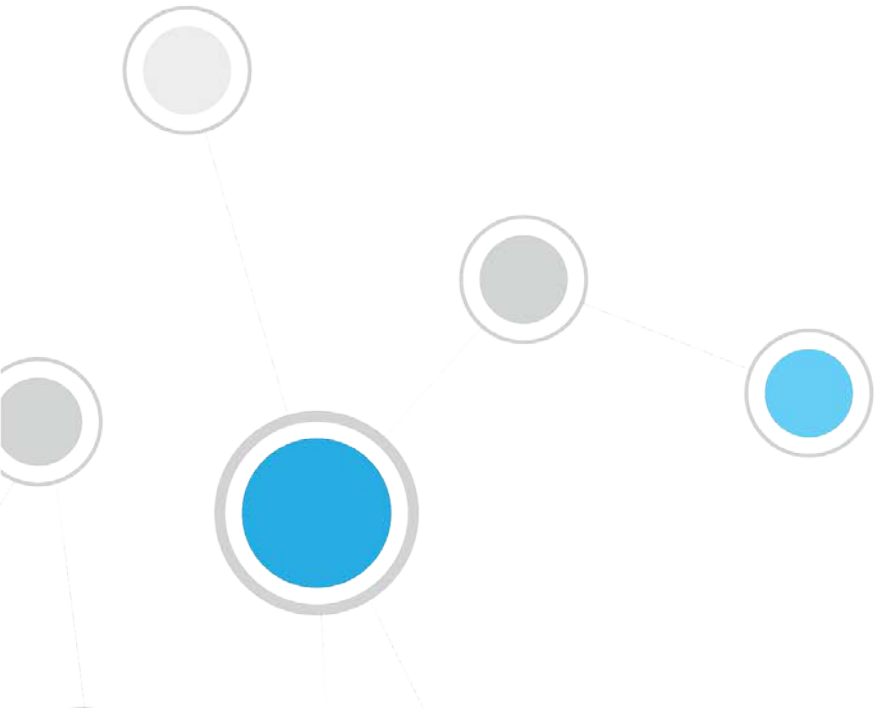
# ForeScout CounterACT®

## מכשיר CounterACT בודד

מדריך התקנה מהירה

**גרסה 8.0**



# תוכן העניינים

# ברוך הבא אל CounterACT גרסה 8.0

פלטפורמת CounterACT מספקת תשתית ונראות מכשירים, ניהול מדיניות, תיאום והתייעלות של זרימות עבודה, לחיזוק האבטחה ברשת. CounterACT מספק לארגונים מידע עם הקשר בזמן אמת על מכשירים ועל משתמשים ברשת. המדיניות מוגדרת ב-CounterACT 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.***

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

כמו כן, ניתן לנווט אל אתר התמיכה בכתובת: http://www.forescout.com/support לעיון בתיעוד עדכני, במאמרים ממאגר היעד ובעדכונים עבור המכשיר שברשותך.

## *תכולת חבילת* CounterACT

החבילה של CounterACT 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" (למכשירי 51xx בלבד)

# סקירה כללית

כדי להתקין את 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 הנה חיונית לפריסה מוצלחת ולביצועים מיטביים של CounterACT. 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 CounterACT*. כדי ללמוד כיצד לגשת אל מדריך זה, ראה תיעוד נוסף של CounterACT.

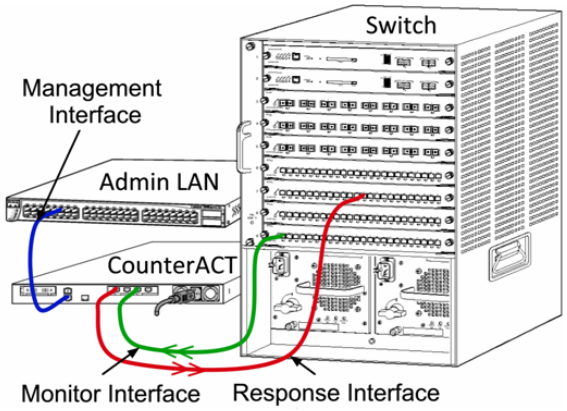
## חיבורי ממשק של המכשיר

באופן כללי, המכשיר מוגדר עם שלושה חיבורים למתג הרשת.

### ממשק ניהול

ממשק הניהול מאפשר לנהל את CounterACT 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 מסוף CounterACT. ליציאת הניהול נדרשת גישה אל שירותי רשת נוספים.




דרישות הגישה ברשת

| יציאה | שירות | אל או מ- CounterACT | פונקציה |
|---|---|---|---|
| TCP/22 | SSH | מ- | מאפשרת בדיקה מרחוק של נקודות קצה ב-OS X וב-Linux.<br>מאפשרת ל-CounterACT לתקשר עם מתגי ונתבי רשת. |

| יציאה | שירות | אל או מ-CounterACT | פונקציה |
|---|---|---|---|
| | | אל | מאפשרת גישה אל ממשק שורת הפקודה של CounterACT. |
| TCP/2222 | SSH | אל | (זמינות גבוהה) מאפשרת גישה למכשירים הפיזיים של CounterACT, המהווים חלק מצמד הזמינות הגבוהה.<br>השתמש ב-TCP/22 כדי לגשת לכתובת ה-IP המשותפת (הווירטואלית) של הצמד. |
| TCP/25 | SMTP | מ- | מאפשרת ל-CounterACT לגשת לממסר הדואר הארגוני. |
| UDP/53 | DNS | מ- | מאפשרת ל-CounterACT לפענח כתובות IP פנימיות. |
| TCP/80 | HTTP | אל | מאפשרת ניתוב מחדש ב-HTTP. |
| UDP/123 | NTP | מ- | מאפשרת ל-CounterACT לגשת אל שרת שעון מקומי או אל ntp.forescout.net.<br>כברירת מחדל, CounterACT ייגש אל ntp.foreScout.net |
| TCP/135 | MS-WMI | מ- | מאפשרת בדיקה מרחוק של נקודות קצה ב-Windows. |
| TCP/139 | SMB, MS-RPC | מ- | מאפשרת בדיקה מרחוק של נקודות קצה ב-Windows (עבור נקודות קצה שבהן פועל Windows 7 וישן יותר). |
| TCP/445 | | | מאפשרת בדיקה מרחוק של נקודות קצה ב-Windows. |
| UDP/161 | SNMP | מ- | מאפשרת ל-CounterACT לתקשר עם מתגי ונתבי רשת.<br>למידע על הגדרת SNMP, עיין ב*מדריך הניהול של CounterACT*. |
| UDP/162 | SNMP | אל | מאפשרת ל-CounterACT לקבל מלכודות SNMP ממתגים ומנתבים של הרשת.<br>למידע על הגדרת SNMP, עיין ב*מדריך הניהול של CounterACT*. |
| TCP/389<br>(636) | LDAP | מ- | מאפשרת ל-CounterACT לתקשר עם Active Directory.<br>מאפשרת תקשורת עם פורטלים אינטרנטיים של CounterACT. |
| TCP/443 | HTTPS | אל | מאפשרת ניתוב מחדש ב-HTTP באמצעות TLS. |
| TCP/2200 | 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. |

| יציאה | שירות | אל או מ-CounterACT | פונקציה |
|---|---|---|---|
| TCP/10003 | 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 CounterACT*.<br>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. |
| TCP/10005 | 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 CounterACT*.<br>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. |
| TCP/13000 | CounterACT | מ-/אל | בסביבות עם מכשיר אחד בלבד – מהמסוף אל המכשיר.<br>בסביבות עם שני מכשירי CounterACT או יותר – מהמסוף אל מכשיר CounterACT, וממכשיר CounterACT אחד למשנהו. התקשורת של מכשירי CounterACT 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 על 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.
- ***VLAN 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

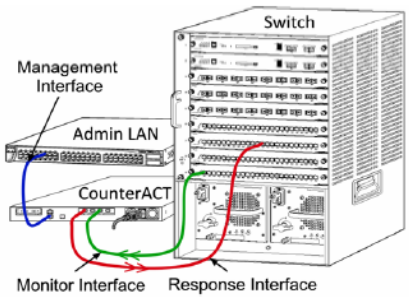
## א. אפשרויות חיבור המתג

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)

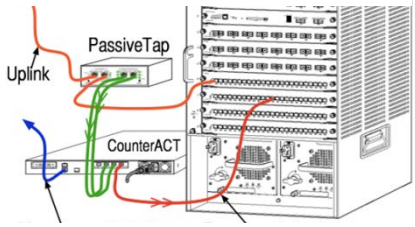
הפריסה המומלצת משתמשת בשלוש יציאות נפרדות. יציאות אלה מתוארות תחת חיבורי ממשק של המכשיר.




### 2 חיבור מוטבע פאסיבי

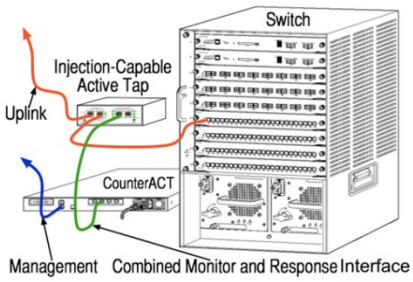
במקום להתחבר ליציאת ניטור המתג, המכשיר יכול להשתמש בחיבור מוטבע פאסיבי.

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 802.1Q VLAN 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

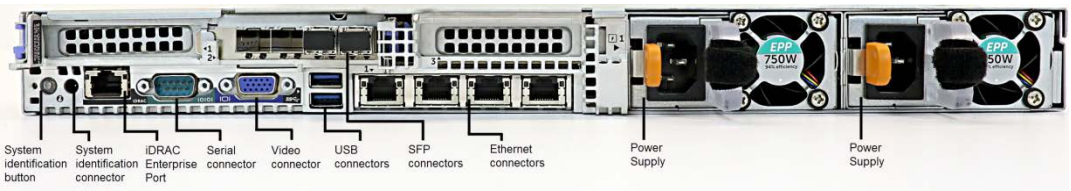
- במקרים הבאים יש לשקף ממשק אחד בלבד (שמאפשר שידור/קליטה):
  - אם המתג לא מסוגל לשקף גם תעבורה משודרת וגם נקלטת
  - אם המתג לא מסוגל לשקף את כל התעבורה במתג
  - אם המתג לא מסוגל לשקף את כל התעבורה דרך VLAN
- יש להימנע מעומס יתר ביציאה לשיקוף.
- במתגים מסוימים (למשל Cisco 6509), ייתכן שיהיה צורך במחיקה 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 CounterACT***




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 CounterACT*.

## ב. תיעוד הקצאות ממשק

בסיום התקנת המכשיר במרכז הנתונים והתקנת מסוף CounterACT, 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. למידע נוסף, עיין ב*מדריך ההתקנה של CounterACT*.
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 CounterACT | 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:

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

1. הקש **Enter**. אם ברשותך מכשיר CounterACT 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 CounterACT 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 ב*מדריך ההתקנה של CounterACT*. לאחר השדרוג או ההתקנה לגרסת 8.0.0, יופיע התפריט המוצג לעיל.
- אם מופיעה הגרסה CounterACT 8.0.0, התפריט מציע אפשרות להתקין את CounterACT 7.0.0 או לקבוע את התצורה של CounterACT 8.0.0, כמוצג להלן. אם תבחר ב-CounterACT 7.0.0, לא תוכל להתקין מחדש את CounterACT 8.0.0 באמצעות תפריט קביעת התצורה. לפרטים על קביעת התצורה של CounterACT 7.0.0, עיין ב*מדריך ההתקנה של CounterACT גרסה 7.0.0*.

```
CounterACT 8.0.0-<build> options:
```

```
                                    <build>-7.0.0Install CounterACT  (1
                                  <build>-8.0.0Configure CounterACT  (2
                                Restore saved CounterACT configuration (3
                              nterfacesIdentify and renumber network i (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 של CounterACT, עליך לבצע הדמייה מחדש של המכשיר עם הגרסה הרלוונטית של קובץ ה-ISO. למידע נוסף על הדמייה מחדש של מכשיר, עיין במדריך ההתקנה של CounterACT.*

**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 ביררת באיזה מצב רישוי משתמשת הפריסה***. כדי לוודא את מצב הרישוי שלך, או אם הזנת מצב לא נכון, צור קשר עם נציג 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 'root' 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-* root *(שורש), 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 CounterACT מתקשרים דרך ממשקי ניהול. מספר ממשקי הניהול שיופיעו תלוי בדגם המכשיר.
- **כתובת ה-IP לניהול** היא כתובתו של הממשק שדרכו מתקשרים הרכיבים של CounterACT. הוסף VLAN ID (מזהה VLAN) עבור ממשק זה רק אם הממשק המשמש לתקשורת בין רכיבי CounterACT 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 CounterACT יש רישיון תקף. מצב רישוי ברירת המחדל במכשיר CounterACT שברשותך תלוי במצב הרישוי שבו משתמשת הפריסה.

- אם הפריסה של CounterACT 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 CounterACT*.

  אם אתה עובד במערכת וירטואלית של CounterACT:

  - 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 CounterACT כנגד שרת הרישיונות של ForeScout. אם לא ניתן לאמת רישיון מסוים למשך חודש אחד, הרישיון יבוטל. אחת ליום, CounterACT ישלח בדואר אלקטרוני אזהרה על שגיאת תקשורת בשרת.

    למידע נוסף, עיין ב*מדריך ההתקנה של CounterACT*.

- אם הפריסה של CounterACT פועלת ב***מצב רישוי מרוכז***, *מנהל הזכאות* אמור לקבל בדואר אלקטרוני הודעה לאחר שהזכאות לרישיון נוצרה ונעשתה זמינה בפורטל הלקוחות של ForeScout. לאחר שהזכאות תיעשה זמינה, *מנהל המערכת של CounterACT* בפריסה זו יוכל להפעיל את הרישיון ממסוף CounterACT. התכונות של CounterACT יתפקדו כראוי רק לאחר הפעלת הרישיון. לדוגמה, כל עוד לא הופעל הרישיון, לא תתבצע הערכת מדיניות ולא יבוצעו פעולות. ב*התקנת המערכת, לא מותקן באופן אוטומטי רישיון הדגמה*.

למידע נוסף על ניהול רישיונות, עיין ב*מדריך הניהול של CounterACT*.

# 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:

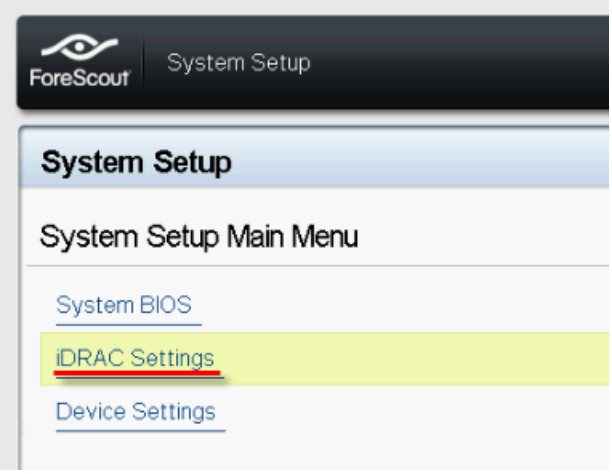
- הפעלה וקביעת תצורה של מודול iDRAC
- חיבור המודול לרשת
- כניסה ל-iDRAC

### הפעלה וקביעת תצורה של מודול iDRAC

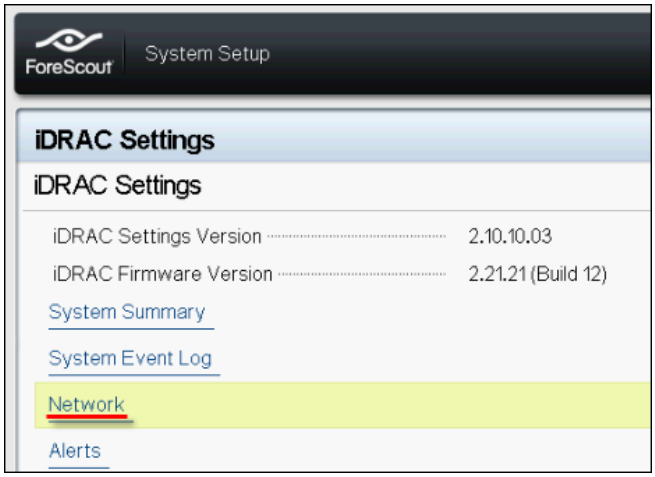
שנה את הגדרות iDRAC כדי לאפשר גישה מרחוק במכשיר CounterACT. סעיף זה מתאר הגדרות שילוב בסיסיות הנחוצות לעבודה עם CounterACT.

**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).

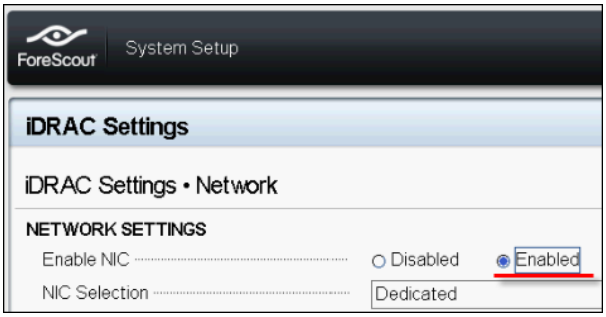



4. בדף הגדרות iDRAC , בחר **Network** (רשת).




**5.** קבע את הגדרות הרשת הבאות:

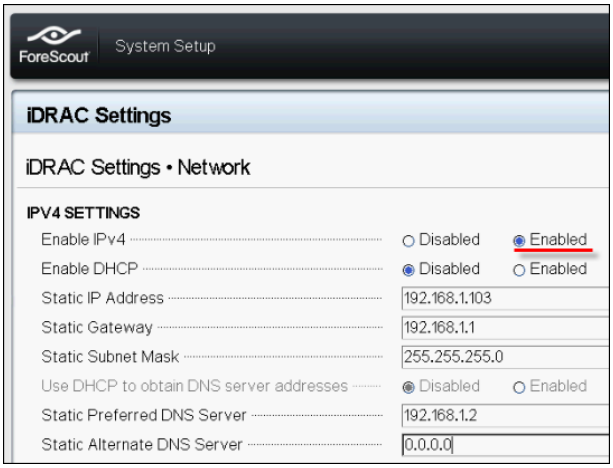
– ***הגדרות רשת***. ודא שהשדה **Enable NIC** (זמינות NIC) מוגדר כ-**Enabled** (מאופשר).




– ***הגדרות משותפות***. 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).

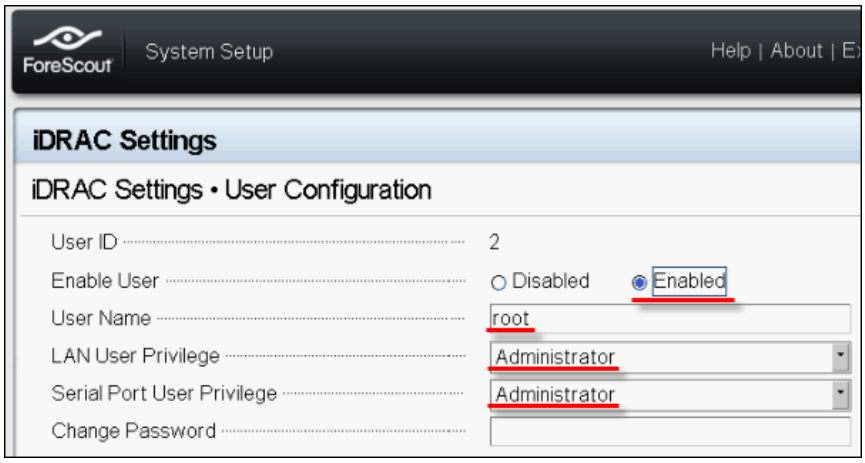



**6.** בחר **Back** (חזרה).

7. בחר **User Configuration** (תצורת משתמש).
8. הגדר עבור משתמש הבסיס 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 CounterACT.*

   - ***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.




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

ההגדרות שקבעת יישמרו, והמערכת תאותחל מחדש.

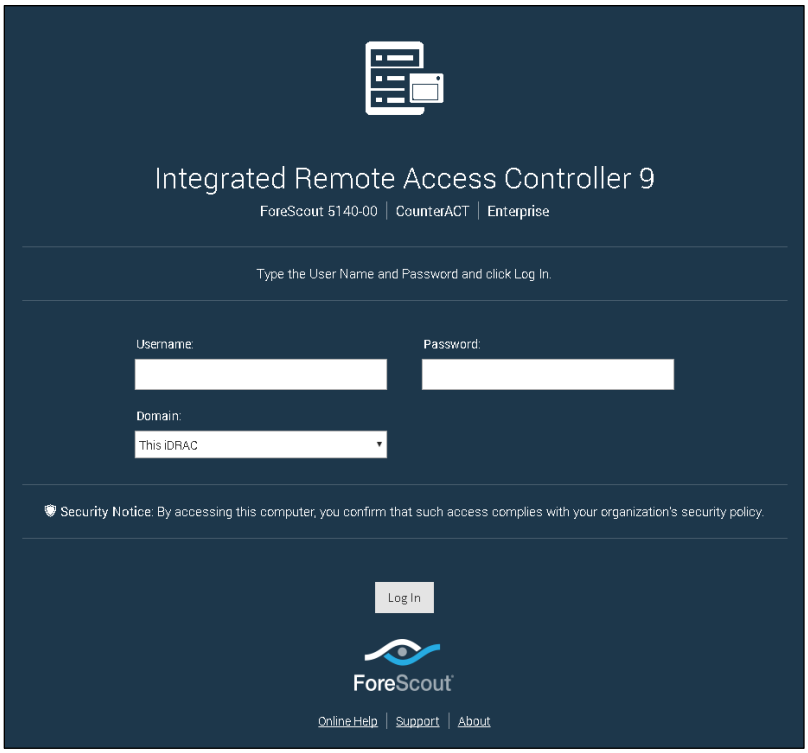
## חיבור המודול לרשת

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 התחום שהוגדרו תחת **iDRAC Settings** (הגדרות iDRAC > **Network** (רשת).




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

למידע נוסף על iDRAC, עיין ב*מדריך למשתמש ב- iDRAC*. ניתן לגשת למדריך זה מאחד המיקומים הבאים, בהתאם למצב הרישוי שבו הפריסה שלך משתמשת:

- מצב רישוי לפי מכשיר - https://updates.forescout.com/downloads/support/iDRAC_user_guide.pdf
- מצב רישוי מרוכז - פורטל הלקוחות, דף התיעוד.

כדי לברר באיזה מצב רישוי הפריסה משתמשת, ראה תיעוד נוסף של CounterACT (*זיהוי מצב הרישוי במסוף*).

*חשוב מאוד לעדכן את סיסמת ברירת המחדל לשורש, 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. הגדרת מסוף CounterACT

## *התקן את מסוף ה-CounterACT*

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

עליך לספק מחשב שיארח את תוכנת היישום של מסוף CounterACT. 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*

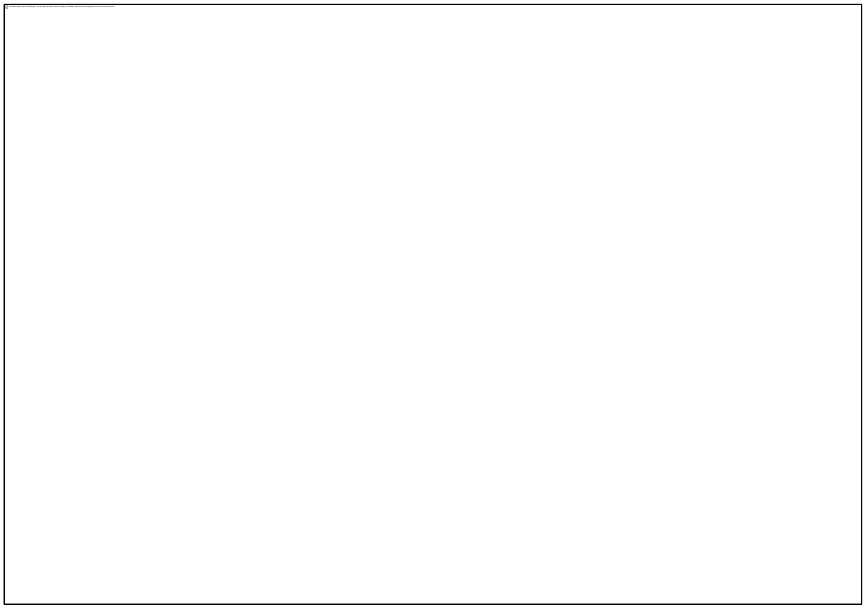
בסיום ההתקנה, תוכל להיכנס למסוף CounterACT.

1. בחר בסמל של CounterACT ממיקום קיצור הדרך שיצרת.


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 CounterACT.



## 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 CounterACT | |
| ממשקי ניטור ותגובה | |
| במקרה של מקטעים/VLAN ללא DHCP, מקטע הרשת/VLAN שאליהם ממשק התגובה מחובר ישירות, וכתובת IP קבועה שבה CounterACT ישתמש 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 תחום, בכלל זה שם וסיסמה של חשבון ניהול התחום | |
| שרתי אימות, כדי ש-CounterACT יוכל 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 CounterACT* או בעזרה המקוונת.

# תיעוד נוסף של CounterACT

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

- תיעוד להורדה
- פורטל התיעוד
- כלי עזרה של CounterACT

## תיעוד להורדה

ניתן לגשת אל התיעוד להורדה דרך אחד משני הפורטלים של ForeScout, בהתאם למצב הרישוי שבו הפריסה שלך משתמשת.

- ***מצב רישוי לפי מכשיר*** - פורטל עדכוני מוצרים
- ***מצב רישוי מרוכז*** - פורטל הלקוחות

*ניתן גם להוריד תוכנות מפורטלים אלה.*

כדי לברר באיזה מצב רישוי הפריסה שלך משתמשת, ראה זיהוי מצב הרישוי במסוף.

### פורטל עדכוני מוצרים

פורטל עדכוני המוצרים מספק קישורים אל מהדורות גרסה של CounterACT, מודולי בסיס ותוכן וכן מודולים מורחבים, כמו גם אל תיעוד רלוונטי. הפורטל מספק גם מגוון מסמכים נוספים.

**כדי לגשת לפורטל עדכוני המוצרים:**

1. עבור אל https://updates.forescout.com/support/index.php?url=counteract.
2. בחר בגרסת CounterACT שברצונך לגלות.

### פורטל הלקוחות

דף ההורדות בפורטל הלקוחות של ForeScout מספק קישורים אל מהדורות גרסה של CounterACT שנרכשו, מודולי בסיס ותוכן וכן מודולים מורחבים, כמו גם אל תיעוד רלוונטי. התוכנה והתיעוד הרלוונטי יופיעו בדף ההורדות רק אם אתה זכאי לרישיון עבור התוכנה. דף התיעוד בפורטל מספק מגוון מסמכים נוספים.

**כדי לגשת לתיעוד בפורטל הלקוחות של ForeScout:**

1. עבור אל https://forescout.force.com/support/.
2. בחר **Downloads** (הורדות) או **Documentation** (תיעוד).

## פורטל התיעוד

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

*אם הפריסה שלך משתמשת במצב רישוי מרוכז, ייתכן שאין לך אישורי גישה אל פורטל זה.*

**כדי לגשת לפורטל התיעוד:**

1. עבור אל www.forescout.com/docportal.
2. היכנס באמצעות אישורי התמיכה ללקוח שלך.

3. בחר בגרסת CounterACT שברצונך לגלות.

## כלי עזרה של CounterACT

גש למידע ישירות ממסוף CounterACT.

***לחצני עזרה של מסוף***

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

***מדריך הניהול של CounterACT***

בחר **CounterACT Help** (עזרה של CounterACT) מהתפריט **Help** (עזרה).

***קבצי עזרה של תוספים***

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

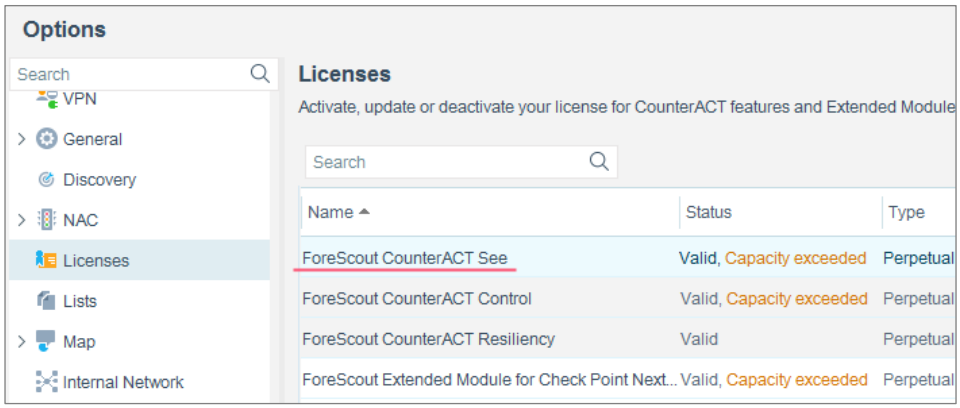
***פורטל התיעוד***

בחר **Documentation Portal** (פורטל התיעוד) מהתפריט **Help** (עזרה).

*זיהוי מצב הרישוי במסוף*

אם ל-Enterprise Manager יש רישיון *ForeScout CounterACT See* הרשום במסוף, הפריסה פועלת במצב רישוי מרוכז. אם לא, הפריסה שלך פועלת במצב רישוי לפי מכשיר.

בחר **Options > Licenses** (אפשרויות > רישיונות) כדי לברר אם יש לך רישיון *ForeScout CounterACT See* הרשום בטבלה.




בכל שאלה בנוגע לבירור מצב הרישוי שלך, פנה לנציג ForeScout.

## אזהרה משפטית



ניתן לשלוח הערות ושאלות בנוגע למסמך זה לכתובת: support@forescout.com

2018-03-2715:05