Besuchen Sie uns im Internet unter
http://www.vobs.at/rb

Vorarlberger Standardschulinstallation

Office365
Active Directory
Verzeichnissynchronisation

Inhalt

Wir Regionalbetreuer hoffen, Euch auch mit der vorliegenden Dokumentation eine brauchbare Step by Step-Anleitung anbieten zu können.

Danke Thomas Hauser! Wo wären wir ohne Deine Hilfe. Ich wüsste nicht, was wir ohne Deinen Support täten.

Änderungswünsche und Feedback bitte an Andreas Renner support@bgbr.snv.at

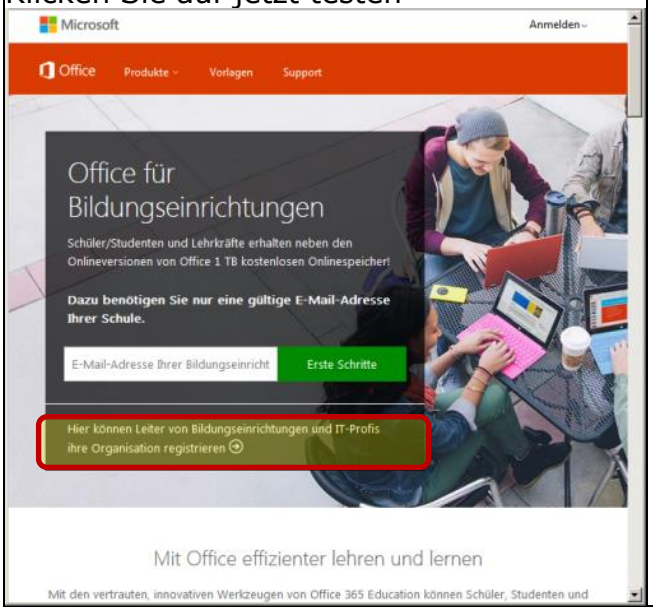
1 Anlegen eines Office 365 Tenants für Bildungseinrichtungen

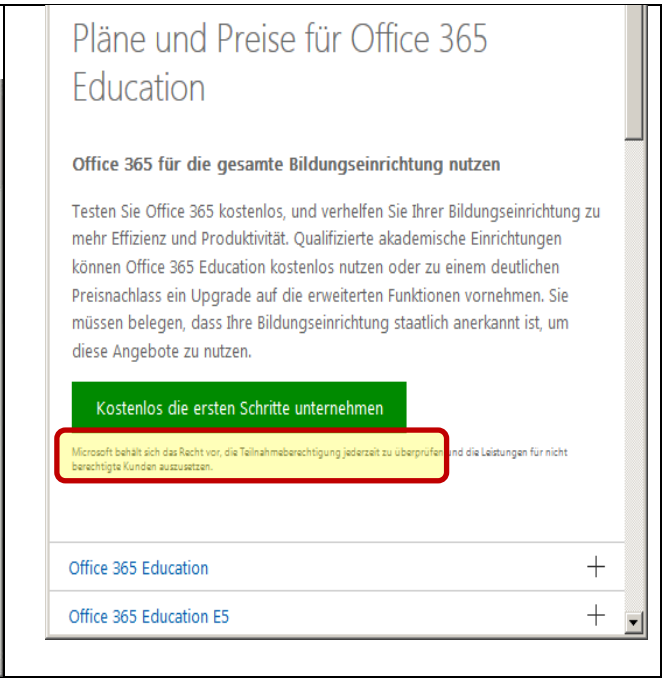
Mit Office 365 Student bietet Microsoft allen SchülerInnen und bald auch LehrerInnen ein gratis Office Paket und die Microsoft Cloud Services. Wir müssen das Angebot von Microsoft umsetzen. Am elegantesten sollte das per Synchronisation des Active Directory funktionieren. Laut Thomas Hauser (Microsoft Austria) könnte man später eine neue Domäne erstellen. Wenn die Benutzer in der neuen Domäne dieselben Benutzernamen erhalten, sollte sich bezüglich dieser online Dienste nichts ändern.
Die folgende Dokumentation zeigt step-by-step, wie Sie Ihr Active Directory mit dem Microsoft online Azure Active Directory synchronisieren.

In dem Beispielfall sind die Kerndaten der Office365 Domäne und AD Domäne wie folgt:
- Active Directory Domäne (AD): schule.ahs
- AD Administrator: admin@schule.ahs
- Office365 Domäne: bgbr.onmicrosoft.com
- Office365 Domäne Administrator: admin@bgbr.onmicrosoft.com
- bgbr ist der Vorarlberger Schulkürzel unserer Schule, wie in den Vorarlberger Bildungsservices (VOBS) und damit auf mail.snv.at definiert.

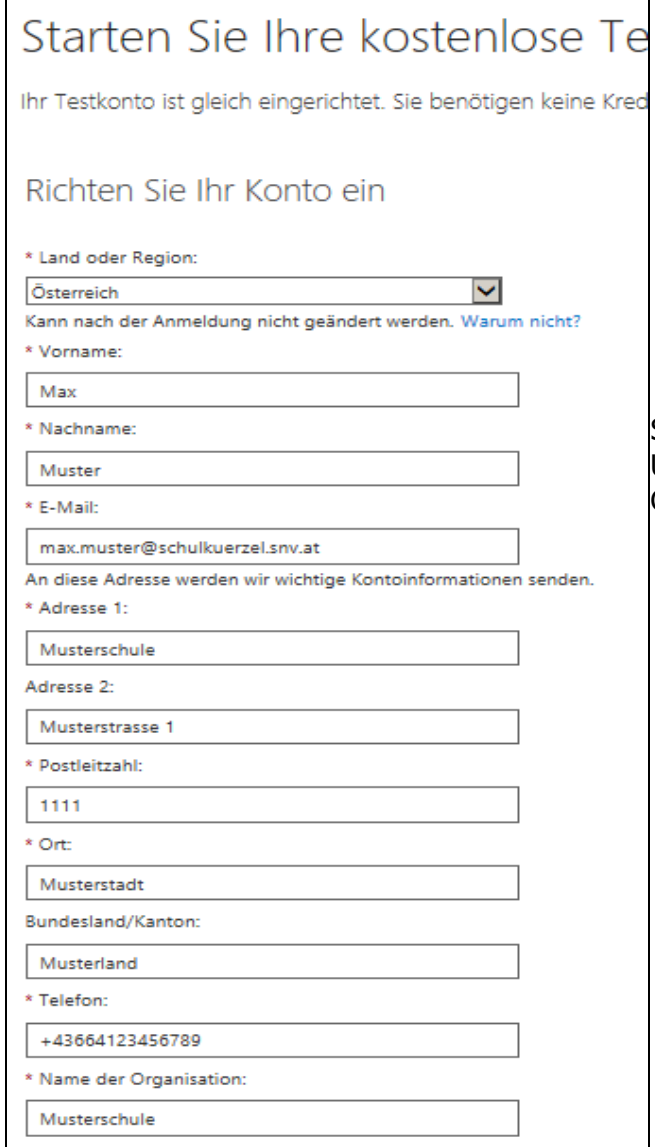
PASSEN SIE DEN SCHULKÜRZEL bgbr AN IHRE AZURE DOMÄNE AN

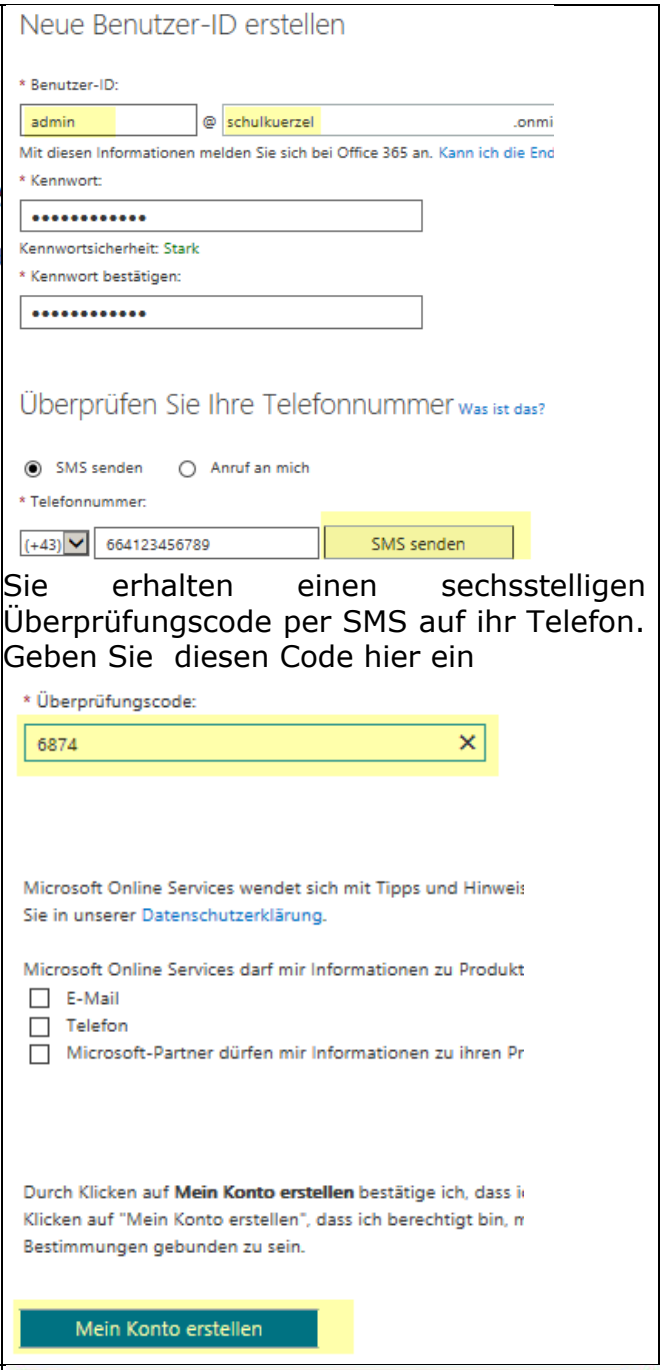
Auf http://office.com/academic
Klicken Sie auf jetzt testen





Das Anmeldeformular wird hin und wieder geändert.



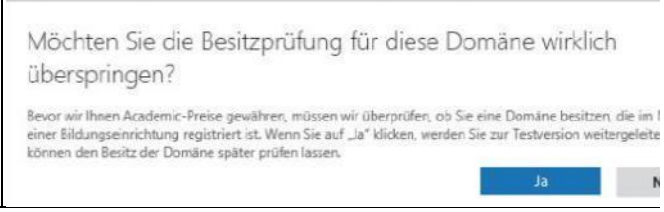


Sie erhalten einen sechsstelligen Überprüfungscode per SMS auf ihr Telefon. Geben Sie diesen Code hier ein

Benutzer ID
admin@schulkuerzel.onmicrosoft.com

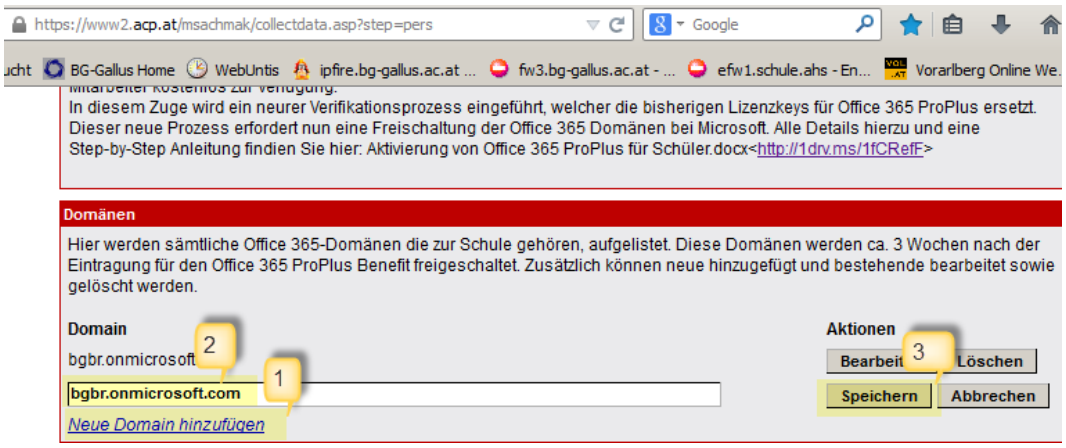
Nach dem Ausfüllen des Anmeldeformulars gelangen Sie auf die Seite „Überprüfen der Berechtigung für Microsoft Office 365 Education“, auf der Sie die Domäne Ihrer Bildungseinrichtung angeben und überprüfen lassen können.

Bestätigen Sie die Abfrage „Möchten Sie die Berechtigung für diese Domäne wirklich überspringen?
mit JA



2 Freischalten der Domäne für OFFICE 365 PROPLUS

Damit Sie mit Ihrem Office 365 Tenant das kostenlose Office 365 ProPlus für Schüler/Lehrer und Personal zur Verfügung stellen können, ist vorab eine Freischaltung Ihrer Office 365 Domäne bei Microsoft erforderlich.
Um Ihre Domäne freischalten zu lassen, tragen Sie diese im MS-ACH Downloadportal http://www2.acp.at/msachmak
ein.
Unsere Domänen haben wir so benannt: schulkürzel.onmicrosoft.com
Zum Beispiel: **bgbr.onmicrosoft.com**
Eine Freischaltung dauert mindestens 3 Wochen.



3 Aktivieren der kostenlosen OFFICE 365 PROPLUS LIZENZEN

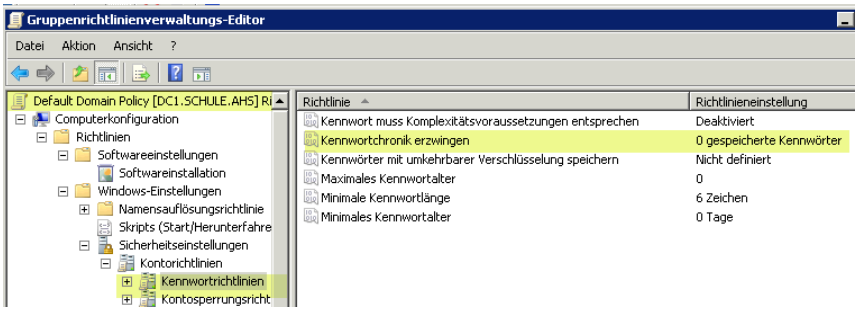
Nachdem Ihre Domäne von Microsoft freigeschaltet wurde, folgen Sie diesen Schritten, um den neuen Lizenzpool auf Ihrem Office 365 Tenant zu aktivieren.

3.1 Neuen Benutzer anlegen:

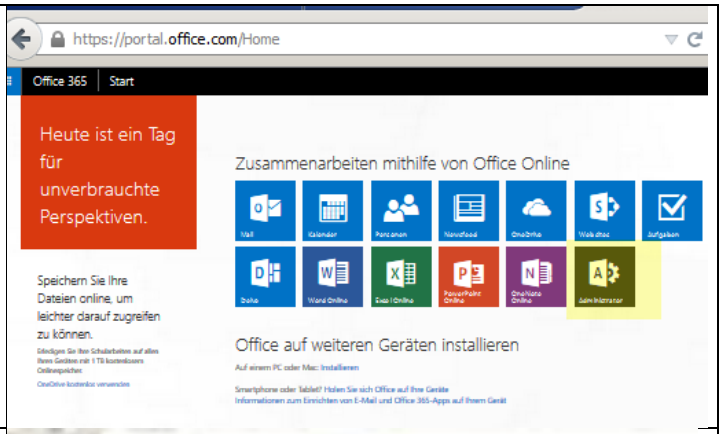
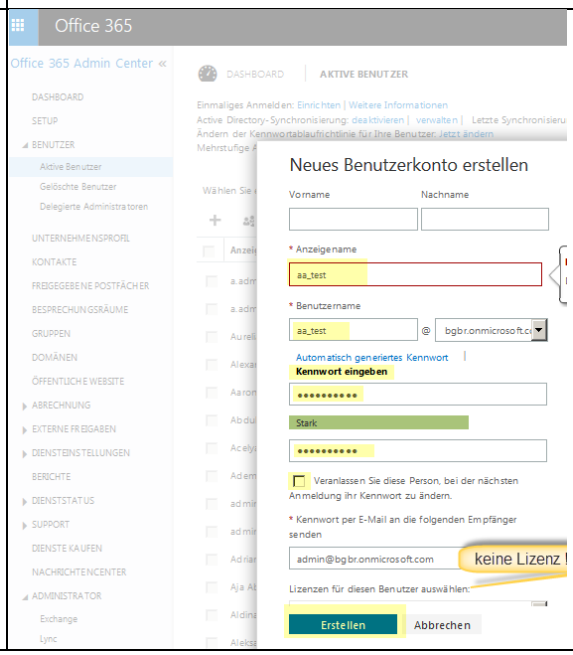
Sie brauchen einfach einen neuen Benutzer, der keine Office 365 Education Lizenz freigeschalten hat (außer eventuell E1 Lizenz). Das geht per Active Directory Synchronisation oder durch manuelles Anlegen eines Benutzers auf http://portal.office.com.

Wenn Sie Ihre Lehrer schon mit dem MS Azure Directory synchronisiert haben, müssen Sie keinen neuen Benutzer anlegen. Wie das geht ist im Kapitel
„Einrichten der Active Directory Synchronisation“
weiter unten beschrieben.

PROBLEM: Bei den Lehrern wurde an mehreren Schulen die Synchronisation der Passwörter erst nach einer ÄNDERUNG des PASSWORTES initialisiert.
SYNCHRONISIERTE Benutzer der OU LEHER MÜSSEN das PASSWORT ÄNDERN.
Das neue Passwort kann mit dem alten identisch sein, wenn in der Default Domain Policy die Kennwortchronik deaktiviert (auf 0 gesetzt) ist
Warten Sie einige Minuten, bis das Passwort aus Ihrer Domäne mit der Azure Domäne synchronisiert wurde.
TEST: Melden Sie sich mit dem Lehreraccount auf http://portal.office.com an.



Alternative: Manuelles Anlegen eines Benutzers auf http://portal.office.com.

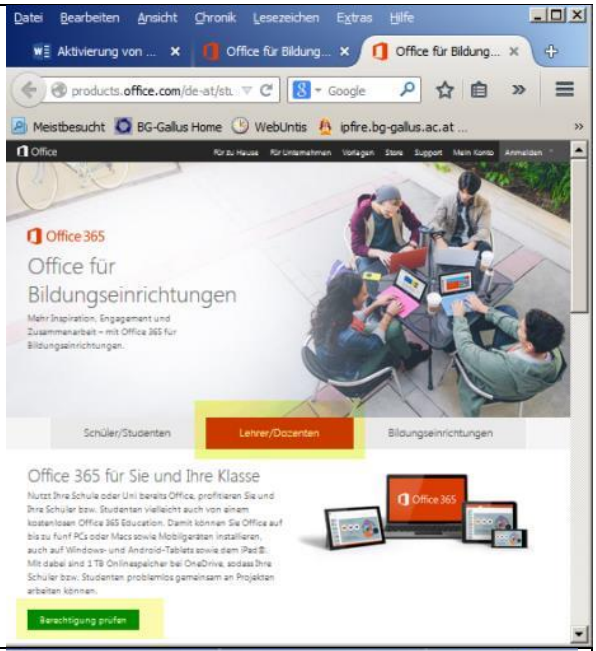
Legen Sie einen neuen Benutzer im Office 365 entsprechend den Schritten im Abschnitt an: https://portal.office.com – Anmelden als Admin. - Gehen Sie auf die Schaltfläche (APP) Administration.	
Legt einen neuen Benutzer an Achten Sie dabei darauf, dass dieser Benutzer keine Lizenz zugewiesen hat.	
Anzeigename: aa_test Benutzername: aa_test Kennwort eingeben Haken: keine Kennwortänderung Keine Lizenz zuweisen Erstellen	

3.2 Lizenzpool auf Ihrem Office 365 Tenant aktivieren

Öffnen Sie im Browser die URL
http://products.office.com/de-at/student/office-in-education

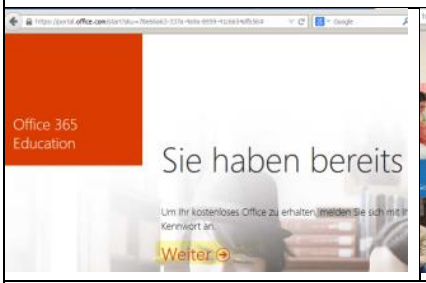
Öffnen Sie im Browser die URL

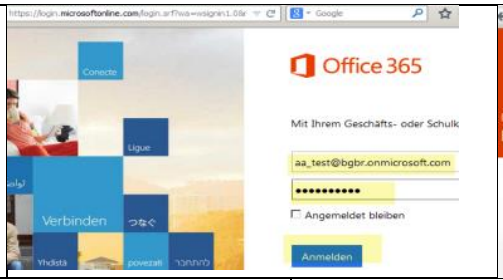
http://products.office.com/de-at/student/office-in-education



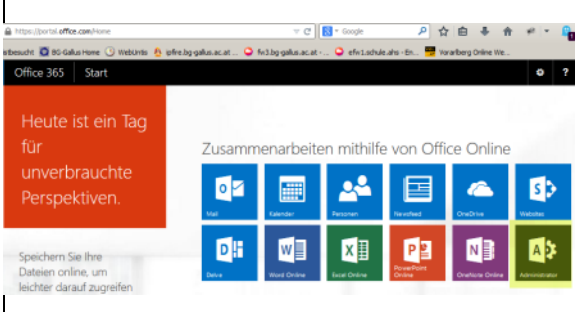
Wir melden uns mit einem unserer neuen Accounts an, denen noch keine Lizenzen zugewiesen wurden.

aa_test@bgbr.onmicrosoft.com



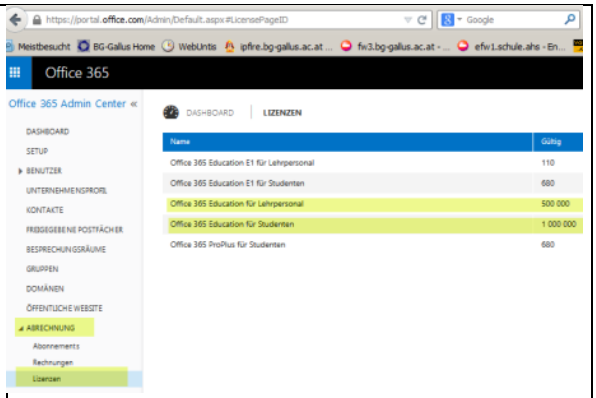


Sie erhalten eine Meldung, dass Sie es 15 Minuten später nochmals versuchen sollen. Dies ist nicht nötig, mit den bereits ausgeführten Schritten haben Sie die Zuweisung der kostenlosen Office 365 ProPlus Lizenzen bereits angestoßen.
Kehren Sie in das Office 365 Admin Center
http://portal.office.com
zurück.
Anmeldung als
admin@bgbr.onmicrosoft.com



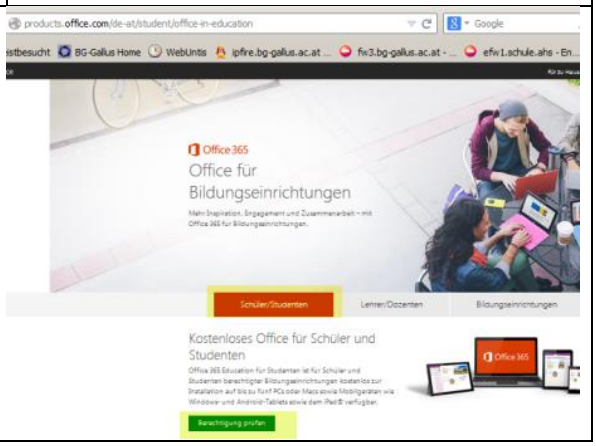
Wechseln Sie zu Abrechungen - Lizenzen

Sie sehen nun unter dem Punkt Abrechnung > Lizenzen die neuen Lizenzpools mit 500.000 Office 365 Education für Lehrpersonal und 1.000.000 Office 365 Education für Studenten.
Diese Lizenzen können Sie nun den Benutzern zuweisen, oder Sie geben an Ihre Benutzer ebenfalls den Link http://office.com/getoffice365 weiter, damit diese sich über das Self-Service Portal die Lizenzen selbst zuweisen.



Wiederholen Sie den Vorgang zur Aktivierung der Schülerlizenzen.

Öffnen Sie im Browser die URL
http://products.office.com/de-at/student/office-in-education
Schüler/Studenten –
Berechtigungen prüfen



3.3 Zuweisung der Lizenzen an Benutzer

Es gibt zwei Möglichkeiten:

- Die Benutzer können sich die Office 365 Lizenzen über das Self-Service Portal selbst zuweisen. Geben Sie Ihren Benutzern folgenden Link: http://office.com/getoffice365 weiter, damit diese sich die Lizenzen selbst zuweisen.

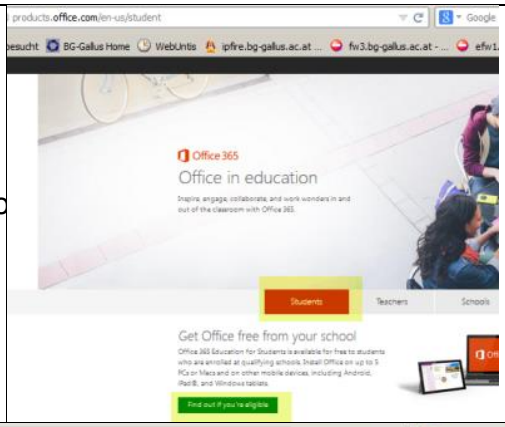
- Sie weisen Ihren Benutzern die Lizenzen per Powershell Script zu.
  Siehe dazu das Kapitel „Zuweisen von Lizenzen mittels Powershell“

Für Benutzer, welche bereits Office 365 ProPlus Lizenzen mittels des Lizenzkeys aus dem Schuljahr 14/15 zugewiesen haben, müssen Sie diese vorhergehende Lizenz durch die neuen Office 365 Education Lizenzen ersetzen. Das machen wir automatisiert per Powershell Skript. Siehe dazu das Kapitel „Zuweisen von Lizenzen mittels Powershell“

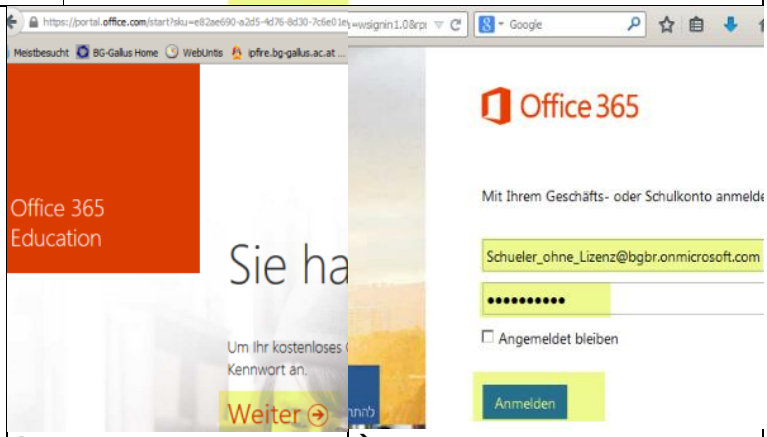
PROBLEM: An mehreren Schulen wurde bei den Lehrern die Synchronisation der Passwörter erst nach einer ÄNDERUNG des PASSWORTES initialisiert.
SYNCHRONISIERTE LEHERENDE MÜSSEN DAS PASSWORT ÄNDERN.
Das neue Passwort kann mit dem alten identisch sein, wenn in der Default Domain Policy die Passwortchronik deaktiviert (auf 0 gesetzt) ist
Warten Sie einige Minuten, bis das Passwort aus Ihrer Domäne mit der Azure Domäne synchronisiert wurde.

Geben Sie Ihren Benutzern folgenden Link: http://office.com/getoffice365 weiter, damit diese sich die Lizenzen selbst zuweisen.

Im Beispiel heißt der Schüler: Schueler_ohne_Lizenz@bgbr.onmicrosoft.com



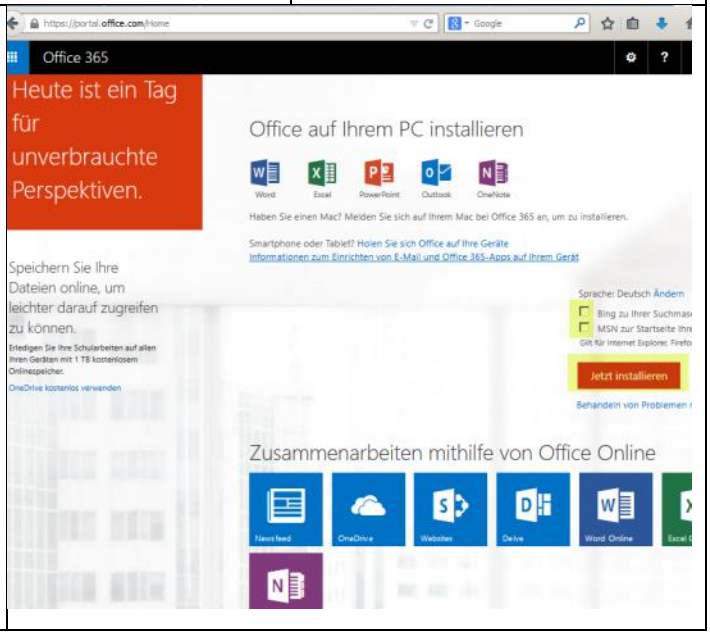
→



→

→

Im folgenden Schritt müssen Benutzer ein paar Minuten warten, bis alle Dienste eingerichtet sind.
Jetzt können Ihre Lehrenden / SchülerInnen Office 365 Pro Plus installieren.



4 Active Directory Synchronisation mit ADConnect

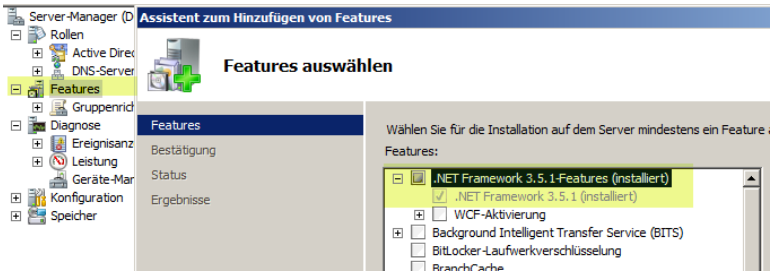
Wir installieren die ADConnect und Office365 Komponenten auf dem **SERVER** oder dem **SRVWSUS, jedoch nicht am Domänencontroller**.

4.1 Voraussetzungen

Windows Server 2016 GUI Version ONLY! (Core Server wird nicht unterstützt.)

- .NET Framework 4.5.1 and later releases are offered through Windows Update.
  https://www.microsoft.com/de-de/download/details.aspx?id=49982
- Make sure you have installed the latest updates to Windows Server in the Control Panel.
- Windows Azure Active Directory-Modul für Windows PowerShell
  Installationdetails mit Screenshots im folgenden Kapitel.
  In einer administrativen Powershell:
  `Install-Module -Name AzureAD`
  Nun kommen Sicherheitsabfragen, die Sie mit `Ja` beziehungsweise `Alle` bestätigen.
  `Install-Module MSOnline`
  Nun kommen Sicherheitsabfragen, die Sie mit `Ja` beziehungsweise `Alle` bestätigen.
- ADConnect Download:
  https://www.microsoft.com/en-us/download/details.aspx?id=47594
- Alternativer Benutzerprinzipalnamen Suffix im Active Directory

Das .NetFramework 3.5.1 muss über die Server Features installiert werden

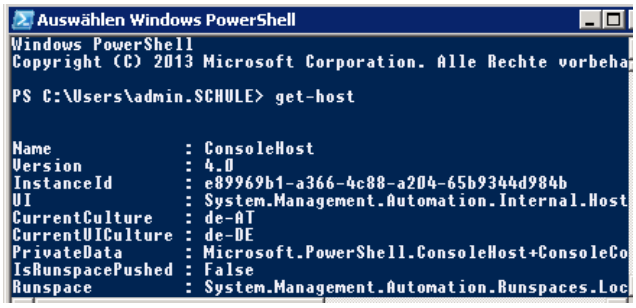


Powershell 4 oder höher Installieren:

Ihre aktuelle Version finden Sie über die Powershell mit dem Command:

get-host

liefert die Version

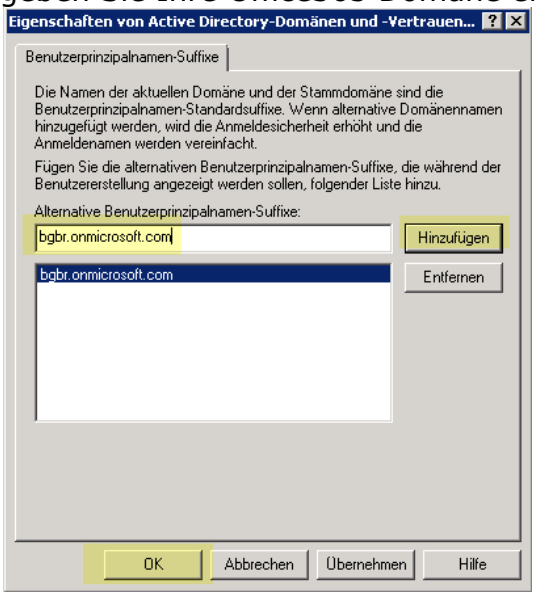


4.3 Hinzufügen eines alternativen Benutzerprinzipalnamens im Active Directory

Einen der wenigen Konfigurationsschritte führen wir am Domänencontroller (DC1) aus. Die Synchronisation des Active Directories mit dem AZURE Active Directory der Microsoft Cloud installieren und konfigurieren wir ausschließlich auf einem Memberserver.

Am Domänencontroller
Start → Verwaltung → Active Directory-Domänen und -Vertrauensstellungen

Als alternative Benutzerprinzipalen geben Sie Ihre Office365 Domäne ein.

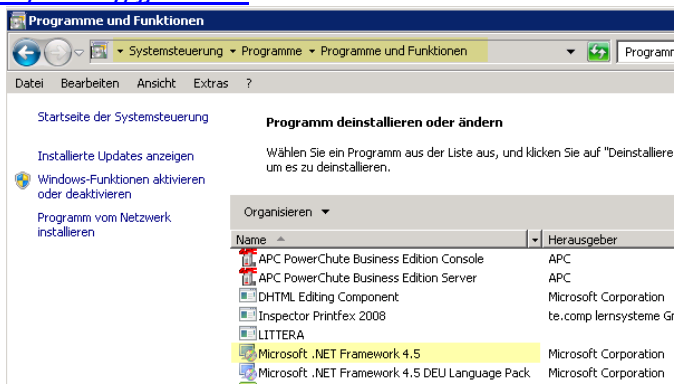


4.4 Vorbereiten der Verzeichnissynchronisierung

Verzeichnissynchronisation nicht am Domänencontroller sondern an einem standalone Server einrichten.

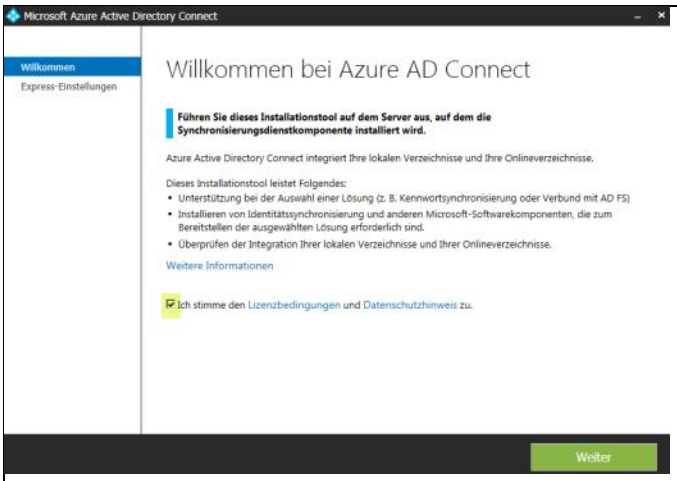
Die Gesamtstrukturfunktionsebene muss mindestens Windows Server 2003 sein. Im Beispielfall handelt es sich um eine Funktionsebene Windows 2008 R2.
Details auf http://technet.microsoft.com/de-de/library/jj151831

Installation der Software machen wir nicht auf dem Domänencontroller. Wählen Sie einen Member Server aus. Hier wähle ich den SRV2 auf dem auch mein WSUS Server, Printserver läuft. Beachten Sie, dass ein SQL Server installiert wird und der Rechner über ausreichend Ressourcen (RAM mindestens 4GB besser 8 GB) verfügt. Es ist möglich einen bereits bestehenden SQL Server als Datenbank für den Synchronisationsdienst zu verwenden. Systemsteuerung – Programme und Funktionen .NET Framework 4.5.1

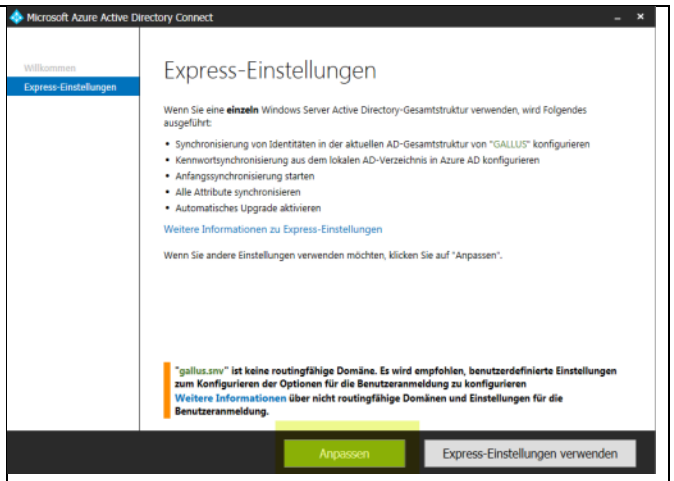


4.5 Installation und Konfiguration von AzureADConnect.msi

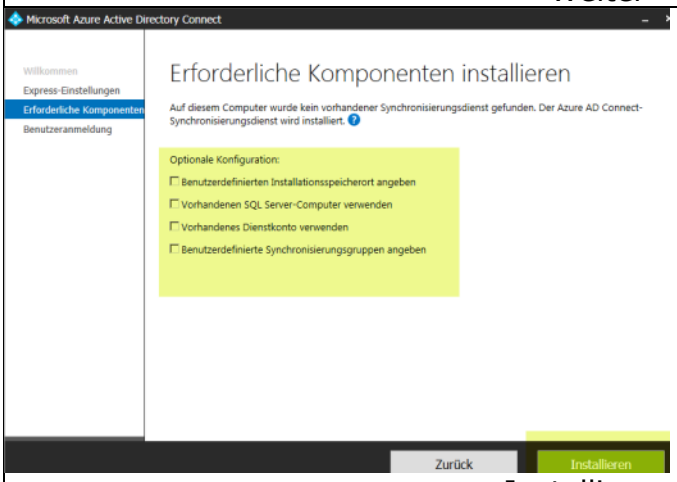
ADConnect Download:
https://www.microsoft.com/en-us/download/details.aspx?id=47594



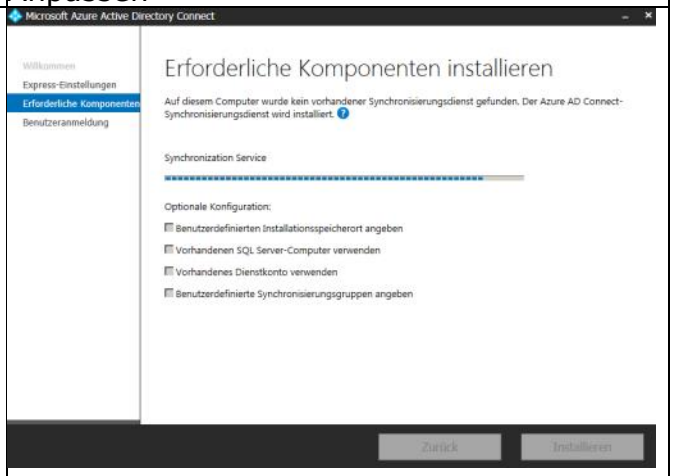
Weiter

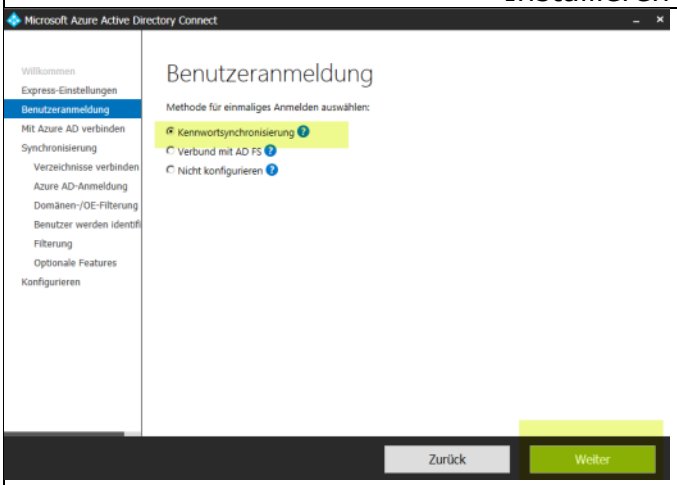


Anpassen

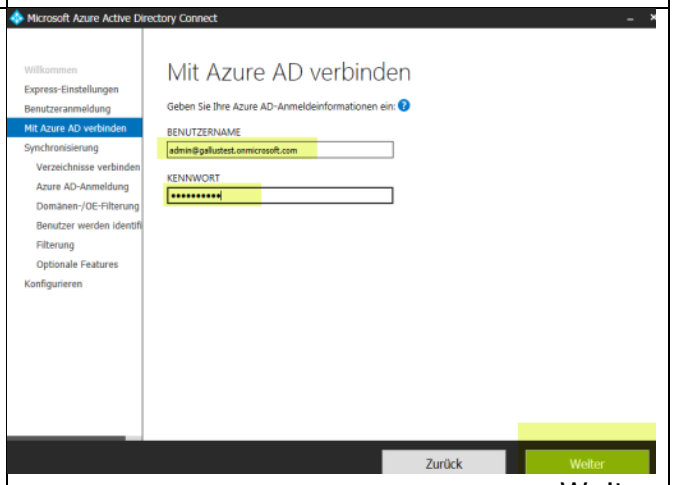


Installieren



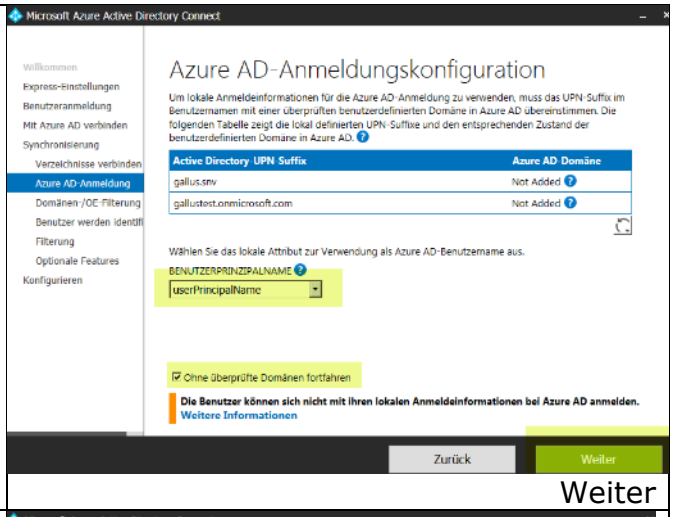


Weiter

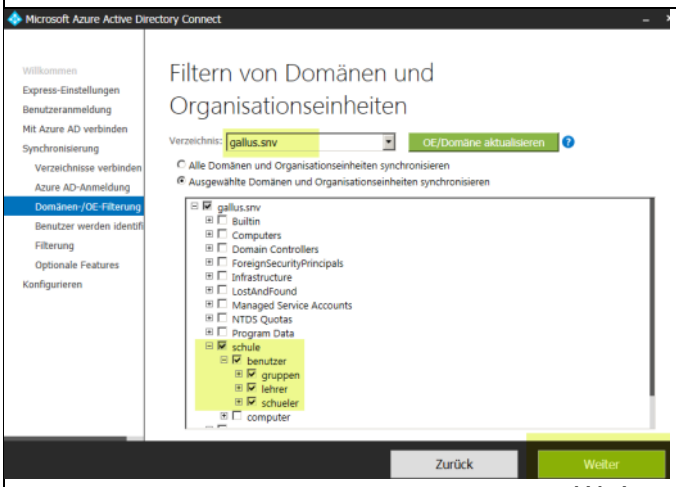


Weiter

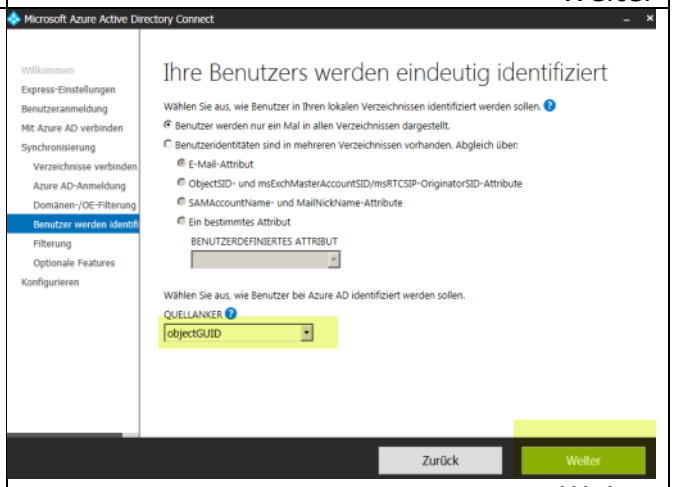
Weiter



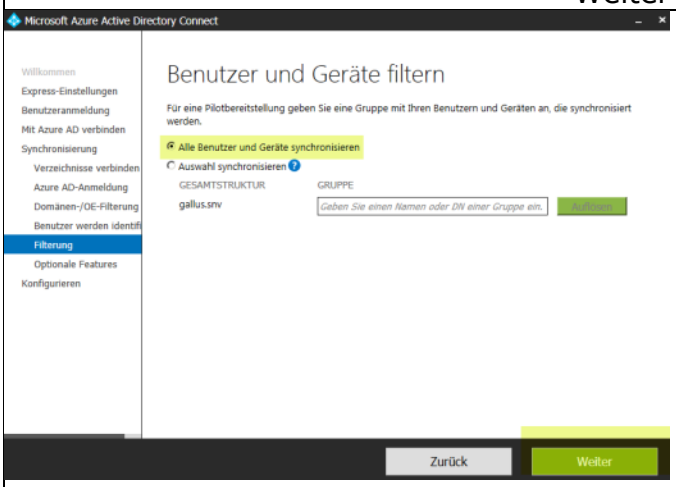
Weiter



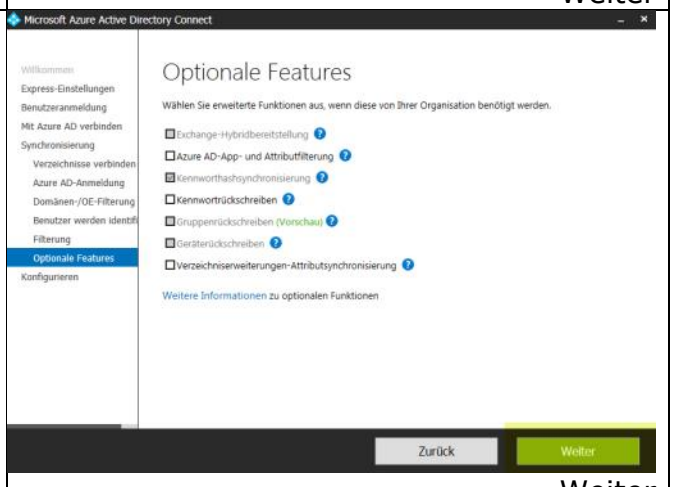
Weiter



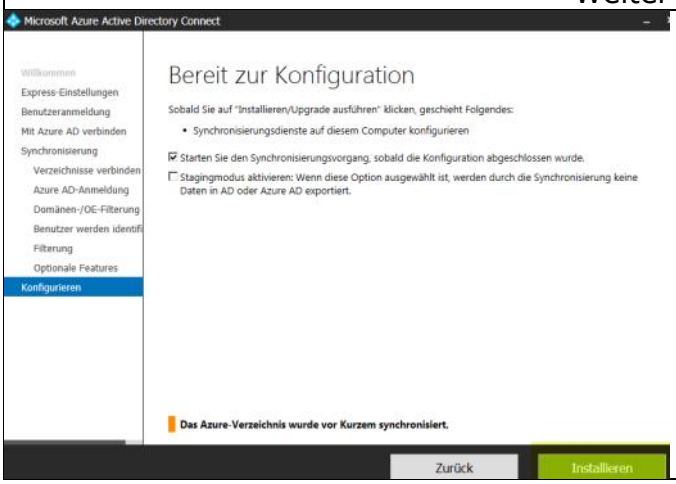
Weiter

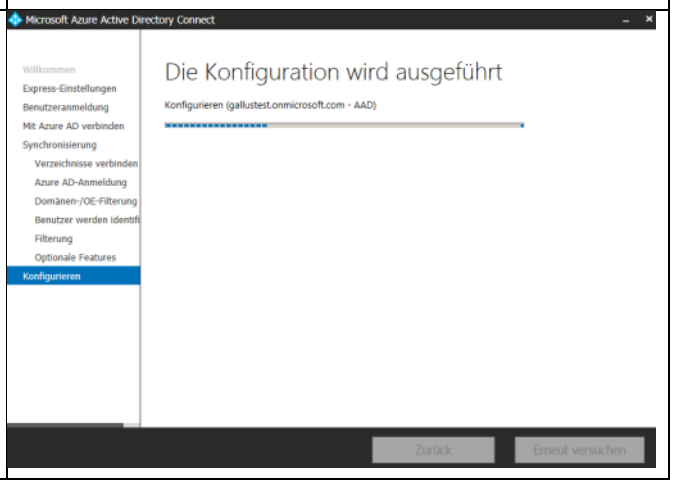


Weiter

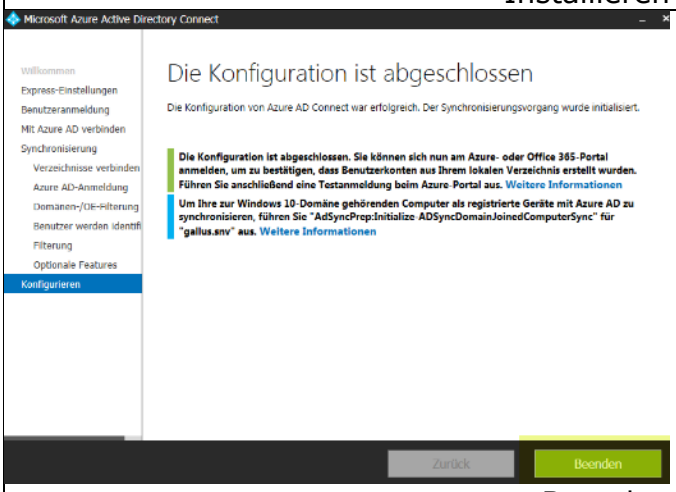


Weiter

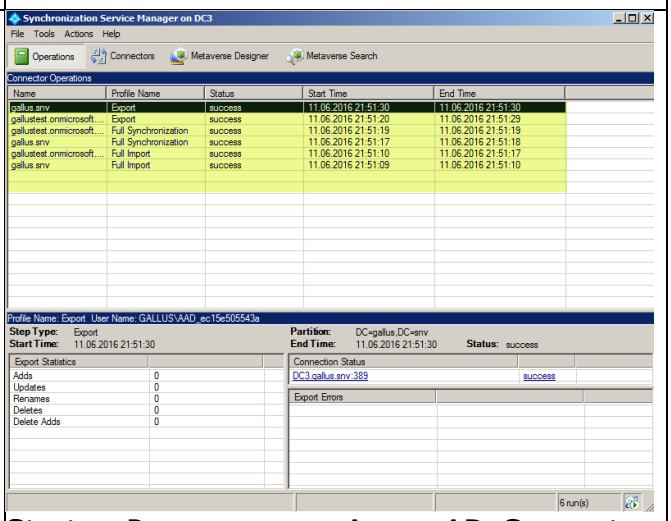




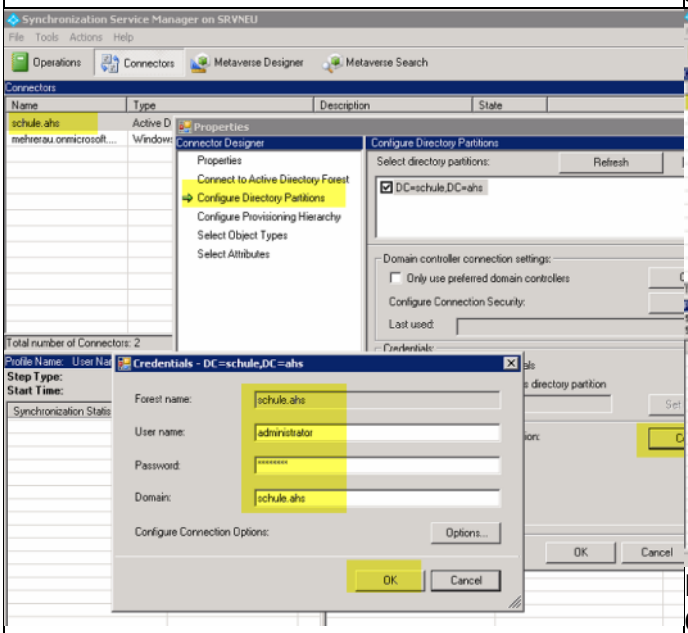
Installieren

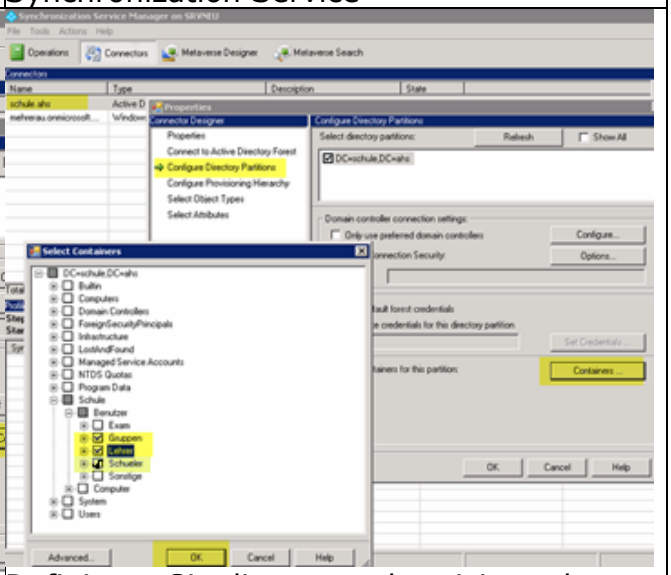


Beenden



Start – Programme – Azure AD Connect – Synchronization Service





Definieren Sie die zu synchronisierenden Organisationseinheiten und bestätigen Sie mit OK

GRUPPEN nicht vergessen!

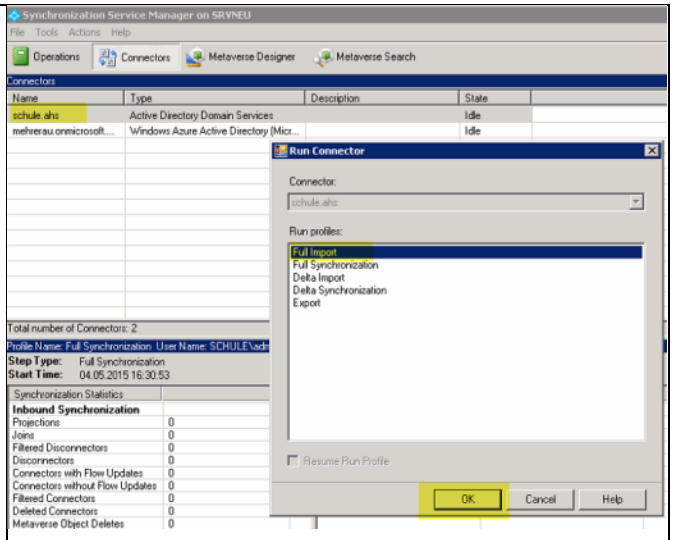
Vergessen Sie nicht Ihre OU mit Ihren Sicherheitsgruppen (grpSchueler, grpLehrer …)

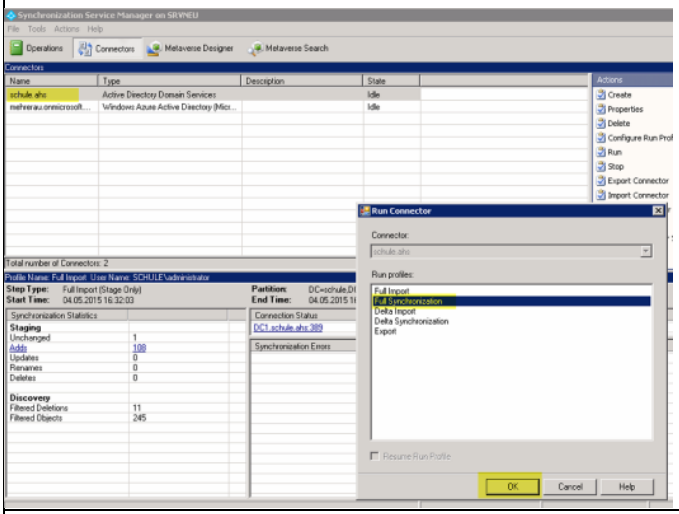
Active Directory Connector

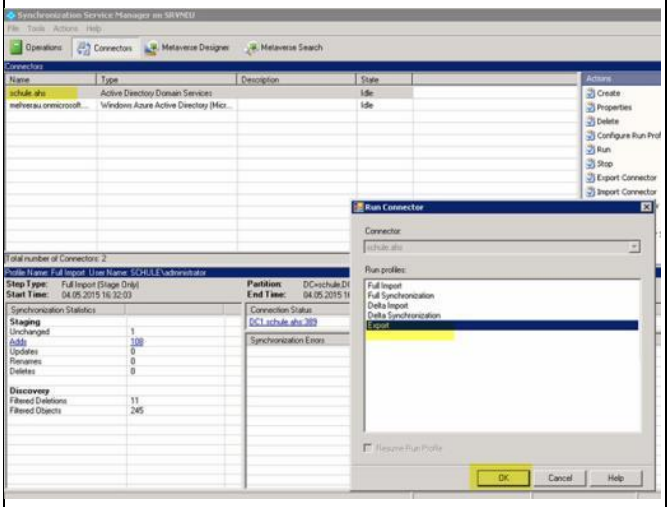
Run Profiles:

- Full Import
- Full Synchronization
- Export

Warten Sie bis die Vorgänge mit „success“ abgeschlossen sind.





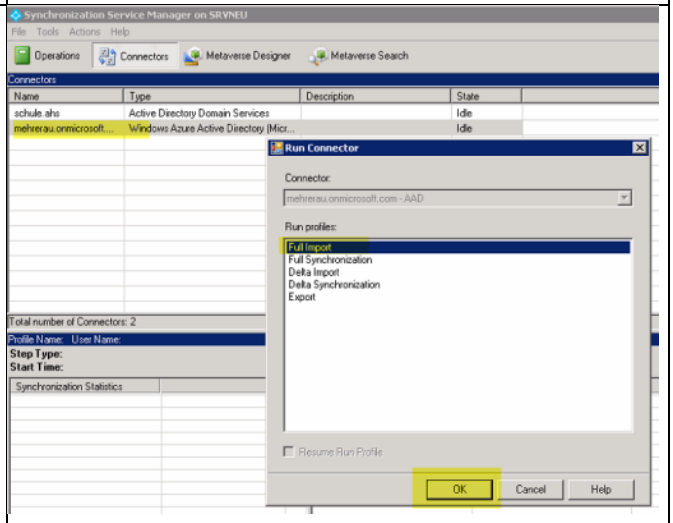


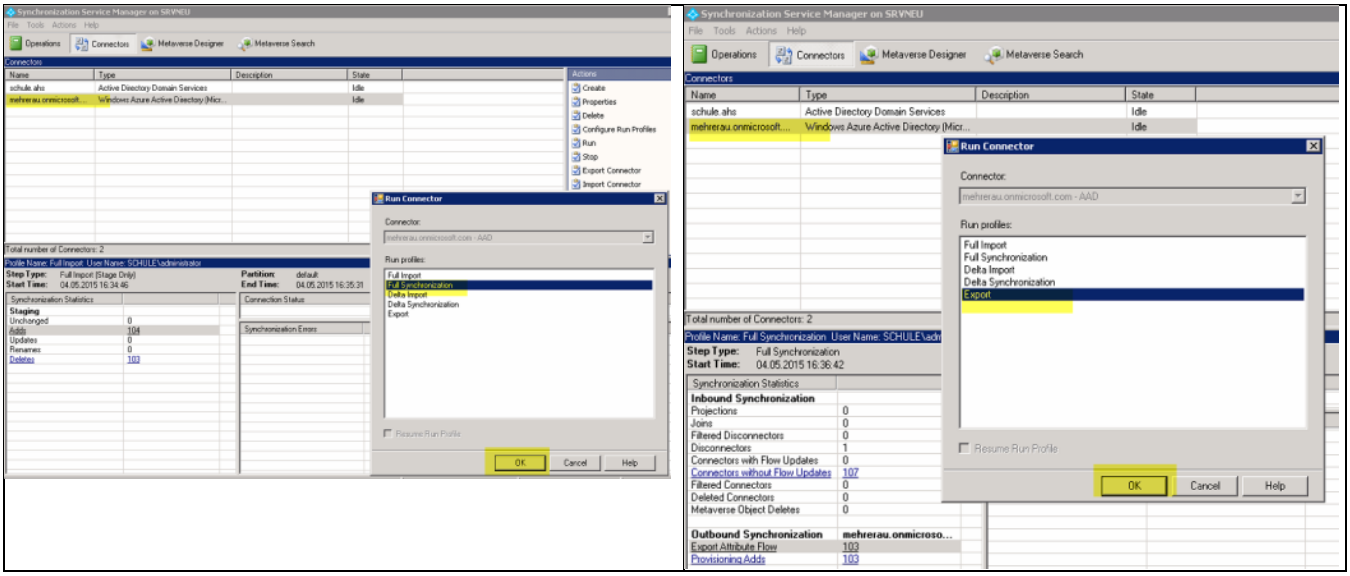
Azure Active Directory Connector

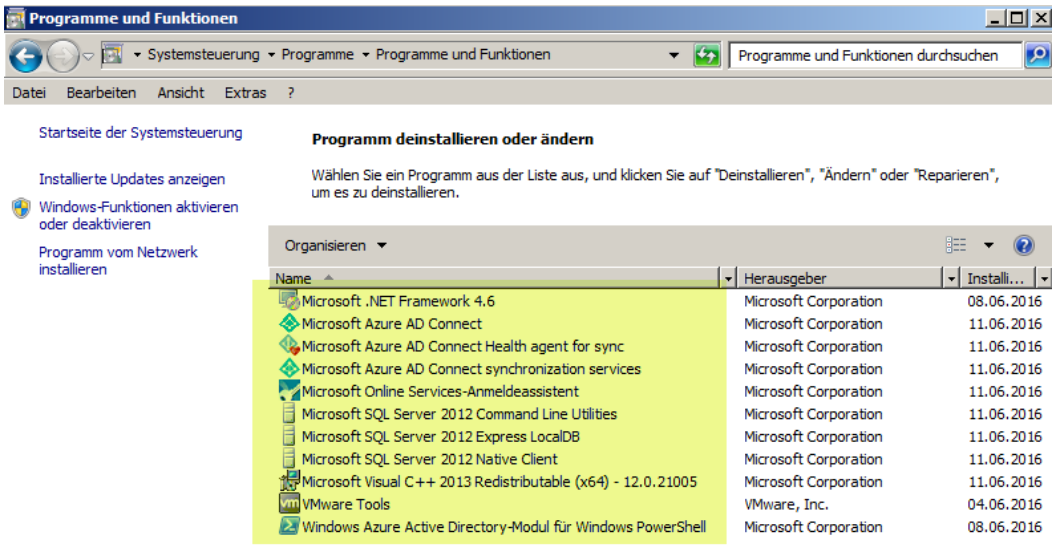
Run Profiles:

- Full Import
- Full Synchronization
- Export

Warten Sie bis die Vorgänge mit „success“ abgeschlossen sind.







Nach Abschluss der Installation finden wir unter Systemsteuerung Programme folgende Komponenten:

5 Zuweisen von Lizenzen mittels Powershell

5.1 Grundlagen

Wichtige PowerShell Tricks:

Kopieren von Code: Markieren und Rechtsklick
Einfügen von Code: Rechtsklick

Zwingende Anpassungen an Ihre Umgebung:

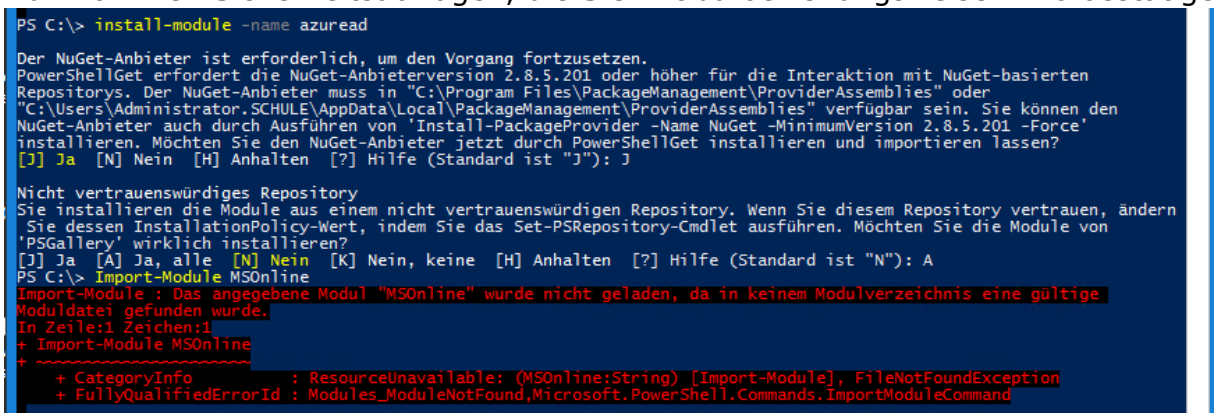
- Schulkürzel **bgbr** durch Ihr Schulkürzel ersetzen
- Gruppen **ID** für grpSchueler, grpLehrer durch **ihre IDs** ersetzen.

5.2 Installation der Software unter Windows Server 16

Wir installieren die ADConnect und Office365 Komponenten auf dem SERVER oder dem SRVWSUS.
In einer administrativen Powershell

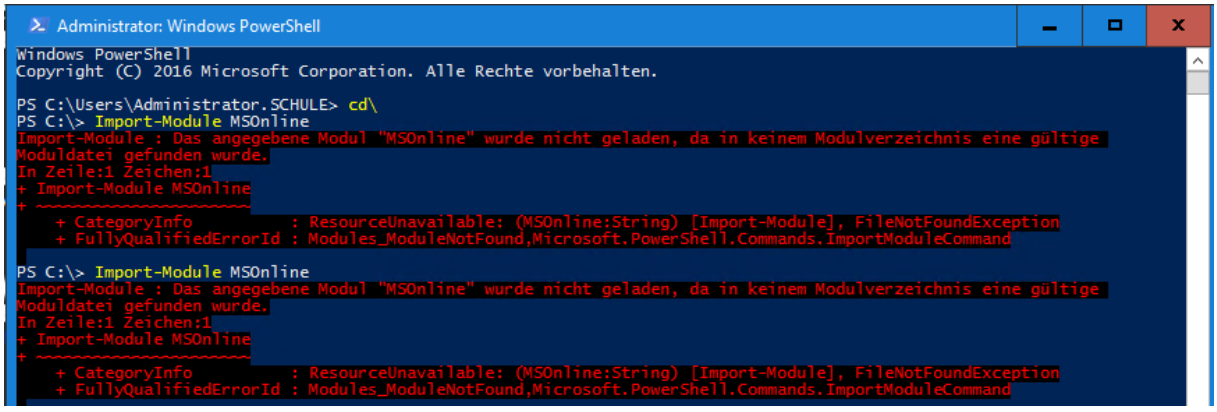
```
Install-Module -Name AzureAD
```

Nun kommen Sicherheitsabfragen, die Sie mit `Ja` beziehungsweise `Alle` bestätigen.




```
Install-Module MSOnline
```

Nun kommen Sicherheitsabfragen, die Sie mit `Ja` beziehungsweise `Alle` bestätigen.



5.3 Verbindung zum Office365 Tennant

Objekte, Eigenschaften und Methoden sind oft CASE sensitive.

Kontrollieren Sie die Version ihrer Powershell:

```
PS C:\> get-host
Name                  : ConsoleHost
Version               : 5.1
```

Importieren Sie die Windows Azure Commandlets mit

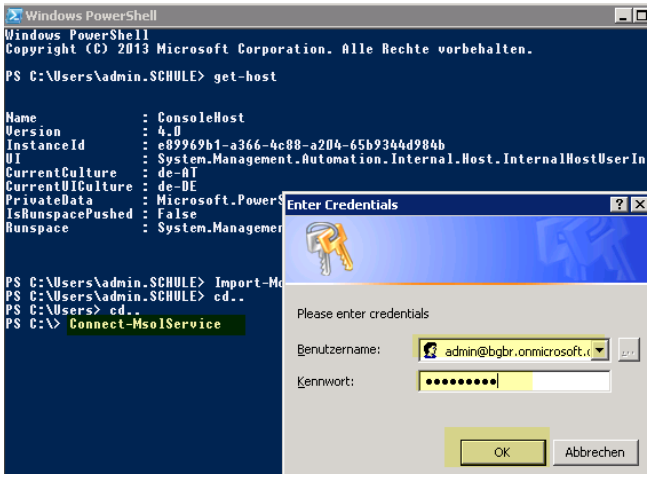
```
PS C:\>Import-Module MSOnline
PS C:\>
```

Die PowerShell ist hier nicht gesprächig.

So verbinden wir uns mit dem Office 365 Dienst.

```
PS C:\>Connect-MsolService
PS C:\>
```

Wir melden uns an mit dem Office365 Domäne Administrator: admin@bgbr.onmicrosoft.com
Get get



5.4 Powershell Befehle und Skripts für Office365 Verwaltungsaufgaben.

Allen Benutzern abfragen

```
PS C:\> Get-MsolUser -All
```

Allen Benutzern weisen wir den Verwendungsstandort AT zu

```
PS C:\> Get-MsolUser -All | Set-MsolUser -UsageLocation AT
```

Das können wir so kontrollieren (alles in einer Zeile eingeben!). Alle unsere AT User werden in eine CSV Datei geschrieben.

```
PS C:\> Get-MsolUser -all | where-object {$_.usagelocation -like
"AT"} | select displayname, usagelocation | Export-Csv
c:\temp\VerwendungsstandortAT.csv
```

Allen Benutzern ohne den Verwendungsstandort AT finden wir so

```
PS C:\> Get-MsolUser -all | where-object {$_.usagelocation -
notlike "AT"} | select displayname, usagelocation | Export-Csv
c:\temp\VerwendungsstandortNotAT.csv
```

Abrufen der angelegten Gruppen

```
PS C:\> Get-MsolGroup
ObjectId                             DisplayName                    GroupType
fe3cfc52-914f-4f6d-95e9-eeca2b171519   Office
cdf5327f-4f92-4d7f-a430-0e217ab2c22b   grpLehrer          Security
a5defc47-6909-4c04-89a1-01597295bc3b   grpBibliothek      Security
39eec1a4-4a49-4db7-9039-568a03913568   grpSchueler        Security
05687601-3690-4d83-8dec-b3972007099d   grp1a              Security
```

Verfügbare Lizenzen abfragen:

```
PS C:\> Get-MsolAccountSku
Office 365 Lizenzpläne anzeigen:
AccountSkuId                          ActiveUnits    WarningUnits    ConsumedUnits
bgbr:OFFICESUBSCRIPTION_STUDENT          680             0               650
bgbr:STANDARDWOFFPACK_FACULTY            110             0               1
bgbr:STANDARDWOFFPACK_IW_FACULTY      500000             0               89
bgbr:STANDARDWOFFPACK_STUDENT            680             0               649
bgbr:STANDARDWOFFPACK_IW_STUDENT     1000000             0               3
```

Allen SchülerInnen (grpSchueler), die noch das alte OFFICESUBSCRIPTION_STUDENT von 2014 haben, OFFICESUBSCRIPTION_STUDENT entfernen."

```
PS C:\>Get-MsolGroupMember -all -GroupObjectID 39eec1a4-4a49-4db7-9039-
568a03913568 | get-MsolUser | where {$_.Licenses.AccountSkuId -contains
"bgbr:OFFICESUBSCRIPTION_STUDENT"} | Set-MsolUserLicense -RemoveLicenses
"bgbr:OFFICESUBSCRIPTION_STUDENT"
```

Allen SchülerInnen (grpSchueler), die noch das alte STANDARDWOFFPACK_STUDENT von 2014 haben, STANDARDWOFFPACK_STUDENT entfernen."

```
PS C:\>Get-MsolGroupMember -all -GroupObjectID 39eec1a4-4a49-4db7-9039-
568a03913568 | get-MsolUser | where {$_.Licenses.AccountSkuId -contains
"bgbr:STANDARDWOFFPACK_STUDENT"} | Set-MsolUserLicense -RemoveLicenses
"bgbr:STANDARDWOFFPACK_STUDENT"
```

Allen SchülerInnen (grpSchueler), die das STANDARDWOFFPACK_IW_STUDENT (OFFICESUBSCRIPTION) nicht haben, STANDARDWOFFPACK_IW_STUDENT (OFFICESUBSCRIPTION) zuweisen."

```
PS C:\>Get-MsolGroupMember -all -GroupObjectID 39eec1a4-4a49-4db7-9039-
568a03913568 | get-MsolUser | where {$_.Licenses.AccountSkuId -notcontains
"bgbr:STANDARDWOFFPACK_IW_STUDENT"} | Set-MsolUserLicense -AddLicenses
"bgbr:STANDARDWOFFPACK_IW_STUDENT"
```

5.5 NEUZUWEISUNG VON LIZENZEN MITTELS POWERSHELL

(von Thomas Hauser)
Aufbauend auf der PowerShell Verbindung die im vorhergehenden Schritt hergestellt wurde, können auch auf einfache Weise bestehende Lizenzen ersetzt werden.

Im folgenden Beispiel werden alle Benutzer welche die Office 365 Education und Office 365 ProPlus Lizenz zugewiesen haben auf die neue Office 365 Education Plus Lizenz umgestellt. Dies wird z.B. benötigt, um von der ehemaligen ProPlus Lizenz mittels Produktschlüssel auf die neue Lizenz umzustellen.

Der folgende Befehl wird in einer Zeile geschrieben; ersetzen Sie `PREFIX` mit Ihrem Domain Prefix (zB: `bgbr`).

```
GET-MSOLUSER –ALL | WHERE {$_.LICENSES.ACCOUNTSKUID –CONTAINS
“PREFIX:STANDARDWOFFPACK_STUDENT” –AND $_.LICENSES.ACCOUNTSKUID –CONTAINS
“PREFIX:OFFICESUBSCRIPTION_STUDENT”} | SET-MSOLUSERLICENSE –REMOVELICENSES
“PREFIX:STANDARDWOFFPACK_STUDENT”,“PREFIX:OFFICESUBSCRIPTION_STUDENT” –
ADDLICENSES “PREFIX:STANDARDWOFFPACK_IW_STUDENT”
```

Da der Befehl in einem Schritt die Lizenzen entfernt und die neue Lizenz zuweist, kann bei eventuellen Fehlern kein Lizenzfreier Zustand eines Benutzers entstehen.

5.6 Office 365 User aus dem Papierkorb löschen oder wiederherstellen

Zunächst einmal alle Benutzer aus dem Directory anzeigen lassen. Tipp: die Ausgabe der ObjectID hilft dann, wenn Sie nur einen User löschen wollen:

```
PS C:\>Import-Module MSOnline
PS C:\>Connect-MsolService

PS C:\>Get-MsolUser -ReturnDeletedUsers | fl UserPrincipalName, ObjectID
```

Um den gesamten Papierkorb zu leeren, verwenden Sie folgenden Befehl

```
PS C:\>Get-MsolUser –ReturnDeletedUsers | Remove-MsolUser -RemoveFromRecycleBin
–Force
```

Der Parameter –Force gibt dabei an, dass nicht jedes Mal eine zusätzliche Sicherheitsabfrage kommt. Dieser Einzeiler kann schon eine ganze Weile laufen, wenn viele User zu löschen sind.

Sollten Sie nur einen Benutzer aus dem Directory löschen wollen, verwenden Sie folgenden Befehl, um zunächst die Object-ID des Users zu erhalten:

```
PS C:\>Get-MsolUser –ReturnDeletedUsers –searchstring user1@contoso.com | fl
UserPrincipalName, ObjectID
```

Danach mit Eingabe der Guid löschen:

```
PS C:\>Remove-MsolUser  -ObjectID <GUID> -RemoveFromRecycleBin –Force
```

5.7 User aus dem Windows Azure Active Directory wieder herstellen

Um einen Benutzer, der im Papierkorb liegt, wieder herzustellen verwenden Sie:

```
PS C:\>Import-Module MSOnline
PS C:\>Connect-MsolService

PS C:\>Restore-MsolUser –UserPrincipalName <UserUPN> -
AutoReconcileProxyConflicts -NewUserPrincipalName <UserUPN>
```

5.8 Weitere hilfreiche Befehle:

Abrufen Mitglieder der Gruppe grpSchueler

```
PS C:\> Get-MsolGroupMember -GroupObjectID 39eec1a4-4a49-4db7-9039-
568a03913568 -all | select displayname | Export-Csv
c:\temp\grpSchueler.csv
```

Einem Benutzer eine bestimmte Lizenz weg nehmen:

```
PS C:\> Set-MsolUserLicense -UserPrincipalName
clarissa.renner@bgbr.onmicrosoft.com -RemoveLicenses
"bgbr:OFFICESUBSCRIPTION_STUDENT"
```

Alle Benutzer der Sicherheitsgruppe grpSchueler mit ihren diversen Attributen in eine csv Datei schreiben.

```
PS C:\>

Get-MsolGroupMember -GroupObjectID 39eec1a4-4a49-4db7-9039-568a03913568 -all |
select DisplayName, EmailAddress, GroupMemberType, IsLicensed,
LastDirSyncTime, OverallProvisioningStatus, ValidationStatus | Export-Csv
$scriptpath\grpSchueler.csv
```

Mehr nützliche Anweisungen finden Sie in der Datei **office365_sync.ps1**

5.9 Automatisierung der Lizenzzuweisung

Einige der Befehle oben fassen wir in einem Powershellscript zusammen, das man später per Aufgabenplanung automatisch ablaufen lassen kann. Damit das automatisch funktioniert, müssen die Zugangsdaten admin@bgbr.onmicrosoft.com und das Passwort verschlüsselt abgespeichert werden. Bitte vergessen Sie nicht, dass diese Entschlüsselung nur unter dem Account funktioniert, der die Verschlüsselung angestoßen hat. Wollen Sie später das Script automatisiert per Aufgabenplanung ablaufen lassen, müssen Sie den Task unter dem Account des „Verschlüsslers" laufen lassen.

In der Powersershell:

```
Get-Credential | Export-Clixml .\Desktop\credentials.xml
```

So werden die credentials.xml im Desktop gespeichert. Wir kopieren sie in unseren `scriptpath`

Diese Verschlüsselten Daten können nur als der Benutzer entschlüsselt werden, der sie angelegt hat. Das Skript unten muss daher unter diesem Benutzer laufen. Es sollte ein lokaler Benutzer (Administrator) sein, der sich am Server lokal anmelden darf.

ToDos:

- Kopieren Sie den Code unten in eine Textdatei namens
- **`office365_sync.ps1`**
- Alle Befehle müssen in einer Zeile stehen!
- Fetter, roter Code muss mit Ihren Daten ersetzt werden.
- Zum Testen stoppt das Script mit Hilfe einer Eingabeaufforderung.
- Soll das Script als Task unbeaufsichtigt laufen, kommentieren Sie die entsprechende Zeile aus.
- Das Powershell Script, office365_sync.ps1, rufen wir über den Batch office365_sync.cmd auf, die beide im gleichen Verzeichnis stehen. Das macht man mit der Anweisung:

office365_sync.ps1 beginnt hier

```
Write "."
Write "-------------------------------------------------------------------------------"
Write "Powershell Skriptsammlung fuer die Verwaltung von Office 365 fuer Schulen"
Write "Andreas Renner 24 April 2015"
Write "."
Write "Passen Sie den Schulkuerzel an Ihre Azure Domain an! Suchen Sie nach dem Wort schulkürzel!"
Write "Passen Sie die GruppenIDs an! Suchen Sie nach dem Wort MeineGruppenID!"
Write "Eventuell passen Sie die Lizenzpläne an, falls notwendig"
Write "Wir stoppen das Script durch eine Eingabeaufforderung."
Write "."
Write "-------------------------------------------------------------------------------"
Write "."

# Soll das Script als Task unbeaufsichtigt laufen, kommentieren Sie die nächste Zeile aus.
$userinput = Read-Host "Enter input here and press Enter Key:"



# Pfad es Skripts ermitteln
$scriptpath = split-path -parent $MyInvocation.MyCommand.Definition

# Bei Bedarf wird dem Pfad ein \ angefügt
# $sub= $scriptpath.substring($scriptpath.length - 1, 1)
# if($sub -NotMatch "\\") {$scriptpath=$scriptpath + "\"}
# write $scriptpath

Import-Module MSOnline
# Powershell zuerst auf Version 4 upgraden
# zuvor muss die credentials.xml mit den verschlüsselten credentials muss erzeugt werden
# in der powsershell:
# Get-Credential | Export-Clixml .\Desktop\credentials.xml
# So werden die credentials.xml im Desktop gespeichert. Wir kopieren sie in unseren scriptpath
# Diese Verschlüsselten Daten können nur als der Benutzer entschluesselt werden, der sie angelegt
hat
# Das Skript unten muss daher unter diesem Benutzer laufen. Es sollte ein lokaler Benutzer sein,
der sich am Server anmelden darf

# ------------------- VERBINDEN MIT MSOLSERVICE ----------------------------------------------
Write "Verbinden mit MsolService"
$cred = Import-Clixml $scriptpath\credentials.xml
Connect-MsolService -Credential $cred
Write "Die Verbindung mit MsolService scheint OK zu sein."
Write "."
Write "."
# ------------------- ENDE VERBINDEN MIT MSOLSERVICE ----------------------------------------
-


# ------------------- VORHANDENE LIZENZPLÄNE -------------------------------------------------
Write "Office 365 Lizenzpläne anzeigen:"
Get-MsolAccountSku
# ------------------- ENDE VORHANDENE LIZENZPLÄNE -------------------------------------------

# ------------------- Detaillierte Lizenzen zu einem Lizenzplan anzeigen ---------------------
-
# Write "Details zum Lizenzplan STANDARDWOFFPACK_IW_FACULTY anzeigen"
# $plans = Get-MsolAccountSku | Where {$_.SkuPartNumber -eq "STANDARDWOFFPACK_IW_FACULTY"}
# $plans.servicestatus
# --- YAMMER_EDU: Yammer is used for private communication within organizations, an enterprise
social software.
# --- OFFICESUBSCRIPTION: Office 365 Pro Plus - die Office Suite, die wir eigentlich wollen
# --- SHAREPOINTWAC_EDU: (This is for the 365 web apps, not Sharepoint)
# --- SHAREPOINTSTANDARD_EDU (Office 365 Sharepoint)
# --- EXCHANGE_S_STANDARD (Exchange)
# --- MCOSTANDARD (Office 365 Lync)
# ------------------- ENDE Detaillierte Lizenzen zu einem Lizenzplan anzeigen ----------------
------



# ------------------- VORHANDENE BENUTZERGRUPPEN ---------------------------------------------
Write "Abrufen der vorhandenen Gruppen"
Get-MsolGroup | format-table
# ------------------- ENDE VORHANDENE BENUTZERGRUPPEN -----------------------------------------
--
```

```
# ------------------- ALLEN BENUTZERN VERWENDUNSSTANDORT AT ZUWEISEN-----------------------------
---------------
Write "Allen Benutzern ohne Verwendungsstandort AT weisen wir den Verwendungsstandort AT zu"
Write "... haben Sie Geduld ..."
Write "."
Get-MsolUser -all | where-object {$_.usagelocation -notlike "AT"} | Set-MsolUser -UsageLocation AT
# ------------------- ENDE ALLEN BENUTZERN VERWENDUNSSTANDORT AT ZUWEISEN-------------------------
---------------------


# ------------------- STOP: GRUPPEN UND LIZENZPLÄNE ANPASSEN -----------------------------------
---------
# Passen Sie unten die GruppenIDs und Lizenzpläne an.
# Wir stoppen das Script durch eine Eingabeaufforderung.
# Soll das Script als Task unbeaufsichtigt laufen, kommentieren Sie die nächste Zeile aus.
# $userinput = Read-Host "Enter input here and press Enter Key:"
# Write-Host $userinput
# Write-Host "Press any key to continue ..."
# $x = $host.UI.RawUI.ReadKey("NoEcho,IncludeKeyDown")
# Write-Host $x.Character
# ------------------- ENDE: GRUPPEN UND LIZENZPLÄNE ANPASSEN -----------------------------------
---------


# ------------------- ALLEN SCHUELERN DEN ALTEN OFFICESUBSCRIPTION_STUDENT (Office 365 Pro Plus)
ENTFERNEN-----------------------------------------------
# Write "Allen SchülerInnen (grpSchueler), die noch das alte OFFICESUBSCRIPTION_STUDENT von 2014
haben, OFFICESUBSCRIPTION_STUDENT entfernen."
# Write "... haben Sie Geduld ..."
# Write "."
# Get-MsolGroupMember -all -GroupObjectID MeineGruppenID | get-MsolUser | where
{$_.Licenses.AccountSkuId -contains "schulkürzel:OFFICESUBSCRIPTION_STUDENT"} | Set-
MsolUserLicense -RemoveLicenses "schulkürzel:OFFICESUBSCRIPTION_STUDENT"
# ------------------- ENDE ALLEN SCHUELERN DEN ALTEN OFFICESUBSCRIPTION_STUDENT ENTFERNEN --------
---------------------------------------


# ------------------- ALLEN SCHUELERN DEN ALTEN STANDARDWOFFPACK_STUDENT (Office 365 Education E1
für Studenten) ENTFERNEN-------------------------------------------
# Write "Allen SchülerInnen (grpSchueler), die noch das alte STANDARDWOFFPACK_STUDENT von 2014
haben, STANDARDWOFFPACK_STUDENT entfernen."
# Write "... haben Sie Geduld ..."
# Write "."
# Get-MsolGroupMember -all -GroupObjectID MeineGruppenID | get-MsolUser | where
{$_.Licenses.AccountSkuId -contains "schulkürzel:STANDARDWOFFPACK_STUDENT"} | Set-MsolUserLicense
-RemoveLicenses "schulkürzel:STANDARDWOFFPACK_STUDENT"
# ------------------- ENDE ALLEN SCHUELERN DEN ALTEN STANDARDWOFFPACK_STUDENT (Office 365
Education E1 für Studenten) ENTFERNEN -------------------------------------------


# ------------------- ALLEN SCHUELERN DEN STANDARDWOFFPACK_IW_STUDENT (OFFICESUBSCRIPTION ETC)
ZUWEISEN -----------------------------------------------
# Write "Allen SchülerInnen (grpSchueler), die das STANDARDWOFFPACK_IW_STUDENT
(OFFICESUBSCRIPTION) nicht haben, STANDARDWOFFPACK_IW_STUDENT (OFFICESUBSCRIPTION) zuweisen."
# Write "... haben Sie Geduld ..."
# Write "."
# Get-MsolGroupMember -all -GroupObjectID MeineGruppenID | get-MsolUser | where
{$_.Licenses.AccountSkuId -notcontains "schulkürzel:STANDARDWOFFPACK_IW_STUDENT"} | Set-
MsolUserLicense -AddLicenses "schulkürzel:STANDARDWOFFPACK_IW_STUDENT"
# ------------------- ENDE ALLEN SCHUELERN DEN STANDARDWOFFPACK_IW_STUDENT (OFFICESUBSCRIPTION
ETC) ZUWEISEN -------------------------------------------


# ------------------- ALLEN LEHRENDEN DEN STANDARDWOFFPACK_IW_FACULTY (OFFICESUBSCRIPTION ETC)
ZUWEISEN -----------------------------------------------
 Write "Allen Lehrenden (grpLehrer), die das STANDARDWOFFPACK_IW_FACULTY (OFFICESUBSCRIPTION ETC)
nicht haben, STANDARDWOFFPACK_IW_FACULTY (OFFICESUBSCRIPTION) zuweisen."
 Write "... haben Sie Geduld ..."
 Write "."
 Get-MsolGroupMember -all -GroupObjectID MeineGruppenID | get-MsolUser | where
{$_.Licenses.AccountSkuId -notcontains "schulkürzel:STANDARDWOFFPACK_IW_FACULTY"} | Set-
MsolUserLicense -AddLicenses "schulkürzel:STANDARDWOFFPACK_IW_FACULTY"
# ------------------- ENDE ALLEN SCHUELERN DEN STANDARDWOFFPACK_IW_STUDENT (OFFICESUBSCRIPTION
ETC) ZUWEISEN -------------------------------------------


# ------------------- ALLEN LEHRENDEN NUR DIE OFFICESUBSCRIPTION AUS STANDARDWOFFPACK_IW_FACULTY
ZUWEISEN -----------------------------------------------
```

```
# Write "Allen Lehrenden (grpLehrer), die das STANDARDWOFFPACK_IW_FACULTY (OFFICESUBSCRIPTION)
nicht haben, NUR DIE OFFICESUBSCRIPTION AUS STANDARDWOFFPACK_IW_FACULTY zuweisen."
# Write "... haben Sie Geduld ..."
# Write "."
# $O365_TEACHER_LICENSES = NEW-MSOLLICENSEOPTIONS –ACCOUNTSKUID
"schulkürzel:STANDARDWOFFPACK_FACULTY" –DISABLEDPLANS
YAMMER_EDU,SHAREPOINTWAC_EDU,SHAREPOINTSTANDARD_EDU,EXCHANGE_S_STANDARD,MCOSTANDARD
# Get-MsolGroupMember -all -GroupObjectID MeineGruppenID | get-MsolUser | where
{$_.Licenses.AccountSkuId -notcontains "schulkürzel:STANDARDWOFFPACK_FACULTY"} | Set-
MsolUserLicense –LICENSEOPTIONS $O365_TEACHER_LICENSES
# ------------------- ENDE ALLEN LEHRENDEN NUR DIE OFFICESUBSCRIPTION AUS
STANDARDWOFFPACK_IW_FACULTY ZUWEISEN ----------------------------------------------



# ------------------- WEITERE HILFREICHE ANWEISUNGEN ------------------------------------------
-
$userinput = Read-Host "Enter input here and press Enter Key:"
# Einen Benutzer abfragen:
# Get-MsolUser -all  | where-object {$_.UserPrincipalName -like "muster.*"}

# Einem Benutzer eine bestimmte Lizenz zuweisen:
# Set-MsolUserLicense -UserPrincipalName muster.schueler@schulkürzel.onmicrosoft.com -AddLicenses
"schulkürzel:STANDARDWOFFPACK_IW_STUDENT"

# Einem Benutzer eine bestimmte Lizenz weg nehmen:
# Set-MsolUserLicense -UserPrincipalName muster.schueler@schulkürzel.onmicrosoft.com -
RemoveLicenses "schulkürzel:STANDARDWOFFPACK_IW_STUDENT"

# Alle Benutzer der Sicherheitsgruppe grpSchueler mit ihren diversen Attributen in eine csv Datei
schreiben.
# Get-MsolGroup listet die GroupObjectIDs aller unserer Gruppen. Diese IDs sind bei jedem anders!!
# Get-MsolGroupMember -GroupObjectID MeineGruppenID -all | select  DisplayName, EmailAddress,
GroupMemberType, IsLicensed, LastDirSyncTime, OverallProvisioningStatus, ValidationStatus |
Export-Csv $scriptpath\grpSchueler.csv

# Alle unsere AT User werden in eine CSV Datei geschrieben.
# Get-MsolUser -all | where-object {$_.usagelocation -like "AT"} | select displayname,
usagelocation | Export-Csv c:\_temp\VerwendungsstandortAT.csv
```

office365_sync.ps1 endet hier

Interessante Anregungen für Powershell Skripting in diesem Umfeld gibt es hier:

https://digitalglue.wordpress.com/2012/11/29/office-365-granular-license-assignment-via-powershell/

6 Probleme und Lösungen

6.1 Problem bei Office 365 Installation

Wenn LehrerInnen oder SchülerInnen Office 365 instalieren wollen, kann folgende Fehlermeldung kommen:

Bitte das Uninstall FixIt (https://support.office.com/en-us/article/Uninstall-Office-2013-or-Office-365-from-a-Windows-computer-9dd49b83-264a-477a-8fcc-2fdf5dbf61d8) ausführen, und anschließend neu installieren.

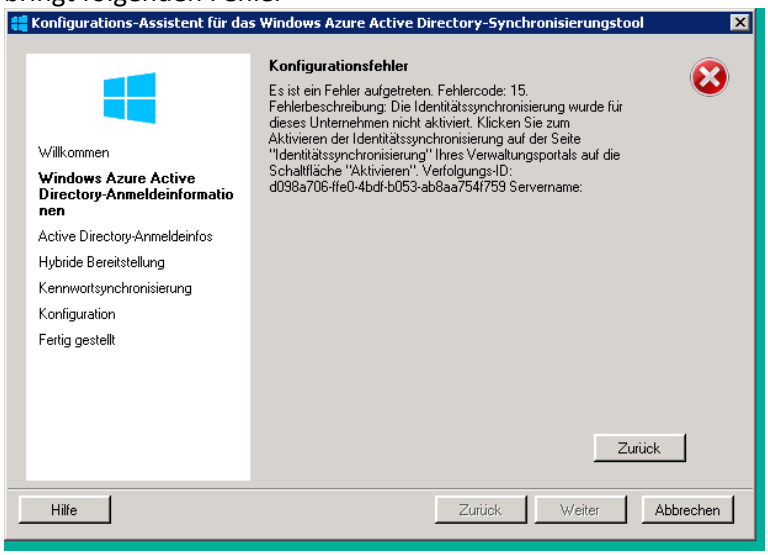
6.2 Active Directory-Synchronisierung kann im portal.office.com nicht eingerichtet werden

Wir ersuchen die AD Synchronisierung am Sportgymnasium Dornbirn einzurichten.
Leider fehlt folgende Punkt auf portal.office.com
BENUTZER – Aktive Benutzer - Active Directory-Synchronisierung: Einrichten
Punkt 3 Active Directory-Synchronisierung einrichten : es fehlt die Schaltfläche Aktivieren.

Die Domäne `sgdo.onmicrosoft.com` ist vorhanden und eingerichtet. Aber die AD Synchronisierung lässt sich nicht aktivieren.
Die Lizenzen funktionieren: Der Domäne sind für Lehrende 500000 zugewiesen und für Student 1000000 Lizenzen zugewiesen.
Benutzer könnten von Hand eingerichtet werden.

Dirssyc.exe wurde installiert.
"C:\Program Files\Windows Azure Active Directory Sync\ConfigWizard.exe"

bringt folgenden Fehler



Lösung:

Azure Active Directory-Modul für Windows PowerShell (64-Bit-Version) öffnen

```
Import-Module MSOnline
PS C:\> Import-Module MSOnline
PS C:\>Connect-MsolService
```

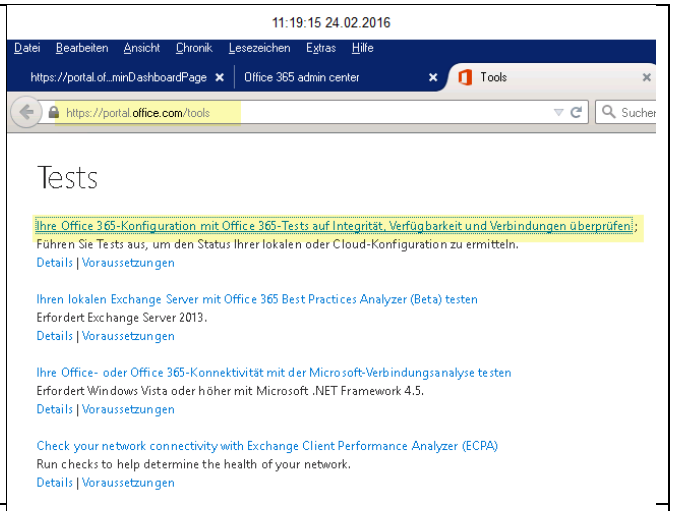
Wir melden uns an mit dem
Office365 Domäne Administrator: admin@bgbr.onmicrosoft.com

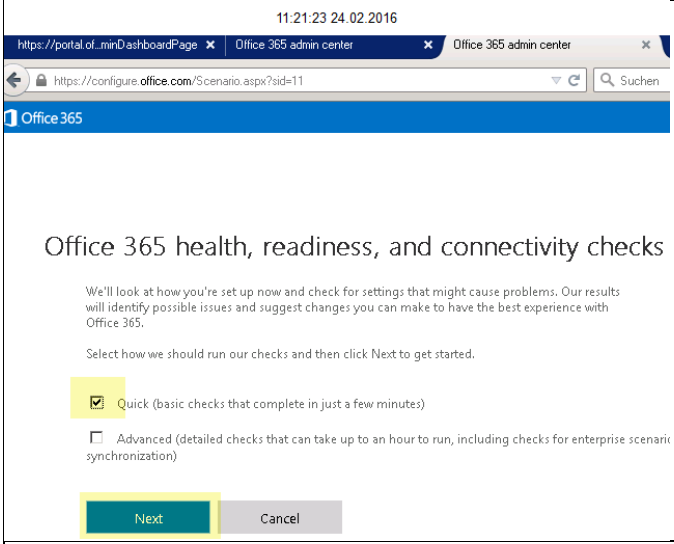
```
Set-MsolDirSyncEnabled -EnableDirSync $true.
```

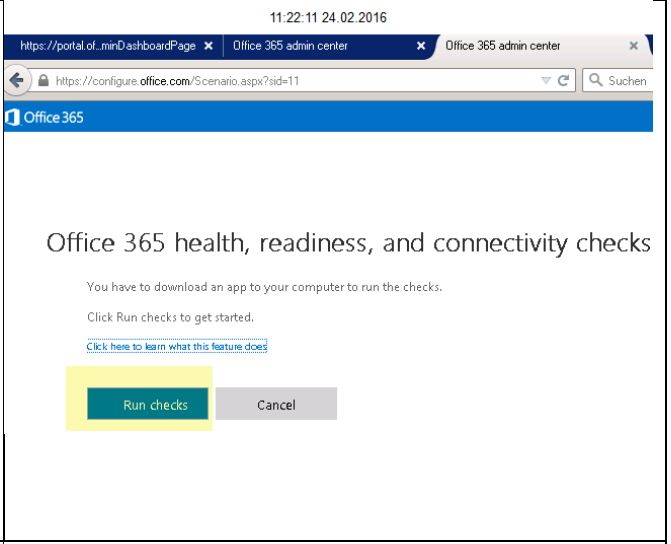
6.3 Office 365 Health Check

Mittlerweile gibt es ein Tool für den Office 365 Health Check:

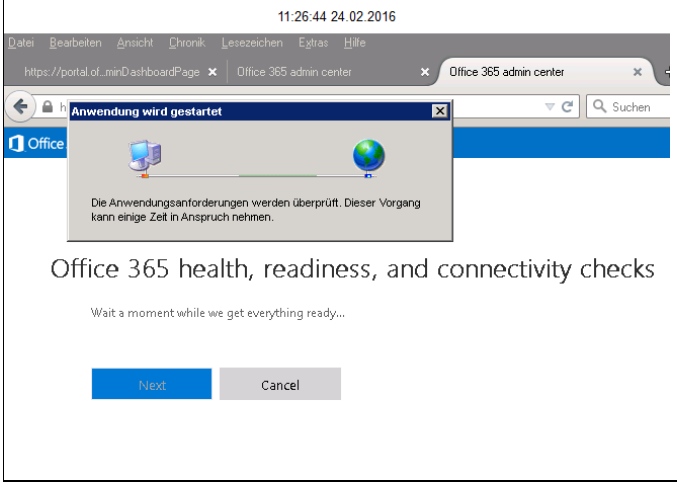
Tools für den Office365 Health check
https://portal.office.com/tools

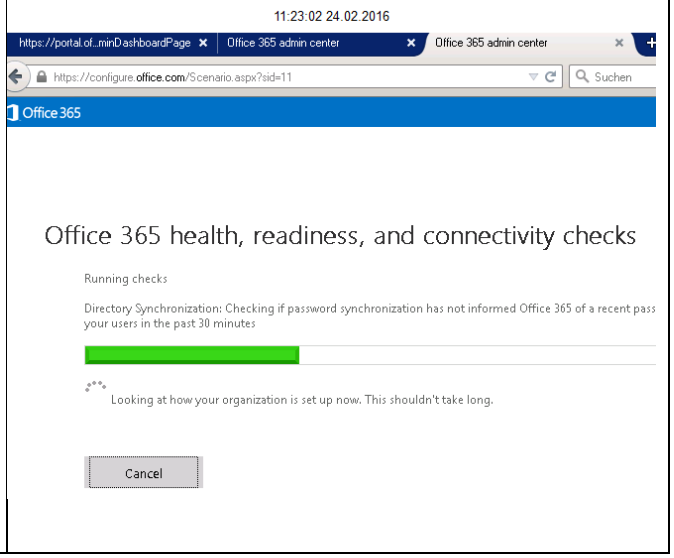


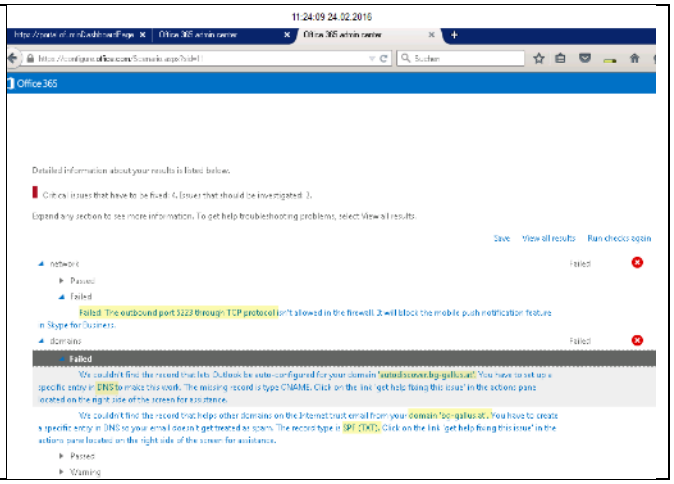




Es werden notwendige Dateien heruntergelaten(ca 15MB – 25MB.





Die Fehler kann man jetzt analysieren. Hier ist ein Port 5223 nach außen nicht offen. Es fehlen auch alle DNS Einträge für Exchange online, da wir weiterhin mail.snv.at nutzen und nicht auf die Exchange Online Dienste von MS setzten.	

6.4 Ports für Office 365

Eine Liste der Ports finden Sie hier:
https://support.office.com/en-us/article/Office-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2?ui=en-US&rs=en-US&ad=US

7 Neue Domäne in bestehenden Office365 Tennant einbinden

7.1 Problem

In Vorarlberg versuchen wir die allgemeinbildende Schul-IT stark zu standardisieren. So entwickelt ein Team ein Serverkonzept (DC, Fileserver, Deployment … Musterclient), das auf einem Host virtualisiert an Schulen ausgeliefert wird. Alle 5-6 Jahre wird so die Domäne gelöscht und durch eine völlig neue (mit weitgehend identischen Benutzern …) ersetzt. Das hat 16 Jahre lang gut funktioniert – unter der Voraussetzung, dass sich die identischen AD Domänen niemals begegnen.

Wenn Sie Ihr Active Directory mit Ihrem Office 365 synchronisieren, stehen Sie vor einem Problem: Synchronisierte Benutzer werden anhand ihrer GUID (aus der in Office 365 eine ImmutableID erzeugt wird) identifiziert.

Szenarien:

1. Sie löschen alle Benutzer in der alten Domäne und synchronisieren:
Alle ihre Benutzer in Office 365 werden gelöscht. Sie befinden sich für 30 Tage im Container „gelöschte Benutzer“. Jetzt könnten Sie diese Benutzer per Powershell endgültig aus dem Papierkorb löschen:
`Get-MsolUser –ReturnDeletedUsers | Remove-MsolUser –RemoveFromRecycleBin –Force`
Sie legen in Ihrer neuen Domäne die Benutzer wieder an und synchronisieren. Die Benutzer werden in Office 365 angelegt. Sie sind völlig neu und haben alle ihre alten Office 365 Daten verloren. Das wird zunehmend unmöglich.
2. Ihre alte Domäne ist noch aktiv. Vor der Umstellung auf die neue Domäne (mit fast identischen Benutzern) beenden Sie in Office 365 die Synchronisierung.
Spätesten nach 72 Stunden haben alle Ihre Benutzer den Synchronisationsstatus von *„Mit Active Directory synchronisiert“* auf *„In Cloud“* geändert.
Wenn Sie jetzt Ihre neue Domäne Synchronisieren werden Benutzer mit gleichem User Principal Name (UPN) mit einer zusätzlichen Nummer im UPN in Office 365 angelegt und sind völlig neue Benutzer. Sie haben ein Chaos.
Beispiel:
Alte Domäne: s1@myDomain.com wird in Office 365 zu s1@myDomain.onmicrosoft.com In Cloud
Neue Domäne: s1@myDomain.com wird in Office 365 zu s14350@myDomain.onmicrosoft.com AD synch.

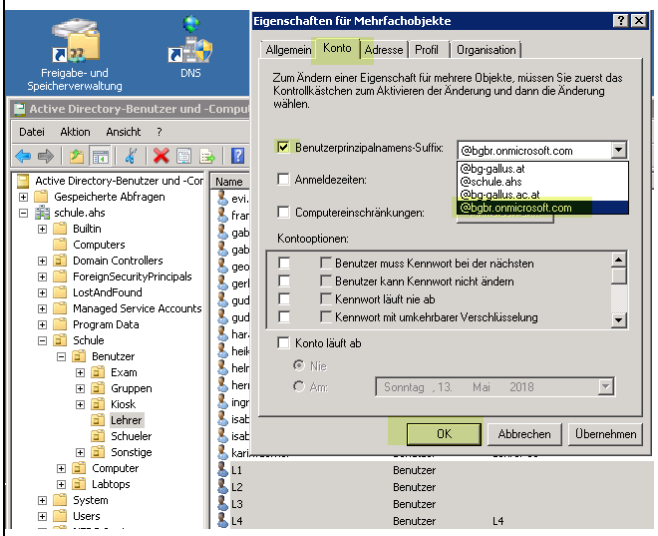
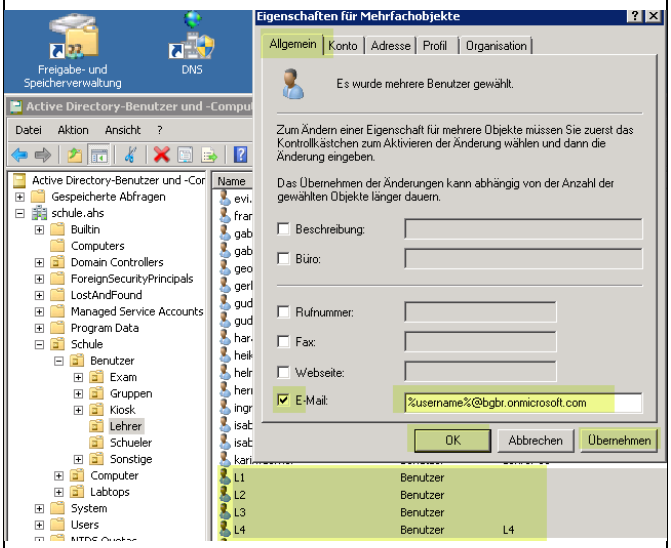
7.2 Lösung:

7.2.1 User Principal Names und identische Email Attribute in der alten Domäne konfigurieren

Ihre alte Domäne ist noch aktiv. Vor der Umstellung auf die neue Domäne (mit fast identischen Benutzern) sorgen Sie für identische UPNs (User Principal Names) und identische Email Attribute.
Beispiel: UPN
max.muster@schulkrzl.onmicrosoft.com

Beispiel Email:
max.muster@schulkrzl.onmicrosoft.com
(%username%@schulkrzl.onmicrosoft.com)

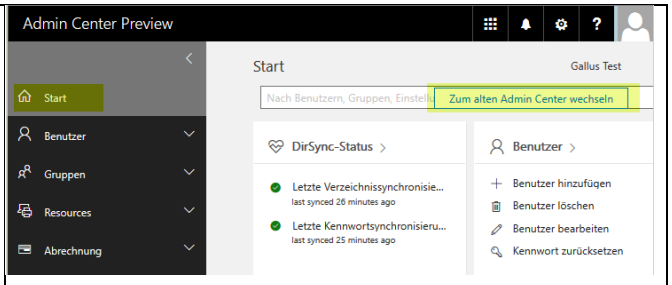
Diese Attribute kann man im AD für mehrer markierte Benutzer ändern:

UPN für mehrere Benutzer ändern	Email für mehrere Benutzer ändern
	

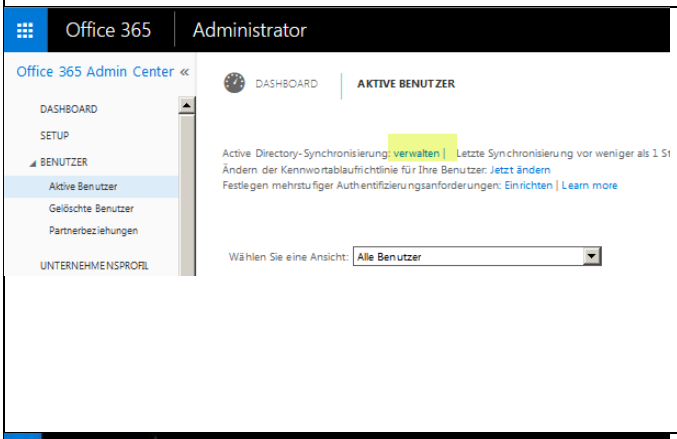
Jetzt synchronisieren Sie Ihre Domäne und überprüfen im Admin Portal ihres Office 365 tennants, ob die Änderungen richtig synchronisert wurden.

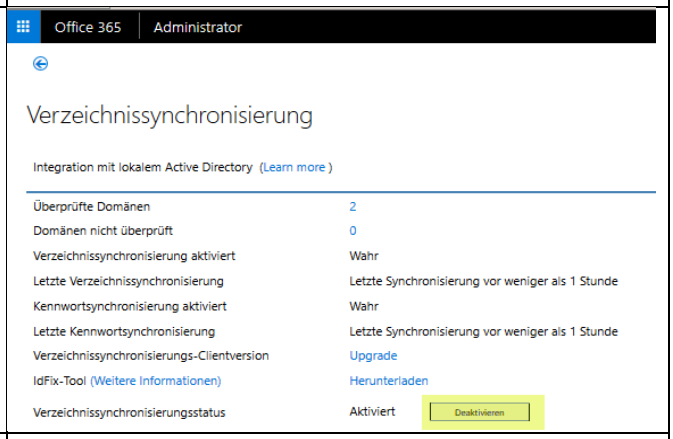
7.2.2 Synchronistation der alten Domäne beenden

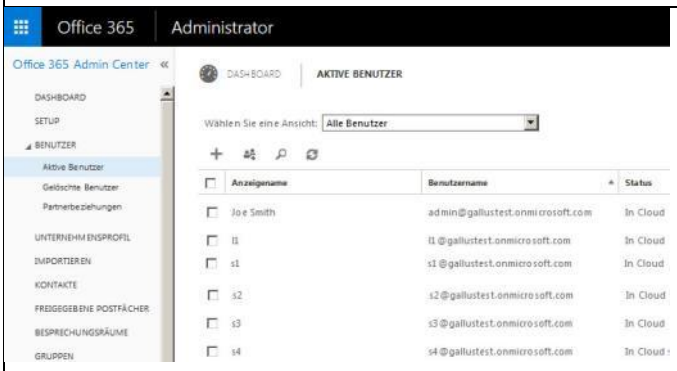
Ihre alte Domäne ist noch aktiv. Vor der Umstellung auf die neue Domäne (mit fast identischen Benutzern) beenden Sie in Office 365 die Synchronisierung. Spätesten nach 72 Stunden haben alle Ihre Benutzer den Synchronisationsstatus von *„Mit Active Directory synchronisiert“* auf *„In Cloud“* geändert.

Zunächst ist unser altes lokales AD noch aktiv und synchronisiert die Benutzer. Leider finde ich Option zum Deaktivieren der Synchronisation nur im alten Office 365 Admin Center: Portal.office.com Anmeldung als Admin Administration – Start – Zum alten Admin Center wechseln Geht nicht mehr?	

Schauen Sie sich die Powershellbefehle auf der nächsten Seite an.





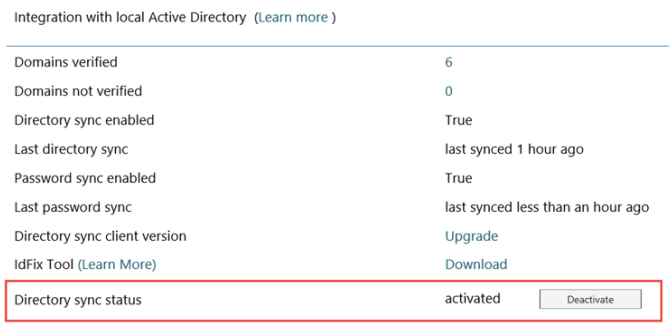


Nach spätestens 72 Stunden sind alle unsere Benutzer InCloud verwaltet und nicht mehr mit dem lokalen AD Synchronisiert.

Where did the "Deactivate" page go in Office365 for Directory Synchronization?

Can't find this page anymore from the Admin Center in Office 365? Quit looking….

Directory synchronization



The "New Way" to Deactivate Directory Synchronization

Pretty much everything with regards to managing Directory Synchronization still exists in the new Admin Center, including really cool "at a glance" reporting features from the main page. But what happened to the "deactivate synchronization"?

The answer = Use PowerShell

When you need to "deactivate" directory synchronization perform the following:

Connect to MSOL services

```
$credential = Get-Credential ""
Import-Module MsOnline
Connect-MsolService -Credential $credential
```

Deactivate Directory Synchronization

```
Set-MsolDirSyncEnabled –EnableDirSync $false
```

Check the status of Directory Synchronization (This could take up to 72 hours to return the result you are expecting to see)

```
(Get-MSOLCompanyInformation).DirectorySynchronizationEnabled
```

7.2.3 ImmutableId in der Office365 Domäne löschen

Was ist die ImmutableId?

Benutzer werden in Office 365 meist über die ImmutableId eindeutig identifiziert. Diese ID leitet sich aus der GUID des Benutzers ab. Wenn wir unser neues lokales Active Directory (mit weitgehend identischen Benutzern) ins Office 365 synchronisieren, findet kein Matching auf Basis des User Principal Name (UPN) und der Emailadresse statt. Die Neuen Benutzer werden mit einem vierstelligen numerischen Zusatz in Office 365 angelegt. Siehe dazu im Screenshot den Benutzer l1.

Wird diese ImmutableId nicht gelöscht, wird bei der Synchronisation des Office 365 Tennants mit der neuen lokalen Active Directory Domäne kein Matching ausgeführt. Das Matching setzt auch einen identischen **User Principal Name (UPN) und die Emailadresse für die richtige Zuordnung voraus.**

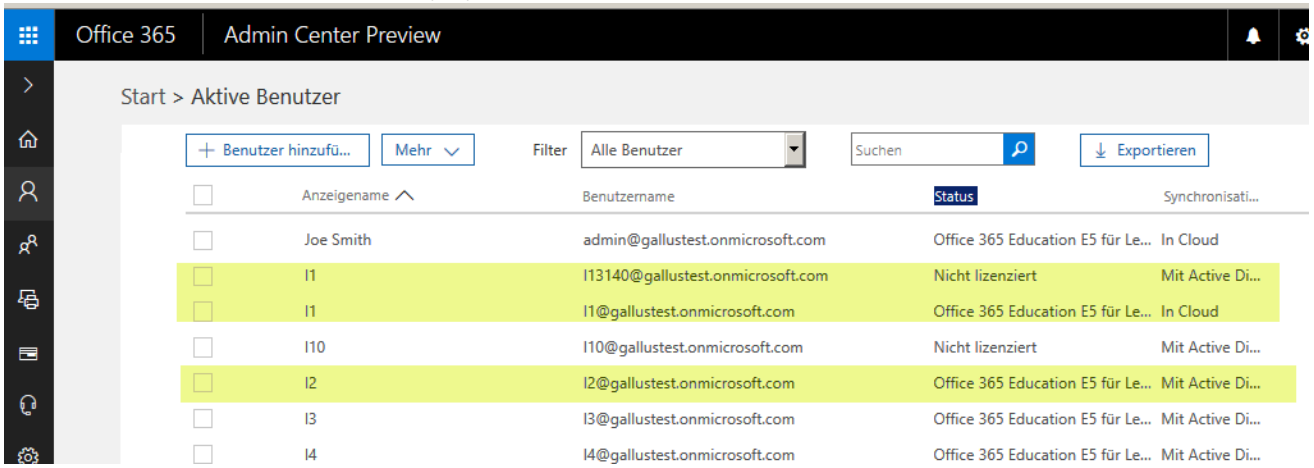
Fall 1:
- ImmutableID nicht gelöscht:

Lokale AD Domäne:	Office365
l1@gallustest.onmicdrosoft .com →	l13140@gallustest.onmicdrosoft .com

Fall 2:
- ImmutableID ist gelöscht:
- User Principal Name (UPN) ist identisch
- Emailadresse ist identisch:
- Unsere Gebete werden erhört
Wird diese ImmutableId gelöscht, wird bei der Synchronisation des Office 365 Tennants mit der neuen lokalen Active Directory Domäne ein Matching ausgeführt, wobei der **User Principal Name (UPN) und die Emailadresse ausschlaggeben für die richtige Zuordnung sind**.

Lokale AD Domäne:	Office365
l2@gallustest.onmicdrosoft .com →	l2@gallustest.onmicdrosoft .com
l3@gallustest.onmicdrosoft .com →	l3@gallustest.onmicdrosoft .com
l4@gallustest.onmicdrosoft .com →	l4@gallustest.onmicdrosoft .com

Fehler bei User l1 und korrekt bei l2, l3, l4.



7.2.4 Löschen der ImmutableID per PowerShell:

```
Set-MsolUser -UserPrincipalName s1@myDomain.onmicrosoft.com -ImmutableId $null
```

In der neuen lokale AD Domäne erstellen Sie dieselben Benutzer **mit identischer Emailadresse und identischem UPN Name und UPN Suffix.!:**

Email: s1@myDomain.onmicrosoft.com

UPN Name: s1@myDomain.onmicrosoft.com

Wenn Sie jetzt die neue Domäne synchronisieren, sollte ein User Matching passieren:

Alte Domäne: s1@myDomain.com wird in Office 365 zu s1@myDomain.onmicrosoft.com In Cloud

Neue Domäne: s1@myDomain.com wird in Office 365 zu s1@myDomain.onmicrosoft.com AD synch.

Dabei handelt es sich um dieselben Acounts. Sowohl Exchange Daten als auch One Drive Daten bleiben in meinen Tests erhalten.

Danke Thomas Hauser! Wo wären wir ohne Deine Hilfe. Wir wüssten nicht, was wir ohne Deinen Support täten.

7.2.5 Löschen der ImmutableId per Powershell für alle Benutzer

Voraussetzungen:

- Die Synchronisierung der Domäne ist beendet.
- Alle unsere Benutzer sind *In Cloud* verwaltet.
- Unsere Gruppen grpLehrer, grpschuler … sind noch vorhanden. Wir haben ja mit den Benutzern auch unsere Gruppen synchronisiert.

Die ImmutalbeId löscht man per Powershell grundsätzlich so:

```
Import-Module MSOnline
Connect-MsolService
Set-MsolUser -UserPrincipalName myUser@mydomain.onmicdrosoft.com -ImmutableId "$null"
```

Anmerkung: in den Tests verwendete ich wie von Thomas Hauser vorgeschlagen.
`Set-MsolUser -UserPrincipalName myUser@mydomain.onmicdrosoft.com -ImmutableId ""`
Die BLOGs sagen man muss "$null" setzen.

Wir wollen die ImmutalbeId nicht für jeden Benutzer einzeln lösen, sondern für alle Mitglieder unserer Gruppen:

Anzeige der vorhandenen Gruppen:

```
PS C:\>Import-Module MSOnline
PS C:\>Connect-MsolService
PS C:\>get-msolgroup

ObjectId                                DisplayName
8725454e-33ba-4900-8735-f5d3b18444ba    grpSchueler                Security
c59cdca3-aa16-4ead-a5b2-9685b042b47d    grpSchueler                Security
66e9ef6e-8ba6-4f1b-aeca-91ad620b43da    grpLehrer                  Security
```

Anzeige aller LehrerInnen, deren ImmutableId nicht leer ist:

```
PS C:\>get-msolgroupmember -all -groupobjectid 66e9ef6e-8ba6-4f1b-aeca-
91ad620b43da | get-MSolUser |
 where {$_.ImmutableId -notlike "$null"} | select displayname

DisplayName
-----------
l2
l3
l4
```

Anzeige aller LehrerInnen, deren ImmutableId nicht leer ist und Export in eine CSV Datei:

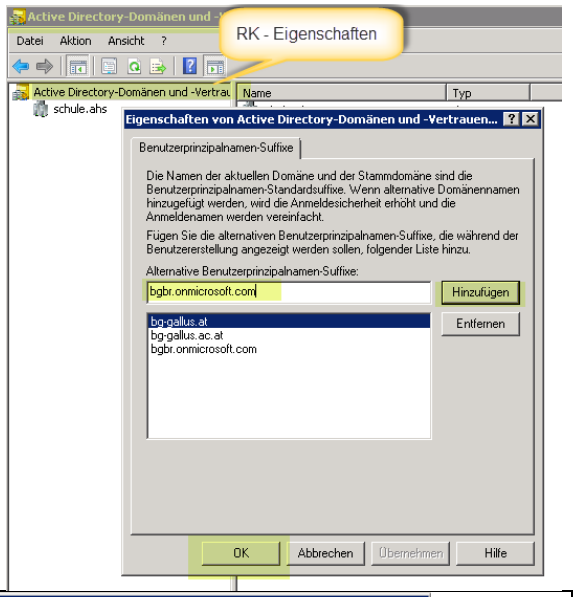
```
PS C:\>get-msolgroupmember -all -groupobjectid 66e9ef6e-8ba6-4f1b-aeca-
91ad620b43da | get-MSolUser | where {$_.ImmutableId -notlike "$null"} | select
SignInName | export-csv -path "c:\temp\result1.txt"
```

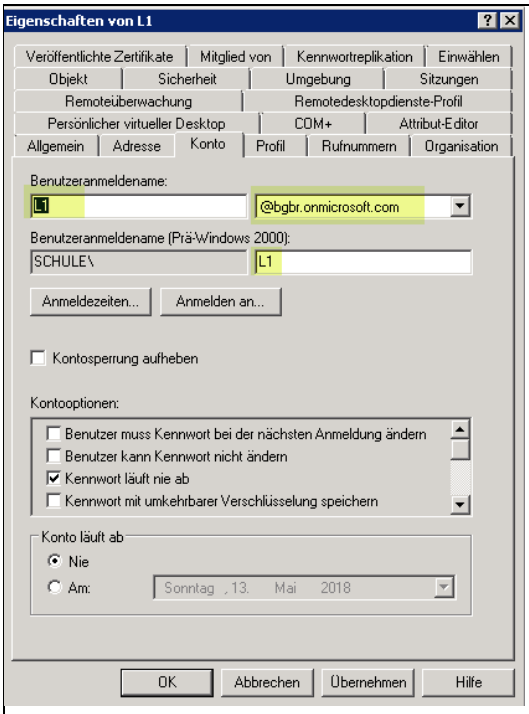
Leeren der ImmutableId aller LehrerInnen, deren ImmutableId nicht leer ist und Export in eine CSV Datei:
Voraussetzung: Alle Benutzer sind **In Cloud** verwaltet.

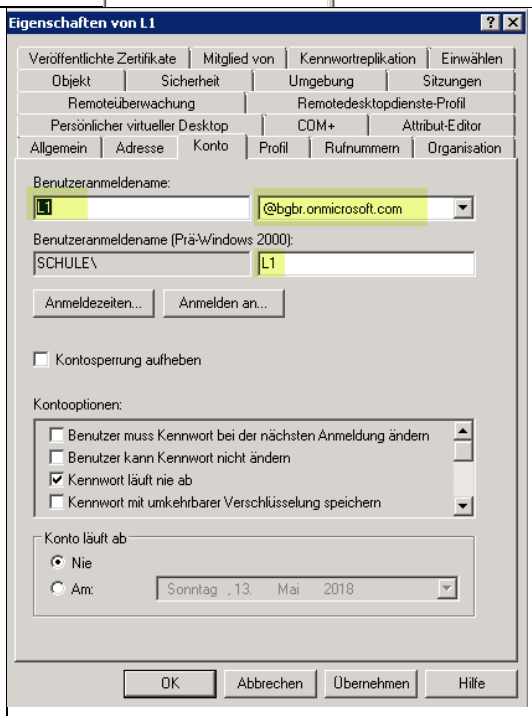
```
PS C:\> get-msolgroupmember -all -groupobjectid 66e9ef6e-8ba6-4f1b-aeca-
91ad620b43da | get-MSolUser | where {$_.Immutabl
eId -notlike "$null"} | Set-MsolUser -immutableId "$null" | select SignInName |
export-csv -path "c:\temp\result1.txt"
```

7.2.6 Neue Domäne Synchronisieren:

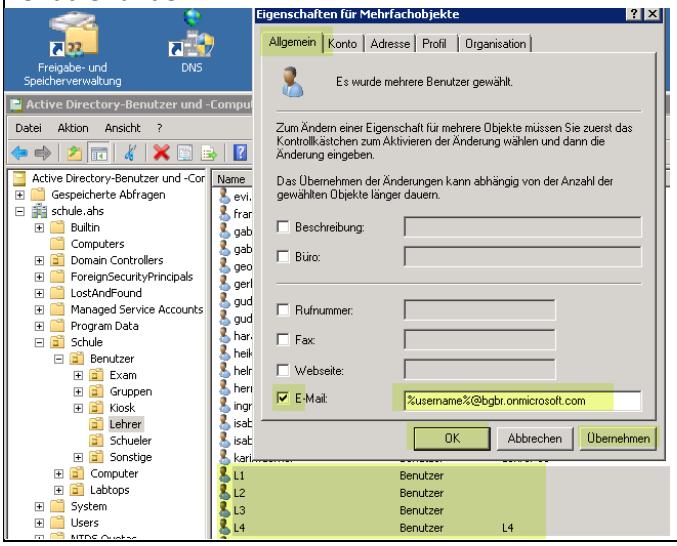
- Erstellen einer neuen Domäne mit dcpromo.exe
- Alternativer Benutzerprinzipalnamen Suffix im Active Directory-Domänen und Vertrauensstellungen: Unsere Office 365 Domain Tennant heißt: bgbr.onmicrosoft.com
- Der alternative Benutzerprinzipalnamensuffix im neuen AD muss der Office 365 Domäne entsprechen und muss auch den Usern zugeordnet sein.
- Gruppen erstellen (grpLehrer, grpSchueler …)
- **Identische Benutzer erstellt mit identischer Emailadresse und Gruppenmitgliedschaft**

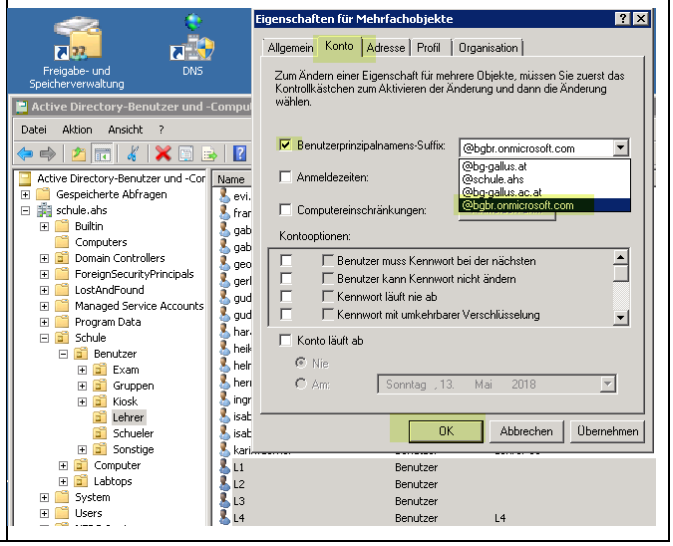






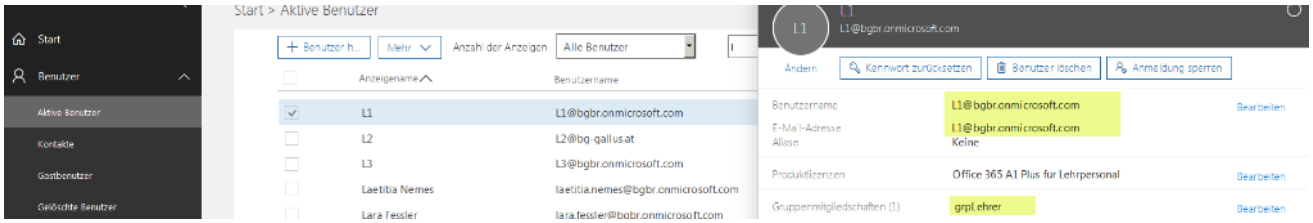
Diese Attribute kann man im AD für mehrer markierte Benutzer ändern:





Diese Benutzer schauen im Office 365 Admin Center so aus und sind in folgenden Punkten ident:

- User Principal Name und Domain Suffix: L1@bgbr.onmicrosoft.com
- Email: L1@bgbr.onmicrosoft.com
- Die ImmutableID ist leer.



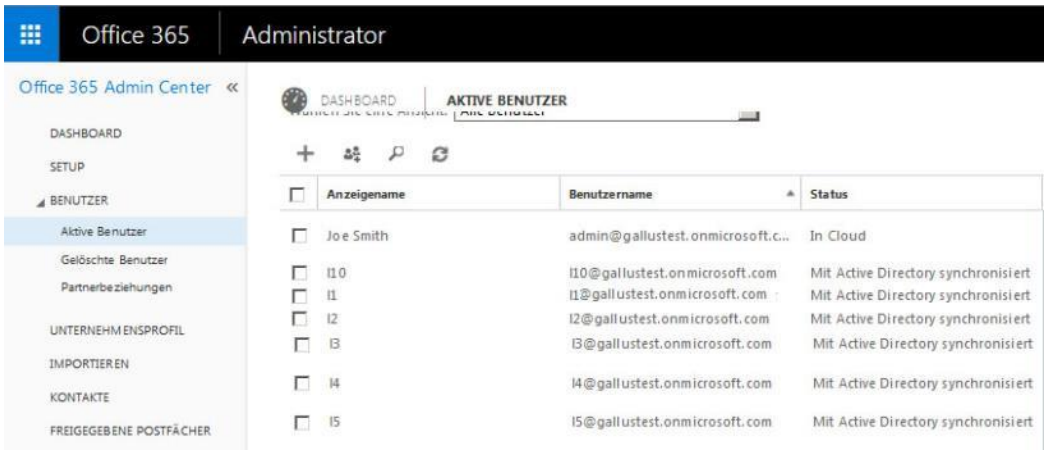
Jetzt starten wir die Synchronisierung und beten ...

- ADConnect installieren und synchronisieren
- AD Synchronisation in der Powershell starten:

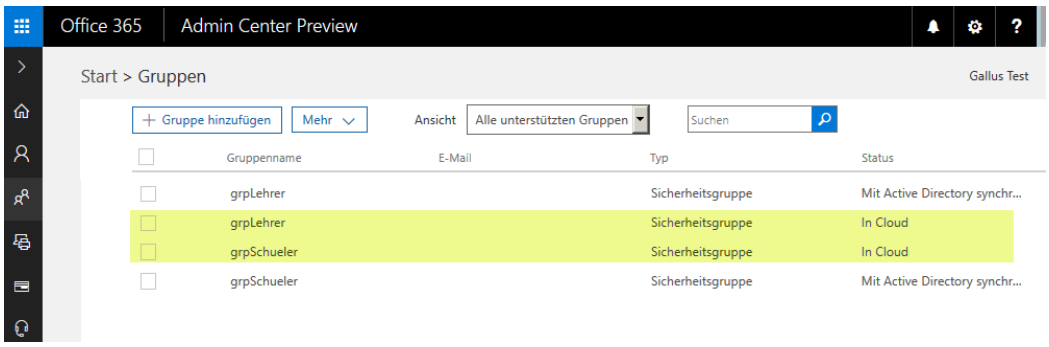
```
Import-Module MSOnline
Connect-MsolService
Start-ADSyncSyncCycle -PolicyType Initial
```

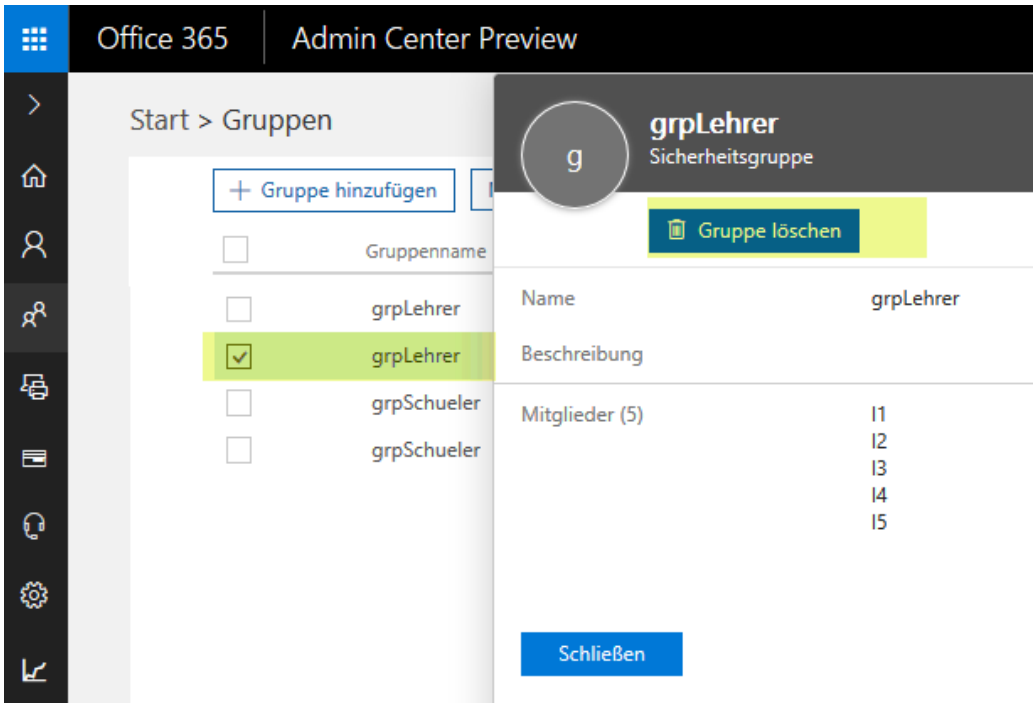
7.2.7 Kontrolle und aufräumen in Office 365

- Wurden die Benutzer sauber synchronisiert?
- Finden sich Benutzer mit vierstelligen Zahlenzusätzen?
- Was befindet sich im Ordner gelöschte Benutzer (Indikator für Probleme) ?



Löschen Sie die Gruppen der alten Domäne.





7.3 Soft (SMTP) vs. Hard (immutableID) matching with Azure AD Connect

by Alex 08. June 2017 Technical 0

If you are setting up Directory Synchronization from scratch (there are no users in the cloud yet), then Azure AD Connect will be pretty straightforward–the on-premises objects (and passwords if you choose that option) will be synchronized to the cloud, and you can assign services to the user accounts from there.

But what if you already have user accounts in the cloud which correspond to already existing user objects in the on-premises directory, and Directory Synchronization has not yet been configured between them? For example, if your organization previously migrated mailboxes to Office 365 using the cutover method or a third party tool. Or, if you had users provisioned for another Microsoft Online Service such as CRM, before you attempted mailbox migration.

In cases like these, you may need to create a matching mechanism between the on-premises accounts and the cloud-based ones, so that Azure AD Connect knows that they refer to the same user. There are two basic methods to create this "matching":

1. Soft match (also known as SMTP matching)
2. Hard match (by immutableID).

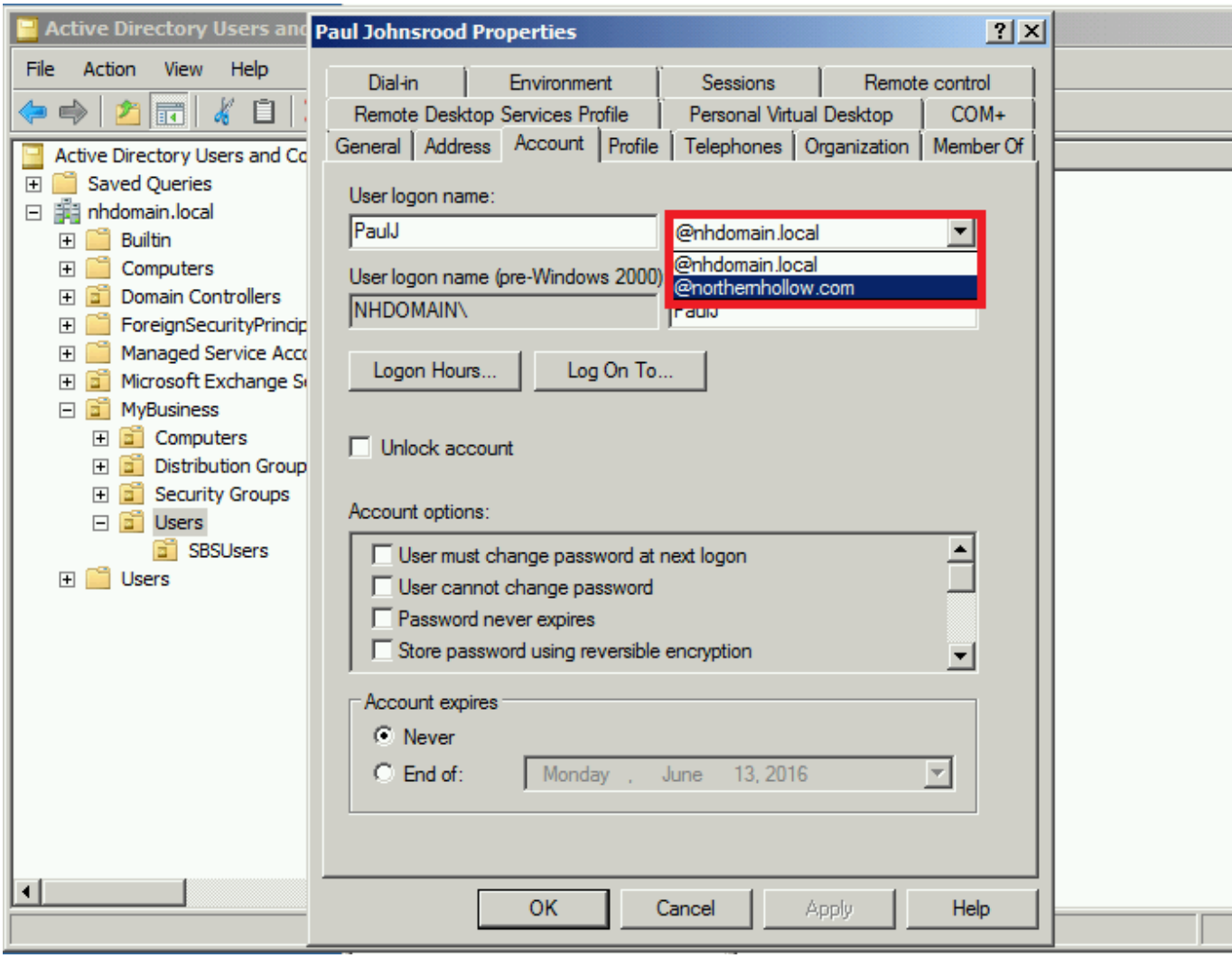
7.3.1 Soft Matching using the SMTP address

To create soft matches, which will be adequate in 95% of situations, you will need to ensure first of all that your UPN suffixes match between on-premises and cloud-based accounts. What do we mean by this? It means that your users' sign-in needs to be tied to the domain of your primary email address in both the local AD and in Azure AD.

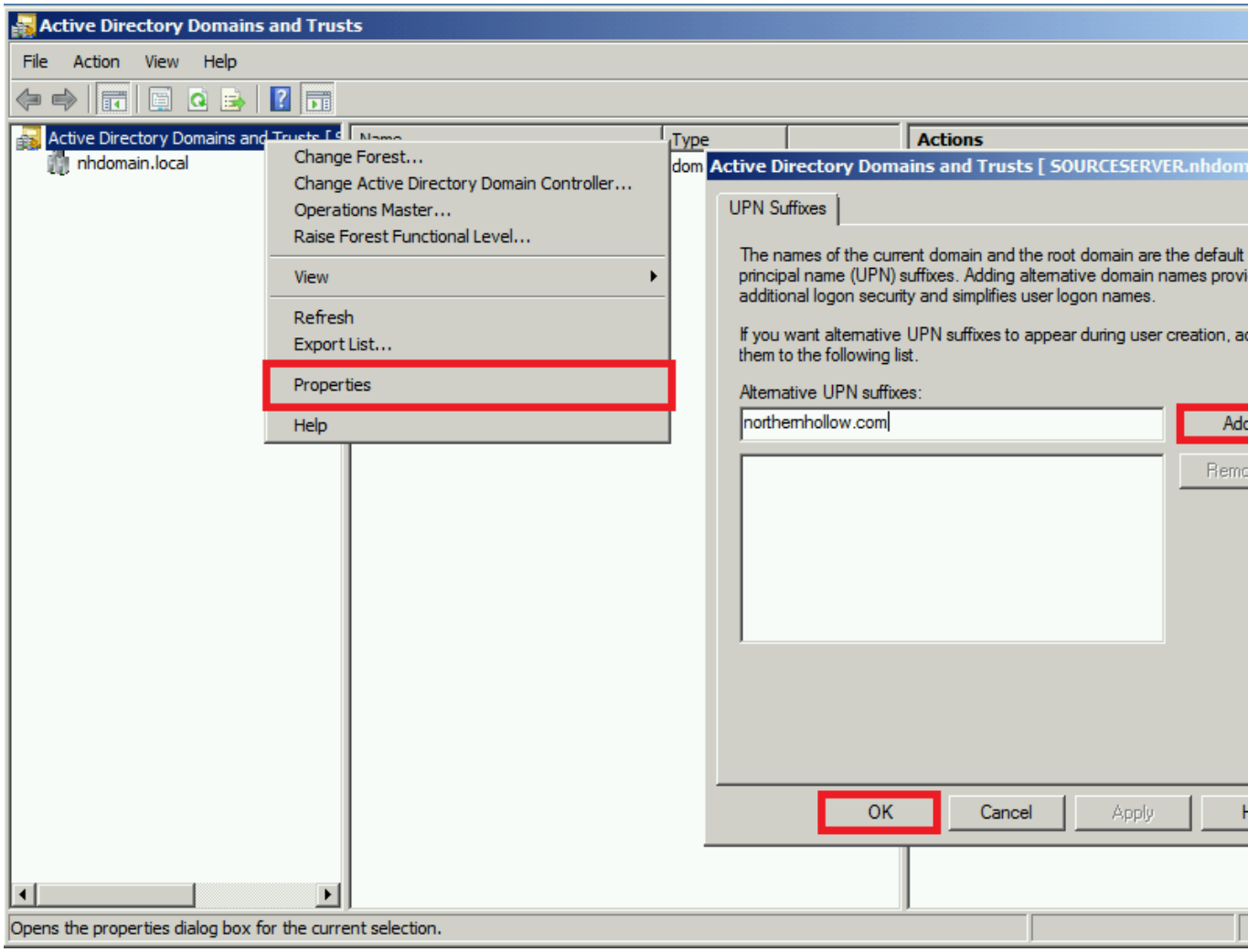
In the On-premises Active **Directory**

First, when you open the properties of a user account object, this object should have the email address field filled out (the primary SMTP address for the user)–so be sure that is the case first. Now take a look under the Account tab, and you should see the user logon name followed by a suffix.

The goal is to have this logon name be *username@domain.com*–that is, the email address–and not the local domain name *username@domain.local*. Note that you can also bulk-select accounts and make this suffix change on many objects at once.



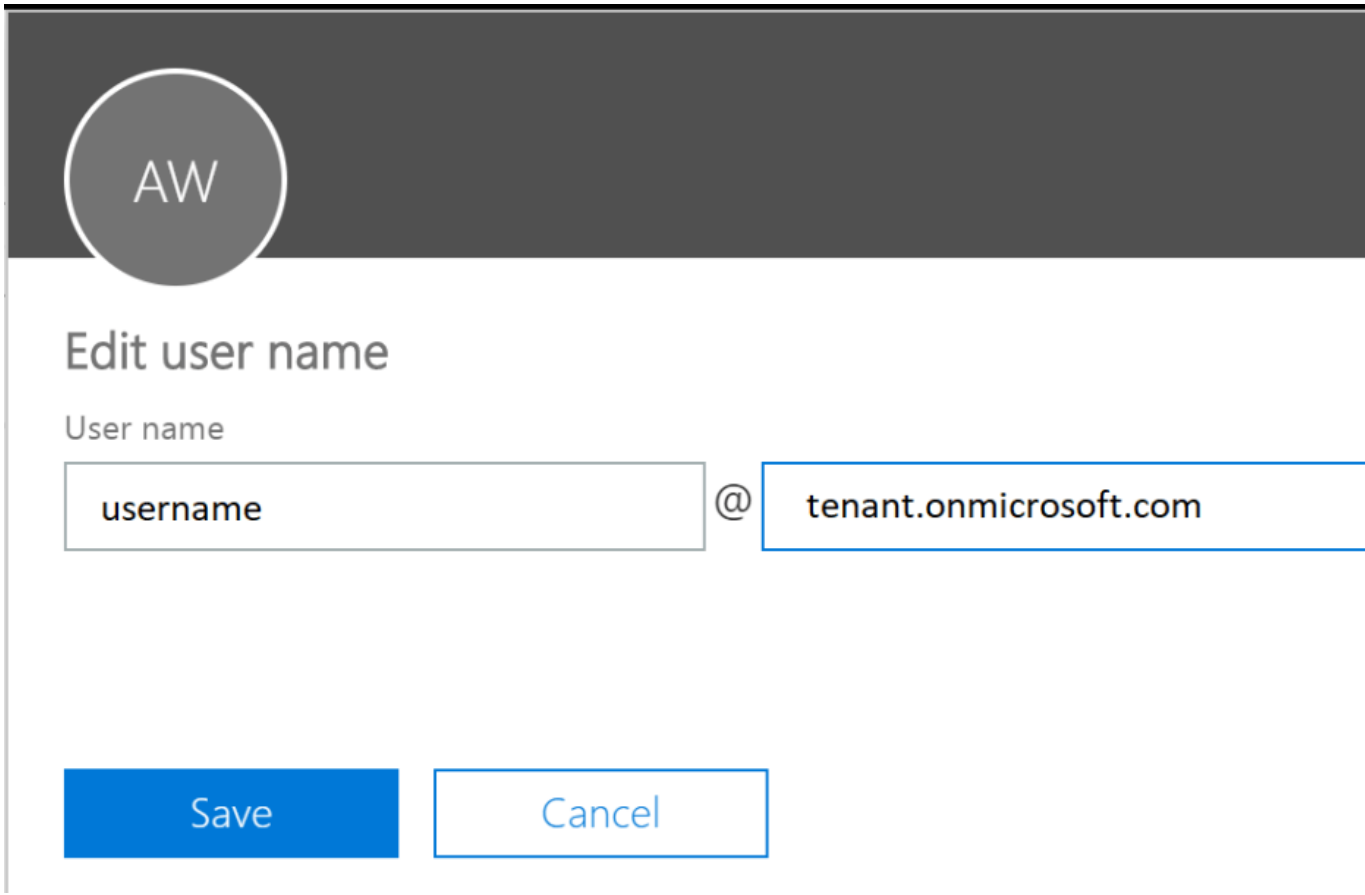
If you do not have the option to drop down your suffix and choose the alternative, you can easily and quickly add the suffix using the Active Directory Domains & Trusts MMC console. Right-click Active Directory Domains and Trusts, and select Properties. Enter your email domain name and click Add. Click OK.



In the Azure AD / Office 365 cloud

In Office 365, you will also want to make sure the sign-in name is the same as on-premises, using the correct UPN suffix for the email domain name. So the goal is to have this match *username@domain.com* again, and not *username@tenant.onmicrosoft.com*.

In the Office 365 Portal, find your Active Users, select a user, then edit the username.



In Exchange Online, you can also see that the primary SMTP address matches what we have listed in the on-premises account. Admin Centers > Exchange > recipients. Edit a recipient and click email addresses.
You can also export bulk lists for comparison from Active Directory as follows:

```
Get-ADUser -SearchBase "DC=company,DC=local" -Filter * -Properties * | Select-Object -Property Name,SamAccountName,EmailAddress | Sort-Object -Property Name | Export-Csv -path C:\export\ADUsers.csv
```

And from Office 365:

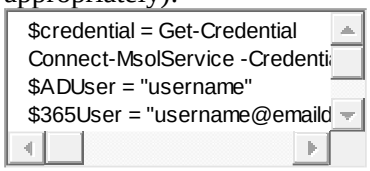
```
Get-MsolUser | select-object -property userprincipalname,displayname,islicensed | export-csv -path c:\export\365Users.csv
```

Now, assuming you have your UPN and email addresses all matching, you should be able to download & install Azure AD Connect. Upon running the first synchronization, SMTP matching should kick in, and figure out that the on-premises accounts already have cloud counterparts existing. When you login to the portal and view your active users again, you should see a field describing the synchronization status, and each account from the on-premises directory should read "*Synced with Active Directory*."

7.3.2 Hard Match using the GUID / immutableID

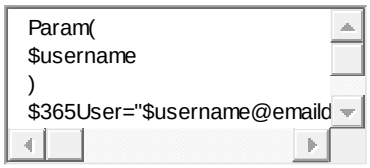
In some circumstances, soft matching may fail, and the on-premises accounts are not properly matched. Sometimes a previously existing cloud account can have certain fields populated already (e.g. immutableID) that will confuse the Directory Synchronization tool, even if the SMTP addresses are matching.
In these scenarios, you can turn to a "hard match," which is performed by taking the on-premises GUID, then converting this value into what is known in the Azure AD cloud as an "immutableID," and then

writing that converted value directly into Azure AD. When Directory Synchronization runs, it will have no question marks about whether this is the same object, because it is being told so explicitly.
Before you proceed with this, you will still want to ensure that the UPN suffixes match the primary email domain on-premises and in the cloud, just as we did above. Then, when you have identified any accounts that failed to sync up, you can run the following for each affected account (be sure to fill in the variables appropriately):



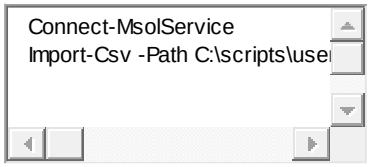

```
1  $credential = Get-Credential
2  Connect-MsolService -Credential $credential
3  $ADUser = "username"
4  $365User = "username@emaildomainname.com"
5  $guid =(Get-ADUser $ADUser).Objectguid
6  $immutableID=[system.convert]::ToBase64String($guid.tobytearray())
7  Set-MsolUser -UserPrincipalName "$365User" -ImmutableId $immutableID
```

And of course, this can also be generalized for bulk changes, for example if you use the variables as fields in a CSV file, and import the CSV, with a for-each loop. You could even do this with a single variable in some cases:




```
1  Param(
2  $username
3  )
4  $365User="$username@emaildomainname.com"
5  $guid=(get-ADUser $username).Objectguid
6  $immutableID=[system.convert]::ToBase64String($guid.tobytearray())
7  Set-MsolUser -UserPrincipalName "$365User" -ImmutableId $immutableID
```

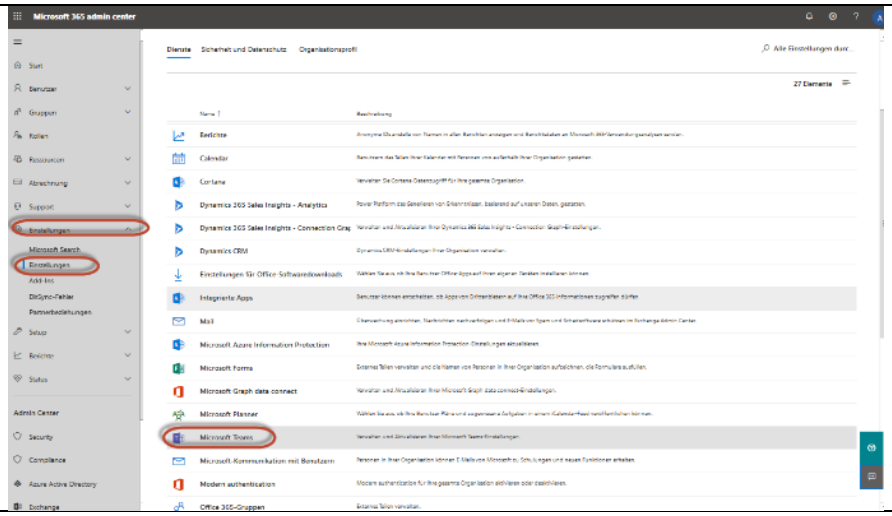
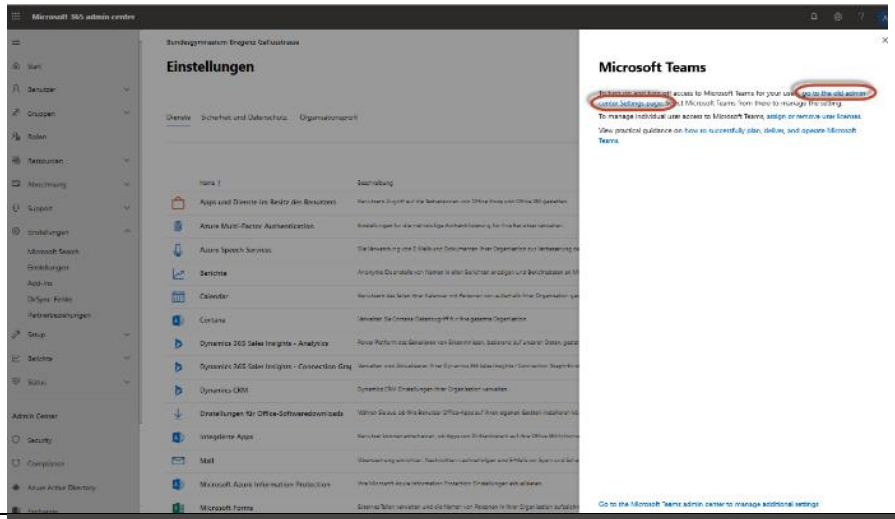
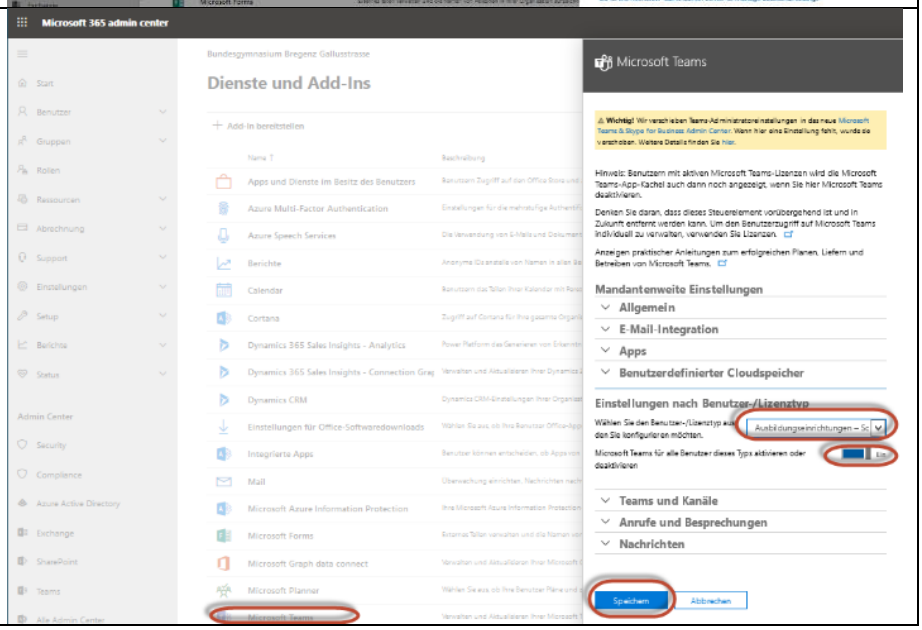
The above would be saved as HardMatch.ps1, then you can run the for-each loop as follows:




```
1  Connect-MsolService
2  Import-Csv -Path C:\scripts\users.csv | ForEach { C:\scripts\HardMatch.ps1 -Username $_.Username
   }
```

No more mis-matches. That should pretty much take care of everyone who is having trouble getting matches made with Directory Synchronization (I've been getting a fair number of inquiries lately). A shout-out to my co-worker Lionel who put this script together for us–nice work, dude!

8 MS Teams aktivieren

Zumindest zwei Schulen berichteten, dass man MS Teams für SchülerInnen explizit im alten Amin Center aktivieren muss:	
Wechsel ins alte Admin Center	
Unter Dineste und Add-Ins MS Teams auswählen MS Teams Ausbildungseinrichtungen Schüler → Schieberegler auf Ein → Speichern	

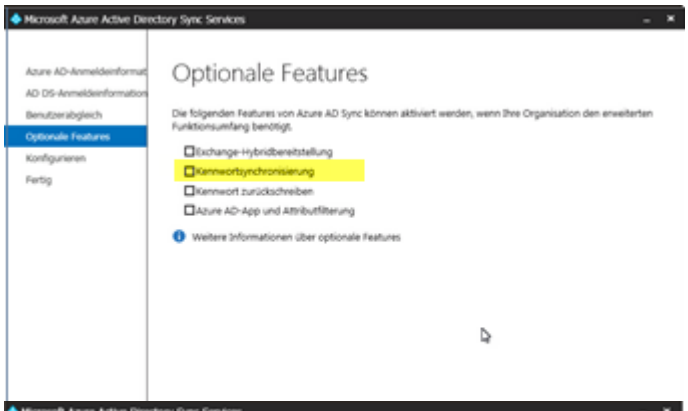
9 Ältere Probleme

9.1 Microsoft Azure Connection Tool synchronisiert keine Passwörter

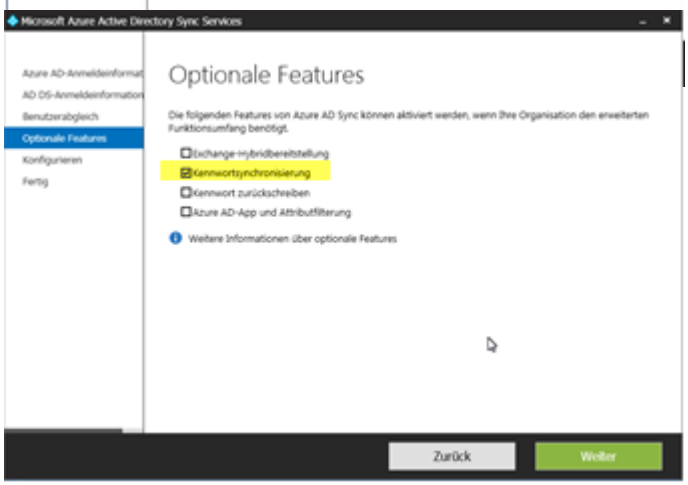
Bei Michael Flatz wurden die Passwörter der Benutzer nicht synchronisiert. Man merkte das sofort, weil man sich im portal.office.com nicht anmelden konnte. Auch eine Änderung des Passwortes im Active Directory führte zu keinem Erfolg. Wie im Screenshot unten wird das AD zwar synchronisiert, aber die Passwörter nicht - LastPasswordSyncTime bleibt leer.

```
PS C:\Users\administrator.SCHULE> Connect-MSOLService
PS C:\Users\administrator.SCHULE> Get-MSOLCompanyInformation


DisplayName                           : Privatgymnasium Mehrerau
PreferredLanguage                     : de
Street                                : Mehrerauerstraße 68
City                                  : Bregenz
State                                 : Vorarlberg
PostalCode                            : 6900
Country                               :
CountryLetterCode                     : AT
TelephoneNumber                       : 05574 71438 67
MarketingNotificationEmails           : {}
TechnicalNotificationEmails           : {michael_flatz@outlook.com}
SelfServePasswordResetEnabled         : True
UsersPermissionToCreateGroupsEnabled  : True
UsersPermissionToCreateLOBAppsEnabled : True
UsersPermissionToReadOtherUsersEnabled : True
UsersPermissionToUserConsentToAppEnabled : True
DirectorySynchronizationEnabled       : True
LastDirSyncTime                       : 05.05.2015 07:21:51
LastPasswordSyncTime                  :
PasswordSynchronizationEnabled        : True


PS C:\Users\administrator.SCHULE> $adConnector  = Get-ADSyncConnector |where {$_.Name -notlike "*- AAD*"}
PS C:\Users\administrator.SCHULE> $aadConnector = Get-ADSyncConnector |where {$_.Name -like "*- AAD*"}
PS C:\Users\administrator.SCHULE> Set-ADSyncAADPasswordSyncConfiguration -SourceConnector $adConnector.Name -TargetConne
ctor $aadConnector.Name -Enable $false
Password Hash Sync Configuration for source "schule.ahs" updated.
PS C:\Users\administrator.SCHULE> Set-ADSyncAADPasswordSyncConfiguration -SourceConnector $adConnector.Name -TargetConne
ctor $aadConnector.Name -Enable $true
Password Hash Sync Configuration for source "schule.ahs" updated.
PS C:\Users\administrator.SCHULE> _
```

Stundenlanges Probieren und Hilfe des Supports waren auch nicht zielführend. Schlussendlich funktionierte es auf einmal und die letzte Aktion zuvor war eine erneute Installation/Konfiguration des Microsoft Azure Connection Tools – diesmal aber mit deaktivierter Kennwortsynchronisation.



Dann erneute Installation/Konfiguration mit Kennwortsynchronisation. Wir glauben das hat den Knoten in der Passwortsynchronisation gelöst. Einen Knoten, den im Übrigen einige Firmen haben, wenn man den Recherchen im Internet Glauben schenkt.

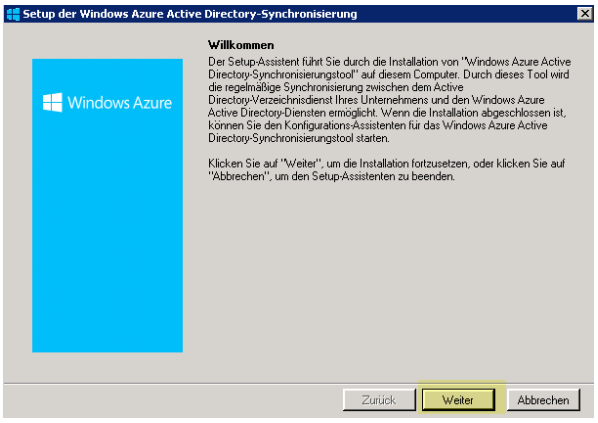


9.2 DirSync: Legacy

Die Verzeichnissynchronisierung mit DirSync ist veraltet und wird seit 2015 nicht mehr verwendet.
AD Connect ersetzt mittlerweile DirSynch
AD Connect hat DirSynch ersetzt. Früher oder Später wird ein Upgrade nötig werden. Das Upgrade sollte die Einstellungen von DirSynch übernehmen.
https://www.microsoft.com/en-us/download/details.aspx?id=47594

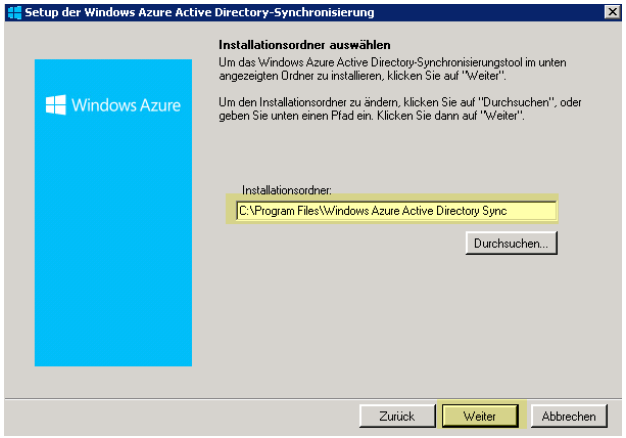
Die Screenshots hier beziehen sich auf das mittlerweile veraltete DirSynch. Nachdem ich für Office 365 keine Testumgebung habe und meine funktionierende Produktivumgebung nicht durch Tests kompromittieren darf, sind die Screenshots unten veraltet.

Jetzt das dirsync.exe als Administrator ausführen. Diese Datei wird von Microsoft laufend aktualisiert und somit könnten die Screenshots von der aktuellen Realität abweichen.

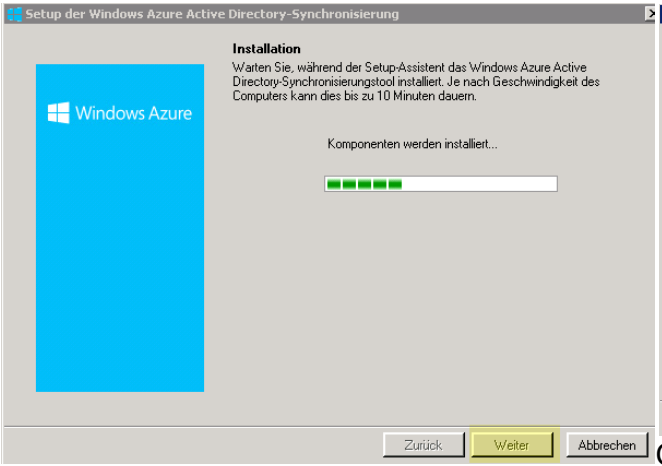


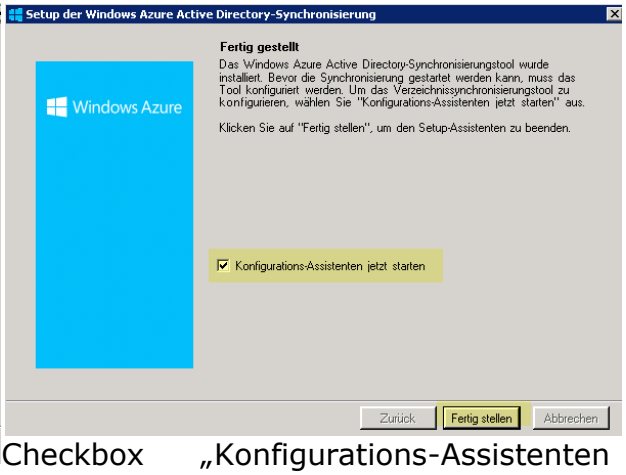
Weiter

Zustimmen - Weiter



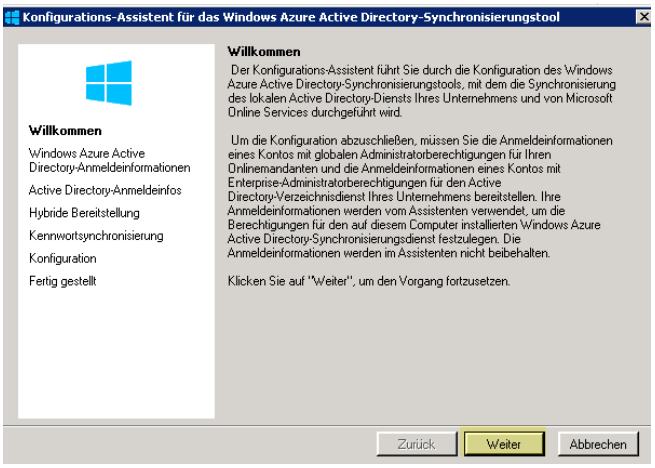
Pfad belassen
Weiter



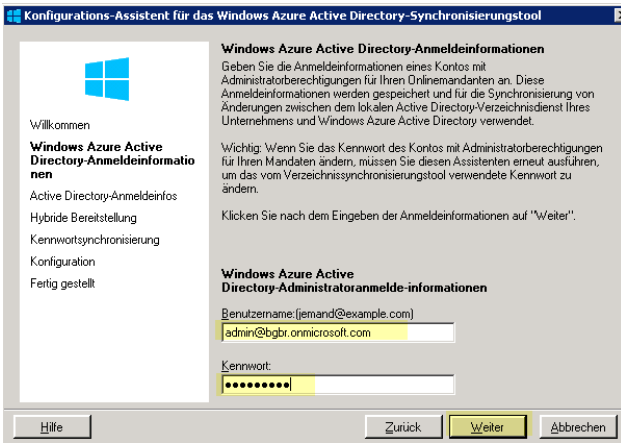


Checkbox „Konfigurations-Assistenten

Die Installation dauert einige Minuten. Nach Abschluss der Installation → Weiter



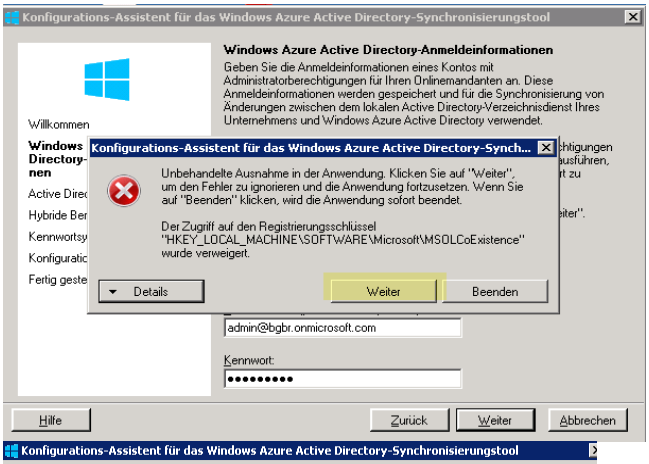
jetzt starten" belassen und Fertig

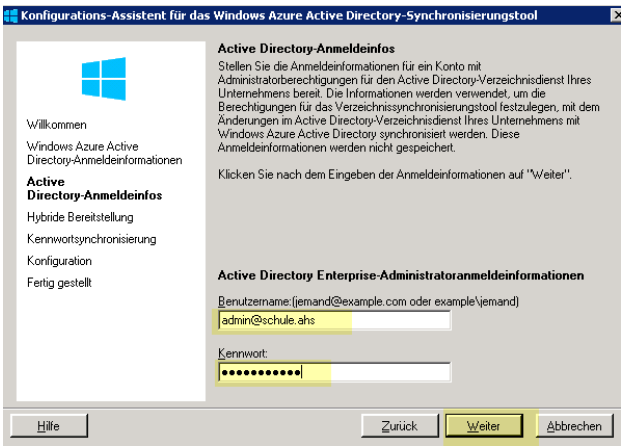


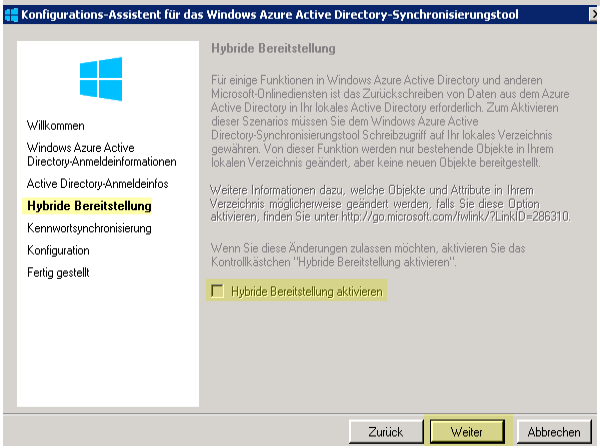
Auf der Willkommensseite des Assistenten klicken Sie auf →Weiter

admin@bgbr.onmicrosoft.com

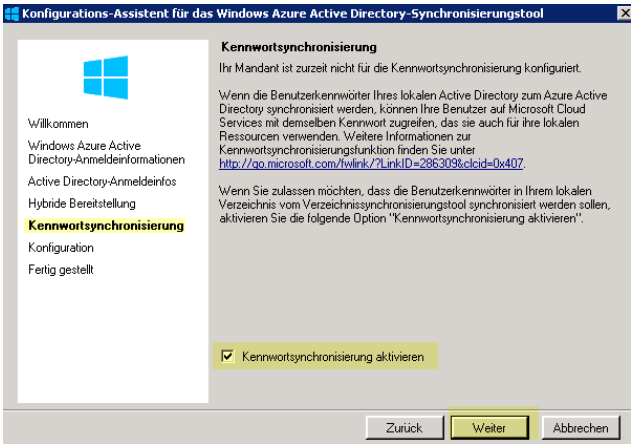
Man muss die Verzeichnissynchronisierungs-konfiguration als Administrator starten. Ansonsten kommt diese Fehlermeldung.

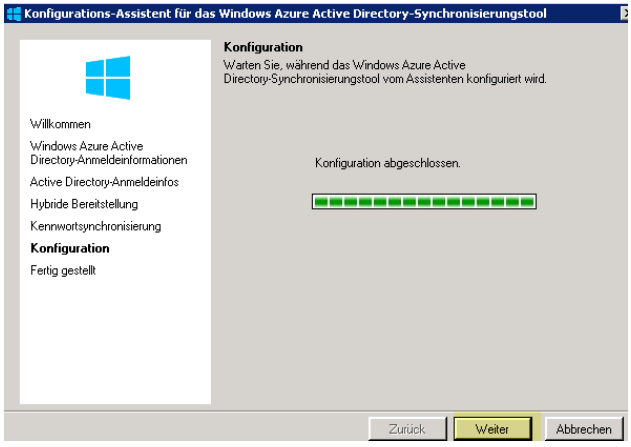




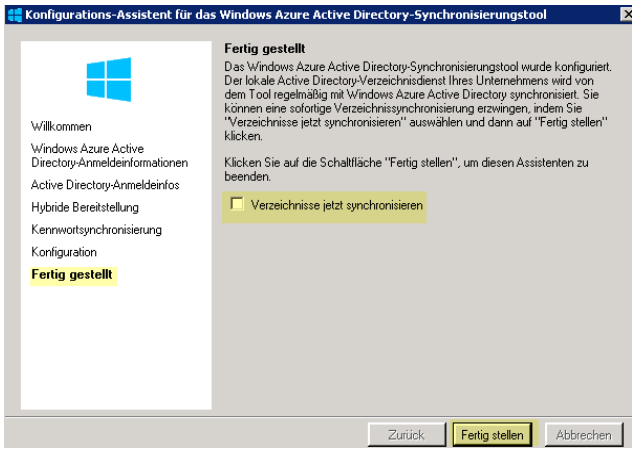


Geben Sie einen Domänenadministrator Account ein. Sie müssen dabei diese Form einhalten: administrator@domäne





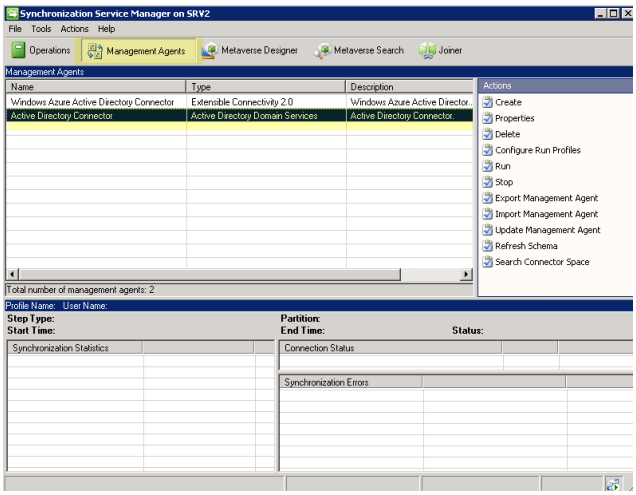
Deaktivieren Sie das Kontrollkästchen „Verzeichnisse jetzt synchronisieren“ und klicken Sie auf Fertig



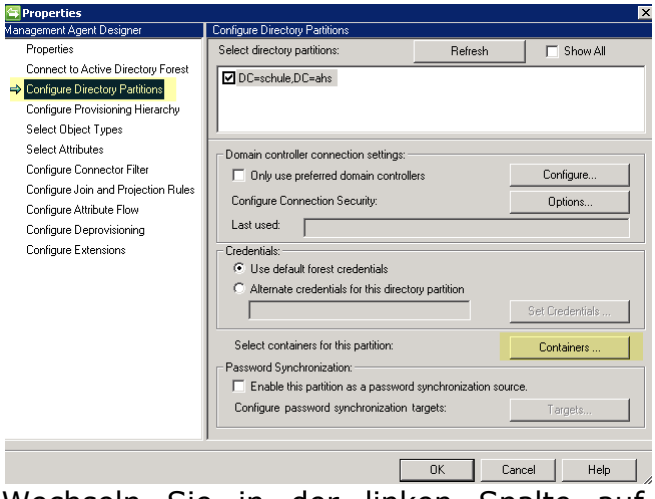
9.3 Konfiguration der Verzeichnissynchronisierung

Wechseln Sie ins Verzeichnis
`C:\Program Files\Windows Azure Active Directory Sync\SYNCBUS\Synchronization Service\UIShell`

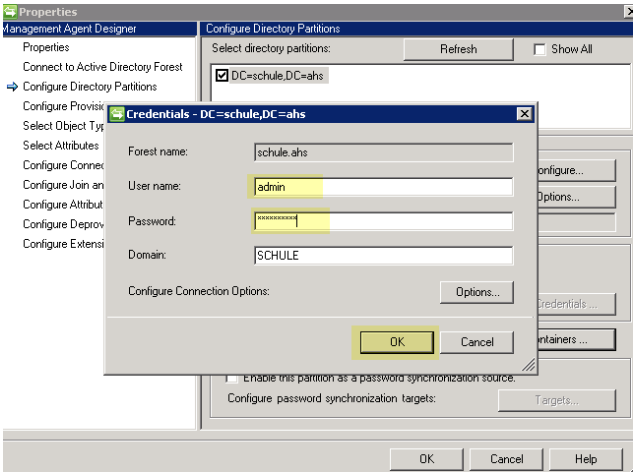
Starten Sie die Anwendung `miisclient.exe`



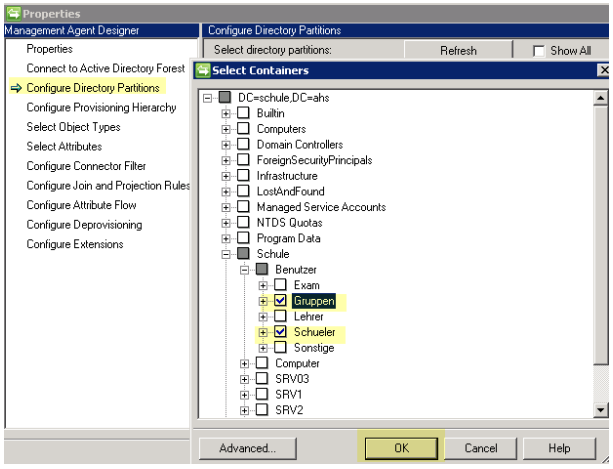
Wechseln Sie ins Register „Management Agents“ und doppelklicken Sie auf „Active Directory Connector“.



Wechseln Sie in der linken Spalte auf „Configure Directory Partitions“.
Klicken Sie auf „Containers“ und →



→ geben Sie die Anmeldeinformationen eines Administrators der Domäne ein.



Definieren Sie die zu synchronisierenden Organisationseinheiten und bestätigen Sie mit OK

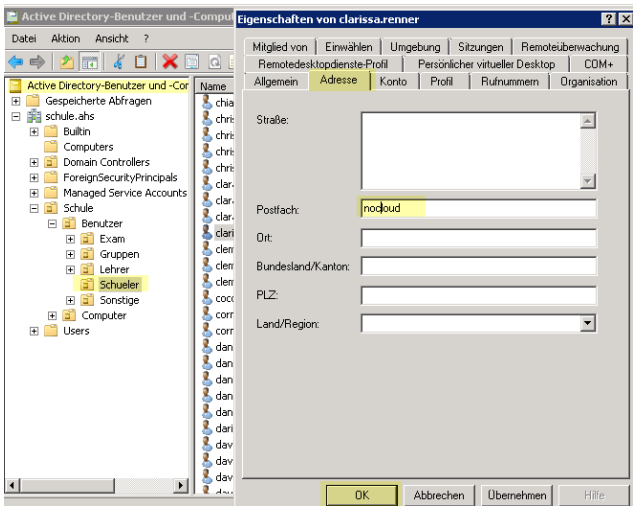
GRUPPEN nicht vergessen!

Vergessen Sie nicht Ihre OU mit Ihren Sicherheitsgruppen (grpSchueler, grpLehrer …)

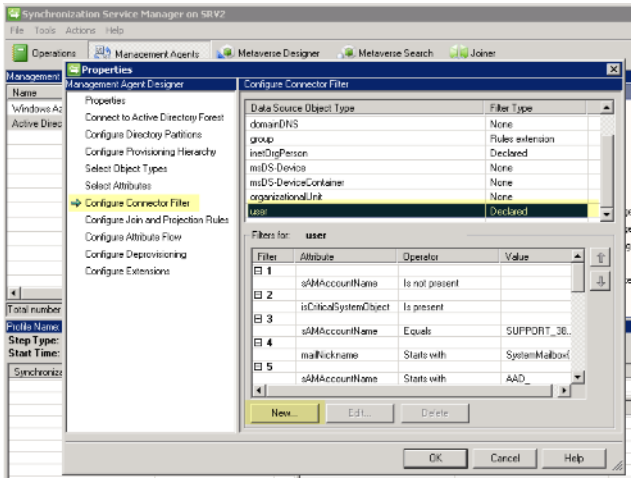
Aktuell sind die LehrerInnen noch nicht Teil des Office365 Agreements. Darum synchronisiere ich sie hier noch nicht.

Eventuell möchten SchülerInnen nicht im Microsoft Azure Directory veröffentlicht werden und verweigern diese gratis Dienste. Wir definieren eine Filterregel, die es uns ermöglicht SchülerInnen von der Synchronisation auszuschließen. Im „Active Directory-Benutzer und Computer" tragen wir diesen SchülerInnen später (aber vor der Synchronisation) in ihren Benutzereigenschaften für die Eigenschaft „postOfficeBox den Wert „noclound" ein.

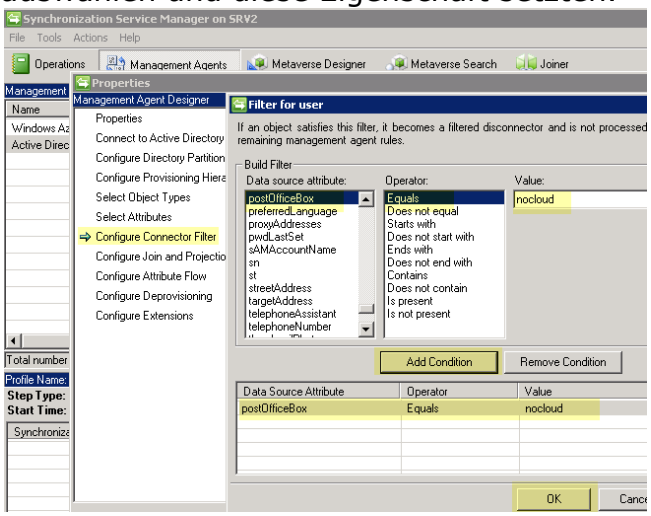
Diese Schülerinnen werden über einen von uns definierten Filter in der Synchronisation nicht berücksichtigt.



Man kann auch mehrere Benutzer auswählen und diese Eigenschaft setzten.



Falls nötig kehren Sie zum „Synchronization Service Manager"



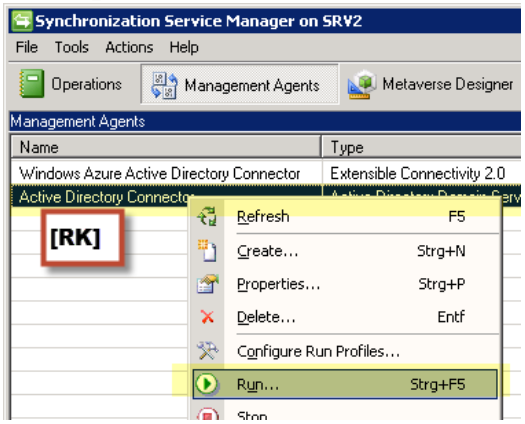
Wählen Sie im linken Bereich PostOffice

zurück. Klicken Sie auf „Configure Connector Filter“

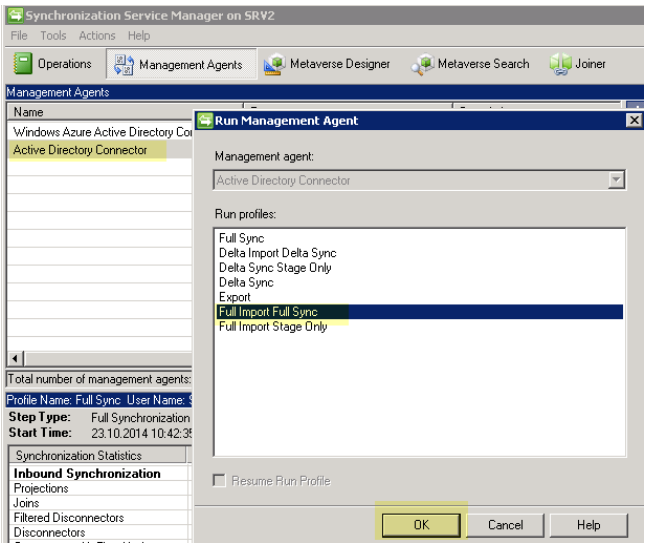
Box, anschließend in der Mitte „ Equals“ und als Value tragen Sie „nocloud“ ein.
Add Condition → OK

9.4 Manuelles Anstoßen der Synchronisierung

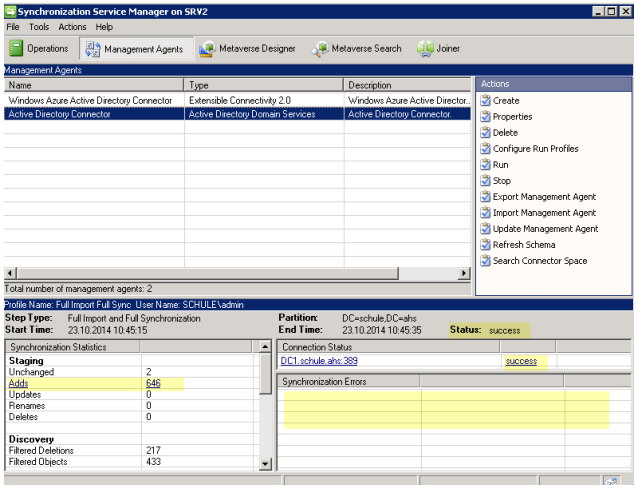
Mit dem alten Synchronization Service Manager
Die Screenshots beziehen sich auf dirsync-de.exe bis ca März 2015
Seit ca April 2015 gibt es einen neuen Synchronization Service Manager, der als Install Datei `dirsync.exe` heißt.



Im Synchronization Service Manager klicken Sie auf die Registerkarte „Management Agents". Rechtsklick auf „**Active Directory Connector**" → Run.

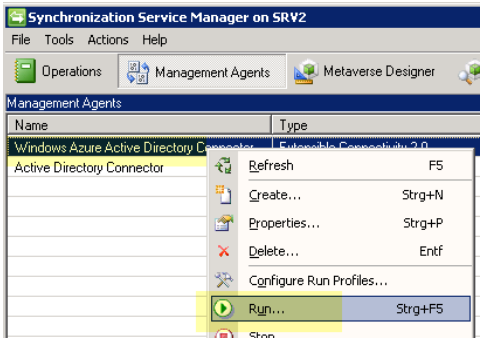


Wählen Sie „**Full Import Full Sync**" und OK

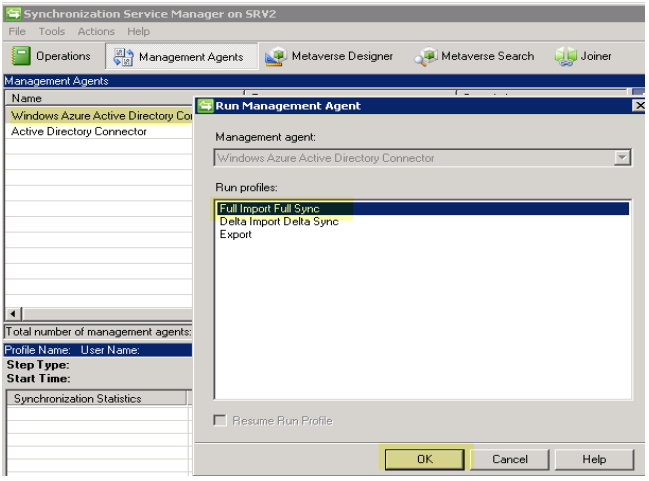


In neueren Versionen (ca April 2015) des Synchronization Service Managers dirsync.exe :

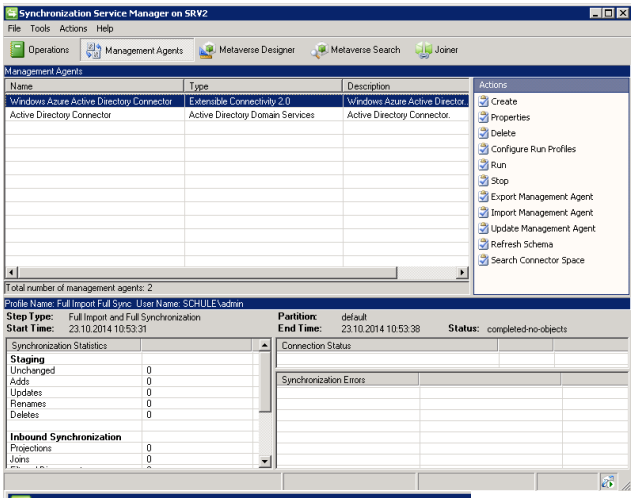
- **Full Import**
- **Full Synchronization**
- **Full Export**



Im Synchronization Service Manager klicken Sie auf die Registerkarte „Management Agents". Rechtsklick auf „**Windows Azure Active Directory Connector**" → Run.

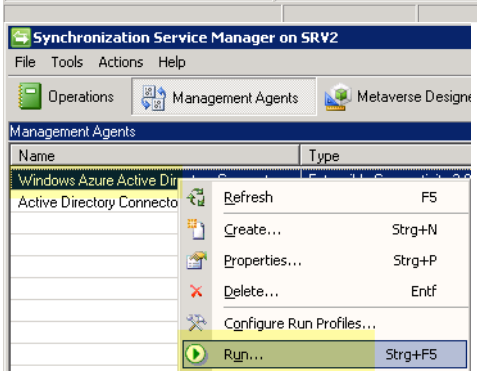


Wählen Sie „**Full Import Full Sync**" und OK

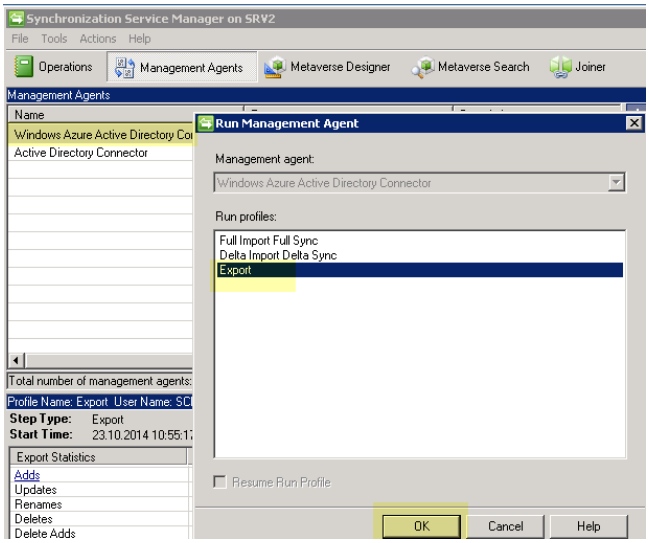


In neueren Version (ca April 2015) des Synchronization Service Managers dirsync.exe :

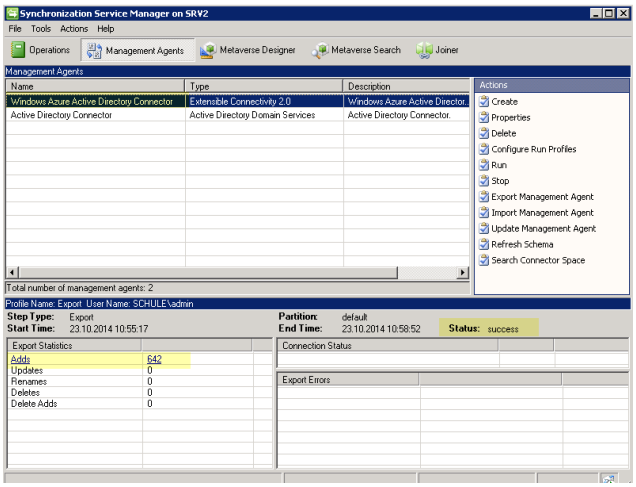
- **Full Import**
- **Full Synchronization**
- **Full Export**



Im Synchronization Service Manager klicken Sie auf die Registerkarte „Management Agents". Rechtsklick auf „**Windows Azure Active Directory Connector**" → Run.



Wählen Sie **Export** und dann OK



PROBLEM: An mehreren Schulen wurde bei den Lehrern die Synchronisation der Passwörter erst nach einer ÄNDERUNG des PASSWORTES initialisiert.
SYNCHRONISIERTE LEHERENDE MÜSSEN DAS PASSWORT ÄNDERN.
Das neue Passwort kann mit dem alten identisch sein, wenn in der Default Domain Policy die Passwortchronik deaktiviert (auf 0 gesetzt) ist
Warten Sie einige Minuten, bis das Passwort aus Ihrer Domäne mit der Azure Domäne synchronisiert wurde.

10 Verwalten von Personen, die Office 365-Gruppen erstellen können

Quelle: https://docs.microsoft.com/de-de/office365/admin/create-groups/manage-creation-of-groups?view=o365-worldwide

Weil es für Benutzer so einfach ist, Office 365-Gruppen selbst zu erstellen, werden Sie vermutlich nicht mit Bitten überflutet, diese Gruppen im Auftrag anderer Personen zu erstellen. Je nach Ihrem Unternehmen möchten Sie jedoch steuern, welche Personen die Möglichkeit zum Erstellen von Gruppen haben sollen.
Hier soll einer Sicherheitsgruppe grpLehrer das Recht erteilt werden Gruppen in Office365 anzulegen. Diese Sicherheitsgruppe wurde aus dem lokalen Active Directory ihrer lokalen Domäne in ihren Office365 Tennant synchronisiert. Alternativ könnten Sie eine separate Sicherheitsgruppe anlegen mit Personen, die Office365 Gruppen erstellen dürfen.

- Outlook
- SharePoint
- Yammer
- Microsoft Teams
- StaffHub
- Planner
- PowerBI
- Roadmap

Sie können Office 365 Gruppenerstellung auf die Mitglieder einer bestimmten Sicherheitsgruppe beschränken. Um dies zu konfigurieren, verwenden Sie Windows PowerShell. In diesem Artikel werden die erforderlichen Schritte erläutert.
Die Schritte in diesem Artikel verhindern nicht, dass Mitglieder bestimmter Rollengruppen erstellen. Office 365 globale Administratoren können Gruppen über beliebige Mittel erstellen, beispielsweise das Microsoft 365 Admin Center, den Planer, Teams, Exchange und SharePoint Online. Andere Rollen können Gruppen mit begrenzten Mitteln erstellen, die unten aufgeführt sind.

- Exchange-Administrator: Exchange Admin Center, Azure AD
- Partner Tier1-Unterstützung: Microsoft 365 Admin Center, Exchange Admin Center, Azure AD
- Partner Tier2-Unterstützung: Microsoft 365 Admin Center, Exchange Admin Center, Azure AD
- Verzeichnis Autoren: Azure AD
- SharePoint-Administrator: SharePoint Admin Center, Azure AD
- Teams-Dienst Administrator: Teams Admin Center, Azure AD
- Benutzer Verwaltungs Administrator: Microsoft 365 Admin Center, Azure AD

Wenn Sie Mitglied einer dieser Rollen sind, können Sie Office 365-Gruppen für Benutzer mit eingeschränktem Zugriff erstellen und anschließend den Benutzer als Besitzer der Gruppe zuweisen.

Lizenzierungsanforderungen
Um zu verwalten, wer Gruppen erstellt, benötigen die folgenden Personen Azure AD Premium-Lizenzen oder Azure AD grundlegende edu-Lizenzen, die Ihnen zugewiesen sind:

- Der Administrator, der diese Gruppen Erstellungseinstellungen konfiguriert
- Die Mitglieder der Sicherheitsgruppe, die Gruppen erstellen dürfen

Die folgenden Personen benötigen keine Azure AD Premium-oder Azure AD Basic edu-Lizenzen, die Ihnen zugewiesen sind:

- Personen, die Mitglied Office 365 Gruppen sind und nicht in der Lage sind, andere Gruppen zu erstellen.

10.1 Bereiten sie das Script Office365Gruppen.ps1 vor

Kopieren Sie diesen Code in eine Textdatei Office365Gruppen.ps1
Passen Sie die Variable $GroupName an eine Ihrer Sicherheitsgruppen an, die Sie ins Office365 synchronisieren.

```
$GroupName = "grpLehrer"
$AllowGroupCreation = "False"

Connect-AzureAD

$settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id
if(!$settingsObjectID)
{
      $template = Get-AzureADDirectorySettingTemplate | Where-object {$_.displayname -eq "group.unified"}
    $settingsCopy = $template.CreateDirectorySetting()
    New-AzureADDirectorySetting -DirectorySetting $settingsCopy
    $settingsObjectID = (Get-AzureADDirectorySetting | Where-object -Property Displayname -Value "Group.Unified" -EQ).id
}

$settingsCopy = Get-AzureADDirectorySetting -Id $settingsObjectID
$settingsCopy["EnableGroupCreation"] = $AllowGroupCreation

if($GroupName)
{
    $settingsCopy["GroupCreationAllowedGroupId"] = (Get-AzureADGroup -SearchString $GroupName).objectid
}

Set-AzureADDirectorySetting -Id $settingsObjectID -DirectorySetting $settingsCopy

(Get-AzureADDirectorySetting -Id $settingsObjectID).Values
```

10.2 In einer Administrativen Powershell

auf einem Windows Server 2016 mit den installierten Azure Tools
oder wie im Beispiel unten auf einem Windows10 1903 Rechner

Ich habe hier die Installation abgebildet, wie sie bei mir funktionierte. Eventuell haben Sie andere Versionen der Module AzureADPreview etc.
Alle meine Eingaben sind hier fett und rot.

Für eine umfassende Anleitung gehen Sie auf
https://docs.microsoft.com/de-de/office365/admin/create-groups/manage-creation-of-groups?view=o365-worldwide

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

Lernen Sie das neue plattformübergreifende PowerShell kennen – https://aka.ms/pscore6
PS C:\WINDOWS\system32> Install-Module -Name AzureADPreview -RequiredVersion 2.0.2.5
Der NuGet-Anbieter ist erforderlich, um den Vorgang fortzusetzen.
PowerShellGet erfordert die NuGet-Anbieterversion 2.8.5.201 oder höher für die Interaktion mit NuGet-basierten
Repositorys. Der NuGet-Anbieter muss in "C:\Program Files\PackageManagement\ProviderAssemblies" oder
"C:\Users\Admin\AppData\Local\PackageManagement\ProviderAssemblies" verfügbar sein. Sie können den
NuGet-Anbieter auch
durch Ausführen von 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'
installieren. Möchten Sie
den NuGet-Anbieter jetzt durch PowerShellGet installieren und importieren lassen?
[J] Ja  [N] Nein  [H] Anhalten  [?] Hilfe (Standard ist "J"): j

Nicht vertrauenswürdiges Repository
Sie installieren die Module aus einem nicht vertrauenswürdigen Repository. Wenn Sie diesem Repository
vertrauen, ändern
 Sie dessen InstallationPolicy-Wert, indem Sie das Set-PSRepository-Cmdlet ausführen. Möchten Sie die
Module von
'PSGallery' wirklich installieren?
[J] Ja  [A] Ja, alle  [N] Nein  [K] Nein, keine  [H] Anhalten  [?] Hilfe (Standard ist "N"): j
```

Führen Sie das Script aus und melden Sie sich mit Ihrem Office365 Administratorkonto an, wenn Sie dazu aufgefordert werden.

```
PS C:\WINDOWS\system32> cd\
PS C:\> cd _mist
PS C:\_mist> .\Office365Gruppen.ps1
.\Office365Gruppen.ps1 : Die Datei "C:\_mist\Office365Gruppen.ps1" kann nicht geladen werden, da die
Ausführung von
Skripts auf diesem System deaktiviert ist. Weitere Informationen finden Sie unter
"about_Execution_Policies"
(https:/go.microsoft.com/fwlink/?LinkID=135170).
In Zeile:1 Zeichen:1
+ .\Office365Gruppen.ps1
+ ~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : Sicherheitsfehler: (:) [], PSSecurityException
    + FullyQualifiedErrorId : UnauthorizedAccess
PS C:\_mist> Set-ExecutionPolicy RemoteSigned

Ausführungsrichtlinie ändern
Die Ausführungsrichtlinie trägt zum Schutz vor nicht vertrauenswürdigen Skripts bei. Wenn Sie die
Ausführungsrichtlinie
 ändern, sind Sie möglicherweise den im Hilfethema "about_Execution_Policies" unter
"https:/go.microsoft.com/fwlink/?LinkID=135170" beschriebenen Sicherheitsrisiken ausgesetzt. Möchten
Sie die
Ausführungsrichtlinie ändern?
[J] Ja  [A] Ja, alle  [N] Nein  [K] Nein, keine  [H] Anhalten  [?] Hilfe (Standard ist "N"): j
PS C:\_mist> .\Office365Gruppen.ps1

Account                   Environment TenantId                            TenantDomain AccountType
-------                   ----------- --------                            ------------ -----------
admin@bgbr.onmicrosoft.com AzureCloud  ec5846b8-a48f-473b-bc11-1cec9d5e681a bg-gallus.at User

Id          : d5c43779-344b-4cf2-8703-8b29858238b2
DisplayName :
TemplateId  : 62375ab9-6b52-47ed-826b-58e47e0e304b
Values      : {class SettingValue {
                Name: EnableMIPLabels
                Value: False
              }
              , class SettingValue {
                Name: CustomBlockedWordsList
                Value:
              }
              , class SettingValue {
                Name: EnableMSStandardBlockedWords
                Value: False
              }
              , class SettingValue {
                Name: ClassificationDescriptions
                Value:
              }
              ...}
Name  : EnableMIPLabels
Value : False
Name  : CustomBlockedWordsList
Value :
Name  : EnableMSStandardBlockedWords
Value : False
Name  : ClassificationDescriptions
Value :
Name  : DefaultClassification
Value :
Name  : PrefixSuffixNamingRequirement
Value :
Name  : AllowGuestsToBeGroupOwner
Value : False
Name  : AllowGuestsToAccessGroups
Value : True
Name  : GuestUsageGuidelinesUrl
Value :
Name  : GroupCreationAllowedGroupId
Value : cdf5327f-4f92-4d7f-a430-0e217ab2c22b
Name  : AllowToAddGuests
Value : True
Name  : UsageGuidelinesUrl
Value :
Name  : ClassificationList
Value :
Name  : EnableGroupCreation
Value : False
```

Für eine umfassende Anleitung gehen Sie auf
https://docs.microsoft.com/de-de/office365/admin/create-groups/manage-creation-of-groups?view=o365-worldwide

Schritt 1: Erstellen einer Sicherheitsgruppe für Benutzer, die Office 365-Gruppen erstellen müssen
Nur eine Sicherheitsgruppe in Ihrer Organisation kann verwendet werden, um zu steuern, wer Gruppen erstellen kann. Sie können jedoch andere Sicherheitsgruppen als Mitglieder dieser Gruppe schachteln. Beispiel: Die Gruppe namens "Gruppenerstellung zulassen" ist die designierte Sicherheitsgruppe, und die Gruppen namens "Microsoft Planner-Benutzer" und "Exchange Online-Benutzer" sind Mitglieder dieser Gruppe.
Administratoren in den oben aufgeführten Rollen müssen nicht Mitglieder dieser Gruppe sein: Sie behalten ihre Fähigkeit, Gruppen zu erstellen.

Wichtig

Achten Sie darauf, mit einer Sicherheitsgruppe einzuschränken, wer Gruppen erstellen kann. Dann können Mitglieder nämlich keine Gruppe auf SharePoint erstellen, weil dort auf eine Sicherheitsgruppe überprüft wird.

1. Wechseln Sie im Admin Center zur Seite Gruppen > Gruppen.
2. Wählen Sie Sicherheit als Gruppentyp aus. Vergessen Sie nicht den Namen der Gruppe! Sie benötigen ihn später noch.
3. Schließen Sie die Einrichtung der Sicherheitsgruppe ab, und fügen Sie Personen oder andere Sicherheitsgruppen hinzu, die in Ihrer Organisation Gruppen erstellen können sollen.

Ausführliche Anweisungen finden Sie unter erstellen, bearbeiten oder Löschen einer Sicherheitsgruppe im Microsoft 365 Admin Center.
Schritt 2: Installieren der Vorschauversion von Azure Active Directory PowerShell für Graph
Für diese Verfahren ist die Vorschauversion von Azure Active Directory PowerShell für Graph erforderlich. Die GA-Version kann nicht verwendet werden.

Wichtig

Sie können nicht gleichzeitig die Versionen Preview und GA auf demselben Computer installieren. Sie können das Modul unter Windows 10, Windows Server 2016, installieren.
Als bewährte Methode empfehlen wir, *immer* die neueste Version zu verwenden: Deinstallieren Sie die alte AzureADPreview- bzw. AzureAD-Version, und holen Sie sich die aktuellste Version.

1. Geben Sie in der Suchleiste Windows PowerShell ein.
2. Klicken Sie mit der rechten Maustaste auf Windows PowerShell, und klicken Sie dann auf Als Administrator ausführen.

3. Überprüfen Sie das installierte Modul:

- `Get-InstalledModule -Name "AzureAD*"`
- Führen Sie zum Deinstallieren einer früheren Version von AzureADPreview oder AzureAD diesen Befehl aus:

```
Uninstall-Module AzureADPreview
```

oder

- `Uninstall-Module AzureAD`
- To install the latest version of AzureADPreview, run this command:

```
5. Install-Module AzureADPreview
```

6. At the message about an untrusted repository, type Y. It will take a minute or so for the new module to install.

Lassen Sie das PowerShell-Fenster für Schritt 3, unten geöffnet.

Schritt 3: Ausführen von PowerShell-Befehlen

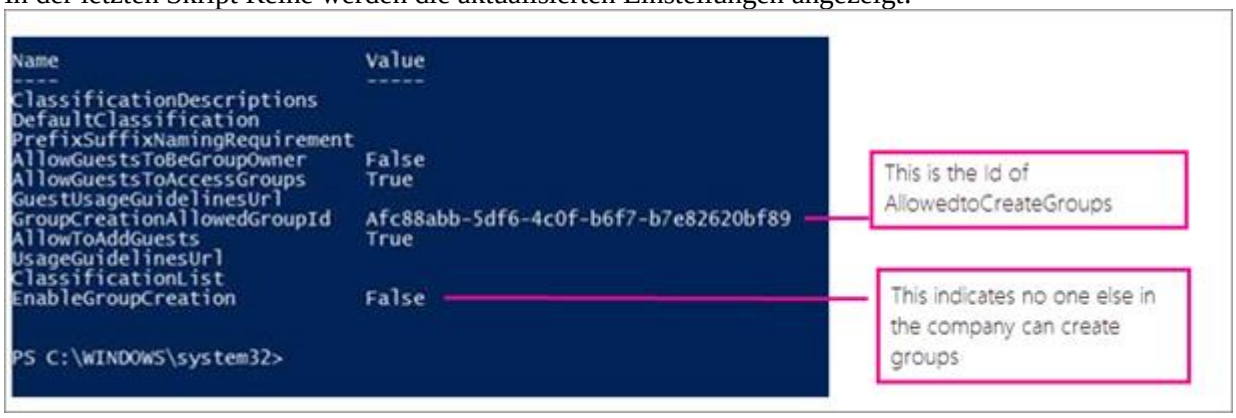
Kopieren Sie das Skript unten in einen Text-Editor wie Notepad oder die Windows PowerShell ISE.
Ersetzen * <Sie> SecurityGroupName* durch den Namen der Sicherheitsgruppe, die Sie erstellt haben. Beispiel:

```
$GroupName = "Group Creators"
```

Speichern Sie die Datei als GroupCreators. ps1.
Navigieren Sie im PowerShell-Fenster zu dem Speicherort, an dem Sie die Datei gespeichert haben (geben Sie "CD" ein).
Führen Sie das Skript aus, indem Sie Folgendes eingeben:

```
.\GroupCreators.ps1
```

und melden Sie sich mit Ihrem Administratorkonto an, wenn Sie dazu aufgefordert werden.
PowerShell
In der letzten Skript Reihe werden die aktualisierten Einstellungen angezeigt:



Wenn Sie in Zukunft die verwendete Sicherheitsgruppe ändern möchten, können Sie das Skript mit dem Namen der neuen Sicherheitsgruppe erneut ausführen.
Wenn Sie die Einschränkung für die Gruppenerstellung deaktivieren und allen Benutzern erneut das Erstellen von Gruppen gestatten `$GroupName` möchten, legen Sie `$AllowGroupCreation` auf "" und auf "true" fest, und führen Sie das Skript erneut aus.

Schritt 4: Überprüfen der Funktionsweise

1. Melden Sie sich bei Office 365 mit dem Benutzerkonto einer Person an, die NICHT die Möglichkeit zum Erstellen von Gruppen haben soll. Dies bedeutet, dass es sich nicht um ein Mitglied der von Ihnen erstellten Sicherheitsgruppe oder eines Administrators handelt.
2. Wählen Sie die Kachel Planer aus.
3. Wählen Sie in Planer im linken Navigationsbereich den neuen Plan aus, um einen Plan zu erstellen.
4. Sie sollten eine Meldung erhalten, dass die Planung und Gruppenerstellung deaktiviert ist.

Versuchen Sie erneut, dasselbe Verfahren mit einem Mitglied der Sicherheitsgruppe auszuführen.

Hinweis

Wenn Mitglieder der Sicherheitsgruppe keine Gruppen erstellen können, stellen Sie sicher, dass Sie nicht durch ihre OWA-Postfachrichtlinieblockiert werden.

11 Windows Management Framework 5.1 für Windows Server 2008R2

Download
https://www.microsoft.com/en-us/download/details.aspx?id=54616
Installation braucht Zeit und der Computer braucht einen Neustart.

Open an elevated Windows PowerShell 64Bit command prompt (run Windows PowerShell as an administrator).

```
PS C:\Windows\system32> $PSVersionTable

Name                           Value
----                           -----
PSVersion                      5.1.14409.1005
PSEdition                      Desktop
PSCompatibleVersions           {1.0, 2.0, 3.0, 4.0...}
BuildVersion                   10.0.14409.1005
CLRVersion                     4.0.30319.36543
WSManStackVersion              3.0
PSRemotingProtocolVersion      2.3
SerializationVersion           1.1.0.1

    Run the Install-Module MSOnline command.
PS C:\Windows\system32> Install-Module -Name MSOnline
man muss mit Y und A bestätigen.
Die roten Fehlermeldungen zeigen mit welchen Parametern installiert werden muss
zB -FORCE und später ein weiterer Parameter

PS C:\Windows\system32> Install-Module -Name AzureAD

 [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Susp
PS C:\Windows\system32> Import-Module AzureAD
PS C:\Windows\system32> Get-Module -Name AzureAD

Versionen der Module:

ModuleType Version    Name
---------- -------    ----
Binary     2.0.2.52   AzureAD

PS C:\Windows\system32> Import-Module MSonline
PS C:\Windows\system32> get-module -name msonline

ModuleType Version    Name
---------- -------    ----
Manifest   1.1.183.17 MSonline

PS C:\Windows\system32>
```

12 EnableSoftMatchOnUpn

Führte zu gravierenden Synchronisationsproblemen:
Losung : Nicht machen!!
Ändern Sie die UPN des Dirsyn Service Accounts mit Hilfe von Azure Powershell von Sync_SRV2_b86c2ab5cfc2@bg-gallus.at zu Sync_SRV2_b86c2ab5cfc2@bgbr.onmicrosoft.com

Im Windows Azure Active Directory-Modul für Windows PowerShell

~~Set-MsolDirSyncFeature -Feature EnableSoftMatchOnUpn -Enable $True~~

Dieser Befehl ist irreversible und ich würde ihn nicht machen!!