

## מדריך בסיסי לחשבון, יוזרים והרשאות

ישנם שני סוגי משתמשים בחשבון AWS

1. **Root User** – היוזר שפתח את החשבון, היוזר הכי חזק בחשבון, רק הוא יכול לסגור אותו

ולבצע פעולות **ברמת החשבון** כמו שינוי פרטי אמצעי תשלום, צפייה בחשבוניות וכד'.

2. **IAM User** – יוזרים פנימיים בחשבון המוגדרים באמצעות IAM ולהם יש הרשאות כפי

שמגדירים להם באופן יזום על **המשאבים** בחשבון.

IAM יוזר שלא הוגדרו לו הרשאות לא יוכל לבצע כלום בחשבון.

IAM יוזר שהוגדרה לו ההרשאה הכי גבוהה AdministratorAccess יוכל לבצע את כל

הפעולות על **המשאבים** בחשבון.

AWS שינו את הגישה בחצי שנה האחרונה לגבי **Root User** והם לא מאפשרים לעבוד איתו ללא

הגנת **MFA** – הגנה נוספת מלבד שם משתמש וסיסמה והיא בירור זהות נוסף מול התקן **פיזי**.

Root User מוכרח להגדיר עבורו MFA כיון שהוא מצריך הגנה מיוחדת, במידה ונגנבים פרטי ה

root user אין שום דרך לשלוט על גניבת הזהות בשונה מ IAM user שתמיד יש מעליו את ה root

user שיכול לשלוט עליו (למחוק אותו או להסיר לו הרשאות וכד')

הוראות להגדרת MFA בהמשך.

### **לצורך עבודה שוטפת בחשבון יש להיכנס עם יוזר מסוג IAM בלבד!**

לצורך צפייה בחשבוניות ניתן להיכנס בברירת מחדל רק באמצעות Root User אולם Root User

יכול להגדיר שגם IAM יוזר יוכל לצפות בחשבוניות.

באופן שוטף, אין צורך להיכנס כ Root User מלבד **סגירת החשבון**.

### לענין ביצוע המטלה שקיבלתן בסיום הקורס:

יש לבצע אותה רק באמצעות ה **user IAM** שכבר יש לכן עוד מתחילת הקורס ולכן אין אף מניעה לבצע אותה גם **בלי** להגדיר MFA.

בת שאין לה יוזר כזה תיאלץ להגדיר MFA ל **root user** שלה ולהיכנס דרכו כדי ליצור קודם כל יוזר IAM בחשבון.

ה MFA שתגדיר יהיה חייב להיות על התקן שנשאר איתה כמו מחשב פרטי וכד' כדי שתוכל בהמשך להיכנס לחשבון שוב כ **Root user** בשביל לסגור את החשבון.  
בת שנמצאת במצב כזה לא תקבל תמיכה כיון שהיא לא מילאה אחר ההוראות והמטלות במהלך הקורס, הדבר אף יוריד לה ציון.

לאחר סיום המטלה, אם ברצונכן **לסגור את החשבון**, תוכלנה להיכנס כ **Root User** להגדיר לו MFA ולסגור את החשבון, כלומר גם אם הגדרת ה MFA תתבצע במחשבי הסמינר וה MFA שהותקן יתאפס זה כבר לא יהיה רלוונטי כי תשתמשנה בו רק לצורך כניסה אחרונה לחשבון לצורך סגירת החשבון, לאחר סגירת החשבון לא ניתן ואין סיבה להיכנס לחשבון.

## איך מגדירים MFA?

ישנו תוסף של כרום המאפשר הגדרת MFA

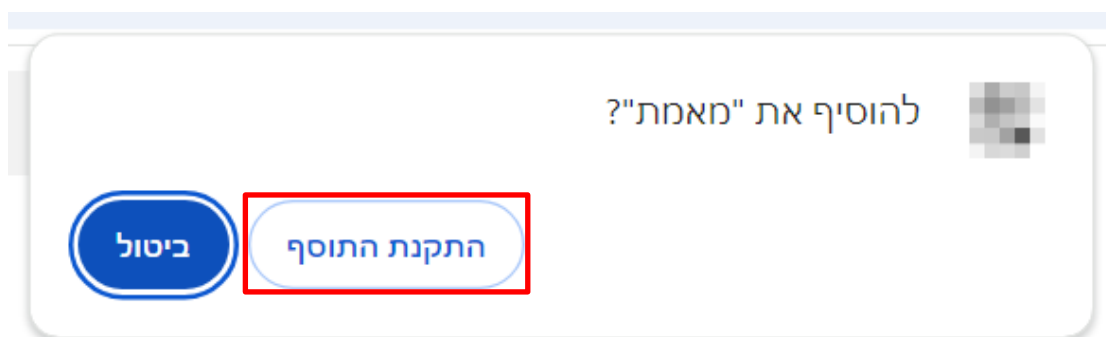
התוסף נמצא בכתובת:

<https://chromewebstore.google.com/detail/%D7%9E%D7%90%D7%9E%D7%AA/bhg%20hoamapcdpbohphigoooaddinpkbai>

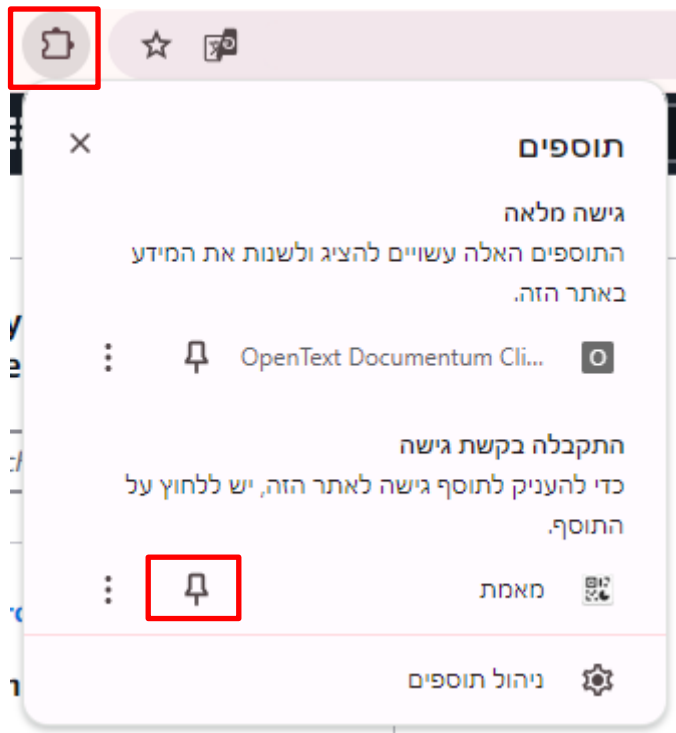
בכניסה לקישור זה ישנו כפתור "הוספה ל-Chrome" יש ללחוץ עליו



בחלון הזה ללחוץ על התקנת התוסף



לאחר שהתוסף מותקן, ניתן ללחוץ על אייקון התוספים ולראות אותו ברשימת התוספים המותקנים, לצורך נוחות כדאי גם לנעוץ אותו



כאשר נבוא עבשיו להגדיר MFA על ה Root User בין אם זה חלון שקפץ בניסיון כניסה לחשבון ובין אם זו הגדרה יזומה דרך מנגנון ה IAM, נקבל מסך כזה:

## Select MFA device [Info](#)

### MFA device name

#### Device name

This name will be used within the identifying ARN for this device.

myChrome


Maximum 64 characters. Use alphanumeric and '+', '=', '@', '-', '\_' characters.

### MFA device

#### Device options


In addition to username and password, you will use this device to authenticate into your account.

☐



**Passkey or security key**  
Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.

☒



**Authenticator app**  
Authenticate using a code generated by an app installed on your mobile device or computer.

☐



**Hardware TOTP token**  
Authenticate using a code generated by Hardware TOTP token or other hardware devices.

[Cancel](#)

[Next](#)

יש לתת בו שם להתקן מולו עובדים, במקרה של התוסף זהו פרופיל הכרום ולכן בדוגמה ניתן לו

השם myChrome ויש לבחור את האפשרות השניה מבין ה-3 שהיא Authenticator app

וללחוץ על next

מתקבל מסך כזה:

## Set up device [Info](#)

### Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#) 

- 2

Show QR code

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

- 3

Type two consecutive MFA codes below

Enter a code from your virtual app below

MFA Code 1

Wait 30 seconds, and enter a second code entry.

MFA Code 2

[Cancel](#)

[Previous](#)

[Add MFA](#)

יש ללחוץ בו על ה Show QR code ונקבל קוד לסריקה:

- 2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

בשלב הזה יש ללחוץ על התוסף למעלה:

us-east-1.o

aws

Search

[Alt+S]

IAM

>

Security credentials

>

Assign MFA device

Step 1

Select MFA device

Step 2

**Set up device**

**Set up device**

Info

**Authenticator app**


A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

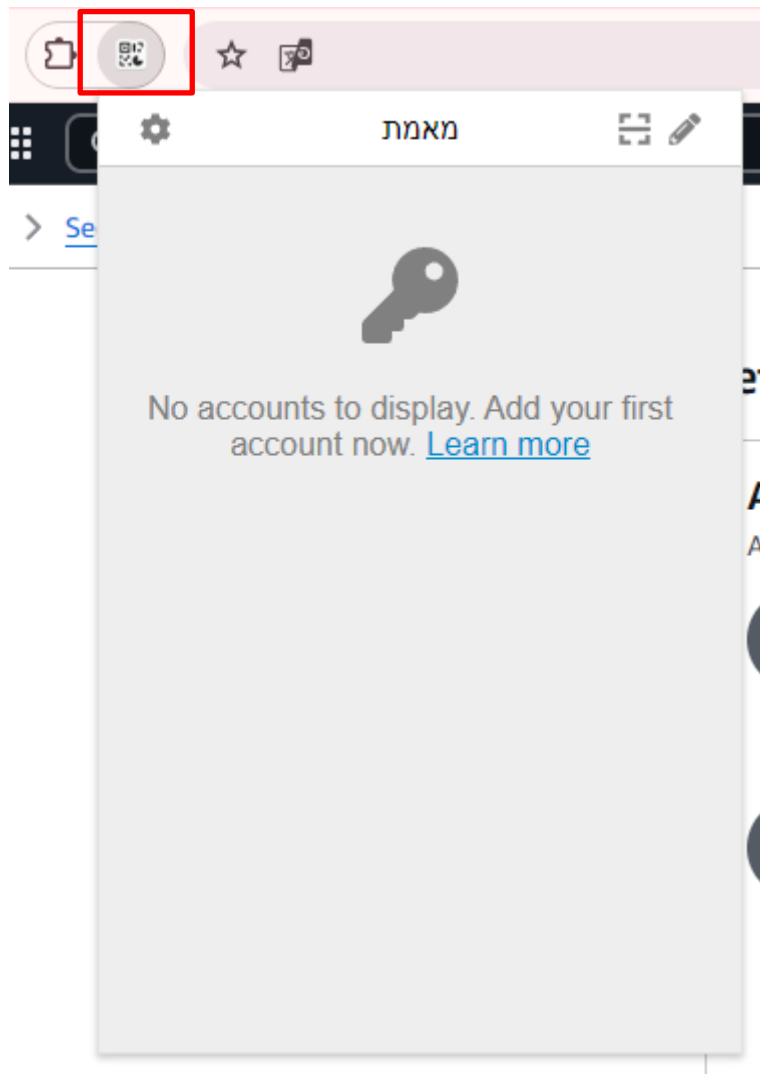
Wait 30 seconds, and enter a second code entry.

Cancel

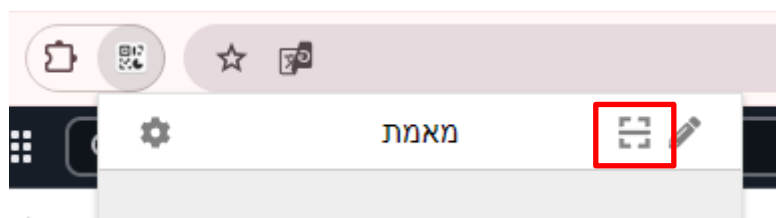
Previous

Add MFA

ונקבל את החלונית הזו:



כאן יש ללחוץ על כפתור הגדרת מאמת חדש:



ונקבל אפשרות לסריקת קוד QR, בשלב הזה יש לסרוק את הקוד שמוצג לנו במסך ואז נקבל הודעה כזו, בה נלחץ על אישור:

[Alt+S]


האתר us-east-1.console.aws.amazon.com אומר  
התוסף 71 myChrome@67

אישור

## Set up device Info

### Authenticator app

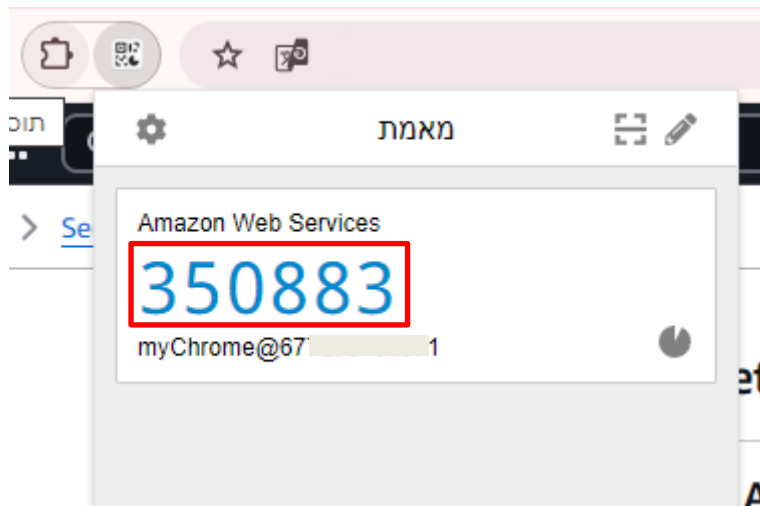
A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

- 1 Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.  
[See a list of compatible applications](#)
- 2 

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)
- 3 Type two consecutive MFA codes below  
**Enter a code from your virtual app below**  
  
**Wait 30 seconds, and enter a second code entry.**

[Cancel](#) [Previous](#) [Add MFA](#)

השלב השלישי הוא לקבל קוד מהתוסף שהוגדר, יש ללחוץ שוב על התוסף, ואז הוא מציג 6 ספרות עליהן יש ללחוץ ולהעתיק אותן



להדביק אותן בשדה הראשון במסך בו אנחנו נמצאים:

## Set up device [Info](#)

### Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

350883

Wait 30 seconds, and enter a second code entry.

MFA Code 2

[Cancel](#)

[Previous](#)

[Add MFA](#)

לחכות 30 שניות ואז ללחוץ שוב על התוסף, לקבל שוב 6 ספרות חדשות אחרות, להעתיק אותן ולהדביק אותן בשדה השני שמחכה לקבל קוד נוסף

## Set up device [Info](#)

### Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

350883

Wait 30 seconds, and enter a second code entry.

915875

[Cancel](#)

[Previous](#)

[Add MFA](#)

ואז ללחוץ על Add MFA

במידה ומצליח, נחזור למסך בו נראה אותו ברשימת ה MFA של ה account

Multi-factor authentication (MFA) (1)				<a href="#">Remove</a>	<a href="#">Resync</a>	<a href="#">Assign MFA device</a>
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. <a href="#">Learn more</a>						
Type	Identifier	Certifications	Created on			
<input checked="" type="radio"/> Virtual	arn:aws:iam::6 mfa/myChrome	Not Applicable	125			

כעת, אם נצא מהחשבון באמצעות sign out וננסה להיכנס שוב כ Root User

נתבקש מעבר לשם משתמש וסיסמה להזין גם קוד MFA

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

MFA code

\_\_\_\_\_

נלחץ על התוסף ונקבל ממנו קוד MFA 6 ספרות, נעתיק אותו ונדביק בשדה המיועד



## Amazon Web Services

937230

myChrome@67

 Try the new sign in UI

See our new improved Amazon Web Services



## Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: pnc[REDACTED].com

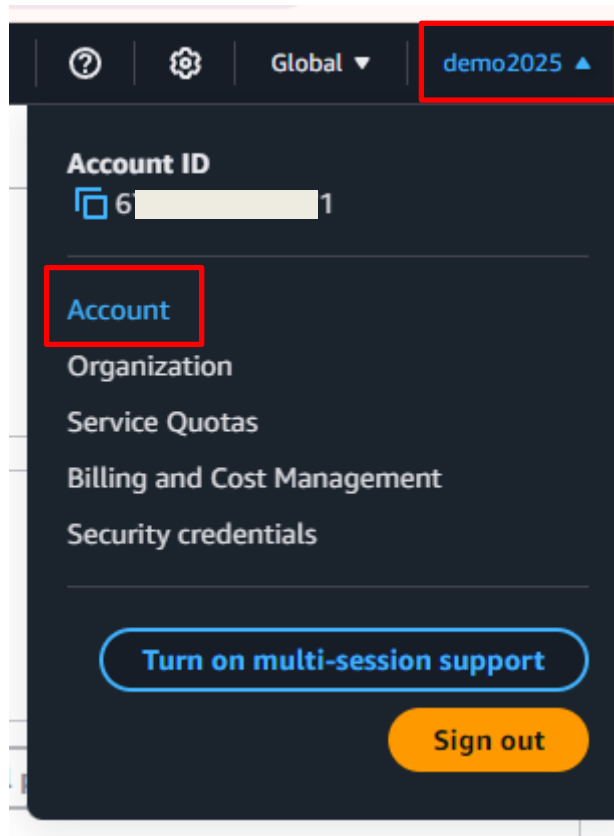
MFA code

Submit

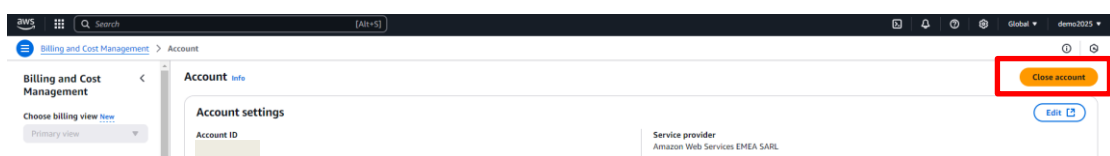
אם הכל הוגדר כמו שצריך עד כה, הבניסה תצליח וניגש לחשבון כ Root User עם הגנת MFA.

## איך סוגרים חשבון?

נכנסים כ **Root User** ואז בצד ימין למעלה בלחיצה על שם החשבון נפתח תפריט ובו גישה ל Account, נלחץ עליו



נגיע למסך ובו בפתור של Close account



נקבל פופאפ המבקש לוודא שאנחנו באמת מעונינים לסגור את החשבון ונפעל כפי המופיע במסך

Are you sure you want to close account 'demo2025' (#671)?



⊖ Confirm account closure

▶ Account closure guidance

Enter the account ID to confirm closure and that you have read and understand the closure guidance.

671

Cancel

Close account