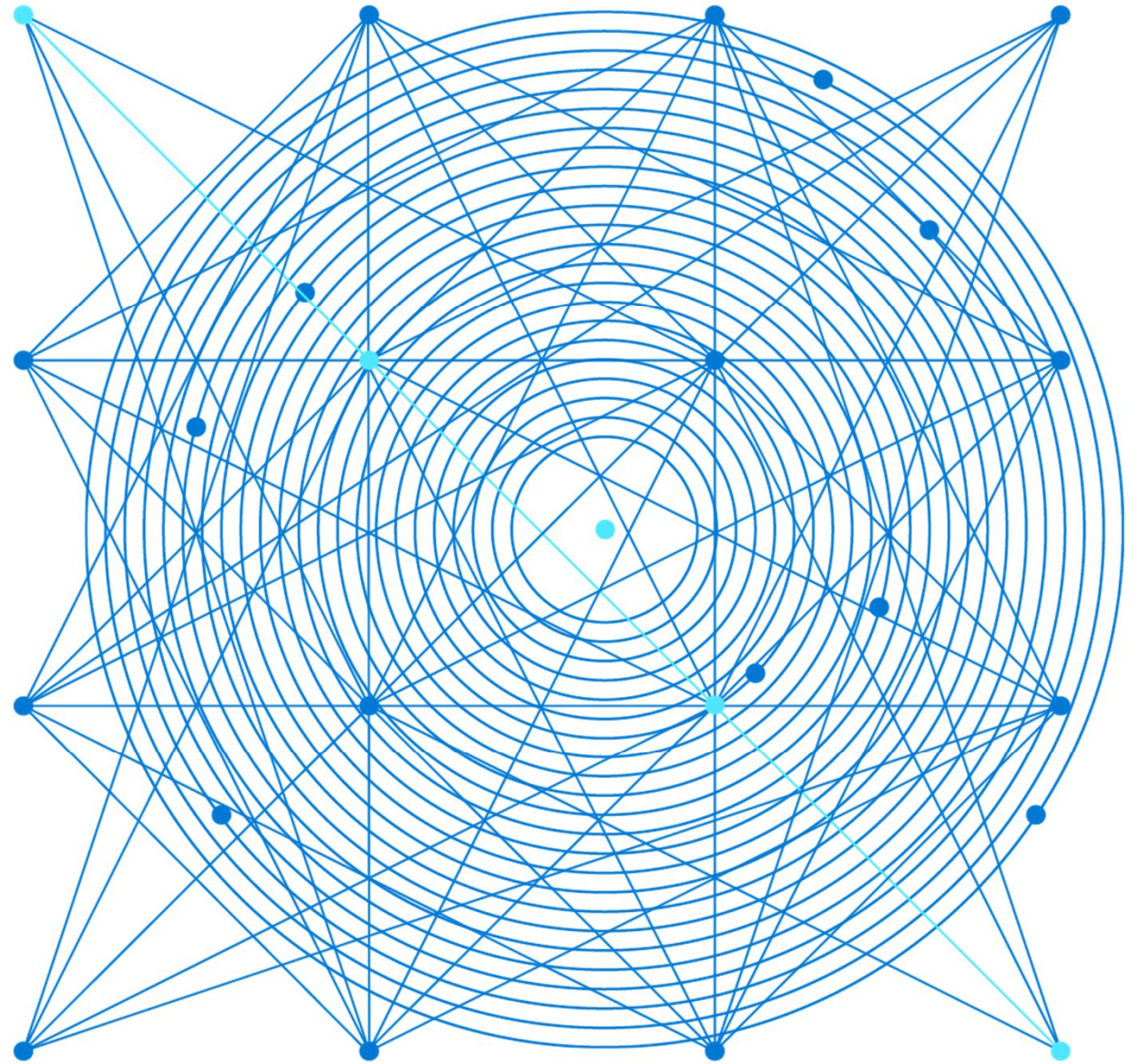


AZ-303: Microsoft Azure Architect Technologies



Module 1: Implement Azure Active Directory

Azure Active Directory, Custom Domains, Identity Protection, and Conditional Access

Learning Objectives

You will learn the following concepts:

- Overview of Azure Active Directory
- Create Management Groups, Subscriptions, and Resource Groups
- Users and Groups
- Domains and Custom Domains
- Azure AD Identity Protection
- Implement Conditional Access
- Configure Fraud Alerts for MFA
- Configure Trusted IPs
- Configure Guest Users in Azure AD

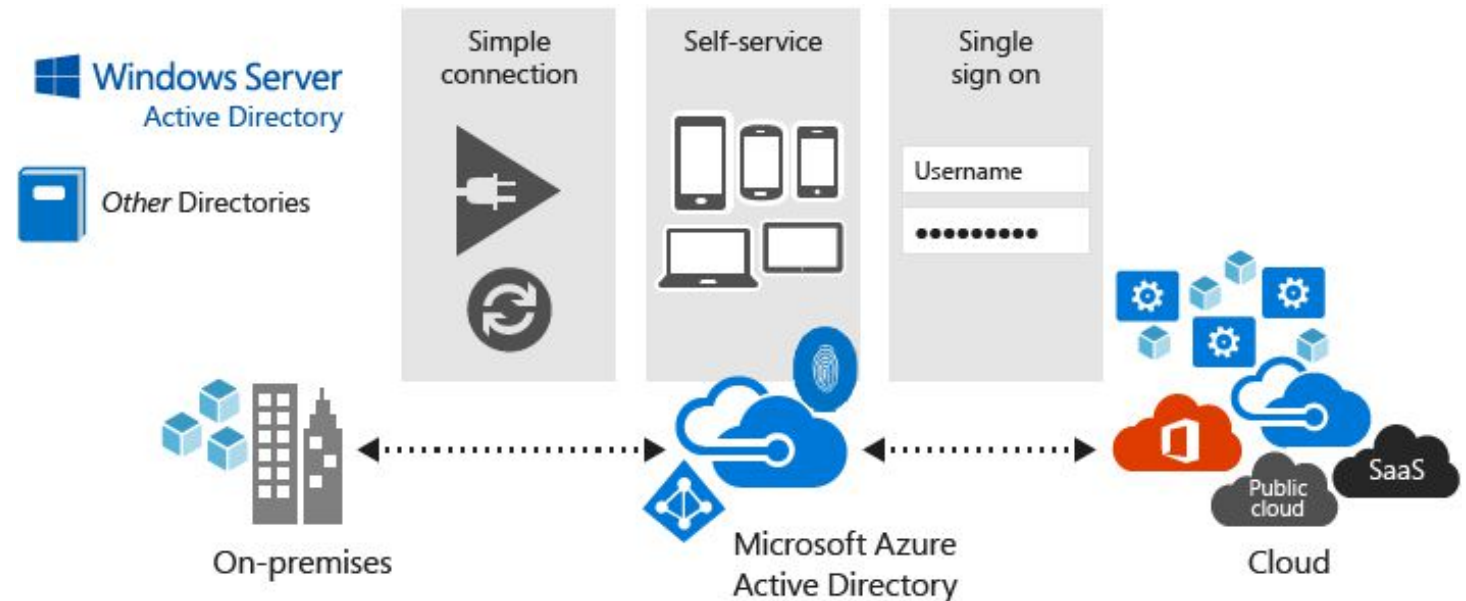


Overview of Azure Active Directory



Azure Active Directory (Azure AD)

- Multi-tenant cloud-based directory and identity management
- Provides single sign-on access to cloud applications and resources
- Facilitates developing apps with a global scope
- Offers a full suite of identity management capabilities:
 - Self-service password and group management
 - Privileged account management
 - Role-based access control
 - App usage monitoring
 - Security monitoring
 - Device Registration
 - Alerting
 - Multi-Factor Authentication (MFA)



Azure AD Concepts

Concept	Description
Identity	An object that can be authenticated.
Account	An identity that has data associated with it.
Azure AD Account	An identity created through Azure AD or another Microsoft cloud service.
Azure tenant	A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription.
Azure AD directory	Each Azure tenant has a dedicated and trusted Azure AD directory.
Azure subscription	Used to pay for Azure cloud services.

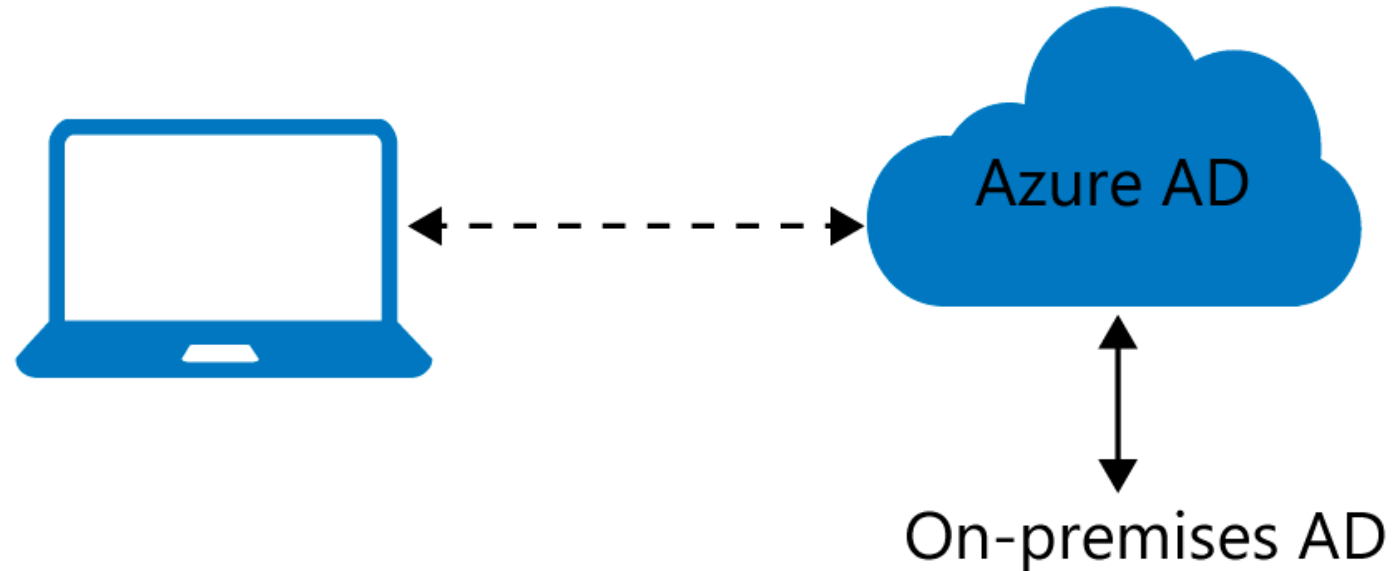
Azure AD Join

Benefits of AD Join:

- Single-sign-on (SSO)
- Enterprise compliant roaming
- Access to Microsoft Store for Business
- Windows Hello
- Seamless access to on-premises resources

Connection options:

- Registering
- Joining



Devices in Azure AD

Azure AD registered

Devices that are Azure AD registered are signed in with a personal Microsoft account or another local account.

- Windows 10
- iOS
- Android
- MacOS

Azure AD joined

Devices that are Azure AD joined are owned by an organization and are signed in with an Azure AD account belonging to that organization. They exist only in the cloud.

- Windows 10
- Windows Server 2019 Virtual Machines running in Azure (Server core is not supported)

Hybrid Azure AD joined

Devices that are hybrid Azure AD joined are owned by an organization and are signed in with an Active Directory Domain Services. They exist in the cloud and on-premises.

- Windows 7, 8.1, or 10
- Windows Server 2008 or newer

Create Management Groups, Subscriptions, and Resource Groups



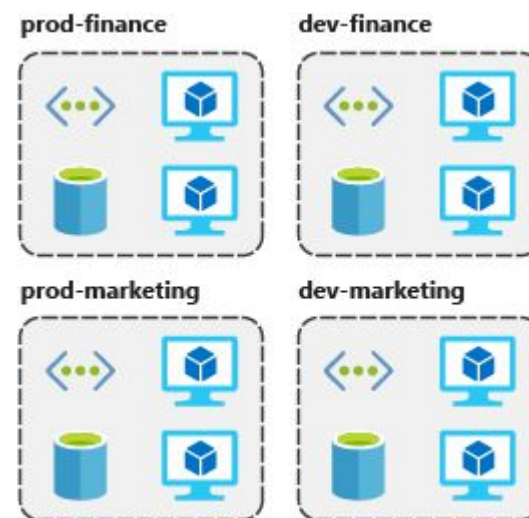
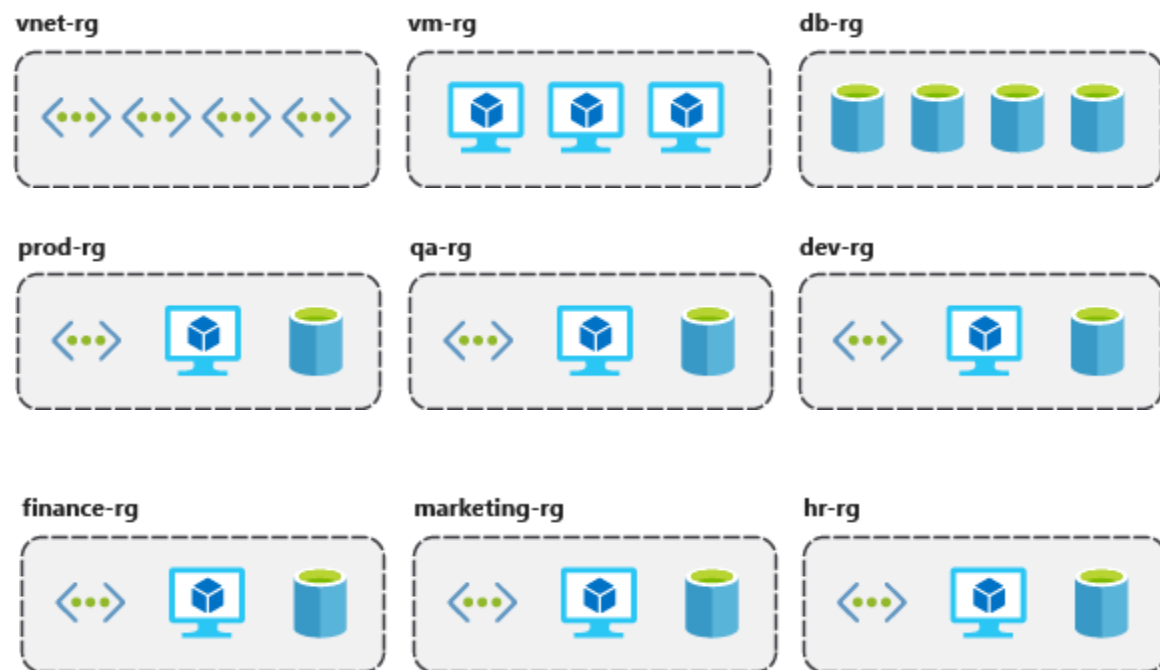
Resource Groups

- A resource groups is a fundamental concept of the Azure platform
 - Serves as a logical grouping of resources
 - Ties to resource life cycle
 - Can't be nested
- Each resource must belong to a resource group
- Most resources can be moved between resource groups



Resource Group Organization (1 of 2)

- Consistent naming convention
- Organizing principles

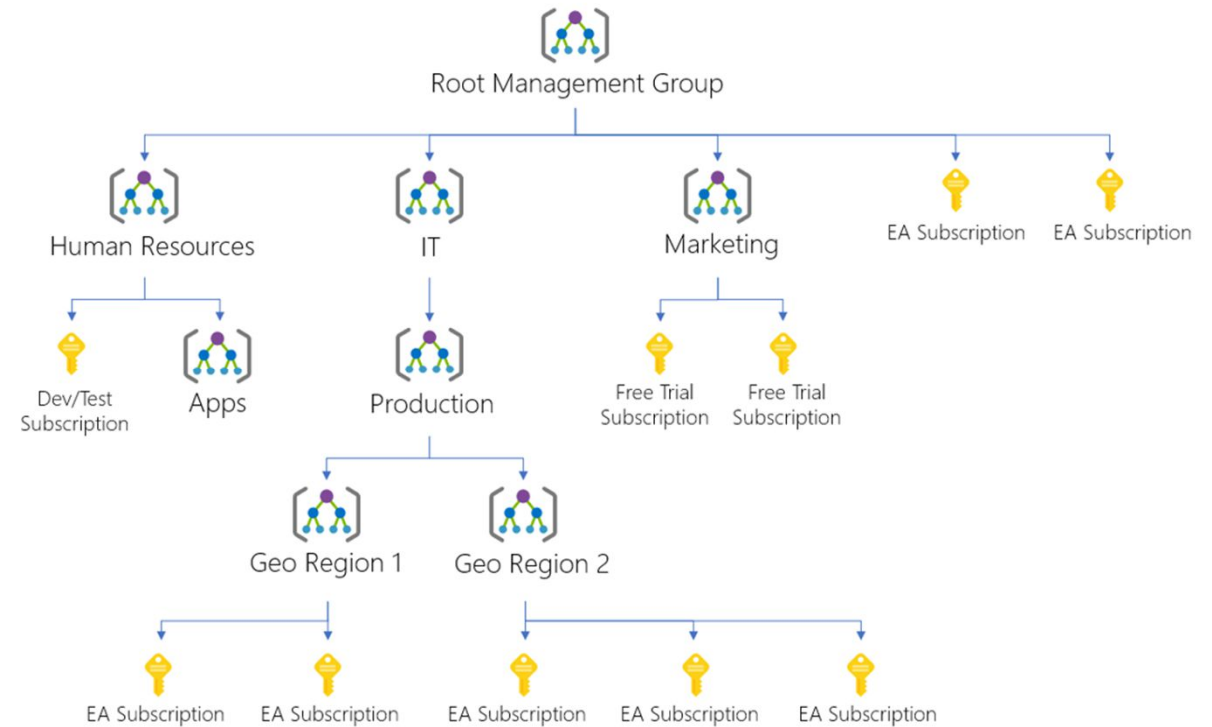


Resource Group Organization (2 of 2)

- Organizing for authorization
- Organizing for life cycle
- Organizing for billing

Management Groups

- Provides a level of scope above subscriptions
- Targeting of policies and spend budgets across subscriptions and inheritance down the hierarchies
- Compliance and cost reporting by organization (business/teams)



Subscriptions and Limits (Quotas)

Azure subscription and service limits:

- Microsoft Azure limits are also called quotas
- Some limits apply on the regional level

Managing limits:

- You can raise soft limits by raising an online customer support request at no charge



Subscription and Service General Limits

- Management group limits
- Subscription limits
- Resource group limits
- Template limits



Users and Groups



User Accounts

- To view the Azure AD users, access the **All users** blade
- Azure AD defines users in three ways:
 - Cloud identities
 - Directory-synchronized identities
 - Guest users

Microsoft Azure

Search resources, services, and docs (G+)

Home > Users | All users

Users | All users
Default Directory - Azure Active Directory

«

All users (Preview)

Deleted users



Password reset

User settings

Diagnose and solve problems

+ New user + New guest user ↑ Bulk create ↑ Bulk invite ↑ Bulk delete ↓ Download users ↻ Refresh 🔑 Reset password

Search users Add filters



	Name	User name	User type
<input type="checkbox"/>			Guest
<input type="checkbox"/>			Member

Create and Manage Users (1 of 3)

Adding users:

- Synchronizing users from Windows Server Active Directory
- Manually creating users by using the Azure portal

The screenshot displays the Microsoft Azure portal interface for managing users. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail shows 'All services > Default Directory > Users | All users (Preview)'. The main heading is 'Users | All users (Preview)' with the subtitle 'Default Directory - Azure Active Directory'. A left-hand sidebar contains navigation links: 'All users (Preview)', 'Deleted users', 'Password reset', 'User settings', 'Diagnose and solve problems', 'Activity', 'Sign-ins', 'Audit logs', and 'Bulk operation results'. The main content area features a toolbar with buttons: '+ New user' (highlighted with a red box), '+ New guest user', 'Bulk create', 'Bulk invite', 'Bulk delete', 'Download users', and 'Refresh'. Below the toolbar is a search bar with the text 'New user' and an 'Add filters' button. A table with two columns, 'Name' and 'User type', is visible. The 'Name' column contains a checkbox, a globe icon, and a text input field. The 'User type' column shows 'Guest' and 'Member'.

Name	User name	User type
<input type="checkbox"/> 	<input type="text"/>	Guest
<input type="checkbox"/> 	<input type="text"/>	Member

Create and Manage Users (2 of 3)

Creating a User...

New user
Default Directory

[Got feedback?](#)

☒ **Create user**
Create a new user in your organization.
This user will have a user name like
alice@callumbrightoutlook.onmicrosoft.com.
[I want to create users in bulk](#)

☐ **Invite user**
Invite a new guest user to collaborate with
your organization. The user will be emailed
an invitation they can accept in order to
begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

User name * ⓘ

Example: chris

@

▼

[The domain name I need isn't shown here](#)

Name * ⓘ

Example: 'Chris Green'

First name

Last name

Groups and roles

Groups

0 groups selected

Roles

User

Settings

Block sign in

YesNo

Usage location

▼

Job info

Job title

Department

Create

Create and Manage Users (3 of 3)

Inviting a user...

New user
Default Directory

[Got feedback?](#)

☐ Create user

Create a new user in your organization. This user will have a user name like `alice@callumbrightoutlook.onmicrosoft.com`.
[I want to create users in bulk](#)

☒ Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

Name ⓘ

Example: 'Chris Green'

Email address * ⓘ

Example: chris@contoso.com

First name

Last name

Personal message

Groups and roles

Groups

0 groups selected

Roles

User

Settings

Block sign in

YesNo

Usage location

Invite

©Microsoft Corporation
Azure

Group Accounts

You can define two different types of groups

- Security groups
- Office 365 groups

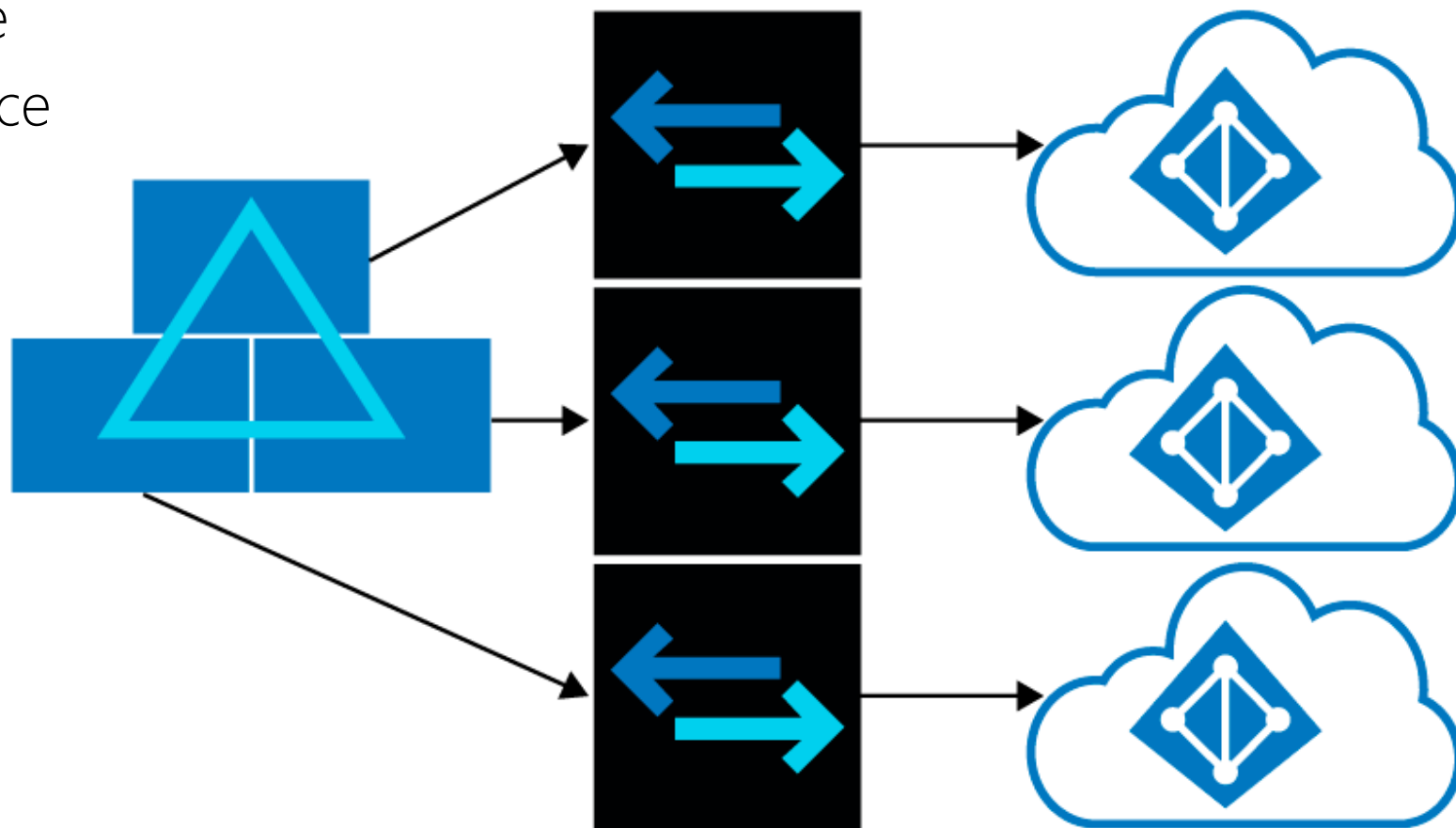
Adding members to groups:

- Assigned
- Dynamic user
- Dynamic device

Search groups		Add filters		
Name		↑↓	Group Type	Membership Type
<input type="checkbox"/>	MA Managers		Security	Assigned
<input type="checkbox"/>	VM Virtual Machine Administrators		Security	Assigned
<input type="checkbox"/>	VN Virtual Network Administrators		Security	Assigned

Managing Multiple Directories

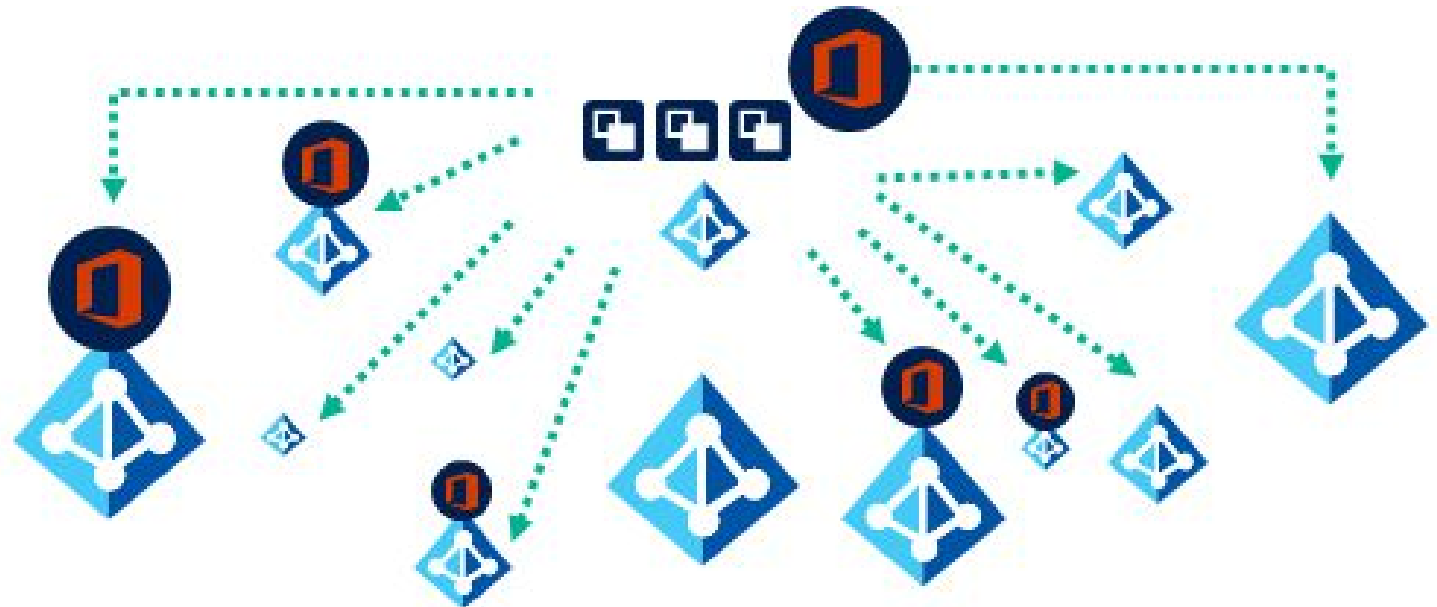
- Independence between tenants:
 - Resource independence
 - Administrative independence
 - Synchronization independence
- You can create multiple Azure AD tenants



Azure AD B2B and B2C (1 of 2)

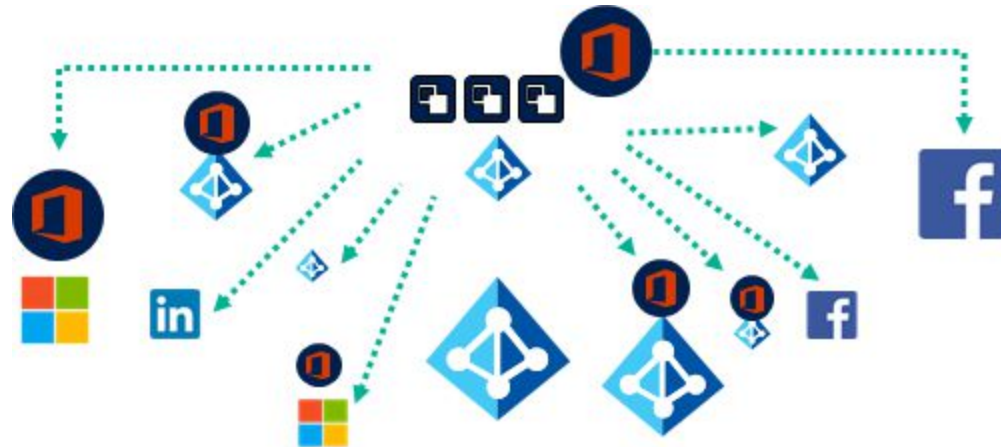
With Azure AD B2B:

- There is no external administrative overhead for your organization
- The partner uses their own identities and credentials; Azure AD is not required
- You don't need to manage external accounts or passwords
- You don't need to sync accounts or manage account lifecycles



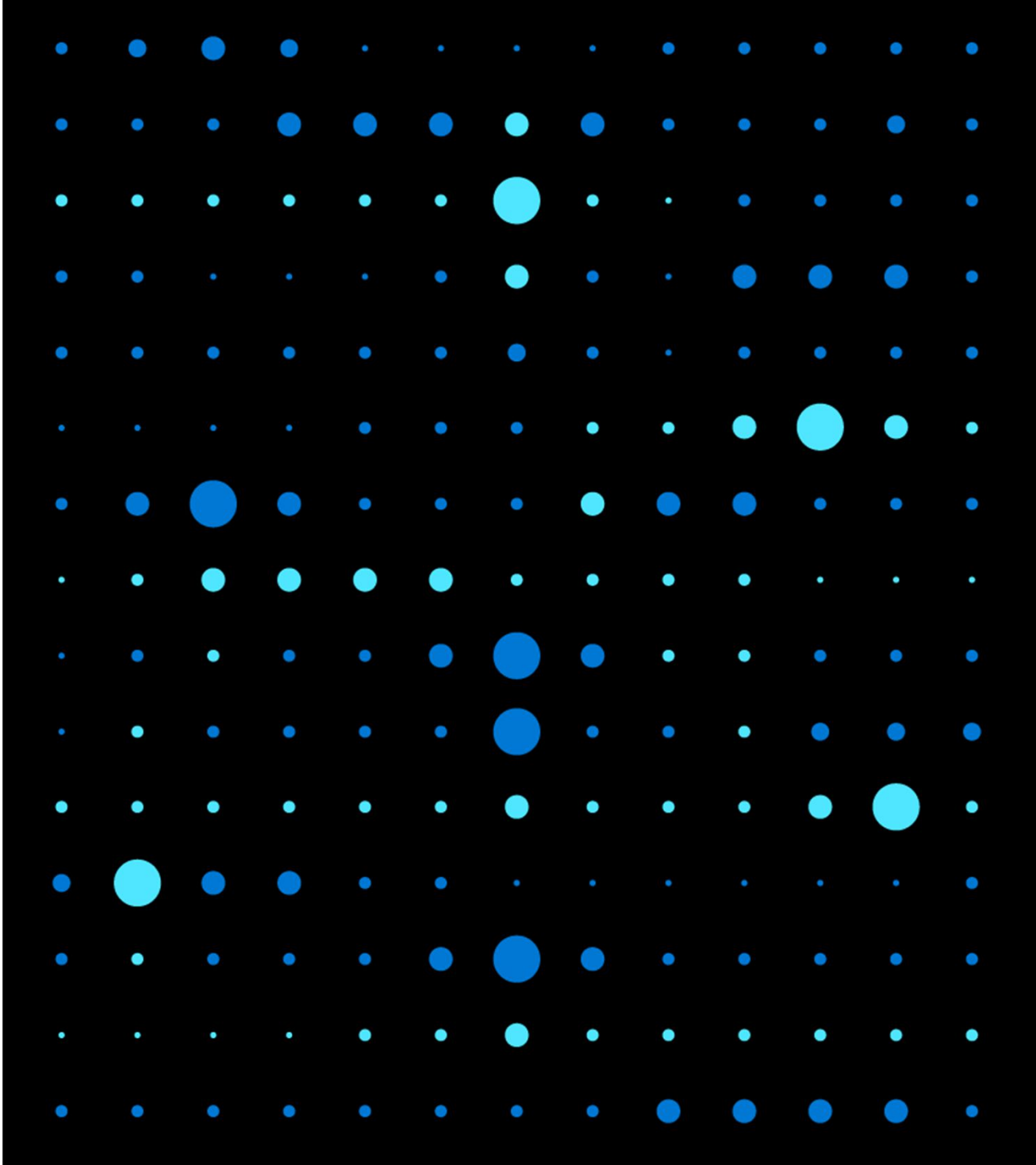
Azure AD B2B and B2C (2 of 2)

- With Azure AD B2C:
 - You invite users from other social media identity providers into your own organization tenant
 - User provisioning is done by the invited party
 - Standards-based authentication protocols are used including OpenID Connect, OAuth 2.0, and SAML.
 - There is integration support for most modern applications and commercial off-the-shelf software
 - The directory can hold 100 custom attributes per user
 - Identity verification and proofing can be performed by collecting user data, then passing it to a third party system for validation, trust scoring, and approval for user account creation



Demonstration: Users and Groups

- Explore Active Directory users and groups
- Explore PowerShell for group management



Domains and Custom Domains



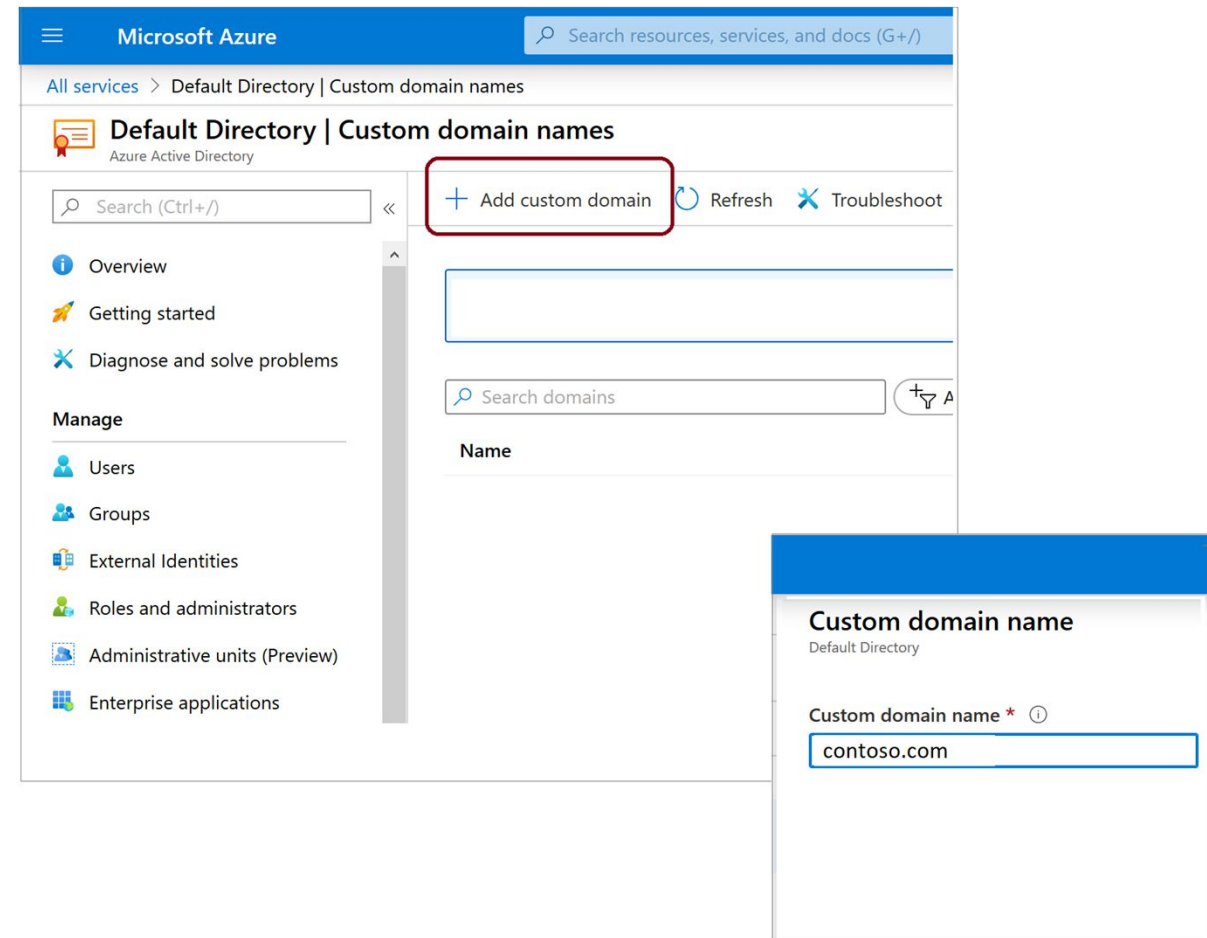
Domains and Custom Domains

Azure AD tenant domain names:

- Initial (mandatory) with onmicrosoft.com suffix
- Custom (optional)

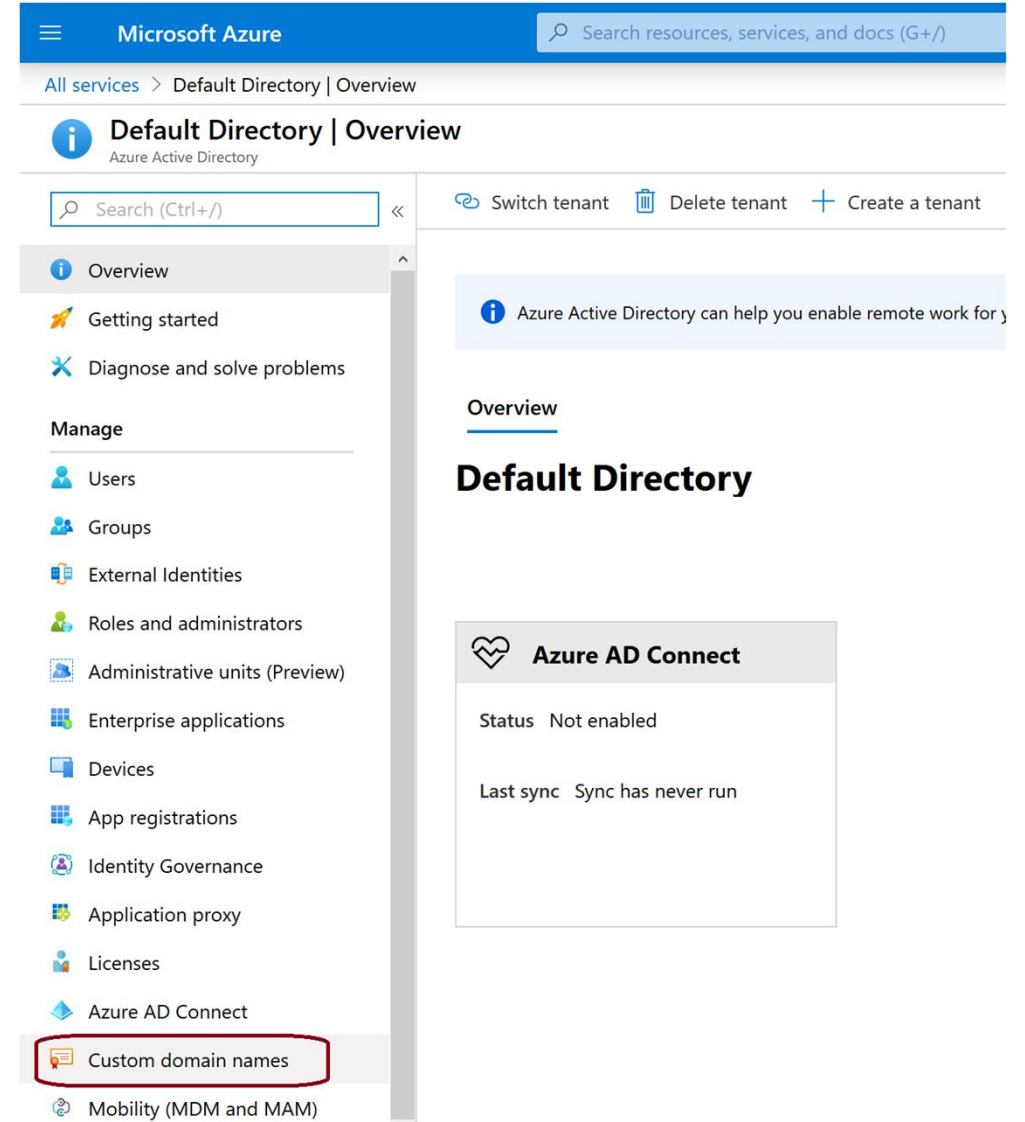
Domain name management:

- Requires global administrator privileges
- Domain names are globally unique
- Custom domain names require verification



Add a Custom Domain Name to Azure AD

After you create your Azure AD tenant, you can add a custom domain name using Azure portal






Verifying Custom Domain Names

- A custom domain name is initially in an unverified state
- To verify a custom domain, you must create a specific TXT or MX DNS record in the corresponding DNS zone

[All services](#) > [Default Directory](#) | [Custom domain names](#) > az303.contoso.com

az303.contoso.com
Custom domain name

 Delete |  Got feedback?

 To use az303.contoso.com with your Azure AD, create a new TXT record with your domain name registrar using the info below.

Record type
☒ TXT ☐ MX

Alias or host name

Destination or points to address

TTL

[Share these settings via email](#)
Verification will not succeed until you have configured your domain with your registrar as described above.

Azure AD Identity Protection



Azure Active Directory Identity Protection (1 of 2)

Protection allows organizations to accomplish three key tasks:

- Automate the detection and remediation of identity-based risks
- Investigate risks using data presented in the Azure portal
- Export risk detection data to third-party utilities for further analysis



Azure Active Directory Identity Protection (2 of 2)

- Risk detection and remediation
- Risk investigation
 - Risky users, risky sign-ins, risk detections

Risk detection type	Description
Atypical travel	Sign in from an atypical location based on the user's recent sign-ins.
Anonymous IP address	Sign in from an anonymous IP address (for example: Tor browser, anonymizer VPNs).
Unfamiliar sign-in properties	Sign in with properties we've not seen recently for the given user.
Malware linked IP address	Sign in from a malware linked IP address
Leaked Credentials	This risk detection indicates that the user's valid credentials have been leaked
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern



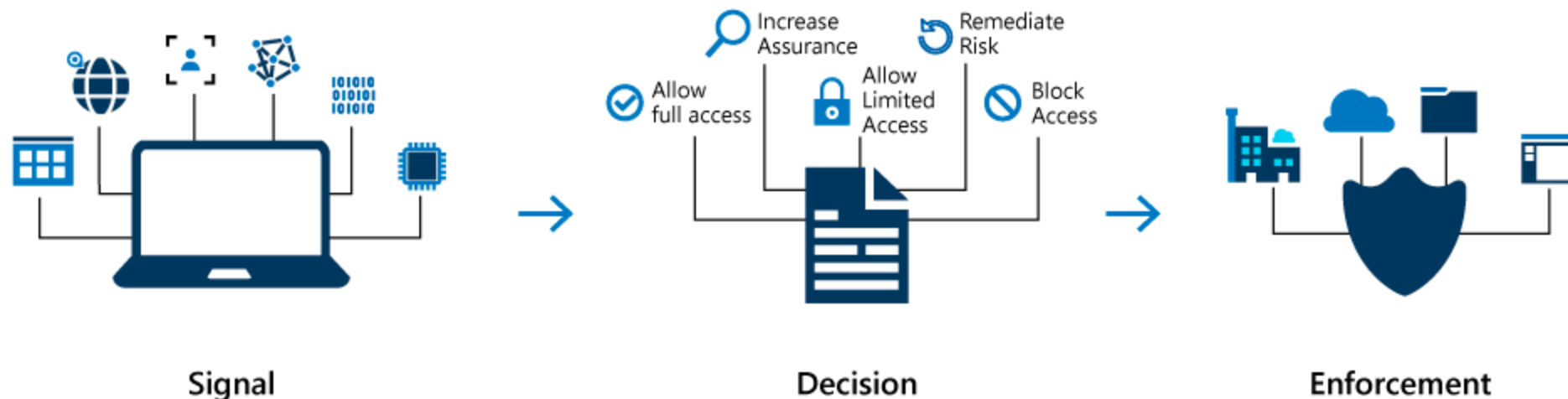
Implement Conditional Access



Overview of Conditional Access

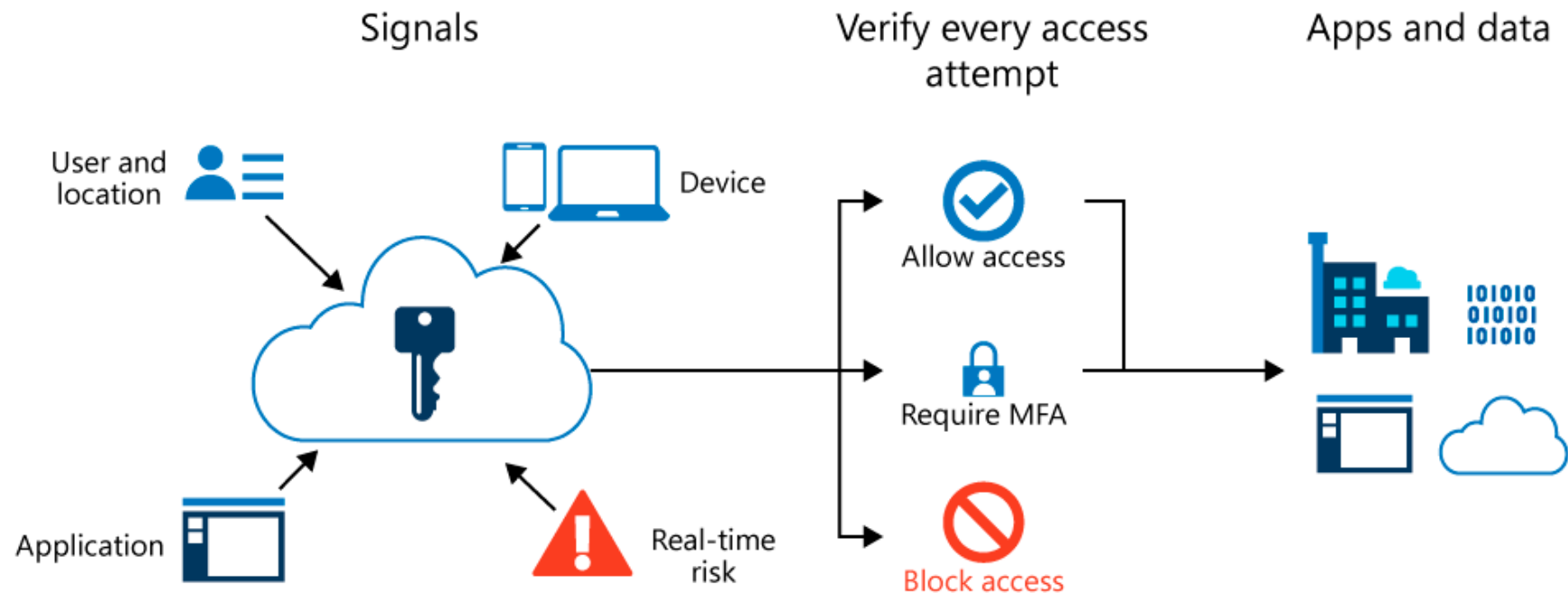
Administrators have two primary goals:

- To empower users to be productive wherever and whenever.
- To protect the organization's assets.
- Conditional Access policies at their simplest are if-then statements—If a user wants to access a resource, then they must complete a particular action first.
- Conditional Access allows you to apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.



Conditional Access and Azure Multi-Factor Authentication

- Provides two step authentication verification
- Lets you enforce controls on access to apps based on specific conditions:
 - Users and groups can be enabled for MFA to prompt for additional verification during sign-in.
 - Alternatively, Conditional Access policies can be used to define events or applications that require MFA.



Conditional Access – Signals and Decisions (1 of 2)

Common signals:

- User or group membership
- IP location information
- Device
- Application
- Real-time and calculated risk detection
- Microsoft Cloud App Security (MCAS)

Common decisions:

- Block access
- Grant access



Conditional Access – Signals and Decisions (2 of 2)

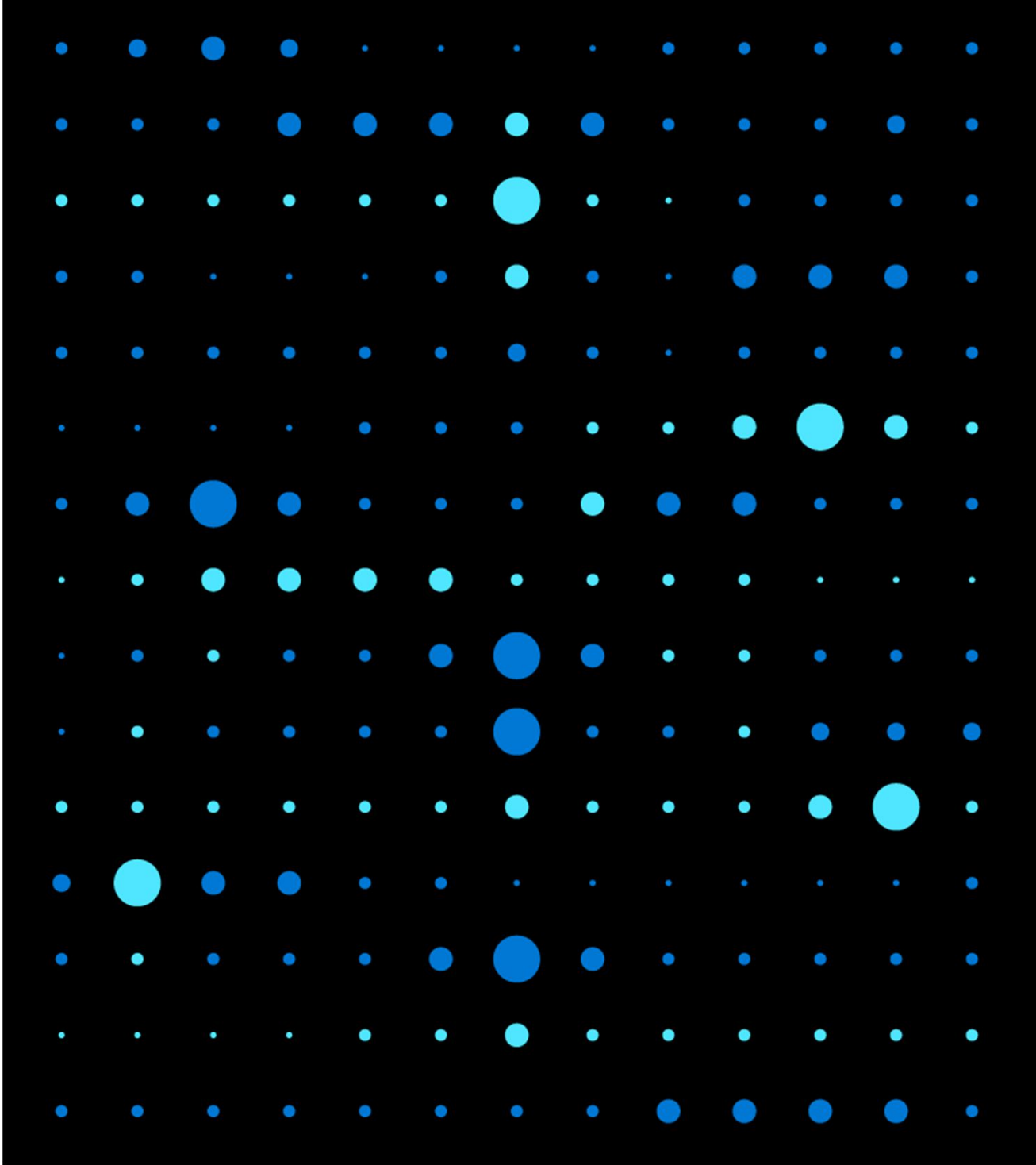
Common applied policies:

- Requiring multi-factor authentication for users with administrative roles
- Requiring multi-factor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Requiring trusted locations for Azure Multi-Factor Authentication registration
- Blocking or granting access from specific locations
- Blocking risky sign-in behaviors
- Requiring organization-managed devices for specific applications



Demonstration: Conditional Access Azure MFA

- Create a conditional access policy
- Configure conditions for multifactor authentication
- Test Azure multifactor authentication



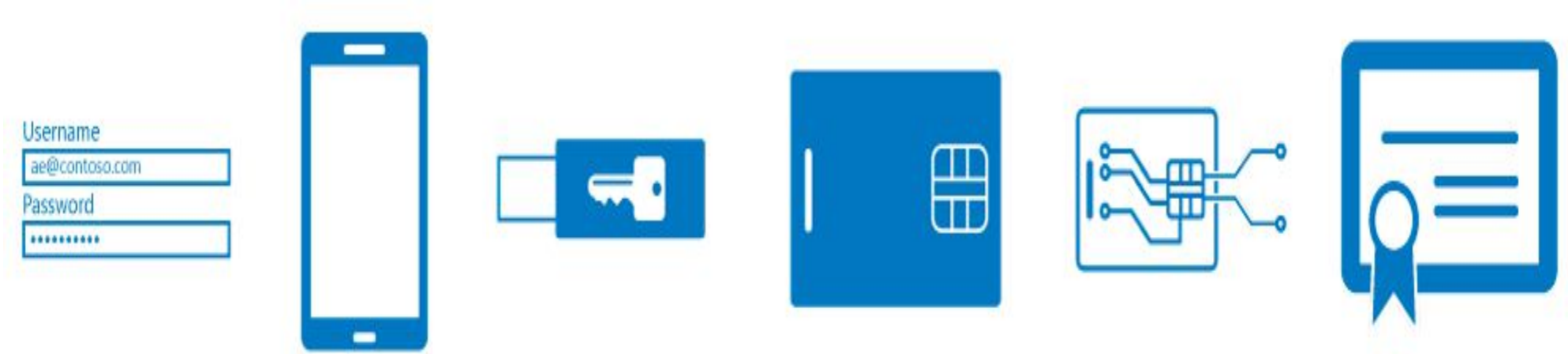
Configure Multi-Factor Authentication



Multi-Factor Authentication (1 of 2)

Azure Multifactor Authentication (MFA) methods:

- Something you know, typically a password
- Something you have, such as a trusted device that is not easily duplicated, like a phone or hardware key
- Something you are - biometrics like a fingerprint or face scan



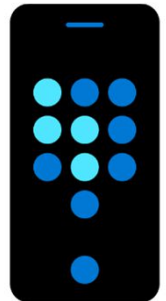
Multi-Factor Authentication (2 of 2)

Available verification methods:

- Microsoft Authenticator app
- OATH hardware token
- SMS

Authentication methods:

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



Self-Service Password Reset (1 of 2)

- Enabling **Self-Service Password Reset** (SSPR) gives the users the ability to bypass the helpdesk and reset their own passwords
- Three options of Password reset properties:
 - None
 - Selected
 - All

Password reset - **Properties**

MANAGE

 Properties

 Authentication methods

 Registration

 Notifications

 Save  Discard

Self service password reset enabled ⓘ

None

Selected

All

Select group

OnPremUsers

Self-Service Password Reset (2 of 2)

SSPR Authentication methods:

- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Password reset - Authentication methods
mitaric (Default Directory) - Azure Active Directory

Save Discard

Diagnose and solve problems

Manage

- Properties
- Authentication methods**
- Registration
- Notifications
- Customization
- On-premises integration

Activity

- Audit logs
- Usage & insights

Troubleshooting + Support

- New support request

Number of methods required to reset ⓘ

1 2

Methods available to users

- ☐ Mobile app notification
- ☐ Mobile app code
- ☒ Email
- ☒ Mobile phone
- ☐ Office phone
- ☒ Security questions

Number of questions required to register ⓘ

3 4 5

Number of questions required to reset ⓘ

3 4 5

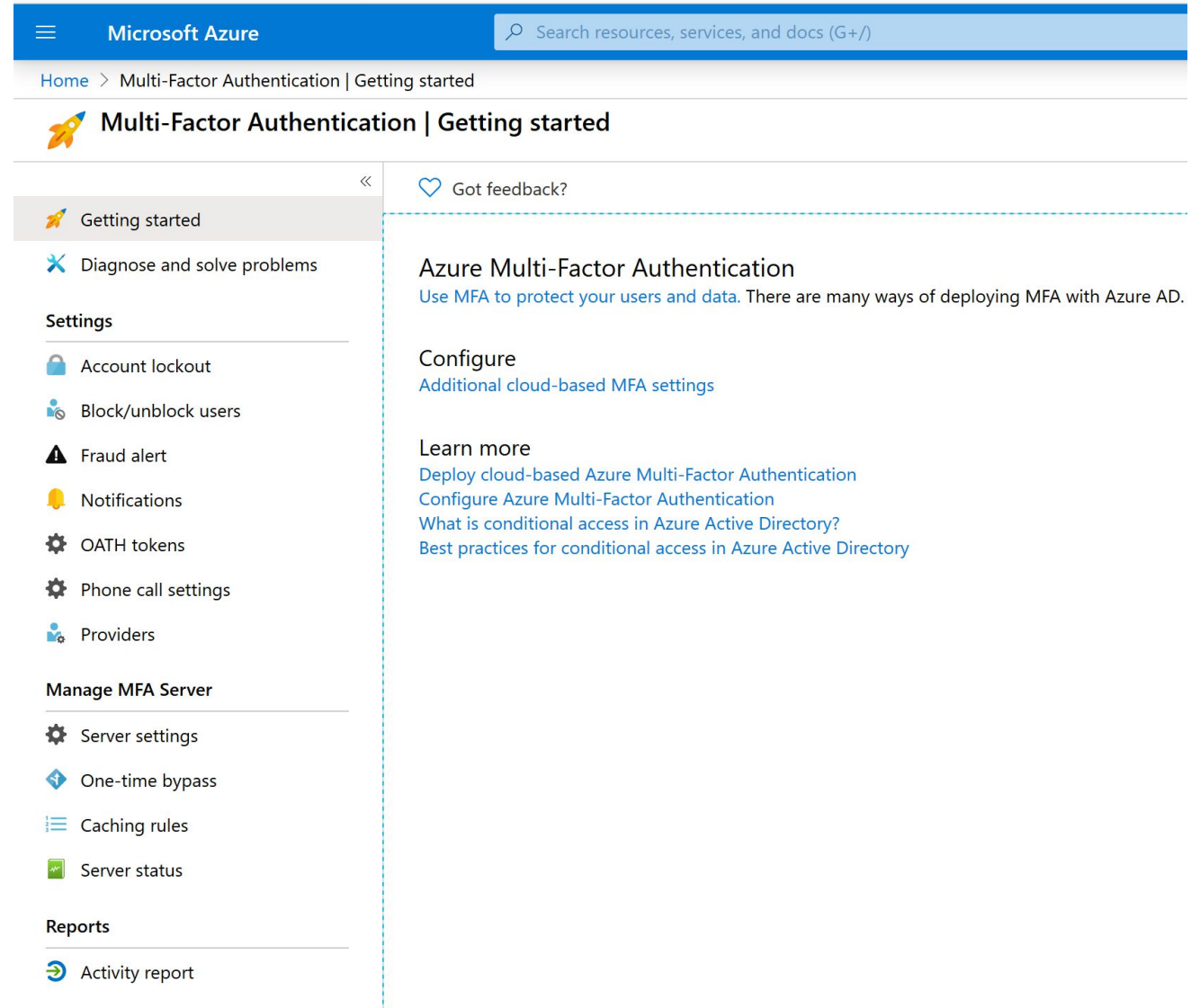
Select security questions

5 security questions selected

Configure Azure MFA Settings (1 of 2)

Settings (via the Azure portal):

- Access the Azure MFA settings by browsing to the **Azure AD** blade
- Select **Security**
- Select **MFA**
- Configure **Settings**



Configure Azure MFA Settings (2 of 2)

Feature	Description
Account lockout	Temporarily lock accounts in the multi-factor authentication service if there are too many denied authentication attempts in a row. This feature only applies to users who enter a PIN to authenticate.
Block/unblock users	Used to block specific users from being able to receive Multi-Factor Authentication requests. Any authentication attempts for blocked users are automatically denied. Users remain blocked for 90 days from the time that they are blocked.
Fraud alert	Configure settings related to users ability to report fraudulent verification requests
Notifications	Enable notifications of events from MFA Server.
OATH tokens	Used in cloud-based Azure MFA environments to manage OATH tokens for users.
Phone call settings	Configure settings related to phone calls and greetings for cloud and on-premises environments.
Providers	This will show any existing authentication providers that you may have associated with your account.

Reports for Azure Multi-Factor Authentication (1 of 2)

- Azure MFA provides reports available in the Azure portal
- View the MFA reports
- Azure AD Sign-ins Report
 - Was the sign-in challenged with MFA?
 - How did the user complete MFA?
 - Why was the user unable to complete MFA?
 - How many users are challenged for MFA?
 - How many users are unable to complete the MFA challenge?
 - What are the common MFA issues end users are running into?

The screenshot shows the Azure portal interface for Multi-Factor Authentication. The browser address bar displays the URL `https://portal.azure.com/#blade/Microsoft_AAD_I`. The page title is "Multi-Factor Authentication | Activity report". On the left sidebar, the "Reports" section is highlighted with a red box, and the "Activity report" option is selected. The main content area shows filters for "Time interval" (set to "Last 24 hours") and "Authentication mode" (set to "All"). Below these filters, a table header is visible with columns "Date/Time" and "Username", followed by the text "No results".

Reports for Azure Multi-Factor Authentication (2 of 2)

Report	Location	Description
Blocked User History	Azure AD > Security > MFA > Block/unblock users	Shows the history of requests to block or unblock users.
Usage and fraud alerts	Azure AD > Sign-ins	Provides information on overall usage, user summary, and user details; as well as a history of fraud alerts submitted during the date range specified.
Usage for on-premises components	Azure AD > Security > MFA > Activity Report	Provides information on overall usage for MFA through the NPS extension, ADFS, and MFA server.
Bypassed User History	Azure AD > Security > MFA > One-time bypass	Provides a history of requests to bypass Multi-Factor Authentication for a user.
Server status	Azure AD > Security > MFA > Server status	Displays the status of Multi-Factor Authentication Servers associated with your account.

Configure Trusted IPs



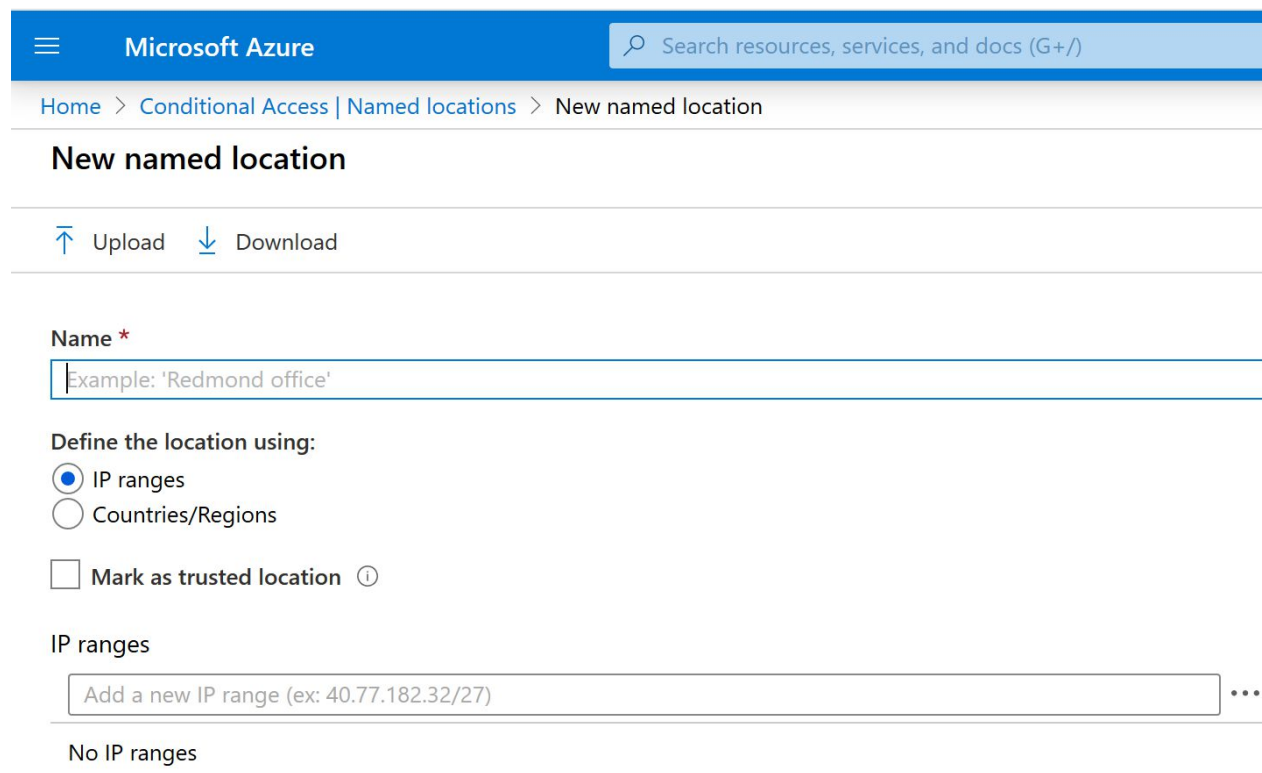
Azure AD Conditional Access Location Condition

- Azure AD enables single sign-on to devices, apps, and services from anywhere on the public internet.
- With the **location** condition of a Conditional Access policy, you can control access to your cloud apps based on the network location of a user.
- Common use cases for the location condition are:
 - Requiring multi-factor authentication for users accessing a service when they are off the corporate network.
 - Blocking access for users accessing a service from specific countries or regions.

Note: A **location** is a label for a network location that either represents a *named location* or *multi-factor authentication Trusted IPs*.

Named Locations

- Create logical groupings of IP address ranges or countries and regions
- Use groupings in the location condition of Conditional Access policies
- A named location has the following components:
 - Name
 - IP ranges
 - Mark as trusted location
 - Countries/regions
 - Include unknown areas



The screenshot shows the 'New named location' page in the Microsoft Azure portal. The top navigation bar is blue with the 'Microsoft Azure' logo and a search bar. Below the navigation bar, the breadcrumb trail reads 'Home > Conditional Access | Named locations > New named location'. The main heading is 'New named location'. Below this, there are 'Upload' and 'Download' buttons. The 'Name' field is required, indicated by a red asterisk, and contains the placeholder text 'Example: 'Redmond office''. Below the name field, the 'Define the location using:' section has two radio button options: 'IP ranges' (which is selected) and 'Countries/Regions'. There is also a checkbox for 'Mark as trusted location' with an information icon. The 'IP ranges' section has a text input field with the placeholder 'Add a new IP range (ex: 40.77.182.32/27)' and a three-dot menu icon to its right. At the bottom, there is a section for 'No IP ranges'.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Conditional Access | Named locations > New named location

New named location

Upload Download

Name *

Example: 'Redmond office'

Define the location using:

☒ IP ranges

☐ Countries/Regions

☐ Mark as trusted location ⓘ

IP ranges

Add a new IP range (ex: 40.77.182.32/27) ...

No IP ranges

Trusted IPs

- You can also configure IP address ranges representing your organization's local intranet in the multi-factor authentication service settings.
 - This feature enables you to configure up to 50 IP address ranges.
 - The IP address ranges are in CIDR format.
- If you have Trusted IPs configured, they show up as **MFA Trusted IPs** in the list of locations for the location condition.



Location Condition Configuration

When you configure the location condition, you have the option to distinguish between:

- Any location
- All trusted locations
- Selected locations

The screenshot displays the Microsoft Azure portal interface for configuring a new conditional access policy. The browser address bar shows the URL: https://portal.azure.com/#blade/Microsoft_AAD_IAM/ConditionalAccessBlade/Policies. The navigation pane on the left shows the path: Home > Conditional Access | Policies > New > Conditions > Locations. The main content area is divided into three panes: 'New', 'Conditions', and 'Locations'. The 'Locations' pane is highlighted with a red border and contains the following configuration options:

- Configure** (Info icon): A toggle switch set to 'Yes' (purple) with a 'No' option.
- Include** (underline) / **Exclude**: Radio button options for 'Any location' (selected), 'All trusted locations', and 'Selected locations'.
- Select** / **None**: A dropdown menu with a right arrow.

The 'New' pane shows a 'Name' field with the example text 'Device compliance app poli' and a red warning icon. The 'Conditions' pane shows a list of conditions: 'Sign-in risk' (Not configured), 'Device platforms' (Not configured), 'Locations' (Not configured), 'Client apps (Preview)' (Not configured), and 'Device state (Preview)' (Not configured). The 'Locations' condition is highlighted with a grey background.

Configure Guest Users in Azure AD



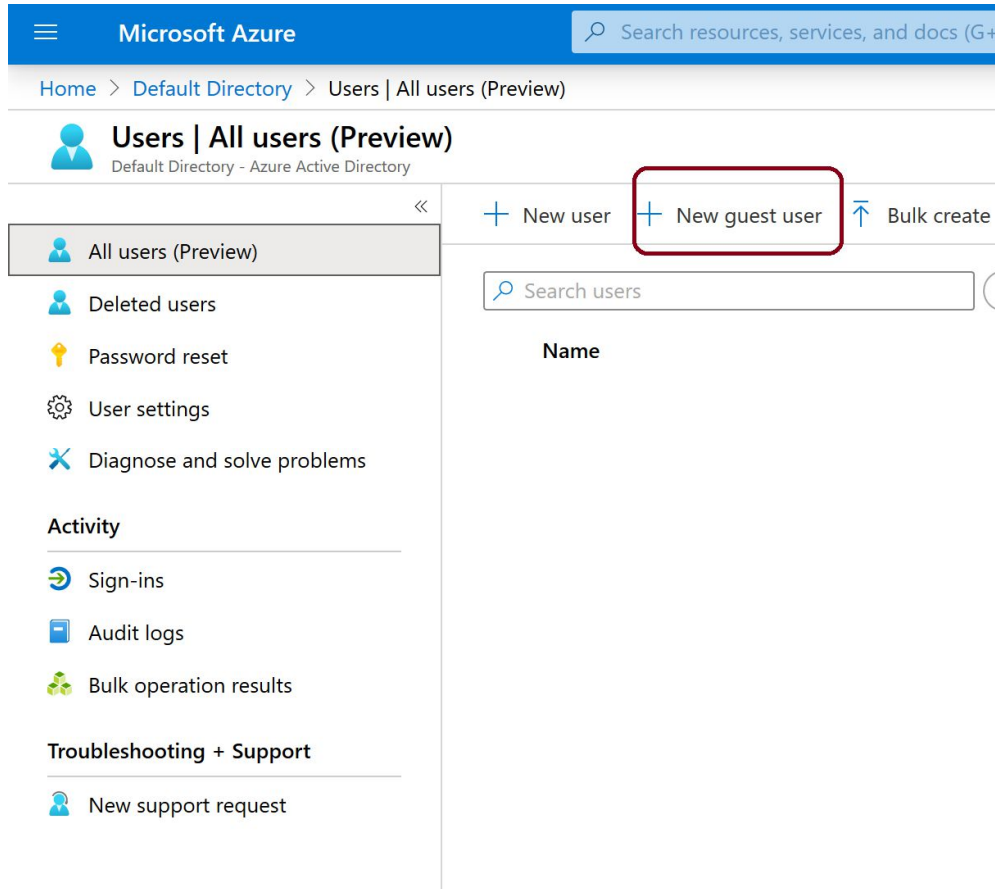
Prerequisites for Guest Users in Azure AD

- You can invite anyone to collaborate with your organization by adding them to your directory as a guest user.
- Guest users can sign in with their own work, school, or social identities.
- To test guest-related scenarios, you need
 - An Azure AD user with a role that allows creating user accounts
 - A valid email account

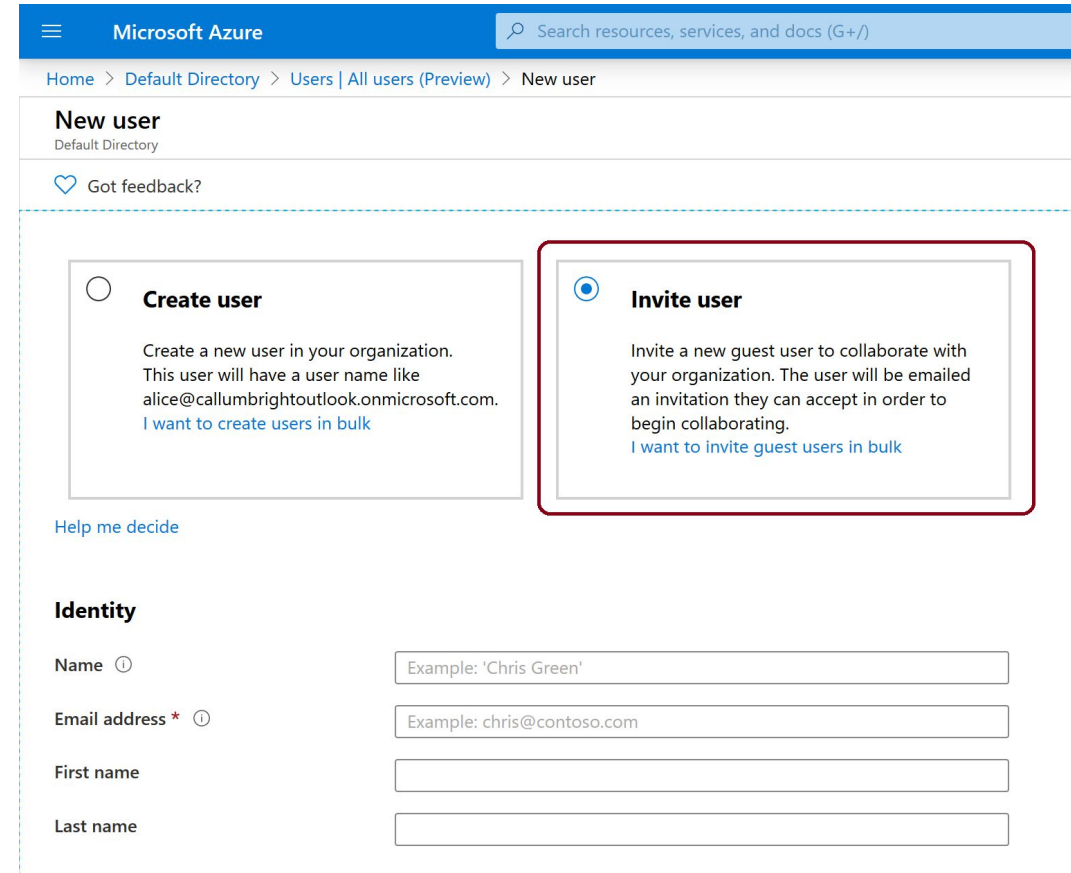


Add Guest Users to Azure AD

Sign into Azure portal and add a guest user



The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the path: Home > Default Directory > Users | All users (Preview). The main heading is 'Users | All users (Preview)' with a subheading 'Default Directory - Azure Active Directory'. On the left sidebar, there are links for 'All users (Preview)', 'Deleted users', 'Password reset', 'User settings', and 'Diagnose and solve problems'. The main content area shows a '+ New user' button, a '+ New guest user' button (highlighted with a red box), and a 'Bulk create' button. Below these buttons is a search bar labeled 'Search users' and a table header 'Name'.

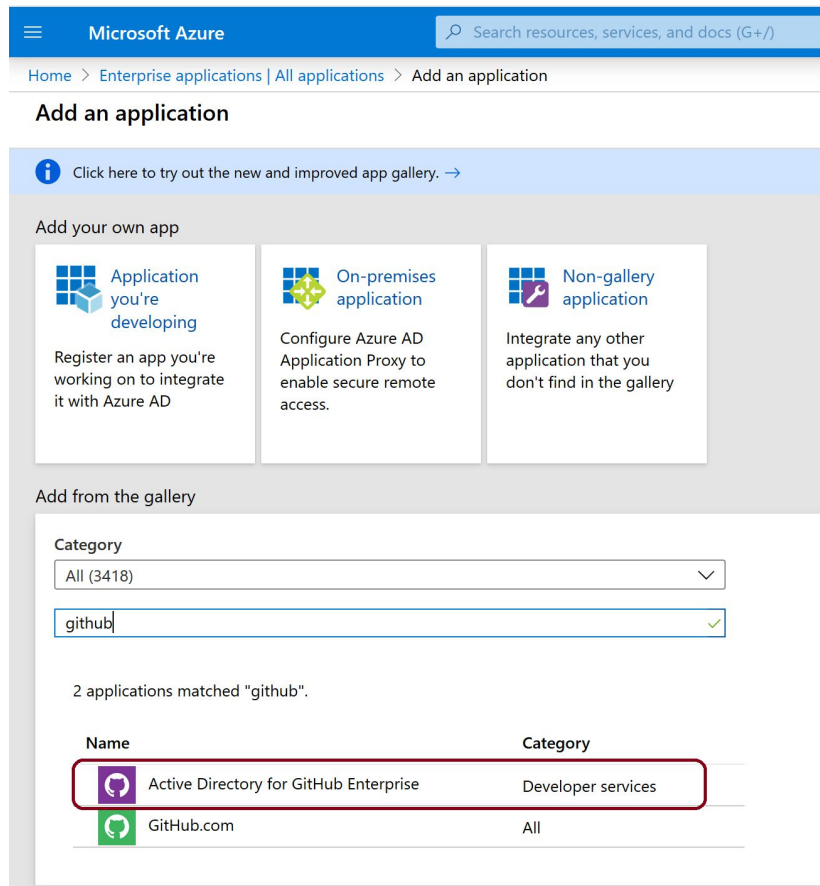


The screenshot shows the 'New user' page in the Microsoft Azure portal. The breadcrumb trail indicates the path: Home > Default Directory > Users | All users (Preview) > New user. The main heading is 'New user' with a subheading 'Default Directory'. Below the heading is a 'Got feedback?' link. The main content area has two options: 'Create user' and 'Invite user' (highlighted with a red box). The 'Create user' option includes a description: 'Create a new user in your organization. This user will have a user name like alice@callumbrightoutlook.onmicrosoft.com. I want to create users in bulk'. The 'Invite user' option includes a description: 'Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating. I want to invite guest users in bulk'. Below these options is a 'Help me decide' link. The 'Identity' section includes fields for 'Name' (with an example: 'Chris Green'), 'Email address' (with an example: 'chris@contoso.com'), 'First name', and 'Last name'.



Assign an App to a Guest User

Add the *Active Directory for GitHub Enterprise* app to your test tenant and assign the test guest user to the app.



Microsoft Azure

Search resources, services, and docs (G+I)

Home > Enterprise applications | All applications > Add an application

Add an application

Click here to try out the new and improved app gallery. →

Add your own app

- Application you're developing**
Register an app you're working on to integrate it with Azure AD
- On-premises application**
Configure Azure AD Application Proxy to enable secure remote access.
- Non-gallery application**
Integrate any other application that you don't find in the gallery

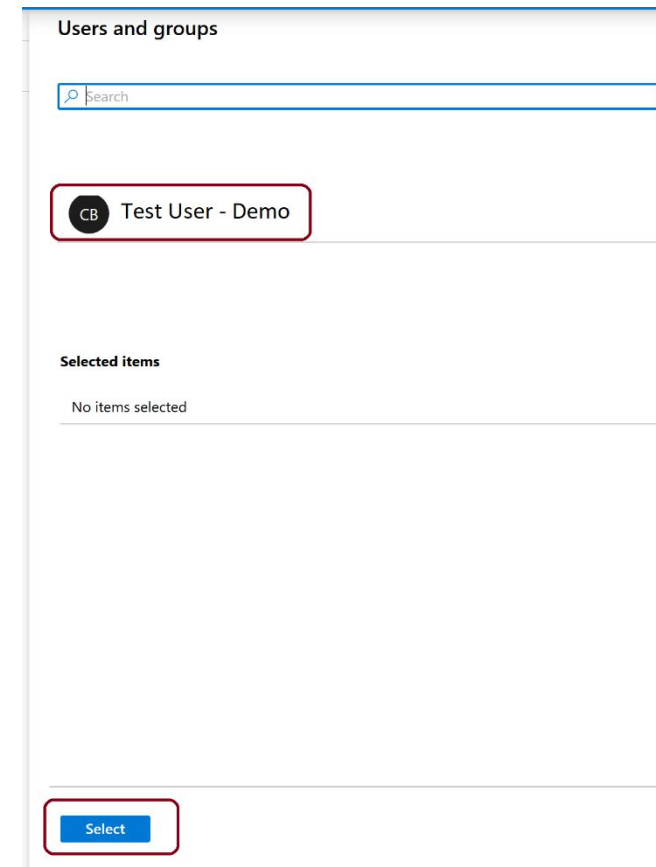
Add from the gallery

Category: All (3418)

Search: github

2 applications matched "github".

Name	Category
Active Directory for GitHub Enterprise	Developer services
GitHub.com	All



Users and groups

Search

Test User - Demo

Selected items

No items selected

Select



Accept the Guest User Invite

- Sign-in to your test guest user's email account
- In the inbox, locate the "*You're invited*" email
- In the email body, select **Get Started**
- Select **Accept Invitation**

Default Directory invited you to access applications within their organization



Microsoft Invitations on behalf of Default Directory <invites@microsoft.com>

If there are problems with how this message is displayed, click here to view it in a web browser.

Please only act on this email if you trust the organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Organization: Default Directory

Domain:

This message was provided by the sender and is not from Microsoft Corporation.



Message from
Default Directory:

“ Test message for guest user invite. ”

If you accept this invitation, you'll be sent to <https://myapps.microsoft.com/>

[Accept invitation](#)

Module Review Questions



Online Role-based training resources:

Microsoft Learn

<https://docs.microsoft.com/en-us/learn/>

Thank you.