EPSON
EXCEED YOUR VISION

DS-790WN

Příručka správce

NPD6726-00 CS

Autorská práva

Ochranné známky

- ❏ EPSON, EPSON EXCEED YOUR VISION, EXCEED YOUR VISION a jejich loga jsou registrované ochranné známky nebo ochranné známky společnosti Seiko Epson.
- ❏ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.
- ❏ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.
- ❏ Chrome is a trademark of Google LLC.
- ❏ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.
- ❏ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.
- ❏ FeliCa a PaSoRi jsou registrované ochranné známky společnosti Sony Corporation.
- ❏ MIFARE je registrovaná ochranná známka společnosti NXP Semiconductor Corporation.
- ❏ 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.

Obsah

Autorská práva

Ochranné známky

Úvod

Nutná nastavení pro váš účel

Síťová nastavení

Software pro nastavení skeneru

Požadované nastavení skenu

Přizpůsobení obrazovky Ovládacího panelu

Základní nastavení zabezpečení

Rozšířené nastavení zabezpečení

Nastavení ověření

Údržba

Úvod

Obsah tohoto dokumentu

Tento dokument poskytuje následující informace pro správu skenerů.

❏ Nastavení sítě

❏ Příprava funkce skenování

❏ Povolení a správa nastavení zabezpečení

❏ Povolení a správa Nastavení ověření

❏ Provádění každodenní údržby

Standardní metody používání skeneru naleznete v *Uživatelská příručka*.

Poznámka:
Tento dokument vysvětluje Nastavení ověření, která poskytují samostatné ověřování bez nutnosti používání serveru ověřování. Navíc k Nastavení ověření uvedenému v této příručce můžete také vytvořit systém ověřování pomocí serveru ověřování. Pro nastavení systému, použijte aplikaci Document Capture Pro Server Authentication Edition (zkráceným jménem Document Capture Pro Server AE).

Pro více informací kontaktujte svou místní pobočku společnosti Epson.

Používání této příručky

Značky a symboly

> ⚠ ***Upozornění:***
> *Instrukce, které je nezbytné dodržovat pro eliminaci rizika zranění.*

> ***Důležité:***
> *Instrukce, které je nutno zohlednit pro eliminaci rizika poškození zařízení.*

Poznámka:
Poskytuje doplňující a referenční informace.

Související informace

➡ Odkazuje na relevantní části.

Popisy používané v této příručce

❏ Kopie obrazovek pro aplikace jsou z operačního systému Windows 10 nebo macOS High Sierra. Obsah zobrazený na obrazovkách se liší v závislosti na modelu a situaci.

❏ Obrázky použité v této příručce jsou pouze orientační. Ačkoli se mohou mírně lišit od skutečného výrobku, jsou postupy při používání stejné.

Odkazy na operační systémy

Windows

Termíny v této příručce, jako například „Windows 10“, „Windows 8.1“, „Windows 8“, „Windows 7“, „Windows Server 2019“,„Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“ a „Windows Server 2008 R2“, odkazují na následující operační systémy. Termín „Windows“ označuje všechny verze a termín „Windows Server“ označuje verze „Windows Server 2019“, „Windows Server 2016“, „Windows Server 2012 R2“, „Windows Server 2012“, a „Windows Server 2008 R2“.

- ❏ 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 Server® 2019
- ❏ 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

Mac OS

Název „Mac OS“ v této příručce odkazuje na systémy macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan a OS X Yosemite.

Nutná nastavení pro váš účel

Nutná nastavení pro váš účel

Viz následující k provedení nezbytného nastavení, které vyhovuje vašemu účelu.

Připojení skeneru k síti

Účel	Požadovaná nastavení
Chci připojit skener k síti.	Nastavte svůj skener pro síťové skenování. „Připojení skeneru k síti“ na str. 13
Chci připojit skener k novému počítači.	Nastavte nastavení sítě pro svůj skener v novém počítači. „Přidání nebo výměna počítače nebo zařízení“ na str. 19

Nastavení pro skenování

Účel	Požadovaná nastavení
Chci odeslat naskenované snímky e-mailem. (Skenovat do e-mailu)	1. Nastavte e-mailový server, který chcete propojit. „Konfigurace poštovního serveru“ na str. 41 2. Zaregistrujte e-mailovou adresu příjemce v části **Kontakty** (volitelné). Registrací e-mailové adresy ji nemusíte zadávat pokaždé, když chcete něco odeslat, můžete ji jednoduše vybrat ze svých Kontaktů. „Zpřístupnění kontaktů“ na str. 62
Chci uložit naskenované snímky do složky na síti. (Skenovat do síťové složky/FTP)	1. Vytvořte složku na síti, do které chcete snímky uložit. „Nastavení sdílené síťové složky“ na str. 44 2. Zaregistrujte cestu do složky v části **Kontakty** (volitelné). Registrací cesty ke složce ji nemusíte zadávat pokaždé, když chcete něco odeslat, můžete ji jednoduše vybrat ze svých Kontaktů. „Zpřístupnění kontaktů“ na str. 62
Chci uložit naskenované snímky do cloudové služby. (Skenovat do cloudu)	Nastavte Epson Connect. Podrobnosti o nastavení najdete na webovém portálu Epson Connect. Při nastavení budete potřebovat uživatelský účet pro službu online úložiště, se kterou se chcete propojit. https://www.epsonconnect.com/ http://www.epsonconnect.eu (pouze pro Evropu)

Přizpůsobení obrazovky Ovládacího panelu

Účel	Požadovaná nastavení
Chci změnit položky zobrazené na ovládacím panelu skeneru.	Nastavte **Předvolby** nebo **Úpravy domovské obrazovky**. Oblíbené nastavení skenování můžete zaregistrovat na ovládacím panelu a upravit zobrazené položky. „Přizpůsobení obrazovky Ovládacího panelu“ na str. 75

Nastavení funkcí základního zabezpečení

Účel	Požadovaná nastavení
Chci zabránit komukoliv jinému než správci, aby měnil nastavení skeneru.	Nastavte heslo správce skeneru. „Nastavení správce“ na str. 84
Chci zakázat používání skenerů s USB připojením.	Zakažte externí rozhraní. „Vypnutí externího rozhraní“ na str. 90

Nastavení funkcí pokročilého zabezpečení

Účel	Požadovaná nastavení
Chci ovládat, jaké protokoly se budou používat.	Povolte nebo zakažte protokoly. „Řízení pomocí protokolů“ na str. 95
Chci šifrovat cestu komunikace.	1. Nastavte svůj digitální certifikát. „Používání digitálního certifikátu“ na str. 98 2. Nastavení komunikace SSL/TLS. „Komunikace SSL/TLS se skenerem“ na str. 103
Chci používat šifrovanou komunikaci (IPsec). Chci moci využívat software pouze z konkrétního počítače (filtrování IP).	Zásady nastavení pro filtrování provozu. „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 105
Chci používat skener v síti IEEE802.1X.	Nastavení IEEE802.1X pro skener. „Připojení skeneru k síti IEEE802.1X“ na str. 116

Funkce nastavení k ověřování skenerem

Účel	Požadovaná nastavení
Chci povolit Nastavení ověření.	Další informace o dostupných nastaveních Nastavení ověření a Způsob ověření naleznete níže. „O Nastavení ověření“ na str. 125 „O Způsob ověření“ na str. 126

Používání systému ověřování serveru

Pomocí Document Capture Pro Server Authentication Edition (kráceno na Document Capture Pro Server AE), můžete vytvořit systém ověřování, který využívá k ověřování server.

Pro více informací kontaktujte svou místní pobočku společnosti Epson.

Síťová nastavení

Připojení skeneru k síti

Tato část vysvětluje, jak připojit skener k síti pomocí ovládacího panelu skeneru.

Poznámka:
Pokud se váš skener a počítač nachází ve stejném segmentu, můžete se také připojit pomocí instalačního programu.

❏ *Nastavení z webové stránky*

Přejděte na uvedenou webovou stránku a zadejte název produktu. Přejděte do části ***Instalace*** *a začněte s nastavováním.*

http://epson.sn

❏ *Nastavení pomocí disku se softwarem (pouze pro modely, které se dodávají s tímto diskem a pro uživatele, kteří mají počítač se systémem Windows a s optickou jednotkou)*

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

Před vytvořením síťového připojení

Před připojením k síti zkontrolujte metodu připojení a informace o nastavení připojení.

Shromažďování informací o nastavení připojení

Připravte si potřebné informace o nastavení pro připojení. Zkontrolujte následující informace předem.

Divize	Položky	Poznámka
Způsob připojení zařízení	❏ Ethernet ❏ Wi-Fi	Rozhodněte se, jak připojit skener k síti. V případě kabelové sítě LAN se připojujte k přepínači LAN. U Wi-Fi se připojujte k síti (SSID) přístupového bodu.
Informace o připojení LAN	❏ IP adresa ❏ Maska podsítě ❏ Výchozí brána	Rozhodněte se pro IP adresu, která bude přiřazena skeneru. Pokud přiřadíte IP adresu staticky, budou požadovány všechny hodnoty. Pokud přiřadíte IP adresu dynamicky pomocí funkce DHCP, nebude tato informace požadována, protože bude nastavena automaticky.
Informace o Wi-Fi připojení	❏ SSID ❏ Heslo	Jedná se o SSID (název sítě) a heslo přístupového bodu, k němuž se skener připojuje. Pokud je nastaveno filtrování MAC adres, předem zaregistrujte MAC adresu skeneru, aby mohl být skener registrován. Informace o podporovaných standardech naleznete níže. „Specifikace sítě“ na str. 26
Informace o serveru DNS	❏ IP adresa pro primární DNS ❏ IP adresa pro sekundární DNS	Tyto údaje jsou vyžadovány při specifikaci serverů DNS. Sekundární DNS se nastavuje, když je v systému redundantní (nadbytečná) konfigurace a když se používá DNS server. Pokud jste malá organizace a nenastavujete DNS server, nastavte IP adresu směrovače (routeru).

Divize	Položky	Poznámka
Informace o proxy serveru	❏ Název proxy serveru	Nastavte tuto funkci, pokud vaše síťové prostředí používá proxy server pro přístup k internetu z intranetu a pokud používáte funkci, která zajišťuje přímý přístup skeneru k internetu. U následujících funkcí se skener připojuje přímo k internetu. ❏ Služby pro připojování Epson ❏ Cloudové služby dalších společností ❏ Aktualizace Firmwaru ❏ Zasílání naskenovaných snímků do služby SharePoint(WebDAV)
Informace o čísle portu	❏ Číslo portu určené k vydání	Zkontrolujte číslo portu používaného skenerem a počítačem; poté v případě potřeby uvolněte port, který je blokován branou firewall. Informace o čísle portu používaného skenerem. „Používání portu pro skener“ na str. 29

Přiřazení adresy IP

Následují typy přiřazení adresy IP.

Statická adresa IP:

Ruční přiřazení předem stanovené adresy IP skeneru (hostitel).

Informace potřebné pro připojení k síti (maska podsítě, výchozí brána, server DNS atd.) je nutné zadat ručně.

Adresa IP se nemění, ani když je zařízení vypnuté. Toto se hodí, pokud chcete spravovat zařízení v prostředí, kde nelze měnit adresu IP, nebo chcete spravovat zařízení pomocí adresy IP. Doporučujeme nastavení skeneru, serveru atd. kam přistupuje velké množství počítačů. Pokud také používáte funkce zabezpečení, jako například filtrování IPsec/IP, přiřaďte fixní adresu IP tak, aby se adresa IP neměnila.

Automatické přiřazení pomocí funkce DHCP (dynamická adresa IP):

Přiřaďte adresu IP automaticky ke skeneru (hostitel) pomocí funkce DHCP serveru DHCP nebo směrovače.

Informace pro připojení k síti (maska podsítě, výchozí brána, server DNS atd.) se nastavují automaticky, takže zařízení lze připojit k síti jednoduše.

Pokud je zařízení nebo směrovač vypnutý, nebo v závislosti na nastaveních serveru DHCP, může dojít ke změně adresy IP při opětovném připojení.

Doporučujeme spravovat jiná zařízení než adresy IP a komunikovat s protokoly, které mohou sledovat adresu IP.

Poznámka:
Pokud používáte funkci rezervace adresy IP DHCP, můžete přiřadit stejnou adresu IP k zařízením kdykoli.

Server DNS a Server Proxy

Název hostitele, název domény e-mailové adresy atd. serveru DNS závisí na informaci o IP adrese.

Komunikace nemůže probíhat, když je druhá strana popsána názvem hostitele, názvem domény atd., pokud počítač nebo skener provádí IP komunikaci.

Na tyto informace se dotazuje serveru DNS a získává IP adresu druhé strany. Tento proces se nazývá překlad IP adres.

Proto mohou zařízení, jako jsou počítače a skenery, komunikovat pomocí IP adresy.

Překlad IP adres je nutný pro to, aby mohl skener komunikovat pomocí e-mailu nebo internetového připojení.

Pokud používáte tyto funkce, proveďte nastavení serveru DNS.

Pokud přiřadíte IP adresu skeneru pomocí funkce DHCP serveru DHCP nebo směrovače, bude automaticky nastavena.

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 IP adresu nebo číslo portu a je očekávána zvýšená míra zabezpečení.

Pokud se připojujete k internetu pomocí serveru proxy, nakonfigurujte server proxy na skeneru.

Připojení k síti pomocí ovládacího panelu

Připojte skener k síti pomocí ovládacího panelu skeneru.

Přiřazování IP adresy

Nastavte základní položky, například Host Address (adresa hostitele), Maska podsítě, Výchozí brána.

V této kapitole je vysvětlen postup pro nastavení statické IP adresy.

1. Zapněte skener.
2. Vyberte možnost **Nast.** na domovské obrazovce ovládacího panelu skeneru.
3. Vyberte možnost **Nastavení sítě** > **Upřesnit** > **TCP/IP**.
4. Vyberte **Ruční** pro **Získat adresu IP**.

   Pokud nastavujete IP adresu automaticky pomocí funkce DHCP na směrovači, zvolte **Automaticky**. V tomto případě jsou **Adresa IP**, **Maska podsítě** a **Výchozí brána** v krocích 5 až 6 také nastavovány automaticky, takže můžete přejít ke kroku 7.
5. Zadávání IP adresy.

   Pokud zvolíte ◀ a ▶, převede se hlavní zaměření na přední segment nebo zadní segment oddělený tečkou.

   Potvrďte hodnotu z předchozí obrazovky.
6. Nastavte **Maska podsítě** a **Výchozí brána**.

   Potvrďte hodnotu z předchozí obrazovky.

   > ***Důležité:***
   >
   > *Pokud je kombinace Adresa IP, Maska podsítě a Výchozí brána nesprávná, **Zahájit instalaci** je neaktivní a nelze pokračovat dále s tímto nastavením. Potvrďte, že v tomto zadání není žádná chyba.*
7. Zadejte IP adresu pro primární server DNS.

   Potvrďte hodnotu z předchozí obrazovky.

Poznámka:
*Pokud pro nastavení přiřazení IP adresy vyberete možnost **Automaticky**, můžete pro server DNS vybrat nastavení **Ruční** nebo **Automaticky**. Pokud nemůžete získat adresu serveru DNS automaticky, vyberte možnost **Ruční** a zadejte adresu serveru DNS. Poté zadejte přímo sekundární adresu serveru DNS. Pokud zvolíte **Automaticky**, přejděte ke kroku 9.*

8. Zadejte IP adresu pro sekundární server DNS.

   Potvrďte hodnotu z předchozí obrazovky.

9. Klepněte na možnost **Zahájit instalaci**.

Nastavení serveru Proxy

Nastavení serveru Proxy v případě pravdivosti obou tvrzení.

❏ Server Proxy je určen pro internetové připojení.

❏ Pokud používáte funkci, v níž je skener připojen přímo k internetu, například službu Epson Connect nebo jinou cloudovou službu společnosti.

1. Vyberte možnost **Nast.** na domovské obrazovce.

   Při provádění nastavení po nastavení IP adresy se objeví obrazovka **Upřesnit**. Přejděte ke kroku 3.

2. Vyberte možnost **Nastavení sítě** > **Upřesnit**.

3. Vyberte **Server proxy**.

4. Vyberte **Použít** pro **Nastavení serveru proxy**.

5. Zadejte adresu pro server Proxy s formátem IPv4 nebo FQDN.

   Potvrďte hodnotu z předchozí obrazovky.

6. Zadejte číslo portu pro server Proxy.

   Potvrďte hodnotu z předchozí obrazovky.

7. Klepněte na možnost **Zahájit instalaci**.

Připojení k Ethernetu

Připojte skener k síti pomocí kabelu sítě LAN a zkontrolujte připojení.

1. Připojte skener k rozbočovači (přepínač sítě LAN) pomocí kabelu sítě LAN.

2. Vyberte možnost  na domovské obrazovce.

3. Vyberte **Router**.

4. Zkontrolujte, zda jsou nastavení Připojení a Adresa IP správná.

5. Klepněte na možnost **Zavřít**.

Připojení k bezdrátové síti LAN (Wi-Fi)

Skener můžete připojit k bezdrátové síti LAN (Wi-Fi) několika způsoby. Vyberte způsob připojení, který odpovídá použitému síťovému prostředí a podmínkám.

Pokud znáte informace o směrovači bezdrátové sítě, jako např. identifikátor SSID a heslo, můžete nastavení provést ručně.

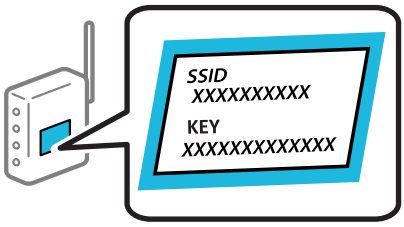
Pokud směrovač bezdrátové sítě podporuje standard WPS, můžete nastavení provést stisknutím jediného tlačítka.

Po připojení skeneru k síti se připojte ke skeneru ze zařízení, které chcete používat (počítač, chytré zařízení, tablet atd.)

Provedení Wi-Fi nastavení zadáním SSID a hesla

Z ovládacího panelu skeneru můžete nastavit síť Wi-Fi zadáním informací nezbytných k připojení k bezdrátovému směrovači. Chcete-li je nastavit touto metodou, potřebujete identifikátor SSID a heslo pro bezdrátový směrovač.

Poznámka:
Pokud používáte bezdrátový směrovač s výchozími nastaveními, nachází se identifikátor SSID a heslo na jeho štítku. Pokud neznáte identifikátor SSID a heslo, obraťte se na osobu, která nastavovala bezdrátový směrovač, nebo si projděte dokumentaci dodanou s bezdrátovým směrovačem.



1. Klepněte na možnost  na domovské obrazovce.

2. Vyberte **Router**.

3. Klepněte na možnost **Zahájit instalaci**.

   Pokud je síťové připojení již nastavené, zobrazí se podrobné informace o připojení. Nastavení můžete změnit klepnutím na možnost **Změňte na připojení Wi-Fi.** nebo **Změnit nastavení**.

4. Vyberte **Průvodce nastavením Wi-Fi**.

5. Podle pokynů na obrazovce vyberte SSID, zadejte heslo bezdrátového směrovače a spusťte nastavení.

   Pokud chcete zkontrolovat stav připojení skeneru k síti po dokončení nastavení, zobrazte si podrobnosti v odkazu níže.

Poznámka:

- ❏ *Pokud neznáte identifikátor SSID, zkontrolujte, zda není uveden na štítku bezdrátového směrovače. Pokud používáte bezdrátový směrovač s výchozími nastaveními, použijte identifikátor SSID uvedený na štítku. Pokud nemůžete najít žádné informace, zobrazte si dokumentaci dodanou s bezdrátovým směrovačem.*
- ❏ *Heslo rozeznává velká a malá písmena.*
- ❏ *Pokud neznáte heslo, zkontrolujte, zda není uveden na štítku bezdrátového směrovače. Na štítku s heslem může být napsáno „Network Key“, „Wireless Password“, atd. Pokud používáte bezdrátový směrovač s výchozími nastaveními, použijte heslo uvedené na štítku.*

Související informace

➡ „Kontrola stavu síťového připojení“ na str. 25

Nastavení Wi-Fi pomocí tlačítka (WPS)

Síť Wi-Fi můžete automaticky nastavit stisknutím tlačítka na bezdrátovém směrovači. Pokud jsou splněny následující podmínky, můžete provést nastavení pomocí této metody.

- ❏ Bezdrátový směrovač je kompatibilní se standardem WPS (Wi-Fi Protected Setup).
- ❏ Aktuální připojení Wi-Fi bylo navázáno stisknutím tlačítka na bezdrátovém směrovači.

Poznámka:
Pokud nemůžete tlačítko najít nebo provádíte nastavení pomocí softwaru, zobrazte si dokumentaci dodanou s bezdrátovým směrovačem.

1. Klepněte na možnost  na domovské obrazovce.
2. Vyberte **Router**.
3. Klepněte na možnost **Zahájit instalaci**.

   Pokud je síťové připojení již nastavené, zobrazí se podrobné informace o připojení. Nastavení můžete změnit klepnutím na možnost **Změňte na připojení Wi-Fi.** nebo **Změnit nastavení**.
4. Vyberte **Nastavení tlačítka (WPS)**.
5. Postupujte podle pokynů na obrazovce.

   Pokud chcete zkontrolovat stav připojení skeneru k síti po dokončení nastavení, zobrazte si podrobnosti v odkazu níže.

   Poznámka:
   Pokud se připojení nezdaří, restartujte bezdrátový směrovač, přemístěte jej blíže ke skeneru a opakujte akci.

Související informace

➡ „Kontrola stavu síťového připojení“ na str. 25

Nastavení Wi-Fi pomocí nastavení kódu PIN (WPS)

K bezdrátovému směrovači se můžete automaticky připojit pomocí kódu PIN. Tuto metodu můžete použít k nastavení, pokud je bezdrátový směrovač kompatibilní s nastavením WPS (chráněné nastavení Wi-Fi). Kód PIN zadejte do bezdrátového směrovače v počítači.

1. Klepněte na možnost  na domovské obrazovce.
2. Vyberte **Router**.
3. Klepněte na možnost **Zahájit instalaci**.

   Pokud je síťové připojení již nastavené, zobrazí se podrobné informace o připojení. Nastavení můžete změnit klepnutím na možnost **Změňte na připojení Wi-Fi.** nebo **Změnit nastavení**.
4. Vyberte možnost **Další** > **Nastavení kódu PIN (WPS)**
5. Postupujte podle pokynů na obrazovce.

   Pokud chcete zkontrolovat stav připojení skeneru k síti po dokončení nastavení, zobrazte si podrobnosti v odkazu níže.

   Poznámka:
   Podrobnosti o zadávání kódu PIN naleznete v dokumentaci dodané s bezdrátovým směrovačem.

Související informace

➡ „Kontrola stavu síťového připojení“ na str. 25

Přidání nebo výměna počítače nebo zařízení

Připojení ke skeneru, který je připojený k síti

Pokud je skener již připojen k síti, můžete k němu pomocí sítě připojit počítač nebo chytré zařízení.

Použití síťového skeneru z druhého počítače

Při připojování skeneru k počítači doporučujeme použít instalační program. Instalační program lze spustit jedním z následujících postupů.

❏ Nastavení z webové stránky

Přejděte na uvedenou webovou stránku a zadejte název produktu. Přejděte do části **Instalace** a začněte s nastavováním.

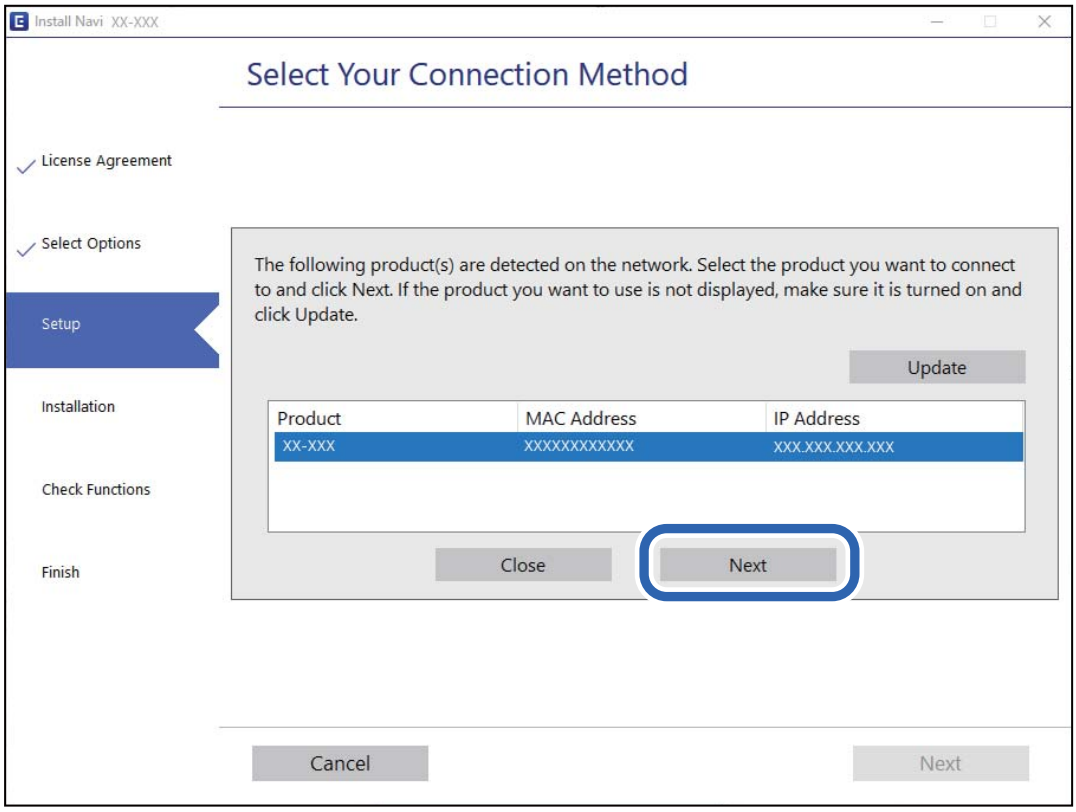
http://epson.sn

❏ Nastavení pomocí disku se softwarem (pouze pro modely, které se dodávají s tímto diskem a pro uživatele, kteří mají počítač se systémem Windows a s optickou jednotkou)

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

Výběr skeneru

Dodržujte pokyny na obrazovce, dokud se nezobrazí následující obrazovka. Vyberte název skeneru, který chcete, a pak klikněte na tlačítko **Další**.



Postupujte podle pokynů na obrazovce.

Použití síťového skeneru z chytrého zařízení

Ke skeneru můžete připojit chytré zařízení pomocí jedné z následujících metod.

Připojení přes bezdrátový směrovač

Připojte chytré zařízení ke stejné síti Wi-Fi (SSID), kterou používá skener.

Další podrobnosti naleznete v následujícím textu.

„Vytvoření nastavení pro připojení k chytrému zařízení“ na str. 24

Připojení pomocí Wi-Fi Direct

Připojte chytré zařízení ke skeneru přímo bez bezdrátového směrovače.

Další podrobnosti naleznete v následujícím textu.

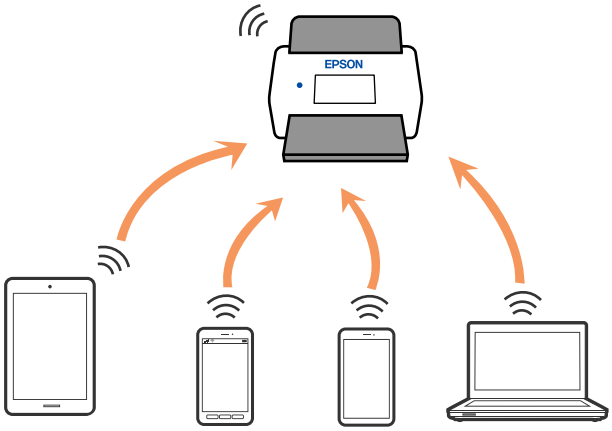
„Přímé připojení chytrého zařízení a skeneru (Wi-Fi Direct)“ na str. 21

Přímé připojení chytrého zařízení a skeneru (Wi-Fi Direct)

Funkce Wi-Fi Direct (jednoduchý přístupový bod) umožňuje připojit chytré zařízení přímo k tiskárně e skeneru bez bezdrátového směrovače a skenovat z chytrého zařízení.

O Wi-Fi Direct

Tuto metodu připojení použijte, když doma nebo v kanceláři nepoužíváte síť Wi-Fi nebo když chcete skener a počítač nebo chytré zařízení propojit přímo. V tomto režimu skener funguje jako bezdrátový směrovač a můžete k němu připojovat zařízení, aniž byste museli použít standardní bezdrátový směrovač. Nicméně, všechna zařízení, připojená přes skener, nemohou komunikovat mezi sebou.



Skener může být současně připojen k síti Wi-Fi nebo Ethernet a Wi-Fi Direct (jednoduchý přístupový bod). Pokud ale zahájíte síťové připojení v režimu Wi-Fi Direct (Jednoduchý přístupový bod), když je skener připojen pomocí sítě Wi-Fi, dojde k dočasnému odpojení sítě Wi-Fi.

Připojení k chytrému zařízení pomocí režimu Wi-Fi Direct

Tato metoda umožňuje připojit skener přímo k chytrým zařízením bez bezdrátového směrovače.

1. Vyberte možnost  na domovské obrazovce.
2. Vyberte **Wi-Fi Direct**.
3. Vyberte **Zahájit instalaci**.
4. Na chytrém zařízení spusťte aplikaci Epson Smart Panel.
5. Chcete-li se připojit ke skeneru, postupujte podle pokynů zobrazených v aplikaci Epson Smart Panel.

   Když se chytré zařízení připojí ke skeneru, přejděte na další krok.
6. Na ovládacím panelu skeneru vyberte možnost **Dokončit**.

Odpojení připojení Wi-Fi Direct (jednoduchý přístupový bod)

Existují dva způsoby, jak zakázat připojení Wi-Fi Direct (jednoduchý přístupový bod). Můžete všechna připojení vypnout pomocí ovládacího panelu skeneru nebo vypnout každé připojení z počítače nebo chytrého zařízení.

Chcete-li deaktivovat všechna připojení, zvolte  > **Wi-Fi Direct** > **Zahájit instalaci** > **Změnit** > **Deaktivovat Wi-Fi Direct**.

Důležité:

Je-li připojení Wi-Fi Direct (jednoduchý přístupový bod) deaktivované, jsou všechny počítače a chytrá zařízení připojená ke skeneru pomocí připojení Wi-Fi Direct (jednoduchý přístupový bod) odpojené.

Poznámka:

Pokud chcete odpojit konkrétní zařízení, proveďte odpojení z daného zařízení a nikoli ze skeneru. Chcete-li odpojit připojení Wi-Fi Direct (jednoduchý přístupový bod) od zařízení, vyberte jednu z následujících metod.

❏ *Odpojte připojení sítě Wi-Fi k názvu sítě (SSID) skeneru.*

❏ *Připojte se k síti s jiným názvem (SSID).*

Změna nastavení Wi-Fi Direct (jednoduchý přístupový bod), například SSID

Když je aktivováno připojení Wi-Fi Direct (jednoduchý přístupový bod), můžete změnit nastavení z  > **Wi-Fi Direct** > **Zahájit instalaci** > **Změnit** a pak se zobrazí následující položky nabídky.

Změnit síťový název

Změňte název sítě Wi-Fi Direct (jednoduchý přístupový bod) (SSID) používaný pro připojení ke skeneru na libovolný název podle svého výběru. Můžete nastavit název sítě (SSID) ve znacích ASCII zobrazených na softwarové klávesnici na ovládacím panelu. Můžete zadat až 22 znaků.

Při změně názvu sítě (SSID) jsou odpojena všechna připojená zařízení. Pokud chcete zařízení opět připojit, zadejte nový název sítě (SSID).

Změnit heslo

Změňte heslo Wi-Fi Direct (jednoduchý přístupový bod) pro připojení ke skeneru na libovolné heslo podle svého výběru. Můžete nastavit heslo ve znacích ASCII zobrazených na softwarové klávesnici na ovládacím panelu. Můžete zadat 8 až 22 znaků.

Při změně hesla jsou odpojena všechna připojená zařízení. Pokud chcete zařízení opět připojit, použijte nové heslo.

Změnit kmitočtový rozsah

Kmitočtový rozsah funkce Wi-Fi Direct používaný k připojení ke skeneru můžete změnit. Můžete vybrat hodnotu 2,4 GHz nebo 5 GHz.

Při změně kmitočtového rozsahu se odpojí všechna připojená zařízení. Zařízení znovu připojte.

Upozorňujeme, že když zvolíte hodnotu 5 GHz, nebude možné se znovu připojit ze zařízení, která nepodporují kmitočtový rozsah 5 GHz.

V závislosti na oblasti se toto nastavení nemusí zobrazit.

Deaktivovat Wi-Fi Direct

Deaktivujte nastavení Wi-Fi Direct (jednoduchý přístupový bod) skeneru. Při deaktivaci jsou všechny počítače a chytrá zařízení připojená ke skeneru v režimu Wi-Fi Direct (jednoduchý přístupový bod) odpojena.

Obnovit výchozí nastavení

Obnovte veškerá nastavení Wi-Fi Direct (jednoduchý přístupový bod) na výchozí hodnoty.

Informace o připojení Wi-Fi Direct (jednoduchý přístupový bod) chytrého zařízení uložené na skeneru budou odstraněny.

Poznámka:
*Můžete také provést následující nastavení z karty **Síť** > **Wi-Fi Direct** na Web Config.*

- ❏ *Aktivace nebo deaktivace Wi-Fi Direct (jednoduchý přístupový bod)*
- ❏ *Změna názvu sítě (SSID)*
- ❏ *Změna hesla*
- ❏ *Změna kmitočtového rozsahu*

  V závislosti na oblasti se toto nastavení nemusí zobrazit.
- ❏ *Obnova nastavení Wi-Fi Direct (jednoduchý přístupový bod)*

Opětovné nastavení síťového připojení

Tato část vysvětluje, jak provést nastavení síťového připojení a změnit způsob připojení při výměně bezdrátového směrovače nebo počítače.

Při výměně bezdrátového směrovače

Při výměně bezdrátového směrovače proveďte nastavení připojení mezi počítačem nebo chytrým zařízením a skenerem.

Tato nastavení potřebujete udělat, pokud změníte poskytovatele internetových služeb a podobně.

Vytvoření nastavení pro připojení k počítači

Při připojování skeneru k počítači doporučujeme použít instalační program. Instalační program lze spustit jedním z následujících postupů.

- ❏ Nastavení z webové stránky

  Přejděte na uvedenou webovou stránku a zadejte název produktu. Přejděte do části **Instalace** a začněte s nastavováním.

  http://epson.sn
- ❏ Nastavení pomocí disku se softwarem (pouze pro modely, které se dodávají s tímto diskem a pro uživatele, kteří mají počítač se systémem Windows a s optickou jednotkou)

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

Výběr metody připojení

Postupujte podle pokynů na obrazovce. Na obrazovce **Vyberte svoji operaci** vyberte možnost **Znovu nastavit připojení Tiskárna (pro nový síťový směrovač nebo při změně USB na síť atd.)** a poté klikněte na tlačítko **Další**.

Podle pokynů na obrazovce dokončete nastavení.

Pokud se nemůžete připojit, prohlédněte si následující a pokuste se problém vyřešit.

„Nelze se připojit k síti“ na str. 30

Vytvoření nastavení pro připojení k chytrému zařízení

Pokud připojíte skener ke stejné síti Wi-Fi (SSID), ke které je připojeno chytré zařízení, můžete z něho skener používat. Pro ovládání skeneru z chytrého zařízení přejděte na následující stránku a poté zadejte název produktu. Přejděte do části **Instalace** a začněte s nastavováním.

http://epson.sn

Na web přejděte z chytrého zařízení, které chcete ke skeneru připojit.

Při výměně počítače

Při výměně počítače proveďte nastavení připojení mezi počítačem a skenerem.

Vytvoření nastavení pro připojení k počítači

Při připojování skeneru k počítači doporučujeme použít instalační program. Instalační program lze spustit jedním z následujících postupů.

❏ Nastavení z webové stránky

Přejděte na uvedenou webovou stránku a zadejte název produktu. Přejděte do části **Instalace** a začněte s nastavováním.

http://epson.sn

❏ Nastavení pomocí disku se softwarem (pouze pro modely, které se dodávají s tímto diskem a pro uživatele, kteří mají počítač se systémem Windows a s optickou jednotkou)

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

Postupujte podle pokynů na obrazovce.

Změna způsobu připojení k počítači

Tato část vysvětluje, jak změnit způsob připojení při připojení počítače a skeneru.

Změna síťového připojení z Ethernetu na Wi-Fi

Změňte připojení Ethernet na připojení Wi-Fi z ovládacího panelu skeneru. Způsob změny připojení je v podstatě stejný jako nastavení připojení Wi-Fi.

Související informace

➡ „Připojení k bezdrátové síti LAN (Wi-Fi)“ na str. 17

Změna síťového připojení z Wi-Fi na Ethernet

Při přechodu z připojení Wi-Fi na připojení Ethernet postupujte podle níže uvedených kroků.

1. Vyberte možnost **Nast.** na domovské obrazovce.

2. Vyberte možnost **Nastavení sítě** > **Instalace drátové LAN**.

3. Postupujte podle pokynů na obrazovce.

Změna z USB na síťové připojení

Použití instalačního programu a znovunastavení v různých metodách připojení.

❏ Nastavení z webové stránky

Přejděte na uvedenou webovou stránku a zadejte název produktu. Přejděte do části **Instalace** a začněte s nastavováním.

http://epson.sn

❏ Nastavení pomocí disku se softwarem (pouze pro modely, které se dodávají s tímto diskem a pro uživatele, kteří mají počítač se systémem Windows a s optickou jednotkou)

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

Výběr Změny metody připojení

Postupujte podle pokynů na obrazovce. Na obrazovce **Vyberte svoji operaci** vyberte možnost **Znovu nastavit připojení Tiskárna (pro nový síťový směrovač nebo při změně USB na síť atd.)** a poté klikněte na tlačítko **Další**.

Vyberte síťové připojení, které chcete použít, **Připojit prostřednictvím bezdrátové sítě (Wi-Fi)** nebo **Připojit prostřednictvím drátové místní sítě LAN (Ethernet)**, a pak klikněte na **Další**.

Podle pokynů na obrazovce dokončete nastavení.

Kontrola stavu síťového připojení

Stav síťového připojení lze zkontrolovat následujícím způsobem.

Kontrola stavu síťového připojení z ovládacího panelu

Stav síťového připojení můžete zkontrolovat pomocí ikony sítě nebo informací o síti na ovládacím panelu skeneru.

Kontrola stavu síťového připojení pomocí ikony sítě

Pomocí ikony sítě na domovské obrazovce skeneru můžete zkontrolovat stav síťové připojení a sílu signálu.

	Zobrazí stav síťového připojení. Pokud chcete zkontrolovat nebo změnit aktuální nastavení, vyberte ikonu. Toto je zkratka pro následující nabídku. **Nast.** > **Nastavení sítě** > **Nast. Wi-Fi**	
		Skener není připojený do bezdrátové sítě (Wi-Fi).
		Skener hledá identifikátor SSID, není nastavená IP adresa nebo nastal problém s bezdrátovou sítí (Wi-Fi).
		Skener je připojený do bezdrátové sítě (Wi-Fi). Počet sloupečků indikuje sílu signálu připojení. Čím více sloupečků, tím silnější připojení.
		Skener není připojený k bezdrátové síti (Wi-Fi) v režimu Wi-Fi Direct (jednoduchý přístupový bod).
		Skener je připojený k bezdrátové síti (Wi-Fi) v režimu Wi-Fi Direct (jednoduchý přístupový bod).
		Tiskárna není připojená do kabelové sítě (Ethernet) nebo není nastavená.
		Tiskárna je připojená do kabelové sítě (Ethernet).

Zobrazení podrobných informací o síti na ovládacím panelu

Pokud je váš skener připojen k síti, informace vztahující se k síti je také možné zobrazit výběrem síťových nabídek, které chcete zkontrolovat.

1. Vyberte možnost **Nast.** na domovské obrazovce.
2. Vyberte možnost **Nastavení sítě** > **Stav sítě**.
3. Chcete-li zkontrolovat informace, vyberte nabídky, které chcete prověřit.
   - ❏ Stav kabelové sítě LAN/Wi-Fi

     Zobrazí informace o síti (název zařízení, připojení, sílu signálu atd.) pro připojení přes síť Ethernet nebo Wi-Fi.
   - ❏ Stav Wi-Fi Direct

     Zobrazí, zda je režim Wi-Fi Direct vypnut nebo zapnut, a zobrazí také identifikátor SSID, heslo atd. pro připojení pomocí režimu Wi-Fi Direct.
   - ❏ Stav poštovního serveru

     Zobrazí informace o síti pro e-mailový server.

Specifikace sítě

Specifikace sítě Wi-Fi

Specifikace Wi-Fi naleznete v následující tabulce.

Země nebo regiony s výjimkou dále uvedených	Tabulka A
Austrálie Nový Zéland Tchaj-Wan Jižní Korea	Tabulka B

Tabulka A

Standardy	IEEE 802.11b/g/n*1
Rozsah frekvence	2,4 GHz
Maximální vysílaný radiofrekvenční výkon	2400–2483,5 MHz: 20 dBm (EIRP)
Kanály	1/2/3/4/5/6/7/8/9/10/11/12/13
Režimy připojení	Infrastruktura, Wi-Fi Direct (jednoduchý přístupový bod)*2*3
Protokoly zabezpečení*4	WEP (64/128bit), WPA2-PSK (AES)*5, WPA3-SAE (AES), WPA2/WPA3-Enterprise

*1 Dostupný pouze pro režim HT20.

*2 Není podporováno pro IEEE 802.11b.

*3 Infrastruktura a režimy Wi-Fi Direct nebo připojení Ethernet lze používat simultánně.

*4 Připojení Wi-Fi Direct podporuje pouze standard WPA2-PSK (AES).

*5 Vyhovuje normě WPA2 s podporou standardu WPA/WPA2 Personal.

Tabulka B

Standardy	IEEE 802.11a/b/g/n*1/ac		
Frekvenční rozsahy	IEEE 802.11b/g/n: 2,4 GHz, IEEE 802.11a/n/ac: 5 GHz		
Kanály	Wi-Fi	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48), W53 (52/56/60/64), W56 (100/104/108/112/116/120/124/128/132/136/140/144), W58 (149/153/157/161/165)
	Wi-Fi Direct	2,4 GHz	1/2/3/4/5/6/7/8/9/10/11/12*2/13*2
		5 GHz*3	W52 (36/40/44/48) W58 (149/153/157/161/165)
Režimy připojení	Infrastruktura, Wi-Fi Direct (jednoduchý přístupový bod)*4, *5		
Protokoly zabezpečení*6	WEP (64/128bit), WPA2-PSK (AES)*7, WPA3-SAE (AES), WPA2/WPA3-Enterprise		

*1 Dostupný pouze pro režim HT20.

*2 Není dostupný na Tchaj-wanu.

*3 Dostupnost těchto kanálů a použití produktu ve venkovním prostředí přes tyto kanály se liší podle lokality. Další informace naleznete v kapitole http://support.epson.net/wifi5ghz/

*4 Není podporováno pro IEEE 802.11b.

*5 Infrastruktura a režimy Wi-Fi Direct nebo připojení Ethernet lze používat simultánně.

*6 Wi-Fi Direct podporuje pouze WPA2-PSK (AES).

*7 Vyhovuje normě WPA2 s podporou standardu WPA/WPA2 Personal.

Údaje k síti Ethernet

Standardy	IEEE802.3i (10BASE-T)*1 IEEE802.3u (100BASE-TX)*1 IEEE802.3ab (1000BASE-T)*1 IEEE802.3az (Energy Efficient Ethernet)*2
Režim komunikace	Automatický, 10 Mb/s plně duplexní, 10 Mb/s poloduplexní, 100 Mb/s plně duplexní, 100 Mb/s poloduplexní
Konektor	RJ-45

*1 Pro prevenci rádiového rušení použijte kabel kategorie 5e nebo vyšší STP (Shielded twisted pair).

*2 Připojené zařízení by mělo být v souladu se standardem IEEE802.3az.

Síťové funkce a IPv4/IPv6

Podporované	**funkce**
Epson Scan 2	IPv4, IPv6
Document Capture Pro/Document Capture	IPv4
Document Capture Pro Server	IPv4, IPv6

Protokol zabezpečení

IEEE802.1X*	
Filtrování protokolu IPsec/IP	
SSL/TLS	HTTPS Server/klient
SMTPS (STARTTLS, SSL/TLS)	
SNMPv3	

* Je nutné použít zařízení, které splňuje standardy IEEE802.1X.

Používání portu pro skener

Skener používá následující port. Tyto porty by měl mít správce sítě podle potřeby k dispozici.

Když je odesílatelem (klientem) scanner

Používat	Destinace (server)	Protokol	Číslo portu
Odesílání souboru (pokud se složka skenování do sítě používá ze skeneru)	Server FTP/FTPS	FTP/FTPS (TCP)	20
			21
	Souborový server	SMB (TCP)	445
		NetBIOS (UDP)	137
			138
		NetBIOS (TCP)	139
	Server WebDAV	Protokol HTTP (TCP)	80
		Protokol HTTPS (TCP)	443
Odesílání e-mailu (pokud se skenování do e-mailu používá ze skeneru)	Server SMTP	SMTP (TCP)	25
		SMTP SSL/TLS (TCP)	465
		SMTP STARTTLS (TCP)	587
POP před připojením SMTP (pokud se skenování do e-mailu používá ze skeneru)	Server POP	POP3 (TCP)	110
Při použití aplikace Epson Connect	Server Epson Connect	HTTPS	443
		XMPP	5222
Shromažďování informací o uživateli (používejte kontakty ze skeneru)	Server LDAP	LDAP (TCP)	389
		LDAP SSL/TLS (TCP)	636
		LDAP STARTTLS (TCP)	389
Ověřování uživatele při shromažďování informací o uživateli (při používání kontaktů ze skeneru) Ověřování uživatele při používání složky skenování do sítě (SMB) ze skeneru	Server KDC	Kerberos	88
Ovládání WSD	Klientský počítač	WSD (TCP)	5357
Prohledávejte počítač po stisknutí tlačítka skenování z aplikace	Klientský počítač	Program Network Push Scan Discovery	2968

Když je odesílatelem (klientem) Klientský počítač

Používat	Destinace (server)	Protokol	Číslo portu
Vyhledejte skener z aplikace (například EpsonNet Config) a ovladače skeneru.	Skener	ENPC (UDP)	3289

Používat	Destinace (server)	Protokol	Číslo portu
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 skenovaných z aplikace	Skener	Síťové skenování (TCP)	1865
Shromažďování informací o úlohách během skenování stisknutím z aplikace	Skener	Program Network Push Scan	2968
Web Config	Skener	HTTP (TCP)	80
		HTTPS (TCP)	443

Řešení problémů

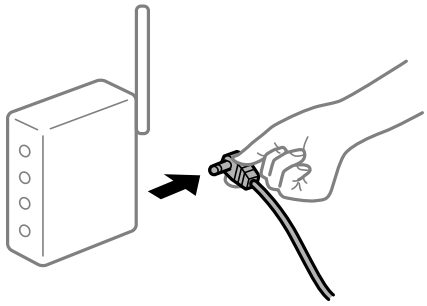
Nelze se připojit k síti

Může se jednat o jeden z následujících problémů.

Na síťových zařízeních pro připojení Wi-Fi je něco v nepořádku.

Řešení

Vypněte zařízení, která chcete připojit k síti. Počkejte asi 10 sekund a potom zařízení zapněte v tomto pořadí: směrovač bezdrátové sítě, počítač nebo chytré zařízení a potom skener. Přesuňte skener a počítač nebo chytré zařízení blíž ke směrovači bezdrátové sítě, abyste usnadnili rádiovou komunikaci, a potom znovu zkuste síť nastavit.



Zařízení nemohou přijímat signály z bezdrátového směrovače, protože jsou příliš daleko od sebe.

Řešení

Po přesunutí počítače nebo chytrého zařízení a skeneru blíže k bezdrátovému směrovači vypněte bezdrátový směrovač a poté jej znovu zapněte.

Při výměně bezdrátového směrovače se nastavení neshoduje s novým směrovačem.

Řešení

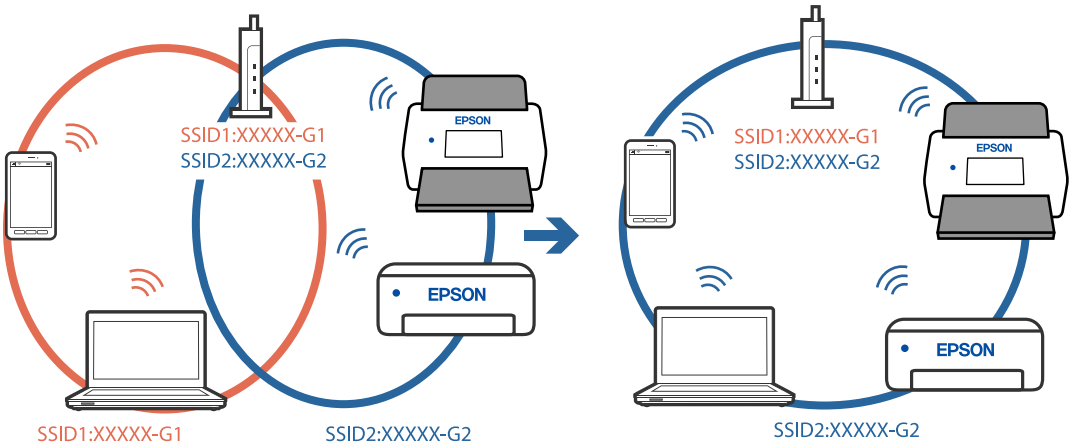
Nastavení připojení proveďte znovu tak, aby odpovídalo novému bezdrátovému směrovači.

Identifikátory SSID připojené z počítače nebo chytrého zařízení a počítače se liší.

Řešení

Pokud současně používáte více bezdrátových směrovačů nebo bezdrátový směrovač má více SSID a zařízení jsou připojena k různým SSID, nelze se k bezdrátovému směrovači připojit.

Připojte počítač nebo chytré zařízení ke stejnému SSID jako skener.



Na bezdrátovém směrovači je k dispozici funkce clona soukromí.

Řešení

Většina směrovačů bezdrátové sítě je vybavena funkcí clony soukromí, která blokuje komunikaci mezi připojenými zařízeními. Pokud skener nemůže komunikovat s počítačem nebo chytrým zařízením, ačkoli jsou připojeny ke stejné síti, zakažte na směrovači bezdrátové sítě funkci clony soukromí. Podrobnosti najdete v příručce dodané se směrovačem bezdrátové sítě.

Adresa IP je nesprávně přiřazena.

Řešení

Pokud je IP adresa přiřazená skeneru ve formátu 169.254.XXX.XXX a maska podsítě je 255.255.0.0, není IP adresa zřejmě přiřazena správně.

Na ovládacím panelu skeneru vyberte **Nast.** > **Nastavení sítě** > **Upřesnit** > **Nastavení TCP/IP** a poté zkontrolujte adresu IP a masku podsítě přiřazenou skeneru.

Restartujte bezdrátový směrovač nebo obnovte síťová nastavení skeneru.

Došlo k problému s nastavením sítě v počítači.

Řešení

Zkuste z počítače přejít na jakýkoli web a ověřit, zda jsou síťová nastavení počítače správná. Pokud se na web nedostanete, problém se týká počítače.

Zkontrolujte síťového připojení počítače. Viz dokumentace dodaná s počítačem, kde naleznete podrobnosti.

Skener je připojen přes síť Ethernet pomocí zařízení, která podporují IEEE 802.3az (Energy Efficient Ethernet).

Řešení

Při připojení skeneru k síti Ethernet pomocí zařízení, která podporují technologii IEEE 802.3az (Energy Efficient Ethernet), se mohou v závislosti na rozbočovači nebo směrovači, které používáte, vyskytnout následující problémy.

- ❏ Připojení je nestabilní, skener se opakovaně připojuje a odpojuje.
- ❏ Nelze se připojit ke skeneru.
- ❏ Rychlost komunikace je pomalá.

Postupujte podle následujících kroků, čímž vypnete technologii IEEE 802.3az pro skener a následně bude provedeno připojení.

1. Odpojte kabel sítě Ethernet připojený k počítači a skeneru.
2. Pokud je technologie IEEE 802.3az pro počítač povolena, zakažte ji.

   Viz dokumentace dodaná s počítačem, kde naleznete podrobnosti.
3. Propojte počítač a skener přímo pomocí kabelu sítě Ethernet.
4. Na skeneru zkontrolujte síťová nastavení.

   Vyberte možnost **Nast.** > **Nastavení sítě** > **Stav sítě** > **Stav kabelové sítě LAN/Wi-Fi**.
5. Zkontrolujte IP adresu skeneru.
6. Otevřete aplikaci Web Config v počítači.

   Spusťte webový prohlížeč a potom zadejte IP adresu skeneru.

   „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35
7. Vyberte kartu **Síť** > **Drátová síť LAN**.
8. Vyberte **Vypnuto** pro **IEEE 802.3az**.
9. Klikněte na položku **Další**.
10. Klikněte na položku **OK**.
11. Odpojte kabel sítě Ethernet připojený k počítači a skeneru.
12. Pokud jste v kroku 2 zakázali technologii IEEE 802.3az pro počítač, povolte ji.
13. Kabely sítě Ethernet, které jste odpojili v kroku 1, připojte k počítači a skeneru.

Pokud problém přetrvává, je možné, že problémy způsobuje jiné zařízení než skener.

Skener je vypnutý.

Řešení

Zkontrolujte, zda je skener zapnutý.

Také počkejte, až stavový indikátor přestane blikat, což znamená, že skener je připraven ke skenování.

Software pro nastavení skeneru

Web Config

Aplikace Web Config se spouští ve webových prohlížečích, například Internet Explorer a Safari v počítači. Můžete potvrdit stav skeneru nebo měnit nastavení síťových služeb a skeneru. Jelikož skenery se kontaktují a provozují v síti odlišně, je vhodné nastavovat jednotlivé skenery postupně. Chcete-li použít aplikaci Web Config, připojte svůj počítač ke stejné síti jako skener.

Jsou podporovány následující prohlížeče.

Microsoft Edge, Windows Internet Explorer 8 nebo novější, Firefox*, Chrome*, Safari*

* Použijte nejnovější verzi.

Spuštění nástroje Web Config ve webovém prohlížeči

1. Zkontrolujte IP adresu skeneru.

   Na ovládacím panelu skeneru vyberte možnost **Nast.** > **Nastavení sítě** > **Stav sítě**. Poté zvolte stav metody aktivního připojení (**Stav kabelové sítě LAN/Wi-Fi** nebo **Stav Wi-Fi Direct**) pro potvrzení IP adresy skeneru.

2. V počítači nebo chytrém zařízení spusťte webový prohlížeč a potom zadejte IP adresu skeneru.

   Formát:

   IPv4: http://IP adresa skeneru/

   IPv6: http://[IP adresa skeneru]/

   Příklady:

   IPv4: http://192.168.100.201/

   IPv6: http://[2001:db8::1000:1]/

   Poznámka:
   Vzhledem k tomu, že skener používá při přístupu k protokolu HTTPS certifikát s vlastním podpisem, při spuštění nástroje Web Config se v prohlížeči zobrazí varování. To neznamená problém a lze jej bezpečně ignorovat.

3. Aby bylo možné změnit nastavení skeneru, přihlaste se jako správce.

   Klikněte na ikonu **Přihlášení správce** v pravém horním rohu obrazovky. Zadejte údaje do polí **Uživatelské jméno** a **Aktuální heslo** a poté klikněte na tlačítko **OK**.

   Poznámka:
   - ❏ *Níže jsou uvedeny prvotní údaje pro administrátory Web Config.*
     ·Uživatelské jméno: není (prázdný)
     ·Heslo: sériové číslo skeneru
     Pro nalezení sériového čísla zkontrolujte štítek nalepený na zadní stranu skeneru.
   - ❏ *Pokud je v horním pravém rohu obrazovky zobrazena ikona **Odhlášení správce**, jste již přihlášeni jako správce.*

Spuštění aplikace Web Config v systému Windows

Při připojování počítače ke skeneru pomocí funkce WSD spusťte podle následujících kroků nástroj Web Config.

1. Na počítači otevřete seznam skenerů.

   ❏ Windows 10

   Klikněte na tlačítko Start a vyberte položku **Systém Windows** > **Ovládací panely** > **Zobrazit zařízení a tiskárny** v části **Hardware a zvuk**.

   ❏ Windows 8.1/Windows 8

   Vyberte možnost **Plocha** > **Nastavení** > **Ovládací panely** > **Zobrazit zařízení a tiskárny** v části **Hardware a zvuk** (nebo **Hardware**).

   ❏ Windows 7

   Klikněte na tlačítko Start a vyberte položku **Ovládací panely** > **Zobrazit zařízení a tiskárny** v části **Hardware a zvuk**.

2. Klikněte pravým tlačítkem na skener a vyberte možnost **Vlastnosti**.

3. Vyberte kartu **Webová služba** a klikněte na adresu URL.

   Vzhledem k tomu, že skener používá při přístupu k protokolu HTTPS certifikát s vlastním podpisem, při spuštění nástroje Web Config se v prohlížeči zobrazí varování. To neznamená problém a lze jej bezpečně ignorovat.

   Poznámka:

   ❏ *Níže jsou uvedeny prvotní údaje pro administrátory Web Config.*

   ·Uživatelské jméno: není (prázdný)

   ·Heslo: sériové číslo skeneru

   Pro nalezení sériového čísla zkontrolujte štítek nalepený na zadní stranu skeneru.

   ❏ *Pokud je v horním pravém rohu obrazovky zobrazena ikona **Odhlášení správce**, jste již přihlášeni jako správce.*

Epson Device Admin

Epson Device Admin je multifunkční aplikace, která umožňuje spravovat zařízení v síti.

Šablony konfigurace můžete použít k jednotnému nastavení více skenerů v síti, což je činí vhodnými k instalaci a správě více skenerů.

Můžete stáhnout aplikaci Epson Device Admin z webových stránek podpory společnosti Epson. Podrobnosti o používání této aplikace naleznete v dokumentaci nebo nápovědě aplikace Epson Device Admin.

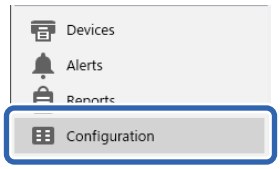
Šablona konfigurace

Vytvoření šablony konfigurace

Nově vytvořte šablonu konfigurace.

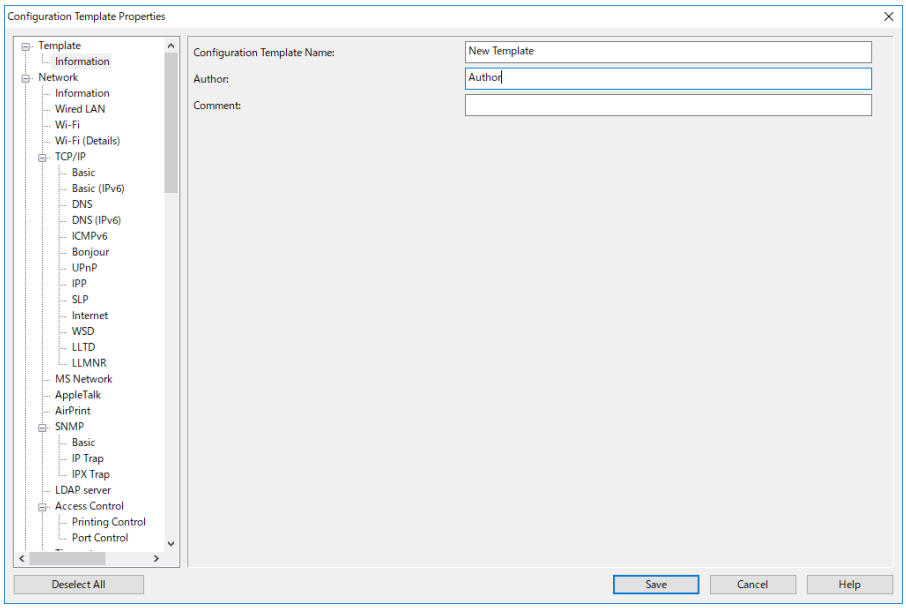
1. Spusťte aplikaci Epson Device Admin.

2. Vyberte možnost **Configuration** v nabídce úloh na bočním panelu.



3. Vyberte **New** v nabídce pásu karet.

4. Nastavte jednotlivé položky.



Položka	Vysvětlení
Configuration Template Name	Název šablony konfigurace. Zadejte maximálně 1024 ve formátu Unicode (UTF-8).
Author	Informace o autorovi šablony. Zadejte maximálně 1024 ve formátu Unicode (UTF-8).
Comment	Zadejte libovolné údaje. Zadejte maximálně 1024 ve formátu Unicode (UTF-8).

5. Nalevo vyberte položky, které chcete nastavit.

Poznámka:
Klikněte na položky nabídky nalevo a přepněte na jednotlivé obrazovky. Nastavená hodnota se uloží, pokud přepnete obrazovku, ale ne, pokud obrazovku zrušíte. Po dokončení všech nastavení klikněte na tlačítko ***Save****.*

Použití šablony konfigurace

Použije uloženou šablonu konfigurace na skener. Použijí se položky vybrané v šabloně. Pokud cílový skener nemá příslušnou funkci, nebude použita.

Poznámka:
Pokud je pro skener nastaveno heslo správce, nakonfigurujte heslo předem.

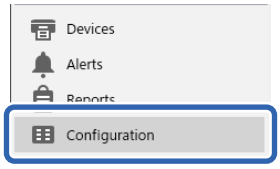
*1. V nabídce pásu karet obrazovky Seznam zařízení vyberte možnosti **Options** > **Password manager**.*

*2. Vyberte položku **Enable automatic password management** a potom klikněte na možnost **Password manager**.*

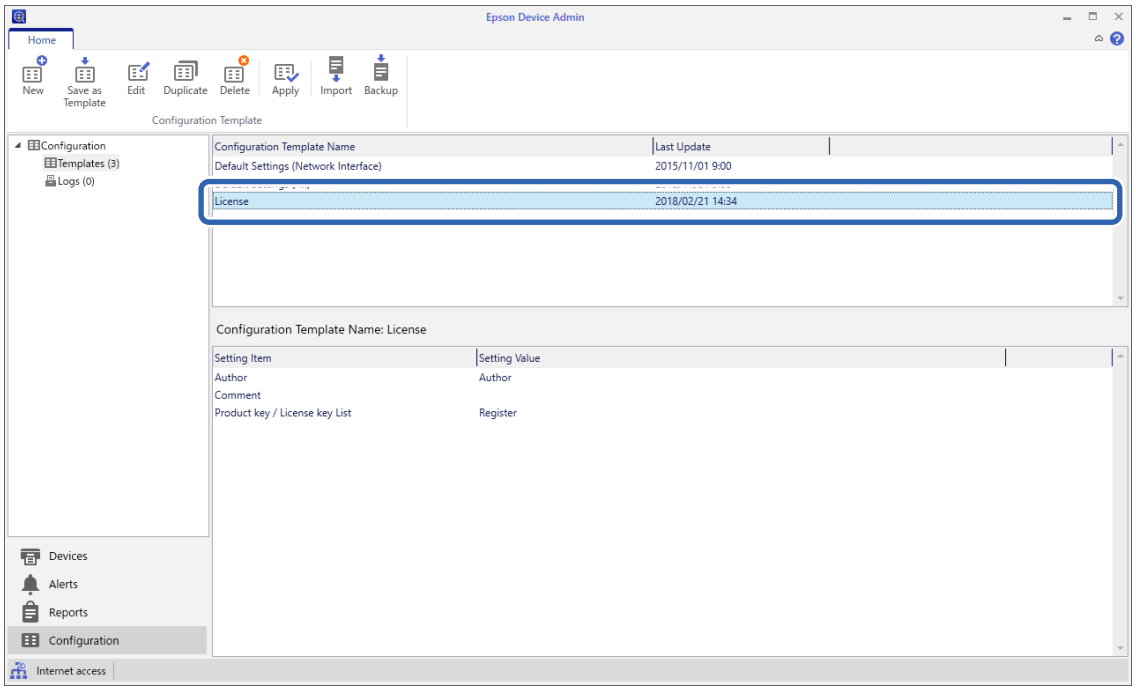
*3. Vyberte příslušný skener a potom klepněte na položku **Edit**.*

*4. Nastavte heslo a pak klikněte na tlačítko **OK**.*

1. Vyberte možnost **Configuration** v nabídce úloh na bočním panelu.



2. Šablonu konfigurace, kterou chcete použít, vyberte z **Configuration Template Name**.



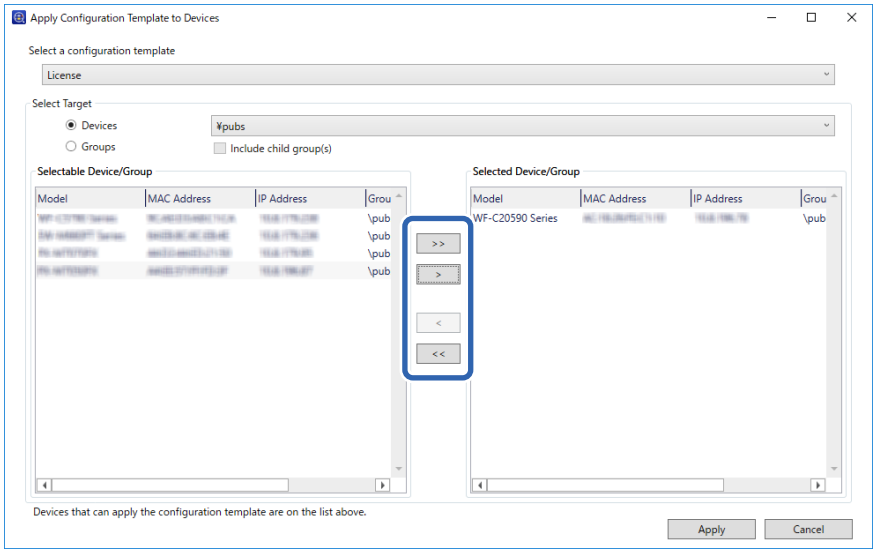
3. Klikněte na možnost **Apply** v nabídce pásu karet.

   Zobrazí se obrazovka výběru zařízení.

4. Vyberte šablonu konfigurace, kterou chcete použít.

   Poznámka:
   - ❏ *Když vyberete možnost **Devices** a skupiny obsahující zařízení z rozevírací nabídky, zobrazí se každé zařízení.*
   - ❏ *Skupiny se zobrazí, když vyberete **Groups**. Vyberte **Include child group(s)** pro automatický výběr podřízených skupin v rámci vybraných skupin.*

5. Přesuňte skener nebo skupiny, ve kterých chcete použít šablonu, do **Selected Device/Group**.



6. Klikněte na položku **Apply**.

   Zobrazí se obrazovka pro potvrzení používané šablony konfigurace.

7. Klikněte na tlačítko **OK** a použijte šablonu konfigurace.

8. Kdy se zobrazí zpráva s informací, že postup byl dokončen, klikněte na tlačítko **OK**.

9. Klikněte na možnost **Details** a zkontrolujte informace.

   Po zobrazení na použitých položkách byla aplikace úspěšně dokončena.

10. Klikněte na položku **Close**.

Požadované nastavení skenu

Konfigurace poštovního serveru

Nastavte poštovní server z nástroje Web Config.

Pokud skener dokáže odeslat e-mail nastavením poštovního serveru, jsou možné následující možnosti.

❏ Přenosy výsledků skenování pomocí e-mailu

❏ Příjem e-mailového oznámení ze skeneru

Před nastavením zkontrolujte stav níže.

❏ Skener je připojen k síti, která má přístup k poštovnímu serveru.

❏ Informace o nastavení e-mailu počítače, který používá stejný poštovní server jako skener.

Poznámka:

❏ *Když použijete poštovní server na internetu, potvrďte informace o nastavení u poskytovatele nebo na webové stránce.*

❏ *Poštovní server můžete také nastavit na ovládacím panelu. Přístup naleznete níže.*

Nast. > ***Nastavení sítě*** > ***Upřesnit*** > ***Poštovní server*** > ***Nastavení serveru***

1. Otevřete nástroj Web Config a vyberte kartu **Síť** > **Poštovní server** > **Základní**.
2. Do všech polí zadejte hodnotu.
3. Vyberte **OK**.

   Zobrazí se vybraná nastavení.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Položky nastavení poštovního serveru

Položky	Nastavení a vysvětlení	
Způsob ověření	Určete metodu ověřování skeneru pro přístup k poštovnímu serveru.	
	Vypnout	Ověřování je při komunikaci s poštovním serverem zakázané.
	OVĚŘENÍ SMTP	Vyžaduje, aby poštovní server podporoval ověřování SMTP.
	POP před SMTP	Při výběru této metody nakonfigurujte server POP3.
Ověřený účet	Vyberete-li **OVĚŘENÍ SMTP** nebo **POP před SMTP** jako **Způsob ověření**, zadejte ověřovaný název účtu od 0 do 255 znaků ve formátu ASCII (0x20–0x7E).	
Ověřené heslo	Pokud nastavíte položku **Způsob ověření** na hodnotu **OVĚŘENÍ SMTP** nebo **POP před SMTP**, zadejte ověřované heslo s 0 až 20 znaky ve formátu ASCII (0x20–0x7E).	
E-mailová adresa odesílatele	Zadejte e-mailovou adresu odesilatele. Zadejte 0 až 255 znaků ve formátu ASCII (0x20–0x7E) vyjma znaků : ( ) < > [ ] ; ¥. Jako první znak nelze použít tečku „.“.	
Adresa serveru SMTP	Zadejte 0 až 255 znaků s použitím znaků A–Z a–z 0–9 . -. Lze použít formát IPv4 nebo FQDN.	
Číslo portu serveru SMTP	Zadejte číslo 1 až 65535.	

Položky	Nastavení a vysvětlení	
Zabezpečené připojení	Určete metodu zabezpečeného připojení poštovního serveru.	
	Žádná	Vyberete-li **POP před SMTP** v **Způsob ověření**, bude metoda připojení nastavena na **Žádná**.
	SSL/TLS	Tato možnost je dostupná, když je položka **Způsob ověření** nastavena na **Vypnout** nebo **OVĚŘENÍ SMTP**.
	STARTTLS	Tato možnost je dostupná, když je položka **Způsob ověření** nastavena na **Vypnout** nebo **OVĚŘENÍ SMTP**.
Ověření certifikátu	Když je tato možnost povolena, certifikát je ověřen. Doporučujeme tuto možnost nastavit na **Povolit**.	
Adresa serveru POP3	Vyberete-li **POP před SMTP** jako **Způsob ověření**, 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.	
Číslo portu serveru POP3	Vyberete-li volbu **POP před SMTP** jako **Způsob ověření**, zadejte číslo v rozmezí hodnot 1 až 65535.	

Kontrola připojení k poštovnímu serveru

Připojení k poštovnímu serveru můžete prověřit provedením kontroly připojení.

1. Otevřete nástroj Web Config a vyberte kartu **Síť** > **Poštovní server** > **Test připojení**.
2. Vyberte **Spustit**.

   Bude zahájen test připojení k e-mailovému serveru. Po dokončení zkoušky bude zobrazena kontrolní zpráva.

   Poznámka:
   Připojení k poštovnímu serveru můžete také prověřit z ovládacího panelu skeneru. Přístup naleznete níže.

   Nast. > ***Nastavení sítě*** > ***Upřesnit*** > ***Poštovní server*** > ***Kontrola připojení***

Reference zkoušky připojení poštovního serveru

Zprávy	Příčina
Test připojení byl úspěšný.	Tato zpráva se zobrazí při úspěšně provedeném připojení k serveru.
Chyba komunikace serveru SMTP. Zkontrolujte následující. - Síťová nastavení	Tato zpráva se zobrazí v následujících situacích ❏ Skener není připojen k síti ❏ Server SMTP není k dispozici ❏ Tiskárna byla v průběhu komunikace odpojena od sítě ❏ Některá přijatá data chybí

Zprávy	Příčina
Chyba komunikace serveru POP3. Zkontrolujte následující. - Síťová nastavení	Tato zpráva se zobrazí v následujících situacích ❏ Skener není připojen k síti ❏ Server POP3 není k dispozici ❏ Tiskárna byla v průběhu komunikace odpojena od sítě ❏ Některá přijatá data chybí
Při připojování k serveru SMTP došlo k chybě. Zkontrolujte následující. - Adresa serveru SMTP - Server DNS	Tato zpráva se zobrazí v následujících situacích ❏ Připojení k serveru DNS se nezdařilo ❏ Překlad adres IP pro server SMTP se nezdařil
Při připojování k serveru POP3 došlo k chybě. Zkontrolujte následující. - Adresa serveru POP3 - Server DNS	Tato zpráva se zobrazí v následujících situacích ❏ Připojení k serveru DNS se nezdařilo ❏ Překlad adres IP pro server POP3 se nezdařil
Chyba ověření serveru SMTP. Zkontrolujte následující. - Metoda ověření - Ověřovaný účet - Ověřované heslo	Tato zpráva se zobrazí při selhání ověření serveru SMTP.
Chyba ověření serveru POP3. Zkontrolujte následující. - Metoda ověření - Ověřovaný účet - Ověřované heslo	Tato zpráva se zobrazí při selhání ověření serveru POP3.
Nepodporovaná metoda komunikace. Zkontrolujte následující. - Adresa serveru SMTP - Číslo portu serveru SMTP	Tato zpráva se zobrazí při pokusu o komunikaci s nepodporovanými protokoly.
Připojení k serveru SMTP se nezdařilo. Změňte Zabezpečené připojení na Žádná.	Tato zpráva se zobrazí, pokud se neshoduje server SMTP mezi serverem a klientem nebo pokud server nepodporuje zabezpečené připojení SMTP (připojení SSL).
Připojení k serveru SMTP se nezdařilo. Změňte Zabezpečené připojení na SSL/TLS.	Tato zpráva se zobrazí, pokud se neshoduje server SMTP mezi serverem a klientem nebo server vyžaduje pro zabezpečené připojení SMTP připojení SSL/TLS.
Připojení k serveru SMTP se nezdařilo. Změňte Zabezpečené připojení na STARTTLS.	Tato zpráva se zobrazí, pokud se neshoduje server SMTP mezi serverem a klientem nebo server vyžaduje pro zabezpečené připojení SMTP připojení STARTTLS.
Nedůvěryhodné připojení. Zkontrolujte následující. - Datum a čas	Tato zpráva se zobrazí, pokud nejsou datum a čas na skeneru nastaveny správně nebo pokud vypršela platnost certifikátu.
Nedůvěryhodné připojení. Zkontrolujte následující. - Certifikát CA	Tato zpráva se zobrazí, pokud nemá skener kořenový certifikát odpovídající serveru nebo nebyl importován certifikát Certifikát CA.
Toto připojení není zabezpečené.	Tato zpráva se zobrazí, pokud je zaslaný certifikát poškozený.
Ověření serveru SMTP se nezdařilo. Změňte Metodu ověření na SMTP-AUTH.	Tato zpráva se zobrazí, pokud se liší metoda ověření serveru a klienta. Server podporuje metodu OVĚŘENÍ SMTP.
Ověření serveru SMTP se nezdařilo. Změňte Metodu ověření na POP před SMTP.	Tato zpráva se zobrazí, pokud se liší metoda ověření serveru a klienta. Server nepodporuje metodu OVĚŘENÍ SMTP.

Zprávy	Příčina
E-mailová adresa odesilatele je nesprávná. Změňte na e-mailovou adresu pro vaši e-mailovou službu.	Tato zpráva se zobrazí, pokud není správně zadaná e-mailová adresa odesílatele.
Do dokončení zpracování nelze produkt zpřístupnit.	Tato zpráva se zobrazí, pokud skener vykonává nějakou činnost.

Nastavení sdílené síťové složky

K uložení naskenovaného snímku nastavte sdílenou síťovou složku.

Při ukládání souboru do složky se skener přihlásí jako uživatel počítače, na kterém byla vytvořena složka.

Tvorba sdílené složky

Související informace

➡ „Před vytvořením sdílené složky“ na str. 44

➡ „Kontrola profilu sítě“ na str. 44

➡ „Umístění vytvořené sdílené složky a příklad zabezpečení“ na str. 45

➡ „Přidání skupiny nebo uživatele povolujícího přístup“ na str. 58

Před vytvořením sdílené složky

Před vytvořením sdílené složky prověřte následující.

❏ Skener je připojen k síti, ze které se může připojit k počítači, na kterém bude vytvořena sdílená složka.

❏ Název počítače, na kterém bude vytvořena sdílená složka, neobsahuje vícebajtové znaky.

Důležité:

Pokud název počítače obsahuje vícebajtové znaky, může dojít k selhání ukládání do sdílené složky.

V tomto případě proveďte změnu počítače na takový, jehož název neobsahuje vícebajtové znaky, nebo změňte název počítače.

Při změně názvu počítače nezapomeňte informovat správce, protože změna názvu může ovlivnit některá nastavení, jako je například správa počítače, přístup k prostředkům atd.

Kontrola profilu sítě

Na počítači, na kterém bude vytvořena sdílená složka, zkontrolujte, zda je dostupné sdílení složky.

1. Přihlaste se do počítače, kde bude prostřednictvím uživatelského účtu s oprávněním správce vytvořena sdílená složka.

2. Vyberte **Ovládací panel** > **Síť a Internet** > **Síť a centrum sdílení**.

3. Klikněte na možnost **Změnit pokročilá nastavení sdílení** a poté klikněte na pro profil s **(aktuální profil)** v zobrazených síťových profilech.

4. Zkontrolujte, zda je možnost **Zapnout sdílení souborů a tiskáren** vybraná v části **Sdílení souborů a tiskáren**.

   Pokud je volba již zvolena, klikněte na položku **Zrušit** a okno zavřete.

   Pokud změníte nastavení, klikněte na možnost **Uložit změny** a okno zavřete.

Umístění vytvořené sdílené složky a příklad zabezpečení

V závislosti na umístění, ve kterém je vytvořena sdílená složka, se mohou měnit podmínky zabezpečení a pracovního komfortu.

Pro řízení sdílené složky ze skenerů nebo jiných počítačů je nutné si přečíst následující informace a dle potřeby změnit oprávnění ke složce.

❏ Karta **Sdílení** > **Rozšíření sdílení** > **Oprávnění**

Řídí oprávnění síťového přístupu ke sdílené složce.

❏ Oprávnění přístupu na kartu **Zabezpečení**

Řídí oprávnění síťového přístupu a místního přístupu ke sdílené složce.

Pokud nastavíte možnost **Všichni** pro sdílenou složku, která je vytvořena na ploše, jako příklad vytvoření sdílené složky, všichni uživatelé, kteří mají přístup do počítače, budou mít oprávnění přístupu k této složce.

Nicméně, uživatel, který nemá oprávnění, nemůže k datům přistupovat, protože plocha (složka) je pod kontrolou složky uživatele, a vztahují se na ni bezpečnostní nastavení složky uživatele. Uživatel, který má oprávnění přístupu na kartu **Zabezpečení** (v tomto případě přihlášený uživatel a správce) může se složkou pracovat.

Níže je uveden postup správného vytvoření umístění.

Tento příklad se týká vytvoření složky „scan_folder“.

Související informace

➡ „Příklad konfigurace pro souborové servery“ na str. 45

➡ „Příklad konfigurace pro osobní počítač“ na str. 52

Příklad konfigurace pro souborové servery

Toto vysvětlení je příkladem pro tvorbu sdílené složky v kořenovém adresáři disku na sdíleném počítači, jako je například souborový server, za následujících podmínek.

Uživatelé, u kterých lze řídit jejich přístup, jako například uživatel s počítačem ve stejné doméně, mají přístup ke sdílené složce.

Tuto konfiguraci nastavte, pokud chcete jakémukoli uživateli povolit čtení i zápis do sdílené složky na počítači, jako je například souborový server nebo sdílený počítač.

❏ Místo pro vytvoření sdílené složky: kořenový adresář na disku

❏ Cesta ke složce: C:\scan_folder

❏ Povolit přístup přes síť (sdílení oprávnění): všichni

❏ Povolit přístup k systému souborů (zabezpečení): ověření uživatelé

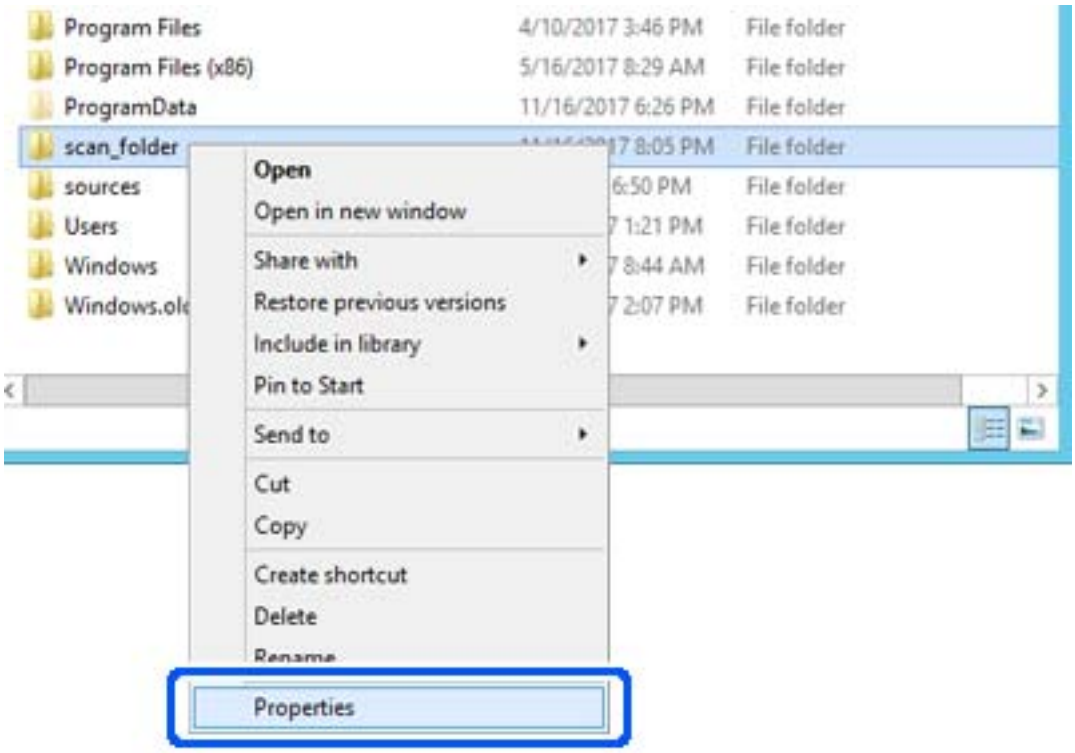
1. Přihlaste se do počítače, kde bude prostřednictvím uživatelského účtu s oprávněním správce vytvořena sdílená složka.

2. Spusťte průzkumníka.

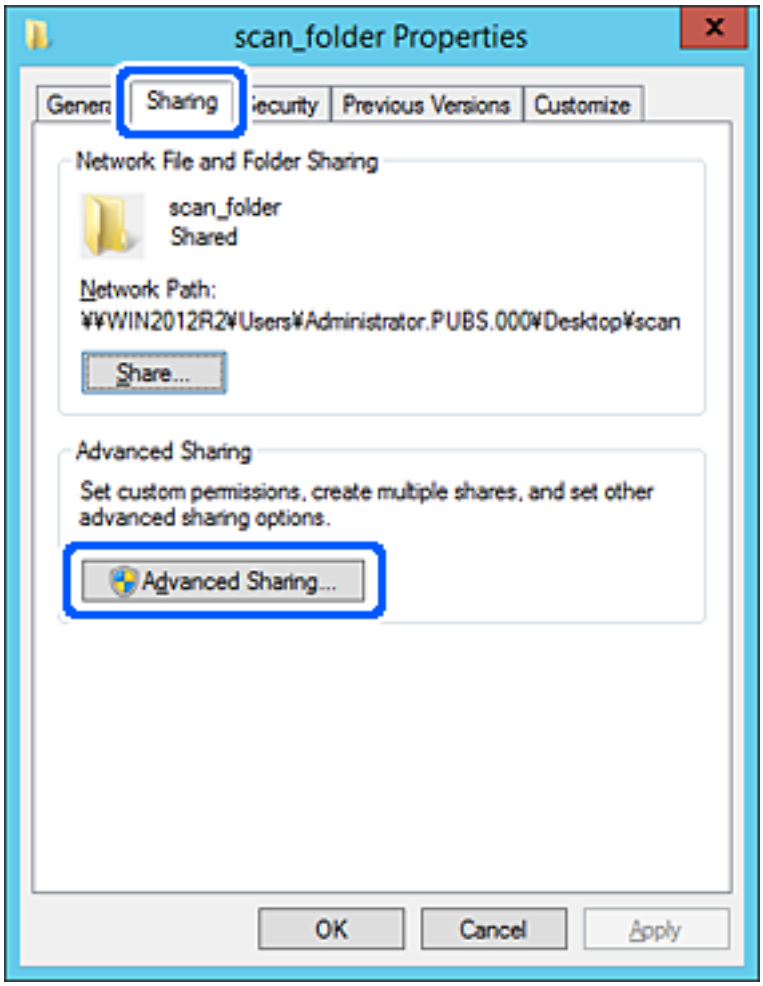
3. Vytvořte složku v kořenovém adresáři na disku, a poté ji pojmenujte „scan_folder“.

   Pro název složky použijte 1 až 12 alfanumerických znaků. Pokud dojde k překročení povoleného množství znaků pro název složky, mohou nastat potíže s přístupem z některých prostředí.

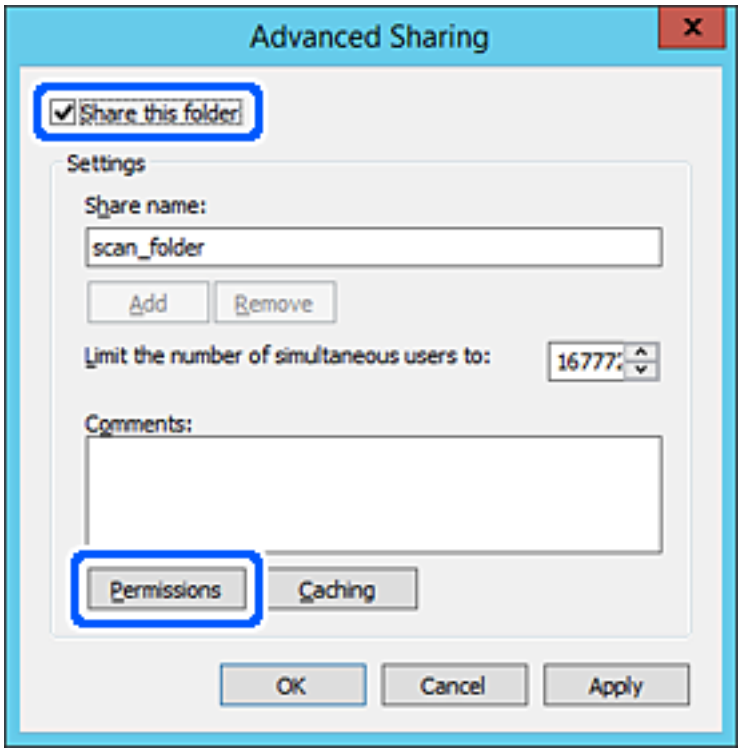
4. Klikněte pravým tlačítkem myši na složku a vyberte možnost **Vlastnosti**.



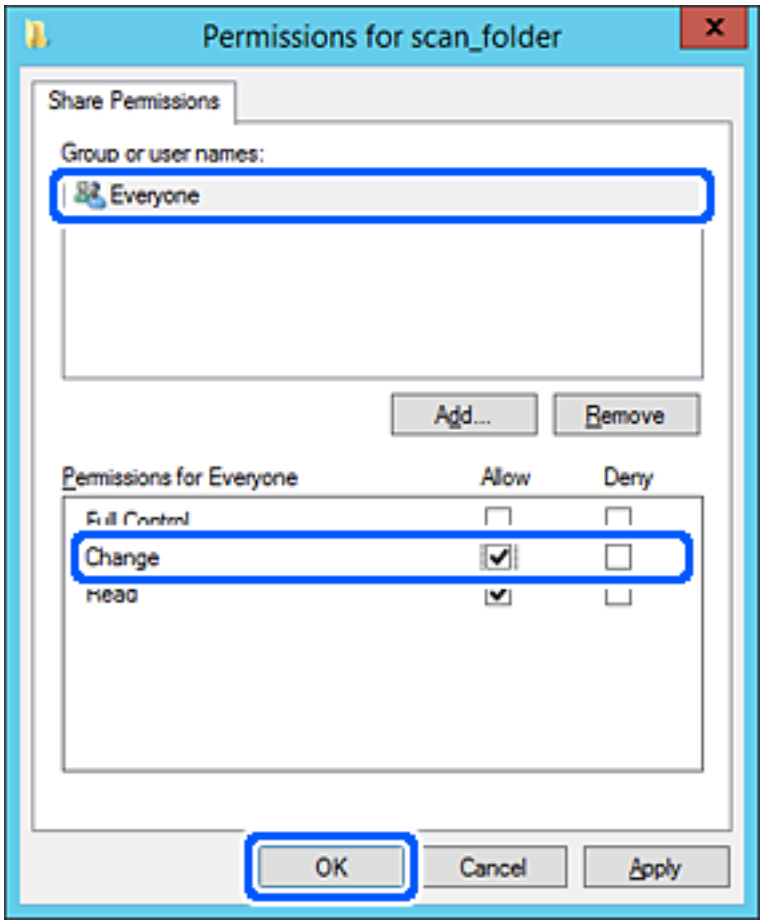
5. Klikněte na kartu **Rozšířené sdílení** v části **Sdílení**.



6. Vyberte možnost **Sdílet tuto složku** a poté klikněte na možnost **Oprávnění**.

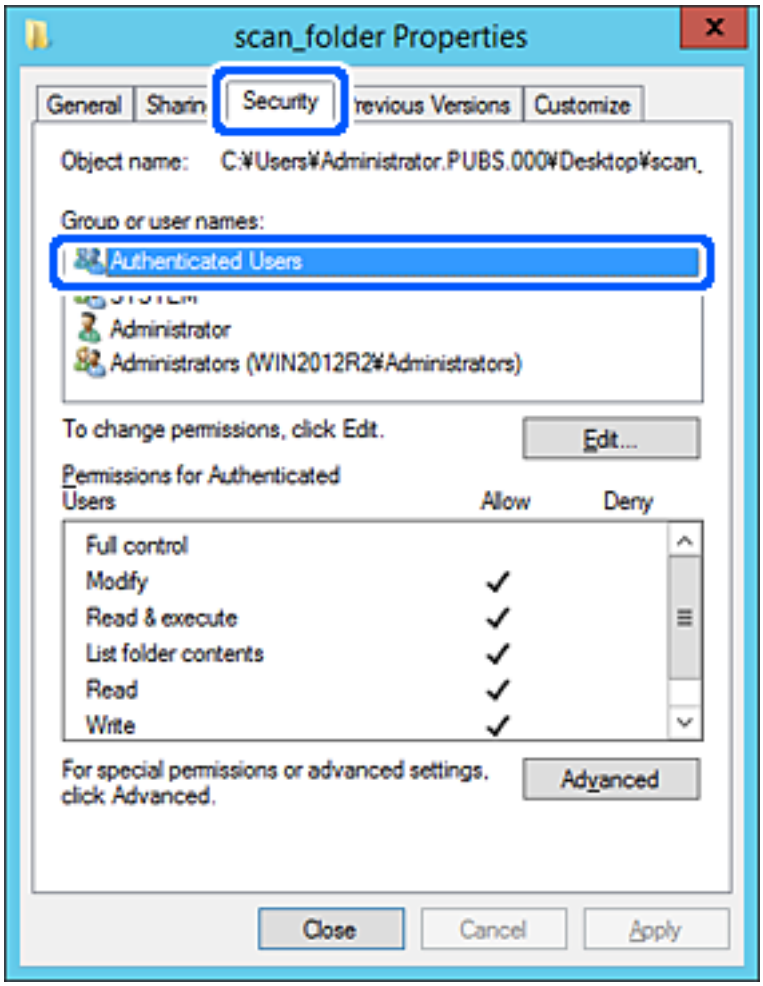


7. Vyberte skupinu **Všichni** v části **Názvy skupin nebo uživatelů**; vyberte možnost **Povolit** v položce **Změna**; poté klikněte na **OK**.



8. Klikněte na tlačítko **OK**.

9. Vyberte kartu **Zabezpečení** a poté vyberte možnost **Ověření uživatelé** v části **Názvy skupin nebo uživatelů**.

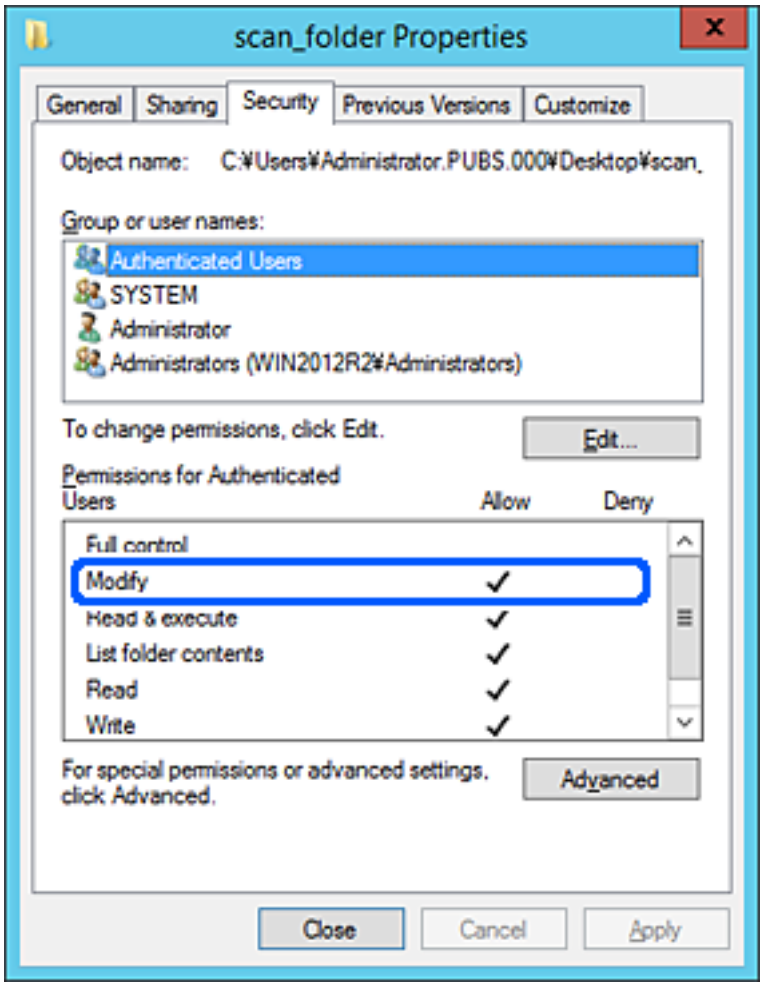


„Ověření uživatelé“ je speciální skupina, která zahrnuje všechny uživatele, kteří se mohou přihlásit k doméně nebo počítači. Tato skupina je zobrazena pouze pokud je složka vytvořena hned pod kořenovým adresářem.

Pokud není zobrazena, můžete ji přidat kliknutím na možnost **Upravit**. Více podrobností naleznete v souvisejících informacích.

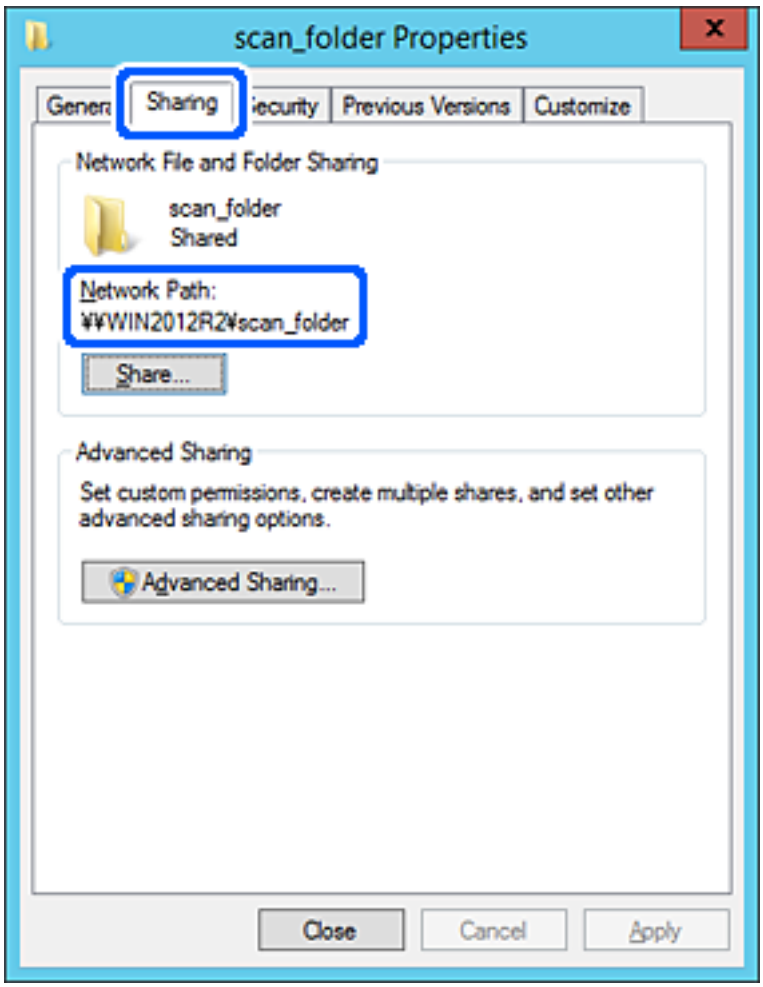
10. Zkontrolujte, zda je zvolena možnost **Povolit** pro **Upravit** v části **Oprávnění pro ověřené uživatele**.

    Pokud tato možnost není zvolena, vyberte možnost **Ověření uživatelé**, klikněte na volbu **Upravit**, vyberte možnost **Povolit** pro **Upravit** v části **Oprávnění pro ověřené uživatele** a poté klikněte na možnost **OK**.



11. Vyberte kartu **Sdílení**.

    Zobrazí se síťová cesta ke sdílené složce. Používá se v případě registrace kontaktu skeneru. Zapište si ji prosím.



12. Kliknutím na tlačítko **OK** nebo **Zavřít** zavřete obrazovku.

    Zkontrolujte, zda lze do souboru zapisovat nebo jej lze číst na sdílené složce z počítačů ve stejné doméně.

Související informace

➡ „Přidání skupiny nebo uživatele povolujícího přístup“ na str. 58

➡ „Zaregistrování cíle do kontaktů pomocí nástroje Web Config“ na str. 63

Příklad konfigurace pro osobní počítač

Toto vysvětlení je příkladem pro tvorbu sdílené složky na ploše uživatele, který je aktuálně přihlášen do počítače.

Uživatel, který se přihlásí k počítači a má práva správce může uskutečnit přístup do složky na ploše a k dokumentu ve složce, které jsou pod složkou Uživatel.

Tuto konfiguraci nastavte, pokud jiným uživatelům NECHCETE povolit čtení a zapisování do sdílené složky na osobním počítači.

❏ Místo pro vytvoření sdílené složky: plocha

❏ Cesta ke složce: C:\Users\xxxx\Desktop\scan_folder

❏ Povolit přístup přes síť (sdílení oprávnění): všichni

❏ Povolit přístup k systému souborů (zabezpečení): nepřidávejte, nebo přidejte názvy uživatelů/skupin pro povolení přístupu

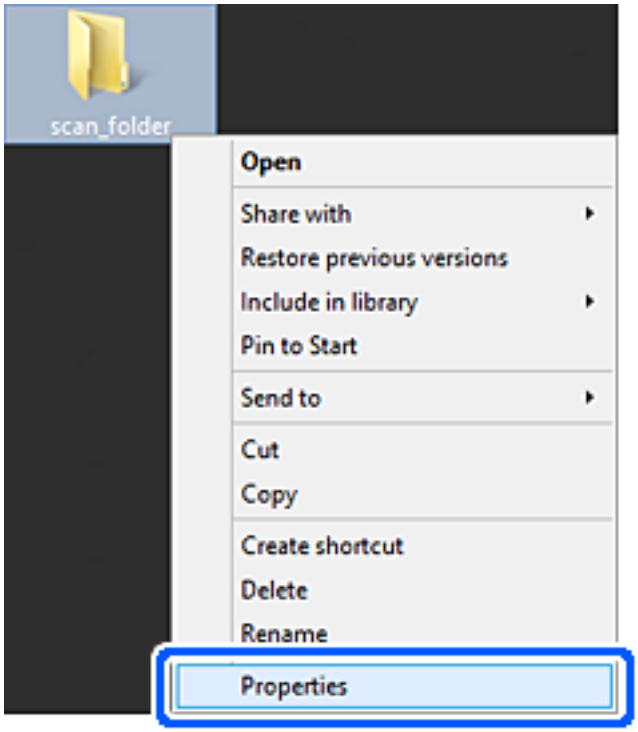
1. Přihlaste se do počítače, kde bude prostřednictvím uživatelského účtu s oprávněním správce vytvořena sdílená složka.

2. Spusťte průzkumníka.

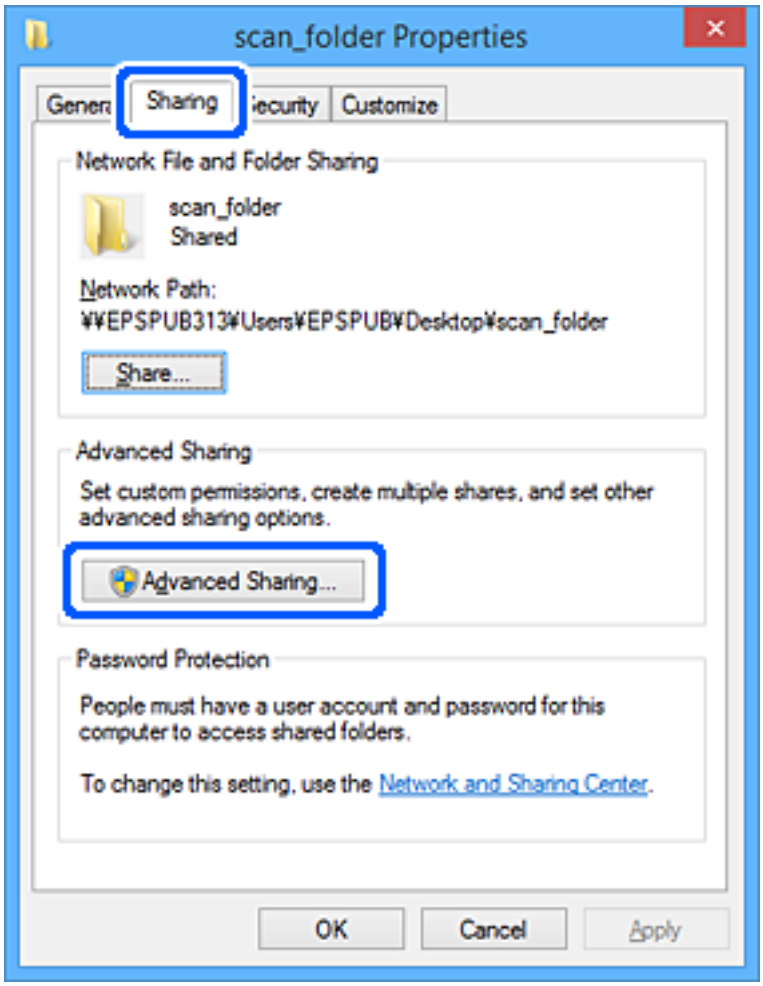
3. Vytvořte složku na ploše, a poté ji pojmenujte „scan_folder“.

   Pro název složky použijte 1 až 12 alfanumerických znaků. Pokud dojde k překročení povoleného množství znaků pro název složky, mohou nastat potíže s přístupem z některých prostředí.

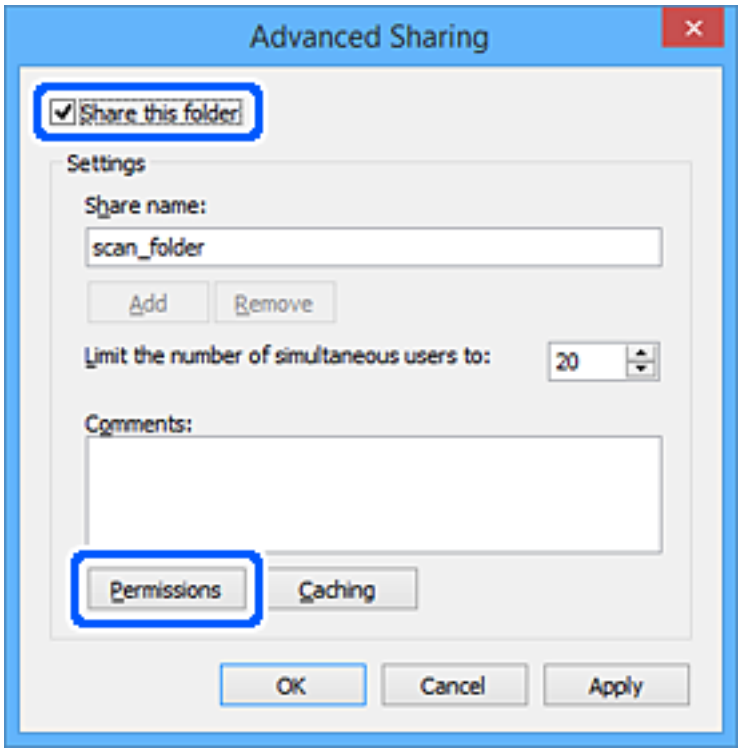
4. Klikněte pravým tlačítkem myši na složku a vyberte možnost **Vlastnosti**.



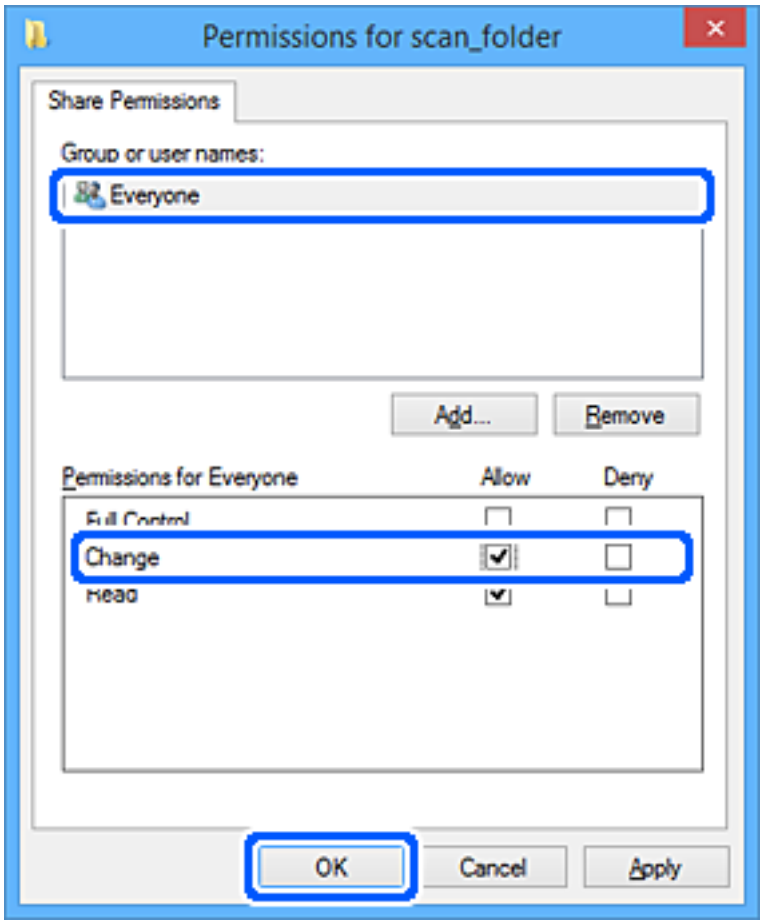
5. Klikněte na kartu **Rozšířené sdílení** v části **Sdílení**.



6. Vyberte možnost **Sdílet tuto složku** a poté klikněte na možnost **Oprávnění**.



7. Vyberte skupinu **Všichni** v části **Názvy skupin nebo uživatelů**; vyberte možnost **Povolit** v položce **Změna**; poté klikněte na **OK**.



8. Klikněte na tlačítko **OK**.

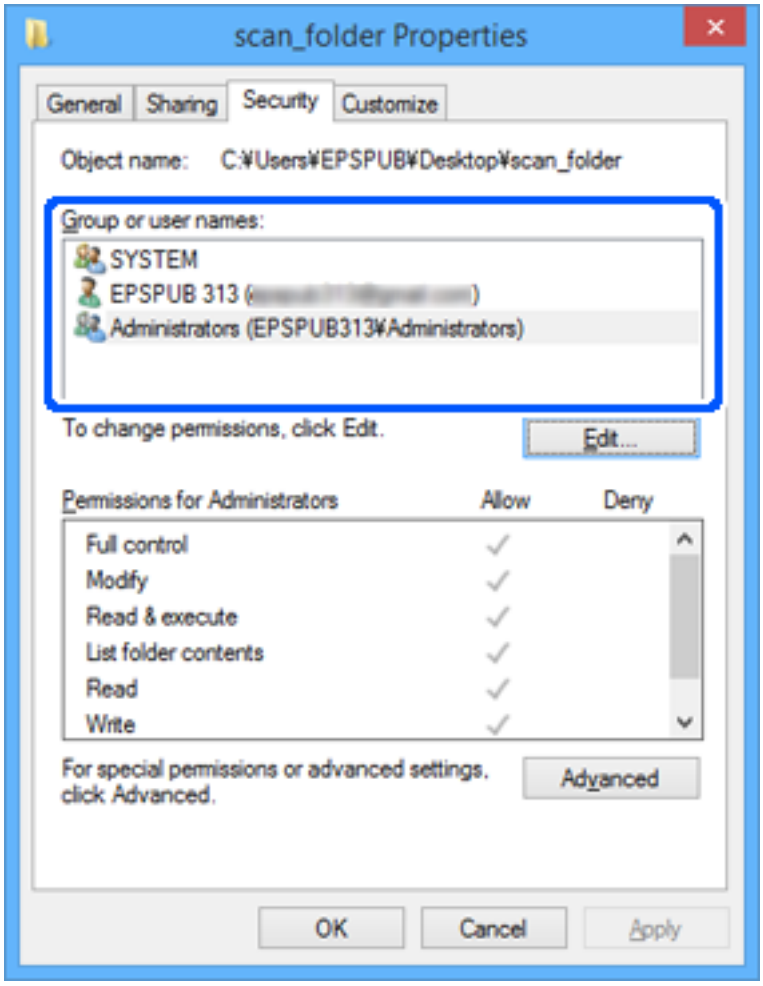
9. Vyberte kartu **Zabezpečení**.

10. Vyberte skupinu nebo uživatele pod položkou **Názvy skupiny nebo uživatelská jména**.

    Zde zobrazená skupina nebo uživatel má přístup do sdílené složky.

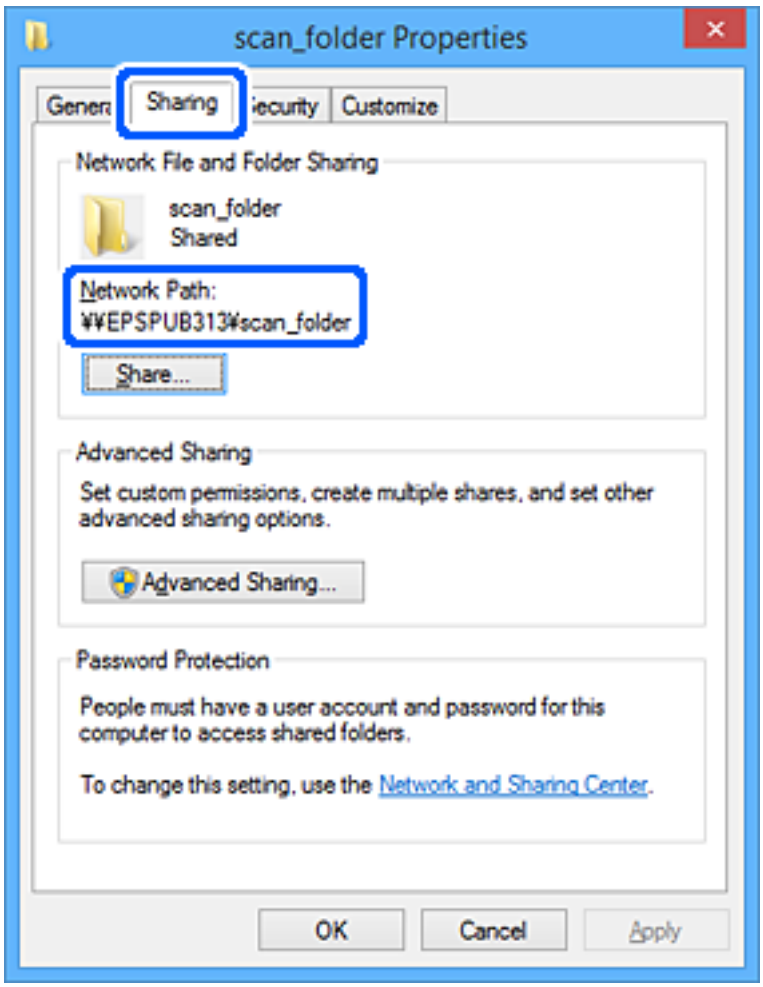
    V tomto případě má uživatel, který se přihlásí k tomuto počítači, a správce přístup ke sdílené složce.

V případě potřeby přidejte další oprávnění přístupu. To přidáte kliknutím na možnost **Upravit**. Více podrobností naleznete v souvisejících informacích.



11. Vyberte kartu **Sdílení**.

    Zobrazí se síťová cesta ke sdílené složce. Používá se v případě registrace kontaktu skeneru. Zapište si ji prosím.



12. Kliknutím na tlačítko **OK** nebo **Zavřít** zavřete obrazovku.

    Zkontrolujte, zda lze do souboru zapisovat nebo jej lze číst na sdílené složce z počítačů uživatelů nebo skupin s povolením k přístupu.

Související informace

➡ „Přidání skupiny nebo uživatele povolujícího přístup“ na str. 58
➡ „Zaregistrování cíle do kontaktů pomocí nástroje Web Config“ na str. 63

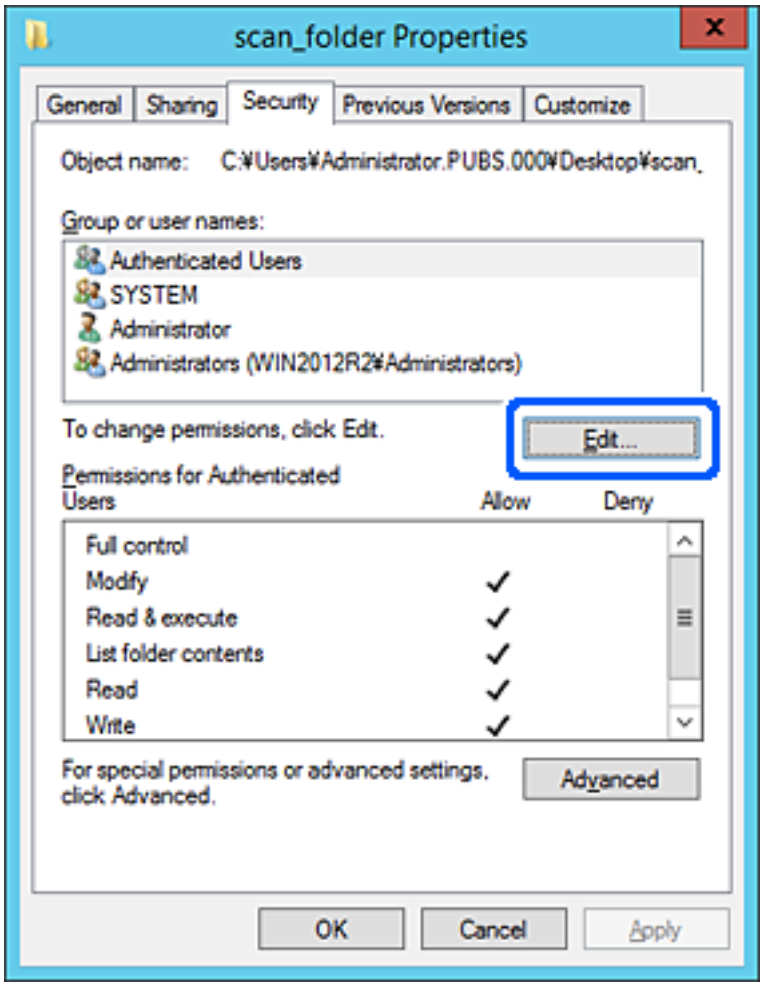
Přidání skupiny nebo uživatele povolujícího přístup

Můžete přidat skupinu nebo uživatele, který povoluje přístup.

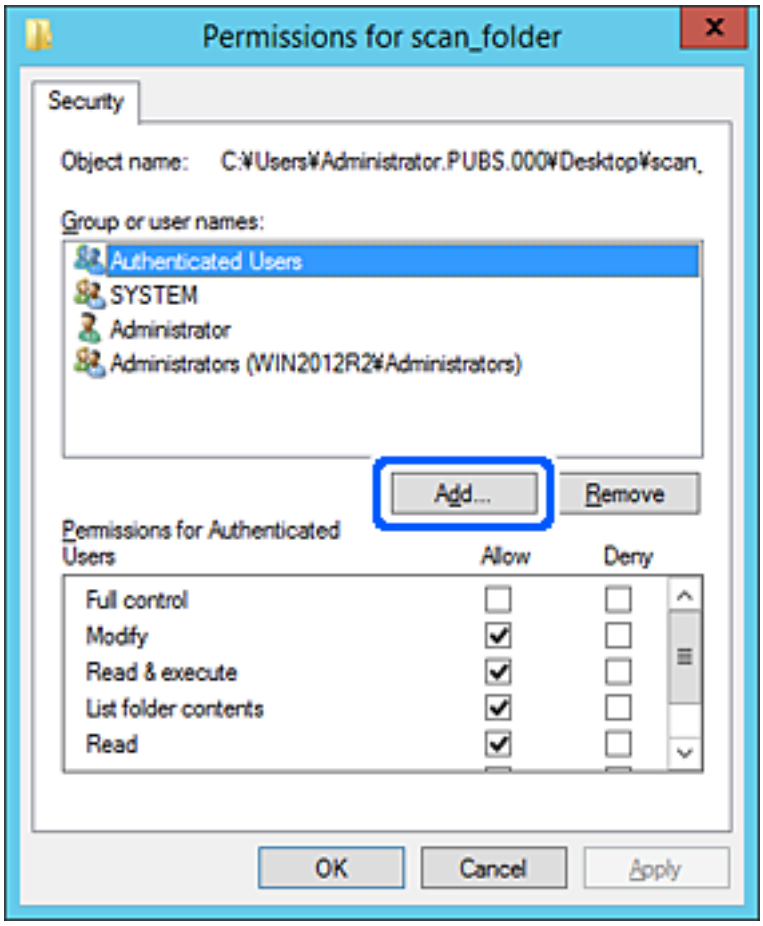
1. Klikněte pravým tlačítkem myši na složku a vyberte možnost **Vlastnosti**.

2. Vyberte kartu **Zabezpečení**.

3. Klikněte na tlačítko **Upravit**.



4. Klikněte na položku **Přidat** pod položkou **Názvy skupin nebo uživatelů**.

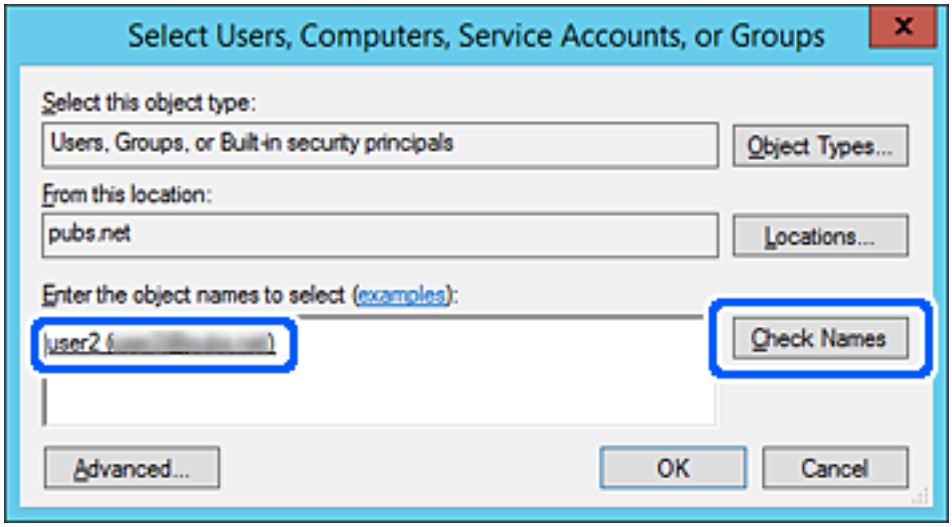


5. Zadejte název skupiny nebo uživatele, kterému chcete povolit přístup, a poté klikněte na možnost **Zkontrolovat názvy**.

   K názvu je přidáno podtržení.

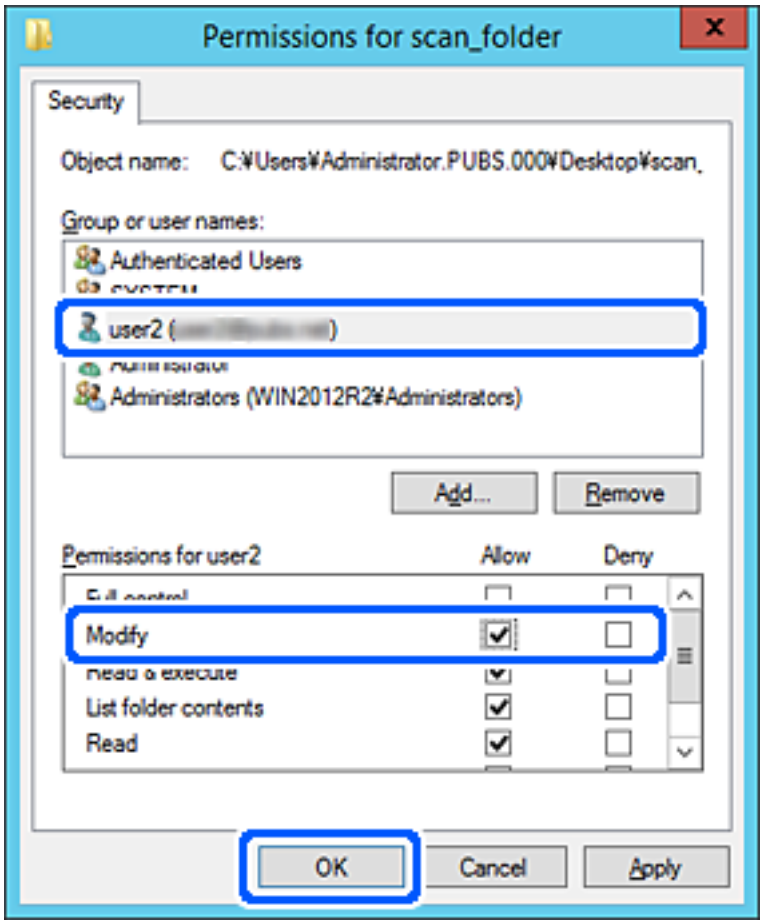
Poznámka:
Pokud neznáte plný název skupiny nebo uživatele, zadejte část názvu a poté klikněte na možnost ***Zkontrolovat názvy****. Zobrazí se seznam skupin nebo uživatelů, jejichž názvy obsahují zadanou část, poté můžete vybrat celý název ze seznamu.*

Pokud dojde ke shodě pouze s jedním záznamem, v části ***Zadejte název objektu, který chcete vybrat*** *se zobrazí celý název s podtržením.*



6. Klikněte na tlačítko **OK**.

7. Na kartě Oprávnění vyberte uživatelské jméno, které je zadané v části **Názvy skupin nebo uživatelů**, povolte možnost **Upravit** a pak klikněte na tlačítko **OK**.



8. Kliknutím na tlačítko **OK** nebo **Zavřít** zavřete obrazovku.

   Zkontrolujte, zda lze do souboru zapisovat nebo jej lze číst na sdílené složce z počítačů uživatelů nebo skupin s povolením k přístupu.

Zpřístupnění kontaktů

Registrace cílových umístění v seznamu kontaktů skeneru umožňuje snadno zadávat cílové umístění při skenování.

Můžete registrovat následující typy cílových umístění v seznamu kontaktů. Můžete zaregistrovat celkem až 300 položek.

Poznámka:
Server LDAP server (hledání LDAP) můžete také použít k zadání cílového umístění.

E-mail	Cílové umístění e-mailu. Nastavení e-mailového serveru musíte nakonfigurovat předem.
Síťová složka	Cílové umístění pro data skenování. Síťovou složku je nutné připravit předem.

Související informace

➡ „Spolupráce mezi serverem LDAP a uživateli“ na str. 69

Srovnání konfigurace kontaktů

K dispozici jsou tři nástroje ke konfigurování kontaktů skeneru: Web Config, Epson Device Admin a ovládací panel skeneru. V následující tabulce jsou uvedeny rozdíly mezi těmito třemi nástroji.

Funkce	Web Config*	Epson Device Admin	Ovládací panel skeneru
Registrace příjemce	✓	✓	✓
Úpravy příjemce	✓	✓	✓
Přidání skupiny	✓	✓	✓
Úpravy skupiny	✓	✓	✓
Odstranění příjemce nebo skupin	✓	✓	✓
Odstranění všech příjemců	✓	✓	–
Importování souboru	✓	✓	–
Exportování souboru	✓	✓	–

* Přihlašte se jako administrátor pro změnu nastavení.

Zaregistrování cíle do kontaktů pomocí nástroje Web Config

Poznámka:
Kontakty můžete zaregistrovat také na ovládacím panelu skeneru.

1. Otevřete nástroj Web Config a vyberte kartu **Sken** > **Kontakty**.
2. Vyberte číslo, které chcete zaregistrovat, a klikněte na možnost **Upravit**.
3. Zadejte hodnoty do polí **Jméno** a **Rejstříkové slovo**.
4. V poli **Typ** vyberte typ cíle.

   Poznámka:
   *Po dokončení registrace nelze možnost **Typ** již změnit. Pokud chcete typ změnit, odstraňte cíl a poté proveďte novou registraci.*
5. Pro každou položku zadejte hodnotu a poté klikněte na možnost **Použít**.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Položky nastavení cíle

Položky	Nastavení a vysvětlení
Běžná nastavení	
Jméno	Zadejte jméno zobrazené v kontaktech. Zadat můžete až 30 znaků ve formátu Unicode (UTF-8). Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
Rejstříkové slovo	Zadané jméno musí mít méně než 30 znaků kódování Unicode (UTF-8) aby se vyhledal kontakt použitím ovládacího panelu skeneru. Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
Typ	Slouží k výběru typu adresy, kterou chcete registrovat.
Přiřadit k část. použití	Slouží k výběru nastavení zaregistrované adresy jako často používané adresy. Pokud adresu nastavíte jako často používanou adresu, bude zobrazena v horní části obrazovky skenování a uživatel bude moci zadat cíl bez nutnosti zobrazit kontakty.
Email	
E-mailová adresa	Zadejte 1 až 255 znaků s použitím znaků A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.
Síťová složka (SMB)	
Uložit do	\\„cesta ke složce“ Zadejte umístění cílové složky. Zadat můžete 1 až 253 znaků ve formátu Unicode (UTF-8), ale není možné použít znak „\\“. Zadejte síťovou cestu zobrazenou v okně Vlastnosti složky. Podrobnosti o nastavení síťové cesty jsou uvedeny dále. „Příklad konfigurace pro osobní počítač“ na str. 52
Uživatelské jméno	Zadejte uživatelské jméno k přístupu k síťové složce. Zadat můžete až 30 znaků ve formátu Unicode (UTF-8). Nepoužívejte však řídicí znaky (0x00 až 0x1F a 0x7F).
Heslo	Zadejte heslo k přístupu k síťové složce. Zadat můžete až 20 znaků ve formátu Unicode (UTF-8). Nepoužívejte však řídicí znaky (0x00 až 0x1F a 0x7F).
FTP	
Zabezpečené připojení	Vyberte FTP nebo FTPS podle toho, jaký protokol pro přenos souborů podporuje server FTP. Chcete-li povolit komunikaci skeneru s opatřeními zabezpečení, vyberte možnost **FTPS**.
Uložit do	Zadejte název serveru. Zadat můžete 1 až 253 znaků ve formátu ASCII (0x20 až 0x7E) bez řetězce „ftp://“ nebo „ftps://“.
Uživatelské jméno	Zadejte uživatelské jméno k přístupu k serveru FTP. Zadat můžete až 30 znaků ve formátu Unicode (UTF-8). Nepoužívejte však řídicí znaky (0x00 až 0x1F a 0x7F). Pokud server povoluje anonymní připojení, zadejte uživatelské jméno, například Anonymní, a protokol FTP. Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
Heslo	Zadejte heslo k přístupu k serveru FTP. Zadat můžete až 20 znaků ve formátu Unicode (UTF-8). Nepoužívejte však řídicí znaky (0x00 až 0x1F a 0x7F). Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
Režim připojení	V nabídce vyberte režim připojení. Pokud je mezi skenerem a serverem FTP nastavena brána firewall, vyberte možnost **Pasivní režim**.

Položky	Nastavení a vysvětlení
Číslo portu	Zadejte číslo portu serveru FTP v rozmezí 1 až 65535.
Ověření certifikátu	Až tuto funkci povolíte, ověří se certifikát serveru FTP. Funkce je dostupná, když je v části **Zabezpečené připojení** vybrána možnost **FTPS**. Při nastavování je nutné importovat do skeneru Certifikát CA.
SharePoint(WebDAV)	
Zabezpečené připojení	Vyberte HTTP nebo HTTPS podle toho, jaký protokol pro přenos souborů server podporuje. Chcete-li povolit komunikaci skeneru s opatřeními zabezpečení, vyberte možnost **HTTPS**.
Uložit do	Zadejte název serveru. Zadat můžete 1 až 253 znaků ve formátu ASCII (0x20 až 0x7E) bez řetězce „http://" nebo „https://".
Uživatelské jméno	Zadejte uživatelské jméno k přístupu k serveru. Zadat můžete až 30 znaků ve formátu Unicode (UTF-8). Nepoužívejte však řídicí znaky (0x00 až 0x1F a 0x7F). Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
Heslo	Zadejte heslo k přístupu k serveru. Zadat můžete až 20 znaků ve formátu Unicode (UTF-8). Nepoužívejte však řídicí znaky (0x00 až 0x1F a 0x7F). Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
Ověření certifikátu	Až tuto funkci povolíte, ověří se certifikát serveru. Funkce je dostupná, když je v části **HTTPS** vybrána možnost **Zabezpečené připojení**. Při nastavování je nutné importovat do skeneru Certifikát CA.
Proxy server	Vyberte, zda chcete používat server proxy či nikoli.

Registrace cílů jako skupiny pomocí Web Config

Pokud je typ cíle nastaven na hodnotu **Email**, můžete cíle zaregistrovat jako skupinu.

1. Otevřete nástroj Web Config a vyberte kartu **Sken** > **Kontakty**.
2. Vyberte číslo, které chcete zaregistrovat, a klikněte na možnost **Upravit**.
3. V nabídce **Typ** vyberte skupinu.
4. U položky **Kontakt(y) pro Skup.** klikněte na možnost **Vybrat**.
   Zobrazí se dostupné cíle.
5. Vyberte cíl, který chcete zaregistrovat do skupiny, a poté klikněte na možnost **Vybrat**.
6. Zadejte hodnoty do polí **Jméno** a **Rejstříkové slovo**.
7. Vyberte, zda chcete přiřadit zaregistrovanou skupinu k často používané skupině.
   Poznámka:
   Cíle lze zaregistrovat k více skupinám.
8. Klikněte na položku **Použít**.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Zálohování a import kontaktů

Pomocí aplikace Web Config nebo jiných nástrojů můžete zálohovat a importovat kontakty.

V případě aplikace Web Config můžete provést zálohu kontaktů pomocí exportu nastavení skeneru, což zahrnuje kontakty. Exportovaný soubor nelze upravovat, protože je exportován jako binární soubor.

V případě importu nastavení skeneru do skeneru dojde k přepsání kontaktů.

V případě použití nástroje Epson Device Admin lze exportovat kontakty pouze z obrazovky vlastností zařízení. Také, pokud neprovádíte export položek zabezpečení, můžete exportované kontakty upravit a poté je importovat, tyto položky lze totiž ukládat ve formátu SYLK nebo CSV.

Import kontaktů pomocí možnosti Web Config

Pokud máte skener, který umožňuje zálohování kontaktů a je kompatibilní s tímto skenerem, můžete kontakty snadno zaregistrovat importováním záložního souboru.

Poznámka:
Pokyny k zálohování kontaktů skeneru naleznete v návodu poskytnutém ke skeneru.

Při importu kontaktů do tohoto skeneru postupujte podle následujících kroků.

1. Přistupte do nástroje Web Config, vyberte kartu **Správa zařízení** > **Exportovat a importovat hodnotu nastavení** > **Importovat**.
2. Zvolte soubor zálohy, vytvořený v **Soubor**, zadejte heslo a pak klikněte na **Další**.
3. Vyberte políčko **Kontakty** a klikněte na tlačítko **Další**.

Zálohování kontaktů pomocí možnosti Web Config

Data kontaktů se mohou ztratit v důsledku závady skeneru. Doporučujeme vytvoření zálohy při každé aktualizaci dat. Společnost Epson nepřebírá odpovědnost za jakoukoli ztrátu dat, za zálohování nebo obnovu dat a/nebo nastavení, a to ani v průběhu záruční doby.

Pomocí nástroje Web Config můžete v počítači zálohovat data kontaktů uložená ve skeneru.

1. Otevřete nástroj Web Config a poté vyberte kartu **Správa zařízení** > **Exportovat a importovat hodnotu nastavení** > **Exportovat**.
2. Zaškrtněte políčko **Kontakty** v rámci kategorie **Sken**.
3. Zadejte heslo, kterým zašifrujete exportovaný soubor.

   Toto heslo budete potřebovat při importu daného souboru. Pokud soubor nechcete zašifrovat, ponechte toto pole prázdné.
4. Klikněte na položku **Exportovat**.

Export a hromadná registrace kontaktů s použitím nástroje

Pokud používáte aplikaci Epson Device Admin, můžete zálohovat kontakty a upravovat exportované soubory, a poté registrovat vše najednou.

To se hodí, když chcete zálohovat pouze kontakty, nebo když chcete vyměnit skener a v rámci výměny potřebujete přenést kontakty ze starého do nového.

Export kontaktů

Informace o kontaktech můžete ukládat do souboru.

Soubory můžete upravovat ve formátu SYLK nebo csv pomocí tabulkové aplikace nebo textového editoru. Registraci můžete provést najednou po odstranění nebo přidání všech informací.

Informace, které obsahují položky zabezpečení, jako jsou například hesla a osobní údaje, můžete uložit v binárním formátu s heslem. Tento soubor nelze upravovat. Lze jej použít jako záložní soubor s informacemi včetně položek zabezpečení.

1. Spusťte aplikaci Epson Device Admin.
2. Vyberte možnost **Devices** v nabídce úloh na bočním panelu.
3. Ze seznamu vyberte zařízení, které chcete konfigurovat.
4. Klikněte na možnost **Device Configuration** na kartě **Home** v nabídce pásu karet.

   Pokud bylo nastaveno heslo správce, zadejte heslo a klikněte na možnost **OK**.
5. Klikněte na tlačítko **Common** > **Contacts**.
6. Vyberte formát exportu z nabídky **Export** > **Export items**.
   - ❏ All Items

     Proveďte export šifrovaného binárního souboru. Vyberte, zda chcete zahrnout položky zabezpečení, jako je například heslo či osobní údaje. Tento soubor nelze upravovat. Pokud vyberete tuto volbu, musíte nastavit heslo. Klikněte na možnost **Configuration** a nastavte heslo s použitím 8 až 63 znaků ve formátu ASCII. Toto heslo bude vyžadováno při importu binárního souboru.
   - ❏ Items except Security Information

     Proveďte export souborů ve formátu SYLK nebo csv. Vyberte, zda chcete upravit informace exportovaného souboru.
7. Klikněte na položku **Export**.
8. Určete, kam chcete soubor uložit, vyberte typ souboru a poté klikněte na možnost **Save**.

   Zobrazí se zpráva o dokončení.
9. Klikněte na položku **OK**.

   Prověřte, zda je soubor uložen na určeném místě.

Import kontaktů

Informace o kontaktech můžete importovat ze souboru.

Můžete importovat soubory uložené ve formátu SYLK nebo csv, nebo zálohované binární soubory, které obsahují položky zabezpečení.

1. Spusťte aplikaci Epson Device Admin.
2. Vyberte možnost **Devices** v nabídce úloh na bočním panelu.
3. Ze seznamu vyberte zařízení, které chcete konfigurovat.
4. Klikněte na možnost **Device Configuration** na kartě **Home** v nabídce pásu karet.

   Pokud bylo nastaveno heslo správce, zadejte heslo a klikněte na možnost **OK**.
5. Klikněte na tlačítko **Common** > **Contacts**.
6. Klikněte na možnost **Browse** v části **Import**.
7. Vyberte soubor, který chcete importovat, a poté klikněte na tlačítko **Open**.

   Pokud vyberete binární soubor, v části **Password** zadejte heslo, které jste nastavili při exportování souboru.
8. Klikněte na položku **Import**.

   Zobrazí se obrazovka potvrzení.
9. Klikněte na položku **OK**.

   Zobrazí se výsledek ověření.

   ❏ Edit the information read

   Klikněte, pokud chcete upravit informace individuálně.

   ❏ Read more file

   Klikněte, pokud chcete importovat více souborů.
10. Klikněte na **Import** a poté na možnost **OK** na obrazovce dokončení importu.

    Vraťte se na obrazovku vlastností zařízení.
11. Klikněte na položku **Transmit**.
12. Klikněte na **OK** na obrazovce s potvrzením.

    Nastavení jsou odeslána do skeneru.
13. Na obrazovce dokončení odeslání klikněte na možnost **OK**.

    Informace o skeneru jsou aktualizovány.

    Otevřete kontakty z aplikace Web Config nebo z ovládacího panelu skeneru a poté prověřte, zda byl kontakt aktualizován.

Spolupráce mezi serverem LDAP a uživateli

Pokud spolupracujete se serverem LDAP, můžete použít informaci o adrese, registrované na server LDAP, jako adresu příjemce e-mailu.

Konfigurace serveru LDAP

Chcete-li používat informace serveru LDAP, musíte jej zaregistrovat na skeneru.

1. Otevřete aplikaci Web Config a vyberte kartu **Síť** > **Server LDAP** > **Základní**.
2. Do všech polí zadejte hodnotu.
3. Vyberte **OK**.

   Zobrazí se vybraná nastavení.

Položky nastavení serveru LDAP

Položky	Nastavení a vysvětlení
Použít server LDAP	Vyberte možnost **Použít** nebo **Nepoužívejte**.
Adresa serveru LDAP	Zadejte adresu serveru LDAP. Zadejte 1 až 255 znaků ve formátu protokolu IPv4 nebo IPv6 nebo jména FQDN. V případě formátu FQDN zadejte alfanumerické znaky ve formátu ASCII (0x20 až 0x7E) nebo znak „-“, který však nezadávejte na začátek nebo konec adresy.
Číslo portu serveru LDAP	Zadejte číslo portu serveru LDAP pomocí čísel 1 až 65535.
Zabezpečené připojení	Určete metodu ověřování, když skener získává přístup k serveru LDAP.
Ověření certifikátu	Když tuto funkci povolíte, bude se ověřovat certifikát serveru LDAP. Doporučujeme tuto možnost nastavit na **Povolit**. Abyste ji mohli nastavit, je nutné do skeneru importovat **Certifikát CA**.
Časový limit hledání (s)	Zvolte časový limit pro vyhledávání, který může být mezi hodnotou 5 až 300.
Způsob ověření	Vyberte jednu z následujících metod. Pokud vyberete metodu **Ověření Kerberos** a chcete zadat nastavení protokolu Kerberos, vyberte možnost **Nastavení Kerberos**. Abyste mohli provádět Ověření Kerberos, je nutné následující prostředí. ❏ Skener může komunikovat se serverem DNS. ❏ Čas skeneru, serveru KDC a serveru nutného pro ověřování (server LDAP, server SMTP, souborový server) je synchronizovaný. ❏ Když se serveru služby přiřadí IP adresa, FQDN serveru služby se zaregistruje do zóny zpětného vyhledávání serveru DNS.
Sféra Kerberos k použití	Pokud nastavíte položku **Způsob ověření** na hodnotu **Ověření Kerberos**, vyberte sféru Kerberos, kterou chcete použít.

Položky	Nastavení a vysvětlení
DN správce / Uživatelské jméno	Zadejte uživatelské jméno serveru LDAP. Zadat můžete až 128 znaků ve formátu Unicode (UTF-8). Nepoužívejte řídicí znaky, například znaky 0x00 až 0x1F nebo 0x7F. Toto nastavení není použito, pokud je položka **Způsob ověření** nastavena na hodnotu **Anonymní ověření**. Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
Heslo	Zadejte heslo ověřování serveru LDAP. Zadat můžete až 128 znaků ve formátu Unicode (UTF-8). Nepoužívejte řídicí znaky, například znaky 0x00 až 0x1F nebo 0x7F. Toto nastavení není použito, pokud je položka **Způsob ověření** nastavena na hodnotu **Anonymní ověření**. Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.

Nastavení protokolu Kerberos

Pokud nastavíte položku **Způsob ověření** v nabídce **Server LDAP** > **Základní** na hodnotu **Ověření Kerberos**, zadejte na kartě **Síť** > **Nastavení Kerberos** následující nastavení protokolu Kerberos. U protokolu Kerberos můžete registrovat až 10 nastavení.

Položky	Nastavení a vysvětlení
Sféra (doména)	Zadejte hodnotu sféry ověřování protokolu Kerberos. Hodnota může být vyjádřena až 255 znaky standardu ASCII (0x20 až 0x7E). Pokud nechcete tuto položku registrovat, ponechte pole prázdné.
Adresa KDC	Zadejte adresu serveru ověřování protokolu Kerberos. Do pole zadejte maximálně 255 znaků ve formátu protokolu IPv4 nebo IPv6 nebo jména FQDN. Pokud nechcete tuto položku registrovat, ponechte pole prázdné.
Číslo portu (Kerberos)	Zadejte číslo portu serveru Kerberos pomocí čísel 1 až 65535.

Konfigurace nastavení vyhledávání serveru LDAP

Pokud nastavíte vyhledávání, můžete používat e-mailovou adresu registrovanou pro server LDAP.

1. Otevřete nástroj Web Config a vyberte kartu **Síť** > **Server LDAP** > **Nastavení hledání**.
2. Do všech polí zadejte hodnotu.
3. Chcete-li zobrazit výsledek nastavení, klepněte na tlačítko **OK**.

   Zobrazí se vybraná nastavení.

Položky nastavení vyhledávání serveru LDAP

Položky	Nastavení a vysvětlení
Báze hledání (rozlišující název)	Pokud chcete vyhledat nějakou doménu, zadejte název domény serveru LDAP. Zadejte 0 až 128 znaků ve formátu Unicode (UTF-8). Pokud nechcete vyhledat libovolný atribut, ponechte toto pole prázdné. Příklad místního adresáře serveru: dc=server,dc=local

Položky	Nastavení a vysvětlení
Počet hledaných položek	Zadejte počet položek vyhledávání. Zadat můžete 5 až 500 položek. Zadaný počet položek vyhledávání je uložen a dočasně zobrazen. I když počet položek vyhledávání přesáhne určený limit a zobrazí se chybové hlášení, vyhledávání bude možné dokončit.
Atribut uživatelského jména	Zadejte název atributu, který se zobrazí při vyhledávání uživatelských jmen. Zadejte 1 až 255 znaků ve formátu Unicode (UTF-8). Prvním znakem musí být některé z písmen a–z nebo A–Z. Příklad: cn, uid
Atribut zobrazení uživatelského jména	Zadejte název atributu, který se zobrazí jako uživatelské jméno. Zadejte 0 až 255 znaků ve formátu Unicode (UTF-8). Prvním znakem musí být některé z písmen a–z nebo A–Z. Příklad: cn, sn
Atribut e-mailové adresy	Zadejte název atributu, který se zobrazí při vyhledávání e-mailových adres. Zadejte kombinaci 1 až 255 znaků. Zadat můžete písmena A–Z a a–z, číslice 0–9 a znak -. Prvním znakem musí být některé z písmen a–z nebo A–Z. Příklad: e-mail
Libovolný atribut 1 - Libovolný atribut 4	Zadat můžete další libovolné atributy, které chcete vyhledat. Zadejte 0 až 255 znaků ve formátu Unicode (UTF-8). Prvním znakem musí být písmena a–z nebo A–Z. Pokud nechcete vyhledat libovolné atributy, ponechte toto pole prázdné. Příklad: o, ou

Kontrola připojení serveru LDAP

Provede test připojení k serveru LDAP pomocí parametrů nastavených v **Server LDAP** > **Nastavení hledání**.

1. Otevřete nástroj Web Config a vyberte kartu **Síť** > **Server LDAP** > **Test připojení**.
2. Vyberte **Spustit**.

   Bude zahájena zkouška připojení. Po dokončení zkoušky bude zobrazena kontrolní zpráva.

Reference ke zkoušce připojení serveru LDAP

Zprávy	Vysvětlení
Test připojení byl úspěšný.	Tato zpráva se zobrazí při úspěšně provedeném připojení k serveru.
Test připojení se nezdařil. Zkontrolujte nastavení.	Zobrazí se v následujících situacích: ❏ Adresa nebo číslo portu serveru LDAP nejsou správné. ❏ Vypršel časový limit. ❏ Položka **Použít server LDAP** je nastavena na hodnotu **Nepoužívejte**. ❏ Pokud je položka **Způsob ověření** nastavena na hodnotu **Ověření Kerberos**, nejsou nastavení, například **Sféra (doména)**, **Adresa KDC** a **Číslo portu (Kerberos)** správná.

Zprávy	Vysvětlení
Test připojení se nezdařil. Zjistěte Datum a čas ve vašem produktu nebo na server.	Tato zpráva se zobrazí, pokud selže připojení, protože nastavení času na skeneru a serveru LDAP se neshodují.
Ověření se nezdařilo. Zkontrolujte nastavení.	Zobrazí se v následujících situacích: ❏ Položky **Uživatelské jméno** a/nebo **Heslo** nejsou správné. ❏ Pokud je položka **Způsob ověření** nastavena na hodnotu **Ověření Kerberos**, nemusí být nakonfigurován čas/datum.
Do dokončení zpracování nelze produkt zpřístupnit.	Tato zpráva se zobrazí, pokud skener vykonává nějakou činnost.

Použití Document Capture Pro Server

Pomocí nástroje Document Capture Pro Server můžete spravovat metodu třídění, formát uložení a příjemce předávání výsledků skenování, provedeného z ovládacího panelu skeneru. Vyvolání a spuštění úlohy, která byla předtím registrována na serveru, můžete provést z ovládacího panelu skeneru.

Proveďte instalaci na serverovém počítači.

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

Nastavení režimu serveru

Chcete-li používat aplikaci Document Capture Pro Server, proveďte nastavení dle následujících instrukcí.

1. Otevřete nástroj Web Config a vyberte kartu **Sken** > **Document Capture Pro**.
2. Vyberte **Režim Server** pro **Režim**.
3. Zadejte adresu serveru s nainstalovanou aplikací Document Capture Pro Server pro **Adresa serveru**.

   Zadejte 2 až 255 znaků ve formátu IPv4, IPv6, název hostitele nebo formát FQDN. V případě formátu FQDN můžete použít alfanumerické znaky ve formátu ASCII (0x20–0x7E) a „-“ s výjimkou začátku a konce adresy.
4. Klikněte na položku **OK**.

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

Nastavení funkce AirPrint

Otevřete Web Config, vyberte kartu **Síť** a pak vyberte **Nastavení služby AirPrint**.

Položky	Vysvětlení
Název služby Bonjour	Zadejte název služby Bonjour pomocí textu ASCII (0x20–0x7E) a až 41 znaků.
Umístění služ. Bonjour	Zadejte popis umístění skeneru pomocí textu Unicode (UTF-8) a až 127 bajtů.

Položky	Vysvětlení
Wide-Area Bonjour	Nastavte, zda chcete používat funkci Wide-Area Bonjour. Pokud ji použijete, skener je třeba registrovat v DNS serveru, aby bylo možné vyhledat skener přes segment.
Povolit AirPrint	Bonjour a AirPrint (služba skenování) jsou povoleny.

Problémy při přípravě síťového skenování

Rady pro řešení problémů

❏ Kontrola přítomnosti chybových zpráv

Pokud došlo k chybě, nejdříve zkontrolujte, zda se na ovládacím panelu skeneru nebo obrazovce ovladače nezobrazily nějaké chybové zprávy. Pokud máte nastavené e-mailové upozornění v případě výskytu chyby, můžete takto rychle zjistit aktuální stav.

❏ Kontrola stavu komunikace

Zkontrolujte stav komunikace na straně serverového počítače nebo klientského počítače například pomocí příkazů ping nebo ipconfig.

❏ Test připojení

Pro kontrolu připojení mezi skenerem a poštovním serverem proveďte test připojení ze strany skeneru. Také proveďte kontrolu připojení z klientského počítače na server a zjistěte stav komunikace.

❏ Inicializace nastavení

Pokud nastavení ani komunikace nezobrazují žádné chyby, můžete problémy zkusit vyřešit vypnutím nebo inicializací síťových nastavení skeneru, a jejich následným novým nastavením.

Přístup Web Config není možný

Adresa IP není přiřazena ke skeneru.

Řešení

Ke skeneru možná není přiřazena adresa IP. Nakonfigurujte IP adresu pomocí ovládacího panelu skeneru. Údaje o aktuálním nastavení lze ověřit prostřednictvím ovládacího panelu skeneru.

Webový prohlížeč nepodporuje Pevnost šifrování pro SSL/TLS.

Řešení

SSL/TLS má Síla šifrování. Web Config můžete otevřít pomocí webového prohlížeče, který podporuje hromadná šifrování, jak je uvedeno níže. Zkontrolujte, zda používáte podporovaný prohlížeč.

❏ 80 bitů: AES256/AES128/3DES

❏ 112 bitů: AES256/AES128/3DES

❏ 128 bitů: AES256/AES128

❏ 192 bitů: AES256

❏ 256 bitů: AES256

Platnost Certifikát podepsaný CA vypršela.

Řešení

Pokud došlo k problému s expiračním datem certifikátu, zobrazí se zpráva „Platnost certifikátu vypršela“; tato zpráva se objeví po připojení k Web Config s komunikací SSL/TLS (https). Pokud se zpráva zobrazí před datem vypršení platnosti, zkontrolujte, zda je datum skeneru správně nakonfigurováno.

Obecný název certifikátu a skeneru se neshodují.

Řešení

Pokud se neshoduje běžný název certifikátu a skeneru, zobrazí se po přístupu na webovou konfiguraci pomocí komunikace SSL/TLS (https) zpráva „Název zabezpečovacího certifikátu se neshoduje···“. K tomu dochází proto, že se neshodují následující IP adresy.

❏ IP adresa skeneru zadaná k obecnému názvu pro vytvoření Certifikát podepsaný sebou samým nebo CSR

❏ IP adresa zadaná do webového prohlížeče během provozu Web Config

Pro Certifikát podepsaný sebou samým aktualizujte certifikát.

Pro Certifikát podepsaný CA použijte znovu certifikát pro skener.

Nastavení místní adresy na proxy serveru není nastaveno podle webového prohlížeče.

Řešení

Pokud je skener nastaven pro použití serveru proxy, nakonfigurujte webový prohlížeč tak, aby se nepřipojoval k místní adrese prostřednictvím serveru proxy.

❏ Windows:

Zvolte postup **Ovládací panel** > **Síť a internet** > **Možnosti internetu** > **Připojení** > **Nastavení LAN** > **Server Proxy**; poté nakonfigurujte systém tak, aby se nepoužíval server proxy pro LAN (místní adresy).

❏ Mac OS:

Vyberte **Předvolby systému** > **Síť** > **Pokročilé nastavení** > **Proxies** a poté registrujte místní adresu pro **Vynechání 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

DHCP je vypnuto v nastavení počítače.

Řešení

Pokud je DHCP pro automatické získávání IP adres na počítači vypnuto, není možné získat přístup k Web Config. Zapněte DHCP.

Příklady pro Windows 10:

Otevřete Ovládací panely a klikněte na **Síť a internet** > **Síť a centrum sdílení** > **Změnit nastavení adaptéru**. Otevřete okno Vlastnosti vašeho připojení a poté otevřete okno Vlastnosti **Internet Protocol Version 4 (TCP/IPv4)** nebo **Internet Protocol Version 6 (TCP/IPv6)**. Zkontroluje že je zvoleno nastavení **Získávat IP adresy automaticky**.

Přizpůsobení obrazovky Ovládacího panelu

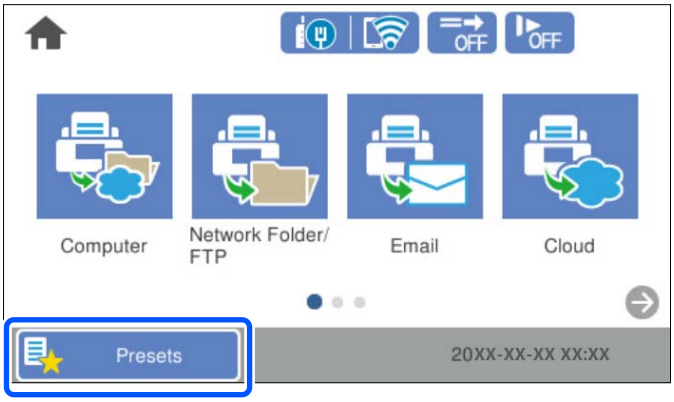
Registrování možností Předvolby

Často používaná nastavení skenování lze zaregistrovat jako **Předvolby**. Můžete zaregistrovat až 48 položek.

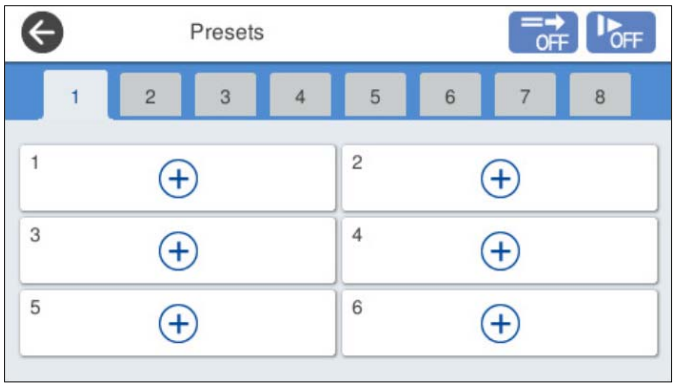
Poznámka:

- *Aktuální nastavení lze zaregistrovat výběrem možnosti* ☆ *na obrazovce Začít skenování.*
- *Možnost **Předvolby** lze též zaregistrovat v nástroji Web Config.*
  *Vyberte kartu **Sken** > **Předvolby**.*
- *Pokud zvolíte **Skenovat do počítače** při registraci, můžete zaregistrovat úlohu vytvořenou v Document Capture Pro jako **Předvolby**. Tato možnost je přístupná pouze pro počítače připojené do sítě. Registrujte úlohu předem v Document Capture Pro.*
- *Pokud je povolena ověřovací funkce, pouze správce může registrovat **Předvolby**.*

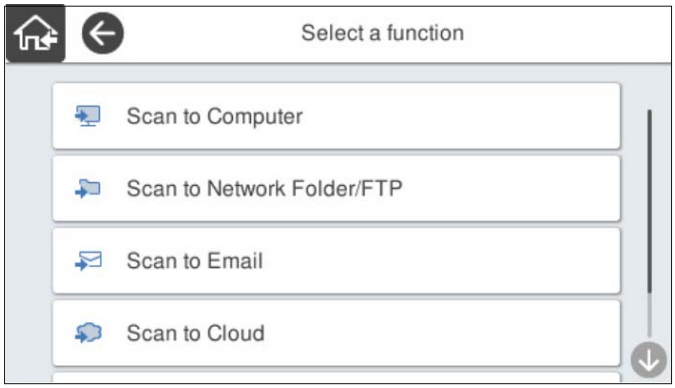
1. Vyberte možnost **Předvolby** na domovské obrazovce ovládacího panelu skeneru.



2. Vyberte možnost ⊕.



3. Vyberte nabídku, kterou chcete registrovat do předvolby.



4. Nastavte jednotlivé položky a pak vyberte možnost ☆+.

Poznámka:
*Když zvolíte **Skenovat do počítače**, zvolte počítač na kterém je nainstalována Document Capture Pro a poté zvolte registrovanou úlohu. Tato možnost je přístupná pouze pro počítače připojené do sítě.*

5. Proveďte nastavení předvolby.
   - ❏ **Název**: nastavte název.
   - ❏ **Nastavit ikonu**: nastavte obrázek a barvy ikony, kterou chcete zobrazit.
   - ❏ **Nastavení Rychlé odeslání**: když je zvolena předvolba, okamžitě zahájí skenování bez potvrzení.

     Při používání Document Capture Pro Server, i když nastavíte software na potvrzení obsahu úlohy před skenování, nastavení **Nastavení Rychlé odeslání** má prioritu nad softwarem.
   - ❏ **Obsah**: zkontrolujte nastavení skenování.

6. Vyberte možnost **OK**.

Možnosti nabídky položky Předvolby

Nastavení předvolby lze změnit výběrem ikony > v každé předvolbě.

Změnit název:

Změní se název předvolby.

Změnit ikonu:

Změní se obrázek ikony a barvu předvolby.

Nastavení Rychlé odeslání:

Když je zvolena předvolba, okamžitě se zahájí skenování bez potvrzení.

Změnit pozici:

Změní se pořadí zobrazení předvoleb.

Odstranit:

Předvolba se odstraní.

Přidat nebo odebrat ikonu na stránce Domů:

Přidá nebo odstraní ikonu předvolby z domovské obrazovky.

Potvrďte podrobnosti:

Zobrazí se nastavení předvolby. Předvolbu lze načíst tak, že vyberete možnost **Použít toto nastavení**.

Úprava domovské obrazovky ovládacího panelu

Domovskou obrazovku lze přizpůsobit výběrem možnosti **Nast.** > **Úpravy domovské obrazovky** na ovládacím panelu skeneru.

- ❏ Uspořádání: změní metodu zobrazení ikon nabídky.
  „Změna Uspořádání domovské obrazovky“ na str. 78
- ❏ Přidat ikonu:přidá ikony k vytvořeným možnostem **Předvolby** nebo obnoví ikony, které byly odstraněny z obrazovky.
  „Přidat ikonu“ na str. 79
- ❏ Odebrat ikonu: odstraní ikony z domovské obrazovky.
  „Odebrat ikonu“ na str. 80
- ❏ Přemístit ikonu: změní pořadí zobrazení ikon.
  „Přemístit ikonu“ na str. 81
- ❏ Obnovit výchozí zobrazení ikon: obnoví výchozí nastavení zobrazení pro domovskou obrazovku.
- ❏ Tapeta: umožňuje změnit barvu tapety domovské obrazovky.

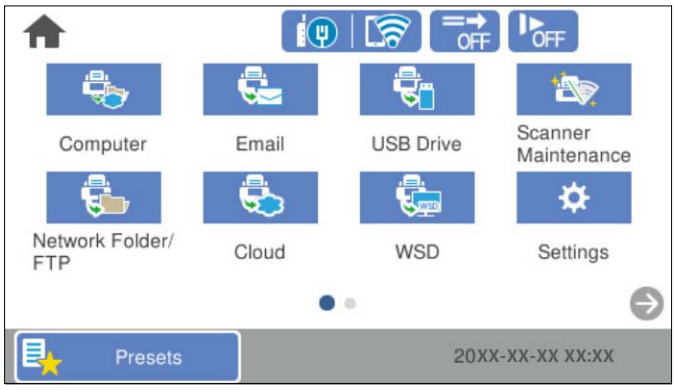
Změna Uspořádání domovské obrazovky

1. Na ovládacím panelu skeneru vyberte možnost **Nast.** > **Úpravy domovské obrazovky** > **Uspořádání**.

2. Vyberte možnost **Čára** nebo **Matice**.

   Čára:

   Matice:



3. Výběrem tlačítka se vraťte na domovskou obrazovku a zkontrolujte ji.

Přidat ikonu

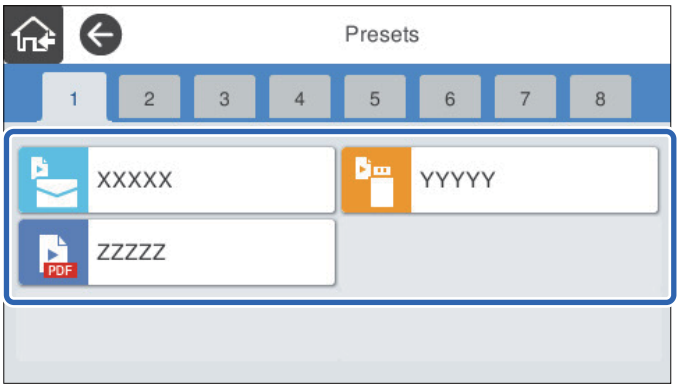
1. Na ovládacím panelu skeneru vyberte možnost **Nast.** > **Úpravy domovské obrazovky** > **Přidat ikonu**.

2. Vyberte možnost **Funkce** nebo **Předvolby**.

   ❏ Funkce: zobrazí výchozí funkce zobrazené na domovské obrazovce.

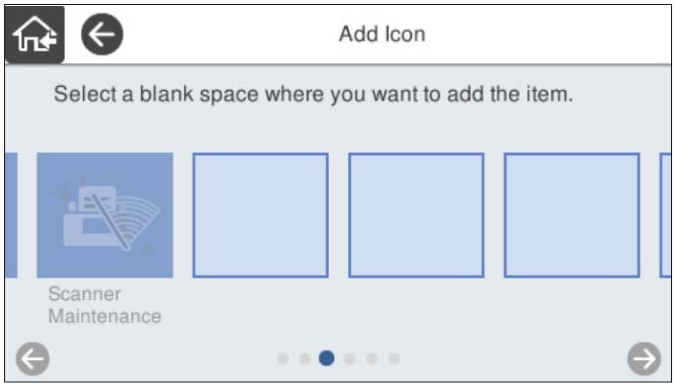
❏ Předvolby: zobrazí uložené předvolby.

3. Vyberte položku, kterou chcete přidat na domovskou obrazovku.



4. Na místě, kam chcete přidat položku, vyberte prázdný prostor.

   Pokud chcete přidat více ikon, opakujte kroky 3 a 4.

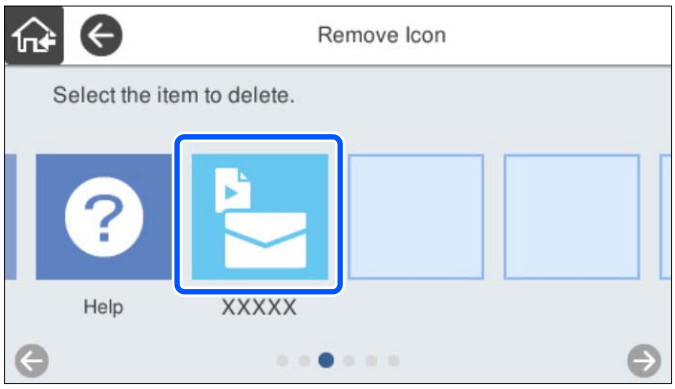


5. Výběrem tlačítka se vraťte na domovskou obrazovku a zkontrolujte ji.

Odebrat ikonu

1. Na ovládacím panelu skeneru vyberte možnost **Nast.** > **Úpravy domovské obrazovky** > **Odebrat ikonu**.

2. Vyberte ikonu, kterou chcete odstranit.



3. Pro dokončení vyberte tlačítko **Ano**.

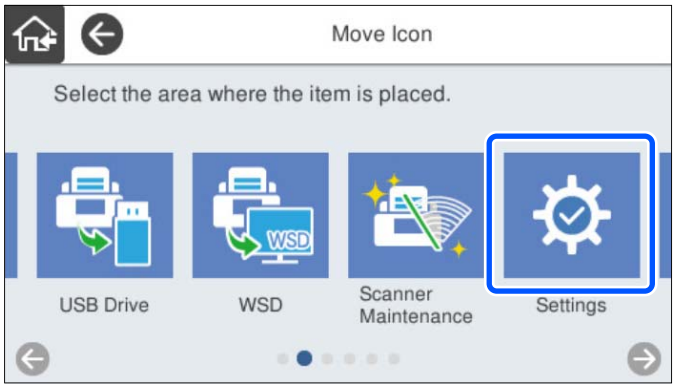
   Pokud chcete odstranit více ikon, opakujte kroky 2 a 3.

4. Výběrem tlačítka se vraťte na domovskou obrazovku a zkontrolujte ji.

Přemístit ikonu

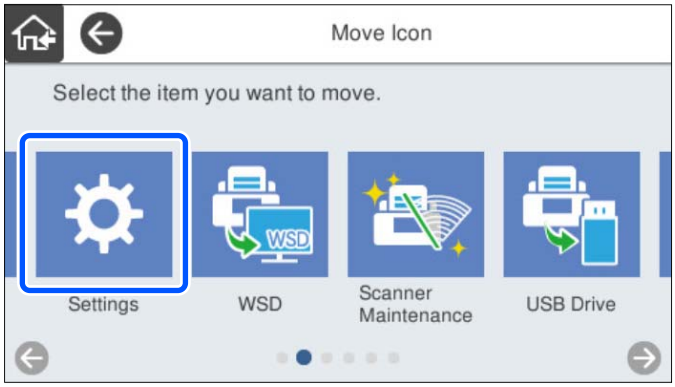
1. Na ovládacím panelu skeneru vyberte možnost **Nast.** > **Úpravy domovské obrazovky** > **Přemístit ikonu**.

2. Vyberte ikonu, kterou chcete přemístit.



3. Vyberte rámeček místa určení.

   Pokud se v rámečku místa určení nachází jiná ikona, bude nahrazena.



4. Výběrem tlačítka se vraťte na domovskou obrazovku a zkontrolujte ji.

Základní nastavení zabezpečení

Úvod do funkcí zabezpečení produktu

Tato část představuje funkce zabezpečení zařízení Epson.

Název funkce	Typ funkce	Co nastavit	Čemu zabránit
Nastavení hesla správce	Uzamkne systémové nastavení, například nastavení připojení sítě nebo USB.	Správce nastaví heslo zařízení. Nastavení nebo změny můžete provádět z nástroje Web Config nebo ovládacího panelu skeneru.	Zabránění nepovoleného čtení a změn informací uložených na zařízení, například ID, hesla, nastavení sítě a podobně. Také omezí širokou řadu rizik zabezpečení, například únik informací síťového prostředí nebo zásad zabezpečení.
Nastavení externího zařízení	Ovládání rozhraní, které se připojuje k zařízení.	Povolí nebo zakáže USB propojení s počítačem.	USB propojení s počítačem: zabrání neoprávněnému používání zařízení zákazem skenování, aniž by procházelo sítí.

Související informace

➡ „Konfigurace hesla správce“ na str. 84
➡ „Vypnutí externího rozhraní“ na str. 90

Nastavení správce

Konfigurace hesla správce

Když nastavíte heslo správce, můžete zabránit uživatelům ve změně nastavení správy systému. Výchozí hodnoty jsou nastaveny v okamžik nákupu. Měňte je dle potřeby.

Poznámka:
Následující poskytuje výchozí hodnoty pro informace o správci.

❏ *Uživatelské jméno (používá se pouze pro Web Config): žádné (prázdné)*

❏ *Heslo: sériové číslo skeneru*

Pro nalezení sériového čísla zkontrolujte štítek nalepený na zadní stranu skeneru.

Heslo správce můžete změnit pomocí nástroje Web Config, ovládacího panelu skeneru nebo nástroje Epson Device Admin. Pokud používáte nástroj Epson Device Admin, projděte si průvodce Epson Device Admin nebo nápovědu.

Změna hesla správce pomocí nástroje Web Config

V poli Web Config změňte heslo správce.

1. Otevřete Web Config a vyberte kartu **Zabezpečení produktu** > **Změnit heslo správce**.

2. Zadejte nezbytné informace do **Aktuální heslo**, **Uživatelské jméno**, **Nové heslo** a **Potvrzení nového hesla**.

   Zadejte alespoň jeden znak pro nové heslo.

   Poznámka:
   Následující poskytuje výchozí hodnoty pro informace o správci.

   ❏ *Uživatelské jméno: není (prázdný)*

   ❏ *Heslo: sériové číslo skeneru*

   Pro nalezení sériového čísla zkontrolujte štítek nalepený na zadní stranu skeneru.

   > ***Důležité:***
   > *Nezapomeňte si uložit nastavení heslo správce. Pokud heslo zapomenete, nebudete jej moci obnovit a budete moci požádat o pomoc personál servisu.*

3. Vyberte **OK**.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Změna hesla správce na ovládacím panelu

Heslo správce můžete změnit na ovládacím panelu skeneru.

1. Na ovládacím panelu skeneru vyberte možnost **Nast.**.

2. Vyberte možnost **Správa systému** > **Nastavení správce**.

3. Vyberte možnost **Heslo správce** > **Změnit**.

4. Zadejte aktuální heslo.

   Poznámka:
   Nastavení v okamžik zakoupení (výchozí hodnota) pro heslo správce je sériové číslo skeneru.

   Pro nalezení sériového čísla zkontrolujte štítek nalepený na zadní stranu skeneru.

5. Zadejte nové heslo.

   Zadejte alespoň jeden znak.

   > ***Důležité:***
   > *Nezapomeňte si uložit nastavení heslo správce. Pokud heslo zapomenete, nebudete jej moci obnovit a budete moci požádat o pomoc personál servisu.*

6. Pro potvrzení znovu zadejte nové heslo.

Zobrazí se zpráva o dokončení.

Použití možnosti Nastavení zámku pro ovládací panel

Možnost Nastavení zámku můžete použít k uzamčení ovládacího panelu a zabránění změně položek týkajících se nastavení systému uživateli.

Poznámka:
Pokud povolíte možnost Nastavení ověření na skeneru, Nastavení zámku bude také povolena na ovládacím panelu. Ovládací panel nelze odemknout, pokud je povolena možnost Nastavení ověření.

I když možnost Nastavení ověření zakážete, možnost Nastavení zámku zůstane povolena. Pokud ji chcete zakázat, můžete nastavení změnit z ovládacího panelu nebo nástroje Web Config.

Nastavení Nastavení zámku z ovládacího panelu

1. Pokud chcete zrušit **Nastavení zámku** po povolení, klepněte na  v pravém horním rohu obrazovky Domů a přihlaste se jako správce.

    se nezobrazí, když je **Nastavení zámku** zakázán. Pokud chcete toto nastavení povolit, přejděte do dalšího kroku.

2. Vyberte **Nast.**.

3. Vyberte možnost **Správa systému** > **Nastavení správce**.

4. Vyberte možnost **Zap.** nebo **Vyp.** jako **Nastavení zámku**.

Nastavení Nastavení zámku z nástroje Web Config

1. Vyberte kartu **Správa zařízení** > **Ovládací panel**.

2. Vyberte **Zapnuto** nebo **Vypnuto** pro **Provozní zámek**.

3. Klikněte na položku **OK**.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Položky Nastavení zámku v nabídce Nast.

Toto je seznam položek, které jsou uzamčeny v nabídce **Nast.** na ovládacím panelu prostřednictvím Nastavení zámku.

✓: k uzamčení.

- : není k uzamčení.

Nabídka Nast.	Nastavení zámku
Základní nastavení	-

Nabídka Nast.		Nastavení zámku
	Jas LCD	-
	Zvuky	-
	Časovač vyp.	✓
	Časovač vypnutí	✓
	Nastavení datumu / času	✓
	Jazyk/Language	✓/-*
	Klávesnice (V závislosti na vaší oblasti nemusí být tato funkce dostupná.)	-
	Časový limit operace	✓
	Přip. PC prostř. USB	✓
	Napájení zapnuto	✓
Nastavení skeneru		-
	Pomalu	-
	Čas zastavení při dvojitém vložení	✓
	Funkce DFDS	-
	Ochrana papíru	✓
	Detekce znečištění skla	✓
	Ultrazv. detekce dvojitého zavedení	✓
	Časový limit režimu automatického zavádění	✓
	Potvrdit příjemce	✓
Úpravy domovské obrazovky		✓
	Uspořádání	✓
	Přidat ikonu	✓
	Odebrat ikonu	✓
	Přemístit ikonu	✓
	Obnovit výchozí zobrazení ikon	✓
	Tapeta	✓
Nastavení uživatele		✓
	Síťová složka/FTP	✓
	Email	✓
	Cloud	✓
	USB disk	✓

Nabídka Nast.		**Nastavení zámku**
Nastavení sítě		✓
	Nast. Wi-Fi	✓
	Instalace drátové LAN	✓
	Stav sítě	✓
	Upřesnit	✓
Nastavení webové služby		✓
	Služby Epson Connect	✓
Document Capture Pro		-
	Změnit nastavení	✓
Správa Kontaktů		-
	Registrovat/Odstranit	✓/-*
	Časté	-
	Zobrazit možnosti	-
	Možnosti vyhledávání	-
Správa systému		✓
	Správa Kontaktů	✓
	Nastavení správce	✓
	Omezení	✓
	Šifrování hesla	✓
	Průzkum mezi zákazníky	✓
	Nastavení WSD	✓
	Obnovit výchozí nastavení	✓
	Aktualizovat firmware	✓
Informace o zařízení		-

Nabídka Nast.			Nastavení zámku
	Sériové číslo		-
	Aktuální verze		-
	Celkový počet skenů		-
	Počet 1stranných skenů		-
	Počet skenů Oboustranně		-
	Počet skenů nosného listu		-
	Počet skenů po výměně válce		-
	Počet skenů po pravidel. čištění		-
	Resetovat počet skenů		✓
Údržba skeneru			-
	Čištění válce		-
	Výměna válce		-
		Resetovat počet skenů	✓
		Pokyny pro výměnu	-
	Pravidelné čištění		-
		Resetovat počet skenů	✓
		Pokyny pro čištění	-
	Čištění skla		-
Nastavení výstrahy výměny válce			✓
	Nast. upozornění počít.		✓
Nastavení upozornění pravidelného čištění			✓
	Nastavení upozornění varování		✓
	Nast. upozornění počít.		✓

* Můžete určit, zda povolit změny v části **Správa systému** > **Omezení** nebo ne.

Přihlašování jako správce na ovládacím panelu

K přihlášení jako správce z ovládacího panelu skeneru můžete použít libovolné z následujících metod.

1. Klepněte na  v pravé horní části obrazovky.
   - ❏ Po povolení možnosti Nastavení ověření se ikona zobrazí na obrazovce **Vítejte** (obrazovka pohotovostního režimu ověřování).
   - ❏ V případě zákazu Nastavení ověření se ikona zobrazí na domovské obrazovce.

2. Po zobrazení potvrzovací obrazovky klepněte na **Ano**.

3. Zadejte heslo správce.

   Zobrazí se zpráva o dokončeném přihlášení a pak se zobrazí domovská obrazovka na ovládacím panelu.

K odhlášení klepněte na  v pravé horní části obrazovky Domů.

Vypnutí externího rozhraní

Rozhraní, které se používá k připojení zařízení ke skeneru, je možné vypnout. Proveďte nastavení omezení, abyste omezili jiné skenování, než prostřednictvím sítě.

Poznámka:
Omezení nastavení lze rovněž provést na ovládacím panelu skeneru.

Přip. PC prostř. USB: ***Nast.*** *>* ***Základní nastavení*** *>* ***Přip. PC prostř. USB***

1. Otevřete nástroj Web Config a vyberte kartu **Zabezpečení produktu** > **Externí rozhraní**.

2. U funkcí, které chcete nastavit, vyberte možnost **Zakázat**.

   Pokud budete zrušit ovládání, zvolte možnost **Povolit**.

   Přip. PC prostř. USB

   Použití připojení USB můžete omezit z počítače. Chcete-li jej omezit, zvolte **Zakázat**.

3. Klikněte na položku **OK**.

4. Ověřte, zda vypnutý port nelze používat.

   Přip. PC prostř. USB

   Pokud je ovladač tiskárny nainstalován v počítači

   Připojte skener k počítači pomocí USB kabelu a ověřte, zda skener neskenuje.

   Pokud není ovladač tiskárny nainstalován v počítači

   Windows:

   Spusťte správce zařízení a nechte jej spuštěný, připojte skener k počítači pomocí kabelu USB a pak ověřte, zda zobrazení obsahu správce zařízení zůstalo nezměněno.

   Mac OS:

   Připojte skener k počítači pomocí USB kabelu a ověřte, zda nelze přidat skener z nabídky **Tiskárny a skenery**.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Sledování vzdáleného skeneru

Kontrola informací pro vzdálený skener

V části **Stav** můžete pomocí nástroje Web Config zjistit následující informace o provozním skeneru.

❏ Stav produktu

Zkontrolujte stav, cloudové služby, číslo produktu, MAC adresu apod.

❏ Stav sítě

Zkontrolujte informace o stavu připojení k síti, IP adresu, DNS server apod.

❏ Stav používání

Zkontrolujte skenování v první den, počet skenování apod.

❏ Stav hardwaru

Zkontrolujte stav jednotlivých funkcí skeneru.

❏ Snímek panelu

Zobrazí snímek obrazovky zobrazené na ovládacím panelu skeneru.

Přijímání e-mailových oznámení když dojde k událostem

O e-mailových upozorněních

Jedná se o funkci upozornění, která v případě události, jako je například zastavení skenování či chyba skeneru, odešle e-mail na určenou adresu.

Můžete zaregistrovat až pět příjemců a u každého z nich můžete upravit nastavení upozornění.

Abyste mohli tuto funkci používat, je nutné před nastavením upozornění provést nastavení poštovního serveru.

Související informace

➡ „Konfigurace poštovního serveru“ na str. 41

Konfigurace e-mailového oznámení

Nakonfigurujte e-mailové oznámení pomocí nástroje Web Config.

1. Otevřete nástroj Web Config a vyberte kartu **Správa zařízení** > **Oznámení e-mailem**.
2. Nastavte e-mailové oznámení subjektu.

   Vybere obsah zobrazený na subjektu ze dvou rozevíracích nabídek.

   ❏ Vybraný obsah se zobrazí vedle položky **Předmět**.

   ❏ Stejný obsah nelze nastavit nalevo nebo napravo.

   ❏ Pokud počet znaků v části **Location** překročí 32 bajtů, znaky překračující 32 bajtů jsou vynechány.

3. Zadejte e-mailovou adresu k odeslání e-mailu s oznámením.

   Použijte znaky A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @ a zadejte od 1 do 255 znaků.

4. Vyberte jazyk e-mailových oznámení.

5. Zaškrtněte políčko u události, pro kterou chcete přijímat oznámení.

   Počet **Nastavení oznámení** je spojen s číslem cílového umístění **Nastavení e-mailové adresy**.

   Příklad:

   Pokud chcete zaslat oznámení na e-mailovou adresu nastavenou pro číslo 1 v části **Nastavení e-mailové adresy** když se změnilo heslo správce, zaškrtněte políčko pro sloupec **1** v řadě **Bylo změněno heslo správce**.

6. Klikněte na položku **OK**.

   Potvrďte, zda bude e-mailové oznámení odesláno způsobením události.

   Příklad: došlo ke změně hesla správce.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Položky pro oznámení e-mailem

Položky	Nastavení a vysvětlení
Bylo změněno heslo správce	Poznámka, když dojde ke změně hesla správce.
Chyba skeneru	Poznámka, když dojde k chybě skeneru.
Funkce Wi-Fi	Poznámka, když došlo k chybě rozhraní bezdrátové sítě LAN.

Řešení problémů

Zapomenuté heslo správce

Potřebujete pomoc od servisního personálu. Obraťte se na místního prodejce.

Poznámka:
Níže jsou uvedeny prvotní údaje pro administrátory Web Config.

❏ *Uživatelské jméno: není (prázdný)*

❏ *Heslo: sériové číslo skeneru*

Pro nalezení sériového čísla zkontrolujte štítek nalepený na zadní stranu skeneru. Při obnovení výchozího nastavení pro heslo správce je heslo vráceno do původního stavu.

Rozšířené nastavení zabezpečení

Nastavení zabezpečení a prevence nebezpečí

Když je skener připojen k síti, můžete na něj přistoupit ze vzdáleného umístění. Navíc skener může sdílet mnoho osob, což je užitečné při zlepšování provozní účinnosti a komfortu. Rizika jako ilegální přístup, ilegální používání a manipulace s daty jsou na vzestupu. Pokud používáte skener v prostředí, kde máte přístup k internetu, jsou rizika ještě větší.

U skenerů, které nemají ochranu přístupu z vnějšího prostředí, bude možné z internetu načítat kontakty, které jsou v nich uloženy.

Chcete-li se riziku vyhnout, skenery Epson mají řadu technologií zabezpečení.

Nastavte skener dle potřeby v souladu podmínkami životního prostředí, které byly vytvořeny prostřednictvím údajů o prostředí zákazníky.

Název	Typ funkce	Co nastavit	Čemu zabránit
Ovládání protokolu	Ovládá protokoly a služby, které budou použity ke komunikaci mezi skenery a počítači a povoluje a zakazuje funkce.	Protokol nebo služba, které jsou použity na samostatně povolené nebo zakázané funkce.	Omezení bezpečnostních rizik, ke kterým může docházet prostřednictvím nezamýšlených použití zabráněním uživatelům v používání zbytečných funkcí.
Komunikace SSL/TLS	Obsah komunikace je zašifrován pomocí komunikace SSL/TLS při přístupu ze skeneru na server Epson na internetu, například při komunikaci s počítačem přes webový prohlížeč pomocí Epson Connect a aktualizace firmwaru.	Získejte certifikát podepsaný certifikační autoritou a poté jej importujte do skeneru.	Vymazání identifikace skeneru pomocí osvědčení podepsaného CA zabrání vzniku falešných identit a neoprávněnému přístupu. Navíc je obsah komunikace SSL/TLS chráněn a zabraňuje úniku obsahu pro data skenování a informace nastavení.
IPsec/IP filtrování	Můžete nastavit povolení ukončení a odříznutí dat, která jsou od jistého klienta nebo jsou konkrétním typem. Jelikož IPsec chrání data pomocí paketovací jednotky IP (šifrování a ověřování), můžete bezpečně komunikovat nezabezpečeným protokolem.	Vytvořte základní zásady a individuální zásady k nastavení klienta nebo zadejte data, která budou mít přístup do skeneru.	Chraňte neoprávněný přístup a manipulaci a zachytávání komunikačních údajů do skeneru.
IEEE 802.1X	Pouze umožňuje oprávněným uživatelům připojení k síti. Umožňuje využívání skeneru pouze oprávněnému uživateli.	Nastavení ověřování na server RADIUS (server ověřování).	Chrání neoprávněný přístup a používání skeneru.

Související informace

- „Řízení pomocí protokolů“ na str. 95
- „Komunikace SSL/TLS se skenerem“ na str. 103
- „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 105
- „Připojení skeneru k síti IEEE802.1X“ na str. 116

Nastavení funkce zabezpečení

Při nastavení IPsec/IP filtrování nebo IEEE 802.1X doporučujeme otevřít Web Config pomocí SSL/TLS ke komunikaci informací nastavení za účelem omezení rizik zabezpečení jako manipulace nebo zachytávání.

Nezapomeňte nakonfigurovat heslo správce před nastavením IPsec/IP filtrování nebo IEEE 802.1X.

Řízení pomocí protokolů

Můžete skenovat do různých umístění a pomocí různých protokolů. Můžete rovněž provést síťové skenování z neurčeného množství síťových počítačů.

Můžete snížit bezpečnostní rizika neoprávněného používání omezením skenování z konkrétních umístění nebo řízením dostupných funkcí.

Řídící protokoly

Nakonfigurujte nastavení protokolů podporovaných skenerem.

1. Otevřete aplikaci Web Config a poté vyberte kartu **Zabezpečení sítě** tab > **Protokol**.
2. Nakonfigurujte jednotlivé položky.
3. Klikněte na položku **Další**.
4. Klikněte na položku **OK**.

   Nastavení se vztahují na skener.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Protokoly, které lze povolit nebo zakázat

Protokol	Popis
Nastavení Bonjour	Můžete zadat, zda používat Bonjour. Protokol Bonjour se používá k vyhledávání zařízení, ke skenování atd.
Nastavení SLP	Můžete povolit nebo zakázat funkci SLP. SLP se používá ke skenování stisknutím tlačítka nebo prohledávání sítě v nástroji EpsonNet Config.
Nastavení WSD	Můžete povolit nebo zakázat funkci WSD. Když je tato funkce povolena, můžete přidávat zařízení WSD a skenovat z portu WSD.
Nastavení LLTD	Můžete povolit nebo zakázat funkci LLTD. Když je tato funkce povolena, je zobrazena na mapě sítě Windows.
Nastavení LLMNR	Můžete povolit nebo zakázat funkci LLMNR. Když je tato funkce zapnutá, můžete rozlišení názvu použít bez NetBIOS, i když nemůžete použít DNS.

Protokol	Popis
Nastavení SNMPv1/v2c	Můžete určit, zda povolit protokol SNMPv1/v2c či nikoli. Ten se používá k nastavení zařízení, monitorování atd.
Nastavení SNMPv3	Můžete určit, zda povolit protokol SNMPv3 či nikoli. Ten se používá k šifrovanému nastavení zařízení, monitorování atd.

Položky nastavení protokolu

Nastavení Bonjour

Položky	Nastavení hodnoty a popisu
Použít Bonjour	Tuto možnost použijte k vyhledání nebo používání zařízení prostřednictvím Bonjour.
Název Bonjour	Zobrazí název Bonjour.
Název služby Bonjour	Zobrazí název služby Bonjour.
Location	Zobrazí název umístění Bonjour.
Wide-Area Bonjour	Nastavte, zda chcete používat Wide-Area Bonjour.

Nastavení SLP

Položky	Nastavení hodnoty a popisu
Povolit SLP	Tuto možnost vyberte k povolení funkce SLP. Tato možnost se používá například k hledání v síti v Epson-Net Config.

Nastavení WSD

Položky	Nastavení hodnoty a popisu
Povolit WSD	Tuto možnost vyberte k povolení přidávání zařízení pomocí WSD a skenování z portu WSD.
Časový limit skenování (s)	Zadejte hodnotu vypršení časového limitu komunikace pro skenování WSD v rozsahu od 3 do 3 600 sekund.
Název zařízení	Zobrazí název zařízení WSD.
Location	Zobrazí název umístění WSD.

Nastavení LLTD

Položky	Nastavení hodnoty a popisu
Povolit LLTD	Tuto možnost vyberte k povolení LLTD. Skener bude zobrazen na mapě sítě Windows.
Název zařízení	Zobrazí název zařízení LLTD.

Nastavení LLMNR

Položky	Nastavení hodnoty a popisu
Povolit LLMNR	Tuto možnost vyberte k povolení LLMNR. Rozlišení názvu můžete použít bez NetBIOS, i když nemůžete použít DNS.

Nastavení SNMPv1/v2c

Položky	Nastavení hodnoty a popisu
Povolit SNMPv1/v2c	Vyberte k povolení SNMPv1/v2c.
Oprávnění k přístupu	Nastaví oprávnění přístupu, pokud je povolena možnost SNMPv1/v2c. Vyberte možnost **Pouze pro čtení** nebo **Čtení/zápis**.
Název komunity (pouze pro čtení)	Zadejte 0 až 32 znaků formátu ASCII (0x20 až 0x7E).
Název komunity (čtení/zápis)	Zadejte 0 až 32 znaků formátu ASCII (0x20 až 0x7E).

Nastavení SNMPv3

Položky		Nastavení hodnoty a popisu
Povolit SNMPv3		SNMPv3 se povolí, pokud je políčko zaškrtnuto.
Uživatelské jméno		Zadejte od 1 do 32 znaků pomocí 1bajtových znaků.
Nastavení ověření		
	Algoritmus	Vyberte algoritmus pro ověřování SNMPv3.
	Heslo	Zadejte heslo pro ověřování SNMPv3. Zadejte od 8 do 32 znaků ve formátu ASCII (0x20–0x7E). Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
	Potvrzení hesla	Pro potvrzení zadejte nakonfigurované heslo.
Nastavení šifrování		
	Algoritmus	Vyberte algoritmus pro šifrování SNMPv3.
	Heslo	Zadejte heslo pro šifrování SNMPv3. Zadejte od 8 do 32 znaků ve formátu ASCII (0x20–0x7E). Pokud nechcete tuto hodnotu určit, ponechte pole prázdné.
	Potvrzení hesla	Pro potvrzení zadejte nakonfigurované heslo.
Kontextový název		Zadejte do 32 znaků nebo méně v kódování Unicode (UTF-8). Pokud nechcete tuto hodnotu určit, ponechte pole prázdné. Počet znaků, které lze zadat, se liší v závislosti na jazyce.

Používání digitálního certifikátu

Informace o digitální certifikaci

❏ Certifikát podepsaný CA

Toto je certifikát podepsaný certifikační autoritou (CA). Můžete ho získat na vyžádání od certifikační autority. Tento certifikát potvrzuje existenci skeneru a používá se pro komunikaci SSL/TLS k zajištění bezpečnosti datové komunikace.

Pro komunikaci SSL/TLS se používá jako certifikát serveru.

Pokud je nastaven na filtrování IPsec/IP nebo komunikaci IEEE 802.1X, používá se jako certifikát klienta.

❏ Certifikát CA

Tento certifikát je součástí řetězce Certifikát podepsaný CA. Také se nazývá certifikát zprostředkující certifikační autority. Používá ho webový prohlížeč k ověřování cesty k certifikátu skeneru při přístupu na server druhé strany nebo do nástroje Web Config.

Pro certifikát CA nastavte, kdy se má ověřovat cesta k certifikátu serveru při přístupu ze skeneru. Pro skener nastavte kvůli potvrzování cesty k certifikátu Certifikát podepsaný CA pro připojení SSL/TLS.

Certifikát CA skeneru můžete získat od certifikační autority, která ho vydala.

Další možnost je získat certifikát CA použitý k ověřování serveru druhé strany od certifikační autority, která vydala Certifikát podepsaný CA druhého serveru.

❏ Certifikát podepsaný sebou samým

Toto je certifikát, který skener sám podepisuje a vydává. Nazývá se také kořenový certifikát. Protože vydavatel certifikuje sám sebe, není takový certifikát spolehlivý a nezabrání vydávání se za někoho jiného.

Použijte ho pro nastavení zabezpečení a provádění jednoduché komunikace SSL/TLS bez certifikátu Certifikát podepsaný CA.

Pokud tento certifikát použijete pro komunikaci SSL/TLS, ve webovém prohlížeči se může zobrazit výstraha zabezpečení, protože certifikát není zaregistrovaný ve webovém prohlížeči. Certifikát Certifikát podepsaný sebou samým lze používat pouze pro komunikaci SSL/TLS.

Související informace

➡ „Konfigurace Certifikát podepsaný CA“ na str. 98

➡ „Aktualizování samopodpisovatelného certifikátu“ na str. 102

➡ „Konfigurace Certifikát CA“ na str. 102

Konfigurace Certifikát podepsaný CA

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. Otevřete aplikaci Web Config a poté vyberte kartu **Zabezpečení sítě**.Dále vyberte položku **SSL/TLS** > **Certifikát** nebo **Filtrování IPsec/IP** > **Certifikát klienta** nebo **IEEE802.1X** > **Certifikát klienta**.

   Bez ohledu na vaši volbu můžete získat stejný certifikát a běžně jej používat.

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

   Otevře se stránka pro vytvoření CSR.

3. Do všech polí zadejte hodnotu.

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

4. Klikněte na možnost **OK**.

   Zobrazí se zpráva o dokončení.

5. Vyberte kartu **Zabezpečení sítě**.Dále vyberte možnost **SSL/TLS** > **Certifikát** nebo **Filtrování IPsec/IP** > **Certifikát klienta** nebo **IEEE802.1X** > **Certifikát klienta**.

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 Certifikát podepsaný CA.*

7. Odešlete CSR certifikační agentuře a získejte Certifikát podepsaný CA.

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

8. Uložte vydaný Certifikát podepsaný CA do počítače připojeného ke skeneru.

   Získání Certifikát podepsaný CA je dokončeno uložením certifikátu do umístění.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Položky nastavení CSR

Položky	Nastavení a vysvětlení
Délka klíče	Vyberte délku klíče pro CSR.

Položky	Nastavení a vysvětlení
Obecné jméno	Můžete zadat od 1 do 128 znaků. Pokud se jedná o IP adresu, měla by být statickou IP adresou. Můžete zadat 1 až 5 adres IPv4, adres IPv6, názvů hostitele, FQDN oddělováním pomocí čárek. První prvek se uloží pod společným názvem a další prvky se uloží do pole aliasu subjektu certifikátu. Příklad: Adresa IP skeneru: 192.0.2.123, Název skeneru: EPSONA1B2C3 Obecné jméno: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
Organizace/ Organizační jednotka/ Lokalita/ Stát/kraj	Můžete zadat od 0 do 64 znaků ve formátu ASCII (0x20–0x7E). Samostatné názvy můžete rozdělit pomocí čárek.
Země	Zadejte kód země pomocí čísla o dvou číslicích určeného pomocí ISO-3166.
E-mailová adresa odesílatele	Můžete zadat e-mailovou adresu odesilatele pro nastavení poštovního serveru. Zadejte stejnou e-mailovou adresu jako činí **E-mailová adresa odesílatele** pro kartu **Síť** > **Poštovní server** > **Základní**.

Import certifikátu podepsaného certifikační autoritou

Importuje získaný certifikát Certifikát podepsaný CA do skeneru.

Důležité:

❏ *Zkontrolujte, zda je nastaveno správné datum a čas skeneru. Certifikát může být neplatný.*

❏ *Pokud certifikát získáte pomocí CSR vytvořeného z nástroje Web Config, můžete certifikát importovat jednou.*

1. Otevřete nástroj Web Config a poté vyberte kartu **Zabezpečení sítě**. Dále vyberte možnost **SSL/TLS** > **Certifikát** nebo **Filtrování IPsec/IP** > **Certifikát klienta** nebo **IEEE802.1X** > **Certifikát klienta**.

2. Klikněte na tlačítko **Importovat**

   Otevře se stránka pro import certifikátu.

3. Do všech polí zadejte hodnotu. Při ověřování cesty k certifikátu ve webovém prohlížeči, který používáte pro přístup ke skeneru, nastavte **Certifikát CA 1** a **Certifikát CA 2**.

   Požadovaná nastavení se můžou lišit podle toho, kde vytvoříte CSR a jaký má certifikát formát souboru. Zadejte hodnoty pro požadované položky podle následujících informací.

   ❏ Certifikát formátu PEM/DER získaný z nástroje Web Config

   ❏ **Soukromý klíč**: nekonfigurujte, protože skener obsahuje soukromý klíč.

   ❏ **Heslo**: neprovádějte konfiguraci.

   ❏ **Certifikát CA 1**/**Certifikát CA 2**: volitelné

   ❏ Certifikát formátu PEM/DER získaný z počítače

   ❏ **Soukromý klíč**: je třeba nastavit.

   ❏ **Heslo**: neprovádějte konfiguraci.

   ❏ **Certifikát CA 1**/**Certifikát CA 2**: volitelné

❏ Certifikát formátu PKCS#12 získaný z počítače

❏ **Soukromý klíč**: neprovádějte konfiguraci.

❏ **Heslo**: volitelné

❏ **Certifikát CA 1/Certifikát CA 2**: neprovádějte konfiguraci.

4. Klikněte na položku **OK**.

   Zobrazí se zpráva o dokončení.

Poznámka:
*Kliknutím na tlačítko **Potvrdit** potvrdíte informace o certifikátu.*

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Importování položek nastavení certifikátu podepsaného CA

Položky	Nastavení a vysvětlení
Certifikát serveru nebo Certifikát klienta	Vyberte formát certifikátu. Pro připojení SSL/TLS se zobrazí Certifikát serveru. Pro IPsec/IP filtrování nebo IEEE 802.1X se zobrazí Certifikát klienta.
Soukromý klíč	Pokud získáte certifikát ve formátu PEM/DER pomocí CSR vytvořeného z počítače, zadejte soubor soukromého klíče, který se shoduje s certifikátem.
Heslo	Pokud je formát souboru **Certifikát se soukromým klíčem (PKCS#12)**, zadejte heslo pro šifrování soukromého klíče, které se nastaví při získání certifikátu.
Certifikát CA 1	Pokud je formát vašeho certifikátu **Certifikát (PEM/DER)**, importujte certifikát certifikační autority, která vydává Certifikát podepsaný CA používaný jako certifikát serveru. Zadejte soubor, který potřebujete.
Certifikát CA 2	Pokud je formát vašeho certifikátu **Certifikát (PEM/DER)**, importujte certifikát certifikační autority, která vydává Certifikát CA 1. Zadejte soubor, který potřebujete.

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. Otevřete aplikaci Web Config a poté vyberte kartu **Zabezpečení sítě**. Dále vyberte položku **SSL/TLS** > **Certifikát** nebo **Filtrování IPsec/IP** > **Certifikát klienta** nebo **IEEE802.1X** > **Certifikát klienta**.

2. Klikněte na tlačítko **Odstranit**.

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

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Aktualizování samopodpisovatelného certifikátu

Certifikát Certifikát podepsaný sebou samým je vydáván skenerem, takže jej můžete aktualizovat, pokud vyprší jeho platnost nebo se změní popisovaný obsah.

1. Otevřete aplikaci Web Config a vyberte kartu **Zabezpečení sítě** tab > **SSL/TLS** > **Certifikát**.
2. Klikněte na možnost **Aktualizovat**.
3. Zadejte informace do pole **Obecné jméno**.

   Můžete zadat 1 až 5 adres IPv4, adres IPv6, názvů hostitele a položek FQDN v rozsahu 1 až 128 znaků. Při zadávání je nutné oddělit položky čárkami. První parametr je uložen do obecného názvu, ostatní elementy jsou uloženy do pole alias v předmětu certifikátu.

   Příklad:

   IP adresa skeneru: 192.0.2.123, Název skeneru: EPSONA1B2C3

   Obecný název: EPSONA1B2C3,EPSONA1B2C3.local,192.0.2.123
4. Určete interval platnosti certifikátu.
5. Klikněte na možnost **Další**.

   Zobrazí se zpráva s potvrzením.
6. Klikněte na možnost **OK**.

   Skener je aktualizován.

Poznámka:
*Informace certifikátu můžete zkontrolovat na kartě **Zabezpečení sítě** > **SSL/TLS** > **Certifikát** > **Certifikát podepsaný sebou samým** a klikněte na **Potvrdit**.*

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Konfigurace Certifikát CA

Když nastavíte Certifikát CA, můžete ověřit cestu k certifikátu CA serveru, na který skener přistupuje. Tím lze zabránit krádeži identity.

Certifikát CA můžete získat od certifikační autority v případě, že byl Certifikát podepsaný CA vydán.

Importování Certifikát CA

Importuje certifikát Certifikát CA do skeneru.

1. Otevřete nástroj Web Config a poté vyberte kartu **Zabezpečení sítě** > **Certifikát CA**.
2. Klikněte na položku **Importovat**.
3. Určete Certifikát CA, který chcete importovat.
4. Klikněte na položku **OK**.

Po dokončení importu se vrátíte na obrazovku **Certifikát CA** a zobrazí se importovaný Certifikát CA.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Odstranění Certifikát CA

Importovaný certifikát Certifikát CA můžete odstranit.

1. Otevřete nástroj Web Config a pak vyberte kartu **Zabezpečení sítě** > **Certifikát CA**.
2. Klilkněte na tlačítko **Odstranit** vedle certifikátu Certifikát CA, který chcete odstranit.
3. Potvrďte, že chcete odstranit certifikát v zobrazené zprávě.
4. Klikněte na tlačítko **Restartovat síť** a pak zkontrolujte, zda není odstraněný certifikát CA uveden na aktualizované obrazovce.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

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.

Konfigurace základních nastavení SSL/TLS

Pokud skener podporuje funkci serveru HTTPS, můžete použít komunikaci SSL/TLS k zašifrování komunikací. Skener můžete nakonfigurovat a spravovat pomocí nástroje Web Config a zajistit tak zabezpečení.

Nakonfigurujte sílu šifrování a funkci přesměrování.

1. Otevřete nástroj Web Config a vyberte kartu **Zabezpečení sítě** > **SSL/TLS** > **Základní**.

2. Vyberte hodnotu pro každou položku.
   - ❏ Síla šifrování
     Vyberte sílu úrovně šifrování.
   - ❏ Přesměrovat protokol HTTP na HTTPS
     Přesměrujte na HTTPS při přístupu HTTP.
3. Klikněte na možnost **Další**.
   Zobrazí se potvrzovací zpráva.
4. Klikněte na možnost **OK**.
   Skener byl aktualizován.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Konfigurování certifikátu serveru pro skener

1. Otevřete nástroj Web Config a vyberte kartu **Zabezpečení sítě** > **SSL/TLS** > **Certifikát**.
2. Zadejte certifikát, který chcete použít s **Certifikát serveru**.
   - ❏ Certifikát podepsaný sebou samým
     Skener vytvořil samopodpisovatelný certifikát. Pokud nezískáte certifikát podepsaný CA, vyberte tuto možnost.
   - ❏ Certifikát podepsaný CA
     Pokud předem získáte a importujete certifikát podepsaný CA, můžete tuto možnost určit.
3. Klikněte na položku **Další**.
   Zobrazí se potvrzovací zpráva.
4. Klikněte na položku **OK**.
   Skener byl aktualizován.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35
➡ „Konfigurace Certifikát podepsaný CA“ na str. 98
➡ „Konfigurace Certifikát CA“ na str. 102

Šifrovaná komunikace pomocí filtrování IPsec/IP

O aplikaci Filtrování IPsec/IP

Můžete filtrovat provoz na základě adres IP, služeb a portu pomocí funkce filtrování IPsec/IP.Zkombinováním filtrování můžete nakonfigurovat skener tak, aby akceptoval nebo blokoval specifikované klienty a data.Kromě toho můžete zvýšit úroveň zabezpečení použitím IPsec.

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

Konfigurace výchozích zásad

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.

1. Otevřete aplikaci Web Config a poté vyberte kartu **Zabezpečení sítě** > **Filtrování IPsec/IP** > **Základní**.
2. Do všech polí zadejte hodnotu.
3. Klikněte na možnost **Další**.

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

   Skener je aktualizován.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Položky nastavení Výchozí zásada

Výchozí zásada

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

❏ **Řízení přístupu**

Nakonfigurujte metodu řízení pro provoz paketů IP.

Položky	Nastavení a vysvětlení
Povolit přístup	Výběrem této volby povolíte průchod nakonfigurovaným paketům IP.
Odmítnout přístup	Výběrem této volby odmítnete průchod nakonfigurovaným paketům IP.
IPsec	Výběrem této volby povolíte průchod nakonfigurovaným paketům IPsec.

❏ **Verze IKE**

Vyberte **IKEv1** nebo **IKEv2** pro **Verze IKE**. Vyberte jednu z možností dle typu zařízení, ke kterému je skener připojen.

❏ IKEv1

Následující položky se zobrazí, pokud nastavíte položku **Verze IKE** na hodnotu **IKEv1**.

Položky	Nastavení a vysvětlení
Způsob ověření	Aby bylo možné vybrat volbu **Certifikát**, je třeba předem získat a naimportovat certifikát podepsaný certifikační autoritou.
Předsdílený klíč	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, zadejte předsdílený klíč o délce 1 až 127 znaků.
Potvrzení předsdíleného klíče	Zadejte klíč nakonfigurovaný pro potvrzení.

❏ IKEv2

Následující položky se zobrazí, pokud nastavíte položku **Verze IKE** na hodnotu **IKEv2**.

Položky		Nastavení a vysvětlení
Místní	Způsob ověření	Aby bylo možné vybrat volbu **Certifikát**, je třeba předem získat a naimportovat certifikát podepsaný certifikační autoritou.
	ID Typ	Pokud vyberete hodnotu **Předsdílený klíč** pro položku **Způsob ověření**, vyberte typ ID skeneru.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Rozlišující název**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „=“. **IP adresa**: 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 (.). **E-mailová adresa**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „@“. **ID klíče**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E).
	Předsdílený klíč	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Potvrzení předsdíleného klíče	Zadejte klíč nakonfigurovaný pro potvrzení.

Položky		Nastavení a vysvětlení
Vzdálené	Způsob ověření	Aby bylo možné vybrat volbu **Certifikát**, je třeba předem získat a naimportovat certifikát podepsaný certifikační autoritou.
	ID Typ	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, vyberte typ ID zařízení, které chcete ověřit.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Rozlišující název**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „=“. **IP adresa**: 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 (.). **E-mailová adresa**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „@“. **ID klíče**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E).
	Předsdílený klíč	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Potvrzení předsdíleného klíče	Zadejte klíč nakonfigurovaný pro potvrzení.

❏ Zapouzdření

Vyberete-li volbu **IPsec** pro položku **Řízení přístupu**, je třeba nakonfigurovat režim zapouzdření.

Položky	Nastavení a vysvětlení
Transportní režim	Vyberte tuto volbu, používáte-li skener ve stejné místní síti LAN. Pakety IP vrstvy 4 nebo pozdější jsou šifrovány.
Tunelový režim	Pokud skener používáte v síti s přístupem k Internetu jako IPsec-VPN, vyberte tuto možnost. Záhlaví a data paketů IP jsou šifrována. **Vzdálená brána(Tunelový režim)**: pokud vyberete **Tunelový režim** pro **Zapouzdření**, zadejte adresu brány o délce 1 až 39 znaků.

❏ Protokol zabezpečení

Pokud nastavíte možnost **Řízení přístupu** na hodnotu **IPsec**, vyberte některou volbu.

Položky	Nastavení a vysvětlení
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.

❏ **Nastavení algoritmu**

Doporučuje se zvolit **Libovolné** pro veškerá nastavení a pak zvolit položku jinou než **Libovolné** pro každé nastavení. Pokud pro některé nastavení vyberete hodnotu **Libovolné** a u jiných nastavení vyberete jinou hodnotu než **Libovolné**, zařízení nemusí v závislosti na jiném zařízení, které chcete ověřit, komunikovat.

Položky		Nastavení a vysvětlení
IKE	Šifrování	Vyberte algoritmus šifrování pro IKE. Položky se mohou lišit v závislosti na verzi IKE.
	Ověření	Vyberte algoritmus ověřování pro IKE.
	Výměna klíčů	Vyberte algoritmus výměny klíčů pro IKE. Položky se mohou lišit v závislosti na verzi IKE.
ESP	Šifrování	Vyberte algoritmus šifrování pro ESP. Funkce je dostupná, když je v části **Protokol zabezpečení** vybrána možnost **ESP**.
	Ověření	Vyberte algoritmus ověřování pro ESP. Funkce je dostupná, když je v části **Protokol zabezpečení** vybrána možnost **ESP**.
AH	Ověření	Vyberte algoritmus šifrování pro AH. Funkce je dostupná, když je v části **Protokol zabezpečení** vybrána možnost **AH**.

Konfigurace zásad 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.

1. Otevřete aplikaci Web Config a poté vyberte kartu **Zabezpečení sítě** > **Filtrování IPsec/IP** > **Základní**.
2. Klikněte na číslovanou kartu, kterou chcete nakonfigurovat.
3. Do všech polí zadejte hodnotu.
4. Klikněte na možnost **Další**.

   Zobrazí se zpráva s potvrzením.
5. Klikněte na možnost **OK**.

   Skener je aktualizován.

Položky nastavení Skupinová zásada

Položky	Nastavení a vysvětlení
Povolit tuto skupinovou zásadu	Můžete povolit nebo zakázat zásadu skupiny.

Řízení přístupu

Nakonfigurujte metodu řízení pro provoz paketů IP.

Položky	Nastavení a vysvětlení
Povolit přístup	Výběrem této volby povolíte průchod nakonfigurovaným paketům IP.
Odmítnout přístup	Výběrem této volby odmítnete průchod nakonfigurovaným paketům IP.
IPsec	Výběrem této volby povolíte průchod nakonfigurovaným paketům IPsec.

Místní adresa (skener)

Vyberte adresu IPv4 nebo IPv6, která odpovídá vašemu síťovému prostředí. Pokud je adresa IP přiřazena automaticky, můžete vybrat nastavení **Použít automaticky získanou adresu IPv4**.

Poznámka:
Pokud je adresa IPv6 přiřazena automaticky, připojení nemusí být dostupné. Nakonfigurujte statickou adresu IPv6.

Vzdálená adresa (hostitel)

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.

Metoda výběru portu

Vyberte metodu určení portů.

❏ Název služby

Pokud nastavíte možnost **Metoda výběru portu** na hodnotu **Název služby**, vyberte některou volbu.

❏ Transportní protokol

Vyberete-li volbu **Číslo portu** pro položku **Metoda výběru portu**, je třeba nakonfigurovat režim zapouzdření.

Položky	Nastavení a vysvětlení
Jakýkoli protokol	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.

❏ Místní port

Vyberete-li volbu **Číslo portu** u položky **Metoda výběru portu** a vyberete-li volbu **TCP** nebo **UDP** u položky **Transportní protokol**, 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.

❏ Vzdálený port

Vyberete-li volbu **Číslo portu** u položky **Metoda výběru portu** a vyberete-li volbu **TCP** nebo **UDP** u položky **Transportní protokol**, 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.

Verze IKE

Vyberte **IKEv1** nebo **IKEv2** pro **Verze IKE**. Vyberte jednu z možností dle typu zařízení, ke kterému je skener připojen.

❏ IKEv1

Následující položky se zobrazí, pokud nastavíte položku **Verze IKE** na hodnotu **IKEv1**.

Položky	Nastavení a vysvětlení
Způsob ověření	Pokud nastavíte možnost **Řízení přístupu** na hodnotu **IPsec**, vyberte některou volbu. Použitý certifikát je společný s výchozí zásadou.
Předsdílený klíč	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, zadejte předsdílený klíč o délce 1 až 127 znaků.
Potvrzení předsdíleného klíče	Zadejte klíč nakonfigurovaný pro potvrzení.

❏ IKEv2

Následující položky se zobrazí, pokud nastavíte položku **Verze IKE** na hodnotu **IKEv2**.

Položky		Nastavení a vysvětlení
Místní	Způsob ověření	Pokud nastavíte možnost **Řízení přístupu** na hodnotu **IPsec**, vyberte některou volbu. Použitý certifikát je společný s výchozí zásadou.
	ID Typ	Pokud vyberete hodnotu **Předsdílený klíč** pro položku **Způsob ověření**, vyberte typ ID skeneru.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Rozlišující název**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „=“. **IP adresa**: 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 (.). **E-mailová adresa**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „@“. **ID klíče**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E).
	Předsdílený klíč	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Potvrzení předsdíleného klíče	Zadejte klíč nakonfigurovaný pro potvrzení.
Vzdálené	Způsob ověření	Pokud nastavíte možnost **Řízení přístupu** na hodnotu **IPsec**, vyberte některou volbu. Použitý certifikát je společný s výchozí zásadou.
	ID Typ	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, vyberte typ ID zařízení, které chcete ověřit.
	ID	Zadejte identifikátor skeneru, který se shoduje s typem ID. Jako první znak nepoužívejte „@“, „#“ a „=“. **Rozlišující název**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „=“. **IP adresa**: 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 (.). **E-mailová adresa**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Zadání musí obsahovat symbol „@“. **ID klíče**: zadejte 1 až 255 1bajtových znaků ve formátu ASCII (0x20 až 0x7E).
	Předsdílený klíč	Pokud nastavíte položku **Způsob ověření** na hodnotu **Předsdílený klíč**, zadejte předsdílený klíč o délce 1 až 127 znaků.
	Potvrzení předsdíleného klíče	Zadejte klíč nakonfigurovaný pro potvrzení.

Zapouzdření

Vyberete-li volbu **IPsec** pro položku **Řízení přístupu**, je třeba nakonfigurovat režim zapouzdření.

Položky	Nastavení a vysvětlení
Transportní režim	Vyberte tuto volbu, používáte-li skener ve stejné místní síti LAN. Pakety IP vrstvy 4 nebo pozdější jsou šifrovány.
Tunelový režim	Pokud skener používáte v síti s přístupem k Internetu jako IPsec-VPN, vyberte tuto možnost. Záhlaví a data paketů IP jsou šifrována. **Vzdálená brána(Tunelový režim)**: pokud vyberete **Tunelový režim** pro **Zapouzdření**, zadejte adresu brány o délce 1 až 39 znaků.

Protokol zabezpečení

Pokud nastavíte možnost **Řízení přístupu** na hodnotu **IPsec**, vyberte některou volbu.

Položky	Nastavení a vysvětlení
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.

Nastavení algoritmu

Doporučuje se zvolit **Libovolné** pro veškerá nastavení a pak zvolit položku jinou než **Libovolné** pro každé nastavení. Pokud pro některé nastavení vyberete hodnotu **Libovolné** a u jiných nastavení vyberete jinou hodnotu než **Libovolné**, zařízení nemusí v závislosti na jiném zařízení, které chcete ověřit, komunikovat.

Položky		Nastavení a vysvětlení
IKE	Šifrování	Vyberte algoritmus šifrování pro IKE. Položky se mohou lišit v závislosti na verzi IKE.
	Ověření	Vyberte algoritmus ověřování pro IKE.
	Výměna klíčů	Vyberte algoritmus výměny klíčů pro IKE. Položky se mohou lišit v závislosti na verzi IKE.
ESP	Šifrování	Vyberte algoritmus šifrování pro ESP. Funkce je dostupná, když je v části **Protokol zabezpečení** vybrána možnost **ESP**.
	Ověření	Vyberte algoritmus ověřování pro ESP. Funkce je dostupná, když je v části **Protokol zabezpečení** vybrána možnost **ESP**.
AH	Ověření	Vyberte algoritmus šifrování pro AH. Funkce je dostupná, když je v části **Protokol zabezpečení** vybrána možnost **AH**.

Kombinace Místní adresa (skener) a Vzdálená adresa (hostitel) v Skupinová zásada

		Nastavení Místní adresa (skener)		
		IPv4	IPv6*2	Jakékoli adresy*3
Nastavení Vzdálená adresa (hostitel)	IPv4*1	✓	–	✓
	IPv6*1, *2	–	✓	✓
	Prázdná	✓	✓	✓

*1 Pokud je zvoleno **IPsec** pro funkci **Řízení přístupu**, nemůžete určit délku předpony.

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

*3 Vyjma místních adres propojení IPv6.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Odkazy na název služby v zásadách skupiny

Poznámka:
Nedostupné služby se zobrazí, ale nelze je vybrat.

Název služby	Typ protokolu	Číslo místního portu	Číslo vzdáleného portu	Ovládané funkce
Libovolné	–	–	–	Všechny služby
ENPC	UDP	3289	Libovolný port	Hledání skeneru z aplikací jako Epson Device Admin a ovladače skeneru
SNMP	UDP	161	Libovolný port	Načítání a konfigurace MIB z aplikací jako Epson Device Admin a ovladače skeneru Epson
WSD	TCP	Libovolný port	5357	Ovládání WSD
WS-Discovery	UDP	3702	Libovolný port	Vyhledávání skenerů WSD
Network Scan	TCP	1865	Libovolný port	Předávání naskenovaných dat z aplikace Document Capture Pro
Network Push Scan	TCP	Libovolný port	2968	Vyžádání informací o úloze pro nabízené skenování z Document Capture Pro
Network Push Scan Discovery	UDP	2968	Libovolný port	Hledání počítače ze skeneru

Název služby	Typ protokolu	Číslo místního portu	Číslo vzdáleného portu	Ovládané funkce
Data FTP (vzdálená)	TCP	Libovolný port	20	Klient FTP (předávání naskenovaných dat) Tímto však můžete ovládat pouze server FTP, který využívá vzdálený port číslo 20.
Ovládání FTP (vzdálené)	TCP	Libovolný port	21	Klient FTP (ovládání předávání naskenovaných dat)
CIFS (vzdálené)	TCP	Libovolný port	445	Klient CIFS (předávání naskenovaných dat do složky)
NetBIOS Name Service (vzdálená)	UDP	Libovolný port	137	Klient CIFS (předávání naskenovaných dat do složky)
NetBIOS Datagram Service (vzdálená)	UDP	Libovolný port	138	
NetBIOS Session Service (vzdálená)	TCP	Libovolný port	139	
HTTP (místní)	TCP	80	Libovolný port	Server HTTP(S) (předávání dat Web Config a WSD)
HTTPS (místní)	TCP	443	Libovolný port	
HTTP (vzdálené)	TCP	Libovolný port	80	Klient HTTP(S) (aktualizace firmwaru a kořenový certifikát)
HTTPS (vzdálené)	TCP	Libovolný port	443	

Příklady konfigurace Filtrování IPsec/IP

Výhradní příjem paketů IPsec

Tento příklad slouží ke výhradně ke konfiguraci výchozích zásad.

Výchozí zásada:

- ❏ **Filtrování IPsec/IP**: **Povolit**
- ❏ **Řízení přístupu**: **IPsec**
- ❏ **Způsob ověření**: **Předsdílený klíč**
- ❏ **Předsdílený klíč**: zadejte až 127 znaků.

Skupinová zásada: neprovádějte konfiguraci.

Příjem údajů o skenování a nastavení skeneru

Tento příklad umožňuje zasílání údajů skenování a konfigurace skeneru z určených služeb.

Výchozí zásada:

- ❏ **Filtrování IPsec/IP**: **Povolit**

❏ **Řízení přístupu**: **Odmítnout přístup**

Skupinová zásada:

❏ **Povolit tuto skupinovou zásadu**: zaškrtněte políčko.

❏ **Řízení přístupu**: **Povolit přístup**

❏ **Vzdálená adresa (hostitel)**: IP adresa klienta

❏ **Metoda výběru portu**: **Název služby**

❏ **Název služby**: zaškrtněte políčko **ENPC**, **SNMP**, **HTTP (místní)**, **HTTPS (místní)** a **Network Scan**.

Získání přístupu pouze z určené IP adresy

Tento příklad ukazuje určenou IP adresu pro přístup ke skeneru.

Výchozí zásada:

❏ **Filtrování IPsec/IP**: **Povolit**

❏ **Řízení přístupu**:**Odmítnout přístup**

Skupinová zásada:

❏ **Povolit tuto skupinovou zásadu**: zaškrtněte políčko.

❏ **Řízení přístupu**: **Povolit přístup**

❏ **Vzdálená adresa (hostitel)**: IP adresa klienta správce

Poznámka:
Bez ohledu na konfiguraci zásad bude klient moci skener používat a konfigurovat.

Konfigurace certifikátu pro IPsec/IP filtrování

Nakonfigurujte certifikát klienta na IPsec/IP filtrování. Když ho nastavíte, budete moci používat certifikát jako metodu ověřování pro IPsec/IP filtrování. Pokud chcete nakonfigurovat certifikační autoritu, přejděte na možnost **Certifikát CA**.

1. Přejděte na Web Config a pak vyberte kartu **Zabezpečení sítě** > **Filtrování IPsec/IP** > **Certifikát klienta**.

2. Importujte certifikát do části **Certifikát klienta**.

   Pokud jste již importovali certifikát publikovaný certifikační autoritou, můžete certifikát zkopírovat a použít ho v IPsec/IP filtrování. Ke zkopírování vyberte certifikát z **Kopírovat z** a pak klikněte na **Kopírovat**.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

➡ „Konfigurace Certifikát podepsaný CA“ na str. 98

➡ „Konfigurace Certifikát CA“ na str. 102

Připojení skeneru k síti IEEE802.1X

Konfigurování sítě IEEE802.1X

Pokud nastavíte IEEE802.1X na skeneru, můžete jej použít na síti připojené k serveru RADIUS, přepínači sítě LAN s funkcí ověření, nebo na přístupovém bodu.

1. Otevřete aplikaci Web Config a poté vyberte kartu **Zabezpečení sítě** > **IEEE802.1X** > **Základní**.

2. Do všech polí zadejte hodnotu.

   Pokud chcete používat skener na síti Wi-Fi, klepněte na možnost **Nastavení Wi-Fi** a vyberte nebo zadejte SSID.

   Poznámka:
   Nastavení můžete sdílet mezi sítí Ethernet a Wi-Fi.

3. Klikněte na možnost **Další**.

   Zobrazí se zpráva s potvrzením.

4. Klikněte na možnost **OK**.

   Skener je aktualizován.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Položky nastavení sítě IEEE 802.1X

Položky	Nastavení a vysvětlení	
IEEE802.1X (drátová LAN)	Můžete povolit nebo zakázat nastavení na stránce (**IEEE802.1X** > **Základní**) pro IEEE802.1X (drátová místní síť LAN).	
IEEE802.1X (Wi-Fi)	Zobrazí se stav připojení IEEE802.1X (Wi-Fi).	
Způsob připojení	Zobrazí se metoda připojení aktuální sítě.	
Typ EAP	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.
	EAP-TTLS	
ID uživatele	Nakonfigurujte ID, které bude použito jako ověření na serveru RADIUS. Zadejte 1 až 128 1bajtových znaků ve formátu ASCII (0x20 až 0x7E).	
Heslo	Nakonfigurujte heslo pro ověření skeneru. Zadejte 1 až 128 1bajtových znaků ve formátu ASCII (0x20 až 0x7E). Používáte-li server Windows jako server RADIUS, můžete zadat až 127 znaků.	

Položky	Nastavení a vysvětlení	
Potvrzení hesla	Pro potvrzení zadejte nakonfigurované heslo.	
ID serveru	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 ve formátu ASCII (0x20 až 0x7E).	
Ověření certifikátu	Můžete nastavit ověření certifikátu bez ohledu na metodu ověření. Importujte certifikát do části **Certifikát CA**.	
Anonymní jméno	Pokud vyberete **PEAP-TLS** nebo **PEAP/MSCHAPv2** pro **Typ EAP**, můžete nakonfigurovat anonymní jméno místo ID uživatele pro fázi 1 ověření PEAP. Zadejte 0 až 128 1bajtových znaků ve formátu ASCII (0x20 až 0x7E).	
Síla šifrování	K dispozici je výběr z následujících možností.	
	Vysoký	AES256/3DES
	Střední	AES256/3DES/AES128/RC4

Konfigurace certifikátu pro IEEE 802.1X

Nakonfigurujte certifikát klienta pro IEEE802.1X. Když ho nastavíte, můžete použít **EAP-TLS** a **PEAP-TLS** jako metodu ověřování IEEE 802.1X. Pokud chcete nakonfigurovat certifikační autoritu certifikátu, přejděte na možnost **Certifikát CA**.

1. Přejděte na Web Config a pak vyberte kartu **Zabezpečení sítě** > **IEEE802.1X** > **Certifikát klienta**.
2. Zadejte certifikát v **Certifikát klienta**.

   Pokud jste již importovali certifikát publikovaný certifikační autoritou, můžete certifikát zkopírovat a použít ho v IEEE802.1X. Ke zkopírování vyberte certifikát z **Kopírovat z** a pak klikněte na **Kopírovat**.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Řešení problémů v rámci rozšířeného zabezpečení

Obnovení nastavení zabezpečení

Pokud vytvoříte vysoce zabezpečené prostředí, jako je například filtrování IPsec/IP, 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.

Zakázaní funkce ochrany pomocí nástroje Web Config

Funkci Filtrování IPsec/IP lze zakázat pomocí nástroje Web Config.

1. Otevřete nástroj Web Config a vyberte kartu **Zabezpečení sítě** > **Filtrování IPsec/IP** > **Základní**.
2. Zakažte možnost **Filtrování IPsec/IP**.

Problémy při používání funkcí zabezpečení sítě

Zapomenutí předsdíleného klíče

Znovu nakonfigurujte předsdílený klíč.

Chcete-li změnit klíč, otevřete aplikaci Web Config a vyberte kartu **Zabezpečení sítě** > **Filtrování IPsec/IP** > **Základní** > **Výchozí zásada** nebo možnost **Skupinová zásada**.

Po změně předsdíleného klíče jej nakonfigurujte pro počítače.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35
➡ „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 105

Nelze komunikovat prostřednictvím IPsec

Určete algoritmus, který skener nebo počítač nepodporuje.

Skener podporuje následující algoritmy. Zkontrolujte nastavení počítače.

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	DH Group1, DH Group2, DH Group5, DH Group14, DH Group15, DH Group16, DH Group17, DH Group18, DH Group19, DH Group20, DH Group21, DH Group22, DH Group23, DH Group24, DH Group25, DH Group26, DH Group27*, DH Group28*, DH Group29*, DH Group30*
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. 105

Nelze náhle komunikovat

Adresa IP skeneru byla změněna nebo ji nelze použít.

Pokud adresa IP, registrovaná na místní adrese na Skupinová zásada, byla změněna, nebo ji nelze použít, nebude možné provozovat komunikaci IPsec. 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 (karta **Zabezpečení sítě** > **Filtrování IPsec/IP** > **Základní** > **Skupinová zásada** > **Místní adresa (skener)**) skeneru pravděpodobně nebude možné najít.

Použijte statickou adresu IP.

Adresa IP počítače byla změněna nebo ji nelze použít.

Pokud adresa IP, registrovaná na vzdálené adrese na Skupinová zásada, byla změněna, nebo ji nelze použít, nebude možné provozovat komunikaci IPsec.

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 (karta **Zabezpečení sítě** > **Filtrování IPsec/IP** > **Základní** > **Skupinová zásada** > **Vzdálená adresa (hostitel)**) skeneru pravděpodobně nebude možné najít.

Použijte statickou adresu IP.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35
➡ „Šifrovaná komunikace pomocí filtrování IPsec/IP“ na str. 105

Po nakonfigurování filtrování IPsec/IP se nelze připojit

Nastavení filtrování IPsec/IP nejsou 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. 105

Po nakonfigurování IEEE 802.1X nelze přistupovat na skener

Nastavení IEEE 802.1X nejsou správná.

Na ovládacím panelu skeneru zakažte protokol IEEE 802.1X a připojení Wi-Fi. Připojte skener k počítači a poté znovu nakonfigurujte protokol IEEE 802.1X.

Připojte skener k počítači a poté znovu nakonfigurujte protokol IEEE 802.1X.

Související informace

➡ „Konfigurování sítě IEEE802.1X“ na str. 116

Problémy při používání digitálního certifikátu

Nelze importovat certifikát Certifikát podepsaný CA

Certifikát podepsaný CA a informace na CSR se neshodují.

Pokud certifikát Certifikát podepsaný CA 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.

Certifikát podepsaný CA je větší než 5KB.

Nelze importovat certifikát Certifikát podepsaný CA, který je větší než 5 kB.

Heslo pro importování certifikátu je nesprávné.

Zadejte správné heslo.Pokud heslo zapomenete, nelze certifikát importovat.Znovu získejte certifikát Certifikát podepsaný CA.

Související informace

➡ „Import certifikátu podepsaného certifikační autoritou“ na str. 100

Nelze aktualizovat samopodpisovatelný certifikát

Nebyla zadána položka Obecné jméno.

Obecné jméno musí být zadán.

Do polí Obecné jméno byly zadány nepodporované znaky.

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

Obecný název obsahuje čárku nebo mezeru.

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

Související informace

➡ „Aktualizování samopodpisovatelného certifikátu“ na str. 102

Nelze vytvořit CSR

Nebyla zadána položka Obecné jméno.

Obecné jméno musí být zadán.

Do polí Obecné jméno, Organizace, Organizační jednotka, Lokalita a Stát/kraj byly zadány nepodporované znaky.

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

Obecné jméno obsahuje čárku nebo mezeru.

Pokud je zadána čárka, **Obecné jméno** 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. 98

Zobrazilo se varování ohledně digitálního certifikátu

Zprávy	Příčina/Postup
Zadejte certifikát serveru.	**Příčina:** Nevybrali jste žádný soubor k importování. **Postup:** Vyberte soubor a klepněte na tlačítko **Importovat**.
Certifikát CA 1 není zadán.	**Příčina:** Certifikát CA 1 není zadán a je zadáno pouze certifikát CA 2. **Postup:** Nejdříve naimportujte certifikát CA 1.
Neplatná hodnota níže.	**Příčina:** Umístění souboru a/nebo heslo obsahuje nepodporované znaky. **Postup:** Zkontrolujte, zda jsou znaky pro položku zadány správně.
Neplatné datum a čas.	**Příčina:** Nebylo nastaveno datum a čas pro skener. **Postup:** Nastavte datum a čas pomocí aplikace Web Config nebo EpsonNet Config.
Neplatné heslo.	**Příčina:** Heslo nastavené pro certifikát CA a zadané heslo se neshodují. **Postup:** Zadejte správné heslo.

Zprávy	Příčina/Postup
Neplatný soubor.	**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.
Nelze použít certifikáty serveru, které obsahují více než tři certifikáty CA.	**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.
Platnost certifikátu vypršela. Zkontrolujte, zda je certifikát platný, nebo zkontrolujte datum a čas v produktu.	**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.
Je vyžadován soukromý klíč.	**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
Nastavení se nezdařilo.	**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

➡ „Informace o digitální certifikaci“ na str. 98

Certifikát podepsaný certifikační agenturou byl omylem odstraněn

Pro certifikát podepsaný certifikační agenturou není k dispozici záloha.

Máte-li záložní soubor, znovu naimportujte certifikát.

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

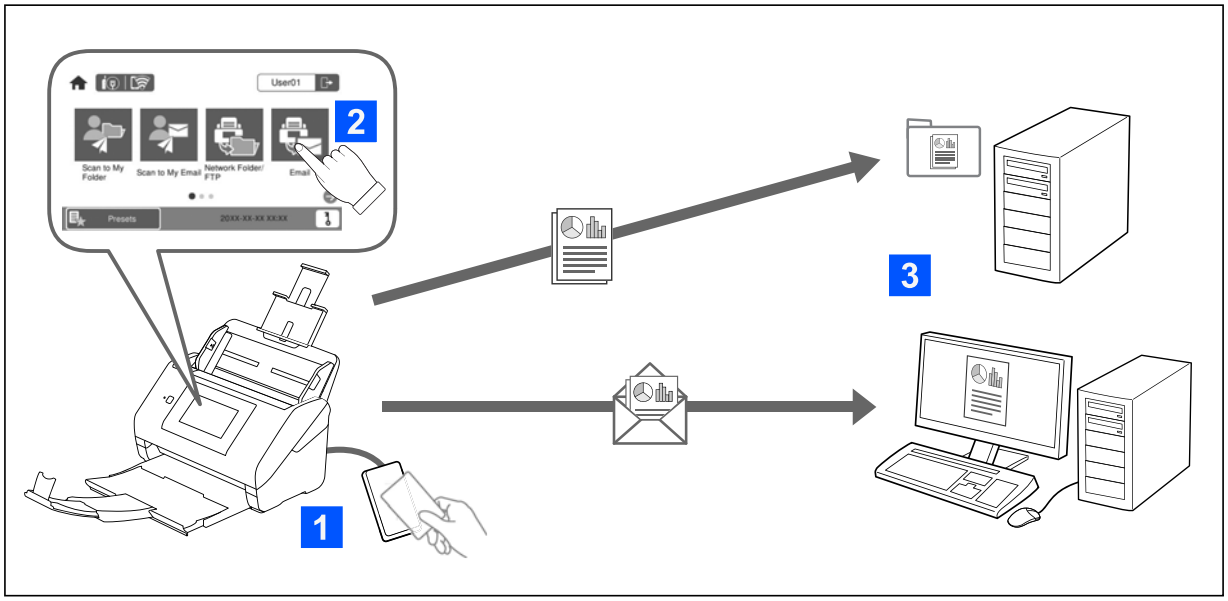
Související informace

➡ „Import certifikátu podepsaného certifikační autoritou“ na str. 100

➡ „Odstranění certifikátu podepsaného certifikační agenturou“ na str. 101

Nastavení ověření

O Nastavení ověření



Po povolení možnosti Nastavení ověření je ověřování uživatele nutné k zahájení skenování. Můžete nastavit metody skenování, které mohou být používány jednotlivými uživateli a zabránit tak náhodným činnostem.

Můžete určit e-mailovou adresu ověřeného uživatele jako cílové umístění skenů (Skenovat do e-mailu) nebo uložit údaje jednotlivých uživatelů do osobní složky (Skenovat do mé složky). Můžete také určit další metody skenování.

Poznámka:

❏ *Při povolení možnosti Nastavení ověření není možné skenovat z počítače nebo chytrého zařízení.*

❏ *Navíc k Nastavení ověření uvedenému v této příručce můžete také vytvořit systém ověřování pomocí serveru ověřování. Pro nastavení systému, použijte aplikaci Document Capture Pro Server Authentication Edition (zkráceným jménem Document Capture Pro Server AE). Pro více informací kontaktujte svou místní pobočku společnosti Epson.*

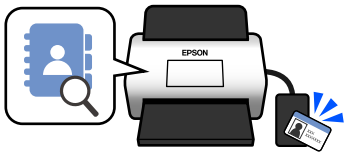
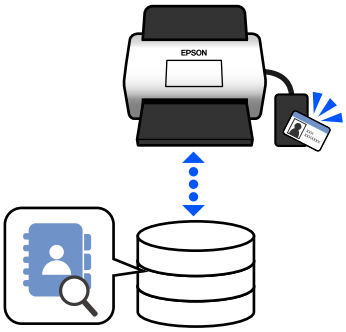
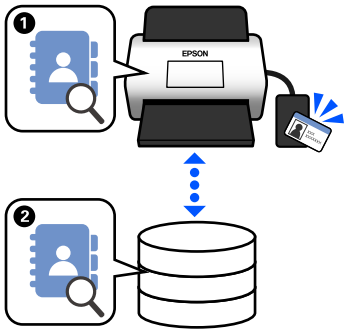
Dostupné funkce pro Nastavení ověření

Funkce skenování na ovládacím panelu	Nastavení ověření	
	Při povolení	Při zákazu
Skenovat do mé složky Uloží snímky do složky přiřazené ověřenému uživateli.	✓	-
Skenovat do e-mailu Odešle snímky na e-mailovou adresu ověřeného uživatele.	✓	-
Sken. do síť. sl./FTP Uloží snímky do složky na síti.	✓	✓
Skenovat do počítače Uloží snímky do připojeného počítače pomocí úloh vytvořených v nástroji Document Capture Pro (Windows)/Document Capture (Mac OS). * Pokud je možnost Nastavení ověření povolena, můžete používat výhradně úlohy registrované v **Předvolby**.	✓*	✓

Funkce skenování na ovládacím panelu	Nastavení ověření	
	Při povolení	**Při zákazu**
Skenovat do e-mailu Odešle snímky na nastavenou e-mailovou adresu.	✓	✓
Skenovat do cloudu Odešle snímky do nastavené cloudové služby.	✓	✓
Skenovat na USB disk Uloží snímky na USB disk připojený ke skeneru. Tato možnost je přístupná, pouze když ke skeneru není připojeno žádné ověřovací zařízení.	✓	✓
Skenovat do WSD Uloží snímky do připojeného počítače pomocí funkce WSD.	-	✓
Předvolby Můžete zaregistrovat až 48 předvoleb funkcí skenování. Můžete přidělit až pět Předvolby uživatelům registrovaným v Místní DB. Přidělené Předvolby jsou dostupné pouze danému uživateli. Předvolby, které nebyly přiděleny žádnému uživateli, mohou využívat všichni uživatelé.	✓	✓

O Způsob ověření

Tento skener dokáže zajistit ověření pomocí následujících metod bez nutnosti sestavit server pro ověřování.

	Místní DB	LDAP	Místní DB a LDAP
Umístění informací o uživateli	**Paměť skeneru** Tato metoda ověřování kontroluje informace o uživateli registrované do skeneru a porovnává je s uživatelem, který využívá funkci skenování.	**Server LDAP*** Tato metoda ověřování kontroluje informace o uživateli serveru LDAP synchronizované se skenerem. Jelikož lze do mezipaměti skeneru dočasně uložit až 300 položek informací o uživateli ze serveru LDAP, lze ověřování provést pomocí mezipaměti, pokud server LDAP nereaguje. * Server, který poskytuje adresářovou službu a dokáže komunikovat s LDAP.	**Paměť skeneru a server LDAP** Nejprve zkontrolujte informace o uživateli registrované ve skeneru (❶) a pokud se neshodují, zkontrolujte informace o uživateli proti serveru LDAP (❷).
			
Počet registrovaných uživatelů	50 (paměť skeneru)	Neomezené (server LDAP)	50 (paměť skeneru) Neomezené (server LDAP)
Vyrovnávací paměť skeneru	-	300	Max. 300 (50 z pozic mezipaměti je sdíleno s Nastavení uživatele v Místní DB)
Metody přihlašování	Můžete používat libovolnou z následujících metod. ❏ Podržení karty ověřování nebo zadání **ID uživatele** a **Heslo** ❏ Podržení karty ověřování nebo zadání **Číslo identity** ❏ Zadejte hodnoty do polí **ID uživatele** a **Heslo** ❏ Zadejte **ID uživatele** ❏ Zadejte **Číslo identity**		
Limity funkce „Skenovat do“	Individuální nastavení pro každého uživatele	Stejné nastavení pro všechny uživatele LDAP	Uživatelé Místní DB: individuální nastavení Uživatelé LDAP: stejné nastavení pro všechny uživatele
Přidělení Předvolby uživatelům	Až 5 na uživatele	- (Nelze nastavit individuálně)	Uživatelé Místní DB: až 5 na uživatele Uživatelé LDAP: -

Software pro nastavení

Nastavení pomocí nástroje Web Config nebo Epson Device Admin.

❏ Když použijete funkci Web Config, můžete nastavit skener pouze pomocí webového prohlížeče.

„Web Config“ na str. 35

❏ Když použijete funkci Epson Device Admin, můžete nastavit více skenerů najednou pomocí šablony konfigurace.

„Epson Device Admin“ na str. 36

Aktualizace firmwaru skeneru

Před povolením Nastavení ověření aktualizujte firmware skeneru na poslední verzi. Připojte skener předem k internetu.

> ***Důležité:***
> *Během aktualizace nevypínejte počítač ani skener.*

Při nastavení z nástroje Web Config:

Vyberte kartu **Správa zařízení** > **Aktualizace firmwaru** a pak aktualizujte firmware podle pokynů na obrazovce.

Při nastavení z nástroje Epson Device Admin:

Vyberte **Home** > **Firmware** > **Update** na obrazovce seznamu zařízení a pak se při aktualizaci firmwaru řiďte pokyny na obrazovce.

Poznámka:
Pokud je poslední firmware již nainstalován, aktualizaci nepotřebujete.

Připojování a konfigurace zařízení pro ověřování

Pokud chcete připojit a používat zařízení pro ověřování jako čtečku karet IC, musíte nejprve nakonfigurovat zařízení. To není nutné, pokud nepoužíváte zařízení pro ověřování.

Související informace

➡ „Připojování zařízení pro ověřování“ na str. 131

➡ „Nastavení zařízení pro ověřování“ na str. 132

Seznam kompatibilních čteček karet

Tento seznam nezaručuje činnost čteček karet v seznamu.

Ano: podporováno (informace ID lze načíst pomocí běžného nastavení čtečky karet.)

Ne: není kompatibilní

Výrobce	Model	Číslo modelu	Ověřovací karta							Režim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
RF IDEAS	pcProx Plus	RDR-80081AKU	Ano	Ano*1	Ano*1	Ano*1	Ne	Ne	Ne	Klávesnice
RF IDEAS	pcProx	RDR-7081BKU	Ano*1	Ne	Ano	Ano	Ne	Ne	Ne	Klávesnice
RF IDEAS	pcProx	RDR-7581AKU	Ano	Ne	Ano*1	Ano*1	Ne	Ne	Ne	Klávesnice
ELATEC	TWN3 MIFARE	T3DT-MB2BEL T3DT-MB2WEL	Ne	Ne	Ano	Ano	Ne	Ne	Ne	Klávesnice
ELATEC	TWN3 MIFARE NFC	T3DT-FB2BEL T3DT-FB2WEL	Ano	Ne	Ano	Ano	Ano	Ano	Ano	Klávesnice
ELATEC	TWN4 MULTI-TECH	T4DT-FB2BEL-PI T4DT-FB2WEL-PI	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Klávesnice
ELATEC	TWN4 Multi-Tech 2 BLE-PI	T4LK-FB4BLZ-PI	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Klávesnice
ELATEC	TWN4 Slim	T4QC-FC3B7	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Klávesnice
HID Global	OMNIKEY 5427	OMNIKEY5427CK OMNIKEY5427CK gen2	Ano	Ano	Ano	Ano	Ano	Ne	Ano	Klávesnice*1
ACS	ACR122U	ACR122U	Ne	Ne	Ano*2	Ano*2	Ano	Ne	Ano*2	PC/SC

Výrobce	Model	Číslo modelu	Ověřovací karta							Režim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/ Lite-S		
ACS	ACR1252	ACR1252	Ne	Ne	Ano*2	Ano*2	Ano	Ano	Ano*2	PC/SC
Sony	PaSoRi	RC-S330/S	Ne	Ne	Ano*2	Ano*2	Ano*2	Ano*2	Ano*2	PaSoRi
Sony	PaSoRi	RC-S380/P RC-S380/S	Ne	Ne	Ano*2	Ano*2	Ano*2	Ano*2	Ano*2	PaSoRi
DMZ	Leitor RFID Universal	DMZ008	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Klávesnice
DMZ	Leitor RFID Multi-125	DMZ087	Ne	Ano	Ne	Ne	Ne	Ne	Ne	Klávesnice
DMZ	Leitor RFID Mifare	DMZ088	Ne	Ne	Ano	Ano	Ne	Ne	Ne	Klávesnice
DMZ	Biometric & RFID Reader	DMZ073	Ne	Ano	Ne	Ne	Ne	Ne	Ne	Klávesnice
inepro	SCR708	SCR708	Ano*1	Ano*1	Ano*1	Ano*1	Ano*1	Ano*1	Ano*1	Klávesnice
Y Soft	YU030888 001	MU0388	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Klávesnice
Cartadis	TCM3 Cartadis MiFare Card Reader	ZTCM3-MIFARE	Ne	Ne	Ano	Ano	Ne	Ne	Ano	Klávesnice
MICI Network Co., Ltd.	EM & Mifare Card Reader	mCR-600	Ne	Ne	Ano	Ano	Ne	Ne	Ano	Klávesnice

Výrobce	Model	Číslo modelu	Ověřovací karta							Režim
			HID Global	DMZ	MIFARE		FeliCa™		IEC/ISO14443 (TypeB) Compliance	
			iClass	EM4002	Classic	Ultralight	Standard	Lite/Lite-S		
NT-ware	MiCard Multi-Tech4-PI	T4DT-FB4WUF-PI	Ano	Ano	Ano	Ano	Ano	Ano	Ano	Klávesnice
NT-ware	MiCard Plus-2-V2	RDR-80081AGU-NT2-20	Ano*1	Ano*1	Ano*1	Ano*1	Ne	Ne	Ne	Klávesnice
NT-ware	MiCard V3 Multi	MiCard V3 Multi	Ano	Ano	Ano	Ano	Ano	Ano	Ne	Klávesnice

*1 Musíte změnit nastavení čtečky karet pomocí příslušného softwaru poskytovaného výrobcem čtečky karet.

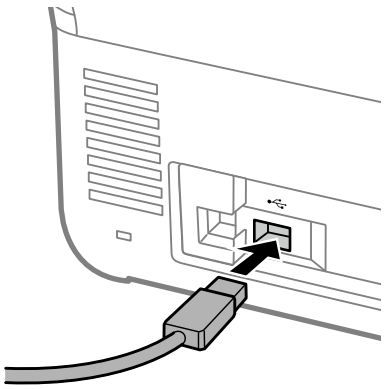
*2 Pokud potřebujete používat údaje v konkrétní oblasti na kartě lišící se od standardního ID karty jako ověřovací ID prostřednictvím konfigurace nastavení produktu, obraťte se na svého partnera Epson nebo místního zástupce ohledně dalších informací týkajících se postupu nastavení produktu.

Připojování zařízení pro ověřování

Důležité:

Když připojíte zařízení pro ověřování k více skenerům, použijte produkt se stejným číslem modelu.

Připojte USB kabel čtečky karet k externímu rozhraní USB portu na skeneru.



Kontrola funkce pro zařízení ověřování

Stav připojení a rozpoznávání ověřovací karty pro ověřovací zařízení můžete zkontrolovat na ovládacím panelu skeneru.

Informace se zobrazí, pokud vyberete možnost **Nast.** > **Informace o zařízení** > **Stav ověřovacího zařízení**.

Nastavení zařízení pro ověřování

Nastavte formát čtení pro ověřování informací přijatých z karty ověřování.

V zařízení pro ověřování můžete nastavit následující metodu čtení.

❏ Načítání konkrétní oblasti karty ověřování, například číslo zaměstnance nebo osobní ID.

❏ Použití informací karty ověřování s výjimkou UID (informace karty ověřování, například sériové číslo.)
Nástroj můžete použít k vygenerování provozních parametrů. O podrobnosti požádejte svého prodejce.

Poznámka:
Používání ověřovacích karet od různých výrobců:

Při používání UID údajů karty (údaje o ID karty, například sériové číslo) můžete použít kombinaci různých typů ověřovacích karet. Tyto údaje nelze kombinovat při používání údajů jiných karet.

Při nastavení z nástroje Web Config:

Vyberte kartu **Správa zařízení** > **Čtečka karet**.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Administrator Settings** > **Authentication Settings** > **Card Reader** ze šablony konfigurace.

Položka	Vysvětlení
Vendor ID	Nastavte ID dodavatele zařízení pro ověřování, které omezuje použití z 0000 na FFFF pomocí 4 alfanumerických znaků. Pokud nechcete provést omezení, nastavte hodnotu na 0000.
Product ID	Nastavte ID produktu zařízení pro ověřování, které omezuje použití z 0000 na FFFF pomocí 4 alfanumerických znaků. Pokud nechcete provést omezení, nastavte hodnotu na 0000.
Provozní parametr	Nastavte provozní parametr zařízení pro ověřování na hodnotu od 0 do 8192 znaků. Dostupné jsou znaky A–Z, a–z, 0–9, +, /, =, mezera a zalomení řádku.
Čtečka karet	Vyberte formát převodu pro zařízení pro ověřování. Můžete zkontrolovat podrobnosti formátu. Viz odkaz uvedený v popisu položky.
Formát uložení ověřovací identifikační karty	Vyberte formát převodu pro údaje ověřování průkazu. Můžete zkontrolovat podrobnosti formátu. Viz odkaz uvedený v popisu položky.
Nastavit ID rozsah karty	Povolte určení polohy čtení.
Výchozí poloha textu	Zadejte počáteční polohu textu ke čtení údajů ID. Můžete určit hodnotu od 1 do 4096.
Počet znaků	Zadejte počet znaků, které budou načteny z počáteční polohy údajů ID. Můžete určit hodnotu od 1 do 4096.

Registrace a nastavení informací

Nastavení

Potřebná nastavení proveďte v závislosti na Způsob ověření a používané metodě skenování.

Důležité:

Před zahájením nastavení zkontrolujte, zda máte správně provedeno nastavení času skeneru.

Pokud je nastavení času chybné, zobrazí se chybová zpráva „Platnost licence vypršela“, což může vést k poruše při nastavování skeneru. Za účelem používání funkce zabezpečení, například komunikace SSL/TLS nebo IPsec je třeba nastavit správný čas. Čas můžete nastavit následovně.

❏ *Karta Web Config:* ***Správa zařízení*** > ***Datum a čas*** > ***Datum a čas****.*

❏ *Ovládací panel skeneru:* ***Nast.*** > ***Základní nastavení*** > ***Nastavení datumu / času****.*

Nastavení	Místní DB	LDAP	Místní DB a LDAP
Povolení ověřování Před provedením nastavení ověřování musíte povolit ověřování. „Povolení ověřování“ na str. 134	✓	✓	✓
Nastavení ověření Nastavení Způsob ověření a jak ověřit uživatele. „Nastavení ověření“ na str. 134	✓	✓	✓
Registrování možností Nastavení uživatele Zaregistruje nastavení pro každého uživatele. Uživatele můžete také hromadně registrovat pomocí souboru CSV. „Registrování možností Nastavení uživatele“ na str. 135	✓	–	✓
Synchronizace se Server LDAP Provede nastavení synchronizace serveru LDAP. „Synchronizace se Server LDAP“ na str. 142	–	✓	✓
Nastavení schránky Poštovní server Provede nastavení e-mailového serveru. Tuto možnost nastavte, pokud používáte funkce vyžadující nastavení e-mailového serveru, například Skenovat do e-mailu. „Nastavení e-mailového serveru“ na str. 145	✓	✓	✓
Nastavení režimu Skenovat do mé složky Nastaví složky cílového umístění. Toto nastavení použijte u funkce Skenovat do mé složky. „Nastavení režimu Skenovat do mé složky“ na str. 146	✓	✓	✓

Nastavení	Místní DB	LDAP	Místní DB a LDAP
Přizpůsobit funkce jedním dotykem Tuto možnost nastavte při změně položek zobrazených na ovládacím panelu skeneru. Na ovládacím panelu můžete zobrazit pouze ikony, které potřebujete, nebo změnit jejich pořadí. „Přizpůsobit funkce jedním dotykem“ na str. 148	✓	✓	✓

Povolení ověřování

Před provedením nastavení ověřování musíte povolit ověřování.

Při nastavení z nástroje Web Config:

Vyberte **Zapnuto (zařízení/Server LDAP)** na kartě **Zabezpečení produktu** > **Základní** > **Ověřování**.

Při nastavení z nástroje Epson Device Admin:

Na šabloně konfigurace vyberte **Zapnuto (zařízení/Server LDAP)** v části **Administrator Settings** > **Authentication Settings** > **Basic** > **Authentication**.

Poznámka:
Pokud povolíte možnost Nastavení ověření na skeneru, Nastavení zámku bude také povolena na ovládacím panelu. Ovládací panel nelze odemknout, pokud je povolena možnost Nastavení ověření.

I když možnost Nastavení ověření zakážete, možnost Nastavení zámku zůstane povolena. Pokud ji chcete zakázat, můžete nastavení změnit z ovládacího panelu nebo nástroje Web Config.

Související informace

➡ „Nastavení Nastavení zámku z ovládacího panelu“ na str. 86
➡ „Nastavení Nastavení zámku z nástroje Web Config“ na str. 86

Nastavení ověření

Nastavení Způsob ověření a jak ověřit uživatele.

Při nastavení z nástroje Web Config:

Vyberte kartu **Zabezpečení produktu** > **Nastavení ověření**.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Administrator Settings** > **Authentication Settings** > **Authentication Settings** ze šablony konfigurace.

Položka	Vysvětlení
Způsob ověření	Vyberte možnost Způsob ověření. ❏ Místní DB Ověřte pomocí Nastavení uživatele registrovaného do skeneru. Je nutné registrovat uživatele do skeneru. ❏ LDAP Ověřte pomocí informací o uživateli na serveru LDAP synchronizovaném se skenerem. Nastavení LDAP serveru musíte nakonfigurovat předem. ❏ Místní DB a LDAP Ověřte pomocí informací o uživateli registrovaných do skeneru nebo na serveru LDAP synchronizovaném se skenerem. Musíte uživatele registrovat do skeneru a nastavit server LDAP.
Jak ověřit uživatele	Vyberte, jak chcete uživatele ověřit. ❏ Karta nebo ID uživatele a heslo Použije ověřovací kartu k ověření uživatelů. K ověření také můžete použít ID uživatele a heslo. ❏ ID uživatele a heslo Použije ID uživatele a heslo k ověření uživatelů. Pokud vyberete tuto funkci, nemůžete použít ověřovací kartu k ověřování. ❏ ID uživatele K ověření uživatelů se použije pouze ID uživatele. Nemusíte nastavovat heslo. ❏ Karta nebo číslo identity Použije ověřovací kartu k ověření uživatelů. Můžete také použít Číslo identity. ❏ Číslo identity Použije k ověření uživatelů pouze identifikační číslo.
Povolit uživatelům registraci ověřovacích kart	Povolte, pokud povolíte uživatelům registraci karty pro ověřování do systému. Pokud vyberete možnost **LDAP** pro **Způsob ověření**, nebudete ji moci nastavit. Pro více informací o postupu registrace ověřovacích karet uživatelů si zobrazte položku „Registrace ověřovací karty“ v části *Uživatelská příručka*.
Minimální počet číslic čísla identity	Vyberte minimální počet číslic pro identifikační číslo.
Ukládání do mezipaměti pro uživatele s ověřením LDAP	Při ověřování pomocí serveru LDAP můžete nastavit, zda používat ukládání informací o uživateli do mezipaměti či nikoli.
Použijte uživatelské informace v ověření SMTP	Při ověřování pomocí ID uživatele a hesla můžete nastavit, zda se mají použít informace o uživateli pro ověření SMTP či nikoli. Systém použije poslední přihlášené ID uživatele a heslo.
Omezení pro uživatele s ověřením LDAP	Pokud používáte LDAP, můžete nastavit funkce dostupné uživateli.

Registrování možností Nastavení uživatele

Zaregistrujte si Nastavení uživatele používané pro ověřování uživatele. Registraci můžete provést libovolnou z následujících metod.

❏ Registrace Nastavení uživatele jedno po druhém (Web Config)

❏ Registrace více Nastavení uživatele dávkou pomocí souboru CSV (Web Config)

❏ Registrace User Settings do více skenerů dávkou pomocí šablony konfigurace (Epson Device Admin)

Související informace

➡ „Individuální registrace Nastavení uživatele (Web Config)“ na str. 136

➡ „Registrace více Nastavení uživatele pomocí souboru CSV (Web Config)“ na str. 137

➡ „Registrace User Settings do více skenerů dávkou (Epson Device Admin)“ na str. 140

Individuální registrace Nastavení uživatele (Web Config)

Otevřete Web Config a vyberte kartu **Zabezpečení produktu** > **Nastavení uživatele** > **Přidat** a pak otevřete Nastavení uživatele.

Položka	Vysvětlení
ID uživatele	Zadejte ID uživatele, které chcete použít pro ověřování v rozsahu od 1 do 83 bajtů, které lze vyjádřit v kódu Unicode (UTF-8). Vzhledem k tomu, že ID uživatele nerozlišuje velká a malá písmena, můžete se přihlásit s použitím velkých nebo malých písmen.
Zobrazení uživatelského jména	Zadejte uživatelské jméno zobrazené na ovládacím panelu skeneru o délce maximálně 32 znaků, které lze vyjádřit ve formátu Unicode (UTF-16). Toto pole můžete ponechat prázdné.
Heslo	Zadejte heslo, které chcete použít k ověření, o délce maximálně 32 znaků ve formátu ASCII. Heslo rozeznává velká a malá písmena. Toto pole ponechte prázdné, pokud vyberete možnost **ID uživatele** pro **Jak ověřit uživatele**.
Ověřovací identifikační karta	Zadejte ID ověřovací karty o délce maximálně 116 znaků ve formátu ASCII. Toto pole můžete ponechat prázdné. Když povolíte možnost **Povolit uživatelům registraci ověřovacích kart** pro část **Nastavení ověření**, projeví se výsledek registrovaný uživateli.
Číslo identity	Tato položka se zobrazí, pokud je v nabídce **Karta nebo číslo identity** nebo **Číslo identity** zvolena možnost **Nastavení ověření** > **Jak ověřit uživatele**. Zadejte číslo, které patří někam mezi číslo nastavené v **Nastavení ověření** > **Minimální počet číslic čísla identity** a má až 8 číslic.
Automaticky generovat	Tato položka se zobrazí, pokud je v nabídce **Karta nebo číslo identity** nebo **Číslo identity** zvolena možnost **Nastavení ověření** > **Jak ověřit uživatele**. Kliknutím automaticky vygenerujete číslo ID se stejným počtem číslic, který je zvolen v části **Minimální počet číslic čísla identity**.
Oddělení	Zadejte název oddělení a další údaje, které identifikují uživatele do rozsahu 40 znaků, které lze vyjádřit ve formátu Unicode (UTF-16). Toto pole můžete ponechat prázdné.
E-mailová adresa	Zadejte e-mailovou adresu uživatele o délce maximálně 200 znaků ve formátu ASCII. Tato adresa se používá jako cílové umístění pro **Skenovat do e-mailu**. Toto pole můžete ponechat prázdné.

Položka	Vysvětlení
Skenovat do mé složky	Nastavte individuálně cílové umístění ukládání při výběru **Jednotlivě** v části **Skenovat do mé složky** > **Typ nastavení**. V níže uvedené části najdete další informace o položkách nastavení. „Nastavení režimu Skenovat do mé složky“ na str. 146
Omezení	Můžete omezit funkce jednotlivých uživatelů. Vyberte funkci, u níž povolujete používání.
Předvolby	Z předvoleb zaregistrovaných ve skeneru můžete nakonfigurovat až pět Předvolby, které jsou k dispozici pouze pro vybraného uživatele. ❏ Předvolby, které byly přiděleny uživateli, mohou být používány pouze tímto uživatelem. Předvolby, které nebyly přiděleny žádnému uživateli, mohou využívat všichni uživatelé. ❏ Pokud má uživatel pouze jednu dostupnou Předvolby, bude po ověření automaticky načtena. Pokud je dostupných více Předvolby, zobrazí se po ověření seznam Předvolby. ❏ Nemůžete vytvořit nebo zobrazit Předvolby, které využívají funkce, jež byly omezeny v části **Omezení**.

Registrace více Nastavení uživatele pomocí souboru CSV (Web Config)

Zadejte nastavení pro každého uživatele do souboru CSV a zaregistrujte je dávkou.

Vytvoření souboru CSV

Vytvořte soubor CSV k importu Nastavení uživatele.

Poznámka:
Pokud si předem zaregistrujete jedno nebo více Nastavení uživatele a pak exportujete formátovaný soubor (soubor CSV), můžete využít registrované nastavení jako referenci pro zadání položek nastavení.

1. Otevřete Web Config a vyberte kartu **Zabezpečení produktu** > **Nastavení uživatele**.
2. Klikněte na položku **Exportovat**.
3. Vyberte formát souboru pro **Formát souboru**.

   Vyberte ho odkazem níže.

Položka	Vysvětlení
CSV UTF-16 (oddělený tabulátory)	Vyberte, kdy upravíte soubor pomocí aplikace Microsoft Excel. Každý parametr je uzavřen závorkami „[ ]“. Zadejte parametry do závorek „[ ]“. Když aktualizujete soubor, doporučujeme ho přepsat. Pokud soubor nově uložíte, vyberte test Unicode (*.txt) pro formát souboru.
CSV UTF-8 (oddělený čárkou)	Vyberte, kdy upravíte soubor pomocí textového editoru nebo makra bez aplikace Microsoft Excel.
CSV UTF-8 (oddělený středníkem)	

4. Klikněte na položku **Exportovat**.

5. Upravte a uložte tento soubor CSV do tabulkové aplikace, například Microsoft Excel nebo do textového editoru.

> ***Důležité:***
> *Při úpravách souboru neměňte šifrování a informace o záhlaví.*

Položky nastavení souboru CSV

Položka	Nastavení a vysvětlení
UserID	Zadejte ID uživatele a použijte ověřování mezi 1 a 83 bajty v Unicode.
UserName	Zadejte uživatelské jméno zobrazené na ovládacím panelu skeneru o délce maximálně 32 znaků ve formátu Unicode. Toto pole můžete ponechat prázdné.
Password	Zadejte heslo, které chcete použít k ověření, o délce maximálně 32 znaků ve formátu ASCII. Při importování je toto nastaveno jako heslo místo **EncPassword**. Toto pole ponechte prázdné, pokud vyberete možnost **ID uživatele** pro **Jak ověřit uživatele**. Při exportování je toto pole vždy prázdné.
AuthenticationCardID	Nastavte výsledek čtení ověřovací karty. Když povolíte možnost **Povolit uživatelům registraci ověřovacích kart** v části **Nastavení ověření**, projeví se výsledek registrovaný uživateli. Zadejte maximálně 116 znaků ve formátu ASCII. Toto pole můžete ponechat prázdné.
IDNumber	Tato položka se zobrazí, pokud je v nabídce **Karta nebo číslo identity** nebo **Číslo identity** zvolena možnost **Nastavení ověření** > **Jak ověřit uživatele**. Zadejte číslo, které patří někam mezi číslo nastavené v **Nastavení ověření** > **Minimální počet číslic čísla identity** a má až 8 číslic. Číslo ID nelze duplikovat. Pokud je duplikováno, budete upozorněni na chybu při importování souboru. Ponecháte-li toto pole prázdné, bude mu automaticky přiřazeno číslo.
Department	Zadejte název oddělení k rozlišení uživatelů. Zadejte až 40 znaků v Unicode. Toto pole můžete ponechat prázdné.
MailAddress	Nastavte e-mailovou adresu pro uživatele. Tato adresa se používá jako cílové umístění pro **Skenovat do e-mailu**. Můžete použít A-Z, a-z, 0-9, !#'%&'*+-./=?^_{|}~@. Zadat můžete maximálně 200 znaků. Jako první znak nemůžete použít „,“ (čárku). Toto pole můžete ponechat prázdné.
FolderProtocol	Nastavte typ funkce Skenovat do mé složky. Síťová složka/FTP (SMB): 0, FTP: 1
FolderPath	Nastavte umístění ukládání pro funkci Skenovat do mé složky.
FolderUserName	Nastavte uživatelské jméno pro funkci Skenovat do mé složky.
FolderPassword	Nastavte heslo pro ověření cílové složky pro funkci Skenovat do mé složky v rozsahu 32 znaků ASCII. Při importování je toto nastaveno jako heslo místo **EncPassword**. Při exportování je toto pole vždy prázdné.

Položka	Nastavení a vysvětlení
FtpPassive	Nastavte režim připojení pro server FTP, když je vybráno **FTP** jako **Typ** pro funkci Skenovat do mé složky. Aktivní režim: 0, pasivní režim: 1
FtpPort	Nastavte číslo portu pro odesílání skenovaných dat na server FTP od 0 do 65535, když je vybráno **FTP** jako **Typ** pro funkci Skenovat do mé složky.
ScanToMemory	Nastavte omezení pro Skenovat na USB disk. Nepovoleno: 0, povoleno: 1
ScanToMail	Nastavte omezení pro Skenovat do e-mailu. Možnost **Skenovat do e-mailu** můžete nastavit, pouze pokud jste povolili možnost **Skenovat do e-mailu**. Nepovoleno: 0, povoleno: 1
ScanToFolder	Nastavte omezení pro Skenovat do síťové složky/FTP. Možnost **Skenovat do mé složky** můžete nastavit, pouze pokud jste povolili možnost **Skenovat do síťové složky/FTP**. Nepovoleno: 0, povoleno: 1
ScanToCloud	Nastavte omezení pro Skenovat do cloudu. Nepovoleno: 0, povoleno: 1
ScanToComputer	Nastavte omezení pro Skenovat do počítače. Nepovoleno: 0, povoleno: 1
PresetIndex	Nastavte Předvolby, které chcete přidružit k uživateli. Můžete nakonfigurovat až pět registračních čísel Předvolby oddělených čárkami.
EncPassword	Při exportu uživatelských nastavení se parametr nastavený pro možnost **Password** zašifruje a pak se hodnota zakóduje pomocí kódu BASE64 a vydá. Při importu s novým heslem pro možnost **Password** se tato hodnota ignoruje. Pokud je položka **Password** prázdná, tato hodnota se použije a heslo zůstane stejné jako před exportem.
EncFolderPassword	Při exportu se parametr nastavený pro možnost **FolderPassword** zašifruje a pak se hodnota zakóduje pomocí kódu BASE64 a vydá. Při importu s novým heslem pro možnost **FolderPassword** se tato hodnota ignoruje. Pokud je položka **FolderPassword** prázdná, tato hodnota se použije a heslo zůstane stejné jako před exportem.

Import souboru CSV

1. Otevřete Web Config a vyberte kartu **Zabezpečení produktu** > **Nastavení uživatele**.
2. Klikněte na položku **Importovat**.
3. Vyberte soubor, který chcete importovat.
4. Klikněte na položku **Importovat**.

5. Po kontrole zobrazených informací klikněte na tlačítko **OK**.

Registrace User Settings do více skenerů dávkou (Epson Device Admin)

User Settings používané v Místní DB můžete registrovat dávkou pomocí serveru LDAP nebo souboru CSV/ENE.

Poznámka:
*Soubor ENE představuje binární soubor poskytovaný společností Epson, který šifruje a ukládá informace pro **Contacts**, například osobní údaje a Nastavení uživatele. Lze ho exportovat z Epson Device Admin a můžete nastavit heslo. Hodí se, pokud chcete importovat Nastavení uživatele ze souboru zálohy.*

Import ze souboru CSV/ENE

1. Vyberte možnost **Administrator Settings** > **Authentication Settings** > **User Settings** ze šablony konfigurace.
2. Klikněte na položku **Import**.
3. Vyberte položku **CSV or ENE File** z nabídky **Import Source**.
4. Klikněte na položku **Browse**.

   Zobrazí se obrazovka výběru souboru.
5. K otevření vyberte soubor, který chcete importovat.
6. Vyberte metodu importu.
   - ❏ Overwrite and Add: přepíše se, pokud existuje ID stejného uživatele; přidá nové ID, pokud neexistuje.
   - ❏ Replace All: nahradí vše nastavením uživatele, které chcete importovat.
7. Klikněte na položku **Import**.

   Zobrazí se obrazovka nastavení potvrzení.
8. Klikněte na položku **OK**.

   Zobrazí se výsledek ověření.

   Poznámka:
   - ❏ *Pokud počet importovaných nastavení uživatele překročí počet, který lze importovat, vyzve vás zpráva k odstranění některých nastavení uživatele. Před importem odstraňte přebytečná nastavení uživatele.*
   - ❏ *Vyberte nastavení uživatele, které chcete před importem odstranit, a pak klikněte na **Delete**.*
9. Klikněte na položku **Import**.

   Informace o nastavení se importují do šablony konfigurace.

Import ze serveru LDAP

1. Vyberte možnost **Administrator Settings** > **Authentication Settings** > **User Settings** ze šablony konfigurace.
2. Klikněte na položku **Import**.

3. Vyberte položku **LDAP** z nabídky **Import Source**.

4. Klikněte na položku **Settings**.

   Zobrazí se nastavení **LDAP Server**.

   Poznámka:
   Toto nastavení serveru LDAP se používá k importu uživatelských nastavení ze serveru LDAP. Importované (zkopírované) uživatelské nastavení se používá k ověřování uživatelů prostřednictvím samotného skeneru.

   *Na druhou stranu, když jako metodu ověřování vyberete **LDAP** nebo **Local DB and LDAP**, budou uživatelé ověřování komunikací se serverem LDAP.*

5. Nastavte každou položku.

   Při importování uživatelského nastavení ze serveru LDAP můžete kromě položek v nastavení LDAP také konfigurovat následující nastavení.

   Další položky naleznete v souvisejících informacích.

Položka			Vysvětlení
LDAP Server Settings	LDAP Server Type		Umožňuje výběr typu serveru LDAP.
Search Settings	Search Filter		Text používaný pro filtr hledání LDAP můžete nastavit. K úpravě textu hledání vyberte **Custom**.
	Options	Type	Typ cílového umístění ukládání pro **Scan To My Folder** můžete nastavit.
		Connection Mode	Po nastavení možnosti **Type** na hodnotu **FTP** můžete nastavit režim připojení FTP.
		Port Number	Po nastavení možnosti **Type** na hodnotu **FTP** můžete nastavit číslo portu, který chcete použít.

6. Proveďte test připojení dle potřeby kliknutím na položku **Connection Test**.

   Načte a zobrazí 10 uživatelských nastavení ze serveru LDAP.

7. Klikněte na položku **OK**.

8. Vyberte metodu importu.

   ❏ Overwrite and Add: přepíše se, pokud existuje ID stejného uživatele; přidá nové ID, pokud neexistuje.

   ❏ Replace All: nahradí vše nastavením uživatele, které chcete importovat.

9. Klikněte na položku **Import**.

   Zobrazí se obrazovka nastavení potvrzení.

10. Klikněte na položku **OK**.

    Zobrazí se výsledek ověření.

11. Klikněte na položku **Import**.

    Informace o nastavení se importují do šablony konfigurace.

Související informace

➡ „Konfigurování serveru LDAP“ na str. 142
➡ „Konfigurace nastavení vyhledávání serveru LDAP“ na str. 144

Synchronizace se Server LDAP

Proveďte nastavení Server LDAP pro skener.

Vytvořte nastavení pro primární server a sekundární server dle potřeby.

Poznámka:
*Nastavení **Server LDAP** je sdíleno s **Kontakty**.*

Dostupné služby

Podporovány jsou následující adresářové služby.

Název služby	Verze
Active Directory	Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019
OpenLDAP	Ver.2.3, Ver.2.4

Konfigurování serveru LDAP

Chcete-li používat server LDAP, je potřeba jej nejprve nakonfigurovat.

Při nastavení z nástroje Web Config:

Vyberte kartu **Síť** > **Server LDAP** > **Základní (Primární server)** nebo **Základní (Sekundární server)**.

Pokud vyberete metodu **Ověření Kerberos** jako **Způsob ověření**, vyberte možnost **Síť** > **Nastavení Kerberos** a proveďte nastavení pro Kerberos.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Network** > **LDAP server** > **Server Settings (Primary Server)** nebo **Server Settings (Secondary Server)** ze šablony konfigurace.

Pokud vyberete metodu **Ověření Kerberos** jako **Způsob ověření**, vyberte možnost **Network — Security** > **Nastavení Kerberos** a proveďte nastavení pro Kerberos.

Položka	Nastavení a vysvětlení
Použít server LDAP	Vyberte možnost **Použít** nebo **Nepoužívejte**.
Adresa serveru LDAP	Zadejte adresu serveru LDAP. Zadejte 1 až 255 znaků ve formátu protokolu IPv4 nebo IPv6 nebo jména FQDN. V případě formátu FQDN můžete použít alfanumerické znaky ve formátu ASCII (0x20–0x7E) a spojovníky s výjimkou začátku a konce adresy.
Číslo portu serveru LDAP (Port number)	Zadejte číslo portu serveru LDAP pomocí čísel 1 až 65535.
Zabezpečené připojení	Určete metodu ověřování skeneru pro přístup k serveru LDAP.

Položka	Nastavení a vysvětlení
Ověření certifikátu	Až tuto funkci povolíte, ověří se certifikát serveru LDAP. Doporučujeme nastavení této možnosti na hodnotu **Povolit**. Abyste ji mohli nastavit, je nutné do skeneru importovat **Certifikát CA**.
Časový limit hledání (s)	Zvolte časový limit pro vyhledávání, který může být mezi hodnotou 5 až 300 sekund.
Způsob ověření	Vyberte metodu ověření. Pokud vyberete **Ověření Kerberos**, proveďte nastavení pro Kerberos předem. Abyste mohli provádět Ověření Kerberos, je nutné následující prostředí. ❏ Skener může komunikovat se serverem DNS. ❏ Čas skeneru, serveru KDC a serveru nutného pro ověřování (server LDAP, server SMTP, souborový server) je synchronizovaný. ❏ Když se serveru služby přiřadí IP adresa, FQDN serveru služby se zaregistruje do zóny zpětného vyhledávání serveru DNS.
Sféra Kerberos k použití	Pokud nastavíte položku **Způsob ověření** na hodnotu **Ověření Kerberos**, vyberte sféru Kerberos, kterou chcete použít.
DN správce / Uživatelské jméno	Zadejte uživatelské jméno serveru LDAP. Zadat můžete až 128 znaků ve formátu Unicode (UTF-8). Nepoužívejte řídicí znaky, například znaky 0x00 až 0x1F nebo 0x7F. Toto nastavení není použito, pokud je položka **Způsob ověření** nastavena na hodnotu **Anonymní ověření**. Pokud nechcete tuto položku určit, ponechte pole prázdné.
Heslo	Zadejte heslo ověřování serveru LDAP. Zadat můžete až 128 znaků ve formátu Unicode (UTF-8). Nepoužívejte řídicí znaky, například znaky 0x00 až 0x1F nebo 0x7F. Toto nastavení není použito, pokud je položka **Způsob ověření** nastavena na hodnotu **Anonymní ověření**. Pokud nechcete tuto položku určit, ponechte pole prázdné.

Nastavení protokolu Kerberos

Pokud vyberete volbu **Ověření Kerberos** jako nastavení **Způsob ověření**, je třeba vybrat konkrétní nastavení protokolu Kerberos. Můžete zaregistrovat až 10 nastavení Kerberos.

Při nastavení z nástroje Web Config:

Vyberte kartu **Síť** > **Nastavení Kerberos**.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Network** > **Security** > **Nastavení Kerberos** ze šablony konfigurace.

Položka	Nastavení a vysvětlení
Sféra (doména)	Zadejte hodnotu sféry ověřování protokolu Kerberos. Hodnota může být vyjádřena až 255 znaky standardu ASCII (0x20 až 0x7E). Pokud nechcete tuto položku registrovat, ponechte pole prázdné.
Adresa KDC	Zadejte adresu serveru ověřování protokolu Kerberos. Do pole zadejte maximálně 255 znaků ve formátu protokolu IPv4 nebo IPv6 nebo jména FQDN. Pokud nechcete tuto položku registrovat, ponechte pole prázdné.
Číslo portu (Kerberos)	Zadejte číslo portu serveru Kerberos pomocí čísel 1 až 65535.

Konfigurace nastavení vyhledávání serveru LDAP

Nastaví atributy vyhledávání pro nastavení uživatele.

Při nastavení z nástroje Web Config:

Vyberte kartu **Síť** > **Server LDAP** > **Prohledat nastavení (ověřování)**.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Administrator Settings** > **Authentication Settings** > **LDAP server** > **Search Settings (Authentication)** ze šablony konfigurace.

Položka	Nastavení a vysvětlení
Search Base (Distinguished Name)	Zadejte počáteční polohu při hledání informací o uživateli ze serveru LDAP. Zadejte 0 až 128 znaků ve formátu Unicode (UTF-8). Pokud nechcete vyhledat libovolný atribut, ponechte toto pole prázdné. Příklad místního adresáře serveru: dc=server,dc=local
User ID Attribute	Zadejte název atributu, který se zobrazí při vyhledávání čísla ID. Zadejte mezi 1 a 255 znaky ve formátu ASCII. Prvním znakem musí být některé z písmen a–z nebo A–Z. Příklad: cn, uid
User name Display Attribute	Zadejte název atributu, který se zobrazí jako uživatelské jméno. Zadejte mezi 0 a 255 znaky ve formátu ASCII. Prvním znakem musí být některé z písmen a–z nebo A–Z. Toto pole můžete ponechat prázdné. Příklad: cn, name
Authentication Card ID Attribute	Zadejte název atributu, který se zobrazí jako ID karty ověřování. Zadejte mezi 0 a 255 znaky ve formátu ASCII. Prvním znakem musí být některé z písmen a–z nebo A–Z. Toto pole můžete ponechat prázdné. Příklad: cn, sn
ID Number Attribute	Zadejte název atributu, který se zobrazí při vyhledávání čísla ID. Zadejte mezi 1 a 255 znaky ve formátu ASCII. Prvním znakem musí být některé z písmen a–z nebo A–Z. Příklad: cn, id
Department Attribute	Zadejte název atributu, který se zobrazí jako název oddělení. Zadejte mezi 0 a 255 znaky ve formátu ASCII. Prvním znakem musí být některé z písmen a–z nebo A–Z. Toto pole můžete ponechat prázdné. Příklad: ou, ou-cl
Email Address Attribute	Zadejte název atributu, který se zobrazí při vyhledávání e-mailových adres. Zadejte mezi 1 a 255 znaky ve formátu ASCII. Prvním znakem musí být některé z písmen a–z nebo A–Z. Příklad: mail
Save To Attribute	Zadejte název atributu, který odkazuje na umístění uložení Scan To My Folder. Zadejte mezi 0 a 255 znaky ve formátu ASCII. Příklad: homeDirectory

Kontrola připojení serveru LDAP

Provede test připojení k serveru LDAP pomocí parametrů nastavených v **Server LDAP** > **Nastavení hledání**.

1. Otevřete nástroj Web Config a vyberte kartu **Síť** > **Server LDAP** > **Test připojení**.
2. Vyberte **Spustit**.

   Bude zahájena zkouška připojení. Po dokončení zkoušky bude zobrazena kontrolní zpráva.

Reference ke zkoušce připojení serveru LDAP

Zprávy	Vysvětlení
Test připojení byl úspěšný.	Tato zpráva se zobrazí při úspěšně provedeném připojení k serveru.
Test připojení se nezdařil. Zkontrolujte nastavení.	Zobrazí se v následujících situacích: ❏ Adresa nebo číslo portu serveru LDAP nejsou správné. ❏ Vypršel časový limit. ❏ Položka **Použít server LDAP** je nastavena na hodnotu **Nepoužívejte**. ❏ Pokud je položka **Způsob ověření** nastavena na hodnotu **Ověření Kerberos**, nejsou nastavení, například **Sféra (doména)**, **Adresa KDC** a **Číslo portu (Kerberos)** správná.
Test připojení se nezdařil. Zjistěte Datum a čas ve vašem produktu nebo na server.	Tato zpráva se zobrazí, pokud selže připojení, protože nastavení času na skeneru a serveru LDAP se neshodují.
Ověření se nezdařilo. Zkontrolujte nastavení.	Zobrazí se v následujících situacích: ❏ Položky **Uživatelské jméno** a/nebo **Heslo** nejsou správné. ❏ Pokud je položka **Způsob ověření** nastavena na hodnotu **Ověření Kerberos**, nemusí být nakonfigurován čas/datum.
Do dokončení zpracování nelze produkt zpřístupnit.	Tato zpráva se zobrazí, pokud skener vykonává nějakou činnost.

Nastavení e-mailového serveru

Pokud používáte **Skenovat do e-mailu**, nastavte e-mailový server.

Poznámka:
*Možnost **Skenovat do e-mailu** můžete nastavit, pouze pokud jste povolili možnost **Skenovat do e-mailu**.*

Při nastavení z nástroje Web Config:

Vyberte kartu **Síť** > **Poštovní server** > **Základní**.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Common** > **Email Server** > **Mail Server Settings** ze šablony konfigurace.

Položka	Nastavení a vysvětlení	
Způsob ověření	Určete metodu ověřování skeneru pro přístup k poštovnímu serveru.	
	Vypnout	Ověřování je při komunikaci s poštovním serverem zakázané.
	OVĚŘENÍ SMTP	E-mailový server musí podporovat ověření SMTP.
	POP před SMTP	Pokud zvolíte tuto položku, nastavte server POP3.
Ověřený účet	Pokud zvolíte možnost **OVĚŘENÍ SMTP** nebo **POP před SMTP** jako **Způsob ověření**, zadejte název ověřovaného účtu. Zadejte od 0 do 255 znaků ve formátu ASCII (0x20–0x7E).	
Ověřené heslo	Pokud zvolíte možnost **OVĚŘENÍ SMTP** nebo **POP před SMTP** jako **Způsob ověření**, zadejte ověřované heslo. Zadejte od 0 do 20 znaků ve formátu ASCII (0x20–0x7E).	
E-mailová adresa odesílatele	Zadejte e-mailovou adresu odesilatele. Zadejte 0 až 255 znaků ve formátu ASCII (0x20–0x7E) vyjma znaků : ( ) < > [ ] ; ¥. Jako první znak nelze použít tečku „.“.	
Adresa serveru SMTP	Zadejte 0 až 255 znaků s použitím znaků A–Z a–z 0–9 . -. Lze použít formát IPv4 nebo FQDN.	
Číslo portu serveru SMTP	Zadejte číslo 1 až 65535.	
Zabezpečené připojení	Určete metodu zabezpečeného připojení poštovního serveru.	
	Žádná	Vyberete-li **POP před SMTP** v **Způsob ověření**, bude metoda připojení nastavena na **Žádná**.
	SSL/TLS	Tato možnost je dostupná, když je položka **Způsob ověření** nastavena na **Vypnout** nebo **OVĚŘENÍ SMTP**.
	STARTTLS	Tato možnost je dostupná, když je položka **Způsob ověření** nastavena na **Vypnout** nebo **OVĚŘENÍ SMTP**.
Ověření certifikátu	Když je tato možnost povolena, certifikát je ověřen. Doporučujeme nastavení této možnosti na hodnotu **Povolit**.	
Adresa serveru POP3	Pokud zvolíte možnost **POP před SMTP** jako **Způsob ověření**, zadejte adresu serveru POP3. Můžete zadat od 0 do 255 znaků s použitím znaků A–Z a–z 0–9. Lze použít formát IPv4 nebo FQDN.	
Číslo portu serveru POP3	Pokud zvolíte možnost **POP před SMTP** jako **Způsob ověření**, zadejte číslo portu. Zadejte číslo 1 až 65535.	

Nastavení režimu Skenovat do mé složky

Uloží naskenované snímky do složky přiřazené jednotlivým uživatelům. Můžete nastavit následující jako specializovanou složku.

Poznámka:
*Možnost **Scan To My Folder** můžete nastavit, pouze pokud jste povolili možnost **Skenovat do síťové složky/FTP**.*

Uložit do nastavení	Způsob ověření	Umístění nastavení cesty ke složce
Zadejte jednu síťovou složku pro veškeré Nastavení ověření a automaticky vytvořte osobní složku pod stanovenou složku pomocí jména a ID uživatele.	❏ Místní DB ❏ LDAP ❏ Místní DB a LDAP	Skener (nastavení Skenovat do mé složky)

Uložit do nastavení	Způsob ověření	Umístění nastavení cesty ke složce
Přiřadit různé síťové složky individuálně každému uživateli.	Místní DB	Skener (Nastavení uživatele)
	LDAP	Atributy LDAP
	Místní DB a LDAP	Skener (Nastavení uživatele) nebo atributy LDAP

Při nastavení z nástroje Web Config:

Vyberte kartu **Zabezpečení produktu** > **Skenovat do síťové složky/FTP**.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Administrator Settings** > **Authentication Settings** > **Skenovat do síťové složky/FTP** > **Scan to My Folder** ze šablony konfigurace.

Položka		Vysvětlení
Uložit do nastavení	Typ nastavení	❏ **Sdílené**: Automaticky vytvoří složku pojmenovanou po ID uživatele v umístění složky nebo na adrese URL určené v nastavení **Uložit do** a uloží naskenované snímky do této složky. ❏ **Jednotlivě**: Slouží k nastavení umístění výsledků skenování pro jednotlivé uživatele. Uživatele Místní DB lze nastavit v nastavení uživatelů. Uživatelé LDAP využívají umístění úložiště získané z atributů hledání serveru LDAP.
	Typ	Vyberte protokol přenosu v souladu s cílovým umístěním výstupu skenování. U síťové složky: **Síťová složka (SMB)** U serveru FTP: **FTP**
	Uložit do	Zadejte cestu nebo adresu URL cesty výstupu. Zadejte až 160 znaků v Unicode (UTF-16).
	Režim připojení	Nastavte, když vyberete **FTP** v **Typ**. Vyberte režim připojení k serveru FTP.
	Číslo portu	Nastavte, když vyberete **FTP** v **Typ**. Zadejte číslo portu v rozsahu 0 až 65535 a odešlete naskenovaná data na server FTP.

Položka		Vysvětlení
Nastavení ověření	Typ nastavení	Nastaví se, když vyberete **Jednotlivě** jako **Typ nastavení** v **Uložit do nastavení**. Nastavením „Uživatelské jméno“ a „Heslo“ otevřete složku. ❏ **Sdílené**: Použijte společné **Uživatelské jméno** a **Heslo** pro všechny uživatele. ❏ **Jednotlivě**: Pro uživatele Místní DB nastavte **Uživatelské jméno** a **Heslo** individuálně v **Nastavení uživatele**. Uživatele LDAP nelze konfigurovat individuálně. Možnosti **Uživatelské jméno** a **Heslo** nastavení prostřednictvím této položky se používají v dávce.
	Uživatelské jméno	Zadejte uživatelské jméno pro přístup do složky cílového výstupu skenování. Zadejte až 30 znaků v Unicode (UTF-16). Tuto možnost nastavte, když používáte **Sdílené** nebo server LDAP.
	Heslo	Zadejte heslo odpovídající **Uživatelské jméno**. Zadejte až 20 znaků v Unicode (UTF-16). Tuto možnost nastavte, když používáte **Sdílené** nebo server LDAP.

Zakázat změnu cílového umístění pro Skenovat do síťové složky/FTP

Položka	Vysvětlení
Zakázat ruční zadání cíle	Po povolení uživatel nemůže změnit výchozí cílové umístění.

Přizpůsobit funkce jedním dotykem

Chcete-li, aby se zobrazovaly pouze nezbytné ikony, můžete upravit rozložení ikon zobrazených na hlavní obrazovce pro ovládací panel.

Při nastavení z nástroje Web Config:

Vyberte kartu **Zabezpečení produktu** > **Přizpůsobit funkce jedním dotykem**.

Při nastavení z nástroje Epson Device Admin:

Vyberte možnost **Administrator Settings** > **Authentication Settings** > **Customize One-touch Functions** ze šablony konfigurace.

Poznámka:
V následujících případech nebudou ikony určených funkcí zobrazeny na hlavní obrazovce.

❏ *Když vyberete funkce, které nejsou povoleny z důvodu **Omezení**.*

❏ *Když není zaregistrována e-mailová adresa pro přihlášeného uživatele. (Skenovat do e-mailu)*

❏ *Když není nastavena cílová složka. (Skenovat do mé složky)*

Položka	Vysvětlení
Maximum funkcí na obrazovku	Vyberte rozložení ikon zobrazených na ovládacím panelu. Obrázek se změní podle vybraného rozložení.

Položka	Vysvětlení
Obrazovka(y)	Vyberte počet stránek.
Číslo	Vyberte funkce, které chcete zobrazit pro každou číslovanou pozici.

Sestavy Job History pomocí Epson Device Admin

Pro každou skupinu a každého uživatele můžete vytvořit sestavu Job History pomocí Epson Device Admin. Do skeneru můžete uložit až 3 000 instancí historií využívání. Sestavu můžete vytvořit zadáním období nebo nastavením běžného rozvrhu.

K exportu Job History jako sestavy vyberte možnost **Options** > **Epson Print Admin Serverless/Authentication Settings** > **Manage the Epson Print Admin Serverless/Authentication compatible devices** v nabídce pásu karet na obrazovce Seznam zařízení.

Podrobnosti o vytvoření uživatelské zprávy naleznete v dokumentaci pro Epson Device Admin.

Položky, které mohou být součástí zprávy

Do uživatelské zprávy můžete uvést následující položky.

Date/Job ID/Operation/User ID/Department/Result/Result details/Scan: Destination type/Scan: Destination/Scan: Paper Size/Scan: 2-Sided/Scan: Color/Scan: Pages/Devices: Model/Devices: IP Address/Devices: Serial Number/Devices: Department/Devices: Location/Devices: Remark/Devices: Note

Přihlašování jako správce na ovládacím panelu

K přihlášení jako správce z ovládacího panelu skeneru můžete použít libovolné z následujících metod.

1. Klepněte na  v pravé horní části obrazovky.
   - ❏ Po povolení možnosti Nastavení ověření se ikona zobrazí na obrazovce **Vítejte** (obrazovka pohotovostního režimu ověřování).
   - ❏ V případě zákazu Nastavení ověření se ikona zobrazí na domovské obrazovce.
2. Po zobrazení potvrzovací obrazovky klepněte na **Ano**.
3. Zadejte heslo správce.

   Zobrazí se zpráva o dokončeném přihlášení a pak se zobrazí domovská obrazovka na ovládacím panelu.

K odhlášení klepněte na  v pravé horní části obrazovky Domů.

Zakázání Nastavení ověření

Funkci Nastavení ověření lze zakázat pomocí nástroje Web Config.

Poznámka:
Nastavení uživatele registrované do skeneru se uloží, i když je možnost Nastavení ověření zakázána. Můžete je odebrat obnovením skeneru do původního nastavení.

1. Otevřete aplikaci Web Config.
2. Vyberte kartu **Zabezpečení produktu** > **Základní** > **Ověřování**.
3. Vyberte **Vypnuto**.
4. Klikněte na položku **Další**.
5. Klikněte na položku **OK**.

Poznámka:
I když možnost Nastavení ověření zakážete, možnost Nastavení zámku zůstane povolena. Pokud ji chcete zakázat, můžete nastavení změnit z ovládacího panelu nebo nástroje Web Config.

Související informace

➡ „Nastavení Nastavení zámku z ovládacího panelu“ na str. 86
➡ „Nastavení Nastavení zámku z nástroje Web Config“ na str. 86

Odstranění údajů Nastavení ověření (Obnovit výchozí nastavení)

Chcete-li odstranit všechny údaje Nastavení ověření (Čtečka karet, Způsob ověření, Nastavení uživatele a tak podobně), obnovte všechna nastavení skeneru do výchozího nastavení v okamžik nákupu.

Vyberte možnost **Nast.** > **Správa systému** > **Obnovit výchozí nastavení** > **Všechna nastavení** na ovládacím panelu.

Důležité:
Budou odstraněny všechny kontakty a další nastavení sítě. Odstraněná nastavení nelze obnovit.

Řešení problémů

Nelze načíst kartu pro ověřování

Zkontrolujte následující možnosti.

❏ Zkontrolujte, zda je zařízení pro ověřování správně připojeno ke skeneru.
Připojte zařízení pro ověřování k USB portu externího rozhraní na zadní straně skeneru.

❏ Zkontrolujte, zda jsou zařízení pro ověřování a karta pro ověřování podporované.

Údržba

Čištění vnější části skeneru

Odstraňte všechny skvrny suchou látkou nebo látkou navlhčenou neagresivním čisticím prostředkem nebo vodou.

Důležité:

- ❏ *K čištění skeneru zásadně nepoužívejte alkohol, ředidlo ani jakékoli jiné agresivní rozpouštědlo. Může dojít k deformacím nebo ztrátě barev.*
- ❏ *Zajistěte, aby do zařízení nepronikla voda. Mohlo by dojít k závadě.*
- ❏ *Nikdy neotevírejte skříň skeneru.*

1. Stisknutím tlačítka ⏻ vypnete skener.
2. Odpojte napájecí adaptér od skeneru.
3. Očistěte vnější kryt látkou navlhčenou neagresivním čisticím prostředkem nebo vodou.

   Poznámka:
   Otřete dotykovou obrazovku měkkým suchým hadříkem.

Čištění vnitřní části skeneru

Pokud je skener používán delší dobu, výskyt prachu z papíru a vzduchu na válečcích a na skle může způsobit potíže při podávání papíru nebo s kvalitou naskenovaných obrázků. Vyčistěte vnitřek skeneru po každých 5,000 skenech.

Aktuální počet skenů můžete zkontrolovat na ovládacím panelu nebo v aplikaci Epson Scan 2 Utility.

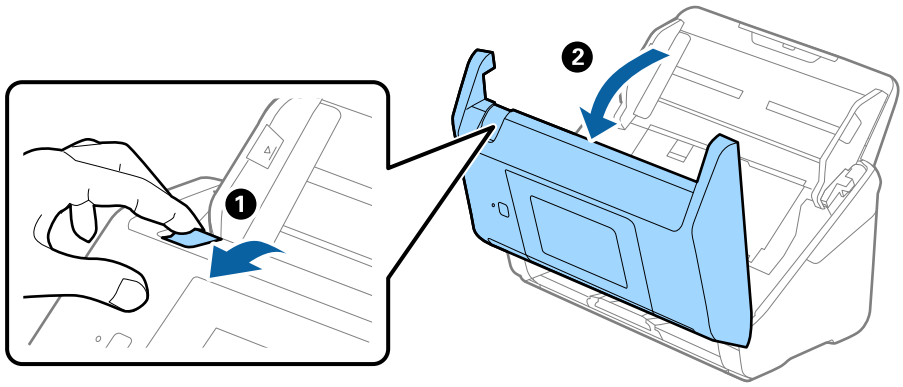
Pokud je povrch znečištěn těžko odstranitelnou látkou, pomocí originální čisticí sady Epson vyčistěte všechna znečištěná místa. Použijte malé množství čisticího prostředku na hadřík a vyčistěte všechny skvrny.

Důležité:

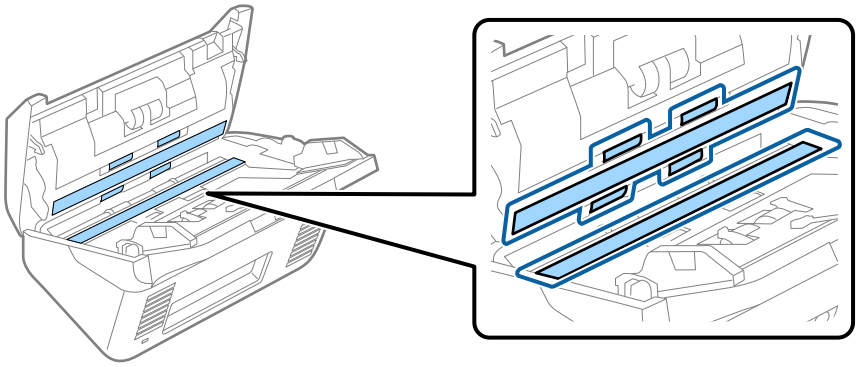
- ❏ *K čištění skeneru zásadně nepoužívejte alkohol, ředidlo ani jakékoli jiné agresivní rozpouštědlo. Může dojít k deformacím nebo ztrátě barev.*
- ❏ *Na skener nikdy nestříkejte žádné lubrikanty ani jiné kapaliny. Poničení zařízení nebo obvodů může vést k nestandardním operacím zařízení.*
- ❏ *Nikdy neotevírejte skříň skeneru.*

1. Stisknutím tlačítka ⏻ vypnete skener.
2. Odpojte napájecí adaptér od skeneru.

3. Zatáhněte za páčku a otevřete kryt skeneru.



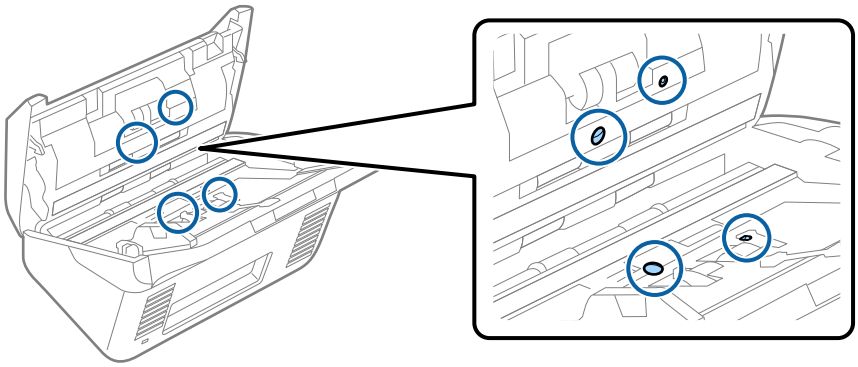
4. Pomocí jemného hadříku nebo originální čisticí sady Epson vyčistěte všechny skvrny na plastovém válečku a na ploše skla v dolní části uvnitř krytu skeneru.



Důležité:

- *Netlačte příliš na skleněný povrch.*
- *Nepoužívejte žádné kartáče ani tvrdé pomůcky. Jakékoli škrábance na skle mohou ovlivnit kvalitu skenování.*
- *Nestříkejte čisticí prostředek přímo na skleněný povrch.*

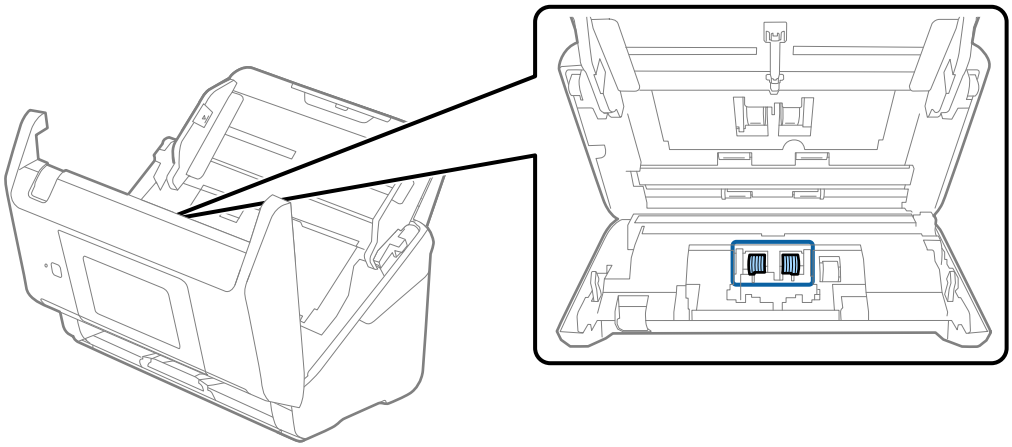
5. Vyčistěte všechny skvrny na senzorech vatovým tamponem.



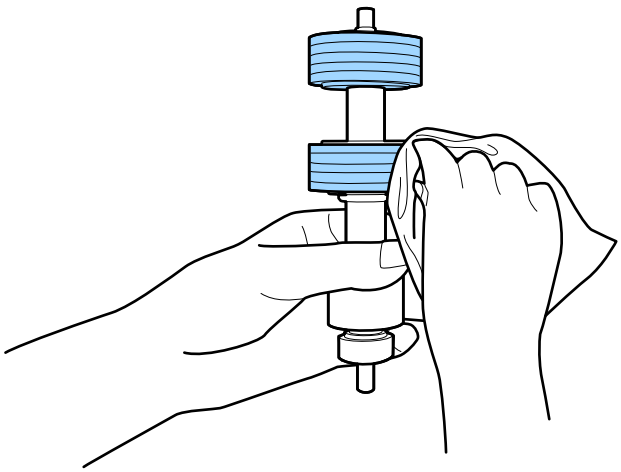
> ***Důležité:***
> *S vatovým tamponem nepoužívejte žádné kapaliny a tekuté čističe.*

6. Otevřete kryt a odeberte oddělovací váleček.

   Více informací naleznete v části „Výměna montážní sady válečků“.



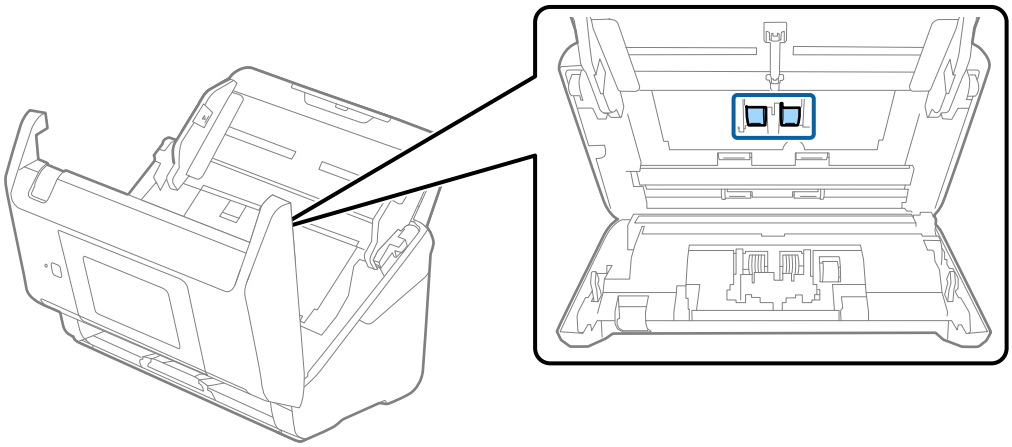
7. Pomocí originální čisticí sady Epson nebo jemného navlhčeného hadříku vyčistěte všechnu špínu nebo prach na oddělovacím válečku.



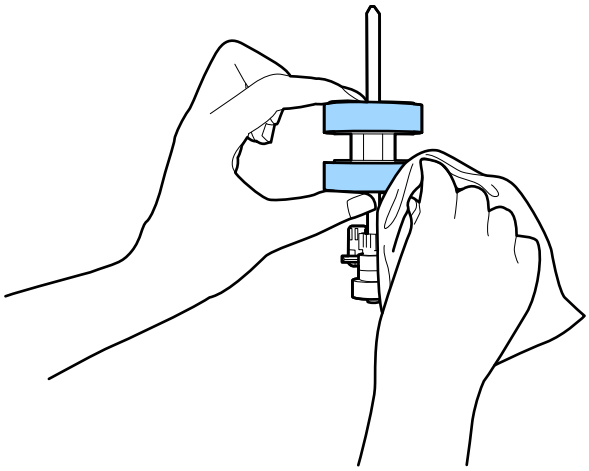
> ***Důležité:***
> *Pro vyčištění válečku použijte pouze originální čisticí sadu Epson nebo měkký navlhčený hadřík. Použití suchého hadříku by mohlo poškodit povrch válečku.*

8. Otevřete kryt a odeberte podávací váleček.

   Více informací naleznete v části „Výměna montážní sady válečků“.



9. Pomocí originální čisticí sady Epson nebo jemného navlhčeného hadříku vyčistěte všechnu špínu nebo prach na podávacím válečku.



> ***Důležité:***
>
> *Pro vyčištění válečku použijte pouze originální čisticí sadu Epson nebo měkký navlhčený hadřík. Použití suchého hadříku by mohlo poškodit povrch válečku.*

10. Zavřete kryt skeneru.

11. Zapojte napájecí adaptér a zapněte skener.

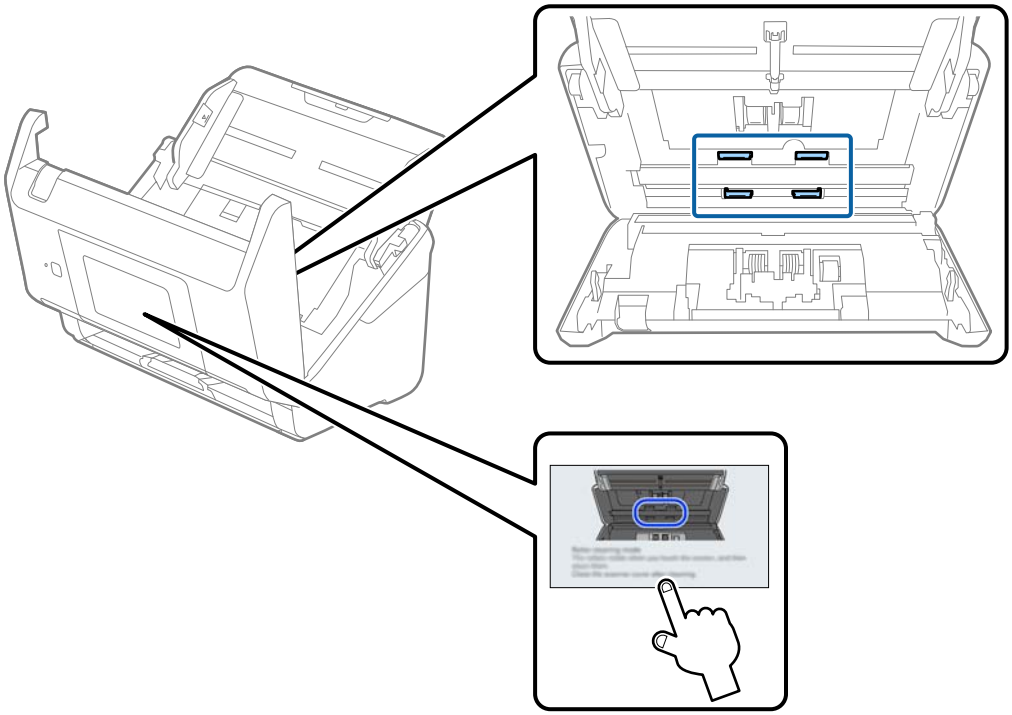
12. Vyberte možnost **Údržba skeneru** na domovské obrazovce.

13. Na obrazovce **Údržba skeneru** vyberte možnost **Čištění válce**.

14. Zatáhněte za páčku a otevřete kryt skeneru.

    Skener vstoupí do čisticího režimu válečku.

15. Pomalu otáčejte válečky ve spodní části poklepáním kdekoli na LCD. Otřete povrch válečků pomocí originální čisticí sady Epson nebo měkkého hadříku, navlhčeného ve vodě. Tento postup opakujte až do vyčištění válečků.



> ⚠ ***Upozornění:***
>
> *Při práci s válečkem si dejte pozor, abyste v mechanismu nenechali ruce nebo aby tam neuvízly vlasy. Mohlo by dojít k úrazu.*

16. Zavřete kryt skeneru.

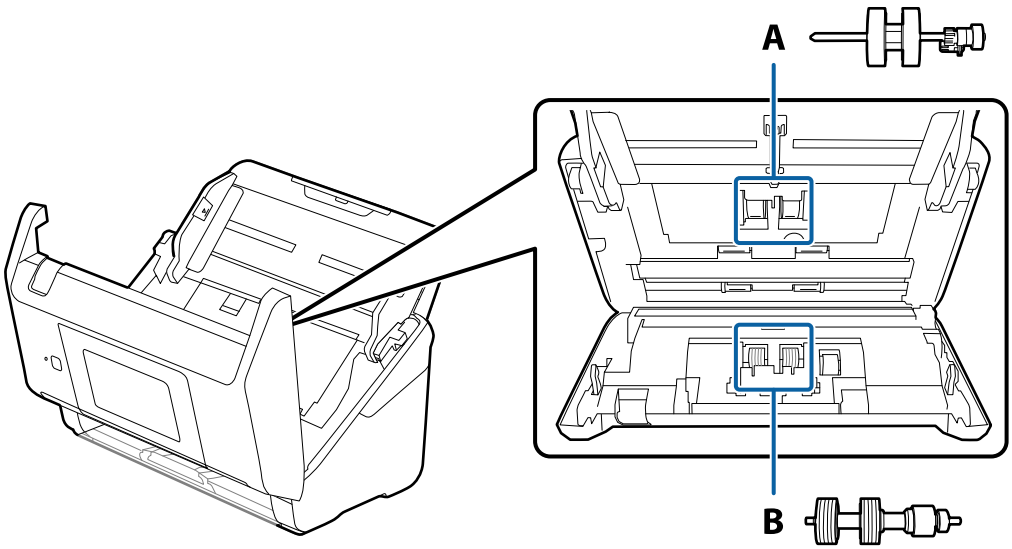
    Skener opustí čisticí režimu válečku.

Související informace

➡ „Výměna montážní sady válečků“ na str. 157

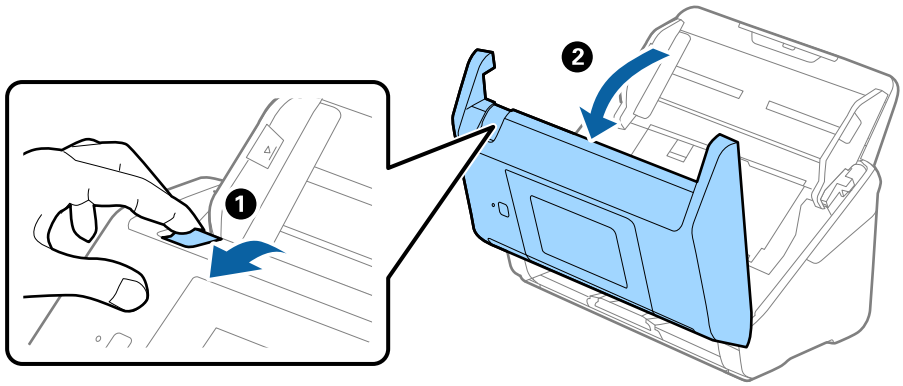
Výměna montážní sady válečků

Montážní sadu válců (podávací a oddělovací válec) je nutné vyměnit, jakmile počet skenů překročí množství určené jako životní cyklus válců. Jakmile se objeví zpráva o výměně na ovládacím panelu nebo na obrazovce vašeho počítače, následujte níže uvedené instrukce k provedení výměny.

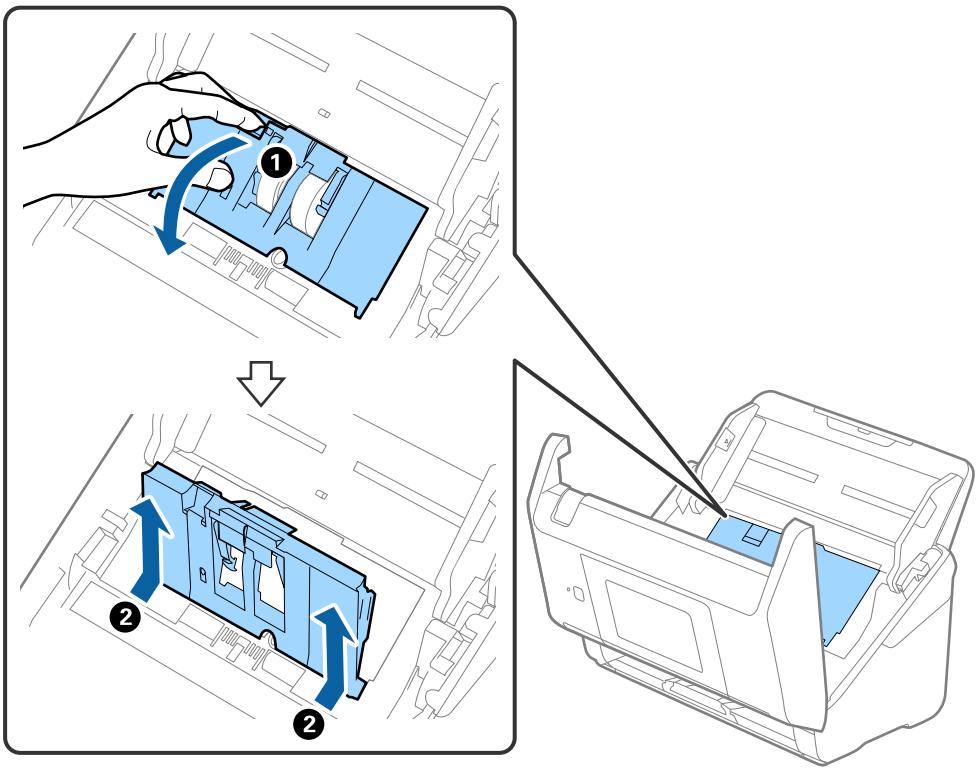


A: podávací válec, B: oddělovací válec

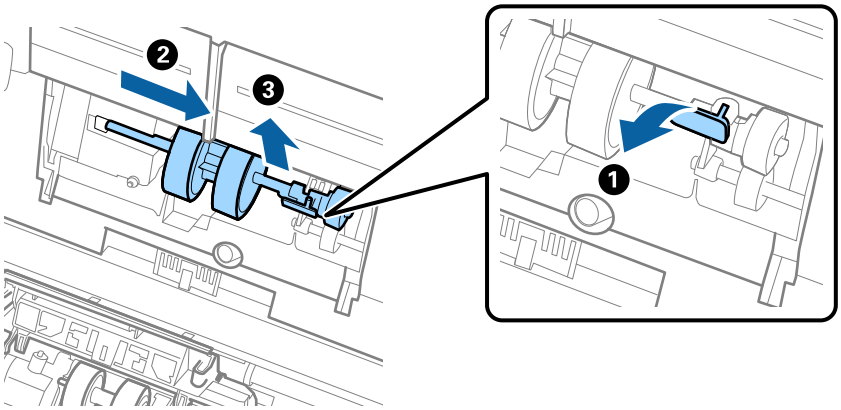
1. Stisknutím tlačítka ⏻ vypnete skener.
2. Odpojte napájecí adaptér od skeneru.
3. Zatáhněte za páčku a otevřete kryt skeneru.



4. Otevřete kryt podávacího válečku a potom jej vysunutím vyndejte.



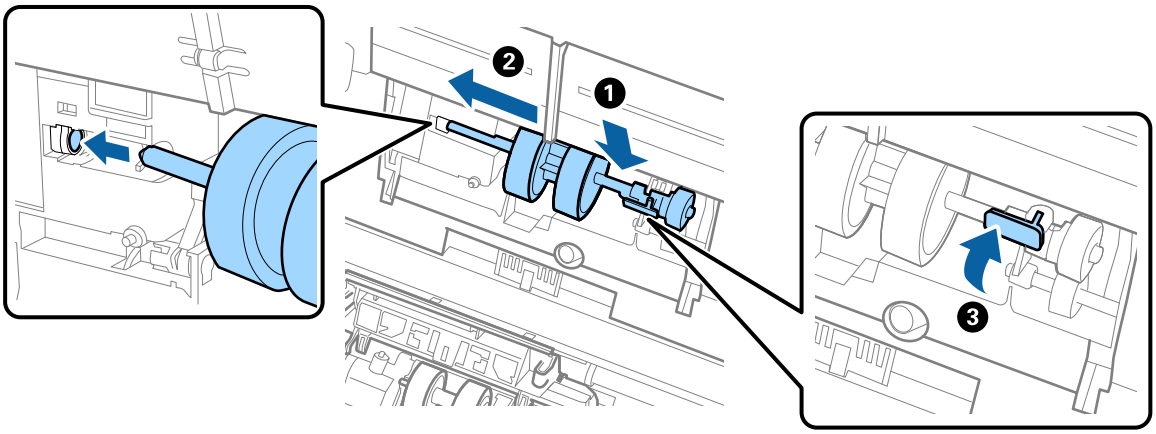
5. Zatáhněte dolů upínací prvek osy válečku a potom vysuňte a odeberte instalované podávací válečky.



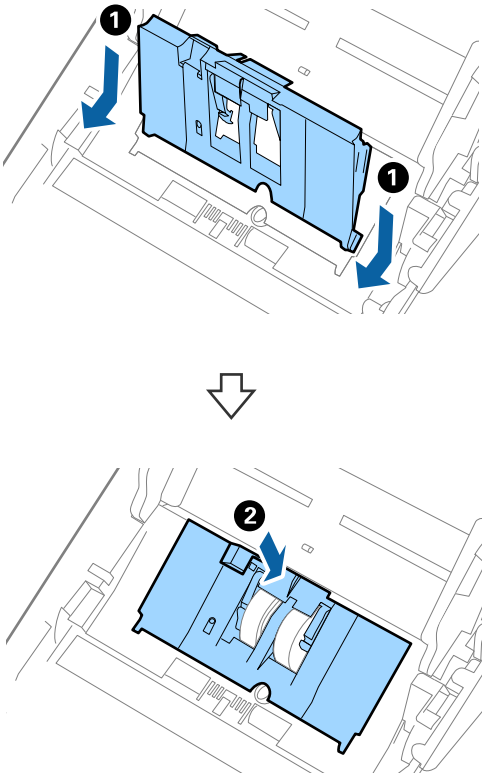
Důležité:

Podávací váleček nevytahujte ven silou. Mohlo by dojít k poškození vnitřních částí skeneru.

6. Držte dole upínací prvek a přitom zasuňte nový podávací váleček na levou stranu a vložte jej do otvoru ve skeneru. Zatlačte na upínací prvek a zabezpečte jej tak.

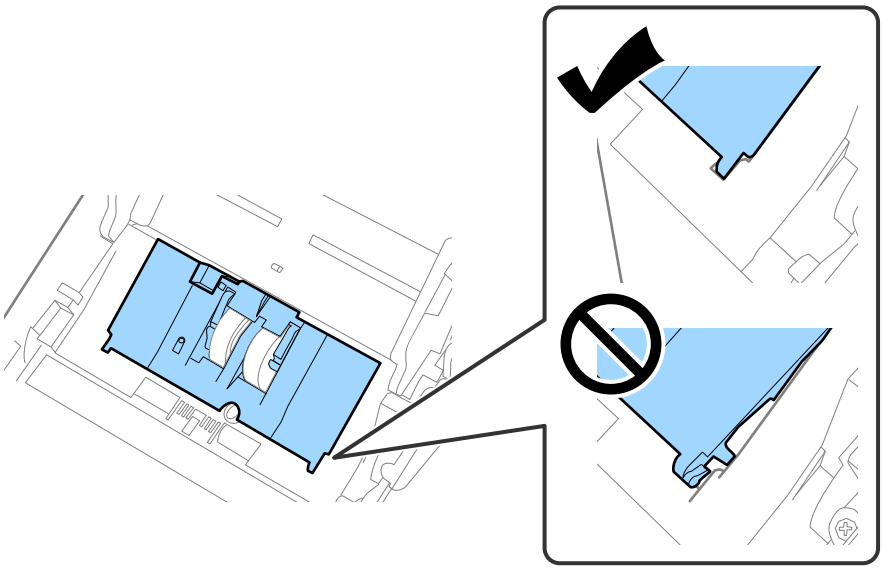


7. Okraj krytu podávacího válečku vložte do drážky a zasuňte jej. Pevně uzavřete kryt.

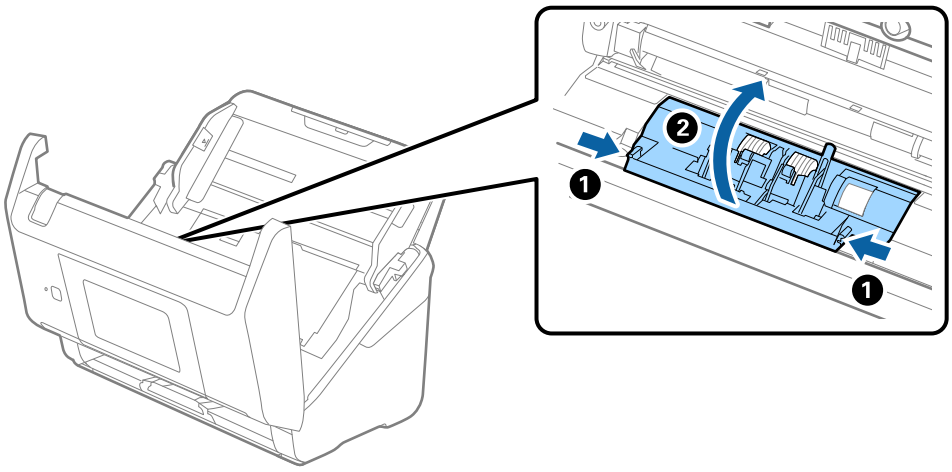


Důležité:

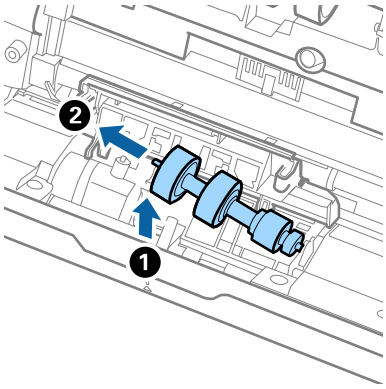
- ❏ *Ujistěte se, že je kryt podávacího válečku zavřený.*
- ❏ *Pokud jde kryt zavřít jen s potížemi, ujistěte se o správné instalaci podávacích válečků.*
- ❏ *Neinstalujte kryt, dokud je zvednutý.*



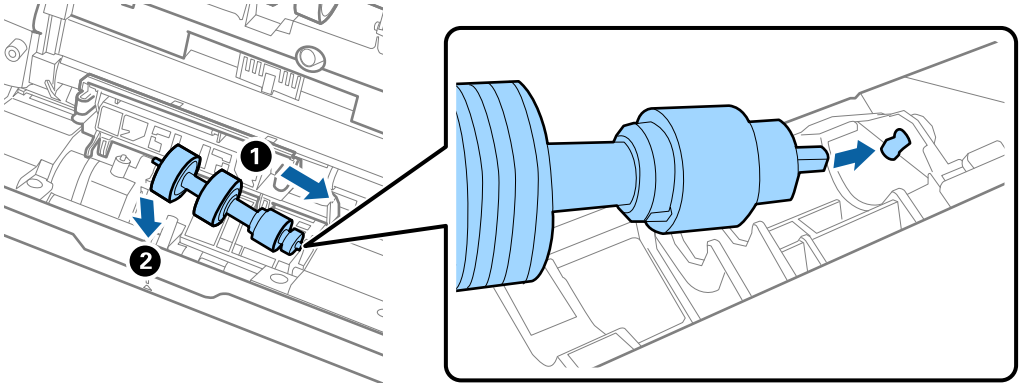
8. Zatlačte na háčky na obou koncích krytu oddělovacího válečku a kryt otevřete.



9. Zdvihněte levou stranu oddělovacího válečku a potom vysuňte a odeberte instalované oddělovací válečky.



10. Vložte novou osu oddělovacího válečku do otvoru na pravé straně a přesuňte váleček do nižší pozice.



11. Zavřete kryt oddělovacího válečku.

> ***Důležité:***
> *Pokud se kryt nedá zavřít, ujistěte se, že jsou válečky nainstalovány správně.*

12. Zavřete kryt skeneru.

13. Zapojte napájecí adaptér a zapněte skener.

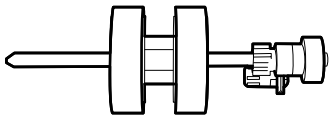
14. Resetujte počet skenů na ovládacím panelu.

Poznámka:
Zlikvidujte podávací a oddělovací váleček v souladu s pravidly určenými místním správním orgánem. Nepokoušejte se o rozmontování.

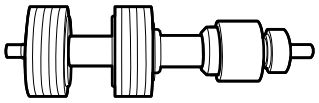
Kódy montážní sady válečků

Součásti (podávací a oddělovací váleček) by měly být po dosažení servisního počtu skenů vyměněny. Aktuální počet skenů můžete zkontrolovat na ovládacím panelu nebo v aplikaci Epson Scan 2 Utility.

A



B



A: podávací váleček, B: oddělovací váleček

Název součásti	Kódy	Životní cyklus
Montážní sada válečků	B12B819671 B12B819681 (pouze pro Indii)	200,000*

* Toto číslo bylo dosaženo skenováním po sobě jdoucích testovacích originálních papírů Epson a je vodítkem pro určení cyklu výměny. Cyklus výměny se může lišit v závislosti na typu papíru. Určité typy papíru vykazují vysokou míru papírového prachu, také papíry s hrubým povrchem mohou zkrátit životní cyklus součástí.

Resetování počtu skenů

Vynuluje počet skenů po výměně montážní sady válečků.

1. Na domovské stránce vyberte možnost **Nast.** > **Informace o zařízení** > **Resetovat počet skenů** > **Počet skenů po výměně válce**.
2. Klepněte na možnost **Ano**.

Související informace

➡ „Výměna montážní sady válečků“ na str. 157

Úspora energie

Pokud skener neprovádí žádné operace, můžete šetřit energii pomocí režimu spánku nebo režimu automatického vypnutí. Můžete zadat časový interval, po kterém skener přejde do režimu spánku, nebo se automaticky vypne. Jakékoli zvýšení bude mít dopad na spotřebu energie produktu. Před prováděním jakýchkoli změn vezměte do úvahy okolní prostředí.

1. Vyberte možnost **Nast.** na domovské obrazovce.
2. Vyberte **Základní nastavení**.

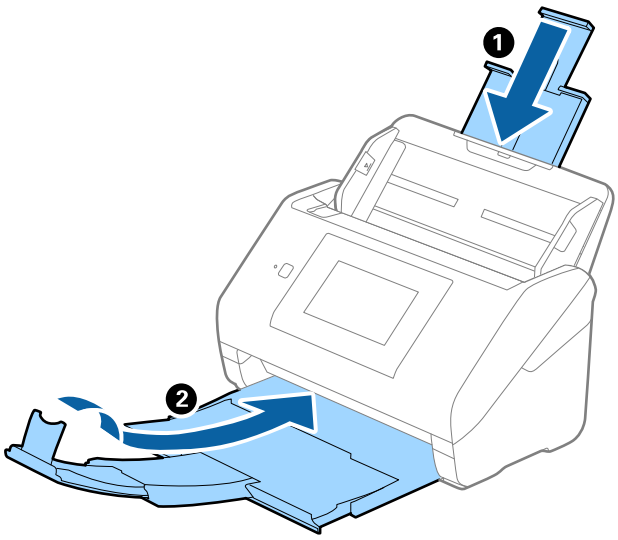
3. Vyberte **Nastavení vypnutí** a proveďte nastavení.

   Poznámka:
   Dostupné funkce se mohou lišit v závislosti na místu zakoupení.

Přeprava skeneru

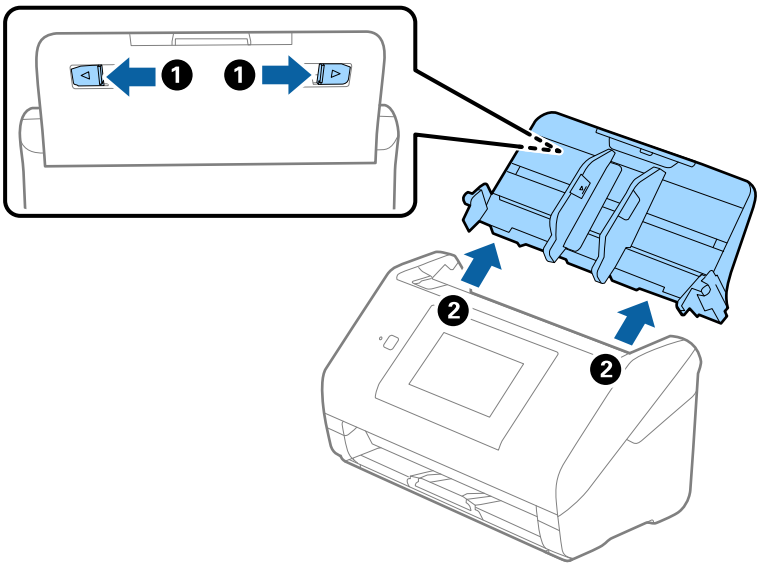
Hodláte-li přepravovat skener z důvodu změny místa nebo opravy, zabalte jej podle následujících pokynů.

1. Stiskněte tlačítko ⏻ pro vypnutí skeneru.
2. Odpojení napájecího adaptéru.
3. Odeberte kabely a zařízení.
4. Zavřete rozšíření vstupního zásobníku a výstupní zásobník.



> ***Důležité:***
> *Ujistěte se, že jste bezpečně zavřeli výstupní zásobník, v opačném případě by mohlo dojít k jeho poškození při přepravě.*

5. Odeberte vstupní zásobník.



6. Přidejte balicí materiály, které přišly se skenerem, poté skener zabalte do původní nebo do jiné odolné krabice.

Záloha nastavení

Můžete exportovat hodnotu nastavení z aplikace Web Config do souboru.Můžete ji použít pro zálohu kontaktů, nastavení hodnot, výměnu skeneru apod.

Exportovaný soubor nelze upravovat, protože je exportován jako binární soubor.

Exportování nastavení

Můžete exportovat nastavení skeneru.

1. Otevřete aplikaci Web Config a poté vyberte kartu **Správa zařízení** > **Exportovat a importovat hodnotu nastavení** > **Exportovat**.

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, kterým zašifrujete exportovaný soubor.

   Toto heslo budete potřebovat při importu daného souboru.Pokud soubor nechcete zašifrovat, ponechte toto pole prázdné.

4. Klikněte na možnost **Exportovat**.

> ***Důležité:***
> *Chcete-li exportovat nastavení sítě skeneru, například název zařízení a adresu IPv6, vyberte možnost **Povolte pro výběr individuálních nastavení zařízení** a vyberte další položky.Pro náhradní skener použijte pouze vybrané hodnoty.*

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Importování nastavení

Importování exportovaného souboru Web Config do tiskárny.

> ***Důležité:***
> *Při importu hodnot, které zahrnují individuální informace jako název skeneru nebo IP adresu se ujistěte, že stejná IP adresa neexistuje na stejné síti.*

1. Vstupte na Web Config a pak vyberte kartu **Správa zařízení** > **Exportovat a importovat hodnotu nastavení** > **Importovat**.
2. Vyberte exportovaný soubor a poté zadejte heslo použité při zašifrování souboru.
3. Klikněte na možnost **Další**.
4. Vyberte nastavení, které chcete importovat, a klikněte na možnost **Další**.
5. Klikněte na možnost **OK**.

Nastavení se vztahují na skener.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Obnovit výchozí nastavení

Na ovládacím panelu vyberte **Nast.** > **Správa systému** > **Obnovit výchozí nastavení** a pak vyberte položky, které chcete obnovit na výchozí hodnoty.

❏ Nastavení sítě: obnovení nastavení, souvisejících se sítí, do výchozího stavu.

❏ Vše kromě Nastavení sítě: obnovení nastavení do výchozího stavu s výjimkou nastavení, které souvisejí se sítí.

❏ Všechna nastavení: obnovení všech nastavení do výchozího stavu při pořízení.

Důležité:

*Pokud zvolíte a spustíte **Všechna nastavení**, všechna data nastavení registrovaná ve skeneru včetně kontaktů a nastavení ověřených uživatelů budou smazána. Odstraněná nastavení nelze obnovit.*

Aktualizace aplikací a firmwaru

Aktualizováním aplikací a firmwaru lze odstranit určité potíže a vylepšit nebo přidat funkce. Používejte pouze nejaktuálnější verze aplikací a firmwaru.

Důležité:

❏ *Během aktualizace nevypínejte počítač ani skener.*

Poznámka:
*Pokud lze skener připojit k internetu, můžete firmware aktualizovat z nástroje Web Config. Vyberte kartu **Správa zařízení** > **Aktualizace firmwaru**, zkontrolujte zobrazenou zprávu a klikněte na tlačítko **Spustit**.*

1. Zkontrolujte, zda je skener připojen k počítači a zda je počítač připojen k Internetu.

2. Spusťte službu EPSON Software Updater a zaktualizujte aplikace nebo firmware.

   Poznámka:
   Operační systémy Windows Server nejsou podporovány.

   ❏ Windows 10

   Klikněte na tlačítko Start a poté vyberte **Epson Software** > **EPSON Software Updater**.

   ❏ Windows 8.1/Windows 8

   Zadejte název aplikace do ovládacího tlačítka Hledat a poté vyberte zobrazenou ikonu.

   ❏ Windows 7

   Klikněte na tlačítko Start a potom vyberte položku **Všechny programy** nebo **Programy** > **Epson Software** > **EPSON Software Updater**.

   ❏ Mac OS

   Vyberte položku **Finder** > **Přejít** > **Aplikace** > **Epson Software** > **EPSON Software Updater**.

Poznámka:
Jestliže se vám v seznamu aplikací nedaří najít aplikaci, kterou chcete aktualizovat, nebudete moci aktualizaci pomocí nástroje EPSON Software Updater provést. Vyhledejte nejnovější verze aplikací na místních webových stránkách společnosti Epson.

http://www.epson.com

Aktualizace firmwaru skeneru z ovládacího panelu

Pokud může být skener připojen k internetu, můžete aktualizovat jeho firmware z ovládacího panelu. Skener můžete též nastavit, aby pravidelně kontroloval dostupnost aktualizací firmwaru a upozornil vás, pokud jsou k dispozici.

1. Vyberte možnost **Nast.** na domovské obrazovce.

2. Vyberte možnost **Správa systému** > **Aktualizovat firmware** > **Aktualizovat**.

   Poznámka:
   *Výběrem volby **Oznámení** > **Zap.** nastavte, aby skener pravidelně kontroloval dostupnost aktualizací firmwaru.*

3. Zkontrolujte zprávu zobrazenou na obrazovce a zahajte vyhledávání dostupných aktualizací.

4. Pokud se na LCD obrazovce zobrazuje zpráva informující, že je dostupná firmwarová aktualizace, postupujte podle pokynů na obrazovce a spusťte aktualizaci.

   Důležité:
   - *V průběhu aktualizace nevypínejte ani neodpojujte skener, dokud se aktualizace nedokončí. V opačném případě se může skener porouchat.*
   - *Pokud není aktualizace firmwaru dokončena nebo je neúspěšná, skener se nespustí normálně a při příštím zapnutí skeneru je na LCD obrazovce zobrazena zpráva „Recovery Mode“. V této situaci je nutné znovu aktualizovat firmware pomocí počítače. Připojte skener k počítači pomocí USB kabelu. Dokud je na skeneru zobrazena zpráva „Recovery Mode“, nelze aktualizovat firmware prostřednictvím síťového připojení. Z počítače se připojte k místní webové stránce společnosti Epson a stáhněte nejnovější firmware skeneru. Další kroky viz pokyny na webové stránce.*

Aktualizace firmwaru pomocí Web Config

Pokud lze skener připojit k internetu, můžete firmware aktualizovat z nástroje Web Config.

1. Otevřete nástroj Web Config a vyberte kartu **Správa zařízení** > **Aktualizace firmwaru**.

2. Klikněte na možnost **Spustit** a poté postupujte podle pokynů na obrazovce.

   Spustí se potvrzení firmwaru a informace o firmwaru se zobrazí, pokud existuje aktualizovaný firmware.

Poznámka:
Firmware můžete také aktualizovat pomocí Epson Device Admin. Informace o firmwaru můžete vizuálně potvrdit na seznamu zařízení. Je to užitečné, když chcete aktualizovat firmware více zařízení. Další podrobnosti naleznete v průvodci Epson Device Admin nebo v nápovědě.

Související informace

➡ „Spuštění nástroje Web Config ve webovém prohlížeči“ na str. 35

Aktualizace firmwaru bez připojení k Internetu

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.

Poznámka:
Před aktualizací se ujistěte, že je ovladač skeneru Epson Scan 2 nainstalován na vašem počítači. Pokud není ovladač Epson Scan 2 nainstalován, nainstalujte jej znovu.

1. Navštivte stránky společnosti Epson, kde najdete nejnovější aktualizace firmwaru.

   http://www.epson.com

- ❏ Pokud jste na stránkách našli firmware pro váš skener, stáhněte ho a pokračujte k dalšímu kroku.
- ❏ Pokud jste na stránkách nenašli žádné informace ohledně firmwaru, nejspíše už používáte nejnovější firmware.

2. Připojte počítač, který obsahuje stažený firmware, ke skeneru pomocí kabelu USB.
3. Dvakrát klikněte na stažený soubor s příponou .exe.

   Spustí se aplikace Epson Firmware Updater.
4. Postupujte podle pokynů na obrazovce.