ENTERPRISE PROGRAM BRIEF

Microsoft Entra Identity Administration Foundations

Administer identities and scoped access in an isolated training tenant.

VNode ITeS | F12

DURATION	LEVEL	FORMAT
24 hours	Foundation	Private cohort

AUDIENCE PROFILE

Built for these roles

Cloud administrators, Security practitioners

OVERVIEW

Executive overview

Administer identities and scoped access in an isolated training tenant. Proposed instructor-led duration; delivery subject to environment and lab validation.

READINESS

Prerequisites

- Basic tenant administration and cloud concepts

PROGRAM OUTCOMES

Capabilities your teams will gain

- Administer isolated user, group and application identities
- Diagnose a sign-in or permission failure from evidence
- Test safely scoped policy and remove obsolete access
- Explain consent, recovery and identity lifecycle responsibilities

ENTERPRISE CUSTOMIZATION

Enterprise customization

Tailor this program to your organization's priorities: Administer identities and scoped access in an isolated training tenant.

- Private cohort scheduling
- Equivalent-experience entry review

CURRICULUM

Curriculum roadmap

1

MODULE 1 · 6 HOURS

Tenant and identity fundamentals

Create test personas and map administrative responsibilities.

- Users and groups
- Roles
- Administrative scope
- Test-tenant boundaries

2

MODULE 2 · 6 HOURS

Authentication and access policy

Evaluate an access policy with test identities and document recovery arrangements.

- MFA concepts
- Conditional Access
- Emergency access
- Report-only testing

3

MODULE 3 · 6 HOURS

Application identities and permissions

Register a sample application and compare permission flows.

- App registrations
- Service principals
- Delegated versus application permissions
- Consent

4

MODULE 4 · 6 HOURS

Identity lifecycle and review

Investigate a denied sign-in and remove obsolete access in the scenario.

- Joiner mover leaver
- Credential lifecycle
- Sign-in logs
- Access reviews and entitlement checks

PREPARATION

Environment prerequisites

Isolated Entra tenant and test users/apps Roles for the required administrative operations Applicable Conditional Access/governance/agent entitlements Emergency access and recovery plan Delivery depends on environment and lab validation. This outline does not include step-by-step lab instructions.

CAPSTONE

Capstone

Investigate a denied sign-in and remove obsolete access in the scenario. Assessed identity administration record Evidence of relevant access, quality and risk controls Demonstration and limitations record

ASSESSMENT

Assessment

Scenario-based practical assessment Administer isolated user, group and application identities 30% Diagnose a sign-in or permission failure from evidence 25% Test safely scoped policy and remove obsolete access 25% Explain consent, recovery and identity lifecycle responsibilities 20% Proposed VNode outline-level assessment; no vendor accreditation or completed lab validation implied.

DELIVERABLES

Participant deliverables

- Assessed identity administration record
- Evidence of relevant access, quality and risk controls
- Demonstration and limitations record

SCOPE

Scope boundaries

Step-by-step lab instructions; Runnable solution code; Packaged source datasets; Executed environment validation

DELIVERY

Delivery options

Count teaching hours, not calendar days. Exclude breaks. Split into 4-hour or 8-hour teaching sessions; schedule complex project work in contiguous blocks. Proposed hours exclude breaks and are subject to pilot validation.

PRIVATE DELIVERY

Plan a private cohort for your team

Scope delivery format, role mix, and rollout timeline with our solutions team.

Plan Private Delivery

Book advisory call