ScrambleID + Microsoft Entra ID: External Authentication Methods for Phishing-Resistant SSO

Buyer's Guide / Last updated 2026-06-11 / https://www.scrambleid.com/learn/scrambleid-with-microsoft-entra-id-deployment-pattern

In one sentence: ScrambleID layers on top of Microsoft Entra ID as either an external authentication method (EAM) for phishing-resistant MFA and step-up, or a federated identity provider for phishing-resistant primary authentication, adding voice/contact-center verification, AI agent identity, and shared-device login while Entra ID continues to handle Conditional Access, user lifecycle, and Microsoft 365 application gating.

TL;DR (canonical)

- **You keep Entra ID.** ScrambleID does not replace it. ScrambleID integrates either as an external authentication method registered in Entra ID (satisfying the MFA or step-up factor), or as a federated identity provider that Entra ID delegates the full authentication ceremony to, which is the pattern for phishing-resistant primary authentication.
- **Conditional Access stays in Entra ID where it should.** Network zones, device compliance, sign-in risk, and application-specific policies continue to live in Entra ID. ScrambleID enforces phishing-resistance at the ceremony layer; Entra ID enforces conditional rules at the access layer.
- **ScrambleID adds what Entra ID doesn't natively cover at depth:** voice channel authentication for contact centers, in-person people verification, AI agent and machine identity with Proof of Possession, and frontline shared-device login.
- **User identity stays synced via Entra ID as the system of record.** SCIM provisioning anchors ScrambleID's `suid` to the user's Entra ID `objectId`. Lifecycle events (hire, transfer, terminate) flow from Entra ID into ScrambleID automatically.
- **Typical deployment lands in 2-4 weeks.** Most calendar time goes to user enrollment and the careful retirement of weak fallbacks, not to integration engineering.

Why an Entra ID-anchored organization adds ScrambleID

Microsoft Entra ID (formerly Azure AD) is the IdP for the majority of Microsoft 365 organizations and a substantial share of broader enterprises. It does federation, lifecycle, Conditional Access, and

Microsoft application access extremely well. What it does not natively cover at depth:

- **Voice / contact-center authentication.** Entra ID's authentication strengths cover web, mobile, and certificate-based scenarios. Inbound calls to a contact center, where the caller needs cryptographic verification before an agent acts, are not in Entra ID's native scope.
- **AI agent and machine identity at scale.** Entra ID has managed identities for Azure workloads, supports workload identity federation, and Microsoft Entra Agent ID (announced 2025) brings directory registration and governance to AI agents. ScrambleID complements that layer with per-action cryptographic proof for agents operating across clouds and third-party surfaces beyond the Microsoft estate.
- **In-person and people verification.** When two people need to verify each other (executive verification, supplier authentication, vendor onboarding), there is no native Entra ID flow. Teams default to email or phone confirmation, which fail under social engineering.
- **Frontline shared-device login.** Entra ID supports shared-device modes for some Microsoft applications. ScrambleID Desktop provides cryptographic shared-device tap-in/tap-out across any Windows or macOS workstation, including non-Microsoft applications and clean rooms.
- **Phishing-resistant primary authentication enforced as default.** Entra ID supports FIDO2 security keys, Windows Hello for Business, and certificate-based authentication. Most deployments still permit OTP or push as fallbacks. ScrambleID enforces phishing-resistant primary authentication by default and explicitly rejects weak fallbacks for high-risk actions.

ScrambleID extends Entra ID into channels and use cases Entra ID was not built around. The integration preserves the Entra ID investment while adding coverage Microsoft does not provide natively.

The two integration patterns

Pattern A: ScrambleID as an external authentication method (EAM)

Microsoft Entra ID supports External Authentication Methods, a model where a third-party authentication provider registers as an MFA or step-up factor inside Entra ID. ScrambleID can register as an EAM so users authenticating to Entra ID-protected applications complete the ScrambleID ceremony as the MFA factor in the sign-in flow. If you want ScrambleID to carry phishing-resistant primary authentication end to end, use the federation model instead (ScrambleID as a federated identity provider that Entra ID delegates the full ceremony to).

This pattern fits when:

- You're an Entra ID-first organization and you want a phishing-resistant MFA factor tied to Entra ID's existing application access policies.
- You want Conditional Access to evaluate the result of the ScrambleID ceremony in its policy decisions.

- You want the user experience to feel native to Entra ID sign-in.

Flow:

1. User navigates to a Microsoft 365 application (or any Entra ID-protected SAML/OIDC application).
2. Entra ID begins the sign-in flow and routes the user to ScrambleID per the configured EAM policy.
3. ScrambleID runs the WebAuthn or QR-based confirmation ceremony, producing a signed assertion.
4. Entra ID consumes the assertion, evaluates Conditional Access policies (network, device compliance, sign-in risk, application context), and issues its standard session token.
5. The application sees Entra ID's standard SSO; nothing changes downstream.

What Entra ID keeps owning: Conditional Access, application access, lifecycle management, B2B / B2C tenancy, license management, audit (Microsoft Graph activity logs).

What ScrambleID owns: the cryptographic authentication ceremony, device enrollment, the ScrambleID app, recovery flows, and the channels Entra ID doesn't cover natively (voice, agent, people verification, frontline).

Pattern B: ScrambleID alongside Entra ID for non-web channels

Entra ID continues to handle web/mobile authentication for Microsoft 365 and Entra ID-protected applications directly. ScrambleID handles voice (Caller Auth), AI agent identity, people verification, and frontline shared-device login as parallel channels that share user identity with Entra ID.

This pattern fits when:

- Web/mobile authentication via Entra ID + Conditional Access is already strong and you don't want to change it.
- You're solving for the contact center, AI agent platform, in-person verification, or shared-device login first.
- You want ScrambleID to extend coverage to channels Entra ID doesn't address rather than replace what Entra ID does well.

The voice flow is illustrative: the caller dials the IVR, the IVR collects account context and asks ScrambleID to open a verification session, and when the caller's number matches an enrolled device, the ScrambleID app on that device receives a push confirmation the caller approves with one tap. When there's no match, the IVR speaks a Dynamic Identifier and the caller confirms it in the app instead. Either way, ScrambleID returns a signed verification result and the IVR routes the call (or the agent's screen displays the verified state) before any sensitive action.

The two patterns can coexist. A common deployment is Pattern A for web (so Entra ID sign-ins gain a phishing-resistant factor) plus Pattern B for voice, agent, and ScrambleID People (so coverage extends beyond what Entra ID natively addresses).

How user identity stays in sync

ScrambleID and Entra ID both reference the same human users; they need a stable cross-system identifier. The recommended pattern:

- **Entra ID is the system of record for user identity.** User creation, group membership, lifecycle events (hire, transfer, terminate) happen in Entra ID or are synced to Entra ID from the HR system through the Microsoft Graph or HR connectors.
- **SCIM provisions users from Entra ID to ScrambleID.** A SCIM connection establishes ScrambleID's `suid` for each user, anchored to the Entra ID `objectId` (the immutable per-user identifier in Entra ID).
- **Group memberships propagate.** ScrambleID's policy can reference Entra ID groups (e.g., "require dual approval for all members of the Production Deploy Approvers group", a rule Lockstep, in development, is designed to enforce).
- **Lifecycle events propagate.** When Entra ID disables or deletes a user, ScrambleID retires every enrolled `zid` against that user's `suid` automatically.

There is no parallel directory. If a user is offboarded in Entra ID, all of their ScrambleID-enrolled devices are retired in the same lifecycle event.

Conditional Access interplay

Microsoft Entra ID Conditional Access is one of the strongest policy engines in any IdP. ScrambleID is designed to complement it, not duplicate it.

Policy decision	Where it lives	Example
Whether the user can access the application	Entra ID Conditional Access	"Block sign-in from non-compliant devices for production-tagged applications."
Whether the network is trusted	Entra ID Conditional Access	"Require MFA from outside the corporate network."
Whether the device is compliant	Entra ID + Intune	"Require Intune-managed and compliant device."
Whether the sign-in is risky (Identity Protection signals)	Entra ID Identity Protection	"Block sign-in when risk level is high."
Whether the authentication ceremony is phishing-resistant	ScrambleID	"Origin-bound WebAuthn or session-bound QR(DID); no SMS/voice OTP for high-risk policies."
Whether step-up is required for a sensitive action	ScrambleID (XFactor, in development)	"Wire-transfer approval requires WebAuthn UV plus hardware key."
Whether dual control is required	ScrambleID (Lockstep, in development)	"Production deploy requires two distinct approvers within 30 minutes."
Whether voice flows allow KBA	ScrambleID	"Caller Auth replaces KBA for all account changes."

Policy decision	Where it lives	Example
Whether AI agents can call sensitive tools	ScrambleID (Agent Tool-Access Rings)	"Agents in Ring 4 require human approval before payment APIs."

The division of labor: Conditional Access answers "who is allowed to access what under which conditions"; ScrambleID answers "is this authentication moment phishing-resistant and does this specific action need higher assurance." Both layers are needed; neither does the other's job.

Risk signal correlation: Entra ID Identity Protection + ScrambleID Overwatch

Microsoft Entra ID Identity Protection produces risk telemetry today; ScrambleID Overwatch (in development) is designed to produce the complementary half across ScrambleID surfaces. The patterns below describe the integration design.

- **Entra ID Identity Protection detects:** anomalous sign-in locations, password spray patterns, leaked credentials, suspicious user-agent strings, impossible travel, unfamiliar sign-in properties.
- **ScrambleID Overwatch is designed to detect:** wrong-DID bursts in voice flows, origin mismatches in QR(DID) confirmations, PoP failures on machine identities, Trust Check anomalies in people verification flows, agent tool-call patterns matching prompt-injection signatures, cross-channel correlation patterns.

A real cross-channel attack often traverses both surfaces. An attacker phishes a credential (Identity Protection signal: leaked credential, anomalous IP), then calls the helpdesk to recover MFA (Overwatch signal: caller cannot complete DID confirmation, wrong-code retries). Independently, each signal might not breach a threshold; correlated, they're a clear attack pattern.

The planned integration: ScrambleID Overwatch will be able to ingest Microsoft Graph sign-in logs and Identity Protection risk events as signals. Entra ID will be able to consume ScrambleID Overwatch alerts via webhook to trigger Conditional Access remediation, Microsoft Sentinel automation, or Logic Apps workflows.

For the deeper risk-engine architecture, see Overwatch: Unified Identity Risk Monitoring.

Deployment timeline (typical)

Week	Activity	Owner
1	Federation or EAM configured. SCIM provisioning enabled. Pilot user group selected.	IAM team + ScrambleID solutions engineer
2	Pilot users enroll on the ScrambleID app. Pattern A or Pattern B activated for the pilot scope. Conditional Access policies updated to incorporate the new authentication	IAM team + pilot users

Week	Activity	Owner
	method.	
3	Pilot expansion. Voice channel (if Pattern B) integrated with the IVR platform. Risk-alert rules tuned against pilot baseline (Microsoft Graph ingestion into Overwatch correlation lands when Overwatch ships).	IAM team + contact-center ops
4+	Phased rollout to remaining workforce. Recovery flows validated. Old fallbacks (KBA, OTP, push without number matching) progressively retired.	IAM team + change management

Larger or more complex Entra ID tenancies (multi-region, B2B / B2C parallel tenants, deeply customized Conditional Access) extend this timeline. Smaller tenancies compress it. Federation and EAM setup itself is days, not months.

Microsoft 365 specific considerations

For organizations whose Entra ID is anchored to Microsoft 365 (the most common case), a few specifics:

- **Microsoft 365 application access** continues through Entra ID's standard OIDC flow with the ScrambleID-enforced authentication ceremony.
- **Outlook, Teams, SharePoint, OneDrive** users see no application change. The sign-in once at Entra ID-level applies.
- **Conditional Access policies** for sensitive applications (admin portals, finance applications, exchange admin) remain enforced and can be tightened to require the phishing-resistant ScrambleID ceremony specifically.
- **Privileged Identity Management (PIM)** continues to gate just-in-time elevation for admin roles. ScrambleID Lockstep (in development) is designed to complement PIM by requiring dual approval for the most sensitive role activations.
- **Windows Hello for Business** continues to work for managed devices. ScrambleID Desktop addresses unmanaged devices, shared workstations, and non-Microsoft-anchored scenarios.

What this does not change

- **Entra ID remains the IdP of record.** Applications integrated with Entra ID continue to integrate with Entra ID. Federation contracts, claim mappings, group rules, and Conditional Access policies do not need to be rebuilt.
- **Provisioning and deprovisioning** continue to flow through Entra ID as the system of record. ScrambleID does not become a parallel directory.
- **Application access policy** stays in Conditional Access. ScrambleID adds a phishing-resistance layer at the ceremony; it does not take over application gating.

- **Audit trail** continues to flow through Microsoft Graph activity logs. ScrambleID emits structured events that complement (not replace) Microsoft's audit data.

The net effect: Entra ID gets stronger primary authentication and gains coverage of channels it doesn't natively address, while remaining the central IdP. The investment in Entra ID and Microsoft 365 is preserved.

Common questions

Does ScrambleID replace Entra ID?

No. ScrambleID layers on top of Entra ID. Entra ID continues to be the IdP, the provisioning system, the policy engine for Conditional Access, and the audit system of record. ScrambleID adds phishing-resistant primary authentication and extends coverage to channels Entra ID doesn't natively address.

How does ScrambleID register as an External Authentication Method?

ScrambleID registers as an EAM through the standard Microsoft EAM enrollment flow, configured in the Entra ID admin console under Authentication Methods. Once registered, ScrambleID can be applied selectively to user populations through Authentication Methods policies and referenced in Conditional Access policies as a satisfied factor.

What about Entra ID free vs Premium P1 vs Premium P2 licensing?

Which authentication-method, Conditional Access, and Identity Protection features your tenant can use depends on your Entra ID tier and Microsoft's current packaging; check Microsoft's licensing documentation for the features each pattern relies on. The ScrambleID integration itself doesn't introduce additional Microsoft licensing requirements.

How does ScrambleID interact with Windows Hello for Business?

They are complementary. Windows Hello for Business is excellent for same-device authentication on managed Windows workstations. ScrambleID extends beyond that scope: cross-device QR-based login, voice/contact-center, AI agent identity, people verification, shared workstations, and macOS / Linux / mixed-device scenarios. Where both apply, the deployment chooses Windows Hello for managed Windows endpoints and ScrambleID for everything else.

Can we start with one channel and expand?

Yes. Most deployments begin with the highest-risk channel (often voice/contact center or executive web access) and expand from there. The architecture is built around channel modularity.

How does the recovery flow work in this architecture?

Recovery is handled by ScrambleID with full integration into the Entra ID lifecycle. Warm-path recovery (step-up from another enrolled device, the role XFactor, in development, is designed to fill) takes seconds. Cold-path recovery requires identity proofing appropriate to the assurance level the deployment demands; for high-risk users, dual approval gates the new device enrollment (Lockstep, in development, is designed to enforce this). Entra ID's existing self-service password reset, Identity Verification, and Authenticator app recovery flows can complement this for break-glass scenarios. See the full Recovery and Fallback Playbook.

What about Entra External ID (B2C)?

ScrambleID can act as a federated identity provider to Entra External ID for customer-facing applications. The most common B2C use case is replacing KBA in customer-facing call centers and, once Verify-Me (in development) ships, adding context-bound trust signals to customer communications. The integration model mirrors the workforce pattern with appropriate adjustments for consumer enrollment flows.

How does this affect Microsoft Sentinel and SOC operations?

ScrambleID Overwatch (in development) is designed to produce structured events that Microsoft Sentinel can ingest via standard log connectors or Logic Apps. This gives the SOC a unified view across Entra ID sign-in logs, Identity Protection alerts, and ScrambleID's cross-channel telemetry. The integration design is event-driven and bidirectional: Sentinel automation rules will be able to trigger ScrambleID actions (force re-authentication, initiate a dual-control approval, retire a device) based on correlated risk signals.

Key Takeaway

ScrambleID and Microsoft Entra ID integrate as a layered architecture, not a replacement. Entra ID remains the IdP, provisioning system, and Conditional Access policy engine; ScrambleID adds a phishing-resistant MFA factor via External Authentication Methods, phishing-resistant primary authentication via federation (Pattern A), and extends coverage to voice, AI agent, person-to-person, and frontline shared-device channels Entra ID doesn't natively address (Pattern B). User identity is synced via SCIM with Entra ID's `objectId` as the anchor. Risk signals from Entra ID Identity Protection and ScrambleID Overwatch (in development) are designed to correlate via Microsoft Graph and webhook integration. Typical deployment lands in 2-4 weeks. The investment in Entra ID and Microsoft 365 is preserved while phishing-resistant authentication is added on top.

References (public)

- Microsoft Entra ID External Authentication Methods documentation: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-external-method-manage
- Microsoft Entra ID Conditional Access overview: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview
- Microsoft Entra ID Identity Protection: https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection
- Microsoft Entra ID SAML federation: https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-fed-saml-idp
- Microsoft Entra ID SCIM provisioning: https://learn.microsoft.com/en-us/entra/identity/app-provisioning/use-scim-to-provision-users-and-groups
- CISA Phishing-Resistant MFA Fact Sheet: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- W3C WebAuthn Level 2: https://www.w3.org/TR/webauthn-2/

Related reading

- ScrambleID Architecture: One Identity Fabric Across Web, Voice, People, Desktop, and Machines
- ScrambleID + Okta: How They Work Together
- Phishing-Resistant Web Authentication: Passkeys, QR Login, and the Patterns That Actually Work
- SSO Integration Quickstart (SAML + OIDC)
- Caller Authentication: Replace KBA and Stop Vishing
- Overwatch: Unified Identity Risk Monitoring
- Recovery and Fallback Playbook
- Compliance Mapping: NIST 800-63 + CISA Phishing-Resistant MFA