הסבר על התחברות ממחשב אישי/ביתי למחשב בעבודה

בס"ד, א' ניסן תש"ף
26 מרץ 2020

עבור
חוקרים ועובדי האוניברסיטה

הוראות חיבור מרחוק תקיפות למשתמשים הרשומים בפקולטה למדעים מדויקים בלבד !

הנחיות אבטחת מידע

עובדות ועובדים יקרים,

לאור המצב שנוצר, פתחנו את האפשרות לעבוד מן הבית לאלו מכם שנדרשו לעשות זאת. עשינו זאת בצורה שתאפשר את מירב הגמישות בביצוע המשימות השונות, ע"י מתן האפשרות להתחבר למחשב האישי בעבודה. גמישות זו כרוכה בסיכונים רבים, שנלקחו בחשבון ואותם אנו משתדלים לצמצם:

- למרות שהמחשבים בעבודה נשארים דלוקים, הם לא נגישים ישירות מבחוץ.
- ההתחברות שלכם אליהם מתבצעת דרך נקודת גישה יחידה מבוקרת ומנוטרת ברשת שלנו.
- המחשבים בעבודה מוגנים ע"י עדכוני אבטחה ועדכוני אנטי-וירוס שוטפים
- מופעלים ברשת כל אמצעי ההגנה והבקרה שפועלים גם בימים כתיקונם

למרות כל אמצעי ההגנה הנ"ל, נדרשים שיתוף הפעולה והערנות שלכם בזמן העבודה מן הבית. חשוב להקפיד במיוחד על הנקודות הבאות:

- אתם מתחברים למחשב בעבודה ממחשב ביתי שאין לנו עליו שליטה ובקרה.
- הכרחי שעל המחשב בבית יותקנו באופן שוטף כל עדכוני האבטחה של מערכת ההפעלה ועדכוני תוכנת האנטי-וירוס.
- לפני ההתחברות הראשונית, חייבים לבצע סריקה באמצעות האנטי-וירוס ולוודא שהמחשב נקי ולא נגוע בנוזקות.
- יש לדאוג לנעילת המסך בסיסמה כאשר עוזבים את המחשב ליותר מ- 15 דקות
- אין לאפשר גישה של בני בית אחרים למחשב הביתי בזמן שהוא מחובר למחשב בעבודה
- יש להתנתק מהחיבור לעבודה לאחר סיום משימת העבודה מהבית
- אין להעביר קבצים מהמחשב הביתי לכונני המחשב בעבודה
- חל איסור חמור להעביר חומר כלשהו מכונני המחשב בעבודה או ממערכות בר אילן למחשב הביתי
- למתקדמים – המלצה שנכונה לכל זמן – לשנות את סיסמת ברירת המחדל של ה admin -בראוטר הביתי, כדי למנוע השתלטות עוינת על הרשת הביתית

בנוסף, יש להגביר את הערנות בנושא הפישינג. קיימת עליה במתקפות אשר מנצלות את רגישות האירועים האחרונים. מרבית המתקפות מבוססות על פניות כגון:

- התחזות לפניות ממשרד החינוך בנושא פלטפורמות למידה מרוחקת (נפוץ מאוד, בד"כ לינקים)
- הנחיות משרד הבריאות (צרופות/ לינקים)
- עדכוני קורונה (לינקים)
- פניות ממשטרת ישראל/ מד"א (לינקים/ קבצים)

כרגיל ההנחיה היא לנסות לבדוק את מקור השולח ובמקרה של חשד להימנע מלחיצה על לינק או פתיחת צרופות.

ע"י הקפדה על הכללים הנ"ל נמשיך לבצע את משימותינו החיוניות ונצלח בבטחה את התקופה המאתגרת שלפנינו.

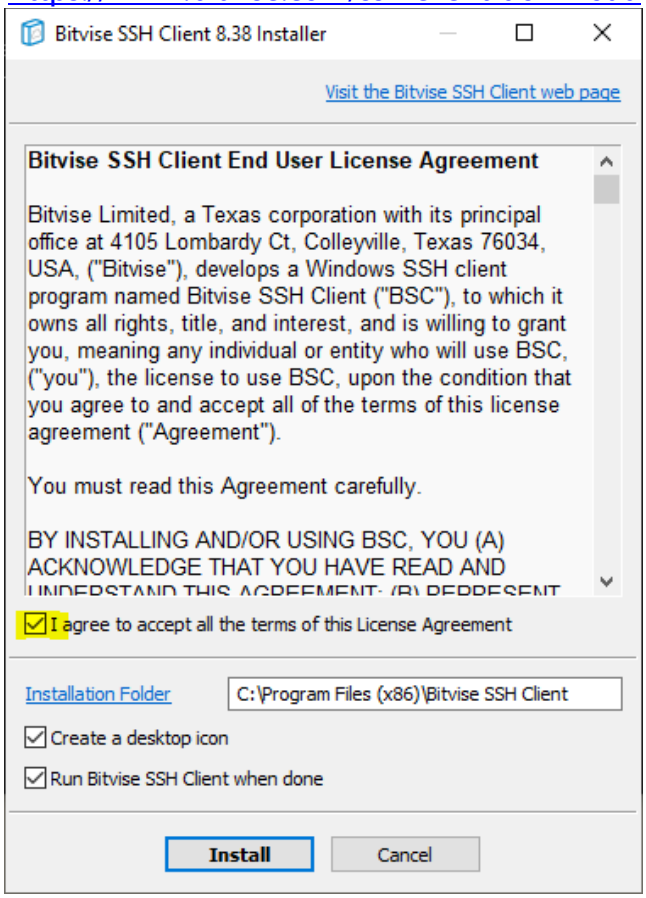
בברכת בריאות לכולנו,

ויקטור שטרנברג | מנהל אבטחת מידע CISO | אגף תקשוב | אוניברסיטת בר אילן

הנחיות להתחברות

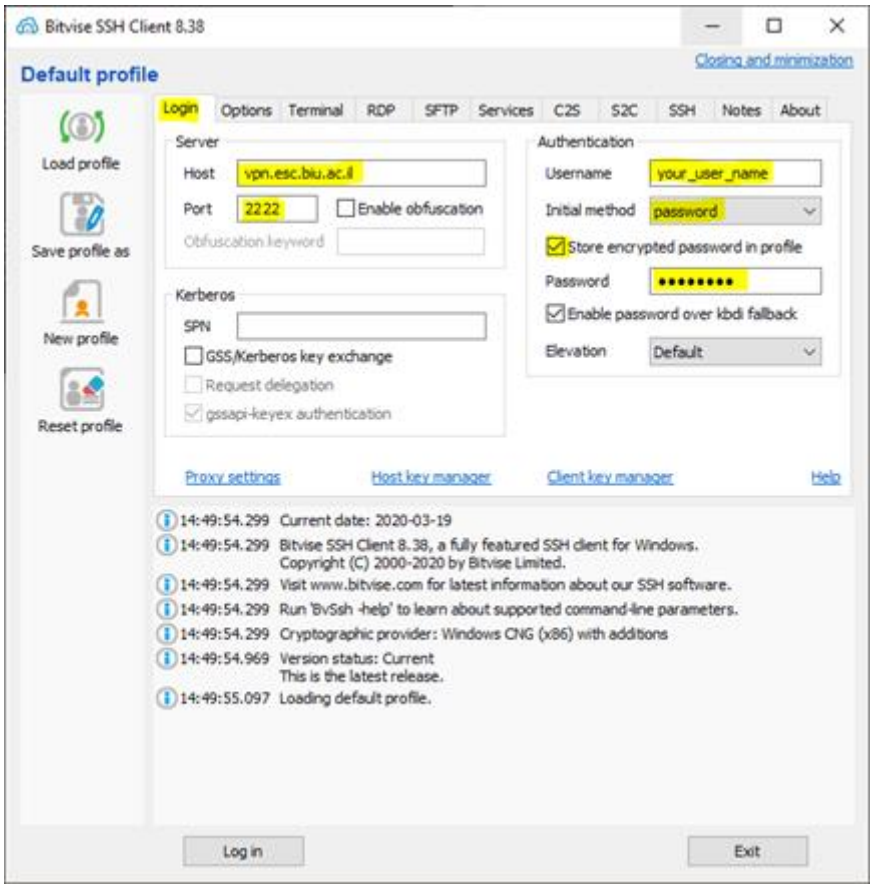
- החיבור מרחוק אפשרי לשרתי המחלקות/הפקולטה. אנשי סגל אקדמי יכולים להתחבר למחשבים ברשת האקדמית **רק** אם ביצעו מראש מספר פעולות מכינות במחשב האוניברסיטה (הסבר מפורט יינתן בנפרד).
- כל איש סגל חייב לדעת את שם המשתמש והסיסמא שלו לפני תחילת ההתחברות. מידע אודות שם המשתמש והסיסמא ניתן למצוא באתר האוניברסיטה.

1. ראשית, יש להוריד ולהתקין את תוכנת **Bitvise SSH Client**
התוכנה נועדה לאפשר חיבור מאובטח ומוצפן בין מחשבים.
https://www.bitvise.com/ssh-client-download

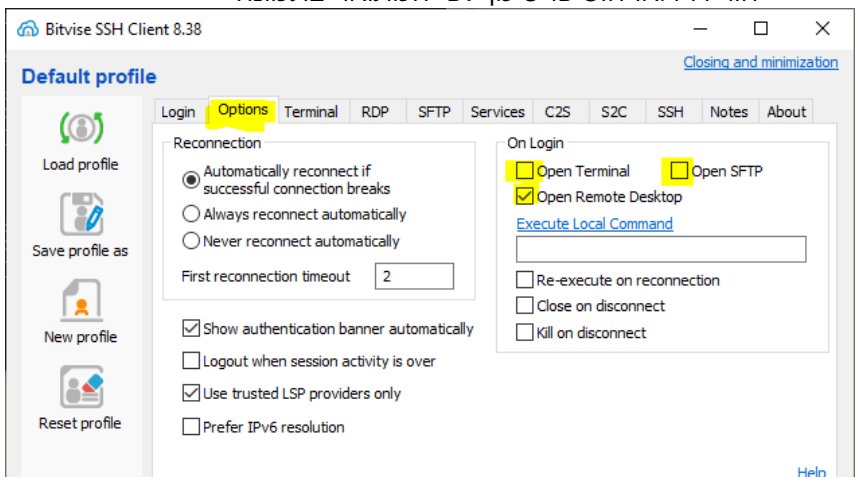


2. הפעילו את התוכנה ומלאו את פרטי שרת ההתחברות (מצורפת תמונת מסך).
לשונית LOGIN

Host: vpn.esc.biu.ac.il
Port: 2222
Username: < שם המשתמש בבר אילן >
Password: < סיסמתכם באוניברסיטה >



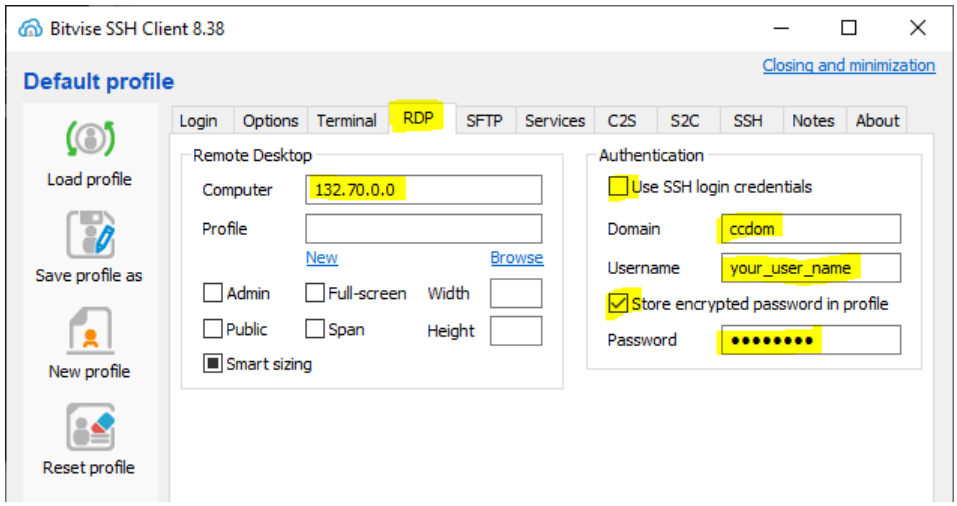
3. לשונית OPTIONS
הורידו ו/או הוסיפו סימן לפי המתואר בתמונה



4. לשונית RDP
בשדה **Computer** יש לרשום את כתובת ה **IP** של המחשב האישי במשרד (בהנחה שביצעתם מספר פעולות מקדימות – ראו הסבר בנספח למטה).

Domain: CCDOM
Username: < שם המשתמש בבר אילן >
Password: < סיסמתכם באוניברסיטה >

(ניתן להתחבר לטווח כתובות 132.70.x.x וכתובות 132.71.x.x)
כמוכן, ניתן להתחבר לשרת הפקולטה הבא (אשר משרת את כל הסטודנטים והסגל האקדמי והמנהלי):
phyts.ph.biu.ac.il
רק הערה לגבי השרת – לא לשמור שם מידע רגיש ו/או חשוב. המידע שנשמר שם יימחק ללא אפשרות לשחזור.



מקווה שהצלחתם.

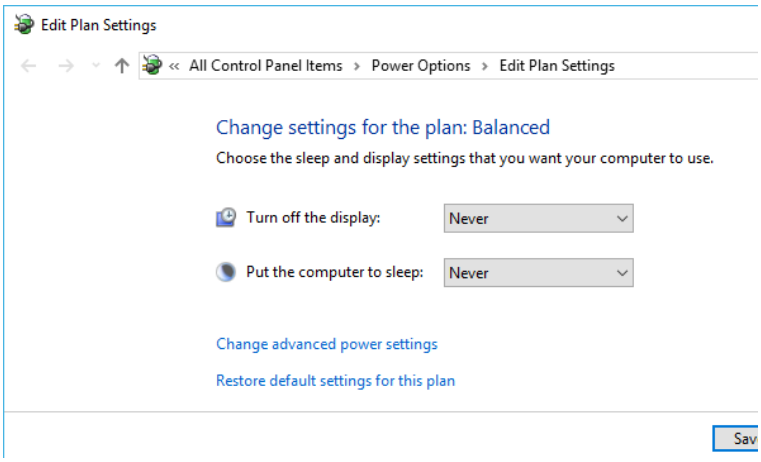
אבל, אם יש בעיות, ניתן לפנות אל צוות המחשוב דרך אתר הפקולטה: https://esc.biu.ac.il/unit_he_computing

או בדואר אלקטרוני.

בכבוד רב,
אדם מלול | צוות המחשוב
הפקולטה למדעים מדויקים

נספח: הנחיות לאפשר השתלטות על תחנות קצה

שינוי הגדרות צריכת חשמל:



1. להיכנס ל-Power& Sleep Settings
2. לבחור Power &Sleep.
3. לסמן ב-Screen את האופציה Never.
4. לסמן ב- Sleep את האופציה Never.

הוספת משתמש הקצה לקבוצה Remote Settings

1. יש לבצע קליק ימני על This Pc
2. לבחור Properties (בתפריט הנפתח, למטה)
3. לבחור Remote Settings (בטור השמאלי)
4. לגשת ללשונית Remote
5. לבחור באופציה ... Allow Remote Connections
6. יש להקיש על הכפתור Select Users
7. להוסיף את המשתמש שלכם במחשב לרשימת המורשים.
8. לאשר הכל OK .