečení, jakým je například úprava dat nebo zachycení komunikace.

Komunikace SSL/TLS se skenerem

Pokud je certifikát nastaven s použitím komunikace SSL/TLS (Secure Sockets Layer/Transport Layer Security) se skenerem, komunikační cestu mezi počítači můžete šifrovat. Učiňte tak, pokud chcete zabránit vzdálenému a neoprávněnému přístupu.

O digitálním certifikátu

❏ Certifikát podepsaný certifikační agenturou

Certifikát podepsaný certifikační agenturou (CA) je nezbytné získat od certifikační agentury. Použitím certifikátu podepsaného certifikační agenturou lze zajistit bezpečnou komunikaci. Certifikát podepsaný certifikační agenturou lze používat pro každou funkci zabezpečení.

❏ Certifikát CA

Certifikát CA znamená, že třetí strana ověřila identitu serveru. Jedná se o klíčovou součást stylu zabezpečení na základě webové důvěryhodnosti. Je třeba získat certifikát CA pro ověřování serveru od certifikační agentury, která jej vydává.

❏ Samopodpisovatelný certifikát

Samopodpisovatelný certifikát je certifikát, který skener sám vydá a podepíše. Tento certifikát není spolehlivý a nemůže zabránit podvodu. Použijete-li tento certifikát jako certifikát SSL/TLS, může se v prohlížeči zobrazit bezpečnostní upozornění. Tento certifikát lze používat pouze pro komunikaci SSL/TLS.

Související informace

➡ „Získání a importování certifikátu podepsaného certifikační agenturou“ na str. 64
➡ „Odstranění certifikátu podepsaného certifikační agenturou“ na str. 67
➡ „Aktualizování samopodpisovatelného certifikátu“ na str. 68

Získání a importování certifikátu podepsaného certifikační agenturou

Získání certifikátu podepsaného certifikační agenturou

Chcete-li získat certifikát podepsaný certifikační agenturou, vytvořte CSR (Certificate Signing Request) a odešlete jej certifikační agentuře. CSR lze vytvořit pomocí aplikace Web Config a počítače.

Podle pokynů vytvořte CSR a získejte certifikát podepsaný certifikační agenturou pomocí aplikace Web Config. Při vytváření CSR pomocí aplikace Web Config je formát certifikátu PEM/DER.

1. Přistupte na aplikaci Web Config a pak vyberte **Network Security Settings**. Dále vyberte **SSL/TLS** > **Certificate** nebo **IPsec/IP Filtering** > **Client Certificate** nebo **IEEE802.1X** > **Client Certificate**.

2. Klepněte na tlačítko **Generate** v části **CSR**.

   Otevře se stránka pro vytvoření CSR.

3. Zadejte hodnotu pro každou položku.

   Poznámka:
   Dostupná délka klíče a zkratky se mohou lišit podle certifikační agentury. Vytvořte požadavek podle pravidel konkrétní certifikační agentury.

4. Klepněte na tlačítko **OK**.

   Zobrazí se zpráva o dokončení.

5. Vyberte volbu **Network Security Settings**. Dále vyberte **SSL/TLS** > **Certificate** nebo **IPsec/IP Filtering** > **Client Certificate** nebo **IEEE802.1X** > **Client Certificate**.

6. Klepnutím na jedno z tlačítek pro stažení **CSR** podle formátu určeného konkrétní certifikační agenturou stáhněte CSR do počítače.

   > ***Důležité:***
   > *Negenerujte znovu CSR. Pokud tak učiníte, pravděpodobně nebude možné importovat vydaný CA-signed Certificate.*

7. Odešlete CSR certifikační agentuře a získejte CA-signed Certificate.

   Postupujte podle pravidel pro metodu odeslání a formu konkrétní certifikační autority.

8. Uložte vydaný CA-signed Certificate do počítače připojeného ke skeneru.

   Získání CA-signed Certificate je dokončeno uložením certifikátu do umístění.

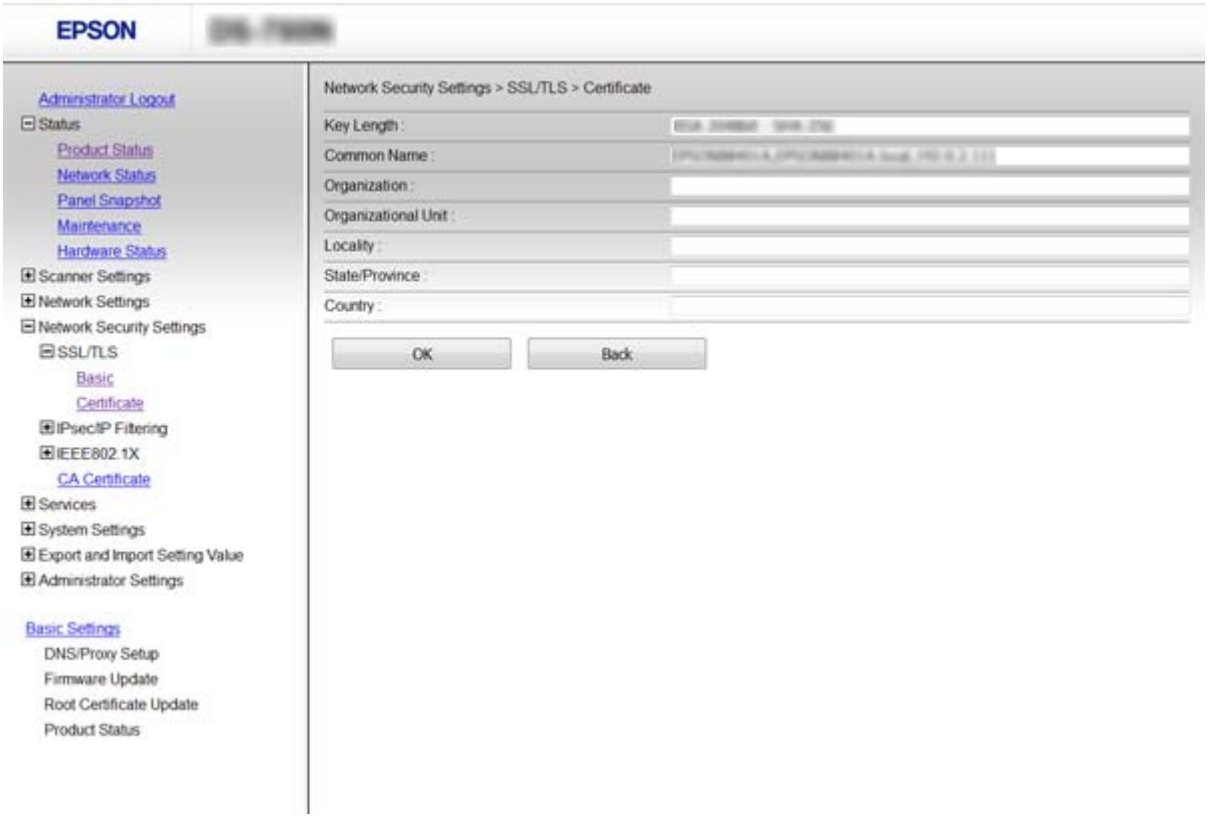
Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

➡ „Položky nastavení nástroje CSR“ na str. 65

➡ „Importování certifikátu podepsaného certifikační agenturou“ na str. 66

Položky nastavení nástroje CSR



Položky	Nastavení a vysvětlení
Key Length	Vyberte délku klíče pro nástroj CSR.
Common Name	Můžete zadat 1 až 128 znaků. Pokud se jedná o adresu IP, musí to být statická adresa IP. Příklad: Adresa URL pro přístup k aplikaci Web Config: https://10.152.12.225 Obecný název: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	Můžete zadat 0 až 64 znaků ve formátu ASCII (0x20–0x7E). Rozlišující názvy můžete oddělit čárkami.
Country	Zadejte kód země jako dvoumístné číslo stanovené normou ISO-3166.

Související informace

➡ „Získání certifikátu podepsaného certifikační agenturou“ na str. 64

Importování certifikátu podepsaného certifikační agenturou

Důležité:

❏ *Zkontrolujte, zda je nastaveno správné datum a čas skeneru.*

❏ *Pokud obdržíte certifikát pomocí CSR vytvořený z aplikace Web Config, můžete naimportovat certifikát jednou.*

1. Přistupte na aplikaci Web Config a pak vyberte **Network Security Settings**. Dále vyberte **SSL/TLS** > **Certificate** nebo **IPsec/IP Filtering** > **Client Certificate** nebo **IEEE802.1X** > **Client Certificate**.

2. Klepněte na tlačítko **Import**.

   Otevře se stránka pro importování certifikátu.

3. Zadejte hodnotu pro každou položku.

   Požadovaná nastavení se mohou lišit podle toho, kde jste vytvořili CSR a podle formátu souboru certifikátu. Zadejte hodnoty pro požadované položky podle následujících pokynů.

   ❏ Certifikát formátu PEM/DER získaný z aplikace Web Config

   ❏ **Private Key**: Nekonfigurujte, protože skener obsahuje soukromý klíč.

   ❏ **Password**: Nekonfigurujte.

   ❏ **CA Certificate 1**/**CA Certificate 2**: Volitelné

   ❏ Certifikát formátu PEM/DER získaný z počítače

   ❏ **Private Key**: Je třeba nastavit.

   ❏ **Password**: Nekonfigurujte.

   ❏ **CA Certificate 1**/**CA Certificate 2**: Volitelné

   ❏ Certifikát formátu PKCS#12 získaný z počítače

   ❏ **Private Key**: Nekonfigurujte.

   ❏ **Password**: Volitelné

   ❏ **CA Certificate 1**/**CA Certificate 2**: Nekonfigurujte.

4. Klepněte na tlačítko **OK**.

   Zobrazí se zpráva o dokončení.

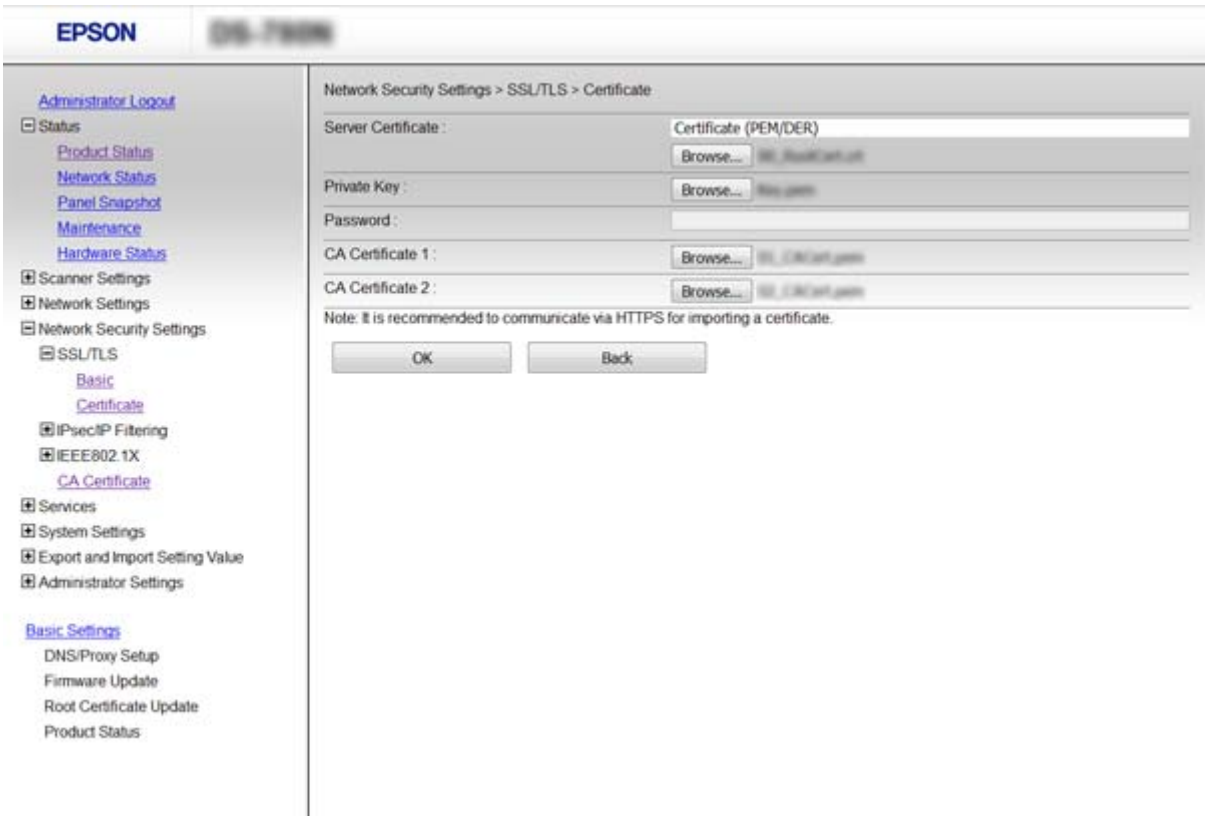
Poznámka:
*Klepnutím na tlačítko **Confirm** ověřte údaje certifikátu.*

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

➡ „Položky nastavení importu certifikátu podepsaného certifikační agenturou“ na str. 67

Položky nastavení importu certifikátu podepsaného certifikační agenturou



Položky	Nastavení a popis
Server Certificate nebo Client Certificate	Vyberte formát certifikátu.
Private Key	Obdržíte-li certifikát formátu PEM/DER pomocí požadavku CSR vytvořeného v počítači, určete soubor soukromého klíče, který se shoduje s certifikátem.
Password	Zadejte heslo pro zašifrování soukromého klíče.
CA Certificate 1	Pokud je formát certifikátu **Certificate (PEM/DER)**, naimportujte certifikát certifikační agentury, která vydala certifikát serveru. Podle potřeby určete soubor.
CA Certificate 2	Pokud je formát certifikátu **Certificate (PEM/DER)**, naimportujte certifikát certifikační agentury, která vydala **CA Certificate 1**. Podle potřeby určete soubor.

Související informace

➡ „Importování certifikátu podepsaného certifikační agenturou“ na str. 66

Odstranění certifikátu podepsaného certifikační agenturou

Naimportovaný certifikát můžete odstranit, když vypršela jeho platnost nebo když šifrované připojení již není zapotřebí.

> ***Důležité:***
> *Pokud obdržíte certifikát pomocí CSR vytvořený z aplikace Web Config, nemůžete znovu naimportovat odstraněný certifikát. V tomto případě vytvořte CSR a znovu získejte certifikát.*

1. Přistupte na aplikaci Web Config a pak vyberte **Network Security Settings**. Dále vyberte **SSL/TLS** > **Certificate** nebo **IPsec/IP Filtering** > **Client Certificate** nebo **IEEE802.1X** > **Client Certificate**.
2. Klikněte na položku **Delete**.
3. V zobrazené zprávě potvrďte, že chcete certifikát odstranit.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Aktualizování samopodpisovatelného certifikátu

Pokud skener podporuje funkci serveru HTTPS, můžete aktualizovat samopodpisovatelný certifikát. Při přístupu k aplikaci Web Config pomocí samopodpisovatelného certifikátu se zobrazí varovná zpráva.

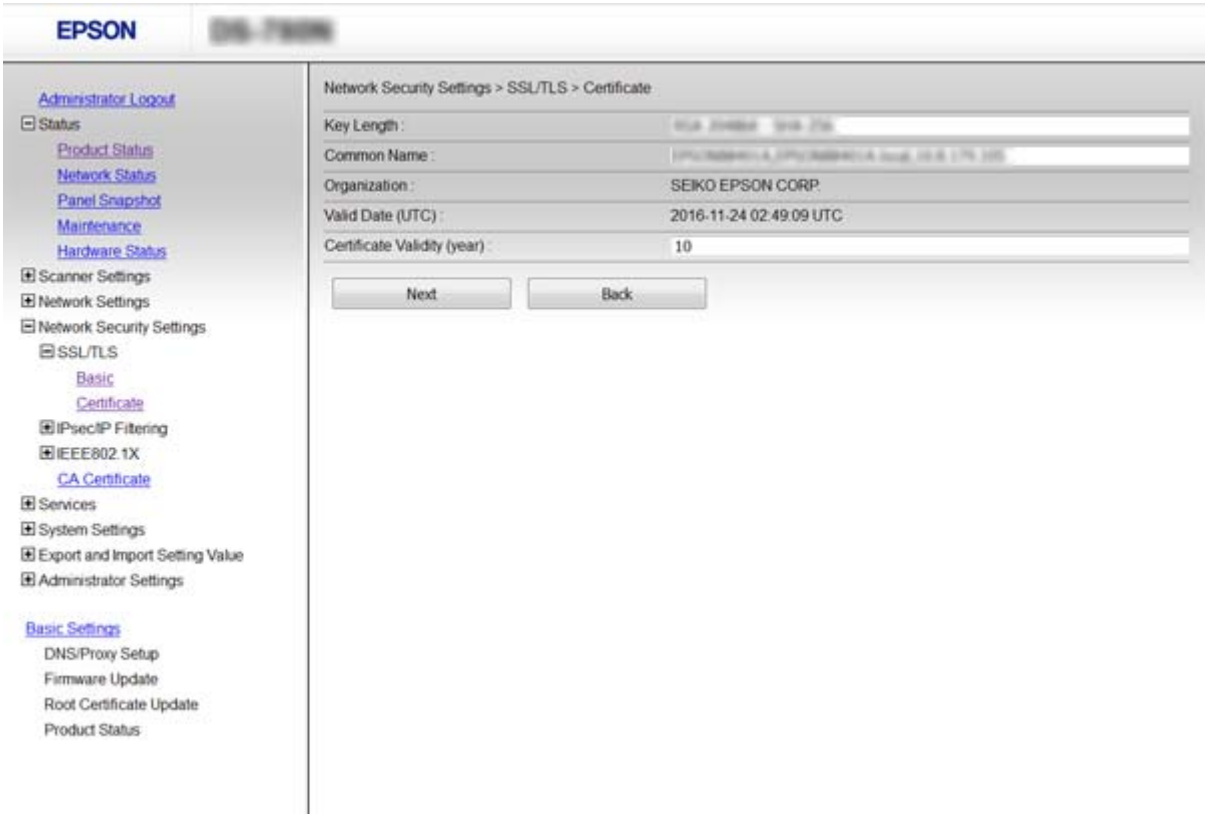
Samopodpisovatelný certifikát používejte dočasně, dokud neobdržíte a nenaimportujete certifikát podepsaný certifikační agenturou.

1. Přistupte na aplikaci Web Config a vyberte **Network Security Settings** > **SSL/TLS** > **Certificate**.
2. Klikněte na položku **Update**.
3. Zadejte informace do pole **Common Name**.

   Zadejte adresu IP nebo jiný identifikátor, například název FQDN pro skener. Můžete zadat 1 až 128 znaků.

   Poznámka:
   Rozlišující název (CN) můžete oddělit čárkami.

4. Určete interval platnosti certifikátu.



5. Klikněte na tlačítko **Next**.

   Zobrazí se zpráva s potvrzením.

6. Klikněte na tlačítko **OK**.

   Skener je aktualizován.

Poznámka:
*Klepnutím na tlačítko **Confirm** ověřte údaje certifikátu.*

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Konfigurování CA Certificate

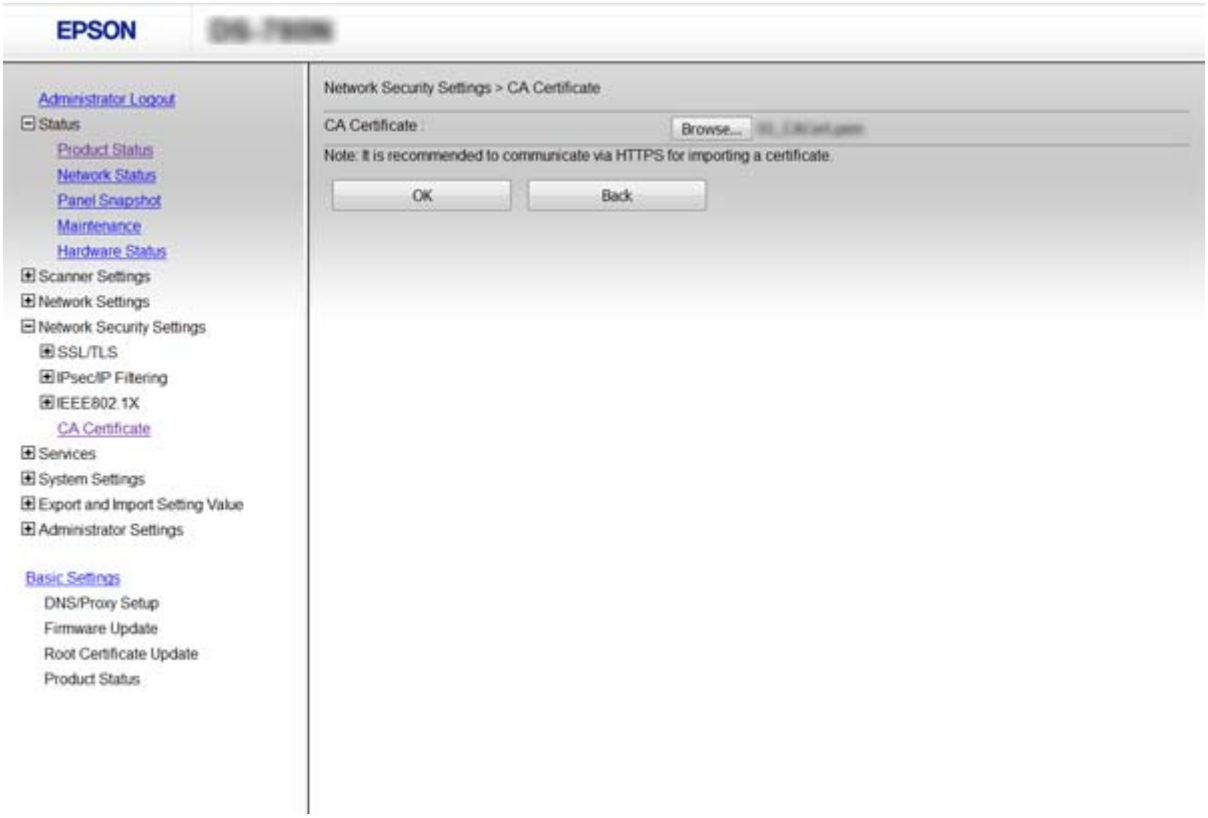
Můžete importovat, zobrazit nebo odstranit CA Certificate.

Importování CA Certificate

1. Přistupte na aplikaci Web Config a pak vyberte **Network Security Settings** > **CA Certificate**.

2. Klepněte na tlačítko **Import**.

3. Určete CA Certificate, který chcete importovat.



4. Klepněte na tlačítko **OK**.

Pod dokončení importování budete přesměrováni zpět na obrazovku **CA Certificate** a zobrazí se naimportovaný CA Certificate.

Související informace

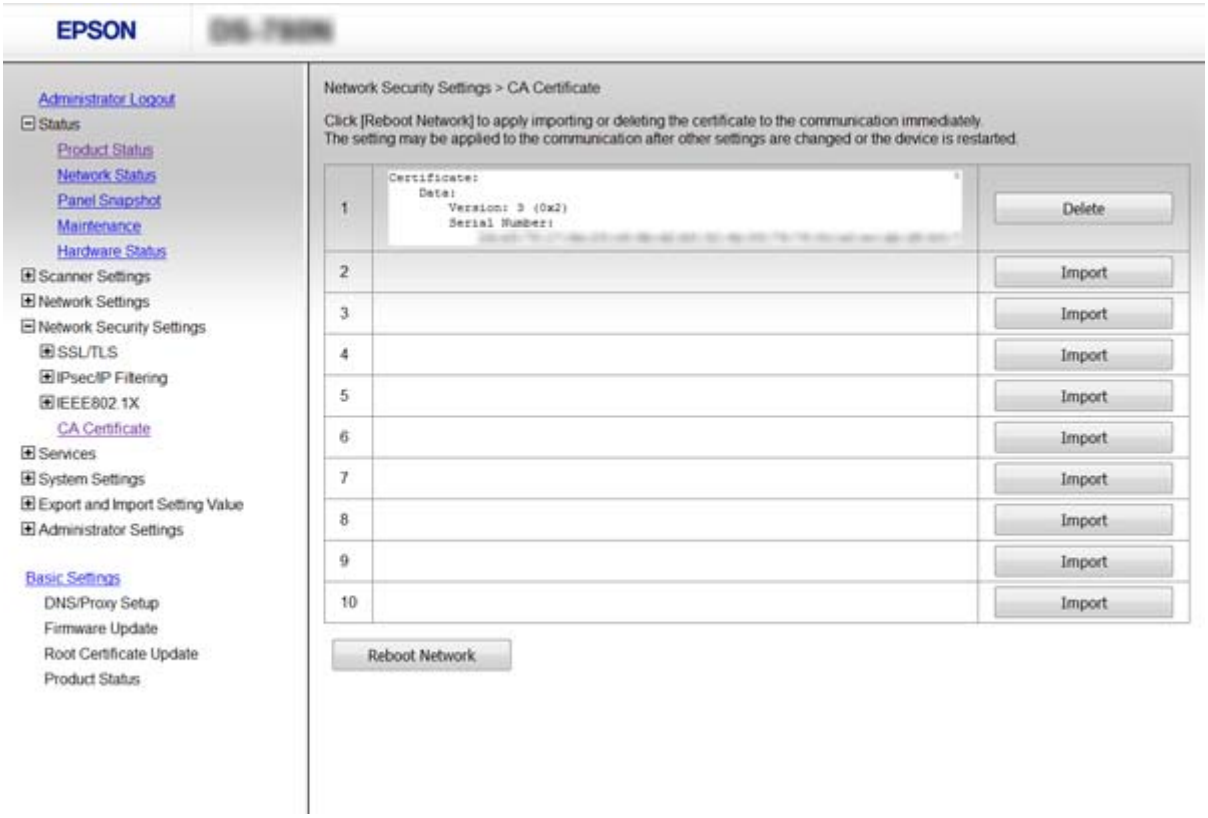
➡ „Přístup k aplikaci Web Config“ na str. 23

Odstranění CA Certificate

Můžete odstranit naimportovaný CA Certificate.

1. Přistupte na aplikaci Web Config a pak vyberte **Network Security Settings** > **CA Certificate**.

2. Klepněte na **Delete** vedle CA Certificate, který chcete odstranit.



3. V zobrazené zprávě potvrďte, že chcete certifikát odstranit.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Šifrovaná komunikace pomocí filtrování IPsec/IP

O aplikaci IPsec/IP Filtering

Pokud skener podporuje filtrování IPsec/IP, můžete filtrovat provoz podle adres IP, služeb a portu. Zkombinováním filtrování můžete nakonfigurovat skener tak, aby akceptoval nebo blokoval specifikované klienty a data. Kromě toho můžete zvýšit úroveň zabezpečení použitím IPsec.

Chcete-li filtrovat provoz, nakonfigurujte výchozí zásadu. Výchozí zásada se vztahuje na každého uživatele nebo skupinu, která se připojuje ke skeneru. Pro jemnější řízení uživatelů nebo skupin uživatelů nakonfigurujte zásady skupiny. Zásada skupiny je jedno nebo více pravidel použitých na uživatele nebo skupinu uživatelů. Skener řídí pakety IP, které se shodují s nakonfigurovanými zásadami. Pakety IP jsou ověřovány v pořadí zásad skupiny 1 až 10, než podle výchozí zásady.

Poznámka:
Počítače s nainstalovaným systémem Windows Vista nebo novějším a Windows Server 2008 nebo novějším podporují IPsec.

Konfigurování Default Policy

1. Přistupte na aplikaci Web Config a vyberte **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Zadejte hodnotu pro každou položku.
3. Klepněte na tlačítko **Next**.

   Zobrazí se zpráva s potvrzením.
4. Klepněte na tlačítko **OK**.

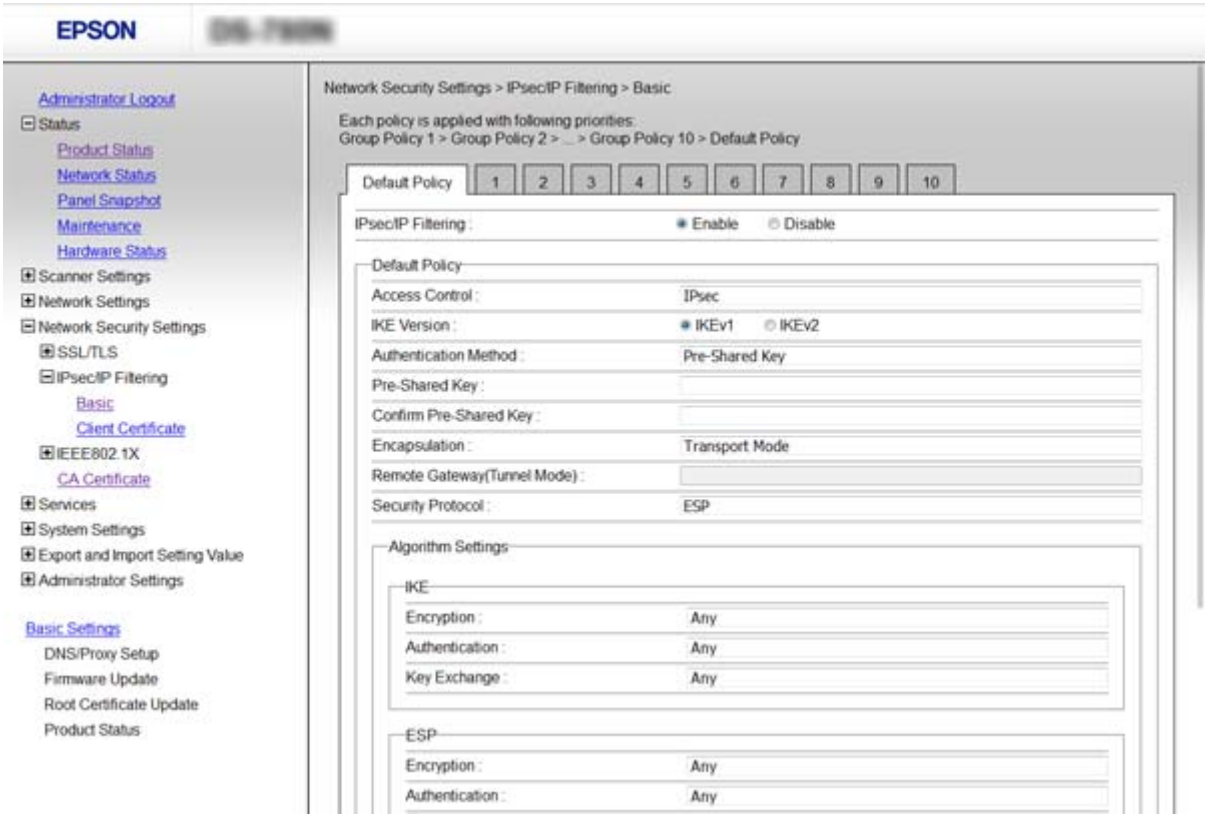
   Skener je aktualizován.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

➡ „Položky nastavení Default Policy“ na str. 72

Položky nastavení Default Policy



Položky	Nastavení a vysvětlení
IPsec/IP Filtering	Můžete povolit nebo zakázat funkci filtrování IPsec/IP.

Rozšířená nastavení zabezpečení pro podnik

Položky	Nastavení a vysvětlení	
Access Control	Nakonfigurujte metodu řízení pro provoz paketů IP.	
	Permit Access	Výběrem této volby povolíte průchod nakonfigurovaným paketům IP.
	Refuse Access	Výběrem této volby odmítnete průchod nakonfigurovaným paketům IP.
	IPsec	Výběrem této volby povolíte průchod nakonfigurovaným paketům IPsec.
IKE Version	Jako verzi IKE vyberte IKEv1 nebo IKEv2. Vyberte jednu z možností dle typu zařízení, ke kterému je skener připojen.	
IKEv1	Následující položky se zobrazí, pokud vyberete pro položku **IKE Version** hodnotu **IKEv1**.	
	Authentication Method	Aby bylo možné vybrat volbu **Certificate**, je třeba předem získat a naimportovat certifikát s podpisem certifikační agentury.
	Pre-Shared Key	Vyberete-li volbu **Pre-Shared Key** pro položku **Authentication Method**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Confirm Pre-Shared Key	Zadejte klíč nakonfigurovaný pro potvrzení.
IKEv2	Následující položky se zobrazí, pokud vyberete pro položku **IKE Version** hodnotu **IKEv2**.	
Local	Authentication Method	Aby bylo možné vybrat volbu **Certificate**, je třeba předem získat a naimportovat certifikát s podpisem certifikační agentury.
	ID Type	Vyberte typ ID skeneru.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Distinguished Name**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „=“. **IP Address**: Zadejte formát IPv4 nebo IPv6. **FQDN**: Zadejte kombinaci 1 až 255 znaků. Použít můžete písmena A–Z, a–z, číslice 0–9, znak „-“ a tečku (.). **Email Address**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „@“. **Key ID**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E).
	Pre-Shared Key	Vyberete-li volbu **Pre-Shared Key** pro položku **Authentication Method**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Confirm Pre-Shared Key	Zadejte klíč nakonfigurovaný pro potvrzení.

Rozšířená nastavení zabezpečení pro podnik

Položky	Nastavení a vysvětlení	
Remote	Authentication Method	Aby bylo možné vybrat volbu **Certificate**, je třeba předem získat a naimportovat certifikát s podpisem certifikační agentury.
	ID Type	Vyberte typ ID pro zařízení, které chcete ověřit.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Distinguished Name**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „=“. **IP Address**: Zadejte formát IPv4 nebo IPv6. **FQDN**: Zadejte kombinaci 1 až 255 znaků. Použít můžete písmena A–Z, a–z, číslice 0–9, znak „-“ a tečku (.). **Email Address**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „@“. **Key ID**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E).
	Pre-Shared Key	Vyberete-li volbu **Pre-Shared Key** pro položku **Authentication Method**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Confirm Pre-Shared Key	Zadejte klíč nakonfigurovaný pro potvrzení.
Encapsulation	Vyberete-li volbu **IPsec** pro položku **Access Control**, je třeba nakonfigurovat režim zapouzdření.	
	Transport Mode	Vyberte tuto volbu, používáte-li skener ve stejné místní síti LAN. Pakety IP vrstvy 4 nebo pozdější jsou šifrovány.
	Tunnel Mode	Pokud skener používáte v síti s přístupem k Internetu jako IPsec-VPN, vyberte tuto možnost. Záhlaví a data paketů IP jsou šifrována.
Remote Gateway(Tunnel Mode)	Vyberete-li volbu **Tunnel Mode** pro položku **Encapsulation**, zadejte adresu brány o délce 1 až 39 znaků.	
Security Protocol	**IPsec** pro **Access Control**, vyberte možnost.	
	ESP	Výběrem této volby bude zajištěna integrita ověřování a dat, která budou šifrována.
	AH	Výběrem této volby bude zajištěna integrita ověřování a dat. I když je šifrování dat zakázáno, můžete použít IPsec.
Algorithm Settings		
IKE	Encryption	Vyberte algoritmus šifrování pro IKE. Položky se mohou lišit v závislosti na verzi IKE.
	Authentication	Vyberte algoritmus ověřování pro IKE.
	Key Exchange	Vyberte algoritmus výměny klíčů pro IKE. Položky se mohou lišit v závislosti na verzi IKE.

Položky	Nastavení a vysvětlení	
ESP	Encryption	Vyberte algoritmus šifrování pro ESP. Tato funkce je dostupná, je-li **ESP** nastavený na **Security Protocol**.
	Authentication	Vyberte algoritmus ověřování pro ESP. Tato funkce je dostupná, je-li **ESP** nastavený na **Security Protocol**.
AH	Authentication	Vyberte algoritmus šifrování pro AH. Tato funkce je dostupná, je-li **AH** nastavený na **Security Protocol**.

Související informace

➡ „Konfigurování Default Policy“ na str. 72

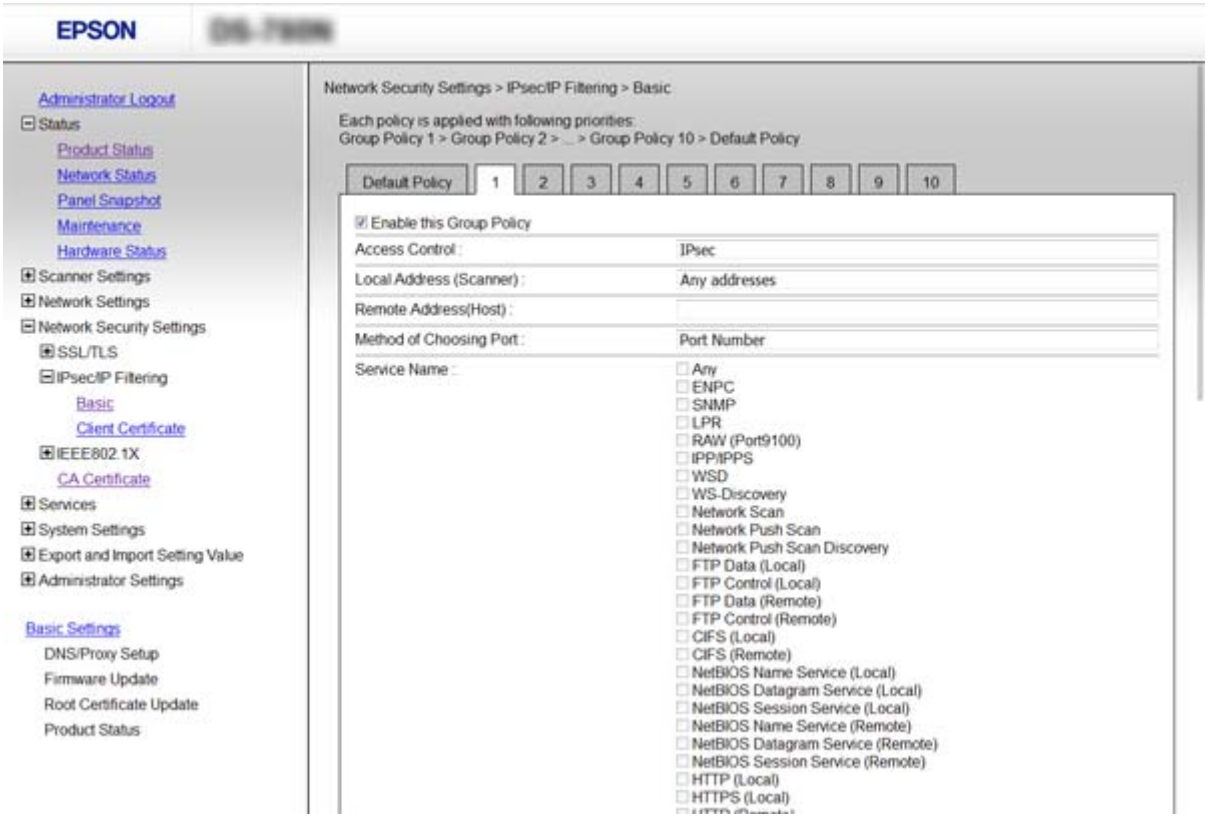
Konfigurování Group Policy

1. Přistupte na aplikaci Web Config a vyberte **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Klepněte na číslovanou kartu, kterou chcete nakonfigurovat.
3. Zadejte hodnotu pro každou položku.
4. Klepněte na tlačítko **Next**.
   Zobrazí se zpráva s potvrzením.
5. Klepněte na tlačítko **OK**.
   Skener je aktualizován.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Položky nastavení Group Policy“ na str. 76

Položky nastavení Group Policy



Položky	Nastavení a vysvětlení	
Enable this Group Policy	Můžete povolit nebo zakázat zásadu skupiny.	
Access Control	Nakonfigurujte metodu řízení pro provoz paketů IP.	
	Permit Access	Výběrem této volby povolíte průchod nakonfigurovaným paketům IP.
	Refuse Access	Výběrem této volby odmítnete průchod nakonfigurovaným paketům IP.
	IPsec	Výběrem této volby povolíte průchod nakonfigurovaným paketům IPsec.
Local Address (Scanner)	Vyberte adresu IPv4 nebo IPv6, která odpovídá vašemu síťovému prostředí. Pokud je adresa IP přiřazena automaticky, můžete vybrat nastavení **Use auto-obtained IPv4 address**.	
Remote Address(Host)	Zadejte adresu IP zařízení, jehož přístup chcete řídit. Adresa IP musí mít délku 43 znaků nebo méně. Nezadáte-li adresu IP, jsou všechny adresy řízené. ***Poznámka:*** *Pokud je některá adresa IP přiřazena automaticky (tzn. je přiřazena serverem DHCP), připojení nemusí být dostupné. Nakonfigurujte statickou adresu IP.*	
Method of Choosing Port	Vyberte metodu určení portů.	
Service Name	Vyberete-li volbu **Service Name** pro položku **Method of Choosing Port**, vyberte některou volbu.	

Rozšířená nastavení zabezpečení pro podnik

Položky	Nastavení a vysvětlení	
Transport Protocol	Vyberete-li volbu **Port Number** pro položku **Method of Choosing Port**, je třeba nakonfigurovat režim zapouzdření.	
	Any Protocol	Tato volba slouží k řízení všech typů protokolů.
	TCP	Tato volba slouží k řízení dat pro jednosměrové vysílání.
	UDP	Tato volba slouží k řízení dat pro vysílání a vícesměrové vysílání.
	ICMPv4	Tato volba slouží k ovládání příkazu ping.
Local Port	Vyberete-li volbu **Port Number** u položky **Method of Choosing Port** a vyberete-li volbu **TCP** nebo **UDP** u položky **Transport Protocol**, zadejte čísla portů k řízení příjmu paketů a oddělte je čárkami. Lze zadat maximálně 10 čísel portů. Příklad: 20,80,119,5220 Nezadáte-li číslo portu, jsou všechny porty řízené.	
Remote Port	Vyberete-li volbu **Port Number** u položky **Method of Choosing Port** a vyberete-li volbu **TCP** nebo **UDP** u položky **Transport Protocol**, zadejte čísla portů k řízení vysílání paketů a oddělte je čárkami. Lze zadat maximálně 10 čísel portů. Příklad: 25,80,143,5220 Nezadáte-li číslo portu, jsou všechny porty řízené.	
IKE Version	Jako verzi IKE vyberte IKEv1 nebo IKEv2. Vyberte jednu z možností dle typu zařízení, ke kterému je skener připojen.	
IKEv1	Následující položky se zobrazí, pokud vyberete pro položku **IKE Version** hodnotu **IKEv1**.	
	Authentication Method	Vyberete-li volbu **IPsec** pro položku **Access Control**, vyberte některou volbu. Použitý certifikát je společný s výchozí zásadou.
	Pre-Shared Key	Vyberete-li volbu **Pre-Shared Key** pro položku **Authentication Method**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Confirm Pre-Shared Key	Zadejte klíč nakonfigurovaný pro potvrzení.
IKEv2	Následující položky se zobrazí, pokud vyberete pro položku **IKE Version** hodnotu **IKEv2**.	

Rozšířená nastavení zabezpečení pro podnik

Položky	Nastavení a vysvětlení	
Local	Authentication Method	Vyberete-li volbu **IPsec** pro položku **Access Control**, vyberte některou volbu. Použitý certifikát je společný s výchozí zásadou.
	ID Type	Vyberte typ ID skeneru.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Distinguished Name**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „=“. **IP Address**: Zadejte formát IPv4 nebo IPv6. **FQDN**: Zadejte kombinaci 1 až 255 znaků. Použít můžete písmena A–Z, a–z, číslice 0–9, znak „-“ a tečku (.). **Email Address**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „@“. **Key ID**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E).
	Pre-Shared Key	Vyberete-li volbu **Pre-Shared Key** pro položku **Authentication Method**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Confirm Pre-Shared Key	Zadejte klíč nakonfigurovaný pro potvrzení.
Remote	Authentication Method	Vyberete-li volbu **IPsec** pro položku **Access Control**, vyberte některou volbu. Použitý certifikát je společný s výchozí zásadou.
	ID Type	Vyberte typ ID pro zařízení, které chcete ověřit.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Distinguished Name**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „=“. **IP Address**: Zadejte formát IPv4 nebo IPv6. **FQDN**: Zadejte kombinaci 1 až 255 znaků. Použít můžete písmena A–Z, a–z, číslice 0–9, znak „-“ a tečku (.). **Email Address**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Zadání musí obsahovat „@“. **Key ID**: Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E).
	Pre-Shared Key	Vyberete-li volbu **Pre-Shared Key** pro položku **Authentication Method**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Confirm Pre-Shared Key	Zadejte klíč nakonfigurovaný pro potvrzení.

Rozšířená nastavení zabezpečení pro podnik

Položky	Nastavení a vysvětlení	
Encapsulation	Vyberete-li volbu **IPsec** pro položku **Access Control**, je třeba nakonfigurovat režim zapouzdření.	
	Transport Mode	Vyberte tuto volbu, používáte-li skener ve stejné místní síti LAN. Pakety IP vrstvy 4 nebo pozdější jsou šifrovány.
	Tunnel Mode	Pokud skener používáte v síti s přístupem k Internetu jako IPsec-VPN, vyberte tuto možnost. Záhlaví a data paketů IP jsou šifrována.
Remote Gateway(Tunnel Mode)	Vyberete-li volbu **Tunnel Mode** pro položku **Encapsulation**, zadejte adresu brány o délce 1 až 39 znaků.	
Security Protocol	Vyberete-li volbu **IPsec** pro položku **Access Control**, vyberte některou volbu.	
	ESP	Výběrem této volby bude zajištěna integrita ověřování a dat, která budou šifrována.
	AH	Výběrem této volby bude zajištěna integrita ověřování a dat. I když je šifrování dat zakázáno, můžete použít IPsec.
Algorithm Settings		
IKE	Encryption	Vyberte algoritmus šifrování pro IKE. Položky se mohou lišit v závislosti na verzi IKE.
	Authentication	Vyberte algoritmus ověřování pro IKE.
	Key Exchange	Vyberte algoritmus výměny klíčů pro IKE. Položky se mohou lišit v závislosti na verzi IKE.
ESP	Encryption	Vyberte algoritmus šifrování pro ESP. Tato funkce je dostupná, je-li **ESP** nastavený na **Security Protocol**.
	Authentication	Vyberte algoritmus ověřování pro ESP. Tato funkce je dostupná, je-li **ESP** nastavený na **Security Protocol**.
AH	Authentication	Vyberte algoritmus ověřování pro AH. Tato funkce je dostupná, je-li **AH** nastavený na **Security Protocol**.

Související informace

➡ „Konfigurování Group Policy“ na str. 75

➡ „Kombinace Local Address (Scanner) a Remote Address(Host) v Group Policy“ na str. 79

➡ „Reference názvu služby v zásadách skupiny“ na str. 80

Kombinace Local Address (Scanner) a Remote Address(Host) v Group Policy

	Nastavení Local Address (Scanner)		
	IPv4	IPv6*2	Any addresses*3

Nastavení Remote Address(Host)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Prázdná	✓	✓	✓

*1 Pokud je zvoleno **IPsec** pro funkci **Access Control**, nemůžete určit délku předpony.

*2 Pokud je zvoleno **IPsec** pro funkci **Access Control**, můžete vybrat místní adresu propojení (fe80::), ale zásady skupiny budou zakázány.

*3 Vyjma místních adres propojení IPv6.

Reference názvu služby v zásadách skupiny

Poznámka:
Nedostupné služby jsou zobrazeny, ale nelze je vybrat.

Název služby	Typ protokolu	Číslo místního portu	Číslo vzdáleného portu	Řízené funkce
Any	–	–	–	Všechny služby
ENPC	UDP	3289	Jakýkoli port	Vyhledávání skeneru z aplikací, jako je EpsonNet Config, a ovladače skeneru
SNMP	UDP	161	Jakýkoli port	Vyžádání a konfigurace MIB z aplikací, jako jsou EpsonNet Config a ovladače skeneru Epson
WSD	TCP	Jakýkoli port	5357	Řízení WSD
WS-Discovery	UDP	3702	Jakýkoli port	Vyhledávání skeneru z WSD
Network Scan	TCP	1865	Jakýkoli port	Předávání dat skenování z Document Capture Pro
Network Push Scan Discovery	UDP	2968	Jakýkoli port	Vyhledání počítače ze skeneru.
Network Push Scan	TCP	Jakýkoli port	2968	Vyžádání informací o úloze skenování stiskem tlačítka z aplikace Document Capture Pro nebo Document Capture
HTTP (Local)	TCP	80	Jakýkoli port	Server HTTP(S) (předávání dat Web Config a WSD)
HTTPS (Local)	TCP	443	Jakýkoli port	
HTTP (Remote)	TCP	Jakýkoli port	80	Klient HTTP(S) (komunikující mezi aktualizací firmwaru a kořenového certifikátu)
HTTPS (Remote)	TCP	Jakýkoli port	443	

Příklady konfigurace IPsec/IP Filtering

Pouze přijímání paketů IPsec

Tento příklad slouží pouze ke konfiguraci výchozí zásady.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **IPsec**

❏ **Authentication Method**: **Pre-Shared Key**

❏ **Pre-Shared Key**: zadejte až 127 znaků.

Group Policy:

Nekonfigurujte.

Přijetí naskenovaného snímku pomocí aplikace Epson Scan 2 a nastavení skeneru

Tento příklad umožňuje komunikaci skenovaných dat a konfigurace skeneru z určených služeb.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**: **Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: zaškrtněte pole.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: adresa IP klienta

❏ **Method of Choosing Port**: **Service Name**

❏ **Service Name**: zaškrtněte pole **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** and **HTTPS (Local)**.

Příjem přístupu pouze z určené adresy IP

Tento příklad umožňuje přístup na skener z určené adresy IP.

Default Policy:

❏ **IPsec/IP Filtering**: **Enable**

❏ **Access Control**:**Refuse Access**

Group Policy:

❏ **Enable this Group Policy**: zaškrtněte pole.

❏ **Access Control**: **Permit Access**

❏ **Remote Address(Host)**: adresa IP klienta správce

Poznámka:
Bez ohledu na konfiguraci zásady bude klient schopen přistoupit na skener a zkonfigurovat jej.

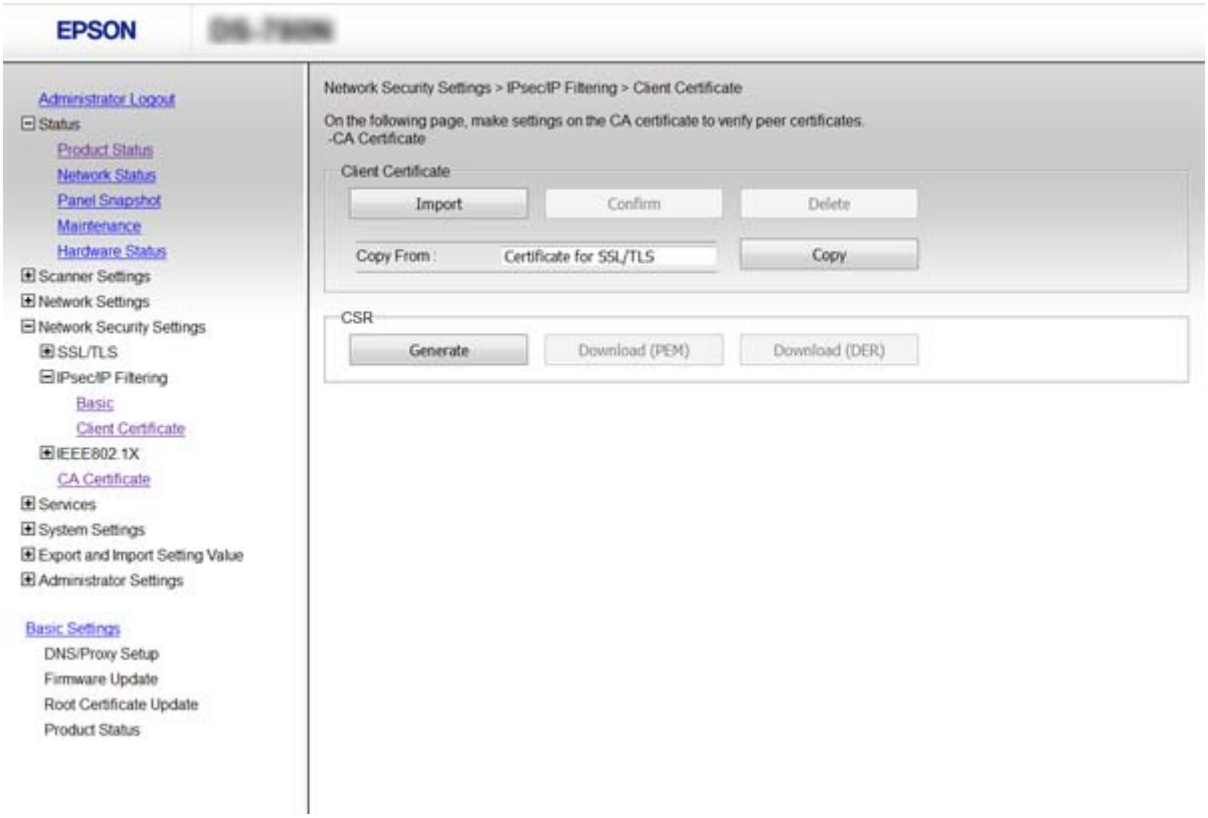
Konfigurování certifikátu pro IPsec/IP Filtering

Nakonfigurujte certifikát klienta pro filtrování IPsec/IP. Chcete-li nakonfigurovat certifikační autoritu, přejděte na **CA Certificate**.

1. Přistupte na aplikaci Web Config a vyberte **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**.

2. Naimportujte certifikát do **Client Certificate**.

   Pokud jste již naimportovali certifikát vydaný certifikační autoritou v IEEE802.1X nebo SSL/TLS, můžete zkopírovat certifikát a použít jej při filtrování IPsec/IP. Chcete-li zkopírovat certifikát, vyberte jej v **Copy From** a potom klepněte na **Copy**.



Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

➡ „Získání a importování certifikátu podepsaného certifikační agenturou“ na str. 64

Používání protokolu SNMPv3

O protokolu SNMPv3

SNMP je protokol, který pomocí sledování a řízení shromažďuje údaje o zařízeních, připojených k síti. SNMPv3 je vylepšená verze bezpečnostní funkce správy.

Při používání SNMPv3 je možné ověřovat a šifrovat sledování stavu a změny nastavení komunikace SNMP (paket) a chránit tak komunikaci SNMP (packet) před riziky na síti, jako je například odposlouchávání, přisvojení totožnosti či neoprávněný zásah.

Konfigurování protokolu SNMPv3

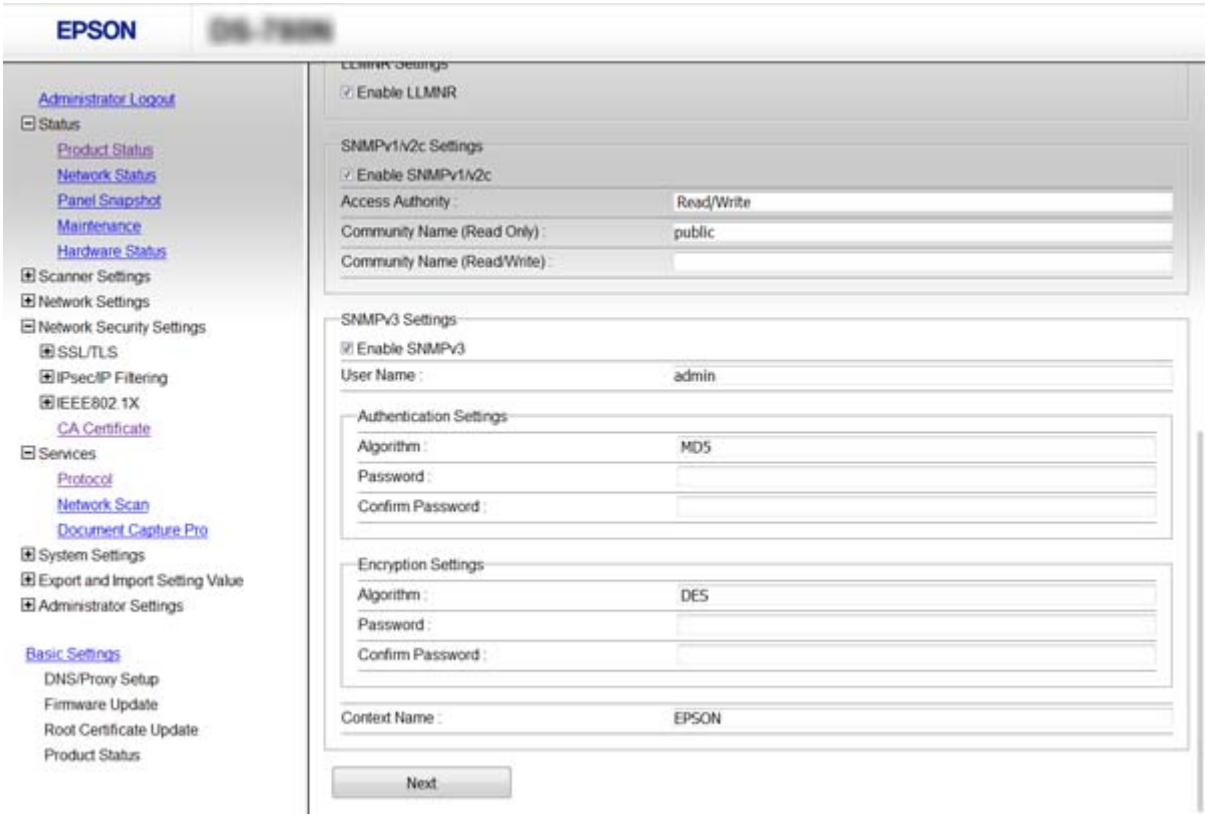
Pokud skener podporuje protokol SNMPv3, můžete monitorovat a řídit přístupy ke skeneru.

1. Přistupte na aplikaci Web Config a vyberte **Services** > **Protocol**.
2. Zadejte hodnotu pro každou položku **SNMPv3 Settings**.
3. Klepněte na tlačítko **Next**.
   Zobrazí se zpráva s potvrzením.
4. Klepněte na tlačítko **OK**.
   Skener je aktualizován.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Položky nastavení SNMPv3“ na str. 83

Položky nastavení SNMPv3



Položky	Nastavení a popis
Enable SNMPv3	Když je toto políčko zaškrtnuto, protokol SNMPv3 je povolen.
User Name	Zadejte 1 až 32 znaků za použití 1bajtových znaků.
Authentication Settings	
Algorithm	Vyberte algoritmus pro ověření.

Položky	Nastavení a popis
Password	Zadejte 8 až 32 znaků ve formátu ASCII (0x20-0x7E).
Confirm Password	Zadejte nakonfigurované heslo pro potvrzení.
Encryption Settings	
Algorithm	Vyberte algoritmus pro šifrování.
Password	Zadejte 8 až 32 znaků ve formátu ASCII (0x20-0x7E).
Confirm Password	Zadejte nakonfigurované heslo pro potvrzení.
Context Name	Zadejte 1 až 32 znaků za použití 1bajtových znaků.

Související informace

➡ „Konfigurování protokolu SNMPv3“ na str. 82

Připojení skeneru k síti IEEE802.1X

Konfigurování sítě IEEE802.1X

Pokud skener podporuje síť IEEE802.1X, můžete používat skener v síti s ověřováním, která je připojena k serveru RADIUS a k rozbočovači jako ověřovateli.

1. Přistupte na aplikaci Web Config a vyberte **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. Zadejte hodnotu pro každou položku.
3. Klikněte na tlačítko **Next**.

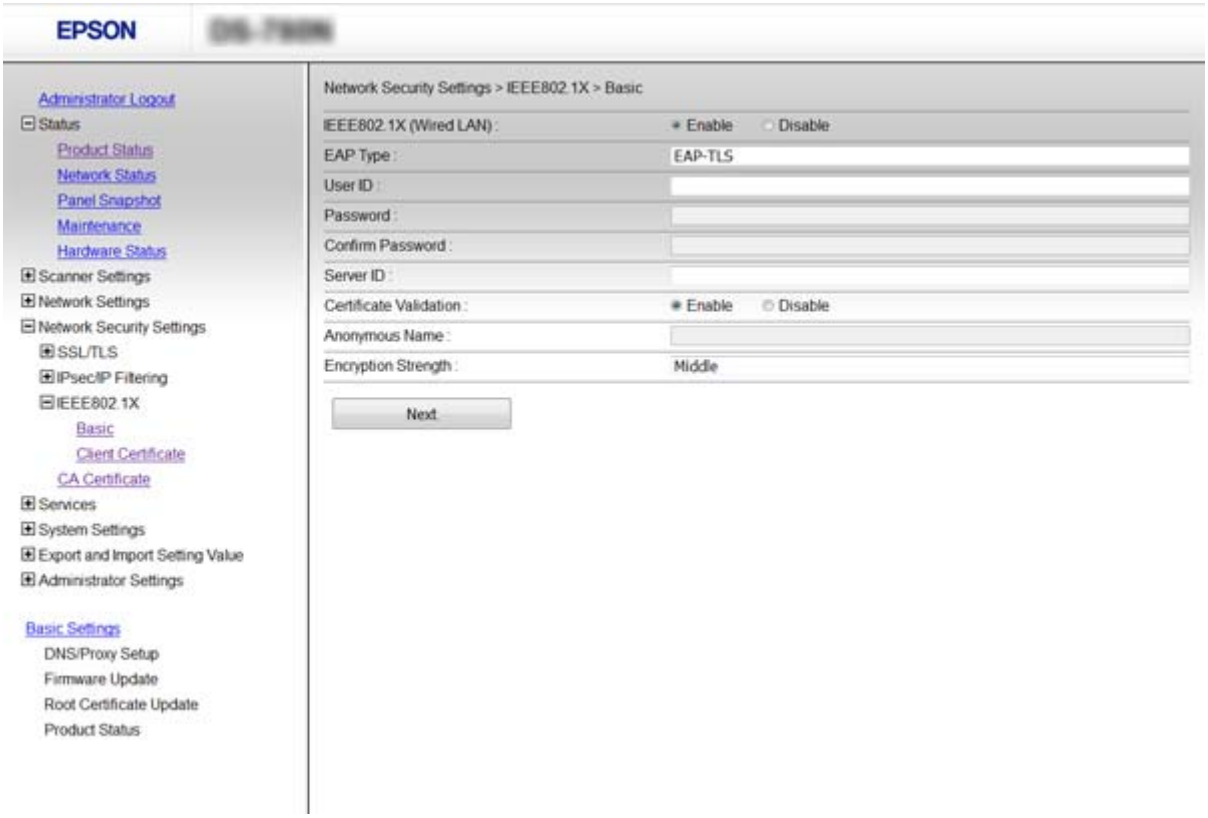
   Zobrazí se zpráva s potvrzením.
4. Klikněte na tlačítko **OK**.

   Skener je aktualizován.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23
➡ „Položky nastavení sítě IEEE802.1X“ na str. 85
➡ „Po nakonfigurování protokolu IEEE802.1X nelze získat přístup k tiskárně nebo ke skeneru“ na str. 89

Položky nastavení sítě IEEE802.1X



Položky	Nastavení a vysvětlení	
IEEE802.1X (Wired LAN)	Můžete povolit nebo zakázat nastavení na stránce (**IEEE802.1X** > **Basic**) pro IEEE802.1X (drátová místní síť LAN).	
EAP Type	Vyberte některou volbu pro metodu ověřování mezi skenerem a serverem RADIUS.	
	EAP-TLS	Musíte získat a importovat certifikát podepsaný certifikační agenturou.
	PEAP-TLS	
	PEAP/MSCHAPv2	Musíte konfigurovat heslo.
User ID	Nakonfigurujte ID, které bude použito jako ověření na serveru RADIUS. Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E).	
Password	Nakonfigurujte heslo pro ověření skeneru. Zadejte 1 až 128 1bajtových znaků ASCII (0x20 až 0x7E). Používáte-li server Windows jako server RADIUS, můžete zadat až 127 znaků.	
Confirm Password	Zadejte heslo nakonfigurované pro potvrzení.	
Server ID	Můžete nakonfigurovat ID serveru pro ověření s určeným serverem RADIUS. Ověřovatel ověřuje, zda je ID serveru obsaženo v poli subject/subjectAltName certifikátu serveru, který je odeslán ze serveru RADIUS, či nikoli. Zadejte 0 až 128 1bajtových znaků ASCII (0x20 až 0x7E).	
Certificate Validation	Můžete nastavit ověření certifikátu bez ohledu na metodu ověření. Naimportujte certifikát do **CA Certificate**.	

Položky	Nastavení a vysvětlení	
Anonymous Name	Vyberete-li u položky **PEAP-TLS** volbu **PEAP/MSCHAPv2** nebo **Authentication Method**, můžete nakonfigurovat anonymní jméno místo ID uživatele pro fázi 1 ověření PEAP. Zadejte 0 až 128 1bajtových znaků ASCII (0x20 až 0x7E).	
Encryption Strength	K dispozici je výběr z následujících možností.	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

Související informace

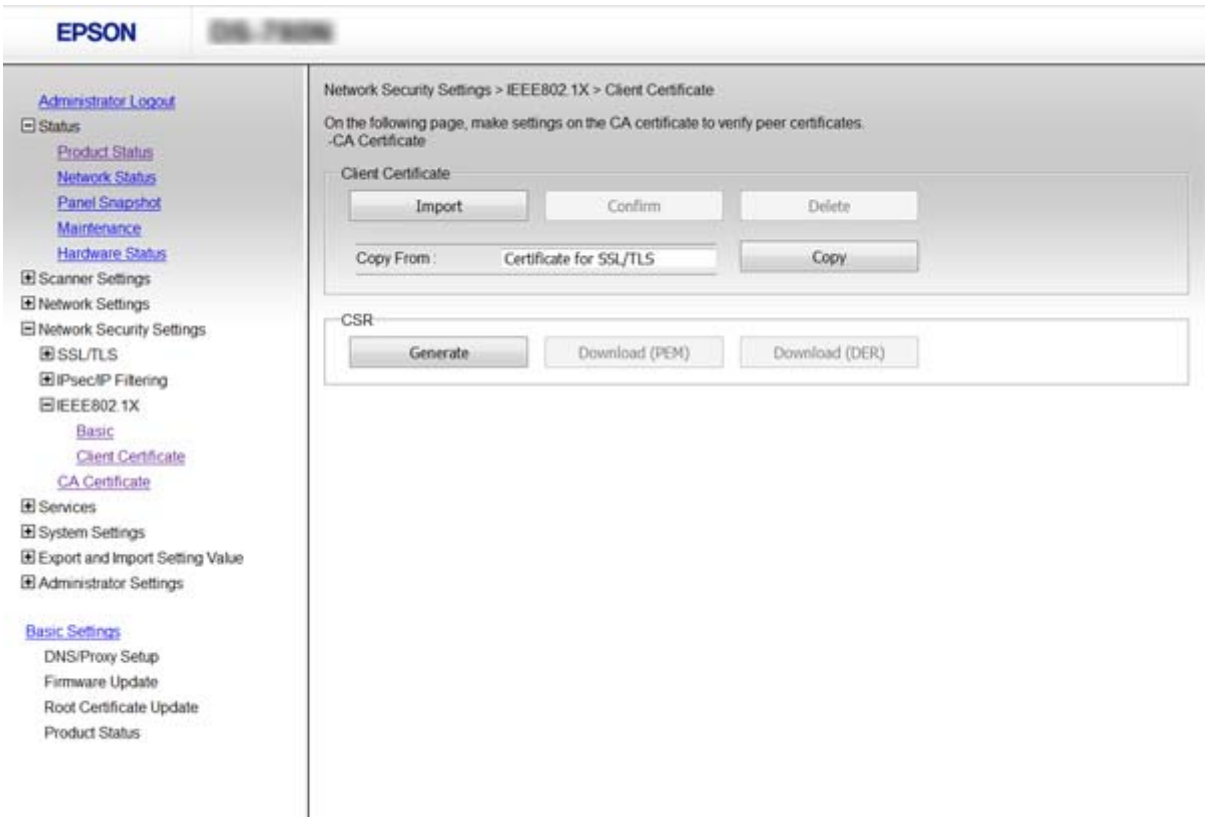
➡ „Konfigurování sítě IEEE802.1X“ na str. 84

Konfigurování certifikátu pro IEEE802.1X

Nakonfigurujte certifikát klienta pro IEEE802.1X. Chcete-li nakonfigurovat certifikát certifikační autority, přejděte na **CA Certificate**.

1. Přistupte na aplikaci Web Config a vyberte **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.
2. Zadejte certifikát do **Client Certificate**.

   Můžete zkopírovat certifikát vydaný certifikační autoritou. Chcete-li zkopírovat certifikát, vyberte jej v **Copy From** a potom klepněte na **Copy**.



Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

➡ „Získání a importování certifikátu podepsaného certifikační agenturou“ na str. 64

Řešení problémů v rámci rozšířeného zabezpečení

Obnovení nastavení zabezpečení

Pokud vytvoříte vysoce zabezpečené prostředí, jako je například filtrování IPsec/IP nebo IEEE802.1X, možná nebudete moci komunikovat se zařízeními z důvodu nesprávného nastavení nebo kvůli potížím se zařízením nebo serverem. V tomto případě obnovte nastavení zabezpečení a opětovně proveďte nastavení zařízení, nebo povolte dočasné použití.

Zakázání funkce zabezpečení pomocí ovládacího panelu

Funkci filtrování IPsec/IP nebo protokol IEEE802.1X můžete zakázat pomocí ovládacího panelu skeneru.

1. Klepněte na položku **Nast.** > **Nastavení sítě**.
2. Klepněte na položku **Změnit nastavení**.
3. Klepnutím vyberte položky, které chcete zakázat.
   - ❏ **Filtrování IPsec/IP**
   - ❏ **IEEE802.1X**
4. Jakmile se zobrazí zpráva o dokončení, klepněte na možnost **Pokrač.**.

Obnovení funkce zabezpečení pomocí aplikace Web Config

V případě funkce IEEE802.1X nemusí být zařízení na síti rozpoznána. V takovém případě zakažte funkci z ovládacího panelu skeneru.

V případě filtrování IPsec/IP můžete tuto funkci zakázat, pokud máte přístup k zařízení z počítače.

Zakázání funkce filtrování IPsec/IP pomocí Web Config

1. Přistupte na aplikaci Web Config a vyberte **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. Vyberte **Disable** pro **IPsec/IP Filtering** v **Default Policy**.
3. Klikněte na **Next** a potom zrušte zaškrtnutí **Enable this Group Policy** pro všechny zásady skupin.
4. Klikněte na položku **OK**.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Problémy při používání funkcí zabezpečení sítě

Zapomenutí předsdíleného klíče

Znovu nakonfigurujte klíč pomocí aplikace Web Config.

Chcete-li klíč změnit, přejděte na aplikaci Web Config a vyberte volbu **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** nebo **Group Policy**.

Po změně předsdíleného klíče jej nakonfigurujte pro počítače.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

Nelze komunikovat prostřednictvím IPsec

Nepoužíváte nepodporovaný algoritmus pro nastavení počítače?

Skener podporuje následující algoritmy.

Metody zabezpečení	Algoritmy
Algoritmus šifrování IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
Algoritmus ověřování IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmus výměny klíčů IKE	Skupina DH 1, Skupina DH 2, Skupina DH 5, Skupina DH 14, Skupina DH 15, Skupina DH 16, Skupina DH 17, Skupina DH 18, Skupina DH 19, Skupina DH 20, Skupina DH 21, Skupina DH 22, Skupina DH 23, Skupina DH 24, Skupina DH 25, Skupina DH 26, Skupina DH 27*, Skupina DH 28*, Skupina DH 29*, Skupina DH 30*
Algoritmus šifrování ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
Algoritmus ověřování ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
Algoritmus ověřování AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* k dispozici pouze pro IKEv2

Související informace

➡ „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 71

Nelze náhle komunikovat

Je adresa IP skeneru neplatná nebo se změnila?

Pomocí ovládacího panelu skeneru zakažte protokol IPsec.

Pokud je protokol DHCP zastaralý, restartování bylo provedeno před delší dobou nebo je adresa IPv6 zastaralá nebo nebyla získána, adresu IP zaregistrovanou pro aplikaci Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**) skeneru pravděpodobně nebude možné najít.

Použijte statickou adresu IP.

Je adresa IP počítače neplatná nebo se změnila?

Pomocí ovládacího panelu skeneru zakažte protokol IPsec.

Pokud je protokol DHCP zastaralý, restartování bylo provedeno před delší dobou nebo je adresa IPv6 zastaralá nebo nebyla získána, adresu IP zaregistrovanou pro aplikaci Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**) skeneru pravděpodobně nebude možné najít.

Použijte statickou adresu IP.

Související informace

➡ „Přístup k aplikaci Web Config“ na str. 23

➡ „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 71

Po nakonfigurování filtrování IPsec/IP se nelze připojit

Hodnota nastavení pravděpodobně není správná.

Na ovládacím panelu skeneru zakažte filtrování IPsec/IP. Připojte skener k počítači a znovu nastavte filtrování IPsec/IP.

Související informace

➡ „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 71

Po nakonfigurování protokolu IEEE802.1X nelze získat přístup k tiskárně nebo ke skeneru

Nastavení mohou být nesprávná.

Na ovládacím panelu skeneru zakažte protokol IEEE802.1X. Připojte skener k počítači a poté znovu nakonfigurujte protokol IEEE802.1X.

Související informace

➡ „Konfigurování sítě IEEE802.1X“ na str. 84

Problémy při používání digitálního certifikátu

Nelze importovat certifikát podepsaný certifikační agenturou

Shoduje se certifikát podepsaný certifikační agenturou s informacemi na shodě CSR?

Pokud certifikát podepsaný certifikační agenturou a CSR neobsahují stejné informace, CSR nelze importovat. Ověřte následující:

❏ Pokoušíte se importovat certifikát do zařízení, které nemá stejné informace?

Zkontrolujte informace CSR a potom naimportujte certifikát do zařízení, které má stejné informace.

❏ Přepsali jste CSR uložené ve skeneru po odeslání CSR certifikační agentuře?

Znovu získejte certifikát podepsaný certifikační agenturou prostřednictvím CSR.

Je certifikát podepsaný certifikační agenturou větší, než 5 kB?

Nelze importovat certifikát podepsaný certifikační agenturou, který je větší než 5 kB.

Je heslo pro importování certifikátu správné?

Pokud heslo zapomenete, nelze certifikát importovat.

Související informace

➡ „Importování certifikátu podepsaného certifikační agenturou“ na str. 66

Nelze aktualizovat samopodpisovatelný certifikát

Je zadán Common Name?

Common Name musí být zadán.

Obsahuje Common Name nepodporované znaky? Například japonština není podporována.

Zadejte 1 až 128 znaků ve formátu IPv4, IPv6, název hostitele nebo FQDN v ASCII (0x20-0x7E).

Obsahuje Common Name čárku nebo mezeru?

Pokud je zadána čárka, **Common Name** je v tomto bodě rozdělen. Pokud je před nebo za čárko vložena mezera, dojde k chybě.

Související informace

➡ „Aktualizování samopodpisovatelného certifikátu“ na str. 68

Nelze vytvořit CSR

Je zadán Common Name?

Common Name musí být zadán.

Obsahuje Common Name, Organization, Organizational Unit, Locality, State/Province nepodporované znaky? Například japonština není podporována.

Zadejte znaky ve formátu IPv4, IPv6, název hostitele nebo FQDN v ASCII (0x20-0x7E).

Obsahuje Common Name čárku nebo mezeru?

Pokud je zadána čárka, **Common Name** je v tomto bodě rozdělen. Pokud je před nebo za čárko vložena mezera, dojde k chybě.

Související informace

➡ „Získání certifikátu podepsaného certifikační agenturou“ na str. 64

Zobrazilo se varování ohledně digitálního certifikátu

Zprávy	Příčina/Postup
Enter a Server Certificate.	**Příčina:** Nevybrali jste žádný soubor k importování. **Postup:** Vyberte soubor a klepněte na tlačítko **Import**.
CA Certificate 1 is not entered.	**Příčina:** Certifikát CA 1 není zadán a je zadáno pouze certifikát CA 2. **Postup:** Nejdříve naimportujte certifikát CA 1.
Invalid value below.	**Příčina:** Umístění souboru a/nebo heslo obsahuje nepodporované znaky. **Postup:** Zkontrolujte, zda jsou znaky pro položku zadány správně.
Invalid date and time.	**Příčina:** Nebylo nastaveno datum a čas pro skener. **Postup:** Nastavte datum a čas pomocí aplikace Web Config nebo EpsonNet Config.
Invalid password.	**Příčina:** Heslo nastavené pro certifikát CA a zadané heslo se neshodují. **Postup:** Zadejte správné heslo.

Rozšířená nastavení zabezpečení pro podnik

Zprávy	Příčina/Postup
Invalid file.	**Příčina:** Importovaný soubor certifikátu nemá formát X509. **Postup:** Zkontrolujte, zda vybíráte správný certifikát odeslaný důvěryhodnou certifikační agenturou.
	Příčina: Naimportovaný soubor je příliš velký. Maximální velikost souboru je 5 kB. **Postup:** Pokud vyberete správný soubor, certifikát je pravděpodobně poškozený nebo smyšlený.
	Příčina: Neplatný řetězec v certifikátu. **Postup:** Další informace o certifikátu viz webové stránky certifikační agentury.
Cannot use the Server Certificates that include more than three CA certificates.	**Příčina:** Soubor certifikátu ve formátu PKCS#12 obsahuje více než 3 certifikáty CA. **Postup:** Naimportujte každý certifikát jako převod z formátu PKCS#12 na formát PEM nebo naimportujte soubor certifikátu ve formátu PKCS#12, který obsahuje maximálně 2 certifikáty CA.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**Příčina:** Certifikát je zastaralý. **Postup:** ❏ Pokud je certifikát zastaralý, získejte a naimportujte nový certifikát. ❏ Pokud certifikát není zastaralý, zkontrolujte, zda je správně nastaveno datum a čas skeneru.
Private key is required.	**Příčina:** S certifikátem není spárován žádný privátní klíč. **Postup:** ❏ Pokud je certifikát ve formátu PEM/DER a je získán z CSR pomocí počítače, určete soubor privátního klíče. ❏ Pokud je certifikát ve formátu PKCS#12 a je získán z CSR pomocí počítače, vytvořte soubor, který obsahuje privátní klíč.
	Příčina: Znovu jste naimportovali certifikát PEM/DER získaný z CSR pomocí aplikace Web Config. **Postup:** Pokud je certifikát ve formátu PEM/DER a je získán z CSR pomocí aplikace Web Config, lze jej naimportovat pouze jednou.

Zprávy	Příčina/Postup
Setup failed.	**Příčina:** Nelze dokončit konfiguraci, protože komunikace mezi skenerem a počítačem selhala nebo soubor nelze načíst z důvodu chyb. **Postup:** Po kontrole určeného souboru a komunikace znovu naimportujte soubor.

Související informace

➡ „O digitálním certifikátu“ na str. 63

Certifikát podepsaný certifikační agenturou byl omylem odstraněn

Existuje záložní soubor certifikátu?

Máte-li záložní soubor, znovu naimportujte certifikát.

Pokud obdržíte certifikát pomocí CSR vytvořený z aplikace Web Config, můžete znovu naimportovat odstraněný certifikát. Vytvořte CSR a získejte nový certifikát.

Související informace

➡ „Odstranění certifikátu podepsaného certifikační agenturou“ na str. 67

➡ „Importování certifikátu podepsaného certifikační agenturou“ na str. 66