



מעבדה 5



CSRP

DFIR

מבוא ל-DFIR

נבסי רשת

- עמוד 1 -

כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383

נושאי המעבדה

התקן והגדר תוכנת ניהול נכס רשת בסיסית.

זמן מוערך

20-30 דקות.

סביבת המעבדה

VirtualBox שכולל Bridged Adapter עם:

• Windows

○ כונן משני קטן

משימת מעבדה:

התקינו והגדירו LanSweeper כדי לקבל מבט על הרשת.

1 על המכונה הוירטואלית Microsoft Windows שלכם, הוסיפו למכונה המקומית את המשתמש johnd עם הסיסמה Aa123456! באמצעות שורת הפקודה. הוסף את המשתמש לקבוצת administrators. **שימו לב:** אסור שבמכונה וירטואלית זו יהיו קבצים פרטיים או סיסמאות. כשמעבדה זו נגמרת, הסירו את המשתמש johnd.

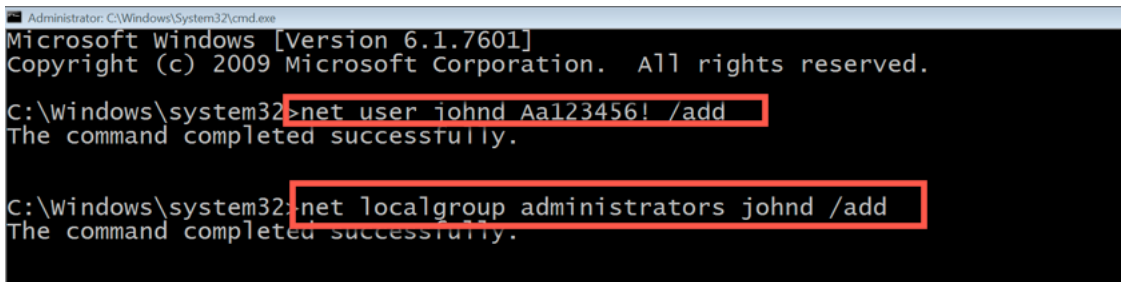
פתרון:

כדי ליצור את המשתמש johnd עם הסיסמה Aa123456!, השתמשו בפקודה הבאה:

```
Net user johnd Aa123456! /add
```

כדי להוסיף את המשתמש לקבוצת administrators, השתמשו בפקודה הבאה:

```
Net localgroup administrators johnd /add
```



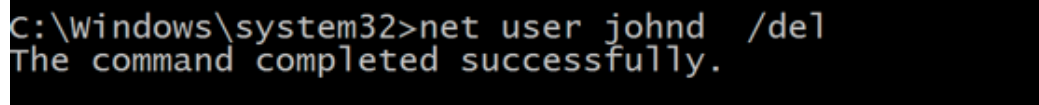
```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net user johnd Aa123456! /add
The command completed successfully.

C:\Windows\system32>net localgroup administrators johnd /add
The command completed successfully.
```

כדי להסיר את המשתמש johnd בסוף המעבדה, השתמשו בפקודה הבאה:

```
Net user johnd /del
```



```
C:\Windows\system32>net user johnd /del
The command completed successfully.
```

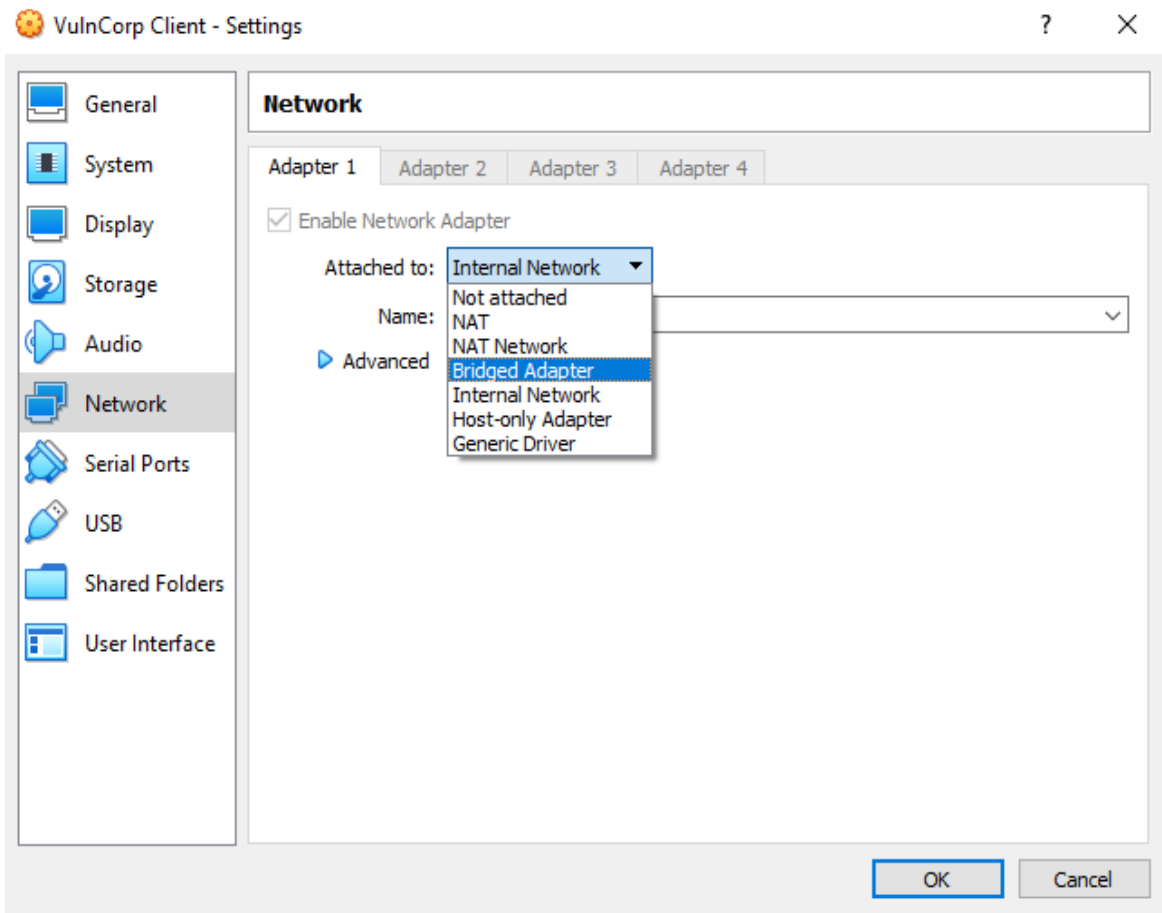
2

ב-VirtualBox, שנה את NIC ל-"Bridged Adapter". **שימו לב:** צעד זה נעשה כדי לשפר את התוצאות ע"י סריקת כל ה-Class (עם כל המכונות בעלי אותה התצורה). אם ה-bridged networking לא עובד עקב בעיות DHCP, ניתן לבצע מעבדה זו בתצורת NAT.

פתרון:

כדי לשנות את כתובת ה-NIC, פתח VirtualBox, לחיצה ימנית על Windows 7 Hosts, ל-Settings-> Network.

ב-Adapter 1, ודא ש-NIC עובד, ועבור Attached to, בחר Bridge Adapter.



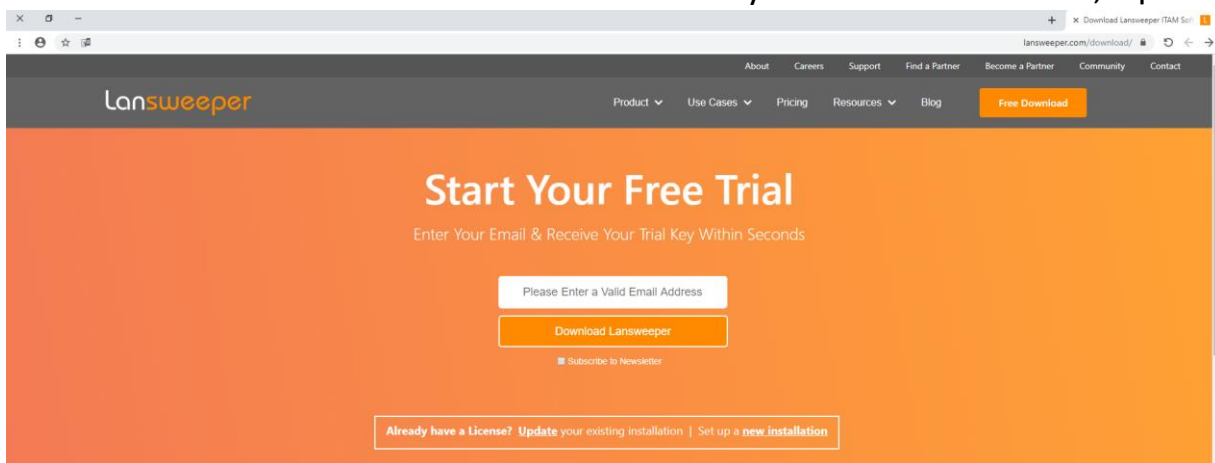
הורידו והתקנו LanSweeper עם הגדרות ברירת המחדל שלו, מהקישור הבא :

3

<https://www.lansweeper.com/download/>

פתרון:

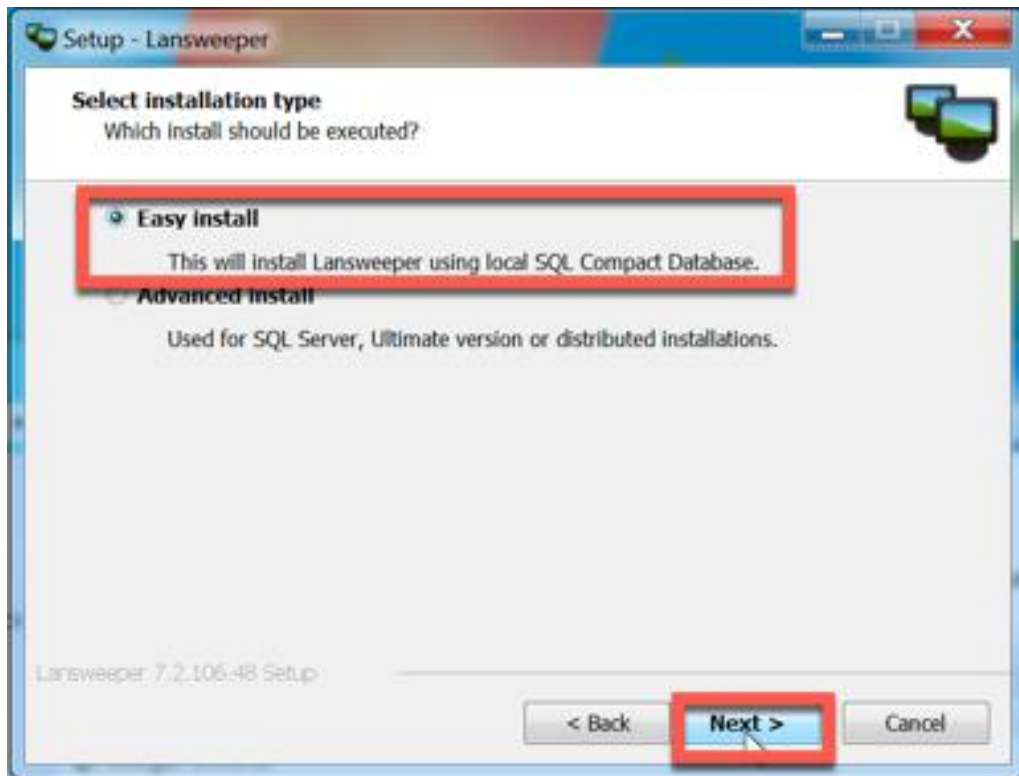
גלושו אל האתר של LanSweeper, היזינו את כתובת המייל שלך, הורידו את קבצי ההתקנה, ובחרו באפשרות Easy Install.



ההתקנה פשוטה. לחצו Next עד הסוף, וזכרו שאם ה-ports משמשים את המחשב שלך, בחרו אחרים, כמו 8181 או 8443.

- עמוד 4 -

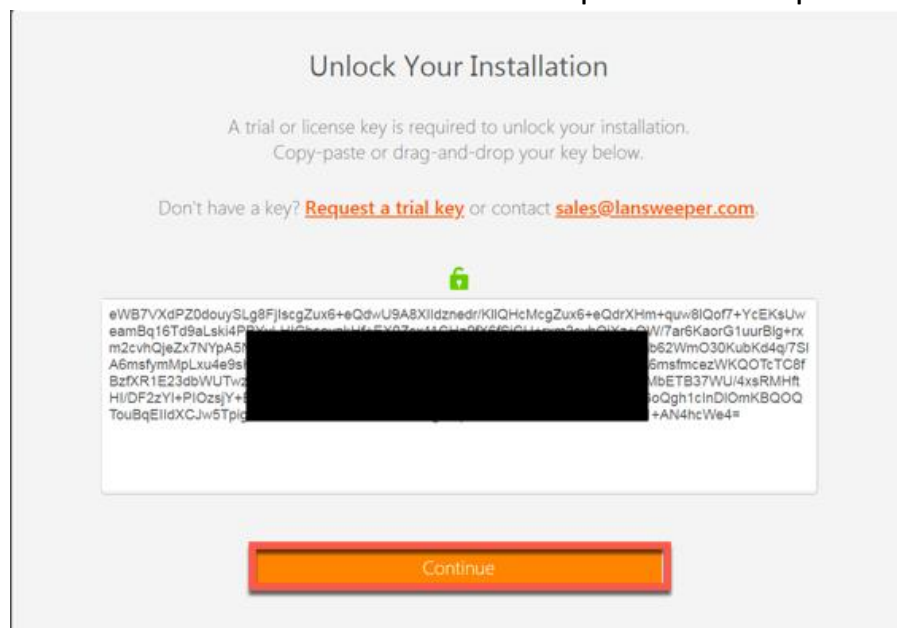
כל הזכויות שמורות © סיבר סקול בע"מ, אילנות 7, כרמיאל | 077-7781383



4 אחרי שההתקנה נגמרת, נווטו אל localhost:[port] כדי לוודא את ההתקנה. הפעילו את ההתקנה באמצעות ה-key שקיבלת באימייל. **שימו לב:** תקופת הניסיון היא לגרסת ה-unlimited. אחרי 30 ימים עדיין תוכלו להשתמש ב-LanSweeper עם יותר מ-100 מכשירים ולאחר הפעלת המפתח יש לחכות 5 דקות. a. במסך "Asset Types", בחרו "only Windows and network devices". b. הזינו את האישורים של johnd כשאתם מתבקשים לעשות זאת.

פתרון:

ה-key אמור להישלח לאימייל שהזנתם באתר Lansweeper. חלצו את ה-key והכניסו אותו בדף הרשת הראשון של הגדרת התצורה.



הגדירו את התצורה של LanSweeper וסרוקו את הרשת באמצעות האישורים של johnd.
פתרון:

LanSweeper אמור לאתר את טווח הרשת לסריקה באופן אוטומטי.

במסך Asset Type, בחרו רק Windows ו- Network Devices. LanSweeper יכול לנסות ולאתר מכשירים אחרים, אך אלו לא רלוונטיים למעבדה זו.

אחרי שבחרתם בנכס Windows, עלייכם להכניס את האישורים של admin ה-domain או של ה-administrator המקומי (השתמשו באישורים של johnd).

Which credentials should be used to scan Windows computers?

Windows ⓘ

Username

Password

Progress bar: Welcome | IP ranges | Asset types | **Credentials** | Finish

Buttons: Previous, Next

שים לב: כיוון שביקשנו מהתלמידים להשתמש ב-bridge adapter ויש להם את אותם אישורים, כל המחשבים ברשת יסרקו וייראו ב-dashboards (אם התלמידים יהיו על אותה הרשת).
 הערה: אין צורך לשנות SMTP כיוון שאנחנו לא הולכים להשתמש בו עבור ההדגמה.

Scanning your network!

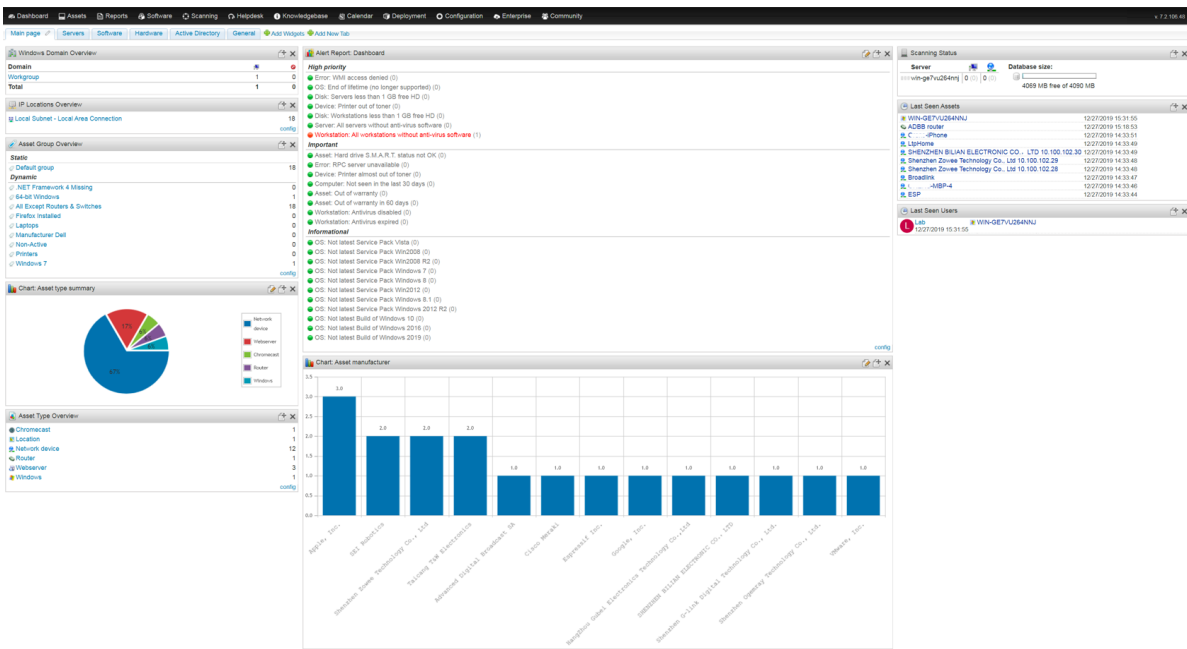
Lansweeper is now gathering data from your network!
 Feel free to browse the web console while scans are taking place.

<p>Scan statistics</p> <ul style="list-style-type: none"> ✓ Completed scans: 1 ⚙ Processing scans: 0 📄 In queue: 0 🔍 Discovered assets: 2 	<p>Scanning queue</p> <p>Scanserver is waiting for scan requests...</p>
--	--

This wizard will automatically close in 25 seconds.

Progress bar: Welcome | IP ranges | Asset types | Credentials | **Finish**

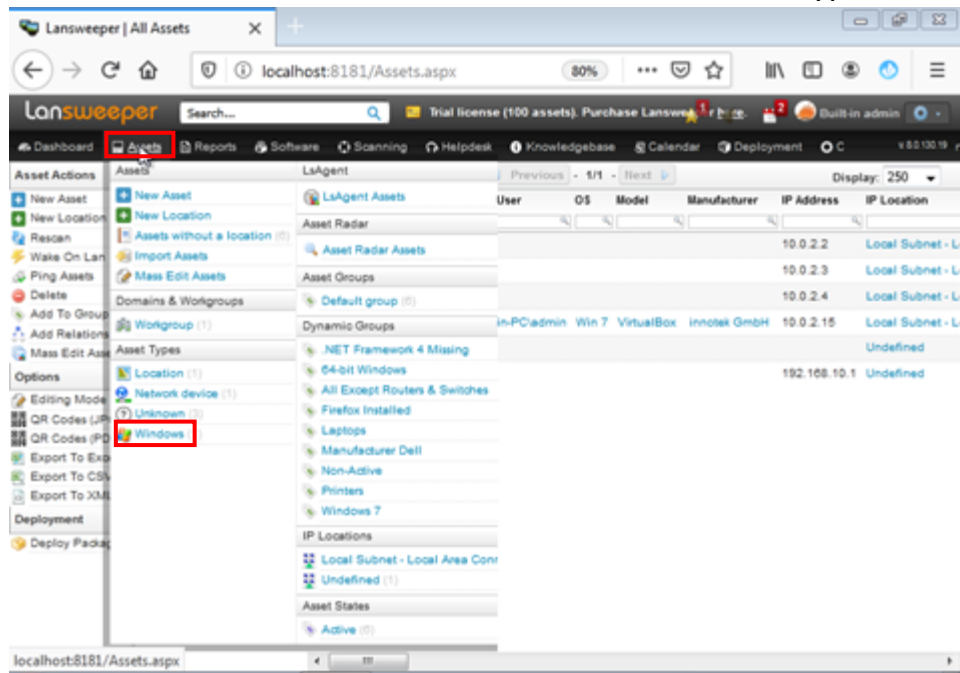
אחרי שלחצת Finish, אתה אמור לראות את ה-Dashboard הבא:



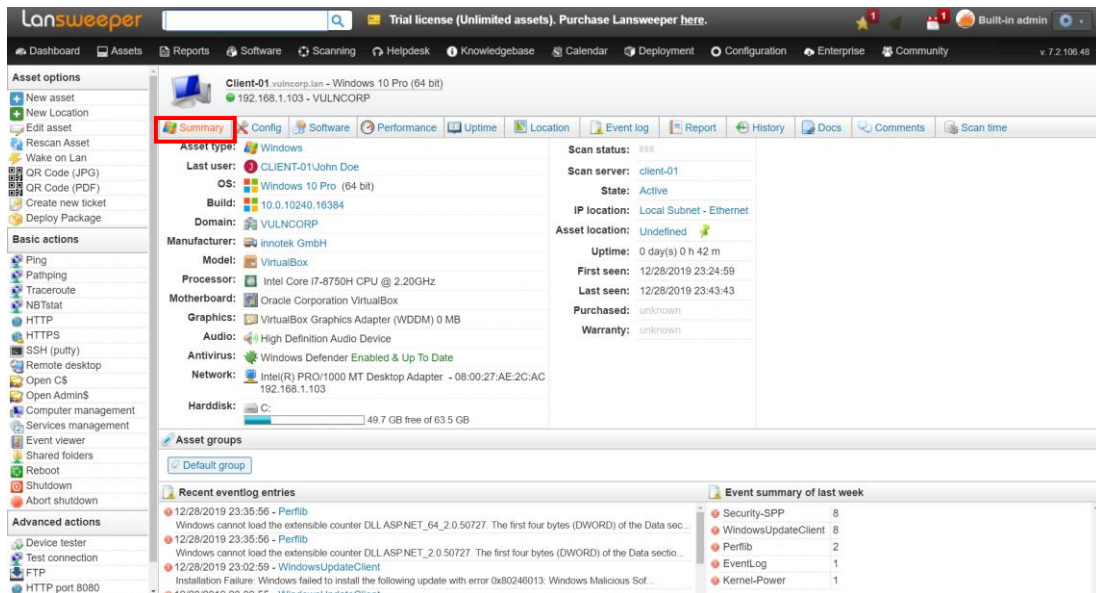
6 בחרו עמדת עבודה וענו על השאלות הבאות:

a. מי המשתמש שהתחבר לאחרונה?
 b. איזו תוכנה מותקנת על הלקוח?
 c. האם האנטי וירוס עובד בעמדת העבודה?
פתרון:

כדי להציג את כל עמדות העבודה לחצו על לשונית ה- Assets, אפשר לסנן ולבחור סוג מסוים במקרה שלנו, בחירה של התקני Windows על ידי לחיצה על Windows מתחת לאזור Assets Types.



ניתן למצוא את רוב נתוני הלקוחות ע"י לחיצה על הלקוח בסרגל הימני, ובחירה בתפריט summary.



לחילופין:

ניתן למצוא את כניסת המשתמש האחרון ב: **Config** <- **User info** <- **Last logon**
 ניתן למצוא את התוכנה המותקנת ב: **Software** <- **Antivirus**
 ניתן למצוא את נתוני האנטי וירוס ב: **Software** <- **Antivirus**

7 ערכו את מידע הנכס כדי שיכלול את הפרטים הבאים:

- a. קשר הנכס לנכס אחר.
- b. יחס הנכס למשתמש.
- c. תגובות על הנכס (החשיבות שלו וכו').
- d. מיקום הנכס.

פתרון:

כדי לערוך את המידע, בחרו נכס ולחצו **Edit Asset** בתפריט בצד שמאל. רוב השדות פשוטים להבנה.

Start Date	End Date	Asset	Type	Asset	Comments
12/29/2019		This asset	Connected To	DC-01	

This asset
Connected To
This asset

User / OU / AD group Relations

Start Date	End Date	Type	User / OU / AD group	Comments
12/29/2019		Used By	CLIENT-01\John Doe	

Used By
None selected

Description:

This Asset is of no importanceS

Comments:



אחרי הזנתם את המידע, שמורו את הנכס על ידי לחיצה על **Save Asset** בתפריט השמאלי.

הערת מעבדה: *LanSweeper* הוא יישום של *IT Asset Management (ITAM)* – ניהול נכסים של *IT* שלא כולל את כל הנכסים החומריים והמופשטים. בדרך כלל ניתן לעקוב אחרי מערך הנכסים השלם באמצעות מסמכי העובדים וגיליונות האלקטרוניים של הארגון.