# מדריך לניהול שולחן העבודה

## מחשבים שולחניים עסקיים

מק"ט מסמך: 361202-BB1

**מאי 2004**

מדריך זה מספק הגדרות והוראות לשימוש בתכונות האבטחה והניהול החכם שהותקנו מראש בדגמים נבחרים.

© 2004 כל הזכויות שמורות לחברת Hewlett-Packard Development, L.P.
המידע הכלול בזאת נתון לשינויים ללא הודעה מראש.

מיקרוסופט וחלונות הם סימנים מסחריים של חברת מיקרוסופט בארה״ב ובמדינות אחרות.

כתבי האחריות היחידים החלים על מוצרים ושירותים של HP מפורטים במפורש בהצהרות האחריות הנלוות לאותם מוצרים ושירותים. אין להבין מתוך הכתוב לעיל כי תחול על המוצר אחריות נוספת כלשהי. חברת HP לא תישא בכל אחריות שהיא לשגיאות טכניות או לשגיאות עריכה או להשמטות במסמך זה.

מסמך זה מכיל נתוני בעלות המעוגנים בזכויות יוצרים. אין להעתיק, לשכפל או לתרגם לשפה אחרת חלקים כלשהם ממסמך זה ללא אישור מראש ובכתב מחברת Hewlett-Packard.

**אזהרה:** טקסט המופיע בצורה זו מציין כי אי מילוי הוראות אלה עלול לגרום לנזק גופני חמור ואף למוות.

**זהירות:** טקסט המופיע בצורה זו מציין כי אי מילוי הוראות אלה עלול לגרום נזק לציוד, וכן לאובדן נתונים או מידע.

**מדריך לניהול שולחן העבודה**

מחשבים שולחניים עסקיים

מהדורה ראשונה: מאי 2004

מק"ט מסמך: 361202-BB1

# תוכן עניינים

## מדריך לניהול שולחן העבודה


הגדרת תצורה ראשונית ופריסה ..... 2
התקנת מערכת מרחוק ..... 3
עדכון וניהול תוכנות ..... 4
HP Client Manager Software (תוכנה לניהול לקוחות של HP) ..... 4
Altiris Client Management Solutions (פתרונות ניהול מחשבי לקוח של Altiris) ..... 4
מנהל תוכנת המערכת ..... 5
Proactive Change Notification (דיווח מראש על שינויים) ..... 6
Subscriber's Choice ..... 6
זיכרון הבזק ROM ..... 6
Remote ROM Flash (זיכרון הבזק ROM מרחוק) ..... 7
HPQFlash ..... 8
FailSafe Boot Block ROM ..... 8
שכפול ההגדרות ..... 10
לחצן הפעלה דו-מצבי ..... 19
אתר האינטרנט ..... 20
אבני בניין ושותפים ..... 20
בקרת נכסים ואבטחה ..... 21
אבטחה באמצעות סיסמה ..... 26
קביעת סיסמת הגדרות באמצעות Computer Setup (הגדרות המחשב) ..... 26
קביעת סיסמת הפעלה (Power-On) באמצעות Computer Setup (הגדרות המחשב) ..... 27
DriveLock ..... 32
Smart Cover Sensor (חיישן הכיסוי החכם) ..... 34
Smart Cover Lock (מנעול הכיסוי החכם) ..... 35
Master Boot Record Security (אבטחת רשומת אתחול ראשית) ..... 38
לפני הגדרת מחיצות או ביצוע פורמט של דיסק האתחול הנוכחי ..... 40
Cable Lock Provision (התקן מנעול כבל) ..... 40
טכנולוגיה לזיהוי טביעות אצבעות ..... 41
הודעות כשל והתאוששות ..... 41

Drive Protection System (מערכת להגנה על כוננים) ..... 41
עמידה בנחשולי מתח ..... 42
חיישן תרמי ..... 42

## אינדקס

# מדריך לניהול שולחן העבודה

ניהול חכם של HP מספק פתרונות המבוססים על סטנדרטים מקובלים לניהול ולבקרה על שולחנות עבודה, תחנות עבודה ומחשבי מחברת בסביבת רשת. בשנת 1995 הפכה חברת HP לחלוצה בכל הקשור ליכולת הניהול של שולחן העבודה, זאת הודות להשקה של ראשוני המחשבים האישיים שתמכו ביכולת ניהול מלאה. חברת HP מחזיקה בפטנט על טכנולוגיית יכולת הניהול (Manageability). מאז, הפכה חברת HP לחברה מובילה בתעשייה במאמציה לפתח סטנדרטים ותשתית הדרושים לפריסה, להגדרות תצורה ולניהול של שולחנות עבודה, תחנות עבודה ומחשבי מחברת. HP פועלת בשיתוף פעולה הדוק עם ספקי פתרונות ניהול כדי להבטיח תאימות בין טכנולוגיית הניהול החכם לבין מוצרים אלה. ניהול חכם מהווה נדבך חשוב בהתחייבות העמוקה שלנו לספק ללקוח פתרונות למשך כל מחזור החיים של המחשב, המסייעים במהלך ארבעת השלבים של תכנון, פריסה, ניהול והעברות.

להלן רשימת היכולות והתכונות המרכזיות של ניהול שולחן העבודה:

- הגדרת תצורה ראשונית ופריסה
- התקנת מערכת מרחוק
- עדכון וניהול תוכנה
- זיכרון הבזק ROM
- בקרת נכסים ואבטחה
- הודעות על מקרי כשל והתאוששות

תמיכה בתכונות ספציפיות המתוארות במדריך זה עלולה להשתנות לאור השוני בין דגמים וגרסאות תוכנה.

# הגדרת תצורה ראשונית ופריסה

המחשב מגיע עם תמונת תוכנת מערכת (system software image) מותקנת מראש. לאחר תהליך קצר של "הוצאת התוכנה מהאריזה", יהיה המחשב מוכן לשימוש.

ייתכן שתעדיף להחליף את תמונת התוכנה המותקנת מראש בתוכנת מערכת ויישומים מותאמים אישית. קיימות כמה שיטות לפריסת תמונת תוכנה מותאמת אישית. שיטות אלה כוללות:

- התקנת יישומי תוכנה נוספים לאחר פתיחת תמונת התוכנה המותקנת מראש.
- שימוש בכלים לפריסת תוכנה, כגון Altiris Deployment Solution™, להחלפת התוכנה המותקנת מראש בתמונת תוכנה מותאמת אישית.
- שכפול דיסק קשיח לצורך העתקת התוכן מכונן קשיח אחד למשנהו.

שיטת הפריסה הטובה ביותר תלויה בסביבת טכנולוגיית המידע שלך ובתהליכים שבהם אתה משתמש. סעיף PC Deployment (פריסת המחשב האישי) באתר HP Lifecycle Solutions (http://whp-sp-orig.extweb.hp.com/country/us/en/solutions.html) מספק מידע שיעזור לך לבחור את שיטת הפריסה הטובה ביותר.

תקליטור *שחזור פלוס!*, ההגדרות מבוססות ה-ROM וחומרת ACPI מספקים סיוע נוסף בנוגע לשחזור תוכנות מערכת, ניהול תצורה, איתור תקלות וניהול צריכת חשמל.

# התקנת מערכת מרחוק

התקנת המערכת מרחוק מאפשרת אתחול והגדרה של המערכת באמצעות שימוש בתוכנה ובנתוני הגדרת תצורה הנמצאים בשרת הרשת באמצעות הפעלת סביבת Preboot Execution Environment (PXE). תכונת התקנת המערכת מרחוק מופעלת בדרך כלל ככלי להתקנה ולהגדרה של תצורת המערכת, וניתן להשתמש בה לביצוע המטלות הבאות:

- פרמוט דיסק קשיח
- פריסת תמונת תוכנה במחשב אישי חדש אחד או יותר
- עדכון מרחוק של BIOS המערכת בזיכרון הבזק ROM ("Remote ROM Flash" בעמוד 7)
- קביעת תצורה של הגדרות BIOS המערכת

כדי להתחיל בהתקנת מערכת מרחוק, הקש **F12** עם הופעת ההודעה F12 = Network Service Boot בפינה הימנית התחתונה של מסך הלוגו של HP. פעל על פי ההוראות המוצגות על המסך כדי להמשיך את התהליך. סדר האתחול המשמש כברירת מחדל הוא הגדרת תצורה של ה-BIOS, שניתן לשנותה כך שהמערכת תמיד תנסה לבצע אתחול PXE.

HP ו-Altiris משתפות פעולה כדי לספק כלים שמטרתם להקל את משימת הפריסה של מחשבים ארגוניים ואת ניהולם, לצמצם את הזמן הנדרש לצרכים ניהוליים אלה, להקטין בצורה קיצונית את עלויות הבעלות ולהפוך את המחשבים האישיים של HP למחשבי הלקוח המציעים את יכולות הניהול הטובות ביותר בסביבות ארגוניות.

# עדכון וניהול תוכנות

HP מספקת כמה כלים לניהול ולעדכון התוכנה במחשבים שולחניים ובתחנות עבודה – HP Client Manager Software, Altiris Client Management Solutions, System Software Manager; Proactive Change Notification ו-Subscriber's Choice.

## HP Client Manager Software (תוכנה לניהול לקוחות של HP)

תוכנת HP Client Manager Software (HP CMS) מסייעת ללקוחות HP בניהול החומרה של מחשבי הלקוח שלהם. התכונות של תוכנה זו כוללות בין היתר:

- תצוגות מפורטות על מצאי החומרה לצורך ניהול נכסים
- בדיקות ניטור ואבחונים לגבי תקינות המחשב
- דיווח מראש לגבי שינויים בסביבת החומרה
- דיווחים דרך האינטרנט על פרטים עסקיים חשובים, כגון מחשבים עם אזהרות תרמיות, התראות זיכרון ועוד.
- עדכון מרחוק של תוכנת המערכת, כגון דרייברים להתקנים ו-ROM BIOS.
- שינוי מרחוק של סדר האתחול

למידע נוסף אודות HP Client Manager, בקר באתר http://h18000.www1.hp.com/im/client_mgr.html.

## Altiris Client Management Solutions (פתרונות ניהול מחשבי לקוח של Altiris)

HP ו-Altiris משתפות פעולה כדי לספק פתרונות ניהול מערכת משולבים ומקיפים, להפחתת העלויות הכרוכות בבעלות על מחשבי לקוח של HP.

תוכנה זו מהווה בסיס לפתרונות נוספים לניהול מחשבי לקוח, המטפלים בין היתר בנושאים הבאים:

- ניהול מצאי ונכסים
  - ❑ תאימות לרישיון SW
  - ❑ מעקב אחר המחשב ודיווח
  - ❑ הסכם חכירה, תיקון בקרת נכסים
- פריסה והגירה

- ❑ הגירה ל- Microsoft Windows XP Professional או Home Edition
- ❑ פריסת מערכת
- ❑ הגירה אישית

■ מרכז תמיכה ופתרון בעיות

- ❑ ניהול כרטיסי מרכז תמיכה
- ❑ איתור תקלות מרחוק
- ❑ פתרון בעיות מרחוק
- ❑ התאוששות מאסון של הלקוח

■ ניהול תוכנה ופעילויות

- ❑ ניהול רציף של שולחן העבודה
- ❑ פריסת SW של מערכת HP
- ❑ החלמה עצמית של יישום

לקבלת מידע ופרטים נוספים אודות אופן ההורדה של גרסת הערכה של הפתרונות של Altiris למשך 30 יום, הכוללת את כל הפונקציות, בקר באתר http://h18000.www1.hp.com/im/prodinfo.html#deploy.

דגמים נבחרים של מחשבים שולחניים ומחשבי מחברת כוללים את סוכן הניהול של Altiris כחלק מהתמונה המותקנת על-ידי היצרן. סוכן זה מאפשר לנהל תקשורת עם Altiris Development Solution (פתרון הפיתוח של Altiris) שיכול לשמש להשלמת פריסת חומרה חדשה או הגירת אישיות למערכת הפעלה חדשה באמצעות אשפים נוחים לשימוש. הפתרונות של Altiris מספקים יכולות הפצת תוכנה נוחות לשימוש. כאשר משתמשים ביכולות אלה יחד עם מנהל תוכנת המערכת, או עם HP Client Manager Software, מנהלי מערכת יכולים גם לעדכן את ה-BIOS של זיכרון ROM ואת תוכנות הדרייברים של ההתקנים מתוך מסוף מרכזי.

למידע נוסף, בקר בכתובת http://h18000.www1.hp.com/im/index.html.

# מנהל תוכנת המערכת

מנהל תוכנת המערכת (SSM) הוא כלי עזר המאפשר לך לעדכן תוכנות ברמת המערכת בכמה מחשבים בו-זמנית. כשמריצים את מנהל תוכנת המערכת במערכת של מחשבי לקוח, SSM מגלה הן את גרסת החומרה והן את גרסת התוכנה, ולאחר מכן מעדכן את התוכנה המתאימה באמצעות תוכנה הנלקחת מהארכיון המרכזי, הידוע גם כמחסן הקבצים. גרסאות דרייברים הנתמכות על-ידי SSM מצוינות בסמל מיוחד באתר הורדת הדרייברים ובתקליטור תוכנת התמיכה. להורדת כלי העזר או לקבלת מידע נוסף בנושא SSM, בקר בכתובת http://www.hp.com/go/ssm.

# Proactive Change Notification (דיווח מראש על שינויים)

התוכנית Proactive Change Notification משתמשת באתר האינטרנט Subscriber's Choice כדי לבצע מראש ובאופן אוטומטי את הפעולות הבאות:

- שליחת הודעות דואר אלקטרוני של Proactive Change Notification (PCN) המדווחות על שינויים ברכיבי חומרה ותוכנה ברוב המחשבים והשרתים המסחריים, עד 60 ימים מראש.
- שליחת הודעות דואר אלקטרוני הכוללות עלונים ללקוח, דפי עזר, הערות ללקוח, עלוני אבטחה והתראות על דרייברים לרוב המחשבים והשרתים המסחריים.

יצירת פרופיל אישי כדי להבטיח שרק אתה אישית תקבל את המידע הדרוש לסביבת טכנולוגיית מידע ספציפית. כדי ללמוד עוד על תוכנית Proactive Change Notification וליצור פרופיל מותאם אישית, בקר בכתובת http://h30046.www3.hp.com/subhub.php?jumpid=go/pcn.

## Subscriber's Choice

Subscriber's Choice הוא שירות מבוסס לקוח של HP. בהתאם לפרופיל שלך, HP תספק לך עצות אישיות לגבי מוצרים, מאמרים ו/או דרייברים והתראות/הודעות בנושא תמיכה. שירות הדרייברים וההתראות/הודעות בנושאי תמיכה ישלח לך הודעות דואר אלקטרוני, שידווחו לך כאשר המידע שאליו נרשמת כמנוי בפרופיל שלך יהיה זמין לעיון ואחזור. למידע נוסף על תוכנית Subscriber's Choice וליצירת פרופיל מותאם אישית, בקר בכתובת http://h30046.www3.hp.com/subhub.php.

## זיכרון הבזק ROM

המחשב האישי שלך כולל זיכרון הבזק ROM (זיכרון לקריאה בלבד) הניתן לתכנות. על-ידי הגדרת סיסמת הגדרות בכלי העזר Computer Setup (F10) (הגדרות המחשב), תוכל להגן על זיכרון ה-ROM מפני עדכון או מפני דריסה בלתי מכוונת. הדבר חשוב כדי להבטיח את שלמות פעולתו של המחשב האישי. אם תרצה לשדרג את זיכרון ה-ROM, תוכל:

- להזמין תקליטון עם ROMPaq™ משודרג מ-HP.
- להוריד תמונות עדכניות של ROMPaq מדף הדרייברים והתמיכה של HP, http://www.hp.com/support/files.

**זהירות:** כדי לספק הגנה מרבית לזיכרון ROM, דאג להגדיר סיסמת הגדרות. סיסמת ההגדרות מונעת שדרוגים לא מורשים של זיכרון ROM. System Software Manager מאפשר למנהל המערכת להגדיר סיסמת הגדרות במחשב אישי אחד או יותר בו-זמנית. למידע נוסף, בקר באתר http://www.hp.com/go/ssm.

## Remote ROM Flash (זיכרון הבזק ROM מרחוק)

Remote ROM Flash (זיכרון הבזק ROM מרחוק) מאפשר למנהל המערכת לשדרג בצורה בטוחה את זיכרון ROM במחשבי HP מרוחקים, ישירות מתוך מסוף ניהול רשת מרכזית. יכולתו של מנהל המערכת לבצע משימה זו מרחוק, במחשבים מרובים, מאפשרת פריסה עקבית ושליטה טובה יותר בתמונות זיכרון ROM במחשבי HP דרך הרשת. כמו כן, היא מאפשרת להגביר את התפוקה ולצמצם בעלויות הבעלות.

כדי לנצל את Remote ROM Flash, המחשב האישי צריך להיות דולק, או שיש להפעילו באמצעות יקיצה מרחוק (Remote Wakeup).

לקבלת מידע נוסף אודות Remote ROM Flash, עיין בתוכנות HP Client Manager Software או System Software Manager בכתובת http://h18000.www1.hp.com/im/prodinfo.html.

## HPQFlash

כלי העזר HPQFlash משמש לעדכון מקומי או לשחזור זיכרון מערכת במחשבים יחידים, באמצעות מערכת ההפעלה חלונות.

למידע נוסף אודות HPQFlash, בקר בכתובת http://www.hp.com/support/files והזן את שם המחשב כאשר תוצג לך בקשה לכך.

## FailSafe Boot Block ROM

FailSafe Boot Block ROM מאפשר לבצע שחזור מערכת במקרים נדירים של כשל זיכרון ההבזק, למשל, אם התרחשה נפילת מתח בזמן שדרוג ROM. ה-Boot Block (בלוק אתחול) הוא אזור מוגן-הבזק של הזיכרון, המוודא את תקפות זיכרון ההבזק של המערכת עם התחלת אספקת המתח למערכת.

- אם זיכרון המערכת תקין, המערכת מתחילה לפעול כרגיל.
- אם זיכרון המערכת נכשל בבדיקות התקינות, FailSafe Boot Block ROM מספק תמיכה מספקת לצורך אתחול המערכת מתקליטון ROMPaq, המתכנת את זיכרון המערכת לתצורה הרצויה.

דגמים אחדים תומכים גם בשחזור מתקליטור ROMPaq. תמונות ISO ROMPaq נכללות בדגמים נבחרים בגרסאות ROM softpaqs הניתנות להורדה.

כשתוכנת האתחול מזהה זיכרון מערכת לא תקף, נורת ההפעלה מהבהבת 8 פעמים בשנייה באור אדום, עם הפסקה של 2 שניות. כמו כן נשמעים 8 צפצופים ברציפות. הודעת שחזור של בלוק אתחול מופיעה על המסך (בדגמים מסוימים).

כדי לאפשר למערכת להתאושש, לאחר שזו נכנסת למצב Boot Block recovery, פעל על פי הצעדים הבאים:

1. אם בכונן התקליטונים נמצא תקליטון או בכונן התקליטורים נמצא תקליטור, הוצא את התקליטון והתקליטור וכבה את המחשב.
2. הכנס תקליטון ROMPaq לכונן התקליטונים, או אם ניתן במחשב זה, תקליטור ROMPaq לכונן התקליטורים.
3. הדלק את המחשב.

אם לא נמצא תקליטון ROMPaq או תקליטור ROMPaq, תתבקש להכניס תקליטון או תקליטור ולהפעיל מחדש את המחשב.

אם הוגדרה סיסמת הגדרות, נורת Caps Lock תידלק, ותתבקש להזין את הסיסמה.

4. הזן את סיסמת ההגדרות.

אם המערכת אותחלה בהצלחה מהתקליטון וביצעה בהצלחה תכנות מחדש של הזיכרון, שלוש הנורות שבמקלדת יידלקו. גם סדרה של צפצופים המתחזקים והולכים תציין את השלמת הפעולה בהצלחה.

5. הוצא את התקליטון או התקליטור וכבה את המחשב.

6. הדלק את המחשב ואתחל אותו.

הטבלאות הבאות מציגות את צירופי הנורות השונים במקלדת המשמשים לצורך ROM בלוק האתחול (Boot Block ROM) (כשמקלדת PS/2 מחוברת למחשב), ומסבירות את המשמעות והפעולה הקשורות לכל צירוף כזה.

**צירופי נורות מקלדת הנמצאים בשימוש על-ידי Boot Block ROM**

| מצב FailSafe Boot Block | צבע נורות המקלדת | פעילות נורות המקלדת | מצב/הודעה |
|---|---|---|---|
| Num Lock | ירוק | דולקות | תקליטון ROMPaq או תקליטור ROMPaq לא נמצא, אינו תקין או שהכונן אינו מוכן. |
| Caps Lock | ירוק | דולקות | הזן סיסמה. |
| Num, Caps, Scroll Lock | ירוק | מהבהבות בזו אחר זו, אחת בכל פעם – N, C, SL | המקלדת נעולה במצב רשת. |
| Num, Caps, Scroll Lock | ירוק | דולקות | Boot Block ROM Flash הושלם בהצלחה. כבה את המחשב ולאחר מכן אתחל אותו. |

נורות האבחון אינן נדלקות במקלדות USB.

# שכפול ההגדרות

ההליכים הבאים מאפשרים למנהל המערכת יכולת להעתיק בקלות רבה תצורת הגדרות מערכת אחת למחשבים אישיים אחרים מאותו דגם. הדבר מאפשר לבצע הגדרת תצורה מהירה ועקבית של מחשבים מרובים.

שני ההליכים מחייבים כונן תקליטורים או התקן USB flash media נתמך, כגון HP Drive Key.

## העתקה למחשב אחד

**זהירות:** תצורת ההגדרות ספציפית לכל דגם. מערכת הקבצים עשויה להיפגם אם מחשב המקור ומחשב היעד אינם מאותו דגם. לדוגמה, אין להעתיק את תצורת ההגדרות ממחשב dc7100 Ultra-slim Desktop למחשב dx6100 Slim Tower.

1. בחר תצורת הגדרות להעתקה. כבה את המחשב. אם אתה במערכת ההפעלה חלונות, לחץ על **'התחל'** > **'כיבוי'** > **'כיבוי'**.
2. אם אתה משתמש בהתקן USB flash media, הכנס אותו כעת.
3. הדלק את המחשב.
4. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup (הגדרות המחשב). במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

5. אם אתה משתמש בתקליטון, הכנס אותו כעת.
6. לחץ על **File (קובץ)** > **Replicated Setup (הגדרות משוכפלות)** > **Save to Removable Media (שמור במדיה נשלפת).** בצע את ההוראות המוצגות על המסך כדי ליצור את תקליטון התצורה או את התקן USB flash media.
7. כבה את המחשב שיש להגדיר, והכנס את תקליטון התצורה או את התקן USB flash media.

8. הדלק את המחשב שיש להגדיר.
9. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup (הגדרות המחשב). במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.
10. לחץ על **File (קובץ)** > **Replicated Setup (הגדרות משוכפלות)** > **Restore from Removable Media (שחזר ממדיה נשלפת)**, ולאחר מכן בצע את ההוראות המוצגות על המסך.
11. הפעל מחדש את המחשב לאחר השלמת קביעת התצורה.

# העתקה למחשבים מרובים

**זהירות:** תצורת ההגדרות ספציפית לכל דגם. מערכת הקבצים עשויה להיפגם אם מחשב המקור ומחשב היעד אינם מאותו דגם. לדוגמה, אין להעתיק את תצורת ההגדרות ממחשב dc7100 Ultra-slim Desktop למחשב dx6100 Slim Tower.

בשיטה זו דרוש מעט יותר זמן להכנת תקליטון התצורה או התקן USB flash media, אך העתקת התצורה למחשבי היעד מהירה יותר באופן משמעותי.

להליך זה או ליצירת התקן USB flash media בר-אתחול דרוש תקליטון בר-אתחול. אם לא ניתן להשתמש בחלונות XP ליצירת תקליטון בר-אתחול, השתמש בשיטה להעתקה למחשב אחד (ראה "העתקה למחשב אחד" בעמוד 10).

1. צור תקליטון בר-אתחול או התקן USB flash media. ראה "התקני USB Flash Media נתמכים" בעמוד 13 או "התקני USB Flash Media שאינם נתמכים, בעמוד 16.

**זהירות:** לא כל המחשבים ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בכלי העזר Computer Setup (F10) (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח, ניתן לאתחל את המחשב מהתקן USB Flash Media. אחרת, יש להשתמש בתקליטון בר-אתחול.

2. בחר תצורת הגדרות להעתקה. כבה את המחשב. אם אתה במערכת ההפעלה חלונות, לחץ על **'התחל'** > **'כיבוי'** > **'כיבוי'**.
3. אם אתה משתמש בהתקן USB flash media, הכנס אותו כעת.
4. הדלק את המחשב.

5. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup (הגדרות המחשב). במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

6. אם אתה משתמש בתקליטון, הכנס אותו כעת.
7. לחץ על **File (קובץ)** > **Replicated Setup (הגדרות משוכפלות)** > **Save to Removable Media (שמור במדיה נשלפת).** בצע את ההוראות המוצגות על המסך כדי ליצור את תקליטון התצורה או את התקן USB flash media.
8. הורד כלי עזר של BIOS לשכפול ההגדרות (repset.exe) והעתק אותו לתקליטון התצורה או להתקן USB flash media. להשגת כלי עזר זה, בקר בכתובת http://welcome.hp.com/support/files והזן את מספר הדגם של המחשב.
9. בתקליטון התצורה או בהתקן USB flash media, צור קובץ autoexec.bat שמכיל את הפקודה הבאה:

   **repset.exe**

10. כבה את המחשב שיש להגדיר. הכנס את תקליטון התצורה, או את התקן USB flash media, והדלק את המחשב. כלי העזר של התצורה יופעל באופן אוטומטי.
11. הפעל מחדש את המחשב לאחר השלמת קביעת התצורה.

# יצירת התקן בר-אתחול

## התקני USB flash media נתמכים

התקנים נתמכים, כגון HP Drive Key או DiskOnKey, כוללים תמונה מותקנת מראש, כדי לפשט את תהליך הפיכתם לניתנים לאתחול. אם התקן USB flash media שנמצא בשימוש אינו כולל תמונה זו, השתמש בהליך המתואר בהמשך סעיף זה (ראה "התקני USB Flash Media שאינם נתמכים" בעמוד 16).

**זהירות:** לא כל המחשבים ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בכלי העזר Computer Setup (F10) (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח, ניתן לאתחל את המחשב מהתקן USB flash media. אחרת, יש להשתמש בתקליטון בר-אתחול.

כדי ליצור התקן USB flash media בר-אתחול, דרושים לך:

- אחת מהמערכות הבאות:
  - ❑ סדרת Business Desktop dc7100 של HP קומפאק
  - ❑ סדרת Business Desktop dx6100 של HP קומפאק
  - ❑ סדרת Business Desktop d530 של HP קומפאק - Ultra-slim Desktop, Small Form Factor או Convertible Minitower
  - ❑ Compaq Evo D510 Ultra-slim Desktop
  - ❑ Compaq Evo D510 Convertible Minitower/Small Form Factor

בהתאם ל-BIOS של כל מחשב, ייתכן שמערכות עתידיות יתמכו אף הן באתחול מהתקן USB flash media.

**זהירות:** אם אתה משתמש במחשב שונה מאלה המפורטים לעיל, ודא כי סדר האתחול המוגדר כברירת מחדל בכלי העזר Computer Setup (F10) (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח.

- אחד ממודולי האחסון הבאים:
  - ❑ 16MB HP Drive Key
  - ❑ 32MB HP Drive Key
  - ❑ 32MB DiskOnKey
  - ❑ 64MB HP Drive Key

- ❑ 64MB DiskOnKey
- ❑ 128MB HP Drive Key
- ❑ 128MB DiskOnKey
- ❑ 256MB HP Drive Key
- ❑ 256MB DiskOnKey

■ תקליטון DOS בר-אתחול עם התוכניות FDISK ו-SYS. אם התוכנית SYS אינה זמינה, ניתן להשתמש בתוכנית FORMAT, אך כל הקבצים הקיימים בהתקן USB flash media יאבדו.

1. כבה את המחשב.
2. הכנס את התקן USB flash media לאחת מיציאות ה-USB של המחשב, והסר את כל התקני אחסון ה-USB האחרים, פרט לכונני תקליטונים של USB.
3. הכנס תקליטון בר-אתחול עם FDISK.COM ו-SYS.COM או FORMAT.COM לכונן תקליטונים והדלק את המחשב כדי לבצע אתחול מתקליטון ה-DOS.
4. הפעל את **FDISK** מתוך שורת הפקודה A:\ על-ידי הקלדת **FDISK** והקשה על Enter. אם תתבקש, לחץ על **Yes (Y)** כדי להפעיל תמיכה בדיסקים גדולים.
5. הקש על **בחירה [5]** כדי להציג את הכוננים במערכת. התקן USB flash media יהיה הכונן שגודלו קרוב ביותר לגודל של **אחד** הכוננים המוצגים. בדרך כלל זה יהיה הכונן האחרון ברשימה. שים לב לאות הכונן.

כונן התקן USB flash media: _____

**זהירות:** אם הכונן אינו תואם להתקן USB flash media, אל תמשיך. במקרה כזה אתה עלול לאבד נתונים. חפש התקני אחסון נוספים בכל יציאות ה-USB. אם תאתר התקנים כאלה, הפעל את המחשב מחדש והמשך מצעד 4. אם לא תמצא אף התקן, ייתכן שהמערכת אינה תומכת בהתקן USB flash media, או שהתקן USB flash media פגום. **אין** להמשיך ולנסות להפוך את התקן USB flash media לבר-אתחול.

6. צא מ-FDISK על-ידי הקשה על מקש **Esc** כדי לחזור לשורת הפקודה A:\.
7. אם תקליטון DOS בר-האתחול מכיל את SYS.COM, עבור לצעד 8. אחרת, עבור לצעד 9.

8. בשורת הפקודה A:\, הזן :**SYS x**. כאשר x מייצג את אות הכונן שצוינה לעיל.

**זהירות:** ודא שהזנת את אות הכונן הנכונה עבור התקן USB flash media.

לאחר העברת קובצי המערכת, התוכנית SYS תחזור לשורת הפקודה A:\. עבור לצעד 13.

9. העתק קבצים שברצונך לשמור מהתקן USB flash media לספרייה זמנית בכונן אחר (לדוגמה, הדיסק הקשיח הפנימי של המחשב).
10. בשורת הפקודה A:\, הזן :**FORMAT /S X**. כאשר x מייצג את אות הכונן שצוינה לפני כן.

**זהירות:** ודא שהזנת את אות הכונן הנכונה עבור התקן USB flash media.

התוכנית FORMAT תציג אזהרה אחת או יותר, ותשאל אותך בכל פעם אם ברצונך להמשיך. הקש **Y** בכל פעם. התוכנית FORMAT תפרמט את התקן USB flash media, תוסיף את קובצי המערכת ותבקש תווית לאמצעי האחסון.

11. הקש על **Enter** אם אינך מעוניין בתווית, או הזן תווית, אם רצונך בכך.
12. העתק קבצים ששמרת בשלב 9 בחזרה להתקן USB flash media.
13. הוצא את התקליטון והפעל את המחשב מחדש. המחשב יבצע אתחול מהתקן USB flash media ככונן C.

סדר האתחול המוגדר כברירת מחדל משתנה ממחשב למחשב, וניתן לשנותו בכלי העזר Computer Setup (F10) (הגדרות המחשב).

אם השתמשת בגרסת DOS מתוך חלונות 9x, ייתכן שתראה את מסך הלוגו של חלונות למשך זמן קצר. אם אינך רואה מסך זה, הוסף קובץ באורך אפס בשם LOGO.SYS לספריית השורש של התקן USB flash media.

חזור לסעיף "העתקה למחשבים מרובים" בעמוד 11.

## התקני USB Flash Media שאינם נתמכים

**זהירות:** לא כל המחשבים ניתנים לאתחול מהתקן USB flash media. אם סדר האתחול בכלי העזר Computer Setup (F10) (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח, ניתן לאתחל את המחשב מהתקן USB Flash Media. אחרת, יש להשתמש בתקליטון בר-אתחול.

כדי ליצור התקן USB flash media בר-אתחול, דרושים לך:

- אחת מהמערכות הבאות:
  - ❑ סדרת Business Desktop dc7100 של HP קומפאק
  - ❑ סדרת Business Desktop dx6100 של HP קומפאק
  - ❑ סדרת Business Desktop d530 של HP קומפאק - Ultra-slim Desktop, Small Form Factor או Convertible Minitower
  - ❑ Compaq Evo D510 Ultra-slim Desktop
  - ❑ Compaq Evo D510 Convertible Minitower/Small Form Factor

בהתאם ל-BIOS של כל מחשב, ייתכן שמערכות עתידיות יתמכו אף הן באתחול מהתקן USB flash media.

**זהירות:** אם אתה משתמש במחשב שונה מאלה המפורטים לעיל, ודא כי סדר האתחול המוגדר כברירת מחדל בכלי העזר Computer Setup (F10) (הגדרות המחשב) מציין את התקן ה-USB לפני הדיסק הקשיח.

- תקליטון DOS בר-אתחול עם התוכניות FDISK ו-SYS. אם התוכנית SYS אינה זמינה, ניתן להשתמש בתוכנית FORMAT, אך כל הקבצים הקיימים בהתקן USB flash media יאבדו.

1. אם קיימים כרטיסי PCI במערכת, שמחוברים אליהם כונני SCSI, ATA RAID או SATA, כבה את המחשב ונתק את חוט החשמל.

**זהירות:** חוט החשמל חייב להיות מנותק.

2. פתח את המחשב והוצא את כרטיסי ה-PCI.
3. הכנס את התקן USB flash media לאחת מיציאות ה-USB של המחשב, והסר את כל התקני אחסון ה-USB האחרים, פרט לכונני תקליטונים של USB. סגור את כיסוי המחשב.

4. חבר את חוט החשמל והדלק את המחשב.
5. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup (הגדרות המחשב). במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

---

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

---

6. עבור ל-**Advanced (מתקדם)** > **PCI devices (התקני PCI)** כדי להשבית את בקרי PATA ו-SATA. בעת השבתת בקר SATA, שים לב ל-IRQ שאליו מוקצה הבקר. יהיה עליך להקצות מחדש את ה-IRQ בשלב מאוחר יותר. יציאה מתוכנית ההגדרות מאשרת את השינויים.
SATA IRQ: _____
7. הכנס תקליטון בר-אתחול עם FDISK.COM ו-SYS.COM או FORMAT.COM לכונן תקליטונים והדלק את המחשב כדי לבצע אתחול מתקליטון ה-DOS.
8. הפעל את FDISK ומחק מחיצות קיימות בהתקן USB flash media. צור מחיצה חדשה וסמן אותה כפעילה. צא מ-FDISK על-ידי הקשה על מקש **Esc**.
9. אם לא מתבצעת הפעלה מחדש של המערכת לאחר יציאה מ-FDISK, הקש **Ctrl+Alt+Del** כדי לבצע אתחול מתקליטון DOS.
10. בשורת הפקודה A:\, הקלד **FORMAT C: /S** והקש על **Enter**. התוכנית FORMAT תפרמט את התקן USB flash media, תוסיף את קובצי המערכת ותבקש תווית לאמצעי האחסון.
11. הקש **Enter** אם אינך מעוניין בתווית, או הזן תווית, אם רצונך בכך.
12. כבה את המחשב ונתק את חוט החשמל. פתח את המחשב והתקן מחדש את כרטיסי PCI שהוצאת לפני כן. סגור את כיסוי המחשב.
13. חבר את חוט החשמל, הוצא את התקליטון והדלק את המחשב.

14. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup (הגדרות המחשב). במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.
15. עבור ל-**Advanced (מתקדם)** > **PCI Devices (התקני PCI)** והפעל מחדש את בקר PATA ו-SATA שהשבתת בצעד 6. הקצה לבקר SATA את ה-IRQ המקורי שלו.
16. שמור שינויים וצא. המחשב יבצע אתחול מהתקן USB flash media ככונן C.

סדר האתחול המוגדר כברירת מחדל משתנה ממחשב למחשב, וניתן לשנותו בכלי העזר Computer Setup (הגדרות המחשב). להוראות, עיין ב*מדריך ל-Computer Setup (הגדרות המחשב)* ב-*Documentation CD* (תקליטור התיעוד).

אם השתמשת בגרסת DOS מתוך חלונות 9x, ייתכן שתראה את מסך הלוגו של חלונות למשך זמן קצר. אם אינך רואה מסך זה, הוסף קובץ באורך אפס בשם LOGO.SYS לספריית השורש של התקן USB flash media.

חזור לסעיף "העתקה למחשבים מרובים" בעמוד 11.

# לחצן הפעלה דו-מצבי

כאשר Advanced Configuration and Power Interface (ACPI) מופעל, לחצן ההפעלה יכול לפעול הן כלחצן הפעלה/כיבוי והן כלחצן המתנה. תכונת ההמתנה אינה מכבה את המחשב באופן מלא, אלא גורמת לו להיכנס למצב המתנה תוך כדי צריכת מתח נמוכה. דבר זה מאפשר לך להוריד במהירות את צריכת המתח ללא סגירת היישומים, ולחזור במהירות למצב הפעלה רגיל מבלי לאבד נתונים.

כדי לשנות את תצורת לחצן ההפעלה, פעל לפי הצעדים הבאים:

1. לחץ לחיצה שמאלית על לחצן **'התחל'**, לאחר מכן בחר **'לוח הבקרה'** > **'אפשרויות צריכת חשמל'**.
2. בחלון **'מאפייני אפשרויות צריכת חשמל'**, לחץ על הכרטיסייה **'מתקדם'**.
3. ב**'לחצן הפעלה'**, בחר באפשרות **'המתנה'**.

לאחר שלחצן ההפעלה מוגדר לתפקד כלחצן המתנה, לחץ על לחצן ההפעלה כדי להעביר את המערכת למצב צריכת המתח הנמוכה ביותר (מצב המתנה). לחץ שוב על הלחצן כדי להחזיר את המערכת במהירות ממצב המתנה למצב פעולה מלא. כדי לנתק לחלוטין את המתח מהמערכת, לחץ על לחצן ההפעלה ברציפות במשך 4 שניות.

**זהירות:** אין להשתמש בלחצן ההפעלה לכיבוי המחשב, אלא אם כן המערכת אינה מגיבה. כיבוי המחשב ללא התערבות מערכת ההפעלה עלול לגרום לנזק או לאובדן נתונים בדיסק הקשיח.

## אתר האינטרנט

מהנדסי HP מבצעים בדיקות וניפוי שגיאות קפדני לכל תוכנה של HP ושל ספקי צד שלישי, ומפתחים תוכנות תמיכה מיוחדות למערכת ההפעלה כדי להבטיח רמה מיטבית של ביצועים, תאימות ואמינות למחשבים אישיים תוצרת HP.

כשעוברים למערכת הפעלה חדשה או משופרת, חשוב להשתמש בתוכנת התמיכה שפותחה למערכת הפעלה זו. אם אתה מתכנן להריץ גרסת חלונות של מיקרוסופט השונה מהגרסה המותקנת במחשב, עליך להתקין דרייברים להתקנים וכלי עזר מתאימים, כדי להבטיח תמיכה ותפקוד הולם של כל התכונות הנתמכות.

חברת HP הקלה את משימות האיתור, הגישה, ההערכה וההתקנה של תוכנת התמיכה החדשה. תוכל להוריד את התוכנה באתר http://www.hp.com/support.

אתר האינטרנט כולל דרייברים להתקנים, כלי עזר ותצורות זיכרון הבזק עדכניים, הדרושים לצורך הרצת גרסת חלונות המתקדמת ביותר במחשב HP שברשותך.

## אבני בניין ושותפים

פתרונות הניהול של HP משתלבים עם יישומי ניהול של מערכות אחרות, המבוססים על סטנדרטים מקובלים בשוק, כגון:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Wake on LAN Technology (טכנולוגיית יקיצה ברשת)
- ACPI
- SMBIOS
- תמיכה ב-Pre-boot Execution (PXE) (ביצוע קדם-אתחול).

# בקרת נכסים ואבטחה

תכונות בקרת נכסים הנכללות במחשב מספקות נתוני מעקב אחר נכסים שניתן לנהלם באמצעות HP Systems Insight Manager, HP Client Manager או יישומי ניהול מערכת אחרים. שילוב אוטומטי וחלק בין תכונות בקרת הנכסים ומוצרים אלה מאפשר לך לבחור את כלי הניהול המתאים ביותר לסביבת העבודה, ולמנף את ההשקעה שבוצעה בכלים הקיימים.

HP מציעה גם כמה פתרונות לבקרת גישה לרכיבים ומידע חשובים במחשב. כאשר ProtectTools Embedded Security מותקן, הוא מונע גישה לא מורשית לנתונים, בודק את תקינות המערכת ומבצע אימות של משתמשי צד שלישי המנסים לבצע גישה למערכת. (למידע נוסף, עיין *במדריך HP ProtectTools Embedded Security, ב-Documentation CD* (תקליטור התיעוד)). תכונות אבטחה הנכללות בדגמים מסוימים, כגון ProtectTools, Smart Cover Sensor (חיישן הכיסוי החכם) ו-Smart Cover Lock (מנעול הכיסוי החכם), מסייעות למנוע גישה לא מורשית לרכיבים פנימיים במחשב. באמצעות השבתת חיבורים מקביליים, טוריים או חיבורי USB, או באמצעות השבתת יכולת אתחול אמצעי אחסון שליפים, ניתן לספק הגנה לנתונים חשובים. את ההתראות על שינויי זיכרון והתראות חיישן הכיסוי החכם ניתן להעביר אוטומטית הלאה ליישומי ניהול מערכת במטרה למסור הודעות מוקדמות על ניסיונות חדירה למרכיבים הפנימיים של המחשב.

התכונות ProtectTools, Smart Cover Sensor ו-Smart Cover זמינות כרכיבים אופציונליים במערכות נבחרות.

השתמש בכלי העזר הבאים כדי לנהל את הגדרות האבטחה במחשב HP:

- באופן מקומי, באמצעות שימוש בכלי העזר Computer Setup (הגדרות המחשב). ראה *מדריך לכלי העזר Computer Setup הגדרות המחשב (F10)* ב-*Documentation CD* (תקליטור התיעוד), שסופק יחד עם המחשב, לקבלת מידע נוסף והוראות לשימוש בכלי העזר Computer Setup.
- מרחוק, באמצעות תוכנת HP Client Manager או System Software Manager. תוכנות אלה מאפשרות בקרה ופריסה מאובטחת ועקבית של הגדרות אבטחה מכלי עזר פשוט המופעל משורת הפקודה.

הטבלה והסעיפים הבאים מתייחסים לניהול מקומי של תכונות האבטחה של המחשב באמצעות שימוש בכלי העזר Computer Setup (הגדרות המחשב) (F10).

**מבט כללי על תכונות אבטחה**

| אפשרות | תיאור |
|---|---|
| Setup Password (סיסמת הגדרות) | מאפשרת להגדיר ולהפעיל סיסמת הגדרות (סיסמת מנהל מערכת).<br>אם הוגדרה סיסמה, היא נדרשת כדי לשנות אפשרויות בכלי העזר Computer Setup, לבצע הבזק זיכרון ולערוך שינויים בהגדרות חבר-והפעל מסוימות בסביבת חלונות.<br>למידע נוסף, ראה *מדריך לאיתור תקלות* ב-*Documentation CD* (תקליטור התיעוד). |
| Power-On Password (סיסמת הפעלה) | מאפשרת להגדיר ולהפעיל סיסמת הפעלה.<br>למידע נוסף, ראה *מדריך לאיתור תקלות* ב-*Documentation CD* (תקליטור התיעוד). |
| Password Options (אפשרויות של סיסמאות)<br>(אפשרות זו תופיע רק אם הוגדרה סיסמת הפעלה). | מאפשרת להגדיר אם לדרוש סיסמה עבור אתחול חם (**CTRL+ALT+DEL**).<br>למידע נוסף, ראה *מדריך לניהול שולחן העבודה* ב-*Documentation CD* (תקליטור התיעוד). |
| Pre-Boot Authorization (הרשאה לפני אתחול) | מאפשרת להפעיל/לבטל כרטיס חכם שישמש כתחליף לסיסמת הפעלה. |
| Smart Cover (כיסוי חכם) | מאפשרת לבצע את הפעולות הבאות:<br>• הפעלה/השבתה של מנעול הכיסוי החכם.<br>• הפעלה/השבתה של חיישן הסרת הכיסוי.<br>*הודעה למשתמש* מתריעה בפני המשתמש כי החיישן גילה שהכיסוי הוסר ממקומו. האפשרות *Setup Password* מחייבת להזין את סיסמת ההגדרות כדי לבצע אתחול של המחשב במקרה שהחיישן גילה שהכיסוי הוסר ממקומו.<br>תכונה זו נתמכת בדגמים נבחרים בלבד. למידע נוסף, ראה *מדריך לניהול שולחן העבודה* ב-*Documentation CD* (תקליטור התיעוד). |

למידע נוסף על Computer Setup, ראה *מדריך לכלי העזר Computer Setup (הגדרות המחשב) (F10)* בתקליטור התיעוד.

התמיכה בתכונות האבטחה עשויה להשתנות בהתאם לתצורת המחשב הספציפית.

*המשך*

**מבט כללי על תכונות אבטחה** *(המשך)*

| אפשרות | תיאור |
|---|---|
| Embedded Security (אבטחה משובצת) | מאפשרת לבצע את הפעולות הבאות:<br>• הפעלה/השבתה של התקן האבטחה המשובצת.<br>• איפוס ההתקן להגדרות היצרן.<br>תכונה זו נתמכת בדגמים נבחרים בלבד. למידע נוסף, ראה *מדריך HP ProtectTools Embedded Security*, ב-*Documentation CD* (תקליטור התיעוד). |
| Device Security (אבטחת התקנים) | הפעלה/השבתה של יציאות טוריות, יציאה מקבילית, יציאות USB קדמיות, שמע המערכת, בקרי רשת (בדגמים נבחרים), התקני MultiBay (בדגמים נבחרים) ובקרי SCSI (בדגמים נבחרים). |
| Network Service Boot (אתחול שירות רשת) | הפעלה/השבתה של יכולת המחשב לבצע אתחול ממערכת הפעלה המותקנת בשרת הרשת. תכונה זו קיימת בדגמי NIC בלבד; בקר הרשת חייב לשכון על אפיק PCI או שעליו להיות משובץ בלוח המערכת). |
| System Ids (זיהויי המערכת) | מאפשרת הגדרה של:<br>• תווית נכס (זיהוי של 18 בתים) ותווית בעלות (זיהוי של 80 בתים) המוצגות במהלך הבדיקה העצמית של המחשב.<br>למידע נוסף, ראה *מדריך לניהול שולחן העבודה* ב-*Documentation CD* (תקליטור התיעוד).<br>• מספר סידורי של המארז או מספר זיהוי אוניברסלי ייחודי (UUID). ניתן לעדכן את UUID רק אם המספר הסידורי הנוכחי של המארז אינו תקף. (מספרי זיהוי אלה נקבעים בדרך-כלל במפעל הייצור והם משמשים לזיהוי חד משמעי של המערכת).<br>הגדרות מקלדת מקומיות (לדוגמה, אנגלית או גרמנית) לצורך הכנסת זיהוי המערכת. |

למידע נוסף על Computer Setup, ראה *מדריך לכלי העזר Computer Setup (הגדרות המחשב) (F10)* בתקליטור התיעוד.

התמיכה בתכונות האבטחה עשויה להשתנות בהתאם לתצורת המחשב הספציפית.

*המשך*

**מבט כללי על תכונות אבטחה** *(המשך)*

| אפשרות | תיאור |
|---|---|
| DriveLock | מאפשרת להקצות או לשנות סיסמה ראשית או סיסמת משתמש לבחירה בדיסק קשיח מסוג MultiBay (אין תמיכה בדיסקים קשיחים מסוג SCSI). כשתכונה זו מופעלת, המשתמש מתבקש להזין את אחת מסיסמאות DriveLock בזמן הבדיקה העצמית של המחשב. אם אף סיסמה לא הוזנה בהצלחה, הדיסק הקשיח לא יהיה נגיש עד להזנת אחת הסיסמאות בהצלחה במהלך רצף האתחול הקר.<br>אפשרות זו תופיע רק במקרה שבו לפחות כונן MultiBay אחד, התומך בתכונת DriveLock, מחובר למערכת.<br>למידע נוסף, ראה *מדריך לניהול שולחן העבודה* ב-*Documentation CD* (תקליטור התיעוד). |
| Master Boot Record Security (אבטחת רשומת אתחול ראשית) | מאפשרת להפעיל או להשבית אבטחת רשומת אתחול ראשית (MBR).<br>כשאפשרות זו זמינה, BIOS דוחה את כל בקשות הכתיבה לרשומת האתחול הראשית על הדיסק בר-האתחול הנוכחי. עם כל הדלקה או אתחול של המחשב, משווה BIOS את רשומת האתחול הראשית בדיסק הקשיח המבצע אתחול לרשומת האתחול הראשית האחרונה שנשמרה. אם יתגלו שינויים, ניתן לשמור את רשומת האתחול הראשית לדיסק הקשיח המבצע אתחול, לחזור לרשומת האתחול הראשית האחרונה שנשמרה, או להשבית את אבטחת רשומת האתחול הראשית. תידרש להכניס סיסמת הגדרות, אם זו הוגדרה.<br>השבת את אבטחת רשומת האתחול הראשית לפני כל שינוי מכוון של פרמוט או חלוקת הדיסק בר-האתחול הנוכחי. כלי עזר אחדים (כגון FDISK ו-FORMAT) ינסו לעדכן את רשומת האתחול הראשית.<br>אם אבטחת רשומת האתחול הראשית זמינה, והגישות אל הדיסק מטופלות על-ידי BIOS, בקשות הכתיבה לרשומת האתחול הראשית יידחו, וכלי העזר ידווחו על שגיאות.<br>אם אבטחת רשומת האתחול הראשית זמינה, והגישות לדיסק מטופלות על-ידי מערכת ההפעלה, כל שינוי ברשומת האתחול הראשית יתגלה על-ידי BIOS במהלך האתחול הבא, ותוצג הודעת התראה של אבטחת רשומת האתחול הראשית. |

למידע נוסף על Computer Setup, ראה *מדריך לכלי העזר Computer Setup (הגדרות המחשב) (F10)* בתקליטור התיעוד.

התמיכה בתכונות האבטחה עשויה להשתנות בהתאם לתצורת המחשב הספציפית.

*המשך*

**מבט כללי על תכונות אבטחה** *(המשך)*

| אפשרות | תיאור |
|---|---|
| Save Master Boot Record (שמור רשומת אתחול ראשית) | שמירת עותק גיבוי של רשומת האתחול הראשית של הדיסק בר האתחול הנוכחי.<br>מופיע אך ורק אם אבטחת רשומת האתחול הראשית מופעלת. |
| Restore Master Boot Record (שחזור רשומת אתחול ראשית) | שחזור רשומת האתחול הראשית בדיסק בר האתחול הנוכחי.<br>אפשרות זו תופיע רק אם יתקיימו כל התנאים הבאים:<br>• אבטחת רשומת האתחול הראשית מופעלת.<br>• עותק גיבוי של רשומת האתחול הראשית כבר נשמר.<br>• דיסק האתחול הנוכחי הוא אותו דיסק שממנו נשמר עותק הגיבוי של רשומת האתחול הראשית.<br>△ **זהירות:** שחזור רשומת האתחול הראשית שכבר נשמרה לאחר שכלי עזר של הדיסק או מערכת ההפעלה שינו אותה, עלול להפוך את הנתונים בדיסק לבלתי נגישים. שחזר רשומת האתחול הראשית שנשמרה בעבר רק אם אתה בטוח כי רשומת האתחול הראשית של דיסק האתחול הנוכחי השתבשה או נפגעה מווירוס. |

למידע נוסף על Computer Setup, ראה *מדריך לכלי העזר Computer Setup (הגדרות המחשב) (F10)* בתקליטור התיעוד.

התמיכה בתכונות האבטחה עשויה להשתנות בהתאם לתצורת המחשב הספציפית.

# אבטחה באמצעות סיסמה

סיסמת ההפעלה מונעת שימוש לא חוקי במחשב בכך שהיא דורשת הזנת סיסמה לצורך גישה ליישומים או נתונים בכל פעם שמפעילים או מבצעים אתחול מחדש של המחשב האישי. סיסמת ההגדרות מיועדת במיוחד למניעת גישה לא חוקית להגדרות מערכת, וניתן להשתמש בה כדי לדרוס את סיסמת ההפעלה. כלומר, במקרה שנדרשים להזין סיסמת הפעלה, ניתן להזין במקום זאת את סיסמת ההגדרות, וכך תתאפשר גישה למחשב האישי.

ניתן להגדיר סיסמת הגדרות לכל הרשת כדי לאפשר למנהל הרשת להתחבר לכל המחשבים ברשת לצורכי תחזוקה, מבלי שיצטרך לדעת את סיסמאות ההפעלה שלהם, גם אם הוגדרו כאלה.

## קביעת סיסמת הגדרות באמצעות Computer Setup (הגדרות המחשב)

אם במערכת מותקן התקן אבטחה משובץ, עיין ב*מדריך HP ProtectTools Embedded Security*, ב-*Documentation CD* (תקליטור התיעוד). יצירת סיסמת הגדרות באמצעות Computer Setup, מונעת ביצוע שינויים בתצורת המחשב (שימוש בכלי העזרComputer Setup (הגדרות המחשב) (F10)) עד להזנת הסיסמה.

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעלה מחדש'**.
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

---

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

---

3. בחר באפשרות **Security** (אבטחה), ולאחר מכן בחר באפשרות **Setup Password** (סיסמת הגדרות) ובצע את ההוראות המוצגות על המסך.
4. לפני היציאה, בחר **File** (קובץ) > **Save Changes and Exit** (שמירת שינויים ויציאה).

## קביעת סיסמת הפעלה (Power-On) באמצעות Computer Setup (הגדרות המחשב)

קביעת סיסמת הפעלה באמצעות Computer Setup מונעת גישה למחשב לאחר הפעלתו, כל עוד לא הוזנה סיסמה. לאחר הגדרת סיסמת הפעלה, Computer Setup מציג את אפשרויות הסיסמה בתפריט Security (אבטחה). אפשרויות הסיסמה כוללות את Password Prompt on Warm Boot (בקשה להזנת סיסמה באתחול חם). כאשר התכונה בקשת Password Prompt on Warm Boot מופעלת, יש להזין את הסיסמה בכל פעם שהמחשב מופעל מחדש.

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעלה מחדש'**.
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. בחר בתפריט **Security** (אבטחה), לאחר מכן בחר **Power-On Password** (סיסמת הפעלה) ובצע את ההוראות המוצגות על המסך.
4. לפני היציאה, בחר **File** (קובץ) > **Save Changes and Exit** (שמירת שינויים ויציאה).

## הזנת סיסמת הפעלה

כדי להזין סיסמת הפעלה, בצע את הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. בחלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעל מחדש'**.
2. לאחר שסמל המפתח מופיע על המסך, הקלד את הסיסמה הנוכחית ולאחר מכן הקש על **Enter**.

הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.

אם טעית בהקלדת הסיסמה, יופיע סמל של מפתח שבור. נסה שנית. לאחר שלושה ניסיונות כושלים, יהיה עליך לכבות את המחשב ולהפעילו מחדש לפני שתוכל להמשיך.

## הזנת סיסמת הגדרות

אם במערכת מותקן התקן אבטחה משובץ, עיין ב*מדריך HP ProtectTools Embedded Security*, ב-*Documentation CD* (תקליטור התיעוד).

אם הוגדרה סיסמת הגדרות במחשב, תתבקש להזין סיסמה זו בכל פעם שבה תפעיל את הגדרות המחשב.

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעלה מחדש'**.
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. לאחר שסמל המפתח מופיע על המסך, הקלד את סיסמת ההגדרות הנוכחית ולאחר מכן הקש על **Enter**.

הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.

אם טעית בהקלדת הסיסמה, יופיע סמל של מפתח שבור. נסה שנית. לאחר שלושה ניסיונות כושלים, יהיה עליך לכבות את המחשב ולהפעילו מחדש לפני שתוכל להמשיך.

# שינוי סיסמת הפעלה או סיסמת הגדרות

אם במערכת מותקן התקן אבטחה משובץ, עיין ב*מדריך HP ProtectTools Embedded Security*, ב-*Documentation CD* (תקליטור התיעוד).

1. הדלק את המחשב או הפעל אותו מחדש. בחלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעל מחדש'**.
2. כדי לשנות את סיסמת ההפעלה, עבור לצעד 3.

   כדי לשנות את סיסמת ההגדרות, ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

---

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

---

3. לאחר הופעת סמל המפתח, הקלד את הסיסמה הנוכחית, קו נטוי (/) או תו הפרדה חלופי, סיסמה חדשה, קו נטוי (/) או תו הפרדה חלופי, והסיסמה החדשה שנית, לפי הדוגמה הבאה:
   **סיסמה נוכחית/סיסמה חדשה/סיסמה חדשה**

---

הקלד בזהירות; מטעמי אבטחה, התווים המוקלדים אינם מוצגים על המסך.

---

4. הקש על **Enter**.

בפעם הבאה שתפעיל את המחשב, הסיסמה החדשה תיכנס לתוקף.

---

לקבלת מידע לגבי תווי הפרדה חלופיים, עיין בסעיף "תווי הפרדה במקלדות של שפות שונות" בעמוד 31. ניתן לשנות את סיסמת ההפעלה וסיסמת ההגדרות על-ידי שימוש באפשרויות האבטחה ב-Computer Setup (הגדרות המחשב).

---

# מחיקת סיסמת הפעלה או סיסמת הגדרות

אם במערכת מותקן התקן אבטחה משובץ, עיין ב*מדריך HP ProtectTools Embedded Security*, ב-*Documentation CD* (תקליטור התיעוד).

1. הדלק את המחשב או הפעל אותו מחדש. בחלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעל מחדש'**.
2. כדי למחוק את סיסמת ההפעלה, עבור לצעד 3.

   כדי למחוק את סיסמת ההגדרות, ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. לאחר הופעת סמל המפתח, הקלד את הסיסמה הנוכחית שלך ואחריה קו נטוי (/) או תו הפרדה חלופי לפי הדוגמה הבאה:
   **'סיסמה נוכחית/'**
4. הקש על **Enter**.

לקבלת מידע לגבי תווי הפרדה חלופיים, עיין בסעיף "תווי הפרדה במקלדות של שפות שונות" בהמשך פרק זה. ניתן לשנות את סיסמת ההפעלה וסיסמת ההגדרות על-ידי שימוש באפשרויות האבטחה ב-Computer Setup (הגדרות המחשב).

# תווי הפרדה במקלדות של שפות שונות

כל מקלדת מתוכננת כך שתתאים לדרישות המיוחדות של כל מדינה ומדינה. התחביר והמקשים שבהם תשתמש לשינוי או למחיקת הסיסמה, תלויים במקלדת שסופקה עם המחשב שלך.

**תווי הפרדה במקלדות של שפות שונות**

| | | | | | |
|---|---|---|---|---|---|
| ערבית | / | יוונית | - | רוסית | / |
| בלגית | = | עברית | . | סלובקית | - |
| BHCSY* | - | הונגרית | - | ספרדית | - |
| ברזילאית | / | איטלקית | - | שוודית/פינית | / |
| סינית | / | יפנית | / | שוויצרית | - |
| צ'כית | - | קוריאנית | / | טיוואנית | / |
| דנית | - | אמל"טית | - | תאי (תאילנדית) | / |
| צרפתית | ! | נורווגית | - | טורקית | . |
| צרפתית-קנדית | é | פולנית | - | אנגלית (בריטניה) | / |
| גרמנית | - | פורטוגזית | - | אנגלית (ארה"ב) | / |

* עבור בוסניה-הרצגובינה, קרואטיה, סלובניה ויוגוסלביה.

# ביטול סיסמאות

אם שכחת את הסיסמה, לא תוכל להפעיל את המחשב. עיין ב*מדריך איתור תקלות* ב-*Documentation CD* (תקליטור התיעוד) לקבלת הוראות אודות ביטול סיסמאות.

אם במערכת מותקן התקן אבטחה משובץ, עיין ב*מדריך HP ProtectTools Embedded Security*, ב-*Documentation CD* (תקליטור התיעוד).

## DriveLock

DriveLock הוא תכונת אבטחה מקובלת בתעשייה המונעת גישה לא חוקית לנתונים בדיסקים קשיחים מסוג MultiBay. DriveLock מיושם כהרחבה להגדרות המחשב. אפשרות זו זמינה רק בעת זיהוי דיסקים קשיחים התומכים ב-DriveLock.

DriveLock מיועד ללקוחות HP שמייחסים חשיבות רבה לנושא אבטחת הנתונים. ללקוחות כאלה, עלות של דיסק קשיח היא זניחה בהשוואה לנזק העלול לנבוע מגישה לא חוקית לתוכן הדיסק הקשיח. כדי לאזן בין רמה גבוהה זו של אבטחה לבין הצורך השכיח לקבלת סיסמה שנשכחה, DriveLock מפעיל סכימת אבטחה בעלת שתי סיסמאות. סיסמה אחת מיועדת לשמש את מנהל המערכת, ואילו הסיסמה השנייה משמשת בדרך כלל את משתמש הקצה. אין שום דרך לשחרור הכונן אם שתי הסיסמאות אובדות. לכן, השימוש ב-DriveLock הוא הבטוח ביותר כשנתונים הנמצאים בדיסק הקשיח מועתקים במערכת מידע שיתופית, או כשהם מגובים באופן סדיר.

במקרה ששתי סיסמאות DriveLock נשכחו, לא ניתן יהיה להשתמש בדיסק הקשיח. לגבי משתמשים שאינם מתאימים לפרופיל הלקוחות המוגדר, הדבר עלול לגרום סיכון חמור. לגבי משתמשים המתאימים לפרופיל הלקוחות, הסיכון הוא סביר בהתחשב באופי הנתונים השמורים בדיסק הקשיח.

## שימוש ב-DriveLock

האפשרות DriveLock מופיעה בתפריט אבטחה שבהגדרות המחשב. למשתמש מוצגת אפשרות להגדיר את הסיסמה הראשית או להפעיל את DriveLock. יש להזין את סיסמת המשתמש כדי להפעיל את DriveLock. מכיוון שהגדרת התצורה הראשונית של DriveLock מבוצעת בדרך כלל על ידי מנהל המערכת, יש להגדיר תחילה סיסמה ראשית. HP מעודדת את מנהלי המערכת להגדיר סיסמה ראשית גם כשבכוונתם להפעיל את DriveLock, וגם כשבכוונתם להשבית את פעולתו. הדבר יספק למנהל המערכת יכולת לשנות את הגדרות DriveLock במקרה שהכונן יינעל בעתיד. לאחר הגדרת הסיסמה הראשית, מנהל המערכת יכול להחליט אם להפעיל את DriveLock או להמשיך להשבית אותו.

אם נמצא דיסק קשיח נעול, תדרוש הבדיקה העצמית של המחשב סיסמה כדי לשחרר את ההתקן. אם הוגדרה סיסמת הפעלה, והיא תואמת את סיסמת המשתמש של ההתקן, הבדיקה העצמית של המחשב לא תדרוש מהמשתמש להזין מחדש את הסיסמה. אחרת, יידרש המשתמש להזין סיסמת DriveLock. גם הסיסמה הראשית וגם סיסמת המשתמש מתאימות

למקרה זה. למשתמשים יינתנו שני ניסיונות להזין את הסיסמה הנכונה. אם שני הניסיונות ייכשלו, הבדיקה העצמית תמשיך להתבצע, אך הנתונים שבכונן לא יהיו זמינים.

## יישומי DriveLock

השימוש המעשי ביותר בתכונת האבטחה של DriveLock הוא בסביבה שיתופית, שבה מנהל המערכת מספק למשתמשים בדיסקים קשיחים של MultiBay לשימוש במחשבים מסוימים. מנהל המערכת אחראי להגדיר תצורת דיסק קשיח מסוג MultiBay, והדבר מחייב בין השאר להגדיר סיסמה ראשית של DriveLock. במקרה שהמשתמש שוכח את סיסמת המשתמש או שהציוד מועבר לעובד אחר, ניתן לעשות שימוש בסיסמה ראשית כדי להגדיר מחדש את סיסמת המשתמש ולזכות בגישה לדיסק הקשיח.

HP ממליצה כי מנהל מערכת שיתופית שיבחר להפעיל את DriveLock, יגדיר גם מדיניות שיתופית לצורך הגדרה ותחזוקה של סיסמאות ראשיות. הדבר חייב להתבצע כדי למנוע מצב שבו העובד יפעיל בשגגה או בזדון את שתי סיסמאות DriveLock לפני פרישתו מהחברה. בתרחיש כזה לא ניתן יהיה להשתמש בכונן הקשיח, ויהיה צורך להחליפו. באופן דומה, אם לא תוגדר סיסמה ראשית, יוכלו מנהלי המערכת לגלות אם הדיסק הקשיח נעול וכי אין ביכולתם לבצע בדיקות שגרתיות לתוכנה לא חוקית, פונקציות בקרת נכסים נוספות ופעולות תמיכה.

למשתמשים בעלי דרישות אבטחה חמורות פחות, HP אינה ממליצה להפעיל את DriveLock. משתמשים הנמצאים בקטגוריה זו כוללים משתמשים אישיים או משתמשים שאינם מחזיקים מידע יומיומי רגיש בדיסקים הקשיחים שלהם. למשתמשים אלה, קריסה אפשרית של הדיסק הקשיח כתוצאה משכיחת שתי הסיסמאות חשובה הרבה יותר מערך הנתונים ש-DriveLock נועד לאבטח. ניתן להגביל את הגישה להגדרות מערכת ול-DriveLock באמצעות סיסמת הגדרות. הגדרת סיסמת הגדרות מבלי למוסרה למשתמשי הקצה מאפשרת למנהלי המערכת להגביל את יכולת המשתמשים להפעיל את DriveLock.

## Smart Cover Sensor (חיישן הכיסוי החכם)

חיישן הסרת הכיסוי הקיים בדגמים מסוימים הוא צירוף של טכנולוגיות חומרה ותוכנה, המאפשר להציג התראות במקרה של הסרת כיסוי המחשב או לוח הצד. קיימות שלוש רמות הגנה, כמתואר בטבלה הבאה.

**רמות הגנה של חיישן הכיסוי החכם**

| רמה | הגדרה | תיאור |
|---|---|---|
| רמה 0 | Disabled (מושבת) | חיישן הכיסוי החכם מושבת (ברירת מחדל). |
| רמה 1 | Notify User (הודעה למשתמש) | כשהמחשב מופעל מחדש, מופיעה על הצג הודעה על כך שכיסוי המחשב או לוח הצד הוסרו. |
| רמה 2 | Setup Password (סיסמת הגדרות) | כשהמחשב מופעל מחדש, מופיעה על הצג הודעה על כך שכיסוי המחשב או לוח הצד הוסרו. יש להזין סיסמת הגדרות כדי להמשיך. |

הגדרות אלה ניתנות לשינוי באמצעות הגדרות המחשב. למידע נוסף על Computer Setup, ראה *מדריך לכלי העזר Computer Setup (הגדרות המחשב) (F10)* ב*תקליטור התיעוד*.

## הגדרת רמת ההגנה של חיישן הכיסוי החכם

כדי להגדיר את רמת האבטחה של חיישן הכיסוי החכם, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעלה מחדש'**.
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. בחר **Security (אבטחה)** > **Smart Cover (כיסוי חכם)** > **Cover Removal Sensor (חיישן הסרת הכיסוי)**, ובחר את רמת האבטחה הרצויה.
4. לפני היציאה, בחר **File (קובץ)** > **Save Changes and Exit (שמירת שינויים ויציאה)**.

## Smart Cover Lock (מנעול הכיסוי החכם)

Smart Cover Lock הוא מנעול כיסוי הנשלט על-ידי תוכנה, הנכלל בדגמים נבחרים של HP. נעילה זו מונעת גישה לא חוקית לרכיבים הפנימיים של המחשב. המחשבים מסופקים כאשר מנעול הכיסוי החכם נמצא במצב לא נעול.

**זהירות:** כדי להגיע לרמת האבטחה המרבית של מנעול הכיסוי החכם, הקפד להגדיר סיסמת הגדרות. סיסמת ההגדרות מונעת גישה בלתי מורשית לכלי העזר Computer Setup (הגדרות המחשב).

מנעול הכיסוי החכם זמין כרכיב אופציונלי בדגמים נבחרים.

# נעילת מנעול הכיסוי החכם

כדי להפעיל ולנעול את מנעול הכיסוי החכם, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל' > 'כיבוי המחשב' > 'הפעלה מחדש'.**
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. בחר באפשרות **Security (אבטחה) > Smart Cover (כיסוי חכם) > Cover Lock (כיסוי חכם) > Lock (נעילה).**
4. לפני היציאה, בחר **File (קובץ) > Save Changes and Exit (שמירת שינויים ויציאה)**.

# שחרור מנעול הכיסוי החכם

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל' > 'כיבוי המחשב' > 'הפעלה מחדש'**.
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. בחר באפשרות **Security (אבטחה) > Smart Cover (כיסוי חכם) > Cover Lock (כיסוי חכם) > Unlock (ביטול נעילה)**.
4. לפני היציאה, בחר **File (קובץ) > Save Changes and Exit (שמירת שינויים ויציאה)**.

## שימוש במפתח FailSafe (אל-כשל) של הכיסוי החכם

אם הפעלת את מנעול הכיסוי החכם, ואינך יכול להזין סיסמה כדי להשבית את המנעול, תצטרך מפתח אל-כשל לכיסוי החכם כדי לפתוח את כיסוי המחשב. יהיה עליך להשתמש במפתח בכל אחד מהמקרים הבאים:

- הפסקת חשמל
- כשל באתחול
- כשל של אחד מרכיבי המחשב האישי (כגון מעבד או ספק כוח)
- סיסמה שנשכחה

**זהירות:** מפתח FailSafe של הכיסוי החכם הוא כלי ייחודי המסופק על ידי HP. הזמן מראש מפתח זה לפני שתזדקק לו בפועל אצל סוכן מכירות מורשה או ספק שירות מורשה.

כדי לקבל את מפתח האל-כשל (FailSafe), בצע אחת מהפעולות הבאות:

- פנה לסוכן מכירות מורשה או לספק שירות מורשה של HP.
- התקשר למספר המופיע בכתב האחריות.

למידע נוסף אודות השימוש במפתח FailSafe לכיסוי החכם, עיין ב*מדריך חומרה* ב-*Documentation CD* (תקליטור התיעוד).

# Master Boot Record Security (אבטחת רשומת אתחול ראשית)

רשומת האתחול הראשית (Master Boot Record, MBR) כוללת מידע הנדרש לביצוע אתחול מוצלח מהדיסק וגישה לנתונים השמורים בדיסק. אבטחת רשומת האתחול הראשית מזהה שינויים שבוצעו בשגגה או בזדון ברשומת האתחול הראשית, כגון שינויים הנגרמים עקב וירוסים או שימוש לא נכון בעזרי דיסק מסוימים, ומדווחת עליהם. האבטחה מאפשרת גם לשחזר את רשומת האתחול הראשית התקינה האחרונה, במקרה שהמערכת תזהה כי בוצעו בה שינויים בעת הפעלה מחדש של המחשב.

כדי להפעיל אבטחת רשומת אתחול ראשית, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעלה מחדש'.**
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. בחר **Security (אבטחה)** > **Master Boot Record Security (אבטחת רשומת אתחול ראשית)** > **Enabled (מופעלת)**.
4. בחר **Security (אבטחה)** > **Save Master Boot Record (שמור את רשומת האתחול הראשית)**.
5. לפני היציאה, בחר **File (קובץ)** > **Save Changes and Exit (שמירת שינויים ויציאה)**.

כאשר אבטחת רשומת האתחול הראשית מופעלת, BIOS מונע ביצוע שינויים ברשומת האתחול הראשית של דיסק האתחול הנוכחי, כל זמן שהמחשב נמצא ב-MS-DOS או במצב בטוח בסביבת חלונות.

רוב מערכות ההפעלה שולטות בגישה לרשומת האתחול הראשית של דיסק האתחול הנוכחי; ל-BIOS אין אפשרות למנוע שינויים המתבצעים בזמן פעולת מערכת ההפעלה.

בכל פעם שמדליקים את המחשב או מפעילים אותו מחדש, ה-BIOS משווה את רשומת האתחול הראשית של דיסק האתחול הנוכחי לרשומת האתחול הראשית שנשמרה קודם. אם מתגלים שינויים ואם דיסק האתחול הנוכחי הוא אותו דיסק שבו נשמרה רשומת האתחול הראשית הקודמת, מוצגת ההודעה הבאה:

1999 - Master Boot Record has changed – (רשומת האתחול הראשית השתנתה).

הקש על מקש כלשהו כדי להיכנס להגדרות להגדיר את תצורת אבטחת רשומת האתחול הראשית.

עם הכניסה ל-Computer Setup (הגדרות המחשב), בצע את הצעדים הבאים:

- שמור את רשומת האתחול הראשית של דיסק האתחול הנוכחי.
- אחזר את רשומת האתחול הראשית שנשמרה קודם לכן, או
- השבת את תכונת אבטחת רשומת האתחול הראשית.
- עליך לדעת את סיסמת ההגדרות, אם היא קיימת.

אם מתגלים שינויים ואם דיסק האתחול הנוכחי **איננו** הדיסק שבו נשמרה רשומת האתחול הראשית לפני כן, תוצג ההודעה הבאה:

2000—Master Boot Record Hard Drive has changed (רשומת האתחול הראשית בדיסק הקשיח השתנתה).

הקש על מקש כלשהו כדי להיכנס להגדרות להגדיר את תצורת אבטחת רשומת האתחול הראשית.

עם הכניסה ל-Computer Setup (הגדרות המחשב), בצע את הצעדים הבאים:

- שמור את רשומת האתחול הראשית של דיסק האתחול הנוכחי, או
- השבת את תכונת אבטחת רשומת האתחול הראשית.

עליך לדעת את סיסמת ההגדרות, אם היא קיימת.

במקרה הבלתי סביר שרשומת האתחול הראשית שנשמרה קודם לכן נפגמה, תוצג ההודעה הבאה:

1998—Master Boot Record has been lost (רשומת האתחול הראשית אבדה).

הקש על מקש כלשהו כדי להיכנס להגדרות להגדיר את תצורת אבטחת רשומת האתחול הראשית.

עם הכניסה ל-Computer Setup (הגדרות המחשב), בצע את הצעדים הבאים:

- שמור את רשומת האתחול הראשית של דיסק האתחול הנוכחי, או
- השבת את תכונת אבטחת רשומת האתחול הראשית.

עליך לדעת את סיסמת ההגדרות, אם היא קיימת.

## לפני הגדרת מחיצות או ביצוע פורמט של דיסק האתחול הנוכחי

ודא שאבטחת רשומת האתחול הראשית מושבתת לפני ביצוע שינויים במחיצות או פרמוט דיסק האתחול הנוכחי. עזרי דיסק מסוימים, כגון FDISK ו-FORMAT, מנסים לעדכן את רשומת האתחול הראשית. אם אבטחת רשומת האתחול הראשית מופעלת בשעת ביצוע שינויים במחיצות או פורמט לדיסק, ייתכן שתתקבל הודעת שגיאה מכלי העזר של הדיסק, או אזהרה מאבטחת רשומת האתחול הראשית בפעם הבאה שהמחשב יודלק או יופעל מחדש. כדי להשבית את אבטחת רשומת האתחול הראשית, פעל לפי הצעדים הבאים:

1. הדלק את המחשב או הפעל אותו מחדש. במערכת ההפעלה חלונות, לחץ **'התחל'** > **'כיבוי המחשב'** > **'הפעלה מחדש'**.
2. ברגע שהמחשב נדלק, לחץ לחיצה ממושכת על מקש **F10** עד שתיכנס לכלי העזר Computer Setup. במקרה הצורך, הקש על **Enter** כדי לעקוף את מסך הפתיחה.

אם לא הקשת על **F10** בזמן המתאים, יהיה עליך להפעיל מחדש את המחשב וללחוץ לחיצה ממושכת פעם נוספת על מקש **F10** כדי לגשת לכלי העזר.

אם אתה משתמש במקלדת PS/2, ייתכן שתוצג לך הודעה על שגיאת מקלדת, התעלם מהודעה זו.

3. בחר **Security (אבטחה)** > **Master Boot Record Security (אבטחת רשומת אתחול ראשית)** > **Disabled (מבוטלת)**.
4. לפני היציאה, בחר **File (קובץ)** > **Save Changes and Exit (שמירת שינויים ויציאה)**.

## Cable Lock Provision (התקן מנעול כבל)

הלוח האחורי של המחשב כולל מנעול כבל, כך שניתן לאבטח את המחשב פיזית למשטח העבודה.

להוראות מלוות באיורים, אנא עיין ב*מדריך חומרה* שב-*Documentation CD* (תקליטור התיעוד).

## טכנולוגיה לזיהוי טביעות אצבעות

הטכנולוגיה לזיהוי טביעות האצבעות של HP מעלה את רמת האבטחה של הרשת באמצעות ביטול הצורך בהזנת סיסמת משתמש, מפשטת את תהליך ההתחברות לרשת ומצמצמת עלויות ניהול של רשתות שיתופיות. זוהי טכנולוגיה שמחיריה סבירים, ואינה מיועדת אך ורק לחברות היי-טק או ארגונים הדורשים רמת אבטחה גבוהה.

התמיכה בטכנולוגית זיהוי טביעות האצבעות משתנה מדגם לדגם.

לקבלת מידע נוסף, בקר בכתובת:

http://h18004.www1.hp.com/products/security/.

## הודעות כשל והתאוששות

תכונות דיווח על תקלות והתאוששות משלבות טכנולוגיה חדשנית של חומרה ותוכנה כדי למנוע אובדן של נתונים קריטיים וכדי להקטין למינימום הפסקות עבודה בלתי מתוכננות.

אם המחשב מחובר לרשת המנוהלת על-ידי HP Client Manager, המחשב שולח הודעה על כשל ליישום ניהול הרשת. באמצעות HP Client Manager Software, תוכל גם לתזמן מרחוק כלי אבחון, שיפעלו באופן אוטומטי בכל המחשבים המנוהלים, ויצרו דוח סיכום של כל הבדיקות שנכשלו.

## Drive Protection System (מערכת להגנה על כוננים)

Drive Protection System (DPS) (מערכת להגנה על כוננים) הוא כלי אבחון הנכלל בדיסקים קשיחים המותקנים במחשבים נבחרים של HP. מערכת הגנת הדיסק הקשיח נועדה לסייע באבחון תקלות, היכולות לגרום להחלפה בלתי מוצדקת של הדיסק הקשיח.

בתהליך ההרכבה של מחשבי HP, כל דיסק קשיח המותקן בהם עובר בדיקה באמצעות DPS, ורשומה קבועה עם פרטי המפתח נכתבת בכונן. בכל פעם שמריצים את DPS, תוצאות הבדיקה מאוחסנות בדיסק הקשיח. ספק השירות יכול להיעזר במידע זה לצורך אבחון הנסיבות שגרמו לך להריץ את תוכנת DPS. עיין ב*מדריך איתור תקלות* ב-*Documentation CD* (תקליטור התיעוד) לקבלת הוראות אודות השימוש ב-DPS.

## עמידה בנחשולי מתח

עמידה בנחשולי מתח מאפשרת אמינות גבוהה יותר במקרים שבהם המחשב האישי נפגע מנחשול מתח בלתי צפוי. אספקת מתח מסוג זה מתוכננת לעמוד בפני נחשולי מתח של עד 2000 וולט ללא קריסת מערכת או אובדן מידע כלשהו.

## חיישן תרמי

חיישן תרמי הוא תכונה המשלבת חומרה ותוכנה, העוקבת אחר הטמפרטורה הפנימית של המחשב. תכונה זו מציגה הודעת אזהרה אם חלה חריגה מהתחום הנורמלי, ובכך ניתן לך די זמן לנקוט פעולה לפני שייגרם נזק לרכיבים פנימיים ולפני שיאבדו נתונים.

# אינדקס


## א

אבטחה
  Drivelock, 31 ; 33
  MultiBay, 31 ; 33
  הגדרות, הגדרה, 21
  חיישן כיסוי חכם (Smart Cover Sensor), 33
  מנעול כיסוי חכם, 35
  סיסמה, 26
  רשומת אתחול ראשית, 38 ; 39
  תכונות, טבלה, 22
אבטחת MultiBay, 31 עד 33
אבטחת מנעול כיסוי, זהירות, 35
אבטחת רשומת אתחול ראשית, 38 עד 39
אמצעי זהירות
  אבטחת מנעול כיסוי, 35
  הגנה על זיכרון ROM 7
  מפתח אל-כשל, 37
אתרי אינטרנט
  Altiris, 5
  HP Client Manager, 4
  HPQFlash, 8
  Proactive Change Notification, 6
  Remote ROM Flash (זיכרון הבזק ROM מרחוק), 7
  ROM Flash (זיכרון הבזק ROM), 7
  Subscriber's Choice, 6
  זיהוי טביעות אצבעות, טכנולוגיה, 41
  טכנולוגיית זיהוי טביעות אצבעות, 41
  מנהל תוכנת מערכת (SSM), 6
  פריסת מחשב אישי, 2
  שכפול הגדרות, 12 ; 13
  תמונות ROMPaq, 7
  תמיכה בתוכנה, 20

## ב

ביטול סיסמה, 31
בקרת נכסים, 21

## ג

גישה למחשב, שליטה, 21

## ד

דיווח על כשל, 41
דיווח על שינוי, 6
דיסק, שכפול, 2
דיסקים קשיחים, כלי אבחון, 41

## ה

הגדרות מרחוק, 3
הגדרות
  ראשוניות, 2
  שכפול, 10
הגדרת לחצן הפעלה, 19
הגנה על דיסק קשיח, 41
הגנה על זיכרון ROM, זהירות, 7
הודעה על שינויים, 6
הזמנת מפתח אל-כשל, 37
הזנה
  סיסמת הגדרות, 28
  סיסמת הפעלה, 27
התאמה אישית של תוכנה, 2
התקן USB flash media, בר-אתחול, 13 ; 18
התקן בר-אתחול
  DiskOnKey, 13 ; 18
  HP Drive Key, 13 ; 18
  התקן USB flash media, 13 ; 18
  יצירה, 13 ; 18
התקן מנעול כבל, 40
התקנת מערכת מרחוק, גישה, 3

## ז

זיכרון מערכת לא תקף, 8

## ח

חיישן כיסוי חכם (Smart Cover Sensor), 33
  רמות הגנה, 33
  הגדרה, 35
חיישן תרמי, 42
חלוקת הדיסק למחיצות, מידע חשוב, 40

## ט

טכנולוגיית זיהוי טביעות אצבעות, 41
טמפרטורה פנימית של המחשב, 42

טמפרטורה פנימית של המחשב, 42

## כ

כונן, הגנה, 41
כיסוי חכם, מנעול, 35
כלי אבחון לדיסקים קשיחים, 41
כלי העזר Computer Setup (הגדרות מחשב) (F10)
כלי פריסה, תוכנה, 2
כלי שכפול, תוכנה, 2
כתובת URL (אתרי אינטרנט). ראה אתרי אינטרנט.
כתובת אינטרנט, ראה אתרי אינטרנט

## ל

לחצן הפעלה דו-מצבי, 19
לחצן הפעלה
  דו-מצבי, 19
  קביעת תצורה, 19

## מ

מחיקת סיסמה, 30
מנהל תוכנת מערכת (SSM), 6
מנעול כיסוי חכם, 35 עד 37
  נעילה, 36
  שחרור נעילה, 36
מפתח FailSafe (אל-כשל)
  הזמנה, 37
  זהירות, 37
מפתח אל-כשל לכיסוי חכם, הזמנה, 37

## נ

נורות מקלדת, ROM, טבלה, 9
נחשולי מתח, עמידה, 42
נעילת מנעול כיסוי חכם, 36

## ס

סיסמה
  אבטחה, 26
  ביטול, 31
  הגדרות, 26 ; 28
  הפעלה, 27
  מחיקה, 30
  שינוי, 29
סיסמת הגדרות
  הגדרה, 26
  הזנה, 28
  מחיקה, 30
  שינוי, 29

## ע

עמידה בנחשולי מתח, 42

## פ

פירמוט תקליטון, מידע חשוב, 40

## ש

שדרוג זיכרון ROM, 7
שחזור מערכת, 8
שחזור מערכת, 8
שחזור, תוכנה, 2
שחרור נעילת מנעול כיסוי חכם, 36
שינוי מערכות הפעלה, מידע חשוב, 20
שינוי מערכות הפעלה, מידע חשוב, 20
שינוי סיסמה, 29
שליטה על הגישה למחשב, 21
שפות שונות, תווי הפרדה של המקלדת, 30

## ת

תווי הפרדה של המקלדת, שפות שונות, 30
תווי הפרדה, טבלה, 30
תוכנה
  Drive Protection System (מערכת להגנה על כוננים), 41
  FailSafe Boot Block ROM, 8
  Remote ROM Flash (זיכרון הבזק ROM מרחוק), 7
  אבטחת רשומת אתחול ראשית, 38 עד 39
  בקרת נכסים, 21
  הודעות כשל והתאוששות, 41
  התאוששות, 2
  התקנת מערכת מרחוק, 3
  כלי העזר Computer Setup (הגדרות מחשב) (F10)
  מנהל תוכנת המערכת, 6
  עדכון מחשבים מרובים, 6
  שילוב, 2
  תמונת תוכנה מותקנת מראש, 2
  תצורה התחלתית, 2
  תקליטון בר-אתחול, מידע חשוב, 40

## A

Altiris, 4

## D

DiskOnKey
בר-אתחול, 13 ; 18
*ראה גם* HP Drive Key.
Drivelock, 31 ; 33

## F

FailSafe Boot Block ROM, 8

## H

HP Client Manager, 4
HP Drive Key
בר-אתחול, 13 ; 18
*ראה גם* DiskOnKey.

## P

PCN (Proactive Change Notification), 6
Power-On Password (סיסמת הפעלה)
הזנה, 27
מחיקה, 30
שינוי, 29
Preboot Execution Environment (PXE), 3
Proactive Change Notification (PCN), 6
PXE (Preboot Execution Environment), 3

## R

Remote ROM Flash (זיכרון הבזק ROM מרחוק), 7
ROM (זיכרון לקריאה בלבד)
Remote Flash, 7
לא תקף, 8
נורות מקלדת, טבלה, 9
שדרוג, 7

## S

SSM (מנהל תוכנת המערכת), 6