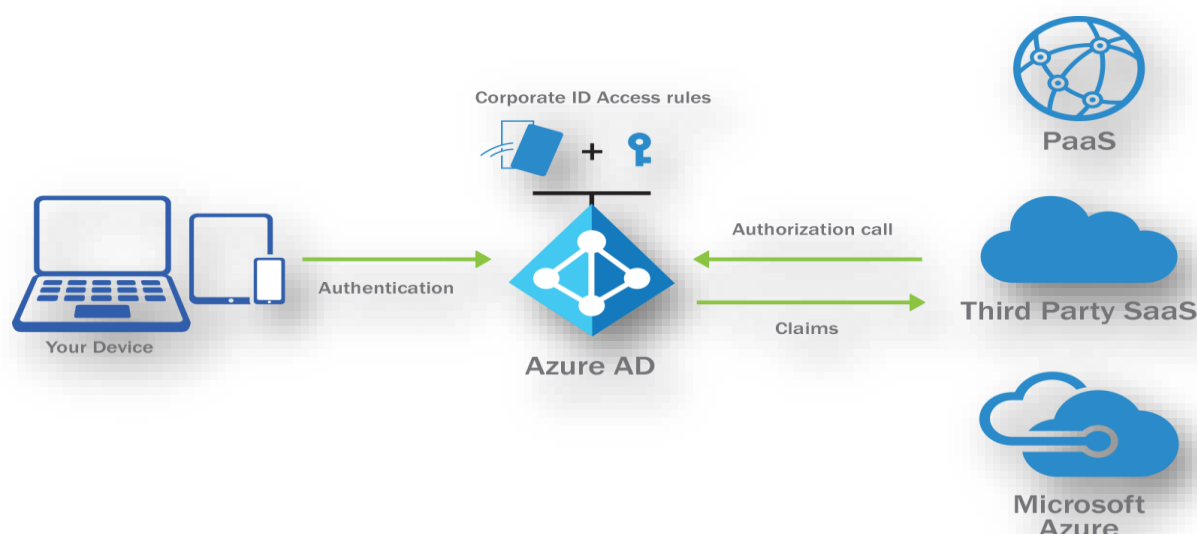


## 1. ENTRA ID

Azure Active Directory (ENTRA ID), הינו מוצר האימות וניהול הזהויות מבוסס הענן של מייקרוסופט. המוצר מאפשר למנהלי רשת להעניק גישה ואפשרות SSO למגוון מוצרי ענן כגון 365 ומוצרים של חברות צד ג'.



### יתרונות השימוש ב-ENTRA ID:

**SSO** – באמצעות שימוש בכלי הזה נוכל לבצע כניסה עם סיסמה אחת למגוון שירותי ענן כולל שירותי ענן חיצוניים ואפליקציות צד ג' שאיתן הארגון שלנו עובד

**תמיכה בהתקנים מרובים** – ENTRA ID יודע לתת תמיכה לגישה ממגוון רב של התקנים כמו ANDROID, IOS, מחשבי מק, עובדים יכולים לגשת לאפליקציות שלהם דרך פורטל אינטרנטי מכל מכשיר המחובר לאינטרנט

**אבטחה** - הגישה לענן מאובטחת ומנוטרת על ידי כללים שמנהל הרשת קובע, כמו כן הגישה לאפליקציות מוגנת ישנה אפשרות מעקב גישה והצפנה ושימוש באימות זהויות מתקדם.

**חיבור של AD DS אל הענן** - ניתן לקשר את בסיס הנתונים הקיים בשרת ולהרחיב אותו אל הענן ובכך להמשיך את העקביות עבור המשתמשים (אותם שמות וסיסמאות הן לשירותי הענן והן לשירותים הניתנים בארגון).

**שירות עצמי** - באמצעות שימוש ב ENTRA ID נוכל ליצור פורטלים לניהול עצמי ולאפשר למשתמשים להחליף לעצמם סיסמאות ובכך להפחית קריאות ל HELP DESK כמו כן נוכל להאציל סמכויות על מנת להוריד עומסי ניהול.

## מושגי יסוד:

**Identity – זהות** - אובייקט הניתן לאימות לדוגמא: משתמש עם שם וסיסמה, זהות יכולה להיות גם אפליקציה או שרת הנדרש לבצע אימות

**Account – חשבון** - זהות שיש לה נתונים מקושרים אליה – לדוגמא: משתמש עם תיבת מייל, לא ניתן ליצור חשבון ללא זהות

**ENTRA ID Account** – זהות שנוצרה באמצעות ENTRA ID או מוצר ענן אחר של מייקרוסופט לדוגמא: 365, לעיתים חשבון זה ייקרא WORK או SCHOOL

**Azure subscription** – זהו למעשה חשבון המשלם של AZURE בארגון, לארגון יכולים להיות מספר מנויים שונים וכל אחד מהם מקושר לאמצעי תשלום כלשהו במייקרוסופט

**Azure tenant** – זהו האובייקט הייחודי המקושר לארגון הנוצר בזמן הרישום לשירותי AZURE או 365, זוהי למעשה היישות המגדירה את הארגון

**ENTRA ID directory** – זהו בסיס הנתונים שנוצר עבור כל ישות, בסיס הנתונים מכיל את חשבונות המשתמשים, הקבוצות האפליקציות והוא משמש למטרות אימות וניהול גישה למשאבי הארגון בענן.

## ההבדל בין AD DS ל-ENTRA ID

ישנו דמיון בין שני המוצרים אך גם הבדלים רבים, ENTRA ID הינו מוצר אימות והוא נועד לבצע אימות באמצעות האינטרנט ע"י HTTP או HTTPS, לא ניתן לבצע שאילתות LDAP אליו הוא אינו יודע לבצע אימות באמצעות מנגנון KERBEROS אלא משתמש במנגנוני אימות ואישור העובדים באמצעות HTTPS כמו SAML, OAUTH ועוד.

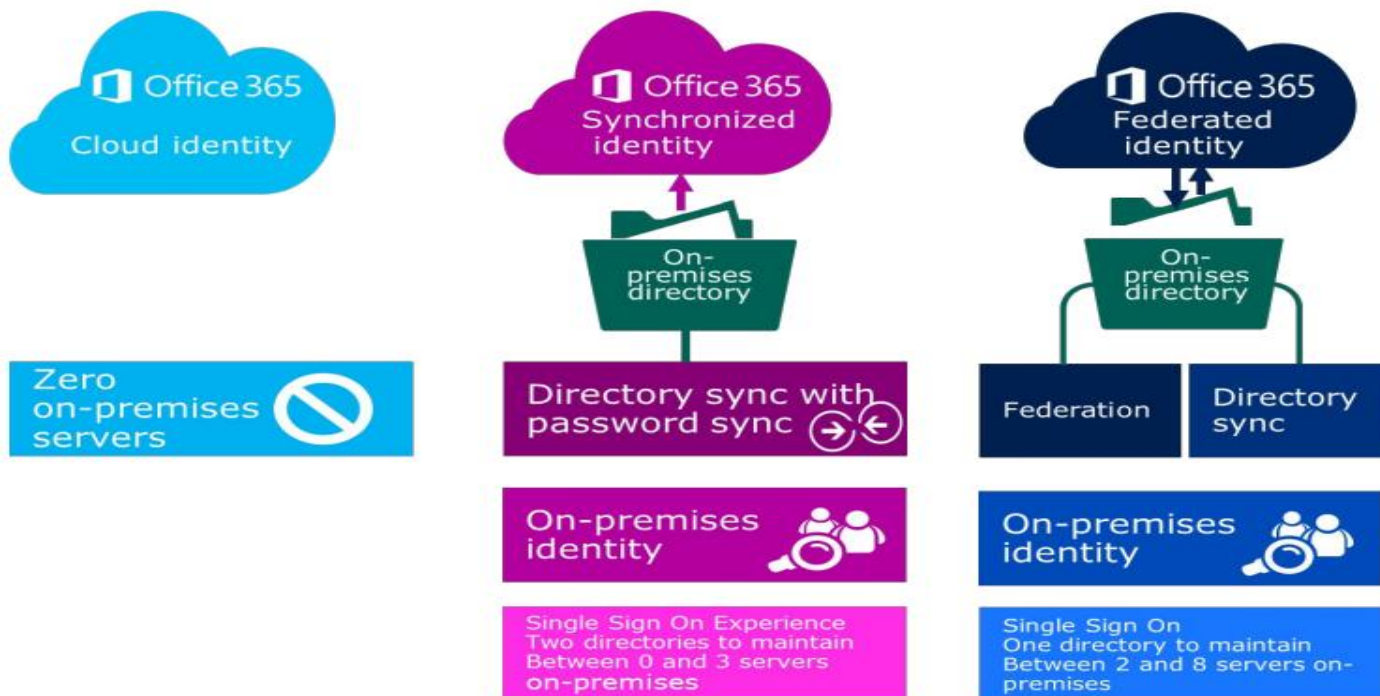
ENTRA ID יודע להתממשק לשירותים צד ג' כמו FACEBOOK ועוד...

המבנה שלו אינו היררכי אלא שטוח אין OU ואין GPO כאשר מסנכרנים משתמשים, קבוצות ואנשי קשר כולם מתקיימים באותו מרחב. עדיין נוכל ליצור סוג של הפרדה בין האובייקטים לפי הרשאות ניהוליות

בקישור הבא נוכל למצוא השוואה בין שני המוצרים הללו:

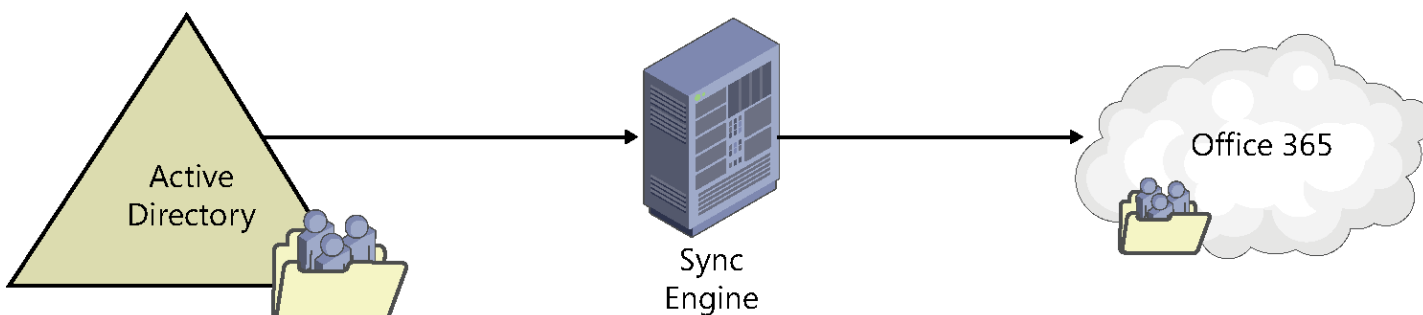
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad>

משתמשי 365 יכולים להגיע ממגוון מקומות ובהתאם לכך נקבעת הזהות שלהם, בהתקנה טיפוסית המשתמשים שלנו יגיעו בעקבות סנכרון משרתי AD הארגוניים. יחד עם זאת משתמשים יכולים להיות מבוססי ענן בלבד כלומר הזהות שלהם רשומה רק ב־AZURE AD בנוסף הם יכולים להיות חיצוניים כלומר מארגונים אחרים.



כל צורת התחברות כזו דורשת הגדרות ייחודיות ובעלת תכונות אבטחה משלה – בתמונה למעלה סקירה של צורות החיבור השונות ל-365.

**Synchronized identities** – ישויות מסונכרנות משרתי AD בארגון שלנו. הסנכרון יבוצע בין תשתית AD בארגון לתשתית הענן באמצעות כלי שנקרא Azure AD Connect, הכלי יותקן בשרת המחובר לדומיין ויאפשר לסנכרן קבוצות ומשתמשים וכן את הסיסמאות שלהם אל הענן על מנת להשתמש בזהויות הקיימות ולתת להן גישה לשירותי 365.

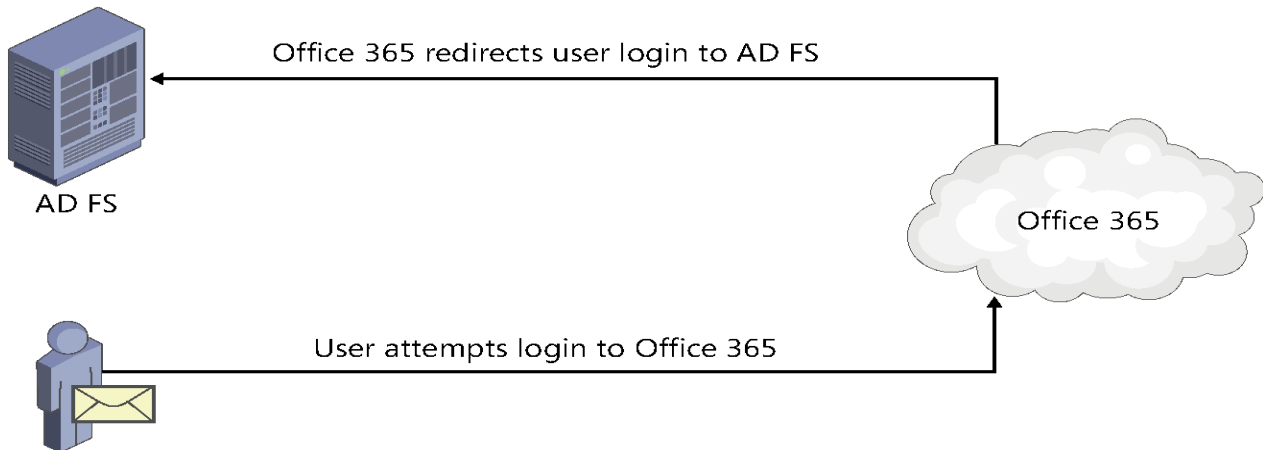


**Cloud identities** - Azure AD אילו חשבונות שנוצרו בצורה ידנית בענן באמצעות פורטל הניהול של 365 או פורטל. סקרנו את היצירה והניהול של משתמשים אילו בפרק הקודם. יש לציין שבשלב ההטמעה של

365 בארגון אנו ניצור קודם משתמשים בענן כיוון שלמשתמשים אילו אין נגיעה לתשתיות הארגוניות.

**Identity federation** - אלו הם משתמשים אשר קיימים בבסיס הנתונים הארגוני ובכל פעם שהם ניגשים לבצע אימות לשירות ענן

האימות מבוצע מול השרת הארגוני.



היתרון שליטה ומעקב על המשתמשים בארגון, ניהול מדיניות סיסמה קפדני יותר. החסרון – כאשר אין תקשורת בין שרתי הענן לשרתים הארגוניים לא תוכל להתבצע כניסה לשירותי הענן.

## סנכרון זהויות

בתור מנהל ארגון 365 אחד הדברים הראשונים אותם תצטרך להבין ולהטמיע הינו סנכרון זהויות, הסנכרון בין AD DS ל-AZURE AD הינו קריטי להצלחה של המעבר לסביבת הענן ויש לו השפעה עצומה על ההצלחה של המעבר.

במונחים פשוטים סנכרון זהויות הינו התהליך של שכפול הסביבה הארגונית, אובייקטים כמו משתמשים, קבוצות ואנשי קשר אל הענן.

אך כיום ישנה אפשרות לסנכרן מידע מהענן אל תוך הארגון והרחבת היכולות של AZURE AD

חלק מהיתרונות של התהליך הינם:

- משתמשים מקבלים את אותה חווית שימוש בשירותי הענן ובשירותים הארגוניים ומבצעים גישה עם אותו שם משתמש וסיסמה
- ניתן להקצות למשתמשים אפשרות לניהול עצמי של סיסמאות ולהפחית קריאות שירות לצוות התמיכה
- רמת האבטחה נשמרת גבוהה היות וכל הסיסמאות הן לפי המדיניות שנקבעה בארגון

## דברים שצריך לקחת בחשבון לפני תחילת התהליך:

- האם יש צורך לבצע עדכון לסכימה של AD
- אילו חשבונות ישמשו לביצוע הסנכרון והאם יש לבצע מעקב על התהליך
- האם יש גישה לרשת והאם הפורטים הדרושים פתוחים
- האם הסנכרון יהיה דו-כיווני ?
- כיצד נסנכרן ארגון עם סיומת בלתי ניתנת לניתוב כמו local. האם נשתמש בעוד upn suffix ?
- אילו אובייקטים נסנכרן והאם נפעיל פילטר מסויים על מנת למנוע מאובייקטים מסויים להסתנכרן לענן
- Data uniqueness – ישנה חשיבות רבה שכל אובייקט יהיה ייחודי כאשר הוא עולה ל-AZURE AD, שני מאפיינים שבד"כ מהווים מקור לבעיות הינם : UserPrincipalName ו-ProxyAddresses.
- כיום בתהליך הסנכרון מופעל מנגנון אשר מתריע למנהל הארגון על כפילויות ושולח לו דו"ח מסודר במייל, בעבר התהליך כולו היה נעצר ונכשל ברגע שהייתה נמצאת כפילות אחת.
- נוכל להשתמש בכלי שנקרא Idfix על מנת לסרוק ולתקן בעיות אילו לפני שנתחיל בתהליך, קישור לכלי והסבר עליו:

<https://microsoft.github.io/idfix>

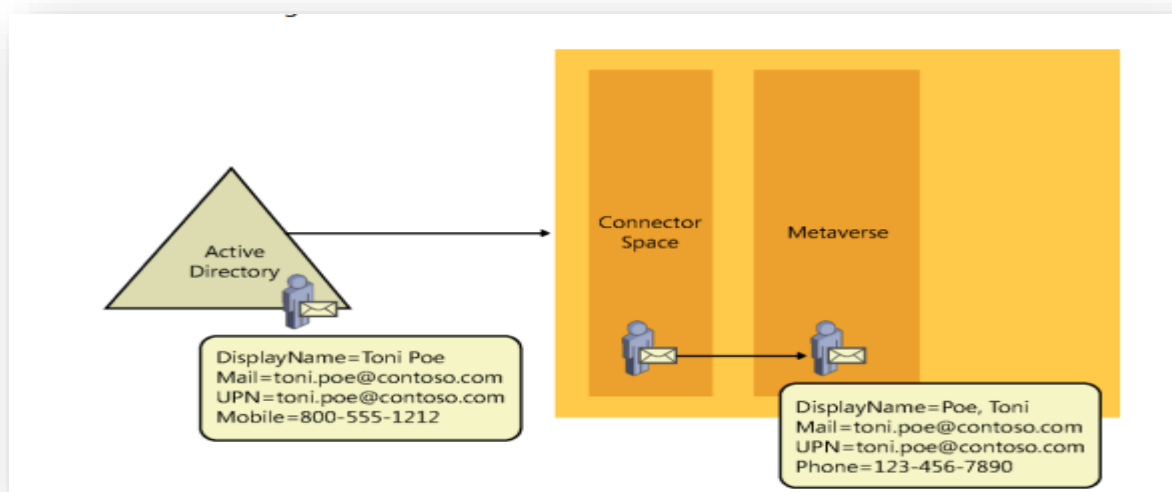
בקישור הבא הסבר על ההכנות שנבצע לפני התחלת התהליך:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-for-directory-synchronization?view=o365-worldwide>

זהו הכלי המעודכן ביותר הנתמך על ידי 365 ליצירת דו-קיום בין סביבת הענן לסביבה הארגונית, כל משתמש שנוצר בסביבה הארגונית מסתנכרן לענן (במידה ולא הופעל סינון המונע זאת), יש לקחת בחשבון שהרשיון לא מופעל באופן אוטומטית אלא ידני.

מאפיינים של משתמשים שעברו שינוי בארגון מתעדכנים גם אל הענן, משתמש אשר נמחק בארגון נמחק גם מהענן אך יש לבטל את הרישיון בצורה ידנית.

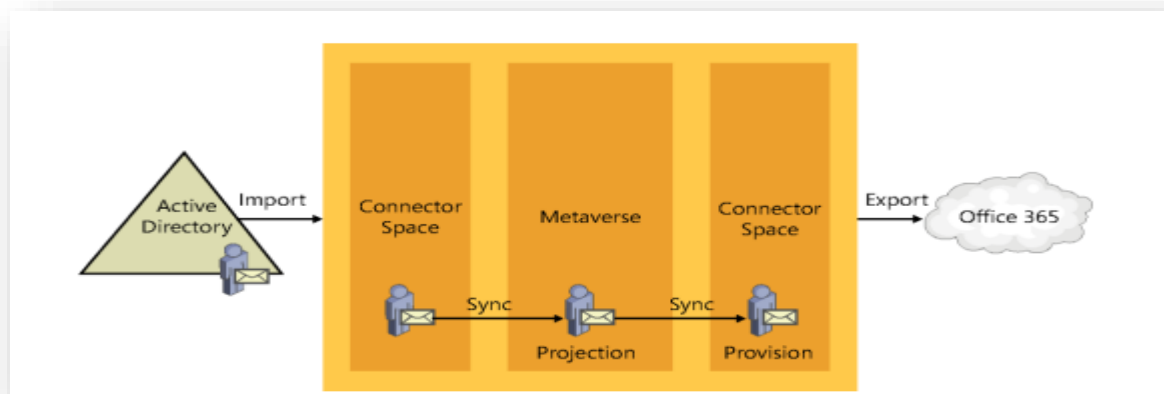
השימוש בכלי מאפשר לנו לערוך את כל השינויים הארגוניים בתוך הארגון ולנהל בסביבת הענן רק את נושאי הרישוי, בענן לא נוכל לערוך מאפיינים של משתמשים שסונכרנו מהארגון.



בתמונה אנו רואים את התהליך שבו מנוע הסנכרון של AD CONNECT מושך מידע משרתי הארגון ומחיל כללי סינון שהוגדרו מראש, אנו יכולים להבחין שהמידע שעולה לענן שונה מהמידע שנמשך מהשרת עקב החלת כללים שהוגדרו מראש

כל המידע הארגוני עובר למקום הנקרא Connector Space שלמעשה מכיל עותק מדויק של AD. בשלב הבא מבוצע סינון לפי כללים שהגדרנו מראש לגבי אילו משתמשים ואילו מאפיינים יסונכרנו לענן, האובייקטים הללו עוברים לאזור שנקרא metaverse ומשם מסונכרנים לענן.

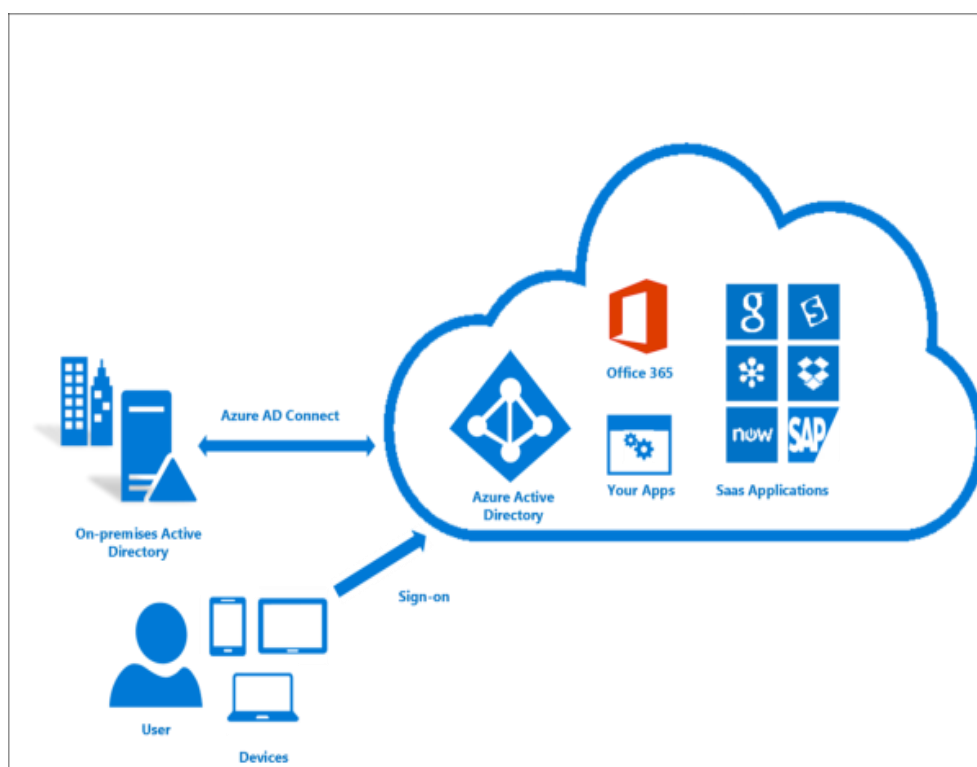
לתהליך בו אובייקט מאופשר להסתנכרן אל הענן ולמעשה לעבור מ- Connector Space אל metaverse ומשם לענן קוראים projection.



בשלב הבא ייווצר אובייקט חדש המכיל את הכללים הרלוונטיים ומשם הוא יסונכרן לענן שם הוא ירשם ב AZURE AD

התהליך הזה יחזור על עצמו כל 30 דקות עבור כל אובייקט ב-AD למשך כל הזמן שהוא קיים.

## התקנת AZURE AD CONNECT



לפני שנתקין את הכלי נצטרך לעמוד בדרישות המקדימות:

- Microsoft .NET Framework 4.5.1 or later.
- Windows PowerShell 3.0 or later.
- Windows Azure AD Module for Windows PowerShell (64-bit version).

כמו כן, המלצה בסביבת עבודה לא להתקין על שרתי DC.

מידע נוסף על הדרישות המקדימות בקישור הבא:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-prerequisites>

### הכלי משתמש במס' חשבונות משתמש:

AD DS Connector account – חשבון זה משמש לכתוב מידע לשרתי AD הארגוניים

ADSync service account – חשבון זה נועד להריץ את שירות הסנכרון ולהתממשק לבסיס הנתונים בשרת SQL

Azure AD Connector account – חשבון זה נועד לכתוב מידע ל AZURE AD

כמו כן, נצטרך הרשאה של מנהל מקומי על מנת להתקין את הכלי והרשאה של Enterprise Admin בארגון והרשאת Global Admin בענן.

בתהליך ההתקנה נוצרים לנו שני חשבונות בסביבה הארגונית:

MSOL\_id – חשבון זה נועד לסנכרן מידע מהארגון אל הענן (לעיתים נרצה להעניק לו הרשאת כתיבה על מנת שיוכל לשנות מאפיינים עבור משתמשים לדוגמא: שינוי סיסמה)

AAD\_id – חשבון זה נועד להריץ את שירות הסנכרון והוא מקבל סיסמה מסובכת רנדומלית שלעולם אינה משתנה, חשבון זה בעל הרשאות קריאה בארגון על מנת שיוכל לקרוא את המידע ויש לו הרשאות כתיבה לענן – אסור לשנות את ההגדרות של חשבון זה לאחר ההתקנה כיוון שדבר זה יוביל לעצירת תהליך הסנכרון

מידע נוסף בקישור הבא:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

AAD Connect דורש גם שימוש בשרת SQL, בתור ברירת מחדל בשלב ההתקנה מותקן שרת SQL 2012 Express שרת חינמי בעל מגבלת בסיס נתונים של 10GB המאפשר לנהל עד 100,000 אובייקטים בערך. לארגונים גדולים יהיה צורך בהתקנת שרת SQL עצמאי.

ניתן להתקין את AAD Connect בשתי תצורות Express ו-Custom – התקנת Express היא ברירת המחדל והיא הנפוצה ביותר.

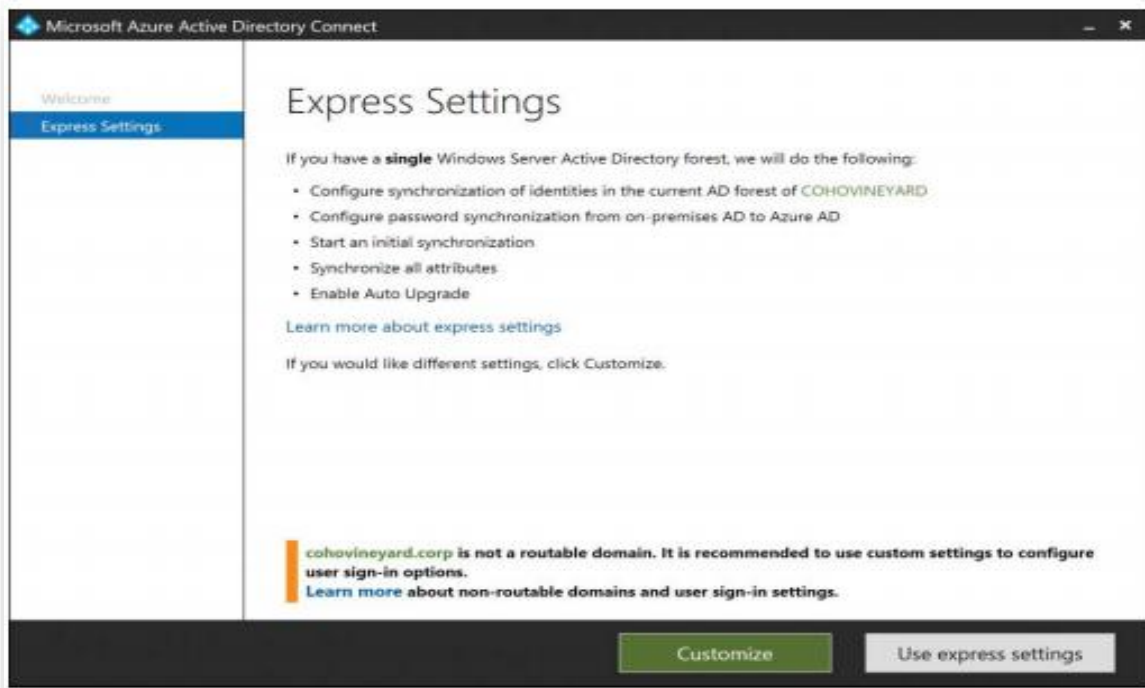
ניתן לשנות מאפיינים רבים גם לאחר ההתקנה ולכן הכי נוח להתחיל בהתקנה מהסוג הזה, ההתקנה הזו מסנכרנת את הסיסמאות הארגוניות בתור ברירת מחדל.



נבחר להשתמש בסוג זה של התקנה כאשר:

יש לנו דומיין אחד ויער אחד, נרצה שהמשתמשים יבצעו גישה באמצעות הסיסמה הארגונית לכלל השירותים. התקנה זו מתאימה למצב בו אנו רוצים להחיל את הסנכרון עם כמה שפחות שאלות ובצורה המהירה ביותר. אם נרצה להחיל כללי סינון או אפשרות של שינוי סיסמה מהענן אל הארגון לא נוכל לבצע זאת בהתקנה מהסוג הזה למרות שנוכל בשלב מאוחר יותר לשנות את ההגדרות.

בתמונה מסך ההתקנה של AAD Connect בו נבחר התקנה מהירה:



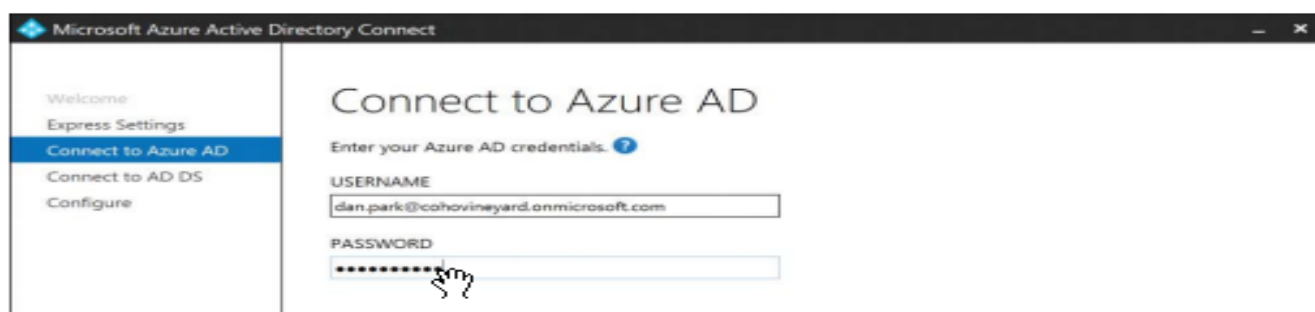
\*\*\* בקישור הבא מעבר על שלבי ההתקנה:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express>

כחלק מתהליך ההתקנה נבדק UPN SUFFIX בו עושה שימוש הארגון, אם הוא לא ניתן לניתוב כלומר הארגון משתמש בסיומת פנימית (local או prod. וכו...) תופיע לנו אזהרה, מה שבפועל יקרה הוא שהמשתמשים יצטרכו לבצע כניסה לדומיין שיוצר לנו בענן בפורמט הבא: onmicrosoft.com. <שם הדומיין שלנו> התוספת של onmicrosoft.com משמעותה שהמשתמשים לא יוכלו לגשת לתיבת המייל הארגונית שלהם כפי שהיא רשומה בארגון ולא נוכל לעשות שימוש בשרתי AD FS. לכן מראש נצטרך לרכוש שם דומיין זהה לדומיין שלנו ולבצע את ההעברה בפורטל של 365. לחילופין נוכל להוסיף UPN נוסף לארגון על מנת לצור חווית כניסה אחידה הן לארגון והן לענן.

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide>

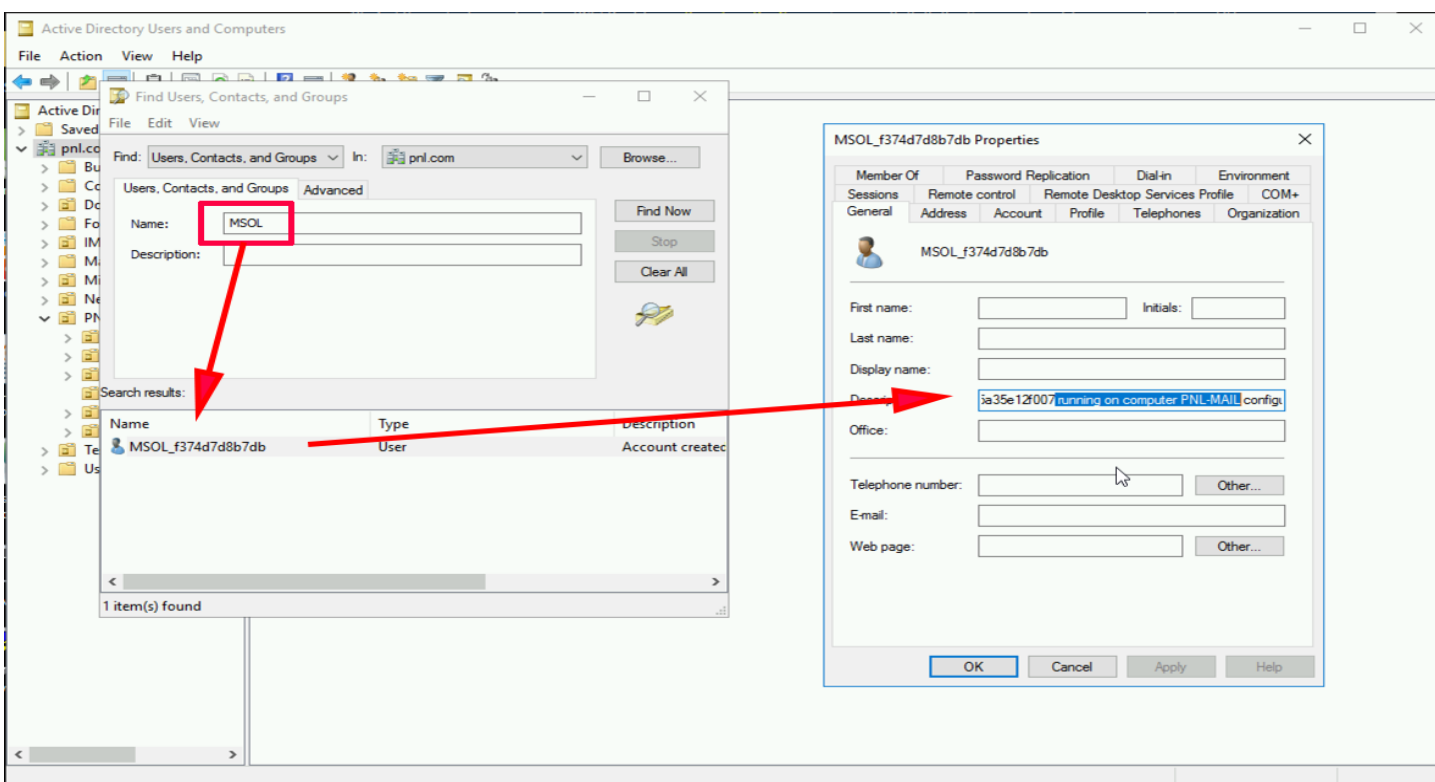
לאחר שנבחר בהתקנה מסוג אקספרס נצטרך להזין את חשבון המנהל ב- AZURE AD



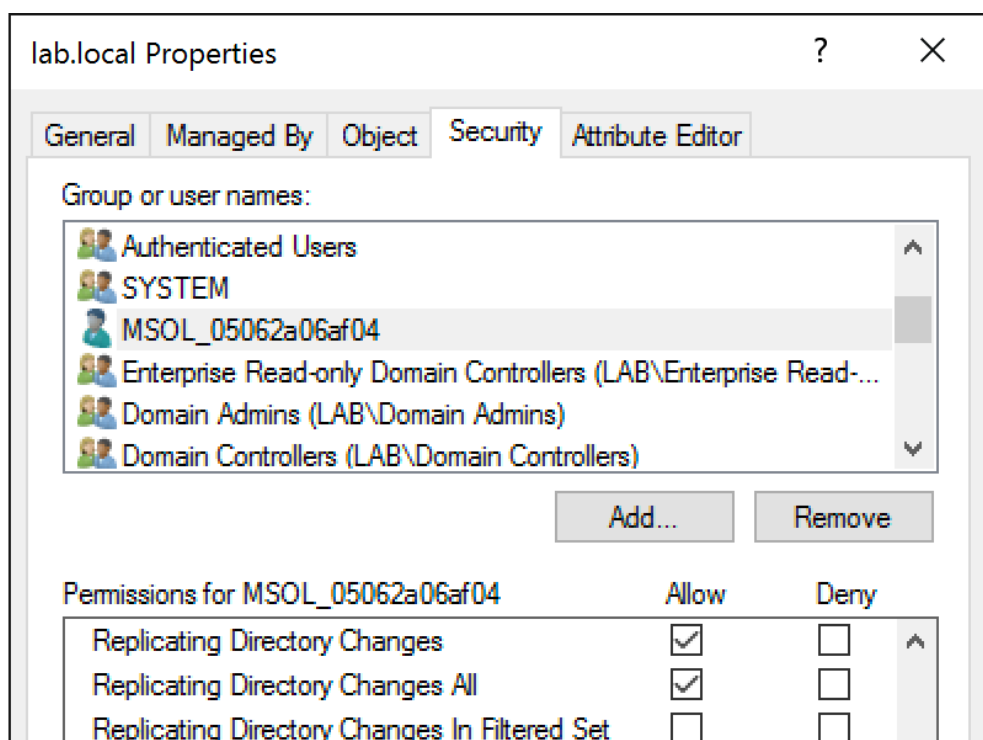
לאחר מכן נתחבר עם הרשאות Enterprise Admin:



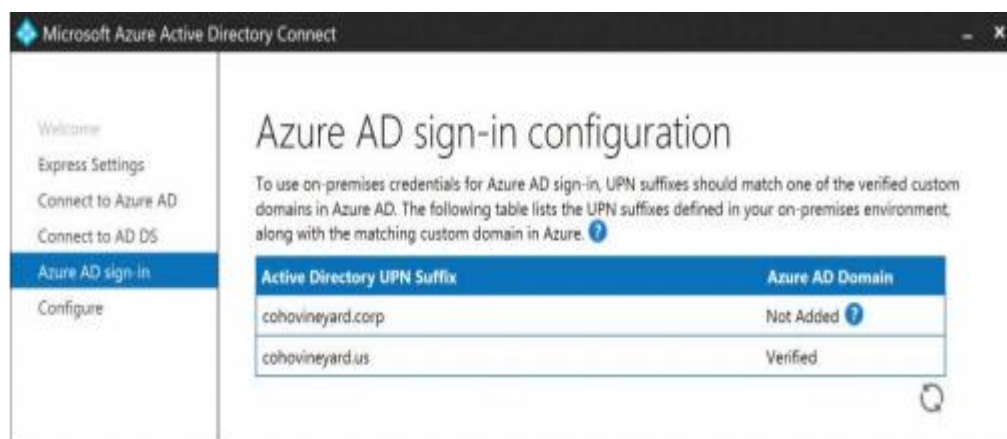
לאחר מכן ייוצר לנו חשבון למטרות הסנכרון שיתחיל ב- MSOL\_ ולאחר מכן GUID רנדומלי



לחשבון הזה יהיו את ההרשאות הנחוצות לסנכרון סיסמאות לענן :

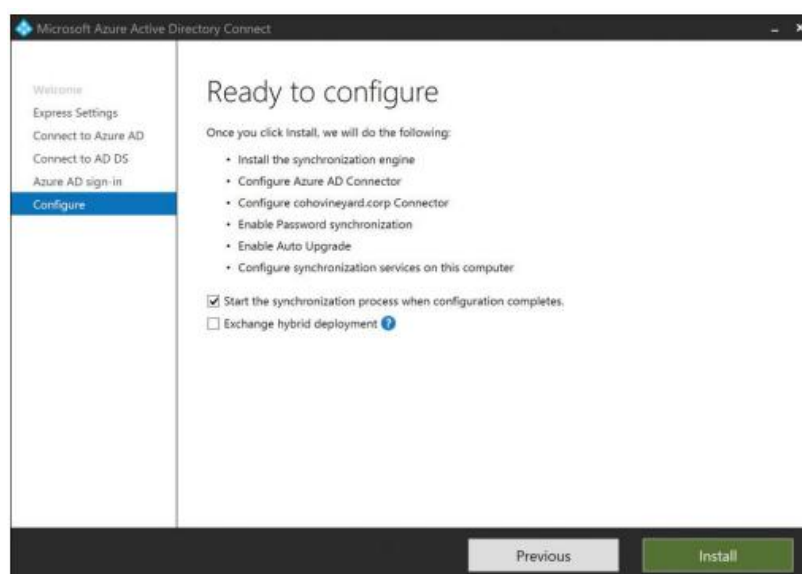


בשלב הבא תוצג לנו רשימת הסימנות בארגון



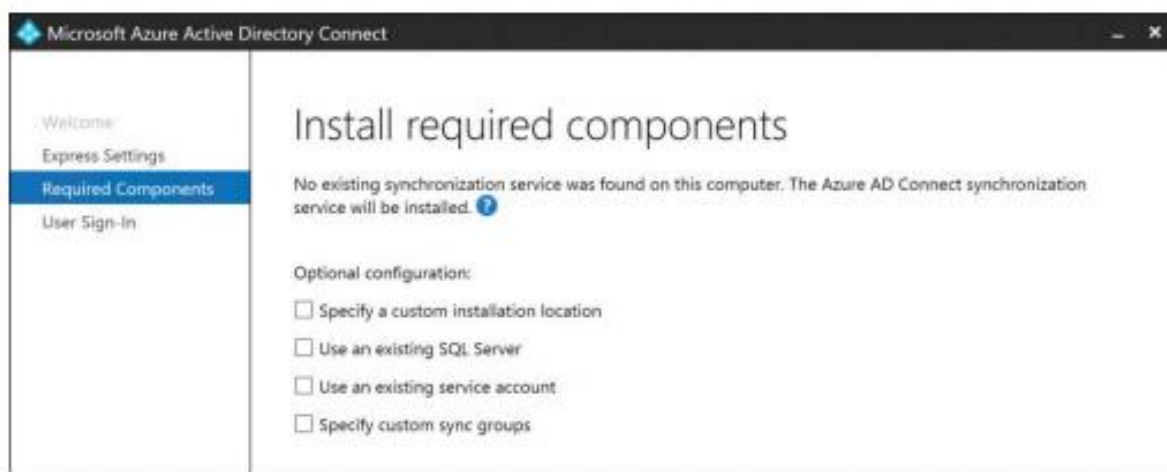
סיומות שיסומנו כ-Not Added יגרמו להצגת אזהרה המתריעה על כך שמשתמשים בארגון לא יוכלו לבצע כניסה לשירותי הענן באמצעות החשבון הארגוני שלהם, אם המשתמשים שלך כבר עובדים עם UPN שרשמת קודם בענן או שאנו מתכוונים לשנות זאת בהמשך.

נוכל להתעלם מהאזהרה הזו ולהתקדם הלאה ולסמן לאשף ההתקנה להתחיל לסנכרן אובייקטים לענן.



## התקנה מותאמת אישית:

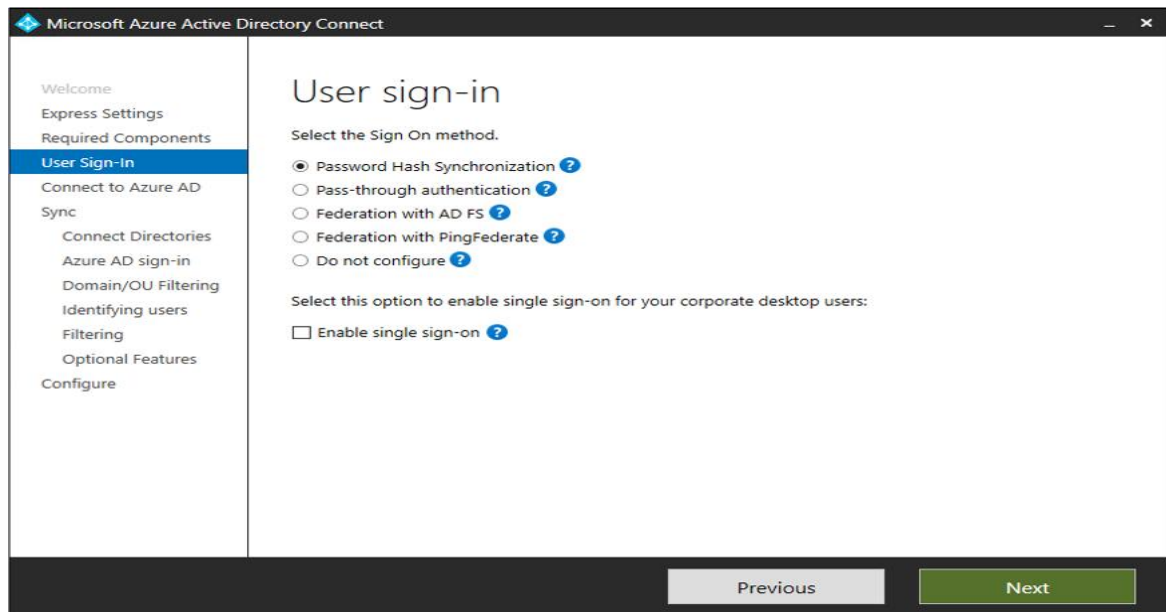
תהליך ההתקנה המותאם אישית שונה משמעותית בכך שיש לנו שליטה על כל פרמטר בכל שלב, במסך הראשון נוכל לבחור את מיקום ההתקנה, שימוש בשרת SQL וחשבונות קיימים וכמו כן שמות קבוצות הסנכרון (מפורטים בטבלה).



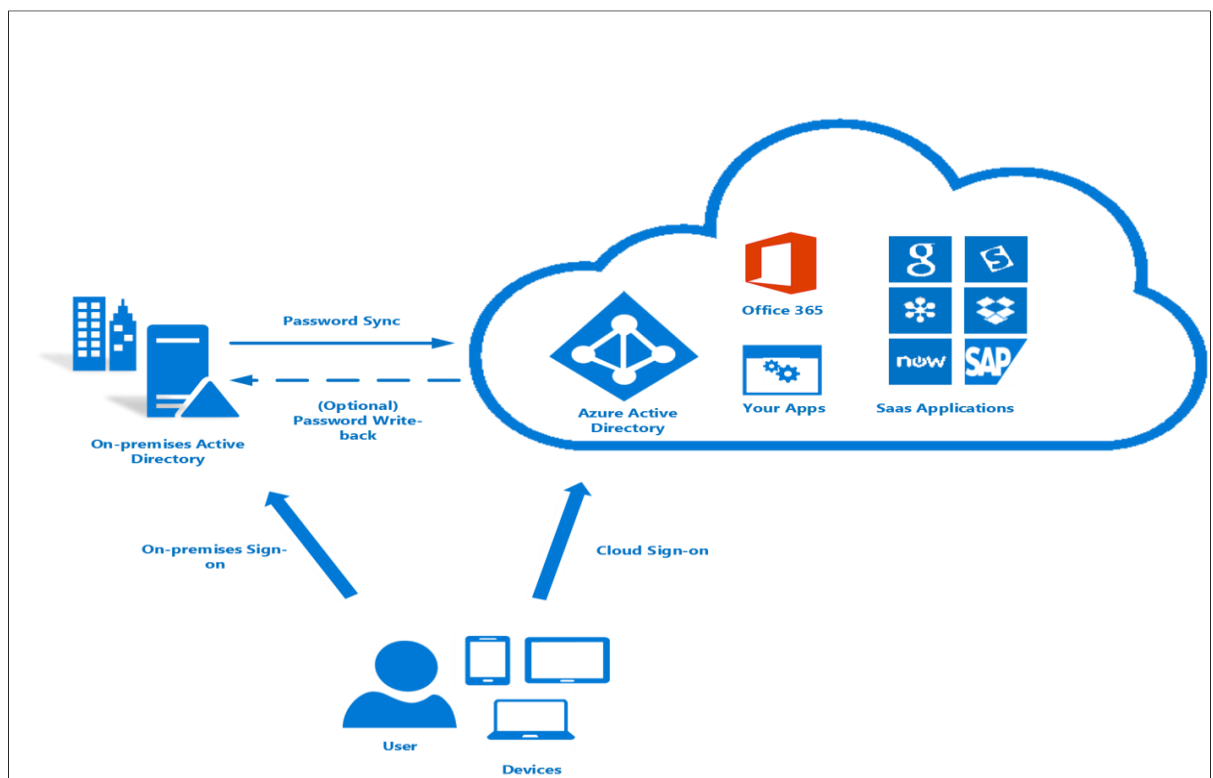
קבוצות הסנכרון שנוצרות בשלב ההתקנה וההרשאות שלהן:

Group Name	Permissions
ADSyncAdmins	Full rights to the AAD Connect tool
ADSyncOperators	Able to view operations run history; cannot view connectors or objects; able to view sync rules but unable to edit or delete
ADSyncBrowse	No access to the Sync service console and cannot view Synchronization rules
ADSyncPasswordSet	No access to the Sync service console and cannot view Synchronization rules

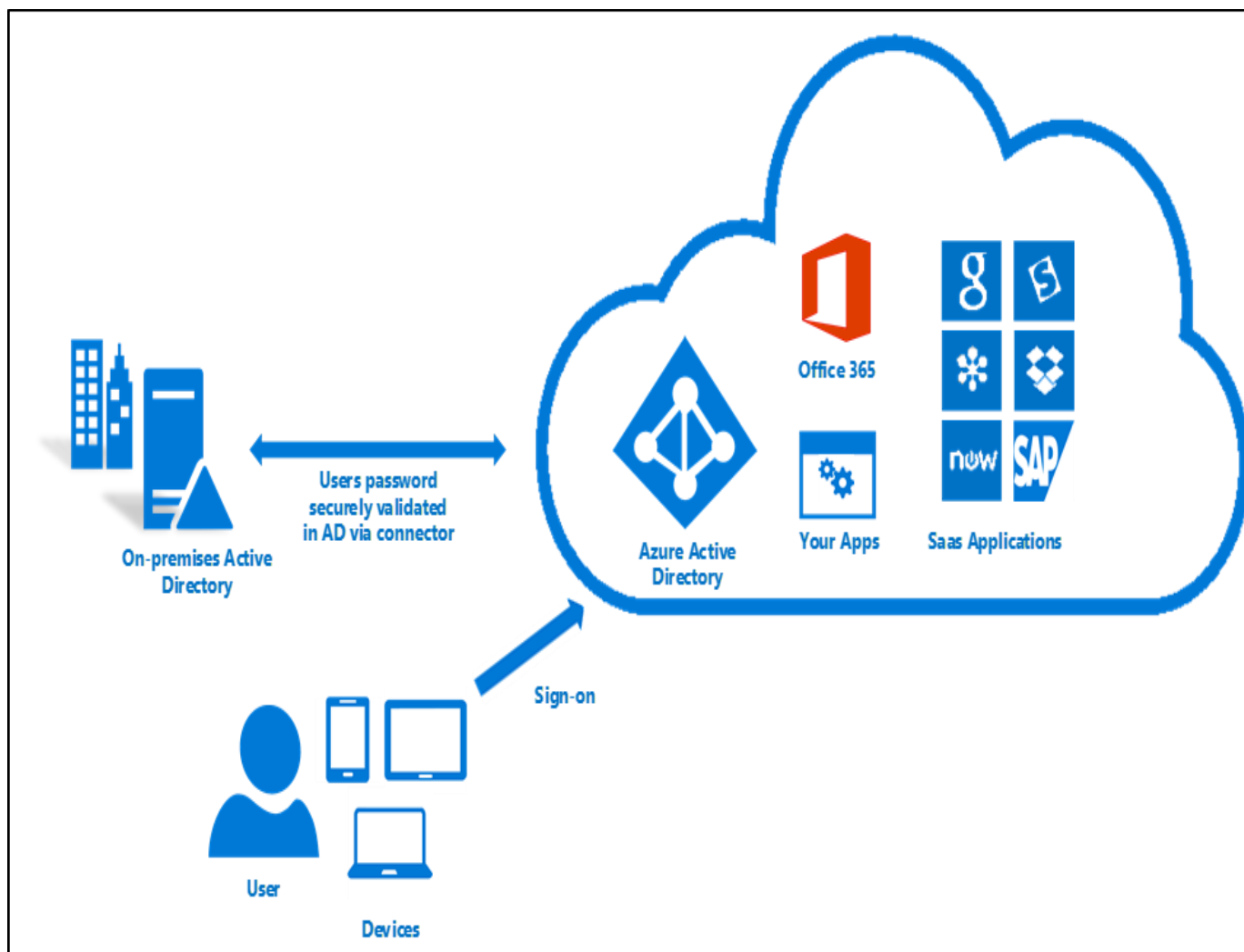
לאחר מכן נצטרך לקבוע כיצד המשתמשים יבצעו גישה לענן ולמעשה כיצד יסונכרנו הסיסמאות:



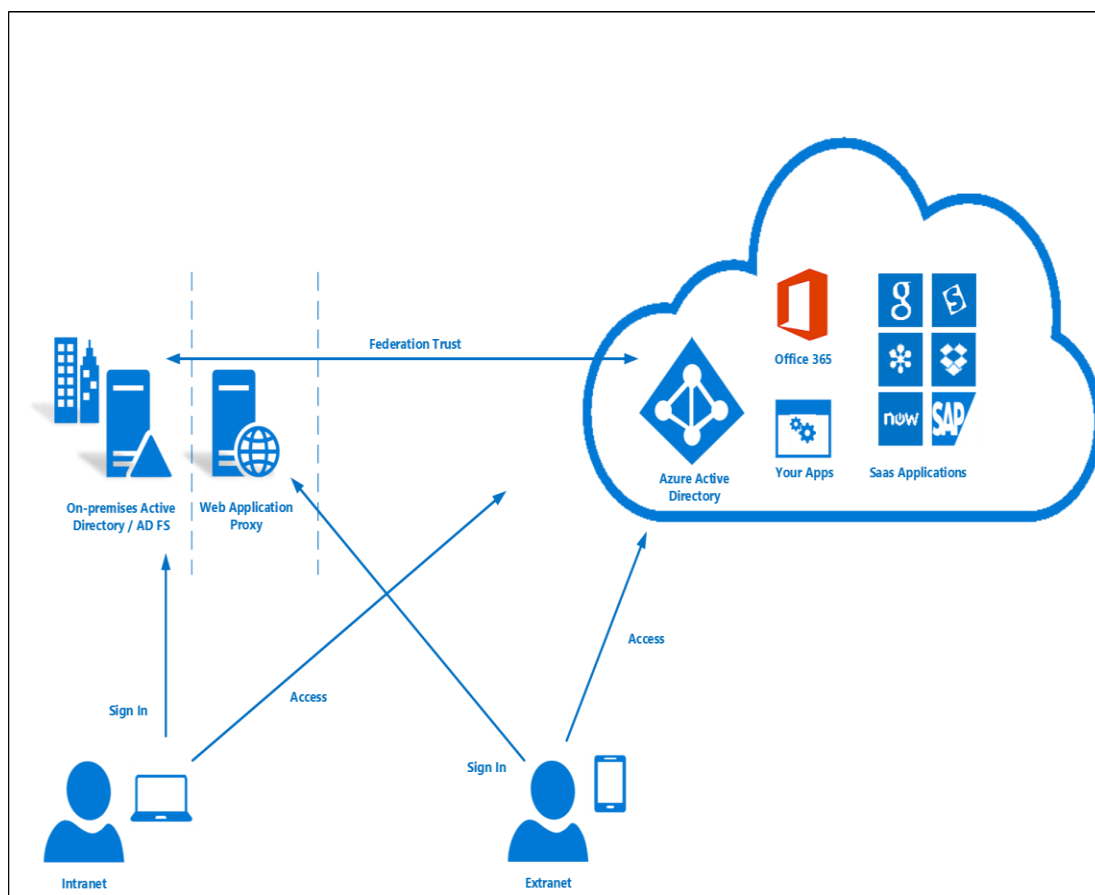
**Password hash synchronization** – הסיסמאות עוברות מגננון ערבול (HASH) והסיסמה המעורבלת מסונכרנת לענן, כאשר קורה שינוי בארגון, הענן מתעדכן לגביו. ניתן להוסיף את היכולת לסנכרן סיסמאות מהענן אל הארגון (password write-back). היתרון עבור המשתמשים הוא היכולת לבצע SSO לכלל השירותים.



**Pass-through authentication** – מנגנון זה מבטיח שהסיסמאות יאומתו מול שרתי הארגון ולא יוחזקו בענן, בצורה כזו נוכל לבצע הגבלות מחמירות יותר כמו לדוגמא מניעת כניסה בשעות מסוימות וביצוע מעקב אחר המשתמשים.

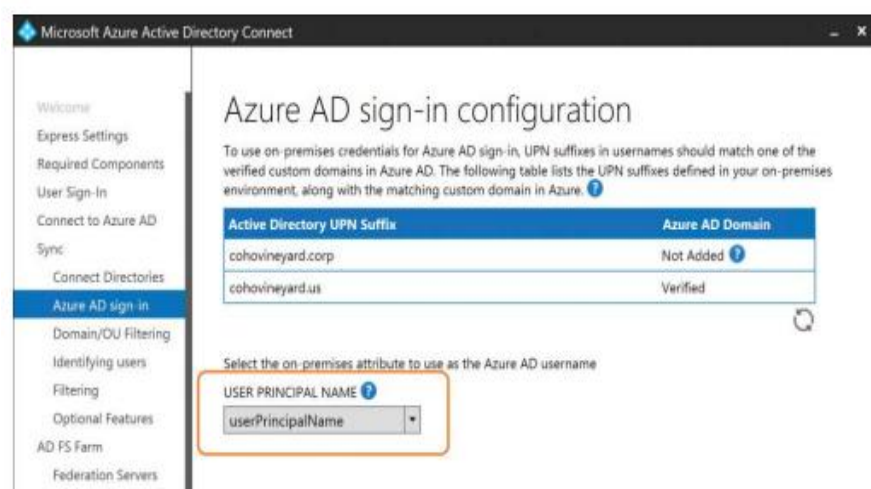


**Federation with AD FS** - בתצורה זו אנו עושים שימוש בשרתי AD FS לביצוע תהליך האימות, נצטרך לבנות תשתית עם שרתי AD FS ושרתי WAP וכמו כן להתקין תעודות SSL.



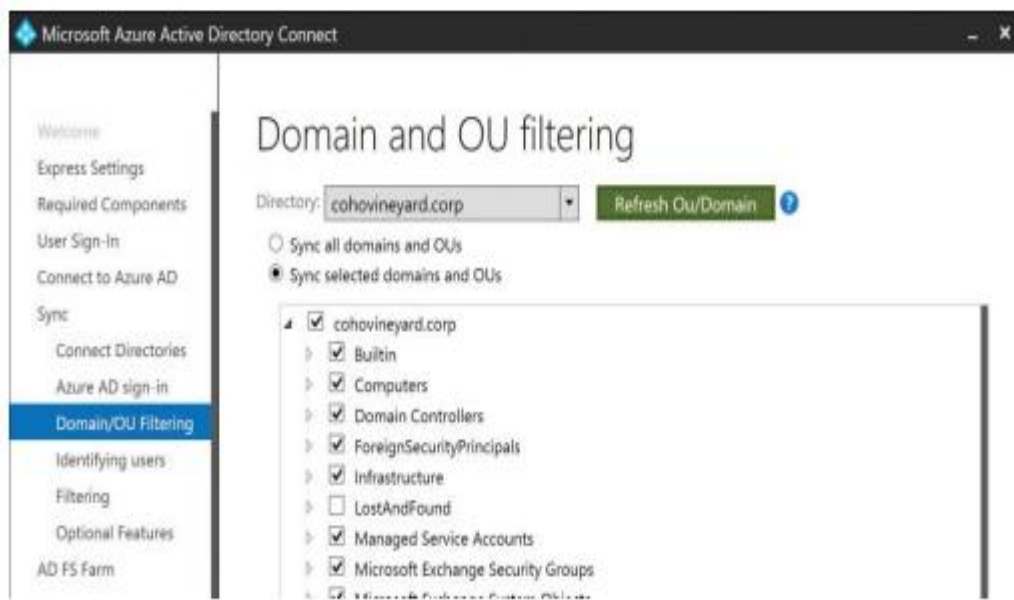
בשלב הבא נתחבר לשירות הענן עם חשבון ניהולי וכמו כן לארגון (זהה להתקנת אקספרס)

לאחר מכן תוצג לנו ההודעה לגבי UPN SUFFIX אותם נרצה לסנכרן, הפעם גם נוכל לבחור איזה מאפיין יישמש כשם המשתמש ב AAD – הפעולה הזו בלתי הפיכה אם נרצה לבצע שינוי למאפיין לאחר ההתקנה נצטרך להסיר את הכלי ולמחוק את המשתמשים מהענן.

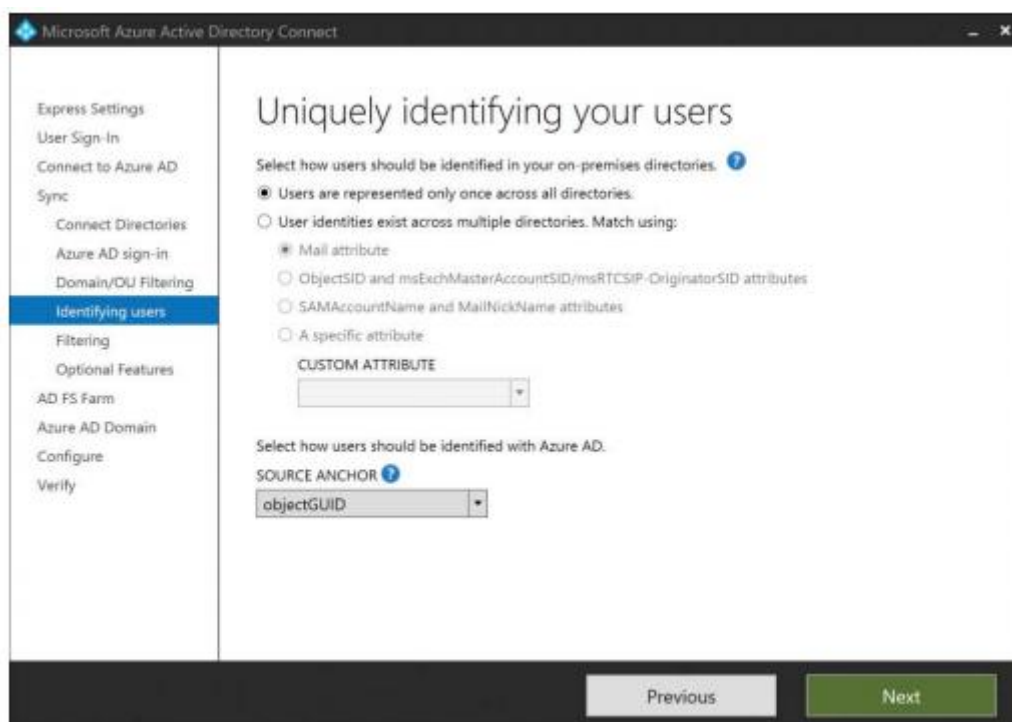




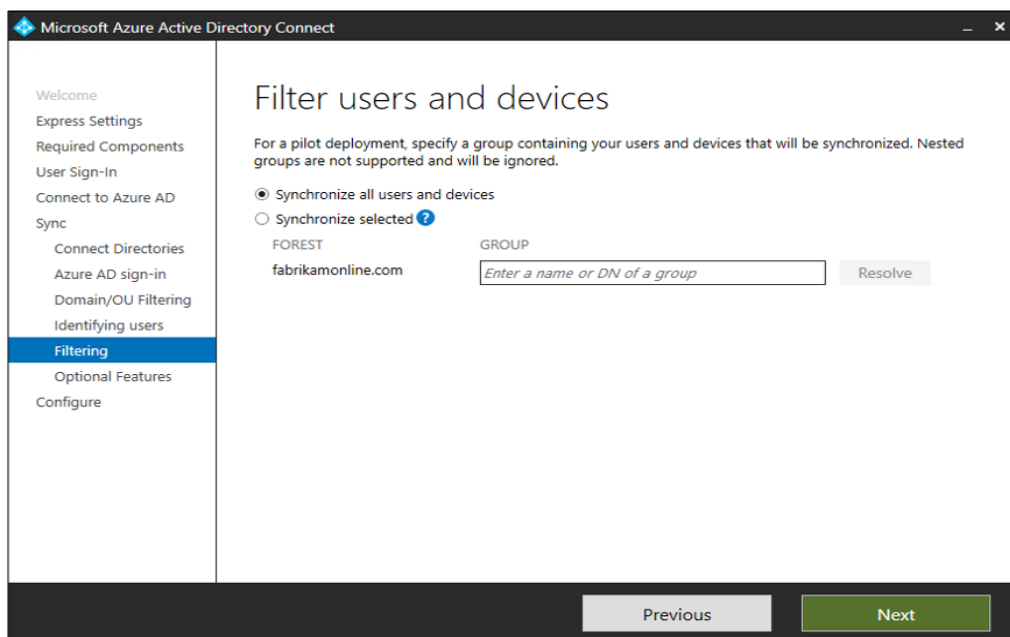
בשלב הבא נוכל לבחור את מי לסנכרן ואת מי לא ולבצע ישירות סינון בשלב ההתקנה.



בשלב הבא נבחר כיצד מנגנון הסנכרון יודא שהמשתמשים הם יחודיים בארגון, בדומיין יחיד ביער נבחר באפשרות הראשונה, ביער מרובה דומיינים יכול להיווצר מצב עם משתמשים בעלי אותו שם לכן נצטרך לבחור מאפיין שמיידח את המשתמשים שלי מיתר המשתמשים.

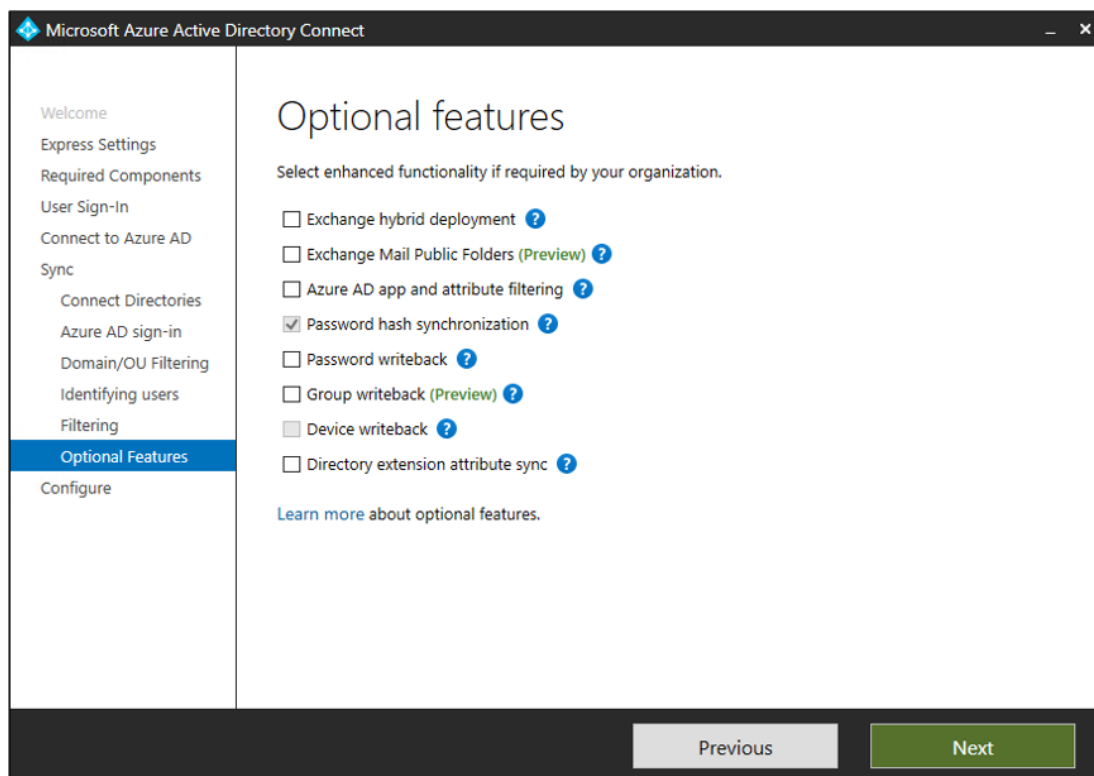


בשלב הבא נוכל לבצע סינון נוסף בהתאם לשיוך קבוצתי של המשתמשים וההתקנים שלהם:



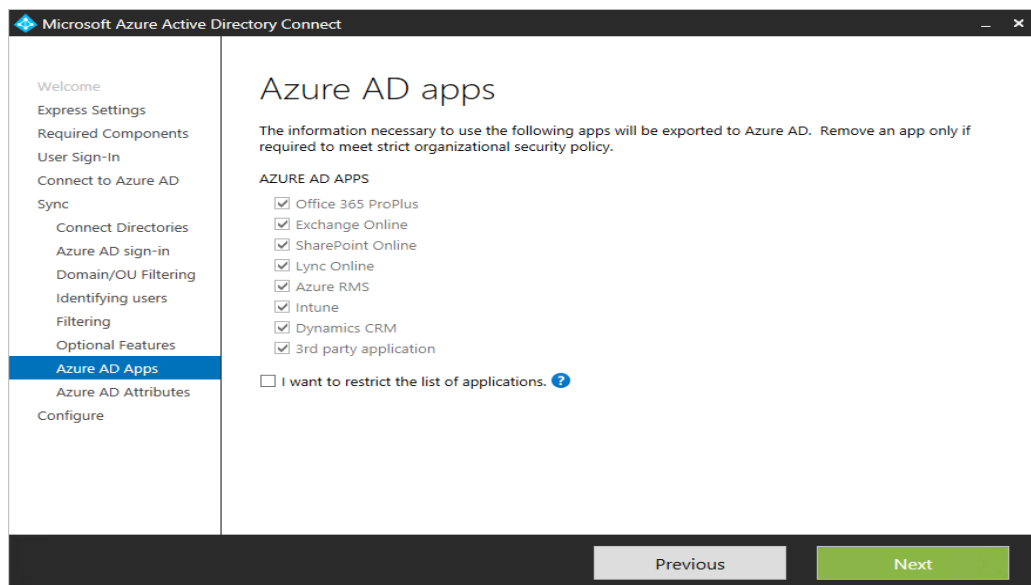
The screenshot shows the 'Filter users and devices' step in the Microsoft Azure Active Directory Connect wizard. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering (highlighted), Optional Features, and Configure. The main content area is titled 'Filter users and devices' and includes the following text: 'For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.' Below this text are two radio buttons: 'Synchronize all users and devices' (selected) and 'Synchronize selected' (with a question mark icon). Under the 'Synchronize selected' option, there are two sections: 'FOREST' with the value 'fabrikamonline.com' and 'GROUP' with a text input field containing the placeholder 'Enter a name or DN of a group'. A 'Resolve' button is located to the right of the input field. At the bottom of the window are 'Previous' and 'Next' buttons.

באפשרויות מתקדמות נוכל לבחור לדוגמא את היכולת לסנכרן סיסמאות מהענן אל הארגון, לסנכרן מאפיינים ספיציפיים לענן ועוד (פירוט נמצא בקישור):



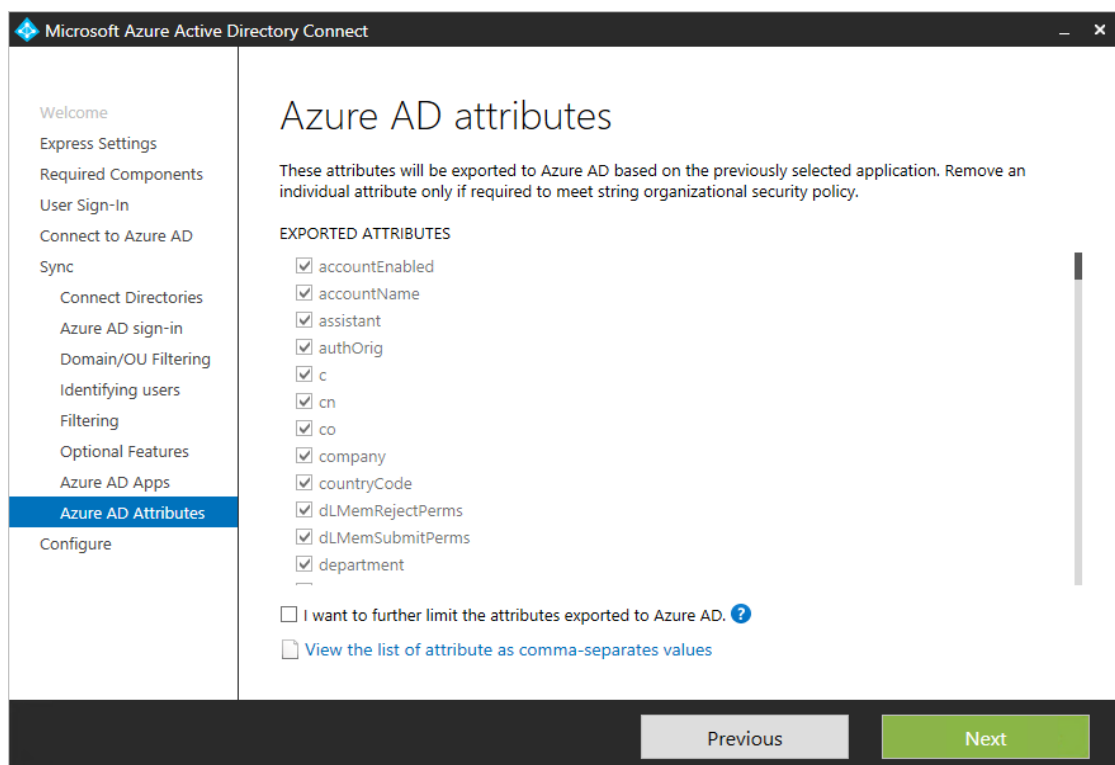
The screenshot shows the 'Optional features' step in the Microsoft Azure Active Directory Connect wizard. The left sidebar is identical to the previous screenshot, with 'Optional Features' highlighted. The main content area is titled 'Optional features' and includes the text: 'Select enhanced functionality if required by your organization.' Below this text is a list of optional features with checkboxes: 'Exchange hybrid deployment' (unchecked), 'Exchange Mail Public Folders (Preview)' (unchecked), 'Azure AD app and attribute filtering' (unchecked), 'Password hash synchronization' (checked), 'Password writeback' (unchecked), 'Group writeback (Preview)' (unchecked), 'Device writeback' (unchecked), and 'Directory extension attribute sync' (unchecked). Each item has a question mark icon to its right. At the bottom of the list is a link: 'Learn more about optional features.' At the bottom of the window are 'Previous' and 'Next' buttons.

נוכל לבחור להגביל אפליקציות שונות בענן מלגשת אל המידע (נעשה זאת רק אם מדיניות האבטחה אוסרת זאת בפירוש).



The screenshot shows the 'Azure AD apps' configuration window. On the left, a navigation pane lists steps from 'Welcome' to 'Configure'. The 'Azure AD Apps' step is selected. The main area, titled 'Azure AD apps', contains a message: 'The information necessary to use the following apps will be exported to Azure AD. Remove an app only if required to meet strict organizational security policy.' Below this, under 'AZURE AD APPS', there is a list of applications with checkboxes: Office 365 ProPlus, Exchange Online, SharePoint Online, Lync Online, Azure RMS, Intune, Dynamics CRM, and 3rd party application. All are checked. At the bottom, there is an unchecked checkbox: 'I want to restrict the list of applications.' with a help icon. 'Previous' and 'Next' buttons are at the bottom right.

נוכל להגביל את המאפיינים שיוסגרו אל הענן – שוב בהתאם למדיניות האבטחה הארגונית (יש לקחת בחשבון את ההשלכות של צעדים אלו)



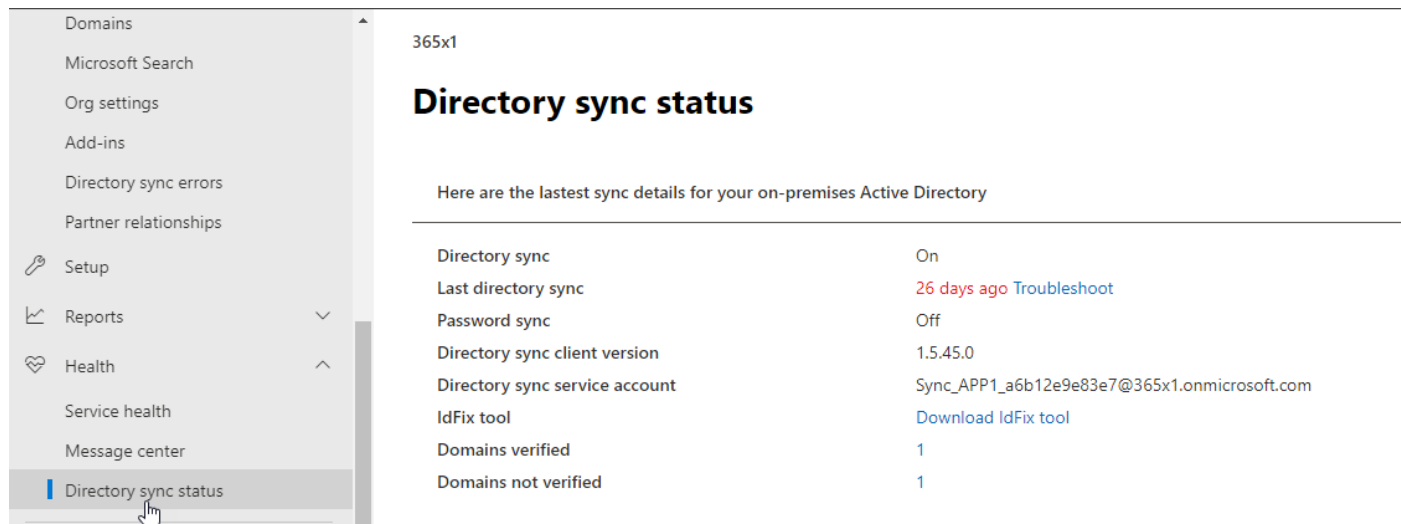
The screenshot shows the 'Azure AD attributes' configuration window. The left navigation pane is the same as the previous screen, with 'Azure AD Attributes' selected. The main area, titled 'Azure AD attributes', contains a message: 'These attributes will be exported to Azure AD based on the previously selected application. Remove an individual attribute only if required to meet string organizational security policy.' Below this, under 'EXPORTED ATTRIBUTES', there is a list of attributes with checkboxes: accountEnabled, accountName, assistant, authOrig, c, cn, co, company, countryCode, dLMemRejectPerms, dLMemSubmitPerms, and department. All are checked. At the bottom, there is an unchecked checkbox: 'I want to further limit the attributes exported to Azure AD.' with a help icon, and a link: 'View the list of attribute as comma-separated values'. 'Previous' and 'Next' buttons are at the bottom right.

מידע מפורט על שלבי ההתקנה נמצא בקישור הבא:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

## ביצוע ניטור לתהליך הסנכרון:

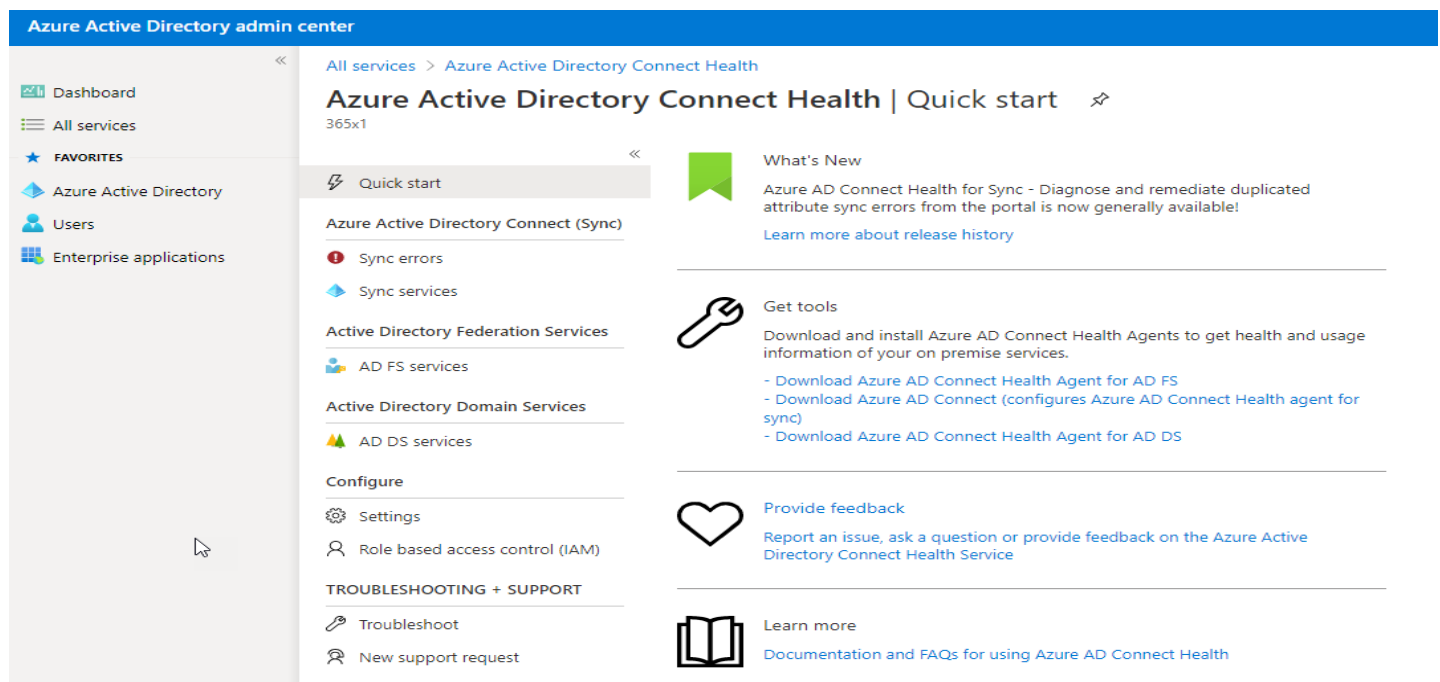
ישנם מספר כלים בהם נוכל להשתמש על מנת לבחון את תקינות תהליך הסנכרון, בפורטל הארגוני של 365 נוכל לקבל מידע כללי על תקינות התהליך:



## Azure AD Connect Health

באמצעות שימוש בכלי אליו ניגש מפורטל הניהול של AZURE AD נוכל לבצע ניטור לתהליך הסנכרון יש לקחת בחשבון שדרוש לנו חשבון Azure AD Premium

על מנת לקבל תמונה מלאה נצטרך להוריד ולהתקין AGENT בשרת בו מותקן AD CONNECT ובשרתי AD.DS



<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-azure-ad-connect>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-sync>

## שימוש ב-Powershell

ניתן להשתמש בפקודות לאחר חיבור לענן על מנת לבחון את מצב הסנכרון:

```
Import-Module MSOnline
```

```
Connect-MsolService
```

```
Get-MsolCompanyInformation | fl LastDirSyncTime
```

```
Get-MSOUser -ALL | Select-Object UserPrincipalName, LastDirSyncTime | Export-CSV  
C:\Temp\SyncStatus.CSV
```

**שימוש ב- EVENTLOG** - נוכל לבצע קריאה של הלוגים שנוצרו במחשב על מנת לוודא את תקינות השירות

## טיפול בבעיות סנכרון

חלק גדול מניהול התהליך הינו איתור וטיפול בתקלות הקורות בזמן הסנכרון.

בקישורים הבאים מידע לגבי טיפול בתקלות נפוצות.

- טיפול בתקלות בשלב ההתקנה:

<https://docs.microsoft.com/en-us/troubleshoot/azure/active-directory/installation-configuration-wizard-errors>

- טיפול בבעיות סנכרון:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-objects-sync>