

התקנת שרת אפליקציה

פריוריטי בממשק וובי / פריוריטי לייט

במסמך זה מפורטות הנחיות להתקנת שרת אפליקציה של פריוריטי בממשק וובי ושל פריוריטי לייט ברשת הארגונית (אינטראנט) ו/או ברשת האינטרנט. כמו כן, מפורטות הוראות ההתקנה של שרת IIS, ועבור התקנות לרשת ארגונית בלבד, הנחיות להתקנה של תעודת SSL עצמית. יש להתקין תחילה את שרת ה-IIS, ואז את תעודת ה-SSL, ורק לאחר מכן את שרת האפליקציה.

1. דרישות מקדימות

דרישות חומרה מינימליות לשרת

לדרישות חומרה מינימליות ומערכות תומכות, הורד את המסמך פריוריטי: חומרה ומערכות נלוות מספריית התעוד במרכז הלקוחות באתר [פריוריטי סופטוור](#).

דרישות נוספות

חשוב! יש לוודא שמותקן בשרת NET Framework 4.5.

שרת אפליקציה הכולל גישה דרך האינטרנט (תעודת SSL מספק מורשה)

שימו לב: לא ניתן לעבוד באפליקציית Priority Mobile ללא התקנה של תעודת SSL מספק מורשה, גם בעבודה ברשת ארגונית.

- רכישת כתובת IP קבועה מספק האינטרנט עבור השרת.
 - הפניית הפורטים 80 ו 443 לכתובת הפנימית של השרת.
 - רכישת דומיין.
 - יצירת **A record** ב-DNS בו מנוהל הדומיין עבור השרת.
 - רכישת תעודת Standard SSL מספק תעודות מורשה, בשם זהה ל **A record** בשרת ה-DNS.
- הערה:** להנחיות כיצד להפיק בקשה לתעודת SSL ולהתקינה בשרת ניתן להיעזר בתמיכה של ספק התעודות המורשה.

לדרישות נוספות עבור התקנות מיוחדות (כגון ריבוי שרתי אפליקציה), ראו **נספח א': התקנות מיוחדות**.

2. התקנת שרת IIS

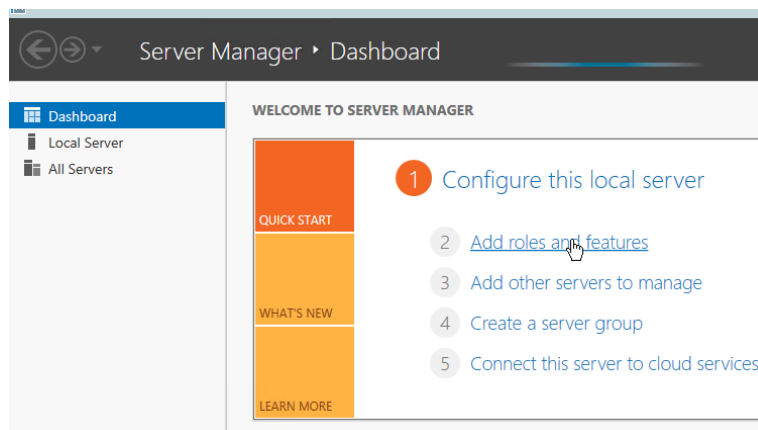
לפני התקנת שרת האפליקציה של פריוריטי, יש להתקין את שרת ה-IIS. לפני ביצוע ההתקנה, יש לוודא שה-IIS המותקן בשרת משמש אך ורק לפריוריטי. אם ההתקנה מתבצעת ב-Windows Server 2008 R2, יש לעבור להנחיות בעמוד 6. עבור Windows 7, יש לעבור להנחיות בעמוד 8.

המלצות שונות הנוגעות להקשחת ואבטחת השרת, אותן ניתן ליישם במהלך ההתקנה או לאחריה, ניתן למצוא ב**נספח ב': המלצות להקשחת השרת**.

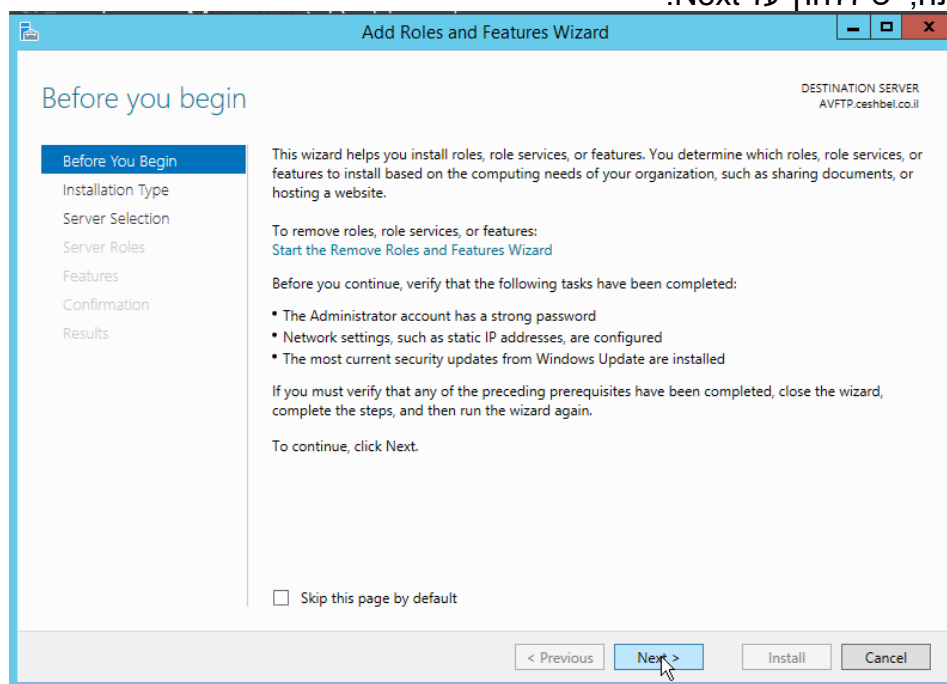
שרת 2012

בשרת Windows 2012, יש לבצע את הצעדים הבאים:

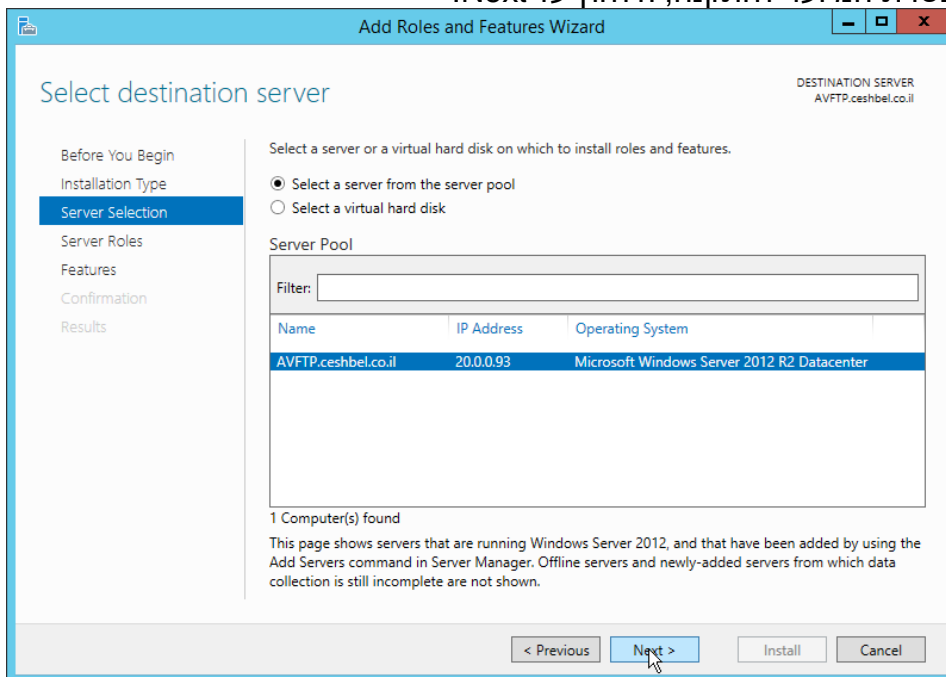
1. יש להפעיל את ממשק ניהול השרת (Server Manager) ולבחור ב- Dashboard > Add roles and features.



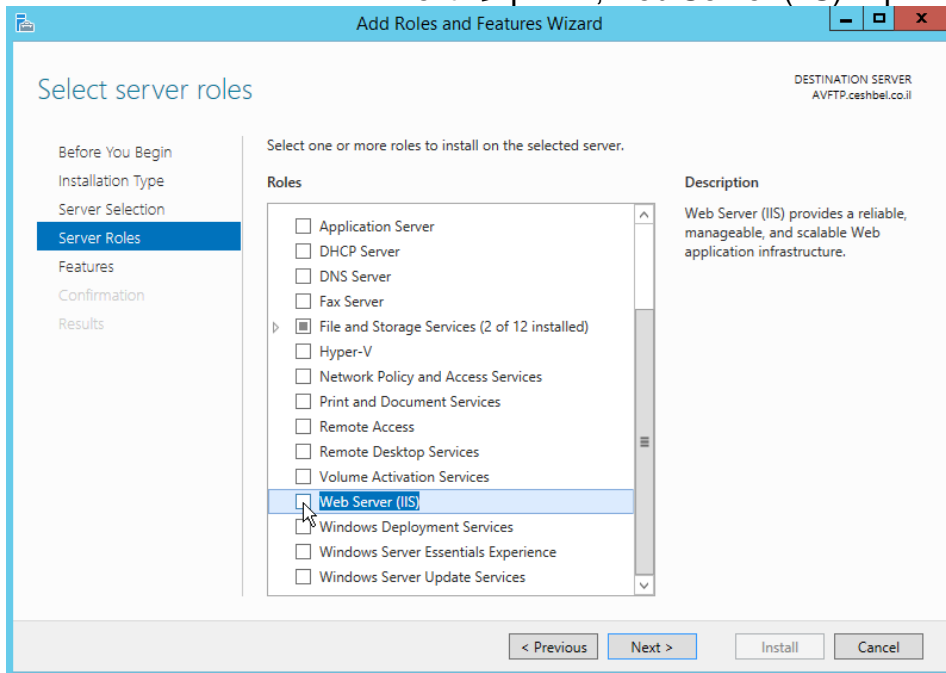
2. בחלון שנפתח, יש ללחוץ על Next.



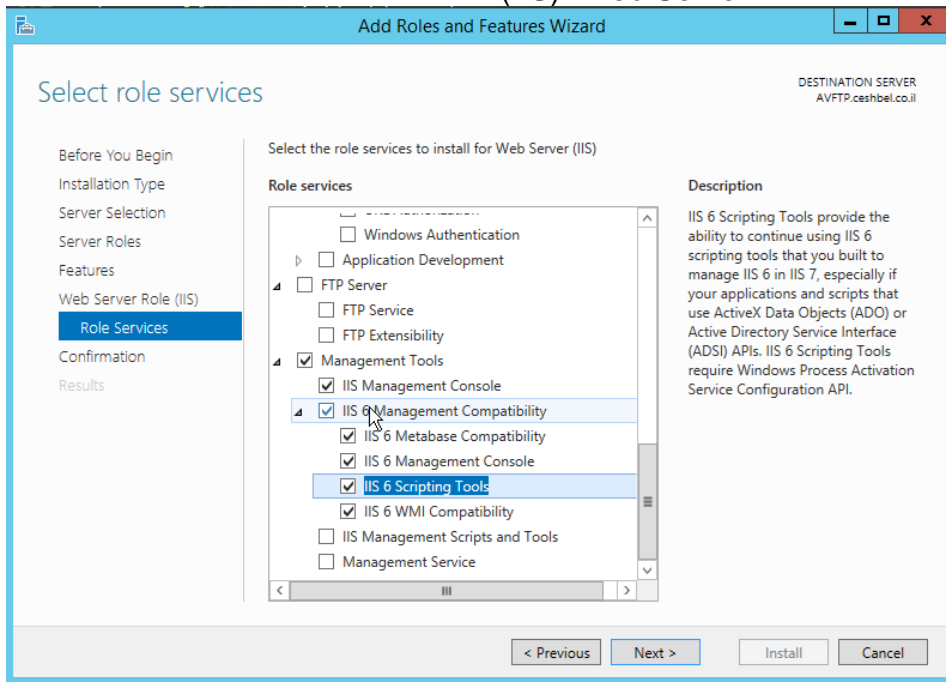
3. יש לבחור בשרת המיועד להתקנה, וללחוץ על Next.



4. יש לבחור בהתקנת Web Server (IIS), וללחוץ על Next.

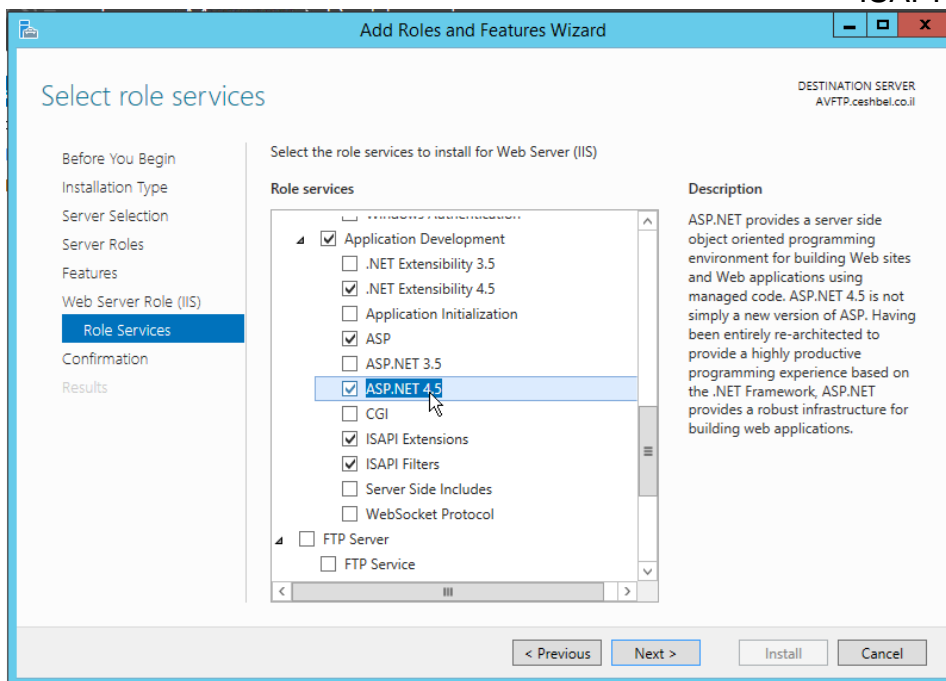


5. יש להוסיף את כל שרותי ה-Web Server (IIS).

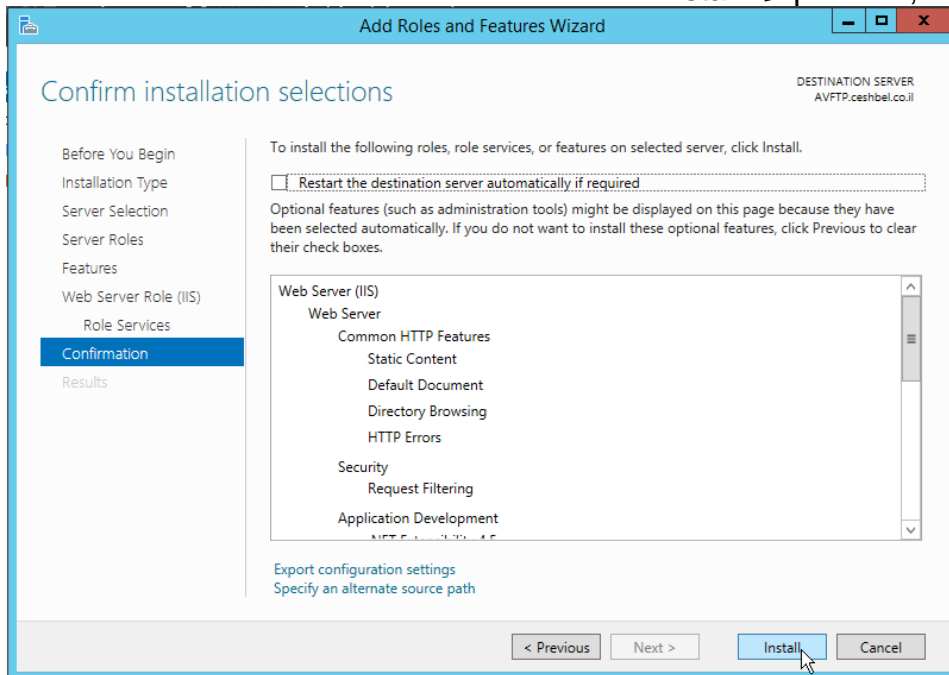


6. בסעיף Application Development יש לבחור באפשרויות הבאות:

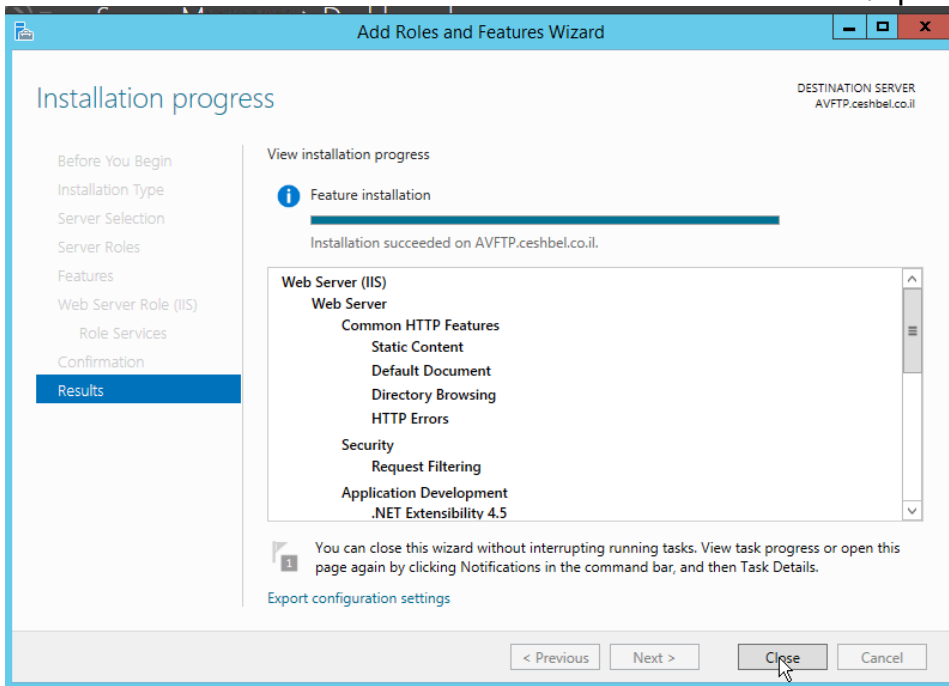
- .NET Extensibility 4.5
- ASP
- ASP.NET 4.5
- ISAPI Extensions
- ISAPI Filters



7. בחלון שיפתי, יש ללחוץ על Install.



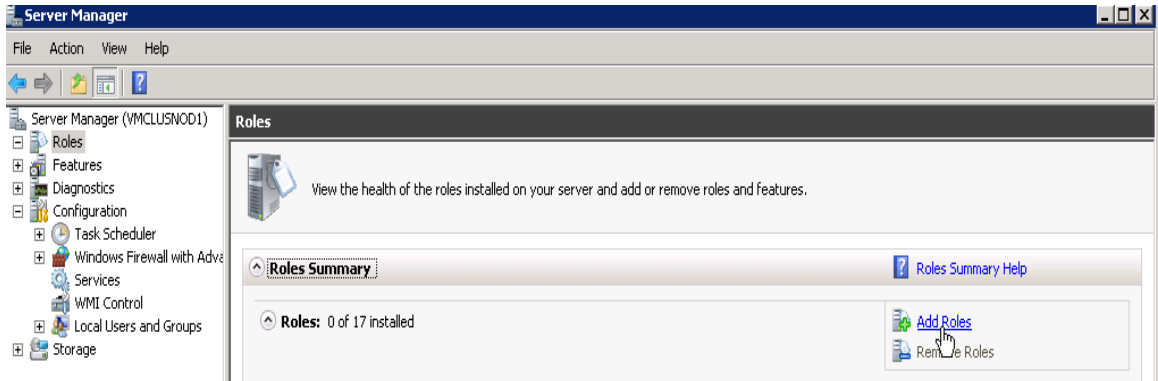
8. לסיום יש ללחוץ על Close.



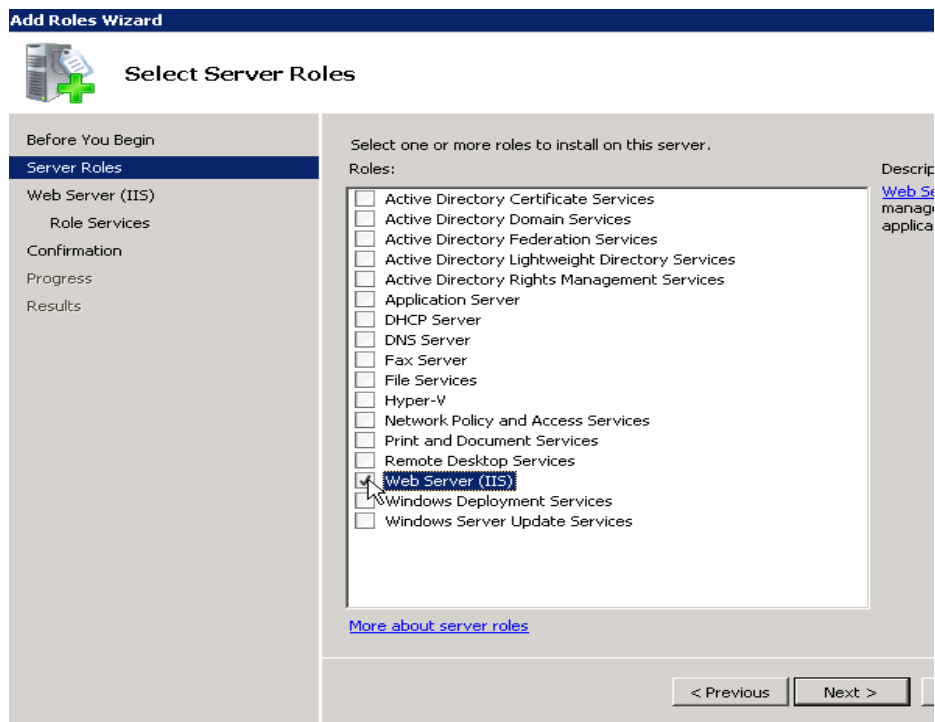
* שרת Windows 2008 R2

בשרתי Windows 2008 R2, יש לבצע את הצעדים הבאים:

1. יש להפעיל את ממשק ניהול השרת (Server Manager) ולבחור ב- Roles > Add Roles:



2. יש לבחור Web Server (IIS) > Select Server Roles



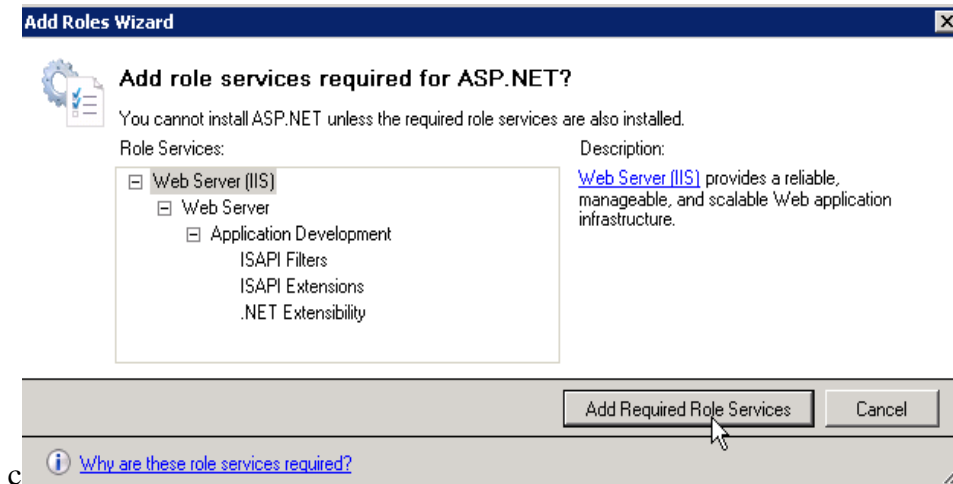
3. במסך Select Role Services יש לסמן את האפשרויות הבאות:

- Static Content
- Default Document
- ASP.NET
- ASP
- IIS6 Management Compatibility
 - a. IIS 6 Metabase Compatibility

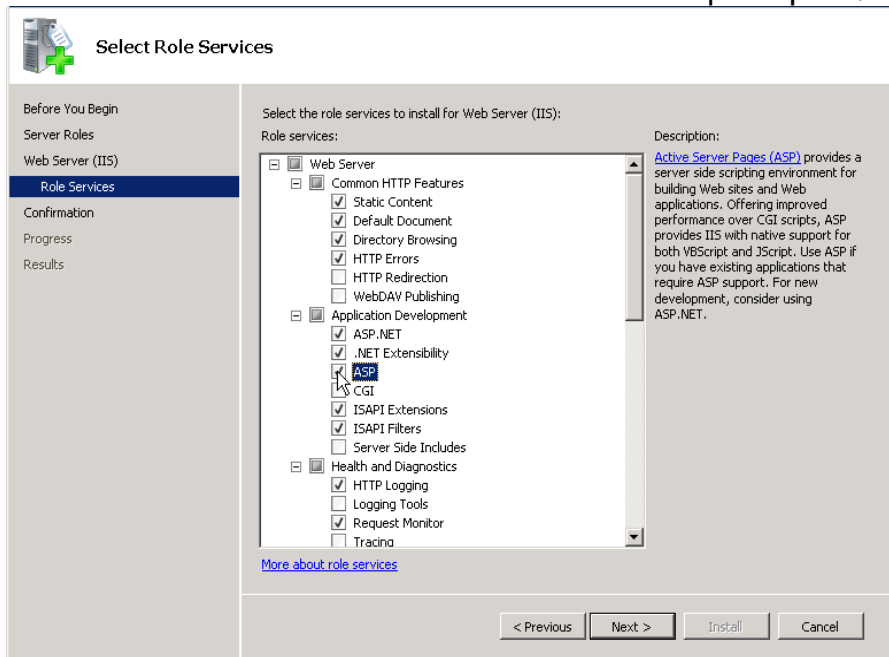
* שימו לב: התמיכה מערכת הפעלה זו מצד מייקרוסופט עומדת להסתיים. מומלץ לעבור למערכת הפעלה עדכנית יותר.

- b. IIS 6 WMI Compatibility
- c. Scripting Tools
- d. Management Console

4. יש ללחוץ Next. בחלון הדו-שיח הנפתח, יש לבחור לקבל את כל ההתקנות הנלוות (Add Required Role Services) ולאשר.



לאחר האישור, יופיע סימון בתפקידים נוספים:

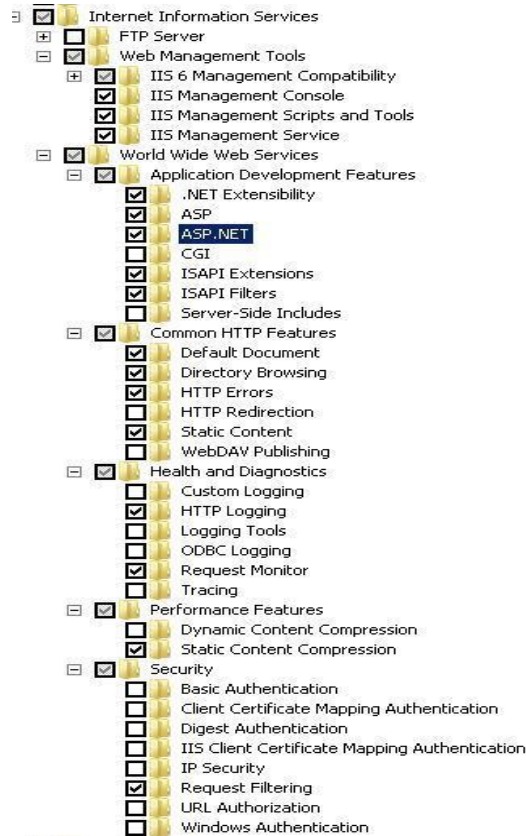


עבודה ב-Windows 7 *

בעבודה עם תחנת עבודה המשמשת כשרת (התקנה של Windows 7):

1. יש לבחור: Control panel > Programs and Features > Turn Windows Features On or Off:

ולוודא שהאפשרויות הבאות מסומנות:



אם ההתקנה מתבצעת ברשת הארגונית, המשיכו לסעיף הבא (3) כדי להתקין תחילה את תעודת ה-SSL העצמית. אחרת, עברו ישירות לסעיף 4.

3. התקנת תעודת SSL עצמית (רשת ארגונית)

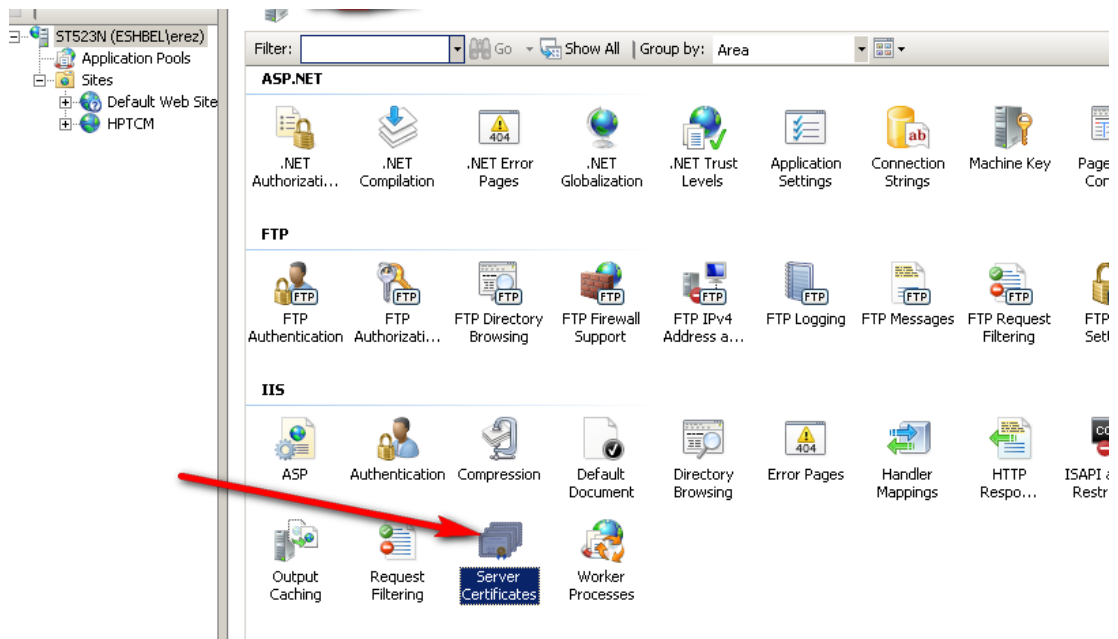
בשרת ה-IIS:

1. יש לפתוח את כלי ניהול שרת ה-IIS:

Start > Control Panel > Administrative Tools > **Internet Information (IIS) Manager**

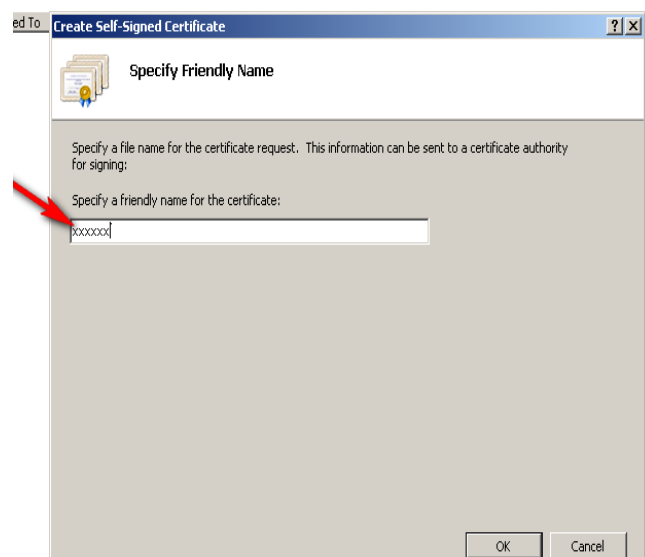
2. יש לבחור ב- **Server Certificates**

שימו לב: התמיכה במערכת הפעלה זו מצד מייקרוסופט עומדת להסתיים. מומלץ לעבור למערכת הפעלה עדכנית יותר.

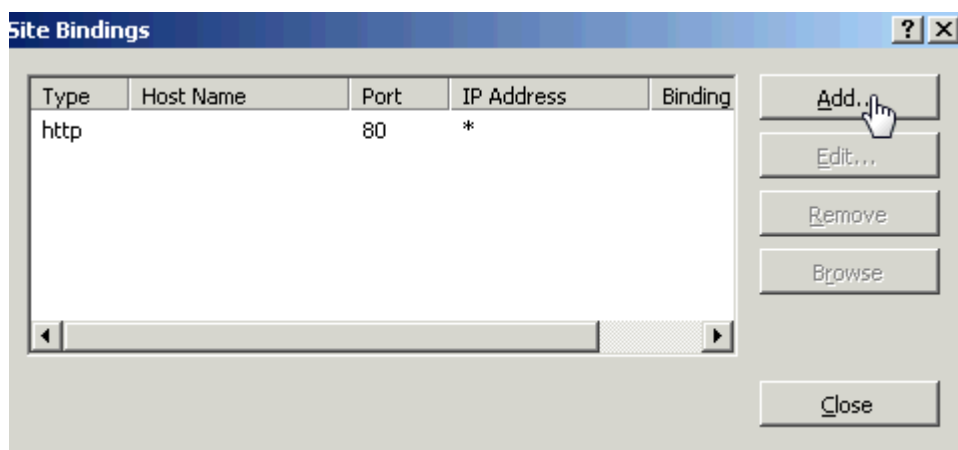
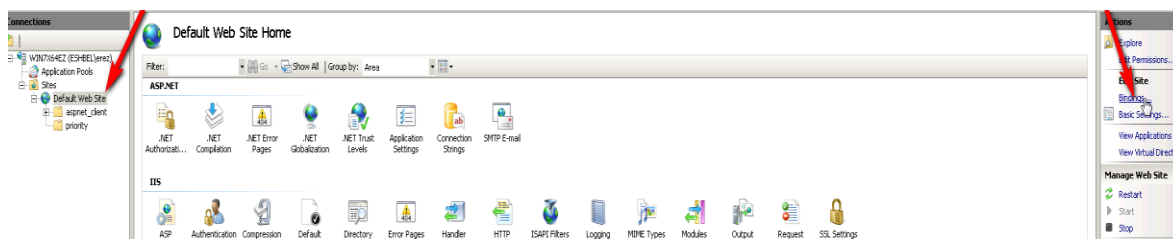


3. יש לבחור ב- **Create Self Signed Certificate** בצדו הימני של המסך.

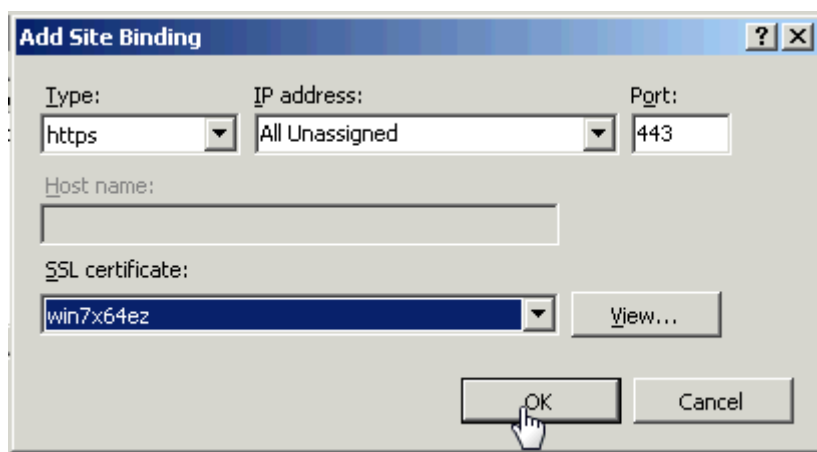
4. יש לרשום כינוי לתעודה, ולאשר.



5. יש לעבור ל- **Default Web Site**, לבחור ב- **Bindings** וללחוץ **Add**.



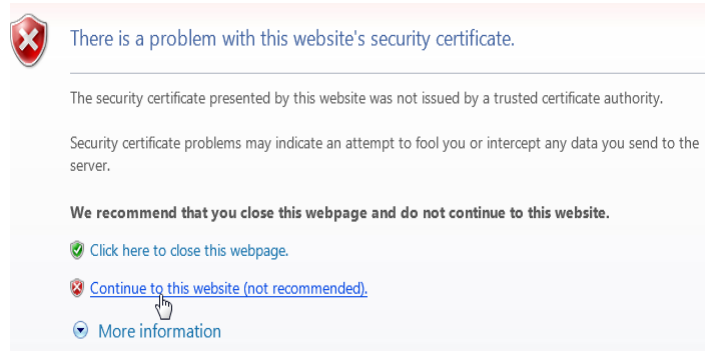
6. ייפתח מסך **Add Site Binding**. תחת **Type** יש לבחור ב-**HTTPS**. ב-**SSL certificate** יש לבחור את שם התעודה שיצרת קודם ולאשר בלחיצה על **OK**. בחלון הבא יש ללחוץ **Close**.



בתחנות העבודה:

הערה: הדוגמאות המופיעות בפרק זה מבוססות על Internet Explorer. בשימוש בדפדפן אחר, יש לבצע את הפעולות המקבילות.

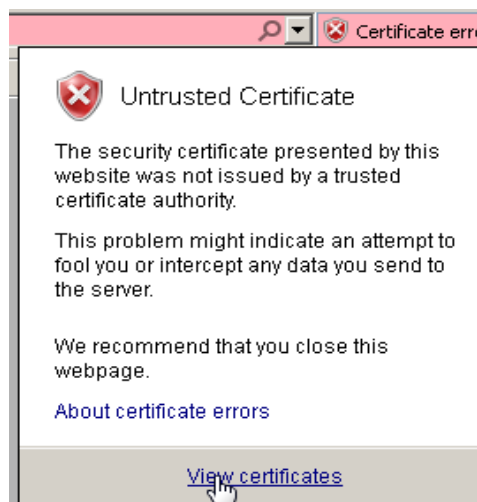
- יש לפתוח דפדפן Internet Explorer ולעבור לקישור לאתר שרת **פריוריטי/יזום**. תתקבל הודעת אזהרה. יש לאשר אותה ולהמשיך על ידי בחירה ב- **Continue to this website (not recommended)**.



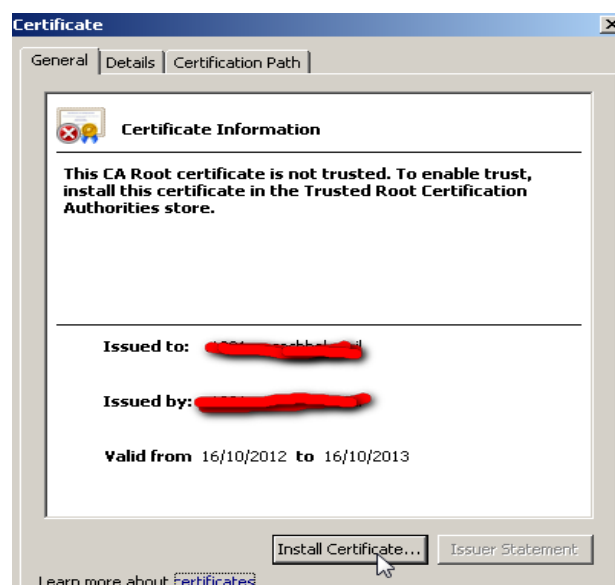
2. בשורת הכתובת בדפדפן, יש ללחוץ על **Certificate error**:



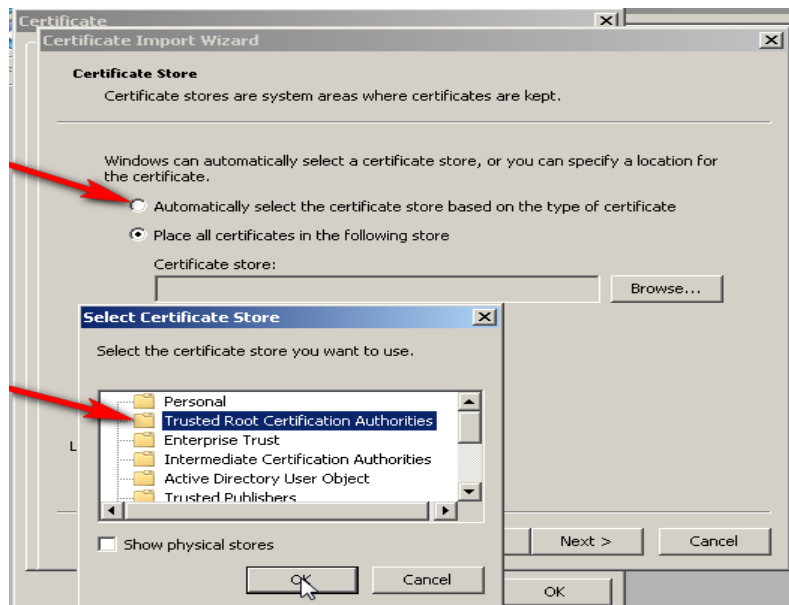
3. יש לבחור ב-**View certificate**:



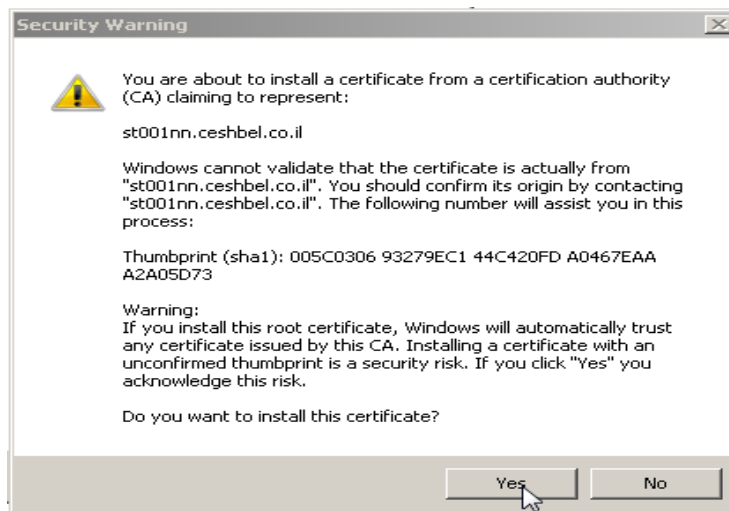
4. יש ללחוץ על **Install certificate**:



Next > Place all certificates in the following store > Browse > Trusted Root certification Authorities > OK > Next > Finish

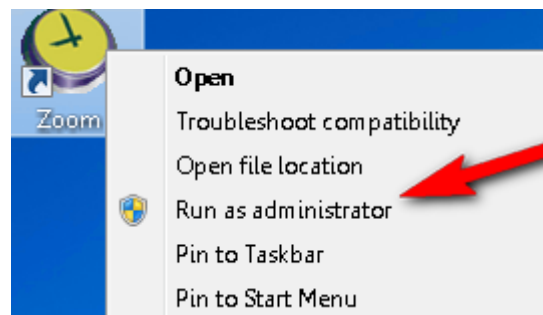


6. תתקבל הודעת אזהרה. לאישור ההודעה יש ללחוץ Yes > Ok:

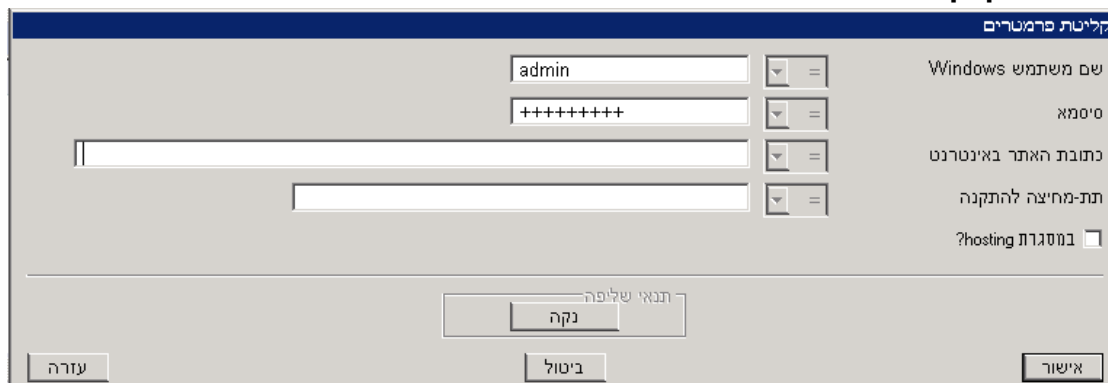


4. התקנת שרת האפליקציה

1. יש להיכנס לשרת האפליקציה כמשתמש מקבוצת administrators.
2. יש לכבות את UAC בשרת: יש לפתוח את Control Panel>User Accounts ולבחור באפשרות Change User Account Control Settings. בחלון שנפתח, יש לגרור את המחווך לאפשרות התחתונה **Never Notify**.
3. אם שרת האפליקציה מותקן על Windows Server 2008 R2 או על Windows Server 2012: במחשב השרת, בתיקיית bin.95 של התקנת **פריוריטי**, יש ללחוץ בקליק ימני על הקובץ winhtml.exe ולבחור ב-Properties. בחלון שנפתח, יש לסמן את האפשרות Run this program in compatibility mode for: (לעובדים ב-Windows Server 2012) או ב-Windows 7 (לעובדים ב-Windows Server 2008 R2).
4. יש לוודא שה-IIS מכובה.
הערה: אם מבצעים התקנה מחדש של שרת האפליקציה, יש לוודא בנוסף שה-service Priority.net מופסק.
5. יש להפעיל את **פריוריטי** בלחיצת מקש ימני על קיצור הדרך בשולחן העבודה ובחירה ב: Run as Administrator.



6. יש להפעיל את **פריוריטי** כמשתמש tabula.
7. יש להפעיל פרוצדורת ההתקנה: **מנהל המערכת < תחזוקת מערכת < הגדרות לאינטרנט < תחזוקת שרת אפליקציה < התקנת שרת אפליקציה**.
8. ייפתח **מסך קליטת פרמטרים**.

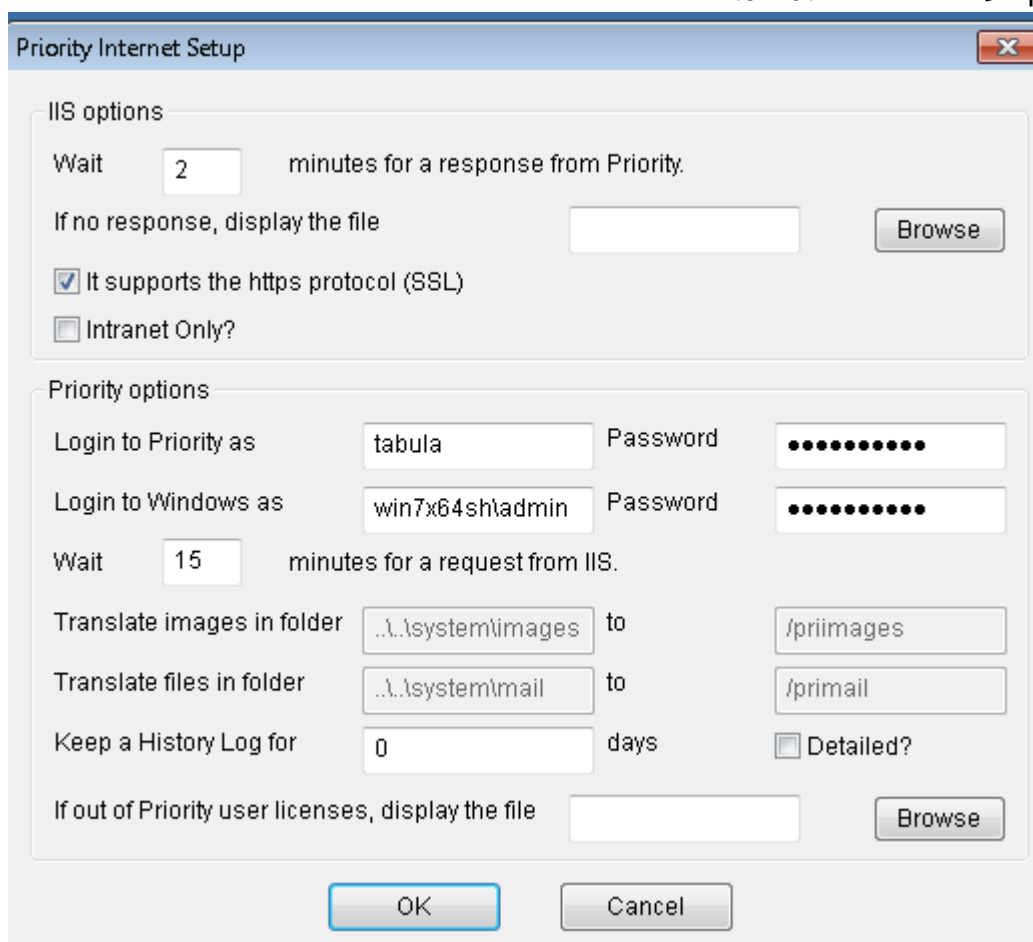


- בעמודה **שם משתמש Windows**, יש לרשום משתמש עם הרשאות מנהל מערכת, ובעמודה **סיסמא** יש לרשום סיסמא מתאימה.
הערה: הרשאות אלו תשמשנה את שרת היישום בעת גישה לבסיס הנתונים ולמתן שרותים נוספים.

- בעמודה **כתובת האתר באינטרנט**, יש להקליד את כתובת ה-URL כפי שהיא מופיעה בתעודת ה-SSL (ראה לעיל). כתובת זו נדרשת להרצת המערכת ע"י המשתמשים.
 - יש לוודא שהעמודה **במסגרת hosting אינה** מסומנת.
9. יש ללחוץ אישור. ייפתח חלון עם אפשרויות התקנה.



10. יש לבחור בין התקנה של ממשק לייט בלבד, או יחד עם הממשק המלא (וובי), ולאשר. ייפתח מסך קביעת תצורה ב-Internet.



:IIS Options

1. יש לרשום את מספר הדקות שאתה מוכן להמתין לתגובה **מפריוריטי**. מומלץ להשאיר את מספר הדקות שנקבע כברירת המחדל.
2. אם בחרת להכין דף שגיאה ב-HTML, יש לרשום את נתיב הדף, כדי שהודעת השגיאה ש תופיע במקרה שהמערכת לא מגיבה.

3. סמן את האפשרות המתאימה אם שרת ה-IIS עליו מותקנת המערכת תומך בפרוטוקול HTTPS.
- הערה:** מומלץ להתאים את השרת לעבודה ב-HTTPS כפי שהוסבר לעיל.
4. אם שרת האפליקציה ישמש אך ורק לעבודה ברשת הארגונית, סמן את העמודה **Intranet Only**. לעבודה באינטרנט, יש להשאיר את העמודה ריקה.

Priority Options:

1. יש לרשום את סיסמת ה-tabula. שם וסימת משתמש ה-Windows יופיעו אוטומטית.
 2. יש לרשום את מספר הדקות בהן יפעל מנוע הקישור בין ה-IIS ל**פריוריטי** ללא פעילות.
- הערה:** בכל פעם שלקוח\ספק או משתמש מהחברה נכנסים לאתר ונוצר קישור עם **פריוריטי**, נפתח מנוע קישור בין ה-IIS לבין **פריוריטי**. בכל כניסה של משתמש נוסף, מופעל מנוע קישור נוסף. כאשר יוצא המשתמש מהאתר, מנוע הקישור הופך ללא פעיל ואחרי מספר דקות יכבה.
3. כדי שהודעת השגיאה שהוגדרה תופיע במקרה שחסרים רישיונות, רשום את הנתביב בו נמצא דף ה-html שהכנת.
11. לחץ **OK**. תתקבל הודעה שההתקנה הסתיימה בהצלחה.
- הערה:** בהתקנה של הממשק הוובי, תתבקש בשלב זה להזין את סיסמת tabula.

התקנת שירות החיפוש בשרת האפליקציה

הנחיות מפורטות להתקנת שירות החיפוש ניתן למצוא [כאן](#).

5. הרצת פריוריטי לייט / פריוריטי בממשק וובי ובדיקת תקינות ההתקנה

פריוריטי לייט

כניסה לממשק מתבצעת מהקישור הבא:

```
https://[Your Server Name]  
priority/prihtml.dll?WWWIPHONE&_portal=1&_tabulaini=tabula.ini
```

כאשר יש לרשום במקום [Your Server Name] את שם השרת שלכם כפי שמופיע בתעודת ה-SSL. לחלופין, אפשר לשלוח קישור למשתמשים אל **פריוריטי לייט** על ידי הרצה של התכנית **שלח קישור להפעלת התוכנה מתפריט מנהל המערכת < תחזוקת מערכת < משתמשי מערכת**.

הרשאות נחוצות בתחנה לעבודה בממשק הוובי

הרשאות במערכת הקבצים

- הרשאה מלאה לספריית ההתקנה (בד"כ C:\Program Files\priority) ותתי-הספריות שלה.
- הרשאה מלאה לספרייה זמנית %TEMP%.

הרשאות ב-Registry

- הרשאות מלאות למפתח: HKEY_CURRENT_USER\Software\priority

התקנת ממשק וובי בתחנה

- הערה חשובה:** את התקנת הממשק הוובי בתחנה וכניסה ראשונה לממשק יש לבצע כמשתמש עם הרשאות Administrator ב-Windows.
- יש לפתוח את הדפדפן המתאים ולגשת לכתובת ה-URL שהוגדרה לעיל בשרת האפליקציה (סעיף 3, שלב 5), ולבצע את הוראות ההתקנה בדף שנפתח.

הערה: חובה להגדיר סיסמא למשתמש ב**פריוריטי** על מנת שתתאפשר כניסתו למערכת.

בדיקת תקינות ההתקנה ופתרון בעיות

לאחר שהממשק הוובי הותקן בתחנה, יש להתחבר אליו (כמשתמש Administrator) בתחנה דרך ה-URL שהוגדר בשרת האפליקציה. כדי לבדוק את ממשק לייט, יש לנסות לפתוח במערכת את **Dashboard מוצר** (נתיב: דו"חות מנהלים < מכירות). לאחר מכן יש לחזור על התהליך כמשתמש רגיל בתחנה.

אם אחת מהבדיקות לעיל נכשלה, יש לבדוק את הדברים הבאים:

- יש לוודא שלמשתמש המנסה להתחבר מוגדרות בשרת הרשאות מלאות לספריות של **פריוריטי**.
- יש לבדוק אם הקובץ `tabula.ini` קיים בתיקיה `C:\Users\username\AppData\Local\VirtualStore\Windows` (כאשר `username` הוא המשתמש שהוגדר בתוכנית להתקנת שרת אפליקציה). אם קיים קובץ כזה, יש למחוק אותו.

ביטול שימוש ב-CDN על ידי הממשק הוובי

החל מגרסה 17.2, הממשק הוובי נטען מרשת ה-CDN של **פריוריטי**. אם רוצים לכבות את השימוש ב-CDN (למשל, מכיוון שהארגון עובד רק עם רשת פנימית), מתוך **פריוריטי** יש לפתוח את מסך **קבועי מערכת** (נתיב: מנהל המערכת < תחזוקת מערכת < קבועי המערכת), ולשנות את ערך הקבוע **REMOTEH5** ל-0.

6. הגדרת סנכרון עם Gmail

ההנחיות הבאות מיועדות לביצוע ע"י איש/אשת סיסטם המנהל את Google Apps, במקרה שהדואר הארגוני מבוסס על Gmail, כך שמשתמשים יוכלו לסנכרן נתונים בין **פריוריטי** לבין Gmail. יש לפעול על פי ההנחיות בקישור הבא:

<https://developers.google.com/google-apps/extensions-console/?hl=iw-IL>

שימו לב:

1. הקבצים `manifest.xml` ו-`extractor.xml` ממוקמים בתיקיית `IIS/priority/google` במחשב השרת.

2. יש לטעון את קובץ ה-`extractor`, למרות שבהנחיות של Google Apps כתוב כי שלב זה הינו רשות.

3. יש לסיים את התהליך בפרק `Installing the application in your own domain`.

לאחר סיום התהליך, בתיבת הדואר של משתמשים הניגשים לדואר הארגוני דרך Gmail יופיע הכפתור הבא, המאפשר את הסנכרון עם **פריוריטי**:

נספח א': התקנות מיוחדות

התקנת שרת אפליקציה בשרת נפרד משרת הנתונים

אם שרת האפליקציה מותקן במחשב נפרד משרת הנתונים, יש להתקין תחילה בשרת האפליקציה תחנה של פריוריטי, על פי ההנחיות במסמך הוראות התקנה למערכת Priority.

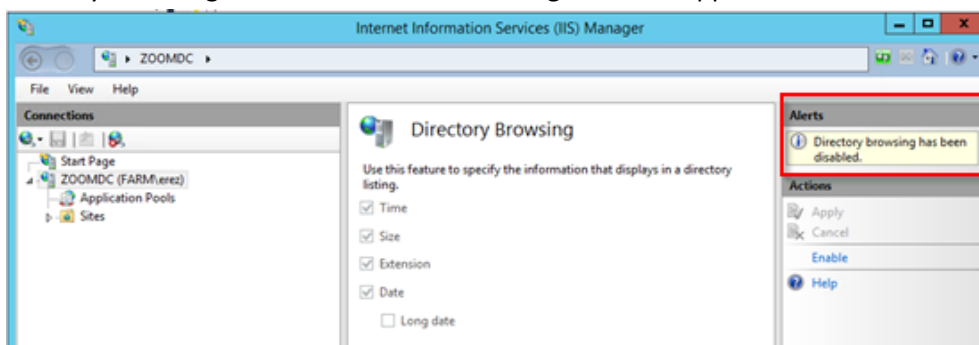
ריבוי שרתי אפליקציה

ניתן להתקין מספר שרתי אפליקציה. עם זאת, יש לשים לב שפריוריטי שומרת את ה-user session state בשרת, ויש להתחשב בכך בעת תכנון הארכיטקטורה של השרת.

נספח ב': המלצות להקשחת השרת

The following is a list of steps you can take to secure your server. Note that these are only recommendations based on our experience; in no way do they replace a thorough assessment of your operations by a security expert.

- When configuring the application server, ensure you use a full address (e.g. <https://appserver.domain.com>) and leave port 443 as the only open port.
- Disable Directory Browsing in IIS and ensure this setting has been applied to all IIS directories.



- Create custom error messages for errors 403 and 404 in the IIS server. You can find detailed instructions how to do so here: <https://technet.microsoft.com/en-us/library/cc753103%28v=ws.10%29.aspx?f=255&MSPPErr=-2147217396>
- Run anti-malware and antivirus scans on your server and run tests on your communications and security software.
- Install a 2048-bit SHA2 SSL certificate.
- Enable only protocols and ciphers using TLS 1.1 and above. Disable older, less secure ones. The screenshot below shows protocols and ciphers which (as of the writing of this appendix) are believed to be secure.

You can use IIS Crypto to manage protocols and ciphers, available here:

<https://www.nartac.com/Downloads/IISCrypto/IISCrypto.exe>

