

LOW LEVEL DESIGN DOCUMENT

Cloud Identity and Access Management (IAM)

Date: May, 2020

TABLE OF CONTENTS

1. Build Overview
 - 1.1 Azure Active Directory
 - 1.2 Azure AD Features
 - 1.3 Decision Tree
 - 1.4 Identity and Access Management services
2. Detailed Design
 - 2.1 Manage Directory
 - 2.2 Manage Groups
 - 2.3 Manage Users
 - 2.4 Bulk activity and downloads in the Azure AD admin portal
 - 2.5 Manage Role assignments
3. Self Service Password Reset (SSPR)
 - 3.1 Configuring self service password reset
 - 3.1.1 Password reset
 - 3.1.2 Authentication method
 - 3.1.3 Registration settings
 - 3.1.4 Notification settings
 - 3.1.5 Customization settings
 - 3.1.6 Password Writeback
4. Multi-Factor Authentication (MFA)
 - 4.1 Available verification methods
5. Implement and manage hybrid identities
 - 5.1 Azure AD Connect using Express Settings
 - 5.2 Enable password hash synchronization/pass-through authentication/AD FS
 - 5.3 Enable password writeback
 - 5.4 Enable password writeback for SSPR
6. Monitoring RBAC Activity Logs
7. Azure Policy
8. Illustrative Design

Cloud Identity and Access Management (IAM)

1. Build Overview

This Section provides low-level design solution, decision tree and architecture to provide Identity and access management to protect <Customer> applications and data in cloud with Azure identity and access management solutions.

<Customer> identity and access management solution in azure is derived using the decision tree based on multiple considerations. The proposed solution includes managing user identity for authentication and authorization using hybrid identity with Azure AD and managing access to azure resources using Azure RBAC.

1.1 Azure Active Directory

Azure Active Directory (Azure AD) is multi-tenant cloud based Identity and access management service which can provide access to <customer's> users, groups, and enterprise applications,

Azure AD allows users and groups to manage access to <customer's> cloud-based apps, on-premises apps, and resources.

Resources can be part of the Azure AD organization, such as permissions to manage objects through roles in Azure AD, or external to the organization, such as for Software as a Service (SaaS) apps, Azure services, SharePoint sites, and on-premises.

Azure AD provides Single Sign-On (SSO) access to customer cloud SaaS applications.

1.2 Azure AD Features:

Enterprise Identity Solution: Create a single identity for user and keep them in sync across the enterprise.

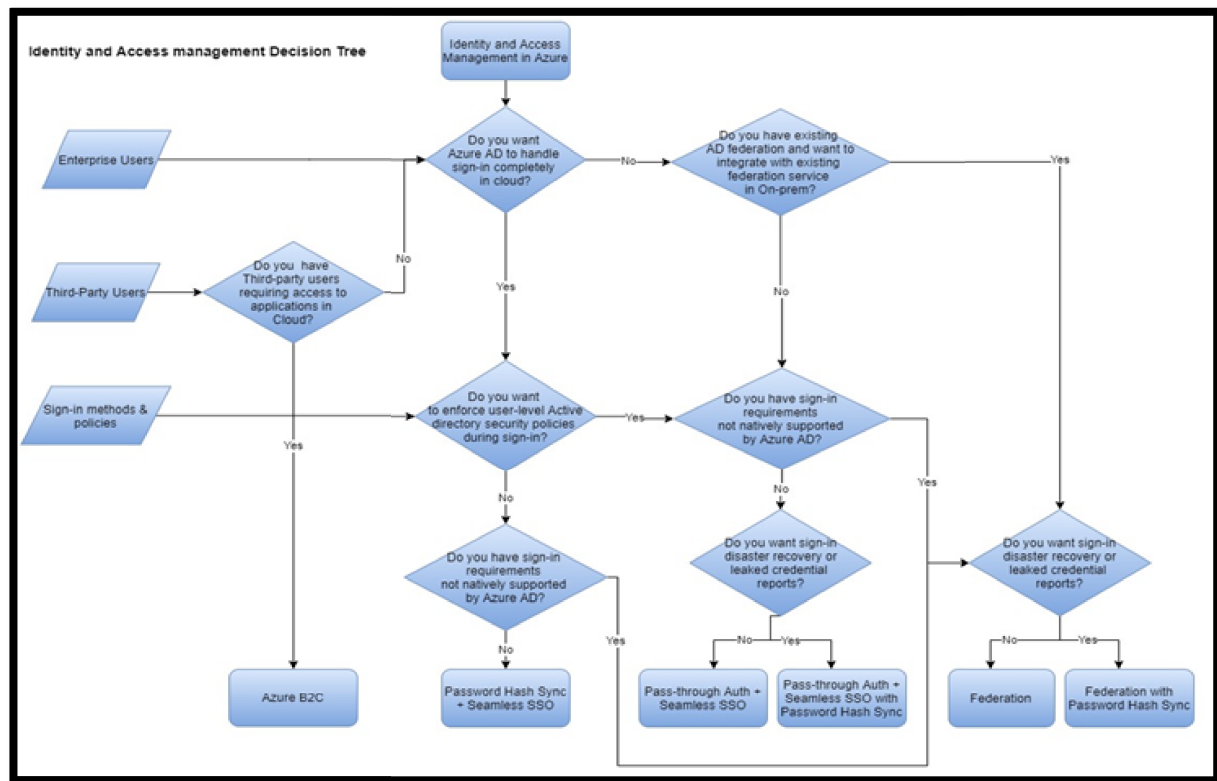
Single Sign-On: provides single sign-on access to applications and infrastructure services.

Multifactor Authentication: Enhance security with additional factors of authentication

Self-Service: Empower customer users to complete password resets themselves, as well as request access to specific apps and services

1.3 Decision Tree:

Hybrid Identity solution decision tree shows a series of decisions that will help <Customer> to choose a appropriate authentication method for Azure Active Directory hybrid identity solution. The flowchart guides through a set of key decision criteria to reach a recommendation.



1.4 Identity and Access Management Services

Secure access to customer resources with Azure Identity and Access Management Solution.

Below are the identity and access management services provided by Azure Active Directory.

For access and authentication

- Multi-factor authentication
- Device Registration
- Role Based Access Control

For Management

- Self Service Password Management
- Self Service Group Management
- Privileged Account Management

For Monitoring and Auditing

- Application Usage Monitoring
- Rich Auditing
- Security Monitoring and Alerting

2. Detailed Design:

2.1 Manage Directory:

Managing <customer> Organization:

- Sign up for Azure AD as an organization
- Sign up for Azure AD Premium
- Add a custom domain name
- Add company branding
- Associate an Azure subscription
- Add customer privacy info

Domain name is a domain name that is owned and used by <customer>

A domain name is an identifier for many directory resources such as,

- User name or email address
- Address for a group
- App ID URI for an application

Azure Active Directory and Azure Active Directory (B2C) enable users to access applications published by <customer> and share same administration experiences.

Below table content shows the parameters that are required to choose directory type for the customer.

Parameter	Value
Select a directory type	<customer specified directory type> <ul style="list-style-type: none">• Azure Active Directory• Azure Active Directory(B2C)

Below table content shows the parameters that are required to create AD Tenent in a cloud directory.

Parameter	Value
Organization name	<customer specified organization name>
Initial Domain Name	< customer specified domain name>
Location	<customer specified Location>

2.2 Manage Groups :

Managing Groups includes:

- Create a group and add members
- Add or remove group members
- Delete a group and its members
- Add or remove a group from another group
- Edit group information
- Add or remove group owners

Below table content shows the parameters are required for creating groups in a <customer> cloud directory

Parameter	Value
Group type	<customer specified group type> <ul style="list-style-type: none">• Security• Office 365
Group name	<customer specified group name>
Group Description	<add customer specified group description>
Member Type	<add customer specified members>

2.3 Manage Users:

Managing Users includes:

- Add or delete a user
- Add or change user profile info
- Reset a user's password
- Assign roles to users
- Assign or remove licenses from users
- Restore a deleted user

Below table shows the parameters that are required for creating users in a <customer> cloud IAM.

Parameter	Value
Name	<name of the user>
User Name	<name of the user>@<customer domain name>
Profile	General → <First name> , <Last name> Work Info → <custome specified Job Title>, <customer specified description for user work>
Properties	<customer specified properties>
Groups	<add user to customer specified group>

Directory Roles	<customer specified role> <ul style="list-style-type: none"> • Users • Global Administrators • Limited Administrators
password	<random generated password>

2.4 Bulk activity and downloads in the Azure AD admin portal:

- <Customer> can perform bulk activities on users and groups in Azure AD by uploading a CSV file in the Azure AD
- <Customer> can create users, delete users, and invite guest users. And customer can add and remove members from a group.
- <Customer> can also download lists of Azure AD resources from the Azure AD admin portal.
- <Customer> can download the list of users in the directory, the list of groups in the directory, and the members of a particular group.

2.5 Manage Role Assignment:

Administrative roles:

Administrative roles can be used to grant access to Azure AD and other Microsoft services.

Below table content shows some of the following Built-in roles that are assigned to <customer> users.

Groups administrator	Can manage all aspects of groups and group settings like naming and expiration policies.
Global reader	Can read everything that a global administrator can, but not update anything.
Password administrator	Can reset passwords for non-administrators and Password administrators.
Security administrator	Can read security information and reports, and manage configuration in Azure AD and in Office 365.
Security reader	Can read security information and reports in Azure AD and Office 365.

Below table shows the parameters required to add role assignments to the users / groups in a <customer> cloud IAM.

Parameter	Value
Subscriptions	<customer specified subscription>
Role	<customer specified role>
Assign Access to	<customer specified>
Select members/groups	<customer specified>

Role-Based Access Control (RBAC):

Use of Role Based Access Control(RBAC) is one of the important aspects for the organizations that want to implement security policies for the data access by restricting access based on the need and least privilege security principles

RBAC can be used to assign permissions to users, groups and applications at a certain scope based on the roles assigned. A role assignment can be done at a single resource, a resource group , subscription or management group level called as scope

To assign custom roles to a user, <customer> needs Azure AD Premium P1 or P2.

Custom role creation in azure portal is generally available.

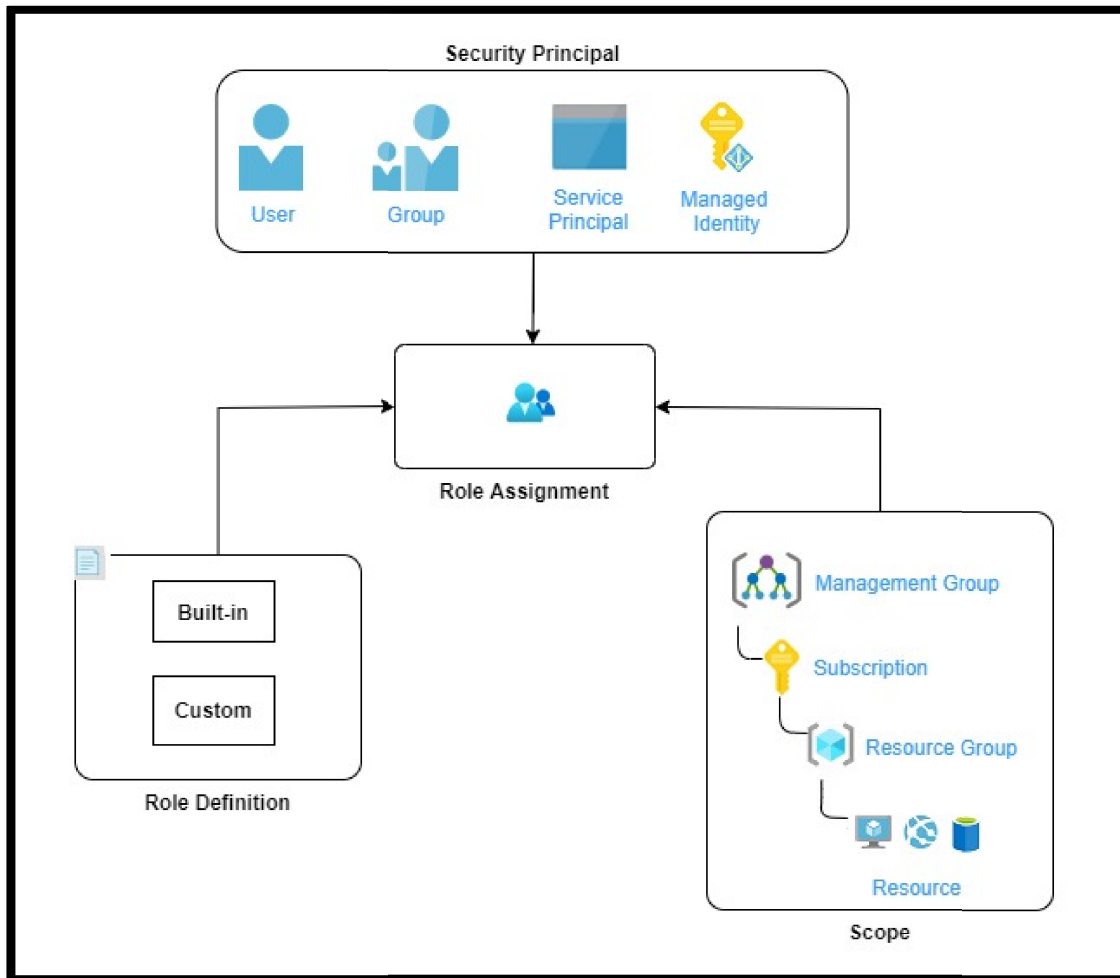
Previously creating and editing custom role was only possible through CLI or azure resources manager API. Now, RBAC workflows can be managed from the portal.

Security principal: A security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources

Role definition: A role definition is a collection of permissions which lists the operations that can be performed, such as read, write, and delete. Roles can be high-level, like owner, or specific, like virtual machine operator.

Scope: Scope is the set of resources that the access applies to management group, subscription, resource group, or resource in Azure.

Below diagram illustrates how access to resources in Azure controlled by creating role assignments in RBAC which consists of of three elements: security principal, role definition, and scope.



Access to resources in Azure is provided by creating role assignment by attaching these role definitions to a user, group, service principal, or managed identity at a particular scope

Custom Role definitions will be created if built-in roles don't meet the <Customer> specific access needs.

The following are the Built-in Azure RBAC roles will be utilized to provide list of privilege access to resources in Azure. Following are Custom RBAC roles that can be created and utilized in <Customer> Cloud environment to specific needs.

AD group Name	RBAC Role Name	Custom RBAC Role Definition	Scope
Azure_Confidential_Compute_Admin	RBAC_Compute_Admin	Create and manage own Microsoft Support requests; Create, update, manage, delete Virtual Machines	Subscription level

		<p>Create, update, manage, delete NICs, private IPs</p> <p>Create, update, manage, delete Public IPs</p> <p>Start/Stop/Restart/De-allocate Virtual Machines</p> <p>Access VM as a JIT user</p> <p>Assign/remove VM extensions</p> <p>Create, update, manage, delete Resource Groups</p> <p>Create, update, manage, delete VM Scale Sets</p> <p>Assign VMs to Availability Zones</p> <p>Create, update, manage, delete Azure load-balancers;</p> <p>Login Virtual Machine as Administrator</p> <p>Create, update, manage, delete Backup Vaults</p> <p>Enroll VMs for Backup into Recovery Services Vaults</p> <p>Create, update, manage, delete Backup and Retention Policies</p> <p>View backup job status</p> <p>Perform Discovery and Restore procedures</p> <p>Create, update, manage, delete ASR Recovery Services Vaults</p> <p>Enroll VMs for Disaster Recovery solution replication (ASR Site Recovery)</p> <p>Create, update, manage, delete Automation accounts;</p> <p>Create, update, manage, delete and run automation runbooks and jobs;</p>	
Azure_Confidential_SharedServices_Network_Admin	RBAC_SharedServices_Network_Admin	<p>Create and manage own Microsoft Support requests</p> <p>Create, update, manage,</p>	Management Group

		delete Virtual Networks Create, update, manage, delete subnets, NSGs, UDRs, ASGs Create, update, manage, delete Gateways Create, update, manage, delete Peering objects Create, update, manage, delete NICs, private IPs Create, update, manage, delete Vnet Service Endpoints Create, update, manage, delete Azure Load-balancers Create, update, manage, delete Application Gateways Create, update, manage, delete Network Watcher Create, update, manage, delete Public Reserved IPs Configure Port forwarding	
Azure_Confidential_Portfolio_Network_Admin	RBAC_Portfolio_Network_Admin	Create and manage own Microsoft Support requests Create, update, manage, delete subnets, NSGs, UDRs, ASGs Create, update, manage, delete Gateways Create, update, manage, delete Peering objects Create, update, manage, delete NICs, private IPs Create, update, manage, delete Vnet Service Endpoints Create, update, manage, delete Azure Load-balancers Create, update, manage, delete Application Gateways Create, update, manage, delete Network Watcher	Subscription level

		Create, update, manage, delete Public Reserved IPs Configure Port forwarding Create and manage Azure Public DNS zones Create and update DNS Zone records Create and manage own Resource Groups	
Azure_Confidential_Storage_Admin	RBAC_Storage_Admin	Create, update, manage, delete Shared Image Gallery Create, update, manage, delete Storage Accounts (blob, table, queue, file) Enable rotation of Storage Account keys Create, update, manage, delete storage account containers Create, update, manage, delete Storage account container access policies Manage geo-replication Create and manage noSQL DB instances Create and manage managed SQL DB Create and manage KeyVault stores	Subscription level
Azure_Confidential_App_Admin	RBAC_App_Admin	Create, update, manage, delete Azure Kubernetes Clusters; Create, update, manage, delete Cluster nodes and pods; Create, update, manage, delete own resource groups; Create, update, manage, delete Azure load-balancers; Create, update, manage, delete Docker Image repository; Create, update, manage, delete ACS Engine;	Subscription level

		Create, update, manage, delete Automation accounts; Create, update, manage, delete Data Factory services; Create, update, manage, delete Data Lake services; Create, update, manage, delete HDInsight services; Create, update, manage, delete Web Sites services;	
Azue_Confidential_Security_Admin	RBAC_Security_Admin	Read-only access to Azure resources Access to Azure Advisor View Azure policies View RBAC Policies Access to Security Center Access to Network Watcher Access and view of Audit/Activity logs Access to Apps Insights data Access to Azure Advisor Access to Log Analytics data Access to view Compliance reports Access to "Just in Time" policies	Management Group
Azure_Confidentail_Monitoring_Admin	RBAC_Monitoring_Admin	View VM monitoring data (ActivityLogAlerts) Access to App Insights Access to Log Analytics Read monitoring data Create, update, manage, delete monitoring metrics Access Network Watcher Monitor Gateways Monitor ExpressRoute circuits Monitor subscription quotas	
Azure_Confidentail_Governance_Admin	RBAC_Governance_Admin	Create Azure Policies Create Policy Definitions	Management

		Create Policy Assignments Create Custom Policies User Access Administration Permissions to invoke DR via Azure Site Recovery (fail-over and fail-back Permissions to make changes to Azure Traffic Manager profiles Access and read Billing Accounts Read Market Place usage billing reports View Cost configuration (budgets) Access to EA Portal as a Billing Administrator	Group
--	--	--	-------

3. Self-Service Password Reset (SSPR):

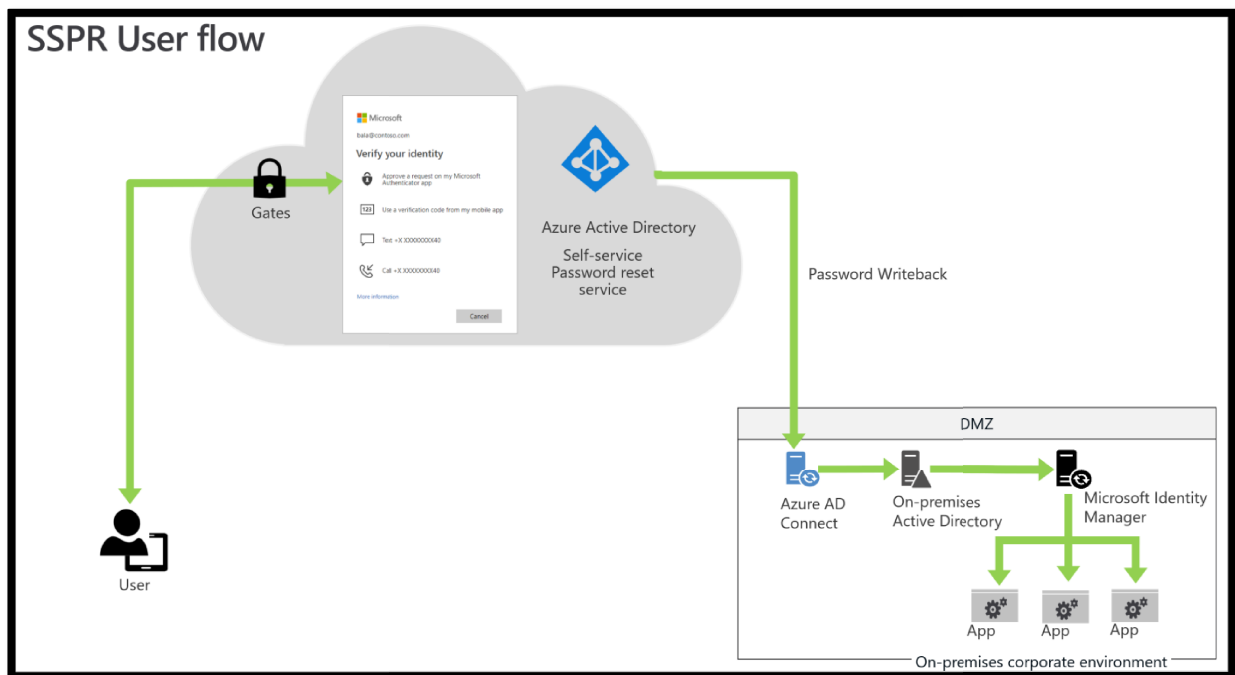
Self-Service Password Reset (SSPR) is an Azure Active Directory (AD) feature that enables users to reset their passwords.

This feature includes a set of capabilities that allow <customer> user's to manage any password from any device, at any time, from any location, while remaining in compliance with the security policies that <customer> define.

Why use self-service password reset?

- **Reduce Cost**
Support-assisted password reset is typically 20% of organization's IT spend
- **Improve User Experiences**
Users don't want to call helpdesk and spend an hour on the phone every time they forget their passwords
- **Lower Helpdesk Volume**
Password Management is the single largest helpdesk driver for most organizations
- **Enable Mobility**
Users can reset their passwords from wherever they are

Solution architecture for SSPR:



Description of workflow:

To reset the password, users go to the password reset portal. They must verify the previously registered authentication method or methods to prove their identity. If they successfully reset the password, they begin the reset process.

- For cloud-only users, SSPR stores the new password in Azure AD.
- For hybrid users, SSPR writes back the password to the on-premise Active Directory via the Azure AD Connect service.

3.1 Configure Self Service Password Reset:

3.1.1 Password Reset:

Below table shows the parameters that are required for setting up a self service password reset feature to the <customer> users/groups/all.

Parameter	Value
Self Service Password reset	<customer specified> <ul style="list-style-type: none">• None• Selected → To select Specific groups• All

3.1.2 Authentication methods:

When SSPR is enabled, users can only reset their password if they have data present in the authentication methods that the administrator has enabled. Methods include phone, Authenticator app notification, security questions, etc.

Set the **Authentication methods required to register** to at least one more than the number required to reset. Allowing multiple authentications gives users flexibility when they need to reset.

Set **Number of methods required to reset** to a level appropriate to <customer> organization. One requires the least friction, while two may increase <customer> security posture.

Below table shows the parameters that are required for setting up authentication method to the <customer> user

Parameter	Value
Number of methods required to reset	<customer specified reset method> <ul style="list-style-type: none">• Either 1 or 2
Methods available to users	<customer specified method to user> <ul style="list-style-type: none">• Mobile App Notification• Mobile App Code• Email• Mobile phone• Office Phone• Security Question

3.1.3 Registration settings:

Set **Require users to register when signing in** to **Yes/No**. This setting requires users to register when signing in, ensuring that all users are protected.

Set **Number of days before users is asked to reconfirm their authentication information** to between **90** and **180** days, unless <customer> organization has a business need for a shorter time frame.

Below table shows the parameters that are required for setting up registration method to the <customer> users.

Parameter	Value
Require users to register when signing in	<customer specified> <ul style="list-style-type: none">• YES/NO

Number of days before users are asked to reconfirm their authentication information	<customer specified> <ul style="list-style-type: none"> • 90 – 180 days
---	--

3.1.4 Notifications settings:

Configure both the **Notify users on password resets** and the **Notify all admins when other admins reset their password** to **Yes**. Selecting **Yes** on both increases security by ensuring that users are aware when their password is reset. It also ensures that all admins are aware when an admin changes a password. If users or admins receive a notification and they haven't initiated the change, they can immediately report a potential security issue.

Below table shows the parameters that are required for setting up notification method to the <customer> user.

Parameter	Value
Notify users on password reset?	<customer specified> <ul style="list-style-type: none"> • YES/NO
Notify all admins when other admins reset their password?	<customer specified> <ul style="list-style-type: none"> • YES/NO

3.1.5 Customization settings:

It's critical to customize the helpdesk email or URL to ensure users who experience problems can get help immediately. <Customer> can set this option to a common helpdesk email address or web page that <customer> users are familiar with.

Below table shows the parameters that are required for setting up customization to <customer> users.

Parameter	Value
Customize helpdesk link	<customer specified> <ul style="list-style-type: none"> • YES/NO
Custom helpdesk email or URL	<customer specified> <ul style="list-style-type: none"> • Support site • email address

3.1.6 Password Writeback:

Password Writeback is enabled with Azure AD Connect and writes password resets in the cloud back to an existing <customer> on-premises directory.

Below table shows the parameters that are required for setting up password write back to <customer> users.

Parameter	Value
Write back passwords to on-premises AD	<customer specified> <ul style="list-style-type: none">• YES/NO
Allow users to unlock account without resetting password	<customer specified> <ul style="list-style-type: none">• YES/NO

By default, Azure AD unlocks accounts when it performs a password reset.

4. Multi-Factor Authentication (MFA):

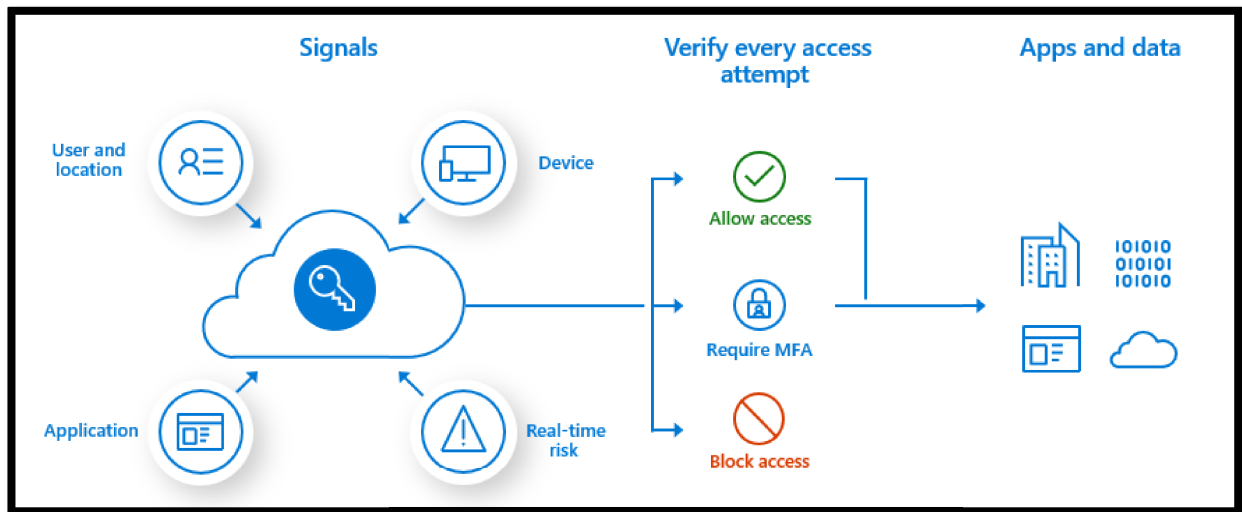
Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as to enter a code on their cellphone or to provide a fingerprint scan.

The recommended way to enable and use Azure Multi-Factor Authentication is with Conditional Access policies. With Conditional Access <customer> create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Why use Azure Multi-Factor Authentication?

- **Secure Application and Data**
Require additional layer of security when accessing on-premises and cloud applications.
- **Simple to Use**
Choose from call, text, or mobile app during registration. End users can change their method anytime.

Solution architecture for MFA:

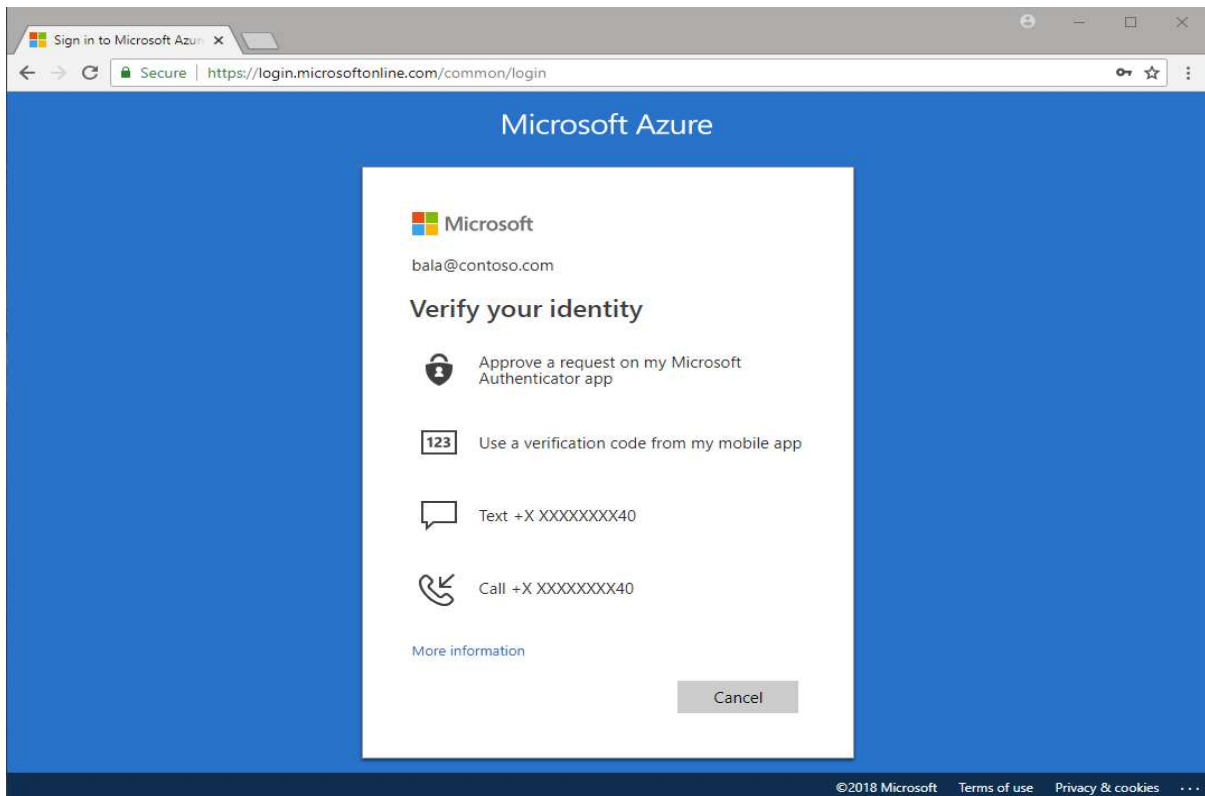


By implementing Azure MFA, an additional security layer is added for protecting <customers> user sign-in and transactions.

By enabling MFA, the user is asked for username, password and a secondary verification method. Secondary verification method can be through text message, phone call or email.

Azure Multi-Factor Authentication works by requiring two or more of the following authentication methods:

- password
- phone or hardware key.
- biometrics like a fingerprint or face scan.



Azure Multi-Factor Authentication helps safeguard access to data and applications while maintaining simplicity for users. It provides additional security by requiring a second form of authentication and delivers strong authentication.

4.1 Available verification methods

<Customer> can avail the following forms of verification with Azure Multi-Factor Authentication:

- Microsoft Authenticator app
- OATH Hardware token
- SMS
- Voice call

Below table shows the parameters that are required for setting up MFA for <customer> needs

Parameter	Value
Conditional access policy	<customer specified access policy>
Verification method	<customer specified> <ul style="list-style-type: none"> • Microsoft Authenticator app • OATH Hardware token • SMS • Voice call

5. Implement and manage hybrid identities

<Customer> can use Azure AD Connect Express Settings to implement and manage hybrid Identities.

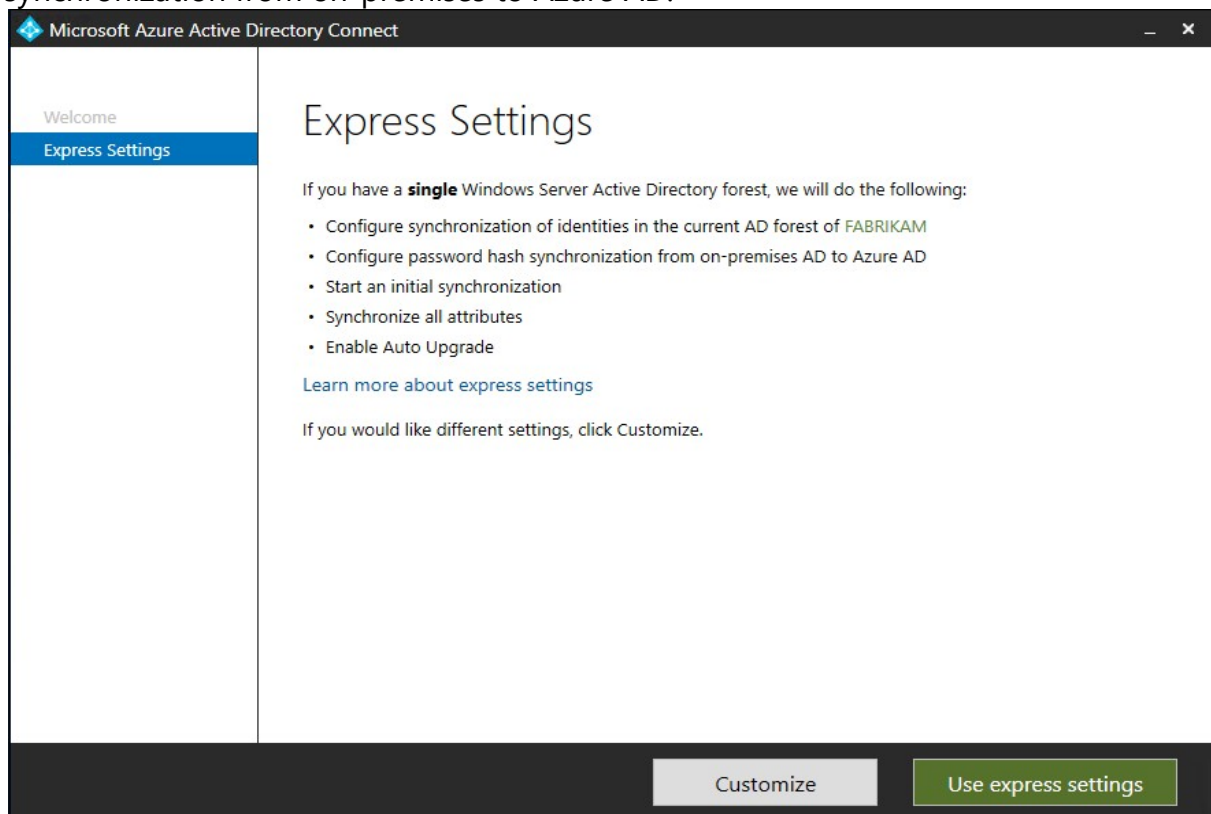
5.1 Azure AD Connect using Express Settings:

Azure AD Connect **Express Settings** can be used when <customer> have a single-forest topology and password hash synchronization for authentication.

Express installation of Azure AD Connect:

Below are the following steps to Install and configure Azure AD Connect; configure federation and single sign-on; manage Azure AD Connect; manage password sync and writeback

Step 1: Install Azure AD Connect for Express setting tool to configure password hash synchronization from on-premises to Azure AD.



Step 2: Connect to Azure AD needs <customer> global administrator credentials.

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure

Connect to Azure AD

Enter your Azure AD global administrator credentials. ?

USERNAME

PASSWORD

Previous Next

Step3: Connect to AD DS needs <customer> enterprise admin account credentials.

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Configure

Connect to AD DS

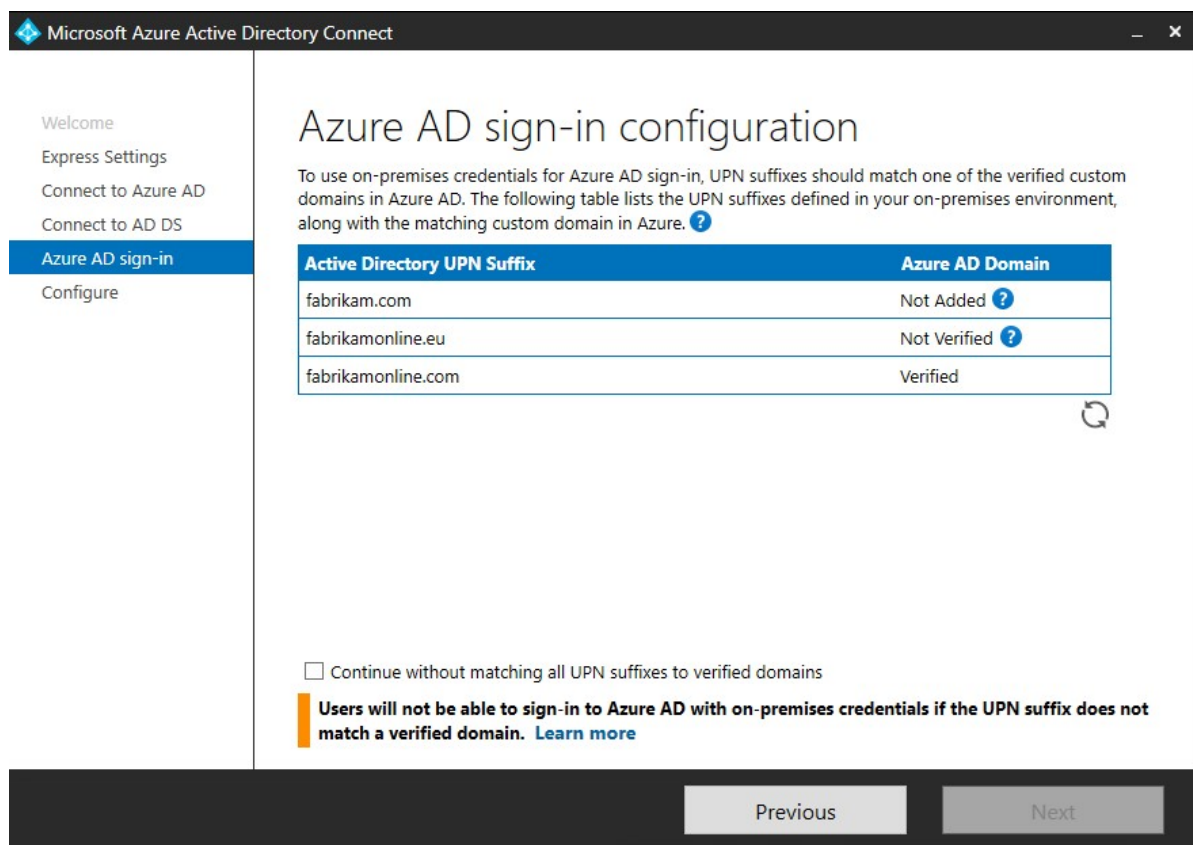
Enter the Active Directory Domain Services enterprise administrator credentials: ?

USERNAME

PASSWORD

Previous Next

Step 4: Azure AD sign-in configuration to verify <customer> domains.



Microsoft Azure Active Directory Connect

Welcome
Express Settings
Connect to Azure AD
Connect to AD DS
Azure AD sign-in
Configure

Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure. ?

Active Directory UPN Suffix	Azure AD Domain
fabrikam.com	Not Added ?
fabrikamonline.eu	Not Verified ?
fabrikamonline.com	Verified

☐ Continue without matching all UPN suffixes to verified domains

Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. [Learn more](#)

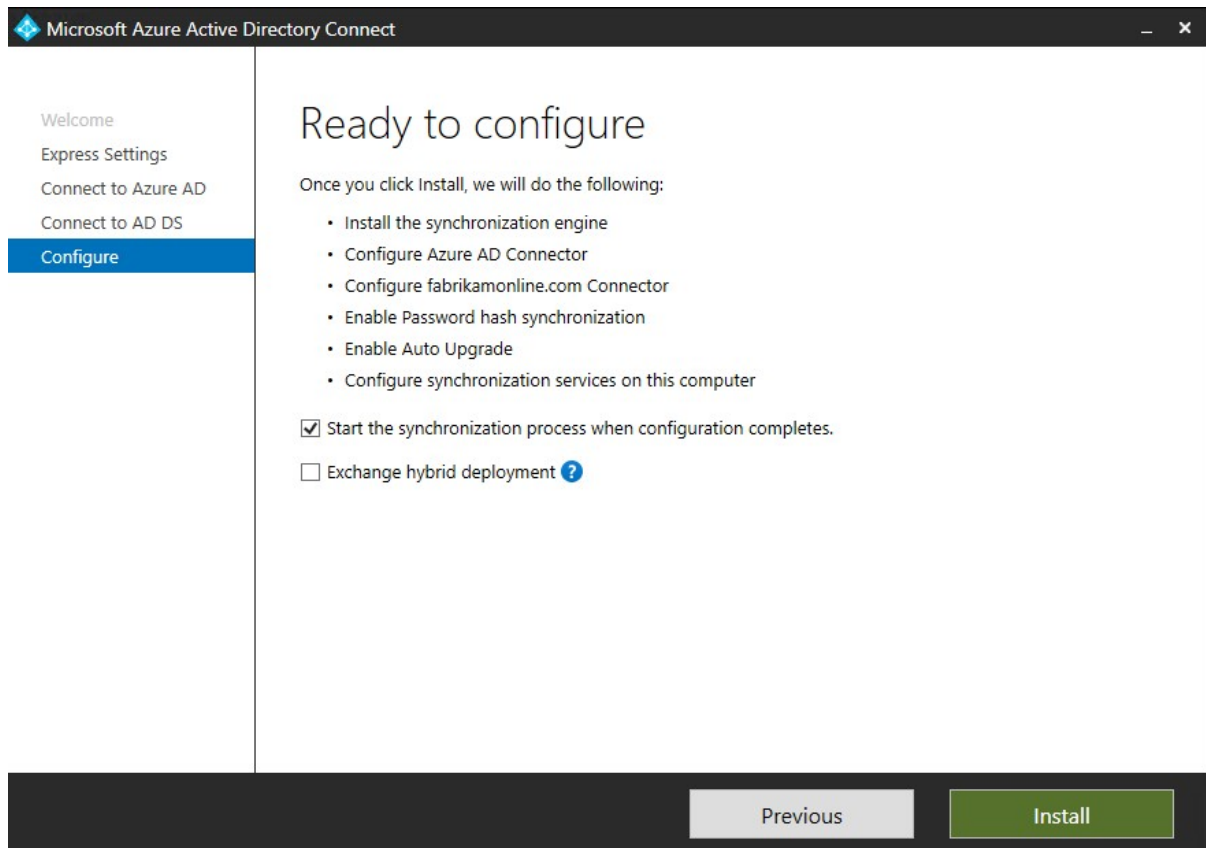
Previous Next

Step 5: Ready to configure

Optionally on the Ready to configure page, <customer> can unselect the **Start the synchronization process as soon as configuration completes** checkbox when <customer> needs additional should unselect this checkbox if <customer> want to do additional configuration, such as filtering.

Leaving the **Start the synchronization process as soon as configuration completes** checkbox enabled will immediately trigger a full synchronization to Azure AD of all users, groups, and contacts.

If <customer> have Exchange in on-premises Active Directory, then <customer> can choose an also option to enable Exchange Hybrid deployment <Customer> can enable this option if <customer> is willing to have Exchange mailboxes both in the cloud and on-premises at the same



After the installation has completed, <customer> can sign off and sign in again to use Synchronization Service Manager or Synchronization Rule Editor.

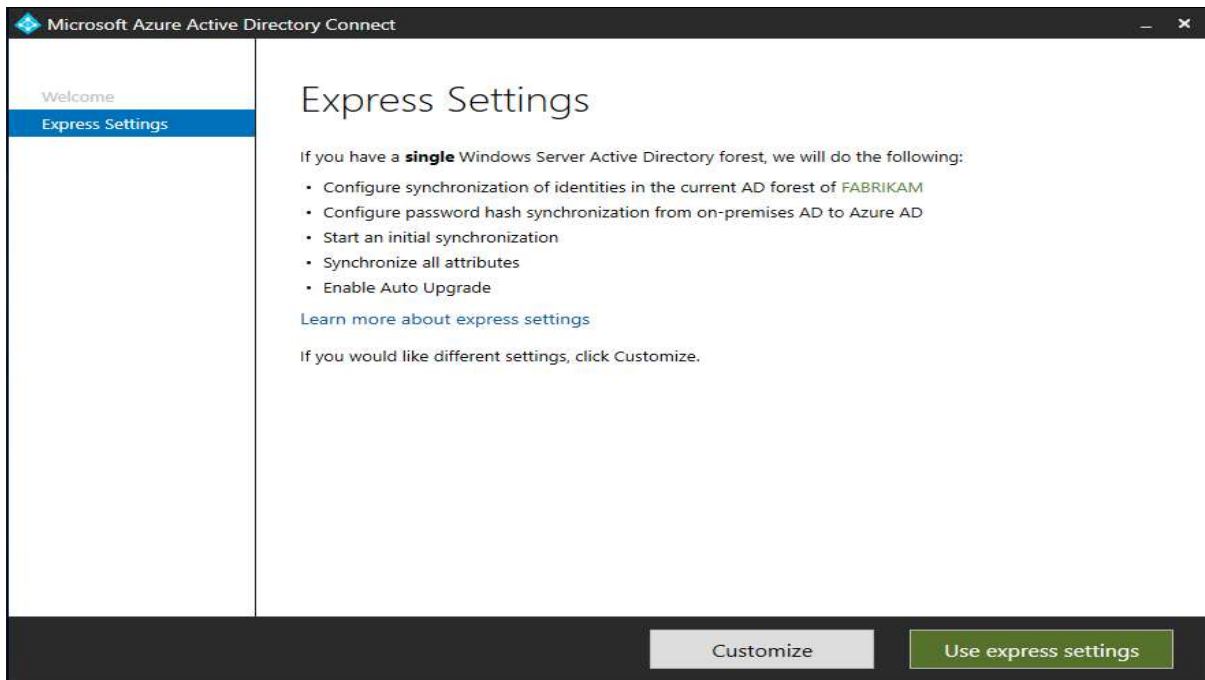
5.2 Enable password hash synchronization/pass-through authentication/AD FS:

<Customer> can use Azure AD Connect **Express Settings** option, to automatically enable password hash synchronization pass-through authentication/AD FS.

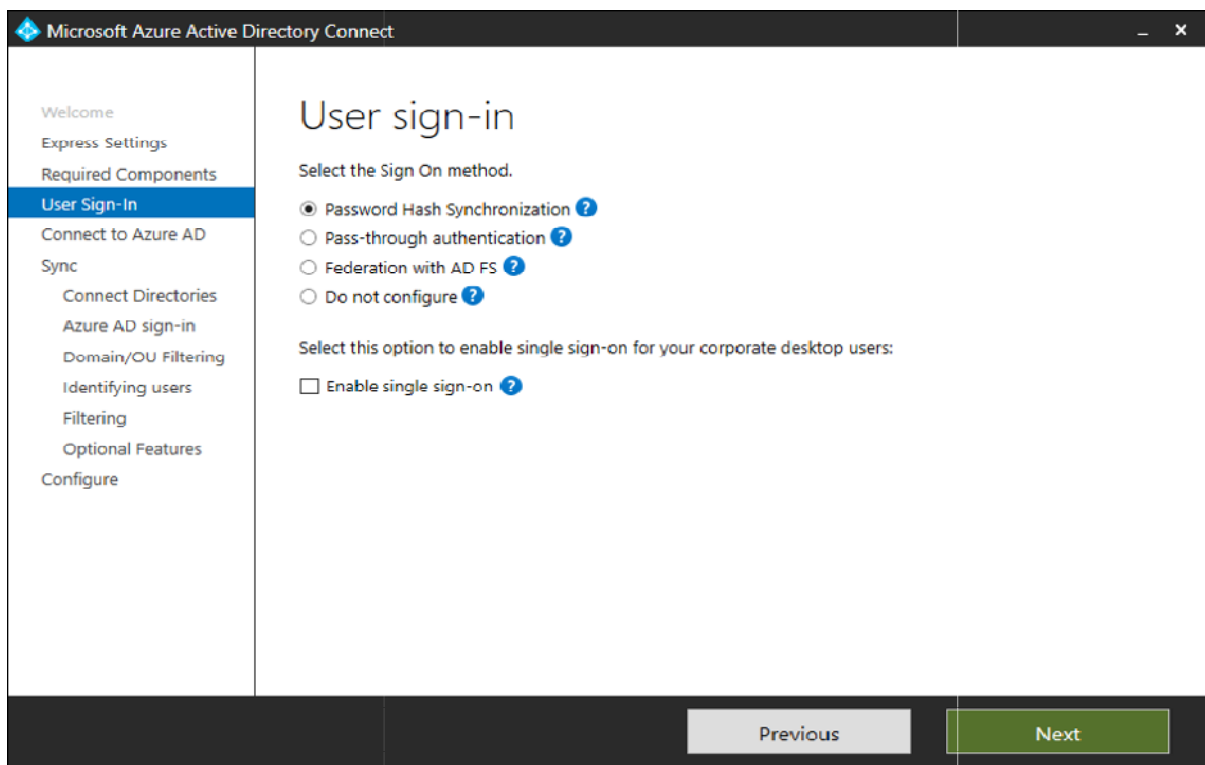
Password hash synchronization: A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD.

Pass-through authentication: A sign-in method that allows users to use the same password on-premises and in the cloud, but doesn't require the additional infrastructure of a federated environment.

Federation integration: Federation is an optional part of Azure AD Connect and can be used to configure a hybrid environment using an on-premises AD FS infrastructure. It also provides AD FS management capabilities such as certificate renewal and additional AD FS server deployments.



<Customer> can use custom settings which is available in Azure AD Connect Express settings for selecting sign on method to users.



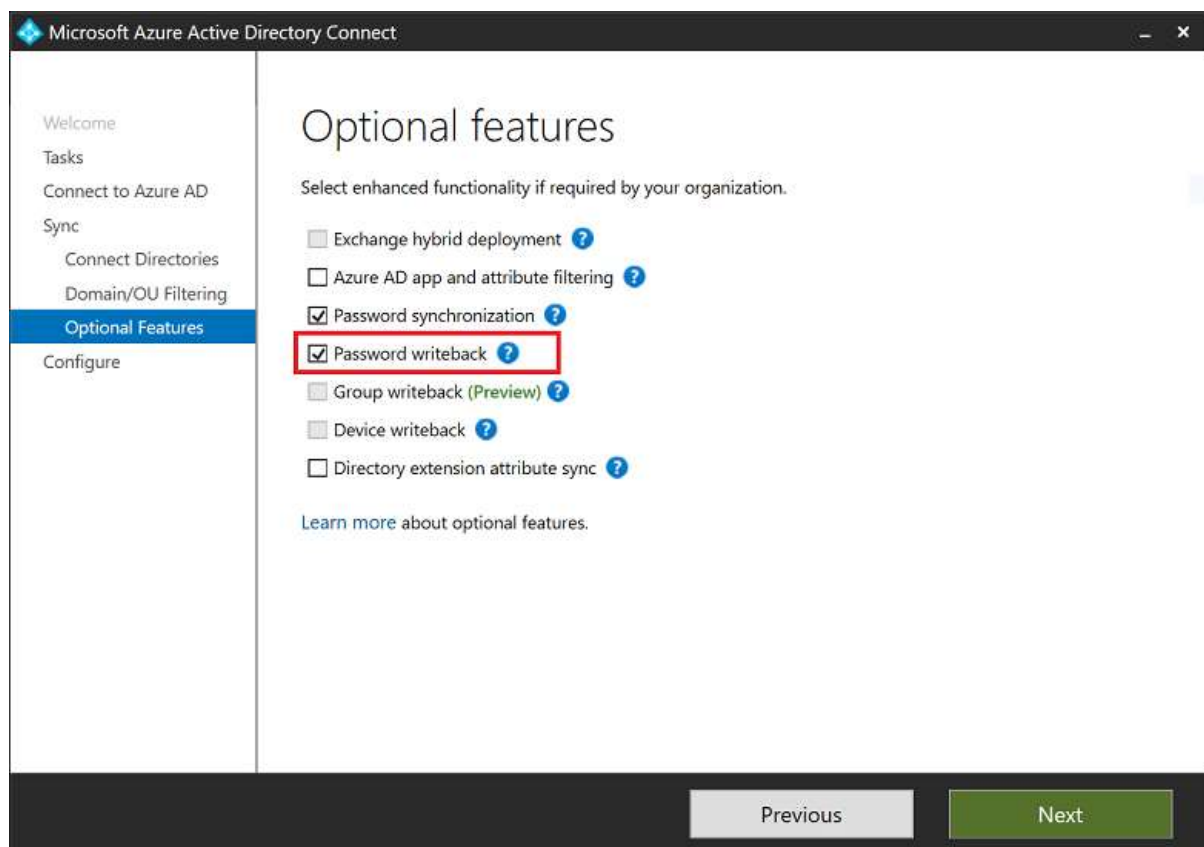
If <customer> decide to use Federation with Active Directory Federation Services (AD FS), <customer> can optionally set up password hash synchronization as a backup in case <customer> AD FS infrastructure fails.

Below table shows the parameters that are required for choosing Sign-On method to <customer> user's sign-in

Parameter	Value
Select Sign on method	<customer specified Sign-On method> <ul style="list-style-type: none">• Password hash synchronization• Pass-through authentication• Federation with AD FS• Do not configure
Enable Single Sign on	<customer specified> <ul style="list-style-type: none">• YES/NO

5.3 Enable password writeback:

<Customer> can make use of configuration options in Azure AD Connect is for password writeback. When this option is enabled, password change events cause Azure AD Connect to synchronize the updated credentials back to the on-premises AD DS environment.

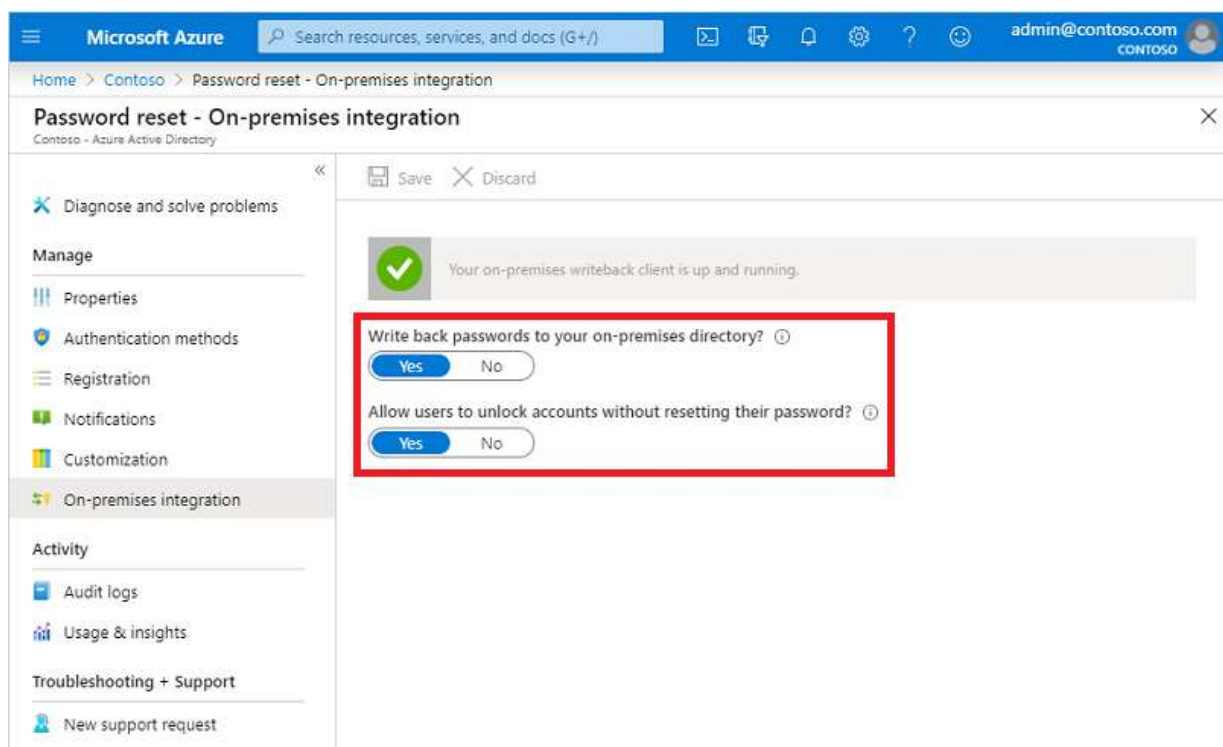


5.4 Enable password writeback for SSPR:

With password writeback enabled in Azure AD Connect, <customer> can configure Azure AD SSPR for writeback. When <customer> enable SSPR to use password writeback, users who change or reset their password have that updated password synchronized back to the on-premises AD DS environment as well.

Setting the option for **Write back passwords to <customer> on-premises directory** to Yes.

Setting the option for **Allow users to unlock accounts without resetting their password** to Yes.



6. Monitoring RBAC Activity Logs:

<Customer> can view activity logs for Azure RBAC changes

<Customer> can view the information about Azure role-based access control (Azure RBAC) changes, such as for auditing or troubleshooting purposes. Anytime someone makes changes to role assignments or role definitions within <customer> subscriptions, the changes get logged in Azure Activity Logs <Customer> can view the activity logs to see all the Azure RBAC changes for the past 90 days.

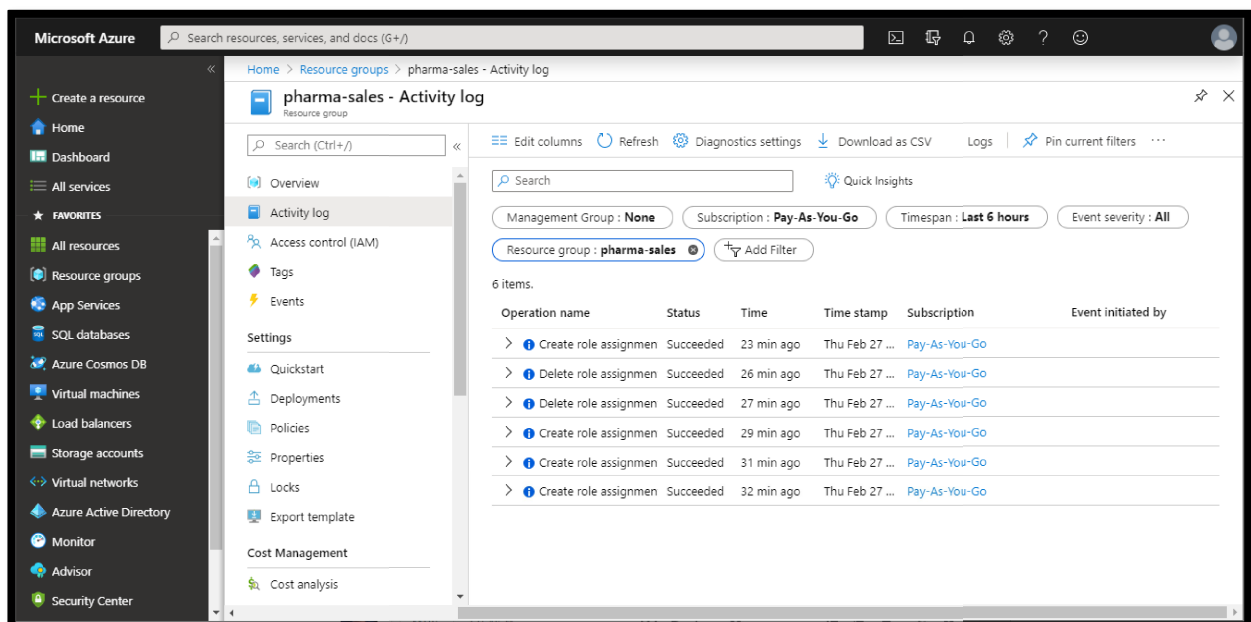
Operations that are logged

Here are the Azure RBAC-related operations that are logged in Activity Log:

- Create role assignment
- Delete role assignment
- Create or update custom role definition
- Delete custom role definition

Azure portal

The screenshot below shows role assignment operations in the activity log. It also includes an option to download the logs as a CSV file.

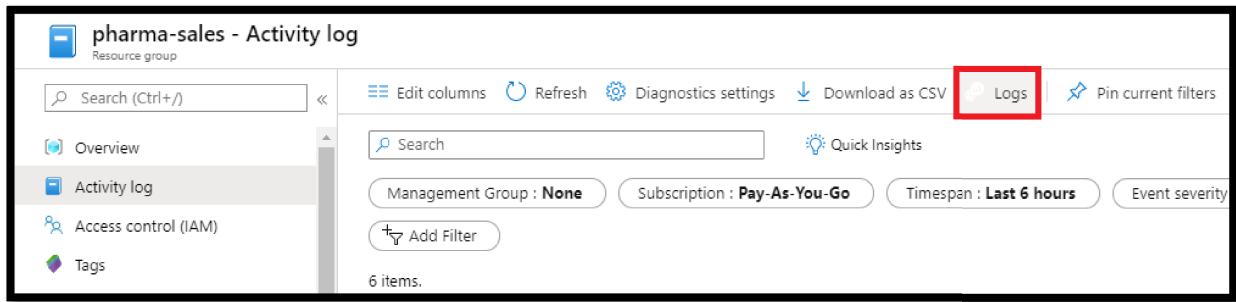


Azure Monitor logs

Azure Monitor logs is tool where <customer> can use to collect and analyze Azure RBAC changes for all the <customer> Azure resources.

Azure Monitor logs has the following benefits:

- Write complex queries and logic
- Integrate with alerts, Power BI, and other tools
- Save data for longer retention periods
- Cross-reference with other logs such as security, virtual machine, and custom



Optionally <customer> can use the Azure Monitor Log Analytics to query and view the logs.

Below table shows some of the Azure RBAC-related operations alerts that are logged in Activity Log for <customer> activity log changes.

Built-In Signals	Severity	Event Level	Recommended <customer> event level	Granularity period
Custom Role Creation	<customer specified>	<customer specified>	<customer specified>	<customer specified>
Custom Role Deletion	<customer specified>	<customer specified>	<customer specified>	<customer specified>
Custom Role modification update	<customer specified>	<customer specified>	<customer specified>	<customer specified>

7. Azure Policy:

Below table show some of the azure built in policies for <customer> cloud IAM:

Policy Assignment Name	Enforcement status	Policy Type	Description
Resource Policy Contributor	Allow/Deny	Build-In	Owner has full rights. Both Contributor and Reader have access to all read Azure Policy operations. Contributor may trigger resource remediation, but can't create definitions or assignments.
deployifNotExists	Allow	Build-In	The managed identity of a deployIfNotExists policy assignment needs enough permissions to create or update resources included in the template.

8. Illustrative Design:

