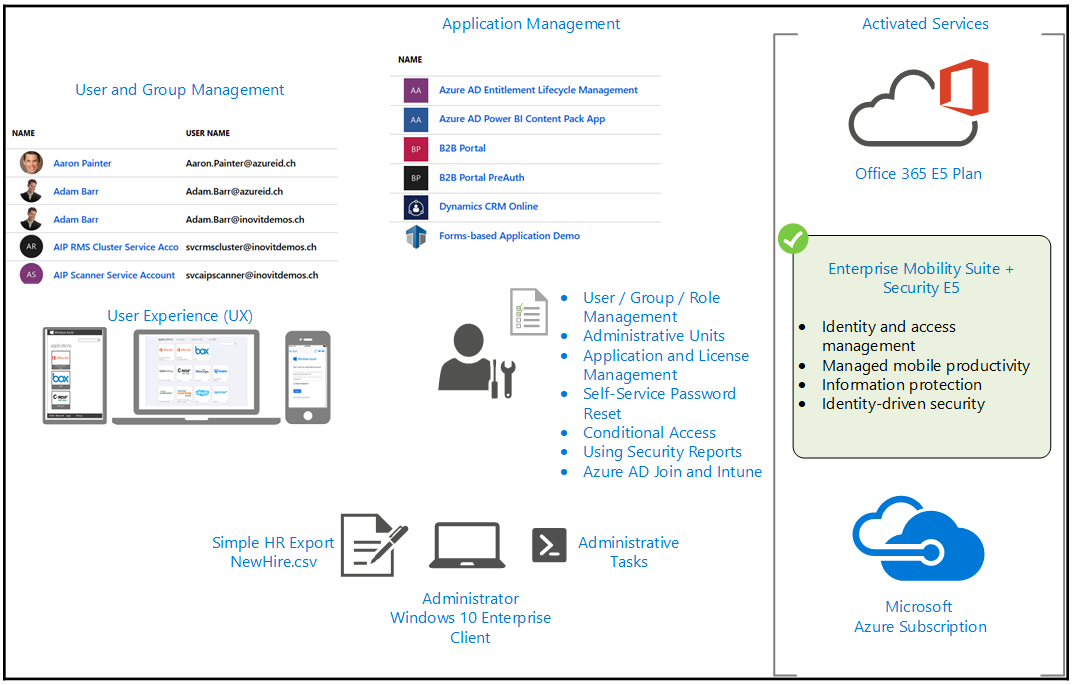
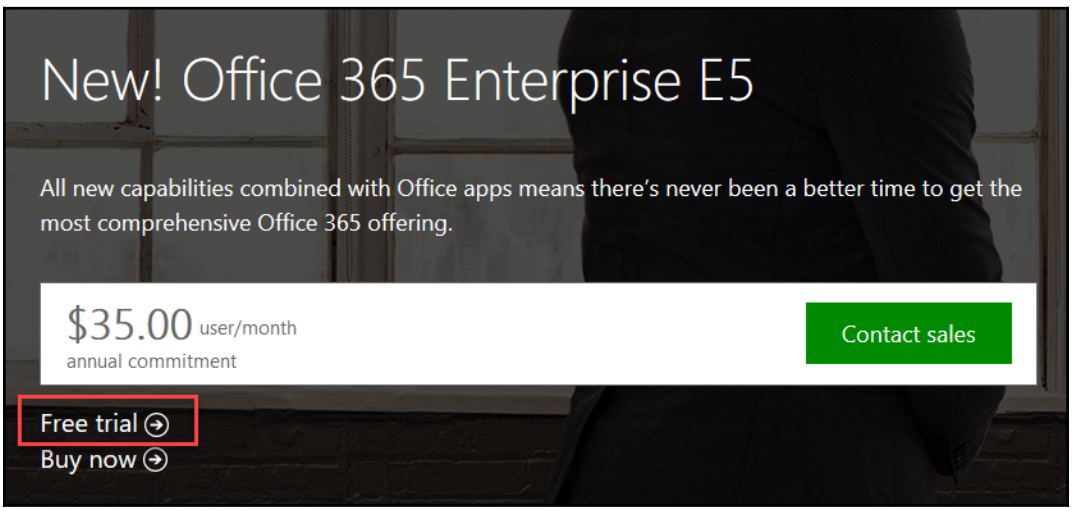
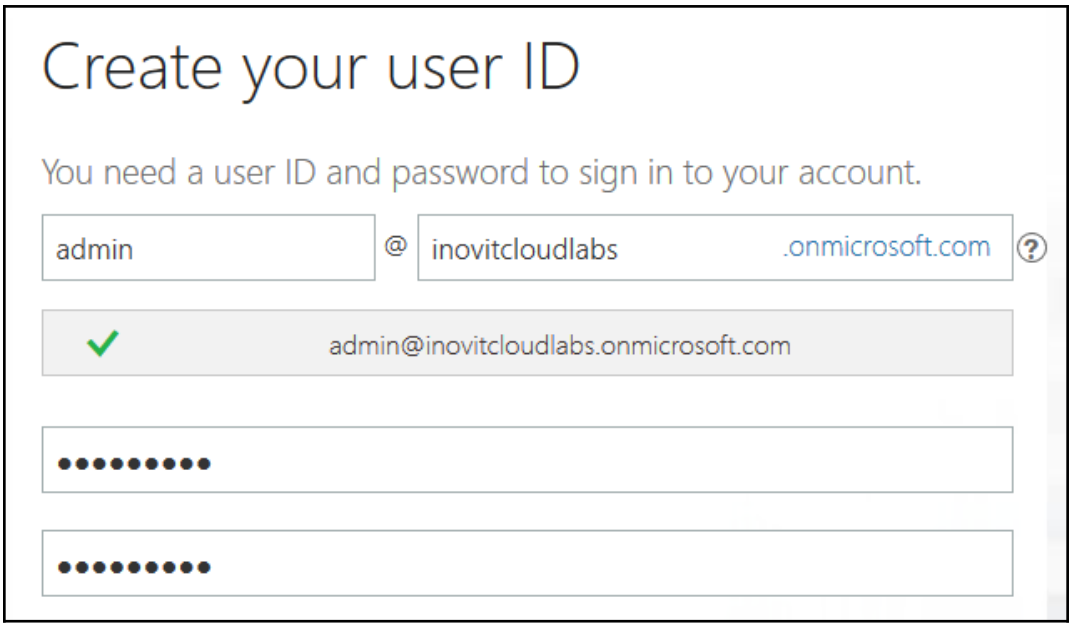
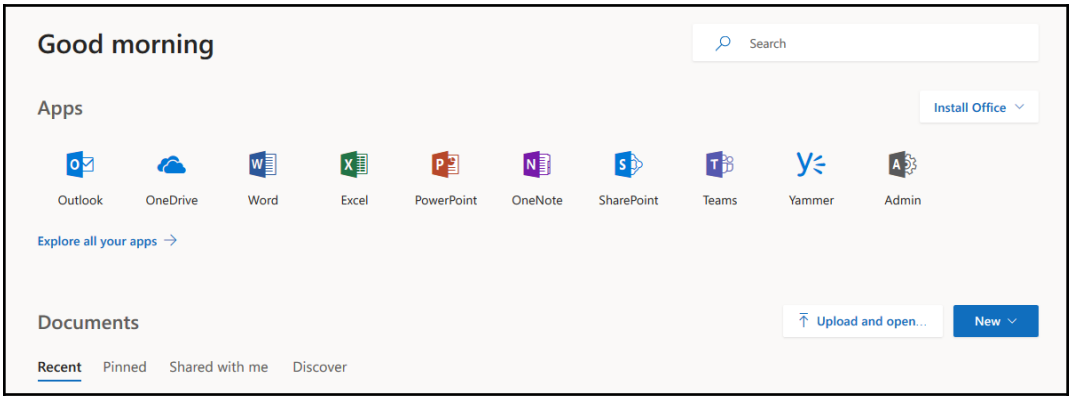
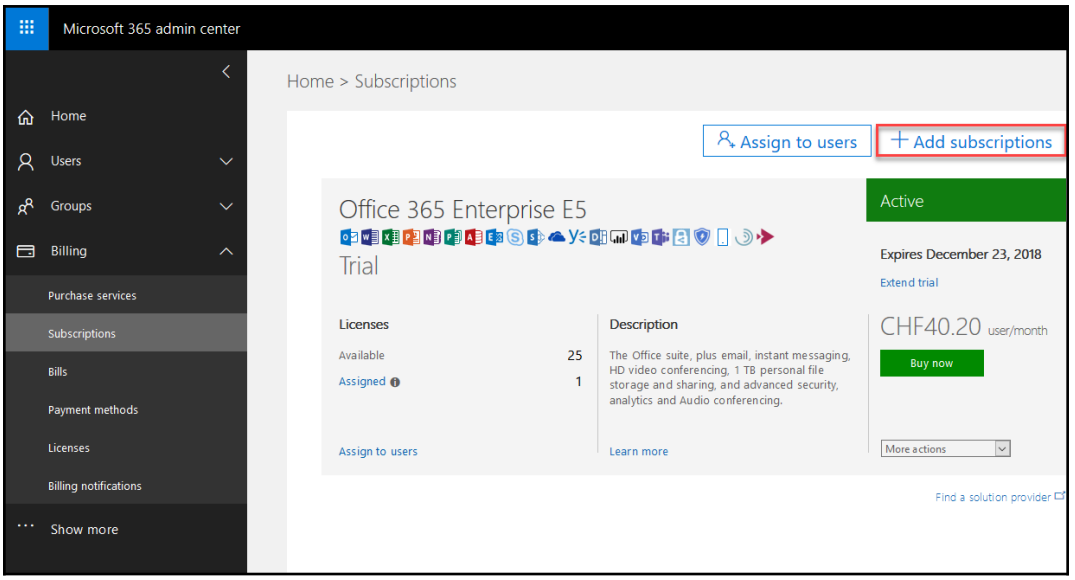
Chapter 1: Building and Managing Azure Active Directory

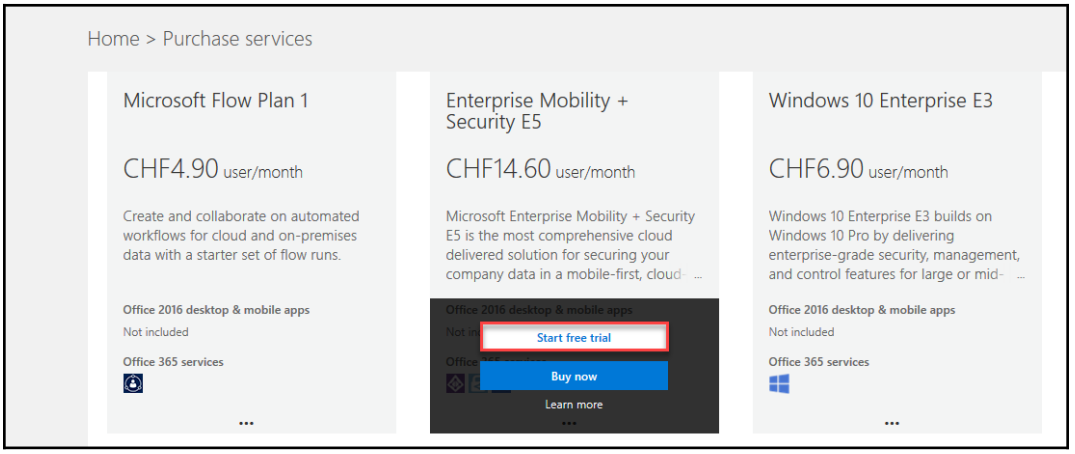


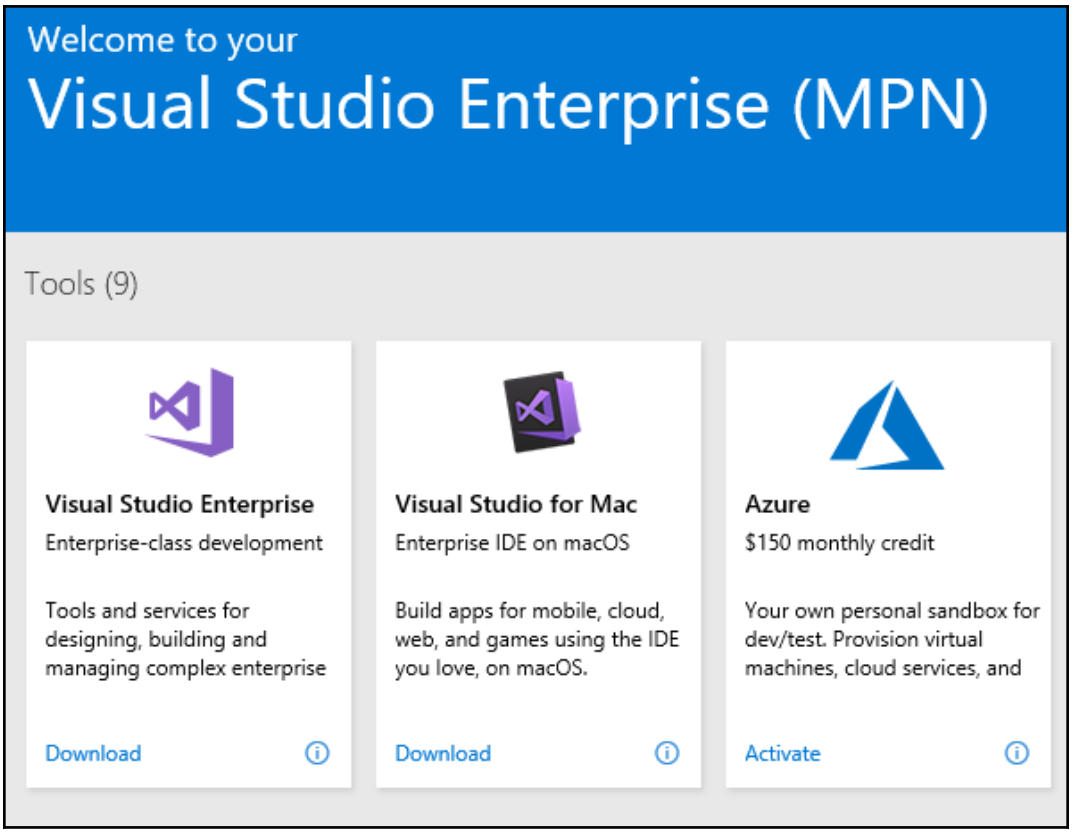


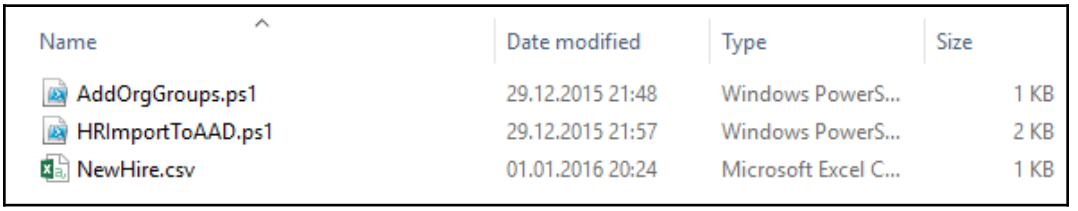

Create your user ID
You need a user ID and password to sign in to your account.
admin
@
inovitcloudlabs
.onmicrosoft.com
admin@inovitcloudlabs.onmicrosoft.com

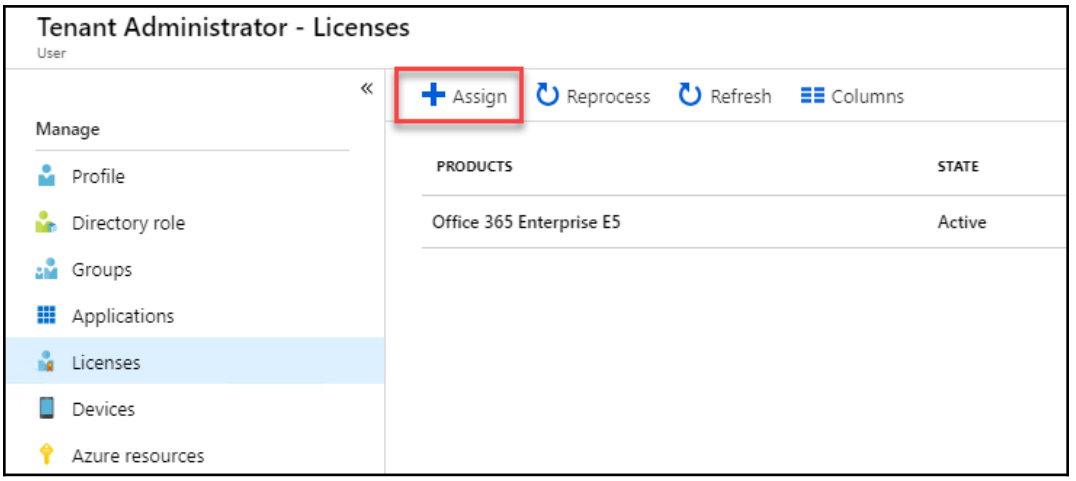

Good morning
Search
Apps
Install Office
Outlook
OneDrive
Word
Excel
PowerPoint
OneNote
SharePoint
Teams
Yammer
Admin
Explore all your apps
Documents
Upload and open...
New
Recent
Pinned
Shared with me
Discover


Microsoft 365 admin center
Home
Users
Groups
Billing
Purchase services
Subscriptions
Bills
Payment methods
Licenses
Billing notifications
Show more
Home > Subscriptions
Assign to users
Add subscriptions
Office 365 Enterprise E5
Trial
Active
Expires December 23, 2018
Extend trial
Licenses
Available 25
Assigned 1
Assign to users
Description
The Office suite, plus email, instant messaging, HD video conferencing, 1 TB personal file storage and sharing, and advanced security, analytics and Audio conferencing.
Learn more
CHF40.20 user/month
Buy now
More actions
Find a solution provider

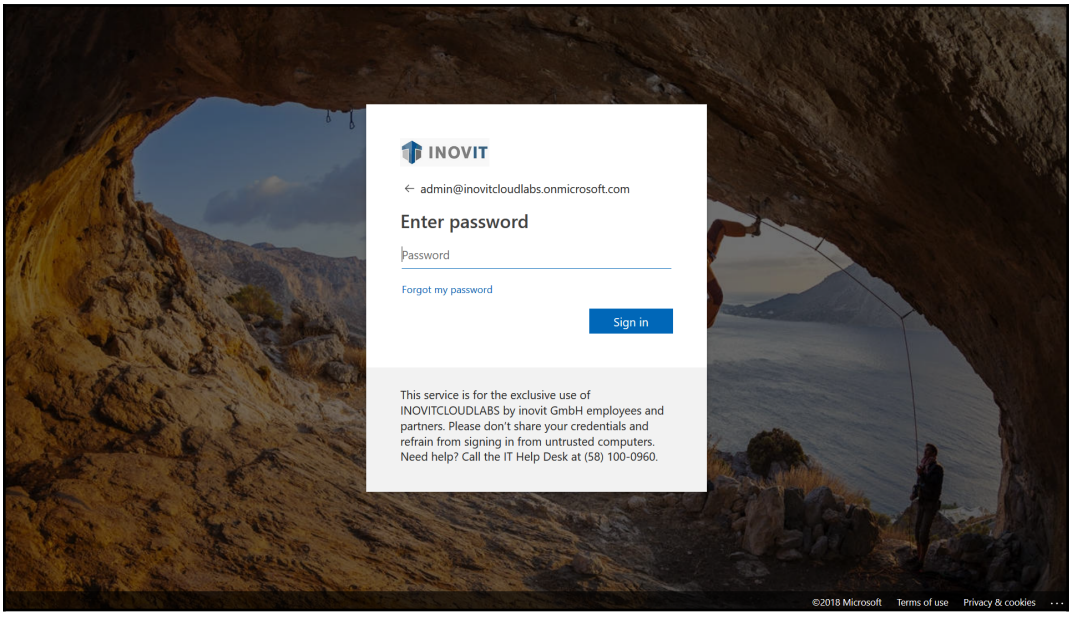

Home > Purchase services
Microsoft Flow Plan 1
CHF4.90 user/month
Create and collaborate on automated workflows for cloud and on-premises data with a starter set of flow runs.
Office 2016 desktop & mobile apps
Not included
Office 365 services
Enterprise Mobility + Security E5
CHF14.60 user/month
Microsoft Enterprise Mobility + Security E5 is the most comprehensive cloud delivered solution for securing your company data in a mobile-first, cloud
Office 2016 desktop & mobile apps
Start free trial
Buy now
Learn more
Windows 10 Enterprise E3
CHF6.90 user/month
Windows 10 Enterprise E3 builds on Windows 10 Pro by delivering enterprise-grade security, management, and control features for large or mid
Office 2016 desktop & mobile apps
Not included
Office 365 services

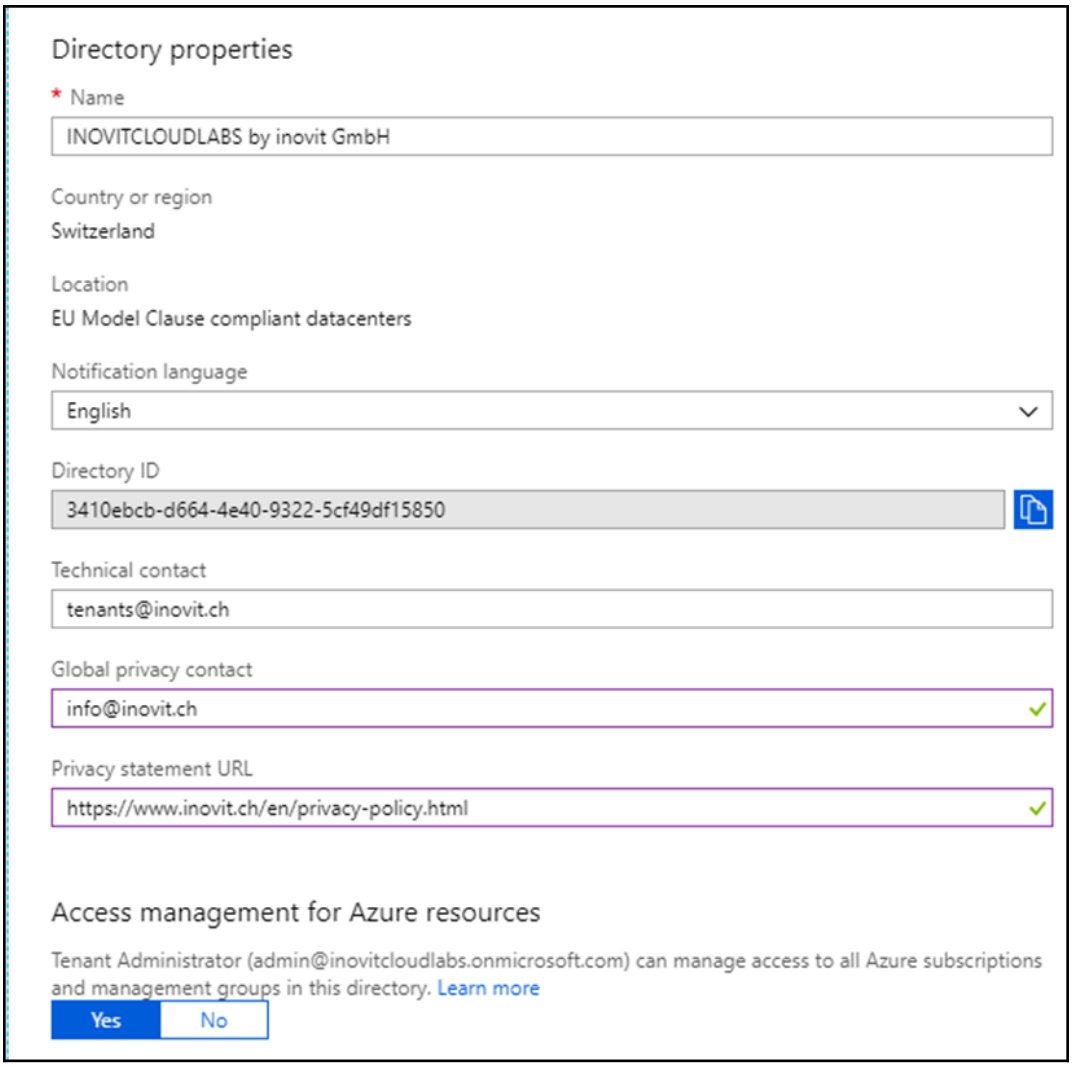

Welcome to your
Visual Studio Enterprise (MPN)
Tools (9)
Visual Studio Enterprise
Enterprise-class development
Tools and services for designing, building and managing complex enterprise
Download
Visual Studio for Mac
Enterprise IDE on macOS
Build apps for mobile, cloud, web, and games using the IDE you love, on macOS.
Download
Azure
$150 monthly credit
Your own personal sandbox for dev/test. Provision virtual machines, cloud services, and
Activate

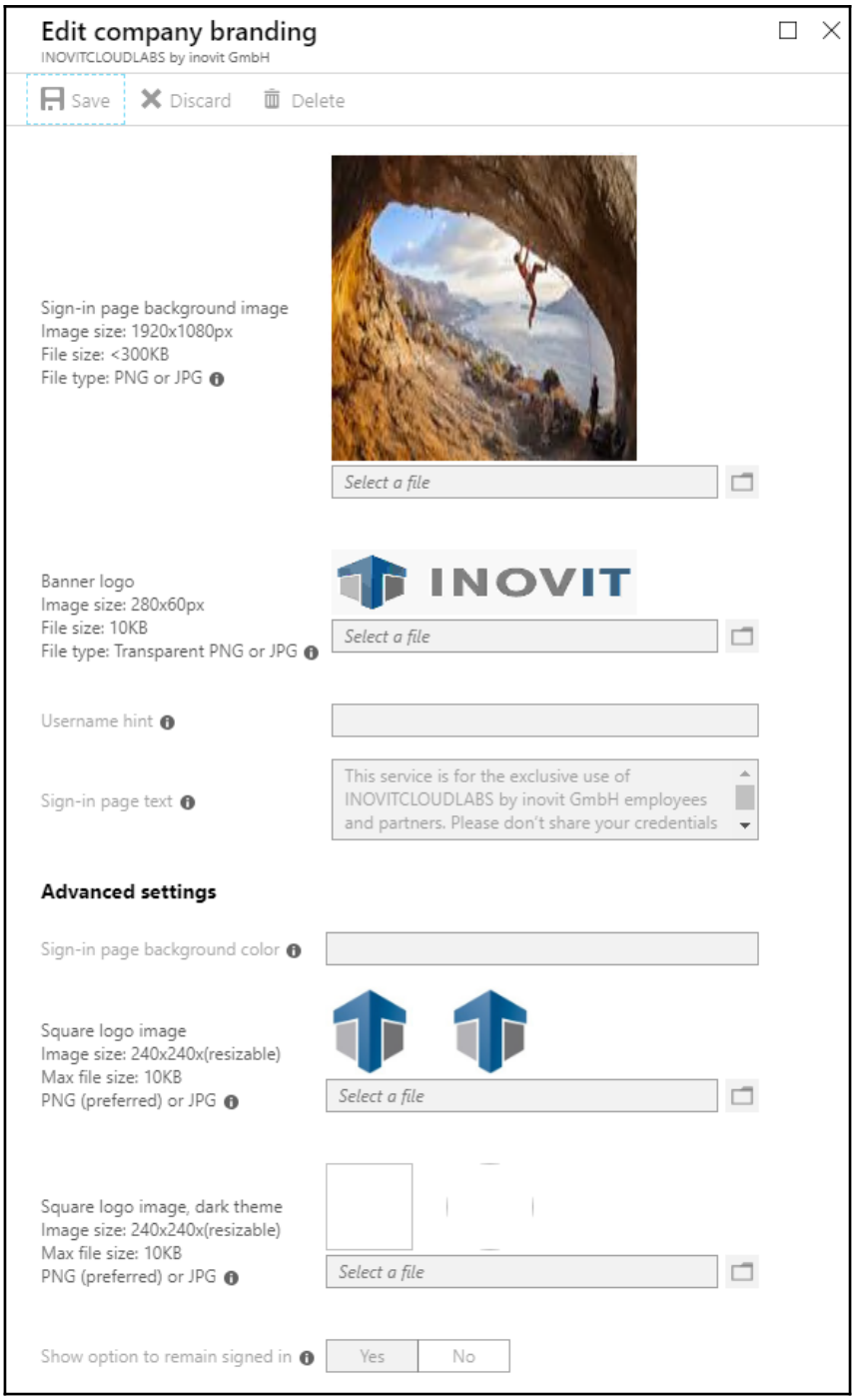

Name
Date modified
Type
Size
AddOrgGroups.ps1
29.12.2015 21:48
Windows PowerS...
1 KB
HRImportToAAD.ps1
29.12.2015 21:57
Windows PowerS...
2 KB
NewHire.csv
01.01.2016 20:24
Microsoft Excel C...
1 KB

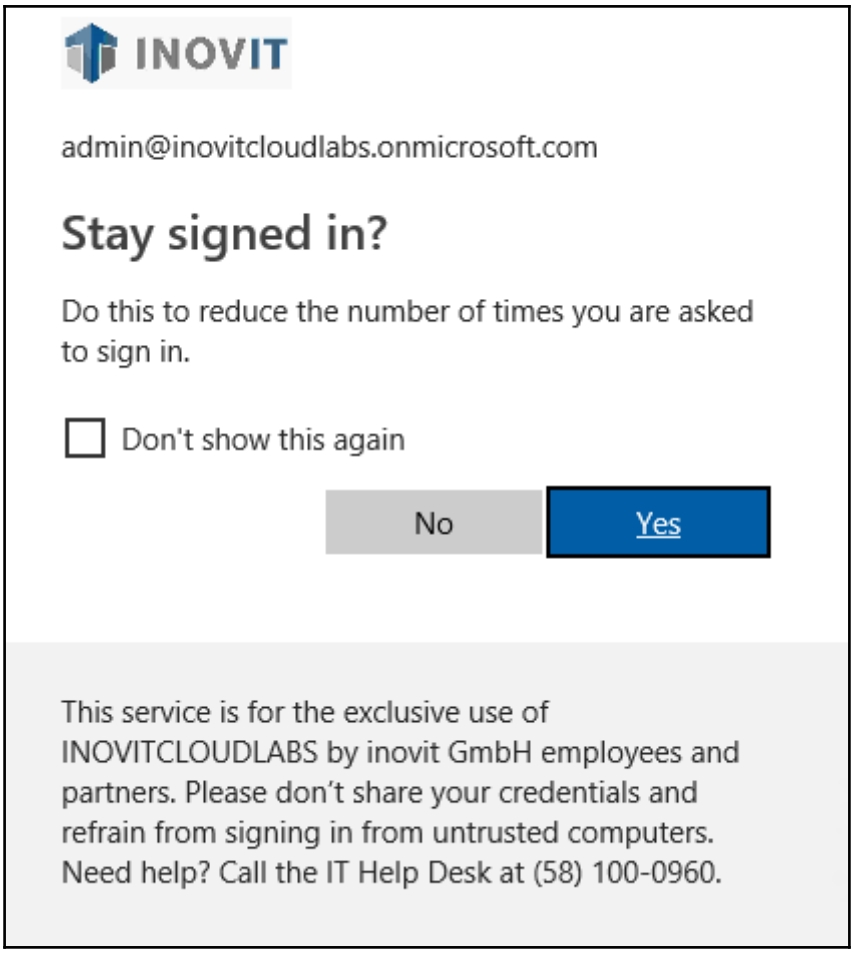


PRODUCTS	STATE	ENABLED SERVICES	ASSIGNMENT PATHS
Enterprise Mobility + Security E5	Active	9/9	Direct
Office 365 Enterprise E5	Active	25/25	Direct

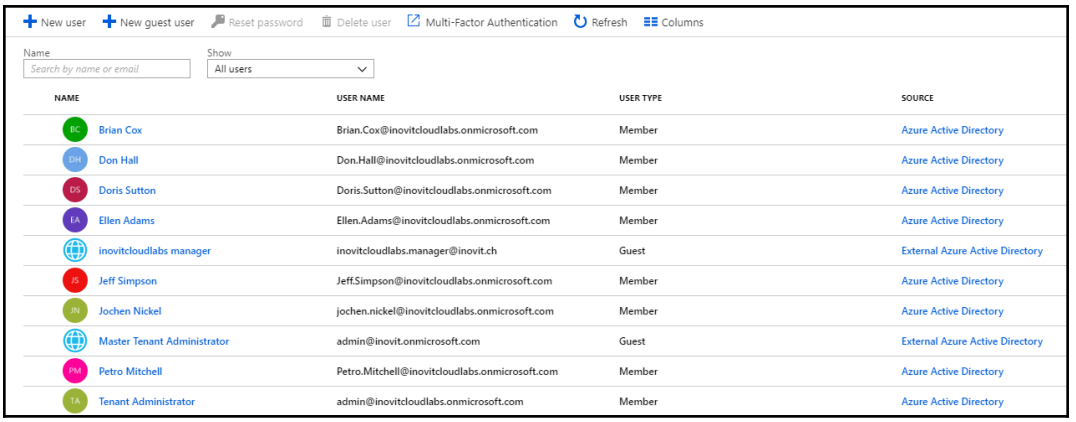


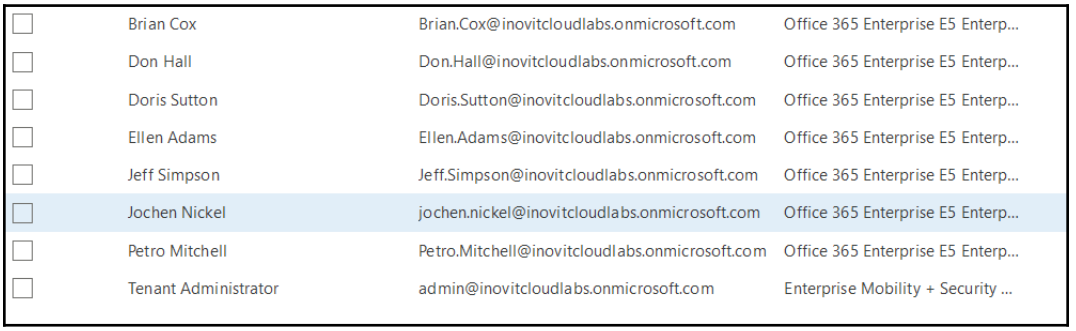

Directory properties
* Name
INOVITCLOUDLABS by inovit GmbH
Country or region
Switzerland
Location
EU Model Clause compliant datacenters
Notification language
English
Directory ID
3410ebcb-d664-4e40-9322-5cf49df15850
Technical contact
tenants@inovit.ch
Global privacy contact
info@inovit.ch
Privacy statement URL
https://www.inovit.ch/en/privacy-policy.html
Access management for Azure resources
Tenant Administrator (admin@inovitcloudlabs.onmicrosoft.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more
Yes
No


Edit company branding
INOVITCLOUDLABS by inovit GmbH
Save
Discard
Delete
Sign-in page background image
Image size: 1920x1080px
File size: <300KB
File type: PNG or JPG
Select a file
Banner logo
Image size: 280x60px
File size: 10KB
File type: Transparent PNG or JPG
INOVIT
Select a file
Username hint
Sign-in page text
This service is for the exclusive use of INOVITCLOUDLABS by inovit GmbH employees and partners. Please don't share your credentials
Advanced settings
Sign-in page background color
Square logo image
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG
Select a file
Square logo image, dark theme
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG
Select a file
Show option to remain signed in
Yes
No

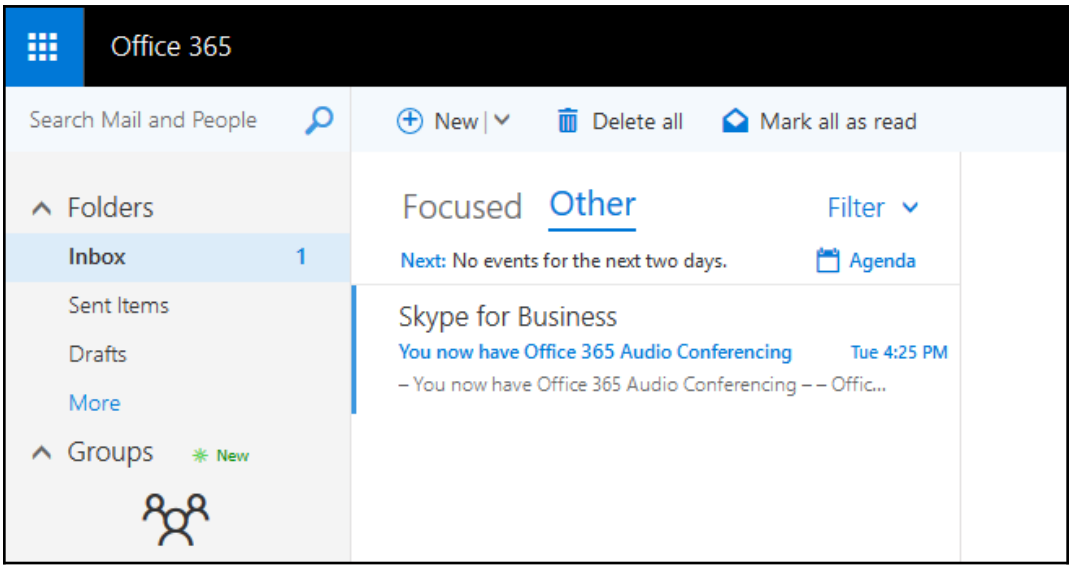

INOVIT
admin@inovitcloudlabs.onmicrosoft.com
Stay signed in?
Do this to reduce the number of times you are asked to sign in.
Don't show this again
No
Yes
This service is for the exclusive use of INOVITCLOUDLABS by inovit GmbH employees and partners. Please don't share your credentials and refrain from signing in from untrusted computers. Need help? Call the IT Help Desk at (58) 100-0960.

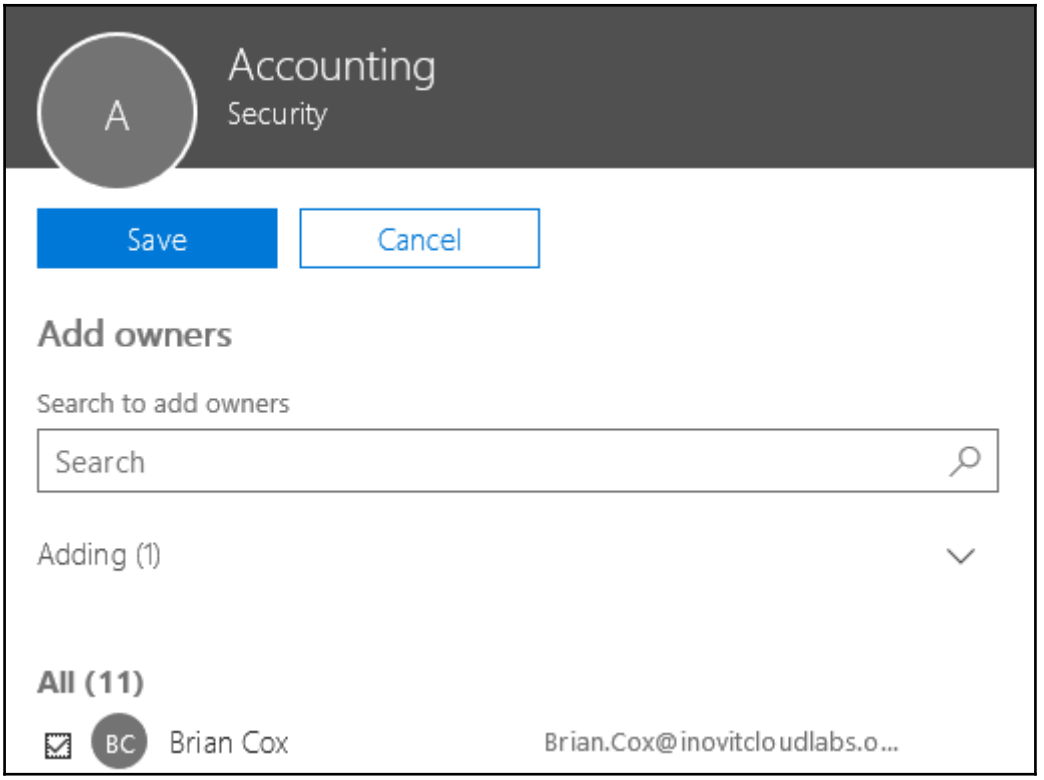

LOCALE
BACKGROUND IMAGE
BANNER LOGO
USERNAME HINT
SIGN-IN PAGE TEXT
Default
This service is for the exclusive use of INOVIT...

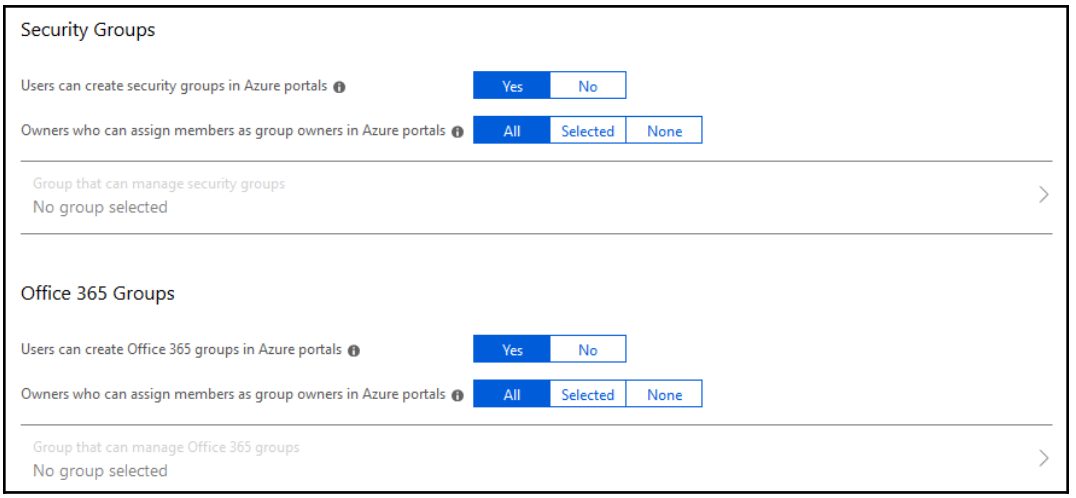

New user
New guest user
Reset password
Delete user
Multi-Factor Authentication
Refresh
Columns
Name
Search by name or email
Show
All users
NAME
USER NAME
USER TYPE
SOURCE
Brian Cox
Brian.Cox@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory
Don Hall
Don.Hall@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory
Doris Sutton
Doris.Sutton@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory
Ellen Adams
Ellen.Adams@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory
inovitcloudlabs manager
inovitcloudlabs.manager@inovit.ch
Guest
External Azure Active Directory
Jeff Simpson
Jeff.Simpson@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory
Jochen Nickel
jochen.nickel@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory
Master Tenant Administrator
admin@inovit.onmicrosoft.com
Guest
External Azure Active Directory
Petro Mitchell
Petro.Mitchell@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory
Tenant Administrator
admin@inovitcloudlabs.onmicrosoft.com
Member
Azure Active Directory

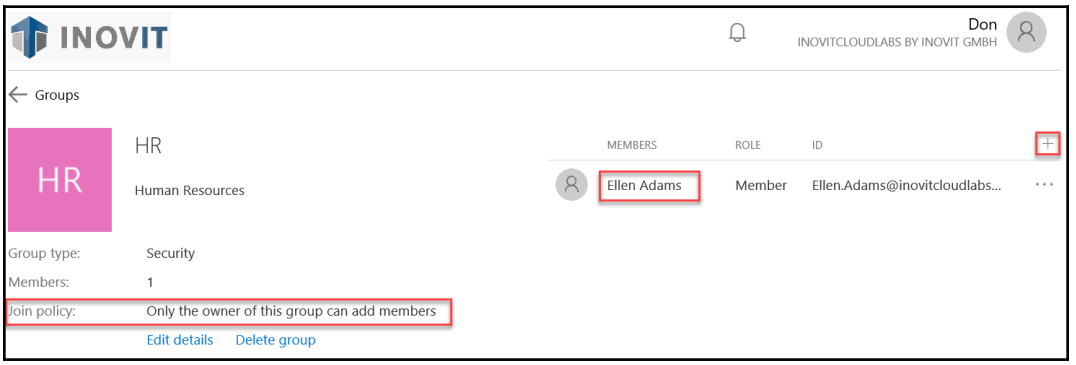

Brian Cox
Brian.Cox@inovitcloudlabs.onmicrosoft.com
Office 365 Enterprise E5 Enterp...
Don Hall
Don.Hall@inovitcloudlabs.onmicrosoft.com
Office 365 Enterprise E5 Enterp...
Doris Sutton
Doris.Sutton@inovitcloudlabs.onmicrosoft.com
Office 365 Enterprise E5 Enterp...
Ellen Adams
Ellen.Adams@inovitcloudlabs.onmicrosoft.com
Office 365 Enterprise E5 Enterp...
Jeff Simpson
Jeff.Simpson@inovitcloudlabs.onmicrosoft.com
Office 365 Enterprise E5 Enterp...
Jochen Nickel
jochen.nickel@inovitcloudlabs.onmicrosoft.com
Office 365 Enterprise E5 Enterp...
Petro Mitchell
Petro.Mitchell@inovitcloudlabs.onmicrosoft.com
Office 365 Enterprise E5 Enterp...
Tenant Administrator
admin@inovitcloudlabs.onmicrosoft.com
Enterprise Mobility + Security ...

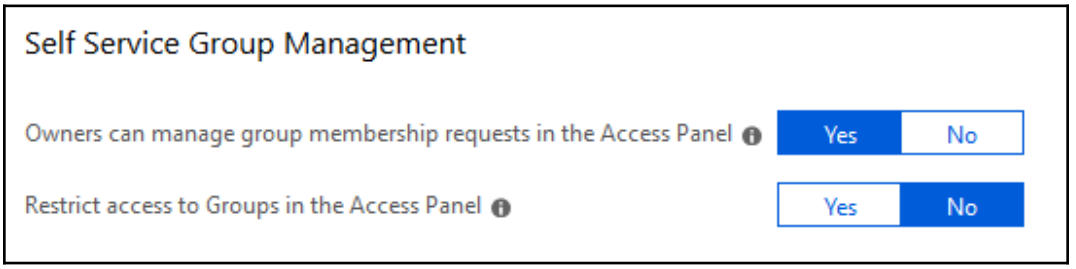

Accounting
Security
Assigned
HR
Security
Assigned
Sales
Security
Assigned

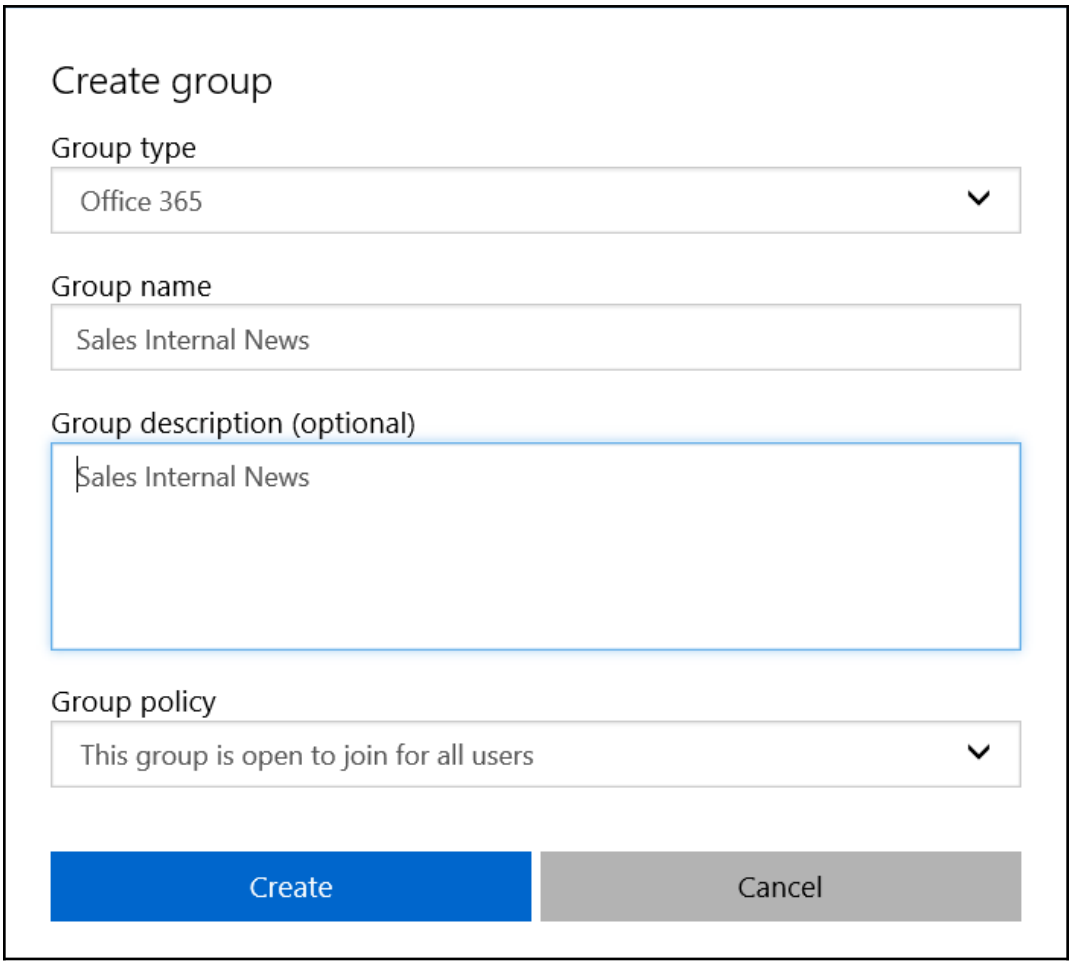

Office 365
Search Mail and People
New
Delete all
Mark all as read
Folders
Inbox 1
Sent Items
Drafts
More
Groups
New
Focused
Other
Filter
Next: No events for the next two days.
Agenda
Skype for Business
You now have Office 365 Audio Conferencing
Tue 4:25 PM
– You now have Office 365 Audio Conferencing – – Offic...

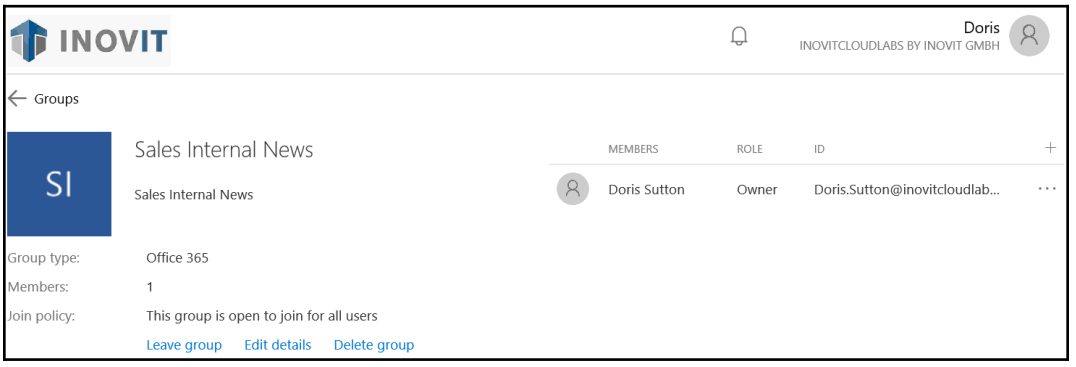

A
Accounting
Security
Save
Cancel
Add owners
Search to add owners
Search
Adding (1)
All (11)
BC
Brian Cox
Brian.Cox@inovitcloudlabs.o...

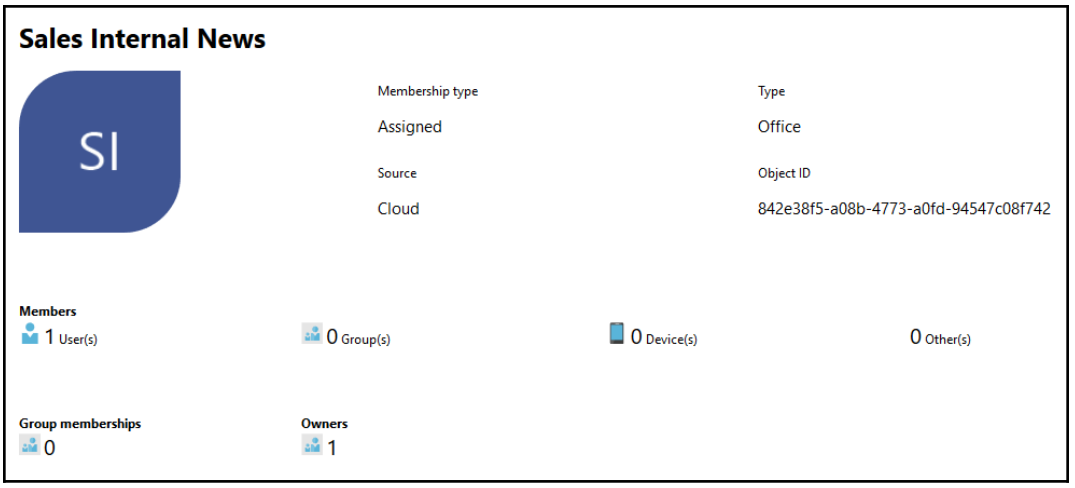

Security Groups
Users can create security groups in Azure portals
Yes
No
Owners who can assign members as group owners in Azure portals
All
Selected
None
Group that can manage security groups
No group selected
Office 365 Groups
Users can create Office 365 groups in Azure portals
Yes
No
Owners who can assign members as group owners in Azure portals
All
Selected
None
Group that can manage Office 365 groups
No group selected

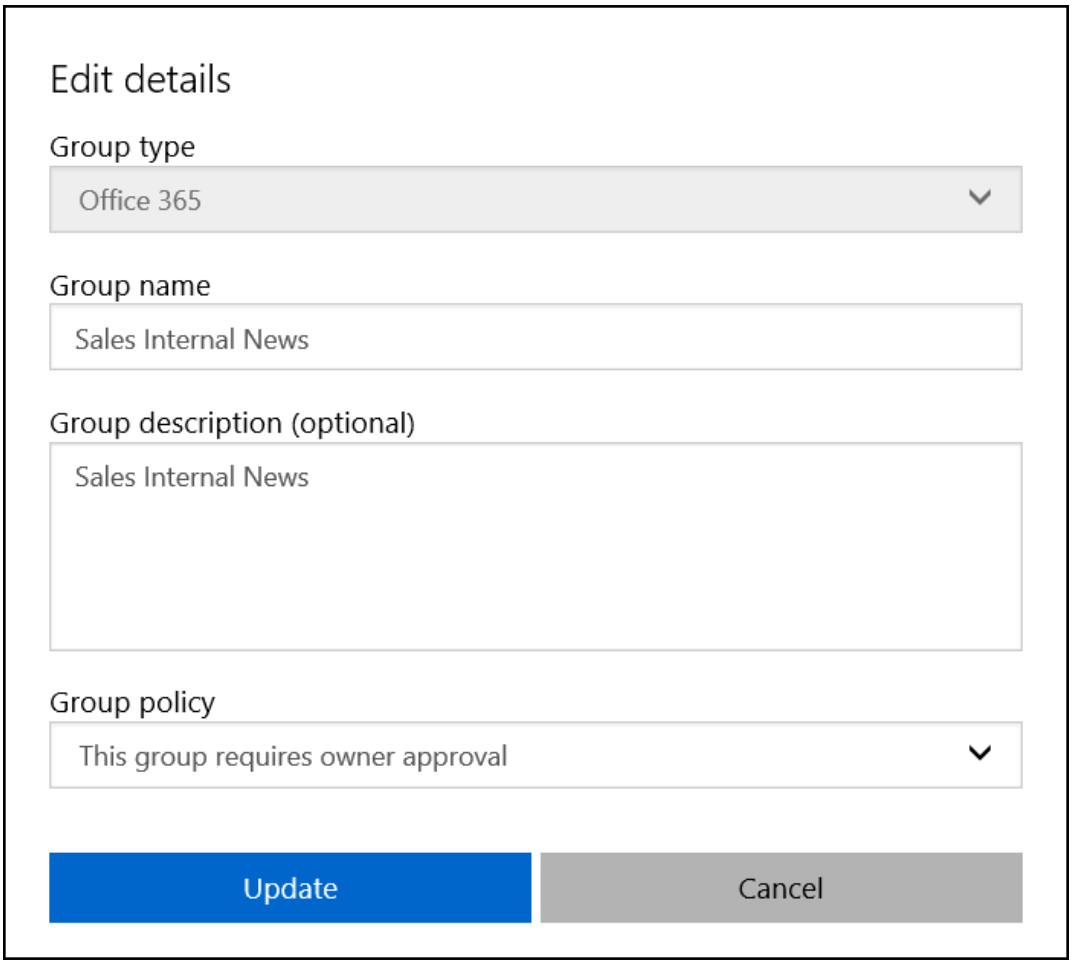

INOVIT
Don
INOVITCLOUDLABS BY INOVIT GMBH
Groups
HR
HR
Human Resources
MEMBERS
ROLE
ID
Ellen Adams
Member
Ellen.Adams@inovitcloudlabs...
Group type:
Security
Members:
1
Join policy:
Only the owner of this group can add members
Edit details
Delete group

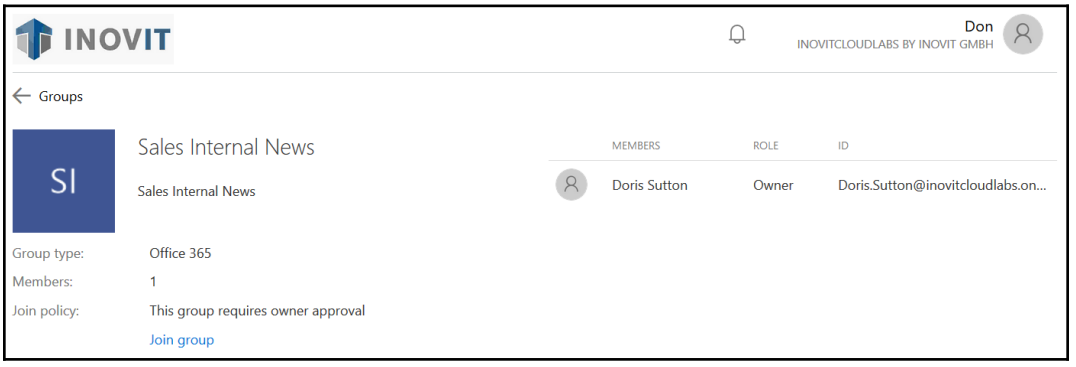

Self Service Group Management
Owners can manage group membership requests in the Access Panel
Yes
No
Restrict access to Groups in the Access Panel
Yes
No

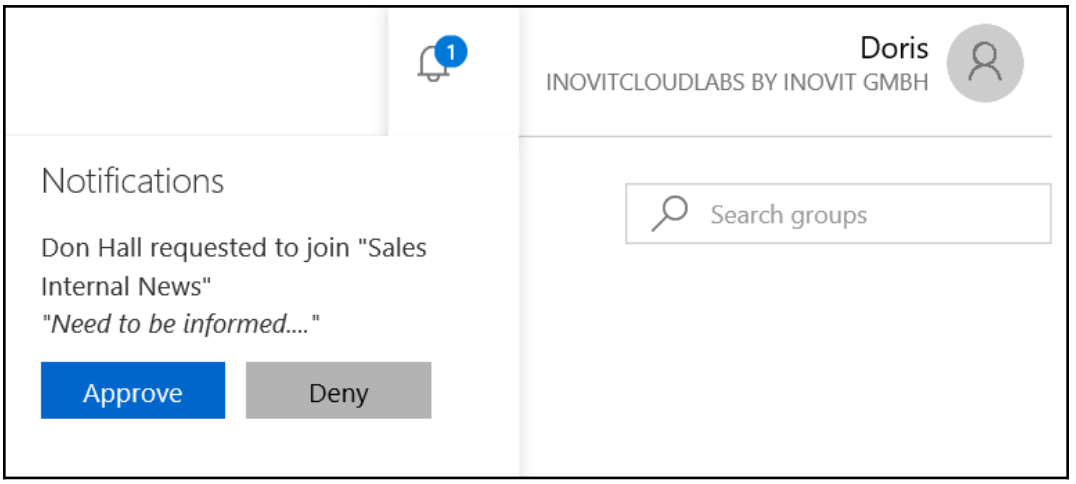

Create group
Group type
Office 365
Group name
Sales Internal News
Group description (optional)
Sales Internal News
Group policy
This group is open to join for all users
Create
Cancel

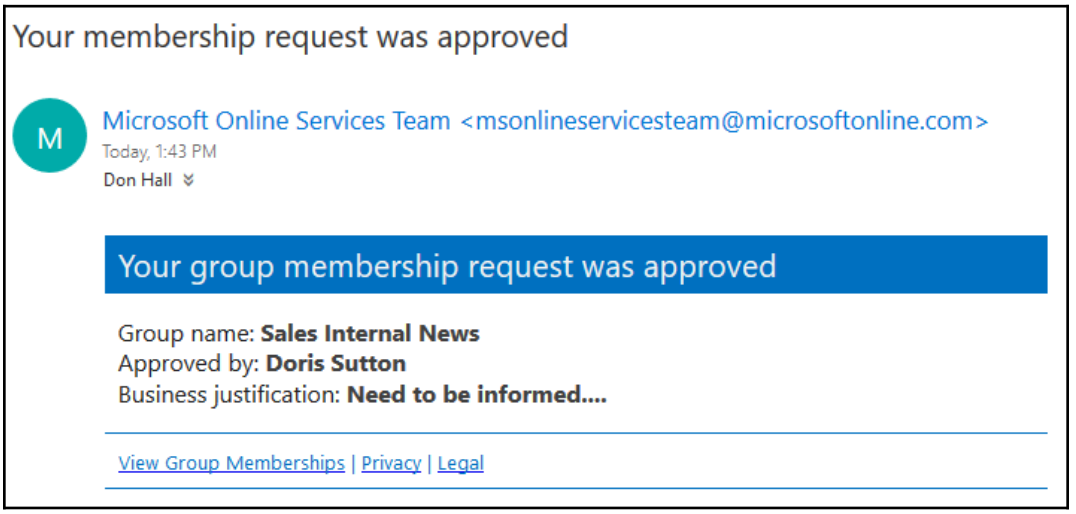

INOVIT
Doris
INOVITCLOUDLABS BY INOVIT GMBH
Groups
SI
Sales Internal News
Sales Internal News
MEMBERS
ROLE
ID
Doris Sutton
Owner
Doris.Sutton@inovitcloudlab...
Group type:
Office 365
Members:
1
Join policy:
This group is open to join for all users
Leave group
Edit details
Delete group

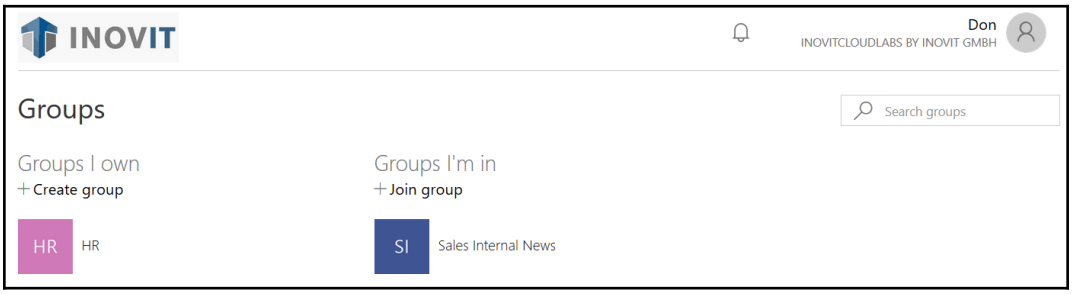

Sales Internal News
SI
Membership type
Assigned
Type
Office
Source
Cloud
Object ID
842e38f5-a08b-4773-a0fd-94547c08f742
Members
1 User(s)
0 Group(s)
0 Device(s)
0 Other(s)
Group memberships
0
Owners
1

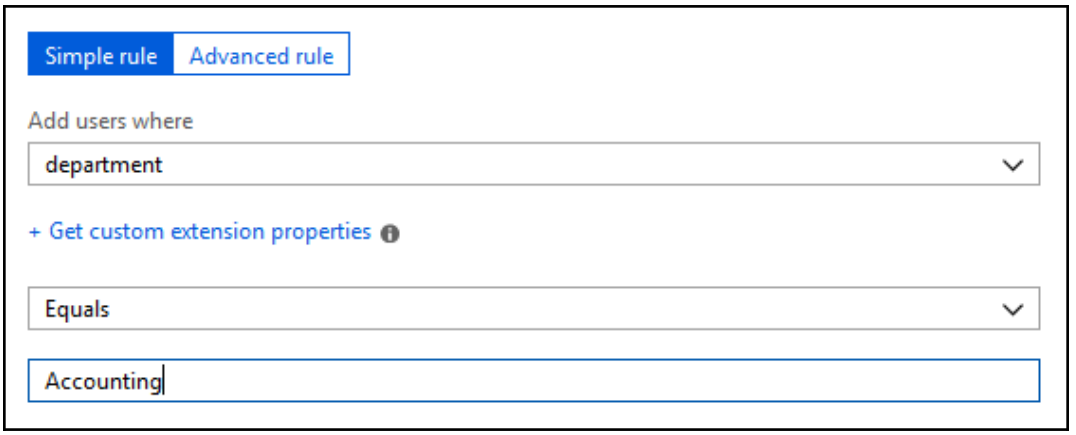

Edit details
Group type
Office 365
Group name
Sales Internal News
Group description (optional)
Sales Internal News
Group policy
This group requires owner approval
Update
Cancel

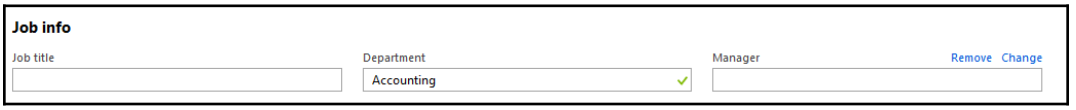

INOVIT
Don
INOVITCLOUDLABS BY INOVIT GMBH
Groups
SI
Sales Internal News
Sales Internal News
MEMBERS
ROLE
ID
Doris Sutton
Owner
Doris.Sutton@inovitcloudlabs.on...
Group type:
Office 365
Members:
1
Join policy:
This group requires owner approval
Join group

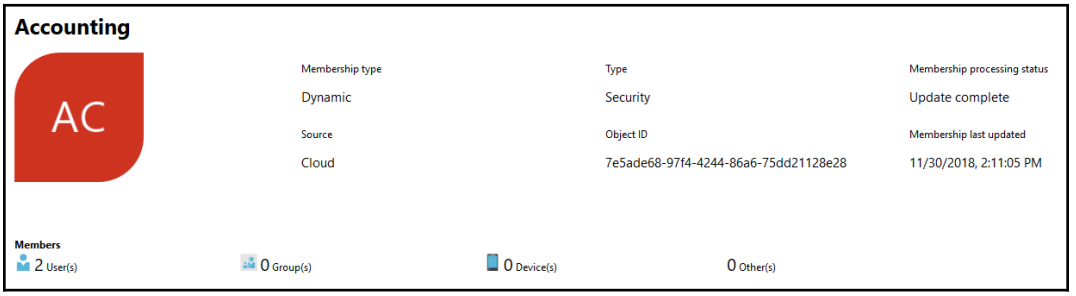

1
Doris
INOVITCLOUDLABS BY INOVIT GMBH
Notifications
Search groups
Don Hall requested to join "Sales Internal News"
"Need to be informed...."
Approve
Deny

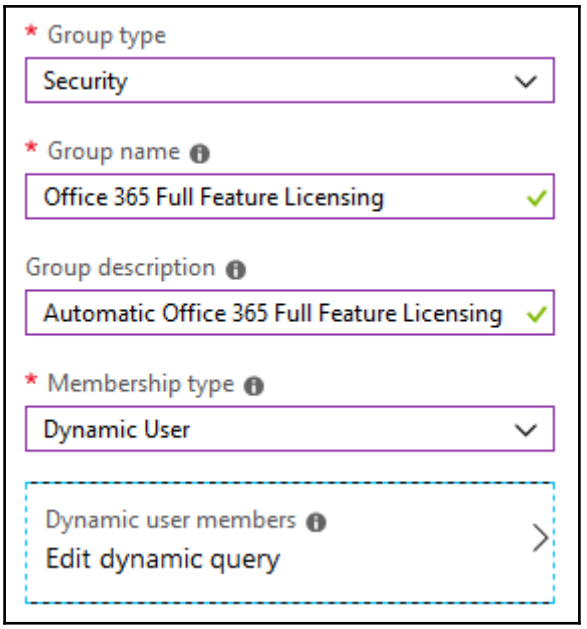

Your membership request was approved
M
Microsoft Online Services Team <msonlineservicesteam@microsoftonline.com>
Today, 1:43 PM
Don Hall
Your group membership request was approved
Group name: Sales Internal News
Approved by: Doris Sutton
Business justification: Need to be informed....
View Group Memberships | Privacy | Legal

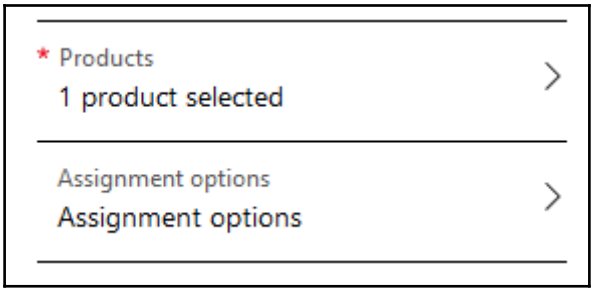

INOVIT
Don
INOVITCLOUDLABS BY INOVIT GMBH
Groups
Search groups
Groups I own
+ Create group
HR
HR
Groups I'm in
+ Join group
SI
Sales Internal News


Simple rule
Advanced rule
Add users where
department
+ Get custom extension properties
Equals
Accounting


Job info
Job title
Department
Accounting
Manager
Remove
Change


Accounting
AC
Membership type
Dynamic
Type
Security
Membership processing status
Update complete
Source
Cloud
Object ID
7e5ade68-97f4-4244-86a6-75dd21128e28
Membership last updated
11/30/2018, 2:11:05 PM
Members
2 User(s)
0 Group(s)
0 Device(s)
0 Other(s)



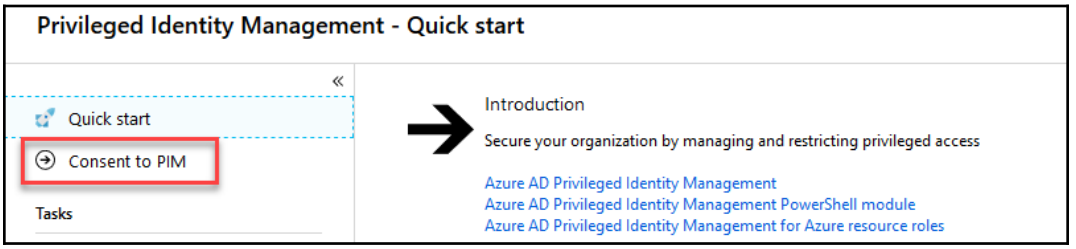


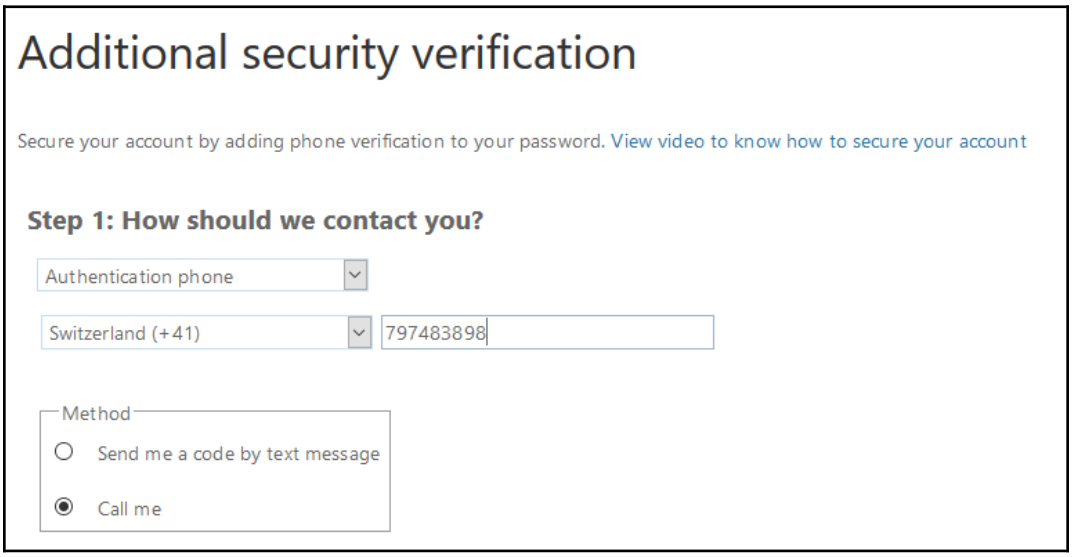
PRODUCTS	STATE	ENABLED SERVICES	ASSIGNMENT PATHS
Enterprise Mobility + Security E5	Active	9/9	Direct
Office 365 Enterprise E5	Active	25/25	Direct, Inherited (Office 365 Full Feature Licensing)

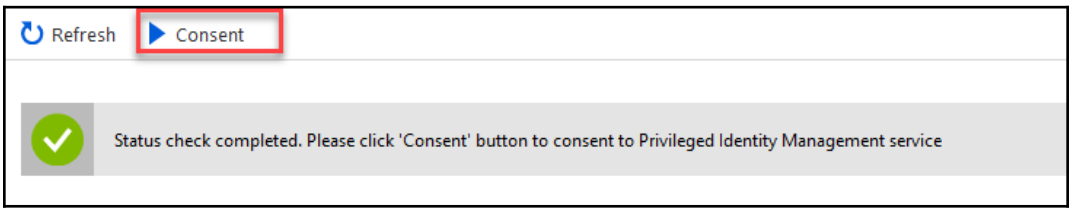
```
ObjectId                             DisplayName Description
--------                             ----------- -----------
8e36f339-b7cc-4f18-ad4f-89188f6f1025 HR          Human Resources Users
```

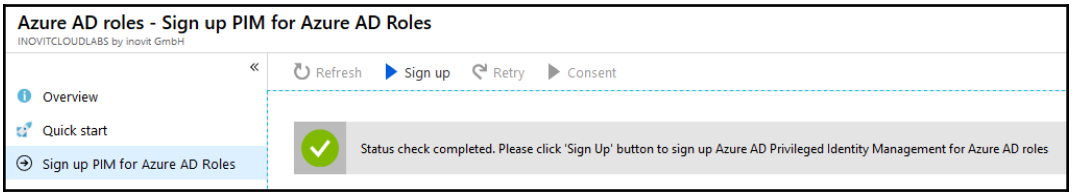
```
ObjectId                             DisplayName UserPrincipalName                                UserType
--------                             ----------- -----------------                                --------
44fb9355-0a23-4487-8059-206b62da16a6 Don Hall    Don.Hall@inovitcloudlabs.onmicrosoft.com     Member
0b242043-acdf-4c8a-8b26-f03eb913cbd7 Ellen Adams Ellen.Adams@inovitcloudlabs.onmicrosoft.com Member
```

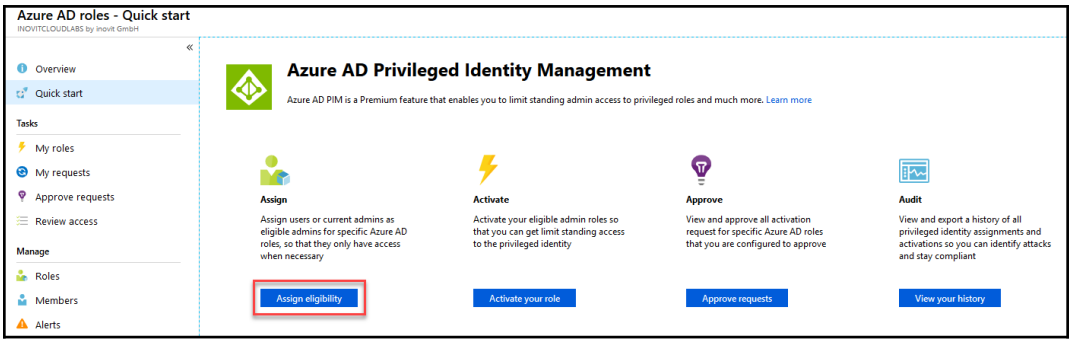
```
ObjectId                             DisplayName              Description
--------                             -----------              -----------
dd0bdb75-7631-49ca-be3f-6831d7428c41 User Account Administrator Can manage all aspects of users and groups, includin...
```

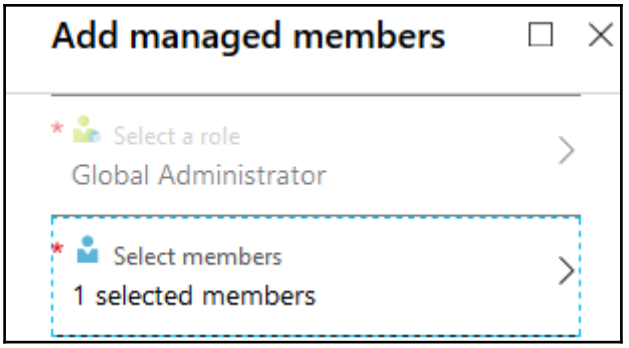


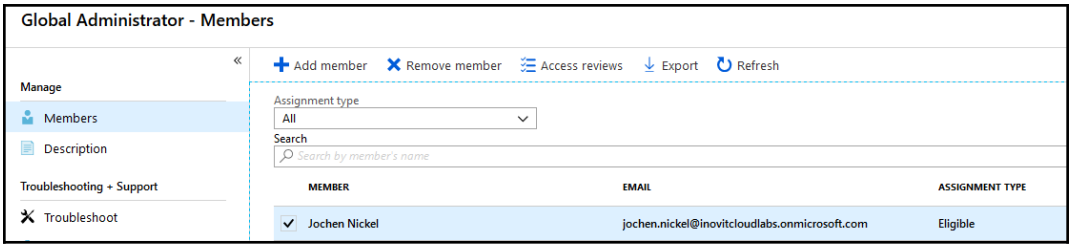


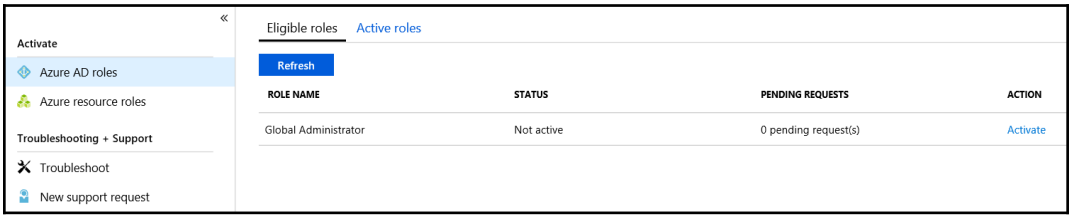


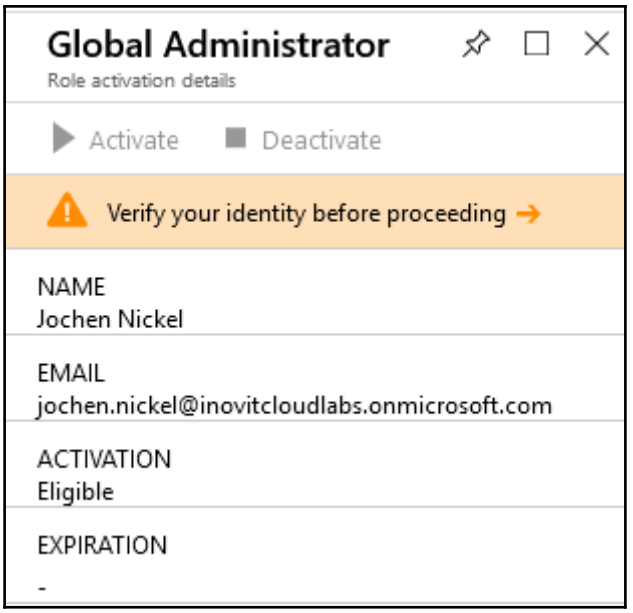


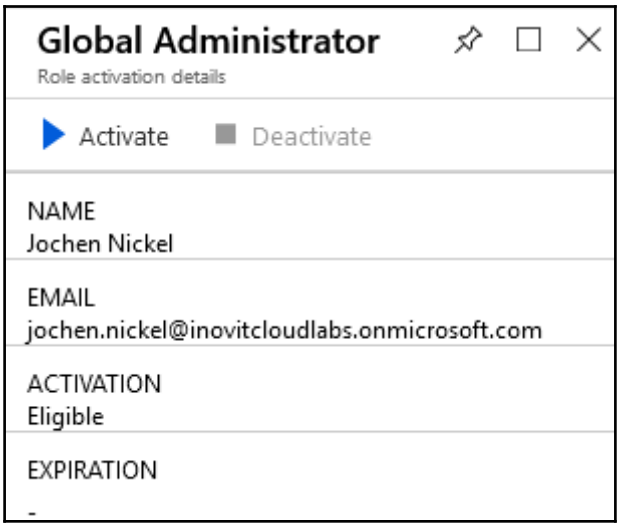

Azure AD roles - Quick start
INOVITCLOUDLABS by inovit GmbH
Overview
Quick start
Tasks
My roles
My requests
Approve requests
Review access
Manage
Roles
Members
Alerts
Azure AD Privileged Identity Management
Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more
Assign
Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary
Assign eligibility
Activate
Activate your eligible admin roles so that you can get limit standing access to the privileged identity
Activate your role
Approve
View and approve all activation request for specific Azure AD roles that you are configured to approve
Approve requests
Audit
View and export a history of all privileged identity assignments and activations so you can identify attacks and stay compliant
View your history

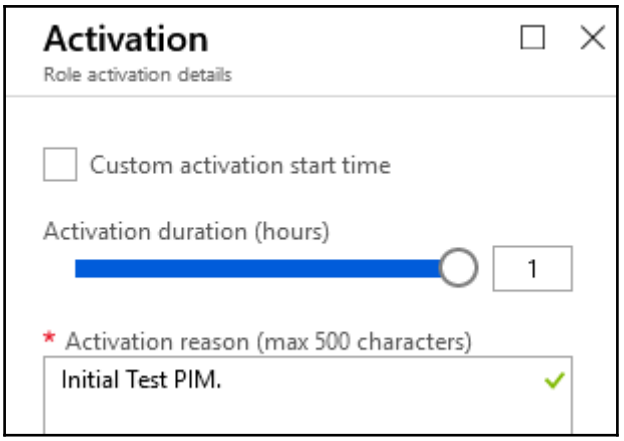

Add managed members
Select a role
Global Administrator
Select members
1 selected members

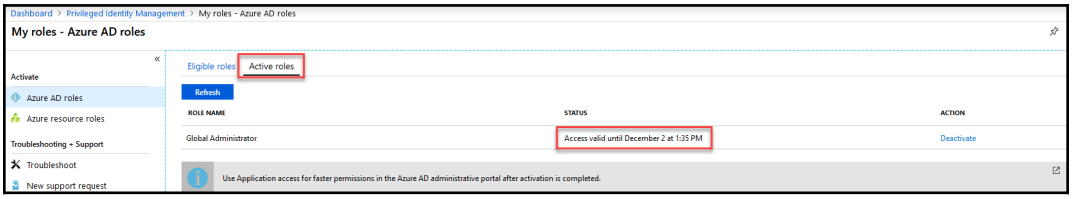

Global Administrator - Members
Manage
Members
Description
Troubleshooting + Support
Troubleshoot
Add member
Remove member
Access reviews
Export
Refresh
Assignment type
All
Search
Search by member's name
MEMBER
EMAIL
ASSIGNMENT TYPE
Jochen Nickel
jochen.nickel@inovitcloudlabs.onmicrosoft.com
Eligible

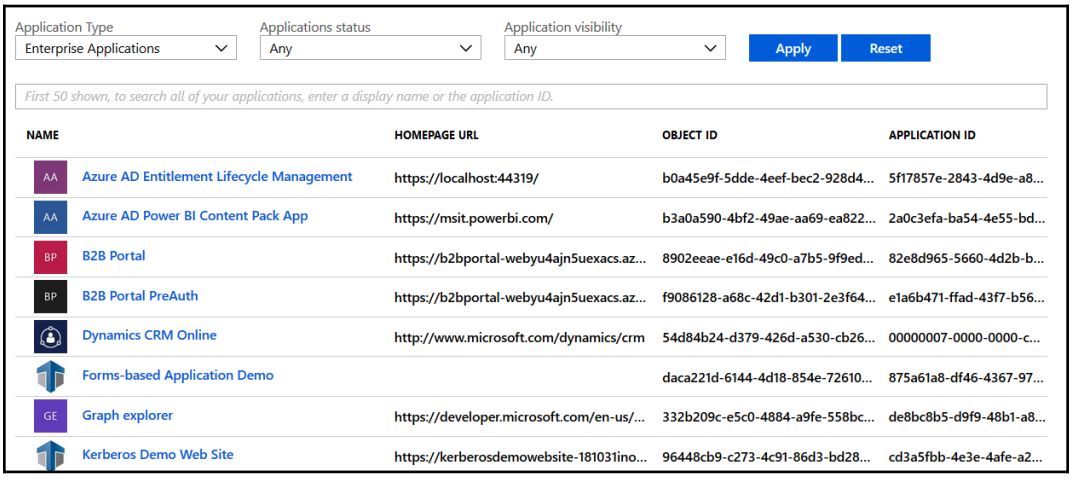

Activate
Azure AD roles
Azure resource roles
Troubleshooting + Support
Troubleshoot
New support request
Eligible roles
Active roles
Refresh
ROLE NAME
STATUS
PENDING REQUESTS
ACTION
Global Administrator
Not active
0 pending request(s)
Activate

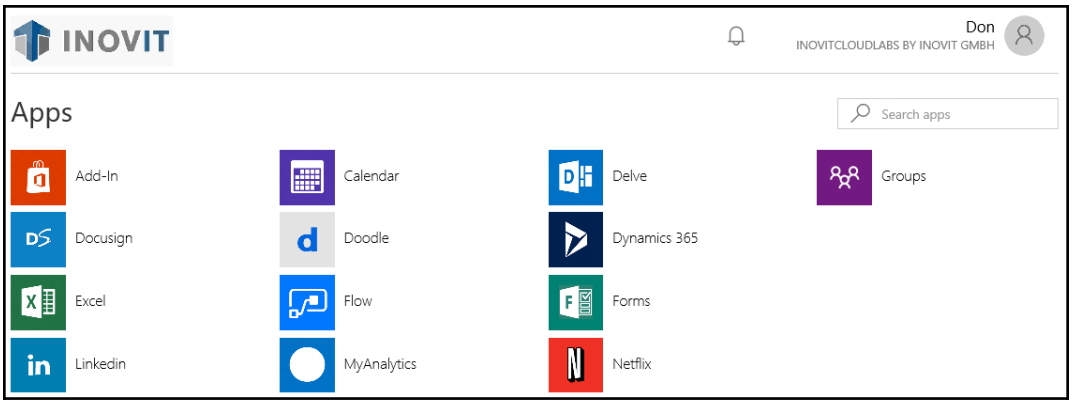

Global Administrator
Role activation details
Activate
Deactivate
Verify your identity before proceeding
NAME
Jochen Nickel
EMAIL
jochen.nickel@inovitcloudlabs.onmicrosoft.com
ACTIVATION
Eligible
EXPIRATION
-

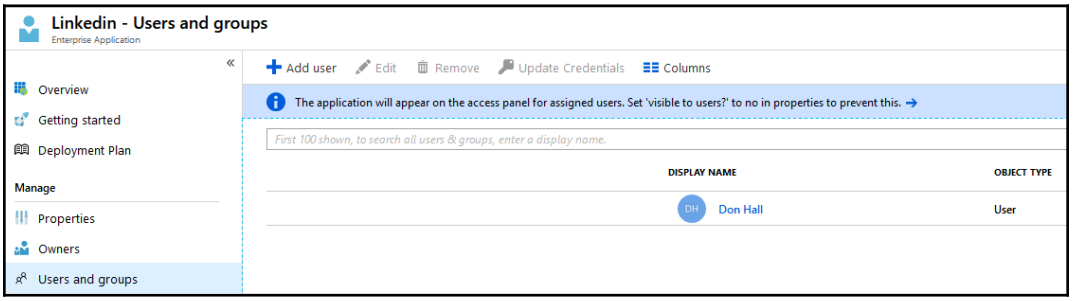

Global Administrator
Role activation details
Activate
Deactivate
NAME
Jochen Nickel
EMAIL
jochen.nickel@inovitcloudlabs.onmicrosoft.com
ACTIVATION
Eligible
EXPIRATION
-

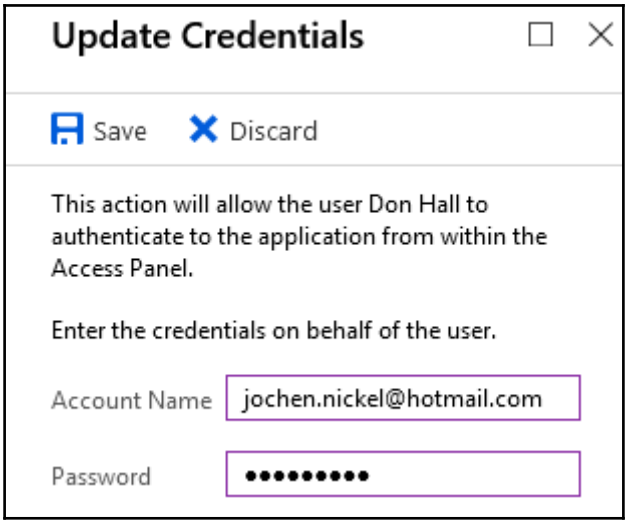

Activation
Role activation details
Custom activation start time
Activation duration (hours)
1
Activation reason (max 500 characters)
Initial Test PIM.

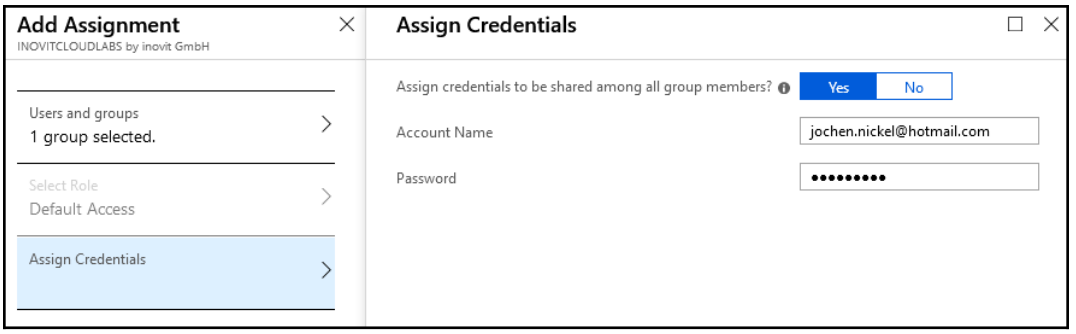

Dashboard > Privileged Identity Management > My roles - Azure AD roles
My roles - Azure AD roles
Activate
Azure AD roles
Azure resource roles
Troubleshooting + Support
Troubleshoot
New support request
Eligible roles
Active roles
Refresh
ROLE NAME
STATUS
ACTION
Global Administrator
Access valid until December 2 at 1:35 PM
Deactivate
Use Application access for faster permissions in the Azure AD administrative portal after activation is completed.

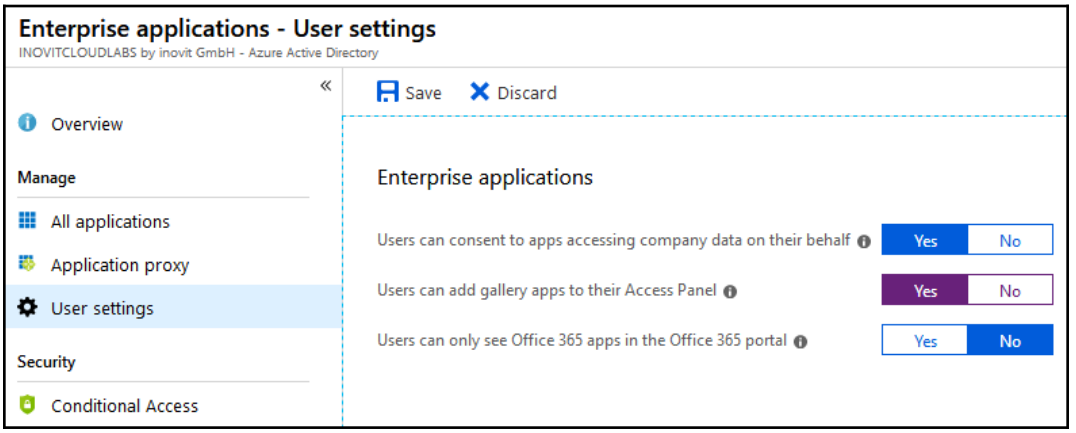

Application Type
Enterprise Applications
Applications status
Any
Application visibility
Any
Apply
Reset
First 50 shown, to search all of your applications, enter a display name or the application ID.
NAME
HOMEPAGE URL
OBJECT ID
APPLICATION ID
Azure AD Entitlement Lifecycle Management
https://localhost:44319/
b0a45e9f-5dde-4eef-bec2-928d4...
5f17857e-2843-4d9e-a8...
Azure AD Power BI Content Pack App
https://msit.powerbi.com/
b3a0a590-4bf2-49ae-aa69-ea822...
2a0c3efa-ba54-4e55-bd...
B2B Portal
https://b2bportal-webyu4ajn5uexacs.az...
8902eeae-e16d-49c0-a7b5-9f9ed...
82e8d965-5660-4d2b-b...
B2B Portal PreAuth
https://b2bportal-webyu4ajn5uexacs.az...
f9086128-a68c-42d1-b301-2e3f64...
e1a6b471-ffad-43f7-b56...
Dynamics CRM Online
http://www.microsoft.com/dynamics/crm
54d84b24-d379-426d-a530-cb26...
00000007-0000-0000-c...
Forms-based Application Demo
daca221d-6144-4d18-854e-72610...
875a61a8-df46-4367-97...
Graph explorer
https://developer.microsoft.com/en-us/...
332b209c-e5c0-4884-a9fe-558bc...
de8bc8b5-d9f9-48b1-a8...
Kerberos Demo Web Site
https://kerberosdemowebsite-181031ino...
96448cb9-c273-4c91-86d3-bd28...
cd3a5fbb-4e3e-4afe-a2...

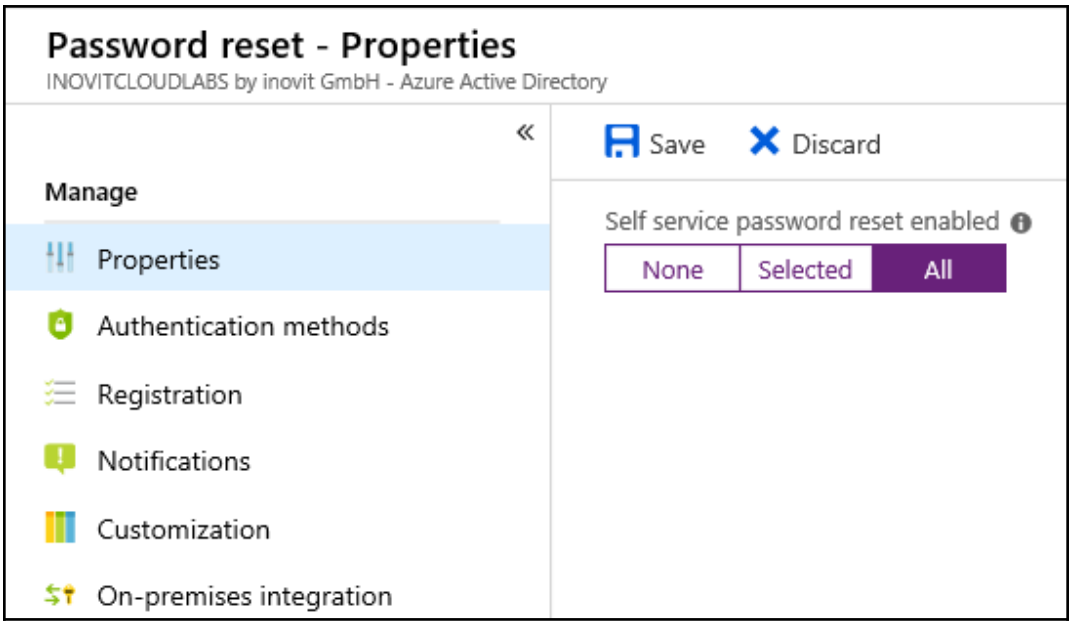

INOVIT
Don
INOVITCLOUDLABS BY INOVIT GMBH
Apps
Search apps
Add-In
Calendar
Delve
Groups
Docusign
Doodle
Dynamics 365
Excel
Flow
Forms
Linkedin
MyAnalytics
Netflix

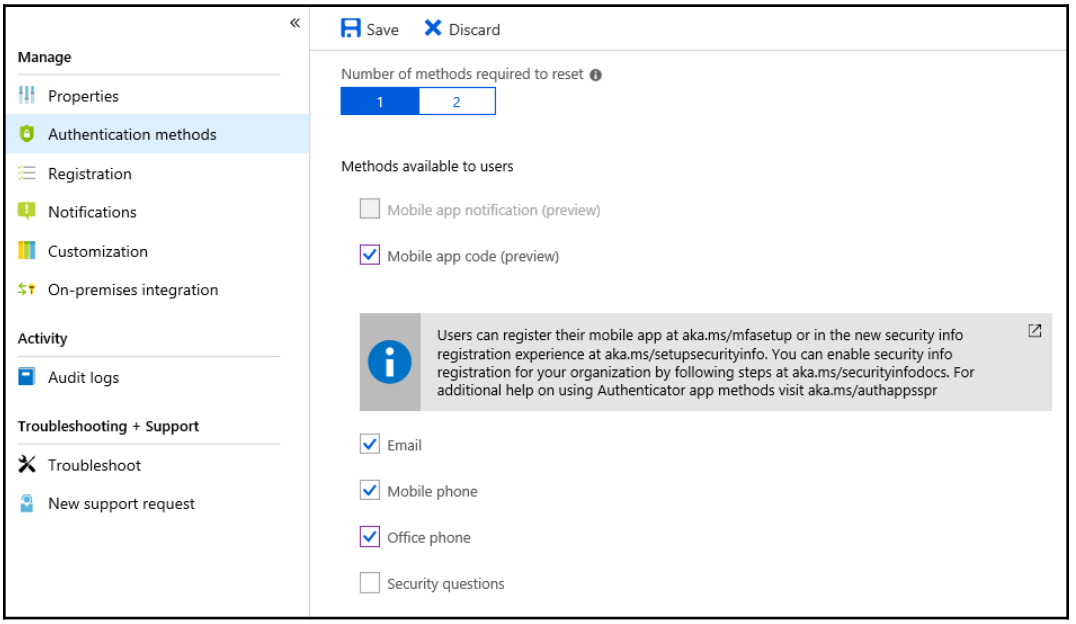

Linkedin - Users and groups
Enterprise Application
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Add user
Edit
Remove
Update Credentials
Columns
The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.
First 100 shown, to search all users & groups, enter a display name.
DISPLAY NAME
OBJECT TYPE
Don Hall
User

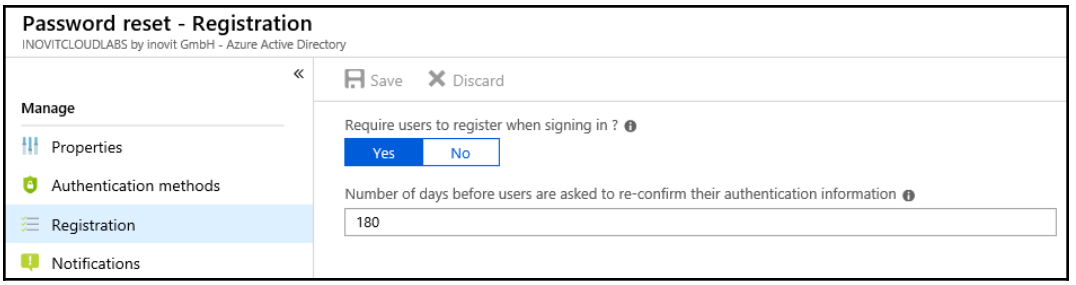

Update Credentials
Save
Discard
This action will allow the user Don Hall to authenticate to the application from within the Access Panel.
Enter the credentials on behalf of the user.
Account Name
jochen.nickel@hotmail.com
Password
••••••••••

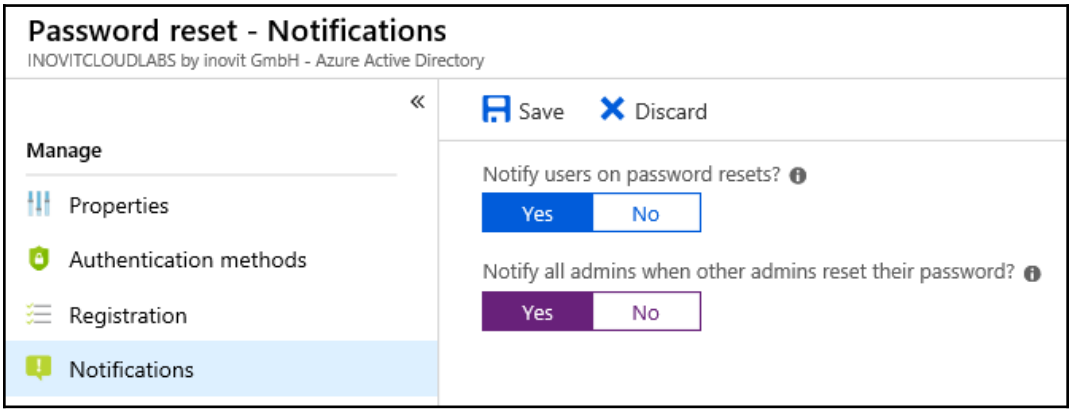

Add Assignment
INOVITCLOUDLABS by inovit GmbH
Users and groups
1 group selected.
Select Role
Default Access
Assign Credentials
Assign Credentials
Assign credentials to be shared among all group members?
Yes
No
Account Name
jochen.nickel@hotmail.com
Password
••••••••

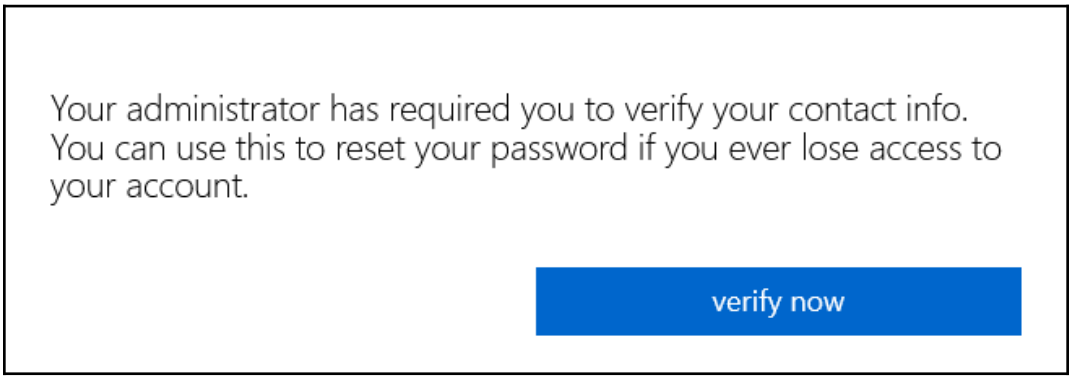

Enterprise applications - User settings
INOVITCLOUDLABS by inovit GmbH - Azure Active Directory
Overview
Manage
All applications
Application proxy
User settings
Security
Conditional Access
Save
Discard
Enterprise applications
Users can consent to apps accessing company data on their behalf
Yes
No
Users can add gallery apps to their Access Panel
Yes
No
Users can only see Office 365 apps in the Office 365 portal
Yes
No

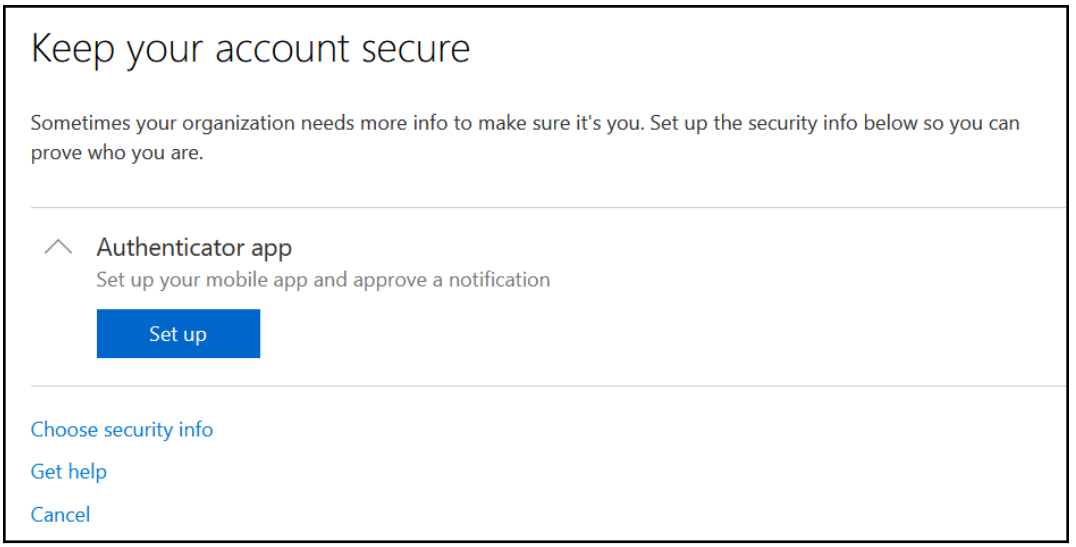

Password reset - Properties
INOVITCLOUDLABS by inovit GmbH - Azure Active Directory
Manage
Properties
Authentication methods
Registration
Notifications
Customization
On-premises integration
Save
Discard
Self service password reset enabled
None
Selected
All

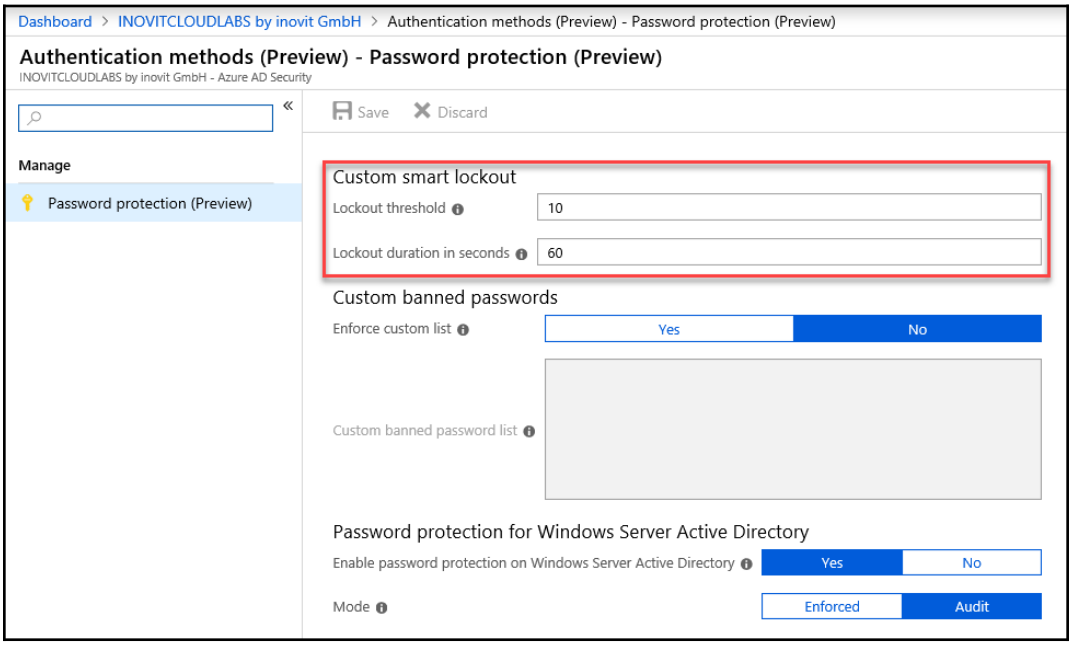

Manage
Properties
Authentication methods
Registration
Notifications
Customization
On-premises integration
Activity
Audit logs
Troubleshooting + Support
Troubleshoot
New support request
Save
Discard
Number of methods required to reset
1
2
Methods available to users
Mobile app notification (preview)
Mobile app code (preview)
Users can register their mobile app at aka.ms/mfasetup or in the new security info registration experience at aka.ms/setupsecurityinfo. You can enable security info registration for your organization by following steps at aka.ms/securityinfodocs. For additional help on using Authenticator app methods visit aka.ms/authappsspr
Email
Mobile phone
Office phone
Security questions

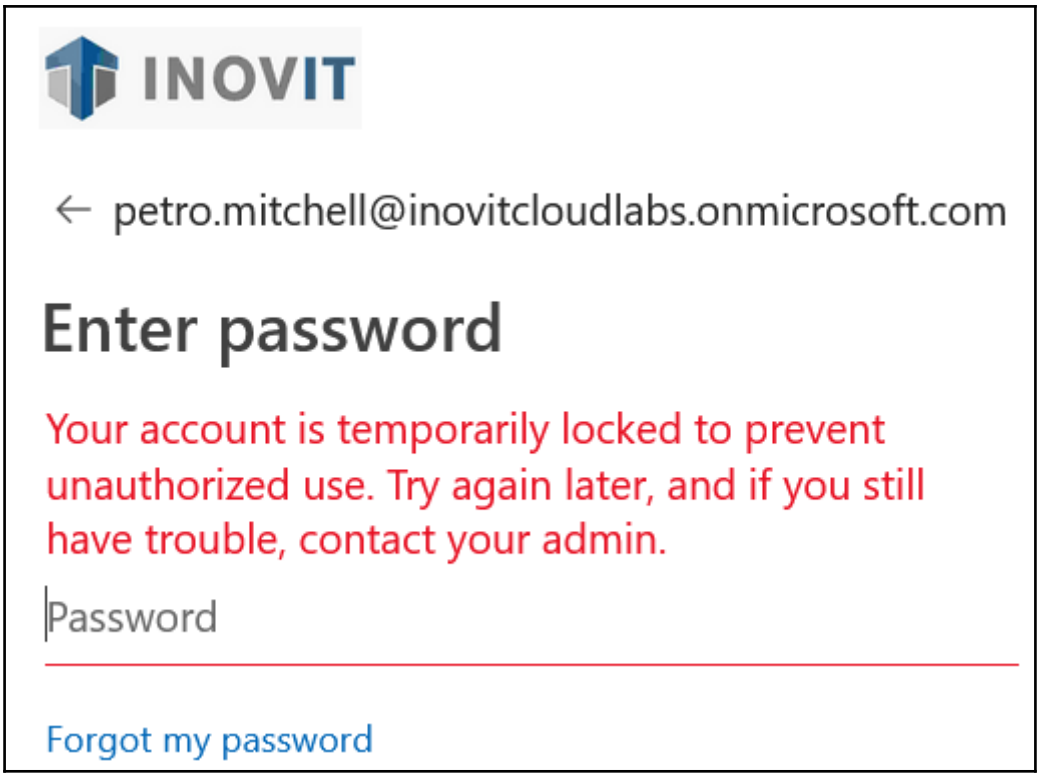

Password reset - Registration
INOVITCLOUDLABS by inovit GmbH - Azure Active Directory
Manage
Properties
Authentication methods
Registration
Notifications
Save
Discard
Require users to register when signing in ?
Yes
No
Number of days before users are asked to re-confirm their authentication information
180

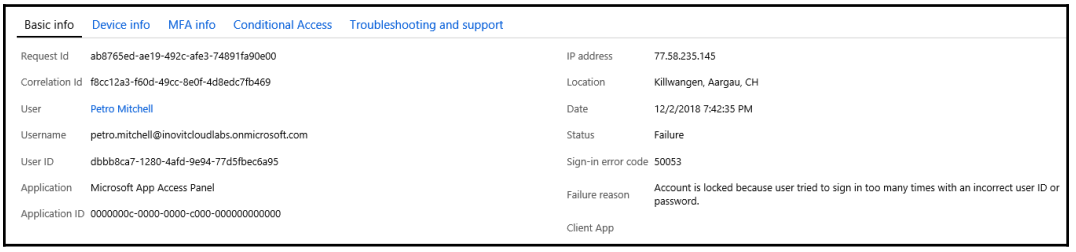

Password reset - Notifications
INOVITCLOUDLABS by inovit GmbH - Azure Active Directory
Manage
Properties
Authentication methods
Registration
Notifications
Save
Discard
Notify users on password resets?
Yes
No
Notify all admins when other admins reset their password?
Yes
No


Your administrator has required you to verify your contact info. You can use this to reset your password if you ever lose access to your account.
verify now

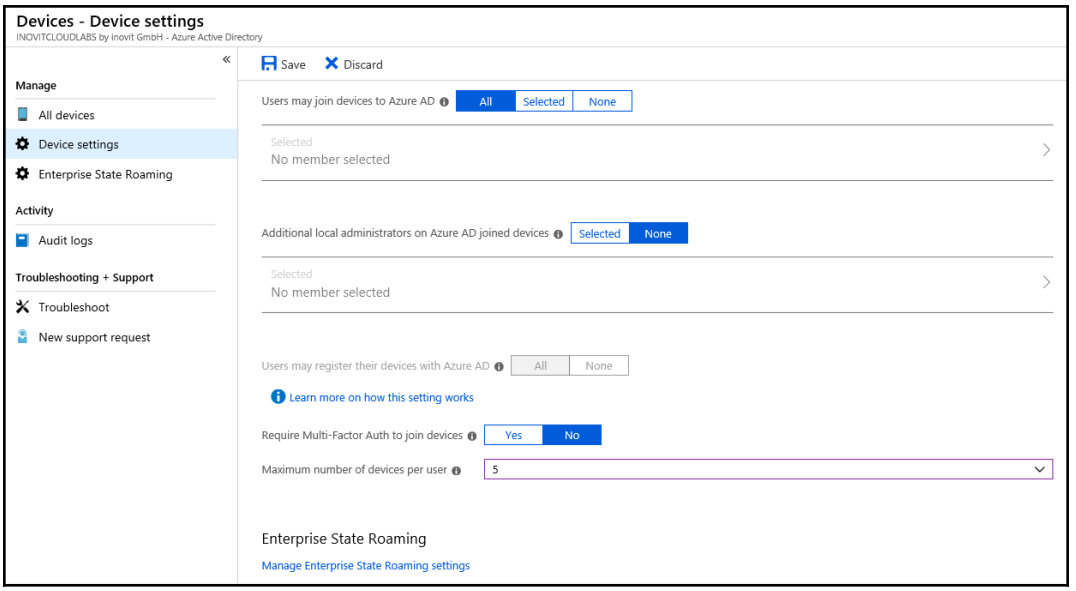

Keep your account secure
Sometimes your organization needs more info to make sure it's you. Set up the security info below so you can prove who you are.
Authenticator app
Set up your mobile app and approve a notification
Set up
Choose security info
Get help
Cancel

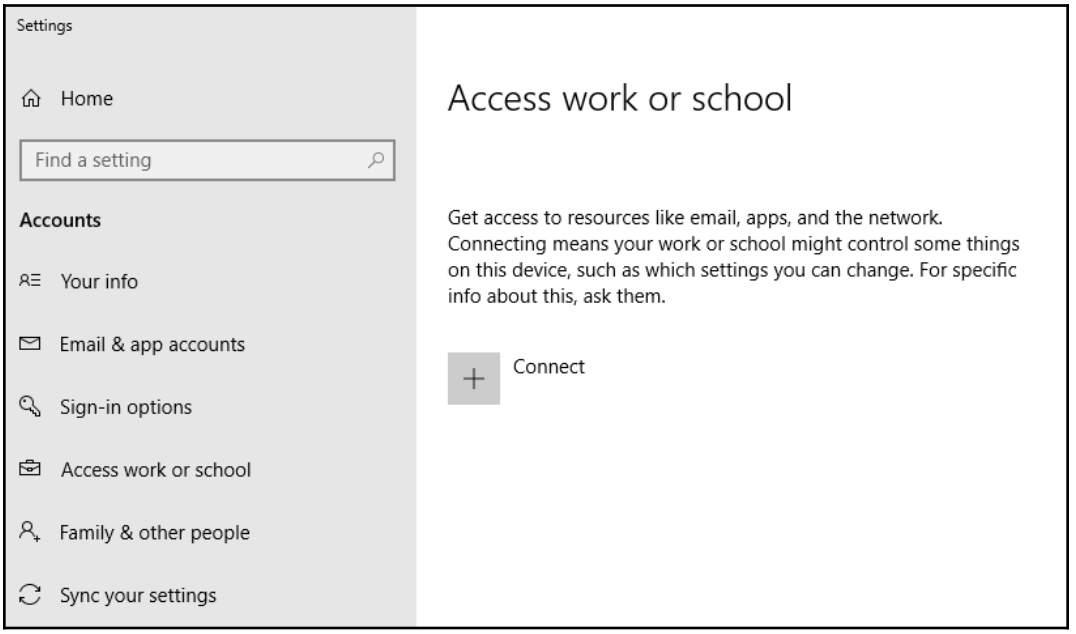

Dashboard > INOVITCLOUDLABS by inovit GmbH > Authentication methods (Preview) - Password protection (Preview)
Authentication methods (Preview) - Password protection (Preview)
INOVITCLOUDLABS by inovit GmbH - Azure AD Security
Save
Discard
Manage
Password protection (Preview)
Custom smart lockout
Lockout threshold
10
Lockout duration in seconds
60
Custom banned passwords
Enforce custom list
Yes
No
Custom banned password list
Password protection for Windows Server Active Directory
Enable password protection on Windows Server Active Directory
Yes
No
Mode
Enforced
Audit

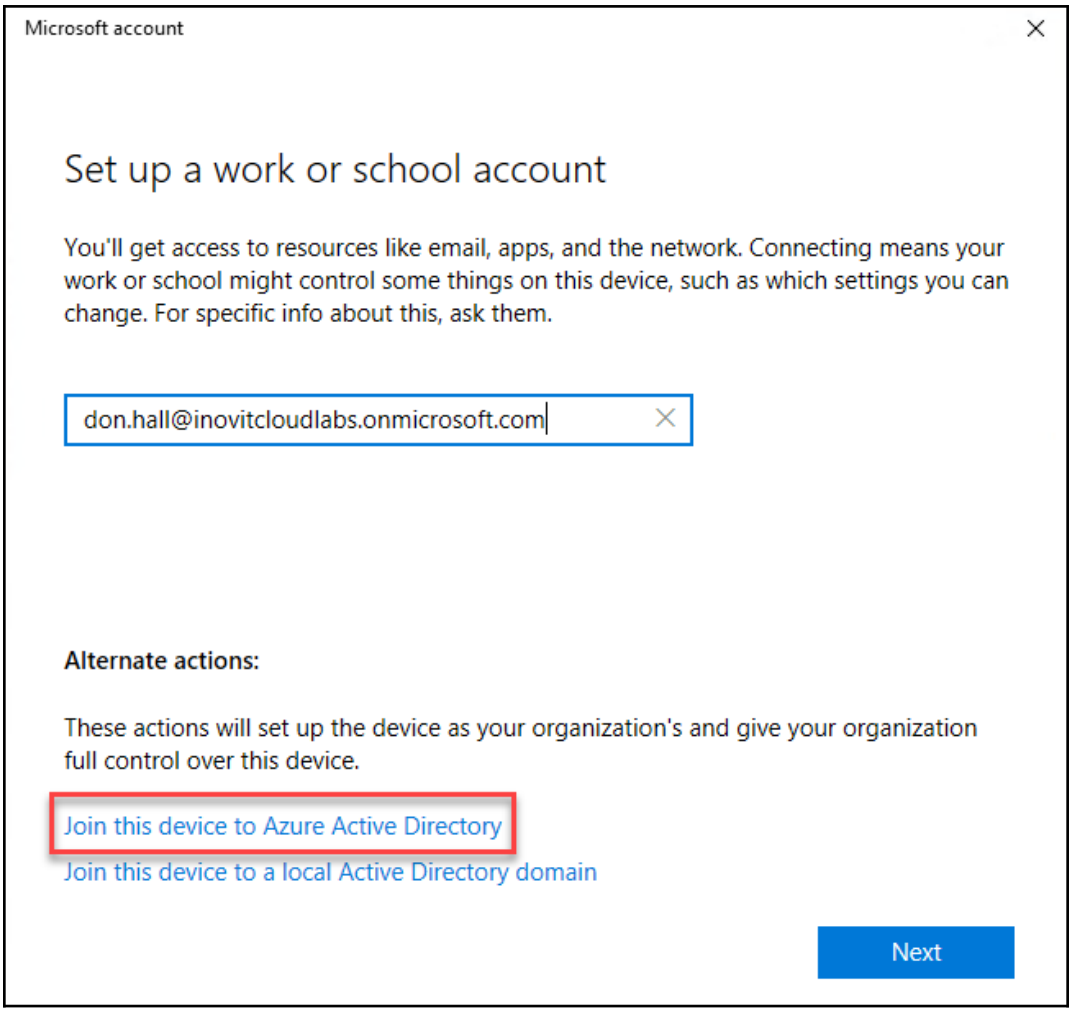

INOVIT
petro.mitchell@inovitcloudlabs.onmicrosoft.com
Enter password
Your account is temporarily locked to prevent unauthorized use. Try again later, and if you still have trouble, contact your admin.
Password
Forgot my password

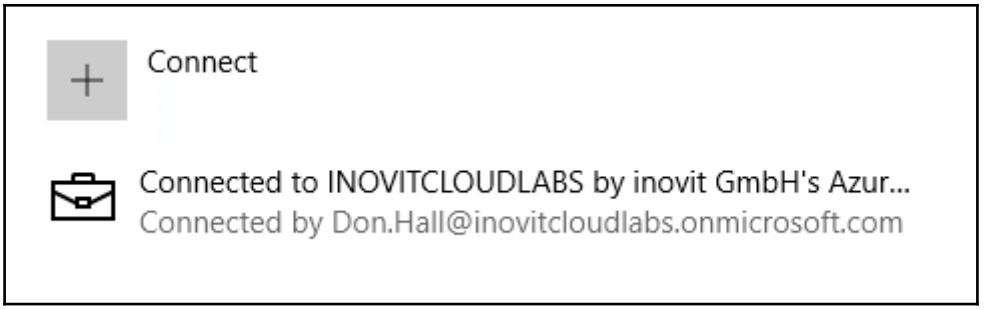

Basic info
Device info
MFA info
Conditional Access
Troubleshooting and support
Request Id
ab8765ed-ae19-492c-afe3-74891fa90e00
Correlation Id
f8cc12a3-f60d-49cc-8e0f-4d8edc7fb469
User
Petro Mitchell
Username
petro.mitchell@inovitcloudlabs.onmicrosoft.com
User ID
dbbb8ca7-1280-4afd-9e94-77d5fbec6a95
Application
Microsoft App Access Panel
Application ID
0000000c-0000-0000-c000-000000000000
IP address
77.58.235.145
Location
Killwangen, Aargau, CH
Date
12/2/2018 7:42:35 PM
Status
Failure
Sign-in error code
50053
Failure reason
Account is locked because user tried to sign in too many times with an incorrect user ID or password.
Client App

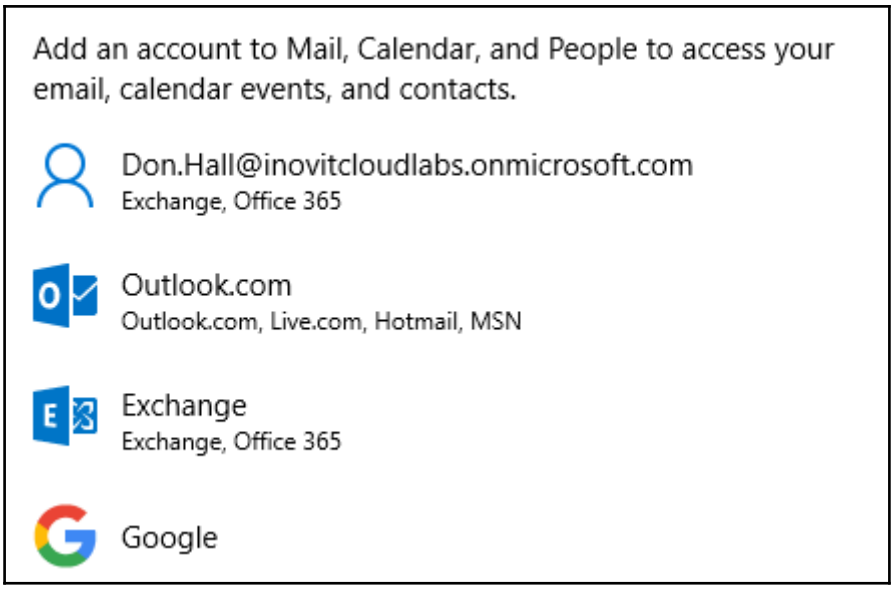

Don Hall
All sign-ins
Reset password
Dismiss all events
Essentials
Risk level
Secured
Status
Remediated
Role
User
Contact
Don.Hall@inovitcloudlabs.onmicrosoft.co...
Location
CH
MFA registered
Yes
Department
N/A
Object Id
44fb9355-0a23-4487-8059-206b62da16a6
Risk events
1
0
09/04
09/22
10/10
10/28
11/15
High
0
Medium
1
Low
0
Closed
0
TIME (UTC)
IP ADDRESS
RISK EVENT TYPE
RISK LEVEL
12/2/2018 6:49 ...
176.10.99.200
Sign-in from anonymous IP address
Medium

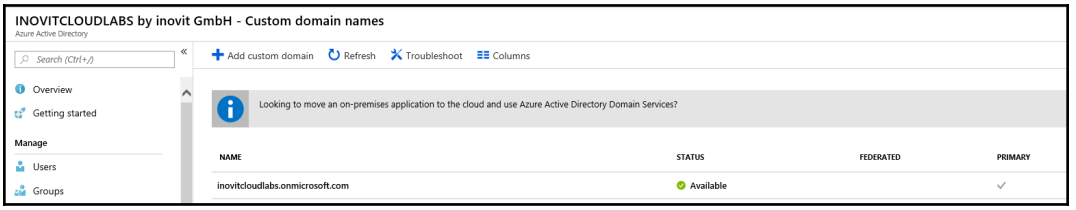

Devices - Device settings
INOVITCLOUDLABS by inovit GmbH - Azure Active Directory
Save
Discard
Manage
All devices
Device settings
Enterprise State Roaming
Activity
Audit logs
Troubleshooting + Support
Troubleshoot
New support request
Users may join devices to Azure AD
All
Selected
None
Selected
No member selected
Additional local administrators on Azure AD joined devices
Selected
None
Selected
No member selected
Users may register their devices with Azure AD
All
None
Learn more on how this setting works
Require Multi-Factor Auth to join devices
Yes
No
Maximum number of devices per user
5
Enterprise State Roaming
Manage Enterprise State Roaming settings

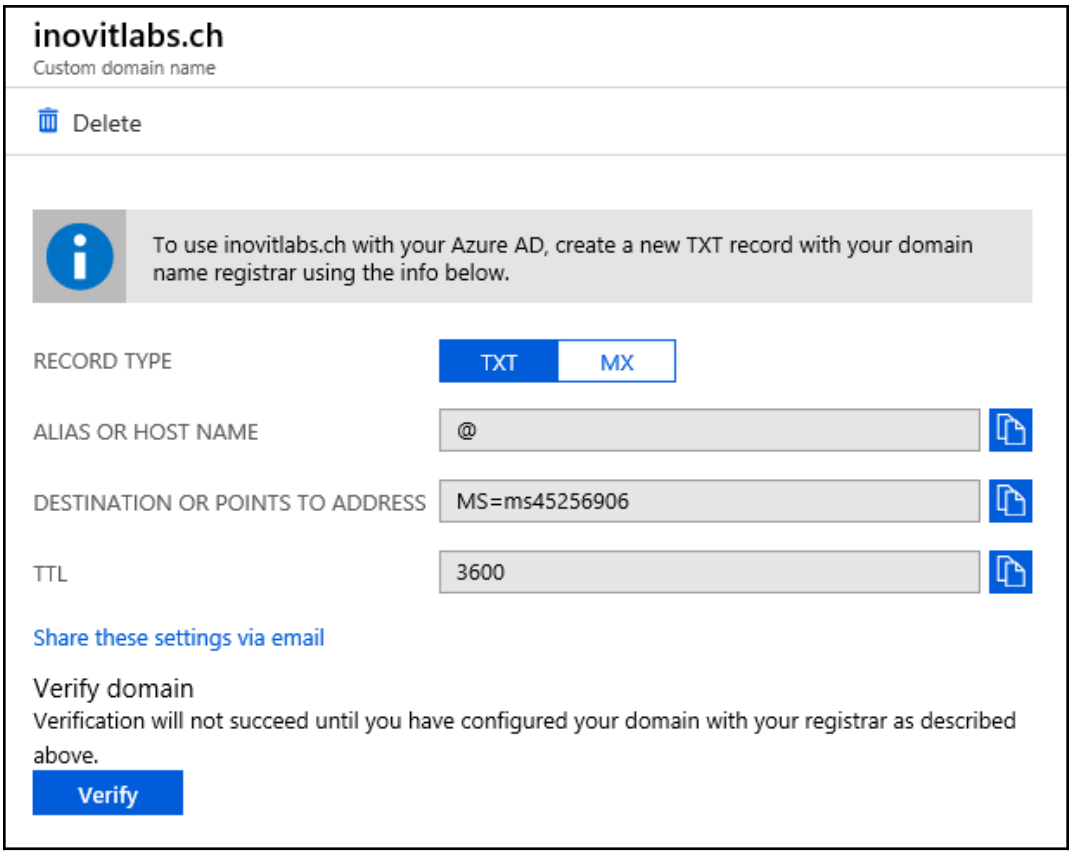

Settings
Home
Find a setting
Accounts
Your info
Email & app accounts
Sign-in options
Access work or school
Family & other people
Sync your settings
Access work or school
Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.
Connect

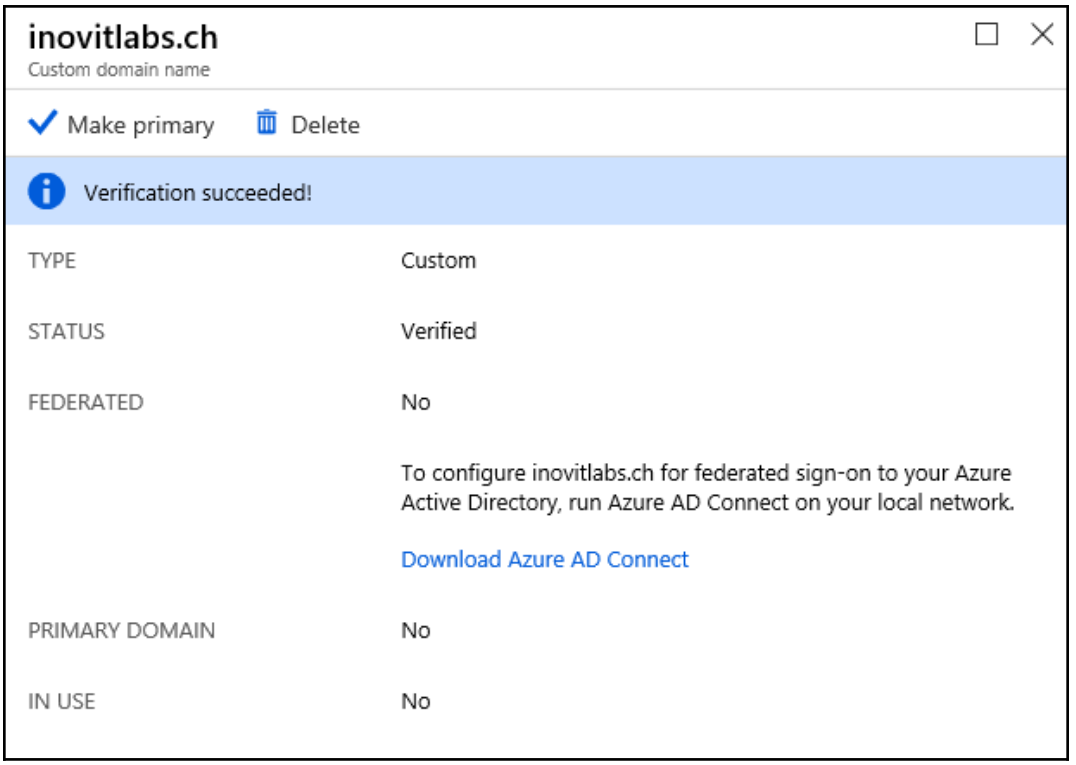

Microsoft account
Set up a work or school account
You'll get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.
don.hall@inovitcloudlabs.onmicrosoft.com
Alternate actions:
These actions will set up the device as your organization's and give your organization full control over this device.
Join this device to Azure Active Directory
Join this device to a local Active Directory domain
Next

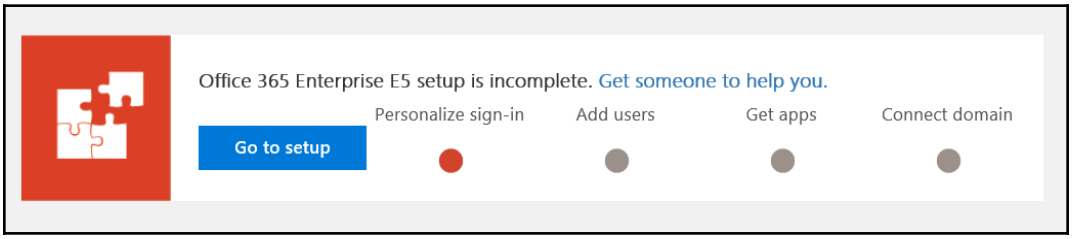

Connect
Connected to INOVITCLOUDLABS by inovit GmbH's Azur...
Connected by Don.Hall@inovitcloudlabs.onmicrosoft.com

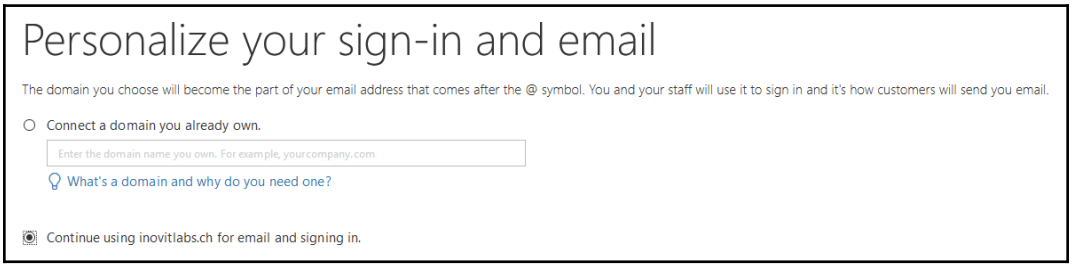

Add an account to Mail, Calendar, and People to access your email, calendar events, and contacts.
Don.Hall@inovitcloudlabs.onmicrosoft.com
Exchange, Office 365
Outlook.com
Outlook.com, Live.com, Hotmail, MSN
Exchange
Exchange, Office 365
Google

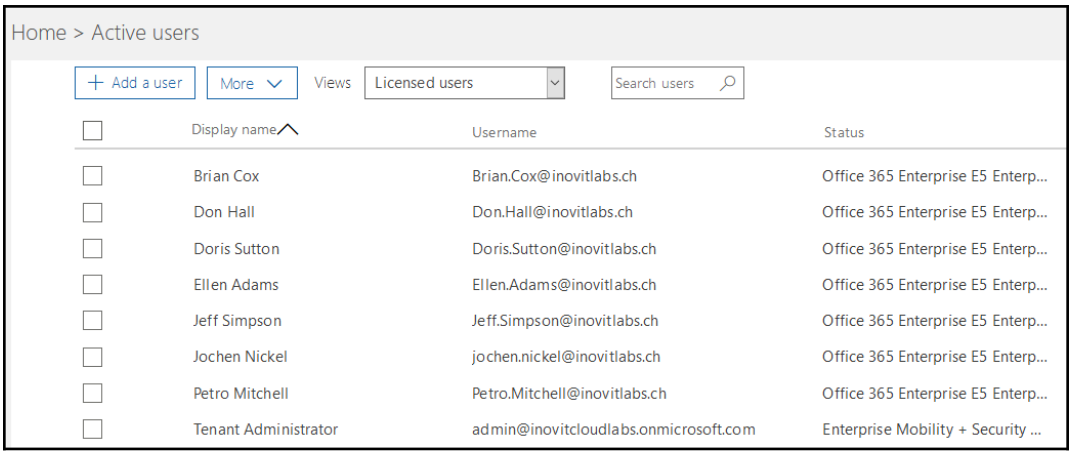

INOVITCLOUDLABS by inovit GmbH - Custom domain names
Azure Active Directory
Search (Ctrl+/)
Overview
Getting started
Manage
Users
Groups
Add custom domain
Refresh
Troubleshoot
Columns
Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?
NAME
STATUS
FEDERATED
PRIMARY
inovitcloudlabs.onmicrosoft.com
Available

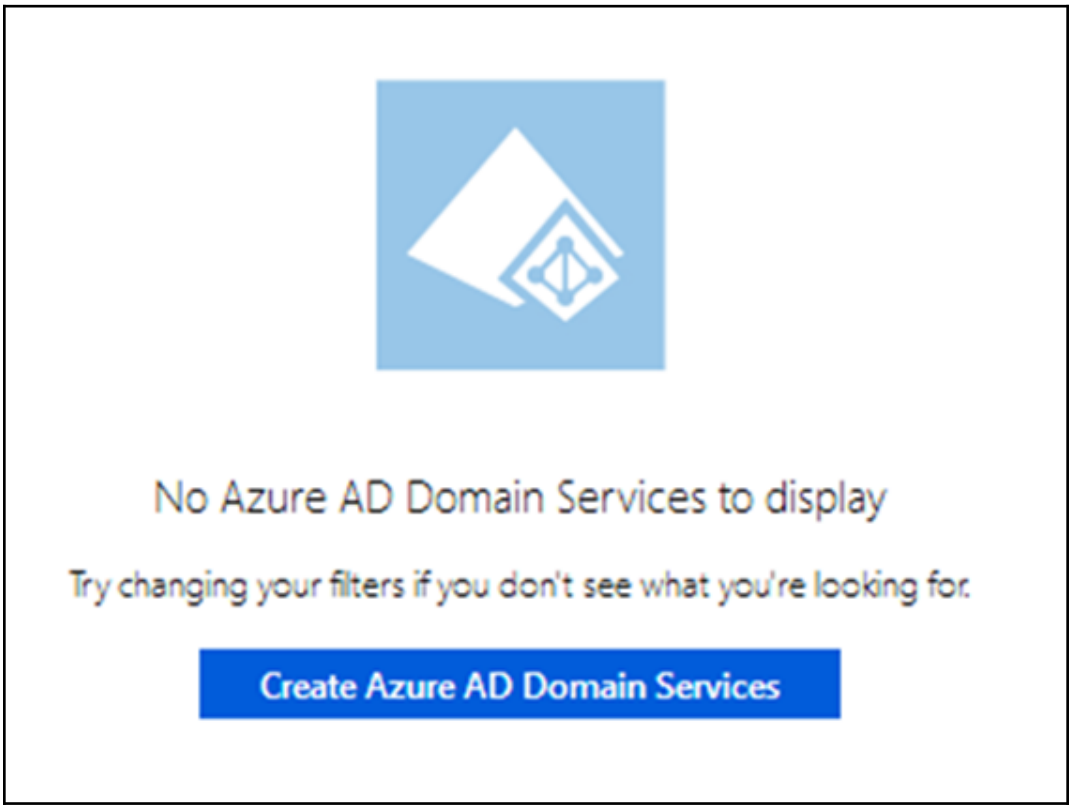

inovitlabs.ch
Custom domain name
Delete
To use inovitlabs.ch with your Azure AD, create a new TXT record with your domain name registrar using the info below.
RECORD TYPE
TXT
MX
ALIAS OR HOST NAME
@
DESTINATION OR POINTS TO ADDRESS
MS=ms45256906
TTL
3600
Share these settings via email
Verify domain
Verification will not succeed until you have configured your domain with your registrar as described above.
Verify

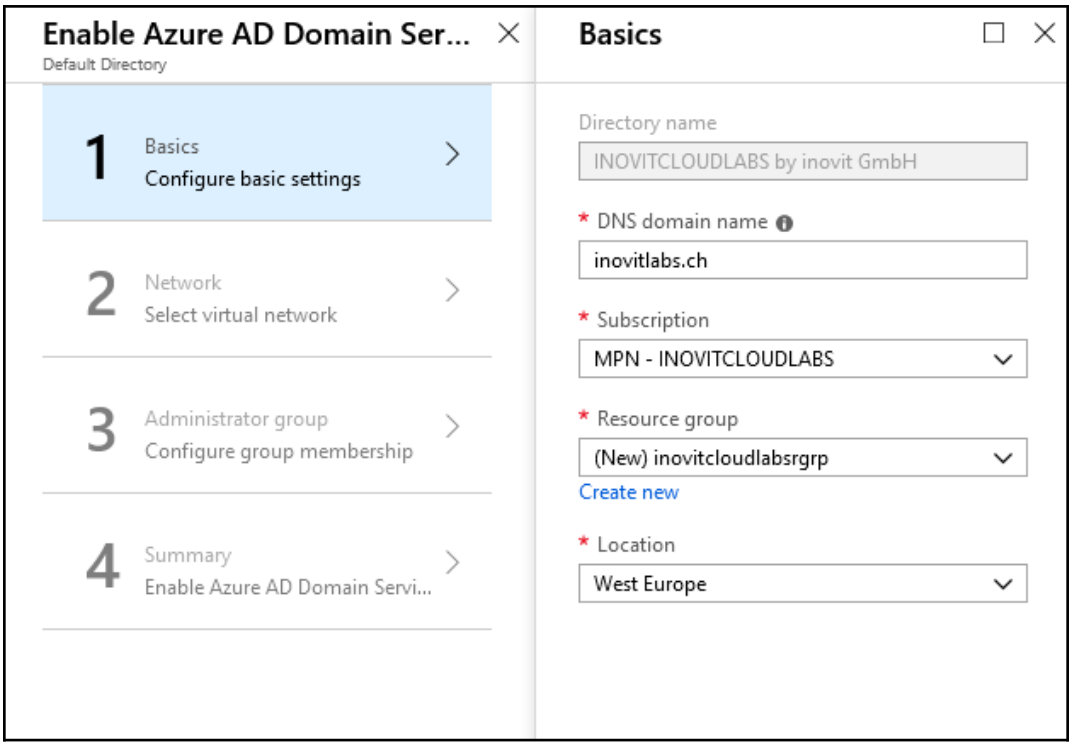

inovitlabs.ch
Custom domain name
Make primary
Delete
Verification succeeded!
TYPE
Custom
STATUS
Verified
FEDERATED
No
To configure inovitlabs.ch for federated sign-on to your Azure Active Directory, run Azure AD Connect on your local network.
Download Azure AD Connect
PRIMARY DOMAIN
No
IN USE
No

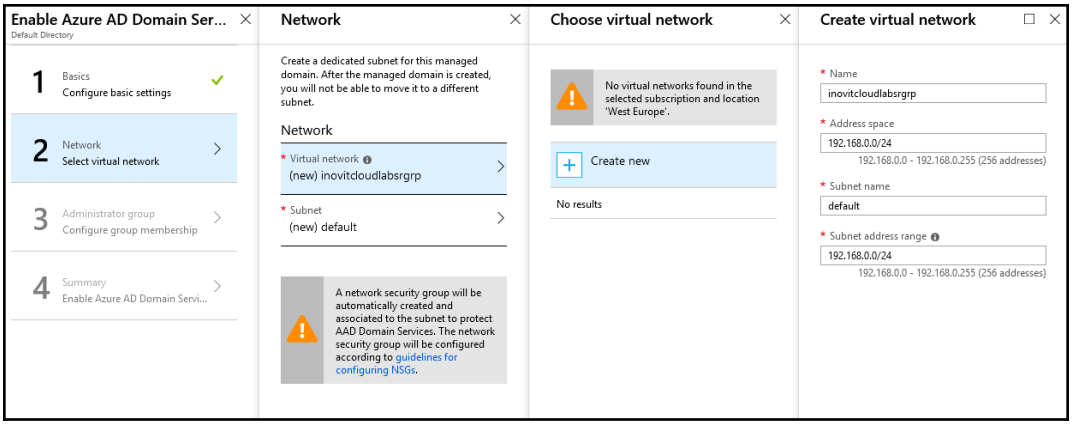

Office 365 Enterprise E5 setup is incomplete. Get someone to help you.
Go to setup
Personalize sign-in
Add users
Get apps
Connect domain

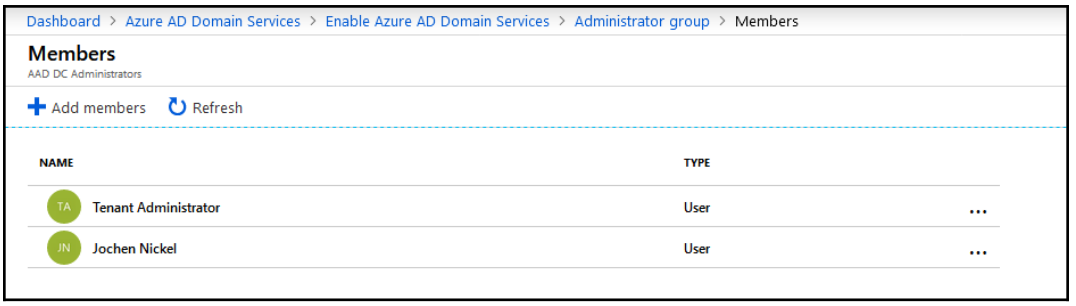

Personalize your sign-in and email
The domain you choose will become the part of your email address that comes after the @ symbol. You and your staff will use it to sign in and it's how customers will send you email.
Connect a domain you already own.
Enter the domain name you own. For example, yourcompany.com
What's a domain and why do you need one?
Continue using inovitlabs.ch for email and signing in.


Home > Active users
+ Add a user
More
Views
Licensed users
Search users
Display name
Username
Status
Brian Cox
Brian.Cox@inovitlabs.ch
Office 365 Enterprise E5 Enterp...
Don Hall
Don.Hall@inovitlabs.ch
Office 365 Enterprise E5 Enterp...
Doris Sutton
Doris.Sutton@inovitlabs.ch
Office 365 Enterprise E5 Enterp...
Ellen Adams
Ellen.Adams@inovitlabs.ch
Office 365 Enterprise E5 Enterp...
Jeff Simpson
Jeff.Simpson@inovitlabs.ch
Office 365 Enterprise E5 Enterp...
Jochen Nickel
jochen.nickel@inovitlabs.ch
Office 365 Enterprise E5 Enterp...
Petro Mitchell
Petro.Mitchell@inovitlabs.ch
Office 365 Enterprise E5 Enterp...
Tenant Administrator
admin@inovitcloudlabs.onmicrosoft.com
Enterprise Mobility + Security ...


No Azure AD Domain Services to display
Try changing your filters if you don't see what you're looking for.
Create Azure AD Domain Services


Enable Azure AD Domain Ser...
Default Directory
1 Basics
Configure basic settings
2 Network
Select virtual network
3 Administrator group
Configure group membership
4 Summary
Enable Azure AD Domain Servi...
Basics
Directory name
INOVITCLOUDLABS by inovit GmbH
* DNS domain name
inovitlabs.ch
* Subscription
MPN - INOVITCLOUDLABS
* Resource group
(New) inovitcloudlabsrgrp
Create new
* Location
West Europe


Enable Azure AD Domain Ser...
Default Directory
1 Basics
Configure basic settings
2 Network
Select virtual network
3 Administrator group
Configure group membership
4 Summary
Enable Azure AD Domain Servi...
Network
Create a dedicated subnet for this managed domain. After the managed domain is created, you will not be able to move it to a different subnet.
Network
* Virtual network
(new) inovitcloudlabsrgrp
* Subnet
(new) default
A network security group will be automatically created and associated to the subnet to protect AAD Domain Services. The network security group will be configured according to guidelines for configuring NSGs.
Choose virtual network
No virtual networks found in the selected subscription and location 'West Europe'.
Create new
No results
Create virtual network
* Name
inovitcloudlabsrgrp
* Address space
192.168.0.0/24
192.168.0.0 - 192.168.0.255 (256 addresses)
* Subnet name
default
* Subnet address range
192.168.0.0/24
192.168.0.0 - 192.168.0.255 (256 addresses)



Basics

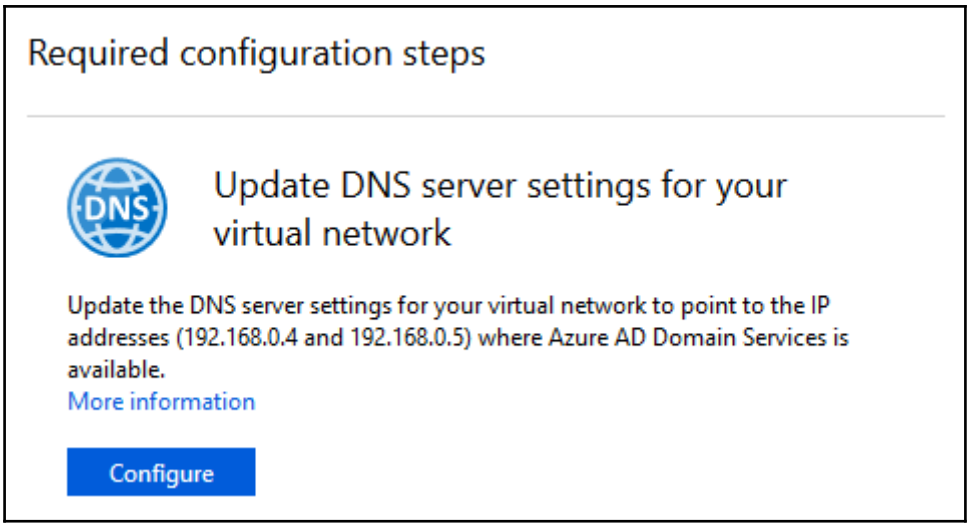
Name	inovitlabs.ch
Subscription	MPN - INOVITCLOUDLABS
Resource group	inovitcloudlabsrgrp
Location	West Europe

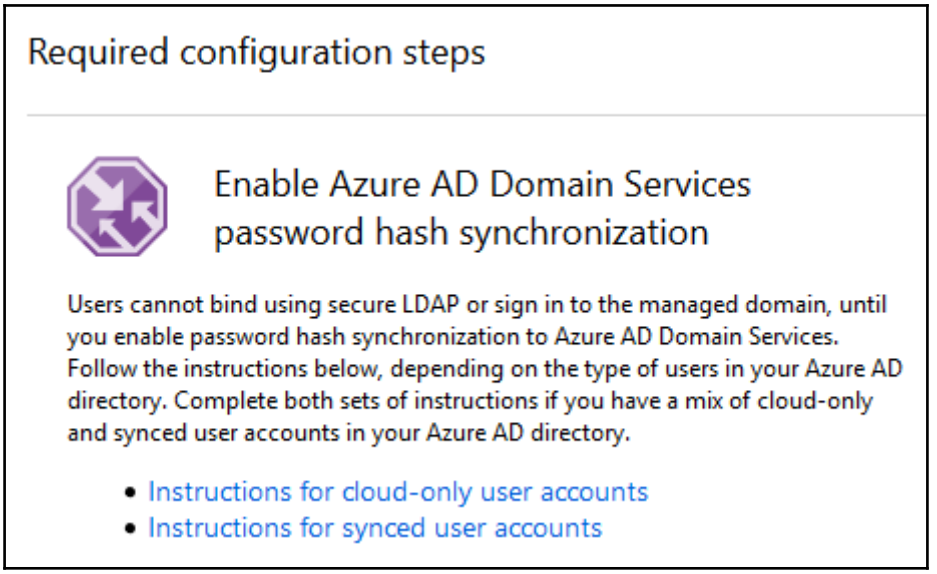
Network

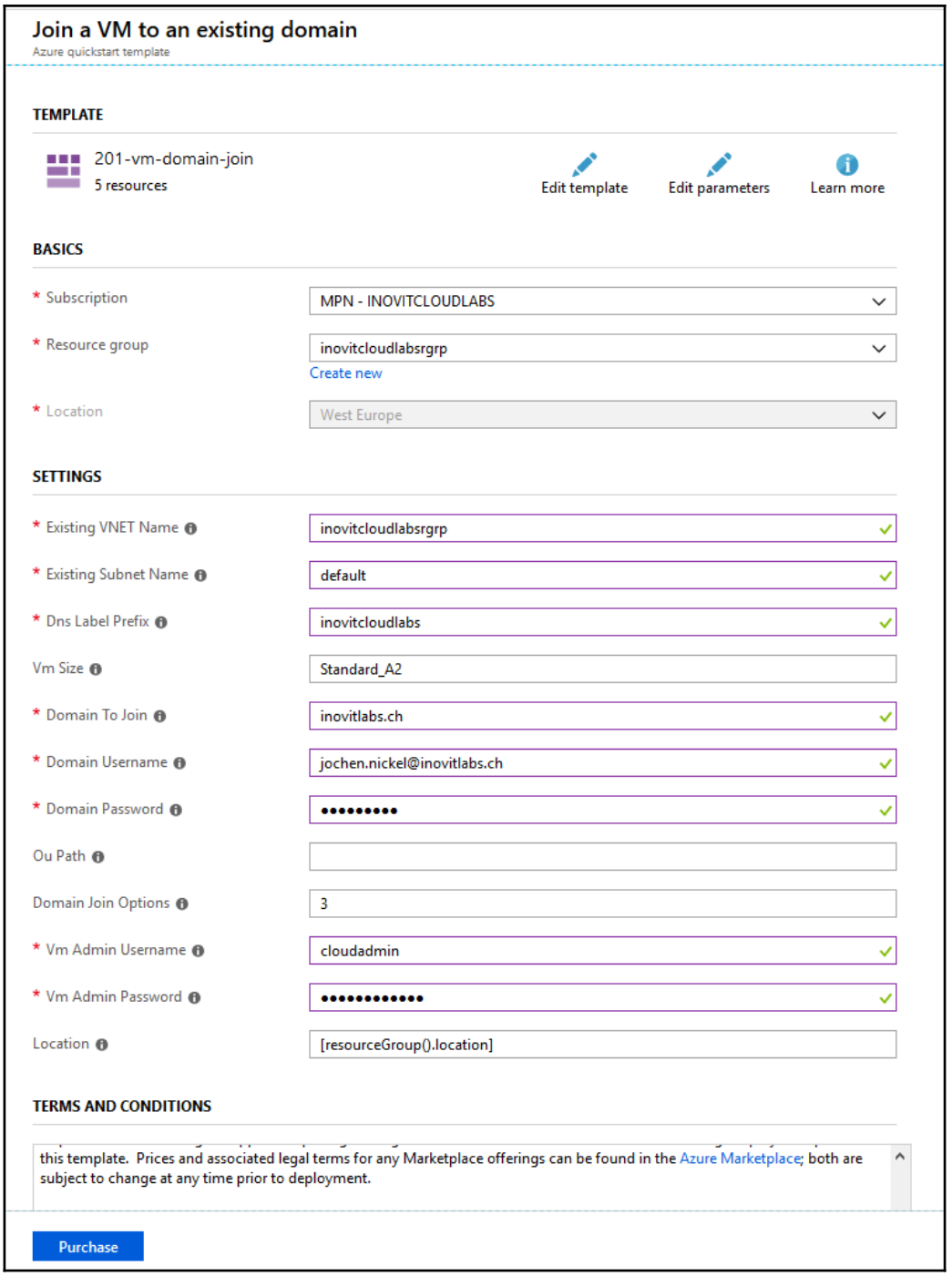
Virtual network	inovitcloudlabsrgrp
Virtual network address	192.168.0.0/24
Subnet	default
Subnet Address	192.168.0.0/24
Network security group (new)	AADDS-inovitlabs.ch-NSG

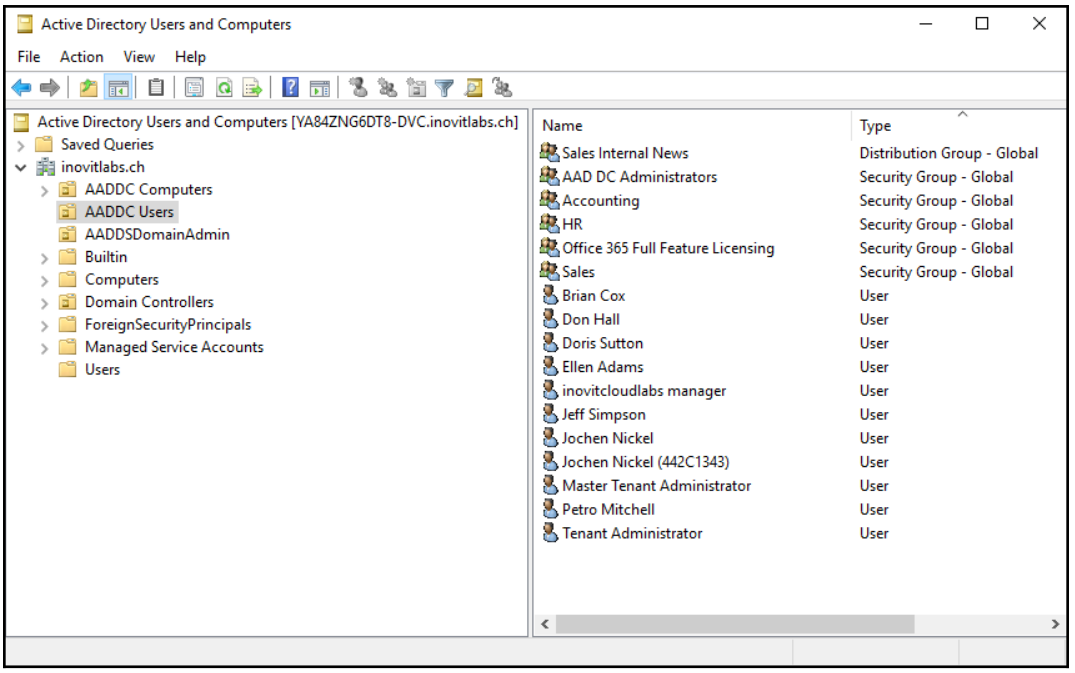
Administrator group

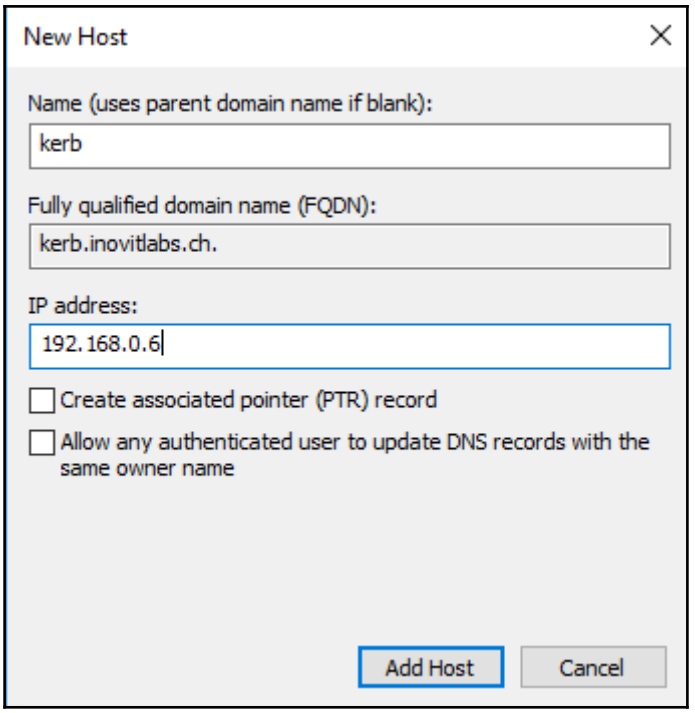
Administrator group	AAD DC Administrators
Membership Type	Assigned

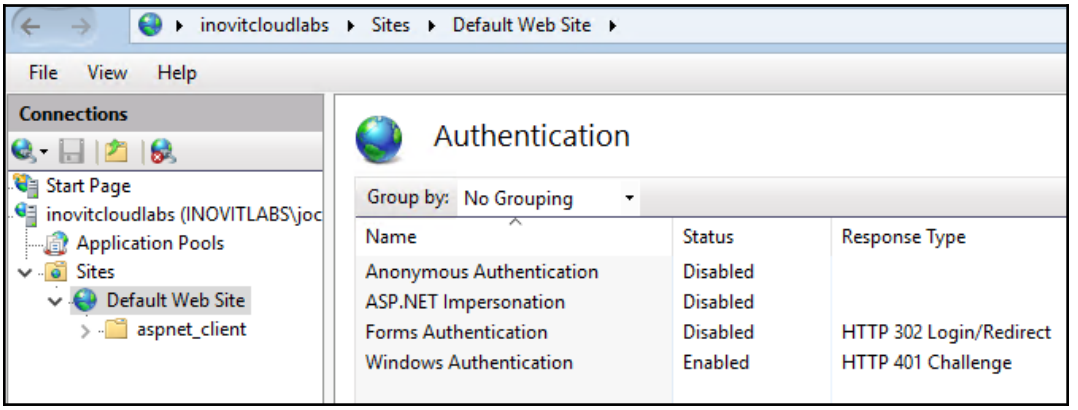

Required configuration steps
DNS
Update DNS server settings for your virtual network
Update the DNS server settings for your virtual network to point to the IP addresses (192.168.0.4 and 192.168.0.5) where Azure AD Domain Services is available.
More information
Configure

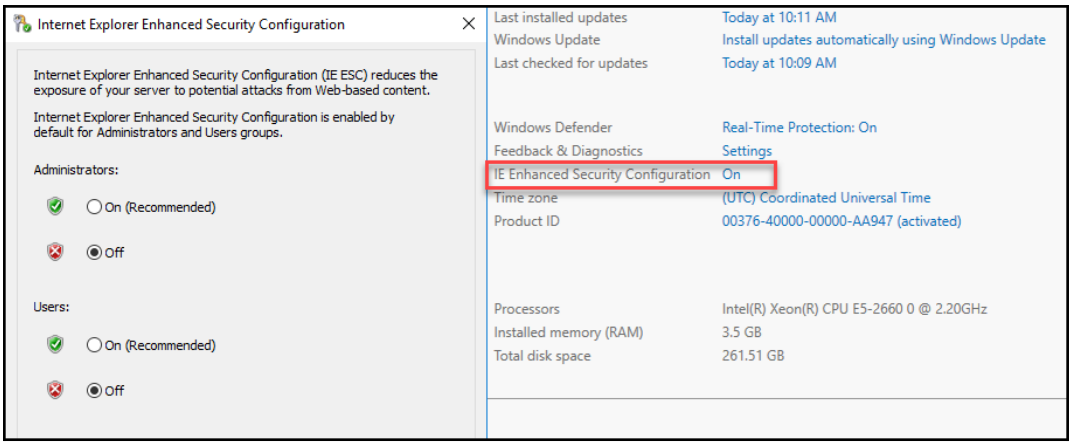

Required configuration steps
Enable Azure AD Domain Services password hash synchronization
Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory.
Instructions for cloud-only user accounts
Instructions for synced user accounts

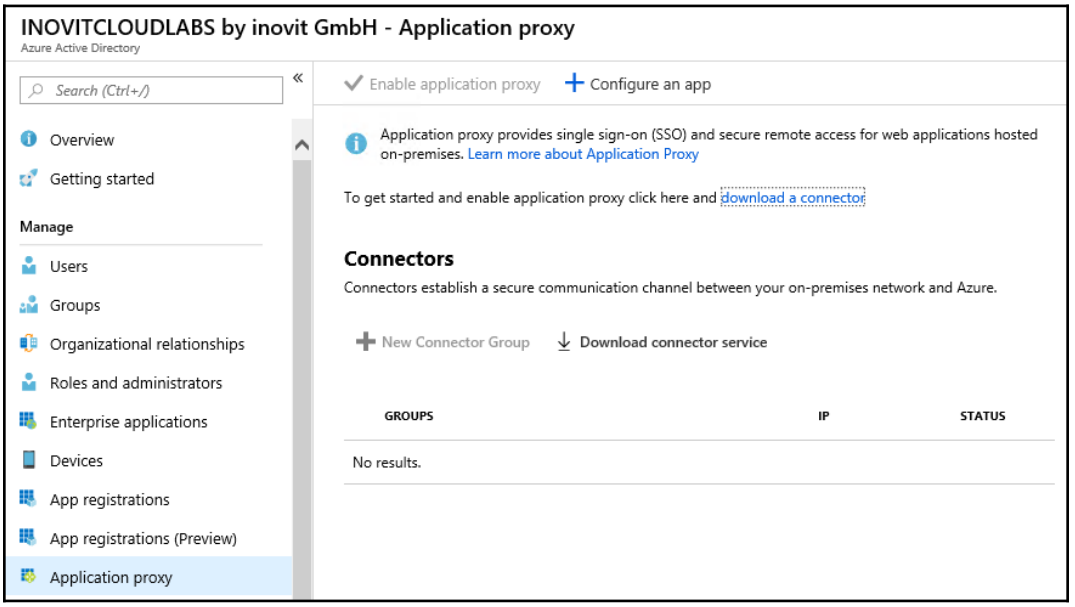

Join a VM to an existing domain
Azure quickstart template
TEMPLATE
201-vm-domain-join
5 resources
Edit template
Edit parameters
Learn more
BASICS
* Subscription
MPN - INOVITCLOUDLABS
* Resource group
inovitcloudlabsrgrp
Create new
* Location
West Europe
SETTINGS
* Existing VNET Name
inovitcloudlabsrgrp
* Existing Subnet Name
default
* Dns Label Prefix
inovitcloudlabs
Vm Size
Standard_A2
* Domain To Join
inovitlabs.ch
* Domain Username
jochen.nickel@inovitlabs.ch
* Domain Password
Ou Path
Domain Join Options
3
* Vm Admin Username
cloudadmin
* Vm Admin Password
Location
[resourceGroup().location]
TERMS AND CONDITIONS
this template. Prices and associated legal terms for any Marketplace offerings can be found in the Azure Marketplace; both are subject to change at any time prior to deployment.
Purchase

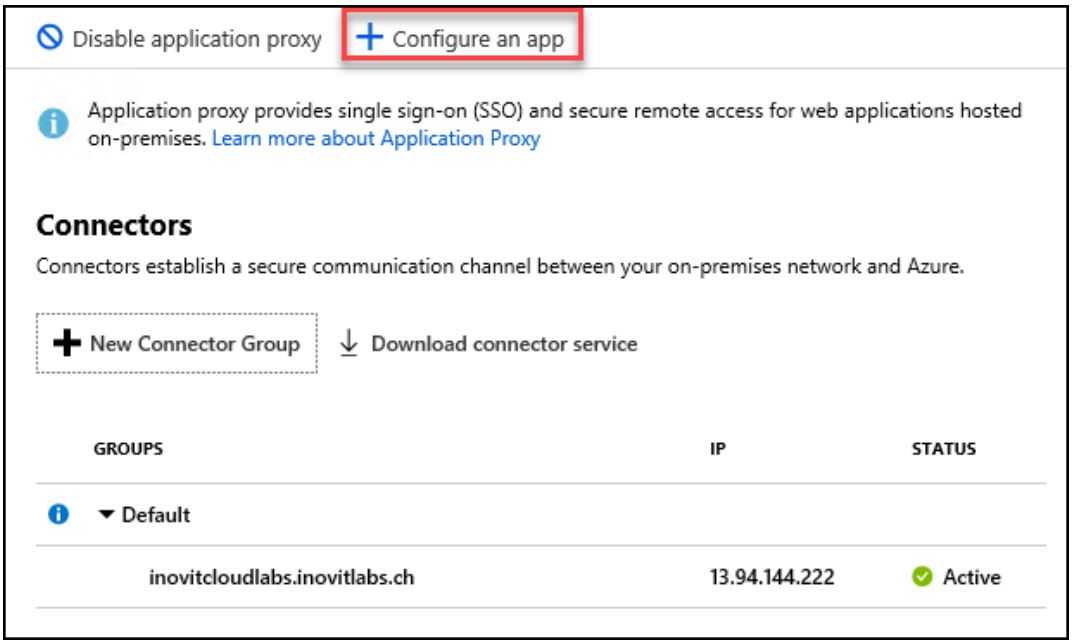

Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [YA84ZNG6DT8-DVC.inovitlabs.ch]
Saved Queries
inovitlabs.ch
AADDC Computers
AADDC Users
AADDSDomainAdmin
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Sales Internal News
Distribution Group - Global
AAD DC Administrators
Security Group - Global
Accounting
Security Group - Global
HR
Security Group - Global
Office 365 Full Feature Licensing
Security Group - Global
Sales
Security Group - Global
Brian Cox
User
Don Hall
User
Doris Sutton
User
Ellen Adams
User
inovitcloudlabs manager
User
Jeff Simpson
User
Jochen Nickel
User
Jochen Nickel (442C1343)
User
Master Tenant Administrator
User
Petro Mitchell
User
Tenant Administrator
User

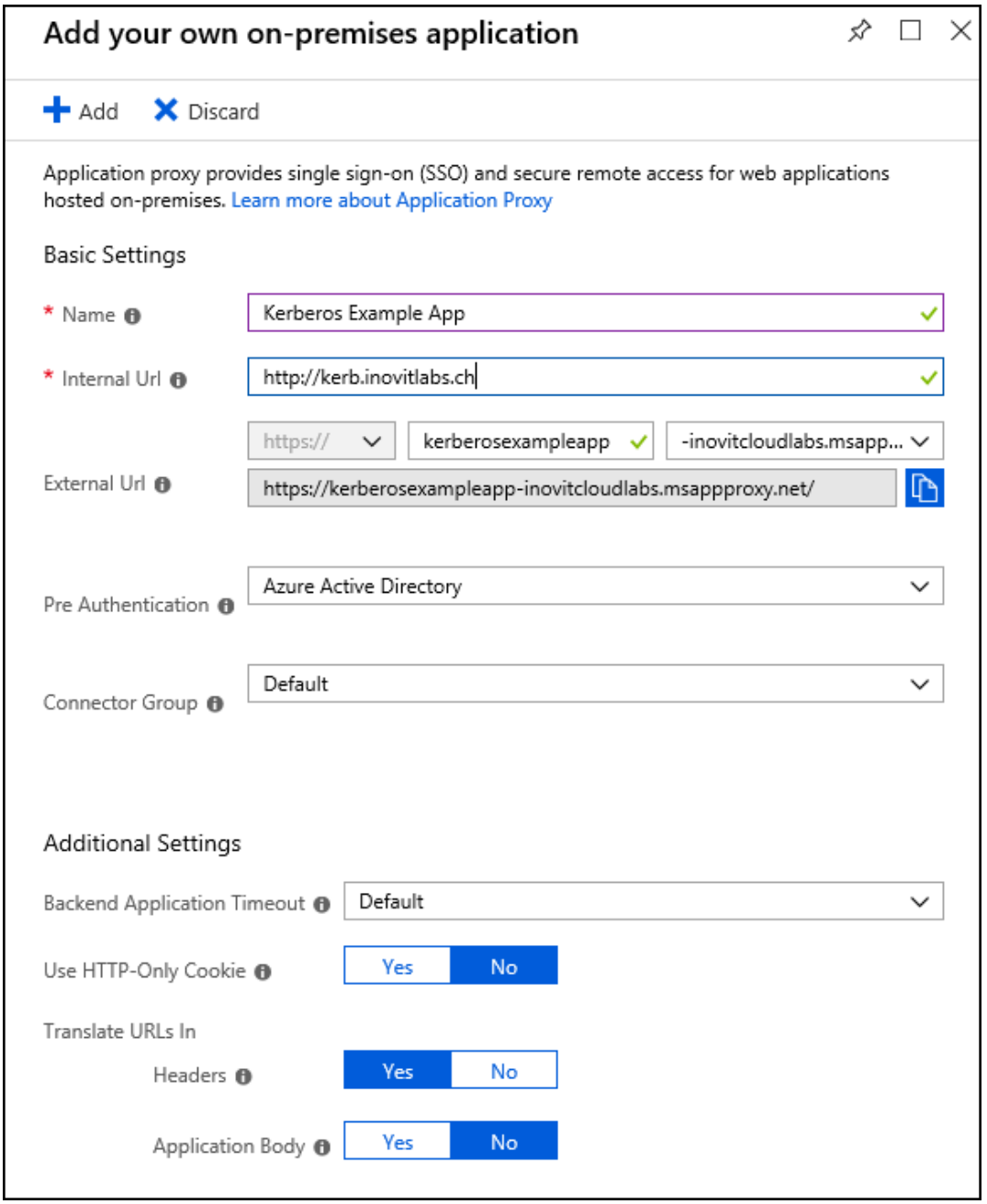

New Host
Name (uses parent domain name if blank):
kerb
Fully qualified domain name (FQDN):
kerb.inovitlabs.ch.
IP address:
192.168.0.6
Create associated pointer (PTR) record
Allow any authenticated user to update DNS records with the same owner name
Add Host
Cancel

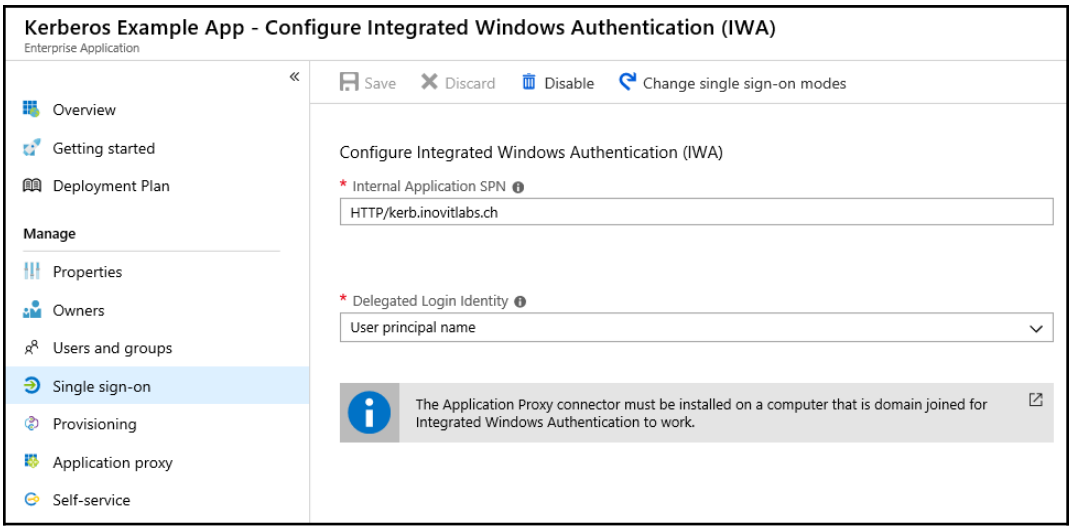

inovitcloudlabs ▸ Sites ▸ Default Web Site ▸
File View Help
Connections
Start Page
inovitcloudlabs (INOVITLABS\joc
Application Pools
Sites
Default Web Site
aspnet_client
Authentication
Group by: No Grouping
Name
Status
Response Type
Anonymous Authentication
Disabled
ASP.NET Impersonation
Disabled
Forms Authentication
Disabled
HTTP 302 Login/Redirect
Windows Authentication
Enabled
HTTP 401 Challenge


Internet Explorer Enhanced Security Configuration
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.
Administrators:
On (Recommended)
Off
Users:
On (Recommended)
Off
Last installed updates
Today at 10:11 AM
Windows Update
Install updates automatically using Windows Update
Last checked for updates
Today at 10:09 AM
Windows Defender
Real-Time Protection: On
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC) Coordinated Universal Time
Product ID
00376-40000-00000-AA947 (activated)
Processors
Intel(R) Xeon(R) CPU E5-2660 0 @ 2.20GHz
Installed memory (RAM)
3.5 GB
Total disk space
261.51 GB

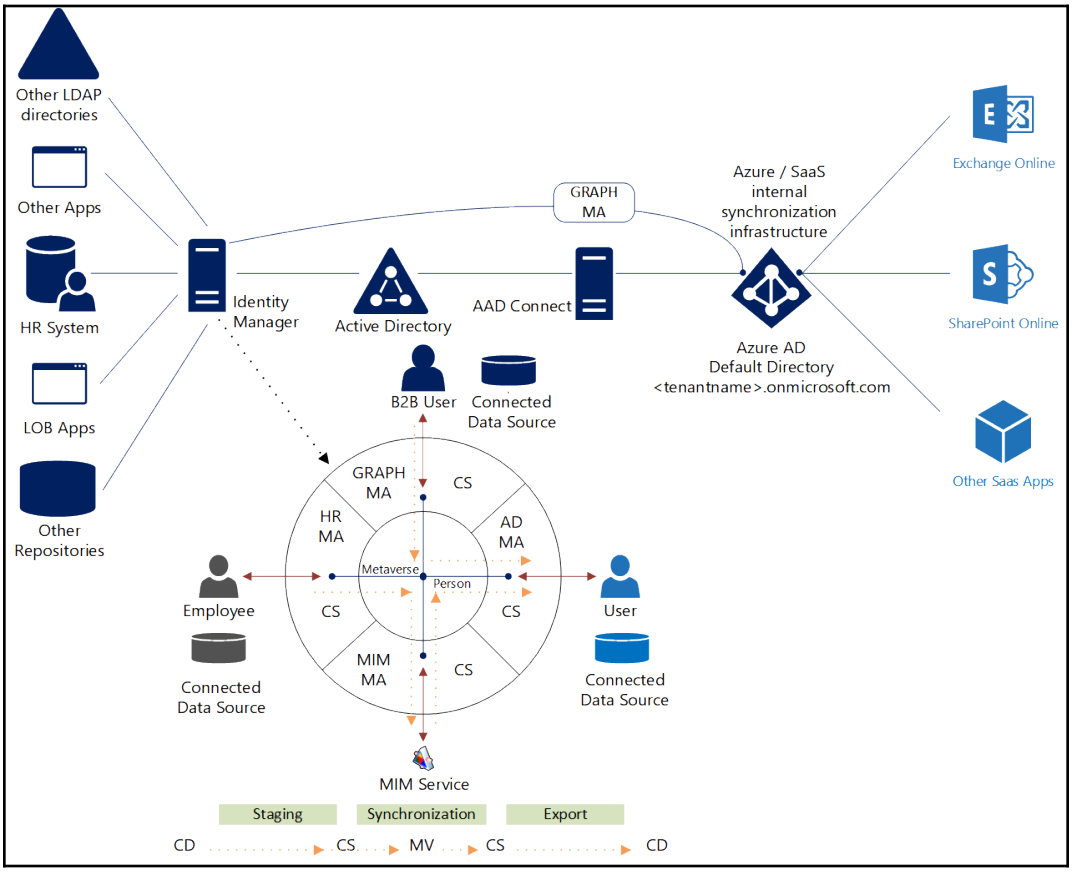

INOVITCLOUDLABS by inovit GmbH - Application proxy
Azure Active Directory
Search (Ctrl+/)
Overview
Getting started
Manage
Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Enable application proxy
Configure an app
Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy
To get started and enable application proxy click here and download a connector
Connectors
Connectors establish a secure communication channel between your on-premises network and Azure.
New Connector Group
Download connector service
GROUPS
IP
STATUS
No results.

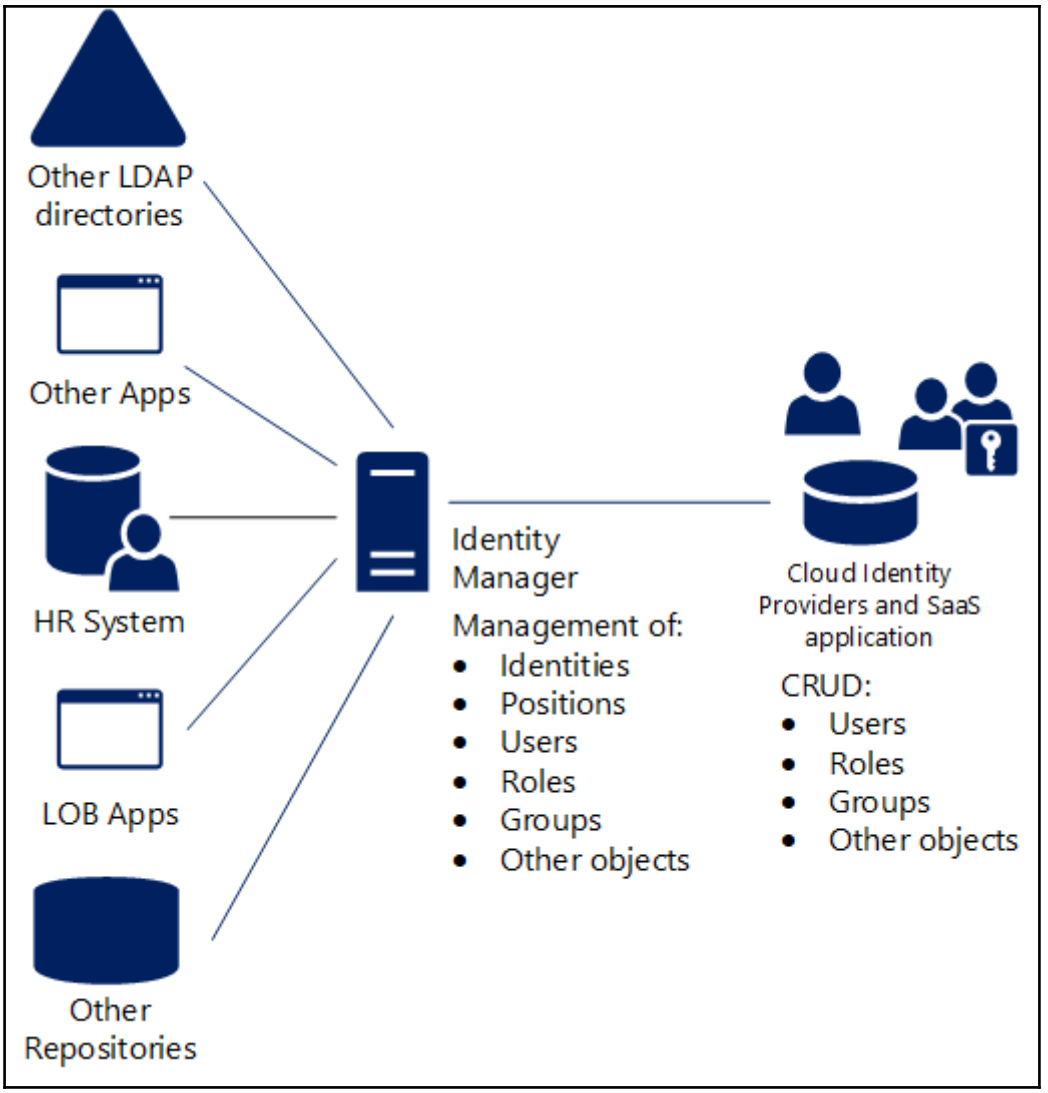

Disable application proxy
Configure an app
Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy
Connectors
Connectors establish a secure communication channel between your on-premises network and Azure.
New Connector Group
Download connector service
GROUPS
IP
STATUS
Default
inovitcloudlabs.inovitlabs.ch
13.94.144.222
Active

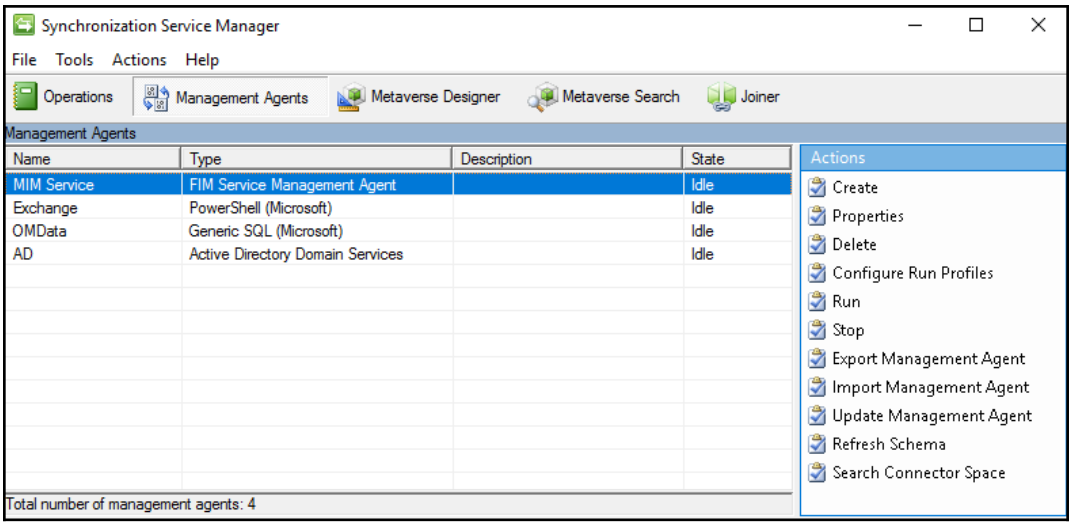

Add your own on-premises application
Add
Discard
Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy
Basic Settings
* Name
Kerberos Example App
* Internal Url
http://kerb.inovitlabs.ch
https://
kerberosexampleapp
-inovitcloudlabs.msapp...
External Url
https://kerberosexampleapp-inovitcloudlabs.msappproxy.net/
Pre Authentication
Azure Active Directory
Connector Group
Default
Additional Settings
Backend Application Timeout
Default
Use HTTP-Only Cookie
Yes
No
Translate URLs In
Headers
Yes
No
Application Body
Yes
No

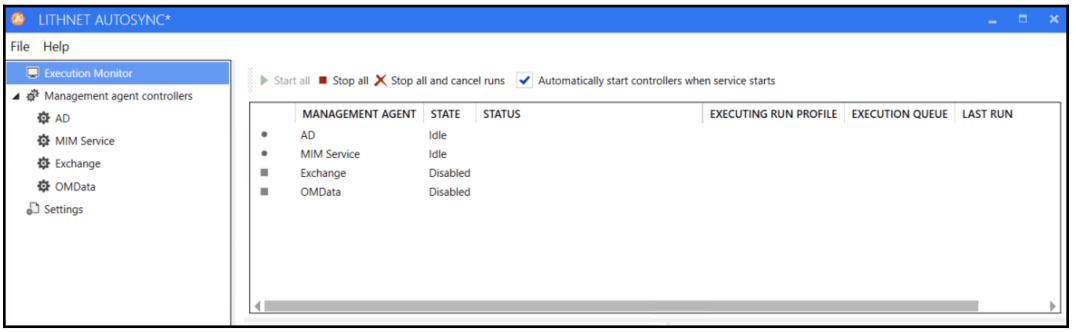

Kerberos Example App - Configure Integrated Windows Authentication (IWA)
Enterprise Application
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Save
Discard
Disable
Change single sign-on modes
Configure Integrated Windows Authentication (IWA)
* Internal Application SPN
HTTP/kerb.inovitlabs.ch
* Delegated Login Identity
User principal name
The Application Proxy connector must be installed on a computer that is domain joined for Integrated Windows Authentication to work.

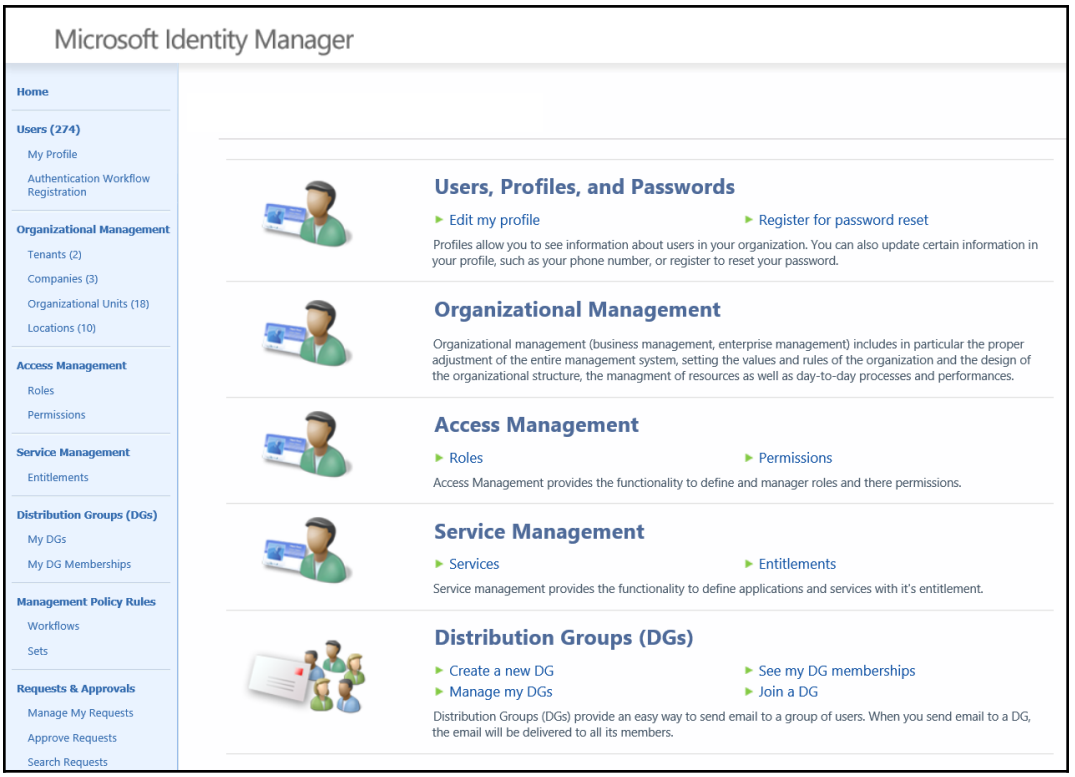
Chapter 2: Understanding Identity Synchronization

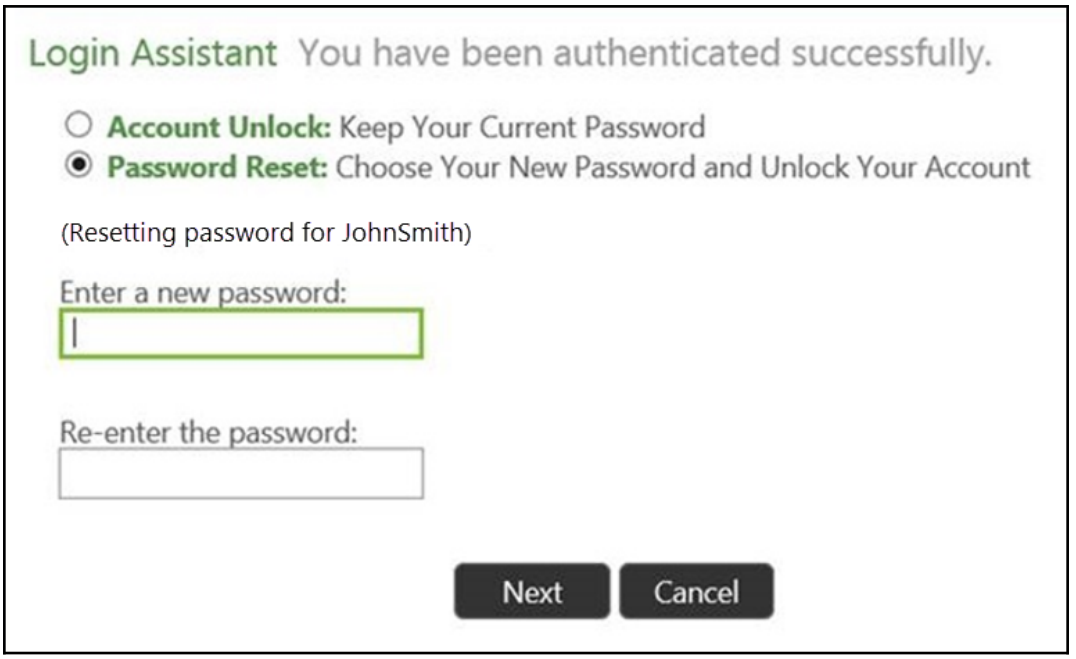


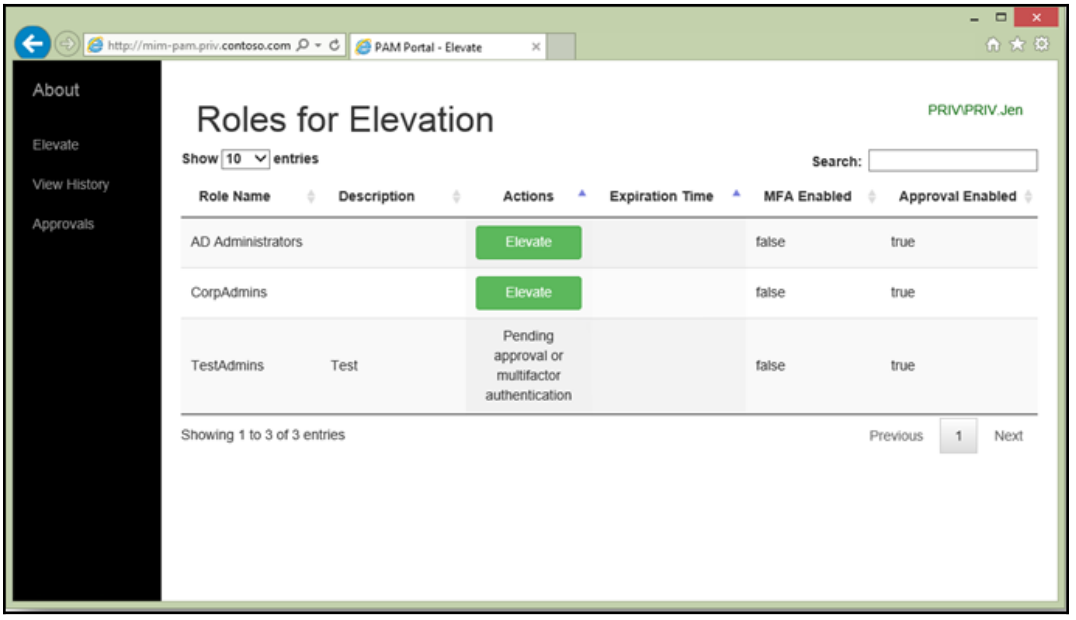

Other LDAP directories
Other Apps
HR System
LOB Apps
Other Repositories
Identity Manager
Management of:
Identities
Positions
Users
Roles
Groups
Other objects
Cloud Identity Providers and SaaS application
CRUD:
Users
Roles
Groups
Other objects


Synchronization Service Manager
File Tools Actions Help
Operations
Management Agents
Metaverse Designer
Metaverse Search
Joiner
Management Agents
Name
Type
Description
State
MIM Service
FIM Service Management Agent
Idle
Exchange
PowerShell (Microsoft)
Idle
OMData
Generic SQL (Microsoft)
Idle
AD
Active Directory Domain Services
Idle
Total number of management agents: 4
Actions
Create
Properties
Delete
Configure Run Profiles
Run
Stop
Export Management Agent
Import Management Agent
Update Management Agent
Refresh Schema
Search Connector Space

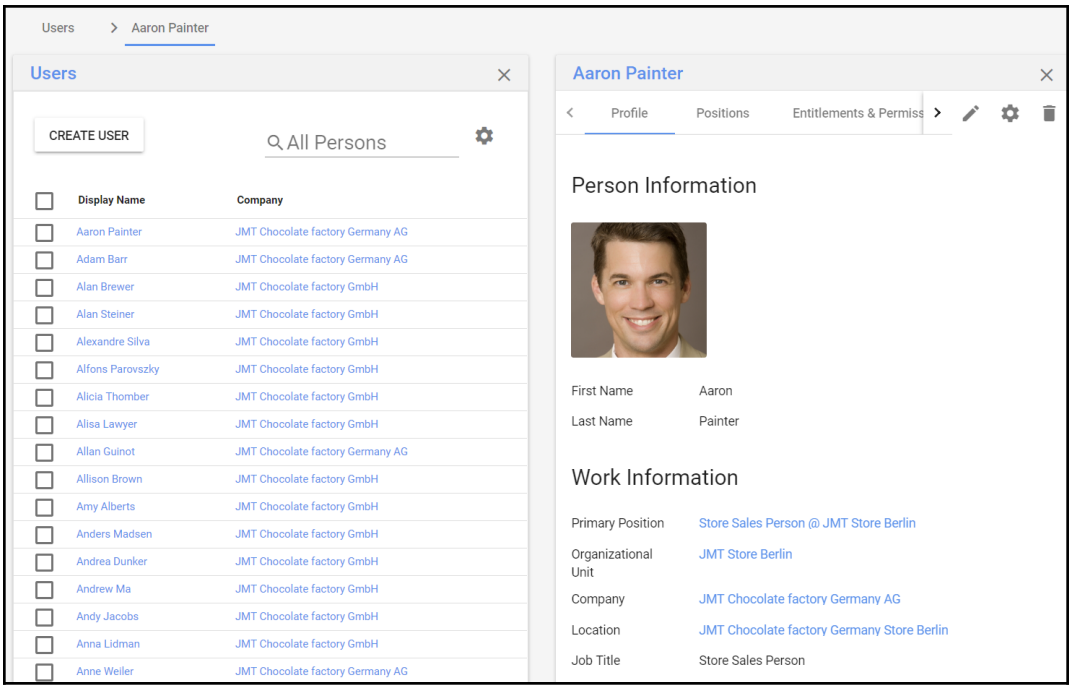

LITHNET AUTOSYNC*
File Help
Execution Monitor
Management agent controllers
AD
MIM Service
Exchange
OMData
Settings
Start all
Stop all
Stop all and cancel runs
Automatically start controllers when service starts
MANAGEMENT AGENT
STATE
STATUS
EXECUTING RUN PROFILE
EXECUTION QUEUE
LAST RUN
AD
Idle
MIM Service
Idle
Exchange
Disabled
OMData
Disabled

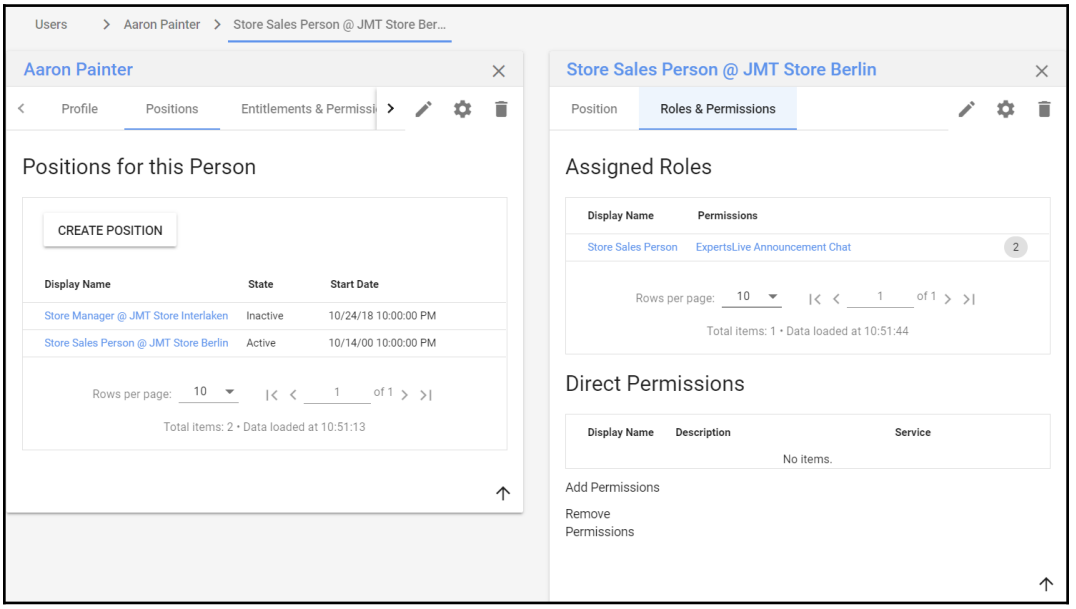

Microsoft Identity Manager
Home
Users (274)
My Profile
Authentication Workflow Registration
Organizational Management
Tenants (2)
Companies (3)
Organizational Units (18)
Locations (10)
Access Management
Roles
Permissions
Service Management
Entitlements
Distribution Groups (DGs)
My DGs
My DG Memberships
Management Policy Rules
Workflows
Sets
Requests & Approvals
Manage My Requests
Approve Requests
Search Requests
Users, Profiles, and Passwords
Edit my profile
Register for password reset
Profiles allow you to see information about users in your organization. You can also update certain information in your profile, such as your phone number, or register to reset your password.
Organizational Management
Organizational management (business management, enterprise management) includes in particular the proper adjustment of the entire management system, setting the values and rules of the organization and the design of the organizational structure, the managment of resources as well as day-to-day processes and performances.
Access Management
Roles
Permissions
Access Management provides the functionality to define and manager roles and there permissions.
Service Management
Services
Entitlements
Service management provides the functionality to define applications and services with it's entitlement.
Distribution Groups (DGs)
Create a new DG
See my DG memberships
Manage my DGs
Join a DG
Distribution Groups (DGs) provide an easy way to send email to a group of users. When you send email to a DG, the email will be delivered to all its members.

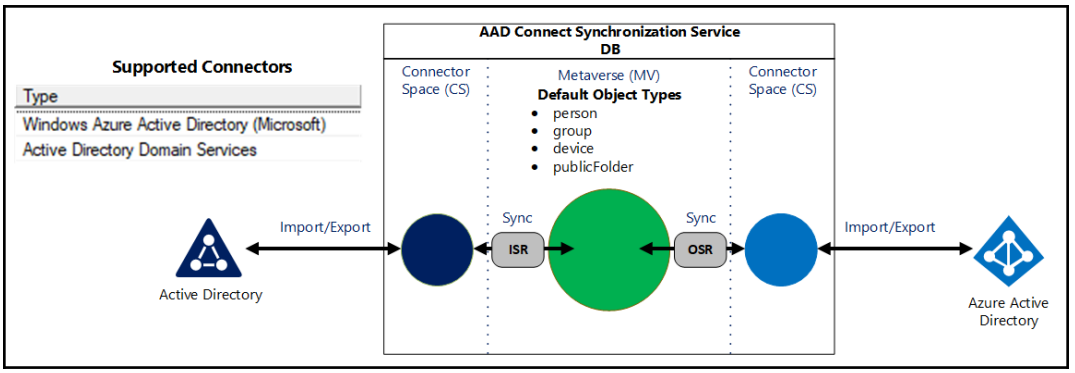

Login Assistant You have been authenticated successfully.
Account Unlock: Keep Your Current Password
Password Reset: Choose Your New Password and Unlock Your Account
(Resetting password for JohnSmith)
Enter a new password:
Re-enter the password:
Next
Cancel

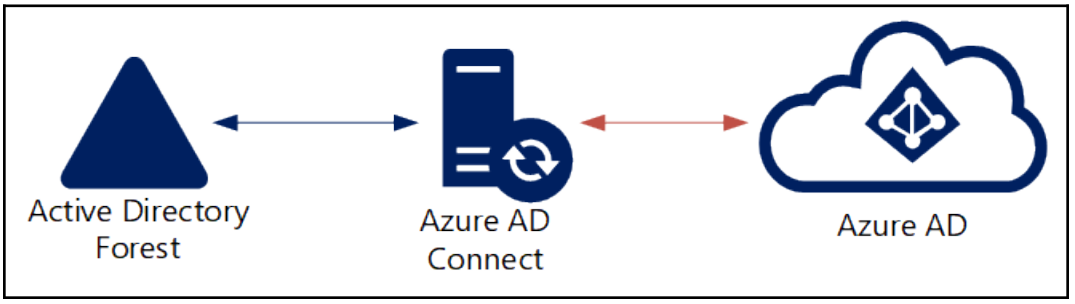

http://mim-pam.priv.contoso.com
PAM Portal - Elevate
About
Elevate
View History
Approvals
Roles for Elevation
PRIV\PRIV.Jen
Show 10 entries
Search:
Role Name
Description
Actions
Expiration Time
MFA Enabled
Approval Enabled
AD Administrators
Elevate
false
true
CorpAdmins
Elevate
false
true
TestAdmins
Test
Pending approval or multifactor authentication
false
true
Showing 1 to 3 of 3 entries
Previous
1
Next

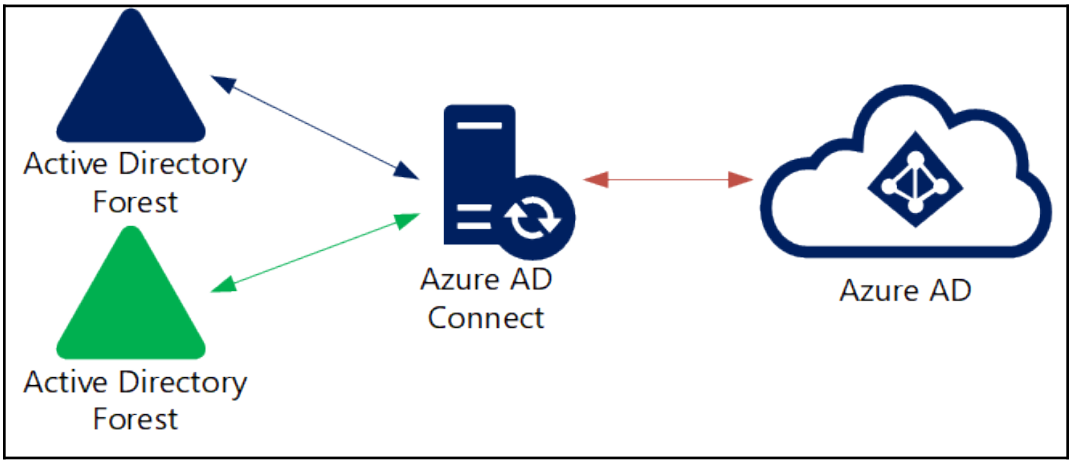

Identity Director
Organizational Management
Service Management
User Management
Access Management

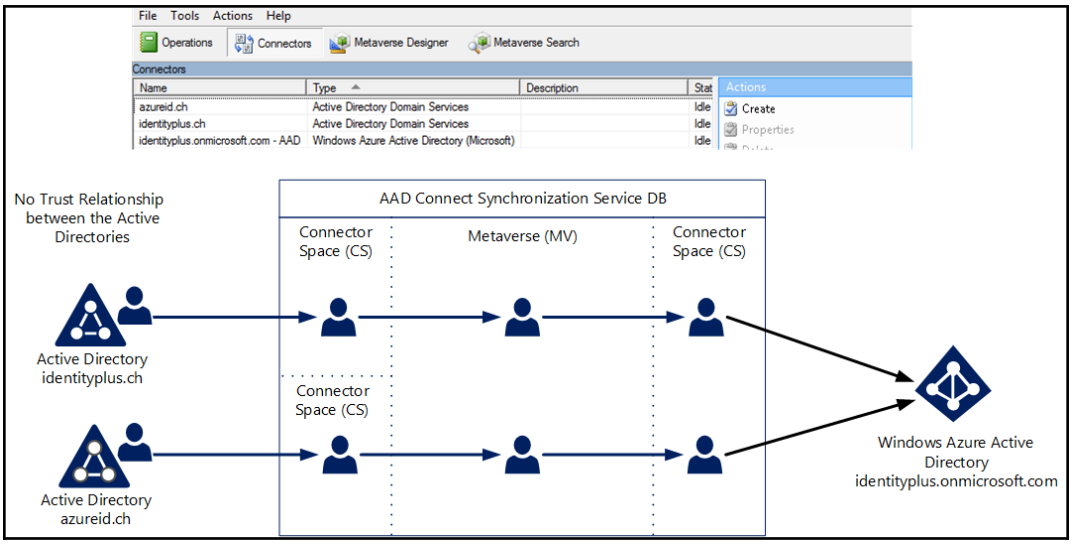

Users
Aaron Painter
Users
CREATE USER
All Persons
Display Name
Company
Aaron Painter
JMT Chocolate factory Germany AG
Adam Barr
JMT Chocolate factory Germany AG
Alan Brewer
JMT Chocolate factory GmbH
Alan Steiner
JMT Chocolate factory GmbH
Alexandre Silva
JMT Chocolate factory GmbH
Alfons Parovszky
JMT Chocolate factory GmbH
Alicia Thomber
JMT Chocolate factory GmbH
Alisa Lawyer
JMT Chocolate factory GmbH
Allan Guinot
JMT Chocolate factory Germany AG
Allison Brown
JMT Chocolate factory GmbH
Amy Alberts
JMT Chocolate factory GmbH
Anders Madsen
JMT Chocolate factory GmbH
Andrea Dunker
JMT Chocolate factory GmbH
Andrew Ma
JMT Chocolate factory GmbH
Andy Jacobs
JMT Chocolate factory GmbH
Anna Lidman
JMT Chocolate factory GmbH
Anne Weiler
JMT Chocolate factory Germany AG
Aaron Painter
Profile
Positions
Entitlements & Permiss
Person Information
First Name
Aaron
Last Name
Painter
Work Information
Primary Position
Store Sales Person @ JMT Store Berlin
Organizational Unit
JMT Store Berlin
Company
JMT Chocolate factory Germany AG
Location
JMT Chocolate factory Germany Store Berlin
Job Title
Store Sales Person

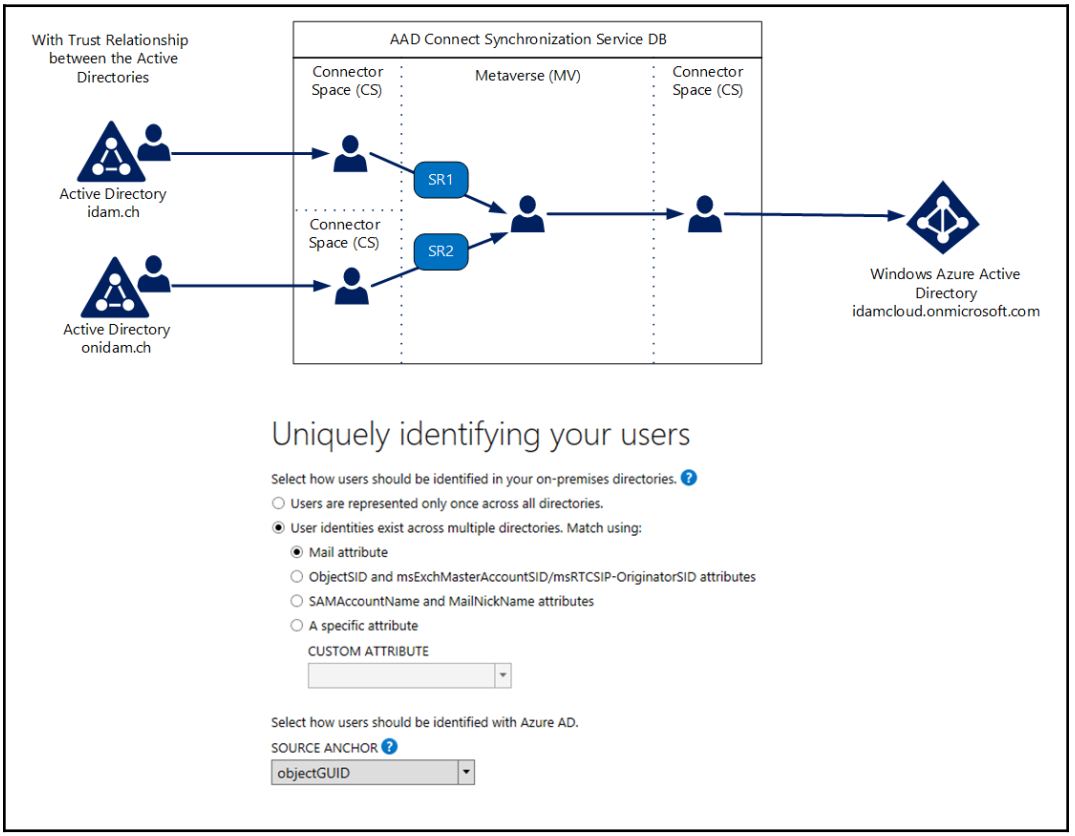

Users
Aaron Painter
Store Sales Person @ JMT Store Ber...
Aaron Painter
Profile
Positions
Entitlements & Permissi
Positions for this Person
CREATE POSITION
Display Name
State
Start Date
Store Manager @ JMT Store Interlaken
Inactive
10/24/18 10:00:00 PM
Store Sales Person @ JMT Store Berlin
Active
10/14/00 10:00:00 PM
Rows per page:
10
1
of 1
Total items: 2 • Data loaded at 10:51:13
Store Sales Person @ JMT Store Berlin
Position
Roles & Permissions
Assigned Roles
Display Name
Permissions
Store Sales Person
ExpertsLive Announcement Chat
2
Rows per page:
10
1
of 1
Total items: 1 • Data loaded at 10:51:44
Direct Permissions
Display Name
Description
Service
No items.
Add Permissions
Remove Permissions

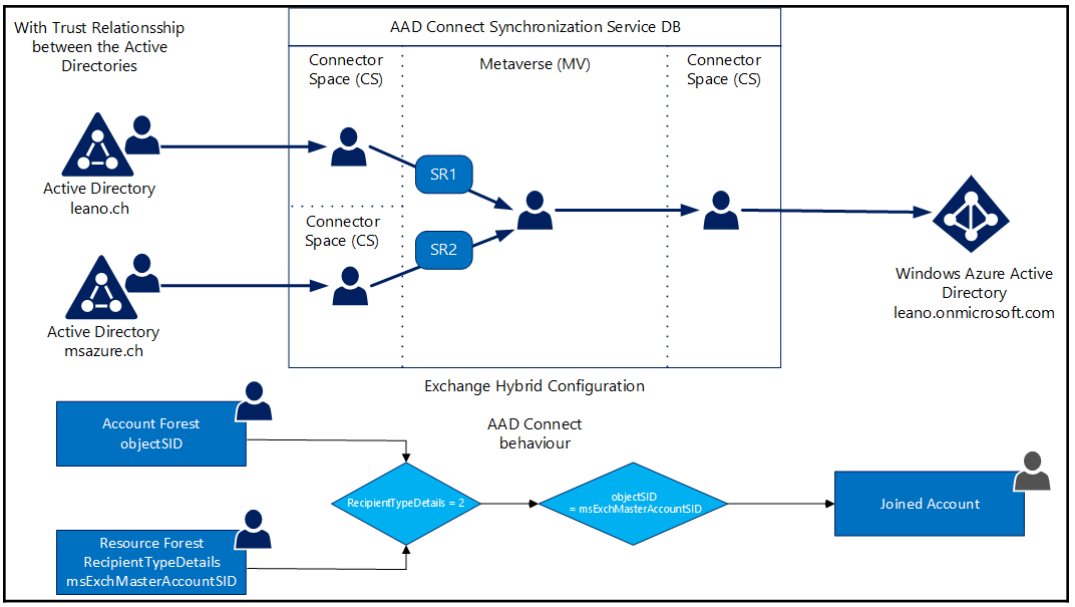

Supported Connectors
Type
Windows Azure Active Directory (Microsoft)
Active Directory Domain Services
AAD Connect Synchronization Service DB
Connector Space (CS)
Metaverse (MV)
Default Object Types
person
group
device
publicFolder
Connector Space (CS)
Import/Export
Sync
ISR
Sync
OSR
Import/Export
Active Directory
Azure Active Directory

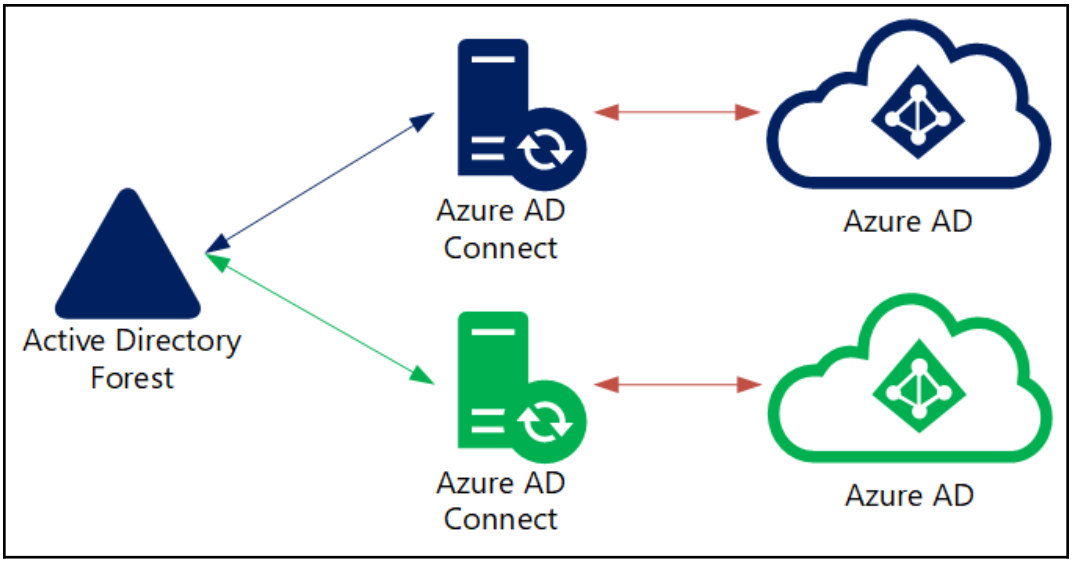

Active Directory Forest
Azure AD Connect
Azure AD

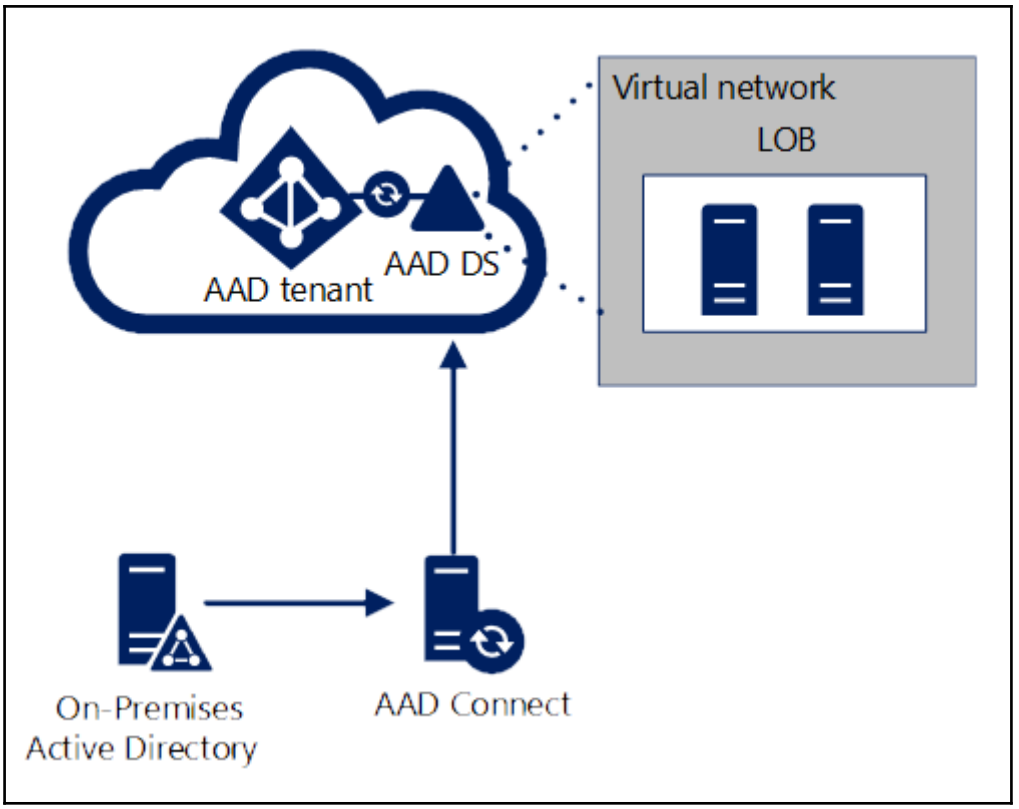

Active Directory Forest
Active Directory Forest
Azure AD Connect
Azure AD

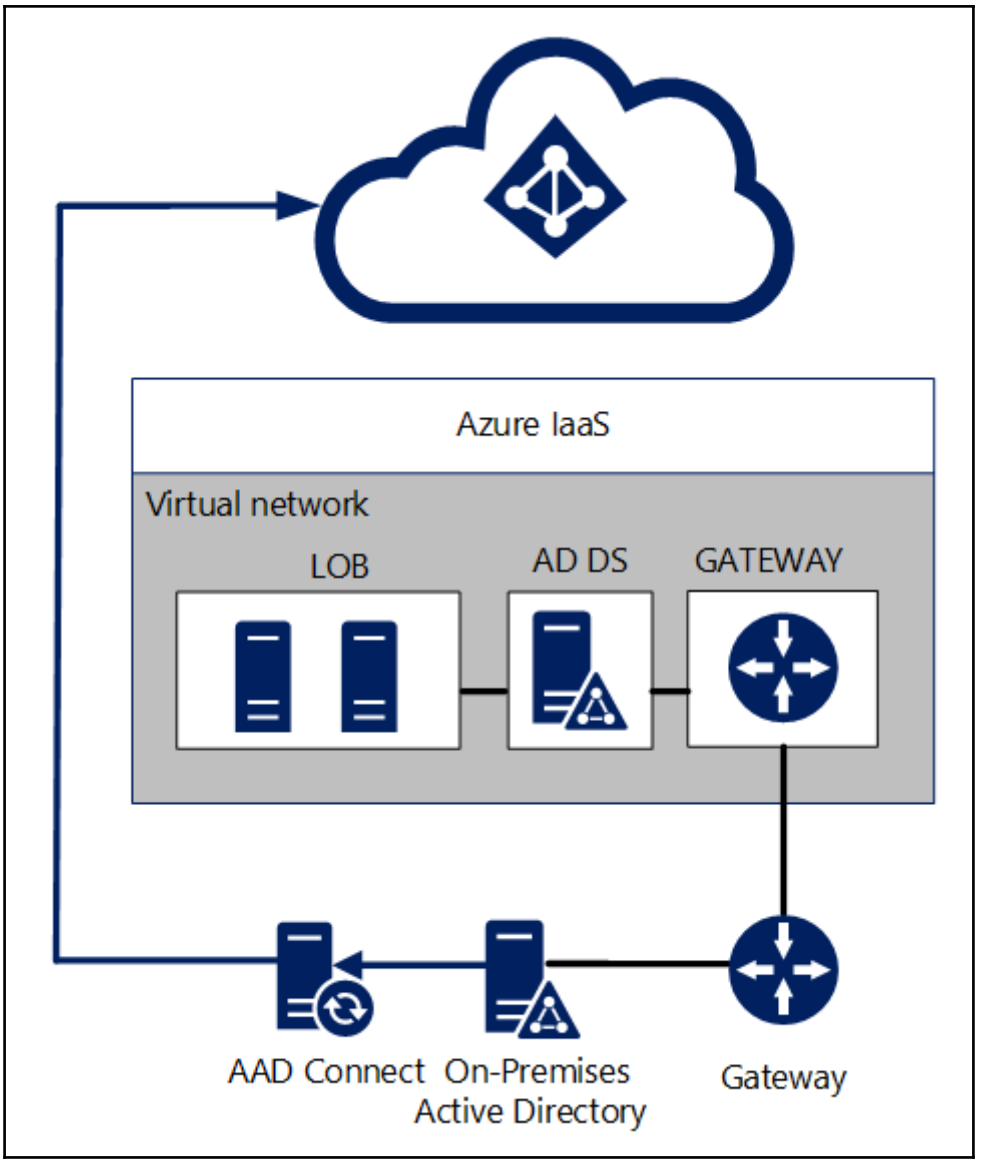

File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connectors
Name
Type
Description
Stat
azureid.ch
Active Directory Domain Services
Idle
identityplus.ch
Active Directory Domain Services
Idle
identityplus.onmicrosoft.com - AAD
Windows Azure Active Directory (Microsoft)
Idle
Actions
Create
Properties
No Trust Relationship between the Active Directories
AAD Connect Synchronization Service DB
Connector Space (CS)
Metaverse (MV)
Connector Space (CS)
Active Directory identityplus.ch
Connector Space (CS)
Active Directory azureid.ch
Windows Azure Active Directory identityplus.onmicrosoft.com

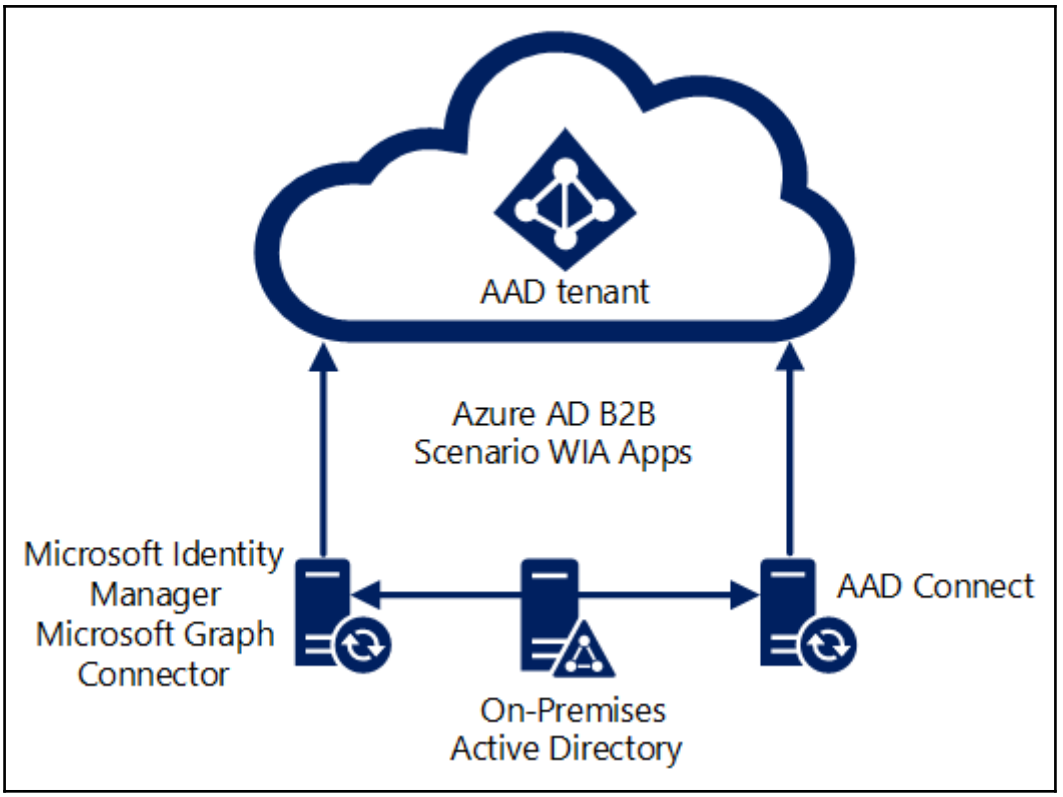

With Trust Relationship between the Active Directories
AAD Connect Synchronization Service DB
Connector Space (CS)
Metaverse (MV)
Connector Space (CS)
Active Directory idam.ch
SR1
Connector Space (CS)
SR2
Active Directory onidam.ch
Windows Azure Active Directory idamcloud.onmicrosoft.com
Uniquely identifying your users
Select how users should be identified in your on-premises directories.
Users are represented only once across all directories.
User identities exist across multiple directories. Match using:
Mail attribute
ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
SAMAccountName and MailNickName attributes
A specific attribute
CUSTOM ATTRIBUTE
Select how users should be identified with Azure AD.
SOURCE ANCHOR
objectGUID

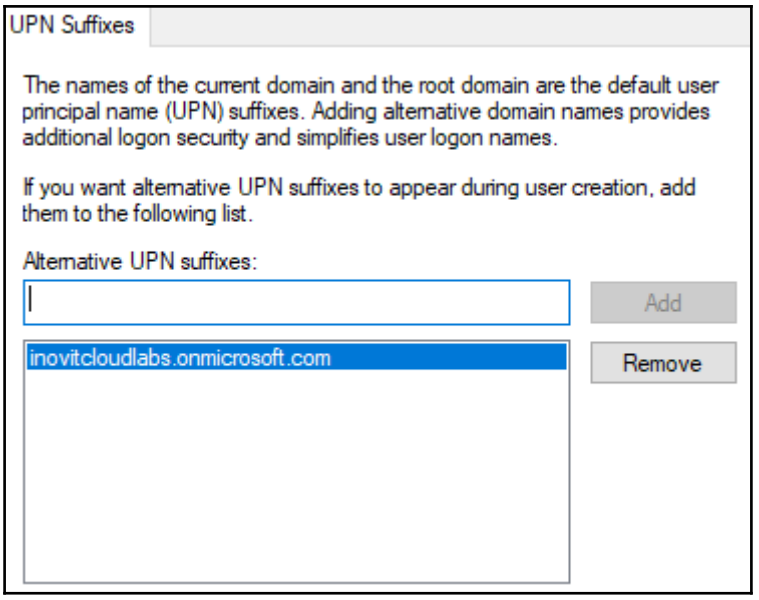

With Trust Relationsship between the Active Directories
AAD Connect Synchronization Service DB
Connector Space (CS)
Metaverse (MV)
Connector Space (CS)
Active Directory leano.ch
SR1
Connector Space (CS)
SR2
Active Directory msazure.ch
Windows Azure Active Directory leano.onmicrosoft.com
Exchange Hybrid Configuration
Account Forest objectSID
AAD Connect behaviour
RecipientTypeDetails = 2
objectSID = msExchMasterAccountSID
Joined Account
Resource Forest RecipientTypeDetails msExchMasterAccountSID

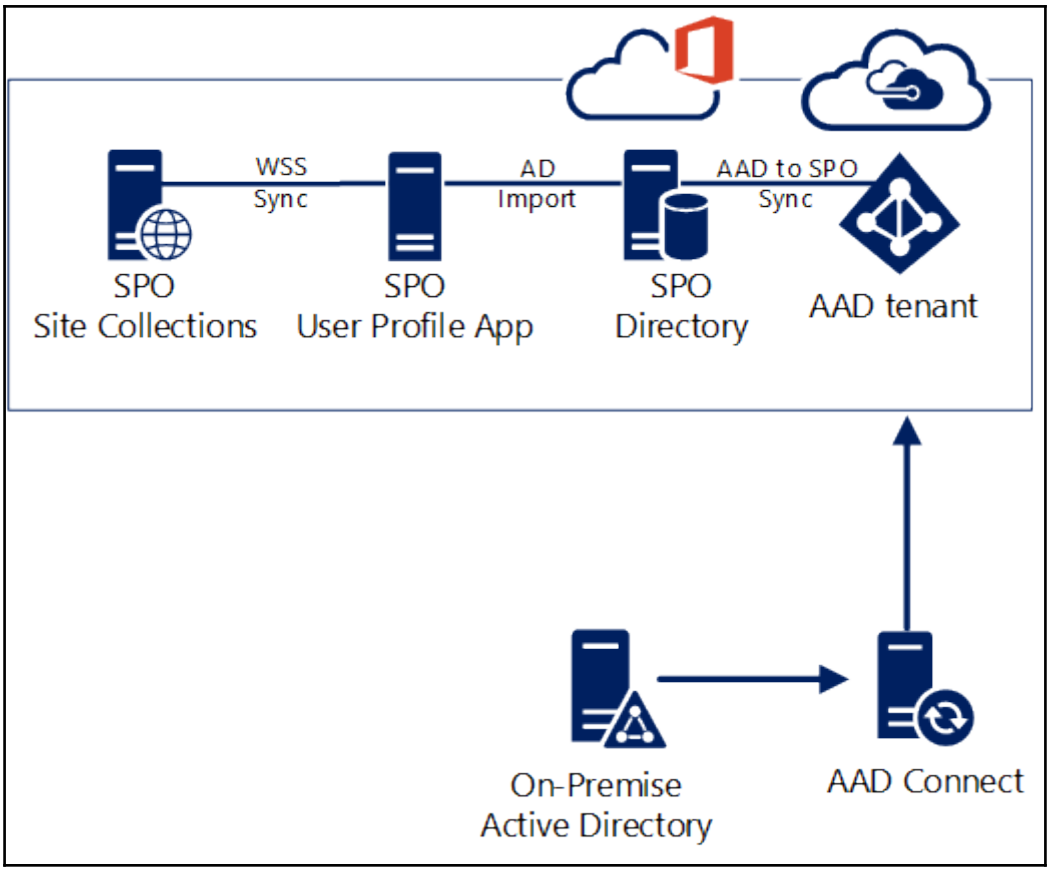

Azure AD Connect
Azure AD
Active Directory Forest
Azure AD Connect
Azure AD

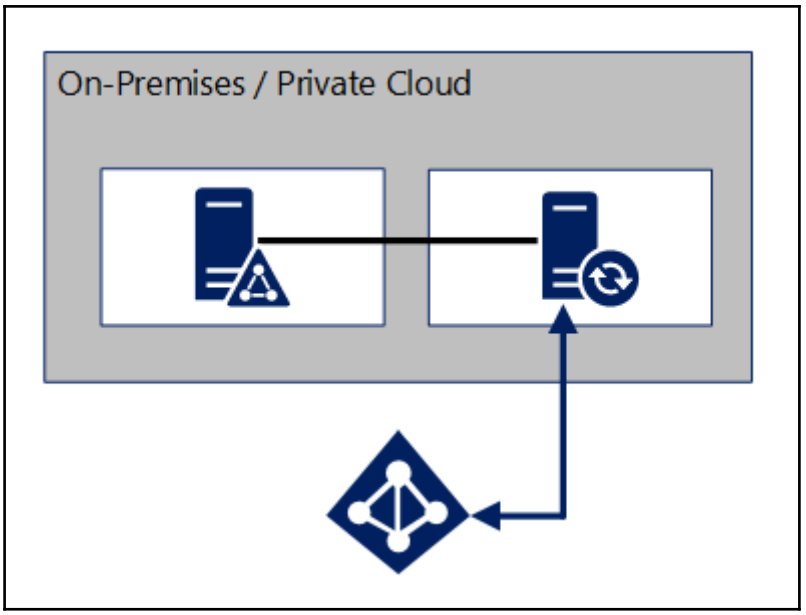

Virtual network
LOB
AAD tenant
AAD DS
On-Premises
Active Directory
AAD Connect

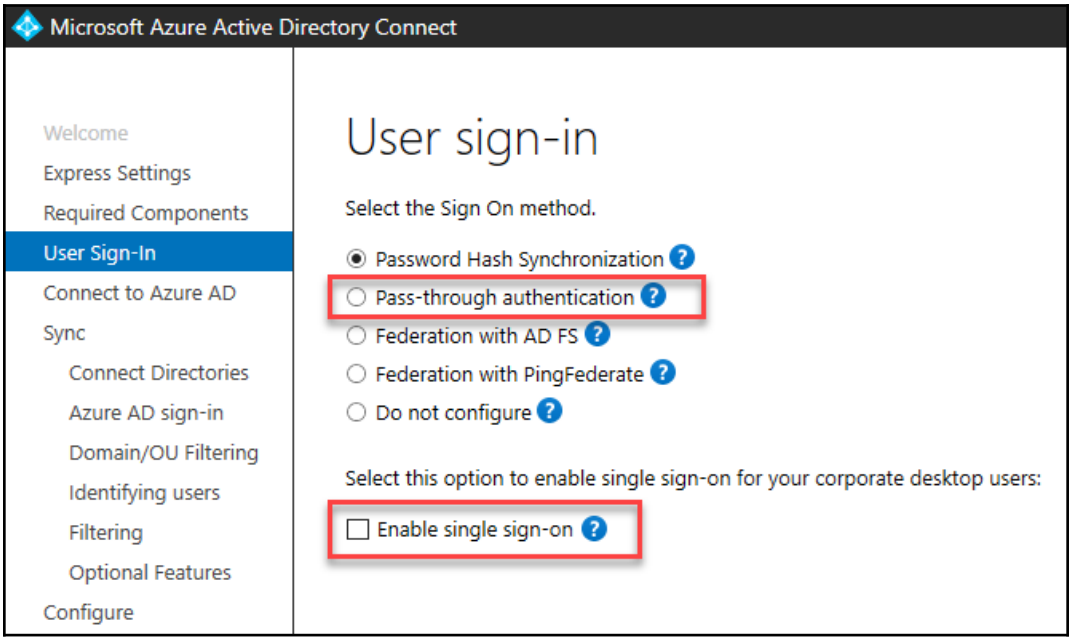

Azure IaaS
Virtual network
LOB
AD DS
GATEWAY
AAD Connect
On-Premises Active Directory
Gateway

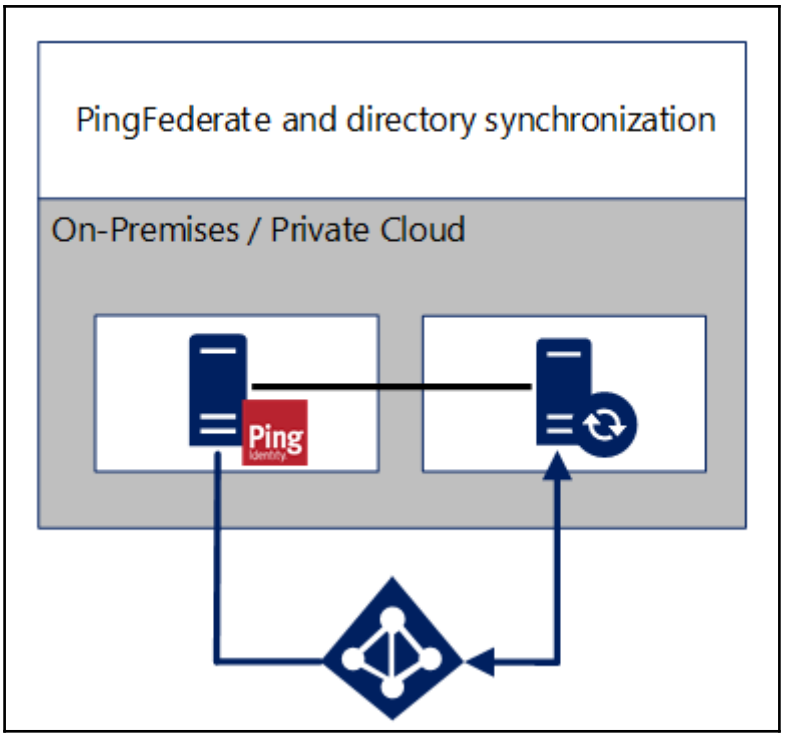

AAD tenant
Azure AD B2B
Scenario WIA Apps
Microsoft Identity
Manager
Microsoft Graph
Connector
AAD Connect
On-Premises
Active Directory

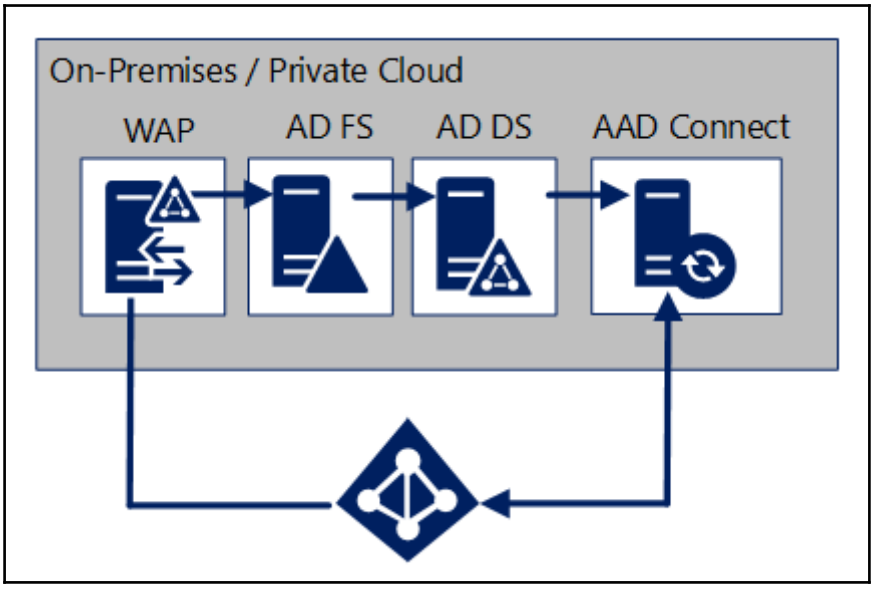

UPN Suffixes
The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.
If you want alternative UPN suffixes to appear during user creation, add them to the following list.
Alternative UPN suffixes:
Add
inovitcloudlabs.onmicrosoft.com
Remove

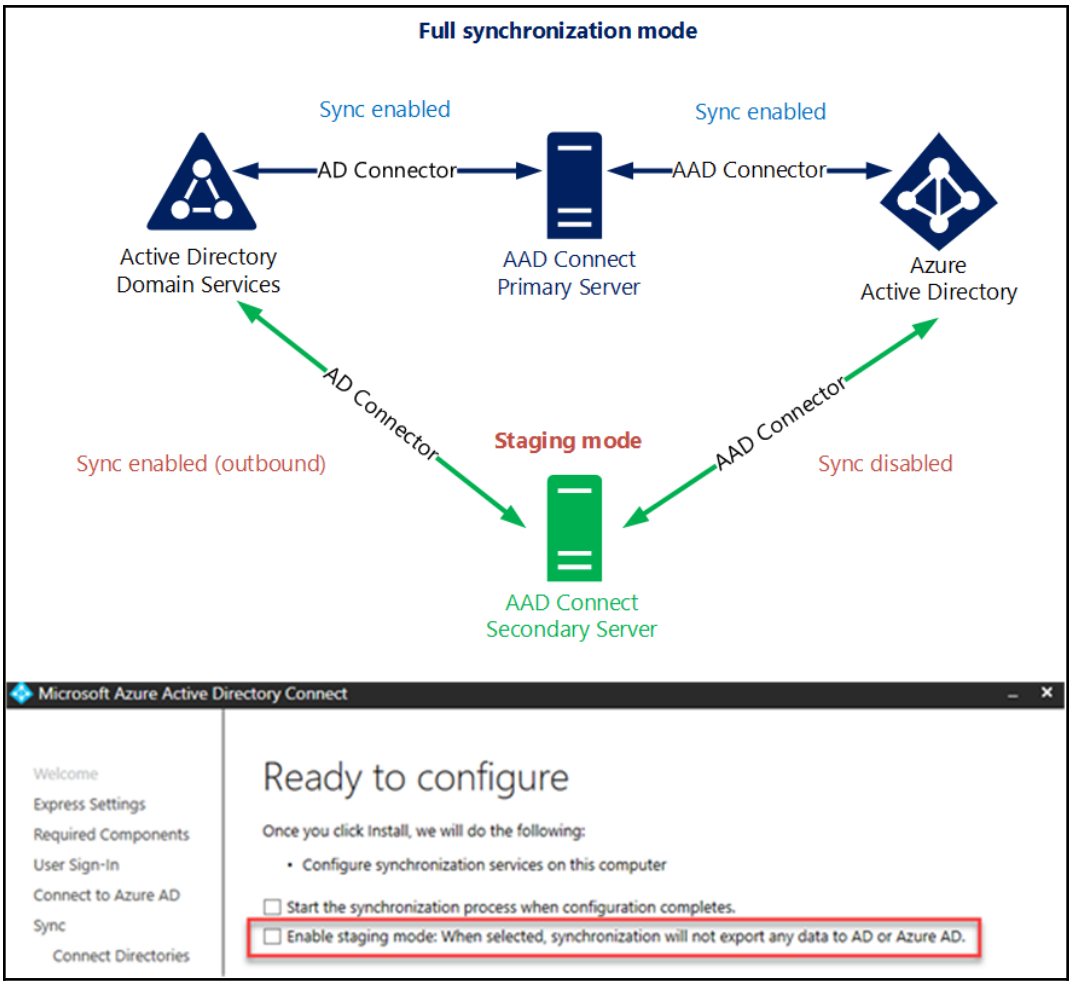

WSS
Sync
AD
Import
AAD to SPO
Sync
SPO
Site Collections
SPO
User Profile App
SPO
Directory
AAD tenant
On-Premise
Active Directory
AAD Connect

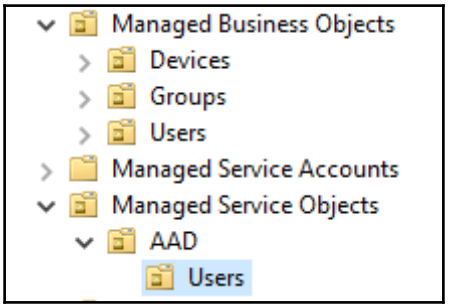

On-Premises / Private Cloud

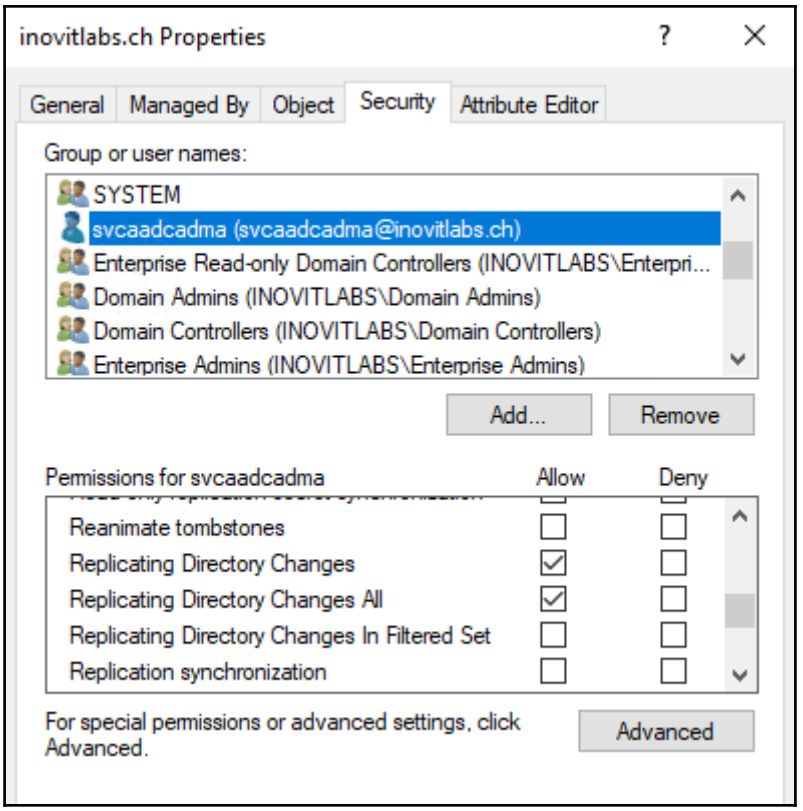

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
User sign-in
Select the Sign On method.
Password Hash Synchronization
Pass-through authentication
Federation with AD FS
Federation with PingFederate
Do not configure
Select this option to enable single sign-on for your corporate desktop users:
Enable single sign-on

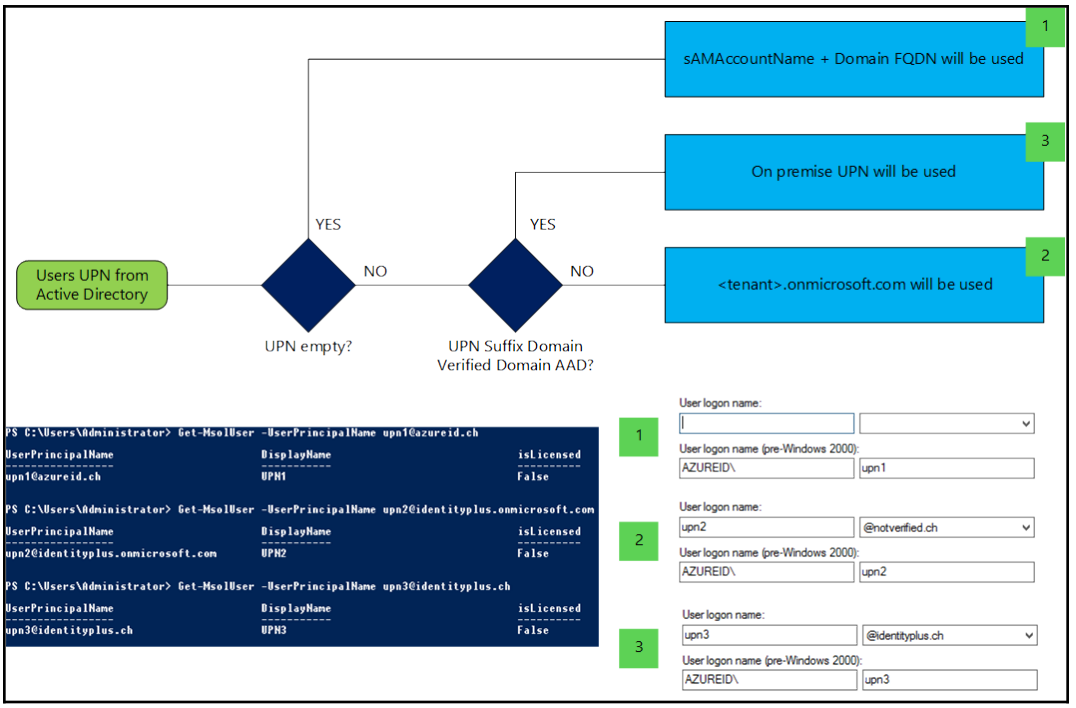

PingFederate and directory synchronization
On-Premises / Private Cloud
Ping
Identity


On-Premises / Private Cloud
WAP
AD FS
AD DS
AAD Connect

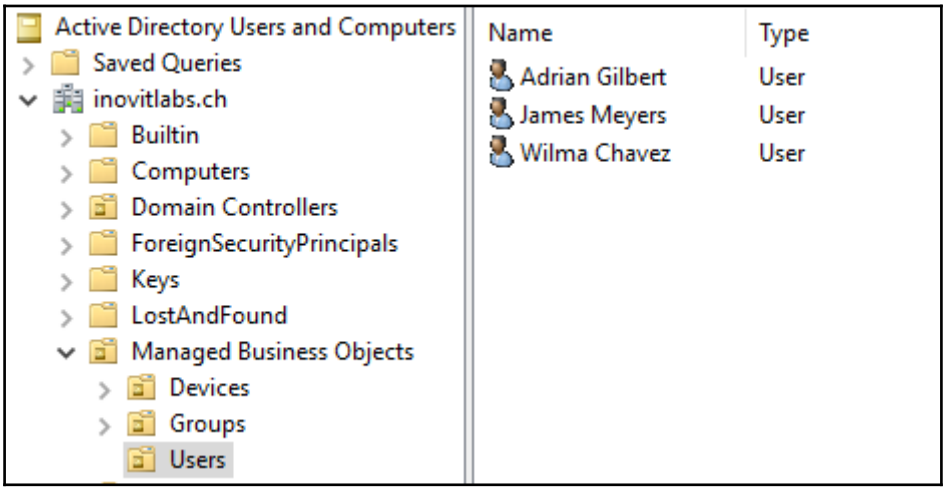

Full synchronization mode
Sync enabled
Sync enabled
AD Connector
AAD Connector
Active Directory
Domain Services
AAD Connect
Primary Server
Azure
Active Directory
AD Connector
AAD Connector
Staging mode
Sync enabled (outbound)
Sync disabled
AAD Connect
Secondary Server
Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Ready to configure
Once you click Install, we will do the following:
• Configure synchronization services on this computer
Start the synchronization process when configuration completes.
Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

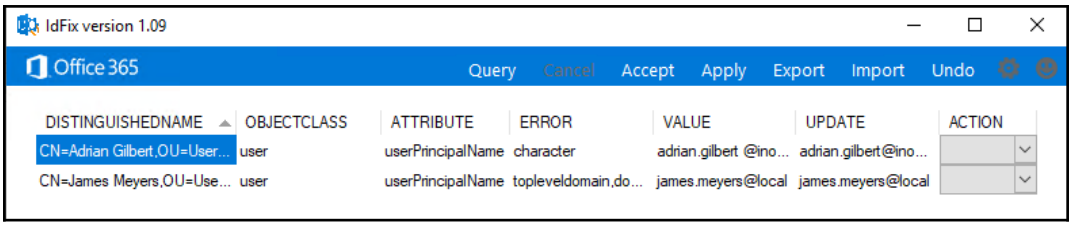

Managed Business Objects
Devices
Groups
Users
Managed Service Accounts
Managed Service Objects
AAD
Users

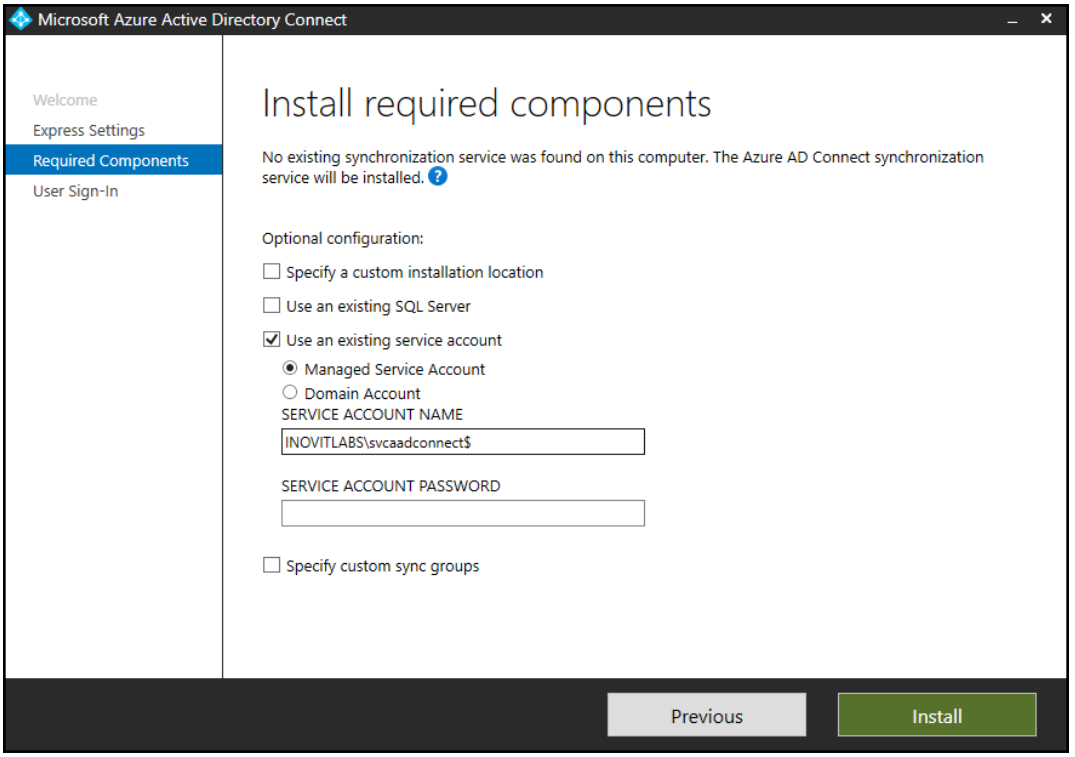

inovitlabs.ch Properties
General
Managed By
Object
Security
Attribute Editor
Group or user names:
SYSTEM
svcaadcadma (svcaadcadma@inovitlabs.ch)
Enterprise Read-only Domain Controllers (INOVITLABS\Enterpri...
Domain Admins (INOVITLABS\Domain Admins)
Domain Controllers (INOVITLABS\Domain Controllers)
Enterprise Admins (INOVITLABS\Enterprise Admins)
Add...
Remove
Permissions for svcaadcadma
Allow
Deny
Reanimate tombstones
Replicating Directory Changes
Replicating Directory Changes All
Replicating Directory Changes In Filtered Set
Replication synchronization
For special permissions or advanced settings, click Advanced.
Advanced

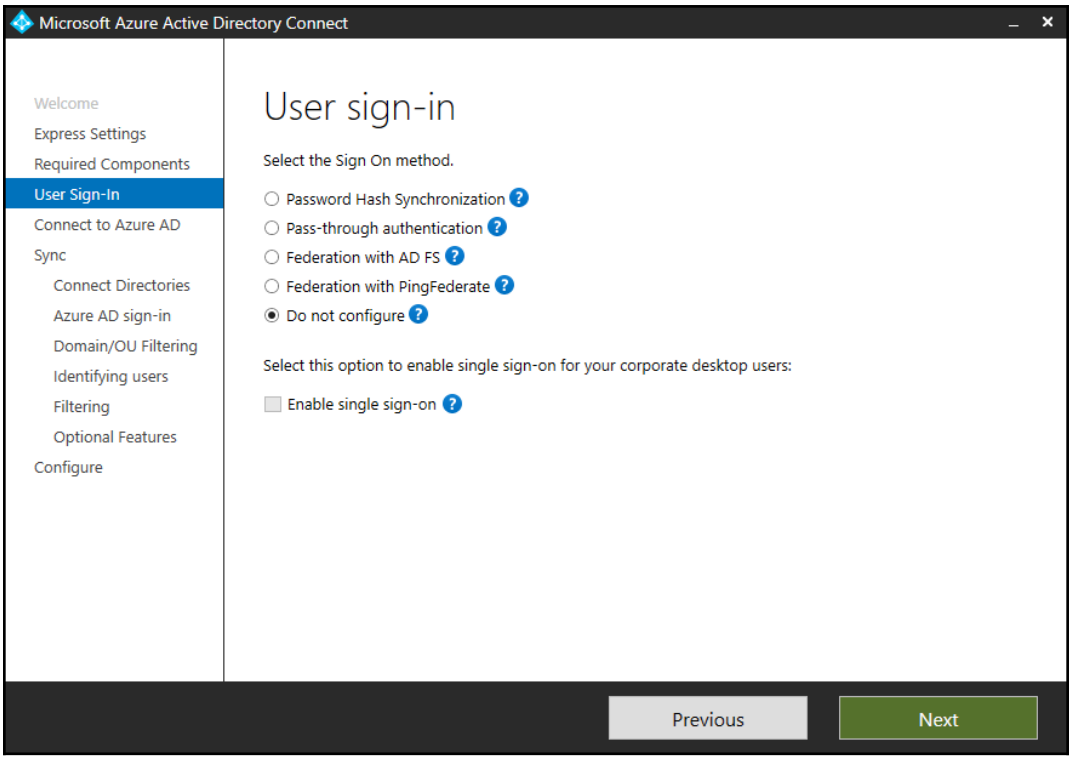

1
sAMAccountName + Domain FQDN will be used
3
On premise UPN will be used
2
<tenant>.onmicrosoft.com will be used
YES
NO
YES
NO
Users UPN from Active Directory
UPN empty?
UPN Suffix Domain Verified Domain AAD?
PS C:\Users\Administrator> Get-MsolUser -UserPrincipalName upn1@azureid.ch
UserPrincipalName DisplayName isLicensed
upn1@azureid.ch UPN1 False
PS C:\Users\Administrator> Get-MsolUser -UserPrincipalName upn2@identityplus.onmicrosoft.com
UserPrincipalName DisplayName isLicensed
upn2@identityplus.onmicrosoft.com UPN2 False
PS C:\Users\Administrator> Get-MsolUser -UserPrincipalName upn3@identityplus.ch
UserPrincipalName DisplayName isLicensed
upn3@identityplus.ch UPN3 False
1
User logon name:
User logon name (pre-Windows 2000):
AZUREID\
upn1
2
User logon name:
upn2
@notverified.ch
User logon name (pre-Windows 2000):
AZUREID\
upn2
3
User logon name:
upn3
@identityplus.ch
User logon name (pre-Windows 2000):
AZUREID\
upn3

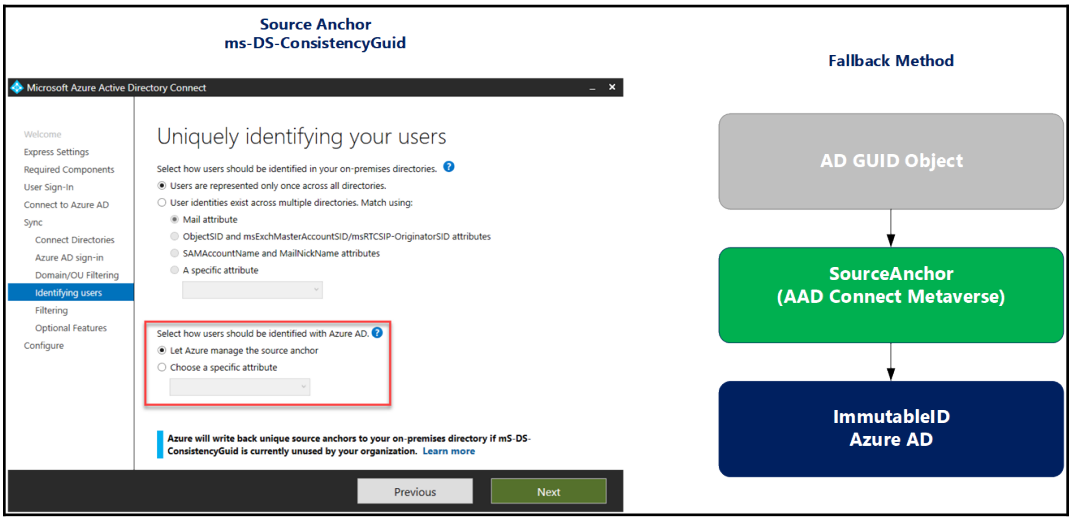

Office 365
Query
Cancel
Accept
Apply
Export
Import
Undo
DISTINGUISHEDNAME
OBJECTCLASS
ATTRIBUTE
ERROR
VALUE
UPDATE
ACTION
CN=Adrian Gilbert,OU=User...
user
userPrincipalName
character
adrian.gilbert @inovitlabs.ch
adrian.gilbert@inovitlabs.ch
CN=James Meyers,OU=Use...
user
userPrincipalName
topleveldomain,domainpart,format
james.meyers@local
james.meyers@local
CN=Wilma Chavez,OU=Us...
user
userPrincipalName
localpart
wilma.chavez'@inovitlabs.ch
wilma.chavez@inovitlabs.ch

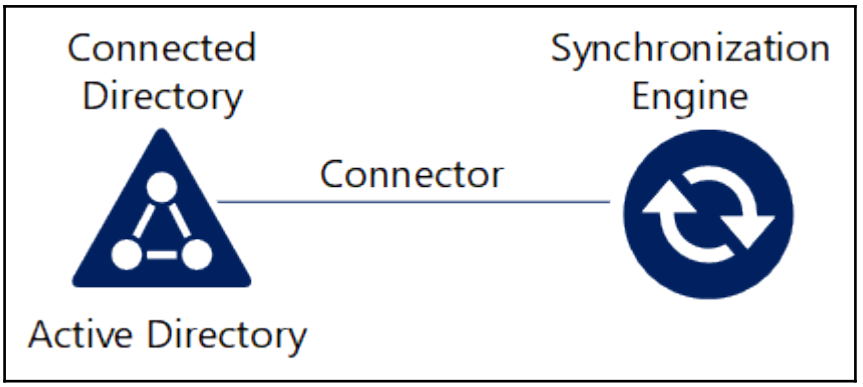

Active Directory Users and Computers
Saved Queries
inovitlabs.ch
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Business Objects
Devices
Groups
Users
Name
Type
Adrian Gilbert
User
James Meyers
User
Wilma Chavez
User

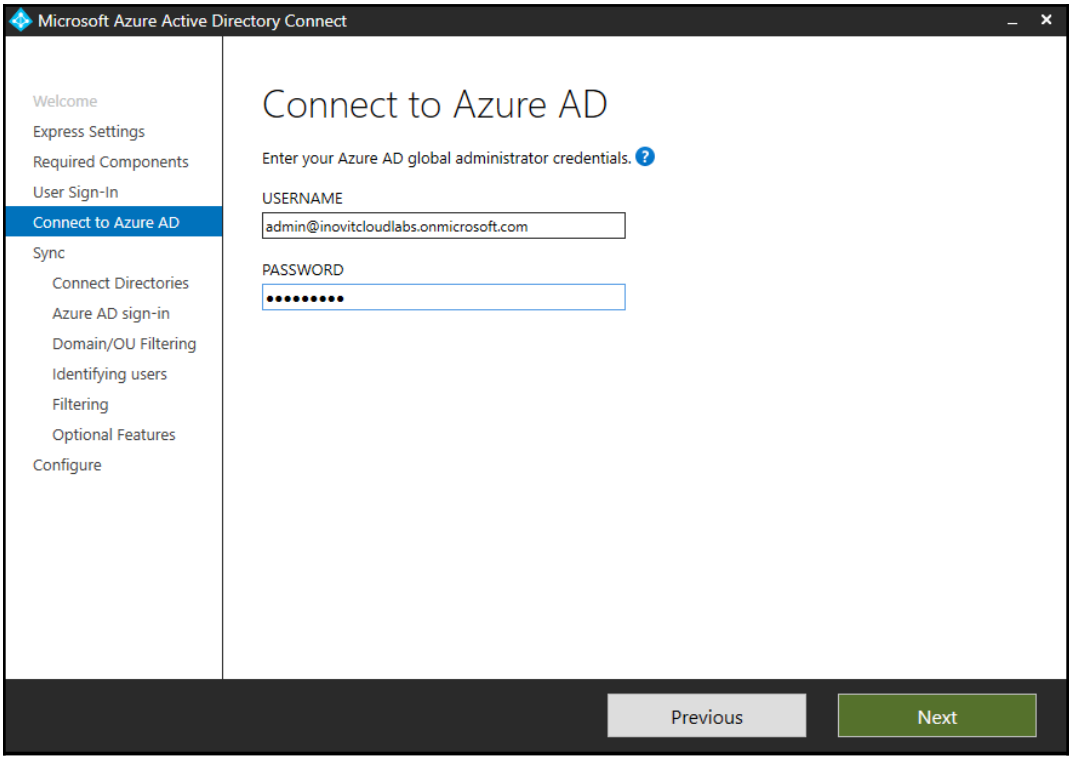

IdFix version 1.09
Office 365
Query
Cancel
Accept
Apply
Export
Import
Undo
DISTINGUISHEDNAME
OBJECTCLASS
ATTRIBUTE
ERROR
VALUE
UPDATE
ACTION
CN=Adrian Gilbert,OU=User...
user
userPrincipalName
character
adrian.gilbert @ino...
adrian.gilbert@ino...
CN=James Meyers,OU=Use...
user
userPrincipalName
topleveldomain,do...
james.meyers@local
james.meyers@local

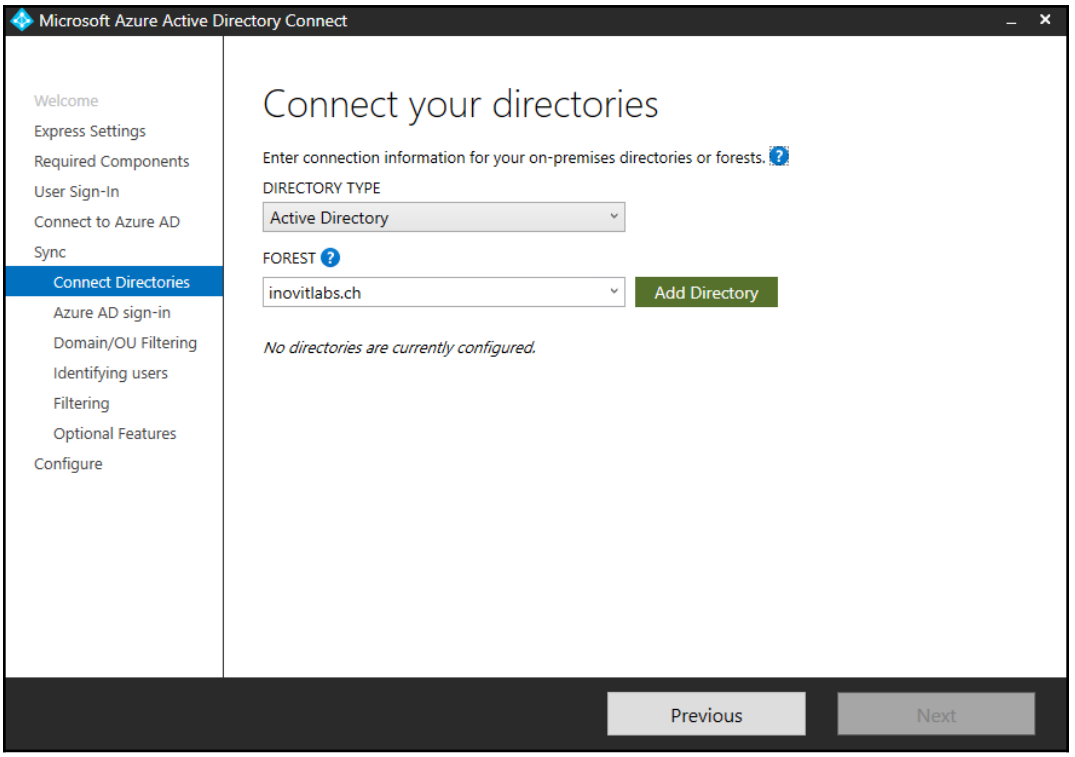

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Install required components
No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.
Optional configuration:
Specify a custom installation location
Use an existing SQL Server
Use an existing service account
Managed Service Account
Domain Account
SERVICE ACCOUNT NAME
INOVITLABS\svcaadconnect$
SERVICE ACCOUNT PASSWORD
Specify custom sync groups
Previous
Install

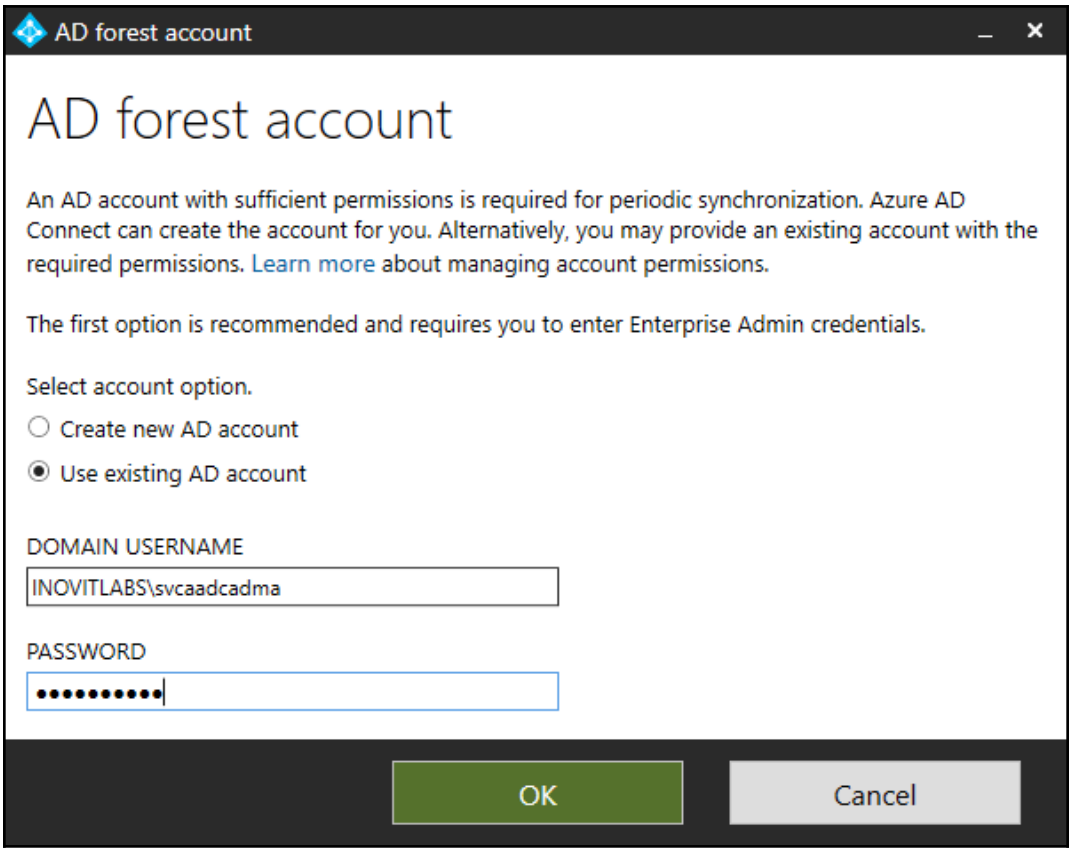

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
User sign-in
Select the Sign On method.
Password Hash Synchronization
Pass-through authentication
Federation with AD FS
Federation with PingFederate
Do not configure
Select this option to enable single sign-on for your corporate desktop users:
Enable single sign-on
Previous
Next

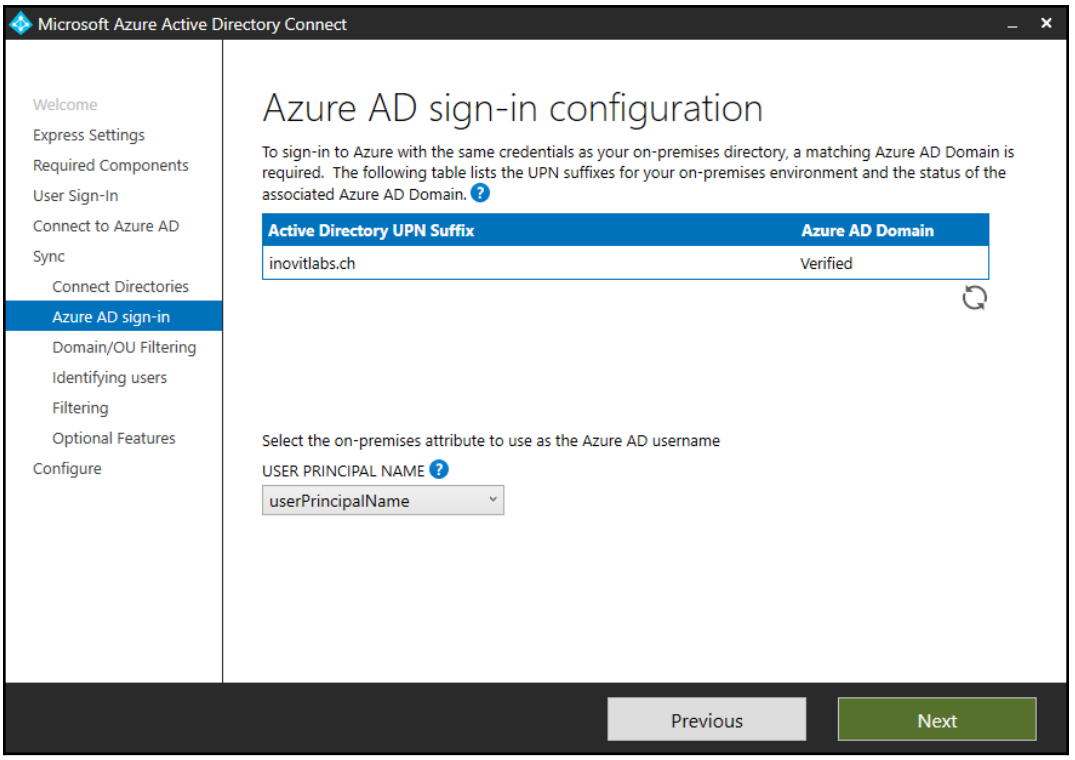

Source Anchor
ms-DS-ConsistencyGuid
Microsoft Azure Active Directory Connect
Uniquely identifying your users
Select how users should be identified in your on-premises directories.
Users are represented only once across all directories.
User identities exist across multiple directories. Match using:
Mail attribute
ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
SAMAccountName and MailNickName attributes
A specific attribute
Select how users should be identified with Azure AD.
Let Azure manage the source anchor
Choose a specific attribute
Azure will write back unique source anchors to your on-premises directory if mS-DS-ConsistencyGuid is currently unused by your organization. Learn more
Previous
Next
Fallback Method
AD GUID Object
SourceAnchor
(AAD Connect Metaverse)
ImmutableID
Azure AD

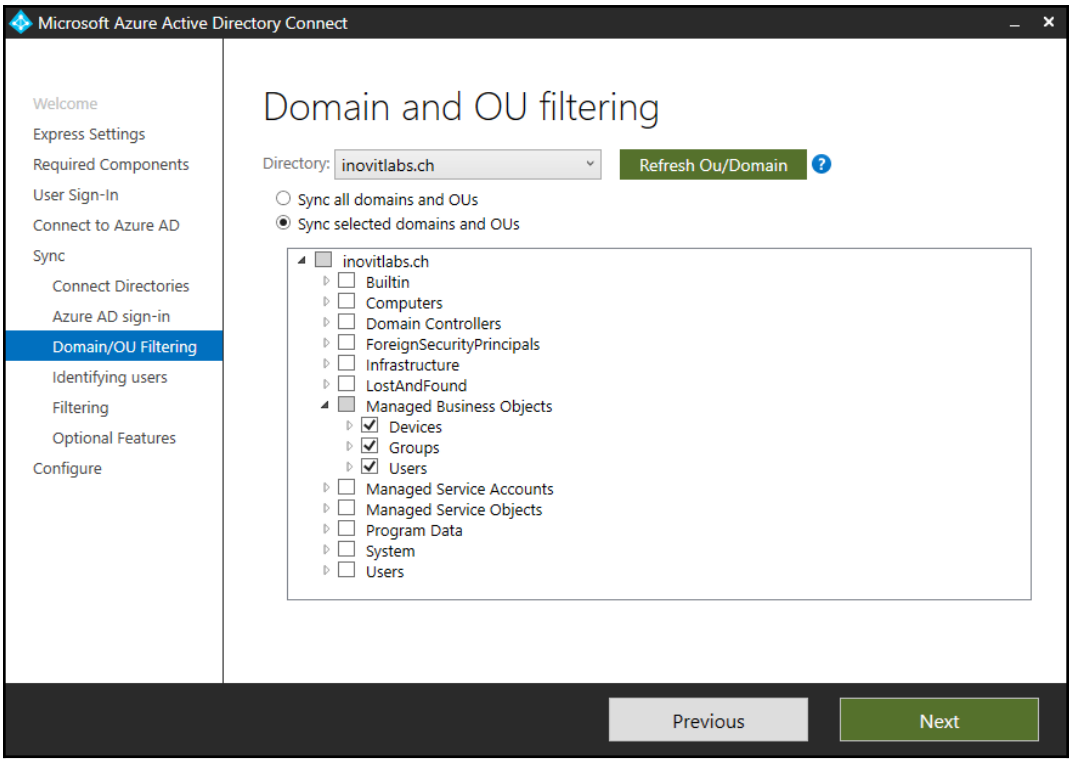

Connected Directory
Synchronization Engine
Connector
Active Directory

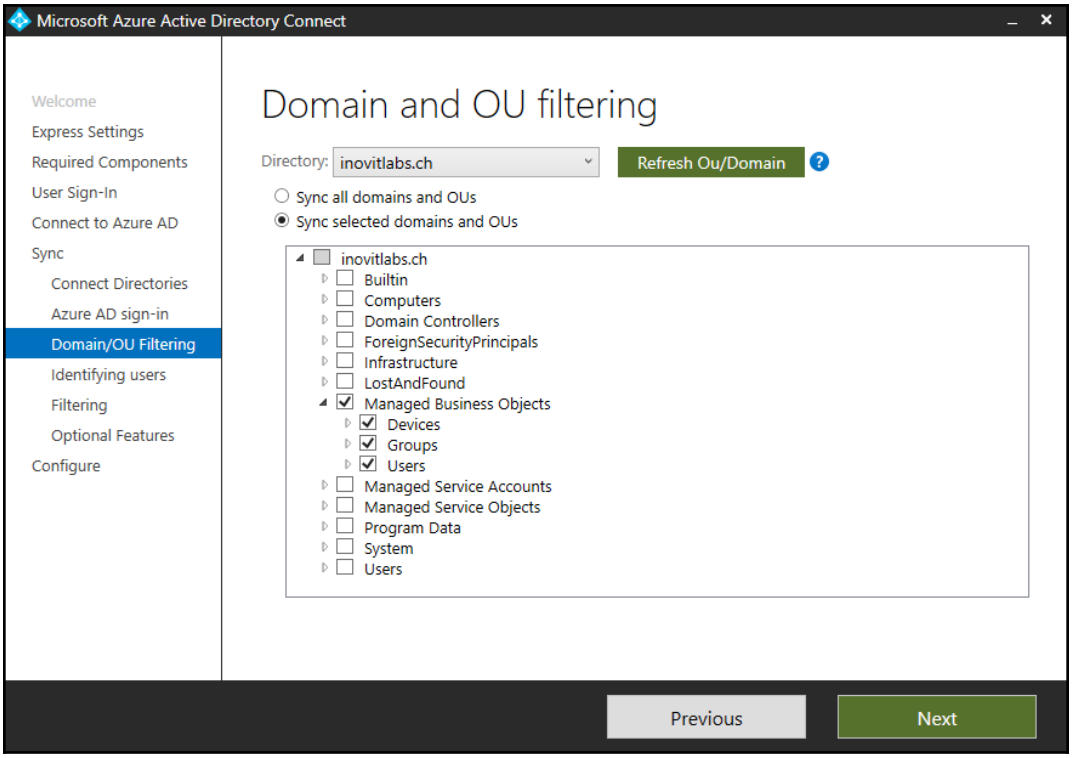

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Connect to Azure AD
Enter your Azure AD global administrator credentials.
USERNAME
admin@inovitcloudlabs.onmicrosoft.com
PASSWORD
Previous
Next

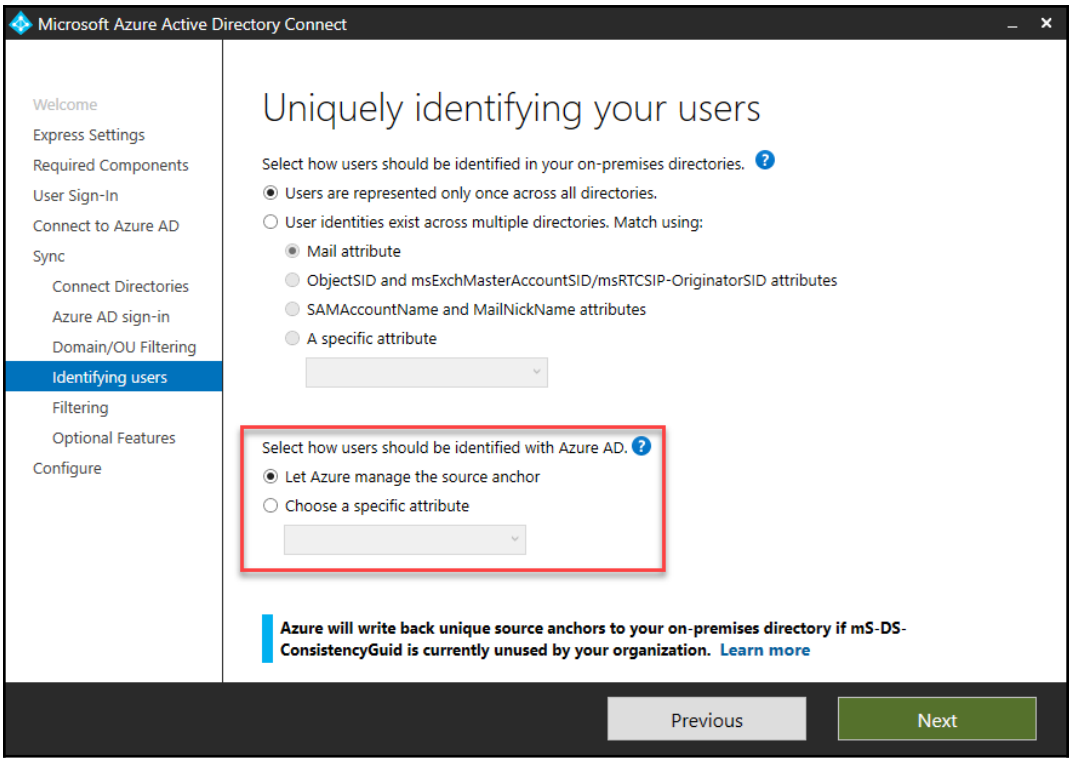

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Connect your directories
Enter connection information for your on-premises directories or forests.
DIRECTORY TYPE
Active Directory
FOREST
inovitlabs.ch
Add Directory
No directories are currently configured.
Previous
Next

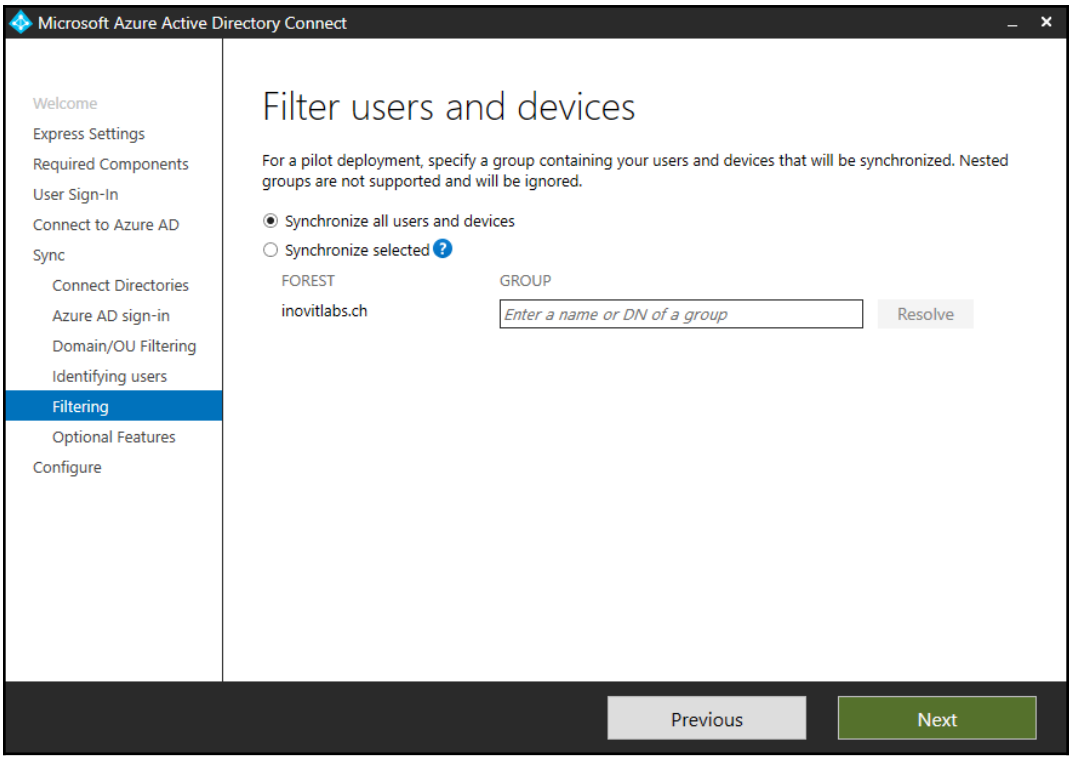

AD forest account
AD forest account
An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. Learn more about managing account permissions.
The first option is recommended and requires you to enter Enterprise Admin credentials.
Select account option.
Create new AD account
Use existing AD account
DOMAIN USERNAME
INOVITLABS\svcaadcadma
PASSWORD
OK
Cancel

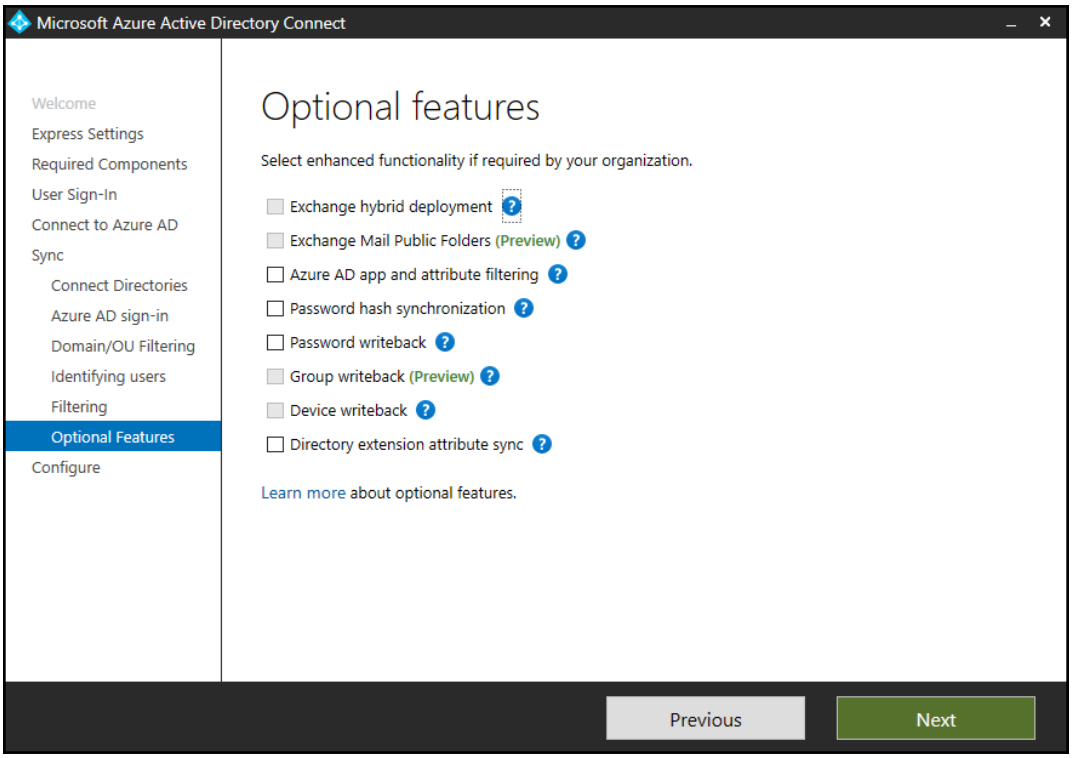

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Azure AD sign-in configuration
To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain.
Active Directory UPN Suffix
Azure AD Domain
inovitlabs.ch
Verified
Select the on-premises attribute to use as the Azure AD username
USER PRINCIPAL NAME
userPrincipalName
Previous
Next

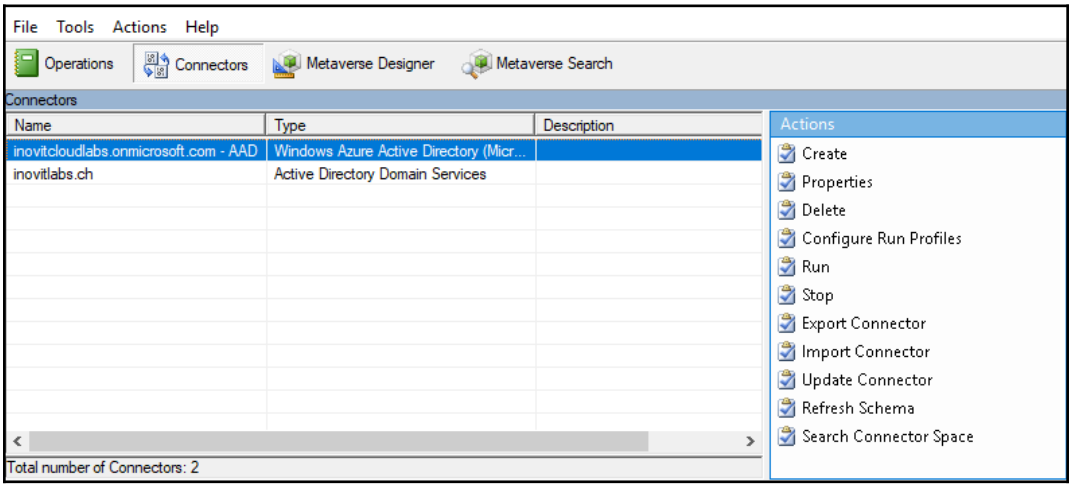

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Domain and OU filtering
Directory: inovitlabs.ch
Refresh Ou/Domain
Sync all domains and OUs
Sync selected domains and OUs
inovitlabs.ch
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
LostAndFound
Managed Business Objects
Devices
Groups
Users
Managed Service Accounts
Managed Service Objects
Program Data
System
Users
Previous
Next

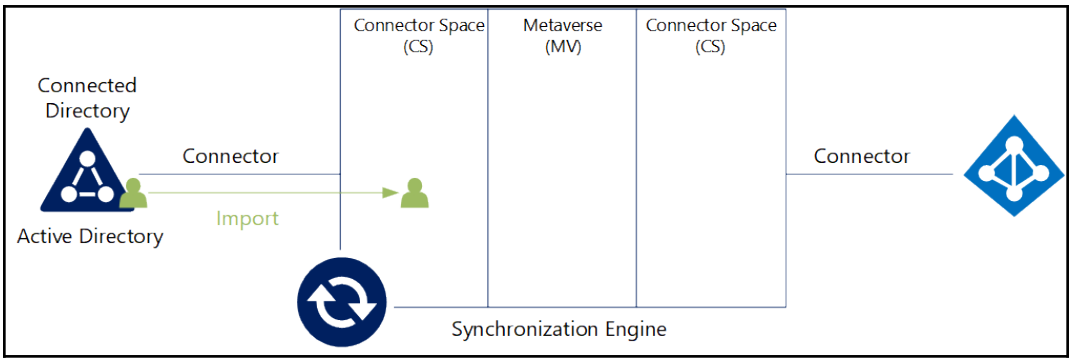

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Domain and OU filtering
Directory: inovitlabs.ch
Refresh Ou/Domain
Sync all domains and OUs
Sync selected domains and OUs
inovitlabs.ch
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
LostAndFound
Managed Business Objects
Devices
Groups
Users
Managed Service Accounts
Managed Service Objects
Program Data
System
Users
Previous
Next

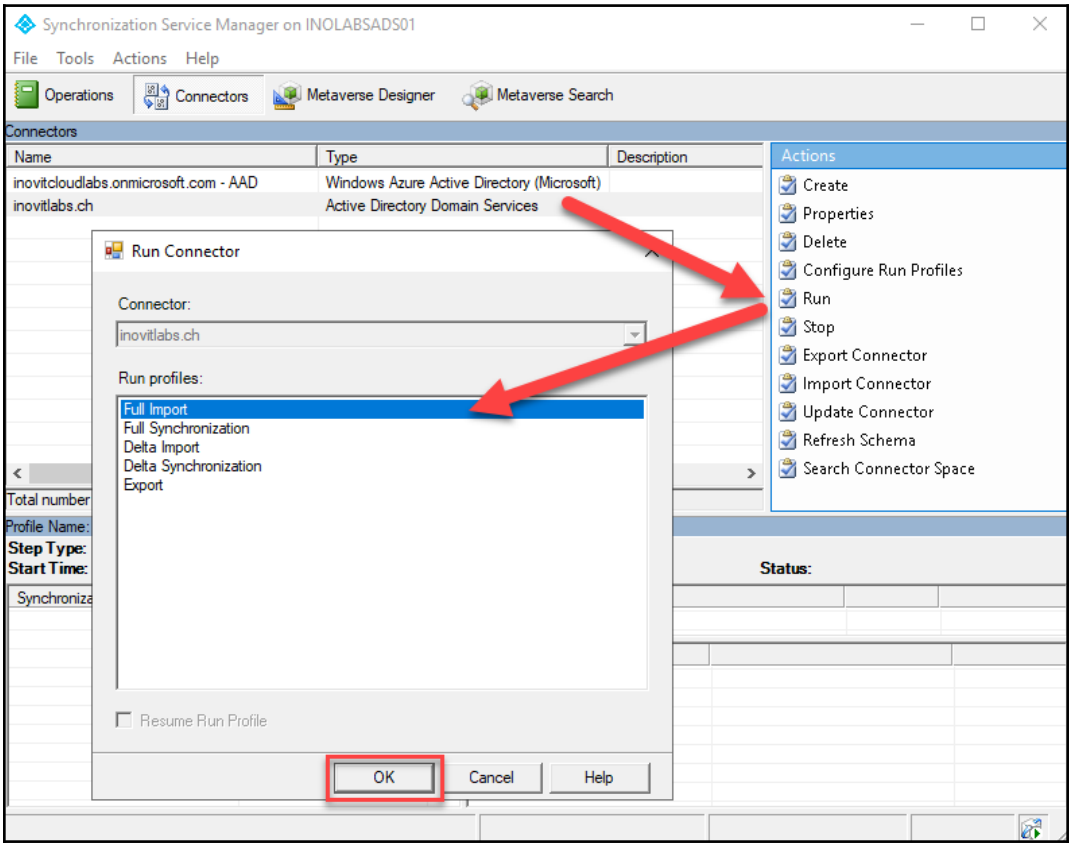

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Uniquely identifying your users
Select how users should be identified in your on-premises directories.
Users are represented only once across all directories.
User identities exist across multiple directories. Match using:
Mail attribute
ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
SAMAccountName and MailNickName attributes
A specific attribute
Select how users should be identified with Azure AD.
Let Azure manage the source anchor
Choose a specific attribute
Azure will write back unique source anchors to your on-premises directory if mS-DS-ConsistencyGuid is currently unused by your organization. Learn more
Previous
Next

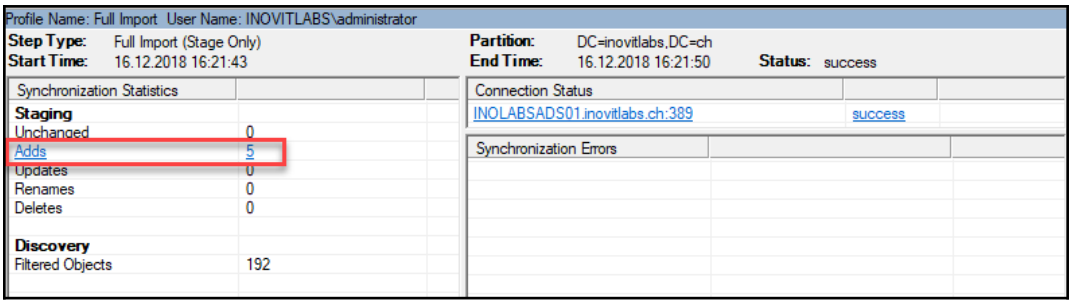

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Filter users and devices
For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.
Synchronize all users and devices
Synchronize selected
FOREST
GROUP
inovitlabs.ch
Enter a name or DN of a group
Resolve
Previous
Next

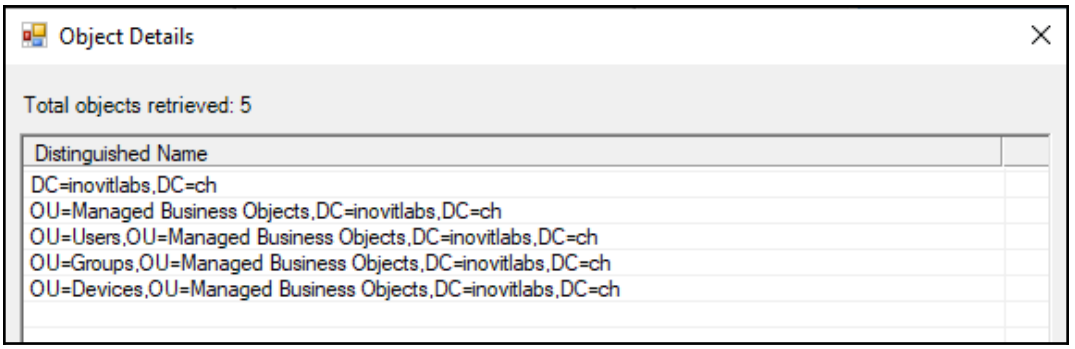

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Exchange Mail Public Folders (Preview)
Azure AD app and attribute filtering
Password hash synchronization
Password writeback
Group writeback (Preview)
Device writeback
Directory extension attribute sync
Learn more about optional features.
Previous
Next

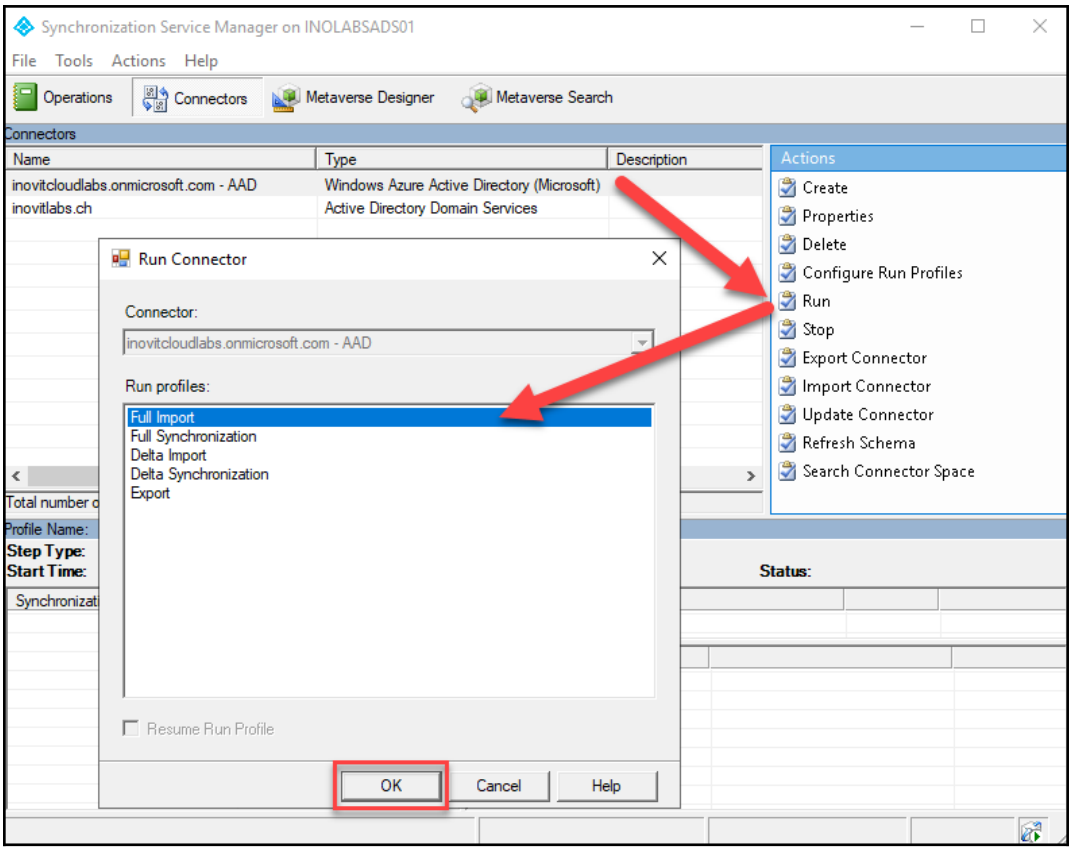

File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connectors
Name
Type
Description
inovitcloudlabs.onmicrosoft.com - AAD
Windows Azure Active Directory (Micr...
inovitlabs.ch
Active Directory Domain Services
Total number of Connectors: 2
Actions
Create
Properties
Delete
Configure Run Profiles
Run
Stop
Export Connector
Import Connector
Update Connector
Refresh Schema
Search Connector Space

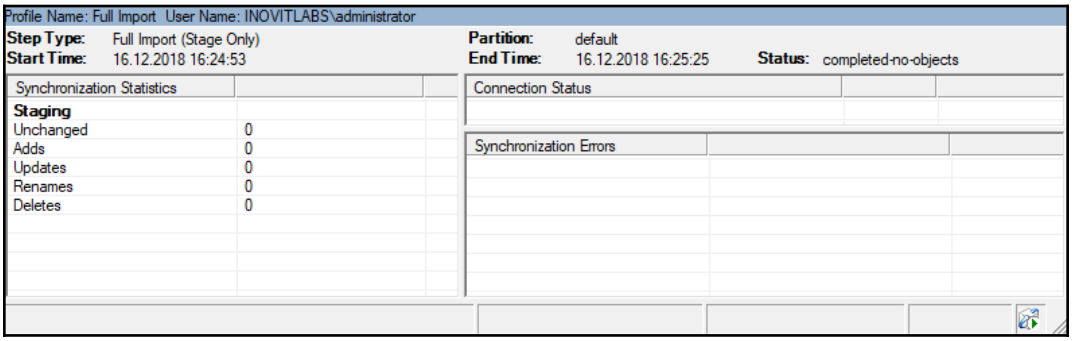

Connector Space
(CS)
Metaverse
(MV)
Connector Space
(CS)
Connected
Directory
Connector
Import
Active Directory
Connector
Synchronization Engine

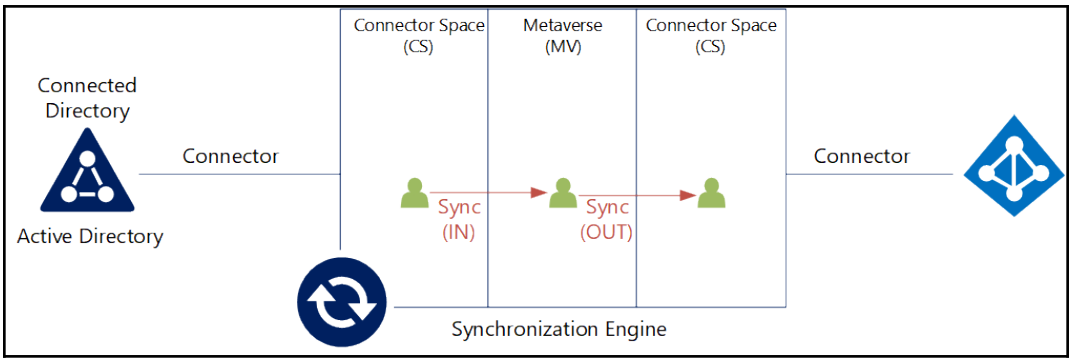

Synchronization Service Manager on INOLABSADS01
File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connectors
Name
Type
Description
inovitcloudlabs.onmicrosoft.com - AAD
Windows Azure Active Directory (Microsoft)
inovitlabs.ch
Active Directory Domain Services
Actions
Create
Properties
Delete
Configure Run Profiles
Run
Stop
Export Connector
Import Connector
Update Connector
Refresh Schema
Search Connector Space
Run Connector
Connector:
inovitlabs.ch
Run profiles:
Full Import
Full Synchronization
Delta Import
Delta Synchronization
Export
Resume Run Profile
OK
Cancel
Help
Total number
Profile Name:
Step Type:
Start Time:
Status:

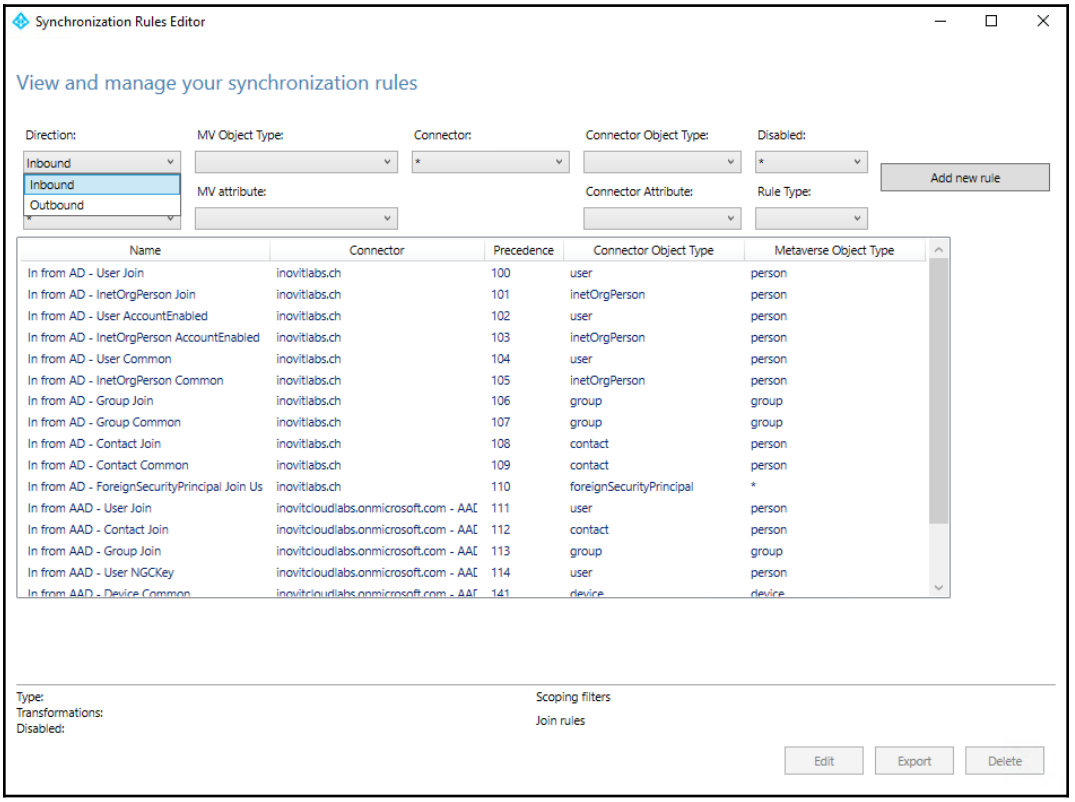

Profile Name: Full Import User Name: INOVITLABS\administrator
Step Type: Full Import (Stage Only)
Start Time: 16.12.2018 16:21:43
Partition: DC=inovitlabs,DC=ch
End Time: 16.12.2018 16:21:50
Status: success
Synchronization Statistics
Staging
Unchanged 0
Adds 5
Updates 0
Renames 0
Deletes 0
Discovery
Filtered Objects 192
Connection Status
INOLABSADS01.inovitlabs.ch:389 success
Synchronization Errors

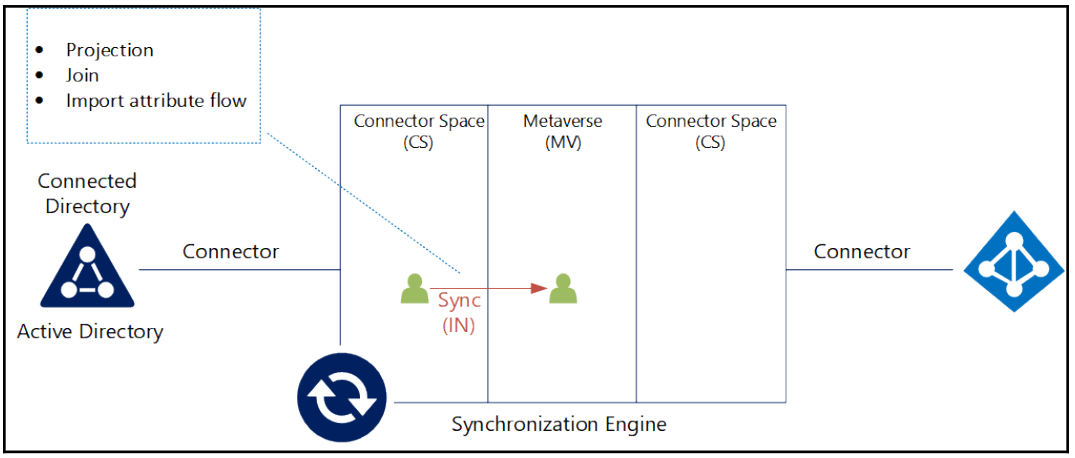

Object Details
Total objects retrieved: 5
Distinguished Name
DC=inovitlabs,DC=ch
OU=Managed Business Objects,DC=inovitlabs,DC=ch
OU=Users,OU=Managed Business Objects,DC=inovitlabs,DC=ch
OU=Groups,OU=Managed Business Objects,DC=inovitlabs,DC=ch
OU=Devices,OU=Managed Business Objects,DC=inovitlabs,DC=ch

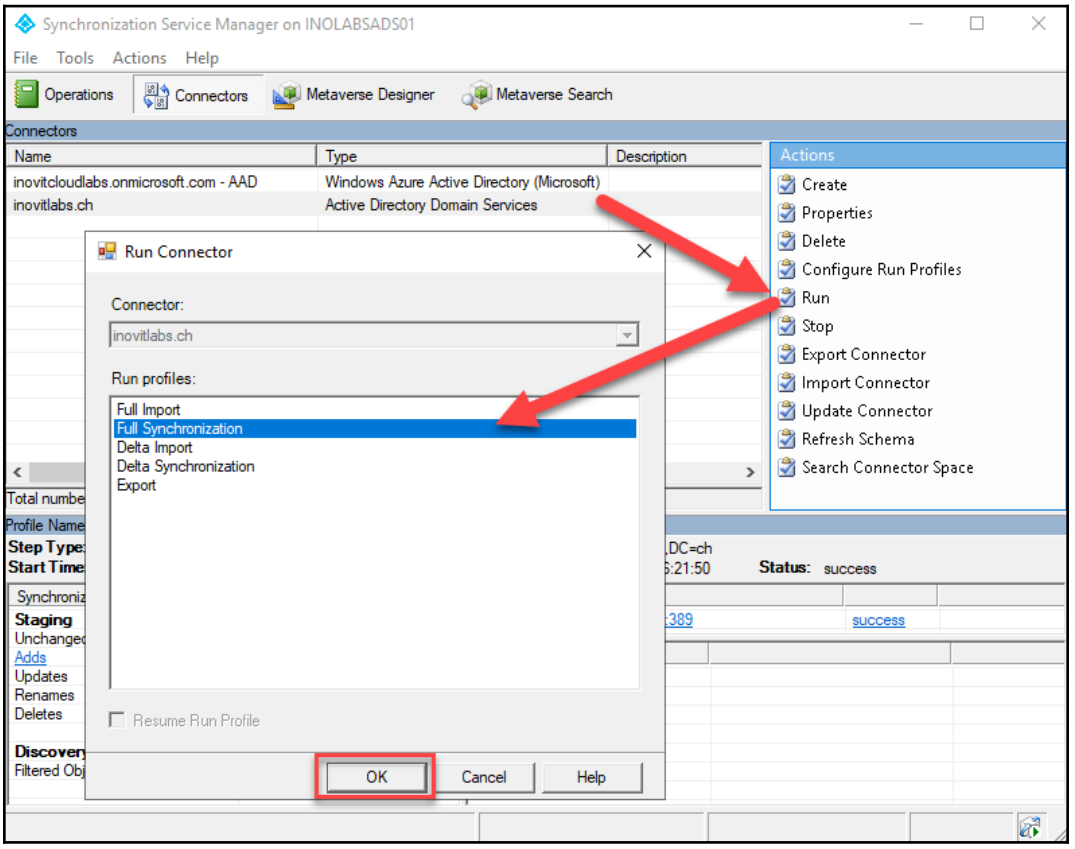

Synchronization Service Manager on INOLABSADS01
File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connectors
Name
Type
Description
inovitcloudlabs.onmicrosoft.com - AAD
Windows Azure Active Directory (Microsoft)
inovitlabs.ch
Active Directory Domain Services
Actions
Create
Properties
Delete
Configure Run Profiles
Run
Stop
Export Connector
Import Connector
Update Connector
Refresh Schema
Search Connector Space
Run Connector
Connector:
inovitcloudlabs.onmicrosoft.com - AAD
Run profiles:
Full Import
Full Synchronization
Delta Import
Delta Synchronization
Export
Resume Run Profile
OK
Cancel
Help
Profile Name:
Step Type:
Start Time:
Status:

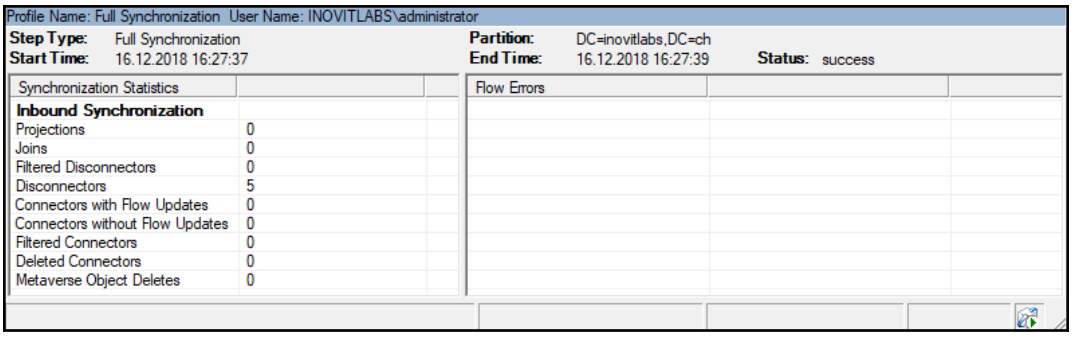

Profile Name: Full Import User Name: INOVITLABS\administrator
Step Type: Full Import (Stage Only)
Start Time: 16.12.2018 16:24:53
Partition: default
End Time: 16.12.2018 16:25:25
Status: completed-no-objects
Synchronization Statistics
Staging
Unchanged 0
Adds 0
Updates 0
Renames 0
Deletes 0
Connection Status
Synchronization Errors

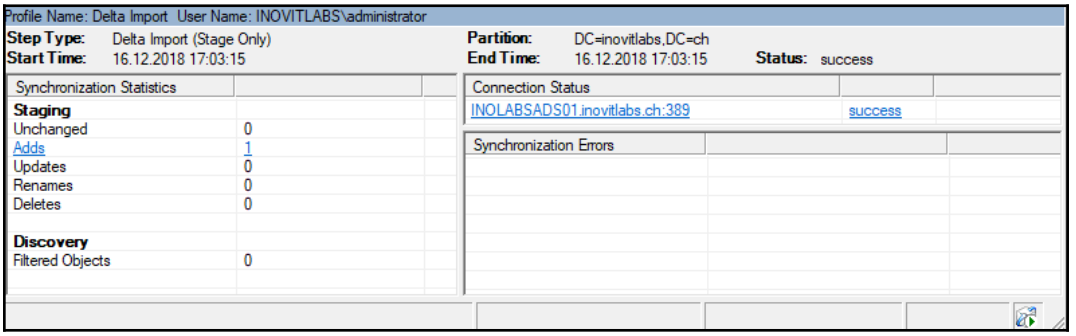

Connector Space
(CS)
Metaverse
(MV)
Connector Space
(CS)
Connected
Directory
Connector
Connector
Sync
(IN)
Sync
(OUT)
Active Directory
Synchronization Engine

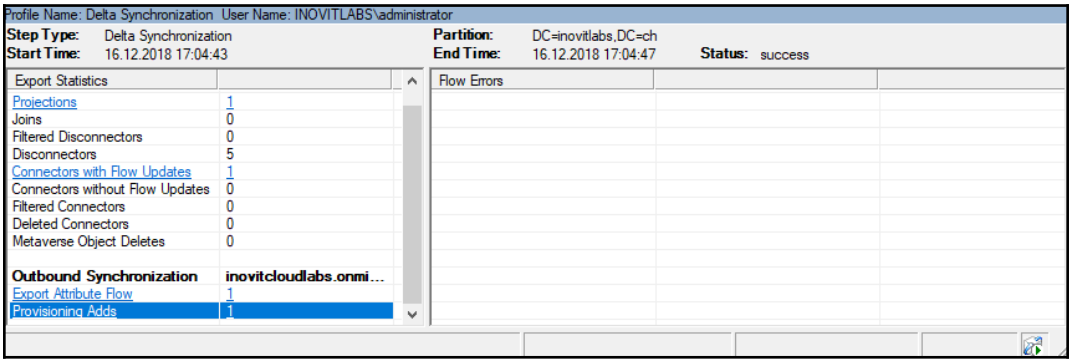

Synchronization Rules Editor
View and manage your synchronization rules
Direction:
Inbound
Outbound
MV Object Type:
Connector:
*
Connector Object Type:
Disabled:
*
Add new rule
MV attribute:
Connector Attribute:
Rule Type:
Name
Connector
Precedence
Connector Object Type
Metaverse Object Type
In from AD - User Join
inovitlabs.ch
100
user
person
In from AD - InetOrgPerson Join
inovitlabs.ch
101
inetOrgPerson
person
In from AD - User AccountEnabled
inovitlabs.ch
102
user
person
In from AD - InetOrgPerson AccountEnabled
inovitlabs.ch
103
inetOrgPerson
person
In from AD - User Common
inovitlabs.ch
104
user
person
In from AD - InetOrgPerson Common
inovitlabs.ch
105
inetOrgPerson
person
In from AD - Group Join
inovitlabs.ch
106
group
group
In from AD - Group Common
inovitlabs.ch
107
group
group
In from AD - Contact Join
inovitlabs.ch
108
contact
person
In from AD - Contact Common
inovitlabs.ch
109
contact
person
In from AD - ForeignSecurityPrincipal Join Us
inovitlabs.ch
110
foreignSecurityPrincipal
*
In from AAD - User Join
inovitcloudlabs.onmicrosoft.com - AAD
111
user
person
In from AAD - Contact Join
inovitcloudlabs.onmicrosoft.com - AAD
112
contact
person
In from AAD - Group Join
inovitcloudlabs.onmicrosoft.com - AAD
113
group
group
In from AAD - User NGCKey
inovitcloudlabs.onmicrosoft.com - AAD
114
user
person
Type:
Transformations:
Disabled:
Scoping filters
Join rules
Edit
Export
Delete

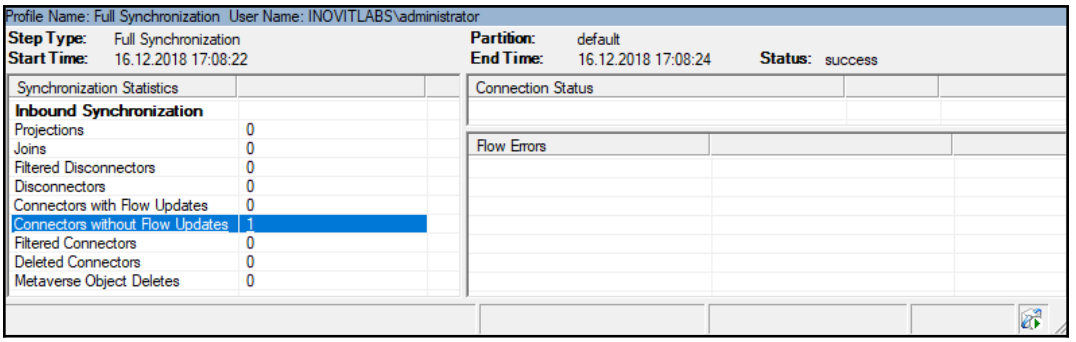

Projection
Join
Import attribute flow
Connector Space (CS)
Metaverse (MV)
Connector Space (CS)
Connected Directory
Connector
Connector
Active Directory
Sync (IN)
Synchronization Engine

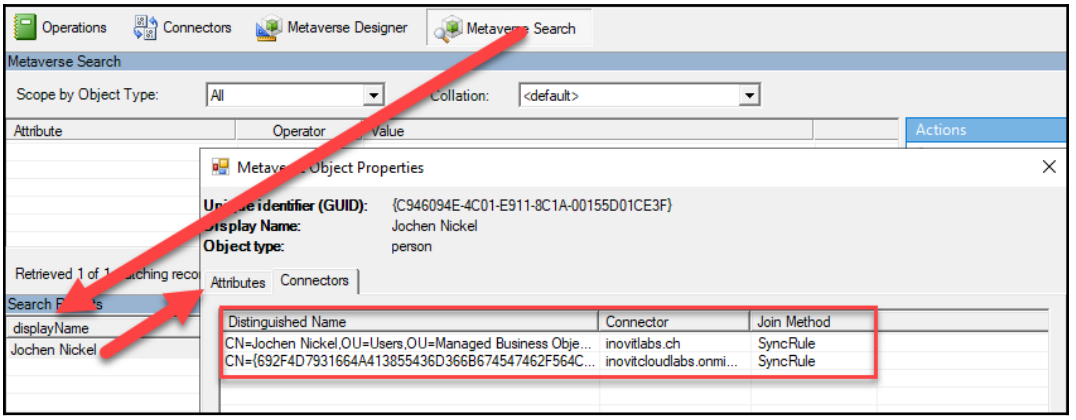

Synchronization Service Manager on INOLABSADS01
File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connectors
Name
Type
Description
inovitcloudlabs.onmicrosoft.com - AAD
Windows Azure Active Directory (Microsoft)
inovitlabs.ch
Active Directory Domain Services
Actions
Create
Properties
Delete
Configure Run Profiles
Run
Stop
Export Connector
Import Connector
Update Connector
Refresh Schema
Search Connector Space
Run Connector
Connector:
inovitlabs.ch
Run profiles:
Full Import
Full Synchronization
Delta Import
Delta Synchronization
Export
Resume Run Profile
OK
Cancel
Help
Status: success

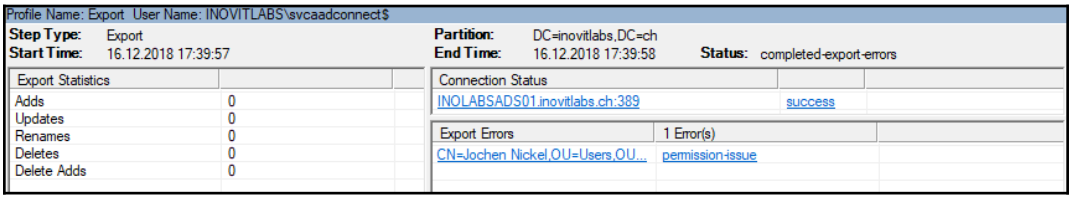

Profile Name: Full Synchronization User Name: INOVITLABS\administrator
Step Type: Full Synchronization
Start Time: 16.12.2018 16:27:37
Partition: DC=inovitlabs,DC=ch
End Time: 16.12.2018 16:27:39
Status: success
Synchronization Statistics
Inbound Synchronization
Projections 0
Joins 0
Filtered Disconnectors 0
Disconnectors 5
Connectors with Flow Updates 0
Connectors without Flow Updates 0
Filtered Connectors 0
Deleted Connectors 0
Metaverse Object Deletes 0
Flow Errors

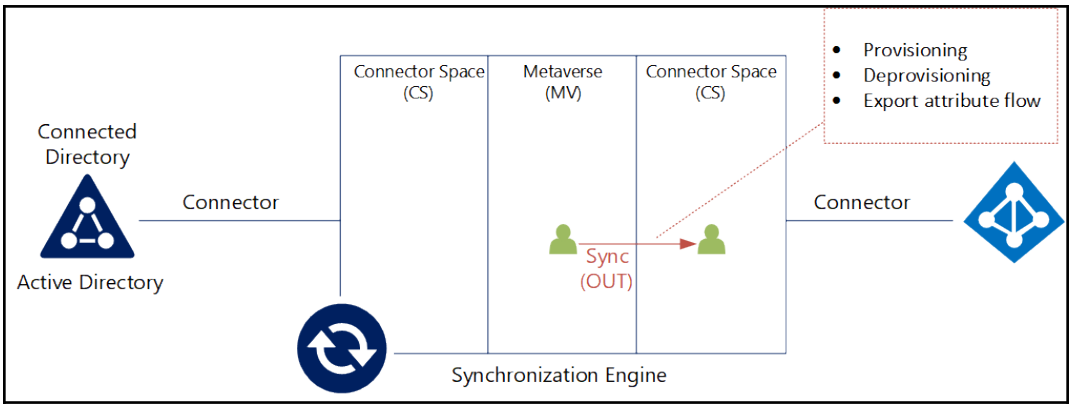

Profile Name: Delta Import User Name: INOVITLABS\administrator
Step Type: Delta Import (Stage Only)
Start Time: 16.12.2018 17:03:15
Partition: DC=inovitlabs,DC=ch
End Time: 16.12.2018 17:03:15
Status: success
Synchronization Statistics
Staging
Unchanged 0
Adds 1
Updates 0
Renames 0
Deletes 0
Discovery
Filtered Objects 0
Connection Status
INOLABSADS01.inovitlabs.ch:389 success
Synchronization Errors

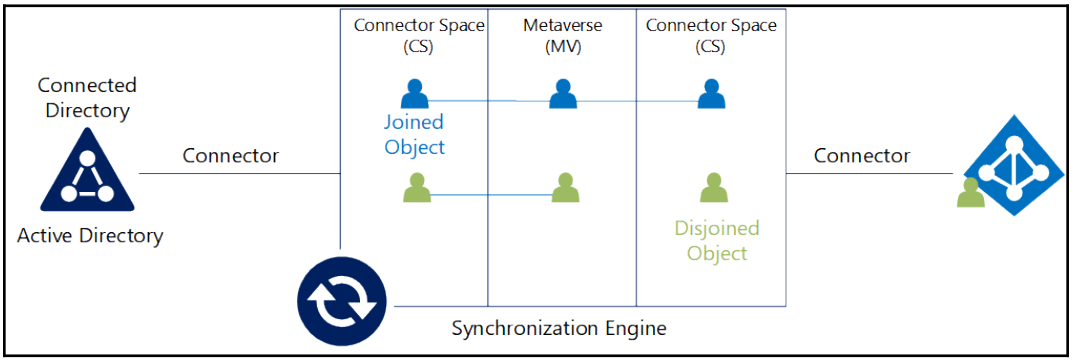

Profile Name: Delta Synchronization User Name: INOVITLABS\administrator
Step Type: Delta Synchronization
Start Time: 16.12.2018 17:04:43
Partition: DC=inovitlabs,DC=ch
End Time: 16.12.2018 17:04:47
Status: success
Export Statistics
Projections 1
Joins 0
Filtered Disconnectors 0
Disconnectors 5
Connectors with Flow Updates 1
Connectors without Flow Updates 0
Filtered Connectors 0
Deleted Connectors 0
Metaverse Object Deletes 0
Outbound Synchronization inovitcloudlabs.onmi...
Export Attribute Flow 1
Provisioning Adds 1
Flow Errors

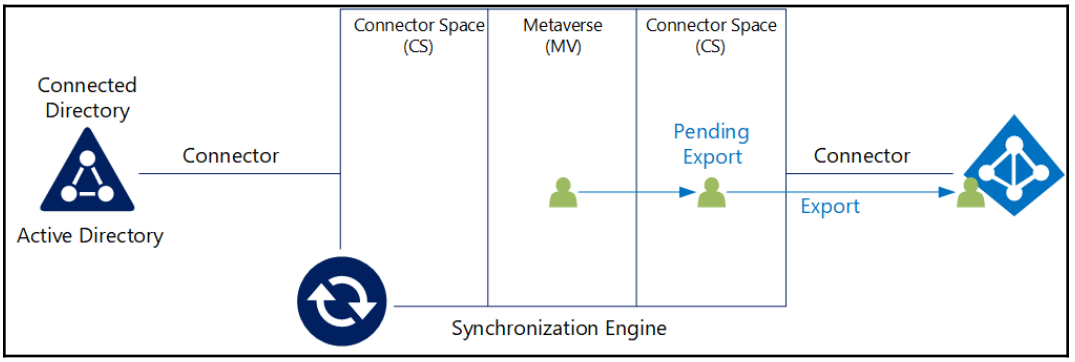

Profile Name: Full Synchronization User Name: INOVITLABS\administrator
Step Type: Full Synchronization
Start Time: 16.12.2018 17:08:22
Partition: default
End Time: 16.12.2018 17:08:24
Status: success
Synchronization Statistics
Inbound Synchronization
Projections 0
Joins 0
Filtered Disconnectors 0
Disconnectors 0
Connectors with Flow Updates 0
Connectors without Flow Updates 1
Filtered Connectors 0
Deleted Connectors 0
Metaverse Object Deletes 0
Connection Status
Flow Errors

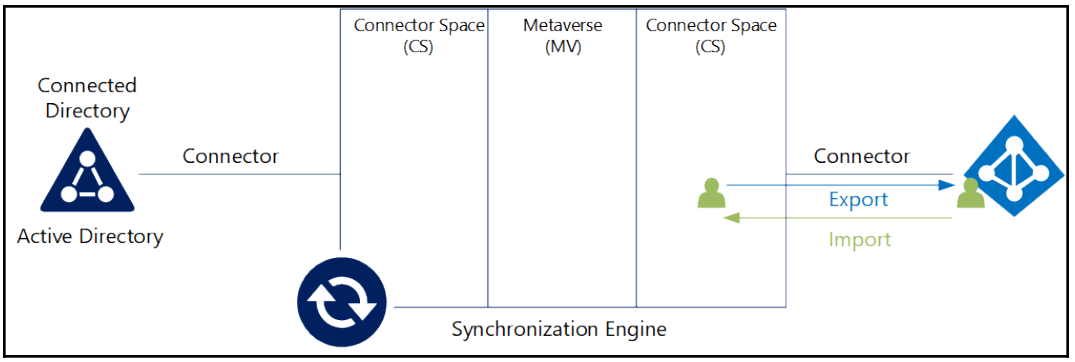

Operations
Connectors
Metaverse Designer
Metaverse Search
Metaverse Search
Scope by Object Type:
All
Collation:
<default>
Attribute
Operator
Value
Actions
Object Properties
Unique identifier (GUID): {C946094E-4C01-E911-8C1A-00155D01CE3F}
Display Name: Jochen Nickel
Object type: person
Attributes
Connectors
displayName
Jochen Nickel
Distinguished Name
Connector
Join Method
CN=Jochen Nickel,OU=Users,OU=Managed Business Obje...
inovitlabs.ch
SyncRule
CN={692F4D7931664A413855436D366B674547462F564C...
inovitcloudlabs.onmi...
SyncRule


Profile Name: Export User Name: INOVITLABS\svcaadconnect$
Step Type: Export
Start Time: 16.12.2018 17:39:57
Partition: DC=inovitlabs,DC=ch
End Time: 16.12.2018 17:39:58
Status: completed-export-errors
Export Statistics
Adds 0
Updates 0
Renames 0
Deletes 0
Delete Adds 0
Connection Status
INOLABSADS01.inovitlabs.ch:389
success
Export Errors
1 Error(s)
CN=Jochen Nickel,OU=Users,OU...
permission-issue

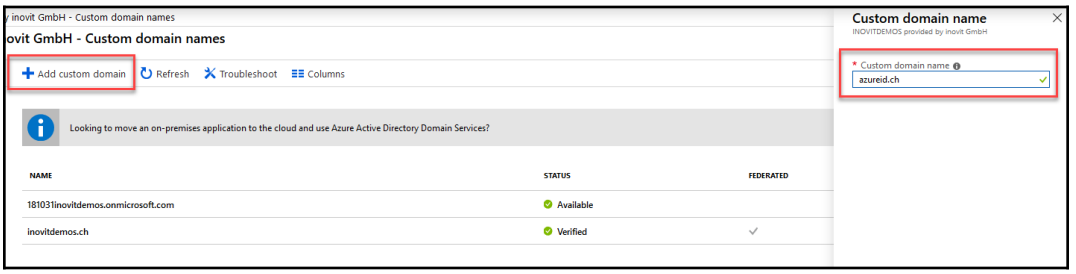

Connector Space (CS)
Metaverse (MV)
Connector Space (CS)
Provisioning
Deprovisioning
Export attribute flow
Connected Directory
Connector
Connector
Active Directory
Sync (OUT)
Synchronization Engine

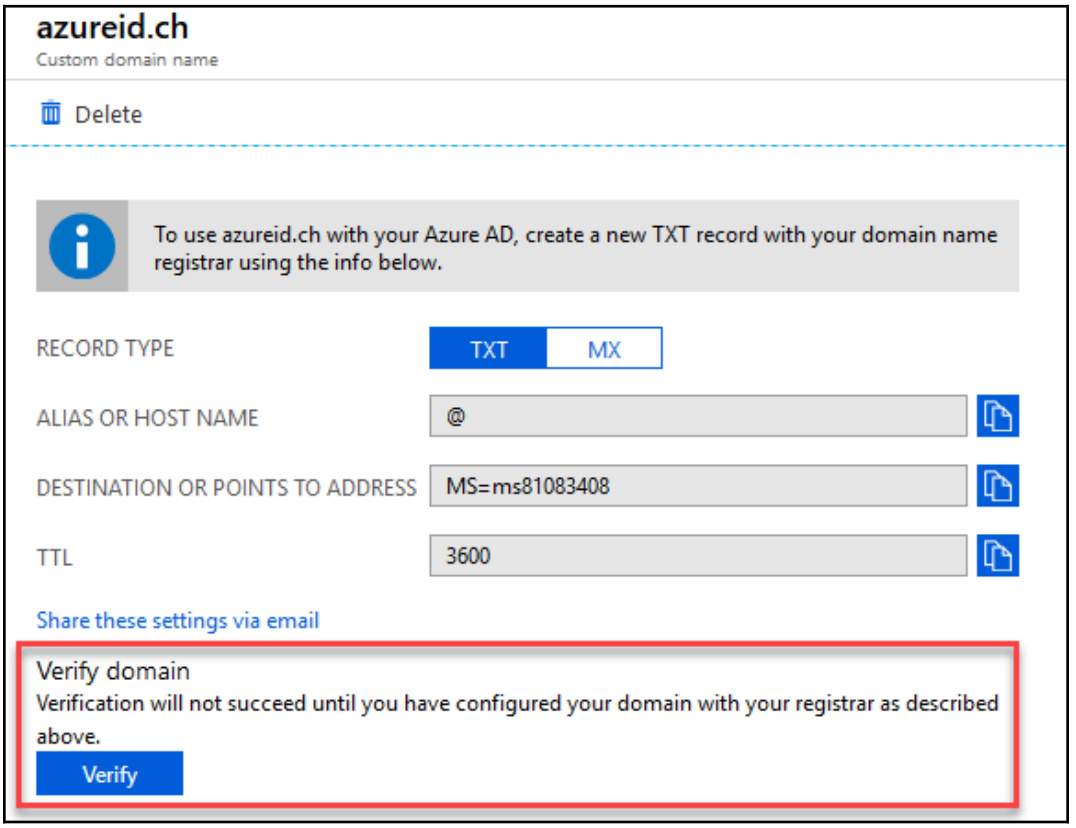

Connector Space (CS)
Metaverse (MV)
Connector Space (CS)
Connected Directory
Joined Object
Connector
Connector
Active Directory
Disjoined Object
Synchronization Engine


Connector Space (CS)
Metaverse (MV)
Connector Space (CS)
Connected Directory
Pending Export
Connector
Connector
Export
Active Directory
Synchronization Engine

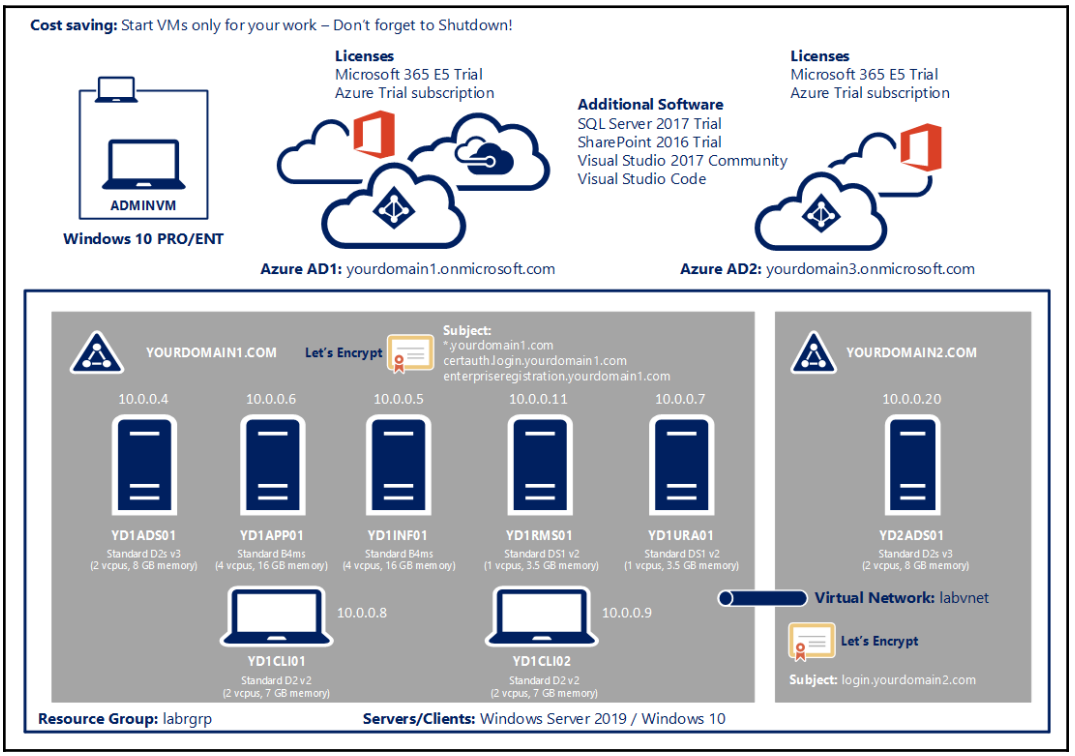

Connector Space
(CS)
Metaverse
(MV)
Connector Space
(CS)
Connected
Directory
Connector
Connector
Export
Import
Active Directory
Synchronization Engine

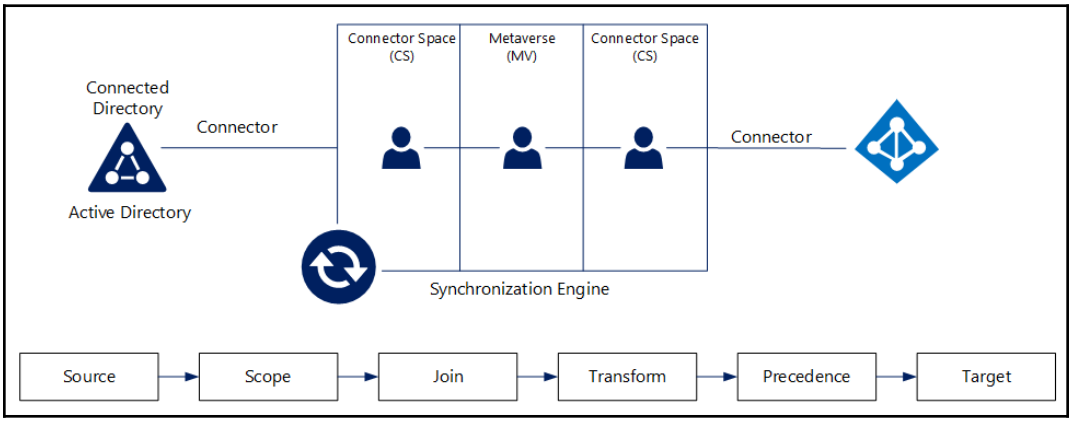
Chapter 3: Exploring Advanced Synchronization Concepts

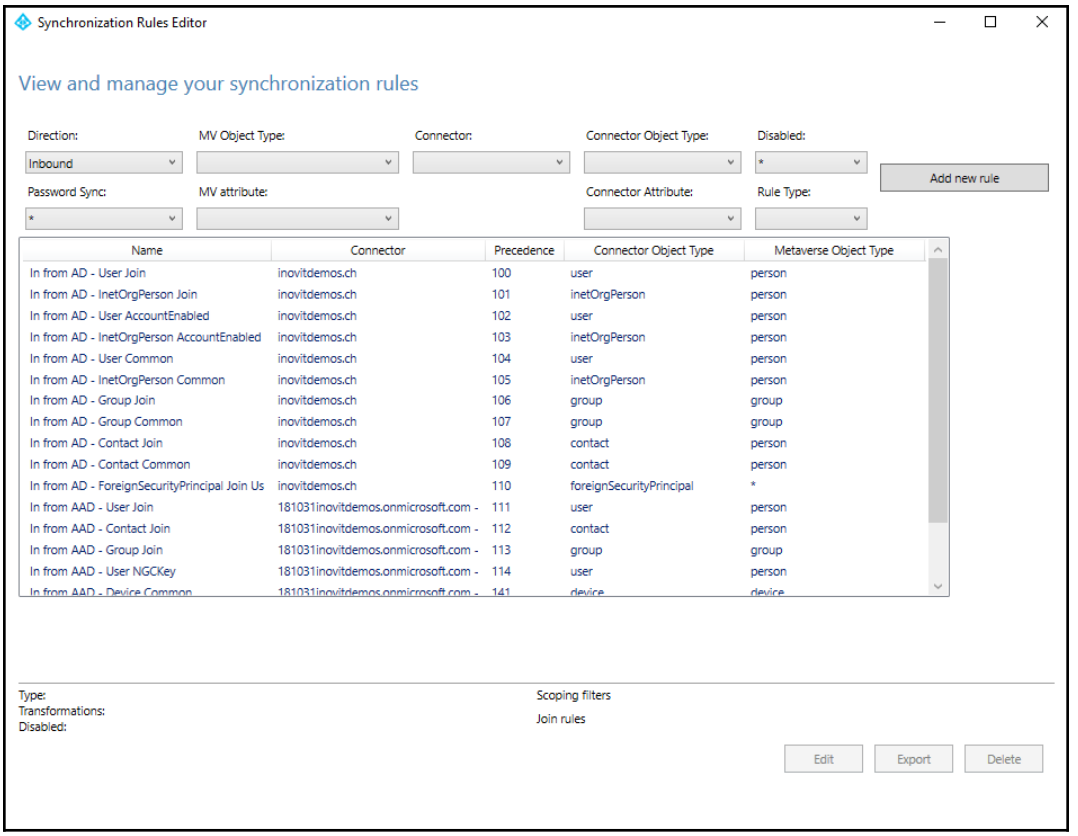


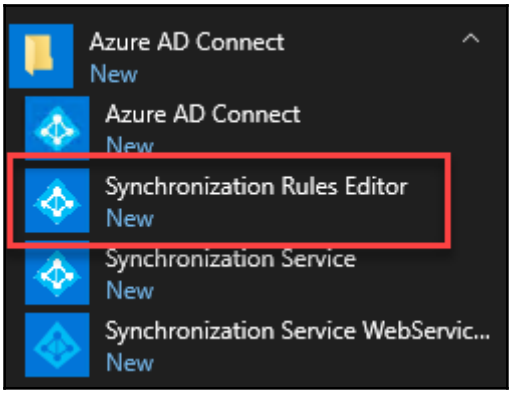


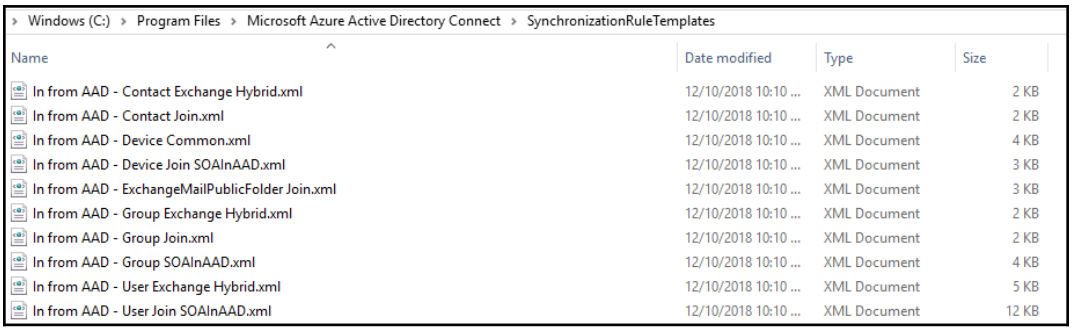
NAME	STATUS	FEDERATED	PRIMARY
azureid.ch	Verified		
181031inovitdemos.onmicrosoft.com	Available		✓
inovitdemos.ch	Verified	✓	

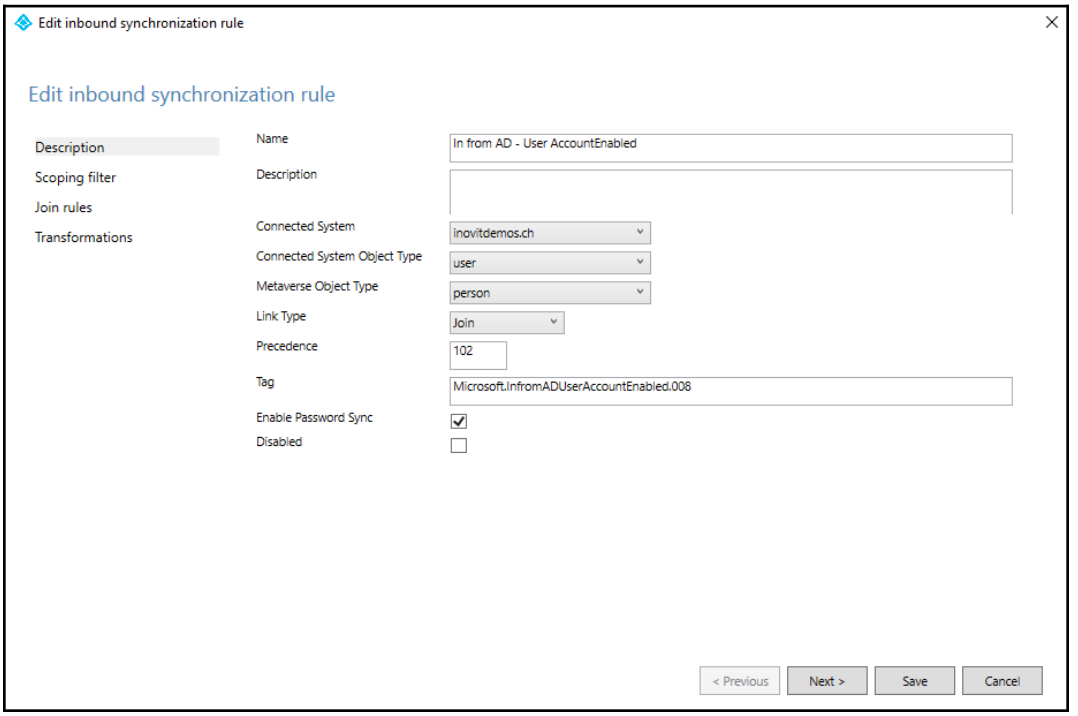


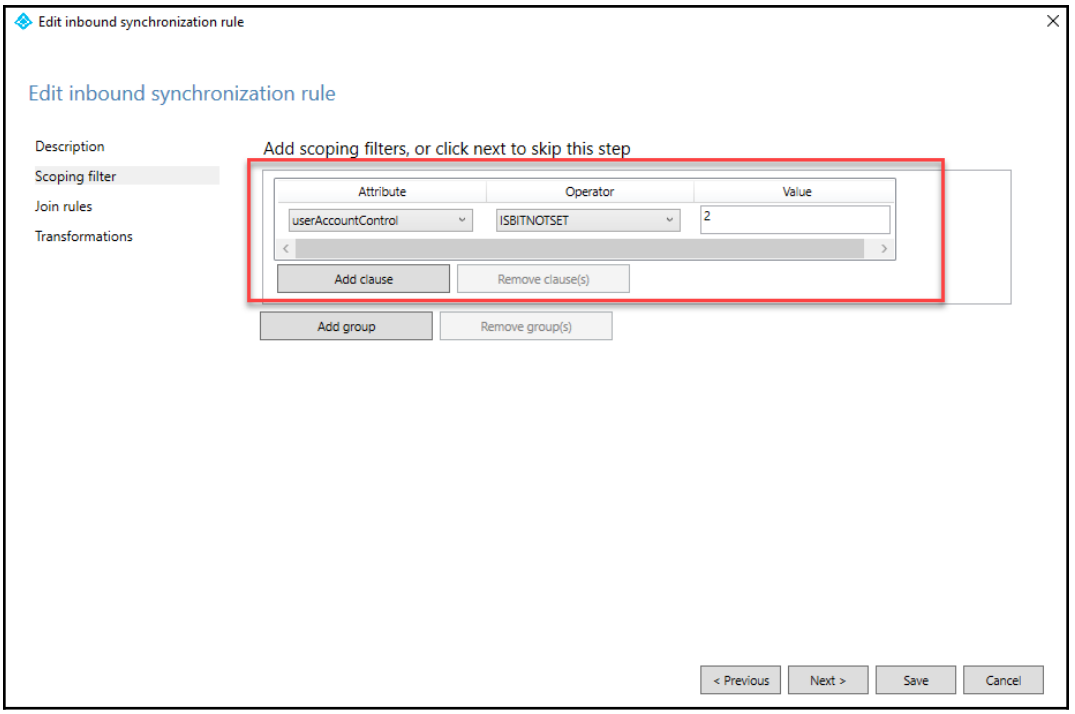


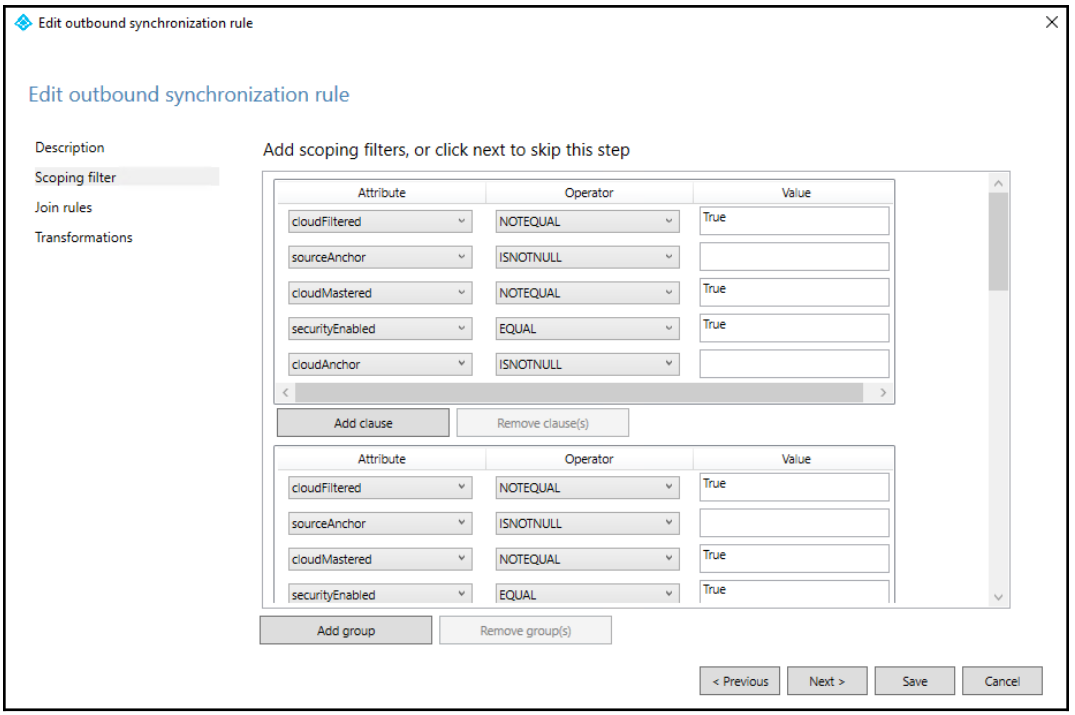

Synchronization Rules Editor
View and manage your synchronization rules
Direction:
Inbound
MV Object Type:
Connector:
Connector Object Type:
Disabled:
*
Add new rule
Password Sync:
*
MV attribute:
Connector Attribute:
Rule Type:
Name
Connector
Precedence
Connector Object Type
Metaverse Object Type
In from AD - User Join
inovitdemos.ch
100
user
person
In from AD - InetOrgPerson Join
inovitdemos.ch
101
inetOrgPerson
person
In from AD - User AccountEnabled
inovitdemos.ch
102
user
person
In from AD - InetOrgPerson AccountEnabled
inovitdemos.ch
103
inetOrgPerson
person
In from AD - User Common
inovitdemos.ch
104
user
person
In from AD - InetOrgPerson Common
inovitdemos.ch
105
inetOrgPerson
person
In from AD - Group Join
inovitdemos.ch
106
group
group
In from AD - Group Common
inovitdemos.ch
107
group
group
In from AD - Contact Join
inovitdemos.ch
108
contact
person
In from AD - Contact Common
inovitdemos.ch
109
contact
person
In from AD - ForeignSecurityPrincipal Join Us
inovitdemos.ch
110
foreignSecurityPrincipal
*
In from AAD - User Join
181031inovitdemos.onmicrosoft.com -
111
user
person
In from AAD - Contact Join
181031inovitdemos.onmicrosoft.com -
112
contact
person
In from AAD - Group Join
181031inovitdemos.onmicrosoft.com -
113
group
group
In from AAD - User NGCKey
181031inovitdemos.onmicrosoft.com -
114
user
person
Type:
Transformations:
Disabled:
Scoping filters
Join rules
Edit
Export
Delete

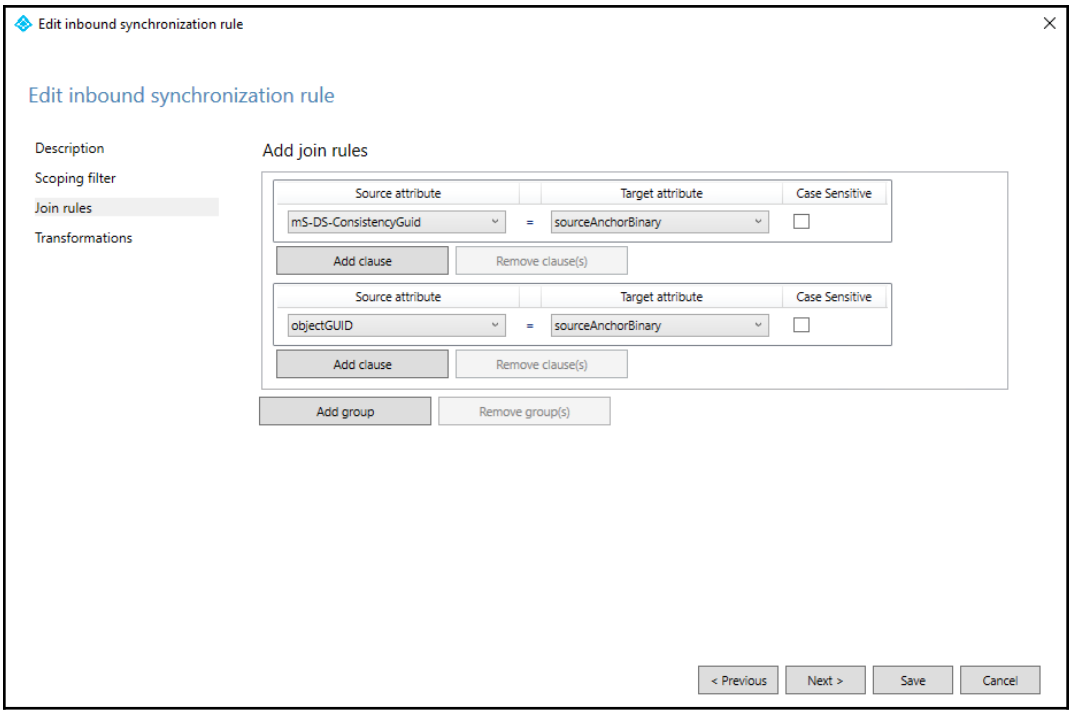

Azure AD Connect
New
Azure AD Connect
New
Synchronization Rules Editor
New
Synchronization Service
New
Synchronization Service WebServic...
New

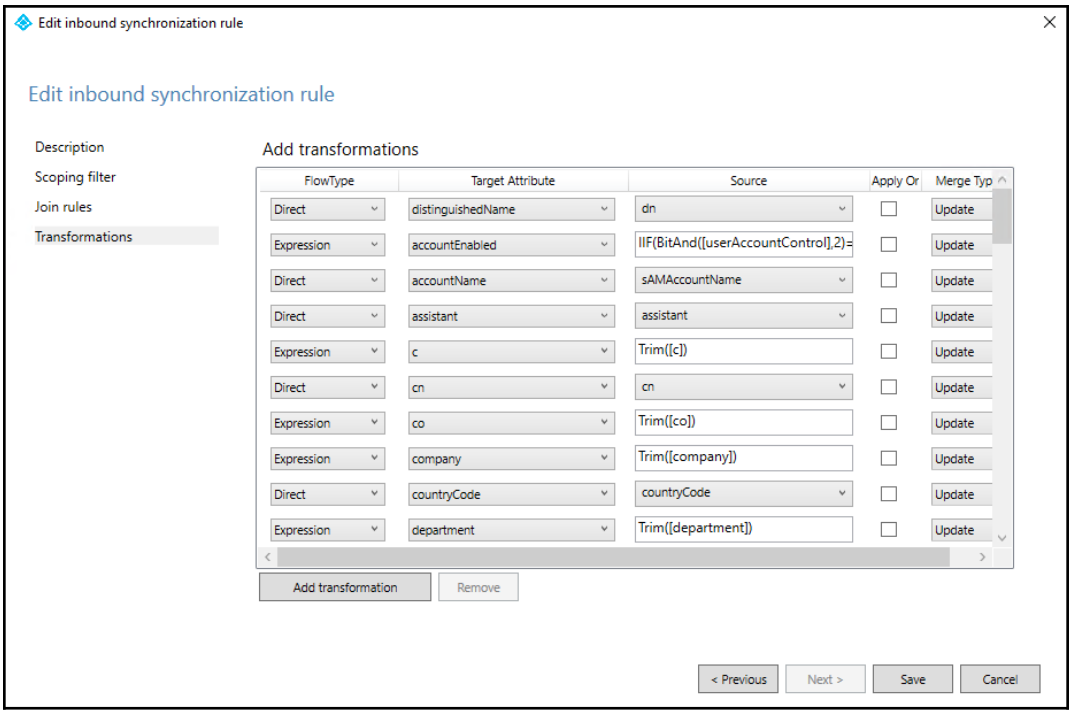

Windows (C:) › Program Files › Microsoft Azure Active Directory Connect › SynchronizationRuleTemplates
Name
Date modified
Type
Size
In from AAD - Contact Exchange Hybrid.xml 12/10/2018 10:10 ... XML Document 2 KB
In from AAD - Contact Join.xml 12/10/2018 10:10 ... XML Document 2 KB
In from AAD - Device Common.xml 12/10/2018 10:10 ... XML Document 4 KB
In from AAD - Device Join SOAInAAD.xml 12/10/2018 10:10 ... XML Document 3 KB
In from AAD - ExchangeMailPublicFolder Join.xml 12/10/2018 10:10 ... XML Document 3 KB
In from AAD - Group Exchange Hybrid.xml 12/10/2018 10:10 ... XML Document 2 KB
In from AAD - Group Join.xml 12/10/2018 10:10 ... XML Document 2 KB
In from AAD - Group SOAInAAD.xml 12/10/2018 10:10 ... XML Document 4 KB
In from AAD - User Exchange Hybrid.xml 12/10/2018 10:10 ... XML Document 5 KB
In from AAD - User Join SOAInAAD.xml 12/10/2018 10:10 ... XML Document 12 KB


Edit inbound synchronization rule
Edit inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Name
In from AD - User AccountEnabled
Description
Connected System
inovitdemos.ch
Connected System Object Type
user
Metaverse Object Type
person
Link Type
Join
Precedence
102
Tag
Microsoft.InfromADUserAccountEnabled.008
Enable Password Sync
Disabled
< Previous
Next >
Save
Cancel

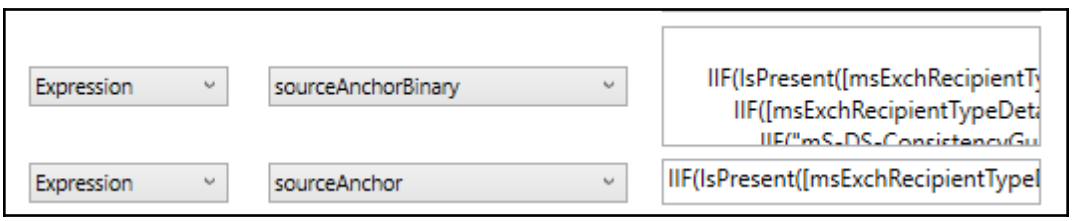

Edit inbound synchronization rule
Edit inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Add scoping filters, or click next to skip this step
Attribute
Operator
Value
userAccountControl
ISBITNOTSET
2
Add clause
Remove clause(s)
Add group
Remove group(s)
< Previous
Next >
Save
Cancel

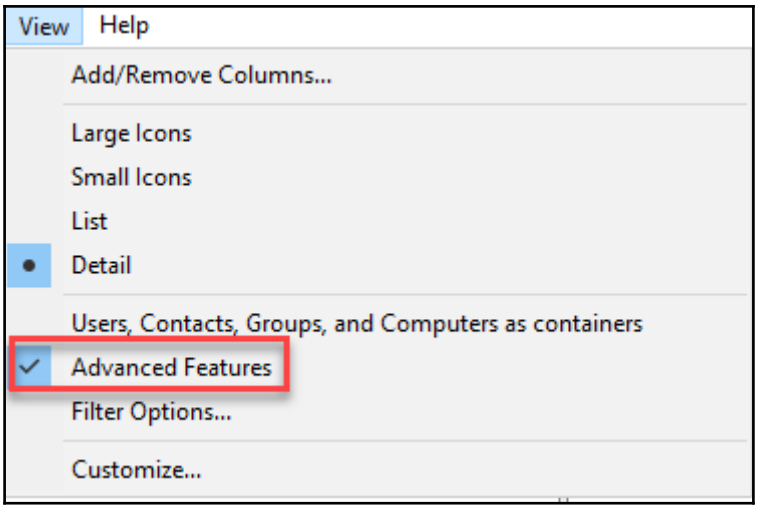

Edit outbound synchronization rule
Edit outbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Add scoping filters, or click next to skip this step
Attribute
Operator
Value
cloudFiltered
NOTEQUAL
True
sourceAnchor
ISNOTNULL
cloudMastered
NOTEQUAL
True
securityEnabled
EQUAL
True
cloudAnchor
ISNOTNULL
Add clause
Remove clause(s)
Attribute
Operator
Value
cloudFiltered
NOTEQUAL
True
sourceAnchor
ISNOTNULL
cloudMastered
NOTEQUAL
True
securityEnabled
EQUAL
True
Add group
Remove group(s)
< Previous
Next >
Save
Cancel

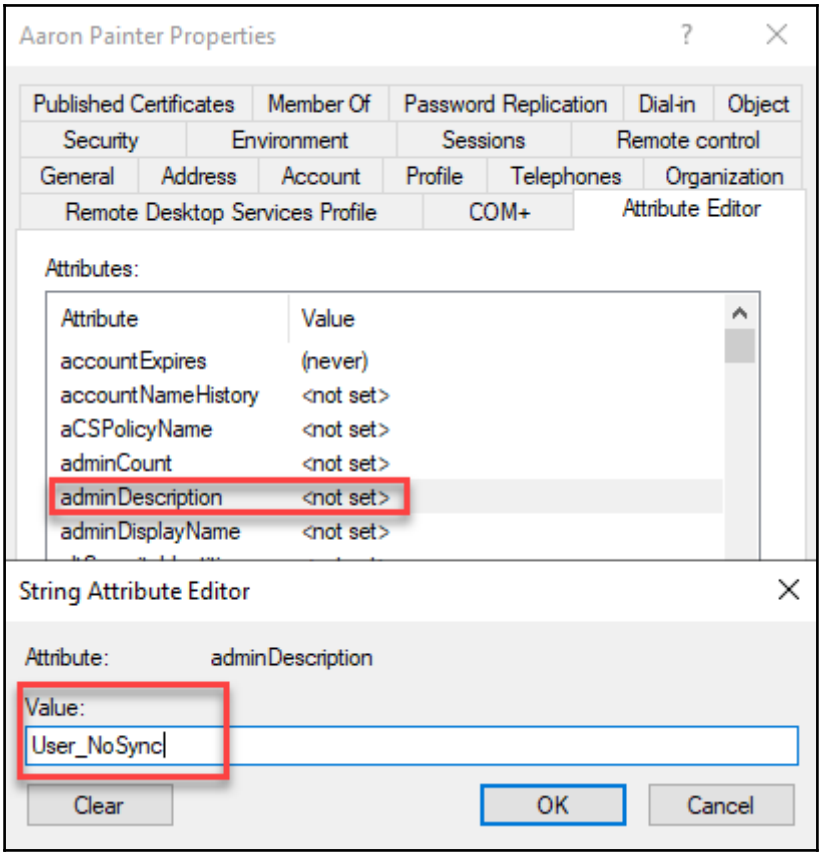

Edit inbound synchronization rule
Edit inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Add join rules
Source attribute
Target attribute
Case Sensitive
mS-DS-ConsistencyGuid
=
sourceAnchorBinary
Add clause
Remove clause(s)
Source attribute
Target attribute
Case Sensitive
objectGUID
=
sourceAnchorBinary
Add clause
Remove clause(s)
Add group
Remove group(s)
< Previous
Next >
Save
Cancel

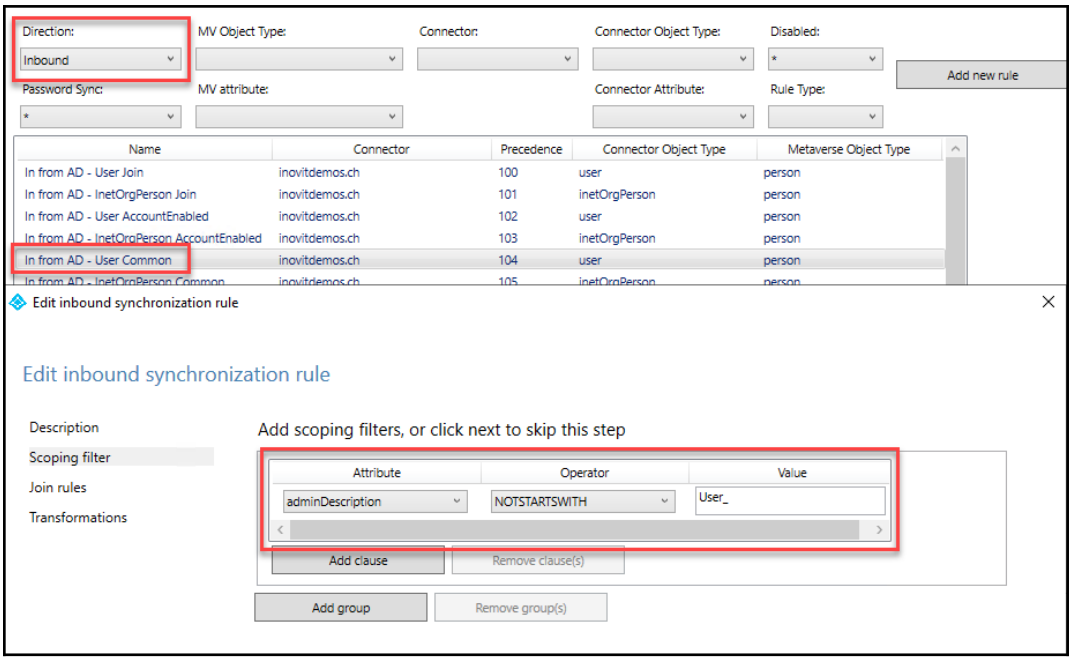

Edit inbound synchronization rule
Edit inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Add transformations
FlowType
Target Attribute
Source
Apply Or
Merge Typ
Direct
distinguishedName
dn
Update
Expression
accountEnabled
IIF(BitAnd([userAccountControl],2)=
Update
Direct
accountName
sAMAccountName
Update
Direct
assistant
assistant
Update
Expression
c
Trim([c])
Update
Direct
cn
cn
Update
Expression
co
Trim([co])
Update
Expression
company
Trim([company])
Update
Direct
countryCode
countryCode
Update
Expression
department
Trim([department])
Update
Add transformation
Remove
< Previous
Next >
Save
Cancel


Expression
sourceAnchorBinary
IIF(IsPresent([msExchRecipientTy
IIF([msExchRecipientTypeDeta
Expression
sourceAnchor
IIF(IsPresent([msExchRecipientTypeI

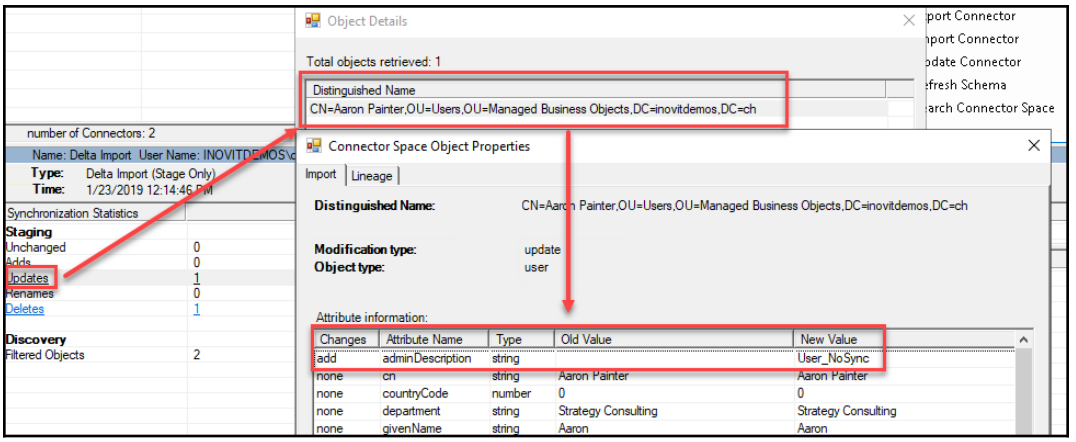

Expression
sourceAnchorBinary
IIF(IsPresent([msExchRecipientTy
IIF([msExchRecipientTypeDeta
Expression
sourceAnchor
IIF(IsPresent([msExchRecipientTypeI

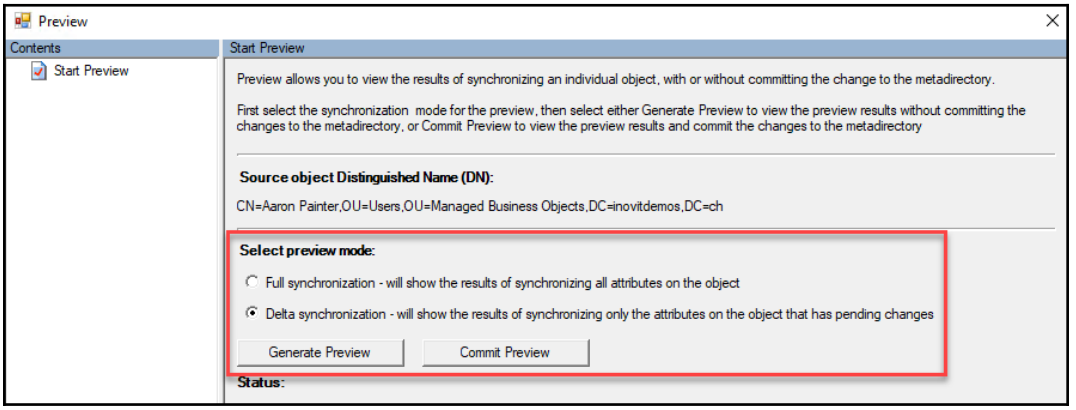

View
Help
Add/Remove Columns...
Large Icons
Small Icons
List
Detail
Users, Contacts, Groups, and Computers as containers
Advanced Features
Filter Options...
Customize...

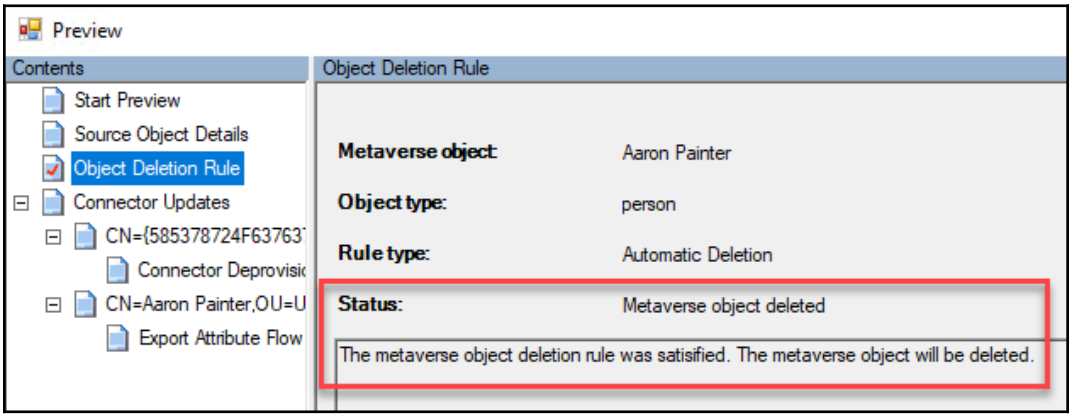

Aaron Painter Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Remote Desktop Services Profile
COM+
Attribute Editor
Attributes:
Attribute
Value
accountExpires
(never)
accountNameHistory
<not set>
aCSPolicyName
<not set>
adminCount
<not set>
adminDescription
<not set>
adminDisplayName
<not set>
String Attribute Editor
Attribute:
adminDescription
Value:
User_NoSync
Clear
OK
Cancel

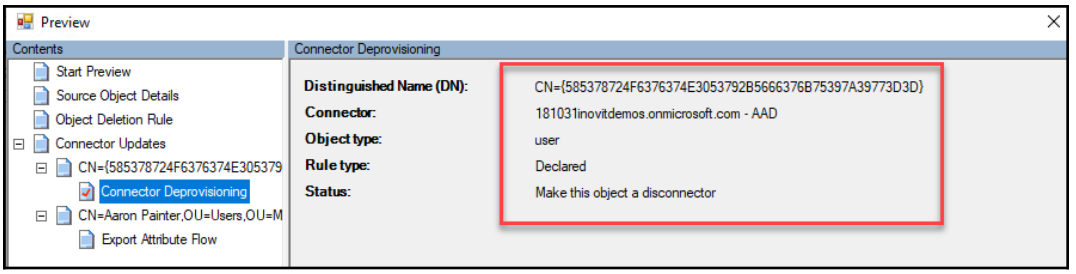


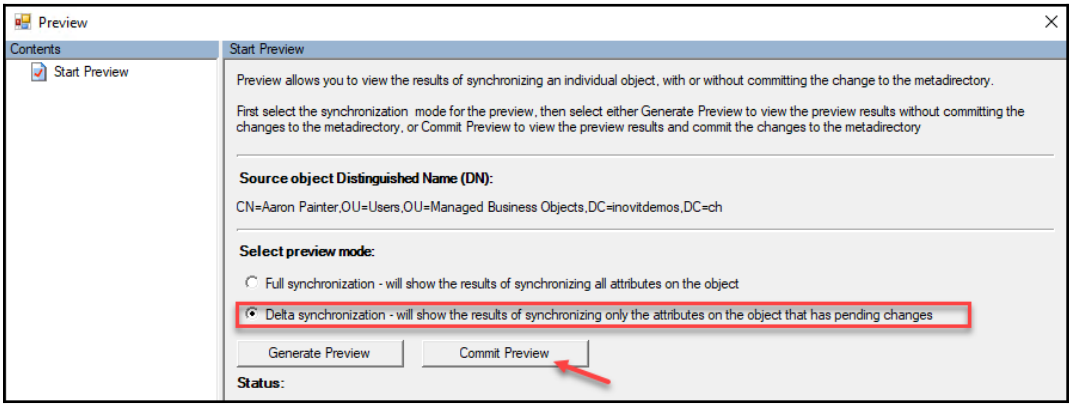
Synchronization Statistics	
Staging	
Unchanged	0
Adds	0
Updates	1
Renames	0
Deletes	1
Discovery	
Filtered Objects	2

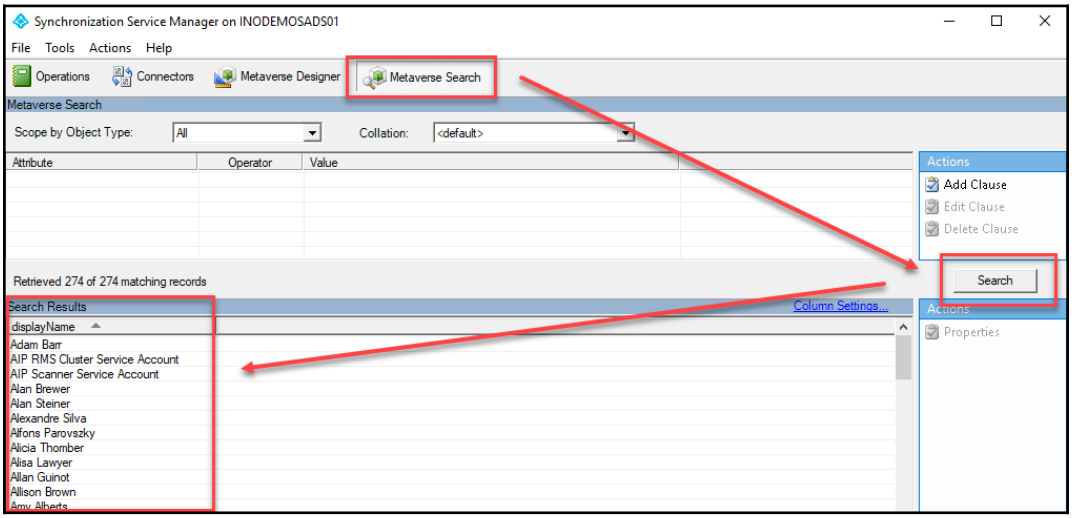

Object Details
Total objects retrieved: 1
Distinguished Name
CN=Aaron Painter,OU=Users,OU=Managed Business Objects,DC=inovitdemos,DC=ch
number of Connectors: 2
Type: Delta Import (Stage Only)
Time: 1/23/2019 12:14:46 PM
Synchronization Statistics
Staging
Unchanged 0
Adds 0
Updates 1
Renames 0
Deletes 1
Discovery
Filtered Objects 2
Connector Space Object Properties
Import
Lineage
Distinguished Name: CN=Aaron Painter,OU=Users,OU=Managed Business Objects,DC=inovitdemos,DC=ch
Modification type: update
Object type: user
Attribute information:
Changes
Attribute Name
Type
Old Value
New Value
add adminDescription string User_NoSync
none cn string Aaron Painter Aaron Painter
none countryCode number 0 0
none department string Strategy Consulting Strategy Consulting
none givenName string Aaron Aaron

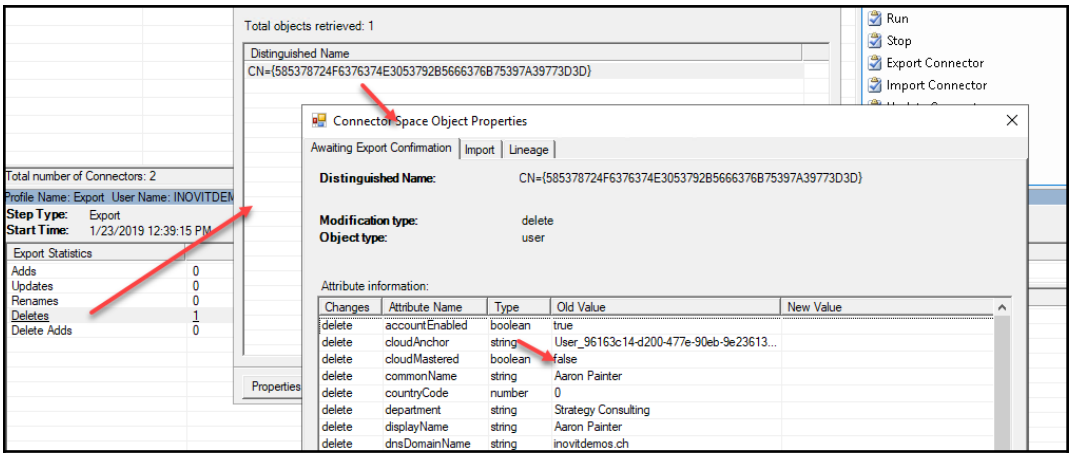

Preview
Contents
Start Preview
Start Preview
Preview allows you to view the results of synchronizing an individual object, with or without committing the change to the metadirectory.
First select the synchronization mode for the preview, then select either Generate Preview to view the preview results without committing the changes to the metadirectory, or Commit Preview to view the preview results and commit the changes to the metadirectory
Source object Distinguished Name (DN):
CN=Aaron Painter,OU=Users,OU=Managed Business Objects,DC=inovitdemos,DC=ch
Select preview mode:
Full synchronization - will show the results of synchronizing all attributes on the object
Delta synchronization - will show the results of synchronizing only the attributes on the object that has pending changes
Generate Preview
Commit Preview
Status:

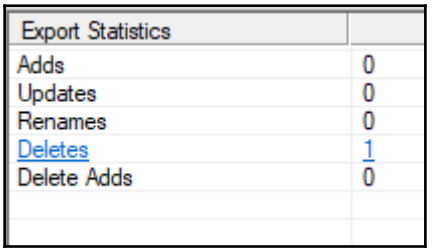

Preview
Contents
Start Preview
Source Object Details
Object Deletion Rule
Connector Updates
CN={585378724F63763
Connector Deprovisic
CN=Aaron Painter,OU=U
Export Attribute Flow
Object Deletion Rule
Metaverse object: Aaron Painter
Object type: person
Rule type: Automatic Deletion
Status: Metaverse object deleted
The metaverse object deletion rule was satisfied. The metaverse object will be deleted.

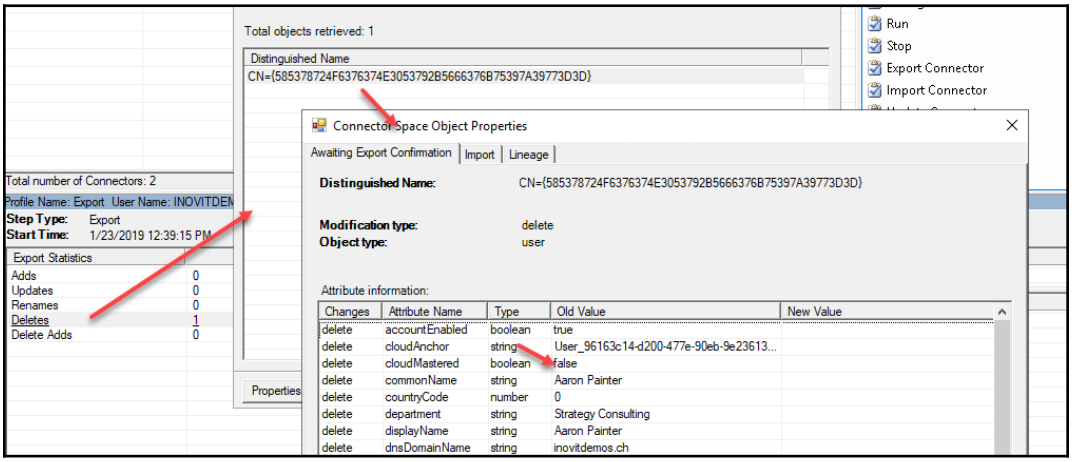

Preview
Contents
Start Preview
Source Object Details
Object Deletion Rule
Connector Updates
CN={585378724F6376374E305379
Connector Deprovisioning
CN=Aaron Painter,OU=Users,OU=M
Export Attribute Flow
Connector Deprovisioning
Distinguished Name (DN):
CN={585378724F6376374E3053792B5666376B75397A39773D3D}
Connector:
181031inovitdemos.onmicrosoft.com - AAD
Object type:
user
Rule type:
Declared
Status:
Make this object a disconnector

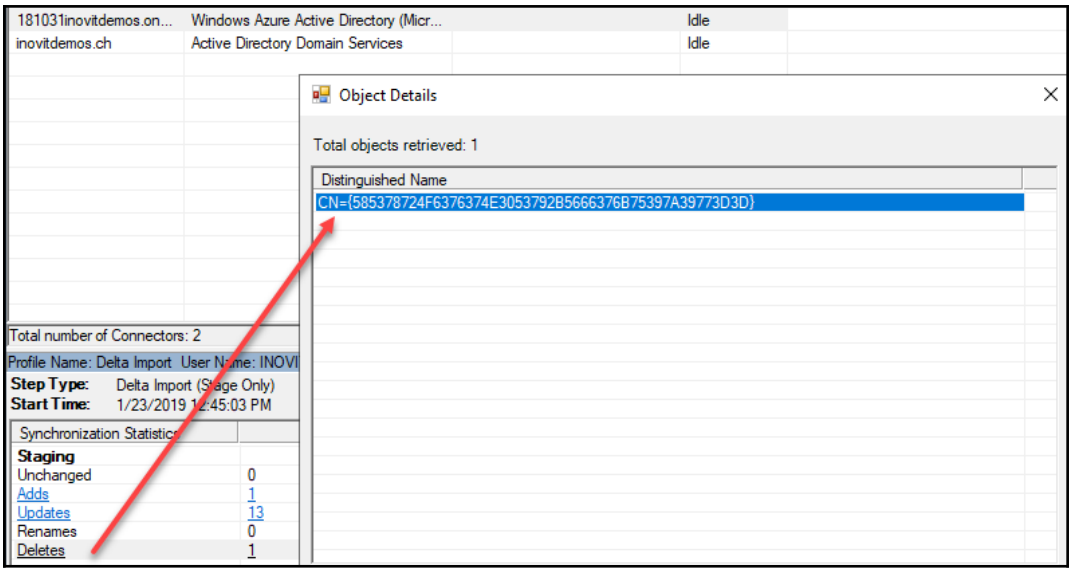

Preview
Contents
Start Preview
Start Preview
Preview allows you to view the results of synchronizing an individual object, with or without committing the change to the metadirectory.
First select the synchronization mode for the preview, then select either Generate Preview to view the preview results without committing the changes to the metadirectory, or Commit Preview to view the preview results and commit the changes to the metadirectory
Source object Distinguished Name (DN):
CN=Aaron Painter,OU=Users,OU=Managed Business Objects,DC=inovitdemos,DC=ch
Select preview mode:
Full synchronization - will show the results of synchronizing all attributes on the object
Delta synchronization - will show the results of synchronizing only the attributes on the object that has pending changes
Generate Preview
Commit Preview
Status:

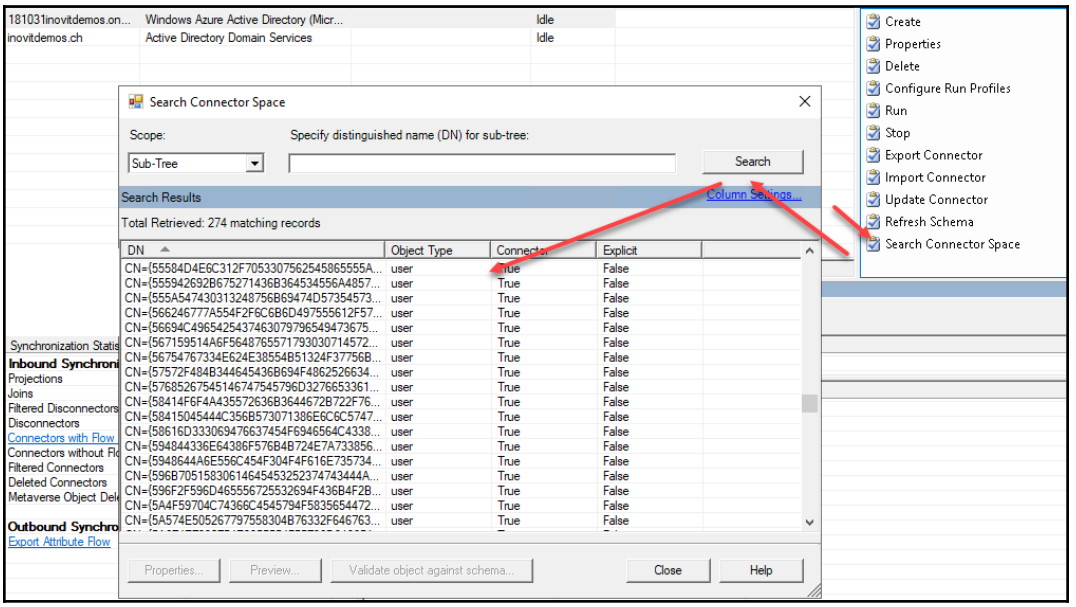

Synchronization Service Manager on INODEMOSADS01
File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Metaverse Search
Scope by Object Type:
All
Collation:
<default>
Attribute
Operator
Value
Actions
Add Clause
Edit Clause
Delete Clause
Search
Retrieved 274 of 274 matching records
Search Results
Column Settings...
displayName
Adam Barr
AIP RMS Cluster Service Account
AIP Scanner Service Account
Alan Brewer
Alan Steiner
Alexandre Silva
Alfons Parovszky
Alicia Thomber
Alisa Lawyer
Allan Guinot
Allison Brown
Actions
Properties

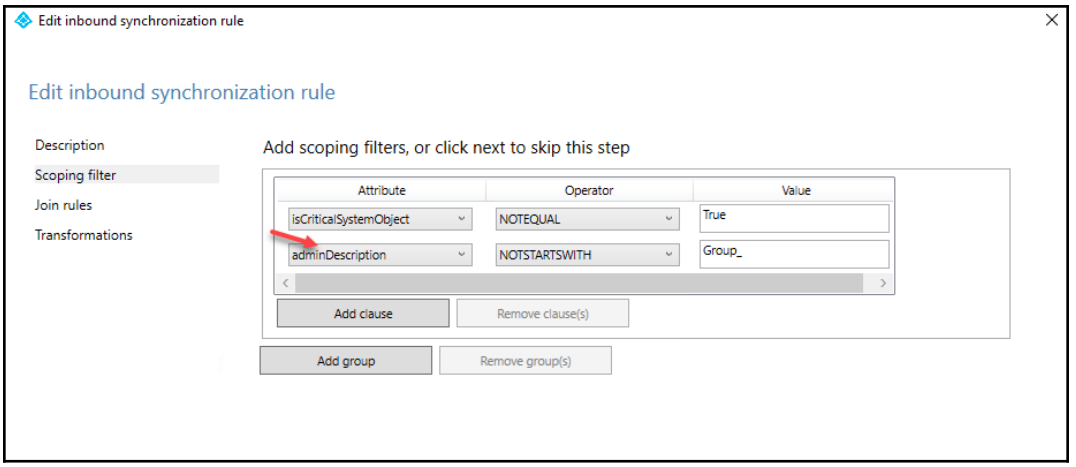

Total objects retrieved: 1
Distinguished Name
CN={585378724F6376374E3053792B5666376B75397A39773D3D}
Run
Stop
Export Connector
Import Connector
Total number of Connectors: 2
Profile Name: Export User Name: INOVITDEM
Step Type: Export
Start Time: 1/23/2019 12:39:15 PM
Export Statistics
Adds 0
Updates 0
Renames 0
Deletes 1
Delete Adds 0
Properties
Connector Space Object Properties
Awaiting Export Confirmation
Import
Lineage
Distinguished Name: CN={585378724F6376374E3053792B5666376B75397A39773D3D}
Modification type: delete
Object type: user
Attribute information:
Changes
Attribute Name
Type
Old Value
New Value
delete accountEnabled boolean true
delete cloudAnchor string User_96163c14-d200-477e-90eb-9e23613...
delete cloudMastered boolean false
delete commonName string Aaron Painter
delete countryCode number 0
delete department string Strategy Consulting
delete displayName string Aaron Painter
delete dnsDomainName string inovitdemos.ch

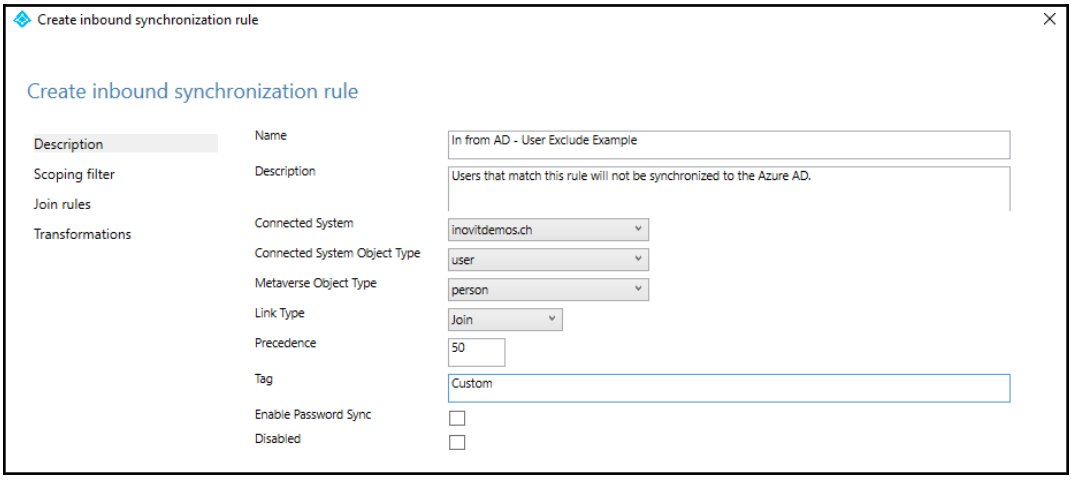

Export Statistics
Adds 0
Updates 0
Renames 0
Deletes 1
Delete Adds 0

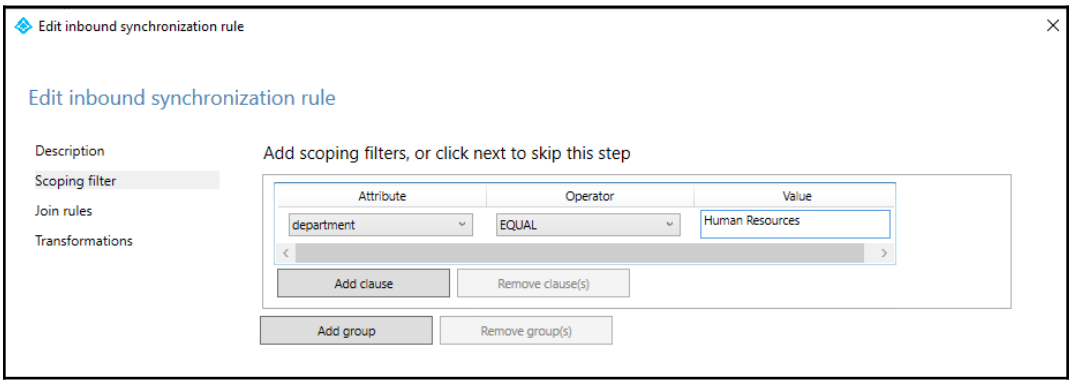

Total objects retrieved: 1
Distinguished Name
CN={585378724F6376374E3053792B5666376B75397A39773D3D}
Run
Stop
Export Connector
Import Connector
Total number of Connectors: 2
Profile Name: Export User Name: INOVITDEM
Step Type: Export
Start Time: 1/23/2019 12:39:15 PM
Export Statistics
Adds 0
Updates 0
Renames 0
Deletes 1
Delete Adds 0
Properties
Connector Space Object Properties
Awaiting Export Confirmation
Import
Lineage
Distinguished Name: CN={585378724F6376374E3053792B5666376B75397A39773D3D}
Modification type: delete
Object type: user
Attribute information:
Changes
Attribute Name
Type
Old Value
New Value
delete accountEnabled boolean true
delete cloudAnchor string User_96163c14-d200-477e-90eb-9e23613...
delete cloudMastered boolean false
delete commonName string Aaron Painter
delete countryCode number 0
delete department string Strategy Consulting
delete displayName string Aaron Painter
delete dnsDomainName string inovitdemos.ch

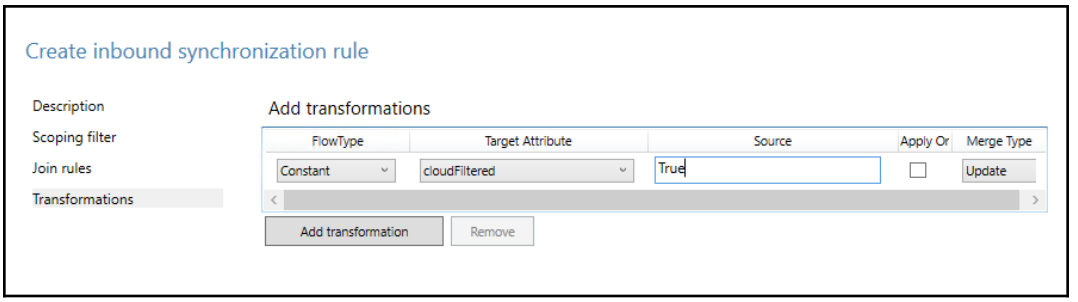

181031inovitdemos.on...
Windows Azure Active Directory (Micr...
Idle
inovitdemos.ch
Active Directory Domain Services
Idle
Object Details
Total objects retrieved: 1
Distinguished Name
CN={585378724F6376374E3053792B5666376B75397A39773D3D}
Total number of Connectors: 2
Profile Name: Delta Import User Name: INOVI
Step Type: Delta Import (Stage Only)
Start Time: 1/23/2019 12:45:03 PM
Synchronization Statistics
Staging
Unchanged 0
Adds 1
Updates 13
Renames 0
Deletes 1

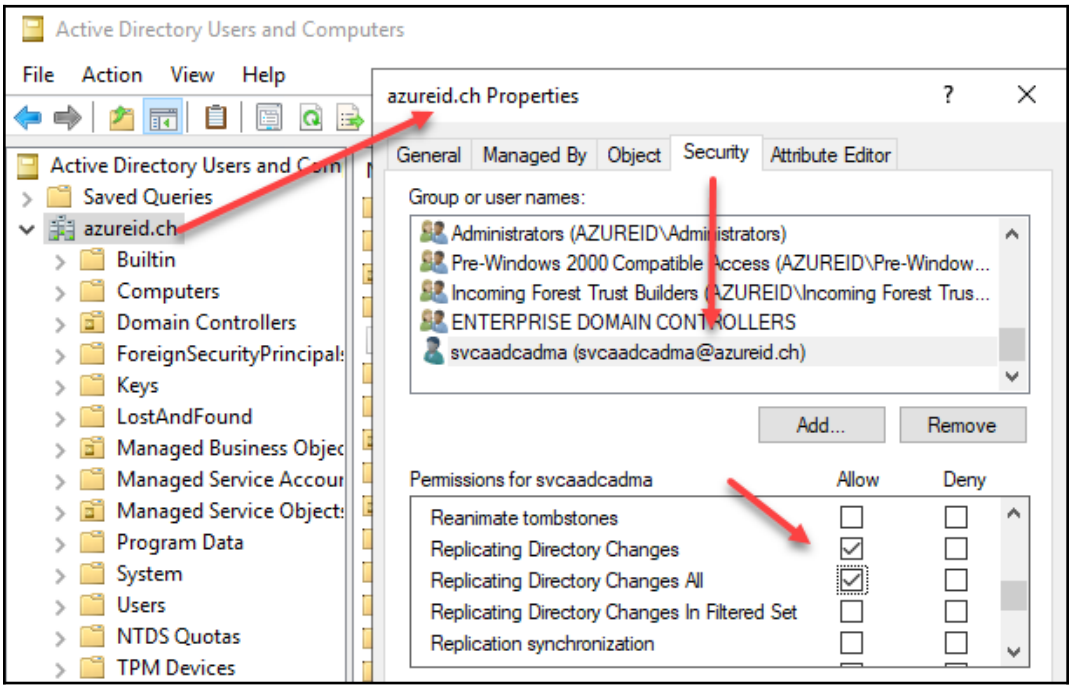

181031inovitdemos.on...
Windows Azure Active Directory (Micr...
Idle
inovitdemos.ch
Active Directory Domain Services
Idle
Search Connector Space
Scope:
Specify distinguished name (DN) for sub-tree:
Sub-Tree
Search
Search Results
Column Settings...
Total Retrieved: 274 matching records
DN
Object Type
Connector
Explicit
Properties...
Preview...
Validate object against schema...
Close
Help
Create
Properties
Delete
Configure Run Profiles
Run
Stop
Export Connector
Import Connector
Update Connector
Refresh Schema
Search Connector Space

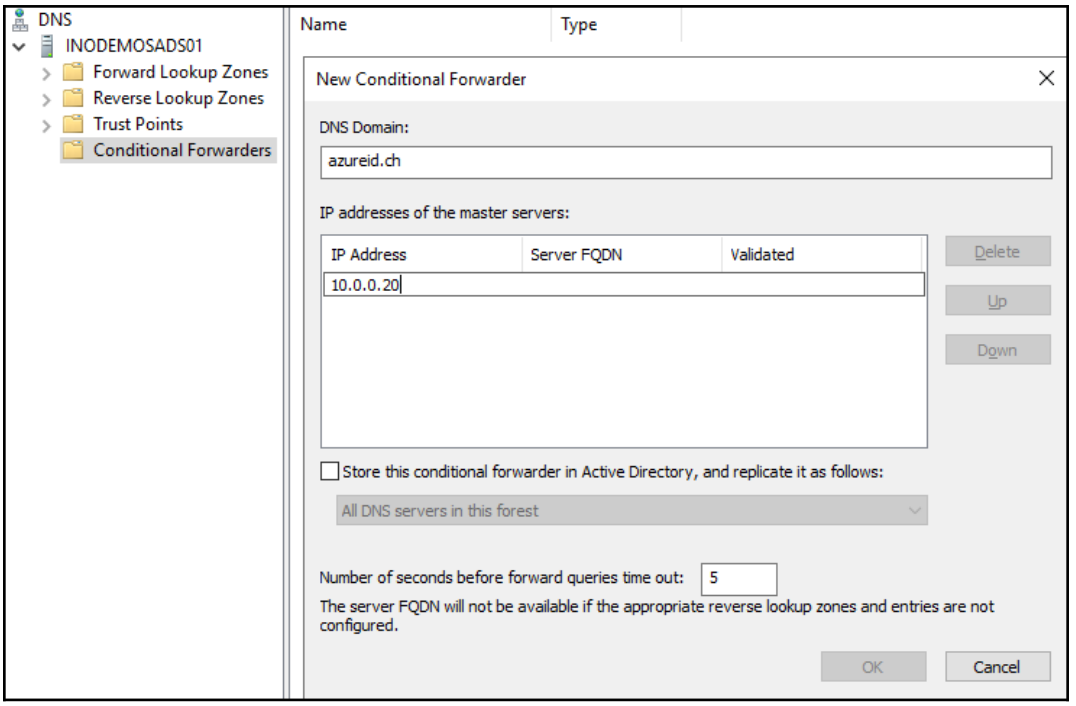

Edit inbound synchronization rule
Edit inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Add scoping filters, or click next to skip this step
Attribute
Operator
Value
isCriticalSystemObject
NOTEQUAL
True
adminDescription
NOTSTARTSWITH
Group_
Add clause
Remove clause(s)
Add group
Remove group(s)

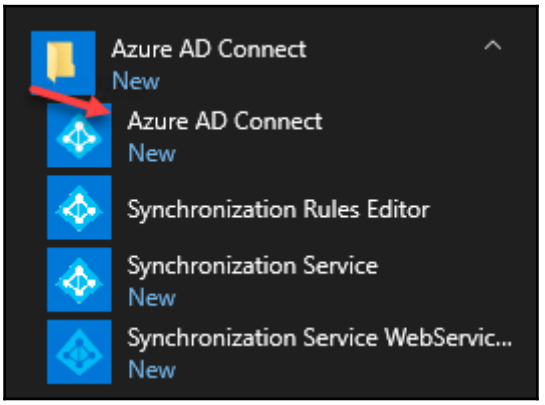

Create inbound synchronization rule
Create inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Name
In from AD - User Exclude Example
Description
Users that match this rule will not be synchronized to the Azure AD.
Connected System
inovitdemos.ch
Connected System Object Type
user
Metaverse Object Type
person
Link Type
Join
Precedence
50
Tag
Custom
Enable Password Sync
Disabled

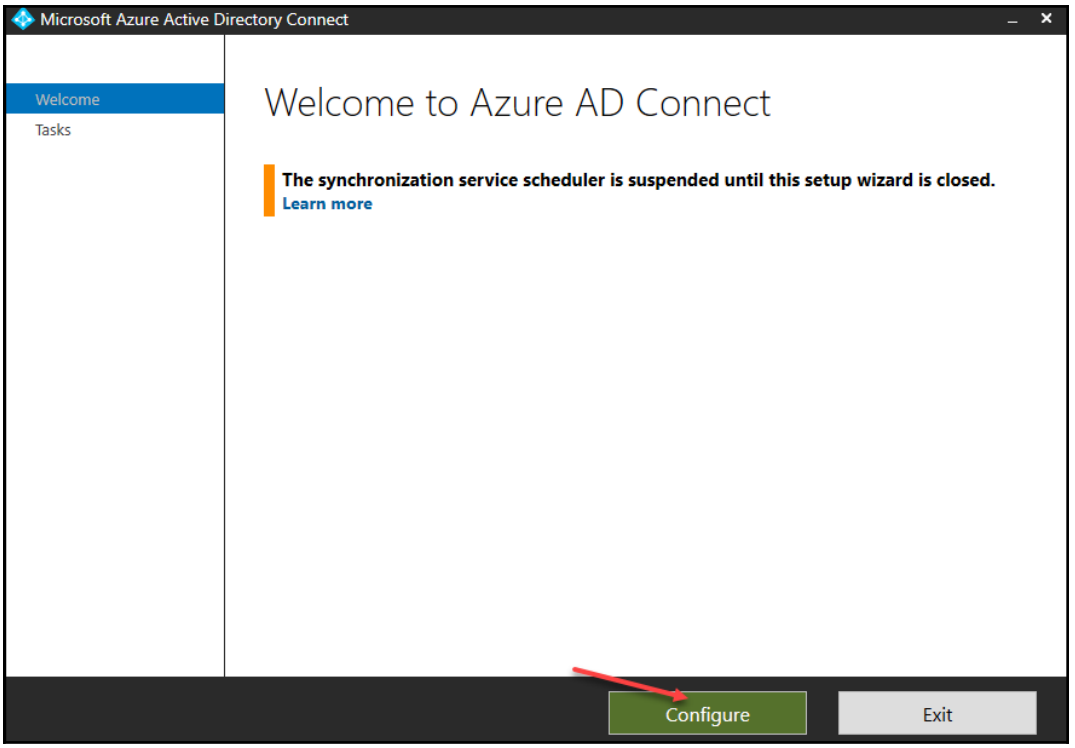

Edit inbound synchronization rule
Edit inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Add scoping filters, or click next to skip this step
Attribute
Operator
Value
department
EQUAL
Human Resources
Add clause
Remove clause(s)
Add group
Remove group(s)

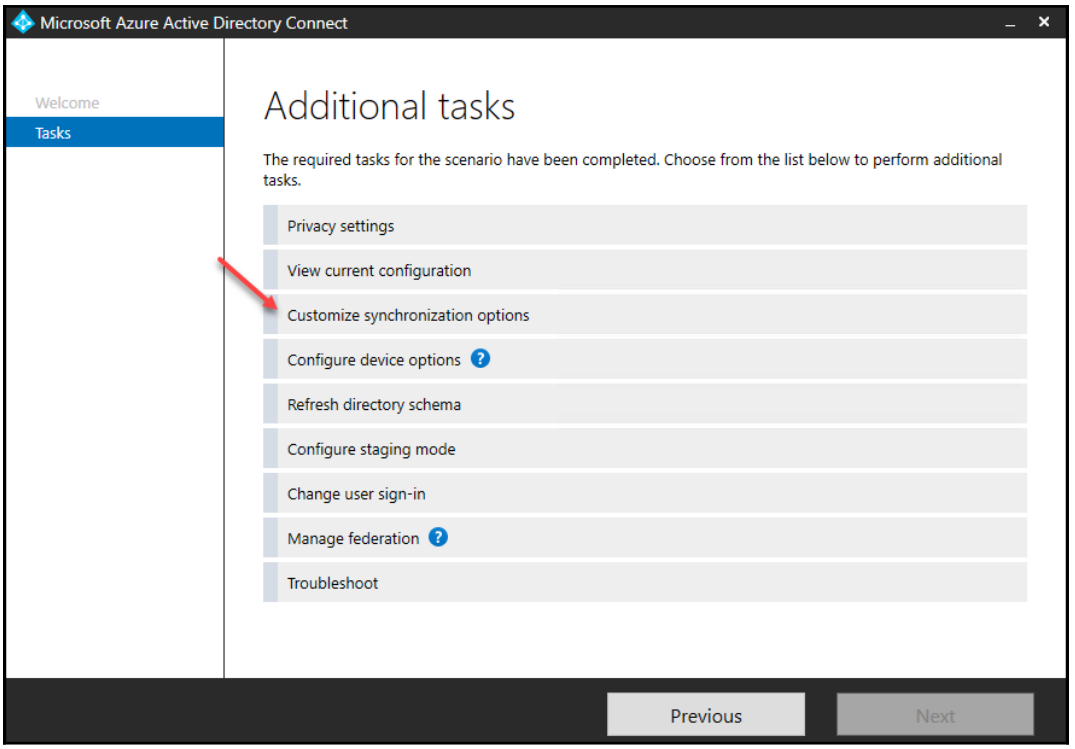

Create inbound synchronization rule
Description
Scoping filter
Join rules
Transformations
Add transformations
FlowType
Target Attribute
Source
Apply Or
Merge Type
Constant
cloudFiltered
True
Update
Add transformation
Remove

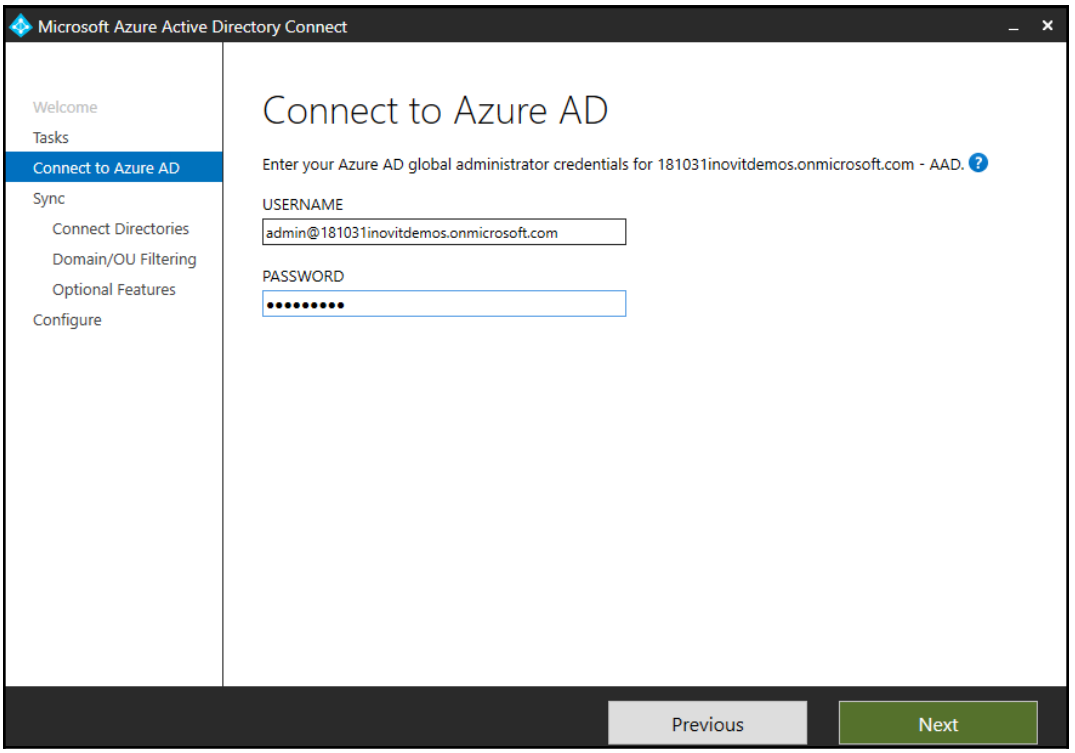

Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Com
Saved Queries
azureid.ch
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Business Objec
Managed Service Accour
Managed Service Objects
Program Data
System
Users
NTDS Quotas
TPM Devices
azureid.ch Properties
General
Managed By
Object
Security
Attribute Editor
Group or user names:
Administrators (AZUREID\Administrators)
Pre-Windows 2000 Compatible Access (AZUREID\Pre-Window...
Incoming Forest Trust Builders (AZUREID\Incoming Forest Trus...
ENTERPRISE DOMAIN CONTROLLERS
svcaadcadma (svcaadcadma@azureid.ch)
Add...
Remove
Permissions for svcaadcadma
Allow
Deny
Reanimate tombstones
Replicating Directory Changes
Replicating Directory Changes All
Replicating Directory Changes In Filtered Set
Replication synchronization

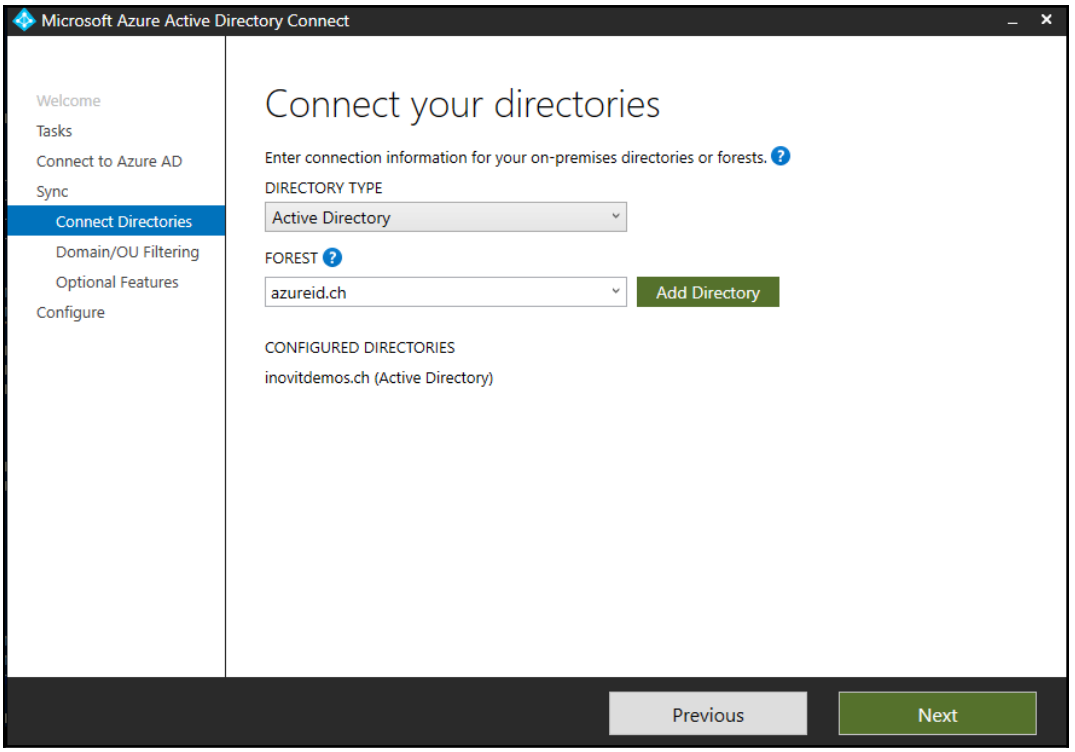

DNS
INODEMOSADS01
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
Name
Type
New Conditional Forwarder
DNS Domain:
azureid.ch
IP addresses of the master servers:
IP Address
Server FQDN
Validated
10.0.0.20
Delete
Up
Down
Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this forest
Number of seconds before forward queries time out:
5
The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.
OK
Cancel

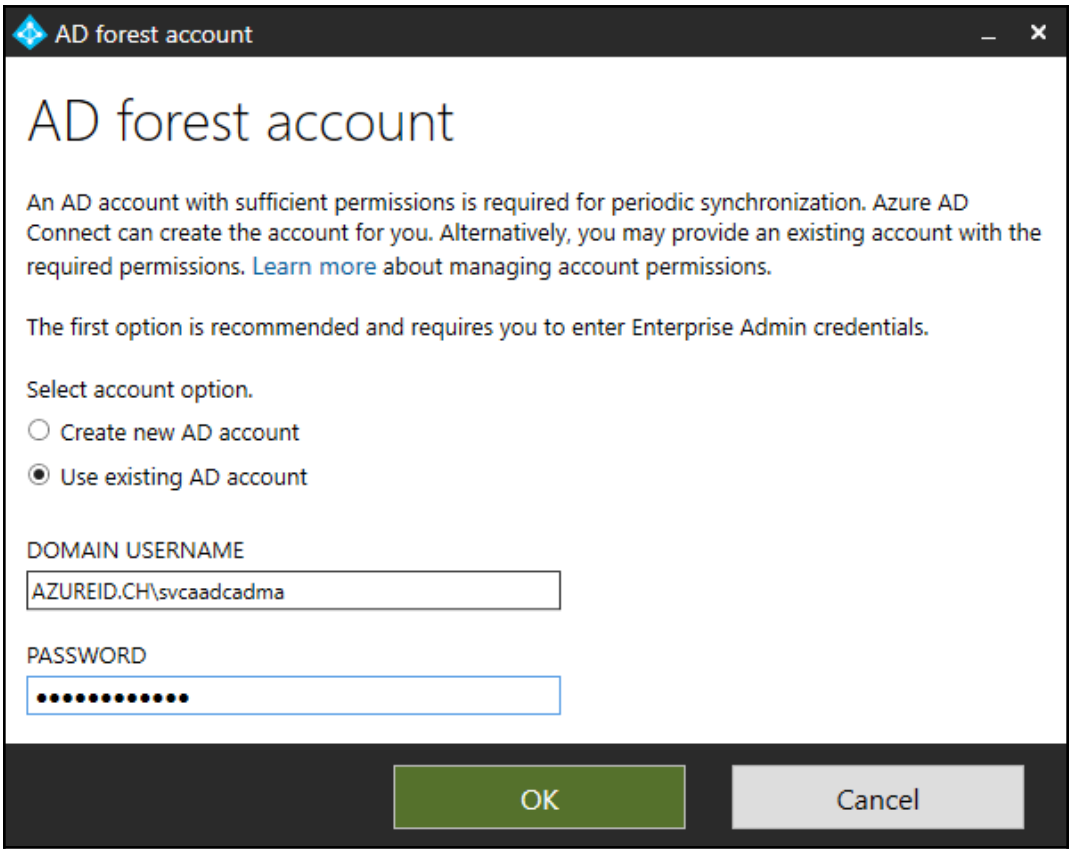

Azure AD Connect
New
Azure AD Connect
New
Synchronization Rules Editor
Synchronization Service
New
Synchronization Service WebServic...
New


Microsoft Azure Active Directory Connect
Welcome
Tasks
Welcome to Azure AD Connect
The synchronization service scheduler is suspended until this setup wizard is closed.
Learn more
Configure
Exit

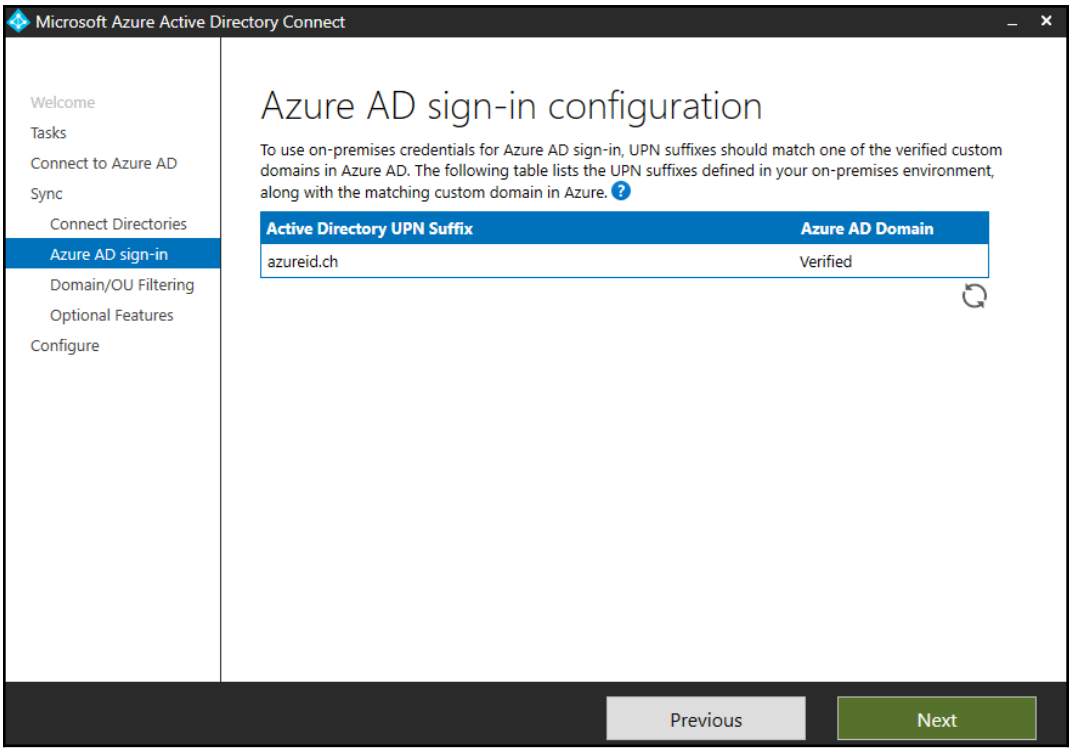

Microsoft Azure Active Directory Connect
Welcome
Tasks
Additional tasks
The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.
Privacy settings
View current configuration
Customize synchronization options
Configure device options
Refresh directory schema
Configure staging mode
Change user sign-in
Manage federation
Troubleshoot
Previous
Next

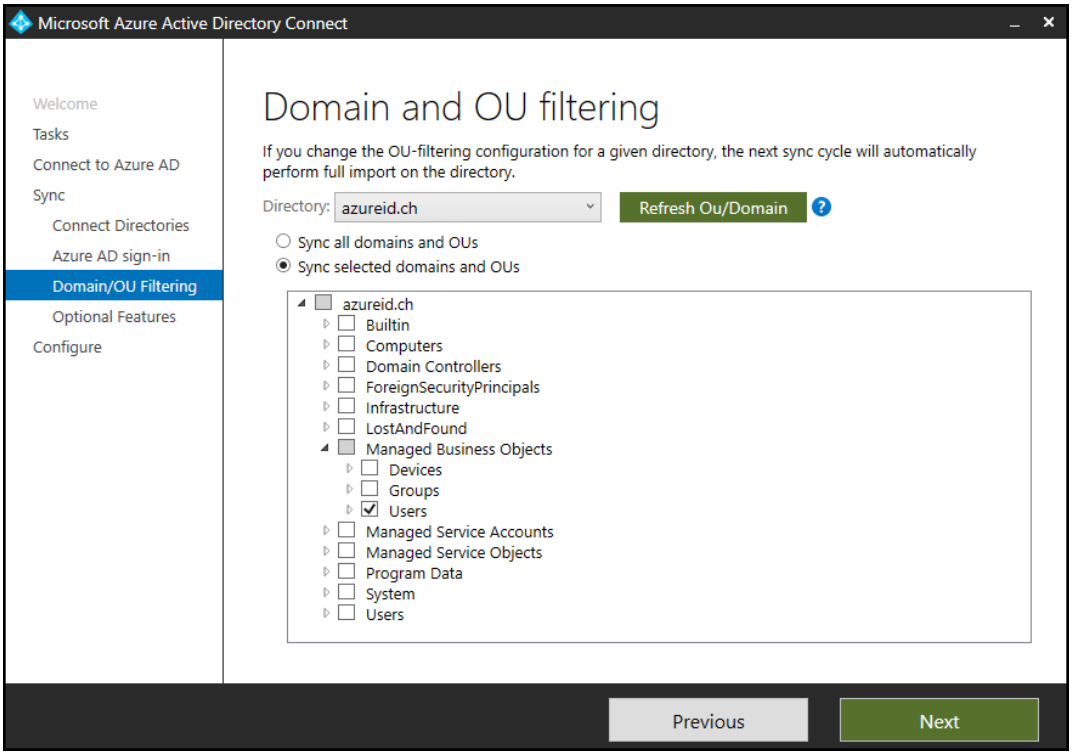

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Domain/OU Filtering
Optional Features
Configure
Connect to Azure AD
Enter your Azure AD global administrator credentials for 181031inovitdemos.onmicrosoft.com - AAD.
USERNAME
admin@181031inovitdemos.onmicrosoft.com
PASSWORD
Previous
Next

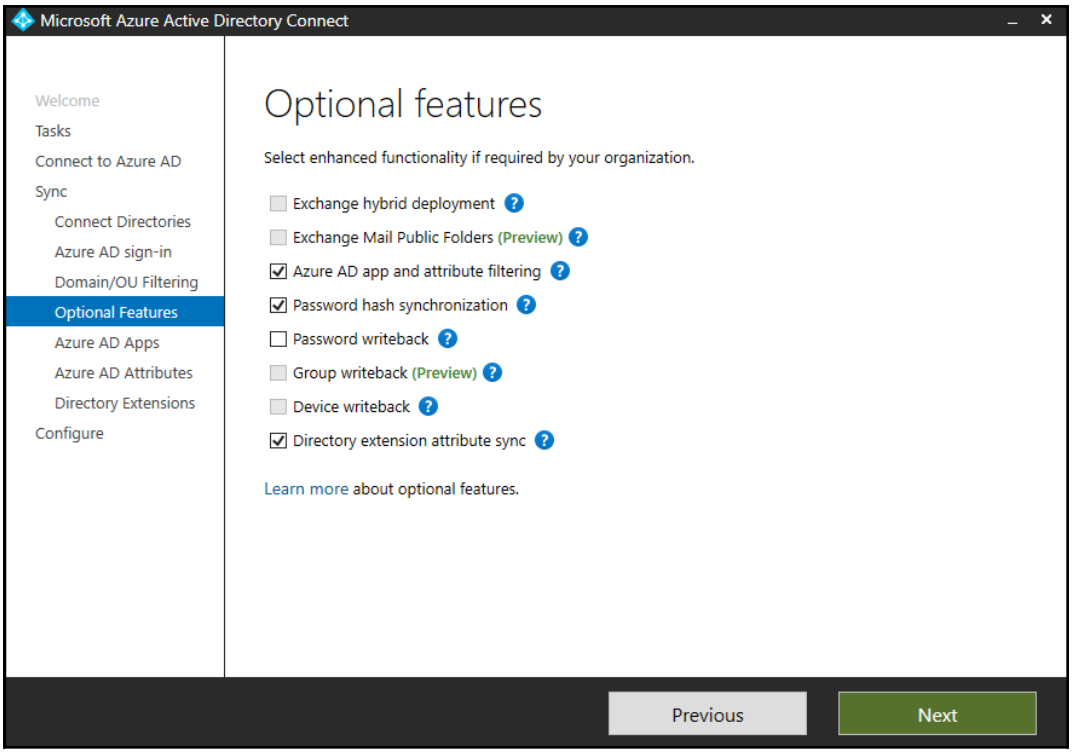

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Domain/OU Filtering
Optional Features
Configure
Connect your directories
Enter connection information for your on-premises directories or forests.
DIRECTORY TYPE
Active Directory
FOREST
azureid.ch
Add Directory
CONFIGURED DIRECTORIES
inovitdemos.ch (Active Directory)
Previous
Next

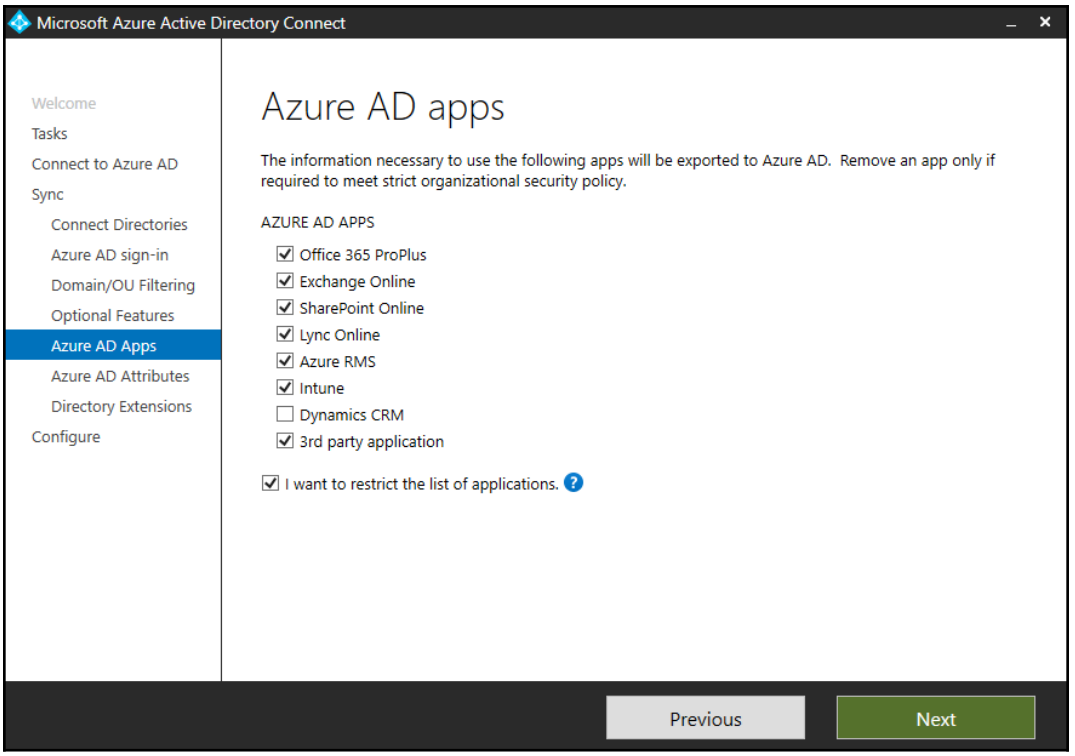

AD forest account
AD forest account
An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. Learn more about managing account permissions.
The first option is recommended and requires you to enter Enterprise Admin credentials.
Select account option.
Create new AD account
Use existing AD account
DOMAIN USERNAME
AZUREID.CH\svcaadcadma
PASSWORD
OK
Cancel

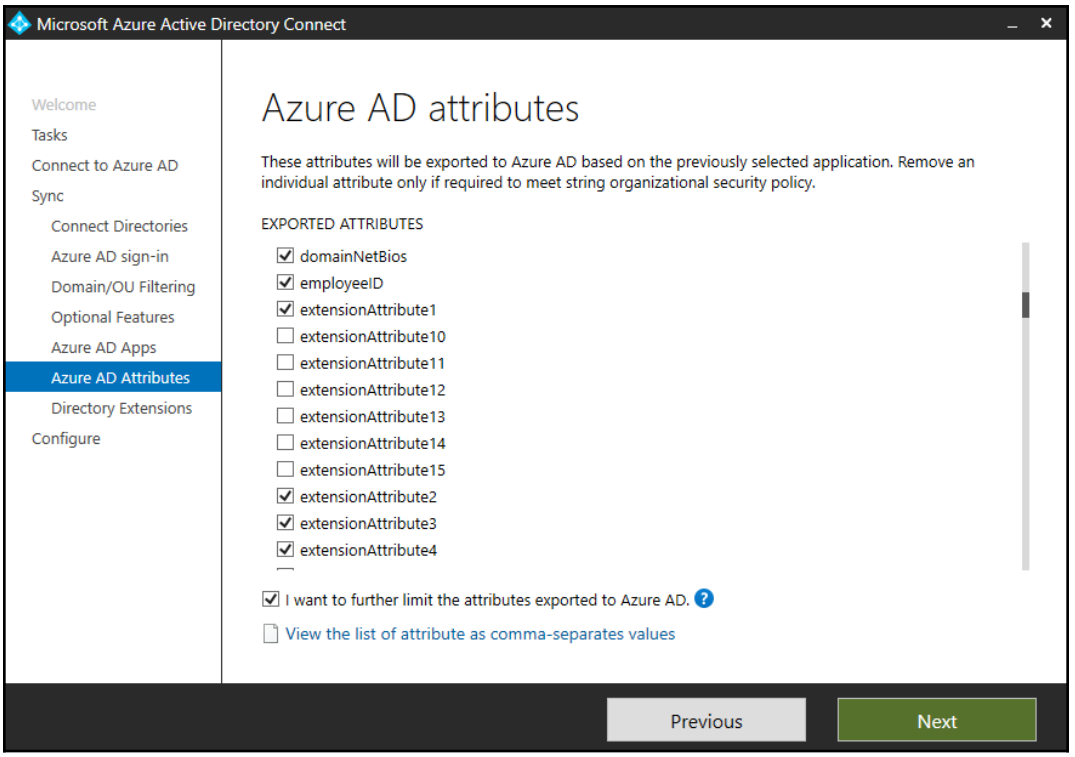

CONFIGURED DIRECTORIES
inovitdemos.ch (Active Directory)
azureid.ch (Active Directory)

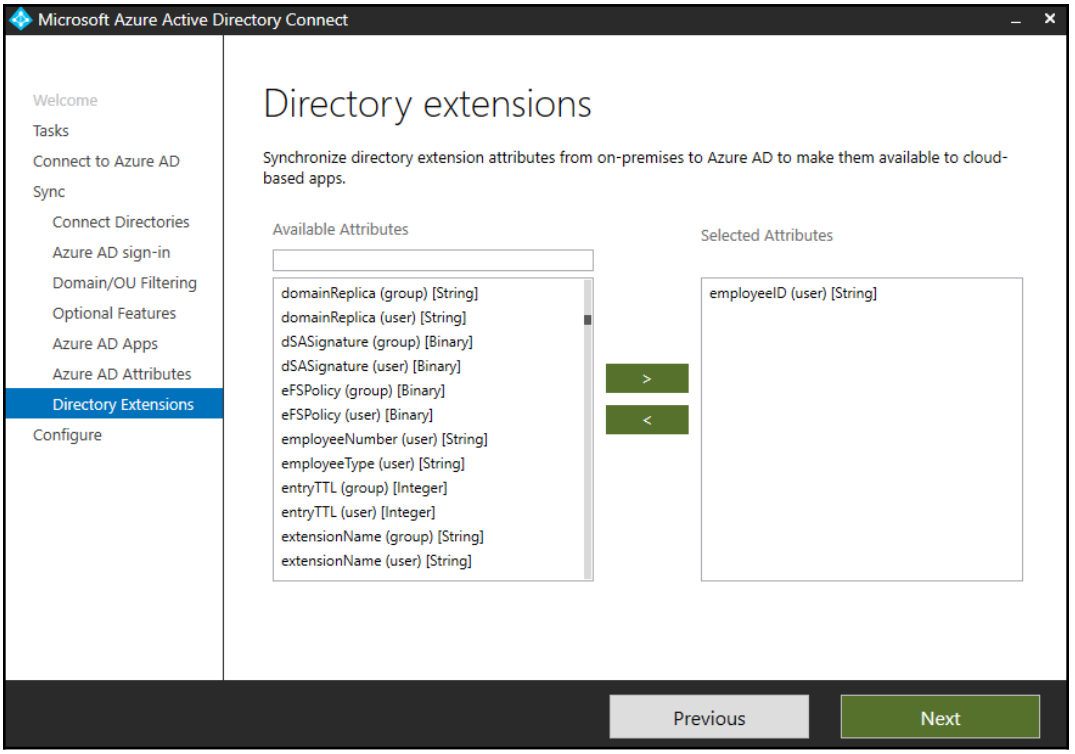

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Optional Features
Configure
Azure AD sign-in configuration
To use on-premises credentials for Azure AD sign-in, UPN suffixes should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure.
Active Directory UPN Suffix
Azure AD Domain
azureid.ch
Verified
Previous
Next

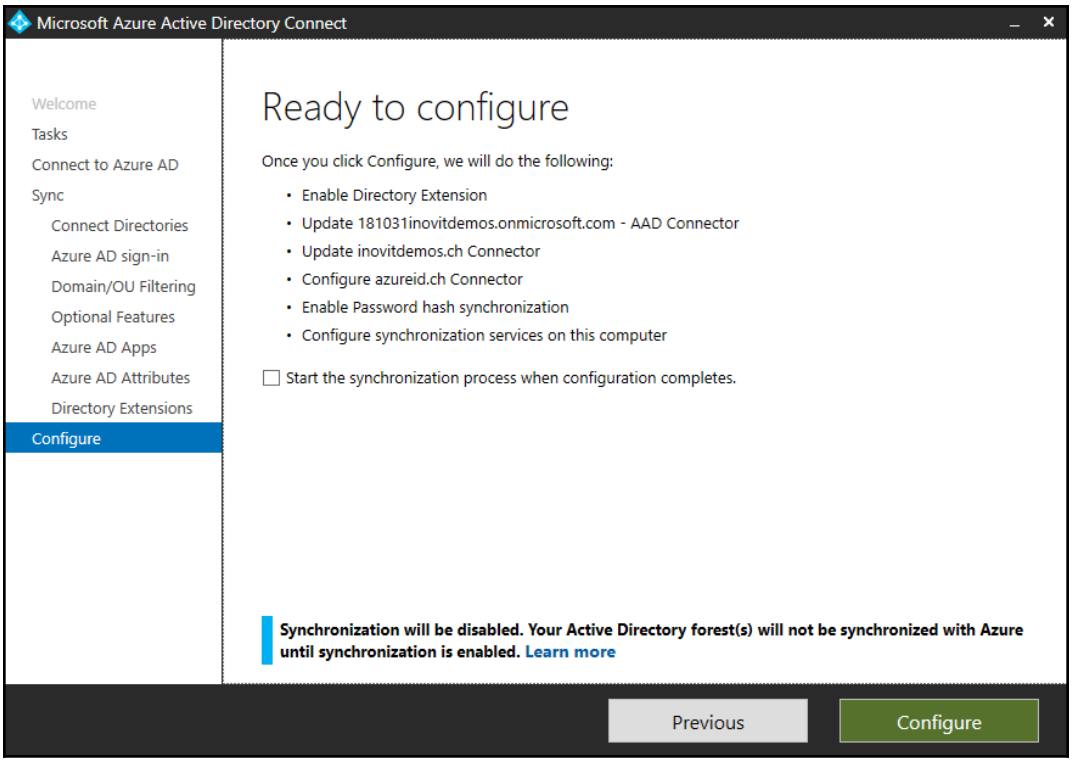

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Optional Features
Configure
Domain and OU filtering
If you change the OU-filtering configuration for a given directory, the next sync cycle will automatically perform full import on the directory.
Directory: azureid.ch
Refresh Ou/Domain
Sync all domains and OUs
Sync selected domains and OUs
azureid.ch
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Infrastructure
LostAndFound
Managed Business Objects
Devices
Groups
Users
Managed Service Accounts
Managed Service Objects
Program Data
System
Users
Previous
Next

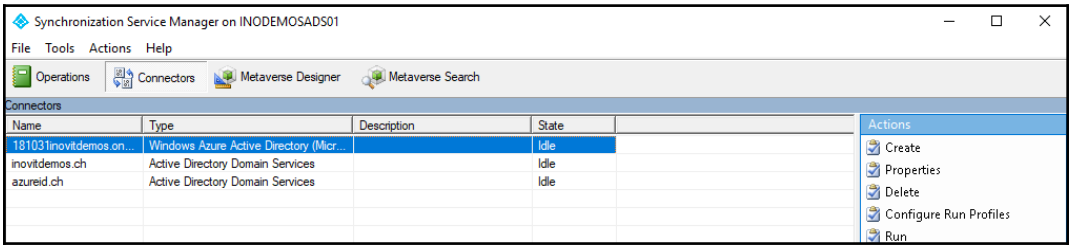

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Optional Features
Azure AD Apps
Azure AD Attributes
Directory Extensions
Configure
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Exchange Mail Public Folders (Preview)
Azure AD app and attribute filtering
Password hash synchronization
Password writeback
Group writeback (Preview)
Device writeback
Directory extension attribute sync
Learn more about optional features.
Previous
Next


Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Optional Features
Azure AD Apps
Azure AD Attributes
Directory Extensions
Configure
Azure AD apps
The information necessary to use the following apps will be exported to Azure AD. Remove an app only if required to meet strict organizational security policy.
AZURE AD APPS
Office 365 ProPlus
Exchange Online
SharePoint Online
Lync Online
Azure RMS
Intune
Dynamics CRM
3rd party application
I want to restrict the list of applications.
Previous
Next

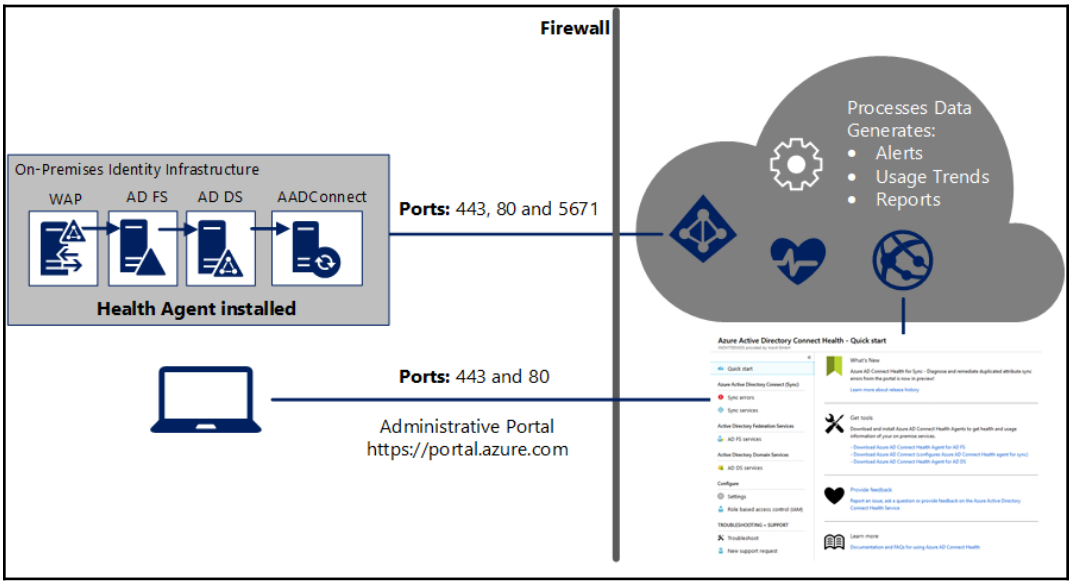

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Optional Features
Azure AD Apps
Azure AD Attributes
Directory Extensions
Configure
Azure AD attributes
These attributes will be exported to Azure AD based on the previously selected application. Remove an individual attribute only if required to meet string organizational security policy.
EXPORTED ATTRIBUTES
domainNetBios
employeeID
extensionAttribute1
extensionAttribute10
extensionAttribute11
extensionAttribute12
extensionAttribute13
extensionAttribute14
extensionAttribute15
extensionAttribute2
extensionAttribute3
extensionAttribute4
I want to further limit the attributes exported to Azure AD.
View the list of attribute as comma-separates values
Previous
Next

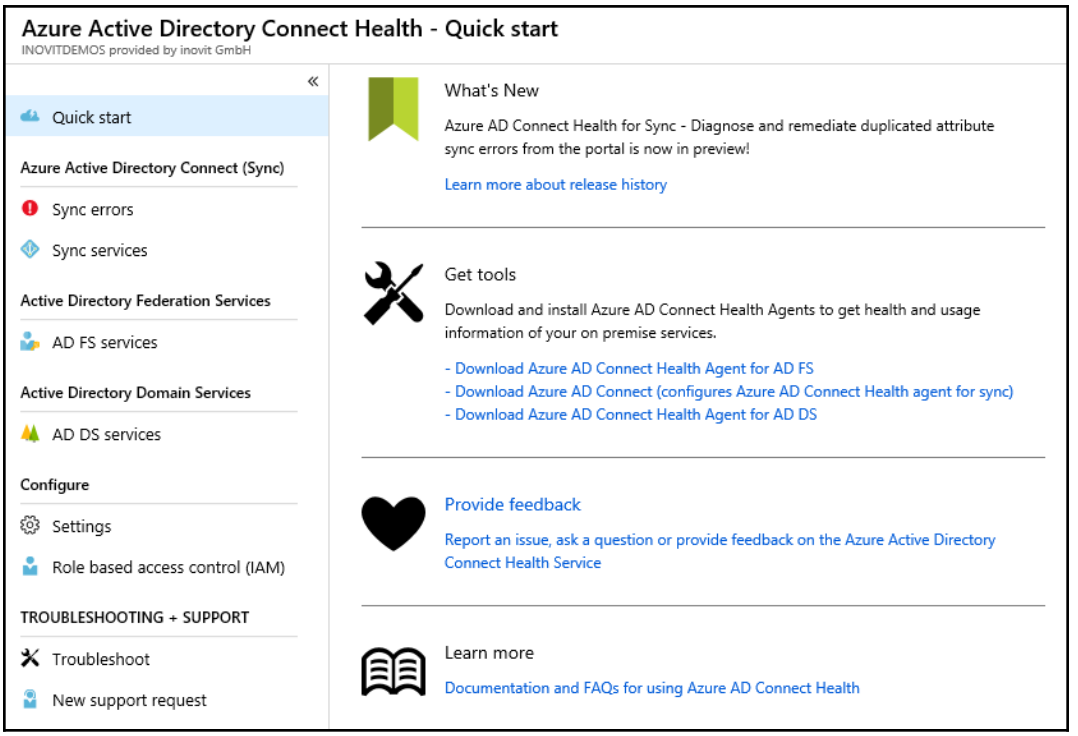

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Optional Features
Azure AD Apps
Azure AD Attributes
Directory Extensions
Configure
Directory extensions
Synchronize directory extension attributes from on-premises to Azure AD to make them available to cloud-based apps.
Available Attributes
domainReplica (group) [String]
domainReplica (user) [String]
dSASignature (group) [Binary]
dSASignature (user) [Binary]
eFSPolicy (group) [Binary]
eFSPolicy (user) [Binary]
employeeNumber (user) [String]
employeeType (user) [String]
entryTTL (group) [Integer]
entryTTL (user) [Integer]
extensionName (group) [String]
extensionName (user) [String]
>
<
Selected Attributes
employeeID (user) [String]
Previous
Next

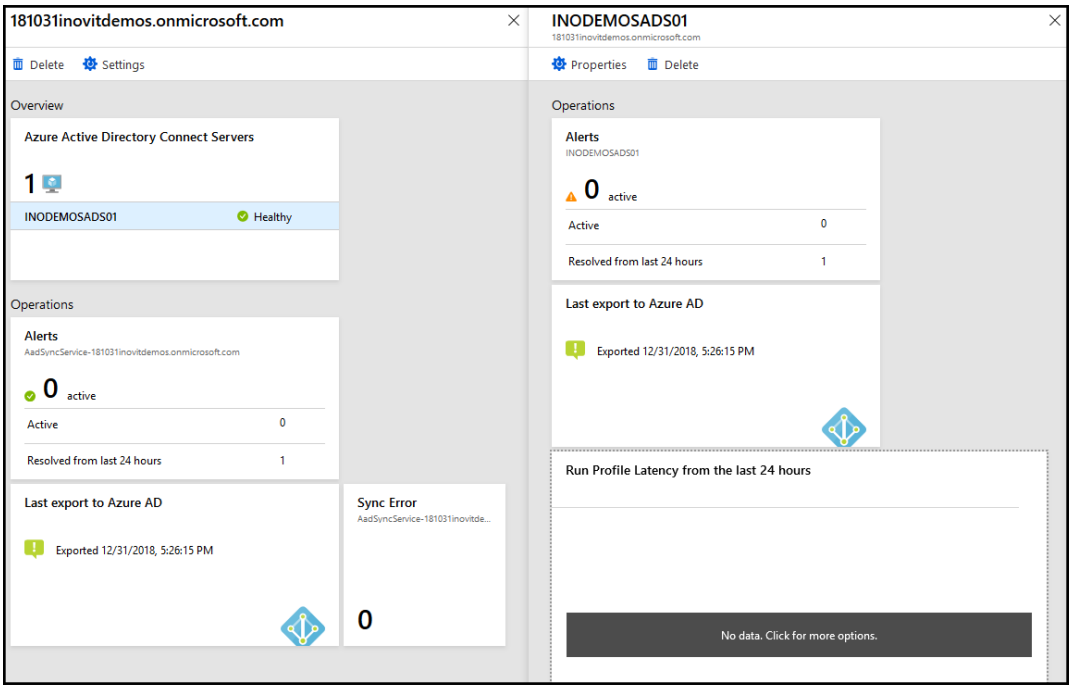

Microsoft Azure Active Directory Connect
Welcome
Tasks
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Optional Features
Azure AD Apps
Azure AD Attributes
Directory Extensions
Configure
Ready to configure
Once you click Configure, we will do the following:
Enable Directory Extension
Update 181031inovitdemos.onmicrosoft.com - AAD Connector
Update inovitdemos.ch Connector
Configure azureid.ch Connector
Enable Password hash synchronization
Configure synchronization services on this computer
Start the synchronization process when configuration completes.
Synchronization will be disabled. Your Active Directory forest(s) will not be synchronized with Azure until synchronization is enabled. Learn more
Previous
Configure

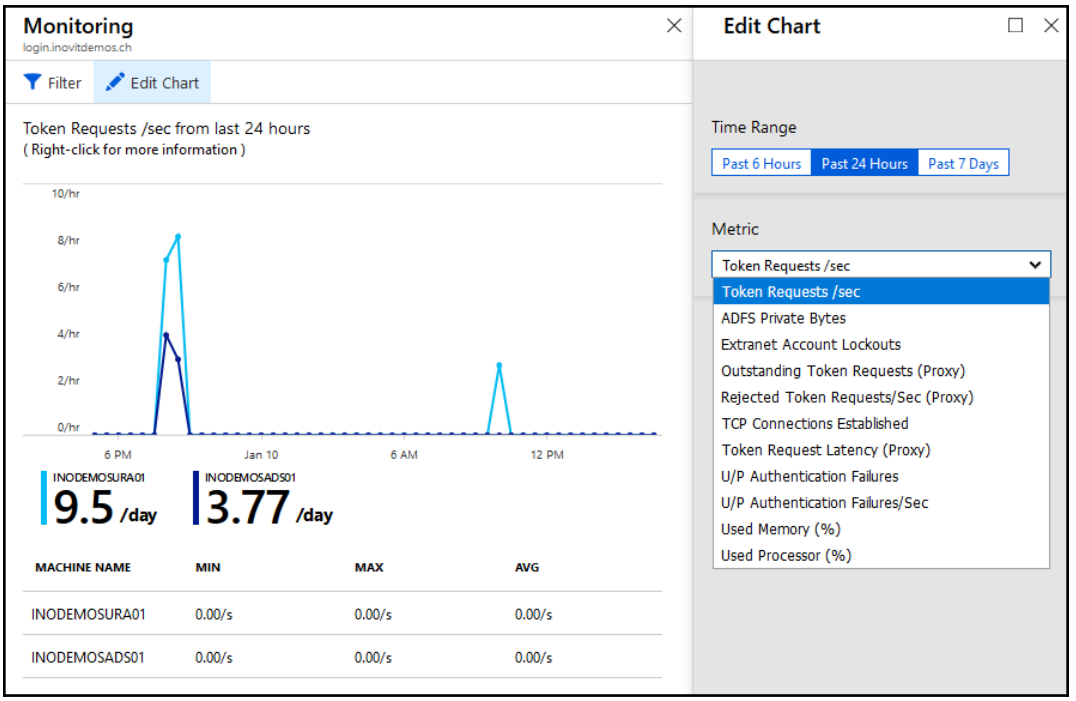

Synchronization Service Manager on INODEMOSADS01
File Tools Actions Help
Operations
Connectors
Metaverse Designer
Metaverse Search
Connectors
Name
Type
Description
State
181031inovitdemos.on...
Windows Azure Active Directory (Micr...
Idle
inovitdemos.ch
Active Directory Domain Services
Idle
azureid.ch
Active Directory Domain Services
Idle
Actions
Create
Properties
Delete
Configure Run Profiles
Run

Chapter 4: Monitoring Your Identity Bridge

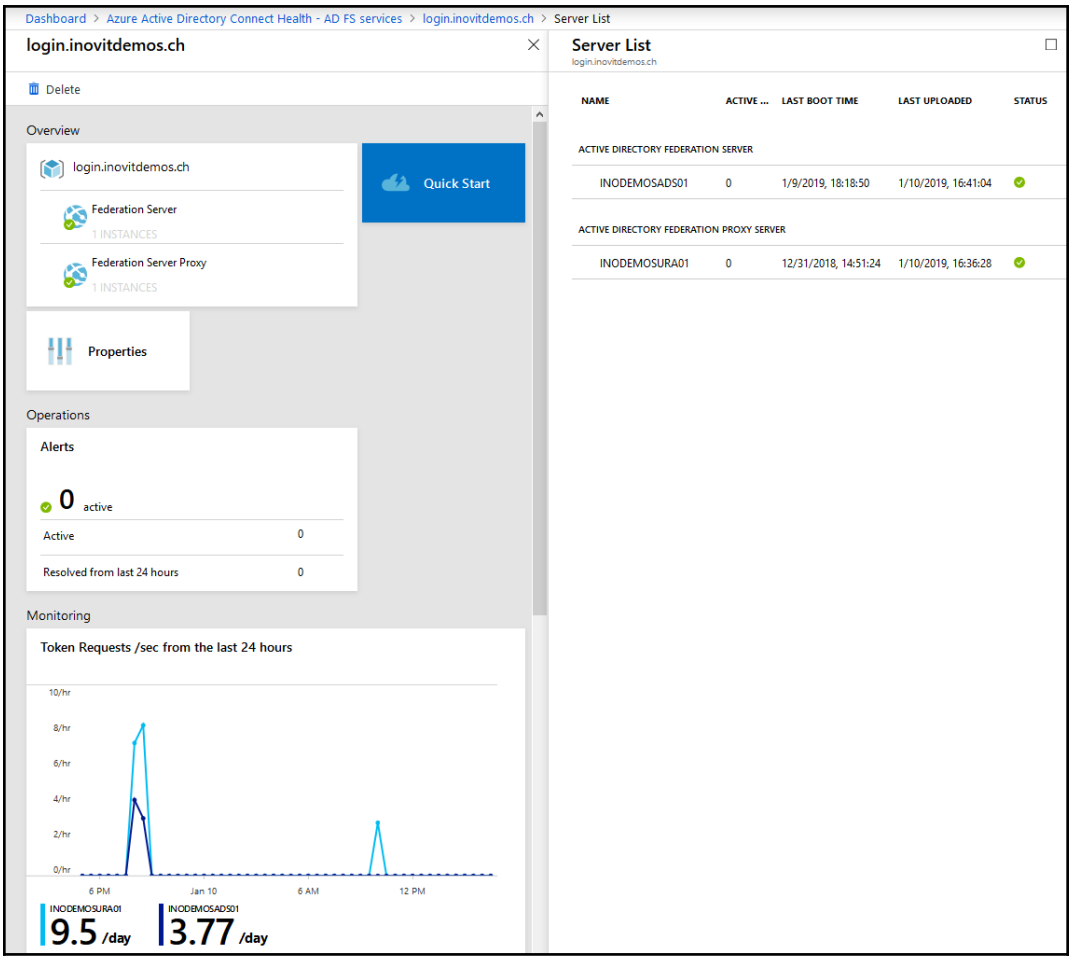


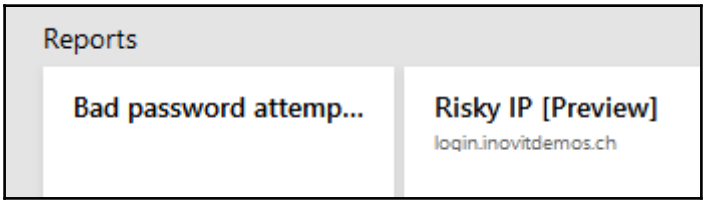

Azure Active Directory Connect Health - Quick start
INOVITDEMOS provided by inovit GmbH
Quick start
Azure Active Directory Connect (Sync)
Sync errors
Sync services
Active Directory Federation Services
AD FS services
Active Directory Domain Services
AD DS services
Configure
Settings
Role based access control (IAM)
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request
What's New
Azure AD Connect Health for Sync - Diagnose and remediate duplicated attribute sync errors from the portal is now in preview!
Learn more about release history
Get tools
Download and install Azure AD Connect Health Agents to get health and usage information of your on premise services.
- Download Azure AD Connect Health Agent for AD FS
- Download Azure AD Connect (configures Azure AD Connect Health agent for sync)
- Download Azure AD Connect Health Agent for AD DS
Provide feedback
Report an issue, ask a question or provide feedback on the Azure Active Directory Connect Health Service
Learn more
Documentation and FAQs for using Azure AD Connect Health


181031inovitdemos.onmicrosoft.com
Delete
Settings
Overview
Azure Active Directory Connect Servers
1
INODEMOSADS01
Healthy
Operations
Alerts
AadSyncService-181031inovitdemos.onmicrosoft.com
0
active
Active
0
Resolved from last 24 hours
1
Last export to Azure AD
Exported 12/31/2018, 5:26:15 PM
Sync Error
AadSyncService-181031inovitde...
0
INODEMOSADS01
181031inovitdemos.onmicrosoft.com
Properties
Delete
Operations
Alerts
INODEMOSADS01
0
active
Active
0
Resolved from last 24 hours
1
Last export to Azure AD
Exported 12/31/2018, 5:26:15 PM
Run Profile Latency from the last 24 hours
No data. Click for more options.

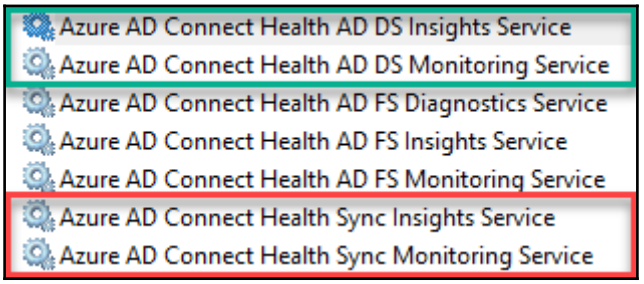

Monitoring
login.inovitdemos.ch
Filter
Edit Chart
Token Requests /sec from last 24 hours
(Right-click for more information)
10/hr
8/hr
6/hr
4/hr
2/hr
0/hr
6 PM
Jan 10
6 AM
12 PM
INODEMOSURA01
9.5 /day
INODEMOSADS01
3.77 /day
MACHINE NAME
MIN
MAX
AVG
INODEMOSURA01
0.00/s
0.00/s
0.00/s
INODEMOSADS01
0.00/s
0.00/s
0.00/s
Edit Chart
Time Range
Past 6 Hours
Past 24 Hours
Past 7 Days
Metric
Token Requests /sec
Token Requests /sec
ADFS Private Bytes
Extranet Account Lockouts
Outstanding Token Requests (Proxy)
Rejected Token Requests/Sec (Proxy)
TCP Connections Established
Token Request Latency (Proxy)
U/P Authentication Failures
U/P Authentication Failures/Sec
Used Memory (%)
Used Processor (%)

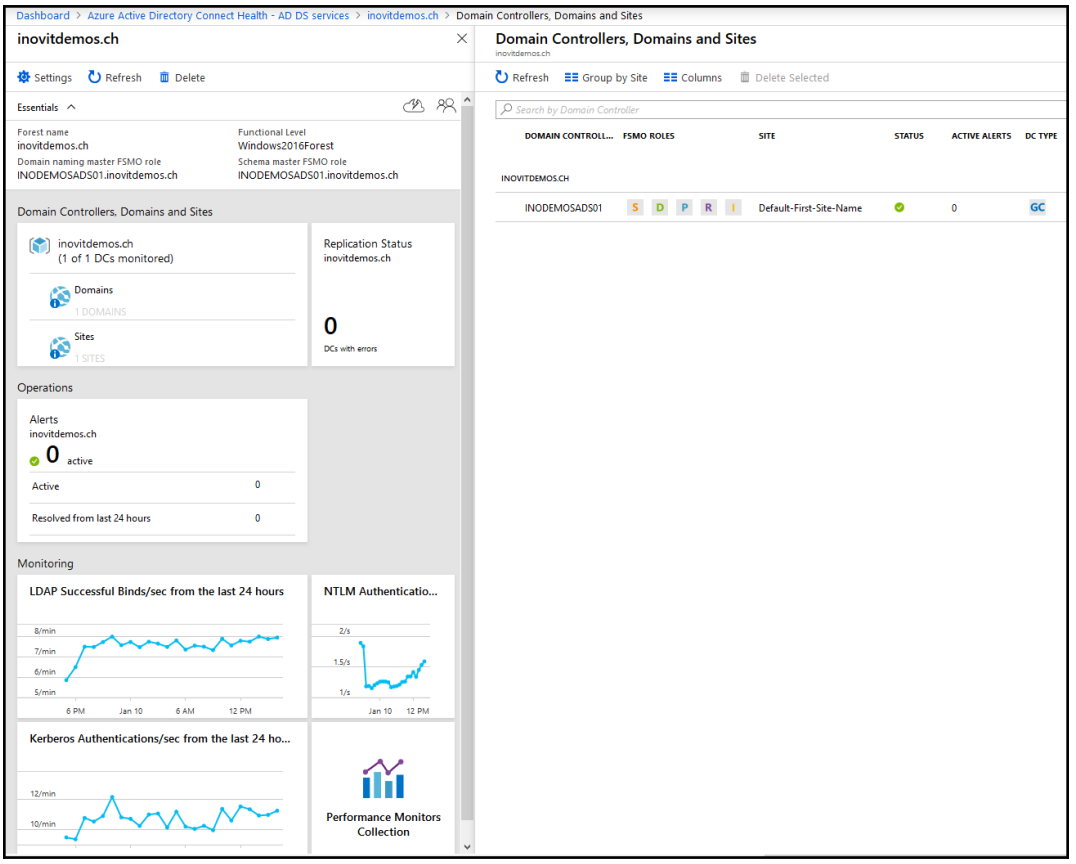

Azure AD Connect Health AD FS Agent Setup
Azure AD Connect Health AD FS Agent
Microsoft Azure AD Connect Health Agent is designed for use solely in conjunction with Azure Active Directory. This agent will collect and transmit configuration, event log and login data to Microsoft Azure Active Directory for the purposes of monitoring and providing you with additional insights into operational activity (including logins).
Microsoft Azure Subscription Agreement.
Version 3.1.24.0
Install
Close


Dashboard > Azure Active Directory Connect Health - AD FS services > login.inovitdemos.ch > Server List
login.inovitdemos.ch
Delete
Overview
login.inovitdemos.ch
Federation Server
1 INSTANCES
Federation Server Proxy
1 INSTANCES
Quick Start
Properties
Operations
Alerts
0 active
Active 0
Resolved from last 24 hours 0
Monitoring
Token Requests /sec from the last 24 hours
10/hr
8/hr
6/hr
4/hr
2/hr
0/hr
6 PM
Jan 10
6 AM
12 PM
INODEMOSURA01
9.5 /day
INODEMOSADS01
3.77 /day
Server List
login.inovitdemos.ch
NAME
ACTIVE ...
LAST BOOT TIME
LAST UPLOADED
STATUS
ACTIVE DIRECTORY FEDERATION SERVER
INODEMOSADS01 0 1/9/2019, 18:18:50 1/10/2019, 16:41:04
ACTIVE DIRECTORY FEDERATION PROXY SERVER
INODEMOSURA01 0 12/31/2018, 14:51:24 1/10/2019, 16:36:28

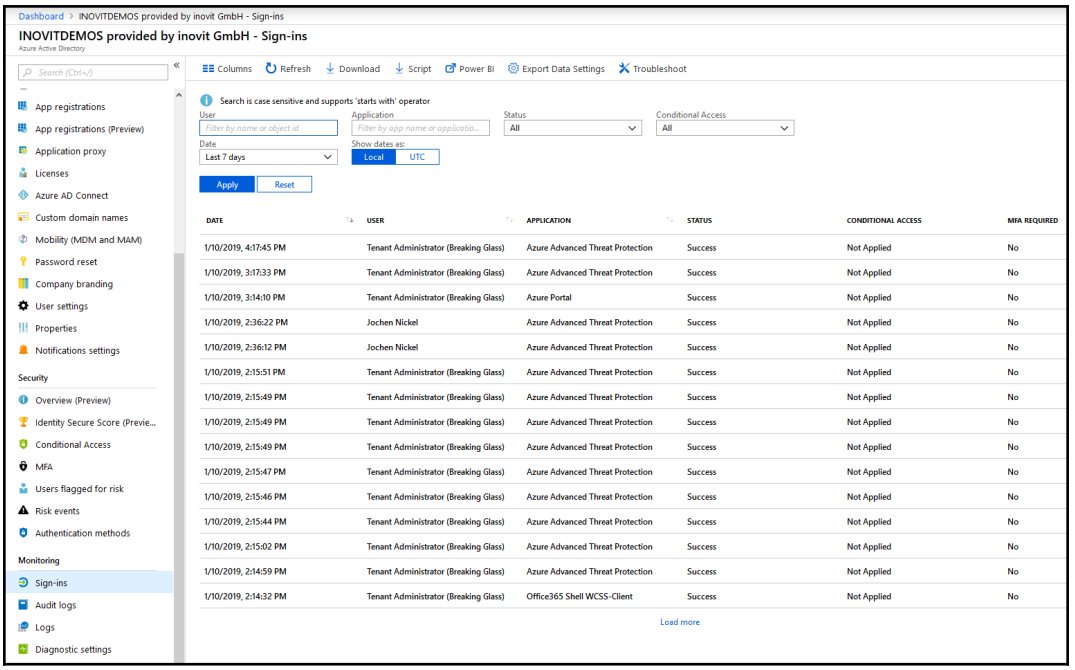

Reports
Bad password attemp...
Risky IP [Preview]
login.inovitdemos.ch

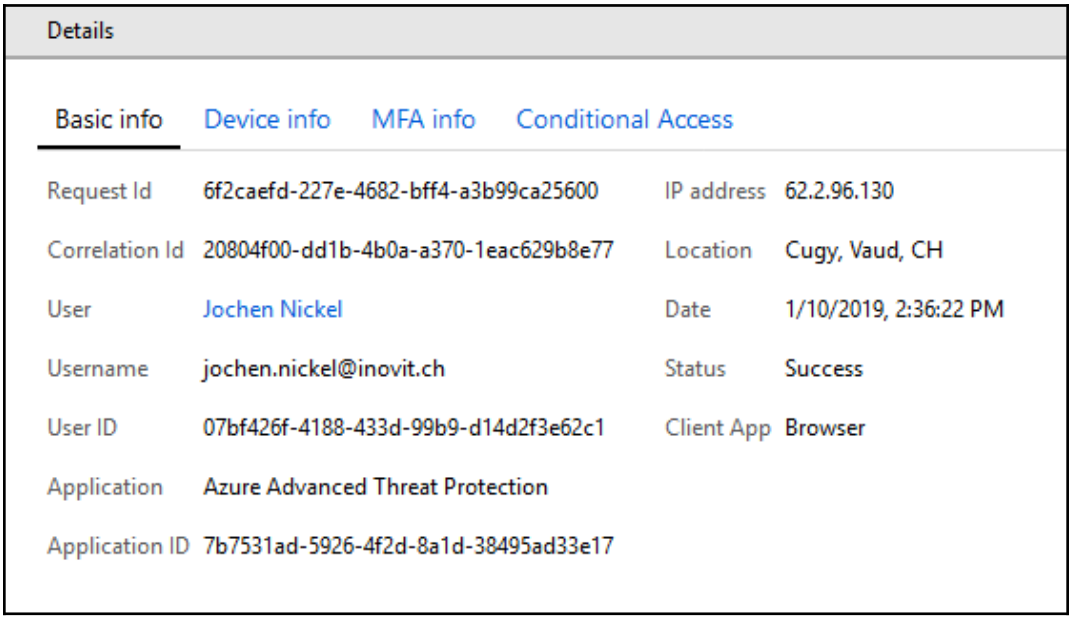

Microsoft Azure AD Connect Health agent for AD DS Setup
Microsoft Azure AD Connect Health agent for AD DS
Microsoft Azure AD Connect Health Agent is designed for use solely in conjunction with Azure Active Directory. This agent will collect and transmit configuration, event log and login data to Microsoft Azure Active Directory for the purposes of monitoring and providing you with additional insights into operational activity (including logins).
Before installing, please ensure all application pre-requisites are met:
• PowerShell 4.0
• Outbound connectivity to Azure service endpoints*
• Open firewall ports: TCP/IP port 443 and 5671
• Allow necessary websites* if IE Enhanced Security Configuration is enabled
*For a complete list, please see: aka.ms/aadchprereqs
Microsoft Azure Subscription Agreement.
Version 3.1.24.0
Install
Close

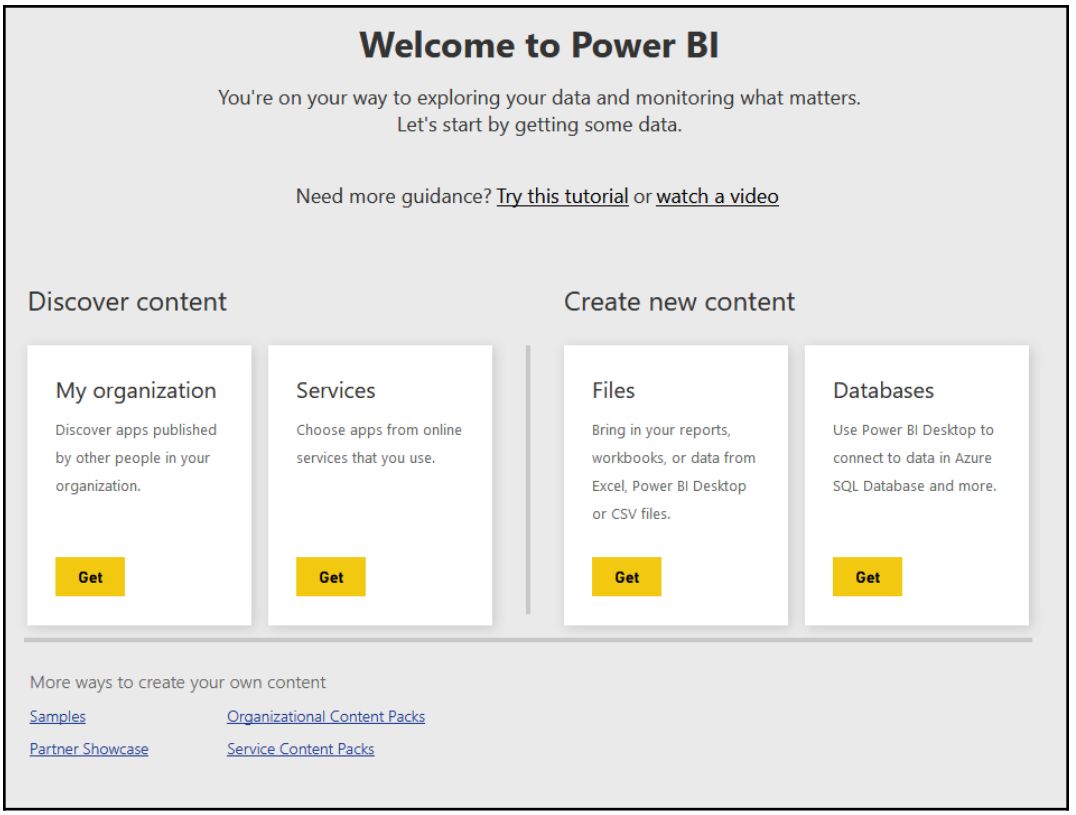

Azure AD Connect Health AD DS Insights Service
Azure AD Connect Health AD DS Monitoring Service
Azure AD Connect Health AD FS Diagnostics Service
Azure AD Connect Health AD FS Insights Service
Azure AD Connect Health AD FS Monitoring Service
Azure AD Connect Health Sync Insights Service
Azure AD Connect Health Sync Monitoring Service

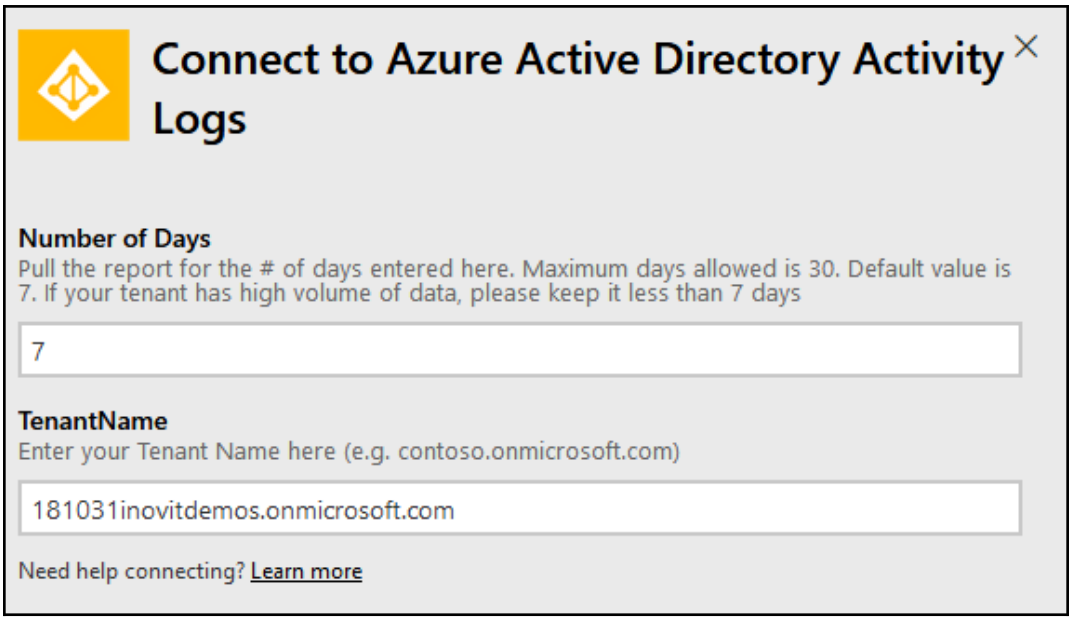


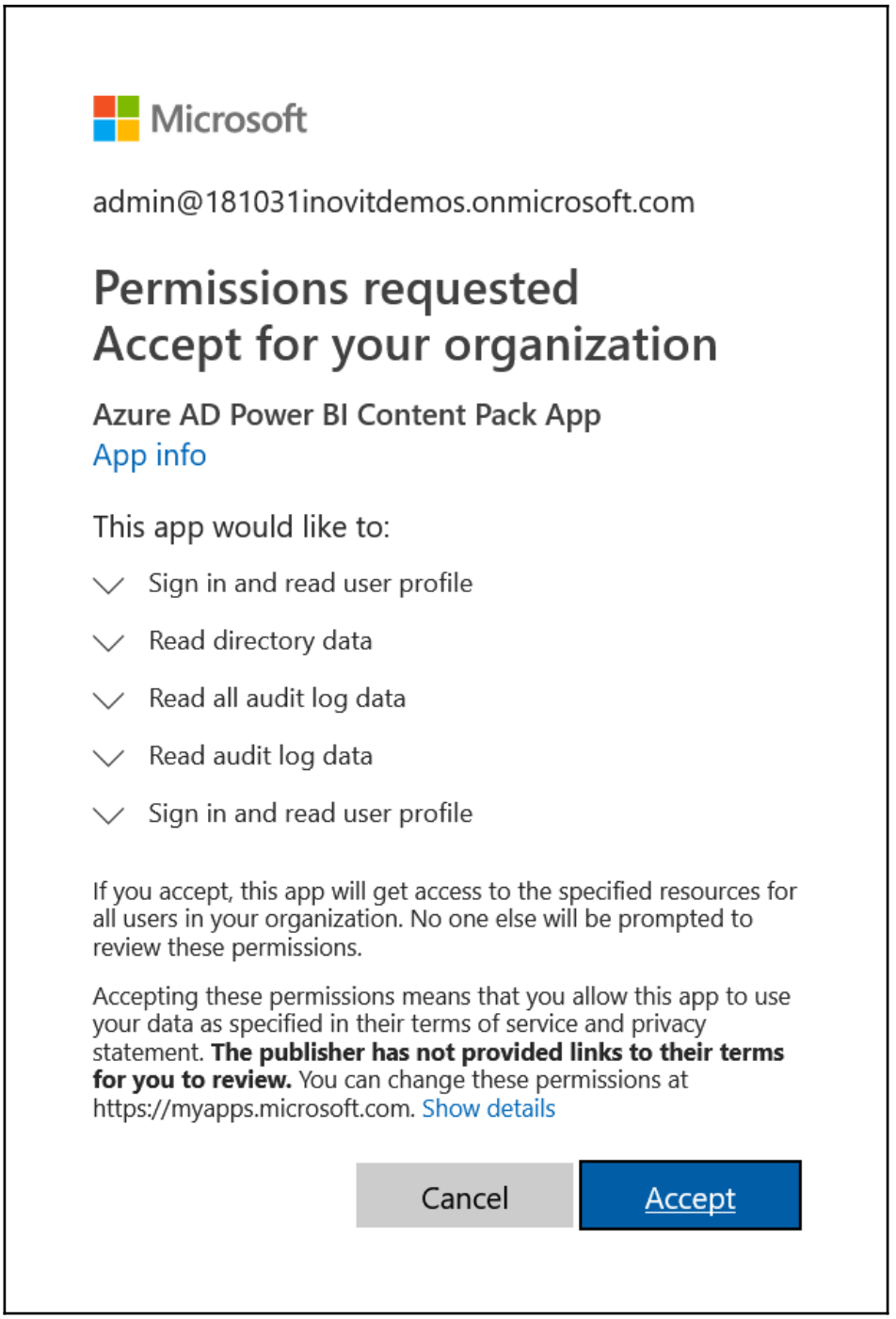

```
PS C:\Users\cloudadmin> Test-AzureADConnectHealthConnectivity -Role ADFS
Test-AzureADConnectHealthConnectivity's execution in details are as follows:
Starting Test-AzureADConnectHealthConnectivity ...

Connectivity Test Step 1 of 3: Testing dependent service endpoints begins ...
AAD CDN connectivity is skipped.
Connecting to endpoint https://login.microsoftonline.com
Endpoint validation for https://login.microsoftonline.com is Successful.
Connecting to endpoint https://login.windows.net
Endpoint validation for https://login.windows.net is Successful.
Connecting to endpoint https://policykeyservice.dc.ad.msft.net/clientregistrationmanager.svc
Endpoint validation for https://policykeyservice.dc.ad.msft.net/clientregistrationmanager.svc is Successful.
Connecting to endpoint https://policykeyservice.dc.ad.msft.net/policymanager.svc
Endpoint validation for https://policykeyservice.dc.ad.msft.net/policymanager.svc is Successful.
Connectivity Test Step 1 of 3 - Testing dependent service endpoints completed successfully.

Connectivity Test Step 2 of 3 - Blob data upload procedure begins ...
Tenant Id is successfully collected during agent registration.
Connectivity Test Step 2 of 3 - Blob data upload procedure completed successfully.

Connectivity Test Step 3 of 3 - EventHub data upload procedure begins ...
Tenant Id is successfully collected during agent registration.
Connectivity Test Step 3 of 3 - EventHub data upload procedure completed successfully.

Test-AzureADConnectHealthConnectivity completed successfully...
```

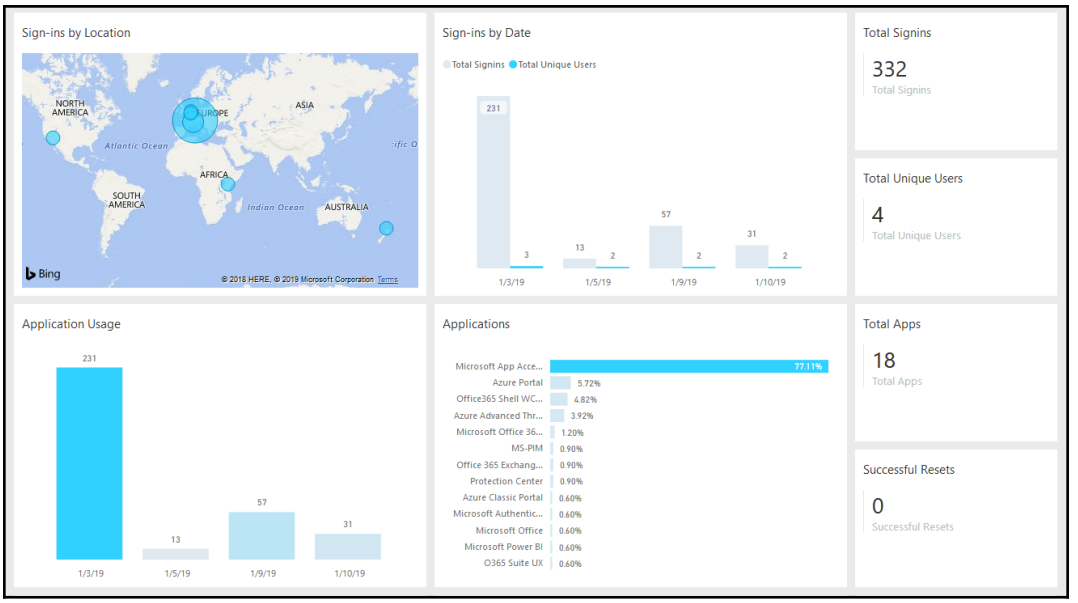

Dashboard > INOVITDEMOS provided by inovit GmbH - Sign-ins
INOVITDEMOS provided by inovit GmbH - Sign-ins
Azure Active Directory
Search (Ctrl+/)
App registrations
App registrations (Preview)
Application proxy
Licenses
Azure AD Connect
Custom domain names
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Notifications settings
Security
Overview (Preview)
Identity Secure Score (Previe...
Conditional Access
MFA
Users flagged for risk
Risk events
Authentication methods
Monitoring
Sign-ins
Audit logs
Logs
Diagnostic settings
Columns
Refresh
Download
Script
Power BI
Export Data Settings
Troubleshoot
Search is case sensitive and supports 'starts with' operator
User
Filter by name or object id
Application
Filter by app name or applicatio...
Status
All
Conditional Access
All
Date
Last 7 days
Show dates as:
Local
UTC
Apply
Reset
DATE
USER
APPLICATION
STATUS
CONDITIONAL ACCESS
MFA REQUIRED
1/10/2019, 4:17:45 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 3:17:33 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 3:14:10 PM
Tenant Administrator (Breaking Glass)
Azure Portal
Success
Not Applied
No
1/10/2019, 2:36:22 PM
Jochen Nickel
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:36:12 PM
Jochen Nickel
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:51 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:49 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:49 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:49 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:47 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:46 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:44 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:15:02 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:14:59 PM
Tenant Administrator (Breaking Glass)
Azure Advanced Threat Protection
Success
Not Applied
No
1/10/2019, 2:14:32 PM
Tenant Administrator (Breaking Glass)
Office365 Shell WCSS-Client
Success
Not Applied
No
Load more

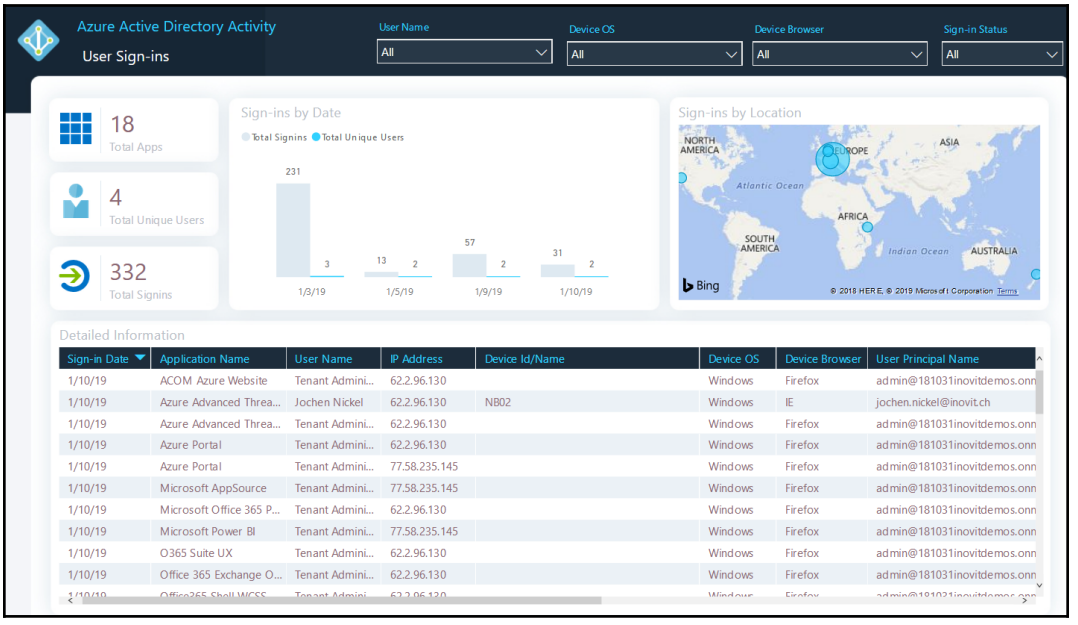

Details
Basic info
Device info
MFA info
Conditional Access
Request Id
6f2caefd-227e-4682-bff4-a3b99ca25600
Correlation Id
20804f00-dd1b-4b0a-a370-1eac629b8e77
User
Jochen Nickel
Username
jochen.nickel@inovit.ch
User ID
07bf426f-4188-433d-99b9-d14d2f3e62c1
Application
Azure Advanced Threat Protection
Application ID
7b7531ad-5926-4f2d-8a1d-38495ad33e17
IP address
62.2.96.130
Location
Cugy, Vaud, CH
Date
1/10/2019, 2:36:22 PM
Status
Success
Client App
Browser


Welcome to Power BI
You're on your way to exploring your data and monitoring what matters.
Let's start by getting some data.
Need more guidance? Try this tutorial or watch a video
Discover content
Create new content
My organization
Discover apps published by other people in your organization.
Get
Services
Choose apps from online services that you use.
Get
Files
Bring in your reports, workbooks, or data from Excel, Power BI Desktop or CSV files.
Get
Databases
Use Power BI Desktop to connect to data in Azure SQL Database and more.
Get
More ways to create your own content
Samples
Organizational Content Packs
Partner Showcase
Service Content Packs

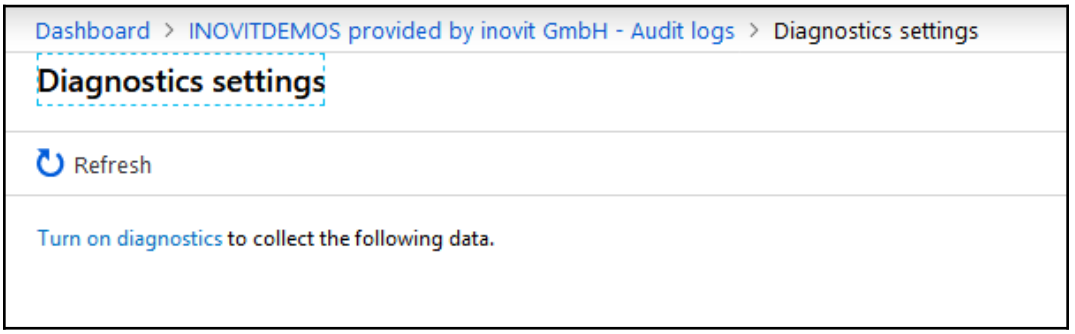

Connect to Azure Active Directory Activity Logs
Number of Days
Pull the report for the # of days entered here. Maximum days allowed is 30. Default value is 7. If your tenant has high volume of data, please keep it less than 7 days
7
TenantName
Enter your Tenant Name here (e.g. contoso.onmicrosoft.com)
181031inovitdemos.onmicrosoft.com
Need help connecting? Learn more

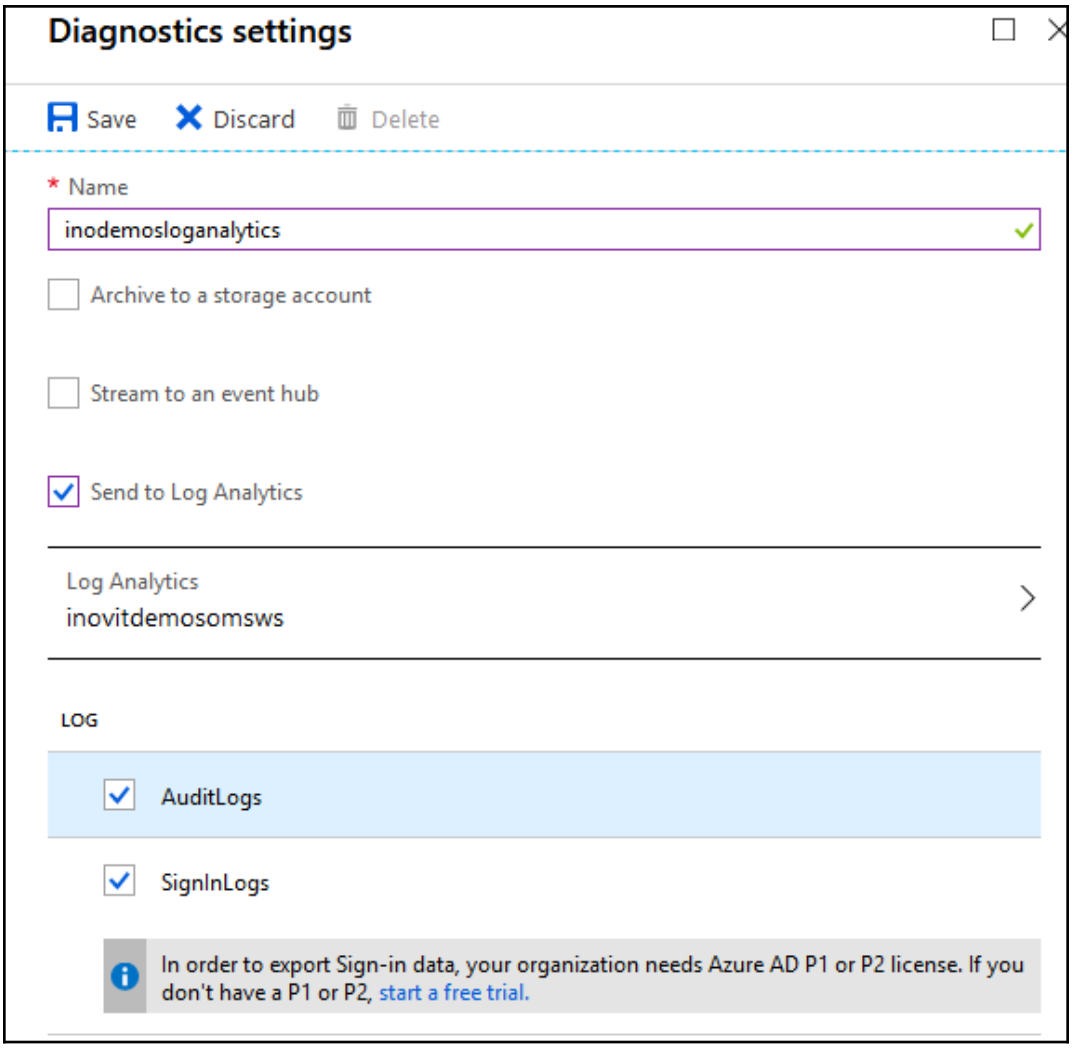

Microsoft
admin@181031inovitdemos.onmicrosoft.com
Permissions requested
Accept for your organization
Azure AD Power BI Content Pack App
App info
This app would like to:
Sign in and read user profile
Read directory data
Read all audit log data
Read audit log data
Sign in and read user profile
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept

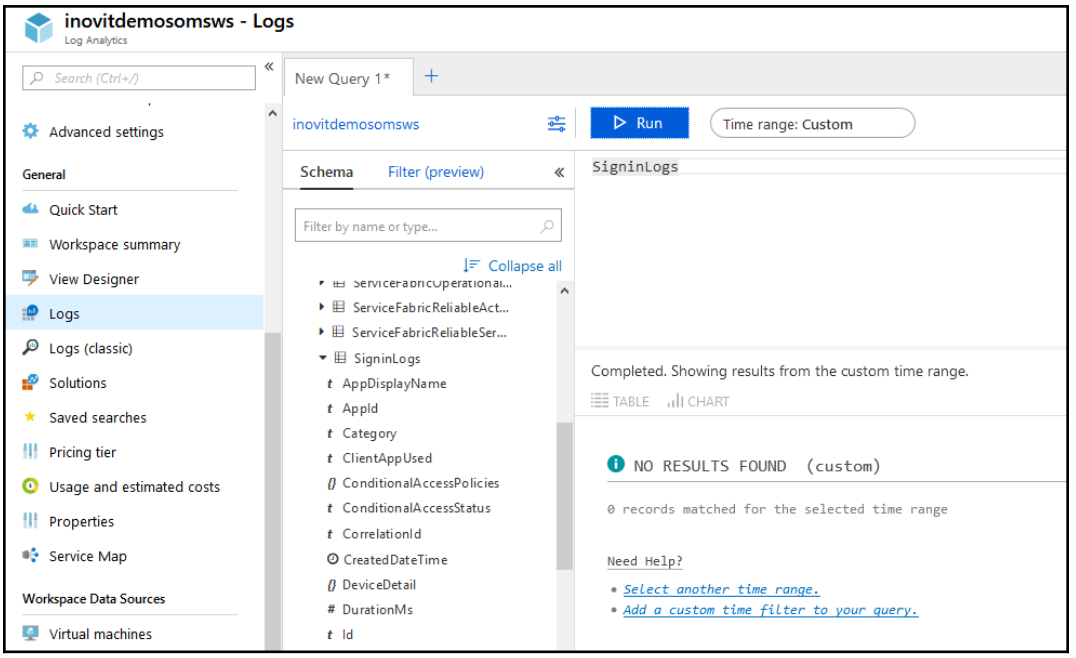

Sign-ins by Location
NORTH AMERICA
EUROPE
ASIA
Atlantic Ocean
AFRICA
SOUTH AMERICA
Indian Ocean
AUSTRALIA
Bing
© 2018 HERE, © 2019 Microsoft Corporation Terms
Sign-ins by Date
Total Signins
Total Unique Users
231
3
13
2
57
2
31
2
1/3/19
1/5/19
1/9/19
1/10/19
Total Signins
332
Total Signins
Total Unique Users
4
Total Unique Users
Application Usage
231
13
57
31
1/3/19
1/5/19
1/9/19
1/10/19
Applications
Microsoft App Acce... 77.11%
Azure Portal 5.72%
Office365 Shell WC... 4.82%
Azure Advanced Thr... 3.92%
Microsoft Office 36... 1.20%
MS-PIM 0.90%
Office 365 Exchang... 0.90%
Protection Center 0.90%
Azure Classic Portal 0.60%
Microsoft Authentic... 0.60%
Microsoft Office 0.60%
Microsoft Power BI 0.60%
O365 Suite UX 0.60%
Total Apps
18
Total Apps
Successful Resets
0
Successful Resets

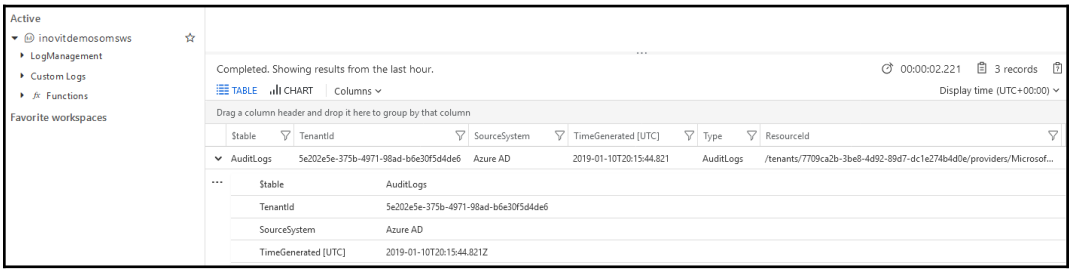

Azure Active Directory Activity
User Sign-ins
User Name
All
Device OS
All
Device Browser
All
Sign-in Status
All
18
Total Apps
4
Total Unique Users
332
Total Signins
Sign-ins by Date
Total Signins
Total Unique Users
231
3
13
2
57
2
31
2
1/3/19
1/5/19
1/9/19
1/10/19
Sign-ins by Location
NORTH AMERICA
EUROPE
ASIA
Atlantic Ocean
AFRICA
SOUTH AMERICA
Indian Ocean
AUSTRALIA
Bing
Detailed Information
Sign-in Date
Application Name
User Name
IP Address
Device Id/Name
Device OS
Device Browser
User Principal Name
1/10/19 ACOM Azure Website Tenant Admini... 62.2.96.130 Windows Firefox admin@181031inovitdemos.onn
1/10/19 Azure Advanced Threa... Jochen Nickel 62.2.96.130 NB02 Windows IE jochen.nickel@inovit.ch
1/10/19 Azure Advanced Threa... Tenant Admini... 62.2.96.130 Windows Firefox admin@181031inovitdemos.onn
1/10/19 Azure Portal Tenant Admini... 62.2.96.130 Windows Firefox admin@181031inovitdemos.onn
1/10/19 Azure Portal Tenant Admini... 77.58.235.145 Windows Firefox admin@181031inovitdemos.onn
1/10/19 Microsoft AppSource Tenant Admini... 77.58.235.145 Windows Firefox admin@181031inovitdemos.onn
1/10/19 Microsoft Office 365 P... Tenant Admini... 62.2.96.130 Windows Firefox admin@181031inovitdemos.onn
1/10/19 Microsoft Power BI Tenant Admini... 77.58.235.145 Windows Firefox admin@181031inovitdemos.onn
1/10/19 O365 Suite UX Tenant Admini... 62.2.96.130 Windows Firefox admin@181031inovitdemos.onn
1/10/19 Office 365 Exchange O... Tenant Admini... 62.2.96.130 Windows Firefox admin@181031inovitdemos.onn

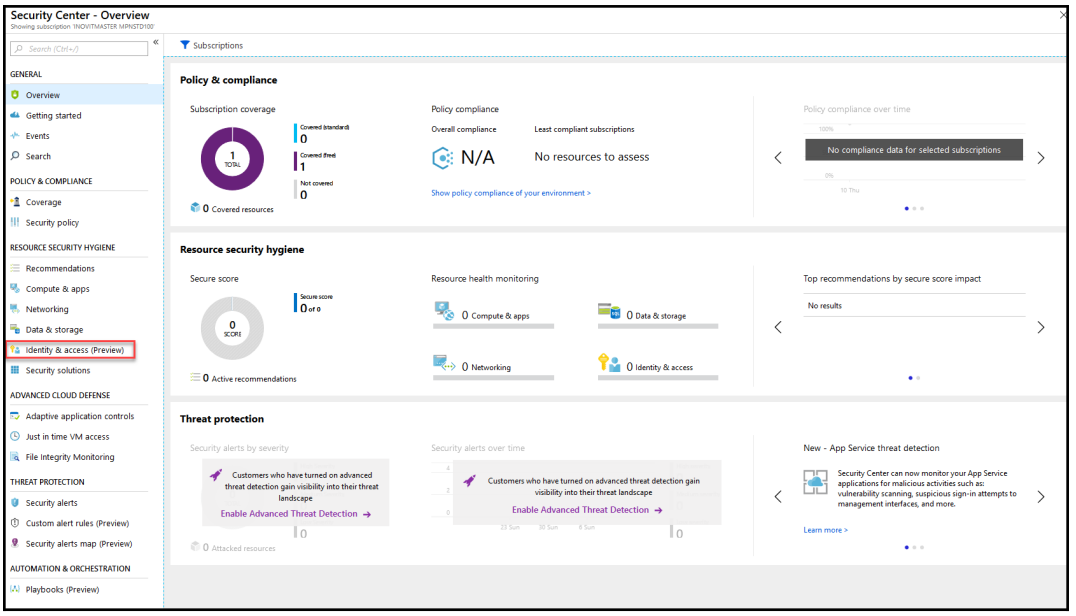
1/10/2019, 8:55:44 PM	ServicePrincipal : Azure AD Power BI Content Pack App	admin@181031inovitdemos.onmicrosoft.com	Consent to application
1/10/2019, 8:55:44 PM	ServicePrincipal : Azure AD Power BI Content Pack App, User :...	admin@181031inovitdemos.onmicrosoft.com	Add app role assignment grant to user
1/10/2019, 8:55:44 PM	ServicePrincipal : Microsoft Graph, ServicePrincipal : b3a0a59...	admin@181031inovitdemos.onmicrosoft.com	Add OAuth2PermissionGrant
1/10/2019, 8:55:44 PM	ServicePrincipal : Windows Azure Active Directory, ServicePri...	admin@181031inovitdemos.onmicrosoft.com	Add OAuth2PermissionGrant
1/10/2019, 8:55:44 PM	ServicePrincipal : Microsoft Graph, ServicePrincipal : https://...	admin@181031inovitdemos.onmicrosoft.com	Add app role assignment to service principal
1/10/2019, 8:55:44 PM	ServicePrincipal : Windows Azure Active Directory, ServicePri...	admin@181031inovitdemos.onmicrosoft.com	Add app role assignment to service principal
1/10/2019, 8:55:43 PM	ServicePrincipal : Azure AD Power BI Content Pack App	admin@181031inovitdemos.onmicrosoft.com	Add service principal

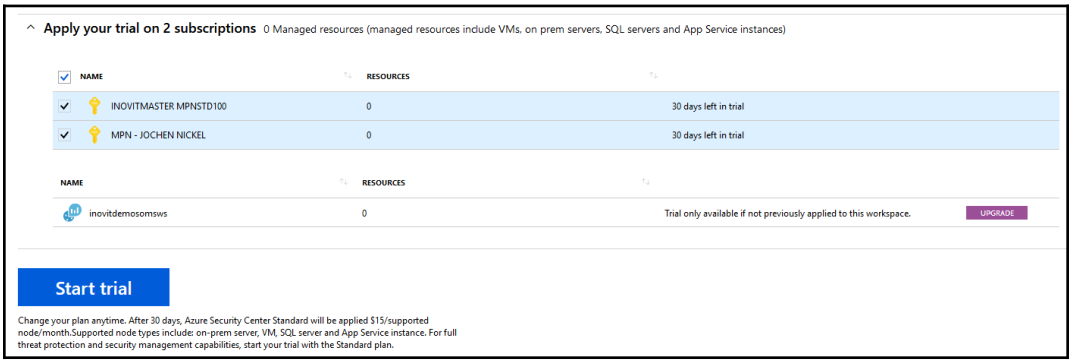



Diagnostics settings
Save
Discard
Delete
* Name
inodemosloganalytics
Archive to a storage account
Stream to an event hub
Send to Log Analytics
Log Analytics
inovitdemosomsws
LOG
AuditLogs
SignInLogs
In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, start a free trial.

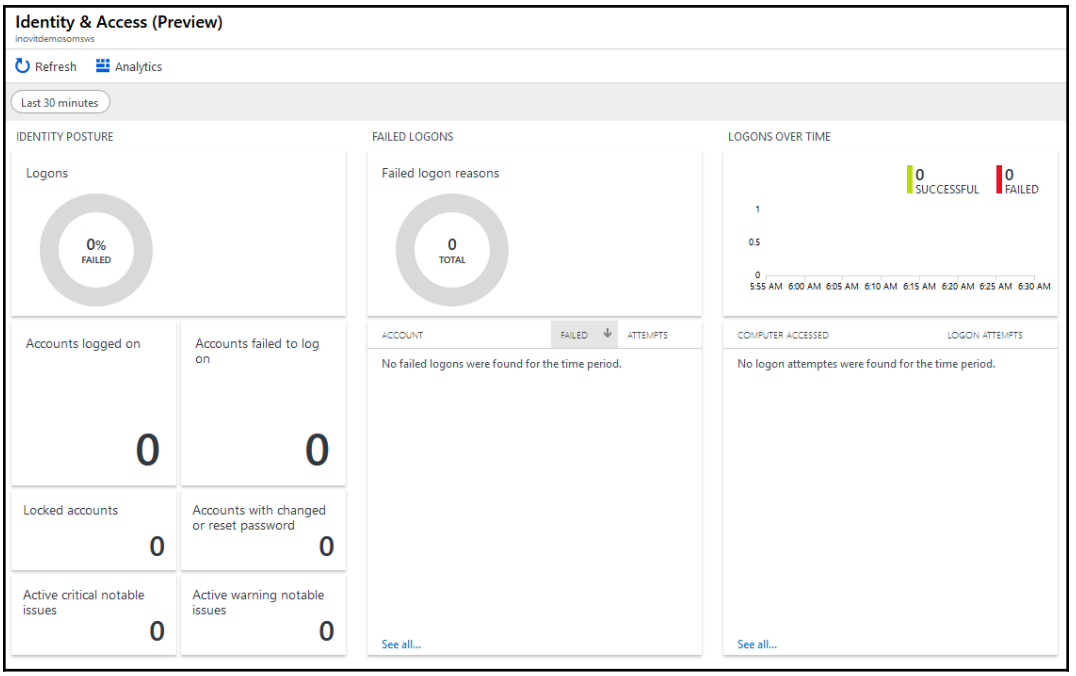

inovitdemosomsws - Logs
Log Analytics
Search (Ctrl+/)
Advanced settings
General
Quick Start
Workspace summary
View Designer
Logs
Logs (classic)
Solutions
Saved searches
Pricing tier
Usage and estimated costs
Properties
Service Map
Workspace Data Sources
Virtual machines
New Query 1*
inovitdemosomsws
Run
Time range: Custom
Schema
Filter (preview)
Filter by name or type...
Collapse all
ServiceFabricReliableAct...
ServiceFabricReliableSer...
SigninLogs
AppDisplayName
AppId
Category
ClientAppUsed
ConditionalAccessPolicies
ConditionalAccessStatus
CorrelationId
CreatedDateTime
DeviceDetail
DurationMs
Id
SigninLogs
Completed. Showing results from the custom time range.
TABLE
CHART
NO RESULTS FOUND (custom)
0 records matched for the selected time range
Need Help?
Select another time range.
Add a custom time filter to your query.


Active
inovitdemosomsws
LogManagement
Custom Logs
Functions
Favorite workspaces
Completed. Showing results from the last hour.
00:00:02.221
3 records
TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column
$table
TenantId
SourceSystem
TimeGenerated [UTC]
Type
ResourceId
AuditLogs
5e202e5e-375b-4971-98ad-b6e30f5d4de6
Azure AD
2019-01-10T20:15:44.821
AuditLogs
/tenants/7709ca2b-3be8-4d92-89d7-dc1e274b4d0e/providers/Microsof...
$table
AuditLogs
TenantId
5e202e5e-375b-4971-98ad-b6e30f5d4de6
SourceSystem
Azure AD
TimeGenerated [UTC]
2019-01-10T20:15:44.821Z

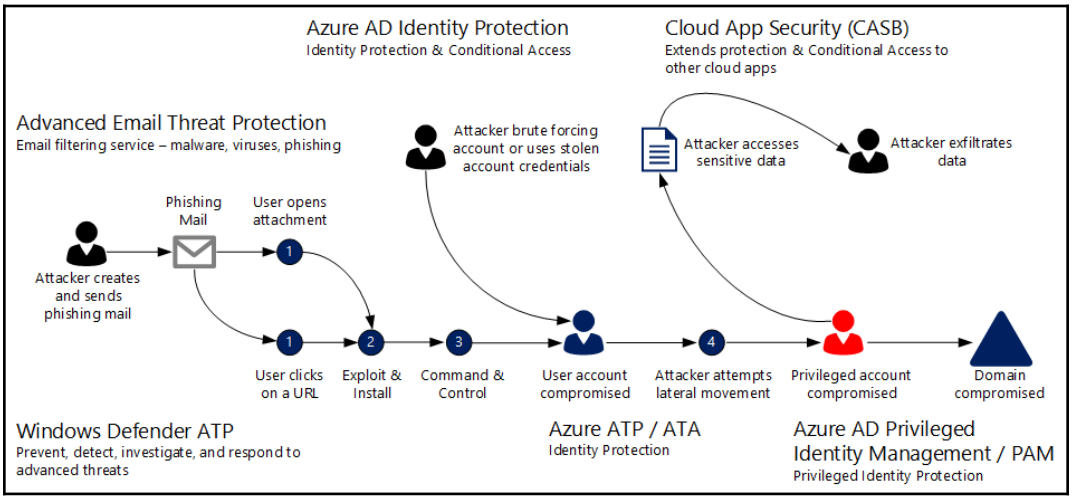

Security Center - Overview
Showing subscription 'INOVITMASTER MPNSTD100'
Search (Ctrl+/)
Subscriptions
GENERAL
Overview
Getting started
Events
Search
POLICY & COMPLIANCE
Coverage
Security policy
RESOURCE SECURITY HYGIENE
Recommendations
Compute & apps
Networking
Data & storage
Identity & access (Preview)
Security solutions
ADVANCED CLOUD DEFENSE
Adaptive application controls
Just in time VM access
File Integrity Monitoring
THREAT PROTECTION
Security alerts
Custom alert rules (Preview)
Security alerts map (Preview)
AUTOMATION & ORCHESTRATION
Playbooks (Preview)
Policy & compliance
Subscription coverage
1 TOTAL
Covered (standard)
0
Covered (free)
1
Not covered
0
0 Covered resources
Policy compliance
Overall compliance
Least compliant subscriptions
N/A
No resources to assess
Show policy compliance of your environment >
Policy compliance over time
No compliance data for selected subscriptions
Resource security hygiene
Secure score
0 SCORE
Secure score
0 of 0
0 Active recommendations
Resource health monitoring
0 Compute & apps
0 Data & storage
0 Networking
0 Identity & access
Top recommendations by secure score impact
No results
Threat protection
Security alerts by severity
Customers who have turned on advanced threat detection gain visibility into their threat landscape
Enable Advanced Threat Detection
0 Attacked resources
Security alerts over time
Customers who have turned on advanced threat detection gain visibility into their threat landscape
Enable Advanced Threat Detection
New - App Service threat detection
Security Center can now monitor your App Service applications for malicious activities such as: vulnerability scanning, suspicious sign-in attempts to management interfaces, and more.
Learn more >

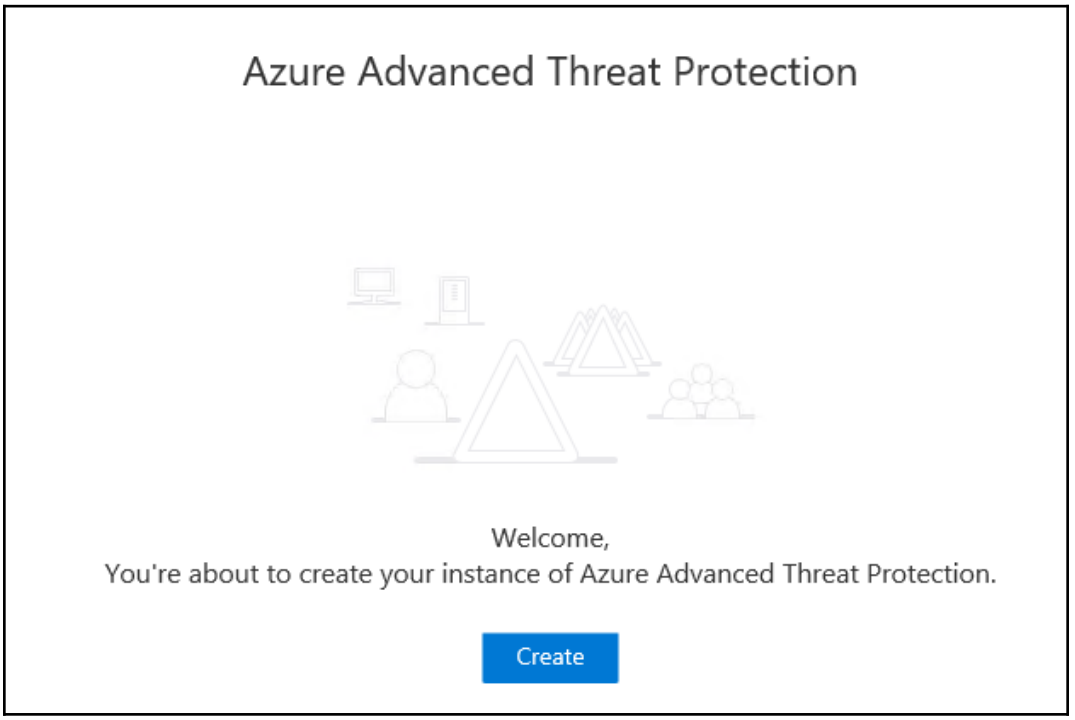

Apply your trial on 2 subscriptions
0 Managed resources (managed resources include VMs, on prem servers, SQL servers and App Service instances)
NAME
RESOURCES
INOVITMASTER MPNSTD100
0
30 days left in trial
MPN - JOCHEN NICKEL
0
30 days left in trial
NAME
RESOURCES
inovitdemosomsws
0
Trial only available if not previously applied to this workspace.
UPGRADE
Start trial
Change your plan anytime. After 30 days, Azure Security Center Standard will be applied $15/supported node/month.Supported node types include: on-prem server, VM, SQL server and App Service instance. For full threat protection and security management capabilities, start your trial with the Standard plan.

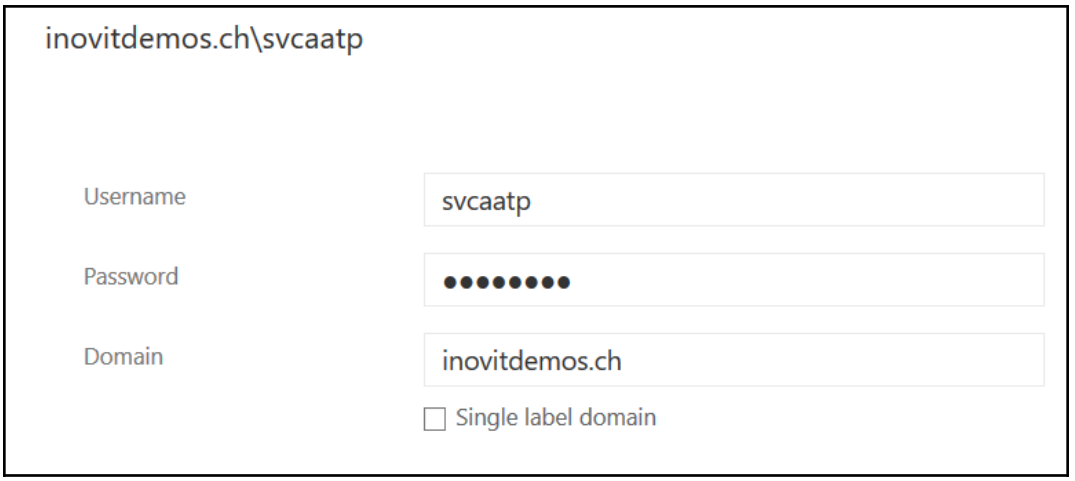

NAME
RESOURCES
inovitdemosomsws
0
Trial only available if not previously applied to this workspace.
✓ UPGRADED

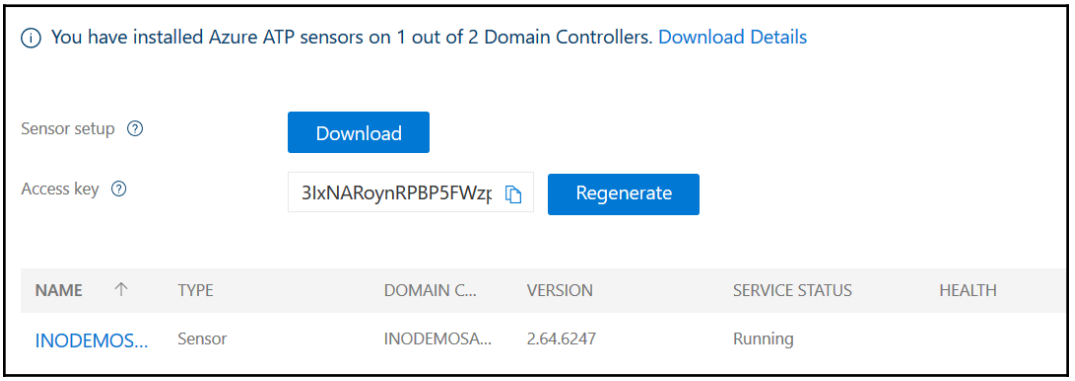

Identity & Access (Preview)
inovitdemosomsws
Refresh
Analytics
Last 30 minutes
IDENTITY POSTURE
Logons
0%
FAILED
Accounts logged on
0
Accounts failed to log on
0
Locked accounts
0
Accounts with changed or reset password
0
Active critical notable issues
0
Active warning notable issues
0
FAILED LOGONS
Failed logon reasons
0
TOTAL
ACCOUNT
FAILED
ATTEMPTS
No failed logons were found for the time period.
See all...
LOGONS OVER TIME
0
SUCCESSFUL
0
FAILED
1
0.5
0
5:55 AM
6:00 AM
6:05 AM
6:10 AM
6:15 AM
6:20 AM
6:25 AM
6:30 AM
COMPUTER ACCESSED
LOGON ATTEMPTS
No logon attemptes were found for the time period.
See all...

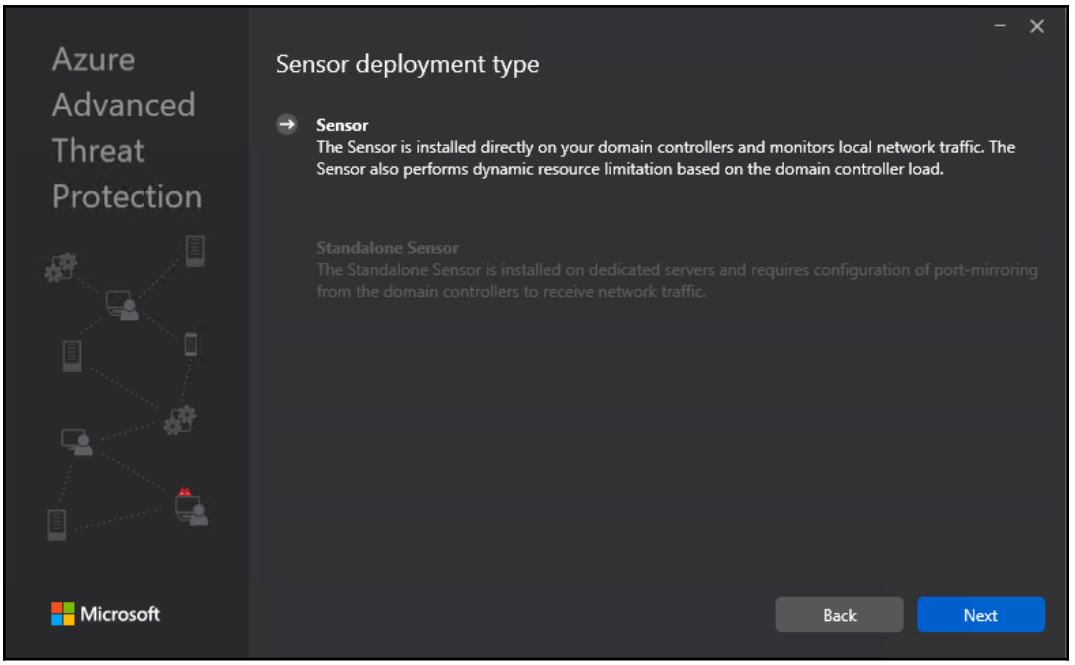
Chapter 5: Configuring and Managing Identity Protection

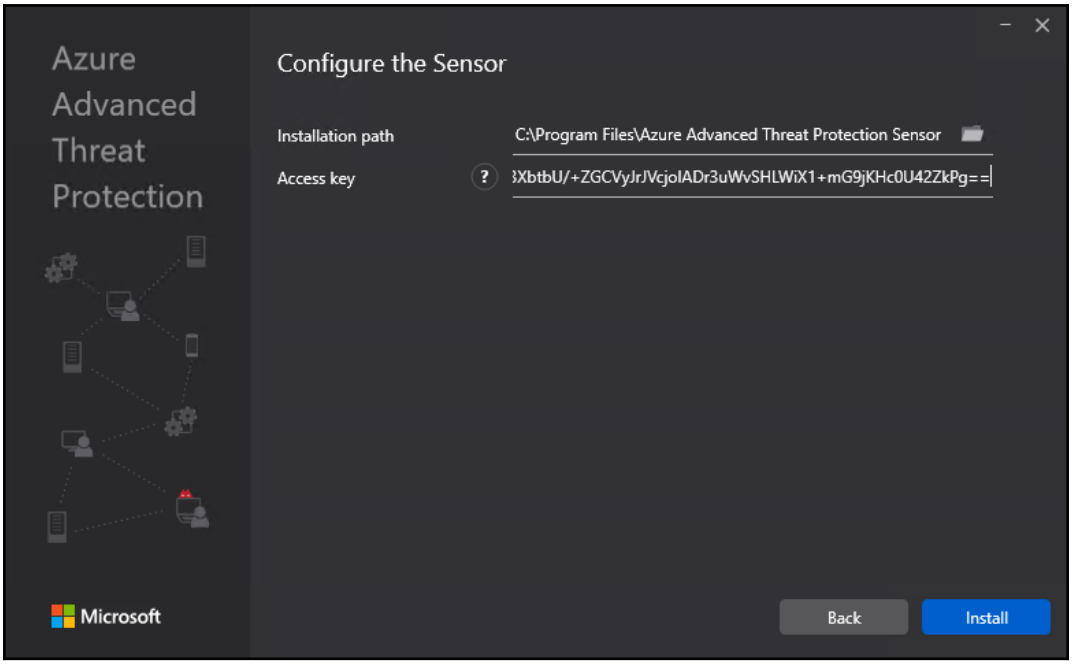


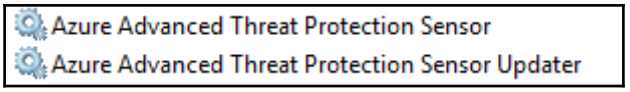


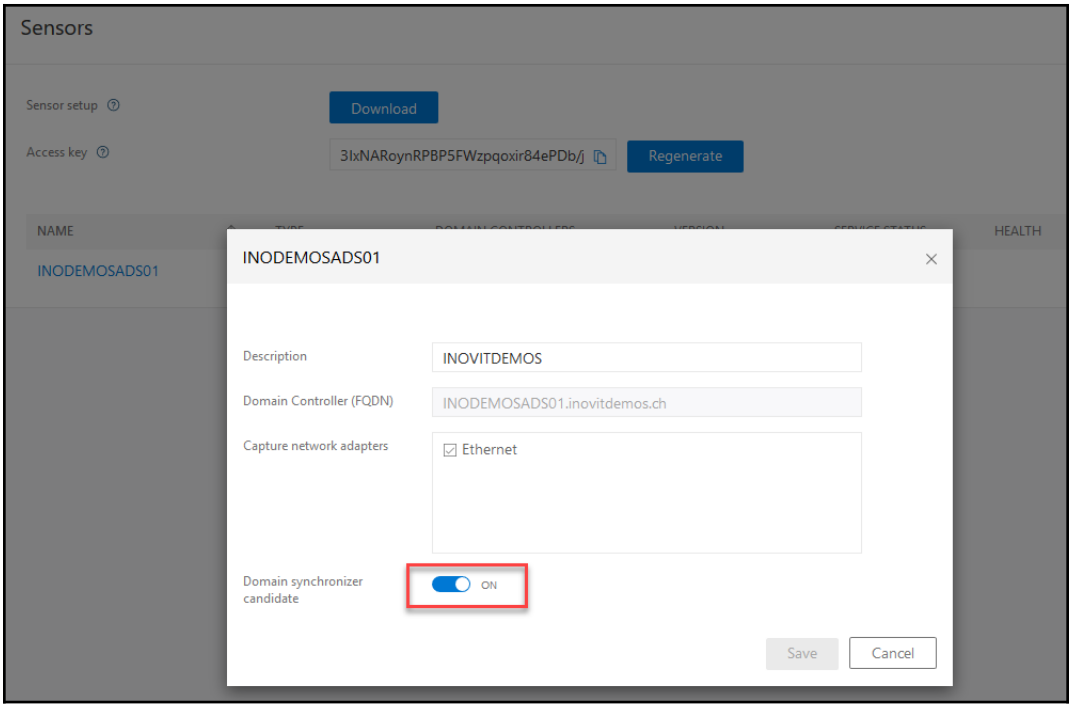

inovitdemos.ch\svcaatp
Username
svcaatp
Password
Domain
inovitdemos.ch
Single label domain


You have installed Azure ATP sensors on 1 out of 2 Domain Controllers. Download Details
Sensor setup
Download
Access key
3IxNARoynRPBP5FWzp
Regenerate
NAME
TYPE
DOMAIN C...
VERSION
SERVICE STATUS
HEALTH
INODEMOS...
Sensor
INODEMOSA...
2.64.6247
Running

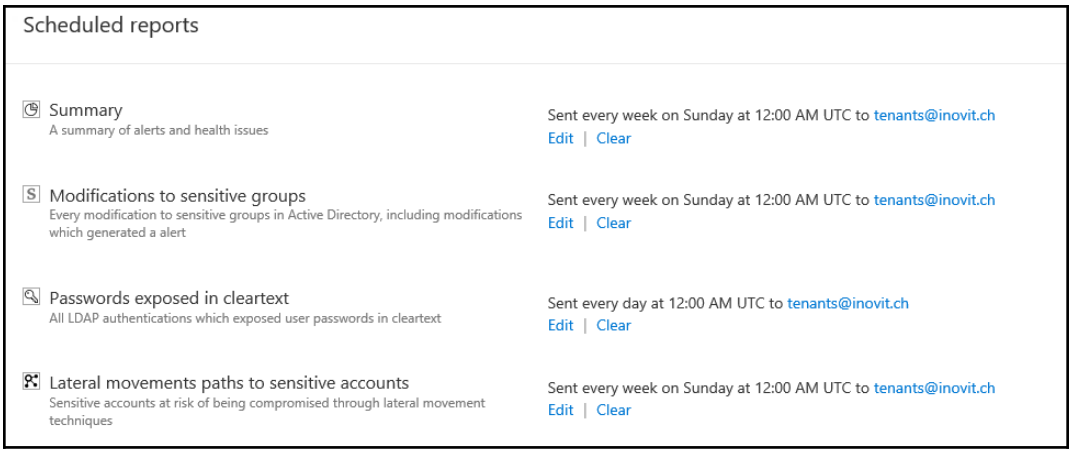

Azure
Advanced
Threat
Protection
Sensor deployment type
Sensor
The Sensor is installed directly on your domain controllers and monitors local network traffic. The Sensor also performs dynamic resource limitation based on the domain controller load.
Standalone Sensor
The Standalone Sensor is installed on dedicated servers and requires configuration of port-mirroring from the domain controllers to receive network traffic.
Microsoft
Back
Next

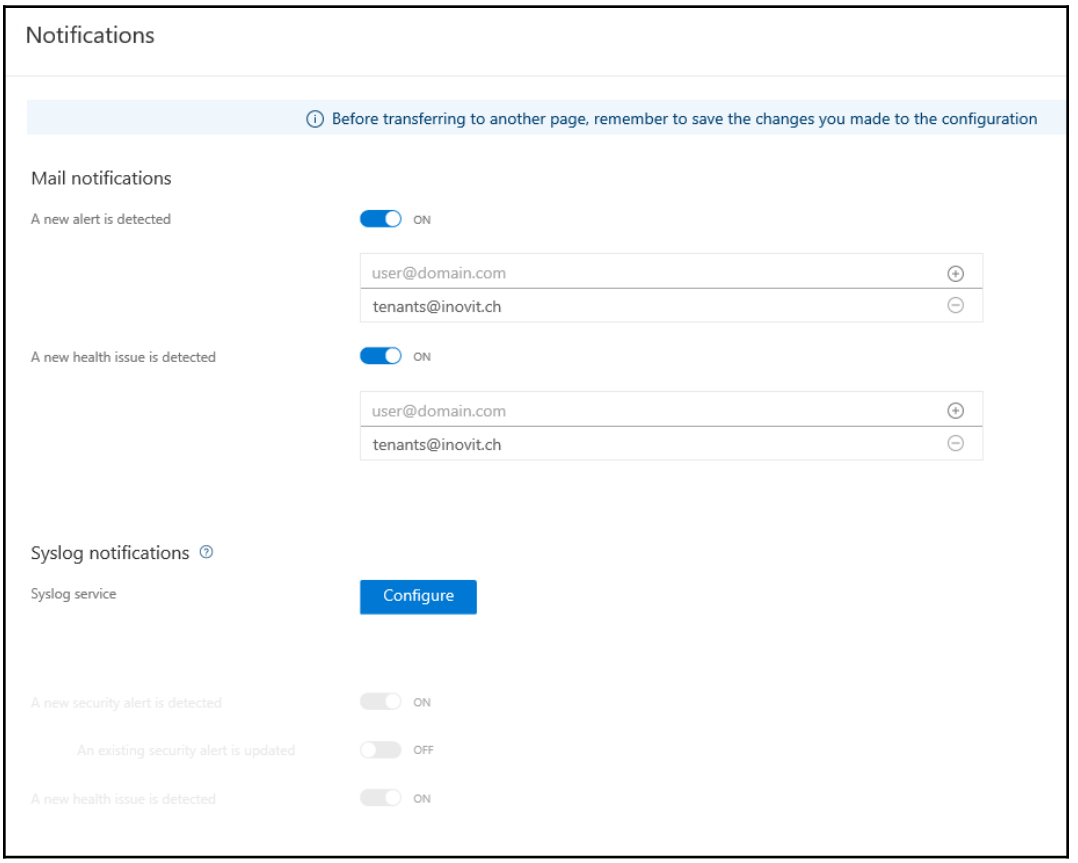

Azure
Advanced
Threat
Protection
Configure the Sensor
Installation path
C:\Program Files\Azure Advanced Threat Protection Sensor
Access key
?
XbtbU/+ZGCVyJrJVcjolADr3uWvSHLWiX1+mG9jKHc0U42ZkPg==
Microsoft
Back
Install

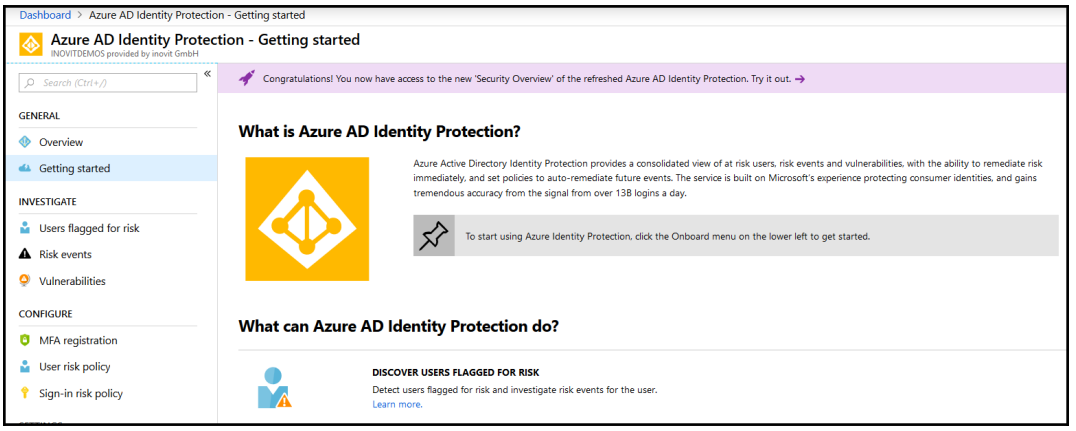

Azure Advanced Threat Protection Sensor
Azure Advanced Threat Protection Sensor Updater

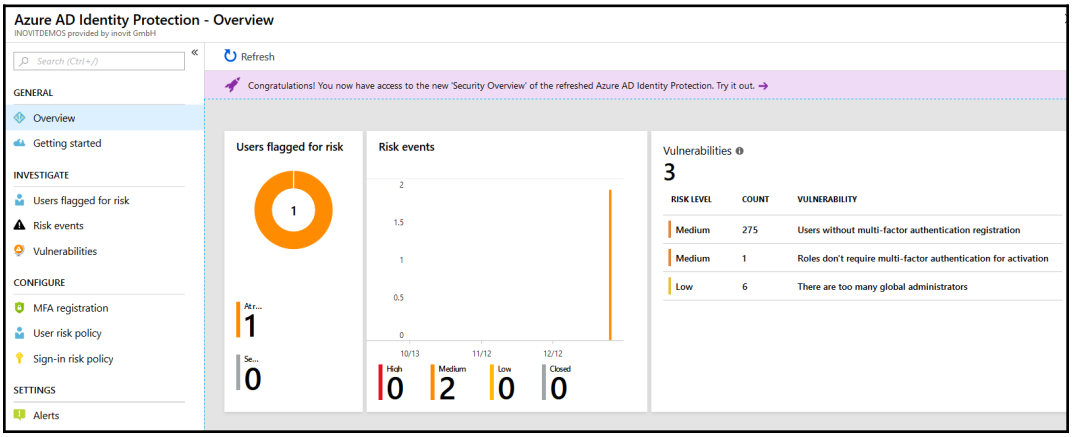

Sensors
Sensor setup
Download
Access key
3IxNARoynRPBP5FWzpqoxir84ePDb/j
Regenerate
NAME
HEALTH
INODEMOSADS01
INODEMOSADS01
Description
INOVITDEMOS
Domain Controller (FQDN)
INODEMOSADS01.inovitdemos.ch
Capture network adapters
Ethernet
Domain synchronizer candidate
ON
Save
Cancel

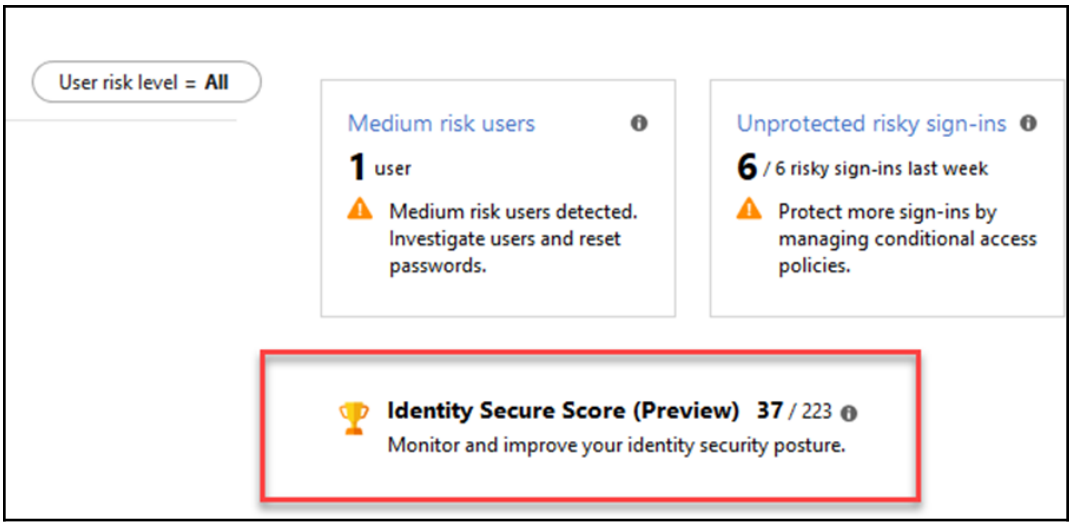

Detections
Suspected Golden Ticket usage (ticket anomaly)
ON

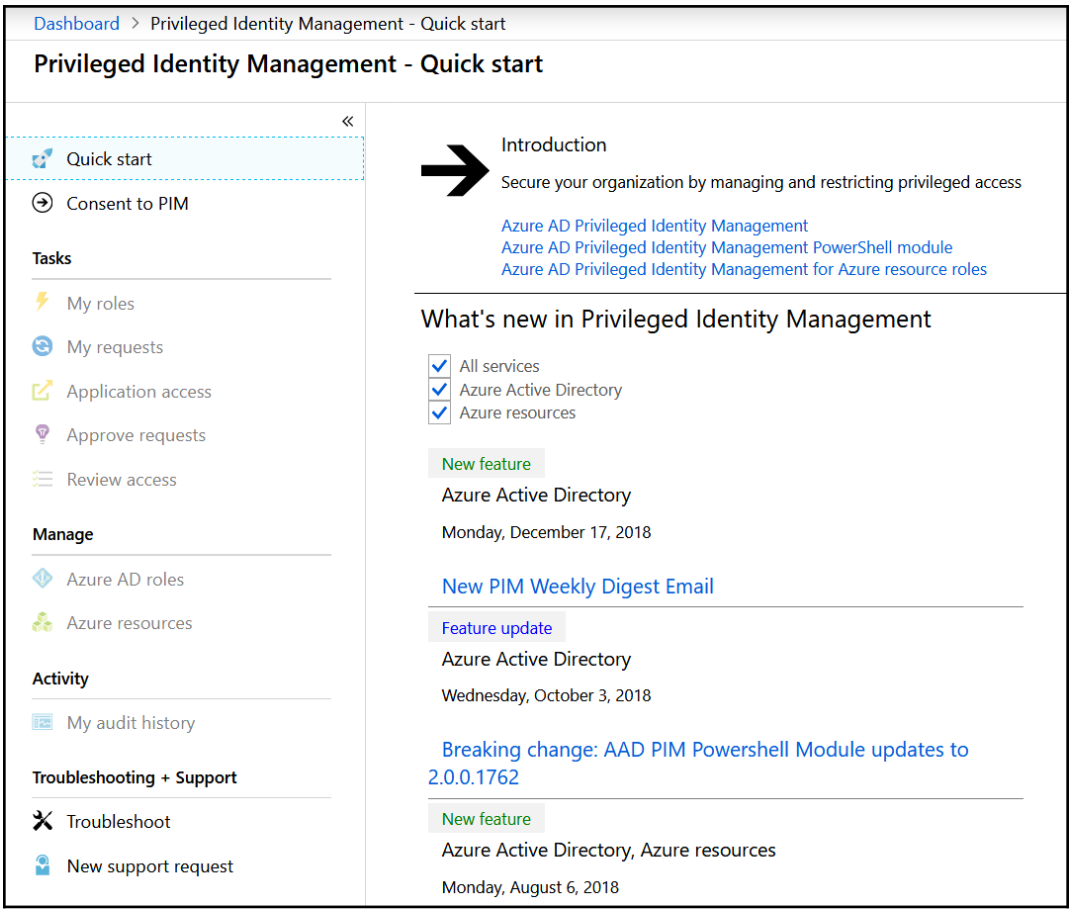

Scheduled reports
Summary
A summary of alerts and health issues
Sent every week on Sunday at 12:00 AM UTC to tenants@inovit.ch
Edit | Clear
Modifications to sensitive groups
Every modification to sensitive groups in Active Directory, including modifications which generated a alert
Sent every week on Sunday at 12:00 AM UTC to tenants@inovit.ch
Edit | Clear
Passwords exposed in cleartext
All LDAP authentications which exposed user passwords in cleartext
Sent every day at 12:00 AM UTC to tenants@inovit.ch
Edit | Clear
Lateral movements paths to sensitive accounts
Sensitive accounts at risk of being compromised through lateral movement techniques
Sent every week on Sunday at 12:00 AM UTC to tenants@inovit.ch
Edit | Clear

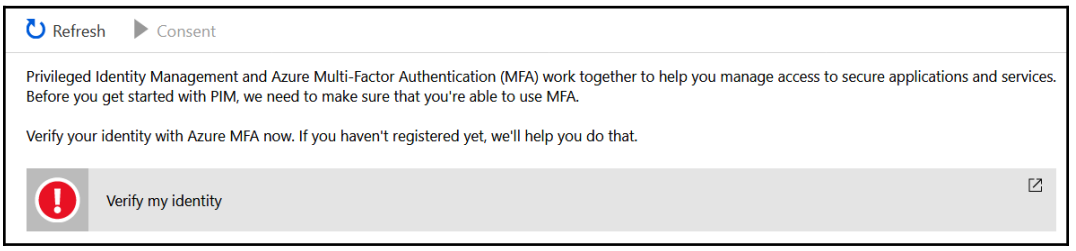

Notifications
Before transferring to another page, remember to save the changes you made to the configuration
Mail notifications
A new alert is detected
ON
user@domain.com
tenants@inovit.ch
A new health issue is detected
ON
user@domain.com
tenants@inovit.ch
Syslog notifications
Syslog service
Configure
A new security alert is detected
ON
An existing security alert is updated
OFF
A new health issue is detected
ON


Dashboard > Azure AD Identity Protection - Getting started
Azure AD Identity Protection - Getting started
INOVITDEMOS provided by inovit GmbH
Search (Ctrl+/)
GENERAL
Overview
Getting started
INVESTIGATE
Users flagged for risk
Risk events
Vulnerabilities
CONFIGURE
MFA registration
User risk policy
Sign-in risk policy
Congratulations! You now have access to the new 'Security Overview' of the refreshed Azure AD Identity Protection. Try it out.
What is Azure AD Identity Protection?
Azure Active Directory Identity Protection provides a consolidated view of at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft's experience protecting consumer identities, and gains tremendous accuracy from the signal from over 13B logins a day.
To start using Azure Identity Protection, click the Onboard menu on the lower left to get started.
What can Azure AD Identity Protection do?
DISCOVER USERS FLAGGED FOR RISK
Detect users flagged for risk and investigate risk events for the user.
Learn more.

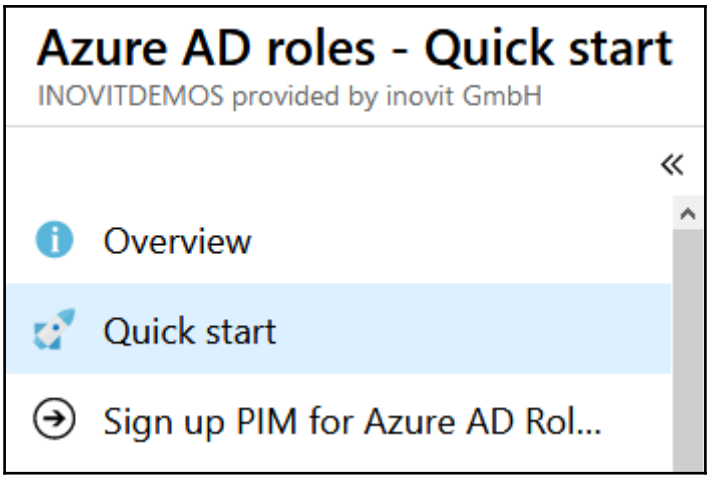

Azure AD Identity Protection - Overview
INOVITDEMOS provided by inovit GmbH
Search (Ctrl+/)
Refresh
GENERAL
Overview
Getting started
INVESTIGATE
Users flagged for risk
Risk events
Vulnerabilities
CONFIGURE
MFA registration
User risk policy
Sign-in risk policy
SETTINGS
Alerts
Congratulations! You now have access to the new 'Security Overview' of the refreshed Azure AD Identity Protection. Try it out.
Users flagged for risk
1
Risk events
2
1.5
1
0.5
0
10/13
11/12
12/12
High 0
Medium 2
Low 0
Closed 0
Vulnerabilities
3
RISK LEVEL
COUNT
VULNERABILITY
Medium 275 Users without multi-factor authentication registration
Medium 1 Roles don't require multi-factor authentication for activation
Low 6 There are too many global administrators

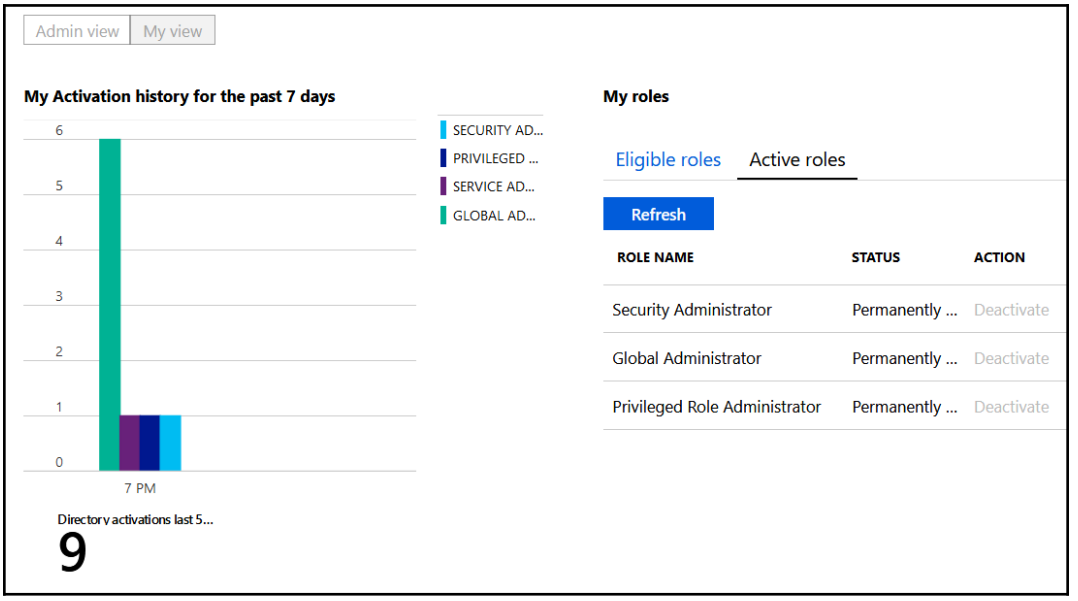

User risk level = All
Medium risk users
1 user
Medium risk users detected. Investigate users and reset passwords.
Unprotected risky sign-ins
6 / 6 risky sign-ins last week
Protect more sign-ins by managing conditional access policies.
Identity Secure Score (Preview) 37 / 223
Monitor and improve your identity security posture.

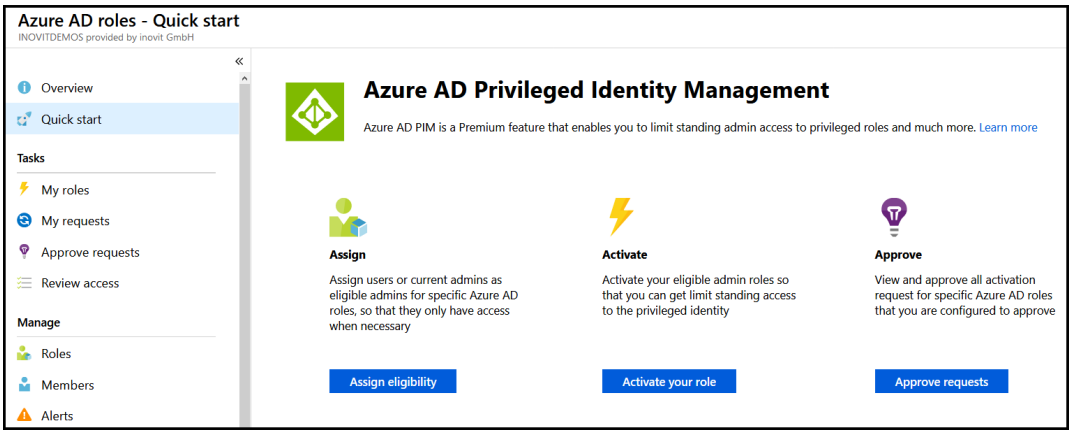

Dashboard > Privileged Identity Management - Quick start
Privileged Identity Management - Quick start
Quick start
Consent to PIM
Tasks
My roles
My requests
Application access
Approve requests
Review access
Manage
Azure AD roles
Azure resources
Activity
My audit history
Troubleshooting + Support
Troubleshoot
New support request
Introduction
Secure your organization by managing and restricting privileged access
Azure AD Privileged Identity Management
Azure AD Privileged Identity Management PowerShell module
Azure AD Privileged Identity Management for Azure resource roles
What's new in Privileged Identity Management
All services
Azure Active Directory
Azure resources
New feature
Azure Active Directory
Monday, December 17, 2018
New PIM Weekly Digest Email
Feature update
Azure Active Directory
Wednesday, October 3, 2018
Breaking change: AAD PIM Powershell Module updates to 2.0.0.1762
New feature
Azure Active Directory, Azure resources
Monday, August 6, 2018

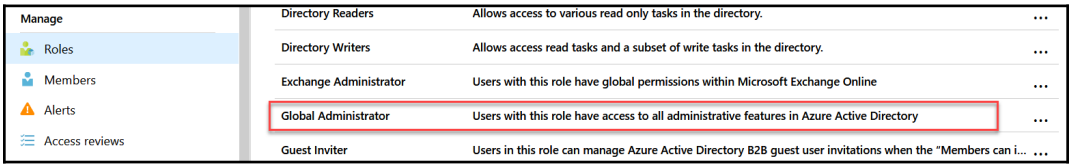

Refresh
Consent
Privileged Identity Management and Azure Multi-Factor Authentication (MFA) work together to help you manage access to secure applications and services. Before you get started with PIM, we need to make sure that you're able to use MFA.
Verify your identity with Azure MFA now. If you haven't registered yet, we'll help you do that.
Verify my identity

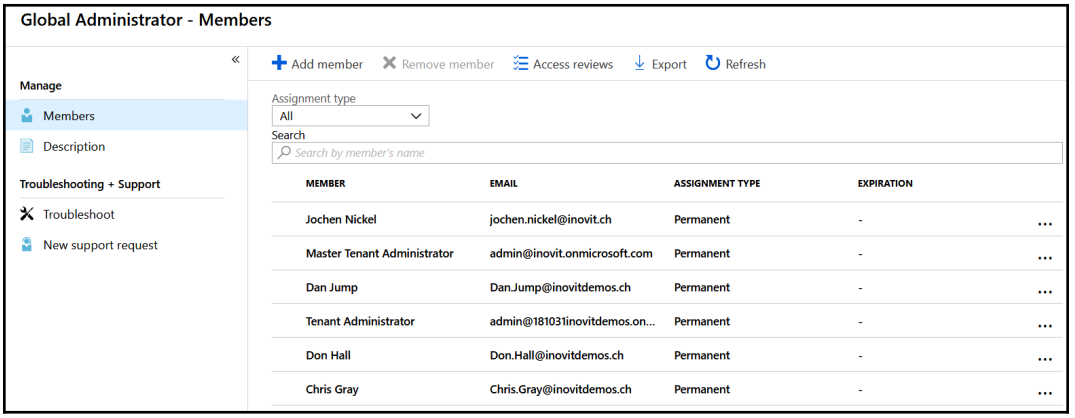

Refresh
Consent


Azure AD roles - Quick start
INOVITDEMOS provided by inovit GmbH
Overview
Quick start
Sign up PIM for Azure AD Rol...

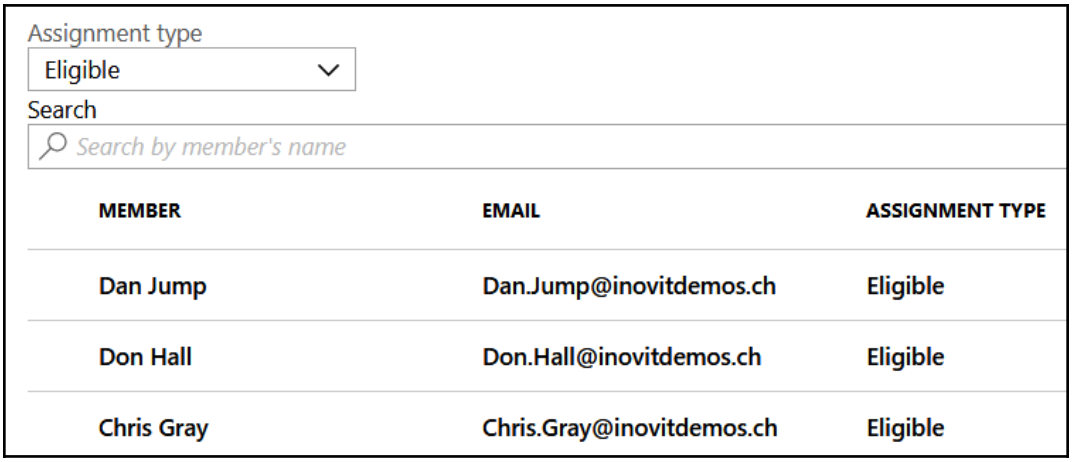

Admin view
My view
My Activation history for the past 7 days
6
5
4
3
2
1
0
7 PM
SECURITY AD...
PRIVILEGED ...
SERVICE AD...
GLOBAL AD...
Directory activations last 5...
9
My roles
Eligible roles
Active roles
Refresh
ROLE NAME
STATUS
ACTION
Security Administrator
Permanently ...
Deactivate
Global Administrator
Permanently ...
Deactivate
Privileged Role Administrator
Permanently ...
Deactivate

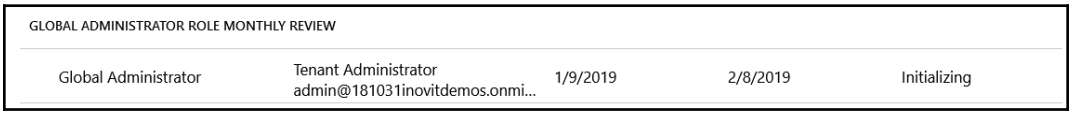

Azure AD roles - Quick start
INOVITDEMOS provided by inovit GmbH
Overview
Quick start
Tasks
My roles
My requests
Approve requests
Review access
Manage
Roles
Members
Alerts
Azure AD Privileged Identity Management
Azure AD PIM is a Premium feature that enables you to limit standing admin access to privileged roles and much more. Learn more
Assign
Assign users or current admins as eligible admins for specific Azure AD roles, so that they only have access when necessary
Assign eligibility
Activate
Activate your eligible admin roles so that you can get limit standing access to the privileged identity
Activate your role
Approve
View and approve all activation request for specific Azure AD roles that you are configured to approve
Approve requests

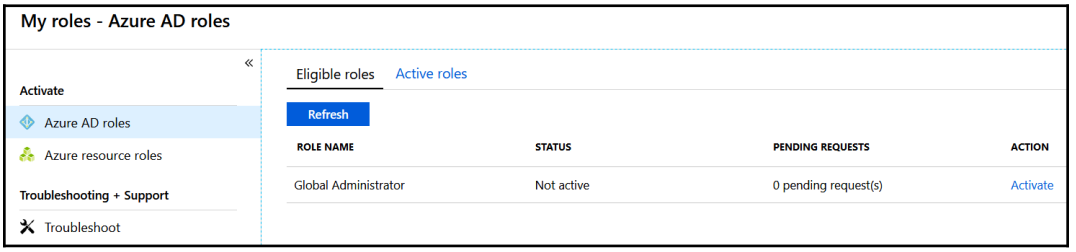

Manage
Roles
Members
Alerts
Access reviews
Directory Readers
Allows access to various read only tasks in the directory.
Directory Writers
Allows access read tasks and a subset of write tasks in the directory.
Exchange Administrator
Users with this role have global permissions within Microsoft Exchange Online
Global Administrator
Users with this role have access to all administrative features in Azure Active Directory
Guest Inviter
Users in this role can manage Azure Active Directory B2B guest user invitations when the "Members can i...

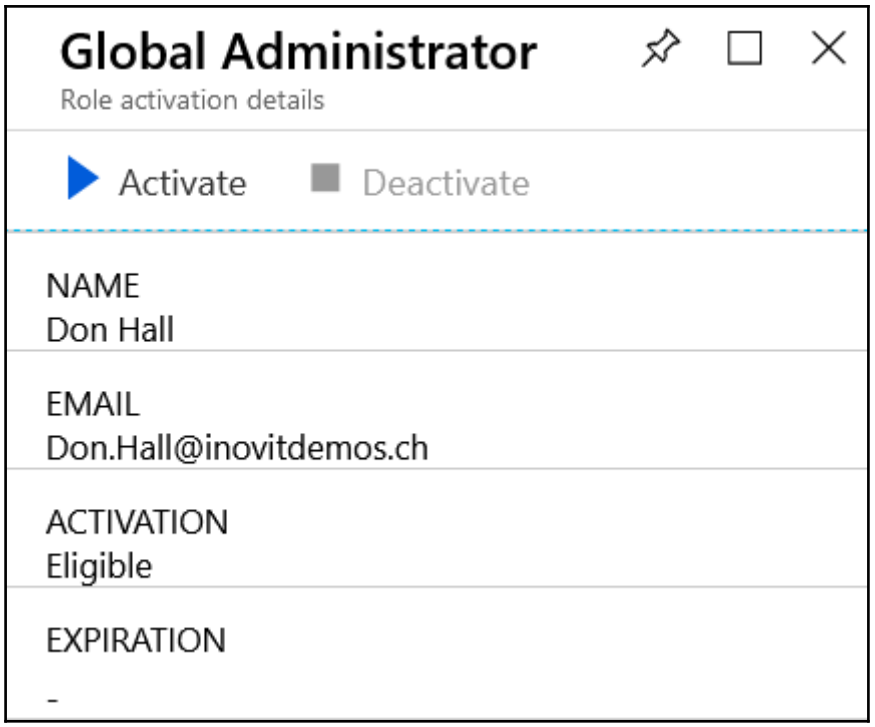

Global Administrator - Members
Manage
Members
Description
Troubleshooting + Support
Troubleshoot
New support request
Add member
Remove member
Access reviews
Export
Refresh
Assignment type
All
Search
Search by member's name
MEMBER
EMAIL
ASSIGNMENT TYPE
EXPIRATION
Jochen Nickel
jochen.nickel@inovit.ch
Permanent
Master Tenant Administrator
admin@inovit.onmicrosoft.com
Permanent
Dan Jump
Dan.Jump@inovitdemos.ch
Permanent
Tenant Administrator
admin@181031inovitdemos.on...
Permanent
Don Hall
Don.Hall@inovitdemos.ch
Permanent
Chris Gray
Chris.Gray@inovitdemos.ch
Permanent

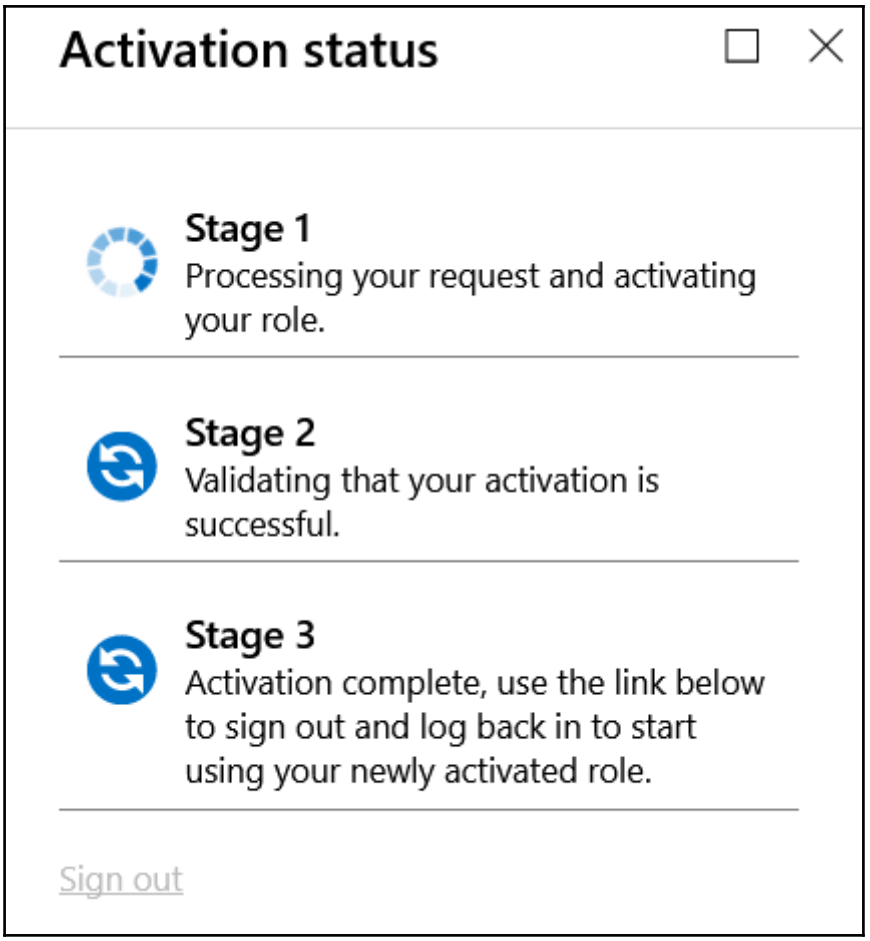

Make eligible
Make permanent
Remove


Assignment type
Eligible
Search
Search by member's name
MEMBER
EMAIL
ASSIGNMENT TYPE
Dan Jump
Dan.Jump@inovitdemos.ch
Eligible
Don Hall
Don.Hall@inovitdemos.ch
Eligible
Chris Gray
Chris.Gray@inovitdemos.ch
Eligible

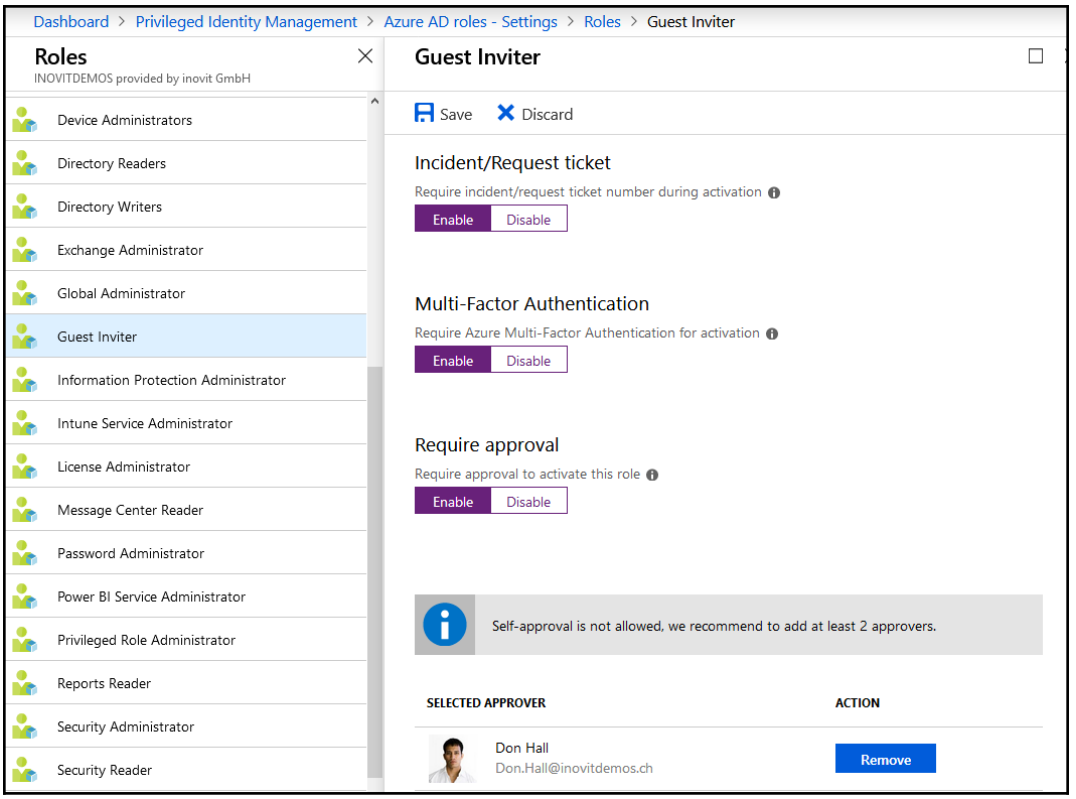

GLOBAL ADMINISTRATOR ROLE MONTHLY REVIEW
Global Administrator
Tenant Administrator
admin@181031inovitdemos.onmi...
1/9/2019
2/8/2019
Initializing

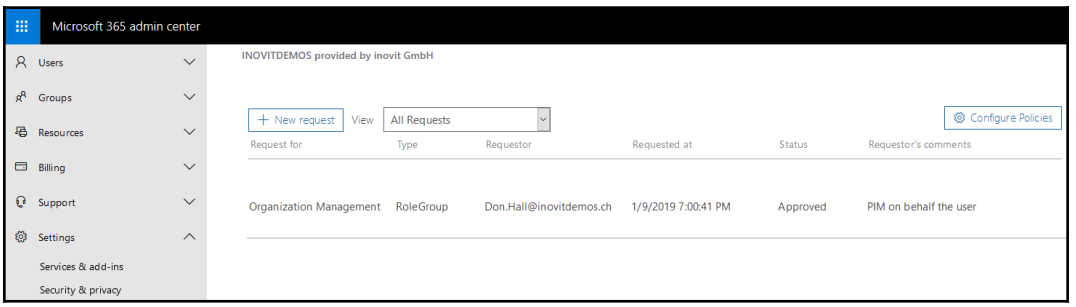

My roles - Azure AD roles
Activate
Azure AD roles
Azure resource roles
Troubleshooting + Support
Troubleshoot
Eligible roles
Active roles
Refresh
ROLE NAME
STATUS
PENDING REQUESTS
ACTION
Global Administrator
Not active
0 pending request(s)
Activate


Global Administrator
Role activation details
Activate
Deactivate
NAME
Don Hall
EMAIL
Don.Hall@inovitdemos.ch
ACTIVATION
Eligible
EXPIRATION
-

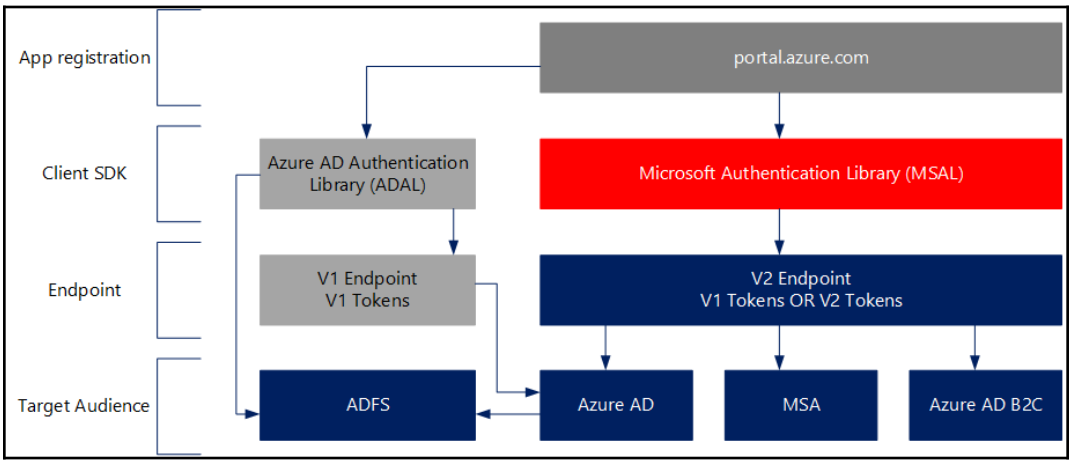

Activation status
Stage 1
Processing your request and activating your role.
Stage 2
Validating that your activation is successful.
Stage 3
Activation complete, use the link below to sign out and log back in to start using your newly activated role.
Sign out

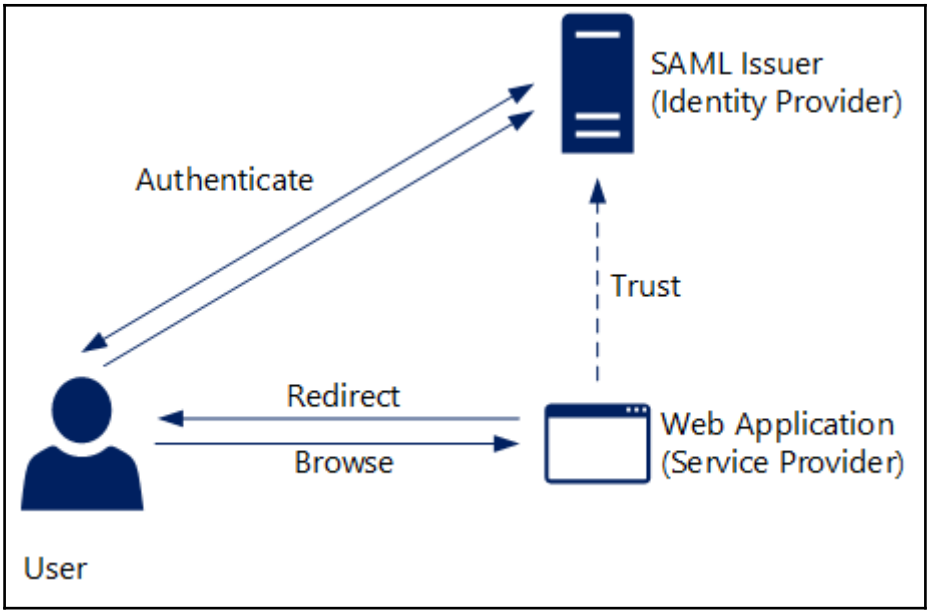

Activation history
6
5
4
3
2
1
0
7 PM
7:15 PM
7:30 PM
7:45 PM
8 PM
SECURITY AD...
PRIVILEGED R...
SERVICE AD...
GLOBAL AD...
Total
10 Activations
Max
10 Activations per day
Average
10 Activations per day
Sort:
Time
Action
Role
TIME
REQUESTOR
ACTION
MEMBER
ROLE
REASONING
EXPIRATION
1/9/2019, 8:00:42 PM
Don Hall
Activate
Don Hall
Don.Hall@inovitdemos.ch
Global Administrator
First try with PIM
1/9/2019, 9:00:42 P...
1/9/2019, 8:00:11 PM
Don Hall
Activation requested
Don Hall
Don.Hall@inovitdemos.ch
Global Administrator
First try with PIM
-
1/9/2019, 7:46:15 PM
Tenant Administrator
Create access review
-
Global Administrator
Access review created. Review Name...
-

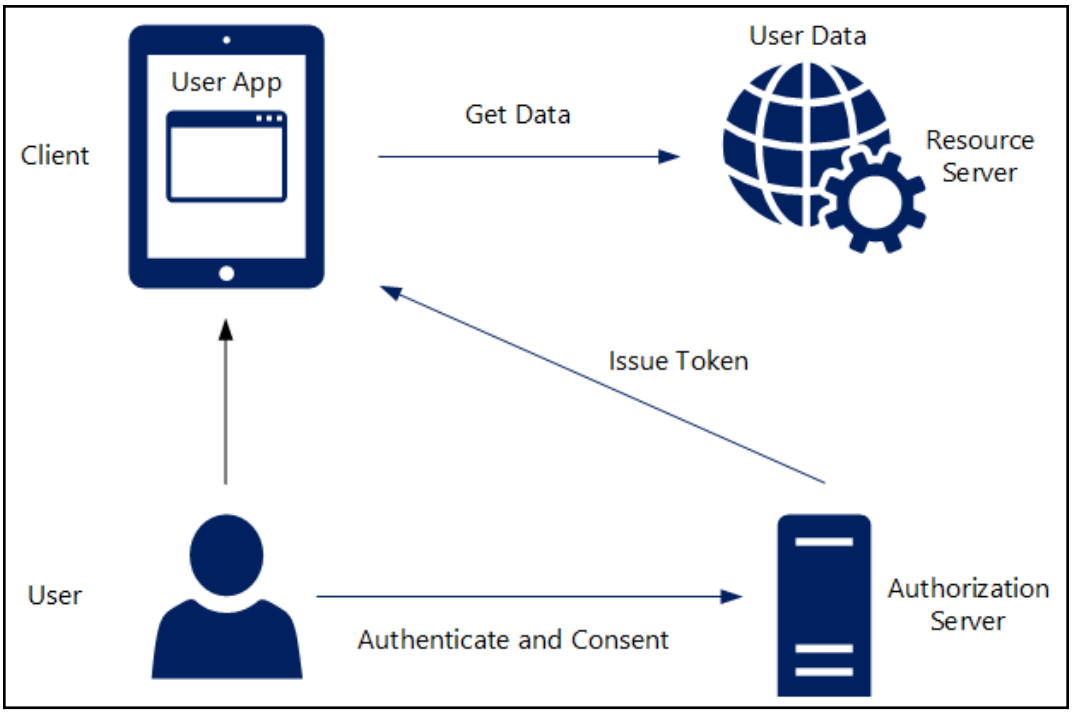

Dashboard > Privileged Identity Management > Azure AD roles - Settings > Roles > Guest Inviter
Roles
INOVITDEMOS provided by inovit GmbH
Device Administrators
Directory Readers
Directory Writers
Exchange Administrator
Global Administrator
Guest Inviter
Information Protection Administrator
Intune Service Administrator
License Administrator
Message Center Reader
Password Administrator
Power BI Service Administrator
Privileged Role Administrator
Reports Reader
Security Administrator
Security Reader
Guest Inviter
Save
Discard
Incident/Request ticket
Require incident/request ticket number during activation
Enable
Disable
Multi-Factor Authentication
Require Azure Multi-Factor Authentication for activation
Enable
Disable
Require approval
Require approval to activate this role
Enable
Disable
Self-approval is not allowed, we recommend to add at least 2 approvers.
SELECTED APPROVER
ACTION
Don Hall
Don.Hall@inovitdemos.ch
Remove

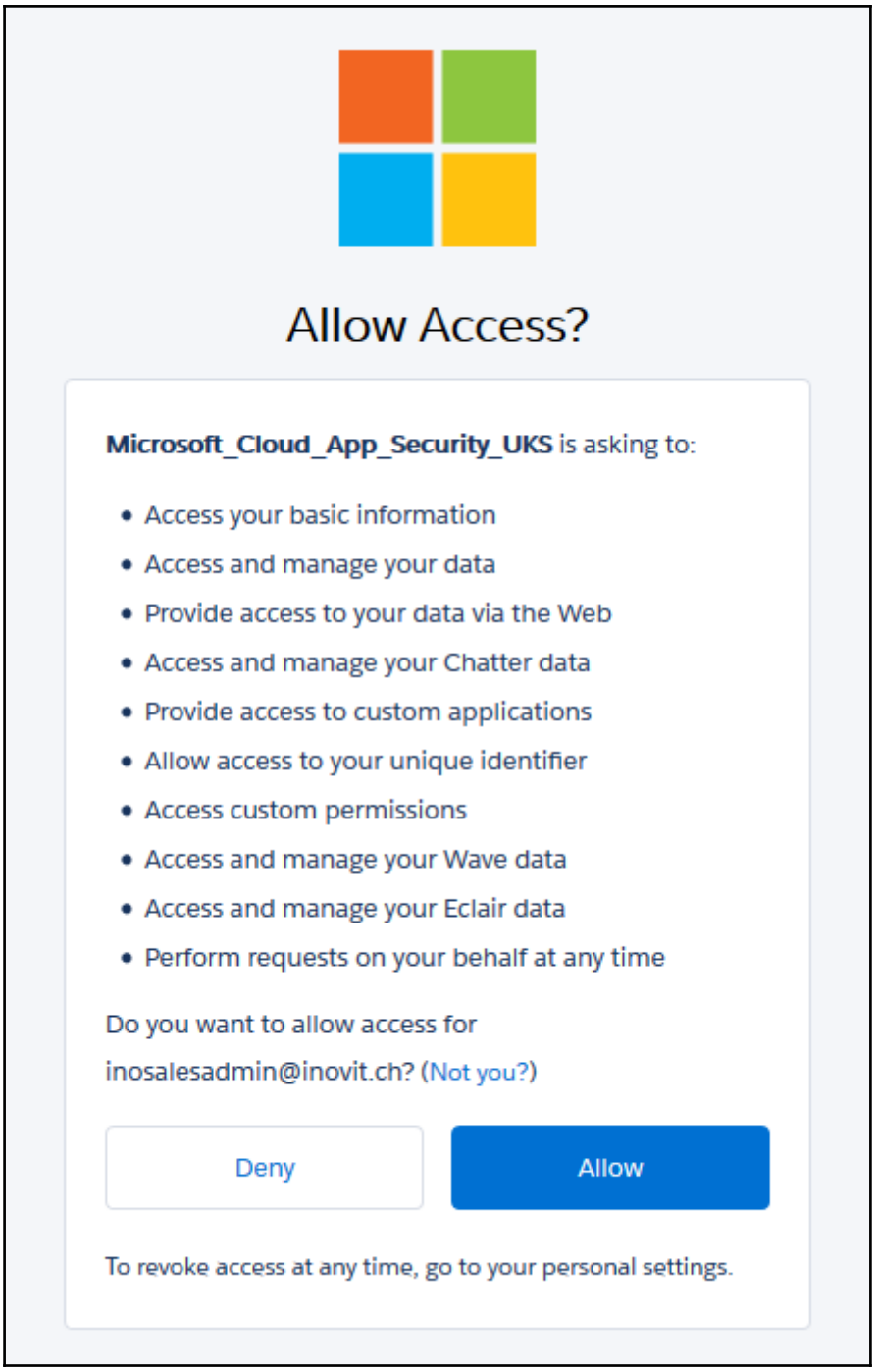

Microsoft 365 admin center
Users
Groups
Resources
Billing
Support
Settings
Services & add-ins
Security & privacy
INOVITDEMOS provided by inovit GmbH
New request
View
All Requests
Configure Policies
Request for
Type
Requestor
Requested at
Status
Requestor's comments
Organization Management
RoleGroup
Don.Hall@inovitdemos.ch
1/9/2019 7:00:41 PM
Approved
PIM on behalf the user

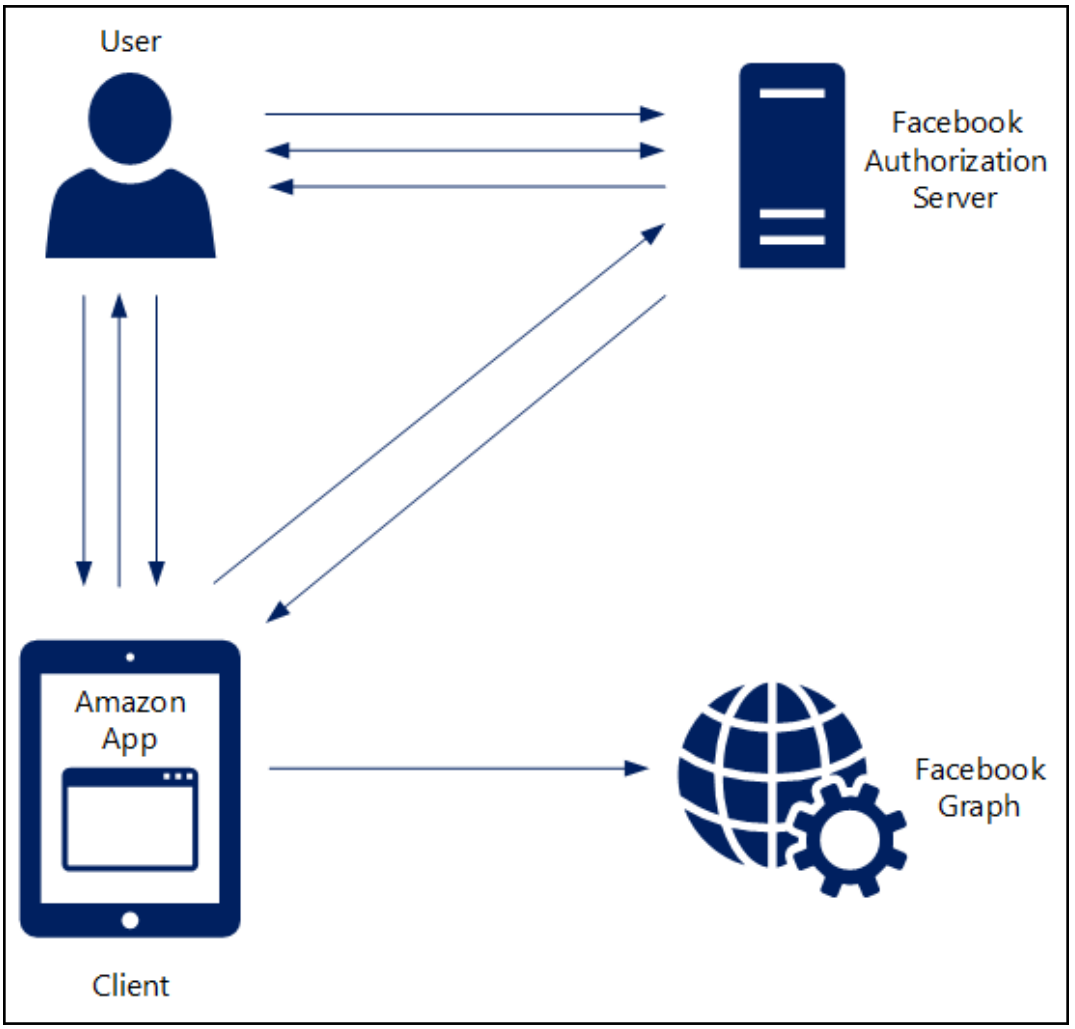
Chapter 6: Managing Authentication Protocols

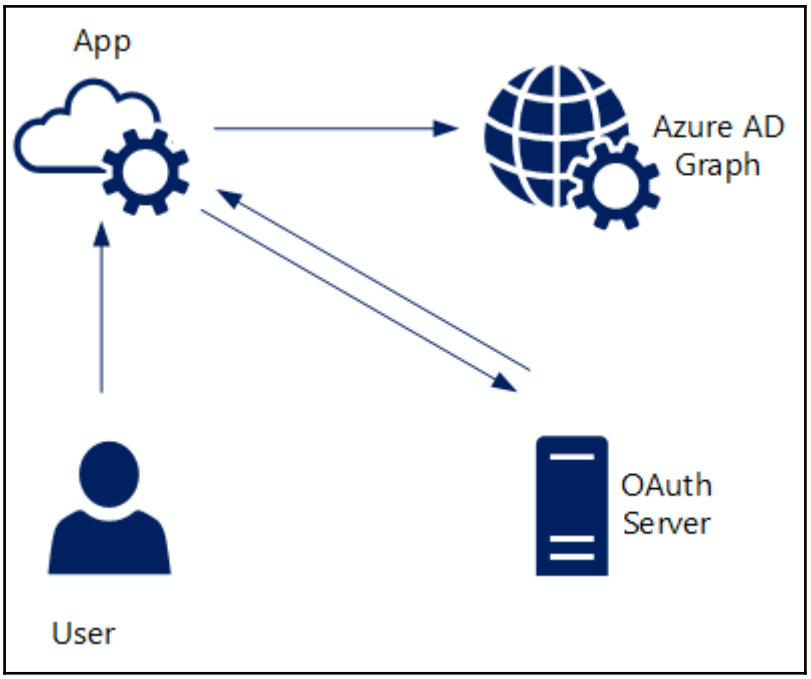


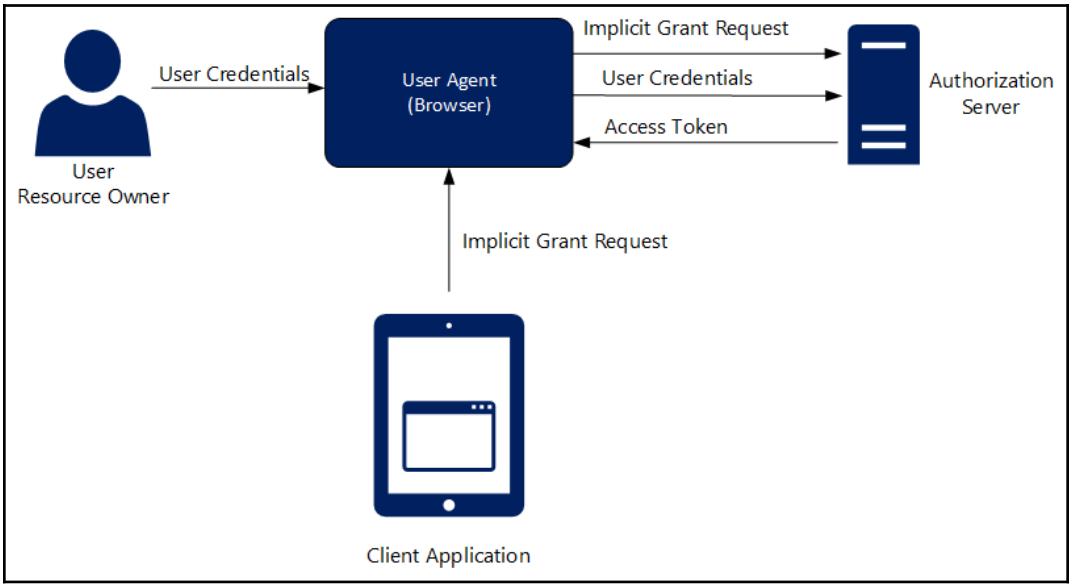


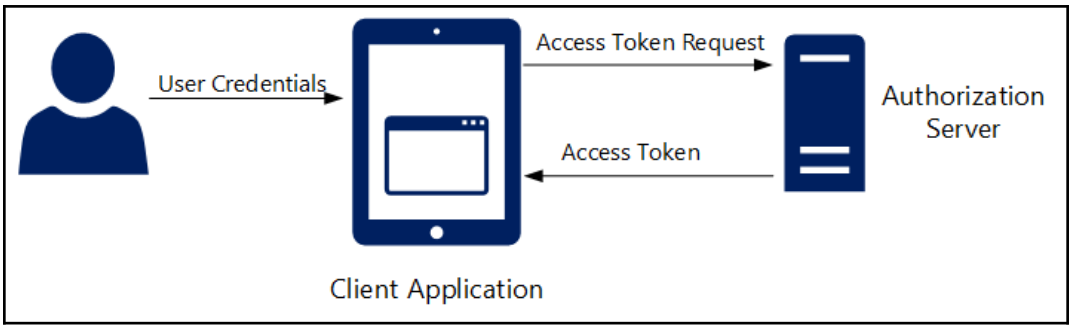

User Data
User App
Get Data
Client
Resource
Server
Issue Token
User
Authorization
Server
Authenticate and Consent

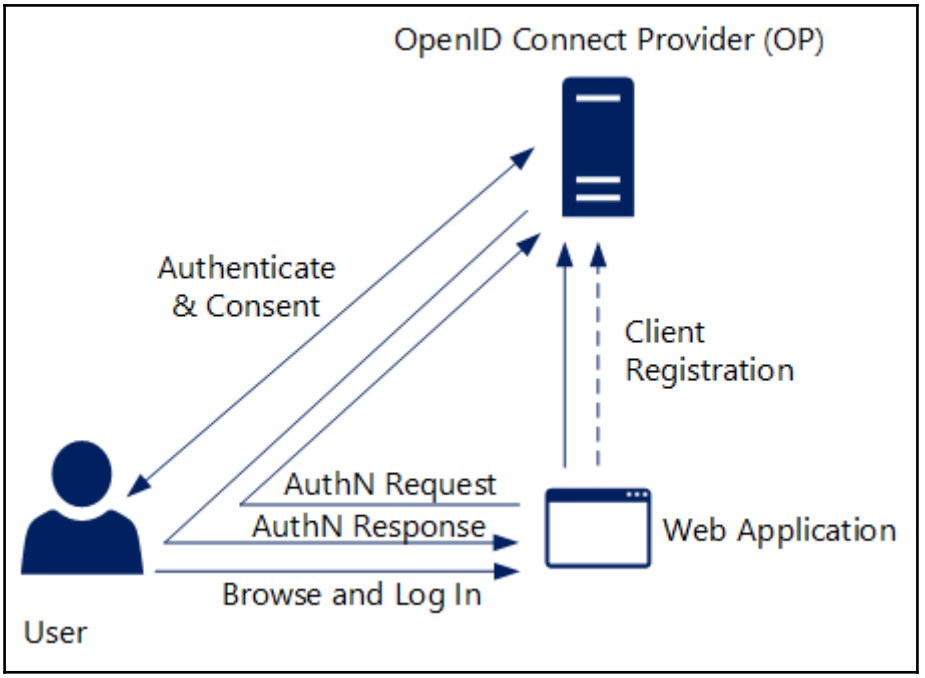

Allow Access?
Microsoft_Cloud_App_Security_UKS is asking to:
Access your basic information
Access and manage your data
Provide access to your data via the Web
Access and manage your Chatter data
Provide access to custom applications
Allow access to your unique identifier
Access custom permissions
Access and manage your Wave data
Access and manage your Eclair data
Perform requests on your behalf at any time
Do you want to allow access for inosalesadmin@inovit.ch? (Not you?)
Deny
Allow
To revoke access at any time, go to your personal settings.

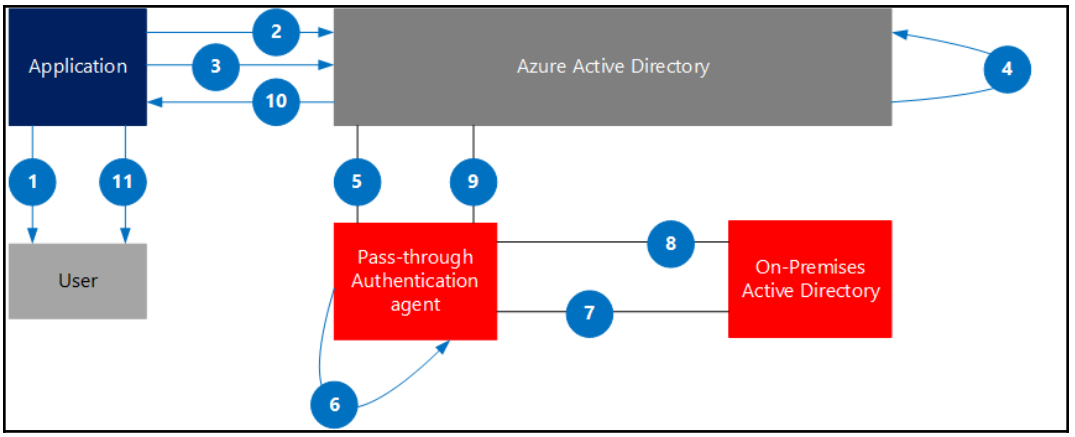

User
Facebook
Authorization
Server
Amazon
App
Client
Facebook
Graph


App
Azure AD
Graph
OAuth
Server
User

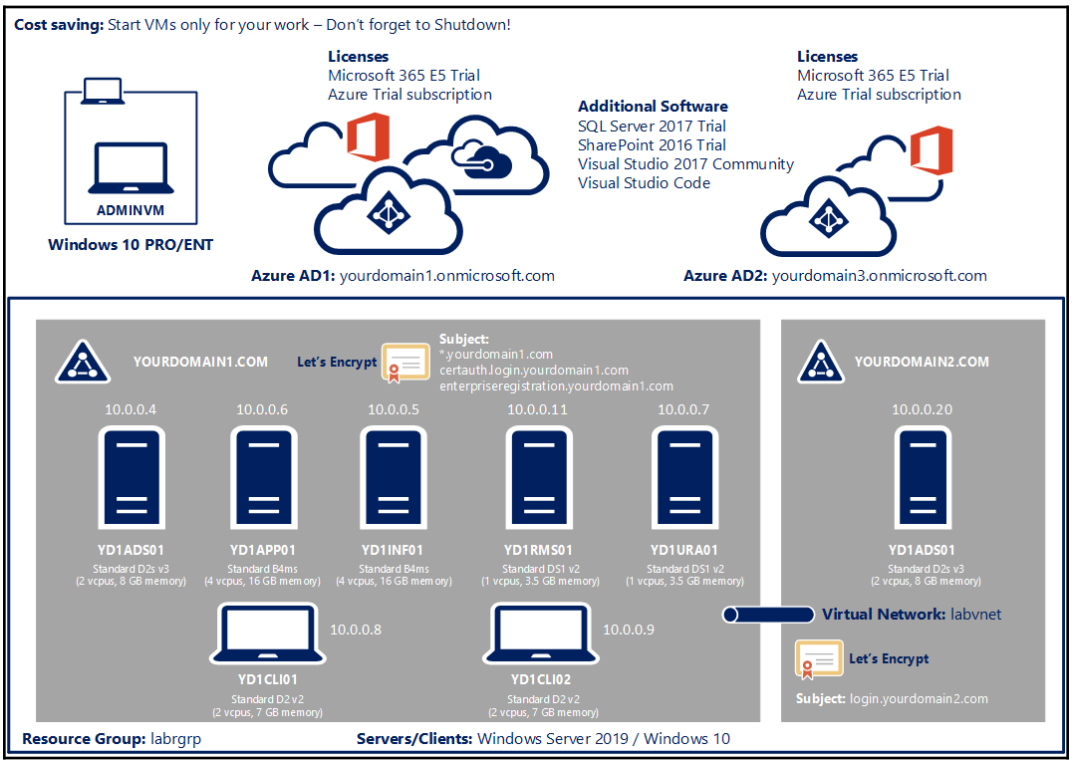

User Credentials
User Agent
(Browser)
Implicit Grant Request
User Credentials
Access Token
Authorization
Server
User
Resource Owner
Implicit Grant Request
Client Application


User Credentials
Access Token Request
Access Token
Authorization Server
Client Application

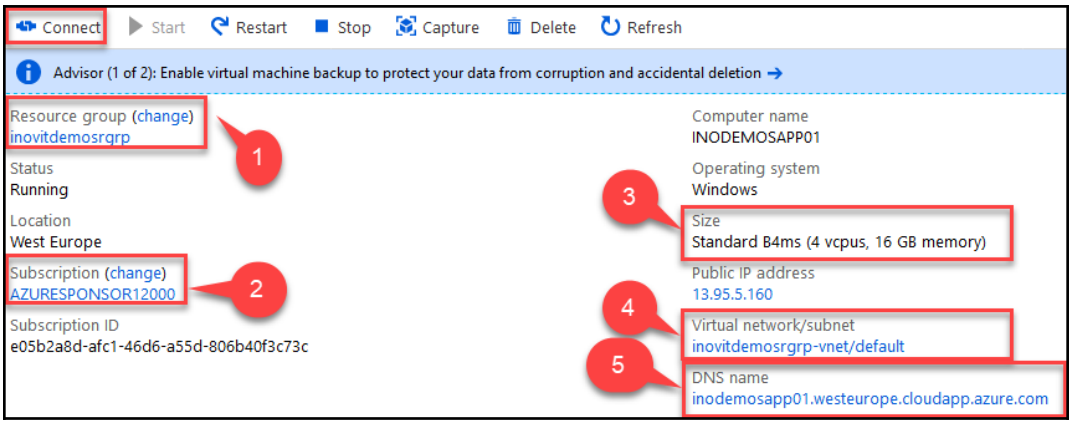

OpenID Connect Provider (OP)
Authenticate & Consent
Client Registration
AuthN Request
AuthN Response
Web Application
Browse and Log In
User

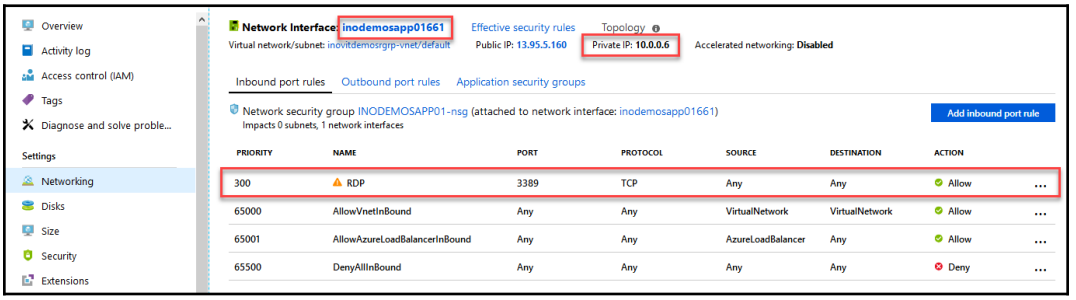

Application
2
3
10
Azure Active Directory
4
1
11
5
9
User
Pass-through Authentication agent
8
On-Premises Active Directory
7
6

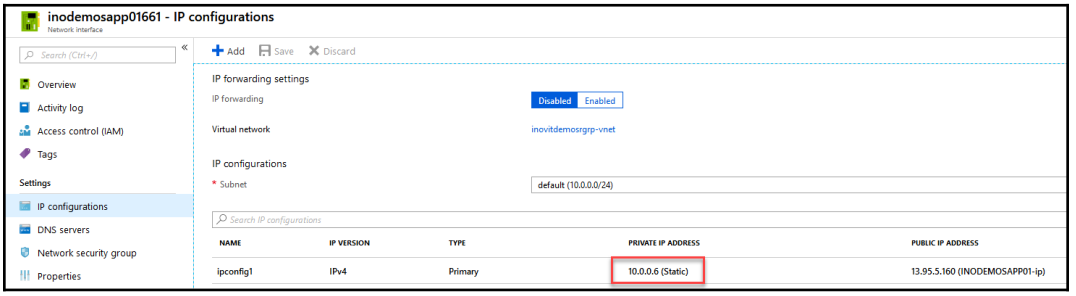
Chapter 7: Deploying Solutions on Azure AD and ADFS

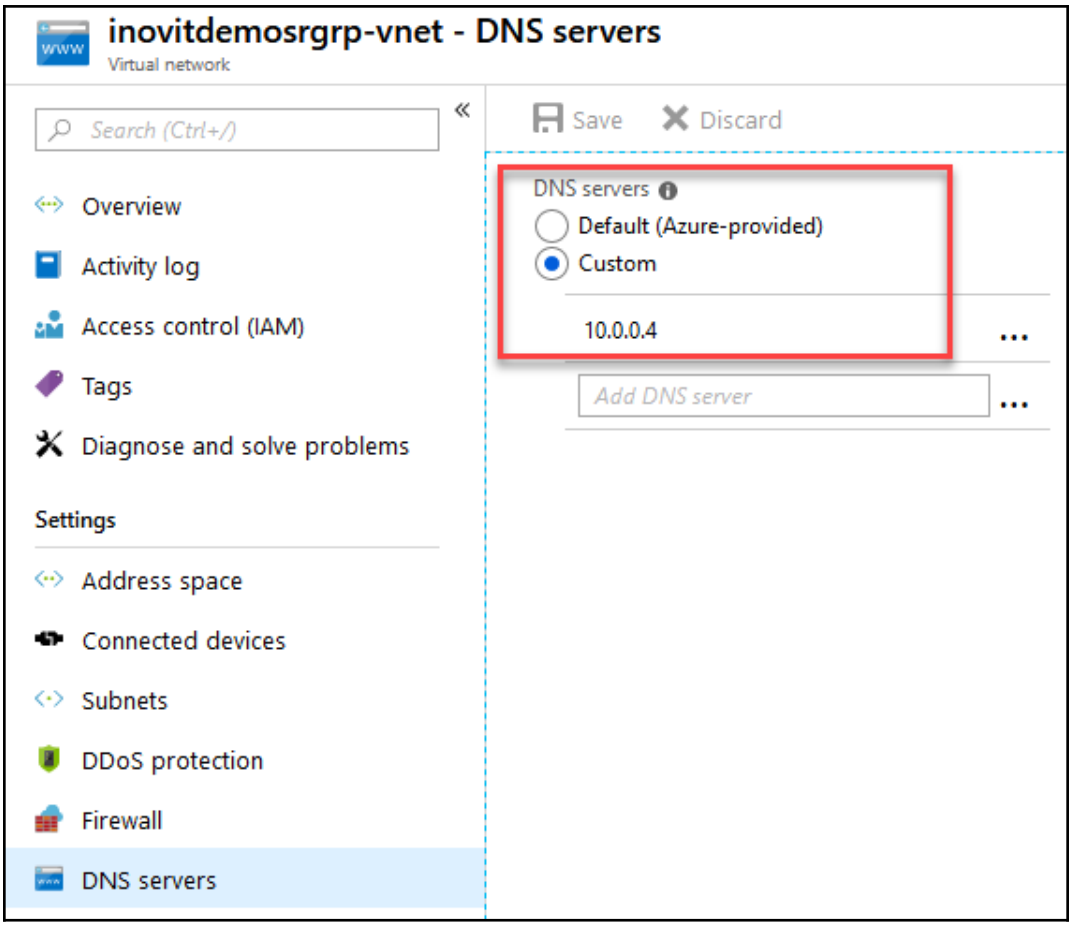


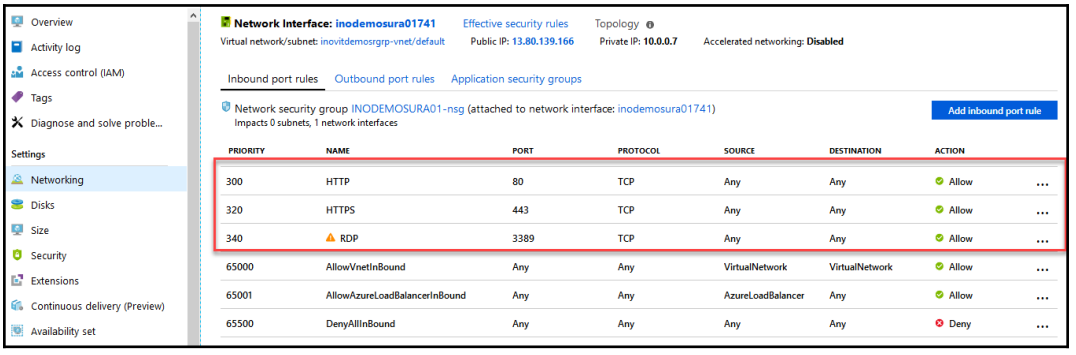
INOAZUREIDADS01	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000
INODEMOSADS01	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000
INODEMOSAPP01	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000
INODEMOSCLI01	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000
INODEMOSCLI02	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000
INODEMOSINF01	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000
INODEMOSRMS01	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000
INODEMOSURA01	Running	inovitdemosrgrp	West Europe	AZURESPONSOR12000


Connect
Start
Restart
Stop
Capture
Delete
Refresh
Advisor (1 of 2): Enable virtual machine backup to protect your data from corruption and accidental deletion
Resource group (change)
inovitdemosrgrp
1
Status
Running
Location
West Europe
Subscription (change)
AZURESPONSOR12000
2
Subscription ID
e05b2a8d-afc1-46d6-a55d-806b40f3c73c
Computer name
INODEMOSAPP01
Operating system
Windows
3
Size
Standard B4ms (4 vcpus, 16 GB memory)
Public IP address
13.95.5.160
4
Virtual network/subnet
inovitdemosrgrp-vnet/default
5
DNS name
inodemosapp01.westeurope.cloudapp.azure.com


Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve proble...
Settings
Networking
Disks
Size
Security
Extensions
Network Interface: inodemosapp01661
Effective security rules
Topology
Virtual network/subnet: inovitdemosrgrp-vnet/default
Public IP: 13.95.5.160
Private IP: 10.0.0.6
Accelerated networking: Disabled
Inbound port rules
Outbound port rules
Application security groups
Network security group INODEMOSAPP01-nsg (attached to network interface: inodemosapp01661)
Impacts 0 subnets, 1 network interfaces
Add inbound port rule
PRIORITY
NAME
PORT
PROTOCOL
SOURCE
DESTINATION
ACTION
300
RDP
3389
TCP
Any
Any
Allow
65000
AllowVnetInBound
Any
Any
VirtualNetwork
VirtualNetwork
Allow
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
Any
Allow
65500
DenyAllInBound
Any
Any
Any
Any
Deny


inodemosapp01661 - IP configurations
Network interface
Search (Ctrl+/)
Add
Save
Discard
Overview
Activity log
Access control (IAM)
Tags
Settings
IP configurations
DNS servers
Network security group
Properties
IP forwarding settings
IP forwarding
Disabled
Enabled
Virtual network
inovitdemosrgrp-vnet
IP configurations
* Subnet
default (10.0.0.0/24)
Search IP configurations
NAME
IP VERSION
TYPE
PRIVATE IP ADDRESS
PUBLIC IP ADDRESS
ipconfig1
IPv4
Primary
10.0.0.6 (Static)
13.95.5.160 (INODEMOSAPP01-ip)


inovitdemosrgrp-vnet - DNS servers
Virtual network
Search (Ctrl+/)
Save
Discard
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
DDoS protection
Firewall
DNS servers
DNS servers
Default (Azure-provided)
Custom
10.0.0.4
Add DNS server

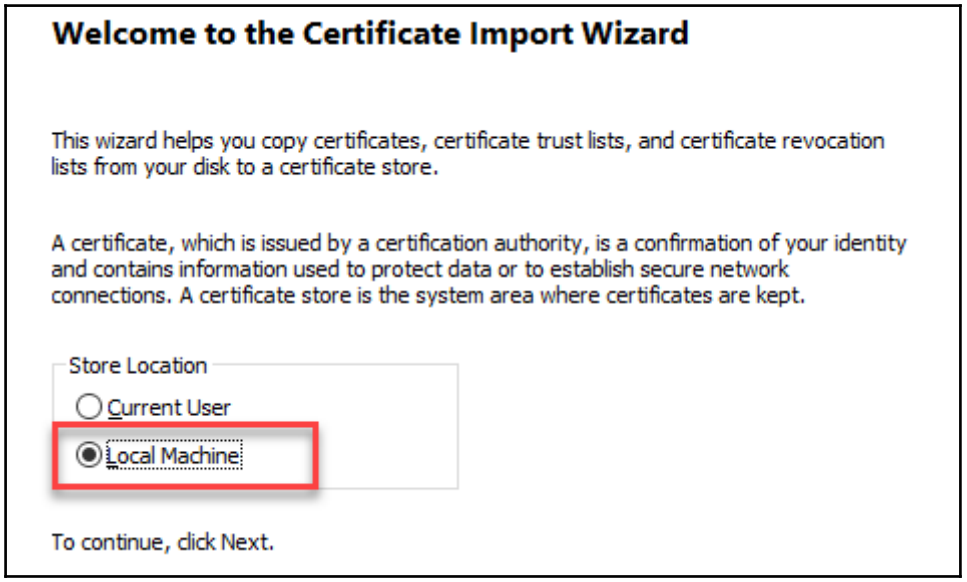

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve proble...
Settings
Networking
Disks
Size
Security
Extensions
Continuous delivery (Preview)
Availability set
Network Interface: inodemosura01741
Effective security rules
Topology
Virtual network/subnet: inovitdemosrgrp-vnet/default
Public IP: 13.80.139.166
Private IP: 10.0.0.7
Accelerated networking: Disabled
Inbound port rules
Outbound port rules
Application security groups
Network security group INODEMOSURA01-nsg (attached to network interface: inodemosura01741)
Impacts 0 subnets, 1 network interfaces
Add inbound port rule
PRIORITY NAME PORT PROTOCOL SOURCE DESTINATION ACTION
300 HTTP 80 TCP Any Any Allow
320 HTTPS 443 TCP Any Any Allow
340 RDP 3389 TCP Any Any Allow
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowAzureLoadBalancerInBound Any Any AzureLoadBalancer Any Allow
65500 DenyAllInBound Any Any Any Any Deny

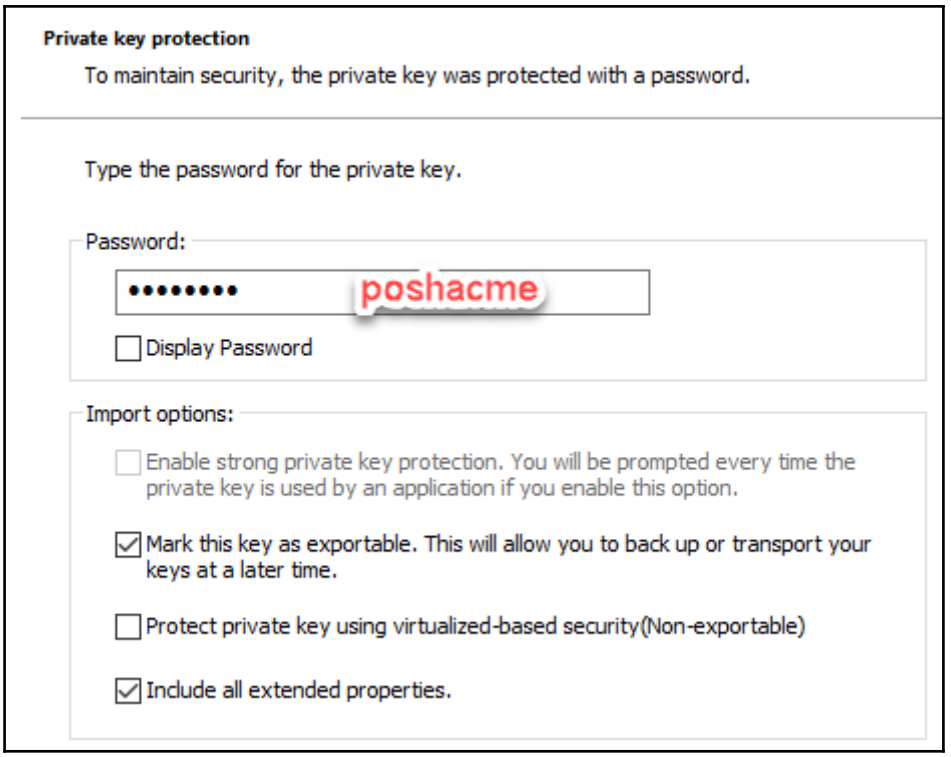
```
Please create the following TXT records:
----------------------------------------
_acme-challenge.inovitdemos.ch -> OtORHpZ1CruSu2Tb-iZ1oSnU7oMOsiT0fMPq8pDDeVM
_acme-challenge.certauth.login.inovitdemos.ch -> 5je--CO7tiMYFXdclcFQKu9UwxnbQTVuzV4U8xpIBQs
----------------------------------------
```

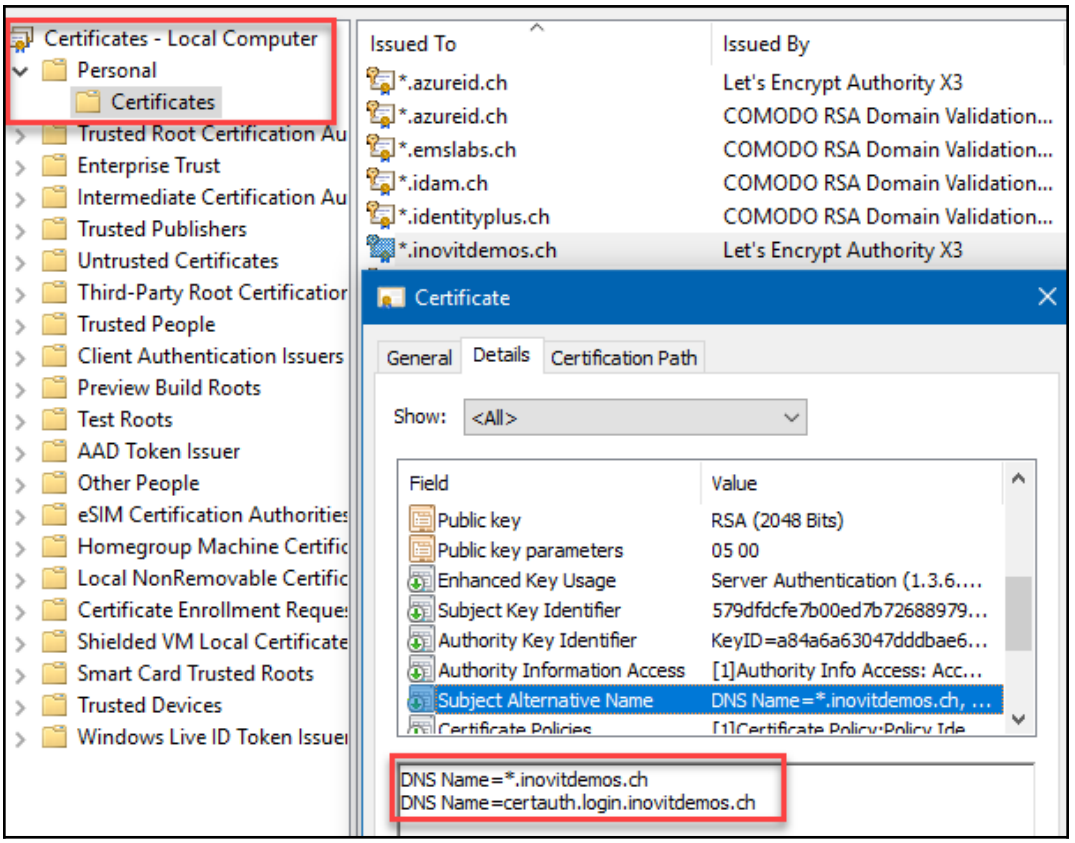
```
Please remove the following TXT records:
----------------------------------------
_acme-challenge.inovitdemos.ch -> OtORHpZ1CruSu2Tb-iZ1oSnU7oMOsiT0fMPq8pDDeVM
_acme-challenge.certauth.login.inovitdemos.ch -> 5je--CO7tiMYFXdclcFQKu9UwxnbQTVuzV4U8xpIBQs
----------------------------------------
```

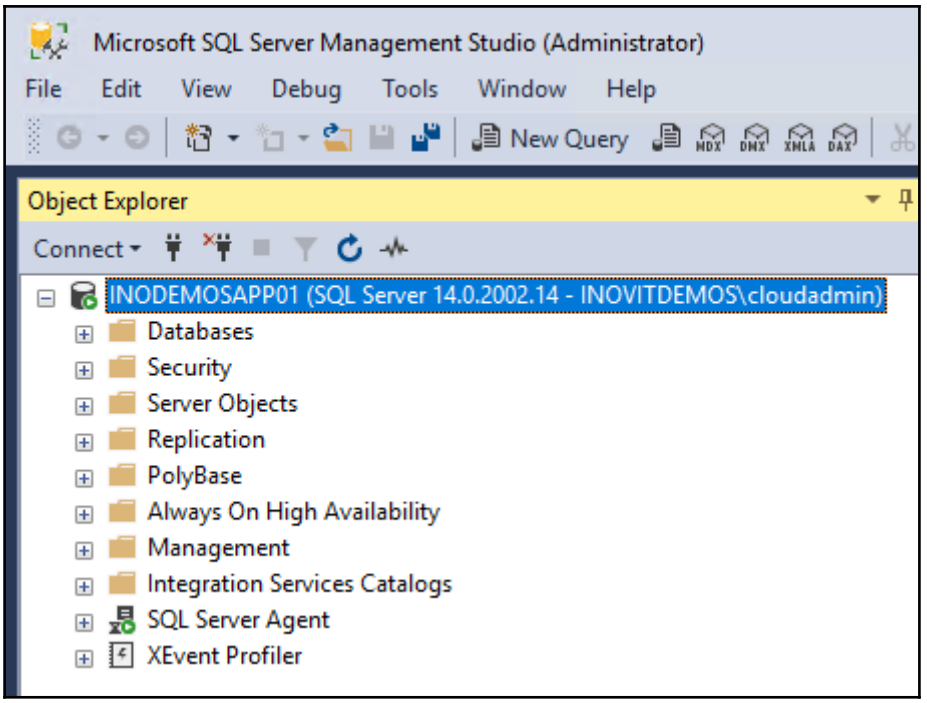
```
Subject            NotAfter              KeyLength Thumbprint                              AllSANs
-------            --------              --------- ----------                              -------
CN=*.inovitdemos.ch 4/12/2019 3:45:09 PM 2048      B7440A0C8D7BADB3E740BE01F18A461E411FAB3D {*.inovitdemos.ch, certauth.login.inovitdemos.ch}
```

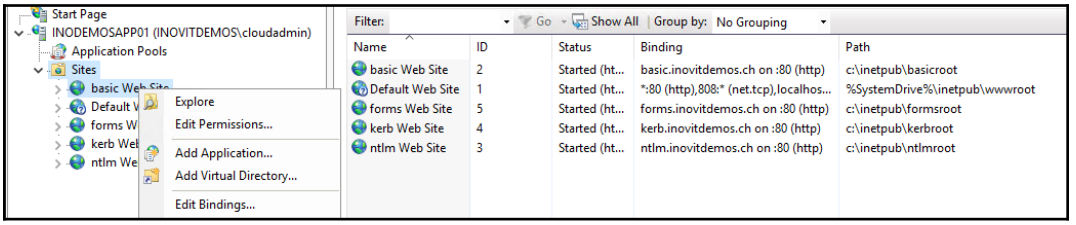
```
Subject      : CN=*.inovitdemos.ch
NotBefore    : 1/12/2019 2:45:09 PM
NotAfter     : 4/12/2019 3:45:09 PM
KeyLength    : 2048
Thumbprint   : B7440A0C8D7BADB3E740BE01F18A461E411FAB3D
AllSANs      : {*.inovitdemos.ch, certauth.login.inovitdemos.ch}
CertFile     : C:\Users\jochen.nickel\AppData\Local\Posh-ACME\acme-v02.api.letsencrypt.org\49385785\!.inovitdemos.ch\cert.cer
KeyFile      : C:\Users\jochen.nickel\AppData\Local\Posh-ACME\acme-v02.api.letsencrypt.org\49385785\!.inovitdemos.ch\cert.key
ChainFile    : C:\Users\jochen.nickel\AppData\Local\Posh-ACME\acme-v02.api.letsencrypt.org\49385785\!.inovitdemos.ch\chain.cer
FullChainFile : C:\Users\jochen.nickel\AppData\Local\Posh-ACME\acme-v02.api.letsencrypt.org\49385785\!.inovitdemos.ch\fullchain.cer
PfxFile      : C:\Users\jochen.nickel\AppData\Local\Posh-ACME\acme-v02.api.letsencrypt.org\49385785\!.inovitdemos.ch\cert.pfx
PfxFullChain : C:\Users\jochen.nickel\AppData\Local\Posh-ACME\acme-v02.api.letsencrypt.org\49385785\!.inovitdemos.ch\fullchain.pfx
PfxPass      : System.Security.SecureString
```

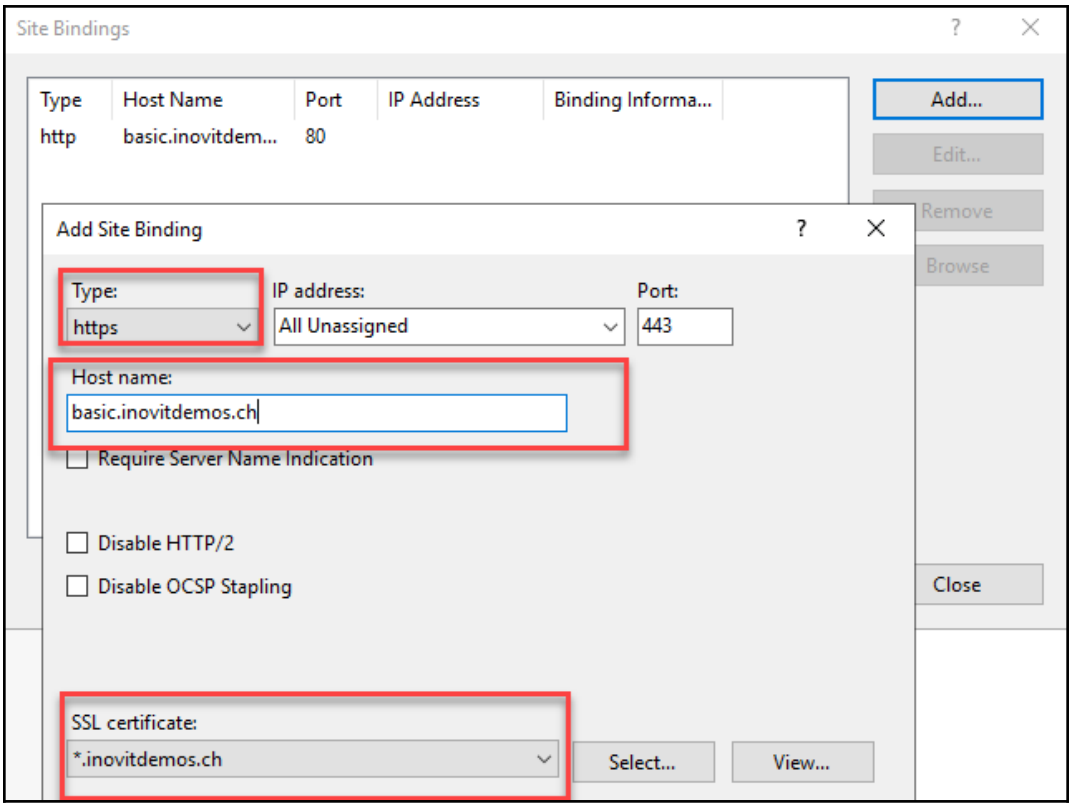


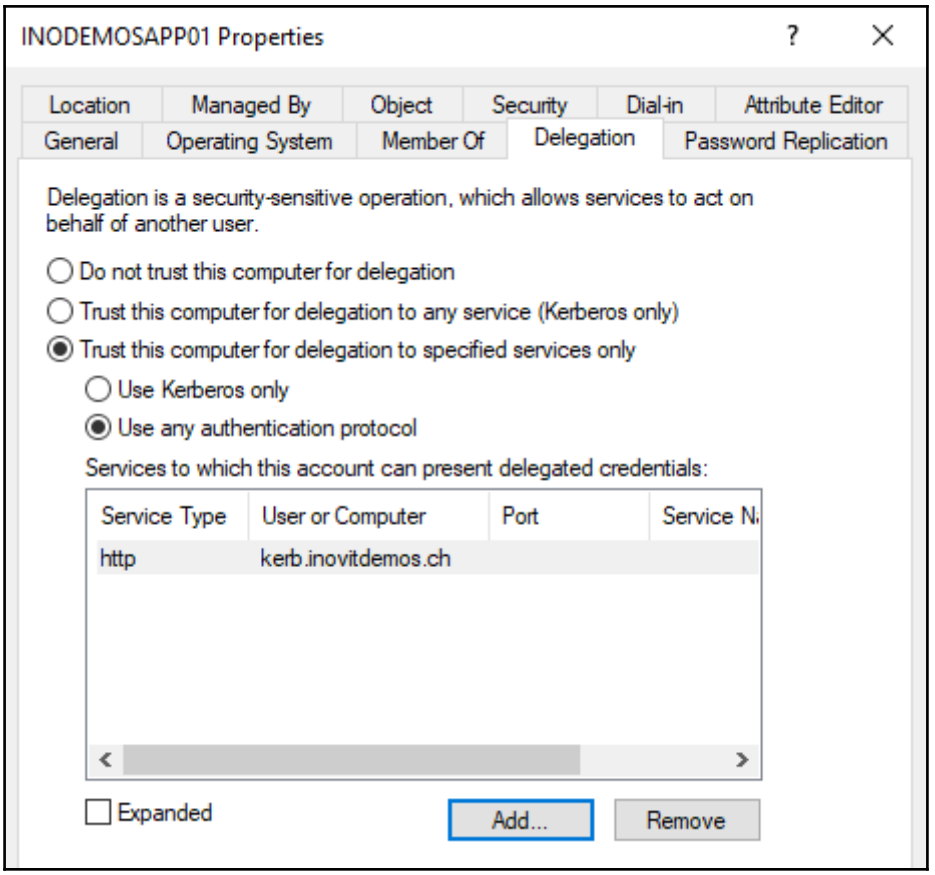

Private key protection
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
••••••••
poshacme
Display Password
Import options:
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
Protect private key using virtualized-based security(Non-exportable)
Include all extended properties.

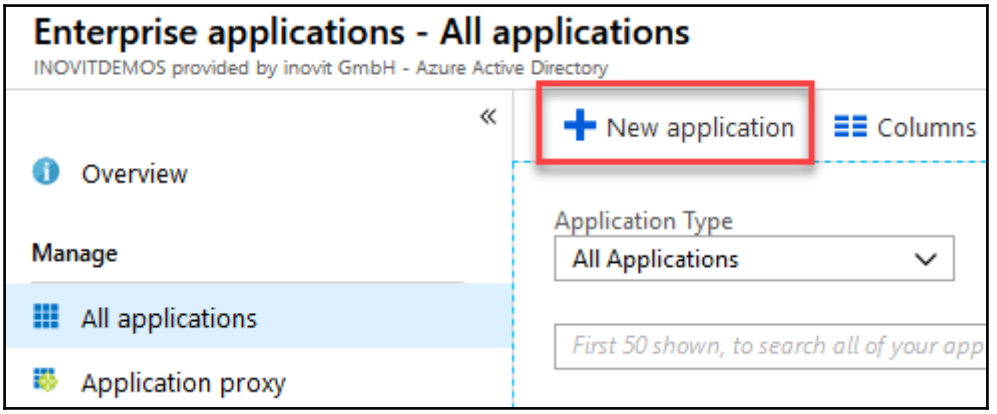

Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Preview Build Roots
Test Roots
AAD Token Issuer
Other People
eSIM Certification Authorities
Homegroup Machine Certific
Local NonRemovable Certific
Certificate Enrollment Reque
Shielded VM Local Certificate
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issue
Issued To
Issued By
*.azureid.ch
Let's Encrypt Authority X3
*.azureid.ch
COMODO RSA Domain Validation...
*.emslabs.ch
COMODO RSA Domain Validation...
*.idam.ch
COMODO RSA Domain Validation...
*.identityplus.ch
COMODO RSA Domain Validation...
*.inovitdemos.ch
Let's Encrypt Authority X3
Certificate
General
Details
Certification Path
Show:
<All>
Field
Value
Public key
RSA (2048 Bits)
Public key parameters
05 00
Enhanced Key Usage
Server Authentication (1.3.6....
Subject Key Identifier
579dfdcfe7b00ed7b72688979...
Authority Key Identifier
KeyID=a84a6a63047dddbae6...
Authority Information Access
[1]Authority Info Access: Acc...
Subject Alternative Name
DNS Name=*.inovitdemos.ch, ...
DNS Name=*.inovitdemos.ch
DNS Name=certauth.login.inovitdemos.ch

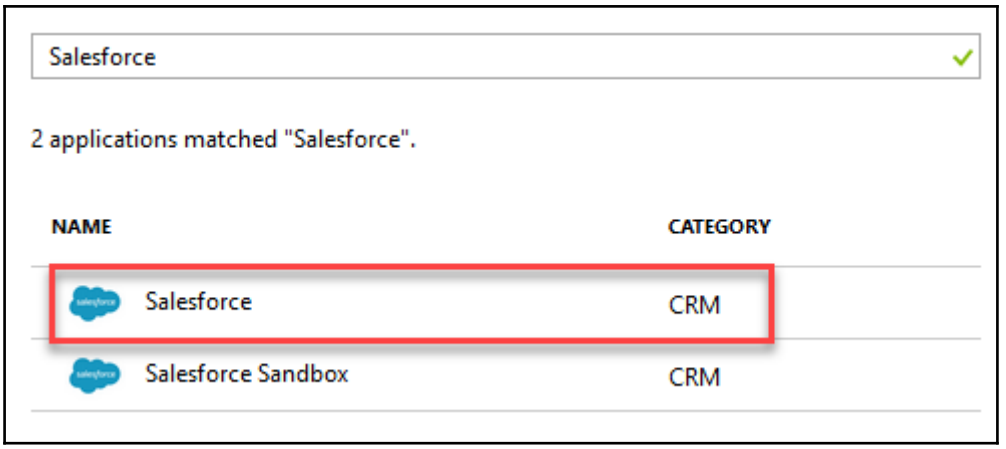

Microsoft SQL Server Management Studio (Administrator)
File
Edit
View
Debug
Tools
Window
Help
New Query
Object Explorer
Connect
INODEMOSAPP01 (SQL Server 14.0.2002.14 - INOVITDEMOS\cloudadmin)
Databases
Security
Server Objects
Replication
PolyBase
Always On High Availability
Management
Integration Services Catalogs
SQL Server Agent
XEvent Profiler

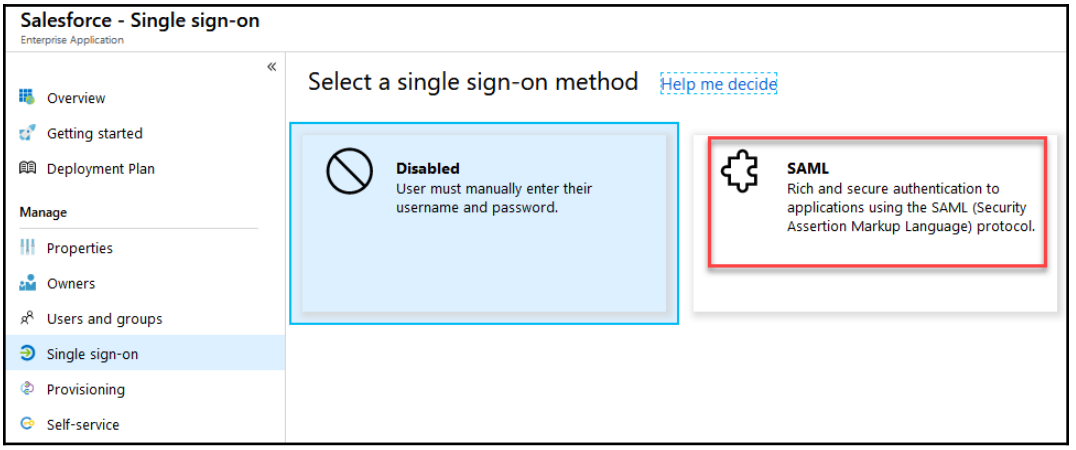

Start Page
INODEMOSAPP01 (INOVITDEMOS\cloudadmin)
Application Pools
Sites
Explore
Edit Permissions...
Add Application...
Add Virtual Directory...
Edit Bindings...
Filter:
Go
Show All
Group by:
No Grouping
Name
ID
Status
Binding
Path
basic Web Site
2
Started (ht...
basic.inovitdemos.ch on :80 (http)
c:\inetpub\basicroot
Default Web Site
1
Started (ht...
:80 (http),808: (net.tcp),localhos...
%SystemDrive%\inetpub\wwwroot
forms Web Site
5
Started (ht...
forms.inovitdemos.ch on :80 (http)
c:\inetpub\formsroot
kerb Web Site
4
Started (ht...
kerb.inovitdemos.ch on :80 (http)
c:\inetpub\kerbroot
ntlm Web Site
3
Started (ht...
ntlm.inovitdemos.ch on :80 (http)
c:\inetpub\ntlmroot


Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
http
basic.inovitdem...
80
Add...
Edit...
Remove
Browse
Close
Add Site Binding
Type:
https
IP address:
All Unassigned
Port:
443
Host name:
basic.inovitdemos.ch
Require Server Name Indication
Disable HTTP/2
Disable OCSP Stapling
SSL certificate:
*.inovitdemos.ch
Select...
View...

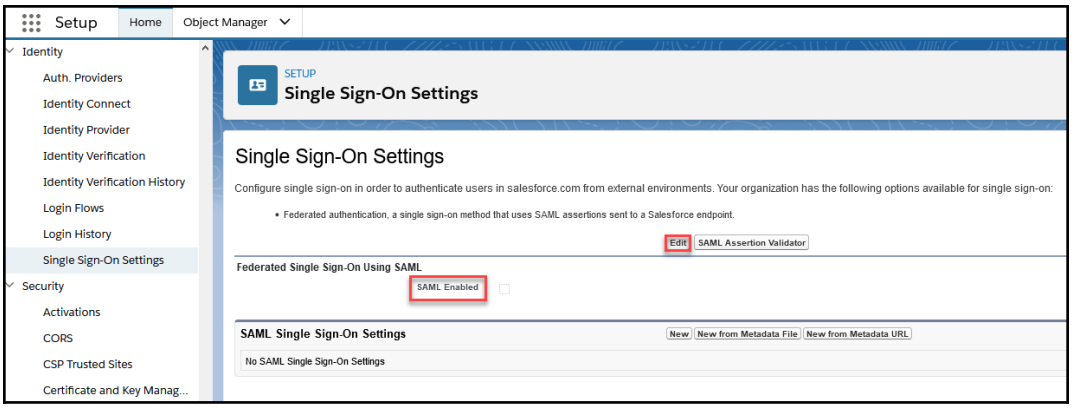

INODEMOSAPP01 Properties
Location
Managed By
Object
Security
Dial-in
Attribute Editor
General
Operating System
Member Of
Delegation
Password Replication
Delegation is a security-sensitive operation, which allows services to act on behalf of another user.
Do not trust this computer for delegation
Trust this computer for delegation to any service (Kerberos only)
Trust this computer for delegation to specified services only
Use Kerberos only
Use any authentication protocol
Services to which this account can present delegated credentials:
Service Type
User or Computer
Port
Service N
http
kerb.inovitdemos.ch
Expanded
Add...
Remove

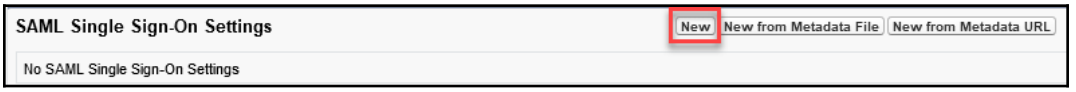

Enterprise applications - All applications
INOVITDEMOS provided by inovit GmbH - Azure Active Directory
New application
Columns
Overview
Manage
All applications
Application proxy
Application Type
All Applications
First 50 shown, to search all of your app

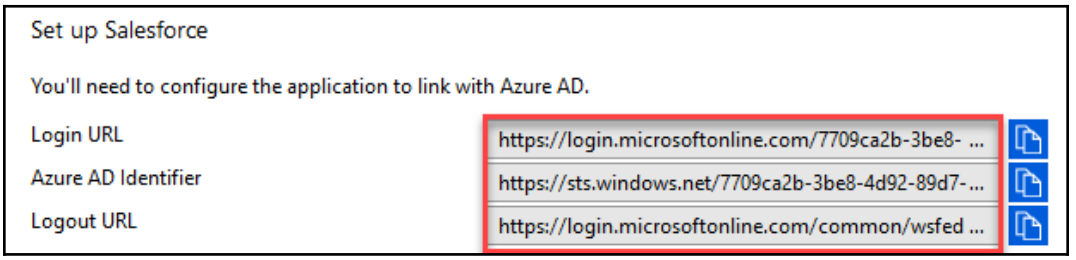

Salesforce
2 applications matched "Salesforce".
NAME
CATEGORY
Salesforce
CRM
Salesforce Sandbox
CRM

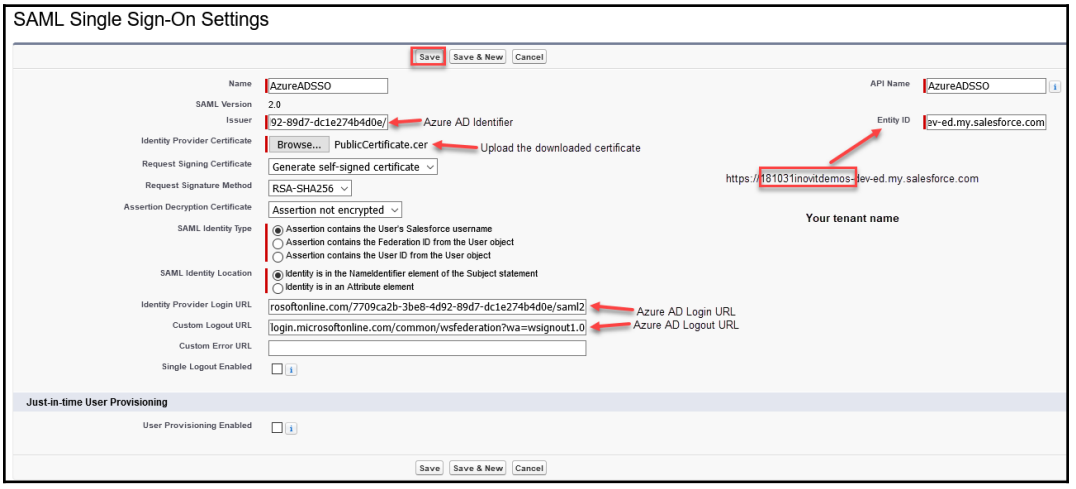

Salesforce - Single sign-on
Enterprise Application
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Self-service
Select a single sign-on method
Help me decide
Disabled
User must manually enter their username and password.
SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

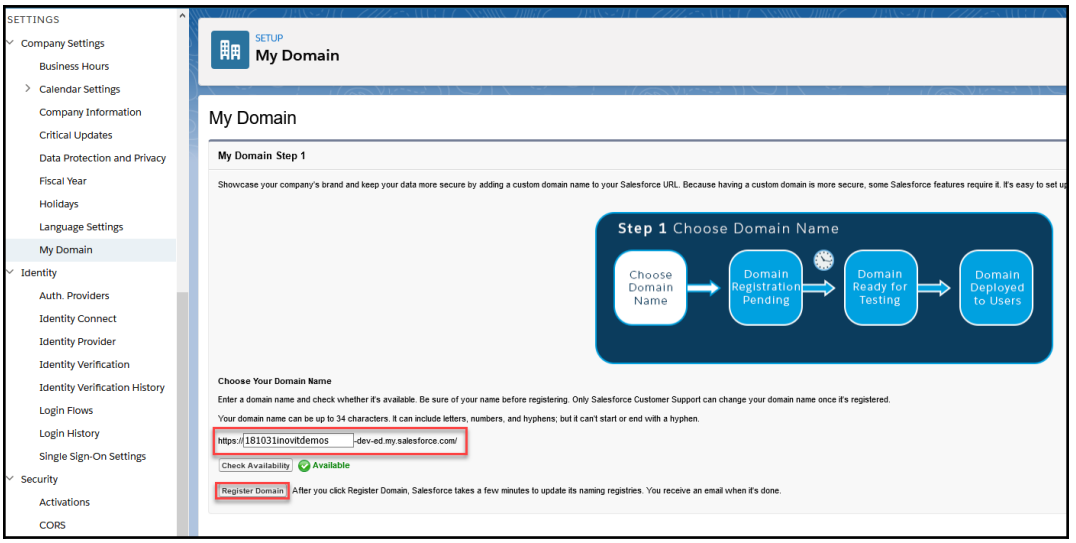

SAML Signing Certificate
Status
Active
Thumbprint
291DE7E9A7702406367550F0CC07C6191828AFC0
Expiration
1/13/2022, 3:41:03 PM
Notification Email
admin@181031inovitdemos.onmicrosoft.com
App Federation Metadata Url
https://login.microsoftonline.com/7709ca2b-3be8- ...
Certificate (Base64)
Download
Certificate (Raw)
Download
Federation Metadata XML
Download


Setup
Home
Object Manager
Identity
Auth. Providers
Identity Connect
Identity Provider
Identity Verification
Identity Verification History
Login Flows
Login History
Single Sign-On Settings
Security
Activations
CORS
CSP Trusted Sites
Certificate and Key Manag...
SETUP
Single Sign-On Settings
Single Sign-On Settings
Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:
Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.
Edit
SAML Assertion Validator
Federated Single Sign-On Using SAML
SAML Enabled
SAML Single Sign-On Settings
New
New from Metadata File
New from Metadata URL
No SAML Single Sign-On Settings

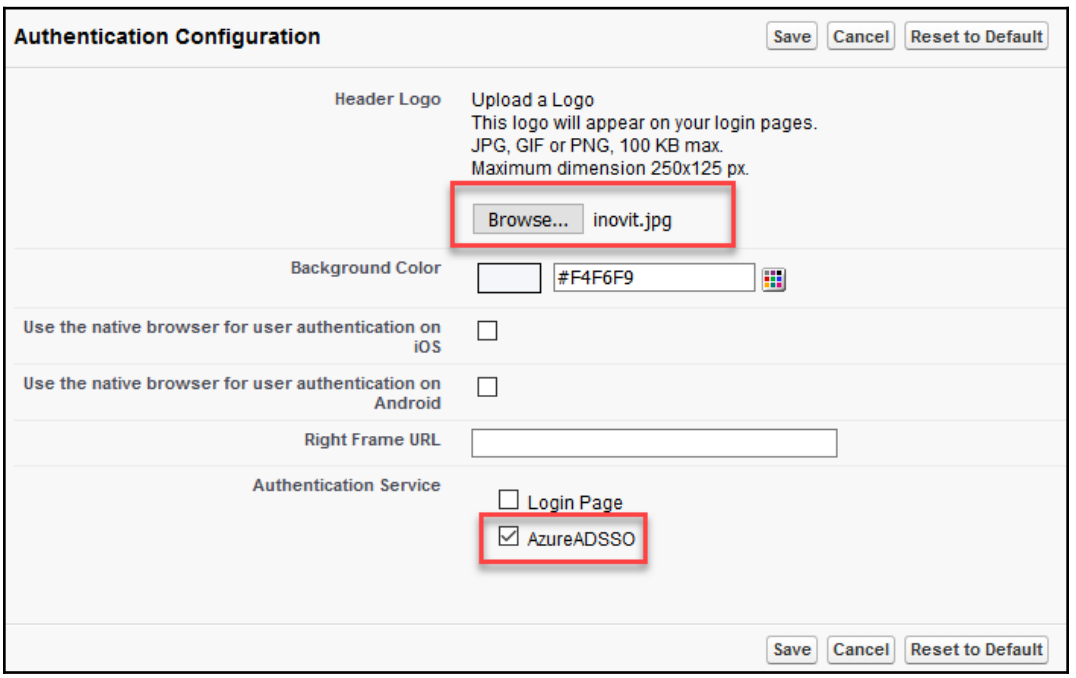

SAML Single Sign-On Settings
New
New from Metadata File
New from Metadata URL
No SAML Single Sign-On Settings

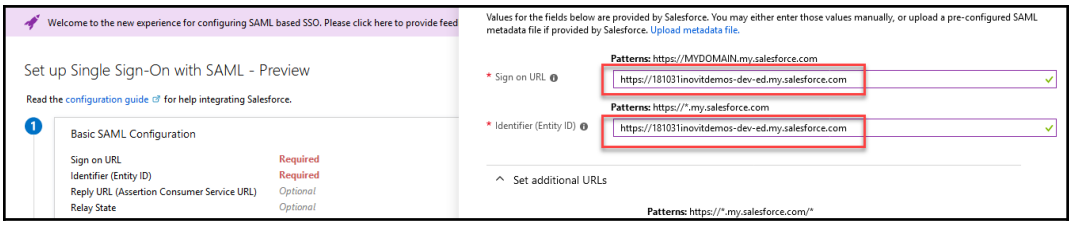

Set up Salesforce
You'll need to configure the application to link with Azure AD.
Login URL
https://login.microsoftonline.com/7709ca2b-3be8- ...
Azure AD Identifier
https://sts.windows.net/7709ca2b-3be8-4d92-89d7-...
Logout URL
https://login.microsoftonline.com/common/wsfed ...


SAML Single Sign-On Settings
Save
Save & New
Cancel
Name
AzureADSSO
API Name
AzureADSSO
SAML Version
2.0
Issuer
92-89d7-dc1e274b4d0e/
Azure AD Identifier
Entity ID
ev-ed.my.salesforce.com
Identity Provider Certificate
Browse...
PublicCertificate.cer
Upload the downloaded certificate
Request Signing Certificate
Generate self-signed certificate
Request Signature Method
RSA-SHA256
https://181031inovitdemos-dev-ed.my.salesforce.com
Assertion Decryption Certificate
Assertion not encrypted
Your tenant name
SAML Identity Type
Assertion contains the User's Salesforce username
Assertion contains the Federation ID from the User object
Assertion contains the User ID from the User object
SAML Identity Location
Identity is in the NameIdentifier element of the Subject statement
Identity is in an Attribute element
Identity Provider Login URL
rosoftonline.com/7709ca2b-3be8-4d92-89d7-dc1e274b4d0e/saml2
Azure AD Login URL
Custom Logout URL
login.microsoftonline.com/common/wsfederation?wa=wsignout1.0
Azure AD Logout URL
Custom Error URL
Single Logout Enabled
Just-in-time User Provisioning
User Provisioning Enabled
Save
Save & New
Cancel

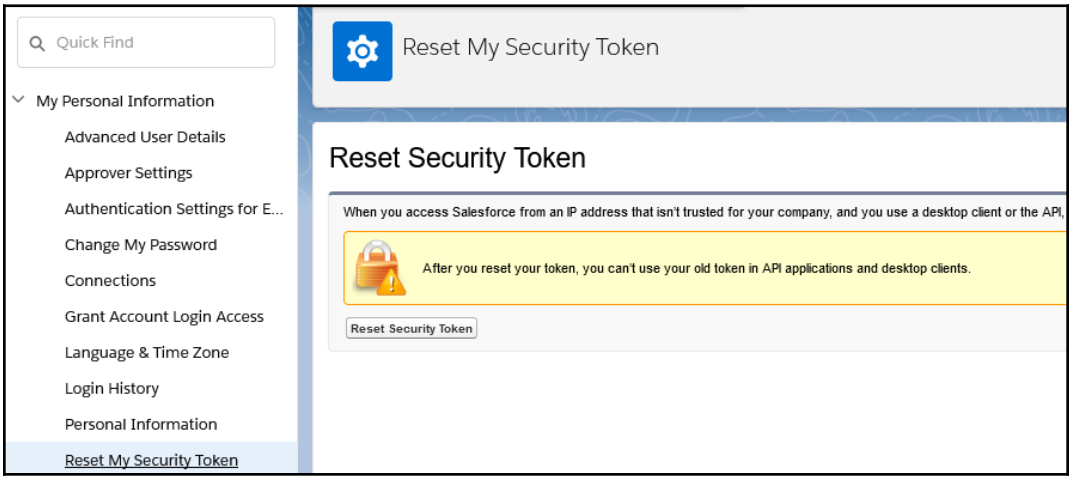

SETTINGS
Company Settings
Business Hours
Calendar Settings
Company Information
Critical Updates
Data Protection and Privacy
Fiscal Year
Holidays
Language Settings
My Domain
Identity
Auth. Providers
Identity Connect
Identity Provider
Identity Verification
Identity Verification History
Login Flows
Login History
Single Sign-On Settings
Security
Activations
CORS
SETUP
My Domain
My Domain
My Domain Step 1
Showcase your company's brand and keep your data more secure by adding a custom domain name to your Salesforce URL. Because having a custom domain is more secure, some Salesforce features require it. It's easy to set up
Step 1 Choose Domain Name
Choose Domain Name
Domain Registration Pending
Domain Ready for Testing
Domain Deployed to Users
Choose Your Domain Name
Enter a domain name and check whether it's available. Be sure of your name before registering. Only Salesforce Customer Support can change your domain name once it's registered.
Your domain name can be up to 34 characters. It can include letters, numbers, and hyphens, but it can't start or end with a hyphen.
https://181031inovitdemos
-dev-ed.my.salesforce.com/
Check Availability
Available
Register Domain
After you click Register Domain, Salesforce takes a few minutes to update its naming registries. You receive an email when it's done.

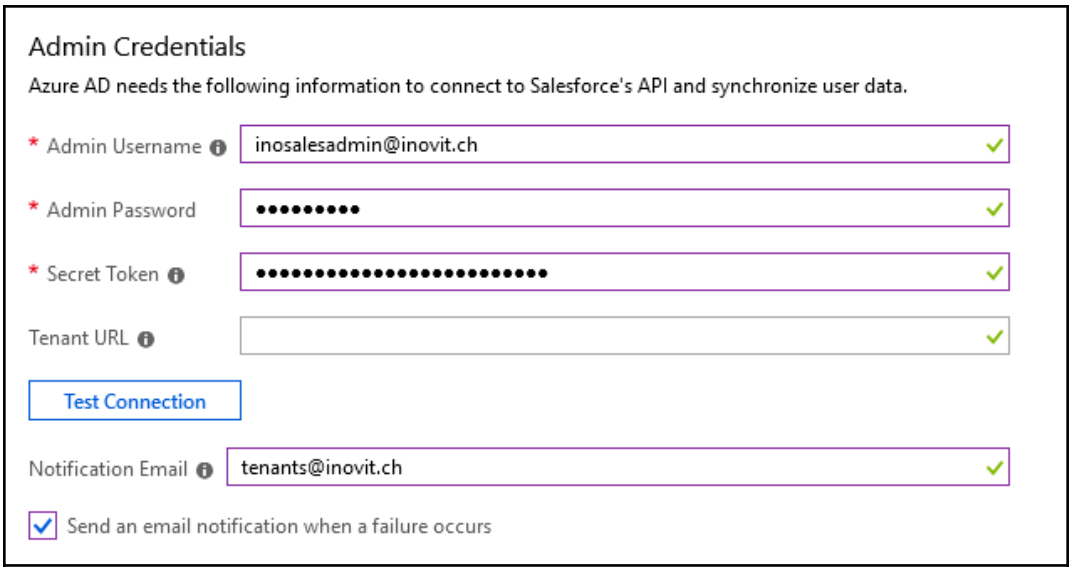

Authentication Configuration
Edit

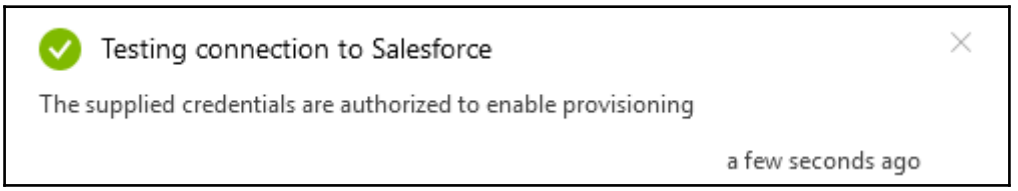

Authentication Configuration
Save
Cancel
Reset to Default
Header Logo
Upload a Logo
This logo will appear on your login pages.
JPG, GIF or PNG, 100 KB max.
Maximum dimension 250x125 px.
Browse...
inovit.jpg
Background Color
#F4F6F9
Use the native browser for user authentication on iOS
Use the native browser for user authentication on Android
Right Frame URL
Authentication Service
Login Page
AzureADSSO
Save
Cancel
Reset to Default

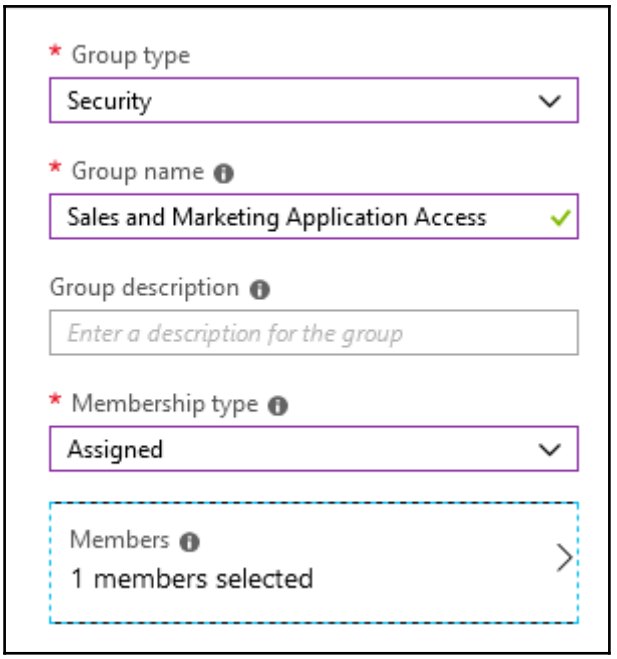

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feed
Set up Single Sign-On with SAML - Preview
Read the configuration guide for help integrating Salesforce.
Basic SAML Configuration
Sign on URL Required
Identifier (Entity ID) Required
Reply URL (Assertion Consumer Service URL) Optional
Relay State Optional
Values for the fields below are provided by Salesforce. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by Salesforce. Upload metadata file.
Patterns: https://MYDOMAIN.my.salesforce.com
* Sign on URL
https://181031inovitdemos-dev-ed.my.salesforce.com
Patterns: https://*.my.salesforce.com
* Identifier (Entity ID)
https://181031inovitdemos-dev-ed.my.salesforce.com
Set additional URLs
Patterns: https://*.my.salesforce.com/*

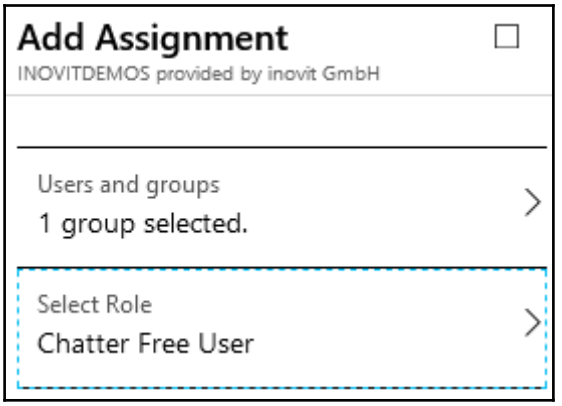

Switch to Lightning Experience
Jochen Nickel
My Profile
My Settings
Developer Console
Switch to Lightning Experience
Logout

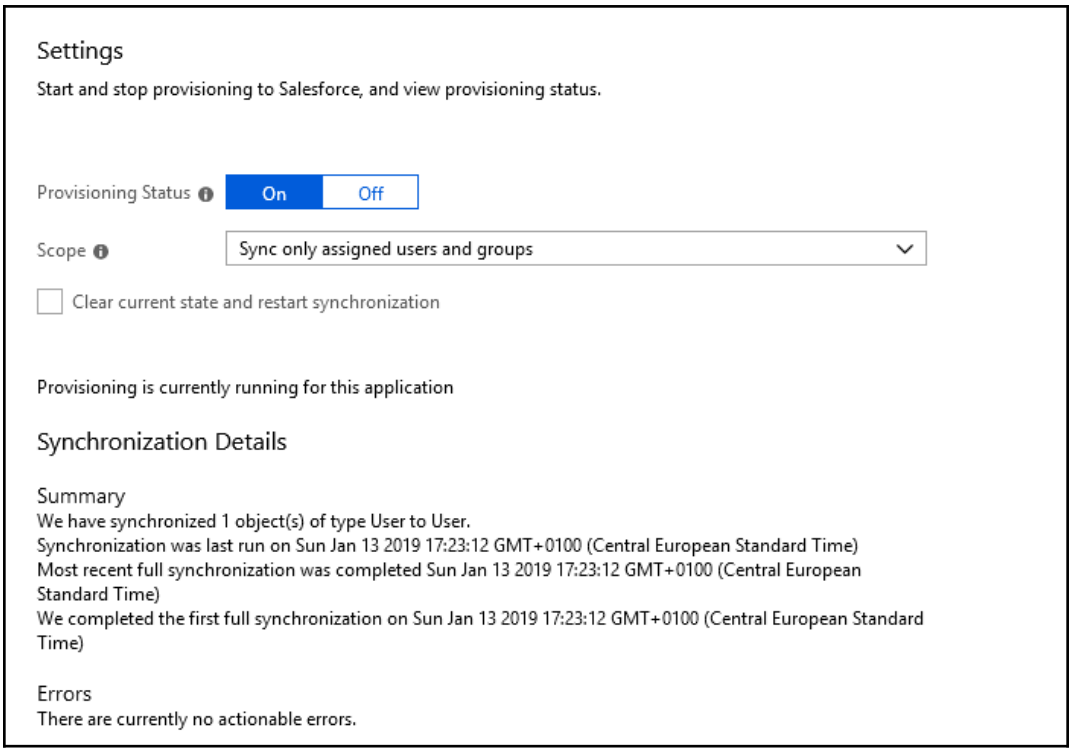

Quick Find
My Personal Information
Advanced User Details
Approver Settings
Authentication Settings for E...
Change My Password
Connections
Grant Account Login Access
Language & Time Zone
Login History
Personal Information
Reset My Security Token
Reset My Security Token
Reset Security Token
When you access Salesforce from an IP address that isn't trusted for your company, and you use a desktop client or the API,
After you reset your token, you can't use your old token in API applications and desktop clients.
Reset Security Token

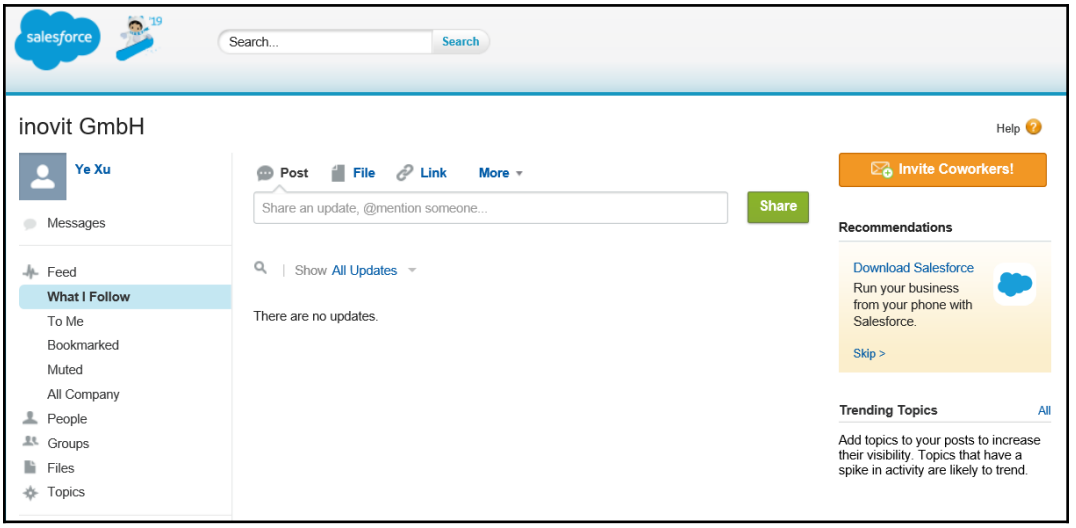

Admin Credentials
Azure AD needs the following information to connect to Salesforce's API and synchronize user data.
* Admin Username
inosalesadmin@inovit.ch
* Admin Password
••••••••••
* Secret Token
••••••••••••••••••••••••••
Tenant URL
Test Connection
Notification Email
tenants@inovit.ch
Send an email notification when a failure occurs

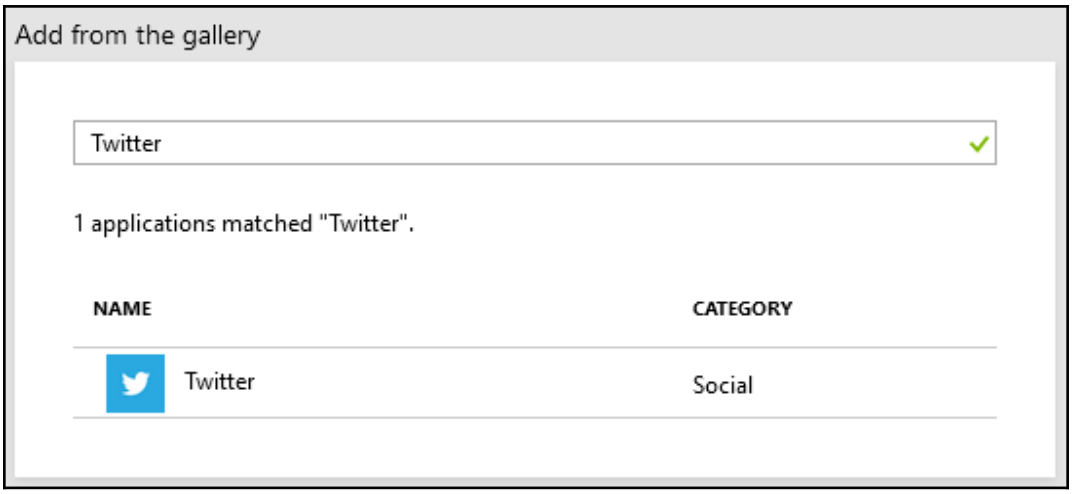

Testing connection to Salesforce
The supplied credentials are authorized to enable provisioning
a few seconds ago

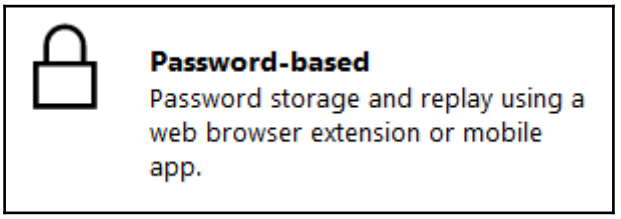

* Group type
Security
* Group name
Sales and Marketing Application Access
Group description
Enter a description for the group
* Membership type
Assigned
Members
1 members selected

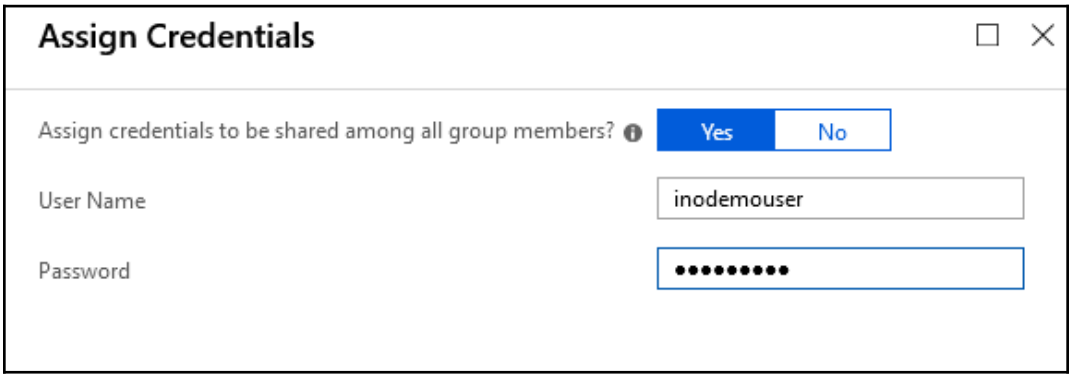

Add Assignment
INOVITDEMOS provided by inovit GmbH
Users and groups
1 group selected.
Select Role
Chatter Free User

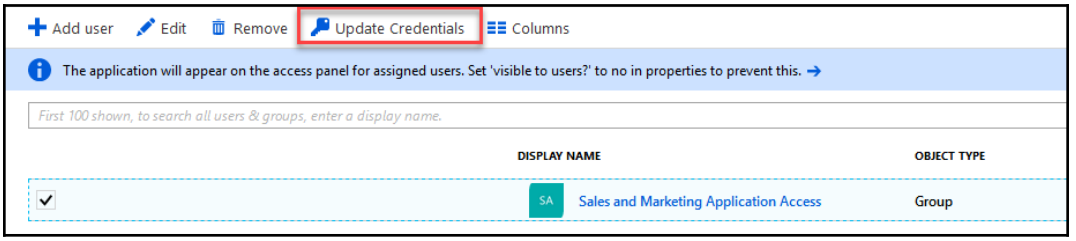

Settings
Start and stop provisioning to Salesforce, and view provisioning status.
Provisioning Status
On
Off
Scope
Sync only assigned users and groups
Clear current state and restart synchronization
Provisioning is currently running for this application
Synchronization Details
Summary
We have synchronized 1 object(s) of type User to User.
Synchronization was last run on Sun Jan 13 2019 17:23:12 GMT+0100 (Central European Standard Time)
Most recent full synchronization was completed Sun Jan 13 2019 17:23:12 GMT+0100 (Central European Standard Time)
We completed the first full synchronization on Sun Jan 13 2019 17:23:12 GMT+0100 (Central European Standard Time)
Errors
There are currently no actionable errors.

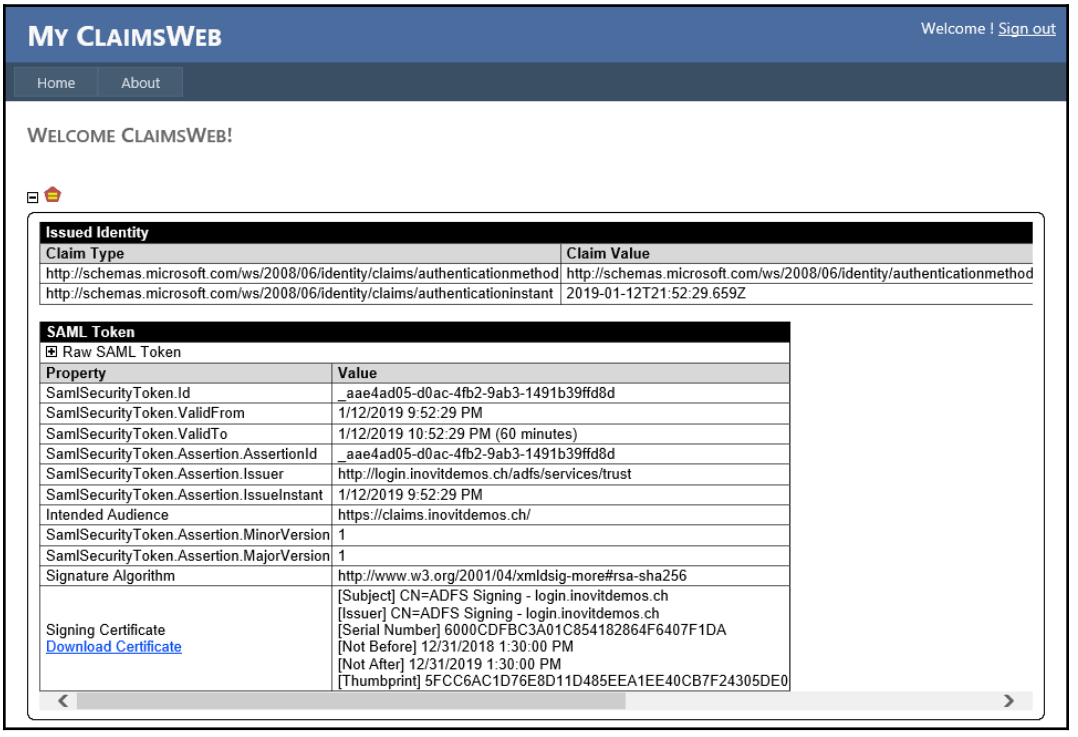

salesforce
Search...
Search
inovit GmbH
Help
Ye Xu
Post
File
Link
More
Share an update, @mention someone...
Share
Invite Coworkers!
Messages
Feed
What I Follow
To Me
Bookmarked
Muted
All Company
People
Groups
Files
Topics
Show All Updates
There are no updates.
Recommendations
Download Salesforce
Run your business from your phone with Salesforce.
Skip >
Trending Topics
All
Add topics to your posts to increase their visibility. Topics that have a spike in activity are likely to trend.


Add from the gallery
Twitter
1 applications matched "Twitter".
NAME
CATEGORY
Twitter
Social

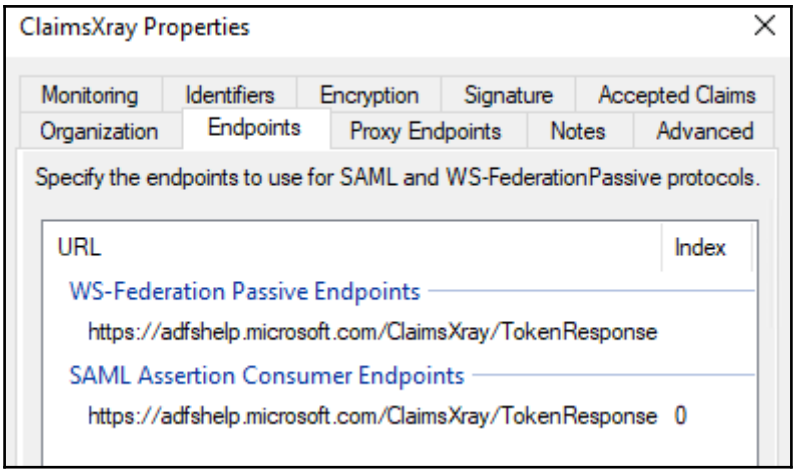

Password-based
Password storage and replay using a web browser extension or mobile app.


Assign Credentials
Assign credentials to be shared among all group members?
Yes
No
User Name
inodemouser
Password


Add user
Edit
Remove
Update Credentials
Columns
The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.
First 100 shown, to search all users & groups, enter a display name.
DISPLAY NAME
OBJECT TYPE
SA
Sales and Marketing Application Access
Group




```
CertificateType : Token-Signing
IsPrimary       : True
StoreLocation   : CurrentUser
StoreName       : My
Thumbprint      : 5FCC6AC1D76E8D11D485EEA1EE40CB7F24305DE0
```

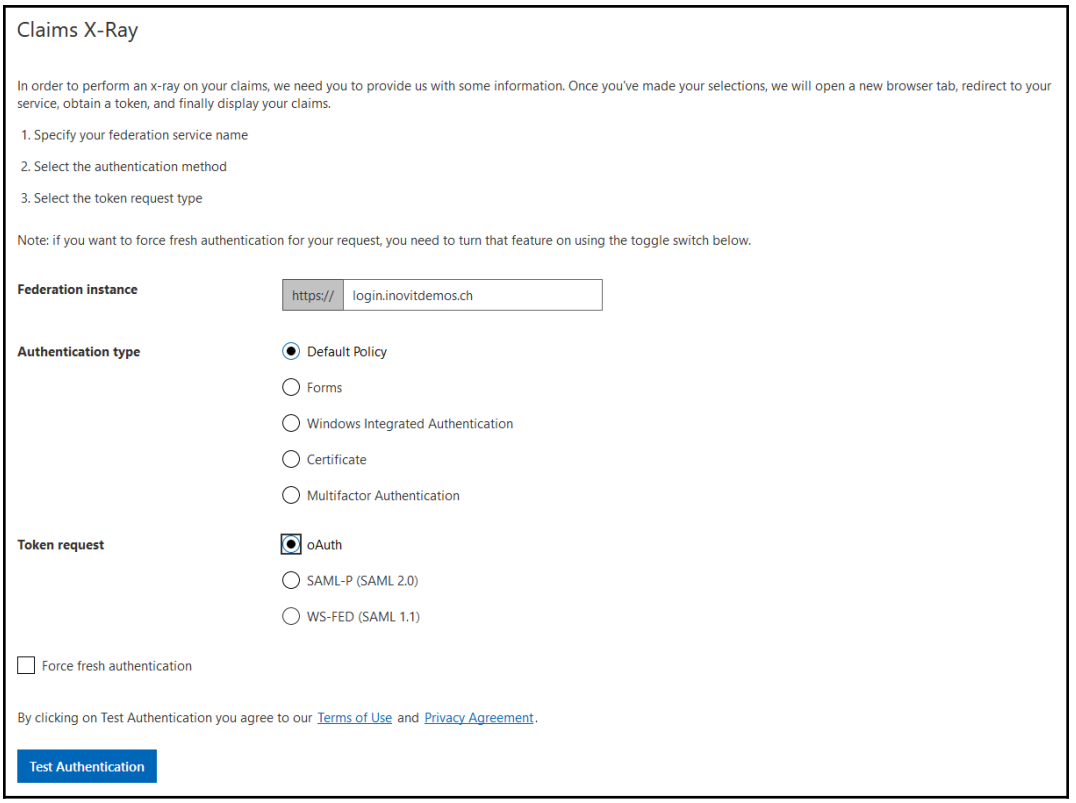


Federation request referrer

https://login.inovitdemos.ch/adfs/oauth2/authorize?response_type=code&client_id=claimsxrayclient&resource=urn:microsoft:adfs:claimsxray&redirect_uri=https://adfshelp.microsoft.com/ClaimsXray/TokenResponse&prompt=login

Token Claims 33

Claim	Value
alternateloginid	jochen.nickel@inovitdemos.ch
amp	FormsAuthentication
amr	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
anchor	winaccountname
appid	claimsxrayclient
apptype	Public
aud	urn:microsoft:adfs:claimsxray
auth_time	1/12/2019 10:22:04 PM
authmethod	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
clientip	10.0.0.7
clientreqid	7f403322-5481-49a5-0e02-0080000000c5
clientuseragent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
endpointpath	/adfs/oauth2/authorize


Claims X-Ray
In order to perform an x-ray on your claims, we need you to provide us with some information. Once you've made your selections, we will open a new browser tab, redirect to your service, obtain a token, and finally display your claims.
1. Specify your federation service name
2. Select the authentication method
3. Select the token request type
Note: if you want to force fresh authentication for your request, you need to turn that feature on using the toggle switch below.
Federation instance
https://
login.inovitdemos.ch
Authentication type
Default Policy
Forms
Windows Integrated Authentication
Certificate
Multifactor Authentication
Token request
oAuth
SAML-P (SAML 2.0)
WS-FED (SAML 1.1)
Force fresh authentication
By clicking on Test Authentication you agree to our Terms of Use and Privacy Agreement.
Test Authentication

Federation request referrer

https://login.inovitdemos.ch/adfs/oauth2/authorize?response_type=code&client_id=claimsxrayclient&resource=urn:microsoft:adfs:claimsxray&redirect_uri=https://adfshelp.microsoft.com/ClaimsXray/TokenResponse&prompt=login

Token Claims 33

Claim	Value
alternateloginid	jochen.nickel@inovitdemos.ch
amp	FormsAuthentication
amr	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
anchor	winaccountname
appid	claimsxrayclient
apptype	Public
aud	urn:microsoft:adfs:claimsxray
auth_time	1/12/2019 10:22:04 PM
authmethod	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
clientip	10.0.0.7
clientreqid	7f403322-5481-49a5-0e02-0080000000c5
clientuseragent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
endpointpath	/adfs/oauth2/authorize

Welcome to the Add Relying Party Trust Wizard

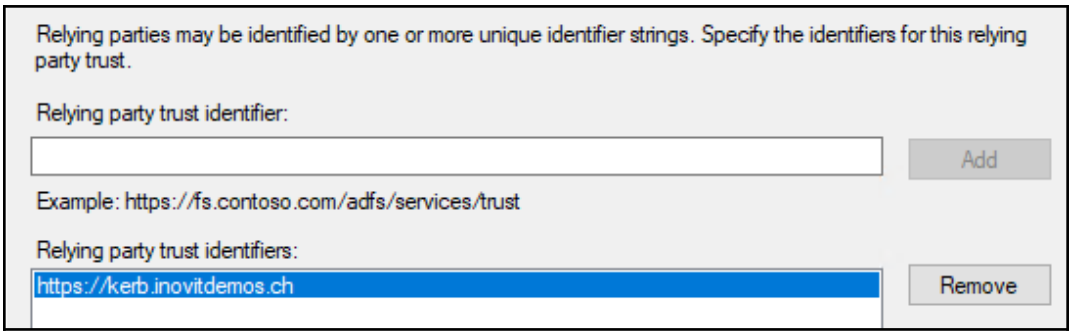
Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

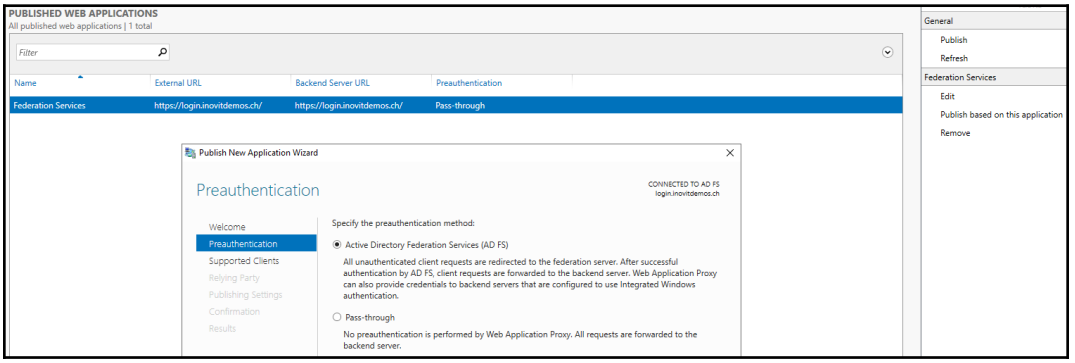
- ○ Claims aware
- ◉ Non claims aware

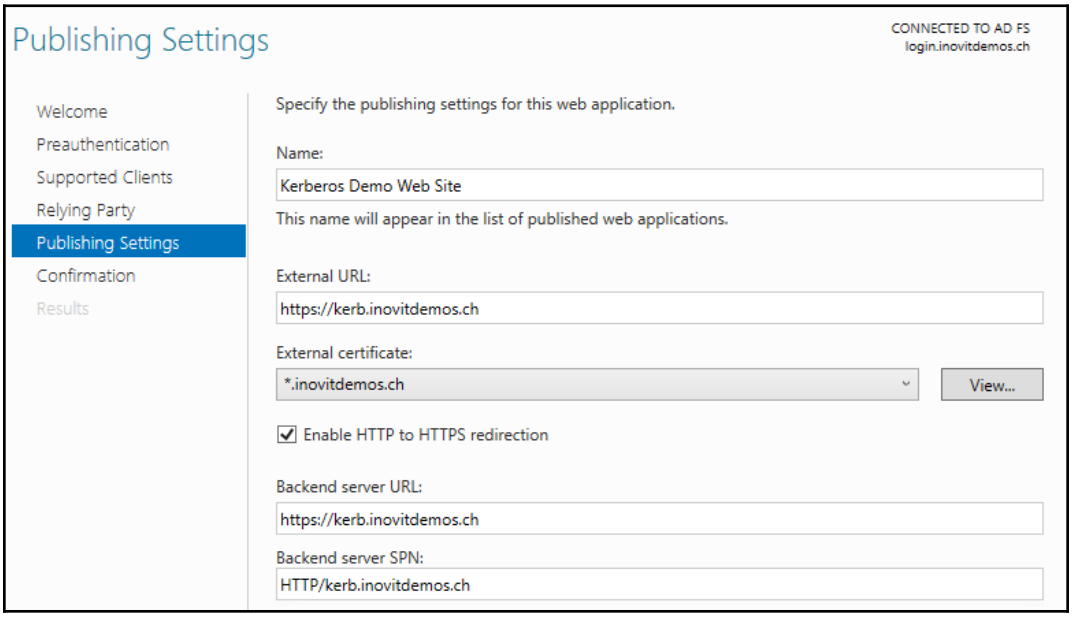
Enter the display name and any optional notes for this relying party.

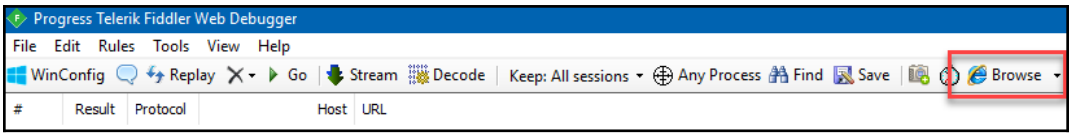
Display name:

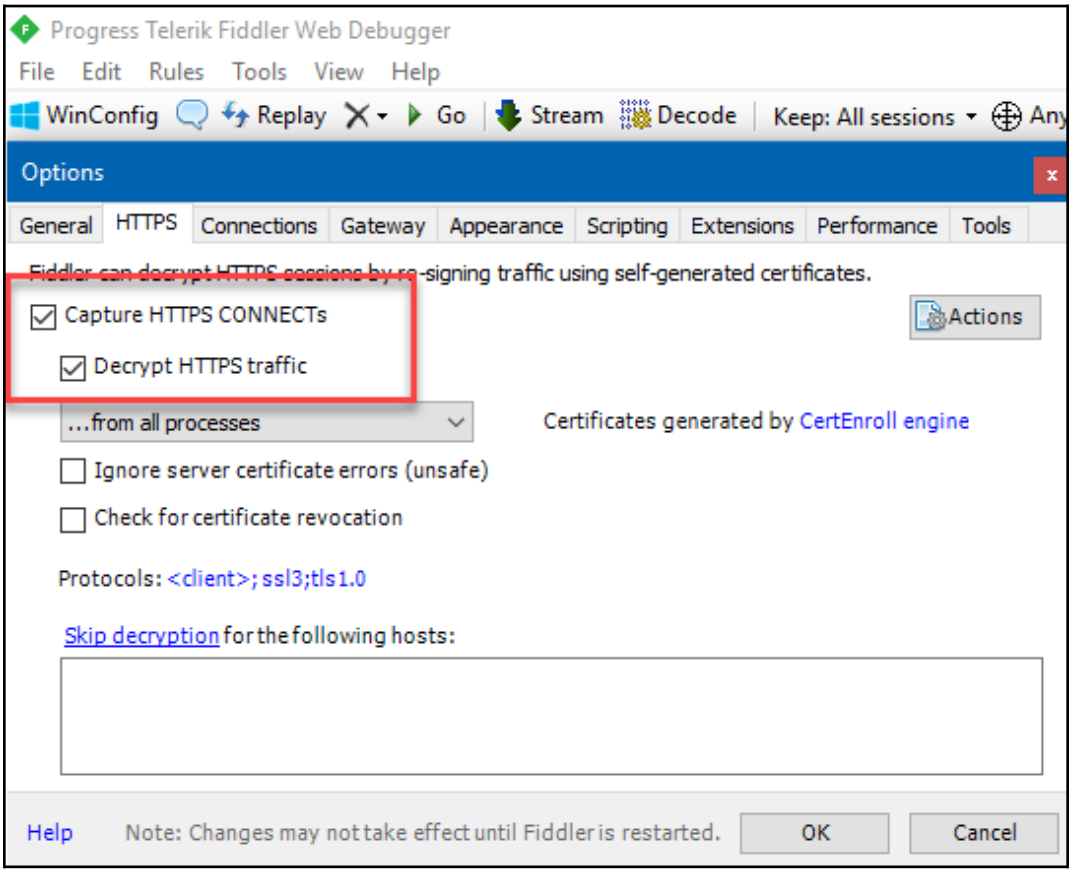
Kerberos Demo Web Site

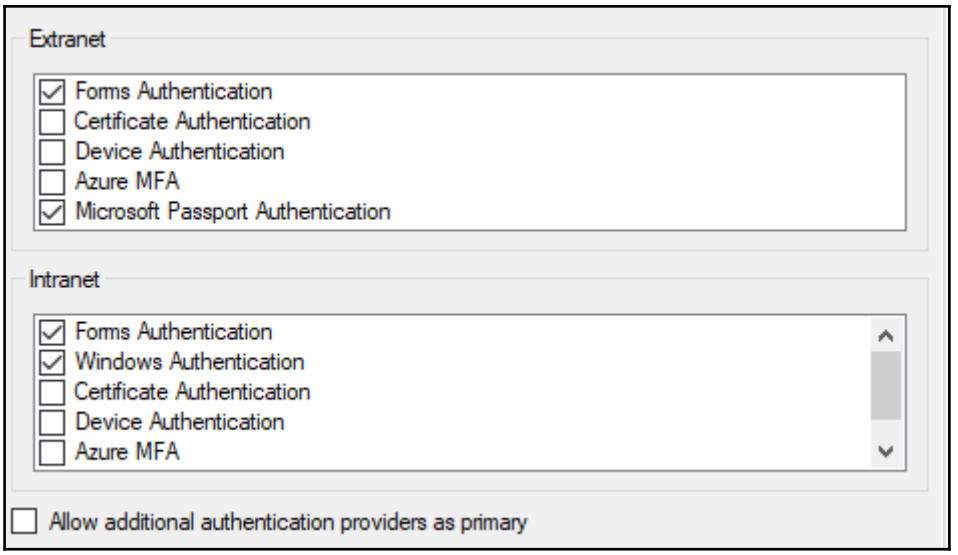

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.
Relying party trust identifier:
Add
Example: https://fs.contoso.com/adfs/services/trust
Relying party trust identifiers:
https://kerb.inovitdemos.ch
Remove


PUBLISHED WEB APPLICATIONS
All published web applications | 1 total
Filter
Name
External URL
Backend Server URL
Preauthentication
Federation Services
https://login.inovitdemos.ch/
https://login.inovitdemos.ch/
Pass-through
General
Publish
Refresh
Federation Services
Edit
Publish based on this application
Remove
Publish New Application Wizard
Preauthentication
CONNECTED TO AD FS
login.inovitdemos.ch
Welcome
Preauthentication
Supported Clients
Relying Party
Publishing Settings
Confirmation
Results
Specify the preauthentication method:
Active Directory Federation Services (AD FS)
All unauthenticated client requests are redirected to the federation server. After successful authentication by AD FS, client requests are forwarded to the backend server. Web Application Proxy can also provide credentials to backend servers that are configured to use Integrated Windows authentication.
Pass-through
No preauthentication is performed by Web Application Proxy. All requests are forwarded to the backend server.

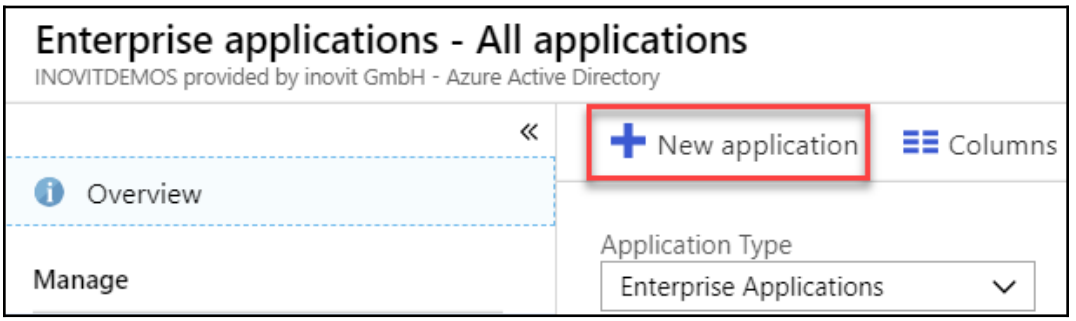

Publishing Settings
CONNECTED TO AD FS
login.inovitdemos.ch
Welcome
Preauthentication
Supported Clients
Relying Party
Publishing Settings
Confirmation
Results
Specify the publishing settings for this web application.
Name:
Kerberos Demo Web Site
This name will appear in the list of published web applications.
External URL:
https://kerb.inovitdemos.ch
External certificate:
*.inovitdemos.ch
View...
Enable HTTP to HTTPS redirection
Backend server URL:
https://kerb.inovitdemos.ch
Backend server SPN:
HTTP/kerb.inovitdemos.ch

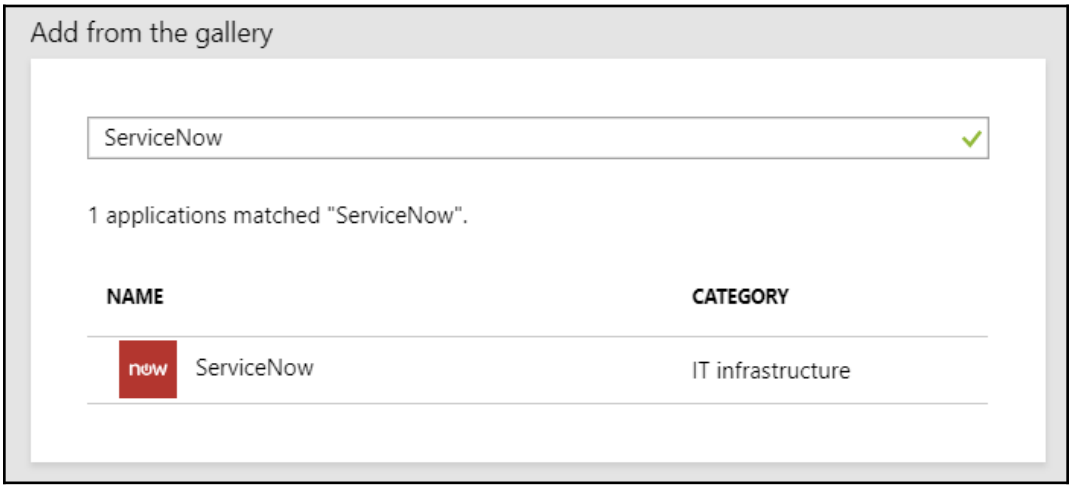

Progress Telerik Fiddler Web Debugger
File Edit Rules Tools View Help
WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse
Result Protocol Host URL

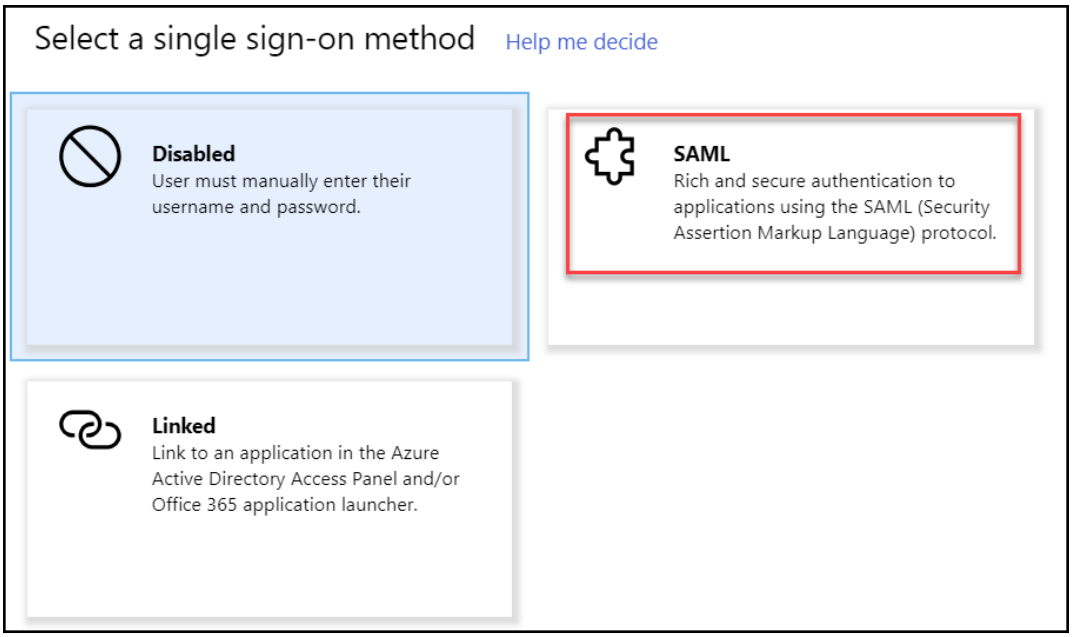

Progress Telerik Fiddler Web Debugger
File Edit Rules Tools View Help
WinConfig Replay Go Stream Decode Keep: All sessions
Options
General HTTPS Connections Gateway Appearance Scripting Extensions Performance Tools
Fiddler can decrypt HTTPS sessions by re-signing traffic using self-generated certificates.
Capture HTTPS CONNECTs
Decrypt HTTPS traffic
Actions
...from all processes
Certificates generated by CertEnroll engine
Ignore server certificate errors (unsafe)
Check for certificate revocation
Protocols: <client>; ssl3;tls1.0
Skip decryption for the following hosts:
Help
Note: Changes may not take effect until Fiddler is restarted.
OK
Cancel

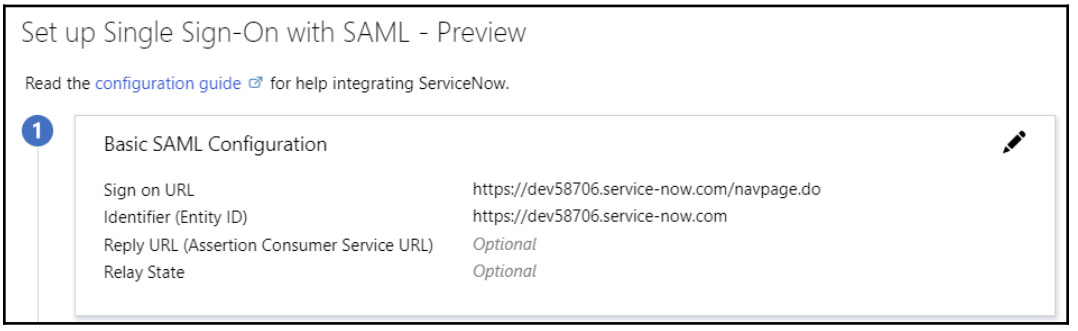

Extranet
Forms Authentication
Certificate Authentication
Device Authentication
Azure MFA
Microsoft Passport Authentication
Intranet
Forms Authentication
Windows Authentication
Certificate Authentication
Device Authentication
Azure MFA
Allow additional authentication providers as primary

Chapter 8: Using the Azure AD App Proxy and the Web Application Proxy

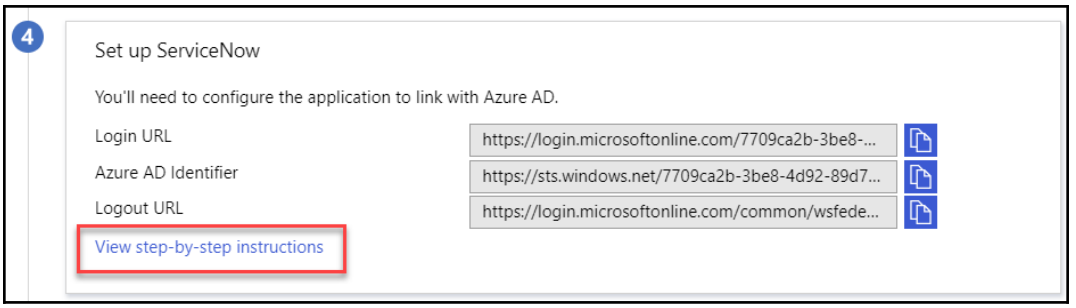


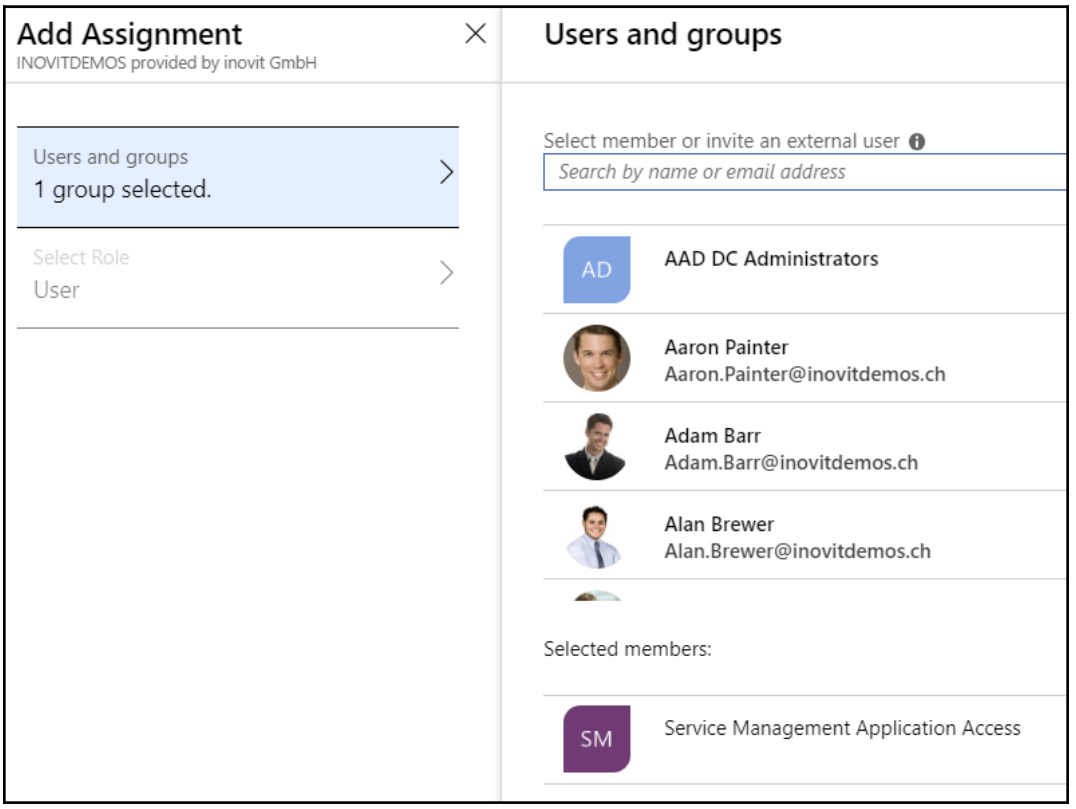


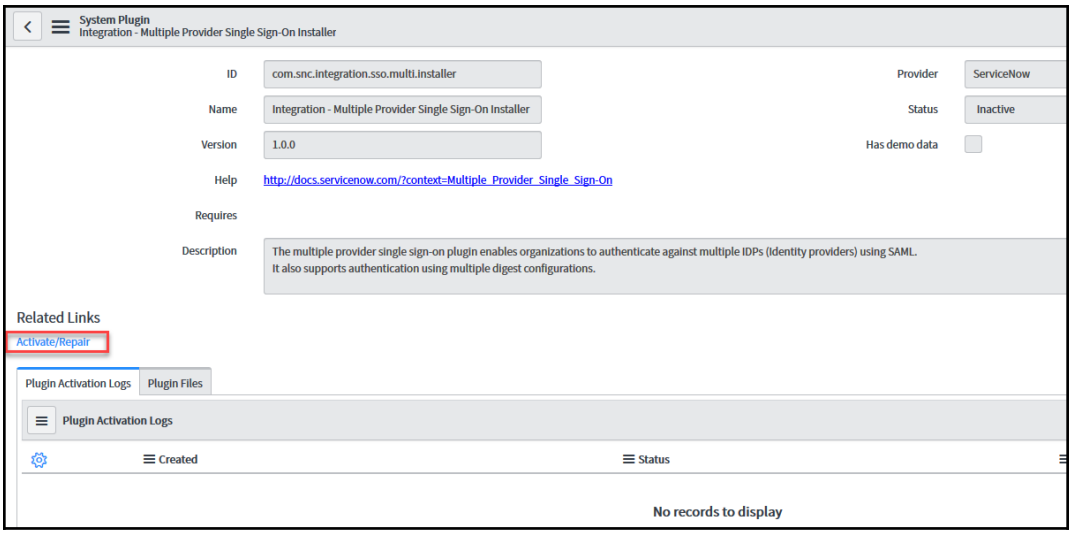

Select a single sign-on method
Help me decide
Disabled
User must manually enter their username and password.
SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

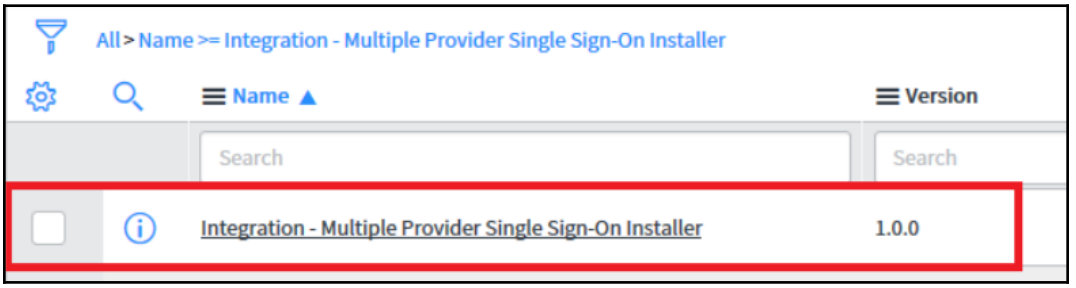

Set up Single Sign-On with SAML - Preview
Read the configuration guide for help integrating ServiceNow.
1
Basic SAML Configuration
Sign on URL
https://dev58706.service-now.com/navpage.do
Identifier (Entity ID)
https://dev58706.service-now.com
Reply URL (Assertion Consumer Service URL)
Optional
Relay State
Optional

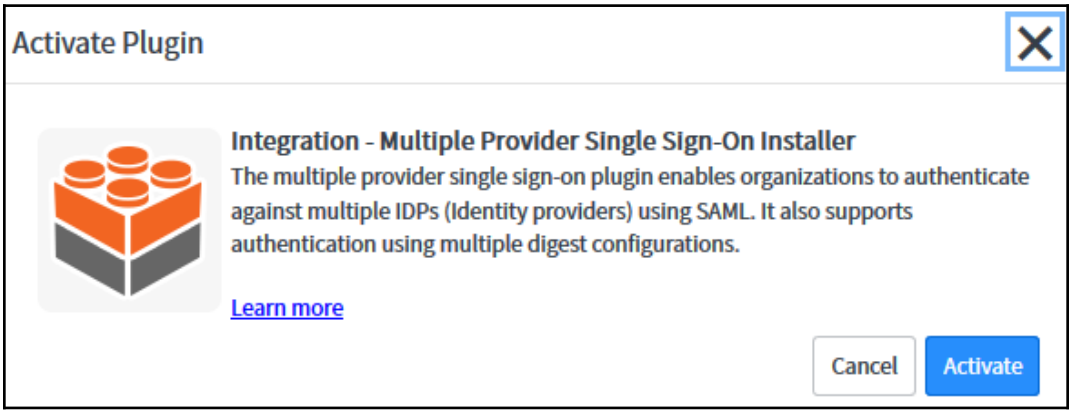

3
SAML Signing Certificate
Status
Active
Thumbprint
27ECBC35516E790E773DF6148BAFBC86538C44C0
Expiration
1/14/2022, 7:21:15 AM
Notification Email
admin@181031inovitdemos.onmicrosoft.com
App Federation Metadata Url
https://login.microsoftonline.com/7709ca2b-3be8-...
Certificate (Base64)
Download
Certificate (Raw)
Download
Federation Metadata XML
Download

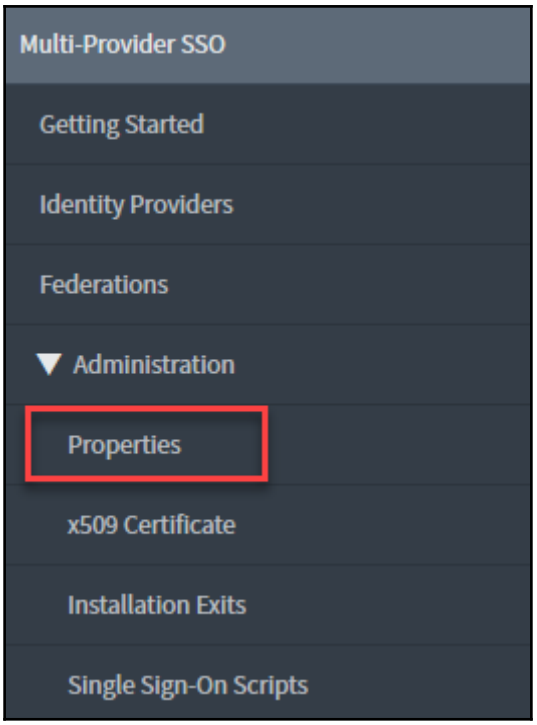

4
Set up ServiceNow
You'll need to configure the application to link with Azure AD.
Login URL
https://login.microsoftonline.com/7709ca2b-3be8-...
Azure AD Identifier
https://sts.windows.net/7709ca2b-3be8-4d92-89d7...
Logout URL
https://login.microsoftonline.com/common/wsfede...
View step-by-step instructions

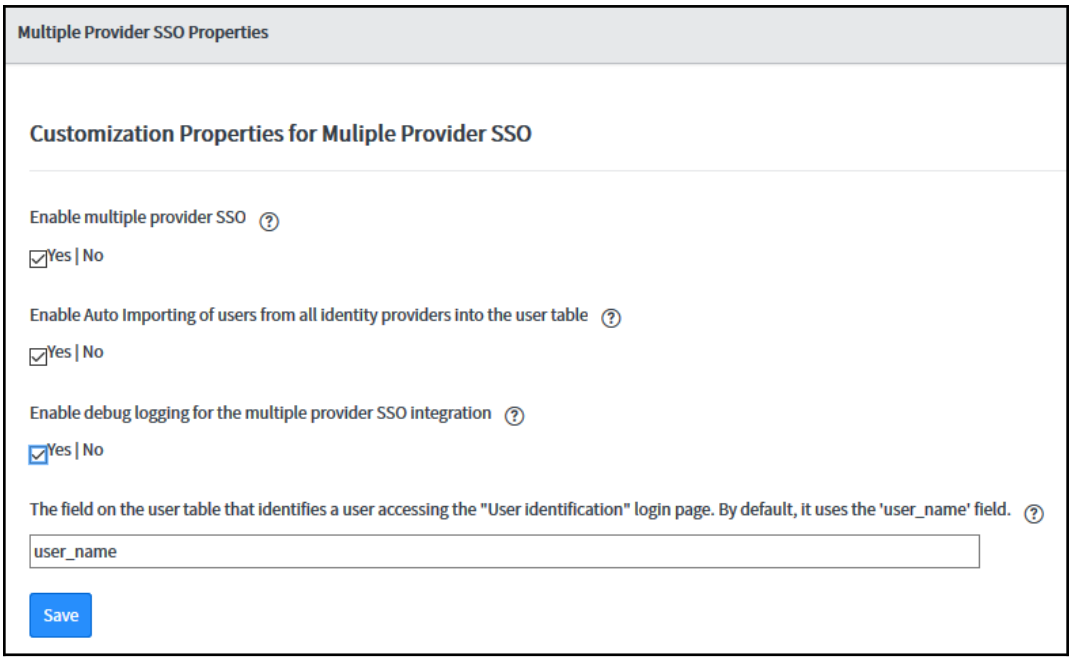

Add Assignment
INOVITDEMOS provided by inovit GmbH
Users and groups
1 group selected.
Select Role
User
Users and groups
Select member or invite an external user
Search by name or email address
AD
AAD DC Administrators
Aaron Painter
Aaron.Painter@inovitdemos.ch
Adam Barr
Adam.Barr@inovitdemos.ch
Alan Brewer
Alan.Brewer@inovitdemos.ch
Selected members:
SM
Service Management Application Access

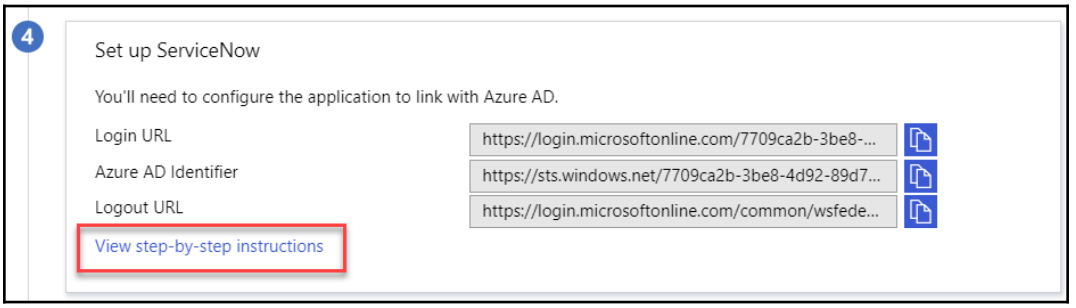

System Plugin
Integration - Multiple Provider Single Sign-On Installer
ID
com.snc.integration.sso.multi.installer
Provider
ServiceNow
Name
Integration - Multiple Provider Single Sign-On Installer
Status
Inactive
Version
1.0.0
Has demo data
Help
http://docs.servicenow.com/?context=Multiple_Provider_Single_Sign-On
Requires
Description
The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML.
It also supports authentication using multiple digest configurations.
Related Links
Activate/Repair
Plugin Activation Logs
Plugin Files
Plugin Activation Logs
Created
Status
No records to display

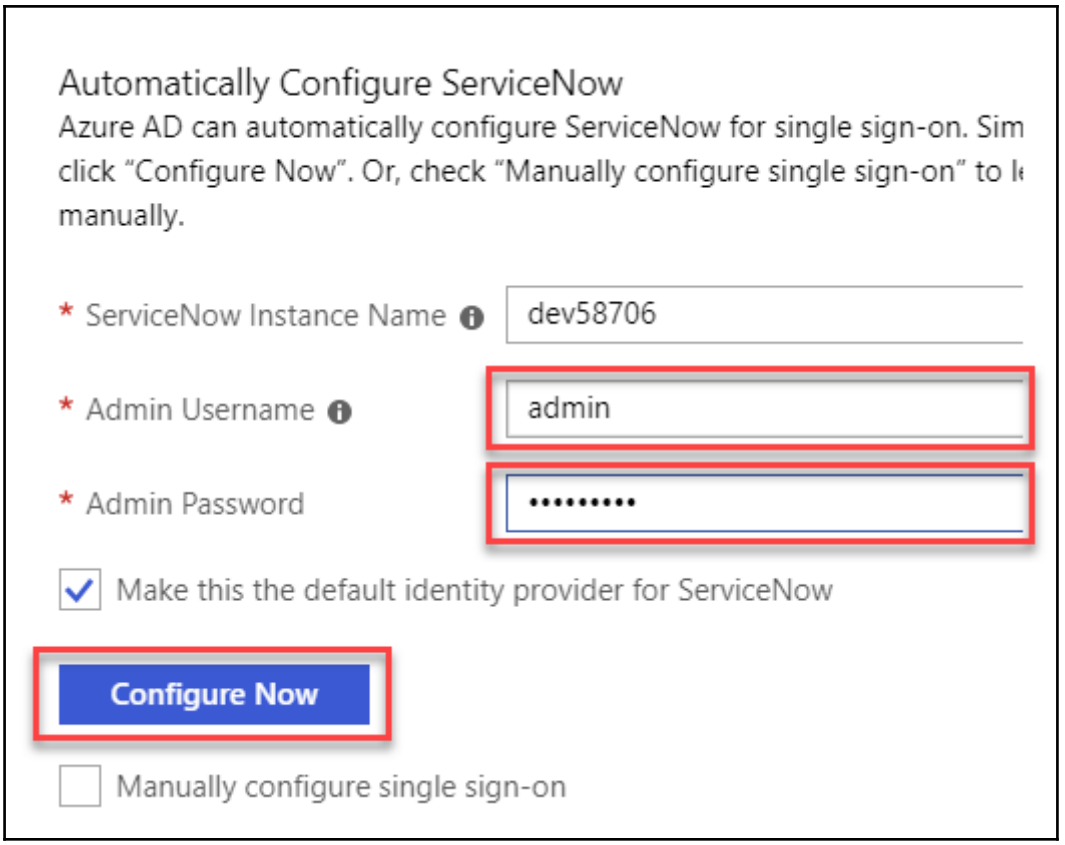

All > Name >= Integration - Multiple Provider Single Sign-On Installer
Name
Version
Search
Search
Integration - Multiple Provider Single Sign-On Installer
1.0.0

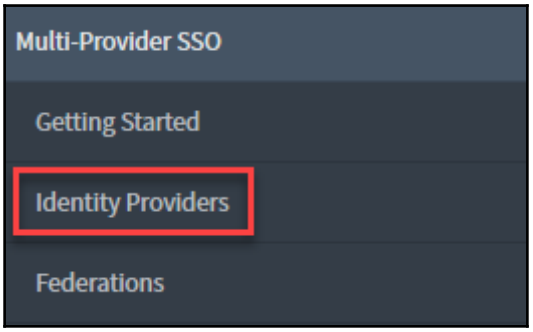

Activate Plugin
Integration - Multiple Provider Single Sign-On Installer
The multiple provider single sign-on plugin enables organizations to authenticate against multiple IDPs (Identity providers) using SAML. It also supports authentication using multiple digest configurations.
Learn more
Cancel
Activate

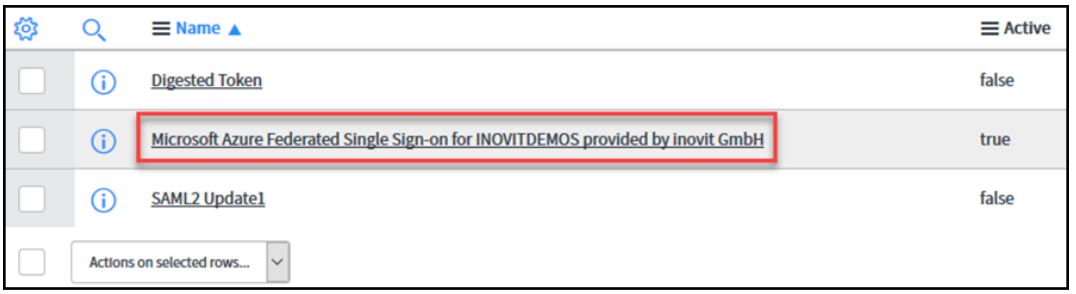

Multi-Provider SSO
Getting Started
Identity Providers
Federations
Administration
Properties
x509 Certificate
Installation Exits
Single Sign-On Scripts

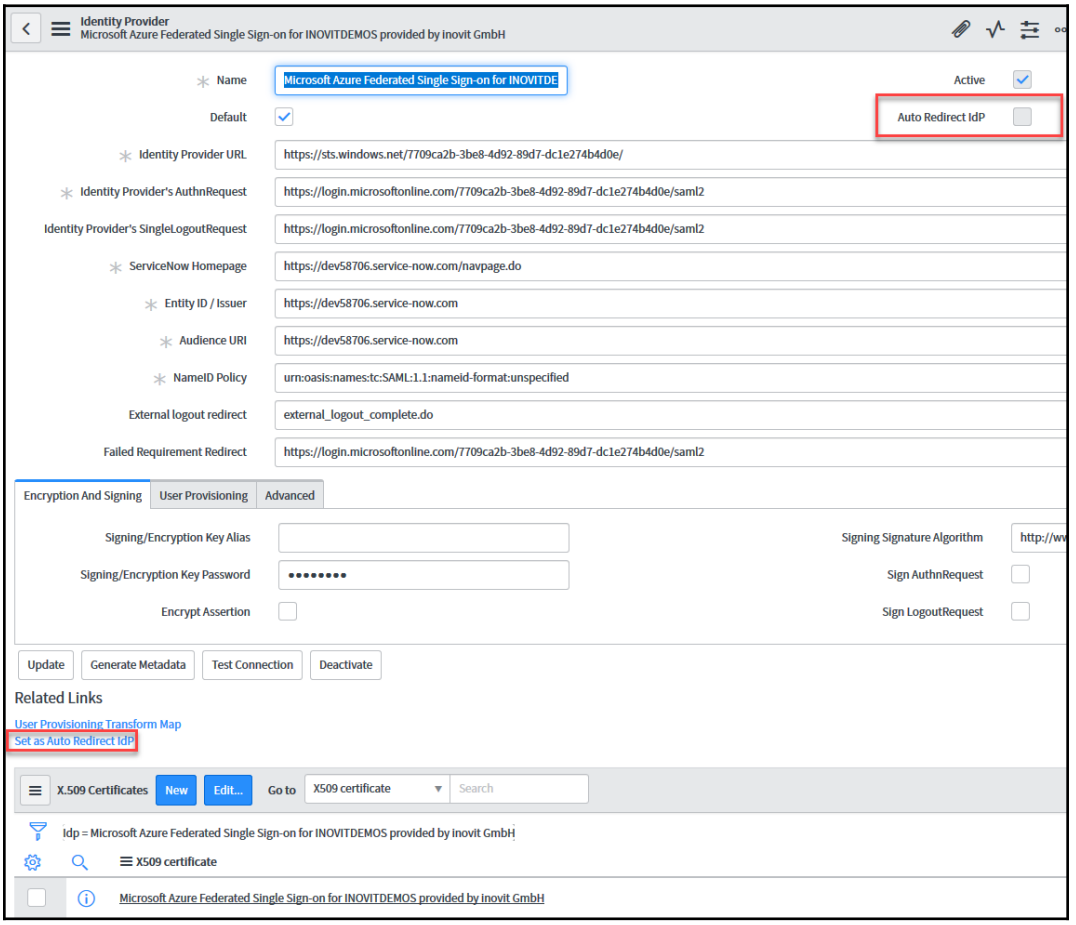

Multiple Provider SSO Properties
Customization Properties for Muliple Provider SSO
Enable multiple provider SSO
Yes | No
Enable Auto Importing of users from all identity providers into the user table
Yes | No
Enable debug logging for the multiple provider SSO integration
Yes | No
The field on the user table that identifies a user accessing the "User identification" login page. By default, it uses the 'user_name' field.
user_name
Save


4
Set up ServiceNow
You'll need to configure the application to link with Azure AD.
Login URL
https://login.microsoftonline.com/7709ca2b-3be8-...
Azure AD Identifier
https://sts.windows.net/7709ca2b-3be8-4d92-89d7...
Logout URL
https://login.microsoftonline.com/common/wsfede...
View step-by-step instructions

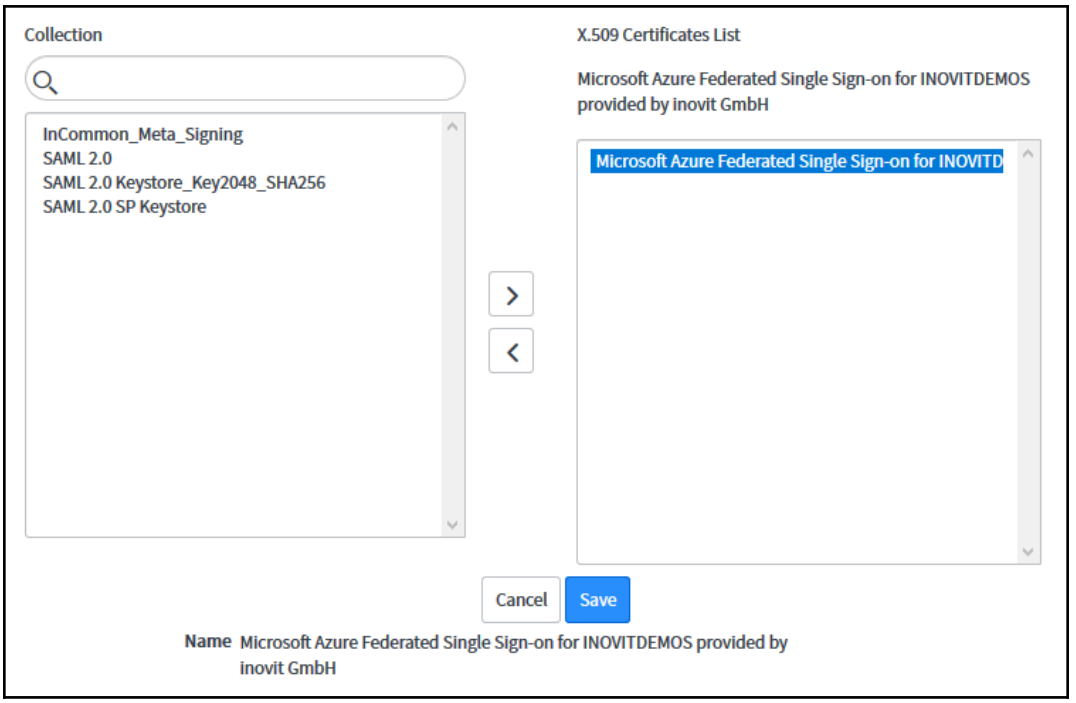

Automatically Configure ServiceNow
Azure AD can automatically configure ServiceNow for single sign-on. Sim
click "Configure Now". Or, check "Manually configure single sign-on" to l
manually.
* ServiceNow Instance Name
dev58706
* Admin Username
admin
* Admin Password
Make this the default identity provider for ServiceNow
Configure Now
Manually configure single sign-on

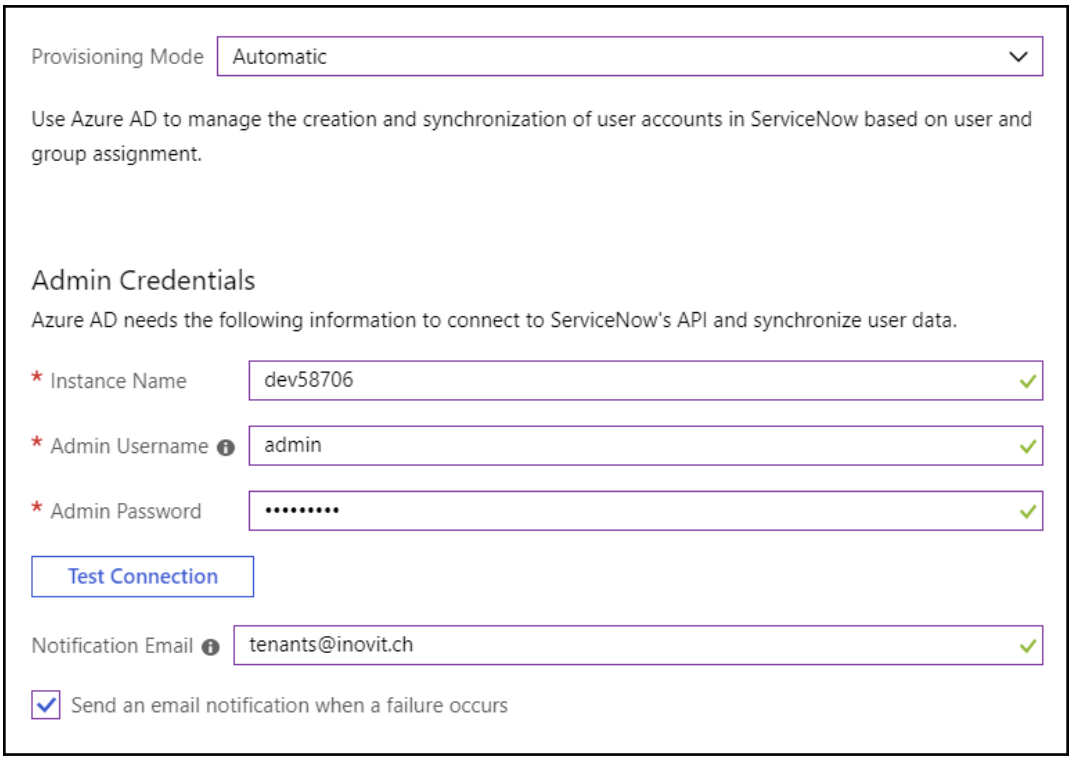

Multi-Provider SSO
Getting Started
Identity Providers
Federations

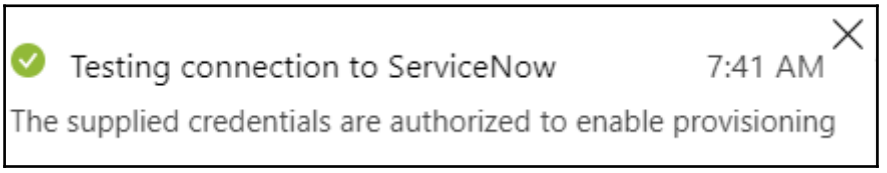

Name
Active
Digested Token
false
Microsoft Azure Federated Single Sign-on for INOVITDEMOS provided by inovit GmbH
true
SAML2 Update1
false
Actions on selected rows...

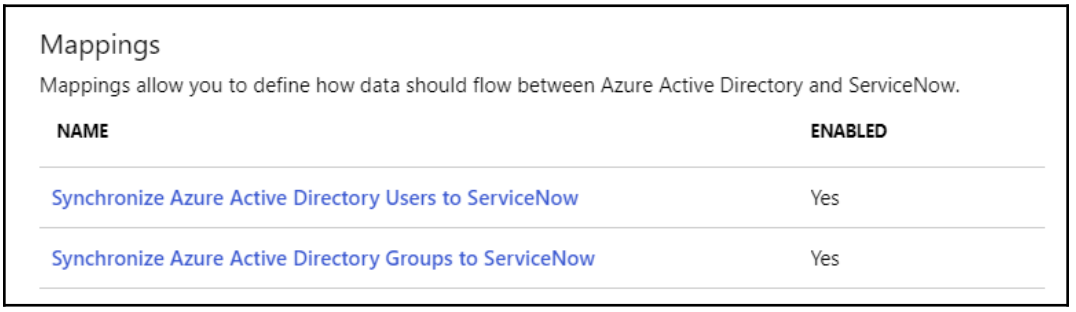

Identity Provider
Microsoft Azure Federated Single Sign-on for INOVITDEMOS provided by inovit GmbH
Name
Microsoft Azure Federated Single Sign-on for INOVITDE
Active
Default
Auto Redirect IdP
Identity Provider URL
https://sts.windows.net/7709ca2b-3be8-4d92-89d7-dc1e274b4d0e/
Identity Provider's AuthnRequest
https://login.microsoftonline.com/7709ca2b-3be8-4d92-89d7-dc1e274b4d0e/saml2
Identity Provider's SingleLogoutRequest
https://login.microsoftonline.com/7709ca2b-3be8-4d92-89d7-dc1e274b4d0e/saml2
ServiceNow Homepage
https://dev58706.service-now.com/navpage.do
Entity ID / Issuer
https://dev58706.service-now.com
Audience URI
https://dev58706.service-now.com
NameID Policy
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
External logout redirect
external_logout_complete.do
Failed Requirement Redirect
https://login.microsoftonline.com/7709ca2b-3be8-4d92-89d7-dc1e274b4d0e/saml2
Encryption And Signing
User Provisioning
Advanced
Signing/Encryption Key Alias
Signing Signature Algorithm
Signing/Encryption Key Password
Sign AuthnRequest
Encrypt Assertion
Sign LogoutRequest
Update
Generate Metadata
Test Connection
Deactivate
Related Links
User Provisioning Transform Map
Set as Auto Redirect IdP
X.509 Certificates
New
Edit...
Go to
X509 certificate
Search
Idp = Microsoft Azure Federated Single Sign-on for INOVITDEMOS provided by inovit GmbH
X509 certificate
Microsoft Azure Federated Single Sign-on for INOVITDEMOS provided by inovit GmbH

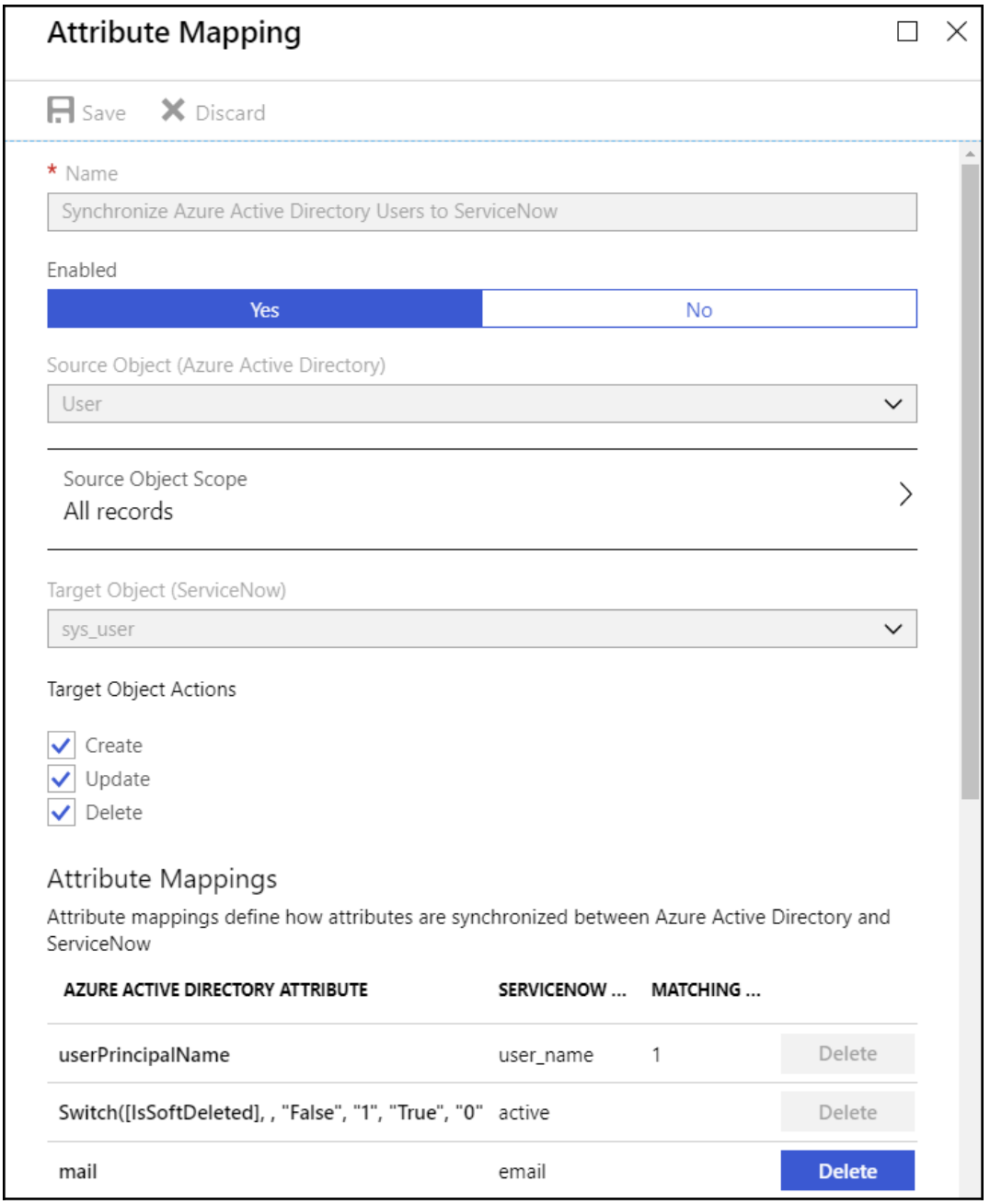

Auto Redirect IdP


Collection
InCommon_Meta_Signing
SAML 2.0
SAML 2.0 Keystore_Key2048_SHA256
SAML 2.0 SP Keystore
X.509 Certificates List
Microsoft Azure Federated Single Sign-on for INOVITDEMOS provided by inovit GmbH
Microsoft Azure Federated Single Sign-on for INOVITD
Cancel
Save
Name
Microsoft Azure Federated Single Sign-on for INOVITDEMOS provided by inovit GmbH


Provisioning Mode
Automatic
Use Azure AD to manage the creation and synchronization of user accounts in ServiceNow based on user and group assignment.
Admin Credentials
Azure AD needs the following information to connect to ServiceNow's API and synchronize user data.
* Instance Name
dev58706
* Admin Username
admin
* Admin Password
Test Connection
Notification Email
tenants@inovit.ch
Send an email notification when a failure occurs


Testing connection to ServiceNow
7:41 AM
The supplied credentials are authorized to enable provisioning


Mappings
Mappings allow you to define how data should flow between Azure Active Directory and ServiceNow.
NAME
ENABLED
Synchronize Azure Active Directory Users to ServiceNow
Yes
Synchronize Azure Active Directory Groups to ServiceNow
Yes


Attribute Mapping
Save
Discard
* Name
Synchronize Azure Active Directory Users to ServiceNow
Enabled
Yes
No
Source Object (Azure Active Directory)
User
Source Object Scope
All records
Target Object (ServiceNow)
sys_user
Target Object Actions
Create
Update
Delete
Attribute Mappings
Attribute mappings define how attributes are synchronized between Azure Active Directory and ServiceNow
AZURE ACTIVE DIRECTORY ATTRIBUTE
SERVICENOW ...
MATCHING ...
userPrincipalName
user_name
1
Delete
Switch([IsSoftDeleted], , "False", "1", "True", "0"
active
Delete
mail
email
Delete

Provisioning is currently running for this application

Synchronization Details

Summary

We have synchronized 1 object(s) of type Group to sys_user_group.We have synchronized 1 object(s) of type User to sys_user.
Synchronization was last run on Mon Jan 14 2019 07:44:56 GMT+0100 (Central European Standard Time)
Most recent full synchronization was completed Mon Jan 14 2019 07:44:56 GMT+0100 (Central European Standard Time)
We completed the first full synchronization on Mon Jan 14 2019 07:44:56 GMT+0100 (Central European Standard Time)

Errors

There are currently no actionable errors.

View the "Account Provisioning" category in the audit logs for full details

Activity

Date : 1/14/2019, 7:44:54 AM

Name : Import

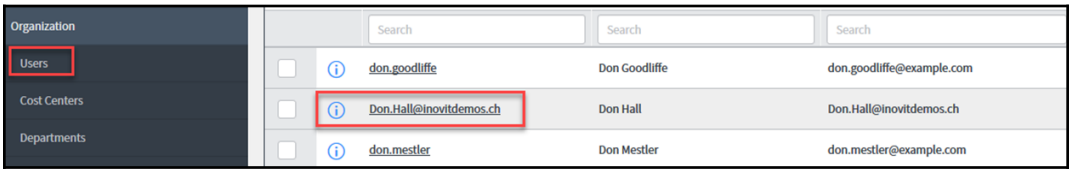
CorrelationId : aa3d4a7a-52df-4ed5-9a6b-b502fb958d9f

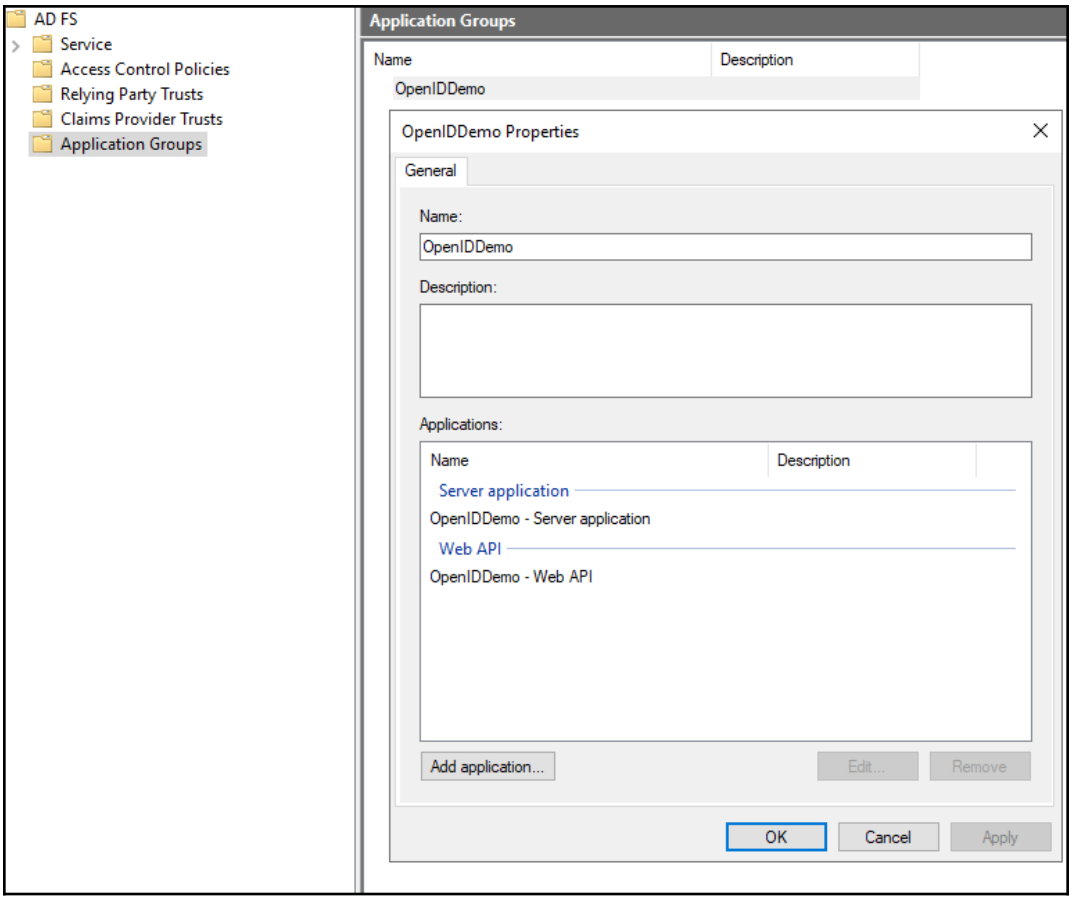
Category : Account Provisioning

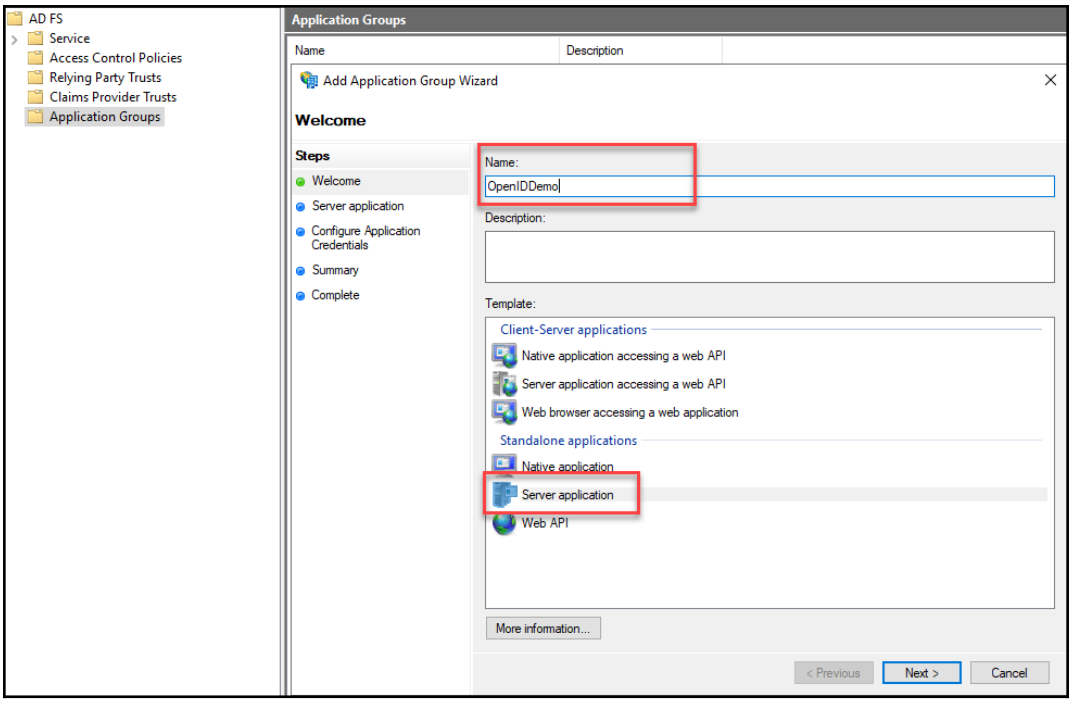
Activity Status

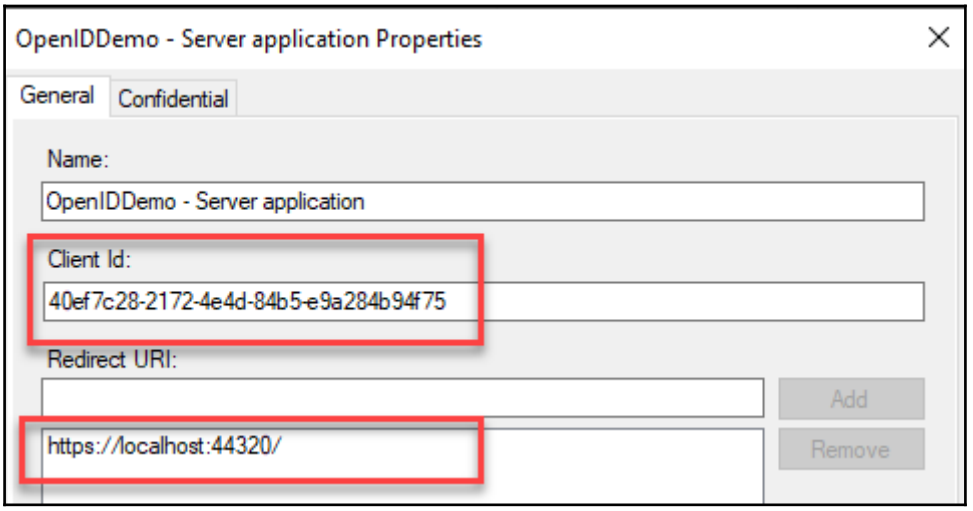
Status : Success

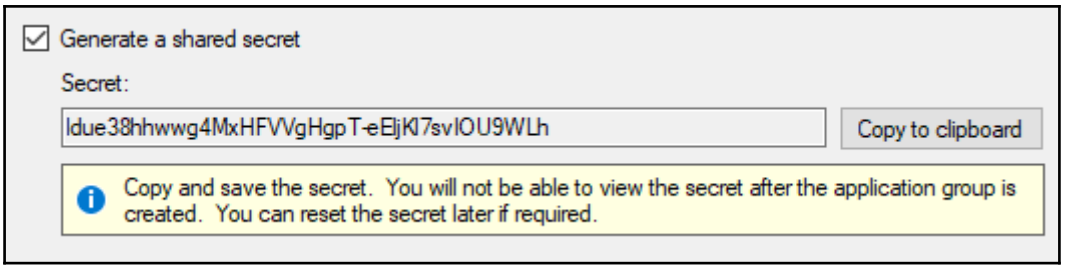
Reason : Retrieved User Don.Hall@inovitdemos.ch from Azure Active Directory



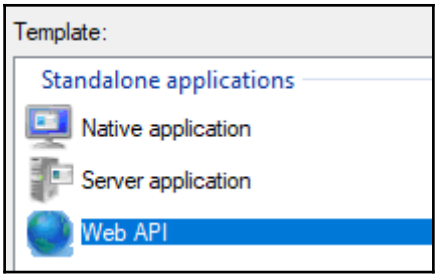

AD FS
Service
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Application Groups
Name
Description
OpenIDDemo
OpenIDDemo Properties
General
Name:
OpenIDDemo
Description:
Applications:
Name
Description
Server application
OpenIDDemo - Server application
Web API
OpenIDDemo - Web API
Add application...
Edit...
Remove
OK
Cancel
Apply

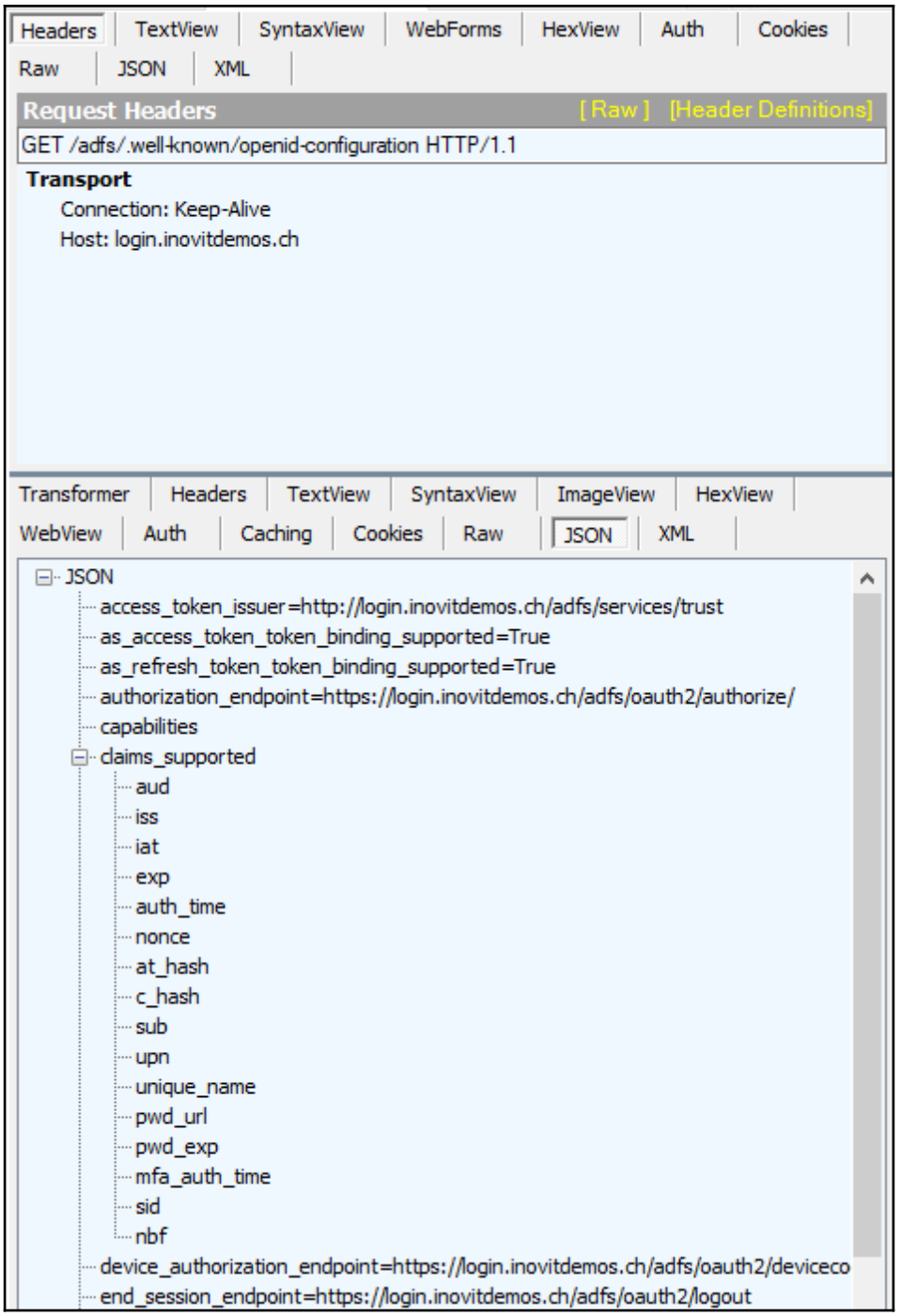

AD FS
Service
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Application Groups
Name
Description
Add Application Group Wizard
Welcome
Steps
Welcome
Server application
Configure Application Credentials
Summary
Complete
Name:
OpenIDDemo
Description:
Template:
Client-Server applications
Native application accessing a web API
Server application accessing a web API
Web browser accessing a web application
Standalone applications
Native application
Server application
Web API
More information...
< Previous
Next >
Cancel

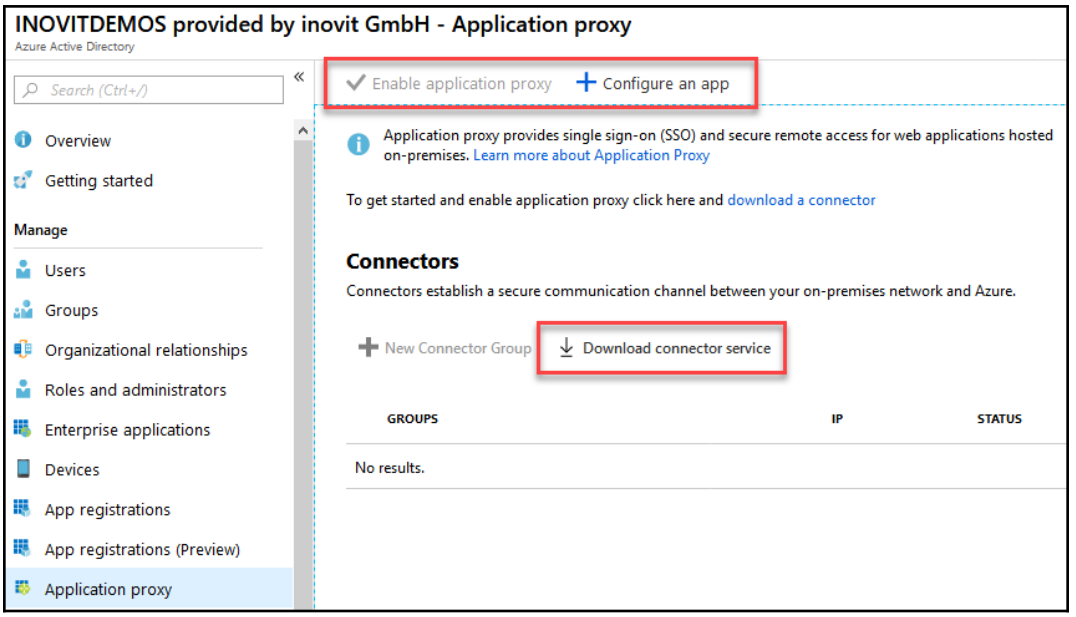

OpenIDDemo - Server application Properties
General
Confidential
Name:
OpenIDDemo - Server application
Client Id:
40ef7c28-2172-4e4d-84b5-e9a284b94f75
Redirect URI:
https://localhost:44320/
Add
Remove

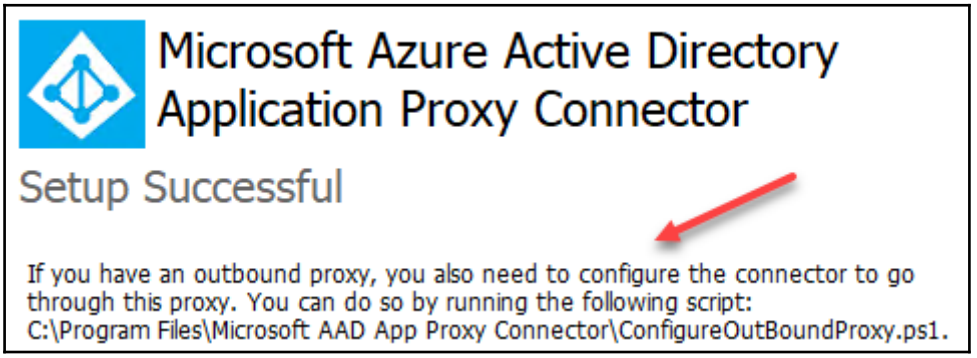

Generate a shared secret
Secret:
ldue38hhwwg4MxHFVVgHgpT-eEljKI7svIOU9WLh
Copy to clipboard
Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.


Add application...
Edit...
Remove

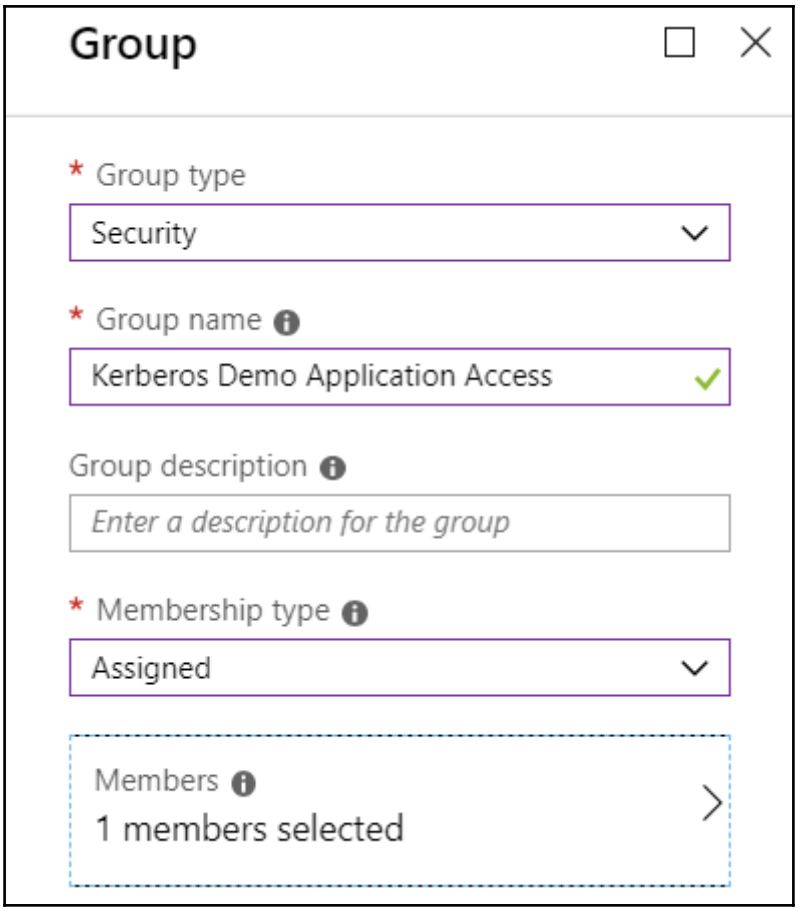

Template:
Standalone applications
Native application
Server application
Web API

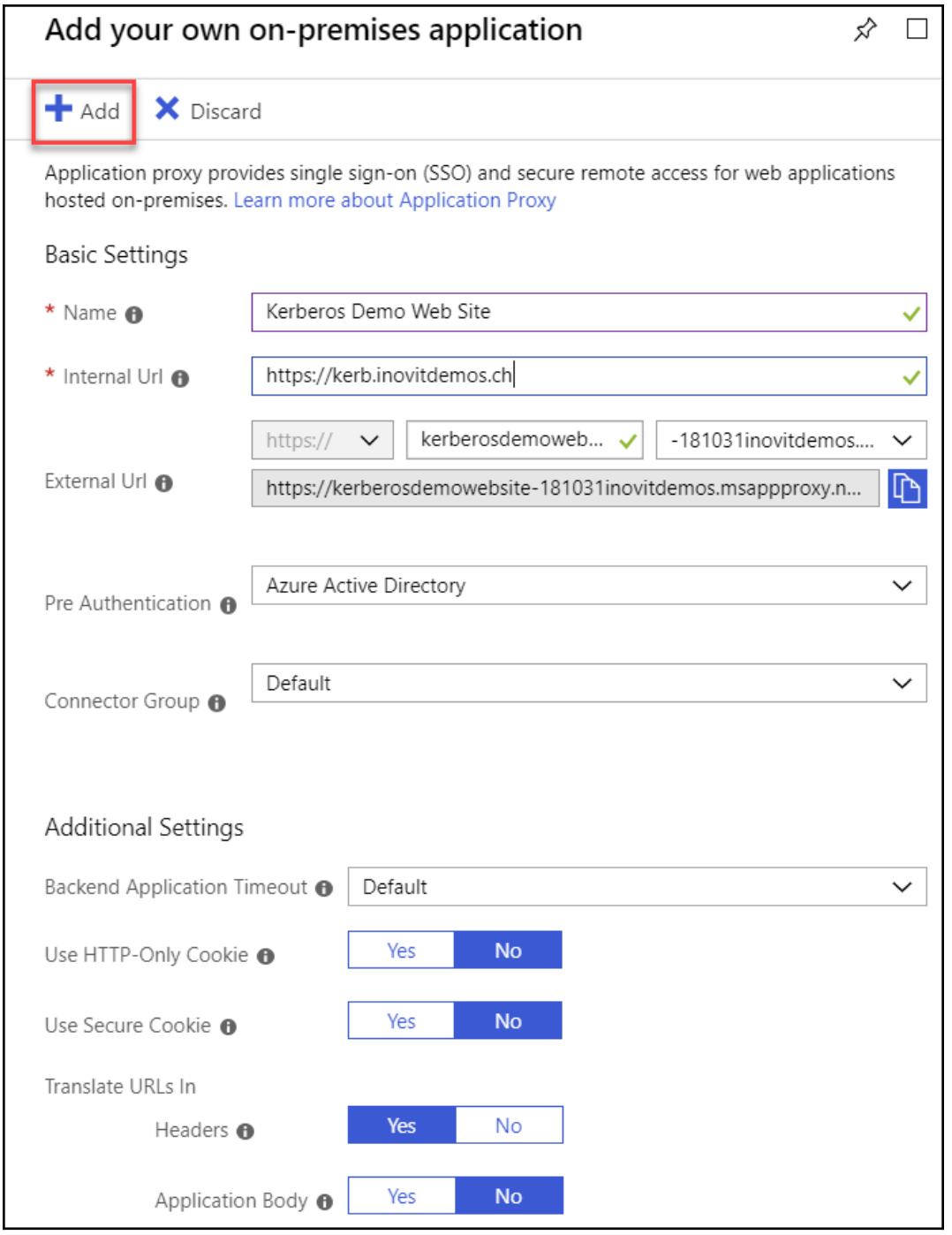

Headers
TextView
SyntaxView
WebForms
HexView
Auth
Cookies
Raw
JSON
XML
Request Headers
[Raw]
[Header Definitions]
GET /adfs/.well-known/openid-configuration HTTP/1.1
Transport
Connection: Keep-Alive
Host: login.inovitdemos.ch
Transformer
Headers
TextView
SyntaxView
ImageView
HexView
WebView
Auth
Caching
Cookies
Raw
JSON
XML
JSON
access_token_issuer=http://login.inovitdemos.ch/adfs/services/trust
as_access_token_token_binding_supported=True
as_refresh_token_token_binding_supported=True
authorization_endpoint=https://login.inovitdemos.ch/adfs/oauth2/authorize/
capabilities
claims_supported
aud
iss
iat
exp
auth_time
nonce
at_hash
c_hash
sub
upn
unique_name
pwd_url
pwd_exp
mfa_auth_time
sid
nbf
device_authorization_endpoint=https://login.inovitdemos.ch/adfs/oauth2/deviceco
end_session_endpoint=https://login.inovitdemos.ch/adfs/oauth2/logout

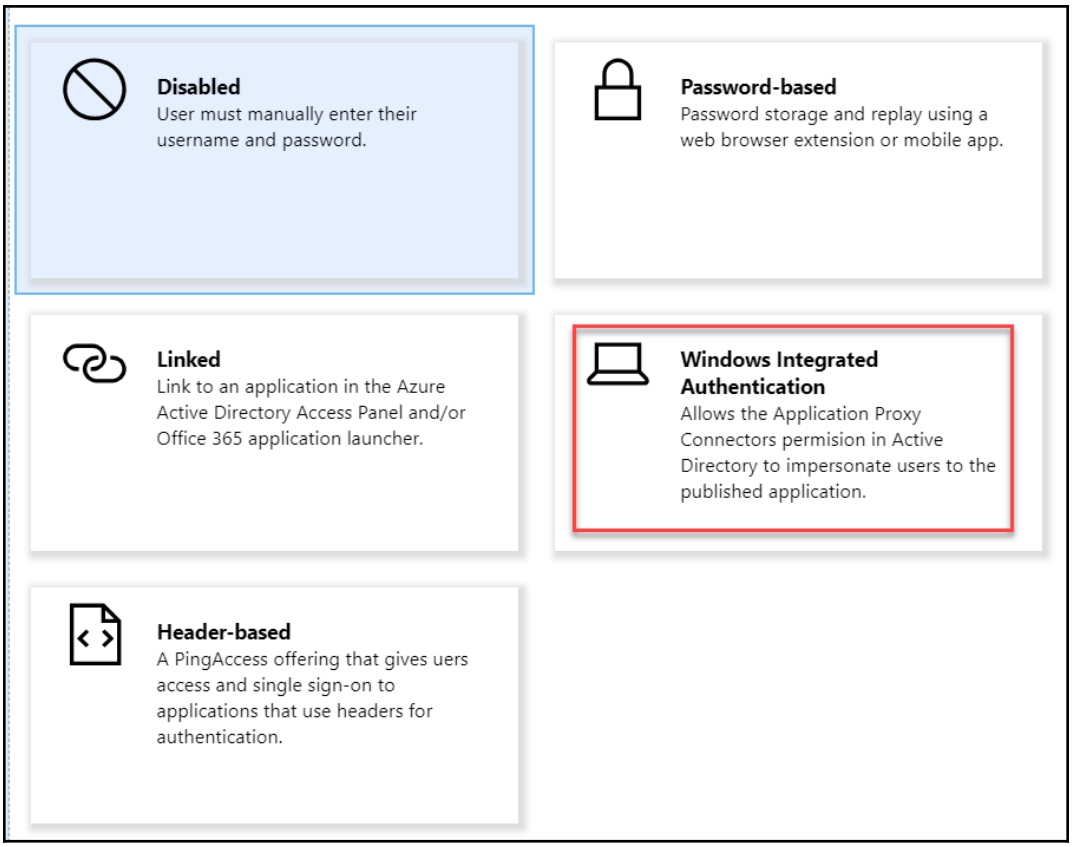

INOVITDEMOS provided by inovit GmbH - Application proxy
Azure Active Directory
Search (Ctrl+/)
Overview
Getting started
Manage
Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
App registrations (Preview)
Application proxy
Enable application proxy
Configure an app
Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy
To get started and enable application proxy click here and download a connector
Connectors
Connectors establish a secure communication channel between your on-premises network and Azure.
New Connector Group
Download connector service
GROUPS
IP
STATUS
No results.

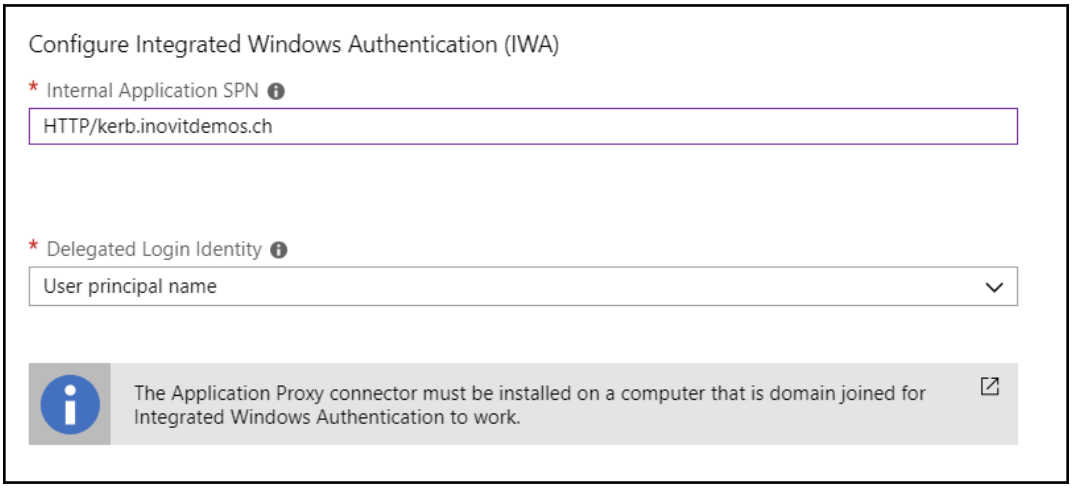

Microsoft Azure Active Directory
Application Proxy Connector
Setup Successful
If you have an outbound proxy, you also need to configure the connector to go through this proxy. You can do so by running the following script:
C:\Program Files\Microsoft AAD App Proxy Connector\ConfigureOutBoundProxy.ps1.


GROUPS
IP
STATUS
Default
INODEMOSAPP01.inovitdemos.ch
13.95.5.160
Active

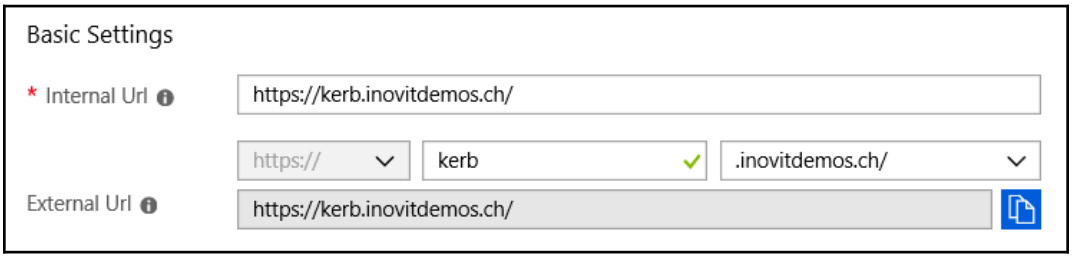

Group
* Group type
Security
* Group name
Kerberos Demo Application Access
Group description
Enter a description for the group
* Membership type
Assigned
Members
1 members selected

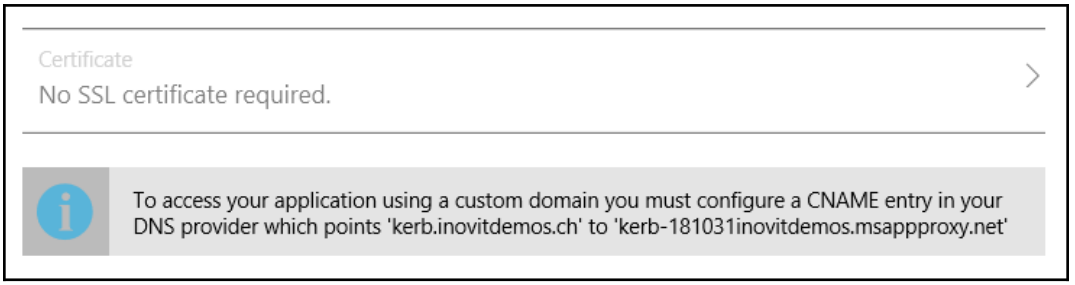

Add your own on-premises application
Add
Discard
Application proxy provides single sign-on (SSO) and secure remote access for web applications hosted on-premises. Learn more about Application Proxy
Basic Settings
* Name
Kerberos Demo Web Site
* Internal Url
https://kerb.inovitdemos.ch
https://
kerberosdemoweb...
-181031inovitdemos....
External Url
https://kerberosdemowebsite-181031inovitdemos.msappproxy.n...
Pre Authentication
Azure Active Directory
Connector Group
Default
Additional Settings
Backend Application Timeout
Default
Use HTTP-Only Cookie
Yes
No
Use Secure Cookie
Yes
No
Translate URLs In
Headers
Yes
No
Application Body
Yes
No

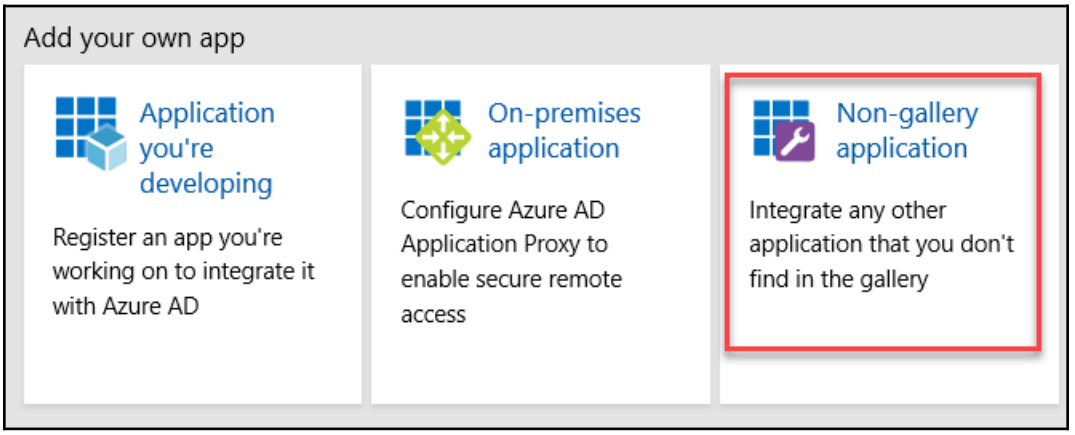

Disabled
User must manually enter their username and password.
Password-based
Password storage and replay using a web browser extension or mobile app.
Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.
Windows Integrated Authentication
Allows the Application Proxy Connectors permision in Active Directory to impersonate users to the published application.
Header-based
A PingAccess offering that gives uers access and single sign-on to applications that use headers for authentication.

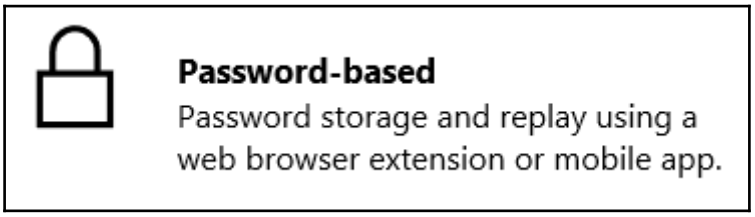

Configure Integrated Windows Authentication (IWA)
* Internal Application SPN
HTTP/kerb.inovitdemos.ch
* Delegated Login Identity
User principal name
The Application Proxy connector must be installed on a computer that is domain joined for Integrated Windows Authentication to work.

Authentication Method	**Negotiate (KERBEROS)**	Request.ServerVariables("AUTH_TYPE")
Identity	**INOVITDEMOS\donh**	Request.ServerVariables("AUTH_USER") or System.Threading.Thread.CurrentPrincipal.Identity
Windows identity	**INOVITDEMOS\svckrbapp**	System.Security.Principal.WindowsIdentity.Getcurrent









Sign-on URL

The URL where users enter their username and password to sign in to Forms-based Application Demo.

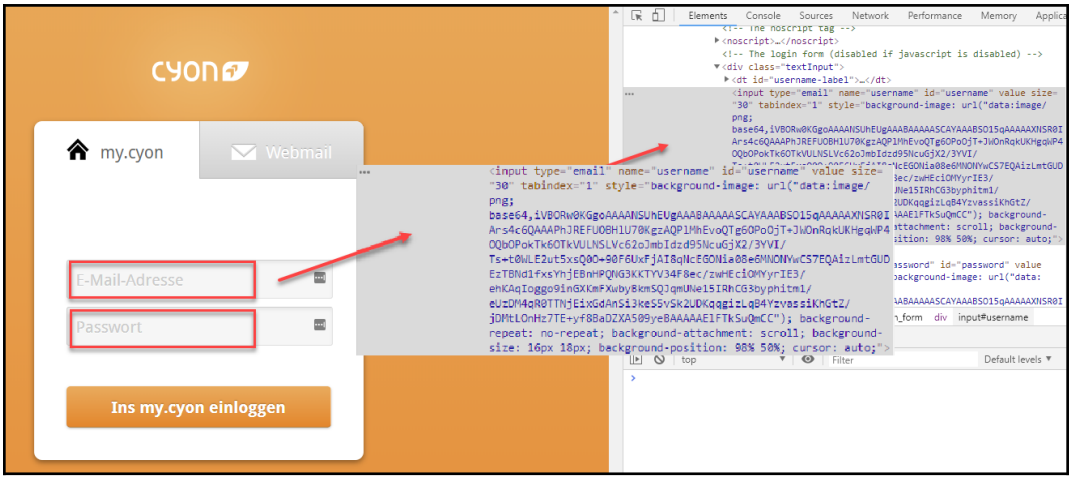
Sign on URL https://my.cyon.ch/

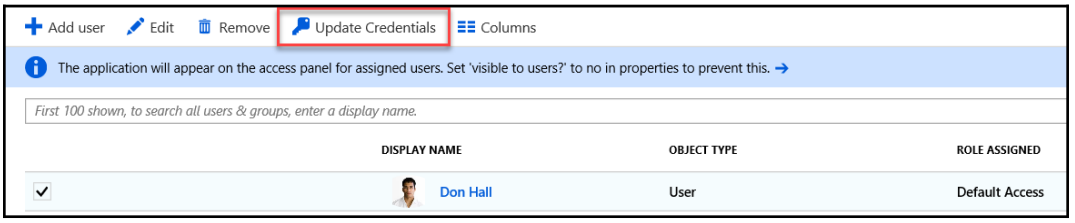
Forms-based Application Demo Configuration

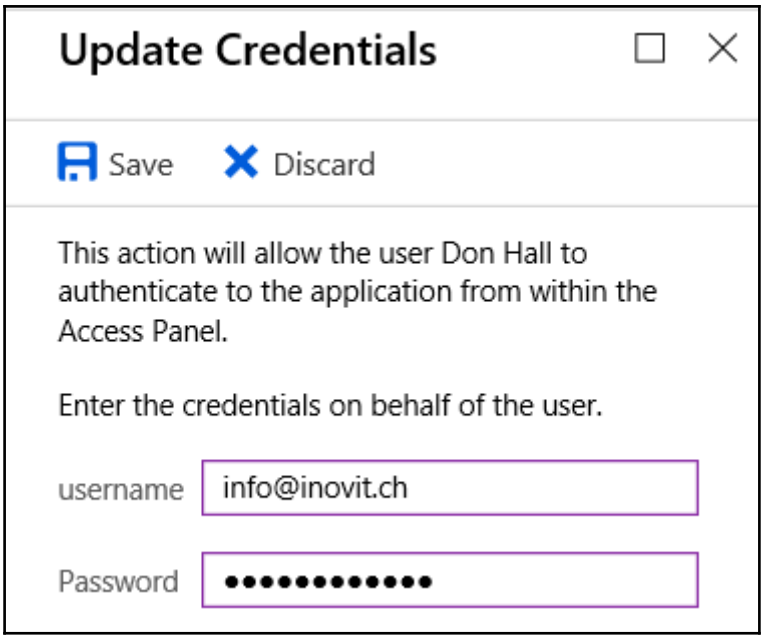
A sign-in form was successfully detected at the provided URL. You can now assign users to this app and test it using the Access Panel

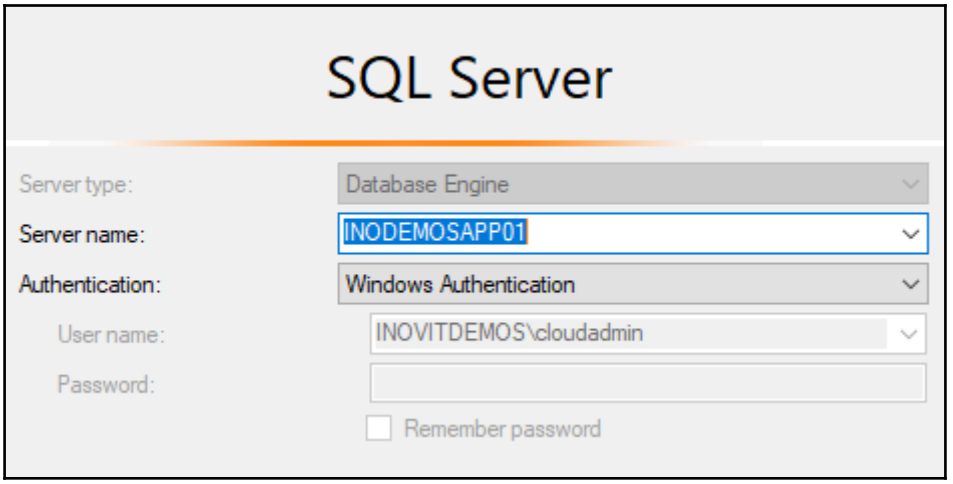
Use this option to try re-detecting the sign-in fields on the sign on URL above.
Configure Forms-based Application Demo Password Single Sign-on Settings

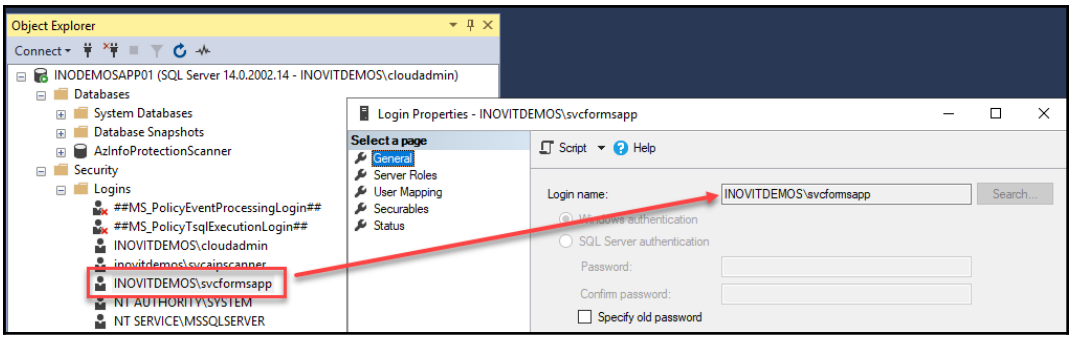
Advanced: View and edit sign in field labels

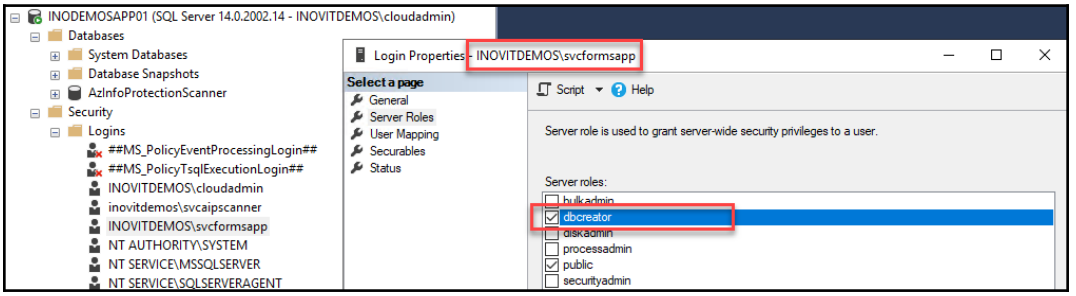


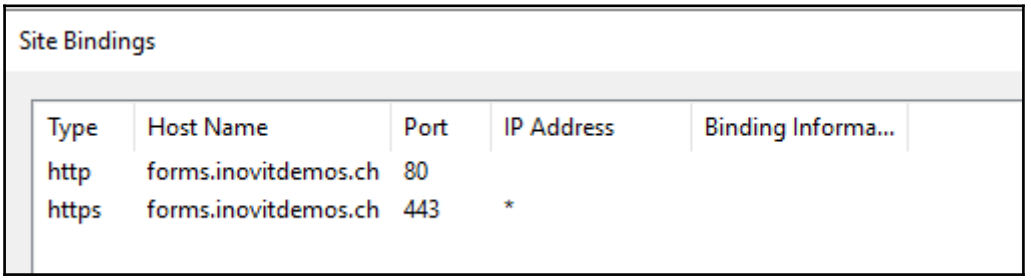


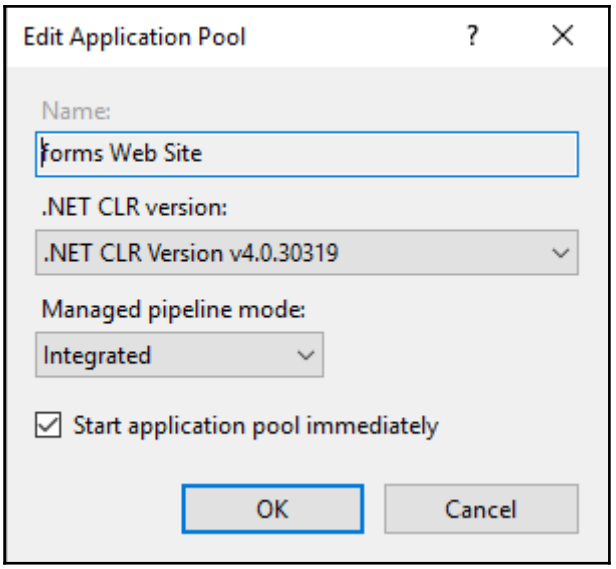

Update Credentials
Save
Discard
This action will allow the user Don Hall to authenticate to the application from within the Access Panel.
Enter the credentials on behalf of the user.
username
info@inovit.ch
Password
••••••••••••

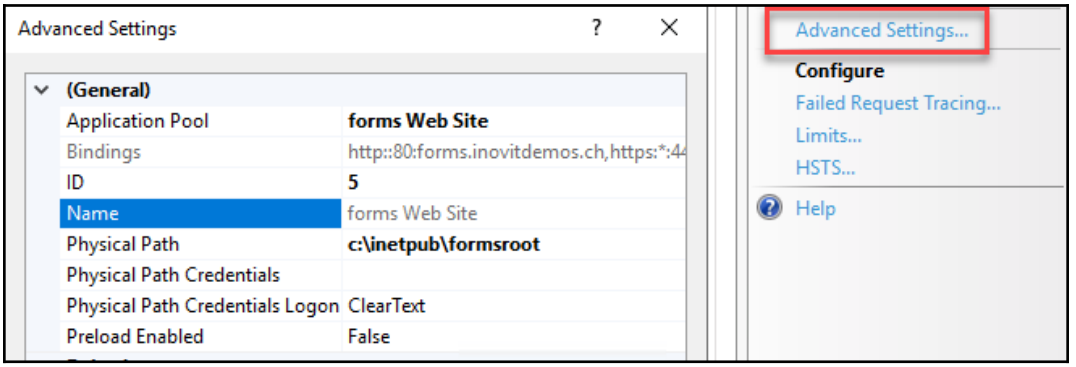

SQL Server
Server type:
Database Engine
Server name:
INODEMOSAPP01
Authentication:
Windows Authentication
User name:
INOVITDEMOS\cloudadmin
Password:
Remember password

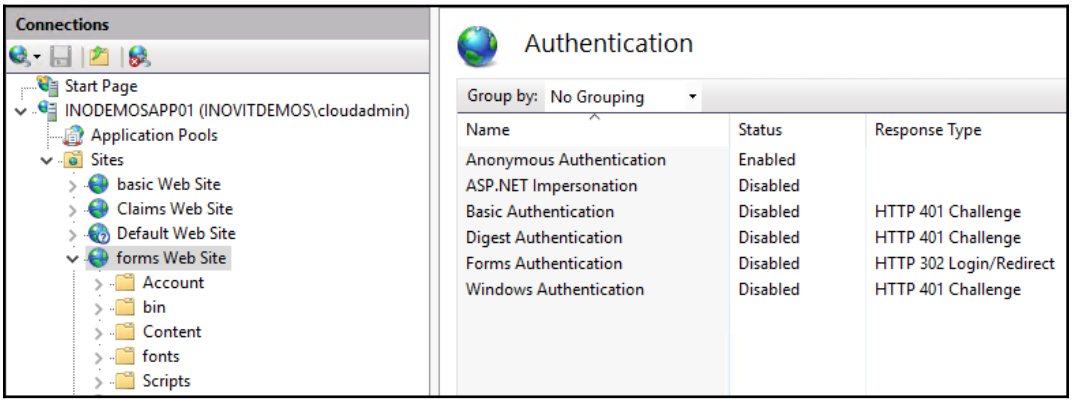

Object Explorer
Connect
INODEMOSAPP01 (SQL Server 14.0.2002.14 - INOVITDEMOS\cloudadmin)
Databases
System Databases
Database Snapshots
AzInfoProtectionScanner
Security
Logins
##MS_PolicyEventProcessingLogin##
##MS_PolicyTsqlExecutionLogin##
INOVITDEMOS\cloudadmin
inovitdemos\svcaipscanner
INOVITDEMOS\svcformsapp
NT AUTHORITY\SYSTEM
NT SERVICE\MSSQLSERVER
Login Properties - INOVITDEMOS\svcformsapp
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Login name:
INOVITDEMOS\svcformsapp
Search...
Windows authentication
SQL Server authentication
Password:
Confirm password:
Specify old password

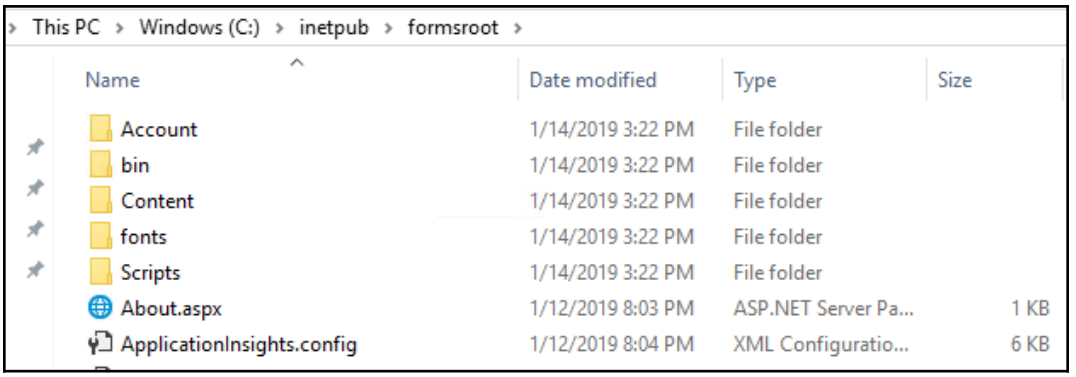

INODEMOSAPP01 (SQL Server 14.0.2002.14 - INOVITDEMOS\cloudadmin)
Databases
System Databases
Database Snapshots
AzInfoProtectionScanner
Security
Logins
##MS_PolicyEventProcessingLogin##
##MS_PolicyTsqlExecutionLogin##
INOVITDEMOS\cloudadmin
inovitdemos\svcaipscanner
INOVITDEMOS\svcformsapp
NT AUTHORITY\SYSTEM
NT SERVICE\MSSQLSERVER
NT SERVICE\SQLSERVERAGENT
Login Properties - INOVITDEMOS\svcformsapp
Select a page
General
Server Roles
User Mapping
Securables
Status
Script
Help
Server role is used to grant server-wide security privileges to a user.
Server roles:
bulkadmin
dbcreator
diskadmin
processadmin
public
securityadmin

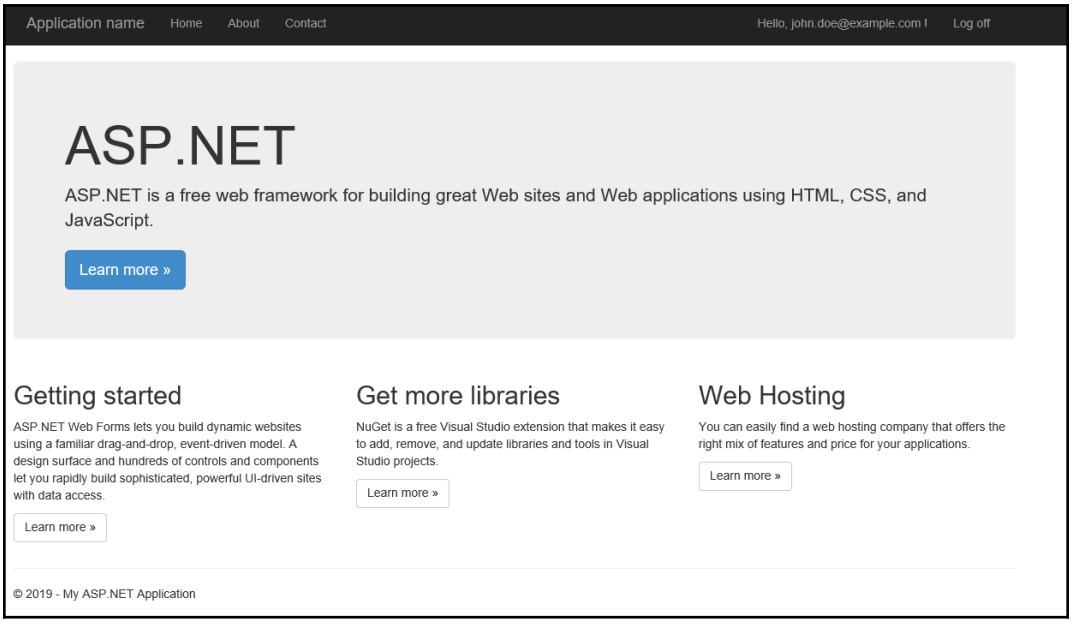

Site Bindings
Type
Host Name
Port
IP Address
Binding Informa...
http
forms.inovitdemos.ch
80
https
forms.inovitdemos.ch
443
*

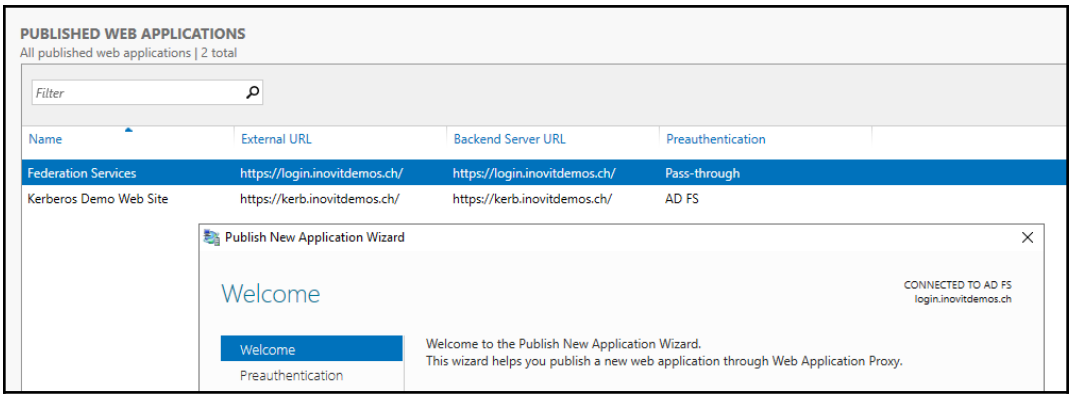

Edit Application Pool
Name:
forms Web Site
.NET CLR version:
.NET CLR Version v4.0.30319
Managed pipeline mode:
Integrated
Start application pool immediately
OK
Cancel

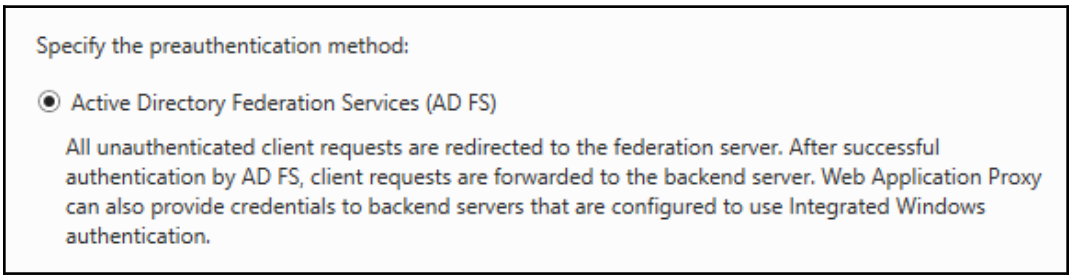

Advanced Settings
(General)
Application Pool
forms Web Site
Bindings
http::80:forms.inovitdemos.ch,https:*:44
ID
5
Name
forms Web Site
Physical Path
c:\inetpub\formsroot
Physical Path Credentials
Physical Path Credentials Logon
ClearText
Preload Enabled
False
Advanced Settings...
Configure
Failed Request Tracing...
Limits...
HSTS...
Help

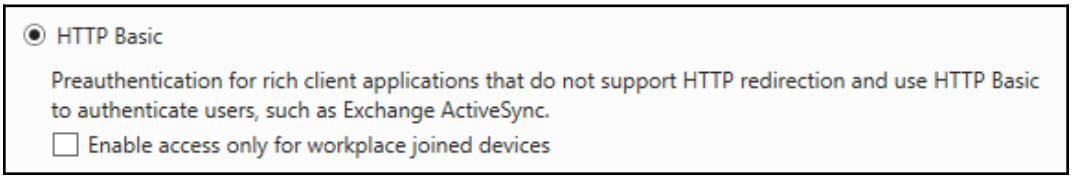

Connections
Start Page
INODEMOSAPP01 (INOVITDEMOS\cloudadmin)
Application Pools
Sites
basic Web Site
Claims Web Site
Default Web Site
forms Web Site
Account
bin
Content
fonts
Scripts
Authentication
Group by: No Grouping
Name
Status
Response Type
Anonymous Authentication
Enabled
ASP.NET Impersonation
Disabled
Basic Authentication
Disabled
HTTP 401 Challenge
Digest Authentication
Disabled
HTTP 401 Challenge
Forms Authentication
Disabled
HTTP 302 Login/Redirect
Windows Authentication
Disabled
HTTP 401 Challenge

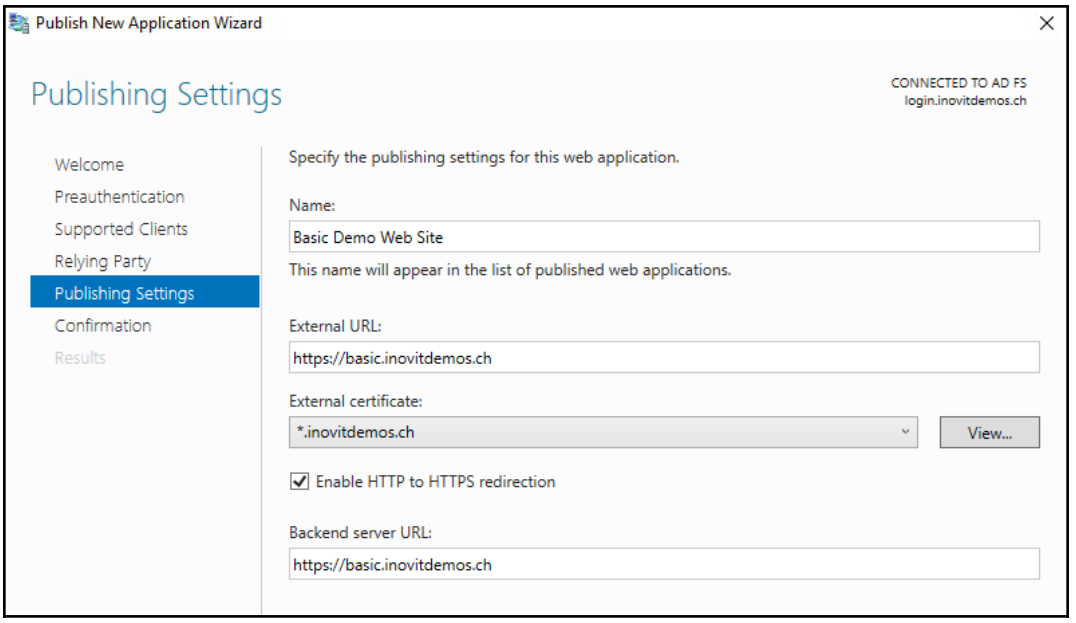

This PC › Windows (C:) › inetpub › formsroot ›
Name
Date modified
Type
Size
Account
1/14/2019 3:22 PM
File folder
bin
1/14/2019 3:22 PM
File folder
Content
1/14/2019 3:22 PM
File folder
fonts
1/14/2019 3:22 PM
File folder
Scripts
1/14/2019 3:22 PM
File folder
About.aspx
1/12/2019 8:03 PM
ASP.NET Server Pa...
1 KB
ApplicationInsights.config
1/12/2019 8:04 PM
XML Configuratio...
6 KB

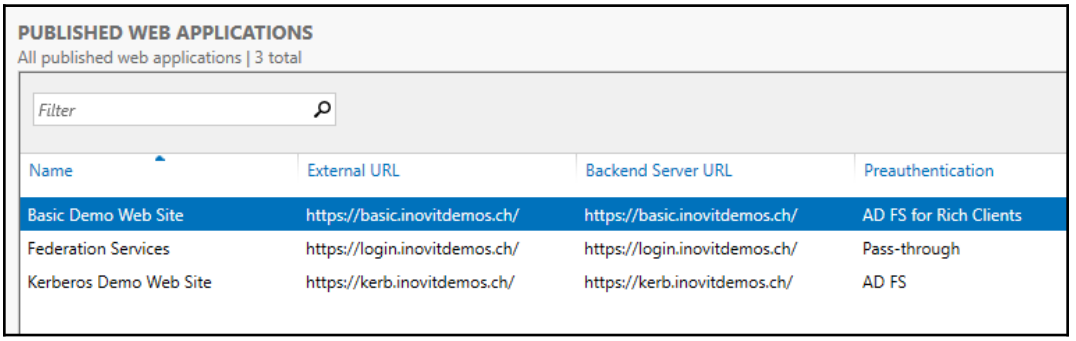

Application name
Home
About
Contact
Hello, john.doe@example.com !
Log off
ASP.NET
ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS, and JavaScript.
Learn more »
Getting started
ASP.NET Web Forms lets you build dynamic websites using a familiar drag-and-drop, event-driven model. A design surface and hundreds of controls and components let you rapidly build sophisticated, powerful UI-driven sites with data access.
Learn more »
Get more libraries
NuGet is a free Visual Studio extension that makes it easy to add, remove, and update libraries and tools in Visual Studio projects.
Learn more »
Web Hosting
You can easily find a web hosting company that offers the right mix of features and price for your applications.
Learn more »
© 2019 - My ASP.NET Application

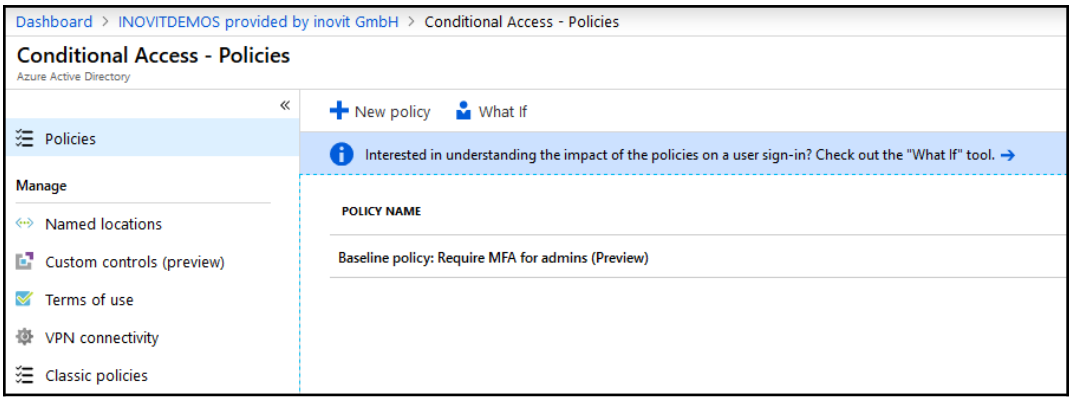

PUBLISHED WEB APPLICATIONS
All published web applications | 2 total
Filter
Name
External URL
Backend Server URL
Preauthentication
Federation Services
https://login.inovitdemos.ch/
https://login.inovitdemos.ch/
Pass-through
Kerberos Demo Web Site
https://kerb.inovitdemos.ch/
https://kerb.inovitdemos.ch/
AD FS
Publish New Application Wizard
Welcome
CONNECTED TO AD FS
login.inovitdemos.ch
Welcome
Preauthentication
Welcome to the Publish New Application Wizard.
This wizard helps you publish a new web application through Web Application Proxy.

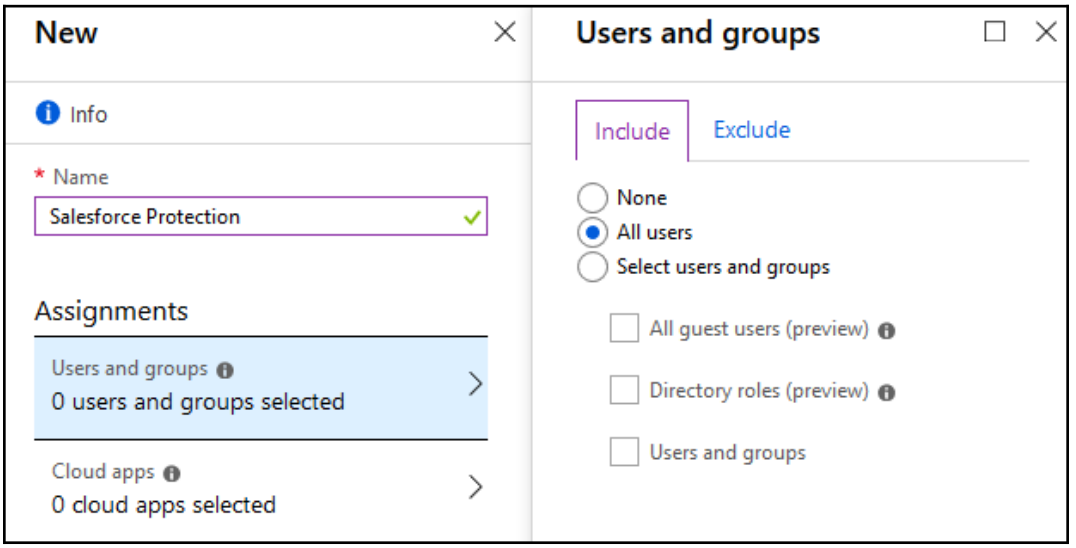

Specify the preauthentication method:
Active Directory Federation Services (AD FS)
All unauthenticated client requests are redirected to the federation server. After successful authentication by AD FS, client requests are forwarded to the backend server. Web Application Proxy can also provide credentials to backend servers that are configured to use Integrated Windows authentication.

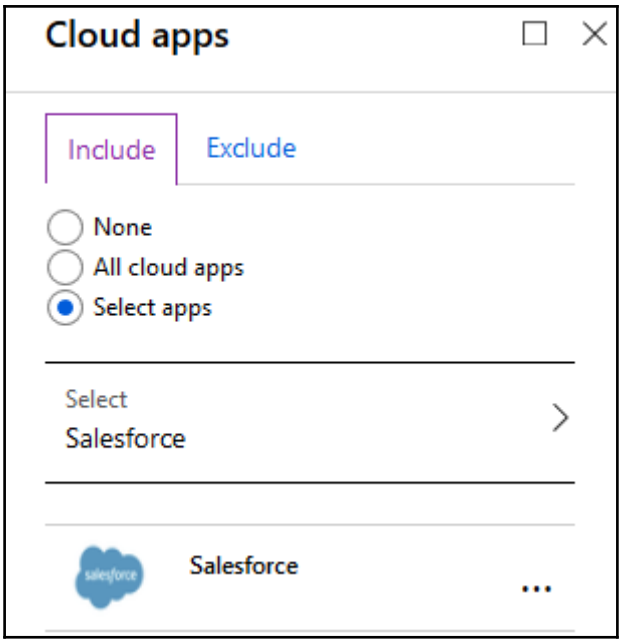

HTTP Basic
Preauthentication for rich client applications that do not support HTTP redirection and use HTTP Basic to authenticate users, such as Exchange ActiveSync.
Enable access only for workplace joined devices

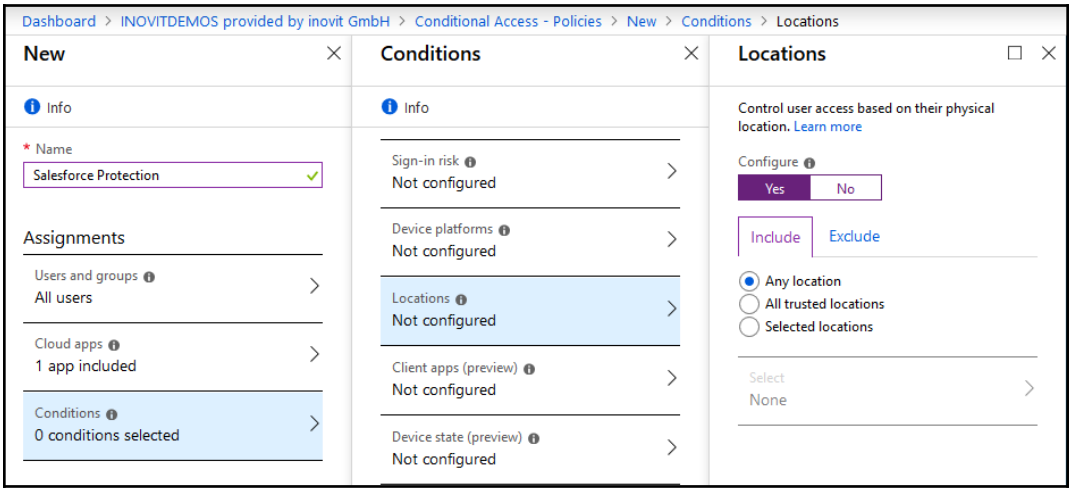

Publish New Application Wizard
Publishing Settings
CONNECTED TO AD FS
login.inovitdemos.ch
Welcome
Preauthentication
Supported Clients
Relying Party
Publishing Settings
Confirmation
Results
Specify the publishing settings for this web application.
Name:
Basic Demo Web Site
This name will appear in the list of published web applications.
External URL:
https://basic.inovitdemos.ch
External certificate:
*.inovitdemos.ch
View...
Enable HTTP to HTTPS redirection
Backend server URL:
https://basic.inovitdemos.ch

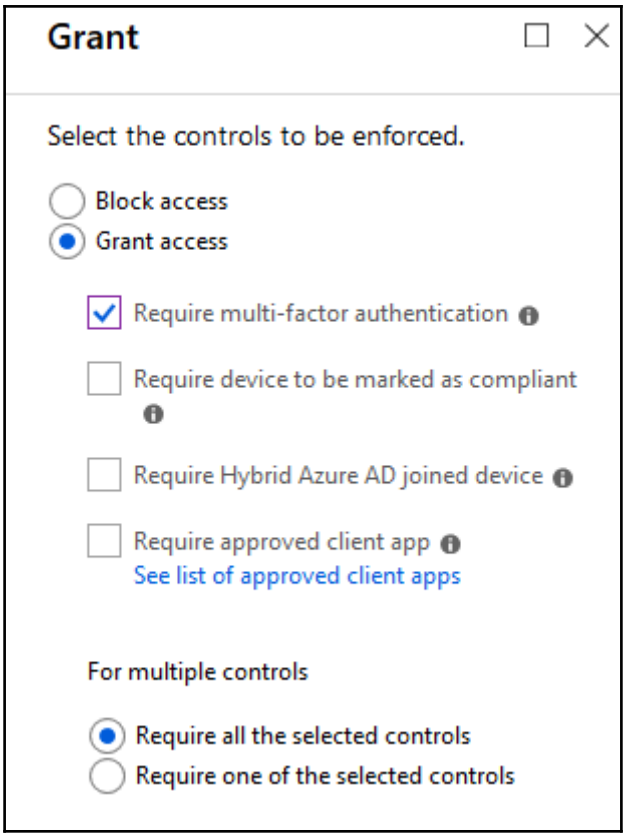

PUBLISHED WEB APPLICATIONS
All published web applications | 3 total
Filter
Name
External URL
Backend Server URL
Preauthentication
Basic Demo Web Site
https://basic.inovitdemos.ch/
https://basic.inovitdemos.ch/
AD FS for Rich Clients
Federation Services
https://login.inovitdemos.ch/
https://login.inovitdemos.ch/
Pass-through
Kerberos Demo Web Site
https://kerb.inovitdemos.ch/
https://kerb.inovitdemos.ch/
AD FS


Dashboard > INOVITDEMOS provided by inovit GmbH > Conditional Access - Policies
Conditional Access - Policies
Azure Active Directory
Policies
Manage
Named locations
Custom controls (preview)
Terms of use
VPN connectivity
Classic policies
New policy
What If
Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool.
POLICY NAME
Baseline policy: Require MFA for admins (Preview)

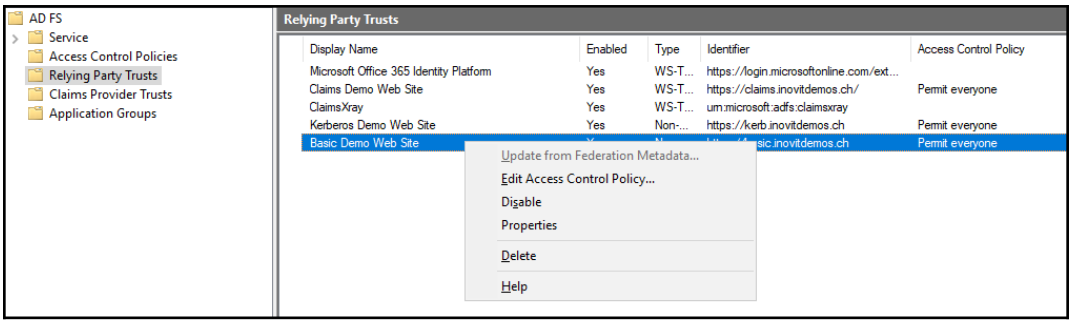

New
Info
* Name
Salesforce Protection
Assignments
Users and groups
0 users and groups selected
Cloud apps
0 cloud apps selected
Users and groups
Include
Exclude
None
All users
Select users and groups
All guest users (preview)
Directory roles (preview)
Users and groups

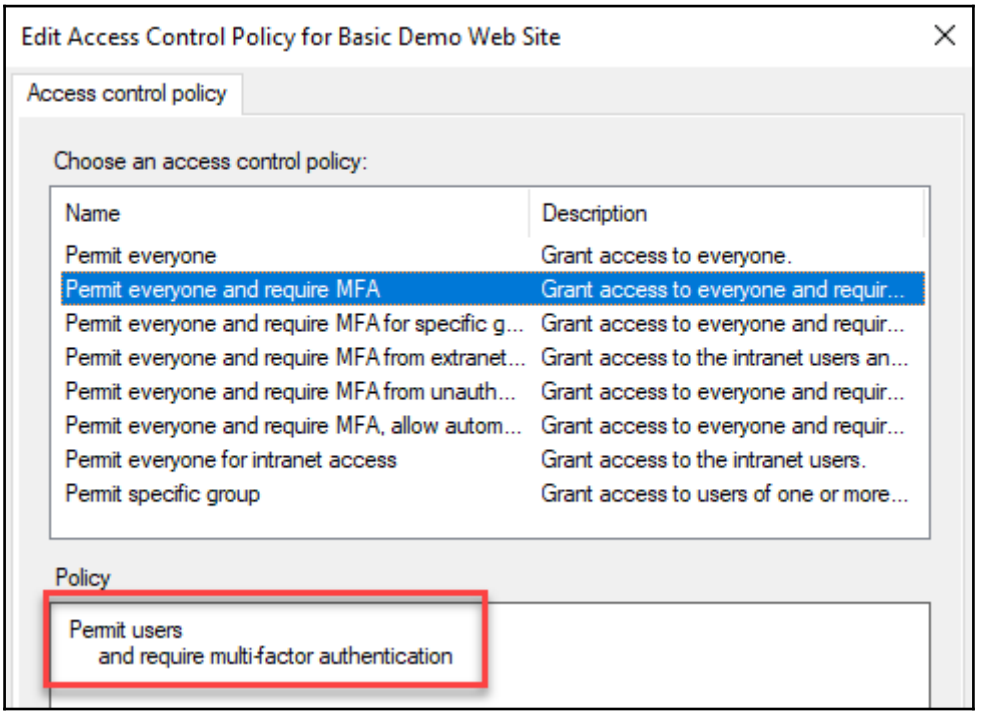

Cloud apps
Include
Exclude
None
All cloud apps
Select apps
Select
Salesforce
Salesforce

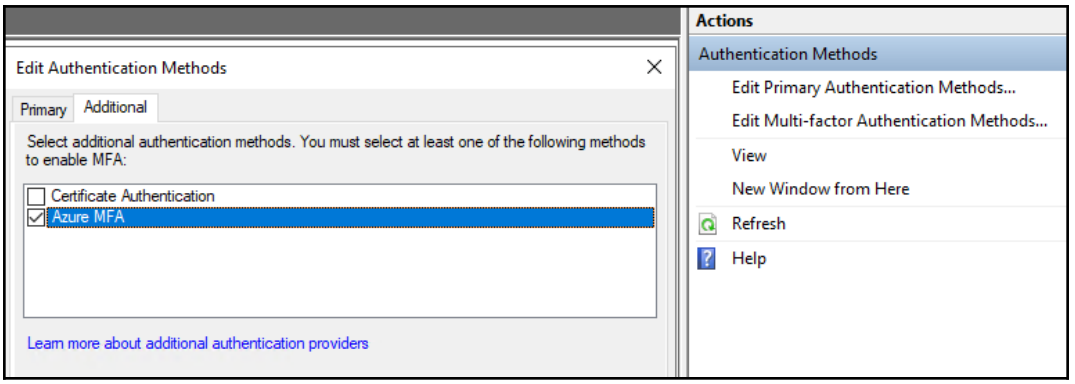

Dashboard > INOVITDEMOS provided by inovit GmbH > Conditional Access - Policies > New > Conditions > Locations
New
Info
* Name
Salesforce Protection
Assignments
Users and groups
All users
Cloud apps
1 app included
Conditions
0 conditions selected
Conditions
Info
Sign-in risk
Not configured
Device platforms
Not configured
Locations
Not configured
Client apps (preview)
Not configured
Device state (preview)
Not configured
Locations
Control user access based on their physical location. Learn more
Configure
Yes
No
Include
Exclude
Any location
All trusted locations
Selected locations
Select
None



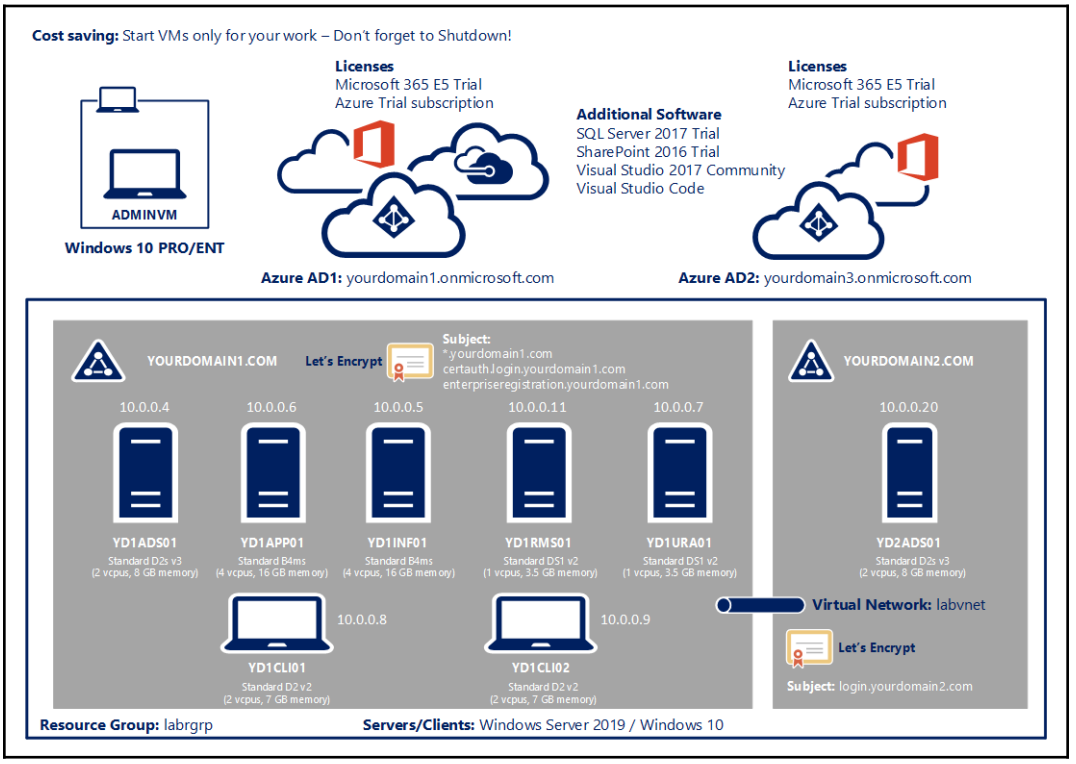
POLICY NAME
Baseline policy: Require MFA for admins (Preview)
Salesforce Protection

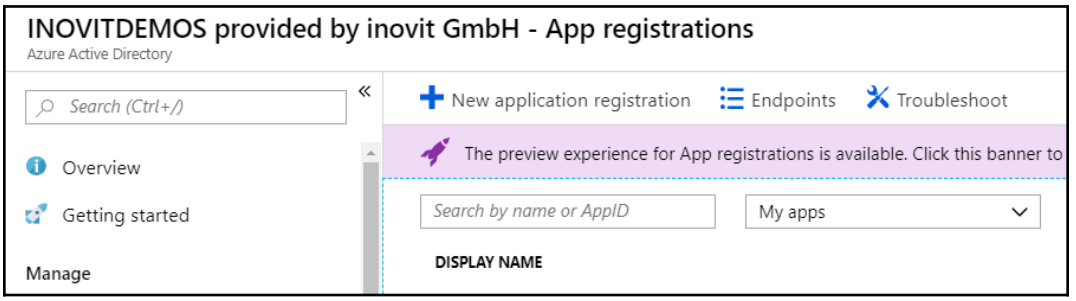

AD FS
Service
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Relying Party Trusts
Display Name
Enabled
Type
Identifier
Access Control Policy
Microsoft Office 365 Identity Platform
Yes
WS-T...
https://login.microsoftonline.com/ext...
Claims Demo Web Site
Yes
WS-T...
https://claims.inovitdemos.ch/
Permit everyone
ClaimsXray
Yes
WS-T...
urn:microsoft:adfs:claimsxray
Kerberos Demo Web Site
Yes
Non-...
https://kerb.inovitdemos.ch
Permit everyone
Basic Demo Web Site
Permit everyone
Update from Federation Metadata...
Edit Access Control Policy...
Disable
Properties
Delete
Help

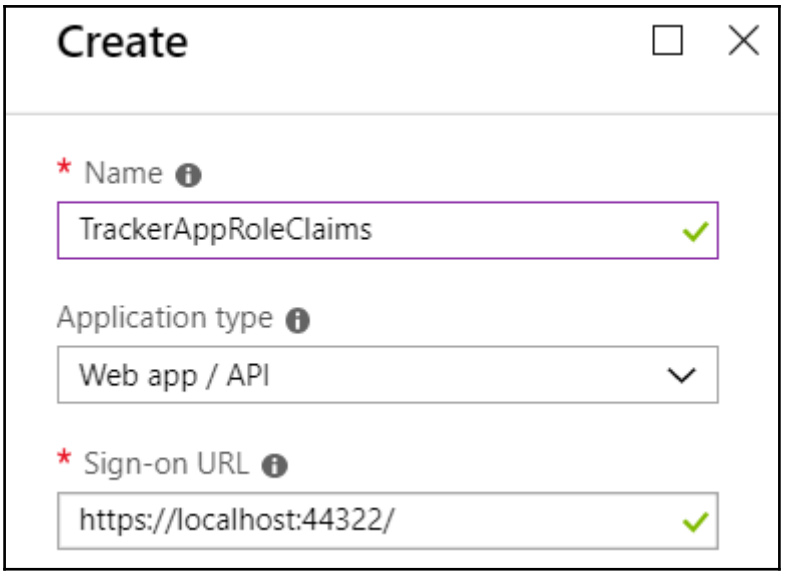

Edit Access Control Policy for Basic Demo Web Site
Access control policy
Choose an access control policy:
Name
Description
Permit everyone
Grant access to everyone.
Permit everyone and require MFA
Grant access to everyone and requir...
Permit everyone and require MFA for specific g...
Grant access to everyone and requir...
Permit everyone and require MFA from extranet...
Grant access to the intranet users an...
Permit everyone and require MFA from unauth...
Grant access to everyone and requir...
Permit everyone and require MFA, allow autom...
Grant access to everyone and requir...
Permit everyone for intranet access
Grant access to the intranet users.
Permit specific group
Grant access to users of one or more...
Policy
Permit users
and require multi-factor authentication

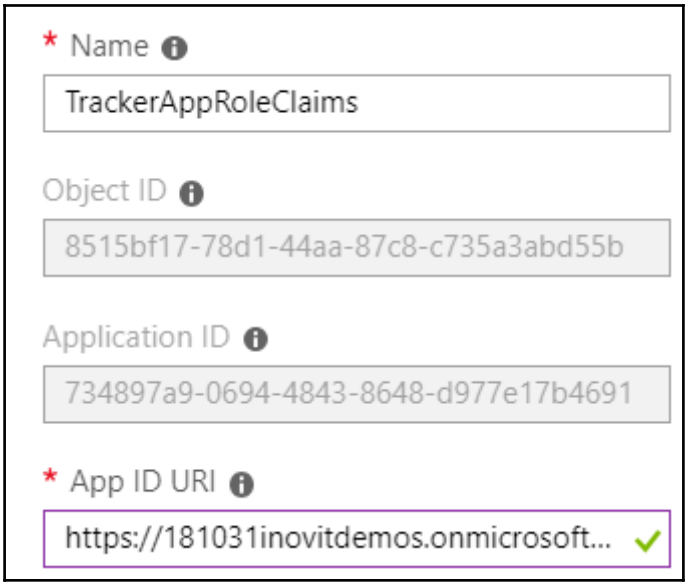

Edit Authentication Methods
Primary
Additional
Select additional authentication methods. You must select at least one of the following methods to enable MFA:
Certificate Authentication
Azure MFA
Learn more about additional authentication providers
Actions
Authentication Methods
Edit Primary Authentication Methods...
Edit Multi-factor Authentication Methods...
View
New Window from Here
Refresh
Help

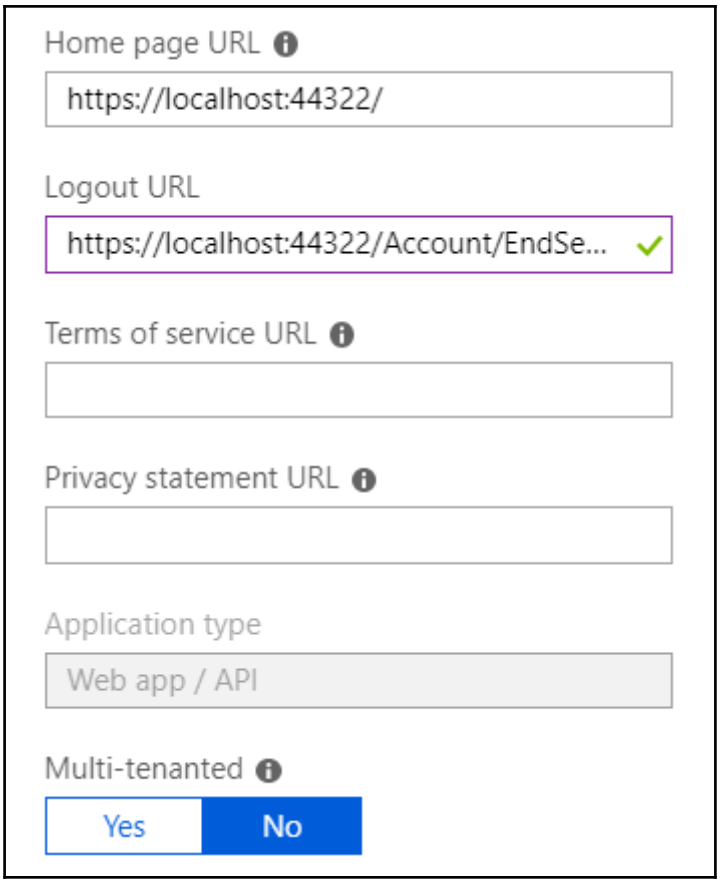
Chapter 9: Deploying Additional Applications on Azure AD

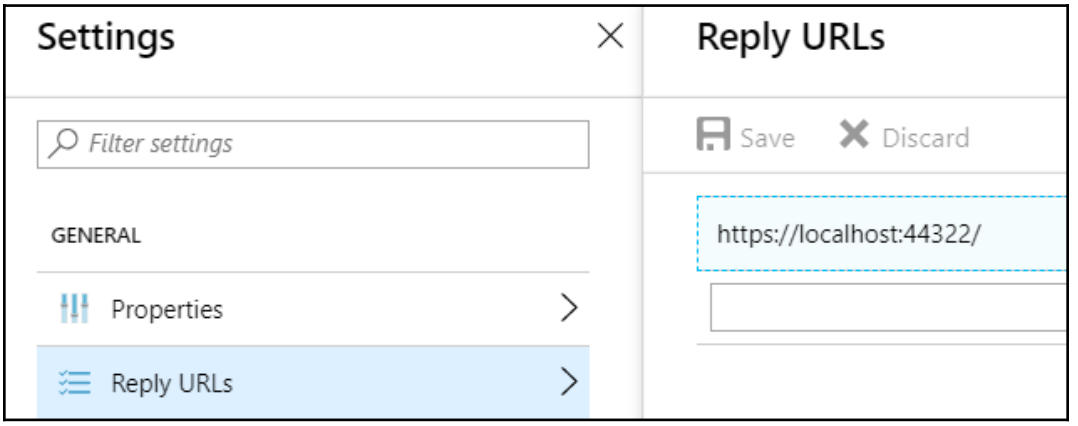


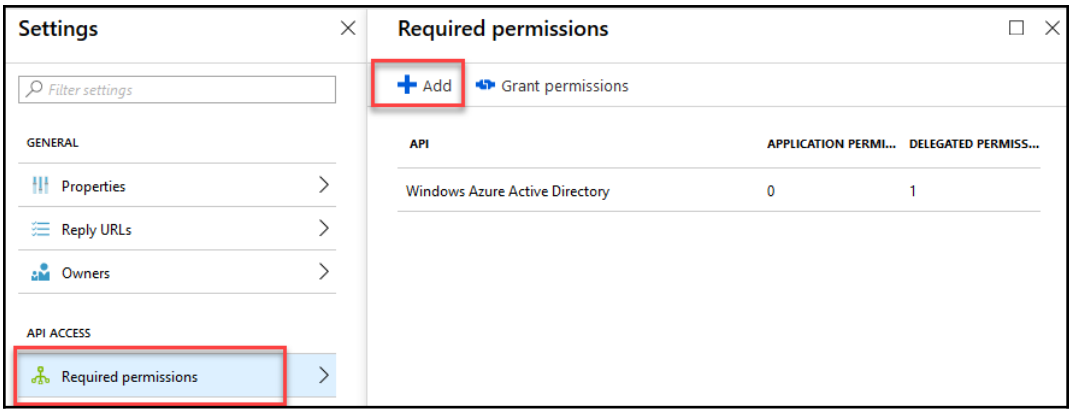


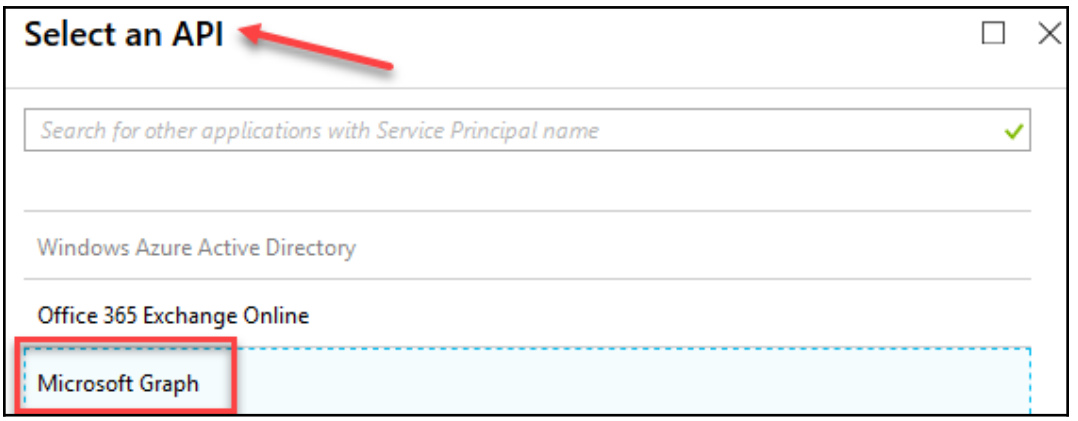

Create
* Name
TrackerAppRoleClaims
Application type
Web app / API
* Sign-on URL
https://localhost:44322/

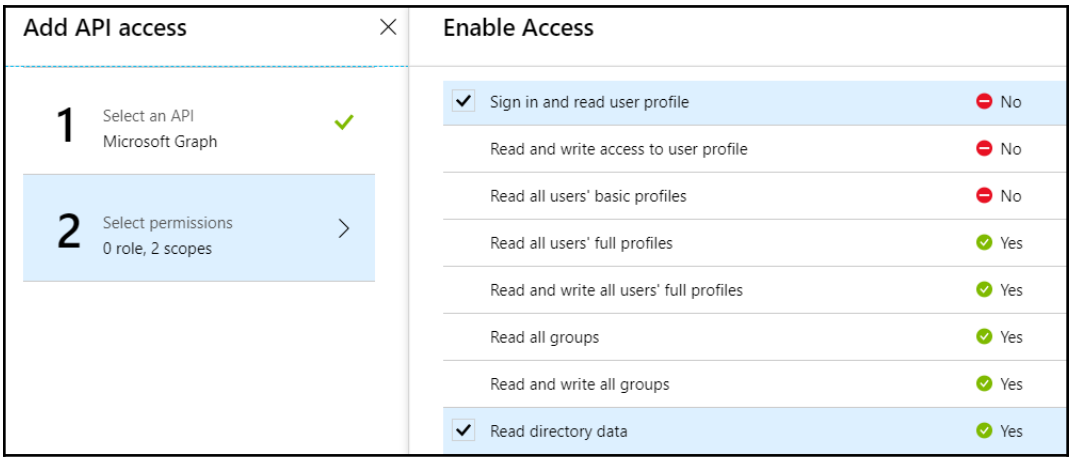

* Name
TrackerAppRoleClaims
Object ID
8515bf17-78d1-44aa-87c8-c735a3abd55b
Application ID
734897a9-0694-4843-8648-d977e17b4691
* App ID URI
https://181031inovitdemos.onmicrosoft...

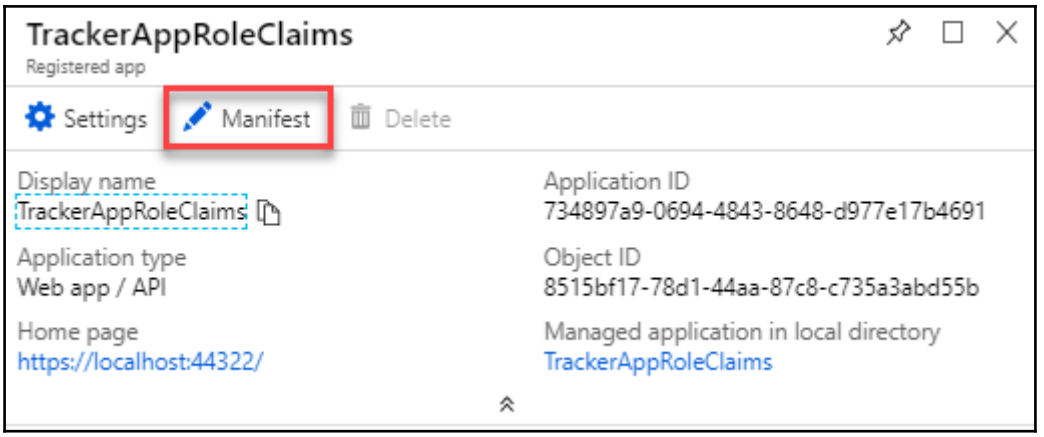

Home page URL
https://localhost:44322/
Logout URL
https://localhost:44322/Account/EndSe...
Terms of service URL
Privacy statement URL
Application type
Web app / API
Multi-tenanted
Yes
No


Settings
Filter settings
GENERAL
Properties
Reply URLs
Reply URLs
Save
Discard
https://localhost:44322/

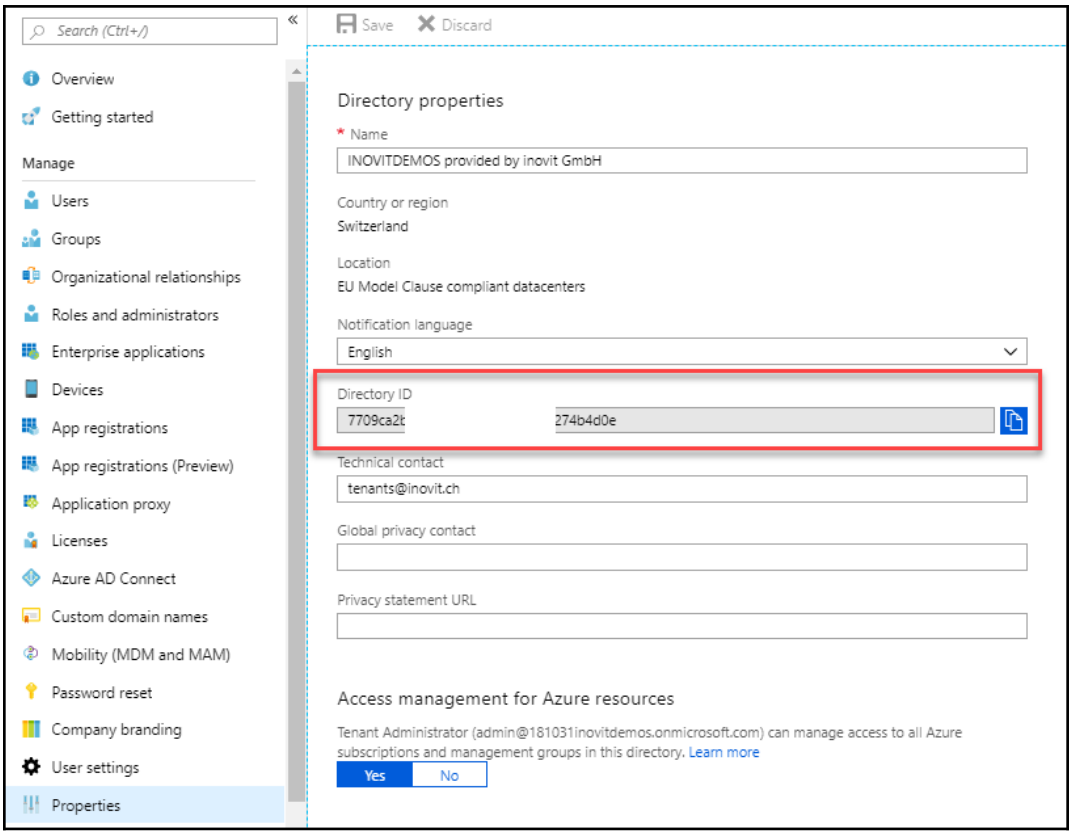

Settings
Filter settings
GENERAL
Properties
Reply URLs
Owners
API ACCESS
Required permissions
Required permissions
Add
Grant permissions
API
APPLICATION PERMI...
DELEGATED PERMISS...
Windows Azure Active Directory
0
1


Select an API
Search for other applications with Service Principal name
Windows Azure Active Directory
Office 365 Exchange Online
Microsoft Graph

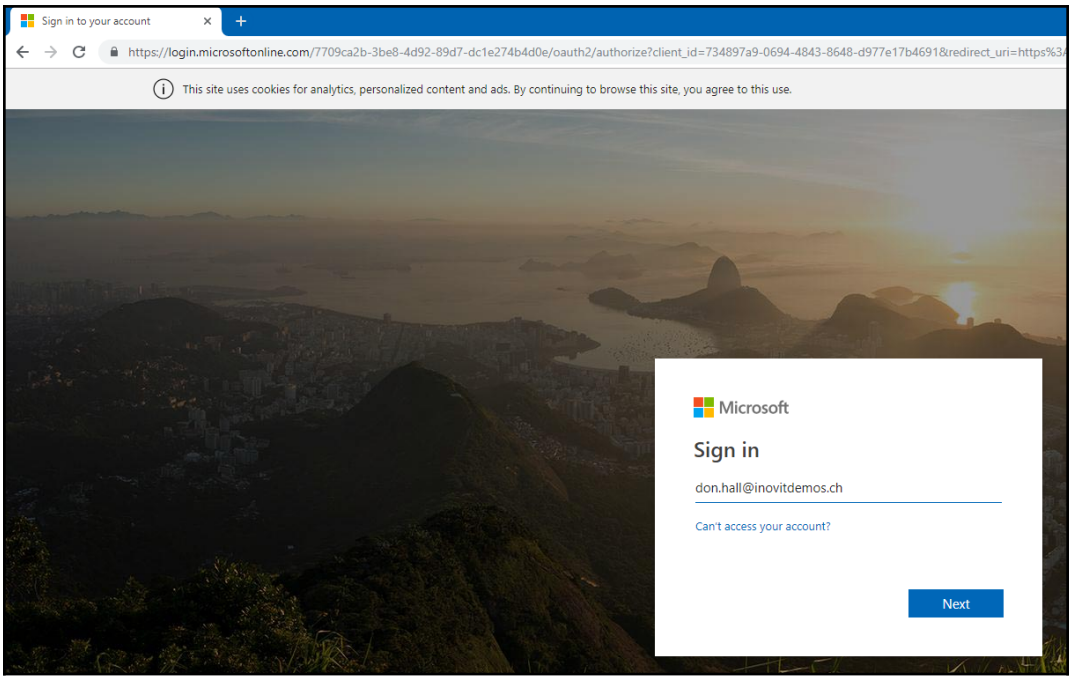

Add API access
1
Select an API
Microsoft Graph
2
Select permissions
0 role, 2 scopes
Enable Access
Sign in and read user profile
No
Read and write access to user profile
No
Read all users' basic profiles
No
Read all users' full profiles
Yes
Read and write all users' full profiles
Yes
Read all groups
Yes
Read and write all groups
Yes
Read directory data
Yes

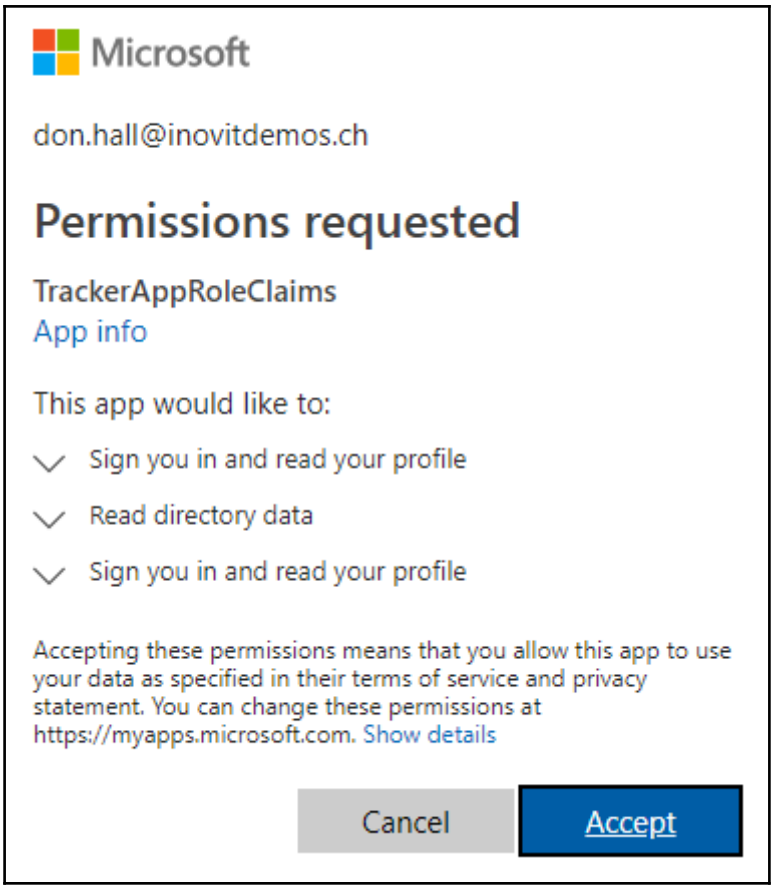

TrackerAppRoleClaims
Registered app
Settings
Manifest
Delete
Display name
TrackerAppRoleClaims
Application ID
734897a9-0694-4843-8648-d977e17b4691
Application type
Web app / API
Object ID
8515bf17-78d1-44aa-87c8-c735a3abd55b
Home page
https://localhost:44322/
Managed application in local directory
TrackerAppRoleClaims

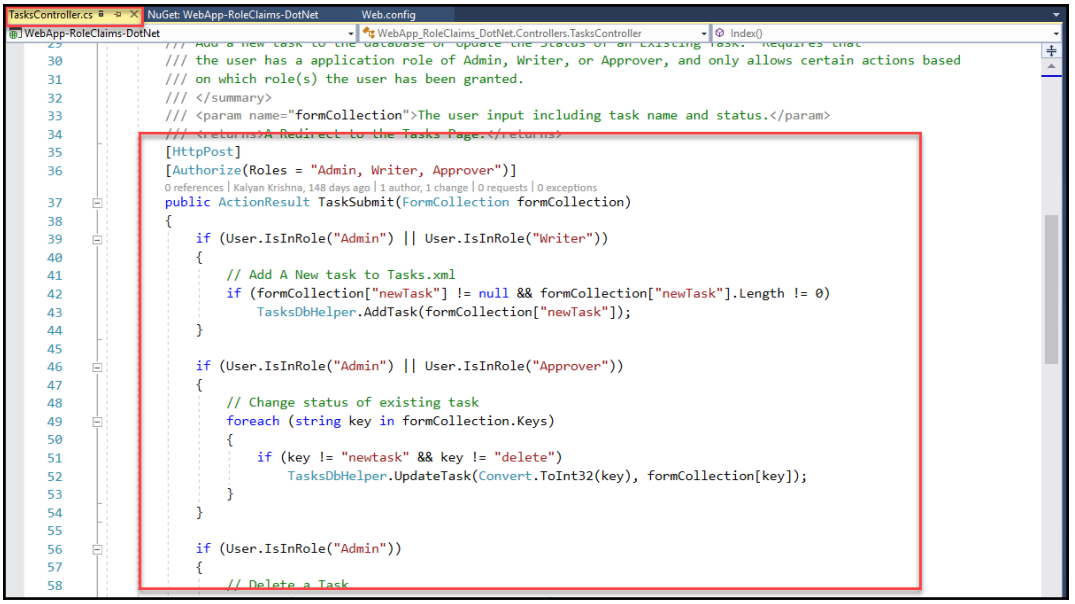
```
  "appRoles": [
{
      "allowedMemberTypes": [
        "User"
      ],
      "displayName": "Writer",
      "id": "d1c2ade8-98f8-45fd-aa4a-6d06b947c66f",
      "isEnabled": true,
      "description": "Writers Have the ability to create tasks.",
      "value": "Writer"
    },
    {
      "allowedMemberTypes": [
        "User"
      ],
      "displayName": "Observer",
      "id": "fcac0bdb-e45d-4cfc-9733-fbea156da358",
      "isEnabled": true,
      "description": "Observers only have the ability to view tasks and their statuses.",
      "value": "Observer"
    },
    {
      "allowedMemberTypes": [
        "User"
      ],
      "displayName": "Approver",
      "id": "fc803414-3c61-4ebc-a5e5-cd1675c14bbb",
      "isEnabled": true,
      "description": "Approvers have the ability to change the status of tasks.",
      "value": "Approver"
    },
    {
      "allowedMemberTypes": [
        "User"
      ],
      "displayName": "Admin",
      "id": "81e10148-16a8-432a-b86d-ef620c3e48ef",
      "isEnabled": true,
      "description": "Admins can manage roles and perform all task actions.",
      "value": "Admin"
    }
  ],
```

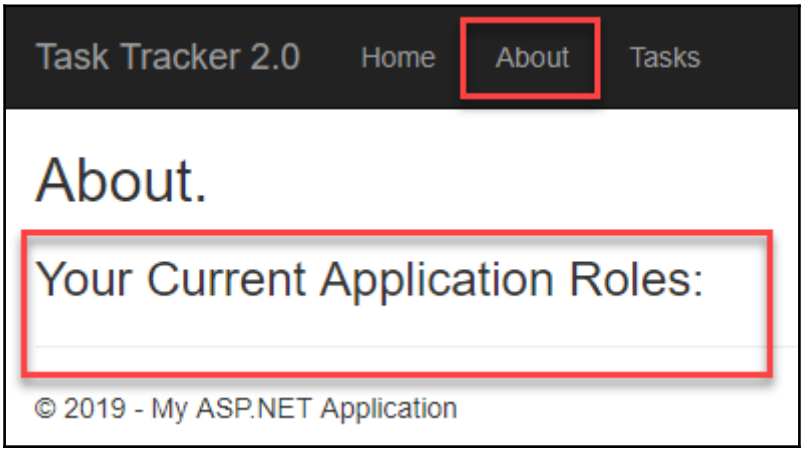


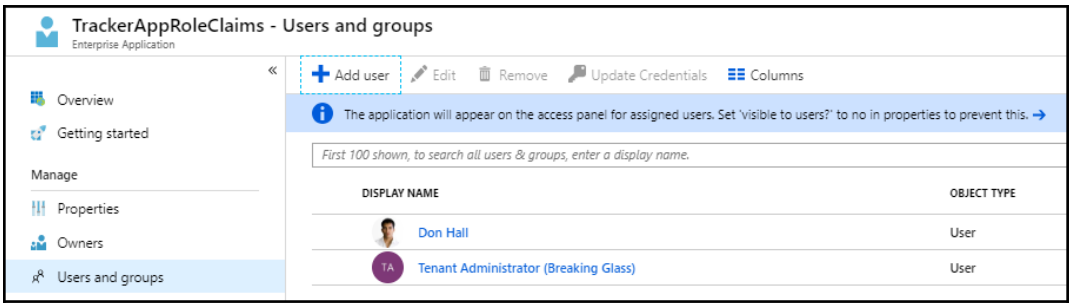

```
<appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="ida:AADInstance" value="https://login.microsoftonline.com/{0}" />
  <add key="ida:ClientId" value="734897                    e17b4691" />
  <add key="ida:TenantId" value="7709ca                    274b4d0e" />
  <add key="ida:PostLogoutRedirectUri" value="https://localhost:44322/" />
```

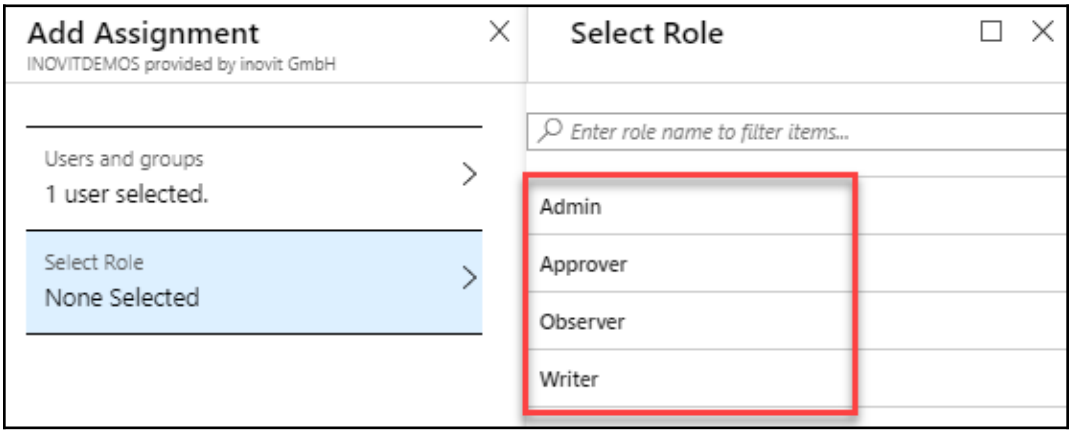

Sign in to your account
https://login.microsoftonline.com/7709ca2b-3be8-4d92-89d7-dc1e274b4d0e/oauth2/authorize?client_id=734897a9-0694-4843-8648-d977e17b4691&redirect_uri=https%3
This site uses cookies for analytics, personalized content and ads. By continuing to browse this site, you agree to this use.
Microsoft
Sign in
don.hall@inovitdemos.ch
Can't access your account?
Next

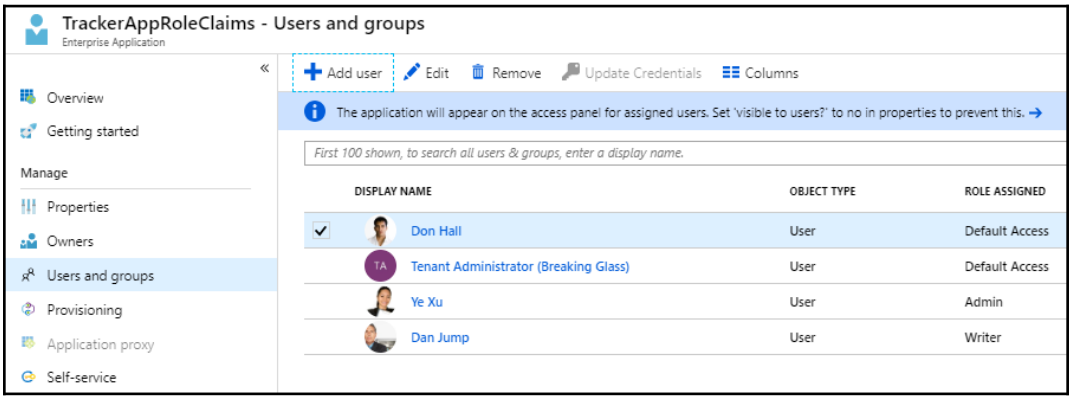

Microsoft
don.hall@inovitdemos.ch
Permissions requested
TrackerAppRoleClaims
App info
This app would like to:
Sign you in and read your profile
Read directory data
Sign you in and read your profile
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept

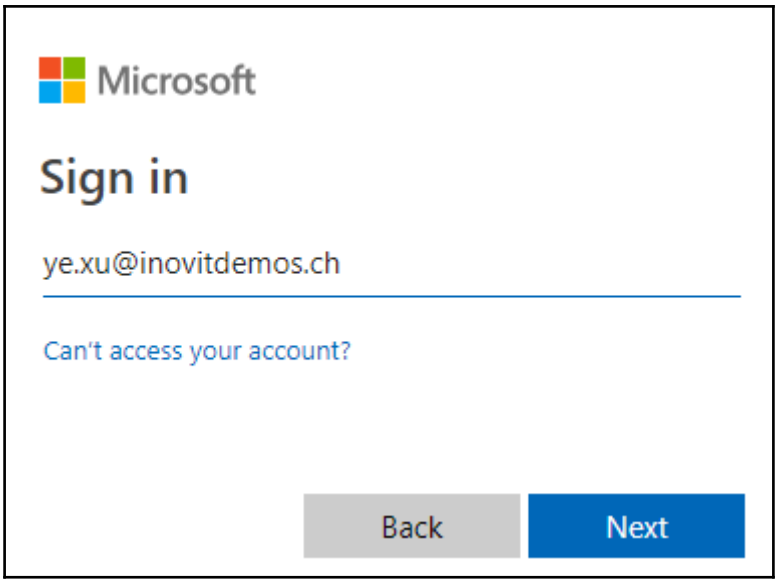

TasksController.cs
NuGet: WebApp-RoleClaims-DotNet
Web.config
WebApp-RoleClaims-DotNet
WebApp_RoleClaims_DotNet.Controllers.TasksController
Index()
/// the user has a application role of Admin, Writer, or Approver, and only allows certain actions based
/// on which role(s) the user has been granted.
/// </summary>
/// <param name="formCollection">The user input including task name and status.</param>
/// <returns>A Redirect to the Tasks Page.</returns>
[HttpPost]
[Authorize(Roles = "Admin, Writer, Approver")]
0 references | Kalyan Krishna, 148 days ago | 1 author, 1 change | 0 requests | 0 exceptions
public ActionResult TaskSubmit(FormCollection formCollection)
{
if (User.IsInRole("Admin") || User.IsInRole("Writer"))
{
// Add A New task to Tasks.xml
if (formCollection["newTask"] != null && formCollection["newTask"].Length != 0)
TasksDbHelper.AddTask(formCollection["newTask"]);
}
if (User.IsInRole("Admin") || User.IsInRole("Approver"))
{
// Change status of existing task
foreach (string key in formCollection.Keys)
{
if (key != "newtask" && key != "delete")
TasksDbHelper.UpdateTask(Convert.ToInt32(key), formCollection[key]);
}
}
if (User.IsInRole("Admin"))
{
// Delete a Task

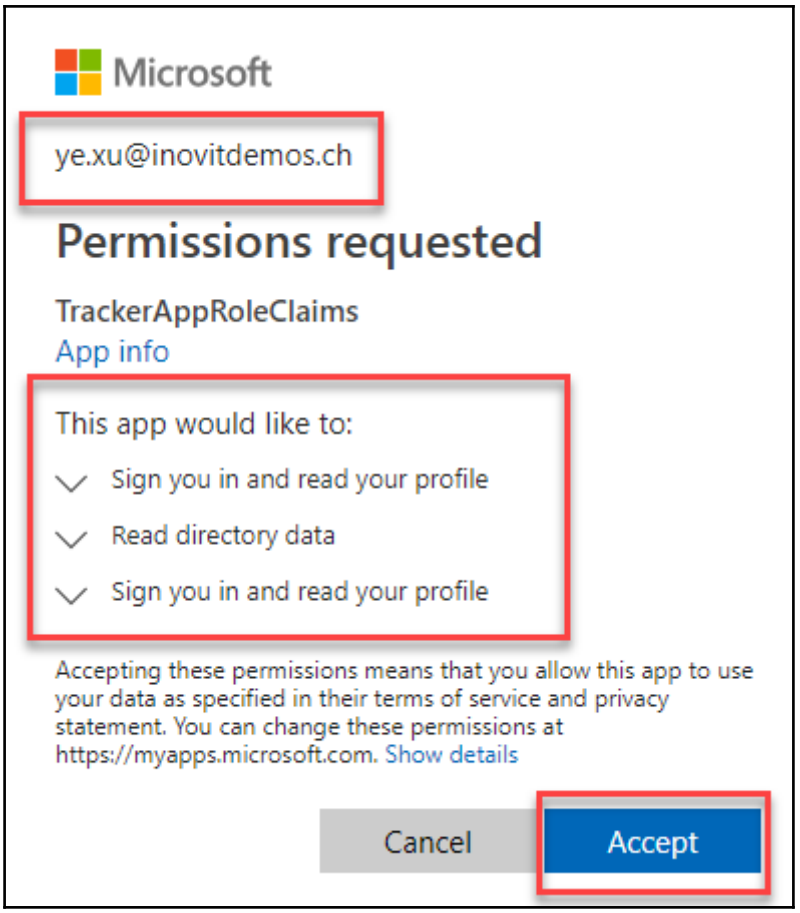

Task Tracker 2.0
Home
About
Tasks
About.
Your Current Application Roles:
© 2019 - My ASP.NET Application

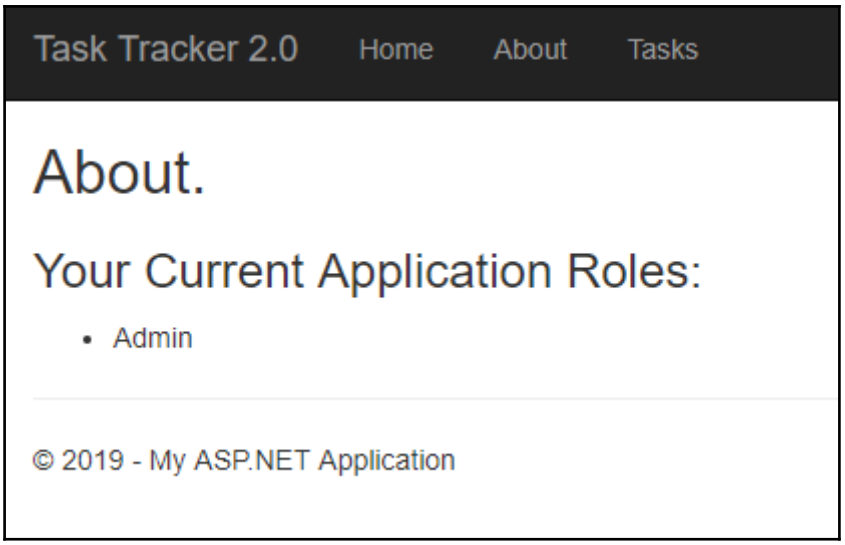

TrackerAppRoleClaims - Users and groups
Enterprise Application
Add user
Edit
Remove
Update Credentials
Columns
Overview
Getting started
Manage
Properties
Owners
Users and groups
The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.
First 100 shown, to search all users & groups, enter a display name.
DISPLAY NAME
OBJECT TYPE
Don Hall
User
Tenant Administrator (Breaking Glass)
User

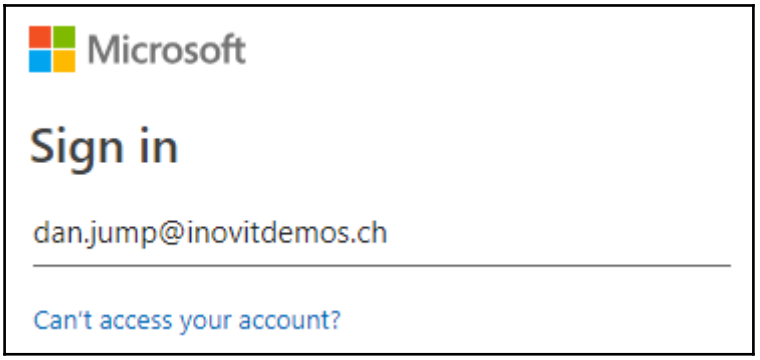

Add Assignment
INOVITDEMOS provided by inovit GmbH
Users and groups
1 user selected.
Select Role
None Selected
Select Role
Enter role name to filter items...
Admin
Approver
Observer
Writer

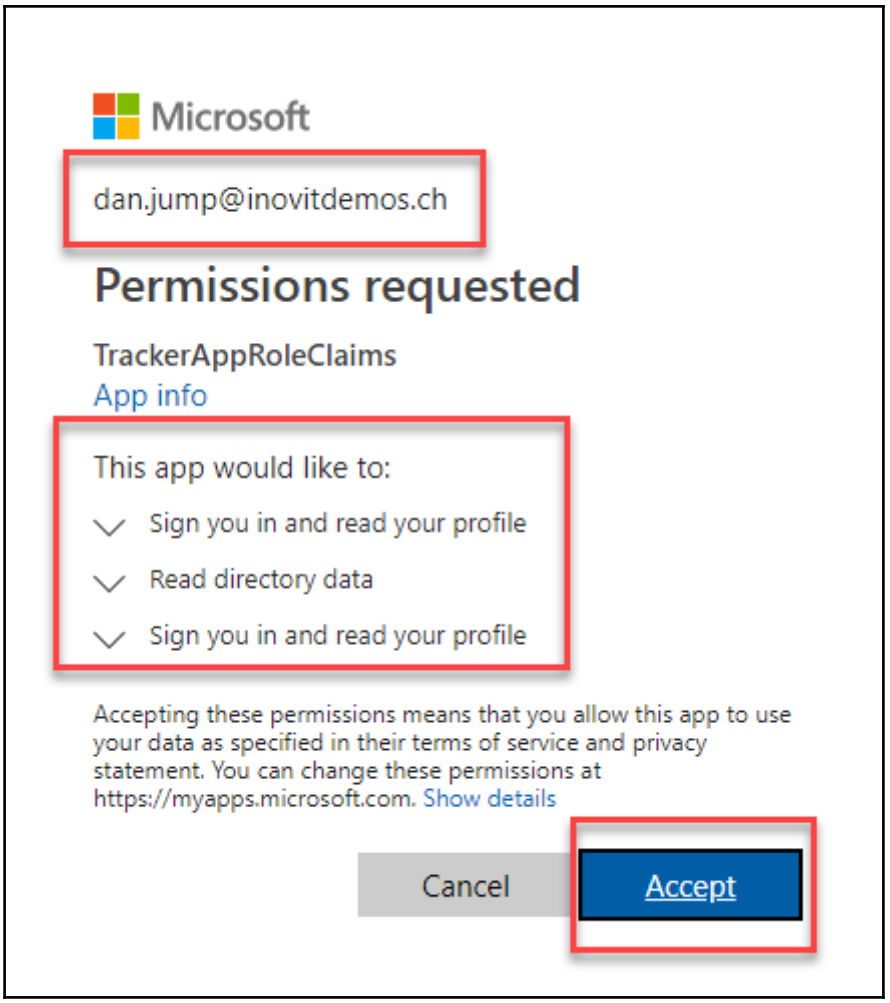

TrackerAppRoleClaims - Users and groups
Enterprise Application
Add user
Edit
Remove
Update Credentials
Columns
Overview
Getting started
Manage
Properties
Owners
Users and groups
Provisioning
Application proxy
Self-service
The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.
First 100 shown, to search all users & groups, enter a display name.
DISPLAY NAME
OBJECT TYPE
ROLE ASSIGNED
Don Hall
User
Default Access
Tenant Administrator (Breaking Glass)
User
Default Access
Ye Xu
User
Admin
Dan Jump
User
Writer


Microsoft
Sign in
ye.xu@inovitdemos.ch
Can't access your account?
Back
Next

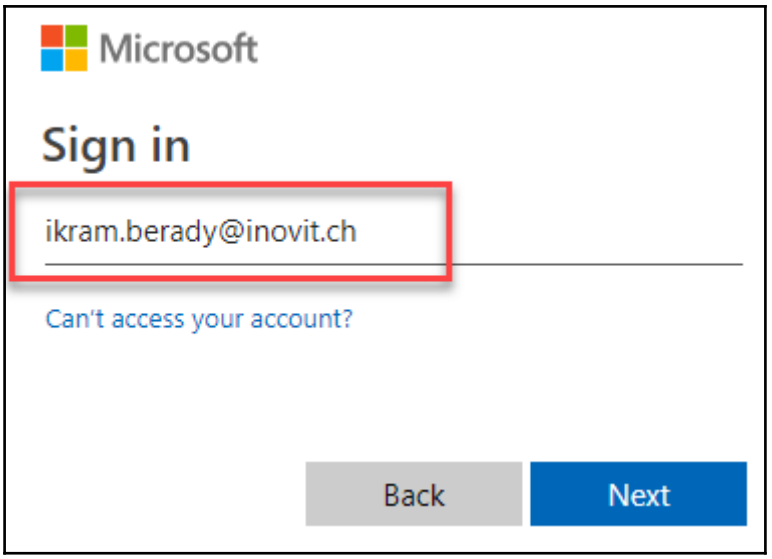

Microsoft
ye.xu@inovitdemos.ch
Permissions requested
TrackerAppRoleClaims
App info
This app would like to:
Sign you in and read your profile
Read directory data
Sign you in and read your profile
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept

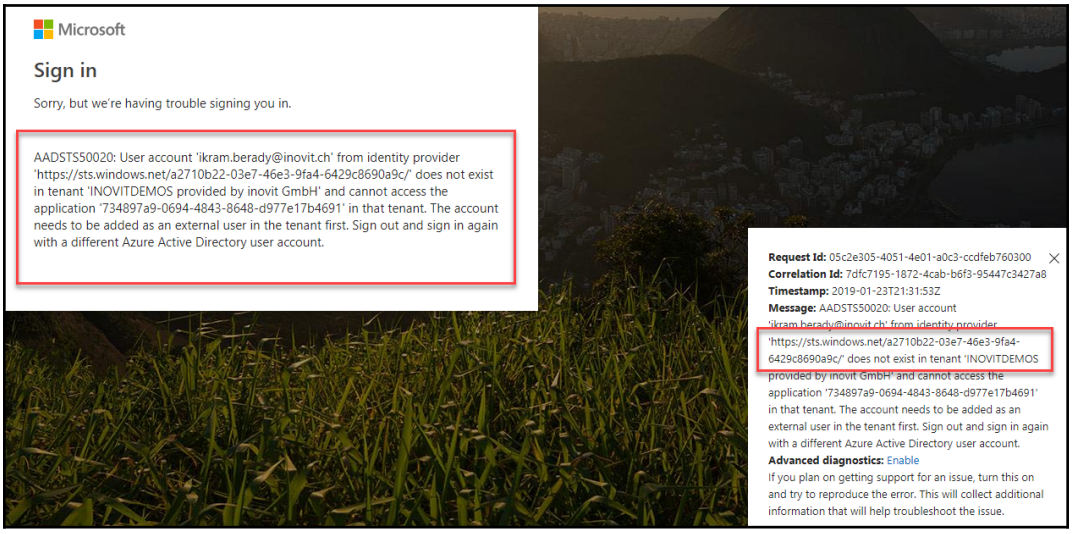

Task Tracker 2.0
Home
About
Tasks
About.
Your Current Application Roles:
Admin
© 2019 - My ASP.NET Application

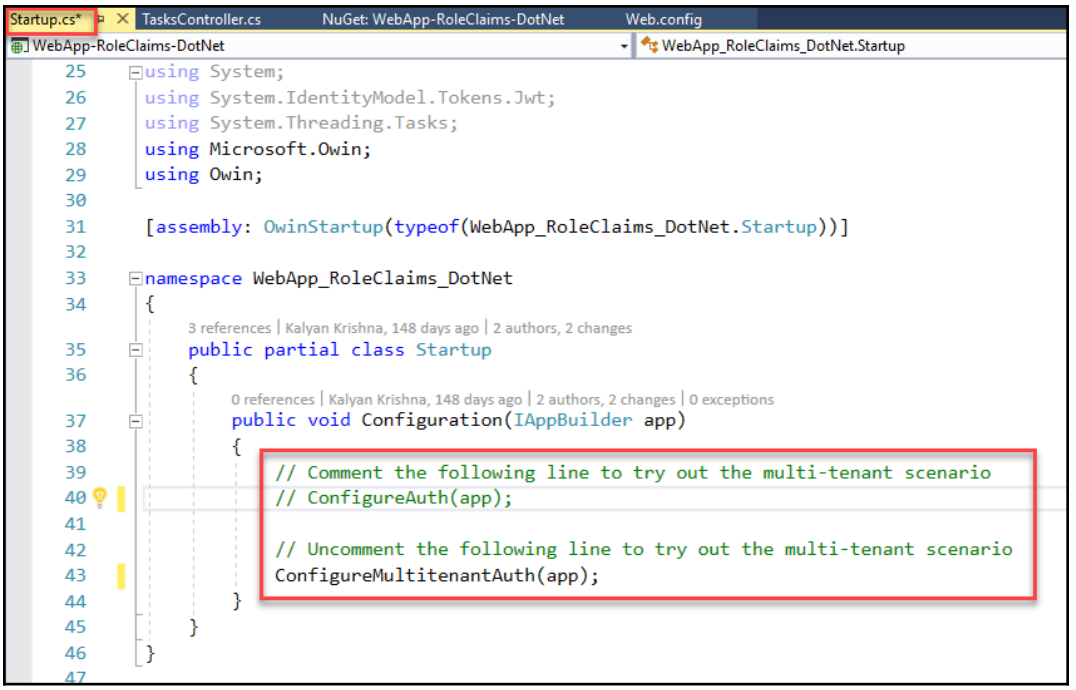

Microsoft
Sign in
dan.jump@inovitdemos.ch
Can't access your account?


Microsoft
dan.jump@inovitdemos.ch
Permissions requested
TrackerAppRoleClaims
App info
This app would like to:
Sign you in and read your profile
Read directory data
Sign you in and read your profile
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept

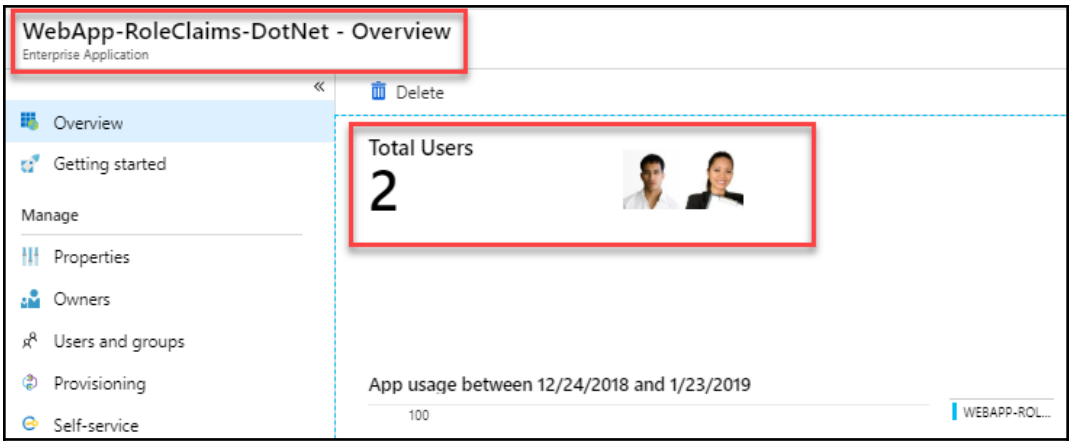

Task Tracker 2.0
Home
About
Tasks
Hello, Dan.Jump@inovitdemos.ch!
About.
Your Current Application Roles:
Writer
© 2019 - My ASP.NET Application

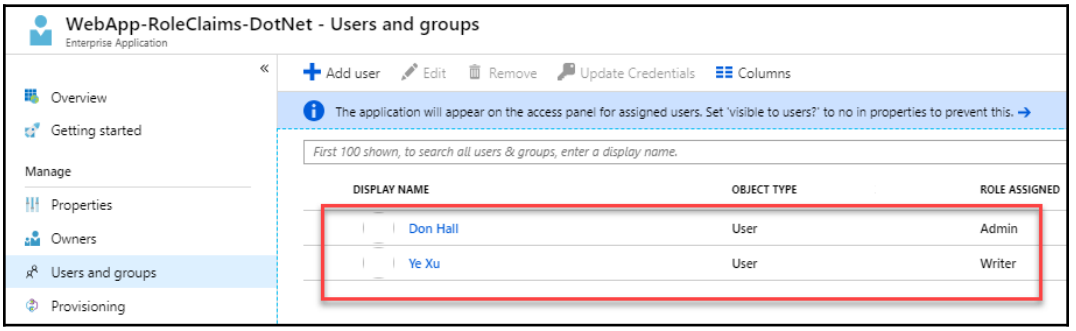

Microsoft
Sign in
ikram.berady@inovit.ch
Can't access your account?
Back
Next


Microsoft
Sign in
Sorry, but we're having trouble signing you in.
AADSTS50020: User account 'ikram.berady@inovit.ch' from identity provider 'https://sts.windows.net/a2710b22-03e7-46e3-9fa4-6429c8690a9c/' does not exist in tenant 'INOVITDEMOS provided by inovit GmbH' and cannot access the application '734897a9-0694-4843-8648-d977e17b4691' in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account.
Request Id: 05c2e305-4051-4e01-a0c3-ccdfeb760300
Correlation Id: 7dfc7195-1872-4cab-b6f3-95447c3427a8
Timestamp: 2019-01-23T21:31:53Z
Message: AADSTS50020: User account 'ikram.berady@inovit.ch' from identity provider 'https://sts.windows.net/a2710b22-03e7-46e3-9fa4-6429c8690a9c/' does not exist in tenant 'INOVITDEMOS provided by inovit GmbH' and cannot access the application '734897a9-0694-4843-8648-d977e17b4691' in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account.
Advanced diagnostics: Enable
If you plan on getting support for an issue, turn this on and try to reproduce the error. This will collect additional information that will help troubleshoot the issue.

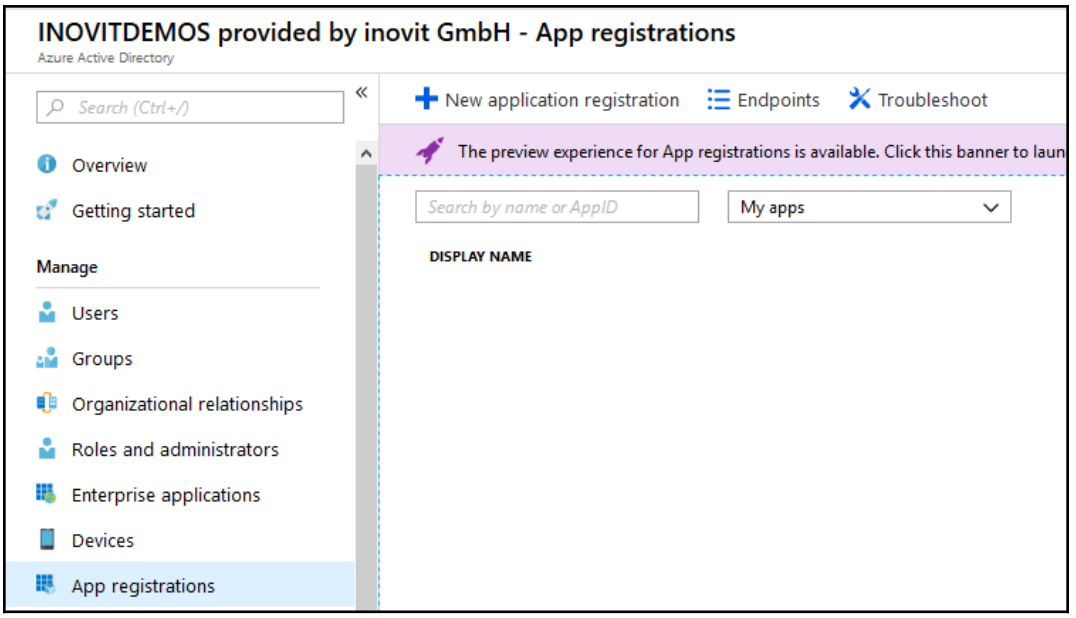


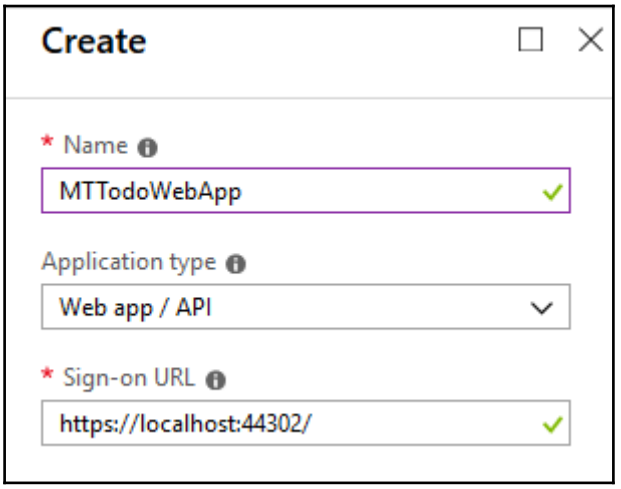

```
<appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="ida:AADInstance" value="https://login.microsoftonline.com/{0}"
  <add key="ida:ClientId" value="734897a9-0694-4843-8648-d977e17b4691" />
  <add key="ida:TenantId" value="181031inovitdemos.onmicrosoft.com" />
  <add key="ida:PostLogoutRedirectUri" value="https://localhost:44322/" />
</appSettings>
```

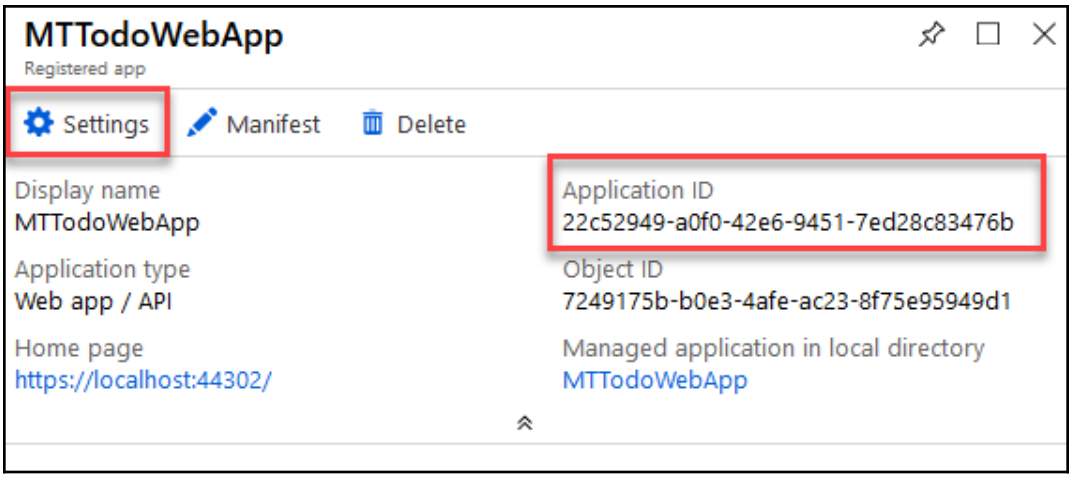

WebApp-RoleClaims-DotNet - Overview
Enterprise Application
Delete
Overview
Getting started
Manage
Properties
Owners
Users and groups
Provisioning
Self-service
Total Users
2
App usage between 12/24/2018 and 1/23/2019
100
WEBAPP-ROL...

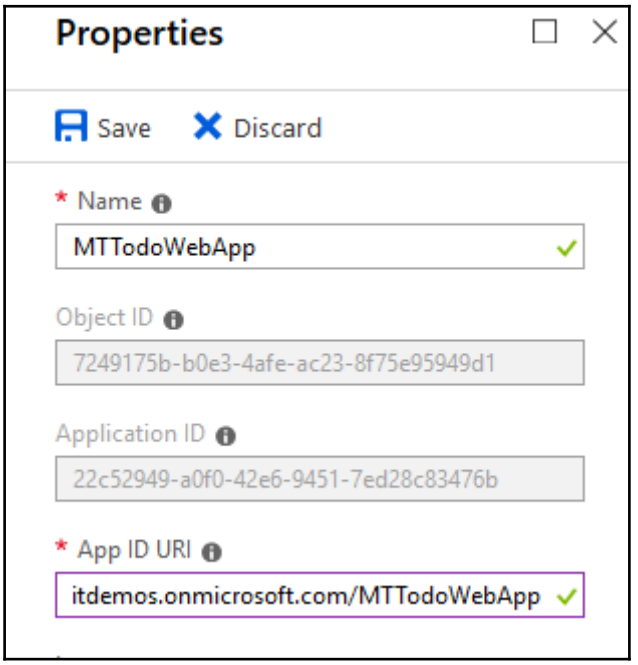

WebApp-RoleClaims-DotNet - Users and groups
Enterprise Application
Overview
Getting started
Manage
Properties
Owners
Users and groups
Provisioning
Add user
Edit
Remove
Update Credentials
Columns
The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.
First 100 shown, to search all users & groups, enter a display name.
DISPLAY NAME
OBJECT TYPE
ROLE ASSIGNED
Don Hall
User
Admin
Ye Xu
User
Writer

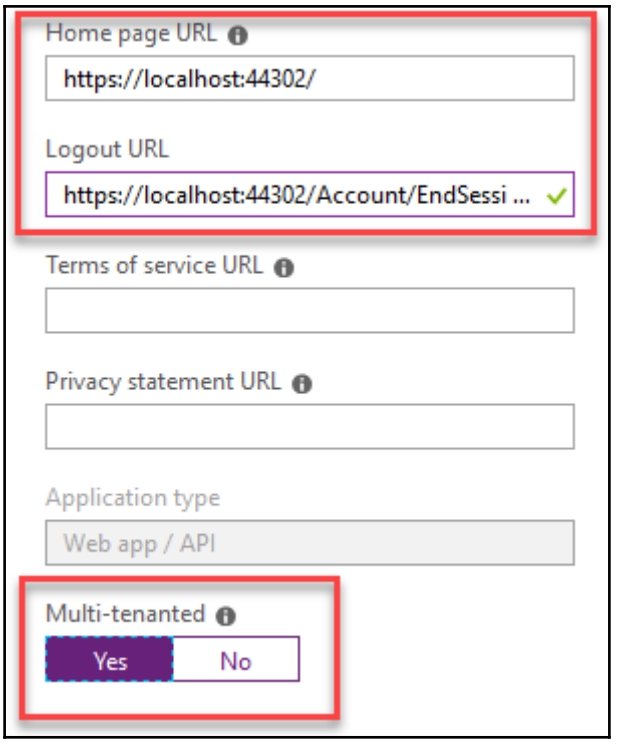

Task Tracker 2.0
Home
About
Tasks
Hello, ikram.berady@inovit.ch!
Sign out

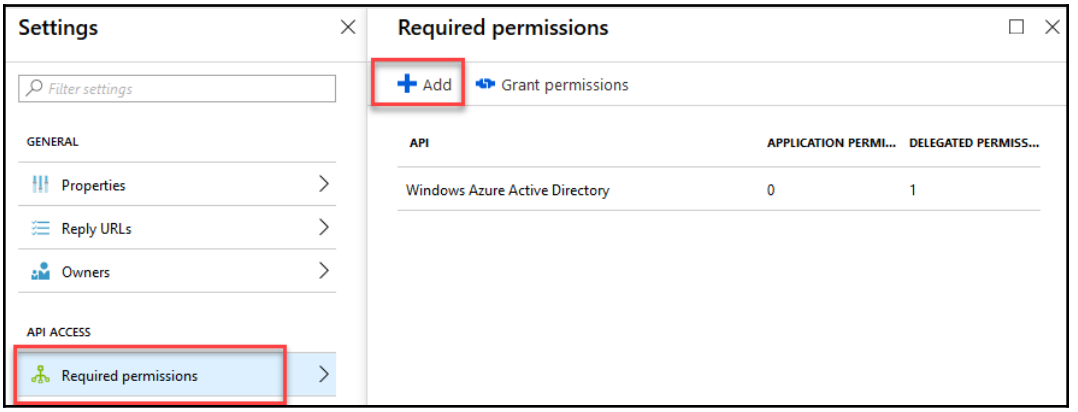

INOVITDEMOS provided by inovit GmbH - App registrations
Azure Active Directory
Search (Ctrl+/)
Overview
Getting started
Manage
Users
Groups
Organizational relationships
Roles and administrators
Enterprise applications
Devices
App registrations
New application registration
Endpoints
Troubleshoot
The preview experience for App registrations is available. Click this banner to laun
Search by name or AppID
My apps
DISPLAY NAME

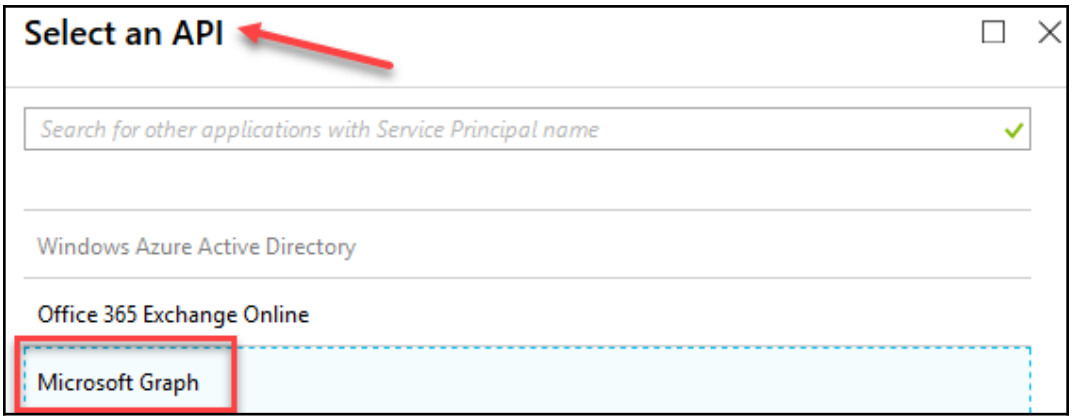

Create
* Name
MTTodoWebApp
Application type
Web app / API
* Sign-on URL
https://localhost:44302/

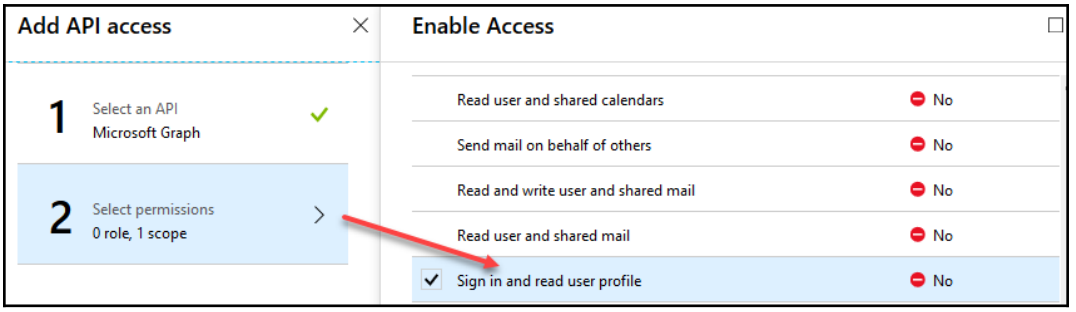

MTTodoWebApp
Registered app
Settings
Manifest
Delete
Display name
MTTodoWebApp
Application type
Web app / API
Home page
https://localhost:44302/
Application ID
22c52949-a0f0-42e6-9451-7ed28c83476b
Object ID
7249175b-b0e3-4afe-ac23-8f75e95949d1
Managed application in local directory
MTTodoWebApp

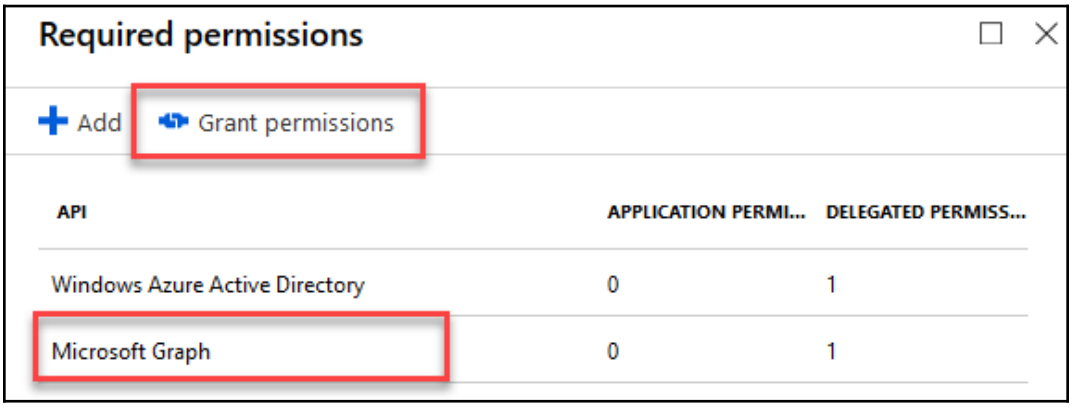

Properties
Save
Discard
* Name
MTTodoWebApp
Object ID
7249175b-b0e3-4afe-ac23-8f75e95949d1
Application ID
22c52949-a0f0-42e6-9451-7ed28c83476b
* App ID URI
itdemos.onmicrosoft.com/MTTodoWebApp

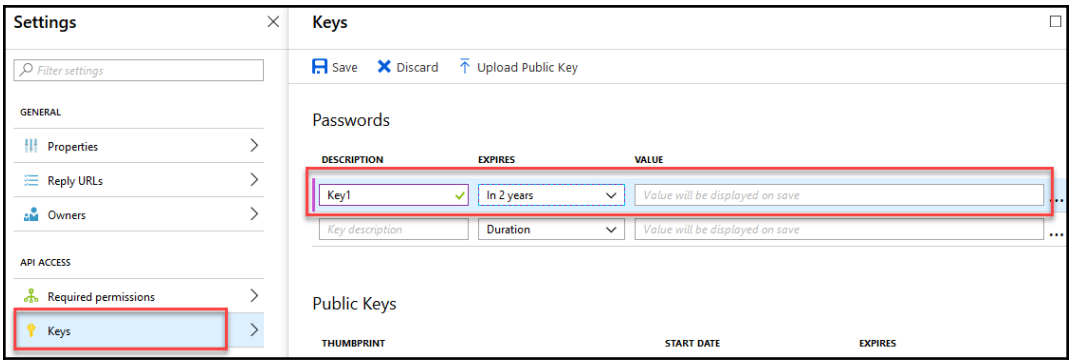

Home page URL
https://localhost:44302/
Logout URL
https://localhost:44302/Account/EndSessi ...
Terms of service URL
Privacy statement URL
Application type
Web app / API
Multi-tenanted
Yes
No

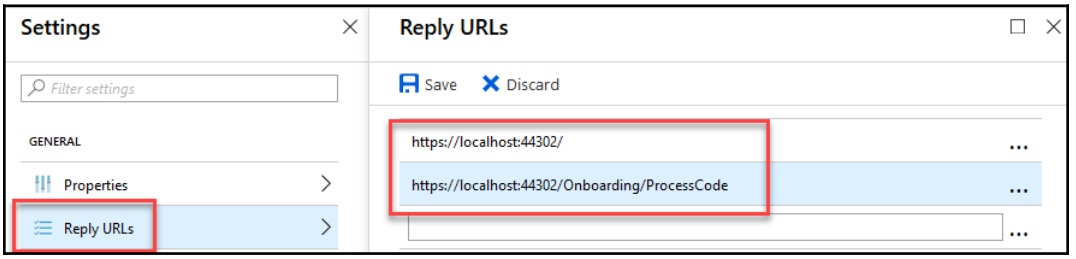

Settings
Filter settings
GENERAL
Properties
Reply URLs
Owners
API ACCESS
Required permissions
Required permissions
Add
Grant permissions
API
APPLICATION PERMI...
DELEGATED PERMISS...
Windows Azure Active Directory
0
1


Select an API
Search for other applications with Service Principal name
Windows Azure Active Directory
Office 365 Exchange Online
Microsoft Graph

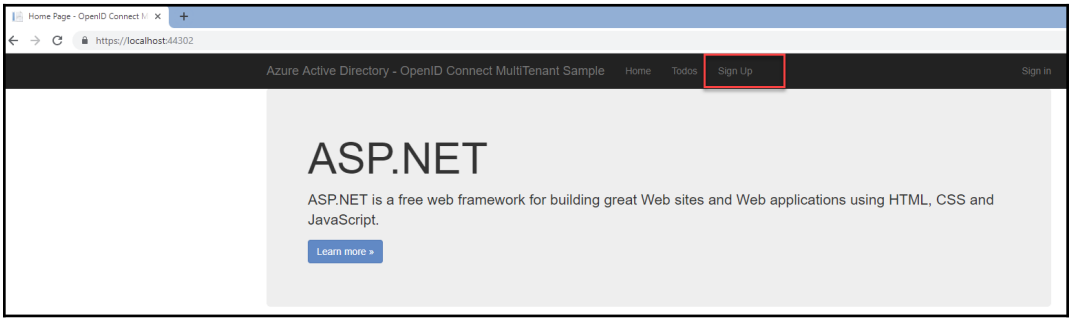

Add API access
1
Select an API
Microsoft Graph
2
Select permissions
0 role, 1 scope
Enable Access
Read user and shared calendars
No
Send mail on behalf of others
No
Read and write user and shared mail
No
Read user and shared mail
No
Sign in and read user profile
No

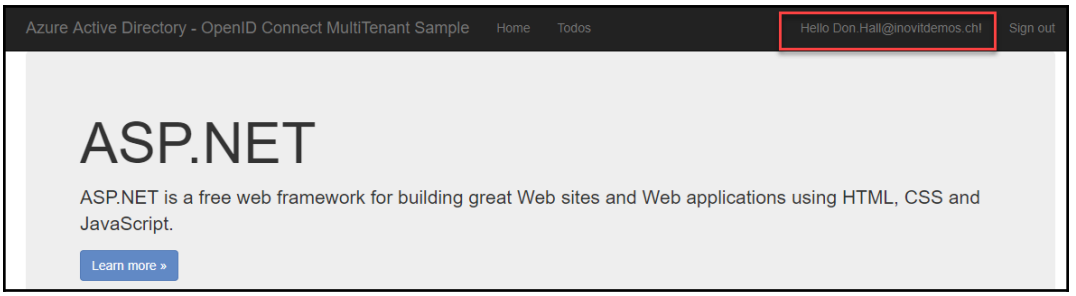

Required permissions
Add
Grant permissions
API
APPLICATION PERMI...
DELEGATED PERMISS...
Windows Azure Active Directory
0
1
Microsoft Graph
0
1

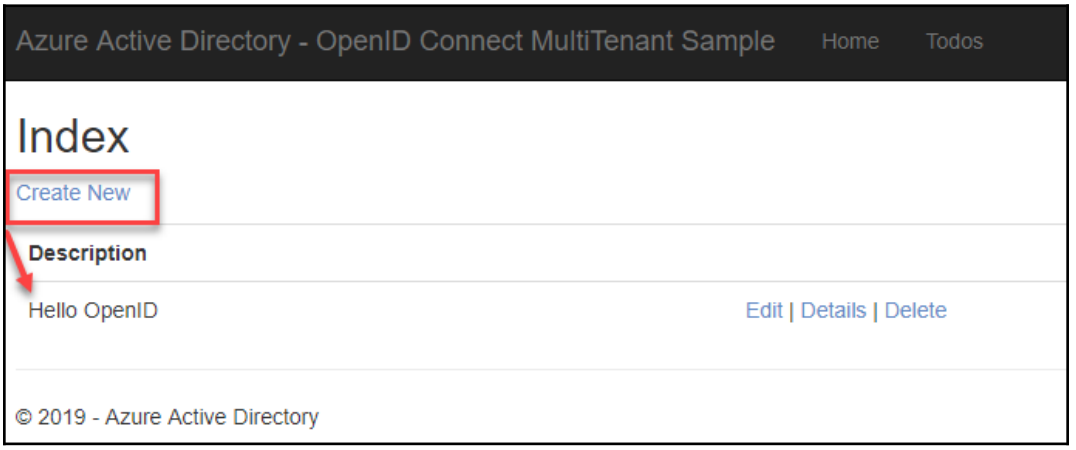


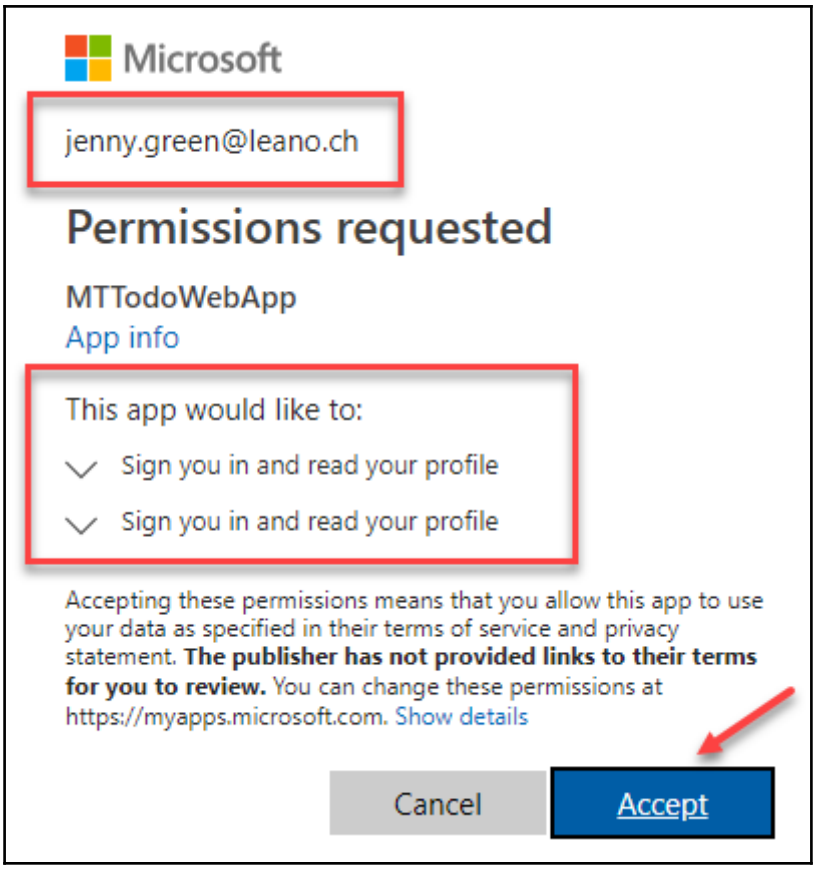


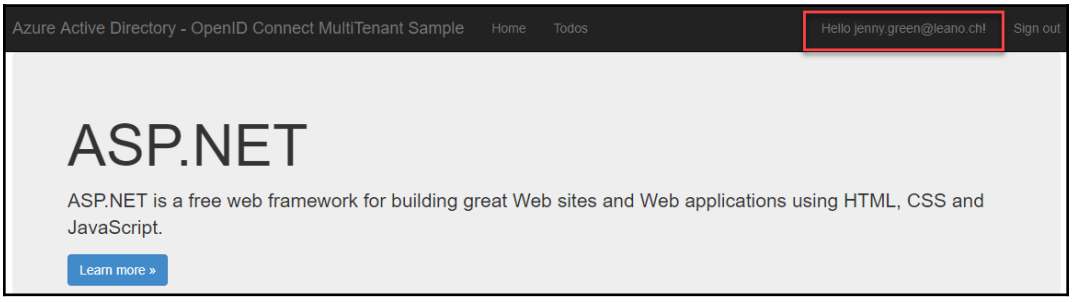

```
<appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="ida:ClientID" value="22c5294[redacted]476b"/>
  <add key="ida:Password" value="Jh8SAPS[redacted]yOhVyVHT8ZQ="  />
</appSettings>
```

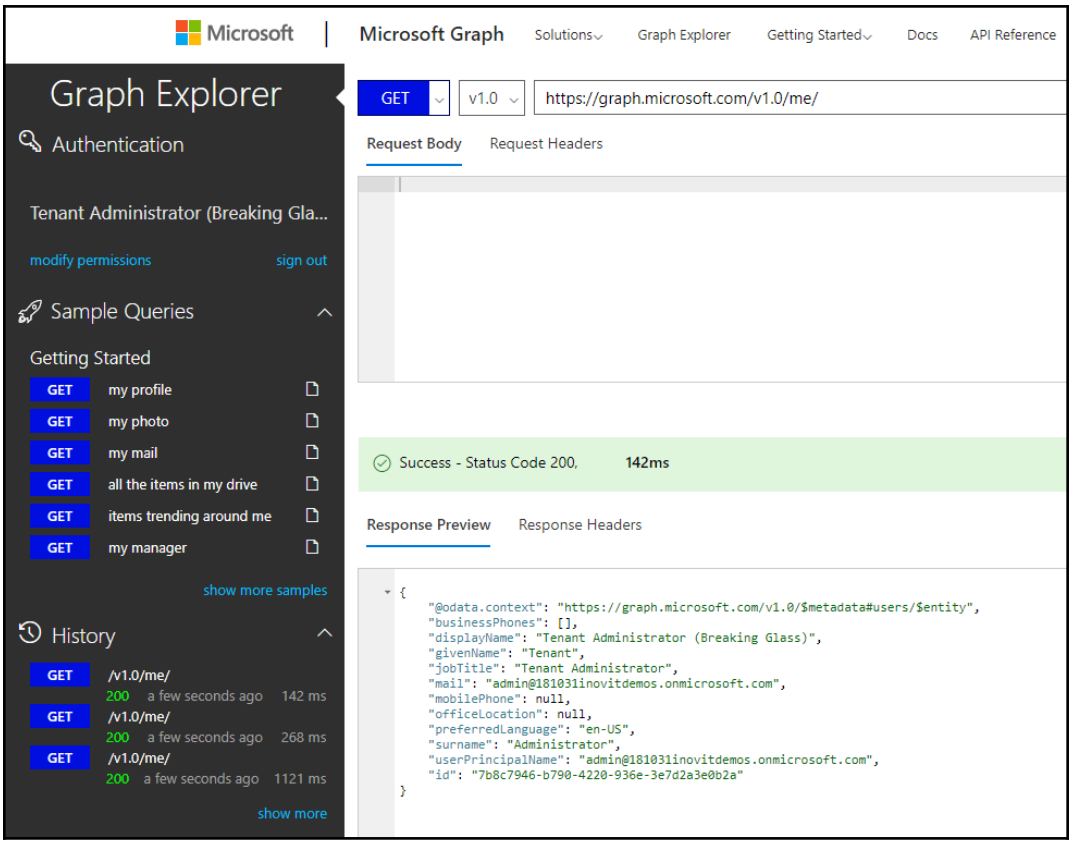



Azure Active Directory - OpenID Connect MultiTenant Sample
Home
Todos
Hello Don.Hall@inovitdemos.ch!
Sign out
ASP.NET
ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS and JavaScript.
Learn more »

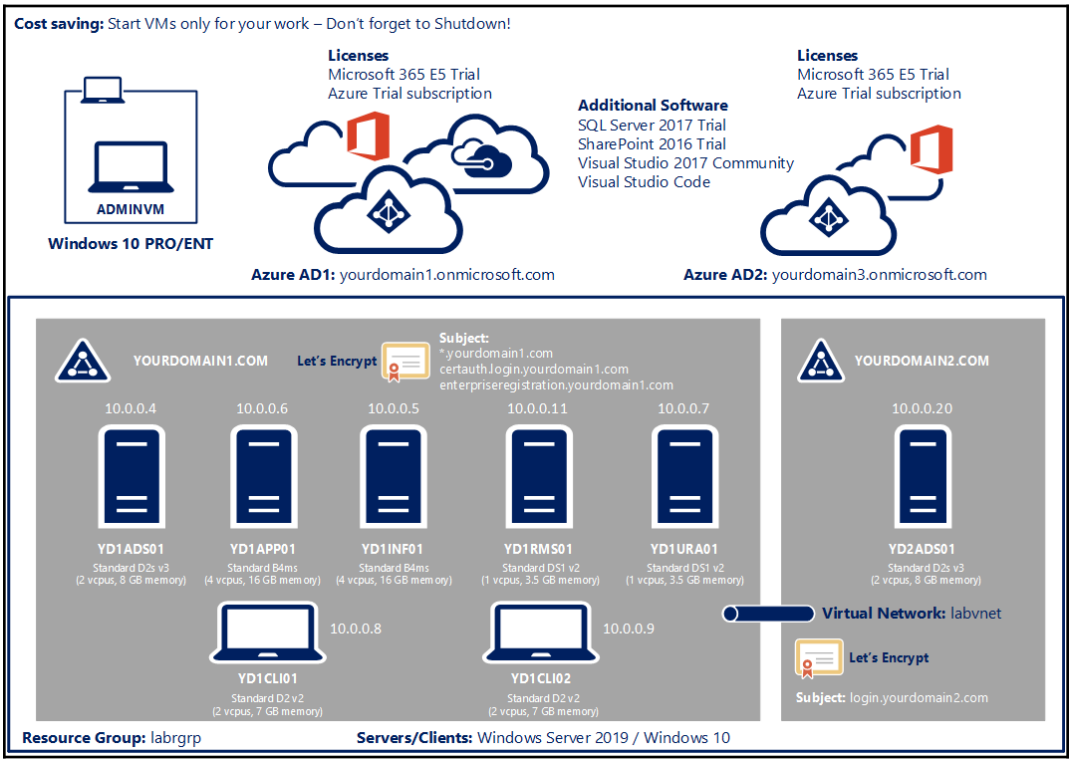

Azure Active Directory - OpenID Connect MultiTenant Sample
Home
Todos
Index
Create New
Description
Hello OpenID
Edit | Details | Delete
© 2019 - Azure Active Directory

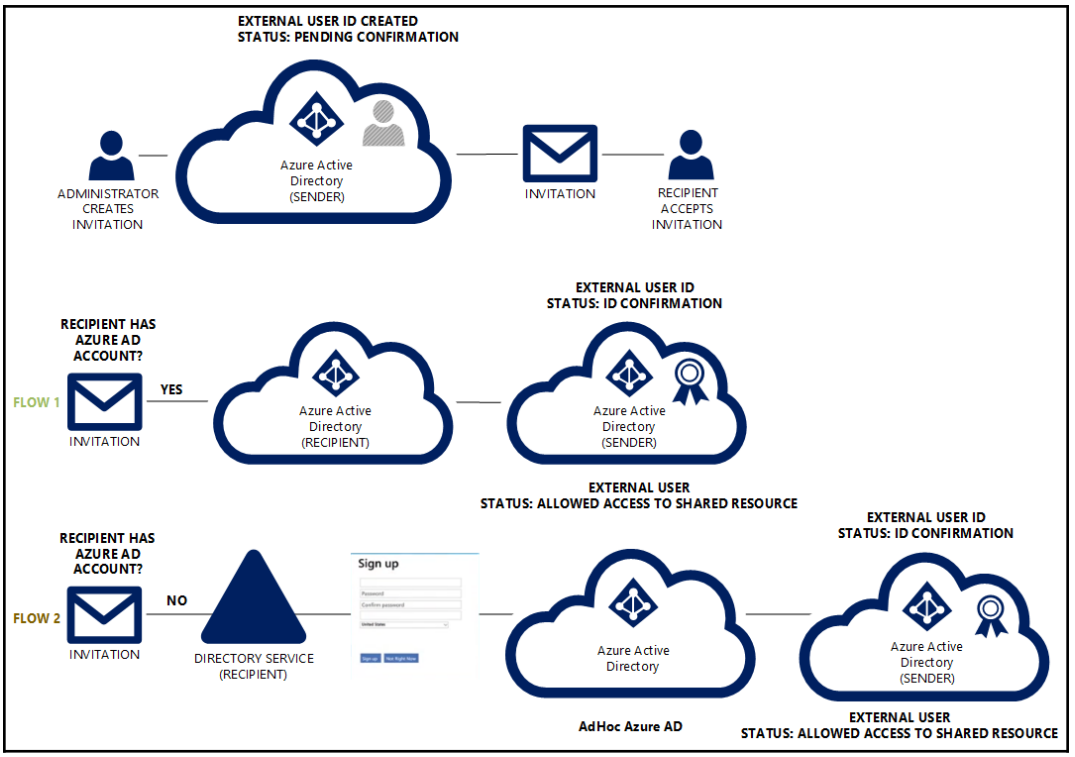

Microsoft
jenny.green@leano.ch
Permissions requested
MTTodoWebApp
App info
This app would like to:
Sign you in and read your profile
Sign you in and read your profile
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. The publisher has not provided links to their terms for you to review. You can change these permissions at https://myapps.microsoft.com. Show details
Cancel
Accept

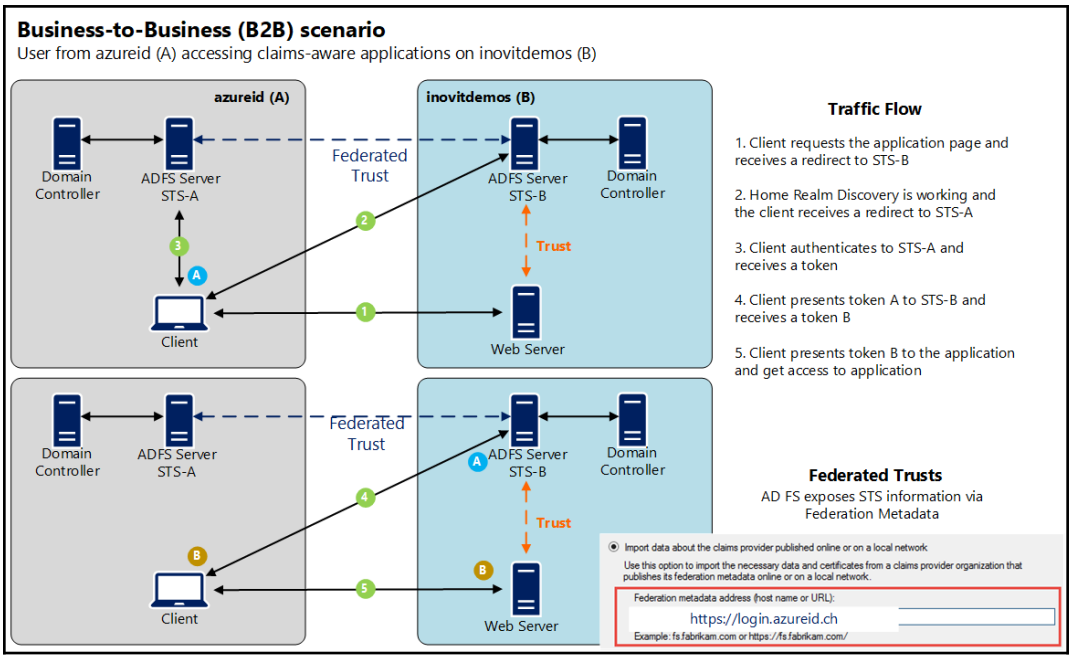

Azure Active Directory - OpenID Connect MultiTenant Sample
Home
Todos
Hello jenny.green@leano.ch!
Sign out
ASP.NET
ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS and JavaScript.
Learn more »

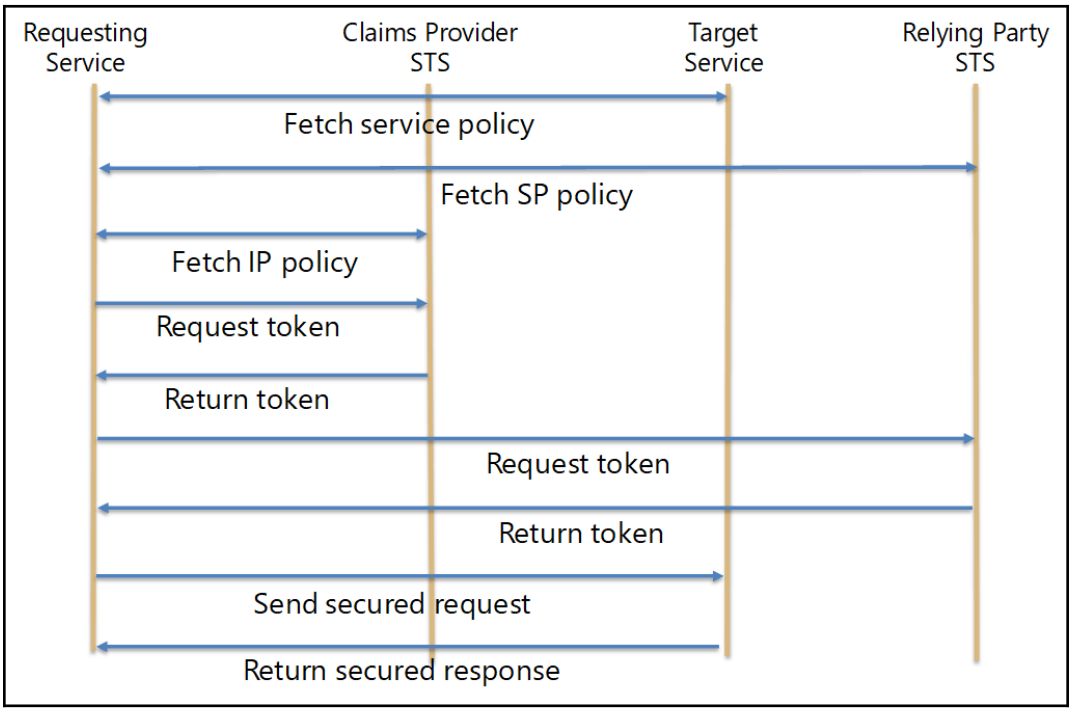

Microsoft
Microsoft Graph
Solutions
Graph Explorer
Getting Started
Docs
API Reference
Graph Explorer
Authentication
Tenant Administrator (Breaking Gla...
modify permissions
sign out
Sample Queries
Getting Started
GET my profile
GET my photo
GET my mail
GET all the items in my drive
GET items trending around me
GET my manager
show more samples
History
GET /v1.0/me/
200 a few seconds ago 142 ms
GET /v1.0/me/
200 a few seconds ago 268 ms
GET /v1.0/me/
200 a few seconds ago 1121 ms
show more
GET
v1.0
https://graph.microsoft.com/v1.0/me/
Request Body
Request Headers
Success - Status Code 200,
142ms
Response Preview
Response Headers
{
"@odata.context": "https://graph.microsoft.com/v1.0/$metadata#users/$entity",
"businessPhones": [],
"displayName": "Tenant Administrator (Breaking Glass)",
"givenName": "Tenant",
"jobTitle": "Tenant Administrator",
"mail": "admin@181031inovitdemos.onmicrosoft.com",
"mobilePhone": null,
"officeLocation": null,
"preferredLanguage": "en-US",
"surname": "Administrator",
"userPrincipalName": "admin@181031inovitdemos.onmicrosoft.com",
"id": "7b8c7946-b790-4220-936e-3e7d2a3e0b2a"
}

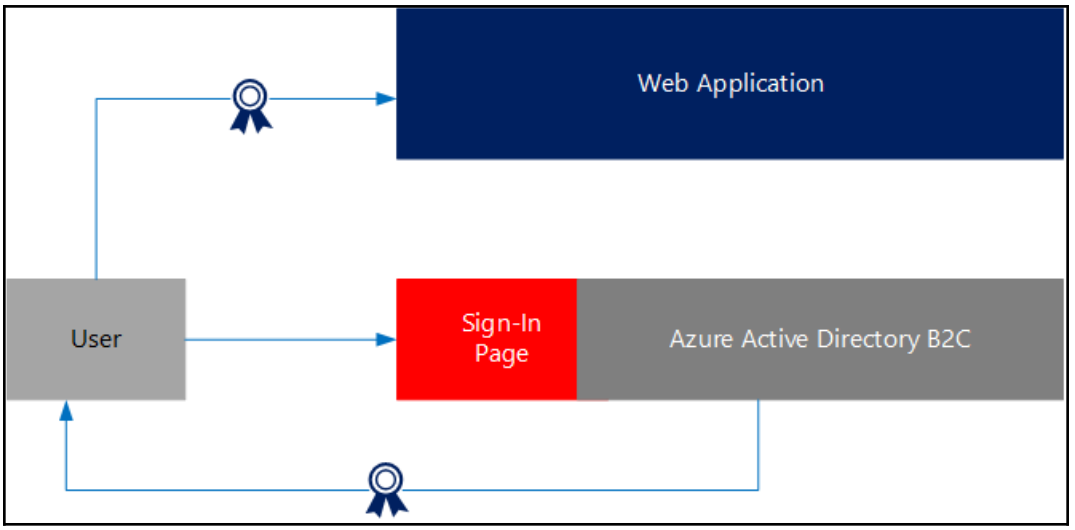
Chapter 10: Exploring Azure AD Identity Services

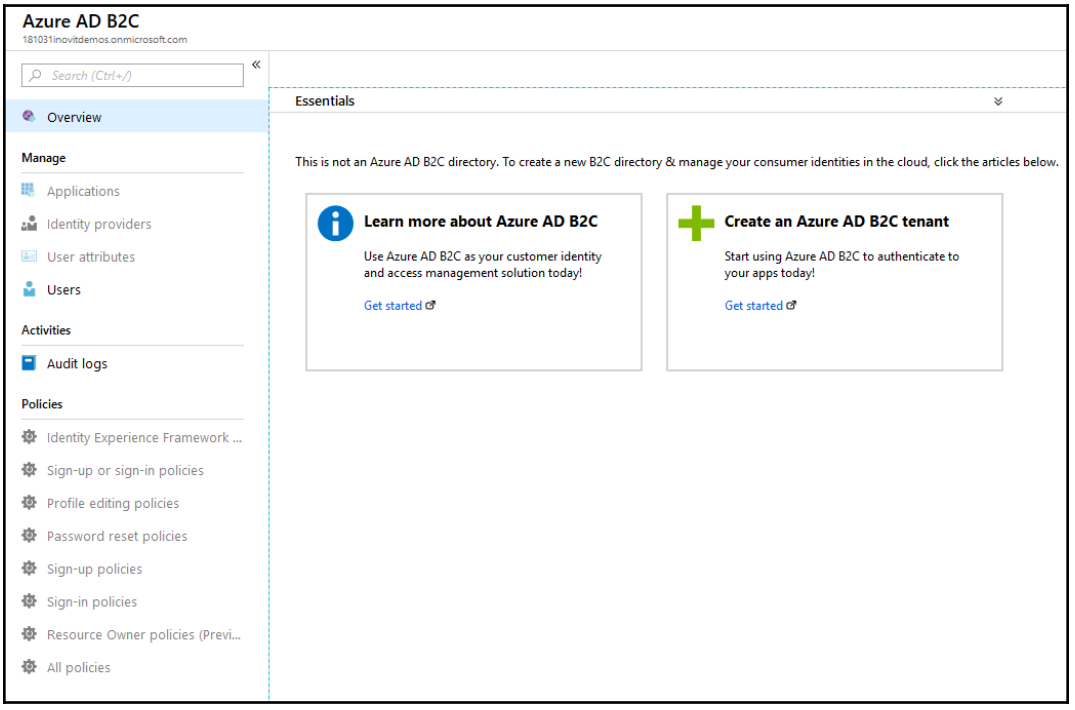


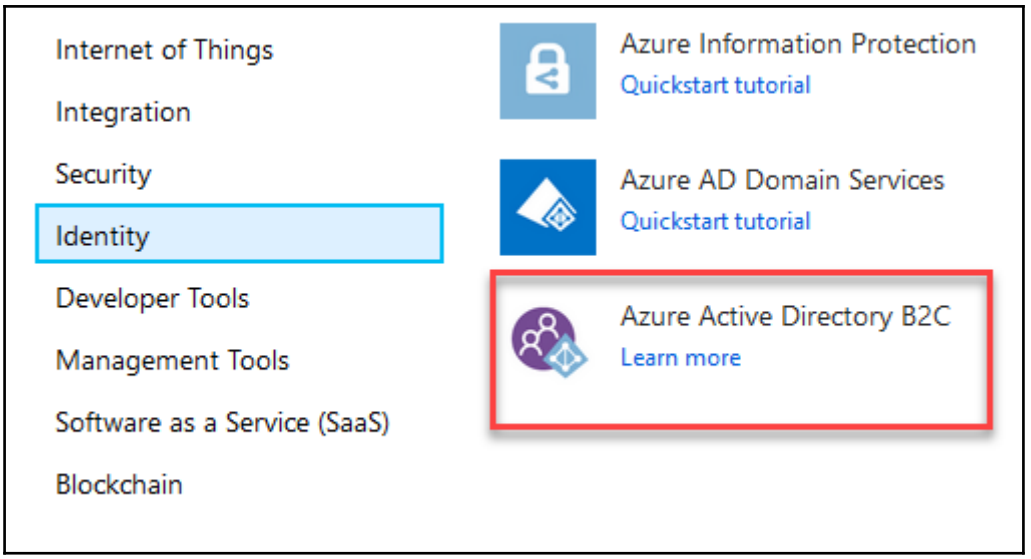

EXTERNAL USER ID CREATED
STATUS: PENDING CONFIRMATION
ADMINISTRATOR CREATES INVITATION
Azure Active Directory (SENDER)
INVITATION
RECIPIENT ACCEPTS INVITATION
EXTERNAL USER ID
STATUS: ID CONFIRMATION
RECIPIENT HAS AZURE AD ACCOUNT?
FLOW 1
YES
INVITATION
Azure Active Directory (RECIPIENT)
Azure Active Directory (SENDER)
EXTERNAL USER
STATUS: ALLOWED ACCESS TO SHARED RESOURCE
EXTERNAL USER ID
STATUS: ID CONFIRMATION
RECIPIENT HAS AZURE AD ACCOUNT?
FLOW 2
NO
INVITATION
DIRECTORY SERVICE (RECIPIENT)
Sign up
Azure Active Directory
Azure Active Directory (SENDER)
AdHoc Azure AD
EXTERNAL USER
STATUS: ALLOWED ACCESS TO SHARED RESOURCE


Business-to-Business (B2B) scenario
User from azureid (A) accessing claims-aware applications on inovitdemos (B)
azureid (A)
inovitdemos (B)
Domain Controller
ADFS Server STS-A
Federated Trust
ADFS Server STS-B
Domain Controller
Trust
Client
Web Server
Traffic Flow
1. Client requests the application page and receives a redirect to STS-B
2. Home Realm Discovery is working and the client receives a redirect to STS-A
3. Client authenticates to STS-A and receives a token
4. Client presents token A to STS-B and receives a token B
5. Client presents token B to the application and get access to application
Federated Trusts
AD FS exposes STS information via Federation Metadata
Import data about the claims provider published online or on a local network
Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.
Federation metadata address (host name or URL):
https://login.azureid.ch
Example: fs.fabrikam.com or https://fs.fabrikam.com/

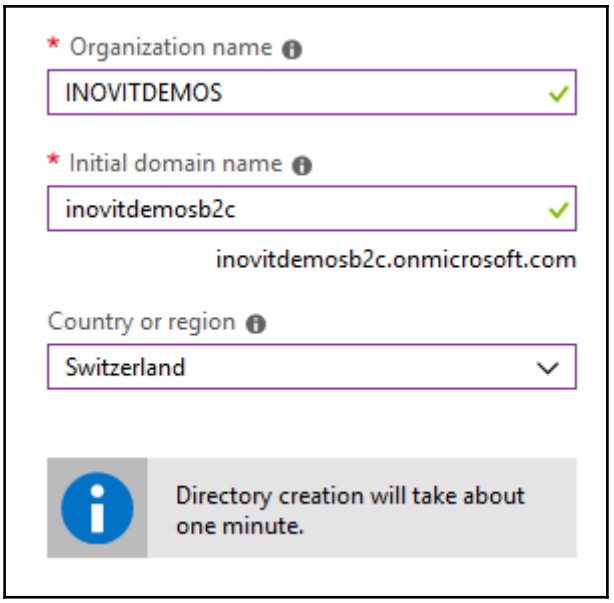

Requesting Service
Claims Provider STS
Target Service
Relying Party STS
Fetch service policy
Fetch SP policy
Fetch IP policy
Request token
Return token
Request token
Return token
Send secured request
Return secured response

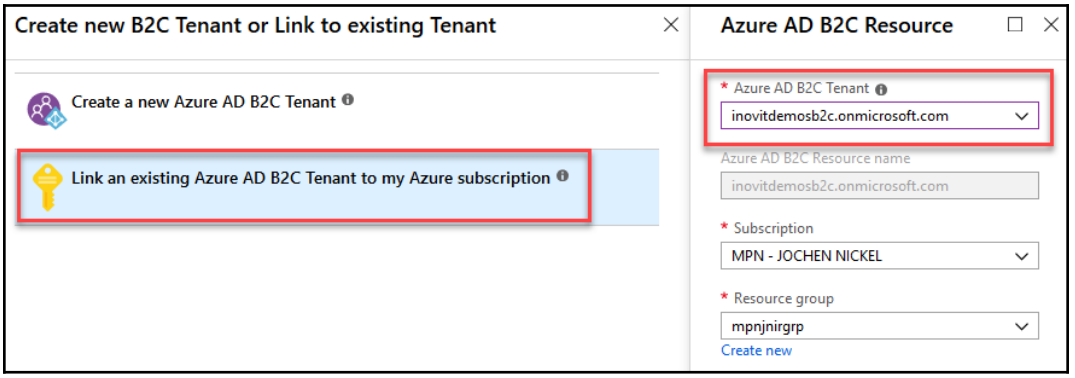

Web Application
User
Sign-In Page
Azure Active Directory B2C

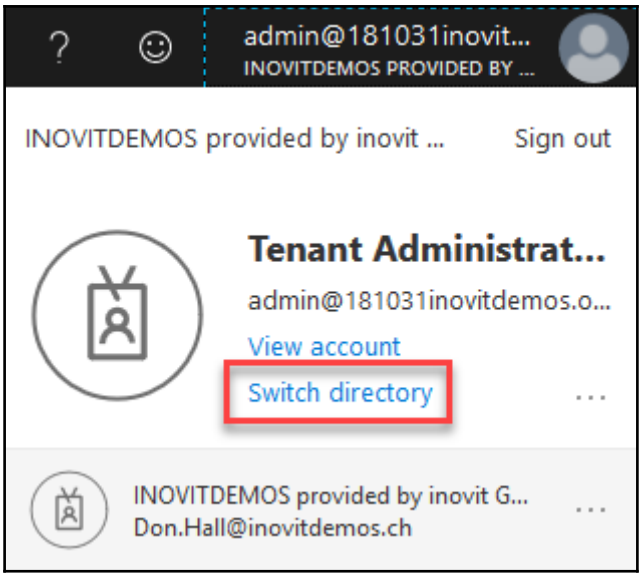

Azure AD B2C
181031inovitdemos.onmicrosoft.com
Search (Ctrl+/)
Overview
Manage
Applications
Identity providers
User attributes
Users
Activities
Audit logs
Policies
Identity Experience Framework ...
Sign-up or sign-in policies
Profile editing policies
Password reset policies
Sign-up policies
Sign-in policies
Resource Owner policies (Previ...
All policies
Essentials
This is not an Azure AD B2C directory. To create a new B2C directory & manage your consumer identities in the cloud, click the articles below.
Learn more about Azure AD B2C
Use Azure AD B2C as your customer identity and access management solution today!
Get started
Create an Azure AD B2C tenant
Start using Azure AD B2C to authenticate to your apps today!
Get started

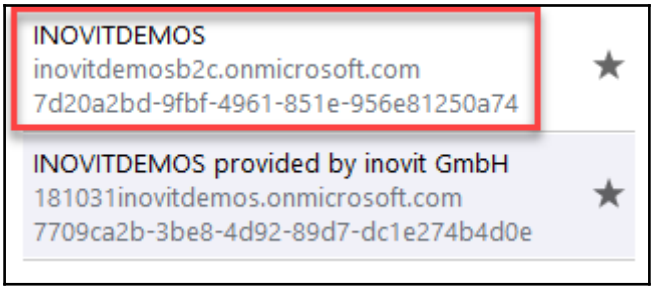

Internet of Things
Integration
Security
Identity
Developer Tools
Management Tools
Software as a Service (SaaS)
Blockchain
Azure Information Protection
Quickstart tutorial
Azure AD Domain Services
Quickstart tutorial
Azure Active Directory B2C
Learn more

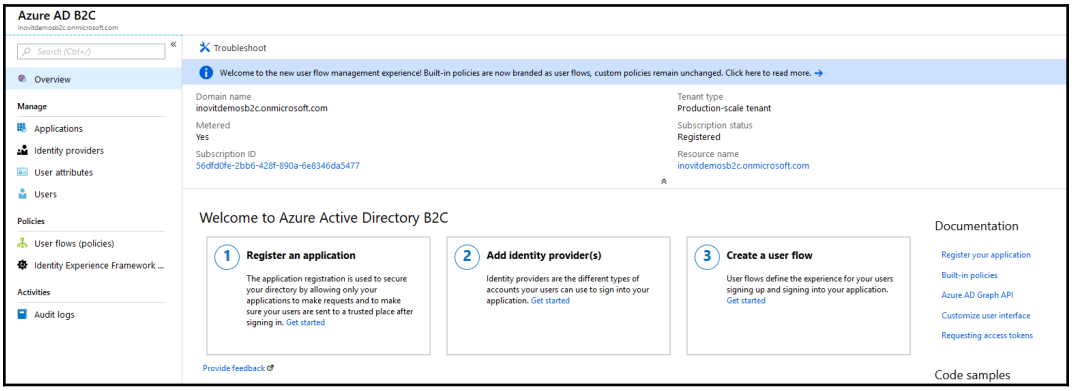

Create new B2C Tenant or Link to existing Tenant
Create a new Azure AD B2C Tenant

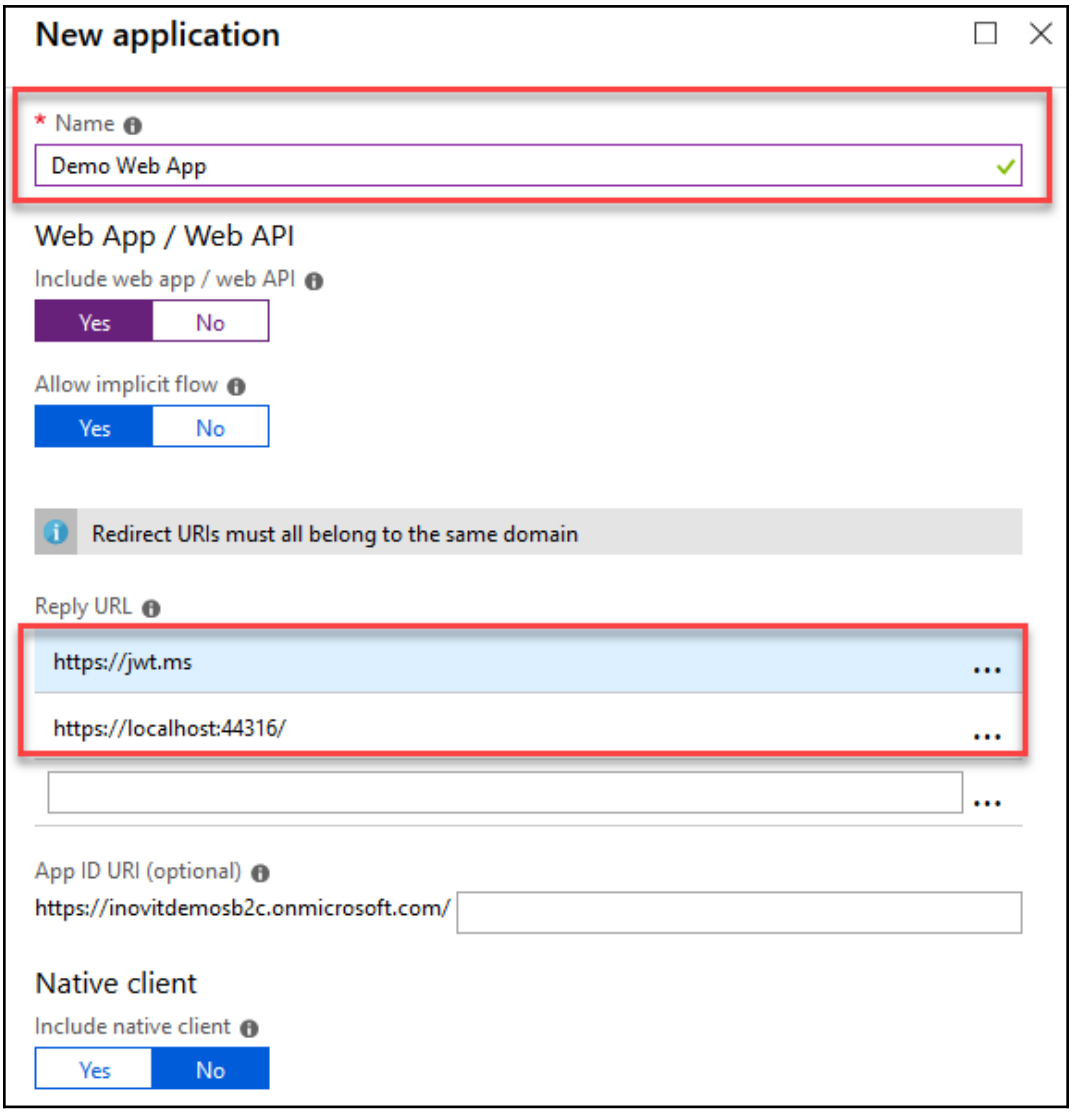

* Organization name
INOVITDEMOS
* Initial domain name
inovitdemosb2c
inovitdemosb2c.onmicrosoft.com
Country or region
Switzerland
Directory creation will take about one minute.

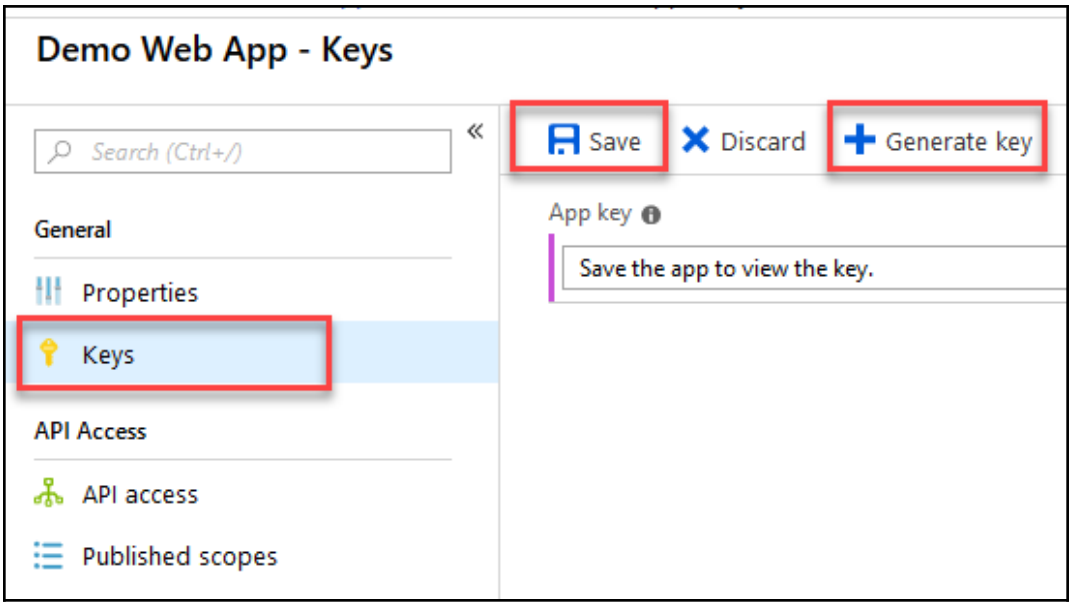

Create new B2C Tenant or Link to existing Tenant
Create a new Azure AD B2C Tenant
Link an existing Azure AD B2C Tenant to my Azure subscription
Azure AD B2C Resource
* Azure AD B2C Tenant
inovitdemosb2c.onmicrosoft.com
Azure AD B2C Resource name
inovitdemosb2c.onmicrosoft.com
* Subscription
MPN - JOCHEN NICKEL
* Resource group
mpnjnirgrp
Create new

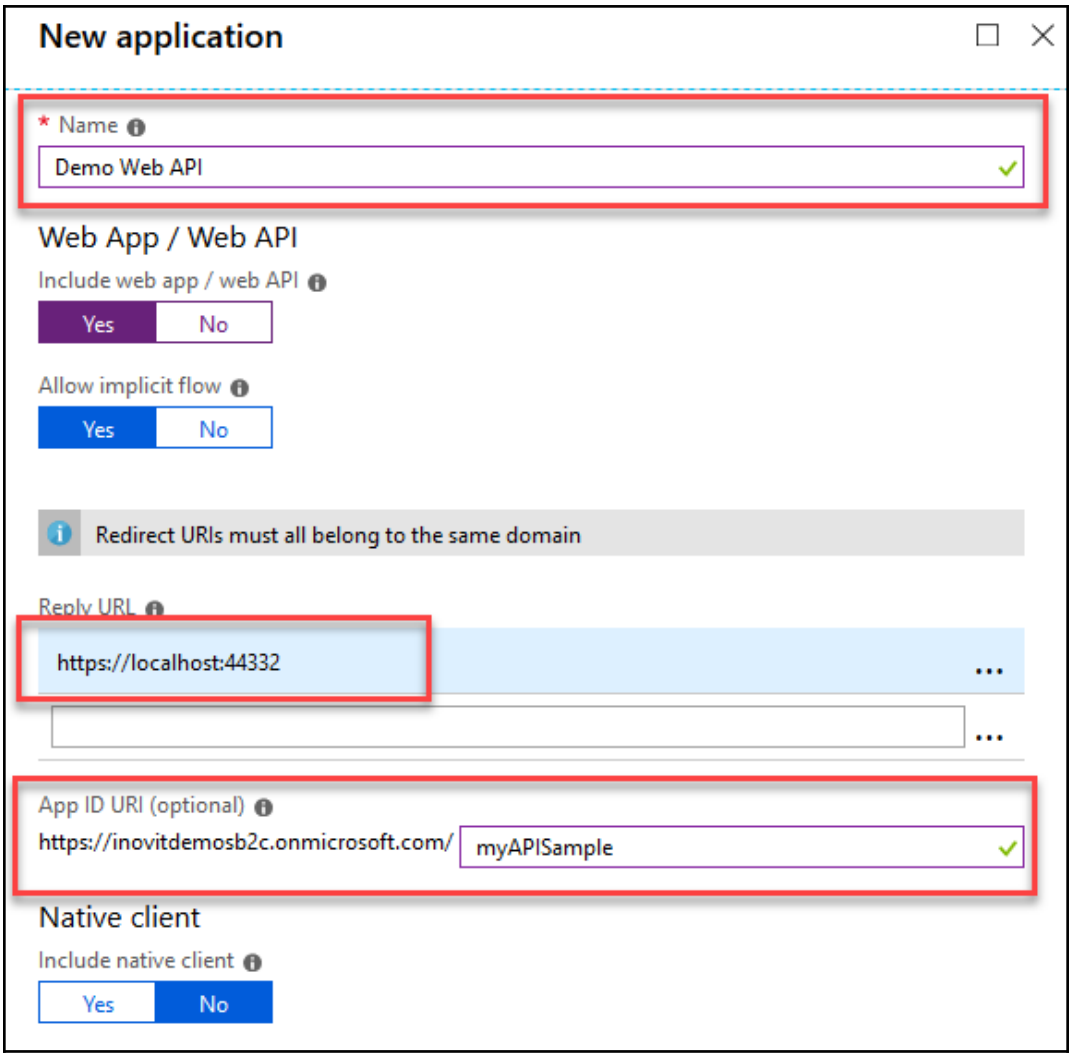

admin@181031inovit...
INOVITDEMOS PROVIDED BY ...
INOVITDEMOS provided by inovit ...
Sign out
Tenant Administrat...
admin@181031inovitdemos.o...
View account
Switch directory
INOVITDEMOS provided by inovit G...
Don.Hall@inovitdemos.ch

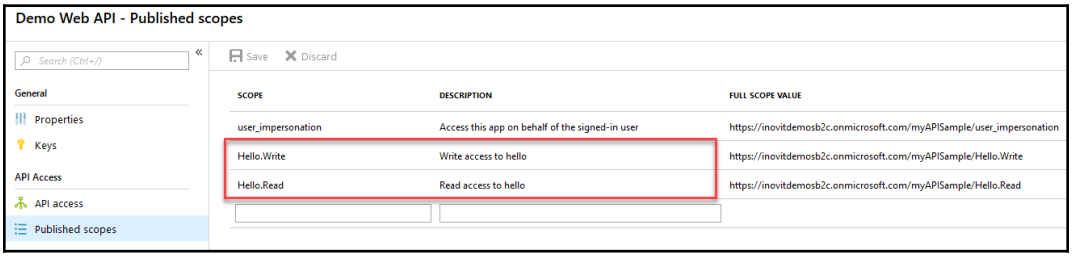

INOVITDEMOS
inovitdemosb2c.onmicrosoft.com
7d20a2bd-9fbf-4961-851e-956e81250a74
INOVITDEMOS provided by inovit GmbH
181031inovitdemos.onmicrosoft.com
7709ca2b-3be8-4d92-89d7-dc1e274b4d0e

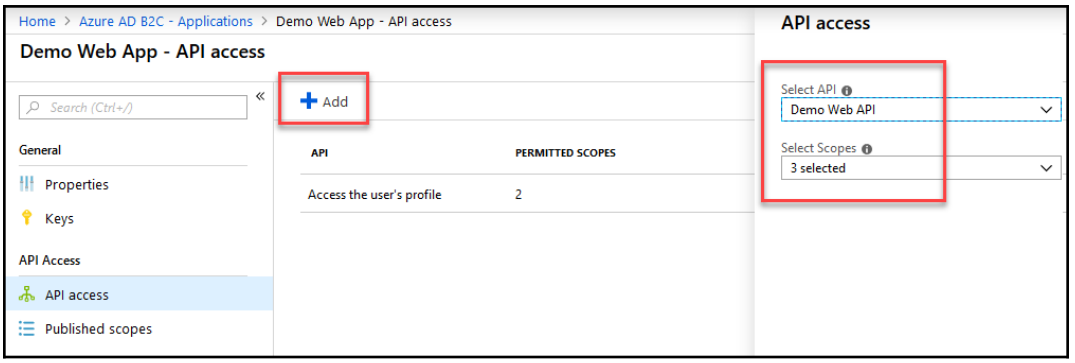

Azure AD B2C
Troubleshoot
Overview
Manage
Applications
Identity providers
User attributes
Users
Policies
User flows (policies)
Identity Experience Framework ...
Activities
Audit logs
Welcome to the new user flow management experience! Built-in policies are now branded as user flows, custom policies remain unchanged. Click here to read more.
Domain name
inovitdemosb2c.onmicrosoft.com
Tenant type
Production-scale tenant
Metered
Yes
Subscription status
Registered
Subscription ID
56dfd0fe-2bb6-428f-890a-6e8346da5477
Resource name
inovitdemosb2c.onmicrosoft.com
Welcome to Azure Active Directory B2C
1 Register an application
The application registration is used to secure your directory by allowing only your applications to make requests and to make sure your users are sent to a trusted place after signing in. Get started
2 Add identity provider(s)
Identity providers are the different types of accounts your users can use to sign into your application. Get started
3 Create a user flow
User flows define the experience for your users signing up and signing into your application. Get started
Provide feedback
Documentation
Register your application
Built-in policies
Azure AD Graph API
Customize user interface
Requesting access tokens
Code samples

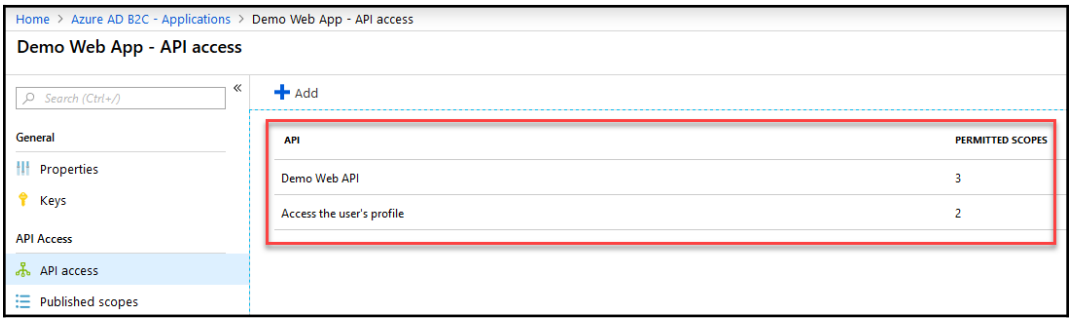

New application
* Name
Demo Web App
Web App / Web API
Include web app / web API
Yes
No
Allow implicit flow
Yes
No
Redirect URIs must all belong to the same domain
Reply URL
https://jwt.ms
https://localhost:44316/
App ID URI (optional)
https://inovitdemosb2c.onmicrosoft.com/
Native client
Include native client
Yes
No

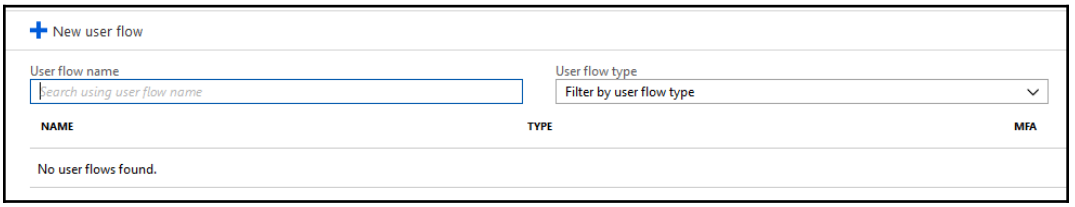

Demo Web App - Keys
Search (Ctrl+/)
Save
Discard
Generate key
General
Properties
Keys
API Access
API access
Published scopes
App key
Save the app to view the key.

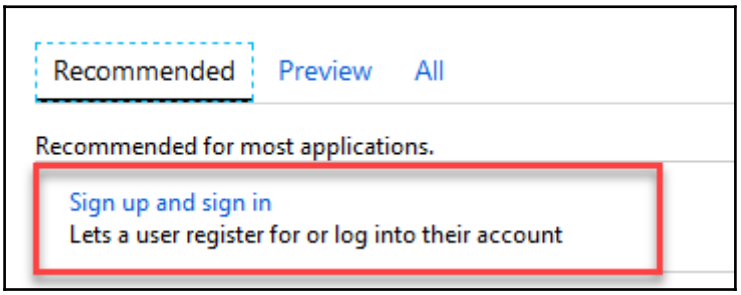

New application
* Name
Demo Web API
Web App / Web API
Include web app / web API
Yes
No
Allow implicit flow
Yes
No
Redirect URIs must all belong to the same domain
Reply URL
https://localhost:44332
App ID URI (optional)
https://inovitdemosb2c.onmicrosoft.com/
myAPISample
Native client
Include native client
Yes
No

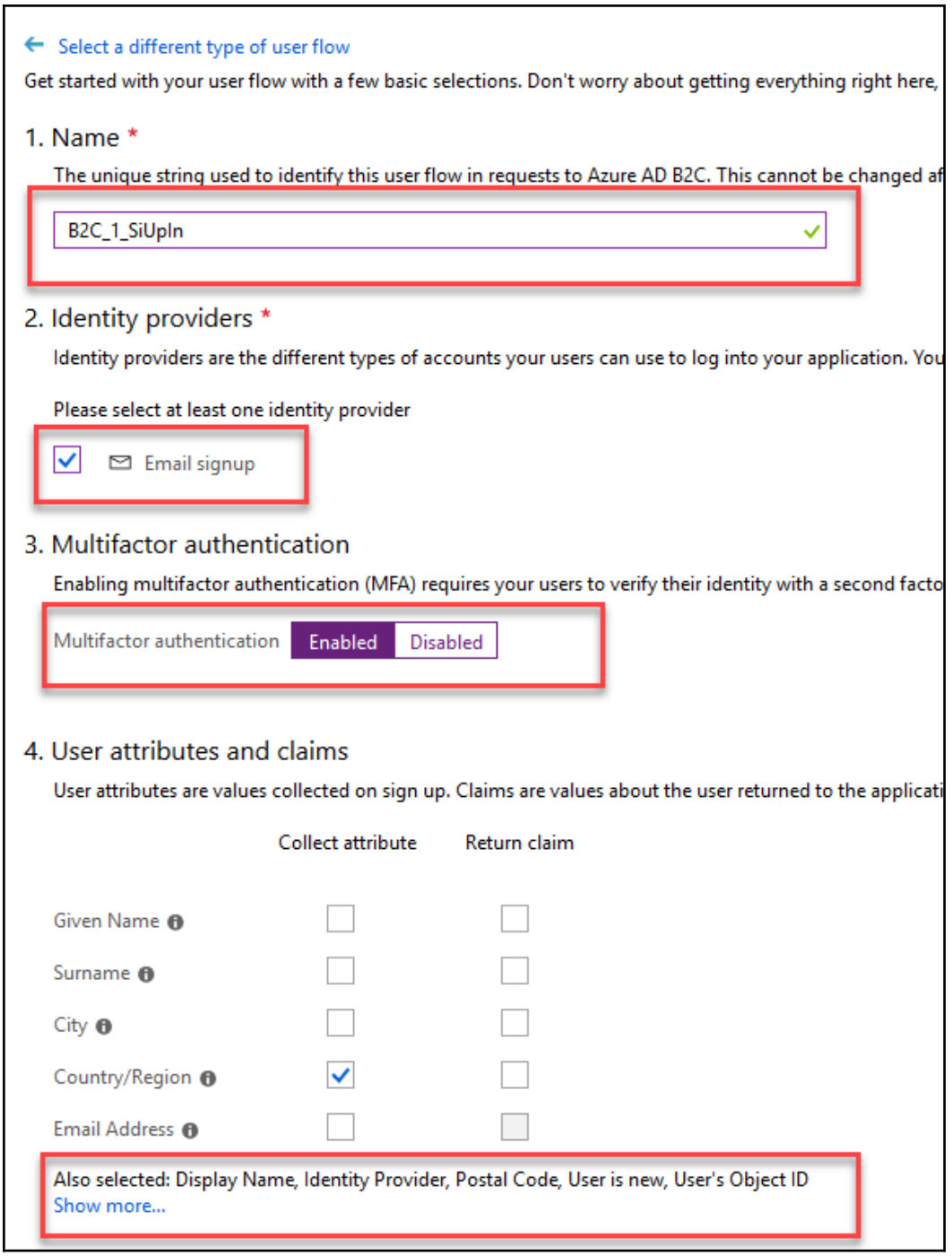

Demo Web API - Published scopes
Search (Ctrl+/)
Save
Discard
General
Properties
Keys
API Access
API access
Published scopes
SCOPE
DESCRIPTION
FULL SCOPE VALUE
user_impersonation
Access this app on behalf of the signed-in user
https://inovitdemosb2c.onmicrosoft.com/myAPISample/user_impersonation
Hello.Write
Write access to hello
https://inovitdemosb2c.onmicrosoft.com/myAPISample/Hello.Write
Hello.Read
Read access to hello
https://inovitdemosb2c.onmicrosoft.com/myAPISample/Hello.Read

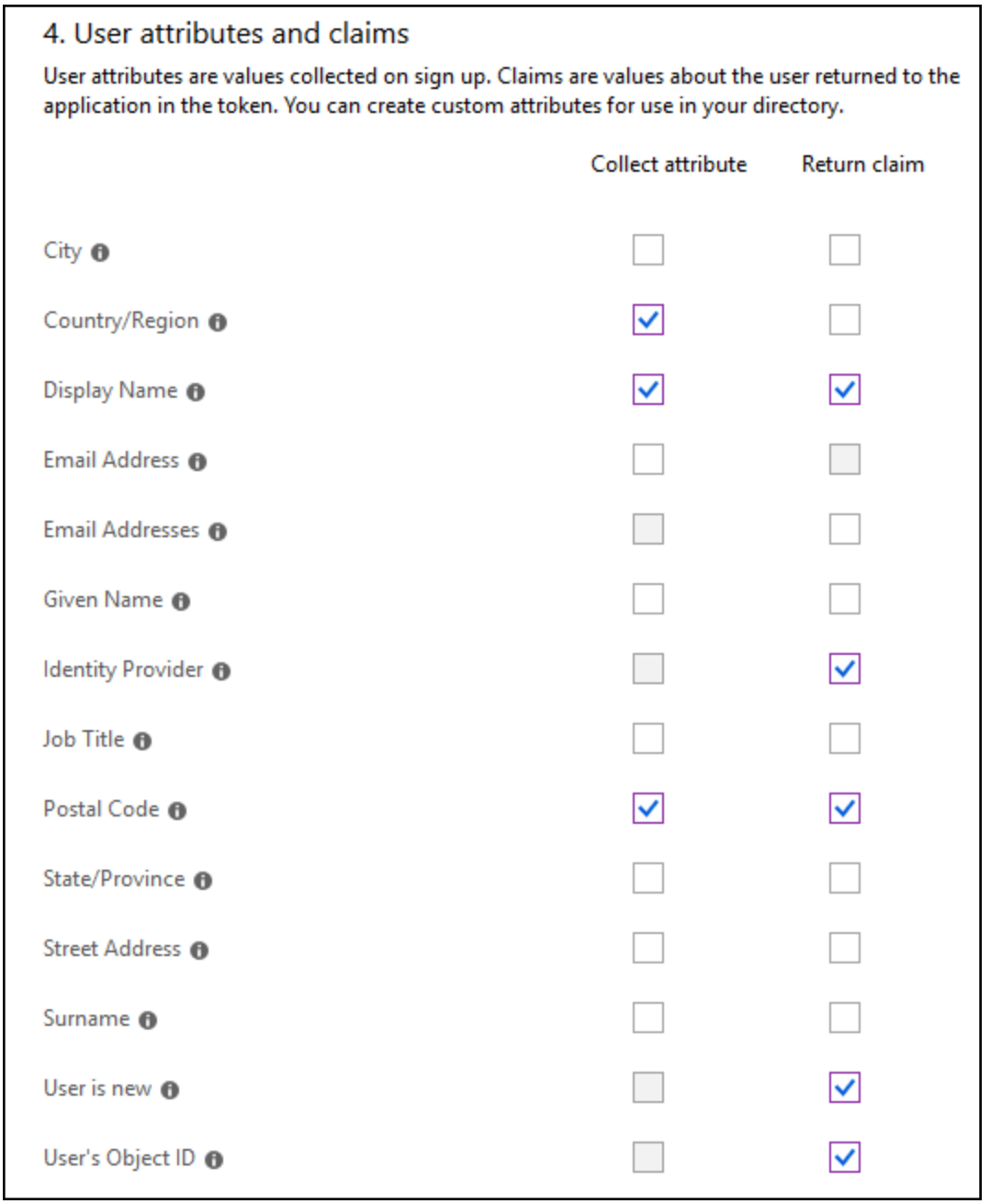

Home > Azure AD B2C - Applications > Demo Web App - API access
Demo Web App - API access
Search (Ctrl+/)
Add
General
Properties
Keys
API Access
API access
Published scopes
API
PERMITTED SCOPES
Access the user's profile
2
API access
Select API
Demo Web API
Select Scopes
3 selected


Home > Azure AD B2C - Applications > Demo Web App - API access
Demo Web App - API access
Search (Ctrl+/)
Add
General
Properties
Keys
API Access
API access
Published scopes
API
PERMITTED SCOPES
Demo Web API
3
Access the user's profile
2


New user flow
User flow name
Search using user flow name
User flow type
Filter by user flow type
NAME
TYPE
MFA
No user flows found.

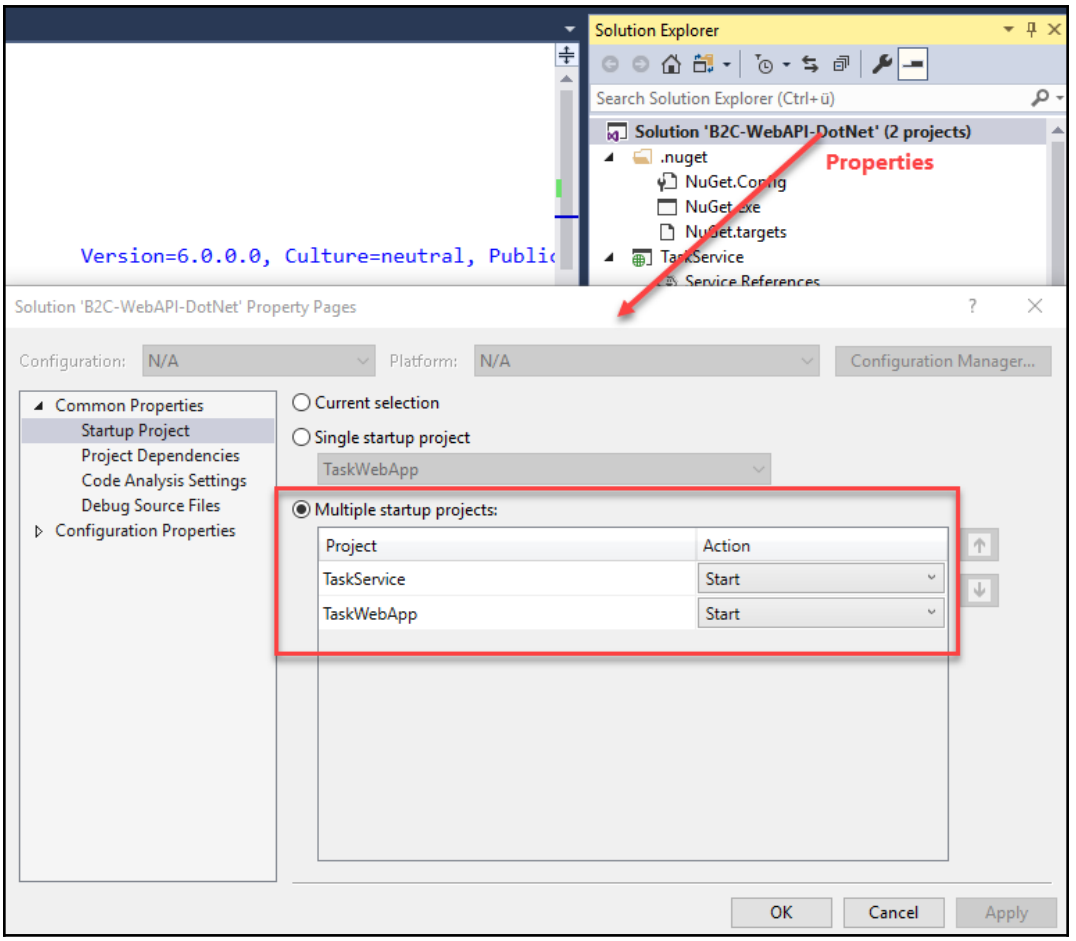

Recommended
Preview
All
Recommended for most applications.
Sign up and sign in
Lets a user register for or log into their account

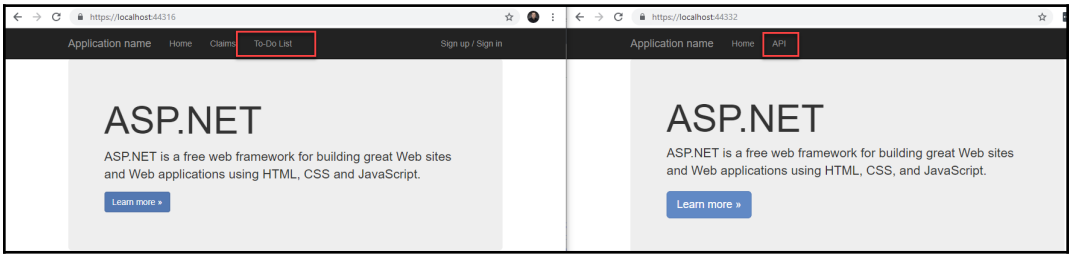

Select a different type of user flow
Get started with your user flow with a few basic selections. Don't worry about getting everything right here,
1. Name *
The unique string used to identify this user flow in requests to Azure AD B2C. This cannot be changed af
B2C_1_SiUpIn
2. Identity providers *
Identity providers are the different types of accounts your users can use to log into your application. You
Please select at least one identity provider
Email signup
3. Multifactor authentication
Enabling multifactor authentication (MFA) requires your users to verify their identity with a second facto
Multifactor authentication
Enabled
Disabled
4. User attributes and claims
User attributes are values collected on sign up. Claims are values about the user returned to the applicati
Collect attribute
Return claim
Given Name
Surname
City
Country/Region
Email Address
Also selected: Display Name, Identity Provider, Postal Code, User is new, User's Object ID
Show more...

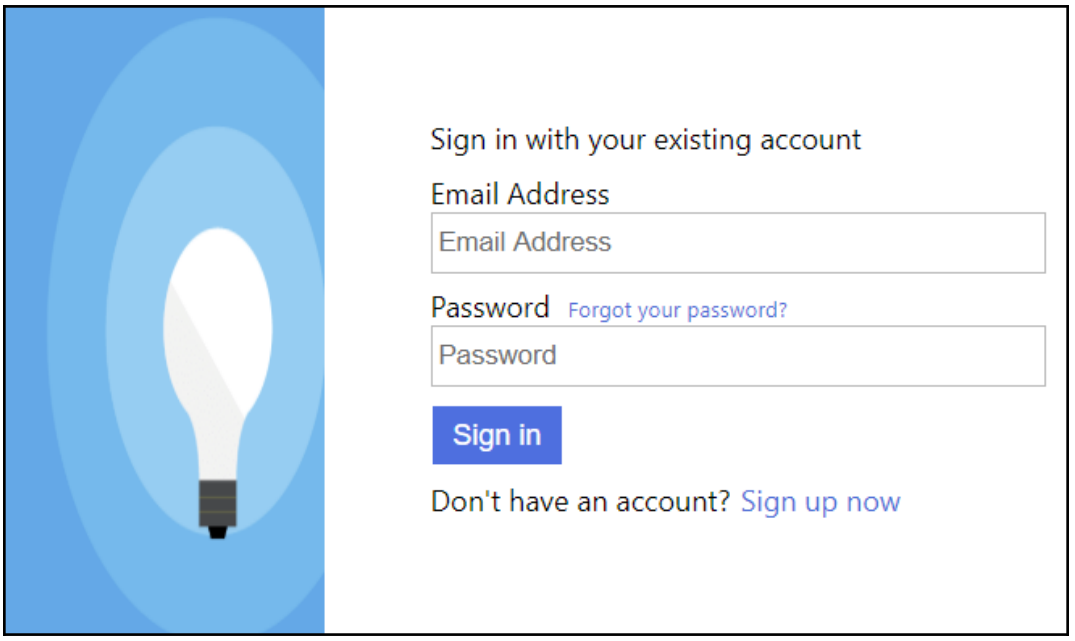

4. User attributes and claims
User attributes are values collected on sign up. Claims are values about the user returned to the application in the token. You can create custom attributes for use in your directory.
Collect attribute
Return claim
City
Country/Region
Display Name
Email Address
Email Addresses
Given Name
Identity Provider
Job Title
Postal Code
State/Province
Street Address
Surname
User is new
User's Object ID

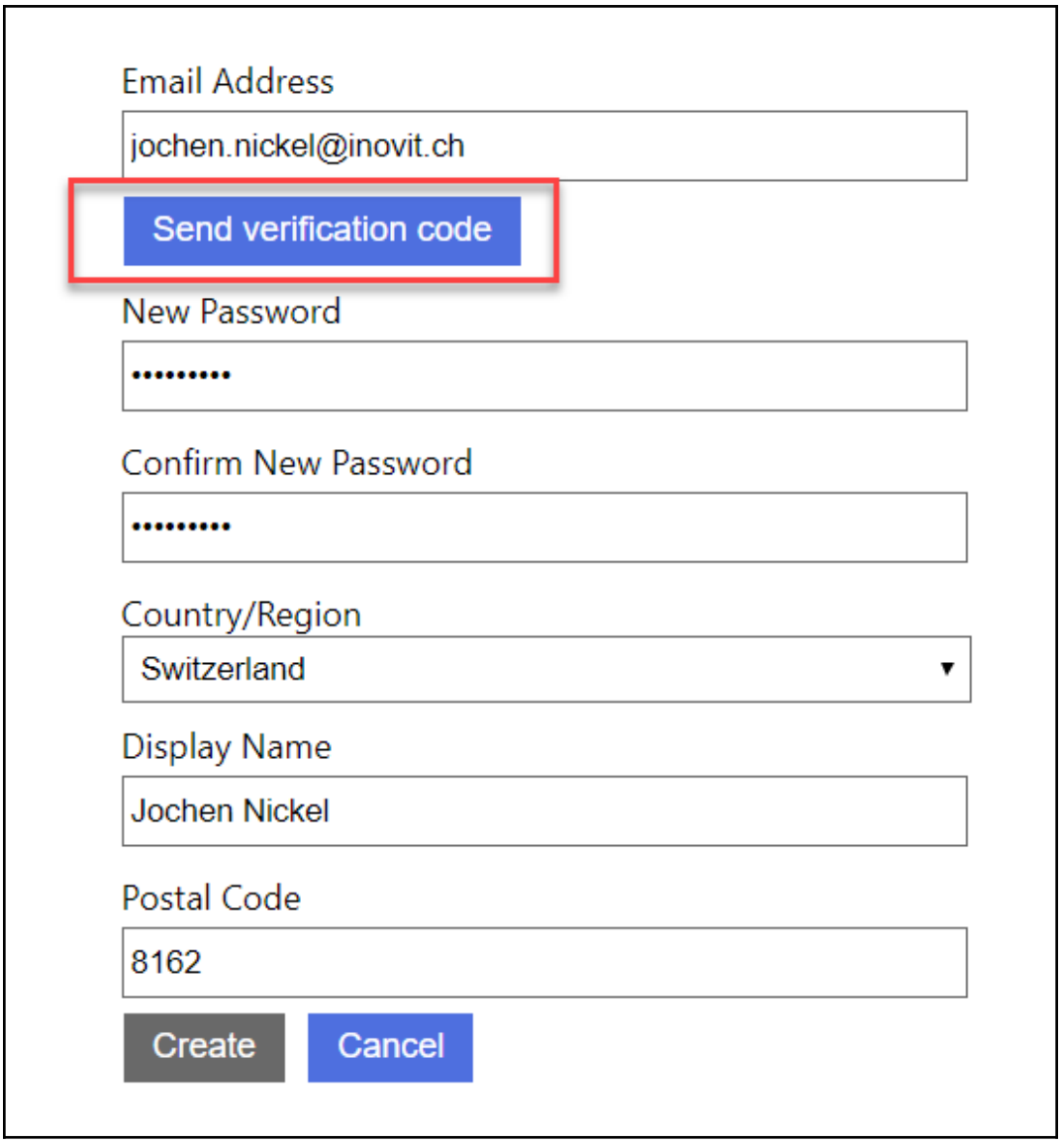
```
<configuration>
  <appSettings>
    <add key="webpages:Version" value="3.0.0.0" />
    <add key="webpages:Enabled" value="false" />
    <add key="ClientValidationEnabled" value="true" />
    <add key="UnobtrusiveJavaScriptEnabled" value="true" />
    <add key="ida:Tenant" value="inovitdemosb2c.onmicrosoft.com" />
    <add key="ida:ClientId" value="d92c671f-c576-45b1-9d53-0510f306bccc" />
    <add key="ida:ClientSecret" value="WdLrw#+DZ6L#vW7,3(ryS.uP" />
    <add key="ida:AadInstance" value="https://login.microsoftonline.com/tfp/{0}/{1}/v2.0/.well-known/openid-configuration" />
    <add key="ida:RedirectUri" value="https://localhost:44316/" />
    <add key="ida:SignUpSignInPolicyId" value="b2c_1_SiUpIn" />
    <add key="ida:EditProfilePolicyId" value="b2c_1_SiPe" />
    <add key="ida:ResetPasswordPolicyId" value="b2c_1_SSPR" />
    <!-- Uncomment the localhost url if you want to run the API locally -->
    <add key="api:TaskServiceUrl" value="https://localhost:44332/" />
    <!--add key="api:TaskServiceUrl" value="https://localhost:44332/" /-->
    <!-- The following settings is used for requesting access tokens -->
    <add key="api:ApiIdentifier" value="https://inovitdemosb2c.onmicrosoft.com/myAPISample/" />
    <add key="api:ReadScope" value="Hello.Read" />
    <add key="api:WriteScope" value="Hello.Write" />
  </appSettings>
```

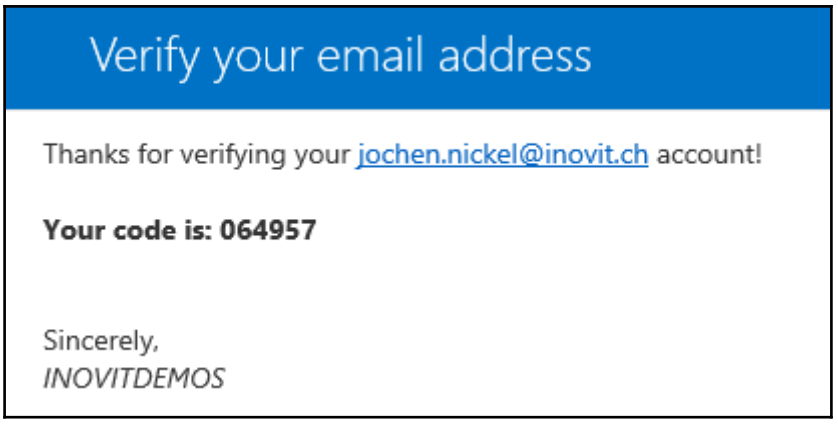
```
<appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="ida:AadInstance" value="https://login.microsoftonline.com/{0}/v2.0/.well-known/openid-configuration?p={1}" />
  <add key="ida:Tenant" value="inovitdemosb2c.onmicrosoft.com" />
  <add key="ida:ClientId" value="2f73f192-e9c5-4fa8-8429-9aa3fd13293e" />
  <add key="ida:SignUpSignInPolicyId" value="B2C_1_SiUpIn" />
  <!-- The following settings is used for requesting access tokens -->
  <add key="api:ReadScope" value="Hello.Read" />
  <add key="api:WriteScope" value="Hello.Write" />
</appSettings>
<!--
```

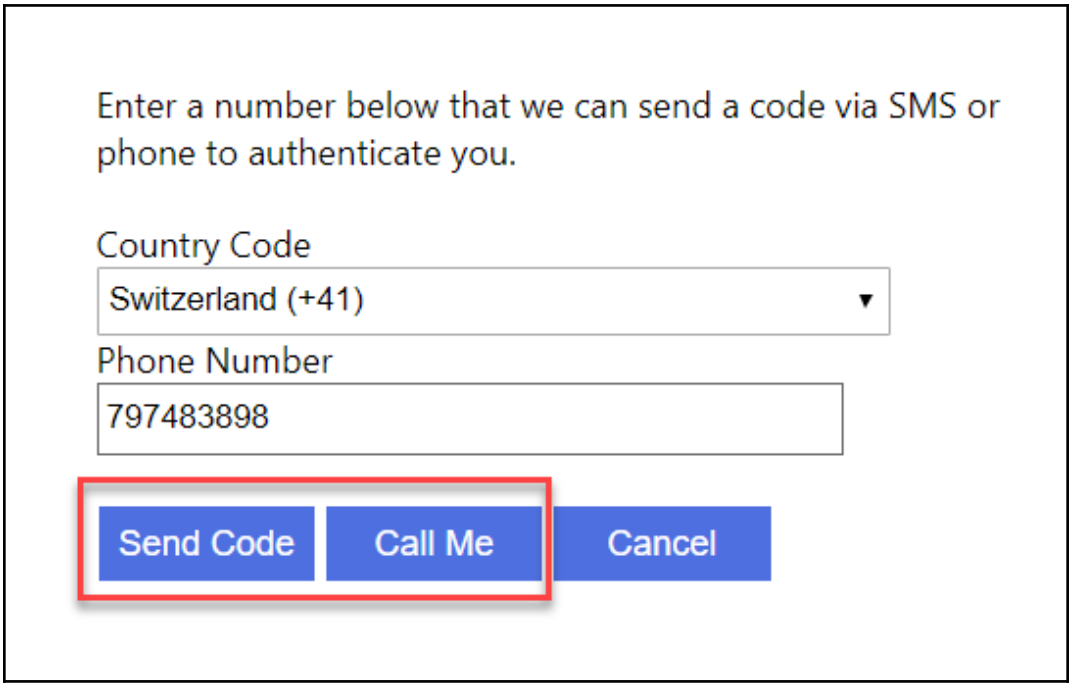

Solution Explorer
Search Solution Explorer (Ctrl+ü)
Solution 'B2C-WebAPI-DotNet' (2 projects)
.nuget
NuGet.Config
NuGet.exe
NuGet.targets
TaskService
Service References
Properties
Version=6.0.0.0, Culture=neutral, Publi
Solution 'B2C-WebAPI-DotNet' Property Pages
Configuration: N/A
Platform: N/A
Configuration Manager...
Common Properties
Startup Project
Project Dependencies
Code Analysis Settings
Debug Source Files
Configuration Properties
Current selection
Single startup project
TaskWebApp
Multiple startup projects:
Project
Action
TaskService
Start
TaskWebApp
Start
OK
Cancel
Apply

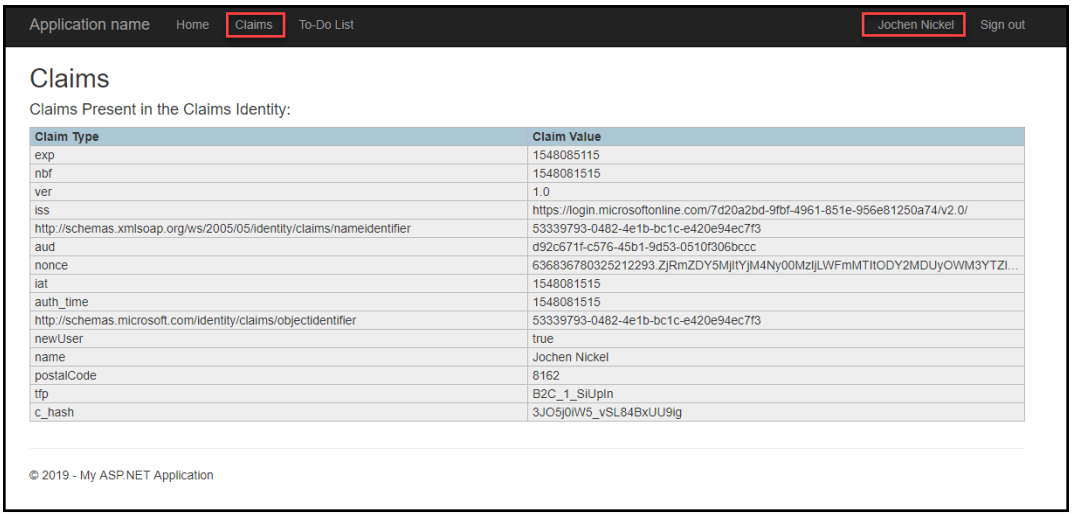

https://localhost:44316
Application name
Home
Claims
To-Do List
Sign up / Sign in
ASP.NET
ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS and JavaScript.
Learn more »
https://localhost:44332
Application name
Home
API
ASP.NET
ASP.NET is a free web framework for building great Web sites and Web applications using HTML, CSS, and JavaScript.
Learn more »

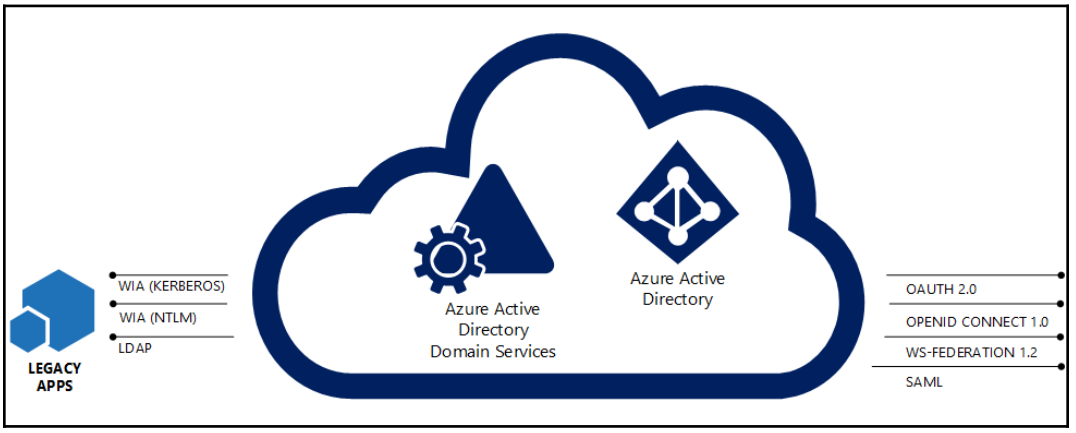

Sign in with your existing account
Email Address
Email Address
Password
Forgot your password?
Password
Sign in
Don't have an account?
Sign up now

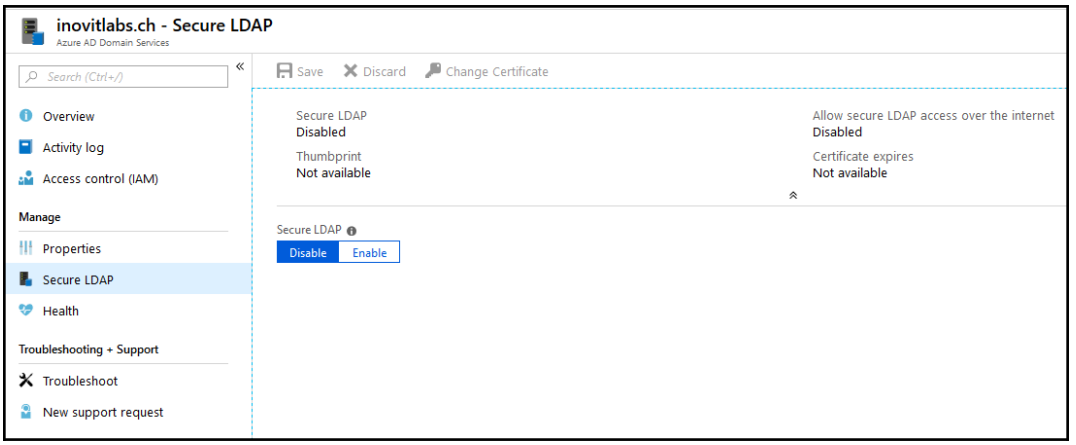

Email Address
jochen.nickel@inovit.ch
Send verification code
New Password
Confirm New Password
Country/Region
Switzerland
Display Name
Jochen Nickel
Postal Code
8162
Create
Cancel

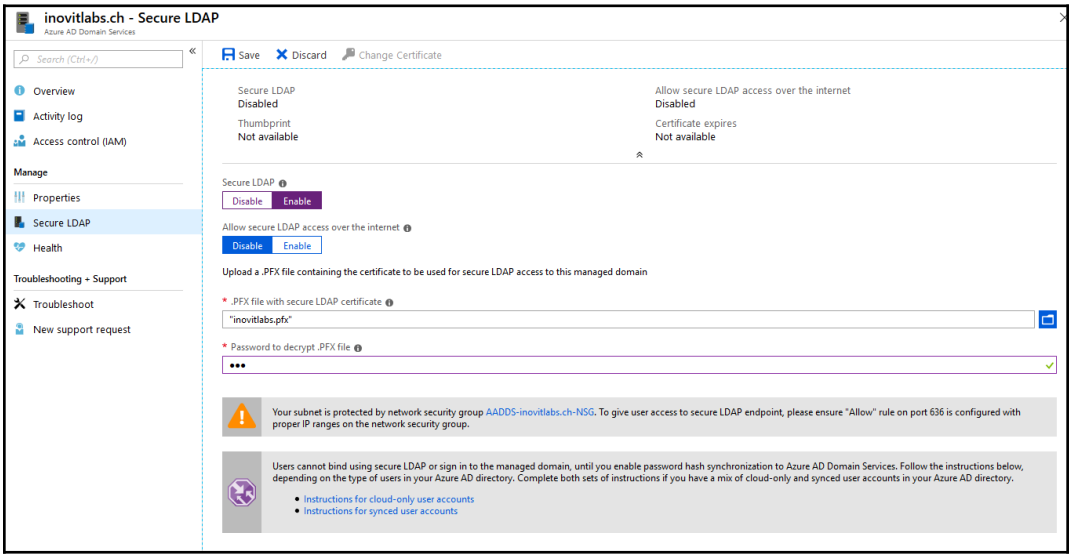

Verify your email address
Thanks for verifying your jochen.nickel@inovit.ch account!
Your code is: 064957
Sincerely,
INOVITDEMOS

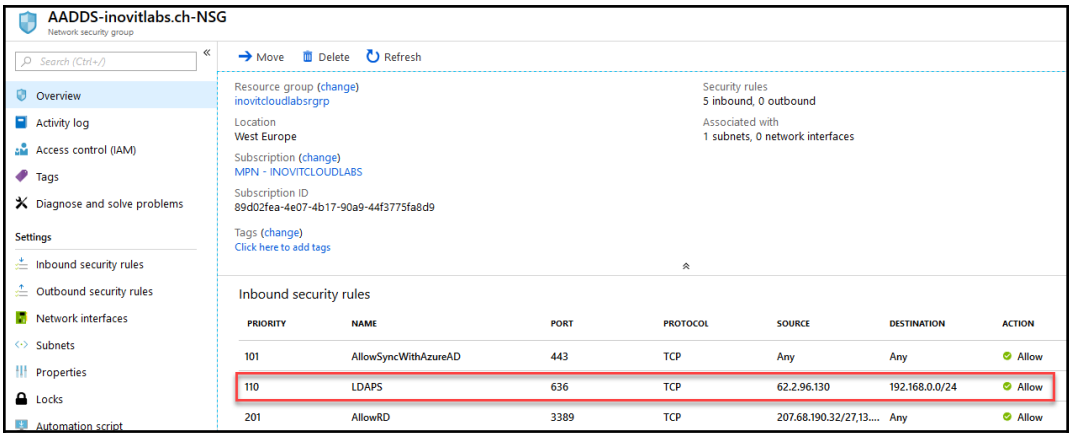

Enter a number below that we can send a code via SMS or phone to authenticate you.
Country Code
Switzerland (+41)
Phone Number
797483898
Send Code
Call Me
Cancel

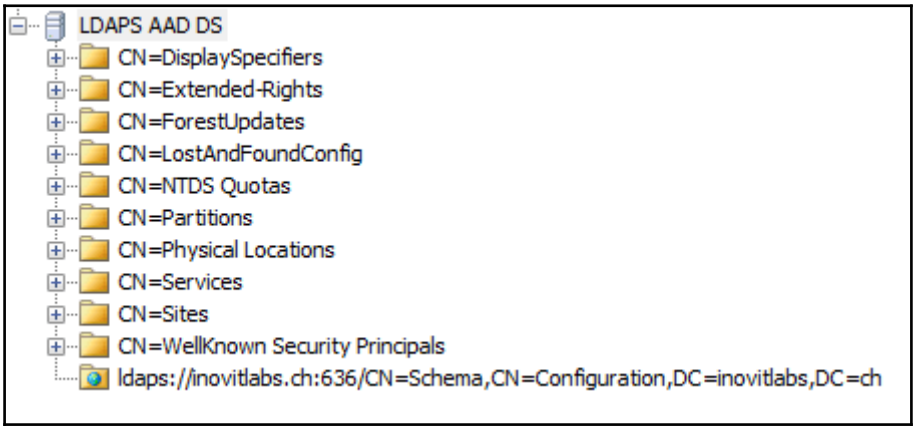

Application name
Home
Claims
To-Do List
Jochen Nickel
Sign out
Claims
Claims Present in the Claims Identity:
Claim Type
Claim Value
exp
1548085115
nbf
1548081515
ver
1.0
iss
https://login.microsoftonline.com/7d20a2bd-9fbf-4961-851e-956e81250a74/v2.0/
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier
53339793-0482-4e1b-bc1c-e420e94ec7f3
aud
d92c671f-c576-45b1-9d53-0510f306bccc
nonce
636836780325212293.ZjRmZDY5MjItYjM4Ny00MzljLWFmMTItODY2MDUyOWM3YTZl...
iat
1548081515
auth_time
1548081515
http://schemas.microsoft.com/identity/claims/objectidentifier
53339793-0482-4e1b-bc1c-e420e94ec7f3
newUser
true
name
Jochen Nickel
postalCode
8162
tfp
B2C_1_SiUpIn
c_hash
3JO5j0iW5_vSL84BxUU9Ig
© 2019 - My ASP.NET Application

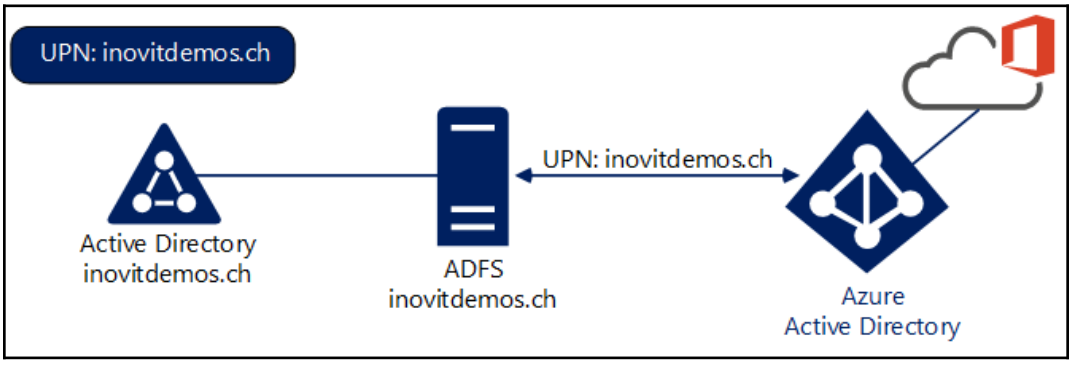

LEGACY APPS
WIA (KERBEROS)
WIA (NTLM)
LDAP
Azure Active Directory Domain Services
Azure Active Directory
OAUTH 2.0
OPENID CONNECT 1.0
WS-FEDERATION 1.2
SAML

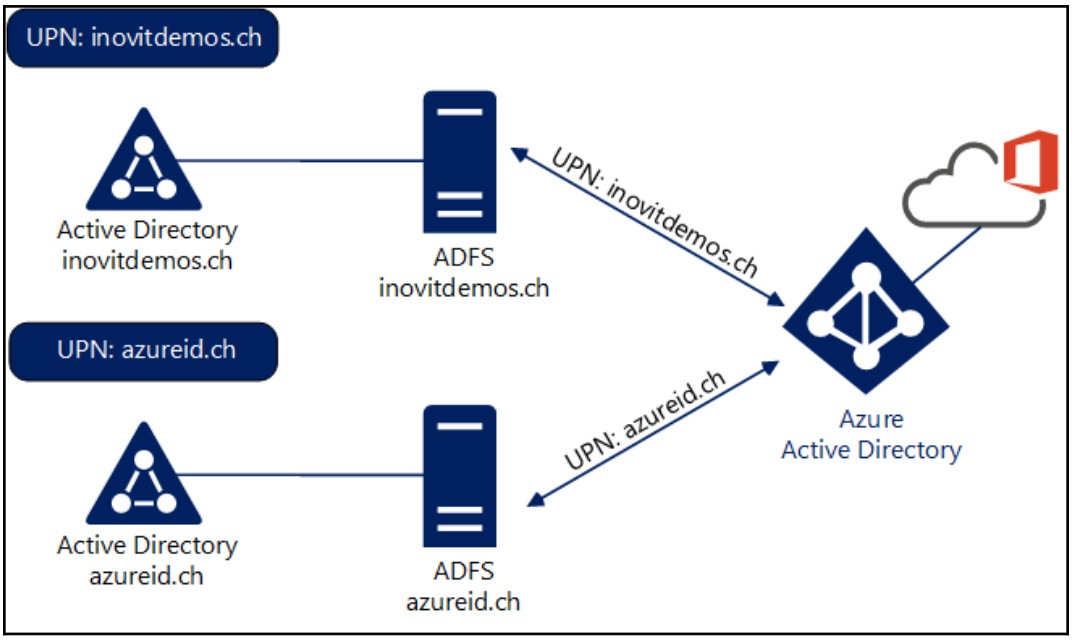

inovitlabs.ch - Secure LDAP
Azure AD Domain Services
Search (Ctrl+/)
Save
Discard
Change Certificate
Overview
Activity log
Access control (IAM)
Manage
Properties
Secure LDAP
Health
Troubleshooting + Support
Troubleshoot
New support request
Secure LDAP
Disabled
Thumbprint
Not available
Allow secure LDAP access over the internet
Disabled
Certificate expires
Not available
Secure LDAP
Disable
Enable

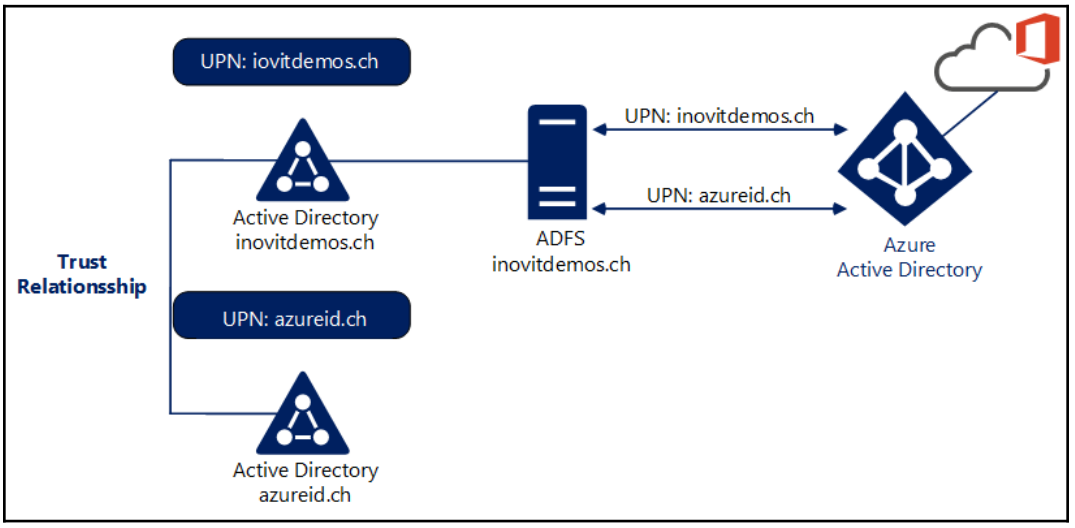

inovitlabs.ch - Secure LDAP
Azure AD Domain Services
Search (Ctrl+/)
Save
Discard
Change Certificate
Overview
Activity log
Access control (IAM)
Manage
Properties
Secure LDAP
Health
Troubleshooting + Support
Troubleshoot
New support request
Secure LDAP
Disabled
Thumbprint
Not available
Allow secure LDAP access over the internet
Disabled
Certificate expires
Not available
Secure LDAP
Disable
Enable
Allow secure LDAP access over the internet
Disable
Enable
Upload a .PFX file containing the certificate to be used for secure LDAP access to this managed domain
* .PFX file with secure LDAP certificate
"inovitlabs.pfx"
* Password to decrypt .PFX file
Your subnet is protected by network security group AADDS-inovitlabs.ch-NSG. To give user access to secure LDAP endpoint, please ensure "Allow" rule on port 636 is configured with proper IP ranges on the network security group.
Users cannot bind using secure LDAP or sign in to the managed domain, until you enable password hash synchronization to Azure AD Domain Services. Follow the instructions below, depending on the type of users in your Azure AD directory. Complete both sets of instructions if you have a mix of cloud-only and synced user accounts in your Azure AD directory.
Instructions for cloud-only user accounts
Instructions for synced user accounts

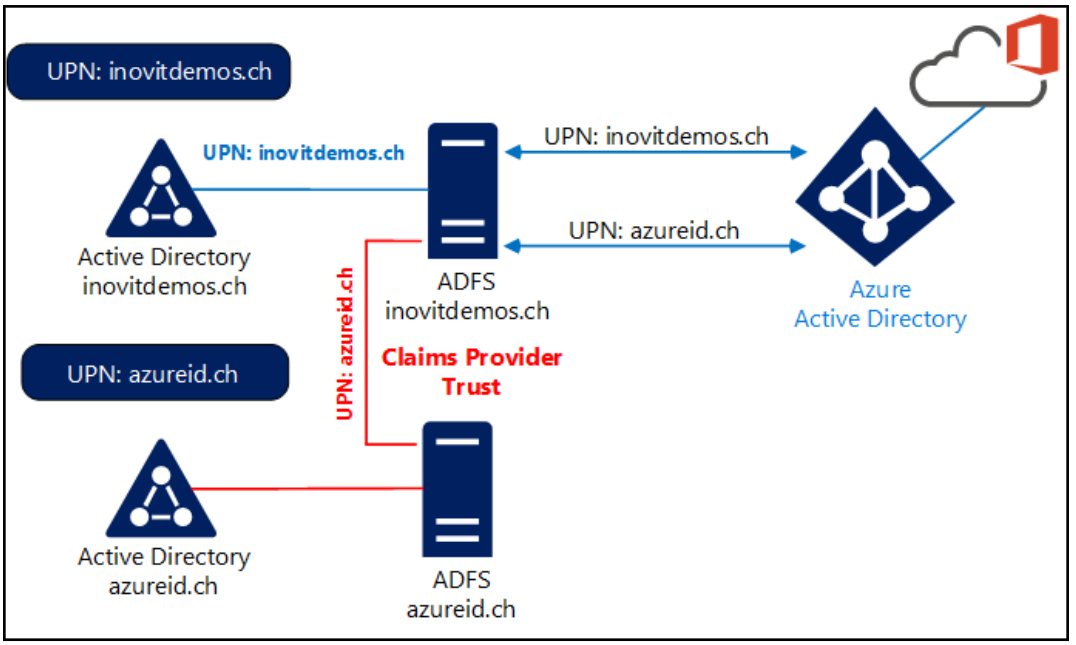

AADDS-inovitlabs.ch-NSG
Network security group
Search (Ctrl+/)
Move
Delete
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Automation script
Resource group (change)
inovitcloudlabsrgrp
Location
West Europe
Subscription (change)
MPN - INOVITCLOUDLABS
Subscription ID
89d02fea-4e07-4b17-90a9-44f3775fa8d9
Tags (change)
Click here to add tags
Security rules
5 inbound, 0 outbound
Associated with
1 subnets, 0 network interfaces
Inbound security rules
PRIORITY NAME PORT PROTOCOL SOURCE DESTINATION ACTION
101 AllowSyncWithAzureAD 443 TCP Any Any Allow
110 LDAPS 636 TCP 62.2.96.130 192.168.0.0/24 Allow
201 AllowRD 3389 TCP 207.68.190.32/27,13.... Any Allow

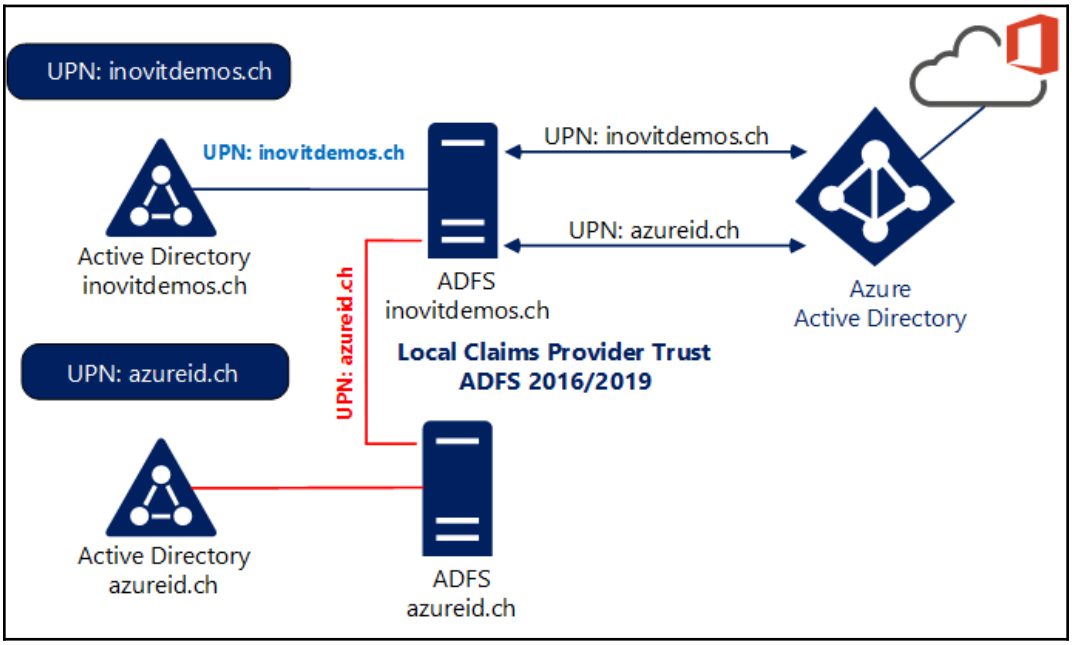

LDAPS AAD DS
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundConfig
CN=NTDS Quotas
CN=Partitions
CN=Physical Locations
CN=Services
CN=Sites
CN=WellKnown Security Principals
ldaps://inovitlabs.ch:636/CN=Schema,CN=Configuration,DC=inovitlabs,DC=ch

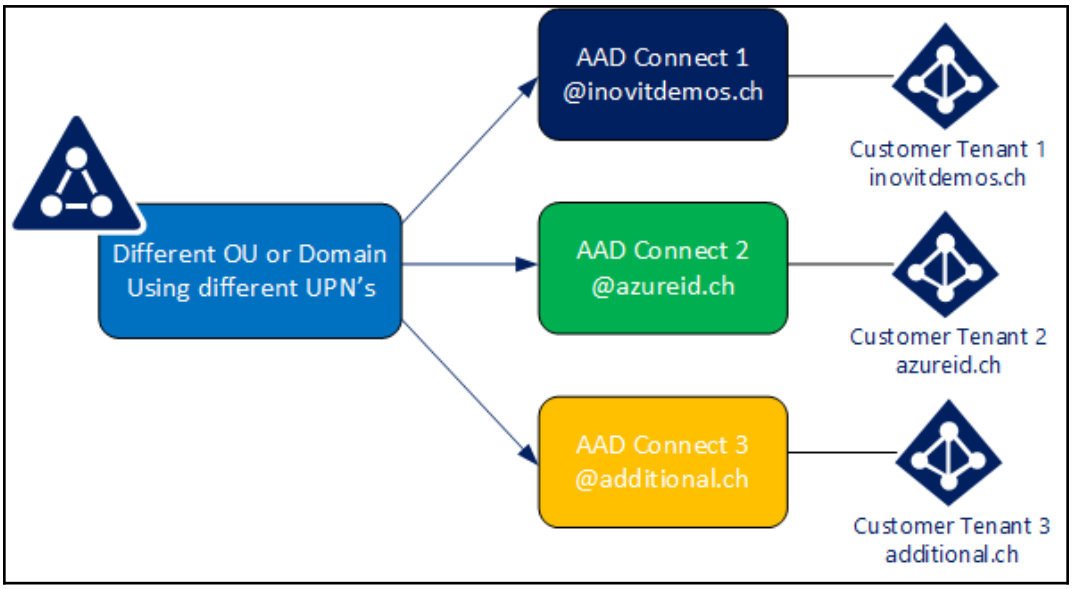

UPN: inovitdemos.ch
Active Directory
inovitdemos.ch
ADFS
inovitdemos.ch
UPN: inovitdemos.ch
Azure
Active Directory

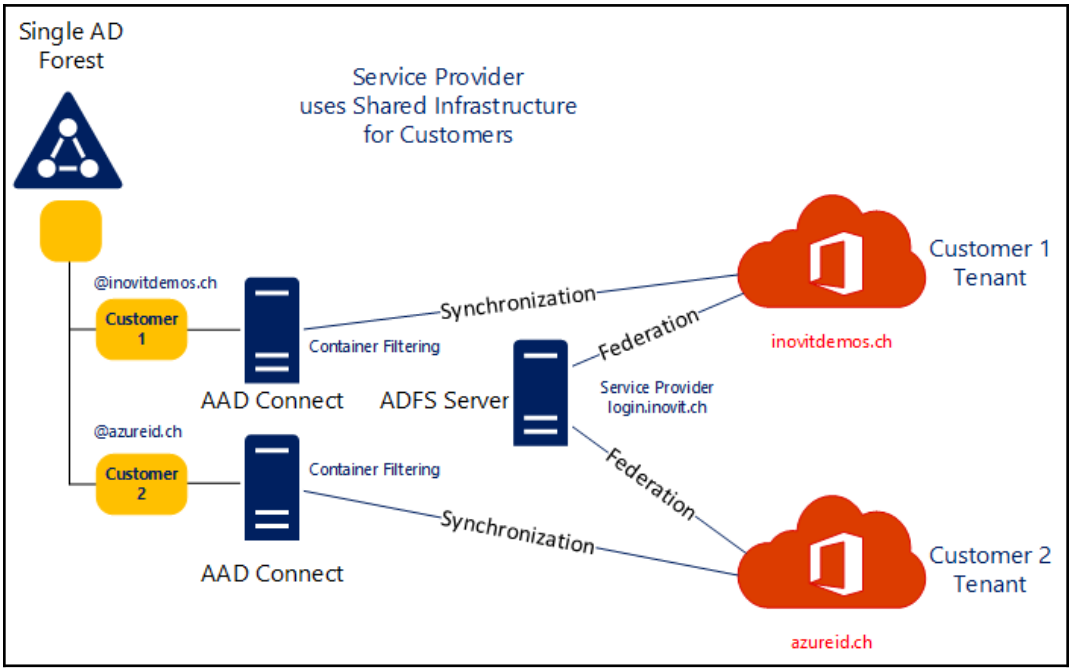

UPN: inovitdemos.ch
Active Directory
inovitdemos.ch
ADFS
inovitdemos.ch
UPN: inovitdemos.ch
UPN: azureid.ch
Azure
Active Directory
UPN: azureid.ch
Active Directory
azureid.ch
ADFS
azureid.ch

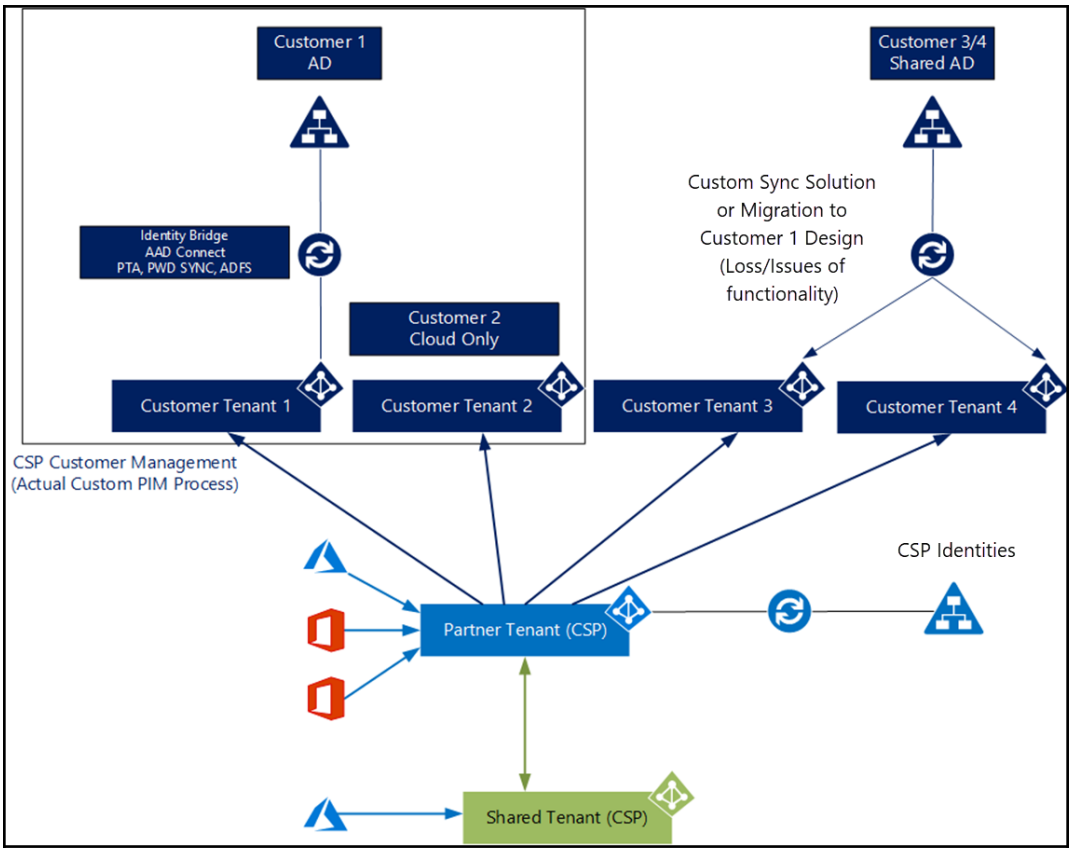

UPN: iovitdemos.ch
Active Directory
inovitdemos.ch
UPN: inovitdemos.ch
UPN: azureid.ch
ADFS
inovitdemos.ch
Azure
Active Directory
Trust
Relationsship
UPN: azureid.ch
Active Directory
azureid.ch


UPN: inovitdemos.ch
UPN: inovitdemos.ch
Active Directory
inovitdemos.ch
UPN: inovitdemos.ch
UPN: azureid.ch
ADFS
inovitdemos.ch
Azure
Active Directory
UPN: azureid.ch
Claims Provider
Trust
UPN: azureid.ch
Active Directory
azureid.ch
ADFS
azureid.ch

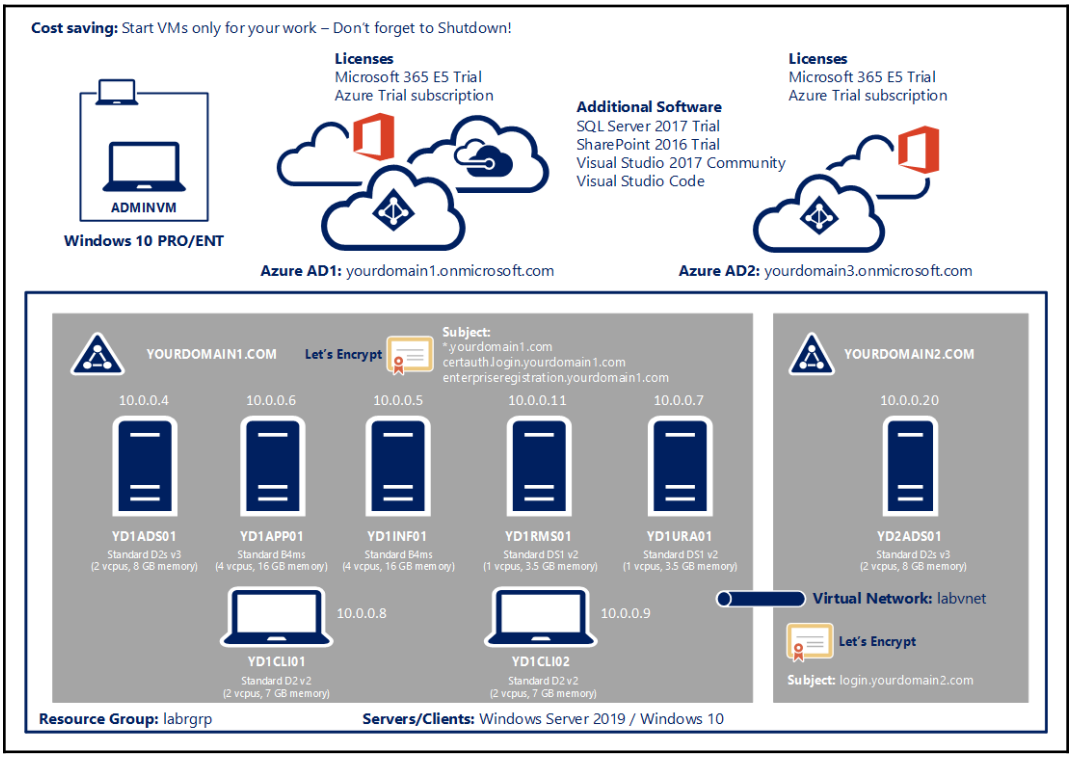

UPN: inovitdemos.ch
UPN: inovitdemos.ch
Active Directory
inovitdemos.ch
UPN: inovitdemos.ch
UPN: azureid.ch
ADFS
inovitdemos.ch
Azure
Active Directory
UPN: azureid.ch
Local Claims Provider Trust
ADFS 2016/2019
UPN: azureid.ch
Active Directory
azureid.ch
ADFS
azureid.ch

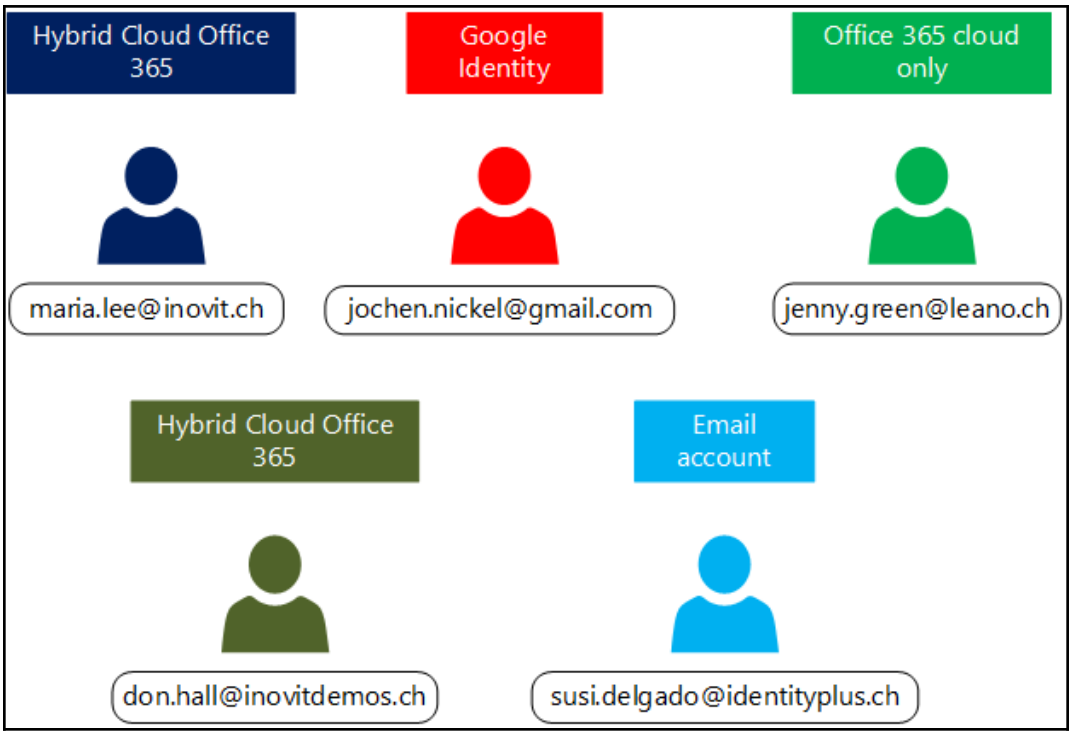

AAD Connect 1
@inovitdemos.ch
Customer Tenant 1
inovitdemos.ch
Different OU or Domain
Using different UPN's
AAD Connect 2
@azureid.ch
Customer Tenant 2
azureid.ch
AAD Connect 3
@additional.ch
Customer Tenant 3
additional.ch

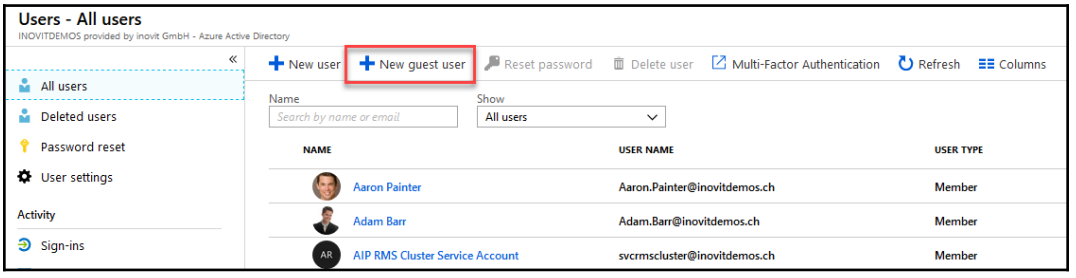

Single AD
Forest
Service Provider
uses Shared Infrastructure
for Customers
@inovitdemos.ch
Customer
1
Container Filtering
AAD Connect
Synchronization
Federation
Customer 1
Tenant
inovitdemos.ch
ADFS Server
Service Provider
login.inovit.ch
@azureid.ch
Customer
2
Container Filtering
AAD Connect
Federation
Synchronization
Customer 2
Tenant
azureid.ch

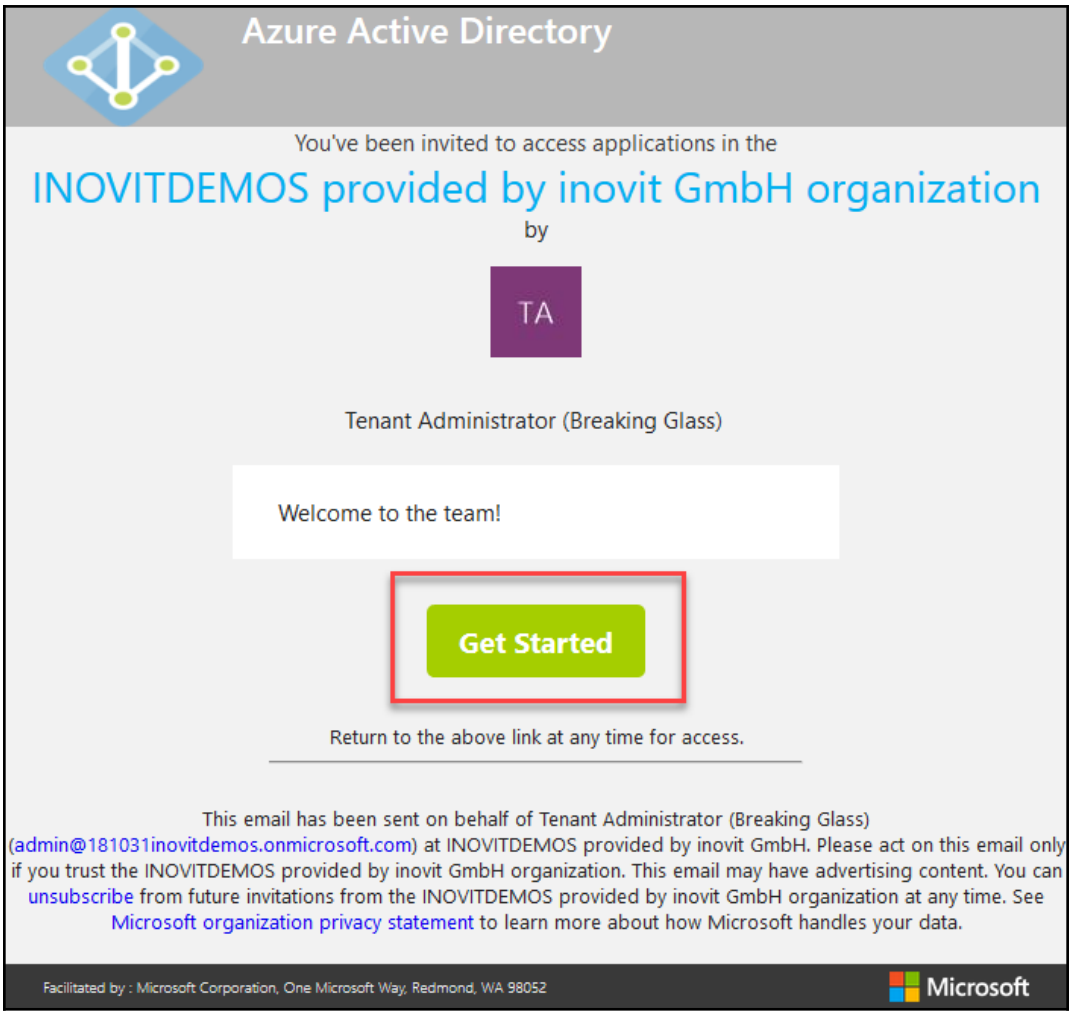

Customer 1
AD
Customer 3/4
Shared AD
Custom Sync Solution
or Migration to
Customer 1 Design
(Loss/Issues of
functionality)
Identity Bridge
AAD Connect
PTA, PWD SYNC, ADFS
Customer 2
Cloud Only
Customer Tenant 1
Customer Tenant 2
Customer Tenant 3
Customer Tenant 4
CSP Customer Management
(Actual Custom PIM Process)
CSP Identities
Partner Tenant (CSP)
Shared Tenant (CSP)

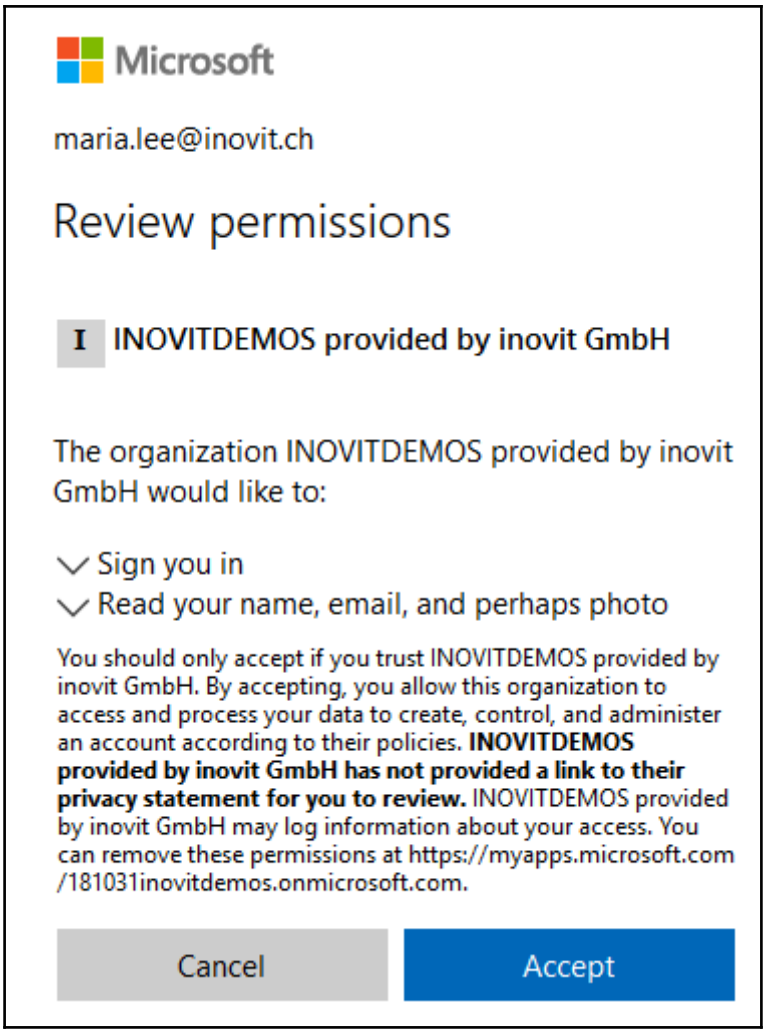
Chapter 11: Creating Identity Life Cycle Management in Azure

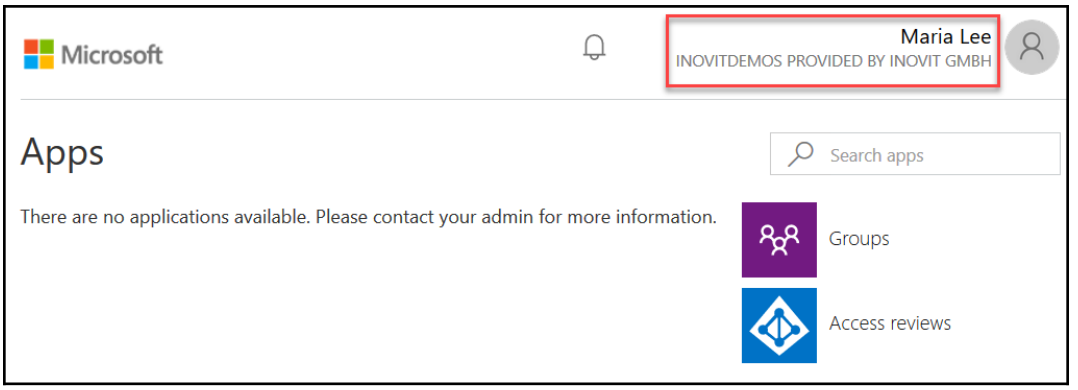


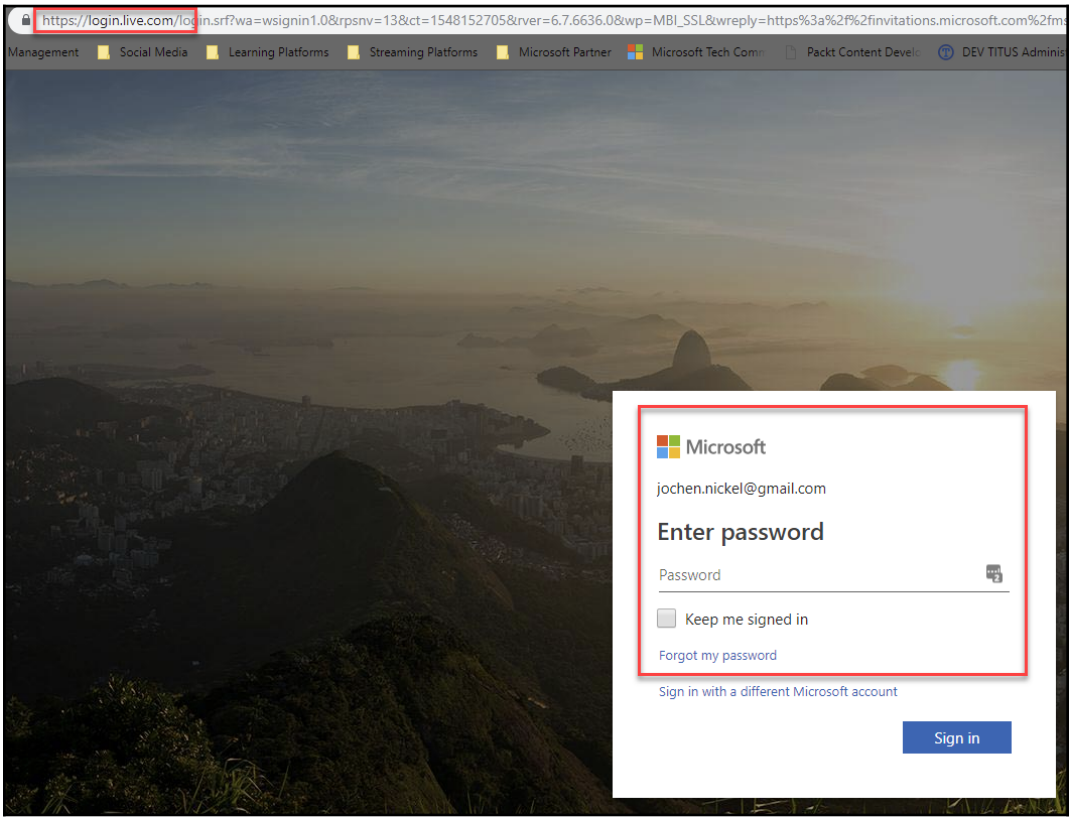

Hybrid Cloud Office 365
Google Identity
Office 365 cloud only
maria.lee@inovit.ch
jochen.nickel@gmail.com
jenny.green@leano.ch
Hybrid Cloud Office 365
Email account
don.hall@inovitdemos.ch
susi.delgado@identityplus.ch

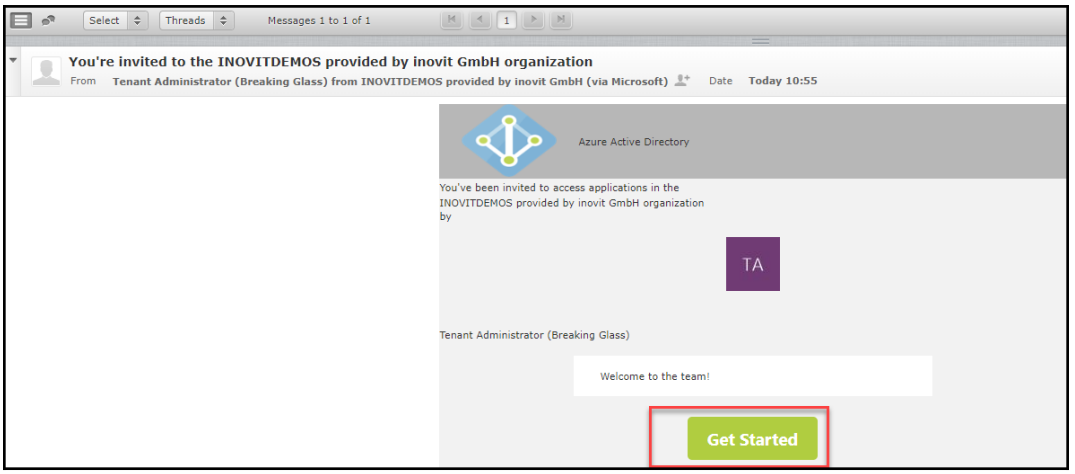

Users - All users
INOVITDEMOS provided by inovit GmbH - Azure Active Directory
New user
New guest user
Reset password
Delete user
Multi-Factor Authentication
Refresh
Columns
All users
Deleted users
Password reset
User settings
Activity
Sign-ins
Name
Search by name or email
Show
All users
NAME
USER NAME
USER TYPE
Aaron Painter
Aaron.Painter@inovitdemos.ch
Member
Adam Barr
Adam.Barr@inovitdemos.ch
Member
AIP RMS Cluster Service Account
svcrmscluster@inovitdemos.ch
Member

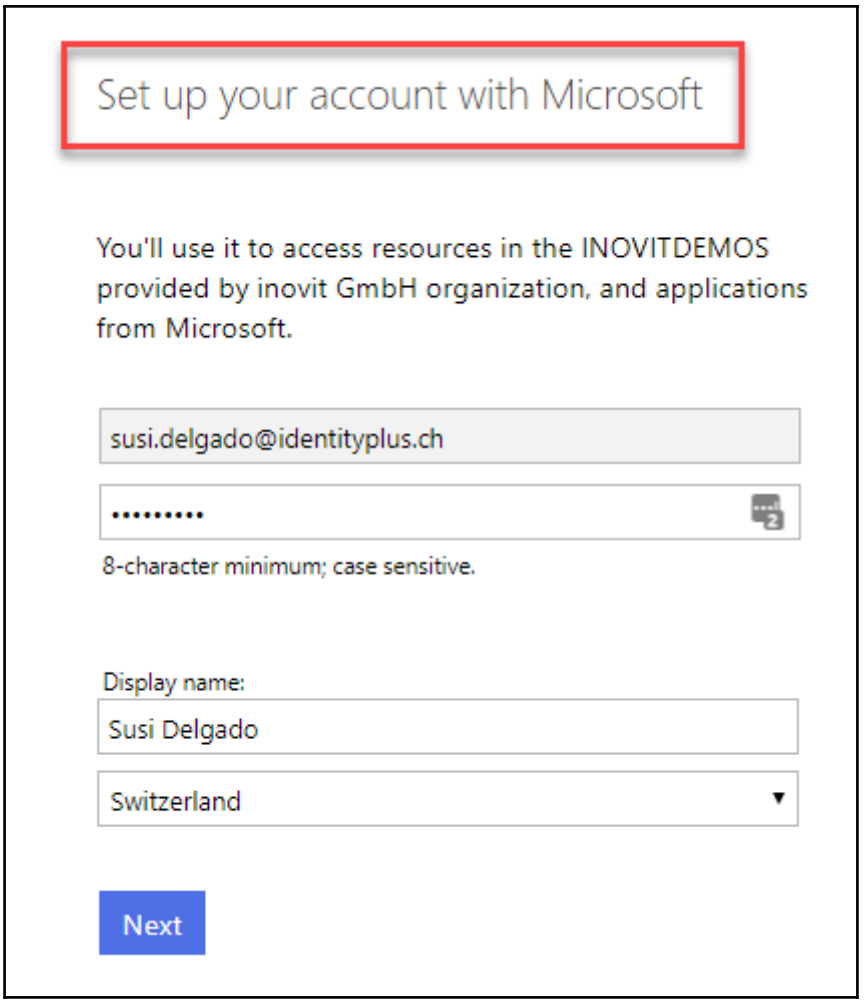

Azure Active Directory
You've been invited to access applications in the
INOVITDEMOS provided by inovit GmbH organization
by
TA
Tenant Administrator (Breaking Glass)
Welcome to the team!
Get Started
Return to the above link at any time for access.
This email has been sent on behalf of Tenant Administrator (Breaking Glass) (admin@181031inovitdemos.onmicrosoft.com) at INOVITDEMOS provided by inovit GmbH. Please act on this email only if you trust the INOVITDEMOS provided by inovit GmbH organization. This email may have advertising content. You can unsubscribe from future invitations from the INOVITDEMOS provided by inovit GmbH organization at any time. See Microsoft organization privacy statement to learn more about how Microsoft handles your data.
Facilitated by : Microsoft Corporation, One Microsoft Way, Redmond, WA 98052
Microsoft

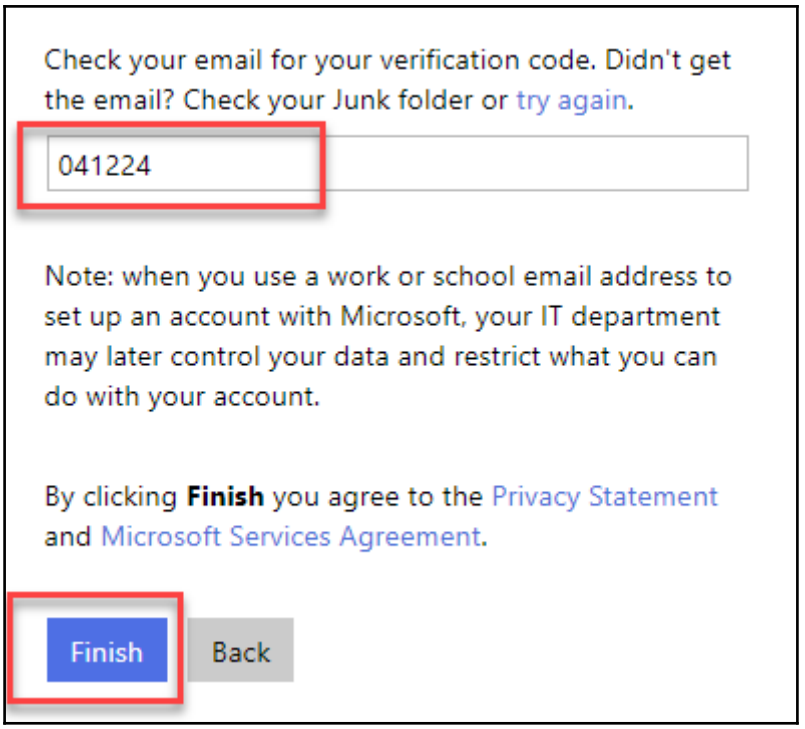

Microsoft
maria.lee@inovit.ch
Review permissions
I INOVITDEMOS provided by inovit GmbH
The organization INOVITDEMOS provided by inovit GmbH would like to:
Sign you in
Read your name, email, and perhaps photo
You should only accept if you trust INOVITDEMOS provided by inovit GmbH. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. INOVITDEMOS provided by inovit GmbH has not provided a link to their privacy statement for you to review. INOVITDEMOS provided by inovit GmbH may log information about your access. You can remove these permissions at https://myapps.microsoft.com/181031inovitdemos.onmicrosoft.com.
Cancel
Accept

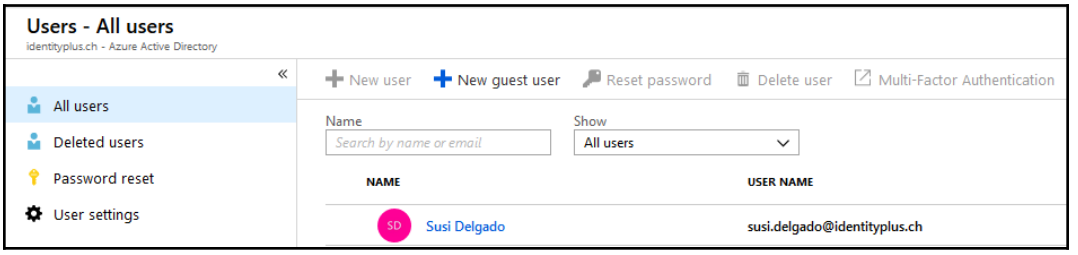

Microsoft
Maria Lee
INOVITDEMOS PROVIDED BY INOVIT GMBH
Apps
Search apps
There are no applications available. Please contact your admin for more information.
Groups
Access reviews

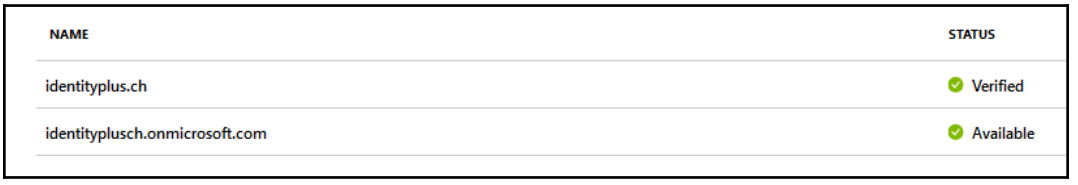

https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1548152705&rver=6.7.6636.0&wp=MBI_SSL&wreply=https%3a%2f%2finvitations.microsoft.com%2fms
Management
Social Media
Learning Platforms
Streaming Platforms
Microsoft Partner
Microsoft Tech Comm
Packt Content Develo
DEV TITUS Adminis
Microsoft
jochen.nickel@gmail.com
Enter password
Password
Keep me signed in
Forgot my password
Sign in with a different Microsoft account
Sign in

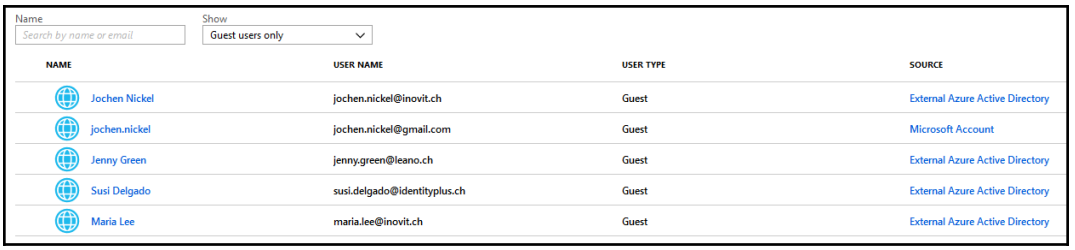

Select
Threads
Messages 1 to 1 of 1
1
You're invited to the INOVITDEMOS provided by inovit GmbH organization
From Tenant Administrator (Breaking Glass) from INOVITDEMOS provided by inovit GmbH (via Microsoft)
Date Today 10:55
Azure Active Directory
You've been invited to access applications in the INOVITDEMOS provided by inovit GmbH organization by
TA
Tenant Administrator (Breaking Glass)
Welcome to the team!
Get Started

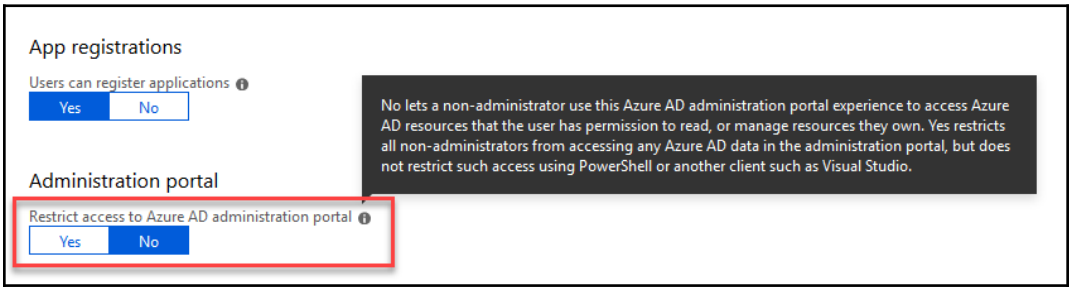

Set up your account with Microsoft
You'll use it to access resources in the INOVITDEMOS provided by inovit GmbH organization, and applications from Microsoft.
susi.delgado@identityplus.ch
8-character minimum; case sensitive.
Display name:
Susi Delgado
Switzerland
Next

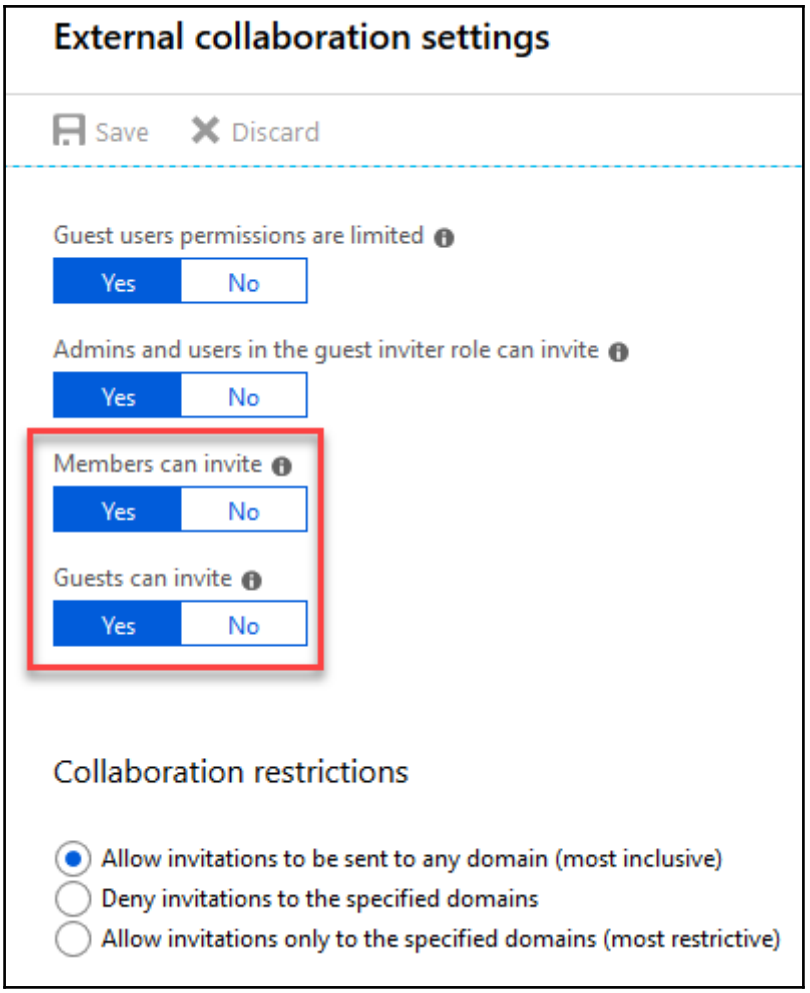

Check your email for your verification code. Didn't get the email? Check your Junk folder or try again.
041224
Note: when you use a work or school email address to set up an account with Microsoft, your IT department may later control your data and restrict what you can do with your account.
By clicking Finish you agree to the Privacy Statement and Microsoft Services Agreement.
Finish
Back

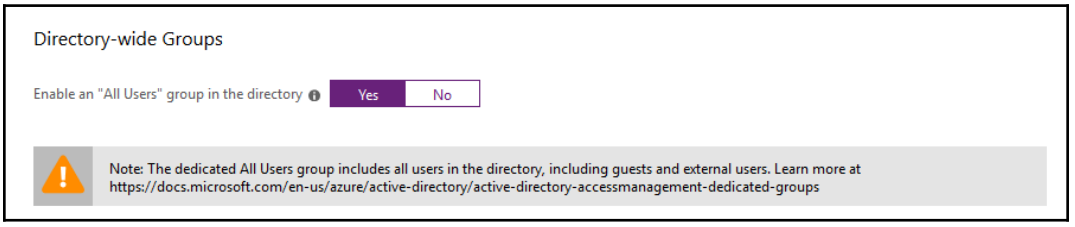

Users - All users
identityplus.ch - Azure Active Directory
All users
Deleted users
Password reset
User settings
New user
New guest user
Reset password
Delete user
Multi-Factor Authentication
Name
Search by name or email
Show
All users
NAME
USER NAME
SD
Susi Delgado
susi.delgado@identityplus.ch

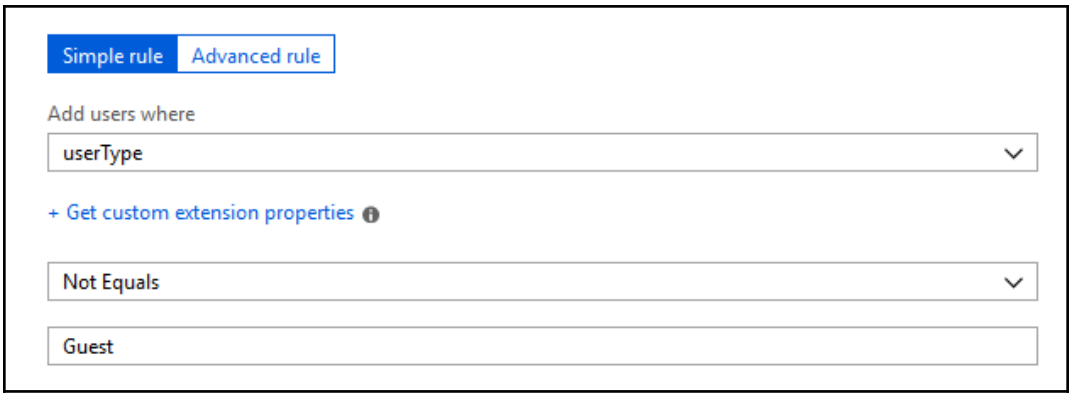

NAME
STATUS
identityplus.ch
Verified
identityplusch.onmicrosoft.com
Available

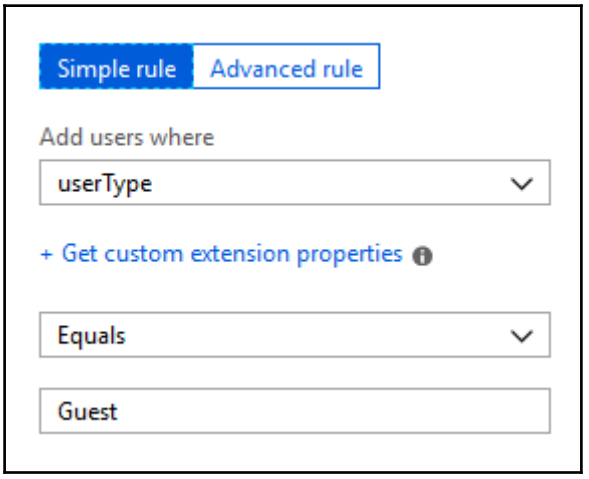

Name
Search by name or email
Show
Guest users only
NAME
USER NAME
USER TYPE
SOURCE
Jochen Nickel
jochen.nickel@inovit.ch
Guest
External Azure Active Directory
jochen.nickel
jochen.nickel@gmail.com
Guest
Microsoft Account
Jenny Green
jenny.green@leano.ch
Guest
External Azure Active Directory
Susi Delgado
susi.delgado@identityplus.ch
Guest
External Azure Active Directory
Maria Lee
maria.lee@inovit.ch
Guest
External Azure Active Directory

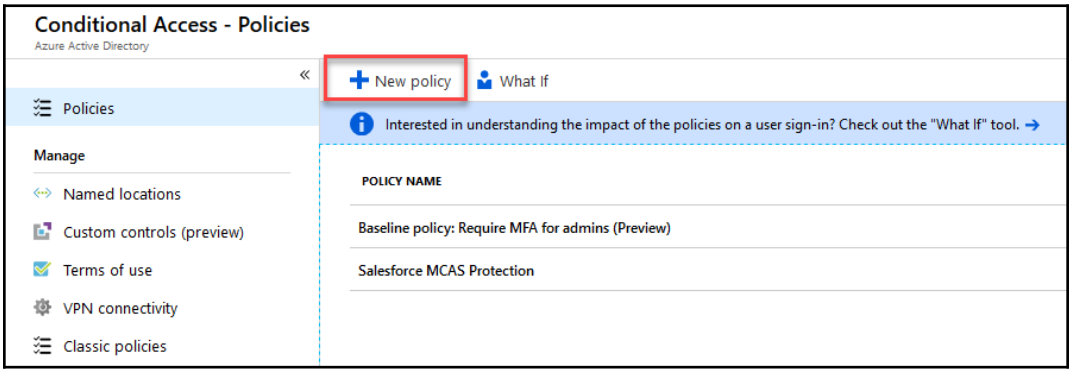

App registrations
Users can register applications
Yes
No
No lets a non-administrator use this Azure AD administration portal experience to access Azure AD resources that the user has permission to read, or manage resources they own. Yes restricts all non-administrators from accessing any Azure AD data in the administration portal, but does not restrict such access using PowerShell or another client such as Visual Studio.
Administration portal
Restrict access to Azure AD administration portal
Yes
No

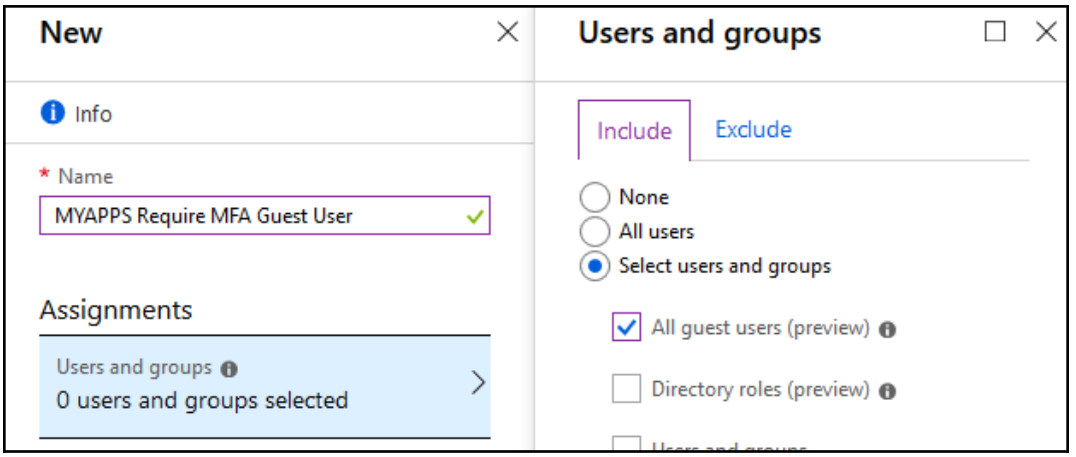

External collaboration settings
Save
Discard
Guest users permissions are limited
Yes
No
Admins and users in the guest inviter role can invite
Yes
No
Members can invite
Yes
No
Guests can invite
Yes
No
Collaboration restrictions
Allow invitations to be sent to any domain (most inclusive)
Deny invitations to the specified domains
Allow invitations only to the specified domains (most restrictive)

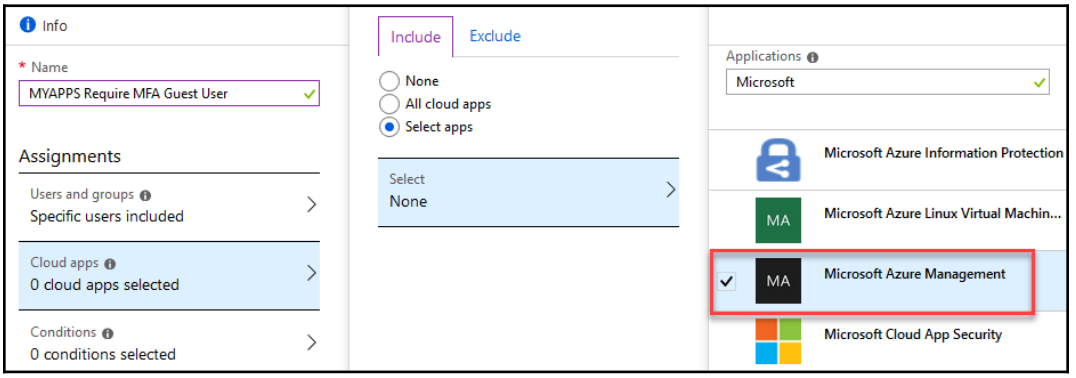

Directory-wide Groups
Enable an "All Users" group in the directory
Yes
No
Note: The dedicated All Users group includes all users in the directory, including guests and external users. Learn more at
https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-dedicated-groups

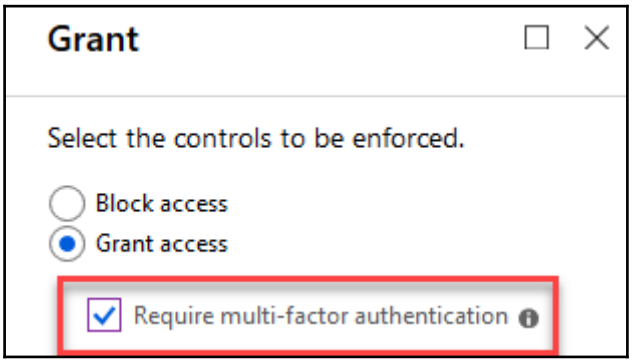

Simple rule
Advanced rule
Add users where
userType
+ Get custom extension properties
Not Equals
Guest

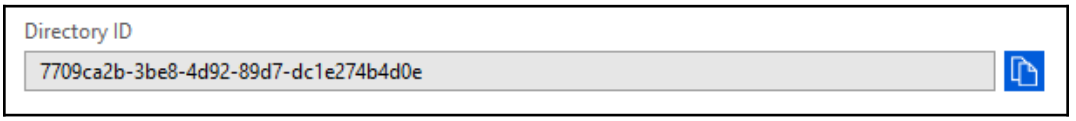

Simple rule
Advanced rule
Add users where
userType
+ Get custom extension properties
Equals
Guest

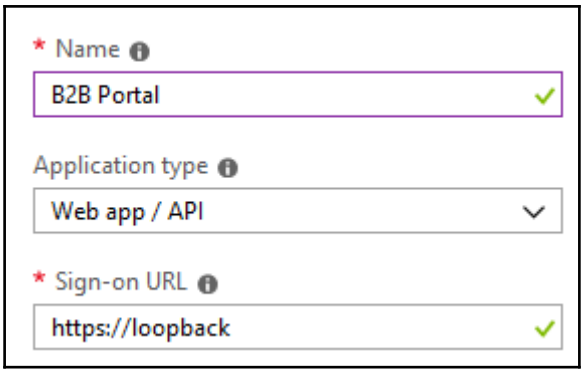

Conditional Access - Policies
Azure Active Directory
New policy
What If
Policies
Interested in understanding the impact of the policies on a user sign-in? Check out the "What If" tool.
Manage
POLICY NAME
Named locations
Baseline policy: Require MFA for admins (Preview)
Custom controls (preview)
Terms of use
Salesforce MCAS Protection
VPN connectivity
Classic policies

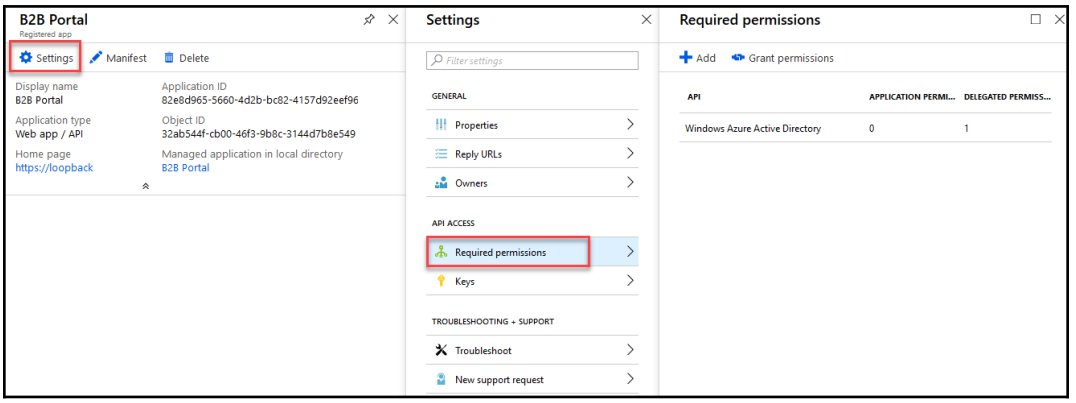

New
Info
* Name
MYAPPS Require MFA Guest User
Assignments
Users and groups
0 users and groups selected
Users and groups
Include
Exclude
None
All users
Select users and groups
All guest users (preview)
Directory roles (preview)

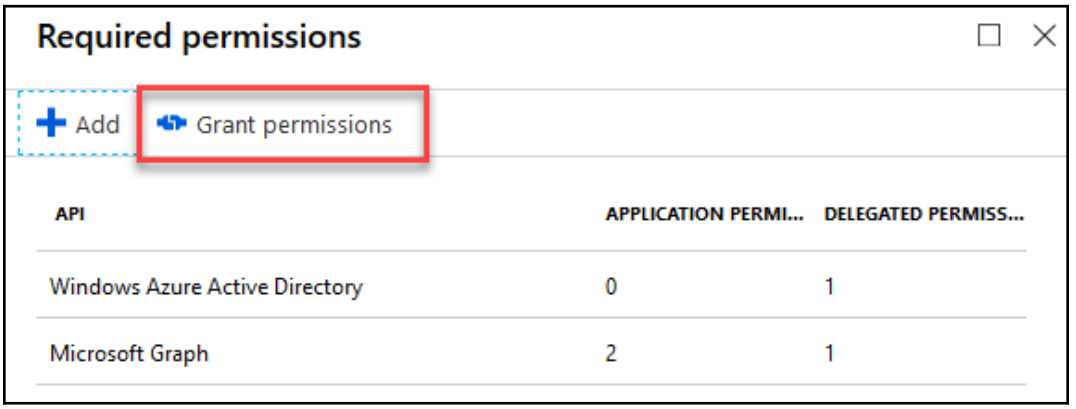

Info
* Name
MYAPPS Require MFA Guest User
Assignments
Users and groups
Specific users included
Cloud apps
0 cloud apps selected
Conditions
0 conditions selected
Include
Exclude
None
All cloud apps
Select apps
Select
None
Applications
Microsoft
Microsoft Azure Information Protection
Microsoft Azure Linux Virtual Machin...
Microsoft Azure Management
Microsoft Cloud App Security

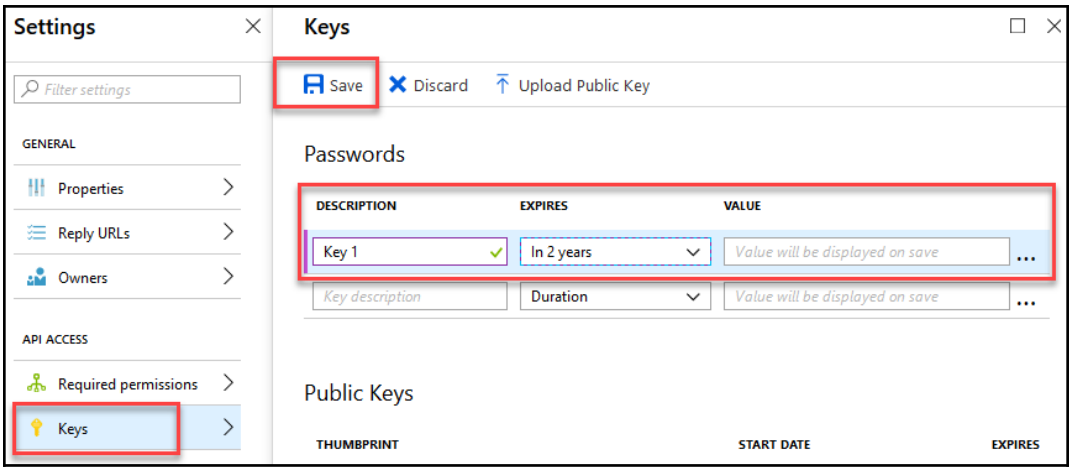

Grant
Select the controls to be enforced.
Block access
Grant access
Require multi-factor authentication

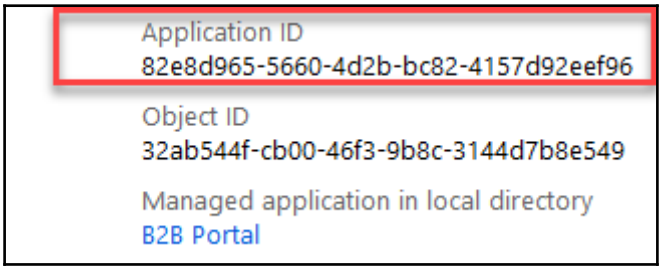

Directory ID
7709ca2b-3be8-4d92-89d7-dc1e274b4d0e

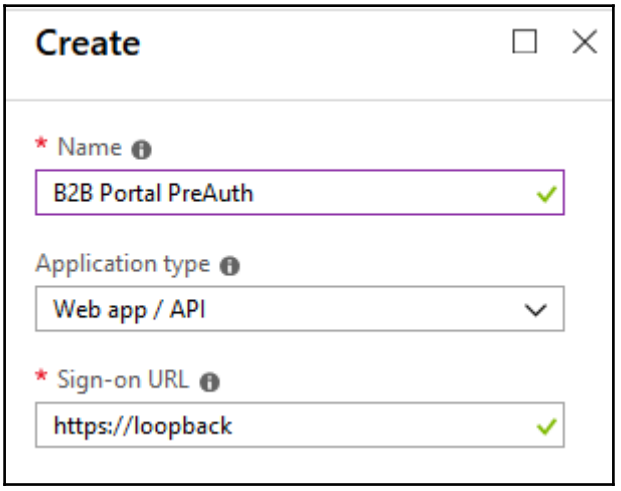

* Name
B2B Portal
Application type
Web app / API
* Sign-on URL
https://loopback

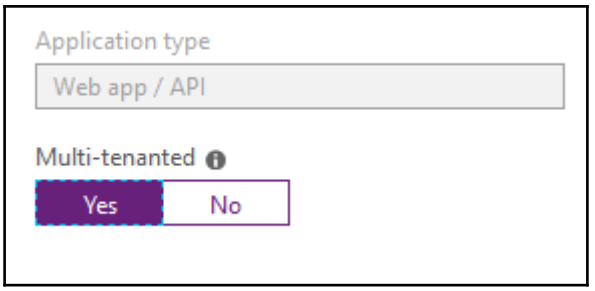

B2B Portal
Registered app
Settings
Manifest
Delete
Display name
B2B Portal
Application ID
82e8d965-5660-4d2b-bc82-4157d92eef96
Application type
Web app / API
Object ID
32ab544f-cb00-46f3-9b8c-3144d7b8e549
Home page
https://loopback
Managed application in local directory
B2B Portal
Settings
Filter settings
GENERAL
Properties
Reply URLs
Owners
API ACCESS
Required permissions
Keys
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request
Required permissions
Add
Grant permissions
API
APPLICATION PERMI...
DELEGATED PERMISS...
Windows Azure Active Directory
0
1

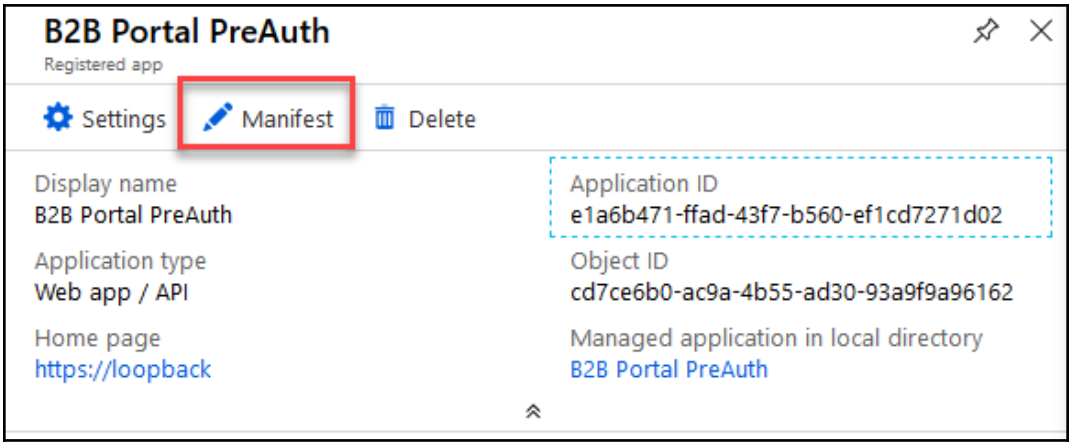

Required permissions
Add
Grant permissions
API
APPLICATION PERMI...
DELEGATED PERMISS...
Windows Azure Active Directory
0
1
Microsoft Graph
2
1

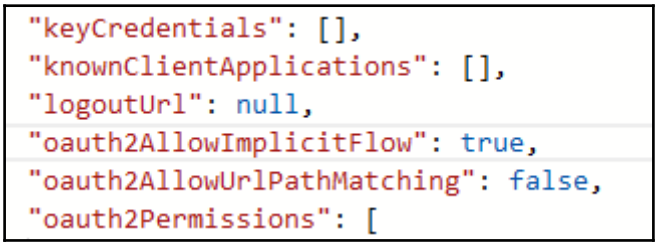

Settings
Filter settings
GENERAL
Properties
Reply URLs
Owners
API ACCESS
Required permissions
Keys
Keys
Save
Discard
Upload Public Key
Passwords
DESCRIPTION
EXPIRES
VALUE
Key 1
In 2 years
Value will be displayed on save
Key description
Duration
Value will be displayed on save
Public Keys
THUMBPRINT
START DATE
EXPIRES

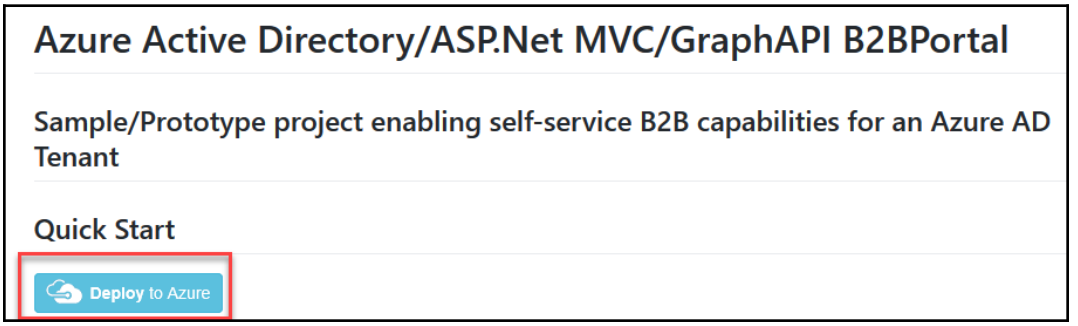

Application ID
82e8d965-5660-4d2b-bc82-4157d92eef96
Object ID
32ab544f-cb00-46f3-9b8c-3144d7b8e549
Managed application in local directory
B2B Portal

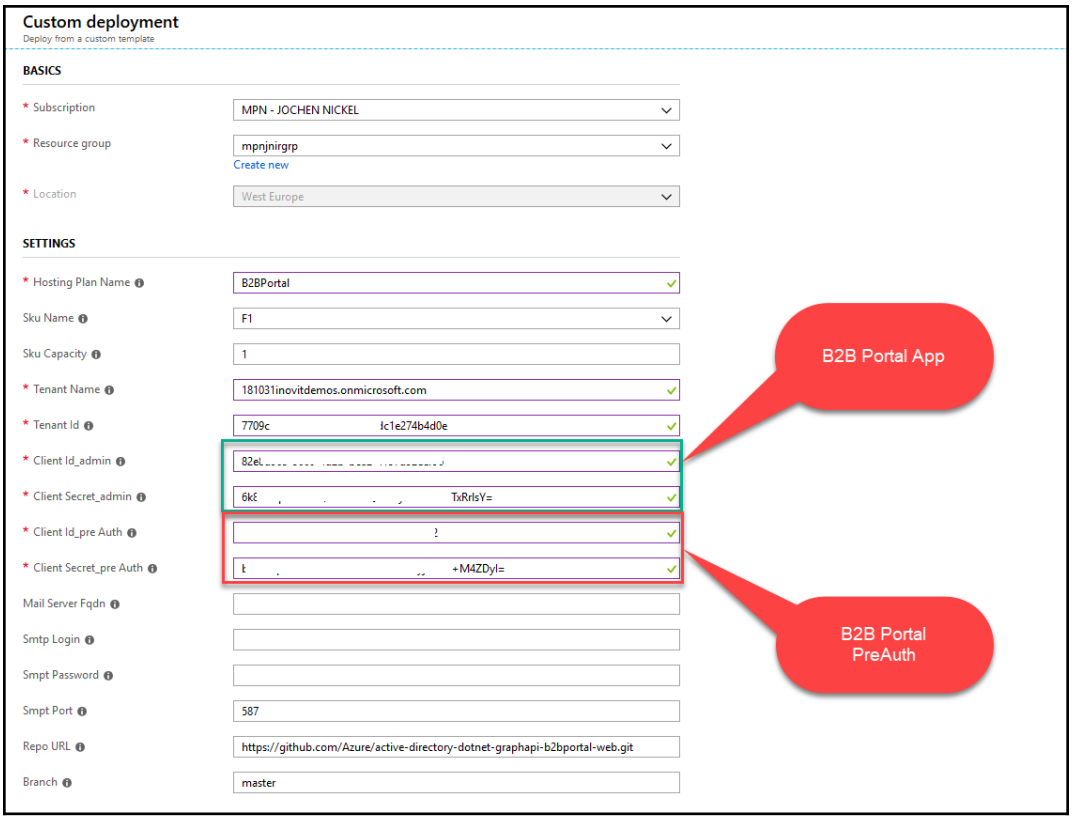

Create
* Name
B2B Portal PreAuth
Application type
Web app / API
* Sign-on URL
https://loopback

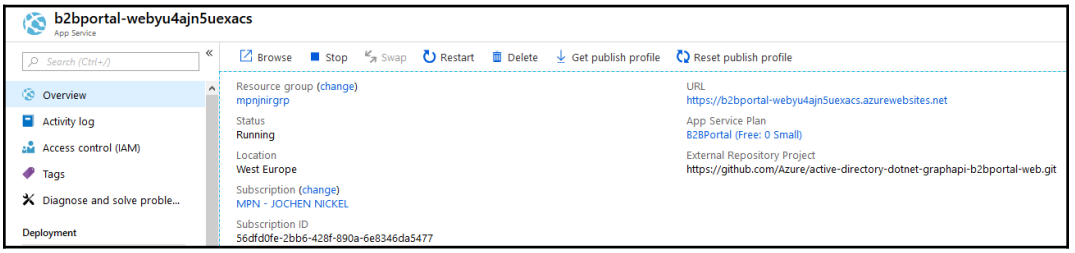

Application type
Web app / API
Multi-tenanted
Yes
No

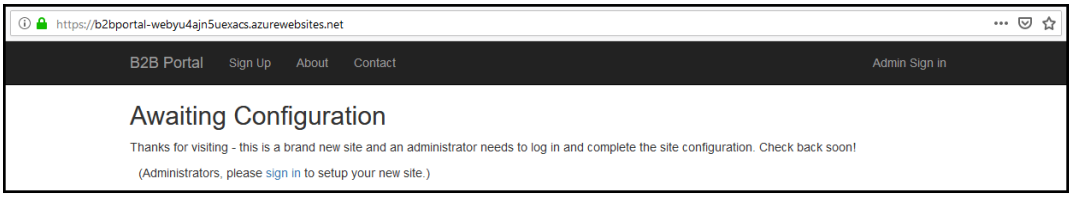

B2B Portal PreAuth
Registered app
Settings
Manifest
Delete
Display name
B2B Portal PreAuth
Application type
Web app / API
Home page
https://loopback
Application ID
e1a6b471-ffad-43f7-b560-ef1cd7271d02
Object ID
cd7ce6b0-ac9a-4b55-ad30-93a9f9a96162
Managed application in local directory
B2B Portal PreAuth

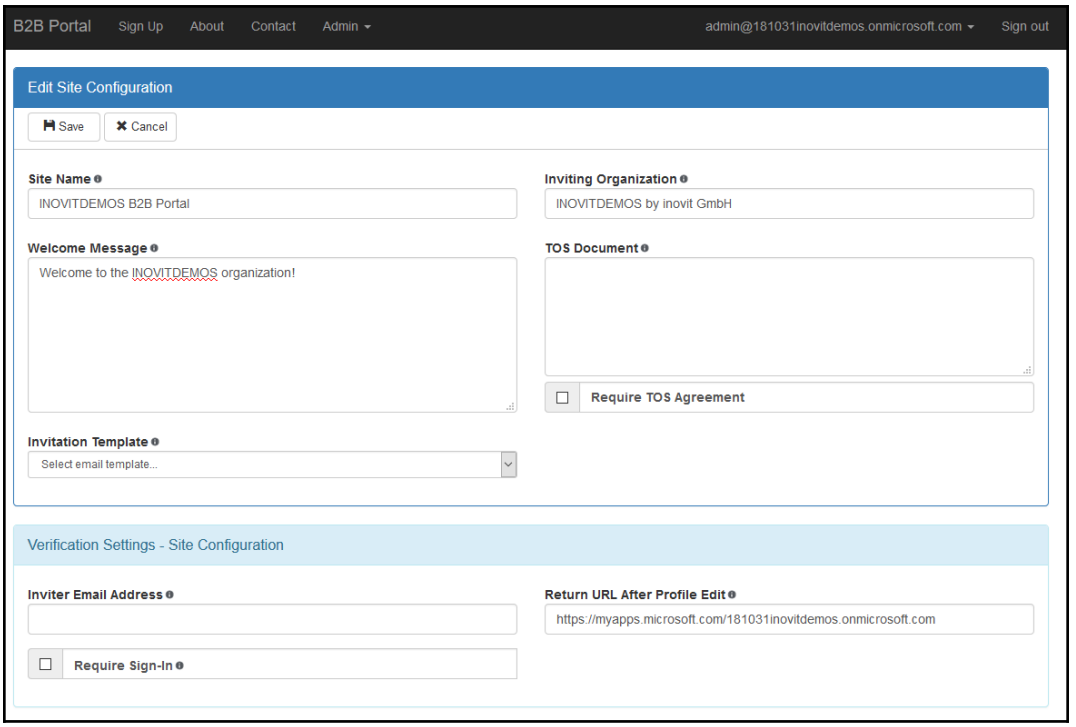

"keyCredentials": [],
"knownClientApplications": [],
"logoutUrl": null,
"oauth2AllowImplicitFlow": true,
"oauth2AllowUrlPathMatching": false,
"oauth2Permissions": [

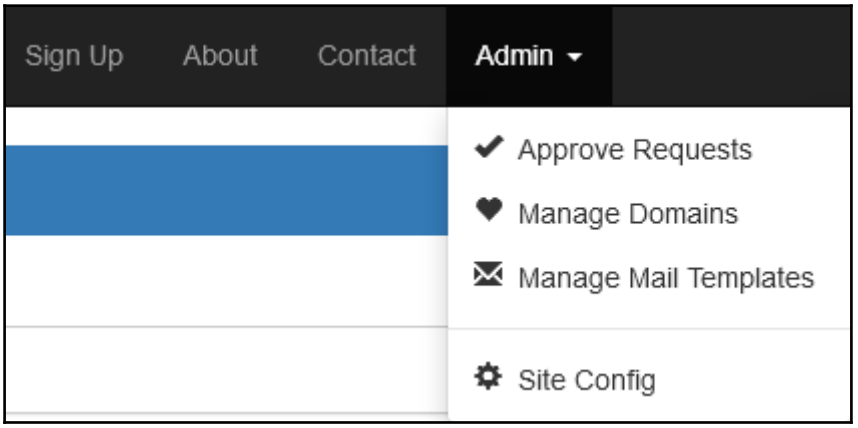

Azure Active Directory/ASP.Net MVC/GraphAPI B2BPortal
Sample/Prototype project enabling self-service B2B capabilities for an Azure AD Tenant
Quick Start
Deploy to Azure

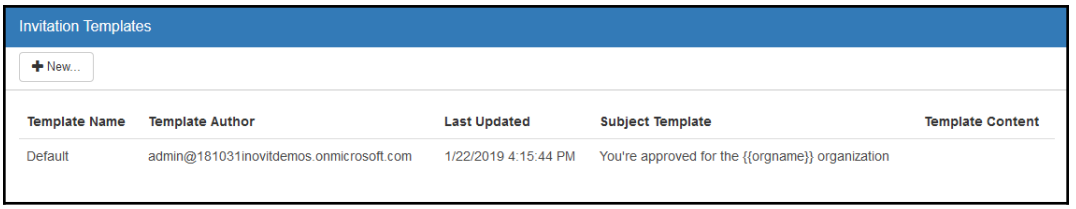

Custom deployment
Deploy from a custom template
BASICS
* Subscription
MPN - JOCHEN NICKEL
* Resource group
mpnjnirgrp
Create new
* Location
West Europe
SETTINGS
* Hosting Plan Name
B2BPortal
Sku Name
F1
Sku Capacity
1
* Tenant Name
181031inovitdemos.onmicrosoft.com
* Tenant Id
7709c
fc1e274b4d0e
* Client Id_admin
* Client Secret_admin
TxRrlsY=
* Client Id_pre Auth
* Client Secret_pre Auth
+M4ZDyI=
Mail Server Fqdn
Smtp Login
Smpt Password
Smpt Port
587
Repo URL
https://github.com/Azure/active-directory-dotnet-graphapi-b2bportal-web.git
Branch
master
B2B Portal App
B2B Portal PreAuth

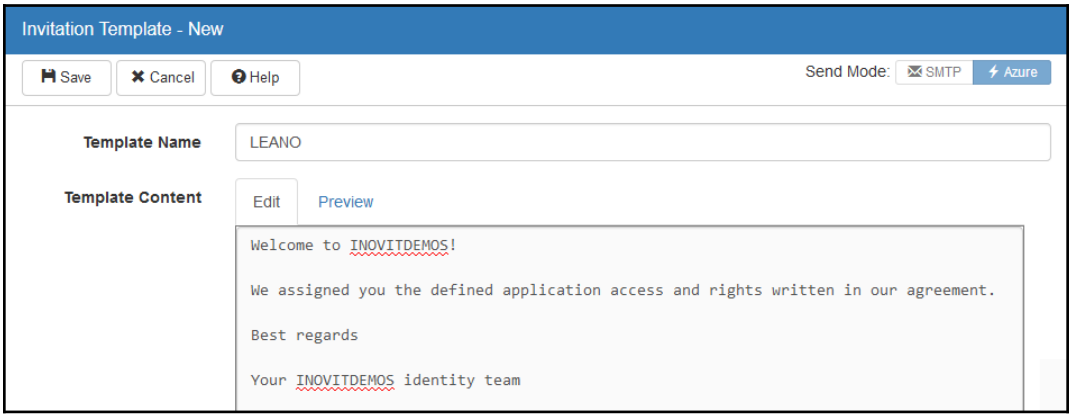

b2bportal-webyu4ajn5uexacs
App Service
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve proble...
Deployment
Browse
Stop
Swap
Restart
Delete
Get publish profile
Reset publish profile
Resource group (change)
mpnjnirgrp
Status
Running
Location
West Europe
Subscription (change)
MPN - JOCHEN NICKEL
Subscription ID
56dfd0fe-2bb6-428f-890a-6e8346da5477
URL
https://b2bportal-webyu4ajn5uexacs.azurewebsites.net
App Service Plan
B2BPortal (Free: 0 Small)
External Repository Project
https://github.com/Azure/active-directory-dotnet-graphapi-b2bportal-web.git

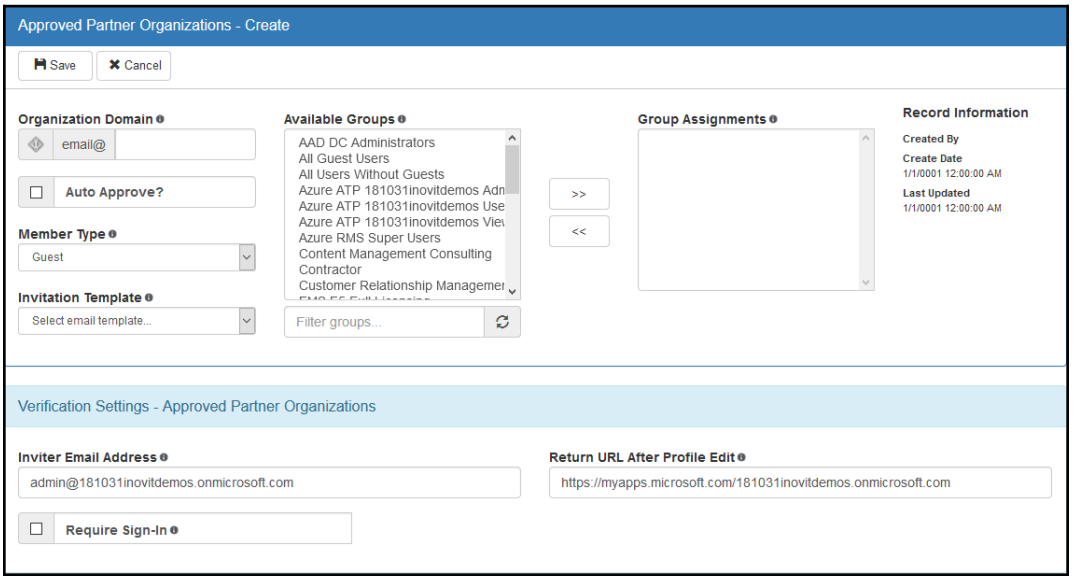

https://b2bportal-webyu4ajn5uexacs.azurewebsites.net
B2B Portal
Sign Up
About
Contact
Admin Sign in
Awaiting Configuration
Thanks for visiting - this is a brand new site and an administrator needs to log in and complete the site configuration. Check back soon!
(Administrators, please sign in to setup your new site.)

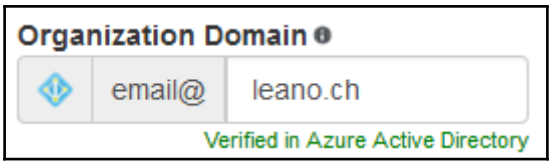

B2B Portal
Sign Up
About
Contact
Admin
admin@181031inovitdemos.onmicrosoft.com
Sign out
Edit Site Configuration
Save
Cancel
Site Name
INOVITDEMOS B2B Portal
Inviting Organization
INOVITDEMOS by inovit GmbH
Welcome Message
Welcome to the INOVITDEMOS organization!
TOS Document
Require TOS Agreement
Invitation Template
Select email template...
Verification Settings - Site Configuration
Inviter Email Address
Return URL After Profile Edit
https://myapps.microsoft.com/181031inovitdemos.onmicrosoft.com
Require Sign-In

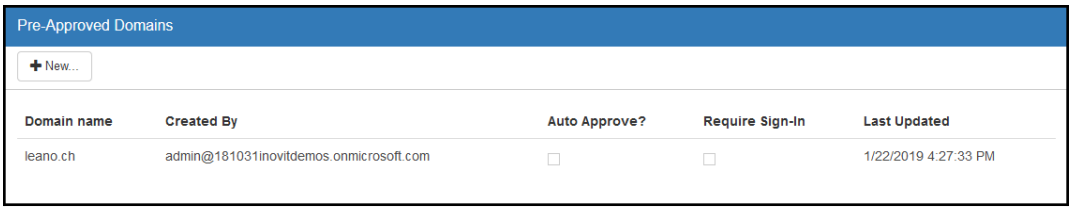

Sign Up
About
Contact
Admin
Approve Requests
Manage Domains
Manage Mail Templates
Site Config

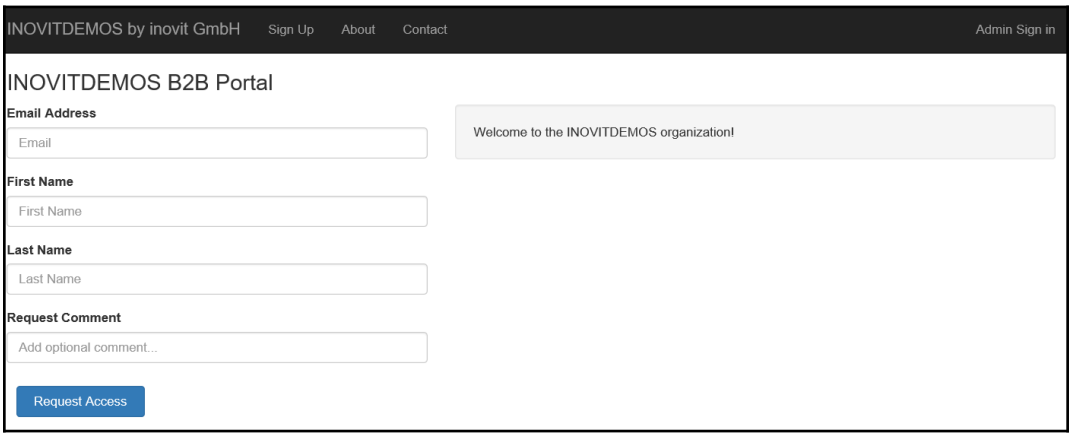

Invitation Templates
New...
Template Name
Template Author
Last Updated
Subject Template
Template Content
Default
admin@181031inovitdemos.onmicrosoft.com
1/22/2019 4:15:44 PM
You're approved for the {{orgname}} organization

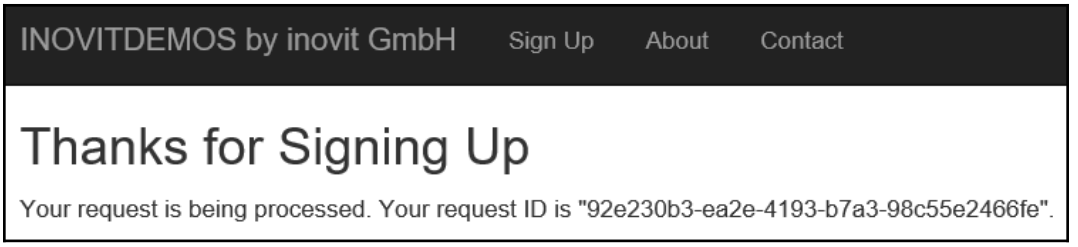

Invitation Template - New
Save
Cancel
Help
Send Mode:
SMTP
Azure
Template Name
LEANO
Template Content
Edit
Preview
Welcome to INOVITDEMOS!
We assigned you the defined application access and rights written in our agreement.
Best regards
Your INOVITDEMOS identity team

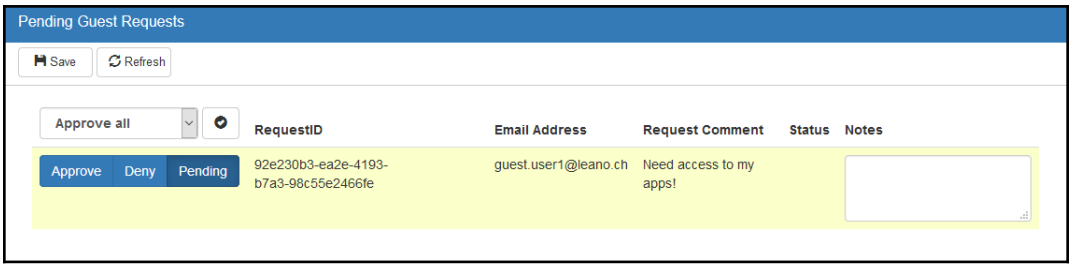

Approved Partner Organizations - Create
Save
Cancel
Organization Domain
email@
Auto Approve?
Member Type
Guest
Invitation Template
Select email template...
Available Groups
AAD DC Administrators
All Guest Users
All Users Without Guests
Azure ATP 181031inovitdemos Adn
Azure ATP 181031inovitdemos Use
Azure ATP 181031inovitdemos Vie
Azure RMS Super Users
Content Management Consulting
Contractor
Customer Relationship Manageme
Filter groups...
>>
<<
Group Assignments
Record Information
Created By
Create Date
1/1/0001 12:00:00 AM
Last Updated
1/1/0001 12:00:00 AM
Verification Settings - Approved Partner Organizations
Inviter Email Address
admin@181031inovitdemos.onmicrosoft.com
Return URL After Profile Edit
https://myapps.microsoft.com/181031inovitdemos.onmicrosoft.com
Require Sign-In

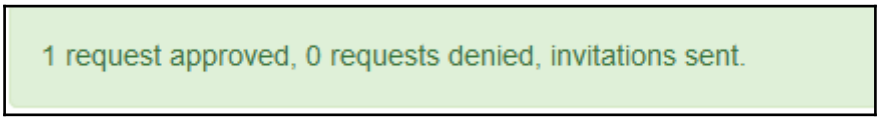

Organization Domain
email@
leano.ch
Verified in Azure Active Directory

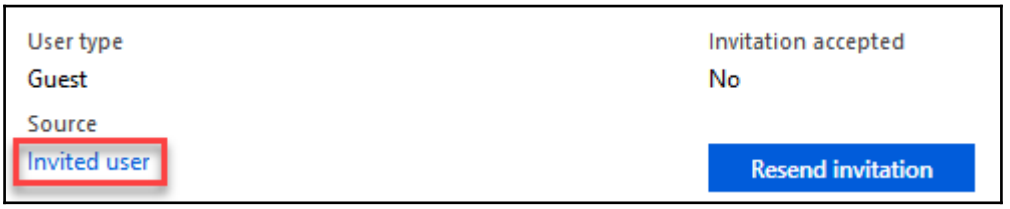

Pre-Approved Domains
New...
Domain name
Created By
Auto Approve?
Require Sign-In
Last Updated
leano.ch
admin@181031inovitdemos.onmicrosoft.com
1/22/2019 4:27:33 PM

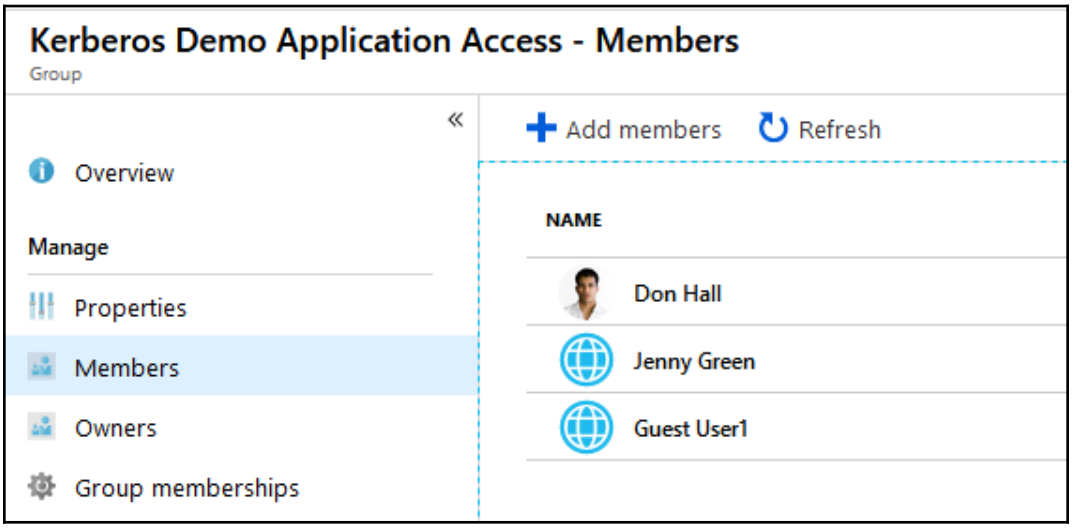

INOVITDEMOS by inovit GmbH
Sign Up
About
Contact
Admin Sign in
INOVITDEMOS B2B Portal
Email Address
Email
First Name
First Name
Last Name
Last Name
Request Comment
Add optional comment...
Request Access
Welcome to the INOVITDEMOS organization!

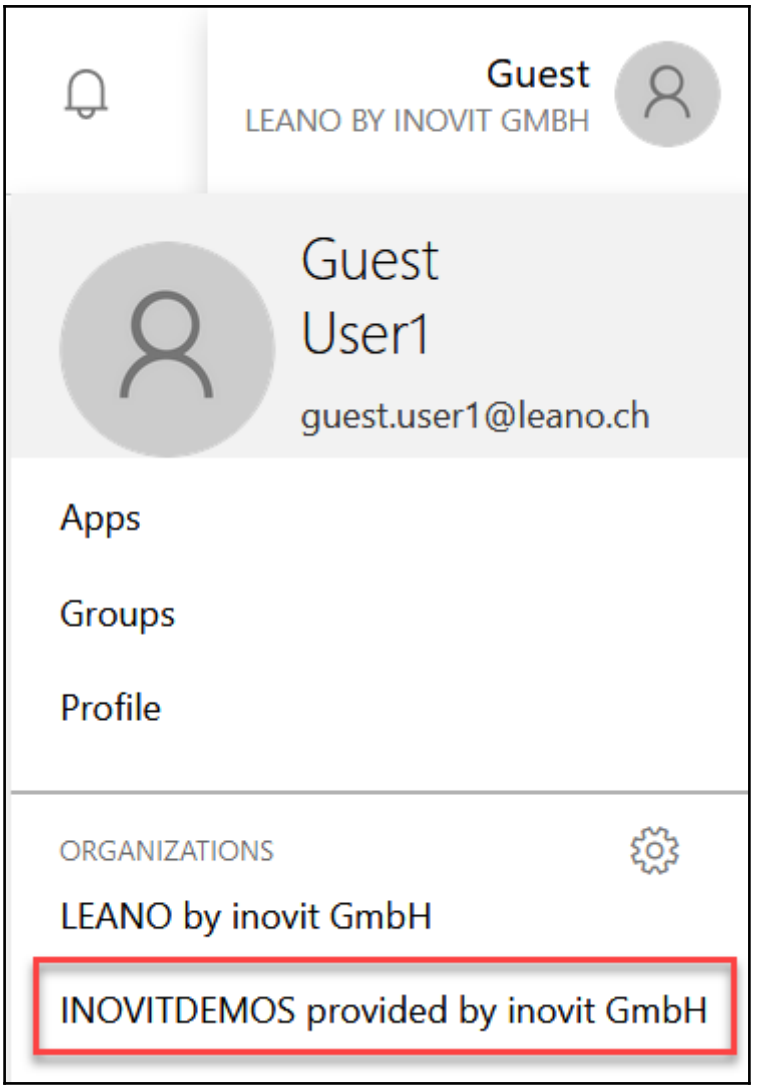

INOVITDEMOS by inovit GmbH
Sign Up
About
Contact
Thanks for Signing Up
Your request is being processed. Your request ID is "92e230b3-ea2e-4193-b7a3-98c55e2466fe".

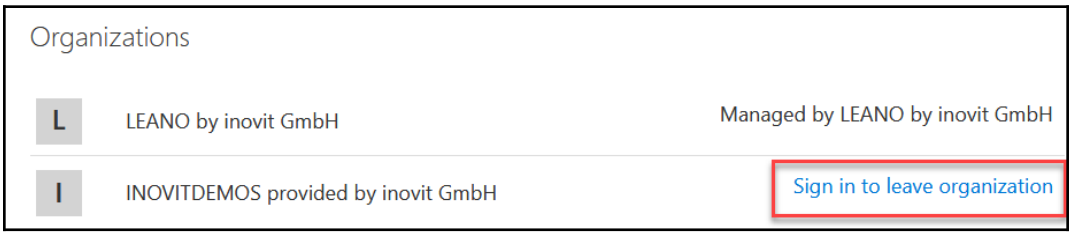

Pending Guest Requests
Save
Refresh
Approve all
RequestID
Email Address
Request Comment
Status
Notes
Approve
Deny
Pending
92e230b3-ea2e-4193-b7a3-98c55e2466fe
guest.user1@leano.ch
Need access to my apps!

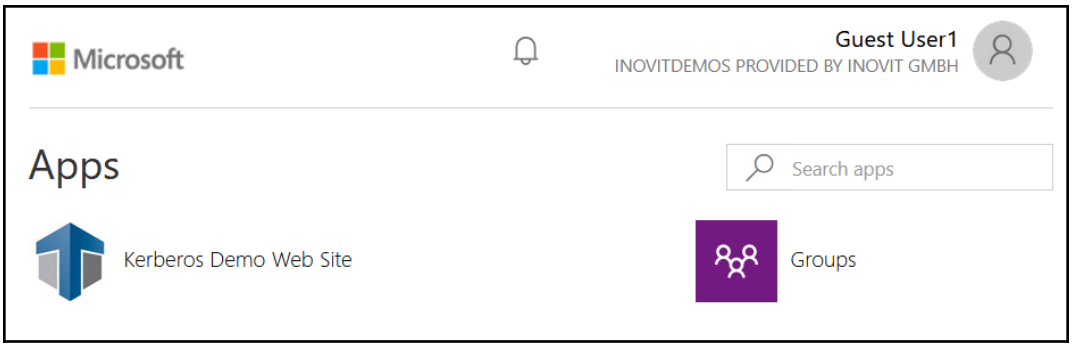

1 request approved, 0 requests denied, invitations sent.

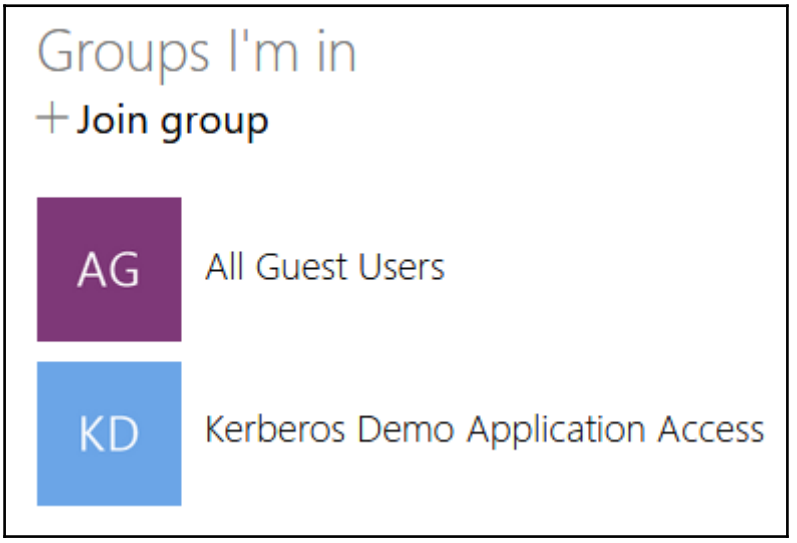

User type
Guest
Invitation accepted
No
Source
Invited user
Resend invitation

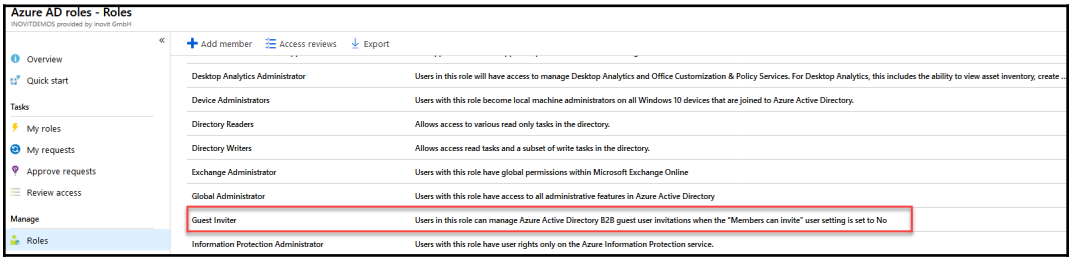

Kerberos Demo Application Access - Members
Group
Overview
Manage
Properties
Members
Owners
Group memberships
Add members
Refresh
NAME
Don Hall
Jenny Green
Guest User1

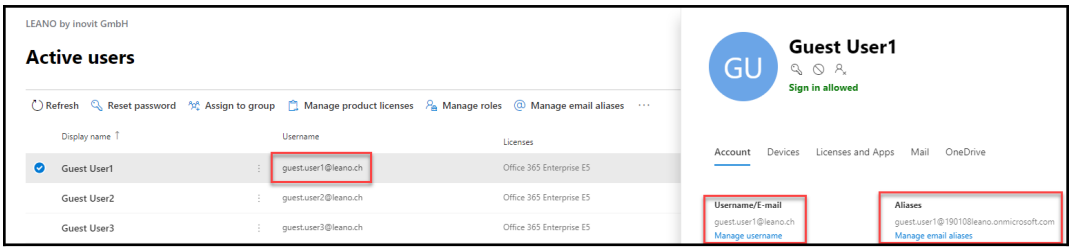

Guest
LEANO BY INOVIT GMBH
Guest
User1
guest.user1@leano.ch
Apps
Groups
Profile
ORGANIZATIONS
LEANO by inovit GmbH
INOVITDEMOS provided by inovit GmbH

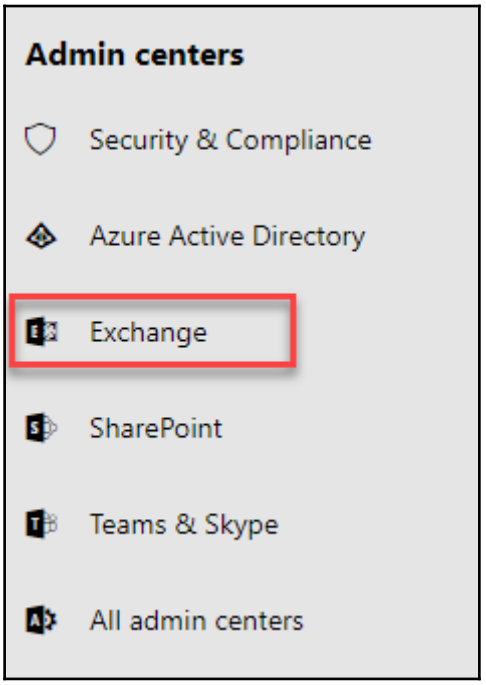

Organizations
L
LEANO by inovit GmbH
Managed by LEANO by inovit GmbH
I
INOVITDEMOS provided by inovit GmbH
Sign in to leave organization

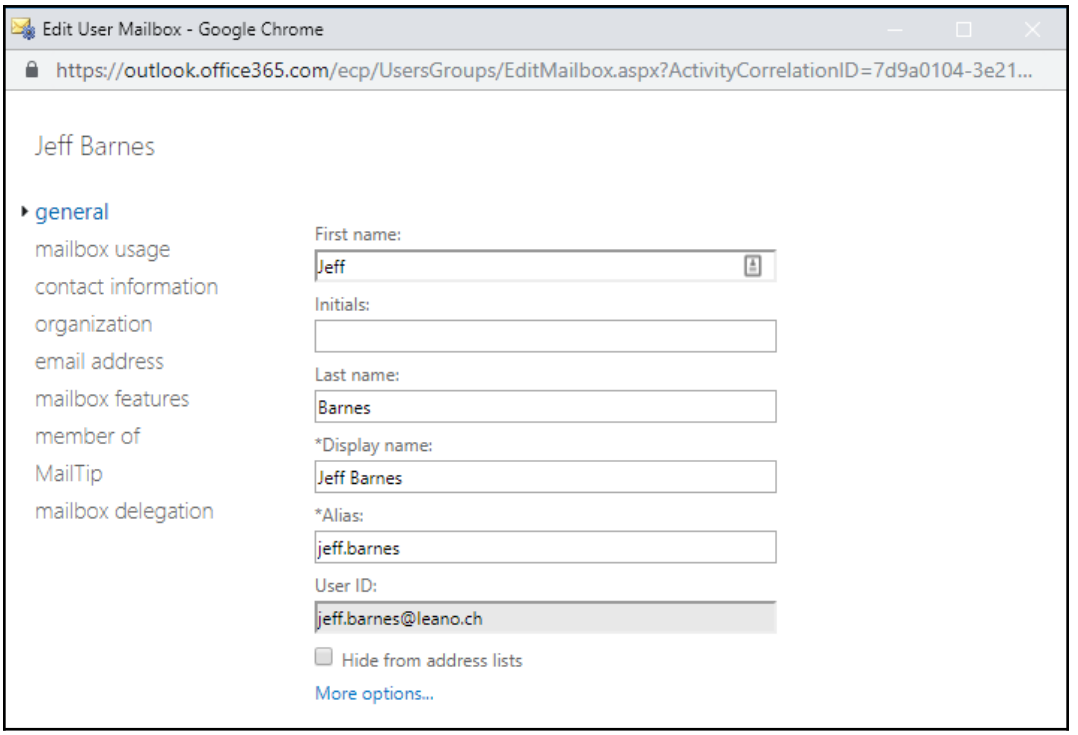

Microsoft
Guest User1
INOVITDEMOS PROVIDED BY INOVIT GMBH
Apps
Search apps
Kerberos Demo Web Site
Groups


Groups I'm in
+ Join group
AG
All Guest Users
KD
Kerberos Demo Application Access

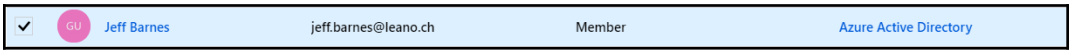

Azure AD roles - Roles
INOVITDEMOS provided by inovit GmbH
Add member
Access reviews
Export
Overview
Quick start
Tasks
My roles
My requests
Approve requests
Review access
Manage
Roles
Desktop Analytics Administrator
Users in this role will have access to manage Desktop Analytics and Office Customization & Policy Services. For Desktop Analytics, this includes the ability to view asset inventory, create
Device Administrators
Users with this role become local machine administrators on all Windows 10 devices that are joined to Azure Active Directory.
Directory Readers
Allows access to various read only tasks in the directory.
Directory Writers
Allows access read tasks and a subset of write tasks in the directory.
Exchange Administrator
Users with this role have global permissions within Microsoft Exchange Online
Global Administrator
Users with this role have access to all administrative features in Azure Active Directory
Guest Inviter
Users in this role can manage Azure Active Directory B2B guest user invitations when the "Members can invite" user setting is set to No
Information Protection Administrator
Users with this role have user rights only on the Azure Information Protection service.

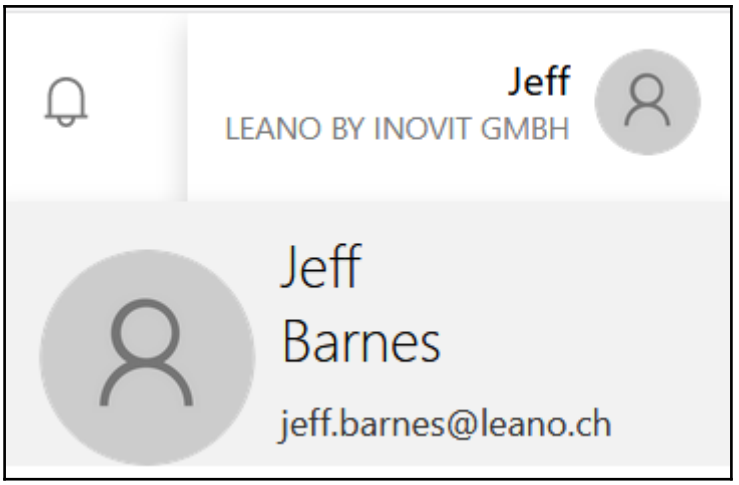

LEANO by inovit GmbH
Active users
Refresh
Reset password
Assign to group
Manage product licenses
Manage roles
Manage email aliases
Display name
Username
Licenses
Guest User1
guest.user1@leano.ch
Office 365 Enterprise E5
Guest User2
guest.user2@leano.ch
Office 365 Enterprise E5
Guest User3
guest.user3@leano.ch
Office 365 Enterprise E5
GU
Guest User1
Sign in allowed
Account
Devices
Licenses and Apps
Mail
OneDrive
Username/E-mail
guest.user1@leano.ch
Manage username
Aliases
guest.user1@190108leano.onmicrosoft.com
Manage email aliases

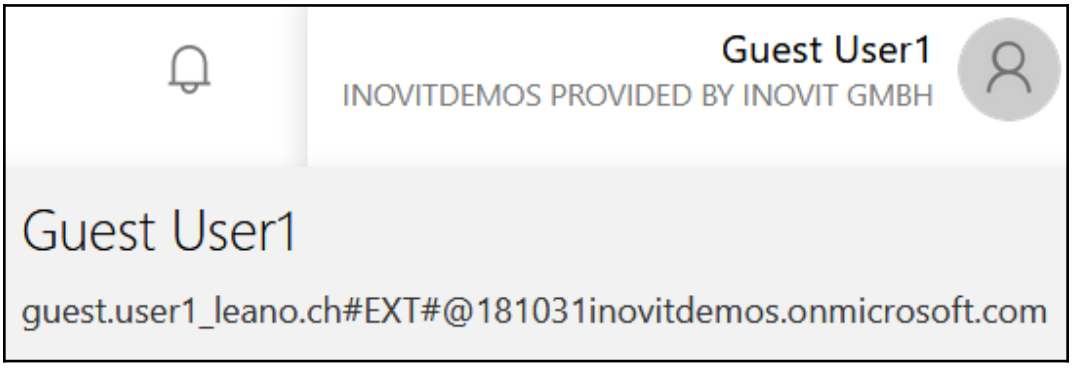

Admin centers
Security & Compliance
Azure Active Directory
Exchange
SharePoint
Teams & Skype
All admin centers


Edit User Mailbox - Google Chrome
https://outlook.office365.com/ecp/UsersGroups/EditMailbox.aspx?ActivityCorrelationID=7d9a0104-3e21...
Jeff Barnes
general
mailbox usage
contact information
organization
email address
mailbox features
member of
MailTip
mailbox delegation
First name:
Jeff
Initials:
Last name:
Barnes
*Display name:
Jeff Barnes
*Alias:
jeff.barnes
User ID:
jeff.barnes@leano.ch
Hide from address lists
More options...

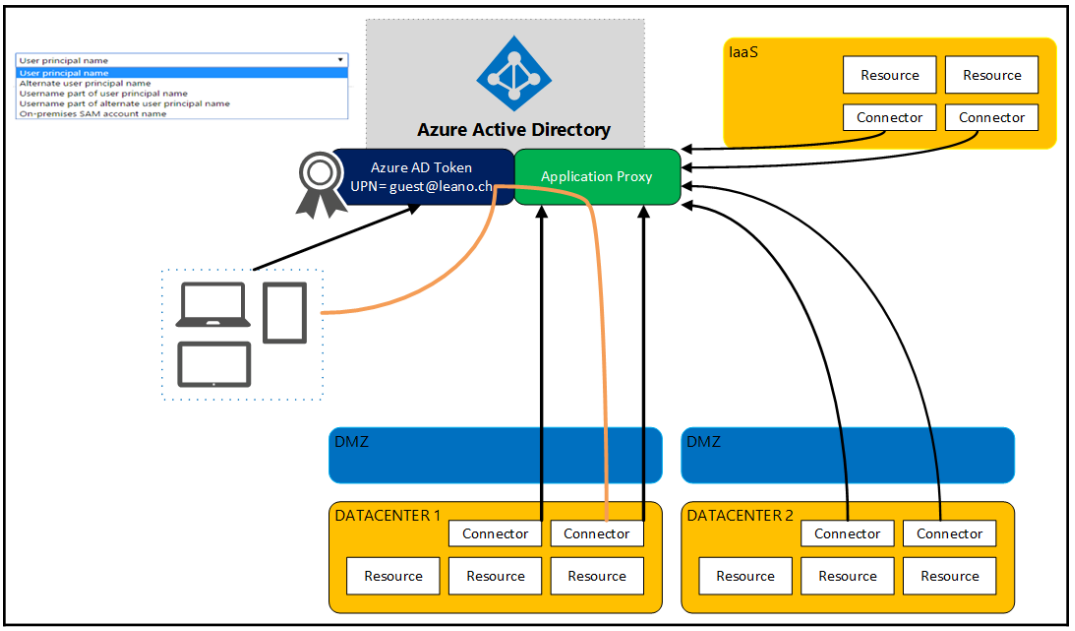

Email address:
TYPE
EMAIL ADDRESS
SIP
jeff.barnes@leano.ch
SMTP
jeff.barnes@leano.ch
SPO
SPO_e73550b7-e29e-44a1-89eb-c...


Jeff Barnes
jeff.barnes@leano.ch
Member
Azure Active Directory

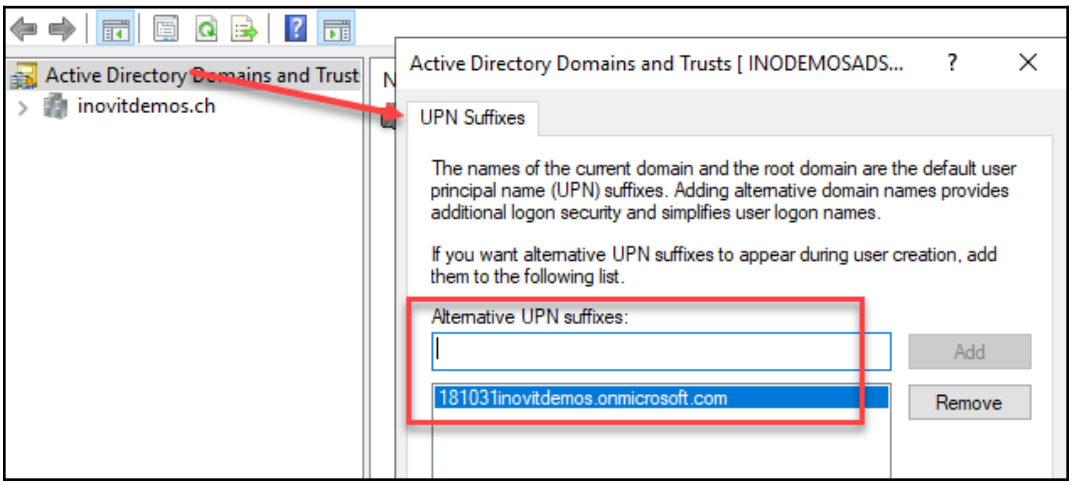

Jeff
LEANO BY INOVIT GMBH
Jeff
Barnes
jeff.barnes@leano.ch

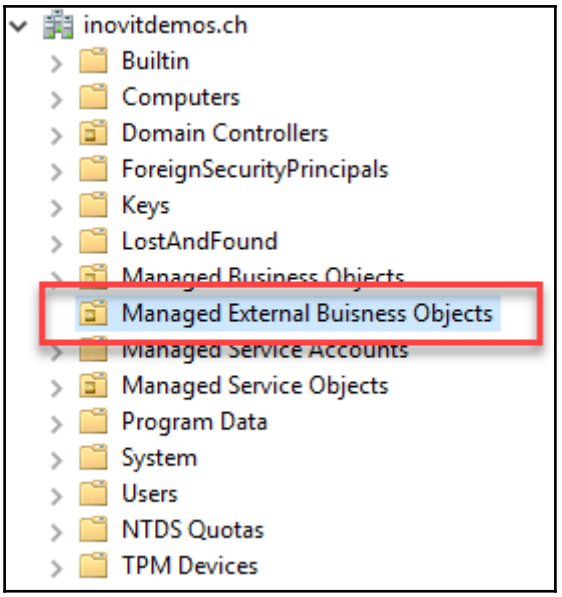

Guest User1
INOVITDEMOS PROVIDED BY INOVIT GMBH
Guest User1
guest.user1_leano.ch#EXT#@181031inovitdemos.onmicrosoft.com

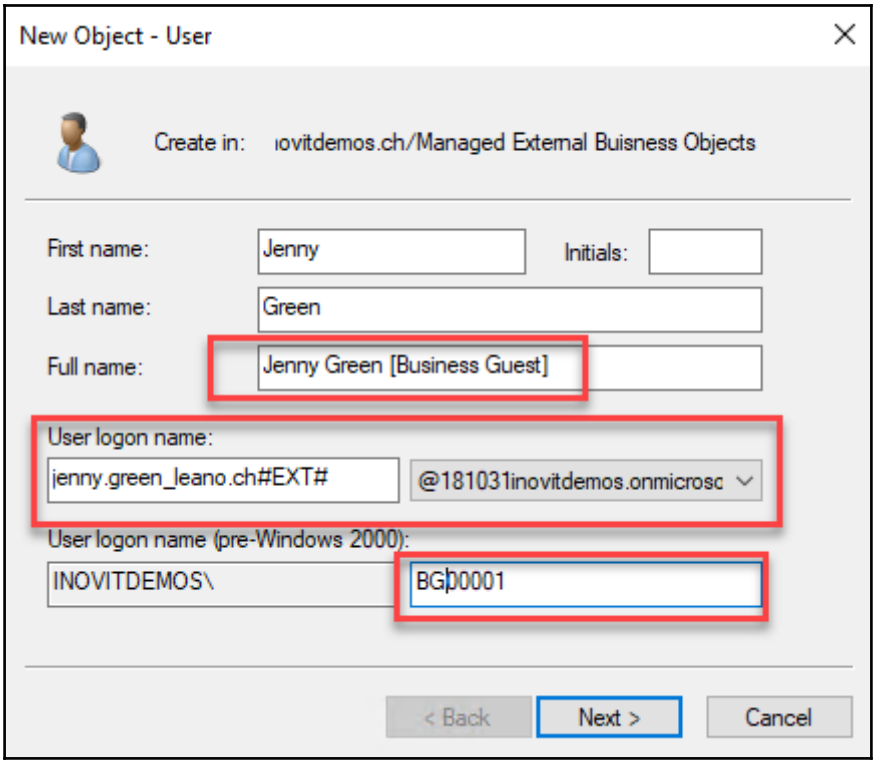

Identity
Name
Jeff Barnes
First name
Jeff
Last name
Barnes
User name
guest.user1@leano.ch
User type
Guest
Invitation accepted
Yes
Object ID
427314ed-5a15-4b66-b10b-312a458e7e25
Source
External Azure Active Directory



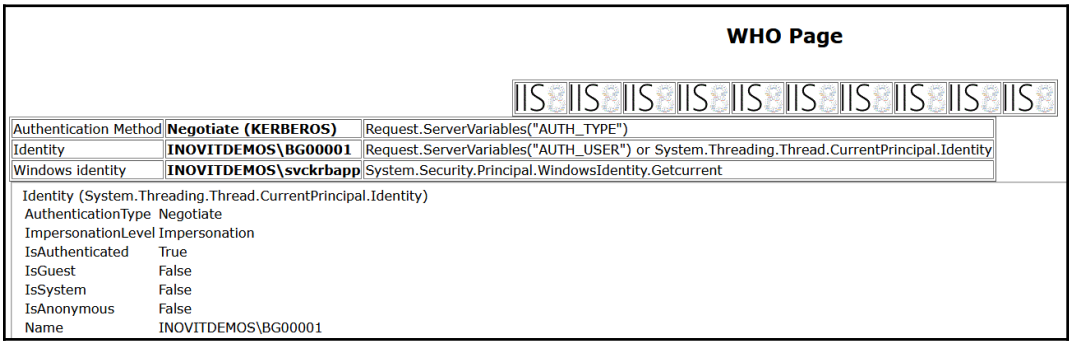

```
PS C:\Users\cloudadmin> Get-AzureADUser -Filter "UserType eq 'Guest'"

ObjectId                             DisplayName    UserPrincipalName
--------                             -----------    -----------------
07bf426f-4188-433d-99b9-d14d2f3e62c1 Jochen Nickel  jochen.nickel_inovit.ch#EXT#@181031inovitdemos.onmicrosoft.com
f0288126-8b6d-47b1-9984-acb48e66f851 jochen.nickel  jochen.nickel_gmail.com#EXT#@181031inovitdemos.onmicrosoft.com
7efba417-267c-478a-b038-8161bcb0f558 Jenny Green    jenny.green_leano.ch#EXT#@181031inovitdemos.onmicrosoft.com
b3664d12-adfa-4cc1-9f90-b23ddf968e08 Susi Delgado   susi.delgado_identityplus.ch#EXT#@181031inovitdemos.onmicrosoft.com
7448d477-0aa2-4677-bb2f-3e1cff6a6c3f Maria Lee      maria.lee_inovit.ch#EXT#@181031inovitdemos.onmicrosoft.com
427314ed-5a15-4b66-b10b-312a458e7e25 Guest User1    guest.user1_leano.ch#EXT#@181031inovitdemos.onmicrosoft.com
```

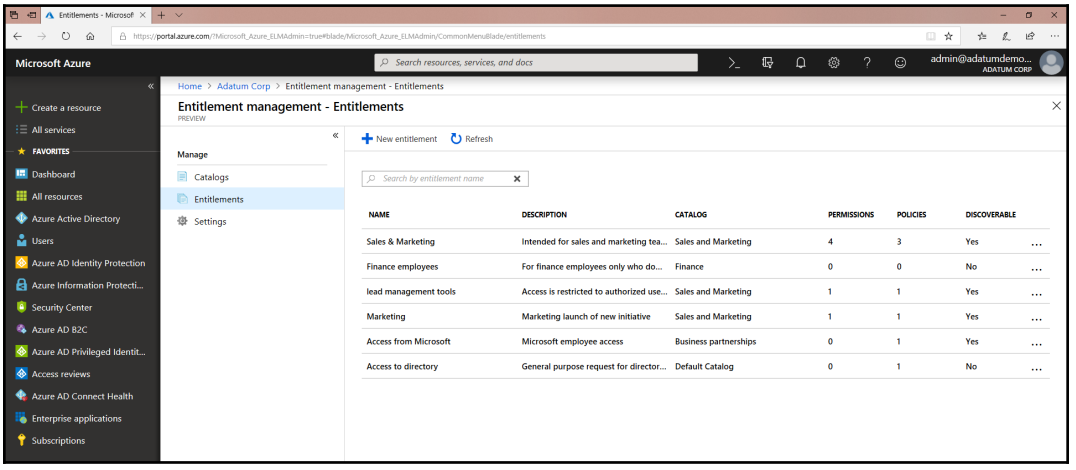


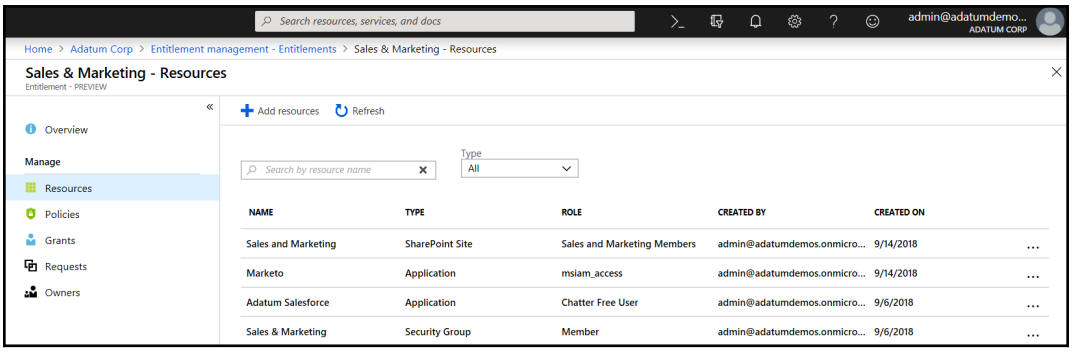

inovitdemos.ch
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Keys
LostAndFound
Managed Business Objects
Managed External Buisness Objects
Managed Service Accounts
Managed Service Objects
Program Data
System
Users
NTDS Quotas
TPM Devices

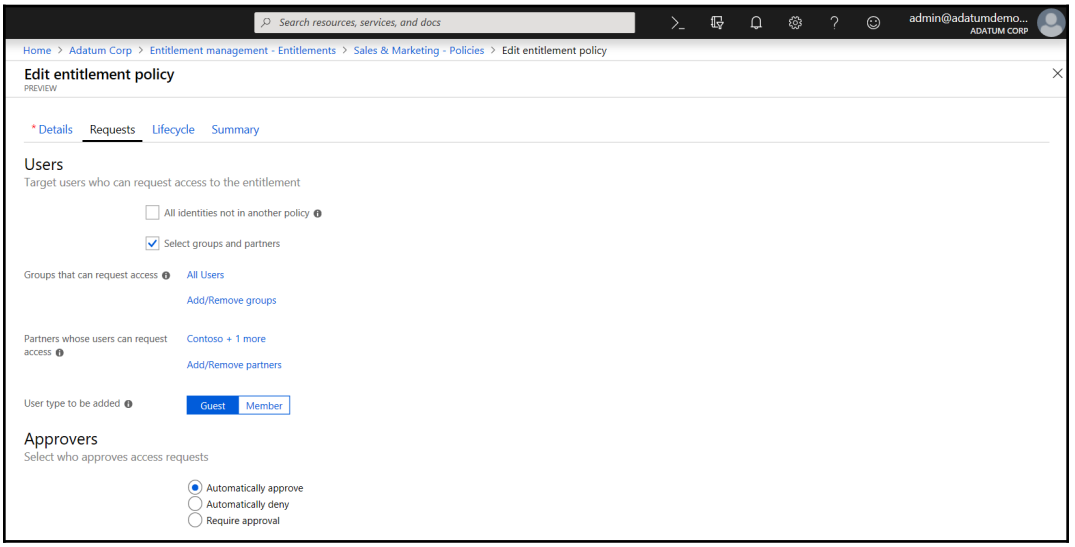

New Object - User
Create in: iovitdemos.ch/Managed External Buisness Objects
First name:
Jenny
Initials:
Last name:
Green
Full name:
Jenny Green [Business Guest]
User logon name:
jenny.green_leano.ch#EXT#
@181031inovitdemos.onmicrosc
User logon name (pre-Windows 2000):
INOVITDEMOS\
BG0001
< Back
Next >
Cancel


Kerberos Demo Application Access - Members
Group
Overview
Manage
Properties
Members
Owners
Add members
Refresh
NAME
TYPE
Don Hall
User
Guest User1
User

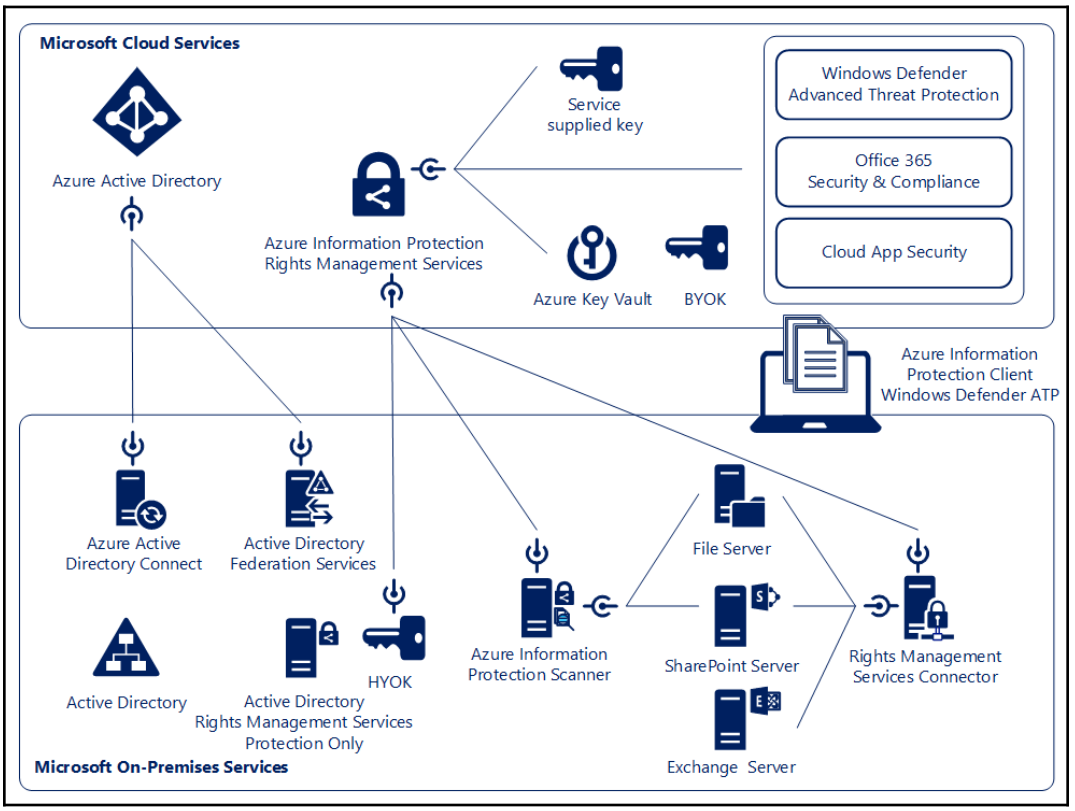

WHO Page
Authentication Method
Negotiate (KERBEROS)
Request.ServerVariables("AUTH_TYPE")
Identity
INOVITDEMOS\BG00001
Request.ServerVariables("AUTH_USER") or System.Threading.Thread.CurrentPrincipal.Identity
Windows identity
INOVITDEMOS\svckrbapp
System.Security.Principal.WindowsIdentity.Getcurrent
Identity (System.Threading.Thread.CurrentPrincipal.Identity)
AuthenticationType Negotiate
ImpersonationLevel Impersonation
IsAuthenticated True
IsGuest False
IsSystem False
IsAnonymous False
Name INOVITDEMOS\BG00001

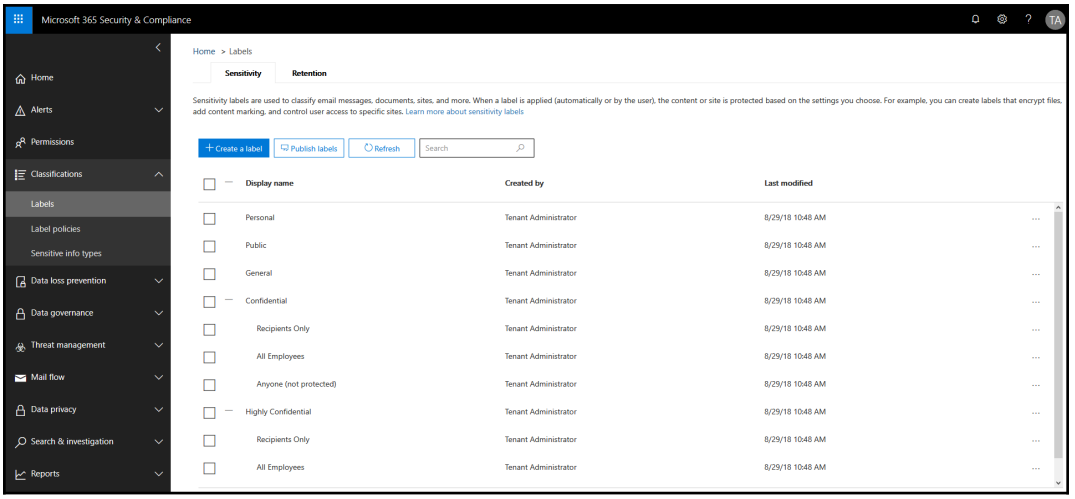

Microsoft Azure
Search resources, services, and docs
admin@adatumdemo...
ADATUM CORP
Home > Adatum Corp > Entitlement management - Entitlements
Entitlement management - Entitlements
PREVIEW
Create a resource
All services
FAVORITES
Dashboard
All resources
Azure Active Directory
Users
Azure AD Identity Protection
Azure Information Protecti...
Security Center
Azure AD B2C
Azure AD Privileged Identit...
Access reviews
Azure AD Connect Health
Enterprise applications
Subscriptions
Manage
Catalogs
Entitlements
Settings
New entitlement
Refresh
Search by entitlement name
NAME
DESCRIPTION
CATALOG
PERMISSIONS
POLICIES
DISCOVERABLE
Sales & Marketing
Intended for sales and marketing tea...
Sales and Marketing
4
3
Yes
Finance employees
For finance employees only who do...
Finance
0
0
No
lead management tools
Access is restricted to authorized use...
Sales and Marketing
1
1
Yes
Marketing
Marketing launch of new initiative
Sales and Marketing
1
1
Yes
Access from Microsoft
Microsoft employee access
Business partnerships
0
1
Yes
Access to directory
General purpose request for director...
Default Catalog
0
1
No


Search resources, services, and docs
admin@adatumdemo...
ADATUM CORP
Home > Adatum Corp > Entitlement management - Entitlements > Sales & Marketing - Resources
Sales & Marketing - Resources
Entitlement - PREVIEW
Overview
Manage
Resources
Policies
Grants
Requests
Owners
Add resources
Refresh
Search by resource name
Type
All
NAME
TYPE
ROLE
CREATED BY
CREATED ON
Sales and Marketing
SharePoint Site
Sales and Marketing Members
admin@adatumdemos.onmicro...
9/14/2018
Marketo
Application
msiam_access
admin@adatumdemos.onmicro...
9/14/2018
Adatum Salesforce
Application
Chatter Free User
admin@adatumdemos.onmicro...
9/6/2018
Sales & Marketing
Security Group
Member
admin@adatumdemos.onmicro...
9/6/2018

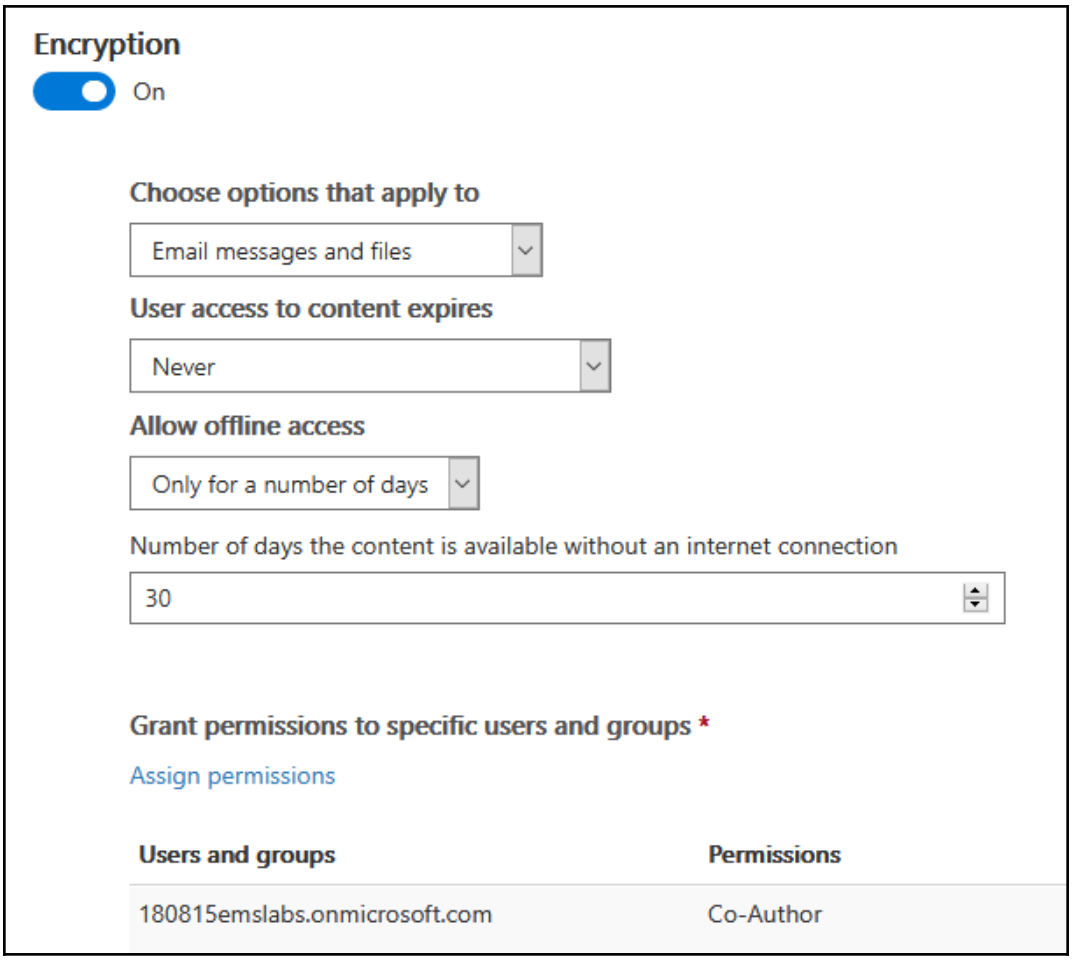

Search resources, services, and docs
admin@adatumdemo...
ADATUM CORP
Home > Adatum Corp > Entitlement management - Entitlements > Sales & Marketing - Policies > Edit entitlement policy
Edit entitlement policy
PREVIEW
* Details
Requests
Lifecycle
Summary
Users
Target users who can request access to the entitlement
All identities not in another policy
Select groups and partners
Groups that can request access
All Users
Add/Remove groups
Partners whose users can request access
Contoso + 1 more
Add/Remove partners
User type to be added
Guest
Member
Approvers
Select who approves access requests
Automatically approve
Automatically deny
Require approval

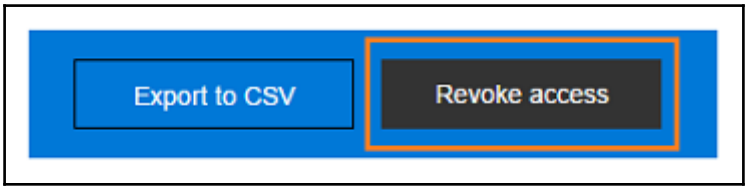
Chapter 12: Creating a Security Culture

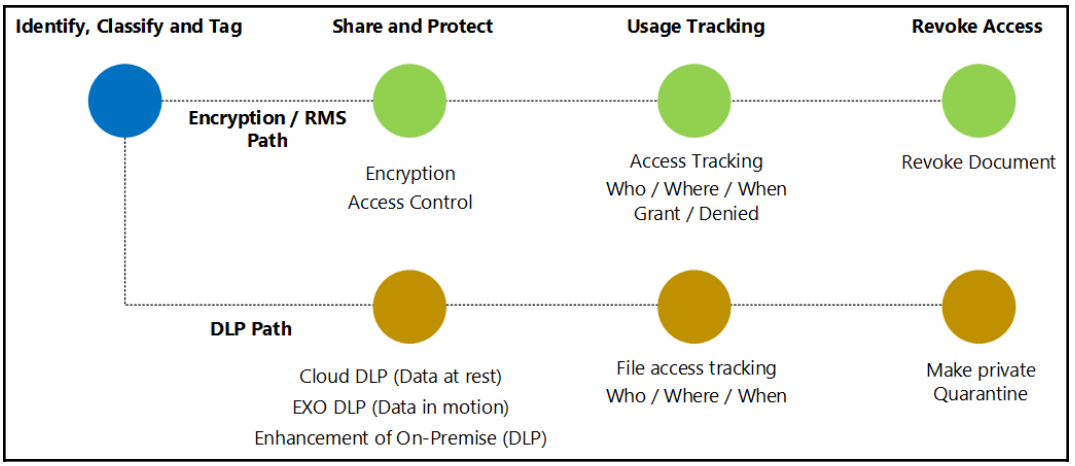



Microsoft 365 Security & Compliance
Home
Alerts
Permissions
Classifications
Labels
Label policies
Sensitive info types
Data loss prevention
Data governance
Threat management
Mail flow
Data privacy
Search & investigation
Reports
Home > Labels
Sensitivity
Retention
Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. Learn more about sensitivity labels
Create a label
Publish labels
Refresh
Search
Display name
Created by
Last modified
Personal
Tenant Administrator
8/29/18 10:48 AM
Public
Tenant Administrator
8/29/18 10:48 AM
General
Tenant Administrator
8/29/18 10:48 AM
Confidential
Tenant Administrator
8/29/18 10:48 AM
Recipients Only
Tenant Administrator
8/29/18 10:48 AM
All Employees
Tenant Administrator
8/29/18 10:48 AM
Anyone (not protected)
Tenant Administrator
8/29/18 10:48 AM
Highly Confidential
Tenant Administrator
8/29/18 10:48 AM
Recipients Only
Tenant Administrator
8/29/18 10:48 AM
All Employees
Tenant Administrator
8/29/18 10:48 AM

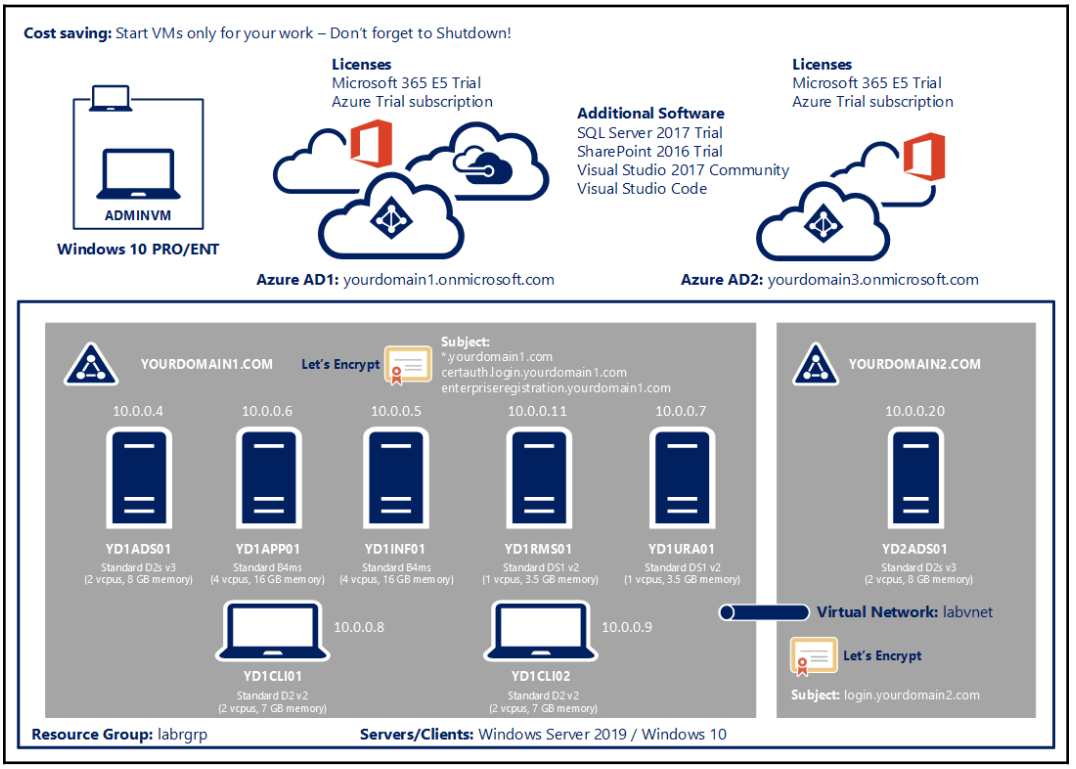

It is recommended to label this file as Confidential \ All Employees
Change now
Dismiss

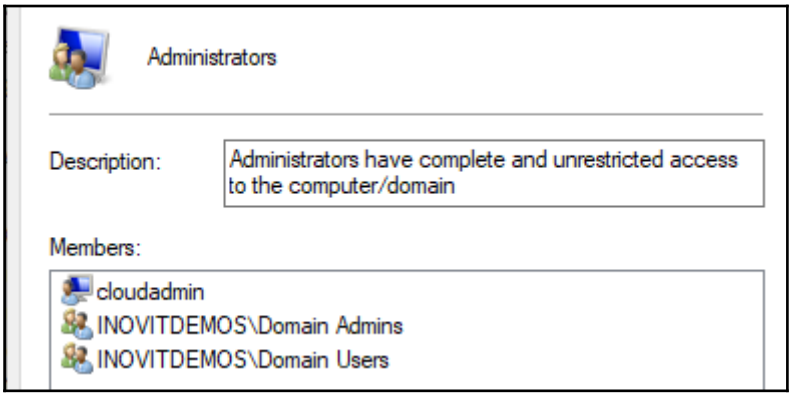

Encryption
On
Choose options that apply to
Email messages and files
User access to content expires
Never
Allow offline access
Only for a number of days
Number of days the content is available without an internet connection
30
Grant permissions to specific users and groups *
Assign permissions
Users and groups
Permissions
180815emslabs.onmicrosoft.com
Co-Author

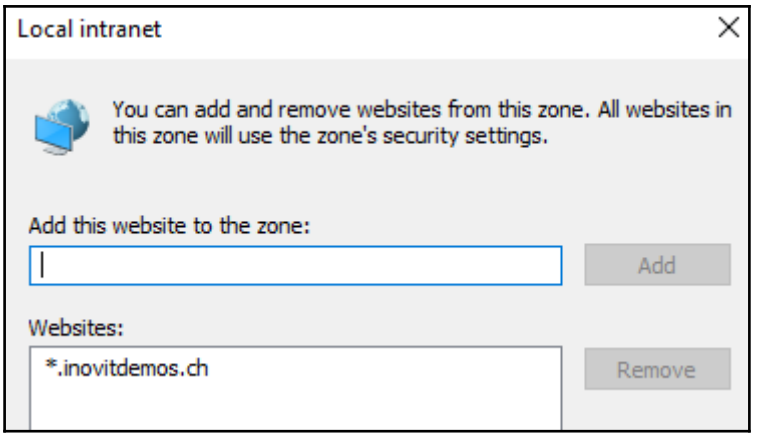

Export to CSV
Revoke access

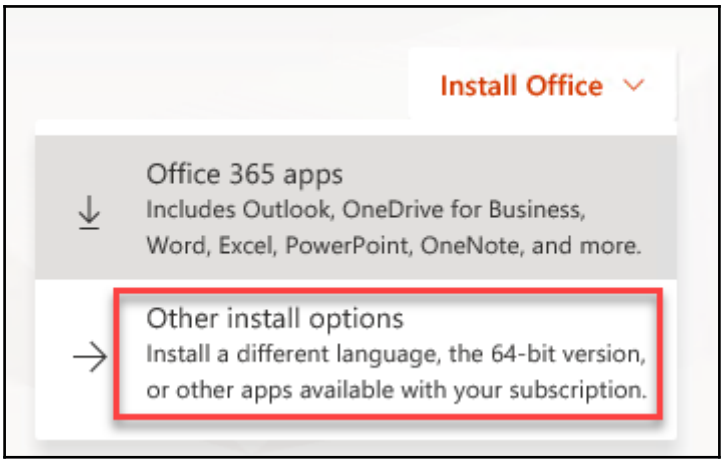

Identify, Classify and Tag
Share and Protect
Usage Tracking
Revoke Access
Encryption / RMS Path
Encryption
Access Control
Access Tracking
Who / Where / When
Grant / Denied
Revoke Document
DLP Path
Cloud DLP (Data at rest)
EXO DLP (Data in motion)
Enhancement of On-Premise (DLP)
File access tracking
Who / Where / When
Make private
Quarantine

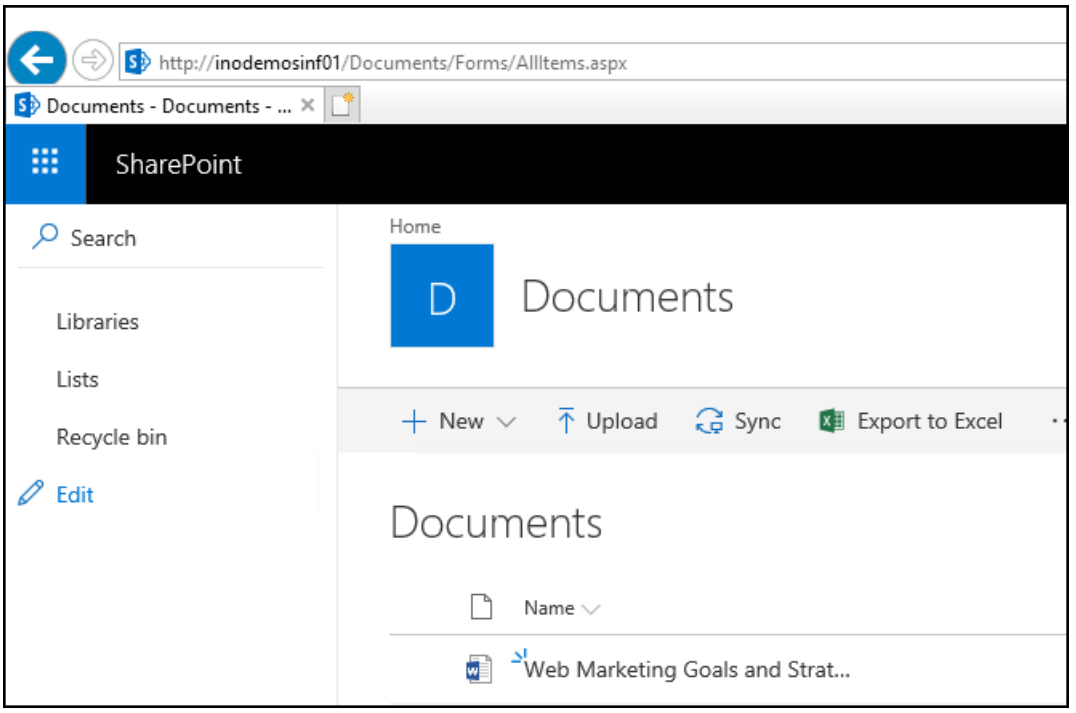
Chapter 13: Identifying and Detecting Sensitive Data



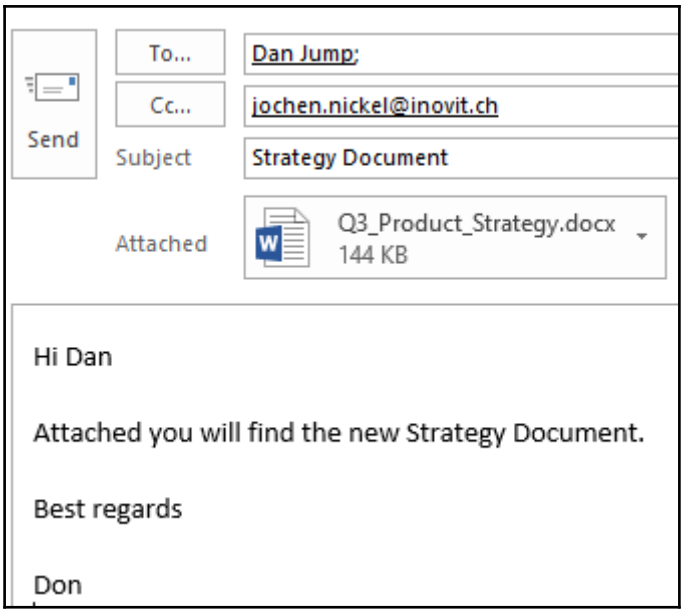


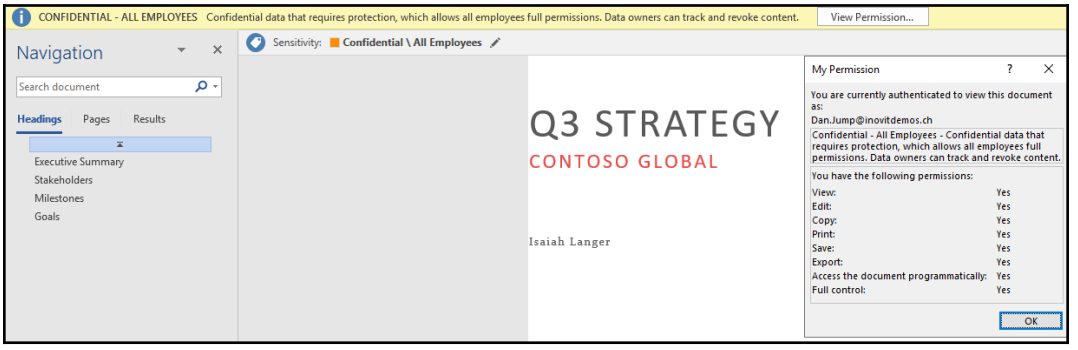

Local intranet
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
Add
Websites:
*.inovitdemos.ch
Remove

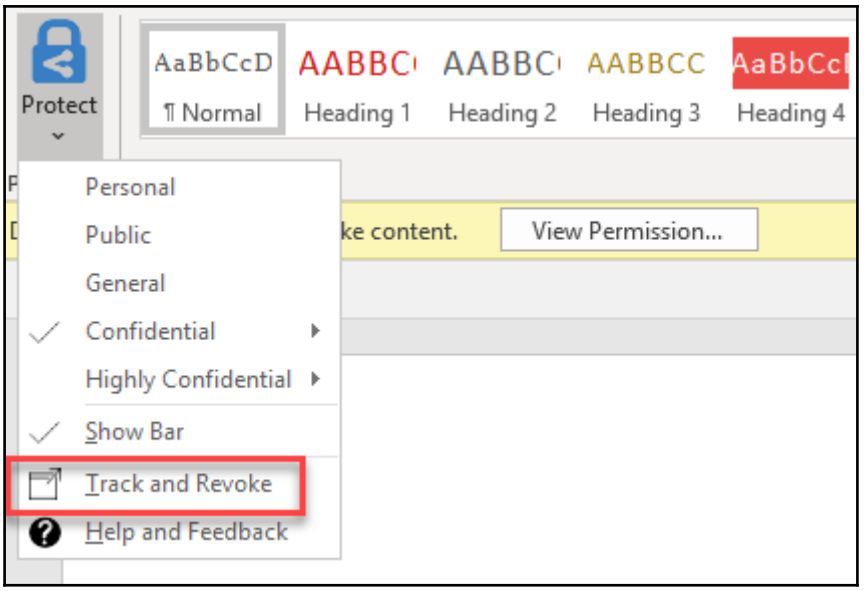

Install Office
Office 365 apps
Includes Outlook, OneDrive for Business, Word, Excel, PowerPoint, OneNote, and more.
Other install options
Install a different language, the 64-bit version, or other apps available with your subscription.

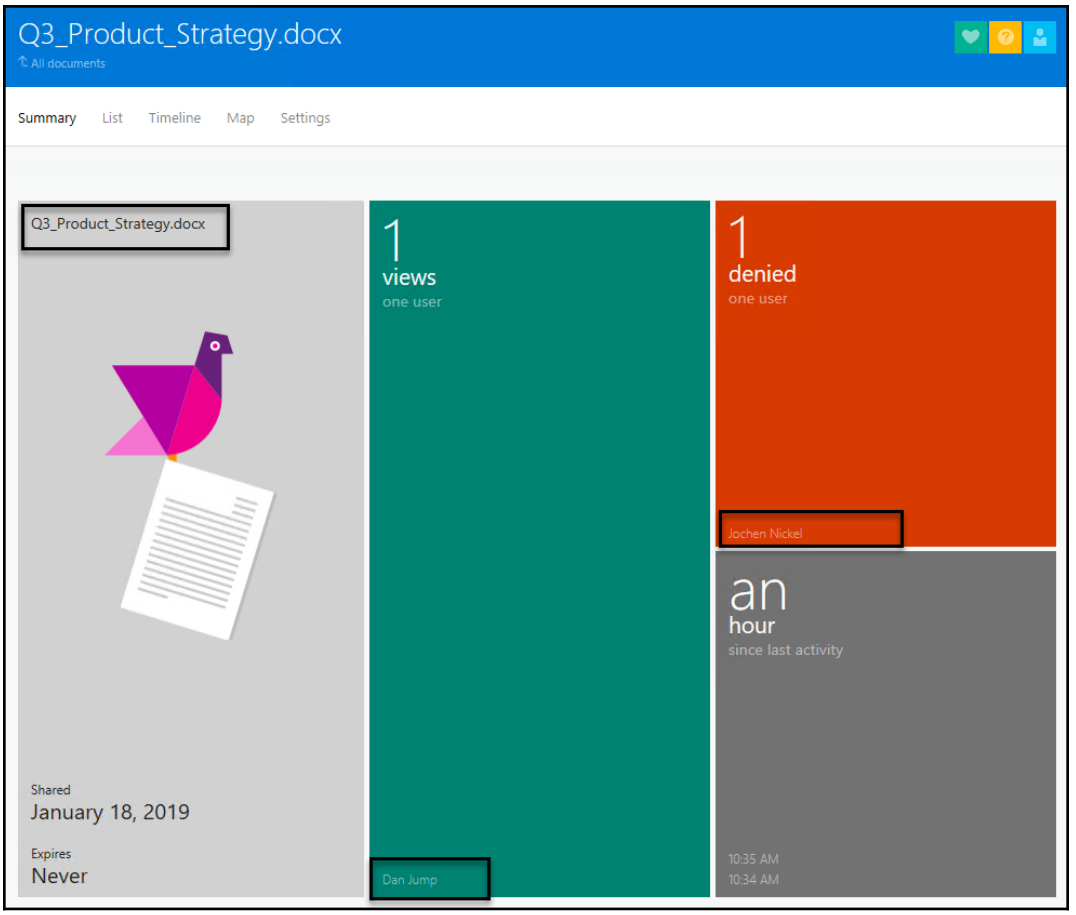

http://inodemosinf01/Documents/Forms/AllItems.aspx
Documents - Documents - ...
SharePoint
Search
Libraries
Lists
Recycle bin
Edit
Home
D
Documents
New
Upload
Sync
Export to Excel
Documents
Name
Web Marketing Goals and Strat...

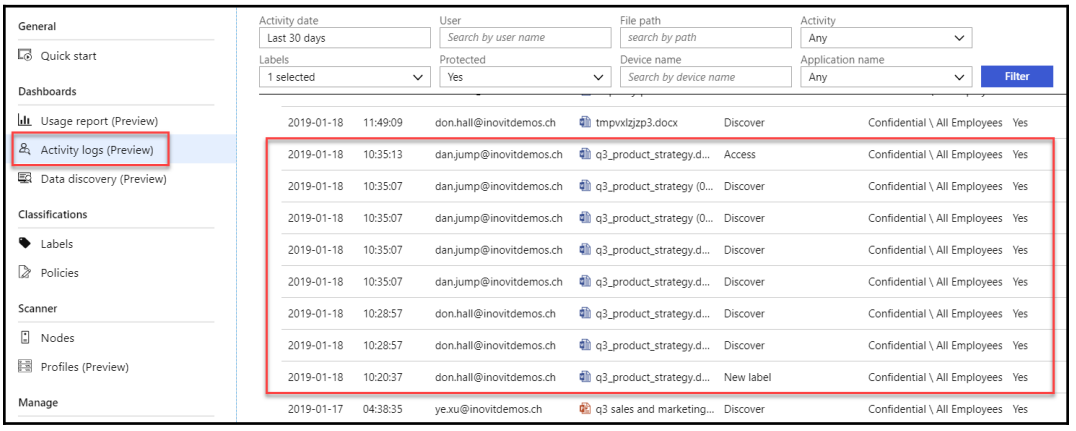

Personal
Public
General
Confidential
Highly Confidential
All Employees
Anyone (not protected)
Q3 STRATEGY
CONTOSO GLOBAL

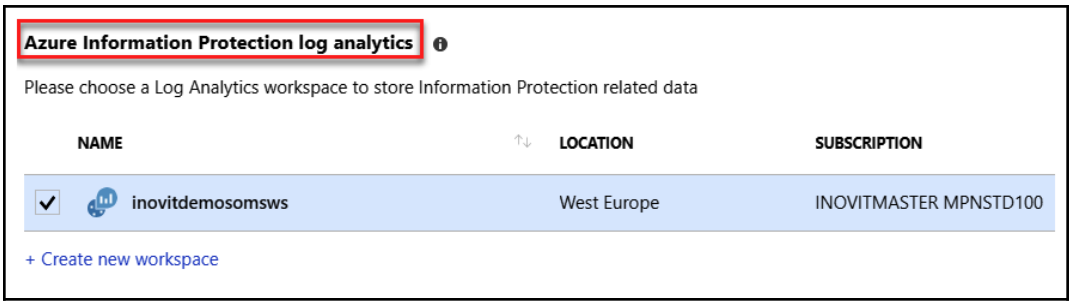

Send
To...
Dan Jump;
Cc...
jochen.nickel@inovit.ch
Subject
Strategy Document
Attached
Q3_Product_Strategy.docx
144 KB
Hi Dan
Attached you will find the new Strategy Document.
Best regards
Don

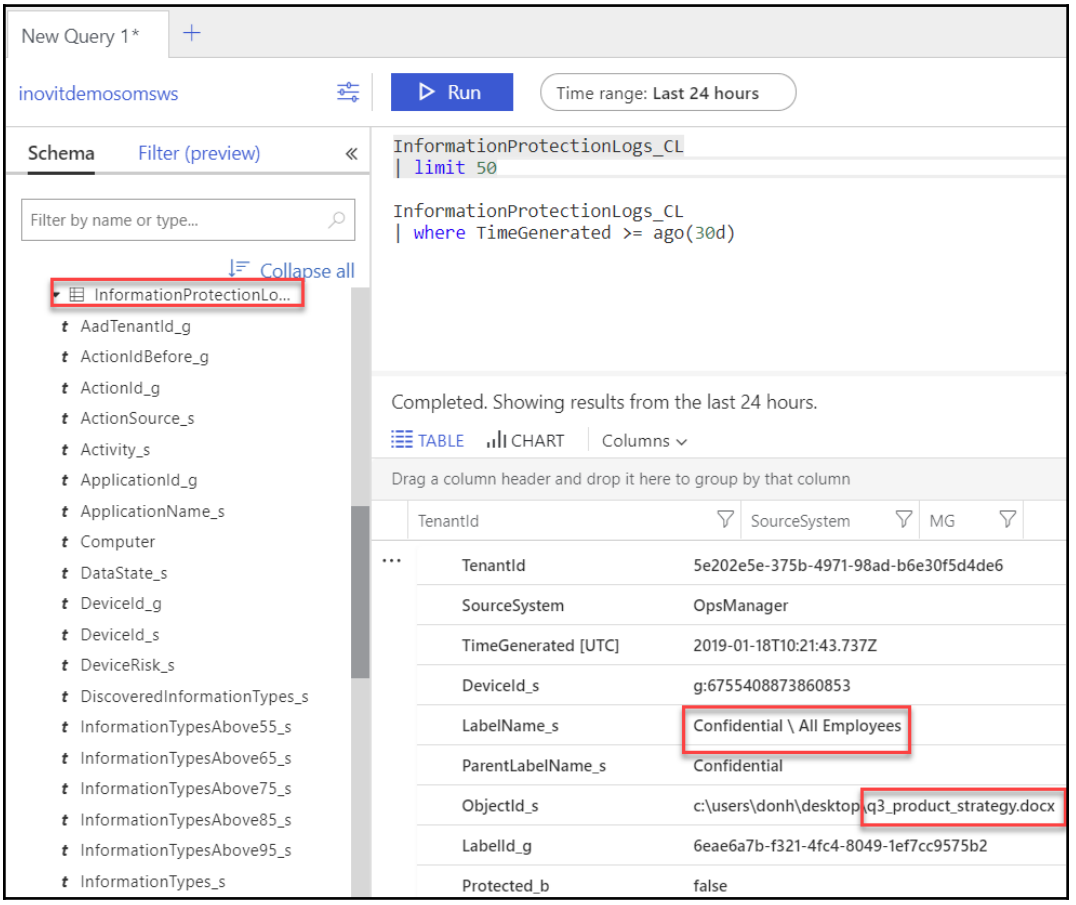

CONFIDENTIAL - ALL EMPLOYEES Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.
View Permission...
Navigation
Search document
Headings
Pages
Results
Executive Summary
Stakeholders
Milestones
Goals
Sensitivity: Confidential \ All Employees
Q3 STRATEGY
CONTOSO GLOBAL
Isaiah Langer
My Permission
You are currently authenticated to view this document as:
Dan.Jump@inovitdemos.ch
Confidential - All Employees - Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.
You have the following permissions:
View: Yes
Edit: Yes
Copy: Yes
Print: Yes
Save: Yes
Export: Yes
Access the document programmatically: Yes
Full control: Yes
OK

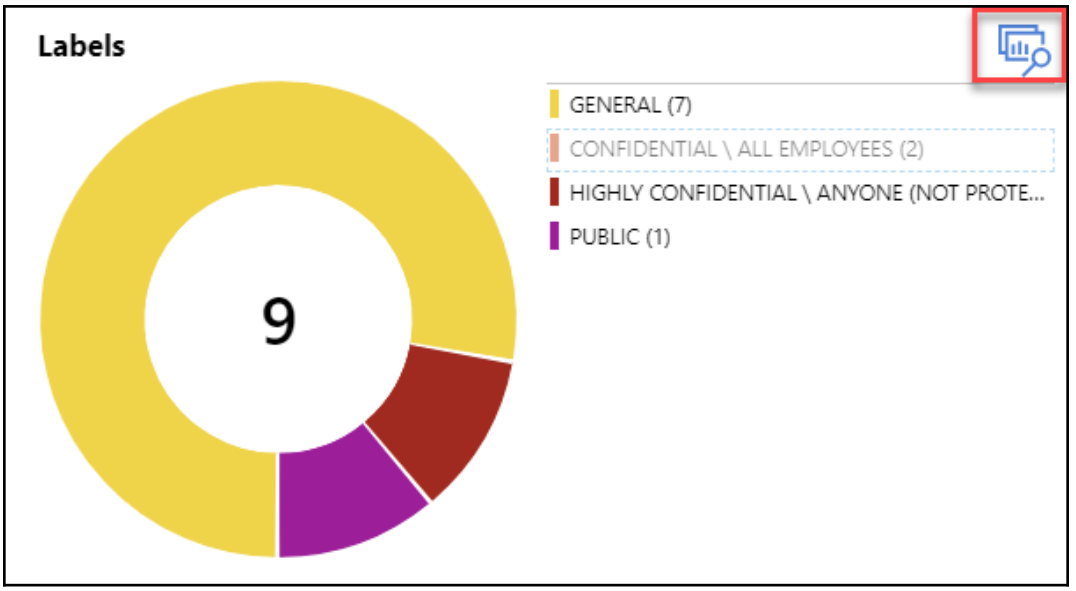

Protect
AaBbCcD
¶ Normal
AABBC
Heading 1
AABBC
Heading 2
AABBCC
Heading 3
AaBbCc
Heading 4
Personal
Public
General
Confidential
Highly Confidential
Show Bar
Track and Revoke
Help and Feedback
ke content.
View Permission...

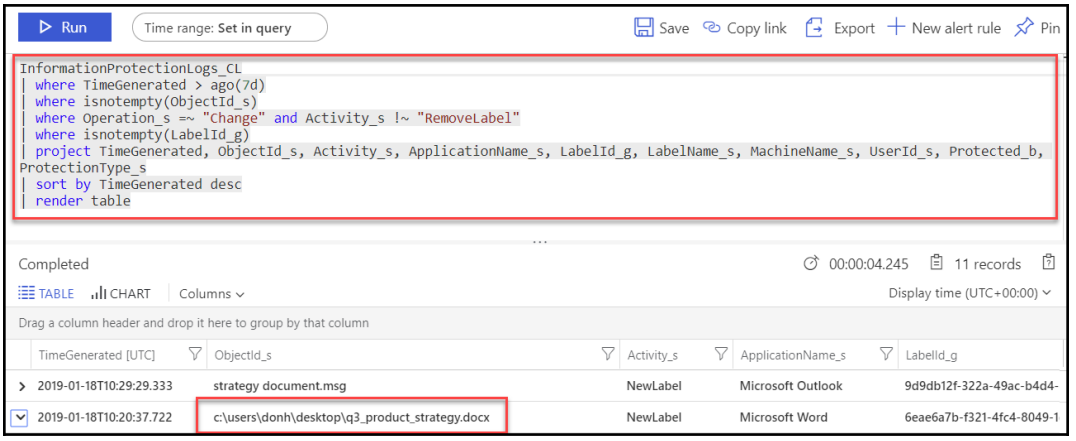

Q3_Product_Strategy.docx
All documents
Summary
List
Timeline
Map
Settings
Q3_Product_Strategy.docx
Shared
January 18, 2019
Expires
Never
1
views
one user
Dan Jump
1
denied
one user
Jochen Nickel
an
hour
since last activity
10:35 AM
10:34 AM

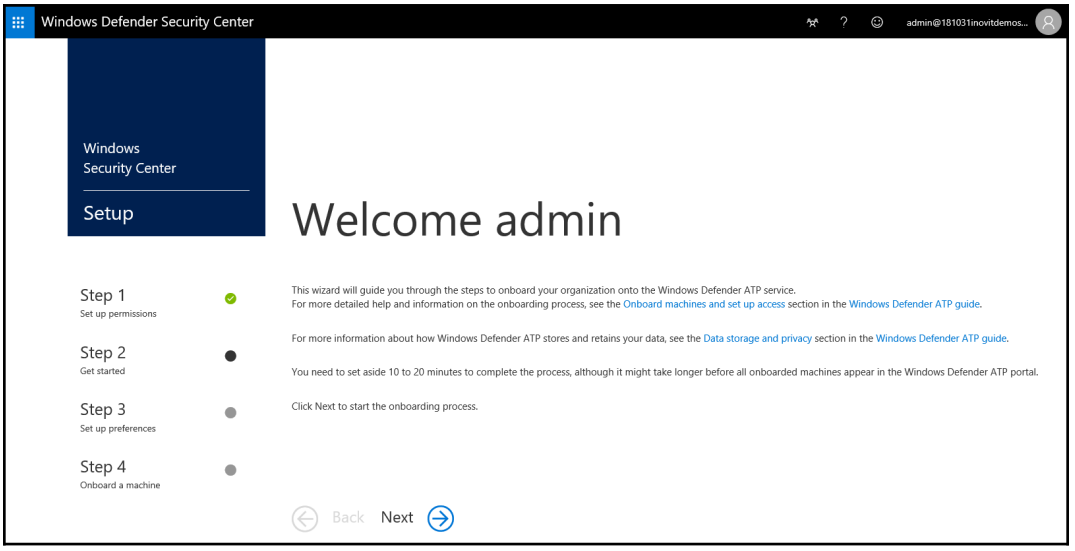

General
Quick start
Dashboards
Usage report (Preview)
Activity logs (Preview)
Data discovery (Preview)
Classifications
Labels
Policies
Scanner
Nodes
Profiles (Preview)
Manage
Activity date
Last 30 days
User
Search by user name
File path
search by path
Activity
Any
Labels
1 selected
Protected
Yes
Device name
Search by device name
Application name
Any
Filter
2019-01-18 11:49:09 don.hall@inovitdemos.ch tmpvxlzjzp3.docx Discover Confidential \ All Employees Yes
2019-01-18 10:35:13 dan.jump@inovitdemos.ch q3_product_strategy.d... Access Confidential \ All Employees Yes
2019-01-18 10:35:07 dan.jump@inovitdemos.ch q3_product_strategy (0... Discover Confidential \ All Employees Yes
2019-01-18 10:35:07 dan.jump@inovitdemos.ch q3_product_strategy (0... Discover Confidential \ All Employees Yes
2019-01-18 10:35:07 dan.jump@inovitdemos.ch q3_product_strategy.d... Discover Confidential \ All Employees Yes
2019-01-18 10:35:07 dan.jump@inovitdemos.ch q3_product_strategy.d... Discover Confidential \ All Employees Yes
2019-01-18 10:28:57 don.hall@inovitdemos.ch q3_product_strategy.d... Discover Confidential \ All Employees Yes
2019-01-18 10:28:57 don.hall@inovitdemos.ch q3_product_strategy.d... Discover Confidential \ All Employees Yes
2019-01-18 10:20:37 don.hall@inovitdemos.ch q3_product_strategy.d... New label Confidential \ All Employees Yes
2019-01-17 04:38:35 ye.xu@inovitdemos.ch q3 sales and marketing... Discover Confidential \ All Employees Yes

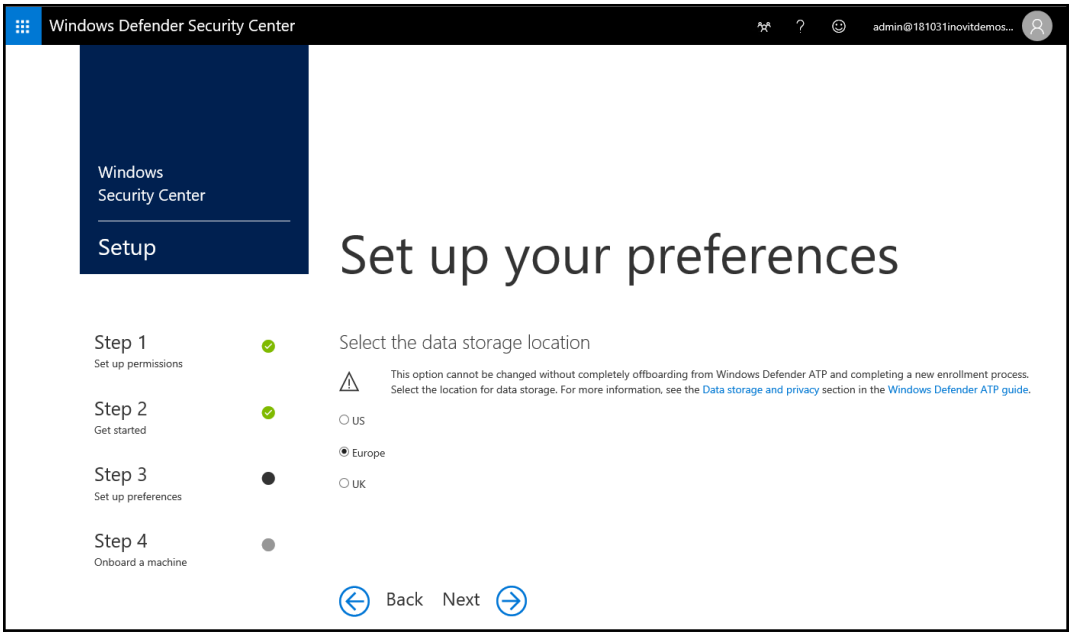

Azure Information Protection log analytics
Please choose a Log Analytics workspace to store Information Protection related data
NAME
LOCATION
SUBSCRIPTION
inovitdemosomsws
West Europe
INOVITMASTER MPNSTD100
+ Create new workspace

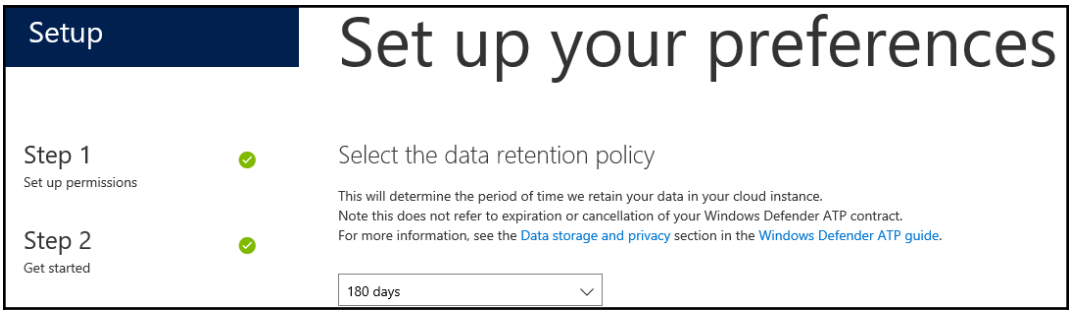

New Query 1*
inovitdemosomsws
Run
Time range: Last 24 hours
Schema
Filter (preview)
Filter by name or type...
Collapse all
InformationProtectionLo...
AadTenantId_g
ActionIdBefore_g
ActionId_g
ActionSource_s
Activity_s
ApplicationId_g
ApplicationName_s
Computer
DataState_s
DeviceId_g
DeviceId_s
DeviceRisk_s
DiscoveredInformationTypes_s
InformationTypesAbove55_s
InformationTypesAbove65_s
InformationTypesAbove75_s
InformationTypesAbove85_s
InformationTypesAbove95_s
InformationTypes_s
InformationProtectionLogs_CL
| limit 50
InformationProtectionLogs_CL
| where TimeGenerated >= ago(30d)
Completed. Showing results from the last 24 hours.
TABLE
CHART
Columns
Drag a column header and drop it here to group by that column
TenantId
SourceSystem
MG
TenantId 5e202e5e-375b-4971-98ad-b6e30f5d4de6
SourceSystem OpsManager
TimeGenerated [UTC] 2019-01-18T10:21:43.737Z
DeviceId_s g:6755408873860853
LabelName_s Confidential \ All Employees
ParentLabelName_s Confidential
ObjectId_s c:\users\donh\desktop\q3_product_strategy.docx
LabelId_g 6eae6a7b-f321-4fc4-8049-1ef7cc9575b2
Protected_b false


Labels
9
GENERAL (7)
CONFIDENTIAL \ ALL EMPLOYEES (2)
HIGHLY CONFIDENTIAL \ ANYONE (NOT PROTE...
PUBLIC (1)


Run
Time range: Set in query
Save
Copy link
Export
New alert rule
Pin
InformationProtectionLogs_CL
| where TimeGenerated > ago(7d)
| where isnotempty(ObjectId_s)
| where Operation_s =~ "change" and Activity_s !~ "RemoveLabel"
| where isnotempty(LabelId_g)
| project TimeGenerated, ObjectId_s, Activity_s, ApplicationName_s, LabelId_g, LabelName_s, MachineName_s, UserId_s, Protected_b, ProtectionType_s
| sort by TimeGenerated desc
| render table
Completed
00:00:04.245
11 records
TABLE
CHART
Columns
Display time (UTC+00:00)
Drag a column header and drop it here to group by that column
TimeGenerated [UTC]
ObjectId_s
Activity_s
ApplicationName_s
LabelId_g
2019-01-18T10:29:29.333
strategy document.msg
NewLabel
Microsoft Outlook
9d9db12f-322a-49ac-b4d4-
2019-01-18T10:20:37.722
c:\users\donh\desktop\q3_product_strategy.docx
NewLabel
Microsoft Word
6eae6a7b-f321-4fc4-8049-1


Windows Defender Security Center
admin@181031inovitdemos...
Windows
Security Center
Setup
Welcome admin
Step 1
Set up permissions
Step 2
Get started
Step 3
Set up preferences
Step 4
Onboard a machine
This wizard will guide you through the steps to onboard your organization onto the Windows Defender ATP service.
For more detailed help and information on the onboarding process, see the Onboard machines and set up access section in the Windows Defender ATP guide.
For more information about how Windows Defender ATP stores and retains your data, see the Data storage and privacy section in the Windows Defender ATP guide.
You need to set aside 10 to 20 minutes to complete the process, although it might take longer before all onboarded machines appear in the Windows Defender ATP portal.
Click Next to start the onboarding process.
Back
Next


Windows Defender Security Center
admin@181031inovitdemos...
Windows
Security Center
Setup
Set up your preferences
Step 1
Set up permissions
Step 2
Get started
Step 3
Set up preferences
Step 4
Onboard a machine
Select the data storage location
This option cannot be changed without completely offboarding from Windows Defender ATP and completing a new enrollment process.
Select the location for data storage. For more information, see the Data storage and privacy section in the Windows Defender ATP guide.
US
Europe
UK
Back
Next



To start experiencing Windows Defender ATP, you need to onboard at least one machine and run a detection test on that machine. Ensure you:

1. Onboard a machine

First machine onboarded: Incomplete

Onboard machines to Windows Defender ATP using the onboarding configuration package that matches your preferred deployment method. For other machine preparation instructions, read Onboard and set up.

Deployment method

Local Script (for up to 10 machines)

You can configure a single machine by running a script locally.
Note: This script has been optimized for usage with a limited number of machines (1-10). To deploy at scale, please see other deployment options above.
For more information on how to configure and monitor Windows Defender ATP machines, see Configure machines using a local script section in the Windows Defender ATP guide.

Download package

2. Run detection test

Detection test: Incomplete

To verify that the machine is properly onboarded and reporting to the service, run the detection script on the newly onboarded machine:

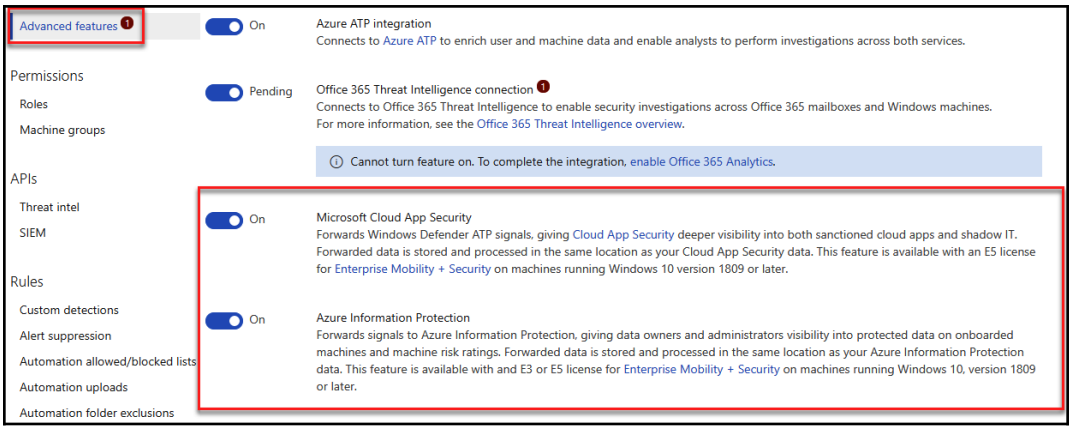
a. Open a Command Prompt window

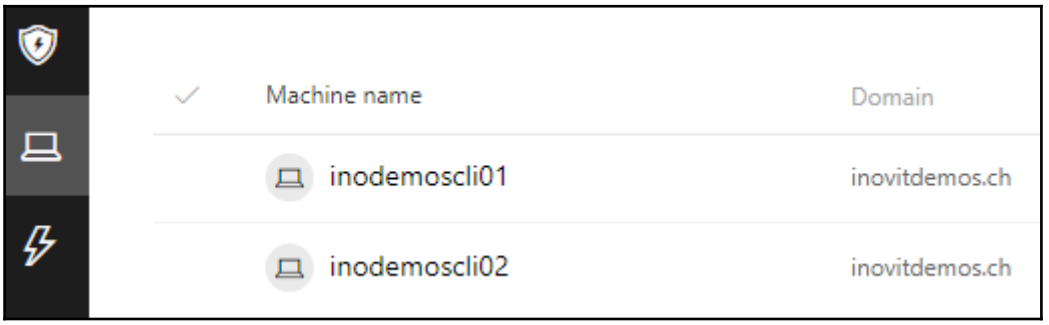
b. At the prompt, copy and run the command below. The Command Prompt window will close automatically.

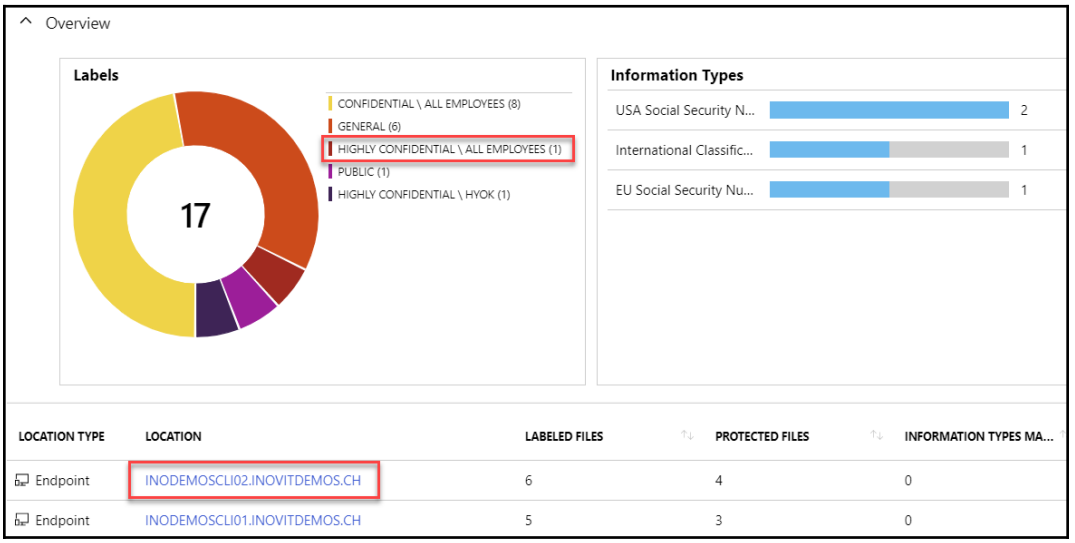
```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden
$ErrorActionPreference= 'silentlycontinue';(New-Object
System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\test-WDATP-
```

Copy

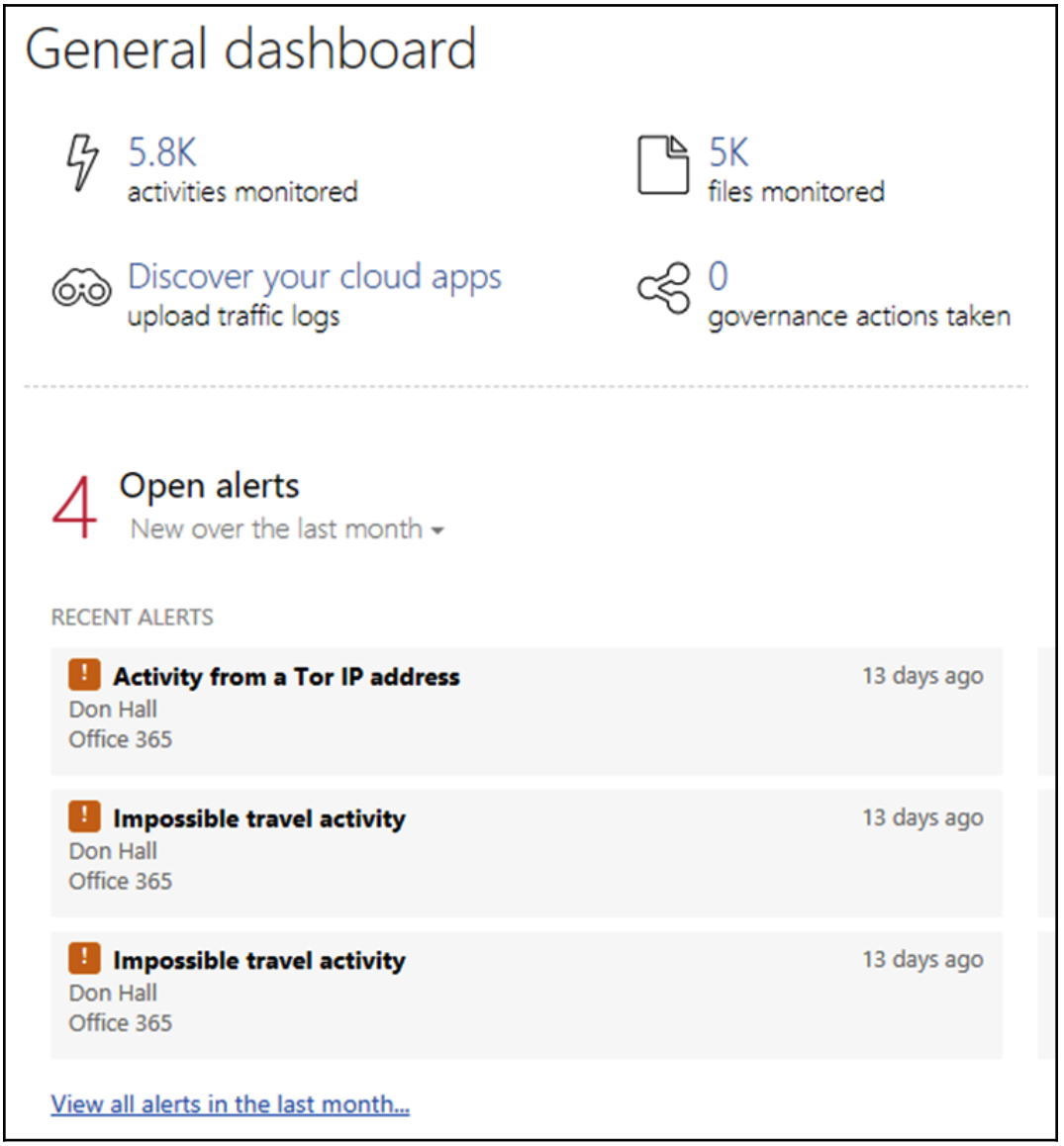
If successful, the detection test will be marked as completed and a new alert will appear in few minutes.

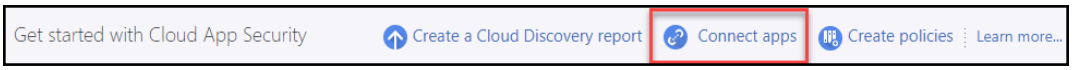

Advanced features
On
Azure ATP integration
Connects to Azure ATP to enrich user and machine data and enable analysts to perform investigations across both services.
Permissions
Roles
Machine groups
Pending
Office 365 Threat Intelligence connection
Connects to Office 365 Threat Intelligence to enable security investigations across Office 365 mailboxes and Windows machines.
For more information, see the Office 365 Threat Intelligence overview.
Cannot turn feature on. To complete the integration, enable Office 365 Analytics.
APIs
Threat intel
SIEM
On
Microsoft Cloud App Security
Forwards Windows Defender ATP signals, giving Cloud App Security deeper visibility into both sanctioned cloud apps and shadow IT. Forwarded data is stored and processed in the same location as your Cloud App Security data. This feature is available with an E5 license for Enterprise Mobility + Security on machines running Windows 10 version 1809 or later.
Rules
Custom detections
Alert suppression
Automation allowed/blocked lists
Automation uploads
Automation folder exclusions
On
Azure Information Protection
Forwards signals to Azure Information Protection, giving data owners and administrators visibility into protected data on onboarded machines and machine risk ratings. Forwarded data is stored and processed in the same location as your Azure Information Protection data. This feature is available with and E3 or E5 license for Enterprise Mobility + Security on machines running Windows 10, version 1809 or later.

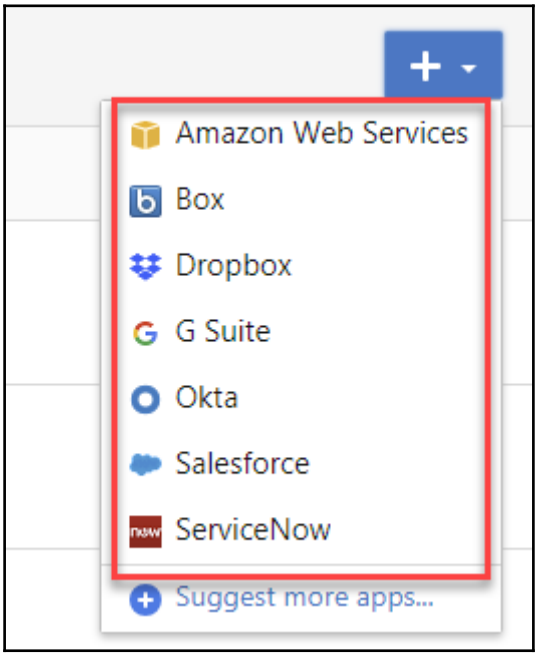

Machine name
Domain
inodemoscli01
inovitdemos.ch
inodemoscli02
inovitdemos.ch

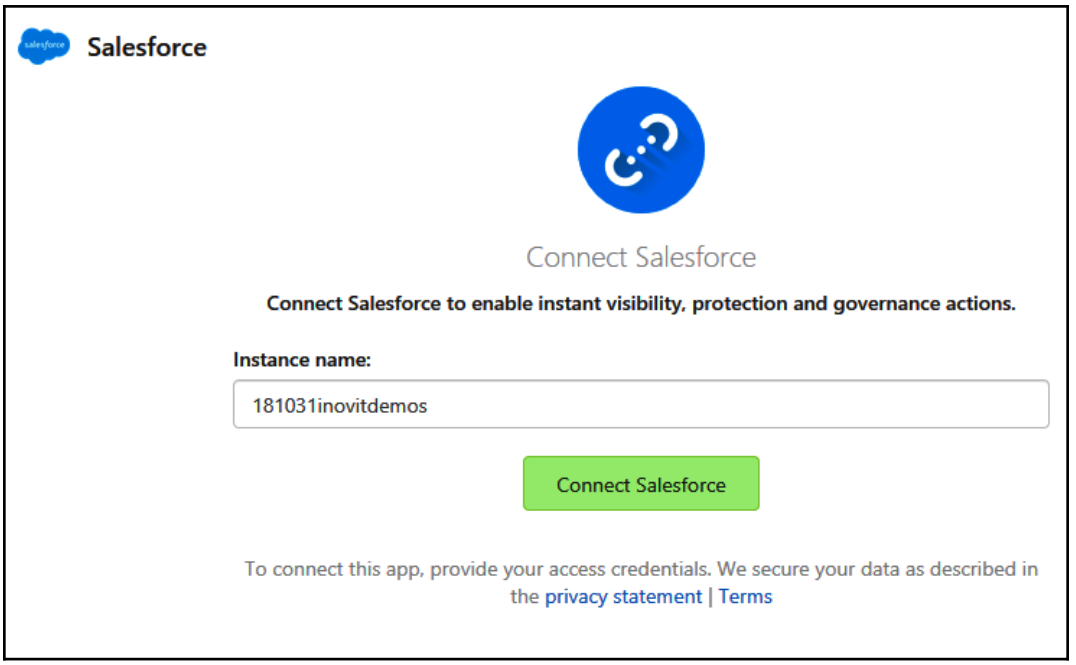

Overview
Labels
17
CONFIDENTIAL \ ALL EMPLOYEES (8)
GENERAL (6)
HIGHLY CONFIDENTIAL \ ALL EMPLOYEES (1)
PUBLIC (1)
HIGHLY CONFIDENTIAL \ HYOK (1)
Information Types
USA Social Security N... 2
International Classific... 1
EU Social Security Nu... 1
LOCATION TYPE
LOCATION
LABELED FILES
PROTECTED FILES
INFORMATION TYPES MA...
Endpoint
INODEMOSCLI02.INOVITDEMOS.CH
6
4
0
Endpoint
INODEMOSCLI01.INOVITDEMOS.CH
5
3
0

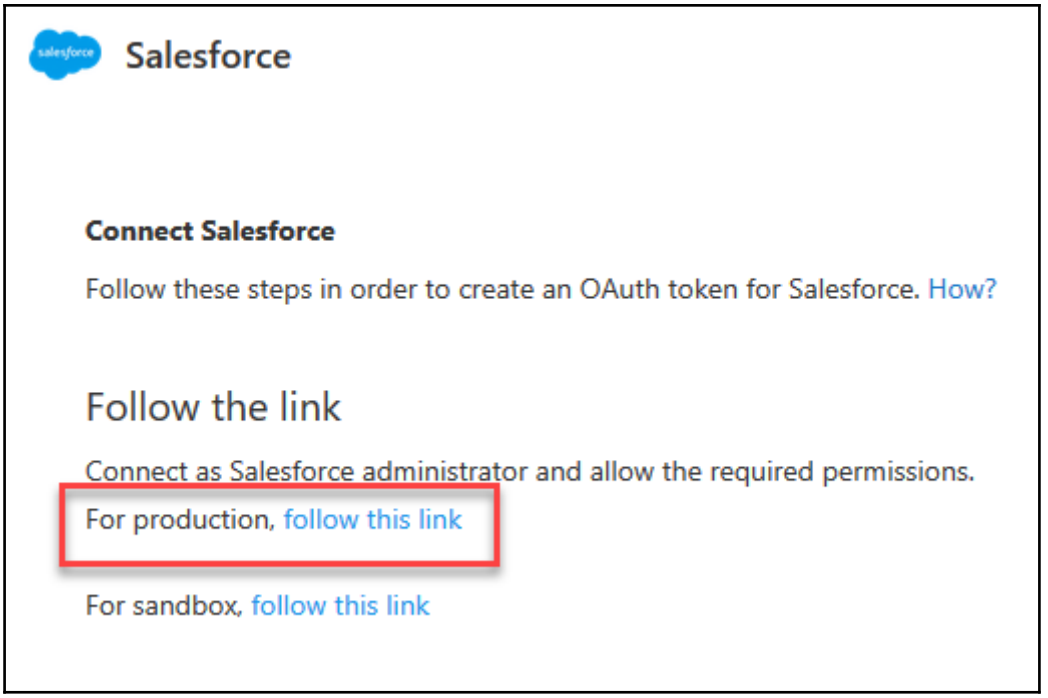
FILE PATH	NAME	LABEL	PROTECTION	INFORMATION TYPES MATCHES	LAST MODIFIED BY	LAST MODIFIED DATE
c:\users\danj\desktop\employee details.xlsx	employee details.xlsx	Highly Confidential \ All Empl...	No		dan.jump@inovitdemos.ch	2019-01-18
c:\users\danj\appdata\local\microsoft\win...	q3_product_strategy (002)....	Confidential \ All Employees	Yes		dan.jump@inovitdemos.ch	2019-01-18
c:\users\danj\appdata\local\microsoft\win...	q3_product_strategy.docx	Confidential \ All Employees	Yes		dan.jump@inovitdemos.ch	2019-01-18

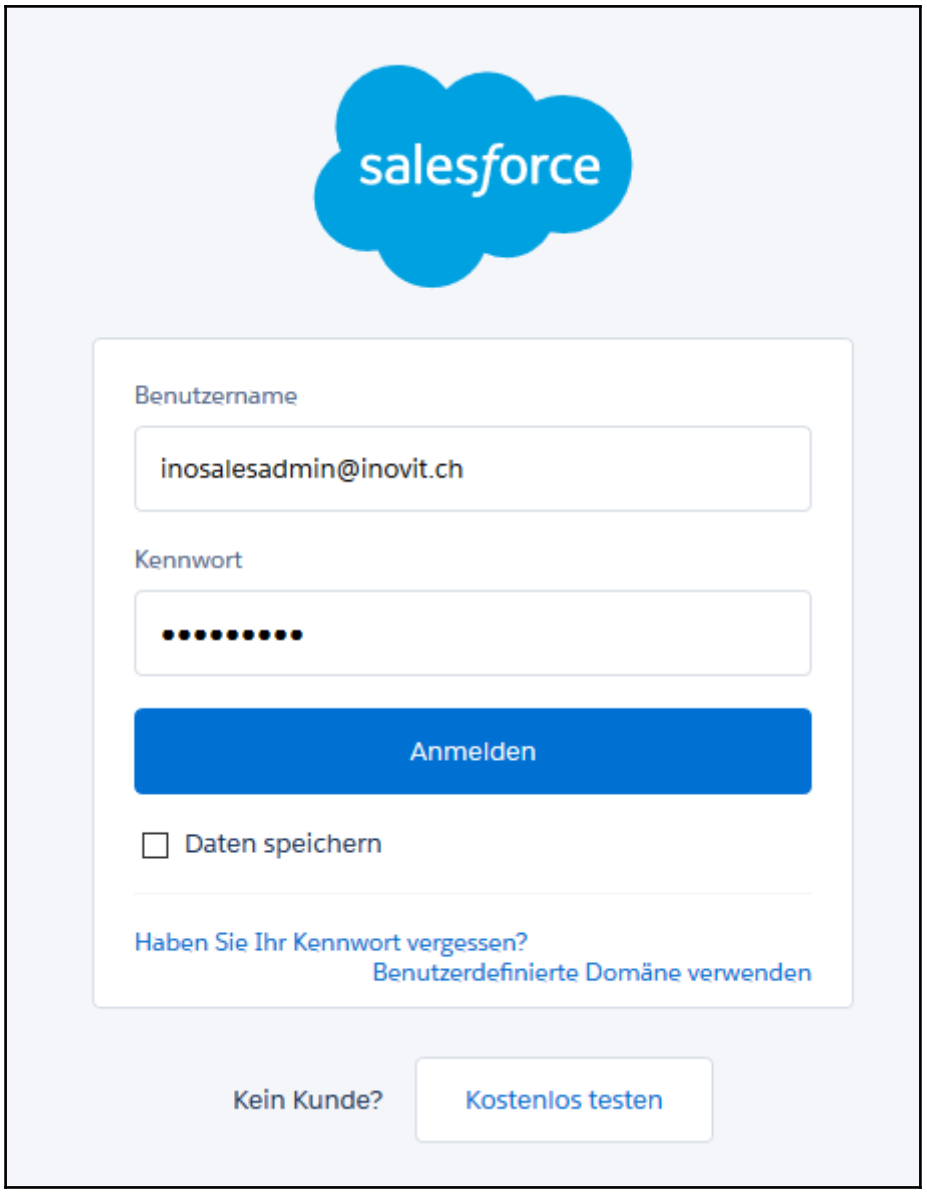


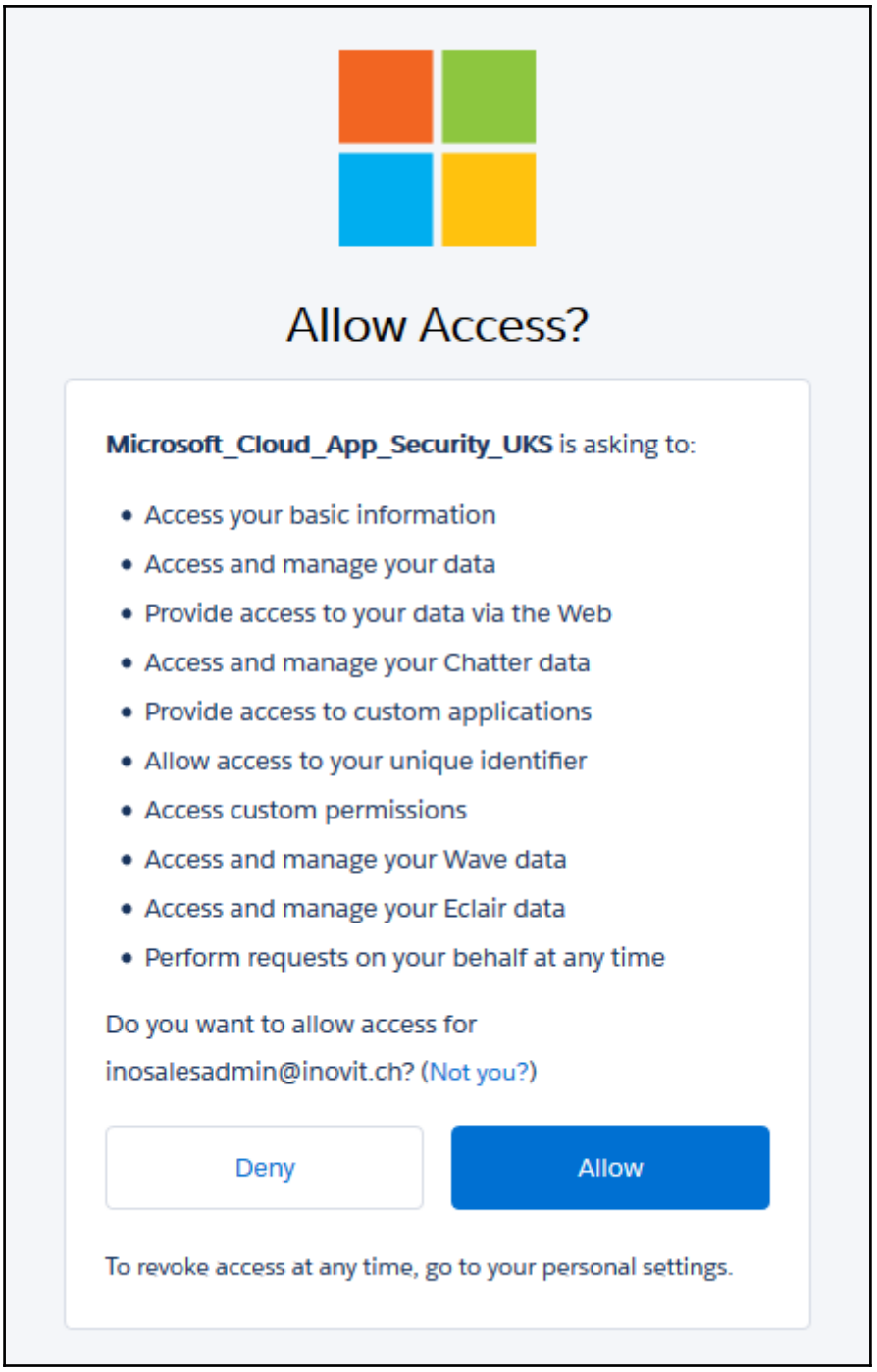

Get started with Cloud App Security
Create a Cloud Discovery report
Connect apps
Create policies
Learn more...

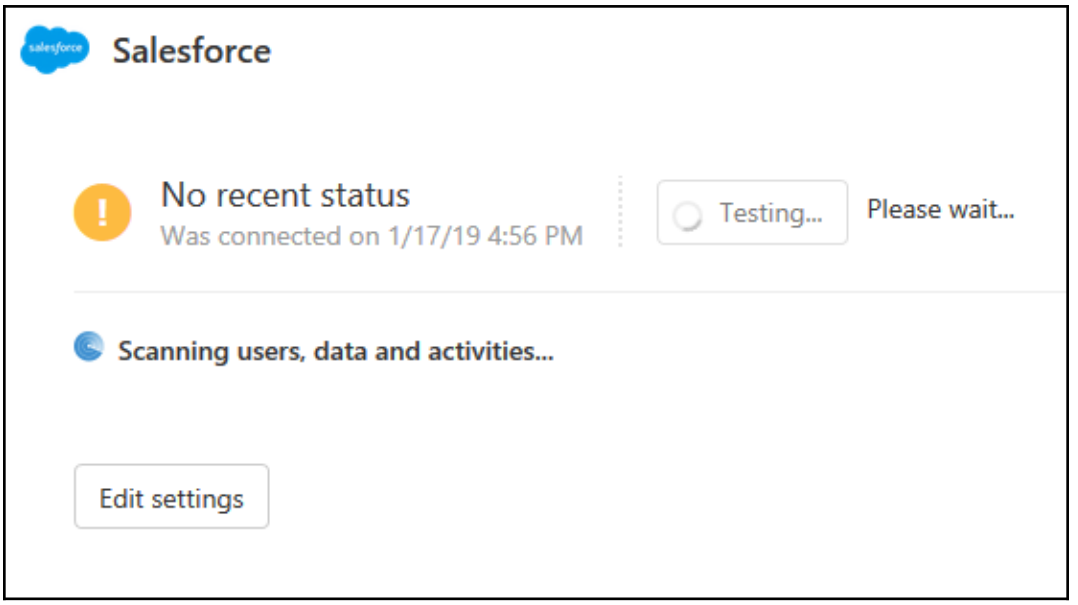

Amazon Web Services
Box
Dropbox
G Suite
Okta
Salesforce
ServiceNow
Suggest more apps...

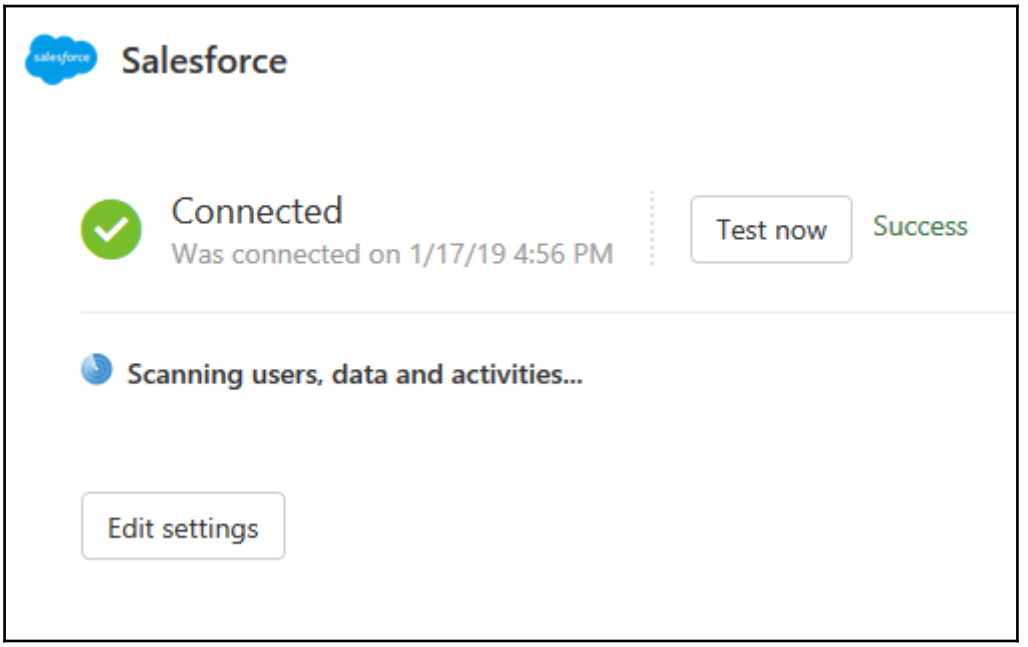

Salesforce
Connect Salesforce
Connect Salesforce to enable instant visibility, protection and governance actions.
Instance name:
181031inovitdemos
Connect Salesforce
To connect this app, provide your access credentials. We secure your data as described in the privacy statement | Terms

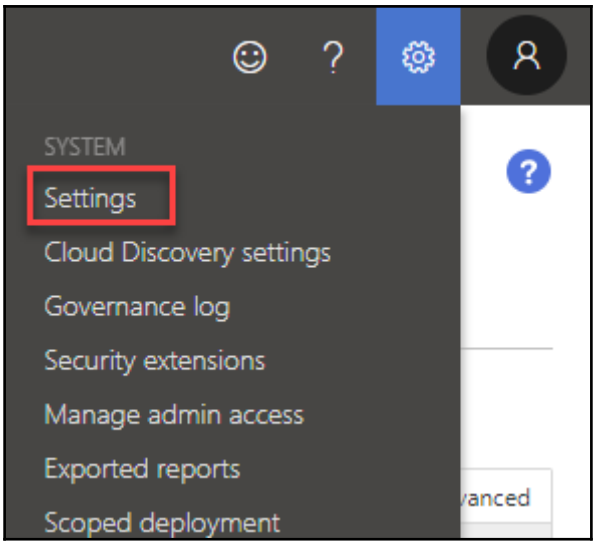

Salesforce
Connect Salesforce
Follow these steps in order to create an OAuth token for Salesforce. How?
Follow the link
Connect as Salesforce administrator and allow the required permissions.
For production, follow this link
For sandbox, follow this link

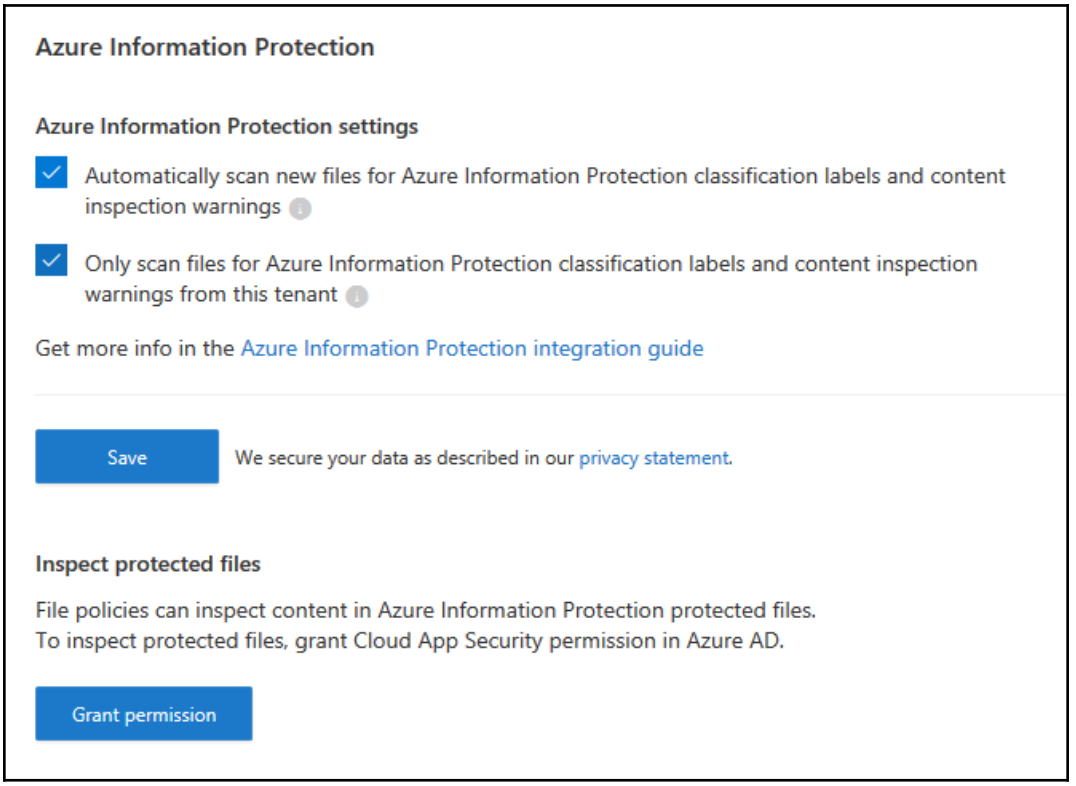

salesforce
Benutzername
inosalesadmin@inovit.ch
Kennwort
Anmelden
Daten speichern
Haben Sie Ihr Kennwort vergessen?
Benutzerdefinierte Domäne verwenden
Kein Kunde?
Kostenlos testen

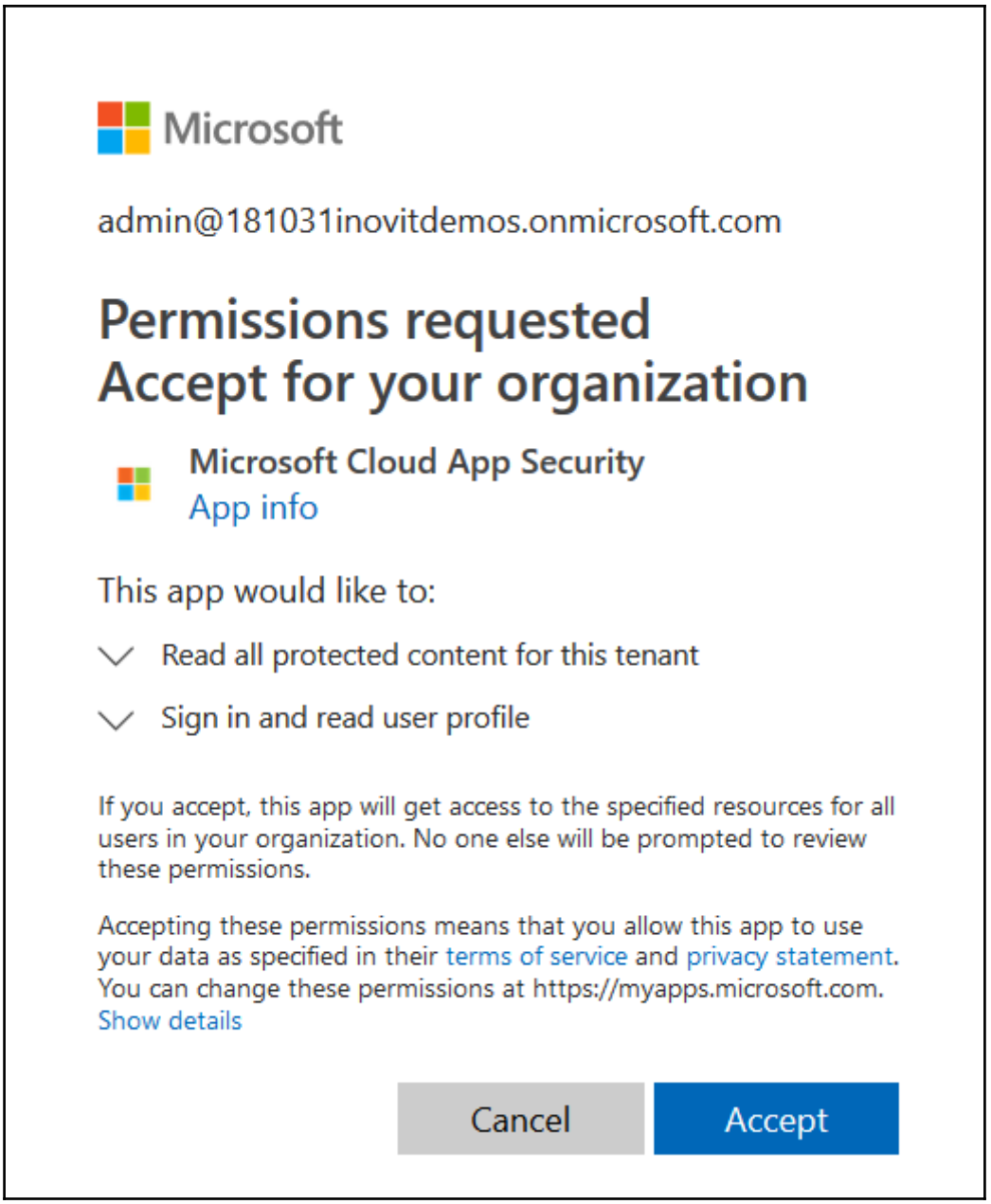

Allow Access?
Microsoft_Cloud_App_Security_UKS is asking to:
Access your basic information
Access and manage your data
Provide access to your data via the Web
Access and manage your Chatter data
Provide access to custom applications
Allow access to your unique identifier
Access custom permissions
Access and manage your Wave data
Access and manage your Eclair data
Perform requests on your behalf at any time
Do you want to allow access for inosalesadmin@inovit.ch? (Not you?)
Deny
Allow
To revoke access at any time, go to your personal settings.

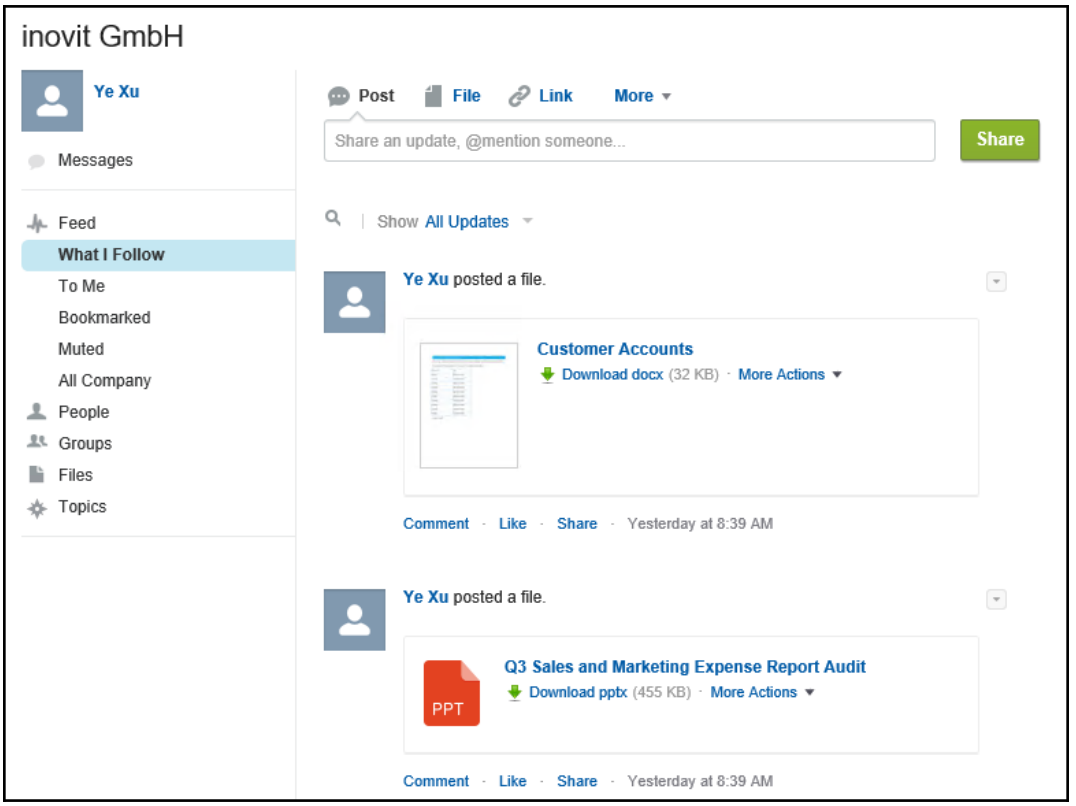

Salesforce
No recent status
Was connected on 1/17/19 4:56 PM
Testing...
Please wait...
Scanning users, data and activities...
Edit settings

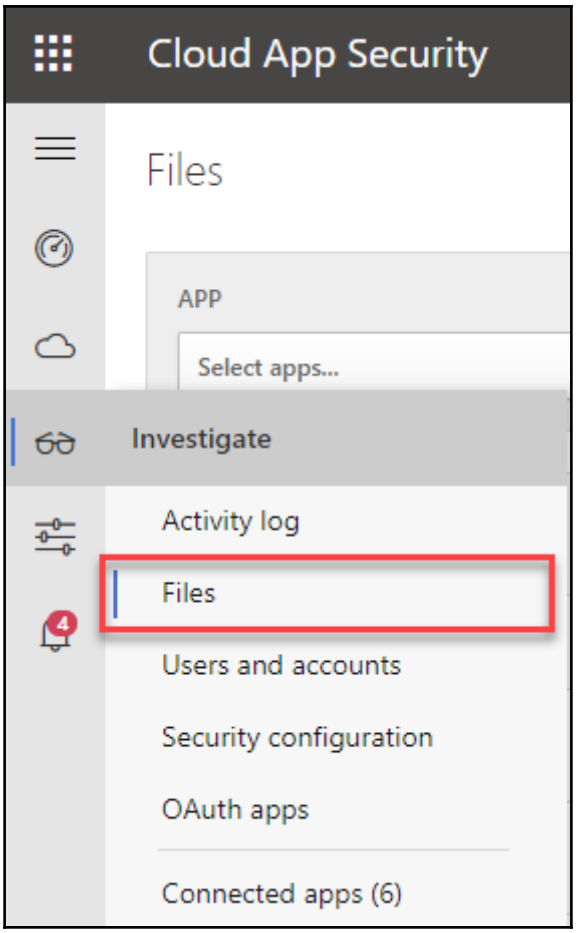

Salesforce
Connected
Was connected on 1/17/19 4:56 PM
Test now
Success
Scanning users, data and activities...
Edit settings

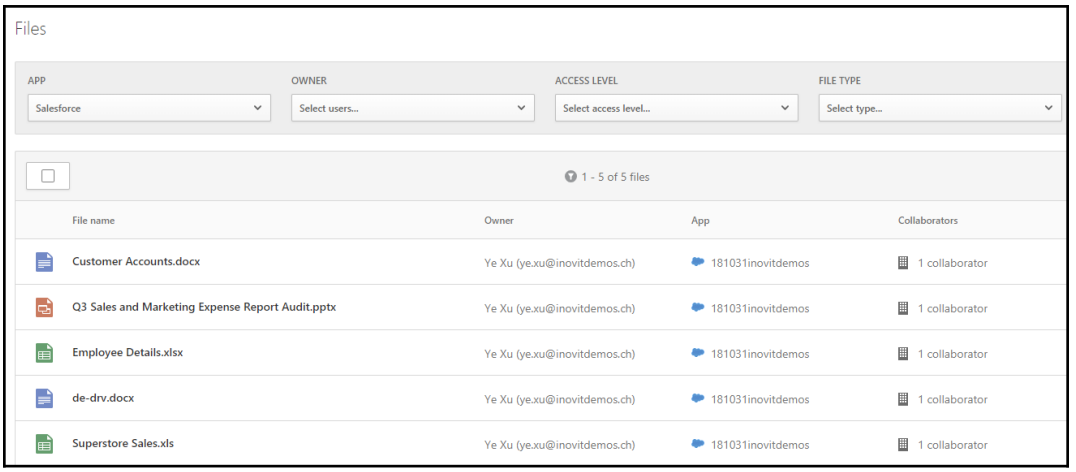

SYSTEM
Settings
Cloud Discovery settings
Governance log
Security extensions
Manage admin access
Exported reports
Scoped deployment

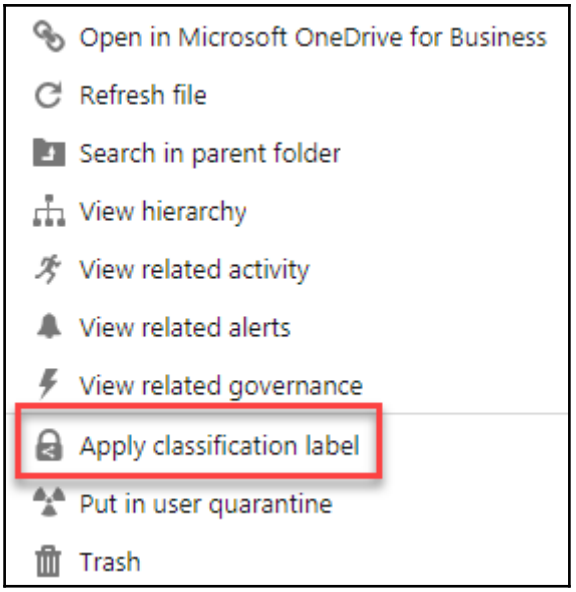

Azure Information Protection
Azure Information Protection settings
Automatically scan new files for Azure Information Protection classification labels and content inspection warnings
Only scan files for Azure Information Protection classification labels and content inspection warnings from this tenant
Get more info in the Azure Information Protection integration guide
Save
We secure your data as described in our privacy statement.
Inspect protected files
File policies can inspect content in Azure Information Protection protected files.
To inspect protected files, grant Cloud App Security permission in Azure AD.
Grant permission

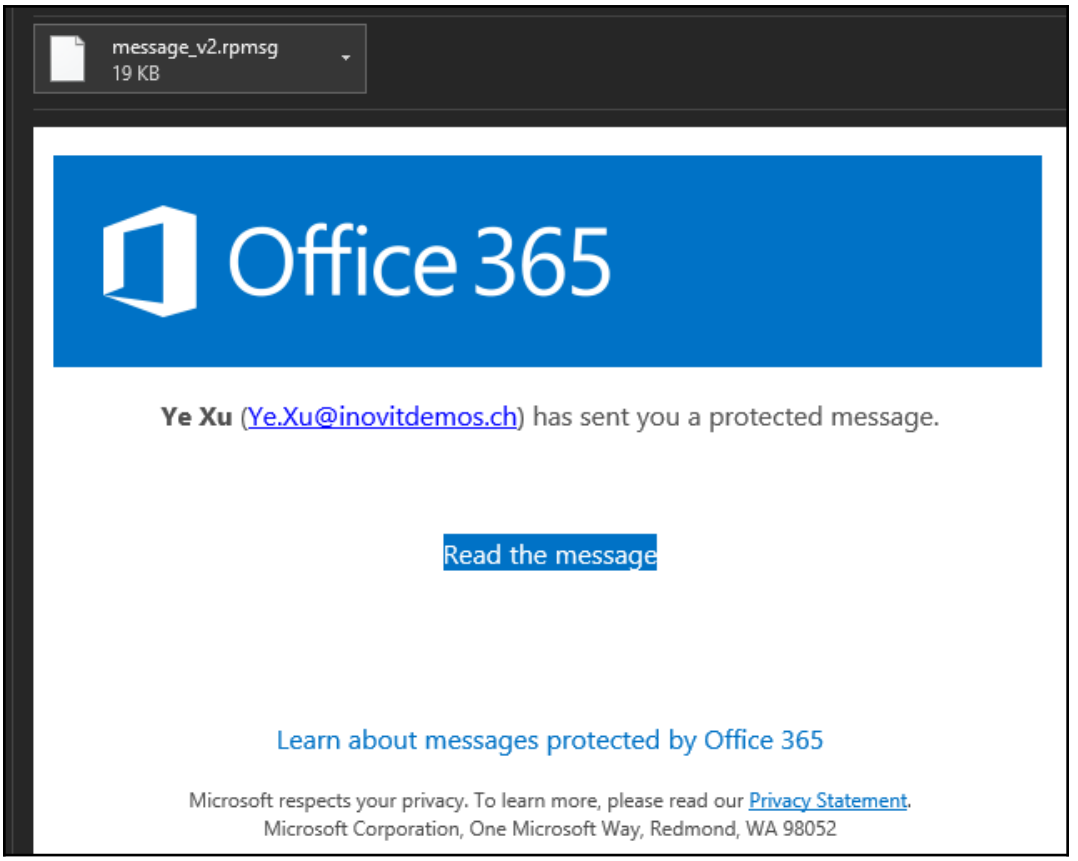

Microsoft
admin@181031inovitdemos.onmicrosoft.com
Permissions requested
Accept for your organization
Microsoft Cloud App Security
App info
This app would like to:
Read all protected content for this tenant
Sign in and read user profile
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com.
Show details
Cancel
Accept


inovit GmbH
Ye Xu
Messages
Feed
What I Follow
To Me
Bookmarked
Muted
All Company
People
Groups
Files
Topics
Post
File
Link
More
Share an update, @mention someone...
Share
Show All Updates
Ye Xu posted a file.
Customer Accounts
Download docx (32 KB) · More Actions
Comment · Like · Share · Yesterday at 8:39 AM
Ye Xu posted a file.
Q3 Sales and Marketing Expense Report Audit
PPT
Download pptx (455 KB) · More Actions
Comment · Like · Share · Yesterday at 8:39 AM


Cloud App Security
Files
APP
Select apps...
Investigate
Activity log
Files
Users and accounts
Security configuration
OAuth apps
Connected apps (6)


Files
APP
Salesforce
OWNER
Select users...
ACCESS LEVEL
Select access level...
FILE TYPE
Select type...
1 - 5 of 5 files
File name
Owner
App
Collaborators
Customer Accounts.docx
Ye Xu (ye.xu@inovitdemos.ch)
181031inovitdemos
1 collaborator
Q3 Sales and Marketing Expense Report Audit.pptx
Ye Xu (ye.xu@inovitdemos.ch)
181031inovitdemos
1 collaborator
Employee Details.xlsx
Ye Xu (ye.xu@inovitdemos.ch)
181031inovitdemos
1 collaborator
de-drv.docx
Ye Xu (ye.xu@inovitdemos.ch)
181031inovitdemos
1 collaborator
Superstore Sales.xls
Ye Xu (ye.xu@inovitdemos.ch)
181031inovitdemos
1 collaborator


Open in Microsoft OneDrive for Business
Refresh file
Search in parent folder
View hierarchy
View related activity
View related alerts
View related governance
Apply classification label
Put in user quarantine
Trash

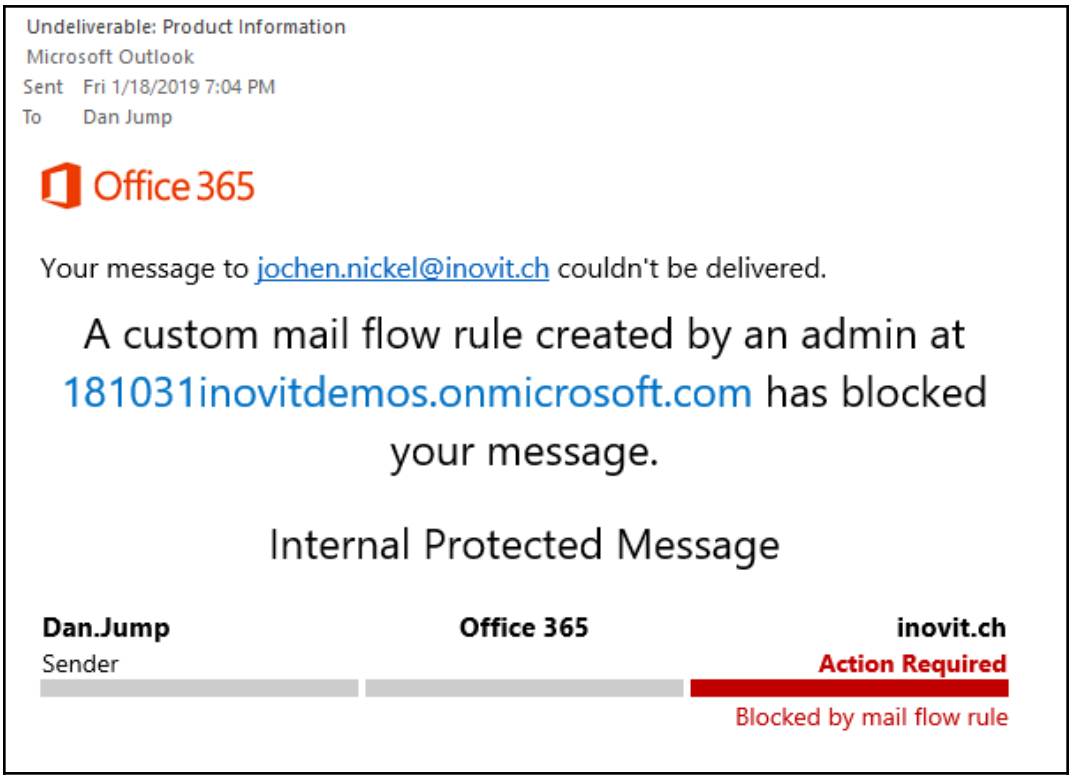


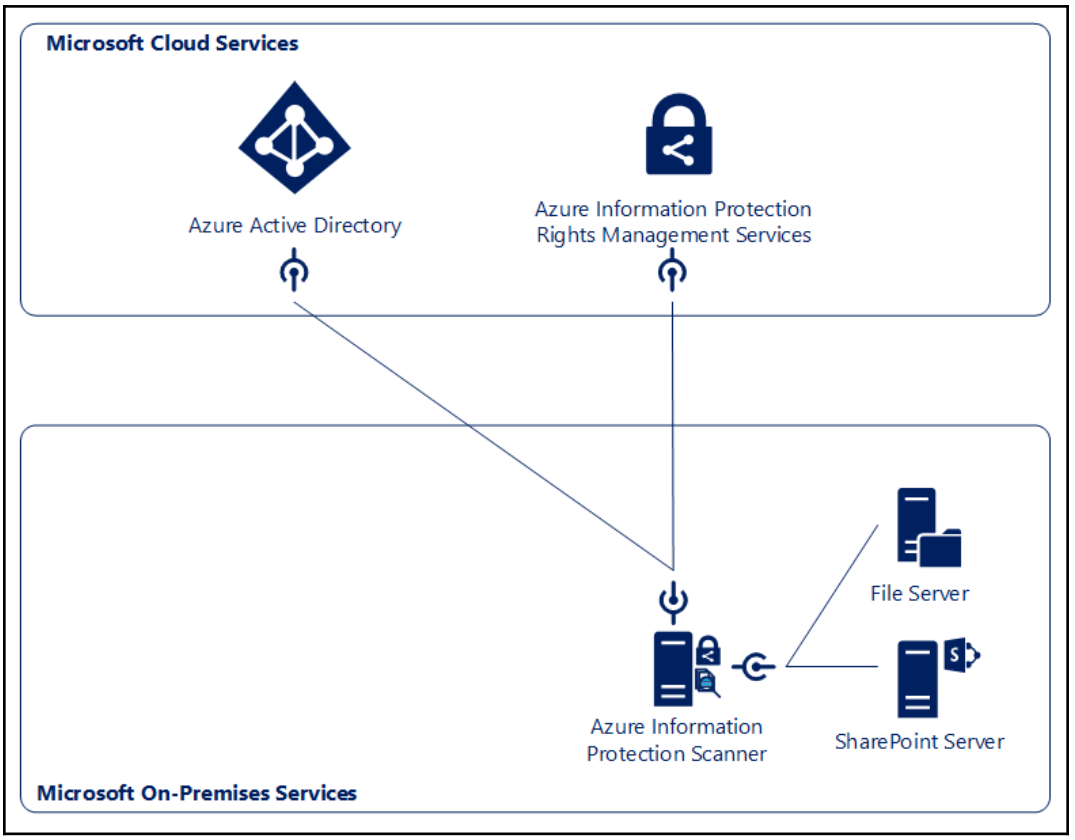
Hi Ye,

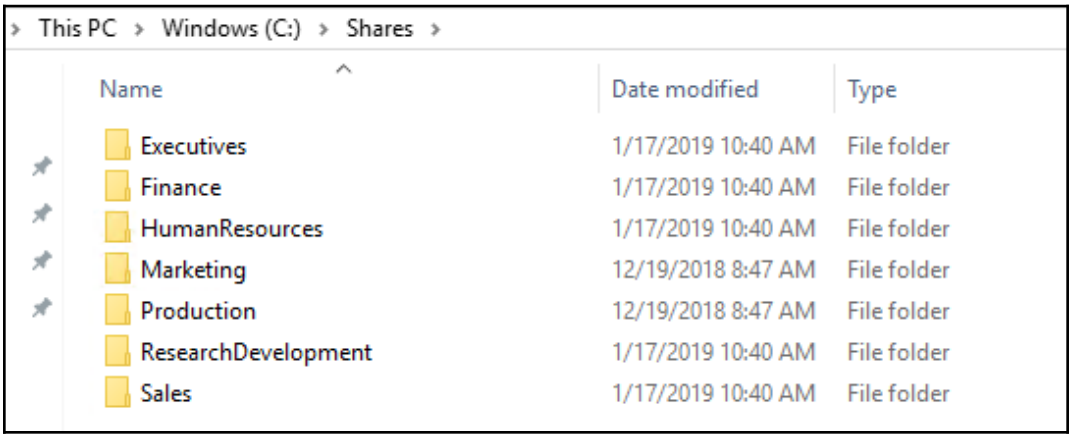
We're planning a big merger to create a new product. The code name for the product is "Identity Director".

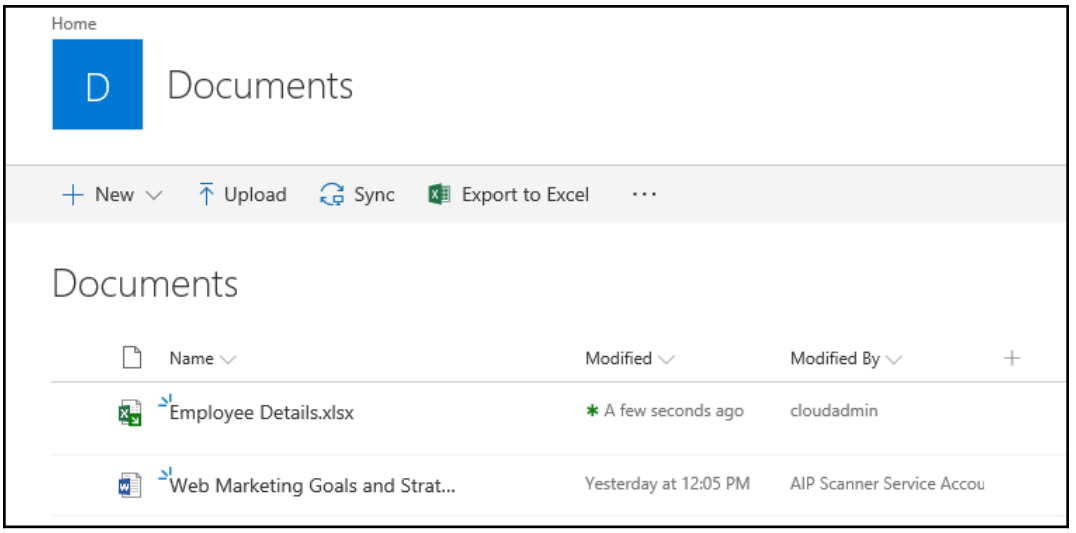
It will be a revolution and a new market-leading product in the field of Identity and Access Management in the cloud.

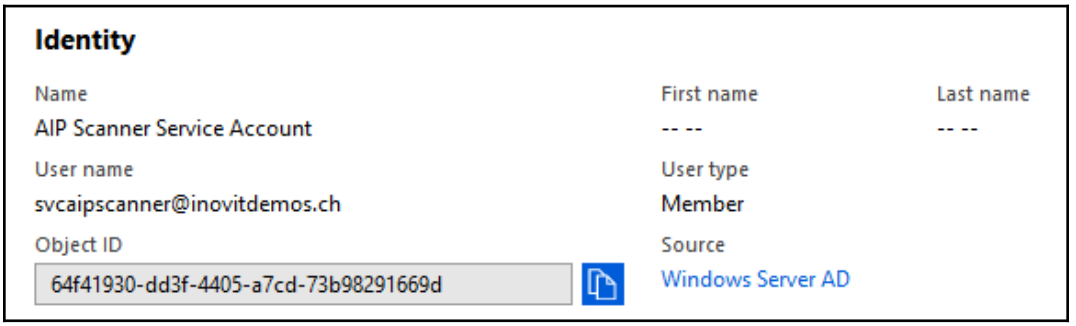
Regards,
Dan Jump
CEO

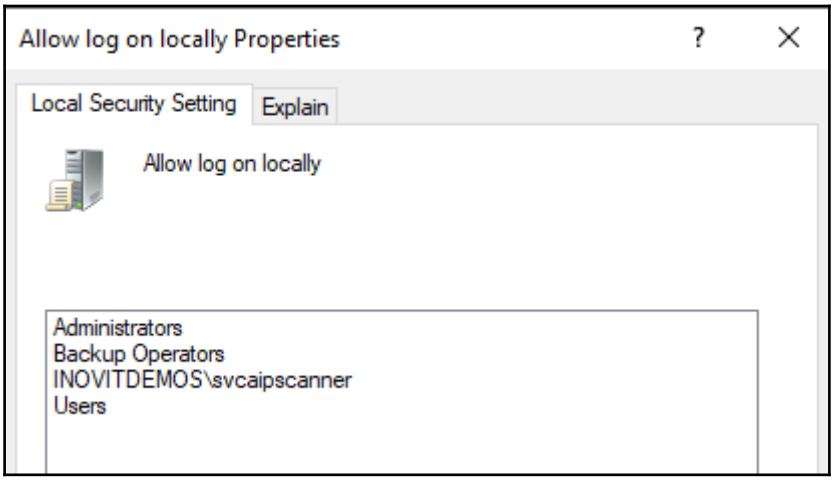

Undeliverable: Product Information
Microsoft Outlook
Sent Fri 1/18/2019 7:04 PM
To Dan Jump
Office 365
Your message to jochen.nickel@inovit.ch couldn't be delivered.
A custom mail flow rule created by an admin at 181031inovitdemos.onmicrosoft.com has blocked your message.
Internal Protected Message
Dan.Jump
Sender
Office 365
inovit.ch
Action Required
Blocked by mail flow rule

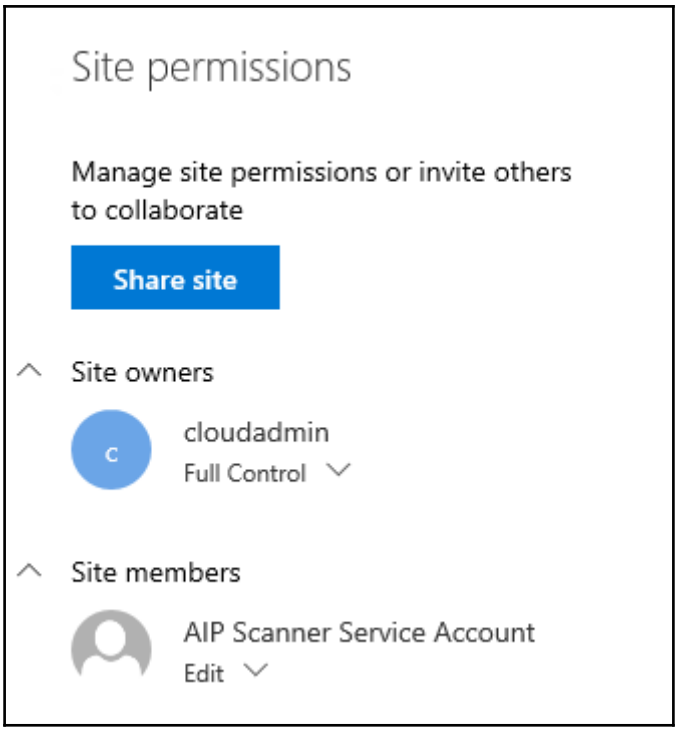

Microsoft Cloud Services
Azure Active Directory
Azure Information Protection
Rights Management Services
File Server
Azure Information
Protection Scanner
SharePoint Server
Microsoft On-Premises Services

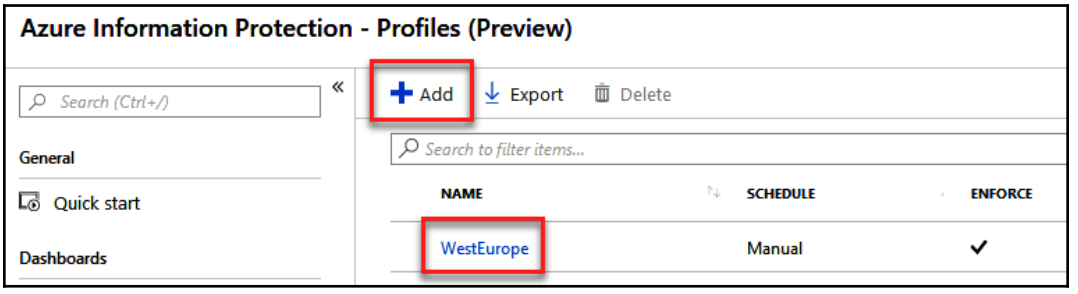

This PC › Windows (C:) › Shares ›
Name
Date modified
Type
Executives 1/17/2019 10:40 AM File folder
Finance 1/17/2019 10:40 AM File folder
HumanResources 1/17/2019 10:40 AM File folder
Marketing 12/19/2018 8:47 AM File folder
Production 12/19/2018 8:47 AM File folder
ResearchDevelopment 1/17/2019 10:40 AM File folder
Sales 1/17/2019 10:40 AM File folder


Home
D
Documents
New
Upload
Sync
Export to Excel
Documents
Name
Modified
Modified By
Employee Details.xlsx
A few seconds ago
cloudadmin
Web Marketing Goals and Strat...
Yesterday at 12:05 PM
AIP Scanner Service Accou

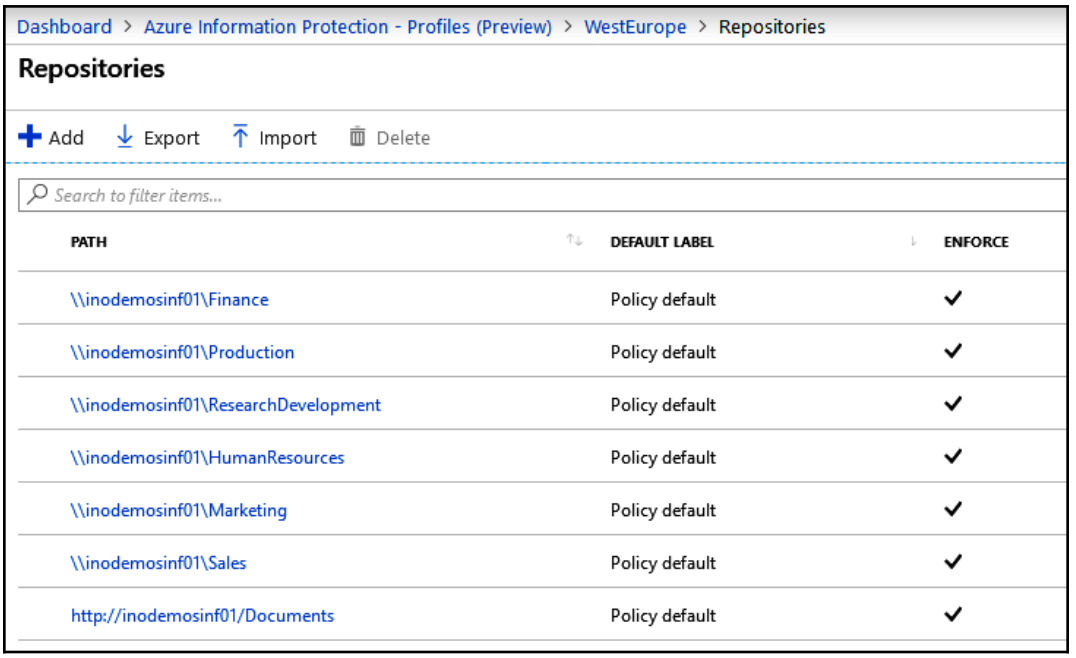

Identity
Name
AIP Scanner Service Account
First name
-- --
Last name
-- --
User name
svcaipscanner@inovitdemos.ch
User type
Member
Object ID
64f41930-dd3f-4405-a7cd-73b98291669d
Source
Windows Server AD

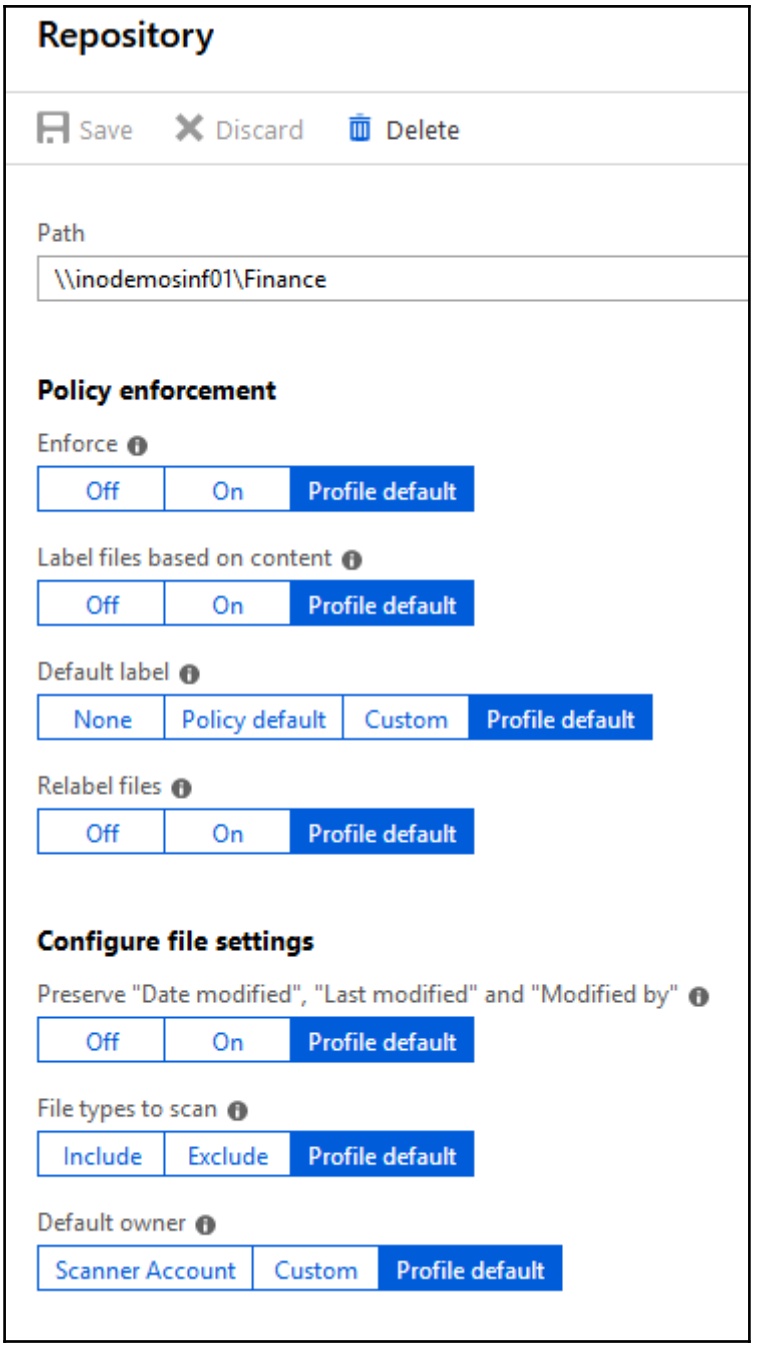

Allow log on locally Properties
Local Security Setting
Explain
Allow log on locally
Administrators
Backup Operators
INOVITDEMOS\svcaipscanner
Users

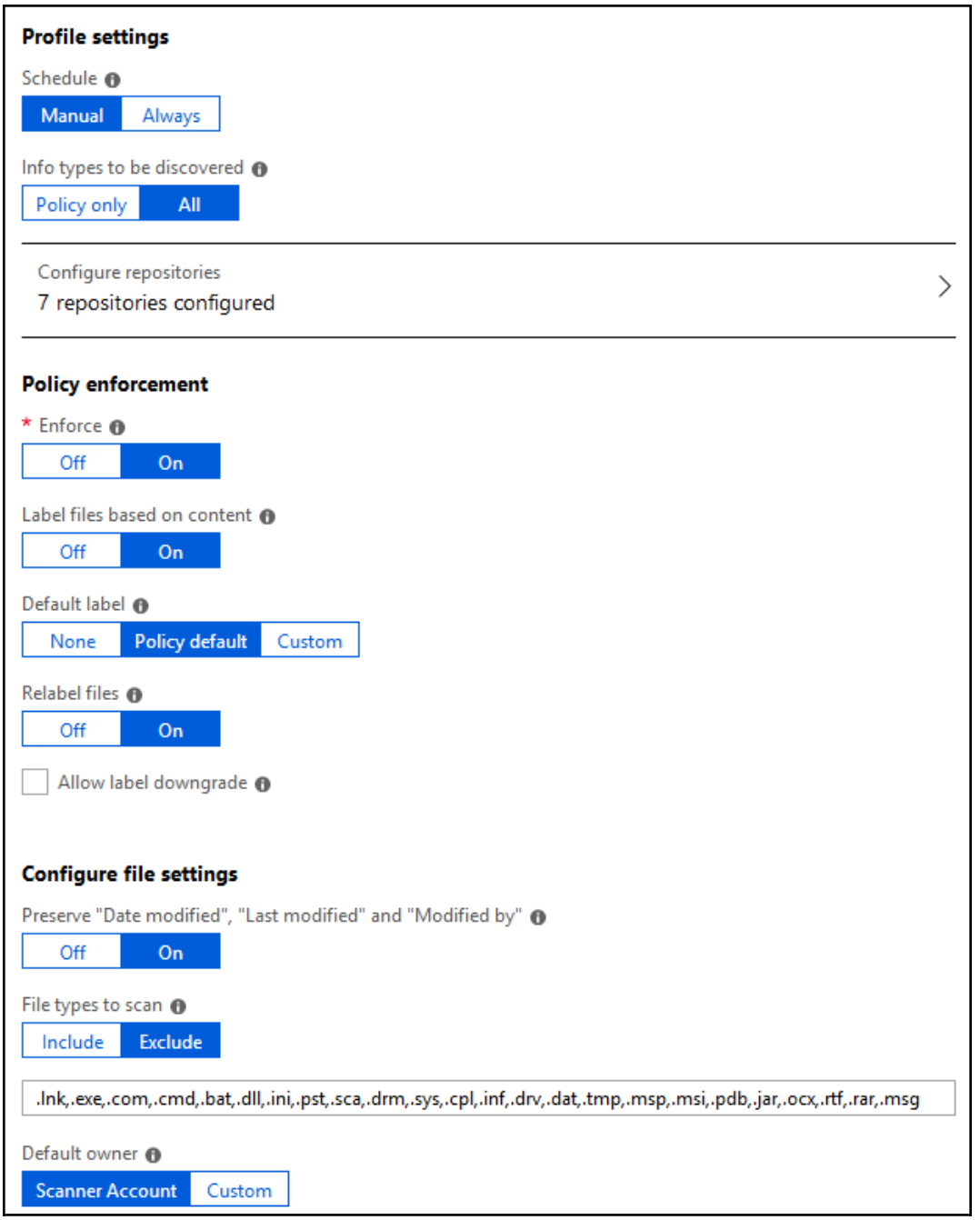

Site permissions
Manage site permissions or invite others to collaborate
Share site
Site owners
c
cloudadmin
Full Control
Site members
AIP Scanner Service Account
Edit

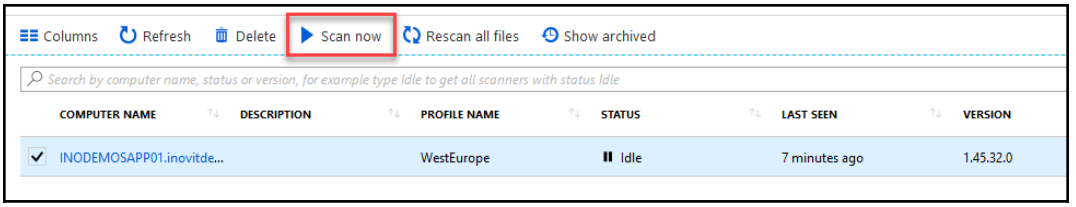

Azure Information Protection - Profiles (Preview)
Search (Ctrl+/)
General
Quick start
Dashboards
Add
Export
Delete
Search to filter items...
NAME
SCHEDULE
ENFORCE
WestEurope
Manual


INODEMOSAPP01 (SQL Server 14.0.2002.14 - INOVITDEMOS\cloudadmin)
Databases
System Databases
Database Snapshots
AIPScanner_WestEurope


Dashboard > Azure Information Protection - Profiles (Preview) > WestEurope > Repositories
Repositories
Add
Export
Import
Delete
Search to filter items...
PATH
DEFAULT LABEL
ENFORCE
\\inodemosinf01\Finance
Policy default
\\inodemosinf01\Production
Policy default
\\inodemosinf01\ResearchDevelopment
Policy default
\\inodemosinf01\HumanResources
Policy default
\\inodemosinf01\Marketing
Policy default
\\inodemosinf01\Sales
Policy default
http://inodemosinf01/Documents
Policy default

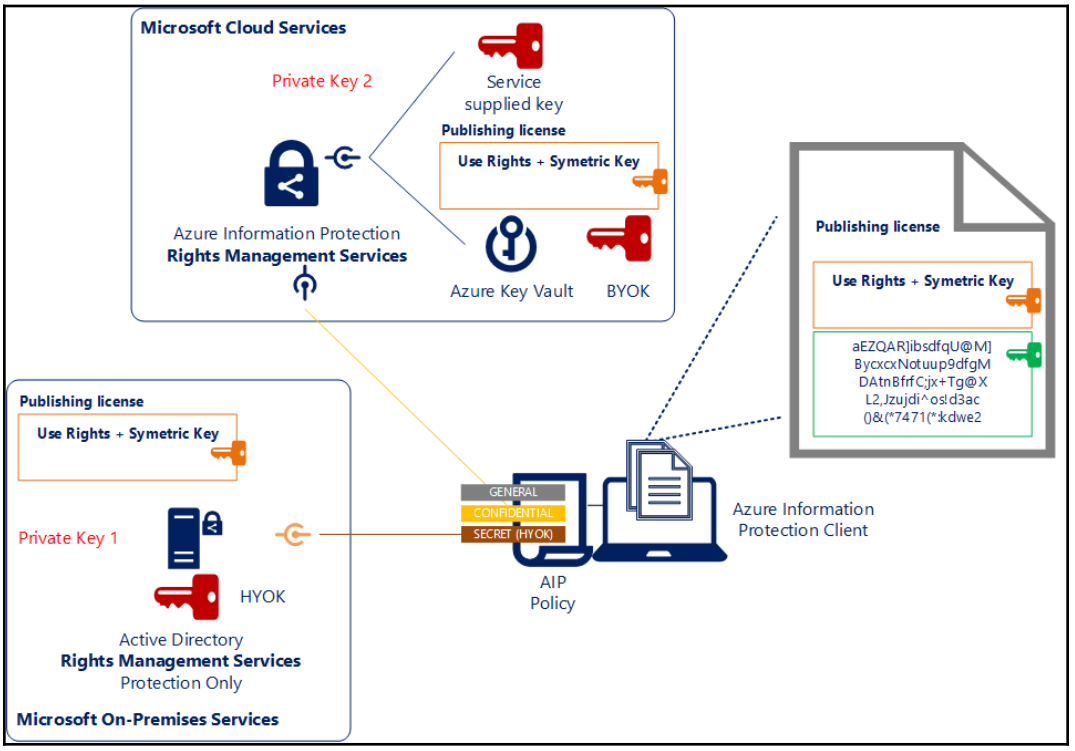

Repository
Save
Discard
Delete
Path
\\inodemosinf01\Finance
Policy enforcement
Enforce
Off
On
Profile default
Label files based on content
Off
On
Profile default
Default label
None
Policy default
Custom
Profile default
Relabel files
Off
On
Profile default
Configure file settings
Preserve "Date modified", "Last modified" and "Modified by"
Off
On
Profile default
File types to scan
Include
Exclude
Profile default
Default owner
Scanner Account
Custom
Profile default

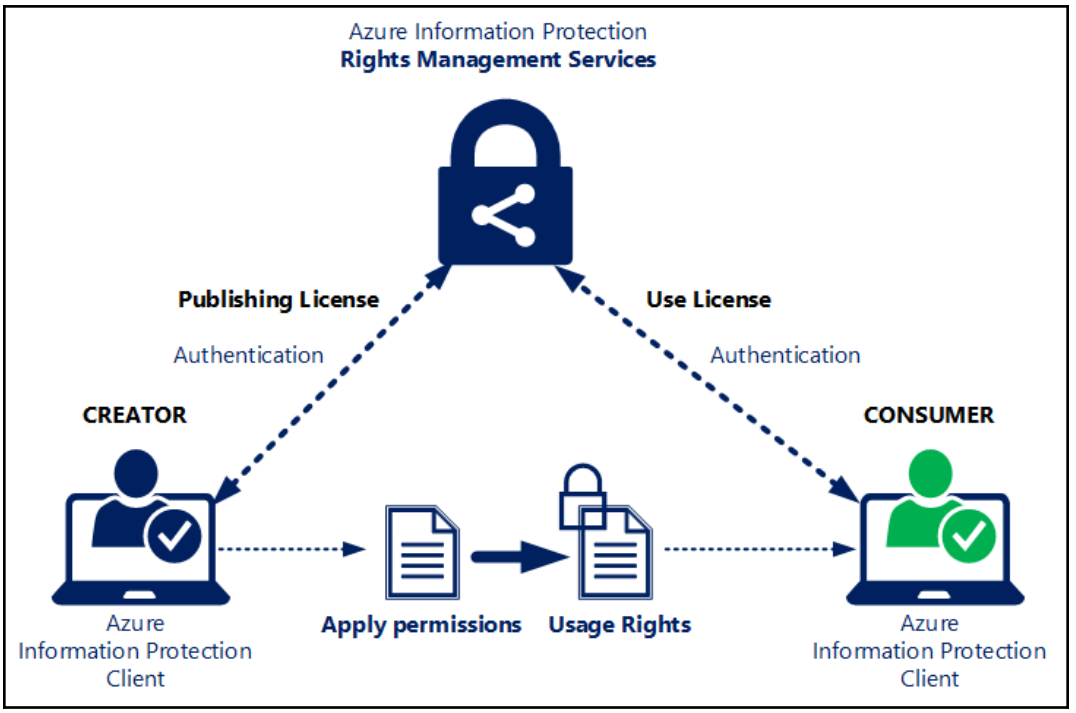

Profile settings
Schedule
Manual
Always
Info types to be discovered
Policy only
All
Configure repositories
7 repositories configured
Policy enforcement
* Enforce
Off
On
Label files based on content
Off
On
Default label
None
Policy default
Custom
Relabel files
Off
On
Allow label downgrade
Configure file settings
Preserve "Date modified", "Last modified" and "Modified by"
Off
On
File types to scan
Include
Exclude
.lnk,.exe,.com,.cmd,.bat,.dll,.ini,.pst,.sca,.drm,.sys,.cpl,.inf,.drv,.dat,.tmp,.msp,.msi,.pdb,.jar,.ocx,.rtf,.rar,.msg
Default owner
Scanner Account
Custom

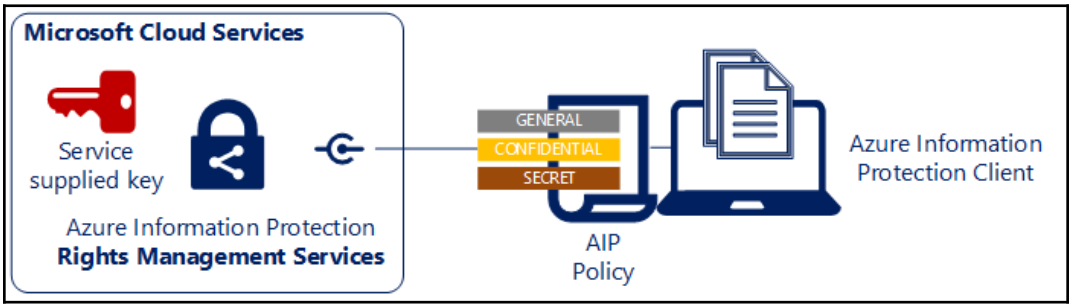


LOCATION TYPE	LOCATION	LABELED FILES	PROTECTED FILES	INFORMATION TYPES MATCHES
Endpoint	INODEMOSCLI02.INOVITDEMOS.CH	6	4	0
Endpoint	INODEMOSCLI01.INOVITDEMOS.CH	5	3	0
File repository	\\inodemosinf01\sales\	2	0	1
File repository	\\inodemosinf01\finance\	1	0	0
File repository	http://inodemosinf01/documents/	1	0	0
File repository	\\inodemosinf01\humanresources\	1	0	1
File repository	\\inodemosinf01\researchdevelopment\	1	0	1

Chapter 14: Understanding Encryption Key Management Strategies

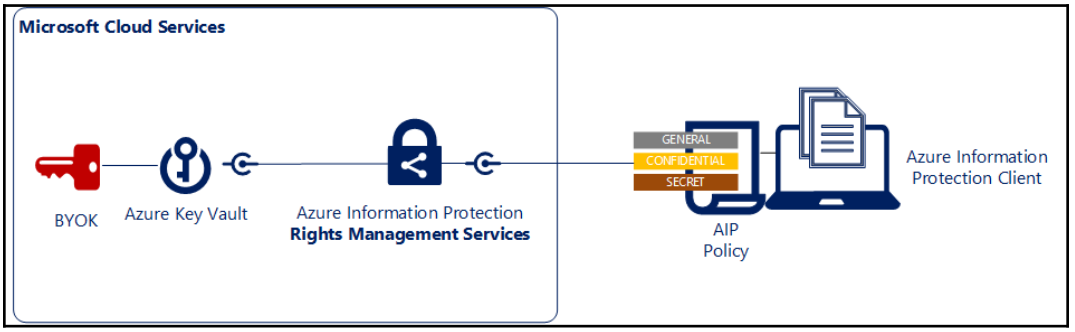


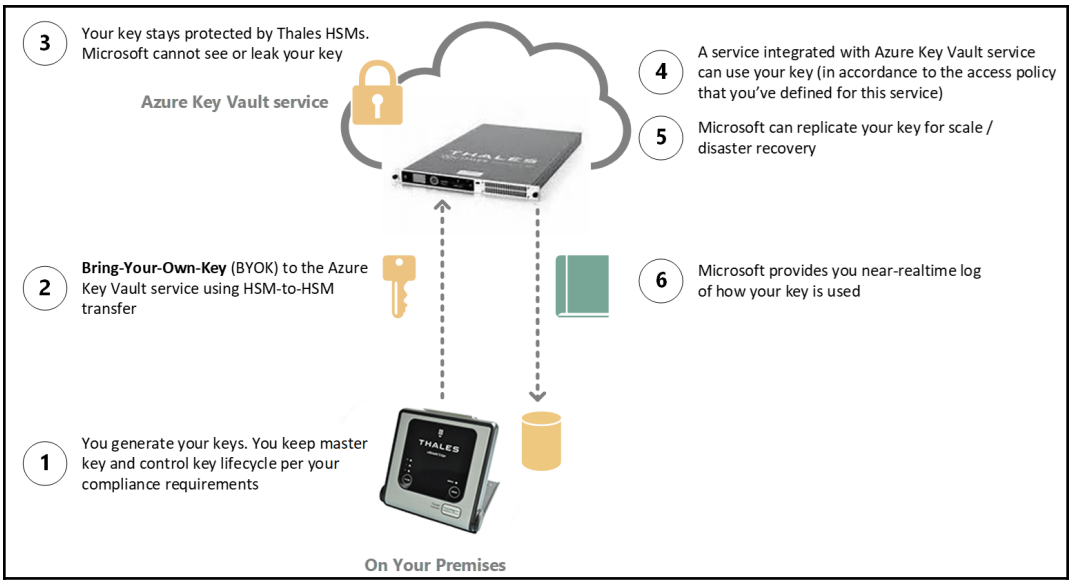

Azure Information Protection
Rights Management Services
Publishing License
Authentication
Use License
Authentication
CREATOR
CONSUMER
Azure
Information Protection
Client
Apply permissions
Usage Rights
Azure
Information Protection
Client

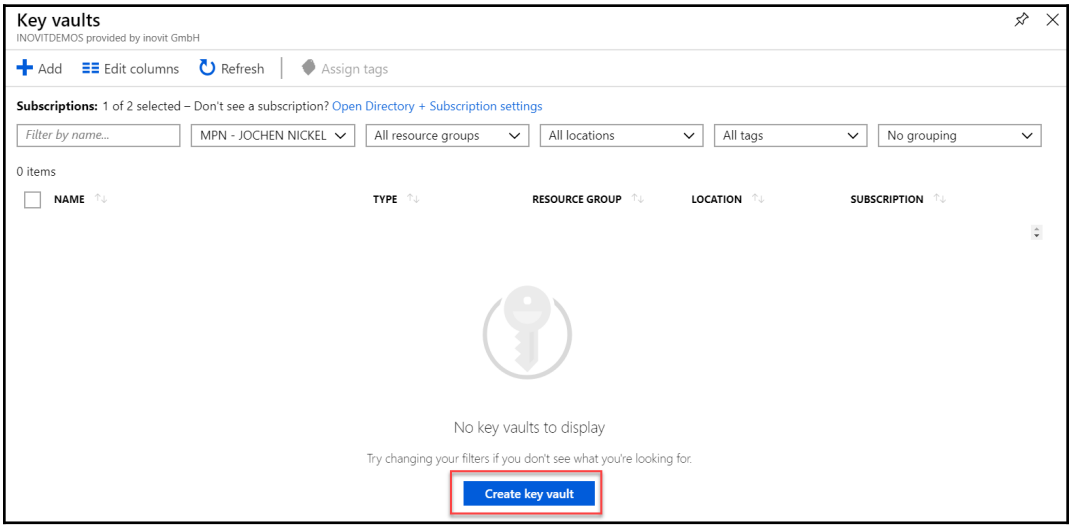

Microsoft Cloud Services
Service
supplied key
Azure Information Protection
Rights Management Services
GENERAL
CONFIDENTIAL
SECRET
AIP
Policy
Azure Information
Protection Client

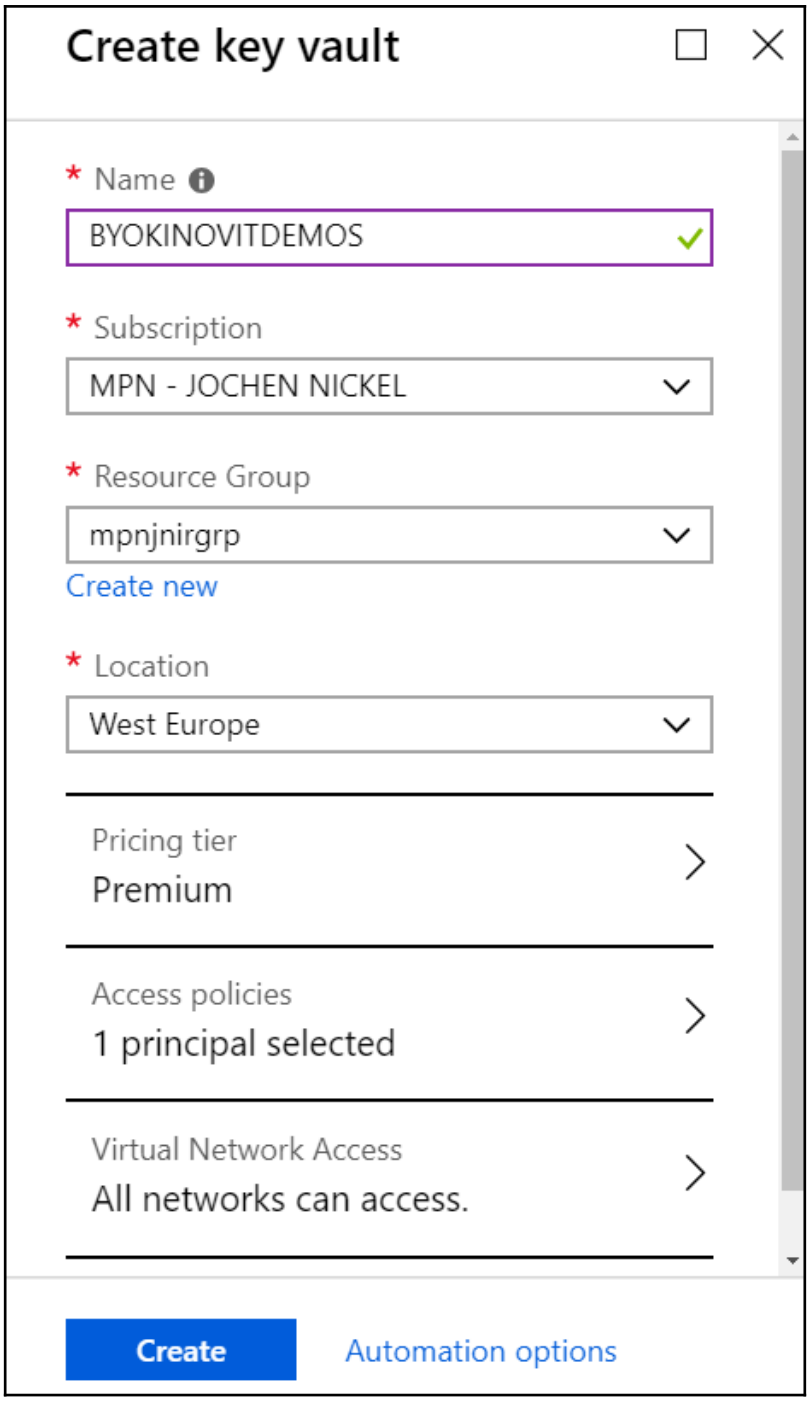
```
PS C:\WINDOWS\system32> Get-AadrmKeys


KeyIdentifier   : a4fd8a9b-e573-48fb-afda-814f8ed31aec
CreationTime    : 10/31/2018 2:51:23 PM
Status          : Active
KeyType         : Microsoft-managed
FriendlyName    : INOVITDEMOS by inovit GmbH
PublicKey       :
KeyVaultKeyUrl  :
```

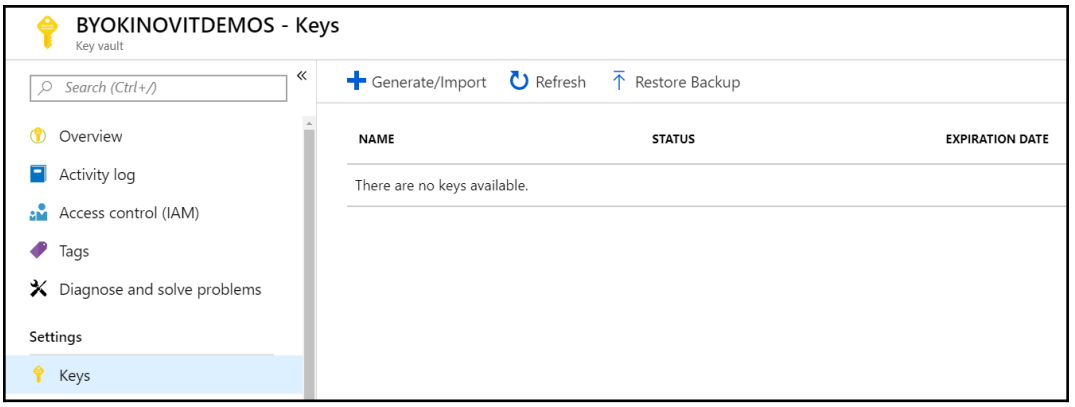
```
PS C:\WINDOWS\system32> Get-AadrmConfiguration


BPOSId                                  : 7709ca2b-3be8-4d92-89d7-dc1e274b4d0e
RightsManagementServiceId               : 94ce956b-a527-4b88-9266-3901f927b033
LicensingIntranetDistributionPointUrl   : https://94ce956b-a527-4b88-9266-3901f927b033.rms.eu.aadrm.com/_wmcs/licensing
LicensingExtranetDistributionPointUrl   : https://94ce956b-a527-4b88-9266-3901f927b033.rms.eu.aadrm.com/_wmcs/licensing
CertificationIntranetDistributionPointUrl : https://94ce956b-a527-4b88-9266-3901f927b033.rms.eu.aadrm.com/_wmcs/certification
CertificationExtranetDistributionPointUrl : https://94ce956b-a527-4b88-9266-3901f927b033.rms.eu.aadrm.com/_wmcs/certification
AdminConnectionUrl                      : https://admin.eu.aadrm.com/admin/admin.svc/Tenants/94ce956b-a527-4b88-9266-3901f927b033
AdminV2ConnectionUrl                    : https://admin.eu.aadrm.com/adminV2/admin.svc/Tenants/94ce956b-a527-4b88-9266-3901f927b033
OnPremiseDomainName                     :
Keys                                    : {a4fd8a9b-e573-48fb-afda-814f8ed31aec}
CurrentLicensorCertificateGuid          : a4fd8a9b-e573-48fb-afda-814f8ed31aec
Templates                               : {026be843-becf-425f-a776-27d4c1b8fd54, 68ab2d70-f65e-4b83-b3fb-8ed3e7f06ee7}
FunctionalState                         : Enabled
SuperUsersEnabled                       : Disabled
SuperUsers                              : {}
AdminRoleMembers                        : {}
KeyRolloverCount                        : 0
ProvisioningDate                        : 10/31/2018 2:51:23 PM
IPCv3ServiceFunctionalState             : Enabled
DevicePlatformState                     : {Windows -> True, WindowsStore -> True, WindowsPhone -> True, Mac -> True...}
FciEnabledForConnectorAuthorization     : True
DocumentTrackingFeatureState            : Enabled
```

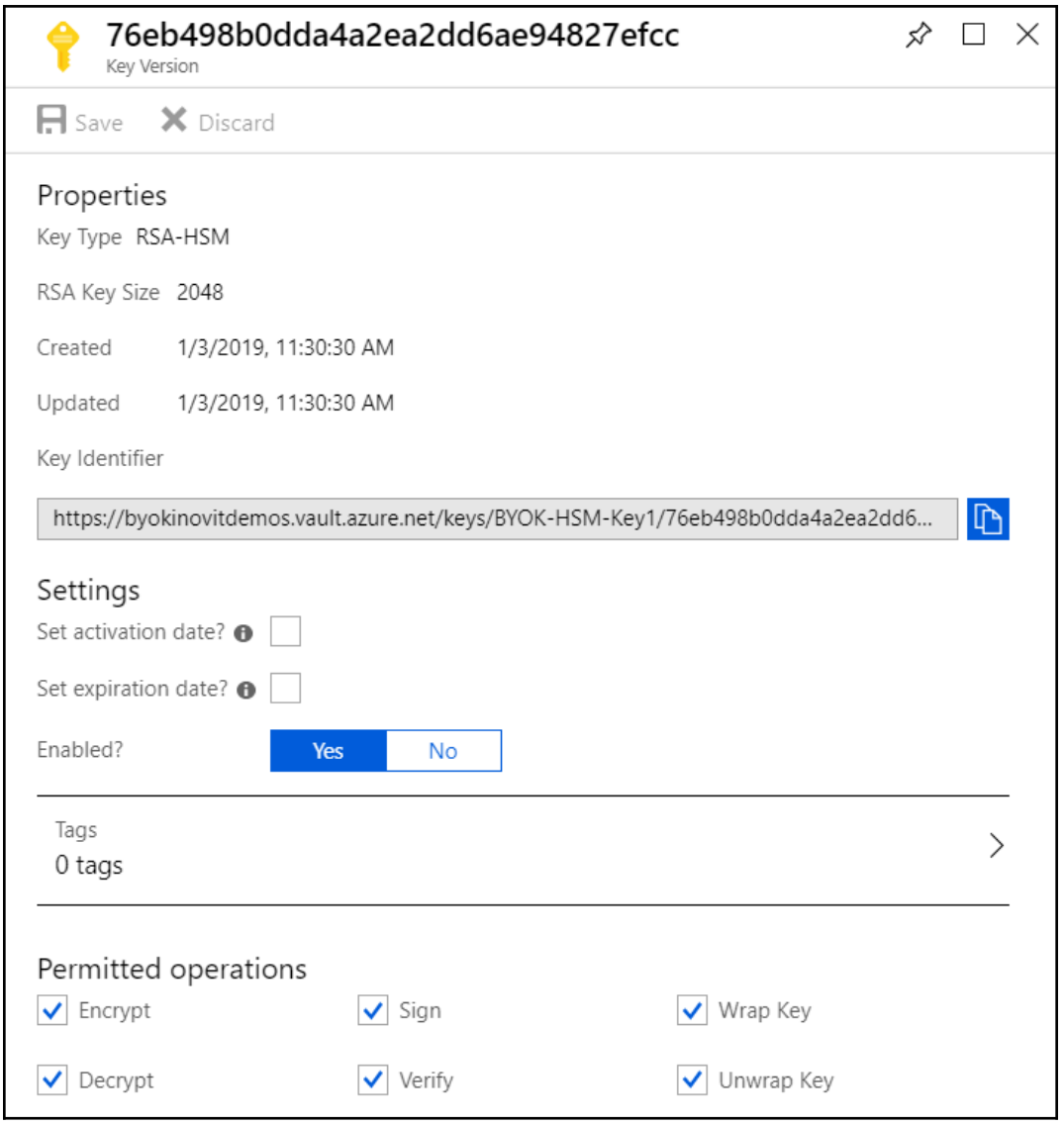


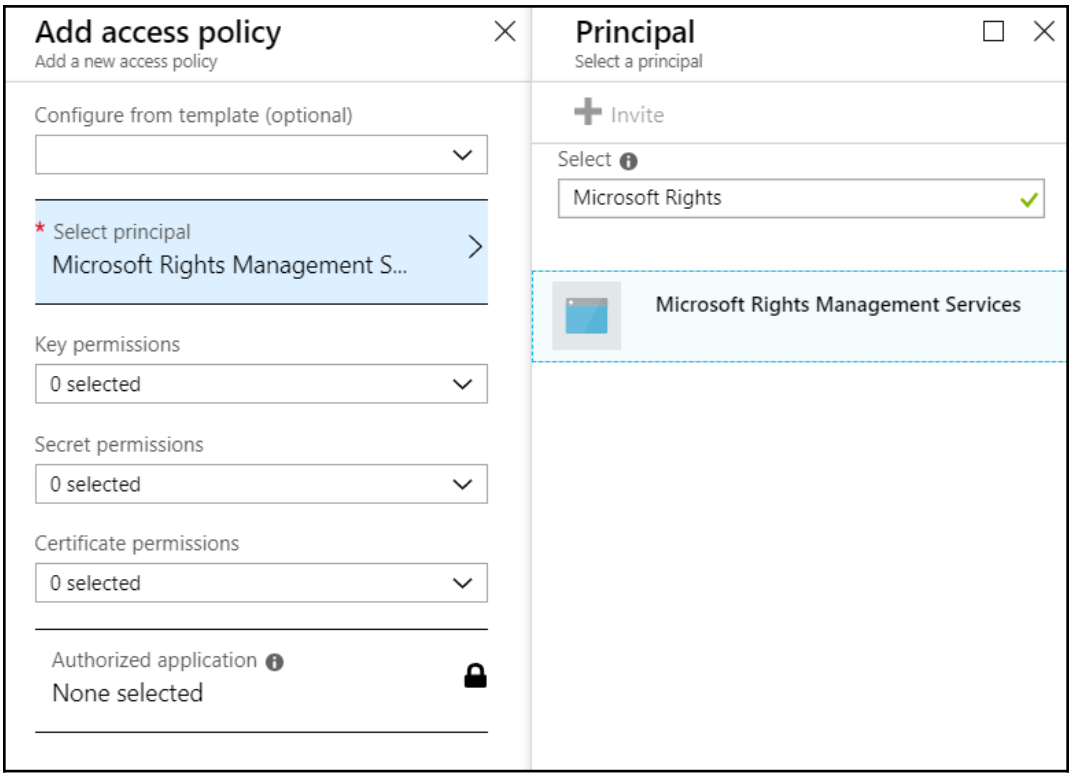

3
Your key stays protected by Thales HSMs. Microsoft cannot see or leak your key
Azure Key Vault service
4
A service integrated with Azure Key Vault service can use your key (in accordance to the access policy that you've defined for this service)
5
Microsoft can replicate your key for scale / disaster recovery
2
Bring-Your-Own-Key (BYOK) to the Azure Key Vault service using HSM-to-HSM transfer
6
Microsoft provides you near-realtime log of how your key is used
1
You generate your keys. You keep master key and control key lifecycle per your compliance requirements
On Your Premises

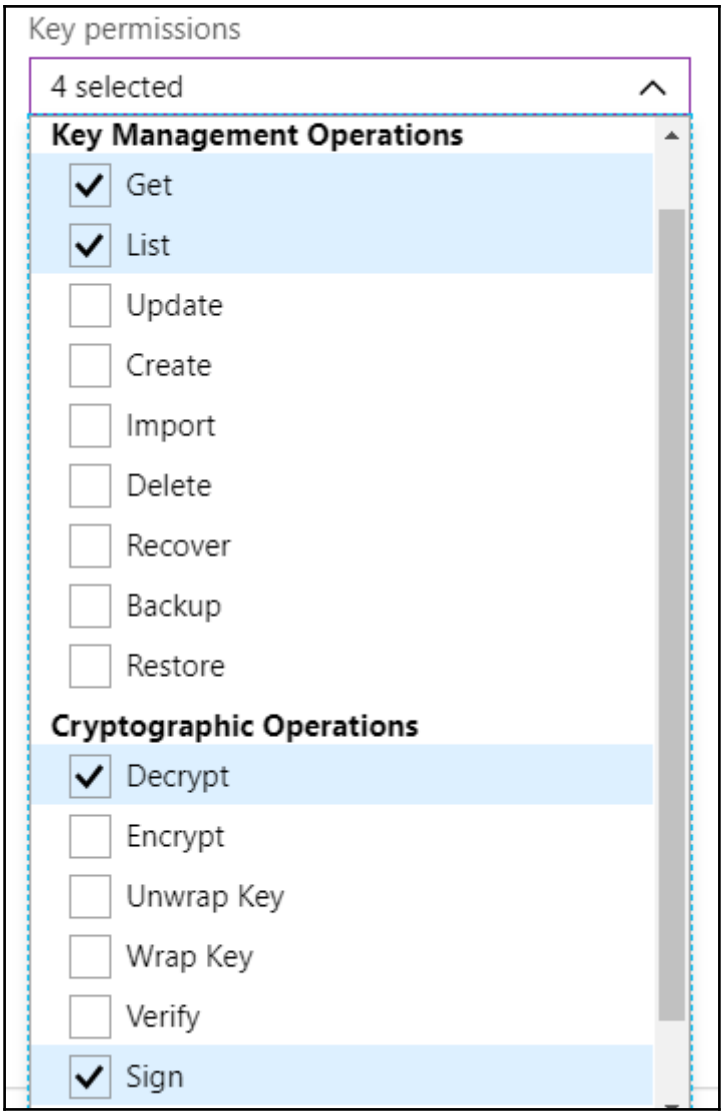

Key vaults
INOVITDEMOS provided by inovit GmbH
Add
Edit columns
Refresh
Assign tags
Subscriptions: 1 of 2 selected – Don't see a subscription? Open Directory + Subscription settings
Filter by name...
MPN - JOCHEN NICKEL
All resource groups
All locations
All tags
No grouping
0 items
NAME
TYPE
RESOURCE GROUP
LOCATION
SUBSCRIPTION
No key vaults to display
Try changing your filters if you don't see what you're looking for.
Create key vault

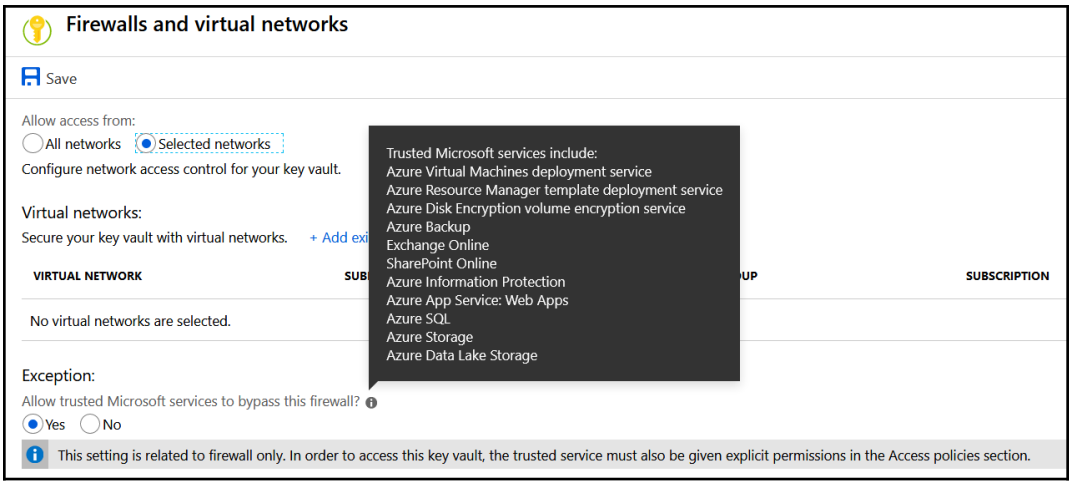

Create key vault
* Name
BYOKINOVITDEMOS
* Subscription
MPN - JOCHEN NICKEL
* Resource Group
mpnjnirgrp
Create new
* Location
West Europe
Pricing tier
Premium
Access policies
1 principal selected
Virtual Network Access
All networks can access.
Create
Automation options


BYOKINOVITDEMOS - Keys
Key vault
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Keys
Generate/Import
Refresh
Restore Backup
NAME
STATUS
EXPIRATION DATE
There are no keys available.


76eb498b0dda4a2ea2dd6ae94827efcc
Key Version
Save
Discard
Properties
Key Type RSA-HSM
RSA Key Size 2048
Created 1/3/2019, 11:30:30 AM
Updated 1/3/2019, 11:30:30 AM
Key Identifier
https://byokinovitdemos.vault.azure.net/keys/BYOK-HSM-Key1/76eb498b0dda4a2ea2dd6...
Settings
Set activation date?
Set expiration date?
Enabled?
Yes
No
Tags
0 tags
Permitted operations
Encrypt
Sign
Wrap Key
Decrypt
Verify
Unwrap Key


Add access policy
Add a new access policy
Configure from template (optional)
* Select principal
Microsoft Rights Management S...
Key permissions
0 selected
Secret permissions
0 selected
Certificate permissions
0 selected
Authorized application
None selected
Principal
Select a principal
Invite
Select
Microsoft Rights
Microsoft Rights Management Services

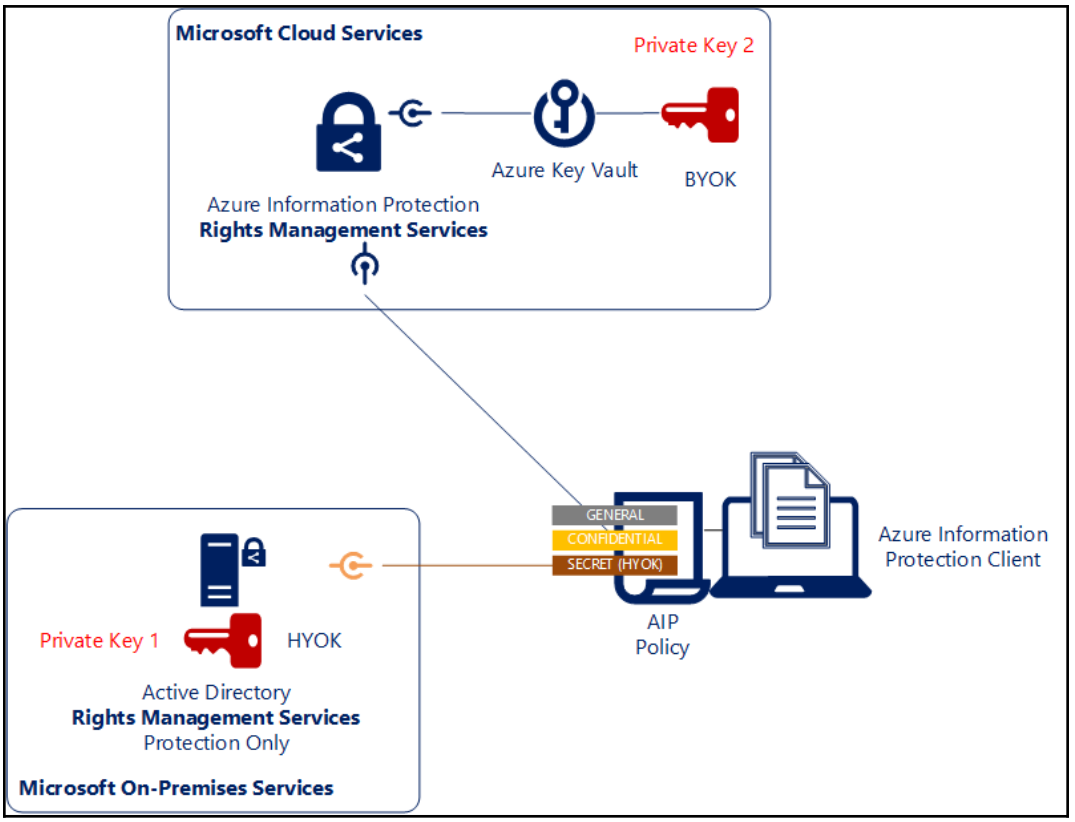

Key permissions
4 selected
Key Management Operations
Get
List
Update
Create
Import
Delete
Recover
Backup
Restore
Cryptographic Operations
Decrypt
Encrypt
Unwrap Key
Wrap Key
Verify
Sign

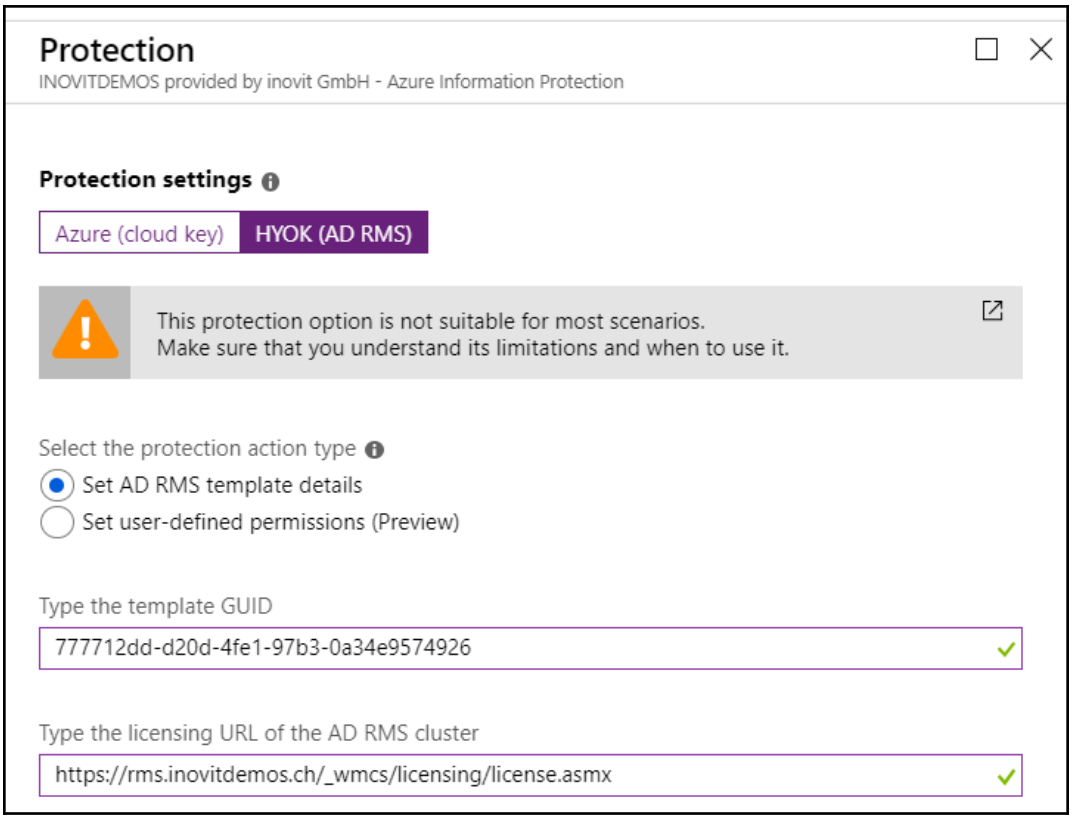


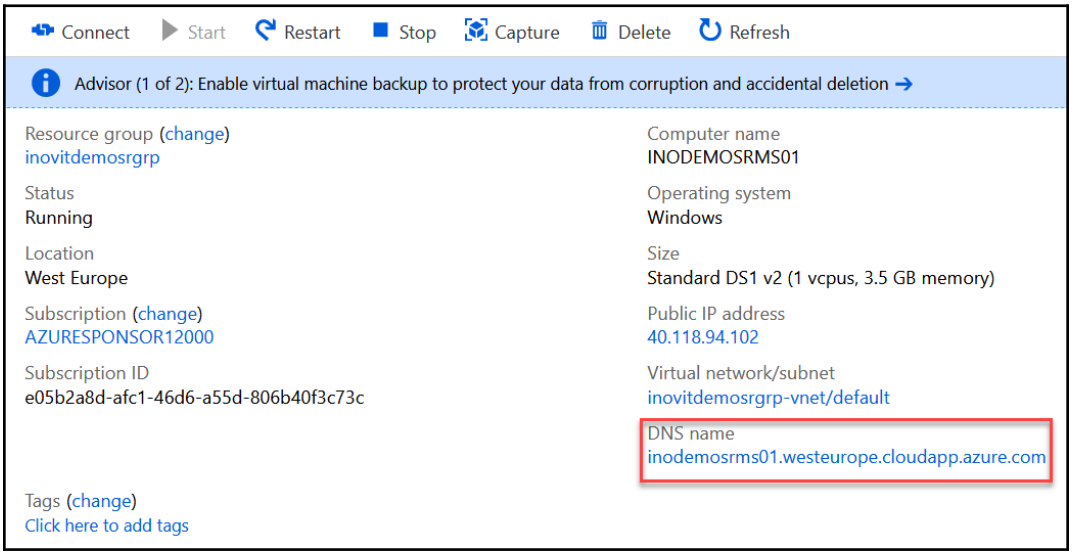

```
PS C:\WINDOWS\system32> Use-AadrmKeyVaultKey -KeyVaultKeyUrl "https://byokinovitdemos.vault.azure.net/keys/BYOK-HSM-Key1/76eb498b0dda4a2ea2dd6ae94827efcc" -FriendlyName
tBYOKKey -Verbose
WARNING: This operation tells the Rights Management service to use the specified key in Key Vault.

Confirm
Are you sure you want to perform this action?
Performing the operation "Use-AadrmKeyVaultKey" on target "current organization".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y
The Rights Management service successfully added the key.
```

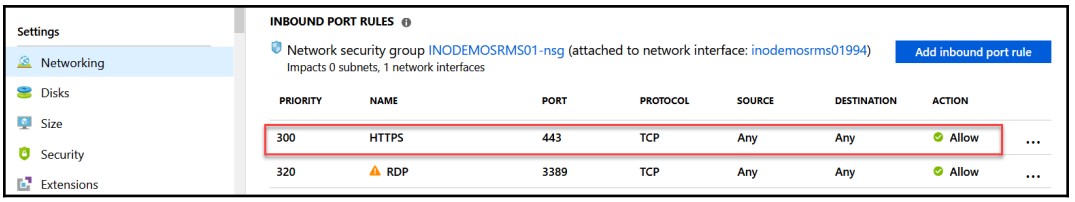
```
PS C:\WINDOWS\system32> Set-AadrmKeyProperties -KeyIdentifier a9cfc5ea-00e4-4749-b768-625d421bf9a2 -Active $true
WARNING: This operation sets the selected key as the active key, and archives the currently active key.

Confirm
Are you sure you want to perform this action?
Performing the operation "Set-AadrmKeyProperties" on target "current organization".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): Y
The Rights Management service successfully added the key.
```

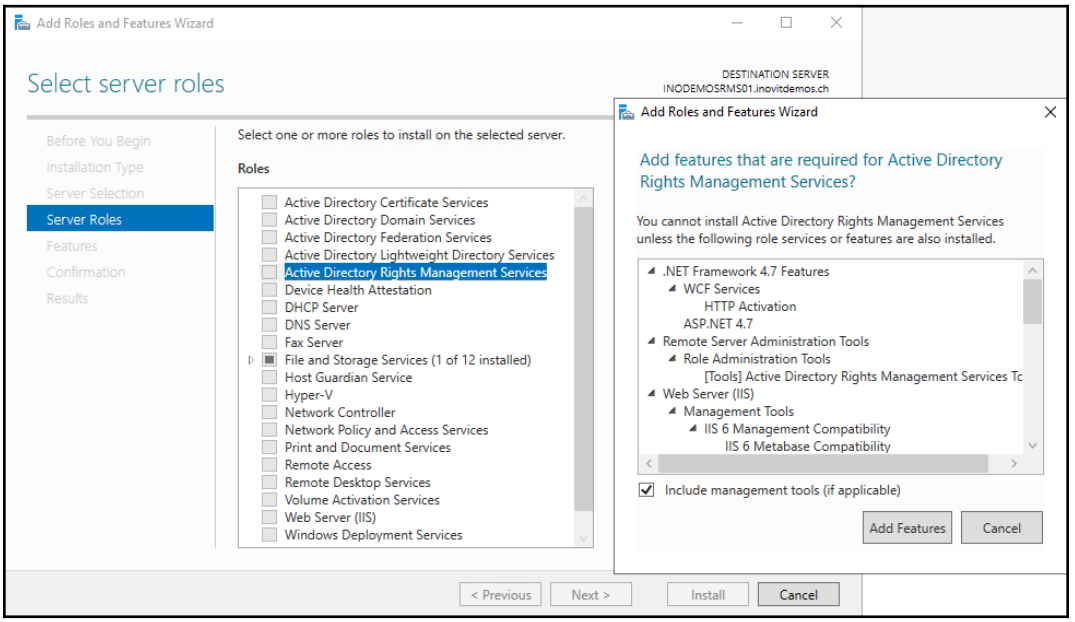
```
PS C:\WINDOWS\system32> Get-AadrmKeys


KeyIdentifier  : a4fd8a9b-e573-48fb-afda-814f8ed31aec
CreationTime   : 10/31/2018 2:51:23 PM
Status         : Archived
KeyType        : Microsoft-managed
FriendlyName   : INOVITDEMOS by inovit GmbH
PublicKey      :
KeyVaultKeyUrl :

KeyIdentifier  : a9cfc5ea-00e4-4749-b768-625d421bf9a2
CreationTime   : 1/3/2019 10:30:58 AM
Status         : Active
KeyType        : Customer-managed (BYOK)
FriendlyName   : FirstBYOKKey
PublicKey      : {"n":"tFFz0ml2e2GSzbQfvOttKXyeZ1ucNu4F5iJQuXd9B_3fN-mXtgt7S39MXSRC_x2lncgTVGXVjZ11Mv3g5yJ-Y7onanCdsogiV3ZoA-fPt1bT-wT8mVZ8F9rAgl6COHCxHlQWhfTX0sa7m47i0B2G
                 si2oYZ39W4QMaIPRv9Gx3hCM6pcrg0W0XEpSt_SVo-oEbw_8ooAWkBkqBFbNc7AvpfNQHcMMkqJ5342AS0UcUz2sfxl0pO5Aiq5MzRICPXZ9ZHb36ZZgChCKOXjGqySONJUTuk1VdGSpqITYehrPVz8zclO
                 IFFhAr1DI1rrn5yqNenE7z0iJEhix8uE2rUgww", "e":"AQAB"}
KeyVaultKeyUrl : https://byokinovitdemos.vault.azure.net/keys/BYOK-HSM-Key1/76eb498b0dda4a2ea2dd6ae94827efcc
```

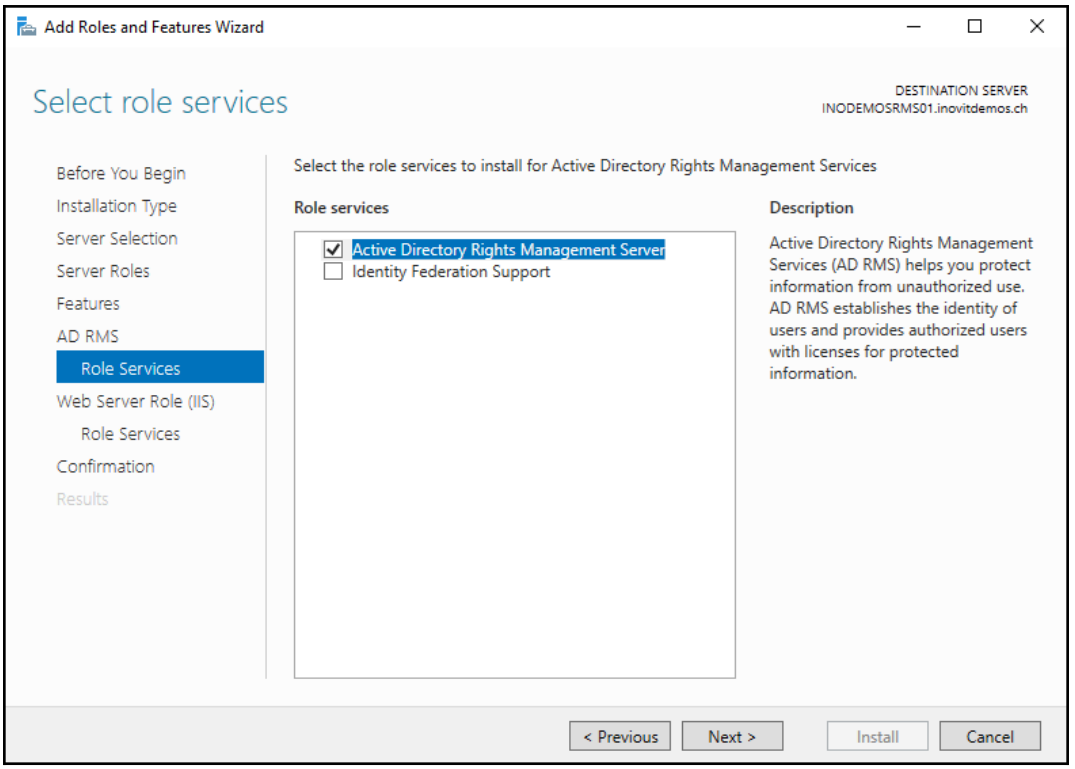

Microsoft Cloud Services
Private Key 2
Azure Key Vault
BYOK
Azure Information Protection
Rights Management Services
GENERAL
CONFIDENTIAL
SECRET (HYOK)
Azure Information
Protection Client
AIP
Policy
Private Key 1
HYOK
Active Directory
Rights Management Services
Protection Only
Microsoft On-Premises Services

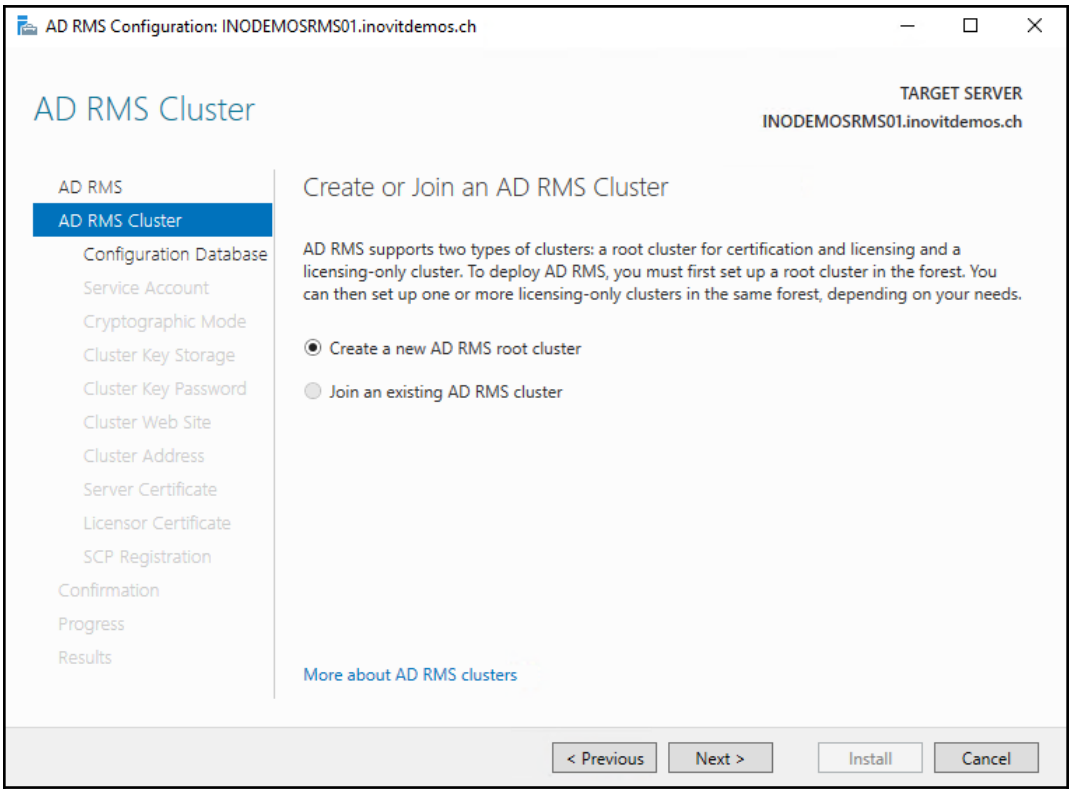

Protection
INOVITDEMOS provided by inovit GmbH - Azure Information Protection
Protection settings
Azure (cloud key)
HYOK (AD RMS)
This protection option is not suitable for most scenarios.
Make sure that you understand its limitations and when to use it.
Select the protection action type
Set AD RMS template details
Set user-defined permissions (Preview)
Type the template GUID
777712dd-d20d-4fe1-97b3-0a34e9574926
Type the licensing URL of the AD RMS cluster
https://rms.inovitdemos.ch/_wmcs/licensing/license.asmx

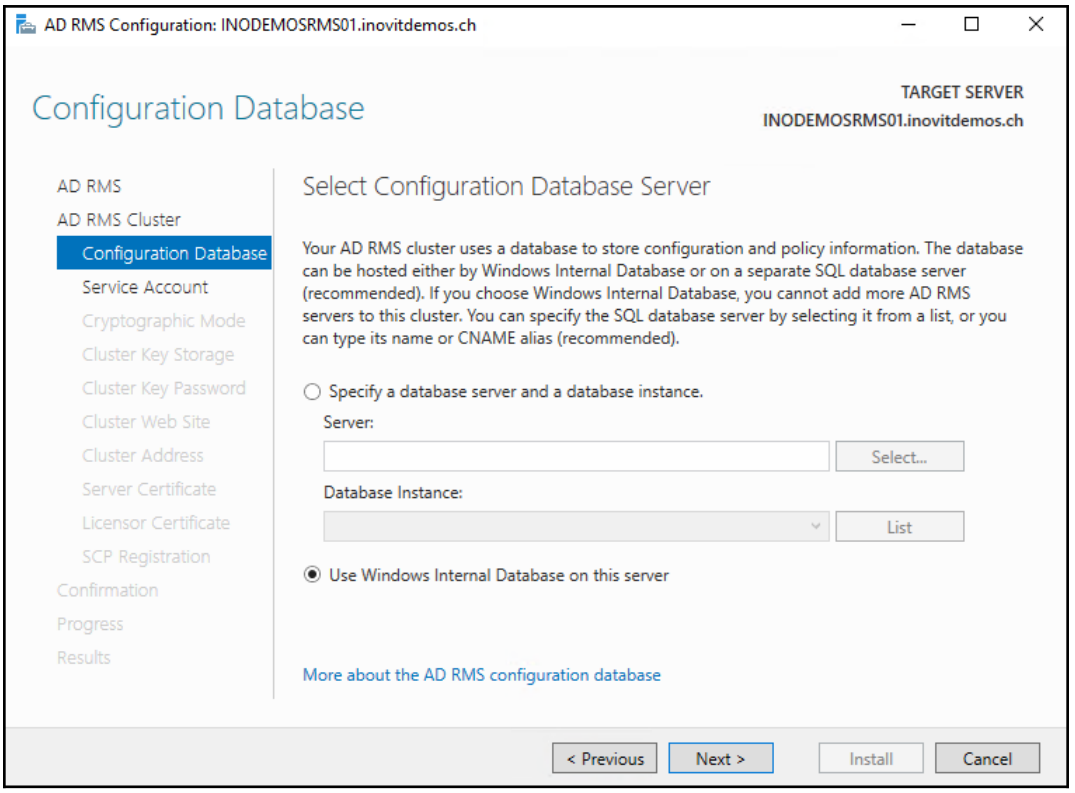

Connect
Start
Restart
Stop
Capture
Delete
Refresh
Advisor (1 of 2): Enable virtual machine backup to protect your data from corruption and accidental deletion
Resource group (change)
inovitdemosrgrp
Status
Running
Location
West Europe
Subscription (change)
AZURESPONSOR12000
Subscription ID
e05b2a8d-afc1-46d6-a55d-806b40f3c73c
Tags (change)
Click here to add tags
Computer name
INODEMOSRMS01
Operating system
Windows
Size
Standard DS1 v2 (1 vcpus, 3.5 GB memory)
Public IP address
40.118.94.102
Virtual network/subnet
inovitdemosrgrp-vnet/default
DNS name
inodemosrms01.westeurope.cloudapp.azure.com

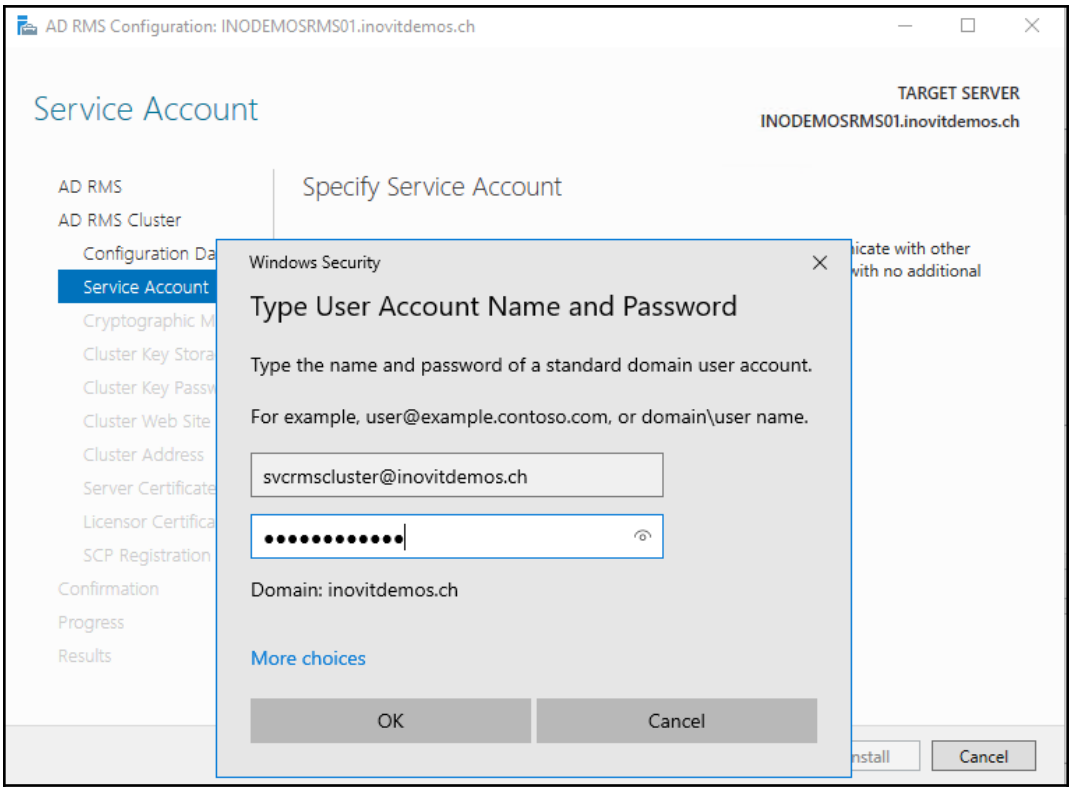

Settings
Networking
Disks
Size
Security
Extensions
INBOUND PORT RULES
Network security group INODEMOSRMS01-nsg (attached to network interface: inodemosrms01994)
Impacts 0 subnets, 1 network interfaces
Add inbound port rule
PRIORITY NAME PORT PROTOCOL SOURCE DESTINATION ACTION
300 HTTPS 443 TCP Any Any Allow
320 RDP 3389 TCP Any Any Allow

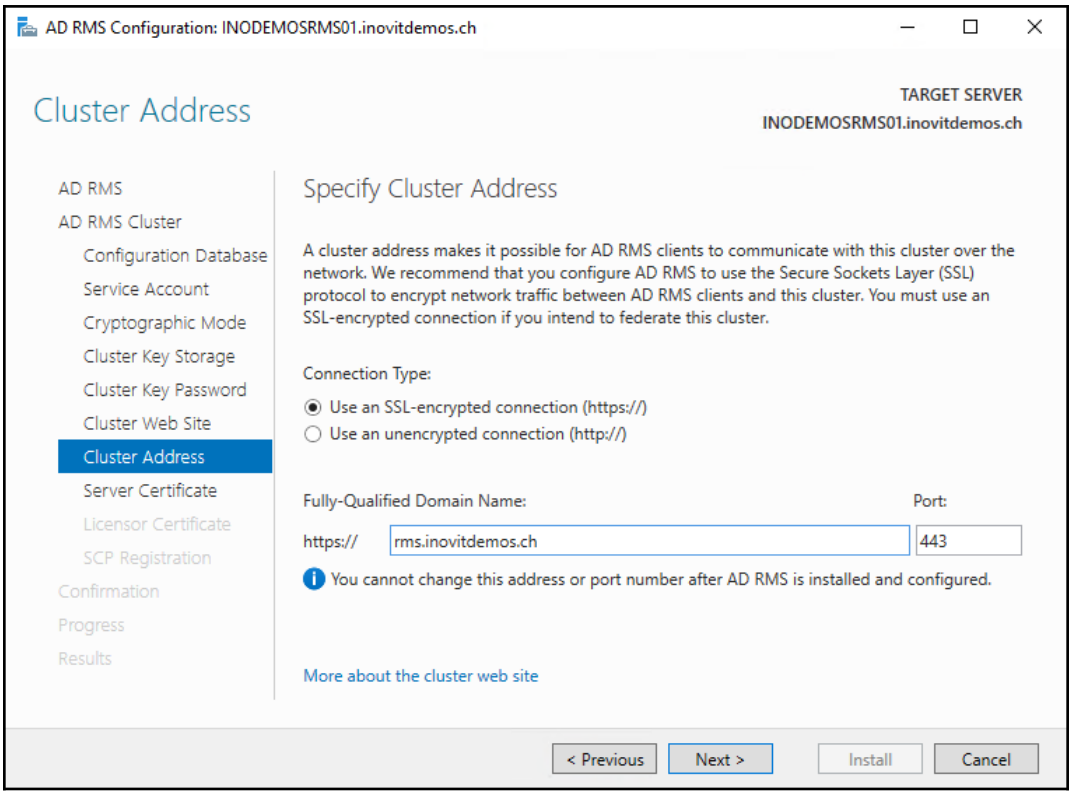

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
INODEMOSRMS01.inovitdemos.ch
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Controller
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
< Previous
Next >
Install
Cancel
Add Roles and Features Wizard
Add features that are required for Active Directory Rights Management Services?
You cannot install Active Directory Rights Management Services unless the following role services or features are also installed.
.NET Framework 4.7 Features
WCF Services
HTTP Activation
ASP.NET 4.7
Remote Server Administration Tools
Role Administration Tools
[Tools] Active Directory Rights Management Services Tc
Web Server (IIS)
Management Tools
IIS 6 Management Compatibility
IIS 6 Metabase Compatibility
Include management tools (if applicable)
Add Features
Cancel

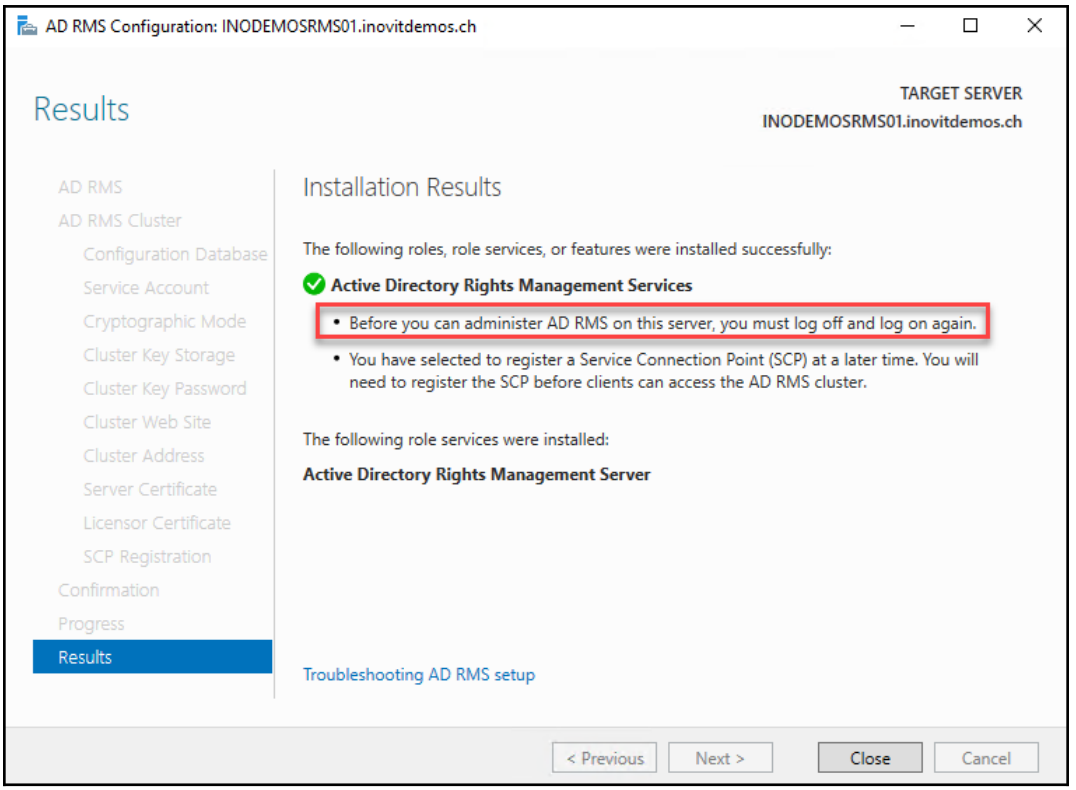

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
INODEMOSRMS01.inovitdemos.ch
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD RMS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Active Directory Rights Management Services
Role services
Active Directory Rights Management Server
Identity Federation Support
Description
Active Directory Rights Management Services (AD RMS) helps you protect information from unauthorized use. AD RMS establishes the identity of users and provides authorized users with licenses for protected information.
< Previous
Next >
Install
Cancel

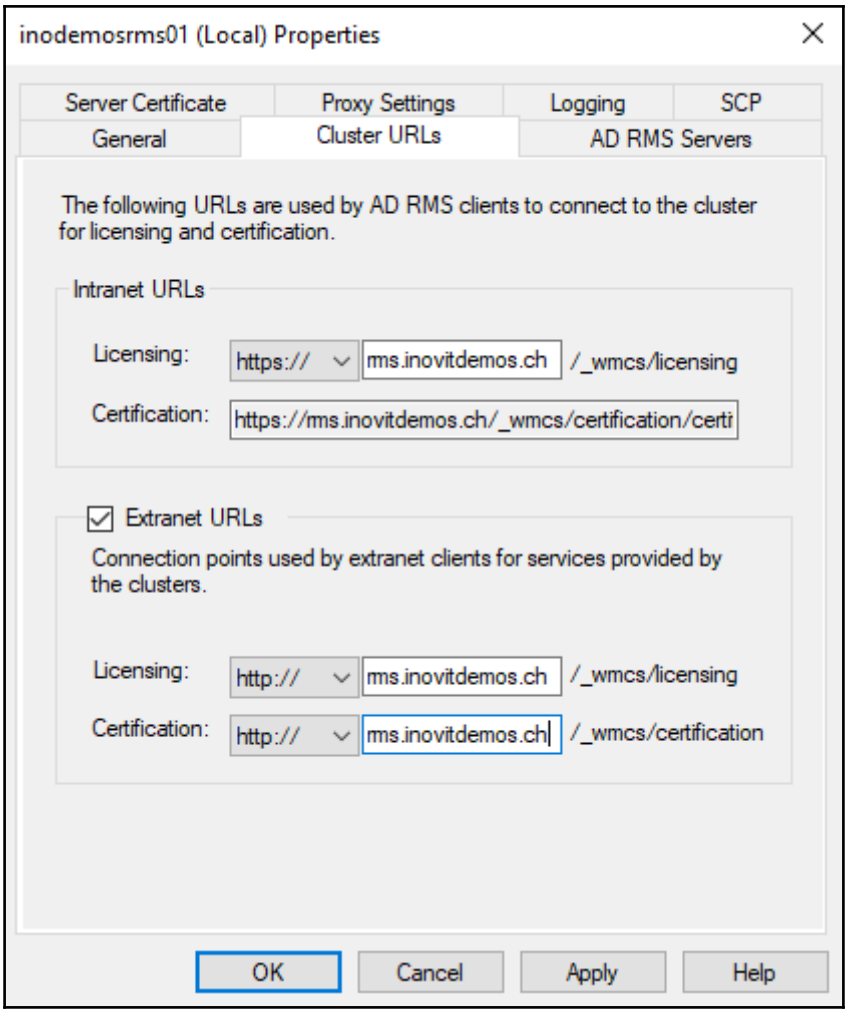

AD RMS Configuration: INODEMOSRMS01.inovitdemos.ch
AD RMS Cluster
TARGET SERVER
INODEMOSRMS01.inovitdemos.ch
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Create or Join an AD RMS Cluster
AD RMS supports two types of clusters: a root cluster for certification and licensing and a licensing-only cluster. To deploy AD RMS, you must first set up a root cluster in the forest. You can then set up one or more licensing-only clusters in the same forest, depending on your needs.
Create a new AD RMS root cluster
Join an existing AD RMS cluster
More about AD RMS clusters
< Previous
Next >
Install
Cancel


AD RMS Configuration: INODEMOSRMS01.inovitdemos.ch
Configuration Database
TARGET SERVER
INODEMOSRMS01.inovitdemos.ch
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Select Configuration Database Server
Your AD RMS cluster uses a database to store configuration and policy information. The database can be hosted either by Windows Internal Database or on a separate SQL database server (recommended). If you choose Windows Internal Database, you cannot add more AD RMS servers to this cluster. You can specify the SQL database server by selecting it from a list, or you can type its name or CNAME alias (recommended).
Specify a database server and a database instance.
Server:
Select...
Database Instance:
List
Use Windows Internal Database on this server
More about the AD RMS configuration database
< Previous
Next >
Install
Cancel

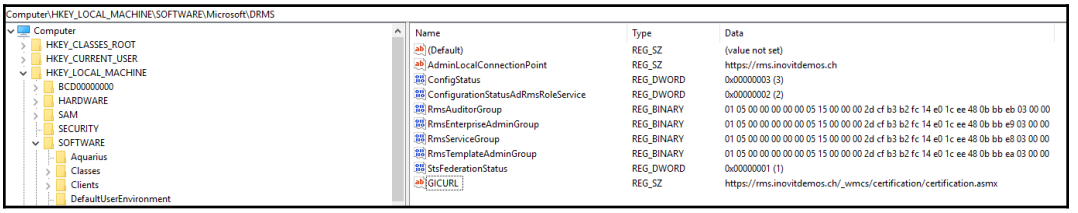

AD RMS Configuration: INODEMOSRMS01.inovitdemos.ch
Service Account
TARGET SERVER
INODEMOSRMS01.inovitdemos.ch
AD RMS
AD RMS Cluster
Configuration Da
Service Account
Cryptographic M
Cluster Key Stora
Cluster Key Passw
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certifica
SCP Registration
Confirmation
Progress
Results
Specify Service Account
icate with other
with no additional
Windows Security
Type User Account Name and Password
Type the name and password of a standard domain user account.
For example, user@example.contoso.com, or domain\user name.
svcrmscluster@inovitdemos.ch
Domain: inovitdemos.ch
More choices
OK
Cancel
nstall
Cancel

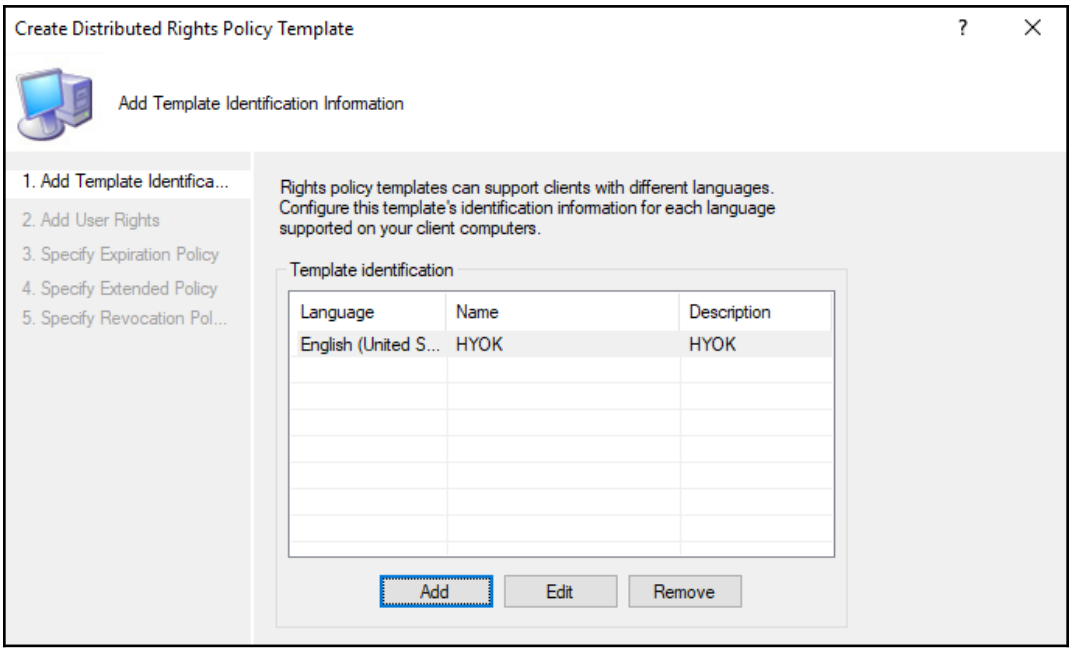

AD RMS Configuration: INODEMOSRMS01.inovitdemos.ch
Cluster Address
TARGET SERVER
INODEMOSRMS01.inovitdemos.ch
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Specify Cluster Address
A cluster address makes it possible for AD RMS clients to communicate with this cluster over the network. We recommend that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and this cluster. You must use an SSL-encrypted connection if you intend to federate this cluster.
Connection Type:
Use an SSL-encrypted connection (https://)
Use an unencrypted connection (http://)
Fully-Qualified Domain Name:
Port:
https://
rms.inovitdemos.ch
443
You cannot change this address or port number after AD RMS is installed and configured.
More about the cluster web site
< Previous
Next >
Install
Cancel

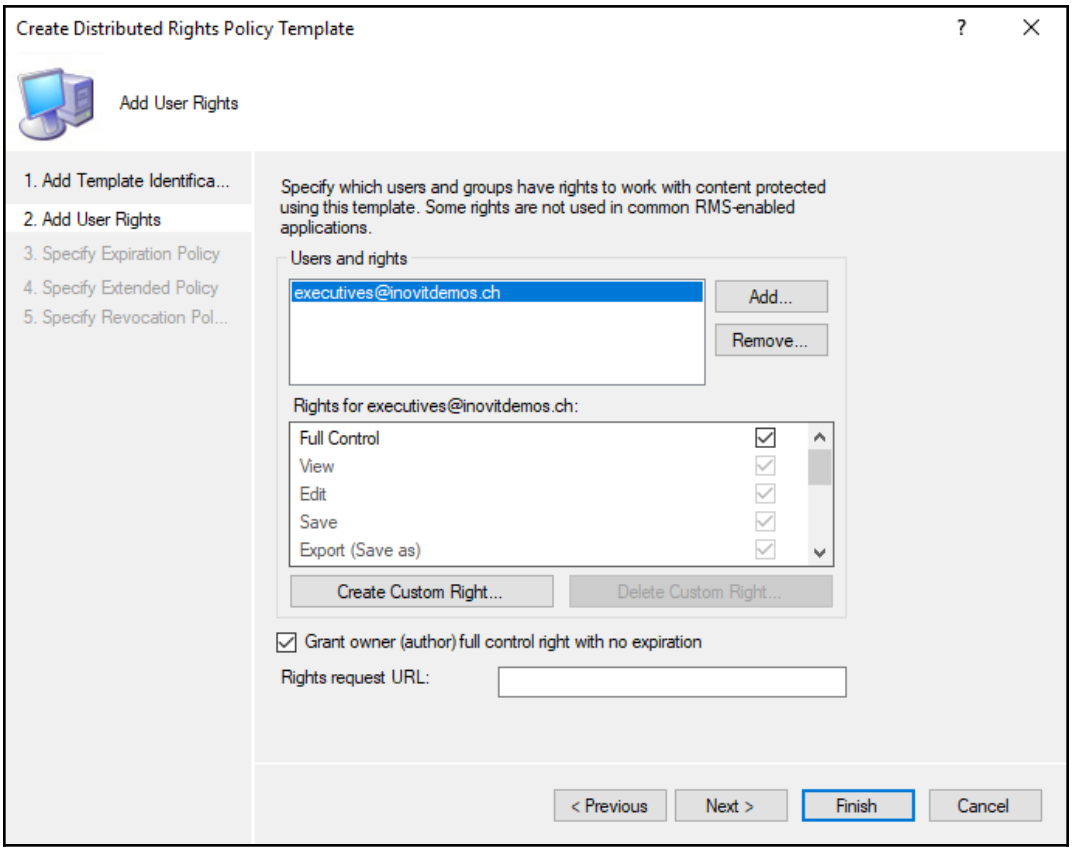

AD RMS Configuration: INODEMOSRMS01.inovitdemos.ch
Results
TARGET SERVER
INODEMOSRMS01.inovitdemos.ch
AD RMS
AD RMS Cluster
Configuration Database
Service Account
Cryptographic Mode
Cluster Key Storage
Cluster Key Password
Cluster Web Site
Cluster Address
Server Certificate
Licensor Certificate
SCP Registration
Confirmation
Progress
Results
Installation Results
The following roles, role services, or features were installed successfully:
Active Directory Rights Management Services
Before you can administer AD RMS on this server, you must log off and log on again.
You have selected to register a Service Connection Point (SCP) at a later time. You will need to register the SCP before clients can access the AD RMS cluster.
The following role services were installed:
Active Directory Rights Management Server
Troubleshooting AD RMS setup
< Previous
Next >
Close
Cancel

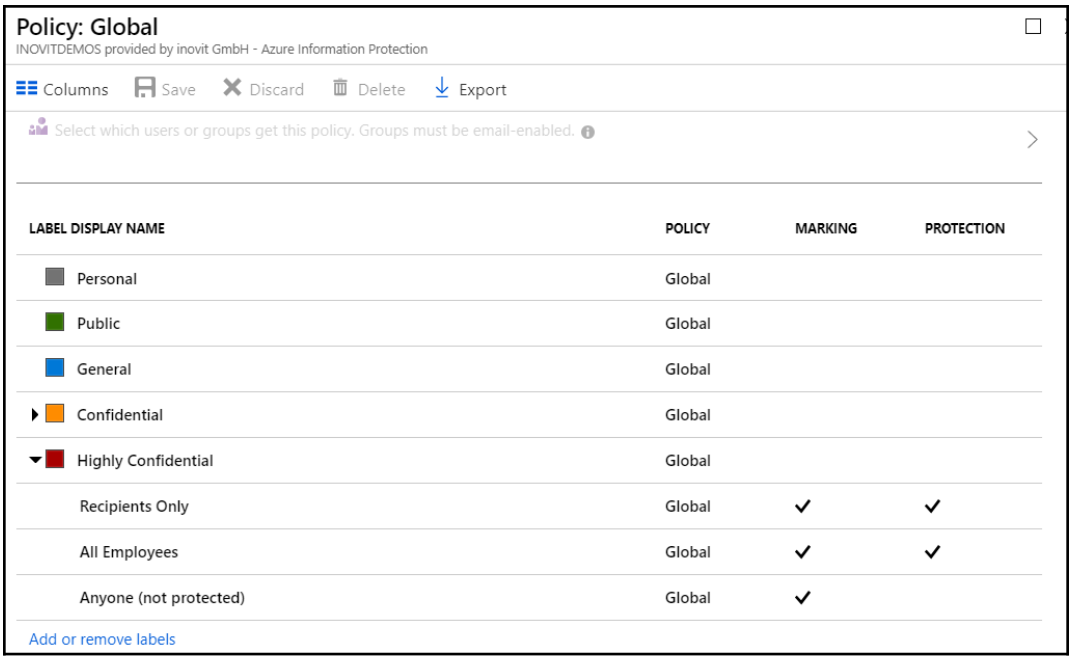

inodemosrms01 (Local) Properties
Server Certificate
Proxy Settings
Logging
SCP
General
Cluster URLs
AD RMS Servers
The following URLs are used by AD RMS clients to connect to the cluster for licensing and certification.
Intranet URLs
Licensing:
https://
rms.inovitdemos.ch
/_wmcs/licensing
Certification:
https://rms.inovitdemos.ch/_wmcs/certification/certi
Extranet URLs
Connection points used by extranet clients for services provided by the clusters.
Licensing:
http://
rms.inovitdemos.ch
/_wmcs/licensing
Certification:
http://
rms.inovitdemos.ch
/_wmcs/certification
OK
Cancel
Apply
Help

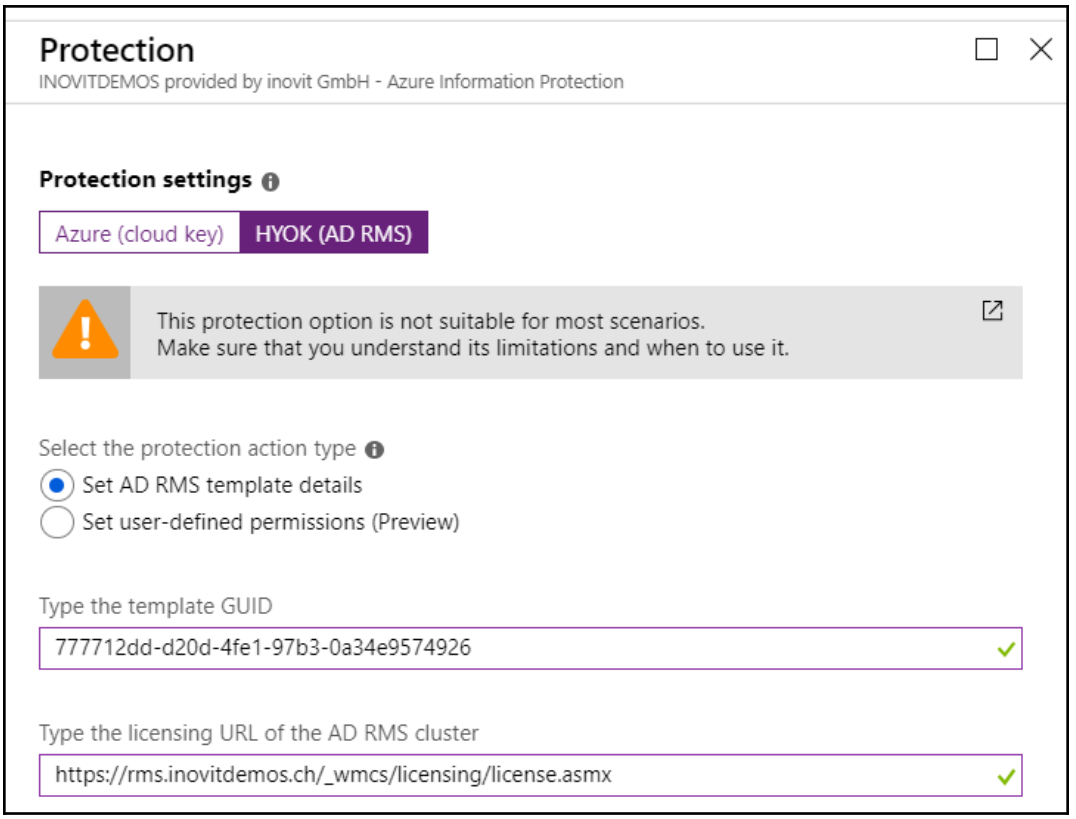

Super Users
Super User Group
Specify the super user group name in the format group@domain.com. The group that you specify must be an Active Directory Domain Services distribution group that has an e-mail name that exactly matches the group name.
Super user group:
aiprmssuperusers@inovitdemos.ch
Browse...
OK
Cancel
Apply
Help


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DRMS
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
Aquarius
Classes
Clients
DefaultUserEnvironment
Name
Type
Data
(Default)
REG_SZ
(value not set)
AdminLocalConnectionPoint
REG_SZ
https://rms.inovitdemos.ch
ConfigStatus
REG_DWORD
0x00000003 (3)
ConfigurationStatusAdRmsRoleService
REG_DWORD
0x00000002 (2)
RmsAuditorGroup
REG_BINARY
01 05 00 00 00 00 00 05 15 00 00 00 2d cf b3 b2 fc 14 e0 1c ee 48 0b bb eb 03 00 00
RmsEnterpriseAdminGroup
REG_BINARY
01 05 00 00 00 00 00 05 15 00 00 00 2d cf b3 b2 fc 14 e0 1c ee 48 0b bb e9 03 00 00
RmsServiceGroup
REG_BINARY
01 05 00 00 00 00 00 05 15 00 00 00 2d cf b3 b2 fc 14 e0 1c ee 48 0b bb e8 03 00 00
RmsTemplateAdminGroup
REG_BINARY
01 05 00 00 00 00 00 05 15 00 00 00 2d cf b3 b2 fc 14 e0 1c ee 48 0b bb ea 03 00 00
StsFederationStatus
REG_DWORD
0x00000001 (1)
GICURL
REG_SZ
https://rms.inovitdemos.ch/_wmcs/certification/certification.asmx

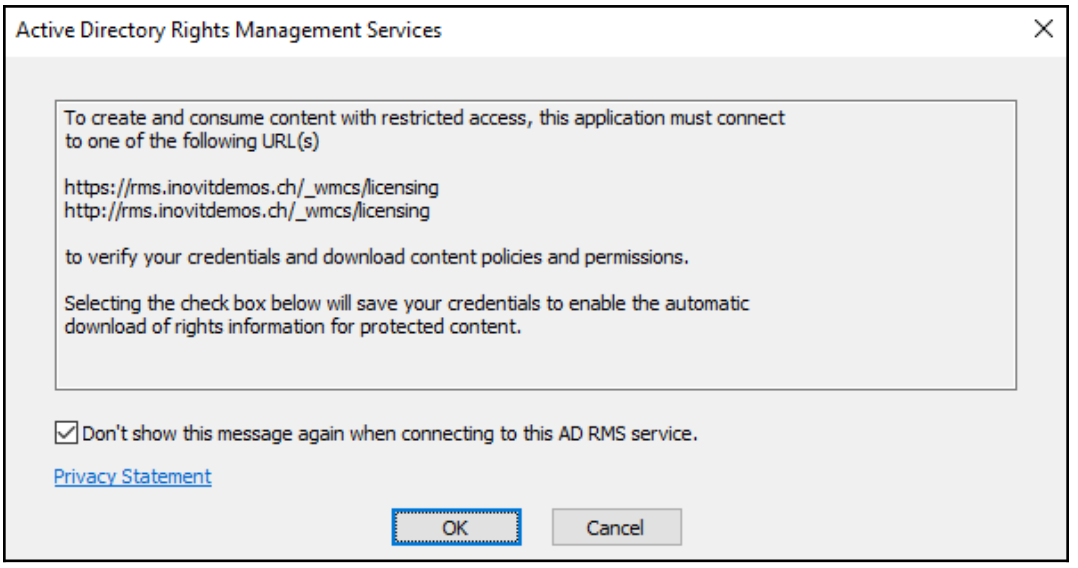

Create Distributed Rights Policy Template
Add Template Identification Information
1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...
Rights policy templates can support clients with different languages. Configure this template's identification information for each language supported on your client computers.
Template identification
Language
Name
Description
English (United S...
HYOK
HYOK
Add
Edit
Remove

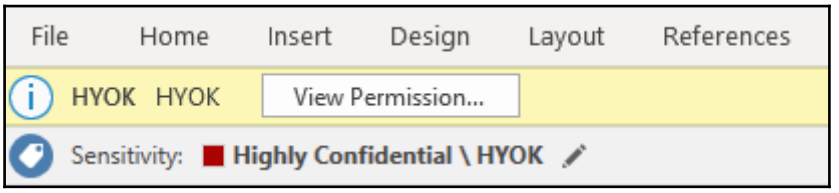

Create Distributed Rights Policy Template
Add User Rights
1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...
Specify which users and groups have rights to work with content protected using this template. Some rights are not used in common RMS-enabled applications.
Users and rights
executives@inovitdemos.ch
Add...
Remove...
Rights for executives@inovitdemos.ch:
Full Control
View
Edit
Save
Export (Save as)
Create Custom Right...
Delete Custom Right...
Grant owner (author) full control right with no expiration
Rights request URL:
< Previous
Next >
Finish
Cancel

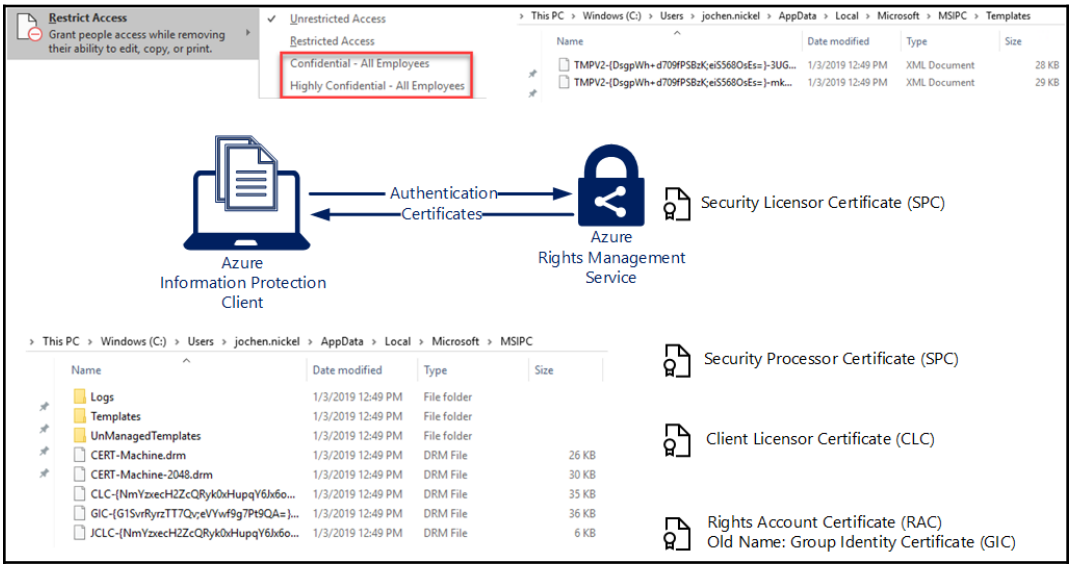

Policy: Global
INOVITDEMOS provided by inovit GmbH - Azure Information Protection
Columns
Save
Discard
Delete
Export
Select which users or groups get this policy. Groups must be email-enabled.
LABEL DISPLAY NAME
POLICY
MARKING
PROTECTION
Personal
Global
Public
Global
General
Global
Confidential
Global
Highly Confidential
Global
Recipients Only
Global
All Employees
Global
Anyone (not protected)
Global
Add or remove labels

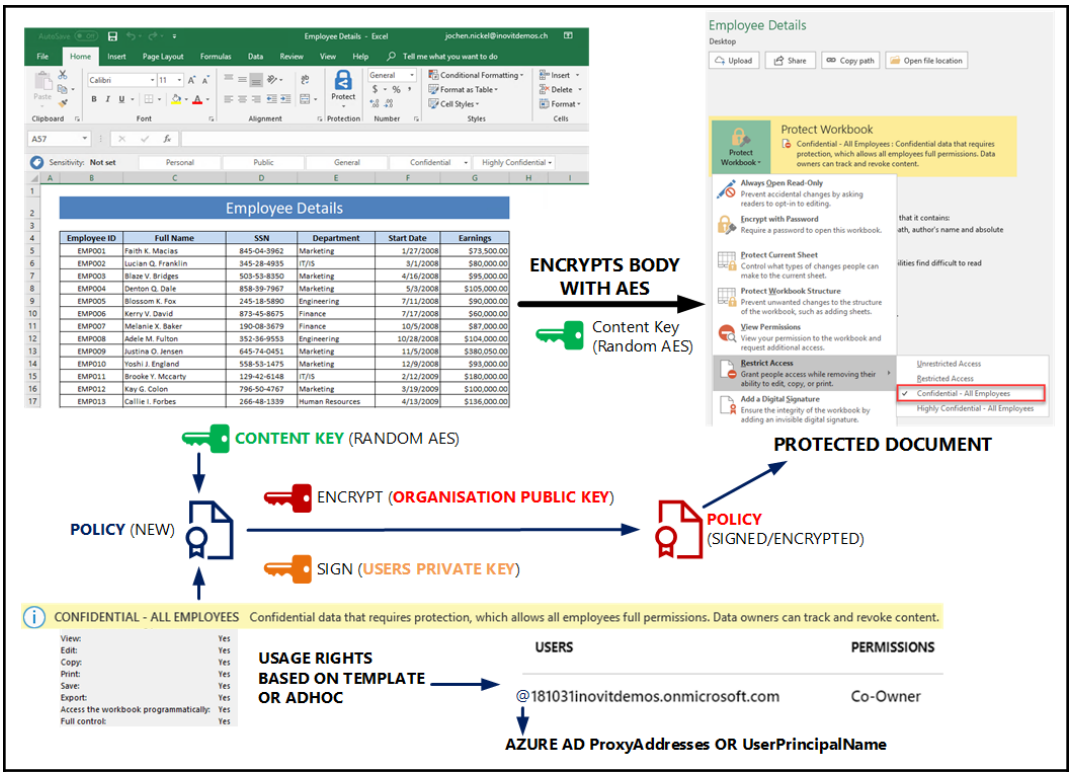

Protection
INOVITDEMOS provided by inovit GmbH - Azure Information Protection
Protection settings
Azure (cloud key)
HYOK (AD RMS)
This protection option is not suitable for most scenarios.
Make sure that you understand its limitations and when to use it.
Select the protection action type
Set AD RMS template details
Set user-defined permissions (Preview)
Type the template GUID
777712dd-d20d-4fe1-97b3-0a34e9574926
Type the licensing URL of the AD RMS cluster
https://rms.inovitdemos.ch/_wmcs/licensing/license.asmx

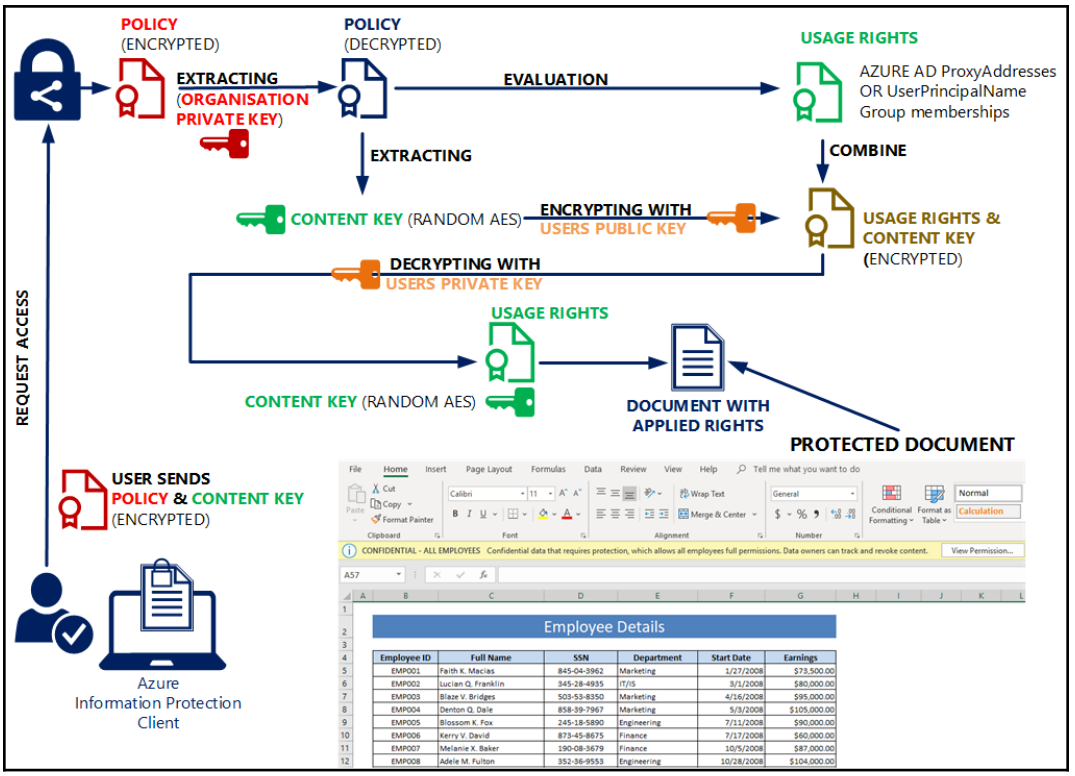

Policy: Add or remove labels
Select labels available in this policy
Search to filter items...
LABEL DISPLAY NAME
POLICY
Personal
Global
Public
Global
General
Global
Confidential
Global
Recipients Only
Global
All Employees
Global
Anyone (not protected)
Global
Highly Confidential
Global
Recipients Only
Global
All Employees
Global
Anyone (not protected)
Global
HYOK


Active Directory Rights Management Services
To create and consume content with restricted access, this application must connect to one of the following URL(s)
https://rms.inovitdemos.ch/_wmcs/licensing
http://rms.inovitdemos.ch/_wmcs/licensing
to verify your credentials and download content policies and permissions.
Selecting the check box below will save your credentials to enable the automatic download of rights information for protected content.
Don't show this message again when connecting to this AD RMS service.
Privacy Statement
OK
Cancel


File
Home
Insert
Design
Layout
References
HYOK HYOK
View Permission...
Sensitivity:
Highly Confidential \ HYOK

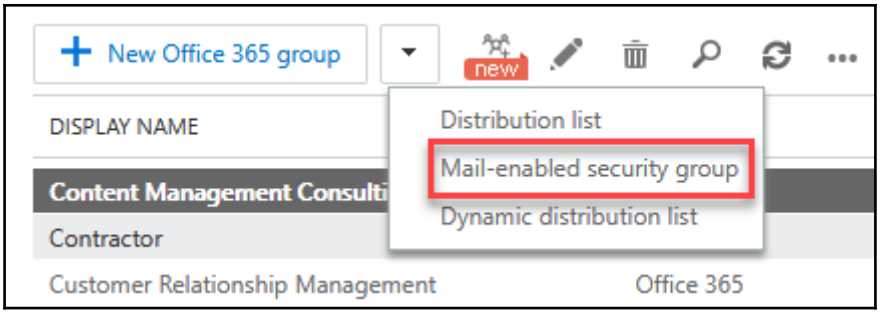

Restrict Access
Grant people access while removing their ability to edit, copy, or print.
Unrestricted Access
Restricted Access
Confidential - All Employees
Highly Confidential - All Employees
This PC › Windows (C:) › Users › jochen.nickel › AppData › Local › Microsoft › MSIPC › Templates
Name
Date modified
Type
Size
TMPV2-{DsgpWh+d709fPSBzKeiS568OsEs=}-3UG...
1/3/2019 12:49 PM
XML Document
28 KB
TMPV2-{DsgpWh+d709fPSBzKeiS568OsEs=}-mk...
1/3/2019 12:49 PM
XML Document
29 KB
Authentication
Certificates
Azure
Information Protection
Client
Azure
Rights Management
Service
Security Licensor Certificate (SPC)
This PC › Windows (C:) › Users › jochen.nickel › AppData › Local › Microsoft › MSIPC
Name
Date modified
Type
Size
Logs
1/3/2019 12:49 PM
File folder
Templates
1/3/2019 12:49 PM
File folder
UnManagedTemplates
1/3/2019 12:49 PM
File folder
CERT-Machine.drm
1/3/2019 12:49 PM
DRM File
26 KB
CERT-Machine-2048.drm
1/3/2019 12:49 PM
DRM File
30 KB
CLC-{NmYzxecH2ZcQRyk0xHupqY6Jx6o...
1/3/2019 12:49 PM
DRM File
35 KB
GIC-{G1SvrRyrzTT7Qv;eVYwf9g7Pt9QA=}...
1/3/2019 12:49 PM
DRM File
36 KB
JCLC-{NmYzxecH2ZcQRyk0xHupqY6Jx6o...
1/3/2019 12:49 PM
DRM File
6 KB
Security Processor Certificate (SPC)
Client Licensor Certificate (CLC)
Rights Account Certificate (RAC)
Old Name: Group Identity Certificate (GIC)

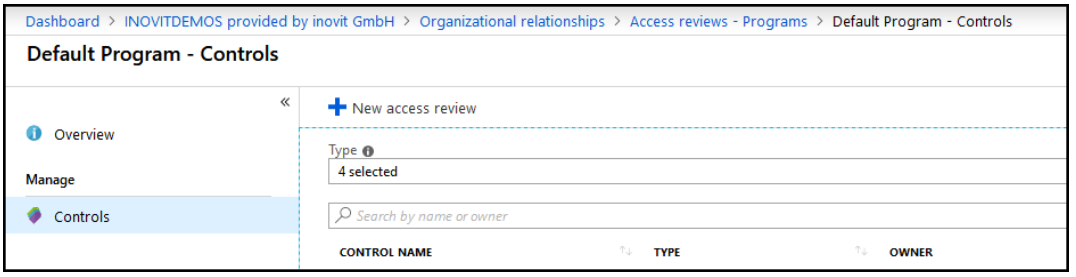

Employee Details
ENCRYPTS BODY WITH AES
Content Key (Random AES)
Protect Workbook
CONTENT KEY (RANDOM AES)
PROTECTED DOCUMENT
ENCRYPT (ORGANISATION PUBLIC KEY)
POLICY (NEW)
POLICY (SIGNED/ENCRYPTED)
SIGN (USERS PRIVATE KEY)
CONFIDENTIAL - ALL EMPLOYEES
Confidential data that requires protection, which allows all employees full permissions. Data owners can track and revoke content.
USAGE RIGHTS BASED ON TEMPLATE OR ADHOC
USERS
PERMISSIONS
@181031inovitdemos.onmicrosoft.com
Co-Owner
AZURE AD ProxyAddresses OR UserPrincipalName

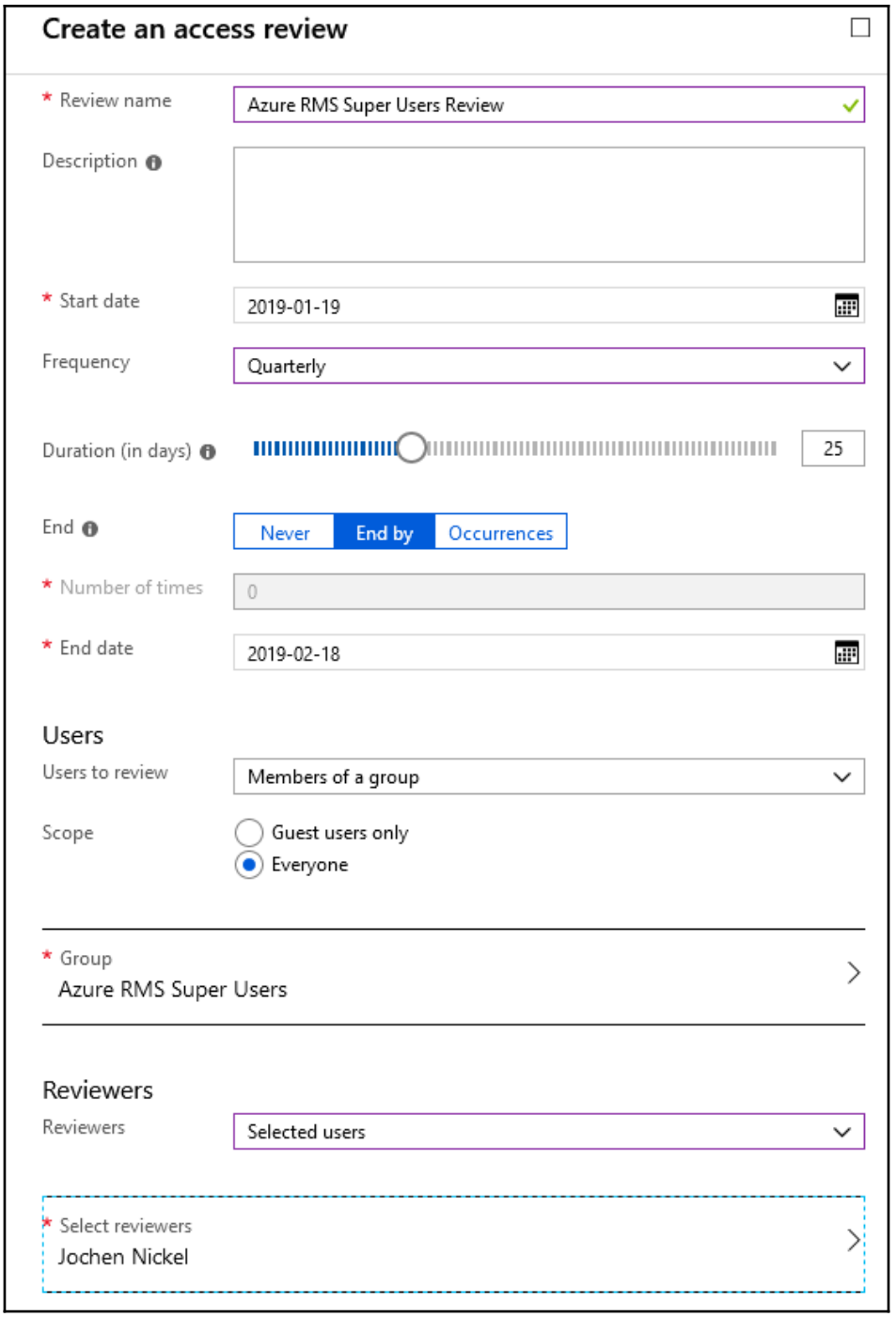

POLICY
(ENCRYPTED)
EXTRACTING
(ORGANISATION
PRIVATE KEY)
POLICY
(DECRYPTED)
EVALUATION
USAGE RIGHTS
AZURE AD ProxyAddresses
OR UserPrincipalName
Group memberships
EXTRACTING
COMBINE
CONTENT KEY (RANDOM AES)
ENCRYPTING WITH
USERS PUBLIC KEY
USAGE RIGHTS &
CONTENT KEY
(ENCRYPTED)
DECRYPTING WITH
USERS PRIVATE KEY
REQUEST ACCESS
USAGE RIGHTS
CONTENT KEY (RANDOM AES)
DOCUMENT WITH
APPLIED RIGHTS
PROTECTED DOCUMENT
USER SENDS
POLICY & CONTENT KEY
(ENCRYPTED)
Azure
Information Protection
Client
Employee Details
Employee ID
Full Name
SSN
Department
Start Date
Earnings
EMP001 Faith K. Macias 845-04-3962 Marketing 1/27/2008 $73,500.00
EMP002 Lucian Q. Franklin 345-28-4935 IT/IS 3/1/2008 $80,000.00
EMP003 Blaze V. Bridges 503-53-8350 Marketing 4/16/2008 $95,000.00
EMP004 Denton D. Dale 858-39-7967 Marketing 5/3/2008 $105,000.00
EMP005 Blossom K. Fox 245-18-5890 Engineering 7/11/2008 $90,000.00
EMP006 Kerry V. David 873-45-8675 Finance 7/17/2008 $60,000.00
EMP007 Melanie X. Baker 190-08-3679 Finance 10/5/2008 $87,000.00
EMP008 Adele M. Fulton 352-36-9553 Engineering 10/28/2008 $104,000.00

Chapter 15: Configuring Azure Information Protection Solutions

Name	Department	Job Title	Manager
Dan Jump	Executive	CEO	
Adam Barr	Operations	General Manager of Professional Services	Dan Jump
Karim Manar	Accounting	Controller	Diane Tibbot
Dan Park	Sales	Vice President NA Sales	Adam Barr
Christa Geller	Executive	CVP of Online	Jeff Hay
Alan Brewer	Sales	Regional Sales Manager	Jack Creasey
Aaron Painter	Strategy Consulting	Strategy Consulting Manager	Christine Koch
Amy Alberts	Human Resources	HR Manager	Garth Fort
Scott Bishop	Project Management	Senior Project Manager	Alan Steiner
Don Hall	Strategy Consulting	Strategy Consultant	Ellen Adams
Chase Carpenter	Accounting	Accountant	Karim Manar
Lars Hansson	Accounting	Accounting Manager	Karim Manar
David Wright	Sales	Salesperson	David Simpson
Greg Winston	Senior Management	President of Management	Jeff Hay
Ye Xu	Sales Engagement Management	Salesperson	Arthur Yasinski
Ian Tien	Human Resources	HR Specialist	Amy Alberts
Brian Cox	Operations	Procurement Manager	Keith Dishmo

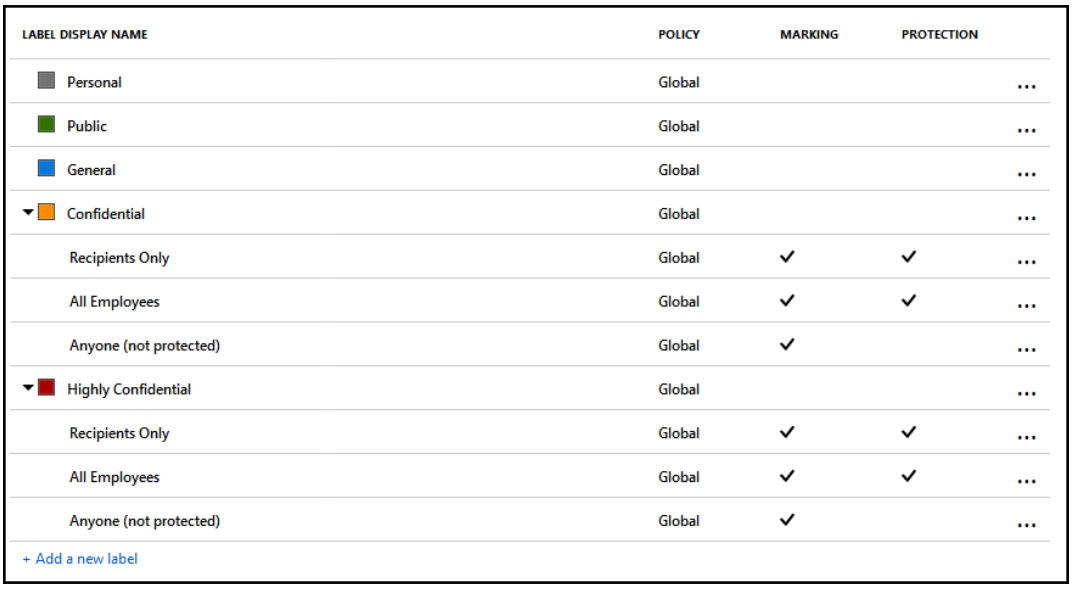


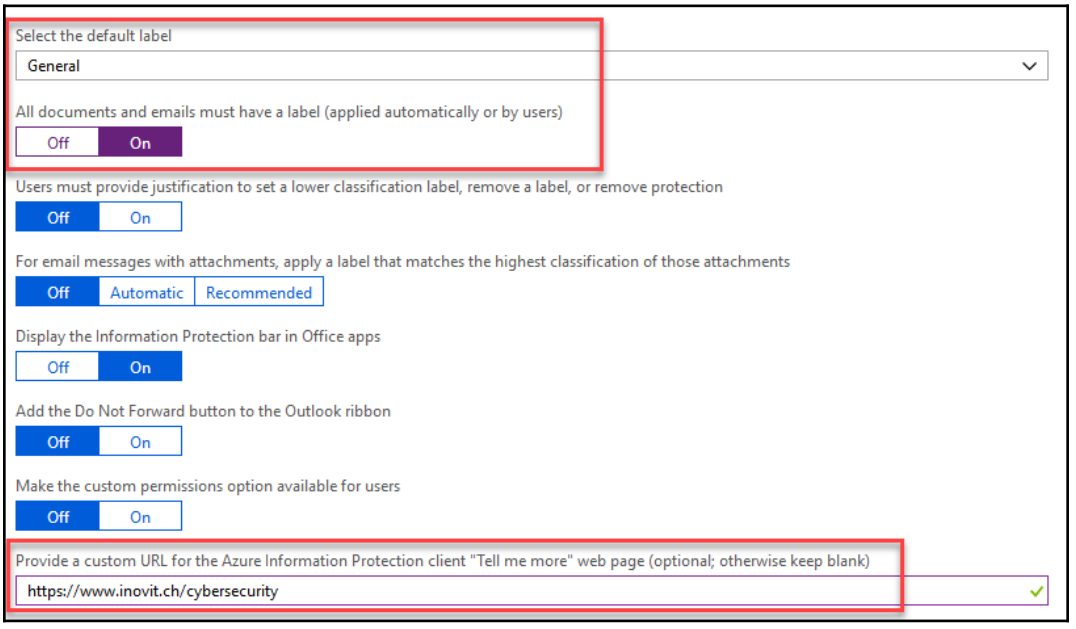



Create an access review
* Review name
Azure RMS Super Users Review
Description
* Start date
2019-01-19
Frequency
Quarterly
Duration (in days)
25
End
Never
End by
Occurrences
* Number of times
0
* End date
2019-02-18
Users
Users to review
Members of a group
Scope
Guest users only
Everyone
* Group
Azure RMS Super Users
Reviewers
Reviewers
Selected users
* Select reviewers
Jochen Nickel


```
PS C:\> Get-AadrmTemplate


TemplateId  : 026be843-becf-425f-a776-27d4c1b8fd54
Name        : Confidential - All Employees
Description : Confidential data that requires protection, which allows all employees full permissions. Data owners can
              track and revoke content.

TemplateId  : 68ab2d70-f65e-4b83-b3fb-8ed3e7f06ee7
Name        : Highly Confidential - All Employees
Description : Highly confidential data that allows all employees view, edit, and reply permissions to this content.
              Data owners can track and revoke content.
```

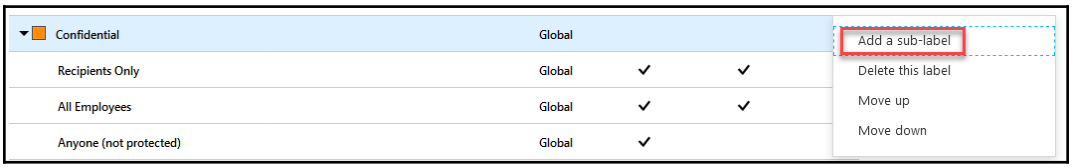
```
PS C:\Users\donh\Desktop> Get-AIPFileStatus .\Q3_Product_Strategy.docx


FileName         : C:\Users\donh\Desktop\Q3_Product_Strategy.docx
IsLabeled        : True
MainLabelId      : de82bccd-c50f-4162-b113-8aa9e98ed45f
MainLabelName    : Confidential
SubLabelId       : 6eae6a7b-f321-4fc4-8049-1ef7cc9575b2
SubLabelName     : All Employees
LabelingSiteId   : 7709ca2b-3be8-4d92-89d7-dc1e274b4d0e
Owner            : Don.Hall@inovitdemos.ch
LabelingMethod   : Manual
LabelDate        : 1/18/2019 10:20:31 AM
IsRMSProtected   : True
RMSTemplateId    : 026be843-becf-425f-a776-27d4c1b8fd54
RMSTemplateName  : Confidential - All Employees
RMSIssuedTime    : 1/18/2019 10:21:00 AM
RMSOwner         : Don.Hall@inovitdemos.ch
RMSIssuer        : Don.Hall@inovitdemos.ch
```

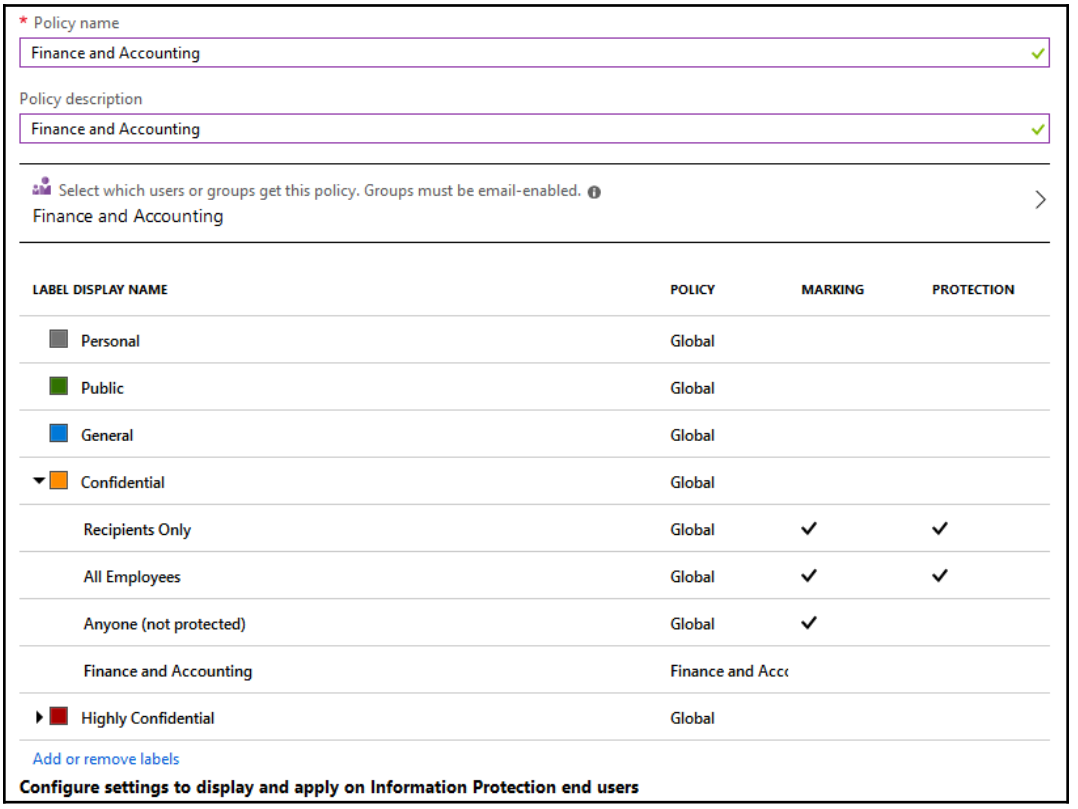

LABEL DISPLAY NAME
POLICY
MARKING
PROTECTION
Personal
Global
Public
Global
General
Global
Confidential
Global
Recipients Only
Global
All Employees
Global
Anyone (not protected)
Global
Highly Confidential
Global
Recipients Only
Global
All Employees
Global
Anyone (not protected)
Global
+ Add a new label

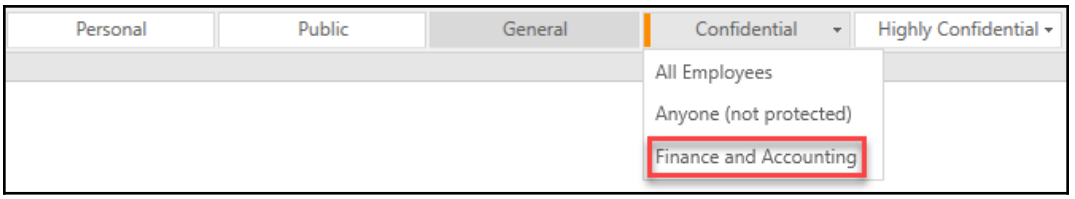

Select the default label
General
All documents and emails must have a label (applied automatically or by users)
Off
On
Users must provide justification to set a lower classification label, remove a label, or remove protection
Off
On
For email messages with attachments, apply a label that matches the highest classification of those attachments
Off
Automatic
Recommended
Display the Information Protection bar in Office apps
Off
On
Add the Do Not Forward button to the Outlook ribbon
Off
On
Make the custom permissions option available for users
Off
On
Provide a custom URL for the Azure Information Protection client "Tell me more" web page (optional; otherwise keep blank)
https://www.inovit.ch/cybersecurity

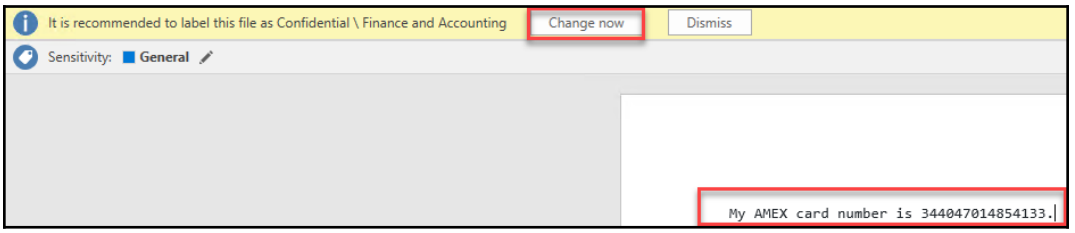

Set permissions for documents and emails containing this label
Not configured
Protect
Remove Protection

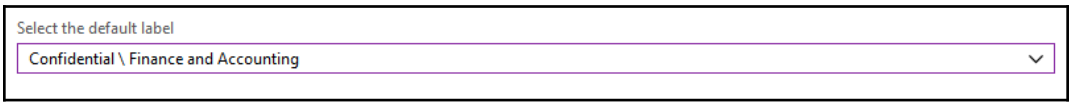

Sensitivity: General
Personal
Public
General
Confidential
Highly Confidential


Confidential
Global
Recipients Only
Global
All Employees
Global
Anyone (not protected)
Global
Add a sub-label
Delete this label
Move up
Move down

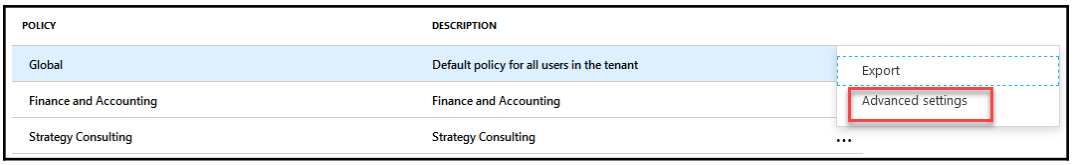

* Policy name
Finance and Accounting
Policy description
Finance and Accounting
Select which users or groups get this policy. Groups must be email-enabled.
Finance and Accounting
LABEL DISPLAY NAME
POLICY
MARKING
PROTECTION
Personal
Global
Public
Global
General
Global
Confidential
Global
Recipients Only
Global
All Employees
Global
Anyone (not protected)
Global
Finance and Accounting
Finance and Acc
Highly Confidential
Global
Add or remove labels
Configure settings to display and apply on Information Protection end users

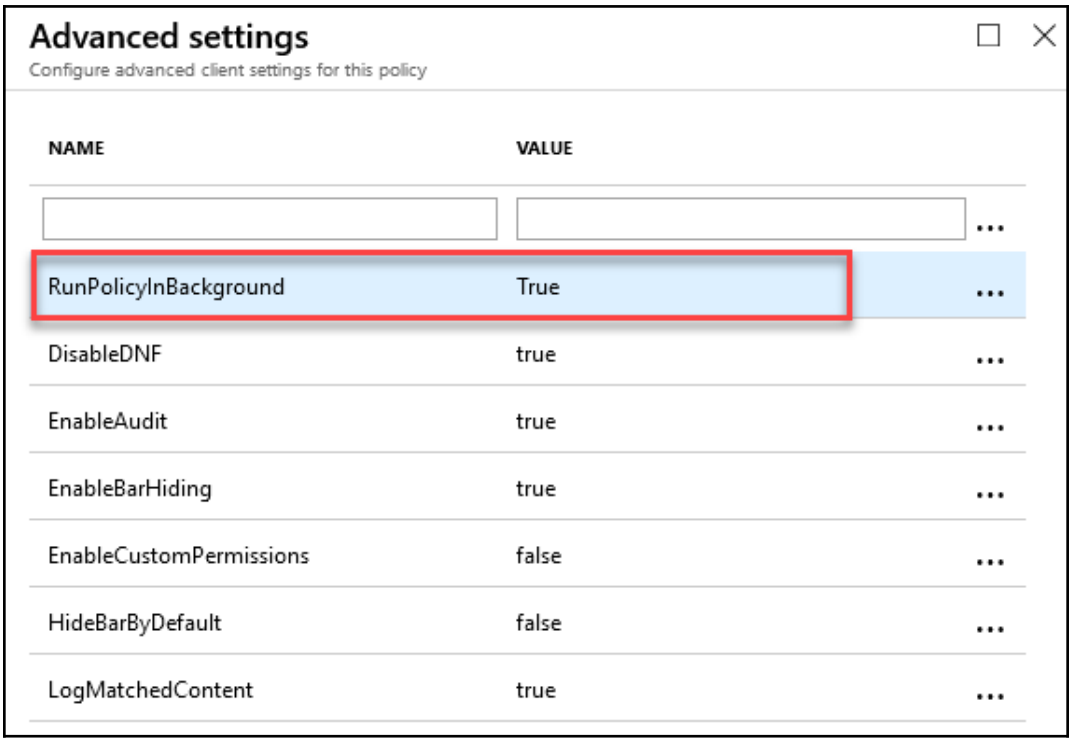


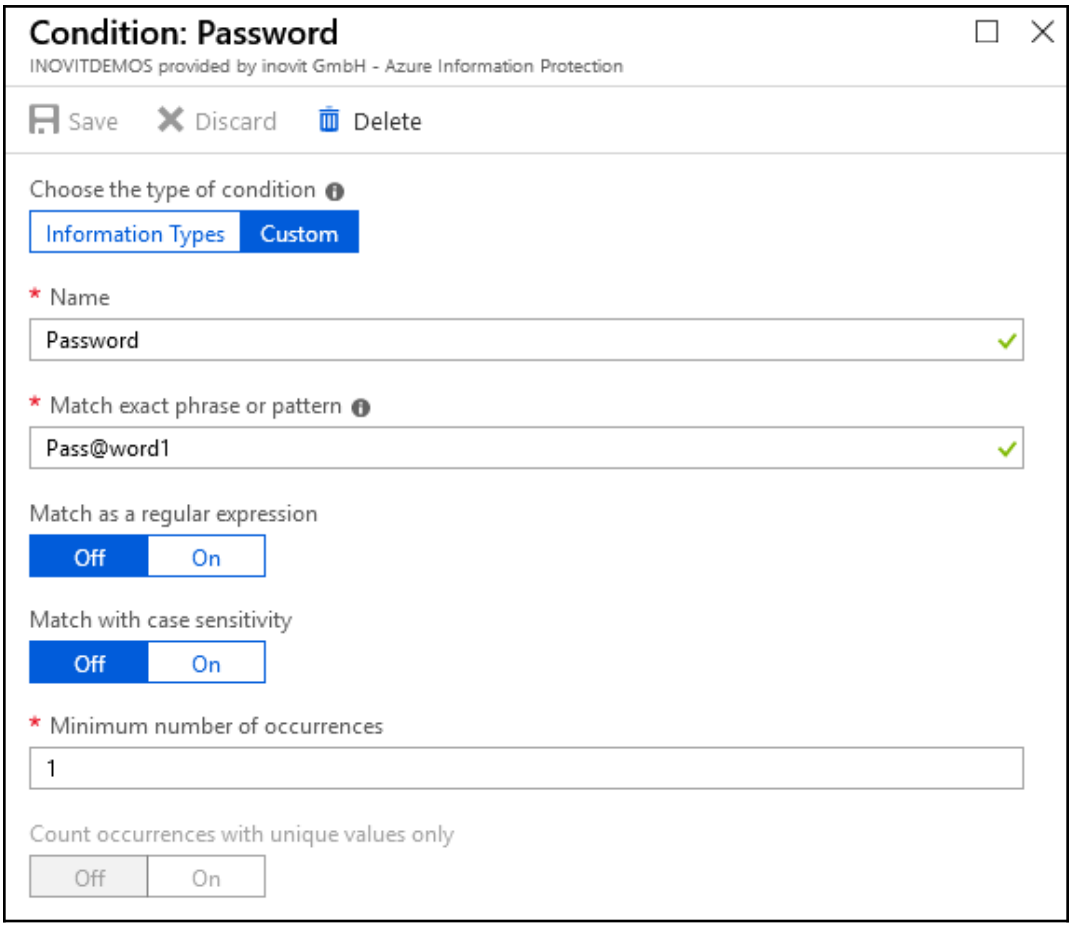


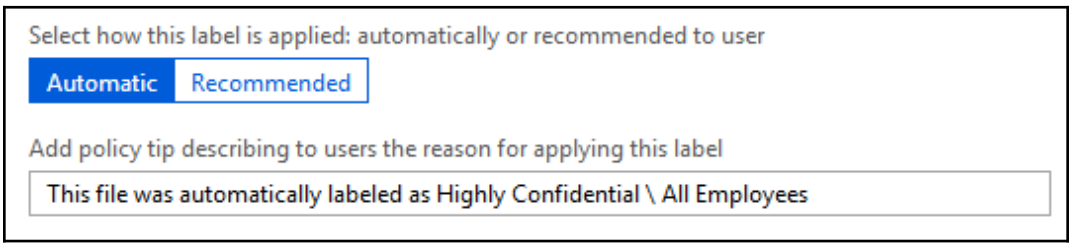


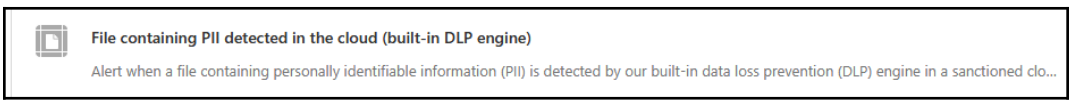
LABEL DISPLAY NAME	POLICY	MARKING	PROTECTION
Personal	Global		
Public	Global		
General	Global		
Confidential	Global		
Finance and Accounting	Finance and Accounting		
Strategy Consulting	Strategy Consulting		
Senior Management	Senior Management		
Human Resources	Human Resources		
Executives	Executives		
Recipients Only	Global	✓	
All Employees	Global	✓	
Anyone (not protected)	Global	✓	
Highly Confidential	Global		

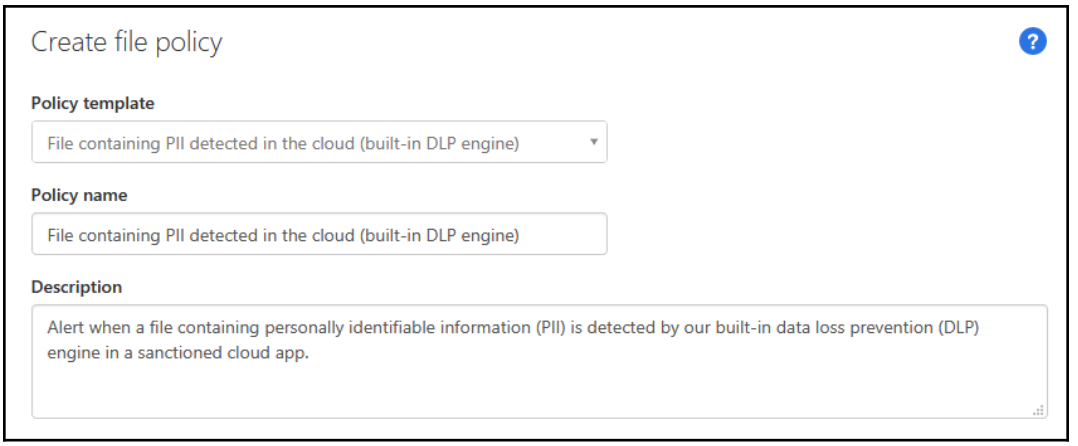

POLICY
DESCRIPTION
Global
Default policy for all users in the tenant
Finance and Accounting
Finance and Accounting
Strategy Consulting
Strategy Consulting
Export
Advanced settings

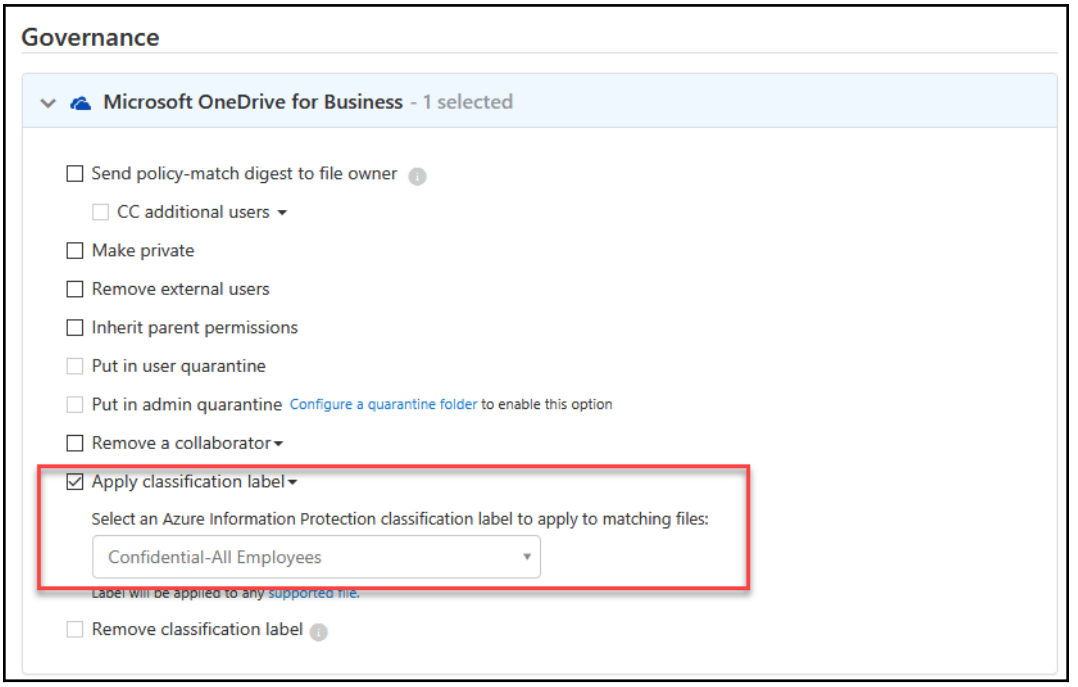

Advanced settings
Configure advanced client settings for this policy
NAME
VALUE
RunPolicyInBackground
True
DisableDNF
true
EnableAudit
true
EnableBarHiding
true
EnableCustomPermissions
false
HideBarByDefault
false
LogMatchedContent
true

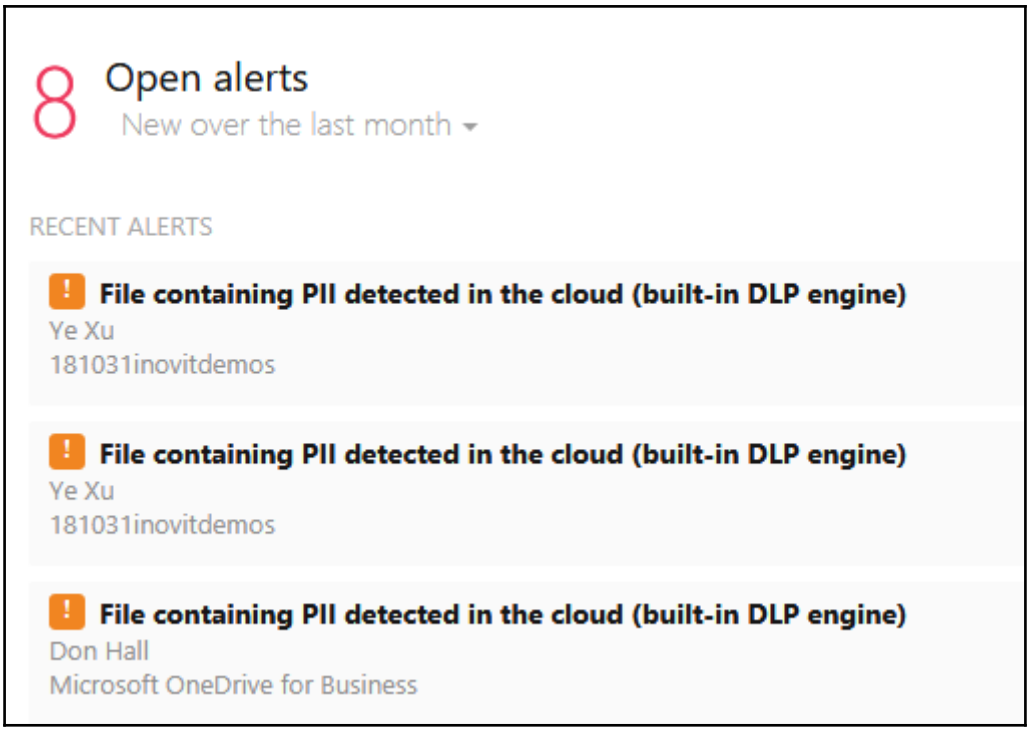

Condition: Password
INOVITDEMOS provided by inovit GmbH - Azure Information Protection
Save
Discard
Delete
Choose the type of condition
Information Types
Custom
* Name
Password
* Match exact phrase or pattern
Pass@word1
Match as a regular expression
Off
On
Match with case sensitivity
Off
On
* Minimum number of occurrences
1
Count occurrences with unique values only
Off
On

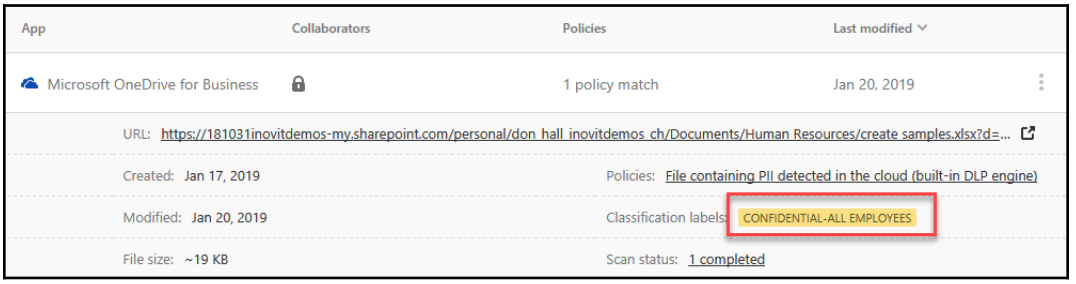

Select how this label is applied: automatically or recommended to user
Automatic
Recommended
Add policy tip describing to users the reason for applying this label
This file was automatically labeled as Highly Confidential \ All Employees

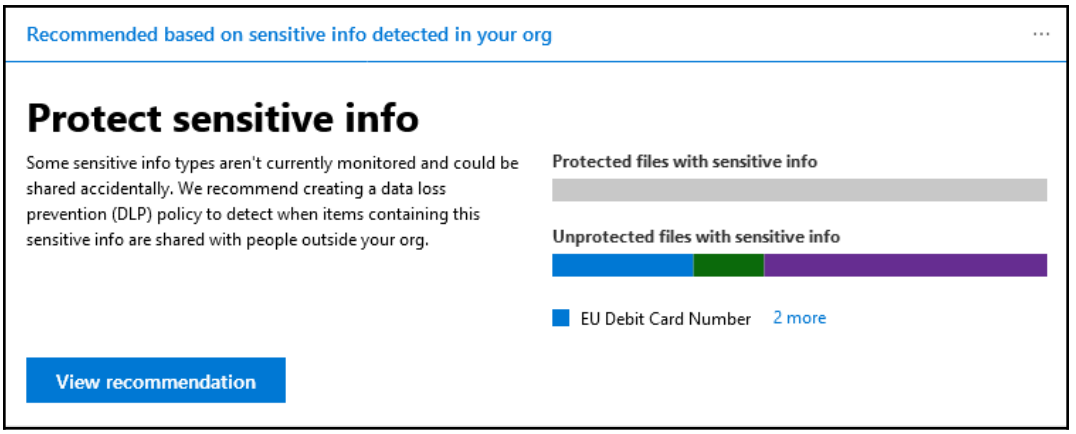

File containing PII detected in the cloud (built-in DLP engine)
Alert when a file containing personally identifiable information (PII) is detected by our built-in data loss prevention (DLP) engine in a sanctioned clo...

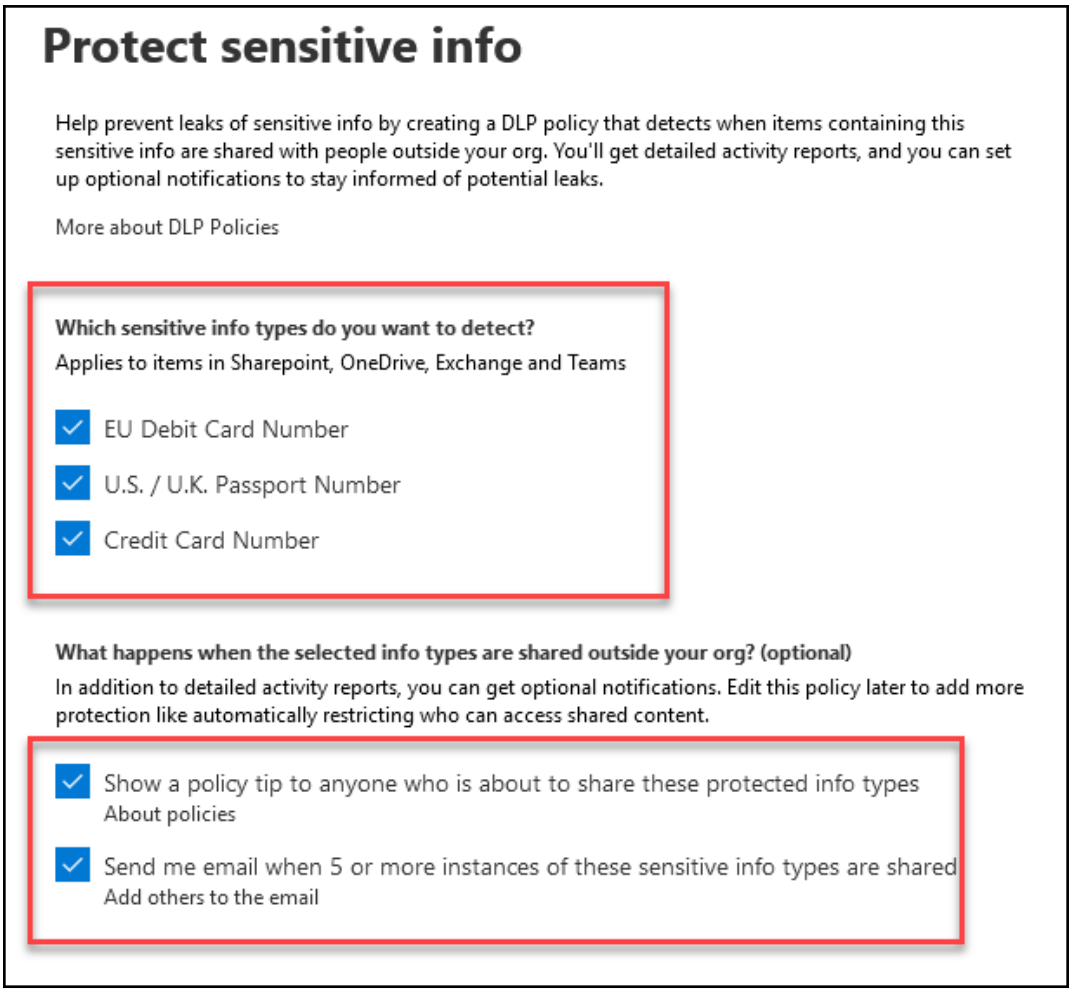

Create file policy
Policy template
File containing PII detected in the cloud (built-in DLP engine)
Policy name
File containing PII detected in the cloud (built-in DLP engine)
Description
Alert when a file containing personally identifiable information (PII) is detected by our built-in data loss prevention (DLP) engine in a sanctioned cloud app.

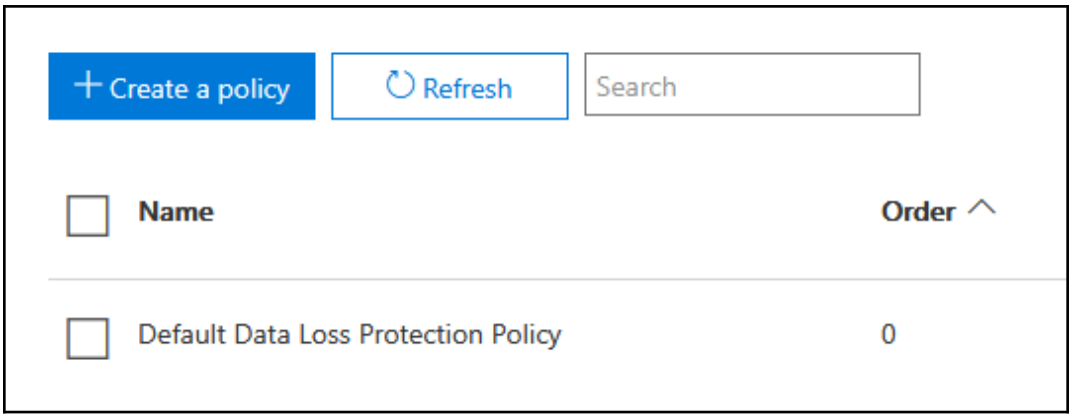

Governance
Microsoft OneDrive for Business - 1 selected
Send policy-match digest to file owner
CC additional users
Make private
Remove external users
Inherit parent permissions
Put in user quarantine
Put in admin quarantine Configure a quarantine folder to enable this option
Remove a collaborator
Apply classification label
Select an Azure Information Protection classification label to apply to matching files:
Confidential-All Employees
Label will be applied to any supported file.
Remove classification label

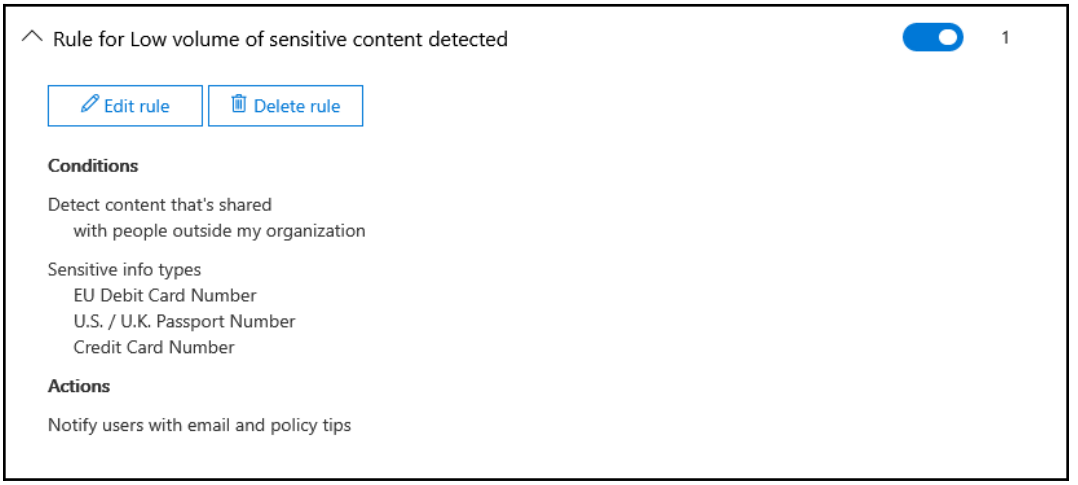

8
Open alerts
New over the last month
RECENT ALERTS
File containing PII detected in the cloud (built-in DLP engine)
Ye Xu
181031inovitdemos
File containing PII detected in the cloud (built-in DLP engine)
Ye Xu
181031inovitdemos
File containing PII detected in the cloud (built-in DLP engine)
Don Hall
Microsoft OneDrive for Business

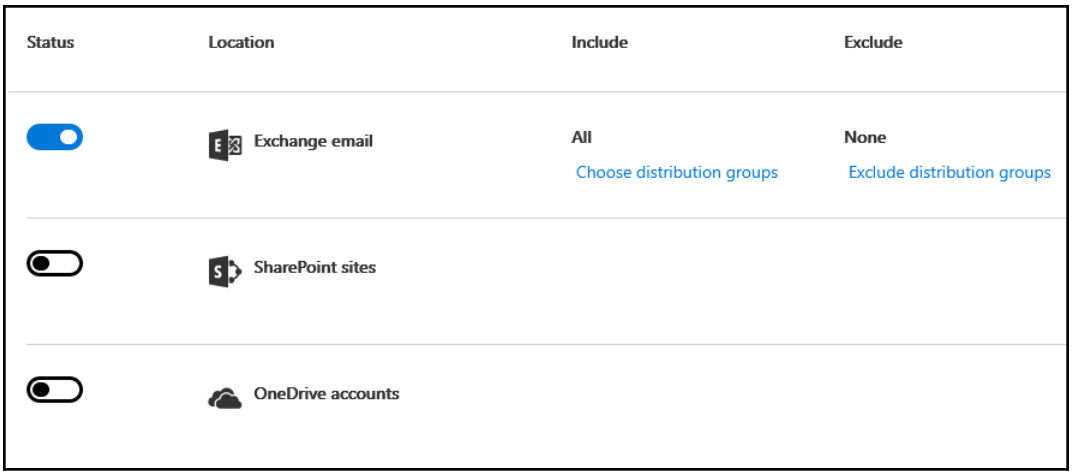

App
Collaborators
Policies
Last modified
Microsoft OneDrive for Business
1 policy match
Jan 20, 2019
URL: https://181031inovitdemos-my.sharepoint.com/personal/don_hall_inovitdemos_ch/Documents/Human Resources/create samples.xlsx?d=...
Created: Jan 17, 2019
Policies: File containing PII detected in the cloud (built-in DLP engine)
Modified: Jan 20, 2019
Classification labels: CONFIDENTIAL-ALL EMPLOYEES
File size: ~19 KB
Scan status: 1 completed

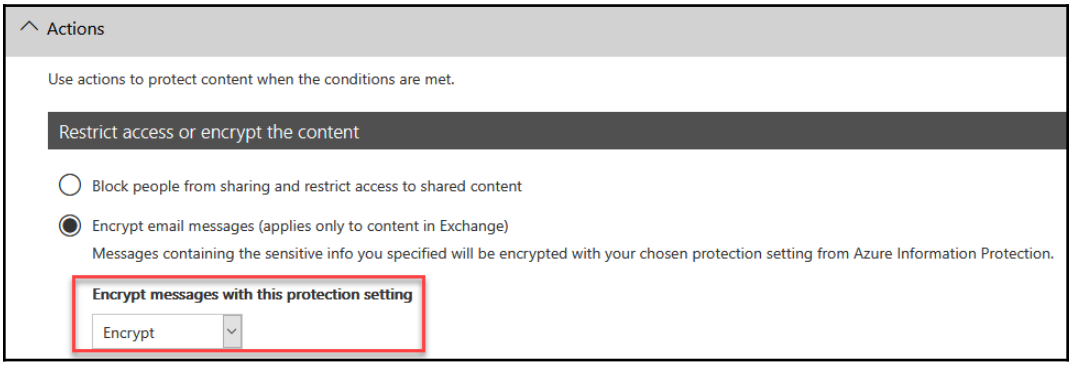

Recommended based on sensitive info detected in your org
Protect sensitive info
Some sensitive info types aren't currently monitored and could be shared accidentally. We recommend creating a data loss prevention (DLP) policy to detect when items containing this sensitive info are shared with people outside your org.
Protected files with sensitive info
Unprotected files with sensitive info
EU Debit Card Number
2 more
View recommendation

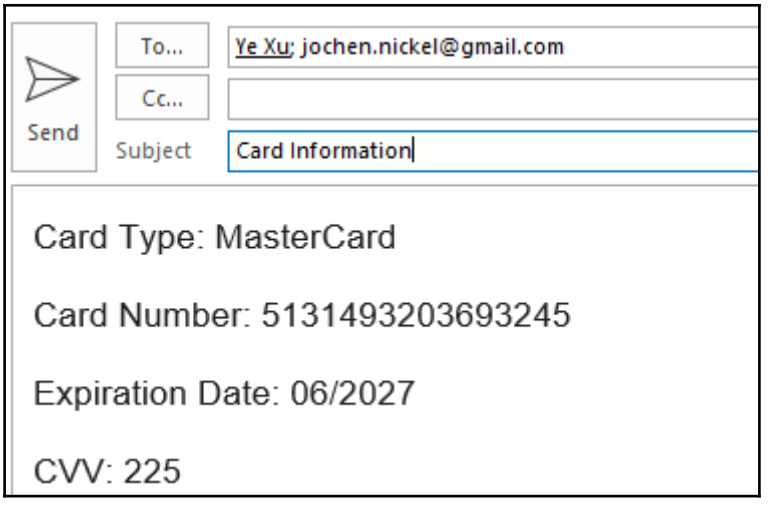

Protect sensitive info
Help prevent leaks of sensitive info by creating a DLP policy that detects when items containing this sensitive info are shared with people outside your org. You'll get detailed activity reports, and you can set up optional notifications to stay informed of potential leaks.
More about DLP Policies
Which sensitive info types do you want to detect?
Applies to items in Sharepoint, OneDrive, Exchange and Teams
EU Debit Card Number
U.S. / U.K. Passport Number
Credit Card Number
What happens when the selected info types are shared outside your org? (optional)
In addition to detailed activity reports, you can get optional notifications. Edit this policy later to add more protection like automatically restricting who can access shared content.
Show a policy tip to anyone who is about to share these protected info types
About policies
Send me email when 5 or more instances of these sensitive info types are shared
Add others to the email

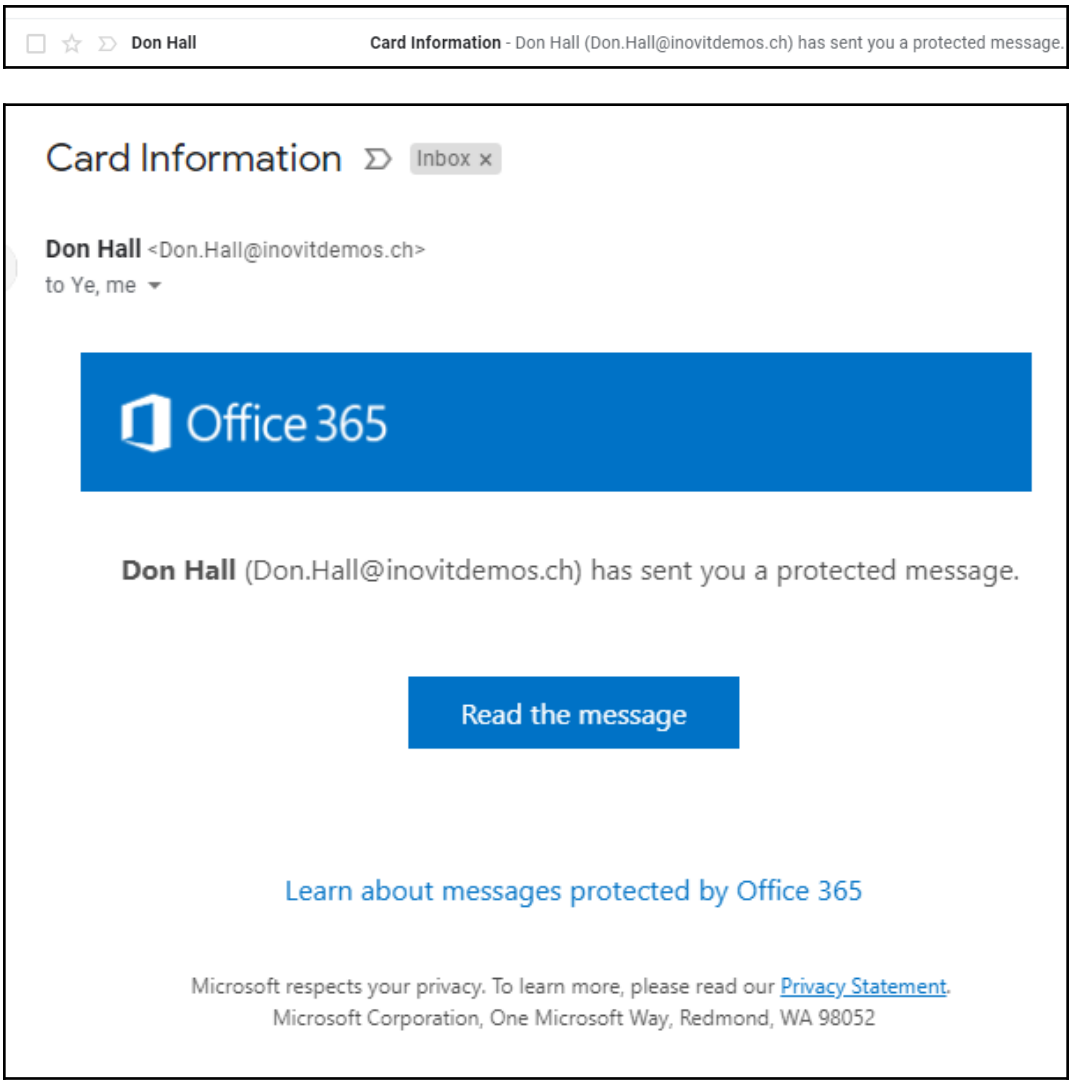

Create a policy
Refresh
Search
Name
Order
Default Data Loss Protection Policy
0

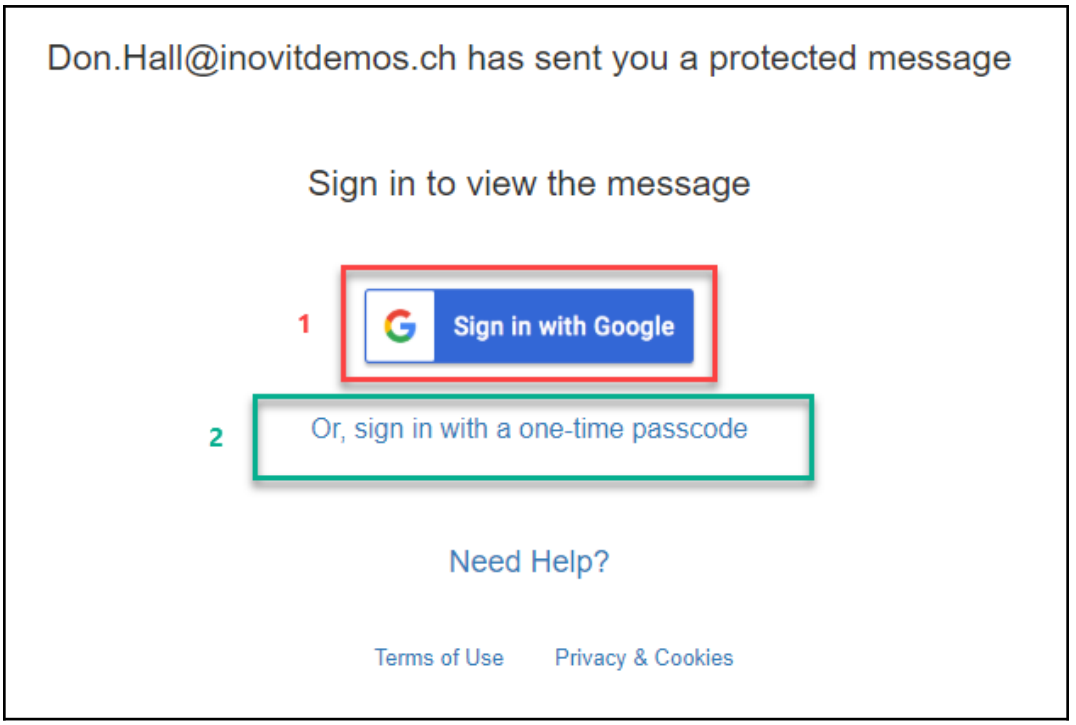

Rule for Low volume of sensitive content detected
1
Edit rule
Delete rule
Conditions
Detect content that's shared
with people outside my organization
Sensitive info types
EU Debit Card Number
U.S. / U.K. Passport Number
Credit Card Number
Actions
Notify users with email and policy tips

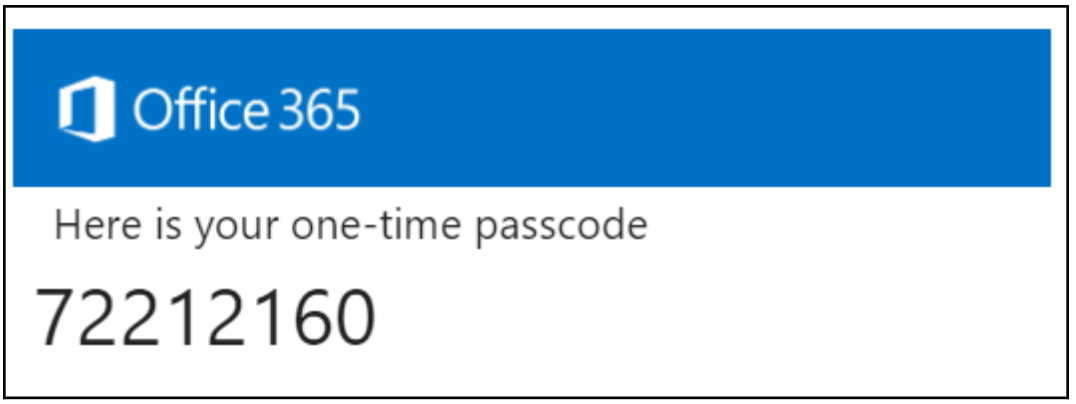

Status
Location
Include
Exclude
Exchange email
All
Choose distribution groups
None
Exclude distribution groups
SharePoint sites
OneDrive accounts

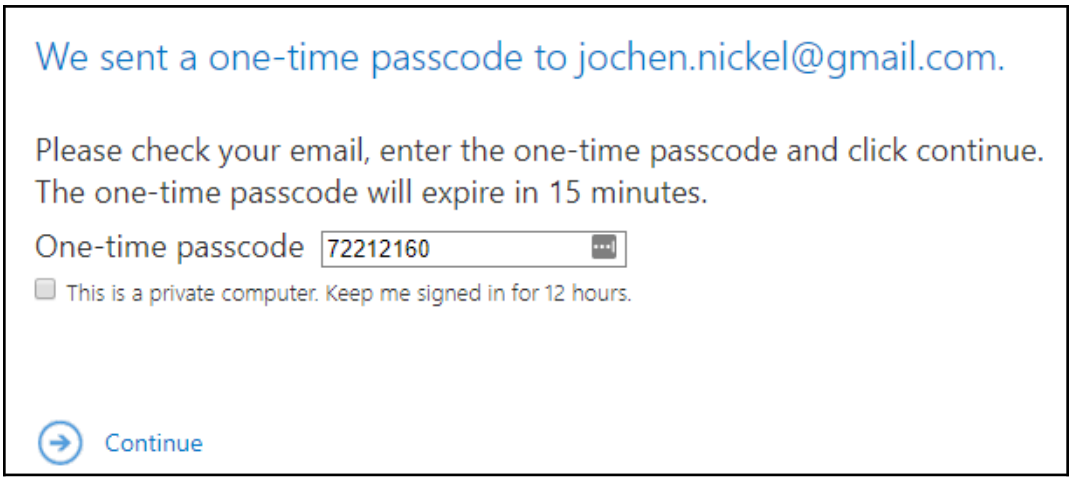

Actions
Use actions to protect content when the conditions are met.
Restrict access or encrypt the content
Block people from sharing and restrict access to shared content
Encrypt email messages (applies only to content in Exchange)
Messages containing the sensitive info you specified will be encrypted with your chosen protection setting from Azure Information Protection.
Encrypt messages with this protection setting
Encrypt

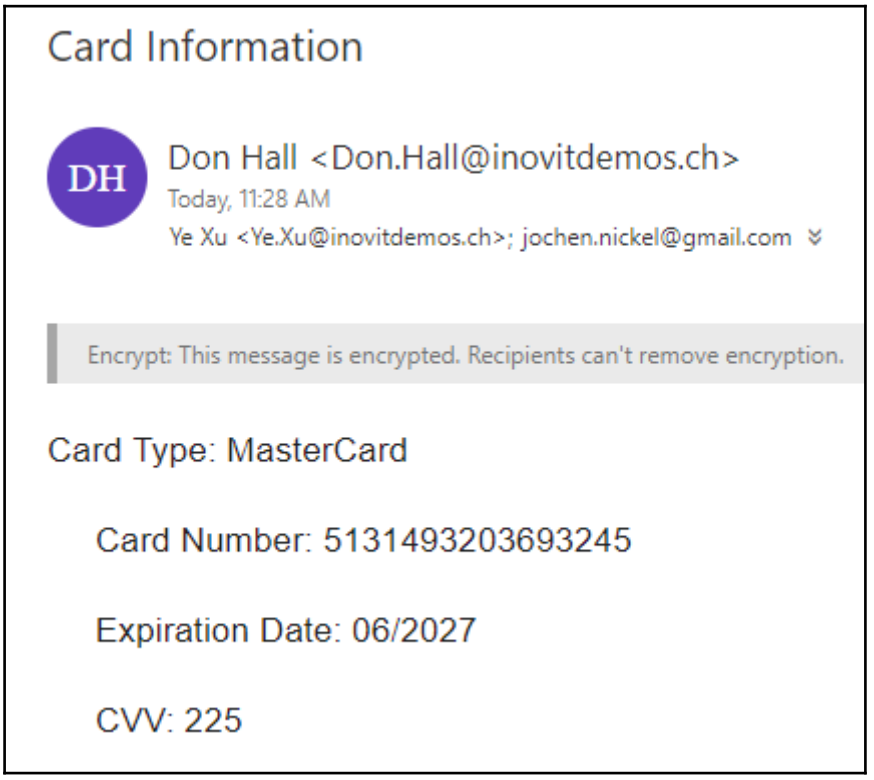

Send
To...
Ye Xu; jochen.nickel@gmail.com
Cc...
Subject
Card Information
Card Type: MasterCard
Card Number: 5131493203693245
Expiration Date: 06/2027
CVV: 225

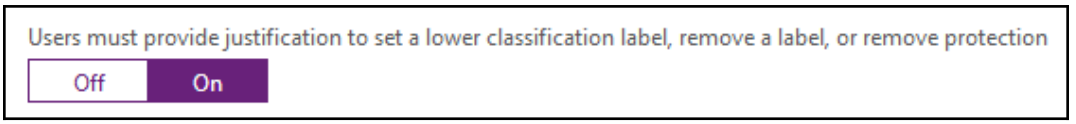

Don Hall
Card Information - Don Hall (Don.Hall@inovitdemos.ch) has sent you a protected message.
Card Information
Inbox ×
Don Hall <Don.Hall@inovitdemos.ch>
to Ye, me
Office 365
Don Hall (Don.Hall@inovitdemos.ch) has sent you a protected message.
Read the message
Learn about messages protected by Office 365
Microsoft respects your privacy. To learn more, please read our Privacy Statement.
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

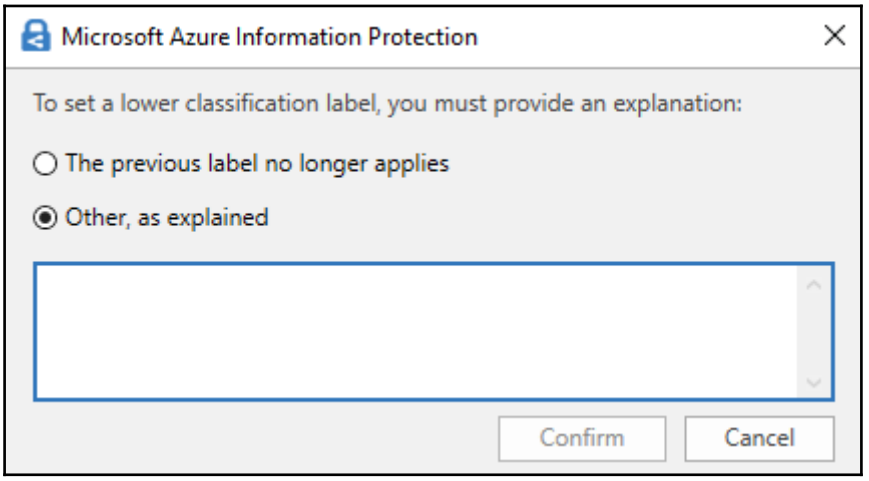

Don.Hall@inovitdemos.ch has sent you a protected message
Sign in to view the message
1
Sign in with Google
2
Or, sign in with a one-time passcode
Need Help?
Terms of Use
Privacy & Cookies

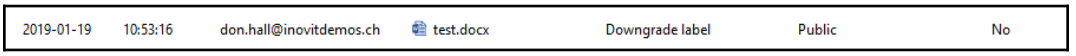

Office 365
Here is your one-time passcode
72212160

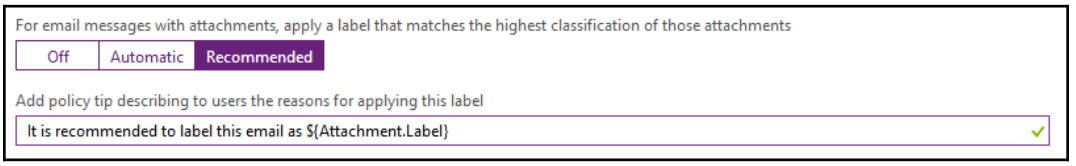

We sent a one-time passcode to jochen.nickel@gmail.com.
Please check your email, enter the one-time passcode and click continue.
The one-time passcode will expire in 15 minutes.
One-time passcode
72212160
This is a private computer. Keep me signed in for 12 hours.
Continue

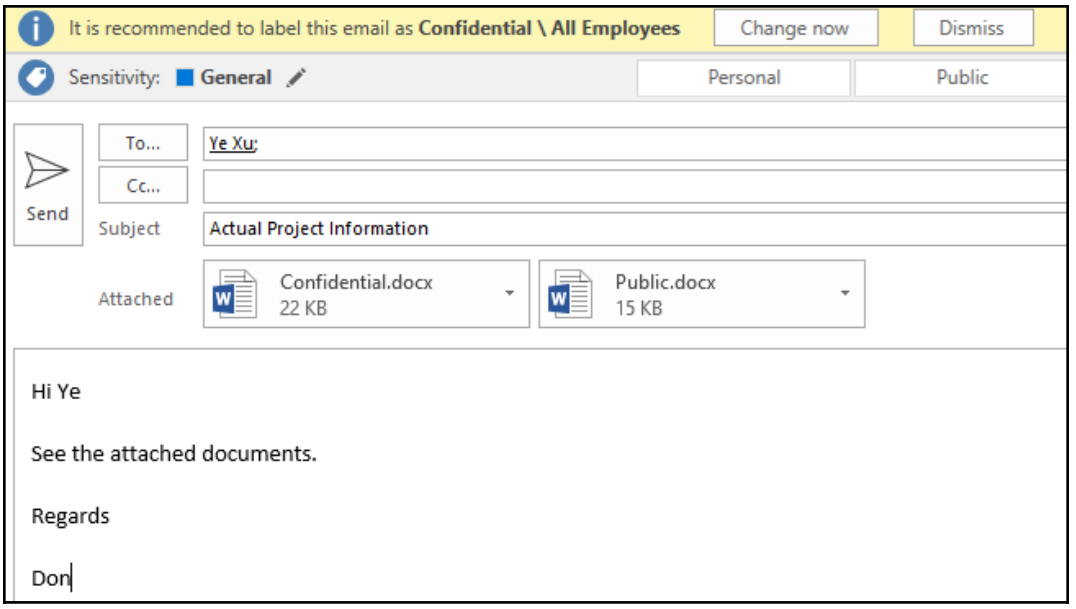

Card Information
DH
Don Hall <Don.Hall@inovitdemos.ch>
Today, 11:28 AM
Ye Xu <Ye.Xu@inovitdemos.ch>; jochen.nickel@gmail.com
Encrypt: This message is encrypted. Recipients can't remove encryption.
Card Type: MasterCard
Card Number: 5131493203693245
Expiration Date: 06/2027
CVV: 225

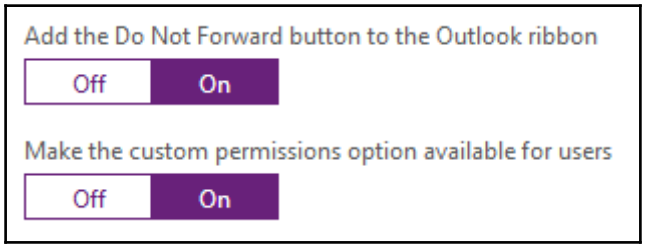

Users must provide justification to set a lower classification label, remove a label, or remove protection
Off
On

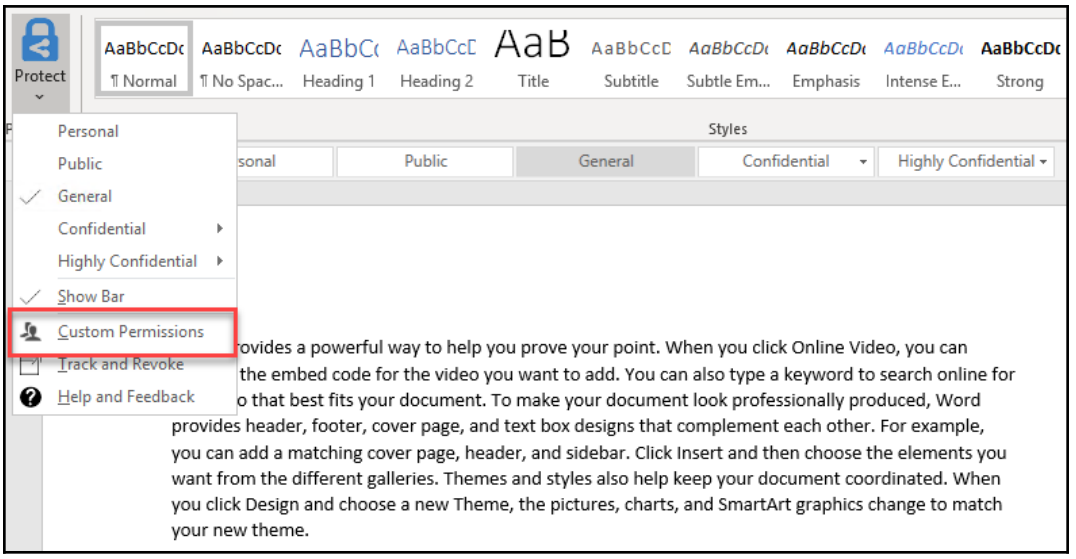

Microsoft Azure Information Protection
To set a lower classification label, you must provide an explanation:
The previous label no longer applies
Other, as explained
Confirm
Cancel

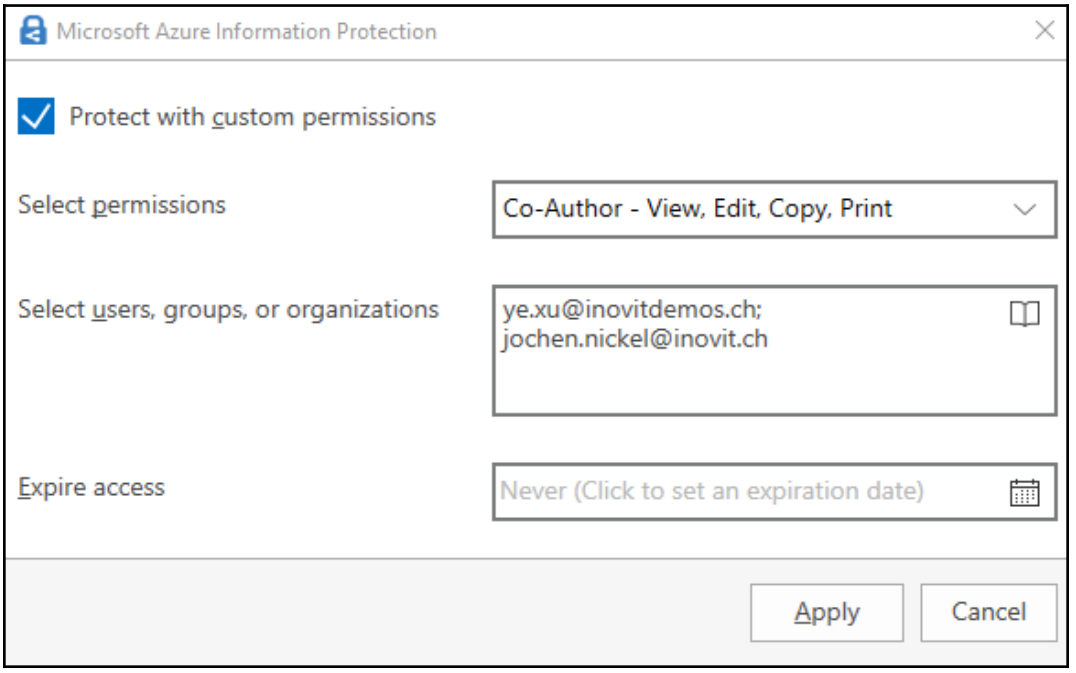

2019-01-19 10:53:16 don.hall@inovitdemos.ch test.docx Downgrade label Public No

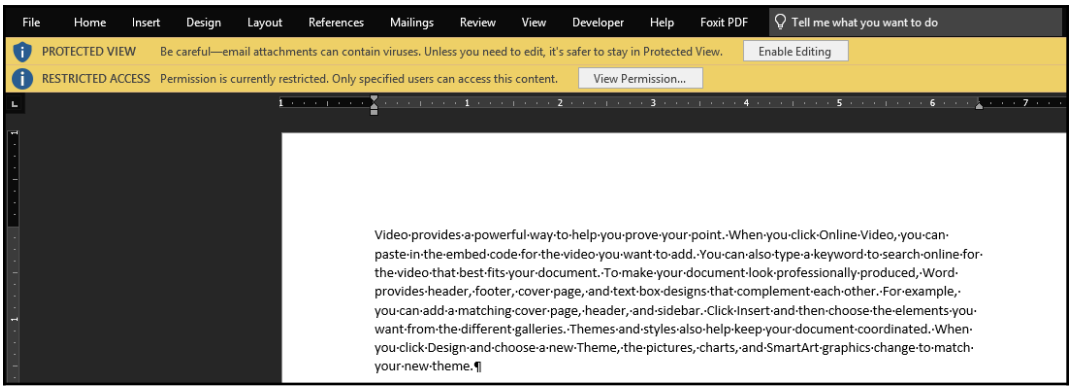

For email messages with attachments, apply a label that matches the highest classification of those attachments
Off
Automatic
Recommended
Add policy tip describing to users the reasons for applying this label
It is recommended to label this email as ${Attachment.Label}

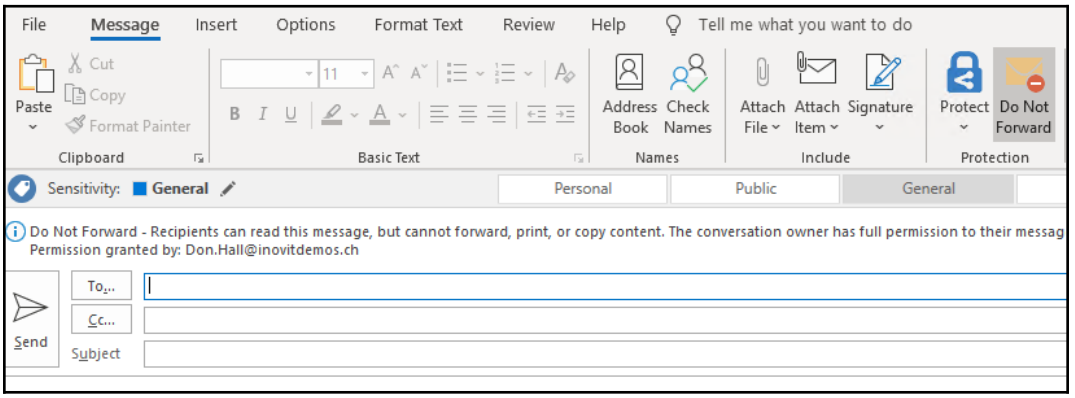

It is recommended to label this email as Confidential \ All Employees
Change now
Dismiss
Sensitivity: General
Personal
Public
Send
To...
Ye Xu;
Cc...
Subject
Actual Project Information
Attached
Confidential.docx
22 KB
Public.docx
15 KB
Hi Ye
See the attached documents.
Regards
Don

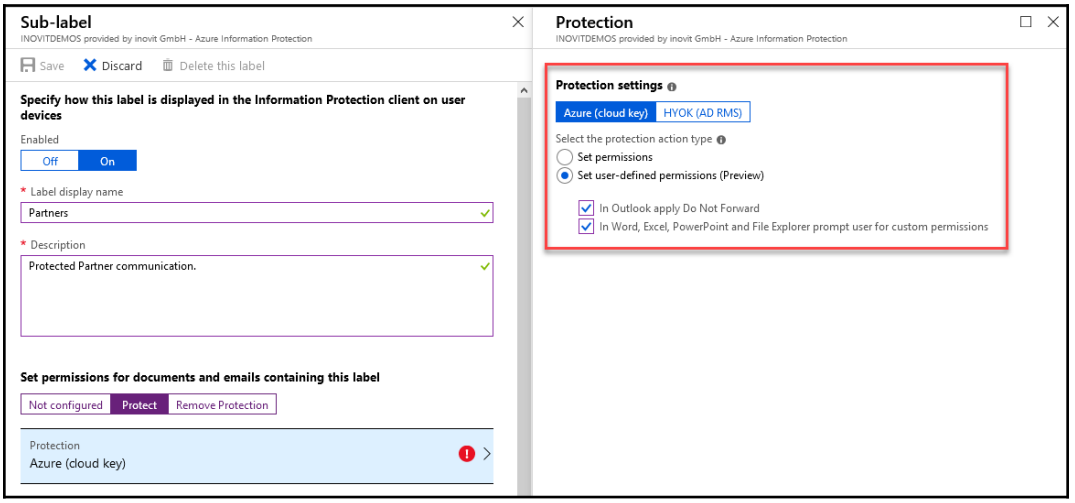

Add the Do Not Forward button to the Outlook ribbon
Off
On
Make the custom permissions option available for users
Off
On

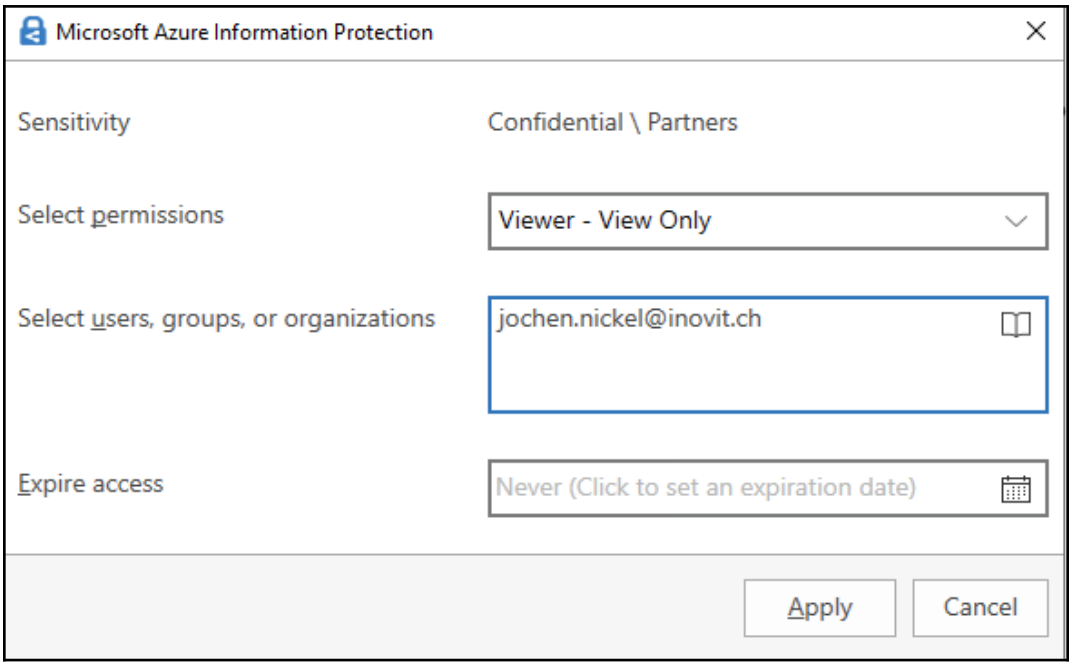

Protect
AaBbCcDc ¶ Normal
AaBbCcDc ¶ No Spac...
AaBbC Heading 1
AaBbCcE Heading 2
AaB Title
AaBbCcE Subtitle
AaBbCcDc Subtle Em...
AaBbCcDc Emphasis
AaBbCcDc Intense E...
AaBbCcDc Strong
Styles
Personal
Public
General
Confidential
Highly Confidential
Show Bar
Custom Permissions
Track and Revoke
Help and Feedback
Public
General
Confidential
Highly Confidential
ovides a powerful way to help you prove your point. When you click Online Video, you can
the embed code for the video you want to add. You can also type a keyword to search online for
o that best fits your document. To make your document look professionally produced, Word
provides header, footer, cover page, and text box designs that complement each other. For example,
you can add a matching cover page, header, and sidebar. Click Insert and then choose the elements you
want from the different galleries. Themes and styles also help keep your document coordinated. When
you click Design and choose a new Theme, the pictures, charts, and SmartArt graphics change to match
your new theme.

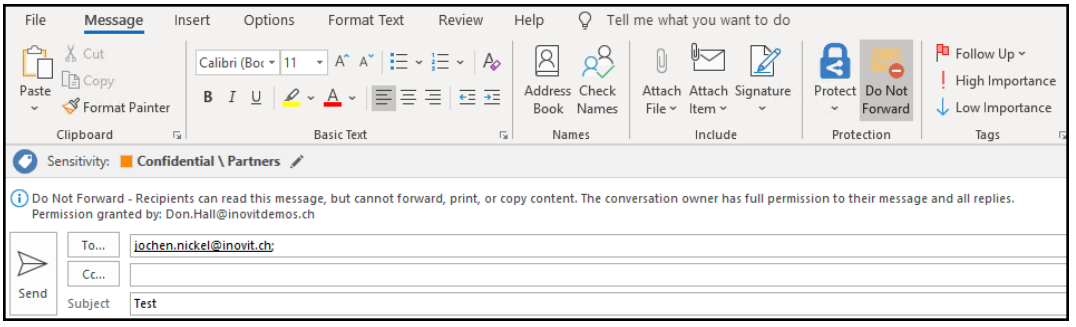

Microsoft Azure Information Protection
Protect with custom permissions
Select permissions
Co-Author - View, Edit, Copy, Print
Select users, groups, or organizations
ye.xu@inovitdemos.ch;
jochen.nickel@inovit.ch
Expire access
Never (Click to set an expiration date)
Apply
Cancel

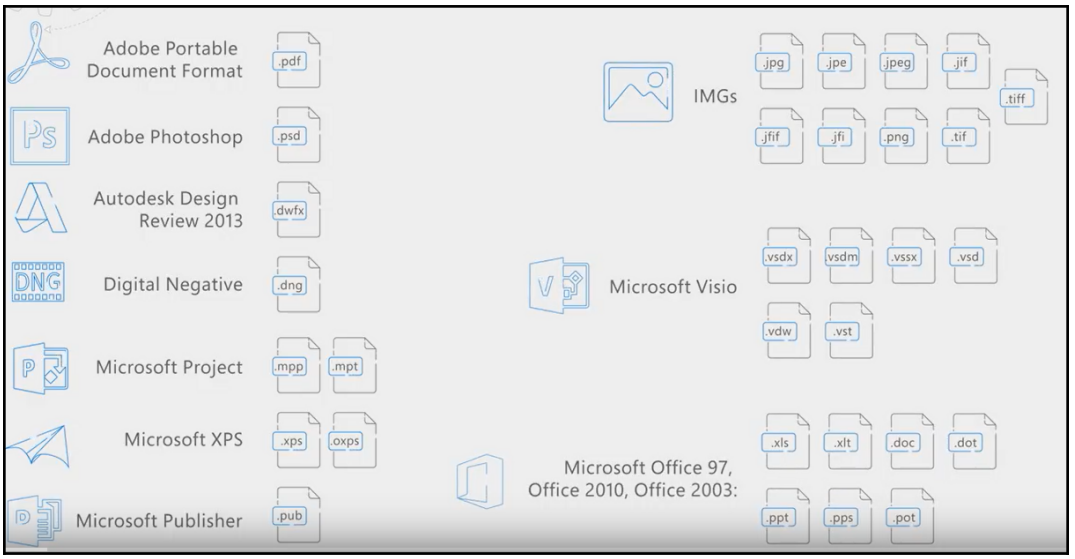

File Home Insert Design Layout References Mailings Review View Developer Help Foxit PDF Tell me what you want to do
PROTECTED VIEW Be careful—email attachments can contain viruses. Unless you need to edit, it's safer to stay in Protected View. Enable Editing
RESTRICTED ACCESS Permission is currently restricted. Only specified users can access this content. View Permission...
Video·provides·a·powerful·way·to·help·you·prove·your·point.·When·you·click·Online·Video,·you·can·paste·in·the·embed·code·for·the·video·you·want·to·add.·You·can·also·type·a·keyword·to·search·online·for·the·video·that·best·fits·your·document.·To·make·your·document·look·professionally·produced,·Word·provides·header,·footer,·cover·page,·and·text·box·designs·that·complement·each·other.·For·example,·you·can·add·a·matching·cover·page,·header,·and·sidebar.·Click·Insert·and·then·choose·the·elements·you·want·from·the·different·galleries.·Themes·and·styles·also·help·keep·your·document·coordinated.·When·you·click·Design·and·choose·a·new·Theme,·the·pictures,·charts,·and·SmartArt·graphics·change·to·match·your·new·theme.¶

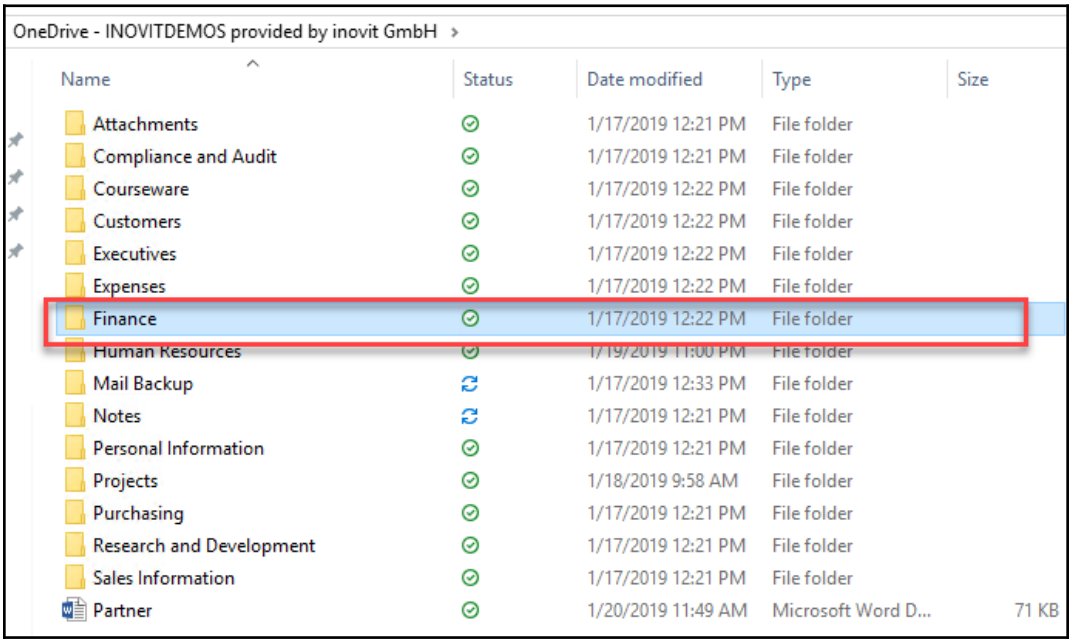

File Message Insert Options Format Text Review Help Tell me what you want to do
Paste Cut Copy Format Painter
Clipboard
Basic Text
Address Book Check Names
Names
Attach File Attach Item Signature
Include
Protect Do Not Forward
Protection
Sensitivity: General
Personal Public General
Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their messag
Permission granted by: Don.Hall@inovitdemos.ch
Send
To...
Cc...
Subject

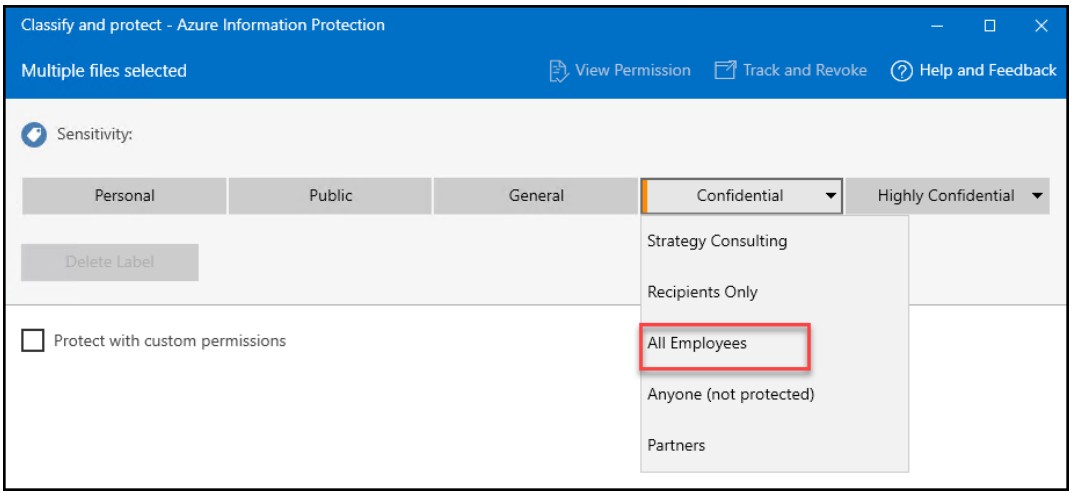

Sub-label
INOVITDEMOS provided by inovit GmbH - Azure Information Protection
Save Discard Delete this label
Specify how this label is displayed in the Information Protection client on user devices
Enabled
Off On
* Label display name
Partners
* Description
Protected Partner communication.
Set permissions for documents and emails containing this label
Not configured Protect Remove Protection
Protection
Azure (cloud key)
Protection
INOVITDEMOS provided by inovit GmbH - Azure Information Protection
Protection settings
Azure (cloud key) HYOK (AD RMS)
Select the protection action type
Set permissions
Set user-defined permissions (Preview)
In Outlook apply Do Not Forward
In Word, Excel, PowerPoint and File Explorer prompt user for custom permissions

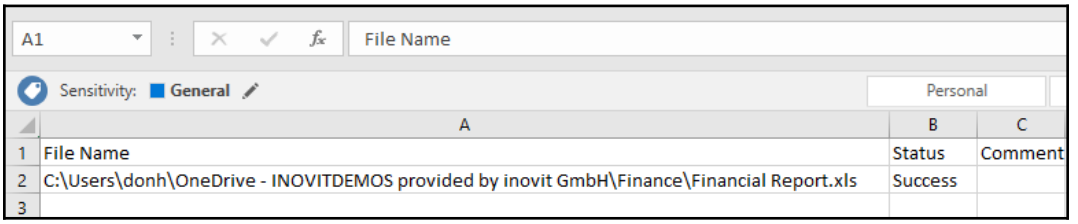

Microsoft Azure Information Protection
Sensitivity
Confidential \ Partners
Select permissions
Viewer - View Only
Select users, groups, or organizations
jochen.nickel@inovit.ch
Expire access
Never (Click to set an expiration date)
Apply
Cancel

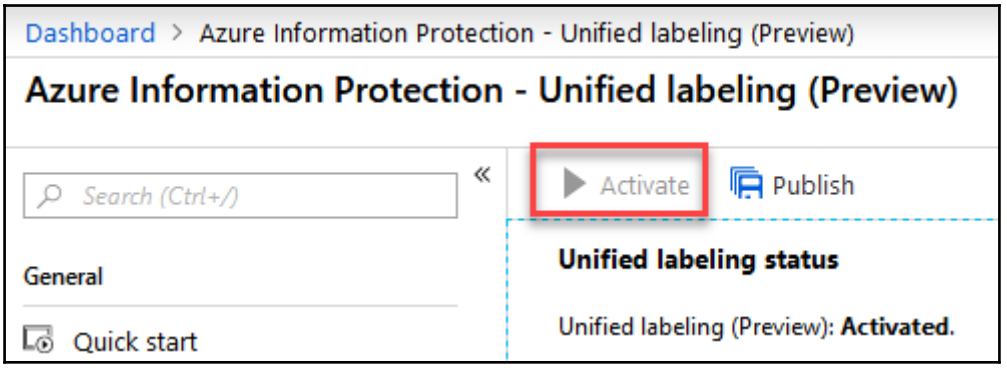

File
Message
Insert
Options
Format Text
Review
Help
Tell me what you want to do
Paste
Cut
Copy
Format Painter
Clipboard
Basic Text
Address Book
Check Names
Names
Attach File
Attach Item
Signature
Include
Protect
Do Not Forward
Protection
Follow Up
High Importance
Low Importance
Tags
Sensitivity: Confidential \ Partners
Do Not Forward - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies.
Permission granted by: Don.Hall@inovitdemos.ch
Send
To...
jochen.nickel@inovit.ch;
Cc...
Subject
Test


Adobe Portable Document Format
.pdf
Adobe Photoshop
.psd
Autodesk Design Review 2013
.dwfx
Digital Negative
.dng
Microsoft Project
.mpp
.mpt
Microsoft XPS
.xps
.oxps
Microsoft Publisher
.pub
IMGs
.jpg
.jpe
.jpeg
.jif
.tiff
.jfif
.jfi
.png
.tif
Microsoft Visio
.vsdx
.vsdm
.vssx
.vsd
.vdw
.vst
Microsoft Office 97, Office 2010, Office 2003:
.xls
.xlt
.doc
.dot
.ppt
.pps
.pot

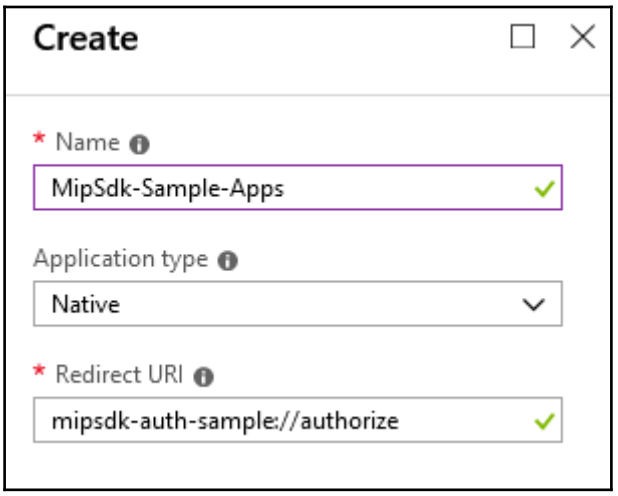

OneDrive - INOVITDEMOS provided by inovit GmbH
Name
Status
Date modified
Type
Size
Attachments 1/17/2019 12:21 PM File folder
Compliance and Audit 1/17/2019 12:21 PM File folder
Courseware 1/17/2019 12:22 PM File folder
Customers 1/17/2019 12:22 PM File folder
Executives 1/17/2019 12:22 PM File folder
Expenses 1/17/2019 12:22 PM File folder
Finance 1/17/2019 12:22 PM File folder
Human Resources
Mail Backup 1/17/2019 12:33 PM File folder
Notes 1/17/2019 12:21 PM File folder
Personal Information 1/17/2019 12:21 PM File folder
Projects 1/18/2019 9:58 AM File folder
Purchasing 1/17/2019 12:21 PM File folder
Research and Development 1/17/2019 12:21 PM File folder
Sales Information 1/17/2019 12:21 PM File folder
Partner 1/20/2019 11:49 AM Microsoft Word D... 71 KB

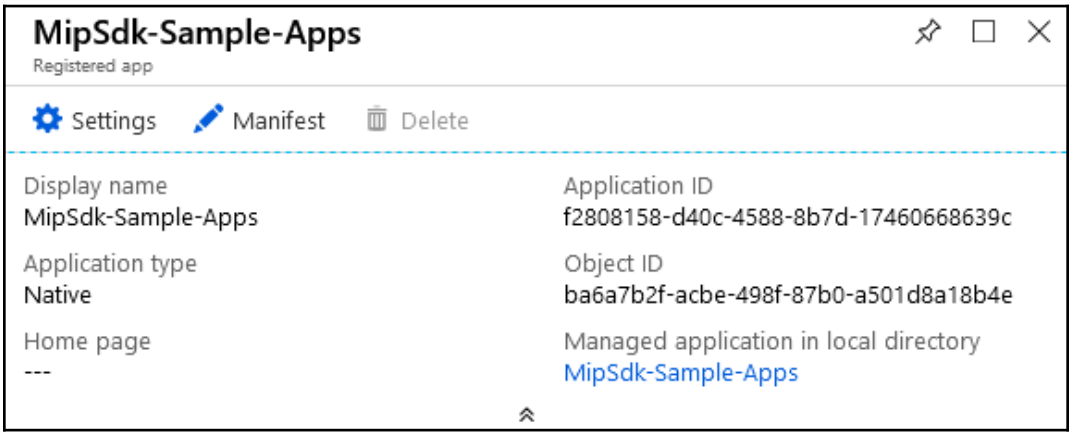

Classify and protect - Azure Information Protection
Multiple files selected
View Permission
Track and Revoke
Help and Feedback
Sensitivity:
Personal
Public
General
Confidential
Highly Confidential
Delete Label
Strategy Consulting
Recipients Only
Protect with custom permissions
All Employees
Anyone (not protected)
Partners

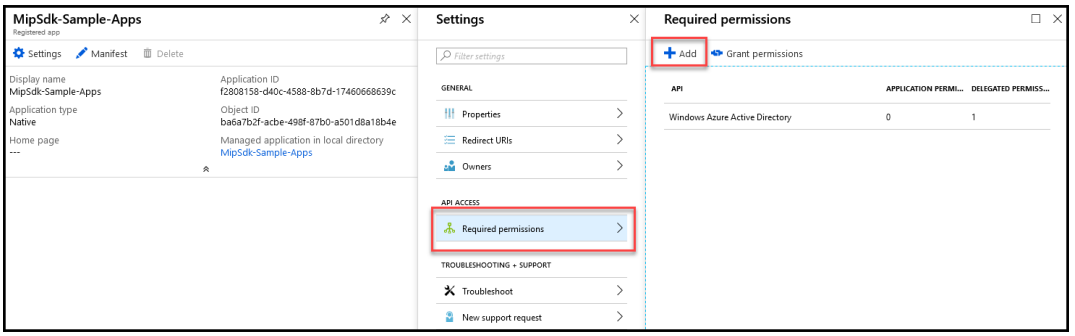

A1
File Name
Sensitivity: General
Personal
A
B
C
1 File Name Status Comment
2 C:\Users\donh\OneDrive - INOVITDEMOS provided by inovit GmbH\Finance\Financial Report.xls Success
3


Dashboard > Azure Information Protection - Unified labeling (Preview)
Azure Information Protection - Unified labeling (Preview)
Search (Ctrl+/)
Activate
Publish
General
Unified labeling status
Quick start
Unified labeling (Preview): Activated.

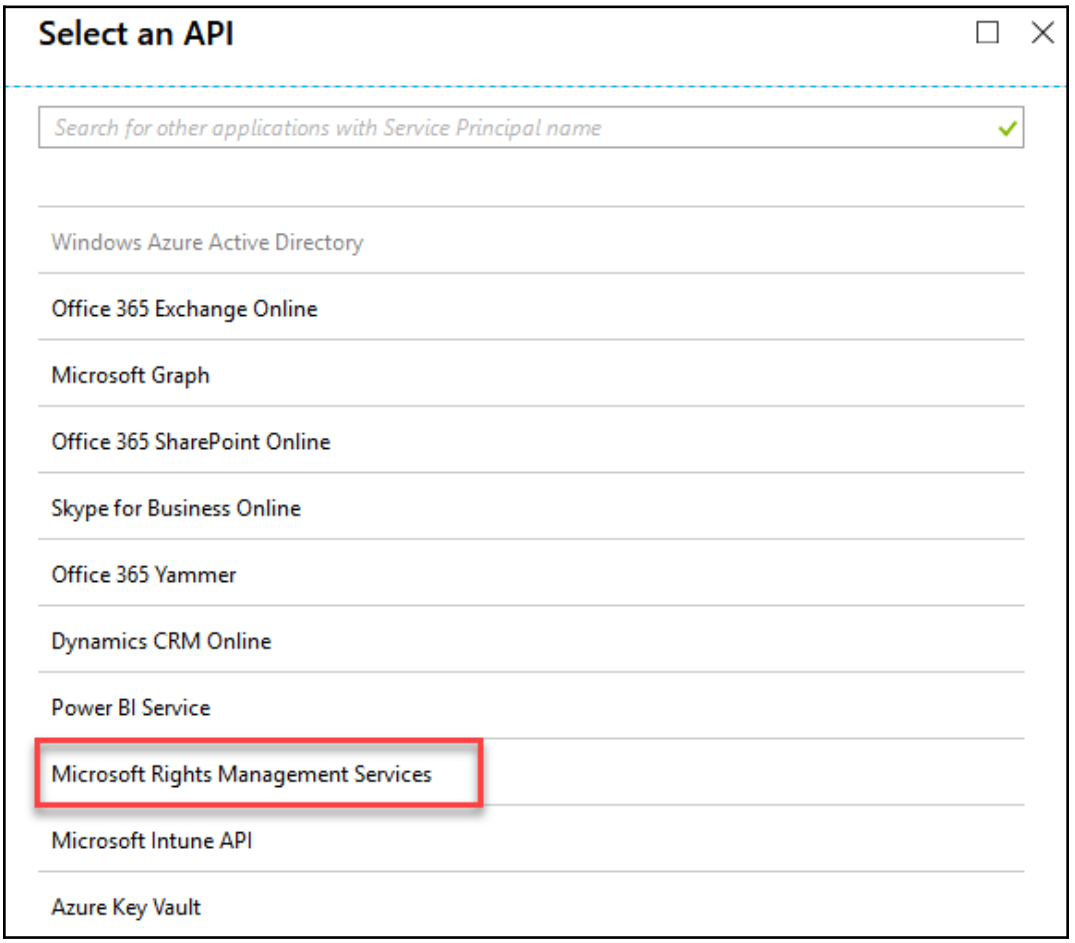
Chapter 16: Azure Information Protection Development

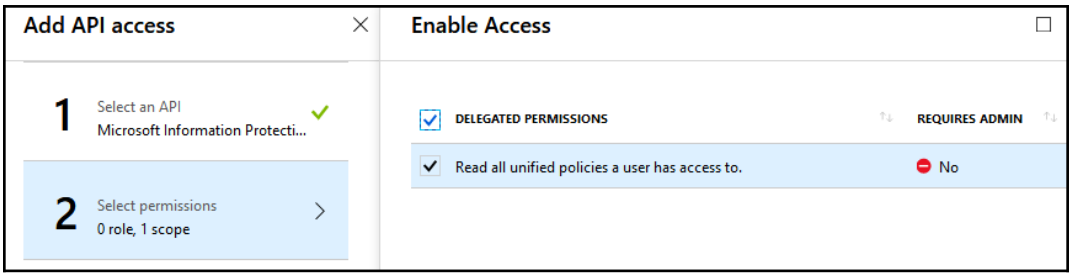


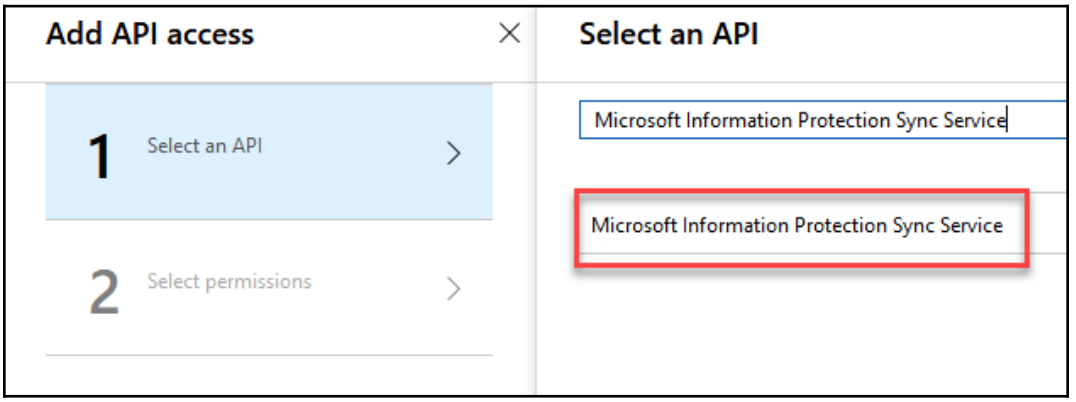



MipSdk-Sample-Apps
Registered app
Settings
Manifest
Delete
Display name
MipSdk-Sample-Apps
Application ID
f2808158-d40c-4588-8b7d-17460668639c
Application type
Native
Object ID
ba6a7b2f-acbe-498f-87b0-a501d8a18b4e
Home page

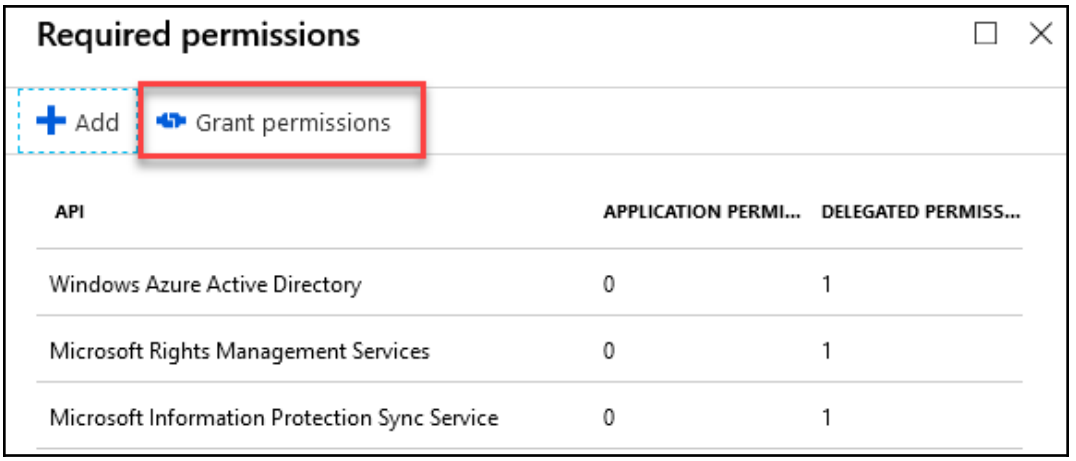
Managed application in local directory
MipSdk-Sample-Apps
Settings
Filter settings
GENERAL
Properties
Redirect URIs
Owners
API ACCESS
Required permissions
TROUBLESHOOTING + SUPPORT
Troubleshoot
New support request
Required permissions
Add
Grant permissions
API
APPLICATION PERMI...
DELEGATED PERMISS...
Windows Azure Active Directory
0
1


Select an API
Search for other applications with Service Principal name
Windows Azure Active Directory
Office 365 Exchange Online
Microsoft Graph
Office 365 SharePoint Online
Skype for Business Online
Office 365 Yammer
Dynamics CRM Online
Power BI Service
Microsoft Rights Management Services
Microsoft Intune API
Azure Key Vault


Add API access
1
Select an API
Microsoft Information Protecti...
2
Select permissions
0 role, 1 scope
Enable Access
DELEGATED PERMISSIONS
REQUIRES ADMIN
Read all unified policies a user has access to.
No


Add API access
1
Select an API
2
Select permissions
Select an API
Microsoft Information Protection Sync Service
Microsoft Information Protection Sync Service


1
Select an API
Microsoft Rights Management ...
2
Select permissions
0 role, 1 scope
DELEGATED PERMISSIONS
REQUIRES ADMIN
Create and access protected content for users
No




```
54    // Create the mip::ApplicationInfo object.
55    // Client ID should be the client ID registered in Azure AD for your custom application.
56    // Friendly Name should be the name of the application as it should appear in reports.
57    mip::ApplicationInfo appInfo{"f2808158-d40c-4588-8b7d-17460668639c", "MipSdkFileApiCppSampleBasic" };
58
59    // All actions for this tutorial project are implemented in samples::file::Action
60    // Source files are Action.h/cpp.
61    // "File" was chosen because this example is specifically for the MIP SDK File API.
62    // Action's constructor takes in the mip::ApplicationInfo object and uses the client ID for auth.
63    // Username and password are required in this sample as the oauth2 token is obtained via Python script and basic auth.
64    Action action = Action(appInfo, "don.hall@inovitdemos.ch","K[redacted]3");
```

```
PS C:\Python27> .\file_sample.exe
Microsoft Information Protection File SDK Sample Version: 1.0.54
Usage:
  file_sample [OPTION...] <Extra args>

  -f, --file File path          Path to the file to work on.
  -g, --getfilestatus           Show the labels and protection that applies on
                                the file.
  -s, --setlabel arg            Set a label with <labelId>. If downgrading
                                label - will apply <justification message>, if
                                needed and specified.
  -d, --delete                  Delete the current label from the file with
                                <justification message>, if needed and specified.
  -p, --protect arg             Protect with custom permissions protection to
                                comma-separated user list.<rights> as
                                permissions to those users
  -r, --rights arg              Comma-separated list of rights to users
      --templateid arg          Protect using Template ID
  -l, --listlabels              Show all available labels with their ID
                                values.
  -u, --unprotect               Remove protection from the given file.
      --standard                The label will be standard label adn will
                                override standard label only.
      --privileged              The label will be privileged label and will
                                override any label.
      --auto                    The label will be standard label and will
```

```
PS C:\> $ServicePrincipalName="RMSPowerShell"
PS C:\> Connect-AadrmService
A connection to the Microsoft Azure AD Rights Management (AADRM) service was opened.
PS C:\> $bposTenantID=(Get-AadrmConfiguration).BPOSId
PS C:\> Disconnect-AadrmService
Connection to the AADRM service closed.
PS C:\> Connect-MsolService
PS C:\> New-MsolServicePrincipal -DisplayName $ServicePrincipalName
The following symmetric key was created as one was not supplied e[redacted]k=


DisplayName           : RMSPowerShell
ServicePrincipalNames : {701[redacted]c936b98d9df4}
ObjectId              : e5df[redacted]a2bbf7041ef
AppPrincipalId        : 7017[redacted]936b98d9df4
TrustedForDelegation  : False
AccountEnabled        : True
Addresses             : {}
KeyType               : Symmetric
KeyId                 : 4c867324-412c-41f5-91c6-e62a8458a72d
StartDate             : 1/22/2019 10:31:47 PM
EndDate               : 1/22/2020 10:31:47 PM
Usage                 : Verify
```

```
$symmetricKey="eGr+Q                                    iMF2Mnj+vk="
$appPrincipalID=(Get-MsolServicePrincipal | Where { $_.DisplayName -eq $ServicePrincipalName }).AppPrincipalId
Set-RMSServerAuthentication -Key $symmetricKey -AppPrincipalId $appPrincipalID -BposTenantId $bposTenantID
```