

WHAT ABOUT THAT ENTRA ID?

The CDE may occupy one corner of the environment. Entra ID can still hold the keys to the doors, the badge printer, the emergency entrance, and several robots nobody invited to the access review.

PRACTITIONER POSITION

My practitioner position is that Microsoft Entra ID is difficult to assess because it is not one system, one population, one access list, or one control. It is an identity plane that can authenticate people, represent workloads, synchronize identities, evaluate Conditional Access, activate privileged roles, issue tokens, broker federation, carry guest relationships, and expose several distinct authorization systems. The assessment should therefore begin with the capabilities and paths that reach, connect into, administer, or can impact the security of the CDE—not with the entire tenant by default, and not with a short export of users assigned to one payment application. Microsoft provider assurance can support reliance on provider-operated services; it does not establish that the assessed entity's tenant configuration, role model, policy targeting, identity lifecycle, workload credentials, emergency access, hybrid dependencies, monitoring, retention, or evidence is compliant. The assessable object is the bounded identity path and its operating history.

THE FIELD PATTERN

WHAT THIS LOOKS LIKE IN PRACTICE

The assessed entity produces an Entra user export, a screenshot showing Conditional Access is enabled, a list of Global Administrators, and Microsoft's compliance materials. The CDE application uses enterprise groups. Azure administrators receive eligible subscription roles through PIM. A deployment pipeline authenticates through a service principal. A managed identity can read a payment-related vault. Contractors arrive as guests. Emergency accounts are excluded from normal policies. On-premises Active Directory synchronizes users and groups into the tenant. Nobody has joined these facts into one population or shown which policy, role store, scope, activation, credential, log, owner, and review applies to each path. Every artifact may be authentic. Together they still do not prove the identity claim.

SIGNALS DETECTED

WHAT SHOULD MAKE YOU STOP

- The assessment population is described as either 'the whole tenant' or 'users assigned to the payment app,' with no capability-based boundary between those extremes.
- Microsoft Entra directory roles, Azure resource roles, and application roles or permissions are flattened into one access-review spreadsheet.
- Group-based access is listed without resolving nested membership, dynamic membership, guests, synced objects, role-assignable groups, or the effective privileges inherited at the assessment date.

- A Conditional Access policy screenshot substitutes for policy state, targeting, exclusions, conditions, grant controls, report-only status, authentication strength, and observed evaluation results.
- PIM eligibility is treated as no access, even though activation creates time-bound capability that must be reconstructed and reviewed during the period.
- Service principals, managed identities, federated workload identities, certificates, secrets, and application permissions are omitted because the access review was built around human users.
- Emergency access accounts are absent from normal control evidence because they are intentionally excluded from ordinary dependencies and Conditional Access restrictions.
- Hybrid synchronization or federation appears nowhere in the CDE diagram even though on-premises identities, groups, agents, or federation services can change or authenticate access used by the CDE.
- Sign-in, audit, provisioning, service-principal, managed-identity, Conditional Access, and PIM data are requested after their native retention window has expired.
- A premium feature or green portal result is treated as proof without establishing the licensed coverage, configuration, population, period, exception handling, and evidence behind it.

WHY IT MATTERS

THE COST OF LEAVING IT UNEXPLAINED

Start with capability, not tenant membership. A tenant can contain thousands of identities unrelated to payment security, while one workload identity or synchronized administrative group outside the obvious application list can still affect the CDE. Bound the population by actual authentication, authorization, administration, deployment, recovery, secret, policy, directory, and logging capabilities. Record unrelated populations as excluded with a defensible reason rather than silently ignoring them or sweeping the entire tenant into scope without analysis.

Entra authentication and authorization are layered. A human or workload presents an identity; policies evaluate signals and targeting; groups may add membership; Microsoft Entra roles govern directory resources; Azure RBAC governs Azure resources at management-group, subscription, resource-group, or resource scope; applications may interpret their own roles, groups, scopes, and permissions. A defensible access claim identifies which decision point grants which capability over which resource. One column named 'role' cannot carry that story.

The control is time-shaped. Permanent assignments, eligible assignments, PIM activations, access packages, guest relationships, group changes, consent grants, credential additions, Conditional Access changes, emergency-account use, and sign-in decisions can alter effective access during the assessment period. Current-state exports are necessary but insufficient when the claim covers a period. Native Entra retention varies by log and license; the evidence design must preserve the events required for the organization's assessment and operating commitments before those events expire.

Human and workload identities need different tests. A service principal does not attend security awareness training or respond to an MFA challenge. Its control story may depend on workload identity federation, managed identity, certificate or secret lifecycle, permission grants, Conditional Access for workload identities where applicable, use telemetry, ownership, and a removal path. Applying a human access checklist to robots creates a reassuringly complete worksheet about the wrong population.

Provider compliance and tenant compliance are different claims. Microsoft can operate an assessed service while the customer still owns tenant configuration, identity inventory, privilege design, policy targeting, access reviews, customer-managed credentials, hybrid components, monitoring, retention, exceptions, and the evidence used in its PCI DSS assessment. The provider relationship changes the responsibility map; it does not eliminate the need to assess the customer's use of the identity plane.

QUESTIONS

QUESTIONS THAT EXPOSE THE WACK

- 01 Which human, guest, emergency, service-principal, managed, and federated workload identities can authenticate to, administer, deploy, recover, monitor, or otherwise impact the security of the CDE?
- 02 For each capability, which decision point grants it: directory role, Azure RBAC role, group membership, application role, delegated permission, application permission, access package, token claim, local application authorization, or another mechanism?
- 03 What is the effective scope of each assignment, including tenant, administrative unit, management group, subscription, resource group, resource, application, API, vault, pipeline, and environment?
- 04 Which assignments are permanent, eligible, activated, inherited, nested, dynamic, synced, guest-based, consented, or emergency-only-and what history reconstructs their effective state during the period?
- 05 Which Conditional Access policies actually target each in-scope path, and what do policy state, exclusions, conditions, authentication strength, grant controls, session controls, and sign-in evaluation show?
- 06 Which on-premises directories, synchronization agents, federation services, privileged groups, service accounts, or recovery dependencies can change or authenticate identities used by the CDE?
- 07 Which evidence sources preserve sign-ins, directory changes, provisioning, workload authentications, PIM activations, consent, credential changes, policy decisions, access reviews, and emergency-account use for the required period?
- 08 Which licenses and integrations make the intended controls and retention available, and how is the entity handling a control or evidence need that the current license does not provide?
- 09 What provider-operated activity is supported by current Microsoft assurance, and which tenant configuration, customer operation, monitoring, review, and evidence duties remain with the assessed entity?
- 10 What identity, role, group, application, permission, policy, federation, license, logging, or architectural change automatically reopens the scope and access claims?

THE CLUSTER OF WACK

FIND / MAP / EXPLAIN / REDUCE / PROVE

ESCAPE THE WACK

01 / FIND

Inventory identities as actors and capabilities, not just directory objects. Include human users, guests, emergency accounts, groups, service principals, managed identities, federated workload identities, app registrations, credentials, directory roles, Azure roles, application roles and permissions, Conditional Access policies, PIM, access reviews, hybrid synchronization and federation, logs, licenses, owners, and relied-upon Microsoft services.

02 / MAP

Build an identity-plane graph from subject to authentication method, policy evaluation, group or consent path, role or permission, scope, target resource, CDE-relevant capability, provider/customer responsibility, owner, evidence stream, retention, exception, and reopening trigger. Draw hybrid sources and emergency paths on the same map, even when they bypass ordinary flows by design.

03 / EXPLAIN

Write one bounded claim for each materially distinct path: who or what can do which action to which resource, through which authorization plane, under which policy and time condition, for which period, supported by which evidence. Separate Microsoft's service assurance, the entity's representation, and the assessor's testing and conclusion.

04 / REDUCE

Remove unused applications, stale service principals, broad consent, excessive directory and Azure roles, unnecessary permanent assignments, uncontrolled guest paths, long-lived secrets, policy exclusions, nested indirection, duplicate federation paths, and retention gaps. Simplify only after preserving the facts and owners needed to explain the change.

05 / PROVE

Select representative paths by meaningful variation-human, workload, privileged, guest, emergency, hybrid, permanent, eligible, and exceptional where present. Reconstruct each path from assignment and policy through actual authentication or activation, target capability, logging, review, exception handling, and revocation. Then reconcile the result to the system inventory, data and influence diagrams, vulnerability and penetration-test boundaries, provider matrix, claims ledger, and report language.

THE FIELD LAW

THE LINE WORTH REMEMBERING

ONE TENANT IS NOT ONE POPULATION. ONE EXPORT IS NOT ONE IDENTITY STORY.

Download the Entra Identity Plane Assessment Map. Trace one human path, one workload path, one privileged activation, and one emergency or hybrid path from identity source to effective CDE-relevant capability and retained evidence. If the map cannot name the authorization plane, scope, policy decision, time condition, owner, and proof, the access claim is not ready for assessment.

TECHNICAL GROUNDING

START WITH THE SOURCE MATERIAL

These references ground the practitioner interpretation. They do not turn the metaphor or method into official PCI DSS terminology.

- WACK-SOURCE-0001 / PCI DSS v4.0.1 / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0036 / Information Supplement: PCI SSC Cloud Computing Guidelines v3 / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0044 / FAQ 1454: What is the intent of administrative access in PCI DSS? / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0045 / FAQ 1591: MFA and access into the CDE / PCI Security Standards Council / [Open source](#)
- WACK-SOURCE-0046 / Overview of role-based access control in Microsoft Entra ID / Microsoft / [Open source](#)
- WACK-SOURCE-0047 / Azure roles, Microsoft Entra roles, and classic subscription administrator roles / Microsoft / [Open source](#)
- WACK-SOURCE-0048 / Application and service principal objects in Microsoft Entra ID / Microsoft / [Open source](#)
- WACK-SOURCE-0049 / Microsoft Entra Conditional Access overview / Microsoft / [Open source](#)
- WACK-SOURCE-0050 / Conditional Access for workload identities / Microsoft / [Open source](#)
- WACK-SOURCE-0051 / Microsoft Entra data retention / Microsoft / [Open source](#)
- WACK-SOURCE-0052 / View audit history for Microsoft Entra roles in Privileged Identity Management / Microsoft / [Open source](#)
- WACK-SOURCE-0053 / Manage emergency access admin accounts in Microsoft Entra ID / Microsoft / [Open source](#)
- WACK-SOURCE-0054 / Authentication for Microsoft Entra hybrid identity solutions / Microsoft / [Open source](#)

AUTHORITY CLASSIFICATION / PCI_SSC_SOURCE / PRACTITIONER_POSITION / PRACTITIONER_METHOD / AI_ASSISTED

Practitioner reviewed by Scott Norton on 2026-09-09 against canonical digest

cdf2f21b0311070b691ebf9b27ffe1067e520feeda5b8d9f91cb9b05b533c59a. Educational content, not a compliance determination. Independent practitioner resource; not affiliated with or endorsed by PCI SSC. Authorship and authority classification do not determine legal intellectual-property ownership.