FERMILAB-SLIDES-18-104-CD

Fermilab

Managed by Fermi Research Alliance, LLC for the U.S. Department of Energy Office of Science

Office 365 Integration At Fermilab

Al Lilianstrom

National Laboratories Information Technology Summit

May 2015

This manuscript has been authored by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy, Office of Science, Office of High Energy Physics.

About Fermilab

- Since 1967, Fermilab has worked to answer fundamental questions and enhance our understanding of everything we see around us. As the United States' premier particle physics laboratory, we work on the world's most advanced particle accelerators and dig down to the smallest building blocks of matter.
- Fermilab collaborates with more than 20 countries on physics experiments based in the United States and elsewhere.
- Fermilab's 6,800-acre site is located in Batavia, Illinois, and is managed by the Fermi Research Alliance LLC for the U.S. Department of Energy Office of Science. FRA is a partnership of the University of Chicago and Universities Research Association Inc., a consortium of 86 research universities.

Abstract

- Fermilab is migrating to Office 365. The initial offering is to provide the Office application to laboratory owned devices - desktops, laptops, and mobile. As the Office 365 licensing model moves from per device to per user the deployment of an authentication infrastructure to allow only authorized use of the application was required. As Fermilab relies on centrally managed authentication services for daily operations the Office 365 authentication had to be integrated into these services.
- This talk will focus on the configuration of the necessary on-premise software to integrate Office 365 with our authentication services, how we are managing the licensing of users, and integration into our future Identity Management service.

Office 365

- Fermilab is a long term user of Microsoft Office
  - Arguably the standard for document processing for desktops

- Existing On Premise Services
  - Exchange
  - SharePoint

- Enterprise Agreement
  - License costs
  - Device vs User

Deployment

- Authentication
  - Microsoft Cloud
  - Federated Identity

- User Provisioning
  - Microsoft Cloud
  - On Premise Active Directory
  - Synchronization between Active Directory and the Microsoft Cloud

Deployment

- Preparation
  - Target users with 5 or less device licenses
  - Provision user accounts
  - Multiple installs available to each user

- Windows
  - System Center Configuration Manager 2007
  - Deploy Click-to-Install version

- OSX
  - Casper 9
  - Delete License File

Authentication

- Microsoft Cloud Account
  - Unique username and password

    user@yourdomain.onmicrosoft.com
    - Onboarding
    - Off-boarding

- Federated Identity
  - Existing username and password

    user@yourdomain
  - Federated Identity Provider required

- Fermilab chose to use Federated Identity
  - Active Directory Federation Services (ADFS)

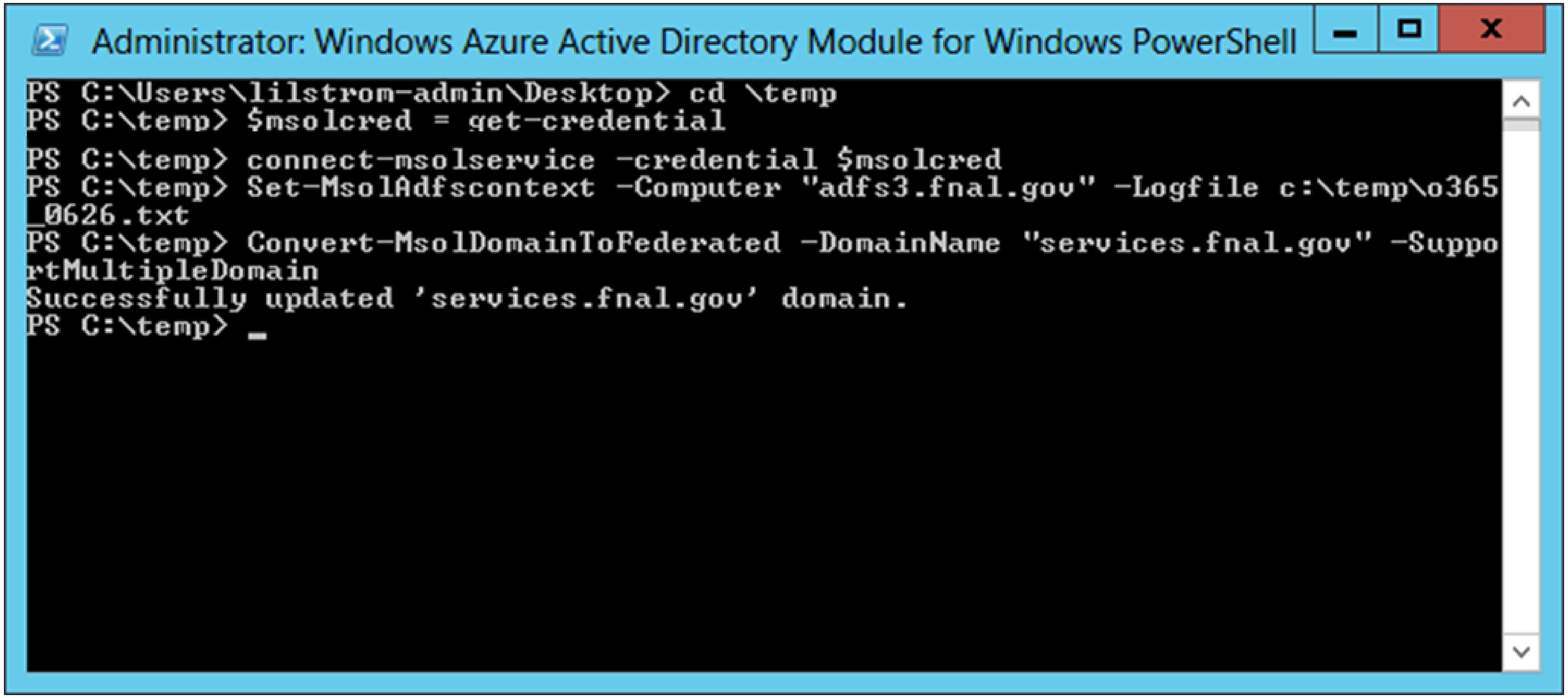
Connection

- Multi-step Process
  - Active Directory (AD) Universal Principal Name (UPN)
    - Will be part of the Office 365 username
    - UPN needs to be added to Office 365
    - Requires DNS record for the UPN domain

      services.fnal.gov text = "MS=ms11931651”
  - “Clean” AD
    - Accounts with duplicate email addresses
  - Install and configure Federation application
      - If necessary
    - Must be the same domain as UPN you are using

Connection

- Connect ADFS to Microsoft Cloud
  - PowerShell
    - – Host not Service name
  - Be Patient
    - – Convert command can take some time

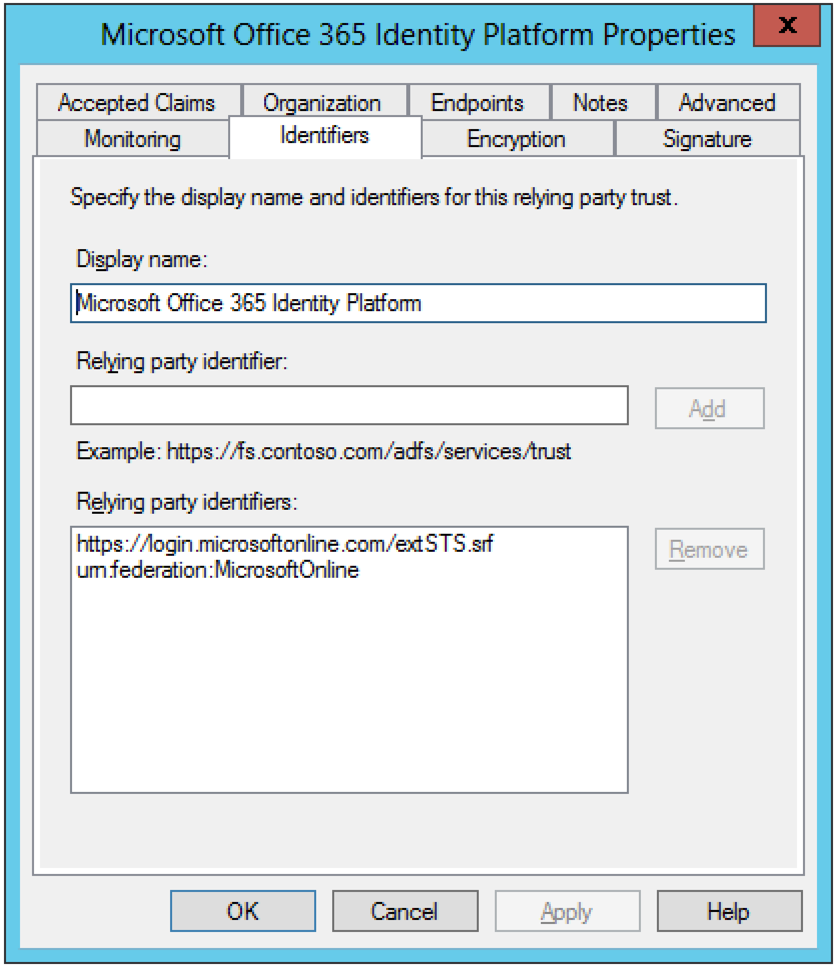


Administrator: Windows Azure Active Directory Module for Windows PowerShell

```
PS C:\Users\lilstrom-admin\Desktop> cd \temp
PS C:\temp> $msolcred = get-credential
PS C:\temp> connect-msolservice -credential $msolcred
PS C:\temp> Set-MsolAdfscontext -Computer "adfs3.fnal.gov" -Logfile c:\temp\o365
_0626.txt
PS C:\temp> Convert-MsolDomainToFederated -DomainName "services.fnal.gov" -Suppo
rtMultipleDomain
Successfully updated 'services.fnal.gov' domain.
PS C:\temp> _
```

Connection

- The Convert command makes a change in the Office Cloud and adds a Relying Party Trust to ADFS



Microsoft Office 365 Identity Platform Properties

Specify the display name and identifiers for this relying party trust.

Display name:

Microsoft Office 365 Identity Platform

Relying party identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers:

https://login.microsoftonline.com/extSTS.srf
urn:federation:MicrosoftOnline

Connection

- Synchronize User Account Information
- Assign Licenses
- Use

Simple

Synchronize

- Special Accounts
  - Cloud Service Account
    - Global Admin
    - Password Expiration
    - No License Required
  - Active Directory Service Account
    - Created as part of Windows Azure Active Directory Sync tool install
    - No Elevated Access
  - Cloud Admin Accounts
    - Recommended

Synchronize

- Synchronize User Account Information
  - Activate in Office 365
  - Install Windows Azure Active Directory Sync
    - Requires .Net 3

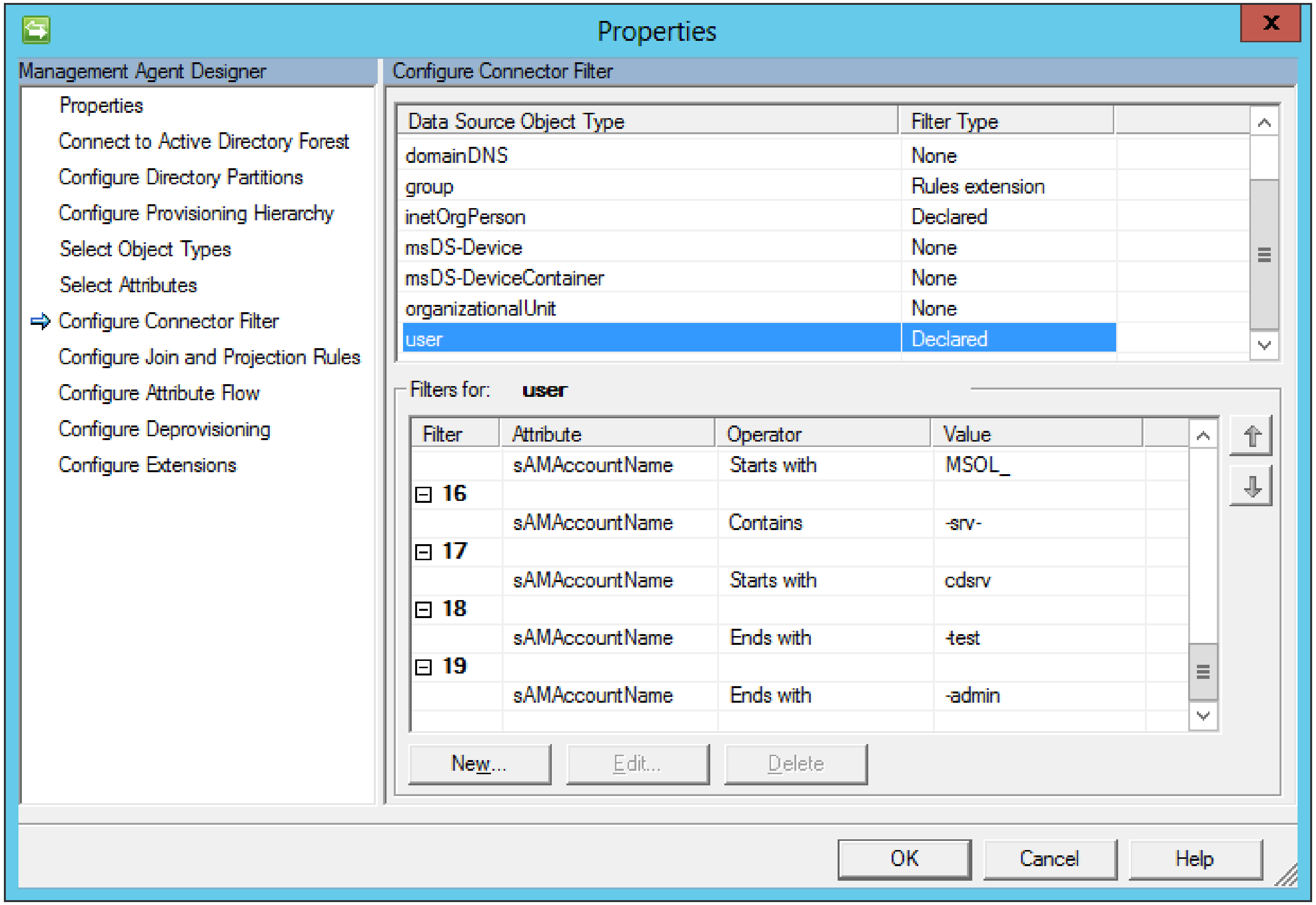
      dism /online /enable-feature /featurename:NETFX3 /all /source:DRIVE:\sources\sxs /limitaccess
  - Only synchronize what you need to the cloud
    - OU based filters
      - http://blogs.msdn.com/b/denotation/archive/2012/11/21/installing-and-configure-dirsync-with-ou-level-filtering-for-office365.aspx
  - Don’t synchronize passwords

Synchronize

- Synchronization Service Manager Client
  - Debugging information
  - Manually sync AD to Cloud
- Sync Schedule
  - Default is every 3 hours
  - Easy to change
    - Edit C:\Program Files\Windows Azure Active Directory Sync\Microsoft.Online.DirSync.Scheduler.exe.Config
    - Change <add key="SyncTimeInterval" value="3:0:0" /> to the necessary value
    - Save the file
    - Restart the Windows Azure Active Directory Sync Service
- Filters

Synchronize

- User based filters
  - In the Synchronization Service Manager Client



Properties

Management Agent Designer

- Properties
- Connect to Active Directory Forest
- Configure Directory Partitions
- Configure Provisioning Hierarchy
- Select Object Types
- Select Attributes
- ⇨ Configure Connector Filter
- Configure Join and Projection Rules
- Configure Attribute Flow
- Configure Deprovisioning
- Configure Extensions

Configure Connector Filter

Data Source Object Type	Filter Type
domainDNS	None
group	Rules extension
inetOrgPerson	Declared
msDS-Device	None
msDS-DeviceContainer	None
organizationalUnit	None
user	Declared

Filters for: **user**

Filter	Attribute	Operator	Value
	sAMAccountName	Starts with	MSOL_
⊟ **16**			
	sAMAccountName	Contains	-srv-
⊟ **17**			
	sAMAccountName	Starts with	cdsrv
⊟ **18**			
	sAMAccountName	Ends with	-test
⊟ **19**			
	sAMAccountName	Ends with	-admin

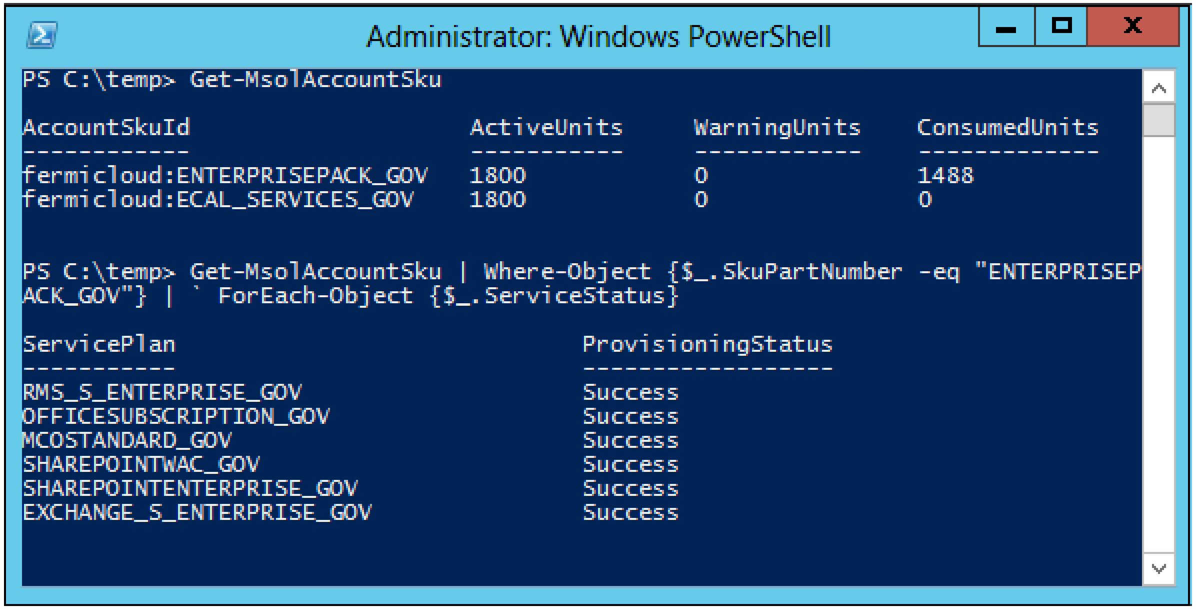
Licensing

- Assign licenses
  - Web Interface
    - Manual process
  - PowerShell Commands
    - Simple

```
PS> get-msoluser -UserPrincipalName user@services.fnal.gov | Set-MsolUserLicense -AddLicense fermicloud:ENTERPRISEPACK_GOV
```

Licensing

- Office 365 Applications



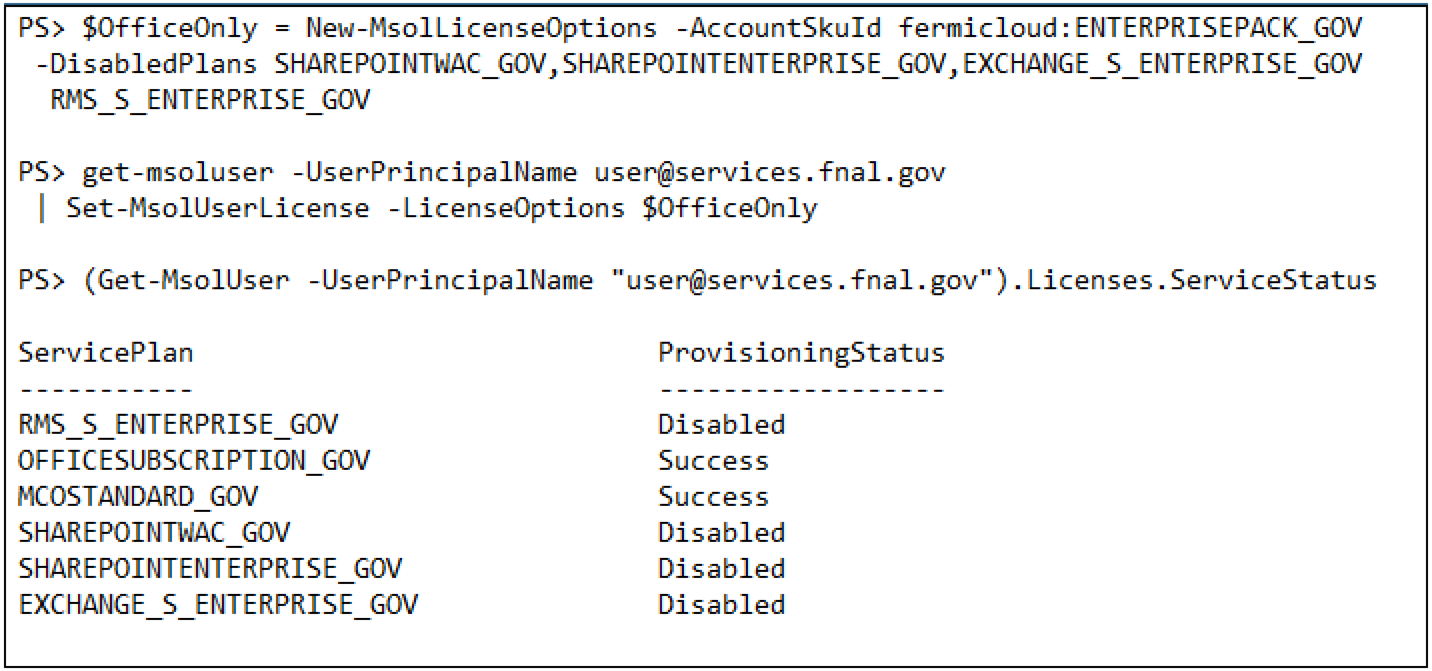
```
PS C:\temp> Get-MsolAccountSku

AccountSkuId                    ActiveUnits     WarningUnits    ConsumedUnits
------------                    -----------     ------------    -------------
fermicloud:ENTERPRISEPACK_GOV   1800            0               1488
fermicloud:ECAL_SERVICES_GOV    1800            0               0


PS C:\temp> Get-MsolAccountSku | Where-Object {$_.SkuPartNumber -eq "ENTERPRISEP
ACK_GOV"} | ` ForEach-Object {$_.ServiceStatus}

ServicePlan                             ProvisioningStatus
-----------                             ------------------
RMS_S_ENTERPRISE_GOV                    Success
OFFICESUBSCRIPTION_GOV                  Success
MCOSTANDARD_GOV                         Success
SHAREPOINTWAC_GOV                       Success
SHAREPOINTENTERPRISE_GOV                Success
EXCHANGE_S_ENTERPRISE_GOV               Success
```

  - Each application can be enabled or disabled per user
  - License management can be automated using AD group membership

    http://365lab.net/2014/04/22/office-365-assign-licenses-based-on-groups-using-powershell-advanced-version/

Licensing

- Our click-to-run licensing



```
PS> $OfficeOnly = New-MsolLicenseOptions -AccountSkuId fermicloud:ENTERPRISEPACK_GOV
 -DisabledPlans SHAREPOINTWAC_GOV,SHAREPOINTENTERPRISE_GOV,EXCHANGE_S_ENTERPRISE_GOV
  RMS_S_ENTERPRISE_GOV

PS> get-msoluser -UserPrincipalName user@services.fnal.gov
 | Set-MsolUserLicense -LicenseOptions $OfficeOnly

PS> (Get-MsolUser -UserPrincipalName "user@services.fnal.gov").Licenses.ServiceStatus

ServicePlan                             ProvisioningStatus
-----------                             ------------------
RMS_S_ENTERPRISE_GOV                    Disabled
OFFICESUBSCRIPTION_GOV                  Success
MCOSTANDARD_GOV                         Success
SHAREPOINTWAC_GOV                       Disabled
SHAREPOINTENTERPRISE_GOV                Disabled
EXCHANGE_S_ENTERPRISE_GOV               Disabled
```

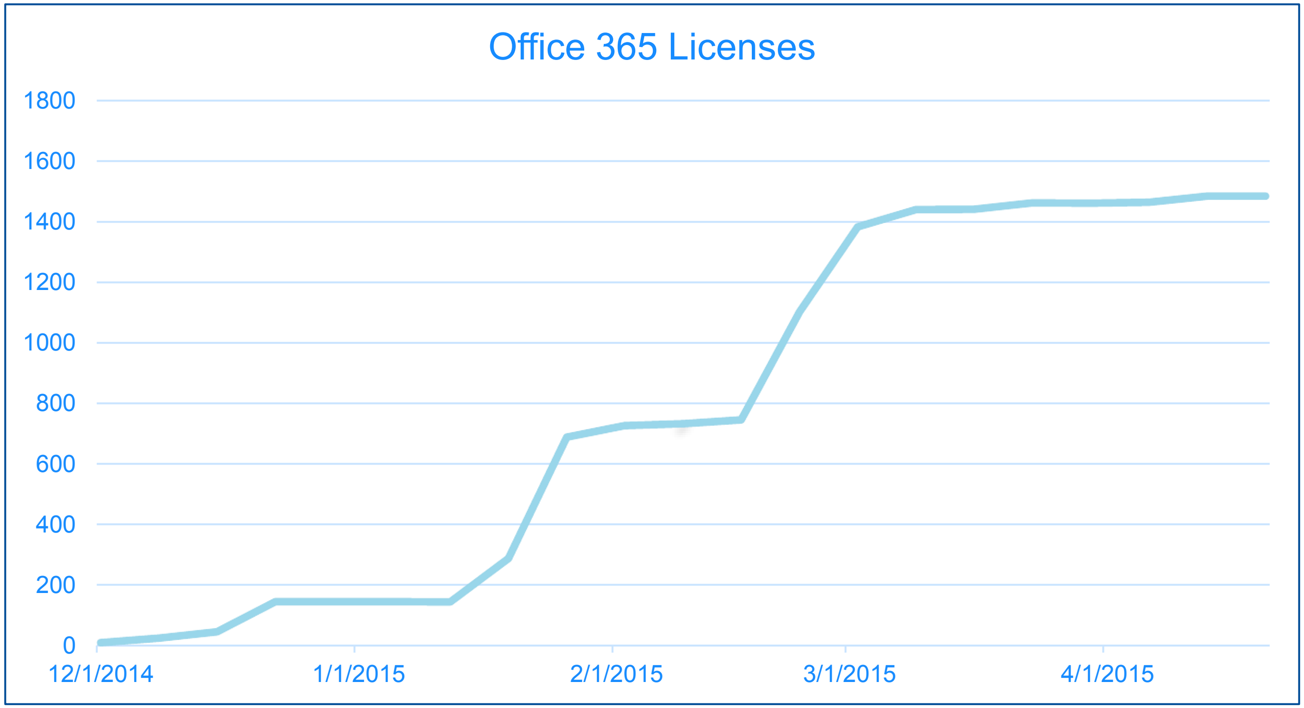
Licensing

- Off-boarding
  - Account deletion
  - OU change
    - Properly defined synchronization rules remove user from Office 365 freeing up the license
  - Script linked above will remove licenses from users once they are removed from the groups

Licensing

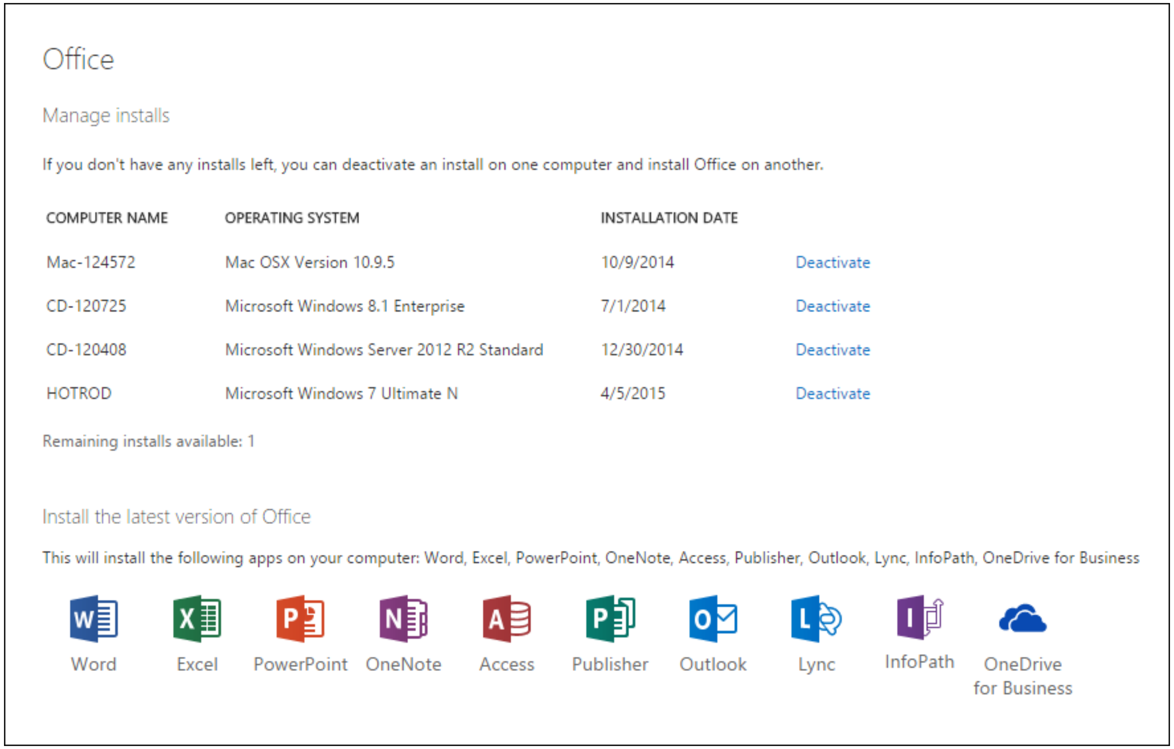
- Usage
  - Per application
    - PowerShell

```
Get-MsolUser -all | Where-Object {$_.Licenses.AccountSkuID -eq "fermicloud:ENTERPRISEPACK_GOV"}|Select DisplayName, UserPrincipalName

Get-MsolAccountsku
```



Licensing

- End user can see how many systems they have Office installed on



Office

Manage installs

If you don't have any installs left, you can deactivate an install on one computer and install Office on another.

COMPUTER NAME	OPERATING SYSTEM	INSTALLATION DATE	
Mac-124572	Mac OSX Version 10.9.5	10/9/2014	Deactivate
CD-120725	Microsoft Windows 8.1 Enterprise	7/1/2014	Deactivate
CD-120408	Microsoft Windows Server 2012 R2 Standard	12/30/2014	Deactivate
HOTROD	Microsoft Windows 7 Ultimate N	4/5/2015	Deactivate

Remaining installs available: 1

Install the latest version of Office

This will install the following apps on your computer: Word, Excel, PowerPoint, OneNote, Access, Publisher, Outlook, Lync, InfoPath, OneDrive for Business

- Office 365 admins are unable to query Office 365 and see how many installs each authorized used has used

Identity Management

- Roles
  - Group membership for Office 365 application licensing
    - Easily integrated with IdM applications
  - Our Goal
    - IDM role assignment enables each Office 365 application as necessary

Office 365

- Next Steps
  - OneDrive
  - Lync
  - Exchange Online
  - SharePoint Online
    - With group managed access each online application can be deployed in an orderly manner

Lessons Learned

- Federated Access to Office 365 allows for a known password to access the application
  - Is this password 'approved' for web applications?

- Think about what users in your AD need to be in the cloud

- Automate the (de)provisioning of users
  - Integration into IdM
  - License recovery
  - Automation leads to relaxation

Questions

- Al Lilianstrom
  - lilstrom@fnal.gov

Special thanks to Quinton Healy, Desktop Engineering Group Leader at Fermilab, for his valuable input to this presentation