

**FACILITAMOS LA
METAMORFOSIS DIGITAL
DE LAS ORGANIZACIONES**

**Identidad: Núcleo de la
seguridad en la nube**

izertis
Passion for Technology





Juan Jose Diaz Antuña

*Cloud Solutions Manager
Microsoft and AWS Product Owner en Izertis*



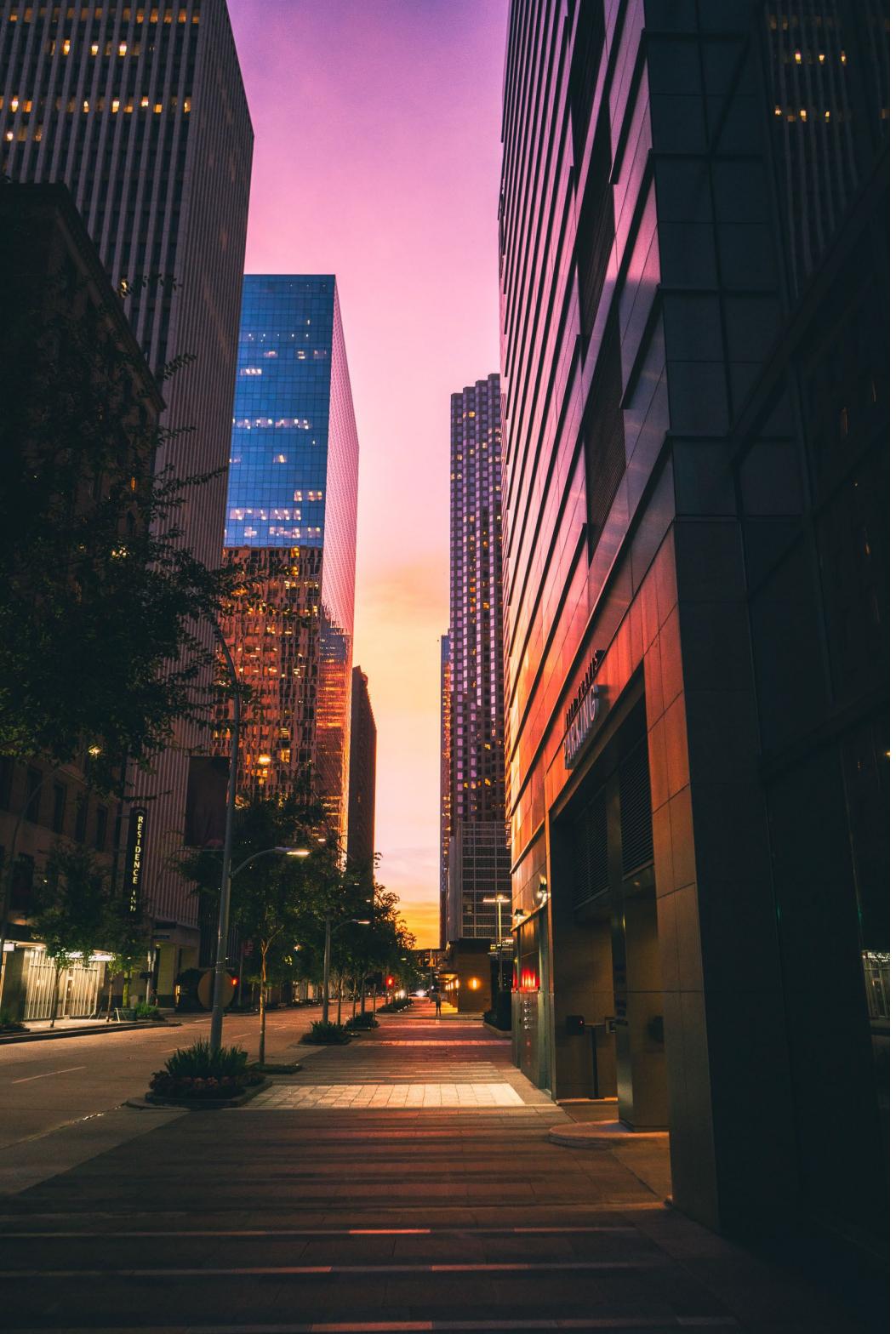
Introducción Identidad





¿Qué es la identidad en la tecnología de la información?

- La identidad digital es la información que identifica a alguien en línea.
- Las credenciales de inicio de sesión son la forma principal de autenticación de la identidad digital.
- La identidad digital es fundamental en la seguridad de la información.
- La autenticación multifactorial es una forma efectiva de proteger la identidad digital.



¿Por qué la identidad es clave en seguridad?

- La identidad es el núcleo de la seguridad digital
- La autenticación y autorización de identidad son críticos
- La identidad digital es vulnerable a ataques
- El robo de identidad es una amenaza constante



La gestión de identidad como medida de seguridad

- La gestión de identidad reduce el riesgo de brechas de seguridad
- La autenticación multifactorial es una herramienta eficaz
- La gestión de identidad aumenta la eficiencia y reduce los costos
- La gestión de identidad mejora la experiencia del usuario



Los desafíos de la gestión de identidad

- El manejo de grandes cantidades de datos es un desafío
- El equilibrio entre seguridad y experiencia del usuario
- El cumplimiento normativo es crucial
- La gestión de identidad debe ser escalable y flexible

¿A quien le suena esto?

The screenshot shows the Active Directory Users and Computers (ADUC) console. The left pane displays a tree view of the directory structure under 'adnfsrv4.lab.netapp.com'. The right pane shows a table titled 'Users 48 objects' with columns 'Name' and 'Type'. The table lists various security groups and user accounts, including 'Domain Computers', 'Domain Controllers', 'Domain Guests', 'Domain Users', 'Enterprise Admins', 'Group Policy Creator Owners', 'Group2', 'Guest', 'IUSR_ANT-CO', 'IWAM_ANT-CO', and 'krbtgt'. The 'Guest' account is highlighted.

Name	Type
Domain Computers	Security Group
Domain Controllers	Security Group
Domain Guests	Security Group
Domain Users	Security Group
Enterprise Admins	Security Group
Group Policy Creator Owners	Security Group
Group2	Security Group
Guest	User
IUSR_ANT-CO	User
IWAM_ANT-CO	User
krbtgt	User

The screenshot shows the 'Windows 2000 Configure Your Server' window. The title bar says 'Microsoft Windows 2000 Configure Your Server'. The main message area says 'You have successfully completed Windows 2000 Server Setup.' Below it, instructions say 'You can now configure this server. Select the first option if you have one server in your network. Select the second option if you have more than one server in your network.' Three radio button options are listed: 'This is the only server in my network.' (selected), 'One or more servers are already running in my network.', and 'I will configure this server later.' A 'Next' button is at the bottom right.



EntralID

Identidad como servicio adaptada al siglo XXI

Formas de llevar tu Identidad a la nube: EntraID

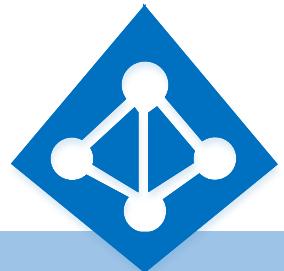
Password Hash Synchronization



EntraID Connect sync
with password hashes

Active Directory Domain Services

Pass-Through Authentication



EntraID Connect sync

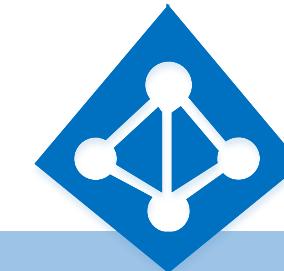
Authentication Agent

Active Directory Domain Services

EntraID hace la autenticación usando hashes de contraseña sincronizados

AD DS hace la autenticación vía agentes de autenticación que envían las peticiones a los controladores de dominio.

Federated Authentication



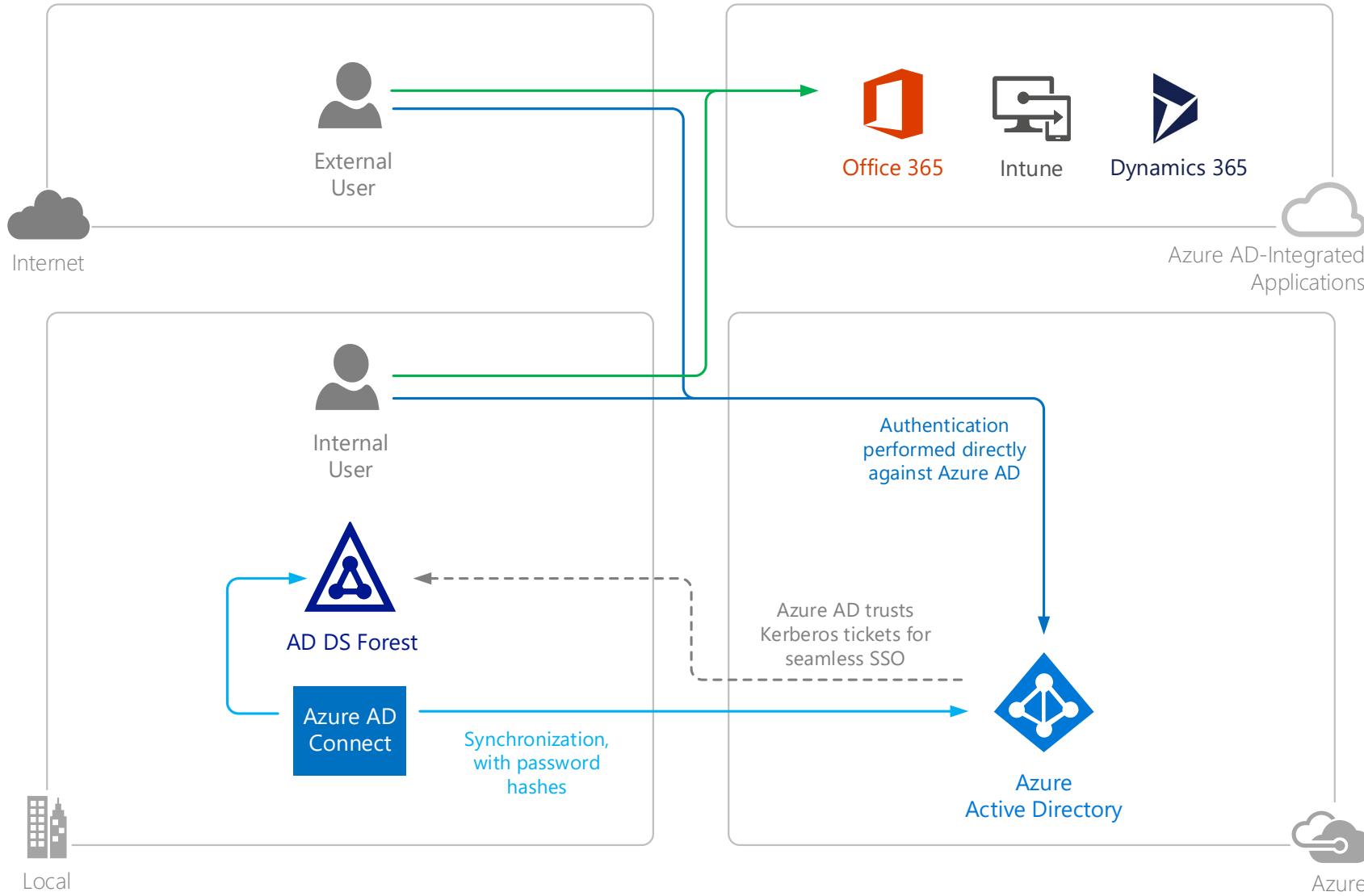
EntraID Connect sync

Federated Identity Provider

Active Directory Domain Services

AD DS hace la autenticación vía un proveedor de identidad federada

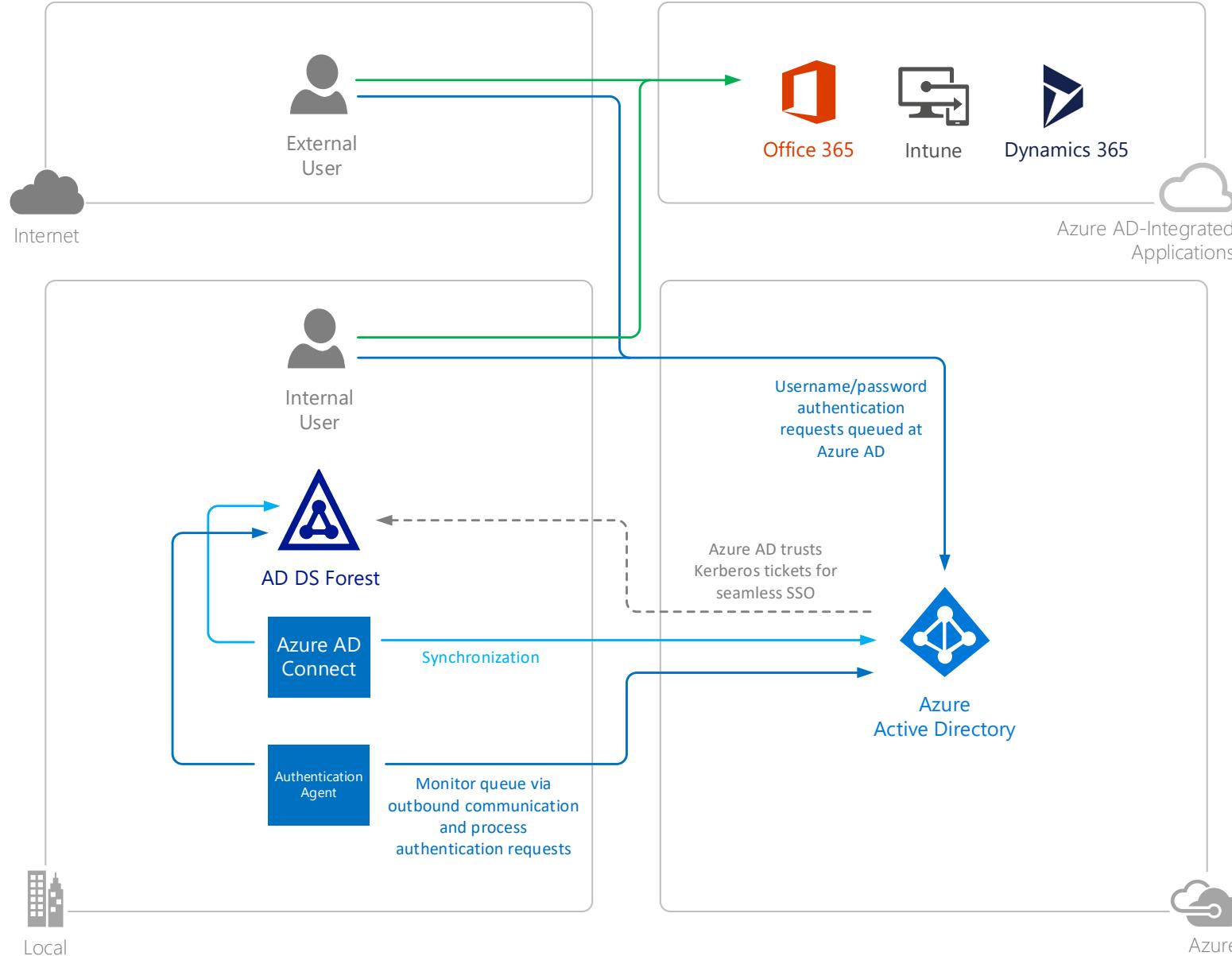
Password Hash Synchronization



1. El usuario solicita acceso a la aplicación y es redirigido a EntralID
2. EntralID pregunta por las credenciales y verifica la contraseña a través del hash sincronizado desde el AD DS on premise.

EntralID Seamless SSO
disponible para equipos unidos a dominio

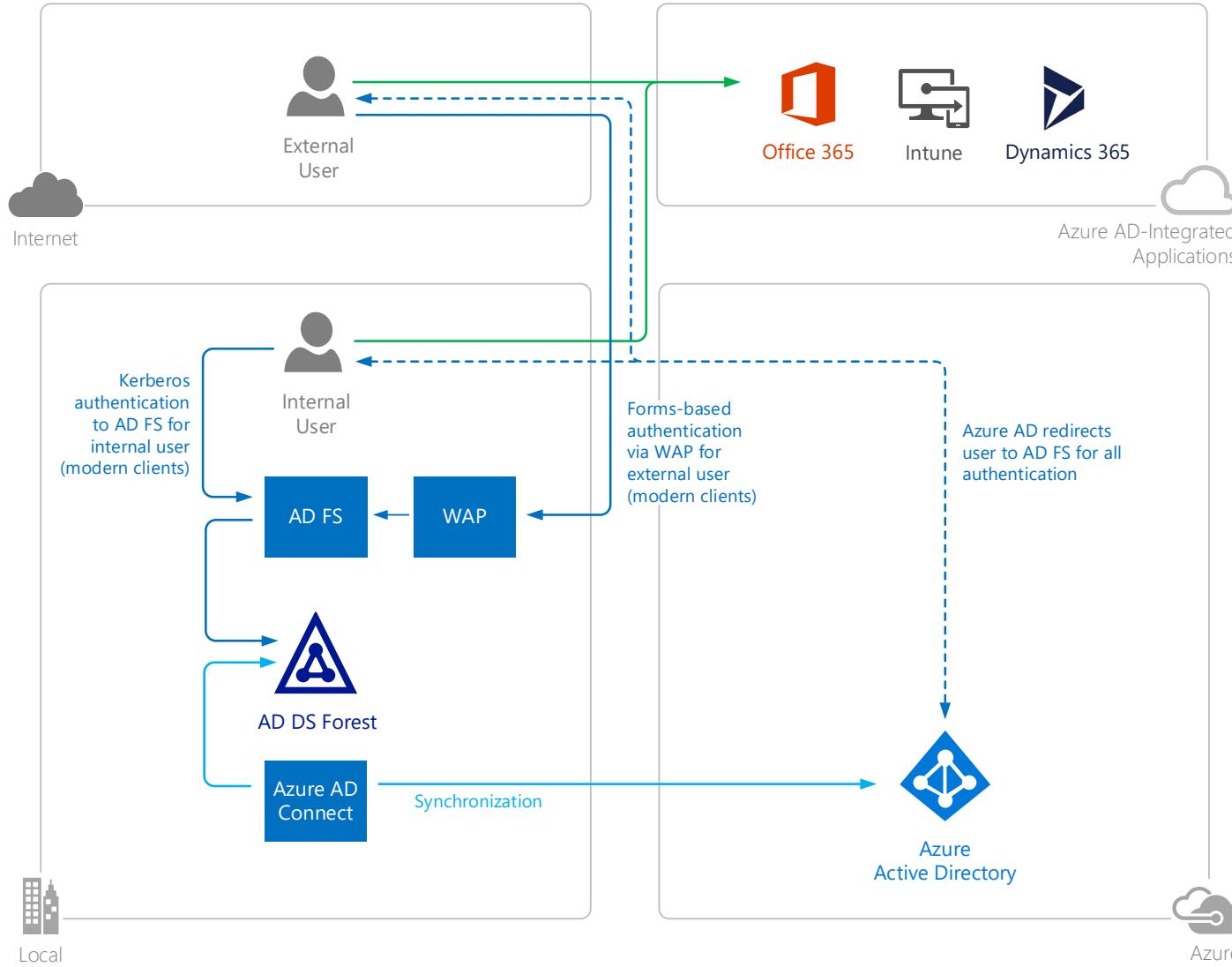
Pass-Through Authentication



1. El usuario solicita acceso a la aplicación y es redirigido a EntralID
2. Azure AD pregunta por las credenciales y ubica el UPN y la contraseña cifrada en una cola
3. El agente de autenticación monitoriza la cola y autentica al usuario a través de AD DS

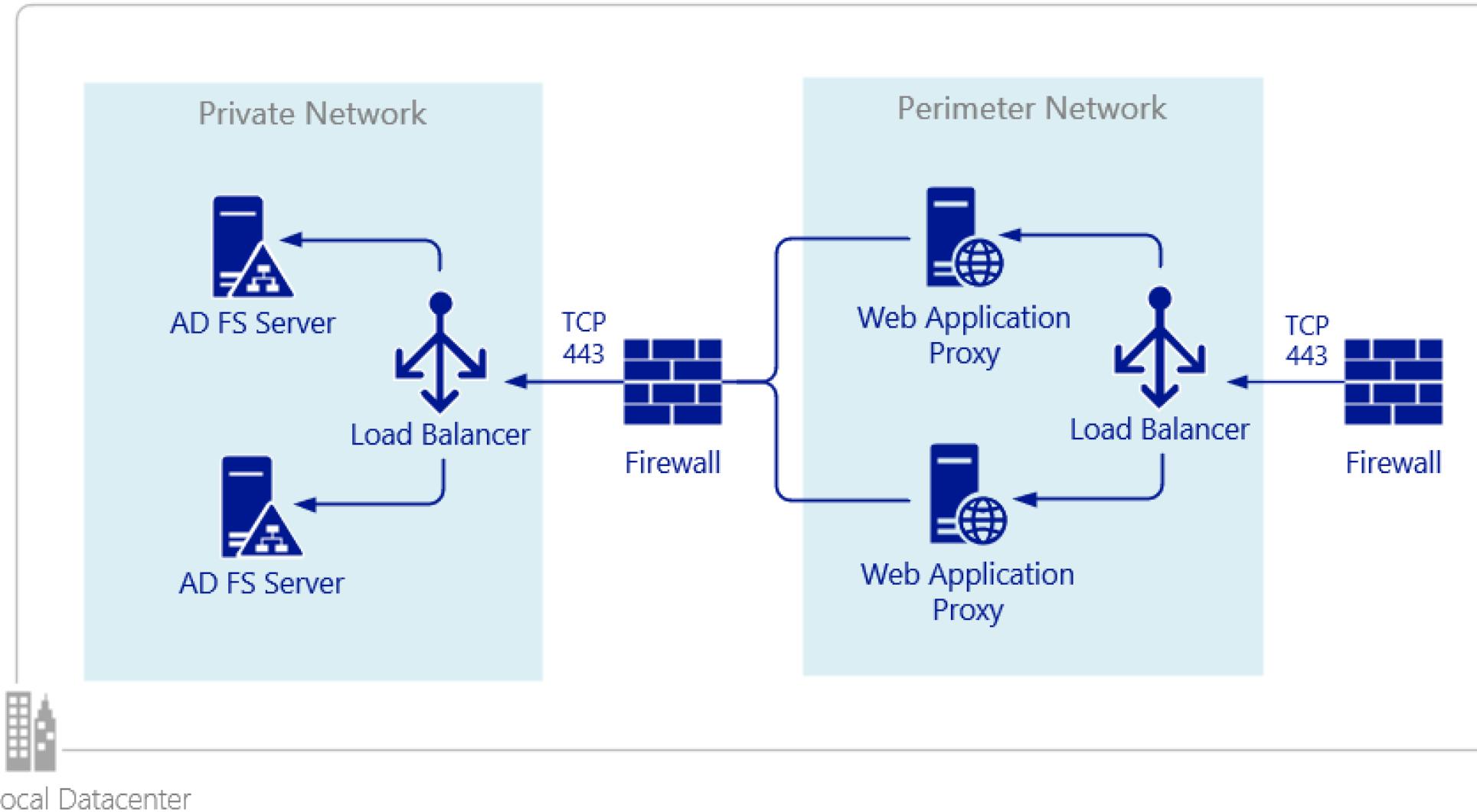
EntralID Seamless SSO
disponible para equipos unidos
a dominio

Federated Authentication

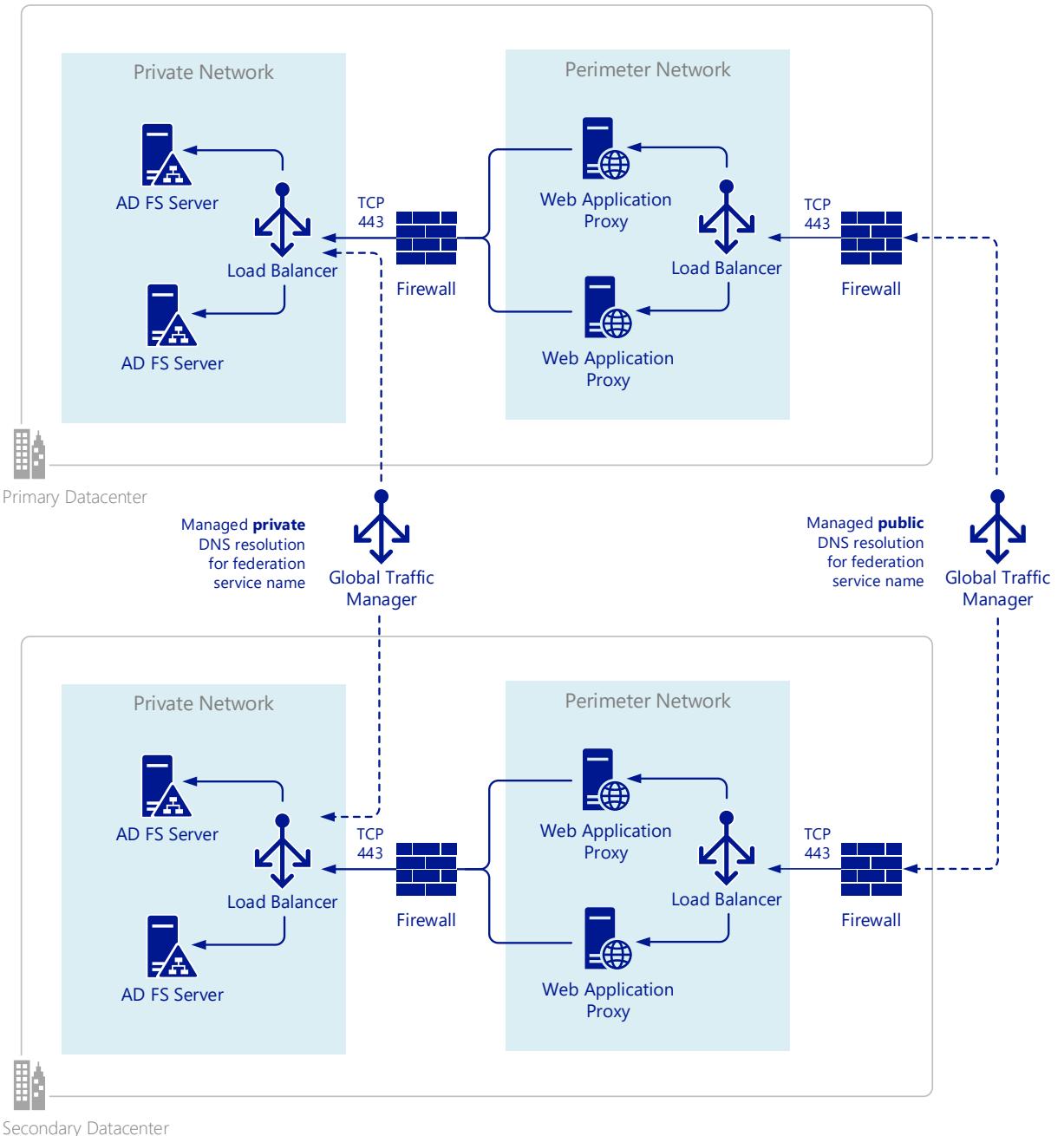


1. El usuario solicita acceso a la aplicación y es redirigido a EntraID
2. El usuario es identificado en EntraID y redirigido al proveedor de identidad federado (IdP).
3. IdP autentica al usuario, vía seamless SSO cuando sea posible.
4. Se emite un token al usuario y se retorna a EntraID
5. EntraID verifica el token y devuelve al usuario a la aplicación con un token de recurso.

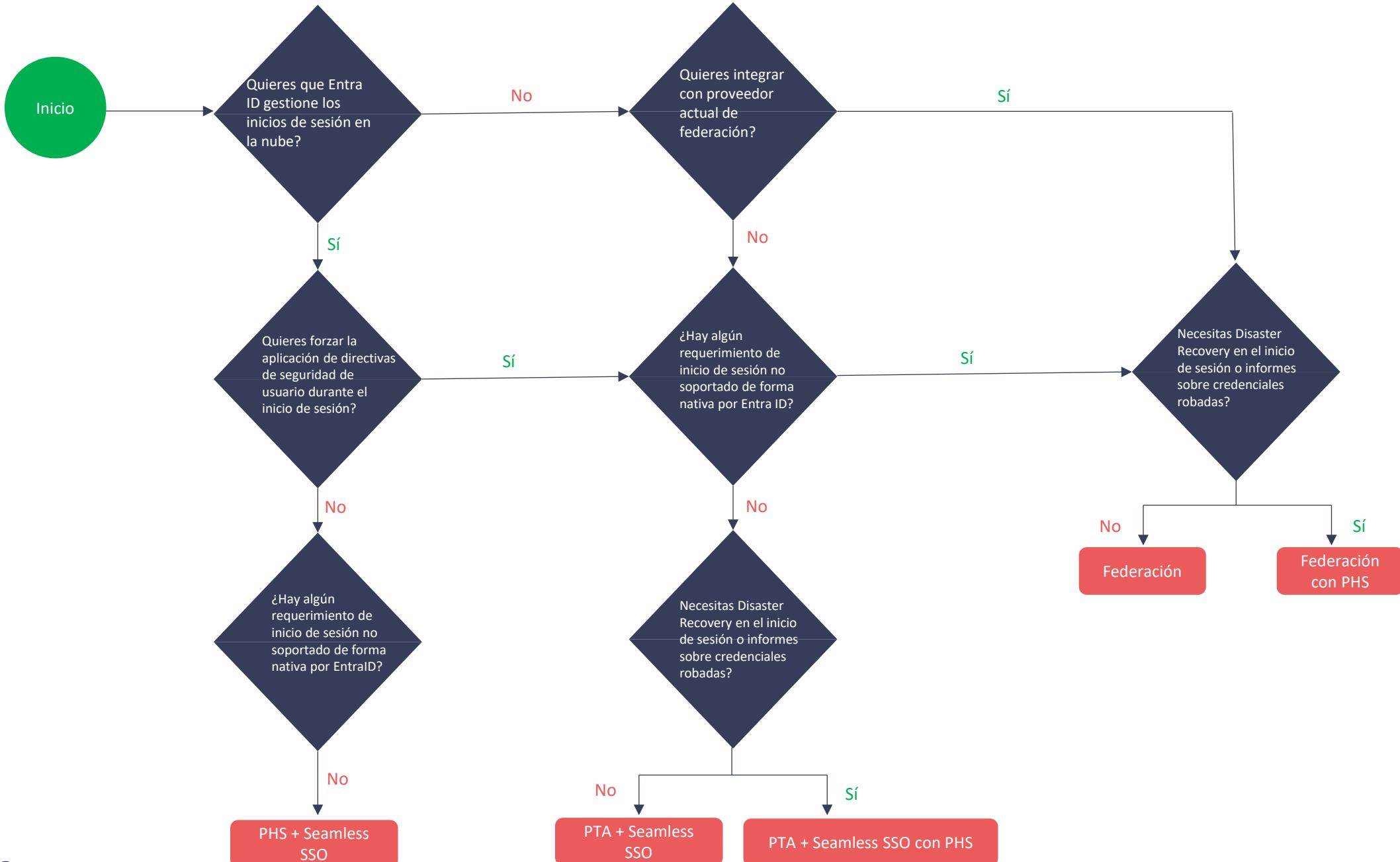
AD FS Infrastructure



AD FS Geo Redundancy



Árbol de Decisión





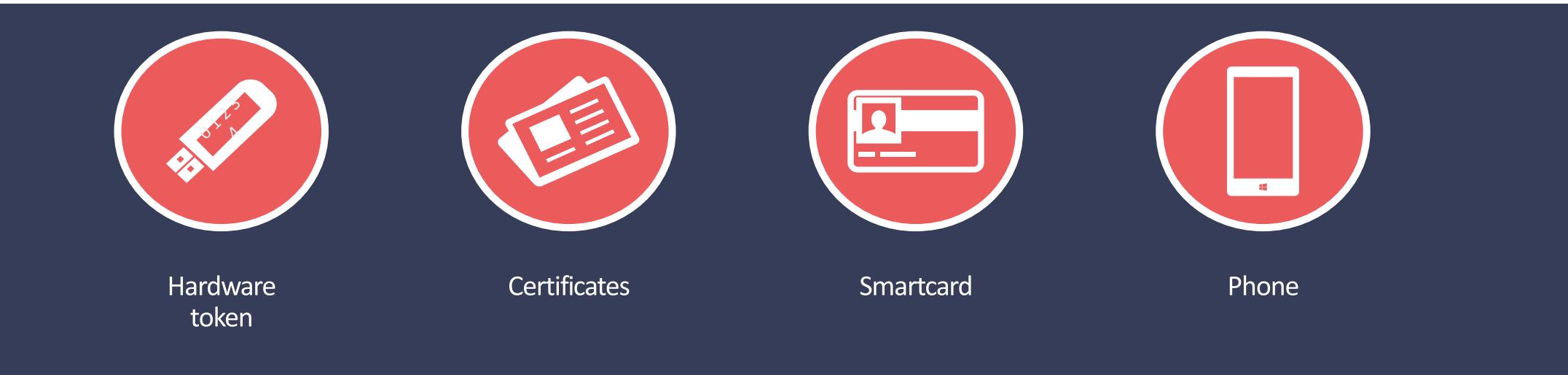
Multi Factor Authentication



¿Que es Multi-Factor Authentication?

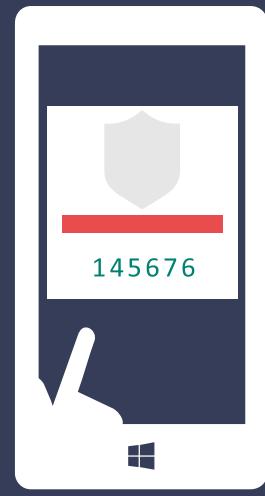
El uso de dos o más elementos:

- Algo que tu conoces como una contraseña o PIN.
- Algo que tienes, como un teléfono, tarjeta de crédito o token de hardware.
- Algo que físicamente te identifica, como una huella dactilar, escáner de retina o otros elementos biométricos.



The Azure MFA Challenge

Mobile Apps



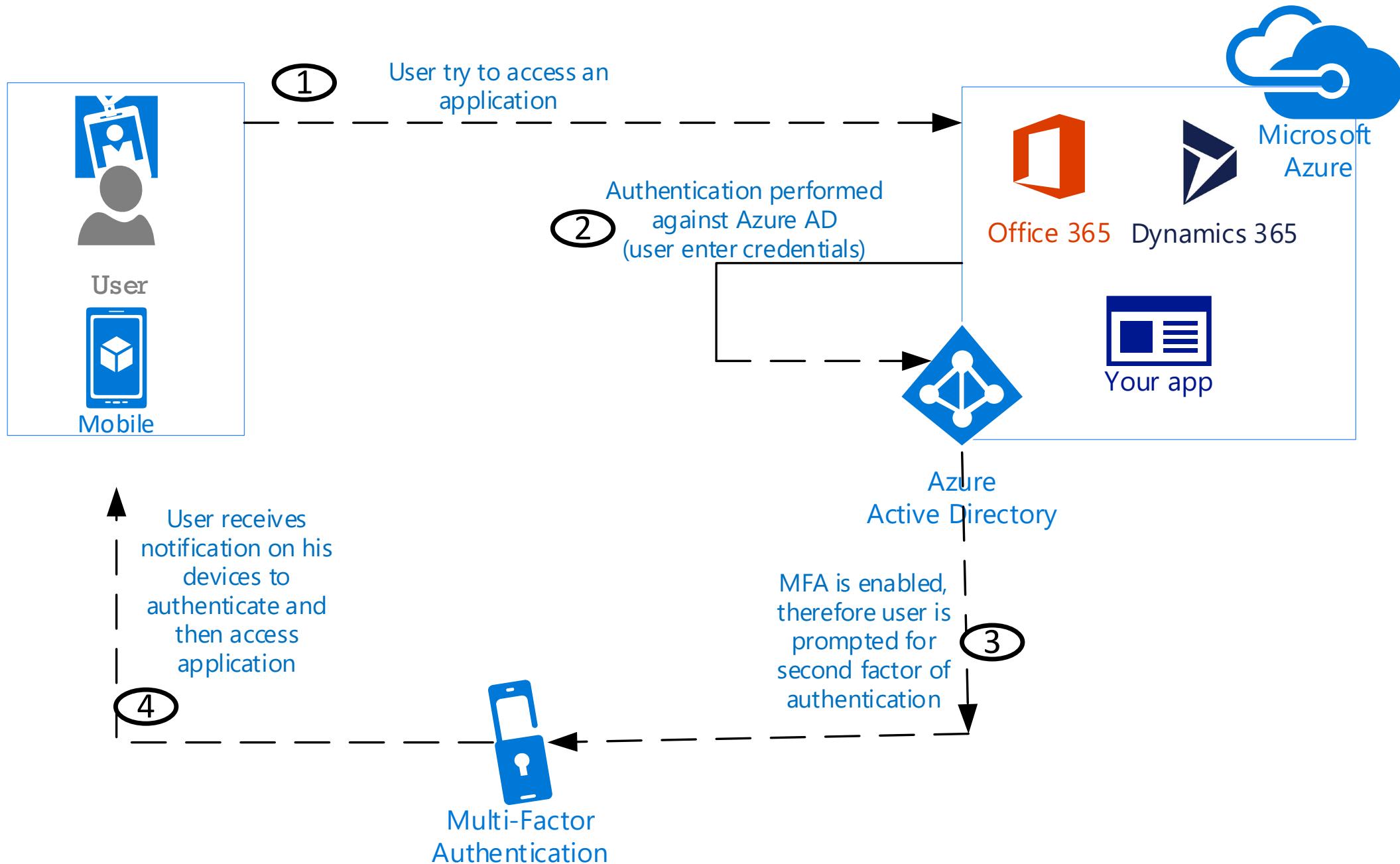
Phone calls



Text messages



Solución MFA – Habilitación de usuario



Demo

MFA





¿Que es acceso condicional?

El acceso condicional es una funcionalidad de Entra ID que permite aplicar controles sobre el acceso a las aplicaciones de su entorno en función de condiciones específicas desde una ubicación central.

Nota: Esto complementa otros controles de autorización: asignación de aplicaciones, roles y licencias



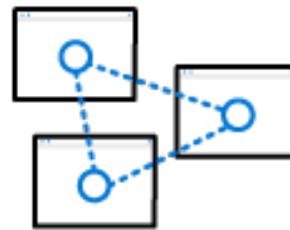
Acceso condicional
basado en el usuario y
la ubicación

Mantenga protegidos los datos confidenciales limitando el acceso de los usuarios en función de la ubicación geográfica o la dirección IP con directivas de acceso condicional basadas en la ubicación.



Acceso condicional
basado en dispositivos

Asegúrese de que solo los dispositivos inscritos y aprobados puedan acceder a los datos corporativos con acceso condicional basado en dispositivos.
Compatible con Linux



Acceso condicional
basado en
aplicaciones

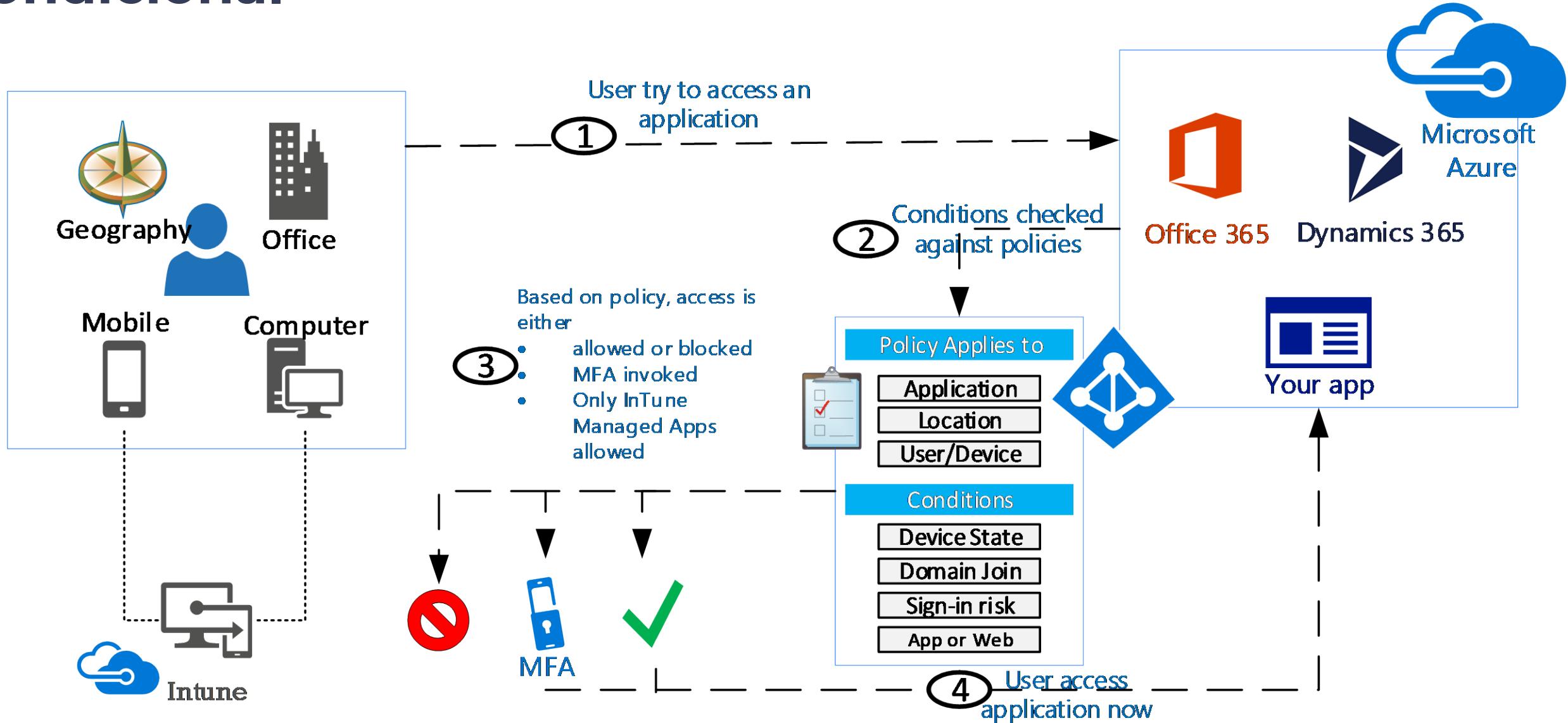
El trabajo no tiene que detenerse cuando un usuario no está en la red corporativa. Proteja el acceso a la nube corporativa y a las aplicaciones locales y mantenga el control con el acceso condicional.



Acceso condicional
basado en riesgos

Proteja sus datos de hackers malintencionados con una directiva de acceso condicional basada en riesgos que se puede aplicar a todas las aplicaciones y a todos los usuarios, ya sea en el entorno local o en la nube.

Información general sobre la solución Acceso condicional



¿Cómo funciona el acceso condicional?

Asignaciones



Policy Application

Condiciones



Policy Evaluation

Mandos



Apply Restrictions

Plantillas de acceso condicional

The screenshot shows two windows side-by-side. The left window is titled 'Conditional Access | Policies' and displays a list of existing policies. The right window is titled 'Create new policy from template' and shows a template selection interface.

Conditional Access | Policies (Left Window):

- Policies:** Create new policy, Create new policy from template (highlighted with a red box).
- Manage:** Named locations, Custom controls (Preview), Terms of use, VPN connectivity, Authentication context (Preview), Classic policies.
- Monitoring:** Sign-in logs, Audit logs.
- Troubleshooting + Support:** Virtual assistant (Preview), New support request.

Create new policy from template (Right Window):

Customize your build **Select template** Review + create

We recommend the following templates based on your response

Template	Description	Action
Require multi-factor authentication for admins	Secure when and how users register for Azure AD Multi-Factor Authentication and self-service password.	View policy summary
Securing security info registration	Block legacy authentication endpoints that can be used to bypass multi-factor authentication.	View policy summary
Block legacy authentication	Block legacy authentication for all users	View policy summary
Require multi-factor authentication for all users	Require multi-factor authentication for all user accounts to reduce risk of compromise.	View policy summary
CA001: Require multi-factor authentication for admins	Require multi-factor authentication for privileged administrative accounts to reduce risk of compromise. This policy will target the same roles as Security Default.	View policy summary
CA002: Securing security info registration	Secure when and how users register for Azure AD Multi-Factor Authentication and self-service password.	View policy summary
CA003: Block legacy authentication	Block legacy authentication endpoints that can be used to bypass multi-factor authentication.	View policy summary
CA004: Require multi-factor authentication for all users	Block legacy authentication for all users	View policy summary
CA005: Require multi-factor authentication for guest access	Block legacy authentication for guest access	View policy summary
CA006: Require multi-factor authentication for Azure management	Require multi-factor authentication for Azure management	View policy summary
CA007: Require multi-factor authentication for risky sign-in	Require multi-factor authentication for risky sign-in	View policy summary
CA008: Require password change for high-risk users	Require password change for high-risk users	View policy summary
CA009: Require compliant or Hybrid Azure AD joined device for ad...	Require compliant or Hybrid Azure AD joined device for ad...	View policy summary
CA010: Block access for unknown or unsupported device platform	Block access for unknown or unsupported device platform	View policy summary
CA011: No persistent browser session	No persistent browser session	View policy summary
CA012: Require approved client apps and app protection	Require approved client apps and app protection	View policy summary
CA013: Require compliant or Hybrid Azure AD joined device or mult...	Require compliant or Hybrid Azure AD joined device or mult...	View policy summary
CA014: Use application enforced restrictions for unmanaged devices	Use application enforced restrictions for unmanaged devices	View policy summary

Name your policy: CA001: Require multi-factor authentication for admins

Policy state: Off On Report-only

[Create Policy](#) [Previous](#) [Next](#)

Características de acceso condicional

Las directivas de acceso condicional tienen desencadenadores basados en condiciones y, a continuación, el acceso se concede en función de los controles. Las condiciones son lógicamente 'ANDed'.

"Cuando esto sucede" se llama condiciones.

"Entonces haz esto" se llama controles de acceso.

Condiciones disponibles:

Usuarios y grupos

Aplicaciones en la nube

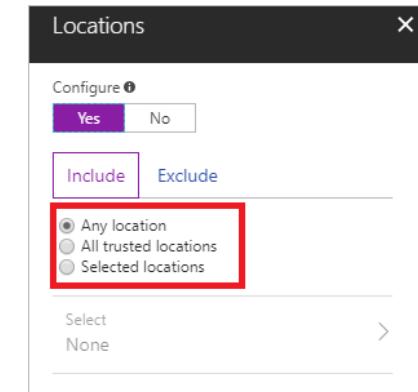
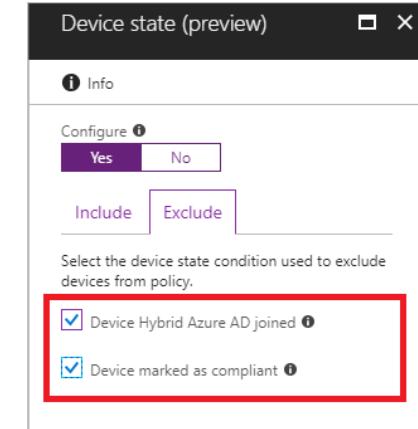
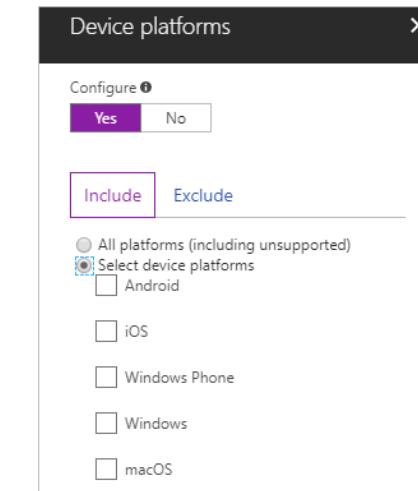
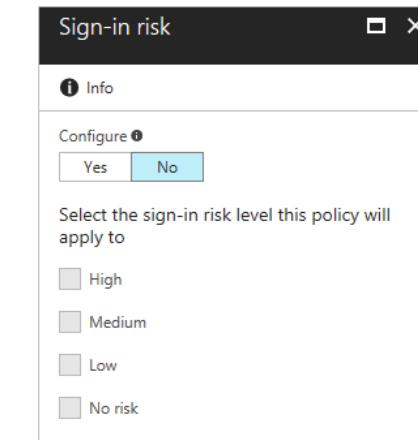
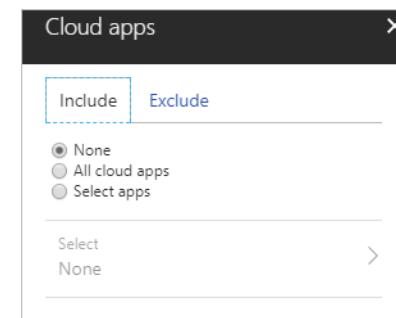
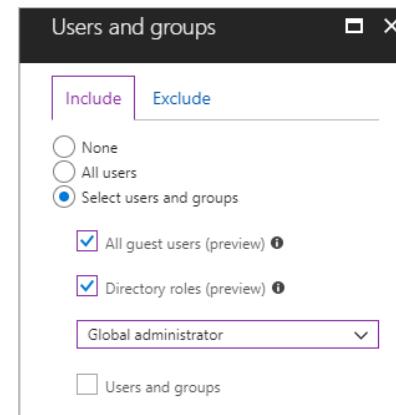
Riesgo de inicio de sesión

Plataformas de dispositivos

Estado del dispositivo

Ubicaciones

Aplicaciones cliente



The screenshot shows the 'Client apps (preview)' configuration dialog. It has two tabs: 'Info' (selected) and 'Configure'. Under 'Configure', there are two buttons: 'Yes' (selected) and 'No'. Below this, there are two tabs: 'Include' (selected) and 'Exclude'. Under 'Include', there are four checkboxes: 'Browser' (selected), 'Mobile apps and desktop clients' (selected), 'Modern authentication clients' (selected), and 'Exchange ActiveSync clients' (unchecked). There is also a note: 'Apply policy only to supported platforms' and a checked checkbox for 'Other clients'. At the bottom, there is a warning message: 'Exchange ActiveSync currently does not support all other conditions'.

Client apps (preview)

Configure Yes No

Select the client apps this policy will apply to

Browser

Mobile apps and desktop clients

Modern authentication clients

Exchange ActiveSync clients

Apply policy only to supported platforms

Other clients

Exchange ActiveSync currently does not support all other conditions

Cloud apps

Include Exclude

None

All cloud apps

Select apps

Select Office 365 Exchange Online ...

Office 365 Exchange Online ...

Mandos

Cada control es un requisito que debe cumplir la persona o el sistema que inicia sesión, o una restricción sobre lo que el usuario puede hacer después de iniciar sesión.

Hay dos tipos de controles:

Conceder controles: para el acceso a la puerta

Controles de sesión: para restringir el acceso dentro de una sesión

Grant controls:
Con los controles de concesión, puede bloquear el acceso por completo o permitir el acceso con requisitos adicionales seleccionando los controles deseados.

Conceder

Aplique controles de acceso para bloquear o conceder acceso. [Más información](#)

- Bloquear acceso
 Conceder acceso
- Requerir autenticación multifactor (i)
 - Requerir intensidad de autenticación (versión preliminar) (i)
 - Requerir que el dispositivo esté marcado como compatible (i)
 - Requerir dispositivo unido a Azure AD híbrido (i)
 - Requerir aplicación cliente aprobada (i)
[Ver la lista de aplicaciones cliente aprobadas](#)
 - Requerir directiva de protección de aplicaciones (i)
[Ver la lista de aplicaciones cliente protegidas por directivas](#)
 - Requerir cambio de contraseña (i)

Session controls:

Las aplicaciones en la nube aplican los controles de sesión y se basan en la información adicional proporcionada por Azure AD a la aplicación sobre la sesión.

Sesión

Controle el acceso con controles de sesión para habilitar experiencias limitadas en determinadas aplicaciones en la nube.
[Más información](#)

- Usar restricciones que exige la aplicación (i)

(i) Este control solo funciona con aplicaciones compatibles. Actualmente, Office 365, Exchange Online y SharePoint Online son las únicas aplicaciones en la nube compatibles con las restricciones que exige la aplicación. Haga clic aquí para obtener más información.

- Utilizar el Control de aplicaciones de acceso condicional (i)
- Frecuencia de inicio de sesión (i)
- Sesión del explorador persistente (i)
- Personalizar evaluación continua de acceso (i)
- Deshabilitar valores predeterminados de resistencia (i)

Tarea: Aplicación de la directiva de acceso condicional

¿Quién obtiene esta póliza?

Usuarios y grupos

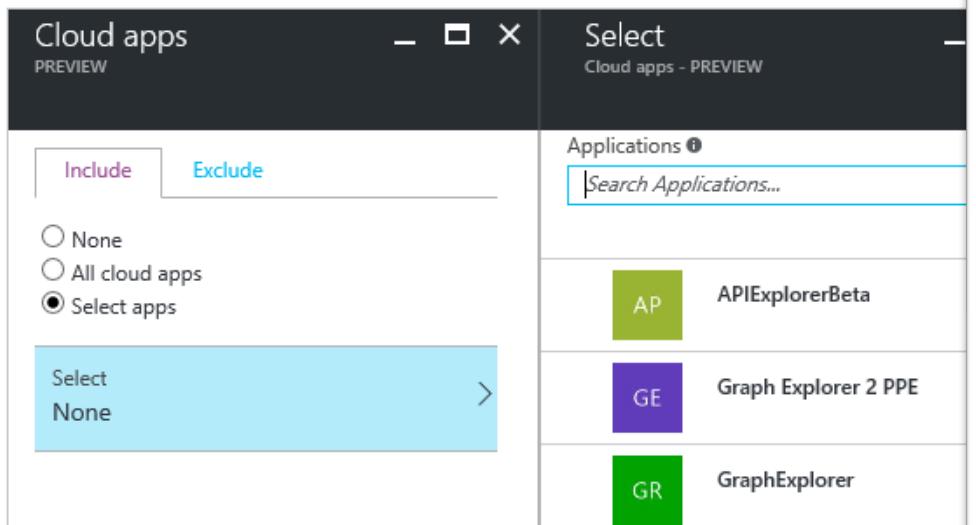
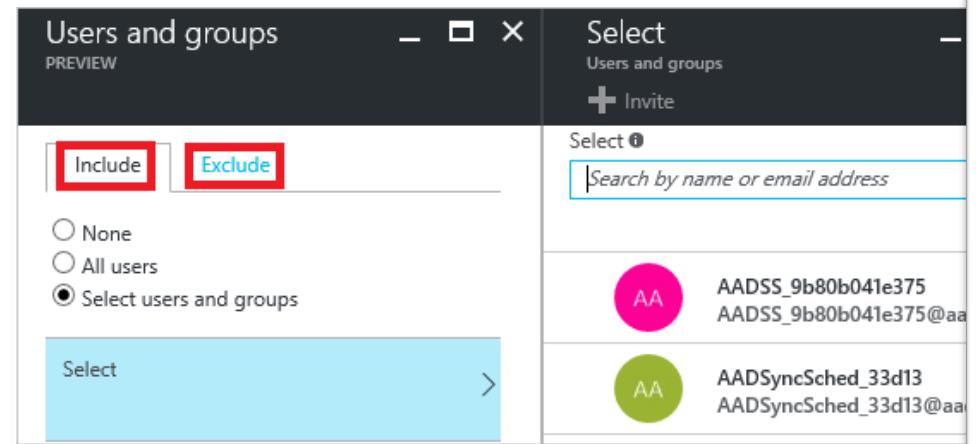
Incluir o excluir usuarios y/o grupos específicos

Aplicaciones

Incluya o excluya aplicaciones de AAD específicas o aplíquelas a todas las aplicaciones. Esto es específicamente en lo que los usuarios de la aplicación hacen clic en el Portal de aplicaciones.

Modo de empleo

Estos filtros admiten tanto la inclusión como la exclusión. Esto permite que una directiva se "centre" en un grupo o aplicaciones, o permite que otras aplicaciones o usuarios estén exentos de esta política.



Nueva ...

Directiva de acceso condicional

Controle el acceso de los usuarios con la directiva de acceso condicional para reunir señales, tomar decisiones y aplicar directivas de la organización. [Más información](#)

Nombre *
Ejemplo: 'directiva de aplicaciones de cumpl...

Tareas

Usuarios o identidades de la carga de trabajo [\(1\)](#)
0 usuarios o identidades de carga de trabajo seleccionadas

Aplicaciones en la nube o acciones [\(1\)](#)
No se ha seleccionado ninguna aplicación o acción ni ningún contexto de autenticación.

Condiciones [\(1\)](#)
0 condiciones seleccionadas

Controles de acceso

Conceder [\(1\)](#)
0 controles seleccionados

Sesión [\(1\)](#)
0 controles seleccionados

Habilitar directiva

[Solo informe](#) Activado Desactivado

Contexto de autenticación (versión preliminar)

Dashboard > Contoso > Security > Conditional Access

Conditional Access | Authentication context

Azure Active Directory

[+ New authentication context](#) [Refresh](#) [Got feedback?](#)

[Policies](#)

[Insights and reporting](#)

[Diagnose and solve problems](#)

[Manage](#)

[Named locations](#)

[Custom controls \(Preview\)](#)

[Terms of use](#)

[VPN connectivity](#)

[Authentication context](#)

[Classic policies](#)

[Troubleshooting + Support](#)

[Virtual assistant \(Preview\)](#)

[New support request](#)

Get started Authentication context

Authentication context is used to secure application data and actions in apps like SharePoint, Microsoft Cloud App Security, and Privileged Identity Management. The below list of recommended configurations provide an overview of all the actions that are required. After configuring them, apply authentication contexts to cloud apps, SharePoint sites and other resources. [Learn more](#)

Configuration steps

Item	Documentation
Configure authentication contexts	Learn more
Assign Conditional Access policies to the authentication context	Learn more
Tag resources with an authentication context	Learn more

Control user access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Authentication context

Authentication context is used to secure application data and actions in apps like SharePoint and Microsoft Cloud App Security. [Learn more](#)

Select the authentication contexts this policy will apply to

Strong Authentication

```
Set-SPOSite -Identity https://contoso.sharepoint.com/sites/research -  
ConditionalAccessPolicy AuthenticationContext -AuthenticationContextName "MFA"
```

Condición: ¿qué plataforma obtiene esta política?

Plataforma de dispositivos

- *Android*
- *iOS*
- *Windows Phone*
- *Windows Desktop*
- *Linux Desktop*
- *macOS*

Si utilizas la opción "Todas las plataformas", puedes excluir plataformas específicas en la pestaña "Excluir"

The screenshot shows a configuration interface for a policy. On the left, there's a sidebar with sections like 'Riesgo de usuario' (User Risk), 'Riesgo de inicio de sesión' (Session Risk), 'Plataformas de dispositivo' (Device Platforms), 'Ubicaciones' (Locations), 'Aplicaciones cliente' (Client Applications), and 'Filtro para dispositivos' (Device Filter). The 'Plataformas de dispositivo' section is currently selected. On the right, a large panel titled 'Plataformas de dispositivo' contains the following text: 'Apply policy to selected device platforms.' and 'Más información'. Below this is a 'Configurar' button with 'Sí' (Yes) and 'No' options, where 'No' is highlighted. Underneath the button are two tabs: 'Incluir' (Include) and 'Excluir' (Exclude), with 'Incluir' being the active tab. A list of platform checkboxes follows: 'Cualquier dispositivo' (Any device) and 'Seleccionar plataformas de dispositivo' (Select device platforms), both of which are unselected. Below these are individual checkboxes for each platform: Android, iOS, Windows Phone, Windows, macOS, and Linux.

Condición: ¿qué ubicación obtiene esta política?

Ubicaciones

Marcar como ubicación de confianza, por lo general, las ubicaciones de confianza son áreas de red controladas por el departamento de TI.

Los informes de seguridad de Azure Identity Protection y Azure AD también usan ubicaciones con nombre de confianza para reducir los falsos positivos.

País/Regiones: esta opción le permite seleccionar uno o más países o regiones para definir una ubicación con nombre. Considere la posibilidad de definir los países en un Doing Business In frente a Not Doing Business In para definir las políticas.

Incluir áreas desconocidas: algunas direcciones IP no están asignadas a un país específico. Esta opción le permite elegir si estas direcciones IP deben incluirse en la ubicación nombrada. Podrían comprobarse cuándo la directiva que utiliza la ubicación con nombre debe aplicarse a ubicaciones desconocidas.

Nueva ubicación (Países o reg... >

Información: A los países o regiones solo se les pueden asignar direcciones IPv4. Las direcciones IPv6 están incluidas en países o regiones desconocidos.

Nombre *: Asigne un nombre a esta ubicación

Determinación de la ubicación por dirección IP (solo IPv4) ▾

Incluir países o regiones desconocidos ⓘ

Buscar países

Nombre

Afganistán

Albania

...

Nombre *: Asigne un nombre a esta ubicación

Marcar como ubicación de confianza

Configurar ⓘ: Control user access based on their physical location. [Más información](#)

Sí **No**

Incluir **Excluir**

Cualquier ubicación

Todas las ubicaciones de confianza

Ubicaciones seleccionadas

Escriba un nuevo intervalo IPv4 o IPv6
p. ej.: 40.77.182.32/27 o 2a01:111::/32

Agregar **Cancelar**

Condición: aplicaciones cliente

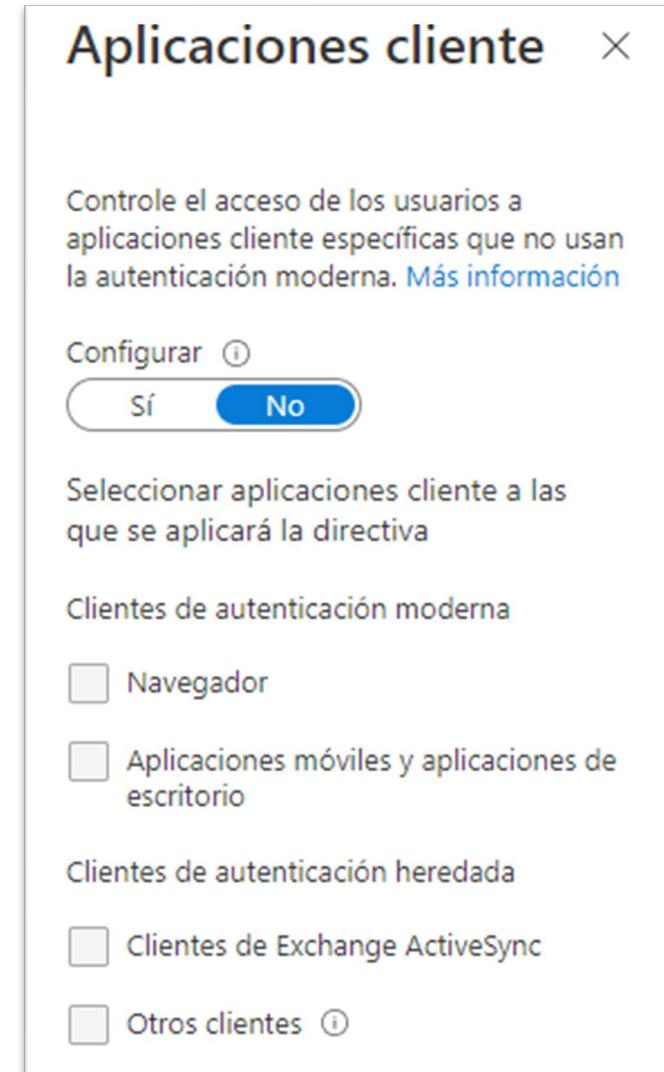
La condición de aplicaciones cliente se usa para aplicar diferentes controles basados en el protocolo:

- Web Browser: Federation (WS-Federation and SAML)
- Mobile apps and desktop clients:
 - Modern Authentication - (OAuth and OpenID Connect)
 - Exchange ActiveSync: EAS
 - Other clients: Legacy Authentication (Basic, WS-Trust, POP/IMAP)

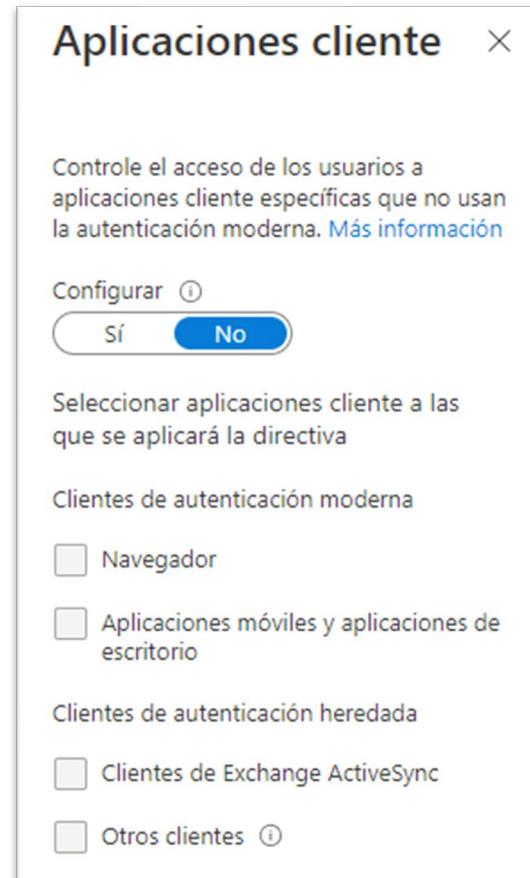
Algunos casos de uso típicos de este control:

- Enforce device controls on machines using apps that can download offline data
- Forcing unmanaged devices to only use the browser for access
- Blocking web access but allowing mobile app access.
- **Blocking legacy protocols**

Nota: El uso de la condición del navegador con los controles del dispositivo requiere versiones específicas de IE, Chrome, Edge y Safari (en Mac/iOS). Chrome requiere una extensión en Win 10 y ediciones de registro en Win 7/8.1.

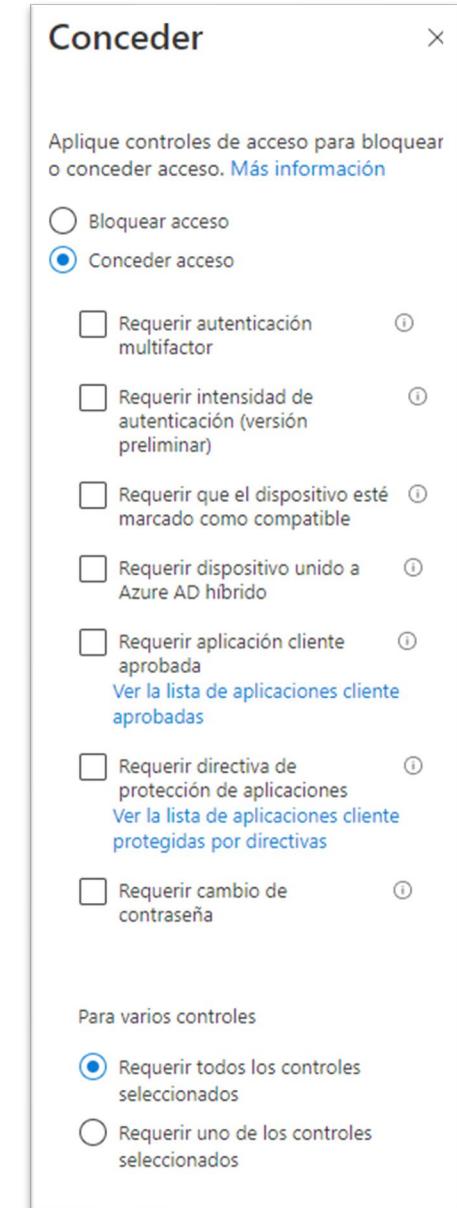


Aplicaciones cliente: tanto una condición como un control



Condición O Control

- Para aplicar diferentes políticas al uso del navegador o de la aplicación.

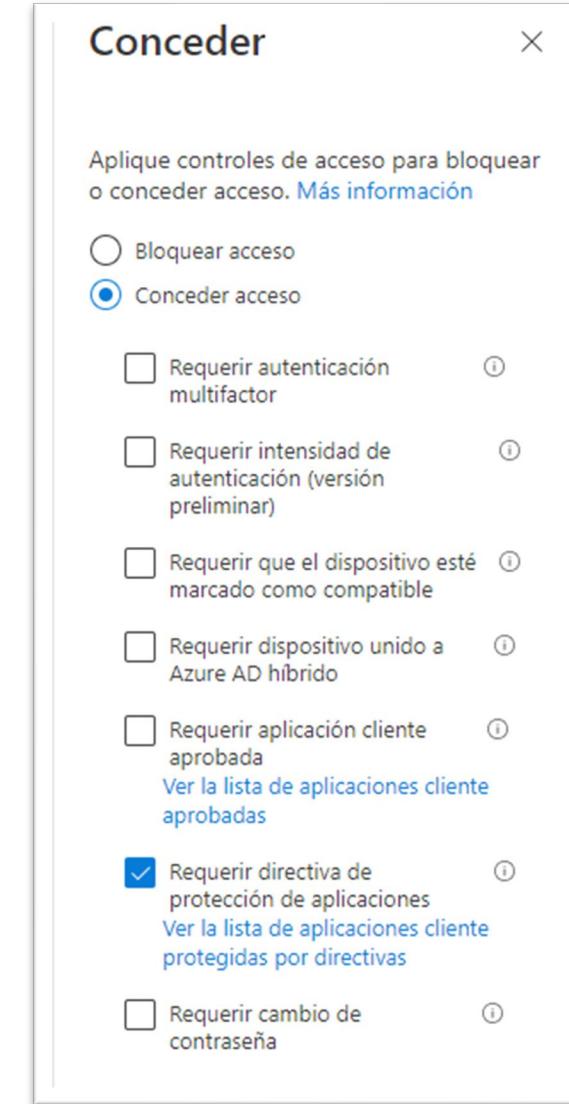


Este control se usa para aplicar directivas de MAM.

Control: directiva de protección de aplicaciones



Control



Condición: riesgo de inicio de sesión

Controle el acceso de los usuarios en función de las señales de las condiciones como el riesgo, la plataforma del dispositivo, la ubicación, las aplicaciones cliente o el estado del dispositivo. [Más información](#)

Riesgo de usuario ⓘ
Sin configurar

Riesgo de inicio de sesión ⓘ
Sin configurar

Riesgo de usuario

Configurar ⓘ [Sí](#) [No](#)

Configure los niveles de riesgo de usuario necesarios para aplicar la directiva.

Alta
 Mediana
 Baja

Riesgo de inicio de sesión

Controle el acceso de los usuarios para responder a niveles de riesgo específicos de inicio de sesión. [Más información](#)

Configurar ⓘ [Sí](#) [No](#)

El nivel de riesgo de inicio de sesión se genera en función de todas las detecciones de riesgo en tiempo real.

Seleccionar el nivel de riesgo de inicio de sesión al que se aplicará la directiva

Alta
 Mediana
 Baja
 Sin riesgo

¿Hay algún comportamiento sospechoso asociado a la actividad de inicio de sesión del usuario?

Esto requiere Azure AD Premium P2

Condición: filtro de dispositivo

Filtro para dispositivos

X

Configure a filter to apply policy to specific devices. [Más información](#)

Configurar ⓘ

Sí No

Dispositivos que coinciden con la regla:

- Incluir los dispositivos filtrados en la directiva
 Excluir los dispositivos filtrados de la directiva

Puede usar el generador de reglas o el cuadro de texto de sintaxis de regla para crear o editar la regla de filtro.

Y/o	Propiedad	Operador	Valor
	OperatingSystem	Es igual a	Agregar un valor

+ Agregar expresión

Sintaxis de regla ⓘ

Editar

Demo

Conditional Access





EntralD Privileged Identity Management

1. Azure Active Directory Privileged Identity Management (PIM), te da la capacidad de administrar, controlar y monitorizar el acceso a tu organización. Se incluye dentro del ámbito de PIM acceso a recursos de Azure, EntralD y otros Servicios online como Office 365 o Microsoft Intune.
2. Privileged Identity Management provee de la capacidad de activar roles con carácter temporal , con requerimiento de aprobación que ayude a mitigar el riesgo de concesión de permisos excesivos, innecesarios o mal utilizados sobre recursos y/o aplicaciones.
 - Proveer acceso just-in-time privileged a EntralD y recursos de Azure
 - Asignación de permisos de accesos temporales sobre recursos
 - Requerir aprobación para activar roles
 - Forzar multi-factor authentication para activar un rol
 - Usar justificación para reflejar la necesidad de un usuario de un rol.
 - Obtener notificaciones por rol activado
 - Auditoria de histórico de uso de privilegios

The screenshot shows the Azure Active Directory Privileged Identity Management (PIM) interface. The left side features a dark sidebar with a vertical list of service icons: a plus sign, three horizontal lines with dots, a star, the Internet Explorer logo, a grid, a box, the Earth, a lightning bolt, three dots, the SQL Server logo, two planets, a monitor, and a green diamond. The main area has a dark header bar with 'Home > Privileged Identity Management' and 'Privileged Identity Management'. Below the header is a light blue 'Quick start' button with a gear icon. The main content area is divided into sections: 'TASKS' (My roles, Approve requests, My requests, Review access), 'MANAGE' (Azure AD directory roles, Azure resources), and 'ACTIVITY' (My audit history). Each section has a corresponding icon next to its title.

Demo

EntraID Priviledge Identity Mangement



Gestión de la protección de la identidad

Identity Protection es una herramienta que permite a las organizaciones ejecutar tres tareas principales:

- Automatizar la detección y remediación de riesgos basados en identidad.
- Investigar los riesgos usando los datos ofrecidos desde el portal.
- Exportar los datos de detección de riesgos a una aplicación de terceros para análisis Avanzado.



Gestión de la protección de la identidad

Identity Protection identifica riesgos basándose en las siguientes clasificaciones:

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	Indicates that the user's valid credentials have been leaked.
Password spray	Indicates that multiple usernames are being attacked using common passwords in a unified, brute-force manner.
Azure AD threat intelligence	Microsoft's internal and external threat intelligence sources have identified a known attack pattern.

Demo

Identity Protection





RBAC

A photograph of a woman from the waist up. She has long, straight hair and is wearing a bright red, belted coat over a light-colored, ribbed sweater. Her hands are raised to her face, with her fingers covering her eyes. She is looking directly at the camera through her fingers. The background is a soft, out-of-focus teal color.

¿Qué es RBAC?

- RBAC es un método para gestionar el acceso a los recursos.
- Se basa en roles en lugar de usuarios o grupos
- Los permisos se asignan a roles, y luego los roles se asignan a usuarios o grupos
- Esto permite una gestión más granular de los permisos de acceso



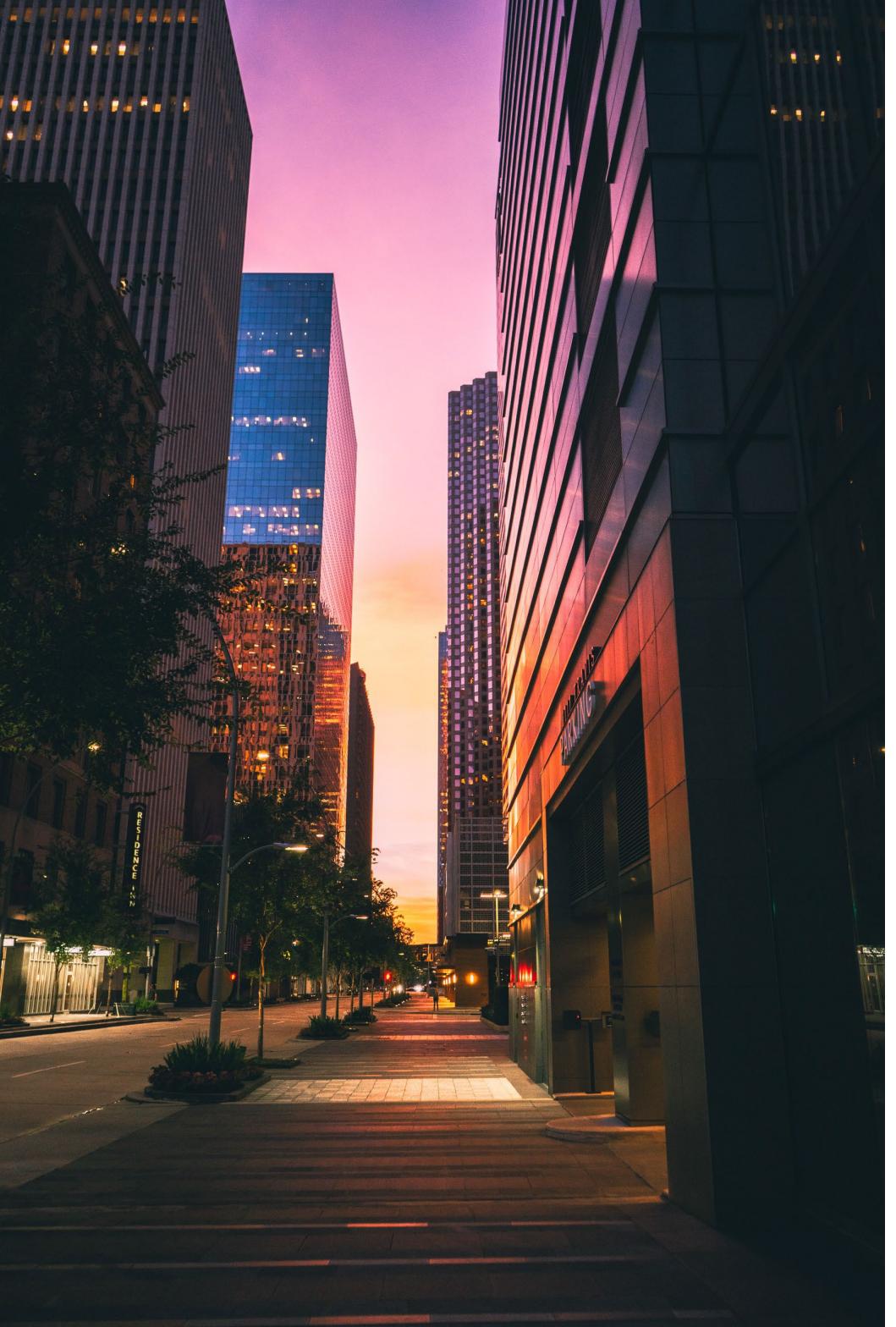
Roles predefinidos de Azure RBAC

- Azure RBAC proporciona varios roles predefinidos
- Cada rol se corresponde con un conjunto de permisos
- Los roles incluyen Propietario, Colaborador, Lector y muchos otros
- Puede personalizar los roles y crear nuevos roles según sea necesario



¿Cómo funciona Azure RBAC?

- Azure RBAC se basa en jerarquías de recursos
- Los permisos se heredan de los recursos superiores a los inferiores
- Los roles se asignan a nivel de suscripción, grupo de recursos o recurso
- Los usuarios y grupos heredan los permisos de los roles asignados en recursos superiores



Beneficios de Azure RBAC

- Azure RBAC permite una gestión más granular de los permisos de acceso
- Reduce la carga administrativa al permitir la asignación de roles en lugar de permisos individuales
- Permite una auditoría más fácil al rastrear los roles asignados a los usuarios
- Ayuda a mejorar la seguridad al controlar el acceso a los recursos de Azure



izertis
Passion for Technology



EMEA

ESPAÑA

A Coruña
Barcelona
Gijón
Madrid
Sevilla
Tenerife
Valencia
Vitoria

PORTUGAL

Lisboa
Aveiro

AMÉRICA

USA

Miami

MÉXICO

Ciudad de México
Guadalajara

COLOMBIA

Medellín

izertis

Passion for Technology

