Forescout®

מכשיר בודד

מדריך התקנה מהירה

גרסה 8.1

פרטי קשר

Forescout Technologies, Inc.
West Tasman Drive 190
San Jose, CA 95134 USA
https://www.forescout.com/support/
טלפון חינם (ארה"ב): 1.866.377.8771
טלפון (בינלאומי): 1.408.213.3191
תמיכה: 1.708.237.6591

אודות התיעוד

- לקבלת מסמכים נוספים פנה לדף 'משאבים' באתר האינטרנט של Forescout: https://www.forescout.com/company/resources/
- יש לך משוב או שאלות? כתוב לנו לכתובת documentation@forescout.com

אזהרה משפטית

2019-02-1316:19

תוכן העניינים

ברוכים הבאים לגרסה 8.1

פלטפורמת Forescout מספקת תשתית ונראות מכשירים, ניהול מדיניות, תיאום והתייעלות של זרימות עבודה, לחיזוק האבטחה ברשת. הפלטפורמה מספקת לארגונים מידע עם הקשר בזמן אמת על מכשירים ועל משתמשים ברשת. המדיניות מוגדרת באמצעות מידע זה עם הקשר, שעוזר להבטיח תאימות, תיקונים, גישה נכונה לרשת ויעילות של פעולות שירות.

מדריך זה מתאר את תהליך ההתקנה של מכשיר CounterACT עצמאי יחיד שהותקן מראש עם גרסה 8.0. חלק מהמכשירים עשויים להגיע כשהם מותקנים מראש עם גרסה מאוחרת יותר. על מנת להשתמש בגרסה 8.1, פעל על פי נתיב השדרוג המאושר, המתואר ב'הערות למהדורה' של הגרסה.

לפרטים נוספים או למידע על שדרוג או פריסה של מספר רב של מכשירים לצורך הגנה על רשת כלל-ארגונית, עיין במדריך *ההתקנה של Forescout* ובמדריך *הניהול של Forescout.* כדי למצוא כיצד לגשת אל מדריכים אלה, ראה תיעוד נוסף של Forescout.

בנוסף לכך, תוכל לנווט לאתר התמיכה הממוקם בכתובת: http://www.forescout.com/support לעיון בתיעוד עדכני, במאמרים ממאגר היעד ובעדכונים עבור המכשיר שברשותך.

תכולת חבילת Forescout

החבילה של Forescout כוללת את הרכיבים הבאים:

- מכשיר CounterACT
- מסגרת קדמית
- ערכות מסילה (תושבות הרכבה)
- כבל/י חשמל
- כבל לחיבור מסוף DB9 (לחיבורים טוריים בלבד)
- מידע בנושאי בטיחות, סביבה ותקינה עבור מוצרים ארגוניים
- מסמך 'תחילת העבודה' (מכשירי CT-xxxx המבוססים על חומרה מגרסה 5x ומכשירי 51xx Forescout בלבד)

סקירה כללית

פעל על פי ההנחיות הבאות כדי להתקין את Forescout:

1. צור תוכנית פריסה
2. הגדרת המתג
3. חיבור כבלי רשת והפעלה
4. קביעת תצורה של המכשיר
5. ניהול מרחוק
6. אימות הקישוריות
7. הגדר את מסוף CounterACT

1. צור תוכנית פריסה

לפני ביצוע ההתקנה, עליך להחליט היכן לפרוס את המכשיר ולהכיר את חיבורי הממשקים של המכשיר.

בחירת מיקום לפריסת המכשיר

בחירת המיקום הנכון ברשת להתקנת המכשיר היא חיונית לפריסה מוצלחת ולביצועים מיטביים. המיקום הנכון תלוי במטרות המיועדות ליישום ובמדיניות הגישה שלך לרשת. צריך לאפשר למכשיר לנטר את התעבורה הרלוונטית למדיניות הרצויה. לדוגמה, אם המדיניות תלויה בניטור של אירועים ארגוניים מנקודות קצה אל שרתי האימות הארגוניים, יש להתקין את המכשיר כך שיוכל לראות את זרימת התעבורה מנקודות הקצה אל שרתי האימות.

למידע נוסף על התקנה ופריסה, עיין ב*מדריך ההתקנה של Forescout*. כדי למצוא כיצד לגשת אל מדריך זה, ראה תיעוד נוסף של Forescout.

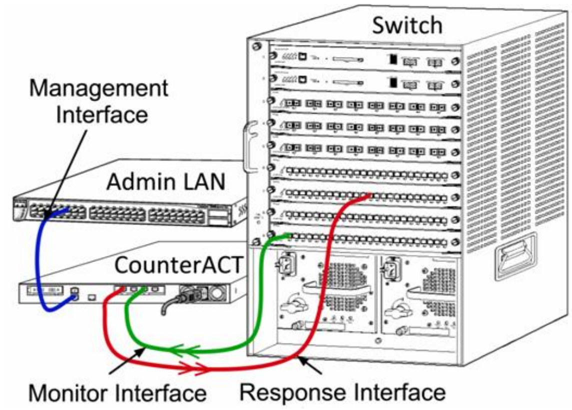
חיבורי ממשק של המכשיר

באופן כללי, המכשיר מוגדר עם שלושה חיבורים למתג הרשת.

ממשק ניהול

ממשק הניהול מאפשר לנהל את פלטפורמת Forescout ולבצע שאילתות ובדיקות מעמיקות של נקודות קצה. יש לחבר את הממשק ליציאת מיתוג עם גישה אל כל נקודות הקצה ברשת.

כל מכשיר מחייב חיבור ניהול יחיד אל הרשת. לחיבור זה דרושה כתובת IP ב-LAN המקומי וגישה ליציאה TCP/13000 מהמחשב שאמור להפעיל את יישום הניהול של המסוף. ליציאת הניהול נדרשת גישה אל שירותי רשת נוספים.



דרישות הגישה ברשת

יציאה	שירות	אל פלטפורמת **Forescout** או ממנה	פונקציה
22/TCP	SSH	מ-	מאפשרת בדיקה מרחוק של נקודות קצה ב-OS X וב-Linux. מאפשרת לפלטפורמת Forescout לתקשר עם מתגי ונתבי רשת.
		אל	מאפשרת גישה לממשק שורת הפקודה של פלטפורמת Forescout.
2222/TCP	SSH	אל	(זמינות גבוהה) מאפשרת גישה למכשירים הפיזיים, המהווים חלק מצמד הזמינות הגבוהה. השתמש ב-22/TCP כדי לגשת לכתובת ה-IP המשותפת (הווירטואלית) של הצמד.
25/TCP	SMTP	מ-	מאפשרת לפלטפורמת Forescout לגשת לממסר הדואר הארגוני.
53/UDP	DNS	מ-	מאפשרת לפלטפורמת Forescout לפענח כתובות IP פנימיות.
80/TCP	HTTP	אל	מאפשרת ניתוב מחדש ב-HTTP.
123/UDP	NTP	מ-	מאפשרת לפלטפורמת Forescout לגשת אל שרת שעון מקומי או אל ntp.forescout.net. כברירת מחדל פלטפורמת Forescout ניגשת אל ntp.foreScout.net
135/TCP	MS-WMI	מ-	מאפשרת בדיקה מרחוק של נקודות קצה ב-Windows.
139/TCP	SMB, MS-RPC	מ-	מאפשרת בדיקה מרחוק של נקודות קצה ב-Windows (עבור נקודות קצה שבהן פועל Windows 7 וישן יותר).
445/TCP			מאפשרת בדיקה מרחוק של נקודות קצה ב-Windows.
161/UDP	SNMP	מ-	מאפשרת לפלטפורמת Forescout לתקשר עם מתגי ונתבי רשת. למידע על הגדרת SNMP, עיין ב*מדריך הניהול של Forescout*.

יציאה	שירות	אל פלטפורמת Forescout או ממנה	פונקציה
162/UDP	SNMP	אל	מאפשרת לפלטפורמת Forescout לקבל מלכודות SNMP ממתגים ומנתבים של הרשת. למידע על הגדרת SNMP, עיין ב*מדריך הניהול של Forescout*.
389/TCP (636(	LDAP	מ-	מאפשרת לפלטפורמת Forescout לתקשר עם Active Directory. מאפשרת תקשורת עם פורטלים אינטרנטיים של פלטפורמת Forescout.
443/TCP	HTTPS	אל	מאפשרת ניתוב מחדש ב-HTTP באמצעות TLS.
2200/TCP	SecureConnector ל-Linux	אל	מאפשרת ל-SecureConnector ליצור חיבור מאובטח (SSH מוצפן) עם המכשיר ממחשבי Linux. *SecureConnector* הוא סוכן מבוסס Script, המאפשר ניהול של נקודות קצה ב-Linux כאשר הן מחוברות אל הרשת.
10003/TCP	SecureConnector ל-Windows	אל	מאפשרת ל-SecureConnector ליצור חיבור מאובטח (TLS מוצפן) עם המכשיר ממחשבי Windows. *SecureConnector* הוא סוכן המאפשר ניהול של נקודות קצה ב-Windows כאשר הן מחוברות אל הרשת. למידע נוסף על SecureConnector, עיין ב*מדריך הניהול של Forescout*. כאשר SecureConnector מתחבר למכשיר או ל-Enterprise Manager, הוא מנותב מחדש אל המכשיר שאליו הוקצה המארח שלו. יש לוודא שיציאה זו פתוחה לכל המכשירים ול-Enterprise Manager, על מנת לאפשר ניידות שקופה בתוך הארגון.
10005/TCP	SecureConnector עבור OS X	אל	מאפשרת ל-SecureConnector ליצור חיבור מאובטח (TLS מוצפן) עם המכשיר ממחשבי OS X. *SecureConnector* הוא סוכן המאפשר ניהול של נקודות קצה ב-OS X כאשר הן מחוברות אל הרשת. למידע נוסף על SecureConnector, עיין ב*מדריך הניהול של Forescout*. כאשר SecureConnector מתחבר למכשיר או ל-Enterprise Manager, הוא מנותב מחדש אל המכשיר שאליו הוקצה המארח שלו. יש לוודא שיציאה זו פתוחה לכל המכשירים ול-Enterprise Manager, על מנת לאפשר ניידות שקופה בתוך הארגון.
13000/TCP	פלטפורמת Forescout	מ-/אל	בפריסות עם מכשיר אחד בלבד – מהמסוף אל המכשיר. בפריסות עם יותר ממכשיר אחד – מהמסוף אל המכשיר ומהמכשיר אל מכשיר אחר. התקשורת של המכשיר כוללת תקשורת עם Enterprise Manager ועם Recovery Enterprise Manager, באמצעות TLS.

ממשק ניטור

ממשק הניטור מאפשר למכשיר לנטר את התעבורה ברשת ולעקוב אחריה. ניתן להשתמש בכל ממשק זמין כממשק הניטור.

התעבורה תשתקף ביציאה שעל המתג, והמכשיר ינטר אותה. השימוש בתיוג 802.1Q VLAN תלוי במספר ה-VLAN לשיקוף.

- ***VLAN יחיד***: לניטור תעבורה שמגיעה מ-VLAN יחיד, התעבורה לשיקוף לא צריכה לקבל תיוג VLAN.
- ***VLANs מרובים***: בניטור תעבורה שמגיעה משני מכשירי VLAN או יותר, יש להגדיר תיוג 802.1Q VLAN עבור התעבורה לשיקוף.

כאשר שני מתגים מחוברים כצמד עודף, על המכשיר לנטר תעבורה משני המתגים.

אין צורך בכתובת IP בממשק הניטור.

ממשק תגובה

המכשיר מגיב לתעבורה באמצעות ממשק התגובה. תעבורת התגובה משמשת להגנה מפני פעילות זדונית ולביצוע פעולות מדיניות. לדוגמה, פעולות אלה עשויות לכלול ניתוב מחדש של דפדפני אינטרנט או ביצוע של חסימת הפעלה. תצורת יציאת הרשת הקשורה תלויה בניטור התעבורה.

ניתן להשתמש בכל ממשק זמין כממשק התגובה.

- ***VLAN יחיד***: לניטור תעבורה שמגיעה מ-VLAN יחיד, יציאת התגובה חייבת להשתייך לאותו ה-VLAN. במקרה כזה, למכשיר נחוצה כתובת IP יחידה ב-VLAN זה.
- ***VLANs מרובים***: בניטור תעבורה שמגיעה משני מכשירי VLAN או יותר, יש להגדיר גם ביציאת התגובה תיוג 802.1Q VLAN עבור אותם VLAN. למכשיר נחוצה כתובת IP עבור כל VLAN מנוטר.

2. הגדרת המתג

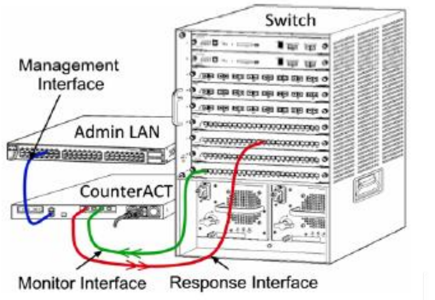
א. אפשרויות חיבור המתג

המכשיר מיועד לשילוב חלק עם מגוון רחב של סביבות רשת. כדי לשלב בהצלחה את המכשיר ברשת שלך, ודא שהמתג הותקן כך שינטר את התעבורה הדרושה.

יש כמה אפשרויות לחיבור המכשיר אל המתג.

1 פריסה סטנדרטית (ממשקים נפרדים לניהול, לניטור ולתגובה)

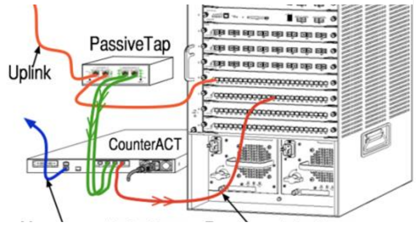
הפריסה המומלצת משתמשת בשלוש יציאות נפרדות. יציאות אלה מתוארות תחת חיבורי ממשק של המכשיר.



2 חיבור מוטבע פאסיבי

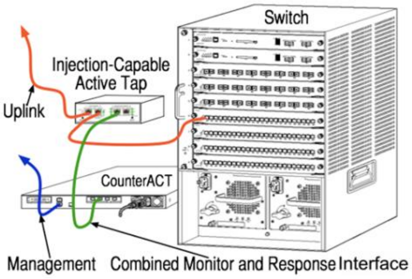
במקום להתחבר ליציאת ניטור המתג, המכשיר יכול להשתמש בחיבור מוטבע פאסיבי.

לחיבור מוטבע פאסיבי דרושות שתי יציאות ניטור (אחת לתעבורה במעלה הזרם ואחת לתעבורה במורד הזרם), אלא אם מדובר בחיבור *רקומבינציה*, המשלב את שני הזרמים הדו-סטריים ליציאה אחת. שים לב: אם לתעבורה המחוברת יש תיוג 802.1Q VLAN, נדרש תיוג 802.1Q VLAN גם ביציאת התגובה.



3 חיבור מוטבע אקטיבי (תומך הזרקה)

המכשיר מסוגל להשתמש בחיבור מוטבע אקטיבי. אם החיבור תומך בהזרקה, המכשיר משלב את יציאות הניטור והתגובה, ולכן אין צורך בהגדרת יציאת תגובה נפרדת במתג. ניתן להשתמש באפשרות זו ללא תלות בסוג תצורת המתגים במעלה או במורד הזרם.



4 תגובה בשכבת IP (בהתקנות מתג שכבה 3)

המכשיר מסוגל להגיב לתעבורה באמצעות ממשק ניהול משלו. למרות שניתן להשתמש באפשרות זו עם כל תעבורה לניטור, מומלץ להשתמש בה רק במצבים שבהם המכשיר מנטר יציאות שלא מהוות חלק משום VLAN, ולכן אינו מסוגל להגיב לתעבורה המנוטרת באמצעות אף יציאת מתג אחרת. זהו המצב האופייני במקרה של ניטור קישור המחבר בין שני נתבים. באפשרות זו, לא ניתן להגיב לבקשות Address Resolution Protocol (ARP), דבר המגביל את יכולתו של המכשיר לזהות סריקות המיועדות לכתובות ה-IP הכלולות ברשת המשנה המנוטרת. מגבלה זו אינה חלה על ניטור של תעבורה בין שני נתבים.

ב. הערות לגבי הגדרת מתגים

תגי VLAN (802.1Q)

- ***ניטור VLAN יחיד***: בניטור תעבורה שמגיעה מ-VLAN יחיד, אין צורך בתגי VLAN 802.1Q של התעבורה.
- ***ניטור VLANs מרובים***: בניטור תעבורה שמגיעה משני VLAN או יותר, יש להגדיר תיוג 802.1Q VLAN כזמין ביציאות הניטור *וגם* ביציאות התגובה. מומלץ לנטר VLAN מרובים, משום שכך מתקבל כיסוי מיטבי כללי, תוך צמצום של מספר יציאות השיקוף.
- אם המתג לא מסוגל להשתמש בתג 802.1Q VLAN ביציאת השיקוף, בצע אחת מהפעולות הבאות:
  - בצע שיקוף של VLAN אחד בלבד
  - בצע שיקוף של יציאה בלתי-מתויגת של ערוץ שידור יוצא
  - השתמש באפשרות לתגובה בשכבת IP
- אם המתג מסוגל לשקף יציאה אחת בלבד, בצע שיקוף של יציאה יחידה של ערוץ שידור יוצא. ייתכן שיהיו תיוגים. באופן כללי, אם המתג מסיר תגי 802.1Q VLAN, יש להשתמש באפשרות התגובה בשכבת IP.

הנחיות נוספות

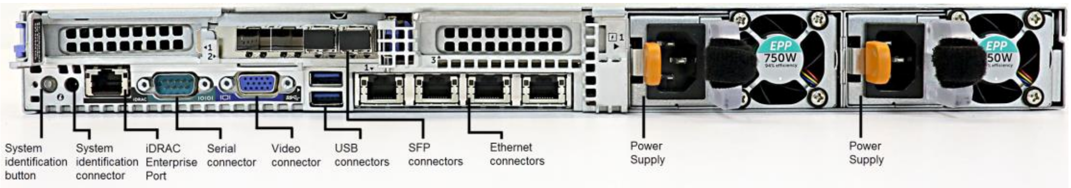
- במקרים הבאים יש לשקף ממשק אחד בלבד (שמאפשר שידור/קליטה):
  - אם המתג לא מסוגל לשקף גם תעבורה משודרת וגם נקלטת
  - אם המתג לא מסוגל לשקף את כל התעבורה במתג
  - אם המתג לא מסוגל לשקף את כל התעבורה דרך VLAN
- יש להימנע מעומס יתר ביציאה לשיקוף.
- במתגים מסוימים (למשל Cisco 6509), ייתכן שיהיה צורך במחיקה מלאה של תצורת היציאה הנוכחית לפני הזנה של תצורה חדשה. במקרים רבים, אי מחיקה של מידע יציאה ישן תגרום למתג להסיר תגי 802.1Q.

3. חיבור כבלי רשת והפעלה

א. הוצאת המכשיר מהאריזה וחיבור הכבלים

1. הוצא את המכשיר וכבל החשמל מאריזת המשלוח
2. הוצא את ערכת המסילה שמצורפת למכשיר.
3. הרכב את ערכת המסילה על המכשיר, והתקן את המכשיר על מערכת המדפים.
4. חבר את כבלי הרשת בין ממשקי הרשת בלוח האחורי של המכשיר לבין יציאות המתג.

לוח אחורי לדוגמה - מכשיר Forescout



באפשרותך להחליף את ה-SFP שסופקו על-ידי Forescout ב-SFP מבית Finisar, אשר נבדקו ואושרו על-ידי Forescout. לפרטים נוספים, עיין ב*מדריך ההתקנה של Forescout*.

ב. תיעוד הקצאות ממשק

בסיום התקנת המכשיר במרכז הנתונים והתקנת מסוף Forescout, תתבקש לרשום את הקצאות הממשק. הקצאות אלה, הנקראות *הגדרות ערוצים*, יוזנו ב'אשף ההתקנה הראשונית' אשר ייפתח בכניסה הראשונה למסוף.

תעד להלן את הקצאות הממשק הפיזיות, והשתמש בהן בעת השלמת התקנת הערוץ מהמסוף.

ממשק Eth	הקצאת ממשקים (כגון ניהול, ניטור, תגובה)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	

ג. הפעלת המכשיר

1. חבר את כבל החשמל למחבר החשמל בלוח האחורי של המכשיר.
2. חבר את הקצה השני של כבל החשמל לשקע חשמל מוארק.
3. חבר את המקלדת והצג למכשיר, או הכן את המכשיר לחיבור טורי. לפרטים נוספים, עיין ב*מדריך ההתקנה של Forescout*.
4. הפעל את המכשיר מהלוח הקדמי.

4. קביעת תצורה של המכשיר

הכן את המידע הבא לפני קביעת התצורה של המכשיר.

שם מחשב מארח של המכשיר	
סיסמת מנהל מערכת של Forescout	שמור את הסיסמה במיקום מאובטח
ממשק ניהול	
כתובת IP של המכשיר	
מסיכת רשת	
כתובת IP של שער ברירת מחדל	
שם דומיין ב-DNS	
כתובת שרת DNS	

לאחר ההפעלה, ההודעה הבאה תבקש ממך להתחיל בהגדרה:

ההודעות הבאות מבוססות על גרסה 8.0. חלק מהמכשירים עשויים להגיע כשהם מותקנים מראש עם גרסה מאוחרת יותר הכוללת הודעות מעט שונות.

```
CounterACT Appliance boot is complete.
Press <Enter> to continue.
```

1. הקש **Enter**. אם ברשותך מכשיר Forescout 51xx, יופיע התפריט הבא:

```
CounterACT 8.0.0-<build> options:
        Configure CounterACT  (1
Restore saved CounterACT configuration  (2
Identify and renumber network interfaces  (3
        Configure keyboard layout  (4
              Turn machine off  (5
           Reboot the machine  (6

                  Choice (1-6)  :1
```

אם יש ברשותך מכשיר CT-xxxx, תופיע בראש התפריט הגרסה CounterACT 7.0.0 או CounterACT 8.0.0.

– אם מופיעה הגרסה CounterACT 7.0.0, תוכל לשדרג או לבצע התקנה נקייה של גרסה 8.0.0. לפרטים, עיין במדריך *ההתקנה של Forescout*. לאחר השדרוג או ההתקנה לגרסת 8.0.0, יופיע התפריט המוצג לעיל.

– אם מופיעה הגרסה CounterACT 8.0.0, התפריט מציע אפשרות להתקין את 7.0.0 או לקבוע את התצורה של 8.0.0, כמוצג להלן. אם תבחר ב-7.0.0, לא תוכל להתקין מחדש את 8.0.0 באמצעות תפריט קביעת התצורה. לפרטים על קביעת התצורה של גרסה 7.0.0, עיין במדריך *ההתקנה של Forescout גרסה 7.0.0*.

```
CounterACT 8.0.0-<build> options:
 <Install CounterACT 7.0.0-<build (1
 <Configure CounterACT 8.0.0-<build (2
 Restore saved CounterACT configuration (3
 Identify and renumber network interfaces (4
 Configure keyboard layout (5
 Turn machine off (6
 Reboot the machine (7

 : (1-7) Choice
```

אם קביעת התצורה הופסקה באמצע, או אם בחרת בגרסה לא נכונה, עליך לבצע הדמיה מחדש של המכשיר עם הגרסה הרלוונטית של קובץ ה-ISO. למידע נוסף על הדמיה מחדש של מכשיר, עיין במדריך ההתקנה של Forescout.

2. בחר **Configure CounterACT** (קביעת תצורה של CounterACT). כשתופיע ההנחיה:

?להמשיך? (כן/לא)

הקש **Enter** כדי להתחיל בהתקנה.

3. תיפתח הנחיה של High Availability Mode (מצב זמינות גבוהה). הקש **Enter** כדי לבחור בהתקנה סטנדרטית.

4. תופיע הנחיית ההגדרה הראשונית של CounterACT. הקש **Enter** כדי להמשיך.

5. תיפתח ההנחיה Select CounterACT Installation Type (בחירת סוג התקנה של CounterACT). הקלד **1** והקש **Enter** כדי להתקין מכשיר CounterACT סטנדרטי.

ההגדרה תתחיל. התהליך עשוי להימשך מספר רגעים.

6. תיפתח הנחיה Select Licensing Mode (בחירת מצב רישוי). בחר את מצב הרישוי שבו משתמשת הפריסה. מצב הרישוי נקבע בעת הרכישה. ***אל תקליד ערך אם טרם בירורת באיזה מצב רישוי משתמשת הפריסה.*** כדי לוודא את מצב הרישוי שלך, או אם הזנת מצב לא נכון, צור קשר עם נציג מכירות של Forescout.

7. בהנחיה להזנת תיאור מחשב, הזן טקסט קצר המתאר את המכשיר, והקש **Enter.**

יופיע:

```
>>>>>> Set Administrator Password <<<<<<
This password will be used to log in as 'cliadmin' to the
machine Operating System and as ’admin’ to the CounterACT
 Console.
The password must be between 6 and 15 characters long and should
 contain at least one non-alphabetic character.
 Administrator password :
```

8. בהנחיה Set Administrator Password (הגדרת סיסמה של מנהל מערכת), הקלד את המחרוזת שבו תרצה להשתמש כסיסמה (המחרוזת לא תוצג במסך), והקש **Enter.** תתבקש לאשר את הסיסמה. נדרשת סיסמה באורך 6-15 תווים, המכילה תו אחד לפחות שאינו אלפביתי.

היכנס למכשיר כ-cliadmin, והיכנס למסוף כ-admin (מנהל מערכת).

9. בהנחיה Set Host Name (הגדרת שם מחשב מארח), הקלד שם מחשב מארח, והקש **Enter.** ניתן להשתמש בשם המחשב המערכת בעת הכניסה למסוף, והוא מופיע במסוף כדי לעזור לך לדעת איזה מכשיר CounterACT מוצג כעת. שם המחשב המארח לא יעלה על 13 תווים.

10. המסך Configure Network Settings (קביעת הגדרות רשת) יבקש ממך סדרה של פרמטרי תצורה. הקלד ערך בכל הנחיה, והקש **Enter** כדי להציג את ההנחיה הבאה.

- הרכיבים של פלטפורמת Forescout מתקשרים דרך ממשקי ניהול. מספר ממשקי הניהול שיופיעו תלוי בדגם המכשיר.
- **כתובת ה-IP לניהול** היא כתובתו של הממשק שדרכו מתקשרים הרכיבים של פלטפורמת Forescout. הוסף VLAN ID (מזהה VLAN) עבור ממשק זה רק אם הממשק המשמש לתקשורת בין רכיבי פלטפורמת Forescout מחובר ליציאה מתויגת.
- אם קיימת יותר מאשר **כתובת שרת DNS** אחת, הפרד בין הכתובות באמצעות תווי רווח. רוב שרתי ה-DNS הפנימיים מפענחים כתובות חיצוניות ופנימיות, אך ייתכן שתצטרך לכלול שרת חיצוני לפענוח של DNS. מאחר שכמעט כל שאילתות ה-DNS שהמכשיר יבצע הן עבור כתובות פנימיות, יש לציין את שרת ה-DNS החיצוני אחרון ברשימה.

11. יופיע המסך Setup Summary (סיכום הגדרה). תתבקש לבצע בדיקות קישוריות כלליות, לקבוע מחדש הגדרות או להשלים את ההגדרה. הקלד **D** כדי להשלים את ההגדרה.

רישיון

לאחר קביעת התצורה, ודא שלמכשיר שלך יש רישיון תקף. מצב רישוי ברירת המחדל במכשיר שברשותך תלוי במצב הרישוי שבו משתמשת הפריסה.

- אם הפריסה של Forescout פועלת ב***מצב רישוי לפי מכשיר***, תוכל כעת להתחיל ולעבוד עם רישיון ההדגמה, התקף למשך 30 יום. בפרק זמן זה, עליך לקבל רישיון קבוע מ-Forescout ולהציב אותו בתיקייה נגישה בדיסק או ברשת שלך. התקן את הרישיון ממיקום זה לפני תום רישיון ההדגמה של 30 יום (אם צריך, תוכל לבקש להאריך את רישיון ההדגמה).

  זמן קצר לפני תפוגת רישיון ההדגמה, תקבל התראות על כך בכמה דרכים שונות. למידע נוסף על התראות לגבי רישיון ההדגמה, עיין ב*מדריך הניהול של Forescout*.

  אם אתה עובד במערכת וירטואלית של Forescout:

  - רישיון ההדגמה אינו מותקן בשלב זה באופן אוטומטי. עליך להתקין את רישיון ההדגמה שקיבלת מנציג Forescout בדואר אלקטרוני.
  - יש להעניק גישה לאינטרנט למכשיר CounterACT אחד לפחות. חיבור זה משמש לאימות של רישיונות Forescout כנגד שרת הרישיונות של Forescout. אם לא ניתן לאמת רישיון מסוים למשך חודש אחד, הרישיון יבוטל. אחת ליום, פלטפורמת Forescout תשלח בדואר אלקטרוני אזהרה על שגיאת תקשורת בשרת.

    לפרטים נוספים, עיין ב*מדריך ההתקנה של Forescout*.

    למידע נוסף על ניהול רישיונות במצב רישוי לפי מכשיר, עיין ב*מדריך הניהול של Forescout*.

- אם הפריסה של Forescout פועלת ב***מצב רישוי Flexx***, *מנהל הזכאות* אמור לקבל בדואר אלקטרוני הודעה לאחר שהזכאות לרישיון נוצרה והפכה לזמינה בפורטל הלקוחות של Forescout. לאחר שהזכאות הופכת זמינה, *מנהל הפריסה* יוכל להפעיל את הרישיון במסוף. עד להפעלת הרישיון, תופעל אכיפת רישיון, ושינויים מסוימים בתצורת המסוף עשויים להיות מוגבלים. *בהתקנת המערכת, מותקן באופן אוטומטי רישיון מלא.*

  לפרטים נוספים, עיין ב*מדריך ההפעלה של Forescout Flexx*.

5. ניהול מרחוק

הגדרת iDRAC

Integrated Dell Remote Access Controller (iDRAC) הוא פתרון משולב למערכת שרתים, המעניק לך גישה מרחוק אל מכשירי CounterACT, שאינה תלויה במיקום או במערכת ההפעלה, דרך ה-LAN או האינטרנט. השתמש במודול זה לצורך גישת KVM, להפעלה/כיבוי/איפוס וכדי לבצע משימות של פתרון בעיות ותחזוקה.

כדי לעבוד עם מודול iDRAC, בצע את הפעולות הבאות:

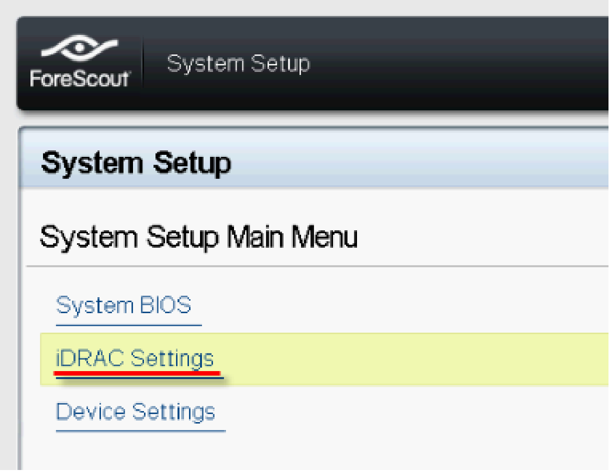
- הפעלה וקביעת תצורה של מודול iDRAC
- חיבור המודול לרשת
- כניסה ל-iDRAC

הפעלה וקביעת תצורה של מודול iDRAC

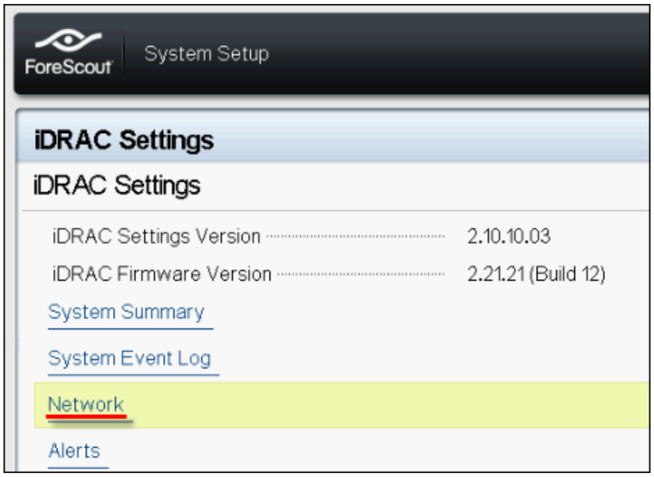
שנה את הגדרות iDRAC כדי לאפשר גישה מרחוק במכשיר CounterACT. סעיף זה מתאר הגדרות שילוב בסיסיות הנחוצות לעבודה עם פלטפורמת Forescout.

כדי לקבוע את התצורה של iDRAC:

1. הפעל את המכשיר המנוהל.
2. בעת האתחול, הקש F2.
3. בדף התפריט הראשי של התקנת המערכת, בחר **iDRAC Settings** (הגדרות iDRAC).



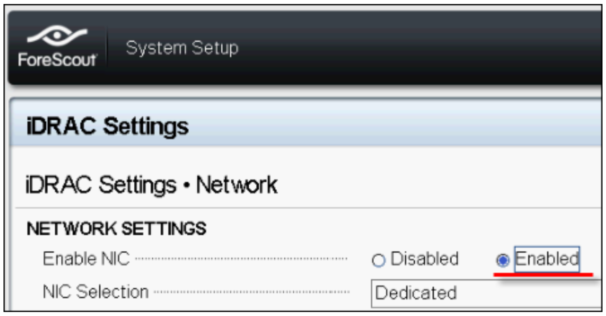
4. בדף הגדרות iDRAC , בחר **Network** (רשת).



iDRAC Settings Version 2.10.10.03
iDRAC Firmware Version 2.21.21 (Build 12)

5. קבע את הגדרות הרשת הבאות:

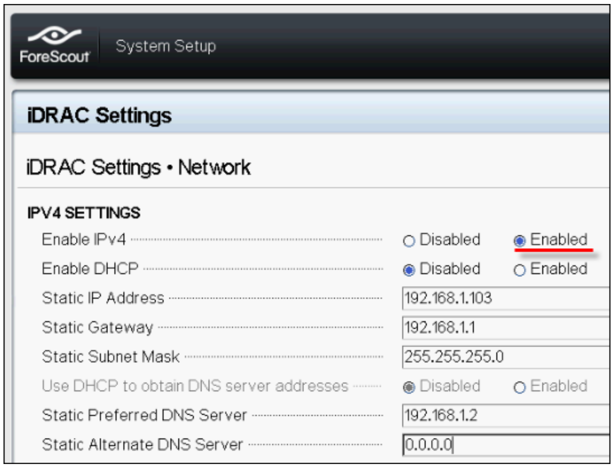
   - ***הגדרות רשת***. ודא שהשדה **Enable NIC** (זמינות NIC) מוגדר כ-**Enabled** (מאופשר).



Enable NIC ○ Disabled ● Enabled
NIC Selection Dedicated

   - ***הגדרות משתמש***. בשדה DNS DRAC Name (שם DNS DRAC), ניתן לעדכן DNS דינמי (אופציונלי).
   - ***הגדרות IPV4***. ודא שהשדה **Enable IPv4** (אפשר IPv4) מוגדר כ-**Enabled** (מאופשר).

   הגדר את השדה **Enable DHCP** (זמינות DHCP) כ-**Enabled** (מאופשר) כדי להשתמש במיעון IP דינמי, או כ-**Disabled** (מושבת) כדי להשתמש במיעון IP סטטי. אם זמין, DHCP יקצה באופן אוטומטי את כתובת ה-IP, השער ומסיכת רשת המשנה ל-iDRAC. אם לא זמין, הזן ערכים עבור השדות **Static IP Address** (כתובת IP סטטית), **Static Gateway** (שער סטטי) ו-**Static Subnet Mask** (מסיכת רשת משנה).



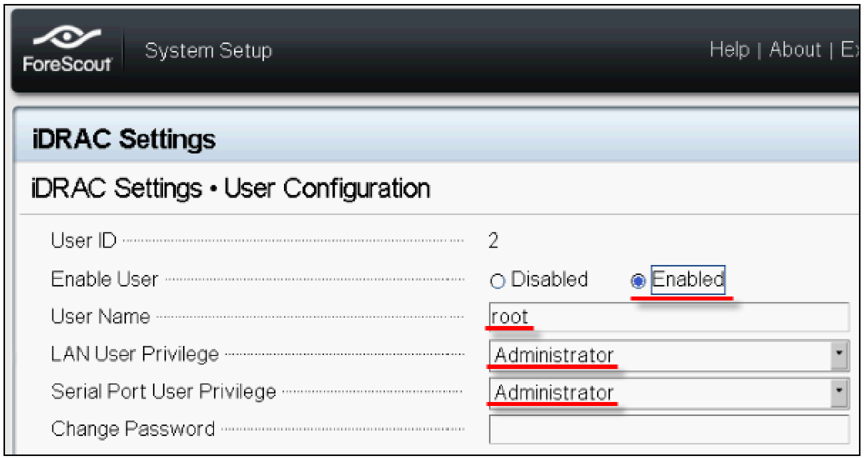
Enable IPv4 ○ Disabled ● Enabled
Enable DHCP ● Disabled ○ Enabled
Static IP Address 192.168.1.103
Static Gateway 192.168.1.1
Static Subnet Mask 255.255.255.0
Use DHCP to obtain DNS server addresses ● Disabled ○ Enabled
Static Preferred DNS Server 192.168.1.2
Static Alternate DNS Server 0.0.0.0

6. בחר **Back** (חזרה).

7. בחר **User Configuration** (תצורת משתמש).
8. הגדר עבור משתמש ' root'(שורש) את השדות הבאים של User Configuration (תצורת משתמש):
   - ***Enable User*** (אפשר משתמש). ודא ששדה זה מוגדר כ-Enabled (מאופשר).

     שם המשתמש המוגדר כאן אינו זהה לשם המשתמש של Forescout.

   - ***LAN and Serial Port User Privileges*** (הרשאות משתמש ב-LAN וביציאה טורית). הגדר רמות הרשאה כ-Administrator (מנהל מערכת).
   - ***Change Password*** (החלף סיסמה). הגדר סיסמה לכניסת המשתמש.



iDRAC Settings

iDRAC Settings • User Configuration

User ID: 2
Enable User: ○ Disabled ● Enabled
User Name: root
LAN User Privilege: Administrator
Serial Port User Privilege: Administrator
Change Password:

9. בחר **Back** (חזרה) ולאחר מכן בחר **Finish** (סיום). אשר את השינוי בהגדרות.

   ההגדרות שקבעת יישמרו, והמערכת תאותחל מחדש.

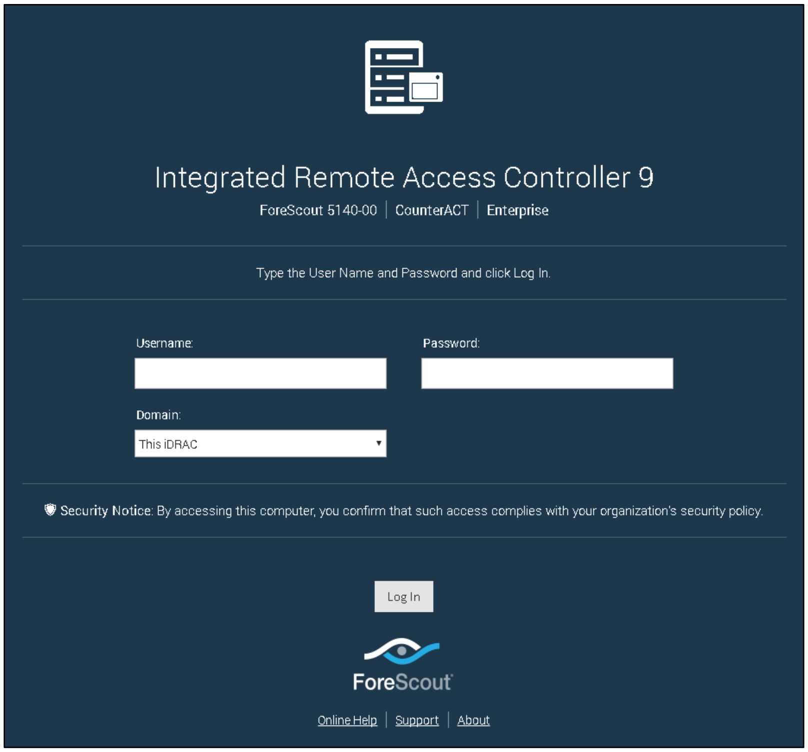
חיבור המודול לרשת

iDRAC מתחבר לרשת Ethernet. נהוג לחבר אותו לרשת ניהול. התמונה הבאה מראה את המיקום של יציאת iDRAC בלוח האחורי של מכשיר CT-1000:

כניסה ל-iDRAC

כדי להיכנס ל-iDRAC:

1. נווט אל כתובת ה-IP או שם הדומיין שהוגדרו תחת **iDRAC Settings** (הגדרות iDRAC) < **Network** (רשת).


Integrated Remote Access Controller 9

ForeScout 5140-00 | CounterACT | Enterprise

Type the User Name and Password and click Log In.

Username:

Password:

Domain: This iDRAC

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

2. הזן את שם המשתמש והסיסמה שהוגדרו בדף תצורת המשתמש בהתקנת מערכת iDRAC.
3. בחר **Submit** (שלח).

למידע נוסף על iDRAC, עיין *במדריך למשתמש ב- iDRAC*. ניתן לגשת למדריך זה מהמיקום הבא:
https://forescout.com/company/resources/idrac-9-user-guide/

על מנת לזהות את מצב הרישוי שלך:

- מהמסוף, בחר **Help > About Forescout** (עזרה < אודות Forescout).

חשוב מאוד לעדכן את סיסמת ברירת המחדל לroot (שורש), אם טרם עשית זאת.

6. אימות הקישוריות

אימות החיבור לממשק הניהול

כדי לבדוק את חיבור ממשק הניהול, היכנס למכשיר, והפעל את הפקודה הבאה:

```
fstool linktest
```

יופיע המידע הבא:

```
Management Interface status
Pinging default gateway information
Ping statistics
Performing Name Resolution Test
Test summary
```

ביצוע בדיקת איתות (ping)

כדי לוודא קישוריות, הרץ את הפקודה הבאה מהמכשיר במחשב המחובר לרשת:

```
Ping <network_desktop_IP_address>
```

7. הגדר את מסוף CounterACT

התקן את המסוף

המסוף הוא יישום הניהול של Forescout, המשמש להצגת מידע מפורט חשוב על נקודות הקצה ולשליטה בהן. מכשירי CounterACT אוספים מידע זה. למידע נוסף, עיין ב*מדריך הניהול של Forescout*.

עליך לספק מחשב שיארח את תוכנת היישום של מסוף Forescout. דרישות המינימום לחומרה:

- מחשב לא-ייעודי, עם:
  - Windows 7/8/8.1/10
  - Windows Server 2008/2008 R2/2012/2012 R2/2016
  - Linux RHEL/CentOS 7
- 2GB RAM
- 1GB שטח דיסק

ניתן להתקין את המסוף בשיטה הבאה:

השתמש בתוכנת ההתקנה הכלולה במכשיר.

1. פתח חלון דפדפן ממחשב המסוף.
2. בשורת הכתובת בדפדפן, הקלד:

   `http://<Appliance_ip>/install`

   כאשר Appliance_ip היא כתובת ה-IP של מכשיר זה. חלון ההתקנה של המסוף יופיע בדפדפן.
3. פעל בהתאם להוראות המוצגות במסך.

כניסה

בסיום ההתקנה, תוכל להיכנס למסוף.

1. בחר בסמל של Forescout ממיקום קיצור הדרך שיצרת.

IP/Name:

Login Method: Password

User Name:

Password:

☑ Remember this address and user name

2. הזן את כתובת ה-IP או שם המחשב המארח של המכשיר בשדה **IP/Name** (IP/שם).
3. בשדה **User Name** (שם משתמש), הזן admin.
4. בשדה **Password** (סיסמה), הזן את הסיסמה שיצרת במהלך התקנת המכשיר.
5. בחר **Login** (כניסה) כדי להפעיל את המסוף.

ביצוע הגדרה ראשונית

כשתיכנס למערכת בפעם הראשונה, ייפתח אשף ההגדרה הראשונית. האשף ינחה אותך בשלבי קביעת התצורה החיוניים, להקמה מהירה ויעילה של פלטפורמת Forescout.

לפני שתתחיל בהגדרה הראשונית

לפני שתעבוד עם האשף, הכן את המידע הבא:

מידע הדרוש לאשף	ערך
כתובת שרת ה-NTP שבה משתמש הארגון (אופציונלי)	
כתובת IP פנימית של ממסר דואר, כדי לאפשר מסירה של התראות בדואר אלקטרוני אם אין הרשאה לתעבורת SMTP מהמכשיר (אופציונלי)	
כתובת דואר אלקטרוני נוכחית של מנהל המערכת של Forescout	
ממשקי ניטור ותגובה	
במקרה של מקטעים/VLAN ללא DHCP, מקטע הרשת/VLAN שאליהם ממשק התגובה מחובר ישירות, וכתובת IP קבועה שבה פלטפורמת Forescout תשתמש בכל VLAN	
טווח כתובות ה-IP שמכשיר זה ינטר (כל הכתובות הפנימיות, בכלל זה כתובות שאינן בשימוש)	
פרטי חשבון של משתמש LDAP וכתובת IP של שרת LDAP	
אישורי דומיין, בכלל זה שם וסיסמה של חשבון ניהול הדומיין	
שרתי אימות, כדי שפלטפורמת Forescout תוכל לנתח אילו מארחים ברשת אומתו בהצלחה	
כתובת IP של מתג, פרמטרים של הספק ו-SNMP	

למידע על עבודה עם האשף, עיין ב*מדריך הניהול של Forescout* או בעזרה המקוונת.

תיעוד נוסף של Forescout

למידע על תכונות ומודולים נוספים של Forescout, עיין במשאבים הבאים:

- תיעוד להורדה
- פורטל התיעוד
- כלי עזרה של Forescout

תיעוד להורדה

ניתן לגשת אל התיעוד להורדה דרך דף המשאבים של Forescout, או דרך אחד משני הפורטלים של Forescout, בהתאם למצב הרישוי שבו הפריסה שלך משתמשת.

- ***מצב רישוי לפי מכשיר*** – פורטל עדכוני מוצרים
- ***מצב רישוי Flexx*** – פורטל הלקוחות

ניתן גם להוריד תוכנות מפורטלים אלה.

על מנת לזהות את מצב הרישוי שלך:

- מהמסוף, בחר **Help > About Forescout** (עזרה > אודות Forescout).

דף המשאבים של Forescout

דף המשאבים של Forescout מספק קישורים לכל התיעוד הטכני.

על מנת לגשת לדף המשאבים של Forescout:

- עבור אל https://www.Forescout.com/company/resources, בחר **Technical Documentation** (תיעוד טכני) וחפש את המסמכים.

פורטל עדכוני מוצרים

פורטל עדכוני המוצרים מספק קישורים אל מהדורות גרסה של Forescout, מודולי בסיס ותוכן וכן מוצרי eyeExtend, כמו גם אל תיעוד רלוונטי. הפורטל מספק גם מגוון מסמכים נוספים.

כדי לגשת לפורטל עדכוני המוצרים:

- עבור אל https://updates.forescout.com/support/index.php?url=counteract ובחר בגרסה שברצונך לגלות.

פורטל הלקוחות

דף ההורדות בפורטל הלקוחות של Forescout מספק קישורים אל מהדורות גרסה של Forescout שנרכשו, מודולי בסיס ותוכן וכן מוצרי eyeExtend, כמו גם אל תיעוד רלוונטי. התוכנה והתיעוד הרלוונטי יופיעו בדף ההורדות רק אם אתה זכאי לרישיון עבור התוכנה.

כדי לגשת לתיעוד בפורטל הלקוחות של Forescout:

- עבור אל https://Forescout.force.com/support ובחר **Downloads** (הורדות).

פורטל התיעוד

פורטל התיעוד של Forescout הוא ספריית אינטרנט שאפשר לערוך בה חיפוש, והיא מכילה מידע על כלים, תכונות, פונקציונליות ושילובים של Forescout.

🗎 *אם הפריסה שלך משתמשת במצב רישוי Flexx, ייתכן שלא תקבל אישורי גישה אל פורטל זה.*

כדי לגשת לפורטל התיעוד:

- עבור אל https://updates.forescout.com/support/files/counteract/docs_portal והשתמש באישורי התמיכה ללקוח שלך.

כלי עזרה של Forescout

גש למידע ישירות מהמסוף.

לחצני עזרה של מסוף

השתמש בלחצני *Help* (עזרה) תלויי-הקשר כדי לגשת במהירות למידע על משימות ונושאים שעמם אתה עובד.

מדריך הניהול של Forescout

- בחר **Forescout Help** (עזרה של Forescout) מהתפריט **Help** (עזרה).

קובצי עזרה של תוספים

- לאחר התקנת התוסף, בחר **Tools** (כלים) > **Options** (אפשרויות) > **Modules** (מודולים), בחר את התוסף ולאחר מכן בחר **Help** (עזרה).

תיעוד מקוון

- בחר **Online Documentation** (תיעוד מקוון) מתפריט **Help** (עזרה) כדי לגשת אל דף המשאבים של Forescout (רישוי Flexx) או אל פורטל התיעוד (רישוי לפי מכשיר).