EPSON
EXCEED YOUR VISION

מדריך למנהל המערכת

NPD5668-00 HE

תוכן עניינים

זכויות יוצרים

סימנים מסחריים

על אודות מדריך זה

סימנים וסמלים. .6
תיאורים המשמשים במדריך זה. 6
אזכורים של מערכות הפעלה. 6

מבוא

רכיב המדריך. 8
הגדרות מונחים המופיעים במדריך זה. 8

הכנה

זרימת הגדרות סורק וניהול. 10
דוגמאות לסביבת רשת. 11
מבוא לדוגמת הגדרת חיבור סורק. 11
הכנת חיבור לרשת. 12
איסוף מידע על הגדרת החיבור. 12
מפרט הסורק. 13
השימוש במספר יציאה. 13
סוג הקצאת כתובת IP. 13
שרת DNS ושרת פרוקסי. 13
שיטה להגדרת חיבור רשת. 13

חיבור

התחברות אל הרשת. 15
התחברות לרשת מלוח הבקרה. 15
חיבור לרשת באמצעות תוכנת ההתקנה. 19

הגדרות פונקציות

תוכנה עבור הגדרות. 22
Web Config (דף אינטרנט עבור התקן). 22
השימוש בפונקציות סריקה. 24
סריקה ממחשב. 24
סריקה באמצעות לוח הבקרה. 26
ביצוע הגדרות מערכת. 28
ביצוע הגדרות מערכת בלוח הבקרה. 28
ביצוע הגדרות מערכת באמצעות Web Config. 30

הגדרות אבטחה בסיסיות

מבוא למאפייני אבטחה בסיסיים. 32
הגדרת סיסמת מנהל מערכת. 32
הגדרת התצורה של סיסמת המנהל מתוך לוח הבקרה. 33
הגדרת תצורת סיסמת המנהל באמצעות Web Config. 33
פריטים המיועדים לנעילה באמצעות סיסמת המנהל. 34
בקרת פרוטוקולים. 35
פרוטוקולים שניתן לאפשר או להשבית. 36
פריטי הגדרת פרוטוקולים. 37

הגדרות תפעול וניהול

אשר מידע על התקן. 40
ניהול התקנים (Epson Device Admin). . . .40
קבלת התראות בדואר אלקטרוני כאשר מתרחשים אירועים. .41
אודות התראות דואר אלקטרוני. 41
הגדרת התראות דואר אלקטרוני. 41
הגדרת שרת דואר. 42
בדיקת חיבור לשרת דואר. 44
עדכון קושחה. 46
עדכון קושחה באמצעות Web Config. 46
עדכון קושחה באמצעות Epson Firmware Updater. 47
גיבוי ההגדרות. 47
יצא את ההגדרות. 47
יבא את ההגדרות. 48

פתרון בעיות

טיפים לפתרון בעיות. 49
בדיקת קובץ הרישום עבור שרת והתקן רשת. 49
אתחול הגדרות הרשת. 49
שחזור הגדרות הרשת מלוח הבקרה. 49
בדיקת התקשורת בין התקנים למחשבים. 49
בדיקת החיבור באמצעות פקודת — PingWindows. 49
בדיקת החיבור שלך באמצעות פקודת Ping — Mac OS51. . . . .
בעיות בשימוש בתוכנת רשת. 52
לא ניתן לגשת אל Web Config. 52
שם דגם ו/או כתובת UP אינם מוצגים ב-EpsonNet Config53. . . . .

תוכן עניינים

נספח

מבוא לתוכנת רשת. 55
Epson Device Admin. 55
EpsonNet Config. 55
EpsonNet SetupManager. 56
הקצאת כתובת IP באמצעות EpsonNet Config. 56
הקצאת כתובת IP באמצעות הגדרות אצווה. 56
הקצאת כתובת IP לכל התקן. 59
השימוש ביציאה עבור הסורק. 60

הגדרות אבטחה מתקדמות עבור ארגון

הגדרות אבטחה ומניעת סכנה. 62
הגדרות תכונת האבטחה. 63
תקשורת SSL/TLS עם הסורק. 63
אודות אישורים דיגיטליים. 63
השגה וייבוא של אישור החתום על-ידי ר"מ. 64
מחיקת אישור החתום בידי רשות אישורים. . . . 68
עדכון אישור בחתימה עצמית. 68
הגדר CA Certificate. 69
תקשורת מוצפנת באמצעות IPsec/סינון IP. . . . 71
אודות IPsec/IP Filtering. 71
הגדרת Default Policy. 72
הגדרת Group Policy. 76
דוגמאות לתצורת IPsec/IP Filtering. 82
הגדרת אישור עבור IPsec/IP Filtering. 84
שימוש בפרוטוקול SNMPv3. 84
על אודות SNMPv3. 84
הגדרת SNMPv3. 85
חיבור הסורק לרשת IEEE802.1X. 86
הגדרת תצורה לרשת IEEE802.1X. 86
הגדרת אישור עבור IEEE802.1X. 88
פתירת בעיות עבור אבטחה מתקדמת. 89
שחזור הגדרות האבטחה. 89
בעיות בשימוש בתכונות אבטחת רשת. 90
בעיות במהלך השימוש באישור דיגיטלי. 92

זכויות יוצרים

אין לשכפל, לאחסן במערכת אחזור, או לשדר פרסום זה בכל צורה שהיא או בכל אמצעי שהוא, בין אלקטרוני, בין מכני, בין בצילום, הקלטה או כל דרך אחרת, בלא הסמכה בכתב מראש של חברת Seiko Epson. אין הנחה של חבות פטנט כלשהי ביחס לשימוש במידה הכלול כאן. אף אין הנחה של חבות כלשהי בגין נזקים שמקורם בשימוש במידע הכלול כאן. המידע הכלול כאן נועד אך ורק לשימוש עם מוצר Epson זה. Epson אינה אחראית לשימוש כלשהו במידע זה ביחס למוצרים אחרים.

חברת Seiko Epson והחברות המסונפות לה לא תישאנה בכל חבות כלפי רוכש מוצר זה או צד שלישי כלשהו בגין נזקים, אובדן, עלויות או הוצאות שנגרמו לרוכש או לצד שלישי כלשהו כתוצאה מתאונה, שימוש שגוי, או שימוש לרעה במוצר זה או ביצוע שינויים בלתי מורשים, תיקונים או שינויים אחרים במוצר זה, או (לא כולל ארה"ב) אי הקפדה על ציות להוראות התפעול והתחזוקה של חברת Seiko Epson.

חברת Seiko Epson והחברות המסונפות לה לא תשאנה בכל חבות בגין נזקים או בעיות שמקורם בשימוש באפשרות כלשהי או במוצרי צריכה אחרים כלשהם פרט לאלו שהוגדרו כמוצרי Epson מקוריים או מוצרי Epson מאושרים על ידי חברת Seiko Epson.

חברת Seiko Epson לא תישא בכל חבות בגין נזק שמקורו בהפרעות אלקטרומגנטיות המתרחשות כתוצאה מהשימוש בכבלי ממשק כלשהם מחוץ לאלא שהוגדרו כמוצרי Epson מאושרים על ידי חברת Seiko Epson.

©Seiko Epson Corporation 2016.

תוכן מדריך זה ומפרטי מוצר זה נתונים לשינויים ללא הודעה מראש.

סימנים מסחריים

- ❏ ®EPSON הוא סימן מסחרי רשום והביטויים EPSON EXCEED YOUR VISION או EXCEED YOUR VISION הם סימנים מסחריים של 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.
- ❏ הערה כללית: שמות מוצרים אחרים הנזכרים כאן נועדו לשם זיהוי בלבד וייתכן שהם יהיו סימנים מסחריים של בעליהם. Epson מתנערת מכל זכות בסימנים אלה.

על אודות מדריך זה

סימנים וסמלים

זהירות:
מכילים הוראות שיש להקפיד לציית להן כדי למנוע פציעה.

חשוב:
יש להקפיד על מילוי ההוראות הללו כדי למנוע נזק לציוד.

לתשומת לבך:
הוראות המכילות טיפים שימושיים והגבלות על פעולת הסורק.

מידע קשור
➡ לחיצה על סמל זה תעביר אותך אל המידע הרלבנטי.

תיאורים המשמשים במדריך זה

❏ צילומי המסך של מנהל התקן הסורק ושל ה- Epson Scan 2 (מנהל התקן סורק) לקוחים מתוך Windows 10 או OS X El Capitan. התוכן המוצג על המסך משתנה, תלוי בדגם ובמצב.

❏ האיורים המשמשים במדריך זה הם להמחשה בלבד. אמנם יכולים להיות הבדלים קלים בתפעול, תלוי בדגם, אולם שיטת התפעול היא אותה השיטה.

❏ פריטי תפריט מסוימים במסך ה-LCD משתנים, תלוי בדגם ובהגדרות.

אזכורים של מערכות הפעלה

Windows

במדריך זה, מונחים כגון "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", ו-"Windows Server 2003" מתייחסים למערכות ההפעלה הבאות. כמו כן, המונח Windows משמש לציון כל הגרסאות.

❏ מערכת ההפעלה Microsoft® Windows® 10

❏ מערכת ההפעלה Microsoft® Windows® 8.1

❏ מערכת ההפעלה Microsoft® Windows® 8

❏ מערכת ההפעלה Microsoft® Windows® 7

על אודות מדריך זה

- ❑ מערכת ההפעלה Microsoft® Windows Vista®
- ❑ מערכת ההפעלה Microsoft® Windows® XP
- ❑ מערכת ההפעלה Microsoft® Windows® XP Professional x64 Edition
- ❑ מערכת ההפעלה Microsoft® Windows Server® 2016
- ❑ מערכת ההפעלה Microsoft® Windows Server® 2012 R2
- ❑ מערכת ההפעלה Microsoft® Windows Server® 2012
- ❑ מערכת ההפעלה Microsoft® Windows Server® 2008 R2
- ❑ מערכת ההפעלה Microsoft® Windows Server® 2008
- ❑ מערכת ההפעלה Microsoft® Windows Server® 2003 R2
- ❑ מערכת ההפעלה Microsoft® Windows Server® 2003

Mac OS

במדריך זה, "Mac OS" משתמש כדי להתייחס אל macOS Sierra, OS X El Capitan, OS X Yosemite, OS X Mavericks, OS X Mountain Lion, Mac OS X v10.7.x, ו- Mac OS X v10.6.8.

מבוא

רכיב המדריך

מדריך זה נועד עבור מנהל ההתקן האחראי לחיבור המדפסת או הסורק אל הרשת והוא מכיל מידע המסביר כיצד לבצע הגדרות כדי להשתמש בפונקציות.

עיין ב-*מדריך למשתמש* עבור מידע על השימוש בפונקציה.

הכנה

מסביר את משימות המנהל, כיצד להגדיר התקנים, ואת התוכנה לניהול.

חיבור

מסביר כיצד לחבר התקן אל הרשת או אל קו טלפון. מסביר גם את סביבת הרשת, כגון השימוש ביציאה עבור ההתקן ומידע על DNS ושרת פרוקסי.

הגדרות פונקציות

מסביר את ההגדרות עבור כל פונקציה בהתקן.

הגדרות אבטחה בסיסיות

מסביר את ההגדרות עבור כל פונקציה, כגון הדפסה, סריקה ופעולות פקס.

הגדרות תפעול וניהול

מסביר את הפעולות אחרי התחלת השימוש בהתקנים, כגון בדיקת מידע ותחזוקה.

פתרון בעיות

מסביר את אתחול ההגדרות וכיצד לפתור בעיות ברשת.

הגדרות אבטחה מתקדמות עבור ארגון

מסביר את שיטת ההגדרות לשיפור האבטחה של ההתקן, כגון השימוש באישור CA, תקשורת SSL/TLS, וסינון IPsec/IP.

בהתאם לדגם, אפשר שלא תהיה תמיכה בכמה מהפונקציות המתוארות בפרק זה.

הגדרות מונחים המופיעים במדריך זה

המונחים הבאים מופיעים במדריך זה.

מנהל

האשם האחראי להתקנה והגדרה של ההתקן או של הרשת במשרד או בארגון. בארגונים קטנים, אפשר שאדם זה יהיה אחראי הן על ניהול ההתקן והרשת כאחד. בארגונים גדולים, למנהלים יש סמכות לטפל ברשת או בהתקנים של

יחידה קבוצתית במחלקה או חטיבה, בעוד שמנהלי רשת אחראים על הגדרות התקשורת החורגות אל מחוץ לארגון, כגון האינטרנט.

מנהל רשת

האדם האחראי לשליטה בתקשורת ברשת. האדם שמגדיר את הנתב, את שרת הפרוקסי, את שרת ה-DNS ואת שרת הדואר על מנת לשלוט בתקשורת באינטרנט או ברשת.

משתמש

האדם המשתמש בהתקנים כמו מדפסות או סורקים.

Web Config (דף האינטרנט של ההתקן)

שרת האינטרנט המובנה בתוך ההתקן. הוא נקרא Web Config. תוכל לבדוק בו את סטטוס ההתקן ולשנותו באמצעות הדפדפן.

כלי

שם כללי עבור תוכנה המגדירה או מנהל התקן, כגון Epson Device Admin, EpsonNet Config, EpsonNet SetupManager, וכו'.

סריקה בלחיצה

שם כללי לסריקה מלוח הבקרה של ההתקן.

ASCII (קוד אמריקני תקני לחילופי מידע)

אחת מהקודים הסטנדרטים עבור תווים. קוד זה מגדיר 128 תווים, כולל תווים כמו אותיות האלפבית האנגלי (a–z, A–Z), ספרות רגילות (0–9), סמלים, תווים ריקים ותווי בקרה. כאשר מוזכר "ASCII" במדריך זה, מדובר ברצף 0x20–0x7E (מספר הקסדצימאלי) הרשום להלן, ואינו כולל תווי בקרה.

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	{			}	~	

* תו הרווח.

Unicode (קידוד UTF-8)

קוד סטנדרטי בינלאומי, המכסה את שפות העולם העיקריות. כאשר מוזכר "UTF-8" במדריך זה, הכוונה היא לתווי הקידוד הכלולים בפורמט UTF-8.

הכנה

פרק זה מסביר את תפקיד המנהל ואת ההכנה לפני ביצוע ההגדרות.

זרימת הגדרות סורק וניהול

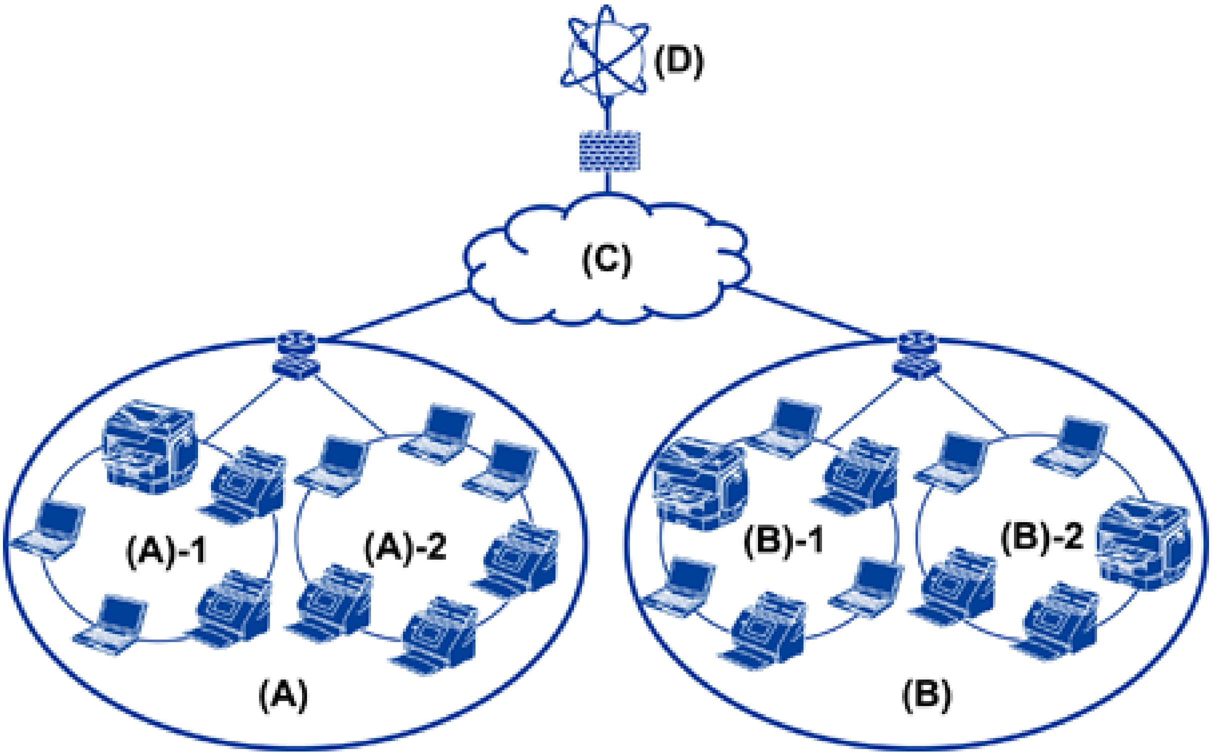
המנהל מבצע את הגדרות חיבור הרשת ואת ההגדרות והתחזוקה הראשוניות של הסורק כדי שיהיו זמינים למשתמשים.

1. מכינה
   - ❏ אוספת מידע על הגדרת החיבור
   - ❏ החלטה על שיטות החיבור
2. מתחברת
   - ❏ חיבור רשת מתוך לוח הבקרה של הסורק
3. הגדרת הפונקציות
   - ❏ הגדרות מנהל התקן סורק
   - ❏ הגדרות מתקדמות אחרות
4. הגדרת אבטחה
   - ❏ הגדרות מנהל
   - ❏ SSL/TLS
   - ❏ בקרת פרוטוקול
   - ❏ הגדרות אבטחה מתקדמות (אופציה)
5. תפעול וניהול
   - ❏ בדיקת מצב ההתקן
   - ❏ הטיפול בהופעתם של אירועים
   - ❏ גיבוי הגדרות ההתקן

מידע קשור

➡ "הכנה" בעמוד 10
➡ "חיבור" בעמוד 15
➡ "הגדרות פונקציות" בעמוד 22
➡ "הגדרות אבטחה בסיסיות" בעמוד 32
➡ "הגדרות תפעול וניהול" בעמוד 40

דוגמאות לסביבת רשת



(א): משרד 1

- ❏ (א) – 1: LAN 1
- ❏ (א) – 2: LAN 2

(ב): משרד 2

- ❏ (ב) – 1: LAN 1
- ❏ (ב) – 2: LAN 2

(ג): WAN

(ד): אינטרנט

מבוא לדוגמת הגדרת חיבור סורק

קיימים שני סוגי חיבור בהתאם לאופן שבו אתה משתמש בסורק. שניהם מחברים את הסורק לרשת עם מחשב באמצעות הרכזת.

- ❏ חיבור שרת/לקוח (הסורק משתמש בשרת Windows, ניהול עבודות)
- ❏ חיבור עמית לעמית (חיבור ישיר באמצעות מחשב לקוח)

מידע קשור

➡ "חיבור שרת/לקוח" בעמוד 12
➡ "הגדרות חיבור עמית לעמית" בעמוד 12

חיבור שרת/לקוח

רכז את ניהול הסורק והעבודות עם Document Capture Pro Server המותקן בשרת. תוכנה זו היא המתאימה ביותר לעבודה המשתמשת בריבוי סורקים כדי לסרוק מספר גדול של מסמכים בפורמט מסוים.

מידע קשור

➡ "הגדרות מונחים המופיעים במדריך זה" בעמוד 8

הגדרות חיבור עמית לעמית

עם סורק נבדל יש להשתמש במנהל התקן סורק כגון Epson Scan 2 המותקן במחשב הלקוח. התקנת Document Capture Pro (Document Capture) במחשב הלקוח מאפשרת לך לבצע עבודות במחשבי הלקוח של הסורק הנבדל.

מידע קשור

➡ "הגדרות מונחים המופיעים במדריך זה" בעמוד 8

הכנת חיבור לרשת

איסוף מידע על הגדרת החיבור

אתה זקוק לכתובת IP, לכתובת שער, וכו', עבור חיבור רשת. בדוק את הפרטים הבאים מראש.

מחלקות	פריטים	הערה
שיטת חיבור ההתקן	❏ Ethernet	יש להשתמש בכבל STP (זוג שזור מסוכך) מקטגוריה 5e ומעלה עבור חיבור ה-Ethernet.
מידע על חיבור ה-LAN	❏ כתובת IP ❏ מסכת רשת משנה ❏ שער ברירת מחדל	אם הגדרת באופן אוטומטי את כתובת ה-IP באמצעות פונקציית ה-DHCP של הנתב, אין בכך צורך.
מידע על שרת DNS	❏ כתובת IP עבור DNS ראשי ❏ כתובת IP עבור DNS משני	אם אתה משתמש בכתובת IP סטטית ככתובת ה-IP, הגדר את תצורת שרת ה-DNS. הגדרת את התצורה כאשר אתה מקצה אוטומטית באמצעות פונקציית ה-DHCP וכאשר לא ניתן להקצות את שרת ה-DNS באופן אוטומטי.
מידע על שרת הפרוקסי	❏ שם שרת הפרוקסי ❏ מספר יציאה	הגדר תצורה בעת השימוש בשרת פרוקסי עבור חיבור אינטרנט ובעת השימוש בשירות Epson Connect או פונקציית העדכון האוטומטית של הקושחה.

מפרט הסורק

למפרט המתאר את תמיכת הסורק במצב רגיל או במצב חיבור, עיין ב-*מדריך למשתמש*.

השימוש במספר יציאה

עיין ב"נספח" עבור מספר היציאה בו משתמש הסורק.

מידע קשור

➡ "השימוש ביציאה עבור הסורק" בעמוד 60

סוג הקצאת כתובת IP

קיימים שני סוגים של הקצאת כתובת IP לסורק.

כתובת IP סטטית:

הקצה לסורק את כתובת ה-IP הייחודית שנקבעה מראש.

כתובת ה-IP אינה משתנה כאשר מכבים את הסורק או את הנתב, ולכן תוכל לנהל את ההתקן על פי כתובת IP.

סוג זה של הקצאת IP מתאים לרשת שבה מנהלים סורקים רבים, כגון זו של משרד גדול או בית ספר.

הקצאה אוטומטית באמצעות פונקציית DHCP:

כתובת ה-IP הנכונה מוקצית באופן אוטומטי כאשר מצליחה התקשורת בין הסורק לבין הנתב התומכת בתפקוד ה-DHCP.

אין זה נוח לשנות את כתובת ה-IP עבור התקן ספציפי, לשמור את כתובת ה-IP מראש ואז להקצות אותה.

שרת DNS ושרת פרוקסי

אם אתה משתמש בשירות חיבור אינטרנטי, הגדר את תצורת שרת ה-DNS. אם לא תגדיר את התצורה, יהיה עליך לציין את כתובת ה-IP לגישה משום שאתה עשוי להיכשל ברזולוציה של השם.

שרת הפרוקסי ממוקם בשער שבין הרשת לבין האינטרנט, והוא מתקשר עם המחשב, הסורק והאינטרנט (השרת הנגדי) מטעם כל אחד מהם. השרת הנגדי מתקשר רק עם שרת הפרוקסי. לכן, לא ניתן לקרוא מידע על הסורק, כגון כתובת ה-IP ומספר היציאה, ולכן ניתן לצפות לאבטחה מוגברת.

תוכל לאסור גישה אל URL ספציפי באמצעות פונקציית הסינון, מאחר ושרת הפרוקסי מסוגל לבדוק את תכולת התקשורת.

שיטה להגדרת חיבור רשת

פעל בהתאם להוראות הבאות כדי לבצע הגדרות חיבור עבור כתובת ה-IP של הסורק, מסיכת רשת משנה, ושער ברירת המחדל.

הכנה

השימוש בלוח הבקרה:

הגדר את תצורת ההגדרות באמצעות לוח בקרת הסורק של כל סורק. התחבר אל הרשת אחרי הגדרת תצורת הגדרות החיבור של הסורק.

השימוש בתוכנת ההתקנה:

אם אתה משתמש בתוכנת התקנה, יוגדרו הרשת של הסורק והמחשב הלקוח באופן אוטומטי. ההגדרה זמינה אם פועלים בהתאם להוראות תוכנת ההתקנה, גם אם אין לך ידע מעמיק על הרשת.

השימוש בכלי:

תוכל להשתמש בכלי ממחשב המנהל. תוכל לגלות סורק ואז להגדיר את הסורק, או ליצור קובץ SYLK כדי לבצע הגדרות אצווה עבור סורקים. תוכל להגדיר סורקים רבים, אך עליהן להיות מחוברים פיזית באמצעות כבל Ethernet לפני ביצוע ההגדרה. לכן, שיטה זו מומלצת אם ביכולתך לבנות Ethernet עבור ההגדרה.

מידע קשור

➡ "התחברות לרשת מלוח הבקרה" בעמוד 15
➡ "חיבור לרשת באמצעות תוכנת ההתקנה" בעמוד 19
➡ "הקצאת כתובת IP באמצעות EpsonNet Config" בעמוד 56

חיבור

פרק זה מסביר את הסביבה או את הנוהל כדי לחבר את הסורק לרשת.

התחברות אל הרשת

התחברות לרשת מלוח הבקרה

חבר את הסורק לרשת באמצעות לוח הבקרה של המדפסת.

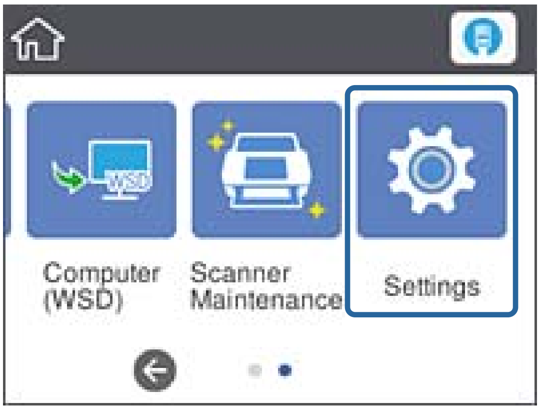
לפרטים נוספים על לוח הבקרה של הסורק עיין ב-*מדריך למשתמש*.

הקצאת כתובת ה-IP

הגדר פרטים בסיסיים כמו כתובת IP, מסכת רשת משנה, ו- שער ברירת מחדל.

1. הדלק את הסורק.

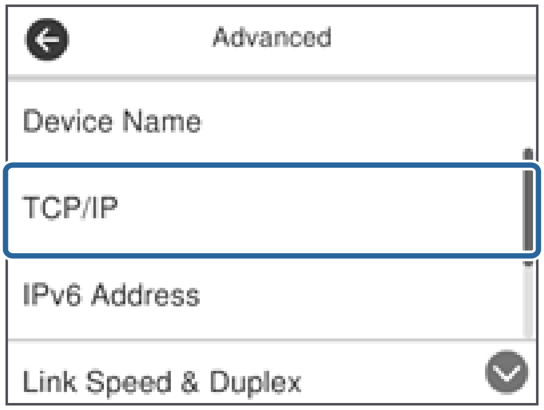
2. החלק את המסך שמאלה בלוח הבקרה של הסורק, ואז הקש **הגדרות**.



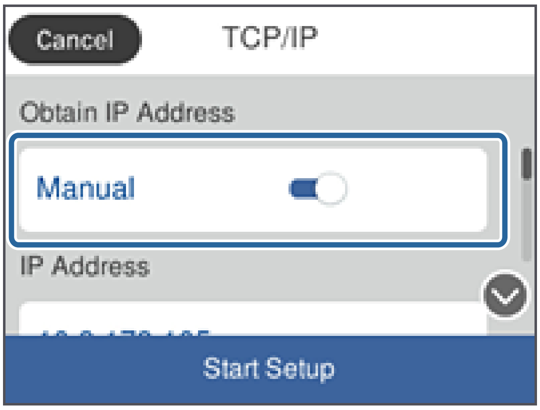
3. הקש **הגדרות רשת** > **שינוי ההגדרות**.

   אם הפריט אינו מוצג, החלק את המסך כלפי מעלה כדי להציגו.

4. הקש TCP/IP.

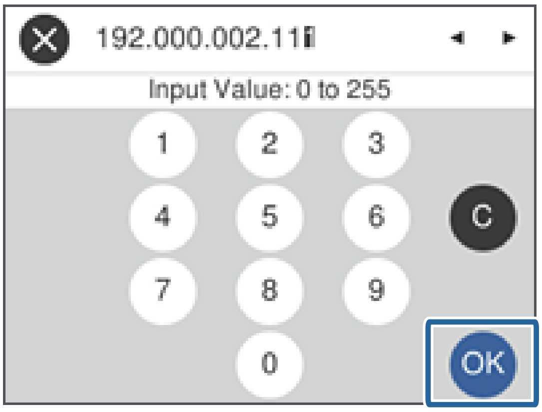


5. בחר ידני עבור קבל כתובת IP.



לתשומת לבך:
כאשר אתה מגדיר את כתובת ה-IP באופן אוטומטי באמצעות פונקציית ה-DHCP של הנתב, בחר אוטומטי. במקרה זה, ה-כתובת IP, מסכת רשת משנה, וה-שער ברירת מחדל בשלבים 6 עד 7 מוגדרים אף הם באופן אוטומטי, לכן, עבור אל שלב 8.

6. הקש על השדה **כתובת IP**, הזן את כתובת ה-IP באמצעות המקלדת המוצגת על גבי המסך, ואז הקש אישור.



אשר את הערך המוצג במסך הקודם.

7. הגדר את **מסכת רשת משנה** ואת **שערברירת מחדל**.

   אשר את הערך המוצג במסך הקודם.

   לתשומת לבך:
   *אם השילוב של כתובת IP, מסכת רשת משנה ושל שער ברירת מחדל אינו נכון, **התחל הגדרה** אינו פעיל ולא ניתן להמשיך בביצוע ההגדרות. ודא שאין שגיאה בהזנה.*

8. הקש על השדה DNS **ראשי** עבור ה-**שרת DNS**, הזן את כתובת ה-IP של שרת ה-DNS הראשי באמצעות המקלדת המוצגת על גבי המסך, ואז הקש **אישור**.

   אשר את הערך המוצג במסך הקודם.

   לתשומת לבך:
   *כאשר אתה בוחר **אוטומטי** עבור הגדרות הקצאת כתובת ה-IP, ביכולתך לבחור את הגדרות שרת ה-DNS מתוך **ידני** או **אוטומטי**. אם אין ביכולתך להשיג את כתובת שרת ה-DNS באופן אוטומטי, בחר **ידני** והזן את כתובת שרת ה-DNS. לאחר מכן הזמן ישירות את כתובת שרת ה-DNS המשני. אם בחרת **אוטומטי**, עבור אל שלב 10.*

9. הקש על השדה DNS **משני**, הזן את כתובת ה-IP עבור שרת ה-DNS המשני באמצעות המקלדת המוצגת על גבי המסך, ואז הקש על **אישור**.

   אשר את הערך המוצג במסך הקודם.

10. הקש **התחל הגדרה**.

11. הקש **סגירה** במסך האישור.

    המסך נסגר אוטומטית אחרי פרק זמן מסוים אם לא הקשת **סגירה**.

התחברות ל-Ethernet

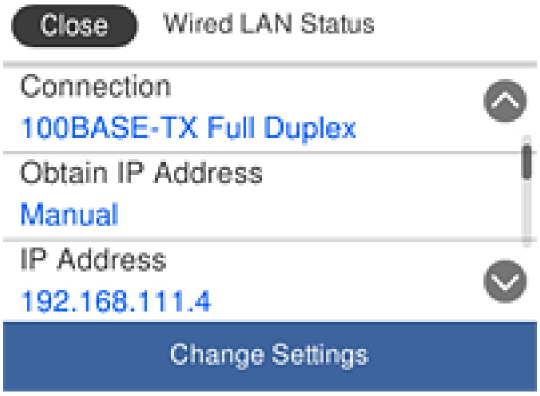
חבר את הסורק לרשת באמצעות כבל Ethernet ובדוק את החיבור.

1. חבר את הסורק ואת הרכזת (מתג L2) באמצעות כבל Ethernet.

   הסמל במסך הבית משתנה ל- .

2. הקש במסך הבית.

3. הסט את המסך כלפי מעלה, ואז ודא שמצב החיבור וכתובת ה-IP נכונים.



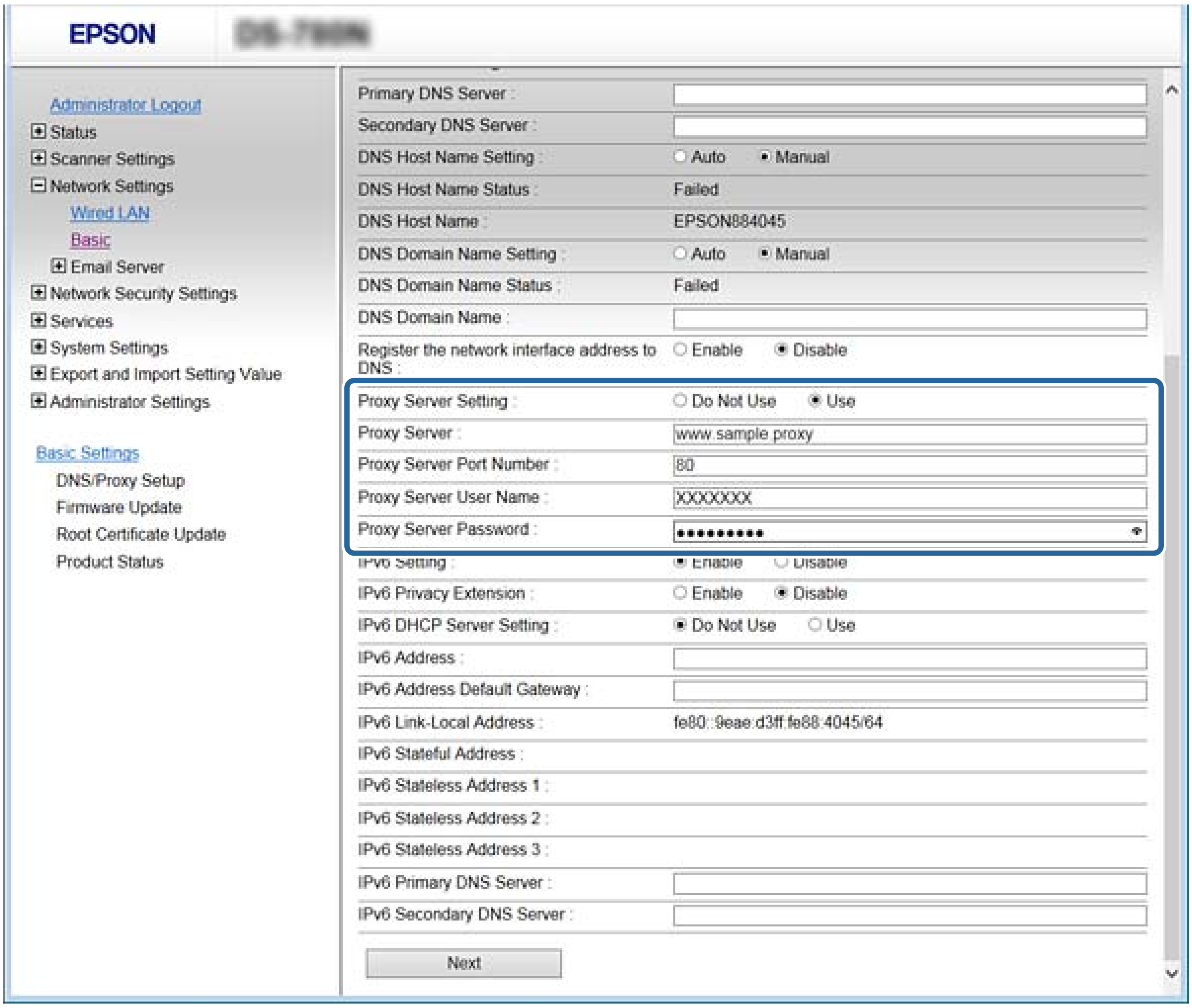
הגדרת שרת הפרוקסי

לא ניתן להגדיר את שרת הפרוקסי בלוח. הגדר באמצעות Web Config.

1. גש אל Web Config ובחר **Network Settings** < **Basic**.
2. בחר **Use** ב-**Proxy Server Setting**.
3. ציין את שרת הפרוקסי בכתובת IPv4 או בפורמט FQDN ב-**שרת פרוקסי**, ואז הזן את מספר היציאה ב-**Proxy Server Port Number**.

   עבור שרתי פרוקסי המחייבים אימות, הזן את שם משתמש אימות שרת הפרוקסי וסיסמת אימות שרת הפרוקסי.

4. לחץ על לחצן **Next**.



5. אשר את ההגדרות ואז לחץ הגדרות.

מידע קשור

← "גישה אל Web Config" בעמוד 23

חיבור לרשת באמצעות תוכנת ההתקנה

אנו ממליצים להשתמש בתוכנת ההתקנה כדי לחבר את הסורק למחשב. תוכל להפעיל את תוכנת ההתקנה באמצעות אחת השיטות הבאות.

❏ הגדרה מתוך אתר האינטרנט

גש לאתר האינטרנט שלהלן, ואז הזן את שם המוצר. גש אל **התקנה**, והתחל בביצוע ההתקנה.

http://epson.sn

❏ התקנה באמצעות דיסק התוכנה (רק עבור דגמים המגיעים עם דיסק תוכנה ומשתמשים שיש להם כונני דיסקים).

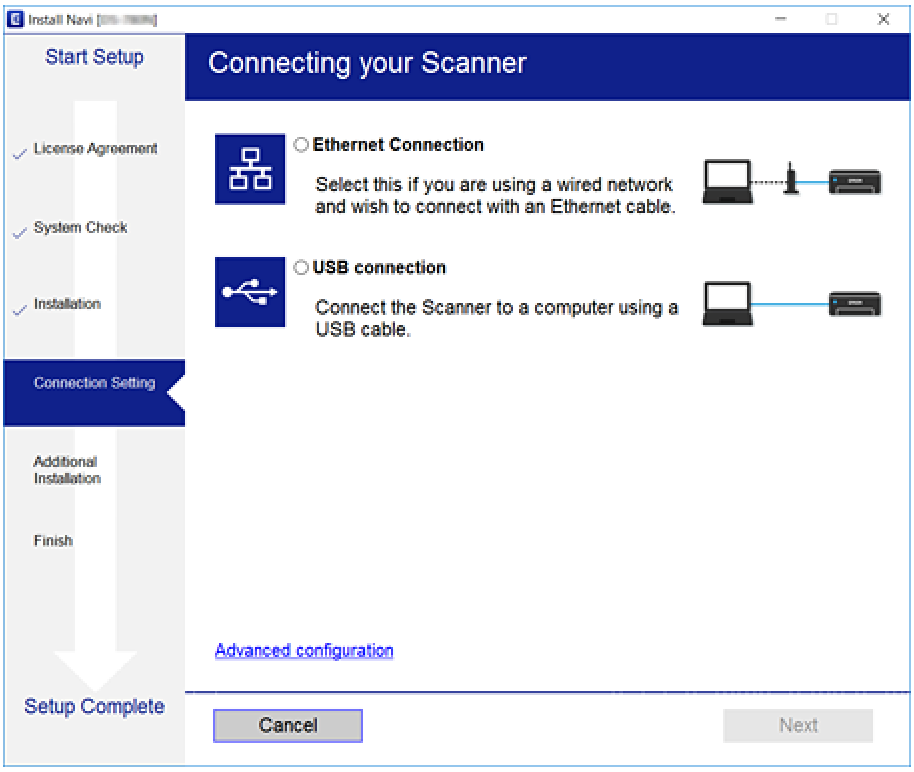
הכנס למחשב את דיסק התוכנה, ולאחר פעל על פי ההנחיות שבמסך.

בחירת שיטות החיבור

פעל בהתאם להוראות המוצגות על גבי המסך עד שיוצג המסך הבא, ואז בחר את שיטת החיבור בין הסורק לבין המחשב.

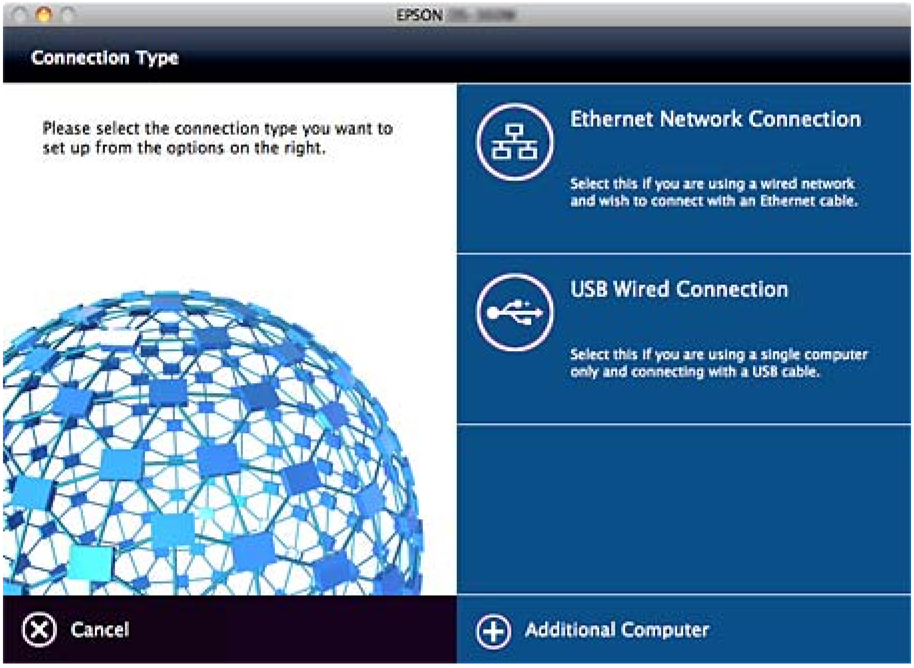
❏ Windows

בחר את סוג החיבור ואז לחץ על **הבא**.



❏ Mac OS

בחר את סוג החיבור.



חיבור

פעל על פי ההוראות המוצגות. התוכנה הדרושה מותקנת.

הגדרות פונקציות

פרק זה מסביר את ההגדרות הראשונות שיש לבצע על מנת להשתמש בכל פונקציה של ההתקן.

תוכנה עבור הגדרות

בנושא זה מוסבר הנוהל לביצוע הגדרות ממחשב המנהל באמצעות Web Config.

Web Config (דף אינטרנט עבור התקן)

אודות Web Config

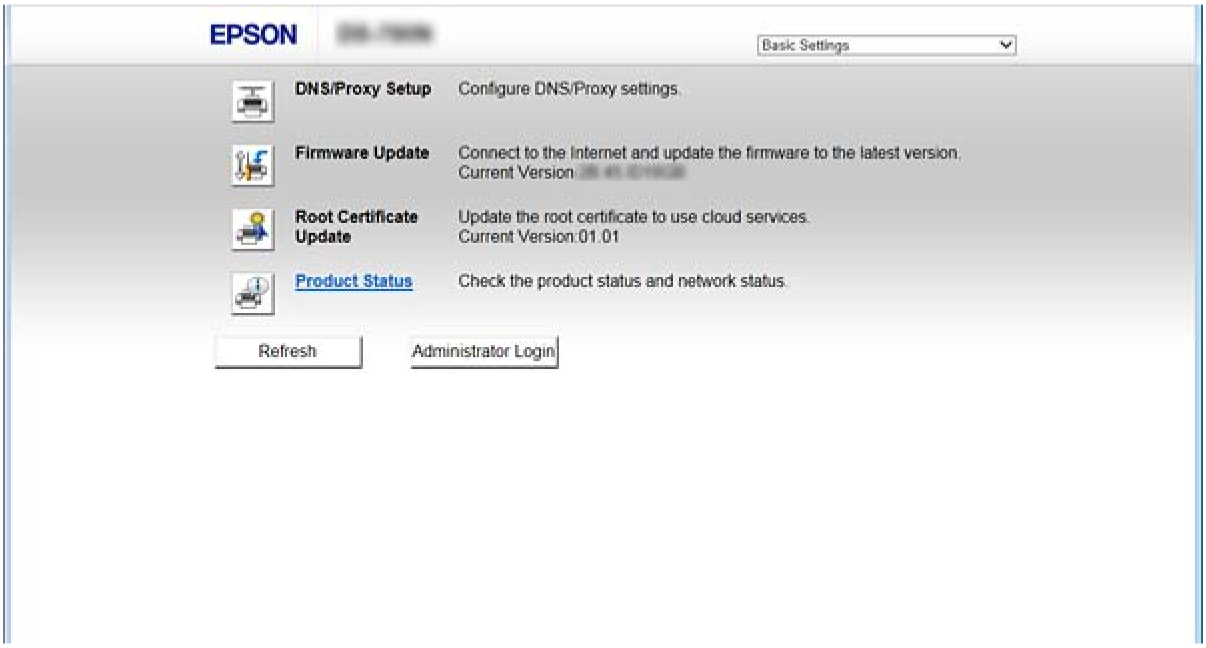
Web Config הוא יישום מבוסס דפדפן לשינוי תצורת הגדרות הסורק.

כדי לגשת אל Web Config, תחילה עליך להקצות כתובת IP לסורק.

לתשומת לבך:
תוכל לנעול את ההגדרות בכך שתגדיר סיסמת מנהל מערכת לסורק.

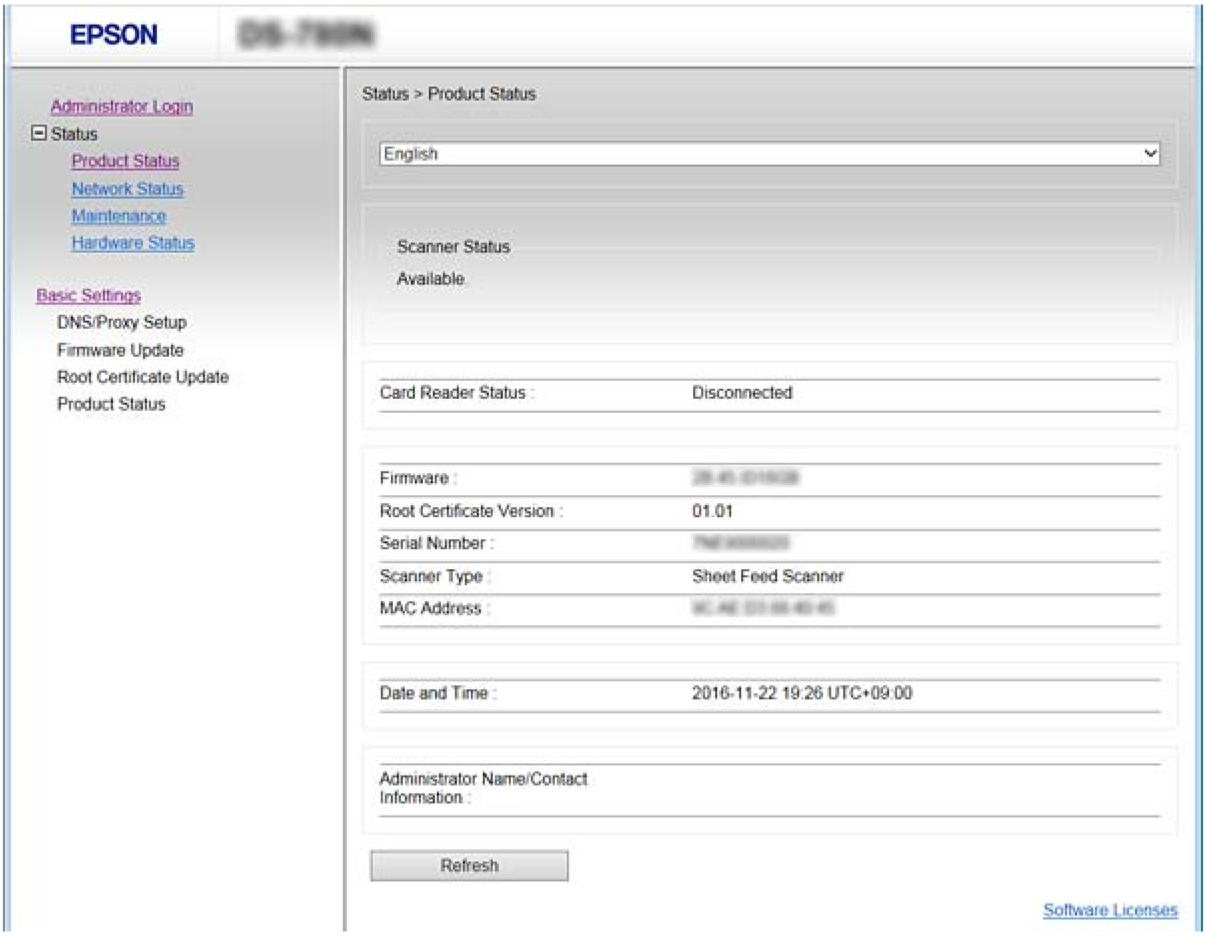
ישנם שני עמודי הגדרות.

❏ Basic Settings
תוכל לשנות את תצורת ההגדרות הבסיסיות של הסורק.



❏ Advanced Settings

תוכל לשנות את תצורת ההגדרות המתקדמות של הסורק. עמוד זה הוא בעיקר עבור מנהל מערכת.



גישה אל Web Config

הזן את כתובת ה-IP של הסורק בדפדפן אינטרנט. יש לאפשר JavaScript. בעת גישה אל Web Config דרך HTTPS, הודעת אזהרה תופיע בדפדפן כיוון שנעשה שימוש באישור בחתימה עצמית המאוחסן בסורק.

❏ גישה דרך HTTPS

IPv4: https://<כתובת ה-IP של הסורק> (ללא < >)

IPv6: https://[כתובת ה-IP של הסורק] (כולל [ ])

❏ גישה דרך HTTP

IPv4: http://<כתובת ה-IP של הסורק> (ללא < >)

IPv6: http://[כתובת ה-IP של הסורק] (כולל [ ])

לתשומת לבך:
- *דוגמאות*
  :IPv4
  /192.0.2.111//:https
  /192.0.2.111//:http
  :IPv6
  /[1000:1::db8:2001]//:https
  /[1000:1::db8:2001]//:http
- *אם שם הסורק רשום בשרת ה-DNS, תוכל להשתמש בשם הסורק במקום בכתובת ה-IP של הסורק.*

מידע קשור

➡ "תקשורת SSL/TLS עם הסורק" בעמוד 63
➡ "אודות אישורים דיגיטליים" בעמוד 63

השימוש בפונקציות סריקה

בהתאם לאופן שבו אתה משתמש בסורק, התקן את התוכנה הבאה והגדר את הגדרות השימוש בה.

- סרוק מהמחשב
  - אשר את החוקיות של שירות סריקת הרשת עם Web Config (חוקי בעת המשלוח מהמפעל).
  - התקן את Epson Scan 2 במחשב שלך והגדר את כתובת ה-IP
  - כאשר אתה סורק באמצעות עבודות, התקן Document Capture Pro (Document CaptureDocument Capture Pro) והגדר הגדרות עבודה.
- סרוק מלוח ההפעלה
  - כאשר אתה משתמש ב-Document Capture Pro או Document Capture Pro Server:
    התקן את Document Capture Pro או Document Capture Pro Server
    הגדרות DCP (מצב שרת, מצב לקוח).
  - כאשר אתה משתמש בפרוטוקול WSD:
    אשר את חוקיות ה- WSD ב-Web Config או בלוח ההפעלה (חוקי בעת המשלוח מהמפעל)
    הגדרות התקן נוספות (מחשב Windows).

סריקה ממחשב

התקן את התוכנה ובדוק ששירות סריקת הרשת אופשר לסריקה מהמחשב באמצעות רשת.

מידע קשור

➡ "תוכנה שיש להתקין" בעמוד 25
➡ "אפשר סריקת רשת" בעמוד 25

תוכנה שיש להתקין

- ❏ Epson Scan 2

זהו מנהל התקן סורק. אם אתה משתמש בהתקן ממחשב, התקן את מנהל ההתקן בכל מחשב לקוח. אם הותקן Document CaptureDocument Capture Pro/ תוכל לבצע את הפעולות שהוקצו ללחצני ההתקן.

עם EpsonNet SetupManager, אפשר שמנהלי התקן מדפסת יופצו יחד בחבילות.

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

התקן במחשב הלקוח. תוכל להזמין ולבצע עבודות הרשומות במחשב כאשר Document Capture Pro/ Document Capture מותקן ברשת ממחשב ולוח הבקרה של הסורק.

תוכל גם לסרוק ממחשב באמצעות הרשת. Epson Scan 2 דרושה לשם ביצוע סריקה.

מידע קשור

➡ "EpsonNet SetupManager" בעמוד 56

הגדר את כתובת ה-IP של הסורק כ-Epson Scan 2

הגדר את כתובת ה-IP של הסורק כך שניתן יהיה להשתמש בסורק ברשת.

1. הפעל את תוכנת העזר **Epson Scan 2 Utility** מתוך התחל > **כל התוכניות** > **EPSON** > **Epson Scan 2**.

   אם קיים סורק אחר שכבר רשום, עבור לשלב 2.

   אם אינו רשום, עבור לשלב 4.

2. לחץ ▼ ב- סורק.

3. לחץ על הגדרות.

4. לחץ **אפשר ביצוע עריכה**, ואז לחץ הוסף.

5. בחר את שם דגם הסורק מתוך **דגם**.

6. בחר את כתובת ה-IP של הסורק המיועד לשימוש מתוך **כתובת** ב-**חפש רשת**.

   לחץ ואז לחץ על כדי לעדכן את הרשימה. אם אין ביכולתך למצוא את כתובת ה-IP של הסורק, בחר הזן **כתובת** והזן את כתובת ה-IP.

7. לחץ על הוסף.

8. לחץ על אישור.

אפשר סריקת רשת

תוכל להגדיר את שירות סריקת הרשת כאשר אתה סורק ממחשב לקוח דרך הרשת. הגדרת ברירת המחדל היא מאופשרת.

1. גש אל Web Config ובחר **Services** > **Network Scan**.
2. ודא שנבחר **Enable scanning** של **EPSON Scan**.
   אם הוא נבחר, המשימה הושלמה. סגור את Web Config.
   אם הוא לא נבחר, בחר אותו ועבור לשלב הבא.
3. לחץ על **Next**.
4. לחץ על **OK**.
   הרשת מתחברת מחדש ואז מאופשרות ההגדרות.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

סריקה באמצעות לוח הבקרה

פונקציית 'סרוק לתיקיה' ופונקציית 'סרוק למייל' תוך שימוש בלוח הבקרה של הסורק, ואף העברת תוצאות סריקה למייל, לתיקיות וכו', מתבצעות באמצעות ביצוע עבודה מהמחשב.

בעת העברת תוצאות סריקה, הגדר את העבודה עם Document Capture Pro Server או Document Capture Pro.

לפרטים על ההגדרות, ועל הגדרת העבודה, עיין בתיעוד או בעזרה עבור Document Capture Pro Server או Document Capture Pro.

מידע קשור

➡ "הגדרות Document Capture Pro Server/Document Capture Pro" בעמוד 26
➡ "הגדרות של שרתים ותיקיות" בעמוד 27

תוכנה להתקנה במחשב

❏ **Document Capture Pro Server**
זוהי גירסת השרת של Document Capture Pro. התקן אותה בשרת Windows. השרת מסוגל לנהל באופן מרכזי התקנים רבים ועבודות רבות. ניתן לבצע עבודות בו-זמנית ממספר סורקים.
באמצעות השימוש בגירסה המאושרת של Document Capture Pro Server, תוכל לנהל עבודות והיסטוריה של סריקות הקשורים למשתמשים וקבוצות.
לפרטים על Document Capture Pro Server, צור קשר עם משרד Epson המקומי שלך.

❏ **Document Capture Pro** (Windows)/Document Capture (Mac OS)
בדיוק כמה סריקה מהמחשב, תוכל לקרוא מלוח הבקרה לעבודות הרשומות במחשב ולבצע אותן. לא ניתן להפעיל עבודות מחשב בו-זמנית ממספר סורקים.

הגדרות Document Capture Pro Server/Document Capture Pro

הגדר הגדרות לשימוש בפונקציית הסריקה מלוח הבקרה של הסורק.

1. גש אל Web Config ובחר **Services** > **Document Capture Pro**.

2. בחר מצב פעולה.

❏ Server Mode:

בחר אפשרות זו כאשר אתה משתמש ב-Document Capture Pro Server או כאשר אתה משתמש ב-Document Capture Pro רק עבור עבודות שהוגדרו עבור מחשב ספציפי.

❏ Client Mode:

הגדר זאת כאשר אתה בוחר את הגדרות העבודה של Document Capture Pro (DocumentDocument Capture) המותקנים בכל מחשב לקוח ברשת בלא לציין את המחשב.

3. הגדר את ההגדרות הבאות בהתאם למצב שנבחר.

❏ Server Mode:

ב-**Server Address**, ציין את השרת שבו מותקןDocument Capture Pro Server. ניתן להזין בין 2 לבין 252 תווים בפורמט IPv4, IPv6, שם מארח או פורמט FQDN. ניתן להשתמש בפורמט FQDN, אותיות US-ASCII, מספרים, אלפביתיים ומקפים (פרט למקף מוביל ומקף עוקב).

❏ Client Mode:

ציין **Group Settings** כדי להשתמש בקבוצת סורקים שצויינה מתוך Document Capture Pro (Document Capture)).

4. לחץ על הגדרות.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

הגדרות של שרתים ותיקיות

Document Capture Pro ו-Document Capture Pro Server שומרים את הנתונים הסרוקים לשרת או למחשב לקוח ומשתמשים בפונקציית ההעברה כדי לבצע את פונקציית 'סרוק לתיקייה' ואת פונקציית 'סרוק למייל'.

אתה זקוק להרשאה ולמידע כדי להעביר ממחשב שבו Document Capture Pro, Document Capture Pro Server הותקנו למחשב או לשירות ענן.

הכן את המידע על הפונקציה שבה תשתמש, תוך התייחסות לנקודות הבאות.

תוכל להגדיר הגדרות עבור פונקציות אלו באמצעות Document Capture Pro או Document Capture Pro Server. לפרטים על ההגדרות, עיין בתיעוד או בעזרה עבור Document Capture Pro Server או Document Capture Pro.

שם	הגדרות	דרישות
תיקיית סרוק לרשת (SMB)	צור והגדר את השיתוף של תיקיית השמירה	חשבון המשתמש המנהל של המחשב שיוצר תיקיות שמירה.
	היעד עבור תיקיית סרוק לרשת (SMB)	שם משתמש וסיסמה כדי להיכנס למחשב שבו נמצאת תיקיית השמירה, וההרשאה לעדכן את תיקיית השמירה.

שם	הגדרות	דרישות
תיקיית סרוק לרשת (FTP)	הגדרה עבור כניסה לשרת ה-FTP	מידע כניסה עבור שרת ה-FTP וההרשאות לעדכן את תיקיית השמירה.
סריקה לדוא"ל	הגדרה עבור שרת הדוא"ל	מידע הגדרה עבור שרת הדוא"ל
סרוק למסמך באמצעות Capture Pro (כאשר משתמשים ב- Document Capture Pro Server)	הגדרה עבור כניסה לשירות ענן	סביבת חיבור האינטרנט רישום החשבון עבור שירותי ענן

יש להשתמש בסריקת WSD (במערכת הפעלה Windows בלבד)

אם המחשב משתמש במערכת הפעלה Windows Vista או מאוחרת ממנה, תוכל להשתמש בסריקת WSD.

כאשר ניתן להשתמש בפרוטוקול WSD, תפריט **מחשב (WSD)** יוצג בלוח הבקרה של הסורק.

1. גש אל Web Config ובחר **Services** > **Protocol**.
2. ודא ש- **Enable WSD** סומן ב-**WSD Settings**.
   אם הוא מסומן, השלמת את המשימה ואתה רשאי לסגור את Web Config.
   אם הוא אינו מסומן, סמן אותו והמשך לשלב הבא.
3. לחץ על לחצן **Next**.
4. אשר את ההגדרות ולחץ **הגדרות**.

ביצוע הגדרות מערכת

ביצוע הגדרות מערכת בלוח הבקרה

הגדרת את בהירות המסך

הגדרת את בהירות מסך הגביש הנוזלי.

1. הקש **הגדרות** במסך הבית.
2. הקש **הגדרות משותפות** > **בהירות מסך**.
3. הקש ⊕ או ⊖ כדי לשנות את הבהירות.
   תוכל לשנות מ1- עד 9.
4. הקש **אישור**.

הגדר צליל

הגדר צליל פעולת לוח וצליל שגיאה.

1. הקש הגדרות במסך הבית.
2. הקש **הגדרות משותפות** > **צליל**.
3. הגדר את הפריטים הבאים לפי הצורך.
   - ❏ צליל פעולה
     הגדרת את עוצמת הקול של צליל הפעולה של לוח הבקרה.
   - ❏ צליל שגיאה
     הגדרת את עוצמת הקול של צליל שגיאה.
4. הקש **אישור**.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

גלה הזנה כפולה של מסמך מקור

הגדר את הפונקציה לגילוי הזנה כפולה של המסמך המיועד לסריקה ולעצירת הסריקה כאשר מתרחשת הזנה של יותר ממסמך אחד.

כדי לסרוק מסמכי מקור שקיימת לגביהם אפשרות של הזנת יותר מאחד, כגון מעטפות, או נייר עם מדבקות, הגדר פונקציה זו למצב כבוי.

לתשומת לבך:
ניתן להגדיר אותה גם מתוך Web Config או Epson Scan 2.

1. הקש הגדרות במסך הבית.
2. הקש **הגדרות סריקה חיצוניות** > **זיהוי על-קולי להזנה כפולה**.
3. הקש **זיהוי על-קולי להזנה כפולה** כדי להפעיל או לכבות.
4. הקש סגירה.

הגדר מצב מהירות נמוכה

הגדר את הסריקה במהירות נמוכה כדי למנוע חסימות נייר בעת סריקת מסמכים דקים כמו תלושי משכורת.

1. הקש הגדרות במסך הבית.
2. הקש **הגדרות סריקה חיצוניות** > **לאט**.
3. הקש **לאט** כדי להפעיל או לכבות.
4. הקש **סגירה**.

ביצוע הגדרות מערכת באמצעות Web Config

הגדרות חסכון בחשבון בזמן חוסר פעילות

בצע את הגדרת החסכון בחשבון עבור תקופות העדר הפעילות של הסורק. הגדר את השעה בהתאם לסביבות השימוש שלך.

לתשומת לבך:
ביכולתך גם להגדיר את הגדרות החסכון בחשמל בלוח הבקרה של הסורק.

1. גש אל Web Config ובחר **System Settings** < **Power Saving**.
2. הזן את השעה שבה ה-**Sleep Timer** יעבור למצב חסכון בחשמל בעת תקופות של העדר פעילות.

   תוכל להגדיר עד 240 דקות במרווחים של דקה.
3. בחר את זמן הכיבוי עבור ה-**Power Off Timer**.
4. לחץ על **OK**.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

הגדרת לוח הבקרה

הגדרה עבור לוח הבקרה של הסורק. תוכל לבצע את ההגדרות הבאות.

1. גש אל Web Config ובחר **System Settings** < **Control Panel**.
2. הגדר את הפריטים הבאים בהתאם לצורך.

   ❏ Language

   בחר את השפה המוצגת בלוח הבקרה.

   ❏ Panel Lock

   אם תבחר ON, יהיה עליך להזין את סיסמת המנהל כאשר תבצע פעולה המחייבת את סמכות המנהל. אם סיסמת המנהל לא הוגדרה, נעילת הלוח מושבתת.

   ❏ Operation Timeout

   אם תבחר ON, כאשר תיכנס למערכת כמנהל, תוצא באופן אוטומטי מהמערכת ותועבר למסך ההתחלה אם לא תהיה פעילות במשך פרק זמן מסוים.

   תוכל להגדיר בין 10 שניות עד 240 דקות במרווחים של שנייה.
3. לחץ על **OK**.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

הגדרת ההגבלה עבור הממשק החיצוני

תוכל להגביל את חיבור ה-USB מהמחשב. הגדר אותו כך שיגביל סריקה שאינה באמצעות הרשת.

1. גש אל Web Config ובחר **System Settings** < **External Interface**.
2. בחר **Enable** או **Disable**.
   כדי להגביל, בחר **Disable**.
3. הקש **OK**.

סנכרון התאריך והשעה עם שרת השעה

אם אתה משתמש באישור CA, תוכל למנוע בעיות עם השעה.

1. גש אל Web Config ובחר **System Settings** < **Date and Time** < **Time Server**.
2. בחר **Use** עבור **Use Time Server**.
3. הזן את כתובת שרת השעה עבור **Time Server Address**.
   תוכל להשתמש בפורמט IPv4, IPv6 או FQDN. הזן 252 תווים או פחות. אם לא תציין זאת, השאר את המקום ריק.
4. הזן **Update Interval (min)**.
   תוכל להגדיר עד 10,800 דקות במרווחים של דקה.
5. לחץ על **OK**.
   לתשומת לבך:
   תוכל לאשר את סטטוס החיבור עם שרת השעה ב-Time Server Status.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

הגדרות אבטחה בסיסיות

פרק זה מסביר את הגדרות האבטחה הבסיסיות שאינן מחייבות סביבה מיוחדת.

מבוא למאפייני אבטחה בסיסיים

אנו מציגים את מאפייני האבטחה הבסיסיים של התקני Epson.

שם מאפיין	סוג מאפיין	מה להגדיר	מה למנוע
הגדרה עבור סיסמת מנהל	נעל את ההגדרות הקשורות למערכת, כגון הגדרות חיבור רשת וחיבור USB, כך שרק המנהל יוכל לשנותן.	מנהל מגדיר סיסמה עבור התקן. תצורה או עדכון זמינים בכל מקום מתוך Web Config, לוח הבקרה, Epson Device Admin, ו-EpsonNet Config.	מנע קריאה ושינוי בלתי חוקיים של המידע המאוחסן בהתקן כגון זהות, סיסמה, הגדרות רשת ואנשי קשר. בנוסף לכך, מזער טווח רחב של סיכוני אבטחה כגון דליפת מידע עבור סביבת הרשת או מדיניות האבטחה.
תקשורת SSL/TLS	כאשר ניגשים לשרת Epson באינטרנט מתוך התקן, כגון תקשורת עם מחשב באמצעות דפדפן עו עדכון קושחה, תוכן התקשורת מוצפן באמצעות תקשורת SSL/TLS.	השג אישור החתום על ידי רשות אישורים, ואז ייבא אותו לתוך הסורק.	איפוס זיהוי של התקן באמצעות אישור החתום על ידי רשות אישורים מונע התחזות וגישה בלתי מורשית. בנוסף לכך, תכני התקשורת של SSL/TLS מוגנים, והדבר מונע דליפה של תכנים עבור נתוני הדפסה ומידע הגדרה.
פרוטוקולי בקרות	פרוטוקולי בקרות משמשים לתקשורת בין התקנים למחשבים, ומאפשרים/משביתים פונקציות.	פרוטוקול של שירות המיושם על מאפיינים שהותרו או נאסרו בנפרד.	מפחית את סיכוני האבטחה שעלולים להתרחש כתוצאה משימוש לא מכוון בכך שמונע מהמשתמשים להשתמש בפונקציות מיותרות.

מידע קשור

➡ "אודות Web Config" בעמוד 22
➡ "EpsonNet Config" בעמוד 55
➡ "Epson Device Admin" בעמוד 55
➡ "הגדרת סיסמת מנהל מערכת" בעמוד 32
➡ "בקרת פרוטוקולים" בעמוד 35

הגדרת סיסמת מנהל מערכת

כאשר אתה מגדיר את סיסמת המנהל, משתמשים אחרים מאשר המנהלים לא יהיו מסוגלים לשנות את ההגדרות עבור ניהול המערכת. תוכל להגדיר ולשנות את סיסמת המנהל באמצעות Web Config, לוח הבקרה של הסורק או

תוכנה (Epson Device Admin או EpsonNet Config). כאשר אתה משתמש בתוכנה, עיין בתיעוד עבור כל תוכנה.

מידע קשור

➡ "הגדרת התצורה של סיסמת המנהל מתוך לוח הבקרה" בעמוד 33
➡ "הגדרת תצורת סיסמת המנהל באמצעות Web Config" בעמוד 33
➡ "EpsonNet Config" בעמוד 55
➡ "Epson Device Admin" בעמוד 55

הגדרת התצורה של סיסמת המנהל מתוך לוח הבקרה

תוכל להגדיר את סיסמת המנהל מלוח הבקרה של הסורק.

1. הקש הגדרות במסך הבית.
2. הקש **ניהול מערכת** > **הגדרות מנהל מערכת**.
   אם הפריט אינו מוצג, החלק את המסך כלפי מעלה כדי להציג את הפריט.
3. הקש **סיסמת מנהל** > **שמור**.
4. בדוק את הסיסמה החדשה, ואז הקש **אישור**.
5. הזן שוב את הסיסמה החדשה, ואז הקש **אישור**.
6. הקש **אישור** במסך האישור.
   מוצג מסך הגדרות המנהל.
7. הקש **הגדרת נעילה**, ואז הקש **אישור** במסך האישור.
   הגדרת נעילה הוגדר למצב **On**, וסיסמת המנהל תידרש כאשר תפעיל את פריט התפריט הנעול.

לתשומת לבך:

❏ *אם תגדיר **הגדרות** > **הגדרות משותפות** > **זמן קצוב לפעולה** למצב **On**, הסורק יוציא אותך מהמערכת אחרי תקופה של חוסר פעילות בלוח הבקרה.*

❏ *תוכל לשנות או למחוק את סיסמת המנהל כאשר תבחר **שנה** או **איפוס** במסך **סיסמת מנהל** והזן את סיסמת המנהל.*

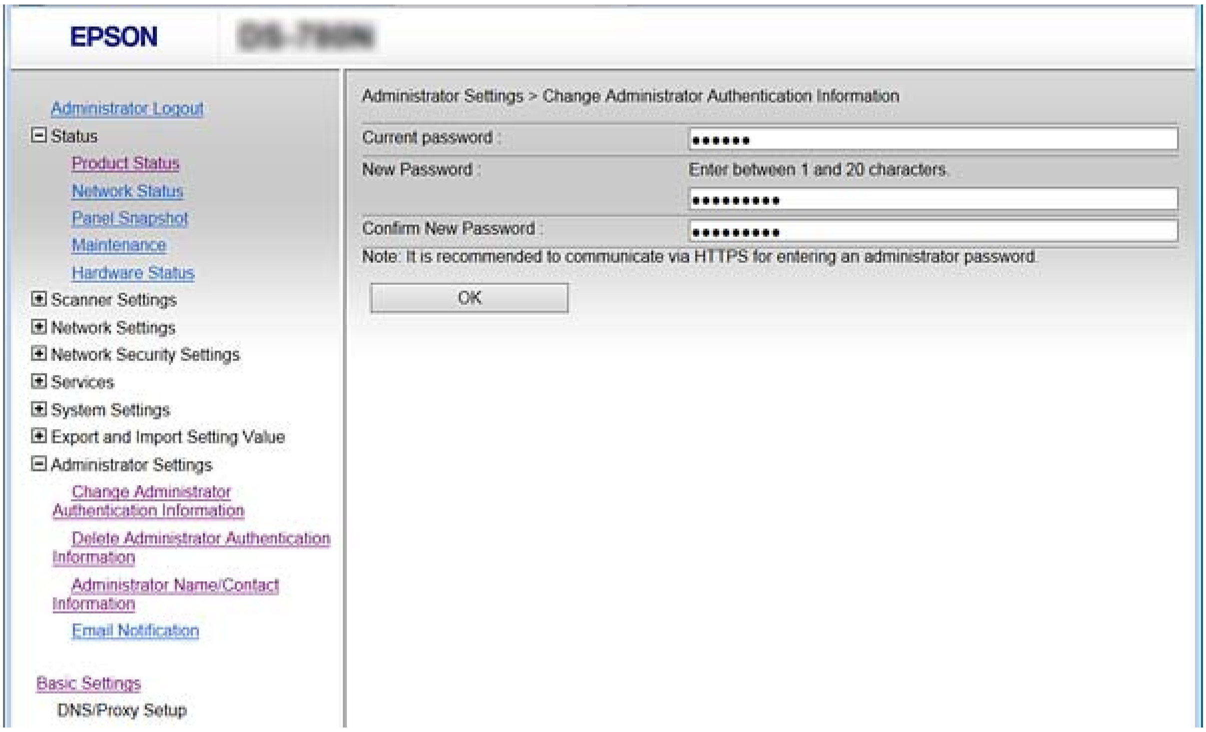
הגדרת תצורת סיסמת המנהל באמצעות Web Config

תוכל להגדיר את סיסמת המנהל באמצעות Web Config.

1. גש אל Web Config ובחר **Administrator Settings** > **Change Administrator Authentication Information**.

2. הזן סיסמה בשדה **New Password** ו-**Confirm New Password**. במידת הצורך, הזן את שם המשתמש.

אם תרצה לשנות את הסיסמה לסיסמה חדשה, הזן את הסיסמה הנוכחית.



3. בחר **OK**.

לתשומת לבך:

- ❑ *כדי להגדיר או לשנות את פריטי התפריט הנעולים, לחץ **Administrator Login**, ואז הזן את סיסמת המנהל.*
- ❑ *על מנת למחוק את סיסמת המנהל, לחץ **Administrator Settings** > **Delete Administrator Authentication Information**, ואז הזן את סיסמת המנהל.*

מידע קשור

➔ "גישה אל Web Config" בעמוד 23

פריטים המיועדים לנעילה באמצעות סיסמת המנהל

למנהלים יש זכויות הגדרה ושינוי לעבור כל המאפיינים בהתקנים.

כמו כן, אם תגדיר בהתקן סיסמת מנהל, תוכל לנעול אותו כך שלא תוכל לשנות פריטים הקשורים לניהול ההתקן.

להלן הפריטים בהם יכול המנהל לשלוט.

פריט	תיאור
הגדרת סורק	הגדרת זיהוי הזנה כפולה ומצב מהירות נמוכה.

פריט	תיאור
הגדרות חיבור Ethernet	שינוי שם ההתקנים וכתובת ה-IP, הגדרת שרת ה-DNS או שרת הפרוקסי, והגדרת שינויים הקשורים לחיבורי רשת.
הגדרת שירותי משתמש	הגדרה עבור שליטה בפרוטוקולי תקשורת, סריקת רשת, ושירותי Document Capture Pro.
הגדרות שרת דוא"ל	הגדרת שרת דוא"ל עימו יוצרים התקנים תקשורת ישירה.
הגדרת אבטחה	הגדרות עבור אבטחת רשת, כגון תקשורת SSL/TLS, סינון IPsec/IP ו-IEEE802.1X.
עדכון תעודת שורש	עדכון תעודות שורש הדרושות עבור אימות Document Capture Pro Server ועדכון קושחה מתוך Web Config.
עדכון קושחה	בדוק ועדכן את קושחת ההתקנים.
שעה, הגדרת טיימר	משך הזמן עד למעבר לשינה, כיבוי אוטומטי, תאריך/שעה, טיימר אי-פעולה, הגדרות אחרות הקשורות לטיימר.
שחזור את כל הגדרות ברירת המחדל	הגדרה לאיפוס הסורק להגדרות המפעל.
הגדרת מנהל	הגדרת נעילת מנהל או סיסמת מנהל.
הגדרת התקן מאושר	הגדרת הזהות של התקן האימות. הגדר בעת שימוש בסורק במערכת אימות התומכת בהתקני אימות.

בקרת פרוטוקולים

תוכל לסרוק באמצעות מגוון נתיבים ופרוטוקולים. תוכל להשתמש בסריקת רשת גם ממספר בלתי-ספציפי של מחשבי רשת. כך למשל, מותרת רק סריקה המשתמשת בנתיבים ופרוטוקולים שצוינו מראש. תוכל לצמצם את סיכוני האבטחה שאינם מכוונים באמצעות הגבלת הסריקה מנתיבים מסוימים או באמצעות בקרה על הפונקציות הזמינות.

קבע את תצורת הגדרות הפרוטוקולים.

1. גש אל Web Config ובחר **Services** > **Protocol**.
2. הגדר כל פריט.
3. לחץ על **Next**.
4. לחץ על **OK**.

   ההגדרות יחולו על הסורק.

מידע קשור

➔ "גישה אל Web Config" בעמוד 23
➔ "פרוטוקולים שניתן לאפשר או להשבית" בעמוד 36
➔ "פריטי הגדרת פרוטוקולים" בעמוד 37

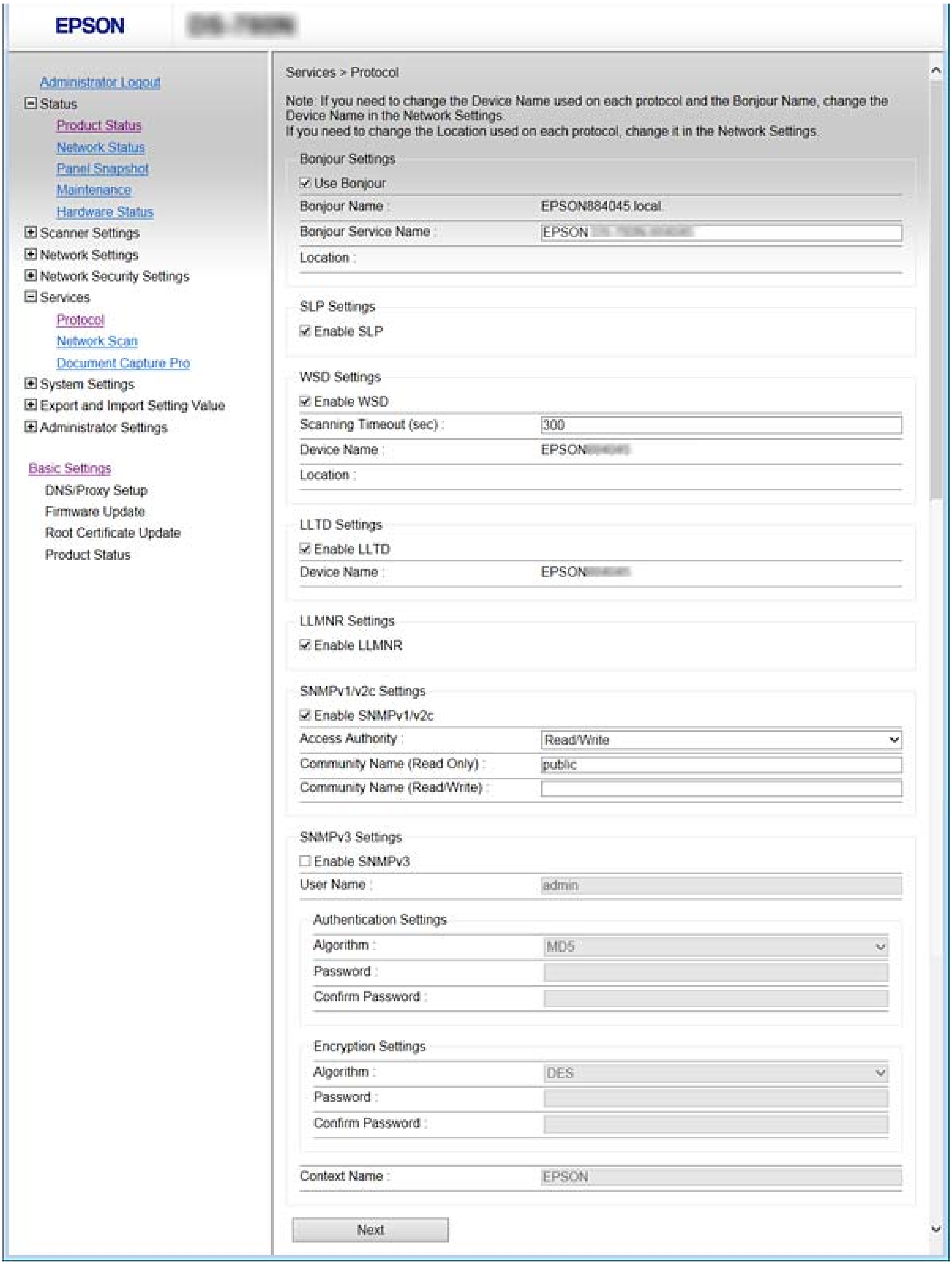
פרוטוקולים שניתן לאפשר או להשבית

פרוטוקול	תיאור
Bonjour Settings	תוכל לציין אם להשתמש ב-BonjourBonjour .. משמש לחיפוש אחר התקנים, לסריקה וכדומה.
SLP Settings	תוכל להפעיל ולהשבית את הפונקציה SLPSLP . משמש עבור Epson Scan 2 וחיפוש רשת ב-.EpsonNet Config
WSD Settings	תוכל לאפשר או להשבית את הפונקציה WSD. כאשר הפונקציה מאופשרת, תוכל להוסיף התקני WSD או לסרוק דרך יציאת WSD.
LLTD Settings	תוכל להפעיל ולהשבית את הפונקציה LLTD. כאשר הפונקציה מאופשרת, היא מוצגת על מפת הרשת של Windows.
LLMNR Settings	תוכל להפעיל ולהשבית את הפונקציה LLMNR. כאשר הפונקציה מאופשרת, תוכל להשתמש בזיהוי שמות ללא NetBIOS גם אם אינך יכול להשתמש ב-DNS.
SNMPv1/v2c Settings	תוכל לציין אם לאפשר את SNMPv1/v2c או לא. משמש להגדרת התקנים, לניטור וכדומה.
SNMPv3 Settings	תוכל לציין אם לאפשר את SNMPv3 או לא. אפשרות זו משמשת להגדרת התקנים מוצפנים, לניטור וכדומה.

מידע קשור

➡ "בקרת פרוטוקולים" בעמוד 35
➡ "פריטי הגדרת פרוטוקולים" בעמוד 37

פריטי הגדרת פרוטוקולים



פריטים	ערך ההגדרה ותיאורה
Bonjour Settings	

הגדרות אבטחה בסיסיות

פריטים	ערך ההגדרה ותיאורה
Use Bonjour	בחר בפריט זה כדי לחפש התקנים או להשתמש בהם באמצעות Bonjour.
Bonjour Name	מציג את השם אצל Bonjour.
Bonjour Service Name	תוכל להציג ולהגדיר את שם שירות Bonjour.
Location	מציג את שם המיקום אצל Bonjour.
SLP Settings	
Enable SLP	בחר בפריט זה כדי להפוך את הפונקציה SLP לזמינה. הוא משמש לגילוי רשת ב-Epson Scan 2 וב-EpsonNet Config.
WSD Settings	
Enable WSD	בחר בפריט זה כדי לאפשר הוספת התקנים באמצעות WSD וכדי להדפיס ולסרוק מיציאת WSD.
Scanning Timeout (sec)	הזן את ערך פסק הזמן של התקשורת בשביל סריקה ב-WSD, בין 3 ל-3, 600 שניות.
Device Name	מציג את שם ההתקן אצל WSD.
Location	מציג את שם המיקום אצל WSD.
LLTD Settings	
Enable LLTD	בחר בפריט כדי להפוך את LLTD לזמין. הסורק מוצגת במפת הרשת של Windows.
Device Name	מציג את שם ההתקן אצל LLTD.
LLMNR Settings	
Enable LLMNR	בחר בפריט כדי להפוך את LLMNR לזמין. תוכל להשתמש בזיהוי שמות ללא NetBIOS אפילו אם אינך יכול להשתמש ב-DNS.
SNMPv1/v2c Settings	
Enable SNMPv1/v2c	בחר בפריט כדי להפוך את SNMPv1/v2c לזמין. בתצוגה מופיעים רק הסורקים התומכים ב-SNMPv3.
Access Authority	הגדר את סמכות הגישה כאשר SNMPv1/v2c מאופשר. בחר **Read Only** או **Read/Write**.
Community Name (Read Only)	הזן 0 עד 32 תווי ASCII ‏(0x20 עד 0x7E).
Community Name (Read/Write)	הזן 0 עד 32 תווי ASCII ‏(0x20 עד 0x7E).

הגדרות אבטחה בסיסיות

פריטים	ערך ההגדרה ותיאורה
SNMPv3 Settings	
Enable SNMPv3	SNMPv3 מאופשר כאשר התיבה מסומנת.
User Name	הזן בין 1 ל-32 תווים בשימוש בתווים באורך בייט אחד.
Authentication Settings	
Algorithm	בחר אלגוריתם לאימות עבור SNMPv3.
Password	הזן סיסמה לאימות עבור SNMPv3. הזן בין 8 ל-32 תווים ב-ASCII (0x20–0x7E). אם לא תציין זאת, השאר את המקום ריק.
Confirm Password	הזן את הסיסמה שהגדרת לאישור.
Encryption Settings	
Algorithm	בחר אלגוריתם להצפנה עבור SNMPv3.
Password	הזן סיסמה להצפנה עבור SNMPv3. הזן בין 8 ל-32 תווים ב-ASCII (0x20–0x7E). אם לא תציין זאת, השאר את המקום ריק.
Confirm Password	הזן את הסיסמה שהגדרת לאישור.
Context Name	הזן עד 32 תווים או פחות ב-Unicode (קידוד UTF-8). אם לא תציין זאת, השאר את המקום ריק. מספר התווים שניתן להזין תלוי בשפה.

מידע קשור

➡ "בקרת פרוטוקולים" בעמוד 35

➡ "פרוטוקולים שניתן לאפשר או להשבית" בעמוד 36

הגדרות תפעול וניהול

פרק זה מביר את הפריטים הקשורים לתפעול וניהול יומיומי של ההתקן.

אשר מידע על התקן

תוכל לבדוק את המידע הבא ביחס להתקן הפועל מתוך **Status** באמצעות Web Config.

❏ Product Status

בדוק את השפה, הסטטוס, מספר המוצר, כתובת ה-MAC וכו'.

❏ Network Status

בדוק את המידע על מצב חיבור הרשת, כתובת ה-IP, שרת ה-DNS, וכו'.

❏ Panel Snapshot

הצג צילום מסך שיוצג בלוח הבקרה של ההתקן.

❏ Maintenance

בדוק את תאריך התחילה, מידע סריקה, וכו'.

❏ Hardware Status

בדוק את מצב הסורק.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

ניהול התקנים (Epson Device Admin)

תוכל לנהל ולהפעיל התקנים רבים באמצעות Epson Device AdminEpson Device Admin . מאפשר לך לנהל התקנים הממוקמים ברשת אחרת. המידע שלהלן מתווה את תכונות הניהול המרכזיות.

למידע נוסף על הפונקציות והשימוש בתוכנה עיין בתיעוד או בעזרה של Epson Device Admin.

❏ גילוי התקנים

ביכולתך לגלות התקנים ברשת, ואז לרשום אותם ברשימה. אם התקני Epson כגון מדפסות וסורקים מחוברים לאותו מקטע רשת כמו מחשבו של המנהל, תוכל למצוא אותם גם אם לא הוקצתה להם כתובת IP.

תוכל גם לגלות התקנים המחוברים למחשבים ברשת באמצעות כבלי USB. עליך להתקין במחשב את Epson Device USB Agent.

❏ הגדרת התקנים

תוכל להכין תבנית המכילה פריטי הגדרות כמו ממשק הרשת ומקור הנייר, ולהחיל אותה על התקנים אחרים כהגדרות משותפות. כאשר הוא מחובר לרשת, תוכל להקצות כתובת IP גם להתקן שלא הוקצתה לו כתובת IP.

❏ ניטור התקנים

תוכל להשיג ברשת באופן סדיר את הסטטוס של התקנים ומידע מפורט על אודותם. תוכל גם לנטר התקנים המחוברים למשחבים ברשת באמצעות כבלי USB והתקנים של חברות אחרות שנרשמו ברשימת ההתקנים. על מנת לנטר התקנים המחוברים באמצעות כבלי USB, עליך להתקין את Epson Device USB Agent.

❏ ניהול התראות

תוכל לנטר התראות על אודות הסטטוס של התקנים וחומרים מתכלים. המערכת שולחת באופן אוטומטי הודעות דוא"ל אל המנהל בהתאם לתנאים שהוגדרו.

❏ ניהול דווחים

תוכל ליצור דווחים סדרים ככל שהמערכת צוברת נתונים על שימוש בהתקנים ובחומרים מתכלים. תוכל אז לשמור דווחים אלה שנוצרו ולשלוח אותם באמצעות הדוא"ל.

מידע קשור

➡ "Epson Device Admin" בעמוד 55

קבלת התראות בדואר אלקטרוני כאשר מתרחשים אירועים

אודות התראות דואר אלקטרוני

תוכל להשתמש בתכונה זאת כדי לקבל התראות בדואר אלקטרוני כאשר מתרחשים אירועים. תוכל לרשום עד 5 כתובות דואר אלקטרוני ולבחור עבור אילו אירועים תרצה לקבל התראה.

יש להגדיר את תצורת שרת הדואר כדי להשתמש בפונקציה זו.

מידע קשור

➡ "הגדרת שרת דואר" בעמוד 42

הגדרת התראות דואר אלקטרוני

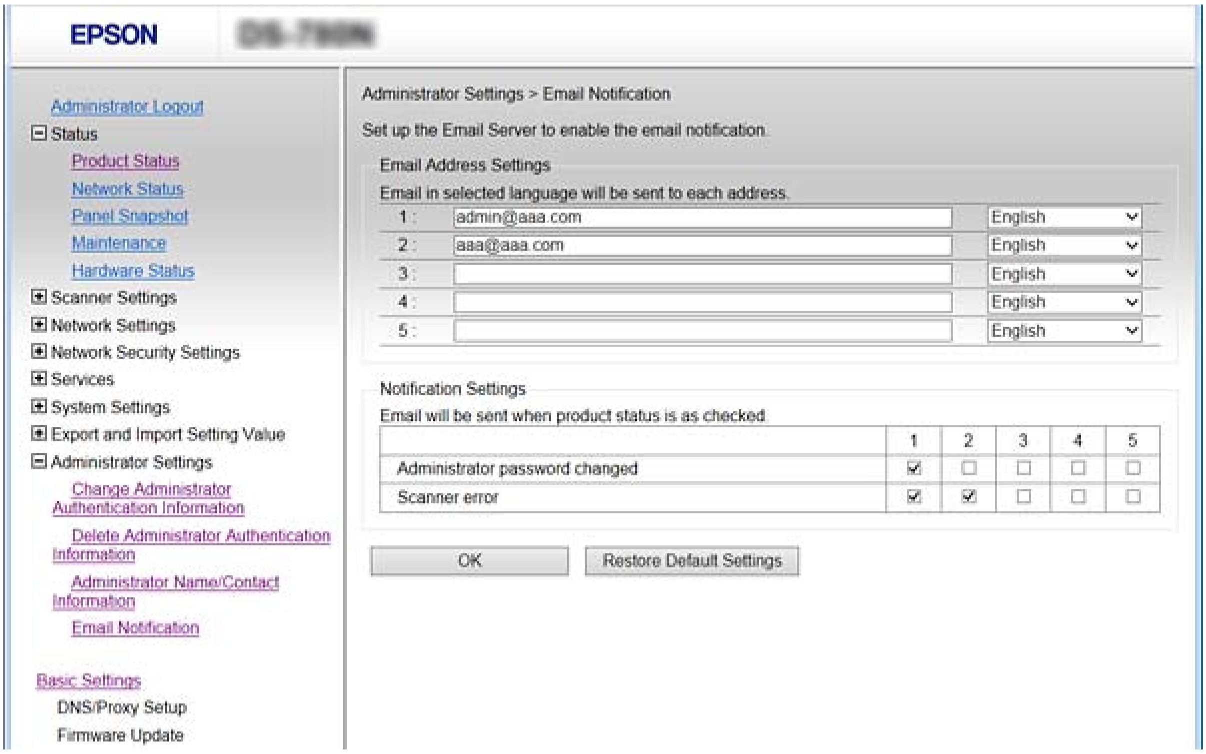
כדי להשתמש בתכונה זו, יהיה עליך להגדיר שרת דואר.

1. גש אל Web Config ובחר **Administrator Settings** > **Email Notification**.

2. הזן כתובת דואר אלקטרוני שאליה תרצה לשלוח התראות דואר אלקטרוני.

3. בחר בשפה להתראות הדואר האלקטרוני.

4. סמן את התיבות עבור התראות שתרצה לקבל.



5. לחץ על OK.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

➡ "הגדרת שרת דואר" בעמוד 42

הגדרת שרת דואר

לפני ההגדרה עליך לבדוק את הדברים המפורטים להלן.

❏ הסורק מחובר לרשת.

❏ נתוני שרת הדואר האלקטרוני של המחשב.

1. גש אל Web Config ובחר Network Settings < Email Server < Basic.

2. הזן ערך עבור כל פריט.

3. בחר OK.

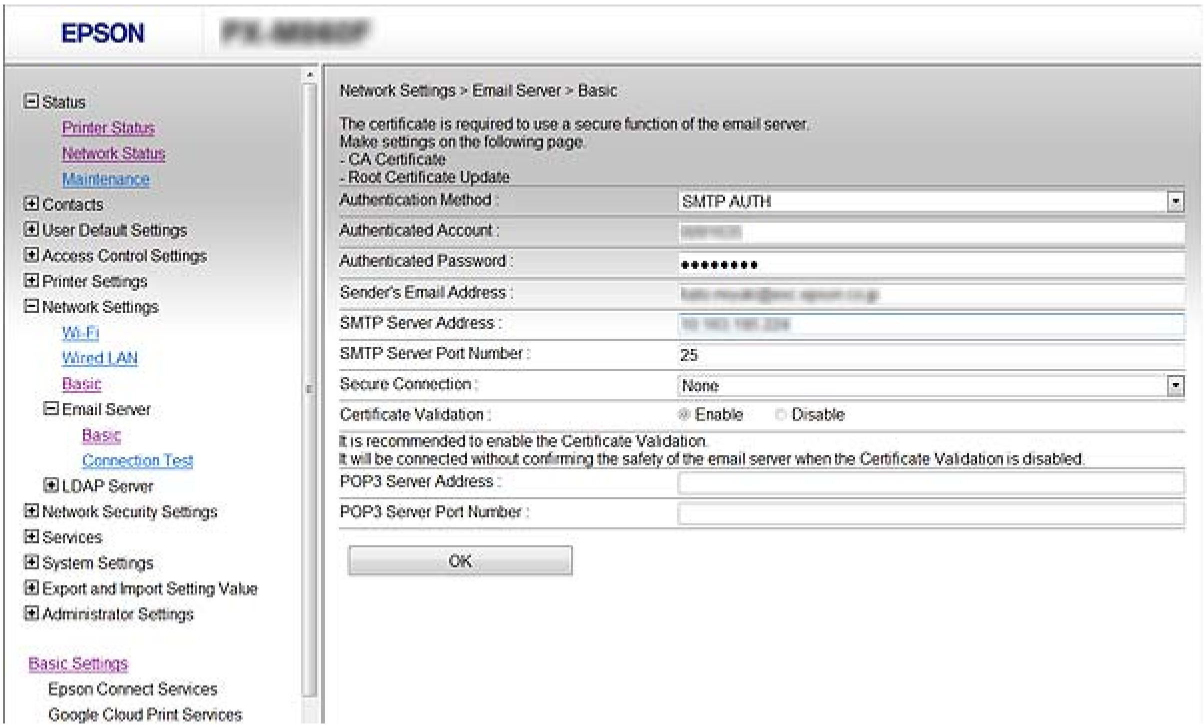
ההגדרות הנבחרות תוצגנה.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

➡ "פריטי הגדרות שרת דואר" בעמוד 43

פריטי הגדרות שרת דואר



פריטים	הגדרות והסבר	
Authentication Method	ציין את שיטת האימות עבור גישת הסורק אל שרת הדואר.	
	Off	אימות מושבת בתקשורת עם שרת דואר.
	SMTP AUTH	מחייב תמיכה של שרת הדואר באימות SMTP.
	POP before SMTP	אם בחרת בשיטה זו, הגדר את שרת POP3.
Authenticated Account	אם אתה בוחר **SMTP AUTH** או **POP before SMTP** בתור **Authentication Method**, הזן את שם החשבון באורך בין 0 ל-255 תווים ב-ASCII (0x20–0x7E).	
Authenticated Password	אם אתה בוחר **SMTP AUTH** או **POP before SMTP** בתור **Authentication Method**, הזן סיסמה מאומתת באורך בין 0 ל-20 תווים המכילה את הסימנים 0–9 a–z A–Z ! # $ % & ' * + - . / = ? ^ _ { | } ~ @.	
Sender's Email Address	הזן את כתובת הדואר האלקטרוני של השולח. הזן בין 0 ל-255 תווי ASCII (0x20–0x7E) למעט : ( ) < > [ ] ; ¥. התו הראשון לא יכול להיות נקודה ".".	
SMTP Server Address	הזן בין 0 ל-255 תווים מסוג אותיות A–Z, a–z וכן 0–9. - . תוכל להשתמש בתבנית IPv4 או FQDN.	
SMTP Server Port Number	הזן מספר בין 1 ל-65535.	

פריטים	הגדרות והסבר	
Secure Connection	ציין את שיטת החיבור המאובטח לשרת הדואר האלקטרוני.	
	None	אם אתה בוחר **POP before SMTP** ב-**Authentication Method**, שיטת החיבור מוגדרת כ-**None**.
	SSL/TLS	אפשרות זו זמינה כאשר **Authentication Method** מוגדר כ-**Off** או כ-**SMTP AUTH**.
	STARTTLS	אפשרות זו זמינה כאשר **Authentication Method** מוגדר כ-**Off** או כ-**SMTP AUTH**.
Certificate Validation	האישור מאומת כאשר מצב זה זמין. מומלץ להגדיר אותו כ-**Enable** (זמין).	
POP3 Server Address	אם אתה בוחר **POP before SMTP** בתור **Authentication Method**, הזן את כתובת שרת POP3 בין 0 ל-255 תווים תוך שימוש באותיות A–Z, a–z וכן 0–9 . - . תוכל להשתמש בתבנית IPv4 או FQDN.	
POP3 Server Port Number	אם אתה בוחר **POP before SMTP** כ- **Authentication Method**, הזן מספר בין 1 ל-65535.	

מידע קשור

➡ "הגדרת שרת דואר" בעמוד 42

בדיקת חיבור לשרת דואר

1. גש אל Web Config ובחר **Network Settings** > **Email Server** > **Connection Test**.
2. בחר **Start**.

   חיבור הבדיקה עם שרת הדואר יתחיל. בסיום הבדיקה, יוצג דוח הבדיקה.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23
➡ "מקורות בדיקה לחיבור שרת דואר" בעמוד 44

מקורות בדיקה לחיבור שרת דואר

הודעות	הסבר
Connection test was successful.	ההודעה מופיעה אם החיבור לשרת הצליח.

הודעות	הסבר
SMTP server communication error. Check the following. - Network Settings	ההודעה מופיעה כאשר ❏ הסורק אינו מחובר לרשת ❏ שרת SMTP מושבת ❏ החיבור לרשת התנתק במהלך החיבור ❏ התקבלו נתונים חלקיים
POP3 server communication error. Check the following. - Network Settings	ההודעה מופיעה כאשר ❏ הסורק אינו מחובר לרשת ❏ שרת POP3 מושבת ❏ החיבור לרשת התנתק במהלך החיבור ❏ התקבלו נתונים חלקיים
An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server	ההודעה מופיעה כאשר ❏ ההתחברות אל שרת ה-DNS נכשלה ❏ זיהוי שמות עבור שרת SMTP נכשל
An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server	ההודעה מופיעה כאשר ❏ ההתחברות אל שרת ה-DNS נכשלה ❏ זיהוי שמות עבור שרת POP3 נכשל
SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	ההודעה מופיעה כאשר אימות שרת SMTP נכשל.
POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password	ההודעה מופיעה כאשר אימות שרת POP3 נכשל.
Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number	ההודעה מופיעה כאשר אתה מנסה לקיים תקשורת באמצעות פרוטוקולים שאינם נתמכים.
Connection to SMTP server failed. Change Secure Connection to None.	ההודעה מופיעה כאשר ישנו חוסר התאמת SMTP בין שרת ולקוח, או כאשר השרת לא תומך בחיבור SMTP בטוח (חיבור SSL).

הודעות	הסבר
Connection to SMTP server failed. Change Secure Connection to SSL/TLS.	ההודעה מופיעה כאשר ישנו חוסר התאמת SMTP בין שרת ולקוח, או כאשר השרת מבקש להשתמש בחיבור SSL/TLS עבור חיבור SMTP בטוח.
Connection to SMTP server failed. Change Secure Connection to STARTTLS.	ההודעה מופיעה כאשר ישנו חוסר התאמת SMTP בין שרת ולקוח, או כאשר השרת מבקש להשתמש בחיבור STARTTLS עבור חיבור SMTP בטוח.
The connection is untrusted. Check the following. - Date and Time	הודעה זו מופיעה כאשר התאריך והשעה של הסורק אינם נכונים או שתוקף האישור פג.
The connection is untrusted. Check the following. - CA Certificate	הודעה זו מופיעה כאשר לסורק אין אישור בסיס המתאים לשרת או אם לא יובא CA Certificate.
The connection is not secured.	הודעה זו מופיעה כאשר האישור שהתקבל הוא פגום.
SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.	הודעה זו מופיעה כאשר יש אי-התאמה בין שיטות האימות של השרת והלקוח. השרת תומך ב-SMTP AUTH.
SMTP server authentication failed. Change Authentication Method to POP before SMTP.	הודעה זו מופיעה כאשר יש אי-התאמה בין שיטות האימות של השרת והלקוח. השרת אינו תומך ב-SMTP AUTH.
Sender's Email Address is incorrect. Change to the email address for your email service.	הודעה זו מופיעה כאשר כתובת הדואר האלקטרוני הנקובה של השולח שגויה.
Cannot access the product until processing is complete.	הודעה זו מופיעה כאשר הסורק עסוק.

מידע קשור

← "בדיקת חיבור לשרת דואר" בעמוד 44

עדכון קושחה

עדכון קושחה באמצעות Web Config

מעדכן את הקושחה באמצעות Web Config. יש לחבר התקן זה לאינטרנט.

1. גש אל Web Config ובחר **Basic Settings** < **Firmware Update**.

2. לחץ על **Start**.

אישור הקושחה מתחיל, ומידע הקושחה מוצג במידה וקיימת קושחה מעודכנת.

3. לחץ **Start**, ופעל על-פי ההוראות שעל המסך.

לתשומת לבך:
באפשרותך גם לעדכן את הקושחה באמצעות Epson Device Admin. תוכל לאשר חזותית את מידע הקושחה ברשימת ההתקנים. יש בכך תועלת כאשר אתה רוצה לעדכן את הקושחה של מספר התקנים. עיין במדריך Epson Device Admin לעזרה ופרטים נוספים.

מידע קשור

➔ "גישה אל Web Config" בעמוד 23
➔ "Epson Device Admin" בעמוד 55

עדכון קושחה באמצעות Epson Firmware Updater

תוכל להוריד את הקושחה של ההתקן מאתר האינטרנט של Epson במחשב, ואז לחבר את ההתקן ואת המחשב באמצעות כבל USB על מנת לעדכן את הקושחה. אם לא תוכל לעדכן באמצעות הרשת, נסה שיטה זו.

1. גש לאתר האינטרנט של Epson והורד את הקושחה.

2. חבר את המחשב המכיל את הקושחה שהורדת אל ההתקן באמצעות כבל USB.

3. לחץ לחיצה כפולה על קובץ ה-.exe שהורדת.

Epson Firmware Updater יתחיל לפעול.

4. פעל על פי ההוראות המוצגות.

גיבוי ההגדרות

באמצעות ייצוא הפריטים שהוגדרו ב-Web Config, תוכל להעתיק את הפריטים לסורקים אחרים.

יצא את ההגדרות

יצא כל אחת מההגדרות בשביל הסורק.

1. גש אל Web Config, ולאחר מכן בחר **Export and Import Setting Value** < **Export**.

2. בחר את ההגדרות שברצונך לייצא.

בחר את ההגדרות שברצונך לייצא. אם בחרת בקטגוריית אב, גם קטגוריות משנה ייבחרו. עם זאת, אי אפשר לבחור קטגוריות משנה הגורמות לשגיאות עקב יצירת כפילות בתוך אותה הרשת (למשל כתובת IP וכן הלאה).

3. הזן סיסמה כדי להצפין את הקובץ המיוצא.

דרושה לך סיסמה כדי לייבא את הקובץ. אם אינך מעוניין להצפין את הקובץ, השאר את השדה הזה ריק.

4. לחץ על **Export**.

> **חשוב:**
> *אם ברצונך לייצא את הגדרות הרשת של הסורק, למשל שם הסורק וכתובת ה-IP שלו, בחר Enable to select the individual settings of device ובחר עוד פריטים. השתמש אך ורק בערכים שנבחרו בשביל הסורק המחליף.*

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

יבא את ההגדרות

יבא אל הסורק את קובץ הWeb Config שכבר יוצא.

> **חשוב:**
> *כאשר מייבאים ערכים הכוללים מידע אינדיבידואלי, למשל שם סורק או כתובת IP שלו, ודא שכתובת ה-IP אינה קיימת באותה הרשת. אם כתובת ה-IP חופפת, הסורק אינו משקף את הערך.*

1. גש אל Web Config, ולאחר מכן בחר **Export and Import Setting Value** > **Import**.
2. בחר את הקובץ המיוצא, ולאחר מכן הזן את הסיסמה המוצפנת.
3. לחץ על **Next**.
4. בחר את ההגדרות שברצונך לייבא, ולאחר מכן לחץ על **Next**.
5. לחץ על **OK**.

ההגדרות יחולו על הסורק.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

פתרון בעיות

טיפים לפתרון בעיות

תוכל למצוא מידע נוסף במדריך הבא.

❑ מדריך למשתמש

מספק הוראות לשימוש בסורק, לתחזוקה ולפתרון בעיות.

בדיקת קובץ הרישום עבור שרת והתקן רשת

במקרה של בעיות בחיבור רשת, אפשר שניתן יהיה לזהות את הסיבה לבעיה באמצעות אישור יומן שרת המייל, שרת ה-LDAP, וכו', ובדיקת המצב באמצעות יומן הרשת של יומני ופקודות ציוד, כגון נתבים.

אתחול הגדרות הרשת

שחזור הגדרות הרשת מלוח הבקרה

תוכל להחזיר את כל הגדרות הרשת לברירות המחדל שלהם.

1. הקש הגדרות במסך הבית.
2. הקש **ניהול מערכת** > **שחזור הגדרות ברירת מחדל** > **הגדרות רשת**.
3. בדוק את ההודעה, ואז הקש כן.
4. כאשר מוצגת הודעה על השלמת התהליך, הקש **סגירה**.

   המסך נסגר אוטומטית אחרי פרק זמן מסויים אם לא הקשת **סגירה**.

בדיקת התקשורת בין התקנים למחשבים

בדיקת החיבור באמצעות פקודת — PingWindows

תוכל להשתמש בפקודה Ping כדי לוודא שהמחשב מחובר לסורק. פעל על פי הצעדים להלן כדי לבדוק את החיבור על ידי שימוש בפקודה Ping.

1. בדוק את כתובת ה-IP של הסורק עבור החיבור שברצונך לבדוק.

   תוכל לבדוק זאת על ידי שימוש ב Epson Scan 2.

פתרון בעיות

2. הצג את מסך שורת הפקודה של המחשב.

❏ Windows 10

לחץ באמצעות לחצן העכבר הימני על הכפתור "התחל", או לחץ עליו לחיצה ממושכת באמצעות לחצן העכבר השמאלי, ולאחר מכן בחר **שורת הפקודה**.

❏ Windows 8.1/Windows 8/Windows Server 2012 R2/Windows Server 2012

הצג את מסך האפליקציה ואז בחר **שורת הפקודה**.

❏ Windows 7/Windows Server 2008 R2/Windows Vista/Windows Server 2008 או ישנה יותר

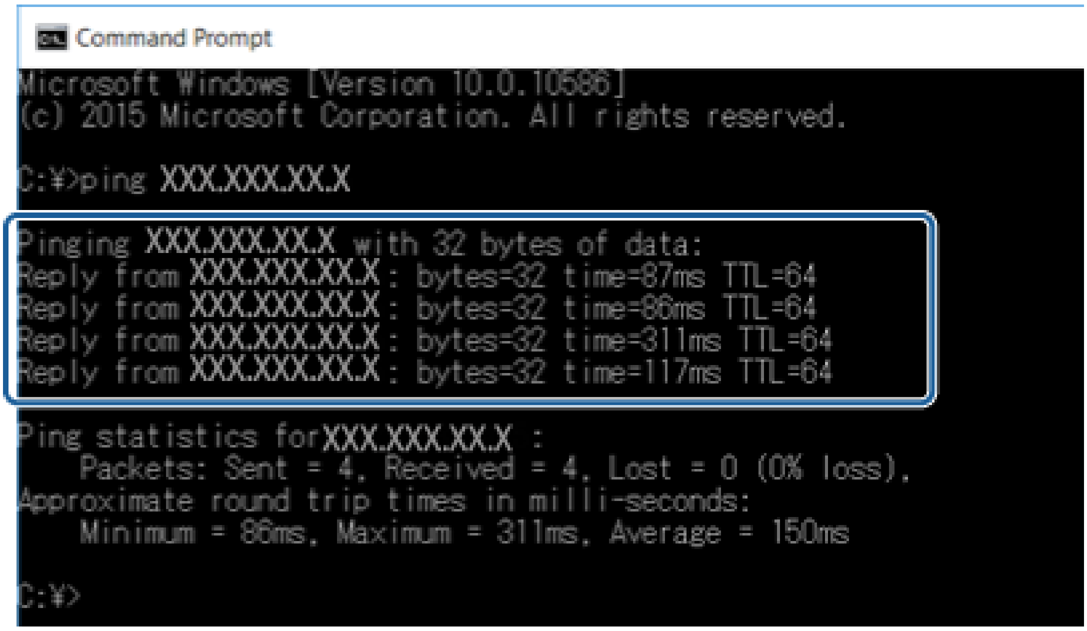
לחץ על הכפתור "התחל", בחר **כל התוכניות** או **תוכניות** > **אביזרים** > **שורת הפקודה**.

3. הזן "ping xxx.xxx.xxx.xxx", ולאחר מכן לחץ על מקש אנטר.

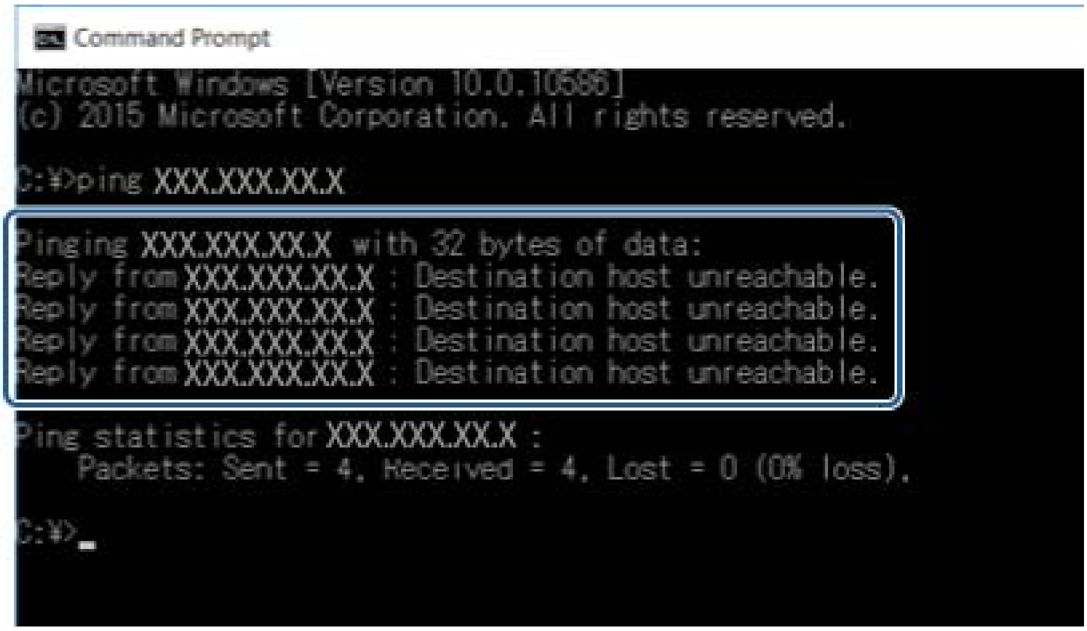
הזן את כתובת ה-IP של הסורק עבור xxx.xxx.xxx.xxx.

4. בדוק את מצב התקשורת.

אם נוצרה תקשורת בין הסורק לבין המחשב, תוצג ההודעה הבאה.



אם לא נוצרה תקשורת בין הסורק לבין המחשב, תוצג ההודעה הבאה.



בדיקת החיבור שלך באמצעות פקודת Mac OS — Ping

תוכל להשתמש בפקודה Ping כדי לוודא שהמחשב מחובר לסורק. פעל על פי הצעדים להלן כדי לבדוק את החיבור על ידי שימוש בפקודה Ping.

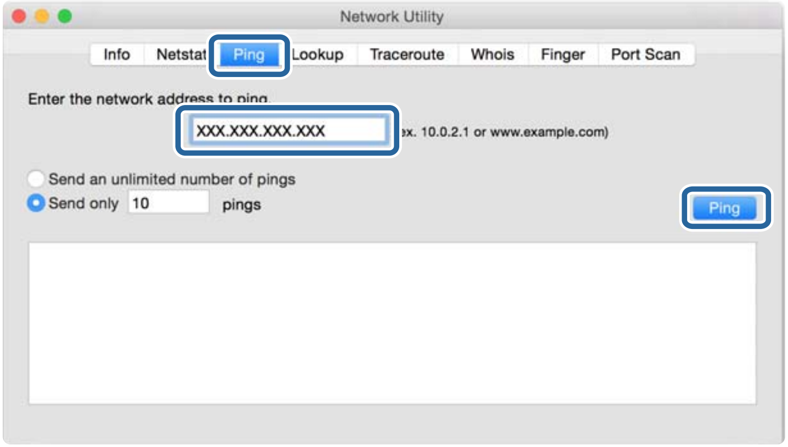
1. בדוק את כתובת ה-IP של הסורק עבור החיבור שברצונך לבדוק.

   תוכל לבדוק זאת על ידי שימוש ב Epson Scan 2.

2. הפעל את תוכנת העזר עבור הרשת.

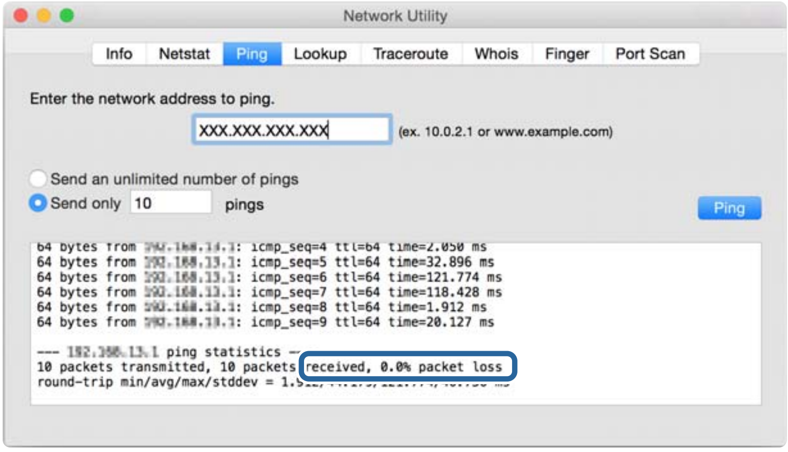
   הזן "תוכנת העזר עבור הרשת" ב-**Spotlight**.

3. לחץ על הלשונית **Ping**, הזן את כתובת ה-IP שבדקת בשלב 1, ואז לחץ על **Ping**.

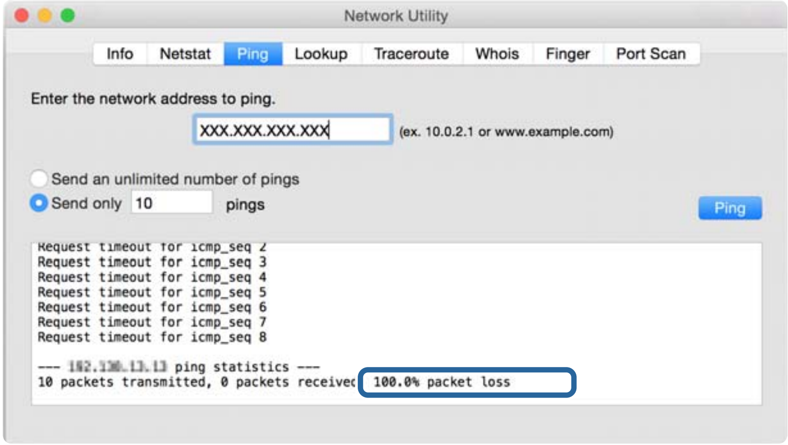


4. בדוק את מצב התקשורת.

אם נוצרה תקשורת בין הסורק לבין המחשב, תוצג ההודעה הבאה.



אם לא נוצרה תקשורת בין הסורק לבין המחשב, תוצג ההודעה הבאה.



בעיות בשימוש בתוכנת רשת

לא ניתן לגשת אל Web Config

האם כתובת ה-IP של הסורק הוגדרה כהלכה?

הגדר את כתובת ה-IP באמצעות Epson Device Admin או באמצעות EpsonNet Config.

האם הדפדפן שלך תומך בהצפנות בצובר בשביל Encryption Strength של SSL/TLS?

ההצפנות בצובר בשביל Encryption Strength של SSL/TLS הן כלהלן. אפשר לגשת אל Web Config רק בדפדפן התומך בהצפנות צובר המפורטות להלן. בדוק את תמיכת ההצפנה בדפדפן שלך.

❏ 80bit: AES256/AES128/3DES

❏ 112bit: AES256/AES128/3DES

- ❏ AES256/AES128 :128bit
- ❏ AES256 :192bit
- ❏ AES256 :256bit

מופיעה הודעת "פג תוקף" בעת גישה ל-Web Config באמצעות תקשורת SSL (https).

אם האישור פג תוקף, השג את האישור שוב. אם ההודעה מופיעה לפני תאריך התפוגה שלו, ודא כי הגדרות התאריך בסורק תקינות.

מופיעה ההודעה "שם אישור האבטחה אינו תואם···" בעת גישה ל-Web Config באמצעות תקשורת SSL (https).

כתובת ה-IP של הסורק הוכנסה עבור Common Name ליצירת אישור בחתימה עצמית או CSR אינה תואמת את הכתובת שהוכנסה לדפדפן. השג וייבא את האישור שוב או שנה את שם הסורק.

הגישה לסורק נעשית דרך שרת proxy.

אם אתה משתמש בשרת proxy עם הסורק שלך, עליך לשנות את תצורת הגדרות ה-proxy של הדפדפן שלך.

❏ Windows:

בחר **לוח הבקרה** > **רשת ואינטרנט** > **אפשרויות אינטרנט** > **חיבורים** > **הגדרות LAN** > **שרת Proxy**, ואז הגדר שלא להשתמש בשרת proxy עבור כתובות מקומיות.

❏ Mac OS:

בחר **העדפות מערכת** > **רשת** > **מתקדם** > **שרתי Proxy**, ואז רשום את הכתובת המקומית עבור **עקוף הגדרות Proxy עבור יציאות ותחומים אלה**.

לדוגמה:

192.168.1.*: כתובת מקומית 192.168.1.XXX, מסיכת רשת משנה 255.255.255.0

192.168.*.*: כתובת מקומית 192.168.XXX.XXX, מסיכת רשת משנה 255.255.0.0

מידע קשור

➡ "גישה אל Web Config" בעמוד 23
➡ "הקצאת כתובת ה-IP" בעמוד 15
➡ "הקצאת כתובת IP באמצעות EpsonNet Config" בעמוד 56

שם דגם ו/או כתובת UP אינם מוצגים ב-EpsonNet Config

האם בחרת באפשרות חסום, בטל, או כבה כאשר הוצג מסך אבטחה או מסך חומת-אש של Windows?

אם בחרת באפשרות **חסום**, **בטל**, או **כבה**, כתובת ה-IP ושם הדגם לא יופיעו ב-EpsonNet Config או EpsonNet Setup.

על מנת לתקן זאת, רשום את EpsonNet Config כיוצא דופן באמצעות חומת-האש של Windows ותוכנות אבטחה מסחריות. אם אתה משתמש באנטי-וירוס או בתוכנת אבטחה, סגור אותה ואז נסה להשתמש ב-EpsonNet Config.

האם הזמן שהוקצב לשגיאת התקשורת קצר מדי?

הפעל את EpsonNet Config ובחר **Tools** < **Options** < **Timeout**, ולאחר מכן הארך את משך הזמן עבור הגדרת **Communication Error**. שים לב שפעולה זו יכולה לגרום ל-EpsonNet Config לעבוד לאט יותר.

מידע קשור

➡ "הפעלת EpsonNet Config — Windows" בעמוד 56

➡ "הפעלת EpsonNet Config — Mac OS" בעמוד 56

נספח

מבוא לתוכנת רשת

להלן מתוארת התוכנה המגדירה ומנהלת את ההתקנים.

Epson Device Admin

Epson Device Admin הנו יישום המאפשר התקנה של התקנים ברשת ולאחר מכן להגדיר ולנהל את ההתקנים הללו. תוכל לרכוש מידע מפורט עבור התקנים כמו הסטטוס והחומרים המתכלים, שליחת הודעות על התראות, ויצירת דוחים על שימוש בהתקן. תוכל גם להכין תבנית המכילה פריטי הגדרות ולהחיל אותה על התקנים אחרים כהגדרות משותפות. תוכל להוריד את Epson Device Admin מאתר התמיכה של Epson. למידע נוסף, עיין בתיעוד או בעזרה של Epson Device Admin.

הפעלת Epson Device Admin (Windows בלבד)

בחר כל התוכניות < EPSON < Epson Device Admin < Epson Device Admin.

לתשומת לבך:
אם מופיעה התראת חומת-אש, אפשר גישה ל-Epson Device Admin.

EpsonNet Config

EpsonNet Config מאפשר למנהל המערכת לקבוע את תצורת הגדרות הרשת של הסורק, כגון הקצאת כתובת IP ושינוי מצב החיבור. תכונת הגדרת האצווה נתמכת ב-Windows. למידע נוסף, עיין בתיעוד או בעזרה של EpsonNet Config.

הפעלת WindowsEpsonNet Config —

בחר כל התוכניות > EpsonNet > EpsonNet Config SE > EpsonNet Config.

לתשומת לבך:
אם מופיעה התראת חומת-אש, אפשר גישה ל-EpsonNet Config.

הפעלת Mac OSEpsonNet Config —

בחר באפשרות עבור אל > יישומים > Epson Software > EpsonNet > EpsonNet Config SE > EpsonNet Config.

EpsonNet SetupManager

EpsonNet SetupManager הוא תוכנה המיועדת ליצירת חבילה ההופכת את התקנת הסורק לתהליך קל, למשל התקנה של מנהל התקן הסורק וקביעת התצורה שלו, והתקנת Document Capture Pro. התוכנה מאפשרת למנהל המערכת ליצור חבילות תוכנה ייחודיות ולהפיץ אותן בקרב קבוצות.

לפרטים נוספים, בקר באתר Epson באזורך.

הקצאת כתובת IP באמצעות EpsonNet Config

תוכל להקצות כתובת IP לסורק באמצעות EpsonNet ConfigEpsonNet Config . מאפשר לך להקצות כתובת IP לסורק שלא הוקצתה לו כתובת כזאת אחרי ביצוע חיבור באמצעות כבל Ethernet.

הקצאת כתובת IP באמצעות הגדרות אצווה

יצירת הקובץ עבור הגדרות אצווה

באמצעות כתובת ה-MAC ושם הדגם כמפתחות, תוכל ליצור קובץ SYLK חדש על מנת להגדיר את כתובת ה-IP.

1. פתח יישום גליון אלקטרוני (כגון Microsoft Excel) או עורך טקסט.

2. הזן"Info_MACAddress", "Info_ModelName", ו- "TCPIP_IPAddress" בשורה הראשונה כשמות פריט ההגדרה.

   הזן את פריטי ההגדרה עבור מחרוזות הטקסט שלהלן. יש להבחין בין אותיות גדולות/אותיות קטנות באנגלית ובין תווי בית-כפול/בית-יחיד. די בתו אחד שונה כדי שהפריט לא יזוהה.

   הזן את שם פריט ההגדרה כמתואר להלן; אחרת EpsonNet Config לא תוכל לזהות את פריטי ההגדרה.

Info_MACAddress	Info_ModelName	TCPIP_IPAddress

3. הזן את כתובת ה-MAC address, את שם הדגם, ואת כתובת ה-IP עבור כל אחד מממשקי הרשת.

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. הזן שם ושמור כקובץ SYLK עם סיומת מתאימה (*.slk).

ביצוע הגדרות אצווה באמצעות קובץ הגדרת תצורה

הקצה בבת אחת כתובות IP בקובץ הגדרת התצורה (קובץ SYLK). עליך ליצור את קובץ הגדרת התצורה לפני ההקצאה.

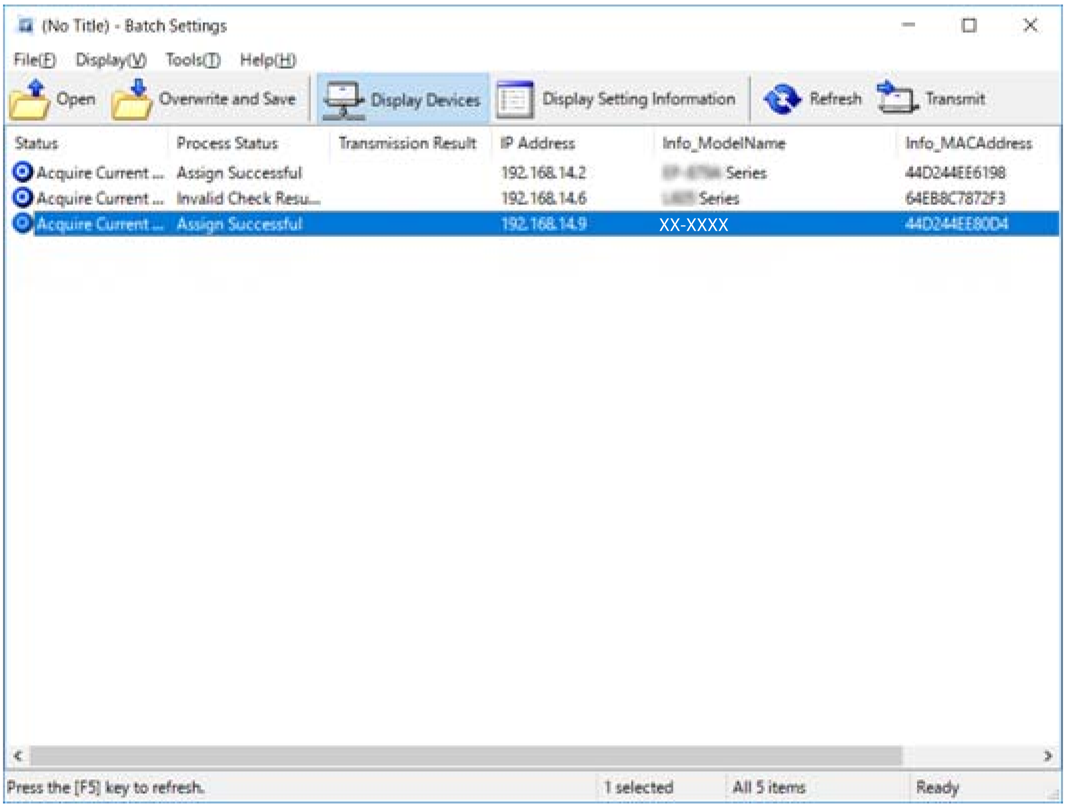
1. חבר את כל ההתקנים לרשת באמצעות כבל Ethernet.
2. הדלק את הסורק.
3. התחל את EpsonNet Config.

   תוצג רשימה של סורקים המחוברים לרשת. אפשר שיעבור זמן מה לפני שהם יוצגו.
4. לחץ על **Tools** > **Batch Settings**.
5. לחץ על **Open**.
6. במסך בחירת הקובץ, בחר את קובץ ה- slk.*) SYLK) המכיל את ההגדרות, ואז לחץ על **Open**.

נספח

7. בחר את ההתקנים שעבורם ברצונך לבצע הגדרות אצווה, כאשר עמודת ה-**Status** מוגדרת כ-**Unassigned**, ו-**Process Status** מוגדר כ-**Assign Successful**.

בעת ביצוע בחירות מרובות, לחץ **Ctrl** או **Shift** ולחץ או גרור את העכבר שלך.



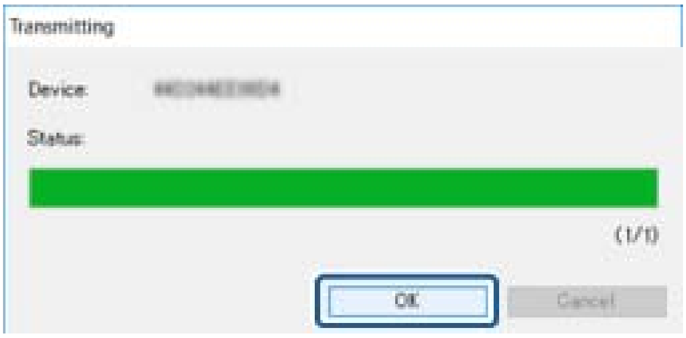
8. לחץ על **Transmit**.

9. כאשר מוצג מסך הזנת הסיסמה, הזן את הסיסמה ואז לחץ על **OK**.

שדר את ההגדרות.

לתשומת לבך:
המידע ישודר לממשק הרשת עד שמד-ההתקדמות יסתיים. אל תכבה את ההתקן או את המתאם האלחוטי, ואל תשלח נתונים כלשהם להתקן.

10. במסך **Transmitting Settings** לחץ **OK**.



11.בדוק את הסטטוס של ההתקן שהגדרת.

בהתקנים שמציגים או , בדוק את התוכן של קובץ ההגדרות, או שההתקן אותחל בצורה תקינה.

סמל	Status	Process Status	הסבר
	Setup Complete	Setup Successful	ההגדרה הושלמה באופן תקין.
	Setup Complete	Rebooting	אחרי שהמידע שודר, צריך כל התקן לבצע אתחול על מנת לאפשר את ההגדרות. מתבצעת בדיקה כדי לברר אם ניתן לחבר את ההתקן אחרי האתחול, או לא.
	Setup Complete	Reboot Failed	לא ניתן לאשר את ההתקן אחרי שידור ההגדרות. בדוק שההתקן דלוק, או שהוא אותחל באופן תקין.
	Setup Complete	Searching	מחפש את ההתקן שצוין בקובץ ההגדרות.*
	Setup Complete	Search Failed	לא ניתן לבדוק התקנים שכבר הוגדרו. בדו שההתקן דלוק, או שהוא אותחל באופן תקין.*

* רק כאשר מוצג מידע על הגדרות.

מידע קשור

➡ "הפעלת EpsonNet Config — Windows" בעמוד 56
➡ "הפעלת EpsonNet Config — Mac OS" בעמוד 56

הקצאת כתובת IP לכל התקן

הקצה כתובת IP לסורק באמצעות EpsonNet Config.

1. הדלק את הסורק.

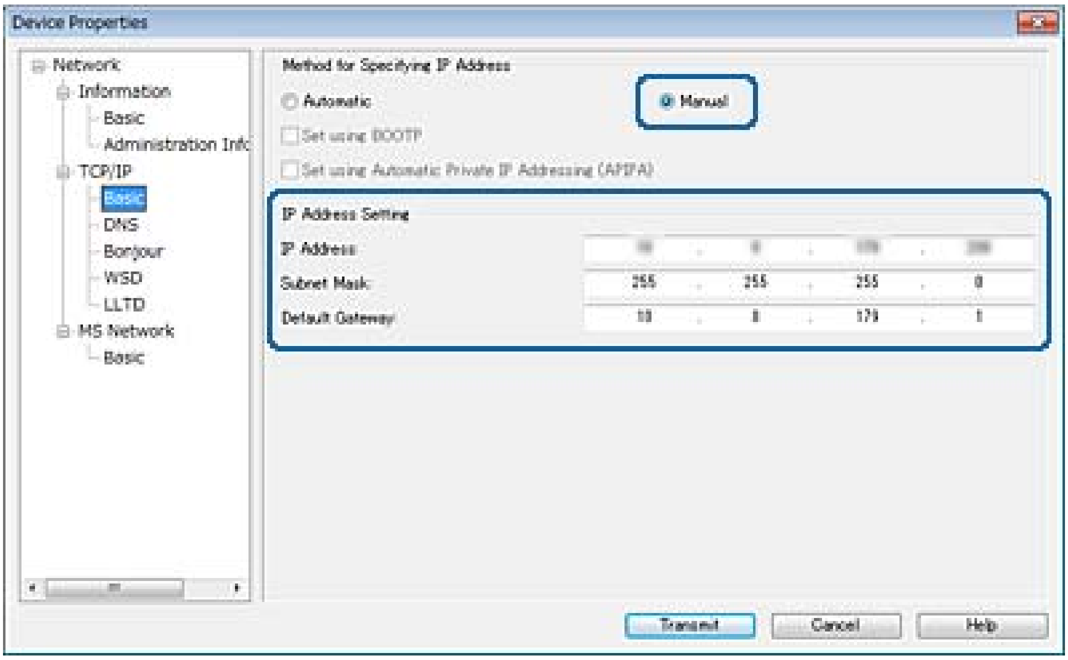
2. חבר את הסורק לרשת באמצעות כבל Ethernet.

3. התחל את EpsonNet Config.
   תוצג רשימה של סורקים המחוברים לרשת. אפשר שיעבור זמן מה לפני שהם יוצגו.

4. לחץ לחיצה כפולה על הסורק שאליו תרצה להקצות.
   לתשומת לבך:
   אם חיברת כמה סורקים מאותו דגם, תוכל לזהות את הסורק באמצעות כתובת ה-MAC.

5. בחר **Network** < **TCP/IP** < **Basic**.

6. הזן את הכתובות עבור **IP Address**, **Subnet Mask** ו- **Default Gateway**.



לתשומת לבך:
הזן כתובת סטטית כאשר אתה מחבר את הסורק על מנת לאבטח רשת.

7. לחץ על **Transmit**.

מוצג המסך המאשר את שידור המידע.

8. לחץ על **OK**.

מוצג מסך השלמת השידור.

לתשומת לבך:
המידע משודר אל ההתקן, ואז מוצגת ההודעה "הגדרת התצורה הושלמה בהצלחה". אל תכבה את ההתקן, ואל תשלח נתונים כלשהם לשירות.

9. לחץ על **OK**.

מידע קשור

➡ "הפעלת EpsonNet Config — Windows" בעמוד 56
➡ "הפעלת EpsonNet Config — Mac OS" בעמוד 56

השימוש ביציאה עבור הסורק

הסורק משתמש ביציאה הבאה. מנהל הרשת צריך לאפשר את זמינותן של יציאות אלה בהתאם לצורך.

נספח

שולח (לקוח)	שימוש	יעד (שרת)	פרוטוקול	מספר יציאה
סורק	שליחת דוא"ל (הודעת דוא"ל)	שרתץ SMTP	SMTP (TCP)	25
			SMTP SSL/ TLS (TCP)	465
			SMTP STARTTLS (TCP)	587
	חיבור POP לפני SMTP (הודעת דוא"ל)	שרת POP	(POP3 (TCP	110
	Control WSD	מחשב לקוח	WSD (TCP)	5357
	חפש במחשב בעת ביצוע סריקה בלחיצה מתוך Document Capture Pro	מחשב לקוח	גילוי סריקה בלחיצה ברשת	2968
	איסוף נתוני העבודה בעת ביצוע סריקה בלחיצה מתוך Document Capture Pro	מחשב לקוח	סריקה בלחיצה ברשת	2968
מחשב לקוח	גלה את הסורק מתוך אפליקציה כגון EpsonNet Config, ומנהל התקן של הסורק.	סורק	ENPC (UDP)	3289
	אסוף והגדר את מידע ה-MIB מתוך אפליקציה כגון EpsonNet Config, ומנהל התקן של הסורק.	סורק	SNMP (UDP)	161
	חיפוש סורק WSD	סורק	WS-Discovery ((UDP	3702
	העברת נתוני הסריקה מ-Document Capture Pro	סורק	סריקת רשת (TCP)	1865

הגדרות אבטחה מתקדמות עבור ארגון

בפרק זה אנו מתארים תכונות אבטחה מתקדמות.

הגדרות אבטחה ומניעת סכנה

כאשר התקן מחובר לרשת, ניתן לגשת אליו מאתר מרוחק. בנוסף לכך, אנשים רבים יכולים להתחלק בהתקן, והדבר מועיל לשיפור היעילות והנוחות התפעולית. עם זאת, גוברים הסיכונים כגון גישה בלתי חוקית, שימוש בלתי חוקי, ופגיעה בנתונים. אם אתה משתמש בהתקן בסביבה שבה יש לכך גישה לאינטרנט, הסיכונים יהיו אף יותר גבוהים.

על מנת למנוע סיכון זה, התקני Epson מצוידים במגוון של טכנולוגיות אבטחה.

הגדר את ההתקן כנדרש בהתאם לתנאים הסביבתיים שנבנו עם מידע על סביבת הלקוח.

שם	סוג מאפיין	מה להגדיר	מה למנוע
תקשורת SSL/TLS	נתיב התקשורת בין מחשב לבין התקן מוצפן באמצעות תקשורת SSL/TLS. תכולת התקשורת באמצעות דפדפן מוגנת.	הגדר אישור CA עבור השרת שהוא אישור החתום בידי CA (רשות אישורים) עבור ההתקן.	מנע דליפה של מידע על הגדרות ותכולת נתונים שהועברו לסורק מהמחשב. ניתן להגן על הגישה מההתקן אל שרת Epson באינטרנט גם באמצעות עדכון קושחה, וכו'.
סינון IPsec/IP	תוכל להגדיר לאפשר קיטוע וחיתוך של נתונים המגיעים מלקוח מסוים או מסוג מסוים. מאחר ו-IPsec מגן על הנתונים באמצעות יחידת מנת IP (הצפנה ואימות), תוכל להעביר בבטחה פרוטוקול סריקה בלתי מאובטח.	צור מדיניות בסיסית ומדיניות אישית להגדרת הלקוח או סוג הנתונים שיכולים לגשת אל ההתקן.	הגן מפני גישה בלתי מורשית, ומפני פגיעה בלתי חוקית ויירוט של נתוני תקשורת המגיעים אל ההתקן.
SNMPv3	נוספים מאפיינים כגון ניטור התקנים מחוברים ברשת, שלמות הנתונים המגיעים אל פרוטוקול SNMP לשם בקרה, הצפנה, אימות משתמש וכו'.	אפשר את SNMPv3 ואז הגדר את שיטת האימות וההצפנה.	תוכל לוודא את החסיון של שינוי הגדרות באמצעות הרשת, ושל ניטור המצב.
IEEE802.1X	מאפשר רק למשתמש שאומת עבור Ethernet להתחבר. מאפשר רק למשתמש מורשה להשתמש בהתקן.	הגדרת האימות עבור שרת ה-RADIUS (שרת אימות).	מגן על ההתקן מפני גישה ושימוש בלתי מורשים.

שם	סוג מאפיין	מה להגדיר	מה למנוע
קרא את כרטיס הזהות	תוכל להשתמש בהתקן באמצעות החזקת כרטיס זהות מעל להתקן המאומת המחובר. תוכל להגביל את רכישת יומני הרישום עבור כל משתמש והתקן, ולהגביל את השימוש הזמין בהתקנים ואת המאפיינים הזמינים לכל משתמש וקבוצה.	חבר התקן אימות אל ההתקן, ואז הגדר את המידע של המשתמש במערכת האימות.	מונע שימוש בלתי מורשה והונאות התחזות של ההתקן.

מידע קשור

← "תקשורת SSL/TLS עם הסורק" בעמוד 63
← "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 71
← "שימוש בפרוטוקול SNMPv3" בעמוד 84
← "חיבור הסורק לרשת IEEE802.1X" בעמוד 86

הגדרות תכונת האבטחה

כאשר מגדירים סינון IPsec/IP או IEEE802.1X, מומלץ לגשת אל Web Config באמצעות SSL/TLS על מנת להעביר מידע על ההגדרות כדי לצמצם סיכוני אבטחה כמו טיפול בלתי חוקי או יירוט.

תקשורת SSL/TLS עם הסורק

כאשר אישור השרת מוגדר באמצעות תקשורת SSL/TLS (שכבת שקעים מאובטחים/בטחון שכבת העברה) אל הסורק, תוכל להצפין את נתיב התקשורת בין מחשבים. עשה זאת אם ברצונך למנוע גישה בלתי מורשית.

אודות אישורים דיגיטליים

❏ אישור חתום בידי רשות אישורים

את האישור החתום בידי רשות האישורים חובה לקבל מרשות האישורים. תוכל לאפשר תקשורת מאובטחת באמצעות שימוש באישור חתום בידי רשות אישורים. תוכל להשתמש באישור החתום בידי רשות אישורים עבור כל תכונת אבטחה.

❏ אישור של רשות אישורים

אישור של רשות אישורים מעיד על כך שגורם צד שלישי אישר את זהות השרת. זהו מרכיב מרכזי בביטחון מסוג רשת-של-אמון (web-of-trust). עליך להשיג אישור של רשות אישורים לאימות שרת מרשות האישורים המנפיקה אותו.

❏ אישור בחתימה עצמית

אישור בחתימה עצמית הוא אישור שהסורק מנפיק וחותם עליו בעצמו. אישור זה אינו מהימן ואינו יכול למנוע זיופים. אם אתה משתמש באישור זהה לאישור SSL/TLS, ייתכן שתוצג התראת אבטחה בדפדפן. תוכל להשתמש באישור זה אך ורק לתקשורת SSL/TLS.

מידע קשור

➡ "השגה וייבוא של אישור החתום על-ידי ר"מ" בעמוד 64
➡ "מחיקת אישור החתום בידי רשות אישורים" בעמוד 68
➡ "עדכון אישור בחתימה עצמית" בעמוד 68

השגה וייבוא של אישור החתום על-ידי ר"מ

השגת אישור החתום בידי רשות אישורים

כדי להשיג אישור החתום בידי רשות אישורים יש ליצור CSR (בקשת חתימה על אישור) ולשלוח אותה אל רשות האישורים. תוכל ליצור CSR באמצעות Web Config ומחשב.

פעל על פי ההוראות ליצירת CSR והשגת אישור חתום בידי רשות אישורים באמצעות Web Config. בעת יצירת CSR תוך שימוש ב-Web Config, האישור הוא תבנית PEM/DER.

1. גש אל Web Config, ולאחר מכן בחר **Network Security Settings**. בשלב הבא, בחר **SSL/TLS** > **Certificate** או **IPsec/IP Filtering** > **Client Certificate** או **IEEE802.1X** > **Client Certificate**.

2. לחץ על **Generate** של CSR.

   דף יצירת CSR ייפתח.

3. הזן ערך עבור כל פריט.

   לתשומת לבך:
   אורך המפתח הזמין והקיצורים ישתנה בהתאם לרשות האישורים. צור בקשה בהתאם לכללים של כל רשות אישורים.

4. לחץ על **OK**.

   מוצגת הודעת סיום.

5. בחר **Network Security Settings**. בשלב הבא, בחר **SSL/TLS** > **Certificate**, או **IPsec/IP Filtering** > **Client Certificate** או **IEEE802.1X** > **Client Certificate**.

6. לחץ על אחד מלחצני ההורדה של CSR בהתאם לתבנית המצוינת בידי כל אחת מרשות האישורים להורדת CSR למחשב.

> **חשוב:**
> *אל תייצר CSR שוב. אם תעשה זאת, ייתכן שלא תוכל לייבא אישור מונפק מסוג CA-signed Certificate.*

7. שלח את ה-CSR לרשות אישורים וקבל CA-signed Certificate.

   פעל על פי הכללים של כל רשות אישורים בנוגע לשיטת שליחה וטופס.

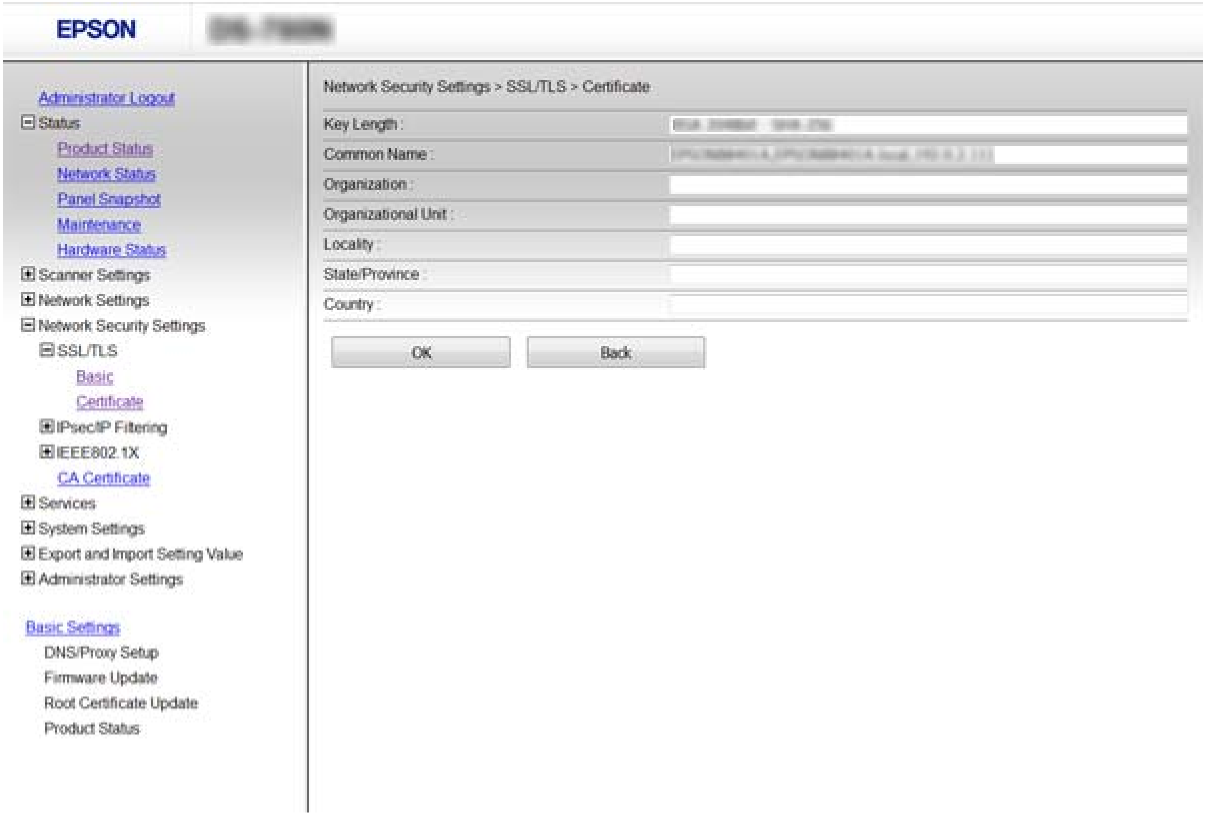
8. שמור את האישור המונפק מסוג CA-signed Certificate במחשב שמחובר לסורק.

   השגת אישור מסוג CA-signed Certificate תושלם לאחר שתשמור את האישור ביעדו.

מידע קשור

← "גישה אל Web Config" בעמוד 23
← "פריטי הגדרת CSR" בעמוד 65
← "ייבוא אישור החתום בידי רשות אישורים" בעמוד 66

פריטי הגדרת CSR



פריטים	הגדרות והסבר
Key Length	בחר אורך מפתח ל-CSR.
Common Name	תוכל להזין בין 1 ל-128 תווים. אם זו כתובת IP, עליה להיות כתובת IP סטטית. לדוגמה: קישור לגישה ל-Web Config: https://10.152.12.225 שם משותף: 10.152.12.225
Organization/Organizational Unit/Locality/State/Province	תוכל להזין בין 0 ל-64 תווים ב-ASCII (0x20–0x7E). תוכל להפריד בין שמות ייחודיים באמצעות פסיק.
Country	הזן קוד מדינה בשתי ספרות המצוין ב-ISO-3166.

מידע קשור

➡ "השגת אישור החתום בידי רשות אישורים" בעמוד 64

ייבוא אישור החתום בידי רשות אישורים

> **חשוב:**
>
> ❏ *ודא שהתאריך והשעה בסורק מוגדרים כהלכה.*
>
> ❏ *אם אתה מקבל אישור באמצעות CSR הנוצר מ-Web Config, תוכל לייבא את האישור פעם אחת.*

1. גש אל Web Config ולאחר מכן בחר **Network Security Settings**. בשלב הבא, בחר **SSL/TLS** < **Certificate**, או **IPsec/IP Filtering** < **Client Certificate** או **IEEE802.1X** < **Client Certificate**.

2. לחץ על **Import**.

   יוצג לך דף ייבוא אישור.

3. הזן ערך עבור כל פריט.

   ההגדרות הנדרשות משתנות לפי המקום שבו יצרת את ה-CSR ותבנית הקובץ של האישור. הזן ערכים לפריטים הנדרשים בהתאם למידע להלן.

   ❏ אישור של תבנית PEM/DER שהתקבל מ-Web Config

   ❏ **Private Key**: אל תגדיר משום שהסורק מכיל מפתח פרטי.

   ❏ **Password**: אל תגדיר.

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

   ❏ אישור בתבנית PEM/DER שהתקבל ממחשב

   ❏ **Private Key**: עליך להגדיר.

   ❏ **Password**: אל תגדיר.

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

   ❏ אישור בתבנית PKCS#12 שהתקבל ממחשב

   ❏ **Private Key**: אל תגדיר.

   ❏ **Password**: אופציונלי

   ❏ **CA Certificate 1**/**CA Certificate 2**: אל תגדיר.

4. לחץ על **OK**.

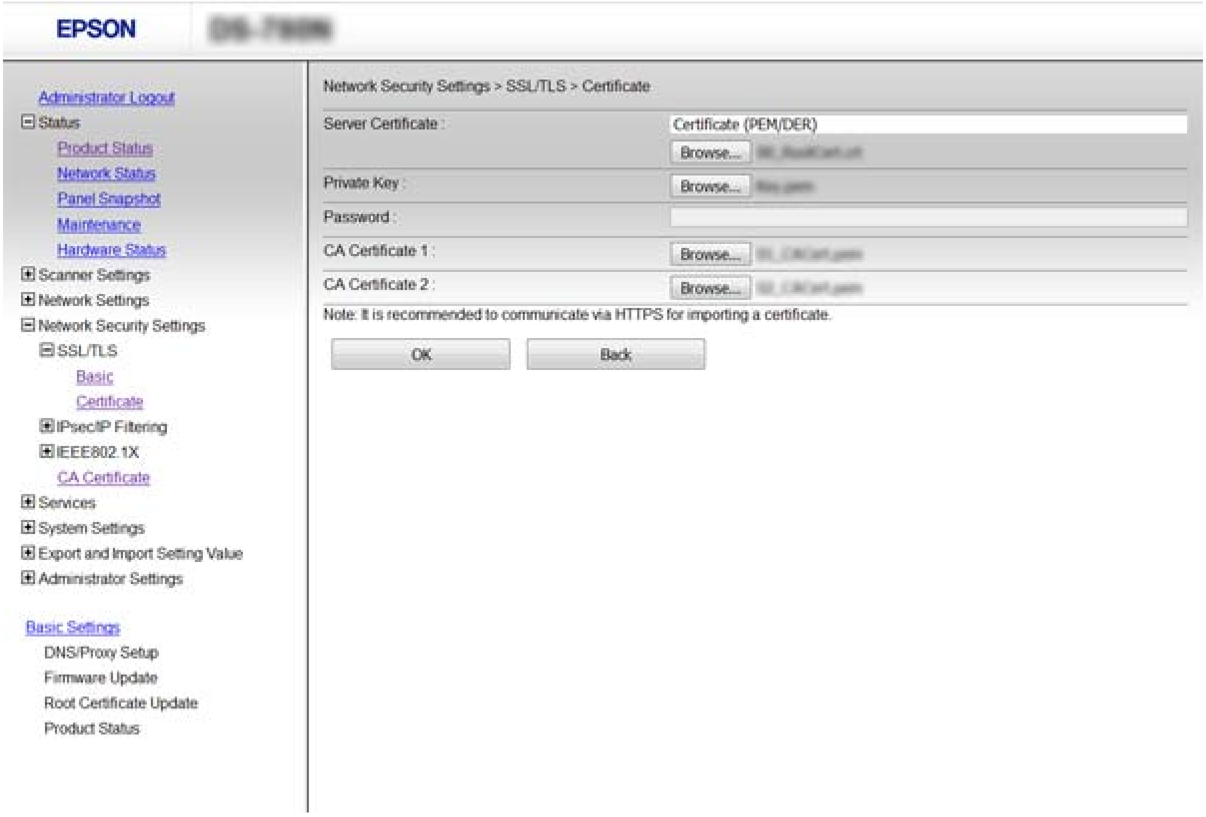
   מוצגת הודעת סיום.

לתשומת לבך:
לחץ על Confirm כדי לאמת את נתוני האישור.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23
➡ "ייבוא פריטי הגדרות באישור החתום בידי רשות אישורים" בעמוד 67

ייבוא פריטי הגדרות באישור החתום בידי רשות אישורים



פריטים	הגדרות והסבר
Server Certificate או Client Certificate	בחר תבנית לאישור.
Private Key	אם אתה מקבל אישור בתבנית PEM/DER באמצעות CSR שנוצר ממחשב, ציין קובץ מפתח פרטי שתואם את האישור.
Password	הזן סיסמה כדי להצפין מפתח פרטי.
CA Certificate 1	אם תבנית האישור היא Certificate (PEM/DER), ייבא אישור מרשות מאשרת המנפיקה אישור שרת. ציין קובץ אם יש בכך הצורך.
CA Certificate 2	אם תבנית האישור היא Certificate (PEM/DER), ייבא אישור מרשות מאשרת המנפיקה CA Certificate 1. ציין קובץ אם יש בכך הצורך.

מידע קשור

➡ "ייבוא אישור החתום בידי רשות אישורים" בעמוד 66

מחיקת אישור החתום בידי רשות אישורים

תוכל למחוק אישור מיובא לאחר שתוקף האישור יפוג או אם כבר אין צורך בחיבור מוצפן.

> **חשוב:**
>
> *אם אתה מקבל אישור באמצעות CSR הנוצר מ-Web Config, אינך צריך לייבא את האישור שוב. במקרה כזה, צור CSR וקבל את האישור שוב.*

1. גש אל Web Config ולאחר מכן בחר **Network Security Settings**. בשלב הבא, בחר **SSL/TLS** > **Certificate**, או **IPsec/IP Filtering** > **Client Certificate** או **IEEE802.1X** > **Client Certificate**.

2. לחץ על **Delete**.

3. אשר שברצונך למחוק את האישור בהודעה המוצגת לפניך.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

עדכון אישור בחתימה עצמית

אם הסורק תומך בתכונת שרת HTTPS, תוכל לעדכן אישור בחתימה עצמית. בגישה ל-Web Config באמצעות אישור בחתימה עצמית, תופיע הודעת אזהרה.

השתמש באישור בחתימה עצמית באופן זמני עד שתשיג ותייבא אישור חתום בידי רשות אישורים.

1. גש אל Web Config ובחר **Network Security Settings** > **SSL/TLS** > **Certificate**.

2. לחץ על **Update**.

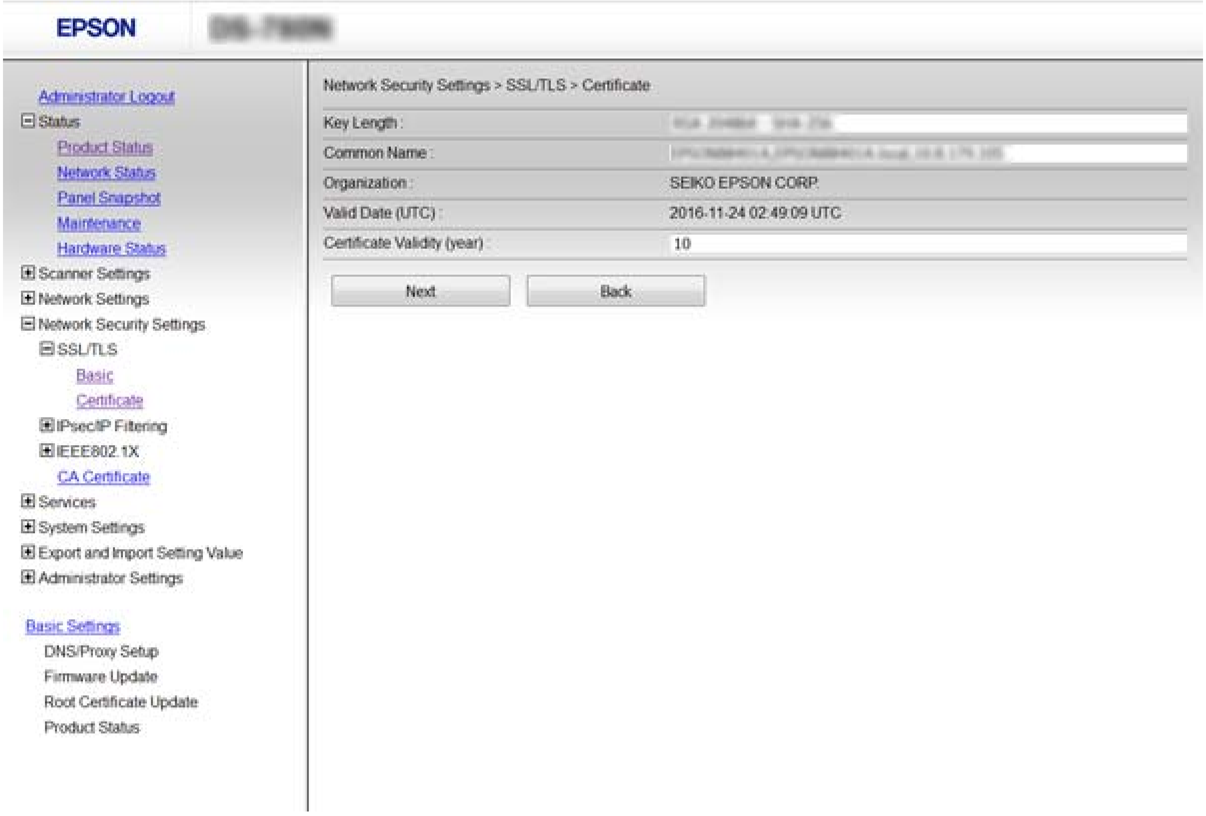
3. הזן **Common Name**.

   הזן כתובת IP או מזהה אחר כגון שם FQDN עבור הסורק. תוכל להזין בין 1 ל-128 תווים.

   לתשומת לבך:

   תוכל להפריד בין שמות ייחודיים (CN) עם פסיקים.

4. ציין תוקף עבור האישור.



5. לחץ על **Next**.

כעת תוצג הודעת אישור.

6. לחץ על **OK**.

הסורק מעודכן.

לתשומת לבך:
*לחץ על **Confirm** כדי לאמת את נתוני האישור.*

מידע קשור

➔ "גישה אל Web Config" בעמוד 23

הגדר CA Certificate

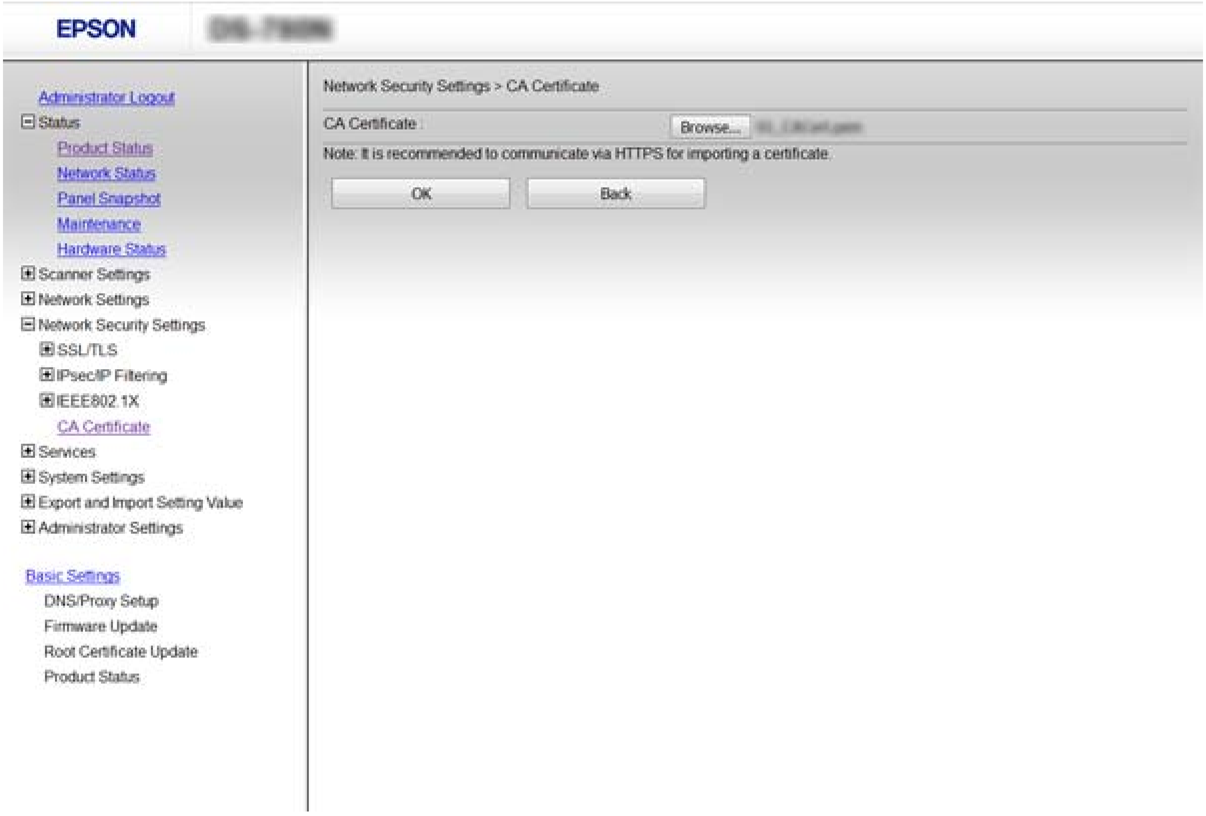
באפשרותך לייבא, להציג ולמחוק CA Certificate.

ייבוא CA Certificate

1. גש אל Web Config, ולאחר מכן בחר **Network Security Settings** < **CA Certificate**.

2. לחץ על **Import**.

3. ציין מהו ה- CA Certificate שברצונך לייבא.



4. לחץ על **OK**.

בגמר הייבוא, המערכת מחזירה אותך אל מסך **CA Certificate**, ואישור ה- CA Certificate שייבאת מוצג בתצוגה.

מידע קשור

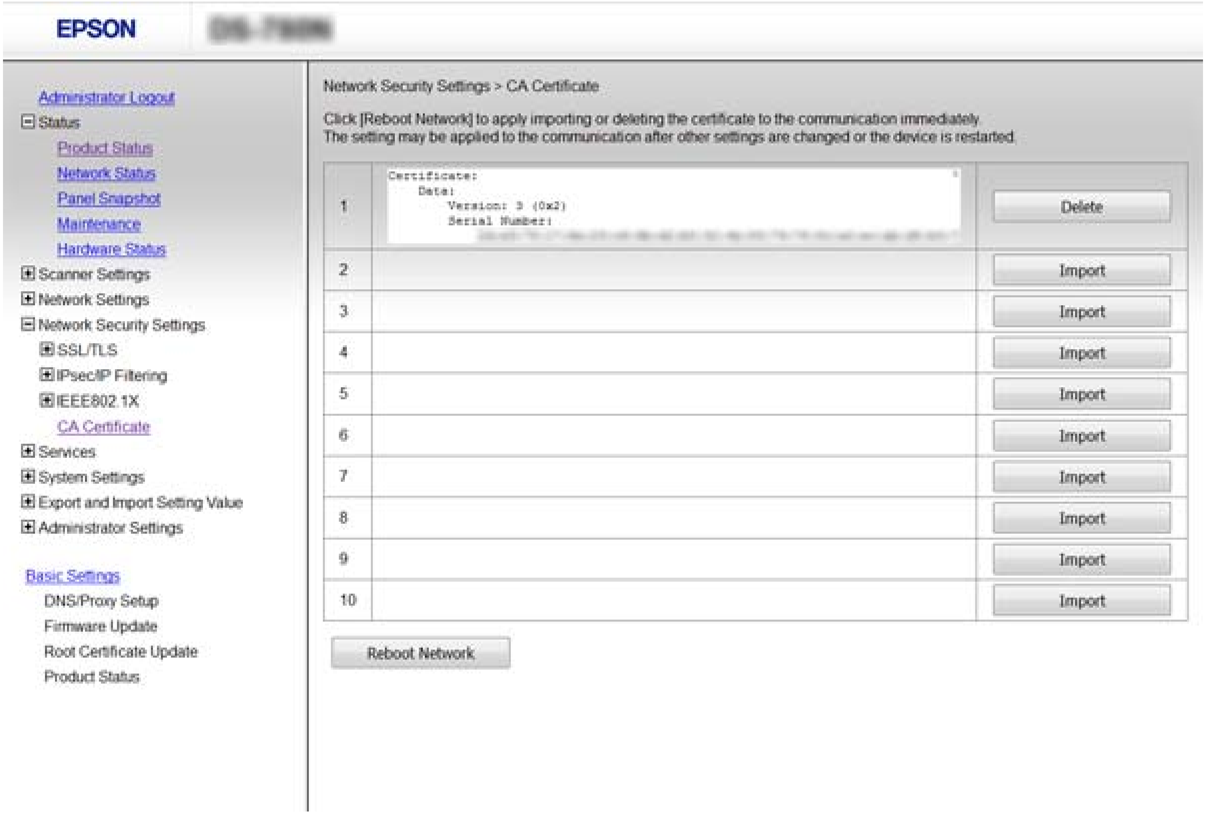
← "גישה אל Web Config" בעמוד 23

מחיקת CA Certificate

באפשרותך למחוק את ה- CA Certificate המיובא.

1. גש אל Web Config, ולאחר מכן בחר **Network Security Settings** < **CA Certificate**.

2. לחץ על **Delete** לצד ה- CA Certificate שברצונך למחוק.



3. אשר שברצונך למחוק את האישור בהודעה המוצגת לפניך.

מידע קשור

← "גישה אל Web Config" בעמוד 23

תקשורת מוצפנת באמצעות IPsec/סינון IP

אודות IPsec/IP Filtering

אם הסורק תומך בסינון IPsec/IP, תוכל לסנן תעבורת נתונים בהתבסס על כתובות IP, שירותים ויציאה. תוכל לשלב את הסינונים ולהגדיר את הסורק לאפשר או לחסום לקוחות ספציפיים או מידע ספציפי. תוכל גם לשפר את רמת האבטחה באמצעות שימוש ב-IPsec.

כדי לסנן תעבורה, שנה את הגדרות מדיניות ברירת המחדל. מדיניות ברירת המחדל חלה על כל משתמש או קבוצה המתחברים אל הסורק. לבקרה פרטנית יותר על משתמשים או קבוצות של משתמשים, שנה את הגדרות מדיניות הקבוצות. מדיניות קבוצות היא כלל אחד או יותר החל על משתמש או קבוצת משתמשים. הסורק שולט במנות IP התואמות למדיניות מוגדרות. מנות IP מאומתות בסדר מדיניות קבוצה 1 עד 10 ואז על פי מדיניות ברירת מחדל.

לתשומת לבך:

מחשבים עם מערכת ההפעלה Windows Vista או מערכת הפעלה מתקדמת יותר, או Windows Server 2008 או מערכת הפעלה מתקדמת יותר, תומכים ב-IPsec.

הגדרת Default Policy

1. גש אל Web Config ובחר Network Security Settings < IPsec/IP Filtering < Basic.
2. הזן ערך עבור כל פריט.
3. לחץ על **Next**.

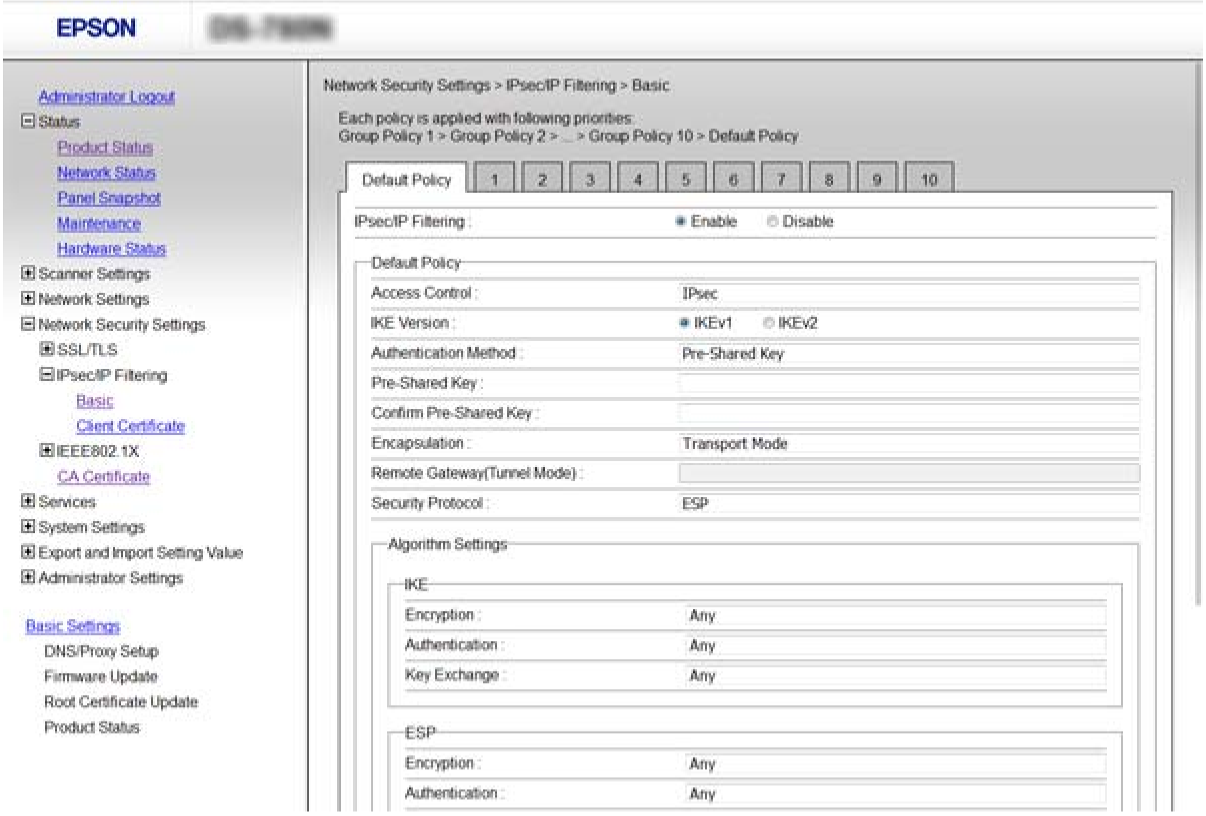
   כעת תוצג הודעת אישור.
4. לחץ על **OK**.

   הסורק מעודכן.

מידע קשור

➜ "גישה אל Web Config" בעמוד 23
➜ "פריטי הגדרת Default Policy" בעמוד 72

פריטי הגדרת Default Policy



פריטים	הגדרות והסבר
IPsec/IP Filtering	תוכל להפעיל או להשבית תכונת סינון IPsec/IP.

הגדרות אבטחה מתקדמות עבור ארגון

פריטים		הגדרות והסבר
Access Control		הגדר שיטת בקרה לתנועת מנות IP.
	Permit Access	בחר באפשרות זו כדי לאפשר מעבר של מנות IP ספציפיות.
	Refuse Access	בחר באפשרות זו כדי למנוע מעבר של מנות IP ספציפיות.
	IPsec	בחר באפשרות זו כדי לאפשר מעבר של מנות IPsec ספציפיות.
IKE Version		בחר IKEv1 או IKEv2 עבור גרסת IKE. בחר אחד מהם בהתאם להתקן אליו מחובר הסורק.
IKEv1		הפריטים הבאים מוצגים כאשר אתה בוחר **IKEv1** עבור **IKE Version**.
	Authentication Method	על מנת לבחור **Certificate**, עליך להשיג או לייבא אישור חתום מראש בידי רשות אישורים.
	Pre-Shared Key	אם בחרת באפשרות **Pre-Shared Key** עבור **Authentication Method**, הזן מפתח ששותף מראש באורך 1–127 תווים.
	Confirm Pre-Shared Key	הזן את המפתח שהגדרת לאישור.
IKEv2		הפריטים הבאים מוצגים כאשר אתה בוחר **IKEv2** עבור **IKE Version**.

הגדרות אבטחה מתקדמות עבור ארגון

פריטים		הגדרות והסבר
Local	Authentication Method	על מנת לבחור **Certificate**, עליך להשיג או לייבא אישור חתום מראש בידי רשות אישורים.
	ID Type	בחר את סוג הזהות של הסורק.
	ID	הזן את מספר הזהות של הסורק התואם לסוג מספר הזהות. לא תוכל להשתמש ב- "@", "#", ו- "=" כתו הראשון. **Distinguished Name**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "=". **IP Address**: הזן פורמט IPv4 או IPv6. **FQDN**: הזן שילוב מתוך 1 עד 255 תווים תוך שימוש ב- A–Z, a–z, 0–9, "-" ונקודה (.). **Email Address**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "@". **Key ID**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E).
	Pre-Shared Key	אם בחרת באפשרות **Pre-Shared Key** עבור **Authentication Method**, הזן מפתח ששותף מראש באורך 1–127 תווים.
	Confirm Pre-Shared Key	הזן את המפתח שהגדרת לאישור.

הגדרות אבטחה מתקדמות עבור ארגון

פריטים	הגדרות והסבר	
Remote	Authentication Method	על מנת לבחור **Certificate**, עליך להשיג או לייבא אישור חתום מראש בידי רשות אישורים.
	ID Type	בחר את סוג הזהות עבור ההתקן שברצונך לאמת.
	ID	הזן את מספר הזהות של הסורק התואם לסוג מספר הזהות. לא תוכל להשתמש ב- "@", "#", ו- "=" כתו הראשון. **Distinguished Name**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "=". **IP Address**: הזן פורמט IPv4 או IPv6. **FQDN**: הזן שילוב מתוך 1 עד 255 תווים תוך שימוש ב- A–Z, a–z, 0–9, "-" ונקודה (.). **Email Address**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "@". **Key ID**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E).
	Pre-Shared Key	אם בחרת באפשרות **Pre-Shared Key** עבור **Authentication Method**, הזן מפתח ששותף מראש באורך 1–127 תווים.
	Confirm Pre-Shared Key	הזן את המפתח שהגדרת לאישור.
Encapsulation	אם אתה בוחר **IPsec** עבור **Access Control**, עליך להגדיר מצב עטיפת נתונים.	
	Transport Mode	אם אתה משתמש בסורק רק באותה רשת LAN, בחר באפשרות זו. מנות IP משכבה 4 ומעלה הן מוצפנות.
	Tunnel Mode	אם אתה משתמש בסורק ברשת עם תמיכה באינטרנט כגון IPsec-VPN, בחר באפשרות זו. הכותרת והנתונים של מנות ה-IP הם מוצפנים.
Remote Gateway(Tunnel Mode)	אם בחרת באפשרות **Tunnel Mode** עבור **Encapsulation**, הזן כתובת שער באורך 1–39 תווים.	
Security Protocol	**IPsec** עבור **Access Control**, בחר אפשרות.	
	ESP	בחר באפשרות זו כדי להבטיח תקינות של אימות ומידע, וכדי להצפין נתונים.
	AH	בחר באפשרות זו כדי להבטיח תקינות של אימות ומידע. תוכל להשתמש ב-IPsec גם אם נאסר על הצפנת נתונים.
Algorithm Settings		

פריטים	הגדרות והסבר	
IKE	Encryption	בחר את אלוגריתם ההצפנה עבור IKE. הפריטים משתנים בהתאם לגרסת ה-IKE.
	Authentication	בחר את אלוגריתם האימות עבור IKE.
	Key Exchange	בחר את אלוגריתם החלפת המפתחות עבור IKE. הפריטים משתנים בהתאם לגרסת ה-IKE.
ESP	Encryption	בחר את אלוגריתם ההצפנה עבור ESP. אפשרות זו זמינה כאשר **ESP** נבחר כ-**Security Protocol**.
	Authentication	בחר את אלוגריתם האימות עבור ESP. אפשרות זו זמינה כאשר **ESP** נבחר כ-**Security Protocol**.
AH	Authentication	בחר את אלוגריתם ההצפנה עבור AH. אפשרות זו זמינה כאשר **AH** נבחר כ-**Security Protocol**.

מידע קשור

➡ "הגדרת Default Policy" בעמוד 72

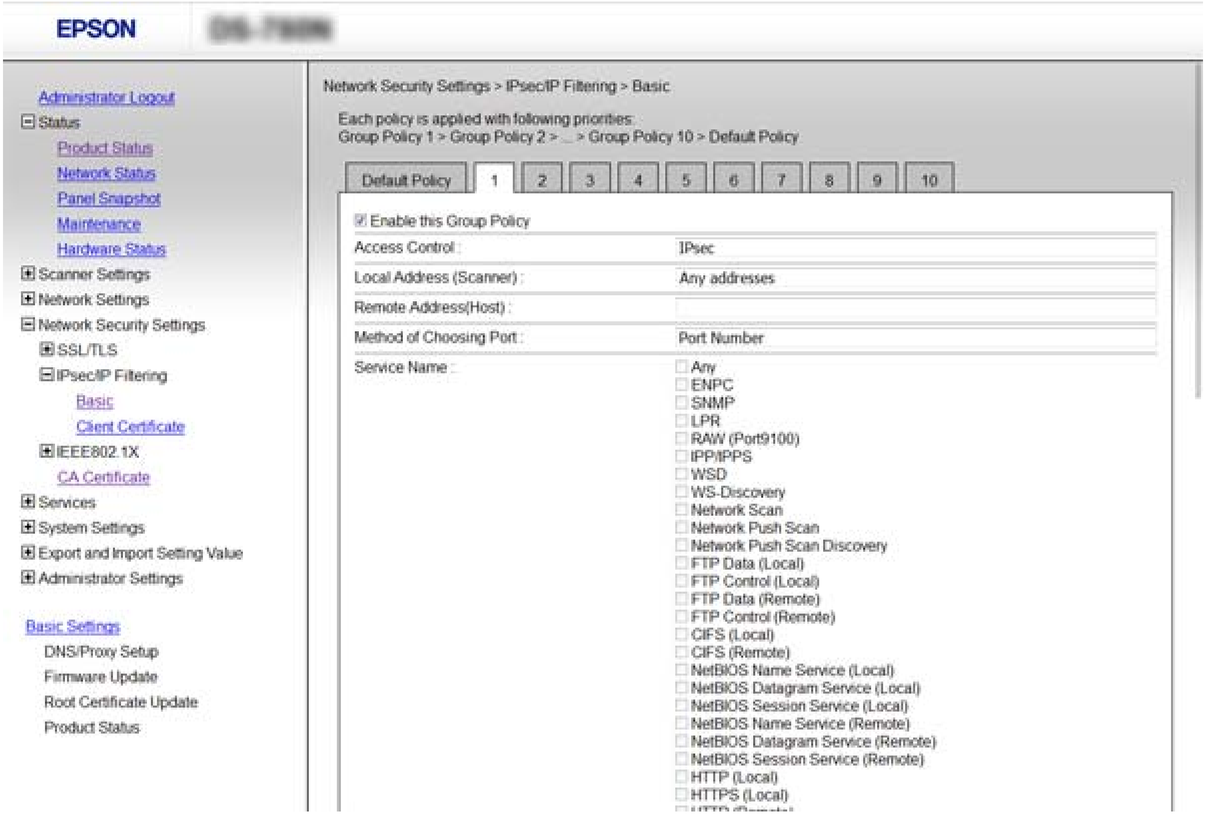
הגדרת Group Policy

1. גש אל Web Config ובחר **Network Security Settings** > **IPsec/IP Filtering** > **Basic**.
2. לחץ על כרטיסייה ממוספרת שאותה תרצה להגדיר.
3. הזן ערך עבור כל פריט.
4. לחץ על **Next**.
   כעת תוצג הודעת אישור.
5. לחץ על **OK**.
   הסורק מעודכן.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23
➡ "פריטי הגדרת Group Policy" בעמוד 77

פריטי הגדרת Group Policy



פריטים	הגדרות והסבר	
Enable this Group Policy	תוכל להפוך מדיניות קבוצה לזמינה או ללא זמינה.	
Access Control	הגדר שיטת בקרה לתנועת מנות IP.	
	Permit Access	בחר באפשרות זו כדי לאפשר מעבר של מנות IP ספציפיות.
	Refuse Access	בחר באפשרות זו כדי למנוע מעבר של מנות IP ספציפיות.
	IPsec	בחר באפשרות זו כדי לאפשר מעבר של מנות IPsec ספציפיות.
Local Address (Scanner)	בחר בכתובת IPv4 או בכתובת IPv6 התואמת את סביבת הרשת שלך. אם הוקצתה כתובת IP באופן אוטומטי, תוכל לבחור **Use auto-obtained IPv4 address**.	
Remote Address(Host)	הזן כתובת IP של התקן כדי לשלוט בגישה. כתובת ה-IP להיות בת 43 תווים או פחות. אם לא תזין כתובת IP, כל הכתובות יהיו בבקרה. ***לתשומת לבך:*** *אם הוקצתה כתובת IP באופן אוטומטי (למשל הוקצתה בידי DHCP), ייתכן שהחיבור לא יהיה זמין. הגדר כתובת IP סטטית.*	
Method of Choosing Port	בחר בשיטה לציון יציאות.	

הגדרות אבטחה מתקדמות עבור ארגון

פריטים		הגדרות והסבר
Service Name		אם אתה בוחר **Service Name** עבור **Method of Choosing Port**, בחר באחת מהאפשרויות.
Transport Protocol		אם אתה בוחר **Port Number** עבור **Method of Choosing Port**, עליך להגדיר מצב עטיפת נתונים.
	Any Protocol	בחר באפשרות זו כדי לשלוט בכל סוגי הפרוטוקולים.
	TCP	בחר באפשרות זו כדי לשלוט בנתוני שידור ליעד בודד (unicast).
	UDP	בחר באפשרות זו כדי לשלוט בנתוני שידור (broadcast) ושידור לקבוצה (multicast).
	ICMPv4	בחר באפשרות זו כדי לשלוט בפקודה ping.
Local Port		אם בחרת באפשרות **Port Number** עבור **Method of Choosing Port** ואם אתה בוחר **TCP** או **UDP** עבור **Transport Protocol**, הזן מספרי יציאה כדי לשלוט במנות שמתקבלות, ולהפריד ביניהם בפסיקים. תוכל להזין עד 10 מספרי יציאות. לדוגמה: 20, 80, 119, 5220 אם לא תזין מספר יציאה, כל היציאות תהיינה בבקרה.
Remote Port		אם בחרת באפשרות **Port Number** עבור **Method of Choosing Port** ואם אתה בוחר **TCP** או **UDP** עבור **Transport Protocol**, הזן מספרי יציאה כדי לשלוט במנות שנשלחות, ולהפריד ביניהם בפסיקים. תוכל להזין עד 10 מספרי יציאות. לדוגמה: 25, 80, 143, 5220 אם לא תזין מספר יציאה, כל היציאות תהיינה בבקרה.
IKE Version		בחר IKEv1 או IKEv2 עבור גרסת IKE. בחר אחד מהם בהתאם להתקן אליו מחובר הסורק.
IKEv1		הפריטים הבאים מוצגים כאשר אתה בוחר **IKEv1** עבור **IKE Version**.
	Authentication Method	אם אתה בוחר **IPsec** עבור **Access Control**, בחר באחת מהאפשרויות. אישור משומש הוא שכיח במדיניות שהיא ברירת מחדל.
	Pre-Shared Key	אם בחרת באפשרות **Pre-Shared Key** עבור **Authentication Method**, הזן מפתח ששותף מראש באורך 1–127 תווים.
	Confirm Pre-Shared Key	הזן את המפתח שהגדרת לאישור.
IKEv2		הפריטים הבאים מוצגים כאשר אתה בוחר **IKEv2** עבור **IKE Version**.

הגדרות אבטחה מתקדמות עבור ארגון

פריטים	הגדרות והסבר	
Local	Authentication Method	אם אתה בוחר **IPsec** עבור **Access Control**, בחר באחת מהאפשרויות. אישור משומש הוא שכיח במדיניות שהיא ברירת מחדל.
	ID Type	בחר את סוג הזהות של הסורק.
	ID	הזן את מספר הזהות של הסורק התואם לסוג מספר הזהות. לא תוכל להשתמש ב- "@", "#", ו- "=" כתו הראשון. **Distinguished Name**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "=". **IP Address**: הזן פורמט IPv4 או IPv6. **FQDN**: הזן שילוב מתוך 1 עד 255 תווים תוך שימוש ב- A–Z, a–z, 0–9, "-" ונקודה (.). **Email Address**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "@". **Key ID**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E).
	Pre-Shared Key	אם בחרת באפשרות **Pre-Shared Key** עבור **Authentication Method**, הזן מפתח ששותף מראש באורך 1–127 תווים.
	Confirm Pre-Shared Key	הזן את המפתח שהגדרת לאישור.

הגדרות אבטחה מתקדמות עבור ארגון

פריטים	הגדרות והסבר	
Remote	Authentication Method	אם אתה בוחר **IPsec** עבור **Access Control**, בחר באחת מהאפשרויות. אישור משומש הוא שכיח במדיניות שהיא ברירת מחדל.
	ID Type	בחר את סוג הזהות עבור ההתקן שברצונך לאמת.
	ID	הזן את מספר הזהות של הסורק התואם לסוג מספר הזהות. לא תוכל להשתמש ב- "@", "#", ו- "=" כתו הראשון. **Distinguished Name**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "=". **IP Address**: הזן פורמט IPv4 או IPv6. **FQDN**: הזן שילוב מתוך 1 עד 255 תווים תוך שימוש ב- A–Z, a–z, 0–9, "-" ונקודה (.). **Email Address**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). עליך לכלול "@". **Key ID**: הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E).
	Pre-Shared Key	אם בחרת באפשרות **Pre-Shared Key** עבור **Authentication Method**, הזן מפתח ששותף מראש באורך 1–127 תווים.
	Confirm Pre-Shared Key	הזן את המפתח שהגדרת לאישור.
Encapsulation	אם אתה בוחר **IPsec** עבור **Access Control**, עליך להגדיר מצב עטיפת נתונים.	
	Transport Mode	אם אתה משתמש בסורק רק באותה רשת LAN, בחר באפשרות זו. מנות IP משכבה 4 ומעלה הן מוצפנות.
	Tunnel Mode	אם אתה משתמש בסורק ברשת עם תמיכה באינטרנט כגון IPsec-VPN, בחר באפשרות זו. הכותרת והנתונים של מנות ה-IP הם מוצפנים.
Remote Gateway(Tunnel Mode)	אם בחרת באפשרות **Tunnel Mode** עבור **Encapsulation**, הזן כתובת שער באורך 1–39 תווים.	
Security Protocol	אם אתה בוחר **IPsec** עבור **Access Control**, בחר באחת מהאפשרויות.	
	ESP	בחר באפשרות זו כדי להבטיח תקינות של אימות ומידע, וכדי להצפין נתונים.
	AH	בחר באפשרות זו כדי להבטיח תקינות של אימות ומידע. תוכל להשתמש ב-IPsec גם אם נאסר על הצפנת נתונים.
Algorithm Settings		

פריטים		הגדרות והסבר
IKE	Encryption	בחר את אלוגריתם ההצפנה עבור IKE. הפריטים משתנים בהתאם לגרסת ה-IKE.
	Authentication	בחר את אלוגריתם האימות עבור IKE.
	Key Exchange	בחר את אלוגריתם החלפת המפתחות עבור IKE. הפריטים משתנים בהתאם לגרסת ה-IKE.
ESP	Encryption	בחר את אלוגריתם ההצפנה עבור ESP. אפשרות זו זמינה כאשר **ESP** נבחר כ-**Security Protocol**.
	Authentication	בחר את אלוגריתם האימות עבור ESP. אפשרות זו זמינה כאשר **ESP** נבחר כ-**Security Protocol**.
AH	Authentication	בחר את אלוגריתם האימות עבור AH. אפשרות זו זמינה כאשר **AH** נבחר כ-**Security Protocol**.

מידע קשור

➡ "הגדרת Group Policy" בעמוד 76
➡ "שילוב Local Address (Scanner) ו-Remote Address(Host) ב-Group Policy" בעמוד 81
➡ "הפניות לשמות שירות במדיניות קבוצה" בעמוד 82

שילוב Local Address (Scanner) ו-Remote Address(Host) ב-Group Policy

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

*1 אם IPsec נבחר עבור **Access Control**, לא תוכל לפרט באורך קידומת.

*2 אם IPsec נבחר עבור **Access Control**, תוכל לבחור כתובת קישור מקומי (fe80::) אך מדיניות הקבוצה תהיה מושבתת.

*3 למעט כתובות קישור מקומי מסוג IPv6.

הפניות לשמות שירות במדיניות קבוצה

לתשומת לבך:
שירותים שאינם זמינים מופיעים בתצוגה אך אי אפשר לבחור אותם.

שם שירות	סוג פרוטוקול	מספר יציאה מקומית	מספר יציאה מרוחקת	תכונות מבוקרות
Any	–	–	–	כל השירותים
ENPC	UDP	3289	כל יציאה	חיפוש אחר סורק מיישומים כגון EpsonNet Config ומנהל התקן הסורק
SNMP	UDP	161	כל יציאה	ייבוא MIB וקביעת התצורה שלו מיישומים כגון EpsonNet Config ומנהל התקן הסורק של Epson
WSD	TCP	כל יציאה	5357	בקרת WSD
WS-Discovery	UDP	3702	כל יציאה	חיפוש סורק מ-WSD
Network Scan	TCP	1865	כל יציאה	העברת נתוני סריקה מ-Document Capture Pro
Network Push Scan Discovery	UDP	2968	כל יציאה	חיפוש מחשב מהסורק.
Network Push Scan	TCP	כל יציאה	2968	ייבוא נתוני עבודה של סריקת דחיפה מ-Document Capture Pro או Document Capture
HTTP (Local)	TCP	80	כל יציאה	שרת HTTP(S) (העברת מידע של Web Config ו-WSD)
HTTPS (Local)	TCP	443	כל יציאה	
HTTP (Remote)	TCP	כל יציאה	80	לקוח HTTP או HTTPS (תקשורת בין עדכון קושחה ועדכון אישור בסיס)
HTTPS (Remote)	TCP	כל יציאה	443	

דוגמאות לתצורת IPsec/IP Filtering

קבלת מנות IPsec בלבד

דוגמה זו מיועדת לקביעת צורת מדיניות ברירת מחדל בלבד.

:Default Policy

- ❏ Enable :IPsec/IP Filtering
- ❏ IPsec :Access Control
- ❏ Pre-Shared Key :Authentication Method
- ❏ Pre-Shared Key: הזן עד 127 תווים.

:Group Policy

אל תגדיר תצורה.

קבלת סריקה באמצעות Epson Scan 2 והגדרות סריקה

בדוגמה זאת מאפשרים העברת נתוני סריקה ותצורת סורקים מתוך שירותים מסוימים.

:Default Policy

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

:Group Policy

- ❏ Enable this Group Policy: סמן תיבה זו.
- ❏ Permit Access :Access Control
- ❏ Remote Address(Host): כתובת IP של לקוח
- ❏ Service Name :Method of Choosing Port
- ❏ Service Name: סמן את התיבות של ENPC, SNMP, Network Scan, HTTP (Local) וכן HTTPS (Local).

קבלת גישה אך ורק מכתובת IP שצוינה

בדוגמה זאת מאפשרים לכתובת IP מסוימת לגשת לסורק.

:Default Policy

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

:Group Policy

- ❏ Enable this Group Policy: סמן תיבה זו.
- ❏ Permit Access :Access Control
- ❏ Remote Address(Host): כתובת IP של לקוח של מנהל מערכת

לתשומת לבך:
הלקוח יוכל לגשת ולשנות את הגדרות הסורק ללא תלות בהגדרת המדיניות.

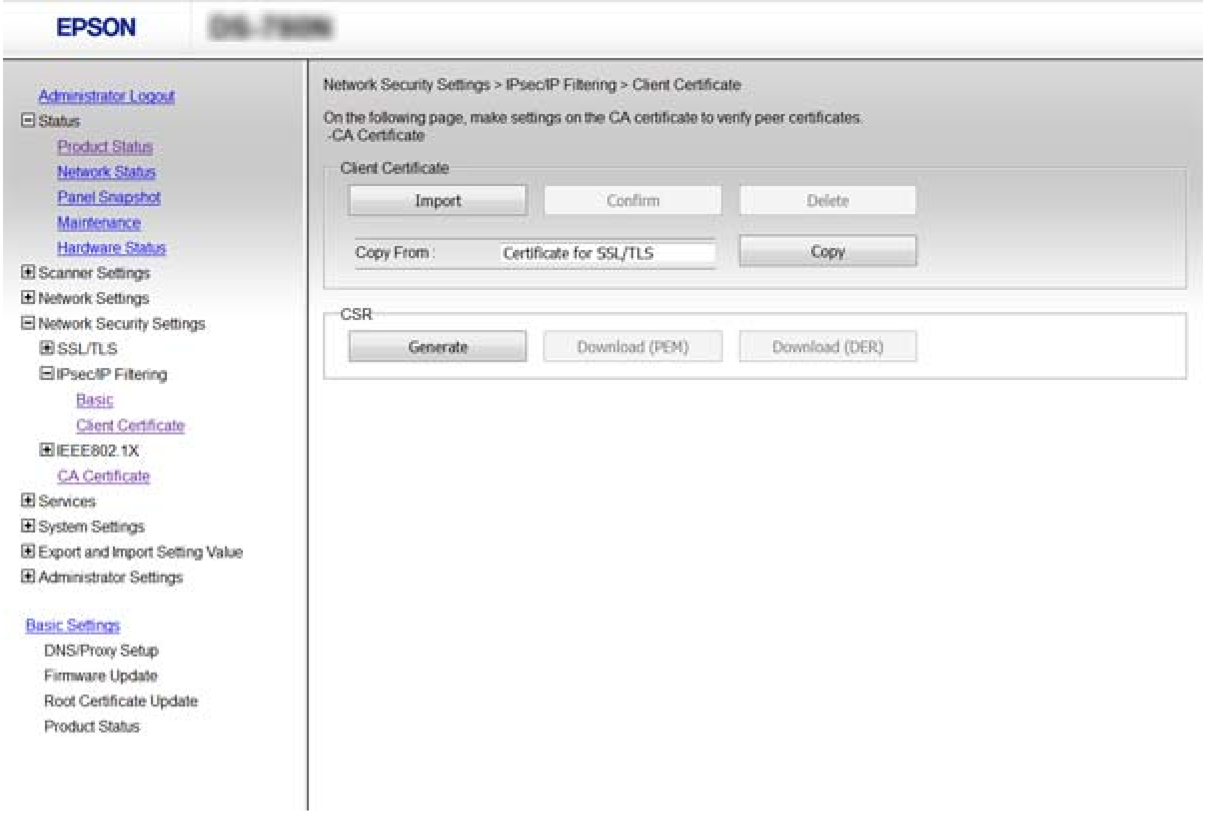
הגדרת אישור עבור IPsec/IP Filtering

קבע את תצורת אישור הלקוח לשם סינון IPsec/IP. אם ברצונך לקבוע את התצורה של הרשות המאשרת, עבור אל CA Certificate.

1. גש אל Web Config ובחר **Network Security Settings** < **IPsec/IP Filtering** < **Client Certificate**.

2. יבא את האישור ב- **Client Certificate**.

   אם כבר ייבאת אישור שפורסם בידי רשות מאשרת ב-IEEE802.1X או ב-SSL/TLS, תוכל להעתיק את האישור ולהשתמש בו בסינון IPsec/IP. כדי להעתיק, בחר את האישור באפשרות **Copy From**, ולאחר מכן לחץ על **Copy**.



מידע קשור

➡ "גישה אל Web Config" בעמוד 23

➡ "השגה וייבוא של אישור החתום על-ידי ר"מ" בעמוד 64

שימוש בפרוטוקול SNMPv3

על אודות SNMPv3

SNMP הוא פרוטוקול שמבצע ניטור ובקרה כדי לאסוף את המידע עבור ההתקנים המחוברים לרשת. SNMPv3 הוא גירסת תכונת אבטחת הניהול ששופרה.

כאשר אתה משתמש ב-SNMPv3, ניתן לאמת ולהצפין את ניטור המצב ואת שינויי ההגדרות בתקשורת SNP (מנה) על מנת להגן על תקשורת ה-SNMP (מנה) מסיכוני רשת, כגון, ציתות, התחזות וטיפול שלא כדין.

הגדרת SNMPv3

אם הסורק תומך בפרוטוקול SNMPv3, תוכל לבקר ולפקח על גישה למדפסת.

1. גש אל Web Config ובחר **Services** < **Protocol** .
2. הזן ערך עבור כל פריט **SNMPv3 Settings**.
3. לחץ על **Next**.

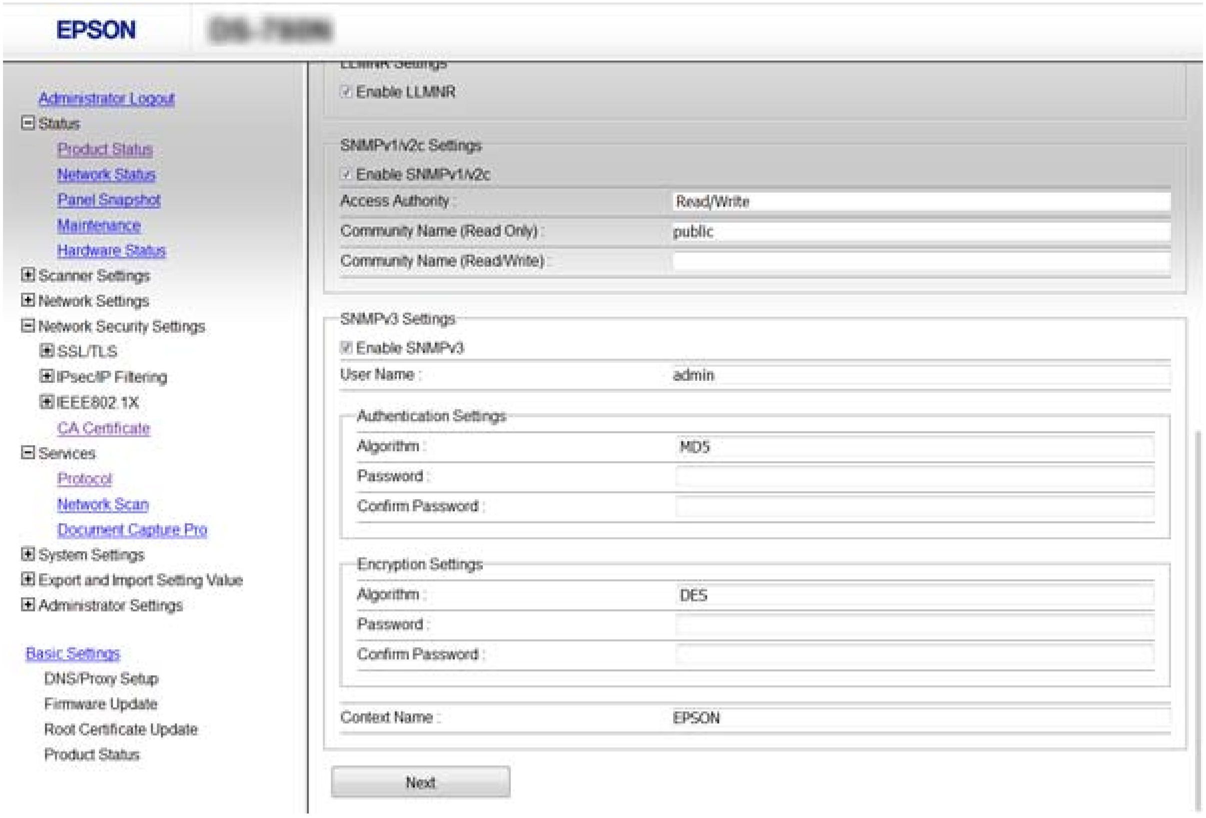
   כעת תוצג הודעת אישור.
4. לחץ על **OK**.

   הסורק מעודכן.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23
➡ "פריטי הגדרת SNMPv3" בעמוד 85

פריטי הגדרת SNMPv3



פריטים	הגדרות והסבר
Enable SNMPv3	SNMPv3 מאופשר כאשר התיבה מסומנת.
User Name	הזן בין 1 ל-32 תווים בשימוש בתווים באורך בייט אחד.
Authentication Settings	
Algorithm	בחר אלגוריתם לאימות.
Password	הזן בין 8 ל-32 תווים ב-ASCII (0x20–0x7E).
Confirm Password	הזן את הסיסמה שהגדרת לאישור.
Encryption Settings	
Algorithm	בחר אלגוריתם להצפנה.
Password	הזן בין 8 ל-32 תווים ב-ASCII (0x20–0x7E).
Confirm Password	הזן את הסיסמה שהגדרת לאישור.
Context Name	הזן בין 1 ל-32 תווים בשימוש בתווים באורך בייט אחד.

מידע קשור

➡ "הגדרת SNMPv3" בעמוד 85

חיבור הסורק לרשת IEEE802.1X

הגדרת תצורה לרשת IEEE802.1X

אם הסורק תומך ב-IEEE802.1X, תוכל להשתמש בסורק ברשת מאומתת המחוברת לשרת RADIUS ולרכזת הפועלת כגורם מאמת.

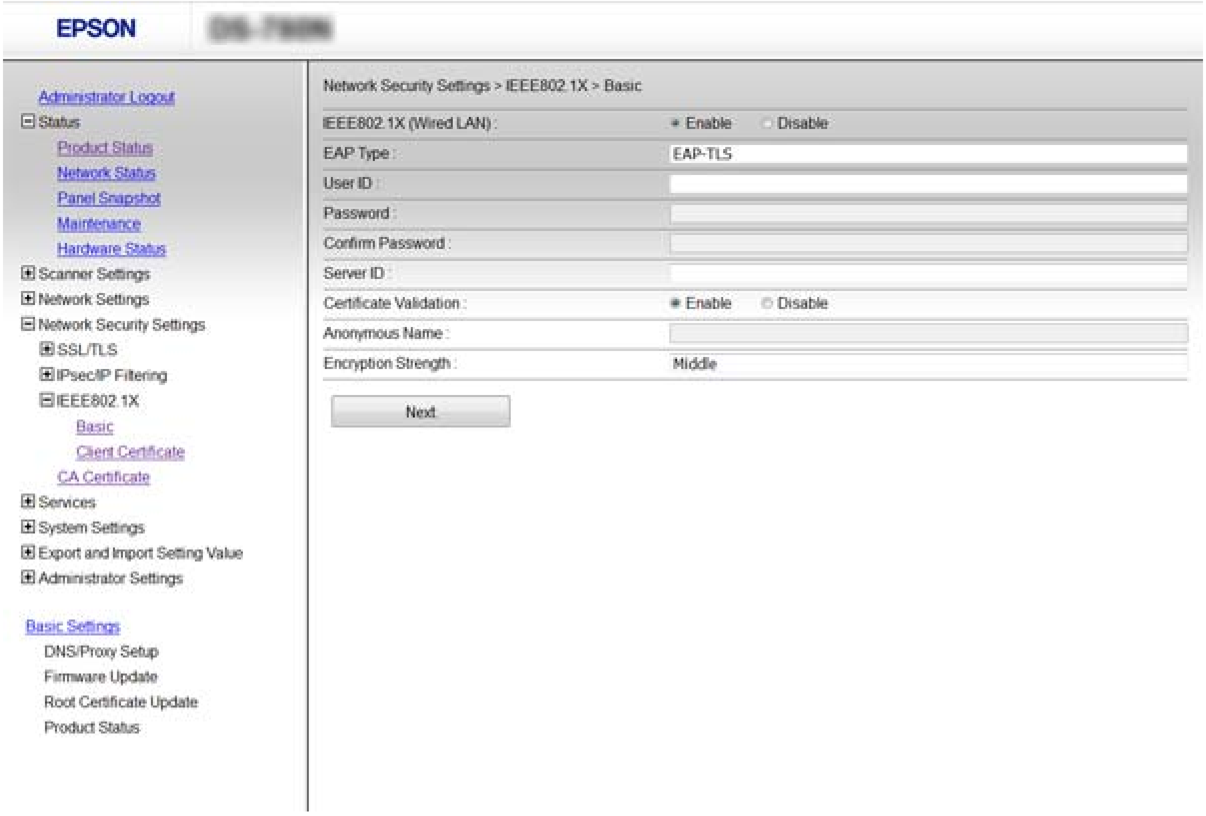
1. גש אל Web Config ובחר **Network Security Settings** > **IEEE802.1X** > **Basic**.
2. הזן ערך עבור כל פריט.
3. לחץ על **Next**.
   כעת תוצג הודעת אישור.
4. לחץ על **OK**.
   הסורק מעודכן.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

← "פריטי הגדרת רשת IEEE802.1X" בעמוד 87
← "אין גישה למדפסת או לסורק לאחר הגדרת תצורת IEEE802.1X" בעמוד 92

פריטי הגדרת רשת IEEE802.1X



פריטים		הגדרות והסבר
IEEE802.1X (Wired LAN)		תוכל להפוך הגדרות לזמינות או ללא זמינות בדף (Basic < IEEE802.1X) עבור IEEE802.1X (LAN קווי).
EAP Type		בחר באפשרות לשיטת אימות בין הסורק לשרת RADIUS.
	EAP-TLS	עליך להשיג ולייבא אישור חתום בידי רשות אישורים.
	PEAP-TLS	
	PEAP/MSCHAPv2	עליך להגדיר סיסמה.
User ID		הגדר מזהה לשימוש עבור אימות שרת RADIUS. הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E).
Password		הגדר סיסמה כדי לאמת את הסורק. הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). אם אתה משתמש בשרת Windows בתור שרת RADIUS, תוכל להזין 127 תווים לכל היותר.
Confirm Password		הזן את הסיסמה שהגדרת לאישור.

הגדרות והסבר		פריטים
תוכל להגדיר מספר זיהוי שרת כדי לאמת באמצעות שרת RADIUS ספציפי. המאמת מוודא אם מזהה השרת מופיע בשדה subject/subjectAltName באישור שרת שנשלח משרת RADIUS או לא. הזן 0 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E).		Server ID
תוכל להגדיר אימות של האישור ללא קשר לשיטת האימות. יבא את האישור ב- **CA Certificate**.		Certificate Validation
אם בחרת באפשרות **PEAP-TLS** או **PEAP/MSCHAPv2** עבור **Authentication Method**, תוכל להגדיר שם אנונימי במקום מספר זיהוי משתמש לשלב 1 של אימות PEAP. הזן 0 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E).		Anonymous Name
תוכל לבחור באחת מהאפשרויות המפורטות להלן.		Encryption Strength
AES256/3DES	High	
AES256/3DES/AES128/RC4	Middle	

מידע קשור

➡ "הגדרת תצורה לרשת IEEE802.1X" בעמוד 86

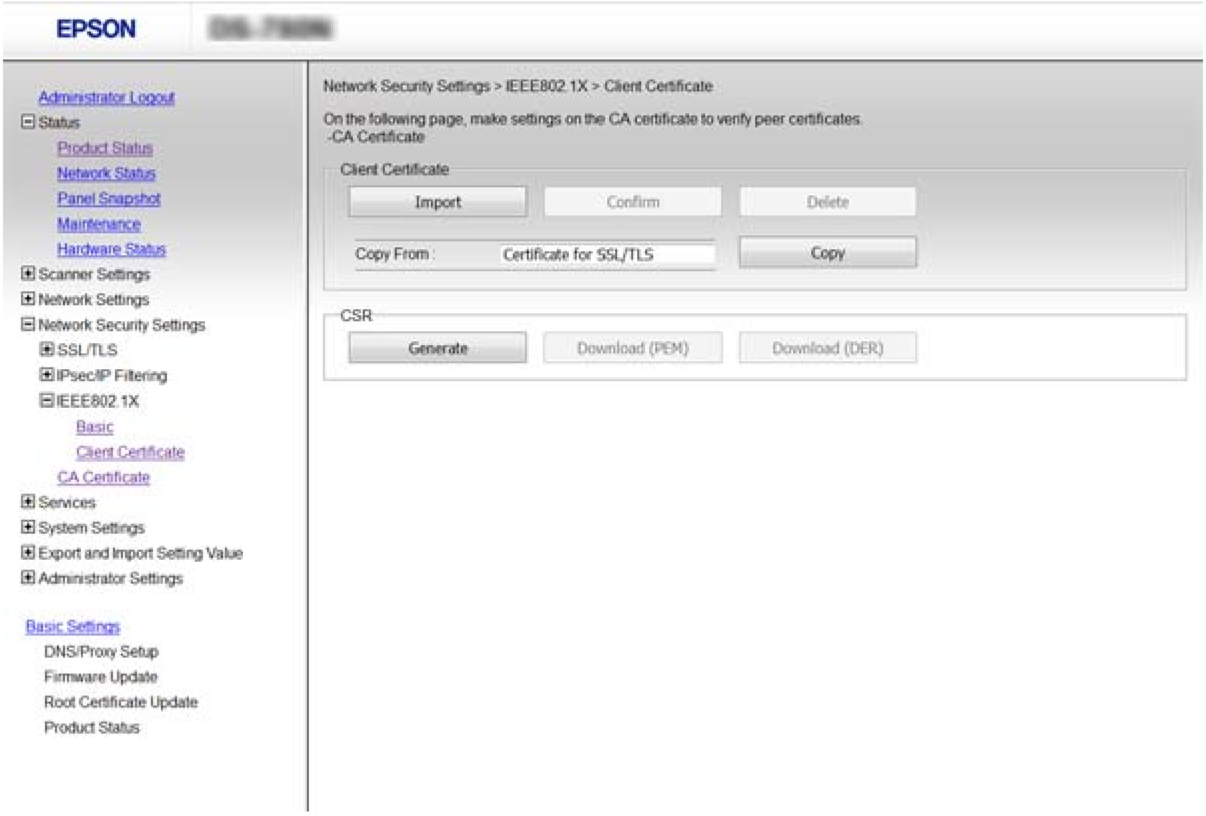
הגדרת אישור עבור IEEE802.1X

הגדר את אישור הלקוח עבור IEEE802.1X. אם ברצונך להגדיר את אישור הרשות המאשרת, עבור אל **CA Certificate**.

1. גש אל Web Config ובחר **Network Security Settings** > **IEEE802.1X** > **Client Certificate**.

2. הזן אישור ב- Client Certificate.

אם האישור פורסם בידי רשות מאשרת תוכל להעתיק אותו. כדי להעתיק, בחר את האישור באפשרות Copy From, ולאחר מכן לחץ על Copy.



מידע קשור

➡ "גישה אל Web Config" בעמוד 23

➡ "השגה וייבוא של אישור החתום על-ידי ר"מ" בעמוד 64

פתירת בעיות עבור אבטחה מתקדמת

שחזור הגדרות האבטחה

כאשר אתה יוצר סביבה בעלת רמת אבטחה גבוהה כגון סינון IPsec/IP או IEEE802.1X, אפשר שלא יהיה ביכולתך ליצור תקשורת עם התקנים כתוצאה מהגדרות שגויות או בעיות עם ההתקן או השרת. במקרה כזה, שחזר את הגדרות האבטחה כדי לבצע שוב את ההגדרות עבור ההתקן או כדי לאפשר לעצמך שימוש זמני.

השבתת פונקציית האבטחה באמצעות לוח הבקרה

תוכל להשבית את סינון IPsec/IP או את IEEE802.1X באמצעות לוח הבקרה של הסורק.

1. הקש הגדרות > הגדרות רשת.

2. הקש שינוי ההגדרות.

3. הקש על הפריטים שברצונך להשבית.
   - ❏ סינון IPsec/IP
   - ❏ IEEE802.1X
4. כאשר מוצגת הודעה על השלמת התהליך, הקש המשך.

שחזור פונקציית האבטחה תוך שימוש ב-Web Config

עבור IEEE802.1X, אפשר שהתקנים לא יזוהו ברשת. במקרה זה, השבת את הפונקציה באמצעות לוח הבקרה של הסורק.

עבור סינון IPsec/IP תוכל להשבית את הפונקציה אם תוכל לגשת להתקן מהמחשב.

השבתת IPsec/ סינון IP באמצעות Web Config

1. גש אל Web Config ובחר **Network Security Settings** < **IPsec/IP Filtering** < **Basic**.
2. בחר **Disable** עבור **IPsec/IP Filtering** בתוך **Default Policy**.
3. לחץ **Next**, ואז נקה את **Enable this Group Policy** עבור כל המדיניויות הקבוצתיות.
4. לחץ על **OK**.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

בעיות בשימוש בתכונות אבטחת רשת

שכחתי מפתח ששותף מראש

הגדר שנית את המפתח באמצעות Web Config.

כדי לשנות את המפתח, גש אל Web Config ובחר **Network Security Settings** < **IPsec/IP Filtering** < **Basic** < **Default Policy** או **Group Policy**.

כאשר אתה משנה את המפתח ששותף-מראש, עליך להגדיר את תצורת המפתח המשותף-מראש עבור מחשבים.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23

לא ניתן לקיים תקשורת באמצעות IPsec

האם אתה משתמש באלגוריתם שלא נתמך עבור הגדרות המחשב?

הסורק תומך באלגוריתמים שלהלן.

שיטות אבטחה	אלגוריתמים
אלגוריתם הצפנה IKE	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128*, AES-GCM-192*, AES-GCM-256*, 3DES
אלגוריתם אימות IKE	SHA-1, SHA-256, SHA-384, SHA-512, MD5
אלגוריתם חילופי מפתחות 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*
אלגוריתם הצפנה ESP	AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128, AES-GCM-192, AES-GCM-256, 3DES
אלגוריתם אימות ESP	SHA-1, SHA-256, SHA-384, SHA-512, MD5
אלגוריתם אימות AH	SHA-1, SHA-256, SHA-384, SHA-512, MD5

* זמין עבור IKEv2 בלבד

מידע קשור

➡ "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 71

התקשורת נקטעת בפתאומיות

האם כתובת ה-IP של הסורק לא חוקית או שהיא השתנתה?

השבת את IPsec באמצעות לוח הבקרה של הסורק.

אם DCHP אינו מעודכן או מופעל מחדש או שכתובת ה-IPv6 אינה בתוקף או לא התקבלה, ייתכן שלא ניתן יהיה למצוא את כתובת ה-IP הרשומה עבור ה- Web Config (Network Security Settings < IPsec/IP Filtering < Basic < Group Policy < Local Address (Scanner)) של הסורק.

השתמש בכתובת IP סטטית.

האם כתובת ה-IP של המחשב לא חוקית או שהיא השתנתה?

השבת את IPsec באמצעות לוח הבקרה של הסורק.

אם DCHP אינו מעודכן או מופעל מחדש או שכתובת ה-IPv6 אינה בתוקף או לא התקבלה, ייתכן שלא ניתן יהיה למצוא את כתובת ה-IP הרשומה עבור ה- Web Config (Network Security Settings < IPsec/IP Filtering < Basic < Group Policy < Remote Address(Host)) של הסורק.

השתמש בכתובת IP סטטית.

מידע קשור

➡ "גישה אל Web Config" בעמוד 23
➡ "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 71

לא ניתן להתחבר אחרי הגדרת סינון IPsec/IP

ייתכן שהערכים המוגדרים שגויים.

השבת את סינון IPsec/IP בלוח הבקרה של הסורק. חבר את הסורק והמחשב ובצע שוב את הגדרות סינון IPsec/IP.

מידע קשור

➡ "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 71

אין גישה למדפסת או לסורק לאחר הגדרות תצורה IEEE802.1X

ייתכן שההגדרות שגויות.

השבת את IEEE802.1X מלוח הבקרה של הסורק. חבר את הסורק למחשב, ואז הגדר שנית את תצורת IEEE802.1X.

מידע קשור

➡ "הגדרת תצורה לרשת IEEE802.1X" בעמוד 86

בעיות במהלך השימוש באישור דיגיטלי

לא ניתן לייבא אישור החתום בידי רשות אישורים

האם האישור החתום בידי רשות אישורים והמידע שב-CSR תואמים?

אם האישור החתום בידי רשות אישורים וה-CSR לא מכילים אותם נתונים, לא ניתן לייבא את ה-CSR. בדוק את הדברים להלן:

- ❏ האם אתה מנסה לייבא אישור להתקן שאין לו אותם הנתונים?
  בדוק את המידע של ה-CSR ולאחר מכן ייבא את האישור להתקן שיש לו אותם הנתונים.
- ❏ האם דרסת את הנתונים השמורים ב-CSR השמור לסורק לאחר שליחת ה-CSR לרשות מאשרת?
  השג שנית את האישור החתום בידי רשות אישורים עם ה-CSR.

האם גודל האישור החתום בידי רשות אישורים עולה על 5 KB?

אינך יכול לייבא אישור חתום בידי רשות אישורים אם גודלו עולה על 5 KB.

האם הסיסמה לייבוא האישור נכונה?

אם שכחת את הסיסמה, לא תוכל לייבא את האישור.

מידע קשור

➡ "ייבוא אישור החתום בידי רשות אישורים" בעמוד 66

לא ניתן לעדכן אישור בחתימה עצמית

האם הוזן Common Name?

יש להזין Common Name.

האם הוזנו תווים שאינם נתמכים בשם ה-Common Name? לדוגמה, יפנית אינה נתמכת.

הזן בין 1 עד 128 תווים תואמי IPv4, IPv6, שם המחשב המארח או בפורמט FQDN ב--ASCII (0x20–0x7E).

האם הוזן רווח או פסיק בשם ה-Common Name?

אם הוזן פסיק, ה-Common Name יהיה מחולק בנקודה זו. אם הוזן רק רווח לפני או אחרי פסיק, הדבר יגרום לשגיאה.

מידע קשור

➡ "עדכון אישור בחתימה עצמית" בעמוד 68

לא ניתן ליצור CSR

האם הוזן Common Name?

יש להזין Common Name.

האם הוזנו תווים שאינם נתמכים בשם ה-Common Name, Organization, Organizational Unit, Locality, State/Province? לדוגמה, יפנית אינה נתמכת.

הזן תווים תואמי IPv4, IPv6, שם המחשב המארח או בפורמט FQDN ב-ASCII (0x20–0x7E).

האם הוזן רווח או פסיק בשם ה-Common Name?

אם הוזן פסיק, ה-Common Name יהיה מחולק בנקודה זו. אם הוזן רק רווח לפני או אחרי פסיק, הדבר יגרום לשגיאה.

מידע קשור

➡ "השגת אישור החתום בידי רשות אישורים" בעמוד 64

הודעות אזהרה הקשורות לאישור דיגיטלי

הודעות	סיבה/מה לעשות
Enter a Server Certificate.	**סיבה:** לא בחרת קובץ לייבוא. **מה לעשות:** בחר קובץ ולאחר מכן לחץ על **Import**.
CA Certificate 1 is not entered.	**סיבה:** אישור של רשות אישורים 1 לא הוזן אלא רק אישור של רשות אישורים 2. **מה לעשות:** תחילה עליך לייבא את אישור של רשות אישורים 1.
Invalid value below.	**סיבה:** נתיב הקובץ והסיסמה מכילים תווים שאינם נתמכים. **מה לעשות:** וודא שהתווים הוזנו כהלכה עבור הפריט.
Invalid date and time.	**סיבה:** לא הוגדרו תאריך ושעה עבור הסורק. **מה לעשות:** הגדר את התאריך ואת השעה באמצעות Web Config או EpsonNet Config.
Invalid password.	**סיבה:** הסיסמה שהוגדרה לאישור רשות האישורים והסיסמה שהוזנה אינן תואמות. **מה לעשות:** הזן את הסיסמה הנכונה.

הגדרות אבטחה מתקדמות עבור ארגון

הודעות	סיבה/מה לעשות
Invalid file.	**סיבה:** אינך מייבא את הקובץ בתבנית X509. **מה לעשות:** וודא שאתה בוחר באישור הנכון שנשלח בידי רשות מאשרת מהימנה.
	סיבה: הקובץ שייבאת גדול מדי. גודל הקובץ המקסימלי הנו 5 KB. **מה לעשות:** אם בחרת בקובץ הנכון, ייתכן שהאישור פגום או מזויף.
	סיבה: השרשרת הכלולה באישור אינה תקינה. **מה לעשות:** למידע נוסף אודות האישור, בקר באתר הרשות המאשרת.
Cannot use the Server Certificates that include more than three CA certificates.	**סיבה:** קובץ האישור בתבנית PKCS#12 מכיל יותר מ-3 אישורי רשות אישורים. **מה לעשות:** ייבא כל אישור תוך המרה מתבנית PKCS#12 לתבנית PEM, או ייבא את קובץ האישור בתבנית PKCS#12 שמכיל עד 2 אישורי רשות אישורים.
The certificate has expired. Check if the certificate is valid, or check the date and time on the product.	**סיבה:** האישור אינו בתוקף. **מה לעשות:** ❏ אם האישור פג תוקף, השג וייבא את האישור החדש. ❏ אם האישור אינו פג תוקף, ודא שהשעה והתאריך מוגדרים כהלכה בסורק.

הודעות	סיבה/מה לעשות
Private key is required.	**סיבה:** אין מפתח פרטי המוצמד לאישור. **מה לעשות:** ❏ אם האישור הוא בתבנית PEM/DER והוא הושג מ-CSR באמצעות מחשב, ציין את קובץ המפתח הפרטי. ❏ אם האישור הוא בתבנית PKCS#12 והוא הושג מ-CSR באמצעות מחשב, צור קובץ שיכיל את המפתח הפרטי.
	סיבה: ייבאת מחדש את אישור ה-PEM/DER שהושג מ-CSR באמצעות Web Config. **מה לעשות:** אם האישור הוא בתבנית PEM/DER והוא הושג מ-CSR באמצעות Web Config, תוכל לייבא אותו רק פעם אחת.
Setup failed.	**סיבה:** לא ניתן לסיים את קביעת התצורה משום שהתקשורת בין הסורק למחשב נכשלה או שלא ניתן לקרוא את הקובץ בגלל שגיאות. **מה לעשות:** לאחר בדיקת הקובץ שצוין והתקשורת, ייבא שוב את הקובץ.

מידע קשור

➡ "אודות אישורים דיגיטליים" בעמוד 63

מחק אישור החתום על-ידי ר"מ בטעות

האם יש קובץ גיבוי לאישור?

אם יש לך קובץ גיבוי, ייבא את האישור שוב.

אם אתה מקבל אישור באמצעות CSR הנוצר מ-Web Config, אינך צריך לייבא את האישור שוב. צור CSR וקבל אישור חדש.

מידע קשור

➡ "מחיקת אישור החתום בידי רשות אישורים" בעמוד 68
➡ "ייבוא אישור החתום בידי רשות אישורים" בעמוד 66