

**DS-790WN**

# מדריך למנהל המערכת

הגדרות הדרושות כדי להתאים למטרתך

הגדרות רשת

הגדרות הדרושות לסריקה

הגדרות אבטחה בסיסיות

הגדרות אבטחה מתקדמות

**Authentication Settings**

# 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 תישאנה 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 לאלו שהוגדרו כמוצרי Epson מאושרים על ידי חברת Seiko Epson.

© Seiko Epson Corporation 2021

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

# סימנים מסחריים

□ EPSON EXCEED YOUR VISION, EPSON EXCEED YOUR VISION, EPSON והלוגואים שלהם הם סימנים מסחריים או סימני מסחר של Seiko Epson.

□ Microsoft®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation.

□ Apple, Mac, macOS, OS X, Bonjour, Safari, and AirPrint are trademarks of Apple Inc., registered in the U.S. and other countries.

□ Chrome is a trademark of Google LLC.

□ The SuperSpeed USB Trident Logo is a registered trademark of USB Implementers Forum, Inc.

□ Firefox is a trademark of the Mozilla Foundation in the U.S. and other countries.

□ FeliCa ו-PaSoRi הם סימנים מסחריים של Sony Corporation.

□ MIFARE היא סימן רשום של חברת NXP Semiconductor Corporation.

□ הערה כללית: שמות מוצרים אחרים הנזכרים כאן נועדו לשם זיהוי בלבד וייתכן שהם יהיו סימנים מסחריים של בעליהם. Epson מתנערת מכל זכות בסימנים אלה.

## תוכן עניינים

### זכויות יוצרים

### סימנים מסחריים

### מבוא

- 7. תוכן מסמך זה.
- 7. שימוש במדריך.
- 7. סימנים וסמלים.
- 7. התיאורים המשמשים במדריך זה.
- 8. אזכורי מערכת הפעלה.

### ההגדרות הדרושות כדי להתאים למטרתך

- 10. ההגדרות הדרושות כדי להתאים למטרתך.

### הגדרות רשת

- 14. חיבור הסורק לרשת.
- 14. לפני ביצוע חיבור רשת.
- 16. התחברות אל הרשת מלוח הבקרה.
- 20. הוספה או החלפה של המחשב או ההתקנים.
- 20. התחברות לסורק שחובר לרשת.
- 20. חיבור ישיר בין התקן חכם לבין סורק (Wi-Fi Direct).
- 22. הגדרה מחדש של חיבור הרשת.
- 24. הגדרה מחדש של חיבור הרשת.
- 26. בדיקת מצב חיבור הרשת.
- 26. בדיקת מצב חיבור הרשת מלוח הבקרה.
- 28. מפרטי רשת.
- 28. מפרט Wi-Fi.
- 29. מפרט Ethernet.
- 30. פונקציות רשת ו-IPv4/IPv6.
- 30. פרוטוקול אבטחה.
- 30. השימוש ביציאה עבור הסורק.
- 32. פתרון בעיות.
- 32. לא ניתן להתחבר לרשת.

### תוכנה להתקנת הסורק

- 36. Web Config.
- 36. הפעלת Web Config בדפדפן אינטרנט.
- 37. הפעלת Web Config ב-Windows.
- 37. Epson Device Admin.
- 37. תבנית תצורה.

### ההגדרות הדרושות לסריקה

- 42. הגדרת שרת דואר.
- 42. פריטי הגדרות שרת דואר.
- 43. בדיקת חיבור לשרת דואר.
- 45. הגדרת תיקיית רשת משותפת.
- 46. יצירת התיקיה המשותפת.
- 61. הפיכת אנשי קשר לזמינים.
- 62. השוואת הגדרות אנשי קשר.
- 62. רישום יעד לאנשי קשר באמצעות Web Config.
- 62. רישום יעדים כקבוצה באמצעות Web Config.
- 64. גיבוי וייבוא של אנשי קשר.
- 65. ייצוא ורישום של אנשי קשר בצובר באמצעות כלי.
- 66. שיתוף פעולה עם שרת ומשתמשי LDAP.
- 68. השימוש ב-Document Capture Pro Server.
- 71. הגדרת מצב שרת.
- 72. הגדרת AirPrint.
- 72. בעיות בעת הכנת סריקת רשת.
- 72. רמזים לפתרון בעיות.
- 73. לא ניתן לגשת אל Web Config.

### התאמה אישית של תצוגת לוח הבקרה

- 76. רישום קבוע מראש.
- 77. אפשרויות תפריט של קבוע מראש.
- 78. עריכת מסך הבית של לוח הבקרה.
- 78. שינוי ה-פריסה של מסך הבית.
- 79. הוסף סמל.
- 80. הסר סמל.
- 81. הזז סמל.

### הגדרות אבטחה בסיסיות

- 84. מבוא למאפייני אבטחת מוצר.
- 84. הגדרות מנהל מערכת.
- 84. הגדרת סיסמת מנהל מערכת.
- 84. השימוש ב-הגדרת נעילה עבור לוח הבקרה.
- 86. כניסה כמנהל מלוח הבקרה.
- 90. השבתת הממשק החיצוני.
- 90. ניטור סורק מרוחק.
- 91. בדיקת מידע עבור סורק מרוחק.

|          |  |
|----------|--|
| 137..... | חיבור התקן אימות.  |
| 138..... | הגדרות התקן אימות.                                       |
| 139..... | רישום והגדרה של מידע.                                    |
| 139..... | ביצוע הגדרות.  |
| 140..... | איפשור אימות.  |
| 141..... | Authentication Settings                                  |
| 143..... | User Settings רישום                                      |
| 150..... | סנכרון עם LDAP Server                                    |
| 154..... | הגדרת שרת הדוא"ל.  |
| 155..... | הגדרת Scan to My Folder<br>Customize One-touch Functions |
| 157..... |  |
|          | Epson Job History דיווחי באמצעות                         |
| 158..... | Device Admin   |
| 158..... | פריטים שניתן לכלול בדוח.                                 |
| 158..... | כניסה כמנהל מלוח הבקרה.                                  |
| 159..... | השבתת Authentication Settings                            |
|          | מחיקת מידע Authentication Settings                       |
| 159..... | (שחזור להגדרות ברירת המחדל).                             |
| 160..... | פתרון בעיות.   |
| 160..... | לא ניתן לקרוא את כרטיס האימות.                           |

## תחזוקה

|          |                                     |
|----------|-------------------------------------|
| 162..... | ניקוי המעטפת החיצונית של הסורק.     |
| 162..... | ניקוי בתוך הסורק.                   |
| 167..... | החלפת ערכת מכלול הגלגלת.            |
| 172..... | קודי ערכת מכלול גלילים.             |
| 172..... | איפוס מספר הסריקות.                 |
| 172..... | חסכון באנרגיה.                      |
| 173..... | העברת הסורק ממקום למקום.            |
| 174..... | גיבוי ההגדרות.                      |
| 174..... | יצא את ההגדרות.                     |
| 175..... | יבא את ההגדרות.                     |
| 175..... | שחזור להגדרות ברירת המחדל.          |
| 176..... | עדכון אפליקציות וקושחה.             |
|          | עדכון קושחת הסורק באמצעות לוח הבקרה |
| 176..... |                                     |
| 177..... | עדכון קושחה באמצעות Web Config      |
| 177..... | עדכון קושחה בלא להתחבר לאינטרנט.    |

|         |                                 |
|---------|---------------------------------|
|         | קבלת התראות בדואר אלקטרוני כאשר |
| 92..... | מתרחשים אירועים.                |
| 93..... | פתרון בעיות.                    |
| 93..... | שכחת את סיסמת המנהל שלך.        |

## הגדרות אבטחה מתקדמות

|          |  |
|----------|--|
| 95.....  | הגדרות אבטחה ומניעת סכנה.              |
| 96.....  | הגדרות תכונת אבטחה.                    |
| 96.....  | בקרה באמצעות פרוטוקולים.               |
| 96.....  | בקרת פרוטוקולים.                       |
| 96.....  | פרוטוקולים שניתן לאפשר או להשבית.      |
| 97.....  | פריטי הגדרת פרוטוקולים.                |
| 99.....  | שימוש באישור דיגיטלי.                  |
| 99.....  | אודות אישורים דיגיטליים.               |
|          | הגדרת התצורה של                        |
| 100..... | CA-signed Certificate                  |
| 103..... | עדכון אישור בחתימה עצמית.              |
| 104..... | הגדרת התצורה של CA Certificate         |
| 105..... | תקשורת SSL/TLS עם הסורק.               |
|          | הגדרת התצורה של ההגדרות הבסיסיות של    |
| 105..... | SSL/TLS                                |
| 105..... | הגדרת אישור שרת עבור הסורק.            |
| 106..... | תקשורת מוצפנת באמצעות IPsec/סינון IP   |
| 106..... | אודות IPsec/IP Filtering               |
| 106..... | הגדרת תצורת מדיניות ברירת המחדל.       |
| 110..... | הגדרת תצורת מדיניות קבוצתית.           |
| 117..... | דוגמאות לתצורת IPsec/IP Filtering      |
|          | הגדרת תצורה של אישור עובר סינון IPsec/ |
| 118..... | IP                                     |
| 119..... | חיבור הסורק לרשת IEEE802.1X            |
| 119..... | הגדרת תצורה לרשת IEEE 802.1X           |
|          | הגדרת התצורה של אישור עבור IEEE        |
| 120..... | 802.1X                                 |
| 121..... | פתירת בעיות עבור אבטחה מתקדמת.         |
| 121..... | שחזור הגדרות האבטחה.                   |
| 121..... | בעיות בשימוש בתכונות אבטחת רשת.        |
| 123..... | בעיות במהלך השימוש באישור דיגיטלי.     |

## Authentication Settings

|          |                               |
|----------|-------------------------------|
| 129..... | אודות Authentication Settings |
|          | הפונקציות הזמינות עבור        |
| 129..... | Authentication Settings       |
| 130..... | אודות Authentication Method   |
| 132..... | תוכנה לביצוע הגדרות.          |
| 132..... | עדכון קושחת הסורק.            |
| 132..... | חיבור והגדרה של התקן אימות.   |
| 133..... | רשימה תואמת קורא כרטיסים.     |

---

# מבוא



7..... תוכן מסמך זה.

7..... שימוש במדריך.

## תוכן מסמך זה

מסמך זה מספק את המידע הבא עבור מנהלי הסורק.

הגדרות רשת

הכנסת פונקציית הסריקה

אפשר ונהל את הגדרות האבטחה

אפשר ונהל את Authentication Settings

בצע תחזוקה יומית

עבור השיטות הסטנדרטיות של שימוש בסורק, עיינו ב-מדריך למשתמש.

לתשומת לבך:

מסמך זה מסביר את Authentication Settings שמספקות אימות נבדל בלא שיהיה צורך להשתמש בשרת אימות. בנוסף ל-Authentication Settings שהונהגו במדריך זה, תוכל גם לבנות מערכת אימות באמצעות שרת אימות. על מנת לבנות מערכת, השתמש ב-Document Capture Pro Server Authentication Edition (השם המקוצר הוא Document Capture Pro Server AE). למידע נוסף, צור קשר עם משרד Epson המקומי שלך.

## שימוש במדריך

### סימנים וסמלים

 זהירות:

הוראות שיש לקיים בזהירות כדי למנוע פגיעה גופנית.

 חשוב:

הוראות שיש לקיים כדי למנוע נזק לציוד שלך.

לתשומת לבך:

מספק מידע משלים ומקורות לעיון.

מידע קשור

← קישורים לסעיפים קשורים.

### התיאורים המשמשים במדריך זה

צילומי המסך עבור האפליקציות נלקחו ממערכת הפעלה Windows 10 או macOS High Sierra. התכנים המוצגים במסכים משתנים בהתאם לדגם ולמצב.

□ האיורים המובאים במדריך זו נועדו לשם עיון בלבד. למרות שהם עשויים להיות שונים מעט מהמוצר הממשי, שיטות ההפעלה זהות.

## אזכורי מערכת הפעלה

### Windows

במדריך זה, מונחים כמו "Windows 10", "Windows 8.1", "Windows 8", "Windows 7", "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", "Windows Server 2012", ו-"Windows Server 2008 R2" מתייחסים למערכות ההפעלה הבאות. בנוסף לכך, "Windows" משמש כדי להתייחס לכל הגרסאות בעוד ש-"Windows Server" משמש כדי להתייחס אל "Windows Server 2019", "Windows Server 2016", "Windows Server 2012 R2", ו-"Windows Server 2008 R2".

□ מערכת הפעלה Microsoft® Windows® 10

□ מערכת הפעלה Microsoft® Windows® 8.1

□ מערכת הפעלה Microsoft® Windows® 8

□ מערכת הפעלה Microsoft® Windows® 7

□ מערכת הפעלה Microsoft® Windows Server® 2019

□ מערכת הפעלה Microsoft® Windows Server® 2016

□ מערכת הפעלה Microsoft® Windows Server® 2012 R2

□ מערכת הפעלה Microsoft® Windows Server® 2012

□ מערכת הפעלה Microsoft® Windows Server® 2008 R2

### Mac OS

במדריך זה, המונח "Mac OS" משמש כדי להתייחס אל macOS Big Sur, macOS Catalina, macOS Mojave, macOS High Sierra, macOS Sierra, OS X El Capitan, ו-OS X Yosemite.



---

# ההגדרות הדרושות כדי להתאים למטרתך

10. ....ההגדרות הדרושות כדי להתאים למטרתך.

## ההגדרות הדרושות כדי להתאים למטרתך

ראה את הפרטים הבאים כדי לבצע את ההגדרות המתאימות למטרתך.

### חיבור הסורק לרשת

| המטרה                             | הגדרות דרושות  |
|-----------------------------------|--|
| אני רוצה לחבר את הסורק אל הרשת.   | הגדר את הסורק שלך עבור סריקה ברשת.<br>"חיבור הסורק לרשת" בעמוד 14                              |
| אני רוצה לחבר את הסורק למחשב חדש. | הגדר את הגדרות הרשת עבור הסורק שלך במחשב חדש.<br>"הוספה או החלפה של המחשב או ההתקנים" בעמוד 20 |

### הגדרות לסריקה

| המטרה  | הגדרות דרושות   |
|--|---|
| אני רוצה לשלוח תמונות סרוקות באמצעות הדוא"ל.<br>(Scan to Email)            | 1. הגדר את שרת הדוא"ל שברצונך לקשר.<br>"הגדרת שרת דואר" בעמוד 42<br>2. רשום את כתובת הדוא"ל של הנמען בתוך <b>Contacts</b> (אופציונלי). באמצעות רישום כתובת הדוא"ל אינך צריך להזין אותה בכל פעם שברצונך לשלוח משהו, תוכל פשוט לבחור אותה מתוך אנשי הקשר שלך.<br>"הפיכת אנשי קשר לזמינים" בעמוד 61  |
| אני רוצה לשמור תמונות סרוקות לתיקייה ברשת.<br>(Scan to Network Folder/FTP) | 1. צור תיקייה ברשת שבה ברצונך לשמור את התמונות.<br>"הגדרת תיקיית רשת משותפת" בעמוד 45<br>2. רשום את הנתביב אל התיקייה בתוך <b>Contacts</b> (אופציונלי). באמצעות רישום הנתביב לתיקייה אינך צריך להזין אותה בכל פעם שברצונך לשלוח משהו, תוכל פשוט לבחור אותה מתוך אנשי הקשר שלך.<br>"הפיכת אנשי קשר לזמינים" בעמוד 61                                   |
| אני רוצה לשמור תמונות סרוקות אל שירות ענן.<br>(Scan to Cloud)              | הגדר את <b>Epson Connect</b> . עיין בפורטל <b>Epson Connect</b> עבור פרטים נוספים על הגדרה.<br>בעת ביצוע הגדרה, אתה זקוק לחשבון משתמש עבור שירות האחסון המקוון שאליו אתה רוצה לקשר.<br><a href="https://www.epsonconnect.com/">https://www.epsonconnect.com/</a><br><a href="http://www.epsonconnect.eu">http://www.epsonconnect.eu</a> (אירופה בלבד) |

התאמה אישית של תצוגת לוח הבקרה

| המטרה  | הגדרות דרושות  |
|--|--|
| אני רוצה לשנות את הפריטים המוצגים בלוח הבקרה של הסורק. | הגדר קבוע מראש או ערוך את מסך הבית. תוכל לרשום את הגדרות הסריקה המועדפות שלך בלוח הבקרה ולערוך את הפריטים שהוצגו.<br>"התאמה אישית של תצוגת לוח הבקרה" בעמוד 75 |

הגדרת פונקציות אבטחה בסיסיות

| המטרה   | הגדרות דרושות   |
|---|---|
| אני רוצה למנוע מכל אחד שאינו מנהל להחליף את הגדרות הסורק. | הגדר סיסמת מנהל עבור הסורק.<br>"הגדרות מנהל מערכת" בעמוד 84 |
| אני רוצה להשבית את השימוש בסורקים עם חיבורי USB.          | השבת את הממשק החיצוני.<br>"השבת הממשק החיצוני" בעמוד 90     |

הגדרת פונקציות אבטחה מתקדמות

| המטרה   | הגדרות דרושות   |
|---|---|
| אני רוצה לשלוט באלו פרוטוקולים יש להשתמש.   | אפשר או השבת פרוטוקולים.<br>"בקרה באמצעות פרוטוקולים" בעמוד 96  |
| ברצוני להצפין את נתיב התקשורת.  | 1. הגדר את התעודה הדיגיטלית שלך.<br>"שימוש באישור דיגיטלי" בעמוד 99<br>2. הגדר תקשורת SSL/TLS.<br>"תקשורת SSL/TLS עם הסורק" בעמוד 105 |
| ברצוני להשתמש בתקשורת מוצפנת (IPsec).<br>ברצוני להיות מסוגל להשתמש בתוכנה ממחשב ספציפי בלבד (סינון IP). | הגדר מדיניות עובר סינון תעבורה.<br>"תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 106   |
| אני רוצה להשתמש בסורק ברשת IEEE802.1X.  | הגדר IEEE802.1X עבור הסורק.<br>"חיבור הסורק לרשת IEEE802.1X" בעמוד 119  |

הגדרת פונקציות עבור אימות על ידי הסורק

| המטרה                                      | הגדרות דרושות  |
|--|--|
| אני רוצה לאפשר את Authentication Settings. | <p>עיין בפרטים שלהלן עבור מידע נוסף על Authentication Settings ו-1</p> <p>Authentication Method.</p> <p>"אודות Authentication Settings" בעמוד 129</p> <p>"אודות Authentication Method" בעמוד 130</p> |

השימוש במערכת האימות של השרת

באמצעות Document Capture Pro Server Authentication Edition (או בשם המקוצר Document Capture Pro Server AE), תוכל לבנות מערכת אימות שמשתמשת בשרת עבור אימות. למידע נוסף, צור קשר עם משרד Epson המקומי שלך.

---

## הגדרות רשת

- 14. .... חיבור הסורק לרשת.
- 20. .... הוספה או החלפה של המחשב או ההתקנים.
- 26. .... בדיקת מצב חיבור הרשת.
- 28. .... מפרטי רשת.
- 32. .... פתרון בעיות.

## חיבור הסורק לרשת

מקטע זה מסביר כיצד לחבר את הסורק לרשת באמצעות לוח הבקרה של הסורק.

לתשומת לבך:

אם הסורק שלך והמחשב נמצאים באותו מקטע, תוכל גם לחבר באמצעות תוכנת ההתקנה.

☐ התקנה מתוך אתר האינטרנט

גש לאתר האינטרנט שלהלן, והזן את שם המוצר. גש אל התקנה, והתחל לבצע את ההגדרה.

<http://epson.sn>

☐ הגדרה באמצעות דיסק תוכנה (רק עבור דגמים שהגיעו עם דיסק תוכנה ומשתמשים שמחשבים ה-Windows שלהם מצוידים בכונני דיסקים).

הכנס את דיסק התוכנה לתוך המחשב, ולאחר מכן פעל על פי ההוראות המוצגות על גבי המסך.

## לפני ביצוע חיבור רשת

על מנת להתחבר לרשת, בדוק מראש את שיטת החיבור ואת מידע ההגדרות עבור החיבור.

## איסוף מידע על הגדרת החיבור

הכן את מידע ההגדרה הדרוש כדי להתחבר. בדוק מראש את המידע הבא.

| מחלקות                | פריטים   | הערה   |
|-----------------------|--|--|
| שיטת חיבור ההתקן      | <input type="checkbox"/> Ethernet<br><input type="checkbox"/> Wi-Fi  | החלט כיצד לחבר את הסורק אל הרשת.<br>עבור LAN מקוון, מתחברת אל מתג ה-LAN.<br>עבור Wi-Fi, מתחברת אל הרשת (SSID) של נקודת הגישה.  |
| מידע על חיבור ה-LAN   | <input type="checkbox"/> כתובת IP<br><input type="checkbox"/> מסכת רשת משנה<br><input type="checkbox"/> שער ברירת מחדל | החלט על כתובת ה-IP שברצונך להקצות לסורק.<br>כאשר אתה מקצה את כתובת ה-IP באופן סטטי, יש צורך בכל הערכים.<br>כאשר אתה מקצה את כתובת ה-IP באופן דינמי באמצעות פונקציית ה-DHCP, אין צורך במידע זה משום שהוא מוגדר אוטומטית.                    |
| מידע על חיבור ה-Wi-Fi | <input type="checkbox"/> SSID<br><input type="checkbox"/> סיסמה  | אלה הם ה-SSID (שם הרשת) והסיסמה של נקודת הגישה שאליה מתחבר הסורק.<br>אם הוגדר סינון כתובת MAC, יש לרשום את כתובת ה-MAC של הסורק מראש כדי לרשום את הסורק.<br>עיין בפרטים הבאים כדי לקרוא על התקנים שיש עבורם תמיכה.<br>"מפרטי רשת" בעמוד 28 |

| מחלקות              | פריטים   | הערה  |
|---------------------|--|---|
| מידע על שרת DNS     | <input type="checkbox"/> כתובת IP עבור DNS ראשי<br><input type="checkbox"/> כתובת IP עבור DNS משני | אלה דרושים כאשר מציינים שרתי DNS. ה-DNS המשני מוגדר כאשר יש למערכת תצורה יתירה וקיים שרת DNS משני.<br>אם אתה נמצא בארגון קטן ואינך מגדיר שרת DNS, הגדר את כתובת ה-IP של הנתב.                             |
| מידע על שרת הפרוקסי | <input type="checkbox"/> שם שרת הפרוקסי  | הגדר זאת כאשר סביבת הרשת שלך משתמש בשרת הפרוקסי כדי לגשת לאינטרנט מהאינטרנט-נט, ואתה משתמש בפונקציה בה ניגש הסורק ישירות אל האינטרנט.<br>עבור הפונקציות הבאות, הסורק מתחבר ישירות אל האינטרנט.            |
| מידע על מספר יציאה  | <input type="checkbox"/> מספר היציאה שיש לשחרר   | בדוק את מספר היציאה בה משתמשים הסורק והמחשב, ולאחר מכן, במידת הצורך, שחרר את היציאה שחומת האש חוסמת.<br>עיין בפרטים הבאים כדי למצוא את מספר היציאה המשמש את הסורק.<br>"השימוש ביציאה עבור הסורק" בעמוד 30 |

## הקצאת כתובת IP

ניתן להקצות את הסוגים הבאים של כתובות IP.

### כתובת IP סטטית:

הקצה באופן ידני לסורק (המארך) את כתובת ה-IP שנקבעה מראש.

יש להגדיר באופן ידני את המידע הדרוש כדי להתחבר לרשת (מסכת תת-רשת, שער ברירת המחדל, שרת ה-DNS, וכן הלאה).

כתובת ה-IP אינה משתנה אפילו כאשר מכבים את ההתקן. לכן אפשרות זו שימושית כאשר רוצים לנהל התקנים בסביבה שבה לא ניתן לשנות את כתובת ה-IP או כאשר רוצים לנהל התקנים תוך שימוש בכתובת ה-IP. אנא ממליצים על הגדרות עבור הסורק, השרת וכו', שאליהם ניגשים מחשבים רבים. כמו כן, בעת השימוש בתכונות אבטחה כמו סינון IPsec/IP, הקצה כתובת IP קבועה כדי שכתובת ה-IP לא תשתנה.

### הקצאה אוטומטיית באמצעות פונקציית ה-DHCP (כתובת IP דינמית):

הקצה את כתוב ה-IP באופן אוטומטי לסורק (מארך) באמצעות השימוש בפונקציית ה-DHCP של שרת או נתב ה-DHCP.

המידע הדרוש לשם התחברות אל הרשת (מסכת תת-רשת, שער ברירת המחדל, שרת ה-DNS, וכן הלאה) מוגדר באופן אוטומטי, ולכן תוכל לחבר את ההתקן בקלות אל הרשת.

אם ההתקן או הנתב מכובים, או בהתאם להגדרות שרת ה-DHCP, אפשר שכתובת ה-IP תשתנה בעת התחברות מחדש.

אנו ממליצים לנהל התקנים מחוץ לכתובת ה-IP וליצור תקשורת עם פרוטוקולים שיכולים לעקוב אחר כתובת ה-IP.

לתשומת לבך:

כאשר משתמשים בפונקציית שמירת הכתובת של ה-DHCP, ניתן להקצות את אותה כתובת IP להתקנים בכל עת.

## שרת DNS ושרת פרוקסי

לשרת ה-DNS יש שם מארח, שם תחום של כתובת הדוא"ל וכו', בהקשר של מידע על כתובת ה-IP. התקשורת אינה אפשרית אם הצד השני תואר בשם מארח, שם תחום, וכו', כאשר המחשב או הסורק מבצעים תקשורת IP.

מתשאל את שרת ה-DNS כדי לקבל מידע ומשיג את כתובת ה-IP של הצד האחר. תהליך זה נקרא רזולוציה.

לכן, התקנים, כגון מחשבים וסורקים מסוגלים לתקשר באמצעות כתובת ה-IP.

רזולוציית השם דרושה כדי שהסורק יוכל לתקשר באמצעות פונקציית הדוא"ל או פונקציית החיבור לאינטרנט.

כאשר אתה משתמש בפונקציית אלה, בצע את הגדרות שרת ה-DNS.

כאשר אתה מקצה לסורק כתובת IP באמצעות פונקציית ה-DHCP של שרת או נתב ה-DHCP היא מוגדרת באופן אוטומטי.

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.

כאשר אתה מתחבר אל האינטרנט באמצעות שרת פרוקסי, הגדר את שרת הפרוקסי בסורק.

## התחברות אל הרשת מלוח הבקרה

חבר את הסורק אל הרשת באמצעות לוח הבקרה של הסורק.

## הקצאת כתובת ה-IP

הגדר פרטים בסיסיים כמו כתובת המארח, מסכת רשת משנה, שער ברירת מחדל.

סעיף זה מסביר את הנוהל עבור הגדרת כתובת IP סטטית.

1. הדלק את הסורק.

2. בחר הגדרות במסך הבית בלוח הבקרה של הסורק.

3. בחר הגדרות רשת < מתקדם < TCP/IP.

4. בחר ידני עבור קבל כתובת IP.

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 5 עד 6 מוגדרים אף הם באופן אוטומטי, לכן, עבור אל שלב 7.



5. הזן את כתובת ה-IP.

המיקוד יעבור למקטע הקדמי או למקטע האחורי המופרד באמצעות נקודה, אם תבחר ◀ ו- ▶.

אשר את הערך המוצג במסך הקודם.

6. הגדר את מסכת רשת משנה ואת שער ברירת מחדל.

אשר את הערך המוצג במסך הקודם.

**חשוב!**

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.

7. הזן את כתובת ה-IP עבור שרת ה-DNS הראשי.

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 9.

8. הזן את כתובת ה-IP עבור שרת ה-DNS המשני.

אשר את הערך המוצג במסך הקודם.

9. הקש התחל הגדרה.

**הגדרת שרת הפרוקסי**

הגדר את שרת הפרוקסי אם מתקיימים שני התנאים הבאים.

שרת הפרוקסי בנוי עבור חיבור אינטרנט.

כאשר משתמשים בפונקציה המאפשרת לסורק להתחבר ישירות לאינטרנט, כגון שירות Epson Connect או שירותי ענן של חברה אחרת.

1. בחר את הגדרות במסך הבית.

כאשר מבצעים הגדרות אחרי הגדרת כתובת ה-IP, יוצג המסך מתקדם. עבור לשלב 3.

2. בחר הגדרות רשת < מתקדם.

3. בחר שרת פרוקסי.

4. בחר שימוש עבור הגדרות שרת פרוקסי.

5. הזן את הכתובת עבור שרת הפרוקסי באמצעות IPv4 או FQDN.

אשר את הערך המוצג במסך הקודם.

6. הזן את מספר הכניסה עבור שרת הפרוקסי.

אשר את הערך המוצג במסך הקודם.

7. הקש התחל הגדרה.

## התחברות ל-Ethernet

חבר את הסורק לרשת באמצעות כבל LAN ואז בדוק את החיבור.

1. חבר את הסורק ואת הרכוזת (מתג LAN) באמצעות כבל LAN.

2. בחר  במסך הבית.

3. בחר ראוטר.

4. ודא שהגדרות חיבור ו-כתובת IP נכונות.

5. הקש סגירה.

## התחברות אל ה-LAN האלחוטי (Wi-Fi)

תוכל לחבר את הסורק אל ה-LAN האלחוטי (Wi-Fi) במספר דרכים. בחר את שיטות החיבור המתאימה לסביבה ולתנאים שלך.

אם ידוע לך המידע על הנתב האלחוטי, כגון SSID וסיסמה, תוכל לבצע את ההגדרות באופן ידני.

אם הנתב האלחוטי תומך ב-WPS, תוכל לבצע את ההגדרות באמצעות ההגדרה בלחיצת כפתור.

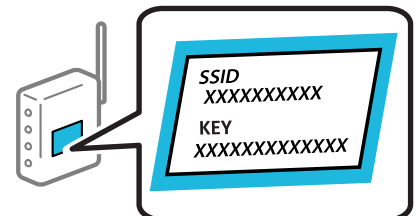
אחרי חיבור הסורק לרשת, חבר את הסורק אל ההתקן בו ברצונך להשתמש (מחשב, התקן חכם, טבלט וכן הלאה).

### ביצוע הגדרות Wi-Fi באמצעות הזנת ה-SSID והסיסמה

תוכל להגדיר רשת Wi-Fi באמצעות הזנת המידע הדרוש כדי להתחבר לנתב אלחוטי מתוך לוח הבקרה של הסורק. על מנת לבצע את ההגדרה בשיטה זו, תהיה זקוק ל-SSID ולסיסמה של נתב אלחוטי.

לתשומת לבך:

אם אתה משתמש בנתב אלחוטי עם הגדרות ברירת המחדל שלו, ה-SSID והסיסמה מופיעות על התווית. אם אינך יודע את ה-SSID ואת הסיסמה, צור קשר עם האדם שהתקין את הנתב האלחוטי, או עיין בתיעוד שנלווה לנתב האלחוטי.



1. הקש   במסך הבית.

2. בחר ראוטר.

3. הקש התחל הגדרה.

אם חיבור הרשת כבר הוגדר, יוצגו פרטי החיבור. הקש שנה לחיבור Wi-Fi. או שינוי ההגדרות כדי לשנות את ההגדרות.

4. בחר אשף הגדרת רשת אלחוטי.

5. פעל בהתאם להוראות המוצגות על גבי המסך כדי לבחור את ה-SSID, להזין את הסיסמה עבור הנתב האלחוטי, ולהתחיל את ההגדרה.

אם ברצונך לבדוק את מצב חיבור הרשת עבור הסורק אחרי השלמת ההגדרה, עיין בקישור המידע הקשור להלן עבור פרטים.

לתשומת לבך:

□ אם אינך יודע את ה-SSID, בדוק אם הוא כתוב על תווית הנתב האלחוטי. אם אתה משתמש בנתב האלחוטי עם הגדרות ברירת המחדל שלו, השתמש ב-SSID המופיע על התווית. אם אין ביכולתך למצוא מידע כלשהו, עיין בתיעוד שסופק עם הנתב האלחוטי.

□ הסיסמה רגישה לאותיות קטנות וגדולות באנגלית.

□ אם אינך יודע את הסיסמה, בדוק אם המידע כתוב על תווית הנתב האלחוטי. אפשר שהסיסמה שמופיעה על התווית מצויינת בשם "Network Key", "Wireless Password", וכן הלאה. אם אתה משתמש בנתב האלחוטי עם הגדרות ברירת המחדל שלו, השתמש בסיסמה המופיעה על התווית.

מידע קשור

← "בדיקת מצב חיבור הרשת" בעמוד 26

### ביצוע הגדרות Wi-Fi באמצעות התקנת לחצן (WPS)

תוכל להתקין רשת Wi-Fi באופן אוטומטי בלחיצת כפתור בנתב האלחוטי. אם התנאים להלן מתקיימים, תוכל לקבוע את ההגדרות תוך שימוש בשיטה זו.

□ הנתב האלחוטי תואם (WPS (Wi-Fi Protected Setup).

□ חיבור ה-Wi-Fi הנוכחי בוצע באמצעות לחיצת כפתור בנתב האלחוטי.

לתשומת לבך:

אם אינך מצליח למצוא את הכפתור או שאתה מבצע את ההתקנה באמצעות תוכנה, עיין בתיעוד שסופק עם הנתב האלחוטי.

1. הקש  במסך הבית.

2. בחר ראوتر.

3. הקש התחל הגדרה.

אם חיבור הרשת כבר הוגדר, יוצגו פרטי החיבור. הקש שנה לחיבור Wi-Fi. או שינוי ההגדרות כדי לשנות את ההגדרות.

4. בחר הגדרה בלחיצת כפתור (WPS).

5. פעל על פי ההוראות המוצגות על גבי המסך.

אם ברצונך לבדוק את מצב חיבור הרשת עבור הסורק אחרי השלמת ההגדרה, עיין בקישור המידע הקשור להלן עבור פרטים.

לתשומת לבך:

אם החיבור נכשל, הפעל את הנתב האלחוטי מחדש, קרב אותו לסורק ונסה שוב.

מידע קשור

← "בדיקת מצב חיבור הרשת" בעמוד 26

### קביעת הגדרות Wi-Fi באמצעות התקנת קוד PIN (WPS)

תוכל להתחבר באופן אוטומטי לנתב אלחוטי באמצעות קוד PIN. תוכל להשתמש בשיטה זו כדי לבצע את ההתקנה אם נתב אלחוטי תומך ב-WPS (הגדרה מוגנת Wi-Fi). יש להשתמש במחשב כדי להזין קוד PIN לתוך הנתב האלחוטי.

1. הקש  במסך הבית.

2. בחר ראוטר.

3. הקש התחל הגדרה.

אם חיבור הרשת כבר הוגדר, יוצגו פרטי החיבור. הקש שנה לחיבור Wi-Fi. או שינוי ההגדרות כדי לשנות את ההגדרות.

4. בחר אחרים < הגדרת קוד PIN (WPS)

5. פעל על פי ההוראות המוצגות על גבי המסך.

אם ברצונך לבדוק את מצב חיבור הרשת עבור הסורק אחרי השלמת ההגדרה, עיין בקישור המידע הקשור להלן עבור פרטים.

לתשומת לבך:

עיין בתיעוד הנלווה לנתב האלחוטי שלך לפרטים על הזנת קוד PIN.

מידע קשור

← "בדיקת מצב חיבור הרשת" בעמוד 26

---

## הוספה או החלפה של המחשב או ההתקנים

### התחברות לסורק שחובר לרשת

כאשר הסורק כבר חובר לרשת, תוכל לחבר מחשב או התקן חכם לסורק דרך הרשת.

## השימוש בסורק רשת מתוך מחשב שני

אנו ממליצים להשתמש בתוכנת ההתקנה כדי לחבר את הסורק למחשב. ניתן להפעיל את תוכנת ההתקנה באחת מהשיטות הבאות.

התקנה מתוך אתר האינטרנט

גש לאתר האינטרנט שלהלן, והזן את שם המוצר. גש אל התקנה, והתחל לבצע את ההגדרה.

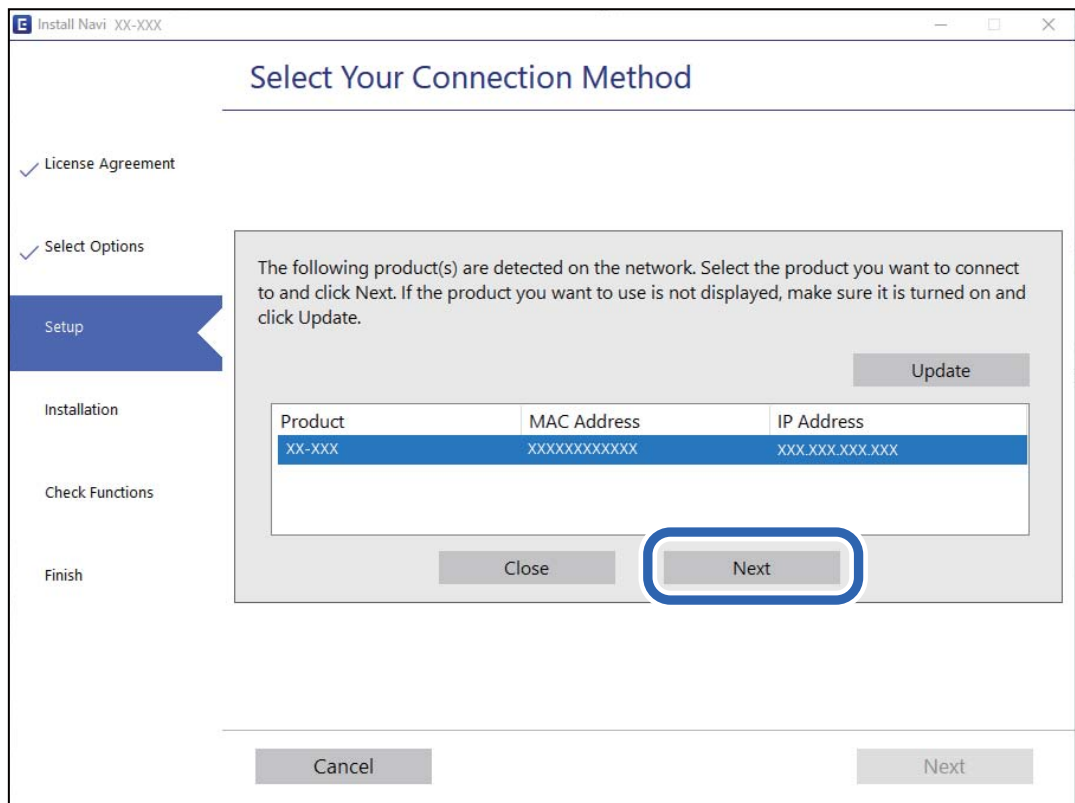
<http://epson.sn>

הגדרה באמצעות דיסק תוכנה (רק עבור דגמים שהגיעו עם דיסק תוכנה ומשתמשים שמחשבים ה-Windows שלהם מצוידים בכונני דיסקים).

הכנס את דיסק התוכנה לתוך המחשב, ולאחר מכן פעל על פי ההוראות המוצגות על גבי המסך.

### בחירת הסורק

פעל בהתאם להוראות המוצגות על גבי המסך עד שיוצג המסך הבא, בחר את שם הסורק שברצונך להתחבר אליו, ואז לחץ הבא.



פעל על פי ההוראות המוצגות על גבי המסך.

## השימוש בסורק רשת מתוך התקן חכם

תוכל לחבר התקן חכם לסורק באמצעות אחת מהשיטות הבאות.

התחברות דרך נתב אלחוטי

חבר את ההתקן החכם לאותה רשת Wi-Fi (אותו SSID) שאליה מחובר הסורק.

לפרטים נוספים עיין במידע שלהלן.

["ביצוע הגדרות עבור התחברות להתקן חכם" בעמוד 25](#)

### התחברות באמצעות Wi-Fi Direct

חבר את ההתקן החכם אל הסורק באופן ישיר ללא נתב אלחוטי.

לפרטים נוספים עיין במידע שלהלן.

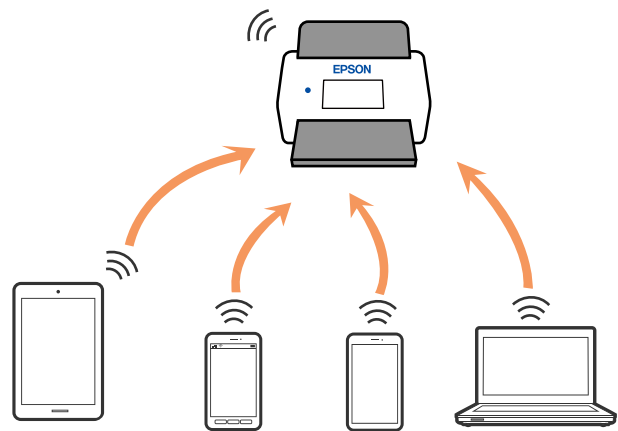
["חיבור ישיר בין התקן חכם לבין סורק \(Wi-Fi Direct\)" בעמוד 22](#)

## חיבור ישיר בין התקן חכם לבין סורק (Wi-Fi Direct)

Wi-Fi Direct (נקודת AP פשוטה) מאפשר לך לחבר התקן חכם ישירות לסורק ללא נתב אלחוטי וסורק מתוך ההתקן החכם.

### אודות Wi-Fi Direct

השתמש באפשרות הזו אם אינך משתמש ברשת Wi-Fi בבית או במשרד, או אם אתה רוצה לחבר ישירות בין הסורק לבין מחשב או מכשיר חכם. במצב הזה הסורק משמש כראוטר אלחוטי ואפשר לחבר אליו מכשירים בלי להשתמש בראוטר אלחוטי רגיל. עם זאת, התקנים המחוברים ישירות לסורק אינם יכולים לתקשר אלו עם אלו באמצעות הסורק.



אפשר לחבר מכשירים אל הסורק באמצעות רשת Wi-Fi או אתרנט וחיבור Wi-Fi Direct (נקודת AP פשוטה) בו-זמנית. עם זאת, אם מתחילים חיבור באמצעות Wi-Fi Direct (נקודת AP פשוטה) כשהסורק מחובר באמצעות רשת Wi-Fi, רשת ה-Wi-Fi מנותקת זמנית.

### התחברות אל התקן חכם באמצעות Wi-Fi Direct

שיטה זאת מאפשרת לחבר את הסורק ישירות עם התקנים חכמים, ללא שימוש בנתב אלחוטי.

1. בחר את  במסך הבית.

2. בחר Wi-Fi Direct.

3. בחר התחל הגדרה.

4. הפעל את Epson Smart Panel בהתקן החכם שלך.

5. פעל בהתאם להוראות ב-Epson Smart Panel כדי להתחבר אל הסורק שלך.  
כאשר ההתקן החכם שלך מחובר לסורק, גש אל הצעד הבא.

6. בלוח הבקרה של הסורק, בחר סיום.

## ניתוק חיבור Wi-Fi Direct (נקודת AP פשוטה)

יש שתי שיטות זמינות להשבתת חיבור Wi-Fi Direct (נקודת AP פשוטה); תוכל להשבית את כל החיבורים באמצעות לוח הבקרה של הסורק, או להשבית כל חיבור מהמחשב או מההתקן החכם.

כאשר אתה רוצה להשבית את כל החיבורים, בחר  < Wi-Fi Direct < התחל הגדרה < שנה < השבתת Wi-Fi Direct.

**חשוב!**

כאשר חיבור Wi-Fi Direct (נקודת AP פשוטה) מושבת, כל המחשבים וההתקנים החכמים המחוברים לסורק בחיבור Wi-Fi Direct (נקודת AP פשוטה) מנותקים.


**לתשומת לבך:**

אם ברצונך לנתק התקן ספציפי, התנתק מההתקן במקום מהסורק. השתמש באחת השיטות הבאות כדי לנתק את חיבור Wi-Fi Direct (נקודת AP פשוטה) מתוך ההתקן.

נתק את חיבור ה-Wi-Fi אל שם הרשת של הסורק (SSID).

התחבר לשם רשת אחרת (SSID).

## שינוי הגדרות Wi-Fi Direct (נקודת AP פשוטה) כגון ה-SSID

כאשר אופשר חיבור Wi-Fi Direct (נקודת AP פשוטה), תוכל לשנות את ההגדרות מתוך  < Wi-Fi Direct < התחל הגדרה < שנה, ואז יוצגו פריטי התפריט הבאים.

**שינוי שם הרשת**

שנה את שם הרשת של Wi-Fi Direct (נקודת AP פשוטה) (SSID) עבור חיבור הסורק לשם שרירותי כלשהו. תוכל להגדיר את שם הרשת (SSID) בתווי ASCII המוצגים במקלדת התוכנה בלוח הבקרה. תוכל להזין עד 22 תווים.

בעת שינוי שם הרשת (SSID), מנותקים כל ההתקנים המחוברים. השתמש בשם הרשת החדש (SSID) אם ברצונך לחבר מחדש את ההתקן.

**שינוי הסיסמה**

שנה את סיסמת Wi-Fi Direct (נקודת AP פשוטה) עבור חיבור הסורק לערך השרירותי שלך. תוכל להגדיר את הסיסמה בתווי ASCII המוצגים במקלדת התוכנה בלוח הבקרה. תוכל להזין 8 עד 22 תווים.

בעת שינוי סיסמה, מנותקים כל ההתקנים המחוברים. השתמש בסיסמה החדשה אם ברצונך לחבר מחדש את ההתקן.

### שינוי טווח התדרים

שנה את תחום התדרים של Wi-Fi Direct המשמשים לשם חיבור הסורק. תוכל לבחור 2.4 GHz או 5 GHz.

בעת שינוי טווח התדרים מנותקים כל ההתקנים המחוברים. חבר מחדש את ההתקן.  
שים לב שלא תוכל להתחבר מחדש מהתקנים שאינם תומכים בטווח התדרים של 5 GHz כאשר תעבור ל-5 GHz.  
יתכן שההגדרה לא תוצג, תלוי באזור.

### השבתת Wi-Fi Direct

השבת את הגדרות Wi-Fi Direct (נקודת AP פשוטה) עבור הסורק. בעת ההשבתה, כל ההתקנים המחוברים לסורק באמצעות חיבור Wi-Fi Direct (נקודת AP פשוטה) ינותקו.

### שחזור הגדרות ברירת מחדל

שחזור כל הגדרות Wi-Fi Direct (נקודת AP פשוטה) לערכי ברירת המחדל שלהם.  
יימחק המידע על חיבור Wi-Fi Direct (נקודת AP פשוטה) של ההתקן החכם שנשמר בסורק.  
לתשומת לבך:  
תוכל גם להגדיר מתוך לשונית *Wi-Fi Direct < Network* בתוך *Web Config* עבור ההגדרות הבאות.

איפשר או השבתה של *Wi-Fi Direct* (נקודת AP פשוטה)

שינוי שם הרשת (SSID)

שינוי סיסמה

שינוי טווח התדרים

יתכן שההגדרה לא תוצג, תלוי באזור.

שחזור הגדרות *Wi-Fi Direct* חיבור (נקודת AP פשוטה)

## הגדרה מחדש של חיבור הרשת

סעיף זה מסביר כיצד לבצע את הגדרות חיבור הרשת ולשנות את שיטת החיבור כאשר מחליפים את הנתב האלחוטי או את המחשב.

### בעת החלפת הנתב האלחוטי

כאשר אתה מחליף את הנתב האלחוטי, בצע הגדרות עבור החיבור בין המחשב לבין ההתקן החכם והסורק. עליך לבצע הגדרות אלה אם אתה משנה את ספק שירותי האינטרנט שלך וכן הלאה.

### ביצוע הגדרות עבור התחברות למחשב

אנו ממליצים להשתמש בתוכנת ההתקנה כדי לחבר את הסורק למחשב. ניתן להפעיל את תוכנת ההתקנה באחת מהשיטות הבאות.



□ התקנה מתוך אתר האינטרנט

גש לאתר האינטרנט שלהלן, והזן את שם המוצר. גש אל התקנה, והתחל לבצע את ההגדרה.

<http://epson.sn>

□ הגדרה באמצעות דיסק תוכנה (רק עבור דגמים שהגיעו עם דיסק תוכנה ומשתמשים שמחשבים ה-Windows שלהם מצוידים בכונני דיסקים).

הכנס את דיסק התוכנה לתוך המחשב, ולאחר מכן פעל על פי ההוראות המוצגות על גבי המסך.

בחירת שיטות החיבור

פעל על פי ההוראות המוצגות על גבי המסך. במסך בחר את הפעולה הרצויה בחר יצירת חיבור מחדש אל מדפסת (לראוטר חדש ברשת או להחלפה מ-USB לרשת וכו'), ואז לחץ הבא.

פעל בהתאם להוראות המוצגות על המסך כדי לסיים את ההתקנה.

אם לא תוכל להתחבר, עיין בפרטים הבאים כדי לנסות לפתור את הבעיה.

"לא ניתן להתחבר לרשת" בעמוד 32

**ביצוע הגדרות עבור התחברות להתקן חכם**

תוכל להשתמש בסורק מהתקן חכם כאשר אתה מחבר את הסורק לאותה רשת Wi-Fi (רשת SSID) כמו ההתקן החכם. על מנת להשתמש בסורק מתוך מכשיר חכם, גש אל האתר הבא, ואז הזן את שם המוצר. גש אל התקנה, והתחל לבצע את ההגדרה.

<http://epson.sn>

גישה לאתר האינטרנט מההתקן החכם שברצונך לחבר לסורק.

**בעת שינוי המחשב**

בעת שינוי המחשב, בצע הגדרות חיבור בין המחשב לבין הסורק.

**ביצוע הגדרות עבור התחברות למחשב**

אנו ממליצים להשתמש בתוכנת ההתקנה כדי לחבר את הסורק למחשב. ניתן להפעיל את תוכנת ההתקנה באמצעות השיטה הבאה.

□ הגדרה מתוך אתר האינטרנט

גש לאתר האינטרנט שלהלן, והזן את שם המוצר. גש אל התקנה, והתחל לבצע את ההגדרה.

<http://epson.sn>

□ הגדרה באמצעות דיסק תוכנה (רק עבור דגמים שהגיעו עם דיסק תוכנה ומשתמשים שמחשבים ה-Windows שלהם מצוידים בכונני דיסקים).

הכנס את דיסק התוכנה לתוך המחשב, ולאחר מכן פעל על פי ההוראות המוצגות על גבי המסך.

פעל על פי ההוראות המוצגות על גבי המסך.

**שינוי שיטת החיבור למחשב**

סעיף זה מסביר כיצד לשנות את שיטת החיבור כאשר המחשב והסורק חוברים.

### שינוי חיבור הרשת מ-Wi-Fi ל-Ethernet

שנה את חיבור ה-Ethernet לחיבור Wi-Fi מלוח הבקרה של הסורק. שיטת שינוי החיבור זהה במהותה לזו של הגדרות חיבור ה-Wi-Fi.

מידע קשור

← "התחברות אל ה-LAN האלחוטי (Wi-Fi)" בעמוד 18

### שינוי חיבור הרשת מ-Wi-Fi ל-Ethernet

פעל על פי הצעדים הבאים כדי לשנות את החיבור מ-Wi-Fi ל-Ethernet.

1. בחר את הגדרות במסך הבית.
2. בחר הגדרות רשת < הגדרת רשת קוויית.
3. פעל על פי ההוראות המוצגות על גבי המסך.

### מעבר מחיבור USB לחיבור רשת

השימוש בתוכנת ההתקנה כדי להתקין מחדש עם שיטת חיבור שונה.

התקנה מתוך אתר האינטרנט

גש לאתר האינטרנט שלהלן, והזן את שם המוצר. גש אל התקנה, והתחל לבצע את ההגדרה.

<http://epson.sn>

הגדרה באמצעות דיסק תוכנה (רק עבור דגמים שהגיעו עם דיסק תוכנה ומשתמשים שמחשבים ה-Windows שלהם מצוידים בכונני דיסקים).

הכנס את דיסק התוכנה לתוך המחשב, ולאחר מכן פעל על פי ההוראות המוצגות על גבי המסך.

בחירת שינוי שיטות החיבור

פעל על פי ההוראות המוצגות על גבי המסך. במסך בחר את הפעולה הרצויה בחר יצירת חיבור מחדש אל מדפסת (לראוטר חדש ברשת או להחלפה מ-USB לרשת וכו'), ואז לחץ הבא.

בחר את חיבור הרשת שבו ברצונך להשתמש, חיבור באמצעות רשת אלחוטית (Wi-Fi) או התחברות באמצעות רשת קוויית (אתרנט), ואז לחץ הבא.

פעל בהתאם להוראות המוצגות על המסך כדי לסיים את ההתקנה.

---

## בדיקת מצב חיבור הרשת

תוכל לבדוק את מצב חיבור הרשת בדרך הבאה.

## בדיקת מצב חיבור הרשת מלוח הבקרה

תוכל לבדוק את מצב החיבור של הרשת באמצעות סמל הרשת או מידע הרשת בלוח הבקרה של הסורק.

## בדיקת מצב חיבור הרשת באמצעות סמל הרשת

תוכל לבדוק את מצב החיבור של הרשת ואת עוצמת גל הרדיו באמצעות סמל הרשת במסך הבית של הסורק.



|  |  |
|--|--|
| מציג את מצב חיבור הרשת.<br>בחר את הסמל כדי בדוק ולשנות את ההגדרות הנוכחיות. זהו קיצור הדרך עבור התפריט שלהלן.<br>הגדרות < הגדרות רשת < הגדרת Wi-Fi |  |
| הסורק אינה מחובר לרשת אלחוטית (Wi-Fi).   |  |
| הסורק מחפש SSID, כתובת ה-IP אינה מוגדרת, או שקיימת בעיה עם רשת אלחוטית (Wi-Fi).  |  |
| הסורק מחובר לרשת אלחוטית (Wi-Fi).<br>מספר הפסים מציין את עוצמת השידור של החיבור. ככל שיש יותר פסים כך החיבור חזק יותר.                             |  |
| הסורק אינו מחובר לרשת אלחוטית (Wi-Fi) במצב Wi-Fi Direct (נקודת AP פשוטה).  |  |
| הסורק מחובר לרשת אלחוטית (Wi-Fi) במצב Wi-Fi Direct (נקודת AP פשוטה).   |  |
| הסורק אינו מחובר לרשת קווית (Ethernet) או שההגדרה עבור רשת כזאת בוטלה.   |  |
| הסורק מחובר לרשת קווית (Ethernet).   |  |

## הצגת מידע מפורט על הרשת מתוך לוח הבקרה

כשהסורק שלך מחובר לרשת, אתה יכול לצפות במידע נוסף הקשור לרשת באמצעות בחירת תפריטי הרשת שברצונך לבדוק.

1. בחר את הגדרות במסך הבית.

2. בחר הגדרות רשת < סטטוס הרשת.

3. כדי לבדוק את המידע, לחץ על התפריטים שאתה רוצה לבדוק.

סטטוס רשת Wi-Fi/קווית

מציג את המידע על הרשת (שם ההתקן, החיבור, עוצמת האות, וכן האלה) עבור חיבורי Ethernet או Wi-Fi.

מצב Wi-Fi Direct

מציג אם Wi-Fi Direct מאופשר או מושבת ואת סיסמת SSID, וכן הלאה, עבור חיבורי Wi-Fi Direct.

□ מצב שרת דוא"ל

מציג את מידע הרשת עבור שרת הדוא"ל.

## מפרטי רשת

### מפרט Wi-Fi

עיין בטבלה הבאה עבור מפרטי ה-Wi-Fi.

|  |        |
|--|--------|
| מדינות או אזורים פרט לאלו הרשומים להלן         | טבלה א |
| אוסטרליה<br>ניו זילנד<br>קוריאה<br>דרום קוריאה | טבלה ב |

טבלה א

|                                |   |
|--------------------------------|---|
| תקנים                          | IEEE 802.11b/g/n <sup>1*</sup>  |
| טווח תדרים                     | GHz 2.4   |
| עוצמת שידור מירבית של תדר רדיו | 2, 400-2, 483.5 MHz :20 dBm (EIRP)  |
| ערוצים                         | 1/2/3/4/5/6/7/8/9/10/11/12/13   |
| מצבי חיבור                     | תשתית, Wi-Fi Direct (נקודת AP פשוטה) <sup>2*3*</sup>                                    |
| פרוטוקולי אבטחה <sup>4*</sup>  | WPA2/ , WPA3-SAE (AES) , WPA2-PSK (AES) <sup>5*</sup> , WEP (64/128bit) WPA3-Enterprise |

<sup>1\*</sup> זמין רק עבור HT20.

<sup>2\*</sup> לא נתמך עבור תקן IEEE 802.11b.

<sup>3\*</sup> ניתן להשתמש בתשתית ובמצבי Wi-Fi Direct או בחיבור Ethernet בעת ובעונה אחת.

<sup>4\*</sup> Wi-Fi Direct תומך ב-WPA2-PSK (AES) בלבד.

<sup>5\*</sup> תואם לתקן ההצפנה WPA2 עם תמיכה בהצפנת WPA/WPA2 אישית.

טבלה ב

|             |  |
|-------------|--|
| תקנים       | ac/ <sup>1*</sup> IEEE 802.11a/b/g/n                 |
| תחומי תדרים | IEEE 802.11b/g/n :2.4 GHz , IEEE 802.11a/n/ac :5 GHz |

|   |                     |              |                                |
|---|---------------------|--------------|--------------------------------|
| 2 <sup>*2</sup> /13 <sup>*</sup> 1/2/3/4/5/6/7/8/9/10/11/12   | 2.4 GHz             | Wi-Fi        | ערוצים                         |
| (W52 (36/40/44/48),<br>(W53 (52/56/60/64),<br>W56<br>(100/104/108/112/116/120/124/128/132/136/140/<br>,144),<br>(W58 (149/153/157/161/165 | 5 GHz <sup>3*</sup> |              |                                |
| 2 <sup>*2</sup> /13 <sup>*</sup> 1/2/3/4/5/6/7/8/9/10/11/12   | 2.4 GHz             | Wi-Fi Direct | מצבי חיבור                     |
| (W52 (36/40/44/48),<br>(W58 (149/153/157/161/165  | 5 GHz <sup>3*</sup> |              |                                |
| תשתית, Wi-Fi Direct (נקודת AP פשוטה) 4 <sup>*</sup> , 5 <sup>*</sup>  |                     |              | פרוטוקולי אבטחה 6 <sup>*</sup> |
| WPA2/ ,WPA3-SAE (AES) ,7 <sup>*</sup> WPA2-PSK (AES) ,WEP (64/128bit)<br>WPA3-Enterprise  |                     |              |                                |

1\* זמין רק עבור HT20.

2\* לא זמין בטאיוואן.

3\* הזמינות של ערוצים אלה והשימוש במוצר מחוץ לבית על גבי ערוצים אלה, משתנים על פי מיקום. למידע נוסף, ראה <http://support.epson.net/wifi5ghz/>

4\* לא נתמך עבור תקן IEEE 802.11b.

5\* ניתן להשתמש בתשתית ובמצבי Wi-Fi Direct או בחיבור Ethernet בעת ובעונה אחת.

6\* Wi-Fi Direct תומך רק ב-WPA2-PSK (AES).

7\* תואם לתקן ההצפנה WPA2 עם תמיכה בהצפנת WPA/WPA2 אישית.

## מפרט Ethernet

|   |            |
|---|------------|
| 1 <sup>*</sup> (IEEE802.3i (10BASE-T<br>1 <sup>*</sup> (IEEE802.3u (100BASE-TX<br>1 <sup>*</sup> (IEEE802.3ab (1000BASE-T<br>2 <sup>*</sup> (IEEE802.3az (Energy Efficient Ethernet | תקנים      |
| אוטומטית, דופלקס מלא 10 Mbps, חצי דופלקס 10 Mbps, דופלקס מלא 100 Mbps<br>חצי דופלקס 100 Mbps  | מצב תקשורת |
| RJ-45   | מחבר       |

1\* יש להשתמש בכבל STP (זוג שזור מסוכך) מקטגוריה 5e ומעלה כדי למנוע סיכון של הפרעת רדיו.

2\* המכשיר המחובר צריך להתאים לתקני IEEE802.3az.

## פונקציות רשת ו- IPv4/IPv6

| פונקציות                               | נתמכות     |
|--|------------|
| Epson Scan 2                           | IPv6 ,IPv4 |
| Document Capture Pro /Document Capture | IPv4       |
| Document Capture Pro Server            | IPv6 ,IPv4 |

## פרוטוקול אבטחה

|                           |         |
|---------------------------|---------|
| *IEEE802.1X               |         |
| סינון IPsec/IP            |         |
| שרת/לקוח HTTPS            | SSL/TLS |
| (SSL/TLS ,SMTPS (STARTTLS |         |
| SNMPv3                    |         |

\* עליך להשתמש בהתקן התחברות תואם IEEE802.1X.

## השימוש ביציאה עבור הסורק

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

כאשר השולח (הלקוח) הוא הסורק

| מספר יציאה | פרוטוקול            | יעד (שרת)    | שימוש  |
|------------|---------------------|--------------|--|
| 20         | FTP/FTPS (TCP)      | שרת FTP/FTPS | שליחת קובץ (כאשר משתמשים בסריקה לתיקית רשת מהסורק) |
| 21         |                     |              |  |
| 445        | SMB (TCP)           | שרת קבצים    |  |
| 137        | NetBIOS (UDP)       |              |  |
| 138        |                     |              |  |
| 139        | NetBIOS (TCP)       |              |  |
| 80         | פרוטוקול HTTP (TCP) | שרת WebDAV   |  |
| 443        | פרוטוקול HTTPS(TCP) |              |  |

| מספר יציאה | פרוטוקול                | יעד (שרת)         | שימוש  |
|------------|-------------------------|-------------------|--|
| 25         | SMTP (TCP)              | שרת SMTP          | שליחת דוא"ל (כאשר משתמשים בסריקה לדואר מהסורק)   |
| 465        | SMTP SSL/TLS (TCP)      |                   |  |
| 587        | SMTP STARTTLS (TCP)     |                   |  |
| 110        | (POP3 (TCP              | שרת POP           | חיבור POP לפני SMTP (כאשר משתמשים בסריקה לדואר מהסורק)   |
| 443        | HTTPS                   | שרת Epson Connect | כאשר משתמשים ב-Epson Connect   |
| 5222       | XMPP                    |                   |  |
| 389        | LDAP (TCP)              | שרת LDAP          | איסוף מידע על המשתמש (שימוש באנשי הקשר מהסורק)   |
| 636        | LDAP SSL/TLS (TCP)      |                   |  |
| 389        | LDAP STARTTLS (TCP)     |                   |  |
| 88         | Kerberos                | שרת KDC           | אימות משתמש בעת איסוף מידע על המשתמש (בעת השימוש באנשי הקשר מהסורק)<br>אימות משתמש בעת שימוש בפונקציה 'סרוק אל תיקית רשת' (SMB) מהסורק |
| 5357       | WSD (TCP)               | מחשב לקוח         | Control WSD  |
| 2968       | גילוי סריקה בלחיצה ברשת | מחשב לקוח         | חפש במחשב בעת ביצוע סריקה בלחיצה מתוך אפליקציה   |

כאשר השולח (הלקוח) הוא המחשב הלקוח

| מספר יציאה | פרוטוקול           | יעד (שרת) | שימוש   |
|------------|--------------------|-----------|---|
| 3289       | ENPC (UDP)         | סורק      | גלה את הסורק מתוך אפליקציה כגון EpsonNet Config, ומנהל התקן של הסורק.             |
| 161        | SNMP (UDP)         | סורק      | אסוף והגדר את מידע ה-MIB מתוך אפליקציה כגון EpsonNet Config, ומנהל התקן של הסורק. |
| 3702       | (WS-Discovery (UDP | סורק      | חיפוש סורק WSD  |
| 1865       | סריקת רשת (TCP)    | סורק      | העברת נתוני הסריקה מתוך אפליקציה  |
| 2968       | סריקה בלחיצה ברשת  | סורק      | איסוף נתוני העבודה בעת ביצוע סריקה בלחיצה מתוך אפליקציה                           |
| 80         | HTTP (TCP)         | סורק      | Web Config  |
| 443        | HTTPS (TCP)        |           |   |

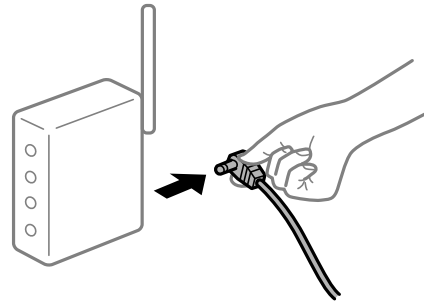
## פתרון בעיות

לא ניתן להתחבר לרשת  
הבעיה יכולה להיות אחת מהבעיות הבאות.

■ משהו השתבש בהתקני הרשת עבור חיבור Wi-Fi.

### פתרונות

כבה את ההתקנים שאתה רוצה לחבר אל הרשת. המתן בערך 10 שניות, ולאחר מכן הדלק את ההתקנים בסדר הבא: נתב אלחוטי, מחשב או התקן חכם, ואז את הסורק. קרב את הסורק והמחשב או ההתקן החכם אל הנתב האלחוטי כדי לסייע לתקשורת גלי הרדיו, ואז נסה לבצע שוב את הגדרות הרשת.



■ התקנים לא יכולים לקבל אותות מהנתב האלחוטי משום שהם מרוחקים מדי אלו מאלו.

### פתרונות

אחרי הזזת המחשב או ההתקן החכם והסורק קרוב יותר אל הנתב האלחוטי, כבה את הנתב האלחוטי, וחזור והדלק אותו.

■ כאשר משנים את הנתב האלחוטי, ההגדרות אינן תואמות את הנתב החדש.

### פתרונות

בצע שוב את הגדרות החיבור כך שהן תואמות את הנתב האלחוטי החדש.

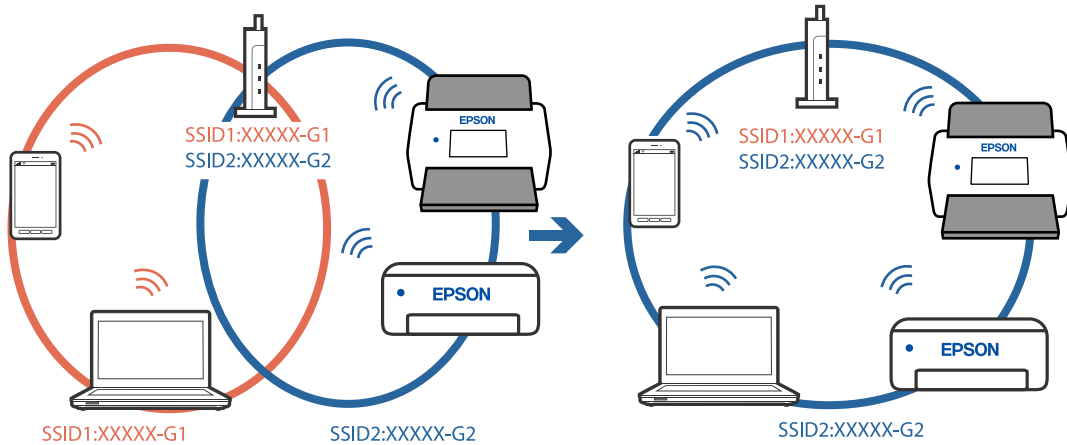
■ ה-SSIDים המחוברים מהמחשב או מההתקן החכם והמחשב שונים.

### פתרונות

כאשר אתה משתמש בנתבים אלחוטיים מרובים בעת ובעונה אחת או שיש לנתב האלחוטי SSIDים מרובים והתקנים שמחוברים ל-SSIDים שונים, אין ביכולתך להתחבר אל הנתב האלחוטי.



חבר את המחשב או את ההתקן החכם לאותו SSID של הסורק.



### מפריד פרטיות זמין בנתב האלחוטי.

#### פתרונות

למרבת הנתבים האלחוטיים יש תכונת מפריד פרטיות החוסם את התקשורת בין ההתקנים מחוברים. אם אין ביכולתך ליצור תקשורת בין הסורק לבין המחשב או התקן החכם אף על פי שהם מחוברים לאותה הרשת, השבת את מפריד הפרטיות בנתב האלחוטי. לפרטים נוספים, עיין במדריך שסופק עם הנתב האלחוטי.

### כתובת ה-IP הוקצתה באופן שגוי.

#### פתרונות

אם כתובת ה-IP שהוקצתה לסורק היא XXX.XXX.169.254, ומסכת תת-הרשת היא 255.255.0, אפשר שכתובת ה-IP לא הוקצתה נכונה. בחר הגדרות < הגדרות רשת > מתקדם < TCP/IP בלוח הבקרה של הסורק, ואז בדוק את כתובת ה-IP ואת מסכת תת-הרשת שהוקצו לסורק. אתחל שוב את הנתב האלחוטי או אפס את הגדרות הרשת עבור הסורק.

### קיימת בעיה בהגדרות הרשת במחשב.

#### פתרונות

נסה לגשת לכל אתר אינטרנט מהמחשב כדי לוודא שהגדרות הרשת של המחשב נכונות. אם אינך יכול לגשת לשום אתר אינטרנט, הרי שיש בעיה במחשב. בדוק את חיבור הרשת של המחשב. לפרטים, עיין בתיעוד שסופק עם המחשב.

### הסורק חובר באמצעות Ethernet תוך שימוש בהתקנים שתומכים ב-IEEE 802.3az (חיבור Ethernet בעל יעילות אנרגטית).

#### פתרונות

כאשר אתה מחבר את הסורק באמצעות Ethernet תוך שימוש בהתקנים התומכים ב-IEEE 802.3az (בעל יעילות אנרגטית Ethernet), אפשר שהבעיות הבאות תופענה בהתאם לרכות או לנתב שבו אתה משתמש.

- החיבור מאבד את היציבות שלו, הסורק מתחבר ומתנתק שוב ושוב.
  - לא ניתן להתחבר לסורק.
  - מהירות התקשורת מואטת.
- פעל בהתאם לצעדים הבאים כדי להשבית את IEEE 802.3az עבור הסורק, ואז חבר.
1. הסר את כבל ה-Ethernet המוחבר למחשב ולסורק.
  2. כאשר ה-IEEE 802.3az עבור המחשב מאופשר, השבת אותו. לפרטים, עיין בתיעוד שסופק עם המחשב.
  3. חבר את המחשב והסורק ישירות באמצעות כבל Ethernet.
  4. בסורק, בדוק את הגדרות הרשת.
- בחר הגדרות < הגדרות רשת < סטטוס הרשת < סטטוס רשת Wi-Fi/קווית.
5. בדוק את כתובת ה-IP של הסורק.
  6. במחשב, גש אל Web Config. הפעל דפדפן אינטרנט ולאחר מכן הזן את כתובת ה-IP של הסורק. ["הפעלת Web Config בדפדפן אינטרנט" בעמוד 36](#)
  7. בחר בלשונית Network < Wired LAN.
  8. בחר OFF עבור IEEE 802.3az.
  9. לחץ על Next.
  10. לחץ על OK.
  11. הסר את כבל ה-Ethernet המוחבר למחשב ולסורק.
  12. אם השבתת את IEEE 802.3az עבור המחשב בצעד 2, אפשר אותו.
  13. חבר את כבלי ה-Ethernet שהסרת בצעד 1 אל המחשב ואל הסורק. אם הבעיה עדיין נמשכת, אפשר שהתקנים אחרים חוץ מהסורק גורמים את הבעיה.

■ הסורק מכובה.

#### פתרונות

ודא שהסורק דלוק.  
 כמו כן, המתן עד שנורית המצב תפסיק להבהב — עדות לכך שהסורק מוכן לסרוק.

---

# תוכנה להתקנת הסורק

36.....Web Config

37.....Epson Device Admin

## Web Config

Web Config היא אפליקציה הפועלת בדפדפני אינטרנט כגון Internet Explorer ו-Safari, במחשב. באפשרותך לאשר את מצב הסורק או לשנות את הגדרות שירותי הרשת ואת הגדרות הסורק. מאחר והגישה והתפעול של הסורקים מתבצעים ישירות מתוך הרשת, ניתן להתקין סורק אחד בכל פעם. על מנת להשתמש ב-Web Config, חבר את המחשב שלך לאותה רשת כמו הסורק. הדפדפנים להלן נתמכים.

Microsoft Edge, Windows Internet Explorer 8 ואילך, \*Firefox, \*Chrome, \*Safari \*  
 \* השתמש בגרסה העדכנית ביותר.

## הפעלת Web Config בדפדפן אינטרנט

1. בדוק את כתובת ה-IP של הסורק.

בחר הגדרות < הגדרות רשת < סטטוס הרשת בלוח הבקרה של הסורק. לאחר מכן בחר את סטטוס שיטת החיבור הפעילה (סטטוס רשת Wi-Fi/קווית או את מצב Wi-Fi Direct) כדי לאשר את כתובת ה-IP של הסורק.

2. הפעל דפדפן אינטרנט ממחשב או מהתקן חכם ולאחר מכן הזן את כתובת ה-IP של הסורק. פורמט:

IPv4: http://:כתובת ה-IP של הסורק/

IPv6: http://:כתובת ה-IP של הסורק/

דוגמאות:

IPv4: http://192.168.100.201/

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

לתשומת לבך:

מאחר והסורק משתמש בתעודה עם חתימה עצמית בעת גישה ל-HTTPS, מוצגת אזהרה בדפדפן כאשר אתה מפעיל את Web Config; אין בכך כדי להצביע על בעיה וניתן להתעלם מכך בבטחה.

3. היכנס בתור מנהל כדי לשנות את הגדרות הסורק.

לחץ Administrator Login בפינה הימנית העליונה של המסך. הזן את ה User Name ואז Current password, ואז לחץ על OK.

לתשומת לבך:

להלן מוצגים הערכים הראשוניים עבור מידע מנהל Web Config.

שם משתמש: ללא (ריק)

סיסמה: המספר הסידורי של הסורק

כדי למצוא את המספר הסידורי, בדוק את התווית המחוברת אל גב הסורק.

אם מוצגת Administrator Logout בפינה הימנית העליונה של המסך, הרי שכבר נכנסת בתור מנהל.

## הפעלת Web Config ב-Windows

בעת חיבור של מחשב לסורק באמצעות WSD, בצע את הפעולות שלהלן להפעלת Web Config.

1. פתח את רשימת הסורקים במחשב.

Windows 10

לחץ על לחצן 'התחל' ואז בחר מערכת < Windows לוח הבקרה < הצג התקנים ומדפסות תחת חומרה וקול.

Windows 8.1/Windows 8

בחר שולחן עבודה < הגדרות < לוח בקרה < הצג התקנים ומדפסות ב חומרה וקול (או חומרה).

Windows 7

לחץ על לחצן 'התחל' ובחר לוח הבקרה < הצג התקנים ומדפסות תחת חומרה וקול.

2. לחץ לחיצת עכבר ימנית על הסורק שלך ובחר מאפיינים.

3. בחר בלשונית שירותי אינטרנט ולחץ על ה-URL.

מאחר והסורק משתמש בתעודה עם חתימה עצמית בעת גישה ל-HTTPS, מוצגת אזהרה בדפדפן כאשר אתה מפעיל את Web Config; אין בכך כדי להצביע על בעיה וניתן להתעלם מכך בבטחה.

לתשומת לבך:

להלן מוצגים הערכים הראשוניים עבור מידע מנהל Web Config.

שם משתמש: ללא (ריק)

סיסמה: המספר הסידורי של הסורק

כדי למצוא את המספר הסידורי, בדוק את התווית המחוברת אל גב הסורק.

אם מוצגת Administrator Logout בפינה הימנית העליונה של המסך, הרי שכבר נכנסת בתור מנהל.

## Epson Device Admin

Epson Device Admin היא אפליקציה רב-תפקודית שמאפשרת לך לנהל התקנים ברשת.

תוכל להשתמש בתבניות תצורה כדי להחיל הגדרות מאוחדות על סורקים רבים ברשת. שיטה זו מתאימה להתקנה וניהול של סורקים רבים.

תוכל להוריד את Epson Device Admin מאתר התמיכה של Epson. עבור פרטים כיצד להשתמש באפליקציה זו, עיין בתיעוד או בעזרה עבור Epson Device Admin.

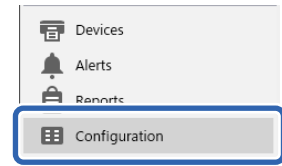
## תבנית תצורה

### יצירת תבנית התצורה

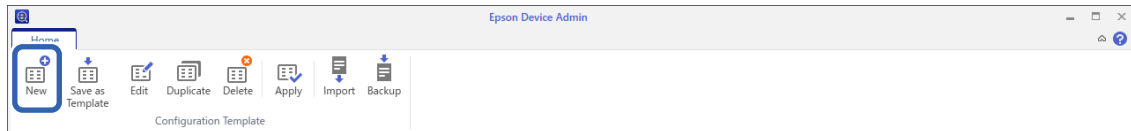
צור מחדש את תבנית התצורה.

1. הפעל את Epson Device Admin.

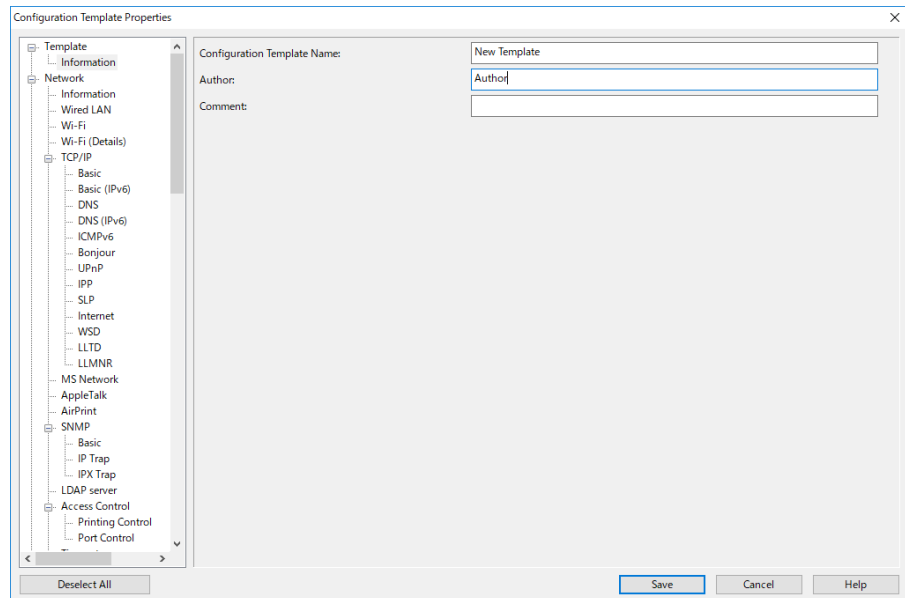
2. בחר **Configuration** בתפריט המשימות בסרגל הצד.



3. בחר **New** בתפריט הסרט.



4. הגדר כל פריט.



| פריט                        | הסבר  |
|-----------------------------|---|
| Configuration Template Name | שם תבנית התצורה.<br>הזן עד 1, 24 תווים ב-Unicode (קידוד UTF-8).     |
| Author                      | מידע על יוצר התבנית.<br>הזן עד 1, 24 תווים ב-Unicode (קידוד UTF-8). |
| Comment                     | הזן מידע שרירותי.<br>הזן עד 1, 24 תווים ב-Unicode (קידוד UTF-8).    |

5. בחר את הפריטים שברצונך להגדיר משמאל.

לתשומת לבך:

לחץ על פריטי התפריט משמאל כדי לעבור לכל מסך. הערך שהוגדר נשמר אם אתה מחליף את המסך אך לא אם תבטל את המסך. כשתסיים את כל ההגדרות, לחץ על *Save*.

## החלת תבנית התצורה

החל את תבנית התצורה השמורה על הסורק. הוחלו הפריטים שנבחרו בתבנית. אם הפונקציה המתאימה אינה נמצאת בסורק המטרה, היא לא תוחל.

לתשומת לבך:

כאשר מגדירים סיסמת מנהל עבור סורק, יש להגדיר את תצורת הסיסמה מראש.

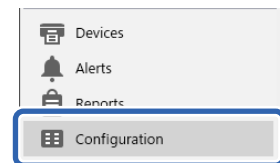
1. בתפריט הסרט של מסך רשימת ההתקנים, בחר *Options < Password manager*.

2. בחר *Enable automatic password management*, ואז לחץ *Password manager*.

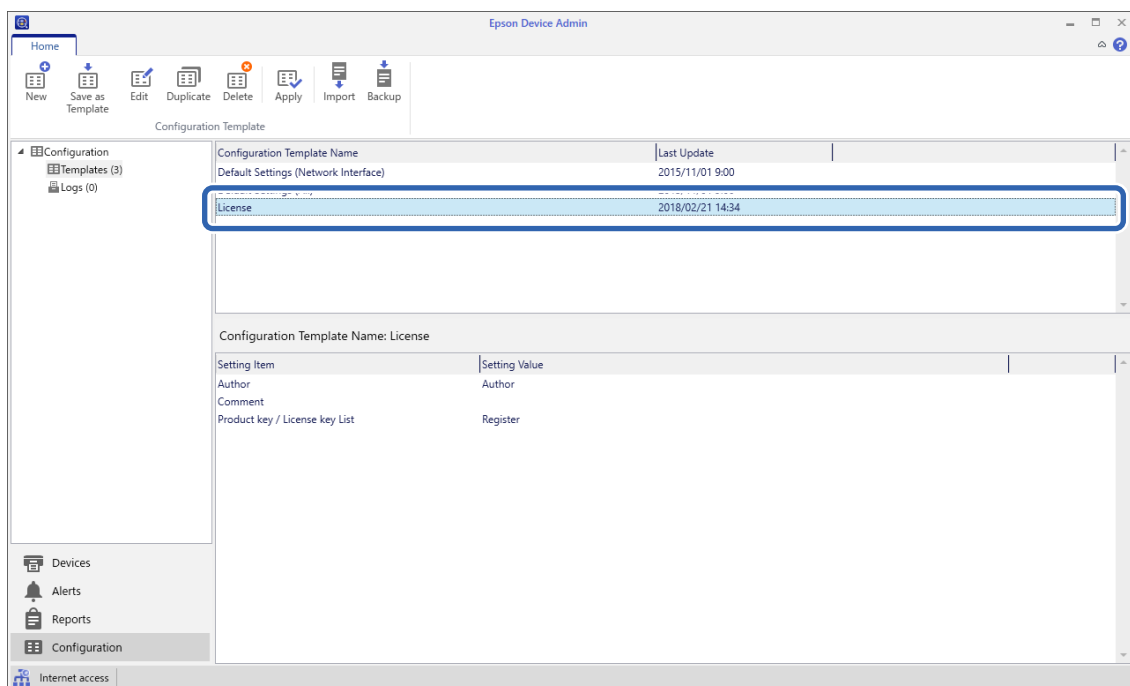
3. בחר את הסורק המתאים ואז לחץ *Edit*.

4. הגדר את הסיסמה ואז לחץ *OK*.

1. בחר **Configuration** בתפריט המשימות בסרגל הצד.



2. בחר את תבנית התצורה שברצונך להחיל מתוך **Configuration Template Name**.



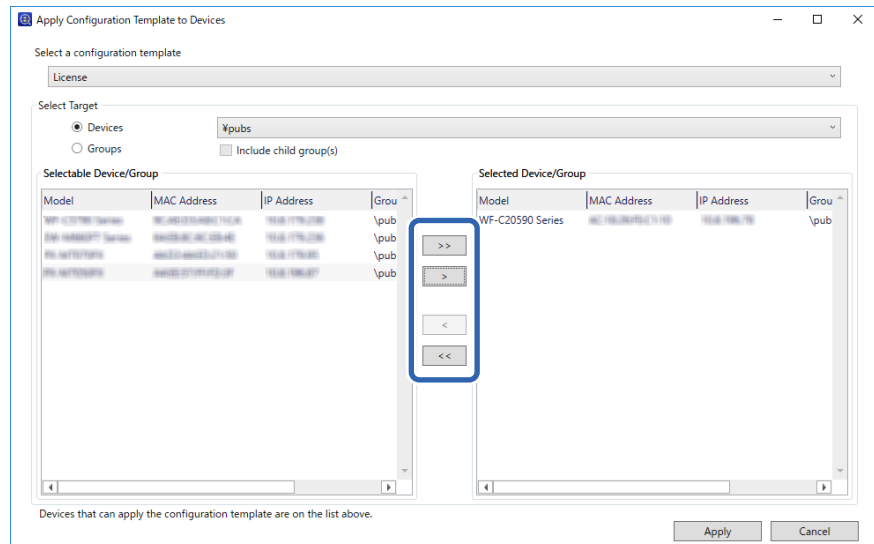
3. לחץ **Apply** בתפריט הסרט.  
מוצג מסך בחירת ההתקן.



4. בחר את תבנית התצורה שברצונך להחיל.  
לתשומת לבך:

- כאשר אתה בוחר **Devices** וקבוצות המכילות התקנים מתוך התפריט הנפתח, כל התקן מוצג.
- קבוצות מוצגות כאשר אתה בוחר **Groups**. בחר **Include child group(s)** כדי לבחור באופן אוטומטי קבוצות צאצא בתוך הקבוצה הנבחרת.

5. העבר את הסורק או את הקבוצות שעליהם ברצונך להחיל את התבנית אל **Selected Device/Group**.



6. לחץ על **Apply**.

יוצג מסך אישור של תבנית התצורה שיש להחיל.

7. לחץ **OK** כדי להחיל את תבנית התצורה.

8. כאשר תוצג הודעה המודיעה לכם שהנהול הושלם, לחץ על **OK**.

9. לחץ על **Details** ובדוק את המידע.

כאשר  מוצג בפריטים שהחלת, ההחלה הושלמה בהצלחה.

10. לחץ על **Close**.



---

# ההגדרות הדרושות לסריקה

42..... הגדרת שרת דואר.

45..... הגדרת תיקיית רשת משותפת.

61..... הפיכת אנשי קשר לזמינים.

71..... השימוש ב-Document Capture Pro Server.

72..... הגדרת AirPrint.

72..... בעיות בעת הכנת סריקת רשת.

## הגדרת שרת דואר

הגדר את שרת הדוא"ל מתוך Web Config. כאשר הסורק מסוגל לשלוח דוא"ל באמצעות הגדרת שרת הדוא"ל, מתאפשרות הפעולות הבאות.

העברת תוצאות הסריקה באמצעות הדוא"ל

מקבל הודעת דוא"ל מהסורק

בדוק להלן לפני ביצוע ההגדרה.

הסורק מחובר לרשת שיכולה לגשת לשרת דוא"ל.

מידע על הגדרת הדוא"ל במחשב המשתמש באותו שרת דוא"ל כמו הסורק.

לתשומת לבך:

כאשר אתה משתמש בשרת הדוא"ל באינטרנט, אשר את מידע ההגדרה מהספק או מהאינטרנט.

תוכל גם להגדיר את שרת הדוא"ל מלוח הבקרה של הסורק. הגישה מתבצעת כדלהלן.

הגדרות < הגדרות רשת < מתקדם < שרת דוא"ל < הגדרות שרת

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

2. הזן ערך עבור כל פריט.

3. בחר OK.

ההגדרות שבחרת תוצגנה.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## פריטי הגדרות שרת דואר

| הגדרות והסבר  | פריטים                |                       |
|---|-----------------------|-----------------------|
| ציין את שיטת האימות עבור גישת הסורק אל שרת הדואר.   | Authentication Method |                       |
| אימות מושבת בתקשורת עם שרת דואר.  |                       | Off                   |
| מחייב תמיכה של שרת הדואר באימות SMTP.   |                       | SMTP AUTH             |
| אם בחרת בשיטה זו, הגדר את שרת POP3.   | POP before SMTP       | Authenticated Account |
| אם אתה בוחר SMTP AUTH או POP before SMTP בתור Authentication Method, הזן את שם החשבון באורך בין 5 ל-25 תווים ב-ASCII. | ((0x20-0x7E           |                       |

| הגדרות והסבר   | פריטים                  |
|--|-------------------------|
| אם אתה בוחר SMTP AUTH או POP before SMTP בתור Authentication Method, הזן את הסיסמה המאומתת באורך בין 0 לבין 20 תווים ב-ASCII (0x20-0x7E).                            | Authenticated Password  |
| הזן את כתובת הדוא"ל של השולח. הזן בין 0 ל-255 תווי ASCII (0x20-0x7E) למעט: ( ) > < [ ] ; ¥. התו הראשון לא יכול להיות נקודה ".".                                      | Sender's Email Address  |
| הזן בין 0 ל-255 תווים מסוג אותיות A-Z, a-z, מספרים, 0-9, נקודה (.) ומקף (-). תוכל להשתמש בתבנית IPv4 או FQDN.  | SMTP Server Address     |
| הזן מספר בין 1 ל-65535.  | SMTP Server Port Number |
| ציין את שיטת החיבור המאובטח לשרת הדואר האלקטרוני.  | Secure Connection       |
| אם אתה בוחר POP before SMTP ב-Authentication Method, שיטת החיבור מוגדרת כ-None.  | None                    |
| אפשרות זו זמינה כאשר Authentication Method מוגדר כ-Off או כ-SMTP AUTH.   | SSL/TLS                 |
| אפשרות זו זמינה כאשר Authentication Method מוגדר כ-Off או כ-SMTP AUTH.   | STARTTLS                |
| האישור מאומת כאשר מצב זה זמין. מומלץ להגדיר אותו כ-Enable.   | Certificate Validation  |
| 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 Address     |
| אם אתה בוחר POP before SMTP כ-Authentication Method, הזן מספר בין 1 ל-65535.   | POP3 Server Port Number |

## בדיקת חיבור לשרת דואר

תוכל לבדוק את החיבור אל שרת הדואר באמצעות ביצוע בדיקת החיבור.

1. גש אל Web Config ובחר את לשונית Network < Email Server < Connection Test.

2. בחר Start.

חיבור הבדיקה עם שרת הדואר יתחיל. אחרי הבדיקה, יוצג דו"ח בדיקה.

לתשומת לבך:

תוכל גם לבדוק את החיבור אל שרת הדוא"ל מתוך לוח הבקרה. הגישה מתבצעת כדלהלן.

הגדרות < הגדרות רשת < מתקדם < שרת דוא"ל < בדיקת חיבור

מקורות בדיקה לחיבור שרת דואר

| סיבה  | הודעות   |
|---|--|
| הודעה זו מופיעה כאשר הקשר עם השרת הצליח.  | Connection test was successful.  |
| <p>הודעה זו מופיעה כאשר</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> הסורק אינו מחובר לרשת</li> <li><input type="checkbox"/> שרת SMTP מושבת</li> <li><input type="checkbox"/> חיבור הרשת נותק בזמן התקשרות</li> <li><input type="checkbox"/> הנתונים שהתקבלו אינם שלמים</li> </ul> | SMTP server communication error. Check the following. - Network Settings   |
| <p>הודעה זו מופיעה כאשר</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> הסורק אינו מחובר לרשת</li> <li><input type="checkbox"/> שרת POP3 מושבת</li> <li><input type="checkbox"/> חיבור הרשת נותק בזמן התקשרות</li> <li><input type="checkbox"/> הנתונים שהתקבלו אינם שלמים</li> </ul> | POP3 server communication error. Check the following. - Network Settings   |
| <p>הודעה זו מופיעה כאשר</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> החיבור לשרת DNS נכשל</li> <li><input type="checkbox"/> רזולוציית השם עבור שרת SMTP נכשלה</li> </ul>   | An error occurred while connecting to SMTP server. Check the followings. - SMTP Server Address - DNS Server                      |
| <p>הודעה זו מופיעה כאשר</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> החיבור לשרת DNS נכשל</li> <li><input type="checkbox"/> נכשל זיהוי שם עבור שרת POP3</li> </ul>   | An error occurred while connecting to POP3 server. Check the followings. - POP3 Server Address - DNS Server                      |
| הודעה זו מופיעה כאשר אימות שרת SMTP נכשל.   | SMTP server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password |
| הודעה זו מופיעה כאשר אימות שרת POP3 נכשל.   | POP3 server authentication error. Check the followings. - Authentication Method - Authenticated Account - Authenticated Password |
| הודעה זו מופיעה כאשר אתה מנסה ליצור תקשורת עם פרוטוקולים שאין להם תמיכה.  | Unsupported communication method. Check the followings. - SMTP Server Address - SMTP Server Port Number                          |

| סיבה  | הודעות   |
|---|--|
| הודעה זו מופיעה כאשר מתרחשת אי-התאמת SMTP בין שרת לבין לקוח, או כאשר השרת אינו תומך בחיבור SMTP מאובטח (חיבור SSL).           | Connection to SMTP server failed. Change Secure Connection to None.                      |
| הודעה זו מופיעה כאשר מתרחשת אי-התאמת SMTP בין שרת לבין לקוח, או כאשר השרת מבקש להשתמש בחיבור SSL/TLS עבור חיבור SMTP מאובטח.  | Connection to SMTP server failed. Change Secure Connection to SSL/TLS.                   |
| הודעה זו מופיעה כאשר מתרחשת אי-התאמת SMTP בין שרת לבין לקוח, או כאשר השרת מבקש להשתמש בחיבור STARTTLS עבור חיבור SMTP מאובטח. | Connection to SMTP server failed. Change Secure Connection to STARTTLS.                  |
| הודעה זו מופיעה כאשר התאריך והשעה של הסורק אינם נכונים או שתוקף התעודה פג.  | The connection is untrusted. Check the following. - Date and Time                        |
| הודעה זו מופיעה כאשר אין לסורק תעודת שורש התואמת לשרת או כאשר לא יובאה CA Certificate.  | The connection is untrusted. Check the following. - CA Certificate                       |
| הודעה זו מופיעה כאשר התעודה שהושגה פגומה.   | The connection is not secured.   |
| הודעה זו מופיעה כאשר שיטת אימות בלתי תואמת מתרחשת בין השרת לבין לקוח. הלקוח תומך ב-SMTP AUTH.                                 | SMTP server authentication failed. Change Authentication Method to SMTP-AUTH.            |
| הודעה זו מופיעה כאשר שיטת אימות בלתי תואמת מתרחשת בין השרת לבין לקוח. הלקוח אינו תומך ב-SMTP AUTH.                            | SMTP server authentication failed. Change Authentication Method to POP before SMTP.      |
| הודעה זו מופיעה כאשר כתובת הדוא"ל שצוינה עבור השולח שגויה.  | Sender's Email Address is incorrect. Change to the email address for your email service. |
| הודעה זו מופיעה כאשר הסורק תפוס.  | Cannot access the product until processing is complete.                                  |

## הגדרת תיקיית רשת משותפת

הגדרת תיקיית רשת משותפת כדי לשמור את התמונה הסרוקה. בעת שמירת קובץ לתיקייה, הסורק נכנס למערכת כמשתמש של המחשב שבו נוצרה התיקייה.

## יצירת התיקה המשותפת

מידע קשור

- ← "לפני יצירת התיקה המשותפת" בעמוד 46
- ← "בדיקת פרופיל הרשת" בעמוד 46
- ← "המיקום שבו יוצרים את התיקה המשותפת ודוגמה של אבטחה" בעמוד 46
- ← "הוספת קבוצה או משתמש המאפשרים גישה" בעמוד 58

## לפני יצירת התיקה המשותפת

לפני יצירת התיקה המשותפת, בדוק את הדברים הבאים.

הסורק מחובר לרשת שממנה הוא יכול לגשת למחשב שבו תיווצר התיקה המשותפת.


שם המחשב שבו תיווצר התיקה המשותפת אינו כולל תו רב-בייטים.

### חשוב!

אם שם המחשב כולל תו רב-בייטים, יש אפשרות ששמירת הקובץ לתיקה המשותפת תיכשל. במקרה זה, עבור למחשב שאינו כולל תו רב-בייטים בשמו או שנה את שם המחשב. בעת שינוי שם המחשב, ודא לאשר זאת מראש עם המנהל משום ששינוי זה עלול להשפיע על כמה הגדרות, כגון ניהול המחשב, גישה למשאבים וכו'.

## בדיקת פרופיל הרשת

במחשב שבו תיווצר התיקה המשותפת, בדוק אם שיתוף התיקה זמין.

1. כנס למחשב שבו תיווצר התיקה המשותפת על ידי חשבון משתמש שיש לו סמכות מנהל.
2. בחר לוח הבקרה < רשת ואינטרנט < מרכז רשת ושיתוף.
3. לחץ שנה הגדרות שיתוף מתקדמות, ואז לחץ  עבור הפרופיל (פרופיל נוכחי) בפרופילים המוצגים של הרשת.
4. בדוק אם האפשרות הפעל שיתוף קבצים ומדפסת נבחרה בשיתוף קבצים ומדפסת. אם היא כבר נבחרה, לחץ ביטול וסגור את החלון. כאשר אתה משנה את ההגדרות, לחץ שמור שינויים וסגור את החלון.

## המיקום שבו יוצרים את התיקה המשותפת ודוגמה של אבטחה

האבטחה והנוחות תלויים במיקום שבו יוצרים את התיקה המשותפת.

כדי להפעיל את התיקה המשותפת מסורקים או מחשבים אחרים, יש צורך בהרשאות הקריאה והשינוי הבאות עבור התיקה.

לשונית שיתוף < שיתוף מתקדם < הרשאות  
שולט בהרשאות הגישה לרשת של התיקיה המשותפת.

הרשאת גישה של לשונית אבטחה  
שולט בהרשאות הגישה לרשת והגישה המקומית של התיקיה המשותפת.

כאשר אתה מגדיר כל אחד עובר התיקיה המשותפת שנוצרה בשולחן העבודה, כדוגמה ליצירת תיקיה משותפת, תותר הגישה לכל המשתמשים שיכולים לגשת למחשב.

עם זאת, משתמש שאין לו רשות לכך לא יכול לגשת אליהם משום ש(התיקיה) בשולחן העבודה נמצאת תחת שליטת תיקית המשתמש, ולכן הגדרות האבטחה של תיקית המשתמש מועברות לה בירושה. משתמש שיש לו הרשאת גישה בלשונית אבטחה (במקרה זה מדובר במשתמש שנכנס למערכת והוא המנהל) יוכל לבצע פעולות בתיקיה.

ראה להלן, כיצד ליצור את המיקום המתאים.

דוגמה זו מתייחסת ליצירה של תיקיית "scan\_folder".

מידע קשור

← "דוגמה של הגדרת תצורה עבור שרתי קבצים" בעמוד 47

← "דוגמה של הגדרת תצורה עבור מחשב אישי" בעמוד 53

### דוגמה של הגדרת תצורה עבור שרתי קבצים

הסבר זה הוא דוגמה ליצירת התיקיה המשותפת בשורש הכונן במחשב משותף, כגון שרת הקבצים בהתאם לתנאי הבא.

צור גישה למשתמשים שניתן לשלוט בהם, כגון אדם שיש לו אותו תחום כמו מחשב כדי ליצור תיקיה משותפת, יכול לגשת לתיקיה המשותפת.

הגדרת תצורה זו כאשר תתיר למשתמש כלשהו לקרוא ולכתוב אל התיקיה המשותפת במחשב, כגון שרת הקבצים והמחשב המשותף.

מקום ליצירת תיקיה משותפת: שורש הכונן

נתיב התיקיה: scan\_folder\C

הרשאת גישה באמצעות הרשת (שתף הרשאות): כולם

הרשאת גישה במערכת קבצים (אבטחה): משתמשים מאומתים

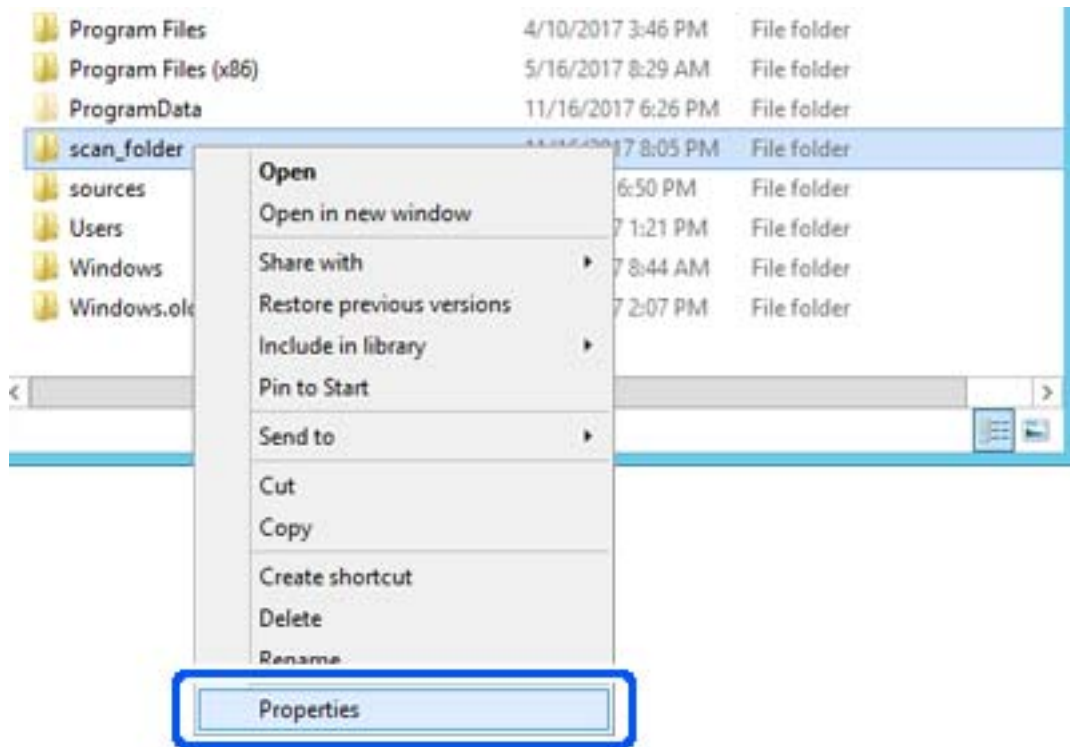
1. כנס למחשב שבו תיווצר התיקיה המשותפת על ידי חשבון משתמש שיש לו סמכות מנהל.

2. הפעל את סייר הקבצים.

3. צור את התיקיה בשורש הכונן, ואז קרא לה "scan\_folder".

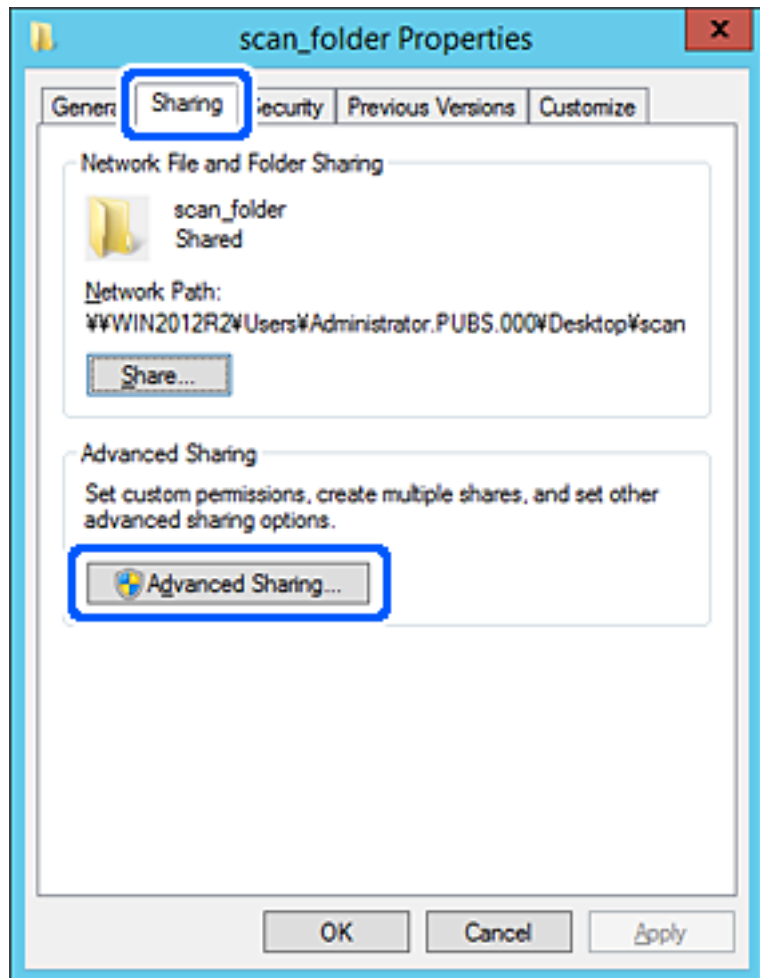
עבור שם התיקיה, הזן בין 1 ל-12 - תווים אלפנומריים. אם תחרוג מגבול התווים עבור שם התיקיה, אפשר שלא תוכל לגשת אליה באופן רגיל בסביבה מגוונת.

4- לחץ לחיצה ימנית על התיקה, ואז בחר תכונות.

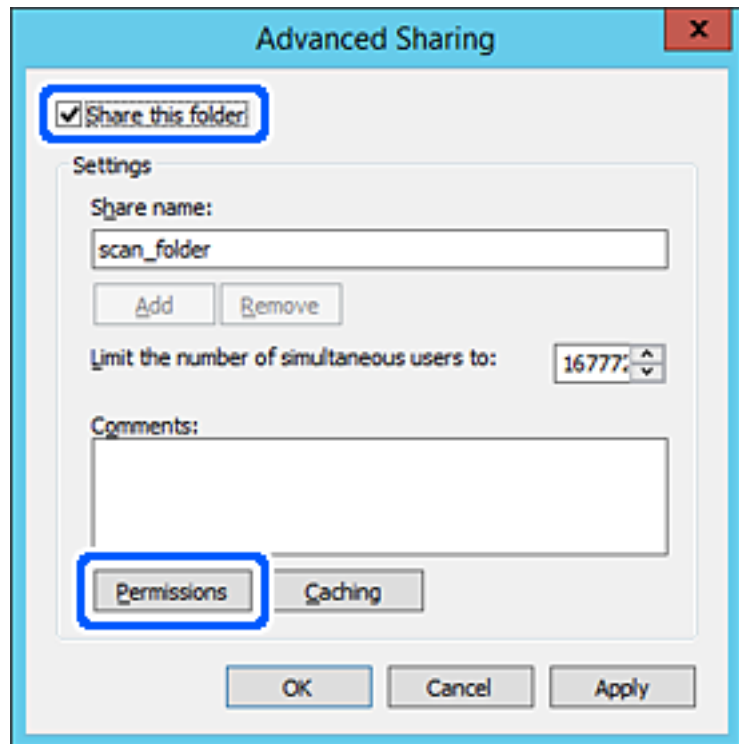




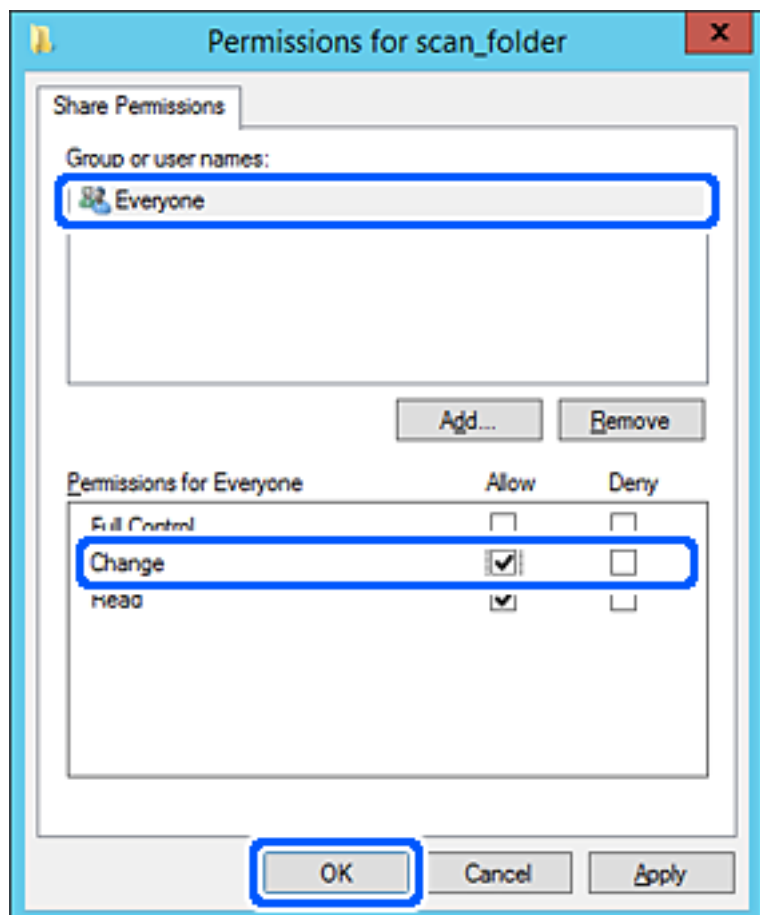
5. לחץ שיתוף מתקדם בלשונית שיתוף.



6. בחר שתף תיקיה זו, ואז לחץ הרשאות.

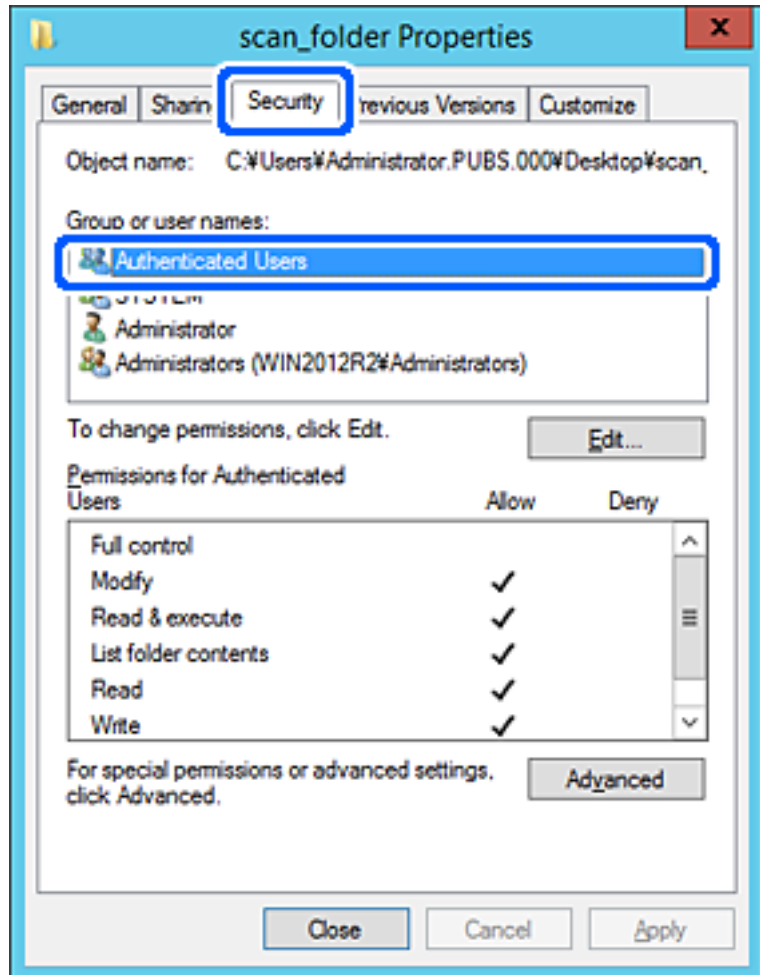


7. בחר בקבוצת כולם מתוך קבוצה או שמות משתמשים, בחר אפשר בתוך שנה, ואז לחץ על OK.



8. לחץ OK.

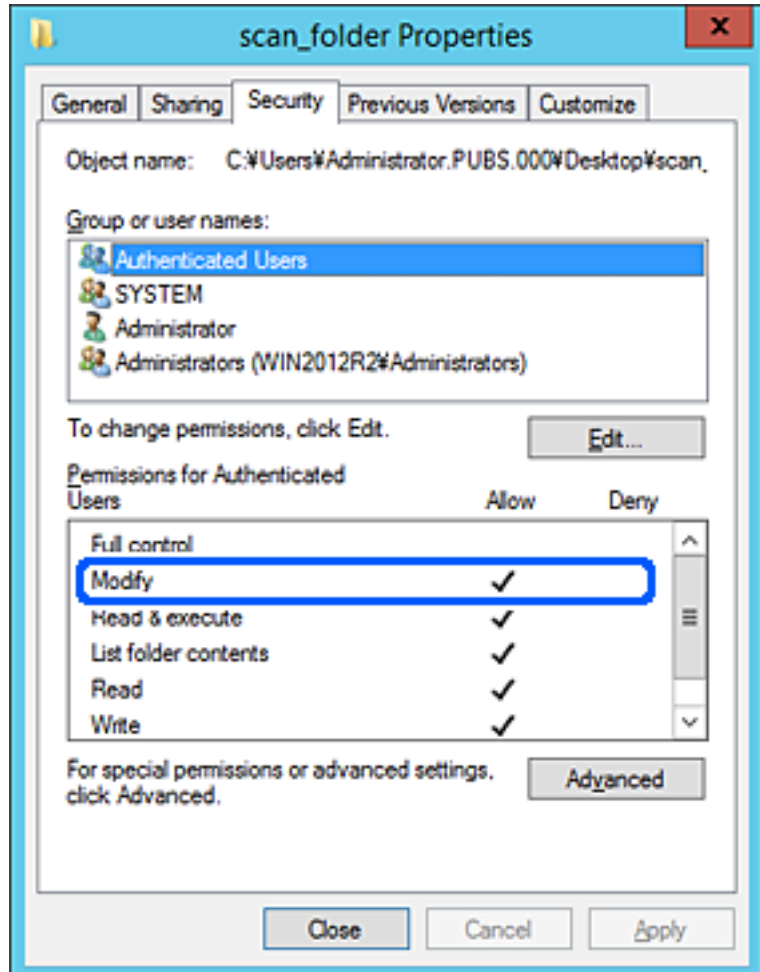
9. בחר בלשונית אבטחה ואז בחר משתמשים מאומתים בתוך קבוצה או שמות משתמשים.



"משתמשים מאומתים" היא הקבוצה המיוחדת שכוללת את כל המשתמשים שיכולים להיכנס לתוך התחום או המחשב. קבוצה זו מוצגת רק כאשר התיקיה נוצרה ישירות מתחת לתיקית השורש.

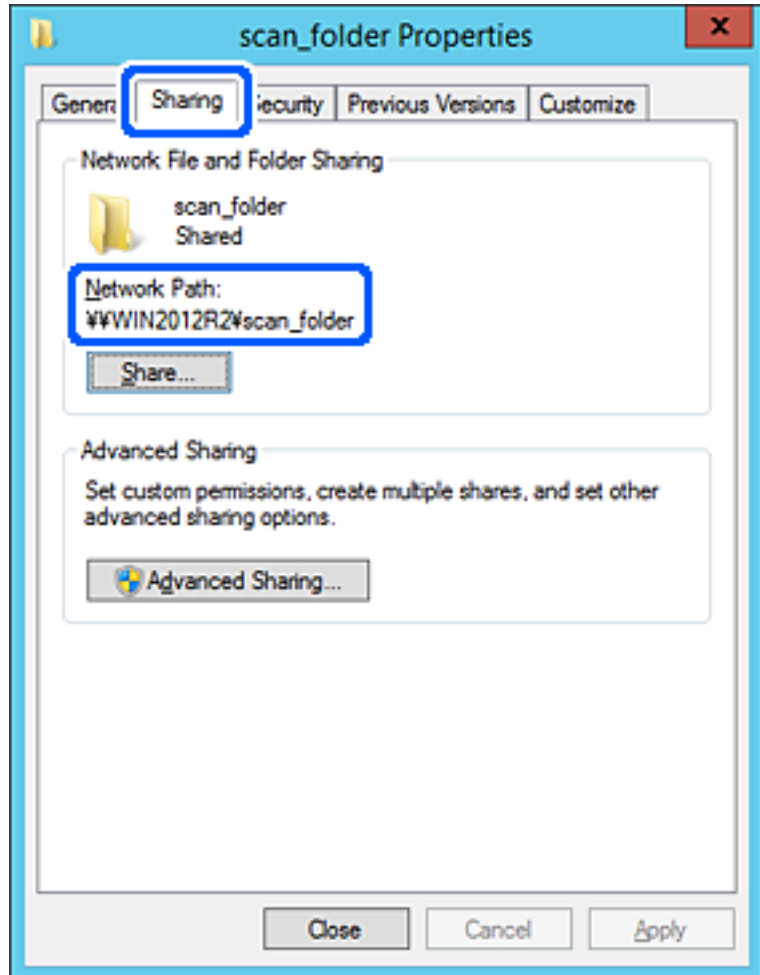
אם אין היא מוצגת, תוכל להוסיף אותה באמצעות לחיצה על ערוך. לפרטים נוספים, עיין במידע קשור.

10. ודא ש התר או שנה נבחרו בתוך הרשאות למשתמשים מאומתים.  
 אם הוא לא נבחר, בחר משתמשים מאומתים, לחץ ערוך, בחר התר או שנה בתוך הרשאות למשתמשים מאומתים, ואז לחץ OK.



11. בחר בלשונית שיתוף.

מוצג נתיב הרשת של התיקה המשותפת. משתמשים בזה כאשר רושמים אל אנשי הקשר של הסורק. אנא רשום זאת.



12. לחץ OK או סגור כדי לסגור את המסך.

בדוק אם ניתן לכתוב או לקרוא את הקובץ בתיקה המשותפת ממחשבים השייכים לאותו תחום.

מידע קשור

- ← "הוספת קבוצה או משתמש המאפשרים גישה" בעמוד 58
- ← "רישום יעד לאנשי קשר באמצעות Web Config" בעמוד 62

### דוגמה של הגדרת תצורה עבור מחשב אישי

הסבר זה הוא דוגמה ליצירת תיקיה משותפת על שולחן העבודה של המשתמש המחובר כרגע למחשב. המשתמש שנכנס למחשב ויש לו סמכות מנהל יכול לגשת לתיקה בשולחן העבודה ולתיקיית הקבצים הנמצאים תחת תיקיית המשתמש.

הגדרת תצורה זו כאשר אינך מתיר למשתמש אחר לקרוא ולכתוב לתיקה המשותפת במחשב אישי.

☐ מקום ליצירת תיקיה משותפת: שולחן עבודה

□ נתיב התיקיה: Users\xxxx\Desktop\scan\_folder\C:

□ הרשאת גישה באמצעות הרשת (שתף הרשאות): כולם

□ הרשאות גישה במערכת הקבצים (אבטחה): 'אל תוסיף' או 'הוסף' שמות משתמשים/קבצים כדי להתיר גישה

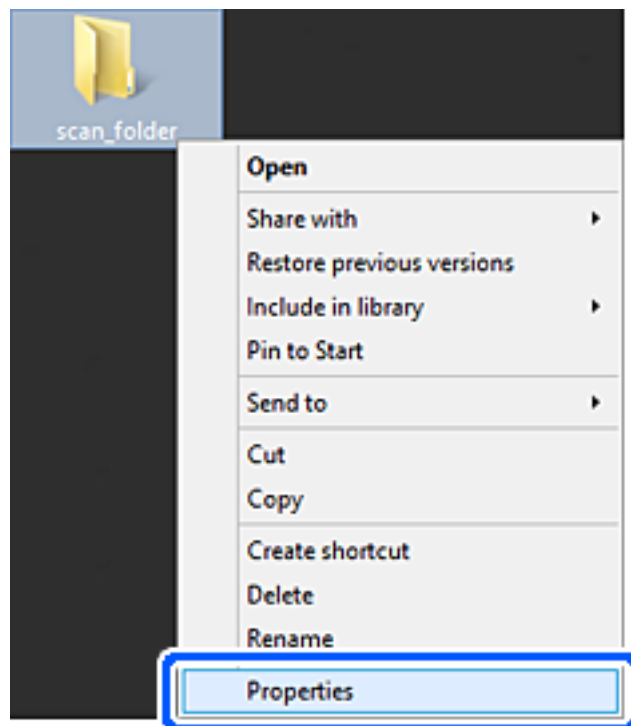
1. כנס למחשב שבו תיווצר התיקיה המשותפת על ידי חשבון משתמש שיש לו סמכות מנהל.

2. הפעל את סייר הקבצים.

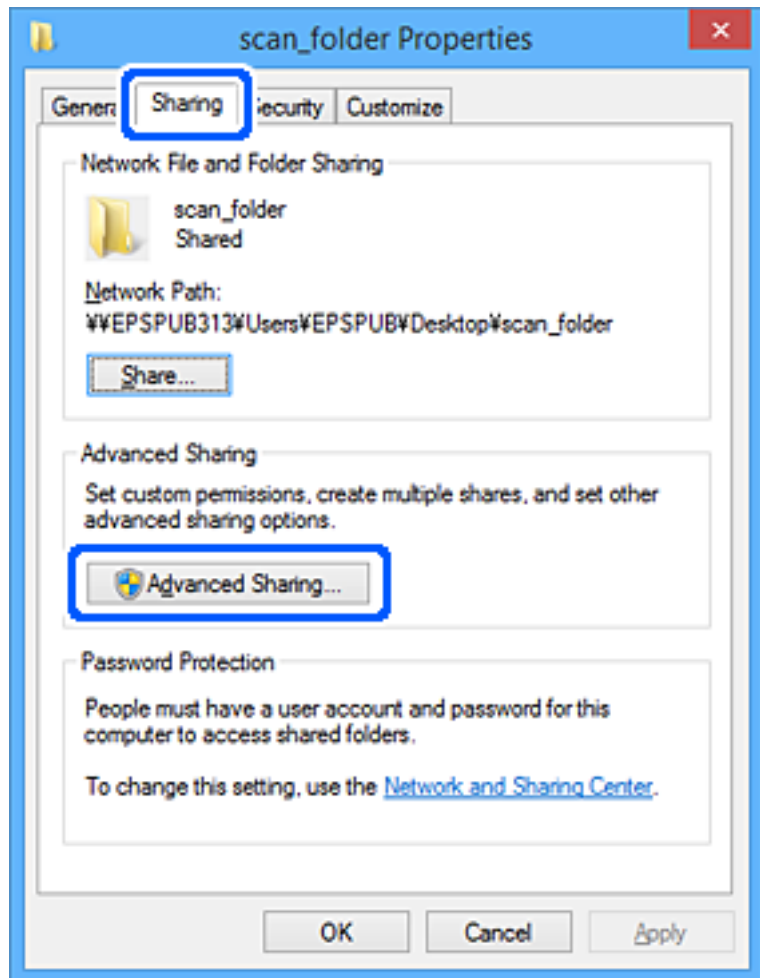
3. צור את התיקיה בשולחן העבודה, ואז קרא לה "scan\_folder".

עבור שם התיקיה, הזן בין 1 ל-12 תווים אלפנומריים. אם תחרוג מגבול התווים עבור שם התיקיה, אפשר שלא תוכל לגשת אליה באופן רגיל בסביבה מגוונת.

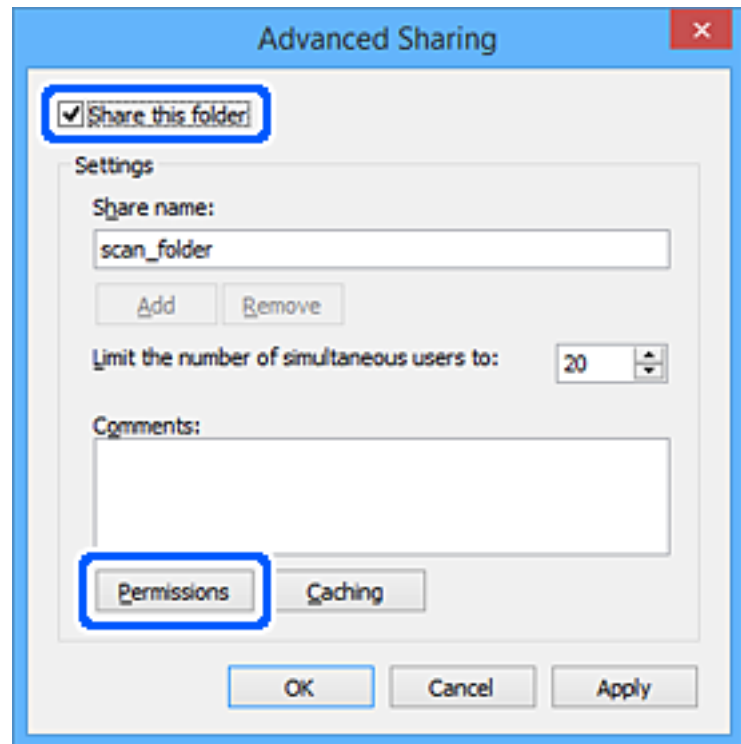
4. לחץ לחיצה ימנית על התיקיה, ואז בחר תכונות.



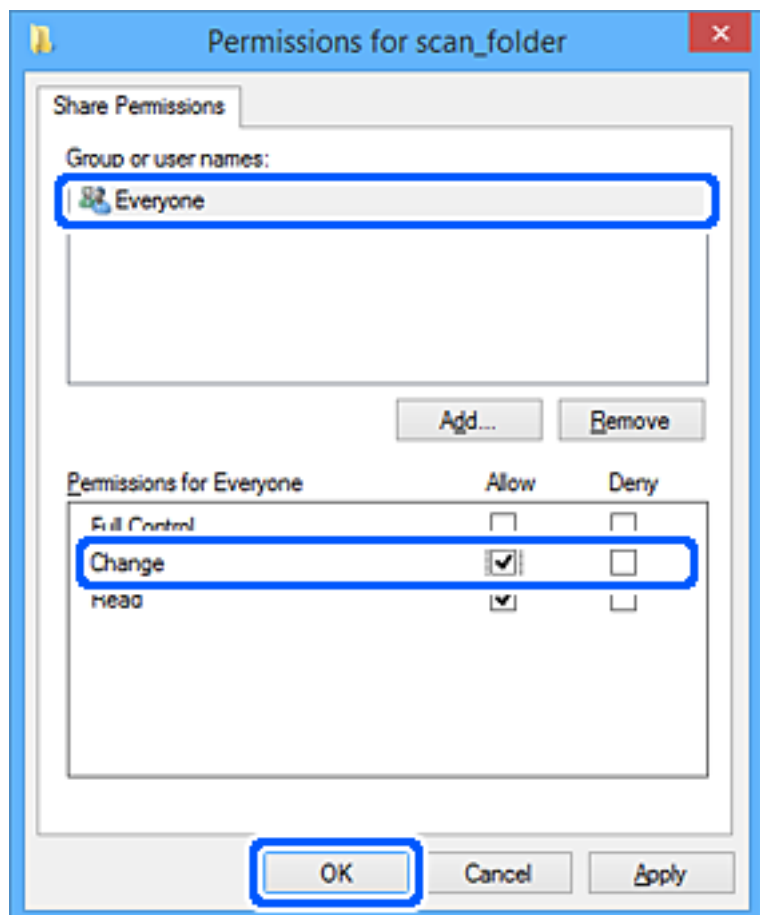
5. לחץ שיתוף מתקדם בלשונית שיתוף.



6. בחר שתף תיקיה זו, ואז לחץ הרשאות.



7. בחר בקבוצת כולם מתוך קבוצה או שמות משתמשים, בחר אפשר בתוך שנה, ואז לחץ על OK.





8. לחץ OK.

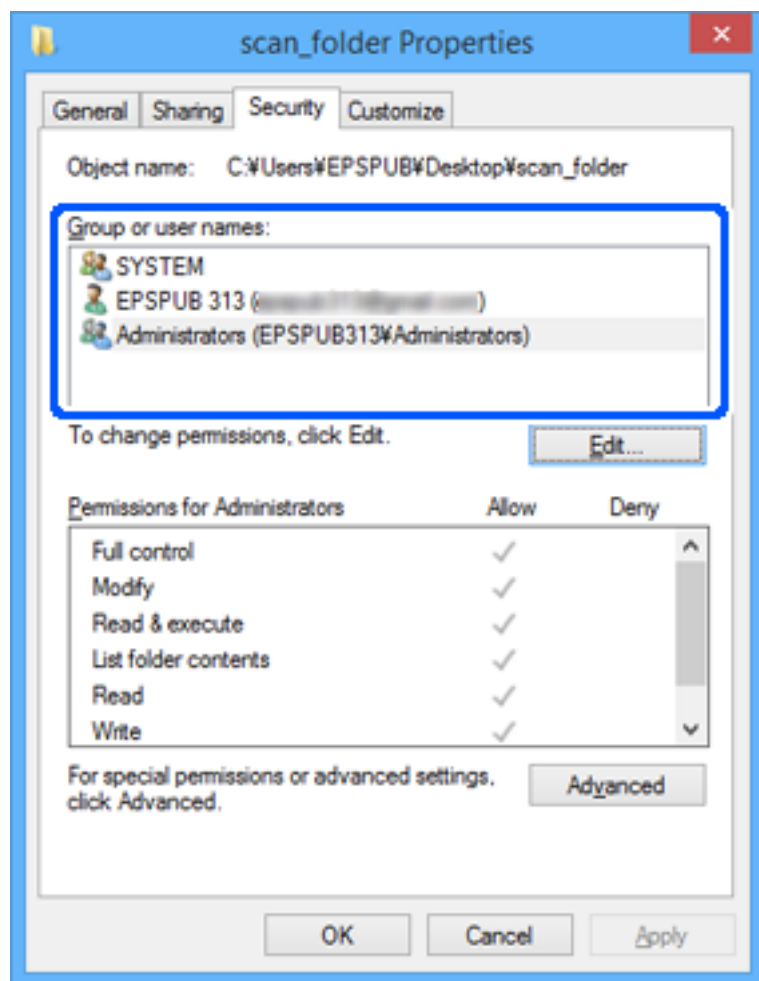
9. בחר בלשונית אבטחה.

10. בדוק את הקבוצה או המשתמש בתוך קבוצה או שמות משתמשים.

הקבוצה או המשתמש המוצגים כאן יכולים לגשת לתיקיה המשותפת.

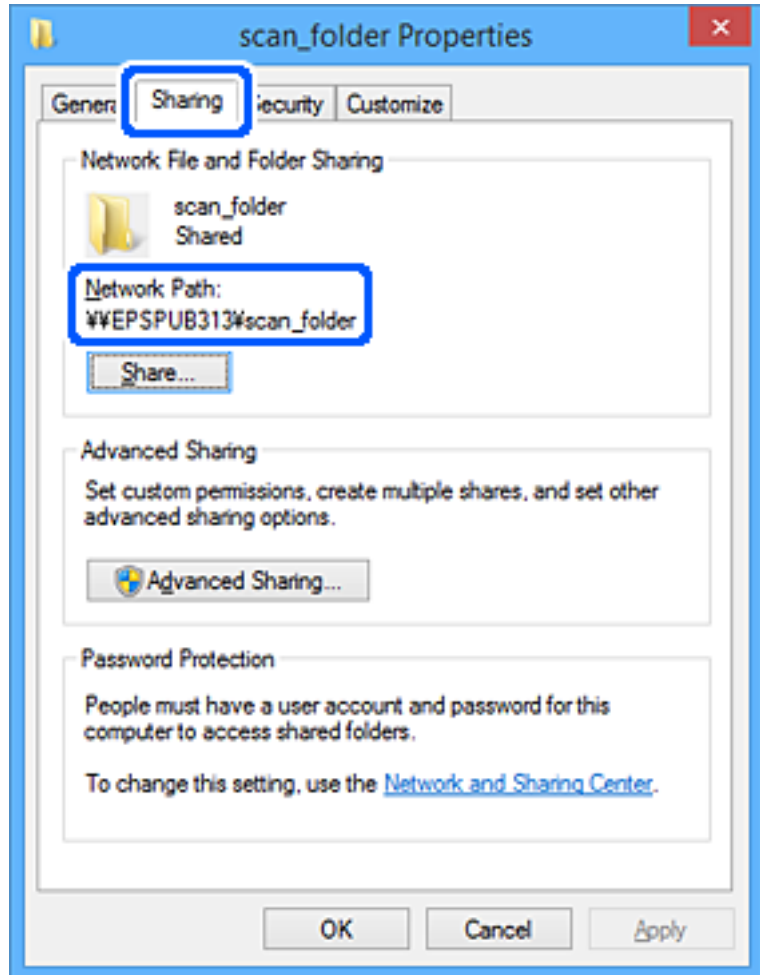
במקרה זה, המשתמש המתחבר למחשב שלו והמנהל יכולים לגשת לתיקיה המשותפת.

במידת הצורך, הוסף השראת גישה. תוכל להוסיף אותה באמצעות לחיצה על ערוך. לפרטים נוספים, עיין במידע קשור.



11. בחר בלשונית שיתוף.

מוצג נתיב הרשת של התיקה המשותפת. משתמשים בזה כאשר רושמים אל אנשי הקשר של הסורק. אנא רשום זאת.



12. לחץ OK או סגור כדי לסגור את המסך.

בדוק אם ניתן לכתוב או לקרוא את הקובץ בתיקה המשותפת מהמחשבים של משתמשים או קבוצות עם הרשאות גישה.

מידע קשור

- ← "הוספת קבוצה או משתמש המאפשרים גישה" בעמוד 58
- ← "רישום יעד לאנשי קשר באמצעות Web Config" בעמוד 62

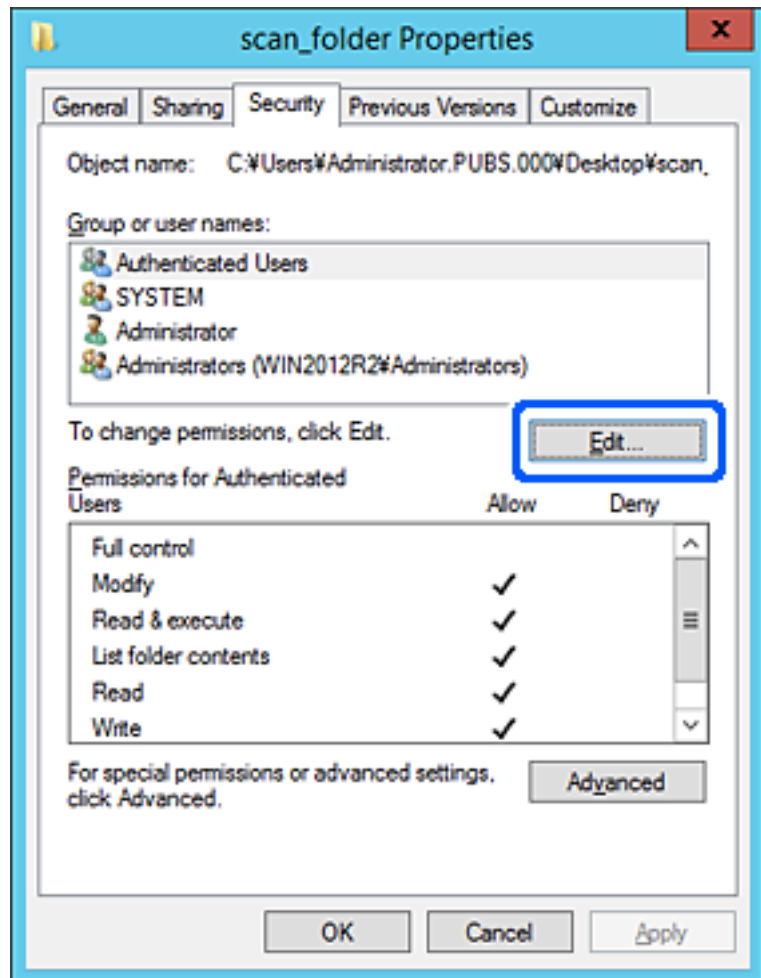
## הוספת קבוצה או משתמש המאפשרים גישה

תוכל להוסיף קבוצה או משתמש המאפשרים גישה.

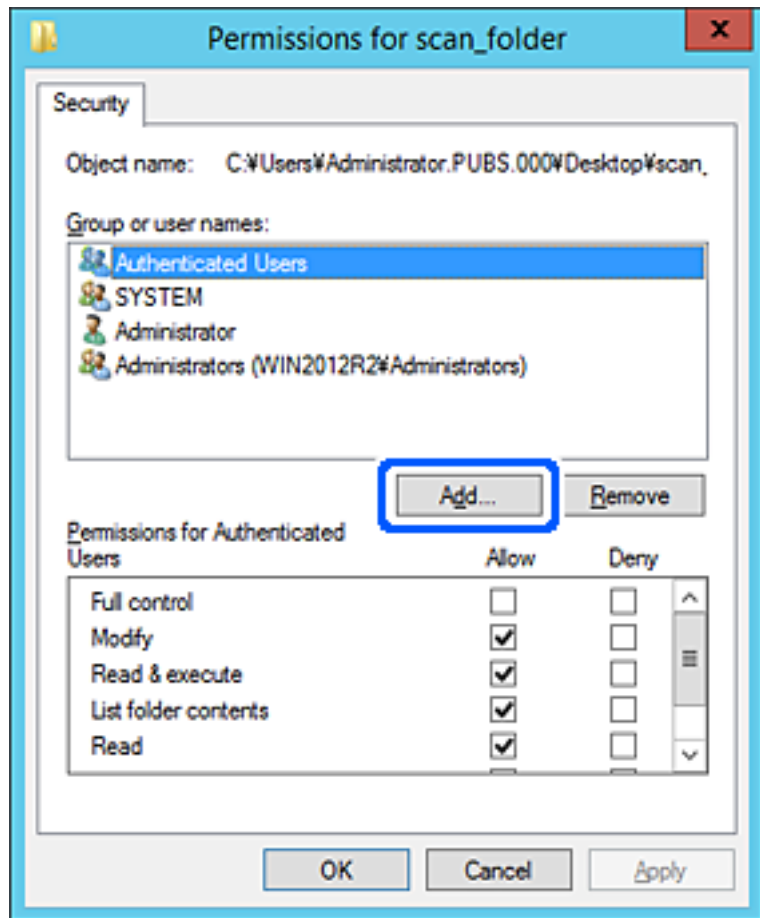
1. לחץ לחיצה ימנית על התיקה, ובחר תכונות.

2. בחר בלשונית אבטחה.

3. לחץ ערוך.



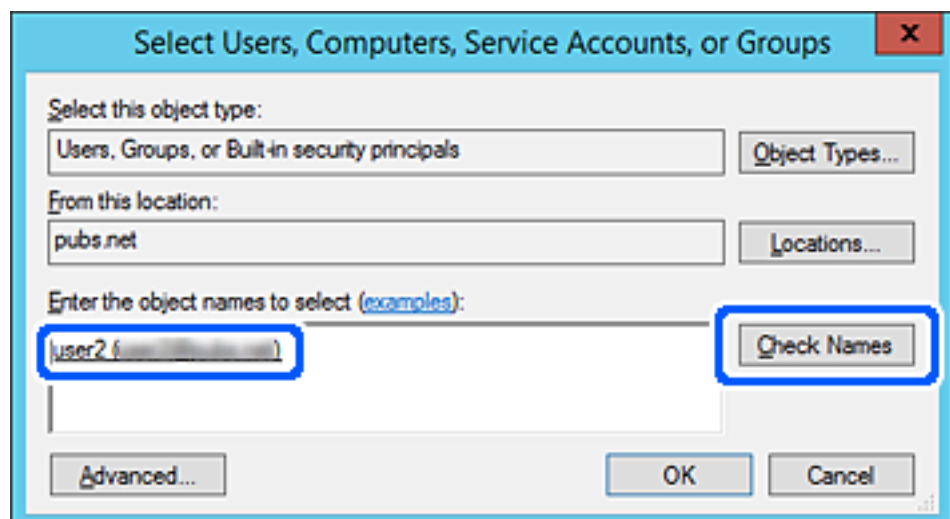
4. לחץ הוסף תחת לשם קבוצה או שמות משתמשים.



5. הזן את שם הקבוצה או המשתמש שאתה רוצה להתיר להם גישה, ואז לחץ על בדוק שמות. יתווסף קו תחתון אל השם.

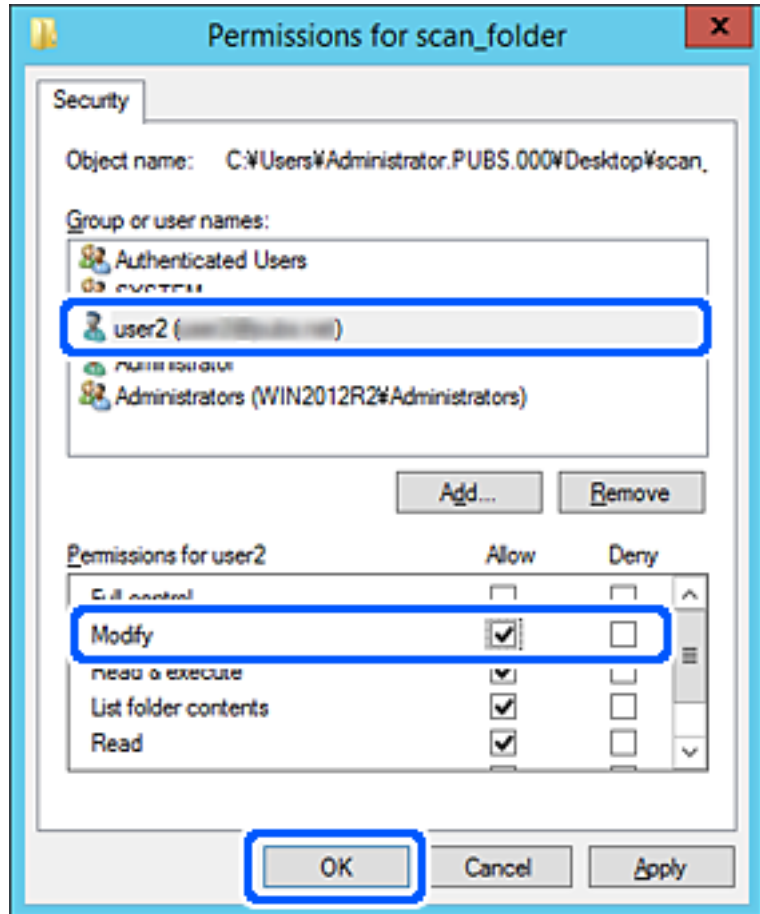
לתשומת לבך:

אם אינך יודע את השם המלא של הקבוצה או המשתמש, הזן חלק מהשם, ואז לחץ על בדוק שמות. שמות הקבוצה או המשתמש התואמים לחלק השם יוצגו ברשימה, ואז תוכל לבחור את השם המלא מהרשימה. אם רק שם אחד תואם, השם המלא המודגש בקו תחתון יוצג בתוך הזן את שם העצם המיועד לבחירה.



6. לחץ אישור.

7. במסך ההרשאות, בחר את שם המשתמש שהזון בתוך קבוצה או שמות משתמשים, בחר את הרשאת הגישה בתוך שנה, ואז לחץ אישור.



8. לחץ אישור או סגור כדי לסגור את המסך.

בדוק אם ניתן לכתוב או לקרוא את הקובץ בתיקיה המשותפת מהמחשבים של משתמשים או קבוצות עם הרשאות גישה.

## הפיכת אנשי קשר לזמינים

רישום יעדים ברשימת אנשי הקשר של הסורק מאפשר לך להזין בקלות את היעד בעת סריקה. תוכל לרשום את סוגי היעדים הבאים ברשימת אנשי הקשר. תוכל לרשום עד 300 ערכים בסך הכל.

לתשומת לבך:

תוכל גם להשתמש בשרת LDAP (חיפוש LDAP) כדי להזין את היעד.

|       |  |
|-------|--|
| דוא"ל | יעד עבור דוא"ל.                                  |
|       | עליך להגדיר מראש את התצורה של הגדרות שרת הדוא"ל. |

|            |  |
|------------|--|
| תיקיית רשת | יעד עבור נתוני סריקה.<br>עליך להכין מראש את תיקיית הרשת. |
|------------|--|

מידע קשור

← "שיתוף פעולה עם שרת ומשתמשי LDAP" בעמוד 68

## השוואת הגדרות אנשי קשר

קיימים שלושה כלים להגדרת אנשי הקשר של הסורק: Web Config, Epson Device Admin ולוח הבקרה של הסורק. ההבדלים בין 3 הכלים מוצגים בטבלה הבאה.

| מאפיינים              | Web Config* | Epson Device Admin | לוח הבקרה של הסורק |
|-----------------------|-------------|--------------------|--------------------|
| רישום יעד             | ✓           | ✓                  | ✓                  |
| עריכת יעד             | ✓           | ✓                  | ✓                  |
| הוספת קבוצה           | ✓           | ✓                  | ✓                  |
| עריכת קבוצה           | ✓           | ✓                  | ✓                  |
| מחיקת יעדים או קבוצות | ✓           | ✓                  | ✓                  |
| מחיקת כל היעדים       | ✓           | ✓                  | -                  |
| ייבוא קובץ            | ✓           | ✓                  | -                  |
| ייצוא לקובץ           | ✓           | ✓                  | -                  |

\* היכנס למערכת כמנהל כדי לבצע את ההגדרות.

## רישום יעד לאנשי קשר באמצעות Web Config

לתשומת לבך:

תוכל גם לרשום את אנשי הקשר בלוח הבקרה של הסורק.

1. גש אל Web Config ובחר את לשונית **Scan < Contacts**.

2. בחר את המספר שברצונך לרשום, ואז לחץ על **Edit**.

3. הזן **Name** ו-**Index Word**.

4. בחר את סוג היעד כאפשרות **Type**.

לתשומת לבך:

לא תוכל לשנות את האפשרות **Type** אחרי שהרישום יושלם. אם ברצונך לשנות את הסוג, מחק את היעד ואז רשום אותו שוב.

5. הזן ערך עבור כל פריט, ואז לחץ Apply.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

### פריטי הגדרות יעד

| פריטים                 | הגדרות והסבר   |
|------------------------|--|
| הגדרות נפוצות          |  |
| Name                   | הזן שם המוצג באנשי הקשר ב-30 תווים או פחות בפורמט Unicode (קידוד UTF-8). אם לא תציין זאת, השאר את המקום ריק.   |
| Index Word             | הזן שם בן 30 תווי UTF-8 (Unicode) או פחות, כדי לחפש את אנשי הקשר בלוח הבקרה של הסורק. אם לא תציין זאת, השאר את המקום ריק.  |
| Type                   | בחר את סוג הכתובת שברצונך לרשום.   |
| Assign to Frequent Use | בחר להגדיר את הכתובת הרשומה ככתובת הנמצאת בשימוש תדיר. כאשר אתה מגדיר כתובת הנמצאת בשימוש תדיר, היא מוצגת במסך העליון של הסריקה, ותוכל לציין את היעד בלא להציג את אנשי הקשר.   |
| Email                  |  |
| Email Address          | הזן בין 1 ל-255 תווים מסוג אותיות A-Z, a-z וכן 0-9 ! # \$ % & ' * + , - . / ? ^ _ {   } ~ .@   |
| Network Folder (SMB)   |  |
| Save to                | \\נתיב תיקיה"<br>הזן את המיקום שבו תיקיית המטרה ממוקמת בין 1 לבין 253 תווים בתווי Unicode (תווי UTF-8), תוך השמטת "\\".<br>הזן את נתיב הרשת המוצג במסך המאפיינים של התיקייה. הצג את הפרטים הבאים ביחס להגדרות נתיב הרשת.<br><a href="#">"דוגמה של הגדרת תצורה עבור מחשב אישי" בעמוד 53</a> |
| User Name              | הזן שם משתמש כדי לגשת לתיקיית רשת ב-30 תווים או פחות בפורמט Unicode (קידוד UTF-8). עם זאת, עליך להימנע מהשימוש בתווי בקרה (0x00-0x1F, 0x7F).   |
| Password               | הזן סיסמה כדי לגשת לתיקיית רשת ב-20 תווים או פחות בפורמט Unicode (קידוד UTF-8). עם זאת, עליך להימנע מהשימוש בתווי בקרה (0x00-0x1F, 0x7F).  |
| FTP                    |  |
| Secure Connection      | בחר FTP או FTPS בהתאם לפרוטוקול העברת הקבצים בו תומך שרת ה-FTP. בחר FTPS כדי לאפשר לסורק ליצור תקשורת ללא אמצעי אבטחה.   |

| פריטים                 | הגדרות והסבר  |
|------------------------|---|
| Save to                | הזן את שם השרת, בין 1 לבין 253 תווי ASCII (דהיינו, 0x20-0x7E), תוך השמטת "://:ftps" או "://:ftp".   |
| User Name              | הזן שם משתמש כדי לגשת לשרת FTP ב-30 תווים או פחות בפורמט Unicode (קידוד UTF-8). עם זאת, עליך להימנע מהשימוש בתווי בקרה (0x00-0x1F, 0x7F). אם השרת מאפשר חיבורים אנונימיים, הזן שם משתמש כגון Anonymous ו-FTP. אם לא תציין זאת, השאר את המקום ריק. |
| Password               | הזן סיסמה כדי לגשת לשרת FTP ב-20 תווים או פחות בפורמט Unicode (קידוד UTF-8). עם זאת, עליך להימנע מהשימוש בתווי בקרה (0x00-0x1F, 0x7F). אם לא תציין זאת, השאר את המקום ריק.  |
| Connection Mode        | בחר את מצב החיבור מהתפריט. אם הוגדרה חומת אש בין הסורק לבין שרת ה-FTP, בחר <b>Passive Mode</b> .  |
| Port Number            | הזן את מספר כניסת שרת ה-FTP בין 1 לבין 65535.   |
| Certificate Validation | אישור שרת ה-FTP אומת כאשר מאפשרים זאת. אפשרות זו זמינה כאשר <b>FTPS</b> נבחר כ- <b>Secure Connection</b> . על מנת לבצע את ההגדרה, עליך לייבא את CA Certificate אל הסורק.  |
| SharePoint(WebDAV)     |   |
| Secure Connection      | בחר HTTP או HTTPS בהתאם לפרוטוקול העברת הקבצים בו תומך השרת. בחר <b>HTTPS</b> כדי לאפשר לסורק ליצור תקשורת ללא אמצעי אבטחה.   |
| Save to                | הזן את שם השרת, בין 1 לבין 253 תווי ASCII (דהיינו, 0x20-0x7E), תוך השמטת "://:http" או "://:https".   |
| User Name              | הזן שם משתמש כדי לגשת לשרת ב-30 תווים או פחות בפורמט Unicode (קידוד UTF-8). עם זאת, עליך להימנע מהשימוש בתווי בקרה (0x00-0x1F, 0x7F). אם לא תציין זאת, השאר את המקום ריק.   |
| Password               | הזן סיסמה כדי לגשת לשרת ב-20 תווים או פחות בפורמט Unicode (קידוד UTF-8). עם זאת, עליך להימנע מהשימוש בתווי בקרה (0x00-0x1F, 0x7F). אם לא תציין זאת, השאר את המקום ריק.  |
| Certificate Validation | אישור השרת מאומת כאשר מאפשרים זאת. אפשרות זו זמינה כאשר <b>HTTPS</b> נבחר כ- <b>Secure Connection</b> . על מנת לבצע את ההגדרה, עליך לייבא את CA Certificate אל הסורק.   |
| Proxy Server           | בחר אם ברצונך להשתמש בשרת הפרוקסי או לא.  |

## רישום יעדים כקבוצה באמצעות Web Config

אם סוג היעד הוגדר כ- **Email** תוכל לרשום את היעדים כקבוצה.

1. גש אל Web Config ובחר את לשונית **Scan < Contacts**.



2. בחר את המספר שברצונך לרשום, ואז לחץ על **Edit**.
3. בחר קבוצה מתוך **Type**.
4. לחץ **Select** עבור **Contact(s) for Group**.  
היעדים הזמינים יוצגו.
5. בחר את היעד שברצונך לרשום עבור הקבוצה, ואז לחץ על **Select**.
6. הזן **Name** ו-**Index Word**.
7. בחר אם להקצות את הקבוצה הרשומה לקבוצה הנמצאת בשימוש תדיר.  
**לתשומת לבך:**  
ניתן לרשום יעדים למספר רב של קבוצות.
8. לחץ על **Apply**.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## גיבוי וייבוא של אנשי קשר

באמצעות Web Config או כלים אחרים, תוכל לגבות ולייבא אנשי קשר. עבור Web Config, תוכל לגבות אנשי קשר באמצעות ייצוא הגדרות הסורק הכוללות אנשי קשר. לא ניתן לערוך את הקובץ שיוצא משום שהוא מיוצא כקובץ בינארי. בעת ייבוא הגדרות הסורק לסורק, יימחקו אנשים הקשר. עבור Epson Device Admin, ניתן לייצא רק אנשי קשר ממסך התכונות של ההתקן. כמו כן, אם לא תייצא את הפריטים הקשורים לאבטחה, תוכל לערוך את אנשי הקשר שיוצאו ולייבא אותם משום שניתן לשמור אותם כקובץ SYLK או CSV.

## ייבוא אנשי קשר באמצעות Web Config

אם יש לך סורק שמאפשר לך לגבות אנשי קשר והוא תואם לסורק זה, תוכל לרשום בקלות את אנשי הקשר באמצעות ייבוא קובץ הגיבוי.

**לתשומת לבך:**

להוראות כיצד לגבות את אנשי הקשר של הסורק, אנא עיין במדריך שסופק עם הסורק.

פעל בהתאם לשלבים הבאים כדי לייבא את אנשי הקשר לסורק זה.

1. גש אל Web Config, בחר **Device Management** לשונית < **Import < Export and Import Setting Value**.
2. בחר את קובץ הגיבוי שיצרת בתוך **File**, הזן את הסיסמה, ואז לחץ על **Next**.
3. בחר את תיבת הסימון **Contacts** ואז לחץ על **Next**.

## גיבוי אנשי קשר באמצעות Web Config

נתוני אנשי קשר יכולים לאבוד בגלל תקלה בסורק. מומלץ לגבות את הנתונים בכל פעם שמעדכנים אותם. Epson לא תהיה אחראית על אבדן נתונים ולא תגבה או תשחזר את הנתונים ו/או ההגדרות גם במהלך תקופת האחריות. באמצעות Web Config, באפשרותך לגבות למחשב את נתוני אנשי הקשר שמאוחסנים בסורק.

1. גש אל Web Config, ואז בחר את לשונית **Device Management < Export < Export and Import Setting Value**.

2. בחר את תיבת הסימון **Contacts** תחת הקטגוריה **Scan**.

3. הזן סיסמה כדי להצפין את הקובץ שיוצא.

אתה זקוק לסיסמה כדי ליבא את הקובץ. השאר זאת ריק אם אין ברצונך להצפין את הקובץ.

4. לחץ על **Export**.

## ייצוא ורישום של אנשי קשר בצובר באמצעות כלי

אם תשתמש ב-Epson Device Admin, תוכל לגבות רק את אנשי הקשר ולערוך את הקבצים שיוצאו, ואז לרשום את כולם בבת אחת.

אפשרות זו שימושית אם אתה רוצה לגבות רק את אנשי הקשר או כאשר אתה מחליף את הסורק ורוצה להעביר את אנשי הקשר מהישנה אל החדשה.

## ייצוא אנשי קשר

שמור את המידע של אנשי הקשר בקובץ.

תוכל לערוך קבצים שנשמרו בפורמט SYLK או בפורמט csv באמצעות אפליקציית גליון נתונים או עורך טקסט. תוכל לרשום את כולם בבת אחת אחרי מחיקה או הוספה של מידע.

ניתן לשמור מידע הכולל פריטי אבטחה כגון סיסמה ומידע אישי בפורמט בינרי עם סיסמה. לא תוכל לערוך את הקובץ. ניתן להשתמש בקובץ זה כקובץ הגיבוי של המידע, כולל פריטי האבטחה.

1. הפעל את **Epson Device Admin**.

2. בחר **Devices** בתפריט המשימות בסרגל הצד.

3. בחר את ההתקן שברצונך להגדיר מתוך רשימת ההתקנים.

4. לחץ **Device Configuration** בלשונית **Home** שעל תפריט הסרט.

כאשר הוגדרה סיסמת מנהל, הזן את הסיסמה ולחץ על **OK**.

5. לחץ על **Contacts < Common**.

6. בחר את פורמט הייצוא מתוך **Export items < Export**.

All Items

ייצא את הקובץ הבינרי המוצפן. בחר כאשר ברצונך לכלול פריטי אבטחה כגון סיסמה ומידע אישי. לא תוכל לערוך את הקובץ. אם תבחר באפשרות זו, יהיה עליך להגדיר את הסיסמה. לחץ **Configuration** והגדר סיסמה שאורכה בין 8 ל- 63 תווים בפורמט ASCII. סיסמה זו דרושה בעת ייבוא הקובץ הבינרי.

Items except Security Information

יצא את הקבצים בפורמט SYLK או csv. בחר באפשרות זו כשברצונך לערוך את המידע בקובץ שיוצא.

7. לחץ על **Export**.

8. ציין את המקום שבו יש לשמור את הקובץ, בחר את סוג הקובץ, ואז לחץ על **Save**. מוצגת הודעת הסיום.

9. לחץ על **OK**.

ודא שהקובץ נשמר במקום שציינת.

## ייבוא אנשי קשר

ייבא את המידע של אנשי הקשר מתוך הקובץ.

תוכל לייבא את הקבצים השמורים בפורמט SYLK או csv או בקובץ הגיבוי הבינארי המכיל את פריטי האבטחה.

1. הפעל את **Epson Device Admin**.

2. בחר **Devices** בתפריט המשימות בסרגל הצד.

3. בחר את ההתקן שברצונך להגדיר מתוך רשימת ההתקנים.

4. לחץ **Device Configuration** בלשונית **Home** שעל תפריט הסרט. כאשר הוגדרה סיסמת מנהל, הזן את הסיסמה ולחץ על **OK**.

5. לחץ על **Common < Contacts**.

6. לחץ **Browse** ב- **Import**.

7. בחר את הקובץ שברצונך לייבא, ולאחר מכן לחץ על **Open**.

כאשר אתה בוחר את הקובץ הבינארי בתוך **Password** הזן את הסיסמה שאתה מגדיר בעת ייצוא הקובץ.

8. לחץ על **Import**.

יצג מסך האישור.

9. לחץ על **OK**.

מוצגת תוצאת האימות.

Edit the information read

לחץ כאשר ברצונך לערוך את המידע באופן פרטני.

Read more file

לחץ כאשר ברצונך לייבא קבצים רבים.

10. לחץ **Import**, ואז לחץ **OK** במסך השלמת הייבוא.

חזור למסך תכונות ההתקן.

11. לחץ על **Transmit**.

12. לחץ **OK** בהודעת האישור.

ההגדרות נשלחו אל הסורק.

13. במסך השלמת השליחה, לחץ **OK**.

מידע הסורק מתעדכן.

פתח את אנשי הקשר מתוך Web Config או מתוך לוח הבקרה של הסורק, ואז ודא שאיש הקשר עודכן.

## שיתוף פעולה עם שרת ומשתמשי LDAP

בעת שיתוף פעולה עם שרת LDAP, תוכל להשתמש במידע הכתובת הרשומה בשרת LDAP כיעד של דוא"ל.

### הגדרת התצורה של שרת LDAP

על מנת להשתמש במידע שרת LDAP, רשום אותו בסורק.

1. גש אל Web Config ובחר את לשונית **Basic < LDAP Server < Network**.

2. הזן ערך עבור כל פריט.

3. בחר **OK**.

ההגדרות שבחרת תוצגנה.

### פריטי הגדרות בשרת LDAP

| פריטים                  | הגדרות והסבר   |
|-------------------------|--|
| Use LDAP Server         | בחר Use או Do Not Use.   |
| LDAP Server Address     | הזן את כתובת שרת LDAP. הזן בין 1 לבין 255 תווים בפורמט IPv4, IPv6 או פורמט FQDN. עבור פורמט FQDN, תוכל להשתמש בתווים אלפאנומריים ב-ASCII (0x20-0x7E) וכן "-" למעט בתחילת ובסוף הכתובת. |
| LDAP server Port Number | הזן את מספר כניסת שרת ה-LDAP בין 1 לבין 65535.   |

| פריטים                       | הגדרות והסבר  |
|------------------------------|---|
| Secure Connection            | ציין את שיטת האימות כאשר הסורק ניגש אל שרת ה-LDAP.  |
| Certificate Validation       | כאשר מאפשרים זאת, יש תיקוף לתעודת שרת ה-LDAP. מומלץ להגדיר אותו כ- <b>Enable</b> . כדי לבצע את ההגדרה, יש לייבא את <b>CA Certificate</b> אל הסורק.  |
| Search Timeout (sec)         | הגדר את משך זמן החיפוש לפני פסק זמן בין 5 לבין 300.   |
| Authentication Method        | בחר אחת מהשיטות.<br>אם תבחר <b>Kerberos Authentication</b> , בחר <b>Kerberos Settings</b> כדי לבצע את ההגדרות עבור <b>Kerberos</b> .<br>כדי לבצע <b>Kerberos Authentication</b> , דרושה הסביבה הבאה.<br><input type="checkbox"/> יש תקשורת בין הסורק לבין שרת ה-DNS.<br><input type="checkbox"/> מתבצע סינכרון בין זמן הסורק, שרת ה-KDC והשרת הדרוש לשם אימות (שרת LDAP, שרת SMTP, שרת קבצים).<br><input type="checkbox"/> כאשר מקצים את שרת השירות בתור כתובת ה-IP, ה-FQDN של שרת השירות נרשם באזור הבדיקה אחורה של שרת ה-DNS. |
| Kerberos Realm to be Used    | אם תבחר <b>Kerberos Authentication</b> עבור <b>Authentication Method</b> , בחר את תחום ה-Kerberos בו ברצונך להשתמש.   |
| Administrator DN / User Name | הזן שם משתמש עבור שרת LDAP ב-128 תווים או פחות בפורמט Unicode (קידוד UTF-8). לא ניתן להשתמש בתווי בקרה כגון 0x00-0x1F ו-0x7F. הגדרה זו אינה בשימוש כאשר בוחרים <b>Anonymous Authentication</b> בתור <b>Authentication Method</b> . אם לא תציין זאת, השאר את המקום ריק.  |
| Password                     | הזן הסיסמה עבור אימות שרת LDAP ב-128 תווים או פחות בפורמט Unicode (קידוד UTF-8). לא ניתן להשתמש בתווי בקרה כגון 0x00-0x1F ו-0x7F. הגדרה זו אינה בשימוש כאשר בוחרים <b>Anonymous Authentication</b> בתור <b>Authentication Method</b> . אם לא תציין זאת, השאר את המקום ריק.  |

### הגדרות Kerberos

אם תבחר **Kerberos Authentication** עבור **Authentication Method** של **LDAP Server** < **Basic**, בצע את ההגדרות Kerberos הבאות מתוך לשונית **Kerberos Settings**. תוכל לרשום עד 10 הגדרות Kerberos.

| פריטים         | הגדרות והסבר  |
|----------------|---|
| Realm (Domain) | הזן את התחום לאימות Kerberos ב-255 תווי ב-ASCII או פחות (0x20-) 0x7E). אם לא תרשום זאת, השאר את המקום ריק.                |
| KDC Address    | הזן את כתובת שרת האימות של Kerberos. הזן 255 תווים או פחות בפורמט IPv4, IPv6 או FQDN. אם לא תרשום זאת, השאר את המקום ריק. |

| פריטים                 | הגדרות והסבר                                       |
|------------------------|--|
| Port Number (Kerberos) | הזן את מספר כניסת שרת ה-Kerberos בין 1 לבין 65535. |

## הגדרת התצורה של הגדרות החיפוש של שרת LDAP

כאשר אתה מגדיר את הגדרות החיפוש, אתה יכול להשתמש בכתובת הדוא"ל הרשומה בשרת LDAP.

1. גש אל Web Config ובחר את לשונית **LDAP Server < Network < Search Settings**.
2. הזן ערך עבור כל פריט.
3. לחץ **OK** כדי להציג את תוצאת ההגדרה.  
ההגדרות שבחרת תוצגנה.

## חפש בין פריטי הגדרות בשרת LDAP

| פריטים   | הגדרות והסבר   |
|--|--|
| Search Base (Distinguished Name)                 | אם ברצונך לחפש תחום אקראי, ציין את שם התחום של שרת ה-LDAP. הזן בין 0 ל-128 תווים ב-Unicode (קידוד UTF-8). אם אינך מחפש מאפיין אקראי, השאר זאת ריק.<br>למשל, עבור תיקיית השרת המקומי: <code>dc=local,dc=server</code> |
| Number of search entries                         | ציין את מספר פריטי החיפוש בין 5 לבין 500. מספר פריטי החיפוש יישמור ויוצג זמנית. ניתן להשלים את החיפוש גם אם מספר פריטי החיפוש גדול מהמספר שצוין ומופיעה הודעת שגיאה.   |
| User name Attribute                              | ציין את שם המאפיין שיש להציג בעת חיפוש אחר שמות משתמשים. הזן בין 1 ל-255 תווים ב-Unicode (קידוד UTF-8). התו הראשון צריך להיות a-z או A-Z.<br>דוגמה: <code>uid, cn</code>   |
| User name Display Attribute                      | ציין את שם המאפיין שיש להציג כשם המשתמש. הזן בין 0 ל-255 תווים ב-Unicode (קידוד UTF-8). התו הראשון צריך להיות a-z או A-Z.<br>דוגמה: <code>sn, cn</code>  |
| Email Address Attribute                          | ציין את שם המאפיין שיש להציג בעת חיפוש אחר כתובות דוא"ל. הזן שילוב מתוך 1 עד 255 תווים תוך שימוש ב-A-Z, a-z, 0-9, ו"-". התו הראשון צריך להיות a-z או A-Z.<br>דוגמה: <code>mail</code>                                |
| - Arbitrary Attribute 1<br>Arbitrary Attribute 4 | תוכל לציין מאפיינים אקראיים אחרים לחיפוש. הזן בין 0 ל-255 תווים ב-Unicode (קידוד UTF-8). התו הראשון צריך להיות a-z או A-Z. אם אין ברצונך לחפש אחר מאפיינים אקראיים, השאר זאת ריק.<br>דוגמה: <code>ou, o</code>       |

## בדיקת החיבור עם שרת LDAP

מבצעת את בדיקת החיבור אל שרת LDAP באמצעות הפרמטר שהוגדר בתוך **LDAP Server** < **Search Settings**.

1. גש אל **Web Config** ובחר את לשונית **Network** < **LDAP Server** < **Connection Test**.
  2. בחר **Start**.
- בדיקת החיבור התחילה. אחרי הבדיקה, יוצג דו"ח בדיקה.

### הפניות בבדיקת חיבור שרת LDAP

| הודעות  | הסבר  |
|---|---|
| Connection test was successful.   | הודעה זו מופיעה כאשר הקשר עם השרת הצליח.  |
| Connection test failed.<br>Check the settings.                                | <p>ההודעה מופיעה מהסיבות הבאות:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> כתובת שרת LDAP או מספר היציאה שגויים.</li> <li><input type="checkbox"/> התרחש פסק זמן.</li> <li><input type="checkbox"/> <b>Do Not Use</b> נבחר בתור <b>Use LDAP Server</b>.</li> <li><input type="checkbox"/> אם בוחרים את <b>Kerberos Authentication</b> כ- <b>Authentication Method</b>, הגדרות כגון <b>Realm (Domain)</b>, <b>KDC Address</b> ו- <b>Port Number (Kerberos)</b> שגויות.</li> </ul> |
| Connection test failed.<br>Check the date and time on your product or server. | הודעה זו מופיעה כאשר החיבור נכשל משום שאין התאמה בין הגדרות הזמן עבור הסורק ועבור שרת LDAP.   |
| Authentication failed.<br>Check the settings.                                 | <p>ההודעה מופיעה מהסיבות הבאות:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> <b>User Name</b> ו/או <b>Password</b> שגויים.</li> <li><input type="checkbox"/> אם בוחרים <b>Kerberos Authentication</b> כ- <b>Authentication Method</b>, אפשר שתצורת השעה/תאריך לא הוגדרה.</li> </ul>  |
| Cannot access the product until processing is complete.                       | הודעה זו מופיעה כאשר הסורק תפוס.  |

## השימוש ב- Document Capture Pro Server

באמצעות השימוש ב- Document Capture Pro Server, תוכל לנהל את שיטות המיון, פורמט השמירה ויעד ההעברה של תוצאת סריקה שבוצעה מתוך לוח הבקרה של הסורק. תוכל לקרוא ולבצע עבודה שנרשמה בשרת קודם לכן מלוח הבקרה של הסורק.

התקן אותו במחשב השרת.

למידע נוסף על Document Capture Pro Server, צור קשר עם משרד Epson המקומי שלך.

## הגדרת מצב שרת

כדי להשתמש ב-Document Capture Pro Server, הגדר את ההגדרות הבאות.

1. גש אל Web Config ובחר את לשונית Document Capture Pro < Scan.

2. בחר Server Mode עבור Mode.

3. הזן את כתובת השרת שבו מותקן Document Capture Pro Server עבור Server Address.

הזן בין 2 לבין 255 תווים בפורמט IPv4, IPv6, שם מארח או פורמט FQDN. עבור פורמט FQDN, תוכל להשתמש בתווים אלפאנומריים ב-ASCII (0x20-0x7E) וכן "-" למעט בתחילת ובסוף הכתובת.

4. לחץ על OK.

הרשת מתחברת מחדש ואז מאופשרות ההגדרות.

## הגדרת AirPrint

גש אל Web Config, בחר את הלשונית Network ואז בחר AirPrint Setup.

| פריטים               | הסבר  |
|----------------------|---|
| Bonjour Service Name | הזן שם שירות Bonjour תוך שימוש בטקסט ASCII (0x20-0x7E) ועד 41 תווים.  |
| Bonjour Location     | הזן תיאור של מיקום הסורק, תוך שימוש בטקסט Unicode (UTF-8) ועד 127 בתים.   |
| Wide-Area Bonjour    | הגדר אם להשתמש ב-Wide-Area Bonjour או לא. אם תשתמש בו, הסורק חייב להיות רשום בשרת DNS על מנת שניתן יהיה לחפש את הסורק על פני המקטע. |
| Enable AirPrint      | אופשרו Bonjour ו-AirPrint (שירות סריקה).  |

## בעיות בעת הכנת סריקת רשת

### רמזים לפתרון בעיות

בדיקת הודעת השגיאה

כאשר מופיעה תקלה, בדוק תחילה אם קיימות הודעות כלשהן בלוח הבקרה של הסורק או במסך של מנהל ההתקן. אם הגדרת את האפשרות של קבלת הודעות דוא"ל כאשר מתרחשים אירועים, תוכל ללמוד באופן מיידי על המצב.



□ בדיקת מצב התקשורת

בדוק את מצב התקשורת של מחשב השרת או מחשב הלקוח באמצעות פקודה כמו ping או ipconfig.

□ בדיקת חיבור

כדי לבדוק את החיבור בין הסורק לבין שרת הדוא"ל, בצע את בדיקת החיבור מהסורק. כמו כן, בדוק את החיבור ממחשב הלקוח אל השרת על מנת לבדוק את מצב התקשורת.

□ אתחול ההגדרות

אם לא נראה שקיימת בעיה במצב ההגדרות והתקשורת, אפשר שניתן יהיה לפתור את הבעיות באמצעות השבתה או אתחול של הגדרות הרשת של הסורק, ולאחר מכן ביצוע חוזר של ההגדרות.

לא ניתן לגשת אל Web Config

■ כתובת ה-IP לא הוקצתה לסורק.

פתרונות

אפשר שלא הוקצתה כתובת IP חוקית לסורק. הגדר את כתובת ה-IP באמצעות לוח הבקרה של הסורק. תוכל לאשר את מידע ההגדרה הנוכחית מתוך לוח הבקרה של הסורק.

■ דפדפן האינטרנט אינו תומך בעוצמת ההצפנה עבור SSL/TLS.

פתרונות

ל-SSL/TLS יש Encryption Strength. תוכל לפתוח את Web Config באמצעות דפדפן אינטרנט שתומך בהצפנות בצובר כפי שמצוין להלן. ודא שאתה משתמש בדפדפן שיש עבורו תמיכה.

□ 80 סיביות: AES256/AES128/3DES

□ 112 סיביות: AES256/AES128/3DES

□ 128 סיביות: AES256/AES128

□ 192 סיביות: AES256

□ 256 סיביות: AES256

■ פג התוקף של CA-signed Certificate.

פתרונות

אם קיימת בעיה עם תאריך התפוגה של האישור, תוצג ההודעה "תוקף האישור פג" בעת התחברות עם Web Config (https עם תקשורת SSL/TLS). אם ההודעה מופיעה לפני תאריך תפוגת התוקף, ודא שתצורת תאריך הסורק הוגדרה בצורה נכונה.

■ אין התאמה בין השם המשותף של האישור לבין הסורק.

פתרונות

אם אין התאמה בין השם המשותף של האישור ושל הסורק, מוצגת ההודעה "אין התאמה עם שם אישור האבטחה..." בעת הנסיון לגשת אל Web Config באמצעות תקשורת SSL/TLS (https). הדבר קורה משום שאין התאמה בין כתובות ה-IP הבאות.

❑ כתובת ה-IP של הסורק שהוזנה לתוך שם משותף עבור יצירת Self-signed Certificate או CSR

❑ כתובת IP שהוזנה לדפדפן אינטרנט בעת הפעלה של Web Config

עבור Self-signed Certificate, עדכן את האישור.

עבור CA-signed Certificate, קח שוב את האישור עבור הסורק.

■ הגדרת שרת ה-proxy של הכתובת המקומית לא הוגדרה בדפדפן האינטרנט.

#### פתרונות

כאשר הסורק מוגדר לשימוש עם שרת proxy, יש להגדיר את תצורת דפדפן האינטרנט כך שהוא לא יתחבר אל הכתובת המקומית באמצעות שרת ה-proxy.

❑ Windows:

בחר לוח בקרה < רשת ואינטרנט < אפשרויות אינטרנט < חיבורים < הגדרות < LAN שרת Proxy, ואז הגדר את התצורה לא להשתמש בשרת ה-proxy עבור LAN (כתובות מקומיות).

❑ Mac OS:

בחר העדפות מערכת < רשת < מתקדם < שרתי Proxy, ואז רשום את הכתובת המקומית עבור עקוף הגדרות proxy עבור מארחים ותחומים אלה.

דוגמה:

192.168.1.\*: כתובת מקומית XXX.192.168.1, מסכת תת-רשת 255.255.255.0

192.168.\*.\*: כתובת מקומית XXX.XXX.192.168, מסכת תת-רשת 255.255.0.0

■ DHCP מושבת בהגדרות המחשב.

#### פתרונות

אם ה-DHCP להשגת כתובת IP מושבת באופן אוטומטי במחשב שלך, לא תוכל לגשת אל Web Config. אפשר DHCP.

דוגמה עבור Windows 10:

פתח את לוח הבקרה ואז לחץ על רשת ואינטרנט < מרכז הרשת והשיתוף < שנה את הגדרות המתאם פתח את מסך המאפיינים של החיבור שבו אתה משתמש ואז פתח את מסך המאפיינים עבור פרוטוקול אינטרנט גרסה 4 (TCP/IPv4) או פרוטוקול אינטרנט גרסה 6 (TCP/IPv6). ודא שהאפשרות השג כתובת IP באופן אוטומטי נבחר במסך שמוצג.

---

# התאמה אישית של תצוגת לוח הבקרה


76.....רישום קבוע מראש.

78.....עריכת מסך הבית של לוח הבקרה.

## רישום קבוע מראש

תוכל לרשום הגדרות סריקה הנמצאות בשימוש נפוץ, בתור קבוע מראש. תוכל לרשום עד 48 הגדרות קבועות מראש.

לתשומת לבך:

תוכל לרשום את ההגדרות הנוכחיות באמצעות בחירת  במסך התחלת הסריקה.

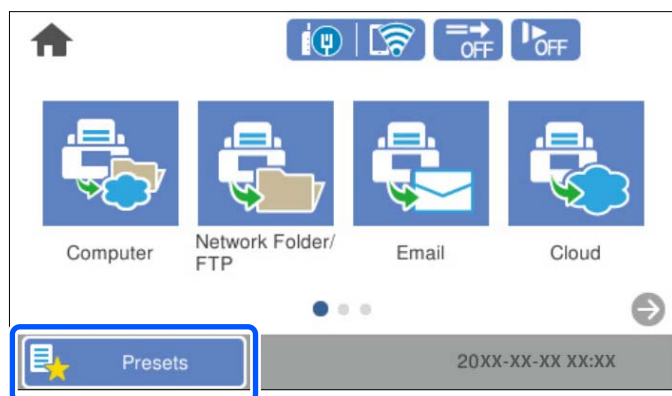
תוכל גם לרשום Presets ב-Web Config.

בחר את הלשונית *Presets < Scan*.

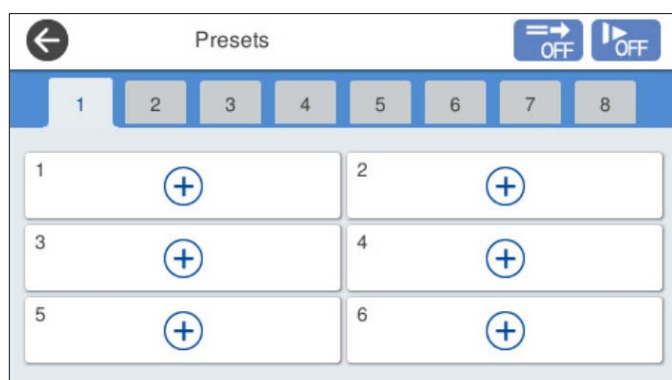
אם תבחר סריקה למחשב בעת רישום, תוכל לרשום את העבודה שנוצרה ב-Document Capture Pro בתור Presets. אפשרות זו זמינה רק עבור משחבים המחוברים באמצעות רשת. רשום מראש את העבודה ב-Document Capture Pro.

אם פונקציית האימות מאופשרת, רק המנהל יכול לרשום Presets.

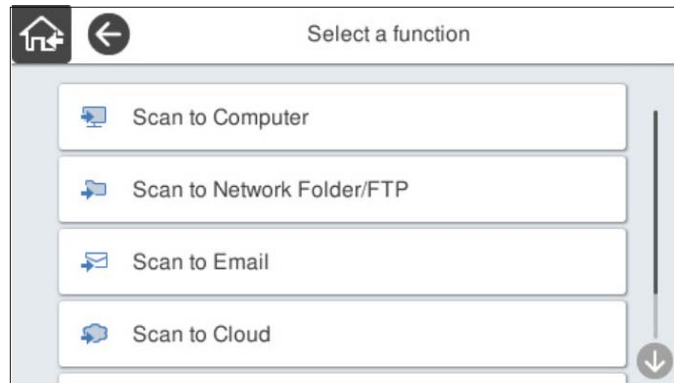
1. בחר קבוע מראש במסך הבית בלוח הבקרה של הסורק.



2. בחר .



3. בחר את התפריט שבו אתה רוצה להשתמש כדי לרשום הגדרה קבועה מראש.



4. הגדר כל פריט ואז בחר .

לתשומת לבך:

כאשר אתה בוחר סריקה למחשב, בחר את המחשב שבו מותקנת Document Capture Pro, ואז בחר עבודה רשומה. אפשרות זו זמינה רק עבור משחבים המחוברים באמצעות רשת.

5. בצע את הגדרות עבור ההגדרות הקבועות מראש.

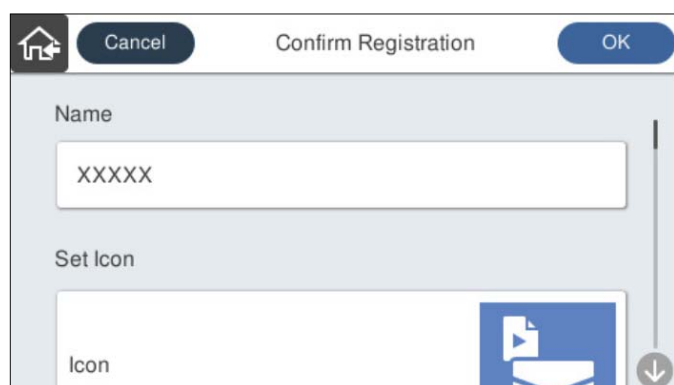
שם: הגדר את השם.

הגדרת סמל: הגדר את התמונה והצבע של הסמל שיש להציג.

הגדרת שליחה מהירה: מתחילה מיד לסרוק ללא אישור כאשר בוחרים את ההגדרה הקבועה מראש.

בעת השימוש ב-Document Capture Pro Server, אפילו אם מגדירים לתוכנה לאשר את תוכן העבודה לפני ביצוע הסריקה, עדיין ה-הגדרת שליחה מהירה בהגדרה הקבועה מראש של הסורק מקבלת עדיפות על פני התוכנה.

תוכן: בדוק הגדרות סריקה.



6. בחר OK.

## אפשרויות תפריט של קבוע מראש

תוכל לשנות את ההגדרות של הגדרה קבועה מראש באמצעות בחירת > בכל הגדרה קבועה מראש.

שינוי השם:

משנה את שם ההגדרה הקבועה מראש.

שינוי הסמל:

משנה את תמונת הסמל ואת הצבע של ההגדרה הקבועה מראש.

הגדרת שליחה מהירה:

מתחילה מיד לסרוק ללא אישור כאשר בוחרים את ההגדרה הקבועה מראש.

שינוי המיקום:

משנה את סדר ההצגה של ההגדרות הקבועות מראש.

מחיקה:

מוחקת את ההגדרה הקבועה מראש.

הוספה או הסרה של סמל בבית:

מוסיפה או מוחקת את סמל ההגדרה הקבועה מראש ממסך הבית.

אישור הפרטים:

הצג את ההגדרות של הגדרה קבועה מראש. תוכל להטעין את ההגדרה הקבועה מראש באמצעות בחירת השתמש בהגדרה הזו.

---

## עריכת מסך הבית של לוח הבקרה

תוכל להתאים אישית את מסך הבית באמצעות בחירת הגדרות < ערוך את מסך הבית בלוח הבקרה של הסורק.

פריסה: משנה את שיטת ההצגה של סמלי התפריט.

"שינוי ה-פריסה של מסך הבית" בעמוד 78

הוסף סמל: מוסיפה סמלים אל הגדרות קבוע מראש שבצעת, או משחזרת סמלים שהוסרו מהמסך.

"הוסף סמל" בעמוד 79

הסר סמל: מסירה סמלים ממסך הבית.

"הסר סמל" בעמוד 80

הזז סמל: משנה את סדר ההצגה של הסמלים.

"הזז סמל" בעמוד 81

שחזור ברירת המחדל לתצוגת הסמלים: משחזרת את הגדרות ברירת המחדל של התצוגה עבור מסך הבית.

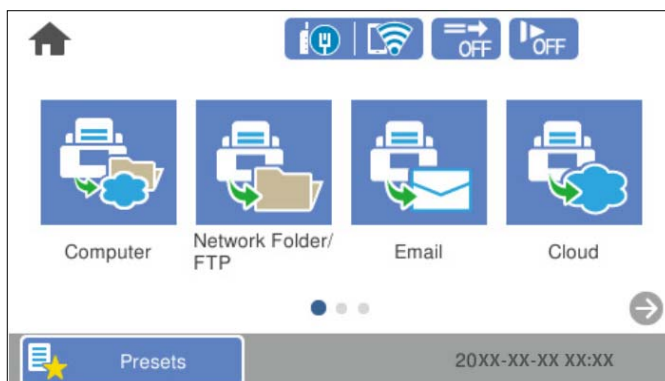
טפט: שנה את צבע הטפט של מסך הבית.

## שינוי ה-פריסה של מסך הבית

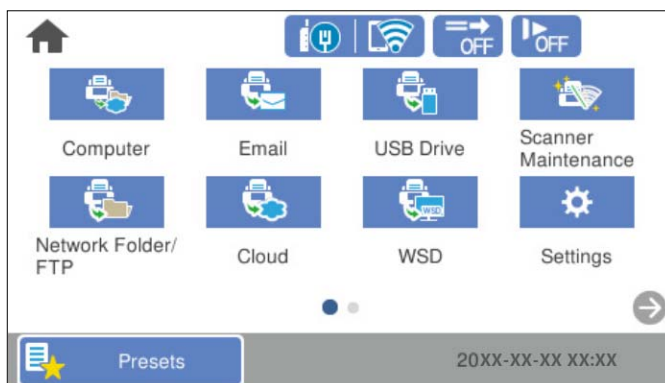
1. בחר הגדרות < ערוך את מסך הבית < פריסה בלוח הבקרה של הסורק.


2. בחר שורה או מטריצה.

שורה:



מטריצה:



3. בחר  כדי לחזור ולבדוק את מסך הבית.

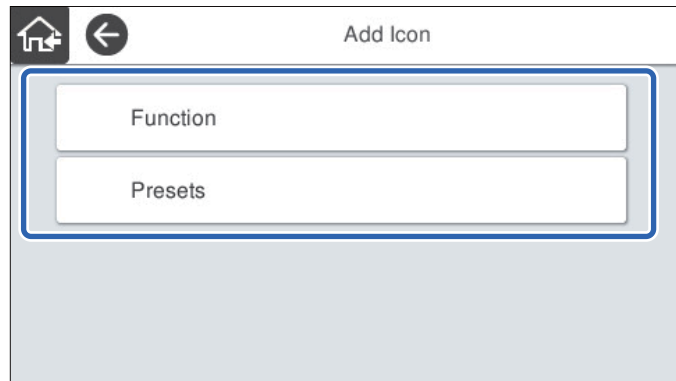
## הוסף סמל

1. בחר הגדרות < ערוך את מסך הבית < הוסף סמל בלוח הבקרה של הסורק.

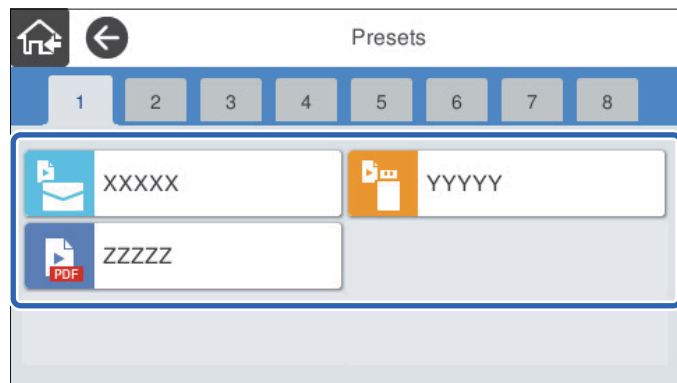
2. בחר פונקציה או קבוע מראש.

פונקציה: מציגה את פונקציות ברירת המחדל המוצגות במסך הבית.

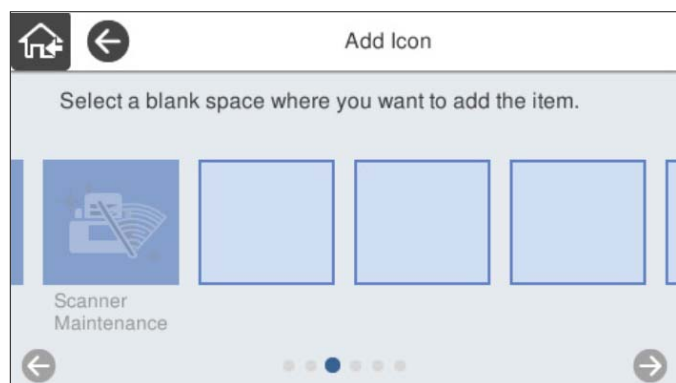
□ קבוע מראש: מציגה הגדרות מוגדרות מראש שנרשמו.




3. בחר את הפריט שאתה רוצה להוסיף למסך הבית.



4. בחר את המקום הריק שבו אתה רוצה להוסיף את הפריט. אם אתה רוצה להוסיף סמלים רבים, חזור על הצעדים 3 עד 4.



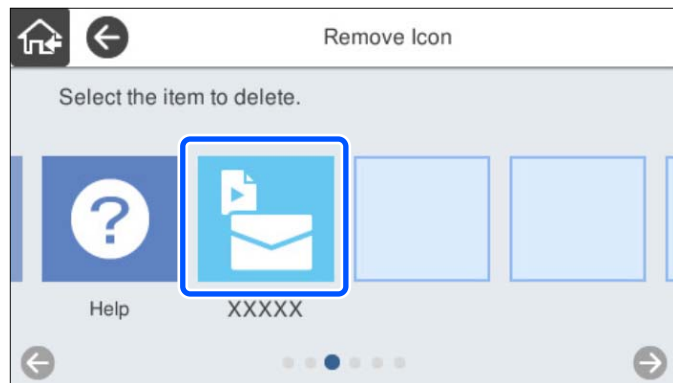
5. בחר  כדי לחזור ולבדוק את מסך הבית.

## הסר סמל

1. בחר הגדרות < ערוך את מסך הבית < הסר סמל בלוח הבקרה של הסורק.




2. בחר את הסמל שברצונך להסיר.



3. בחר כן כדי לסיים.

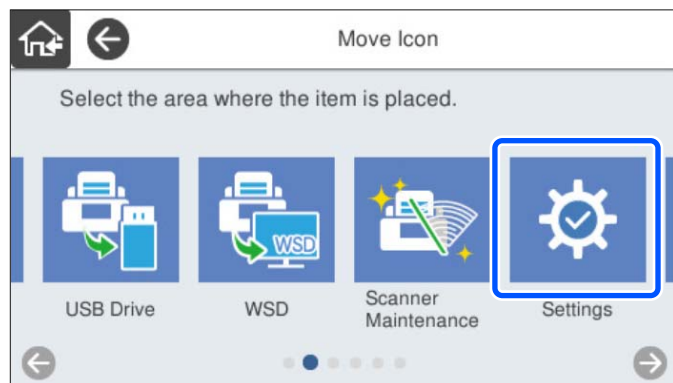
אם ברצונך להוסיף סמלים רבים, חזור על נוהל 2 עד 3.

4. בחר  כדי לחזור ולבדוק את מסך הבית.

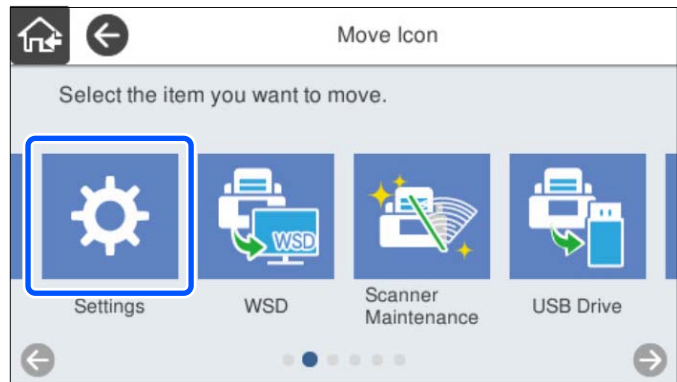
## הזז סמל


1. בחר הגדרות < ערוך את מסך הבית < הזז סמל בלוח הבקרה של הסורק.

2. בחר את הסמל שאתה רוצה להזיז.



3. בחר את מסגרת היעד.  
אם כבר הוגדר סמל אחר במסגרת היעד, הסמלים מוחלפים.



4. בחר  כדי לחזור ולבדוק את מסך הבית.

---

## הגדרות אבטחה בסיסיות

- 84.....מבוא למאפייני אבטחת מוצר.
- 84.....הגדרות מנהל מערכת.
- 90.....השבתת הממשק החיצוני.
- 91.....ניטור סורק מרוחק.
- 93.....פתרון בעיות.

## מבוא למאפייני אבטחת מוצר

סעיף זה מציג את פונציית האבטחה של התקני Epson.

| שם מאפיין              | סוג מאפיין  | מה להגדיר  | מה למנוע   |
|------------------------|---|--|--|
| הגדרה עבור סיסמת מנהל  | נועלת את הגדרות המערכת, כגון הגדרת חיבור עבור רשת או USB. | מנהל מגדיר סיסמה עבור התקן.<br>תוכל להגדיר או לשנות הן מתוך Web Config הן מתוך לוח הבקרה של הסורק. | מנע קריאה ושינוי בלתי חוקיים של המידע המאוחסן בהתקן כגון זהות, סיסמה, הגדרות רשת וכן הלאה. בנוסף לכך, מזער טווח רחב של סיכוני אבטחה כגון דליפת מידע עבור סביבת הרשת או מדיניות האבטחה. |
| הגדרה עבור ממשק חיצוני | שולט בממשק שמתחבר להתקן.                                  | אפשר או השבת חיבור USB עם המחשב.   | חיבור USB של המחשב: מונע שימוש בלתי מורשה בהתקן באמצעות איסור סריקה בלא לעבור דרך הרשת.  |

מידע קשור

← "הגדרת סיסמת מנהל מערכת" בעמוד 84

← "השבתת הממשק החיצוני" בעמוד 90

## הגדרות מנהל מערכת

### הגדרת סיסמת מנהל מערכת

כאשר אתה מגדיר סיסמת מנהל, אתה יכול למנוע ממשתמשים לשנות את הגדרות ניהול המערכת. ערכי ברירת המחדל כבר מוגדרים בעת הרכישה. שנה אותם בהתאם לצורך.

לתשומת לבך:

להלן מובאים ערכי ברירת המחדל עבור מידע המנהל.

☐ שם המשתמש (משמש עבור Web Config בלבד): אין (ריק)

☐ סיסמה: המספר הסידורי של הסורק

כדי למצוא את המספר הסידורי, בדוק את התווית המחוברת אל גב הסורק.

תוכל לשנות את סיסמת המנהל מתוך Web Config, לוח הבקרה של הסורק, או Epson Device Admin. בעת השימוש ב-Epson Device Admin, עיין במדריך Epson Device Admin או בעזרה.

### שינוי סיסמת המנהל באמצעות Web Config

שנה את סיסמת המנהל Web Config.

1. גש אל Web Config ובחר את לשונית Product Security < **Change Administrator Password**.

2. הזן את המידע הדרוש **Current password**, **User Name**, **New Password**, ו-**Confirm New Password**.

הזן לפחות תו אחד עבור הסיסמה החדשה.

לתשומת לבך:

להלן מובאים ערכי ברירת המחדל עבור מידע המנהל.

שם משתמש: ללא (ריק)

סיסמה: המספר הסידורי של הסורק

כדי למצוא את המספר הסידורי, בדוק את התווית המחוברת אל גב הסורק.

**חשוב!**

דאג לזכור את סיסמת המנהל שהגדרת. אם תשכח את הסיסמה שלך, לא יהיה ביכולתך לאפס אותה והיה עליך לבקש עזרה מסגל השירות.

3. בחר OK.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## שינוי סיסמת המנהל מתוך לוח הבקרה

תוכל לשנות את סיסמת המנהל מלוח הבקרה של הסורק.

1. בחר הגדרות בלוח הבקרה של הסורק.

2. בחר גיהול מערכת < הגדרות מנהל מערכת.

3. בחר סיסמת מנהל < שנה.

4. הזן את הסיסמה הנוכחית שלך.

לתשומת לבך:

ההגדרה בעת הרכישה (ערך ברירת המחדל) עבור סיסמת המנהל היא המספר הסידורי של הסורק.

כדי למצוא את המספר הסידורי, בדוק את התווית המחוברת אל גב הסורק.

5. הזן את הסיסמה החדשה שלך.

הזן לפחות תו אחד.

**חשוב!**

דאג לזכור את סיסמת המנהל שהגדרת. אם תשכח את הסיסמה שלך, לא יהיה ביכולתך לאפס אותה והיה עליך לבקש עזרה מסגל השירות.

6. הזן שוב את הסיסמה החדש הכדי לאשר.

מוצגת הודעת סיום.

## השימוש ב-הגדרת נעילה עבור לוח הבקרה


תוכל להשתמש ב-הגדרת נעילה כדי לנעול את לוח הבקרה על מנת למנוע ממשתמשים לשנות פריטים הקשורים להגדרות המערכת.


לתשומת לבך:

אם תאפשר *Authentication Settings* בסורק, גם הגדרת נעילה תאפשר בלוח הבקרה. לא ניתן לפתוח את נעילת לוח הבקרה כאשר *Authentication Settings* מאופשרת.

גם אם תשבית את *Authentication Settings*, הגדרת נעילה תישאר מאופשרת. אם תרצה להשבית אותה, תוכל לבצע הגדרות מתוך לוח הבקרה או *Web Config*.

## הגדרת הגדרת נעילה מלוח הבקרה

1. אם ברצונך לבטל את הגדרת נעילה מרגע שהיא אופשרה, הקש על  בפינה הימנית העליונה של מסך הבית כדי להיכנס כמנהל.

 אינה מוצגת כאשר הגדרת נעילה מושבתת. אם ברצונך לאפשר הגדרה זו, גש אל הצד הבא.

2. בחר הגדרות.

3. בחר ניהול מערכת < הגדרות מנהל מערכת.

4. בחר **On** או **Off** בתור הגדרת נעילה.

## הגדרת הגדרת נעילה מתוך Web Config

1. בחר בלשונית *Control Panel < Device Management*.

2. בחר **ON** או **OFF** עבור *Panel Lock*.

3. לחץ על **OK**.

מידע קשור

← "הפעלת *Web Config* בדפדפן אינטרנט" בעמוד 36

## פריטי הגדרת נעילה בתפריט הגדרות

זוהי רשימה של פריטים שנעולים בתוך תפריט הגדרות בלוח הבקרה באמצעות הגדרת נעילה.

✓: מיועד לנעילה.

- : לא לנעילה.

| הגדרת נעילה | תפריט הגדרות   |
|-------------|--|
| -           | הגדרות בסיסיות   |
| -           | בהירות מסך   |
| -           | צלילים   |
| ✓           | טיימר שינה   |
| ✓           | טיימר כיבוי  |
| ✓           | הגדרות תאריך/שעה                                       |
| *-/✓        | שפה/Language   |
| -           | מקלדת<br>(אפשר שתכונה זו אינה זמינה, בהתאם לאזור שלך). |
| ✓           | פרק הזמן הקצוב חלף                                     |
| ✓           | חיבור מחשב באמצעות USB                                 |
| ✓           | הדלקה ישירה פועלת                                      |
| -           | הגדרות הסורק   |
| -           | לאט  |
| ✓           | תזמון ההפסקה בהזנה כפולה                               |
| -           | פונקציית DFDS  |
| ✓           | הגנה על הנייר  |
| ✓           | גילוי לכלוך על משטח הסריקה                             |
| ✓           | זיהוי על-קולי להזנה כפולה                              |
| ✓           | פרק זמן לסיום מצב הזנה אוטומטית                        |
| ✓           | אישור הנמען  |
| ✓           | ערוך את מסך הבית                                       |

| הגדרת נעילה | תפריט הגדרות                    |  |
|-------------|---------------------------------|--|
| ✓           | פריסה                           |  |
| ✓           | הוסף סמל                        |  |
| ✓           | הסר סמל                         |  |
| ✓           | הזז סמל                         |  |
| ✓           | שחזור ברירת המחדל לתצוגת הסמלים |  |
| ✓           | טפט                             |  |
| ✓           | הגדרות המשתמש                   |  |
| ✓           | תיקייה ברשת/FTP                 |  |
| ✓           | דוא"ל                           |  |
| ✓           | ענן                             |  |
| ✓           | כונן USB                        |  |
| ✓           | הגדרות רשת                      |  |
| ✓           | הגדרת Wi-Fi                     |  |
| ✓           | הגדרת רשת קווית                 |  |
| ✓           | סטטוס הרשת                      |  |
| ✓           | מתקדם                           |  |
| ✓           | הגדרות שירות רשת                |  |
| ✓           | שירותי Epson Connect            |  |
| -           | Document Capture Pro            |  |
| ✓           | שינוי ההגדרות                   |  |
| -           | מנהל אנשי קשר                   |  |
| ✓/-*        | הירשם/מחק                       |  |
| -           | ערכים נפוצים                    |  |
| -           | הצג אפשרויות                    |  |
| -           | אפשרויות חיפוש                  |  |
| ✓           | ניהול מערכת                     |  |





| הגדרת נעילה | תפריט הגדרות                   |  |
|-------------|--------------------------------|--|
| ✓           | מנהל אנשי קשר                  |  |
| ✓           | הגדרות מנהל מערכת              |  |
| ✓           | מגבלות                         |  |
| ✓           | הצפנה באמצעות סיסמה            |  |
| ✓           | סקרי לקוחות                    |  |
| ✓           | הגדרות WSD                     |  |
| ✓           | שחזר להגדרות ברירת המחדל       |  |
| ✓           | עדכון קושחה                    |  |
| -           | פרטי המכשיר                    |  |
| -           | מספר סידורי                    |  |
| -           | גרסה נוכחית                    |  |
| -           | סה"כ סריקות                    |  |
| -           | מספר סריקות חד-צדדיות          |  |
| -           | מספר סריקות דו-צדדיות          |  |
| -           | מספר סריקות עם ניילונית הזנה   |  |
| -           | מספר הסריקות אחרי החלפת הגלגלת |  |
| -           | מספר הסריקות אחרי ניקוי שוטף   |  |
| ✓           | איפוס מספר הסריקות             |  |
| -           | תחזוקת הסורק                   |  |
| -           | ניקוי הגלגלת                   |  |
| -           | החלפת הגלגלת                   |  |
| ✓           | איפוס מספר הסריקות             |  |
| -           | הוראות החלפה                   |  |
| -           | ניקוי שוטף                     |  |
| ✓           | איפוס מספר הסריקות             |  |
| -           | אופן הניקוי                    |  |
| -           | ניקוי משטח הסריקה              |  |

| הגדרת נעילה | תפריט הגדרות                         |
|-------------|--------------------------------------|
| ✓           | הגדרת התראה להחלפת הגלגלת            |
| ✓           | הגדרת התראת מונה                     |
| ✓           | הגדרת ההתראות על ניקוי בזמנים קבועים |
| ✓           | הגדרת האזהרות                        |
| ✓           | הגדרת התראת מונה                     |

\* תוכל לציין אם לאפשר שינויים או לא ב-ניהול מערכת < מגבלות.

## כניסה כמנהל מלוח הבקרה

תוכל להשתמש בכל אחת מהשיטות הבאות כדי להיכנס כמנהל מלוח הבקרה של הסורק.

1. הקש  בפינה הימנית העליונה של המסך.  
 כאשר Authentication Settings מאופשרות, הסמל מוצג במסך ברוכים הבאים (מסך ההמתנה לאימות).  
 כאשר Authentication Settings, מוצגות, הסמל מוצג במסך הבית.
2. הקש כן כאשר מסך האישור מוצג.
3. הזן את סיסמת המנהל.  
 מוצגת הודעה שהכניסה הושלמה ולאחר מכן מוצג מסך הבית בלוח הבקרה.  
 כדי לצאת מהמערכת, הקש  בפינה הימנית העליונה של מסך הבית.

## השבתת הממשק החיצוני

תוכל להשבית את הממשק שבו משתמשים כדי לחבר את ההתקן לסורק. בצע את הגדרות ההגבלה כדי להגביל סריקה מכל מקור אחר פרט לרשת.

להשומת לבך:

ביכולתך להגדיר את הגדרות ההגבלה גם בלוח הבקרה של הסורק.

חיבור מחשב באמצעות USB: הגדרות < הגדרות בסיסיות < חיבור מחשב באמצעות USB

1. גש אל Web Config ובחר את לשונית External Interface < Product Security.
2. בחר **Disable** עבור הפוקנציות שברצונך להגדיר.  
 בחר **Enable** כאשר אתה רוצה לבטל את השליטה.  
 חיבור מחשב באמצעות USB  
 תוכל להגביל את השימוש בחיבור USB מהמחשב. אם ברצונך להגביל אותו, בחר **Disable**.

3. לחץ על OK.

4. ודא שלא ניתן להשתמש ביציאה המושבתת.

חיבור מחשב באמצעות USB

אם מנהל ההתקן הותקן במחשב

חבר את הסורק למחשב עם כבל USB ואז אשר שהסורק אינו סורק.

אם מנהל ההתקן לא הותקן במחשב

:Windows

פתח את מנהל ההתקן ושמור אותו, חבר את הסורק למחשב באמצעות כבל USB, ואז אשר שתכולת תצוגת מנהל ההתקן נשארת ללא שינוי.

:Mac OS

חבר את הסורק למחשב באמצעות כבל USB ואז אשר שאין ביכולתך להוסיף את הסורק מתוך מדפסות וסורקים.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

---

## ניטור סורק מרוחק

### בדיקת מידע עבור סורק מרוחק

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

Product Status

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

Network Status

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

Usage Status

בדוק את היום הראשון של הסריקה, את ספירת הסריקה, וכו'.

Hardware Status

בדוק את הסטטוס של כל פונקציה של הסורק.

Panel Snapshot

מציגה תצלום של המסך המוצג בלוח הבקרה של המדפסת.

## קבלת התראות בדואר אלקטרוני כאשר מתרחשים אירועים

### אודות התראות דואר אלקטרוני

זוהי פונקציית ההודעות השולחת דוא"ל לכתובת שצויינה במקרה של אירועים כמו עצירת סריקה או שגיאת סורק. תוכל לרשום עד חמשה יעדים ולהגדיר את הגדרות ההודעה עבור כל יעד. על מנת להשתמש בפונקציה זו, עליך להגדיר את שרת הדוא"ל לפני שתגדיר הודעות.

מידע קשור

← "הגדרת שרת דואר" בעמוד 42

### הגדרת הודעות דוא"ל

הגדר הודעות דוא"ל באמצעות Web Config.

1. גש אל Web Config ובחר את לשונית **Email Notification < Device Management**.

2. בחר נושא הודעת הדוא"ל.

בחר את התוכן שיוצג בשורת הנושא מתוך שני תפריטים נפתחים.

התכולה הנבחרת תוצג לצד **Subject**.

לא ניתן להגדיר את אותה תכולה משמאל ומימין.

כאשר מספר התווים בתוך **Location** חורג אל מעבר ל- 32 בייטים, מושמטים תווים החורגים אל מעבר ל- 32 בייטים.

3. הזן את כתובת הדוא"ל עבור שליחת הודעת הדוא"ל.

השתמש בתווים A-Z a-z 0-9 ! # \$ % & \* ' / . = ? ^ \_ { | } ~ @ , והזן בין 1 לבין 255 תווים.

4. בחר בשפה להתראות הדואר האלקטרוני.

5. בחר את תיבת הסימון לצד האירוע שעבורו אתה רוצה לקבל הודעה.

מספר **Notification Settings** מקושר למספר היעד של **Email Address Settings**. לדוגמה:

אם ברצונך לשלוח הודעה אל כתובת הדוא"ל שהוגדרה עבור מספר 1 ב-**Email Address Settings** כאשר משנים את סיסמת המנהל, בחר את תיבת הסימון עבור עמודה 1 בשורת **Administrator password changed**.

6. לחץ על OK.

אשר שקרות אירוע יגרום לשליחת הודעת דוא"ל.

לדוגמה: סיסמת המנהל הוחלפה.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

פריטים עבור הודעת דוא"ל

| הגדרות והסבר                                 | פריטים                         |
|--|--------------------------------|
| הודעה כאשר החולפה סיסמת המנהל.               | Administrator password changed |
| הודעה כאשר מתרחשת שגיאת סורק.                | Scanner error                  |
| הודעה כאשר מתרחשת שגיאה בממשק ה-LAN האלחוטי. | תקלת Wi-Fi                     |

## פתרון בעיות

### שכחת את סיסמת המנהל שלך

אתה זקוק לעזרה מעובדי שירות. צור קשר עם הסוכן המקומי שלך.

לתשומת לבך:

להלן מוצגים הערכים הראשוניים עבור מנהל Web Config.

שם משתמש: ללא (ריק)

סיסמה: המספר הסידורי של הסורק

כדי למצוא את המספר הסידורי, בדוק את התווית המחוברת אל גב הסורק. אם תשחזר את הגדרות ברירת המחדל עבור סיסמת המנהל שלך, היא תאופס לערכים המקוריים שלה.

---

# הגדרות אבטחה מתקדמות

|     |                                      |
|-----|--------------------------------------|
| 95  | הגדרות אבטחה ומניעת סכנה             |
| 96  | בקרה באמצעות פרוטוקולים              |
| 99  | שימוש באישור דיגיטלי                 |
| 105 | תקשורת SSL/TLS עם הסורק              |
| 106 | תקשורת מוצפנת באמצעות IPsec/סינון IP |
| 119 | חיבור הסורק לרשת IEEE802.1X          |
| 121 | פתירת בעיות עבור אבטחה מתקדמת        |

## הגדרות אבטחה ומניעת סכנה

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

עבור סורקים שאין להם הגנת מפני גישה מבחוץ, יהיה ניתן לקרוא מהאינטרנט את אנשי הקשר השמורים בסורק.

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

הגדר את הסורק כנדרש בהתאם לתנאים הדרושים לסביבה שבנית.

| שם              | סוג מאפיין   | מה להגדיר  | מה למנוע  |
|-----------------|--|--|---|
| שליטה בפרוטוקול | שולט בפרוטוקולים ובשירותים שישמשו לשם תקשורת בין סורקים לבין מחשבים, ומאפשר ומשבית מאפיינים.   | 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.  |
| תקשורת SSL/TLS  | תכולת התקשורת מוצפנת בתקשורת SSL/TLS כאשר ניגשים מהסורק אל שרת Epson דרך האינטרנט, כגון תקשורת עם המחשב באמצעות דפדפן אינטרנט תוך שימוש ב-Epson Connect, ועדכון קושחה.               | השג אישור החתום על ידי רשות אישורים, ואז יבא אותו לתוך הסורק.                        | איפוס זיהוי של סורק 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 סריקה ומידע הגדרה. |
| 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 בלתי מאובטח. | צור מדיניות בסיסית ומדיניות אישית להגדרת הלקוח או סוג הנתונים שיכולים לגשת אל הסורק. | הגן מפני גישה בלתי מורשית, ומפני פגיעה בלתי חוקית ויירוט של נתוני תקשורת המגיעים אל הסורק.  |
| IEEE 802.1X     | מאפשר רק למשתמשים מאומתים להתחבר אל הרשת. מאפשר רק למשתמש מורשה להשתמש בסורק.  | הגדרת האימות עבור שרת ה-RADIUS (שרת אימות).  | מגן על הסורק מפני גישה ושימוש בלתי מורשים.  |

מידע קשור

- ← "בקרה באמצעות פרוטוקולים" בעמוד 96
- ← "תקשורת SSL/TLS עם הסורק" בעמוד 105
- ← "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 106
- ← "חיבור הסורק לרשת IEEE802.1X" בעמוד 119

## הגדרות תכונת אבטחה

בעת הגדרה של סינון IPsec/IP או IEEE 802.1X, מומלץ לגשת אל Web Config באמצעות SSL/TLS כדי לתקשר מידע הגדרות על מנת לצמצם את סיכוני האבטחה כמו גישה שלא כדן או יירוט. דאג להגדיר את התצורה של סיסמת המנהל לפני שתגדיר סינון IPsec/IP או IEEE 802.1X.

## בקרה באמצעות פרוטוקולים

תוכל לסרוק באמצעות מגוון נתיבים ופרוטוקולים. כמו כן, תוכל להשתמש בסריקת רשת גם ממספר בלתי-ספציפי של מחשבי רשת. תוכל לצמצם את סיכוני האבטחה שאינם מכוונים באמצעות הגבלת הסריקה מנתיבים מסוימים או באמצעות בקרה על הפונקציות הזמינות.

## בקרת פרוטוקולים

הגדר את התצורה של הגדרות הפרוטוקול שהסורק תומך בהן.

1. גש אל Web Config ואז בחר את לשונית Protocol < tab Network Security.
  2. הגדר כל פריט.
  3. לחץ על Next.
  4. לחץ על OK.
- ההגדרות יחולו על הסורק.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## פרוטוקולים שניתן לאפשר או להשבית

| תיאור   | פרוטוקול         |
|---|------------------|
| תוכל לציין אם להשתמש ב-BonjourBonjour .. משמש לחיפוש אחר התקנים, לסריקה וכדומה.                         | Bonjour Settings |
| תוכל להפעיל ולהשבית את הפונקציה SLPSLP. משמש לסריקות בדחיפה וחיפוש אחר רשתות דרך EpsonNet Config.       | SLP Settings     |
| תוכל להפעיל ולהשבית את הפונקציה WSD. כאשר הפונקציה מאופשרת, תוכל להוסיף התקני WSD ולסרוק דרך יציאת WSD. | WSD Settings     |
| תוכל להפעיל ולהשבית את הפונקציה LLTD. כאשר הפונקציה מאופשרת, היא מוצגת על מפת הרשת של Windows.          | LLTD Settings    |



| פרוטוקול            | תיאור   |
|---------------------|---|
| 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.                                      |

## פריטי הגדרת פרוטוקולים

### Bonjour Settings

| 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 | מציג את שם השירות אצל Bonjour.                              |
| Location             | מציג את שם המיקום אצל Bonjour.                              |
| Wide-Area Bonjour    | הגדר אם להשתמש ב-Wide-Area Bonjour.                         |

### SLP Settings

| פריטים     | ערך ההגדרה ותיאורה   |
|------------|--|
| Enable SLP | בחר בפריט זה כדי להפוך את הפונקציה SLP לזמינה. הוא משמש במקרים כמו חיפוש רשת בתוך EpsonNet Config. |

### WSD Settings

| פריטים                 | ערך ההגדרה ותיאורה  |
|------------------------|---|
| Enable WSD             | בחר בפריט זה כדי לאפשר הוספת התקנים באמצעות WSD, וכדי לסרוק 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

| פריטים      | ערך ההגדרה ותיאורה   |
|-------------|--|
| 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

| פריטים       | ערך ההגדרה ותיאורה   |
|--------------|--|
| 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

| פריטים                      | ערך ההגדרה ותיאורה   |
|-----------------------------|--|
| Enable SNMPv1/v2c           | בחר בפריט כדי להפוך את SNMPv1/v2c לזמין.                                 |
| 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).                                   |

### SNMPv3 Settings

| פריטים                  | ערך ההגדרה ותיאורה  |
|-------------------------|---|
| 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     |   |

| פריטים           | ערך ההגדרה ותיאורה  |
|------------------|---|
| Algorithm        | בחר אלגוריתם להצפנה עבור SNMPv3.  |
| Password         | הזן את הסיסמה להצפנה עבור SNMPv3.<br>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. |

## שימוש באישור דיגיטלי

### אודות אישורים דיגיטליים

#### CA-signed Certificate

זהו מסמך חתום על ידי CA (Certificate Authority). תוכל להשיג אותו באמצעות פניה אל Certificate Authority. אישור זה מאשר את קיומו של הסורק ומשמש עבור תקשורת SSL/TLS באופן המאפשר לך להבטיח את בטיחות נתוני התקשורת.

כאשר אתה משתמש בו עבור תקשורת SSL/TLS, הוא משמש כאישור שרת. כאשר מגדירים אותו עבור סינון IPsec/IP או תקשורת IEEE 802.1X הוא משמש כאישור לקוח.

#### אישור CA

זהו אישור הנמצא בשרשרת של CA-signed Certificate, הנקרא גם אישור CA ביניים. הוא משמשת את דפדפן האינטרנט לתקף את הנתיב של אישור הסורק בעת גישה אל השרת של הצד השני או Web Config. עבור אישור CA, הגדר מתי לתקף את נתיב אישור השרת הניגש מהסורק. עבור הסורק, הגדר לאשר את נתיב ה-CA-signed Certificate עבור חיבור SSL/TLS.

תוכל להשיג את אישור ה-CA של הסורק מרשות האישורים המנפיקה אישורי CA. תוכל גם להשיג את אישור ה-CA המשמש כדי לתקף את השרת של הצד האחר מרשות האישורים שהוציאה את ה-CA-signed Certificate של השרת האחר.

#### Self-signed Certificate

זהו אישור שהסורק חותם עליו ומנפיק בעצמו. הוא נקרא גם אישור השורש. עקב העובדה שהמנפיק מאשר את עצמו, אין הוא אמין ואין ביכולתו למנוע התחזות.

יש להשתמש בו כאשר מבצעים את הגדרות האבטחה ומבצעים תקשורת SSL/TLS פשוטה ללא CA-signed Certificate.

אם תשתמש באישור זה עבור תקשורת SSL/TLS, אפשר שתוצג התראת אבטחה בדפדפן האינטרנט משום שהאישור אינו רשום בדפדפן אינטרנט. תוכל להשתמש ב-Self-signed Certificate אך ורק לתקשורת SSL/TLS.

מידע קשור

◀ "הגדרת התצורה של CA-signed Certificate" בעמוד 100

- ← "עדכון אישור בחתימה עצמית" בעמוד 103
- ← "הגדרת התצורה של CA Certificate" בעמוד 104

## הגדרת התצורה של CA-signed Certificate

### 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, ואז בחר את לשונית Network Security. בשלב הבא, בחר SSL/TLS < Certificate, או IPsec/IP Filtering < Client Certificate או IEEE802.1X < Client Certificate. בלא קשר למה שתבחר, תוכל לקבל את אותו אישור ולהשתמש בה במשותף.

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 בלשונית Network Security. 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 ביעד.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

### פריטי הגדרת CSR

| פריטים   | הגדרות והסבר   |
|--|--|
| Key Length   | בחר אורך מפתח ל-CSR.   |
| Common Name  | <p>תוכל להזין בין 1 ל-128 תווים. אם זו כתובת IP, עליה להיות כתובת IP סטטית. תוכל להזין בין 1 לבין 5 כתובות IPv4, כתובות IPv6, שמות מארחים, שמות FQDN באמצעות הפרדתם בפסיקים.</p> <p>המרכיב הראשון מאוחסן בשם השמות, האלמנטים האחרים מאוחסנים בשדה הכינוי של נושא האישור.</p> <p>לדוגמה:</p> <p>כתובת ה-IP של הסורק: 192.0.2.123, שם הסורק: EPSONA1B2C3</p> <p>Common Name:<br/>192.0.2.123, EPSONA1B2C3.local, EPSONA1B2C3</p> |
| /Organization<br>/Locality/Organizational Unit<br>State/Province | <p>תוכל להזין בין 0 ל-64 תווים ב-ASCII (0x20-0x7E). תוכל להפריד בין שמות ייחודיים באמצעות פסיק.</p>  |
| Country  | הזן קוד מדינה בשתי ספרות המצוין ב-ISO-3166.  |
| Sender's Email Address   | <p>תוכל להזין את כתובת הדוא"ל של השולח עבור הגדרות שרת הדוא"ל. הזן את אותה כתובת דוא"ל כמו זו של <b>Sender's Email Address</b> עבור הלשונית <b>Network &lt; Basic &lt; Email Server</b>.</p>   |

### ייבוא אישור החתום בידי רשות אישורים

יבא את קובץ CA-signed Certificate שהושג אל הסורק.

**חשוב!**

ודא שהתאריך והשעה בסורק מוגדרים כהלכה. אפשר שהאישור חסר תוקף.

אם אתה מקבל אישור באמצעות CSR הנוצר מ-Web Config, תוכל לייבא את האישור פעם אחת.

1. גש אל Web Config, ואז בחר את לשונית **Network Security**. 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. הגדר את **CA Certificate 1** ואת **CA Certificate 2** כאשר אתה מוודא את נתיב האישור בדפדפן האינטרנט שניגש אל הסורק.

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 את התצורה.

**CA Certificate 2/CA Certificate 1**: אופציונלי

אישור בתבנית PEM/DER שהתקבל ממחשב

**Private Key**: עליך להגדיר.

**Password**: אל תגדיר את התצורה.

**CA Certificate 2/CA Certificate 1**: אופציונלי

אישור בתבנית PKCS#12 שהתקבל ממחשב

**Private Key**: אל תגדיר את התצורה.

**Password**: אופציונלי

**CA Certificate 2/CA Certificate 1**: אל תגדיר את התצורה.

4. לחץ על **OK**.

מוצגת הודעת סיום.

לתשומת לבך:

לחץ על **Confirm** כדי לאמת את נתוני האישור.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

אישור בחתימת CA ייבוא פריטי הגדרה

| הגדרות והסבר  | פריטים                                   |
|---|--|
| בחר את התבנית של האישור.<br>עבור חיבור SSL/TLS מוצג <b>Server Certificate</b> .<br>עבור סינון IPsec/IP או IEEE 802.1X, מוצג <b>Client Certificate</b> . | Server Certificate או Client Certificate |
| אם השגת אישור בתבנית PEM/DER באמצעות CSR שנוצר ממחשב, ציין קובץ מפתח פרטי התואם לאישור.   | Private Key                              |
| אם תבנית הקובץ היא <b>Certificate with Private Key (PKCS#12)</b> , הזן את הסיסמה להצפנת המפתח הפרטי שהוגדר כאשר השגת את האישור.                         | Password                                 |

| הגדרות והסבר   | פריטים           |
|--|------------------|
| אם תבנית האישור שלך היא Certificate (PEM/DER), יבא אישור של רשות האישורים המנפיקה CA-signed Certificate המשמש כאישור שרת. ציין קובץ במידת הצורך. | CA Certificate 1 |
| אם תבנית האישור שלך היא Certificate (PEM/DER), יבא אישור של רשות האישורים המנפיקה CA Certificate 1. ציין קובץ במידת הצורך.                       | CA Certificate 2 |

## 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, ואז בחר את לשונית Network Security. 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

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## עדכון אישור בחתימה עצמית

כתוצאה מכך שהסורק מנפיק את Self-signed Certificate, תוכל לעדכן אותו כאשר תוקפו יפוג או כאשר ישתנה התוכן המתואר בו.

1. גש אל Web Config ובחר את Network Security < tab SSL/TLS < Certificate.

2. לחץ על Update.

3. הזן Common Name.

תוכל להזין עד 5 כתובות IPv4, כתובות IPv6, שמות מארח, FQDNים בין 1 לבין 128 תווים ולהפריד אותם בפסיקים. הפרמטר הראשון נשמר בשם המשותף, והאחרים נשמרים בשדה הכינוי עבור הנושא של האישור.

דוגמה:

כתובת ה-IP של הסורק: 192.0.2.123, שם הסורק: EPSONA1B2C3  
 שם משותף: EPSONA1B2C3.local, 192.0.2.123, EPSONA1B2C3

4. ציין תקופת תוקף עבור האישור.

5. לחץ על Next.

מוצגת הודעת אישור.

6. לחץ על OK.

הסורק עודכן.

לתשומת לבך:

תוכל לבדוק את המידע על האישור בלשונית *Network Security < SSL/TLS < Certificate < Self-signed Certificate* ולחץ *Confirm*.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## הגדרת התצורה של CA Certificate

כאשר את מגדיר את CA Certificate, ביכולתך לתקף את הנתיב אל אישור CA של השרת שאליו ניגש הסורק. הגדרה זו עלולה למנוע התחזות.

תוכל להשיג את CA Certificate מרשות האישורים המנפיקה את CA-signed Certificate.

## ייבוא CA Certificate

יבא את קובץ CA Certificate אל הסורק.

1. גש אל Web Config ואז בחר את לשונית *CA Certificate < Network Security*.

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

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## מחיקת CA Certificate

תוכל למחוק את ה- CA Certificate המיובא.

1. גש אל Web Config, ואז בחר את לשונית *CA Certificate < Network Security*.

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

3. אשר שאתה רוצה למחוק את האישור בהודעה המוצגת.



4. לחץ **Reboot Network**, ואז בדוק שאישור ה-CA שנמחק אינו רשום במסמך שעודכן.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

---

## 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.

### הגדרת התצורה של ההגדרות הבסיסיות של SSL/TLS

אם הסורק תומך בתכונת שרת HTTPS, תוכל להשתמש בתקשורת SSL/TLS כדי להצפין את התקשורות. תוכל להגדיר את התצורה ולנהל את הסורק באמצעות Web Config תוך אבטחת האבטחה. הגדר את התצורה של חוזק ההצפנה ותכונת הניתוב מחדש.

1. גש אל **Web Config** ובחר את הלשונית **Basic < SSL/TLS < Network Security**.

2. ברך ערך עבור כל פריט.

**Encryption Strength**

בחר את רמת חוזק ההצפנה.

**Redirect HTTP to HTTPS**

נתב מחדש אל HTTPS כאשר מתבצעת גישה אל HTTP.

3. לחץ על **Next**.

מוצגת הודעת אישור.

4. לחץ על **OK**.

הסורק עודכן.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

### הגדרת אישור שרת עבור הסורק

1. גש אל **Web Config** ובחר את הלשונית **Certificate < SSL/TLS < Network Security**.

2. ציין אישור לשימוש ב-**Server Certificate**.

**Self-signed Certificate**

אישור בחתימה עצמית הופק בידי הסורק. אם אין ברשותך אישור חתום בידי רשות אישורים, בחר באפשרות זו.

## CA-signed Certificate □

אם כבר קיים ברשותך אישור חתום בידי רשות אישורים ואתה מייבא אותו, תוכל לציין זאת.

3. לחץ על **Next**.

כעת תוצג הודעת אישור.

4. לחץ על **OK**.

הסורק מעודכן.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

← "הגדרת התצורה של CA-signed Certificate" בעמוד 100

← "הגדרת התצורה של CA Certificate" בעמוד 104

---

## תקשורת מוצפנת באמצעות IPsec/סינון IP

### אודות IPsec/IP Filtering

תוכלן לסנן תנועה על פי כתובות IP, שירותים ויאה באמצעות השימוש בפונקצית הסינון IPsec/IP. 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.

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 תצורת מדיניות ברירת המחדל

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.

1. גש אל **Web Config**, ואז בחר את לשונית **Basic < IPsec/IP Filtering < Network Security**.

2. הזן ערך עבור כל פריט.

3. לחץ על **Next**.

כעת תוצג הודעת אישור.

4. לחץ על **OK**.

הסורק מעודכן.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## פריטי הגדרת Default Policy

### Default Policy

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

### Access Control

הגדר שיטת בקרה לתנועת מנות IP.

| פריטים        | הגדרות והסבר  |
|---------------|---|
| 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 IKE Version. בחר אחד מהם בהתאם להתקן אליו מחובר הסורק.

IKEv1

הפריטים הבאים מוצגים כאשר אתה בוחר IKEv1 עבור IKE Version.

| פריטים                 | הגדרות והסבר  |
|------------------------|---|
| 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.

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

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

### Encapsulation

אם אתה בוחר IPsec עבור **Access Control**, עליך להגדיר מצב עטיפת נתונים.

| פריטים         | הגדרות והסבר   |
|----------------|--|
| Transport Mode | <p>אם אתה משתמש בסורק רק באותה רשת LAN, בחר באפשרות זו. מנות IP משכבה 4 ומעלה הן מוצפנות.</p>  |
| Tunnel Mode    | <p>אם אתה משתמש בסורק ברשת עם תמיכה באינטרנט כגון IPsec-VPN, בחר באפשרות זו. הכותרת והנתונים של מנות ה-IP הם מוצפנים.</p> <p><b>Remote Gateway(Tunnel Mode)</b>: אם תבחר <b>Tunnel Mode</b> עבור <b>Encapsulation</b>, הזן כתובת שער באורך 1-39 תווים.</p> |

## Security Protocol □

אם אתה בוחר IPsec עבור Access Control, בחר באחת מהאפשרויות.

| פריטים | הגדרות והסבר   |
|--------|--|
| 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 □

מומלץ לבחור Any עבור כל ההגדרות או בחר פריט אחר מ-Any עבור הגדרה. אם תבחר Any עבור חלק מההגדרות ותבחר פריט אחר מאשר Any עבור ההגדרות האחרות, אפשר שלא יהיה ביכולתו של ההתקן לתקשר בהתאם להתקן האחר שברצונך לאמת.

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

## הגדרת תצורת מדיניות קבוצתית

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.

1. גש אל Web Config, ואז בחר את לשונית Network Security < 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.

## 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.

| פריטים        | הגדרות והסבר  |
|---------------|---|
| 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**.

לתשומת לבך:

אם הוקצתה כתובת IPv6 באופן אוטומטי, ייתכן שהחיבור לא יהיה זמין. הגדר כתובת IPv6 סטטית.

## 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.

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.

| פריטים       | הגדרות והסבר   |
|--------------|--|
| 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: 5220, 119, 80, 20. 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: 5220, 143, 80, 25. אם לא תזין מספר יציאה, כל היציאות תהיינה בבקרה.

### IKE Version

בחר **IKEv1** או **IKEv2** עבור **IKE Version**. בחר אחד מהם בהתאם להתקן אליו מחובר הסורק.

### IKEv1

הפריטים הבאים מוצגים כאשר אתה בוחר **IKEv1** עבור **IKE Version**.

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

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

## Encapsulation

אם אתה בוחר IPsec עבור Access Control, עליך להגדיר מצב עטיפת נתונים.

| פריטים         | הגדרות והסבר  |
|----------------|---|
| 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.<br>Remote Gateway(Tunnel Mode): אם תבחר Tunnel Mode עבור Encapsulation, הזן כתובת שער באורך 1-39 תוים. |

## Security Protocol

אם אתה בוחר IPsec עבור Access Control, בחר באחת מהאפשרויות.

| פריטים | הגדרות והסבר   |
|--------|--|
| ESP    | בחר באפשרות זו כדי להבטיח תקינות של אימות ומידע, וכדי להצפין נתונים. |

| פריטים | הגדרות והסבר   |
|--------|--|
| AH     | בחר באפשרות זו כדי להבטיח תקינות של אימות ומידע. תוכל להשתמש ב-IPsec גם אם נאסר על הצפנת נתונים. |

### Algorithm Settings

מומלץ לבחור **Any** עבור כל ההגדרות או בחר פריט אחר מ-**Any** עבור הגדרה. אם תבחר **Any** עבור חלק מההגדרות ותבחר פריט אחר מאשר **Any** עבור ההגדרות האחרות, אפשר שלא יהיה ביכולתו של ההתקן לתקשר בהתאם להתקן האחר שברצונך לאמת.

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

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

| הגדרות Local Address (Scanner) |                    |      |   |                              |
|--------------------------------|--------------------|------|---|------------------------------|
| Any addresses <sup>3*</sup>    | IPv6 <sup>2*</sup> | IPv4 |   |                              |
| ✓                              | -                  | ✓    | IPv4 <sup>1*</sup>                      | הגדרות Remote Address (Host) |
| ✓                              | ✓                  | -    | IPv6 <sup>1*</sup> , IPv6 <sup>2*</sup> |                              |
| ✓                              | ✓                  | ✓    | ריק                                     |                              |

<sup>1\*</sup> אם IPsec נבחר עבור **Access Control**, לא תוכל לפרט באורך קידומת.

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

<sup>3\*</sup> למעט כתובות קישור מקומי מסוג IPv6.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## הפניות לשמות שירות במדיניות קבוצה

לתשומת לבך:

שירותים שאינם זמינים מופיעים בתצוגה אך אי אפשר לבחור אותם.

| שם השירות                   | סוג פרוטוקול | מספר יציאה מקומית | מספר יציאה מרוחקת | תכונות מבוקרות   |
|-----------------------------|--------------|-------------------|-------------------|--|
| Any                         | -            | -                 | -                 | כל השירותים  |
| ENPC                        | UDP          | 3289              | כל יציאה          | חיפוש אחר סורק מיישומים כגון Epson Device Admin ומנהל התקן הסורק                                     |
| SNMP                        | UDP          | 161               | כל יציאה          | רכישה והגדרת תצורה של MIB מתוך אפליקציות כמו Epson Device Admin ומנהל הסורק של Epson                 |
| WSD                         | TCP          | כל יציאה          | 5357              | בקרת WSD   |
| WS-Discovery                | UDP          | 3702              | כל יציאה          | חיפוש סורקי WSD  |
| Network Scan                | TCP          | 1865              | כל יציאה          | העברת נתונים סרוקים מ-Document Capture Pro   |
| Network Push Scan           | TCP          | כל יציאה          | 2968              | רכישת נתוני עבודה עבור סריקת דחיפה מ-Document Capture Pro  |
| Network Push Scan Discovery | UDP          | 2968              | כל יציאה          | חיפוש מחשב מסורק   |
| FTP Data (Remote)           | TCP          | כל יציאה          | 20                | לקוח FTP (מעביר נתונים סרוקים) עם זאת, פעולה זו יכולה לשלוט רק בשרת FTP שמתמש ביציאה מרוחקת מספר 20. |
| FTP Control (Remote)        | TCP          | כל יציאה          | 21                | לקוח FTP (שליטה בנתונים סרוקים שהועברו)  |
| CIFS (Remote)               | TCP          | כל יציאה          | 445               | לקוח CIFS (מעביר נתונים סרוקים לתיקה)  |

| שם השירות                         | סוג פרוטוקול | מספר יציאה מקומית | מספר יציאה מרוחקת | תכונות מבוקרות                           |
|-----------------------------------|--------------|-------------------|-------------------|--|
| NetBIOS Name Service (Remote)     | UDP          | כל יציאה          | 137               | לקוח CIFS (מעביר נתונים סרוקים לתיקה)    |
|                                   |              |                   | 138               |  |
|                                   |              |                   | 139               |  |
| NetBIOS Datagram Service (Remote) | UDP          | כל יציאה          | 138               | לקוח CIFS (מעביר נתונים סרוקים לתיקה)    |
| NetBIOS Session Service (Remote)  | TCP          | כל יציאה          | 139               |  |
| HTTP (Local)                      | TCP          | 80                | כל יציאה          |  |
| HTTPS (Local)                     | TCP          | 443               | כל יציאה          |  |
| HTTP (Remote)                     | TCP          | כל יציאה          | 80                | לקוח HTTP(S) (עדכון הקושחה ותעודת השורש) |
| 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 את התצורה.

קבלת נתוני סריקה והגדרות סורק

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 HTTP (Local) ,SNMP ,ENPC ,HTTPS (Local) וכן Network Scan

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 תצורה של אישור עובר סינון IPsec/IP

הגדר את התצורה של אישור עובר סינון IPsec/IP. כאשר תגדיר אותו, תוכל להשתמש באישור כשיטת אימות עבור סינון IPsec/IP. אם תרצה להגדיר את רשות האישורים, גש אל CA Certificate.

1. גש אל Web Config, ואז בחר את לשונית Network Security < IPsec/IP Filtering < Client Certificate.

2. יבא את האישור ב-Client Certificate.

אם כבר ייבאת אישור שפורסם בידי רשות אישורים, תוכל להעתיק את האישור ולהשתמש בו בסינון IPsec/IP. כדי להעתיק, בחר את האישור מתוך Copy From, ואז לחץ Copy.

מידע קשור

- ← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36
- ← "הגדרת התצורה של CA-signed Certificate" בעמוד 100
- ← "הגדרת התצורה של CA Certificate" בעמוד 104

## חיבור הסורק לרשת IEEE802.1X

### הגדרת תצורה לרשת IEEE 802.1X

כאשר מגדירים IEEE 802.1X עבור הסורק, תוכל להשתמש בו ברשת המוחברת לשרת RADIUS, למתג LAN עם פונקציית אימות, או נקודת גישה.

1. גש אל Web Config, ואז בחר את לשונית **Basic < IEEE802.1X < Network Security**.

2. הזן ערך עבור כל פריט.

אם תרצה להשתמש בסורק ברשת Wi-Fi, לחץ על **Wi-Fi Setup** ובחר או הזן SSID. **לתשומת לבך:** תוכל לשתף את ההגדרות הללו בין **Ethernet ל-Wi-Fi**.

3. לחץ על **Next**.

כעת תוצג הודעת אישור.

4. לחץ על **OK**.

הסורק מעודכן.

מידע קשור

← ["הפעלת Web Config בדפדפן אינטרנט" בעמוד 36](#)

### פריטי הגדרת רשת IEEE 802.1X

| הגדרות והסבר   | פריטים                 |
|--|------------------------|
| תוכל להפוך הגדרות לזמינות או ללא זמינות בדף <b>(Basic &lt; IEEE802.1X)</b> עבור IEEE802.1X (LAN) (קווי). | IEEE802.1X (Wired LAN) |
| מוצג מצב החיבור של IEEE802.1X (Wi-Fi).   | IEEE802.1X (Wi-Fi)     |
| שיטת החיבור של הרשת הנוכחית מוצגת.   | Connection Method      |
| בחר באפשרות לשיטת אימות בין הסורק לשרת RADIUS.   | EAP Type               |
| עליך להשיג ולייבא אישור חתום בידי רשות אישורים.  | EAP-TLS                |
|  | PEAP-TLS               |
| עליך להגדיר סיסמה.   | PEAP/MSCHAPv2          |
|  | EAP-TTLS               |
| הגדר מזהה לשימוש עבור אימות שרת RADIUS. הזן 1 עד 128 תווי ASCII בגודל בייט אחד (עד 0x7E).                | User ID                |

| הגדרות והסבר  | פריטים                 |
|---|------------------------|
| הגדר סיסמה כדי לאמת את הסורק.<br>הזן 1 עד 128 תווי ASCII בגודל בייט אחד (0x20 עד 0x7E). אם אתה משתמש בשרת Windows בתור שרת RADIUS, תוכל להזין 127 תוים לכל היותר.   | Password               |
| הזן את הסיסמה שהגדרת לאישור.  | Confirm Password       |
| 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.<br>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 EAP Type, תוכל להגדיר שם אנונימי במקום מספר זיהוי משתמש לשלב 1 של אימות PEAP.<br>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                 |

## הגדרת התצורה של אישור עבור IEEE 802.1X

הגדר את תצורתו של לקוח עבור IEEE802.1X. כאשר תגדיר אותו, תוכל להשתמש ב-EAP-TLS וב-PEAP-TLS כשיטת אימות עבור IEEE 802.1X. אם תרצה להגדיר את אישור רשות האישורים, גש אל CA Certificate.

1. גש אל Web Config, ואז בחר את לשונית IEEE802.1X < Network Security < Client Certificate.

2. הזן את האישור ב-Client Certificate.

אם כבר ייבאת אישור שפורסם בידי רשות אישורים, תוכל להעתיק את האישור ולהשתמש בו ב-IEEE802.1X. כדי להעתיק, בחר את האישור מתוך Copy From, ואז לחץ Copy.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36



## פתירת בעיות עבור אבטחה מתקדמת

### שחזור הגדרות האבטחה

כאשר אתה יוצר סביבה בעלת רמת אבטחה גבוהה כגון סינון IPsec/IP, 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 תוך שימוש ב-Web Config

תוכל להשבית את IPsec/IP Filtering תוך שימוש ב-Web Config.

1. גש אל Web Config ובחר את הלשונית **Basic < IPsec/IP Filtering < Network Security**.

2. השבת את IPsec/IP Filtering.

### בעיות בשימוש בתכונות אבטחת רשת

#### שכחתי מפתח ששותף מראש

הגדר מחדש את תצורת מפתח ששותף מראש.

כדי לשנות את המפתח, גש אל Web Config ובחר את לשונית **Network Security < 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

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

← "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 106

### לא ניתן לקיים תקשורת באמצעות IPsec

ציין את האלגוריתם שהסורק או המחשב אינם תומכים בו.

הסורק תומך באלגוריתמים שלהלן. בדוק את הגדרות המחשב.

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

| שיטות אבטחה        | אלגוריתמים   |
|--------------------|--|
| IKE                | ,DH Group14 ,DH Group5 ,DH Group2 ,DH Group1 ,DH Group18 ,DH Group17 ,DH Group16 ,DH Group15 ,DH Group22 ,DH Group21 ,DH Group20 ,DH Group19 ,DH Group26 ,DH Group25 ,DH Group24 ,DH Group23 ,DH ,*DH Group29 ,*DH Group28 ,*DH Group27 *Group30 |
| אלגוריתם הצפנה ESP | AES- ,AES-CBC-256 ,AES-CBC-192 ,AES-CBC-128 ,3DES ,AES-GCM-256 ,AES-GCM-192 ,GCM-128   |
| אלגוריתם אימות ESP | MD5 ,SHA-512 ,SHA-384 ,SHA-256 ,SHA-1  |
| אלגוריתם אימות AH  | MD5 ,SHA-512 ,SHA-384 ,SHA-256 ,SHA-1  |

\* זמין עבור IKEv2 בלבד

מידע קשור

← "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 106

## התקשורת נקטעת בפתאומיות

כתובת ה-IP של הסורק שונתה או שלא ניתן להשתמש בה.

כאשר כתובת ה-IP הרשומה ככתובת המקומית ב- Group Policy שונתה או שלא ניתן להשתמש בה, לא ניתן לבצע תקשורת IPsec. השבת את IPsec באמצעות לוח הבקרה של הסורק.

אם DHCP 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- Network Security) Web Config של הסורק, לשוניית < IPsec/IP Filtering < Basic < Group Policy < (Local Address (Scanner). השתמש בכתובת IP סטטית.

כתובת ה-IP של המחשב שונתה או שלא ניתן להשתמש בה.

כאשר כתובת ה-IP הרשומה ככתובת המרוחקת ב- Group Policy שונתה או שלא ניתן להשתמש בה, לא ניתן לבצע תקשורת IPsec.

השבת את IPsec באמצעות לוח הבקרה של הסורק.

אם DHCP 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- Network Security) Web Config של הסורק, לשוניית < IPsec/IP Filtering < Basic < Group Policy < (Remote Address(Host). השתמש בכתובת IP סטטית.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

← "תקשורת מוצפנת באמצעות IPsec/סינון IP" בעמוד 106

## לא ניתן להתחבר אחרי הגדרת סינון IPsec/IP

הגדרות הסינון של IPsec/IP שגויות.

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 106

## אין גישה לסורק לאחר הגדרות תצורה IEEE 802.1X

ההגדרות של IEEE 802.1X שגויות.

השבת את IEEE 802.1X ואת ה-Wi-Fi מלוח הבקרה של הסורק. חבר את הסורק למחשב, ואז הגדר שנית את תצורת IEEE 802.1X.

חבר את הסורק למחשב, ואז הגדר שנית את תצורת IEEE 802.1X.

מידע קשור

← "הגדרת תצורה לרשת IEEE 802.1X" בעמוד 119

## בעיות במהלך השימוש באישור דיגיטלי

### לא ניתן לייבא CA-signed Certificate

אין התאמה בין CA-signed Certificate לבין המידע ב-CSR.

אם המידע ב-CA-signed Certificate וב-CSR אינו זהה, 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.

CA-signed Certificate גדול מ-5 KB.

לא תוכל לייבא CA-signed Certificate שגודלו עולה על 5KB.

הסיסמה לייבוא האישור שגויה.

הזן את הסיסמה הנכונה. אם שכחת את הסיסמה, לא תוכל לייבא את האישור. השג מחדש את CA-signed Certificate.

מידע קשור

← "ייבוא אישור החתום בידי רשות אישורים" בעמוד 101

## לא ניתן לעדכן אישור בחתימה עצמית

לא הוזן ה-Common Name.

יש להזין Common Name.

הוזנו תוויטם שאין עבורם תמיכה לתוך ה-Common Name.

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

נכללו פסיק או רווח בשם המשותף.

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 103

## לא ניתן ליצור CSR

לא הוזן ה-Common Name.

יש להזין Common Name.

הוזנו תווים שאין עבורם תמיכה לתוך Common Name, Organization, Organizational Unit, Locality, ו-State/Province.

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

נכללו פסיק או רווח בתוך 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 100

## הודעות אזהרה הקשורות לאישור דיגיטלי

| הודעות                      | סיבה/מה לעשות   |
|-----------------------------|---|
| Enter a Server Certificate. | סיבה:<br>לא בחרת קובץ לייבוא.<br>מה לעשות:<br>בחר קובץ ולאחר מכן לחץ על Import. |

| הודעות                           | סיבה/מה לעשות   |
|----------------------------------|---|
| CA Certificate 1 is not entered. | <p><b>סיבה:</b><br/>אישור של רשות אישורים 1 לא הונן אלא רק אישור של רשות אישורים 2.<br/><b>מה לעשות:</b><br/>תחילה עליך לייבא את אישור של רשות אישורים 1.</p> |
| Invalid value below.             | <p><b>סיבה:</b><br/>נתיב הקובץ והסיסמה מכילים תווים שאינם נתמכים.<br/><b>מה לעשות:</b><br/>וודא שהתווים הוננו כהלכה עבור הפריט.</p>                           |
| Invalid date and time.           | <p><b>סיבה:</b><br/>לא הוגדרו תאריך ושעה עבור הסורק.<br/><b>מה לעשות:</b><br/>הגדר את התאריך ואת השעה באמצעות EpsonNet או Web Config Config.</p>              |
| Invalid password.                | <p><b>סיבה:</b><br/>הסיסמה שהוגדרה לאישור רשות האישורים והסיסמה שהוזנה אינן תואמות.<br/><b>מה לעשות:</b><br/>הזן את הסיסמה הנכונה.</p>                        |
| Invalid file.                    | <p><b>סיבה:</b><br/>אינך מייבא את הקובץ בתבנית X509.<br/><b>מה לעשות:</b><br/>וודא שאתה בוחר באישור הנכון שנשלח בידי רשות מאשרת מהימנה.</p>                   |
|                                  | <p><b>סיבה:</b><br/>הקובץ שייבא גודל מדי. גודל הקובץ המקסימלי הנו 5 KB.<br/><b>מה לעשות:</b><br/>אם בחרת בקובץ הנכון, ייתכן שהאישור פגום או מזויף.</p>        |
|                                  | <p><b>סיבה:</b><br/>השרשרת הכלולה באישור אינה תקינה.<br/><b>מה לעשות:</b><br/>למידע נוסף אודות האישור, בקר באתר הרשות המאשרת.</p>                             |

| סיבה/מה לעשות  | הודעות  |
|--|---|
| <p><b>סיבה:</b><br/>קובץ האישור בתבנית PKCS#12 מכיל יותר מ-3 אישורי רשות אישורים.<br/><b>מה לעשות:</b><br/>ייבא כל אישור תוך המרה מתבנית PKCS#12 לתבנית PEM, או ייבא את קובץ האישור בתבנית PKCS#12 שמכיל עד 2 אישורי רשות אישורים.</p>   | <p>Cannot use the Server Certificates that include more than three CA certificates.</p>                           |
| <p><b>סיבה:</b><br/>האישור אינו בתוקף.<br/><b>מה לעשות:</b><br/><input type="checkbox"/> אם האישור פג תוקף, השג וייבא את האישור החדש.<br/><input type="checkbox"/> אם האישור אינו פג תוקף, ודא שהשעה והתאריך מוגדרים כהלכה בסורק.</p>  | <p>The certificate has expired. Check if the certificate is valid, or check the date and time on the product.</p> |
| <p><b>סיבה:</b><br/>אין מפתח פרטי המוצמד לאישור.<br/><b>מה לעשות:</b><br/><input type="checkbox"/> אם האישור הוא בתבנית PEM/DER והוא הושג מ-CSR באמצעות מחשב, ציין את קובץ המפתח הפרטי.<br/><input type="checkbox"/> אם האישור הוא בתבנית PKCS#12 והוא הושג מ-CSR באמצעות מחשב, צור קובץ שיכיל את המפתח הפרטי.</p> | <p>Private key is required.</p>   |
| <p><b>סיבה:</b><br/>ייבאת מחדש את אישור ה-PEM/DER שהושג מ-CSR באמצעות Web Config.<br/><b>מה לעשות:</b><br/>אם האישור הוא בתבנית PEM/DER והוא הושג מ-CSR באמצעות Web Config, תוכל לייבא אותו רק פעם אחת.</p>  |   |
| <p><b>סיבה:</b><br/>לא ניתן לסיים את קביעת התצורה משום שהתקשורת בין הסורק למחשב נכשלה או שלא ניתן לקרוא את הקובץ בגלל שגיאות.<br/><b>מה לעשות:</b><br/>לאחר בדיקת הקובץ שצוין והתקשורת, ייבא שוב את הקובץ.</p>   | <p>Setup failed.</p>  |

מידע קשור

← "אודות אישורים דיגיטליים" בעמוד 99

## מחק אישור החתום על-ידי ר"מ בטעות

אין קובץ גיבוי עבור האישור החתום בידי CA.

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

← "ייבוא אישור החתום בידי רשות אישורים" בעמוד 101

← "מחיקת אישור החתום בידי רשות אישורים" בעמוד 103

---

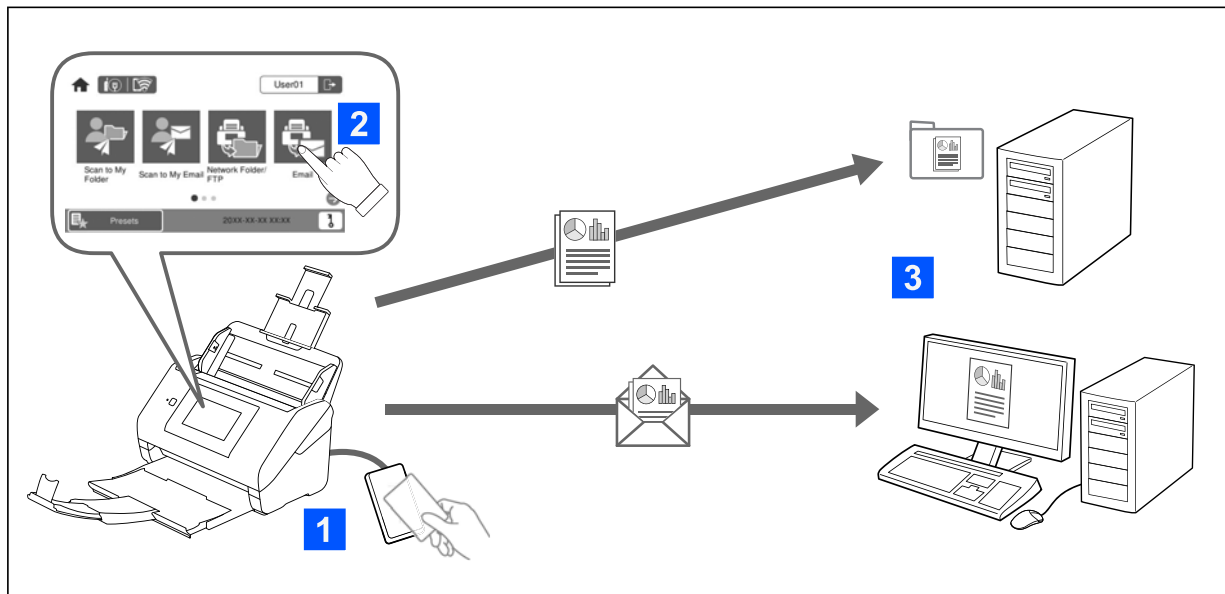
# Authentication Settings



|          |   |
|----------|---|
| 129..... | אודות Authentication Settings                                 |
| 130..... | אודות Authentication Method                                   |
| 132..... | תוכנה לביצוע הגדרות.  |
| 132..... | עדכון קושחת הסורק.  |
| 132..... | חיבור והגדרה של התקן אימות.                                   |
| 139..... | רישום והגדרה של מידע.   |
| 158..... | דיווחי Job History באמצעות Epson Device Admin                 |
| 158..... | כניסה כמנהל מלוח הבקרה.                                       |
| 159..... | השבתת Authentication Settings                                 |
| 159..... | מחיקת מידע Authentication Settings (שחזר להגדרות ברירת המחדל) |
| 160..... | פתרון בעיות.  |



## אודות Authentication Settings



כאשר Authentication Settings מאופשרות, אימות המשתמש דרוש כדי להתחיל בסריקה. תוכל להגדיר את שיטת הסריקה שכל משתמש יכול להפעיל, ולמנוע הפעלות בטעות.

תוכל לציין את כתובת הדוא"ל של המשתמש המאומת בתור יעד הסריקה (Scan to My Email), או לשמור את הנלתונים של כל משתמש בתיקייה אישית (Scan to My Folder). תוכל גם לציין שיטות סריקה אחרות.

לתשומת לבך:

❑ לא ניתן לסרוק מתוך מחשב או מכשיר חכם כאשר Authentication Settings מאופשרות.

❑ בנוסף ל- Authentication Settings שהונהגו במדריך זה, תוכל גם לבנות מערכת אימות באמצעות שרת אימות. על מנת לבנות מערכת, השתמש ב- Document Capture Pro Server Authentication Edition (השם המקוצר הוא Document Capture Pro Server AE). למידע נוסף, צור קשר עם משרד Epson המקומי שלך.

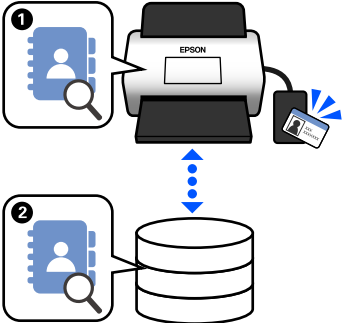
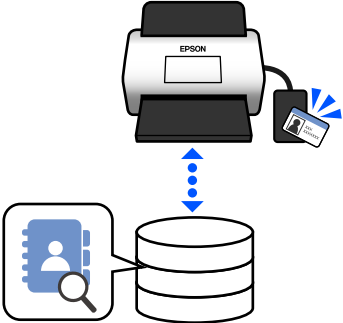
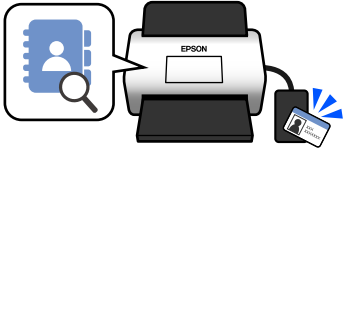
## הפונקציות הזמינות עבור Authentication Settings

| Authentication Settings |                  | פונקציית סריקה בלוח הבקרה   |
|-------------------------|------------------|---|
| כאשר היא מושבתת         | כאשר היא מאופשרת |   |
| -                       | ✓                | סריקה לתיקייה שלי<br>שומרת תמונות אל התיקייה שהוקצתה למשתמש המאומת. |
| -                       | ✓                | סריקה לדוא"ל שלי<br>שולחת תמונות אל כתובת הדוא"ל של המשתמש המאומת.  |
| ✓                       | ✓                | סריקה לתיקייה ברשת/FTP<br>שומרת תמונות לתיקייה ברשת.                |

| Authentication Settings |                  | פונקציית סריקה בלוח הבקרה   |
|-------------------------|------------------|---|
| כאשר היא מושבתת         | כאשר היא מאופשרת |   |
| ✓                       | * ✓              | <p>סריקה למחשב</p> <p>שומרת תמונות למחשב מחובר תוך שימוש בעבודות שנוצרו בתוך Document Capture (Mac OS) / Document Capture (Windows).</p> <p>* כאשר Authentication Settings מאופשרת, תוכל להשתמש רק בעבודות שנרשמו ב-קבוע מראש.</p>          |
| ✓                       | ✓                | <p>סריקה לדוא"ל</p> <p>שולחת תמונות אל כתובת הדוא"ל שהגדרת.</p>   |
| ✓                       | ✓                | <p>סריקה לענן</p> <p>שולחת תמונות אל שירות הענן שהגדרת.</p>   |
| ✓                       | ✓                | <p>סריקה לכונן USB</p> <p>שומרת תמונות בכונן USB המחובר אל הסורק. אפשרות זו זמינה רק כאשר לא מחובר לסורק התקן אימות.</p>  |
| ✓                       | -                | <p>סריקה ל-WSD</p> <p>שומרת תמונות למחשב מחובר באמצעות שימוש בתכונה WSD.</p>  |
| ✓                       | ✓                | <p>קבוע מראש</p> <p>תוכל לרשום עד 48 פונקציות סריקה מוגדרות מראש.</p> <p>תוכל להקצות עד קבוע מראש למשתמשים הרשומים ב-Local DB. קבוע מראש שהוקצו זמינות רק עבור אותו משתמש. קבוע מראש שלא הוקצו למשתמש כלשהו יכולות לשמש את כל המשתמשים.</p> |

## אודות Authentication Method

סורק זה יכול לספק אימות באמצעות השיטות הבאות בלא שיהיה צורך לבנות שרת אימות.

| Local DB and LDAP  | LDAP  | Local DB   |                                   |
|--|---|--|-----------------------------------|
| <p>זכרון הסורק ושרת LDAP</p> <p>בדוק את מידע המשתמש הרשום בסורק תחילה (1), ואם אין התאמה, בדוק את מידע המשתמש מול שרת ה-LDAP (2).</p>  | <p>שרת LDAP*</p> <p>שיטת אימות זו בודקת את מידע המשתמש בשרת ה-LDAP המסונכרן עם הסורק. מאחר ועד 300 פרטי מידע משתמש מתוך שרת LDAP ניתנים לאחסון בסורק בתור מטמון, ניתן לבצע את האימות באמצעות המטמון אם שרת ה-LDAP מושבת.</p> <p>* שרת המספק שירות ספרייה שיכול לתקשר עם LDAP.</p> | <p>זכרון סורק</p> <p>שיטת אימות זו בודקת את מידע המשתמש הרשום עבור הסורק ומשווה אותו עם המשתמש בפונקציית הסריקה.</p> | <p>מיקום מידע משתמש</p>           |
|    |   |                                   |                                   |
| <p>50 (זכרון הסורק)<br/>ללא הגבלה (שרת LDAP)</p>   | <p>ללא הגבלה (שרת LDAP)</p>   | <p>50 (זכרון הסורק)</p>  | <p>מספר המשתמשים הרשומים</p>      |
| <p>מקסימום 300 (50 מבין חריצי המטמון שותפו עם User Settings בתוך Local DB)</p>   | <p>300</p>  | <p>-</p>   | <p>מטמון הזכרון של הסורק</p>      |
| <p>תוכל להשתמש בכל אחת מהשיטות הבאות.</p> <p><input type="checkbox"/> הרם כרטיס אימות או הזן User ID ו-Password</p> <p><input type="checkbox"/> הרם כרטיס אימות, או הזן ID Number</p> <p><input type="checkbox"/> הזן User ID ו-Password</p> <p><input type="checkbox"/> הזן User ID</p> <p><input type="checkbox"/> הזן ID Number</p> |   |  | <p>שיטות כניסה</p>                |
| <p>משתמשי Local DB: הגדר בנפרד</p> <p>משתמשי LDAP: אותן הגדרות עבור כל המשתמשים</p>  | <p>אותן הגדרות עבור כל משתמשי LDAP</p>  | <p>הגדר בנפרד עבור כל משתמש</p>  | <p>הגבלות על התכונה "סרוק אל"</p> |

| Local DB and LDAP                                   | LDAP                        | Local DB         |                           |
|---|-----------------------------|------------------|---------------------------|
| משתמשי Local DB: עד ל-5 לכל משתמש<br>משתמשי LDAP: - | -<br>(לא ניתן להגדיר בנפרד) | עד ל-5 לכל משתמש | הקצאת קבוע מראש למשתמשי ם |

## תוכנה לביצוע הגדרות

בצע את ההגדרה באמצעות Web Config או Epson Device Admin.

כאשר אתה משתמש ב-Web Config, ביכולתך להגדיר את הסורק באמצעות שימוש בדפדפן אינטרנט בלבד.

["Web Config" בעמוד 36](#)

כאשר אתה משתמש ב-Epson Device Admin, ביכולתך להגדיר סורקים רבים בבת אחת באמצעות בניית תצורה.

["Epson Device Admin" בעמוד 37](#)

## עדכון קושחת הסורק

לפני שתאפשר את Authentication Settings, עדכן את קושחת הסורק לגרסה העדכנית ביותר. חבר את הסורק לאינטרנט מראש.

 חשוב:

אל תכבה את המחשב או את הסורק בזמן העדכון.

בעת ביצוע הגדרה מתוך Web Config:

בחר בלשונית **Device Management < Firmware Update**, ואז פעל בהתאם להוראות המוצגות על גבי המסך כדי לעדכן את הקושחה.

בעת ביצוע הגדרה מתוך Epson Device Admin:

בחר **Home < Firmware < Update** במסך רשימת ההתקנים, ואז פעל בהתאם להוראות המוצגות על גבי המסך כדי לעדכן את הקושחה.

לתשומת לבך:

אם הקושחה העדכנית ביותר כבר מותקנת, אין צורך לעדכן.

## חיבור והגדרה של התקן אימות

אם ברצונך להשתמש בהתקן אימות כמו קורא כרטיסים IC, עליך להגדיר תחילה את התצורה של ההתקן. אין צורך לעשות זאת אם אינך משתמש בהתקן אימות.

מידע קשור

← "חיבור התקן אימות" בעמוד 137

← "הגדרות התקן אימות" בעמוד 138

## רשימה תואמת קורא כרטיסים

רשימה זו אינה מבטיחה פעולות עבור קוראי הכרטיסים ברשימה.

כן: תמיכה (ניתן לקרוא את המידע המזהה עם הגדרות סטנדרטיות של קורא כרטיסים).

לא: לא תואם

| מצב   | כרטיס אימות                     |             |          |                  |                  |                  |                  | מספר דגם                       | דגם          | יצרן     |
|-------|---------------------------------|-------------|----------|------------------|------------------|------------------|------------------|--------------------------------|--------------|----------|
|       | IEC/ISO14443 (TypeB) Compliance | FeliCa™     |          | MIFARE           |                  | DMZ              | HID Global       |                                |              |          |
|       |                                 | Lite/Lite-S | Standard | Ultra light      | Classic          | EM4002           | iClasses         |                                |              |          |
| מקלדת | לא                              | לא          | לא       | כן <sup>1*</sup> | כן <sup>1*</sup> | כן <sup>1*</sup> | כן               | RDR-80081 AKU                  | pcPro x Plus | RF IDEAS |
| מקלדת | לא                              | לא          | לא       | כן               | כן               | לא               | כן <sup>1*</sup> | RDR-7081 BKU                   | pcPro x      | RF IDEAS |
| מקלדת | לא                              | לא          | לא       | כן <sup>1*</sup> | כן <sup>1*</sup> | לא               | כן               | RDR-7581 AKU                   | pcPro x      | RF IDEAS |
| מקלדת | לא                              | לא          | לא       | כן               | כן               | לא               | לא               | T3D T-MB2 BEL<br>T3D T-MB2 WEL | TWN 3 MIFARE | ELATEC   |

| מצב   | כרטיס אימות                     |             |          |             |         |        |            | מספר דגם                             | דגם                           | יצרן   |
|-------|---------------------------------|-------------|----------|-------------|---------|--------|------------|--------------------------------------|-------------------------------|--------|
|       | IEC/ISO14443 (TypeB) Compliance | FeliCa™     |          | MIFARE      |         | DMZ    | HID Global |                                      |                               |        |
|       |                                 | Lite/Lite-S | Standard | Ultra light | Classic | EM4002 | iClasses   |                                      |                               |        |
| מקלדת | כן                              | כן          | כן       | כן          | כן      | לא     | כן         | T3D T-FB2B EL<br>T3D T-FB2 WEL       | TWN3<br>MIFARE NFC            | ELATEC |
| מקלדת | כן                              | כן          | כן       | כן          | כן      | כן     | כן         | T4D T-FB2B EL-PI<br>T4D T-FB2 WEL-PI | TWN4<br>MULTITECH             | ELATEC |
| מקלדת | כן                              | כן          | כן       | כן          | כן      | כן     | כן         | T4LK - FB4B LZ-PI                    | TWN4<br>Multi Tech2<br>BLE-PI | ELATEC |
| מקלדת | כן                              | כן          | כן       | כן          | כן      | כן     | כן         | T4QC-FC3B7                           | TWN4<br>Slim                  | ELATEC |

| מצב                 | כרטיס אימות                                   |                  |                  |                  |                  |        |            | מספר דגם                                | דגם                   | יצרן       |
|---------------------|---|------------------|------------------|------------------|------------------|--------|------------|---|-----------------------|------------|
|                     | IEC/<br>ISO1<br>4443<br>(TypeB)<br>Compliance | FeliCa™          |                  | MIFARE           |                  | DMZ    | HID Global |   |                       |            |
|                     |   | Lite/Lite-S      | Standard         | Ultra light      | Classic          | EM4002 | iClasses   |   |                       |            |
| מקלדת <sup>1*</sup> | כן  | לא               | כן               | כן               | כן               | כן     | כן         | OMNIKEY 5427 CK<br>OMNIKEY 5427 CK gen2 | OMNIKEY 5427          | HID Global |
| PC/SC               | כן <sup>2*</sup>                              | לא               | כן               | כן <sup>2*</sup> | כן <sup>2*</sup> | לא     | לא         | ACR122U                                 | ACR122U               | ACS        |
| PC/SC               | כן <sup>2*</sup>                              | כן               | כן               | כן <sup>2*</sup> | כן <sup>2*</sup> | לא     | לא         | ACR1252                                 | ACR1252               | ACS        |
| PaSoRi              | כן <sup>2*</sup>                              | כן <sup>2*</sup> | כן <sup>2*</sup> | כן <sup>2*</sup> | כן <sup>2*</sup> | לא     | לא         | RC-S330/S                               | PaSoRi                | Sony       |
| PaSoRi              | כן <sup>2*</sup>                              | כן <sup>2*</sup> | כן <sup>2*</sup> | כן <sup>2*</sup> | כן <sup>2*</sup> | לא     | לא         | RC-S380/P<br>RC-S380/S                  | PaSoRi                | Sony       |
| מקלדת               | כן  | כן               | כן               | כן               | כן               | כן     | כן         | DMZ008                                  | Leitor RFID Universal | DMZ        |
| מקלדת               | לא  | לא               | לא               | לא               | לא               | כן     | לא         | DMZ087                                  | Leitor RFID Multi-125 | DMZ        |

| מצב   | כרטיס אימות                     |                  |                  |                  |                  |                  |                  | מספר דגם      | דגם                              | יצרן                   |
|-------|---------------------------------|------------------|------------------|------------------|------------------|------------------|------------------|---------------|----------------------------------|------------------------|
|       | IEC/ISO14443 (TypeB) Compliance | FeliCa™          |                  | MIFARE           |                  | DMZ              | HID Global       |               |                                  |                        |
|       |                                 | Lite/Lite-S      | Standard         | Ultra light      | Classic          | EM4002           | iClasses         |               |                                  |                        |
| מקלדת | לא                              | לא               | לא               | כן               | כן               | לא               | לא               | DMZ088        | Leitor RFID Mifare               | DMZ                    |
| מקלדת | לא                              | לא               | לא               | לא               | לא               | כן               | לא               | DMZ073        | Biom etric & RFID Reader         | DMZ                    |
| מקלדת | כן <sup>1*</sup>                | כן <sup>1*</sup> | כן <sup>1*</sup> | כן <sup>1*</sup> | כן <sup>1*</sup> | כן <sup>1*</sup> | כן <sup>1*</sup> | SCR708        | SCR708                           | inepro                 |
| מקלדת | כן                              | כן               | כן               | כן               | כן               | כן               | כן               | MU0388        | YU03088001                       | Y Soft                 |
| מקלדת | כן                              | לא               | לא               | כן               | כן               | לא               | לא               | ZTC M3-MIFARE | TCM3 Cartadis MiFare Card Reader | Cartadis               |
| מקלדת | כן                              | לא               | לא               | כן               | כן               | לא               | לא               | mCR-600       | EM & Mifare Card Reader          | MICI Network Co., Ltd. |



| מצב   | כרטיס אימות                     |             |          |                  |                  |                  |                  | מספר דגם               | דגם                    | יצרן    |
|-------|---------------------------------|-------------|----------|------------------|------------------|------------------|------------------|------------------------|------------------------|---------|
|       | IEC/ISO14443 (TypeB) Compliance | FeliCa™     |          | MIFARE           |                  | DMZ              | HID Global       |                        |                        |         |
|       |                                 | Lite/Lite-S | Standard | Ultra light      | Classic          | EM4002           | iClasses         |                        |                        |         |
| מקלדת | כן                              | כן          | כן       | כן               | כן               | כן               | כן               | T4D T-FB4 WUF-PI       | MiCard Multi Tech 4-PI | NT-ware |
| מקלדת | לא                              | לא          | לא       | כן <sup>1*</sup> | כן <sup>1*</sup> | כן <sup>1*</sup> | כן <sup>1*</sup> | RDR-80081 AGU - NT2-20 | MiCard Plus-2-V2       | NT-ware |
| מקלדת | לא                              | כן          | כן       | כן               | כן               | כן               | כן               | MiCard V3 Multi        | MiCard V3 Multi        | NT-ware |

1\* עליך לשנות את ההגדרות של קרוא הכרטיסים באמצעות שימוש בתוכנה קניינית.

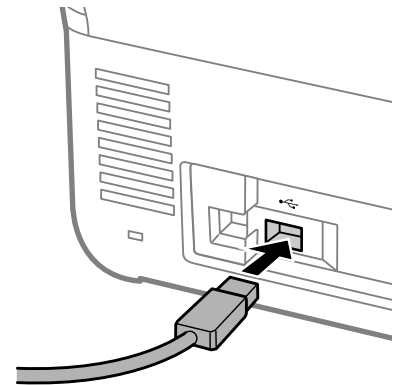
2\* אם עליך להשתמש בנתונים בתחום מסוים בכרטיס שאינו המזהה התקני של הכרטיס בתור מזהה אימות, באמצעות הגדרת התצורה של הגדרות המוצר, אנא צור קשר עם שותף Epson שלך או עם הנציג המקומי של החברה כדי לקבל מידע נוסף על הדרך שבה יש להגדיר את המוצר.

## חיבור התקן אימות

 חשוב:

כאשר אתה מחבר את התקן האימות לסורקים רבים, השתמש במוצר עם אותו מספר דגם.

חבר את כבל ה-USB של קורא הכרטיסים אל יציאת ה-USB של הממשק החיצוני של הסורק.



### בדיקת פעולה עבור התקן אימות

תוכל לבדוק את מצב החיבור ואת זיהוי כרטיס האימות עבור התקן האימות מתוך לוח הבקרה של הסורק. המידע מוצג אם תבחר הגדרות < פרטי המכשיר < סטטוס מכשיר האימות.

### הגדרות התקן אימות

הגדר את תבנית הקריאה עבור מידע האימות שהתקבל מכרטיס אימות. תוכל להגדיר את שיטת הקריאה הבאה עבור התקן האימות.

- קרא את האזור המסוים של כרטיס האימות, כגון מספר עובד או מזהה אישי.
- השתמש במידע כרטיס האימות פרט ל-UID (מידע כרטיס אימות כגון מספר סידורי). תוכל להשתמש בכלי כדי להפיק את הפרמטרים התפעוליים. בקש פרטים מהסוכן שלך.

לתשומת לבך:

השימוש בכרטיסי אימות מיצרנים שונים:

כאשר את המשתמש במידע כרטיס UID (מידע מזהה כרטיס כגון מספר סידורי), ביכולתך להשתמש בתערובת של סוגים שונים של כרטיסי אימות. לא ניתן לערבב זאת כאשר משתמשים במידע כרטיס אחר.

בעת ביצוע הגדרה מתוך Web Config:

בחר בלשונית Card Reader < Device Management.

בעת ביצוע הגדרה מתוך Epson Device Admin:

בחר Card Reader < Authentication Settings < Administrator Settings מתוך תבנית התצורה.

| פריט      | הסבר   |
|-----------|--|
| Vendor ID | הגדר את מזהה הספק של מכשיר האימות שמגביל את השימוש בין 0000 לבין FFFF באמצעות שימוש ב-4 תווים של אותיות ומספרים. אם אינך מעונין להגיב אותו, הגדר אותו בתור 0000. |

| פריט                               | הסבר  |
|------------------------------------|---|
| Product ID                         | הגדר את מזהה המוצר של מכשיר האימות שמגביל את השימוש בין 0000 לבין FFFF באמצעות שימוש ב-4 תווים של אותיות ומספרים. אם אינך מעונין להגיב אותו, הגדר אותו בתור 0000. |
| Operational parameter              | הגדר את הפרמטר התפעולי של התקן האימות בין 0 לבין 8192 תווים. a~z, A~Z, 9~0, +, /, =, רווח והזנת שורה הם התווים הזמינים.   |
| Card Reader                        | בחר את תבנית ההמרה עבור התקן אימות. תוכל לבדוק את פרטי התבנית. עיין בקישור שסופק בתיאור הפריט.  |
| Authentication Card ID save format | הגדר את תבנית ההמרה עבור מידע האימות שהתקבל מכרטיס מזהה. תוכל לבדוק את פרטי התבנית. עיין בקישור שסופק בתיאור הפריט.   |
| Set card ID range                  | אפשר את המפרט של מיקום הקריאה.  |
| Text Start Position                | ציין את נקודת התחילה של הטקסט עבור קריאת המידע המזהה. תוכל לציין בין 1 לבין 4096.   |
| Number of Characters               | ציין את מספר התווים שיש לקרוא מנקודת ההתחלה של המידע המזהה. תוכל לציין בין 1 לבין 4096.   |

## רישום והגדרה של מידע

### ביצוע הגדרות

בצע את ההגדרות הדרושות בהתאם ל-Authentication Method ושיטת הסריקה שבה אתה משתמש.

**חשוב!**

לפני שתתחיל בהתקנה, ודא שהגדרת השעה עבור הסורק היא נכונה.

אם הגדרת השעה שגויה, תוצג הודעת השגיאה "תוקף הרשיון פג", והדבר עלול להוביל לכשל בהגדרת הסורק. כמו כן, על מנת להשתמש בפונקציית אבטחה כמו תקשורת SSL/TLS או IPsec, יש להגדיר את השעה הנכונה. תוכל להגדיר את השעה באופן הבא.

לשונית *Date and Time < Date and Time < Device Management : Web Config*.

לוח הבקרה של הסורק: הגדרות < הגדרות בסיסיות < הגדרות תאריך/שעה.

| הגדרות   | Local DB | LDAP | Local DB and LDAP |
|--|----------|------|-------------------|
| איפשר אימות<br>עליך לאפשר אימות לפני ביצוע הגדרות האימות.<br>"איפשר אימות" בעמוד 140 | ✓        | ✓    | ✓                 |

| הגדרות   | Local DB | LDAP | Local DB and LDAP |
|--|----------|------|-------------------|
| <p><b>Authentication Settings</b></p> <p>הגדרת Authentication Method וכיצד לאמת את המשתמש.</p> <p><a href="#">"Authentication Settings" בעמוד 141</a></p>  | ✓        | ✓    | ✓                 |
| <p><b>User Settings</b> רישום</p> <p>רשום את ההגדרות עבור כל משתמש. תוכל גם לרשום משתמשים בצובר באמצעות קובץ CSV.</p> <p><a href="#">"User Settings" בעמוד 143</a></p>   | ✓        | –    | ✓                 |
| <p><b>LDAP Server</b> עם סנכרון</p> <p>בצע הגדרות סנכרון עבור שרת LDAP.</p> <p><a href="#">"LDAP Server" בעמוד 150</a></p>   | –        | ✓    | ✓                 |
| <p><b>Email Server</b> הגדרת</p> <p>הגדר את ההגדרות של שרת הדוא"ל. הגדר זאת בעת השימוש בפונקציות המחייבות הגדרות שרת דוא"ל כגון Scan to My Email.</p> <p><a href="#">"הגדרת שרת הדוא"ל" בעמוד 154</a></p>  | ✓        | ✓    | ✓                 |
| <p><b>Scan to My Folder</b> הגדרת</p> <p>הגדר את תיקיות היעד. הגדר זאת בעת השימוש בפונקציה Scan to My Folder.</p> <p><a href="#">"הגדרת Scan to My Folder" בעמוד 155</a></p>   | ✓        | ✓    | ✓                 |
| <p><b>Customize One-touch Functions</b></p> <p>הגדר זאת כאשר את משנה את הפריטים המוצגים בלוח הבקרה של הסורק. תוכל להציג רק את הסמלים הדרושים לך בלוח הבקרה, או לשנות את סדר הסמלים.</p> <p><a href="#">"Customize One-touch Functions" בעמוד 157</a></p> | ✓        | ✓    | ✓                 |

## איפשור אימות

עליך לאפשר אימות לפני ביצוע הגדרות האימות.

בעת ביצוע הגדרה מתוך **Web Config**:

בחר מופעל (התקן/שרת LDAP) מתוך לשונית **Product Security < Basic < Authentication**.

בעת ביצוע הגדרה מתוך **Epson Device Admin**:

בתבנית התצורה, בחר מופעל (התקן/שרת LDAP) מתוך **Administrator Settings < Authentication Settings < Basic < Authentication**.

לתשומת לבך:

אם תאפשר Authentication Settings בסורק, גם הגדרת נעילה תאפשר בלוח הבקרה. לא ניתן לפתוח את נעילת לוח הבקרה כאשר Authentication Settings מאפשרת.

גם אם תשבית את Authentication Settings, הגדרת נעילה תישאר מאפשרת. אם תרצה להשבית אותה, תוכל לבצע הגדרות מתוך לוח הבקרה או Web Config.

מידע קשור

← "הגדרת הגדרת נעילה מלוח הבקרה" בעמוד 86

← "הגדרת הגדרת נעילה מתוך Web Config" בעמוד 86

## Authentication Settings

הגדרת Authentication Method וכיצד לאמת את המשתמש.

בעת ביצוע הגדרה מתוך Web Config:

בחר בלשונית Authentication Settings < Product Security.

בעת ביצוע הגדרה מתוך Epson Device Admin:

בחר Authentication Settings < Authentication Settings < Administrator Settings מתוך תבנית התצורה.

| פריט                  | הסבר   |
|-----------------------|--|
| Authentication Method | <p>בחר את לשונית Authentication Method.</p> <p>Local DB <input type="checkbox"/></p> <p>אמת באמצעות User Settings הרשומות עבור הסורק. צריך לרשום את המשתמש לסורק.</p> <p>LDAP <input type="checkbox"/></p> <p>אמת באמצעות מידע המשתמש בשרת LDAP המסונכרן עם הסורק. עליך להגדיר מראש את התצורה של הגדרות שרת LDAP.</p> <p>Local DB and LDAP <input type="checkbox"/></p> <p>אמת באמצעות מידע המשתמש הרשום עבור הסורק או שרת LDAP המסונכרן עם הסורק. עליך לרשום את המשתמש לסורק ולהגדיר את שרת LDAP.</p> |

| הסבר  | פריט  |
|---|---|
| <p>בחר כיצד לאמת משתמש.</p> <p><input type="checkbox"/> Card or User ID and Password</p> <p>השתמש בכרטיס אימות כדי לאמת משתמשים. תוכל גם להשתמש במזהה משתמש וסיסמה כדי לאמת.</p> <p><input type="checkbox"/> User ID and Password</p> <p>השתמש במזהה משתמש ובסיסמה כדי לאמת משתמשים.</p> <p>לא תוכל להשתמש בכרטיס אימות כדי לאמת כאשר אתה בוחר פונקציה זו.</p> <p><input type="checkbox"/> User ID</p> <p>יש להשתמש רק במזהה משתמש כדי לאמת משתמשים. אינך צריך להגדיר סיסמה.</p> <p><input type="checkbox"/> Card or ID Number</p> <p>השתמש בכרטיס אימות כדי לאמת משתמשים. תוכל גם להשתמש ב-ID Number.</p> <p><input type="checkbox"/> ID Number</p> <p>יש להשתמש רק במספר מזהה כדי לאמת משתמשים.</p> | <p>How to Authenticate User</p>                     |
| <p>אפשר זאת אם אתה מרשה למשתמשים לרשום את כרטיס האימות למערכת.</p> <p>אם תבחר LDAP עבור <b>Authentication Method</b>, לא תוכל להגדירו.</p> <p>למידע נוסף על האופן שבו משתמשים יכולים לרשום את כרטיס האימות שלהם, ראה "רישום כרטיס אימות" בתוך ה-מדריך למשתמש.</p>   | <p>Allow users to register authentication cards</p> |
| <p>בחר את מספר הספרות המזערי עבור המספר המזהה.</p>  | <p>The Minimum Digit Number of ID Number</p>        |
| <p>בעת השימוש באימות שרת LDAP, תוכל להגדיר אם להשתמש בשמירת מטמון עבור מידע משתמש או לא.</p>  | <p>Caching for LDAP authenticated users</p>         |
| <p>כאשר אתה משתמש במזהה משתמש וסיסמה עבור אימות, תוכל להגדיר אם להשתמש במידע המשתמש עבור אימות SMTP או לא. המערכת משתמשת במזהה המשתמש ובסיסמה האחרונים שנרשמו.</p>  | <p>Use user information in SMTP authentication</p>  |
| <p>אם אתה משתמש ב-LDAP, תוכל להגדיר את הפונקציות הזמינות למשתמש.</p>  | <p>Restrictions for LDAP authenticated users</p>    |

## רישום User Settings

רישום את User Settings ששימשו עבור אימות המשתמש. תוכל לבצע את הרישום באמצעות כל אחת מהשיטות הבאות.

- ☐ רישום User Settings אחת אחת (Web Config)
- ☐ רישום User Settings מרובות כאצווה באמצעות קובץ (CSV (Web Config
- ☐ רישום User Settings עבור סורקים מרובים כאצווה באמצעות תבנית תצורה (Epson Device Admin)

מידע קשור

- ← "רישום User Settings נפרדות (Web Config)" בעמוד 143
- ← "רישום User Settings מרובות באמצעות קובץ (CSV (Web Config)" בעמוד 144
- ← "רישום User Settings לסורקים רבים כאצווה (Epson Device Admin)" בעמוד 147

## רישום User Settings נפרדות (Web Config)

גש אל Web Config ובחר את לשונית ה-Add < User Settings < Product Security, ואז הזן את User Settings.

| פריט                   | הסבר   |
|------------------------|--|
| User ID                | הזן את מזהה המשתמש שבו ברצונך להשתתף עבור אימות בטווח שבין 1 עד 83 בתים שניתן לבטא ב-UTF-8Unicode). מאחר ומזהה המשתמש אינו רגיש לאותיות גדולות או קטנות, ניתן להיכנס באמצעות אותיות גדולות או קטנות.   |
| User name Display      | הזן את שם המשתמש המוצג בלוח הבקרה של הסורק תוך שימוש בעד 32 תווים שניתן לבטא ב-UTF-16Unicode). תוכל להשאיר זאת ריק.  |
| Password               | הזן את הסיסמה שבה ברצונך להשתמש לשם אימות במסגרת של 32 תווי ASCII. הסיסמה רגישה לאותיות קטנות וגדולות. השאר זאת ריק אם תבחר User ID עבור <b>How to Authenticate User</b> .   |
| Authentication Card ID | הזן את מזהה כרטיס האימות בטווח של 16 תווי ASCII. תוכל להשאיר זאת ריק, כאשר מתירים <b>Allow users to register authentication cards</b> עבור <b>Authentication Settings</b> , משתקפת התוצאה שרשמו המשתמשים.  |
| ID Number              | פריט זה מוצג כאשר בוחרים <b>Card or ID Number</b> או <b>ID Number</b> ב- <b>How to Authenticate User &lt; Authentication Settings</b> . הזן מספר שנמצא בין המספר שהוגדר בתוך <b>Authentication Settings &lt; Authentication Settings</b> <b>The Minimum Digit Number of ID Number</b> ועד 8 ספרות. |
| Auto Generate          | פריט זה מוצג כאשר בוחרים <b>Card or ID Number</b> או <b>ID Number</b> ב- <b>How to Authenticate User &lt; Authentication Settings</b> . לחץ כדי להפיק באופן אוטומטי מספר מזהה בעל מספר זהה של ספרות לזה שבחרת ב- <b>The Minimum Digit Number of ID Number</b> .                                    |

| פריט              | הסבר   |
|-------------------|--|
| Department        | הזן את שם המחלקה וכן הלאה שמזהה את המשתמש בטווח של 40 תווים שניתן לבטא ב-UTF-16Unicode).<br>תוכל להשאיר זאת ריק.   |
| Email Address     | הזן את כתובת הדוא"ל של המשתמש בטווח של 200 תווי ASCII. כתובת זו משמשת כיעד עבור <b>Scan to My Email</b> .<br>תוכל להשאיר זאת ריק.  |
| Scan to My Folder | הגדר את היעדים בנפרד כאשר אתה בוחר <b>Individual</b> בתוך <b>Setting Type &lt; Scan to My Folder</b> . עיין בפרטים שלהלן עבור מידע נוסף על פריטי ההגדרה.<br><b>"הגדרת Scan to My Folder" בעמוד 155</b>   |
| Restrictions      | תוכל להגביל את הפונקציות עבור כל משתמש. בחר את הפונקציה שאת השימוש בה ברצונך להתיר.  |
| Presets           | תוכל להגדיר עד חמש הגדרות קבועות מראש שתהינה זמינות רק למשתמש הנבחר מתוך ה-Presets שנרשמו בסורק.<br><input type="checkbox"/> Presets שהוקצו למשתמש יכולות לשמש רק את אותו משתמש. Presets שלא הוקצו למשתמש כלשהו יכולות לשמש את כל המשתמשים.<br><input type="checkbox"/> אם יש Presets זמינות רק למשתמש אחד, הם ייטענו באופן אוטומטי אחרי האימות. אם קיימות Presets מרובות, תוצג רשימה של Presets אחרי האימות.<br><input type="checkbox"/> לא תוכל ליצור או להציג Presets המשתמשות בפונקציות שלא הוגבלו ב-Restrictions. |

## רישום User Settings מרובות באמצעות קובץ (Web Config) CSV

הזן את ההגדרות עבור כל משתמש בקובץ CSV ורשום אותן כאצווה.

### יצירת קובץ CSV

צור קובץ CSV כדי לייבא User Settings.

לתשומת לבך:

אם תרשום User Settings אחת או יותר מראש ואז תייצא קובץ בתבנית CSV, תוכל להשתמש בהגדרה שרשמת כנקודת ייחוס להזנת פריטי הגדרה.

1. גש אל Web Config ובחר את לשונית **User Settings < Product Security**.

2. לחץ על **Export**.

3. בחר את תבנית הקובץ **File Format**.


בחר אותה באמצעות התייחסות לפרטים שלהלן.



| הסבר   | פריט                            |
|--|---------------------------------|
| <p>בחר כאשר אתה עורך את הקובץ באמצעות Microsoft Excel.<br/>                     כל פרמטר מוקף על ידי "[ ]" (סוגריים מרובעים). הזן את הפרמטרים בתוך "[ ]".<br/>                     כאשר אתה מעדכן את הקובץ, אנו ממליצים להחליף את הקובץ. אם אתה שומר את הקובץ בפעם הראשונה, בחר טקסט (*.txt Unicode) עבור תבנית הקובץ.</p> | CSV UTF-16 (Tab delimited)      |
| <p>בחר כאשר אתה עורך את הקובץ באמצעות עורך טקסט או מאקרו ללא Microsoft Excel.</p>  | CSV UTF-8 (Comma delimited)     |
|  | CSV UTF-8 (Semicolon delimited) |

4. לחץ על **Export**.

5. ערוך ושמור קובץ CSV באפליקציית גליון אלקטרוני כמו Microsoft Excel או בעורך טקסט.

 **חשוב:**  
 בעת עריכת הקובץ, אל תשנה את הקידוד ואת המידע בכותרת.

פריטי הגדרת קובץ CSV

| הגדרות והסבר  | פריט                 |
|---|----------------------|
| <p>הזן את מזהה המשתמש כדי להשתמש באימות בין 1 לבין 83 בתים ב-Unicode.</p>   | UserID               |
| <p>הזן את שם המשתמש המוצג בלוח הבקרה של הסורק תוך שימוש בעד 32 תווים ב-Unicode. תוכל להשאיר זאת ריק.</p>  | UserName             |
| <p>הזן את הסיסמה שבה יש להשתמש לשם אימות במסגרת של 32 תווי ASCII. בעת ביצוע ייבוא, סיסמה זו מוגדרת כסיסמה במקום EncPassword.<br/>                     השאר זאת ריק אם תבחר User ID עבור <b>How to Authenticate User</b>.<br/>                     בעת ביצוע ייצוא, יש להשאיר פרט זה תמיד ריק.</p> | Password             |
| <p>הגדר את תוצאת הקריאה של כרטיס האימות. כאשר מתירים <b>Allow users to register authentication cards</b> ב-<b>Authentication Settings</b>, משתקפת התוצאה שרשמו המשתמשים.<br/>                     הזן בתוך 116 תווי ASCII. תוכל להשאיר זאת ריק.</p>   | AuthenticationCardID |

| פריט           | הגדרות והסבר  |
|----------------|---|
| IDNumber       | <p>פריט זה מוצג כאשר בוחרים <b>Card or ID Number</b> או <b>ID Number</b> ב-<br/> <b>.How to Authenticate User &lt; Authentication Settings</b><br/>                     הזן מספר שנמצא בין המספר שהוגדר בתוך <b>&lt; Authentication Settings</b><br/> <b>The Minimum Digit Number of ID Number</b> ועד 8 ספרות.<br/>                     לא ניתן לשכפל מספר מזהה. אם הוא ישוכפל, תקבל התראה על השגיאה בעת ייבוא<br/>                     הקובץ. כאשר משאירים זאת ריק, מוקצה מספר באופן אוטומטי.</p> |
| Department     | <p>הזן את שם המחלקה באופן שרירותי כדי להבדיל בין המשתמשים.<br/>                     הזן בטווח של 40 תווים ב-Unicode. תוכל להשאיר זאת ריק.</p>   |
| MailAddress    | <p>הגדר את כתובת הדוא"ל עבור המשתמשים. כתובת זו משמשת כיעד עבור<br/> <b>.Scan to My Email</b><br/>                     תוכל להשתמש ב-A-Z, a-z, 0-9, @, ~, {, }, ^, =, /, -, ., #, %, &amp;, *!, הזן 200 תווים או<br/>                     פחות. לא תוכל להשתמש ב-"", (פסיק) עבור התו הראשון. תוכל להשאיר זאת ריק.</p>   |
| FolderProtocol | <p>הגדר את סוג הפונקציה <b>Scan to My Folder</b>.<br/>                     תיקיית רשת/FTP (SMB): 0, FTP: 1</p>  |
| FolderPath     | <p>הגדר את יעד השמירה עבור הפונקציה <b>Scan to My Folder</b>.</p>   |
| FolderUserName | <p>הגדר את שם המשתמש עבור הפונקציה <b>Scan to My Folder</b>.</p>  |
| FolderPassword | <p>הגדר סיסמה כדי לאמת את תיקיית היעד עבור הפונקציה <b>Scan to My Folder</b><br/>                     function בתוך 32 תווי ASCII.<br/>                     בעת ביצוע ייבוא, סיסמה זו מוגדרת כסיסמה במקום <b>EncPassword</b>. בעת ביצוע ייצוא,<br/>                     יש להשאיר פרט זה תמיד ריק.</p>  |
| FtpPassive     | <p>הגדר את מצב החיבור עבור שרת FTP כאשר בוחרים <b>FTP</b> בתור <b>Type</b> עבור הפונקציה<br/> <b>Scan to My Folder</b><br/>                     מצב אקטיבי: 0, מצב פסיבי: 1</p>   |
| FtpPort        | <p>הגדר את מספר היציאה עבור שליחת נתונים סרוקים אל שרת FTP מ-0 עד 65535 כאשר<br/>                     בוחרים <b>FTP</b> בתור <b>Type</b> עבור הפונקציה <b>Scan to My Folder</b>.</p>  |
| ScanToMemory   | <p>הגדר את ההגבלות עבור <b>Scan to USB Drive</b>.<br/>                     אסור: 0, מותר: 1</p>   |
| ScanToMail     | <p>הגדר את ההגבלות עבור <b>Scan to Email</b>.<br/>                     תוכל להגדיר את סריקה לדוא"ל שלי רק כאשר <b>Scan to Email</b> אופשרה.<br/>                     אסור: 0, מותר: 1</p>   |

| פריט           | הגדרות והסבר  |
|----------------|---|
| ScanToFolder   | הגדר את ההגבלות עבור Scan to Network Folder/FTP.<br>תוכל להגדיר את סריקה לתיקייה שלי רק כאשר Scan to Network Folder/FTP אופשרה.<br>אסור: 0, מותר: 1   |
| ScanToCloud    | הגדר את ההגבלות עבור Scan to Cloud.<br>אסור: 0, מותר: 1   |
| ScanToComputer | הגדר את ההגבלות עבור סריקה למחשב.<br>אסור: 0, מותר: 1   |
| PresetIndex    | הגדר את ה-Presets שברצונך לשייך אל המשתמש. תוכל להגדיר עד חמישה מספרי רישום כ-Presets מופרדים על ידי פסיקים.  |
| EncPassword    | בעת הייצוא של הגדרות משתמש, הפרמטר שמוגדר עבור Password מוצפן, ואז הערך מקודד באמצעות BASE64 ופלט.<br>בעת ייבוא עם סיסמה חדשה עבור Password, המערכת מתעלמת מערך זה.<br>אם משאירים את Password ריקה, המערכת משתמשת בערך זה והסיסמה נשאר כפי שהיתה לפני הייצוא.     |
| EncFolderPath  | כאשר הייצוא של הפרמטר שהוגדר עבור FolderPassword מוצפן, אז הערך מקודד באמצעות BASE64 ופלט.<br>בעת ייבוא עם סיסמה חדשה עבור FolderPassword, המערכת מתעלמת מערך זה.<br>אם משאירים את FolderPassword ריקה, המערכת משתמשת בערך זה והסיסמה נשאר כפי שהיתה לפני הייצוא. |

### יבוא קובץ CSV

1. גש אל Web Config ובחר את לשונית User Settings < Product Security.
2. לחץ על Import.
3. בחר את הקובץ שברצונך לייבא.
4. לחץ על Import.
5. אחרי בדיקת המידע שהוצג, לחץ OK.

### רישום User Settings לסורקים רבים כאצווה (Epson Device Admin)

תוכל לרשום את User Settings המשמשות בתוך Local DB כאצווה תוך שימוש בשרת LDAP או קובץ CSV/ENE.

לתשומת לבך:

קובץ ENE הוא קובץ בינרי שמספקת Epson המצפין את המידע עבור Contacts כגון מידע אישי ו-User Settings. ניתן לייצא אותו מתוך Epson Device Admin ותוכל להגדיר סיסמה. הדבר שימושי כאשר אתה רוצה לייבא את User Settings מקובץ גיבוי.

### ייבוא מקובץ CSV/ENE

1. בחר Administrator Settings < Authentication Settings < User Settings מתוך תבנית התצורה.
2. לחץ על Import.
3. בחר CSV or ENE File מ-Import Source.
4. לחץ על Browse. מסך בחירת הקובץ מוצג.
5. בחר את הקובץ שתוצאה לייבא כדי לפתוח אותו.
6. בחר שיטת ייבוא.
  - Overwrite and Add: מחליפה אם אותו מזהה משתמש קיים, מוסיפה מזהה חדש אם הוא אינו קיים.
  - Replace All: מחליפה הכל עם הגדרות המשתמש שברצונך לייבא.
7. לחץ על Import. מוצג מסך אישור ההגדרה.
8. לחץ על OK. מוצגת תוצאת האימות.
 

לתשומת לבך:

אם מספר הגדרות המשתמשים שיובאו עולה על המספר שניתן לייבא, הודעה תבקש ממך למחוק כמה הגדרות משתמשים. מחק הגדרות משתמש עודפות כלשהן לפני ביצוע הייבוא.

בחר את הגדרות המשתמשים שברצונך למחוק לפני ביצוע הייבוא, ואז לחץ על Delete.
9. לחץ על Import. הגדרות המשתמש מייבאות לתוך תבנית התצורה.

### ייבוא משרת LDAP

1. בחר Administrator Settings < Authentication Settings < User Settings מתוך תבנית התצורה.
2. לחץ על Import.
3. בחר LDAP מ-Import Source.

4. לחץ על **Settings**.

מוצגות הגדרות **LDAP Server**.

לתשומת לבך:

הגדרת שרת **LDAP** זו נועדה כדי לייבא את הגדרות המשתמש משרת **LDAP**. הגדרות המשתמש שיובאו (הועתקו) משמשות כדי לאמת משתמשים באמצעות שימוש בסורק עצמו.

מצד שני, כאשר אתה בוחר **LDAP** או **Local DB and LDAP** כשיטת האימות, משתמשים מאומתים באמצעות תקשורת עם שרת **LDAP**.

5. הגדר כל פריט.

בעת ייבוא הגדרות משתמש מתוך שרת **LDAP**, תוכל תמיד להגדיר את התצורה של ההגדרות הבאות בנוסף להגדרות **LDAP**.

לפרטים אחרים, עיין במידע קשור.

| הסבר  | פריט             |                      |
|---|------------------|----------------------|
| מאפשרת לך לבחור את סוג שרת ה- <b>LDAP</b> .   | LDAP Server Type | LDAP Server Settings |
| האם תוכל להגדיר את הטקסט המשמש עבור מסנן חיפוש <b>LDAP</b> . בחר את <b>Custom</b> כדי לערוך את טקסט החיפוש. | Search Filter    |                      |
| תוכל להגדיר את סוג יעד השמירה עבור <b>Scan To My Folder</b> .   | Type             | Options              |
| כאשר מגדירים את <b>Type</b> בתור <b>FTP</b> , ניתן להגדיר את תקשורת ה- <b>FTP</b> .                         | Connection Mode  |                      |
| כאשר מגדירים את <b>Type</b> בתור <b>FTP</b> , ניתן להגדיר את מספר היציאה שבה אתה רוצה להשתמש.               | Port Number      |                      |

6. בצע את מבחן הקישור בהתאם לצורך באמצעות לחיצה על **Connection Test**.

רוכשת ומציגה 10 הגדרות משתמשים מתוך שרת ה-**LDAP**.

7. לחץ על **OK**.

8. בחר שיטת ייבוא.

**Overwrite and Add**: מחליפה אם אותו מזהה משתמש קיים, מוסיפה מזהה חדש אם הוא אינו קיים.

**Replace All**: מחליפה הכל עם הגדרות המשתמש שברצונך לייבא.

9. לחץ על **Import**.

מוצג מסך אישור ההגדרה.

10. לחץ על **OK**.

מוצגת תוצאת האימות.

## 11. לחץ על Import.

הגדרות המשתמש מיובאות לתוך תבנית התצורה.

מידע קשור

- ← "הגדרת התצורה של שרת LDAP" בעמוד 150
- ← "הגדרת התצורה של הגדרות החיפוש של שרת LDAP" בעמוד 152

## סנכרון עס LDAP Server

בצע את הגדרות LDAP Server עבור הסורק.

בצע הגדרות עבור השרת הראשי והשרת המשני כאחד, בהתאם לצורך.

לתשומת לבך:

הגדרות LDAP Server משותפות עם *Contacts*.

## שירותים זמינים

יש תמיכה בשירותי הספרייה הבאים.

| שם שירות         | גירסה  |
|------------------|--|
| Active Directory | Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 |
| OpenLDAP         | Ver.2.3, Ver.2.4   |

## הגדרת התצורה של שרת LDAP

כדי להשתמש בשרת LDAP, עליך להגדיר תחילה את התצורה של שרת LDAP.

בעת ביצוע הגדרה מתוך **Web Config**:

בחר בלשונית **Network < LDAP Server < Basic (Primary Server)** או **Basic (Secondary Server)**.

אם תבחר **Kerberos Authentication** בתור **Authentication Method**, בחר את **Network < Kerberos Settings** כדי לבצע הגדרות עבור Kerberos.

בעת ביצוע הגדרה מתוך **Epson Device Admin**:

בחר **Network < LDAP server < Server Settings (Primary Server)** או **Server Settings (Secondary Server)** מתוך תבנית התצורה.

אם תבחר **Kerberos Authentication** בתור **Authentication Method**, בחר את **Network < Security < Kerberos Settings** כדי לבצע הגדרות עבור Kerberos.

| פריט            | הגדרות והסבר           |
|-----------------|------------------------|
| Use LDAP Server | בחר Use או Do Not Use. |

| פריט                                  | הגדרות והסבר   |
|---------------------------------------|--|
| LDAP Server Address                   | הזן את כתובת שרת LDAP. הזן בין 1 לבין 255 תווים בפורמט IPv4, IPv6 או פורמט FQDN. עבור תבנית FQDN, תוכל להשתמש בתוויות של אותיות ומספרים ב-ASCII (0x20-0x7E) ומקפים, פרט להתחלה ולסיום של הכתובת.   |
| LDAP server Port Number (Port number) | הזן את מספר כניסת שרת ה-LDAP בין 1 לבין 65535.   |
| Secure Connection                     | ציין את שיטת האימות עבור גישת הסורק אל שרת ה-LDAP.   |
| Certificate Validation                | תעודת שרת LDAP מאומתת כאשר מאפשרים אפשרות זו. אנו ממליצים להגדיר זאת בתור <b>Enable</b> . כדי לבצע את ההגדרה, יש לייבא את <b>CA Certificate</b> אל הסורק.  |
| Search Timeout (sec)                  | הגדר את משך זמן החיפוש לפני פסק זמן בין 5 לבין 300 שניות.  |
| Authentication Method                 | בחר את שיטת האימות.<br>אם תבחר את <b>Kerberos Authentication</b> , בצע מראש הגדרות עבור Kerberos.<br>כדי לבצע <b>Kerberos Authentication</b> , דרושה הסביבה הבאה.<br><input type="checkbox"/> יש תקשורת בין הסורק לבין שרת ה-DNS.<br><input type="checkbox"/> מתבצע סינכרון בין הזמן עבור הסורק, שרת ה-KDC והשרת הדרוש לשם אימות (שרת LDAP, שרת SMTP, שרת קבצים).<br><input type="checkbox"/> כאשר מקצים את שרת השירות בתור כתובת ה-IP, ה-FQDN עבור שרת השירות נרשם באזור הבדיקה אחורה של שרת ה-DNS. |
| Kerberos Realm to be Used             | אם תבחר <b>Kerberos Authentication</b> עבור <b>Authentication Method</b> , בחר את תחום ה-Kerberos בו ברצונך להשתמש.  |
| Administrator DN / User Name          | הזן שם משתמש עבור שרת LDAP ב-128 תווים או פחות בפורמט Unicode (קידוד UTF-8). לא ניתן להשתמש בתווי בקרה כגון 0x00 עד 0x1F או 0x7F. הגדרה זו אינה בשימוש כאשר בוחרים <b>Anonymous Authentication</b> בתור <b>Authentication Method</b> . אם אינך מעוניין לציין זאת, השאר את המקום ריק.   |
| Password                              | הזן הסיסמה עבור אימות שרת LDAP ב-128 תווים או פחות בפורמט Unicode (קידוד UTF-8). לא ניתן להשתמש בתווי בקרה כגון 0x00 עד 0x1F או 0x7F. הגדרה זו אינה בשימוש כאשר בוחרים <b>Anonymous Authentication</b> בתור <b>Authentication Method</b> . אם אינך מעוניין לציין זאת, השאר את המקום ריק.   |

### הגדרות Kerberos

אם תבחר את **Kerberos Authentication** בתור **Authentication Method**, יהיה עליך ליצור הגדרות **Kerberos**. תוכל לרשום עד 10 הגדרות **Kerberos**.

בעת ביצוע הגדרה מתוך **Web Config**:

בחר בלשונית **Kerberos Settings < Network**.  
 בעת ביצוע הגדרה מתוך **Epson Device Admin**:  
 בחר **Kerberos Settings < Security < Network** מתוך תבנית התצורה.

| הגדרות והסבר  | פריט                   |
|---|------------------------|
| הזן את התחום לאימות Kerberos ב-255 תווי ב-ASCII או פחות (–0x20 0x7E). אם אינך מעוניין לרשום זאת, השאר את המקום ריק.                 | Realm (Domain)         |
| הזן את כתובת שרת האימות של Kerberos. הזן 255 תווים או פחות בפורמט IPv4, FQDN או IPv6. אם אינך מעוניין לרשום זאת, השאר את המקום ריק. | KDC Address            |
| הזן את מספר כניסת שרת ה-Kerberos בין 1 לבין 65535.  | Port Number (Kerberos) |

## הגדרת התצורה של הגדרות החיפוש של שרת LDAP

מגדירה את תכונות החיפוש עבור הגדרות משתמש.

בעת ביצוע הגדרה מתוך **Web Config**:

בחר בלשונית **Search Settings (Authentication) < LDAP Server < Network**.

בעת ביצוע הגדרה מתוך **Epson Device Admin**:

בחר **LDAP server < Authentication Settings < Administrator Settings < Search Settings (Authentication)** מתוך תבנית התצורה.

| הגדרות והסבר   | פריט                             |
|--|----------------------------------|
| ציין את מיקום ההתחלה בעת חיפוש של מידע משתמש מתוך שרת LDAP. הזן בין 0 ל-28 תווים ב-Unicode (קידוד UTF-8). אם אינך מחפש מאפיין אקראי, השאר זאת ריק.<br>למשל, עבור תיקיית השרת המקומי: dc=local ,dc=server | Search Base (Distinguished Name) |
| ציין את שם המאפיין שיש להציג בעת חיפוש אחר המספר המזהה. הזן בין 1 לבין 255 תווי ASCII. התו הראשון צריך להיות a-z או A-Z.<br>דוגמה: uid ,cn   | User ID Attribute                |
| ציין את שם המאפיין שיש להציג כשם המשתמש. הזן בין 0 לבין 255 תווי ASCII. התו הראשון אמור להיות a-z או A-Z. תוכל להשאיר זאת ריק.<br>דוגמה: name ,cn  | User name Display Attribute      |
| ציין את שם התכונה שיש להציג בתור מזהה כרטיס האימות. הזן בין 0 לבין 255 תווי ASCII. התו הראשון אמור להיות a-z או A-Z. תוכל להשאיר זאת ריק.<br>דוגמה: sn ,cn   | Authentication Card ID Attribute |
| ציין את שם המאפיין שיש להציג בעת חיפוש אחר המספר המזהה. הזן בין 1 לבין 255 תווי ASCII. התו הראשון צריך להיות a-z או A-Z.<br>דוגמה: id ,cn  | ID Number Attribute              |



| פריט                    | הגדרות והסבר   |
|-------------------------|--|
| Department Attribute    | ציין את שם המאפיין שיש להציג כשם המחלקה. הזן בין 0 לבין 255 תווי ASCII. התו הראשון אמור להיות a-z או A-Z. תוכל להשאיר זאת ריק. לדוגמה: ou-cl ,ou |
| Email Address Attribute | ציין את שם המאפיין שיש להציג בעת חיפוש אחר כתובות דוא"ל. הזן בין 1 לבין 255 תווי ASCII. התו הראשון צריך להיות a-z או A-Z. דוגמה: mail            |
| Save To Attribute       | ציין את שם התכונה המצביע על היעד עבור Scan To My Folder. הזן בין 0 לבין 255 תווי ASCII. לדוגמה: homeDirectory                                    |

## בדיקת החיבור עם שרת LDAP

מבצעת את בדיקת החיבור אל שרת LDAP באמצעות הפרמטר שהוגדר בתוך LDAP Server < Search Settings

1. גש אל Web Config ובחר את לשונית Network < LDAP Server < Connection Test.

2. בחר Start.

בדיקת החיבור התחילה. אחרי הבדיקה, יוצג דו"ח בדיקה.

## הפניות בדיקת חיבור שרת LDAP

| הודעות  | הסבר   |
|---|--|
| Connection test was successful.   | הודעה זו מופיעה כאשר הקשר עם השרת הצליח.   |
| Connection test failed.<br>Check the settings.                                | ההודעה מופיעה מהסיבות הבאות:<br><input type="checkbox"/> כתובת שרת LDAP או מספר היציאה שגויים.<br><input type="checkbox"/> התרחש פסק זמן.<br><input type="checkbox"/> Do Not Use נבחר בתור Use LDAP Server.<br><input type="checkbox"/> אם בוחרים את Kerberos Authentication כ- Authentication Method, הגדרות כגון Realm (Domain), KDC Address ו- Port Number (Kerberos) שגויות. |
| Connection test failed.<br>Check the date and time on your product or server. | הודעה זו מופיעה כאשר החיבור נכשל משום שאין התאמה בין הגדרות הזמן עבור הסורק ועבור שרת LDAP.  |

| הודעות  | הסבר  |
|---|---|
| Authentication failed.<br>Check the settings.           | ההודעה מופיעה מהסיבות הבאות:<br><input type="checkbox"/> User Name ו/או Password שגויים.<br><input type="checkbox"/> אם בוחרים Kerberos Authentication כ-<br>Authentication Method, אפשר שתצורת השעה/תאריך לא הוגדרה. |
| Cannot access the product until processing is complete. | הודעה זו מופיעה כאשר הסורק תפוס.  |

## הגדרת שרת הדוא"ל

כאשר אתה משתמש ב-Scan to My Email, הגדר את שרת הדוא"ל.  
לתשומת לבך:  
תוכל להגדיר את Scan to My Email רק כאשר Scan to Email אופשרה.

בעת ביצוע הגדרה מתוך Web Config:

בחר בלשונית Basic < Email Server < Network.

בעת ביצוע הגדרה מתוך Epson Device Admin:

בחר Common < Email Server < Mail Server Settings מתוך תבנית התצורה.

| פריט                    | הגדרות והסבר  |
|-------------------------|---|
| Authentication Method   | ציין את שיטת האימות עבור גישת הסורק אל שרת הדואר.   |
|                         | אימות מושבת בתקשורת עם שרת דואר. Off  |
|                         | שרת הדוא"ל צריך לתמוך באימות SMTP. SMTP AUTH  |
|                         | כאשר אתה בוחר פריט זה, הגדר שרת POP3. POP before SMTP   |
| Authenticated Account   | אם תבחר SMTP AUTH או POP before SMTP בתור Authentication Method, הזן את שם החשבון המאומת. הזן בין 0 לבין 255 תווים ב-ASCII (0x20-0x7E). |
| Authenticated Password  | אם תבחר SMTP AUTH או POP before SMTP בתור Authentication Method, הזן את הסיסמה המאומתת. הזן בין 0 לבין 20 תווים ב-ASCII (0x20-0x7E).    |
| Sender's Email Address  | הזן את כתובת הדוא"ל 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, מספרים, 0-9, נקודה (.) ומקף (-). תוכל להשתמש בתבנית IPv4 או FQDN.                           |
| SMTP Server Port Number | הזן מספר בין 1 ל-65535.   |

| הגדרות והסבר  | פריט                    |
|---|-------------------------|
| ציין את שיטת החיבור המאובטח לשרת הדואר האלקטרוני.   | Secure Connection       |
| אם אתה בוחר POP before SMTP ב-<br>Authentication Method, שיטת החיבור מוגדרת כ-<br>None.   | None                    |
| אפשרות זו זמינה כאשר Authentication Method<br>מוגדר כ-Off או כ-SMTP AUTH.   | SSL/TLS                 |
| אפשרות זו זמינה כאשר Authentication Method<br>מוגדר כ-Off או כ-SMTP AUTH.   | STARTTLS                |
| האישור מאומת כאשר מצב זה מאופשר. אנו ממליצים להגדיר זאת בתור Enable.  | Certificate Validation  |
| אם תבחר POP before SMTP בתור Authentication Method, הזן את כתובת שרת POP3. תוכל להזין בין 0 לבין 255 תווים תוך שימוש באותיות A-Z, a-z וכן 0-9. תוכל להשתמש בתבנית IPv4 או FQDN. | POP3 Server Address     |
| אם תבחר POP before SMTP בתור Authentication Method, ציין את מספר היציאה. הזן מספר בין 1 ל-65535.  | POP3 Server Port Number |

## הגדרת Scan to My Folder

שמור את התמונות הסרוקות בתיקיה שהוקצתה לכל משתמש. תוכל להגדיר את התיקיה הבאה כתיקיה ייעודית.

לתשומת לבך:

תוכל להגדיר את Scan To My Folder רק כאשר Scan to Network Folder/FTP אופשרה.

| מיקום הגדרת נתיב התיקיה             | Authentication Method  | הגדרות 'שמור אל'  |
|-------------------------------------|--|---|
| הגדרת סורק<br>(Scan to My Folder)   | Local DB <input type="checkbox"/><br>LDAP <input type="checkbox"/><br>Local DB and LDAP <input type="checkbox"/> | ציין תיקיית רשת אחת עבור כל Authentication Settings כדי ליצור באופן אוטומטי תיקייה אישית מתחת לתיקיה שצויינה באמצעות השימוש בשם של מזהה המשתמש. |
| סורק (User Settings)                | Local DB   | הקצה תיקיות רשת שונות נבדלות עבור כל משתמש.   |
| תכונות LDAP                         | LDAP   |   |
| תכונות סורק (User Settings) או LDAP | Local DB and LDAP  |   |

בעת ביצוע הגדרה מתוך Web Config:

בחר בלשונית Scan to Network Folder/FTP < Product Security.

בעת ביצוע הגדרה מתוך Epson Device Admin:

בחר Scan to Network Folder/FTP < Authentication Settings < Administrator Settings < Scan to My Folder מתוך תבנית התצורה.

| הסבר   | פריט            |                 |
|--|-----------------|-----------------|
| <p><input type="checkbox"/> <b>Shared</b></p> <p>יוצרת באופן אוטומטי תיקייה שקיבלה את שמה מתולך מזהה המשתמש מתחת לנתיב התיקייה או כתובת ה-URL שצויינו בתוך <b>Save to</b>, ושומרת את התמונות הסרוקות בתיקייה זו.</p> <p><input type="checkbox"/> <b>Individual</b></p> <p>הגדר את יעד השמירה עבור תוצאות סריקה עבור כל משתמש. ניתן להגדיר משתמשי Local DB בהגדרות המשתמש. משתמשי LDAP משתמשים במיקום אחסון שנרכש מתוך תכונות החיפוש של שרת LDAP.</p> | Setting Type    | Save To Setting |
| <p>בחר את פרוטוקול השידור בהתאם ליעד פלט הסריקה.</p> <p>עבור תיקייה רשת: <b>Network Folder (SMB)</b></p> <p>עבור שרת <b>FTP:FTP</b></p>  | Type            |                 |
| <p>ציין את הנתיב או כתובת ה-URL של נתיב הפלט. הזן בטווח של 160 תווים ב-UTF-16Unicode ( ).</p>  | Save to         |                 |
| <p>הגדר כאשר אתה בוחר <b>FTP</b> בתוך <b>Type</b>.<br/>בחקר מצב חיבור אל שרת ה-<b>FTP</b>.</p>   | Connection Mode |                 |
| <p>הגדר כאשר אתה בוחר <b>FTP</b> בתוך <b>Type</b>.<br/>הזן את מספר היציאה כדי לשלוח את הנתונים הסרוקים אל שרת <b>FTP</b> בין 0 לבין 65535.</p>   | Port Number     |                 |

| הסבר   | פריט         |                         |
|--|--------------|-------------------------|
| <p>הגדר כאשר אתה בוחר <b>Individual</b> בתור <b>Setting Type</b> בתוך <b>.Save To Setting</b>.</p> <p>הגדר את <b>User Name</b> ואת <b>Password</b> כדי לגשת אל התיקיה.</p> <p><input type="checkbox"/> <b>:Shared</b></p> <p>השתמש ב-<b>User Name</b> ו-<b>Password</b> משותפים עבור כל המשתמשים.</p> <p><input type="checkbox"/> <b>:Individual</b></p> <p>עבור משתמשי <b>Local DB</b> הגדר את <b>User Name</b> ואת <b>Password</b> בנפרד הגדרות המשתמש. לא ניתן להגדיר את התצורה של משתמשי <b>LDAP</b> בנפרד. <b>User Name</b> ו-<b>Password</b> שהוגדרו על ידי פריט זה משמשים כאצווה.</p> | Setting Type | Authentication Settings |
| <p>הזן את שם המשתמש כדי לגשת אל תיקיית היעד של פלט הסריקה.</p> <p>הזן בטווח של 30 תווים ב-UTF-16 ( ). הגדר זאת כאשר אתה משתמש בשרת <b>Shared</b> או <b>LDAP</b>.</p>   | User Name    |                         |
| <p>הזן את הסיסמה התואמת אל <b>User Name</b>.</p> <p>הזן בטווח של 20 תווים ב-UTF-16 ( ). הגדר זאת כאשר אתה משתמש בשרת <b>Shared</b> או <b>LDAP</b>.</p>   | Password     |                         |

## איסור שינוי היעד עבר **Scan to Network Folder/FTP**

| הסבר  | פריט                                 |
|---|--------------------------------------|
| <p>כאשר מאפשרים זאת, המשתמש לא יכול לשנות את יעד ברירת המחדל.</p> | Prohibit manual entry of destination |

## Customize One-touch Functions

תוכל להציג רק את הסמלים הדרושים באמצעות עריכת פריסת הסמלים המוצגת במסך הבית עבור לוח הבקרה.

בעת ביצוע הגדרה מתוך **Web Config**:

בחר בלשונית **Customize One-touch Functions < Product Security**.

בעת ביצוע הגדרה מתוך **Epson Device Admin**:

בחר **Authentication Settings < Administrator Settings**

**Customize One-touch Functions** מתוך תבנית התצורה.

לתשומת לבך:

במקרים הבאים, סמלים עבור הפונקציות שצוינו אינם מוצגים במסך הבית.

כאשר אתה בוחר פונקציות שאסורות בגין **Restrictions**.

כאשר כתובת דוא"ל עבור משתמש שנכנס למערכת אינה רשומה. (*Scan to My Email*)

כאשר תיקיית היעד לא הוגדרה. (*Scan to My Folder*)

| הסבר  | פריט                         |
|---|------------------------------|
| בחר את הפריסה של הסמלים המוצגים בלוח הבקרה. התמונה משתנה בהתאם לפריסה הנבחרת. | Maximum functions per screen |
| בחר את מספר העמודים.  | Screen(s)                    |
| בחר את הפונקציות שברצונך להציג עבור כל מיקום ממוספר.                          | Number                       |

## דיווחי Job History באמצעות Epson Device Admin

תוכל ליצור דוח Job History עבור כל קבוצה וכל משתמש באמצעות Epson Device Admin. תוכל לשמור בסורק עד 3,000 מופעים של היסטוריות שימוש. תוכל ליצור את הדוח באמצעות ציון תקופה או הגדרת ל"ז סדיר.

על מנת לייצוא את Job History כדוח Options <

< Epson Print Admin Serverless/Authentication Settings

Manage the Epson Print Admin Serverless/Authentication compatible devices

מתפריט הסרט במסך רשימת ההתקנים.

לפרטים כיצד ליצור דוח משתמש, עיין בתיעוד עבור Epson Device Admin.



### פריטים שניתן לכלול בדוח

תוכל להעביר את הפריטים הבאים כפלט לתוך דוח המשתמש.

:Scan/Result details/Result/Department/User ID/Operation/Job ID/Date  
 :Scan/Color :Scan/2-Sided :Scan/Paper Size :Scan/Destination :Scan/Destination type  
 :Devices/Serial Number :Devices/IP Address :Devices/Model :Devices/Pages  
 Note :Devices/Remark :Devices/Location :Devices/Department

## כניסה כמנהל מלוח הבקרה

תוכל להשתמש בכל אחת מהשיטות הבאות כדי להיכנס כמנהל מלוח הבקרה של הסורק.

1. הקש  בפינה הימנית העליונה של המסך.  
 כאשר Authentication Settings מאופשרות, הסמל מוצג במסך ברוכים הבאים (מסך ההמתנה לאימות).  
 כאשר Authentication Settings, מוצגות, הסמל מוצג במסך הבית.
2. הקש כן כאשר מסך האישור מוצג.
3. הזן את סיסמת המנהל.  
מוצגת הודעה שהכניסה הושלמה ולאחר מכן מוצג מסך הבית בלוח הבקרה.  
כדי לצאת מהמערכת, הקש  בפינה הימנית העליונה של מסך הבית.

---

## השבתת Authentication Settings

תוכל להשבית את Authentication Settings תוך שימוש ב-Web Config.

לתשומת לבך:

ה-User Settings הרשומות לסורק יישמרו אפילו אם Authentication Settings יושבתו. תוכל להסירן באמצעות שחזור הסורק להגדרות ברירת המחדל שלו.

1. גש אל "Web Config".

2. בחר בלשונית Authentication < Basic < Product Security.

3. בחר OFF.

4. לחץ על Next.

5. לחץ על OK.

לתשומת לבך:

גם אם תשבית את Authentication Settings, הגדרת נעילה תישאר מאופשרת. אם תרצה להשבית אותה, תוכל לבצע הגדרות מתוך לוח הבקרה או Web Config.

מידע קשור

← "הגדרת הגדרת נעילה מלוח הבקרה" בעמוד 86

← "הגדרת הגדרת נעילה מתוך Web Config" בעמוד 86

---

## מחיקת מידע Authentication Settings (שחזר להגדרות ברירת המחדל)

כדי למחוק את כל המידע של Authentication Settings (Authentication Method, Card Reader), שחזר את כל הגדרות הסורק להגדרות ברירת המחדל בעת הרכישה. User Settings, וכן הלאה), שחזר את כל הגדרות הסורק להגדרות ברירת המחדל בעת הרכישה. בחר הגדרות < ניהול מערכת < שחזר להגדרות ברירת המחדל < כל ההגדרות בלוח הבקרה.

חשוב: 

”ימחקו גם כל אנשי הקשר והגדרות הרשת האחרות. לא ניתן לשחזר הגדרות שנמחקו.

---

## פתרון בעיות

### לא ניתן לקרוא את כרטיס האימות

בדוק את הדברים להלן.

- בדוק אם התקן האימות מחובר אל הסורק בצורה נכונה.  
חבר את התקן האימות אל יציאת ה-USB של הממשק החיצוני בגב הסורק.
- ודא שיש תמיכה בהתקן האימות ובכרטיס האימות.



# תחזוקה

|          |                                 |
|----------|---------------------------------|
| 162..... | ניקוי המעטפת החיצונית של הסורק. |
| 162..... | ניקוי בתוך הסורק.               |
| 167..... | החלפת ערכת מכלול הגלגלת.        |
| 172..... | איפוס מספר הסריקות.             |
| 172..... | חסכון באנרגיה.                  |
| 173..... | העברת הסורק ממקום למקום.        |
| 174..... | גיבוי ההגדרות.                  |
| 175..... | שחזר להגדרות ברירת המחדל.       |
| 176..... | עדכון אפליקציות וקושחה.         |

## ניקוי המעטפת החיצונית של הסורק

נגב כל כתם מהמארז החיצוני באמצעות מטלית יבשה או מטלית לחה שהורטבה בחומר ניקוי עדין ומים.

**חשוב!**

לעולם אין להשתמש באלכוהול, במדלל, או בכל ממש משתך אחר כדי לנקות את הסורק. הדבר עלול לגרום לעיוות או לשינויים בצבע.

אין להניח למים לחדור לתוך המוצר. הדבר עלול לגרום לתקלה.

לעולם אין לפתוח את מארז הסורק.

1. לחץ על לחצן  כדי לכבות את הסורק.

2. הוצא את תקע מתאם ז"ח מהסורק.

3. נקה את המארז החיצוני במטלית לחה שהורטבה בחומר ניקוי עדין ומים.

**לתשומת לבך:**

נגב את מסמך המוגע באמצעות מטלית רכה, יבשה.

## ניקוי בתוך הסורק

אחרי שמשתמשים בסורק זמן מה, ייתכן שאבק מהנייר ומהחדר יצטברו על הגליל או על חלק הזכוכית שבתוך הסורק וייגרמו לבעיות בהזנת הנייר או באיכות התמונות הסרוקות. נקה את פנים הסורק כל 5, 000 סריקות.

תוכל לבדוק את מספר הסריקות העדכני בלוח הבקרה או ב-Epson Scan 2 Utility.

אם פני שטח הוכתמו בחומר שקשה להסיר, תוכל להשתמש בערכת ניקוי מקורית של Epson כדי להסיר את הכתמים. כדי להסיר כתמים, יש להשתמש בכמות קטנה של חומר ניקוי על מטלית הניקוי.

**חשוב!**

לעולם אין להשתמש באלכוהול, במדלל, או בכל ממש משתך אחר כדי לנקות את הסורק. הדבר עלול לגרום לעיוות או לשינויים בצבע.

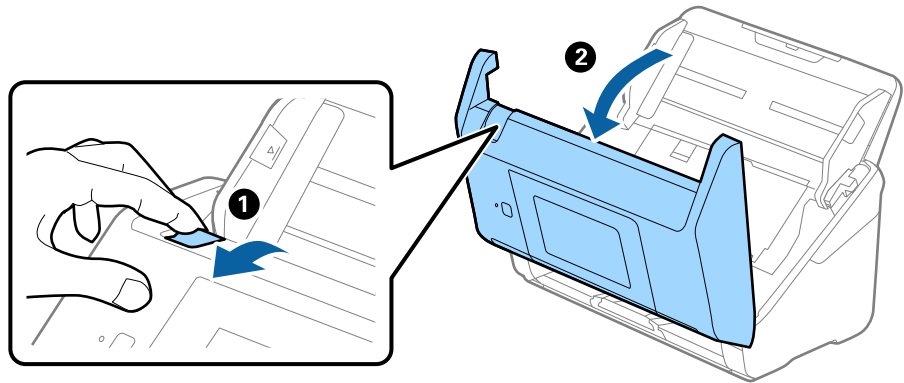
לעולם אין לרסס נוזל או חומר סיכה על הסורק. נזק לציוד או למעגלים עלול לגרום לפעולות בלתי תקינות.

לעולם אין לפתוח את מארז הסורק.

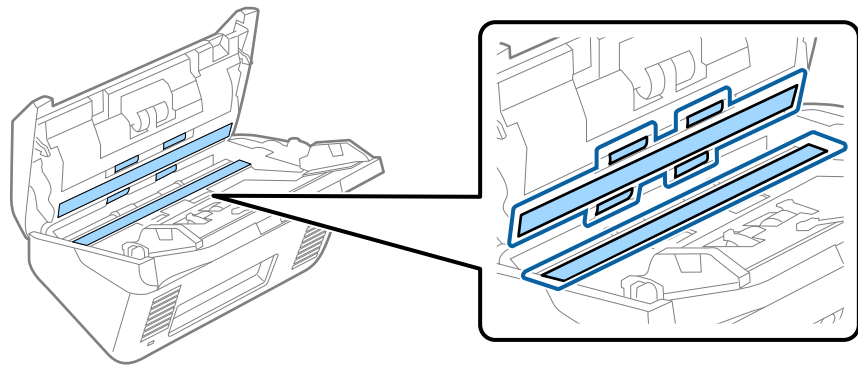
1. לחץ על לחצן  כדי לכבות את הסורק.

2. הוצא את תקע מתאם ז"ח מהסורק.

3. משוך את הידית ופתח את מכסה הסורק.



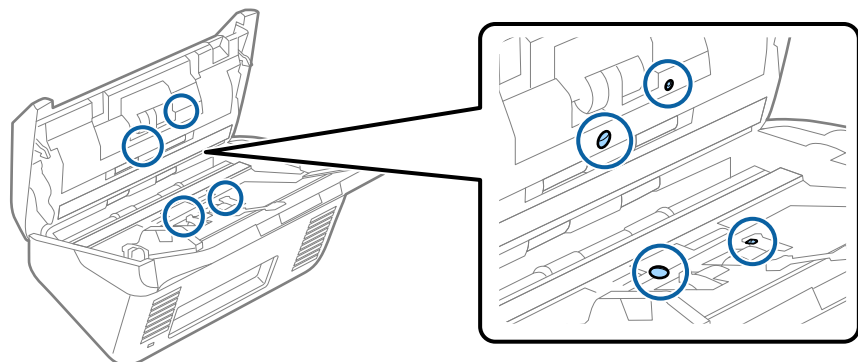
4. יש לנגב כתמים כלשהם מגליל הפלסטיק וממשטח הזכוכית שבתוך תחתית מכסה הסורק באמצעות מטלית לחה או ערכת ניקוי מקורית של Epson.



**חשוב!**

- אין להפעיל כוח רב מדי על משטח הזכוכית.
- אין להשתמש במברשת או בכלי קשיח. כל שריטה של הזכוכית עלולה להשפיע על איכות הסריקה.
- אין לרסס חומר ניקוי ישירות על גבי משטח הזכוכית.

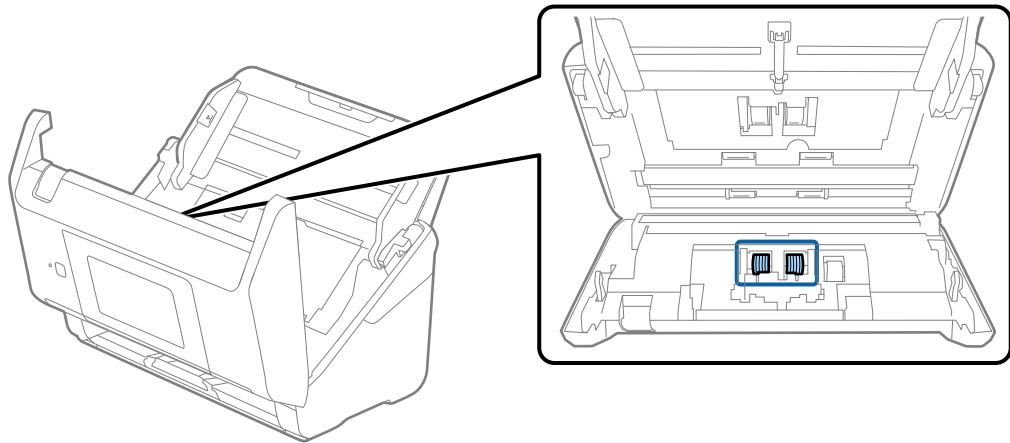
5. יש לנגב כתמים כלשהם על החיישנים באמצעות מטוש כותנה.



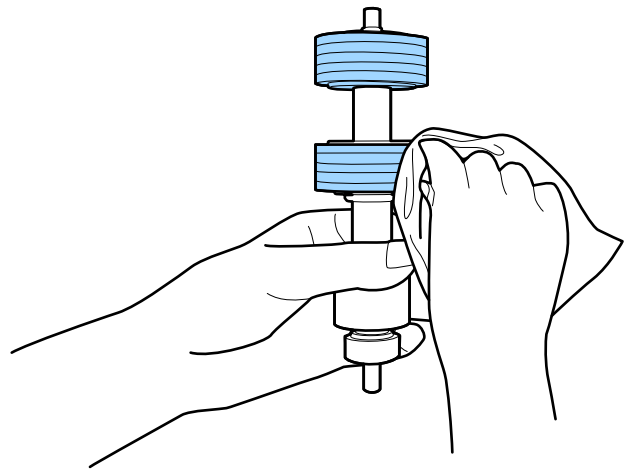
**חשוב:** 

אין להספיג את מטוש הכותנה בנוזל, כגון חומר ניקוי.

6. פתח את המכסה, ואז הסר את גליל ההפרדה. למידע נוסף עיין בסעיף "החלפת ערכת מכלול הגלילים".



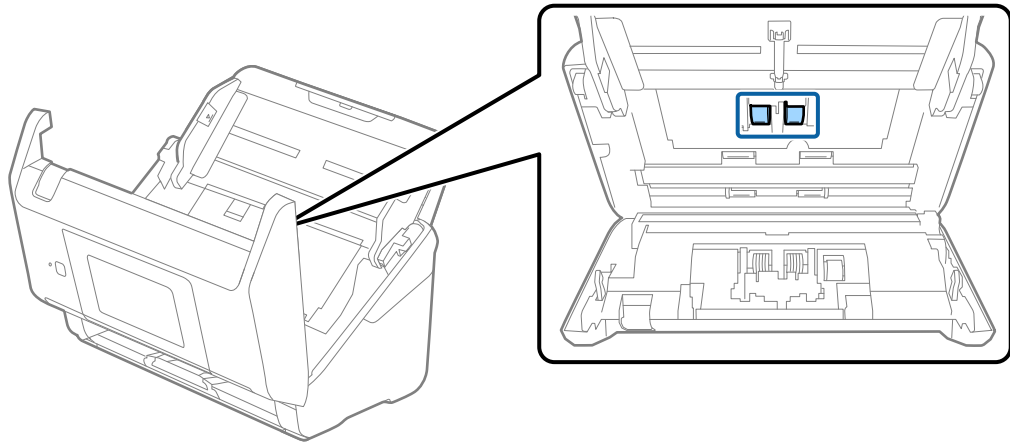
7. נגב אבק או לכלוך כלשהם שהצטברו על גליל ההפרדה, תוך שימוש בערכת ניקוי Epson מקורית או במטלית רכה לחה.



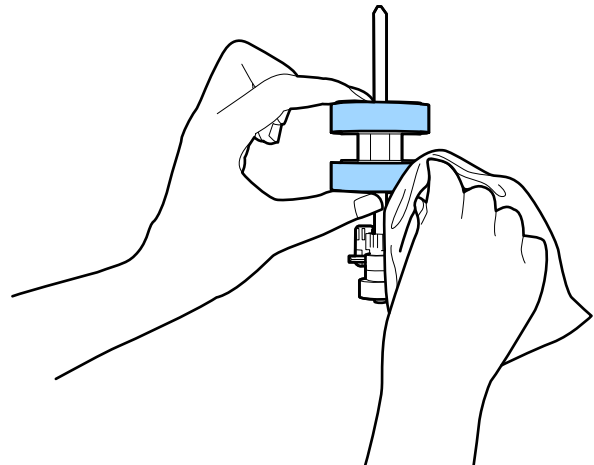
**חשוב:** 

יש להשתמש אך ורק בערכת ניקוי מקורית של Epson או במטלית רכה לחה כדי לנקות את הגליל. השימוש במטלית יבשה עלול להזיק לפני הגליל.

8. פתח את המכסה, ואז הסר את גליל האיסוף. למידע נוסף עיין בסעיף "החלפת ערכת מכלול הגלילים".



9. נגב אבק או לכלוך כלשהם שהצטברו על גליל האיסוף, תוך שימוש בערכת ניקוי Epson מקורית או במטלית רכה לחה.

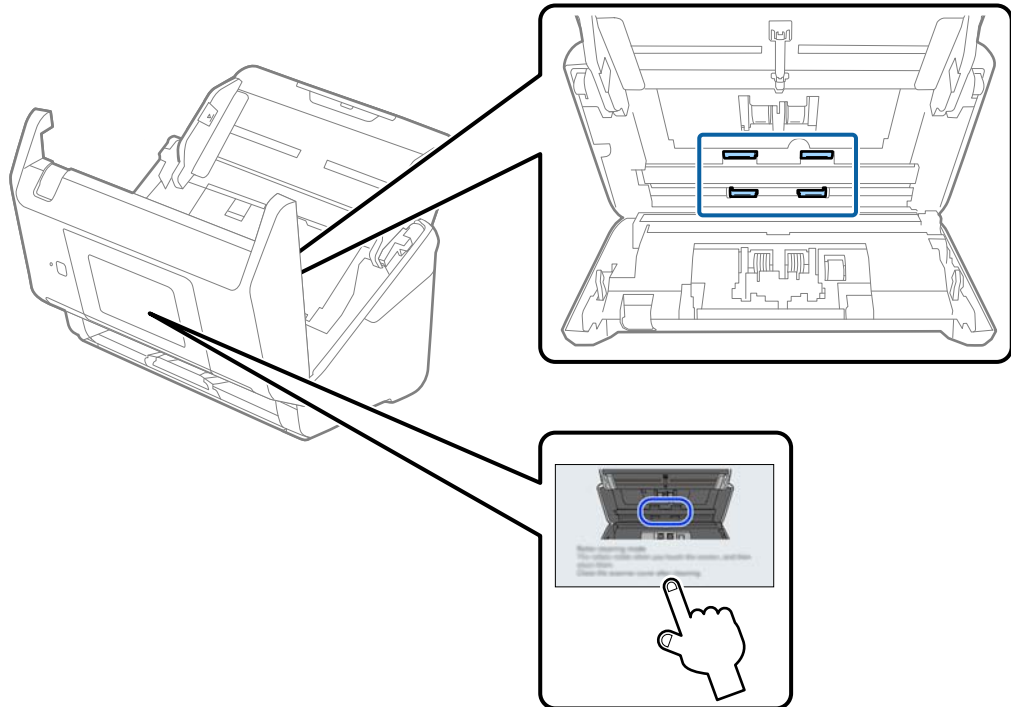


**חשוב:** 

יש להשתמש אך ורק בערכת ניקוי מקורית של Epson או במטלית רכה לחה כדי לנקות את הגליל. השימוש במטלית יבשה עלול להזיק לפני הגליל.

10. סגור את מכסה הסורק.  
 11. תקע את מתאם הז"ח בשקע והדלק את הסורק.  
 12. בחר תחזוקת הסורק ממסך הבית.  
 13. במסך תחזוקת הסורק בחר ניקוי הגלגלת.  
 14. משוך את הידית כדי לפתוח את מכסה הסורק. הסורק נכנס למצב ניקוי גלילים.

15. סובב את את הגלילים בתחתית באמצעות הקשה במקום כלשהו במסך הגביש הנוזלי. נגב את פני השטח של הגלילים באמצעות ערכת ניקוי מקורית של Epson או מטלית רכה שלוחלחה במים. חזור על פעולה זו עד שהגלילים יהיו נקיים.



**⚠ זהירות:**

היזהר שידידך או שערך לא יילכדו במנגנון בעת הפעלת הגליל. הדבר יכול לגרום פציעה.

16. סגור את מכסה הסורק.

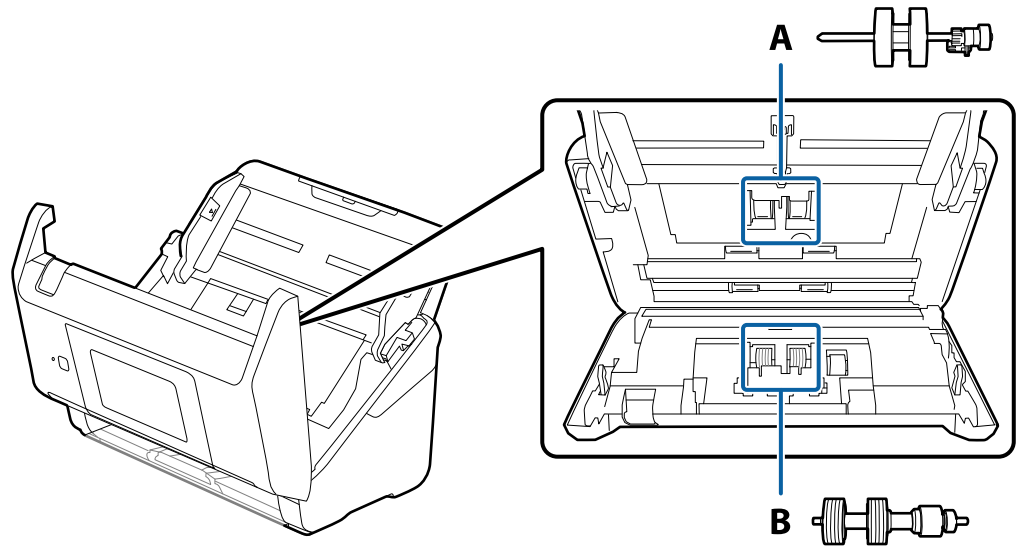
הסורק יוצא ממצב ניקוי גלילים.

מידע קשור


← "החלפת ערכת מכלול הגלגלת" בעמוד 167

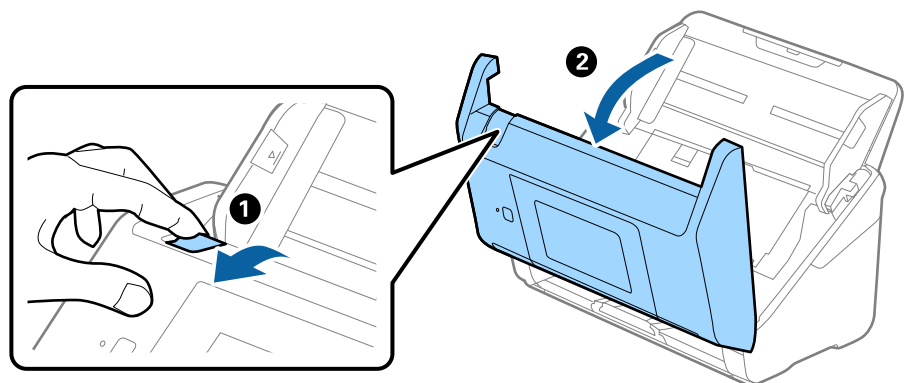
## החלפת ערכת מכלול הגלגלת

יש להחליף את ערכת מכלול הגלגלות (גלגלת האיסוף וגלגלת הפרדה) כאשר מספר הסריקות עולה על מחזור החיים של הגלגלות. כאר מוצגת הודעת החלפה בלוח הבקרה במסך המחשב שלך, פעל בהתאם לצעדים הבאים כדי לבצע את ההחלפה.

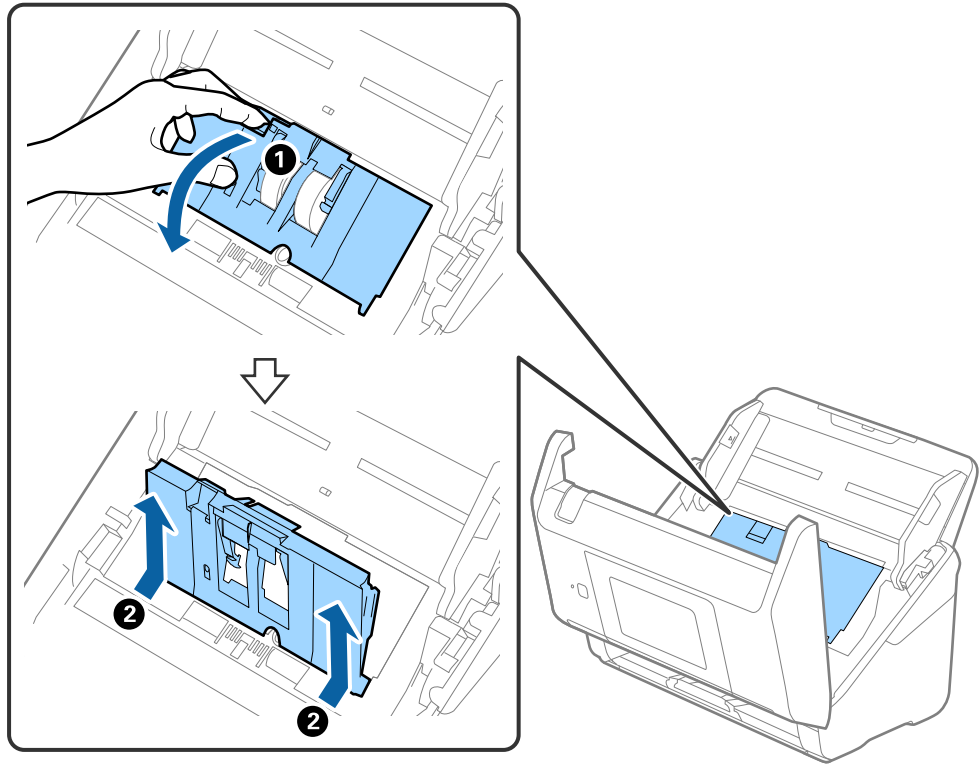


A: גלגלת איסוף, B: גלגלת הפרדה

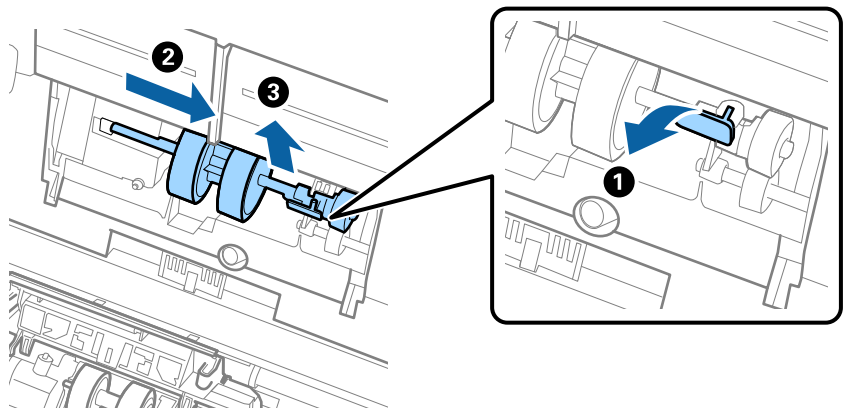
1. לחץ על לחצן  כדי לכבות את הסורק.
2. הוצא את תקע מתאם ז"ח מהסורק.
3. משוך את הידית ופתח את מכסה הסורק.



4. פתח את מכסה גליל האיסוף, ואז החלק אותו והסר אותו.



5. משוך כלפי מטה את האביזר של ציר הגליל, ואז החלק והסר את גלילי האיסוף המותקנים.

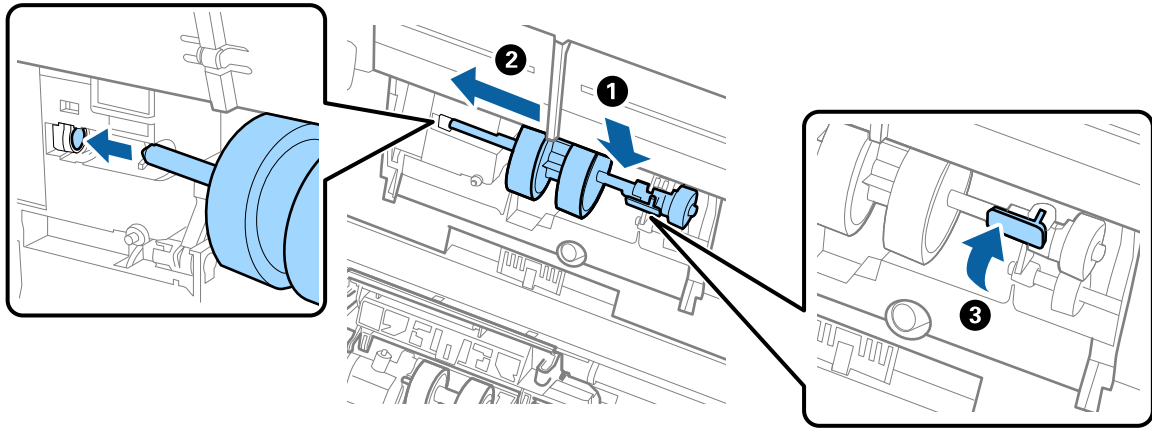


**חשוב!**

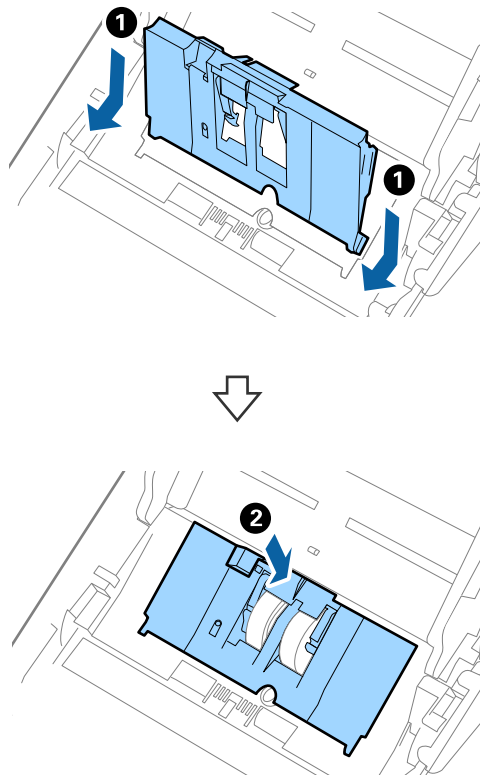
אל תמשוך את גליל האיסוף החוצה בכוח. הדבר עלול להזיק לפנים הסורק.



6. תוך שאתה מחזיק את האביזר, החלק את גליל האיטוף החדשה שמאלה והכנס אותו לתוך החור בסורק. לחץ על האביזר כדי לקבע אותו במקומו.

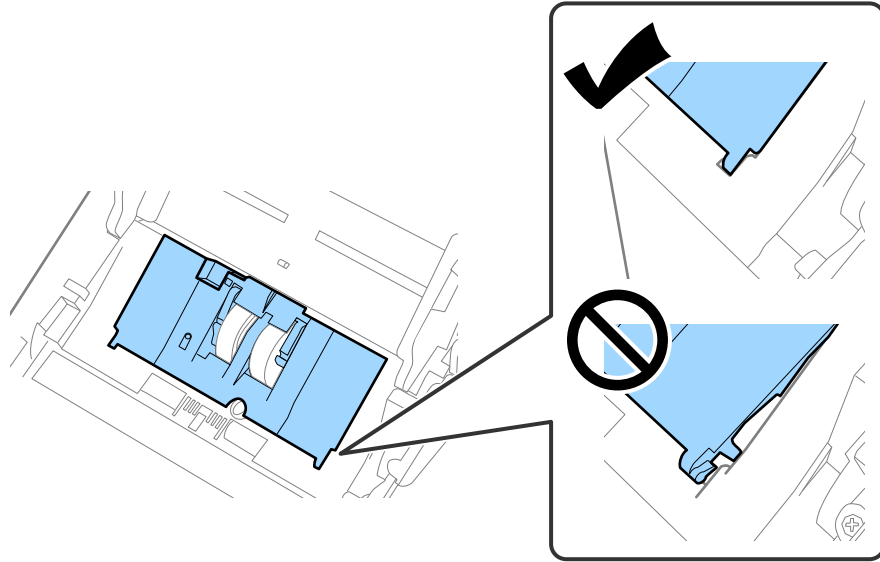


7. הנח את כסה מכסה גליל האיטוף בתוך החרוץ והחלק אותו. סקור את המכסה היטב.

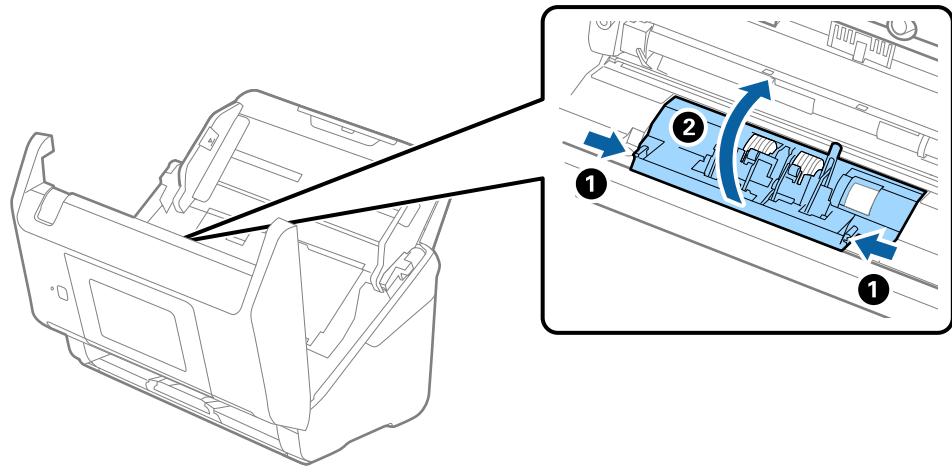


**חשוב!**

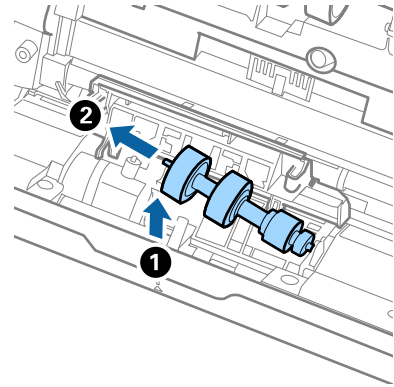
- ❑ ודא שמכסה גליל האיסוף סגור בצורה נכונה.
- ❑ אם קשה לסגור את המכסה, ודא שגלגלת האיסוף הותקנה כהלכה.
- ❑ אל תתקין את המכסה בזמן שהוא מורם.



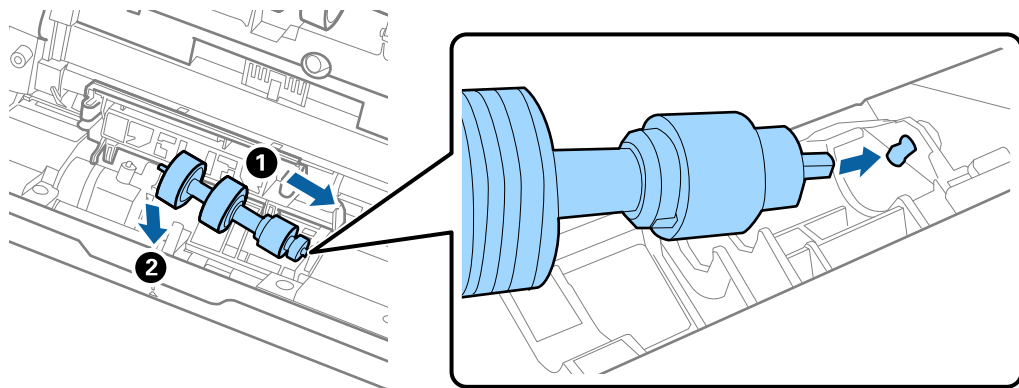
8. דחוף את הווים משני צידי מכסה גליל ההפרדה כדי לפתוח את המכסה.



9. הרם את צידו השמאלי של גליל ההפרדה ואז החלק והסר את גלילי ההפרדה המותקנים.



10. הכנס את ציר גליל ההפרדה החדשה לתוך החור בצד ימין ואז הורד את הגליל.



11. סגור את מכסה גליל ההפרדה.

**חשוב!**

אם קשה לסגור את המכסה, דאג להתקין בצורה נכונה את גלילי ההפרדה.

12. סגור את מכסה הסורק.

13. תקע את מתאם הז"ח בשקע והדלק את הסורק.

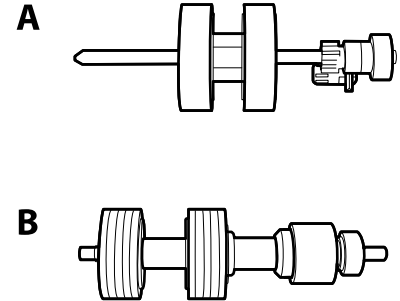
14. אפס את מספר הסורק בלוח הבקרה.

לתשומת לבך:

יש לסלק את גלגלת האיסוף ואת גלגלת ההפרדה בהתאם לכללים ולתקנות של הרשות המקומית שלך. אין לפרק אותם.

## קודי ערכת מכלול גלילים

יש להחליף את החלקים (גלגלת האיסוף וגלגלת ההפרדה) כאשר מספר הסריקות עולה על מספר השירות. תוכל לבדוק את מספר הסריקות העדכני בלוח הבקרה או ב-Epson Scan 2 Utility.



A: גלגלת איסוף, B: גלגלת הפרדה

| שם החלק           | קודים                                | מחזור חיים |
|-------------------|--------------------------------------|------------|
| ערכת מכלול גלילים | B12B819671<br>B12B819681 (הודו בלבד) | 200,000*   |

\* מספר זה הוא תוצאה של סריקה רציפה באמצעות דפי בדיקה מקוריים של Epson והוא משמש כמדריך למחזור החלפה. מחזור ההחלפה עשוי להשתנות בהתאם לסוגי נייר שונים, כגון נייר המפיק הרבה מאוד אבק נייר או נייר בעל פני מרקם מחוספס שעלולים לקצר את מחזור החיים.

## איפוס מספר הסריקות

אפס את מספר הסריקות אחרי החלפת ערכת מכלול הגלגלת.

1. בחר הגדרות < פרטי המכשיר < איפוס מספר הסריקות < מספר הסריקות אחרי החלפת הגלגלת ממסך הבית.
2. הקש כן.

מידע קשור

← "החלפת ערכת מכלול הגלגלת" בעמוד 167

## חסכון באנרגיה


תוכל לחסוך אנרגיה באמצעות מצב שינה או מצב כיבוי אוטומטי כאשר הסורק אינו מבצע פעולות. תוכל להגדיר את פרק הזמן שיחלוף לפני שהסורק ייכנס למצב שינה ויכבה את עצמו אוטומטית. כל הארכה תשפיע על יעילותו האנרגטית של המוצר. קח בחשבון את הסביבה לפני שתבצע שינויים כלשהם.

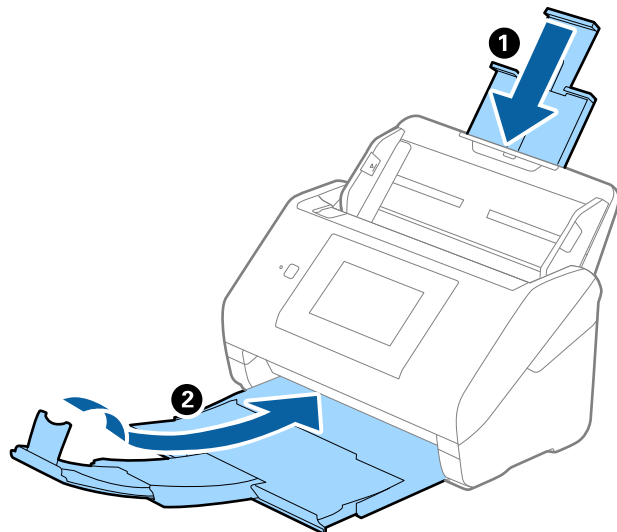
1. בחר את הגדרות במסך הבית.

2. בחר הגדרות בסיסיות.
3. בחר באפשרות הגדרות כיבוי וערוך את ההגדרות.  
לתשומת לבך:  
אפשר שהתכונות הזמינות ישתנו בהתאם למיקום הרכישה.

## העברת הסורק ממקום למקום

כאשר אתה רוצה להעביר את הסורק או להזיז אותו כדי לבצע תיקונים, פעל על פי השלבים המובאים להלן כדי לארוז את הסורק.

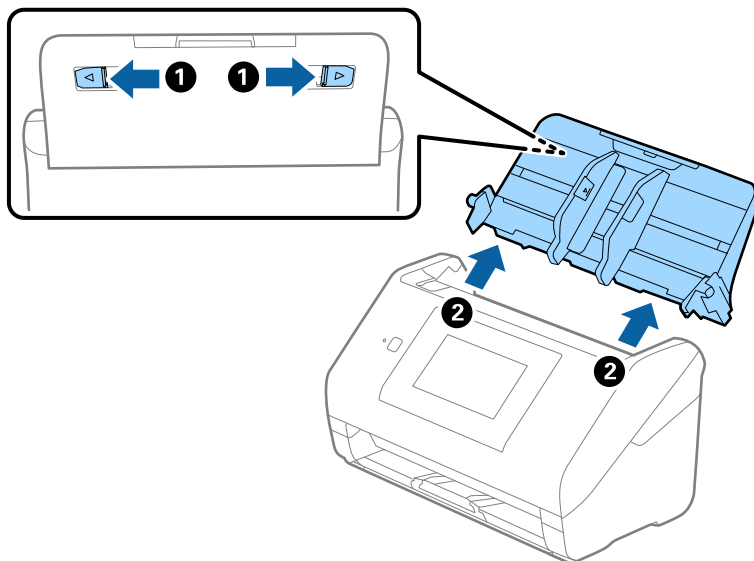
1. לחץ על לחצן  כדי לכבות את הסורק.
2. הוצא את מתאם הז"ח מהשקע.
3. הסר את הכבלים ואת ההתקנים.
4. סגור את הארכת מגש הקלט ואת מגש הפלט.



**חשוב:** 

ודא שסגרת היטב את מגש הקלט; אחרת הוא עלול להינזק במהלך ההעברה.

5. הסר את מגש הקלט.



6. צרף את חומרי האריזה שהגיעו עם הסורק, ואז חזור וארוז את הסורק באריזתו המקורית או בקופסה איתנה.

## גיבוי ההגדרות

תוכל לייבא את ערך ההגדרות שהוגדר מ- Web Config אל הקובץ. תוכל להשתמש בו כדי לגבות אנשי קשר, ערכי הגדרה, החלפת הסורק וכו'.  
לא ניתן לערוך את הקובץ שיוצא משום שהוא מיוצא כקובץ בינארי.

## יצא את ההגדרות

יצא את ההגדרה עבור הסורק.

1. גש אל Web Config, ואז בחר את לשונית **Device Management < Export < Export and Import Setting Value**.

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 שיוצא.

אתה זקוק לסיסמה כדי ליבא את הקובץ. השאר זאת ריק אם אין ברצונך להצפין את הקובץ.

## 4. לחץ על Export.

חשוב: 

אם ברצונך לייצא את הגדרות הרשת של הסורק, למשל שם ההתקן וכתובת ה-IPv6 שלה, בחר *Enable to select the individual settings of device* ובחר עוד פריטים. השתמש אך ורק בערכים שנבחרו בשביל הסורק המחליף.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## יבא את ההגדרות

יבא את קובץ Web Config שיוצא אל הסורק.

חשוב: 

בעת ייבוא ערכים הכוללים מידע פרטי כגון שם סורק או כתובת IP, יש לוודא שאותה כתובת IP אינה קיימת באותה רשת.

1. גש אל Web Config, ואז בחר את לשונית **Device Management < Import < Export and Import Setting Value**.

2. בחר את הקובץ שיוצא, ואז הזמן את הסיסמה המוצפנת.

3. לחץ על Next.

4. בחר את ההגדרות שברצונך לייבא, ואז לחץ על Next.

5. לחץ על OK.

ההגדרות מוחלות על הסורק.

מידע קשור

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## שחזר להגדרות ברירת המחדל

בלוח הבקרה, בחר הגדרות < ניהול מערכת < שחזר להגדרות ברירת המחדל, ואז בחר את הפריטים שברצונך לשחזר לברירות המחדל שלהם.

הגדרות רשת: השב הגדרות הקשורות לרשת למצבן המקורי.

הכל חוץ מהגדרות הרשת: השב הגדרות אחרות למצבן הראשוני פרט להגדרות הקשורות לרשת.

כל ההגדרות: השב את כל ההגדרות למצבן הראשוני כפי שהיה בעת הרכישה.

חשוב: 

אם תבחר ותפעיל כל ההגדרות, יימחקו כל נתוני ההגדרות שנרשמו עבור הסורק, כולל אנשי הקשר והגדרות אימות המשתמש. לא ניתן לשחזר הגדרות שנמחקו.

## עדכון אפליקציות וקושחה

אפשר שיהיה ביכולתך לאפס בעיות מסוימות ולשפר או להוסיף פונקציות באמצעות עדכון האפליקציות והקושחה. דאג להשתמש בגרסה העדכנית ביותר של האפליקציות והקושחה.

חשוב: 

אל תכבה את המחשב או את הסורק בזמן העדכון.

לתשומת לבך:  
כאשר הסורק יכול להתחבר לאינטרנט, תוכל לעדכן את הקושחה מתוך *Web Config*. בחר את לשונית *Device Management < Firmware Update*, בדוק את ההודעה המוצגת, ואז לחץ על *Start*.

1. ודא שהסורק והמחשב מחוברים, ושהמחשב מחובר לאינטרנט.

2. התחל *EPSON Software Updater*, ועדכן את האפליקציות או הקושחה.

לתשומת לבך:

אין תמיכה במערכות הפעלה *Windows Server*.

Windows 10

לחץ על הלחצן 'התחל', ואז בחר *EPSON Software Updater < Epson Software*.

Windows 8.1/Windows 8

הזן את שם האפליקציה בצ'ארם החיפוש ולאחר מכן בחר בסמל המוצג.

Windows 7

לחץ על לחצן 'התחל' ובחר כל התכניות או תוכניות *EPSON Software < Epson Software < Updater*.

Mac OS

בחר מאתר < עבור אל < אפליקציות < *EPSON Software Updater < Epson Software*.

לתשומת לבך:

אם אינך יכול למצוא ברשימה את היישום שברצונך לעדכן אינך יכול לעדכן תוך שימוש ב-*EPSON Software Updater*. חפש את הגרסאות העדכניות ביותר של האפליקציות באתר האינטרנט המקומי של *Epson*.

<http://www.epson.com>

## עדכון קושחת הסורק באמצעות לוח הבקרה

אם ניתן לחבר את הסורק לאינטרנט, תוכל לעדכן את קושחת הסורק באמצעות לוח הבקרה. אפשר גם להגדיר לסורק לבדוק באופן סדיר אם קיימים עדכוני קושחה ולהודיע לך במידה ויש עדכונים זמינים מסוג זה.



1. בחר את הגדרות במסך הבית.
2. בחר ניהול מערכת < עדכון קושחה < עדכון.  
לתשומת לבך:  
בחר התראה < On כדי להגדיר לסורק לבדוק באופן סדיר אם קיימים עדכוני קושחה זמינים.
3. בדוק את ההודעה המוצגת על גבי המסך, והתחל לחפש עדכונים זמינים.
4. אם מוצגת הודעה על גבי מסך הגביש הנוזלי, המודיעה לך שקיים עדכון קושחה זמין, פעל בהתאם להוראות שעל גבי המסך כדי להתחיל את העדכון.

**חשוב!**

- אל תכבה את הסורק ואל תנתק אותו לפני השלמת העדכון; אחרת, עלולה להתרחש בסורק תקלה.
- אם עדכון הקושחה לא הושלם או לא הצליח, הסורק אינה נדלקת באופן רגיל, ומסך הגביש הנוזלי יציג את ההודעה "Recovery Mode" בפעם הבאה שמדליקים את הסורק. במצב זה, עליך לעדכן שוב את הקושחה באמצעות מחשב. חבר את הסורק למחשב באמצעות כבל USB. לא תוכל לעדכן את הקושחה באמצעות חיבור רשת כל זמן שההודעה "Recovery Mode" מוצגת בסורק. במחשב, גש לאתר Epson המקומי שלך, והורד משם את הקושחה העדכנית ביותר עבור הסורק. לשלבים הבאים, עיין בהוראות המוצגות באתר האינטרנט.

## עדכון קושחה באמצעות Web Config

כאשר הסורק יכול להתחבר לאינטרנט, תוכל לעדכן את הקושחה מתוך Web Config.

1. גש אל Web Config ובחר את לשונית **Firmware Update < Device Management**.
2. לחץ **Start**, ואז פעל בהתאם להוראות המוצגות על המסך.  
אישור הקושחה מתחיל, ומידע הקושחה מוצג במידה וקיימת קושחה מעודכנת.  
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

← "הפעלת Web Config בדפדפן אינטרנט" בעמוד 36

## עדכון קושחה בלא להתחבר לאינטרנט

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.

לתשומת לבך:

לפני ביצוע עדכון, ודא שמנהל ההתקן של הסורק **Epson Scan 2** מותקן במחשב שלך. אם **Epson Scan 2** אינה מותקנת, התקן אותה שוב.

1. בדוק באתר של Epson כדי למצוא את מהדורות עדכוני הקשוחה העדכניות ביותר.  
<http://www.epson.com>  
 אם יש קושחה עבור הסורק שלך, הורד אותה ועבור לשלב הבא.  
 אם אין מידע קושחה באתר האינטרנט, את כבר משתמש בקושחה העדכנית ביותר.
2. חבר את המחשב המכיל את הקושחה שהורדת אל הסורק באמצעות כבל USB.
3. לחץ לחיצה כפולה על קובץ ה-exe שהורדת.  
Epson Firmware Updater מופעל.
4. פעל בהתאם להוראות המוצגות על המסך.