EPSON
EXCEED YOUR VISION

คู่มือผู้ดูแลระบบ

NPD5668-02 TH

เนื้อหา

ลิขสิทธิ์

เครื่องหมายการค้า

เกี่ยวกับคู่มือนี้

เครื่องหมายและสัญลักษณ์. 6
รูปอธิบายที่ใช้ในคู่มือเล่มนี้. 6
การอ้างอิงของระบบปฏิบัติการ. 6

บทนำ

องค์ประกอบของคู่มือ. 8
การกำหนดนิยามเทอมที่ใช้ในคู่มือเล่มนี้. 8

การจัดเตรียม

แผงผังการไหลของการตั้งค่าสแกนเนอร์และการจัดการ. 10
ตัวอย่างของสภาพแวดล้อมเครือข่าย. 11
การแนะนำตัวอย่างการตั้งค่าการเชื่อมต่อสแกนเนอร์. 11
การจัดเตรียมการเชื่อมต่อเข้ากับเครือข่าย. 12
การรวบรวมข้อมูลบนการตั้งค่าการเชื่อมต่อ. 12
ข้อมูลจำเพาะของสแกนเนอร์. 12
การใช้หมายเลขพอร์ต. 13
ประเภทของการกำหนดที่อยู่ IP. 13
เซิร์ฟเวอร์ DNS และพร็อกซีเซิร์ฟเวอร์. 13
วิธีการตั้งค่าการเชื่อมต่อเครือข่าย. 13

การเชื่อมต่อ

การเชื่อมต่อเข้ากับเครือข่าย. 15
การเชื่อมต่อเข้ากับเครือข่ายจากแผงควบคุม. . . . 15
การเชื่อมต่อเข้ากับเครือข่ายโดยใช้ตัวติดตั้ง. . . . 19

การตั้งค่าฟังก์ชันการทำงาน

ซอฟต์แวร์สำหรับการตั้งค่า. 22
Web Config (เว็บเพจสำหรับอุปกรณ์). 22
การใช้ฟังก์ชันสแกน. 24
การสแกนจากเครื่องคอมพิวเตอร์. 24
การสแกนโดยใช้แผงควบคุม. 26
การตั้งค่าระบบ. 28
การตั้งค่าระบบจากแผงควบคุม. 28
การตั้งค่าระบบโดยใช้ Web Config. 30

การตั้งค่าความปลอดภัยพื้นฐาน

การแนะนำคุณสมบัติความปลอดภัยพื้นฐาน. 32
การกำหนดรหัสผ่านของผู้ดูแลระบบ. 32
การกำหนดค่ารหัสผ่านผู้ดูแลระบบจากแผงควบคุม. 33
การกำหนดรหัสผ่านของผู้ดูแลระบบโดยใช้ Web Config. 33
รายการที่จะล็อคโดยรหัสผ่านของผู้ดูแลระบบ. 34
การควบคุมโปรโตคอล. 35
โปรโตคอลที่คุณสามารถเปิดใช้งานหรือปิดใช้งาน. 36
รายการการตั้งค่าโปรโตคอล. 37

การตั้งค่าการดำเนินงานและการจัดการ

ยืนยันข้อมูลของอุปกรณ์. 40
การจัดการอุปกรณ์ (Epson Device Admin). 40
การรับการแจ้งเตือนทางอีเมลเมื่อมีเหตุการ์เกิดขึ้น. . 41
เกี่ยวกับการแจ้งเตือนทางอีเมล. 41
การกำหนดค่าการแจ้งเตือนทางอีเมล. 41
การกำหนดค่าเมลเซิร์ฟเวอร์. 42
การตรวจสอบการเชื่อมต่อเมล์เซิร์ฟเวอร์. 44
การอัปเดตเฟิร์มแวร์. 46
การอัปเดตเฟิร์มแวร์โดยใช้ Web Config. 46
การอัปเดตเฟิร์มแวร์โดยใช้ Epson Firmware Updater. 46
การสำรองข้อมูลการตั้งค่า. 47
การส่งออกการตั้งค่า. 47
การนำเข้าการตั้งค่า. 47

การแก้ไขปัญหา

ข้อแนะนำสำหรับการแก้ไขปัญหา. 49
การตรวจสอบบันทึกสำหรับเซิร์ฟเวอร์และอุปกรณ์เครือข่าย. 49
การเตรียมเริ่มต้นการตั้งค่าเครือข่าย. 49
การกู้คืนการตั้งค่าเครือข่ายจากแผงควบคุม. 49
การตรวจสอบการสื่อสารระหว่างอุปกรณ์และคอมพิวเตอร์. 49
การตรวจสอบการเชื่อมต่อโดยใช้คำสั่ง Ping (ปิง) — Windows. 49
การตรวจสอบการเชื่อมต่อโดยใช้คำสั่ง Ping (ปิง) — Mac OS. 51
ปัญหาในการใช้ซอฟต์แวร์เครือข่าย. 52
ไม่สามารถเข้าถึง Web Config. 52

ชื่อรุ่นและ/หรือที่อยู่ IP ไม่แสดงผลใน EpsonNet Config. 53

ภาคผนวก

การแนะนำซอฟต์แวร์เครือข่าย. 55
Epson Device Admin. 55
EpsonNet Config. 55
EpsonNet SetupManager. 56
การกำหนดที่อยู่ IP โดยใช้ EpsonNet Config. 56
การกำหนดที่อยู่ IP โดยใช้การตั้งค่าแบบชุด. . . . 56
การกำหนดที่อยู่ IP ให้กับแต่ละอุปกรณ์. 59
การใช้พอร์ตสำหรับสแกนเนอร์. 60

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

การตั้งค่าความปลอดภัยและการป้องกันอันตราย. . . 62
การตั้งค่าคุณสมบัติความปลอดภัย. 63
การสื่อสาร SSL/TLS กับสแกนเนอร์. 63
เกี่ยวกับใบรับรองดิจิตัล. 63
การขอรับและการนำเข้าใบรับรองที่ลงนามจาก CA. 64
การลบใบรับรองที่ลงนามจาก CA. 67
การอัพเดตใบรับรองที่ลงนามด้วยตัวเอง. 68
การกำหนดค่า CA Certificate. 69
การเข้ารหัสการสื่อสารโดยใช้การกรอง IPsec/IP. . . 71
เกี่ยวกับ IPsec/IP Filtering. 71
การกำหนดค่า Default Policy. 72
การกำหนดค่า Group Policy. 75
ตัวอย่างการกำหนดค่าของ IPsec/IP Filtering. . 81
การกำหนดค่าใบรับรองสำหรับ IPsec/IP Filtering. 82
การใช้โปรโตคอล SNMPv3. 82
เกี่ยวกับ SNMPv3. 82
การกำหนดค่า SNMPv3. 83
การเชื่อมต่อสแกนเนอร์เข้ากับเครือข่าย IEEE802.1X. 84
การกำหนดค่าเครือข่าย IEEE802.1X. 84
การกำหนดค่าใบรับรองสำหรับ IEEE802.1X. . . . 86
การแก้ไขปัญหาสำหรับความปลอดภัยขั้นสูง. 87
การกู้คืนการตั้งค่าความปลอดภัย. 87
ปัญหาในการใช้คุณสมบัติความปลอดภัยของเครือข่าย. 88
ปัญหาในการใช้ใบรับรองดิจิตัล. 90

ลิขสิทธิ์

ห้ามทำซ้ำ จัดเก็บในระบบที่เรียกดูได้ หรือส่งผ่านในรูปแบบใดๆ หรือโดยวิธีการใดๆ ไม่ว่าจะเป็นทางอิเล็กทรอกนิกส์ ทางกล การถ่ายสำเนา การบันทึก หรืออื่นๆ ของส่วนหนึ่งส่วนใดของเนื้อหานี้ โดนไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจาก Seiko Epson Corporation การใช้ข้อมูลในเนื้อหานี้จะไม่เกี่ยวโยงกับความรับผิดชอบทางสิทธิบัตรใดๆ เราจะไม่รับผิดชอบใดๆ สำหรับความเสียหายที่มีผลมาจากการใช้ข้อมูลในเนื้อหานี้ ข้อมูลที่อยู่ในคู่มือนี้ได้รับการออกแบบมาเฉพาะสำหรับใช้กับผลิตภัณฑ์ Epson เท่านั้น Epson จะไม่รับผิดชอบสำหรับการใช้ข้อมูลใดๆ ไปประยุกต์ใช้กับผลิตภัณฑ์อื่น

Seiko Epson Corporation และบริษัทในเครือจะไม่รับผิดชอบใดๆ ต่อผู้ซื้อผลิตภัณฑ์นี้สำหรับความเสียหาย การสูญเสีย ค่าใช้จ่าย ต้นทุน หรือค่าใช้จ่ายที่เกิดขึ้นของผู้ซื้อหรือบุคคลที่สามที่เป็นผลมาจากอุบัติเหตุ การใช้งานไม่ถูกต้องตามวัตถุประสงค์ หรือการใช้ในทางที่ผิดของผลิตภัณฑ์นี้ หรือการดัดแปลงแก้ไข ซ่อมแแซม หรือแปลงผลิตภัณฑ์นี้โดยไม่ได้รับอนุญาต หรือ (ไม่รวมในประเทศสหรัฐอเมริกา) ไม่สามารถปฏิบัติตามคำแนะนำในการใช้งานและการบำรุงรักษาของ Seiko Epson Corporation อย่างเข้มงวด

Seiko Epson Corporation และบริษัทในเครือจะไม่รับผิดชอบสำหรับความเสียหาย หรือปัญหาใดๆ ที่เกิดขึ้นจากการใช้ตัวเลือกใดๆ หรือผลิตภัณฑ์สิ้นเปลืองใดๆ นอกเหนือจากที่ได้กำหนดว่าเป็นผลิตภัณฑ์เดิมของ Epson หรือผลิตภัณฑ์ที่ผ่านการรับรองของ Epson จาก Seiko Epson Corporation

Seiko Epson Corporation จะไม่ถือเป็นความรับผิดชอบสำหรับความเสียหายใๆ ที่มีผลมาจากการรบกวนทางแม่เหล็กไฟฟ้าที่เกิดขึ้นจากการใช้งานสายอินเทอร์เฟสใดๆ ที่นอกเหนือจากที่ได้กำหนดว่าเป็นผลิตภัณฑ์ที่ผ่านการรับรองของ Epson จาก Seiko Epson Corporation

©Seiko Epson Corporation 2019

เนื้อหาของคู่มือเล่มนี้ และข้อมูลจำเพาะของผลิตภัณฑ์นี้สามารถเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ

เครื่องหมายการค้า

- EPSON® เป็นเครื่องหมายการค้าจดทะเบียน และ EPSON EXCEED YOUR VISION หรือ EXCEED YOUR VISION เป็นเครื่องหมายการค้าของ Seiko Epson Corporation
- Epson Scan 2 software is based in part on the work of the Independent JPEG Group.
- Google Cloud Print™, Chrome™, Chrome OS™, and Android™ are trademarks of Google Inc.
- Microsoft®, Windows®, Windows Server®, and Windows Vista® are registered trademarks of Microsoft Corporation.
- Apple, Macintosh, Mac OS, OS X, AirMac, Bonjour, and Safari are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc.
- ประกาศแจ้งทั่วไป: ชื่อผลิตภัณฑ์อื่นๆ ที่ใช้ในที่นี้สำหรับวัตถุประสงค์การบ่งชี้เท่านั้น และไม่ได้เป็นเครื่องหมายการค้าของเจ้าของผลิตภัณฑ์แต่ละราย Epson ไม่ได้รับผิดชอบสิทธิ์ใดๆ หรือทั้งหมดของเครื่องหมายเหล่านั้น

เกี่ยวกับคู่มือนี้

เครื่องหมายและสัญลักษณ์

ข้อควรระวัง:
คำแนะนำที่จะต้องทำตามอย่างระมัดระวังเพื่อหลีกเลี่ยงการได้รับบาดเจ็บ

ข้อความที่สำคัญ:
คำแนะนำที่จะต้องสังเกตเพื่อหลีกเลี่ยงความเสียหายต่ออุปกรณ์ของคุณ

หมายเหตุ:
คำแนะนำที่ประกอบด้วยข้อแนะนำที่มีประโยชน์และข้อจำกัดในการทำงานของสแกนเนอร์

ข้อมูลที่เกี่ยวข้อง

➡ คลิกที่ไอคอนนี้จะนำพาคุณไปยังข้อมูลที่เกี่ยวข้อง

รูปอธิบายที่ใช้ในคู่มือเล่มนี้

❑ ภาพหน้าจอของไดรฟ์เวอร์สแกนเนอร์และ หน้าจอ Epson Scan 2 (ไดรฟ์เวอร์สแกนเนอร์) มาจาก Windows 10 หรือ OS X El Capitan เนื้อหาที่แสดงบนหน้าจอจะแปรผันไปโดยขึ้นอยู่กับรุ่นและสถานการณ์

❑ ภาพตัวอย่างที่ใช้ในคู่มือนี้เป็นตัวอย่างเท่านั้น แม้ว่าจะมีความแตกต่างเล็กน้อยขึ้นอยู่กับรุ่น แต่วิธีการทำงานเหมือนกัน

❑ บางรายการเมนูบนหน้าจอ LCD จะแปรผันโดยขึ้นอยู่กับรุ่นและการตั้งค่า

การอ้างอิงของระบบปฏิบัติการ

Windows

ในคู่มือนี้ คำศัพท์ เช่น "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Vista", "Windows XP", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", "Windows Server 2008 R2", "Windows Server 2008", "Windows Server 2003 R2" และ "Windows Server 2003" หมายถึงระบบปฏิบัติการต่อไปนี้ นอกจากนั้นแล้ว "Windows" ถูกใช้สำหรับอ้างถึงทุกเวอร์ชั่น

❑ ระบบปฏิบัติการ Microsoft® Windows® 10

❑ ระบบปฏิบัติการ Microsoft® Windows® 8.1

❑ ระบบปฏิบัติการ Microsoft® Windows® 8

❑ ระบบปฏิบัติการ Microsoft® Windows® 7

❑ ระบบปฏิบัติการ Microsoft® Windows Vista®

❑ ระบบปฏิบัติการ Microsoft® Windows® XP

เกี่ยวกับคู่มือนี้

- ❑ ระบบปฏิบัติการ Microsoft® Windows® XP Professional x64 Edition
- ❑ ระบบปฏิบัติการ Microsoft® Windows Server® 2016
- ❑ ระบบปฏิบัติการ Microsoft® Windows Server® 2012 R2
- ❑ ระบบปฏิบัติการ Microsoft® Windows Server® 2012
- ❑ ระบบปฏิบัติการ Microsoft® Windows Server® 2008 R2
- ❑ ระบบปฏิบัติการ Microsoft® Windows Server® 2008
- ❑ ระบบปฏิบัติการ Microsoft® Windows Server® 2003 R2
- ❑ ระบบปฏิบัติการ Microsoft® Windows Server® 2003

Mac OS

ในคู่มือนี้ "Mac OS" ถูกใช้ในการอ้างถึง macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x และ Mac OS X v10.6.8

บทนำ

องค์ประกอบของคู่มือ

คู่มือนี้เป็นคู่มือสำหรับผู้ดูแลระบบที่รับผิดชอบสำหรับการเชื่อมต่อเครื่องพิมพ์หรือสแกนเนอร์เข้ากับเครือข่าย และมีข้อมูลเกี่ยวกับวิผะการตั้งค่าเพื่อใช้งานฟังก์ชันต่าง ๆ

ดูข้อมูลฟังก์ชันการใช้งานได้ที่ *คู่มือผู้ใช้*

การจัดเตรียม

อธิบายงานของผู้ดูแลระบบ วิธีการตั้งค่าอุปกรณ์ และซอฟต์แวร์เพื่อการจัดการ

การเชื่อมต่อ

อธิบายวิธีการเชื่อมต่ออุปกรณ์เข้ากับเครือข่ายหรือสายโทรศัพท์ นอกจากนี้ ยังอธิบายสภาพแวดล้อมเครือข่าย เช่น การใช้พอร์ตสำหรับอุปกรณ์ ข้อมูลเซิร์ฟเวอร์ DNS และพร็อกซีเซิร์ฟเวอร์

การตั้งค่าฟังก์ชันการทำงาน

อธิบายการตั้งค่าแต่ละฟังก์ชันของอุปกรณ์

การตั้งค่าความปลอดภัยพื้นฐาน

อธิบายการตั้งค่าของแต่ละฟังก์ชัน เช่น การพิมพ์ การสแกน และการแฟกซ์

การตั้งค่าการดำเนินงานและการจัดการ

อธิบายการดำเนินงานหลังจากเริ่มใช้งานอุปกรณ์ เช่น การตรวจสอบข้อมูลและการดูแลรักษา

การแก้ไขปัญหา

อธิบายการเตรียมเริ่มต้นการตั้งค่าและการแก้ไขปัญหาของเครือข่าย

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

อธิบายวิธีการตั้งค่าเพื่อเพิ่มขีดความสามารถความปลอดภัยของอุปกรณ์ เช่น การใช้ใบรับรอง CA การสื่อสาร SSL/TLS และการกรอง IPsec/IP

ทั้งนี้ขึ้นอยู่กับรุ่น บางฟังก์ชันในบทนี้อาจไม่รองรับ

การกำหนดนิยามเทอมที่ใช้ในคู่มือเล่มนี้

เทอมต่อไปนี้ถูกใช้ในคู่มือเล่มนี้

ผู้ดูแลระบบ

บุคคลที่รับผิดชอบสำหรับการติดตั้งและการตั้งค่าอุปกรณ์หรือเครือข่ายที่สำนักงานหรือองค์กร สำหรับองค์กรขนาดเล็ก บุคคลนี้อาจรับผิดชอบทั้งการดูแลระบบอุปกรณ์และเครือข่าย สำหรับองค์กรขนาดใหญ่ ผู้ดูแลระบบมีอำนาจในการควบคุมดูแลเครือข่ายหรืออุปกรณ์ของชุดกลุ่มของแผนกหรือฝ่าย และผู้ดูแลระบบเครือข่ายจะรับผิดชอบในการตั้งค่าการสื่อสารสำหรับองค์กรข้างต้น เช่น อินเทอร์เน็ต

บทนำ

ผู้ดูแลระบบเครือข่าย

บุคคลที่รับผิดชอบสำหรับการควบคุมการสื่อสารผ่านเครือข่าย บุคคลที่ตั้งค่าเราเตอร์ พร็อกซีเซิร์ฟเวอร์ เซิร์ฟเวอร์ DNS และเมลเซิร์ฟเวอร์เพื่อควบคุมการสื่อสารผ่านอินเทอร์เน็ตหรือเครือข่าย

ผู้ใช้

บุคคลที่ใช้งานอุปกรณ์ เช่น เครื่องพิมพ์หรือสแกนเนอร์

Web Config(เว็บเพจของอุปกรณ์)

เว็บเซิร์ฟเวอร์ที่สร้างขึ้นในอุปกรณ์ เรียกว่า Web Config คุณสามารถตรวจสอบและเปลี่ยนสถานะของอุปกรณ์โดยใช้เบราว์เซอร์

เครื่องมือ

เทอมทั่วไปสำหรับซอฟต์แวร์เพื่อตั้งค่าหรือจัดการอุปกรณ์ เช่น Epson Device Admin, EpsonNet Config, EpsonNet SetupManager ฯลฯ

สแกนแบบดัน

เทอมทั่วไปสำหรับการสแกนจากแผงควบคุมของอุปกรณ์

ASCII (รหัสมาตรฐานอเมริกันสำหรับการแลกเปลี่ยนระหว่างกันของข้อมูล)

หนึ่งในรหัสตัวอักขระมาตรฐาน กำหนดไว้ที่ 128 ตัวอักขระ รวมทั้งตัวอักขระที่เป็นตัวอักษร (a–z, A–Z) ตัวเลขอาระบิก (0–9) สัญลักษณ์ ตัวอักขระว่าง และตัวอักขระควบคุม เมื่อ "ASCII" มีอธิบายไว้ในคู่มือนี้ หมายถึง 0x20–0x7E (ตัวเลขแปดหลัก) ที่แสดงรายการด้านล่าง และไม่เกี่ยวข้องกับตัวอักขระควบคุม

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

* ตัวอักขระเว้นว่าง

Unicode (UTF-8)

รหัสมาตรฐานระหว่างประเทศ ครอบคลุมภาษาระดับสากลหลัก เมื่อ "UTF-8" ได้อธิบายไว้ในคู่มือนี้ เป็นการระบุตัวอักขระรหัสในรูปแบบ UTF-8

การจัดเตรียม

บทนี้อธิบายบทบาทของผู้ดูแลระบบและการจัดเตรียมก่อนทำการตั้งค่า

แผงผังการไหลของการตั้งค่าสแกนเนอร์และการจัดการ

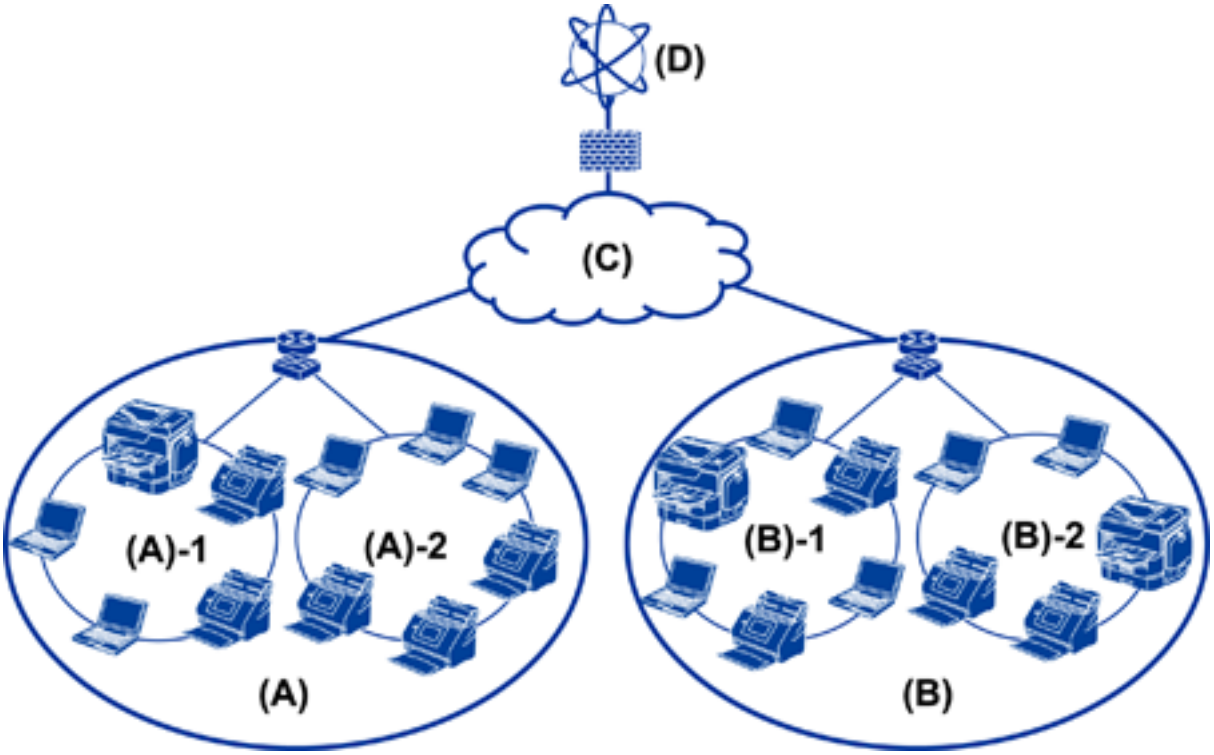
ผู้ดูแลระบบสามารถทำการตั้งค่าการเชื่อมต่อเครือข่าย การตั้งค่าแรกเริ่มและการบำรุงรักษาสแกนเนอร์ เพื่อให้พร้อมใช้งานสำหรับผู้ใช้

1. การจัดเตรียม
   - ❑ รวบรวมข้อมูลการตั้งค่าการเชื่อมต่อ
   - ❑ ตัดสินใจวิธีการเชื่อมต่อ
2. การเชื่อมต่อ
   - ❑ การเชื่อมต่อเครือข่ายจากแผงควบคุมของสแกนเนอร์
3. การตั้งค่าฟังก์ชันการทำงาน
   - ❑ การตั้งค่าไดรฟ์เวอร์สแกนเนอร์
   - ❑ การตั้งค่าขั้นสูงอื่น ๆ
4. การตั้งค่าความปลอดภัย
   - ❑ การตั้งค่าผู้ดูแลระบบ
   - ❑ SSL/TLS
   - ❑ การควบคุมโปรโตคอล
   - ❑ การตั้งค่าความปลอดภัยขั้นสูง (เผื่อเลือก)
5. การดำเนินการและการจัดการ
   - ❑ การตรวจสอบสถานะของอุปกรณ์
   - ❑ การจัดการเหตุการณ์ฉุกเฉิน
   - ❑ การสำรองข้อมูลการตั้งค่าอุปกรณ์

ข้อมูลที่เกี่ยวข้อง

➡ "การจัดเตรียม" บนหน้าที่ 10
➡ "การเชื่อมต่อ" บนหน้าที่ 15
➡ "การตั้งค่าฟังก์ชันการทำงาน" บนหน้าที่ 22
➡ "การตั้งค่าความปลอดภัยพื้นฐาน" บนหน้าที่ 32
➡ "การตั้งค่าการดำเนินงานและการจัดการ" บนหน้าที่ 40

ตัวอย่างของสภาพแวดล้อมเครือข่าย



(A): สำนักงาน 1

❏ (A) – 1: LAN 1

❏ (A) – 2: LAN 2

(B): สำนักงาน 2

❏ (B) – 1: LAN 1

❏ (B) – 2: LAN 2

(C): WAN

(D): อินเทอร์เน็ต

การแนะนำตัวอย่างการตั้งค่าการเชื่อมต่อสแกนเนอร์

มีการเชื่อมต่อหลักๆ 2 ประเภทโดยขึ้นอยู่กับวิธีการใช้สแกนเนอร์ ทั้งสองแบบเชื่อมต่อสแกนเนอร์เข้ากับเครือข่ายโดยใช้คอมพิวเตอร์ผ่านฮับ

❏ การเชื่อมต่อเซิร์ฟเวอร์/ไคลเอ็นต์ (สแกนเนอร์โดยใช้เซิร์ฟเวอร์ Windows การจัดการงาน)

❏ การเชื่อมต่อแบบเพียร์ทูเพียร์ (การเชื่อมต่อโดยตรงโดยคอมพิวเตอร์ไคลเอ็นต์)

ข้อมูลที่เกี่ยวข้อง

➡ "การเชื่อมต่อเซิร์ฟเวอร์/ไคลเอ็นต์" บนหน้าที่ 12

➡ "การเชื่อมต่อแบบเพียร์ทูเพียร์" บนหน้าที่ 12

การเชื่อมต่อเซิร์ฟเวอร์/ไคลเอ็นต์

รวมศูนย์การจัดการสแกนเนอร์และงานด้วย Document Capture Pro Server ที่ติดตั้งไว้บนเซิร์ฟเวอร์ เหมาะที่สุดสำหรับการทำงานที่ใช้สแกนเนอร์หลายเครื่องเพื่อสแกนเอกสารจำนวนมากในบางรูปแบบ

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดนิยามเทอมที่ใช้ในคู่มือเล่มนี้" บนหน้าที่ 8

การเชื่อมต่อแบบเพียร์ทูเพียร์

ใช้สแกนเนอร์แต่ละเครื่องที่มีไดร์เวอร์สแกนเนอร์ เช่น Epson Scan 2 ติดตั้งไว้บนคอมพิวเตอร์ไคลเอ็นต์ การติดตั้ง Document Capture Pro (Document Capture) บนคอมพิวเตอร์ไคลเอ็นต์ช่วยให้คุณสามารถเรียกทำงานบนบนคอมพิวเตอร์ไคลเอ็นต์แต่ละเครื่องได้

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดนิยามเทอมที่ใช้ในคู่มือเล่มนี้" บนหน้าที่ 8

การจัดเตรียมการเชื่อมต่อเข้ากับเครือข่าย

การรวบรวมข้อมูลบนการตั้งค่าการเชื่อมต่อ

คุณจะต้องมีที่อยู่ IP ที่อยู่เกตเวย์ ฯลฯ สำหรับการเชื่อมต่อเครือข่าย ตรวจสอบรายการต่อไปนี้ล่วงหน้า

แผนก	รายการ	หมายเหตุ
วิธีการเชื่อมต่ออุปกรณ์	❑ อีเธอร์เน็ต	ใช้สาย STP ประเภท 5e หรือสูงกว่า (คู่บิดวนมีชั้นป้องกัน) สำหรับการเชื่อมต่ออีเธอร์เน็ต
ข้อมูลการเชื่อมต่อ LAN	❑ ที่อยู่ IP ❑ ซับเน็ตมาสก์ ❑ เกตเวย์ค่าเริ่มต้น	หากคุณตั้งค่าที่อยู่ IP โดยอัตโนมัติโดยใช้ฟังก์ชัน DHCP ของเราเตอร์ ก็ไม่จำเป็น
ข้อมูลเซิร์ฟเวอร์ DNS	❑ ที่อยู่ IP สำหรับ DNS หลัก ❑ ที่อยู่ IP สำหรับ DNS สำรอง	หากคุณใช้ที่อยู่ IP แบบคงที่เป็นที่อยู่ IP ให้กำหนดค่าเซิร์ฟเวอร์ DNS กำหนดค่าเมื่อกำหนดโดยอัตโนมัติโดยใช้ฟังก์ชัน DHCP และเมื่อเซิร์ฟเวอร์ DNS ไม่สามารถถูกกำหนดค่าโดยอัตโนมัติ
ข้อมูลพร็อกซีเซิร์ฟเวอร์	❑ ชื่อพร็อกซีเซิร์ฟเวอร์ ❑ หมายเลขพอร์ต	กำหนดค่าเมื่อใช้พร็อกซีเซิร์ฟเวอร์สำหรับการเชื่อมต่ออินเทอร์เน็ต และเมื่อใช้บริการ Epson Connect หรือฟังก์ชันการอัปเดตอัตโนมัติของเฟิร์มแวร์

ข้อมูลจำเพาะของสแกนเนอร์

ข้อมูลจำเพาะที่สแกนเนอร์รองรับมาตรฐานหรือโหมดการเชื่อมต่อ สามารถดูที่ *คู่มือผู้ใช้*

การใช้หมายเลขพอร์ต

ดูที่ "ภาคผนวก" สำหรับหมายเลขพอร์ตที่สแกนเนอร์ใช้

ข้อมูลที่เกี่ยวข้อง

➡ "การใช้พอร์ตสำหรับสแกนเนอร์" บนหน้าที่ 60

ประเภทของการกำหนดที่อยู่ IP

มี 2 ประเภทสำหรับการกำหนดที่อยู่ IP ให้กับสแกนเนอร์

การกำหนดที่อยู่ IP แบบคงที่

กำหนดที่อยู่ IP แบบไม่ซ้ำกันล่วงหน้าให้กับสแกนเนอร์

ที่อยู่ IP จะไม่เปลี่ยนแม้ว่าจะปิดสแกนเนอร์หรือเราเตอร์ก็ตาม ดังนั้นคุณสามารถจัดการอุปกรณ์ด้วยที่อยู่ IP ได้

ประเภทนี้เหมาะสำหรับเครือข่ายที่มีหลายสแกนเนอร์ที่ต้องจัดการ เช่น สำนักงานหรือโรงเรียนขนาดใหญ่

การกำหนดค่าโดยอัตโนมัติด้วยฟังก์ชัน DHCP:

ที่อยู่ IP ที่ถูกต้องจะถูกกำหนดโดยอัตโนมัติเมื่อมีการสื่อสารระหว่างสแกนเนอร์และเราเตอร์ที่รองรับการทำงานของฟังก์ชัน DHCP

หากไม่สะดวกที่จะเปลี่ยนแปลงที่อยู่ IP สำหรับบางอุปกรณ์ ให้จองที่อยู่ IP ล่วงหน้า จากนั้นกำหนดค่า

เซิร์ฟเวอร์ DNS และพร็อกซีเซิร์ฟเวอร์

หากคุณใช้บริการการเชื่อมต่อผ่านอินเทอร์เน็ต ให้กำหนดค่าเซิร์ฟเวอร์ DNS หากคุณไม่ได้กำหนดค่านี้ คุณจะต้องระบุที่อยู่ IP สำหรับการเข้าถึงเนื่องจากคุณอาจไม่สามารถแก้ไขปัญหาชื่อได้

พร็อกซีเซิร์ฟเวอร์ถูกกำหนดที่เกตเวย์ระหวางเครือข่ายและอินเทอร์เน็ต และทำการสื่อสารไปยังคอมพิวเตอร์ สแกนเนอร์ และอินเทอร์เน็ต (เซิร์ฟเวอร์ฝั่งตรงข้าม) ในนามของแต่ละฝ่าย เซิร์ฟเวอร์ฝั่งตรงข้ามสื่อสารเฉพาะไปยังพร็อกซีเซิร์ฟเวอร์เท่านั้น ดังนั้น ข้อมูลของสแกนเนอร์ เช่น ที่อยู่ IP และหมายเลขพอร์ตจะไม่สามารถอ่าน และมีความปลอดภัยเพิ่มขึ้น

คุณสามารถห้ามการเข้าถึงไปยัง URL เฉพาะ โดยการใช้ฟังก์ชันการกรอง เนื่องจากพร็อกซีเซิร์ฟเวอร์สามารถตรวจสอบเนื้อหาของการสื่อสารได้

วิธีการตั้งค่าการเชื่อมต่อเครือข่าย

สำหรับการตั้งค่าการเชื่อมต่อสำหรับที่อยู่ IP ของสแกนเนอร์ ซับเน็ตมาสก์ และเกตเวย์เริ่มต้น ให้ดำเนินการต่อไปนี้

การใช้แผงควบคุม

กำหนดการตั้งค่าโดยใช้แผงควบคุมของสแกนเนอร์สำหรับสแกนเนอร์แต่ละเครื่อง เชื่อมต่อเข้ากับเครือข่ายหลังจากกำหนดการตั้งค่าการเชื่อมต่อของสแกนเนอร์แล้ว

การใช้ตัวติดตั้ง

หากใช้งานตัวติดตั้ง เครือข่ายของสแกนเนอร์และคอมพิวเตอร์ไคลเอ็นต์จะถูกตั้งค่าโดยอัตโนมัติ การตั้งค่าสามารถใช้ได้โดยทำตามคำแนะนำของตัวติดตั้ง แม้ว่าจะไม่มีความรู้เชิงลึกในระบบเครือข่ายก็ตาม

การจัดเตรียม

การใช้เครื่องมือ

ใช้เครื่องมือจากคอมพิวเตอร์ของผู้ดูแลระบบ คุณสามารถค้นหาเครื่องพิมพ์ จากนั้นตั้งค่าสแกนเนอร์ หรือสร้างไฟล์ SYLK เพื่อทำการตั้งค่าแบบชุดให้กับสแกนเนอร์ คุณสามารถตั้งค่าได้หลายสแกนเนอร์ แต่สแกนเนอร์เหล่านั้นจะต้องเชื่อมต่อทางกายภาพด้วยสายอีเธอร์เน็ตก่อนทำการตั้งค่า ดังนั้น เราขอแนะนำให้ใช้หากคุณมีอีเธอร์เน็ตสำหรับการตั้งค่า

ข้อมูลที่เกี่ยวข้อง

➡ "การเชื่อมต่อเข้ากับเครือข่ายจากแผงควบคุม" บนหน้าที่ 15

➡ "การเชื่อมต่อเข้ากับเครือข่ายโดยใช้ตัวติดตั้ง" บนหน้าที่ 19

➡ "การกำหนดที่อยู่ IP โดยใช้ EpsonNet Config" บนหน้าที่ 56

การเชื่อมต่อ

บทนี้อธิบายสภาพแวดล้อมหรือขั้นตอนในการเชื่อมต่อสแกนเนอร์เข้ากับเครือข่าย

การเชื่อมต่อเข้ากับเครือข่าย

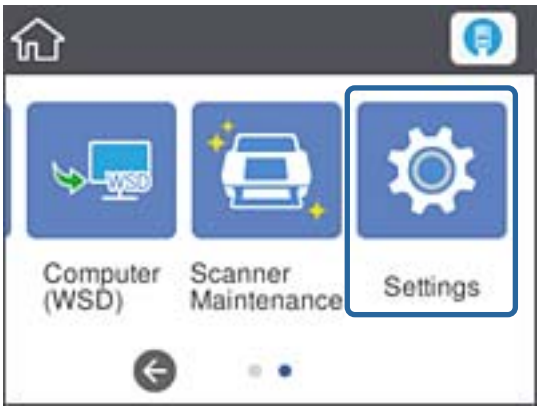
การเชื่อมต่อเข้ากับเครือข่ายจากแผงควบคุม

เชื่อมต่อสแกนเนอร์เข้ากับเครือข่ายโดยใช้แผงควบคุมของสแกนเนอร์
สำหรับแผงควบคุมของสแกนเนอร์ ให้ดูรายละเอียดเพิ่มเติมที่ *คู่มือผู้ใช้*

การกำหนดที่อยู่ IP

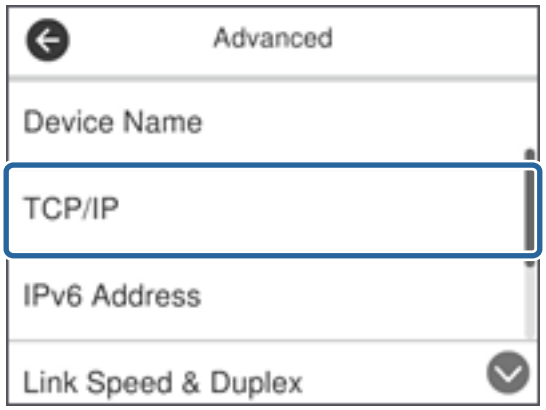
ตั้งค่ารายการพื้นฐาน เช่น ที่อยู่ IP, ซับเน็ตมาสก์ และ เกตเวย์เริ่มต้น

1. เปิดสแกนเนอร์
2. ตวัดหน้าจอไปด้านซ้ายบนแผงควบคุมสแกนเนอร์ จากนั้นแตะ **การตั้งค่า**

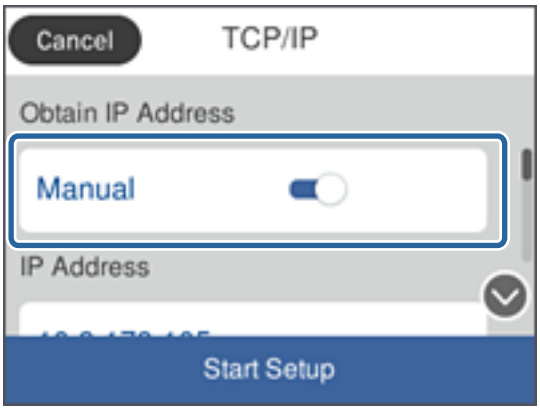


3. แตะที่ **การตั้งค่าเครือข่าย** > **เปลี่ยนการตั้งค่า**
   หากรายการไม่แสดงขึ้นมา ให้ตวัดหน้าจอขึ้นบนเพื่อแสดง

4. แตะที่ **TCP/IP**

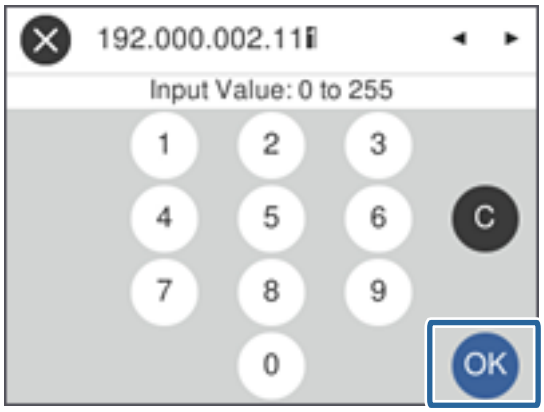


5. เลือก **กำหนดเอง** สำหรับ **รับ IP แอดเดรส**



หมายเหตุ:
*เมื่อคุณตั้งค่าที่อยู่ IP โดยอัตโนมัติโดยใช้ฟังก์ชัน DHCP ของเราเตอร์ ให้เลือก **อัตโนมัติ** ในกรณีดังกล่าว **ที่อยู่ IP**, **ซับเน็ตมาสก์** และ **เกตเวย์เริ่มต้น** จากขั้นตอนที่ 6 ถึง 7 ก็ยังถูกตั้งค่าโดยอัตโนมัติด้วย ให้ไปที่ขั้นตอนที่ 8*

6. แตะที่ช่อง **ที่อยู่ IP** กรอกที่อยู่ IP โดยใช้แป้นพิมพ์ที่แสดงบนหน้าจอ จากนั้นแตะ **ตกลง**



ยืนยันค่าที่ปรากฏบนหน้าจอ

7. ตั้งค่า **ซับเน็ตมาสก์** และ **เกตเวย์เริ่มต้น**

ยืนยันค่าที่ปรากฏบนหน้าจอ

หมายเหตุ:
*หากการผสมกันของ ที่อยู่ IP, ซับเน็ตมาสก์ และ เกตเวย์เริ่มต้น ไม่ถูกต้อง **เริ่มการตั้งค่า** จะไม่ทำงาน และไม่สามารถดำเนินการต่อกับการตั้งค่า ตรวจยืนยันว่าไม่มีข้อผิดพลาดในรายการ*

8. แตะที่ช่อง **DNS หลัก** สำหรับ **เซิร์ฟเวอร์ DNS** กรอกที่อยู่ IP สำหรับเซิร์ฟเวอร์ DNS หลักโดยใช้แป้นพิมพ์ที่แสดงบนหน้าจอ จากนั้นแตะ **ตกลง**

   ยืนยันค่าที่ปรากฏบนหน้าจอ

   หมายเหตุ:
   *เมื่อคุณเลือก **อัตโนมัติ** สำหรับการกำหนดค่าที่อยู่ IP คุณสามารถเลือกการตั้งค่าเซิร์ฟเวอร์ DNS จาก **กำหนดเอง** หรือ **อัตโนมัติ** หากคุณไม่สามารถได้รับที่อยู่ของเซิร์ฟเวอร์ DNS โดยอัตโนมัติ ให้เลือก **กำหนดเอง** และป้อนที่อยู่เซิร์ฟเวอร์ DNS จากนั้น ป้อนที่อยู่เซิร์ฟเวอร์ DNS สำรองได้โดยตรง หากคุณเลือก **อัตโนมัติ** ให้ไปที่ขั้นตอนที่ 10*

9. แตะที่ช่อง **DNS รอง** กรอกที่อยู่ IP สำหรับเซิร์ฟเวอร์ DNS สำรองโดยใช้แป้นพิมพ์ที่แสดงบนหน้าจอ จากนั้นแตะ **ตกลง**

   ยืนยันค่าที่ปรากฏบนหน้าจอ

10. แตะที่ **เริ่มการตั้งค่า**

11. แตะ **ปิด** จากหน้าจอยืนยัน

    หน้าจอจะปิดโดยอัตโนมัติหลังจากผ่านระยะเวลาหนึ่ง หากคุณไม่ได้แตะ **ปิด**

การเชื่อมต่อเข้ากับอีเธอร์เน็ต

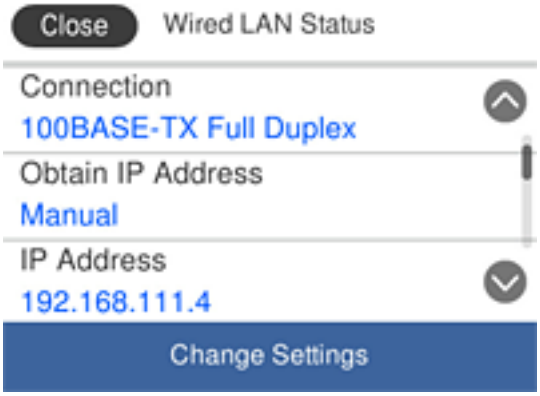
เชื่อมต่อสแกนเนอร์เข้ากับเครือข่ายโดยใช้สายอีเธอร์เน็ต และตรวจสอบการเชื่อมต่อ

1. เชื่อมต่อสแกนเนอร์และฮับ (สวิตช์ L2) ด้วยสายอีเธอร์เน็ต

   ไอคอนบนหน้าจอหลักเปลี่ยนแปลงเป็น

2. แตะ บนหน้าจอหลัก

3. ปิดหน้าจอขึ้น จากนั้นตรวจสอบว่าสถานะการเชื่อมต่อและที่อยู่ IP ถูกต้อง



การตั้งค่าพร็อกซีเซิร์ฟเวอร์

พร็อกซีเซิร์ฟเวอร์ไม่สามารถตั้งค่าบนแผงควบคุม กำหนดค่าโดยใช้ Web Config

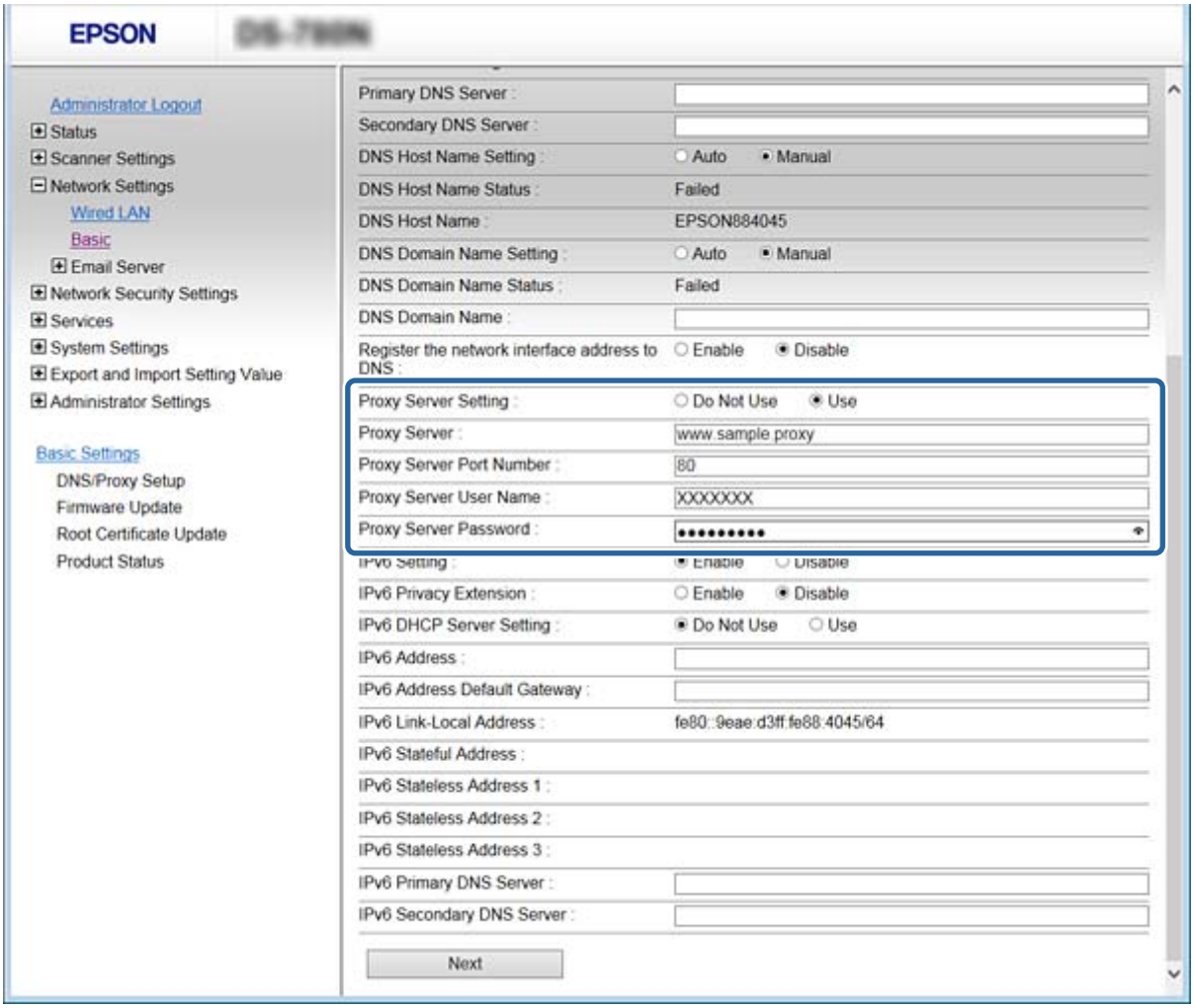
1. เข้าถึง Web Config แล้วเลือก **Network Settings** > **Basic**

2. เลือก **Use** ใน **Proxy Server Setting**

3. ระบุพร็อกซีเซิร์ฟเวอร์ในที่อยู่ IPv4 หรือรูปแบบ FQDN ใน **พร็อกซี่เซิร์ฟเวอร์** จากนั้นป้อนหมายเลขพอร์ตใน **Proxy Server Port Number**

   สำหรับพร็อกซีเซิร์ฟเวอร์ที่จำเป็นต้องตรวจรับรองความถูกต้อง ให้ป้อนชื่อผู้ใช้การตรวจรับรองความถูกต้องพร็อกซีเซิร์ฟเวอร์ และรหัสผ่านการตรวจรับรองความถูกต้องพร็อกซีเซิร์ฟเวอร์

4. คลิกปุ่ม **Next**



5. ยืนยันการตั้งค่า จากนั้น คลิกที่ **การตั้งค่า**

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การเชื่อมต่อเข้ากับเครือข่ายโดยใช้ตัวติดตั้ง

เราแนะนำให้ใช้ตัวติดตั้งเพื่อเชื่อมต่อสแกนเนอร์เข้ากับคอมพิวเตอร์ คณสามารถเรียกใช้ตัวติดตั้งโดยใช้วิธีหนึ่งใดต่อไปนี้

❑ การตั้งค่าจากเว็บไซต์

เข้าไปยังเว็บไซต์ดังต่อไปนี้ จากนั้นป้อนชื่อผลิตภัณฑ์เข้าไป ไปที่ **การตั้งค่า** จากนั้นเริ่มการตั้งค่า

http://epson.sn

❑ การตั้งค่าโดยใช้แผ่นดิสก์ซอฟต์แวร์ (เฉพาะสำหรับรุ่นที่มาพร้อมกับแผ่นดิสก์ซอฟต์แวร์ และผู้ใช้ที่มีคอมพิวเตอร์ที่มีดิสก์ไดรฟ์)

ใส่แผ่นดิสก์ซอฟต์แวร์เข้าไปในคอมพิวเตอร์ จากนั้นทำตามคำแนะนำบนหน้าจอ

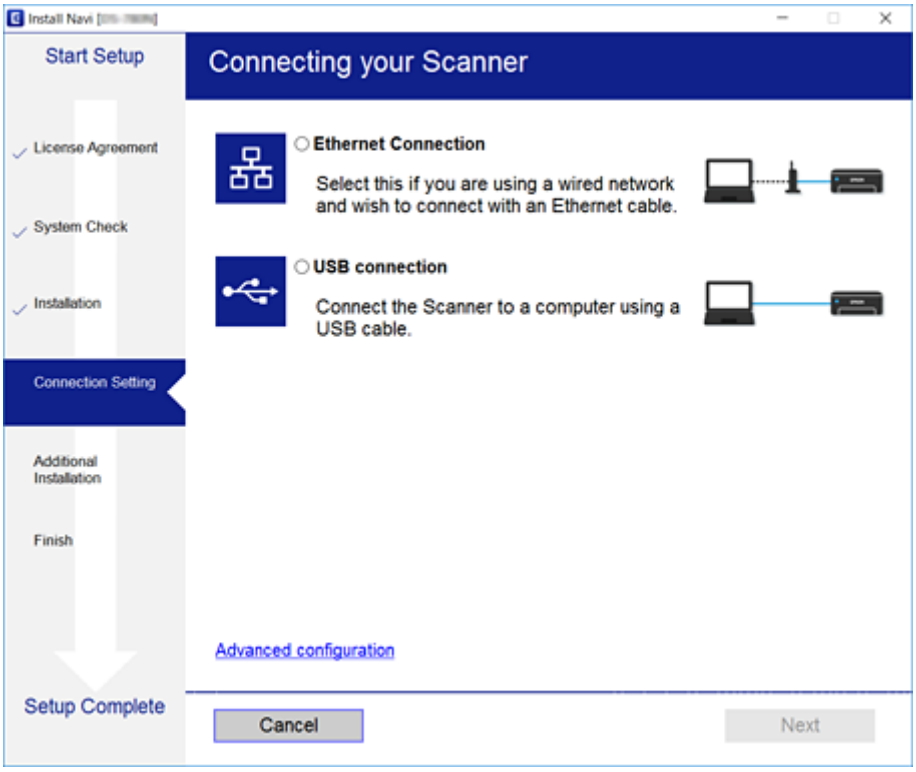
การเชื่อมต่อ

การเลือกวิธีการเชื่อมต่อ

ทำตามคำแนะนำบนหน้าจอจนกว่าหน้าจอต่อไปนี้จะปรากฏขึ้น จากนั้นเลือกวิธีการเชื่อมต่อสแกนเนอร์เข้ากับคอมพิวเตอร์

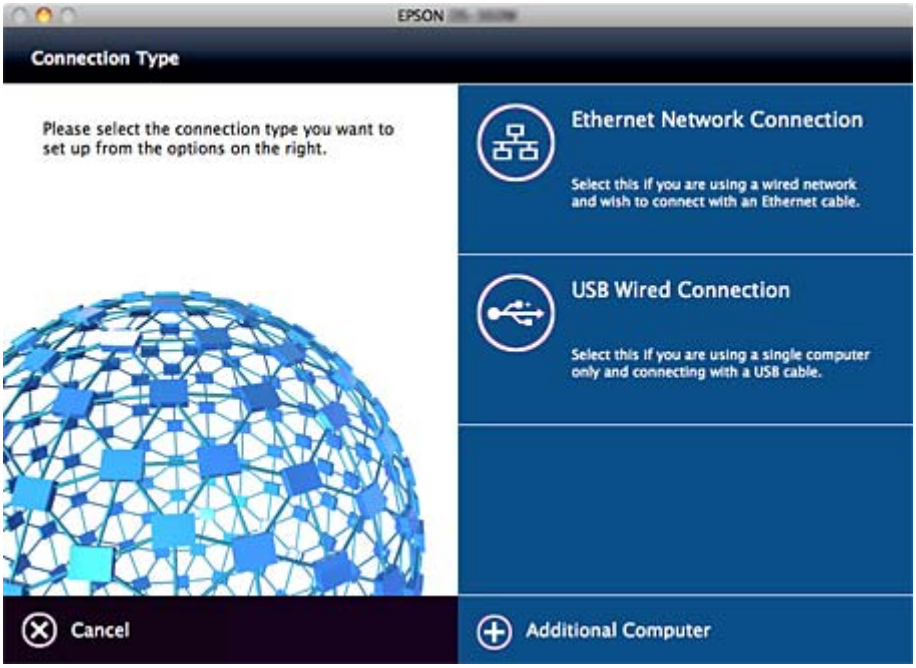
❑ Windows

เลือกประเภทการเชื่อมต่อ จากนั้นคลิก **ถัดไป**



❑ Mac OS

เลือกประเภทการเชื่อมต่อ



การเชื่อมต่อ

ทำตามคำแนะนำบนหน้าจอ ซอฟต์แวร์ที่จำเป็นได้รับการติดตั้ง

การตั้งค่าฟังก์ชันการทำงาน

บทนี้อธิบายการตั้งค่าอันดับแรกเพื่อที่จะใช้งานแต่ละฟังก์ชันของอุปกรณ์

ซอฟต์แวร์สำหรับการตั้งค่า

ในหัวข้อนี้ เป็นขั้นตอนสำหรับการตั้งค่าจากคอมพิวเตอร์ของผู้ดูแลระบบโดยใช้ Web Config ที่ได้อธิบายไว้

Web Config (เว็บเพจสำหรับอุปกรณ์)

เกี่ยวกับ Web Config

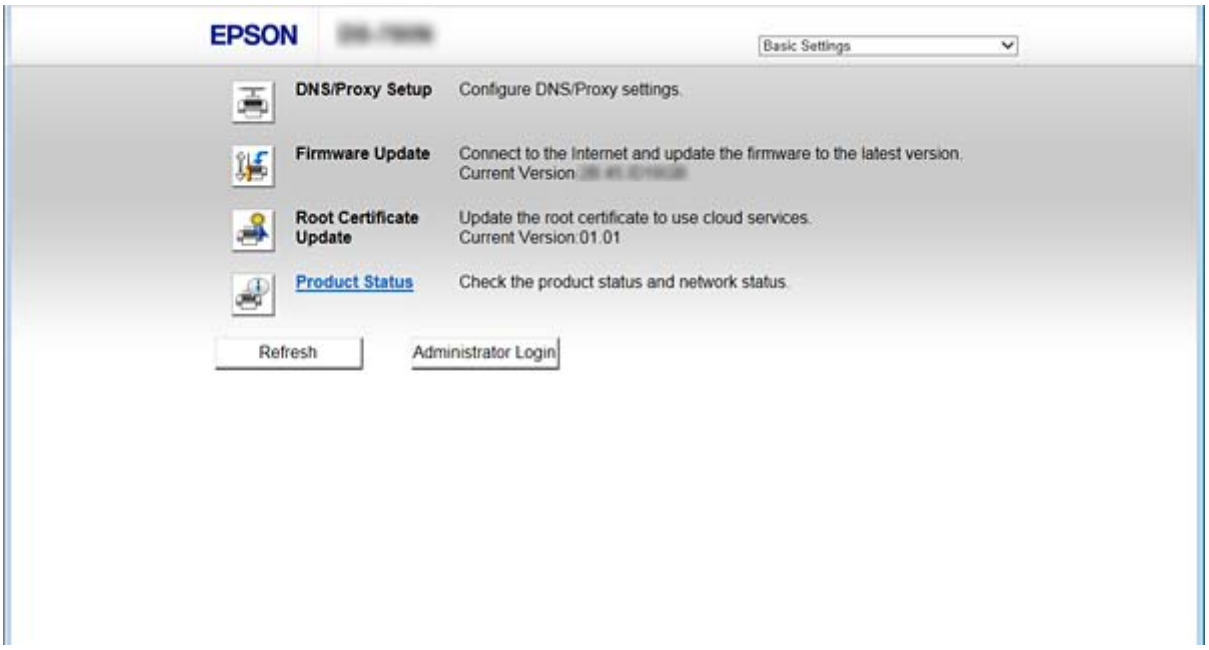
Web Config เป็นโปรแกมบนพื้นฐานของเบราเซอร์สำหรับการกำหนดค่าสแกนเนอร์

สำหรับการเข้าถึง Web Config คุณจะต้องกำหนดที่อยู่ IP ให้กับสแกนเนอร์ก่อน

หมายเหตุ:
คุณสามารถล็อคการตั้งค่าโดยการตั้งรหัสผ่านผู้ดูแลระบบให้กับสแกนเนอร์

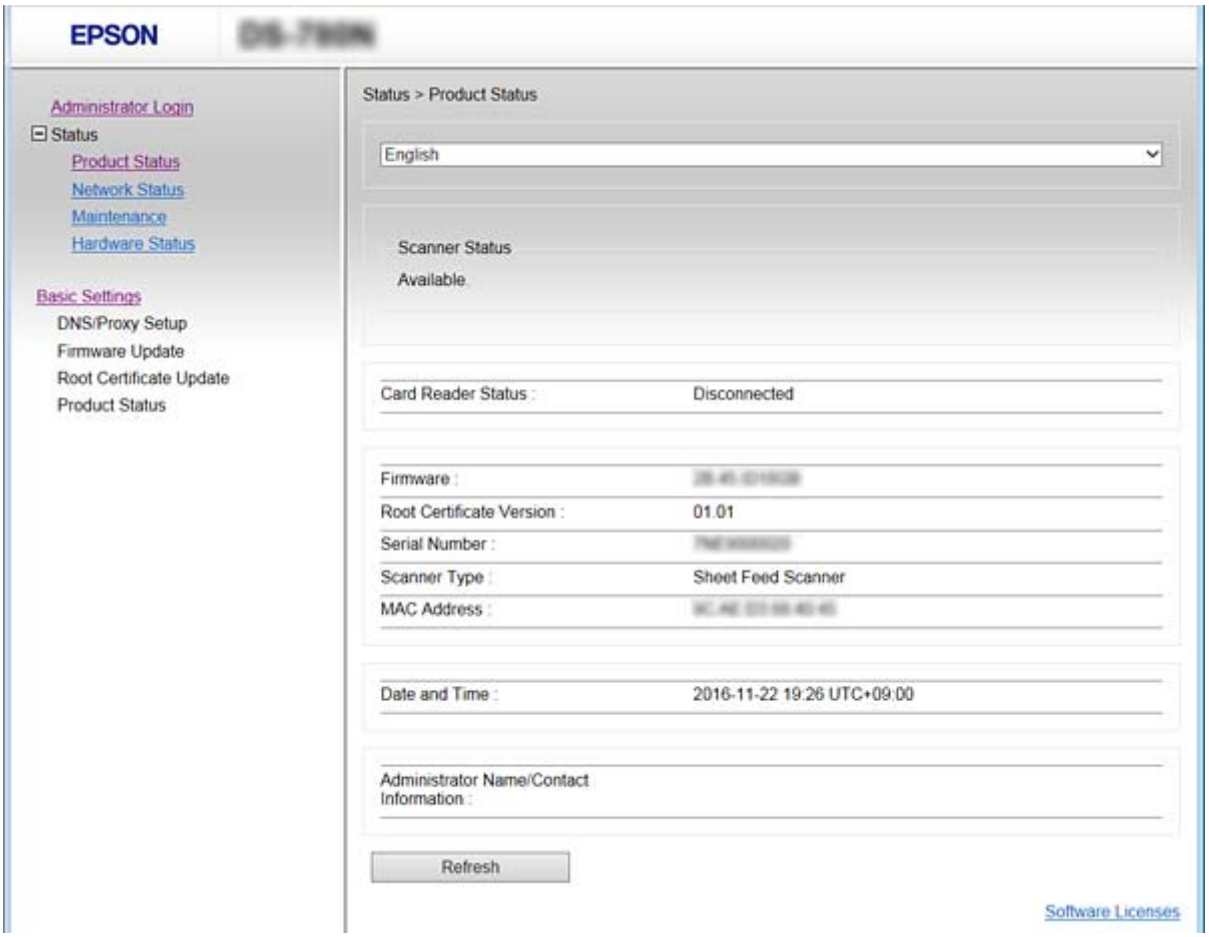
มีสองหน้าการตั้งค่าดังแสดงด้านล่าง

❑ **Basic Settings**
คุณสามารถตั้งค่าพื้นฐานสำหรับสแกนเนอร์



❑ **Advanced Settings**

คุณสามารถตั้งค่าขั้นสูงสำหรับสแกนเนอร์ หน้านี้ใช้สำหรับผู้ดูแลระบบเป็นหลัก



การเข้าถึง Web Config

ป้อนที่อยู่ IP ของสแกนเนอร์เข้าไปที่เว็บเบราเซอร์ ต้องเปิดใช้งาน JavaScript เมื่อเข้าถึง Web Config ผ่าน HTTPS จะมีข้อความแจ้งเตือนปรากฏขึ้นในเบราเซอร์เนื่องจากใบรับรองแบบลงนามเองที่จัดเก็บไว้ในสแกนเนอร์ถูกนำมาใช้

❑ การเข้าถึงผ่าน HTTPS

IPv4: https://<ที่อยู่ IP สแกนเนอร์> (ไม่มีเครื่องหมาย < >)

IPv6: https://[ที่อยู่ IP สแกนเนอร์]/ (มีเครื่องหมาย [ ])

❑ การเข้าถึงผ่าน HTTP

IPv4: http://<ที่อยู่ IP สแกนเนอร์> (ไม่มีเครื่องหมาย < >)

IPv6: http://[ที่อยู่ IP สแกนเนอร์]/ (มีเครื่องหมาย [ ])

หมายเหตุ:

❑ *ตัวอย่าง*

IPv4:

https://192.0.2.111/

http://192.0.2.111/

IPv6:

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

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

❑ *หากลงทะเบียนชื่อสแกนเนอร์ไว้กับ DNS เซิร์ฟเวอร์ คุณสามารถใช้ชื่อสแกนเนอร์แทนที่อยู่ IP ของสแกนเนอร์*

ข้อมูลที่เกี่ยวข้อง

➡ "การสื่อสาร SSL/TLS กับสแกนเนอร์" บนหน้าที่ 63

➡ "เกี่ยวกับใบรับรองดิจิตัล" บนหน้าที่ 63

การใช้ฟังก์ชันสแกน

ทั้งนี้ขึ้นอยู่กับวิธีการใช้สแกนเนอร์ของคุณ ให้ติดตั้งซอฟต์แวร์ต่อไปนี้และทำการตั้งค่าการใช้งาน

❑ **สแกนจากคอมพิวเตอร์**

- ❑ ยืนยันการใช้งานได้ของบริการสแกนผ่านเครือข่ายด้วย Web Config (ใช้ได้ตั้งแต่จัดส่งมาจากโรงงาน)
- ❑ ติดตั้ง Epson Scan 2 บนคอมพิวเตอร์ของคุณและตั้งค่าที่อยู่ IP
- ❑ เมื่อสแกนโดยใช้การทำงาน ให้ติดตั้ง Document Capture Pro (Document Capture) และกำหนดค่าการตั้งค่างาน

❑ **สแกนจากแผงควบคุมการทำงาน**

- ❑ เมื่อใช้งาน Document Capture Pro หรือ Document Capture Pro Server:
  ติดตั้ง Document Capture Pro หรือ Document Capture Pro Server
  การตั้งค่า DCP (โหมดเซิร์ฟเวอร์ โหมดไคลเอ็นต์)
- ❑ เมื่อใช้งานโปรโตคอล WSD:
  ยืนยันการใช้งานได้ของ WSD บน Web Config หรือแผงควบคุมการทำงาน (ใช้ได้ตั้งแต่จัดส่งมาจากโรงงาน)
  การตั้งค่าอุปกรณ์อื่นๆ (คอมพิวเตอร์ระบบ Windows)

การสแกนจากเครื่องคอมพิวเตอร์

ติดตั้งซอฟต์แวร์และตรวจสอบว่าบริการสแกนเครือข่ายถูกเปิดใช้งานเพื่อให้สแกนผ่านเครือข่ายจากเครื่องคอมพิวเตอร์

ข้อมูลที่เกี่ยวข้อง

➡ "ซอฟต์แวร์ที่จะติดตั้ง" บนหน้าที่ 25

➡ "เปิดใช้งานสแกนเครือข่าย" บนหน้าที่ 25

ซอฟต์แวร์ที่จะติดตั้ง

❑ Epson Scan 2

นี่คือไดรเวอร์สแกนเนอร์ หากคุณใช้อุปกรณ์จากคอมพิวเตอร์ ให้ติดตั้งบนคอมพิวเตอร์ไคลเอ็นต์แต่ละเครื่อง หาก Document Capture Pro/Document Capture ถูกติดตั้งไว้ คุณสามารถทำงานที่กำหนดไว้ไปยังปุ่มของอุปกรณ์ได้

ด้วย EpsonNet SetupManager ไดร์เวอร์เครื่องพิมพ์ยังสามารถถูกแจกจ่ายไปด้วยกันในแบบแพคเกจได้

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

ติดตั้งบนคอมพิวเตอร์ไคลเอ็นต์ คุณสามารถเรียกใช้การทำงานสั่งการที่ลงทะเบียนไว้บนคอมพิวเตอร์ที่มี Document Capture Pro/Document Capture ติดตั้งไว้บนเครือข่ายจากแผงควบคุมของคอมพิวเตอร์และสแกนเนอร์ได้

นอกจากนี้คุณยังสามารถสแกนจากคอมพิวเตอร์โดยผ่านเครือข่ายได้ Epson Scan 2 เป็นโปรแกรมที่จำเป็นสำหรับสแกนงาน

ข้อมูลที่เกี่ยวข้อง

➡ "EpsonNet SetupManager" บนหน้าที่ 56

ตั้งค่าที่อยู่ IP ของสแกนเนอร์ให้กับ Epson Scan 2

ระบุที่อยู่ IP ของสแกนเนอร์เพื่อให้สามารถใช้สแกนเนอร์บนเครือข่ายได้

1. เริ่มต้น **Epson Scan 2 Utility** จาก **เริ่ม** > **โปรแกรมทั้งหมด** > **EPSON** > **Epson Scan 2**

   หากมีสแกนเนอร์เครื่องอื่นลงทะเบียนไว้แล้ว ให้ไปที่ขั้นตอนที่ 2

   หากยังไม่ได้ลงทะเบียน ให้ไปที่ขั้นตอนที่ 4

2. คลิก ▼ บน **สแกนเนอร์**

3. คลิกที่ **การตั้งค่า**

4. เลือก **เปิดการแก้ไข** จากนั้นคลิก **เพิ่ม**

5. เลือกชื่อรุ่นสแกนเนอร์จาก **รุ่น**

6. เลือกที่อยู่ IP ของสแกนเนอร์ที่จะใช้งานจาก **ที่อยู่** ใน **ค้นหาเครือข่าย**

   คลิก แล้วคลิก เพื่ออัปเดตรายการ หากคุณไม่พบที่อยู่ IP ของสแกนเนอร์ ให้เลือก **ป้อนที่อยู่** แล้วป้อนที่อยู่ IP

7. คลิกที่ **เพิ่ม**

8. คลิกที่ **ตกลง**

เปิดใช้งานสแกนเครือข่าย

คุณสามารถตั้งค่าบริการสแกนเครือข่ายเมื่อคุณสแกนจากคอมพิวเตอร์ไคลเอ็นต์ผ่านเครือข่าย การตั้งค่าเริ่มต้นถูกเปิดใช้งาน

1. เข้าถึง Web Config แล้วเลือก **Services** > **Network Scan**

2. ตรวจสอบให้แน่ใจว่าเลือกไว้ที่ **Enable scanning** ของ **EPSON Scan**

   หากเลือกรายการนี้ไว้ นั่นคืองานนี้เสร็จสมบูรณ์ ปิด Web Config

   หากล้างออกแล้ว ให้เลือกและไปที่ขั้นตอนถัดไป

3. คลิกที่ **Next**

4. คลิกที่ **OK**

   เครือข่ายจะถูกเชื่อมต่อใหม่ จากนั้นการตั้งค่าจะถูกเปิดใช้งาน

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การสแกนโดยใช้แผงควบคุม

ฟังก์ชันสแกนไปยังโฟลเดอร์ และสแกนไปยังอีเมลโดยใช้แผงควบคุมของสแกนเนอร์ รวมถึงการถ่ายโอนผลการสแกนไปยังเมล โฟลเดอร์ ฯลฯ สามารถกระทำโดยการสั่งทำงานจากคอมพิวเตอร์

ขณะถ่ายโอนผลการสแกน ให้ตั้งค่างานด้วย Document Capture Pro Server หรือ Document Capture Pro

สำหรับรายละเอียดเกี่ยวกับการตั้งค่า และการตั้งค่างาน ให้ดูที่เอกสารกำกับ หรือวิธีใช้สำหรับ Document Capture Pro Server หรือ Document Capture Pro

ข้อมูลที่เกี่ยวข้อง

➡ "การตั้งค่า Document Capture Pro Server/Document Capture Pro" บนหน้าที่ 26

➡ "การตั้งค่าเซิร์ฟเวอร์และโฟลเดอร์" บนหน้าที่ 27

ซอฟต์แวร์ที่จะติดตั้งบนคอมพิวเตอร์

❑ **Document Capture Pro Server**

นี่คือเวอร์ชันเซิร์ฟเวอร์ของ Document Capture Pro ติดตั้งบนเซิร์ฟเวอร์ Windows สามารถจัดการหลายอุปกรณ์และงานแบบรวมศูนย์จากเซิร์ฟเวอร์ สามารถสั่งทำงานได้พร้อมกันจากหลายสแกนเนอร์

โดยการใช้เวอร์ชันที่ได้รับการรับรองของ Document Capture Pro Server คุณสามารถจัดการงานและประวัติการสแกนที่เชื่อมโยงกับผู้ใช้และกลุ่มได้

สำหรับรายละเอียดของ Document Capture Pro Server โปรดติดต่อสำนักงาน Epson ในท้องถิ่นของคุณ

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

เหมือนกับการสแกนจากคอมพิวเตอร์ คุณสามารถเรียกฟังก์ชันการทำงานที่ลงทะเบียนไว้บนคอมพิวเตอร์จากแผงควบคุมและสั่งทำงานได้ ไม่จำเป็นต้องเรียกใช้การทำงานจากคอมพิวเตอร์พร้อมกันจากหลายสแกนเนอร์

การตั้งค่า Document Capture Pro Server/Document Capture Pro

ทำการตั้งค่าสำหรับการใช้ฟังก์ชันการสแกนจากแผงควบคุมการทำงานของสแกนเนอร์

1. เข้าถึง Web Config แล้วเลือก **Services** > **Document Capture Pro**

2. เลือก **โหมดการดำเนินงาน**
   - ❑ Server Mode:
     เลือกตัวเลือกนี้เมื่อใช้ Document Capture Pro Server
   - ❑ Client Mode:
     ตั้งค่าสิ่งนี้เมื่อคุณเลือกการตั้งค่างานของ Document Capture Pro (Document Capture) ที่ติดตั้งไว้บนคอมพิวเตอร์ไคลเอ็นต์แต่ละเครื่องในเครือข่ายโดยไม่ได้ระบุคอมพิวเตอร์
3. ตั้งค่าดังต่อไปนี้ให้สอดคล้องตามโหมดที่เลือก
   - ❑ Server Mode:
     ใน **Server Address** ให้ระบุเซิร์ฟเวอร์ที่ซึ่ง Document Capture Pro Server ได้ติดตั้งไว้ สามารถเป็นตัวอักขระ 2 ถึง 252 ตัวอักขระใน IPv4, IPv6, ชื่อโฮสต์, รูปแบบ FQDN ในรูปแบบ FQDN สามารถใช้ตัวอักษร US-ASCII, ตัวเลข, ตัวอักษร และเครื่องหมายยัติภังค์ (ยกเว้นการนำหน้าและต่อท้าย)
   - ❑ Client Mode:
     ระบุ **Group Settings** ให้ใช้กลุ่มสแกนเนอร์ที่ระบุไว้จาก Document Capture Pro (Document Capture)
4. คลิกที่ **การตั้งค่า**

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การตั้งค่าเซิร์ฟเวอร์และโฟลเดอร์

Document Capture Pro และ Document Capture Pro Server บันทึกข้อมูลที่สแกนได้ไปยังคอมพิวเตอร์เซิร์ฟเวอร์หรือไคลเอ็นต์หนึ่งครั้ง และใช้ฟังก์ชันการถ่ายโอนเพื่อสั่งการฟังก์ชันสแกนไปยังโฟลเดอร์และสแกนไปยังเมล

คุณจะต้องมีสิทธิ์อนุญาตและข้อมูลที่จะถ่ายโอนจากคอมพิวเตอร์ที่มี Document Capture Pro, Document Capture Pro Server ติดตั้งไว้ไปยังคอมพิวเตอร์หรือบริการระบบคลาวด์

จัดเตรียมข้อมูลบนฟังก์ชันที่คุณจะใช้งาน โดยอ้างอิงต่อไปนี้

คุณสามารถทำการตั้งค่าสำหรับฟังก์ชันเหล่านี้โดยใช้ Document Capture Pro หรือ Document Capture Pro Server สำหรับรายละเอียดเกี่ยวกับการตั้งค่า ให้ดูที่เอกสารกำกับ หรือวิธีใช้สำหรับ Document Capture Pro Server หรือ Document Capture Pro

ชื่อ	การตั้งค่า	ข้อกำหนด
สแกนไปยังโฟลเดอร์เครือข่าย (SMB)	สร้างและตั้งค่าการแชร์โฟลเดอร์ที่บันทึก	บัญชีผู้ใช้ที่เป็นผู้ดูแลของคอมพิวเตอร์-ที่สร้างโฟลเดอร์ที่บันทึก
	ปลายทางของการสแกนไปยังโฟลเดอร์-เครือข่าย (SMB)	ชื่อผู้ใช้และรหัสผ่านเพื่อเข้าสู่ระบบของ-คอมพิวเตอร์ที่มีโฟลเดอร์ที่บันทึก และสิทธิ์อนุญาตเพื่ออัปเดตโฟลเดอร์ที่-บันทึก
สแกนไปยังโฟลเดอร์เครือข่าย (FTP)	ตั้งค่าสำหรับการเข้าสู่ระบบเซิร์ฟเวอร์ FTP	ข้อมูลการเข้าสู่ระบบสำหรับเซิร์ฟเวอร์ FTP และสิทธิ์อนุญาตเพื่ออัปเดต-โฟลเดอร์ที่บันทึก
สแกนไปยังอีเมล	ตั้งค่าสำหรับเซิร์ฟเวอร์อีเมล	ข้อมูลการตั้งค่าสำหรับเซิร์ฟเวอร์อีเมล

ชื่อ	การตั้งค่า	ข้อกำหนด
สแกนไปยัง Document Capture Pro (เมื่อใช้งาน Document Capture Pro Server)	การตั้งค่าการบันทึกรายการบนบริการ-ระบบคลาวด์	สภาพแวดล้อมการเชื่อมต่ออินเทอร์เน็ต การลงทะเบียนบัญชีสำหรับบริการระบบ-คลาวด์

ใช้สแกนผ่าน WSD (Windows เท่านั้น)

หากคอมพิวเตอร์ใช้ Windows Vista หรือรุ่นใหม่กว่า คุณสามารถใช้การสแกนผ่าน WSD
เมื่อโปรโตคอล WSD สามารถใช้ได้ เมนู **คอมพิวเตอร์(WSD)** จะแสดงขึ้นมาบนแผงควบคุมสแกนเนอร์

1. เข้าถึง Web Config แล้วเลือก **Services** > **Protocol**
2. ยืนยันว่าได้เลือก **Enable WSD** ไว้ใน **WSD Settings**
   หากเลือกรายการไว้ นั้นคืองานของคุณเสร็จสิ้น และคุณสามารถปิด Web Config
   หากไม่ได้เลือกไว้ ให้เลือกและไปที่ขั้นตอนถัดไป
3. คลิกปุ่ม **Next**
4. ยืนยันการตั้งค่า จากนั้นคลิกที่ **การตั้งค่า**

การตั้งค่าระบบ

การตั้งค่าระบบจากแผงควบคุม

ตั้งค่าความสว่างหน้าจอ

ตั้งค่าความสว่างหน้าจอ LCD

1. แตะ **การตั้งค่า** บนหน้าจอหลัก
2. แตะที่ **การตั้งค่าทั่วไป** > **ความสว่าง LCD**
3. แตะที่ ⊕ หรือ ⊖ เพื่อปรับความสว่าง
   คุณสามารถปรับค่าได้ตั้งแต่ 1 ถึง 9
4. แตะที่ **ตกลง**

ตั้งค่าเสียง

ตั้งค่าเสียงการทำงานของแผงและเสียงแจ้งข้อผิดพลาด

1. แตะ **การตั้งค่า** บนหน้าจอหลัก

2. แตะที่ **การตั้งค่าทั่วไป** > **เสียง**
3. ตั้งค่ารายการต่อไปนี้ตามที่จำเป็น
   - ❑ เสียงของการทำงาน
     ตั้งค่าระดับเสียงของการทำงานของแผงควบคุมการทำงาน
   - ❑ เสียงแจ้งข้อผิดพลาด
     ตั้งค่าระดับเสียงของเสียงแจ้งข้อผิดพลาด
4. แตะที่ **ตกลง**

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

ตรวจจับการป้อนต้นฉบับซ้อนกัน

กำหนดฟังก์ชันที่จะตรวจจับการป้อนต้นฉบับที่จะสแกนซ้อนกัน และเพื่อหยุดการสแกนเมื่อมีการป้อนเอกสารหลายแผ่นเกิดขึ้น

การสแกนต้นฉบับที่เหมือนจะเป็นการป้อนเข้าหลายแผ่น เช่น ซอง หรือกระดาษที่มีสติกเกอร์ ให้ตั้งค่าเป็น ปิดทำงาน

หมายเหตุ:
นอกจากนี้ยังสามารถตั้งค่าจาก Web Config หรือ Epson Scan 2

1. แตะ **การตั้งค่า** บนหน้าจอหลัก
2. แตะที่ **การตั้งค่าสแกน จากภายนอก** > **ตรวจจับการป้อนสองเท่าด้วยคลื่นความถี่สูง**
3. แตะที่ **ตรวจจับการป้อนสองเท่าด้วยคลื่นความถี่สูง** เพื่อเปิดหรือปิดทำงาน
4. แตะที่ **ปิด**

ตั้งค่าโหมดความเร็วต่ำ

ตั้งค่าให้สแกนที่ความเร็วต่ำเพื่อไม่ให้เกิดกระดาษติดเมื่อสแกนเอกสารแบบบาง เช่น กระดาษสลิป

1. แตะ **การตั้งค่า** บนหน้าจอหลัก
2. แตะที่ **การตั้งค่าสแกน จากภายนอก** > **ช้า**
3. แตะที่ **ช้า** เพื่อเปิดหรือปิดทำงาน
4. แตะที่ **ปิด**

การตั้งค่าระบบโดยใช้ Web Config

การตั้งค่าประหยัดพลังงานในระหว่างไม่ได้ใช้งาน

ทำการตั้งค่าประหยัดพลังงานสำหรับช่วงเวลาที่ไม่ได้ใช้งานสแกนเนอร์ ตั้งค่าเวลาโดยขึ้นอยู่กับสภาพแวดล้อมการใช้งานของคุณ

หมายเหตุ:
นอกจากนี้คุณยังสามารถทำการตั้งค่าประหยัดพลังงานบนแผงควบคุมสแกนเนอร์ได้

1. เข้าถึง Web Config แล้วเลือก **System Settings** > **Power Saving**
2. ป้อนค่าเวลาสำหรับ **Sleep Timer** สลับไปยังโหมดประหยัดพลังงานเมื่อไม่ได้ใช้งาน
3. เลือกเวลาปิดเครื่องสำหรับ **Power Off Timer**
4. คลิกที่ **OK**

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การตั้งค่าแผงควบคุม

ตั้งค่าสำหรับแผงควบคุมของสแกนเนอร์ คุณสามารถตั้งค่าได้ดังต่อไปนี้

1. เข้าถึง Web Config แล้วเลือก **System Settings** > **Control Panel**
2. ตั้งค่ารายการต่อไปนี้ตามที่จำเป็น
   - ❑ Language

     เลือกภาษาแสดงผลบนแผงควบคุม
   - ❑ Panel Lock

     หากคุณเลือก **ON** จำเป็นต้องมีรหัสผ่านผู้ดูแลระบบเมื่อคุณทำงานที่จำเป็นต้องใช้สิทธิ์ของผู้ดูแลระบบ หากไม่ได้ตั้งรหัสผ่านของผู้ดูแลระบบไว้ การล็อคแผงควบคุมจะปิดทำงาน
   - ❑ Operation Timeout

     หากคุณเลือก **ON** เมื่อคุณเข้าสู่ระบบเป็นผู้ดูแลระบบ คุณจะถูกนำออกจากระบบโดยอัตโนมัติและไปที่หน้าจอเริ่มต้นหากไม่ได้ทำกิจกรรมใด ๆ เป็นช่วงระยะเวลาหนึ่ง

     คุณสามารถตั้งค่าระหว่าว 10 วินาทีและ 240 นาที
3. คลิกที่ **OK**

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การตั้งค่าจำกัดอินเทอร์เฟสภายนอก

คุณสามารถจำกัดการเชื่อมต่อ USB จากคอมพิวเตอร์ได้ ตั้งค่าให้จำกัดการสแกนที่นอกเหนือจากโดยผ่านเครือข่าย

1. เข้าถึง Web Config แล้วเลือก **System Settings** > **External Interface**
2. เลือก **Enable** หรือ **Disable**
   ในการจำกัด ให้เลือก **Disable**
3. แตะที่ **OK**

การซิงค์วันที่และเวลากับเซิร์ฟเวอร์เวลา

หากคุณใช้ใบรับรอง CA คุณสามารถป้องกันปัญหาเกี่ยวกับเวลาได้

1. เข้าถึง Web Config แล้วเลือก **System Settings** > **Date and Time** > **Time Server**
2. เลือก **Use** สำหรับ **Use Time Server**
3. ป้อนที่อยู่เซิร์ฟเวอร์เวลาสำหรับ **Time Server Address**
   คุณสามารถใช้รูปแบบ IPv4, IPv6 หรือ FQDN ป้อนไม่เกิน 252 ตัวอักขระ หากคุณไม่ได้ระบุสิ่งนี้ ให้เว้นไว้
4. ป้อน **Update Interval (min)**
   คุณสามารถตั้งค่าได้สูงสุด 10,800 นาที
5. คลิกที่ **OK**

   หมายเหตุ:
   คุณสามารถยืนยันสถานะของการเชื่อมต่อด้วยเซิร์ฟเวอร์เวลาที่ ***Time Server Status***

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การตั้งค่าความปลอดภัยพื้นฐาน

บทนี้อธิบายการตั้งค่าความปลอดภัยพื้นฐานที่ไม่จำเป็นต้องใช้สภาพแวดล้อมพิเศษ

การแนะนำคุณสมบัติความปลอดภัยพื้นฐาน

เราขอแนะนำคุณสมบัติความปลอดภัยพื้นฐานของอุปกรณ์ Epson

ชื่อคุณสมบัติ	ประเภทคุณสมบัติ	สิ่งที่จะตั้งค่า	สิ่งที่จะป้องกัน
การตั้งค่าสำหรับรหัสผ่านผู้ดูแลระบบ	ล็อกการตั้งค่าที่เกี่ยวข้องกับระบบ เช่น การตั้งค่าเครือข่ายและการเชื่อมต่อ USB เพื่อให้ไม่สามารถเปลี่ยนแปลงยกเว้นโดยผู้ดูแลระบบเท่านั้น	ผู้ดูแลระบบตั้งรหัสผ่านให้กับอุปกรณ์ การกำหนดค่าหรืออัปเดตมีสามารถใช้งานได้ทุกที่จาก Web Config แผงควบคุม Epson Device Admin และ EpsonNet Config.	ป้องกันจากการอ่านอย่างผิดกฎหมาย และเปลี่ยนแปลงข้อมูลที่จัดเก็บไว้ในอุปกรณ์ เช่น ID รหัสผ่าน การตั้งค่าเครือข่าย และรายชื่อติดต่อ นอกจากนี้ ยังลดช่วงกว้างของความเสี่ยงด้านความปลอดภัยลง เช่น การรั่วไหลของข้อมูลสำหรับสภาพแวดล้อมเครือข่ายหรือนโยบายความปลอดภัย
การสื่อสาร SSL/TLS	เมื่อเชื่อมต่อไปยังเซิร์ฟเวอร์ Epson บนอินเทอร์เน็ตจากอุปกรณ์หนึ่ง การสื่อสารดังกล่าวกับคอมพิวเตอร์ผ่านเบราเซอร์ หรืออัปเดตเฟิร์มแวร์ เนื้อหาการสื่อสารจะถูกเข้ารหัสโดยการสื่อสาร SSL/TLS	ขอรับใบรับรองที่ลงนามโดย CA จากนั้นนำเข้าไปยังสแกนเนอร์	การล้างการบ่งชี้ของอุปกรณ์โดยใบรับรองที่ลงนามโดย CA จะป้องกันไม่ให้เกิดการปลอมแปลงและการเข้าถึงโดยไม่ได้รับอนุญาต นอกจากนี้ เนื้อหาการสื่อสารของ SSL/TLS ก็ได้รับการป้องกัน และป้องกันเนื้อหารั่วไหลสำหรับข้อมูลการพิมพ์และข้อมูลการตั้งค่า
โปรโตคอลตัวควบคุม	โปรโตคอลตัวควบคุมถูกใช้สำหรับการสื่อสารระหว่างอุปกรณ์และคอมพิวเตอร์ และเปิดใช้งาน/ปิดใช้งานฟังก์ชันการทำงาน	โปรโตคอลหรือบริการที่ใช้งานกับคุณสมบัติต่าง ๆ อนุญาตทำงานหรือห้ามทำงานโดยแยกกัน	การลดระดับความเสี่ยงด้านความปลอดภัยที่อาจเกิดขึ้นผ่านการใช้งานโดยไม่ตั้งใจ โดยป้องกันผู้ใช้จากการใช้ฟังก์ชันที่ไม่จำเป็น

ข้อมูลที่เกี่ยวข้อง

➡ "เกี่ยวกับ Web Config" บนหน้าที่ 22
➡ "EpsonNet Config" บนหน้าที่ 55
➡ "Epson Device Admin" บนหน้าที่ 55
➡ "การกำหนดรหัสผ่านของผู้ดูแลระบบ" บนหน้าที่ 32
➡ "การควบคุมโปรโตคอล" บนหน้าที่ 35

การกำหนดรหัสผ่านของผู้ดูแลระบบ

เมื่อคุณตั้งค่ารหัสผ่านผู้ดูแลระบบ ผู้ใช้ที่นอกเหนือจากผู้ดูแลระบบจะไม่สามารถเปลี่ยนแปลงการตั้งค่าสำหรับการดูแลระบบได้ คุณสามารถตั้งค่าและเปลี่ยนแปลงรหัสผ่านผู้ดูแลระบบโดยใช้ทั้ง Web Config แผงควบคุมของสแกน

เนอร์ หรือซอฟต์แวร์ (Epson Device Admin หรือ EpsonNet Config) เมื่อใช้ซอฟต์แวร์ ให้ดูเอกสารคู่มือสำหรับแต่ละซอฟต์แวร์

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดค่ารหัสผ่านผู้ดูแลระบบจากแผงควบคุม" บนหน้าที่ 33
➡ "การกำหนดรหัสผ่านของผู้ดูแลระบบโดยใช้ Web Config" บนหน้าที่ 33
➡ "EpsonNet Config" บนหน้าที่ 55
➡ "Epson Device Admin" บนหน้าที่ 55

การกำหนดค่ารหัสผ่านผู้ดูแลระบบจากแผงควบคุม

คุณสามารถตั้งรหัสผ่านผู้ดูแลระบบจากแผงควบคุมของสแกนเนอร์

1. แตะ **การตั้งค่า** บนหน้าจอหลัก
2. แตะที่ **การดูแลระบบ** > **การตั้งค่าผู้ดูแลระบบ**
   หากรายการไม่แสดงขึ้นมา ให้ตวัดหน้าจอขึ้นบนเพื่อแสดงรายการ
3. แตะที่ **รหัสผ่านผู้ดูแลระบบ** > **ลงทะเบียน**
4. ป้อนรหัสผ่าน จากนั้นแตะที่ **ตกลง**
5. ป้อนรหัสผ่านอีกครั้ง จากนั้นแตะที่ **ตกลง**
6. แตะ **ตกลง** จากหน้าจอยืนยัน
   หน้าจอการตั้งค่าผู้ดูแลระบบจะแสดงขึ้นมา
7. แตะที่ **การตั้งค่าการล็อก** จากนั้นแตะ **ตกลง** บนหน้าจอยืนยัน
   การตั้งค่าการล็อก ถูกตั้งค่าไปที่ **เปิด** และต้องใช้รหัสผ่านผู้ดูแลระบบเมื่อคุณทำงานกับรายการเมนูที่ล็อคไว้

หมายเหตุ:

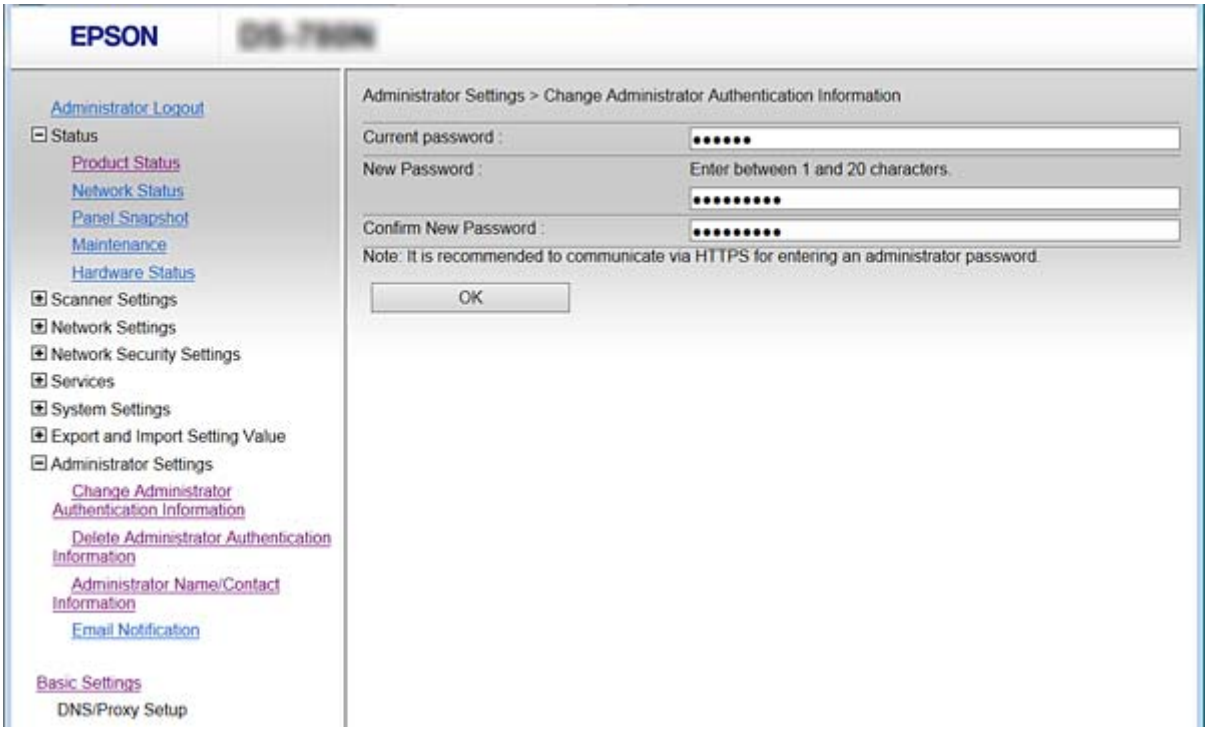
- *หากคุณตั้งค่า **การตั้งค่า** > **การตั้งค่าทั่วไป** > **การทำงานหมดเวลา** เป็น **เปิด** สแกนเนอร์จะนำคุณออกจากระบบหลังจากที่ไม่ได้ทำงานใด ๆ ชั่วครู่บนแผงควบคุม*
- *คุณสามารถเปลี่ยนแปลงหรือลบรหัสผ่านผู้ดูแลระบบเมื่อคุณเลือก **เปลี่ยน** หรือ **รีเซ็ต** บนหน้าจอ **รหัสผ่านผู้ดูแลระบบ** และป้อนรหัสผ่านผู้ดูแลระบบ*

การกำหนดรหัสผ่านของผู้ดูแลระบบโดยใช้ Web Config

คุณสามารถกำหนดค่ารหัสผ่านผู้ดูแลระบบโดยใช้ Web Config

1. เข้าถึง Web Config แล้วเลือก **Administrator Settings** > **Change Administrator Authentication Information**

2. ป้อนรหัสผ่านไปที่ **New Password** และ **Confirm New Password** ป้อนชื่อผู้ใช้ หากจำเป็น
   หากคุณต้องการเปลี่ยนแปลงรหัสผ่านเป็นรหัสใหม่ ให้ป้อนรหัสผ่านปัจจุบัน



3. เลือก **OK**

   หมายเหตุ:
   - ❑ *สำหรับการตั้งค่าหรือเปลี่ยนแปลงรายการเมนูที่ล็อกไว้ ให้คลิก **Administrator Login** จากนั้นป้อนรหัสผ่านผู้ดูแลระบบ*
   - ❑ *สำหรับการลบรหัสผ่านผู้ดูแลระบบ ให้คลิก **Administrator Settings** > **Delete Administrator Authentication Information** จากนั้นป้อนรหัสผ่านผู้ดูแลระบบ*

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

รายการที่จะล็อคโดยรหัสผ่านของผู้ดูแลระบบ

ผู้ดูแลระบบมีสิทธิ์การตั้งค่าและเปลี่ยนแปลงสำรับคุณสมบัติทั้งหมดบนอุปกรณ์

นอกตากนี้หากคุณตั้งรหัสผ่านผู้ดูแลระบบบนอุปกรณ์ คุณสามารถล็อกไว้เพื่อไม่ให้สามารถเปลี่ยนแปลงรายการที่เกี่ยวข้องกับการจัดการอุปกรณ์

ต่อไปนี้เป็นรายการที่ผู้ดูแลระบบสามารถควบคุมได้

รายการ	คำอธิบาย
การตั้งค่าสแกนเนอร์	การตั้งค่าการตรวจจับการป้อนกระดาษซ้อนและโหมดความเร็วต่ำ
การตั้งค่าการเชื่อมต่ออีเธอร์เน็ต	เปลี่ยนแปลงชื่อของอุปกรณ์และที่อยู่ IP ตั้งค่าเซิร์ฟเวอร์ DNS และพร็อกซีเซิร์ฟเวอร์ และเปลี่ยนแปลงการตั้งค่าที่เกี่ยวข้องกับการเชื่อมต่อเครือข่าย

การตั้งค่าความปลอดภัยพื้นฐาน

รายการ	คำอธิบาย
การตั้งค่าบริการของผู้ใช้	ตั้งค่าการควบคุมโปรโตคอลการสื่อสาร สแกนหาเครือข่าย และบริการ Document Capture Pro
การตั้งค่าเซิร์ฟเวอร์อีเมล	ตั้งค่าเซิร์ฟเวอร์อีเมลที่อุปกรณ์สื่อสารโดยตรง
การตั้งค่าความปลอดภัย	การตั้งค่าสำหรับความปลอดภัยของเครือข่าย เช่น การสื่อสาร SSL/TLS การกรอง IPsec/IP และ IEEE802.1X
อัปเดตใบรับรองราก	อัปเดตใบรับรองรากจำเป็นสำหรับการตรวจรับรองความถูกต้อง Document Capture Pro Server และอัปเดตเฟิร์มแวร์จาก Web Config
การอัปเดตเฟร์มแวร์	ตรวจสอบและอัปเดตเฟิร์มแวร์ของอุปกรณ์
การตั้งค่าเวลา ตัวตั้งเวลา	เวลาของการเปลี่ยนสู่โหมดสลีป การปิดเครื่องอัตโนมัติ วันที่/เวลา ตัวตั้งเวลาการไม่ใช้งาน การตั้งค่าอื่น ๆ ที่เกี่ยวข้องกับตัวตั้งเวลา
กู้คืนไปยังการตั้งค่าเริ่มต้น	การตั้งค่าสำหรับสแกนเนอร์ให้รีเซ็ตไปยังการตั้งค่าจากโรงงาน
การตั้งค่าผู้ดูแลระบบ	การตั้งค่าล็อกโดยผู้ดูแลระบบหรือรหัสผ่านผู้ดูแลระบบ
การตั้งค่าอุปกรณ์ที่ได้รับรอง	การตั้งค่า ID ของอุปกรณ์ที่ตรวจรับรองความถูกต้อง ตั้งค่าเมื่อใช้งานสแกนเนอร์บนระบบตรวจรับรองความถูกต้องที่รองรับอุปกรณ์การตรวจรับรองความถูกต้อง

การควบคุมโปรโตคอล

คุณสามารถสแกนโดยใช้เส้นทางและโปรโตคอลที่หลากหลาย นอกจากนี้คุณยังสามารถใช้การสแกนหาเครือข่ายจากจำนวนคอมพิวเตอร์เครือข่ายที่ไม่ได้กำหนดไว้ได้ ตัวอย่างเช่น คุณสามารถทำการสแกนโดยใช้เส้นทางและโปรโตคอลที่กำหนดไว้เท่านั้น คณสามารถปรับลดความเสี่ยงด้านความปลอดภัยที่ไม่คาดหวังให้ลดลงโดยการสร้างการจำกัดการสแกนจากเส้นทางเฉพาะหรือโดยการควบคุมฟังก์ชันที่ใช้งานได้

กำหนดค่าโปรโตคอล

1. เข้าถึง Web Config แล้วเลือก **Services** > **Protocol**
2. กำหนดค่าแต่ละรายการ
3. คลิกที่ **Next**
4. คลิกที่ **OK**

   การตั้งค่าถูกใช้กับสแกนเนอร์

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "โปรโตคอลที่คุณสามารถเปิดใช้งานหรือปิดใช้งาน" บนหน้าที่ 36
➡ "รายการการตั้งค่าโปรโตคอล" บนหน้าที่ 37

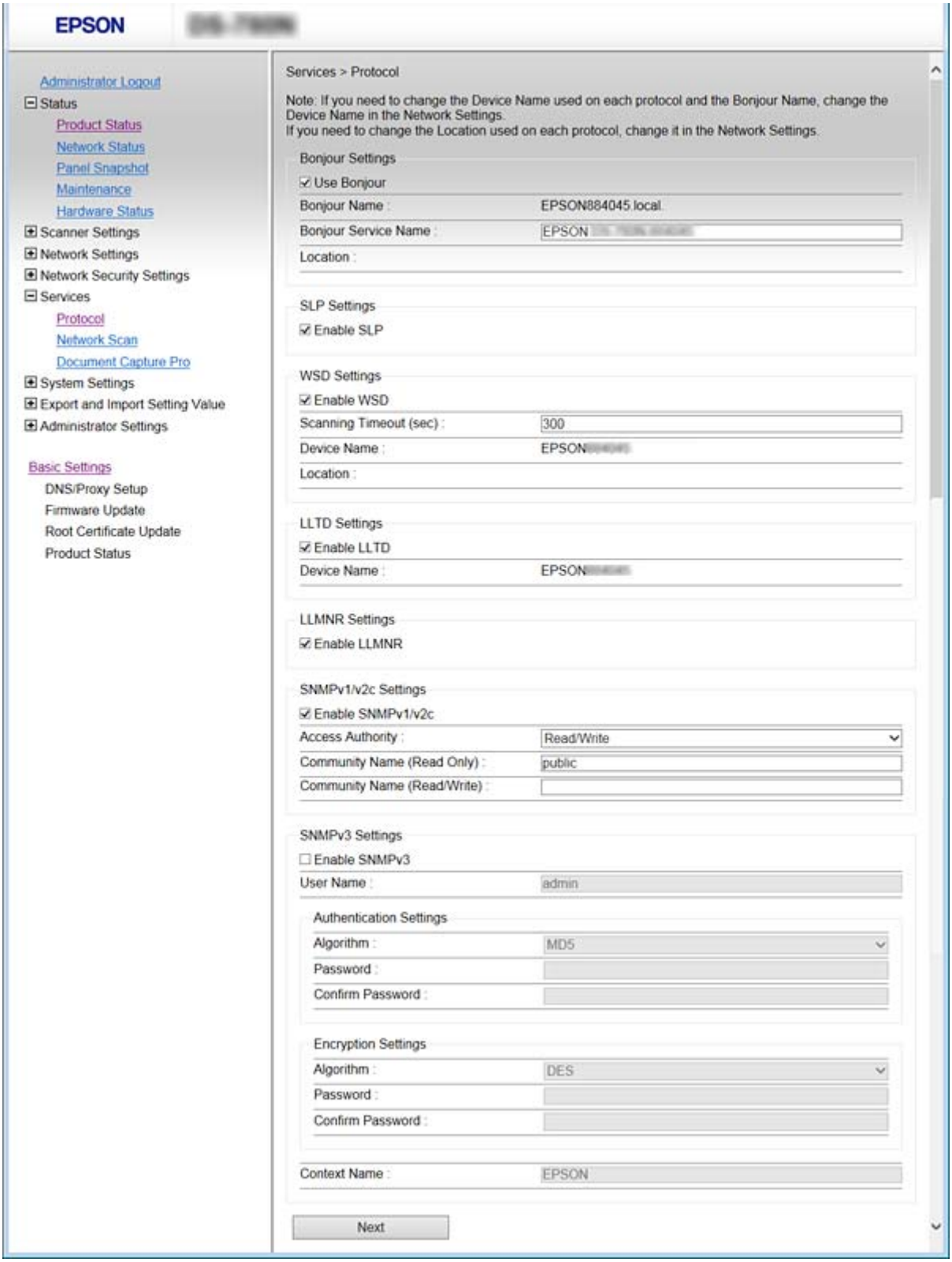
โปรโตคอลที่คุณสามารถเปิดใช้งานหรือปิดใช้งาน

โปรโตคอล	คำอธิบาย
Bonjour Settings	คุณสามารถระบุว่าจะใช้ Bonjour หรือไม่ก็ได้ Bonjour ถูกใช้เพื่อค้นหาอุปกรณ์ สแกน และอื่น ๆ
SLP Settings	คุณสามารถเปิดใช้งานหรือปิดใช้งานฟังก์ชัน SLP SLP ถูกใช้สำหรับ Epson Scan 2 และการค้นหาเครือข่ายใน EpsonNet Config.
WSD Settings	คุณสามารถเปิดใช้งานหรือปิดใช้งานฟังก์ชัน WSD เมื่อตัวเลือกนี้เปิดใช้งาน คุณสามารถเพิ่มอุปกรณ์ WSD หรือสแกนจากพอร์ต WSD
LLTD Settings	คุณสามารถเปิดใช้งานหรือปิดใช้งานฟังก์ชัน LLTD เมื่อตัวเลือกนี้เปิดใช้งาน มันจะแสดงในแผนที่เครือข่ายของ Windows
LLMNR Settings	คุณสามารถเปิดใช้งานหรือปิดใช้งานฟังก์ชัน LLMNR เมื่อตัวเลือกนี้ถูกเปิดใช้งาน คุณสามารถใช้ความละเอียดของชื่อโดยไม่ต้องใช้ NetBIOS แม้ว่าคุณจะไม่สามารถใช้ DNS ก็ตาม
SNMPv1/v2c Settings	คุณสามารถระบุว่าจะเปิดใช้งานหรือปิดใช่งาน SNMPv1/v2c ตัวเลือกนี้ถูกใช้เพื่อการตั้งค่าอุปกรณ์ การเฝ้าตรวจตรา และอื่น ๆ
SNMPv3 Settings	คุณสามารถระบุว่าจะเปิดใช้งานหรือปิดใช่งาน SNMPv3 ตัวเลือกนี้ถูกใช้เพื่อการตั้งค่าอุปกรณ์ การเข้ารหัส การเฝ้าตรวจตรา และอื่น ๆ

ข้อมูลที่เกี่ยวข้อง

➡ "การควบคุมโปรโตคอล" บนหน้าที่ 35
➡ "รายการการตั้งค่าโปรโตคอล" บนหน้าที่ 37

รายการการตั้งค่าโปรโตคอล



รายการ	การตั้งค่าและคำอธิบาย
Bonjour Settings	

การตั้งค่าความปลอดภัยพื้นฐาน

รายการ	การตั้งค่าและคำอธิบาย
Use Bonjour	เลือกตัวเลือกนี้เพื่อค้นหาหรือใช้อุปกรณ์ผ่าน Bonjour
Bonjour Name	แสดงชื่อ Bonjour
Bonjour Service Name	คุณสามารถแสดงผลและตั้งค่าชื่อบริการ Bonjour
Location	แสดงชื่อตำแหน่ง Bonjour
SLP Settings	
Enable SLP	เลือกตัวเลือกนี้เพื่อเปิดใช้งานฟังก์ชัน SLP ใช้สำหรับการ-ค้นหาเครือข่ายใน Epson Scan 2 และ EpsonNet Config
WSD Settings	
Enable WSD	เลือกตัวเลือกนี้เพื่อเปิดใช้งานการเพิ่มอุปกรณ์โดยใช้ WSD และพิมพ์และสแกนจากพอร์ต WSD
Scanning Timeout (sec)	ป้อนค่าหมดเวลาการสื่อสารสำหรับการสแกนผ่าน WSD ระหว่าง 3 ถึง 3600 วินาที
Device Name	แสดงชื่ออุปกรณ์ WSD
Location	แสดงชื่อตำแหน่ง WSD
LLTD Settings	
Enable LLTD	เลือกตัวเลือกนี้เพื่อเปิดใช้งาน LLTD สแกนเนอร์จะแสดงผลใน-แม็ปเครือข่ายของ Windows
Device Name	แสดงชื่ออุปกรณ์ LLTD
LLMNR Settings	
Enable LLMNR	เลือกตัวเลือกนี้เพื่อเปิดใช้งาน LLMNR คุณสามารถใช้ความ-ละเอียดของชื่อโดยไม่ต้องใช้ NetBIOS แม้ว่าคุณจะไม่-สามารถใช้ DNS ก็ตาม
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	เลือกเพื่อเปิดใช้งาน SNMPv1/v2c เฉพาะสแกนเนอร์ที่รองรับ SNMPv3 จะแสดงผลขึ้นมา
Access Authority	ตั้งค่าการอนุญาตให้เข้าถึงเมื่อเปิดใช้งาน SNMPv1/v2c เลือก **Read Only** หรือ **Read/Write**
Community Name (Read Only)	ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ตั้งแต่ 0 ถึง 32 ตัว
Community Name (Read/Write)	ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ตั้งแต่ 0 ถึง 32 ตัว
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 ถูกเปิดใช้งานเมื่อกาเลือกในกล่องเลือกรายการ
User Name	ป้อนระหว่าง 1 และ 32 ตัวอักขระโดยใช้ตัวอักขระขนาด 1 ไบต์
Authentication Settings	
Algorithm	เลือกอัลกอริทึมสำหรับการรับรองความถูกต้องสำหรับ SNMPv3

การตั้งค่าความปลอดภัยพื้นฐาน

รายการ	การตั้งค่าและคำอธิบาย
Password	ป้อนรหัสผ่านสำหรับการรับรองความถูกต้องสำหรับ SNMPv3 ป้อนค่าระหว่าง 8 และ 32 ตัวอักขระในแบบ ASCII (0x20–0x7E) หากคุณไม่ได้ระบุสิ่งนี้ ให้เว้นไว้
Confirm Password	ป้อนรหัสผ่านที่คุณกำหนดค่าไว้เพื่อการยืนยัน
Encryption Settings	
Algorithm	เลือกอัลกอริทึมสำหรับการเข้ารหัสสำหรับ SNMPv3.
Password	ป้อนรหัสผ่านสำหรับการเข้ารหัสสำหรับ SNMPv3 ป้อนค่าระหว่าง 8 และ 32 ตัวอักขระในแบบ ASCII (0x20–0x7E) หากคุณไม่ได้ระบุสิ่งนี้ ให้เว้นไว้
Confirm Password	ป้อนรหัสผ่านที่คุณกำหนดค่าไว้เพื่อการยืนยัน
Context Name	ป้อนไม่เกิน 32 ตัวอักขระในแบบ Unicode (UTF-8) หากคุณไม่ได้ระบุสิ่งนี้ ให้เว้นไว้ จำนวนของตัวอักขระที่สามารถป้อนเข้าจะแปรผันไปตามภาษา

ข้อมูลที่เกี่ยวข้อง

➡ "การควบคุมโปรโตคอล" บนหน้าที่ 35
➡ "โปรโตคอลที่คุณสามารถเปิดใช้งานหรือปิดใช้งาน" บนหน้าที่ 36

การตั้งค่าการดำเนินงานและการจัดการ

บทนี้อธิบายรายการต่าง ๆ ที่เกี่ยวข้องกับการดำเนินงานและการจัดการประจำวันของอุปกรณ์

ยืนยันข้อมูลของอุปกรณ์

คุณสามารถตรวจสอบข้อมูลต่อไปนี้ของอุปกรณ์ที่ทำงานจาก **Status** โดยใช้ Web Config

❏ Product Status

ตรวจสอบภาษา สถานะ หมายเลขผลิตภัณฑ์ ที่อยู่ MAS ฯลฯ

❏ Network Status

ตรวจสอบข้อมูลของสถานะของการเชื่อมต่อเครือข่าย ที่อยู่ IP เซิร์ฟเวอร์ DNS ฯลฯ

❏ Panel Snapshot

แสดงผลภาพสแนปช็อตหน้าจอที่แสดงผลบนแผงควบคุมของอุปกรณ์

❏ Maintenance

ตรวจสอบวันเริ่มต้น ข้อมูลการสแกน ฯลฯ

❏ Hardware Status

ตรวจสอบสถานะของสแกนเนอร์

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การจัดการอุปกรณ์ (Epson Device Admin)

คุณสามารถจัดการและดำเนินการหลายอุปกรณ์โดยใช้ Epson Device Admin Epson Device Admin อนุญาตให้คุณทำการจัดการอุปกรณ์ที่ตั้งอยู่บนเครือข่ายต่างกันได้ ต่อไปนี้แสดงเค้าโครงคุณสมบัติการจัดการหลัก

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับฟังก์ชันและการใช้ซอฟต์แวร์ ให้ดูที่เอกสารคู่มือหรือวิธีใช้ของ Epson Device Admin.

❏ การค้นหาอุปกรณ์

คุณสามารถค้นหาอุปกรณ์บนเครือข่าย จากนั้นลงทะเบียนอุปกรณ์เหล่านั้นไปยังรายการ หากอุปกรณ์ Epson เช่น เครื่องพิมพ์และสแกนเนอร์เชื่อมต่อเข้ากับส่วนย่อยเครือข่ายเดียวกับคอมพิวเตอร์ของผู้ดูแลระบบ คุณสามารถค้นหาอุปกรณ์เหล่านั้นได้แม้ว่าจะไม่ได้กำหนดที่อยู่ IP ก็ตาม

นอกจากนี้ คุณยังสามารถค้นหาอุปกรณ์ที่เชื่อมต่ออยู่กับคอมพิวเตอร์บนเครือข่ายโดยใช้สาย USB คุณจะต้องติดตั้ง Epson Device USB Agent บนคอมพิวเตอร์ของคุณ

❏ การตั้งค่าอุปกรณ์

คุณสามารถจัดทำแม่แบบที่ประกอบด้วยรายการต่างๆ เช่น อินเทอร์เฟสการตั้งค่า และแหล่งกำเนิดกระดาษ และใช้งานกับอุปกรณ์อื่น ๆ เป็นการตั้งค่าแบบแชร์ร่วมกัน เมื่อเชื่อมต่ออุปกรณ์เข้ากับเครือข่ายแล้ว คุณสามารถกำหนดค่าที่อยู่ IP บนอุปกรณ์ที่ยังไม่ได้กำหนดค่าที่อยู่ IP

❑ การเฝ้าตรวจตราอุปกรณ์

คุณสามารถขอดูสถานะและข้อมูลรายละเอียดสำหรับอุปกรณ์บนเครือข่ายได้ตามปกติ นอกจากนี้ คุณยังสามารถเฝ้าตรวจตราอุปกรณ์ที่ได้เชื่อมต่อกับคอมพิวเตอร์บนเครือข่ายโดยใช้ USB และอุปกรณ์จากบริษัทอื่น ๆ ที่ได้ลงทะเบียนไว้ในรายการอุปกรณ์ สำหรับการเฝ้าตรวจตราอุปกรณ์ที่เชื่อมต่อด้วยสาย USB คุณจะต้องติดตั้ง Epson Device USB Agent

❑ การจัดการการแจ้งเตือน

คุณสามารถเฝ้าตรวจตราการแจ้งเตือนเกี่ยวกับสถานะของอุปกรณ์และวัสดุสิ้นเปลืองได้ ระบบจะส่งอีเมลการแจ้งเตือนโดยอัตโนมัติไปยังผู้ดูแลระบบตามเงื่อนไขการตั้งค่าที่ตั้งไว้

❑ การจัดการรายงาน

คุณสามารถสร้างรายงานโดยปกติเนื่องจากระบบเก็บรวบรวมข้อมูลการใช้อุปกรณ์และวัสดุสิ้นเปลือง จากนั้น คุณสามารถบันทึกรายงานเหล่านั้น และส่งไปทางอีเมลได้

ข้อมูลที่เกี่ยวข้อง

➡ "Epson Device Admin" บนหน้าที่ 55

การรับการแจ้งเตือนทางอีเมลเมื่อมีเหตุการ์เกิดขึ้น

เกี่ยวกับการแจ้งเตือนทางอีเมล

คุณสามารถใช้คุณสมบัตินี้เพื่อรับการแจ้งเตือนทางอีเมลเมื่อมีเหตุการณ์ใด ๆ เกิดขึ้น คุณสามารถลงทะเบียนได้มากสุดถึง 5 ที่อยู่อีเมล และเลือกว่าเหตุการณ์ใดที่คุณต้องการได้รับการแจ้งเตือน

เซิร์ฟเวอร์เมลจะต้องถูกกำหนดค่าให้ใช้ฟังก์ชันนี้

ข้อมูลที่เกี่ยวข้อง

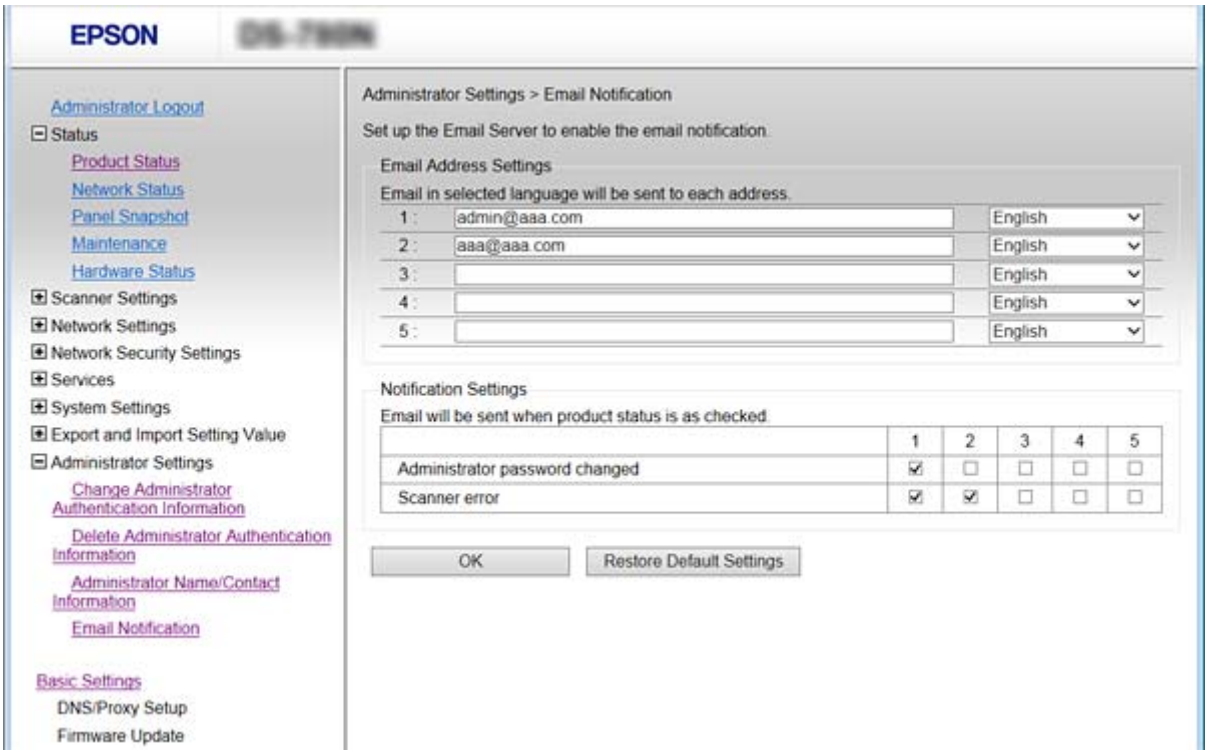
➡ "การกำหนดค่าเมลเซิร์ฟเวอร์" บนหน้าที่ 42

การกำหนดค่าการแจ้งเตือนทางอีเมล

สำหรับการใช้คุณสมบัตินี้ คุณจะต้องกำหนดค่าเมล์เซิร์ฟเวอร์

1. เข้าถึง Web Config แล้วเลือก **Administrator Settings** > **Email Notification**
2. ป้อนที่อยู่อีเมลที่คุณต้องการได้รับการแจ้งเตือนทางอีเมล
3. เลือกภาษาสำหรับการแจ้งเตือนทางอีเมล

4. กาเลือกในกล่องรายการสำหรับการแจ้งเตือนที่คุณต้องการได้รับ



5. คลิก **OK**

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "การกำหนดค่าเมลเซิร์ฟเวอร์" บนหน้าที่ 42

การกำหนดค่าเมลเซิร์ฟเวอร์

ตรวจสอบดังต่อไปนี้ก่อนการกำหนดค่า

❏ สแกนเนอร์เชื่อมต่ออยู่กับเครือข่าย

❏ ข้อมูลเซิร์ฟเวอร์อีเมลของเครื่องคอมพิวเตอร์

1. เข้าถึง Web Config แล้วเลือก **Network Settings** > **Email Server** > **Basic**

2. ป้อนค่าสำหรับแต่ละรายการ

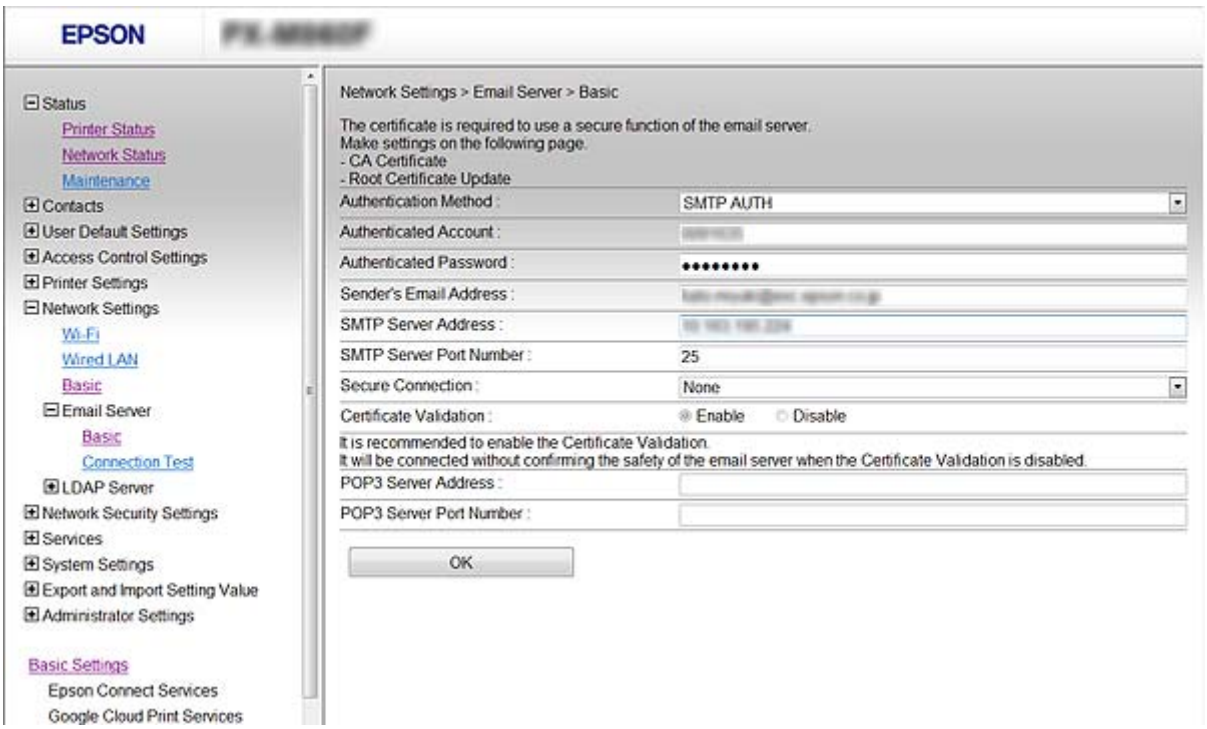
3. เลือก **OK**

   การตั้งค่าที่คุณเลือกไว้จะปรากฏขึ้นมา

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "รายการการตั้งค่าเมล์เซิร์ฟเวอร์" บนหน้าที่ 43

รายการการตั้งค่าเมล์เซิร์ฟเวอร์



รายการ	การตั้งค่าและคำอธิบาย	
Authentication Method	ระบุวิธีการรับรองความถูกต้องสำหรับสแกนเนอร์ที่เข้าสู่เมล์เซิร์ฟเวอร์	
	Off	การรับรองความถูกต้องถูกปิดใช้งานเมื่อทำการสื่อสารกับเซิร์ฟเวอร์
	SMTP AUTH	เมล์เซิร์ฟเวอร์ต้องรองรับการรับรองความถูกต้อง SMTP
	POP before SMTP	กำหนดค่าเซิร์ฟเวอร์ POP3 เมื่อเลือกวิธีการ
Authenticated Account	หากคุณเลือก **SMTP AUTH** หรือ **POP before SMTP** เป็น **Authentication Method** ให้ป้อนชื่อบัญชีรับรองความถูกต้องระหว่าง 0 และ 255 ตัวอักขระในแบบ ASCII (0x20–0x7E)	
Authenticated Password	หากคุณเลือก **SMTP AUTH** หรือ **POP before SMTP** เป็น **Authentication Method** ให้ป้อนชื่อบัญชีรับรองความถูกต้องระหว่าง 0 และ 20 ตัวอักขระโดยใช้ A–Z a–z 0–9 ! # $ % & ' * + - . / = ? ^ _ { | } ~ @	
Sender's Email Address	ป้อนที่อยู่อีเมลผู้ส่ง ป้อนระหว่าง 0 และ 255 ตัวอักขระในแบบ ASCII (0x20–0x7E) ยกเว้นสำหรับ : ( ) < > [ ] ; ¥ คาบเวลา "." ไม่สามารถเป็นตัวอักขระตัวแรก	
SMTP Server Address	ป้อนระหว่าง 0 และ 255 ตัวอักขระโดยใช้ A–Z a–z 0–9 . - . คุณสามารถใช้รูปแบบ IPv4 หรือ FQDN	
SMTP Server Port Number	ป้อนจำนวนระหว่าง 1 และ 65535	

รายการ	การตั้งค่าและคำอธิบาย	
Secure Connection	ระบุวิธีการเชื่อมต่อที่ปลอดภัยสำหรับเซิร์ฟเวอร์อีเมล	
	None	หากคุณเลือก **POP before SMTP** ใน **Authentication Method** วิธีการเชื่อมต่อถูกตั้งค่าเป็น **None**
	SSL/TLS	รายการนี้พร้อมใช้งานเมื่อ **Authentication Method** ถูกตั้งค่าเป็น **Off** หรือ **SMTP AUTH**
	STARTTLS	รายการนี้พร้อมใช้งานเมื่อ **Authentication Method** ถูกตั้งค่าเป็น **Off** หรือ **SMTP AUTH**
Certificate Validation	ใบรับรองสามารถใช้งานได้เมื่อรายการนี้เปิดใช้งาน เราขอแนะนำให้ตั้งค่าเป็น **Enable**	
POP3 Server Address	หากคุณเลือก **POP before SMTP** เป็น **Authentication Method** ให้ป้อนที่อยู่เซิร์ฟเวอร์ POP3 ระหว่าง 0 และ 255 ตัวอักขระโดยใช้ A–Z a–z 0–9 . - . คุณสามารถใช้รูปแบบ IPv4 หรือ FQDN	
POP3 Server Port Number	หากคุณเลือก **POP before SMTP** เป็น **Authentication Method** ให้ป้อนจำนวนระหว่าง 1 และ 65535	

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดค่าเมลเซิร์ฟเวอร์" บนหน้าที่ 42

การตรวจสอบการเชื่อมต่อเมล์เซิร์ฟเวอร์

1. เข้าถึง Web Config แล้วเลือก **Network Settings** > **Email Server** > **Connection Test**
2. เลือก **Start**

   การทดสอบการเชื่อมต่อไปยังเมล์เซิร์ฟเวอร์เริ่มต้นแล้ว หลังจากการทดสอบ รายงานการตรวจสอบจะแสดงขึ้นมา

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

➡ "การอ้างอิงการทดสอบการเชื่อมต่อเซิร์ฟเวอร์เมล" บนหน้าที่ 44

การอ้างอิงการทดสอบการเชื่อมต่อเซิร์ฟเวอร์เมล

ข้อความ	คำอธิบาย
Connection test was successful.	ข้อความนี้ปรากฏขึ้นเมื่อการเชื่อมต่อกับเซิร์ฟเวอร์สำเร็จ
SMTP server communication error. Check the following. - Network Settings	ข้อความนี้ปรากฏเมื่อ ❑ สแกนเนอร์ไม่ได้เชื่อมต่ออยู่กับเครือข่าย ❑ เซิร์ฟเวอร์ SMTP ล่ม ❑ การเชื่อมต่อเครือข่ายถูกตัดการเชื่อมต่อในขณะทำการสื่อสาร ❑ ได้รับข้อมูลที่สมบูรณ์

การตั้งค่าการดำเนินงานและการจัดการ

ข้อความ	คำอธิบาย
POP3 server communication error. Check the following. - Network Settings	ข้อความนี้ปรากฏเมื่อ ❏ สแกนเนอร์ไม่ได้เชื่อมต่ออยู่กับเครือข่าย ❏ เซิร์ฟเวอร์ POP3 ล่ม ❏ การเชื่อมต่อเครือข่ายถูกตัดการเชื่อมต่อในขณะทำการสื่อสาร ❏ ได้รับข้อมูลที่สมบูรณ์
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	ข้อความนี้ปรากฏเมื่อ ❏ การเชื่อมต่อเข้ากับเซิร์ฟเวอร์ DNS ล้มเหลว ❏ ความละเอียดของชื่อสำหรับเซิร์ฟเวอร์ SMTP ล้มเหลว
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	ข้อความนี้ปรากฏเมื่อ ❏ การเชื่อมต่อเข้ากับเซิร์ฟเวอร์ DNS ล้มเหลว ❏ ความละเอียดของชื่อสำหรับเซิร์ฟเวอร์ POP3 ล้มเหลว
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	ข้อความนี้ปรากฏขึ้นเมื่อการยืนยันตัวตนเซิร์ฟเวอร์ SMTP ล้มเหลว
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	ข้อความนี้ปรากฏขึ้นเมื่อการยืนยันตัวตนเซิร์ฟเวอร์ POP3 ล้มเหลว
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	ข้อความนี้ปรากฏขึ้นเมื่อคุณลองสื่อสารกับโปรโตคอลที่ไม่รองรับ
Connection to SMTP server failed. Change Secure Connection to None.	ข้อความนี้ปรากฏขึ้นเมื่อความไม่ตรงกันของ SMTP เกิดขึ้นระหว่างเซิร์ฟเวอร์และไคลเอ็นท์ หรือเมื่อเซิร์ฟเวอร์ไม่รองรับการเชื่อมต่อที่ปลอดภัยของ SMTP (การเชื่อมต่อ SSL)
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	ข้อความนี้ปรากฏขึ้นเมื่อความไม่ตรงกันของ SMTP เกิดขึ้นระหว่างเซิร์ฟเวอร์และไคลเอ็นท์ หรือเมื่อเซิร์ฟเวอร์ร้องขอให้ใช้การเชื่อมต่อ SSL/TLS สำหรับการเชื่อมต่อที่ปลอดภัยของ SMTP
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	ข้อความนี้ปรากฏขึ้นเมื่อความไม่ตรงกันของ SMTP เกิดขึ้นระหว่างเซิร์ฟเวอร์และไคลเอ็นท์ หรือเมื่อเซิร์ฟเวอร์ร้องขอให้ใช้การเชื่อมต่อ STARTTLS สำหรับการเชื่อมต่อที่ปลอดภัยของ SMTP
The connection is untrusted. Check the following. - Date and Time	ข้อความนี้ปรากฏขึ้นเมื่อการตั้งวันที่และเวลาของสแกนเนอร์ไม่ถูกต้องหรือใบรับรองหมดอายุ
The connection is untrusted. Check the following. - CA Certificate	ข้อความนี้ปรากฏขึ้นเมื่อสแกนเนอร์ไม่มีใบรับรองรากที่สอดคล้องกับเซิร์ฟเวอร์ หรือไม่ได้นำเข้า CA Certificate
The connection is not secured.	ข้อความนี้ปรากฏขึ้นเมื่อใบรับรองที่ได้มาได้รับความเสียหาย
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	ข้อความนี้ปรากฏขึ้นเมื่อวิธีการยืนยันตัวตนไม่ตรงกันเกิดขึ้นระหว่างเซิร์ฟเวอร์และไคลเอ็นท์ เซิร์ฟเวอร์นรองรับ SMTP AUTH

ข้อความ	คำอธิบาย
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	ข้อความนี้ปรากฏขึ้นเมื่อวิธีการยืนยันตัวตนไม่ตรงกันเกิดขึ้นระหว่างเซิร์ฟเวอร์และไคลเอ็นท์ เซิร์ฟเวอร์ไม่รองรับ SMTP AUTH
Sender's Email Address is incorrect. Change to the email address for your email service.	ข้อความนี้ปรากฏขึ้นเมื่อที่อยู่อีเมลของผู้ส่งที่กำหนดไว้ไม่ถูกต้อง
Cannot access the product until processing is complete.	ข้อความนี้ปรากฏขึ้นเมื่อสแกนเนอร์ไม่ว่าง

ข้อมูลที่เกี่ยวข้อง

➡ "การตรวจสอบการเชื่อมต่อเมล์เซิร์ฟเวอร์" บนหน้าที่ 44

การอัปเดตเฟิร์มแวร์

การอัปเดตเฟิร์มแวร์โดยใช้ Web Config

อัปเดตเฟิร์มแวร์โดยใช้ Web Config อุปกรณ์จะต้องเชื่อมต่อเข้ากับอินเทอร์เน็ต

1. เข้าถึง Web Config แล้วเลือก **Basic Settings** > **Firmware Update**
2. คลิกที่ **Start**

   การยืนยันเฟิร์แวร์เริ่มต้น และข้อมูลเฟิร์มแวร์จะปรากฏขึ้นหากมีเฟิร์มแวร์ที่อัปเดตแล้วอยู่
3. คลิก **Start** จากนั้นทำตามคำแนะนำบนหน้าจอ

หมายเหตุ:
นอกจากนี้ คุณยังสามารถทำการอัพเดทเฟิร์มแวร์โดยใช้ Epson Device Admin คุณสามารถยืนยันข้อมูลเฟิร์มแวร์บนรายการอุปกรณ์ด้วยสายตา โปรแกรมนี้มีประโยชน์มากเมื่อคุณต้องการอัปเดตเฟิร์มแวร์ของหลายอุปกรณ์ สำหรับรายละเอียดเพิ่มเติม ดูที่คู่มือหรือวิธีใช้ของ Epson Device Admin

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "Epson Device Admin" บนหน้าที่ 55

การอัปเดตเฟิร์มแวร์โดยใช้ Epson Firmware Updater

คุณสามารถดาวน์โหลดเฟิร์มแวร์ของอุปกรณ์ได้จากเว็บไซต์ของ Epson บนคอมพิวเตอร์ จากนั้นเชื่อมต่ออุปกรณ์และคอมพิวเตอร์ด้วยสาย USB เพื่ออัปเดตเฟิร์มแวร์ หากคุณไม่สามารถอัปเดตเฟิร์มแวร์ผ่านเครือข่าย ให้ลองวิธีนี้

1. เข้าสู่เว็บไซต์ Epson และดาวน์โหลดเฟิร์มแวร์
2. เชื่อมต่อคอมพิวเตอร์ที่มีเฟิร์มแวร์ที่ดาวน์โหลดไว้ไปยังอุปกรณ์โดยใช้สาย USB

3. ดับเบิลคลิกไฟล์ .exe ที่ดาวน์โหลดมา

   Epson Firmware Updater จะเริ่มทำงาน

4. ทำตามคำแนะนำบนหน้าจอ

การสำรองข้อมูลการตั้งค่า

ด้วยการส่งออกรายการการตั้งค่าบน Web Config คุณสามารถคัดลอกรายการต่างๆ ไปยังสแกนเนอร์อื่น

การส่งออกการตั้งค่า

ส่งออกแต่ละค่าสำหรับสแกนเนอร์

1. เข้าถึง Web Config แล้วเลือก **Export and Import Setting Value** > **Export**

2. เลือกการตั้งค่าที่คุณต้องการส่งออก

   เลือกการตั้งค่าที่คุณต้องการส่งออก หากคุณเลือกหมวดหมู่หลัก หมวดหมู่ย่อยจะถูกเลือกไปด้วย อย่างไรก็ดี หมวดหมู่ย่อยที่ทำให้เกิดข้อผิดพลาดจากการทำซ้ำข้อมูลภายในเครือข่ายเดียวกัน (เช่น ที่อยู่ IP เป็นต้น) จะไม่สามารถเลือกได้

3. ป้อนรหัสผ่านเพื่อเข้ารหัสไฟล์ที่ส่งออก

   คุณจะต้องใช้รหัสผ่านเพื่อนำเข้าไฟล์ ปล่อยช่องทิ้งว่างหากคุณไม่ต้องการเข้ารหัสไฟล์

4. คลิก **Export**

> ***ข้อความที่สำคัญ:***
>
> *หากคุณต้องการส่งออกการตั้งค่าเครือข่ายของสแกนเนอร์ เช่น ชื่อสแกนเนอร์และที่อยู่ IP ให้เลือก **Enable to select the individual settings of device** และเลือกรายการอื่น ๆ ใช้เฉพาะค่าที่เลือกไว้สำหรับสแกนเนอร์เปลี่ยนแทนเท่านั้น*

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การนำเข้าการตั้งค่า

นำเข้าและส่งออกไฟล์ Web Config ไปยังสแกนเนอร์

> ***ข้อความที่สำคัญ:***
>
> *เมื่อนำเข้าค่าต่าง ๆ ที่มีข้อมูลของแต่ละเครื่อง เช่น ชื่อสแกนเนอร์หรือที่อยู่ IP ตรวจสอบให้แน่ใจว่าไม่มีที่อยู่ IP เดียวกันอยู่บนเครือข่ายเดียวกัน หากที่อยู่ IP เหลื่อมทับซ้อนกัน สแกนเนอร์จะไม่แสดงค่าออกมา*

1. เข้าถึง Web Config แล้วเลือก **Export and Import Setting Value** > **Import**

2. เลือกไฟล์ที่ส่งออกแล้ว จากนั้นป้อนรหัสผ่านที่เข้ารหัสไว้

3. คลิก **Next**
4. เลือกการตั้งค่าที่คุณต้องการนำเข้า จากนั้นคลิก **Next**
5. คลิก **OK**

การตั้งค่าถูกใช้กับสแกนเนอร์

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การแก้ไขปัญหา

ข้อแนะนำสำหรับการแก้ไขปัญหา

คุณสามารถค้นหาข้อมูลเพิ่มเติมได้ในคู่มือต่อไปนี้

❑ คู่มือผู้ใช้
ให้คำแนะนำในการใช้สแกนเนอร์ การบำรุงรักษา และการแก้ไขปัญหา

การตรวจสอบบันทึกสำหรับเซิร์ฟเวอร์และอุปกรณ์เครือข่าย

ในกรณีพบปัญหาการเชื่อมต่อเครือข่าย คุณอาจระบุสาเหตุโดยการยืนยันบันทึกรายการของเซิร์ฟเวอร์เมล เซิร์ฟเวอร์ LDAP ฯลฯ การตรวจสอบสถานะโดยใช้บันทึกรายการเครือข่ายจากบันทึกรายการอุปกรณ์ระบบและคำสั่ง เช่น เราเตอร์

การเตรียมเริ่มต้นการตั้งค่าเครือข่าย

การกู้คืนการตั้งค่าเครือข่ายจากแผงควบคุม

คุณสามารถเรียกคืนค่าการตั้งค่าเครือข่ายทั้งหมดไปยังค่าเริ่มต้นได้

1. แตะ **การตั้งค่า** บนหน้าจอหลัก
2. แตะที่ **การดูแลระบบ** > **คืนค่าการตั้งค่าเริ่มต้น** > **การตั้งค่าเครือข่าย**
3. ตรวจสอบข้อความ จากนั้นแตะที่ **ใช่**
4. เมื่อข้อความแจ้งการดำเนินการเสร็จสิ้นปรากฏขึ้น ให้แตะ **ปิด**
   หน้าจอจะปิดโดยอัตโนมัติหลังจากผ่านระยะเวลาหนึ่ง หากคุณไม่ได้แตะ **ปิด**

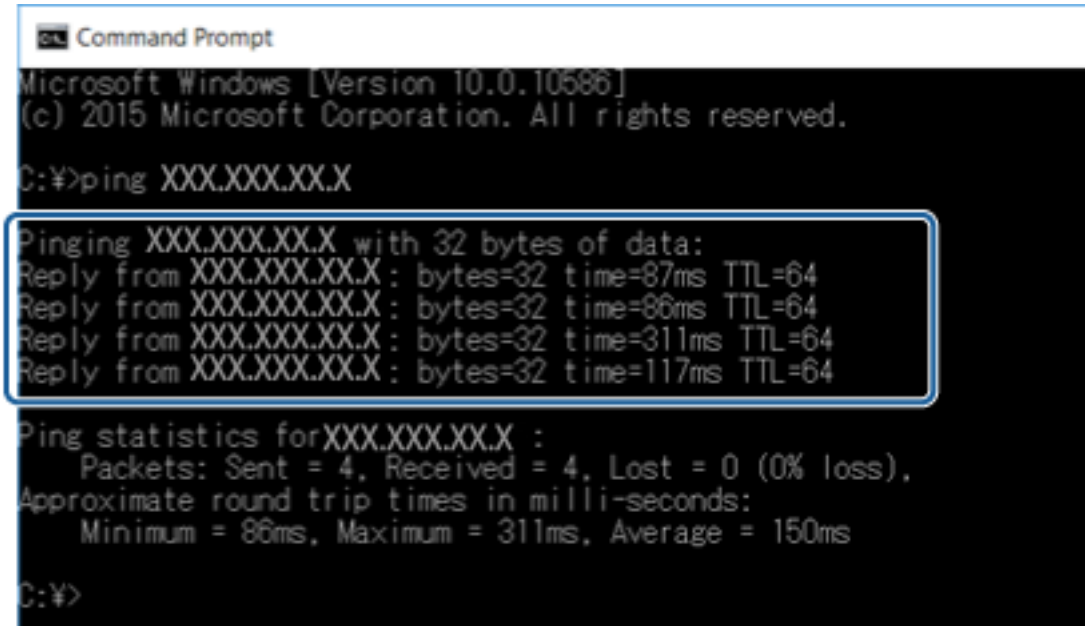
การตรวจสอบการสื่อสารระหว่างอุปกรณ์และคอมพิวเตอร์

การตรวจสอบการเชื่อมต่อโดยใช้คำสั่ง Ping (ปิง) — Windows

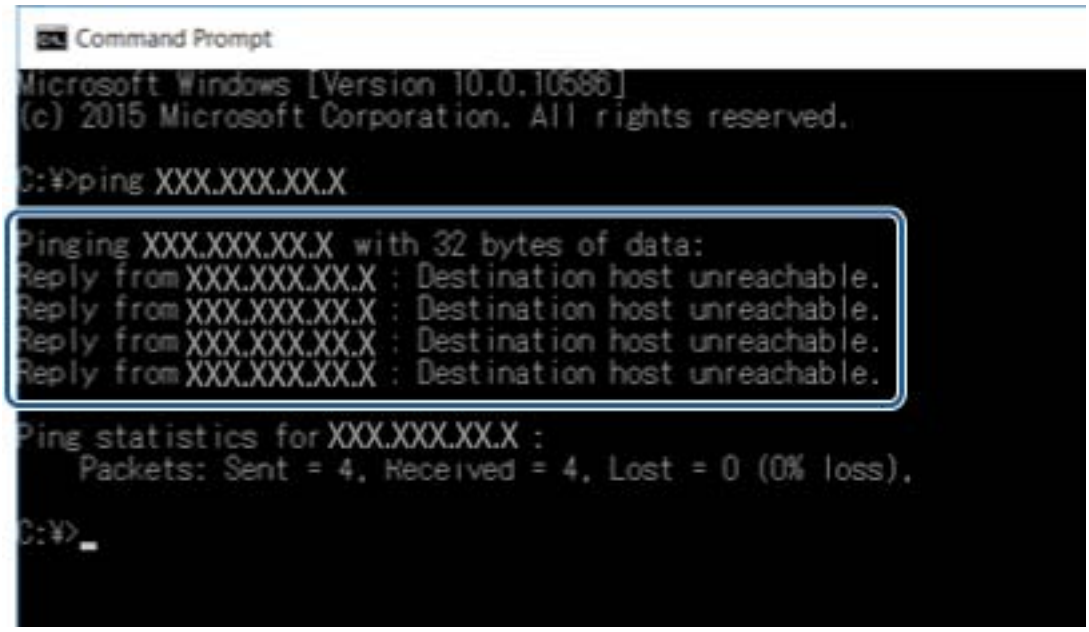
คุณสามารถใช้คำสั่ง Ping (ปิง) เพื่อตรวจสอบว่าคอมพิวเตอร์ของคุณเชื่อมต่อกับสแกนเนอร์แล้ว ทำตามขั้นตอนด้านล่างเพื่อตรวจสอบการเชื่อมต่อโดยใช้คำสั่ง Ping (ปิง)

การแก้ไขปัญหา

1. ตรวจสอบที่อยู่ IP ของสแกนเนอร์สำหรับการเชื่อมต่อที่คุณต้องการตรวจสอบ
   คุณสามารถตรวจสอบดังกล่าวโดยใช้ Epson Scan 2
2. แสดงหน้าจอพร้อมรับคำสั่งของคอมพิวเตอร์
   - ❏ Windows 10
     คลิกขวาที่ปุ่มเริ่มต้นหรือกดค้างไว้ จากนั้นเลือก **พร้อมรับคำสั่ง**
   - ❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012
     แสดงหน้าจอของแอพพลิเคชั่น จากนั้นเลือก **พร้อมรับคำสั่ง**
   - ❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 หรือรุ่นเก่ากว่า
     คลิกที่ปุ่มเริ่มต้น เลือกที่ **โปรแกรมทั้งหมด** หรือ **โปรแกรม** > **อุปกรณ์เสริม** > **พร้อมรับคำสั่ง**
3. ป้อนคำสั่ง "ping xxx.xxx.xxx.xxx" จากนั้นกดปุ่ม (Enter) ตกลง
   ป้อนที่อยู่ IP ของสแกนเนอร์ด้วยค่าแบบ xxx.xxx.xxx.xxx
4. ตรวจสอบสถานะของการสื่อสาร
   หากสแกนเนอร์และคอมพิวเตอร์สื่อสารกัน ข้อความต่อไปนี้จะปรากฏขึ้น



หากสแกนเนอร์และคอมพิวเตอร์ไม่สื่อสารกัน ข้อความต่อไปนี้จะปรากฏขึ้น



การตรวจสอบการเชื่อมต่อโดยใช้คำสั่ง Ping (ปิง) — Mac OS

คุณสามารถใช้คำสั่ง Ping (ปิง) เพื่อตรวจสอบว่าคอมพิวเตอร์ของคุณเชื่อมต่อกับสแกนเนอร์แล้ว ทำตามขั้นตอนด้านล่างเพื่อตรวจสอบการเชื่อมต่อโดยใช้คำสั่ง Ping (ปิง)

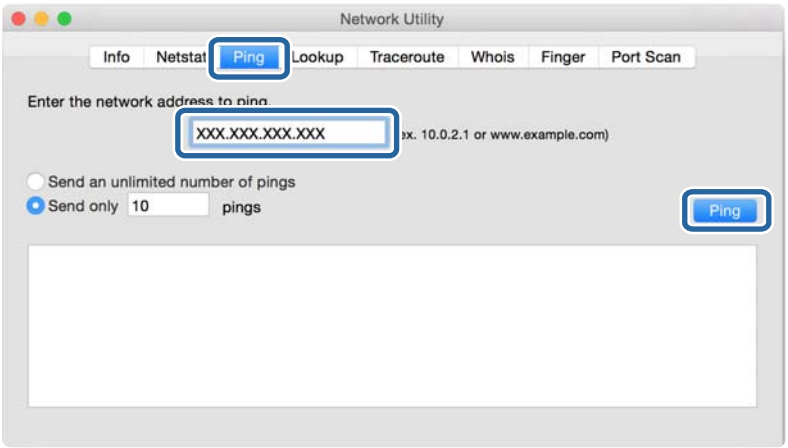
1. ตรวจสอบที่อยู่ IP ของสแกนเนอร์สำหรับการเชื่อมต่อที่คุณต้องการตรวจสอบ

   คุณสามารถตรวจสอบดังกล่าวโดยใช้ Epson Scan 2

2. เรียกใช้โปรแกรมยูทิลิตี้ของเครือข่าย

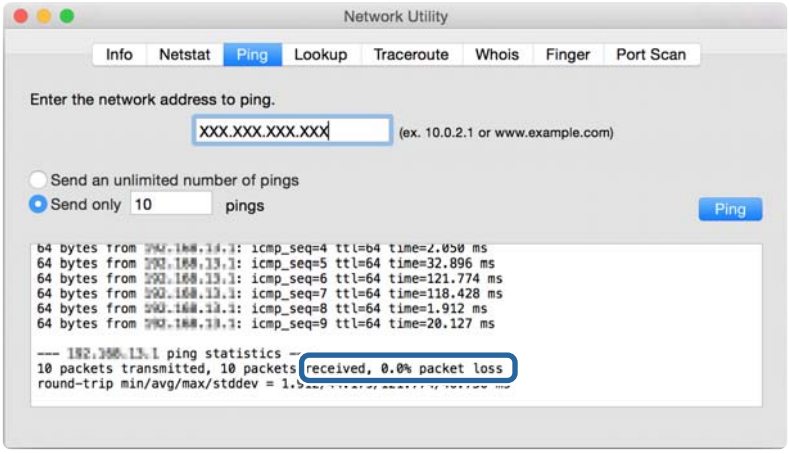
   ป้อนคำว่า "Network Utility" ลงไปใน **Spotlight**

3. คลิกที่แถบ **Ping** ป้อนค่าที่อยู่ IP ที่คุณทำการตรวจสอบในขั้นตอนที่ 1 จากนั้นให้คลิกที่ **Ping**

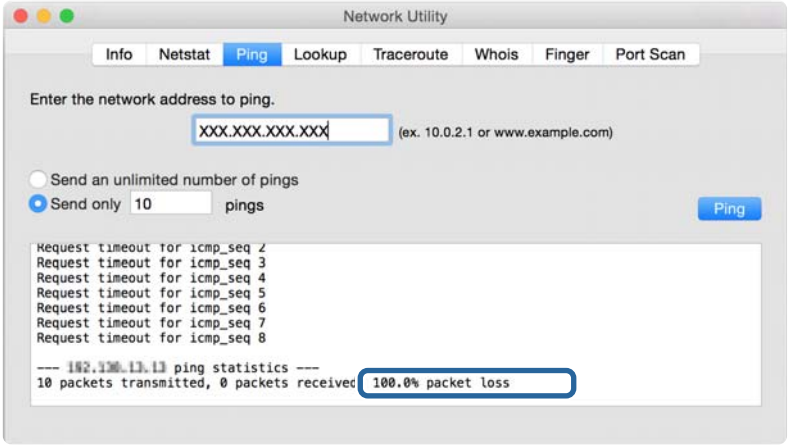


4. ตรวจสอบสถานะของการสื่อสาร

   หากสแกนเนอร์และคอมพิวเตอร์สื่อสารกัน ข้อความต่อไปนี้จะปรากฏขึ้น



   หากสแกนเนอร์และคอมพิวเตอร์ไม่สื่อสารกัน ข้อความต่อไปนี้จะปรากฏขึ้น



ปัญหาในการใช้ซอฟต์แวร์เครือข่าย

ไม่สามารถเข้าถึง Web Config

ได้กำหนดค่าที่อยู่ IP ของสแกนเนอร์เหมาะสมหรือไม่

กำหนดค่าที่อยู่ IP โดยใช้ Epson Device Admin หรือ EpsonNet Config

เบราเซอร์ของคุณรองรับการเข้ารหัสเป็นกลุ่มขนาดใหญ่เพื่อ Encryption Strength สำหรับ SSL/TLS หรือไม่

การเข้ารหัสเป็นกลุ่มขนาดใหญ่เพื่อ Encryption Strength สำหรับ SSL/TLS เป็นดังต่อไปนี้ Web Config สามารถเข้าถึงได้เฉพาะในเบราเซอร์ที่รองรับการเข้ารหัสเป็นกลุ่มขนาดใหญ่ต่อไปนี้ ตรวจสอบการรองรับการเข้ารหัสของเบราเซอร์ของคุณ

- ❑ 80 บิต: AES256/AES128/3DES
- ❑ 112 บิต: AES256/AES128/3DES

❑ 128 บิต: AES256/AES128

❑ 192 บิต: AES256

❑ 256 บิต: AES256

ข้อความ "หมดอายุ" ปรากฏขึ้นเมื่อเข้าถึง Web Config โดยใช้การสื่อสาร SSL (https)

หากใบรับรองหมดอายุ ให้ขอรับใบรับรองใหม่ หากข้อความปรากฏขึ้นก่อนวันหมดอายุ ตรวจสอบว่าวันที่ของสแกนเนอร์ได้ตั้งค่าไว้อย่างถูกต้อง

ข้อความ "ชื่อของใบรับรองความปลอดภัยไม่ตรงกัน…" ปรากฏขึ้นเมื่อเข้าถึง Web Config โดยใช้การสื่อสาร SSL (https)

ที่อยู่ IP ของสแกนเนอร์ที่ป้อนเข้าสำหรับ **Common Name** สำหรับการจัดสร้างใบรับรองแบบลงนามด้วยตัวเอง หรือ CSR ไม่ตรงกับที่อยู่ที่ป้อนเข้าไปในเบราเซอร์ ขอรับและนำเข้าใบรับรองอีกครั้งหรือเปลี่ยนชื่อสแกนเนอร์

สแกนเนอร์กำลังถูกเข้าถึงผ่านพร็อกซีเซิร์ฟเวอร์

หากคุณกำลังใช้พร็อกซีเซิร์ฟเวอร์กับสแกนเนอร์ของคุณ คุณจะต้องกำหนดค่าพร็อกซีของเบราเซอร์ของคุณ

❑ Windows:

เลือก **แผงควบคุม** > **เครือข่ายและอินเทอร์เน็ต** > **ตัวเลือกอินเทอร์เน็ต** > **การเชื่อมต่อ** > **การตั้งค่า LAN** > **พร็อกซีเซิร์ฟเวอร์** จากนั้นตั้งค่าพร็อกซีเซิร์ฟเวอร์สำหรับที่อยู่ภายในเครื่อง

❑ Mac OS:

เลือก **การกำหนดลักษณะของระบบ** > **เครือข่าย** > **ขั้นสูง** > **พร็อกซี** จากนั้นลงทะเบียนที่อยู่ภายในเครื่องสำหรับ **บายพาสการตั้งค่าพร็อกซีสำหรับโฮสต์และโดเมนเหล่านี้**

ตัวอย่าง:

192.168.1.*: ที่อยู่ภายในเครื่อง 192.168.1.XXX, ซับเน็ตมาส์ก 255.255.255.0

192.168.*.*: ที่อยู่ภายในเครื่อง 192.168.XXX.XXX, ซับเน็ตมาส์ก 255.255.0.0

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

➡ "การกำหนดที่อยู่ IP" บนหน้าที่ 15

➡ "การกำหนดที่อยู่ IP โดยใช้ EpsonNet Config" บนหน้าที่ 56

ชื่อรุ่นและ/หรือที่อยู่ IP ไม่แสดงผลใน EpsonNet Config

คุณได้เลือก บล็อค, ยกเลิก หรือ ปิดระบบ เมื่อหน้าจอความปลอดภัยหรือหน้าจอไฟร์วอลล์ Windows ปรากฏขึ้นหรือไม่

หากคุณเลือก **บล็อค**, **ยกเลิก** หรือ **ปิดระบบ** ที่อยู่ IP และชื่อรุ่นจะไม่ปรากฏขึ้นใน EpsonNet Config หรือ EpsonNet Setup

สำหรับการแก้ไข ให้ลงทะเบียน EpsonNet Config เป็นข้อยกเว้นโดยใช้ไฟร์วอลล์ Windows และซอฟต์แวร์ความปลอดภัยเชิงพาณิชย์ หากคุณใช้โปรแกรมป้องกันไวรัสหรือความปลอดภัย ให้ปิดโปรแกรมก่อน จากนั้นลองใช้ EpsonNet Config

การตั้งค่าหมดเวลาข้อผิดพลาดการสื่อสารน้อยเกินไปหรือไม่

เรียกใช้ EpsonNet Config แล้วเลือก **Tools** > **Options** > **Timeout**, จากนั้นเพิ่มระยะเวลาสำหรับการตั้งค่า **Communication Error** พึงทราบว่าการกระทำดังกล่าวสามารถเป็นสาเหตุให้ EpsonNet Config ทำงานช้าลงอีก

ข้อมูลที่เกี่ยวข้อง

➡ "การเรียกใช้ EpsonNet Config — Windows" บนหน้าที่ 56
➡ "การเรียกใช้ EpsonNet Config — Mac OS" บนหน้าที่ 56

ภาคผนวก

การแนะนำซอฟต์แวร์เครือข่าย

ต่อไปนี้อธิบายถึงซอฟต์แวร์ที่กำหนดค่าและจัดการอุปกรณ์

Epson Device Admin

Epson Device Admin เป็นโปรแกรมที่ช่วยให้คุณสามารถติดตั้งอุปกรณ์บนเครือข่าย จากนั้นกำหนดค่าและจัดการอุปกรณ์ได้ คุณสามารถได้รับข้อมูลละเอียดสำหรับอุปกรณ์ เช่น สถานะและวัสดุสิ้นเปลือง การแจ้งเตือนการส่ง และสร้างรายงานการใช้งานอุปกรณ์ นอกจากนี้ คุณยังสามารถจัดทำแม่แบบที่ประกอบด้วยรายการการตั้งค่าและใช้งานกับอุปกรณ์อื่น ๆ เป็นการตั้งค่าแบบแชร์ร่วมกัน คุณสามารถดาวน์โหลด Epson Device Admin ได้จากเว็บไซต์สนับสนุนของ Epson สำหรับข้อมูลเพิ่มเติม สามารถดูที่เอกสารสนับสนุนหรือวิธีใช้ของ Epson Device Admin

การเรียกใช้ Epson Device Admin (Windows เท่านั้น)

เลือก **โปรแกรมทั้งหมด** > **EPSON** > **Epson Device Admin** > **Epson Device Admin**

หมายเหตุ:
หากมีการแจ้งเตือนไฟร์วอลล์เกิดขึ้น ให้อนุญาตเข้าถึง Epson Device Admin

EpsonNet Config

EpsonNet Config ช่วยให้ผู้ดูแลระบบสามารถกำหนดค่าการตั้งค่าเครือข่ายของสแกนเนอร์ เช่น การกำหนดที่อยู่ IP และการเปลี่ยนแปลงโหมดการเชื่อมต่อ คุณสมบัติการตั้งค่าแบบชุดรองรับได้กับ Windows สำหรับข้อมูลเพิ่มเติม สามารถดูที่เอกสารสนับสนุนหรือวิธีใช้ของ EpsonNet Config

การเรียกใช้ EpsonNet Config — Windows

เลือก **โปรแกรมทั้งหมด** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**

หมายเหตุ:
หากมีการแจ้งเตือนไฟร์วอลล์เกิดขึ้น ให้อนุญาตเข้าถึง EpsonNet Config

การเรียกใช้ EpsonNet Config — Mac OS

เลือก **ไป** > **แอพพลิเคชั่น** > **Epson Software** > **EpsonNet** > **EpsonNet Config SE** > **EpsonNet Config**

EpsonNet SetupManager

EpsonNet SetupManager เป็นซอฟต์แวร์ที่ใช้สร้างแพคเกจสำหรับการติดตั้งสแกนเนอร์อย่างง่าย เช่น การติดตั้งและการกำหนดค่าไดร์เวอร์สแกนเนอร์ และการติดตั้ง Document Capture Pro ซอฟต์แวร์นี้ช่วยให้ผู้ดูแลระบบสามารถจัดสร้างแพคเกจซอฟต์แวร์แบบหนึ่งเดียวและแจกจ่ายไปยังกลุ่ม

สำหรับข้อมูลเพิ่มเติม สามารถเข้าไปที่เว็บไซต์ Epson ระดับภูมิภาคของคุณ

การกำหนดที่อยู่ IP โดยใช้ EpsonNet Config

คุณสามารถกำหนดที่อยู่ IP ให้กับสแกนเนอร์โดยใช้ EpsonNet Config EpsonNet Config ช่วยให้คุณสามารถกำหนดค่าที่อยู่ IP ให้กับสแกนเนอร์ที่ยังไม่ได้กำหนดค่าหลังจากเชื่อมต่อโดยใช้สายอีเธอร์เน็ต

การกำหนดที่อยู่ IP โดยใช้การตั้งค่าแบบชุด

การสร้างไฟล์สำหรับการตั้งค่าแบบชุด

การใช้ที่อยู่ MAC และชื่อรุ่นเป็นคีย์ คุณสามารถสร้างไฟล์ SYLK ใหม่เพื่อตั้งค่าที่อยู่ IP

1. เปิดแอปพลิเคชันสเปรดชีต (เช่น Microsoft Excel) หรือโปรแกรมตัวแก้ไขข้อความ
2. ป้อน "Info_MACAddress", "Info_ModelName" และ "TCPIP_IPAddress" ในแถวแรกที่เป็นชื่อรายการการตั้งค่า

   ป้อนรายการการตั้งค่าสำหรับสตริงข้อความต่อไปนี้ สำหรับการแยกความแตกต่างระหว่างตัวอักษรพิมพ์ใหญ่และพิมพ์เล็ก และอักขระไบต์คู่/ไวต์เดี่ยว หากมีตัวอักขระเดียวเท่านั้นที่ต่างกัน ระบบจะไม่รู้จักรายการ

   ป้อนชื่อรายการการตั้งค่าตามที่อธิบายด้านล่าง มิฉะนั้น EpsonNet Config จะไม่รู้จักรายการการตั้งค่า

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. ป้อนที่อยู่ MAC ชื่อรุ่น และที่อยู่ IP สำหรับแต่ละอินเทอร์เฟสเครือข่าย

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

0000XXXX0001	ALC-XXXXX	192.168.100.102
0000XXXX0002	ALC-XXXXX	192.168.100.103
0000XXXX0003	ALC-XXXXX	192.168.100.104

4. ป้อนชื่อและบันทึกเป็นไฟล์ SYLK (*.slk)

การตั้งค่าแบบชุดโดยใช้ไฟล์การกำหนดค่า

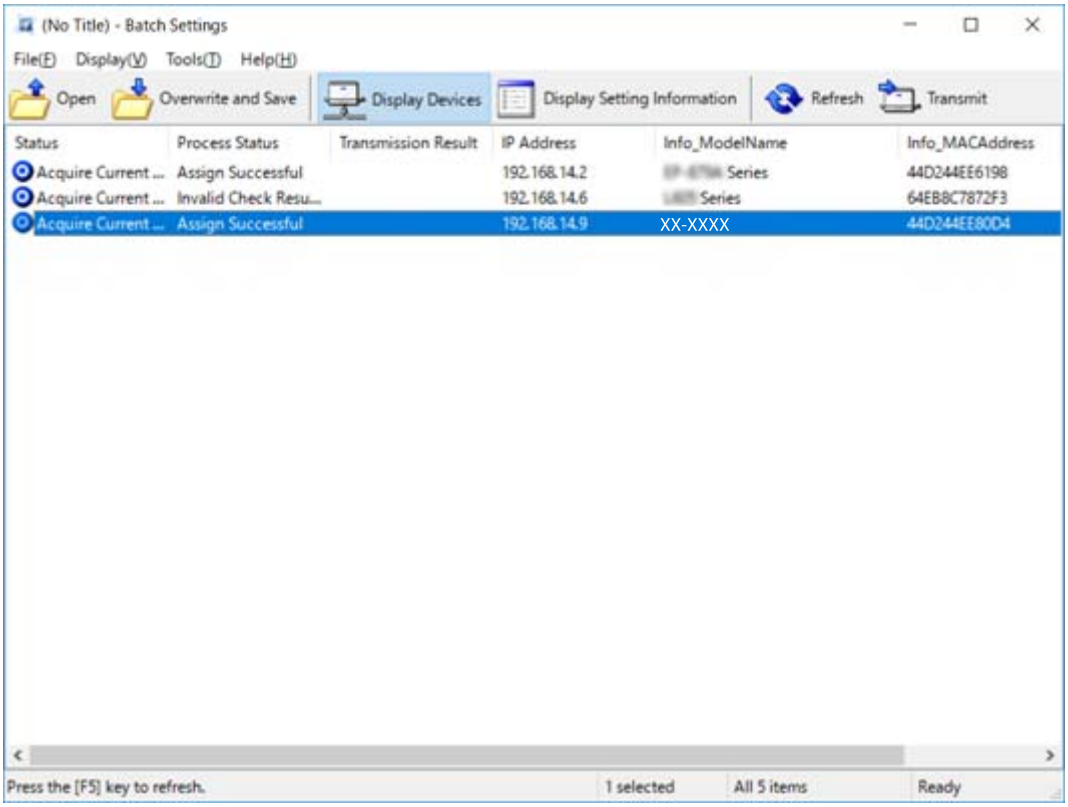
กำหนดที่อยู่ IP ในไฟล์การกำหนดค่า (ไฟล์ SYLK) หนึ่งครั้ง คุณจะต้องสร้างไฟล์การกำหนดค่าขึ้นมาก่อนจะกำหนดค่าได้

1. เชื่อมต่ออุปกรณ์ทั้งหมดเข้ากับเครือข่ายโดยใช้สายอีเธอร์เน็ต
2. เปิดสแกนเนอร์
3. เริ่มต้น EpsonNet Config

   รายการของสแกนเนอร์บนเครือข่ายจะแสดงขึ้นมา อาจใช้เวลาชั่วครู่ก่อนที่จะแสดงขึ้นมา
4. คลิกที่ **Tools** > **Batch Settings**
5. คลิกที่ **Open**
6. จากหน้าจากการเลือก ให้เลือกไฟล์ SYLK (*.slk) ที่มีการตั้งค่าข้างใน จากนั้นคลิก **Open**

7. เลือกอุปกรณ์ที่คุณต้องการทำการตั้งค่าแบบชุดโดยคอลัมน์ **Status** ตั้งค่าไปที่ **Unassigned** และ **Process Status** ตั้งค่าไปที่ **Assign Successful**

   เมื่อทำการเลือกหลายรายการ ให้กดปุ่ม Ctrl หรือ Shift แล้วเลือกหรือลากเมาส์ของคุณ



8. คลิกที่ **Transmit**

9. เมื่อหน้าจอป้อนรหัสผ่านปรากฏขึ้น ให้ป้อนรหัสผ่าน จากนั้นคลิก **OK**

   การตั้งค่าการส่งข้อมูล

> ***ข้อความที่สำคัญ:***
>
> *ข้อมูลจะถูกส่งไปยังอินเทอร์เฟสของเครือข่ายจนกว่ามิเตอร์วัดความคืบหน้าจะสิ้นสุด อย่าปิดอุปกรณ์หรืออะแดปเตอร์ไร้สาย และอย่าส่งข้อมูลใด ๆ ไปยังอุปกรณ์*

10. บนหน้าจอ **Transmitting Settings** คลิก **OK**

11. ตรวจสอบสถานะของอุปกรณ์ที่คุณตั้งค่า

สำหรับอุปกรณ์ที่แสดง หรือ ให้ตรวจสอบเนื้อหาของไฟล์การตั้งค่า หรือที่อุปกรณ์ได้รีบูทโดยปกติ

ไอคอน	Status	Process Status	คำอธิบาย
	Setup Complete	Setup Successful	ตั้งค่าสำเร็จสมบูรณ์
	Setup Complete	Rebooting	เมื่อข้อมูลถูกส่งผ่าน อุปกรณ์แต่ละตัวจะต้องรีบูทเพื่อเปิดใช้งานการตั้งค่า ระบบทำการตรวจสอบเพื่อตรวจหาว่าอุปกรณ์สามารถเชื่อมต่อหลังจากการรีบูทหรือไม่
	Setup Complete	Reboot Failed	ไม่สามารถยืนยันอุปกรณ์หลังจากการตั้งค่าการส่งข้อมูล ตรวจสอบว่าได้เปิดอุปกรณ์ไว้ หรืออุปกรณ์รีบูทอย่างถูกต้องหรือไม่
	Setup Complete	Searching	การค้นหาอุปกรณ์ที่ระบุในไฟล์การตั้งค่า*
	Setup Complete	Search Failed	ไม่สามารถตรวจหาอุปกรณ์ที่ได้ตั้งค่าไว้แล้ว ตรวจสอบว่าได้เปิดอุปกรณ์ไว้ หรืออุปกรณ์รีบูทอย่างถูกต้องหรือไม่*

* เฉพาะเมื่อข้อมูลการตั้งค่าแสดงขึ้นมาเท่านั้น

ข้อมูลที่เกี่ยวข้อง

➡ "การเรียกใช้ EpsonNet Config — Windows" บนหน้าที่ 56
➡ "การเรียกใช้ EpsonNet Config — Mac OS" บนหน้าที่ 56

การกำหนดที่อยู่ IP ให้กับแต่ละอุปกรณ์

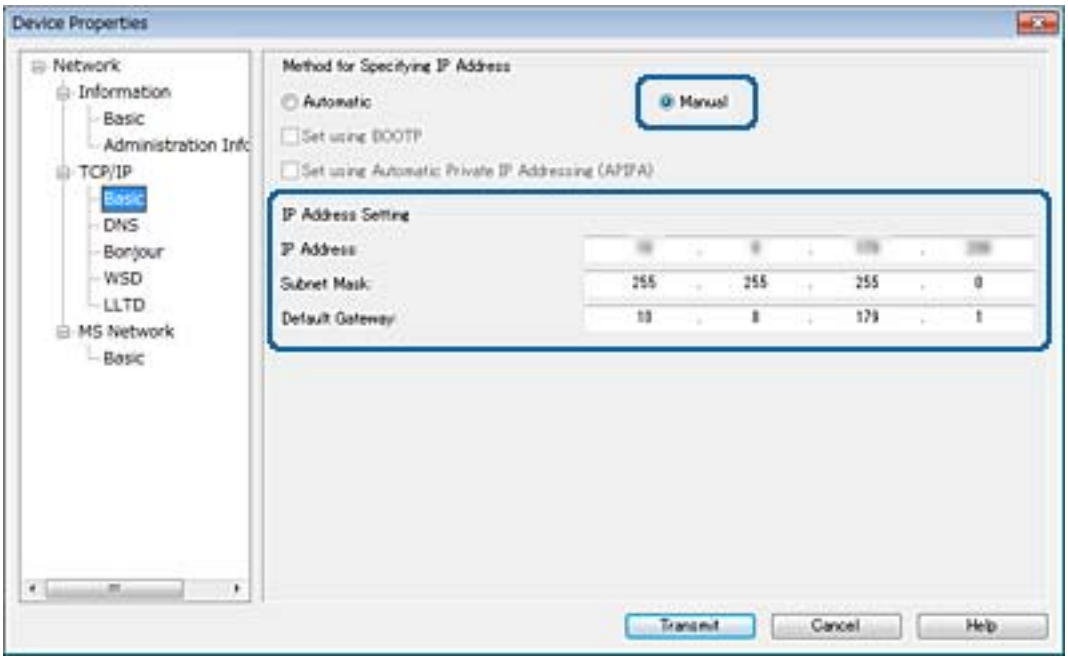
กำหนดที่อยู่ IP ให้กับสแกนเนอร์โดยใช้ EpsonNet Config

1. เปิดสแกนเนอร์
2. เชื่อมต่อสแกนเนอร์เข้ากับเครือข่ายโดยใช้สายอีเธอร์เน็ต
3. เริ่มต้น EpsonNet Config

   รายการของสแกนเนอร์บนเครือข่ายจะแสดงขึ้นมา อาจใช้เวลาชั่วครู่ก่อนที่จะแสดงขึ้นมา
4. ดับเบิลคลิกสแกนเนอร์ที่คุณต้องการกำหนดค่า

   หมายเหตุ:
   หากคุณเชื่อมต่อหลายสแกนเนอร์รุ่นเดียวกัน คุณสามารถระบุเครื่องพิมพ์โดยใช้ที่อยู่ MAS
5. เลือก **Network** > **TCP/IP** > **Basic**

6. ป้อนที่อยู่สำหรับ **IP Address**, **Subnet Mask** และ **Default Gateway**



หมายเหตุ:
ป้อนที่อยู่แบบคงที่เมื่อคุณเชื่อมต่อสแกนเนอร์เข้ากับเครือข่ายที่ปลอดภัยเครือข่ายหนึ่ง

7. คลิกที่ **Transmit**

   หน้าจอยืนยันการส่งข้อมูลจะปรากฏขึ้น

8. คลิกที่ **OK**

   หน้าจอการส่งข้อมูลเสร็จสมบูรณ์จะแสดงขึ้นมา

   หมายเหตุ:
   ข้อมูลถูกส่งไปที่อุปกรณ์ จากนั้นข้อความ "กำหนดค่าเสร็จสมบูรณ์" จะปรากฏขึ้น อย่าปิดอุปกรณ์ และอย่าส่งข้อมูลใด ๆ ไปยังบริการ

9. คลิกที่ **OK**

ข้อมูลที่เกี่ยวข้อง

➡ "การเรียกใช้ EpsonNet Config — Windows" บนหน้าที่ 56
➡ "การเรียกใช้ EpsonNet Config — Mac OS" บนหน้าที่ 56

การใช้พอร์ตสำหรับสแกนเนอร์

สแกนเนอร์ใช้พอร์ตดังต่อไปนี้ พอร์ตเหล่านี้จะต้องอนุญาตให้สามารถใช้งานได้โดยผู้ดูแลระบบเครือข่ายตามที่จำเป็น

ภาคผนวก

ผู้ส่ง (ไคลเอ็นต์)	ใช้	ปลายทาง (เซิร์ฟเวอร์)	โปรโตคอล	หมายเลขพอร์ต
สแกนเนอร์	การส่งอีเมล (การแจ้งเตือนทางอีเมล)	เซิร์ฟเวอร์ SMTP	SMTP (TCP)	25
			SMTP SSL/TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	POP ก่อนการเชื่อมต่อ SMTP (การแจ้งเตือนทางอีเมล	เซิร์ฟเวอร์ POP	POP3 (TCP)	110
	WSD ควบคุม	คอมพิวเตอร์ไคลเอ็นต์	WSD (TCP)	5357
	ค้นหาคอมพิวเตอร์เมื่อสแกนแบบดันจาก Document Capture Pro	คอมพิวเตอร์ไคลเอ็นต์	การค้นหาการสแกนแบบดันผ่านเครือข่าย	2968
	การรวบรวมข้อมูลงานเมื่อสแกนแบบดันจาก Document Capture Pro	คอมพิวเตอร์ไคลเอ็นต์	การสแกนแบบดันผ่านเครือข่าย	2968
คอมพิวเตอร์ไคลเอ็นต์	ค้นหาสแกนเนอร์จากแอปพลิเคชัน เช่น EpsonNet Config ไดรเวอร์สแกนเนอร์	สแกนเนอร์	ENPC (UDP)	3289
	รวบรวมข้อมูลและตั้งค่าข้อมูล MIB จากแอปพลิเคชัน เช่น EpsonNet Config และไดรเวอร์สแกนเนอร์	สแกนเนอร์	SNMP (UDP)	161
	การค้นหาสแกนเนอร์ WSD	สแกนเนอร์	WS-Discovery (UDP)	3702
	การส่งต่อข้อมูลสแกนจาก Document Capture Pro	สแกนเนอร์	การสแกนผ่านเครือข่าย (TCP)	1865

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

ในบทนี้ อธิบายถึงคุณสมบัติความปลอดภัยขั้นสูง

การตั้งค่าความปลอดภัยและการป้องกันอันตราย

หากอุปกรณ์เชื่อมต่ออยู่กับเครือข่าย คุณสามารถเข้าถึงได้จากสถานที่ตั้งระยะไกล นอกจากนี้ หลายบุคคลสามารถแชร์อุปกรณ์ร่วมกัน ซึ่งมีประโยชน์ในการปรับปรุงประสิทธิภาพการทำงานและความสะดวก อย่างไรก็ดี ความเสี่ยงอย่างเช่น การเข้าถึงอย่างไม่ถูกต้องตามกฎระเบียบ การใช้งานที่ไม่ถูกต้องตามกฎระเบียบ และการปลอมแปลงข้อมูลจะเพิ่มขึ้นได้ หากคุณใช้งานอุปกรณในสภาพแวดล้อมที่คุณสามารถเข้าถึงอินเทอร์เน็ตได้ ความเสี่ยงก็จะสูงขึ้นด้วย

เพื่อที่จะหลีกเลี่ยงความเสี่ยงดังกล่าว อุปกรณ์ Epson มีหลากหลายเทคโนโลยีความปลอดภัยที่นำมาใช้

ตั้งค่าอุปกรณ์ตามที่จำเป็นโดยสอดคล้องกับเงื่อนไขแวดล้อมที่ถูกสร้างขึ้นพร้อมกับข้อมูลสภาพแวดล้อมของลูกค้า

ชื่อ	ประเภทคุณสมบัติ	สิ่งที่จะตั้งค่า	สิ่งที่จะป้องกัน
การสื่อสาร SSL/TLS	เส้นทางการสื่อสารของคอมพิวเตอร์และอุปกรณ์ถูกเข้ารหัสโดยใช้การสื่อสาร SSL/TLS เนื้อหาของการสื่อสารผ่านเบราเซอร์ได้รับการปกป้อง	ตั้งค่าใบรับรอง CA สำหรับเซิร์ฟเวอร์ที่ได้มีลงนามรับรองโดย CA (หน่วยงานออกใบรับรอง) ให้กับอุปกรณ์	ป้องกันการรั่วไหลของข้อมูลการตั้งค่าและเนื้อหาของข้อมูลที่ถ่ายโอนไปหาเครื่องพิมพ์จากเครื่องสแกนเนอร์ การเข้าถึงเซิร์ฟเวอร์ Epson บนอินเทอร์เน็ตจากอุปกรณ์ยังสามารถได้รับการป้องกันโดยใช้การอัปเดตเฟิร์มแวร์ ฯลฯ
การกรอง IPsec/IP	คุณสามารถตั้งค่าให้อนุญาตการนำมาและการตัดข้อมูลที่มาจากบางเครื่องไคลเอ็นต์ หรือประเภทพิเศษเฉพาะ เมื่อ IPsec ให้การป้องกันข้อมูลโดยชุดแพกเกต IP (การเข้ารหัสและการตรวจรับรองความถูกต้อง) คุณสามารถสื่อสารโปรโตคอลการสแกนที่ไม่ปลอดภัยได้อย่างปลอดภัย	สร้างนโยบายพื้นฐานและนโยบายเฉพาะเครื่องเพื่อตั้งค่าไคลเอ็นต์หรือประเภทของข้อมูลที่สามารถเข้าถึงอุปกรณ์ได้	ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการทำปลอมแปลงและการดักข้อมูลของการสื่อสารข้อมูลไปยังอุปกรณ์
SNMPv3	คุณสมบัติได้รับการเพิ่มเข้า เช่น การเฝ้าตรวจตราอุปกรณ์ที่เชื่อมต่อในเครือข่าย ความสมบูรณ์ของข้อมูลที่ไปยังโปรโตคอล SNMP เพื่อการควบคุม การเข้ารหัส การตรวจรับรองความถูกต้องผู้ใช้ ฯลฯ	เปิดใช้งาน SNMPv3 จากนั้นตั้งค่าวิธีการตรวจรับรองความถูกต้อง และการเข้ารหัส	ตรวจสอบให้มั่นใจว่าได้เปลี่ยนแปลงการตั้งค่าผ่านเครือข่าย การรักษาความลับในการเฝ้าตรวจตราสถานะ
IEEE802.1X	อนุญาตเฉพาะผู้ใช้ที่ได้รับการตรวจรับรองแล้วเข้าถึงอีเธอร์เน็ตที่จะเชื่อมต่อ อนุญาตเฉพาะผู้ใช้ที่ได้รับอนุญาตแล้วเพื่อเข้าใช้อุปกรณ์	การตั้งค่าการตรวจรับรองความถูกต้องให้กับเซิร์ฟเวอร์ RADIUS (เซิร์ฟเวอร์การตรวจรับรองความถูกต้อง)	ป้องกันการเข้าถึงและการใช้งานอุปกรณ์โดยไม่ได้รับอนุญาต

ชื่อ	ประเภทคุณสมบัติ	สิ่งที่จะตั้งค่า	สิ่งที่จะป้องกัน
อ่านการ์ดไอดี	คุณสามารถใช้อุปกรณ์โดยการเลื่อนไปยังการ์ดไอดีเข้ากับอุปกรณ์การตรวจรับรองความถูกต้องที่เชื่อมต่ออยู่ด้วย คุณสามารถจำกัดการได้รับบันทึกสำหรับผู้ใช้แต่ละรายและอุปกรณ์แต่ละเครื่อง และจำกัดการใช้งานที่พร้อมบริการของอุปกรณ์ และคุณสมบัติที่พร้อมบริการของแต่ละผู้ใช้และกลุ่ม	เชื่อมต่ออุปกรณ์การตรวจรับรองความถูกต้องเข้ากับอุปกรณ์ จากนั้นตั้งค่าข้อมูลผู้ใช้ในระบบการตรวจรับรองความถูกต้อง	ป้องกันการใช้งานโดยไม่ได้รับอนุญาต และการปลอมตัวตนของอุปกรณ์

ข้อมูลที่เกี่ยวข้อง

➡ "การสื่อสาร SSL/TLS กับสแกนเนอร์" บนหน้าที่ 63
➡ "การเข้ารหัสการสื่อสารโดยใช้การกรอง IPsec/IP" บนหน้าที่ 71
➡ "การใช้โปรโตคอล SNMPv3" บนหน้าที่ 82
➡ "การเชื่อมต่อสแกนเนอร์เข้ากับเครือข่าย IEEE802.1X" บนหน้าที่ 84

การตั้งค่าคุณสมบัติความปลอดภัย

เมื่อตั้งค่าการกรอง IPsec/IP หรือ IEEE802.1X ขอแนะนำให้คุณเข้าไปที่ Web Config โดยใช้ SSL/TLS เพื่อสื่อสารข้อมูลการตั้งค่าเพื่อที่จะลดความเสี่ยงด้านความปลอดภัย เช่น การทำปลอมแปลง หรือการดักข้อมูล

การสื่อสาร SSL/TLS กับสแกนเนอร์

หากตั้งค่าใบรับรองซิร์ฟเวอร์โดยใช้การสื่อสาร SSL/TLS (Secure Sockets Layer/Transport Layer Security) ให้กับสแกนเนอร์ คุณสามารถเข้ารหัสเส้นทางการสื่อสารระหว่างคอมพิวเตอร์ต่าง ๆ ทำดังต่อไปนี้ หากคุณต้องการป้องกันการเข้าถึงจากระยะไกลและโดยไม่ได้รับอนุญาต

เกี่ยวกับใบรับรองดิจิตัล

❑ ใบรับรองที่ลงนามจาก CA

ใบรับรองที่ลงนามจาก CA (Certificate Authority) จะต้องได้มาจากผู้ให้บริการออกใบรับรองเท่านั้น คุณสามารถมั่นใจในการสื่อสารที่มีความปลอดภัยโดยการใช้ใบรับรองที่ลงนามจาก CA คุณสามารถใช้ใบรับรองที่ลงนามจาก CA สำหรับแต่ละคุณสมบัติด้านความปลอดภัย

❑ ใบรับรอง CA

ใบรับรอง CA บ่งบอกว่าบริษัทผู้ให้บริการบุคคลภายนอกได้ตรวจสอบข้อมูลเฉพาะตัวของเซิร์ฟเวอร์แล้ว นี่เป็นองค์ประกอบหลักในรูปแบบที่เชื่อถือได้ทางเว็บในด้านความปลอดภัย คุณจะต้องขอรับใบรับรอง CA สำหรับการยืนยันเซิร์ฟเวอร์ที่ออกให้โดย CA

❑ ใบรับรองที่ลงนามด้วยตัวเอง

ใบรับรองที่ลงนามด้วยตัวเองเป็นใบรับรองที่สแกนเนอร์พิมพ์ออกและลงนามด้วยตัวเอง ใบรับรองนี้ไม่น่าเชื่อถือและไม่สามารถหลีกเลี่ยงการปลอมแปลง หากคุณใช้ใบรับรองนี้เป็นใบรับรอง SSL/TLS อาจมีการแจ้งเตือนความปลอดภัยบนเบราเซอร์ของคุณ คุณสามารถใช้ใบรับรองนี้เฉพาะสำหรับการสื่อสาร SSL/TLS เท่านั้น

ข้อมูลที่เกี่ยวข้อง

➡ "การขอรับและการนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 64
➡ "การลบใบรับรองที่ลงนามจาก CA" บนหน้าที่ 67
➡ "การอัพเดตใบรับรองที่ลงนามด้วยตัวเอง" บนหน้าที่ 68

การขอรับและการนำเข้าใบรับรองที่ลงนามจาก CA

การขอรับใบรับรองที่ลงนามจาก CA

สำหรับการขอรับใบรับรองที่ลงนามจาก CA ให้สร้าง CSR (คำร้องขอการลงนามใบรับรอง) และใช้งานกับหน่วยงานออกใบรับรอง คุณสามารถสร้าง CSR โดยใช้ Web Config และคอมพิวเตอร์

ทำตามขั้นตอนต่าง ๆ เพื่อสร้าง CSR และขอรับใบรับรองที่ลงนามจาก CA โดยใช้ Web Config เมื่อจัดสร้าง CSR โดยใช้ Web Config รูปแบบใบรับรองจะเป็นแบบ PEM/DER

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** จากนั้น เลือก **SSL/TLS** > **Certificate** หรือ **IPsec/IP Filtering** > **Client Certificate** หรือ **IEEE802.1X** > **Client Certificate**

2. คลิก **Generate** ของ **CSR**

   หน้าการสร้าง CSR จะเปิดขึ้นมา

3. ป้อนค่าสำหรับแต่ละรายการ

   หมายเหตุ:
   ความยาวคีย์ที่ใช้งานได้และคำย่อจะแปรผันตามแต่ละผู้ให้บริการออกใบรับรอง สร้างคำร้องของโดยสอดคล้องกับกฎเกณฑ์ของแต่ละผู้ให้บริการออกใบรับรอง

4. คลิก **OK**

   ข้อความยืนยันสำเร็จจะแสดงขึ้นมา

5. เลือก **Network Security Settings** จากนั้น เลือก **SSL/TLS** > **Certificate** หรือ **IPsec/IP Filtering** > **Client Certificate** หรือ **IEEE802.1X** > **Client Certificate**

6. คลิกปุ่มดาวน์โหลดหนึ่งใดจาก **CSR** ตามรูปแบบที่กำหนดไว้โดยแต่ละผู้ให้บริการออกใบรับรองเพื่อดาวน์โหลด CSR ไปยังคอมพิวเตอร์

   > ***ข้อความที่สำคัญ:***
   > *อย่าสร้าง CSR ซ้ำอีกครั้ง หากคุณกระทำดังกล่าว คุณอาจไม่สามารถนำเข้า CA-signed Certificate ที่ออกให้แล้ว*

7. ส่ง CSR ไปยังผู้ให้บริการออกใบรับรองและขอรับ CA-signed Certificate

   ทำตามกฎเกณฑ์วิธีการส่งและแบบฟอร์มของแต่ละผู้ให้บริการออกใบรับรอง

8. บันทึก CA-signed Certificate ไว้ในคอมพิวเตอร์ที่เชื่อมต่อกับสแกนเนอร์

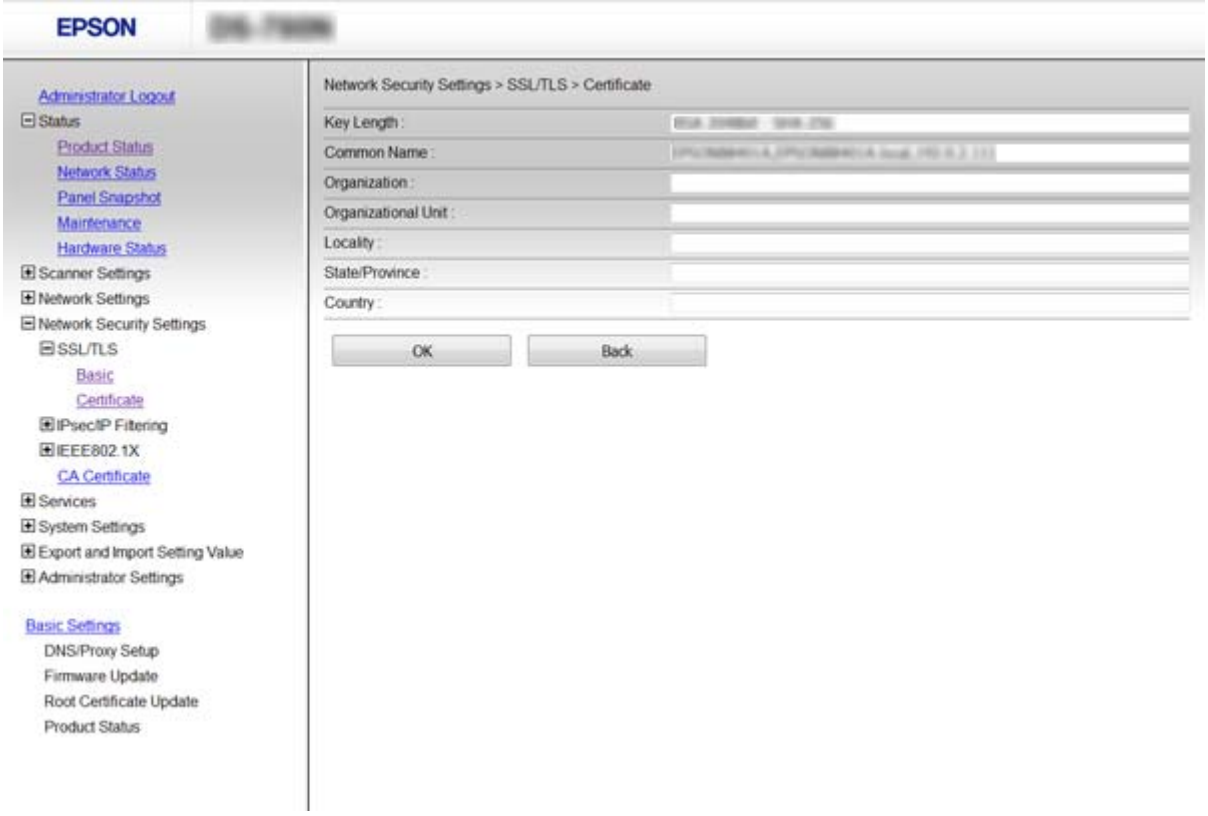
   การขอรับ CA-signed Certificate เสร็จสมบูรณ์เมื่อคุณบันทึกใบรับรองไปที่ปลายทางจัดเก็บ

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

➡ "รายการการตั้งค่า CSR" บนหน้าที่ 65
➡ "การนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 66

รายการการตั้งค่า CSR



รายการ	การตั้งค่าและคำอธิบาย
Key Length	เลือกความยาวคีย์สำหรับ CSR
Common Name	คุณสามารถป้อนระหว่าง 1 และ 128 ตัวอักขระ หากเป็นที่อยู่ IP จะต้องเป็นที่อยู่ IP แบบคงที่ ตัวอย่าง: URL สำหรับการเข้าถึง Web Config: https://10.152.12.225 ชื่อทั่วไป: 10.152.12.225
Organization/ Organizational Unit/ Locality/ State/Province	คุณสามารถป้อนระหว่าง 0 และ 64 ตัวอักขระในแบบ ASCII (0x20–0x7E) คุณสามารถแบ่งส่วนชื่อด้วยเครื่องหมายจุลภาค
Country	ป้อนรหัสประเทศด้วยตัวเลขสองหลักที่กำหนดไว้ด้วยมาตรฐาน ISO-3166

ข้อมูลที่เกี่ยวข้อง

➡ "การขอรับใบรับรองที่ลงนามจาก CA" บนหน้าที่ 64

การนำเข้าใบรับรองที่ลงนามจาก CA

ข้อความที่สำคัญ:

- *ตรวจสอบว่าได้ตั้งค่าวันที่และเวลาของสแกนเนอร์อย่างถูกต้อง*
- *หากคุณได้รับใบรับรองโดยใช้ CSR ที่สร้างจาก Web Config คุณสามารถนำเข้าใบรับรองได้อีกครั้ง*

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** จากนั้น เลือก **SSL/TLS** > **Certificate** หรือ **IPsec/IP Filtering** > **Client Certificate** หรือ **IEEE802.1X** > **Client Certificate**

2. คลิก **Import**

   หน้าที่นำเข้าใบรับรองจะเปิดขึ้นมา

3. ป้อนค่าสำหรับแต่ละรายการ

   การตั้งค่าที่จำเป็นอาจแปรผันทั้งนี้ขึ้นอยู่กับแหล่งที่คุณสร้าง CSR ขึ้นมา และรูปแบบไฟล์ของใบรับรอง ป้อนค่าต่างๆ ไปยังรายการที่จำเป็นโดยสอดคล้องดังต่อไปนี้

   - ใบรับรองรูปแบบ PEM/DER ที่ได้รับมาจาก Web Config
     - **Private Key**: ไม่ต้องกำหนดค่าเนื่องจากสแกนเนอร์มีคีย์ส่วนตัว
     - **Password**: ไม่ต้องกำหนดค่า
     - **CA Certificate 1**/**CA Certificate 2**: ตัวเลือกเสริม
   - ใบรับรองรูปแบบ PEM/DER ที่ได้รับมาจากคอมพิวเตอร์
     - **Private Key**: คุณจะต้องตั้งค่า
     - **Password**: ไม่ต้องกำหนดค่า
     - **CA Certificate 1**/**CA Certificate 2**: ตัวเลือกเสริม
   - ใบรับรองรูปแบบ PKCS#12 ที่ได้รับมาจากคอมพิวเตอร์
     - **Private Key**: ไม่ต้องกำหนดค่า
     - **Password**: ตัวเลือกเสริม
     - **CA Certificate 1**/**CA Certificate 2**: ไม่ต้องกำหนดค่า

4. คลิก **OK**

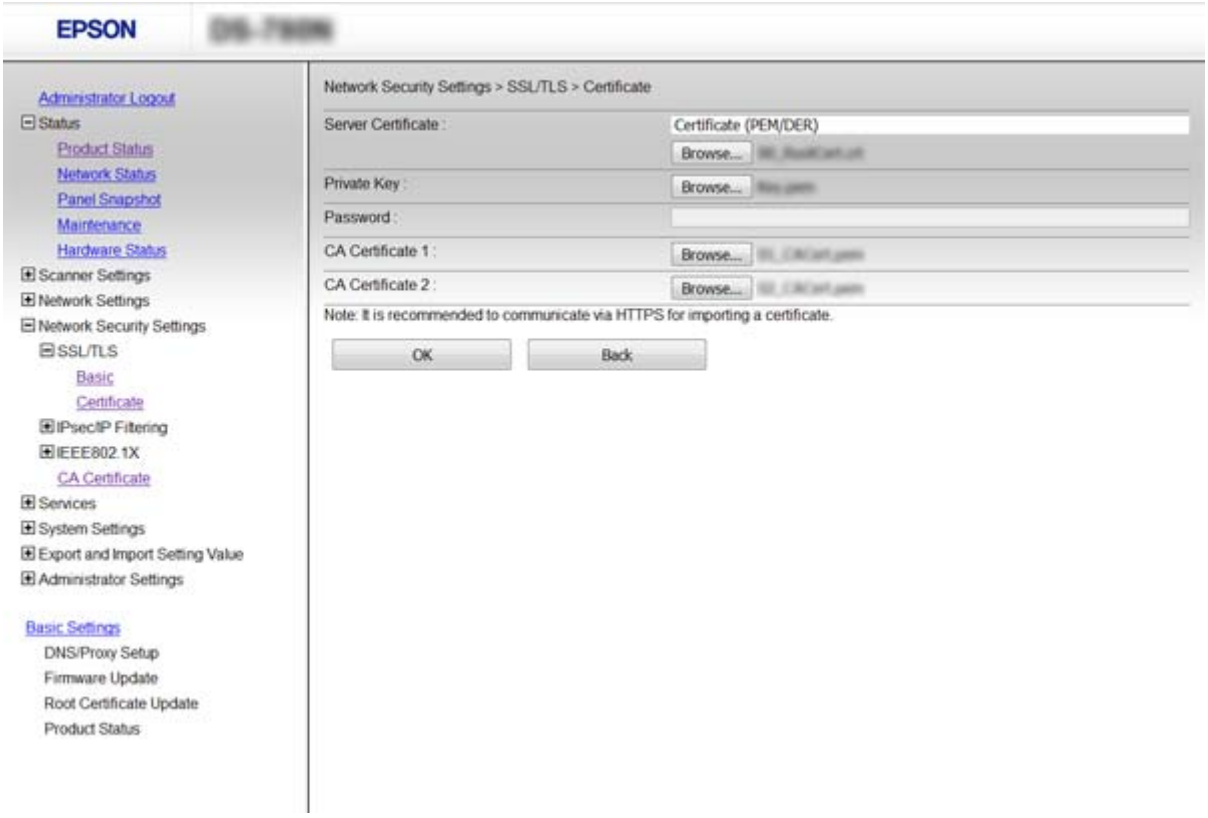
   ข้อความยืนยันสำเร็จจะแสดงขึ้นมา

หมายเหตุ:
*คลิก **Confirm** เพื่อยืนยันข้อมูลใบรับรอง*

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "รายการการตั้งค่าการนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 67

รายการการตั้งค่าการนำเข้าใบรับรองที่ลงนามจาก CA



รายการ	การตั้งค่าและคำอธิบาย
Server Certificate หรือ Client Certificate	เลือกรูปแบบใบรับรอง
Private Key	หากคุณได้รับใบรับรองรูปแบบ PEM/DER โดยใช้ CSR ที่สร้างจากคอมพิวเตอร์ ให้ระบุไฟล์คีย์ส่วนตัวที่ตรงกันกับใบรับรอง
Password	ป้อนรหัสผ่านเพื่อเข้ารหัสคีย์ส่วนตัว
CA Certificate 1	หากรูปแบบของใบรับรองเป็น **Certificate (PEM/DER)** ให้นำเข้าใบรับรองของผู้ให้บริการออกใบรับรองที่ออกใบรับรองเซิร์ฟเวอร์ให้ ระบุไฟล์ที่คุณต้องการ
CA Certificate 2	หากรูปแบบของใบรับรองเป็น **Certificate (PEM/DER)** ให้นำเข้าใบรับรองของผู้ให้บริการออกใบรับรองที่ออก **CA Certificate 1** ระบุไฟล์ที่คุณต้องการ

ข้อมูลที่เกี่ยวข้อง

➡ "การนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 66

การลบใบรับรองที่ลงนามจาก CA

คุณสามารถลบใบรับรองที่นำเข้ามาเมื่อใบรับรองหมดอายุหรือเมื่อการเชื่อมต่อแบบเข้ารหัสไม่จำเป็นอีกต่อไป

ข้อความที่สำคัญ:

หากคุณได้รับใบรับรองโดยใช้ CSR ที่สร้างจาก Web Config คุณจะไม่สามารถนำเข้าใบรับรองที่ลบไปแล้วได้อีกครั้ง ในกรณีนี้ ให้สร้าง CSR และขอรับใบรับรองอีกครั้ง

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** จากนั้น เลือก **SSL/TLS** > **Certificate** หรือ **IPsec/IP Filtering** > **Client Certificate** หรือ **IEEE802.1X** > **Client Certificate**
2. คลิกที่ **Delete**
3. ยืนยันว่าคุณต้องการลบใบรับรองในข้อความที่ปรากฏขึ้น

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การอัพเดตใบรับรองที่ลงนามด้วยตัวเอง

หากสแกนเนอร์รองรับคุณสมบัติเซิร์ฟเวอร์ HTTPS คุณสามารถอัพเดตใบรับรองที่ลงนามด้วยตัวเองได้ เมื่อเข้าถึง Web Config การใช้ใบรับรองที่ลงนามด้วยตัวเอง จะมีข้อความแจ้งเตือนปรากฏขึ้น

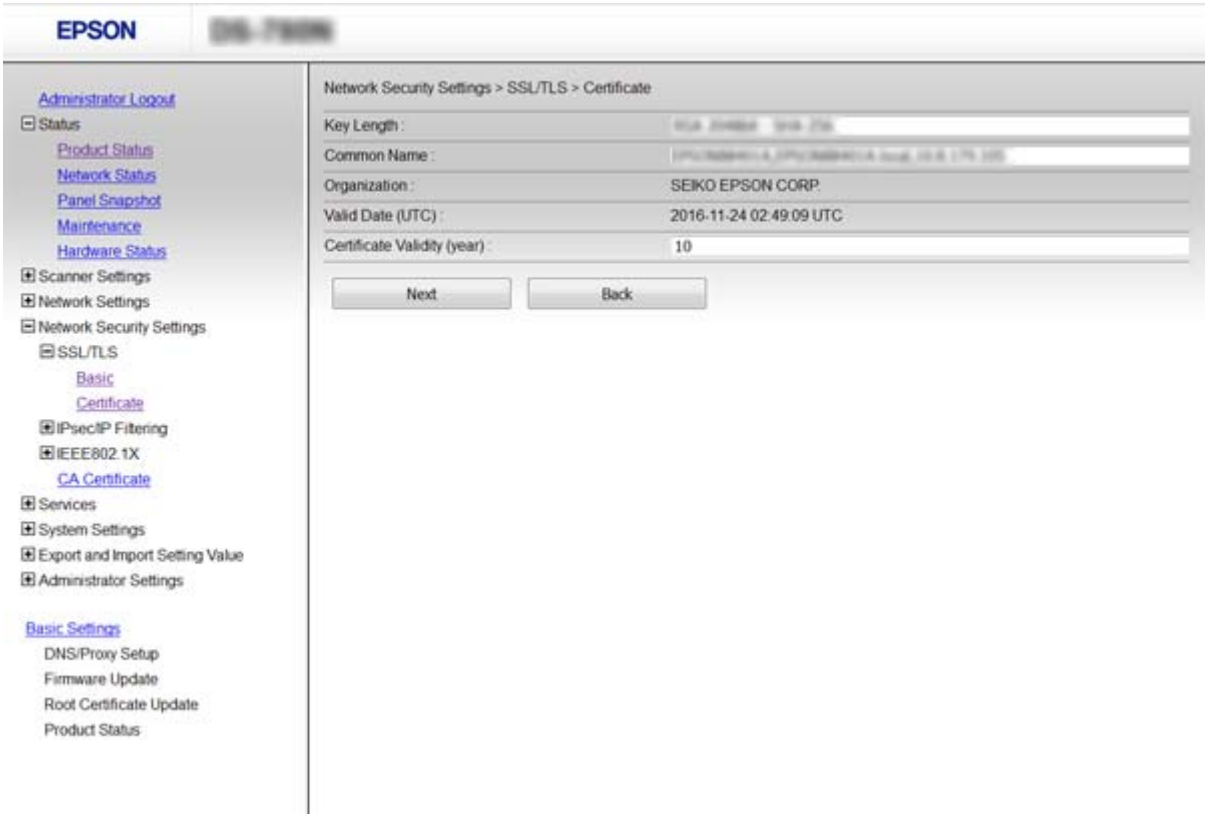
ใช้ใบรับรองที่ลงนามด้วยตัวเองชั่วคราวจนกว่าคุณจะได้รับและนำเข้าใบรับรองที่ลงนามจาก CA

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **SSL/TLS** > **Certificate**
2. คลิกที่ **Update**
3. ป้อน **Common Name**

   ป้อนที่อยู่ IP หรือตัวบ่งชี้ เช่น ชื่อ FQDN สำหรับสแกนเนอร์ คุณสามารถป้อนระหว่าง 1 และ 128 ตัวอักขระ

   หมายเหตุ:
   คุณสามารถแบ่งส่วนชื่อ (CN) ด้วยเครื่องหมายจุลภาค

4. ระบุระยะเวลาที่มีผลใช้ได้สำหรับใบรับรอง



5. คลิกที่ **Next**

   ข้อความยืนยันจะแสดงขึ้นมา

6. คลิกที่ **OK**

   สแกนเนอร์ได้รับการอัพเดทแล้ว

หมายเหตุ:
*คลิก **Confirm** เพื่อยืนยันข้อมูลใบรับรอง*

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การกำหนดค่า CA Certificate

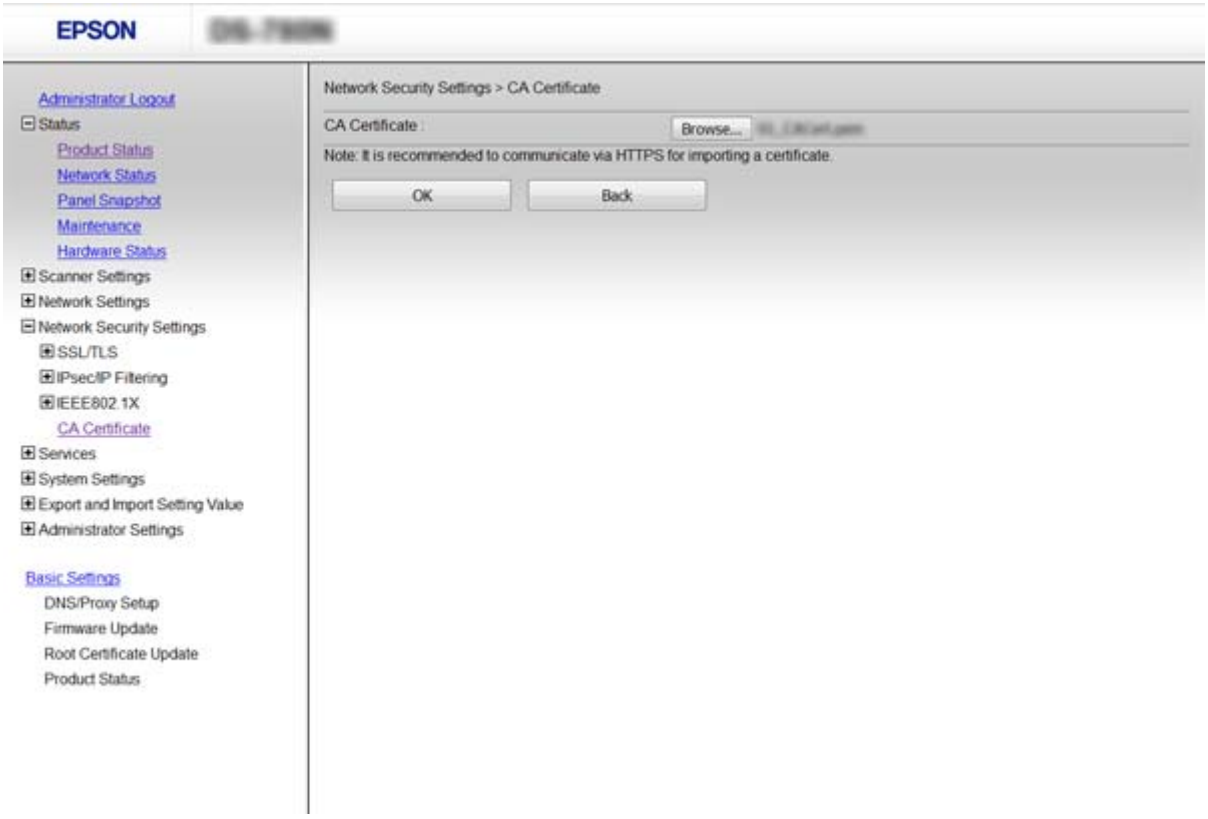
คุณสามารถนำเข้า แสดง ลบ CA Certificate

การนำเข้า CA Certificate

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **CA Certificate**

2. คลิก **Import**

3. ระบุ CA Certificate ที่คุณต้องการนำเข้า



4. คลิก **OK**

เมื่อการนำเข้าเสร็จสิ้น ระบบจะนำกลับไปที่หน้าจอ **CA Certificate** และ CA Certificate ที่เลือกไว้จะแสดงขึ้นมา

ข้อมูลที่เกี่ยวข้อง

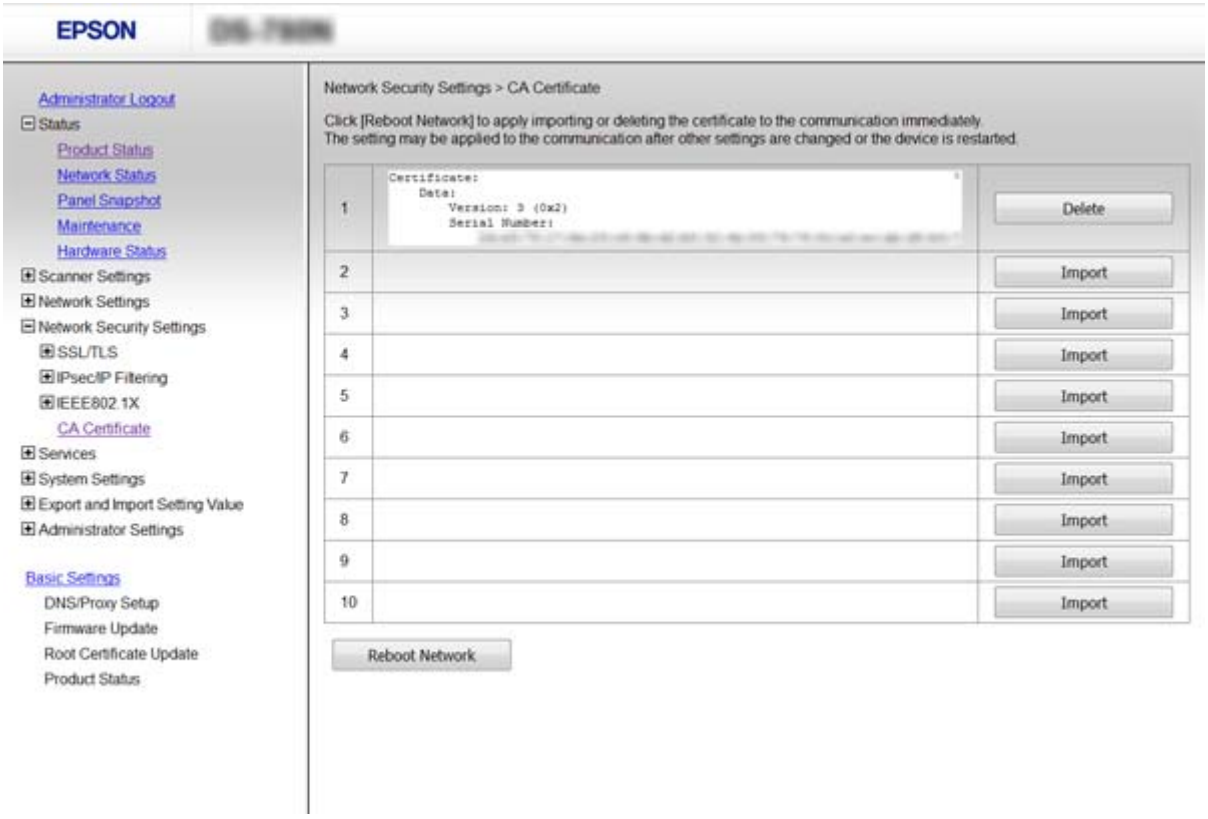
➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การลบ CA Certificate

คุณสามารถลบ CA Certificate ที่นำเข้ามา

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **CA Certificate**

2. คลิก **Delete** ติดกับ CA Certificate ที่คุณต้องการลบ



3. ยืนยันว่าคุณต้องการลบใบรับรองในข้อความที่ปรากฏขึ้น

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

การเข้ารหัสการสื่อสารโดยใช้การกรอง IPsec/IP

เกี่ยวกับ IPsec/IP Filtering

หากสแกนเนอร์รองรับการกรอง IPsec/IP คุณสามารถทำการกรองการส่งผ่านข้อมูลโดยขึ้นอยู่กับที่อยู่ IP บริการและพอร์ตต่าง ๆ โดยการผสมกันของการกรอง คุณสามารถกำหนดค่าสแกนเนอร์ให้ยอมรับหรือบล็อคไคลเอ็นท์ที่กำหนดและข้อมูลที่กำหนดได้ นอกจากนี้ คุณยังสามารถรปรับปรุงระดับความปลอดภัยโดยการใช้งาน IPsec

สำหรับการกรองการส่งผ่านข้อมูล ให้กำหนดค่านโยบายเริ่มต้น นโยบายเริ่มต้นใช้งานกับทุกผู้ใช้หรือกลุ่มที่เชื่อมต่อเข้ากับสแกนเนอร์ สำหรับการควบคุมแบบละเอียดเหนือผู้ใช้และกลุ่มของผู้ใช้นั้น ให้กำหนดเป็นนโยบายกลุ่ม นโยบายกลุ่มเป็นกฎเกณฑ์อย่างน้อยหนึ่งกฎขึ้นไปที่ใช้กับผู้ใช้หรือกลุ่มผู้ใช้ สแกนเนอร์จะควบคุมแพกเกจข้อมูล IP ที่ตรงกันกับนโยบายที่กำหนดไว้ แพกเกจข้อมูล IP จะถูกตรวจยืนยันในลำดับตั้งแต่นโยบายกลุ่ม 1 ไปจนถึงนโยบายกลุ่ม 10 จากนั้นเป็นนโยบายเริ่มต้น

หมายเหตุ:
คอมพิวเตอร์ที่รัน Windows Vista หรือรุ่นใหม่กว่า หรือ Windows Server 2008 หรือรุ่นใหม่กว่าสามารถรองรับ IPsec

การกำหนดค่า Default Policy

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **IPsec/IP Filtering** > **Basic**
2. ป้อนค่าสำหรับแต่ละรายการ
3. คลิก **Next**

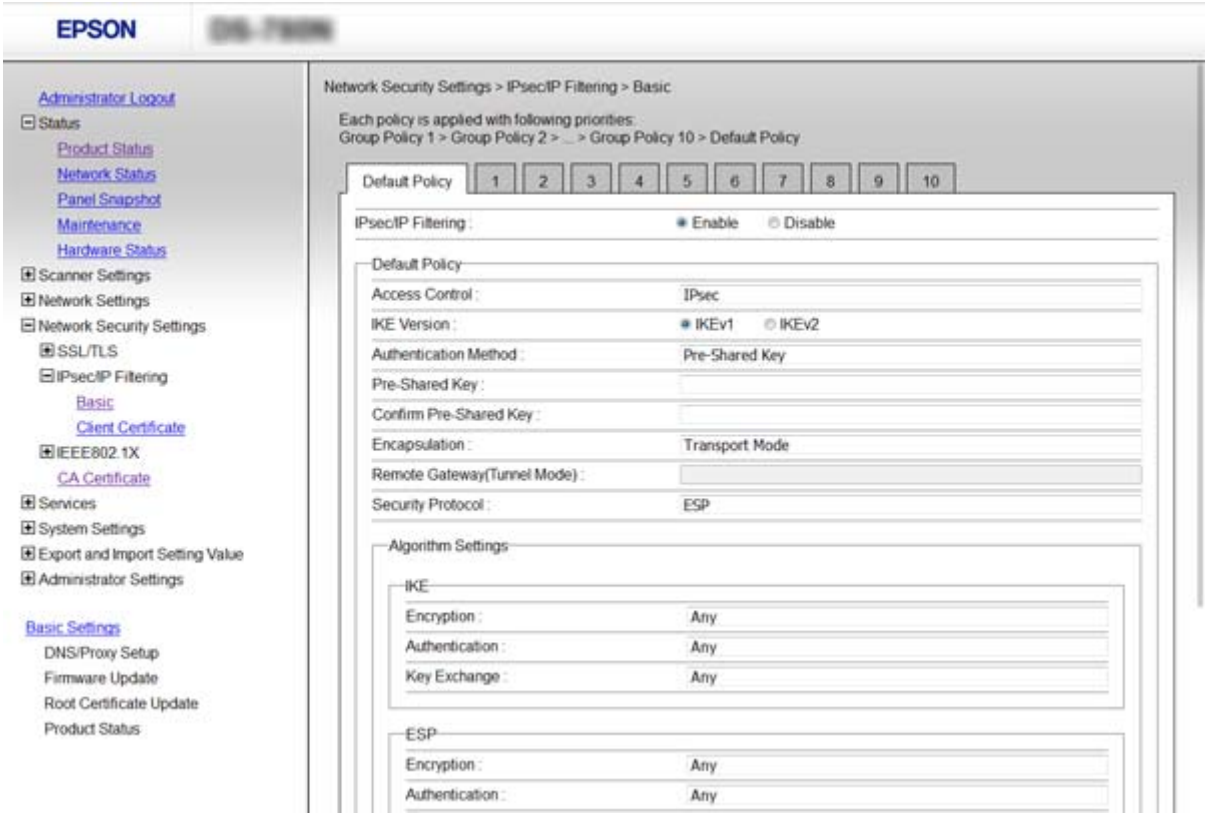
   ข้อความยืนยันจะแสดงขึ้นมา
4. คลิก **OK**

   สแกนเนอร์ได้รับการอัพเดทแล้ว

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "รายการการตั้งค่า Default Policy" บนหน้าที่ 72

รายการการตั้งค่า Default Policy



รายการ	การตั้งค่าและคำอธิบาย
IPsec/IP Filtering	คุณสามารถเปิดใช้งานหรือปิดใช้งานคุณสมบัติการกรอง IPsec/IP

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

รายการ	การตั้งค่าและคำอธิบาย	
Access Control	กำหนดค่าวิธีการควบคุมสำหรับการส่งผ่านข้อมูลของแพกเกจ IP	
	Permit Access	เลือกตัวเลือกนี้เพื่ออนุญาตให้แพกเกจ IP ที่กำหนดค่าแล้วสามารถส่งผ่านตลอด
	Refuse Access	เลือกตัวเลือกนี้เพื่อปฏิเสธให้แพกเกจ IP ที่กำหนดค่าแล้วสามารถส่งผ่านตลอด
	IPsec	เลือกตัวเลือกนี้เพื่ออนุญาตให้แพกเกจ IPsec ที่กำหนดค่าแล้วสามารถส่งผ่านตลอด
IKE Version	เลือกเวอร์ชัน IKEv1 หรือ IKEv2 สำหรับ IKE เลือกรายการหนึ่งโดยสอดคล้องกับอุปกรณ์ที่สแกนเนอร์เชื่อมต่อด้วย	
IKEv1	รายการต่อไปนี้ถูกแสดงผลเมื่อคุณเลือก **IKEv1** สำหรับ **IKE Version**	
	Authentication Method	สำหรับการเลือก **Certificate** คุณจะต้องขอรับและนำเข้าใบรับรองที่ลงนามจาก CA ล่วงหน้า
	Pre-Shared Key	หากคุณเลือก **Pre-Shared Key** สำหรับ **Authentication Method** ให้ป้อนคีย์ที่แชร์เบื้องต้นระหว่าง 1 และ 127 ตัวอักขระ
	Confirm Pre-Shared Key	ป้อนคีย์ที่คุณกำหนดค่าไว้เพื่อการยืนยัน
IKEv2	รายการต่อไปนี้ถูกแสดงผลเมื่อคุณเลือก **IKEv2** สำหรับ **IKE Version**	
Local	Authentication Method	สำหรับการเลือก **Certificate** คุณจะต้องขอรับและนำเข้าใบรับรองที่ลงนามจาก CA ล่วงหน้า
	ID Type	เลือกประเภทของ ID สำหรับสแกนเนอร์
	ID	ป้อน ID ของสแกนเนอร์ที่ตรงกับประเภทของ ID คุณไม่สามารถใช้ตัวอักขระตัวแรกเป็น "@", "#", และ "=" **Distinguished Name**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "=" **IP Address**: ป้อนรูปแบบ IPv4 หรือ IPv6 **FQDN**: ป้อนการผสมกันระหว่าง 1 และ 255 ตัวอักขระโดยใช้ A–Z, a–z, 0–9, "-" และเครื่องหมายมหัพภาค (.) **Email Address**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "@" **Key ID**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว
	Pre-Shared Key	หากคุณเลือก **Pre-Shared Key** สำหรับ **Authentication Method** ให้ป้อนคีย์ที่แชร์เบื้องต้นระหว่าง 1 และ 127 ตัวอักขระ
	Confirm Pre-Shared Key	ป้อนคีย์ที่คุณกำหนดค่าไว้เพื่อการยืนยัน

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

รายการ	การตั้งค่าและคำอธิบาย	
Remote	Authentication Method	สำหรับการเลือก **Certificate** คุณจะต้องขอรับและนำเข้าใบรับรองที่ลงนามจาก CA ล่วงหน้า
	ID Type	เลือกประเภทของ ID สำหรับอุปกรณ์ที่คุณต้องการตรวจรับรองความถูกต้อง
	ID	ป้อน ID ของสแกนเนอร์ที่ตรงกับประเภทของ ID คุณไม่สามารถใช้ตัวอักขระตัวแรกเป็น "@", "#", และ "=" **Distinguished Name**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "=" **IP Address**: ป้อนรูปแบบ IPv4 หรือ IPv6 **FQDN**: ป้อนการผสมกันระหว่าง 1 และ 255 ตัวอักขระโดยใช้ A–Z, a–z, 0–9, "-" และเครื่องหมายมหัพภาค (.) **Email Address**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "@" **Key ID**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว
	Pre-Shared Key	หากคุณเลือก **Pre-Shared Key** สำหรับ **Authentication Method** ให้ป้อนคีย์ที่แชร์เบื้องต้นระหว่าง 1 และ 127 ตัวอักขระ
	Confirm Pre-Shared Key	ป้อนคีย์ที่คุณกำหนดค่าไว้เพื่อการยืนยัน
Encapsulation	หากคุณเลือก **IPsec** สำหรับ **Access Control** คุณจะต้องกำหนดค่าโหมดการปกปิด	
	Transport Mode	หากคุณใช้เฉพาะสแกนเนอร์บน LAN เดียวกัน ให้เลือกรายการนี้ แพกเกจ IP ของเลเยอร์ 4 หรือสูงกว่าถูกเข้ารหัส
	Tunnel Mode	หากคุณใช้สแกนเนอร์บนเครือข่ายที่เข้าถึงอินเทอร์เน็ตได้ เช่น IPsec-VPN ให้เลือกตัวเลือกนี้ หัวเรื่องและข้อมูลของแพกเกจ IP ถูกเข้ารหัส
Remote Gateway(Tunnel Mode)	หากคุณเลือก **Tunnel Mode** สำหรับ **Encapsulation** ให้ป้อนที่อยู่เกตเวย์ระหว่าง 1 และ 39 ตัวอักขระ	
Security Protocol	**IPsec** สำหรับ **Access Control** เลือกตัวเลือก	
	ESP	เลือกตัวเลือกนี้เพื่อให้มั่นใจในความถูกต้องของการรับรองความถูกต้องและข้อมูล และข้อมูลที่เข้ารหัส
	AH	เลือกตัวเลือกนี้เพื่อให้มั่นใจในความถูกต้องของการรับรองความถูกต้องและข้อมูล แม้ว่าจะห้ามการเข้ารหัสข้อมูล แต่คุณสามารถใช้ IPsec ได้
Algorithm Settings		
IKE	Encryption	เลือกอัลกอริทึมการเข้ารหัสสำหรับ IKE รายการจะแปรผันไปตามเวอร์ชันของ IKE
	Authentication	เลือกอัลกอริทึมการตรวจรับรองความถูกต้องสำหรับ IKE
	Key Exchange	เลือกอัลกอริทึมการแลกเปลี่ยนคีย์สำหรับ IKE รายการจะแปรผันไปตามเวอร์ชันของ IKE

รายการ	การตั้งค่าและคำอธิบาย	
ESP	Encryption	เลือกอัลกอริทึมการเข้ารหัสสำหรับ ESP รายการนี้พร้อมใช้งานเมื่อ **ESP** ถูกเลือกสำหรับ **Security Protocol**
	Authentication	เลือกอัลกอริทึมการตรวจรับรองความถูกต้องสำหรับ ESP รายการนี้พร้อมใช้งานเมื่อ **ESP** ถูกเลือกสำหรับ **Security Protocol**
AH	Authentication	เลือกอัลกอริทึมการเข้ารหัสสำหรับ AH รายการนี้พร้อมใช้งานเมื่อ **AH** ถูกเลือกสำหรับ **Security Protocol**

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดค่า Default Policy" บนหน้าที่ 72

การกำหนดค่า Group Policy

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **IPsec/IP Filtering** > **Basic**
2. คลิกแท็บที่มีหมายเลขที่คุณต้องการกำหนดค่า
3. ป้อนค่าสำหรับแต่ละรายการ
4. คลิก **Next**

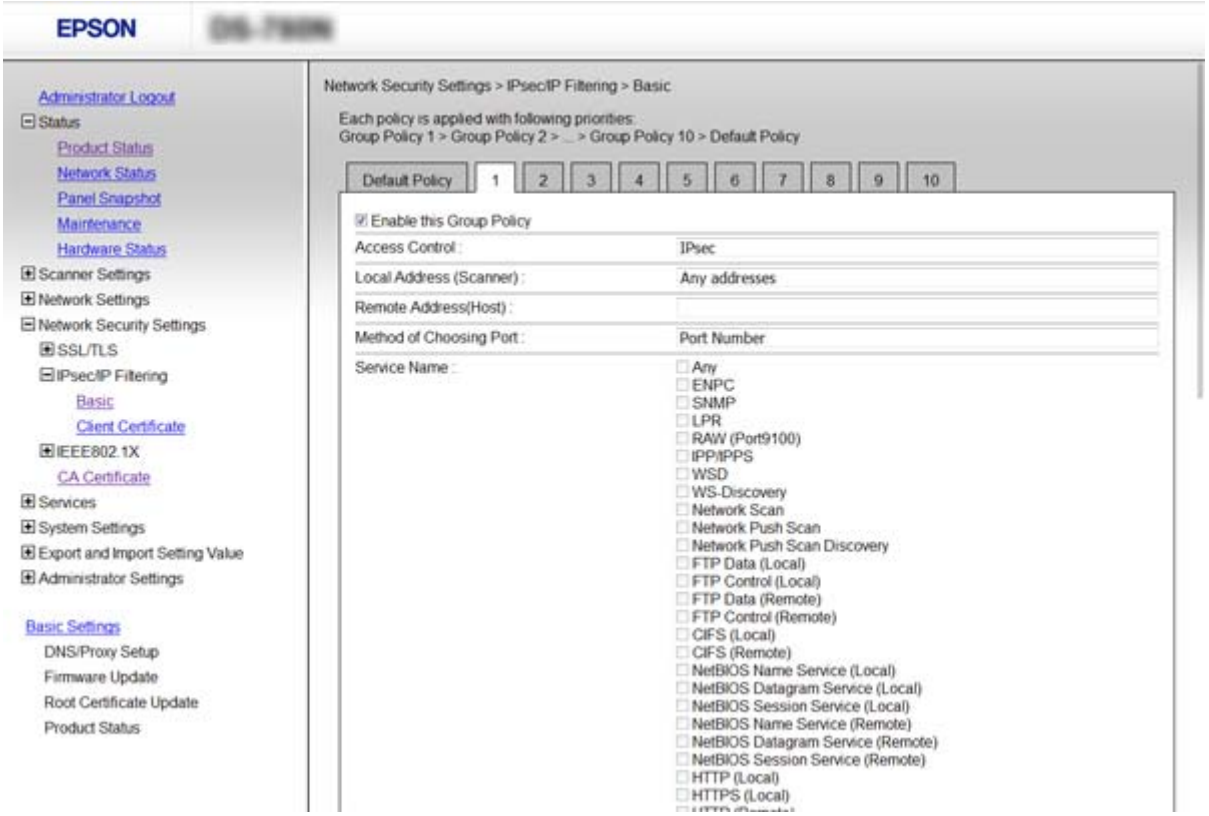
   ข้อความยืนยันจะแสดงขึ้นมา
5. คลิก **OK**

   สแกนเนอร์ได้รับการอัพเดทแล้ว

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "รายการการตั้งค่า Group Policy" บนหน้าที่ 76

รายการการตั้งค่า Group Policy



รายการ	การตั้งค่าและคำอธิบาย	
Enable this Group Policy	คุณสามารถเปิดใช้งานหรือปิดใช้งานนโยบายกลุ่มได้	
Access Control	กำหนดค่าวิธีการควบคุมสำหรับการส่งผ่านข้อมูลของแพกเกจ IP	
	Permit Access	เลือกตัวเลือกนี้เพื่ออนุญาตให้แพกเกจ IP ที่กำหนดค่าแล้วสามารถส่งผ่านตลอด
	Refuse Access	เลือกตัวเลือกนี้เพื่อปฏิเสธให้แพกเกจ IP ที่กำหนดค่าแล้วสามารถส่งผ่านตลอด
	IPsec	เลือกตัวเลือกนี้เพื่ออนุญาตให้แพกเกจ IPsec ที่กำหนดค่าแล้วสามารถส่งผ่านตลอด
Local Address (Scanner)	เลือกที่อยู่ IPv4 หรือที่อยู่ IPv6 ที่ตรงกับสภาพแวดล้อมเครือข่ายของคุณ หากที่อยู่ IP ถูกกำหนดโดยอัตโนมัติ คุณสามารถเลือก **Use auto-obtained IPv4 address**	
Remote Address(Host)	ป้อนที่อยู่ IP ของอุปกรณ์เพื่อควบคุมการเข้าถึง ที่อยู่ IP จะต้องอยู่ไม่เกิน 43 ตัวอักขระ หากคุณไม่ได้ป้อนที่อยู่ IP ที่อยู่ทั้งหมดจะถูกควบคุม ***หมายเหตุ:*** *หากที่อยู่ IP ถูกกำหนดโดยอัตโนมัติ (เช่น กำหนดโดย DHCP) การเชื่อมต่ออาจไม่สามารถใช้งานได้ กำหนดค่าที่อยู่ IP แบบคงที่*	
Method of Choosing Port	เลือกวิธีการระบุพอร์ต	
Service Name	หากคุณเลือก **Service Name** สำหรับ **Method of Choosing Port** ให้เลือกตัวเลือกนี้	

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

รายการ	การตั้งค่าและคำอธิบาย	
Transport Protocol	หากคุณเลือก **Port Number** สำหรับ **Method of Choosing Port** คุณจะต้องกำหนดค่าโหมดการปกปิด	
	Any Protocol	เลือกตัวเลือกนี้เพื่อควบคุมประเภทโปรโตคอล
	TCP	เลือกตัวเลือกนี้เพื่อควบคุมข้อมูลสำหรับการส่งข้อมูลโดยตรง
	UDP	เลือกตัวเลือกนี้เพื่อควบคุมข้อมูลสำหรับการส่งข้อมูลกระจายและแบบหลายผู้รับ
	ICMPv4	เลือกตัวเลือกนี้เพื่อควบคุมคำสั่งปิง (ping)
Local Port	หากคุณเลือก **Port Number** สำหรับ **Method of Choosing Port** และหากคุณเลือก **TCP** หรือ **UDP** สำหรับ **Transport Protocol** ให้ป้อนหมายเลขพอร์ตเพื่อควบคุมแพกเกจรับ โดยแยกด้วยเครื่องหมายจุลภาค คุณสามารถป้อนหมายเลขพอร์ตสูงสุด 10 หมายเลข ตัวอย่าง: 20,80,119,5220 หากคุณไม่ได้ป้อนหมายเลขพอร์ต พอร์ตทั้งหมดจะถูกควบคุม	
Remote Port	หากคุณเลือก **Port Number** สำหรับ **Method of Choosing Port** และหากคุณเลือก **TCP** หรือ **UDP** สำหรับ **Transport Protocol** ให้ป้อนหมายเลขพอร์ตเพื่อควบคุมแพกเกจส่ง โดยแยกด้วยเครื่องหมายจุลภาค คุณสามารถป้อนหมายเลขพอร์ตสูงสุด 10 หมายเลข ตัวอย่าง: 25,80,143,5220 หากคุณไม่ได้ป้อนหมายเลขพอร์ต พอร์ตทั้งหมดจะถูกควบคุม	
IKE Version	เลือกเวอร์ชัน IKEv1 หรือ IKEv2 สำหรับ IKE เลือกรายการหนึ่งโดยสอดคล้องกับอุปกรณ์ที่สแกนเนอร์เชื่อมต่อด้วย	
IKEv1	รายการต่อไปนี้ถูกแสดงผลเมื่อคุณเลือก **IKEv1** สำหรับ **IKE Version**	
	Authentication Method	หากคุณเลือก **IPsec** สำหรับ **Access Control** ให้เลือกตัวเลือกนี้ ใบรับรองที่ใช้งานแล้วจะใช้ร่วมกันกับนโยบายเริ่มต้น
	Pre-Shared Key	หากคุณเลือก **Pre-Shared Key** สำหรับ **Authentication Method** ให้ป้อนคีย์ที่แชร์เบื้องต้นระหว่าง 1 และ 127 ตัวอักขระ
	Confirm Pre-Shared Key	ป้อนคีย์ที่คุณกำหนดค่าไว้เพื่อการยืนยัน
IKEv2	รายการต่อไปนี้ถูกแสดงผลเมื่อคุณเลือก **IKEv2** สำหรับ **IKE Version**	

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

รายการ	การตั้งค่าและคำอธิบาย	
Local	Authentication Method	หากคุณเลือก **IPsec** สำหรับ **Access Control** ให้เลือกตัวเลือกนี้ ใบรับรองที่ใช้งานแล้วจะใช้ร่วมกันกับนโยบายเริ่มต้น
	ID Type	เลือกประเภทของ ID สำหรับสแกนเนอร์
	ID	ป้อน ID ของสแกนเนอร์ที่ตรงกับประเภทของ ID คุณไม่สามารถใช้ตัวอักขระตัวแรกเป็น "@", "#", และ "=" **Distinguished Name**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "=" **IP Address**: ป้อนรูปแบบ IPv4 หรือ IPv6 **FQDN**: ป้อนการผสมกันระหว่าง 1 และ 255 ตัวอักขระโดยใช้ A–Z, a–z, 0–9, "-" และเครื่องหมายมหัพภาค (.) **Email Address**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "@" **Key ID**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว
	Pre-Shared Key	หากคุณเลือก **Pre-Shared Key** สำหรับ **Authentication Method** ให้ป้อนคีย์ที่แชร์เบื้องต้นระหว่าง 1 และ 127 ตัวอักขระ
	Confirm Pre-Shared Key	ป้อนคีย์ที่คุณกำหนดค่าไว้เพื่อการยืนยัน
Remote	Authentication Method	หากคุณเลือก **IPsec** สำหรับ **Access Control** ให้เลือกตัวเลือกนี้ ใบรับรองที่ใช้งานแล้วจะใช้ร่วมกันกับนโยบายเริ่มต้น
	ID Type	เลือกประเภทของ ID สำหรับอุปกรณ์ที่คุณต้องการตรวจรับรองความถูกต้อง
	ID	ป้อน ID ของสแกนเนอร์ที่ตรงกับประเภทของ ID คุณไม่สามารถใช้ตัวอักขระตัวแรกเป็น "@", "#", และ "=" **Distinguished Name**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "=" **IP Address**: ป้อนรูปแบบ IPv4 หรือ IPv6 **FQDN**: ป้อนการผสมกันระหว่าง 1 และ 255 ตัวอักขระโดยใช้ A–Z, a–z, 0–9, "-" และเครื่องหมายมหัพภาค (.) **Email Address**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว คุณจะต้องมีเครื่องหมาย "@" **Key ID**: ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว
	Pre-Shared Key	หากคุณเลือก **Pre-Shared Key** สำหรับ **Authentication Method** ให้ป้อนคีย์ที่แชร์เบื้องต้นระหว่าง 1 และ 127 ตัวอักขระ
	Confirm Pre-Shared Key	ป้อนคีย์ที่คุณกำหนดค่าไว้เพื่อการยืนยัน

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

รายการ	การตั้งค่าและคำอธิบาย	
Encapsulation	หากคุณเลือก **IPsec** สำหรับ **Access Control** คุณจะต้องกำหนดค่าโหมดการปกปิด	
	Transport Mode	หากคุณใช้เฉพาะสแกนเนอร์บน LAN เดียวกัน ให้เลือกรายการนี้ แพกเกจ IP ของเลเยอร์ 4 หรือสูงกว่าถูกเข้ารหัส
	Tunnel Mode	หากคุณใช้สแกนเนอร์บนเครือข่ายที่เข้าถึงอินเทอร์เน็ตได้ เช่น IPsec-VPN ให้เลือกตัวเลือกนี้ หัวเรื่องและข้อมูลของแพกเกจ IP ถูกเข้ารหัส
Remote Gateway(Tunnel Mode)	หากคุณเลือก **Tunnel Mode** สำหรับ **Encapsulation** ให้ป้อนที่อยู่เกตเวย์ระหว่าง 1 และ 39 ตัวอักขระ	
Security Protocol	หากคุณเลือก **IPsec** สำหรับ **Access Control** ให้เลือกตัวเลือกนี้	
	ESP	เลือกตัวเลือกนี้เพื่อให้มั่นใจในความถูกต้องของการรับรองความถูกต้องและข้อมูล และข้อมูลที่เข้ารหัส
	AH	เลือกตัวเลือกนี้เพื่อให้มั่นใจในความถูกต้องของการรับรองความถูกต้องและข้อมูล แม้ว่าจะห้ามการเข้ารหัสข้อมูล แต่คุณสามารถใช้ IPsec ได้
Algorithm Settings		
IKE	Encryption	เลือกอัลกอริทึมการเข้ารหัสสำหรับ IKE รายการจะแปรผันไปตามเวอร์ชันของ IKE
	Authentication	เลือกอัลกอริทึมการตรวจรับรองความถูกต้องสำหรับ IKE
	Key Exchange	เลือกอัลกอริทึมการแลกเปลี่ยนคีย์สำหรับ IKE รายการจะแปรผันไปตามเวอร์ชันของ IKE
ESP	Encryption	เลือกอัลกอริทึมการเข้ารหัสสำหรับ ESP รายการนี้พร้อมใช้งานเมื่อ **ESP** ถูกเลือกสำหรับ **Security Protocol**
	Authentication	เลือกอัลกอริทึมการตรวจรับรองความถูกต้องสำหรับ ESP รายการนี้พร้อมใช้งานเมื่อ **ESP** ถูกเลือกสำหรับ **Security Protocol**
AH	Authentication	เลือกอัลกอริทึมการตรวจรับรองความถูกต้องสำหรับ AH รายการนี้พร้อมใช้งานเมื่อ **AH** ถูกเลือกสำหรับ **Security Protocol**

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดค่า Group Policy" บนหน้าที่ 75
➡ "การผสมกันของ Local Address (Scanner) และ Remote Address(Host) บน Group Policy" บนหน้าที่ 80
➡ "การอ้างอิงชื่อบริการในนโยบายกลุ่ม" บนหน้าที่ 80

การผสมกันของ Local Address (Scanner) และ Remote Address(Host) บน Group Policy

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

*1 หาก **IPsec** ถูกเลือกสำหรับ **Access Control** คุณไม่สามารถระบุในความยาวหมายเลขนำหน้า

*2 หาก **IPsec** ถูกเลือกสำหรับ **Access Control** คุณสามารถเลือกที่อยู่ภายในเครื่องที่เชื่อมโยงกัน (fe80::) แต่นโยบายกลุ่มจะถูกปิดใช้งาน

*3 ยกเว้นที่อยู่ภายในเครื่องที่เชื่อมโยงกันของ IPv6

การอ้างอิงชื่อบริการในนโยบายกลุ่ม

หมายเหตุ:
บริการไม่สามารถใช้งานได้จะแสดงขึ้นมาแต่ไม่สามารถเลือกได้

ชื่อบริการ	ประเภทโปรโตคอล	หมายเลขพอร์ตในเครื่อง	หมายเลขพอร์ตระยะไกล	คุณสมบัติที่ถูกควบคุม
Any	–	–	–	ทุกบริการ
ENPC	UDP	3289	พอร์ตใด ๆ	การค้นหาสแกนเนอร์จากโปรแกรม เช่น EpsonNet Config และไดร์เวอร์สแกนเนอร์
SNMP	UDP	161	พอร์ตใด ๆ	การได้รับและการกำหนดค่า MIB จากโปรแกรมอย่างเช่น EpsonNet Config ไดร์เวอร์สแกนเนอร์ Epson
WSD	TCP	พอร์ตใด ๆ	5357	การควบคุม WSD
WS-Discovery	UDP	3702	พอร์ตใด ๆ	การค้นหาสแกนเนอร์จาก WSD
Network Scan	TCP	1865	พอร์ตใด ๆ	การส่งต่อข้อมูลสแกนจาก Document Capture Pro
Network Push Scan Discovery	UDP	2968	พอร์ตใด ๆ	การค้นหาคอมพิวเตอร์จากสแกนเนอร์
Network Push Scan	TCP	พอร์ตใด ๆ	2968	การได้รับข้อมูลงานของการสแกนแบบดันจาก Document Capture Pro หรือ Document Capture
HTTP (Local)	TCP	80	พอร์ตใด ๆ	เซิร์ฟเวอร์ HTTP(S) (การส่งต่อข้อมูลของ Web Config และ WSD)
HTTPS (Local)	TCP	443	พอร์ตใด ๆ	
HTTP (Remote)	TCP	พอร์ตใด ๆ	80	ไคลเอ็นท์ HTTP(S) (การสื่อสารระหว่างการอัพเดตเฟิร์มแวร์และการอัพเดตใบรับรองราก)
HTTPS (Remote)	TCP	พอร์ตใด ๆ	443	

ตัวอย่างการกำหนดค่าของ IPsec/IP Filtering

การรับเฉพาะแพกเกจ IPsec

ตัวอย่างนี้สำหรับการกำหนดค่านโยบายค่าเริ่มต้นเท่านั้น

Default Policy:

- ❑ **IPsec/IP Filtering**: **Enable**
- ❑ **Access Control**: **IPsec**
- ❑ **Authentication Method**: **Pre-Shared Key**
- ❑ **Pre-Shared Key**: ป้อนค่าไม่เกิน 127 ตัวอักขระ

Group Policy:

ไม่ต้องกำหนดค่า

การยอมรับการสแกนโดยใช้ Epson Scan 2 และการตั้งค่าสแกนเนอร์

ตัวอย่างนี้อนุญาตการสื่อสารของข้อมูลสแกนเนอร์และการกำหนดค่าสแกนเนอร์จากบริการที่กำหนดเท่านั้น

Default Policy:

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

Group Policy:

- ❑ **Enable this Group Policy**: กาเลือกในกล่องรายการ
- ❑ **Access Control**: **Permit Access**
- ❑ **Remote Address(Host)**: ที่อยู่ IP ของไคลเอ็นท์
- ❑ **Method of Choosing Port**: **Service Name**
- ❑ **Service Name**: กาเลือกกล่องรายการของ **ENPC**, **SNMP**, **Network Scan**, **HTTP (Local)** และ **HTTPS (Local)**

การรับการเข้าถึงจากที่อยู่ IP ที่กำหนดไว้เท่านั้น

ตัวอย่างนี้อนุญาตที่อยู่ IP ที่กำหนดไว้สำหรับเข้าถึงสแกนเนอร์

Default Policy:

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

Group Policy:

- ❑ **Enable this Group Policy**: กาเลือกในกล่องรายการ
- ❑ **Access Control**: **Permit Access**
- ❑ **Remote Address(Host)**: ที่อยู่ IP ของไคลเอ็นท์ของผู้ดูแลระบบ

หมายเหตุ:
ทั้งนี้โดยไม่คำนึงถึงการกำหนดค่านโยบาย ไคลเอ็นท์จะสามารถเข้าถึงและกำหนดค่าสแกนเนอร์ได้

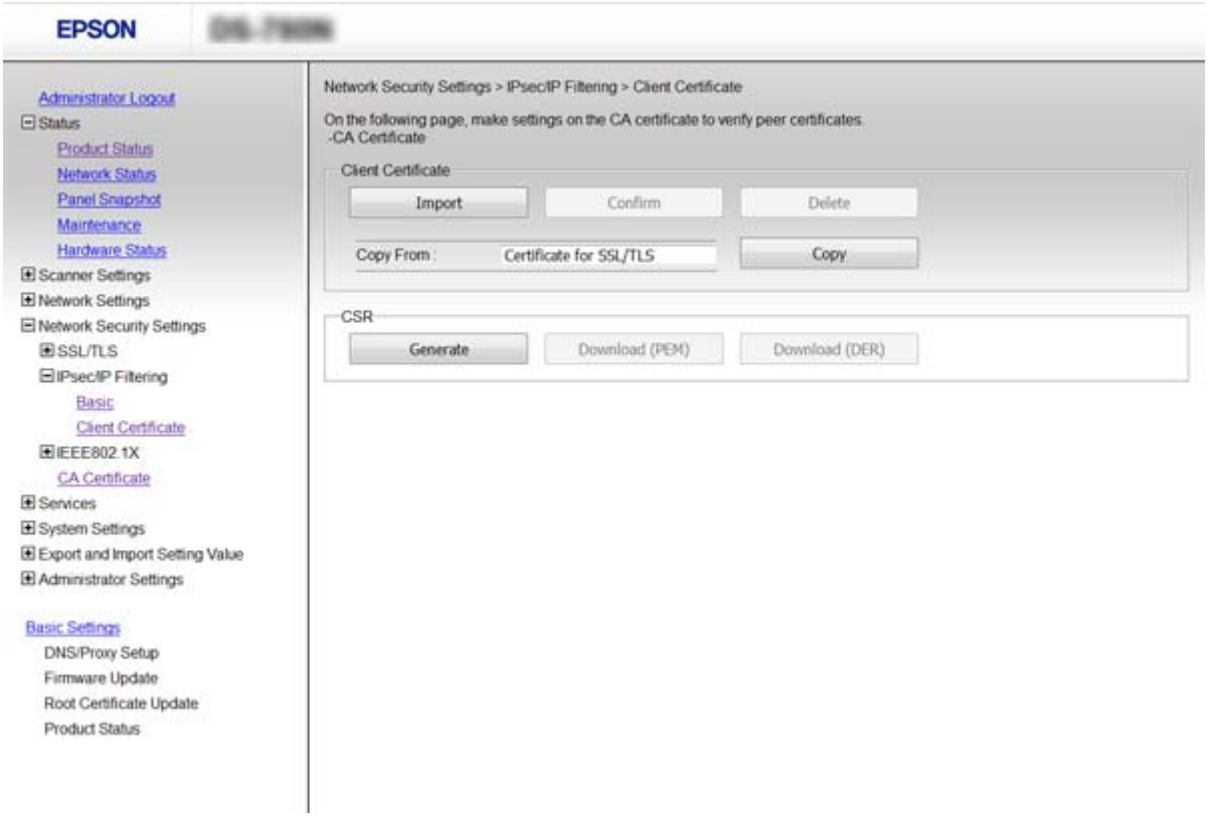
การกำหนดค่าใบรับรองสำหรับ IPsec/IP Filtering

กำหนดค่าใบรับรองไคลเอ็นท์สำหรับการกรอง IPsec/IP หากคุณต้องการกำหนดค่าการอนุญาตการรับรองความถูกต้อง ให้ไปที่ **CA Certificate**

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **IPsec/IP Filtering** > **Client Certificate**

2. นำเข้าใบรับรองใน **Client Certificate**

   หากคุณได้นำเข้าใบรับรองที่จัดพิมพ์ให้โดยหน่วยงานออกใบรับรองในแบบมาตรฐาน IEEE802.1X หรือ SSL/TLS แล้ว คุณสามารถคัดลอกใบรับรองและใช้งานได้ในการกรอง IPsec/IP สำหรับการตัดลอก ให้เลือกใบรับรองจาก **Copy From** จากนั้นคลิก **Copy**



ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

➡ "การขอรับและการนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 64

การใช้โปรโตคอล SNMPv3

เกี่ยวกับ SNMPv3

SNMP เป็นโปรโตคอลที่ดำเนินการเฝ้าตรวจตราและควบคุมสำหรับการรวบรวมข้อมูลของอุปกรณ์ที่เชื่อมต่อเข้ากับเครือข่าย SNMPv3 เป็นเวอร์ชันคุณลักษณะการจัดการความปลอดภัยที่เพิ่มขีดความสามารถ

เมื่อใช้งาน SNMPv3 สถานะของการเฝ้าตรวจตราและการเปลี่ยนแปลงการตั้งค่าของการสื่อสาร SNMP (แพคเกต) สามารถตรวจรับรองและเข้ารหัสเพื่อที่จะให้การป้องกันความเสี่ยงในการสื่อสาร SNMP (แพคเกต) เช่น การดักข้อมูลผ่านสาย การปลอมตัว และการแอบเปิดดูข้อมูล

การกำหนดค่า SNMPv3

หากสแกนเนอร์รองรับโปรโตคอล SNMPv3 คุณสามารถเฝ้าตรวจตราและควบคุมการเข้าถึงสแกนเนอร์ได้

1. เข้าถึง Web Config แล้วเลือก **Services** > **Protocol**
2. ป้อนค่าสำหรับแต่ละรายการของ **SNMPv3 Settings**
3. คลิก **Next**

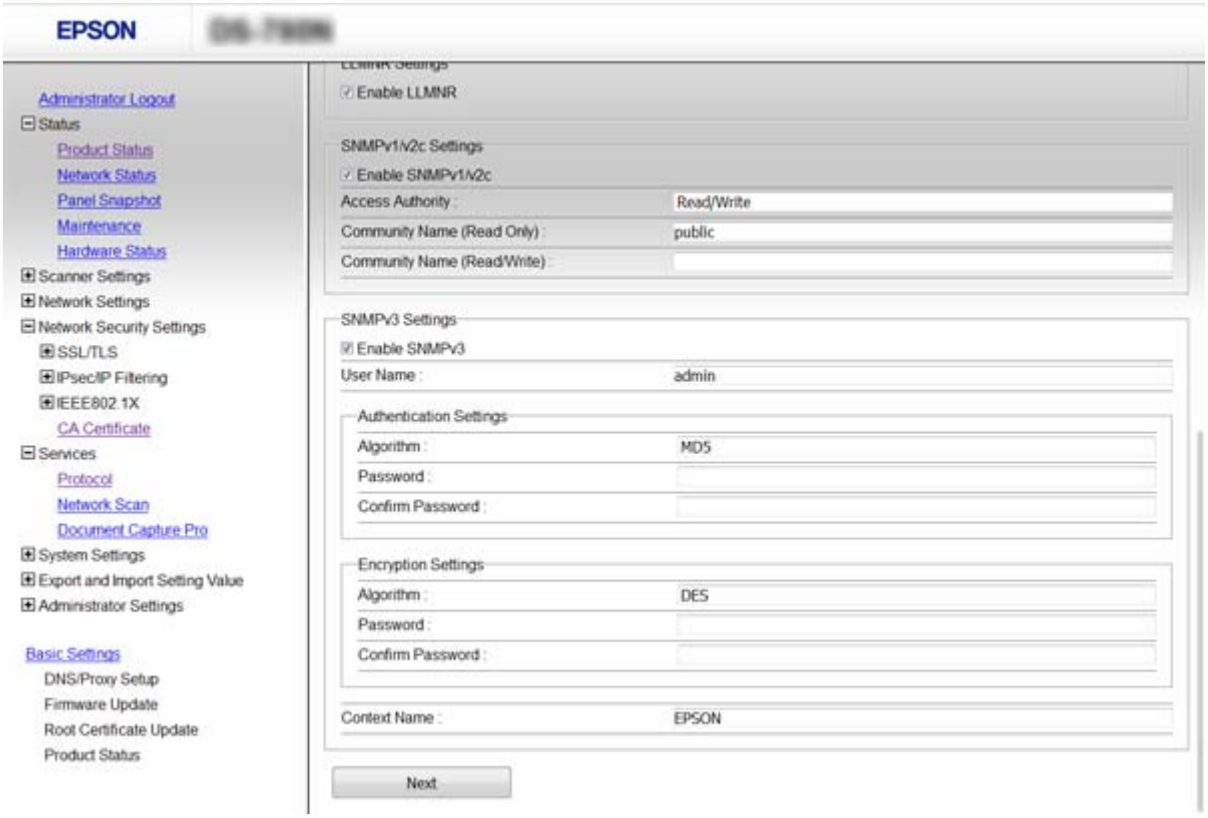
   ข้อความยืนยันจะแสดงขึ้นมา
4. คลิก **OK**

   สแกนเนอร์ได้รับการอัพเดทแล้ว

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "รายการการตั้งค่า SNMPv3" บนหน้าที่ 83

รายการการตั้งค่า SNMPv3



การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

รายการ	การตั้งค่าและคำอธิบาย
Enable SNMPv3	SNMPv3 ถูกเปิดใช้งานเมื่อกาเลือกในกล่องเลือกรายการ
User Name	ป้อนระหว่าง 1 และ 32 ตัวอักขระโดยใช้ตัวอักขระขนาด 1 ไบต์
Authentication Settings	
Algorithm	เลือกอัลกอริทึมสำหรับการรับรองความถูกต้อง
Password	ป้อนค่าระหว่าง 8 และ 32 ตัวอักขระในแบบ ASCII (0x20–0x7E)
Confirm Password	ป้อนรหัสผ่านที่คุณกำหนดค่าไว้เพื่อการยืนยัน
Encryption Settings	
Algorithm	เลือกอัลกอริทึมสำหรับการเข้ารหัส
Password	ป้อนค่าระหว่าง 8 และ 32 ตัวอักขระในแบบ ASCII (0x20–0x7E)
Confirm Password	ป้อนรหัสผ่านที่คุณกำหนดค่าไว้เพื่อการยืนยัน
Context Name	ป้อนระหว่าง 1 และ 32 ตัวอักขระโดยใช้ตัวอักขระขนาด 1 ไบต์

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดค่า SNMPv3" บนหน้าที่ 83

การเชื่อมต่อสแกนเนอร์เข้ากับเครือข่าย IEEE802.1X

การกำหนดค่าเครือข่าย IEEE802.1X

หากสแกนเนอร์รองรับ IEEE802.1X คุณสามารถใช้สแกนเนอร์บนเครือข่ายที่มีการรับรองความถูกต้องแล้วว่าได้เชื่อมต่อกับเซิร์ฟเวอร์ RADIUS และฮับในฐานะของผู้รับรอง

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **IEEE802.1X** > **Basic**
2. ป้อนค่าสำหรับแต่ละรายการ
3. คลิกที่ **Next**

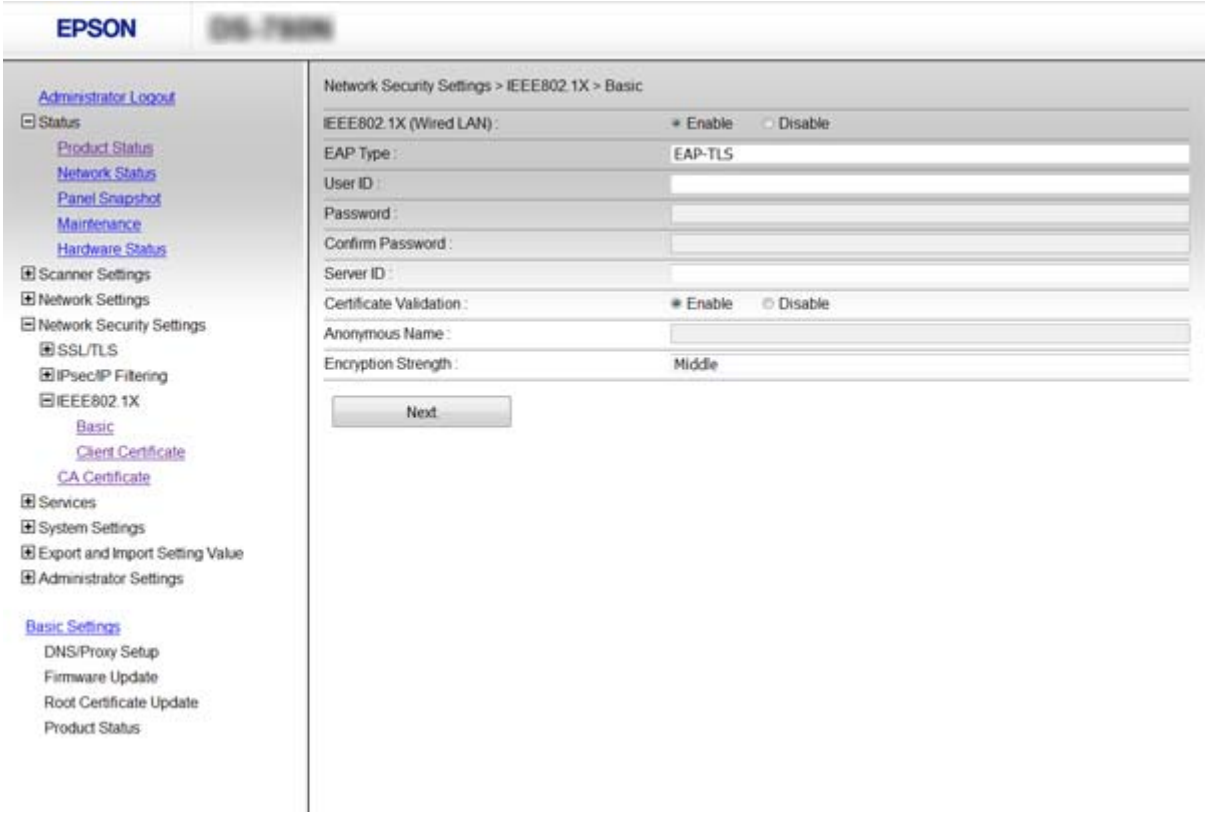
   ข้อความยืนยันจะแสดงขึ้นมา
4. คลิกที่ **OK**

   สแกนเนอร์ได้รับการอัพเดทแล้ว

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23
➡ "รายการการตั้งค่าเครือข่าย IEEE802.1X" บนหน้าที่ 85
➡ "ไม่สามารถเข้าถึงเครื่องพิมพ์หรือสแกนเนอร์หลังจากการกำหนดค่า IEEE802.1X" บนหน้าที่ 89

รายการการตั้งค่าเครือข่าย IEEE802.1X



รายการ	การตั้งค่าและคำอธิบาย	
IEEE802.1X (Wired LAN)	คุณสามารถเปิดใช้งานหรือปิดใช้งานการตั้งค่าของหน้า (**IEEE802.1X** > **Basic**) สำหรับ IEEE802.1X (LAN แบบต่อสาย)	
EAP Type	เลือกตัวเลือกสำหรับวิธีการรับรองความถูกต้องระหว่างสแกนเนอร์และเซิร์ฟเวอร์ RADIUS	
	EAP-TLS	คุณจะต้องขอรับและนำเข้าใบรับรองที่ลงนามจาก CA
	PEAP-TLS	
	PEAP/MSCHAPv2	คุณจะต้องกำหนดค่ารหัสผ่าน
User ID	กำหนดไอดีที่ใช้สำหรับการรับรองความถูกต้องของเซิร์ฟเวอร์ RADIUS ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว	
Password	กำหนดค่ารหัสผ่านเพื่อรับรองความถูกต้องของสแกนเนอร์ ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 1 ไบต์จำนวน 1 ถึง 128 ตัว หากคุณใช้เซิร์ฟเวอร์ Windows เป็นเซิร์ฟเวอร์ RADIUS คุณสามารถป้อนค่าได้มากสุดถึง 127 ตัวอักขระ	
Confirm Password	ป้อนรหัสผ่านที่คุณกำหนดค่าไว้เพื่อการยืนยัน	
Server ID	คุณสามารถกำหนดค่าไอดีเซิร์ฟเวอร์เพื่อรับรองความถูกต้องพร้อมกับเซิร์ฟเวอร์ RADIUS ที่กำหนดไว้ ผู้รับรองความถูกต้องจะตรวจสอบว่าไอดีเซิร์ฟเวอร์มีอยู่ในฟิลด์ subject/subjectAltName ของใบรับรองเซิร์ฟเวอร์ที่ถูกส่งมาจากเซิร์ฟเวอร์ RADIUS หรือไม่ ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 0 ไบต์จำนวน 1 ถึง 128 ตัว	
Certificate Validation	คุณสามารถตั้งค่าการตรวจสอบความถูกต้องใบรับรองโดยไม่ต้องคำนึงถึงวิธีการตรวจรับรองความถูกต้อง นำเข้าใบรับรองใน **CA Certificate**	

รายการ	การตั้งค่าและคำอธิบาย	
Anonymous Name	หากคุณเลือก **PEAP-TLS** หรือ **PEAP/MSCHAPv2** สำหรับ **Authentication Method** คุณจะไม่สามารถกำหนดค่าชื่อแบบไม่ระบุตัวตนแทนไอดีผู้ใช้สำหรับเฟส 1 ของการรับรองความถูกต้องของ PEAP ป้อนตัวอักขระ ASCII (0x20 ถึง 0x7E) ขนาด 0 ไบต์จำนวน 1 ถึง 128 ตัว	
Encryption Strength	คณสามารถเลือกค่าหนึ่งใดต่อไปนี้	
	High	AES256/3DES
	Middle	AES256/3DES/AES128/RC4

ข้อมูลที่เกี่ยวข้อง

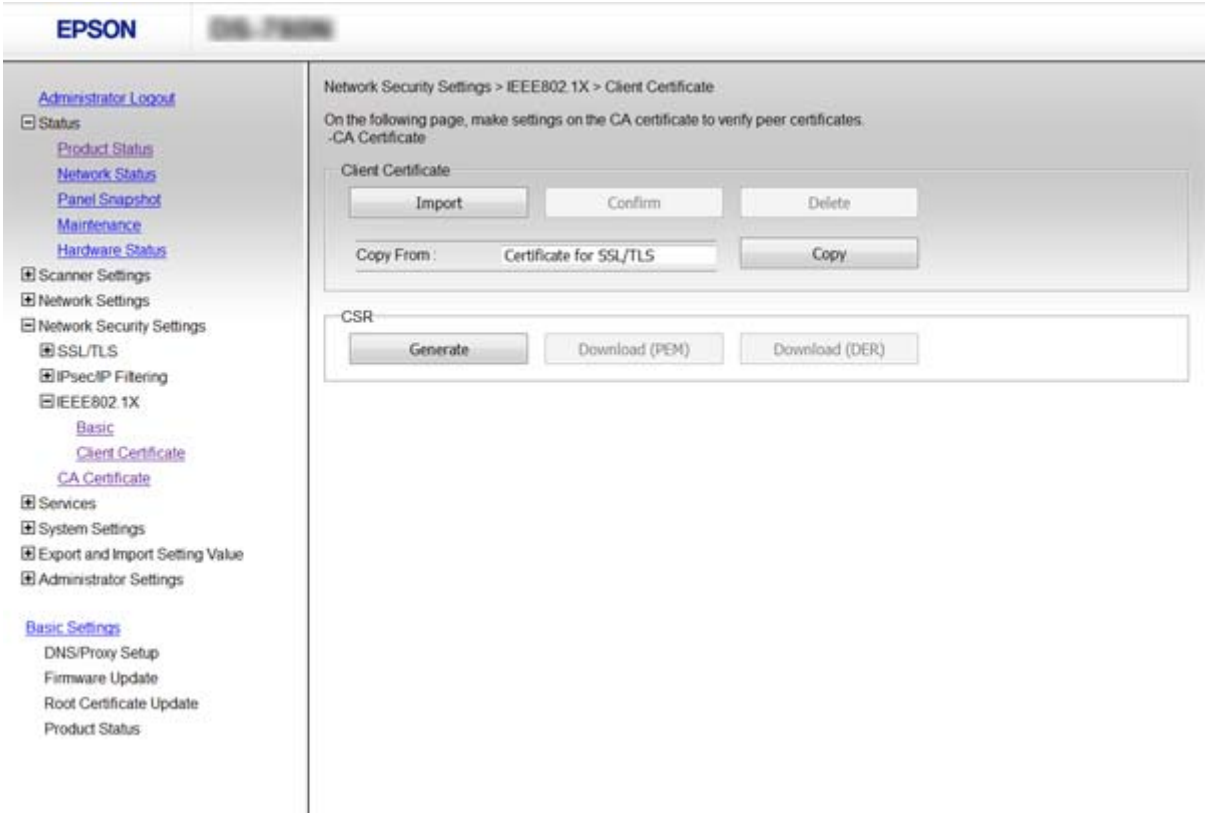
➡ "การกำหนดค่าเครือข่าย IEEE802.1X" บนหน้าที่ 84

การกำหนดค่าใบรับรองสำหรับ IEEE802.1X

กำหนดค่าใบรับรองไคลเอ็นท์สำหรับ IEEE802.1X หากคุณต้องการกำหนดค่าใบรับรองอนุญาตการรับรองความถูกต้อง ให้ไปที่ **CA Certificate**

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **IEEE802.1X** > **Client Certificate**
2. ป้อนใบรับรองใน **Client Certificate**

   คุณสามารถคัดลอกใบรับรองหากได้รับการจัดพิมพ์ให้โดยหน่วยงานอนุญาตออกใบรับรอง สำหรับการตัดลอกให้เลือกใบรับรองจาก **Copy From** จากนั้นคลิก **Copy**



ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

➡ "การขอรับและการนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 64

การแก้ไขปัญหาสำหรับความปลอดภัยขั้นสูง

การกู้คืนการตั้งค่าความปลอดภัย

เมื่อคุณจัดตั้งสภาพแวดล้อมความปลอดภัยระดับสูง เช่น การกรอง IPsec/IP หรือ IEEE802.1X คุณอาจไม่สามารถสื่อสารกับอุปกรณ์ได้เนื่องจากการตั้งค่าไม่ถูกต้อง หรือมีปัญหากับอุปกรณ์หรือเซิร์ฟเวอร์ ในกรณีนี้ ให้กู้คืนการตั้งค่าความปลอดภัยเพื่อที่จะทำการตั้งค่าสำหรับอุปกรณ์อีกครั้ง หรือเพื่ออนุญาตให้คุณใช้งานชั่วคราว

การปิดใช้งานฟังก์ชันความปลอดภัยโดยใช้แผงควบคุม

คุณสามารถปิดใช้งานการกรอง IPsec/IP หรือ IEEE802.1X โดยใช้แผงควบคุมของสแกนเนอร์

1. แตะที่ **การตั้งค่า** > **การตั้งค่าเครือข่าย**
2. แตะที่ **เปลี่ยนการตั้งค่า**
3. แตะรายการที่คุณต้องการปิดใช้งาน
   - ❑ **การกรอง IPsec/IP**
   - ❑ **IEEE802.1X**
4. เมื่อข้อความแจ้งการดำเนินการเสร็จสิ้นปรากฏขึ้น ให้แตะ **ดำเนินการ**

การกู้คืนฟังก์ชันความปลอดภัยโดยใช้ Web Config

สำหรับมาตรฐาน IEEE802.1X เครือข่ายอาจไม่รู้จักอุปกรณ์ ในกรณีนี้ ให้ปิดใช้งานฟังก์ชันโดยการใช้แผงควบคุมของสแกนเนอร์

สำหรับการกรอง IPsec/IP คุณสามารถปิดใช้งานฟังก์ชันหากคุณสามารถเข้าถึงอุปกรณ์จากคอมพิวเตอร์ได้

การปิดใช้งานการกรอง IPsec/IP โดยใช้ Web Config

1. เข้าถึง Web Config แล้วเลือก **Network Security Settings** > **IPsec/IP Filtering** > **Basic**
2. เลือก **Disable** สำหรับ **IPsec/IP Filtering** ใน **Default Policy**
3. คลิก **Next** จากนั้นล้าง **Enable this Group Policy** สำหรับนโยบายกลุ่ม
4. คลิกที่ **OK**

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

ปัญหาในการใช้คุณสมบัติความปลอดภัยของเครือข่าย

ลืมคีย์ที่แชร์ล่วงหน้า

กำหนดค่าคีย์อีกครั้งโดยใช้ Web Config

สำหรับการเปลี่ยนแปลงคีย์ ให้เข้าไปที่ Web Config จากนั้นเลือก **Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Default Policy** หรือ **Group Policy**

เมื่อคุณเปลี่ยนแปลงคีย์ที่แชร์ล่วงหน้า ให้กำหนดค่าคีย์ที่แชร์ล่วงหน้าสำหรับคอมพิวเตอร์

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

ไม่สามารถสื่อสารกับ IPsec

คุณกำลังใช้อัลกอริทึมที่ไม่รองรับสำหรับการตั้งค่าคอมพิวเตอร์หรือไม่

สแกนเนอร์รองรับอัลกอริทึมต่อไปนี้

วิธีการความปลอดภัย	อัลกอริทึม
อัลกอริทึมการเข้ารหัส IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
อัลกอริทึมการตรวจรับรองความถูกต้อง IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
อัลกอริทึมการแลกเปลี่ยนคีย์ 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*
อัลกอริทึมการเข้ารหัส ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
อัลกอริทึมการตรวจรับรองความถูกต้อง ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
อัลกอริทึมการตรวจรับรองความถูกต้อง AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* ใช้งานได้สำหรับ IKEv2 เท่านั้น

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้ารหัสการสื่อสารโดยใช้การกรอง IPsec/IP" บนหน้าที่ 71

ไม่สามารถสื่อสารได้ในทันที

ที่อยู่ IP ของสแกนเนอร์ไม่ถูกต้องหรือถูกเปลี่ยนแปลงหรือไม่

ปิดใช้งาน IPsec โดยใช้แผงควบคุมสแกนเนอร์

หาก DHCP หมดอายุ ให้รีบูท หรือหากที่อยู่ IPv6 หมดอายุหรือไม่ได้รับมา หลังจากนั้นอาจไม่พบที่อยู่ IP ที่ลงทะเบียนไว้สำหรับ Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Local Address (Scanner)**)

ใช้ที่อยู่ IP แบบคงที่

ที่อยู่ IP ของคอมพิวเตอร์ไม่ถูกต้องหรือถูกเปลี่ยนแปลงหรือไม่

ปิดใช้งาน IPsec โดยใช้แผงควบคุมสแกนเนอร์

หาก DHCP หมดอายุ ให้รีบูท หรือหากที่อยู่ IPv6 หมดอายุหรือไม่ได้รับมา หลังจากนั้นอาจไม่พบที่อยู่ IP ที่ลงทะเบียนไว้สำหรับ Web Config (**Network Security Settings** > **IPsec/IP Filtering** > **Basic** > **Group Policy** > **Remote Address(Host)**)

ใช้ที่อยู่ IP แบบคงที่

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้าถึง Web Config" บนหน้าที่ 23

➡ "การเข้ารหัสการสื่อสารโดยใช้การกรอง IPsec/IP" บนหน้าที่ 71

ไม่สามารถเชื่อมต่อกับการกรอง IPsec/IP

การตั้งค่าอาจไม่ถูกต้อง

ปิดใช้งานการกรอง IPsec/IP จากแผงควบคุมสแกนเนอร์ เชื่อมต่อสแกนเนอร์และคอมพิวเตอร์และตั้งค่าการกรอง IPsec/IP อีกครั้ง

ข้อมูลที่เกี่ยวข้อง

➡ "การเข้ารหัสการสื่อสารโดยใช้การกรอง IPsec/IP" บนหน้าที่ 71

ไม่สามารถเข้าถึงเครื่องพิมพ์หรือสแกนเนอร์หลังจากการกำหนดค่า IEEE802.1X

การตั้งค่าอาจไม่ถูกต้อง

ปิดใช้งาน IEEE802.1X จากแผงควบคุมของสแกนเนอร์ เชื่อมต่อสแกนเนอร์และคอมพิวเตอร์ จากนั้นกำหนดค่า IEEE802.1X อีกครั้ง

ข้อมูลที่เกี่ยวข้อง

➡ "การกำหนดค่าเครือข่าย IEEE802.1X" บนหน้าที่ 84

ปัญหาในการใช้ใบรับรองดิจิตัล

ไม่สามารถนำเข้าใบรับรองที่ลงนามจาก CA

ใบรับรองที่ลงนามจาก CA และข้อมูลบน CSR ตรงกันหรือไม่

หากใบรับรองที่ลงนามจาก CA และ CSR มีข้อมูลไม่ตรงกัน จะไม่สามารถนำเข้า CSR ได้ ตรวจสอบดังต่อไปนี้:

- ❑ คุณได้พยายามนำเข้าใบรับรองไปยังอุปกรณ์ที่ไม่มีข้อมูลตรงกันหรือไม่
  ตรวจสอบข้อมูลของ CSR จากนั้นนำเข้าใบรับรองไปยังอุปกรณ์ที่มีข้อมูลตรงกัน
- ❑ คุณได้เขียนทับ CSR ที่บันทึกไว้ในสแกนเนอร์หลังจากส่ง CSR ไปยังหน่วยงานออกใบรับรองหรือไม่
  จัดหาใบรับรองที่ลงนามจาก CA อีกครั้งพร้อมกับ CSR

ใบรับรองที่ลงนามจาก CA มีขนาดมากกว่า 5 KB หรือไม่

คุณไม่สามารถนำเข้าใบรับรองที่ลงนามจาก CA ที่มีขนาดมากกว่า 5 KB

รหัสผ่านสำหรับการนำเข้าใบรับรองถูกต้องหรือไม่

หากลืมรหัสผ่าน คุณจะไม่สามารถนำเข้าใบรับรองได้

ข้อมูลที่เกี่ยวข้อง

➡ "การนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 66

ไม่สามารถอัพเดทใบรับรองที่ลงนามด้วยตัวเอง

ได้ป้อนค่า Common Name เข้าไปหรือไม่

ค่า **Common Name** จะต้องถูกป้อนเข้าไป

มีตัวอักขระที่ไม่รองรับถูกป้อนเข้าไปใน Common Name หรือไม่ ตัวอย่างเช่น ไม่รองรับภาษาญี่ปุ่น

ป้อนตัวอักขระระหว่าง 1 ถึง 128 ของทั้ง IPv4, IPv6, ชื่อโฮสต์ หรือรูปแบบ FQDN ในแบบ ASCII (0x20–0x7E)

มีเครื่องหมายจุลภาคหรือเว้นว่างรวมอยู่ใน Common Name หรือไม่

หากใส่เครื่องหมายจุลภาคเข้าไป **Common Name** จะถูกแบ่งส่วน ณ จุดดังกล่าว หากป้อนเพียงการเคาะเว้นว่างก่อนหรือหลังเครื่องหมายจุลภาค จะมีข้อผิดพลาดเกิดขึ้น

ข้อมูลที่เกี่ยวข้อง

➡ "การอัพเดตใบรับรองที่ลงนามด้วยตัวเอง" บนหน้าที่ 68

ไม่สามารถสร้าง CSR

ได้ป้อนค่า Common Name เข้าไปหรือไม่

ค่า **Common Name** จะต้องถูกป้อนเข้าไป

มีตัวอักขระที่ไม่รองรับถูกป้อนเข้าไปใน Common Name, Organization, Organizational Unit, Locality, State/Province หรือไม่ ตัวอย่างเช่น ไม่รองรับภาษาญี่ปุ่น

ป้อนตัวอักขระของทั้ง IPv4, IPv6, ชื่อโฮสต์ หรือรูปแบบ FQDN ในแบบ ASCII (0x20–0x7E)

มีเครื่องหมายจุลภาคหรือเว้นว่างรวมอยู่ใน Common Name หรือไม่

หากใส่เครื่องหมายจุลภาคเข้าไป **Common Name** จะถูกแบ่งส่วน ณ จุดดังกล่าว หากป้อนเพียงการเคาะเว้นว่างก่อนหรือหลังเครื่องหมายจุลภาค จะมีข้อผิดพลาดเกิดขึ้น

ข้อมูลที่เกี่ยวข้อง

➡ "การขอรับใบรับรองที่ลงนามจาก CA" บนหน้าที่ 64

คำเตือนที่ปรากฏขึ้นเกี่ยวกับใบรับรองดิจิตัล

ข้อความ	สาเหตุ/สิ่งที่ควรทำ
Enter a Server Certificate.	**สาเหตุ:** คุณไม่ได้เลือกไฟล์ที่จะนำเข้า **สิ่งที่ควรทำ:** เลือกไฟล์และคลิก **Import**
CA Certificate 1 is not entered.	**สาเหตุ:** ใบรับรอง CA 1 ไม่ได้ป้อนเข้าไปและมีเพียงใบรับรอง CA 2 ถูกป้อนเข้าไป **สิ่งที่ควรทำ:** นำเข้าใบรับรอง CA 1 ก่อน
Invalid value below.	**สาเหตุ:** มีตัวอักขระที่ไม่รองรับในเส้นทางไฟล์ และ/หรือรหัสผ่าน **สิ่งที่ควรทำ:** ตรวจสอบให้แน่ใจว่าได้ป้อนค่าอย่างถูกต้องแต่ละรายการ
Invalid date and time.	**สาเหตุ:** ไม่ได้ตั้งวันที่และเวลาของสแกนเนอร์ **สิ่งที่ควรทำ:** ตั้งวันที่และเวลาโดยใช้ Web Config หรือ EpsonNet Config
Invalid password.	**สาเหตุ:** รหัสผ่านที่ตั้งไว้สำหรับใบรับรอง CA และรหัสที่ป้อนเข้าไม่ตรงกัน **สิ่งที่ควรทำ:** ป้อนรหัสผ่านที่ถูกต้อง

การตั้งค่าความปลอดภัยขั้นสูงสำหรับองค์กร

ข้อความ	สาเหตุ/สิ่งที่ควรทำ
Invalid file.	**สาเหตุ:** คุณไม่ได้นำเข้าไฟล์ใบรับรองในรูปแบบ X509 **สิ่งที่ควรทำ:** ตรวจสอบให้แน่ใจว่าได้เลือกใบรับรองที่ถูกต้องที่ส่งโดยหน่วยงานออกใบรับรองที่เชื่อถือได้
	สาเหตุ: ไฟล์ที่นำเข้ามีขนาดใหญ่เกินไป ขนาดไฟล์สูงสุดคือ 5 KB **สิ่งที่ควรทำ:** หากคุณเลือกไฟล์ที่ถูกต้อง ใบรับรองอาจจะเสียหายหรือถูกแก้ไข
	สาเหตุ: สายโซ่ที่อยู่ในใบรับรองไม่ถูกต้อง **สิ่งที่ควรทำ:** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับใบรับรอง ดูที่เว็บไซต์ของหน่วยงานออกใบรับรอง
Cannot use the Server Certificates that include more than three CA certificates.	**สาเหตุ:** ไฟล์ใบรับรองในรูปแบบ PKCS#12 มีใบรับรอง CA มากกว่า 3 ใบ **สิ่งที่ควรทำ:** นำเข้าแต่ละใบรับรองโดยการแปลงจากรูปแบบ PKCS#12 ไปยังรูปแบบ PEM หรือนำเข้าไฟล์ใบรับรองในรูปแบบ PKCS#12 ที่ประกอบด้วยใบรับรอง CA 2 ใบ
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**สาเหตุ:** ใบรับรองหมดอายุ **สิ่งที่ควรทำ:** ❑ หากใบรับรองหมดอายุ ให้ขอรับและนำเข้าใบรับรองใหม่ ❑ หากใบรับรองยังไม่หมดอายุ ตรวจสอบว่าได้ตั้งวันที่และเวลาของสแกนเนอร์อย่างถูกต้อง
Private key is required.	**สาเหตุ:** ไม่มีคีย์ส่วนตัวที่จับคู่กันกับใบรับรอง **สิ่งที่ควรทำ:** ❑ หากใบรับรองเป็นรูปแบบ PEM/DER และได้มาจาก CSR โดยใช้คอมพิวเตอร์ ให้ระบุไฟล์คีย์ส่วนตัว ❑ หากใบรับรองเป็นรูปแบบ PKCS#12 และได้มาจาก CSR โดยใช้คอมพิวเตอร์ ให้สร้างไฟล์ที่มีคีย์ส่วนตัว
	สาเหตุ: คุณได้นำเข้าอีกครั้งของใบรับรอง PEM/DER ที่ได้มาจาก CSR ที่ใช้ Web Config **สิ่งที่ควรทำ:** หากใบรับรองเป็นรูปแบบ PEM/DER และได้มาจาก CSR โดยใช้ Web Config คุณสามารถนำเข้าได้ครั้งเดียวเท่านั้น

ข้อความ	สาเหตุ/สิ่งที่ควรทำ
Setup failed.	**สาเหตุ:** ไม่สามารถสิ้นสุดการกำหนดค่าเนื่องจากการสื่อสารระหว่างสแกนเนอร์และคอมพิวเตอร์ล้มเหลว หรือไฟล์ไม่สามารถอ่านได้เนื่องจากมีข้อผิดพลาดบางอย่าง **สิ่งที่ควรทำ:** หลังจากตรวจสอบไฟล์ที่กำหนดไว้และการสื่อสารแล้ว ให้นำเข้าไฟล์อีกครั้ง

ข้อมูลที่เกี่ยวข้อง

➡ "เกี่ยวกับใบรับรองดิจิตัล" บนหน้าที่ 63

การลบใบรับรองที่ลงนามรับรองจาก CA โดยไม่ตั้งใจ

มีไฟล์สำรองของใบรับรองหรือไม่

หากคุณมีไฟล์สำรอง ให้นำเข้าใบรับรองอีกครั้ง

หากคุณได้รับใบรับรองโดยใช้ CSR ที่สร้างจาก Web Config คุณจะไม่สามารถนำเข้าใบรับรองที่ลบไปแล้วได้อีกครั้ง สร้าง CSR และขอรับใบรับรองใหม่

ข้อมูลที่เกี่ยวข้อง

➡ "การลบใบรับรองที่ลงนามจาก CA" บนหน้าที่ 67

➡ "การนำเข้าใบรับรองที่ลงนามจาก CA" บนหน้าที่ 66