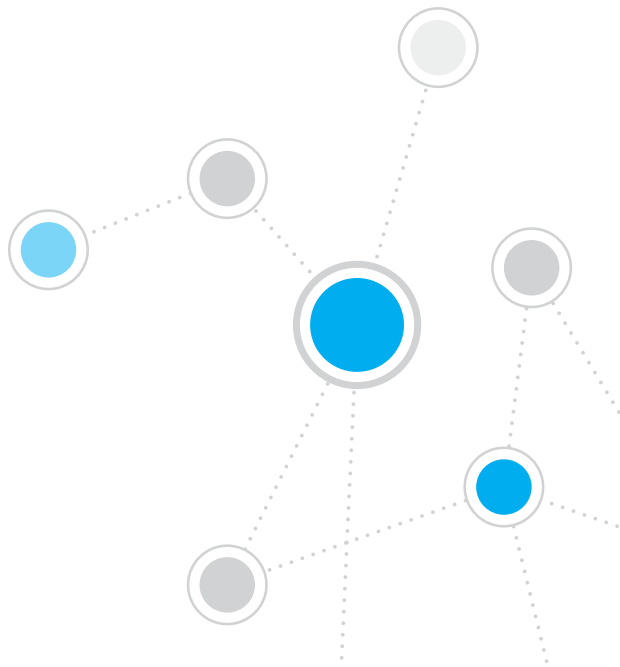


ForeScout CounterACT® 7

מכשיר CounterACT יחיד

מדריך התקנה מהיר



תוכן העניינים

3	ברוך הבא ל-CounterACT ForeScout גרסה 7
3	תכולת האריזה של CounterACT
4	סקירה כללית
5	1. יצירת תכנית פריסה
5	החלטה על מיקום הפריסה של המכשיר
5	חיבורי ממשק המכשיר
8	2. הגדרת המתג
8	א. אפשרויות חיבור המתג
9	ב. הערות לגבי הגדרת המתג
10	3. חיבור כבלי רשת והפעלה
10	א. הוצאת המכשיר וכבלי החיבור מהאריזה
11	ב. להקליט את ההקצאות ממשק
11	ג. כוח ער המכשיר
12	4. הגדרת המכשיר
14	רישיון
14	דרישות חיבור לרשת
15	5. ניהול מרחוק
15	כיוון iDRAC
18	חבר את המודול לרשת
18	היכנס ל-iDRAC
19	6. אימות הקישוריות
19	אימות חיבור ממשק הניהול
19	אימות קישוריות המתג/מכשיר
20	בדיקת איתות (ping)
21	7. הגדרת המסוף CounterACT
21	התקנת המסוף CounterACT
22	כניסה
22	לבצע את ההתקנה הראשונית
24	פרטי קשר

בוחן הבא ל-ForeScout CounterACT®

גרסה 7

ForeScout CounterACT™ הוא מכשיר אבטחה פיזי או וירטואלי שמזהה ובוחן באופן דינמי מכשירים ויישומים ברשת שלך ברגע שהם מתחברים אליה. מכיוון שאפשר להשתמש ב-CounterACT ללא צורך בסוכן, הוא יתאים לכל מכשיר – מנוהל ולא מנוהל, מוכר ולא מוכר, במחשב או בנייד, מוטמע או וירטואלי. CounterACT מזהה במהירות את המשתמש, הבעלים, מערכת ההפעלה, תצורת המכשיר, התוכנות, השירותים, מצב התיקונים וקיומם של תוכנות אבטחה נוספות. לאחר מכן, הוא מבצע תיקון, בקרה וניטור שוטף של המכשירים המתחברים לרשת מעת לעת. כל זה נעשה תוך שילוב חלק בכל תשתית IT קיימת.



מדריך זה מתאר התקנה של מכשיר CounterACT עצמאי יחיד.

למידע מפורט יותר, או למידע על פריסת מספר מכשירים להגנה על רשת ארגונית רחבה, עיין במדריך ההתקנה של CounterACT ובמדריך למשתמש במסוף. מסמכים אלה נמצאים בספרייה <http://www.forescout.com/support> בכתובת: docs/בתקליטור ה-CD של CounterACT.

בנוסף, תוכל לנוות לאתר התמיכה בכתובת: <http://www.forescout.com/support> לקבלת תיעוד עדכני, מאמרי בסיס ידע ועדכונים עבור המכשיר שברשותך.

תכולת האריזה של CounterACT

- מכשיר CounterACT
- מדריך התקנה מהיר
- תקליטור CD של CounterACT, הכולל תוכנת מסוף, מדריך למשתמש במסוף CounterACT ומדריך התקנה
- מסמך אחריות
- תשובות התקנה
- כבל חשמל
- כבל DB9 לחיבור המסוף (לחיבורים טוריים בלבד)

סקירה כללית

להגדרת CounterACT נדרשות הפעולות הבאות:

1. יצירת תכנית פריסה
2. הגדרת המתג
3. חיבור כבלי הרשת והפעלה
4. הגדרת המכשיר
5. ניהול מרחוק
6. אימות הקישוריות
7. הגדרת המסוף CounterACT

1. יצירת תכנית פריסה

לפני ההתקנה, יש להחליט על מיקום הפריסה של המכשיר וללמוד על חיבורי הממשק שלו.

החלטה על מיקום הפריסה של המכשיר

בחירת המיקום הנכון למכשיר ברשת היא קריטית כדי לשמור על הצלחת הפריסה של CounterACT וליהנות מביצועים מיטביים. המיקום הנכון תלוי ביעדי היישום הרצויים ובכללי המדיניות של הגישה לרשת. המכשיר אמור להיות מסוגל לנטר את התעבורה, הרלוונטית למדיניות הרצויה. לדוגמה, אם המדיניות תלויה בניטור אירועי הרשאה מנקודות קצה לשרתי אימות של הארגון, יש להתקין את המכשיר כך שיראה את זרימת התעבורה מנקודת הקצה לשרת(י) האימות.

למידע נוסף על התקנה ופריסה, עיין במדריך ההתקנה של CounterACT הנמצא בתקליטור ה-CD של CounterACT שקיבלת באריזה זו.

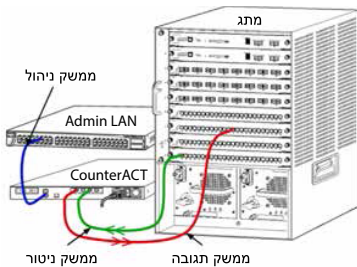
חיבורי ממשק המכשיר

המכשיר מוגדר בדרך כלל לשלושה חיבורים אל מתג הרשת.

ממשק ניהול

ממשק זה מאפשר לנהל את CounterACT, ולבצע שאלות וביקורת מעמיקה של נקודות קצה. חובה לחבר את הממשק ליציאת מתג, המאפשרת גישה לכל נקודות הקצה ברשת.

כל מכשיר דורש חיבור ניהול יחיד לרשת. חיבור זה דורש כתובת IP ב-LAN המקומית, וגישת TCP ליציאה 13000 מהמחשבים שבהם יופעל יישום הניהול למסוף של CounterACT. לממשק הניהול חייבת להיות גישה ליציאות הבאות ברשת:



פונקציה	אל CounterACT או מ-CounterACT	שירות	יציאה
מאפשרת גישה לממשק שורת הפקודה של CounterACT.	אל	SSH	22/TCP
(זמינות גבוהה) מאפשרת גישה להתקני CounterACT הפיזיים, המהווים חלק מאשכול הזמינות גבוהה.			2222/TCP
השתמש ב-22/TCP כדי לגשת לכתובת ה-IP המשותפת (הווירטואלית) של האשכול.			

יציאה	שירות	אל CounterACT או מ-CounterACT	פונקציה
25/TCP	SMTP	מ-	משמשת לשליחת דואר מ-CounterACT
53/UDP	DNS	מ-	מאפשרת ל-CounterACT לפענח כתובות IP פנימיות.
80/TCP	HTTP	אל	מאפשרת ניתוב HTTP מחדש.
123/UDP	NTP	מ-	מאפשרת ל-CounterACT לגשת לשרת זמן NTP. כברירת מחדל, CounterACT משתמש ב-ntp.foreScout.net.
135	WMI	מ-	מאפשרת ל-CounterACT לבצע חקירה ובקרה מעמיקות של נקודות קצה של Windows באמצעות WMI.
139/TCP	SMB, MS-RPP	מ-	מאפשרת לבדוק מרחוק נקודות קצה של Windows (לנקודות קצה עם Windows או גרסאות קודמות)
445/TCP			מאפשרת לבדוק מרחוק נקודות קצה של Windows
161/UDP	SNMP	מ-	מאפשרת ל-CounterACT לתקשר עם ציוד תשתית רשת, כגון מתגים ונתבים. למידע על הגדרת תצורת ה-SNMP, עיין במדריך למשתמש במסוף CounterACT.
162/UDP	SNMP	אל	מאפשרת ל-CounterACT לקבל מלכודות SNMP מציוד תשתית רשת, כגון מתגים ונתבים. למידע על הגדרת תצורת ה-SNMP, עיין במדריך למשתמש במסוף CounterACT.
443/TCP	HTTPS	אל	מאפשרת ניתוב HTTP מחדש באמצעות TLS.
2200/TCP	Secure Connector	אל	מאפשרת ל-SecureConnector ליצור חיבור מאובטח (SSL מוצפן) למכשיר ממחשבי Macintosh/Linux. ה-SecureConnector מאפשר גישה לנקודות קצה שאינן ניתנות לניהול דרך סקריפט מעטפת, הפועל במחשב שולחני בזמן שהמארז מחובר לרשת. SecureConnector היא תוכנה המבוססת על סקריפט שמאפשרת לנהל נקודות קצה של Macintosh ו-Linux כשהן מחוברות לרשת.
10003/TCP	Secure Connector ל-Windows	אל	מאפשרת ל-SecureConnector ליצור חיבור מאובטח (TLS מוצפן) למכשיר ממחשבי Windows. SecureConnector היא תוכנה המבוססת על סקריפט שמאפשרת לנהל נקודות קצה של Windows כשהן מחוברות לרשת.
			למידע נוסף על SecureConnector יש לעיין במדריך למשתמש של המסוף CounterAct. כש-SecureConnector מתחברת למכשיר או לתוכנת הניהול של הארגון היא מנותבת למכשיר שבו נמצא המארז. יש לוודא שהיציאה הזו פתוחה לכל המכשירים ושתוכנת הניהול של הארגון

מאפשרת חיבור מהמסוף למכשיר. במערכות המצוידות במספר מכשירי CounterACT, מאפשרת חיבור מהמסוף ל- Enterprise Manager ומה- Enterprise Manager לכל אחד מהמכשירים.	אל	CounterACT	TCP/13000
--	----	------------	-----------

ממשק ניטור

חיבור זה מאפשר למכשיר לנטר תעבורת רשת ולעקוב אחריה.

התעבורה משוקפת ליציאה במתג, ומנוטרת על ידי המכשיר. בהתאם למספר ה-VLANs המשוקפות, ייתכן שהתעבורה תהיה תעבורת VLAN 802.1Q מתויגת או לא.

- **VLAN יחידה (לא מתויגת):** כשה תעבורה המנוטרת נוצרת מ-VLAN יחידה, התעבורה המשוקפת אינה חייבת להיות תעבורת VLAN מתויגת.
- **מספר VLANs (מתויגות):** כשה תעבורה המנוטרת מגיעה מיותר מ-VLAN אחת, התעבורה המשוקפת חייבת להיות תעבורת VLAN 802.1Q מתויגת.

כששני מתגים מחוברים כזוג יתיר, המכשיר חייב לנטר תעבורה משני המתגים.

ממשק הניטור אינו דורש כתובת IP.

ממשק תגובה

המכשיר מגיב לתעבורה באמצעות ממשק זה. תעבורת התגובה משמשת כדי להגן מפני פעילות זדונית ולבצע פעולות מדיניות NAC. פעולות אלה עשויות לכלול, לדוגמה, ניתוב מחדש של דפדפני אינטרנט או חסימת חומת אש. תצורת היציאה של המתג הקשור תלויה בתעבורה המנוטרת.

- **VLAN יחידה (לא מתויגת):** כשה תעבורה המנוטרת נוצרת מ-VLAN יחידה, חובה להגדיר את ממשק התגובה כחלק מאותה VLAN. במקרה זה, המכשיר דורש כתובת IP יחידה ב-VLAN זו.
- **מספר VLANs (מתויגות):** אם התעבורה המנוטרת מגיעה מיותר מ-VLAN אחת, חובה להגדיר גם את ממשק התגובה לתיוג 802.1Q עבור אותן VLANs. המכשיר דורש כתובת IP עבור כל VLAN מוג.

2. הגדרת המתג

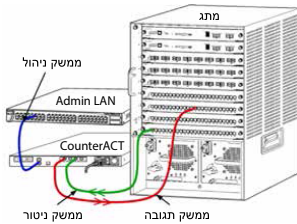
א. אפשרויות חיבור המתג

המכשיר תוכנן להשתלב באופן חלק במגוון רחב של סביבות רשת. כדי לשלב בהצלחה את המכשיר ברשת שברשותך, ודא שהמתג מוגדר לנטר את התעבורה הנדרשת.

מספר אפשרויות זמינות לחיבור המכשיר למתג.

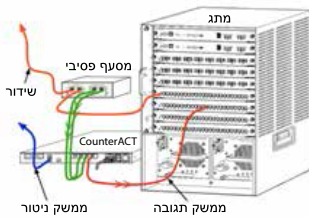
1. פריסה רגילה (ממשקי ניהול, ניטור ותגובה נפרדים)

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



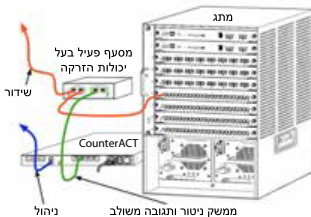
2. מסעף קו פסיבי

במקום להתחבר ליציאת ניטור של מתג, המכשיר יכול להשתמש במסעף פסיבי. מסעף פסיבי דורש שתי יציאות ניטור, למעט במקרה של מסעפי "רקומבינציה", שישלבו את שני זרמי הדופלקס ליציאה יחידה. חובה להגדיר באופן זה את התעבורה בממשק המסועף ואת ממשק התגובה. לדוגמה, אם התעבורה ביציאה המסועפת היא VLAN מתווגת (802.1Q), גם ממשק התגובה חייב להיות יציאת VLAN מתווגת.



3. מסעף קו פעיל (בעל יכולות הזרקה)

כשהמכשיר משתמש במסעף קו פעיל ויכולות הזרקה, ניתן לשלב את ממשקי הניטור והתגובה. אין צורך להגדיר יציאת תגובה נפרדת במתג. ניתן להשתמש באפשרות זו בכל סוג של תצורת מתג עולה או יורד.



4. תגובת שכבת IP (בהתקנות מתג שכבה 3)

המכשיר יכול להשתמש בממשק הניהול שלו כדי להגיב לתעבורה. למרות שניתן להשתמש באפשרות זו בכל תעבורה מנוטרת, מומלץ להשתמש בה כשהמכשיר מנטר יציאות שאינן מהוות חלק מ-VLAN כלשהי כך שהמכשיר לא יוכל להגיב לתעבורה המנוטרת באמצעות אף יציאת מתג אחרת. תופעה זו אופיינית לניטור קישור המחבר בין שני נתבים.

אפשרות זו אינה יכולה להגיב לבקשות פרוטוקול הסדרת כתובות (ARP), המגבילות את יכולתו של המכשיר לזהות סריקות המתמקדות בכתובות ה-IP הכלולות ברשת המשנה המנוטרת. מגבלה זו אינה רלוונטית כשמנטרים תעבורה בין שני נתבים.

ב. הערות לגבי הגדרת המתג

תגיות VLAN (802.1Q)

- **ניטור VLAN יחידה (תעבורה לא מתויגת)** אם התעבורה המנוטרת מגיעה מ-VLAN יחידה, היא אינה זקוקה לתגיות 802.1Q.
- **ניטור מספר VLANs (תעבורה מתויגת)** אם התעבורה המנוטרת מגיעה משתי VLANs או יותר, חובה לאפשר תיוג 802.1Q בממשק הניטור וגם בממשק התגובה. ניטור מספר VLANs הוא האפשרות המומלצת, כיוון שהיא מספקת כיסוי כולל מיטבי תוך מזעור מספר יציאות השיקוף.
- אם המתג אינו יכול להשתמש בתגית VLAN 802.1Q ביציאות השיקוף, בצע אחת מהפעולות הבאות:
 - שקף VLAN אחת בלבד
 - שקף יציאת שידור אחת שאינה מתויגת
 - השתמש באפשרות התגובה לשכבת ה-IP
- אם המתג מסוגל לשקף יציאה אחת בלבד, שקף יציאת שידור אחת. יציאה זו עשויה להיות מתויגת. באופן כללי, אם המתג מנקה תגיות VLAN 802.1Q, עליך להשתמש באפשרות התגובה IP Layer.

מידע נוסף

- אם המתג אינו מסוגל לשקף תעבורת שידור וקליטה, נטר את כל המתג, VLANs שלמות (אפשרות זו מספקת שידור/קליטה) או ממשק אחד בלבד (שאינו מאפשר שידור/קליטה). ודא שאינך מעמיס יתר על המידה את יציאת השיקוף.
- במתגים מסוימים (לדוגמה, Cisco 6509) ייתכן צורך למחוק לחלוטין את תצורות היציאות הקודמות לפני הזנת תצורות חדשות. התוצאה השכיחה ביותר כשלא מוחקים מידע יציאות ישן היא ניקוי תגיות 802.1Q על ידי המתג.

ב. להקליט את ההקצאות ממשק

לאחר סיום התקנת המכשיר במרכז הנתונים, והתקנת המסוף של CounterACT, תתבקש לרשום את הקצאות הממשקים. הקצאות אלה, המכונות הגדרות ערוצים, מוזנות ב-Initial Setup Wizard (אשף ההגדרה הראשונית) שנפתח בכניסה הראשונה למסוף.

רשום להלן את הקצאות הממשקים הפיזיים, והשתמש בהן במהלך השלמת הגדרת הערוצים במסוף.

ממשק Ethernet	הקצאת ממשק (לדוגמה: ניהול, ניטור, תגובה)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

ג. כוח ער המכשיר

1. חבר את כבל החשמל למחבר אספקת החשמל בלוח האחורי של המכשיר.
2. חבר את הקצה השני של כבל החשמל לשקע זרם חילופין (AC) מוארק.
3. חבר את המקלדת ואת הצג למכשיר, או הגדר את המכשיר לחיבור טורי. עיין במדריך ההתקנה של CounterACT הנמצא בתקליטור ה-CD של CounterACT.
4. הפעל את המכשיר מהלוח הקדמי.

חשוב: כבה את המחשב לפני הניתוק.

4. הגדרת המכשיר

הכן את המידע הבא לפני הגדרת המכשיר.

<input type="checkbox"/>	שם המארח של המכשיר
<input type="checkbox"/>	סיסמת מנהל המערכת של CounterACT
<input type="checkbox"/>	שמו של המכשיר
<input type="checkbox"/>	ממשק ניהול
<input type="checkbox"/>	כתובת ה-IP של המכשיר
<input type="checkbox"/>	מסיכת רשת
<input type="checkbox"/>	ברירת המחדל לכתובת ה-IP של השער
<input type="checkbox"/>	שם תחום DNS
<input type="checkbox"/>	כתובות שרתי ה-DNS

לאחר ההפעלה, תתבקש להתחיל בהגדרת התצורה באמצעות ההודעה הבאה:

```
CounterACT Appliance boot is complete.
. (אתחול המכשיר CounterACT הושלם).

Press <Enter> to continue.
. (לחץ <Enter> כדי להמשיך).
```

1. לחץ על **Enter** כדי להציג את התפריט הבא:

```
1) Configure CounterACT (הגדרת CounterACT)
2) Restore saved CounterACT configuration
   (שחזור תצורת CounterACT שמורה)
3) Identify and renumber network interfaces
   (זיהוי ומספור מחדש של ממשקי רשת)
4) Configure keyboard layout (הגדרת פריסת מקלדת)
5) Turn machine off (כיבוי המחשב)
6) Reboot the machine (אתחול המחשב)
1: Choice (1-6) (בחירה)
```

2. בחר **1 - Configure CounterACT**. כשתוצג ההנחיה:

Continue: (yes/no)?

לחץ על **Enter** כדי להתחיל בהגדרה.

3. התפריט **High Availability Mode** יפתח. לחץ על **Enter** כדי לבחור **Standard Installation** (התקנה רגילה).

4. ההנחיה **CounterACT Initial Setup** הגדרה ראשונית של CounterACT תוצג. לחץ על **Enter** כדי להמשיך.


5. התפריט **Select CounterACT Installation Type** (בחר סוג התקנת CounterACT) ייפתח. בחר **Type 1**, ולחץ על **Enter** כדי להתקין מכשיר CounterACT רגיל. ההגדרה תאוחל. פעולה זו עשויה להימשך זמן מה.
6. כשתוצג ההנחיה **Enter Machine Description** (הזן תיאור מחשב), הזן טקסט קצר המזהה התקן זה ולחץ על **Enter**. ההודעה הבאה תוצג:

```

Set Administrator Password >>>>>>
<<<<<< (הגדר סיסמת מנהל מערכת)

This password is used to log in as 'root' to
the machine Operating System and as 'admin'
to the CounterACT Console (סיסמה זו משמשת
לכניסה בתור 'root' למערכת ההפעלה של המחשב ובתור
'admin' למסוף של CounterACT).
The password should be between 6 and 15
characters long and should contain at least one
non-alphabetic character) (סיסמה אמורה להיות
באורך של 6 עד 15 תווים, ולכלול לפחות תו אחד
שאינו אלפביתי).
Administrator password (סיסמת מנהל מערכת):

```

7. כשתוצג ההנחיה **Set Administrator Password** (הגדר סיסמת מנהל מערכת), הקלד את המחרוזת שתשמש כסיסמה שלך (המחרוזת לא תוצג על המסך) ולחץ על **Enter**. תתבקש לאשר את הסיסמה. הסיסמה חייבת להיות באורך של שש עד 15 תווים, ולכלול לפחות תו אחד שאינו אלפביתי.
-  היכנס למכשיר בתור **root**, והיכנס למסוף בתור **admin**.
8. כשתוצג ההנחיה **Set Host Name** (הגדר שם מארח), הקלד שם מארח ולחץ על **Enter**. ניתן להשתמש בשם המארח בכניסה למסוף, והוא מוצג במסוף כדי לסייע לך לזהות את מכשיר ה-CounterACT שבו אתה צופה.
9. המסך **Configure Network Settings** (קבע הגדרות רשת) יבקש ממך סדרה של פרמטרי תצורה. הקלד ערך לכל הנחיה, ואחר כך לחץ על **Enter** כדי להמשיך.
- רכיבי ה-CounterACT מתקשרים דרך ממשקי הניהול. מספר ממשקי הניהול הרשומים תלוי בדגם המכשיר.
 - ה-**Management IP address** (כתובת ה-IP לניהול) היא כתובת הממשק, שדרכו מתקשרים רכיבי ה-CounterACT. הוסף VLAN ID (מזהה VLAN) עבור ממשק זה רק אם הממשק המשמש לתקשורת הרכיבים של CounterACT מחובר ליציאה מתויגת.
 - אם לרשותך יותר מ-**DNS server address** (כתובת שרת DNS אחת, הפרד בין הכתובות ברווח—רוב שרתי ה-DNS הפנימיים מפענחים כתובות חיצוניות ופנימיות, אך ייתכן שתצטרך להוסיף שרת DNS מפענח חיצוני. כיוון שכמעט כל שאליות ה-DNS המבוצעות על ידי המכשיר יהיו לכתובות פנימיות, יש לרשום את שרת ה-DNS החיצוני אחרון.
10. המסך **Setup Summary** (סיכום הגדרה) יוצג. תתבקש לבצע בדיקות קישוריות כלליות, להגדיר מחדש את ההגדרות או להשלים את ההגדרה. הקש **D** כדי להשלים את ההגדרה.

לאחר התקנה, עליך להתקין את רישיון ההדגמה הראשוני שניתן לך על ידי הנציג של CounterACT. הרישיון מותקן במהלך ההגדרה הראשונית של המסוף. רישיון ההדגמה הראשוני תקף למספר ימים. חובה להתקין רישיון קבוע לפני שתקופה זו תפוג. ייווצר עמך קשר בדוא"ל לגבי תאריך התפוגה. כמו כן, מידע לגבי מועד פקיעת הרישיון ומצב הרישיון יוצג בחלונית Appliances/Devices (מכשירים/התקנים) במסוף.

לאחר שתקבל רישיון קבוע, הרישיון יאומת מדי יום על ידי שרת הרישיונות של ForeScout. התרעות והפרות הנוגעות לרישיון יוצגו בחלונית Device Details (פרטי התקנים). רישיונות שלא ניתן לאמת למשך חודש יבוטלו. לפרטים נוספים על רישיונות, עיין במדריך ההתקנה של CounterACT.

דרישות חיבור לרשת

התקן CounterACT אחד לפחות (Appliance או Enterprise Manager) חייב להיות מסוגל לגשת לאינטרנט. חיבור זה משמש לאימות רישיונות CounterACT מול שרת הרישיונות של ForeScout.

רישיונות שלא ניתן לאמת למשך חודש יבוטלו. CounterACT ישלח בדוא"ל הודעת אזהרה אחת ליום, המציינת שקיימת שגיאה בתקשורת עם השרת.

5. ניהול מרחוק

כיוון iDRAC

הבקר המשולב של Dell לגישה מרחוק (iDRAC) הוא פתרון מערכת שרת משולב, המעניק גישה מרחוק שאינה תלויה במיקום או במערכת ההפעלה על גבי ה-LAN או דרך האינטרנט למכשירים או למנהלי ארגונים של CounterACT. השתמש במודול לגישת KVM, להפעלה/כיבוי/איפוס לפתרון בעיות ולביצוע משימות תחזוקה.

בצע את הפעולות הבאות כדי לעבוד עם מודול ה-iDRAC:

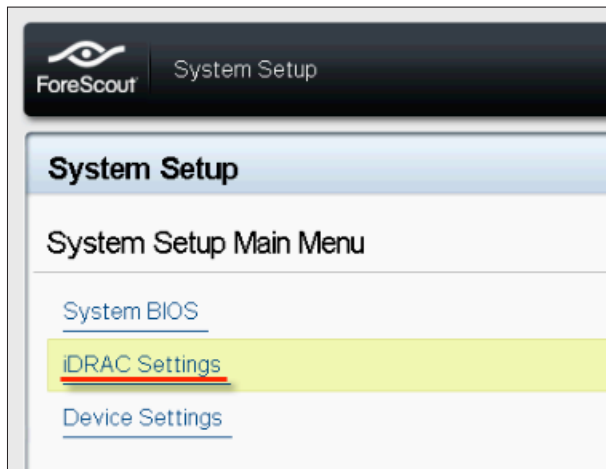
- אפשר והגדר את מודול ה-iDRAC
- חבר את המודול לרשת
- היכנס ל-iDRAC

אפשר והגדר את מודול ה-iDRAC

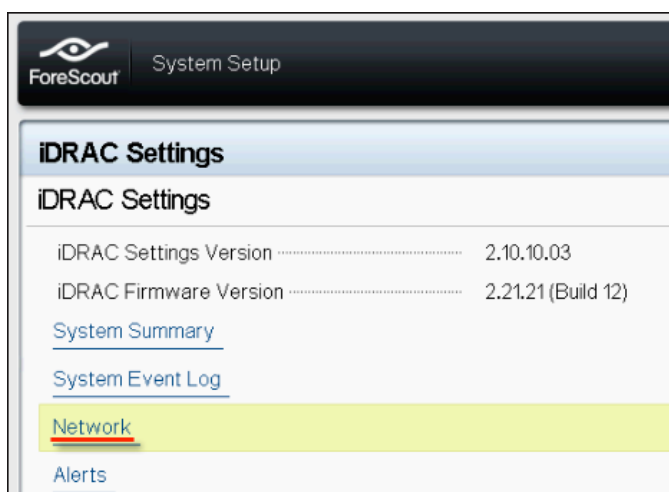
שנה את הגדרות ה-iDRAC כדי לאפשר גישה מרחוק להתקן ה-CounterACT. סעיף זה מתאר את הגדרות השילוב הבסיסיות, הנדרשות לעבודה עם CounterACT.

להגדרת ה-iDRAC:

1. הפעל את המערכת המנוהלת.
2. לחץ F2 במהלך הבדיקה העצמית באתחול (POST).
3. בדף התפריט הראשי System Setup (הגדרת מערכת), בחר **iDRAC Settings** (הגדרות iDRAC).

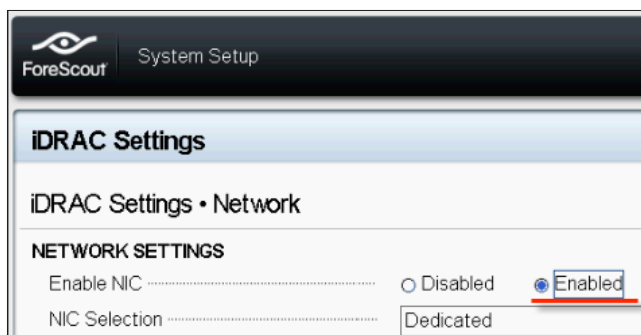


4. בדף iDRAC Settings (הגדרות iDRAC), בחר **Network** (רשת).



5. קבע את הגדרות הרשת הבאות:

- **Network Settings** (הגדרות רשת). ודא שהשדה **Enable NIC** (אפשר NIC) מוגדר למצב **Enabled** (מאפשר).



- **Common Settings** (הגדרות משותפות). בשדה DNS DRAC Name (שם DNS DRAC) ניתן לעדכן DNS דינמי (אופציונלי).

- **IPv4 Settings (הגדרות IPv4)** ודא שהשדה **Enable IPv4** (אפשר IPv4) מוגדר למצב **Enabled** (מאופשר). הגדר את השדה **Enable DHCP** (אפשר DHCP) למצב **Enabled** כדי להשתמש במיעון דינמי של כתובות IP, או למצב **Disabled** (מבוטל) כדי להשתמש במיעון סטטי של כתובות IP. אם פונקציית ה-DHCP מאופשרת, היא תקצה באופן אוטומטי את כתובת ה-IP, את השער ואת מסיכת רשת המשנה ל-iDRAC. אם פונקציית ה-DHCP מבוטלת, הזן ערכים בשדות **Static IP Address** (כתובת IP סטטית), **Static Gateway** (שער סטטי) ו-**Static Subnet Mask** (מסיכת רשת משנה סטטית).

iDRAC Settings

iDRAC Settings • Network

IPv4 SETTINGS

Enable IPv4	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled
Enable DHCP	<input checked="" type="radio"/> Disabled	<input type="radio"/> 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	<input checked="" type="radio"/> Disabled	<input type="radio"/> 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 את שדות תצורת המשתמש הבאים:
 - **Enable User** (אפשר משתמש). ודא ששדה זה מוגדר למצב **Enabled**.
 - **User Name** (שם משתמש). הזן שם משתמש.
 - **LAN and Serial Port User Privileges** (הרשאות משתמש).
 - **LAN ויציאה טורית**. הגדר רמות הרשאה למנהל המערכת.
 - **Change Password** (שנה סיסמה). הגדר סיסמה לכניסה של משתמש.

iDRAC Settings

iDRAC Settings • User Configuration

User ID	2	
Enable User	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled
User Name	root	
LAN User Privilege	Administrator	
Serial Port User Privilege	Administrator	
Change Password		

9. בחר **Back**, ואחר כך בחר **Finish** (סיום). אשר את ההגדרות שהשתנו. הגדרות הרשת יישמרו, והמערכת תאוותחל מחדש.

חבר את המודול לרשת

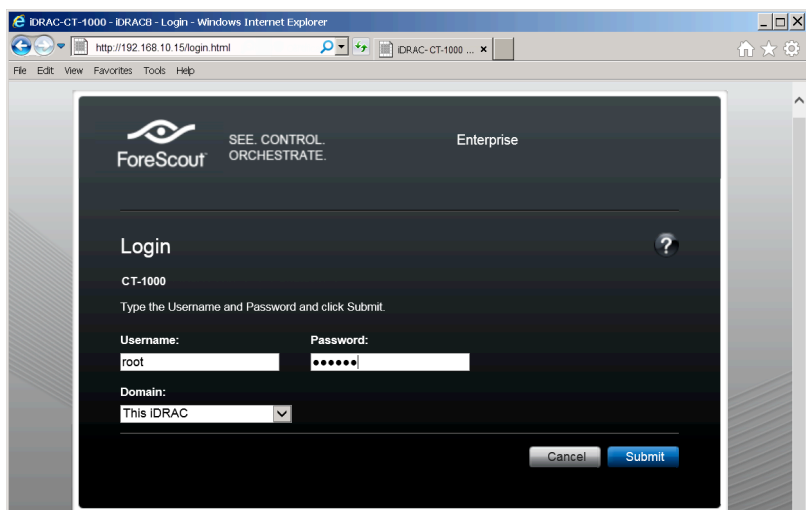
ה- iDRAC מתחבר לרשת Ethernet. נהוג לחבר אותו לרשת ניהול. התמונה הבאה מציגה את מיקום יציאת ה- iDRAC בלוח האחורי של המכשיר CT-1000:



היכנס ל-iDRAC

לכניסה ל-iDRAC:

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



2. הזן את ה- Username ואת ה- Password שהוגדרו בדף User Configuration (תצורת משתמש) בהגדרת מערכת ה-iDRAC.

3. בחר **Submit** (שלח).

למידע נוסף על iDRAC, עיין במדריך למשתמש של iDRAC.
חשוב מאוד לעדכן את אישורי ברירת המחדל.

6. אימות הקישוריות

אימות חיבור ממשק הניהול

לבדיקת החיבור של ממשק הניהול, היכנס למכשיר והפעל את הפקודה הבאה:

```
fstool linktest
```

המידע הבא יוצג:

```
Management Interface status) (מצב ממשק ניהול)
Pinging default gateway information
(מידע על איתות לשער ברירת המחדל)
Ping statistics (סטטיסטיקת איתות)
Performing Name Resolution Test
(ביצוע בדיקת פענוח שמות)
Test summary (סיכום בדיקה)
```

אימות קישוריות המתג/מכשיר

אמת שהמתג מחובר כהלכה למכשיר לפני היציאה ממרכז הנתונים. לשם כך, הפעל את הפקודה `fstool ifcount` במכשיר עבור כל ממשק שזוהה.

```
fstool ifcount eth0 eth1 eth2
```

(הפרד בין הממשקים ברווח).

כלי זה מציג ברציפות את תעבורת הרשת בממשקים שצוינו. הוא פועל בשני מצבים: לפי ממשק או לפי VLAN. ניתן לשנות מצב מהתצוגה. סך הסיביות לשנייה והאחוז של כל אחת מקטגוריות התעבורה הבאות יוצגו:

- ממשק הניטור אמור לראות בעיקר תעבורה משוקפת – מעל 90%.
- ממשק התגובה אמור לראות בעיקר תעבורת שידור.
- הן ממשך הניטור והן ממשק התגובה אמורים לראות את ה-VLANs הצפויים.

אפשרויות פקודה:

v - תצוגה במצב VLAN

I - תצוגה במצב ממשק

P - הצג את הקודם

N - הצג את הבא

q - יציאה מתצוגה

מצב VLAN:

[eth3: 14 vlans]					update=[4]
*From my MAC	*To my MAC	Mirrored	Broadcast	Total	Interface/Vlan
0.0%	0.0%	99.8%	0.2%	4Mbps	eth3.untagged
0.0%	0.0%	100.0%	0.0%	9Mbps	eth3.1
0.0%	0.0%	99.9%	0.1%	3Mbps	eth3.2
0.0%	0.0%	0.0%	100.0%	542bps	eth3.4
0.0%	0.0%	0.0%	100.0%	1Kbps	eth3.20
Show [v]lans [i]nterfaces <-[p]rev [n]ext->					[q]uit

Interface: מצב

[eth0: 32 vlans] [eth1: 1 vlans]					update=[31]
*From my MAC	*To my MAC	Mirrored	Broadcast	Total	Interface
43.7%	14.1%	0.0%	42.3%	3Kbps	eth0
0.0%	0.0%	100.0%	0.0%	475bps	eth1

*To my MAC – ה-Destination MAC היא ה-MAC של המכשיר.

*From my MAC – תעבורה שנשלחה על ידי מכשיר זה (ה-Source MAC היא ה-MAC של המכשיר. היעד עשוי להיות שידור או שידור ליעד בודד).

אם אתה לא רואה כל תעבורה, ודא שהממשק פועל. השתמש בפקודה הבאה במכשיר:

ip [שם מחשק] ifconfig

בדיקת איתות (ping)

הפעל בדיקת איתות מהמכשיר למחשב שולחני ברשת לשם אימות הקישוריות.

להפעלת הבדיקה:

1. היכנס למכשיר.
2. הפעל את הפקודה הבאה: **[כתובת ה-IP של המחשב השולחני ברשת] Ping** כברירת מחדל, המכשיר עצמו אינו משיב לאיתות.

7. הגדרת המסוף CounterACT

התקנת המסוף CounterACT

המסוף של CounterACT הוא יישום ניהול מרכזי, המשמש להצגת הפעילות שזוהתה על ידי המכשיר, למעקב אחריה ולניתוח שלה. ניתן להגדיר (NAC, Threat Protection) (הגנה מפני איומים), Firewall (חומת אש) וסוגי מדיניות אחרים מהמסוף. למידע נוסף, עיין במדריך למשתמש במסוף CounterACT.

על־ך להשתמש במחשב שיארח את יישום התוכנה של מסוף CounterACT. דרישות המינימום של המערכת הן:

- מחשב שאינו ייעודי, עם אחת ממערכות ההפעלה הבאות:
 - Windows Vista, Windows XP או Windows 7
 - Windows Server 2003 או Windows Server 2008
 - Linux
- מעבד 3 Pentium, 1GHz
- זיכרון 2GB - RAM
- שטח דיסק - 1GB

ניתן להתקין את המסוף בשתי שיטות:

השתמש בתוכנת ההתקנה המובנית במכשיר שברשותך.

1. פתח חלון דפדפן ממחשב המסוף.
2. הקלד את הכתובת הבאה בשורת הכתובת של הדפדפן
<http://<Appliance ip>/install>
כש- x.x.x.x הוא כתובת ה- IP של המכשיר. הדפדפן יציג את חלון התקנת המסוף.
3. פעל על פי ההוראות שעל המסך.

התקנה מתקליטור ה-CD-ROM של CounterACT

1. הכנס את תקליטור ה-CD-ROM של CounterACT לכונן ה-DVD.
2. פתח את הקובץ **ManagementSetup.htm** מתקליטור ה-CD-ROM באמצעות דפדפן.
3. פעל על פי ההוראות שעל המסך.

כניסה

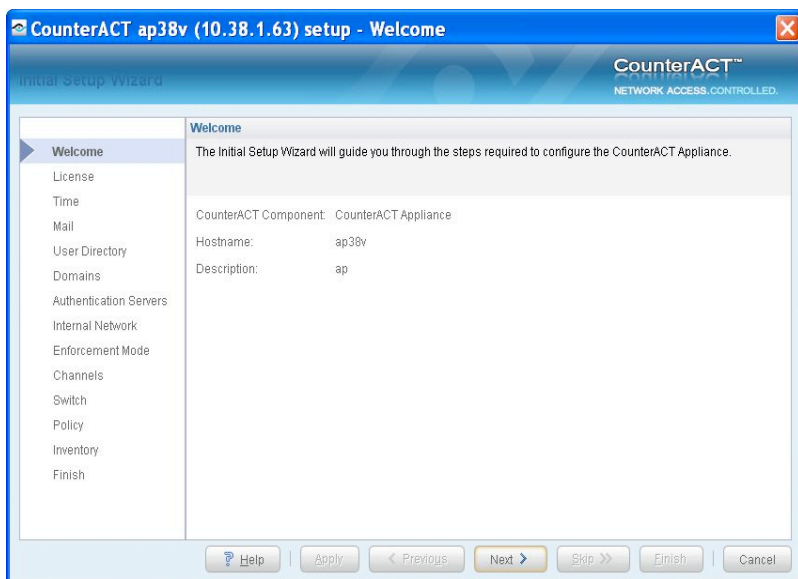
לאחר השלמת ההתקנה, תוכל להיכנס למסוף של CounterACT.

The image shows the CounterACT Login window. It has a blue header with the CounterACT logo and the ForeScout logo. Below the header, there is a yellow key icon. The main area contains a 'Login Method' dropdown menu set to 'Password'. Below this are fields for 'IP/Name', 'User Name', and 'Password'. There is a checkbox labeled 'Save address and user name' which is checked. At the bottom right are 'Login' and 'Cancel' buttons.

1. לחץ על הסמל CounterACT במיקום קיצור הדרך שיצרת.
2. הזן את כתובת ה-IP או את שם המארז של המכשיר בשדה **IP/Name** (כתובת IP / שם).
3. בשדה **User Name**, הזן **admin**.
4. בשדה **Password**, הזן את הסיסמה שיצרת במהלך התקנת המכשיר.
5. בחר **Login** כדי להפעיל את המסוף.

לבצע את ההתקנה הראשונית

לאחר הכניסה הראשונה, יוצג ה-Initial Setup Wizard (אשף ההגדרה הראשונית). האשף ינחה אותך בשלבים החיוניים של הגדרת התצורה כדי להבטיח התחלת שימוש מהירה ויעילה ב-CounterACT.

The image shows the CounterACT Initial Setup Wizard Welcome window. The title bar says 'CounterACT ap38v (10.38.1.63) setup - Welcome'. The window has a blue header with the CounterACT logo and the text 'NETWORK ACCESS CONTROLLED'. On the left is a sidebar with a list of steps: Welcome, License, Time, Mail, User Directory, Domains, Authentication Servers, Internal Network, Enforcement Mode, Channels, Switch, Policy, Inventory, and Finish. The 'Welcome' step is selected. The main area contains the text 'Welcome' and 'The Initial Setup Wizard will guide you through the steps required to configure the CounterACT Appliance.' Below this, it shows 'CounterACT Component: CounterACT Appliance', 'Hostname: ap38v', and 'Description: ap'. At the bottom are buttons for 'Help', 'Apply', '< Previous', 'Next >', 'Skip >>', 'Finish', and 'Cancel'.

לפני התחלת ההתקנה הראשונית

הכן את המידע הבא לפני העבודה עם האשף:

מידע	ערכים
□ כתובת שרת ה-NTP, שבו משתמש הארגון (אופציונאלי).	
□ כתובת ה-IP של ממסר הדואר הפנימי. ממסר זה מאפשר להעביר דוא"ל מה-CounterACT אם תעבורת SMTP אינה מותרת מהמכשיר (אופציונאלי).	
□ כתובת הדוא"ל של מנהל המערכת של CounterACT.	
□ הקצאות ממשקי הניטור והתגובה שהוגדרו במרכז הנתונים.	
□ במקטעים או ב-VLANs ללא DHCP, מקטע הרשת או ה-VLANs שאליו/אליהן מחובר ישירות ממשק הניטור וכתובת IP קבועה לשימוש על ידי CounterACT בכל VLAN מסוג זה. מידע זה אינו נדרש להגדרת Enterprise Manager.	
□ טווחי כתובות ה-IP, שעליהם יגן המכשיר (כל הכתובות הפנימיות, לרבות כתובות שאינן בשימוש).	
□ פרטי חשבון של ה-User Directory (ספריית המשתמשים), וכתובת ה-IP של שרת ה-User Directory.	
□ אישורי תחום, לרבות שם וסיסמה לחשבון המנהלי של התחום.	
□ שרתי אימות, המאפשרים ל-CounterACT לנתח את מארחי הרשת שאומתו בהצלחה.	
□ כתובת ה-IP של מתג הליבה, ספק ופרמטרי SNMP.	

למידע על העבודה עם האשף, עיין במדריך למשתמש במסוף CounterACT או בעזרה המקוונת.

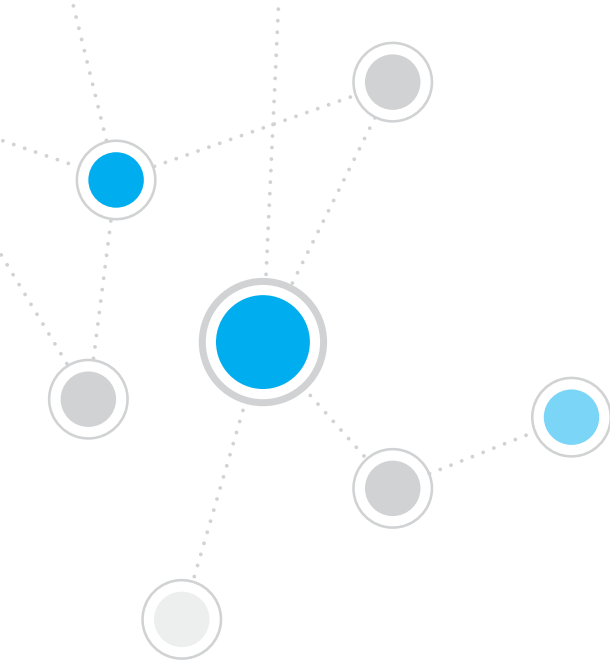
פרטי קשר

לתמיכה הטכנית של ForeScout, שלח דוא"ל לכתובת support@forescout.com או התקשר אלינו לאחד מהמספרים הבאים:

- חיוג חינם (ארה"ב): +1-866-377-8771
- טלפון (בינ"ל): +1-408-213-3191
- תמיכה: +1-708-237-6591
- פקס: +1-408-371-2284

©2016 ForeScout Technologies, Inc. מוצרים המוגנים על ידי הפטנטים האמריקניים מס' 8,363,489, 8,254,286, 8,590,004 ו-8,639,800. כל הזכויות שמורות. ForeScout Technologies והלוגו של ForeScout הם סימנים מסחריים של ForeScout Technologies, Inc שימוש.

במוצר כלשהו של ForeScout כפוף לתנאי הסכם הרישוי למשתמש הקצה של ForeScout שבכתובת www.forescout.com/eula.



ForeScout Technologies, Inc.
900 E. Hamilton Avenue #300
Campbell, CA 95008 USA

חיוג חנם (ארה"ב): +1-866-377-8771
טלפון (בינ"ל): +1-408-213-3191
תמיכה: +1-708-237-6591
פקס: +1-408-371-2284

400-00020-01