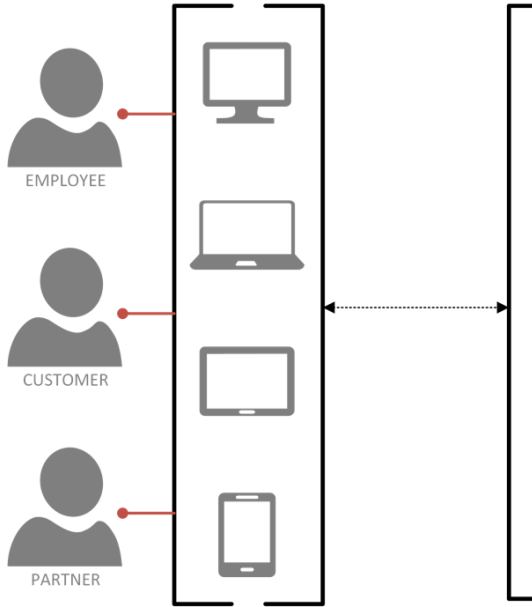


Mastering Identity and Access Management with Microsoft Azure

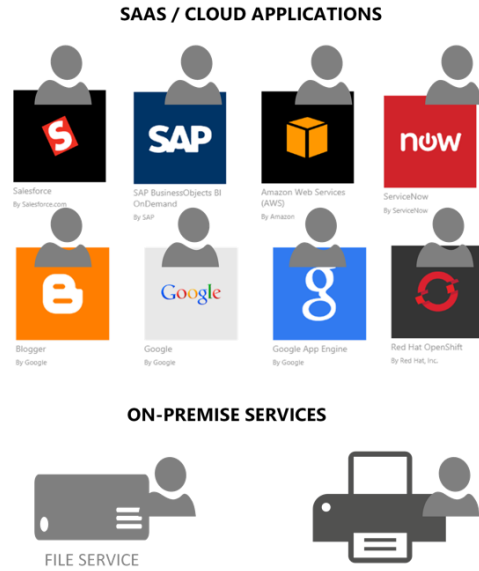
Chapter 1: Getting Started with a Cloud-Only Scenario



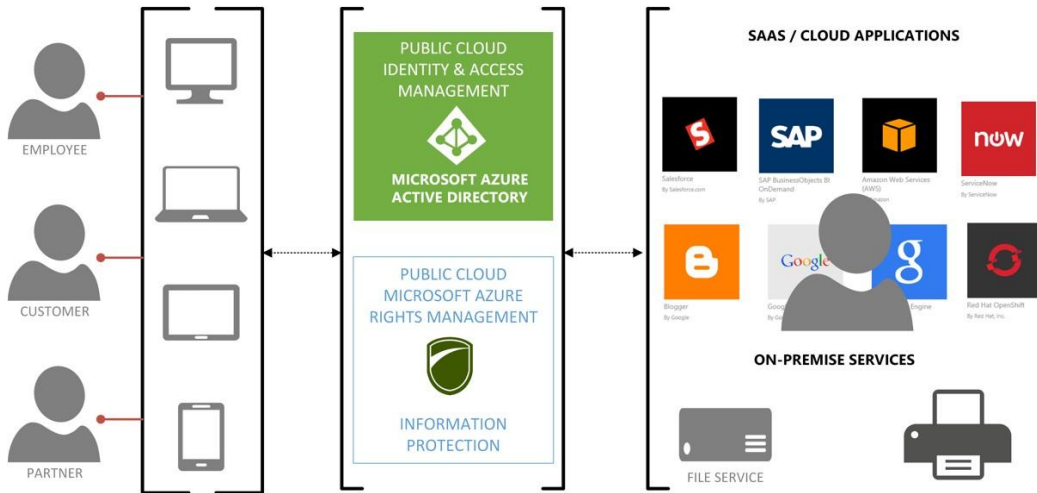
ACCESS FROM ANYWHERE AND ANY DEVICE

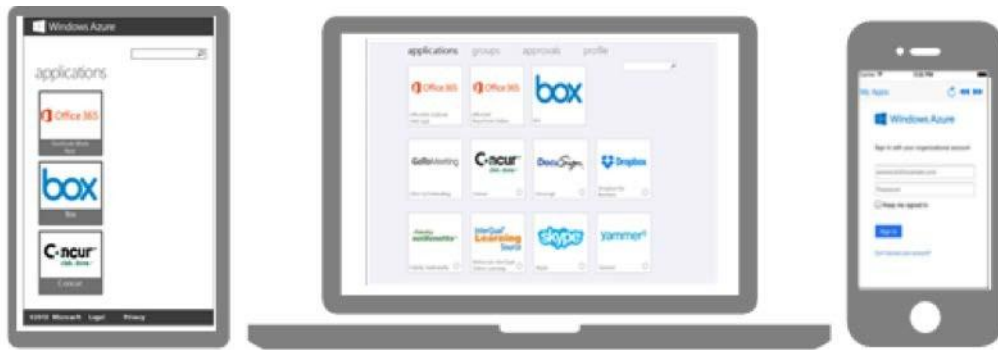


TO BUSINESS SERVICES AND DATA



ACCESS FROM ANYWHERE AND ANY DEVICE MANAGED AND ACCESSED THROUGH AZURE IDAAS TO BUSINESS SERVICES AND DATA








Microsoft Azure

jochen.nickel@inovit.ch | inovit GmbH | ?

applications groups approvals **profile**

 Jochen Nickel		 Change password
USER ID jochen.nickel@inovit.ch	PHONE N/A	 Register for Password Reset
ALTERNATE EMAIL N/A	MOBILE PHONE N/A	
DEPARTMENT N/A	OFFICE N/A	

Microsoft


Get back into your account

Who are you?

To recover your account, begin by entering your user ID and the characters in the picture or audio below.

* User ID:

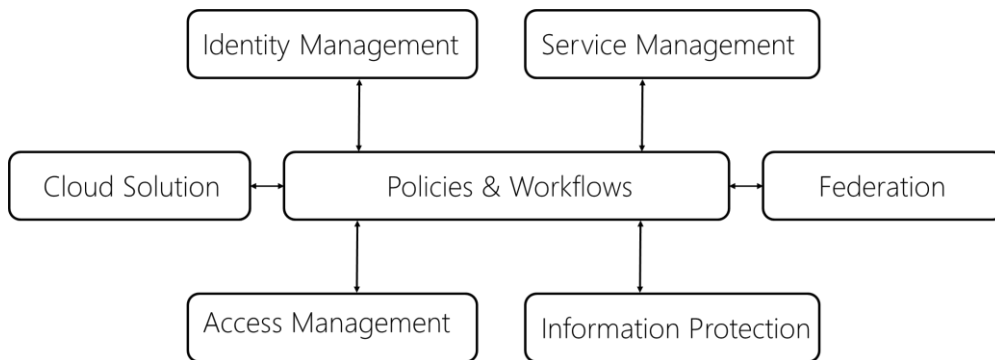
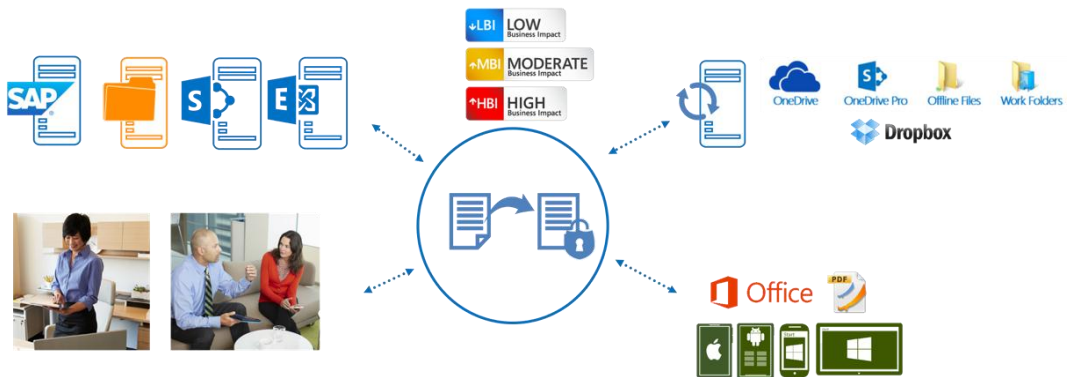
Example: user@contoso.onmicrosoft.com or user@contoso.com



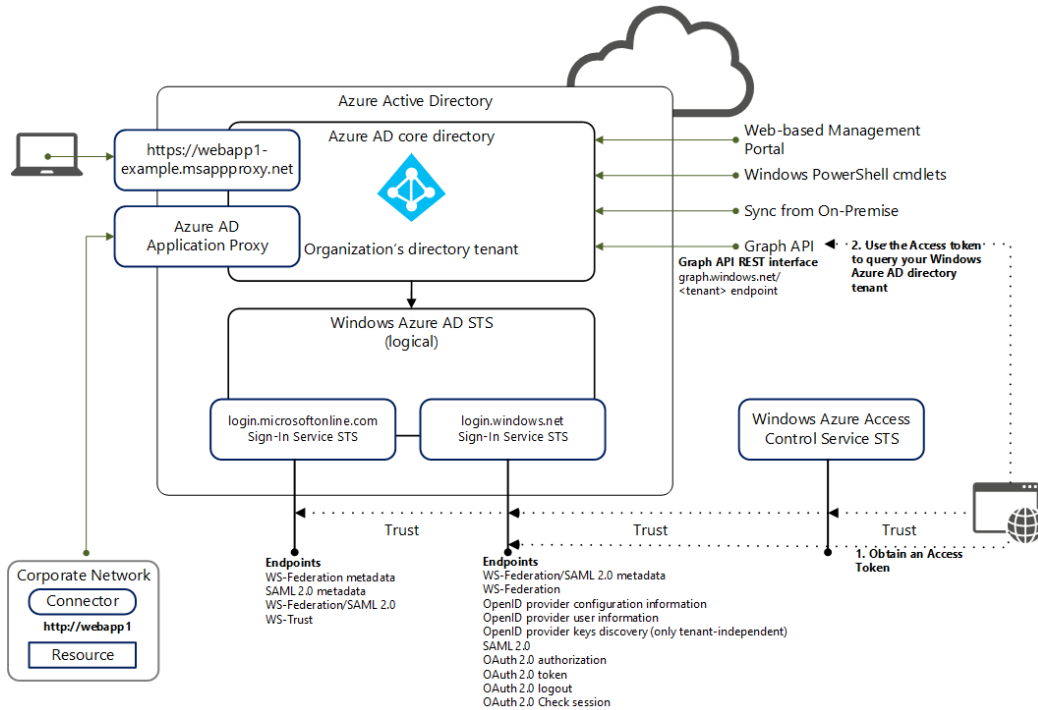
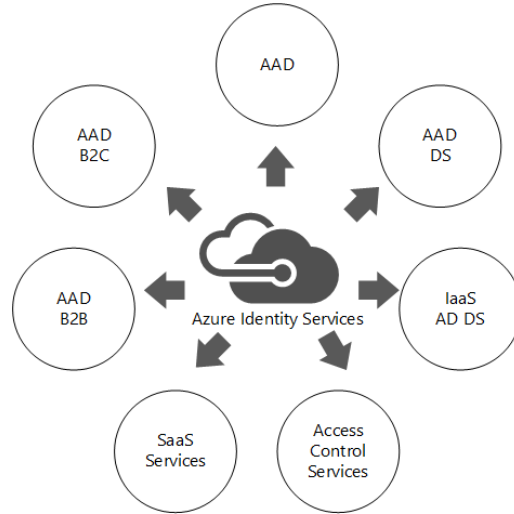
Enter the characters in the picture or the words in the audio.


[Next](#) [Cancel](#)

REPORT	DESCRIPTION
<p>▲ ANOMALOUS ACTIVITY</p>	
Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.
<p>▲ ACTIVITY LOGS</p>	
Audit report	Audited events in your directory
Password reset activity	Provides a detailed view of password resets that occur in your organization.
Password reset registration activity	Provides a detailed view of password reset registrations that occur in your organization.
Groups activity	Provides an activity log to all group related activity in your directory
<p>▲ INTEGRATED APPLICATIONS</p>	
Application usage	Provides a usage summary for all SaaS applications integrated with your directory.
Account provisioning activity	Provides a history of attempts to provision accounts to external applications.
Account provisioning errors	Indicates an impact to users' access to external applications.



Chapter 2: Planning and Designing Cloud Identities



Azure AD Usage Scenarios 

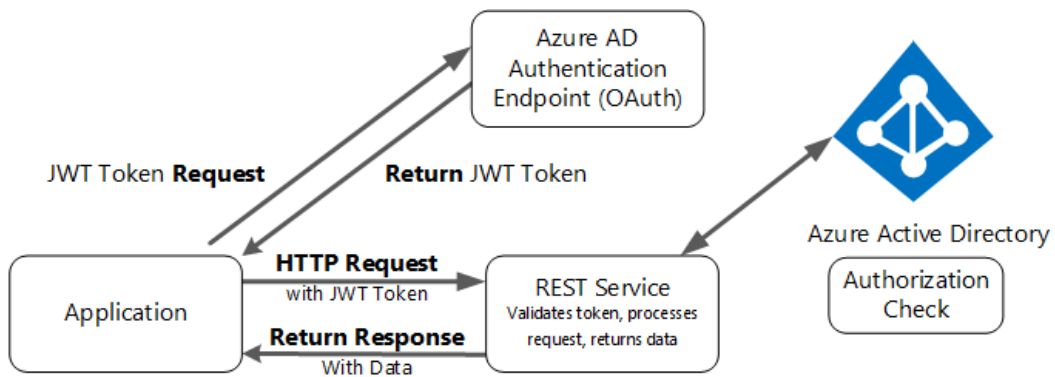
Basic

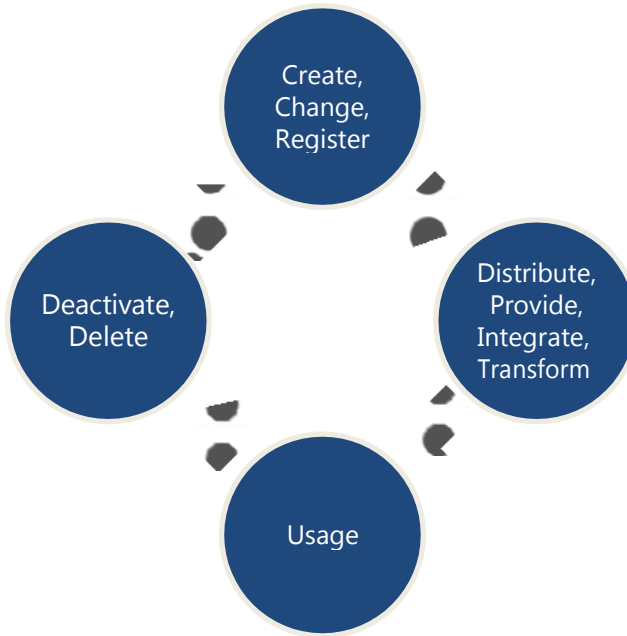
- User Management
- Password Management
- Group Management
- Device Management

Advanced

- Administrative Units Management
- Role-based access Management

Reporting





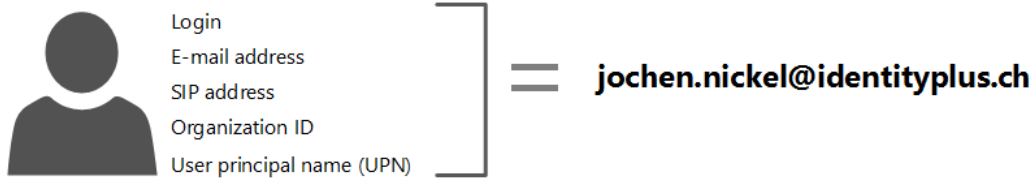
TYPE OF USER

New user in your organization
User with an existing Microsoft account
User in another Microsoft Azure AD directory
Users in partner companies
<input type="text"/> @ identityplus.ch <input type="button" value="v"/>

Jochen Nickel	jochen.nickel@identityplus.ch	Microsoft Azure Active Directory
Jochen Nickel	jochen.nickel@azureid.ch	Local Active Directory
Jochen Nickel	jochen.nickel@outlook.com	Microsoft account
Jochen Nickel	jochen.nickel@identityplus.onmicrosoft.com	Microsoft Azure Active Directory

Jochen Nickel	jochen.nickel@identityplus.ch	Microsoft Azure Active Directory
Jochen Nickel	jochen.nickel@azureid.ch	Local Active Directory
Jochen Nickel	jochen.nickel@outlook.com	Microsoft account
Jochen Nickel	jochen.nickel@identityplus.onmicrosoft.com	Microsoft Azure Active Directory

Jochen Nickel	jochen.nickel@identityplus.ch	Microsoft Azure Active Directory
Jochen Nickel	jochen.nickel@azureid.ch	Local Active Directory
Jochen Nickel	jochen.nickel@outlook.com	Microsoft account
Jochen Nickel	jochen.nickel@identityplus.onmicrosoft.com	Microsoft Azure Active Directory



[DASHBOARD](#)
[USERS](#)
[GROUPS](#)
[APPLICATIONS](#)
[DOMAINS](#)
[DIRECTORY INTEGRATION](#)
[CONFIGURE](#)
[REPORTS](#)
[LICENSES](#)

DISPLAY NAME	USER NAME	SOURCED FROM
Anas Nickel	anas.nickel@azureid.ch	Local Active Directory
Jochen Nickel	jochen.nickel@identityplus.ch	Microsoft Azure Active Directory
Jochen Nickel	jochen.nickel@azureid.ch	Local Active Directory
Jochen Nickel	jochen.nickel@outlook.com	Microsoft account
On-Premises Directory Synchronization Service Account	Sync_AZIDAD501_c4035ede7504@identityplus.onmicrosoft.com	Local Active Directory
Tenant Administrator	admin@identityplus.onmicrosoft.com	Microsoft Azure Active Directory

settings

ALLOW THE USER TO SIGN IN AND ACCESS SERVICES?

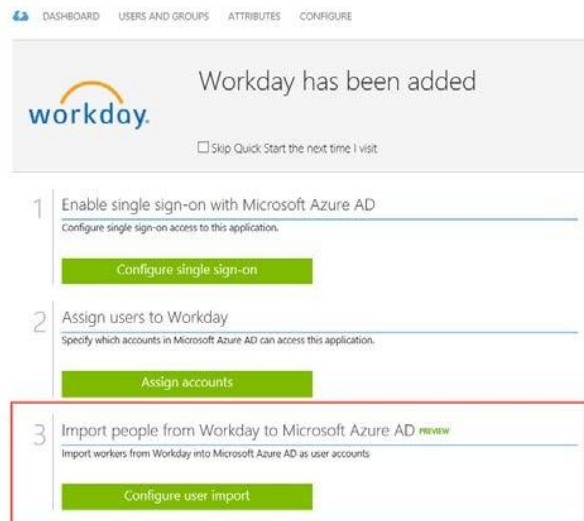
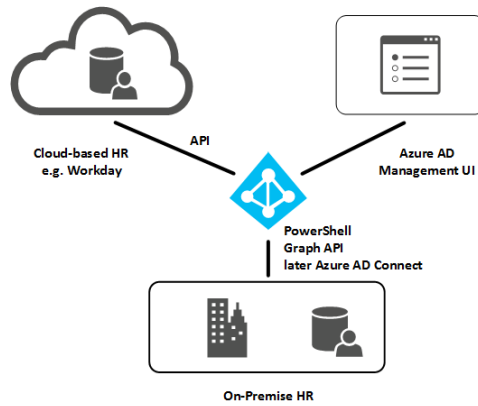
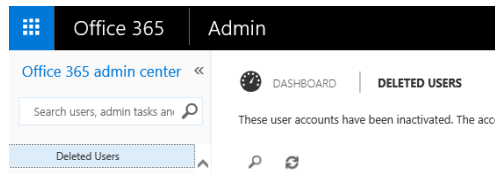
ALLOW BLOCK

Timestamp	Application Name	IP Address	Location	OS
11/25/2015 11:42:57 PM	Microsoft Device Registration Cli...	84.75.23.101	Zuerich, Zuerich, CH	Windows
11/25/2015 11:42:40 PM	Universal Store Native Client	84.75.23.101	Zuerich, Zuerich, CH	Windows
11/25/2015 11:42:37 PM	Accounts Control UI	84.75.23.101	Zuerich, Zuerich, CH	Windows
11/25/2015 11:40:22 PM	Unknown First-Party App	84.75.23.101	Zuerich, Zuerich, CH	Windows
11/25/2015 11:40:05 PM	Device Registration Service	84.75.23.101	Zuerich, Zuerich, CH	Windows

OBJECT ID: 17bc9a00-46bd-49be-b693-baf89bde2b85

MANAGER ID: 17bc9a00-46bd-49be-b693-baf89bde2b85 [VIEW MANAGER](#)

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-Command *user*
CommandType Name Version Source
-----
Function Get-PCoDeviceUserPassword 1.0.0.0 PcsDevice
Cmdlet Add-Admsuperuser 1.0.0.0 AADRM
Cmdlet Add-AzureRemoteAppUser 0.9.7 Azure
Cmdlet Convert-MsOLFederatedUser 1.0 NSOnline
Cmdlet Disable-Admsuperuserfeature 1.0.0.0 AADRM
Cmdlet Enable-Admsuperuserfeature 1.0.0.0 AADRM
Cmdlet Get-Admsuperuser 1.0.0.0 AADRM
Cmdlet Get-Admsuperuserfeature 1.0.0.0 AADRM
Cmdlet Get-AzureRemoteAppUser 0.9.7 Azure
Cmdlet Get-MSolUser 1.0 NSOnline
Cmdlet Get-MSolUser 1.0 NSOnlineExtended
Cmdlet Get-MSolUserByStrongAuthentication 1.0 NSOnline
Cmdlet Get-MSolUserByStrongAuthentication 1.0 NSOnlineExtended
Cmdlet Get-MSolUserRole 1.0 NSOnline
Cmdlet Get-MSolUserRole 1.0 NSOnlineExtended
Cmdlet Get-MSolUserLanguageList 2.0.0.0 International
Cmdlet New-MSolUser 1.0 NSOnlineExtended
Cmdlet New-MSolUserLanguageList 2.0.0.0 International
Cmdlet Redo-MSolProvisionUser 1.0 NSOnline
Cmdlet Redo-MSolProvisionUser 1.0 NSOnlineExtended
Cmdlet Remove-Admsuperuser 1.0.0.0 AADRM
Cmdlet Remove-AzureRemoteAppUser 0.9.7 Azure
Cmdlet Remove-MSolUser 1.0 NSOnline
Cmdlet Remove-MSolUser 1.0 NSOnlineExtended
Cmdlet Restore-MSolUser 1.0 NSOnline
Cmdlet Restore-MSolUser 1.0 NSOnlineExtended
Cmdlet Set-MSolUser 1.0 NSOnline
Cmdlet Set-MSolUser 1.0 NSOnlineExtended
Cmdlet Set-MSolUserLicense 1.0 NSOnline
Cmdlet Set-MSolUserLicense 1.0 NSOnlineExtended
Cmdlet Set-MSolUserPassword 1.0 NSOnline
Cmdlet Set-MSolUserPassword 1.0 NSOnlineExtended
Cmdlet Set-MSolUserPrincipalName 1.0 NSOnline
Cmdlet Set-MSolUserPrincipalName 1.0 NSOnlineExtended
```



2

Enable automatic account provisioning to Salesforce Sandbox

Automatically provision accounts from Microsoft Azure AD to Salesforce Sandbox upon account assignment.

Configure account provisioning

attribute mappings

TARGET ATTRIBUTE (SALESFORCE SAND...	TARGET OBJECT	SOURCE ATTRIBUTE (AZURE AD)	SOURCE OBJECT	REQUIR...	?
IsActive	User	Not([IsSoftDeleted])	User	Yes	
Alias	User	Mid([UserPrincipalName], 1, 8)	User	Yes	
Email	User	mail	User	Yes	
EmailEncodingKey	User	"ISO-8859-1" (default)	-	Yes	
LanguageLocaleKey	User	"en_US" (default)	-	Yes	
FirstName	User	givenName	User	Yes	
LastName	User	surname	User	Yes	
LocaleSidKey	User	Replace([preferredLanguage], "-", "", .)	User	Yes	
ProfileName	User	SingleAppRoleAssignment([appRoleAssignments])	User	Yes	
TimeZoneSidKey	User	"America/Los_Angeles" (default)	-	Yes	
Username	User	userPrincipalName	User	Yes	
UserPermissionsCallCenterAutoLogin	User	"False" (default)	-	Yes	
UserPermissionsMarketingUser	User	"False" (default)	-	Yes	
UserPermissionsOfflineUser	User	"False" (default)	-	Yes	

user password reset policy

USERS ENABLED FOR PASSWORD RESET

 YES NO

RESTRICT ACCESS TO PASSWORD RESET

 YES NO

user password reset policy

USERS ENABLED FOR PASSWORD RESET YES NO ?

RESTRICT ACCESS TO PASSWORD RESET YES NO ?

Before users can reset their passwords, they must first have at least one authentication method defined. [Edit users in 'Identityplus Demo Environment' now.](#)

AUTHENTICATION METHODS AVAILABLE TO USERS ?

- Office Phone
- Mobile Phone
- Alternate Email Address
- Security Questions

NUMBER OF AUTHENTICATION METHODS REQUIRED ?

You can send users to a webpage where they can register their own authentication method information. [Go to this webpage now.](#)

REQUIRE USERS TO REGISTER WHEN SIGNING IN? YES NO ?

NUMBER OF DAYS BEFORE USERS ARE ASKED TO RE-CONFIRM THEIR AUTHENTICATION INFORMATION ?

Microsoft Azure

jochen.nickel@identityplus.ch | ?

don't lose access to your account!

To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. You'll need to set up at least 1 of the options below.

! Authentication Phone is not configured. Set it up now

! Authentication Email is not configured. Set it up now

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

Reset your password

verification step 1 > verification step 2 > choose a new password

Please choose the first contact method we should use for verification:

Email my alternate email

Text my mobile phone

Call my mobile phone

Call my office phone

Answer my security questions

What is your favorite food?

What was the name of your first pet?

What was the make and model of your first car?

Next

Sign in with your work or school account

Keep me signed in

Sign in

Cancel

[Can't access your account?](#)

Get back into your account

Who are you?

To recover your account, begin by entering your user ID and the characters in the picture or audio below.

* User ID:

Example: user@contoso.onmicrosoft.com or user@contoso.com



Enter the characters in the picture or the words in the audio.

Next

Cancel

group management

DELEGATED GROUP MANAGEMENT
ENABLED

 YES NO

USERS CAN CREATE SECURITY GROUPS

 YES NO

USERS WHO CAN USE SELF-SERVICE FOR
SECURITY GROUPS

 ALL SOME

USERS CAN CREATE OFFICE 365 GROUPS

 YES NO

PREVIEW

USERS WHO CAN USE SELF-SERVICE FOR
OFFICE 365 GROUPS

 ALL SOME

ENABLE DEDICATED GROUPS

 YES NO

ENABLE "ALL USERS" GROUP

 YES NO

Create Group



Display name

Sales Team Sharepoint Online

Description (optional)

This group provides access to the Sales team SharePoint Online.








Group policy

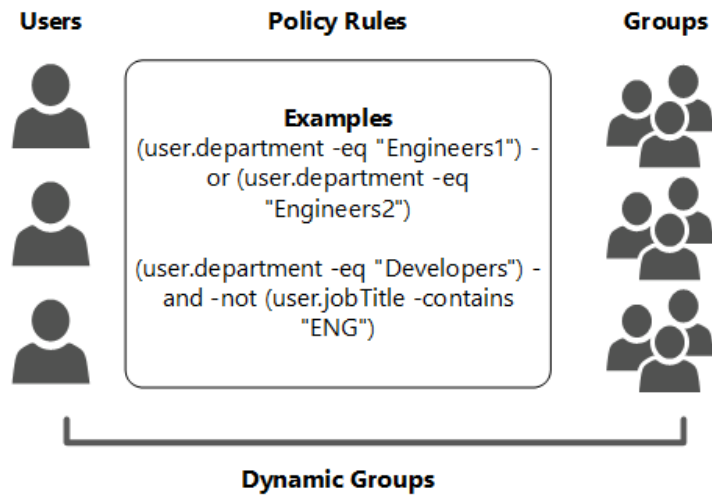
This group requires owner approval

Group type

Security

Create

 Sales Team Sharepoint Online DESCRIPTION This group provides access to the Sales team SharePoint Online. GROUP TYPE Security JOIN POLICY This group requires owner approval OWNERS Jochen Nickel (jochen.nickel@identyplus.ch)	 1 members	 Add member	 Edit
	 Set Owners	 Leave group	 Delete group



sales team sharepoint online

MEMBERS OWNERS PROPERTIES CONFIGURE SELF SERVICE ACTIVITY

dynamic memberships

ENABLE DYNAMIC MEMBERSHIPS

YES NO PREVIEW ?

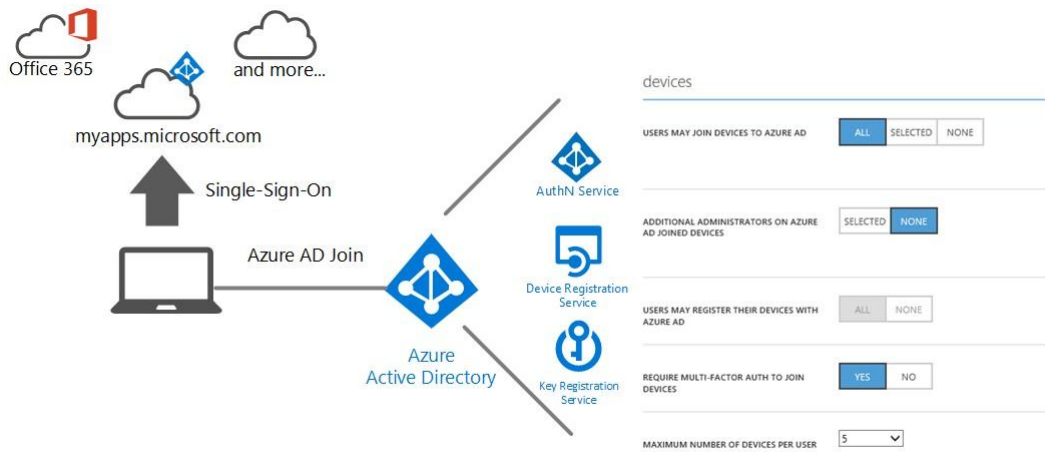
ADD USERS WHERE

department

Equals (-eq)

Sales

ADVANCED RULE

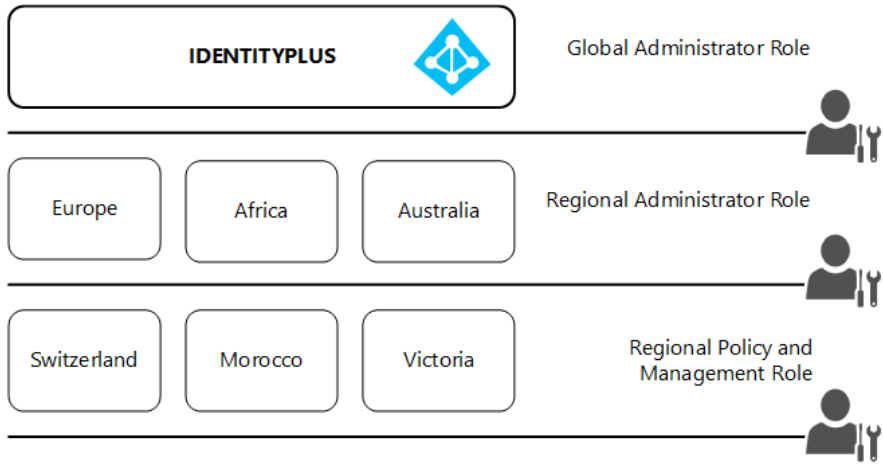
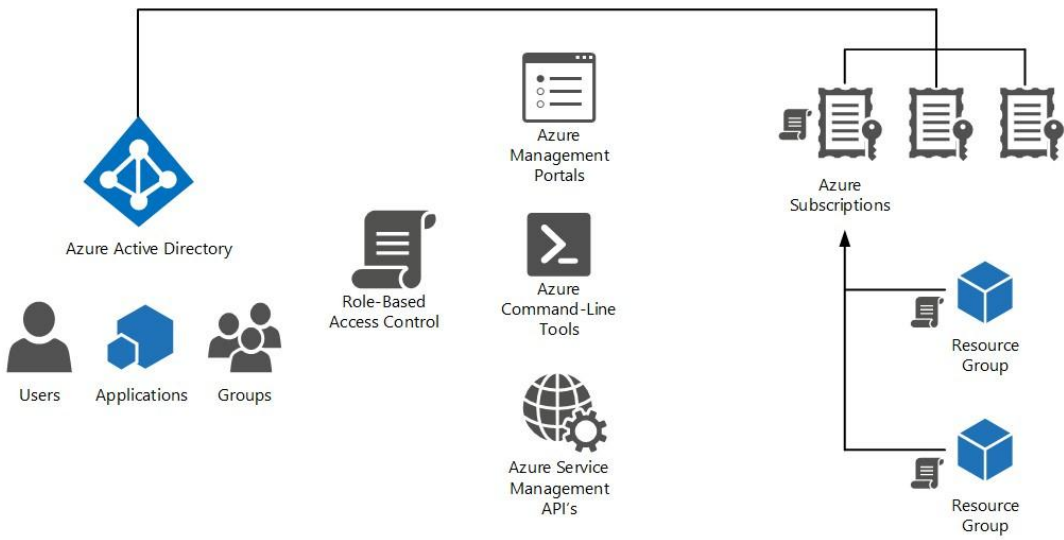


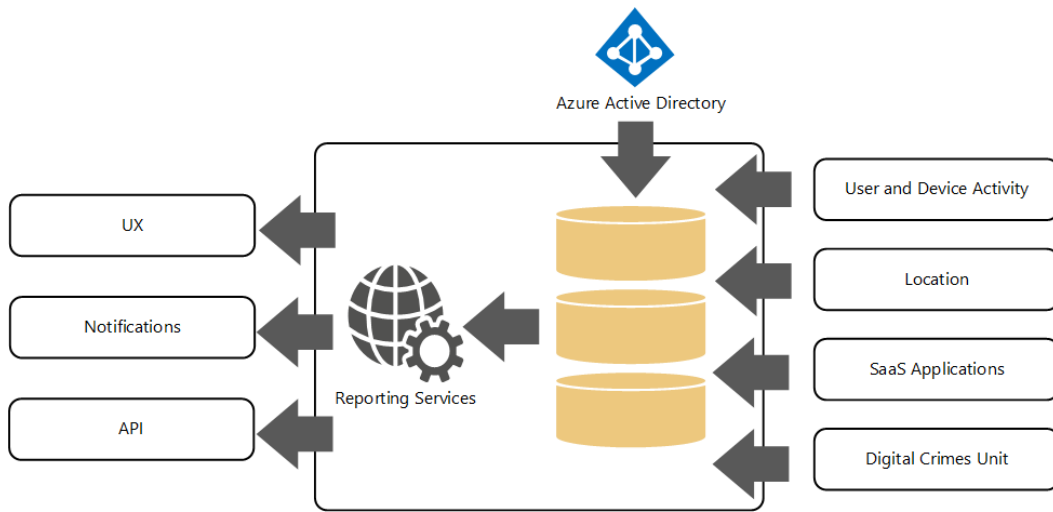
Choose how you'll connect

You can connect Windows to your organization in one of two ways:

- Join Azure AD
- Join a domain

Choose this option if your organization uses Office 365 or other business services from Microsoft. Your organization might collect info about you, install or remove apps, change settings or disable features, delete content, or reset your device. Talk to your support staff to learn more.





SECURITY AND HEALTH STATUS	STATUS (LAST 30 DAYS)	DETAILS	
Users with Anomalous Logins	0	View Anomalous Sign-in Activity	⌵
Application Usage	25	View Application Usage	⌵
Self-Service Password Reset	0	View SSPR Activity	⌵
Self-Service Password Reset Registration	20	View SSPR Registration Activity	
Self-Service Group Management	0	View SSGM Activity	

SEARCH ACTIVITY REPORTS
 FROM TO USER

REPORT	DESCRIPTION
ANOMALOUS ACTIVITY	
Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.
Users with leaked credentials	Users with leaked credentials
Users with threatened credentials	Users with threatened credentials
ACTIVITY LOGS	
Audit report	Audited events in your directory
Password reset activity	Provides a detailed view of password resets that occur in your organization.
Password reset registration activity	Provides a detailed view of password reset registrations that occur in your organization.
Self service groups activity	Provides an activity log to all group self service activity in your directory
INTEGRATED APPLICATIONS	
Application usage	Provides a usage summary for all SaaS applications integrated with your directory.
Account provisioning activity	Provides a history of attempts to provision accounts to external applications.
Password rollover status	Provides a detailed overview of automatic password rollover status of SaaS applications.
Account provisioning errors	Indicates an impact to users' access to external applications.

audit report review

Audited events in your directory

FROM TO

DATE AND TIME	ACTOR	ACTION	TARGET	
11/25/2015 9:36:39 PM	jochen.nicke@identityplus.ch	Change user password.	jochen.nicke@identityplus.ch	
11/25/2015 9:35:47 PM	admin@identityplus.onmicrosoft.com	Reset user password.	jochen.nicke@identityplus.ch	
11/25/2015 1:55:45 PM	admin@identityplus.onmicrosoft.com	Add user.	jochen.nicke_outlook.comEXT4@identity...	
11/25/2015 1:47:04 PM	admin@identityplus.onmicrosoft.com	Add user.	jochen.nicke@identityplus.ch	
11/24/2015 3:19:13 PM	Unknown	Add service principal	BillingExtension	
11/21/2015 12:55:11 PM	Unknown	Add service principal	ItcaPortal	

notifications

EMAIL LANGUAGE PREFERENCE

English ▾

EMAIL NOTIFICATION OF ANOMALOUS
SIGN INS

ENABLED DISABLED

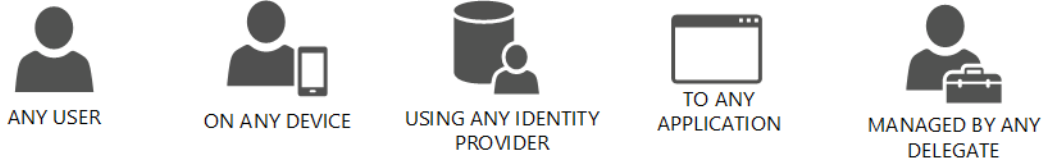
NOTIFY ADMINS WHEN OTHER ADMINS
RESET THEIR OWN PASSWORDS

YES NO

NOTIFY USERS AND ADMINS WHEN THEIR
OWN PASSWORD HAS BEEN RESET

YES NO

Chapter 3: Planning and Designing Authentication and Application Access



**OPEN STANDARDS PROVIDED BY
AZURE ACTIVE DIRECTORY**

WS-*, SAML, OAUTH, OPENID CONNECT



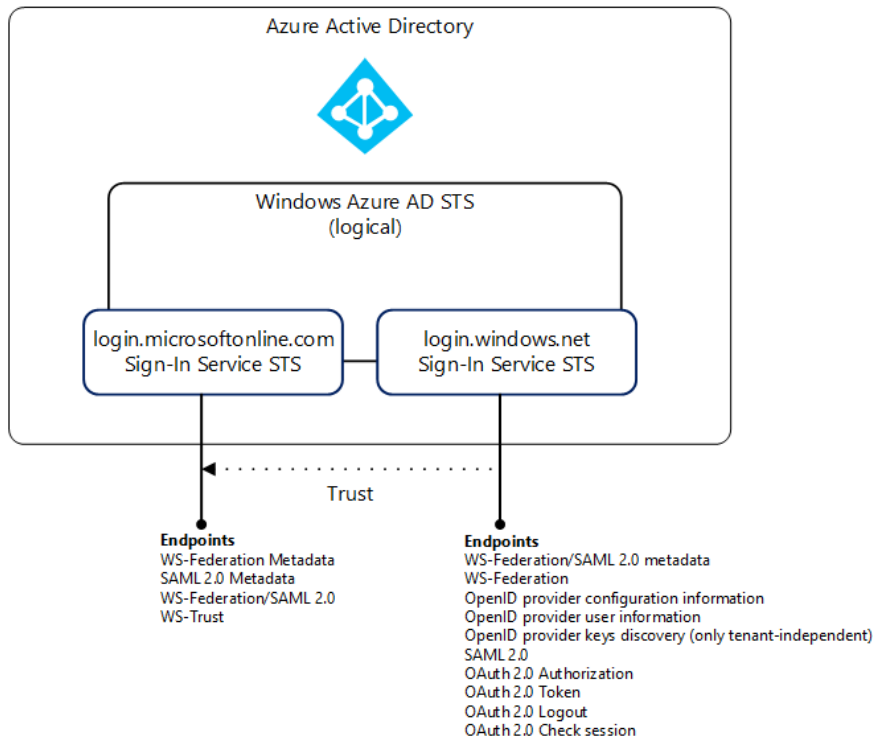
**ON-PREMISE
SERVICES**

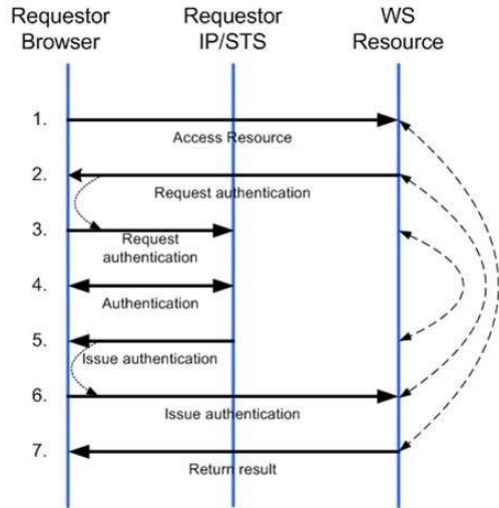
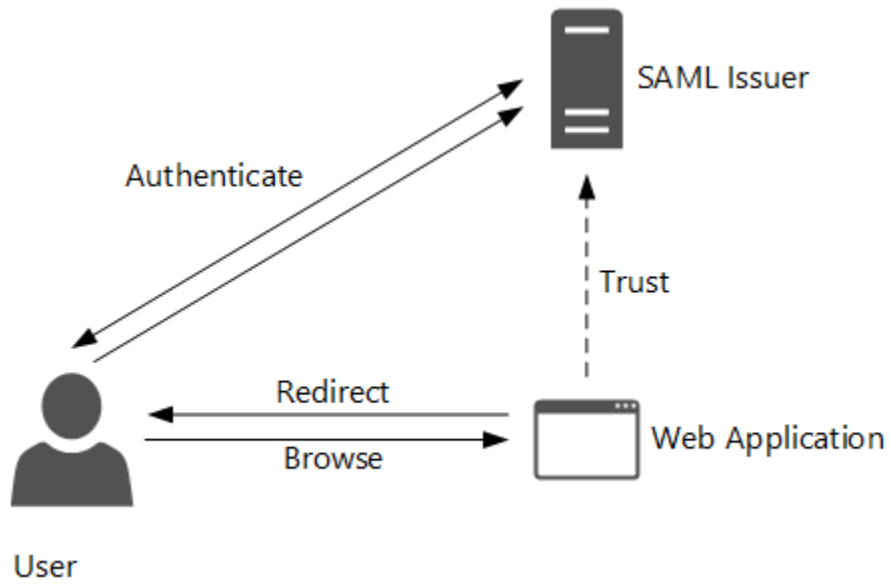


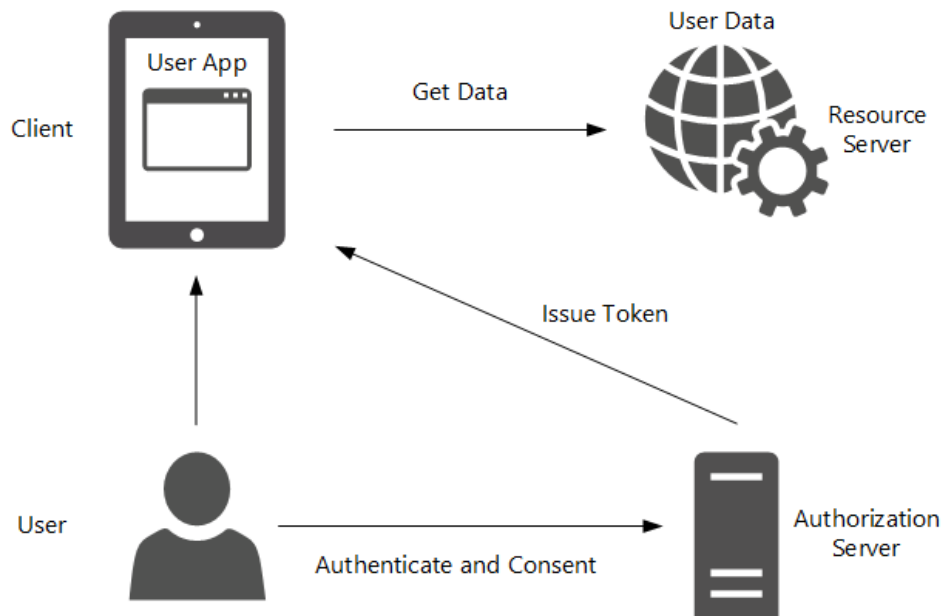
**FEDERATED
IDENTITY**

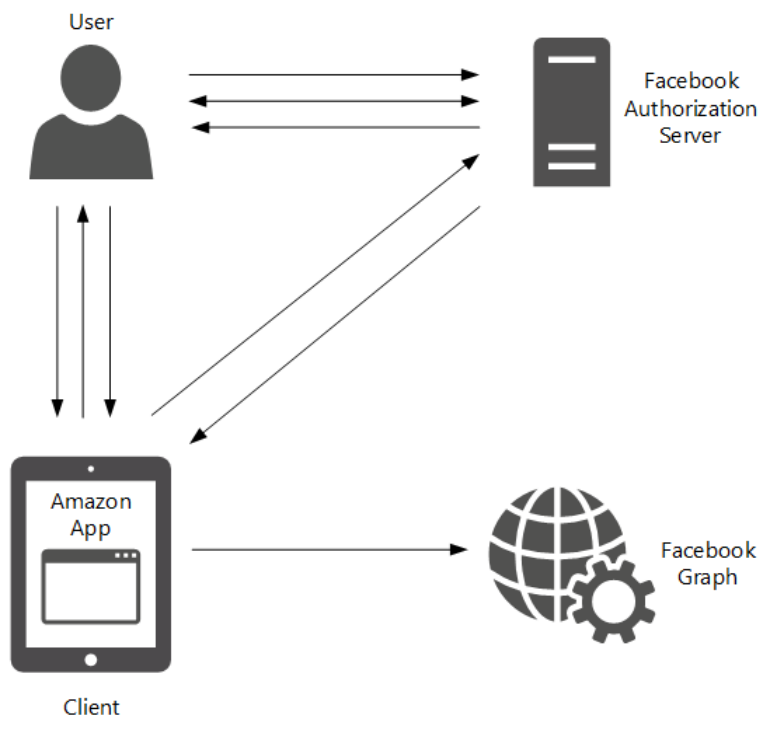


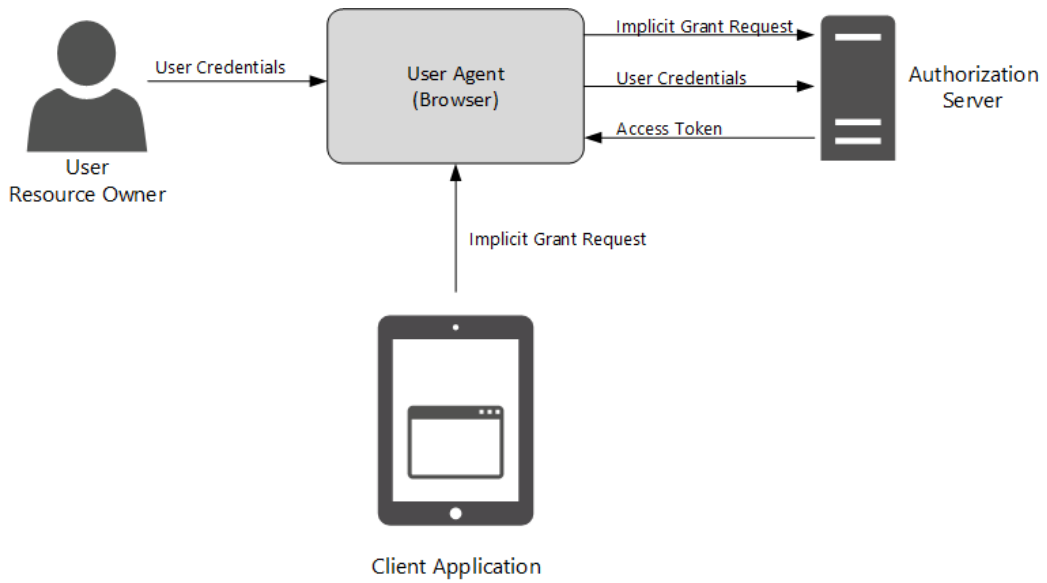
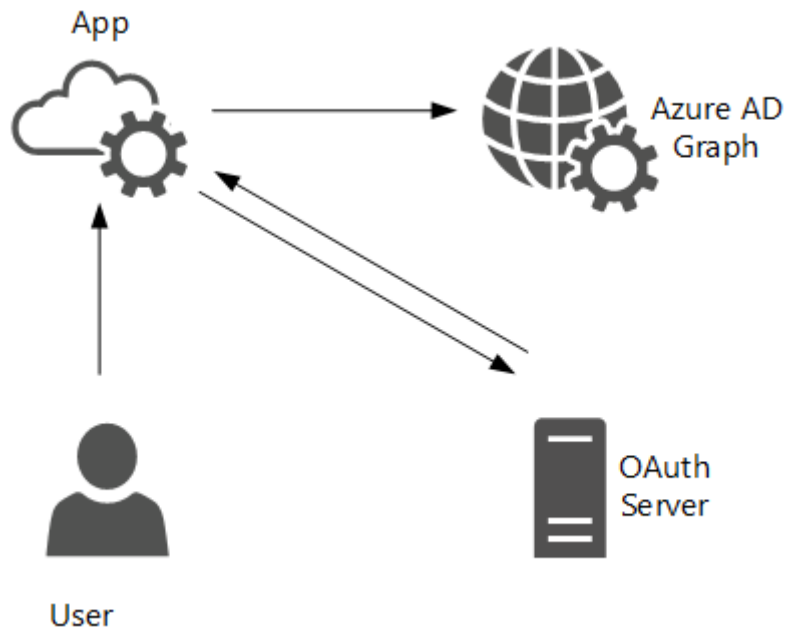
**CLOUD
SERVICES**

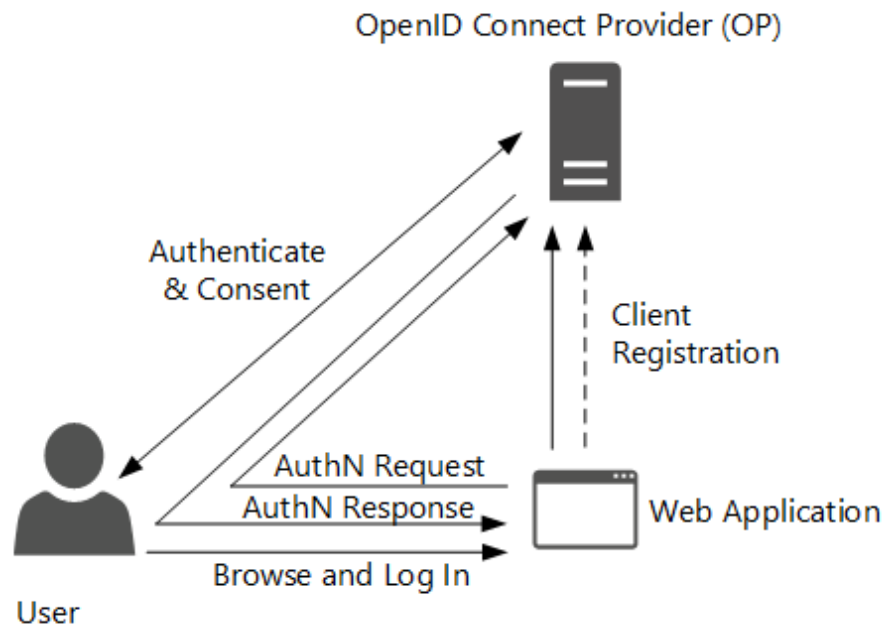
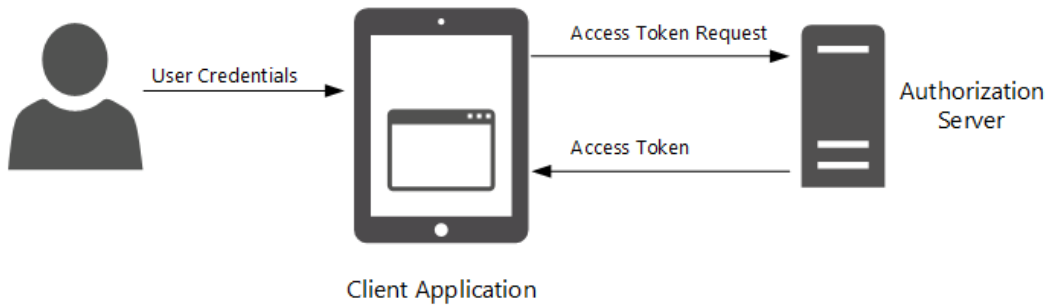


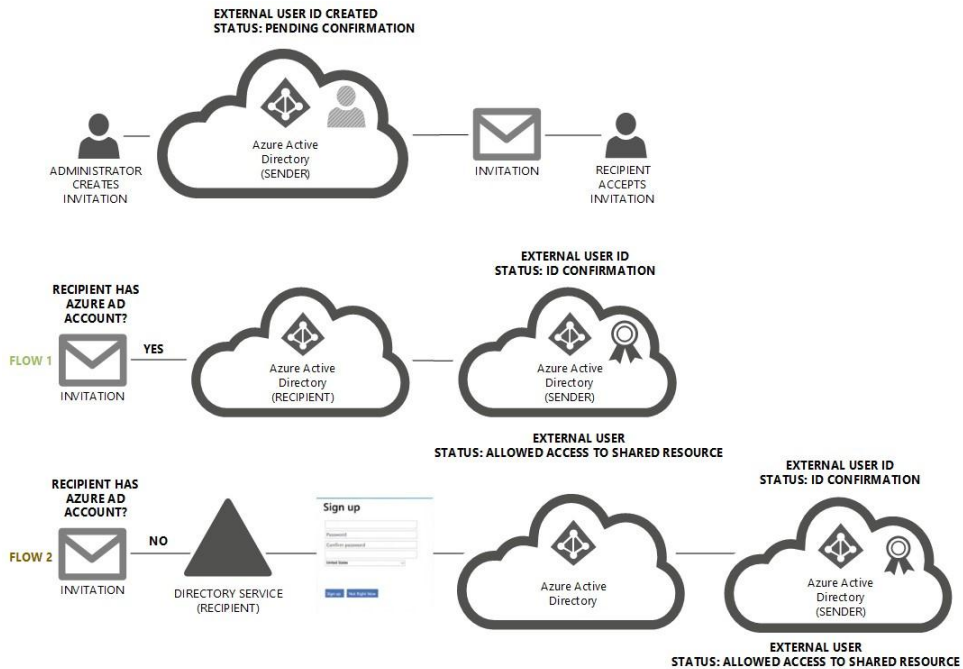
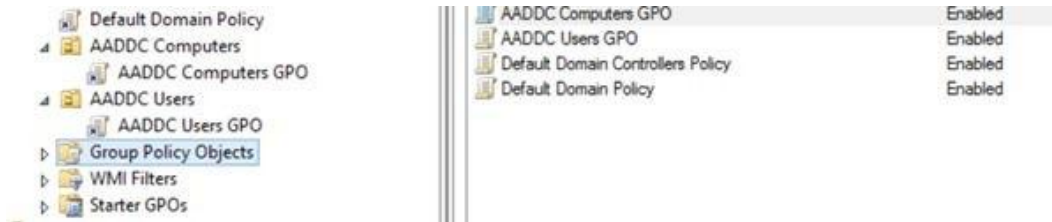
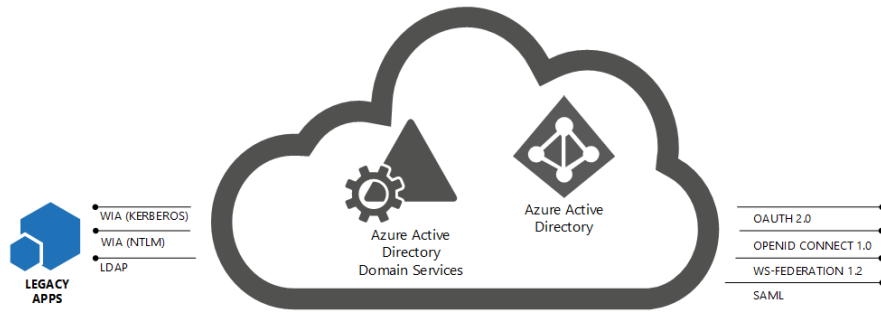


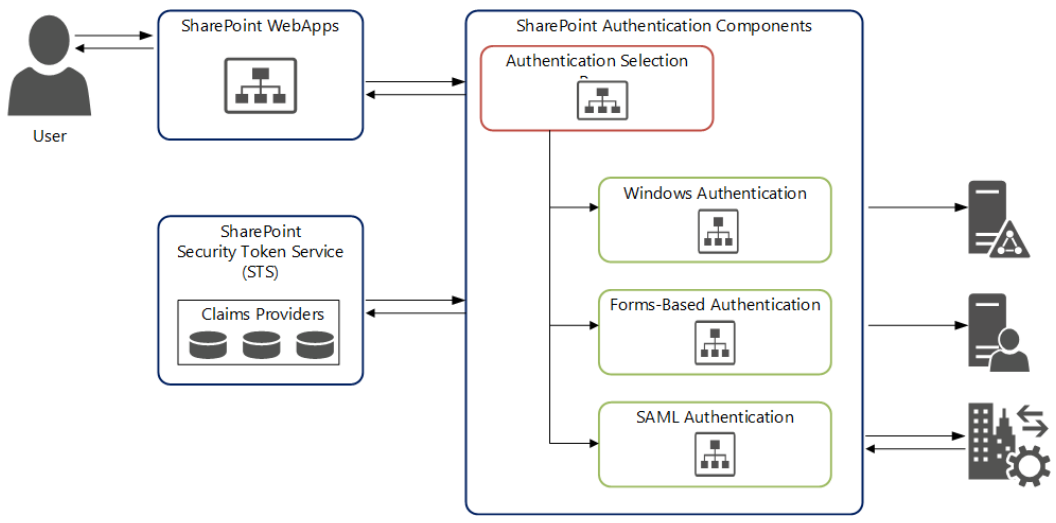
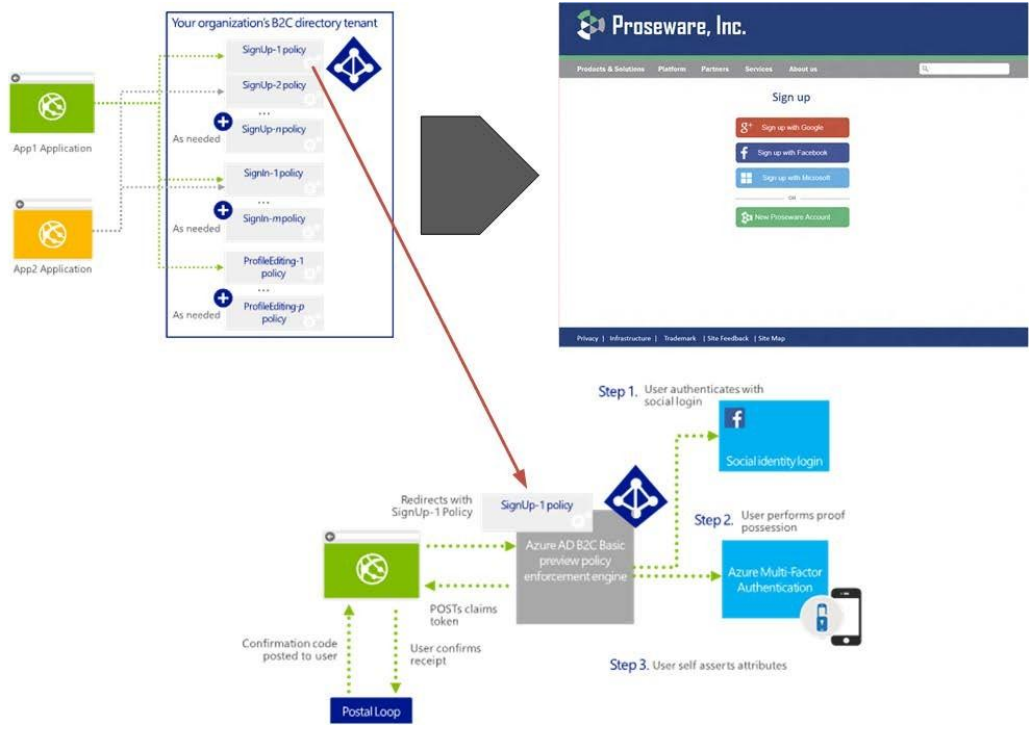


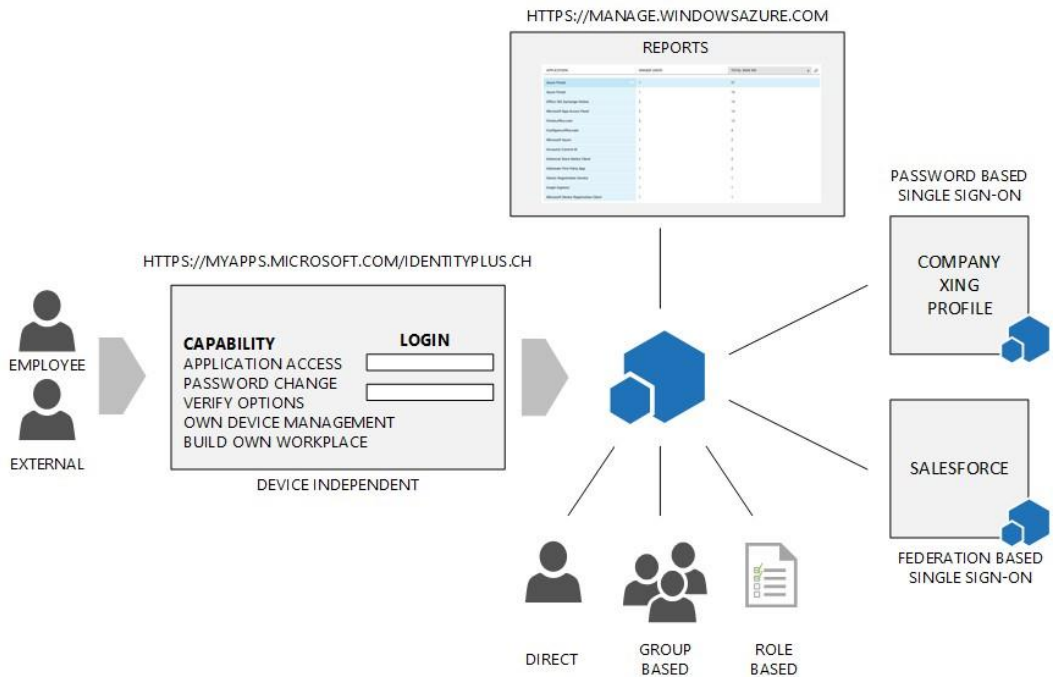
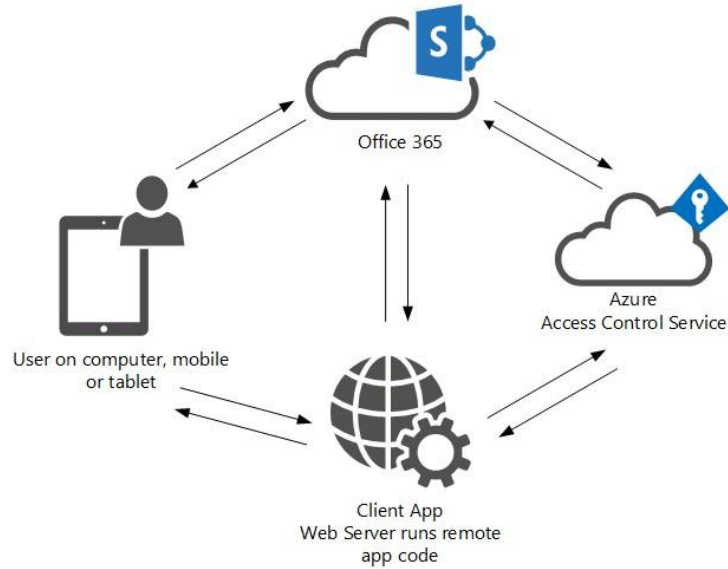










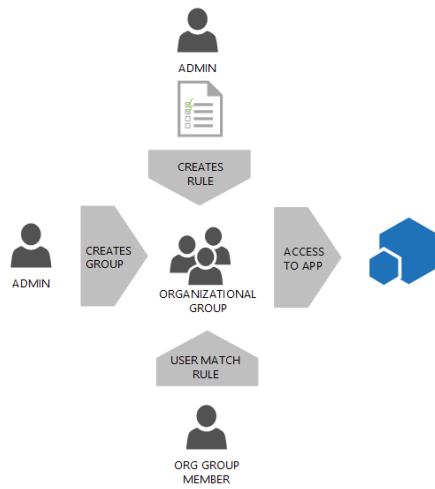


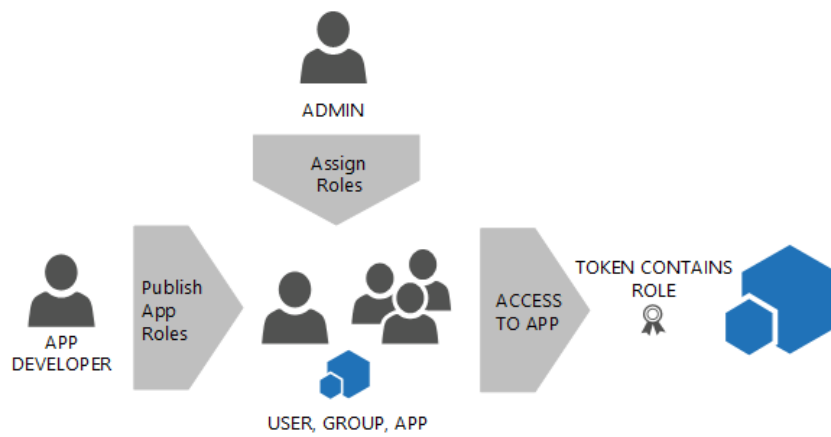
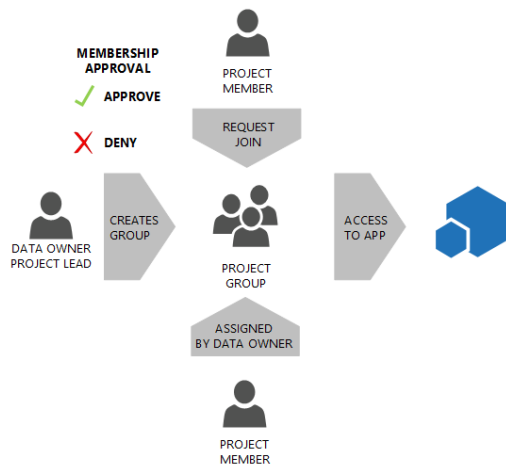
linkedin

[DASHBOARD](#) [USERS AND GROUPS](#) [CONFIGURE](#)

SHOW

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	
Anas Nickel	anas.nickel@azureid.ch			No	Unassigned	
Azureid Postmaster	postmaster@azureid.ch			No	Unassigned	
Ikram Berady	ikram.berady@identityplus...	Senior Sales Manager	Sales	No	Unassigned	
Jochen Nickel	jochen.nickel@identityplus...			Yes	Direct	





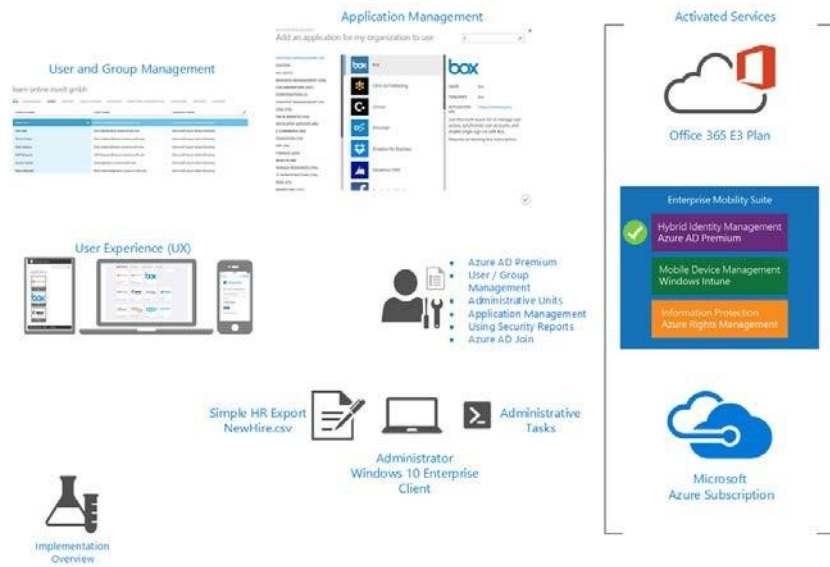
Assign Users

Select TrainingPoint role



Trainee
Trainer

Chapter 4: Building and Configuring a Suitable Azure AD



DASHBOARD | **SUBSCRIPTIONS**

Jochen Nickel
admin@leano.onmicrosoft.com

About me

View account

ACTIVE

Office 365 Enterprise E3 Trial




Check out the new portal jochen.nickel@outlook.com




all items

NAME	TYPE	STATUS	SUBSCRIPTION	LOCATION
identityplus Demo Environment	Directory	Active	Shared by all identitypl...	Europe, United Stat...

all items

NAME	TYPE	STATUS	SUBSCRIPTION	LOCATION
Learning Online inovit GmbH	Directory	✓ Active	Shared by all Learning ...	Europe, United Stat...

Name	Date modified	Type	Size
 AADPowerShellModule_64.msi	29.12.2015 12:11	Windows Installer ...	752 KB
 MSOLSignInAssistant_32.msi	29.12.2015 11:58	Windows Installer ...	4'178 KB
 MSOLSignInAssistant_64.msi	29.12.2015 11:58	Windows Installer ...	6'035 KB

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

Office 365
Enterprise E3 Trial

Welcome, Let's get to know you

Step 1

About you

Step 2

Create an ID

Step 3

You're in

Switzerland

This can't be changed after sign-up. Why not?

Jochen

Nickel

jochen.nickel@inovit.ch

+41564060709

inovit GmbH

5-24 people

Next →

Office 365
Enterprise E3 Trial

Create your user ID

Step 1

About you



Step 2

Create an ID



Step 3

You're in



admin

leano

.onmicrosoft.com



admin@leano.onmicrosoft.com

.....

.....

Next →

Save this info. You'll need it later.

Office 365 sign-in page
<https://portal.office.com>

Your user ID
admin@leano.onmicrosoft.com

★ Bookmark the sign-in page

You're ready to go... →

Microsoft Azure

Sign in with your work or school account



admin@leano.onmicrosoft.co...

Keep me signed in

[Sign in](#) [Cancel](#)

[Can't access your account?](#)

Don't have an account assigned by your work or school?
[Sign in with a Microsoft account](#)

No subscriptions found.

- SIGN OUT ↻
- SIGN UP FOR MICROSOFT AZURE ↻
- MICROSOFT AZURE HOME PAGE ↻
- CONTACT SUPPORT ↻
- PORTAL.AZURE.COM ↻

Before you can start using Microsoft Azure, you need to get a subscription.

We were unable to find any Azure subscriptions where you are a service administrator or co-administrator.

You are signed as admin@leano.onmicrosoft.com in the directory leano.onmicrosoft.com ('inovit GmbH'). If this was not the account you intended to use, please sign out and sign in again using the intended account.

Have DreamSpark or CSP? Visit portal.azure.com

- ALL ITEMS
- WEB APPS
- VIRTUAL MACHINES
- MOBILE SERVICES

all items

NAME	TYPE	STATUS	SUBSCRIPTION	LOCATION	
Learn Online inovit GmbH	→ Directory	✓ Active	Shared by all Learn Onli...	Europe, United Stat...	

learn online inovit gmbh

[USERS](#) [GROUPS](#) [APPLICATIONS](#) [DOMAINS](#) [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#) **LICENSES**

AZURE ACTIVE DIRECTORY PREMIUM

With Azure Active Directory premium you can gain access to richer reports and rule based assignments to applications. Your end users will benefit from self-service capabilities and customized branding. [Learn more](#)

TRY AZURE ACTIVE DIRECTORY PREMIUM NOW [→](#)

ENTERPRISE MOBILITY SUITE

The Enterprise Mobility Suite is the comprehensive cloud solution to address your consumerization of IT, BYOD, and SaaS challenges. In addition to Azure Active Directory premium the suite includes Microsoft Intune and Azure Rights Management. [Learn more](#)


TRY ENTERPRISE MOBILITY SUITE NOW [→](#)

[USERS](#) [GROUPS](#) [APPLICATIONS](#) [DOMAINS](#) [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#) **LICENSES**

LICENSE PLANS	ACTIVE UNITS	ASSIGNED	INFORMATION
Enterprise Mobility Suite →	100	0	Subscription renew date is 1/28/2016 1:...

enterprise mobility suite

[USERS AND GROUPS](#)



Your licenses are active!
Assign licenses to users in your organization.
 Skip. Click Start the next time I visit.

1 Assign licenses to users
Specify which user accounts in Azure AD can use Azure AD Premium features.
[Assign users](#)

USERS AND GROUPS

NAME	USER NAME	JOB TITLE	DEPARTMENT	METHOD	ASSIGNMENT STATUS
Jochen Nickel	admin@leano.onmicroso...			Unassigned	

msdn subscriptions



United States (English) Sign out
Jochen Nickel inovit GmbH
msdn

Home My Account Buy Renew or Upgrade Subscriber Downloads My Product Keys Help

ACCOUNT

My Subscriptions

Visual Studio Enterprise with MSDN (MPN)
JOCHEN NICKEL, jochen.nickel@inovit.ch

Status: Active

Expires on 7/15/2016

[Remove this Subscription](#) from my account
[Add an existing subscription](#) to my account
[Change Microsoft Account](#) for this subscription
[View Support information](#)

SUBSCRIPTION BENEFITS



Software downloads

Over 11 terabytes of Microsoft Products are available to you

Search

[Go to Subscriber Downloads](#) [Go to My Product Keys](#)



Visual Studio Team Services ?

[Create a Visual Studio Team Services account](#) [Learn more](#)
[Link to your work account](#) (optional) [Learn more](#)



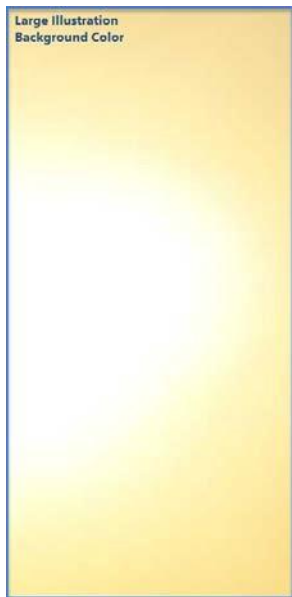
Microsoft Azure ?

[Activate Microsoft Azure](#)
[Go to the Microsoft Azure Management Portal](#)
[Link to your work account](#) (optional) [Learn more](#)



Microsoft Power BI Pro ?

[Activate Microsoft Power BI Pro](#)
[Go to the Microsoft Power BI Pro Portal](#)



Sign in with your work or school account



admin@leano.onmicrosoft.co...

Keep me signed in

[Sign in](#) [Cancel](#)

Can't access your account?

Don't have an account assigned by your work or school?
[Sign in with a Microsoft account](#)

Sign-in Page Text

This service is for the exclusive use of Learning Online 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 156 405-0709.

 Your work or school account can be used anywhere you see this symbol. © 2016 Microsoft [Terms of use](#) [Privacy & Cookies](#)

learn online inovit gmbh

[Dashboard](#) [Users](#) [Groups](#) [Applications](#) [Domains](#) [Directory Integration](#) [Configure](#) [Reports](#) [Licenses](#)

directory properties

NAME

SIGN IN AND ACCESS PANEL PAGE APPEARANCE [Customize Branding](#)

CUSTOMIZE DEFAULT BRANDING

X

Manage how company logos, text, and colors should appear on your organization's Sign In and Access Panel pages. You can also apply unique branding settings for different languages.

[Learn more](#)

BANNER LOGO ?

BROWSE FOR FILE... Remove logo

SQUARE LOGO ?

BROWSE FOR FILE... Remove logo

SQUARE LOGO, DARK THEME ?

BROWSE FOR FILE...

USER ID PLACEHOLDER ?

Leano employee ID

SIGN-IN PAGE TEXT HEADING ?

Learning Online inovit GmbH

SIGN-IN PAGE TEXT ?

This service is for the exclusive use of Learning Online 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 (56) 406-

CUSTOMIZE BRANDING

Manage how company logos, text, and colors should appear on your organization's default Sign In and Access Panel pages. You can also apply unique branding settings for different languages.

[Learn more](#)

EDIT EXISTING BRANDING SETTINGS ?

Default

ADD BRANDING SETTINGS FOR A SPECIFIC LANGUAGE ?

Deutsch (Deutschland)

CUSTOMIZE "CONTACT YOUR ADMINISTRATOR" LINK?

YES NO

CUSTOM EMAIL ADDRESS OR URL

servicedesk@leano.onmicrosoft.com X

learn online inovit gmbh

[DASHBOARD](#) [USERS](#) [GROUPS](#) [APPLICATIONS](#) [DOMAINS](#) [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#) [LICENSES](#)

DISPLAY NAME	USER NAME	SOURCED FROM
Brian Cox	Brian.Cox@leano.onmicrosoft.com	Microsoft Azure Active Directory
Don Hall	Don.Hall@leano.onmicrosoft.com	Microsoft Azure Active Directory
Doris Sutton	Doris.Sutton@leano.onmicrosoft.com	Microsoft Azure Active Directory
Ellen Adams	Ellen.Adams@leano.onmicrosoft.com	Microsoft Azure Active Directory
Jeff Simpson	Jeff.Simpson@leano.onmicrosoft.com	Microsoft Azure Active Directory
Jochen Nickel	admin@leano.onmicrosoft.com	Microsoft Azure Active Directory
Petro Mitchell	Petro.Mitchell@leano.onmicrosoft.com	Microsoft Azure Active Directory

learn online inovit gmbh

[DASHBOARD](#) [USERS](#) [GROUPS](#) [APPLICATIONS](#) [DOMAINS](#) [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#) [LICENSES](#)

NAME	DESCRIPTION	SOURCED FROM
Accounting	Accounting	Microsoft Azure Active Directory
HR	Human Resources	Microsoft Azure Active Directory
Sales	Sales	Microsoft Azure Active Directory

Office 365 admin center <<

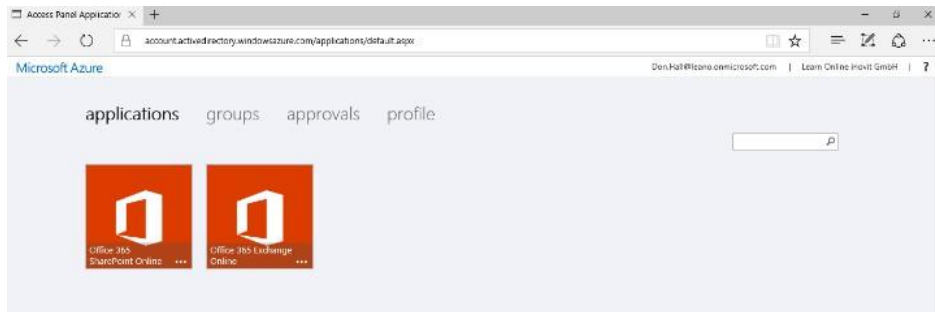
[DASHBOARD](#) | [GROUPS](#)

Search users, admin tasks an

- MEETING ROOMS
- GROUPS**
- DOMAINS
- PUBLIC WEBSITE
- ▶ BILLING
- ▶ EXTERNAL SHARING
- MOBILE MANAGEMENT

Use security groups to assign permissions for SharePoint groups.
Use distribution lists in Exchange to manage email distribution. [Set up distribution lists and other Exchange groups in the Exchange admin center.](#)

<input type="checkbox"/>	Name	Email address	Status
<input type="checkbox"/>	Accounting		In cloud
<input type="checkbox"/>	HR		In cloud
<input type="checkbox"/>	Sales		In cloud



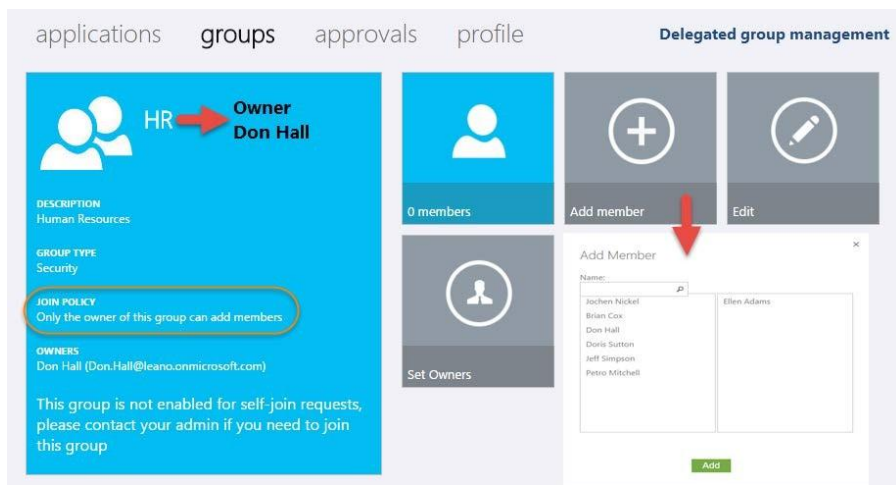
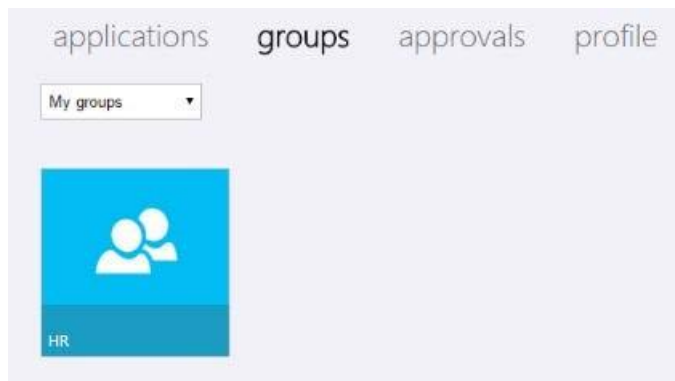
accounting

MEMBERS OWNERS PROPERTIES CONFIGURE SELF-SERVICE ACTIVITY

NAME	USER NAME	DEPARTMENT
Brian Cox	Brian.Cox@leano.onmicrosoft.com	

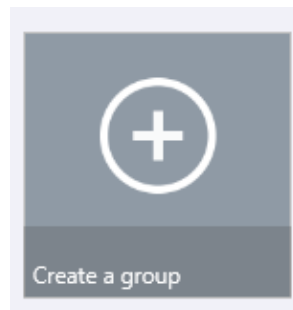
group management

DELEGATED GROUP MANAGEMENT ENABLED	<input checked="" type="radio"/> YES <input type="radio"/> NO
USERS CAN CREATE SECURITY GROUPS	<input type="radio"/> YES <input checked="" type="radio"/> NO
USERS WHO CAN USE SELF-SERVICE FOR SECURITY GROUPS	<input checked="" type="radio"/> ALL <input type="radio"/> SOME
USERS CAN CREATE OFFICE 365 GROUPS	<input type="radio"/> YES <input checked="" type="radio"/> NO <small>PREVIEW</small>
USERS WHO CAN USE SELF-SERVICE FOR OFFICE 365 GROUPS	<input checked="" type="radio"/> ALL <input type="radio"/> SOME
ENABLE DEDICATED GROUPS	<input type="radio"/> YES <input checked="" type="radio"/> NO



group management

DELEGATED GROUP MANAGEMENT ENABLED	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	?
USERS CAN CREATE SECURITY GROUPS	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	?
USERS WHO CAN USE SELF-SERVICE FOR SECURITY GROUPS	<input checked="" type="checkbox"/> ALL <input type="checkbox"/> SOME	?
USERS CAN CREATE OFFICE 365 GROUPS	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	?



Create Group

×

Display name

Sales Internal News

Description (optional)

Sales Internal News

Group policy

This group is open to join for all users

Group type

O365

Create

applications **groups** approvals profile







 Sales Internal News

DESCRIPTION
Sales Internal News

GROUP TYPE
O365

JOIN POLICY
This group is open to join for all users

OWNERS
Doris Sutton (Doris.Sutton@leano.onmicrosoft.com)

 1 members	 Add member	 Edit
 Set Owners	 Leave group	 Delete group

sales internal news

MEMBERS OWNERS **PROPERTIES** CONFIGURE SELF SERVICE ACTIVITY

properties

DISPLAY NAME	Sales Internal News
DESCRIPTION	Sales Internal News
SOURCED FROM	Office 365
GROUP TYPE	Distribution group
OBJECT ID	7c47e743-aaba-4796-9435-95b3d75acb00

Update Group



Display name

Sales Internal News

Description (optional)

Sales Internal News

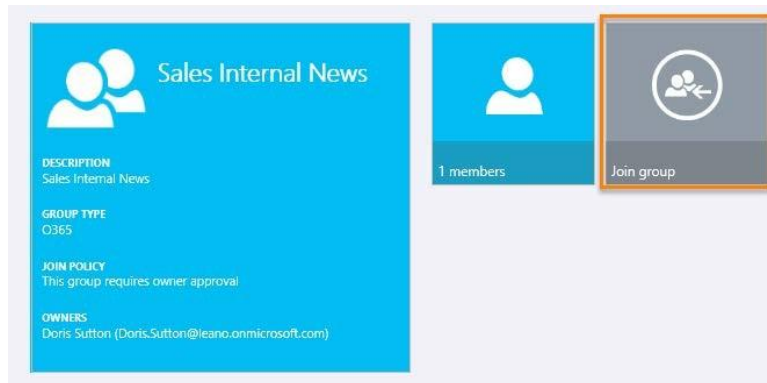
Group policy

This group requires owner approval

Group type

O365

Update



MS msonlineserviceteam@microsoftonline.com
To: Doris Sutton;

Someone wants to join your group

Security group name: **Sales Internal News**
Requestor: **Don.Hall@leano.onmicrosoft.com**

Business justification: **Need to be informed ...**
[Act on this Request](#)

applications groups **approvals** profile

My Approvals ▾

RESOURCE	NAME	REQUESTER	REQUEST	BUSINESS JUSTIFICATION
<input checked="" type="checkbox"/>	GROUP	Sales Internal News	Don.Hall@leano.onmicrosoft.com	Don.Hall@leano.onmicrosoft.com requested to join "Sales Internal News" Need to be informed ...

Approve **Deny**

applications **groups** approvals profile

Sales Internal News

Add members

Don Hall ×

Doris Sutton ×

msonlineserviceteam@microsoftonline.com
01:14

Your membership request was approved
To: Don Hall

Your group membership request was approved

Security group name: **Sales Internal News**
Approved by: **Doris Sutton**

Business justification: **Need to be informed ...**

[View Group Memberships](#) | [Privacy](#) | [Legal](#)

accounting

MEMBERS OWNERS PROPERTIES **CONFIGURE** SELF SERVICE ACTIVITY

dynamic memberships

ENABLE DYNAMIC MEMBERSHIPS **YES** ← **Simple rule** ⓘ

ADD USERS WHERE department Equals (-eq) Accounting ×

ADVANCED RULE

brian cox

PROFILE WORK INFO DEVICES ACTIVITY

job info

JOB TITLE

DEPARTMENT

```
PS C:\> Get-MsolAdministrativeUnit
-----
ExtensionData          Description          DisplayName ObjectID
-----
System.Runtime.Serialization.ExtensionDataObject Human Resources Users HR 1ae30ead-b1d3-4414-8d86-73861db3f0de
```

```
PS C:\> Write-Host $au.ObjectID
1ae30ead-b1d3-4414-8d86-73861db3f0de
PS C:\> Write-Host $user.ObjectID
6a6ddd21-b151-4e19-b319-5204fbf36690
```

```
PS C:\> Get-MsolAdministrativeUnit -UserObjectID $user.ObjectID
-----
ExtensionData          Description          DisplayName ObjectID
-----
System.Runtime.Serialization.ExtensionDataObject Human Resources Users HR 1ae30ead-b1d3-4414-8d86-73861db3f0de

PS C:\> Get-MsolAdministrativeUnitMember -AdministrativeUnitObjectID $au.ObjectID
-----
ExtensionData          DisplayName EmailAddress          ObjectID
-----
System.Runtime.Serialization.ExtensionDataObject Don Hall Don.Hall@leano.onmicrosoft.com 6a6ddd21-b151-4e19-b319-...
```

```

PS C:\> Get-MsolRole
-----
ObjectID                                     Name                                     Description
-----
17315797-102d-40b4-93e0-432062caca18      Compliance Administrator               Compliance administrator.
29232cdf-9323-42fd-ade2-1d097af3e4de      Exchange Service Administrator         Exchange Service Administrator.
2b499bdc-da44-4968-8aec-78e1674fa64d      Device Managers                        Allows access to read and edit device proper...
4ba39ca4-527c-499a-b93d-d9b492c50246      Partner Tier1 Support                  Allows ability to perform tier1 support tasks...
62e90394-69f5-4237-9190-01217145e10      Company Administrator                  Company Administrator role has full access t...
729827e3-9e14-40f7-b01b-9c088f150bb8      Helpdesk Administrator                 Helpdesk Administrator has access to perform...
75941089-915a-4869-abe7-691bf10279e      Lync Service Administrator             Lync Service Administrator.
88d8e3e3-8f55-4a1e-953a-9b9898b8876b      Directory Readers                      Allows access to various read only tasks in ...
9360Feb5-f418-4baa-8175-e2a00bac4301      Directory Writers                       Allows access read tasks and a subset of wrt...
9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3      Application Administrator              Application Administrator role has access to...
9c094953-4995-41c8-84c8-3ebb9b32c93f      Device Join                            Device Join
9f06204d-73c1-4d4c-880a-6edb90606fd8      Device Administrators                  Device Administrators
b0f54661-2d74-4c50-afa3-1ec803f12efe      Billing Administrator                  Billing Administrator has access to perform ...
c34f683f-4d5a-4403-afdf-6615e0e3a7f      Workplace Device Join                  Workplace Device Join
cf1c38e5-3621-4004-a7cb-879624dced7c      Application Developer                  Application Developer role has ability to cr...
d2902b95-8846-44ba-8758-1c26182fcf32      Directory Synchronization Acc...      Directory Synchronization Accounts
d405c60f-0af8-4a3b-95e4-4d06e542189e      Device Users                           Device Users
e0e0864a-17c5-4a4b-9c86-f5b95a8d5bd8      Partner Tier2 Support                  Allows ability to perform tier2 support tasks...
f023fd81-a637-4b56-95fd-791ac0226033      Service Support Administrator          Service Support Administrator has access to ...
f28a1f50-f6e7-4571-818b-6a12f2aff6bc      SharePoint Service Administrator       SharePoint Service Administrator.
fe930be7-5e62-47db-91af-98c3a49a38b1      User Account Administrator             User Account Administrator has access to per...

```

```


PS C:\> Set-MsolUser -UserPrincipalName ellen.adams@leano.onmicrosoft.com -Department HR
PS C:\> Get-MsolUser -UserPrincipalName ellen.adams@leano.onmicrosoft.com | fl

ExtensionData                : System.Runtime.Serialization.ExtensionDataObject
AlternateEmailAddresses      : {}
AlternateMobilePhones        : {}
AlternativeSecurityIds       : {}
BlockCredential              : False
City                          :
CloudExchangeRecipientDisplayType : 1073741824
Country                       :
Department                    : HR
DirSyncProvisioningErrors    : {}
DisplayName                   : Ellen Adams

```

alaska airlines

[DASHBOARD](#) [USERS AND GROUPS](#) [CONFIGURE](#)



Your app has been added!

Enable your app to integrate with Microsoft Azure AD

Skip Quick Start the next time I visit

- 1 Enable single sign-on with Microsoft Azure AD

Configure single sign-on access to this application.

Configure single sign-on


 Single sign-on is enabled for existing application accounts
- 2 Assign users to Alaska Airlines

Specify which accounts in Microsoft Azure AD can access this application.

Assign accounts

Show Search

NAME	PUBLISHER	TYPE	APP URL
Moodle	Moodle™		https://moodle.org/
Doodle	Doodle		https://www.doodle.com/
Google Apps	Google		http://www.google.com/enterprise/apps/b...
DocuSign	DocuSign Inc.		http://www.docuSign.com/
Box	Box		https://www.box.com/
Salesforce	Salesforce.com		http://www.salesforce.com/
Salesforce Sandbox	Salesforce.com		http://test.salesforce.com/
PayPal	PayPal		https://www.paypal.com
Netflix	Netflix, Inc.		https://www.netflix.com/
Microsoft OneDrive	Microsoft Corporation		http://www.onedrive.com/
Facebook	Facebook		https://www.facebook.com/
Skype	Microsoft Corporation		http://www.skype.com/
Alaska Airlines	Alaska Air Group, Inc.		https://www.alaskaair.com/
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cl...
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/
Office 365 Yammer	Microsoft Corporation	Web application	



Box has been added

Skip Quick Start the next time I visit.

- 1 Enable single sign-on with Microsoft Azure AD
Configure single sign-on access to this application.
- 2 Enable automatic account provisioning to Box
Automatically provision accounts from Microsoft Azure AD to Box upon account assignment.
- 3 Assign users to Box
Specify which accounts in Microsoft Azure AD can access this application.

alaska airlines

[DASHBOARD](#) [USERS AND GROUPS](#) [CONFIGURE](#)



Your app has been added!

Enable your app to integrate with Microsoft Azure AD

Skip Quick Start the next time I visit

- 1 Enable single sign-on with Microsoft Azure AD
Configure single sign-on access to this application.
[Configure single sign-on](#) Single sign-on is enabled for existing application accounts
- 2 Assign users to Alaska Airlines
Specify which accounts in Microsoft Azure AD can access this application.
[Assign accounts](#)

Don-Fai@exms.onmicrosoft.com | Learning Online in our Office

applications groups approvals profile

Office 365 Exchange Online ... Office 365 SharePoint Online ... Alaska Airlines ... OneDrive ... Facebook ... Microsoft OneDrive ... Moodle ... Netflix ... PayPal ... Skype ...

Microsoft OneDrive

A new version of the software is required in order to sign-in to this application. Please update now.

[Update Now](#)

Almost done installing...

To finish installing the Access Panel extension for Internet Explorer, complete the following steps:

1. Click "Enable" below

There should be a prompt at the bottom of the window that says that the Access Panel add-on is ready for use.

If you don't see the prompt, check our [Troubleshooting guide](#).

2. Restart Internet Explorer

Close this window, and then open Internet Explorer again.

Then you're done!

© 2015 Microsoft [Legal](#) [Privacy](#)



FEATURED APPLICATIONS (16)

CUSTOM

[ALL \(2577\)](#)

BUSINESS MANAGEMENT (108)

COLLABORATION (297)

CONSTRUCTION (3)

CONTENT MANAGEMENT (91)

CRM (110)

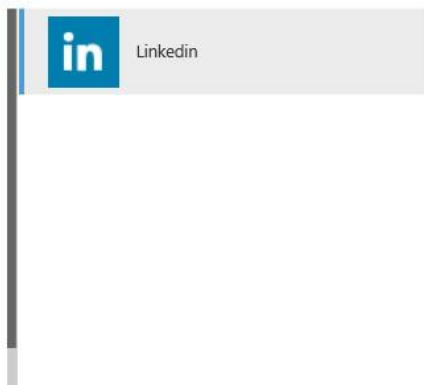
DATA SERVICES (110)

DEVELOPER SERVICES (86)

E-COMMERCE (69)

EDUCATION (74)

ERP (38)



LinkedIn

NAME LinkedIn

PUBLISHER LinkedIn Corporation

APPLICATION URL <https://www.linkedin.com/>

Use Microsoft Azure AD to enable user access to LinkedIn.

Requires an existing LinkedIn subscription.

linkedin

[DASHBOARD](#) [USERS AND GROUPS](#) [CONFIGURE](#)

SHOW

DISPLAY NAME	USER NAME	JOB TITLE	DEPARTMENT	ACCESS	METHOD	
Brian Cox	Brian.Cox@leano.onmicros...			No	Unassigned	
Don Hall	Don.Hall@leano.onmicros...			No	Unassigned	

Assign Users

This action will allow the selected user to authenticate to the LinkedIn application from within the Access Panel. Users can enter and update their LinkedIn credentials using the Access Panel at any time.

I want to enter LinkedIn credentials on behalf of the user

Account Name

Password

I want to enable automatic password rollover.



Log in to Twitter



Log in

Remember me · [Forgot password?](#)

New to Twitter? [Sign up now »](#)

Already using Twitter via text message? [Activate your account »](#)

Twitter

Enter your credentials to sign in for this application

Username

Password

Your sign-in information will be stored securely. Click [here](#) for more information.

Sign in

twitter

DASHBOARD USERS AND GROUPS CONFIGURE

SHOW STARTING WITH

NAME	EMAIL ADDRESS	OWNERS	ASSIGNED	
Accounting		Brian Cox	No	
HR		Don Hall	No	
Sales		Doris Sutton	No	



Assign Groups

This action will allow the members of selected group to authenticate to the Twitter application from within the Access Panel.

I want to enter Twitter credentials to be shared among all group members

User Name

Password

I want to enable automatic password rollover.



integrated applications

USERS MAY GIVE APPLICATIONS PERMISSION TO ACCESS THEIR DATA

USERS MAY ADD INTEGRATED APPLICATIONS

USERS MAY ADD PASSWORD SSO APPLICATIONS FROM THE AZURE AD APP GALLERY

manage applications

Show Applications my company uses Search

NAME	PUBLISHER	TYPE	APP URL	
Alaska Airlines	Alaska Air Group, Inc.	Web application	https://www.alaskaair.com/	
Box	Box	Web application	https://www.box.com/	
DocuSign	DocuSign Inc.	Web application	http://www.docuSign.com/	
Doodle	Doodle	Web application	https://www.doodle.com/	
Facebook	Facebook	Web application	https://www.facebook.com/	
Google Apps	Google	Web application	http://www.google.com/enterprise/apps/b...	
LinkedIn	LinkedIn Corporation	Web application	https://www.linkedin.com/	
MailChimp	The Rocket Science Group	Web application	http://mailchimp.com/	
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cl...	

user password reset policy

USERS ENABLED FOR PASSWORD RESET	<input checked="" type="radio"/> YES <input type="radio"/> NO	?
RESTRICT ACCESS TO PASSWORD RESET	<input type="radio"/> YES <input checked="" type="radio"/> NO	?
Before users can reset their passwords, they must first have at least one authentication method defined. Edit users in 'Learning Online inovit GmbH' now.		
AUTHENTICATION METHODS AVAILABLE TO USERS	<input type="checkbox"/> Office Phone <input checked="" type="checkbox"/> Mobile Phone <input checked="" type="checkbox"/> Alternate Email Address <input type="checkbox"/> Security Questions	?
NUMBER OF AUTHENTICATION METHODS REQUIRED	1	?
You can send users to a webpage where they can register their own authentication method information. Go to this webpage now.		

REQUIRE USERS TO REGISTER WHEN SIGNING IN?	<input checked="" type="radio"/> YES <input type="radio"/> NO	?
NUMBER OF DAYS BEFORE USERS ARE ASKED TO RE-CONFIRM THEIR AUTHENTICATION INFORMATION	180	?
CUSTOMIZE "CONTACT YOUR ADMINISTRATOR" LINK?	<input type="radio"/> YES <input checked="" type="radio"/> NO	?
You need to install Azure Active Directory sync and enable the "Password Writeback" feature to manage on-premises passwords from the cloud. Learn more.		
WRITE BACK PASSWORDS TO ON-PREMISES ACTIVE DIRECTORY	<input checked="" type="radio"/> YES <input type="radio"/> NO	?
PASSWORD WRITE BACK SERVICE STATUS	Not configured	?
Will be configured in hybrid scenarios		
ALLOW USERS TO UNLOCK ACCOUNTS WITHOUT RESETTING THEIR PASSWORD	<input checked="" type="radio"/> YES <input type="radio"/> NO	?

notifications

EMAIL LANGUAGE PREFERENCE	English	?
EMAIL NOTIFICATION OF ANOMALOUS SIGN INS	ENABLED	?
NOTIFY ADMINS WHEN OTHER ADMINS RESET THEIR OWN PASSWORDS	YES	?
NOTIFY USERS AND ADMINS WHEN THEIR OWN PASSWORD HAS BEEN RESET	YES	?

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

Microsoft ONLINE

Don.Hall@leano.onmicrosoft.com | ?

don't lose access to your account!

To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. You'll need to set up at least 1 of the options below.

- 1 Authentication Phone is not configured. Set it up now
- 1 Authentication Email is not configured. Set it up now

finish cancel



So, 03.01.2016 16:33

Microsoft on behalf of Learning Online inovit GmbH <msonlineserviceteam@microsoftonline.com>
Learning Online inovit GmbH account email verification code

To Jochen Nickel


Verify your email address

Thanks for verifying your Don.Hall@leano.onmicrosoft.com account!

Your code is: 624634

Sincerely,
Learning Online inovit GmbH


This message was sent from an unmonitored email address. Please do not reply to this message.



don't lose access to your account!

To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. **You'll need to set up at least 2 of the options below.**

 Authentication Phone is set to [+41 79](tel:+4179) Verify

 Authentication Email is not configured. [Set it up now](#)



Don.Hall@leano.onmicrosoft....

Keep me signed in

Sign in

Cancel

[Can't access your account?](#)



Get back into your account

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

Email my alternate email

You will receive an email containing a verification code at your alternate email address (jo*****@inovit.ch).

Email

sign ins after multiple failures

May indicate a successful brute force attack.

REPORT CONFIGURE

NUMBER OF CONSECUTIVE FAILED SIGN INS CONSIDERED ANOMALOUS:

10

Your account is temporarily locked to prevent unauthorized use. Try again later, and if you still have trouble, contact your support person.

Don.Hall@leano.onmicrosoft.com

Password

settings

ALLOW THE USER TO SIGN IN AND ACCESS SERVICES?

ALLOW

BLOCK



Office 365

Admin



Don Hall

- Details
- Roles
- Settings**
- Licenses
- Email address
- Mailbox permissions
- More

Set sign-in status

- Allowed
The user can sign in and access services.
- Blocked
The user can't sign in or access services.



[USERS](#)
[GROUPS](#)
[APPLICATIONS](#)
[DOMAINS](#)
[DIRECTORY INTEGRATION](#)
[CONFIGURE](#)
[REPORTS](#)
[LICENSES](#)

REPORT	DESCRIPTION
ANOMALOUS ACTIVITY	
Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.
ERROR REPORTS	
Account provisioning errors	Indicates an impact to users' access to external applications.
INTEGRATED APPLICATIONS	
Application usage: summary	Provides a usage summary for all SaaS applications integrated with your directory.
Application usage: detailed	Provides usage details for a specified SaaS application.

sign ins from multiple geographies

May indicate that multiple users are signing in with the same account.

INTERVAL ✓
Sign ins have been processed up to 1/3/2016 3:59:59 PM.

USER	FIRST SIGN IN FROM	SECOND SIGN IN FROM	TIME BETWEEN SIGN INS	ESTIMATED TRAVEL HOU...	TIME OF 2ND SIGN IN
Don Hall	Zuerich, Zuerich, CH	Bucuresti, Bucuresti, RO	00:10:57	2	1/2/2016 11:45:51 PM



users with anomalous sign in activity

Indicates users whose accounts may have been compromised.

INTERVAL ✓
Sign ins after 1/3/2016 2:59:59 PM may not have been processed completely.

Number of users with anomalous activity: 1

USER	REASON	DATE AND TIME
Don Hall	Expand to view details.	1/2/2016 11:45:51 PM
Don Hall	Signed in from a concealed IP address.	1/2/2016 11:45:51 PM
Don Hall	Signed in from geo-distant locations.	1/2/2016 11:45:51 PM

devices

USERS MAY JOIN DEVICES TO AZURE AD	<input checked="" type="radio"/> ALL <input type="radio"/> SELECTED <input type="radio"/> NONE	⊙
ADDITIONAL ADMINISTRATORS ON AZURE AD JOINED DEVICES	<input type="radio"/> SELECTED <input checked="" type="radio"/> NONE	⊙
USERS MAY REGISTER THEIR DEVICES WITH AZURE AD	<input type="radio"/> ALL <input checked="" type="radio"/> NONE	⊙
REQUIRE MULTI FACTOR AUTHN TO JOIN DEVICES	<input type="radio"/> YES <input checked="" type="radio"/> NO	⊙
MAXIMUM NUMBER OF DEVICES PER USER	<input type="text" value="10"/>	⊙

Option will be configured in the hybrid scenarios



PC name DONHALLNB01

Rename PC

Organization WORKGROUP

Join a domain

Join Azure AD

Edition Windows 10 Enterprise

Version 1511

OS Build 10586.36

Let's get you signed in



Work or school account

don.hall@leano.onmicrosoft.com

••••••••

[I forgot my password](#)

Need help?

This service is for the exclusive use of Learning Online 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 (56) 406-0709.

[Privacy statement](#)

Sign in

Cancel

Make sure this is your organization

Make sure this is your organization

If you continue, system policies might be turned on or other changes might be made to your PC.
Is this the right organization?

Connecting to: leano.onmicrosoft.com
User name: Don.Hall@leano.onmicrosoft.com
User type: Administrator

Cancel

Join

Windows 10

PC name DONHALLNB01

Rename PC

Organization Learning Online inovit GmbH

Disconnect from organization

don hall

PROFILE WORK INFO DEVICES ACTIVITY

VIEW

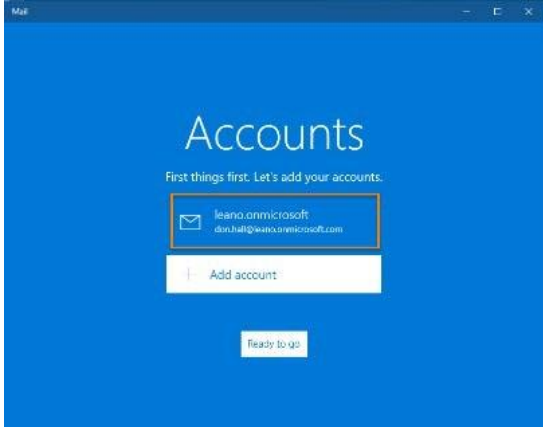
DISPLAY NAME	STATUS	PLATFORM	TRUST TYPE	TRUST LEVEL	
DONHALLNB01	✓ Enabled	Windows	AAD Joined	Authenticated	

Make my PC more secure

You must make your PC more secure to connect to this server. Windows will ensure that your PC complies with any server requirements, including password requirements, requiring sign-in after a specified period of inactivity, and limiting the number of incorrect attempts to sign in to your PC. Windows might also limit sign-in methods such as picture password.

Enforce these policies

Cancel



learning online inovit gmbh

[DASH-BOARD](#) [USERS](#) [GROUPS](#) [APPLICATIONS](#) **DOMAINS** [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#) [LICENSES](#)

Your directory comes with a default domain, leano.onmicrosoft.com. Add a custom domain to improve user sign-on experiences!

[ADD A CUSTOM DOMAIN](#) 

 Successfully verified the domain.

ADD DOMAIN

Verify leano.ch

learning online inovit gmbh

[DASHBOARD](#) [USERS](#) [GROUPS](#) [APPLICATIONS](#) **DOMAINS** [DIRECTORY INTEGRATION](#) [CONFIGURE](#) [REPORTS](#) [LICENSES](#)

DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY DOMAIN	
leano.ch	Custom	✓ Verified	Not Planned	No	
leano.onmicrosoft.com	Basic	✓ Active	Not Available	Yes	

Add Group

NAME 

AAD DC Administrators

DESCRIPTION 

Azure AD Domain Services administrators group

Add members

SHOW ✓

NAME	USER NAME	DEPARTMENT	
Brian Cox	Brian.Cox@leano.onmicrosoft.com	Accounting	
Don Hall	Don.Hall@leano.onmicrosoft.com	HR	
Doris Sutton	Doris.Sutton@leano.onmicrosoft.com		
Ellen Adams	Ellen.Adams@leano.onmicrosoft.com	HR	
Jeff Simpson	Jeff.Simpson@leano.onmicrosoft.com	Accounting	
Jochen Nickel	jnickn@leano.onmicrosoft.com		
Petio Mitchell	Petio.Mitchell@leano.onmicrosoft.com		

SELECTED: Jochen Nickel

NAME

ADDRESS SPACE MAXIMUM VM COUNT

[192.168.0.0 - 192.168.15.255]

LOCATION DNS SERVER

VIRTUAL NETWORKS LOCAL NETWORKS DNS SERVERS

NAME	STATUS	SUBSCRIPTION	LOCATION	
LeanoAzureNet	→ ✓ Created	Free Trial	Central US	

domain services PREVIEW

ENABLE DOMAIN SERVICES FOR THIS DIRECTORY Pending ...

Users will not be able to login to the domain using their credentials until you enable password synchronization.

DNS DOMAIN NAME OF DOMAIN SERVICES leano.onmicrosoft.com

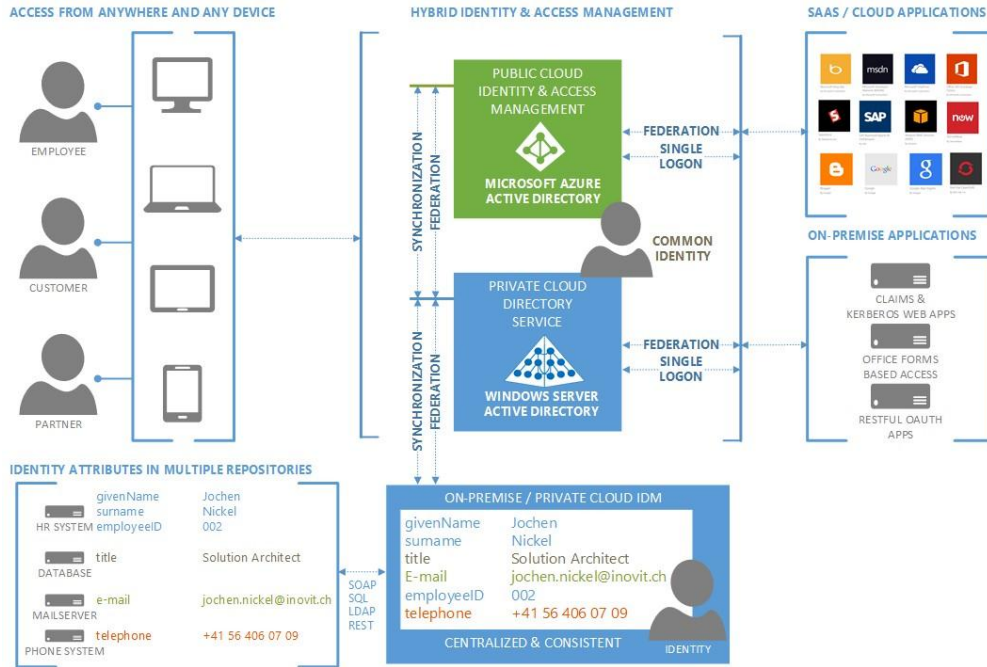
CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK LeanoAzureNet | Subnet-1(192.168.0.0/23) | Central US | Sub...

IP ADDRESS

dns servers

leano.onmicrosoft.com 1	192.168.0.4
leano.onmicrosoft.com 2	192.168.0.5
<input type="text" value="ENTER NAME"/>	<input type="text" value="IP ADDRESS"/>

Chapter 5: Shifting to a Hybrid Scenario



integration with local active directory

DOMAINS VERIFIED FOR DIRECTORY SYNC 2

DOMAINS PLANNED FOR SINGLE SIGN-ON 0

DOMAINS CONFIGURED FOR SINGLE SIGN-ON 1

DIRECTORY SYNC

ACTIVATED DEACTIVATED

LAST SYNC

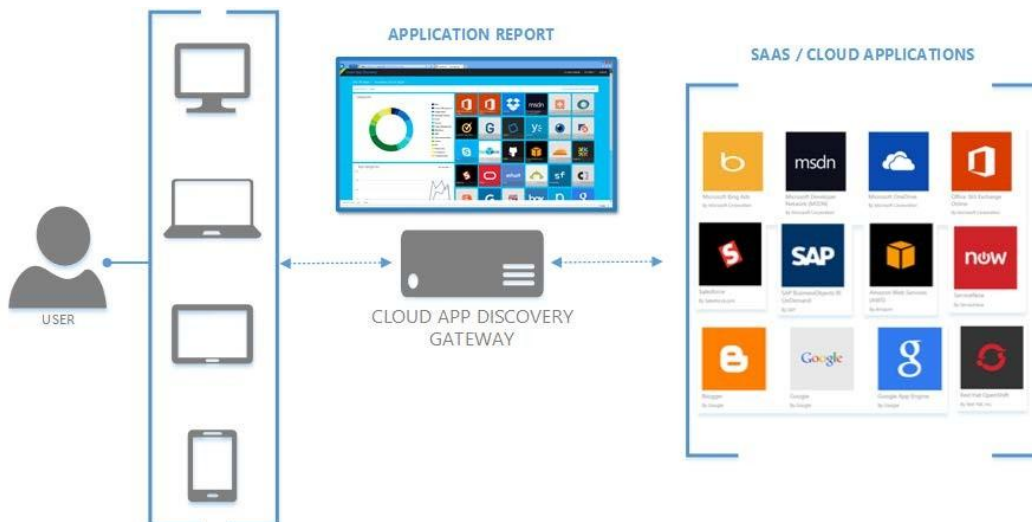
2 hours ago

idam demo environment

USERS GROUPS APPLICATIONS DOMAINS DIRECTORY INTEGRATION CONFIGURE REPORTS LICENSES

DISPLAY NAME	USER NAME	SOURCED FROM
Aaron Painter	aaron.painter@onidam.ch	Local Active Directory
Adam Barr	adam.barr@onidam.ch	Local Active Directory
Alan Brewer	alan.brewer@onidam.ch	Local Active Directory
Alan Steiner	alan.steiner@onidam.ch	Local Active Directory
Alexandre Silva	alexandre.silva@onidam.ch	Local Active Directory
Alfons Parovszky	alfons.parovszky@onidam.ch	Local Active Directory
Alicia Thomber	alicia.thomber@onidam.ch	Local Active Directory
Alisa Lawyer	alisa.lawyer@onidam.ch	Local Active Directory
Allan Guinot	allan.guinot@onidam.ch	Local Active Directory
Allison Brown	allison.brown@onidam.ch	Local Active Directory
Amy Alberts	amy.alberts@onidam.ch	Local Active Directory
Anders Madsen	anders.madsen@onidam.ch	Local Active Directory
Andrea Dunker	andrea.dunker@onidam.ch	Local Active Directory
Andrew Ma	andrew.ma@onidam.ch	Local Active Directory
Andy Jacobs	andy.jacobs@onidam.ch	Local Active Directory
Anna Lidman	anna.lidman@onidam.ch	Local Active Directory
Anne Weiler	anne.weiler@onidam.ch	Local Active Directory
Annelie Zubar	annelie.zubar@onidam.ch	Local Active Directory
Anu Deshpande	anu.deshpande@onidam.ch	Local Active Directory

ADD USER MANAGE MULTI-FACTOR AUTH RESET PASSWORD



Identity Access Management



Mobile Application Management



Mobile Device Management



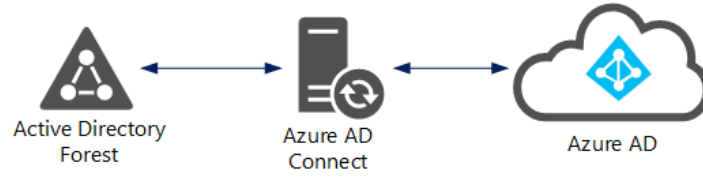
Mobile Information Management



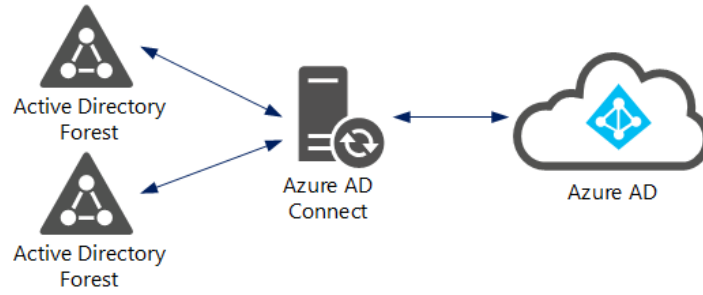
Mobile Content Management



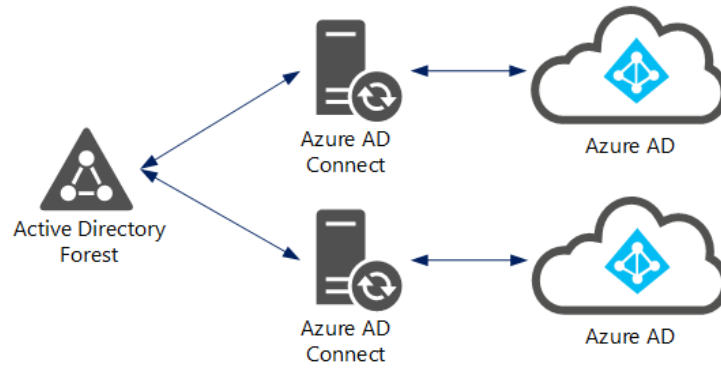
Single Forest scenario

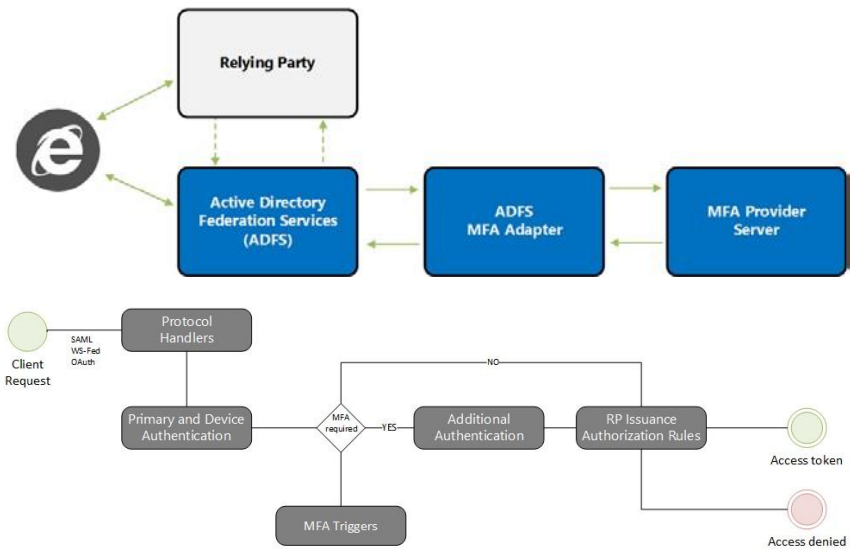
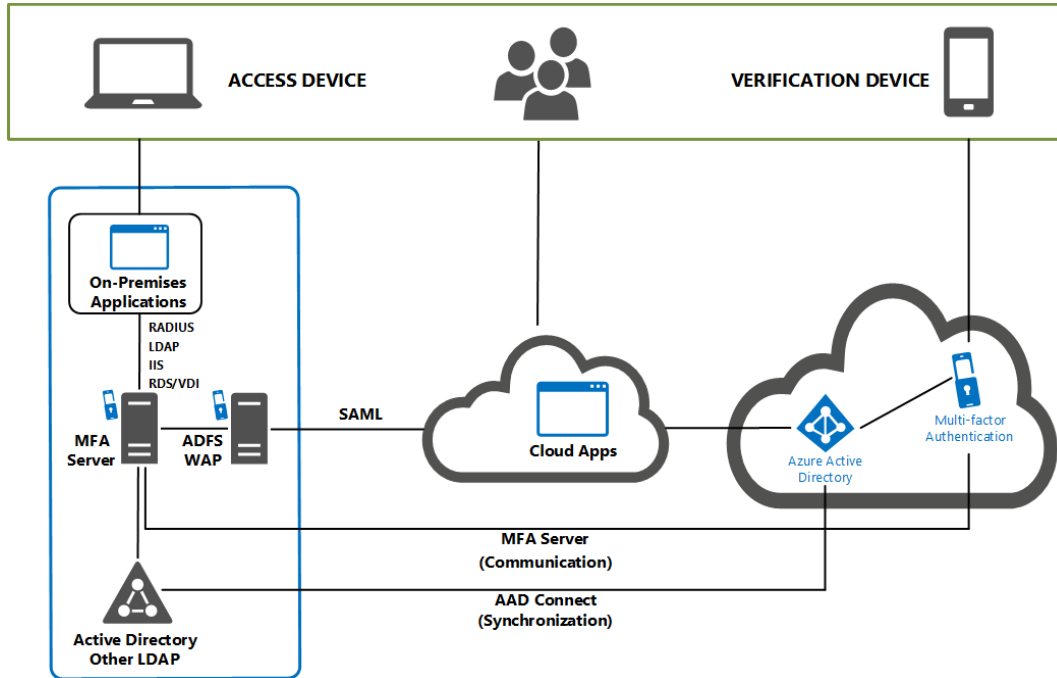


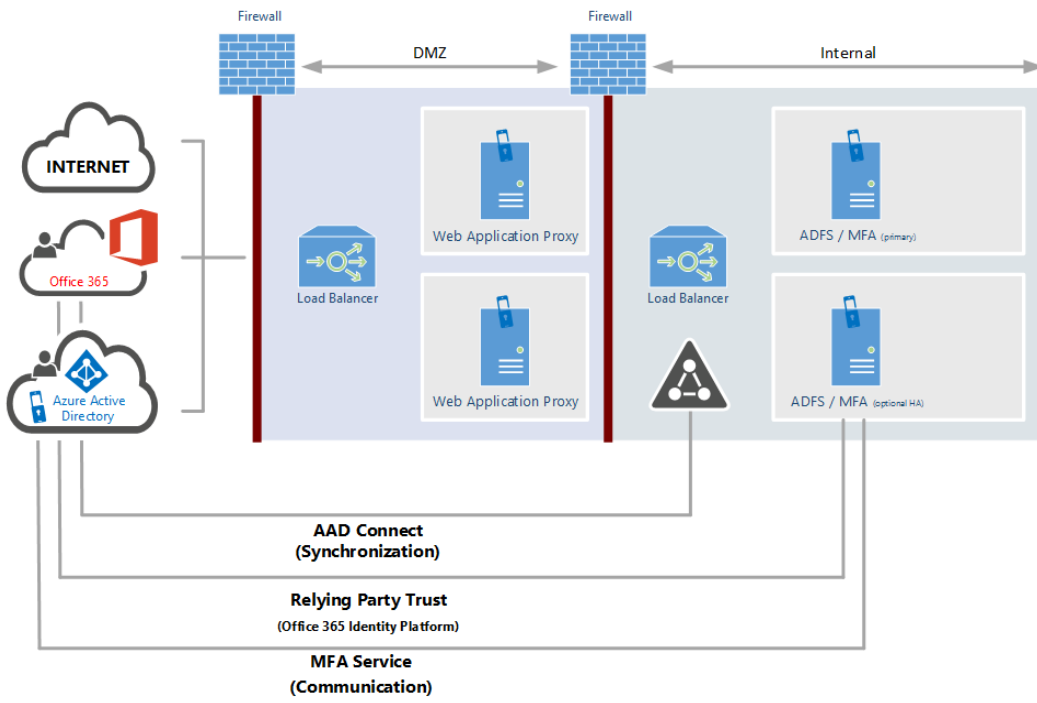
Multi Forest scenario

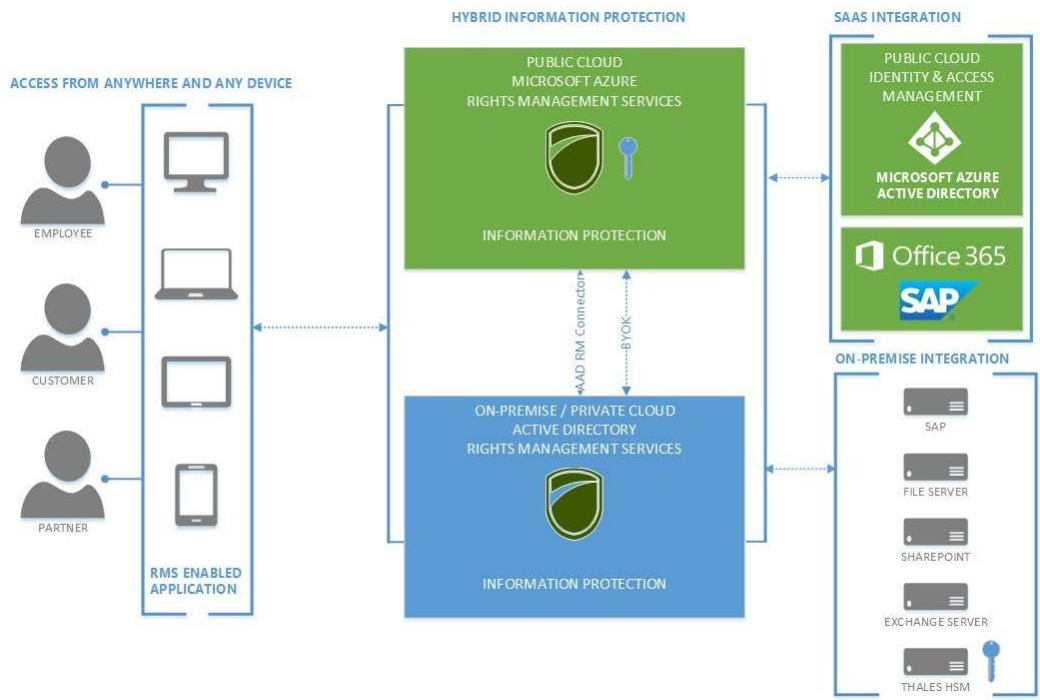


Single/Multi Forest – Multiple Azure AD scenario

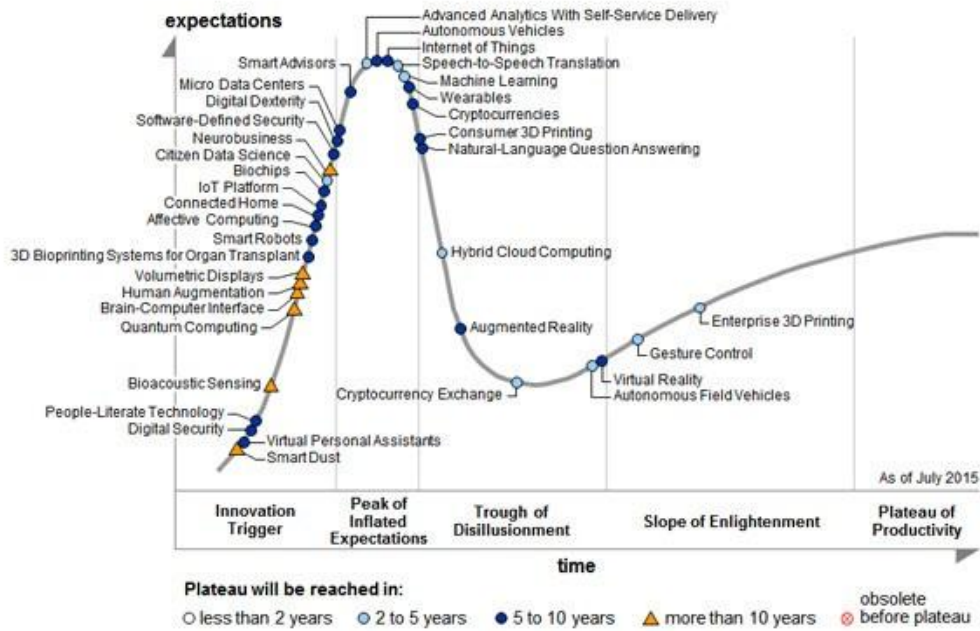


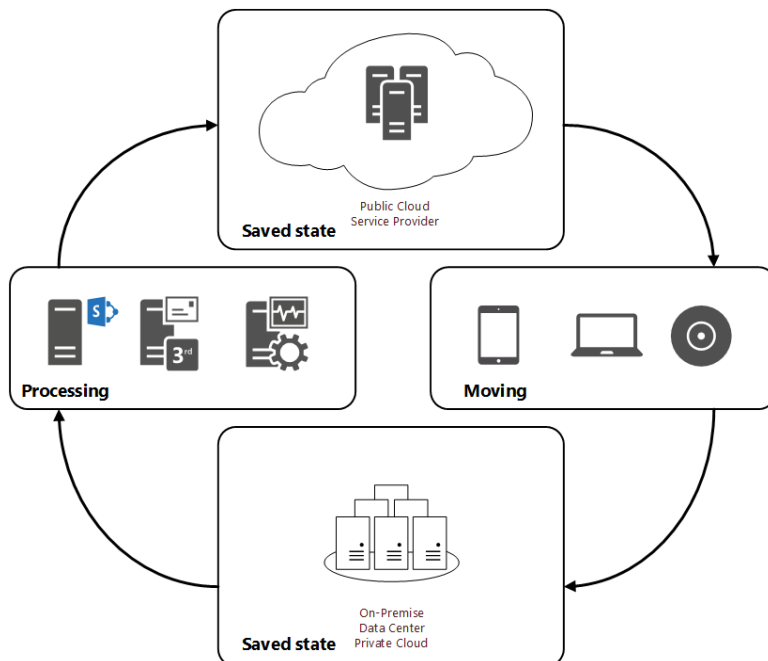
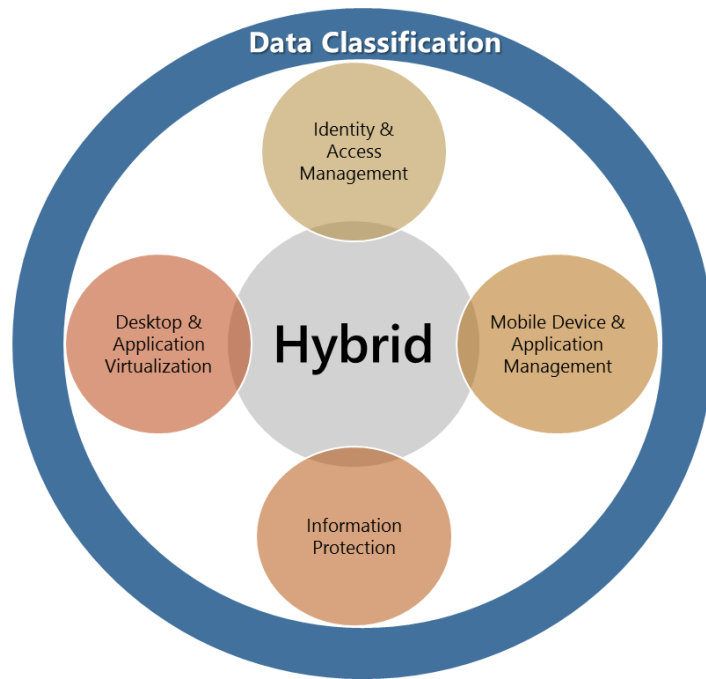






Chapter 6: Extending to a Basic Hybrid Environment





Attribute Name	Value	Contributing MA	Sync Rule	Type
countryCode	0	onidam.ch	In from AD - User ...	number
department	Sales	onidam.ch	In from AD - User ...	string
displayName	April Stewart	onidam.ch	In from AD - User ...	string
domainFQDN	onidam.ch	onidam.ch	In from AD - User ...	string
domainNetBios	ONIDAM	onidam.ch	In from AD - User ...	string
forestFQDN	onidam.ch	onidam.ch	In from AD - User ...	string
forestNetBios	ONIDAM	onidam.ch	In from AD - User ...	string
givenName	April	onidam.ch	In from AD - User ...	string
objectSid	01 05 00 00 00 00 05 15 00 00 00 ...	onidam.ch	In from AD - User ...	binary
objectSidString	S-1-5-21-1323180023-1460257248-12...	onidam.ch	In from AD - User ...	string
pwdLastSet	20140912112941.0Z	onidam.ch	In from AD - User ...	string
sn	Stewart	onidam.ch	In from AD - User ...	string
sourceAnchor	XurqhcNW+0OR7wpaoHIXdg==	onidam.ch	In from AD - User ...	string
sourceAnchorBin...	5E EA EA 85 C3 56 FB 43 91 EF 0A 5...	onidam.ch	In from AD - User ...	binary
sourceObjectType	User	onidam.ch	In from AD - User ...	string
telephoneNumber	(312) 555-5454	onidam.ch	In from AD - User ...	string
thumbnailPhoto	FF D8 FF E0 00 010 4A 46 49 46 00 0...	onidam.ch	In from AD - User ...	binary
title	Sales Manager	onidam.ch	In from AD - User ...	string
userPrincipalName	april.stewart@onidam.ch	onidam.ch	In from AD - User ...	string

Enterprise Cloud Suite

Office 365

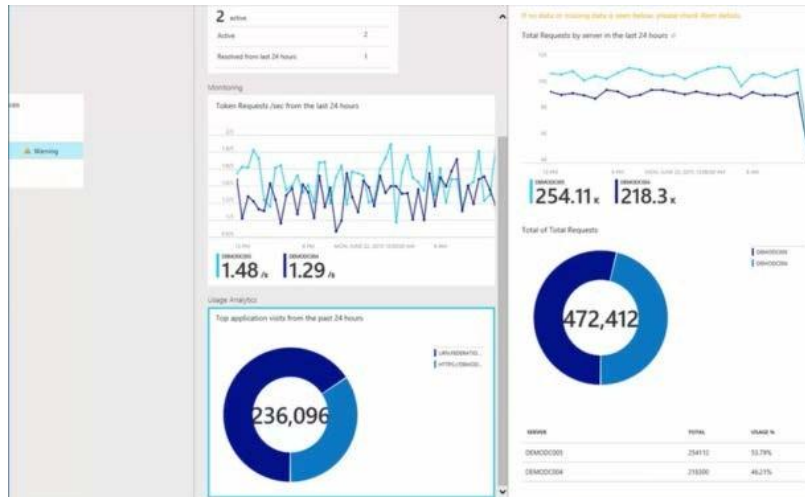
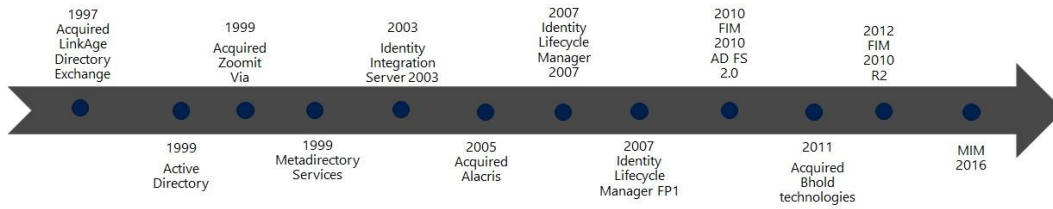
Office 365 Pro Plus
Exchange Online
Lync Online
SharePoint Online
Yammer

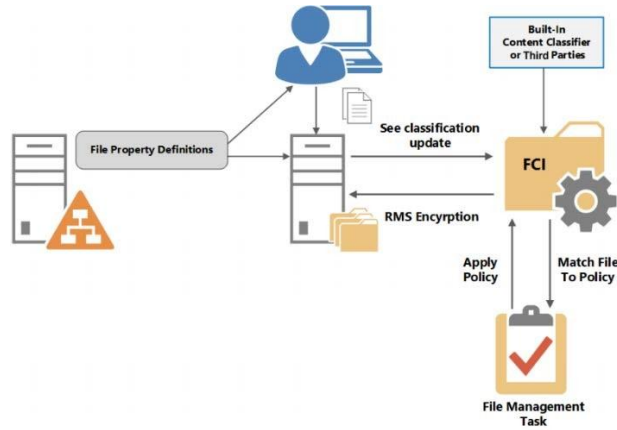
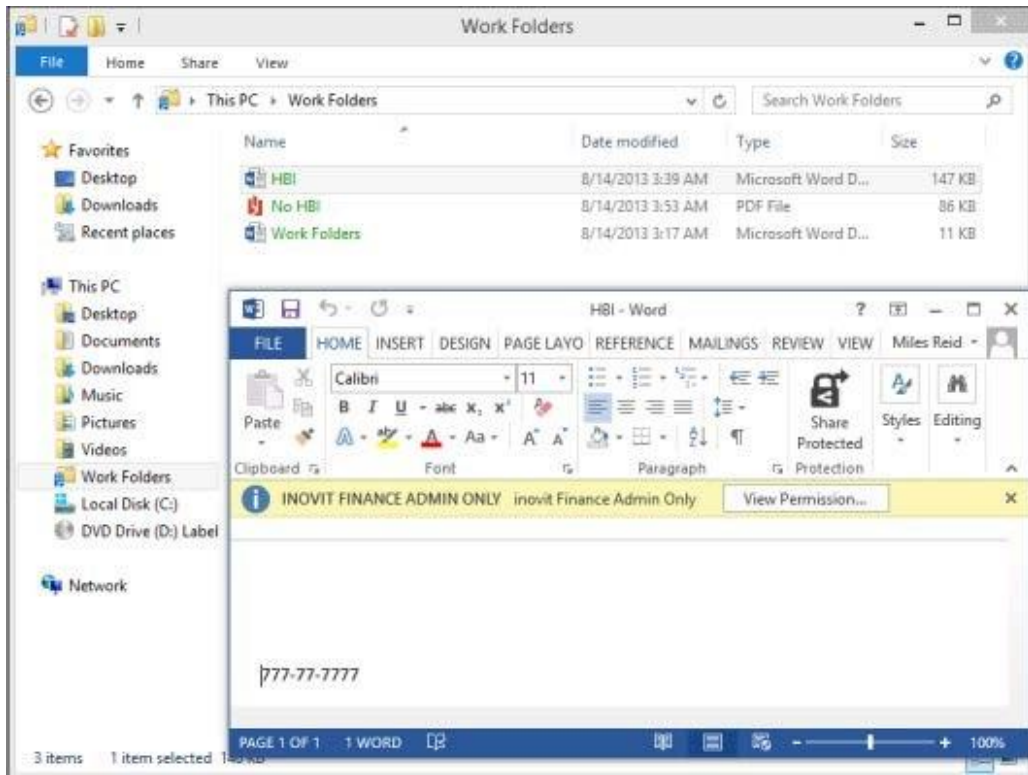
EMS

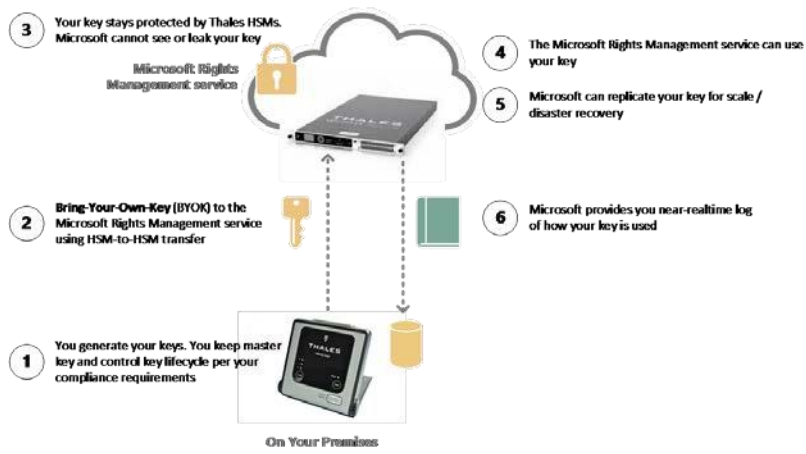
System Center CM
Windows Server CAL
Azure Rights Management
Windows Intune
Azure AD Premium

Windows SA Per User

Identity Synchronization	Delegation of Administration	Dynamic Groups
Provisioning / Deprovisioning	Self Service Password Reset	Certificate Management
Access Request Management	Self Service Group Management	Reporting & Compliance
Access Policy Management	Role Management (RBAC, ABAC, SoD)	Access Certification







Product	EA/VL	Open	CSP	MPN use rights	Direct purchase	Trial
Enterprise Mobility Suite	X	X	X	X		X
Azure AD Premium	X	X	X		X	X
Azure AD Basic	X	X	X	X		

	Global	Central US	East US	East US 2	US Gov Iowa	US Gov Virginia	North Central US	South Central US	West US	North Europe	West Europe	East Asia	Southeast Asia	Japan East	Japan West	Brazil South	Australia East	Australia Southeast
IDENTITY & ACCESS MANAGEMENT																		
Azure AD	●																	
Azure MFA	●																	
Azure AD B2B		●	●	●			●	●	●	●	●	●	●	●	●	●	●	●
Azure AD DS		●	●	●				●	●	●	●	●	●					

Global



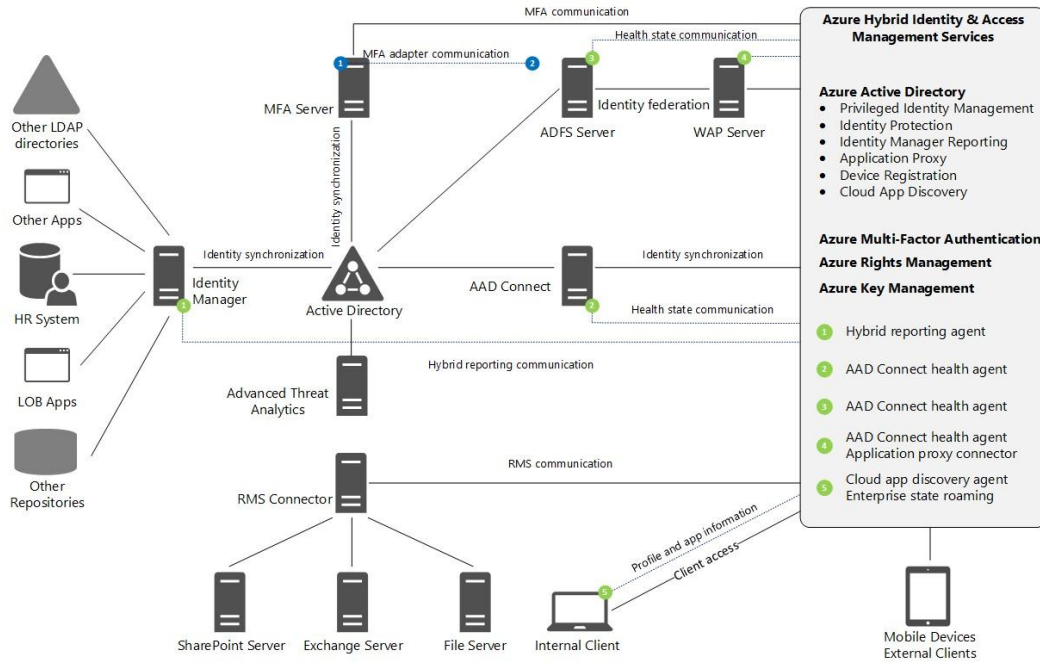
United States



Regional



Chapter 7: Designing Hybrid Identity Management Architecture



details
settings
licenses
more

Assign licenses

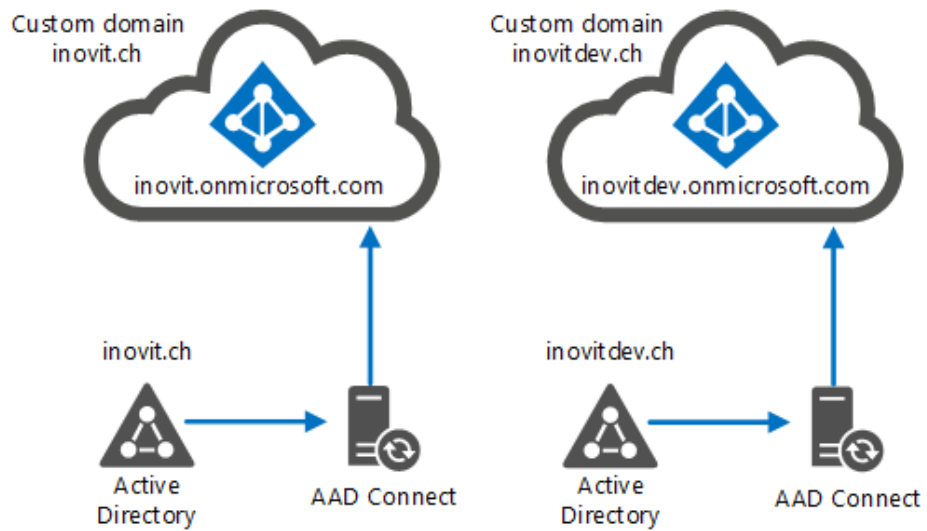
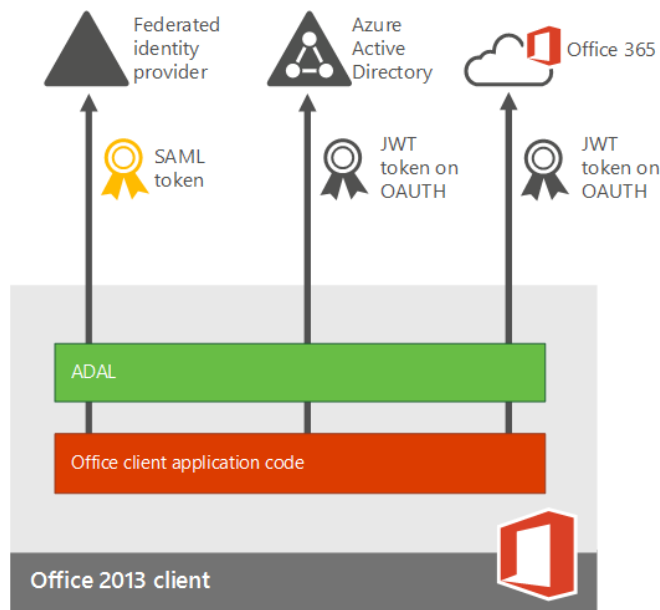
Microsoft Office 365 Plan E3

22 of 25 licenses available

[Buy more licenses](#)

- Yammer Enterprise
These licenses do not need to be individually assigned
- Windows Azure Active Directory Rights
- Office 365 ProPlus
- Lync Online (Plan 2)
- Office Online
- SharePoint Online (Plan 2)
- Exchange Online (Plan 2)

[Compare the various license options](#)



active directory

DIRECTORY ACCESS CONTROL NAMESPACES MULTI-FACTOR AUTH PROVIDERS RIGHTS MANAGEMENT

NAME	STATUS	ROLE	SUBSCRIPTION	DATACENTER REGION	COUNT...
inovit GmbH Development	✓ Active	Global Administrator	Shared by all inovit GmbH...	Europe, United States	Switzerland
inovit GmbH Production	✓ Active	Global Administrator	Shared by all inovit GmbH...	Europe, United States	Switzerland

settings

SUBSCRIPTIONS MANAGEMENT CERTIFICATES ADMINISTRATORS AFFINITY GROUPS USAGE REMOTEAPP

SUBSCRIPTION	SUBSCRIPTION ID	ACCOUNT ADMINISTRATOR	DIRECTORY
--------------	-----------------	-----------------------	-----------

EDIT YOUR SUBSCRIPTION



Make it yours

Personalize your subscriptions to keep them organized. [Privacy & Cookies](#)

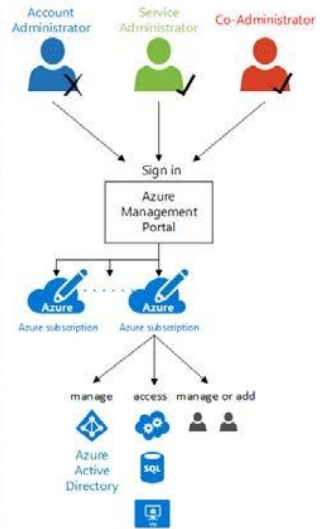
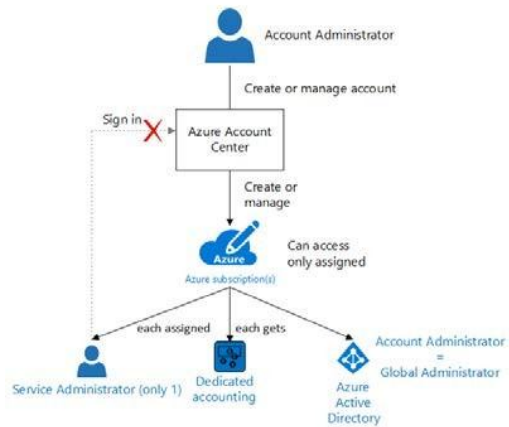
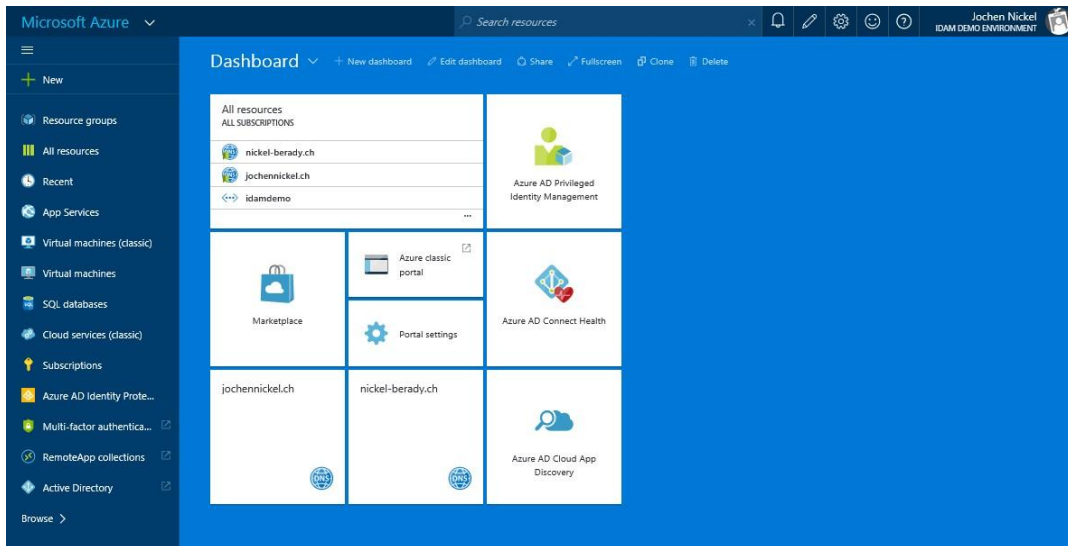
SUBSCRIPTION NAME

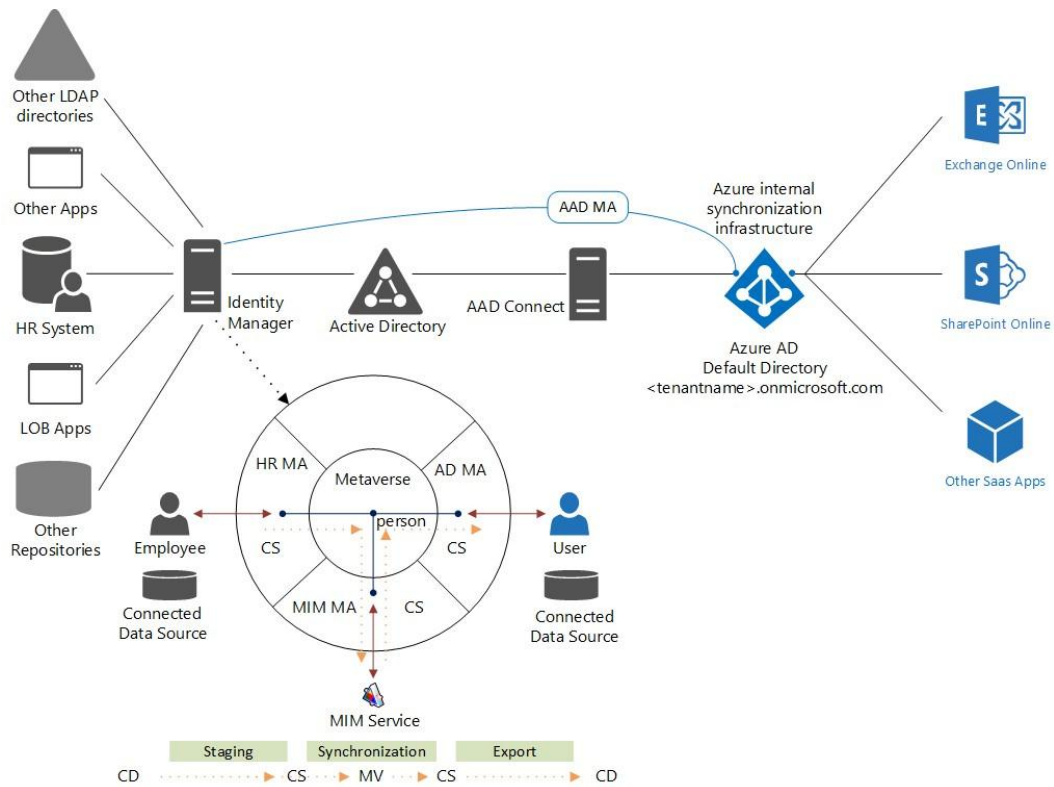
Visual Studio Enterprise with MSDN

SERVICE ADMINISTRATOR

Service.Administrator@outlook.com







SIMPLE

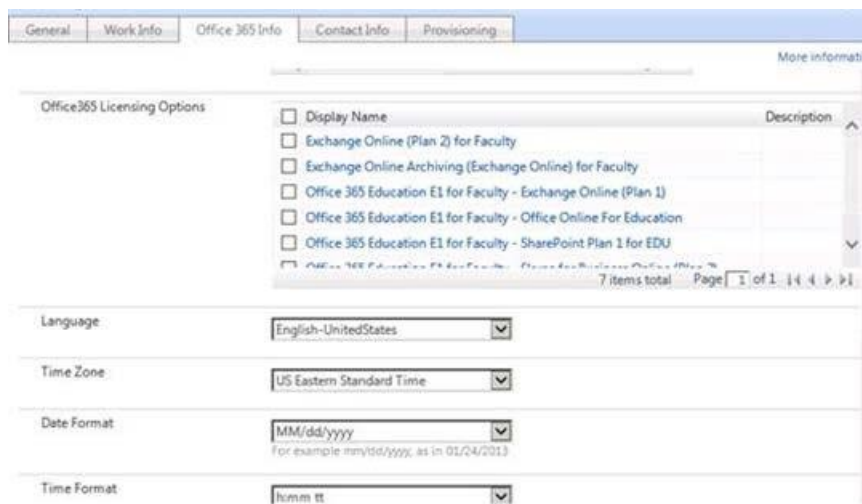
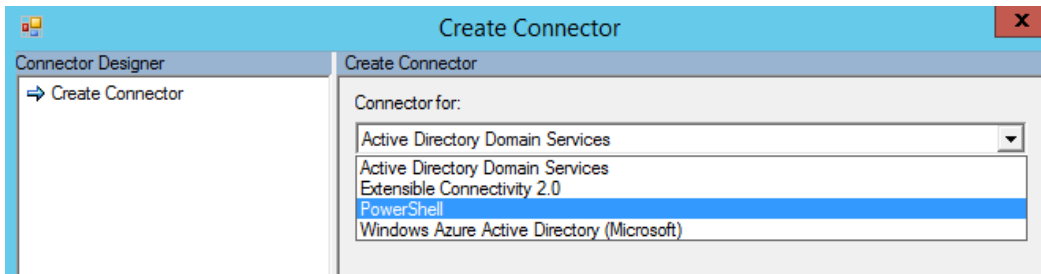
COMPLEX

AAD Connect

- Single-forest environments
- Common multi-forest environments
- Password hash synchronization for single and multi-forest environments
- Other repositories through ECMAv2

Identity Manager

- Advanced environments
- Multiple repositories
- Custom solutions
- Workflow-based solutions



SINGLE SIGN-ON **PROVISIONING**

user (azure ad) - user (salesforce sandbox)

SCOPING FILTERS

SCOPE NAME

EXAMPLE: INCLUDE EVERYONE FROM 'SALES' DEPARTMENT

add scope

ATTRIBUTE MAPPINGS

TARGET ATTRIBUTE (SALESFORCE SANDBOX)	SOURCE ATTRIBUTE (AZURE AD)	REQUIRED
IsActive	Not(!!\$SoftDeleted)	Yes
Alias	Mid(UserPrincipalName, 1, 8)	Yes
Email	mail	Yes
EmailEncodingKey	"ISO-8859-1" (default)	Yes
LanguageLocaleKey	"en_US" (default)	Yes
FirstName	givenName	Yes
LastName	surname	Yes
LocaleSidKey	Replace([preferredLanguage], "-", "_", ,)	Yes
ProfileName	SingleAppRoleAssignment([appRoleAssignments])	Yes
TimeZoneSidKey	"America/Los_Angeles" (default)	Yes
Username	userPrincipalName	Yes
UserPermissionsCallCenterAutoLogin	"False" (default)	Yes
UserPermissionsMarketingUser	"False" (default)	Yes
UserPermissionsOfflineUser	"False" (default)	Yes

add attribute mapping

MATCHING RULES

PRIORITY	TARGET ATTRIBUTE (SALESFORCE SANDBOX)	MATCHES WITH AZURE AD
1	Username	userPrincipalName

add matching rule

Synchronization Service Manager on AZIDIDM01

File Tools Actions Help

Operations Management Agents Metaverse Designer Metaverse Search Joiner

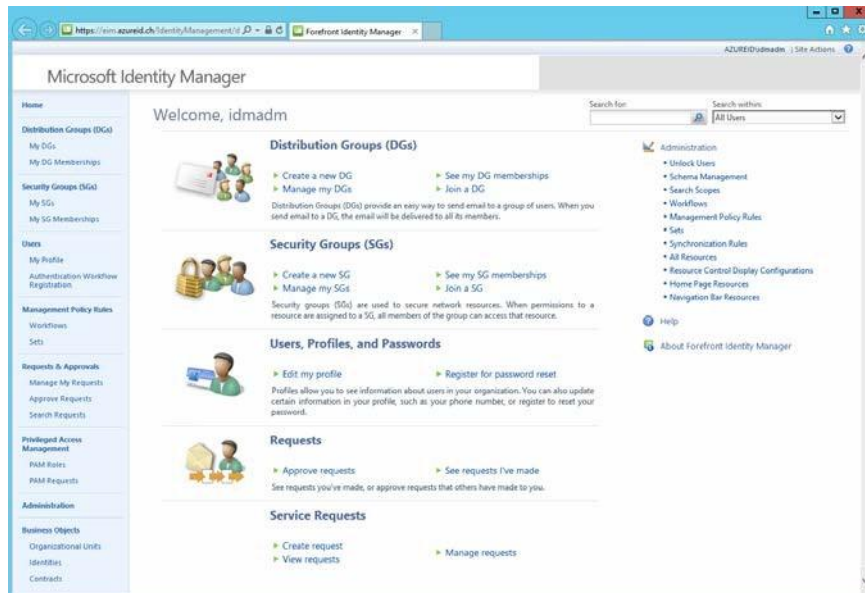
Management Agents

Name	Type	Description	State
IDM	FIM Service Management Agent		Idle
ADS	Active Directory Domain Services		Idle
HRS	SQL Server		Idle

Actions

- Create
- Properties
- Delete
- Configure Run Profiles
- Run
- Stop
- Export Management Agent
- Import Management Agent
- Update Management Agent
- Refresh Schema
- Search Connector Space

Total number of management agents: 3



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

PRIVPRIV.Jen

Roles for Elevation

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

Home / Role / Accounts Payable Clerk

- Modify
- Remove
- Change log
- Help
- ▾ Role attributes
- ▾ Extra Role Attributes
- ▾ Role Attributes
- ▾ Sub-roles (0)
- ▾ Parent roles (0)
- ▾ Inherited permissions (0)
- ▾ Permissions (6)
- ▾ Users (11)
- ▾ Policies (1)
- ▾ Organizational units (1)
- ▾ Proposed linked organizational units (0)
- ▾ Supervision

Microsoft Identity Manager

Profile Template Management

Help

Views

- All profile templates
- Smart card profile templates
- Software profile templates

Quick Links

- Main Menu

You can list profile templates, and then select one to change or copy.

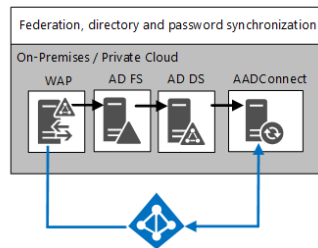
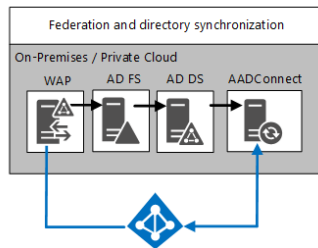
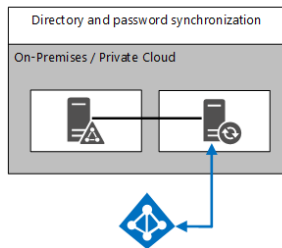
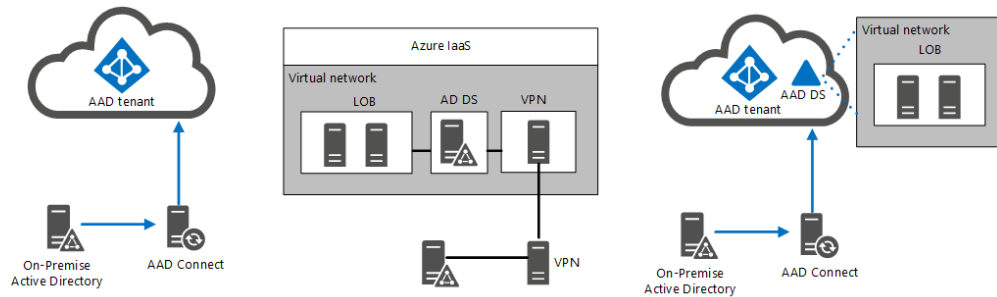
Profile Template List

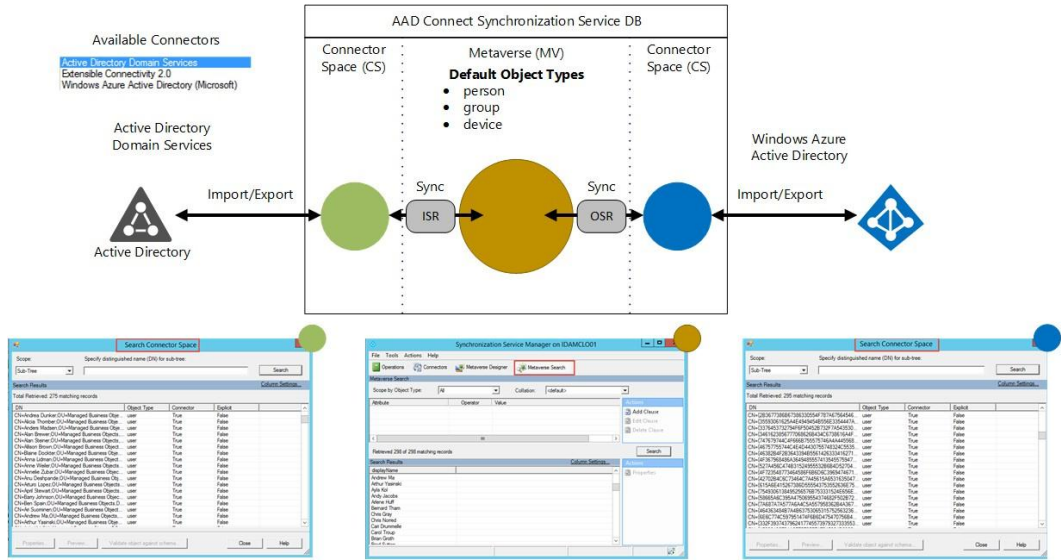
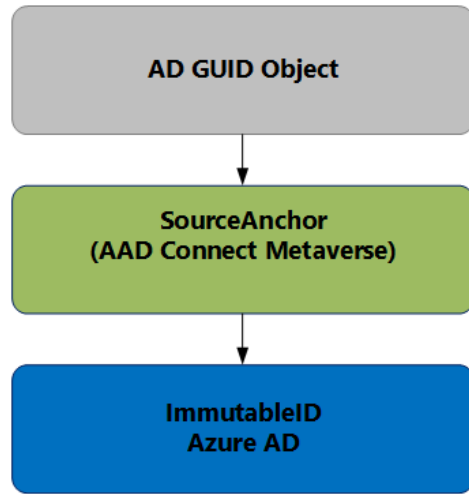
To change a profile template, click the template name.

To copy a template, select the check box, and then click **Copy a selected profile template**.

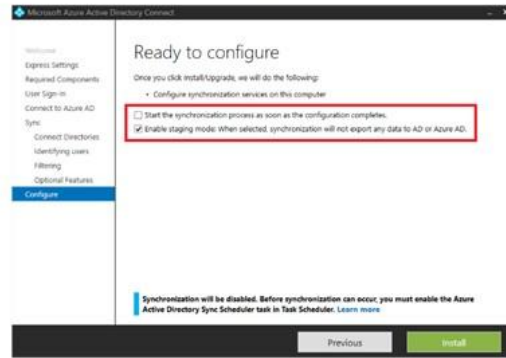
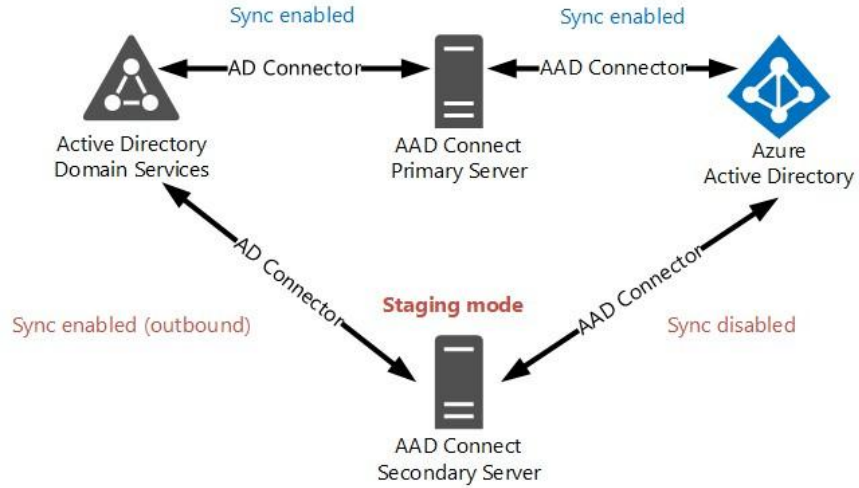
Selected	Name (click to edit)	Read only	Supports smart c...	Version	Description
<input type="checkbox"/>	FIM CM Sample Profile Template	X	X	1	Description of the template goe...
<input type="checkbox"/>	FIM CM Sample Smart Card Logon ...	X	✓	1	Description of the template goe...
<input type="checkbox"/>	Virtual Smart Card Logon Profile T...	X	✓	28	Description of the template goe...

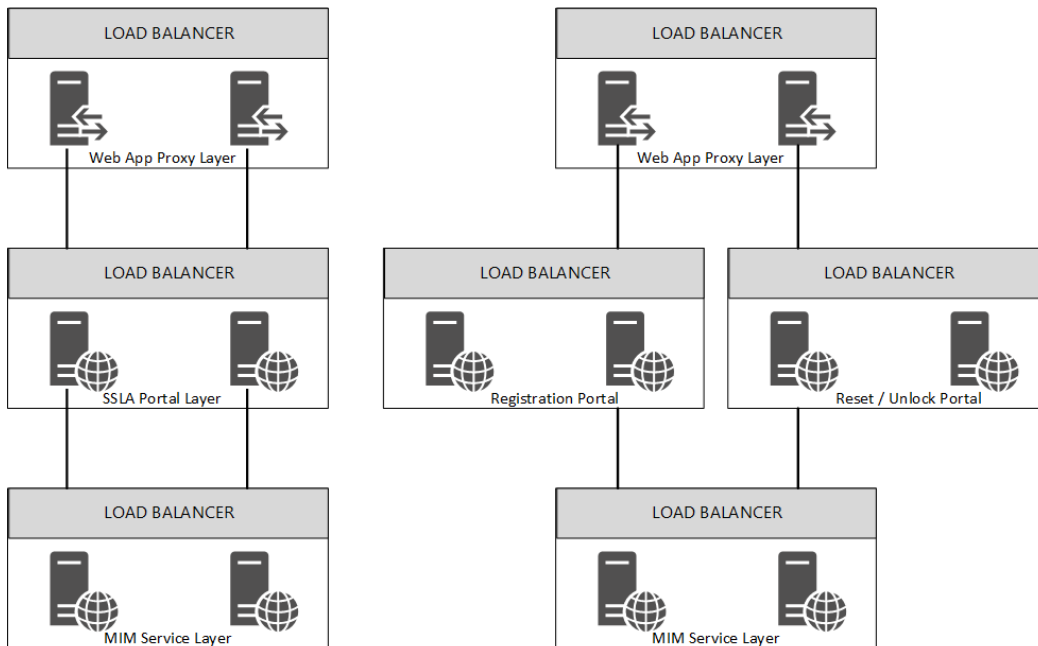
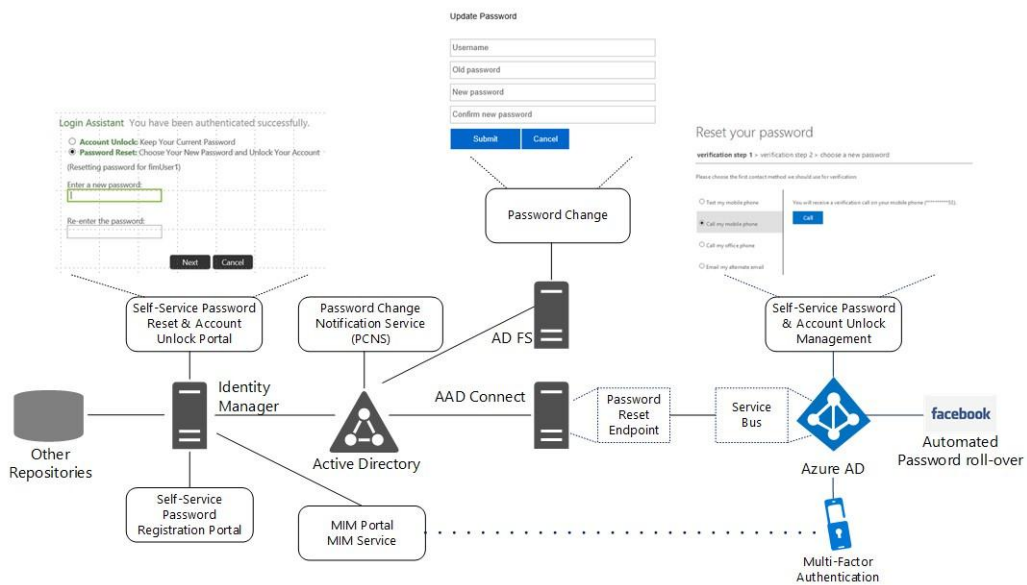
[Copy a selected profile template](#)



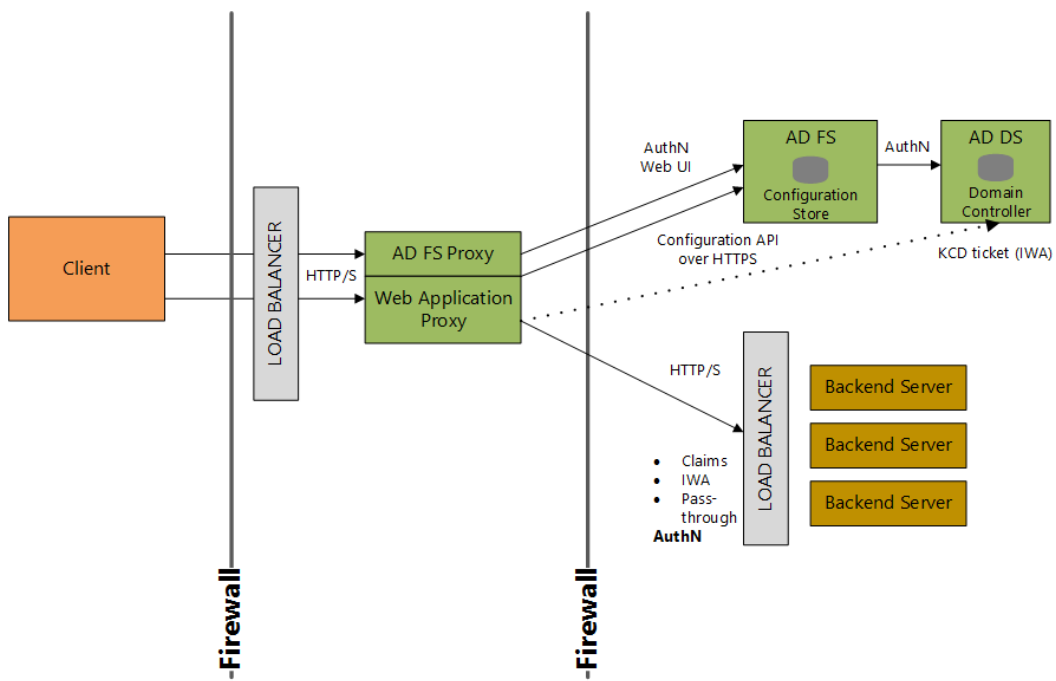


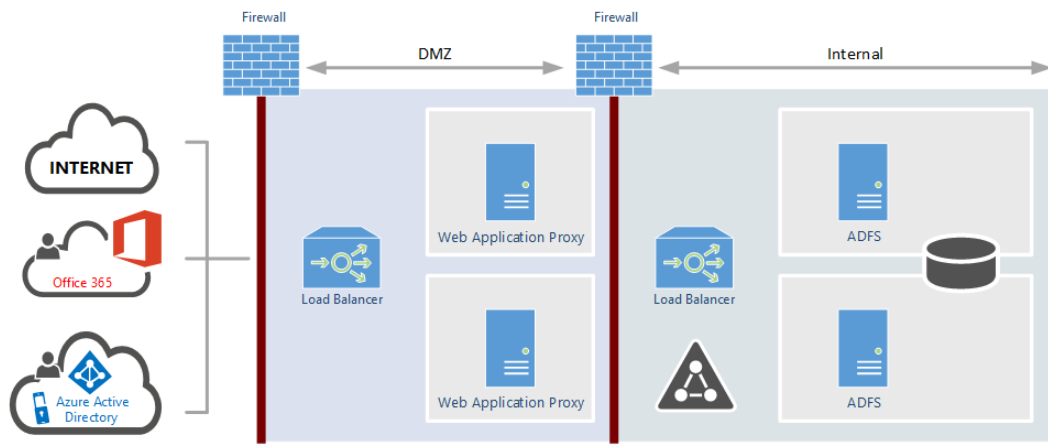
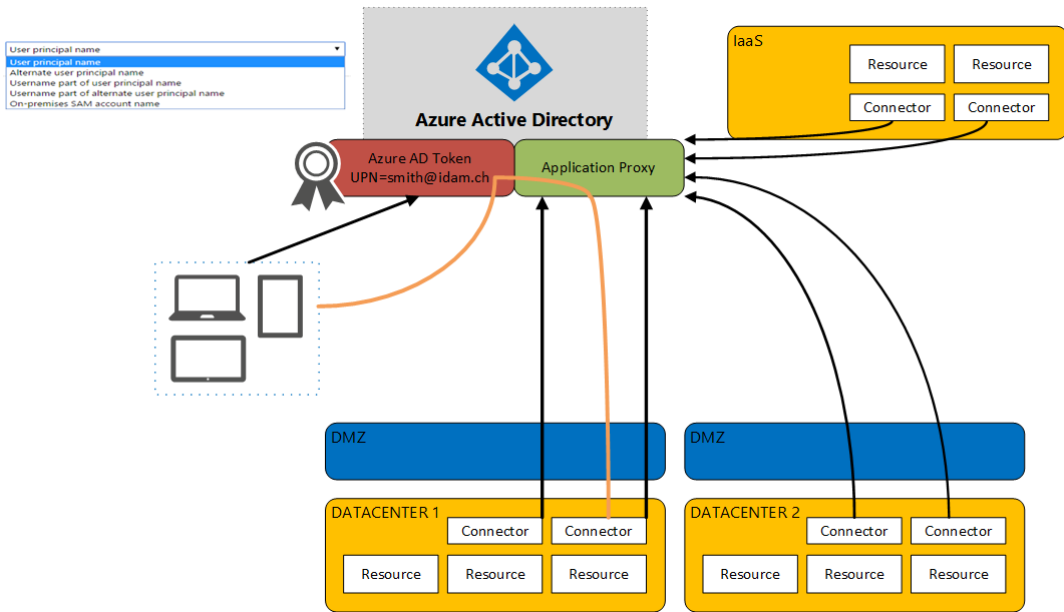
Full synchronization mode

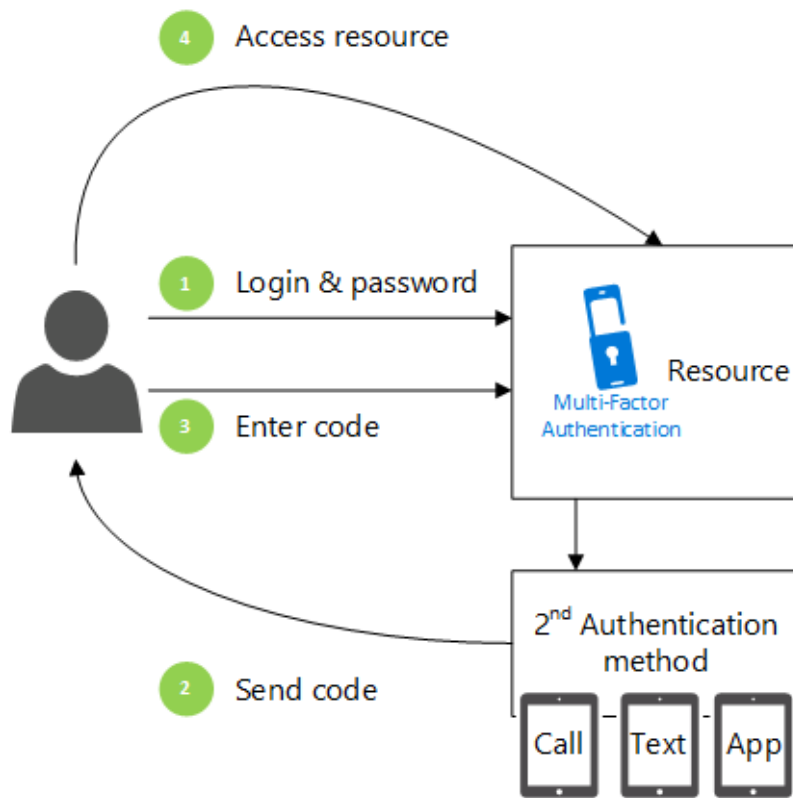


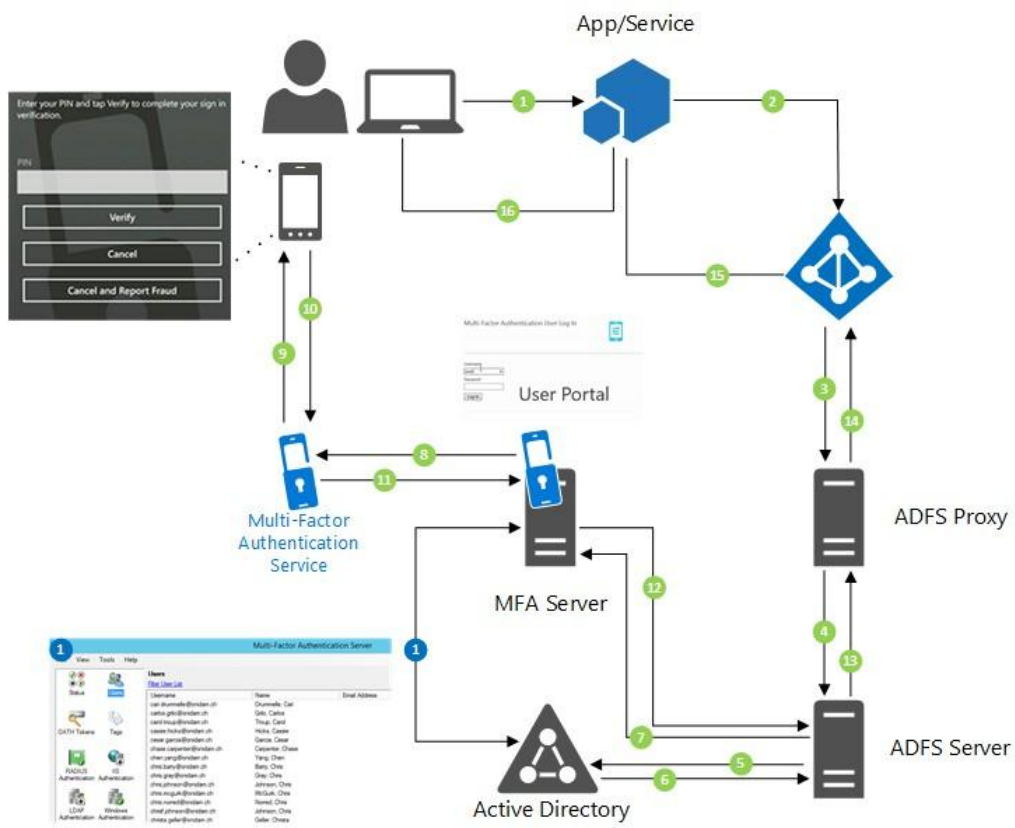


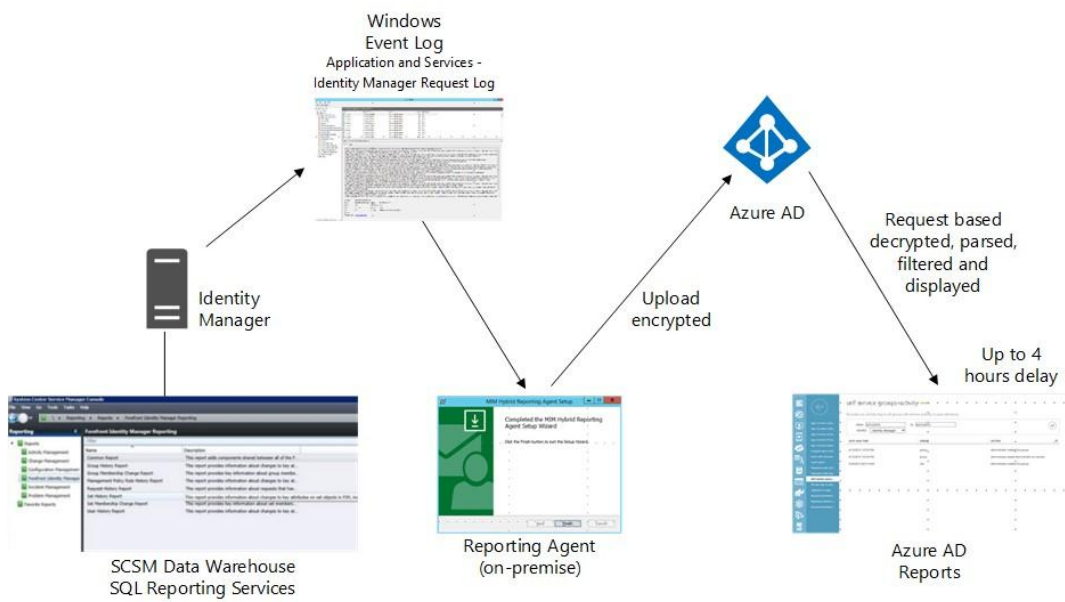
DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRI...
nickel-berady.ch	Custom	✓ Verified	Not Planned	No
jochennickel.ch	Azure AD IDP	✓ Verified	Not Planned	No
msazure.ch	Custom	✓ Verified	Not Planned	No
onidam.ch	On-Premise AD IDP	✓ Verified	Configured	No
idam.ch	Custom	✓ Verified	Configured	No
idamcloud.onmicrosoft.com	Basic	✓ Active	Not Available	Yes











- ←
- Sign ins from unkn...
- Sign ins after multi...
- Sign ins from multi...
- Sign ins from IP ad...
- Sign ins from possi...
- Irregular sign in act...
- Users with anomal...
- Audit report
- Password reset a...**
- Password reset reg...
- Self service groups...
- ...

password reset activity PREVIEW

Provides a detailed view of password resets that occur in your organization.

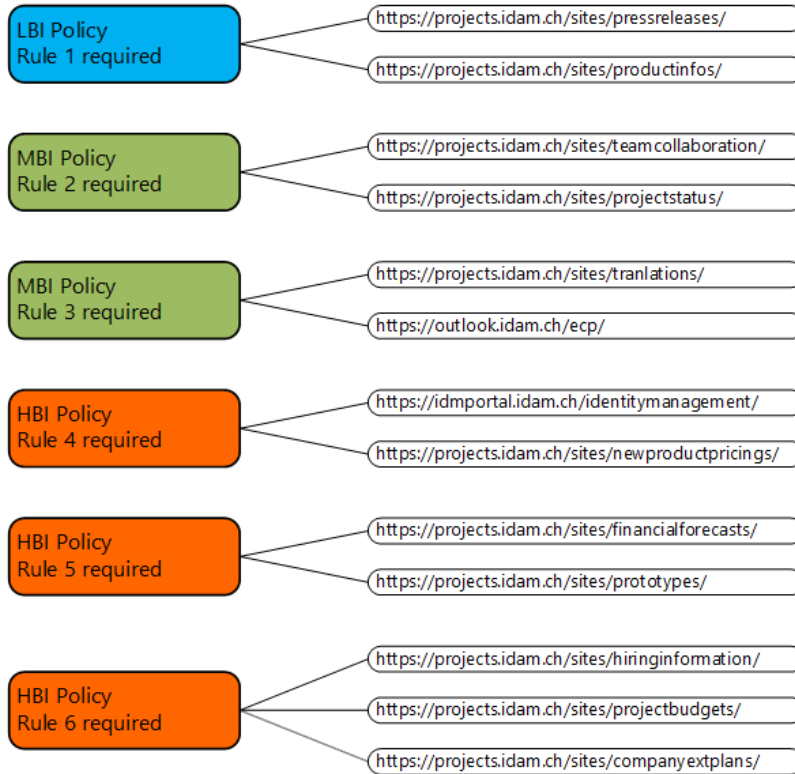
FROM TO

SOURCE

USER	ROLE	DATE AND TIME	METHOD(S) USED	RESULT
John Doe	User	5/10/2015 2:33:00 PM	Security Questions, Azure MFA	Succeeded

REPORT	DESCRIPTION
ANOMALOUS ACTIVITY	
Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Users with threatened credentials	Users with threatened credentials
Users with leaked credentials	Users with leaked credentials
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.
ACTIVITY LOGS	
Audit report	Audited events in your directory
Password reset activity	Provides a detailed view of password resets that occur in your organization.
Password reset registration activity	Provides a detailed view of password reset registrations that occur in your organization.
Self service groups activity	Provides an activity log to all group self service activity in your directory
Office365 Group Name Changes	Creations and name changes to Office 365 groups.
INTEGRATED APPLICATIONS	
Application usage	Provides a usage summary for all SaaS applications integrated with your directory.
Account provisioning activity	Provides a history of attempts to provision accounts to external applications.
Password rollover status	Provides a detailed overview of automatic password rollover status of SaaS applications.
Account provisioning errors	Indicates an impact to users' access to external applications.
RIGHTS MANAGEMENT	
RMS summary	Rights Management (RMS) usage summary
RMS active users	Top 1000 users who accessed content protected by Rights Management (RMS)
RMS device platforms	List of device platforms used to access content protected by Rights Management (RMS)
RMS application usage	Applications that accessed content protected by Rights Management (RMS)
EXTERNAL ACCESS	
Invitation summary	Invitation summary

Chapter 8: Planning Authorization and Information Protection Options



Services (Local)

Device Registration Service

[Stop the service](#)
[Restart the service](#)

Name	Description	Status	Startup Type	Log On As
Device Install Service	Enables a c...		Manual (Trig...	Local System
Device Registration Service	Enables Dev...	Running	Automatic (D...	IDAM\svcidf\$
Device Setup Manager	Enables the ...		Manual (Trig...	Local System
DHCP Client	Registers an...	Running	Automatic	Local Service

Device not joined to Active Directory



Device is Workplace joined



Device is joined in Active Directory



Personal device
with limited Access and
no IT Control
No SSO capabilities

Personal or corporate device
with applied IT governance
and controlled access to
applications
SSO capabilities SaaS
applications

Company owned device
Full IT control and full access
to applications
SSO capabilities on premise and
SaaS applications



User ID

Enter your user ID to get workplace access or turn on device management.

Someone@example.com

Workplace join

Join your workplace network so that you can use network resources like internal websites and business apps

Join

Turn on device management

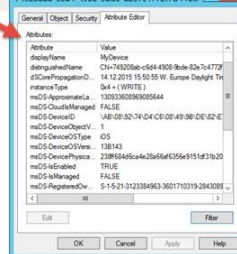
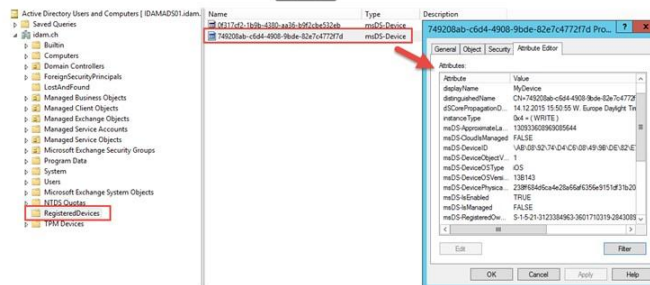
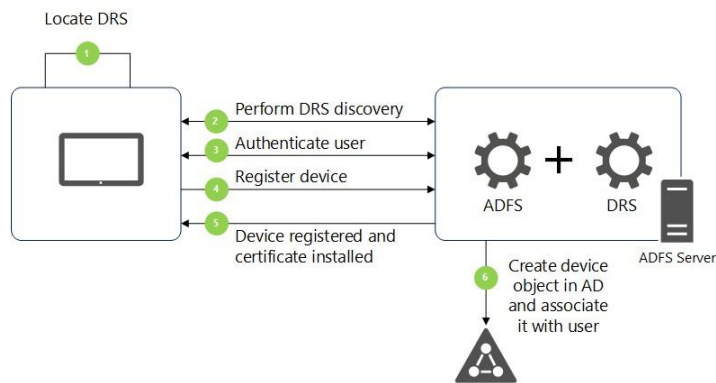
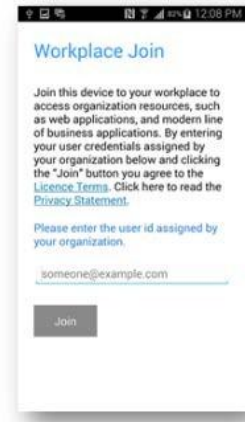
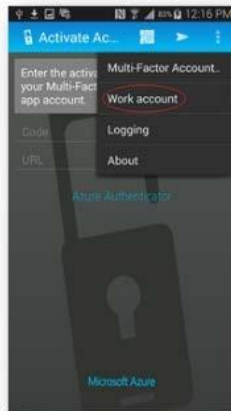
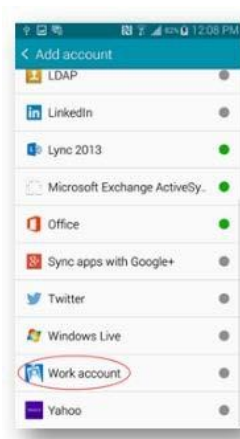
Register with your workplace so your IT admin can manage your device and provide apps and services for you. Try automatically detecting the server address, or if you have a server address from your IT admin, you can enter it manually.

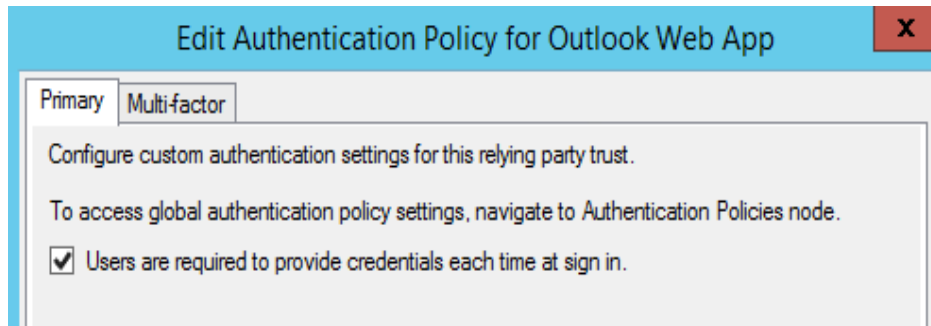
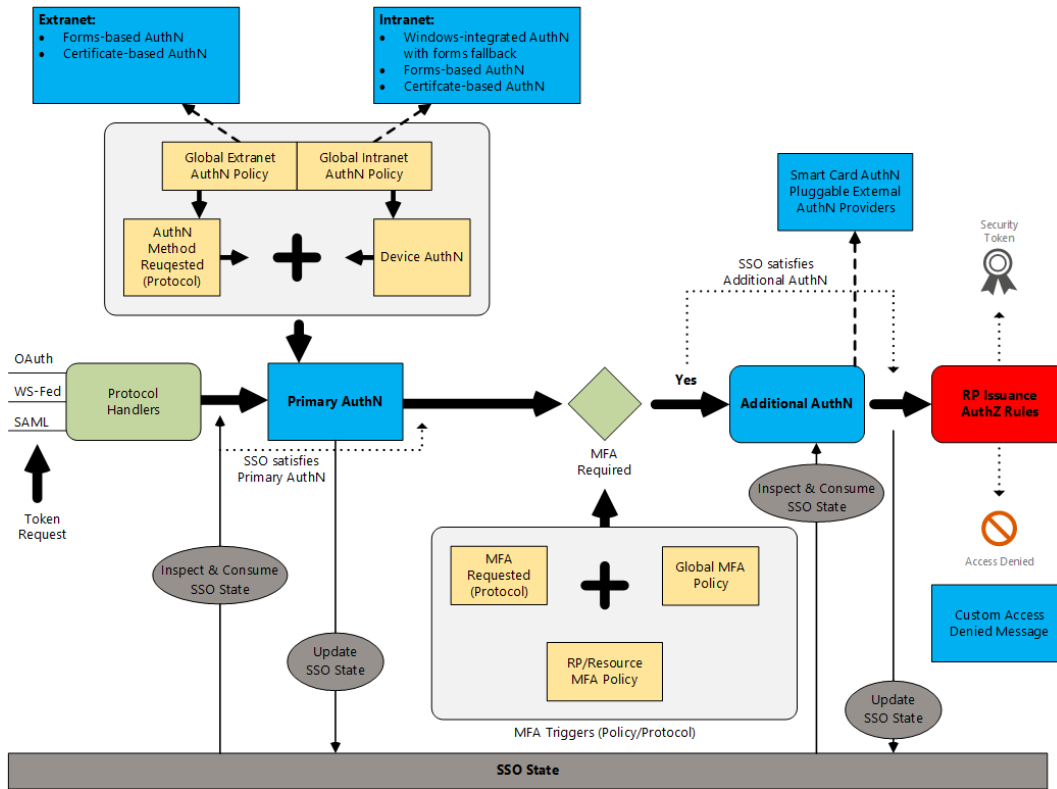
Automatically detect server address

On

Enter server address

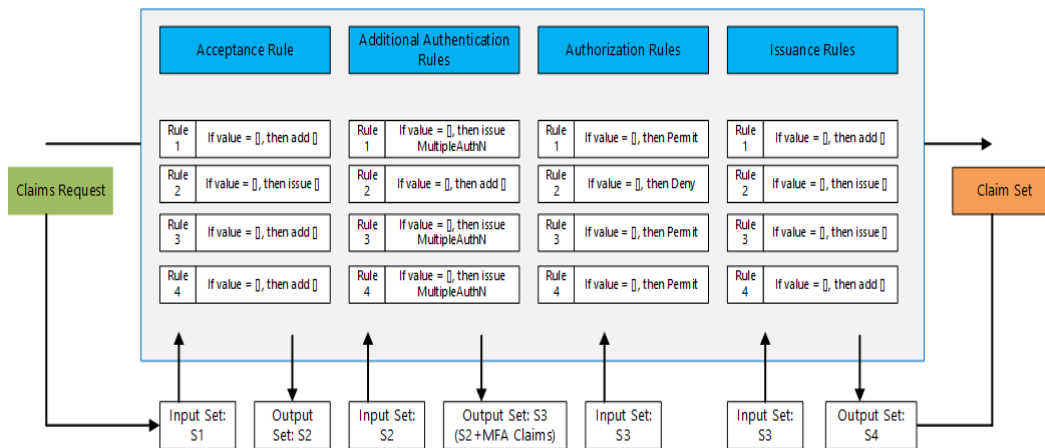
Turn on





Select additional authentication methods. You must select at least one of the following methods to enable MFA:

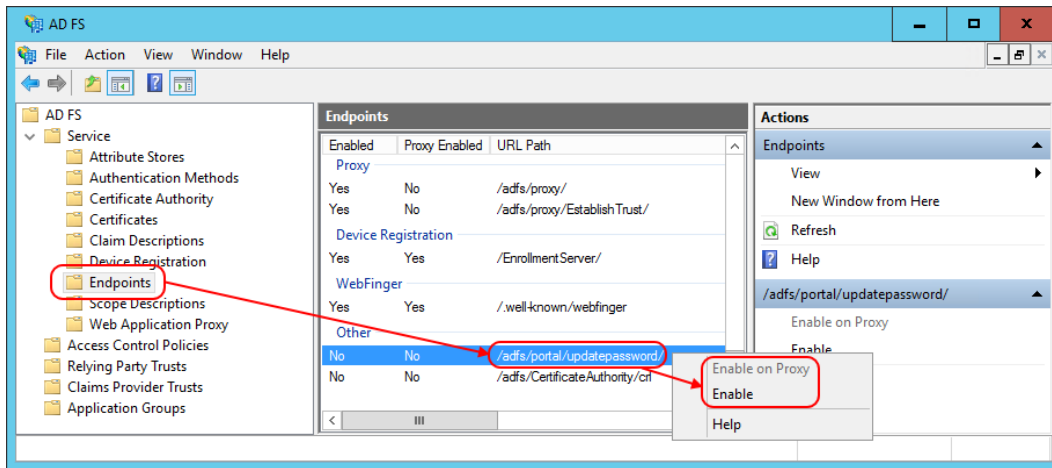
- Certificate Authentication
- WindowsAzureMultiFactorAuthentication



```

Administrator: Windows PowerShell
PS C:\Users\administrator.IDAM> Get-ADGroup sales

DistinguishedName : CN=Sales,OU=Managed Business Objects,DC=idam,DC=ch
GroupCategory     : Distribution
GroupScope       : Universal
Name             : Sales
ObjectClass      : group
ObjectGUID       : 239271ad-1e63-4ccb-972f-b6936ca3a28a
SamAccountName   : Sales
SID              : S-1-5-21-3123384963-3601710319-2843089171-2145
  
```



Edit Authentication Methods

Primary Multi-factor

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

- Certificate Authentication
- Azure MFA

Edit Authentication Methods [X]

Primary | Multi-factor

Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in.

If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication.

[Learn more](#) about Azure MFA (Multi-Factor Authentication).

Extranet

Forms Authentication
 Certificate Authentication
 Device Authentication

Intranet

Forms Authentication
 Windows Authentication
 Certificate Authentication
 Device Authentication

Info Azure MFA authentication methods will not be available until an Azure Active Directory Tenant is configured. [Learn More](#)

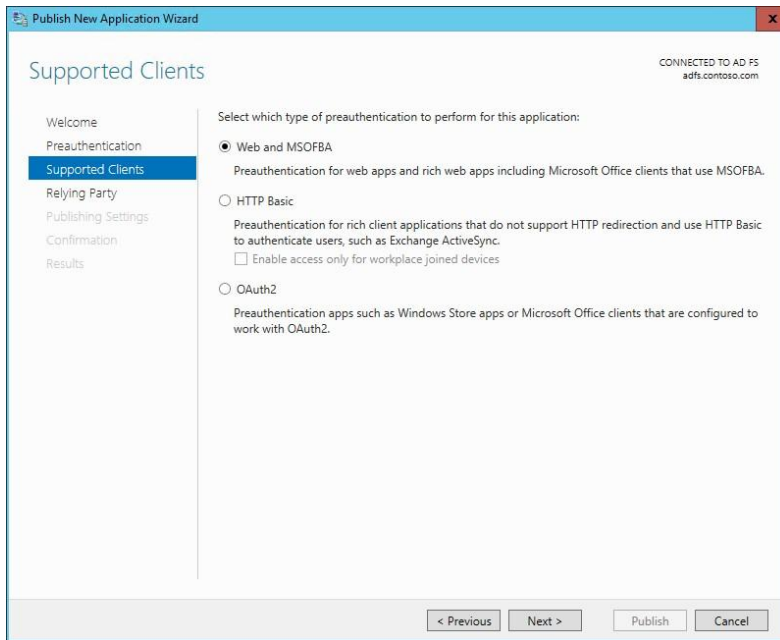
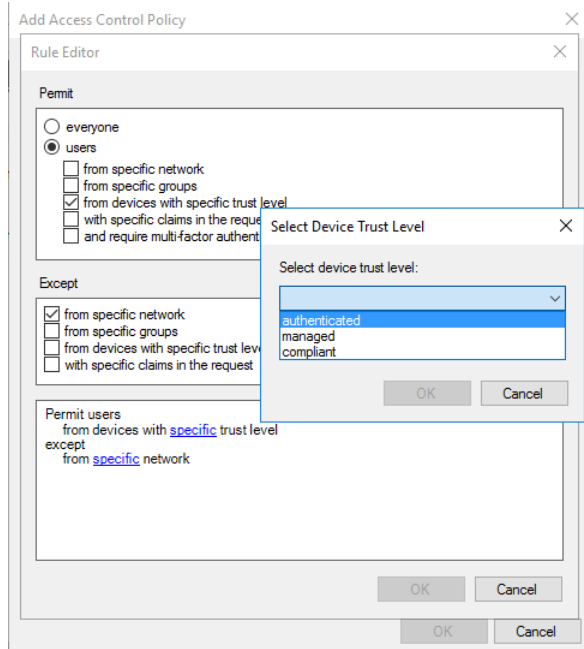
Standalone mode: AD FS issues certificates

Certificates for user logon and VPN access are issued by AD FS. This option is suitable for organizations that do not have an enterprise public key infrastructure set up.

Enrollment agent mode: AD FS requests certificates from Enterprise CA

AD FS requests an enterprise CA running Active Directory Certificate Services (AD CS) to issue certificates for user logon and VPN access. This option is suitable for organizations that have an existing public key infrastructure and require all certificates to be issued by the CA.

AD FS		Access Control Policies				
Service		Name	Built-in	Parameters	Usage	Modified
Attribute Stores		Permit everyone and require MFA from unauthen...	Yes	No	Not in use	11.12.2015 15:29
Authentication Methods		Permit everyone and require MFA	Yes	No	Not in use	11.12.2015 15:29
Certificate Authority		Permit everyone for intranet access	Yes	No	Not in use	11.12.2015 15:29
Certificates		Permit everyone	Yes	No	In use (1)	11.12.2015 15:29
Claim Descriptions		Permit everyone and require MFA from extranet ...	Yes	No	Not in use	11.12.2015 15:29
Device Registration		Permit specific group	Yes	Yes	Not in use	11.12.2015 15:29
Endpoints		Permit everyone and require MFA for specific gro...	Yes	Yes	Not in use	11.12.2015 15:29
Scope Descriptions						
Web Application Proxy						
Access Control Policies						
Relying Party Trusts						
Claims Provider Trusts						
Application Groups						



Publish New Application Wizard CONNECTED TO AD FS
adfs.contoso.com

Publishing Settings

Specify the publishing settings for this web application.

Name:
Claims Web
This name will appear in the list of published web applications.

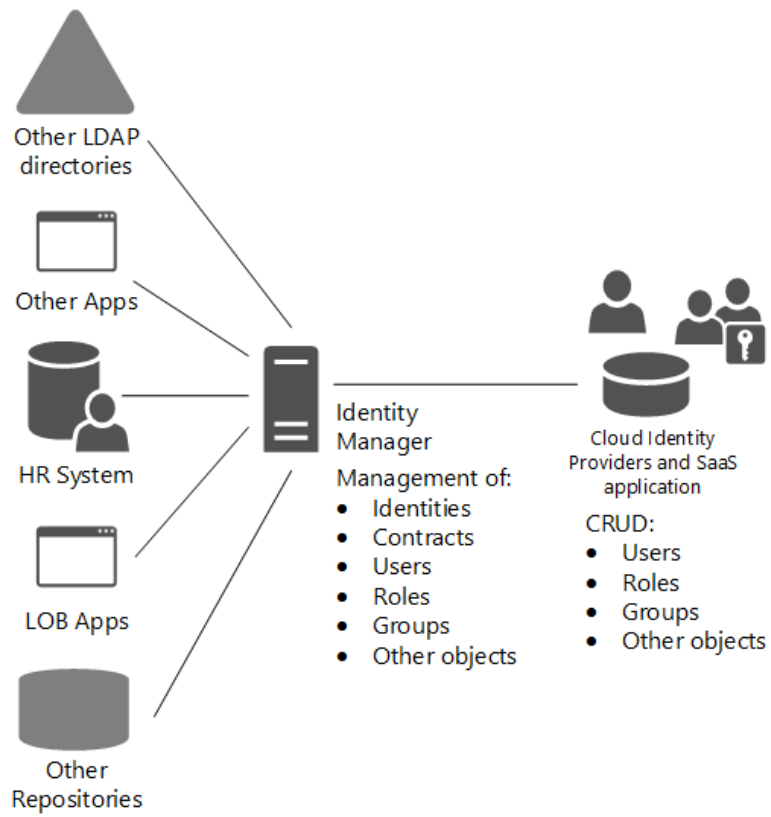
External URL:
https://claimsweb.contoso.com

External certificate:
*.contoso.com View...

Enable HTTP to HTTPS redirection

Backend server URL:
https://claimsweb.contoso.com

< Previous Next > Publish Cancel



Create Security Group

General | Members | Owners | Summary

[More information](#)

Display Name *

E-mail Enabled Enabled
Enable e-mail on a security group

Domain *

Account Name *

Scope *
Secures resources in a forest. Members must be in the same forest.

Member Selection *

- Manual**
Members are manually managed
- Manager-based**
Membership is calculated to include a manager, and all people reporting directly to that manager
- Criteria-based**
Membership is calculated based on one or more attributes of the members

1 Manage your identities and user accounts

Display Name	Domain	Account Name	Job Title	Office Location	Office Phone	E-mail
Paul Cost	CS&S	Paul.Cost				Paul.Cost@idam.ch
Sam Bandy	CS&S	Sam.Bandy				Sam.Bandy@idam.ch
James McFar	CS&S	James.McFar				James.McFar@idam.ch
Manager User1	CS&S	manu1				ManagerUser1@idam.ch
Manager User2	CS&S	manu2				ManagerUser2@idam.ch
Manager User3	CS&S	manu3				ManagerUser3@idam.ch
Manager User4	CS&S	manu4				ManagerUser4@idam.ch
Manager User5	CS&S	manu5				ManagerUser5@idam.ch
Manager User6	CS&S	manu6				ManagerUser6@idam.ch
Manager User7	CS&S	manu7				ManagerUser7@idam.ch
Manager User8	CS&S	manu8				ManagerUser8@idam.ch
Manager User9	CS&S	manu9				ManagerUser9@idam.ch
Manager User10	CS&S	manu10				ManagerUser10@idam.ch
Thomas Bognemann	CS&S	Thomas.Bognemann				Thomas.Bognemann@idam.ch

3 Create, Read, Update and Delete your identities in the cloud

managed user

user name:

last name:

first name:

middle name:

initials:

suffix:

display name:

email:

password:

confirm password:

include user in the organization:

2 Build up organizational or application access groups

Display Name	Description	E-mail
Marketing		Marketing@idam.ch
Sales		Sales@idam.ch
Sales Communications Review		SCR@idam.ch
Sales News		SNS@idam.ch
Sales Training Discussion		STD@idam.ch

4 Create, Read, Update and Delete your groups (roles) in the cloud

roles

name:

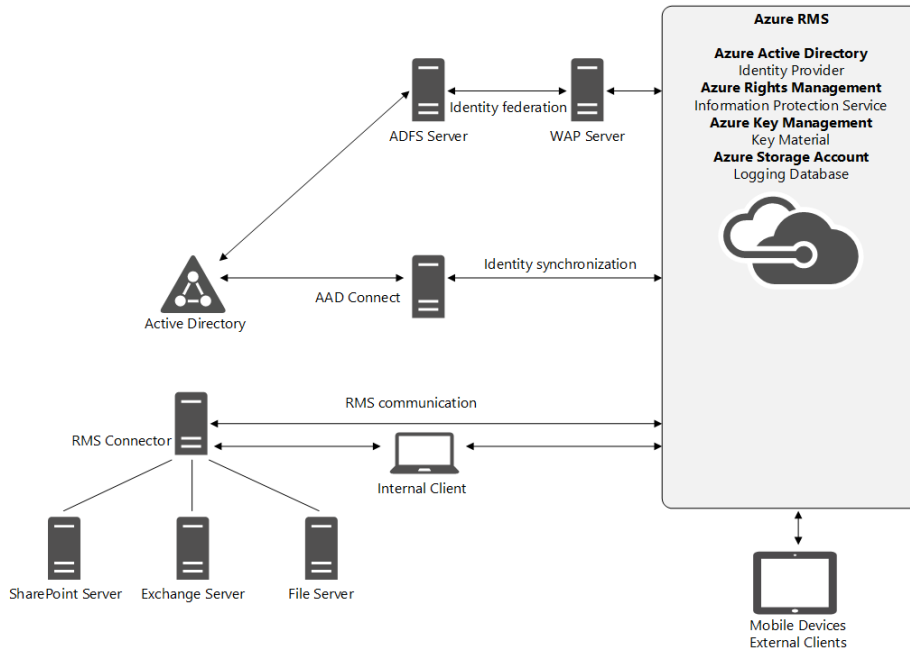
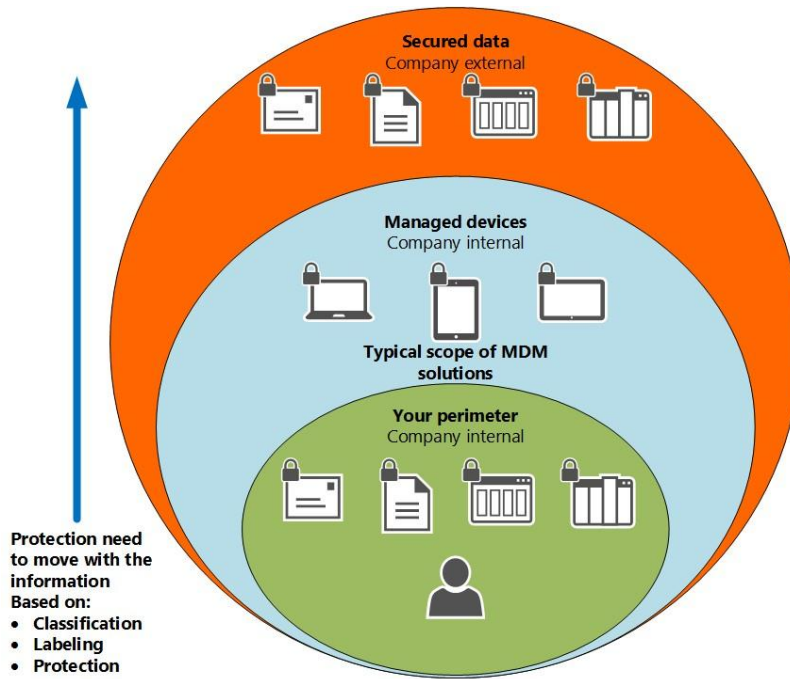
description:

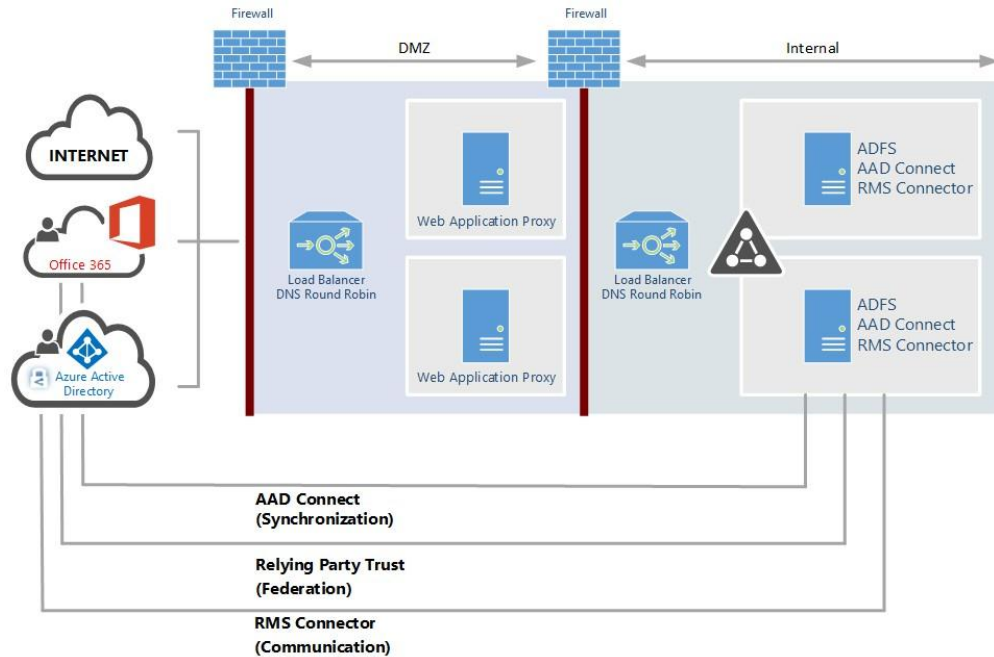
e-mail:

5 Assign access to your group (role)

ASSIGN ROLES

Name	Description	E-mail
Marketing		Marketing@idam.ch
Sales		Sales@idam.ch
Sales Communications Review		SCR@idam.ch
Sales News		SNS@idam.ch
Sales Training Discussion		STD@idam.ch





Attribute Name	User	Contact	Group	Comment
accountEnabled	X			Defines if an account is enabled.
cn	X		X	Common name or alias. Most often the prefix of [mail] value.
displayName	X	X	X	A string that represents the name often shown as the friendly name (first name last name).
mail	X	X	X	full email address.
member			X	
objectSID	X		X	mechanical property. AD user identifier used to maintain sync between Azure AD and AD.
proxyAddresses	X	X	X	mechanical property. Used by Azure AD. Contains all secondary email addresses for the user.
pwdLastSet	X			mechanical property. Used to know when to invalidate already issued tokens.
securityEnabled			X	Derived from groupType.
sourceAnchor	X	X	X	mechanical property. Immutable identifier to maintain relationship between ADDS and Azure AD.
usageLocation	X			mechanical property. The user's country. Used for license assignment.
userPrincipalName	X			This UPN is the login ID for the user. Most often the same as [mail] value.



idam Demo B2C En...

idam Development...

idam Demo Envir...

SEARCH ACTIVITY REPORTS
FROM TO USER

REPORT	DESCRIPTION
--------	-------------

ANOMALOUS ACTIVITY

Sign ins from unknown sources	May indicate an attempt to sign in without being traced.
Sign ins after multiple failures	May indicate a successful brute force attack.
Sign ins from multiple geographies	May indicate that multiple users are signing in with the same account.
Users with threatened credentials	Users with threatened credentials
Users with leaked credentials	Users with leaked credentials
Sign ins from IP addresses with suspicious activity	May indicate a successful sign in after a sustained intrusion attempt.
Sign ins from possibly infected devices	May indicate an attempt to sign in from possibly infected devices.
Irregular sign in activity	May indicate events anomalous to users' sign in patterns.
Users with anomalous sign in activity	Indicates users whose accounts may have been compromised.

ACTIVITY LOGS

Audit report	Audited events in your directory
Password reset activity	Provides a detailed view of password resets that occur in your organization.
Password reset registration activity	Provides a detailed view of password reset registrations that occur in your organization.

Self service groups activity	Provides an activity log to all group self service activity in your directory
Office365 Group Name Changes	Creations and name changes to Office 365 groups.

INTEGRATED APPLICATIONS

Application usage	Provides a usage summary for all SaaS applications integrated with your directory.
Account provisioning activity	Provides a history of attempts to provision accounts to external applications.
Password rollover status	Provides a detailed overview of automatic password rollover status of SaaS applications.
Account provisioning errors	Indicates an impact to users' access to external applications.

RIGHTS MANAGEMENT

RMS summary	Rights Management (RMS) usage summary
RMS active users	Top 1000 users who accessed content protected by Rights Management (RMS)
RMS device platforms	List of device platforms used to access content protected by Rights Management (RMS)
RMS application usage	Applications that accessed content protected by Rights Management (RMS)

EXTERNAL ACCESS

Invitation summary	Invitation summary
--------------------	--------------------

Your shared documents

Name	Date shared	View	Activity	Shared with
Confidential.docx	Aug 21, 2014, 5:04 pm	Today	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word
Confidential.docx	Aug 20, 2014, 11:00 am	Aug 20, 2014	Spn	SharePoint, Microsoft Exchange, Outlook, Microsoft Office Word, Microsoft Office Word, Microsoft Office Word

Confidential.docx

Summary List Timeline Map Notification settings

26 opens
by users

14 failures
by users

3 forwards
by users

3 days
since last activity

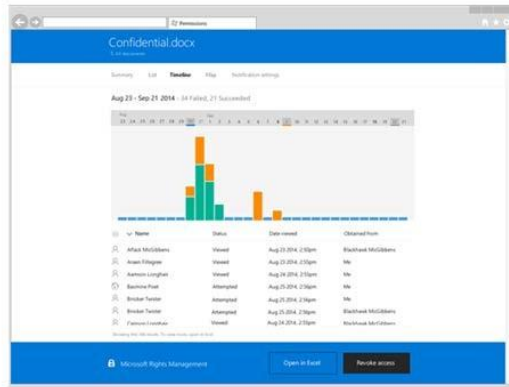
Shared on 5 May 2014
Expires on 5 June 2014

Confidential.docx

Summary List Timeline Map Notification settings

World-wide - 30 Failed, 7% Succeeded

Country	Name	Status	Date received	Obtained from
United States	John McMillen	Viewed	May 21, 2014, 2:30pm	Blackhawk McMillen
United States	Adam Longman	Viewed	May 21, 2014, 2:30pm	Mc
United States	Adam Longman	Viewed	May 21, 2014, 2:30pm	Mc
United States	Adam Longman	Viewed	May 21, 2014, 2:30pm	Mc
United States	Adam Longman	Viewed	May 21, 2014, 2:30pm	Mc



Confidential.docx

Revoke access

Shared on 5/21/14

Some recipients may have already opened the file. If so they will have access for up to 7 days after it is revoked.

I am revoking this document

Notify users that document has been revoked

Cancel Revoke access

Confidential.docx

Summary List Timeline Map Notification settings

26 opens
by users

14 failures
by users

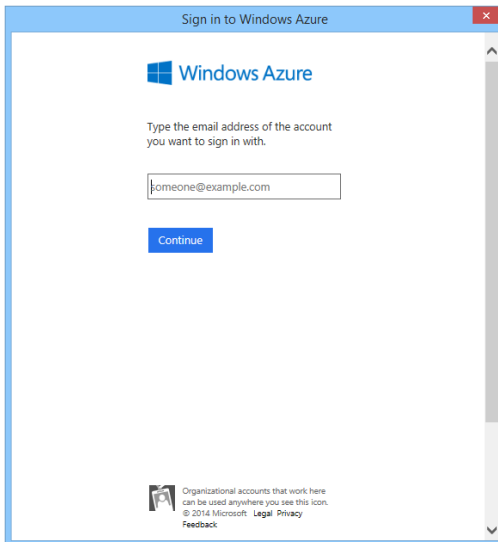
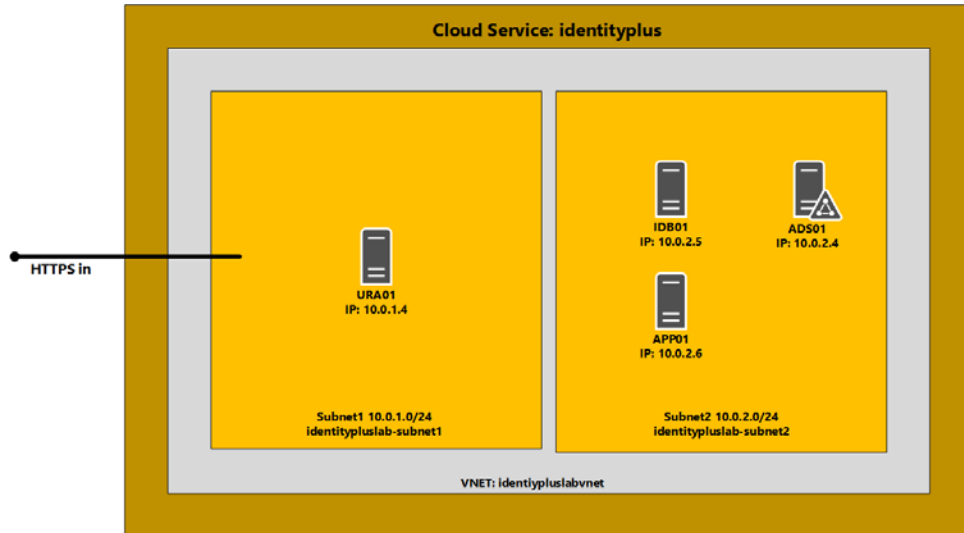
3 forwards
by users

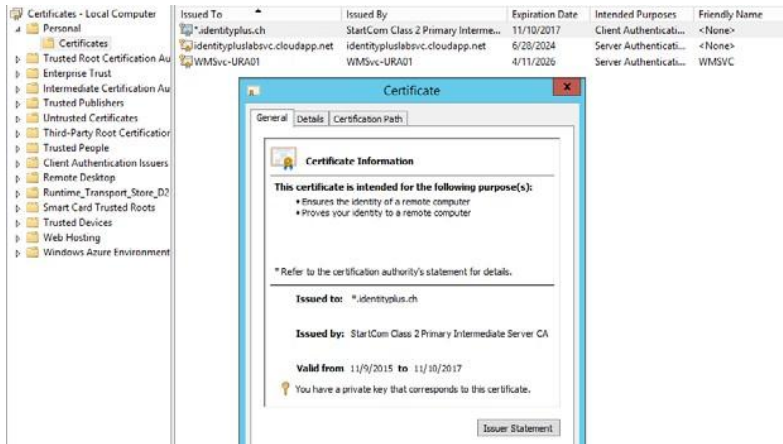
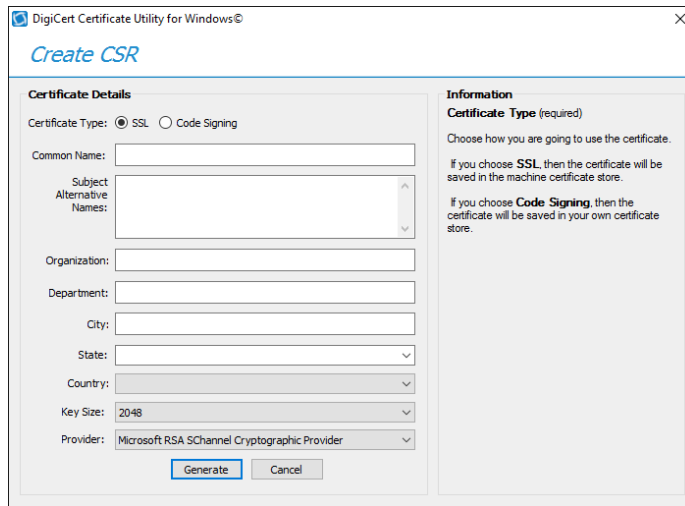
3 days
since last activity

Revoked on 16 May 2014
Shared on 5 May 2014
Expires on 5 June 2014

Open in Excel

Chapter 9: Building Cloud from Common Identities





CREATE A VIRTUAL MACHINE

Virtual machine configuration

identitypluslabsvc cloudapp.net

REGION/AFFINITY GROUP/VIRTUAL NETWORK
identitypluslabnet

VIRTUAL NETWORK SUBNETS
identitypluslabnet-subnet2[10.0.2.0/24]

STORAGE ACCOUNT
identitypluslabstor

AVAILABILITY SET
[None]

ENDPOINTS

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT
Remote Desktop	TCP	AUTO	3389
PowerShell	TCP	5986	5986

ENTER OR SELECT A VALUE

Windows Server 2012 R2 Datacenter

At the heart of the Microsoft Cloud OS vision, Windows Server 2012 R2 brings Microsoft's experience delivering global-scale cloud services into your infrastructure. It offers enterprise-class performance, flexibility for your applications and excellent economics for your datacenter and hybrid cloud environment. This image includes Windows Server 2012 R2 Update.

OS FAMILY
Windows

PUBLISHER
Microsoft Windows Server Group

NUMBER OF DISKS
1

PRICING INFORMATION
Pricing varies based on the subscription you select to provision your virtual machine.

virtual machines

INSTANCES IMAGES DISKS



NAME	STATUS	SUBSCRIPTION	LOCATION	DNS NAME
ads01	Running	Visual Studio Enterprise with MS...	identitypluslabaff (Central US)	identitypluslabsvc.cloudapp.net
app01	Stopped	Visual Studio Enterprise with MS...	identitypluslabaff (Central US)	identitypluslabsvc.cloudapp.net
idb01	Stopped	Visual Studio Enterprise with MS...	identitypluslabaff (Central US)	identitypluslabsvc.cloudapp.net
ura01	Stopped	Visual Studio Enterprise with MS...	identitypluslabaff (Central US)	identitypluslabsvc.cloudapp.net
idplusidm01	Stopped (Deallocated)	Visual Studio Enterprise with MS...	Central US	idplusidm01.cloudapp.net

Select server roles

DESTINATION SERVER
idb01.identityplus.ch

- Before You Begin
- Installation Type
- Server Selection
- Server Roles**
- Features
- AD FS
- Confirmation

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

Description

Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.

Post-deployment Configura... TASKS | X

Configuration required for Active Directory Federation Services at IDB01

[Configure the federation service on this server.](#)

SSL Certificate: login.identityplus.ch Import...

[View](#)

Federation Service Name: login.identityplus.ch

Example: fs.contoso.com

Federation Service Display Name: IDplus Login

Users will see the display name at sign in.
Example: Contoso Corporation

Select the role services to install for Remote Access

Role services

- DirectAccess and VPN (RAS)
- Routing
- Web Application Proxy

Post-deployment Configura... TASKS | X

Configuration required for Web Application Proxy at URA01

[Open the Web Application Proxy Wizard](#)

Type	Host Name	Port	IP Address	Binding Informa...
https	claims.identityplus.ch	443	*	

Buttons: Add..., Edit...

```

CertificateType : Token-Signing
IsPrimary       : True
StoreLocation   : CurrentUser
StoreName       : My
Thumbprint      : 9B578A4742B7E3354B2D9B741D7666D4723E05C6
  
```

Import data about the relying party published online or on a local network
 Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

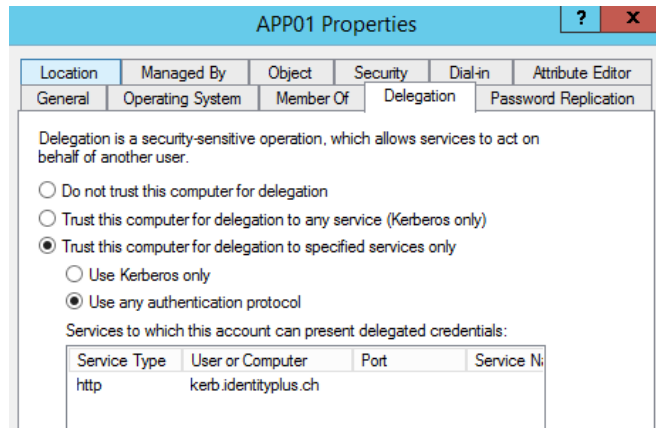
MY CLAIMSWEB Welcome | [Sign out](#)

[Home](#) [About](#)

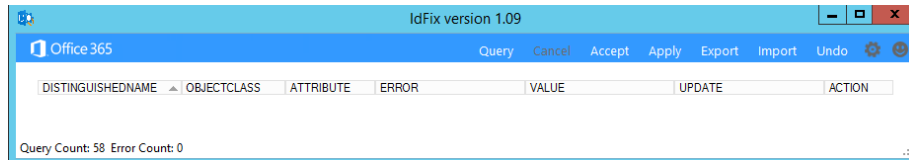
WELCOME CLAIMSWEB!

Issued Identity			
Claim Type	Claim Value	Issuer	OriginalIssuer
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows	http://login.identityplus.ch/adfs/services/trust	http://login.identityplus.ch/adfs/services/trust
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2016-04-16T19:55:58.488Z	http://login.identityplus.ch/adfs/services/trust	http://login.identityplus.ch/adfs/services/trust

SAML Token	
Raw SAML Token	
Property	Value
SamlSecurityToken.Id	_ca5a9619-44b0-46ef-9a8b-959e5b5a6d0c
SamlSecurityToken.ValidFrom	4/16/2016 7:59:11 PM
SamlSecurityToken.ValidTo	4/16/2016 8:59:11 PM (60 minutes)
SamlSecurityToken.Assertion.AssertionId	_ca5a9619-44b0-46ef-9a8b-959e5b5a6d0c
SamlSecurityToken.Assertion.Issuer	http://login.identityplus.ch/adfs/services/trust



Relying Party Trusts				
Display Name	Enabled	Type	Identifier	
Device Registration Service	Yes	WS-T...	um.ms-drs.login.identityplus.ch	
Claims Demo Web Site	Yes	WS-T...	https://claims.identityplus.ch/	
Microsoft Office 365 Identity Platform	Yes	WS-T...	https://login.microsoftonline.com/ext...	







Domain and OU filtering

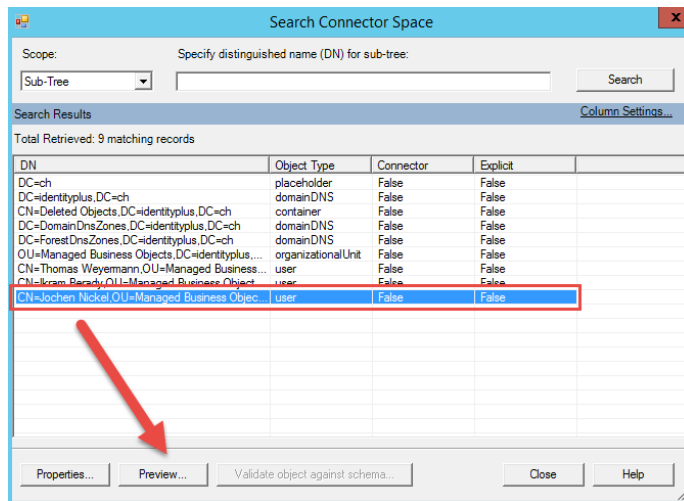
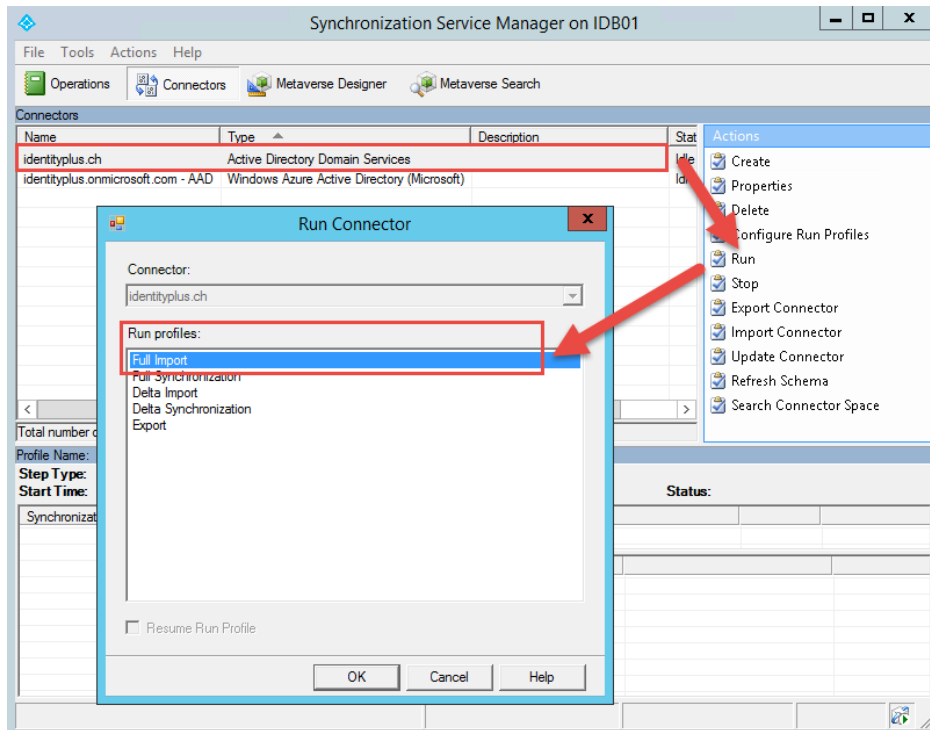
Directory: [Refresh Ou/Domain](#) ?

Sync all domains and OUs
 Sync selected domains and OUs

- identityplus.ch
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Infrastructure
 - LostAndFound
 - Managed Business Objects
 - Managed Service Accounts
 - NTDS Quotas
 - Program Data
 - System
 - Users
 - Configuration

Azure AD Connect

-  Azure AD Connect **NEW**
-  Synchronization Rules Editor **NEW**
-  Synchronization Service **NEW**
-  Synchronization Service Key... **NEW**



Sync Rule	Data Source	Mapping Type	Data Source Attribute	Initial Value	Final Value
Out to AAD - User Join	accountEnabled	Direct	accountEnabled	true	(Unchanged)
Out to AAD - User Join	cn	Direct	commonName	Jochen Nickel	(Unchanged)
Out to AAD - User Join	domainFQDN	Direct	dnsDomainName	identityplus.ch	(Unchanged)
Out to AAD - User Join	pwdLastSet	Direct	lastPasswordChangeTi...	20160416184931...	(Unchanged)
Out to AAD - User Join	domainNetBios	Direct	netBiosName	IDENTITYPLUS	(Unchanged)
Out to AAD - User Join	accountName	Direct	onPremisesSamAccoun...	jni	(Unchanged)
Out to AAD - User Join	objectSid	Direct	onPremiseSecurityIdenti...	01 05 00 00 00 0...	(Unchanged)
Out to AAD - User Join	"CN={}" & Convert ToUT...	Expression	dn		CN=(425A5334
Out to AAD - User Join	IIF(IsPresent([cloud Sour...	Expression	sourceAnchor	BZS4PDARU+L...	(Unchanged)
Out to AAD - User Identity	displayName	Direct	displayName	Jochen Nickel	(Unchanged)
Out to AAD - User Identity	givenName	Direct	givenName	Jochen	(Unchanged)
Out to AAD - User Identity	sn	Direct	sumame	Nickel	(Unchanged)
Out to AAD - User Identity	userPrincipalName	Direct	userPrincipalName	jochen.nickel@id...	(Unchanged)
Out to AAD - User Exchan...	IIF(IsNullOrEmpty([count...	Expression	countryCode	0	(Unchanged)

Operations Connectors Metaverse Designer **Metaverse Search**

Metaverse Search

Scope by Object Type: All Collation: <default>

Attribute	Operator	Value

Retrieved 1 of 1 matching records

Search Results Column Settings...

Attribute	Value
displayName	Jochen Nickel

Actions: Add Clause, Edit Clause, Delete Clause, Search, Properties

```
PS C:\> Get-ADSyncScheduler

AllowedSyncCycleInterval       : 00:30:00
CurrentlyEffectiveSyncCycleInterval : 00:30:00
CustomizedSyncCycleInterval    :
NextSyncCyclePolicyType        : Initial
NextSyncCycleStartTimeInUTC    : 4/18/2016 9:26:27 AM
PurgeRunHistoryInterval       : 7.00:00:00
SyncCycleEnabled               : False
MaintenanceEnabled             : True
StagingModeEnabled             : False
```

Name: In from AD - User Exclude

Description: Users that match this rule will not be synchronized to the Azure Active Directory

Connected System: identityplus.ch

Connected System Object Type: user

Metaverse Object Type: person

Link Type: Join

Precedence: 50

Tag:

Enable Password Sync:

Disabled:

Attribute information:

Changes	Attribute Name	Type	Value
none	cn	string	Ikram Nickel
none	countryCode	number	0
none	givenName	string	Ikram
none	objectGUID	binary	8E D0 AB EF 2C E7 81 4D 81 76 96 97 09 59 8E 5A
none	objectSid	binary	01 05 00 00 00 00 05 15 00 00 00 DE B8 EA C4 30 010 21 53 A3 DE 69 72 38 08 00...
none	pwdLastSet	number	131053061723980085
none	sAMAccountName	string	ini
none	sn	string	Nickel
none	userAccountControl	number	512
none	userPrincipalName	string	ikram.nickel@identityplus.ch

Connector Space Object Properties

Awaiting Export Confirmation | Lineage |

Distinguished Name: CN={6A74437237797A6E675532426470615843566D4F57673D3D}

Modification type: update

Object type: user

Attribute information:

Changes	Attribute Name	Type	Old Value	New Value
none	accountEnabled	boolean	true	true
none	cloudAnchor	string	User_e72d0aa2-7410-4f6f-9510-6b88061a...	User_e72d0aa2-7410-4f6f-9510-6b88061a...
none	cloudMastered	boolean	false	false
modify	commonName	string	Ikram Berady	Ikram Nickel
none	countryCode	number	0	0
modify	displayName	string	Ikram Berady	Ikram Nickel
none	dnsDomainName	string	identityplus.ch	identityplus.ch
none	givenName	string	Ikram	Ikram
none	lastPasswordCha...	string	20160416184932.0Z	20160416184932.0Z
none	netBiosName	string	IDENTITYPLUS	IDENTITYPLUS
none	onPremisesSecurit...	binary	01 05 00 00 00 00 05 15 00 00 00 DE ...	01 05 00 00 00 00 05 15 00 00 00 DE ...
modify	onPremisesSamA...	string	ibe	ini
none	sourceAnchor	string	jtCr7yngU2BdpaXCvmOWg==	jtCr7yngU2BdpaXCvmOWg==
modify	sumame	string	Berady	Nickel
modify	userPrincipalName	string	ikram.berady@identityplus.ch	ikram.nickel@identityplus.ch

Preview... Log... Close Help


```
PS C:\Users\jochen.nickel> Connect-MsolService
PS C:\Users\jochen.nickel> Get-MsolAccountSku

AccountSkuId                ActiveUnits WarningUnits ConsumedUnits
-----
identityplus:AAD_PREMIUM    100         0             4
identityplus:RMSBASIC       1           0             0
identityplus:RIGHTSMANAGEMENT_ADHOC 50000       0             0
identityplus:ENTERPRISEPACK 25          0             2
identityplus:INTUNE_A       100         0             1
```

licensing azure ad premium

MEMBERS OWNERS PROPERTIES CONFIGURE SELF SERVICE ACTIVITY

NAME	USER NAME
Ikram Nickel	ikram.nickel@identityplus.ch
Jochen Nickel	jochen.nickel@identityplus.ch
Thomas Weyermann	thomas.weyermann@identityplus.ch


licensing office 365 e3 plan

MEMBERS OWNERS PROPERTIES CONFIGURE SELF SERVICE ACTIVITY

NAME	USER NAME
Ikram Nickel	ikram.nickel@identityplus.ch
Jochen Nickel	jochen.nickel@identityplus.ch
Thomas Weyermann	thomas.weyermann@identityplus.ch

applications groups approvals profile

You have 1 apps that can't be accessed until you install some software. [Install Now](#)



SageCRM ...

self-service social media applications

MEMBERS OWNERS PROPERTIES CONFIGURE SELF SERVICE ACTIVITY

NAME	USER NAME
Ikram Nickel	ikram.nickel@identityplus.ch
Jochen Nickel	jochen.nickel@identityplus.ch

Specify the publishing settings for this web application.

[Welcome](#)
[Preauthentication](#)
[Publishing Settings](#)
[Confirmation](#)
[Results](#)

Name:

 This name will appear in the list of published web applications.

External URL:

External certificate:
 [View...](#)

Backend server URL:

Welcome

Preauthentication

Relying Party

Publishing Settings

Confirmation

Results

Specify the publishing settings for this web application.

Name:

This name will appear in the list of published web applications.

External URL:

External certificate:

Backend server URL:

MY CLAIMSWEB Welcome! Sign out

[Home](#) [About](#)

WELCOME CLAIMSWEB!

Issued Identity	
Claim Type	Claim Value
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	2016-04-19T20:27:12.995Z

SAML Token	
Raw SAML Token	
Property	Value
SamSecurityToken.Id	2e0a3b7a-6427-4461-9e1d-f5092b50666
SamSecurityToken.ValidFrom	4/19/2016 8:27:14 PM
SamSecurityToken.ValidTo	4/19/2016 9:27:14 PM (60 minutes)
SamSecurityToken.Assertion.AssertionId	2e0a3b7a-6427-4461-9e1d-f5092b50666
SamSecurityToken.Assertion.Issuer	http://login.identityplus.ch/adfs/services/trust
SamSecurityToken.Assertion.IssueInstant	4/19/2016 8:27:14 PM
Intended Audience	https://claims.identityplus.ch/
SamSecurityToken.Assertion.MinorVersion	1
SamSecurityToken.Assertion.MajorVersion	1
Signature Algorithm	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
Signing Certificate	[Subject] CN=ADFS Signing - login.identityplus.ch
Download Certificate	[Issuer] CN=ADFS Signing - login.identityplus.ch
	[Serial Number] 6993FBB8473B65824EAF0D9171527CA1
	[Not Before] 4/16/2016 7:31:02 PM
	[Not After] 4/16/2017 7:31:02 PM
	[Thumbprint] E5D20F214C3DBA86165E0DFDA70FBE3E6F0BAF5

You can configure this rule to permit or deny users based on an incoming claim. Specify the incoming claim type, claim value, and whether the users should be permitted or denied access to the relying party.

Claim rule name:

Deny Domain Adminis Group

Rule template: Authorize Users Based on an Incoming Claim

Incoming claim type:

Group SID

Incoming claim value:

IDENTITYPLUS\Domain Admins

Browse...

Select one of the following options to indicate whether users with this claim will be permitted or denied access to the relying party.

- Permit access to users with this incoming claim
 Deny access to users with this incoming claim

An error occurred

You are not authorized to access this site. Click [here](#) to sign out and sign in again or contact your administrator for permissions.

[Error details](#)

Specify the publishing settings for this web application.

Name:

LOB kerb.identityplus.ch / Pre: ADFS no CLA MFA: No

This name will appear in the list of published web applications.

External URL:

https://kerb.identityplus.ch

External certificate:

*.identityplus.ch

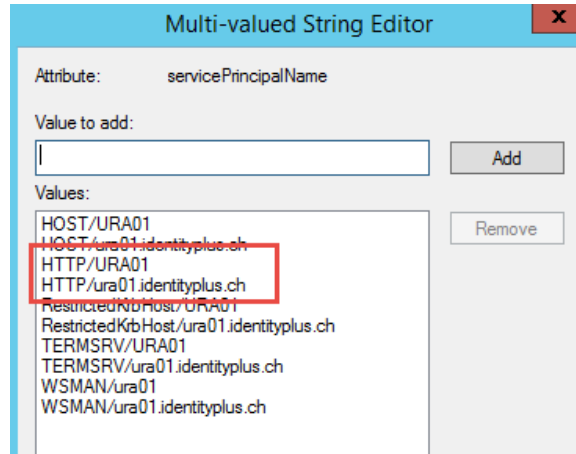
View...

Backend server URL:

https://kerb.identityplus.ch

Backend server SPN:

http/kerb.identityplus.ch



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 Name
http	kerb.identityplus.ch		

← → ↻ <https://kerb.identityplus.ch/?authToken=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzUz>

You successfully signed in with Kerberos

verification options [\(learn more\)](#)

Methods available to users:

- Call to phone
- Text message to phone
- Notification through mobile app
- Verification code from mobile app

remember multi-factor authentication [\(learn more\)](#)

- Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60):

multi-factor authentication

users [service settings](#)

Before you begin, take a look at the multi-factor auth deployment guide.

View: Any

<input type="checkbox"/>	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/>	Administrator	administrator@stansjpaas.ch	Disabled
<input type="checkbox"/>	Admin Assistant	Admin.Assistant@stansjpaas.ch	Disabled
<input checked="" type="checkbox"/>	Jochen Nickel	jochen.nickel@stansjpaas.ch	Disabled
<input type="checkbox"/>	On-premises Directory Synchronizer	sync_2020_01_01@stansjpaas.onmicrosoft.com	Disabled
<input type="checkbox"/>	Service Administrator	admin@stansjpaas.onmicrosoft.com	Disabled
<input type="checkbox"/>	Service User Admin		
<input type="checkbox"/>	Thomas Weisend		

Jochen Nickel
jochen.nickel@stansjpaas.ch

quick steps

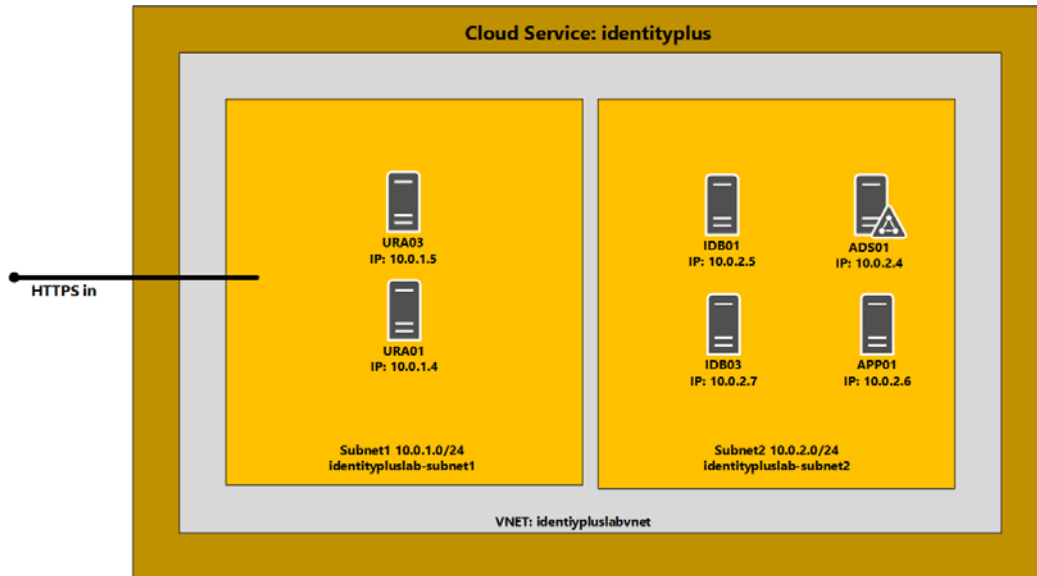
-
-

! About enabling multi-factor auth

Please read the [deployment guide](#) if you haven't already.

If your users are using desktop sign-in through the browser, you can send them to this link to register for multi-factor auth: <https://aka.ms/MFASetup>

Chapter 10: Implementing Access Control Mechanisms



ura03

DASHBOARD MONITOR ENDPOINTS CONFIGURE

NAME	PROTOCOL	PUBLIC PORT	PRIVATE PORT	LOAD-BALANCED SET NA...
PowerShell	TCP	49215	5986	-
Remote Desktop	TCP	60450	3389	-

ADD ENDPOINT

Add an endpoint to a virtual machine

Traffic coming to this endpoint will be sent to the virtual machine.

- ADD A STAND-ALONE ENDPOINT
- ADD AN ENDPOINT TO AN EXISTING LOAD-BALANCED SET ?

IdentityPlusWebFarm ▼

ADD ENDPOINT

Specify the details of the endpoint

NAME

HttpsIn ×

PROTOCOL

TCP ▼

PUBLIC PORT

443

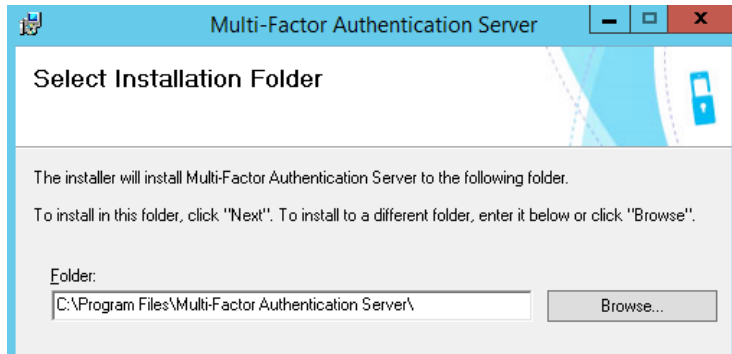
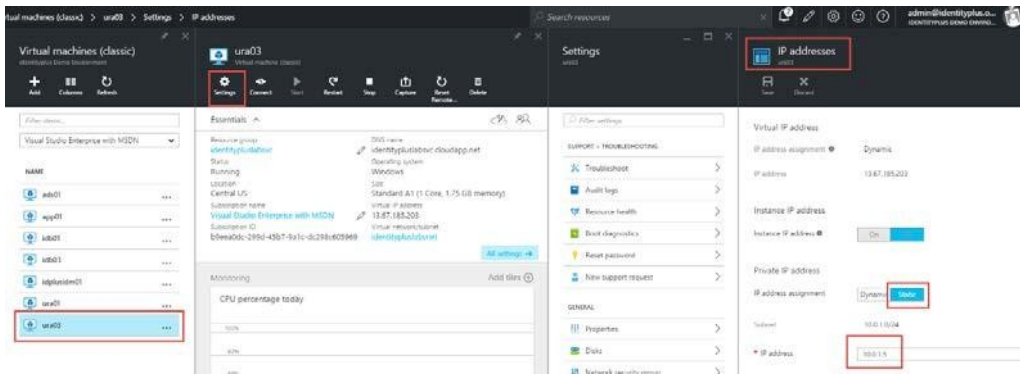
PRIVATE PORT

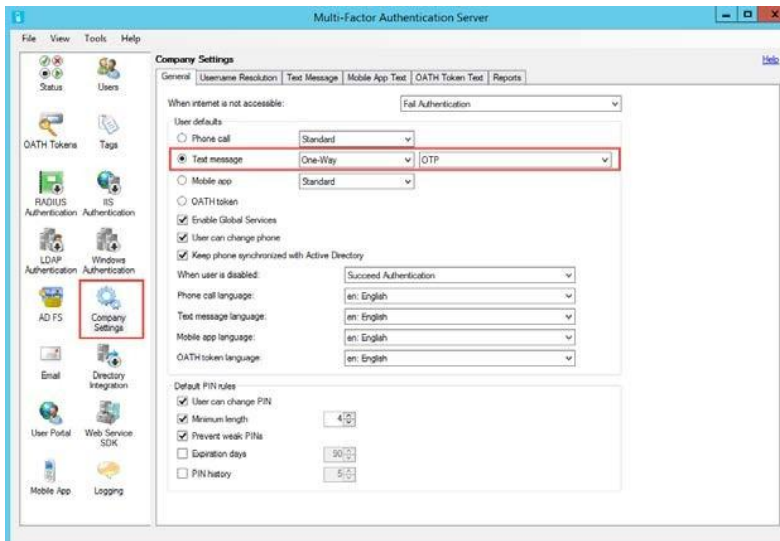
443

- RECONFIGURE THE LOAD-BALANCED SET ?

You can't reconfigure direct server return for existing load-balanced sets.

- ENABLE DIRECT SERVER RETURN ?





Import from Active Directory x

Domain: [Help](#)

List

View:

- identityplus.ch
 - [-] Computers
 - [-] Domain Controllers
 - [-] ForeignSecurityPrincipals
 - [-] Managed Business Objects**
 - [-] Managed Service Accounts
 - [-] Program Data
 - [-] System
 - [-] Users

Username	Name	Email Address	Mobile
anas.nickel@identityplus.ch	Nickel, Anas		
ikram.nickel@identityplus.ch	Nickel, Ikram		
jochen.nickel@identityplus.ch	Nickel, Jochen		
thomas.weyer mann@identityplus.ch	Weyermann, Thomas		

User filter:

Import: Display users 4

Display limit:

Settings | Method Defaults | Language Defaults

- Add new users
- Update existing users**
- Disable/Remove users no longer a member

Import phone:

Backup:

- Enabled
- Send email
- Assign new PIN to updated users

AD FS

Install AD FS Adapter...

- Allow user enrollment
 - Prompt for backup phone
 - Prompt for third-party OATH token
- Allow users to select method
 - Phone call
 - Text message
 - Mobile app
 - OATH Token
- Use security questions for fallback
 - Questions to answer:
- Use OATH token for fallback
- Enable logging

Edit Global Authentication Policy

Primary Multi-factor

Configure multi-factor authentication (MFA) settings.

Users/Groups
MFA is required for the following users and groups:

Devices
MFA is required for the following devices:

Unregistered devices
 Registered devices

Locations
MFA is required when accessing applications from the following locations:

Extranet
 Intranet

Select additional authentication methods. You must select at least one of the following methods to enable MFA:

Certificate Authentication
 Azure Multi-Factor Authentication Server

[What is multi-factor authentication?](#)

Active Directory Users and Computers

- Saved Queries
- identityplus.ch
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - LostAndFound
 - Managed Business Objects
 - Managed Service Accounts
 - Program Data
 - System
 - Users
 - NTDS Quotas
 - RegisteredDevices
 - TPM Devices

Name	Type	Description
2be037ff-6f04-4e97-8eed-14aba5c8b865	msDS-Device	

2be037ff-6f04-4e97-8eed-14aba5c8b865 Prop...

General | Object | Security | Attribute Editor

Attributes:

Attribute	Value
msDS-DeviceObjectVersion	1
msDS-DeviceOSType	Windows
msDS-DeviceOSVersion	6.3.9600.0
msDS-IsEnabled	TRUE
msDS-IsManaged	FALSE
msDS-RegisteredOwner	S-1-5-21-3303717086-1394
msDS-RegisteredUsers	S-1-5-21-3303717086-1394
name	2be037ff-6f04-4e97-8eed-14aba5c8b865
objectCategory	CN=ms-DS-Device,CN=Schema
objectClass	top; msDS-Device
objectGUID	f532c9b0-06ba-43cb-9613-41197
replPropertyMetaData	AttID Ver Loc USN
showInAdvancedViewOnly	TRUE
uSNChanged	41197

OK Cancel Apply Help

Edit Authentication Policy for Claims Demo Web Site

Primary | Multi-factor

Configure multi-factor authentication (MFA) settings.

Global multi-factor authentication settings will apply to this relying party trust.

Users/Groups

MFA is required for the following users and groups:

Add... Remove

Devices

MFA is required for the following devices:

- Unregistered devices
- Registered devices

Locations

MFA is required when accessing applications from the following locations:

- Extranet
- Intranet

What is multi-factor authentication?

OK Cancel Apply

```
Administrator: Windows PowerShell
PS C:\> get-adsproperties | select *extranet* | fl

ExtranetLockoutThreshold : 2147483647
ExtranetLockoutEnabled   : False
ExtranetObservationWindow : 00:30:00
```

IDplus Login

Update Password

IDplus Login

Sign in with your organizational account

[Change password](#)
[Reset password](#)

identityplus demo environment

TEMPLATES



Get started with Rights Management!

Here are a few options to get you started

Skip Quick Start the next time I visit

Rights Management Service Status

Active



Manage

Create a new rights policy template
Manage your rights policy templates



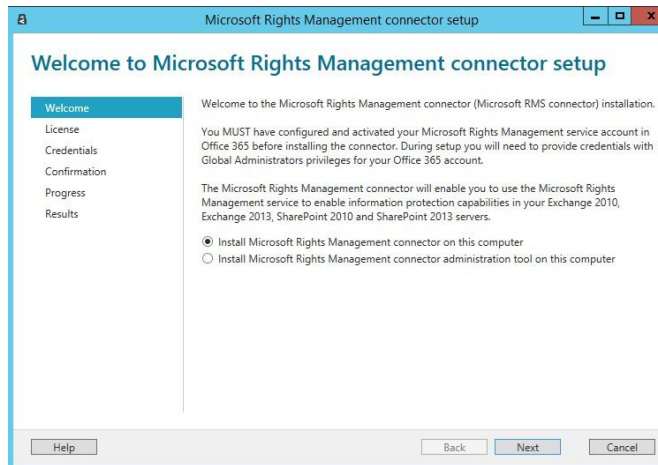
Usage Logging is enabled

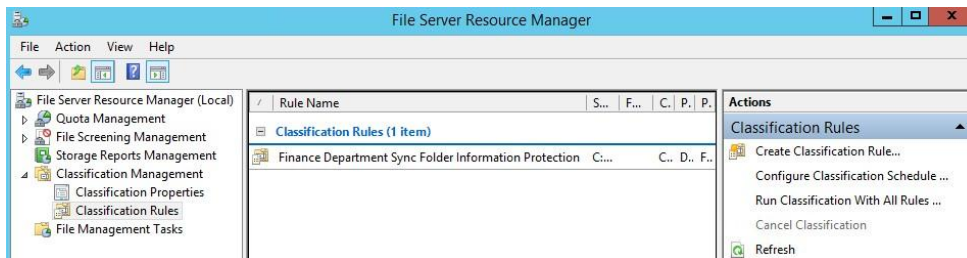
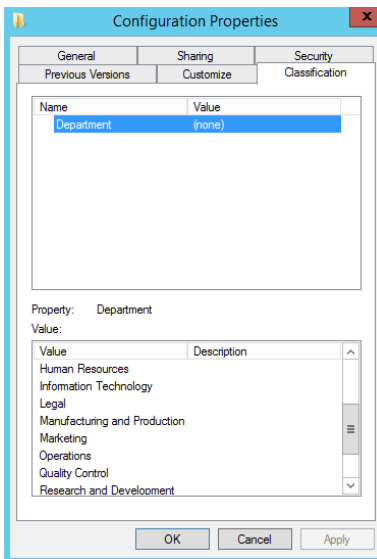
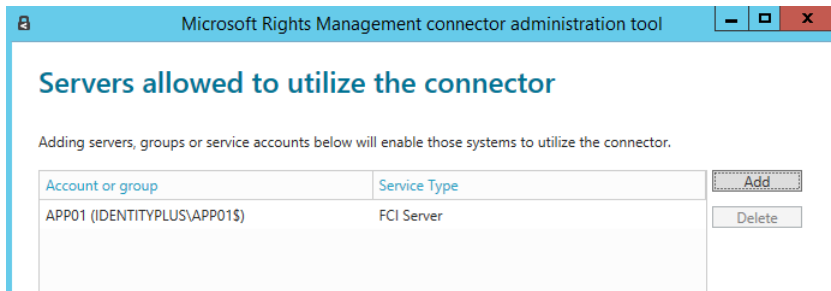
Logging and Analyzing Azure Rights Management Usage

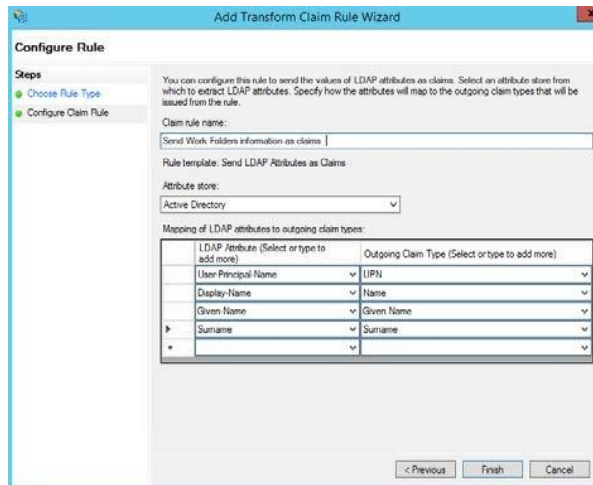
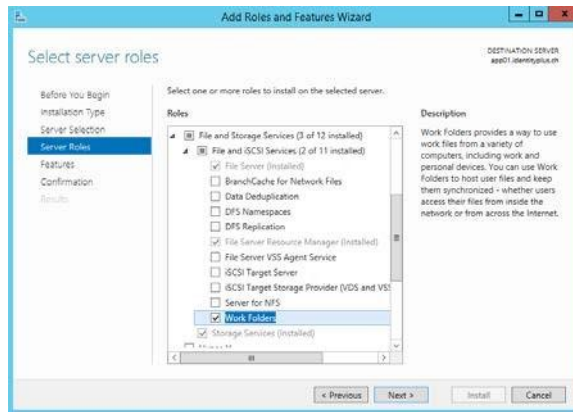


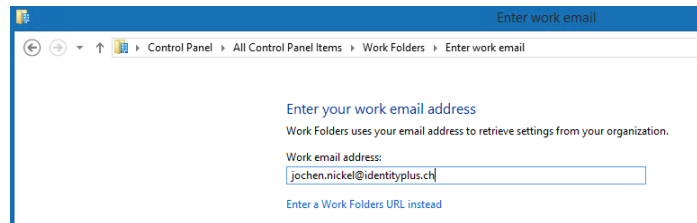
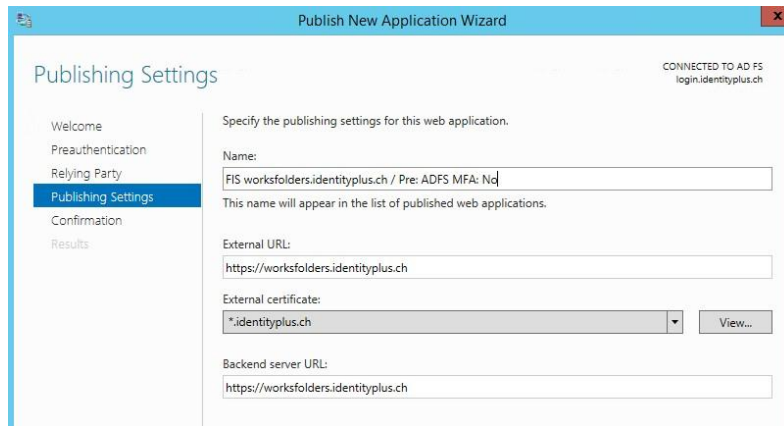
Learn more

Configuring Custom Templates for Rights Management
Microsoft Azure Rights Management









Security policies

To help protect your work files, your organization can make the following changes to your PC at any time:

- Encrypt Work Folders
- Require a password to sign in to your PC, and automatically lock your screen
- Erase all files in Work Folders, for example if you lose this PC

Additionally, files stored in Work Folders are subject to your organization's data policies.

I accept these policies on my PC

his PC > Work Folders

Name	Date modified	Type	Size
Financial Report	24.04.2016 23:01	Microsoft Word D...	183 KB

The screenshot shows the File Server Resource Manager console with a classification rule selected. A red arrow points from the rule name in the console to the 'File Server Resource Manager Options' dialog box. The dialog box has several tabs: 'Email Notifications', 'Notification Limits', 'Storage Reports', 'Report Locations', 'File Screen Audit', 'Automatic Classification', and 'Access-Derived Assistance'. The 'Automatic Classification' tab is active. Under the 'Schedule' section, 'Enable fixed schedule' is checked. The 'Run at' time is set to 9:24:32 PM. The 'Weekly' radio button is selected, and 'Sunday' is checked. The 'Limit (in hours)' is set to 1. Under the 'Allow continuous classification for new files' section, this option is checked, and 'Enable logging' is also checked with a maximum log size of 1024 KB. The 'Generate log' section has 'Log file' and 'Error log' checked. The 'Generate report' section has 'Generate a report' checked, with 'DHTML' selected as the report format. The 'Send reports to the following administrators' field contains '[Admin Email]'. The 'Reports will be saved in' field contains 'C:\StorageReports\Scheduled'. The dialog box has 'OK' and 'Cancel' buttons at the bottom.

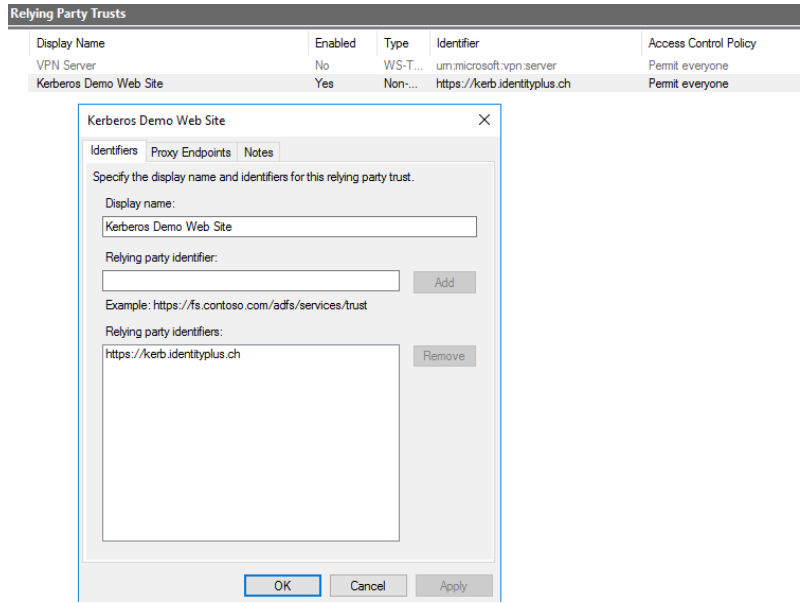
Edit Authentication Methods

The screenshot shows the 'Edit Authentication Methods' dialog box with the 'Multi-factor' tab selected. The dialog box contains the text: 'Select additional authentication methods. You must select at least one of the following methods to enable MFA:'. Below this text is a list of authentication methods with checkboxes: 'Certificate Authentication' (unchecked) and 'Azure MFA' (checked). At the bottom of the dialog box, there is a link that says 'What is multi-factor authentication?'.

The screenshot shows the AD FS console interface. On the left is a navigation tree with the following items: AD FS, Service, Attribute Stores, Authentication Methods, Certificate Authority, Certificates, Claim Descriptions, Device Registration (highlighted), Endpoints, Scope Descriptions, Web Application Proxy, Access Control Policies, Relying Party Trusts, Claims Provider Trusts, and Application Groups. The main pane is titled "Device Registration Overview" and contains the following text: "Allow users to register devices with Active Directory." Below this is a "Status" section with a yellow bar and the text: "The Active Directory forest is configured for device registration with this AD FS farm. Enable device authentication to provide conditional access based on device claims." A link "Enable device authentication" is provided. Underneath is a "Learn More" section with links for "Planning for Device Registration", "Configure a federation server with Device Registration", "Configuring Device Registration", and "AD FS Help".

The "Edit Authentication Methods" dialog box has two tabs: "Primary" and "Multi-factor". The "Multi-factor" tab is selected. The text inside reads: "Select authentication methods. By selecting more than one authentication method, you enable users to have a choice of what method to authenticate with at sign in. If Integrated Windows authentication method is specified, it appears as the default authentication method on browsers that support Integrated Windows authentication. Learn more about Azure MFA (Multi-Factor Authentication)." Below this is an "Extranet" section with a list of authentication methods: "Forms Authentication" (checked), "Certificate Authentication" (unchecked), "Device Authentication" (checked), and "Azure MFA" (unchecked).

The "Properties for Device Registration Service" dialog box has a "Properties" tab. It contains the following settings: "Maximum number of joined devices per user:" with a spinner box set to "10"; a checked checkbox for "Automatically remove unused devices"; and "Number of days before an unused device is removed:" with a spinner box set to "90".



Rule Editor

✕

Permit

everyone

users

- from specific network
- from specific group
- from devices with specific trust level
- with specific claims in the request
- and require multi-factor authentication

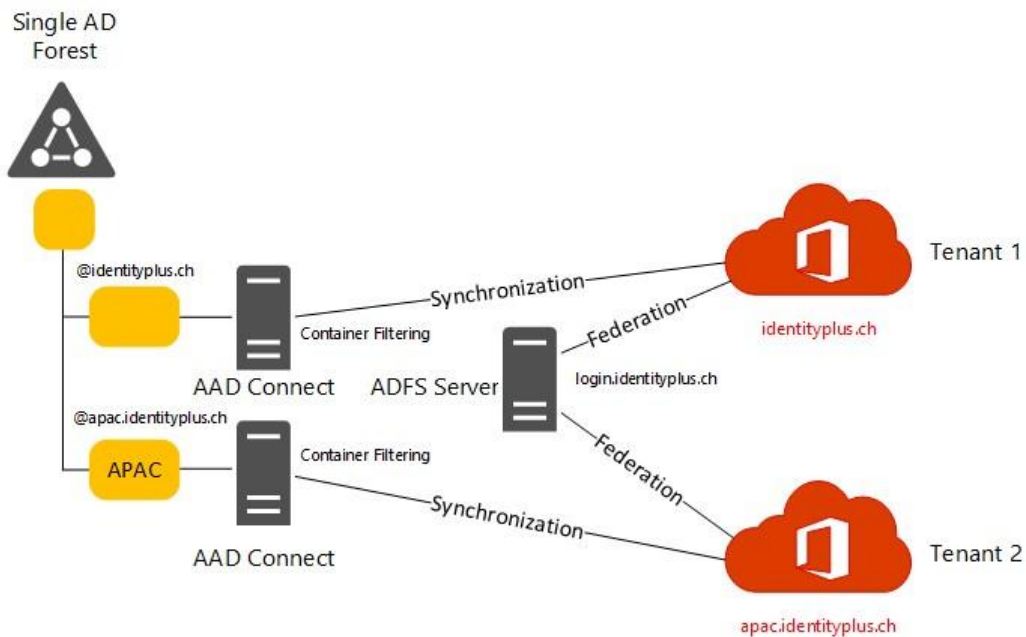
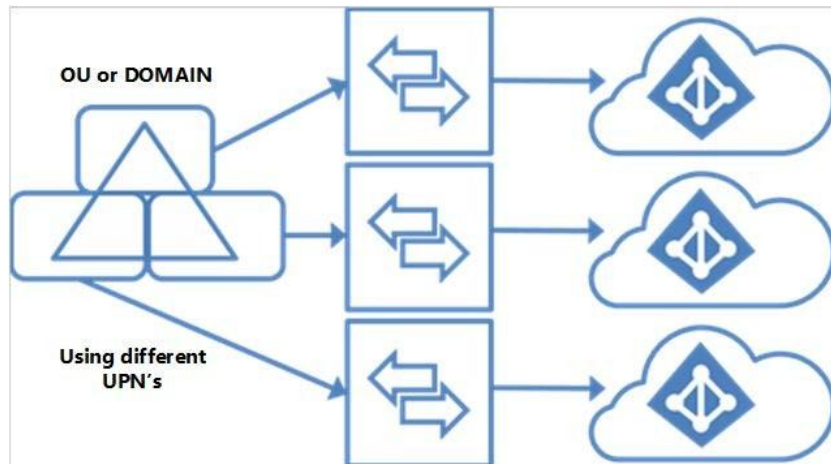
Except

- from specific network
- from specific groups
- from devices with specific trust level
- with specific claims in the request

Permit users
from [IDENTITYPLUS\Sales_Applications](#) group
and require multi-factor authentication
except
from [84.75.23.101](#) network
and from devices with [authenticated](#) trust lev

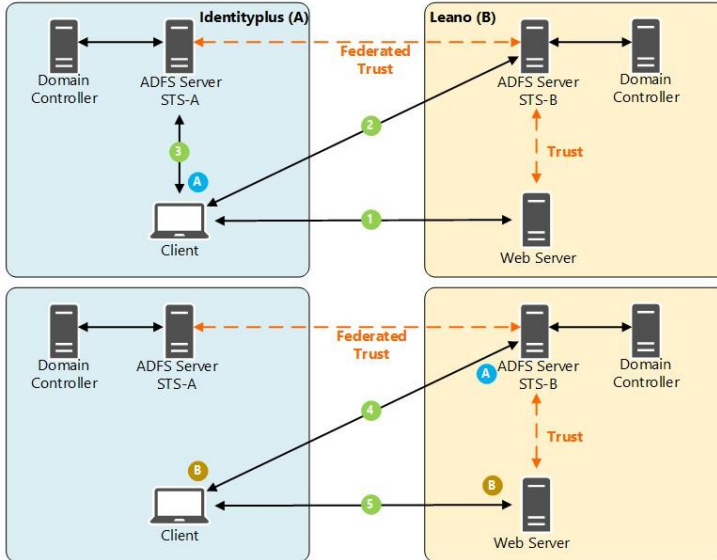
OK Cancel

Chapter 11: Managing Transition Scenarios with Special Scenarios



Business-to-Business (B2B) scenario

User from Identityplus (A) accessing claims-aware applications on Leano (B)



Traffic Flow

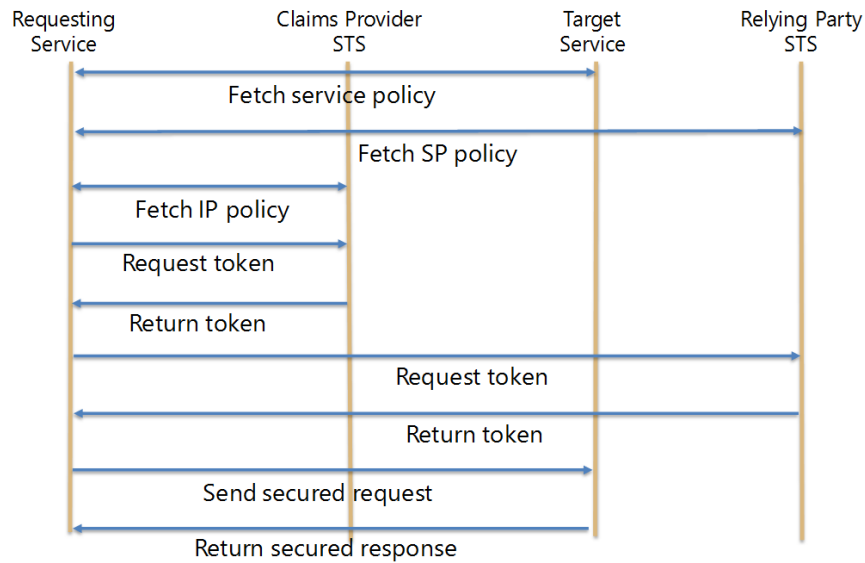
1. Client requests the application page and receives a redirect to STS-B
2. Home Realm Discovery is working and the client receives a redirect to STS-A
3. Client authenticates to STS-A and receives a token
4. Client presents token A to STS-B and receives a token B
5. Client presents token B to the application and get access to application

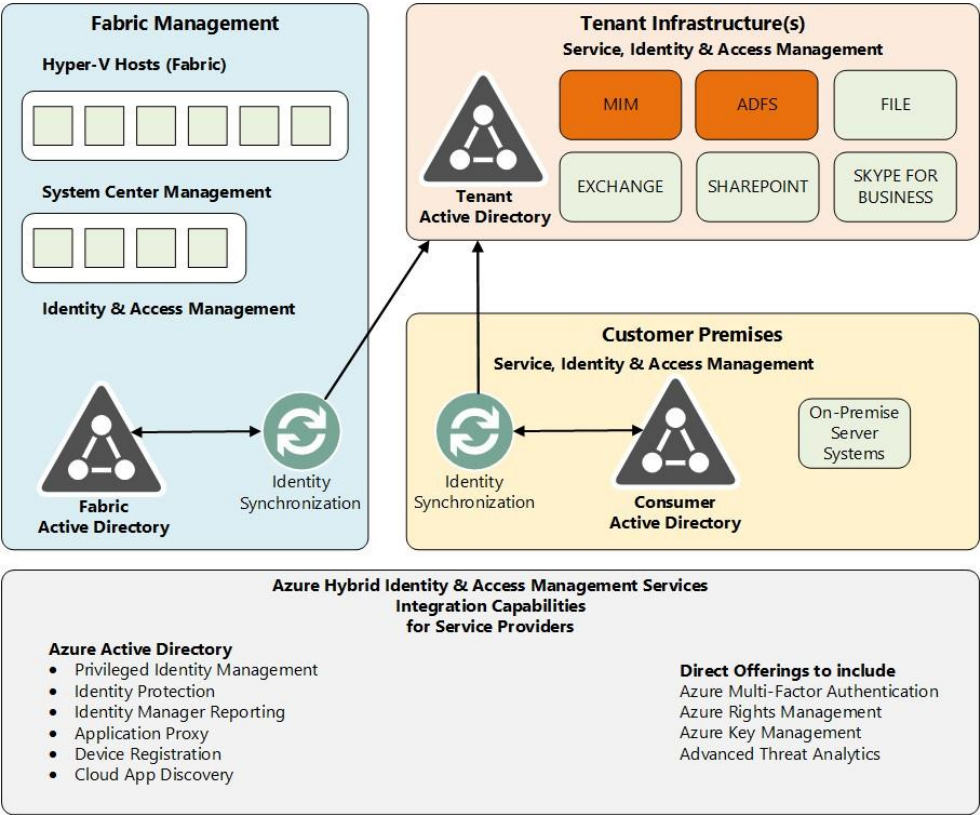
Federated Trusts

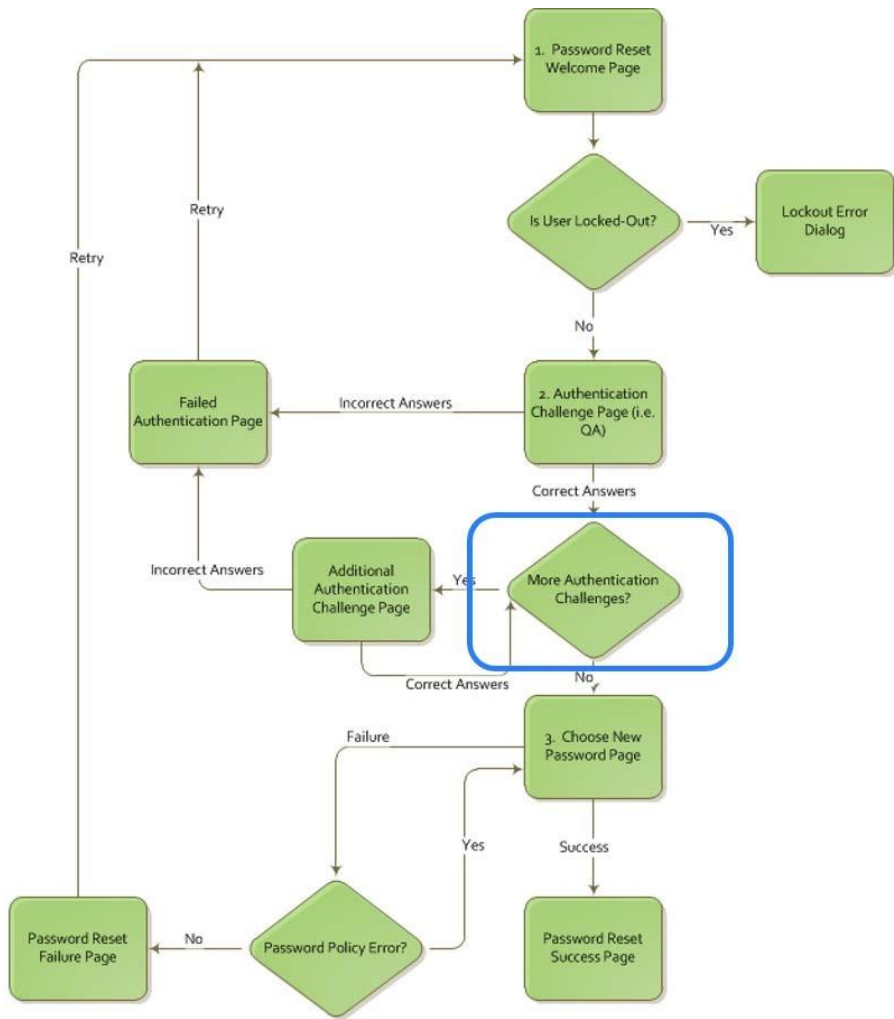
AD FS exposes STS information via Federation Metadata

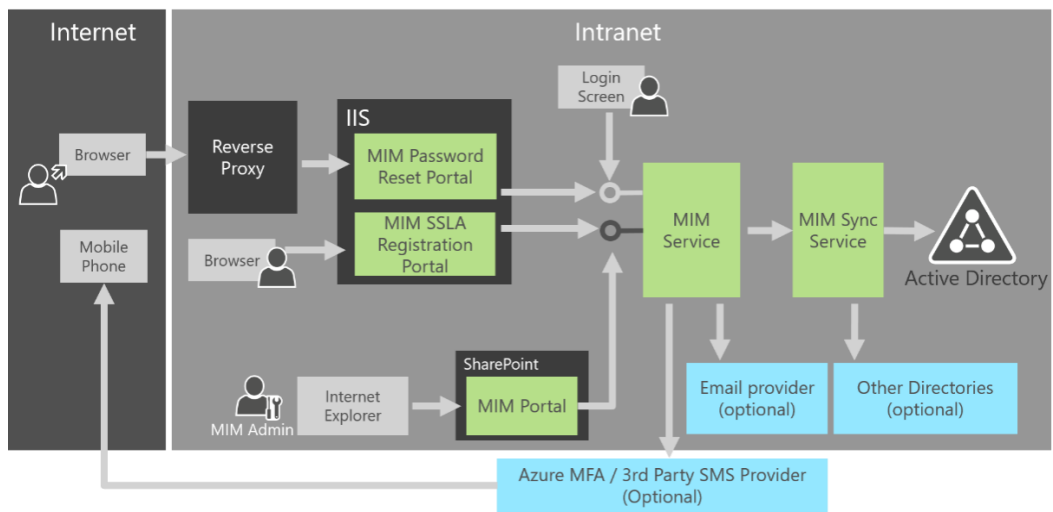
Input data about the claims provider published online or on a local network. Use this option to input the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL): (http://login.name.cz)
Example: https://adfsfabrikam.com or https://fs.fabrikam.com/

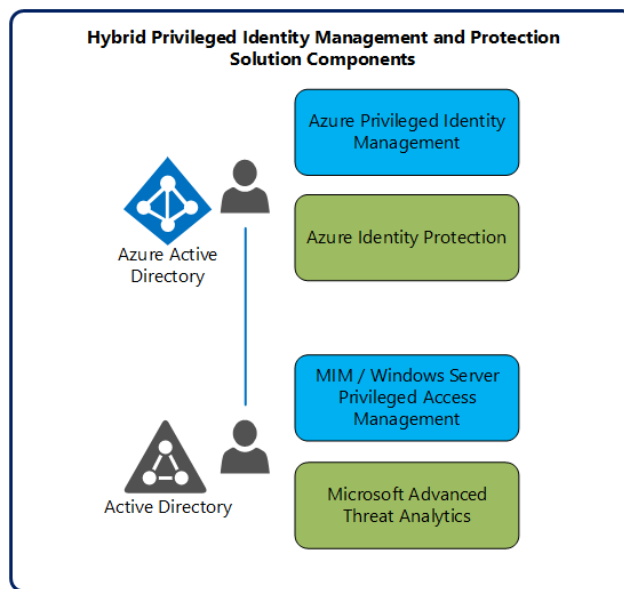


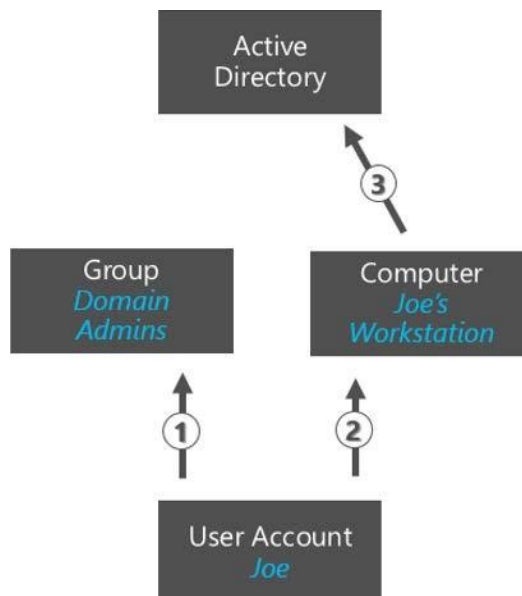
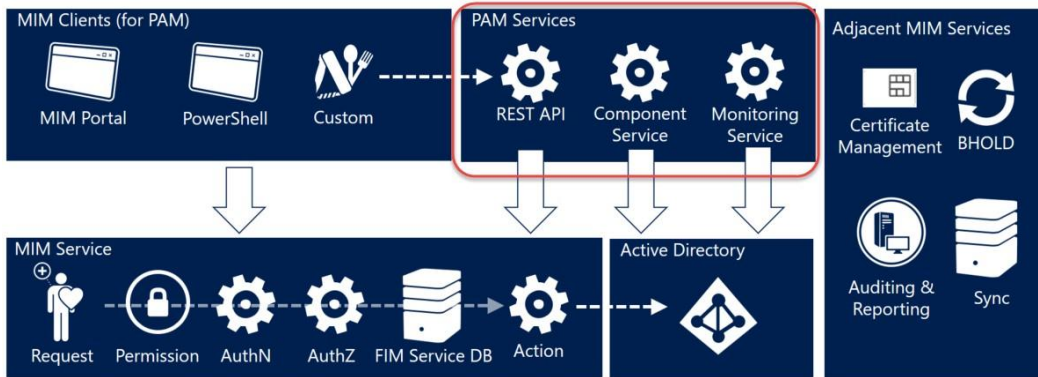
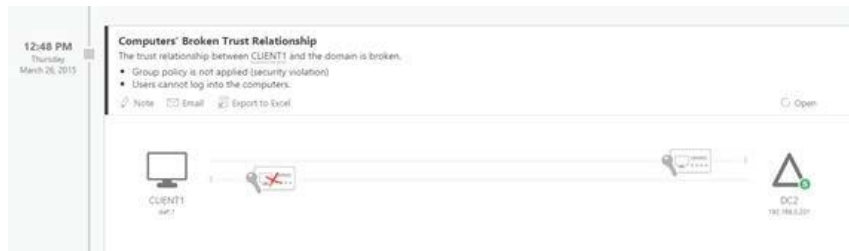


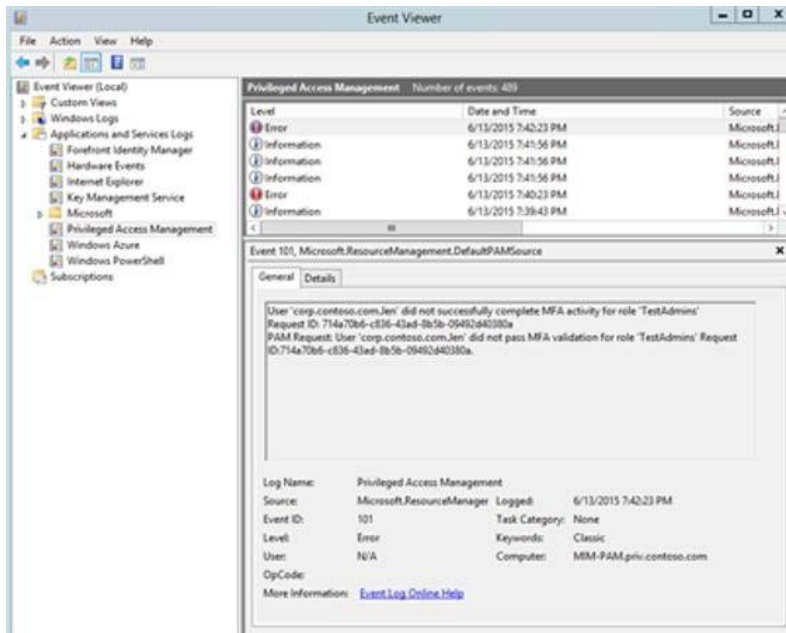
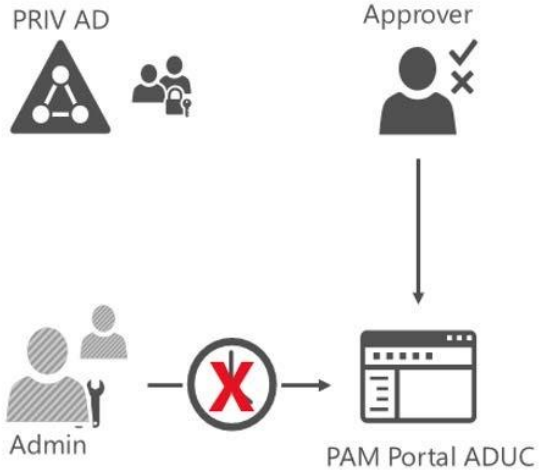


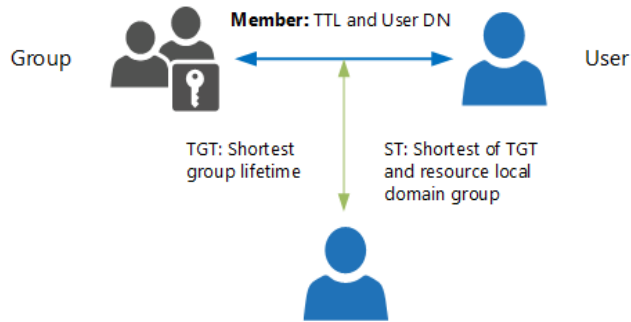
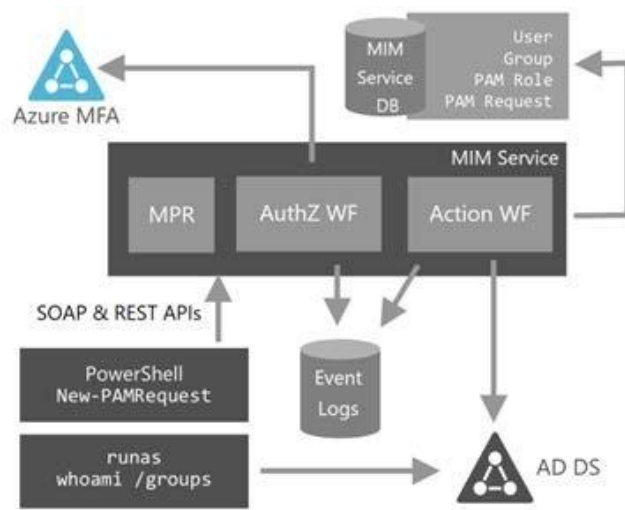


Chapter 12: Advanced Considerations for Complex Scenarios









Azure AD Identity Protection

Last 7 days Settings

Essentials

User risk policy **Not enabled** | Sign-in risk policy **Enabled** | [All settings](#)

Users flagged for risk
0% OF 10 USERS

0

No users detected for the selected date range.

0 SECURED

Risk events

No risk events detected for the selected date range.

0 HIGH | 0 MEDIUM | 0 LOW | 0 CLOSED

Vulnerabilities 2

RISK LEVEL	COUNT	VULNERABILITY
Unknown		Users without multi-factor authentication registration
Medium	21	Roles don't require multi-factor authentication for activation

Settings
AZURE AD IDENTITY PROTECTION

Filter settings

GENERAL

Getting started

CONFIGURE

Notifications

MULTI-FACTOR AUTHENTICATION

Registration

SECURITY POLICIES

User risk

Sign-in risk policy

Sign-in risk
SETTINGS

Save Discard

Description

Set a policy to mitigate sign-in risk. Require multi-factor authentication challenges or block sign-ins based on risk level. [Learn more](#)

Set scope

Select users and groups

Included: All users

Excluded: 0 users, 0 groups

Set controls

Set risk level for multi-factor authentication: Never | Low | Medium | **High**

Set risk level for blocking sign-in: Never | Low | Medium | High

Enable policy: **On** | Off

Review impact

0 CHALLENGED OF 0 | 0 BLOCKED OF 0

MULTI-FACTOR AUTHENTICATION

 **Registration** >

SECURITY POLICIES

 **User risk** >

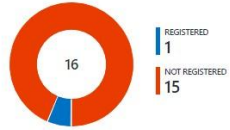
 **Sign-in risk policy** >

Description

Multi-factor authentication helps us protect your accounts. Require users to register for Azure Multi-Factor Authentication by configuring this rule.

[Learn more](#)

Registration status



Set scope

Included
0 users, 1 group >

Excluded
0 users, 0 groups >

Set controls

Number of allowed skip days ●

10

Enable policy ●

On Off

All users On Off

HR

Accounting

CONFIGURE

Notifications >

MULTI-FACTOR AUTHENTICATION

Registration >

SECURITY POLICIES

User risk >

Sign-in risk policy >

Set scope

Select users and groups

Included
All users >

Excluded
0 users, 0 groups >

Set controls

Set risk level for password change ●

Never Low Medium High

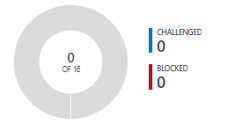
Set risk level for blocking sign-in ●

Never Low Medium High

Enable policy

On Off

Review impact



15 user(s) are not registered for multi-factor authentication. Click here to check your registration policy.

- CONFIGURE
- ☑ Notifications >
- MULTI-FACTOR AUTHENTICATION
- 🟢 Registration >
- SECURITY POLICIES
- 👤 User risk >
- 🔑 Sign-in risk policy >

Set scope

Select users and groups

Included
All users >

Excluded
0 users, 0 groups >

Set controls

Set risk level for multi-factor authentication ●

Never Low **Medium** High

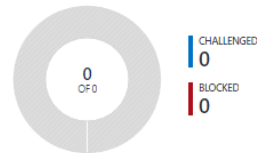
Set risk level for blocking sign-in ●

Never Low Medium **High**

Enable policy

On **Off**

Review impact



⚠️ 15 user(s) are not registered for multi-factor authentication. Click here to check your registration policy.

Protect your organization
identityplus Demo Environment - PREVIEW

- 1** Discover privileged roles >
- 2** Reduce risks to your directory >
- 3** Review the changes to your users in privileged roles >

Discover privileged roles
identityplus Demo Environment - PREVIEW

Review this list of privileged roles that exist in your directory. Select each role to see permanent or eligible users in roles.
[Learn more about privileged roles.](#)

ROLES

PERMANENT

Global Administrator	3 >
----------------------	-----

Global Administrator
PREVIEW

PERMANENT

- Tenant Administrator**
admin@identityplus.onmicroso...
- Tenant Co-Administrator MSD...**
azidadm@outlook.com
- Tenant Co-Administrator MSD...**
jochen.nickel@outlook.com

Role summary Add tiles +

Roles				
ROLE NAME	MFA ENABLED	USERS	ACTIVE	ELIGIBLE
Global Administrator	Yes	3	3 (100%)	0 (0%)
Privileged Role Administra...	Yes	1	1 (100%)	0 (0%)
Security Administrator	Yes	1	1 (100%)	0 (0%)

Office 365 Admin Role	Role In Exchange Online	Role In SharePoint Online	Role In Skype For Business
global admin	<ul style="list-style-type: none"> ▪ Exchange Online admin ▪ Company admin 	SharePoint Online admin	Skype for Business admin
billing administrator	N/A	N/A	N/A
password administrator	Help Desk admin	N/A	Skype for Business Online admin
service administrator	N/A	N/A	N/A
user management administrator	N/A	N/A	Skype for Business Online admin
Exchange administrator	Exchange Online admin	N/A	N/A
SharePoint administrator	N/A	SharePoint Online admin	N/A
Skype for Business administrator	N/A	N/A	Skype for Business Online admin

Privileged Roles >

Alerts Settings >

- Default for all roles
- AdHoc License Administrator
- Billing Administrator
- Compliance Administrator
- Directory Readers
- Directory Writers
- Email Verified User Creator
- Exchange Administrator
- Global Administrator
- Mailbox Administrator
- Partner Tier1 Support
- Partner Tier2 Support
- Password Administrator
- Privileged Role Administrator

Activations

Maximum Activation duration (hours)

Notifications

Send email notifying admins of activation

Incident/Request Ticket

Require Incident/Request ticket number during activation

Multi-Factor Authentication

Require Azure Multi-Factor Authentication for activation

Activity Add tiles

Alerts

0

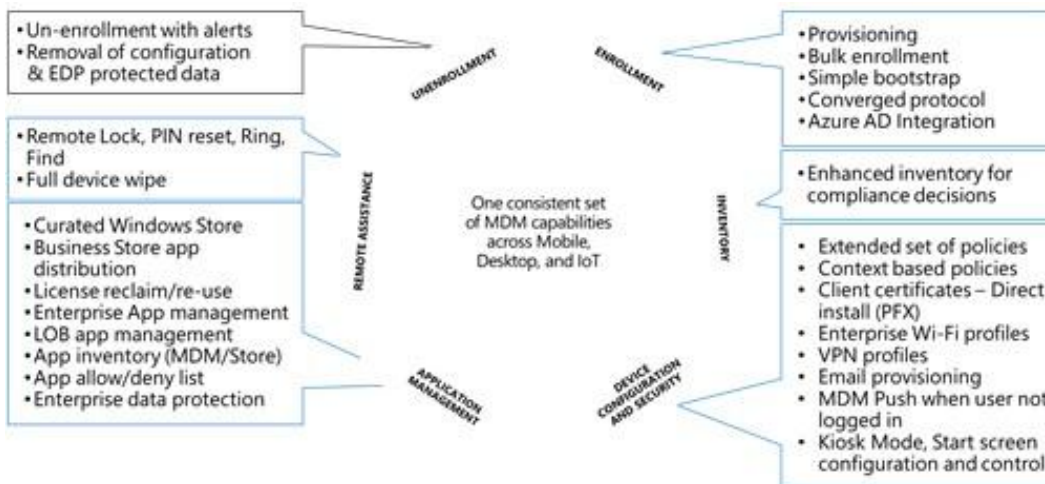
No alerts were found

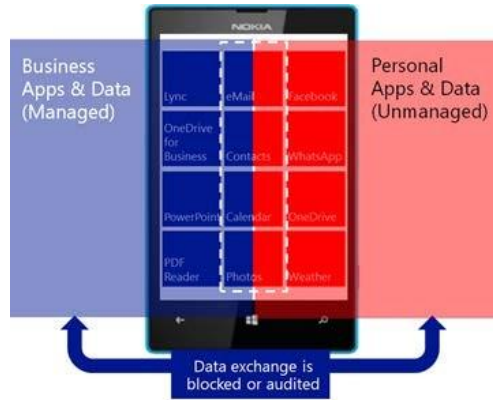
Users in admin roles

3 Users

Audit history

Quick start





Microsoft Identity Manager

Home

Welcome J2AM\jmadm to the Microsoft Forefront Identity Manager 2010 - Certificate Management Portal (274) CH. FIM CH enables you to manage certificates and smart cards.

Use this page to perform tasks related to certificate deployment, certificate management, and reporting. The most commonly used tasks are located in the first section, entitled "Common Tasks." You can point your mouse over any link to find out more information about what each link entails.

Requests

Use this section to perform actions on users, such as enroll, review, receive, or view requests that need approval or completion. You will have to search on the user in order to perform an action on that user.

- Enroll a user for a new set of certificates or a smart card
- View requests that need approvals
- View requests that need completion

Manage Users And Certificates

Use this section to perform actions on a user or on a certificate. You will have to search on the user (or certificate) in order to perform an action on that user or certificate.

- Find a user to view or manage their information
- Find a certificate
- Find a certificate expiration list

Manage their Smart Cards

Use this section to manage a user's smart cards. You can view details of a smart card and perform actions on the smart card, such as unblock.

- Unblock a user's smart card
- Find a smart card
- View details of the smart card currently in the reader

Requests

Use this section to manage requests. You can cancel a request you initiated that is in the pending state, distribute one-time passwords for a request that is approved, and view request information.

- Find a request
- Browse completed requests
- Distribute one-time passwords for a request

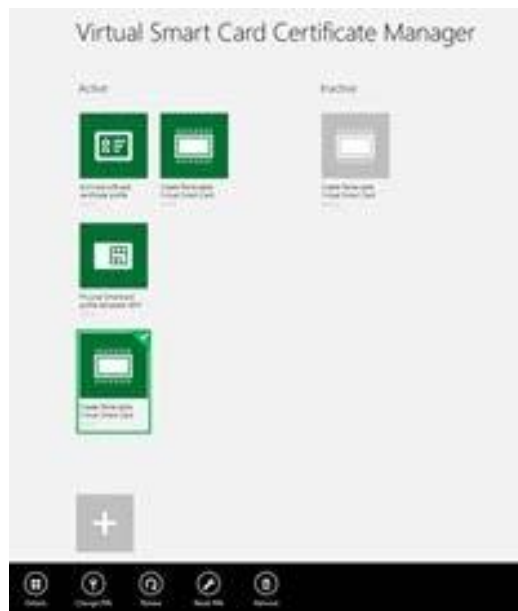
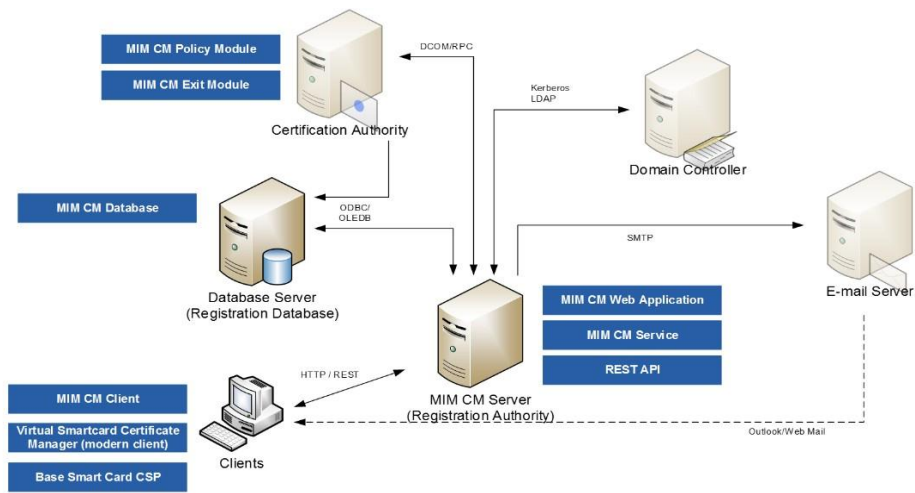
Administration

Use this section to manage profile templates.

- Manage profile templates

Reports

Use this section to produce reports that describe requests, certificates, profiles, or smart cards. Click on the report and then read the necessary criteria to produce the results.



Chapter 13: Delivering Multi-Forest Hybrid Architectures

Chapter 14: Installing and Configuring the Enhanced Identity Infrastructure

Chapter 15: Installing and Configuring Information Protection Features

```
Administrator: Windows PowerShell
PS C:\Windows\system32> Add-AadrmRoleBasedAdministrator -EmailAddress jochen.nickel@idam.ch
jochen.nickel@idam.ch was added to the list of administrators for the Rights Management service.
PS C:\Windows\system32> Get-AadrmRoleBasedAdministrator

ObjectId                DisplayName      EmailAddress                                     Role
-----
5e4583c3-9571-4651-a59b-25b0d5e24a47 Jochen Nickel  smtp:jochen.nicke15265@idamcloud.onmicrosoft.com GlobalAdministrator
```

Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> Get-AadrmRoleBasedAdministrator | fl

ObjectId                : 5e4583c3-9571-4651-a59b-25b0d5e24a47
DisplayName              : Jochen Nickel
EmailAddress              : smtp:jochen.nicke15265@idamcloud.onmicrosoft.com
Role                     : GlobalAdministrator
```

Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> Get-AadrmSuperUser
Aadrm_S-1-5-21-3123384963-3601710319-2843089171-1118@b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com
PS C:\WINDOWS\system32>
```

```

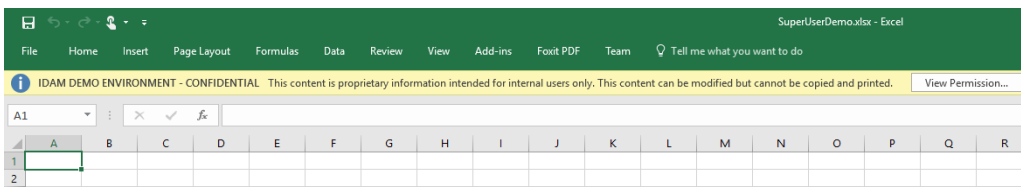
2018-09-27T12:39:16 admin@idamcloud.onmicrosoft.com GetTemplateByid -templateid d9f5b841-9861-4616-8fcr-1559ae09a56 Passed Begin TemplatePrope
TemplateID = d9f5b841-9861-4616-8fcr-1559ae09a56
Names:
1033 -> idam Demo Environment - Human Resources Confidential
Description:
1033 -> idam Demo Environment - Human Resources Confidential
Status = Published
RightsDefinitions:
HumanResource@idam.ch -> VIEW, EXTRACT, REPLY, REPLYALL, PRINT, OSMODEL
ContentExpirationDate = 1/1/2001 12:00:00 AM
ContentValidityDuration = 0
ContentExpirationOption = Never
LicenseValidityDuration = 7
ReadOnly = False
LastModifiedTimeStamp = 6/23/2015 2:39:00 PM
ScopeIdentities:
EnableLegacyApps = False
End TemplateProperties

```

```

PS C:\Users\jochen.nicke\Desktop> Protect-RMSFile -TemplateID 61d62ec9-fe90-40d7-ae18-8617b7e8585c -file ".\SuperUserDemo.xlsx"
InputFile                               EncryptedFile
-----
C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx
PS C:\Users\jochen.nicke\Desktop>

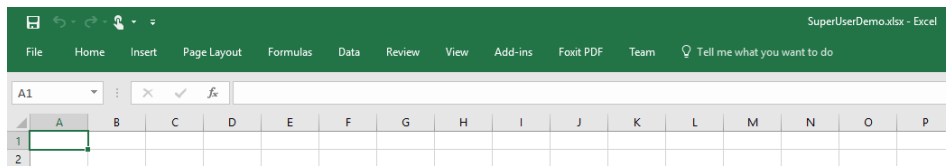
```



```

PS C:\Users\jochen.nicke\Desktop> Unprotect-RMSFile -File ".\SuperUserDemo.xlsx"
InputFile                               DecryptedFile
-----
C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx
PS C:\Users\jochen.nicke\Desktop>

```



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Get-IRMConfiguration

InternalLicensingEnabled : True
ExternalLicensingEnabled : True
JournalReportDecryptionEnabled : True
ClientAccessServerEnabled : True
SearchEnabled : True
TransportDecryptionSetting : Optional
EDiscoverySuperUserEnabled : True
RMSOnlineKeySharingLocation : https://sp-rms.eu.aadrm.com/TenantManagement/ServicePartner.svc
RMSOnlineVersion :
ServiceLocation : https://b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com/_wmcs/certification
PublishingLocation : https://b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com/_wmcs/licensing/publish.asmx
LicensingLocation : {https://b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com/_wmcs/licensing}
```

Applications

Search applications

+ Add app

- Claims Demo Website
- Office 365 Exchange O...
- Office 365 SharePoint...
- Groups

...

- Save draft
- Show From: internal users only. This content can be modified but cannot
- Check names
- Set importance >
- Set permissions >
 - No restrictions
 - Do Not Forward
 - idam Demo Environment - Confidential**
 - idam Demo Environment - Confidential View Only
- Switch to plain text
- Show message options...

Bcc

new rule

Name:
Project Identity and Access Management Private Preview

*Apply this rule if...
The subject or body includes... ['Azure Information Protection'](#)
add condition

*Do the following...
Apply rights protection to the message with... [idam Demo Environment - Confidential View Only](#)
add action

Microsoft Rights Management connector administration tool

Microsoft RMS administrator credentials

In order to administer the Microsoft Rights Management connector configuration, you need to provide administrative credentials for your Microsoft Rights Management service tenant. Enter your Microsoft Rights Management service administrator credentials.

User name: admin@idamcloud.onmicrosoft.com
Password:

[Microsoft RMS administrator credentials](#)

Microsoft Rights Management connector administration tool

Servers allowed to utilize the connector

Adding servers, groups or service accounts below will enable those systems to utilize the connector.

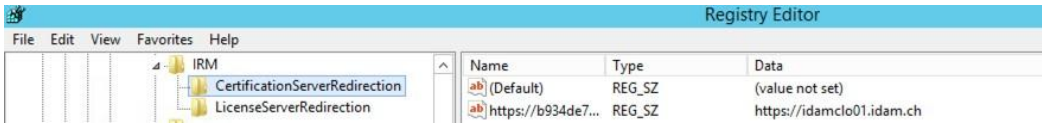
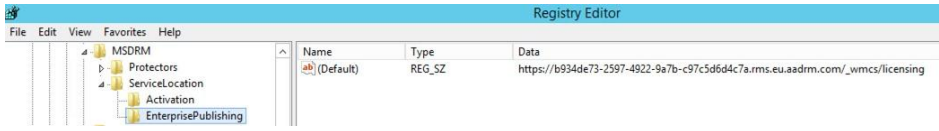
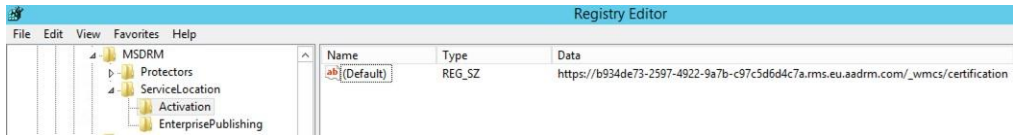
Account or group	Service Type	Add
IDAM\IDAMFIS01\$	FCI Server	Delete
IDAM\IDAMFIS02\$	FCI Server	
IDAM\IDAMEXS01\$	Exchange Server	
IDAM\IDAMSPS01\$	SharePoint Server	

```

Administrator Windows PowerShell
PS C:\Windows\system32> Get-AadrmConfiguration

BPOSId : 153463a9-a394-4bf7-b748-191d6fbf0701
RightsManagementServiceId : 16934de73-2597-4922-9a7b-c97c5d6d4c7a
LicensingIntranetDistributionPointUrl : https://b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com/_wmcs/licensing
LicensingExtranetDistributionPointUrl : https://b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com/_wmcs/licensing
CertificationIntranetDistributionPointUrl : https://b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com/_wmcs/certification
CertificationExtranetDistributionPointUrl : https://b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com/_wmcs/certification
AdminConnectionUrl : https://admin.eu.aadrm.com/admin/admin.svc/Tenants/b934de73-2597-4922-9a7b-c97c5d6d4c7a
AdminV2ConnectionUrl : https://admin.eu.aadrm.com/adminv2/admin.svc/Tenants/b934de73-2597-4922-9a7b-c97c5d6d4c7a
OnPremiseDomainName :
Keys : {2c9b80bb-d122-46e1-a428-2f2bea4ad8ce}
CurrentLicensorCertificateGuid : 2c9b80bb-d122-46e1-a428-2f2bea4ad8ce
Templates : {61d62ec9-fe90-40d7-ae18-8617b7e8585e, a8d26137-2677-4a90-85bf-2ed910350653, d9f53841-9861-4646-8fcf-1559ae049a56, fc7173b1-1109-4ecf-8400-8f24600b9a27}
FunctionalState : Enabled
SuperUsersEnabled : Enabled
SuperUsers : {Aadrm_S-1-5-21-3123384963-3601710319-2843089171-1118@b934de73-2597-4922-9a7b-c97c5d6d4c7a.rms.eu.aadrm.com}
AdminRoleMembers : {Global Administrator -> 5e4583c3-9571-4651-a59b-25b0d5e24a47}
KeyRollOverCount : 0
ProvisioningDate : 20.10.2014 22:33:13
IPCy3ServiceFunctionalState : Enabled
DevicePlatformState : {Windows -> True, WindowsStore -> True, WindowsPhone -> True, Mac -> True...}
FciEnabledForConnectorAuthorization : True
DocumentTrackingFeatureState : Enabled

```



```
GlobalAddressListEnabled : True
OrganizationEnabled      : True
ExplicitLogonEnabled     : True
OWALightEnabled         : True
DelegatesAccessEnabled  : True
IRMEnabled               : True
CalendarEnabled         : True
ContactsEnabled         : True
TasksEnabled            : True
JournalEnabled          : True
NotesEnabled            : True
RemindersAndNotificationsEnabled : True
PremiumClientEnabled    : True
```

```
[PS] C:\Windows\system32>Get-IRMConfiguration

InternalLicensingEnabled      : True
ExternalLicensingEnabled     : False
JournalReportDecryptionEnabled : True
ClientAccessServerEnabled    : True
SearchEnabled                 : True
TransportDecryptionSetting    : Optional
EDiscoverySuperUserEnabled    : True
RMSOnlineKeySharingLocation   :
RMSOnlineVersion              :
ServiceLocation               :
PublishingLocation            :
LicensingLocation             : <>
```


Subject or body contains 'Azure Information Protection'

Name:

Subject or body contains 'Azure Information Protection' x

*Apply this rule if...

The subject or body includes...

'Azure Information Protection'

add condition

*Do the following...

Apply rights protection to the message with...

idam Demo Environment - Confidential View Only

add action

Except if...

add exception

Properties of this rule:

Priority:

0

Audit this rule with severity level:

Not specified

Choose a mode for this rule:

Enforce

Exchange admin center

recipients

permissions

compliance management

organization

protection

mail flow

mobile

public folders

unified messaging

in-place eDiscovery & hold auditing **data loss prevention** retention policies retention tags journal rules

You can use policy tips to notify users about policy matches.

[Manage policy tips](#)

You can use document fingerprints to customize sensitive information types in your policies.

[Manage document fingerprints](#)

Use DLP policies to scan email messages for sensitive information that may be subject to certain regulations or business policies. [Learn more](#)

+ - ✎ 🗑️ 🔄

ON	NAME	MODE
No DLP policies configured.		

DLP policy from template

Name:

Identify German Financial Data

Description:

*Choose a template:

France Data Protection Act	Germany Financial Data 15.0.3.0 Helps detect the presence of information commonly considered to be financial data in Germany like EU debit card numbers. Use of this policy does not ensure compliance with any regulation. After your testing is complete, make the necessary configuration changes in Exchange so the transmission of information complies with your organization's policies. Examples include configuring TLS with known business partners or adding more restrictive transport rule actions, such as adding rights protection to messages that contain this type of data.
France Financial Data	
France Personally Identifiable Information (PII) Data	
Germany Financial Data	
Germany Personally Identifiable Information (PII) Data	
Israel Financial Data	
Israel Personally Identifiable Information (PII) Data	
Israel Protection of Privacy	
Japan Financial Data	
Japan Personally Identifiable Information (PII) Data	

Identify German Financial Data

general

rules

*Name:

Identify German Financial Data

Description:

Helps detect the presence of information commonly considered to be financial data in Germany like EU debit card numbers. Use of this policy does not ensure compliance with any regulation. After your testing is complete, make the necessary configuration changes in Exchange so the transmission of information complies with your organization's policies. Examples include configuring TLS with

Choose the state of this DLP policy:

- Enabled
 Disabled

Choose a mode for the requirements in this DLP policy:

- Enforce
 Test DLP policy with Policy Tips
 Test DLP policy without Policy Tips

i Data Loss Prevention (DLP) is a premium feature that requires an Enterprise Client Access License (CAL). [Learn more](#)

Identify German Financial Data

general

rules

+ - ✎ 📄 🗑️ ↻

<input checked="" type="checkbox"/>	Germany Financial Data: Allow override
<input checked="" type="checkbox"/>	Germany Financial Data: Scan email sent outside - low count
<input checked="" type="checkbox"/>	Germany Financial Data: Scan email sent outside - high count
<input checked="" type="checkbox"/>	Germany Financial Data: Scan text limit exceeded
<input checked="" type="checkbox"/>	Germany Financial Data: Attachment not supported

1 selected of 5 total

If the message...

Is sent to 'Outside the organization'
and The message contains these sensitive information types: 'Credit Card Number' or 'EU Debit Card Number'

Do the following...

Set audit severity level to 'High'
and Notify the sender that the message can't be sent, but allow the sender to override and provide justification. Include the explanation 'Unable to deliver your message. You can override this policy by adding the word 'override' to the subject line' with static code '571'

Germany Financial Data: Scan email sent outside - high count

Name:
Germany Financial Data: Scan email sent outside - high coun

*Apply this rule if...

✘ The recipient is located... Outside the organization

and

✘ The message contains sensitive information... 'Credit Card Number' or 'EU Debit Card Number'

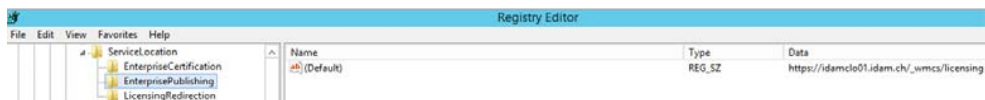
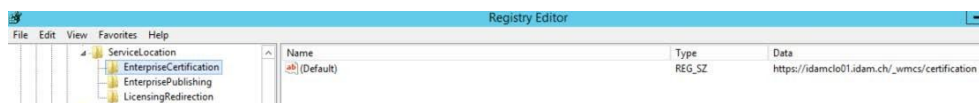
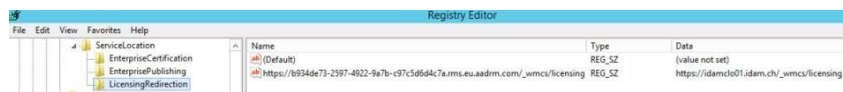
add condition

*Do the following...

Apply rights protection to the message with... idam Demo Environment - Confidential

add action

Name	Publisher
Active Directory Rights Management Services Client 2.1	Microsoft Corporation
AppFabric 1.1 for Windows Server	Microsoft Corporation
Microsoft CCR and DSS Runtime 2008 R3	Microsoft Corporation
Microsoft SharePoint Server 2013	Microsoft Corporation
Microsoft SQL Server 2005 Analysis Services ADOMD.NET	Microsoft Corporation
Microsoft SQL Server 2008 R2 Native Client	Microsoft Corporation
Microsoft Sync Framework Runtime v1.0 SP1 (x64)	Microsoft Corporation
System Center Endpoint Protection	Microsoft Corporation
WCF Data Services 5.0 (OData v3)	Microsoft Corporation
WCF Data Services 5.6 Tools	Microsoft Corporation





Security

Central Administration

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security**
- Upgrade and Migration
- General Application Settings



Users

[Manage the farm administrators group](#) | [Approve or reject distribution groups](#) | [Specify web application user policy](#)



General Security

[Configure managed accounts](#) | [Configure service accounts](#) | [Configure password change settings](#) | [Specify authentication providers](#) | [Manage trust](#) | [Manage antivirus settings](#) | [Define blocked file types](#) | [Manage web part security](#) | [Configure self-service site creation](#)



Information policy

[Configure information rights management](#) | [Configure Information Management Policy](#)

Information Rights Management

Information Rights Management

IRM helps protect sensitive files from being misused or distributed without permission once they have been downloaded from this server.

Specify the location of Windows Rights Management Services (RMS):

- Do not use IRM on this server
- Use the default RMS server specified in Active Directory
- Use this RMS server:

Check this box in multi-tenant configurations to allow tenants to configure tenant level IRM settings.

Information Rights Management (IRM)

Set IRM capabilities to SharePoint for your organization (requires Office 365 IRM service)

- Use the IRM service specified in your configuration
- Do not use IRM for this tenant

[Refresh IRM Settings](#)

We successfully refreshed your settings.

idam demo environment

TEMPLATES

NAME	DESCRIPTION	DATE MODIFIED	S...
idam Demo Environment - Confidential	This content is proprietary informat...	10/21/2014 12:33:00 AM	Publish...
idam Demo Environment - Confidential View Only	This content is proprietary informat...	10/21/2014 12:33:00 AM	Publish...
External Sharing - Confidential content	This content is confidential and onl...	4/20/2016 10:44:00 AM	Publish...
idam Demo Environment - Human Resources Confidential	idam Demo Environment - Human...	6/29/2016 3:45:00 PM	Publish...

active directory

[DIRECTORY](#) [ACCESS CONTROL NAMESPACES](#) [MULTI-FACTOR AUTH PROVIDERS](#) [RIGHTS MANAGEMENT](#)

NAME	RIGHTS MANAGEMENT STATUS
idam Demo Environment →	Active
idam Development Environment	Inactive
idam Demo B2C Environment	Inactive

Add a new rights policy template

Language

Name

Description

idam demo environment - human resources confidential

[RIGHTS](#) [SCOPE](#) [CONFIGURE](#)

The author of a protected document always has Full Control rights.

USER NAME	RIGHTS
HumanResources@idam.ch	Copy and Extract Content, Allow Macros, Print, Reply, Reply All, View Content

Assign custom rights

NAME
<input checked="" type="checkbox"/> View Content
<input type="checkbox"/> Save File
<input type="checkbox"/> Edit Content
<input checked="" type="checkbox"/> Copy and Extract Content
<input type="checkbox"/> View Assigned Rights
<input type="checkbox"/> Change Rights
<input checked="" type="checkbox"/> Allow Macros
<input type="checkbox"/> Export Content (Save As)
<input checked="" type="checkbox"/> Print
<input type="checkbox"/> Forward
<input checked="" type="checkbox"/> Reply
<input checked="" type="checkbox"/> Reply All
<input type="checkbox"/> Full Control

name and description

LANGUAGE	NAME	DESCRIPTION
German - Germany	Idam Demo Environment - Human Resources Con	Idam Demo Environment - Human Resources Con
English - United States	Idam Demo Environment - Human Resources Con	Idam Demo Environment - Human Resources Con
Select language	<i>NAME</i>	<i>DESCRIPTION</i>

content expiration

- Content never expires
- Content expiration (date)
- After the content is protected, content expires after the specified number of days

offline access

- Content is available only with an Internet connection
- Content is always available
- Number of days the content is available without an Internet connection

idam demo environment - human resources confidential

[RIGHTS](#) [SCOPE](#) [CONFIGURE](#)

USER NAME



humanresources@idam.ch

general

STATUS

PUBLISH

ARCHIVE

Info



Protect Document

Control what types of changes people can make to this document.

- Mark as Final**
Let readers know the document is final and make it read-only
- Encrypt with Password**
Password-protect this document
- Restrict Editing**
Control the types of changes others can make
- Restrict Access**
Grant people access while removing their ability to edit, copy, or print.
- Add a Digital Signature**
Ensure the integrity of the document by adding an invisible digital signature

are that it contains:
uthor's name

- Unrestricted Access
- Restricted Access
- idam Demo Environment - Confidential
- idam Demo Environment - Confidential View Only
- idam Demo Environment - Human Resources Confidential

Properties

Size	Not saved yet
Pages	1
Words	0
Total Editing Time	0 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments

Related Dates

Last Modified	
Created	Today, 19:11
Last Printed	

Related People

Author	Jochen Nickel
	Add an author
Last Modified By	Not saved yet

Show All Properties

external sharing - confidential content

 RIGHTS SCOPE CONFIGURE

The author of a protected document always has Full Control rights.

USER NAME	RIGHTS
marketing@idam.ch	View Content, Export Content (Save As)
engineering@identityplus.ch	View Content, Edit Content

```
PS C:\Windows\system32> Get-AdmTemplateProperty -TemplateId fc7173b1-1109-4ecf-8400-8f24600b9a27 -RightsDefinitions | fl
Key : RightsDefinitions
Value : {marketing@idam.ch -> VIEW, EXPORT, engineering@identityplus.ch -> VIEW, DOCEDIT}
```

```
PS C:\Users\jochen.nicke\Desktop> Protect-RMSFile -TemplateID 61d62ec9-fe90-40d7-ae18-8617b7e8585c -File .\SuperUserDemo.xlsx
InputFile                               EncryptedFile
-----
C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx

PS C:\Users\jochen.nicke\Desktop> Unprotect-RMSFile -File ".\SuperUserDemo.xlsx"
InputFile                               DecryptedFile
-----
C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx C:\Users\jochen.nicke\Desktop\SuperUserDemo.xlsx
```



LABEL NAME	TOOLTIP	MARKING	PROTECTION
Personal	This data is meant for personal usage. It must not include any business information and is not monitored by the busin...		...
Public	This data is public and can be used by everyone.		...
Internal	This data can be used by all employees, and can be shared with authorized customers and business partners. This data...		...
Confidential	This data represents sensitive information for the business and can be used by specific individuals and groups of users...	✓	idam Demo Environment - Confid... ..
Secret	This data represents sensitive information for the business and must be protected for individuals or groups of users in...	✓	idam Demo Environment - Confid... ..

All documents and emails must have a label (applied automatically or by users)

Off On

Select the default label

Public ▼

Users must provide justification when lowering the sensitivity level (for example, from Confidential to Public)

Off On

Label: Confidential



Save



Discard



Delete this
label

Specify how this label is displayed in the Information Protection client on user devices

Enabled

On

Off

* Name

Confidential

Tooltip

This data represents sensitive information for the business and can be used by specific individuals and groups of users in the company.

Color

Orange



Set RMS protection for documents and emails containing this label

Select RMS template

idam Demo Environment - Confidential



Set visual marking (such as header or footer)

Documents with this label have a header

Off On

Documents with this label have a footer

Off On

* Text

Document sensitivity: Confidential

* Font size

10

Color

Black ▼

Alignment

Left Center Right

Documents with this label have a watermark

Off On

* Text

Confidential

Configure conditions for automatically applying this label

If any of these conditions are met, this label is applied

CONDITION NAME	OCCURRENCES
International Banking Account Number (IBAN)	1

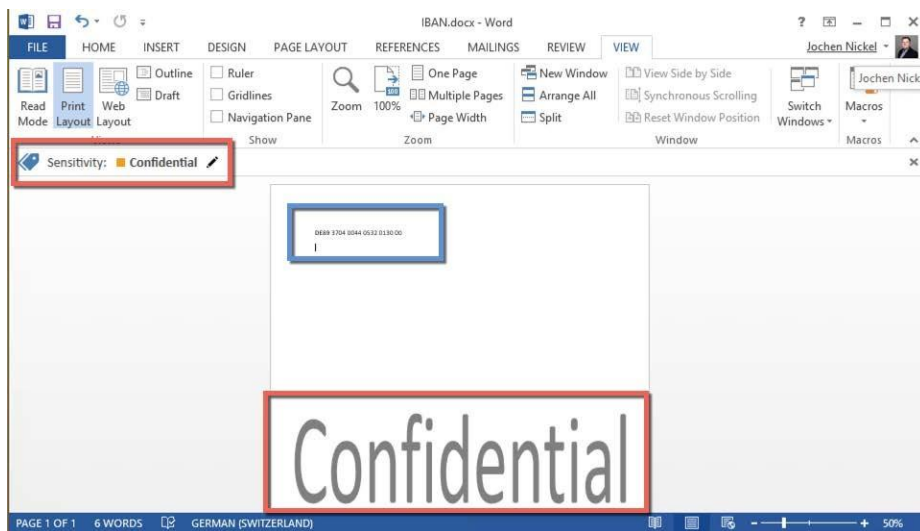
[+ Add a new condition](#)

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

It is recommended to label this file as Confidential



- Info
- New
- Open
- Save
- Save As
- Print

Info

IBAN

Desktop



Protect Document

idam Demo Environment - Confidential : This content is proprietary information intended for internal users only. This content can be modified but cannot be copied and printed.

Financial Statements

Commercial balance sheet USA

OL	Ledger	Currency type	Company code	curr-
10				
FS Item	Text for B/S P&L Item			
1000000	Assets			
1000000	=====			
1010000	Current Assets			
1010000	-----			
1011000	Cash			
1011300	Bank 1			
1011300	113100 Citibank Account			
1011300	113101 Citibank - checks payable			
1011300	Total Bank 1			
1011000	Total Cash			
1013000	Accounts Receivable			
1013200	Trade Receivables- Short Term			
1013200	140000 Trade Receivables - domestic			
1013200	Total Trade Receivables - Short Term			
1013300	Less : Allowance For Doubt. Debts.			
1013300	080000 General Doubtful Debt Provision - lump sum			
1013300	Total : Allowance for Doubt Debts.			
1013000	Total Accounts Receivable			

Choose Download Protection...

The information being downloaded might require protection. Please select an option below.
[Learn more...](#)

Company Policies | My Policies

The list of policies has been automatically filtered. [Click here to view all.](#)

Detail	My Policies
Confidential - View-Only	
Confidential	

This content is proprietary information intended for internal users only. This content cannot be modified.

Save | Save Unprotected | Cancel

Setting was applied

SAP | HTE (1) 800 | HCDEMOIN | OVR

IDAM DEMO ENVIRONMENT - CONFIDENTIAL VIEW ONLY This content is proprietary information intended for internal uses only. This content cannot be modified. View Permission...

Financial Statement Item

Financial Statement Item	Text for B/S P&L Item	Total of reporting period	Total of the comparison period	Absolute difference	Percentage difference
1					
2	1000000	Assets	0.00	0.00	0.00
3	1000000	Current Assets	0.00	0.00	0.00
4	1010000	Cash	0.00	0.00	0.00
5	1011000	Bank 1	0.00	0.00	0.00
6	1011300	113100 Citibank Account	-1846705.18	-1629997.23	-21670794.68 13.3
7	1011300	113101 Citibank - checks payable	-72385398.65	-72385398.65	0.00 0.0
8	1011300	Total Bank 1	-62055916.68	-240385122.00	-21670794.68 9.0
9	1011000	Total Cash	-262055916.68	-240385122.00	-21670794.68 9.0
10	1013000	Accounts Receivable	0.00	0.00	0.00
11	1013200	Trade Receivables - Short Term	0.00	0.00	0.00
12	1013200	140000 Trade Receivables - domestic	10811058.03	10843115.03	-32057.00 0.3
13	1013200	Total Trade Receivables - Short Term	10811058.03	10843115.03	-32057.00 0.3
14	1013300	Less - Allowance For Doubt Debts	0.00	0.00	0.00
15	1013300	090000 General Doubtful Debt Provision - lump sum	-1274890.39	-1274890.39	0.00 0.0
16	1013300	Total Allowance for Doubt Debts	-1274890.39	-1274890.39	0.00 0.0
17	1013000	Total Accounts Receivable	9536167.64	9568224.64	-32057.00 0.3
18	1015000	Inventory	0.00	0.00	0.00
19	1015100	Raw Materials	0.00	0.00	0.00
20	1015100	300000 Inventory - Raw Material 1	-1950056403.48	-1950034972.80	-22330.68 0.0
21	1015100	Total Raw Materials	-1950056403.48	-1950034972.80	-22330.68 0.0
22	1052000	Work In Process	0.00	0.00	0.00
23	1052000	790000 Work in process inventory	9248058.64	9313405.84	-65347.20 0.7
24	1052000	Total Work In Process	9248058.64	9313405.84	-65347.20 0.7
25	1053000	Finished Goods	0.00	0.00	0.00
26	1053000	310000 Inventory - OEM products	-885705438.61	-845321939.11	-59616500.50 6.3
27	1053000	792000 Finished goods inventory	-3614015814.87	-3614008876.87	-792762.00 0.0
28	1053000	Total Finished Goods	-4499721253.48	-4560130515.98	60409262.50 1.3
29	1056000	Packing Materials	0.00	0.00	0.00

Display View "Halocore Client Parameters (RMS Integration)": Details



Halocore Client Parameters (RMS Integration)

RMS is Active

Policy Selection UI

AD Explosion Depth

Documentation URL

License Expiration

"Own Use" Desc.

Program Edit Goto System Help

Flexible Employee Data

Further selections Search helps Sort order Org. structure

Key date

Today
 Other keydate

Key Date

Selection

Personnel Number
 Personnel area 3000

Additional data

Field selection (active)

Flexible Employee Data

Key date: 01.03.2016

Last Name	First Name	Personnel Number	Date of Birth	Entry Date	Nationality	Number of Children	Total basic pay	Crcy	Wage Type
Zubke	Carsten	00010870	25.01.1970	01.01.2002	American	0	1.250,00	USD	
Fredericks	Frank	00010960	12.10.1960	01.06.1999	American	0	2.250,00	USD	
Henning	Anne	00010961	11.02.1960	01.06.1999	American	0	1.750,00	USD	
Jensen	Steve	00010962	10.03.1960	01.06.1999	American	0	1.750,00	USD	
Kyne	Kevin	00010963	13.03.1960	01.06.1999	American	0	1.750,00	USD	
Blackton	Barbara	00010964	10.05.1960	01.06.1999	American	0	1.750,00	USD	
Francis	Nancy	00010965	15.05.1960	01.06.1999	American	0	1.500,00	USD	
Anderson	Andrew	00010966	11.01.1960	01.06.1999	American	0	1.500,00	USD	
Olbright	Ellen	00010967	10.07.1960	01.06.1999	American	0	1.500,00	USD	
Parker	Alan	00010968	22.02.1960	01.06.1999	American	0	1.250,00	USD	
Tendy	Jessica	00010969	19.09.1960	01.06.1999	American	0	1.750,00	USD	
Peter	Russel	00080012	01.03.1969	01.01.2006	American	0	2.000,00	USD	
Porter	Susan	00080014	01.03.1969	01.01.2006	American	0	3.000,00	USD	
Jones	Bobby	00080090	08.09.1960	11.10.2004		0	1.750,00	USD	
Jones	Robert	00080091	09.11.1964	11.10.2004		0	2.500,00	USD	
Stark	Allison	00080200	14.09.1974	25.03.2002		0	2.500,00	USD	
Jones	Gary	00080201	14.02.1964	16.08.2003		0	2.000,00	USD	
Reynolds	Andrea	00080202	14.02.1974	04.06.2002		0	1.250,00	USD	

SAP >> | HTE (1)

A	B	C	D	E	F	G	H	I
Last Name	First Name	Personnel Number	Date of Birth	Entry Date	Nationality	Number of Children	Total basic pay	Currency
1								
2	Zubke	Carsten	10970	1/25/1970	1/1/2002 American	0	1250.00	USD
3	Fredericks	Frank	10960	10/12/1960	6/1/1999 American	0	2250.00	USD
4	Henning	Anne	10961	2/11/1960	6/1/1999 American	0	1750.00	USD
5	Jensen	Steve	10962	3/10/1960	6/1/1999 American	0	1750.00	USD
6	Kyne	Kevin	10963	3/13/1960	6/1/1999 American	0	1750.00	USD
7	Blackton	Barbara	10964	5/10/1960	6/1/1999 American	0	1750.00	USD
8	Francis	Nancy	10965	5/15/1960	6/1/1999 American	0	1500.00	USD
9	Anderson	Andrew	10966	1/11/1960	6/1/1999 American	0	1500.00	USD
10	Olbright	Ellen	10967	7/10/1960	6/1/1999 American	0	1500.00	USD
11	Parker	Alan	10968	2/22/1960	6/1/1999 American	0	1250.00	USD
12	Tendy	Jessica	10969	9/19/1960	6/1/1999 American	0	1750.00	USD
13	Peter	Russel	80012	3/1/1969	1/1/2006 American	0	2000.00	USD
14	Porter	Susan	80014	3/1/1969	1/1/2006 American	0	3000.00	USD
15	Jones	Bobby	80090	9/8/1960	10/11/2004	0	1750.00	USD
16	Jones	Robert	80091	11/9/1964	10/11/2004	0	2500.00	USD
17	Stark	Allison	80200	9/14/1974	3/25/2002	0	2500.00	USD
18	Jones	Gary	80201	2/14/1964	8/16/2003	0	2000.00	USD
19	Reynolds	Andrea	80202	2/14/1974	6/4/2002	0	1250.00	USD
20	Rae	Angela	80203	3/25/1980	11/28/2004	0	2250.00	USD
21	Jones	Stephanie	80204	5/23/1970	2/12/2005	0	2250.00	USD

Simulate Policy Derivation

Domain	Sensitivity	Policy	Match
ENG	CONF	Confidential - View-Only	OO■
ENG	INTERNAL	Confidential - View-Only	OO■
ENG	PUBLIC	Confidential - View-Only	OO■
ENG	SECRET	Confidential	O▲O
FIN	CONF	Confidential - View-Only	OO■
FIN	INTERNAL	Confidential - View-Only	OO■
FIN	PUBLIC	Confidential - View-Only	OO■
FIN	SECRET	Confidential	O▲O
GP	CONF	Confidential - View-Only	OO■
GP	INTERNAL	Confidential - View-Only	OO■
GP	PUBLIC	Confidential - View-Only	OO■
GP	SECRET	Confidential	O▲O
HCM	CONF	Confidential - Human Resources	O▲O
HCM	INTERNAL	Confidential - Human Resources	O▲O
HCM	PUBLIC	Confidential - Human Resources	O▲O
HCM	SECRET	Confidential - Human Resources	O▲O
LOG	CONF	Confidential - View-Only	OO■
LOG	INTERNAL	Confidential - View-Only	OO■
LOG	PUBLIC	Confidential - View-Only	OO■
LOG	SECRET	Confidential	O▲O
SLS	CONF	Confidential - View-Only	OO■
SLS	INTERNAL	Confidential - View-Only	OO■
SLS	PUBLIC	Confidential - View-Only	OO■
SLS	SECRET	Confidential	O▲O

Chapter 16: Choosing the Right Technology, Methods, and Future Trends

