Unlocking Access: Mastering Authentication for Azure Virtual Desktop & Windows 365

MC2MC

CONNECT

MC2MC
CONNECT

Travis Roberts

- Speaker, course author, YouTube creator, blogger
- Sr. Technical Trainer
- 26+ years of IT experience

@ciraltos.bsky.social

youtube.com/@ciraltos

/in/robertst/

www.ciraltos.com

MC2


CONNECT · COLLABORATE · CREATE
MC2MC
CONNECT


2Pint


PATCH
MY PC


robopack


wortell


INGRAM
MICRO


The Collective


bechtle


lebon.IT


ConXioN
The new style of IT


VirtualMetric


veeam


evri

Agenda

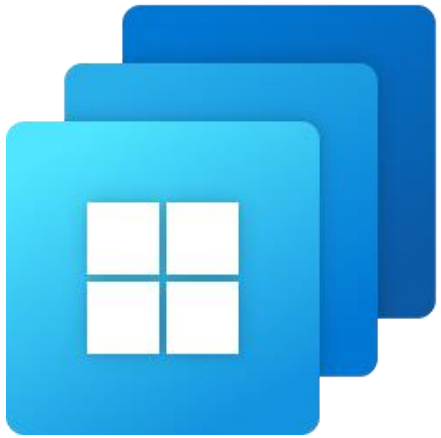
01 Microsoft Directories

02 AVD Identity Models

03 W365 Identity Models

04 AVD and W365 Licensing

05 Best Practices



MC2MC
CONNECT

Microsoft Directories

Microsoft Directory Services

Entra ID

- Microsoft hosted, cloud-based directory service
- Tenant-based
- Three tiers (free, P1, P2) with add-ons
- Supports Zero Trust principles
- OAuth, SAML, and OpenID Connect Authentication

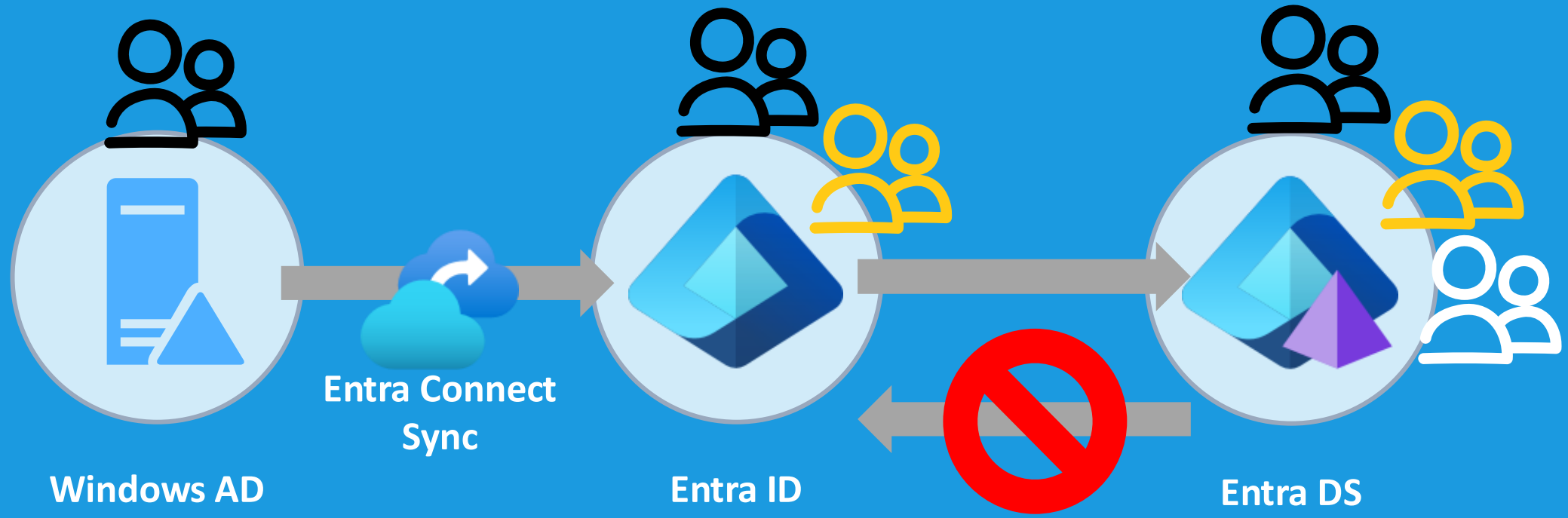
Windows AD

- Hierarchical Directory
- Extensible Schema
- Group Policy Objects
- Dedicated domain controllers
- Standards-based LDAP and DNS
- Kerberos and NTLM authentication

Entra DS

- Windows AD compatible
- Azure PaaS Service
- Unique namespace
- Entra ID integration
- Kerberos, NTLM, DNS and LDAP

Directory Synchronization



Authentication vs. Authorization

Authentication

- Verifies a person, software component, or hardware.
- Requires credentials such as username, password, biometrics, or passcode.

Confirms users are who they say they are.

Authentication vs. Authorization

Authentication

- Verifies a person, software component, or hardware.
- Requires credentials such as username, password, biometrics, or passcode.

Confirms users are who they say they are.

Authorization

- Grants authenticated users, machines, or software components access to resources.

Validates users have permission to complete actions or access resources.

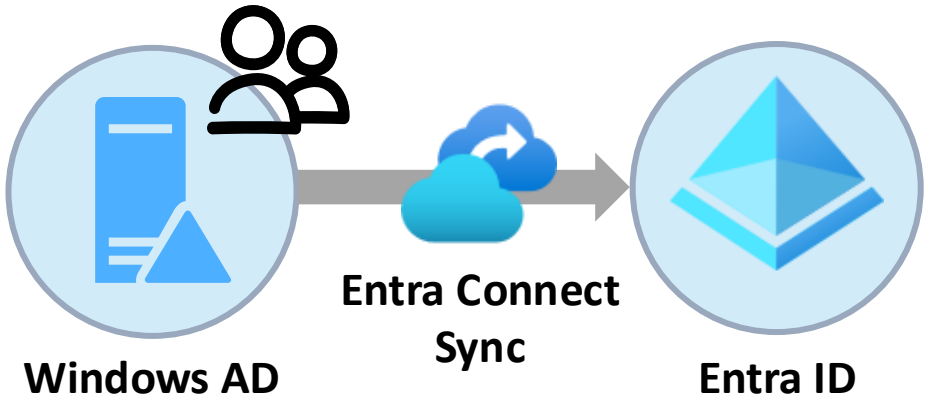
AVD Identity Models

Cloud Native Identity

- Account created in Entra ID.
- Support for OAuth, SAML, and OpenID Connect.
- Entra ID joined session hosts only.
- FSLogix support is in preview.

Hybrid Identities

- Identities sourced from Windows AD.
- Synchronized to Entra ID with Entra Connect Sync or Entra Cloud Sync.
- Supports Windows AD–joined and Entra ID–joined session hosts.
- Only ***GA*** option for FSLogix profiles and Entra ID joined session hosts.



Federated Identities

- User authentication delegated to a third-party identity provider(IdP).

User Sign-in

Entra ID detects the domain is federated when the user signs in.

Redirect to the IdP

The user is redirected to the IdP for authentication.

Token Exchange

The IdP validates credentials and issues a SAML or WS-Fed token to Entra ID.

Access Granted

Entra ID converts the token to an OAuth / OpenID Connect token for AVD access.

AVD External Access

External Users

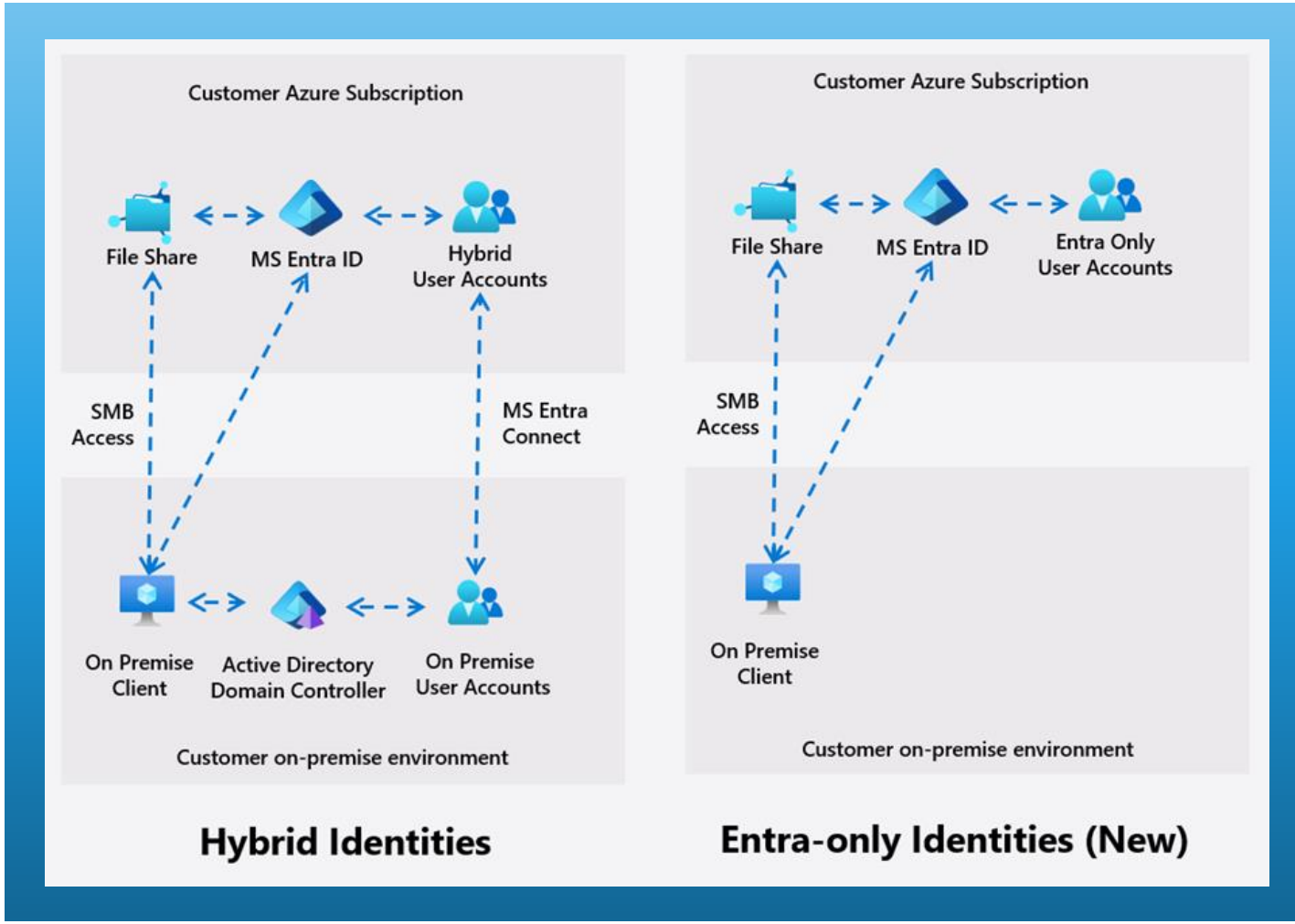
- Provides commercial access to SaaS applications.
- Users created in the resource (AVD) tenant.

External Identities

- B2B guest user account.
- Users authenticated in source tenant, authorized in the resource tenant.
- Requires Windows 11 Enterprise 24H2 with CU 2025-09 or newer.
- Entra ID joined session hosts only.
- SSO must be enabled.
- FSLogix support in preview.

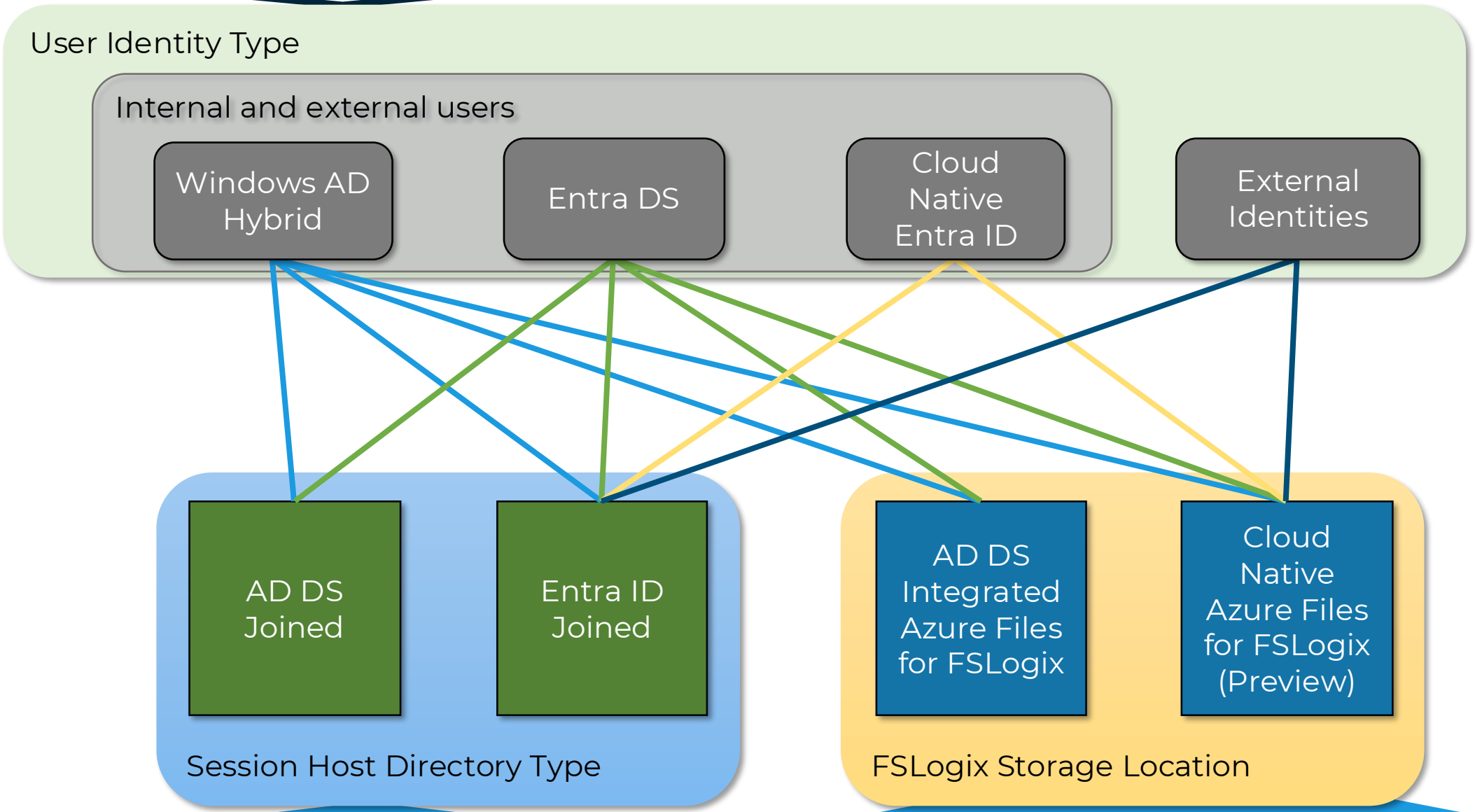
Cloud Native and External Identities and FSLogix

- Entra-only access to Azure Files. No domain controllers needed.
- Supports Azure Files SMB permissions.
- Use pooled host pools with cloud native and external identities.
- Currently in preview.



Demo:
Cloud Native and External Identities

Features and Identity Type



Windows 365 Identity Models

Windows 365 Cloud PC Identities

- Cloud Native Entra ID
  - Easiest deployment option.
  - Microsoft-manage network or Azure private network.
- Hybrid Windows AD
  - Requires Azure private network and line of sight to a domain controller.
  - Devices must be synced to Entra ID.
  - Entra DS is not supported.

Windows 365 Cloud PC Identities

- External Identities
  - B2B guest account.
  - Windows 11 Enterprise 24H2 with CU 2025-09 or newer.
  - Entra ID joined session host.
  - SSO must be configured.
  - Requires the Windows App client.
  - Intune *device* configuration policy.

AVD and Windows 365 Licensing

AVD Licensing

- Windows client OS
  - Microsoft 365 E3, E5, A3, A5, F3, Business Premium, Student Use Benefit.
  - Windows Enterprise E3, E5.
  - Windows Education A3, A5.
  - Windows VDA per user.
- Server OS
  - Remote Desktop Services (RDS) Client Access License (CAL) with Software Assurance (per-user or per-device).
  - RDS User Subscription Licenses.

AVD Licensing

- Windows client OS
  - Microsoft 365 E3, E5, A3, A5, F3, Business Premium, Student Use Benefit.
  - Windows Enterprise E3, E5.
  - Windows Education A3, A5.
  - Windows VDA per user.
- Server OS
  - Remote Desktop Services (RDS) Client Access License (CAL) with Software Assurance (per-user or per-device).
  - RDS User Subscription Licenses.
- Per-user access pricing for external commercial purposes
  - External users, internal identities.
  - Flat fee per user:
    - Apps
    - Apps + Desktop
  - Enrollment at the subscription.

AVD Licensing

- Windows client OS
  - Microsoft 365 E3, E5, A3, A5, F3, Business Premium, Student Use Benefit.
  - Windows Enterprise E3, E5.
  - Windows Education A3, A5.
  - Windows VDA per user.
- Server OS
  - Remote Desktop Services (RDS) Client Access License (CAL) with Software Assurance (per-user or per-device).
  - RDS User Subscription Licenses.
- Per-user access pricing for external commercial purposes.
  - External users, internal identities.
  - Flat fee per user:
    - Apps
    - Apps + Desktop
  - Enrollment at the subscription.
- External, B2B guest identities
  - External authentication, internal authorization.
  - Same licensing requirement as internal users.
  - Licensing in external tenant does not transfer to internal tenant.
  - This includes multi-tenant organizations.

Windows 365 Licensing

- Windows 365 Enterprise
  - Windows 10 or 11 Enterprise.
  - Intune.
  - Entra ID P1 or P2.
  - Windows 365 Cloud PC.
    - Licensed per-user.
- Windows 365 Frontline
  - Windows 10 or 11 Enterprise.
  - Intune.
  - Entra ID P1.
  - Windows 365 Cloud PC.
    - Licensed at the tenant.
    - Assigned by group membership.
- External, B2B guest identities
  - External authentication, internal authorization.
  - Same licensing requirement as internal users.
  - Licensing in external tenant does not transfer to internal tenant.
  - This includes multi-tenant organizations.

Enterprise and Frontline Licensing

Windows 365 Enterprise

- One cloud PC for one user.

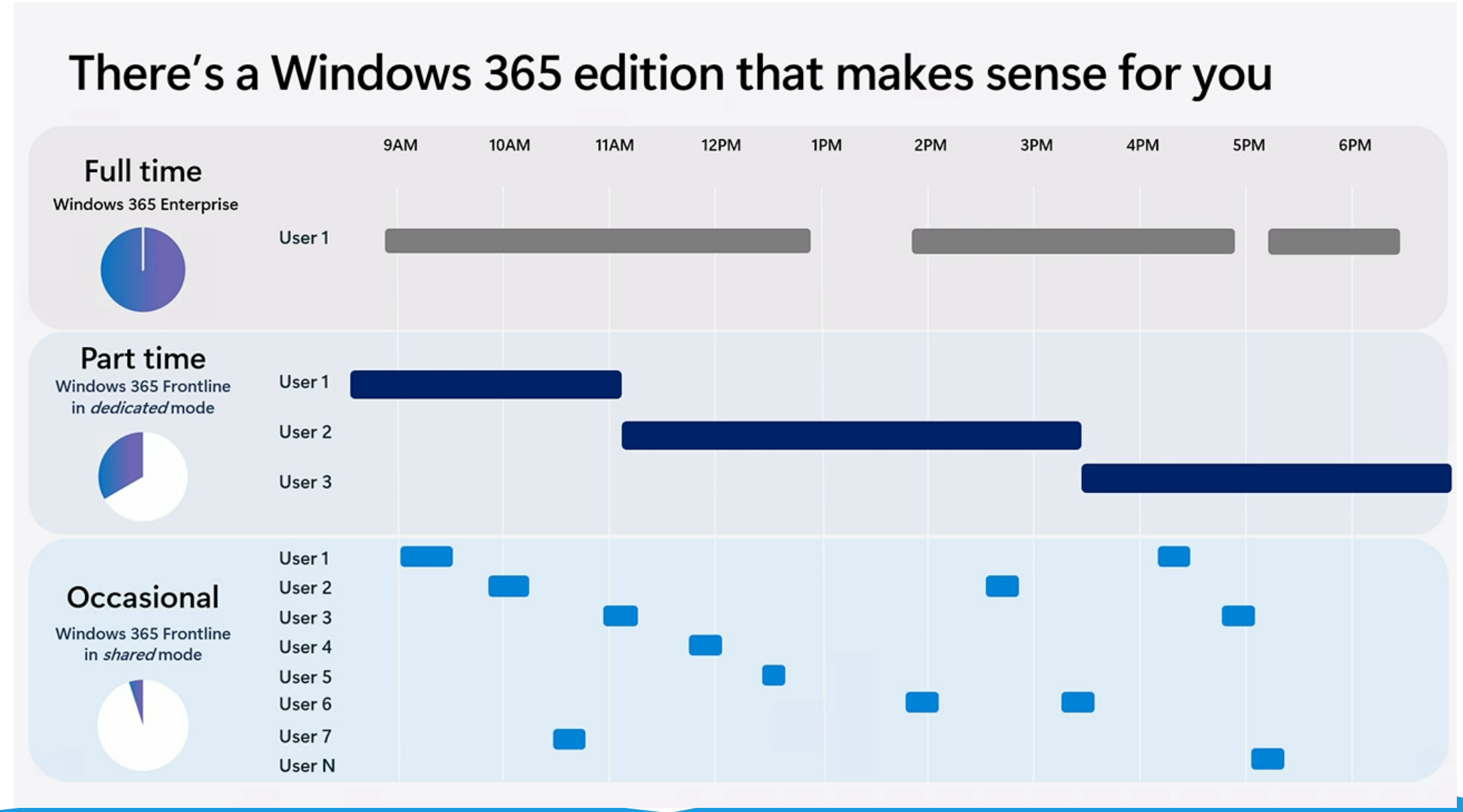
Windows 365 Enterprise Frontline Dedicated

- Three cloud PCs for three users.
- Limit to one concurrent login.

Windows 365 Enterprise Frontline Shared

- One cloud PC per license.
- A pool of users share the cloud PCs for occasional usage.
- Used for Windows 365 Cloud Apps.

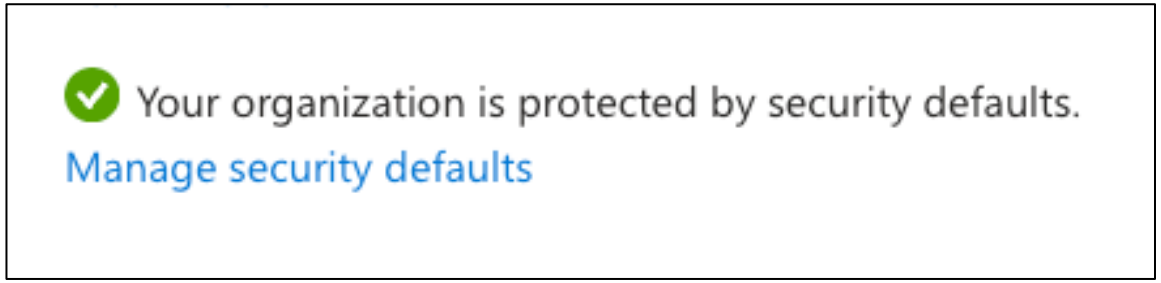
Windows 365 Use Cases

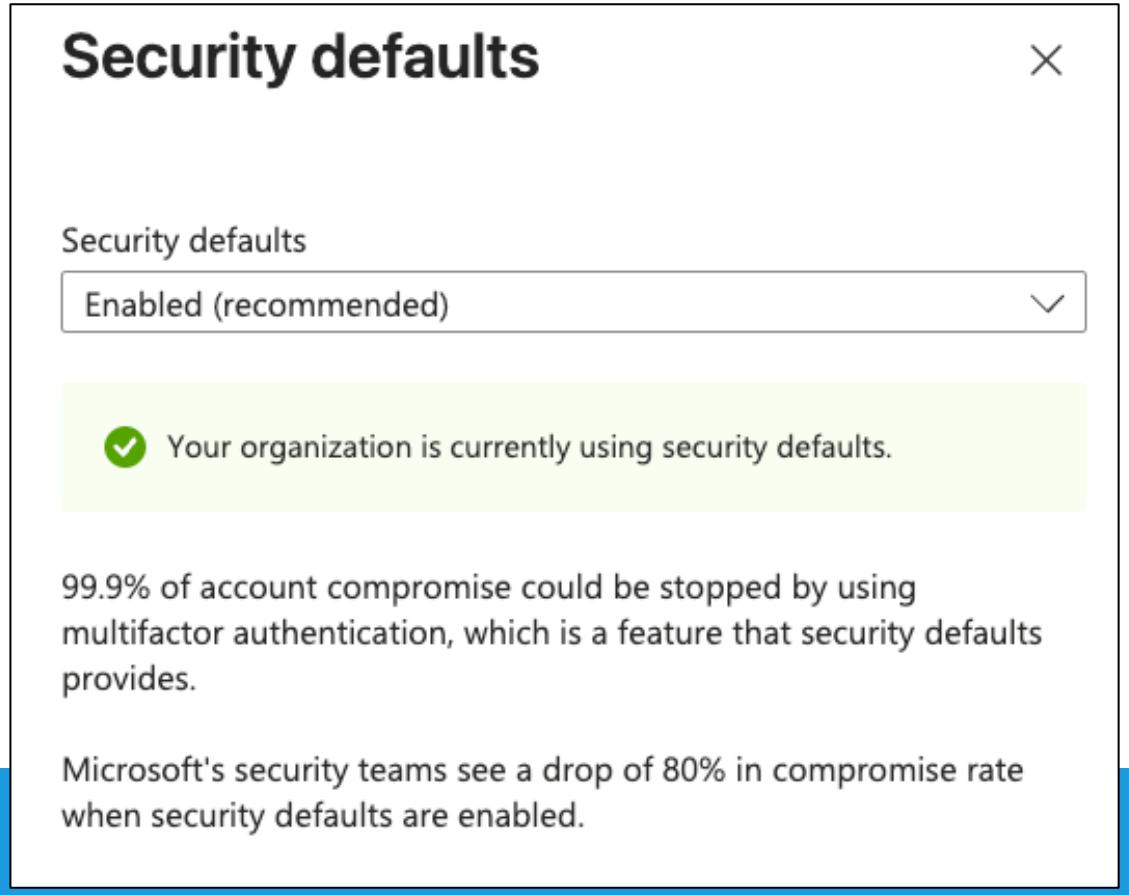


Identity and Authentication Best Practices

Authentication and Access

- Enforce MFA with Conditional Access policies
  - Do not use legacy, per-user MFA.
  - Conditional Access requires Entra P1 or P2.
  - Enable security defaults if Conditional Access is not available.





Authentication and Access

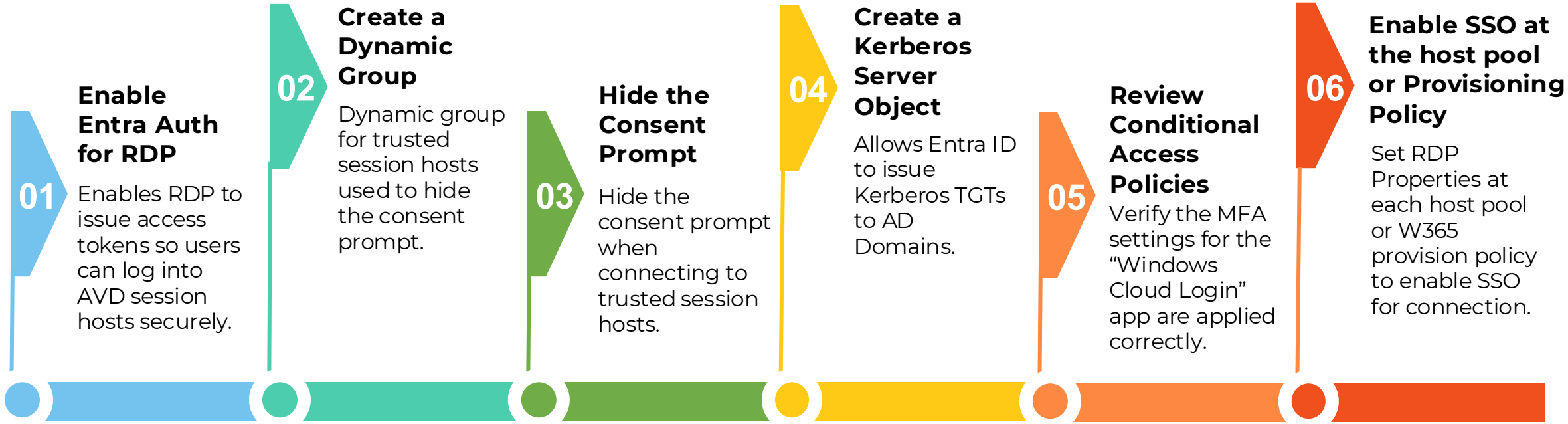
- Enforce MFA with Conditional Access policies
  - Do not use legacy, per-user MFA.
  - Conditional Access requires Entra P1 or P2.
  - Enable security defaults if Conditional Access is not available.
- Conditional Access policy targets:
  - Windows 365 authentication – ***Windows 365 or Cloud PC***, app ID 0af06dc6-e4b5-4f28-818e-e78e62d137a5
  - AVD gateway authentication - ***Azure Virtual Desktop***, app ID 9cdead84-a844-4324-93f2-b2e6bb768d07
  - User authentication to a session host with SSO - ***Windows Cloud Login***, app ID 270efc09-cd0d-444b-a71f-39af4910ec45
- Entra Kerberos authentication for Azure Files - **Exclude** the application representing a storage account from conditional access policies.
  - App name: [Storage Account] <your-storage-account-name>.file.core.windows.net.

Authentication and Access

- Configure Conditional Access Restrictions
  - Device compliance.
  - Geolocation/IP filtering.
  - User and sign-in risk (requires P2).
- Use passwordless authentication
  - Windows Hello for Business.
  - FIDO2 security keys.
  - Microsoft authenticator app.
- Use a KDC Proxy if using Smart card authentication
  - Smart cards require ”line of sight” to AD domain controllers.
  - KDC Proxy allows authentication for RDP over a public network.

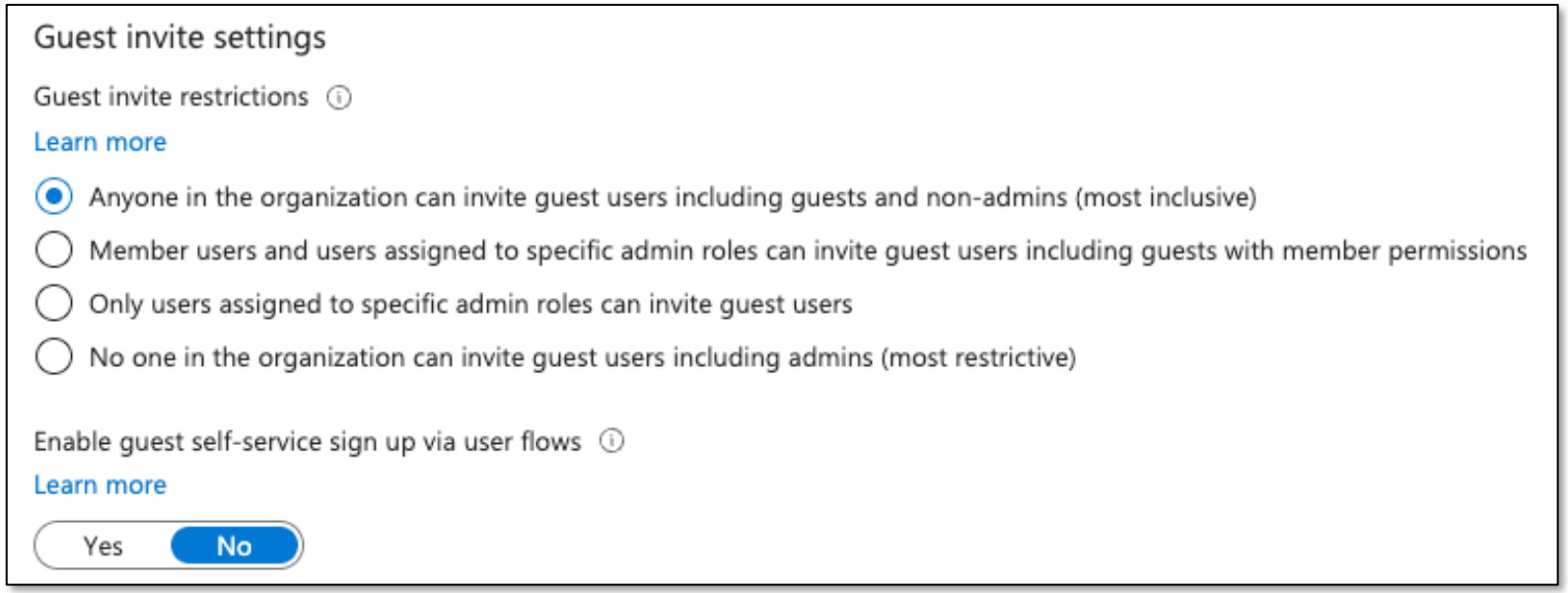
Single sign-on for AVD and W365

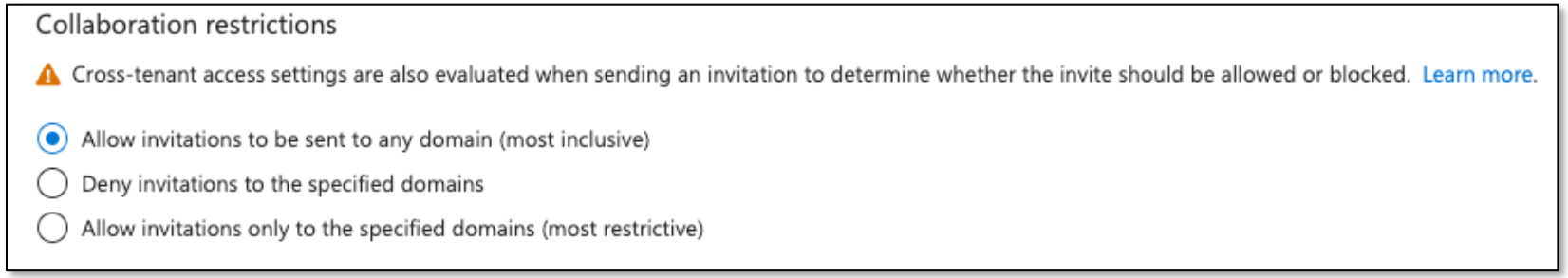
- Bypass the second password.
- Required for external identities (B2B) & Windows 365 Link.



External Identities

- Review the tenant's external identity settings.





Links:

youtube.com/@Ciraltos

AVD + Entra ID Guest Users
bit.ly/4pgRprf

AVD Single Sign-on
bit.ly/4suUQxE

Entra-only Identities with FSLogix
bit.ly/49J6dth

Thank you!

Questions?

Session feedback available in home feed of the app after the session

run events

MC2MC

CONNECT