

Conditional Access Design

ARC404

Design a Conditional Access policy set you can defend. Read an access decision from the sign-in record rather than reasoning about it, state what a policy actually covers as a number, structure a set somebody else can inherit, and change it without finding out what you broke from a user.

Modules	14
Lessons	62
Phases	5
Free preview	Course Orientation

The method

Conditional Access is a policy engine with an evaluation order, and most policy sets are written as if it were a list of rules. This course runs the same loop for every policy it builds.

1. Reason from the evaluation, not the intent. Every policy that applies to a sign-in is evaluated, and the strictest control wins. What you meant is not what the engine does.
2. Scope before condition. Who a policy applies to, and who is excluded, decides more about the outcome than any control on it. Exclusions are where policy sets go wrong quietly.
3. Choose a control you can explain the failure of. Every control blocks somebody eventually. Knowing who, and what they do next, is the difference between a policy and an outage.
4. Run it in report-only and read the result. Report-only tells you who would have been blocked, using real sign-ins rather than a whiteboard. It is the cheapest thing in this course and the most skipped.
5. Design the set, not the policy. Policies interact. A set assembled one policy at a time acquires gaps that no single policy review finds.

The output is a policy set with its exclusions documented and a break-glass path that has been tested rather than assumed.

What this course assumes

No minimum experience and no prerequisite course. The evaluation model, the difference between grant and session controls, and every condition type are explained where first used.

What makes it go faster: a Microsoft 365 tenant with Entra ID P1 or above, even a developer one, so you can build the policies alongside. Not required, and every policy is shown as JSON you can read without a tenant.

What this course does not cover: identity governance, privileged access management, and incident response to an identity compromise. Conditional Access is the enforcement point, and those are the disciplines either side of it.

Full syllabus

Course Orientation

Course Orientation [FREE PREVIEW](#)

What Conditional Access Design teaches: the evaluation engine that decides every sign-in, how scope and conditions and controls combine into one verdict, the policy set that covers a tenant without gaps or conflicts, and the testing, troubleshooting, and operating practice that keeps it working.

Phase 1: The Engine

The Evaluation Engine

How Conditional Access actually decides. Why the firewall mental model produces gaps, the two evaluation phases and what happens in each, the anatomy of a policy as assignments and access controls, what the three policy states change, how to read the verdict the engine writes for every sign-in...

1. 1.1 Conditional Access Is Not a Firewall
2. 1.2 The Two Phases: Collect, Then Enforce
3. 1.3 Anatomy of a Policy
4. 1.4 On, Off, and Report-Only
5. 1.5 Reading the Verdict
6. 1.6 Where Conditional Access Is Not in the Path
7. Module Summary
8. Check My Knowledge

Phase 2: The Policy

Scope and Assignment

Who a Conditional Access policy actually reaches.

1. 2.1 Scope Is Coverage
2. 2.2 Groups as the Scoping Instrument
3. 2.3 Directory Roles as a Target
4. 2.4 Guests and External Identities
5. 2.5 Workload Identities
6. 2.6 Exclusion Debt
7. Module Summary
8. Check My Knowledge

Conditions

The signals that decide when a policy fires.

1. 3.1 Conditions Narrow, They Do Not Strengthen
2. 3.2 Network and Named Locations
3. 3.3 Device Platform and Device Filters
4. 3.4 Risk as a Condition
5. 3.5 Client Apps and Legacy Authentication
6. 3.6 Authentication Flows
7. Module Summary
8. Check My Knowledge

Controls

What actually happens to a request that survives scope and conditions.

1. 4.1 Grant Controls: Block, Grant, and the And/Or Decision
2. 4.2 Authentication Strength
3. 4.3 Device and App Controls
4. 4.4 Session Controls
5. 4.5 Continuous Access Evaluation
6. 4.6 Token Protection and Resilience Defaults
7. Module Summary
8. Check My Knowledge

Phase 3: The Policy Set

Designing the Policy Set

Turning individual policies into a set somebody can inherit.

1. 5.1 The Policy Set as an Object
2. 5.2 Naming and What It Has to Carry
3. 5.3 The Baseline Layer
4. 5.4 Personas and Layering
5. 5.5 Authentication Contexts and Step-Up Access
6. 5.6 Reviewing and Evolving the Set
7. Module Summary
8. Check My Knowledge

Phase 4: Ship and Operate

Ship and Operate

Changing a policy set without breaking anybody.

1. 6.1 What If and What It Can Answer
2. 6.2 Report-Only as a Deployment Instrument
3. 6.3 The Deployment Sequence
4. 6.4 Diagnosing a Failure
5. 6.5 Policy as Code and Standing Measurement
6. 6.6 When It Has Gone Wrong
7. Module Summary
8. Check My Knowledge

Phase 0: Course Resources

Cheatsheets

How evaluation resolves, what each condition and control actually does, and the exclusions that quietly become the policy.

1. How Evaluation Actually Resolves
2. Scope, Conditions and Exclusion Debt
3. Controls, and What Each One Actually Stops
4. Designing the Set, and Shipping It

Cookbooks

Ordered procedures for building a policy set, shipping a change, auditing coverage, and clearing exclusion debt.

1. Building a Policy Set From Nothing
2. Shipping a Policy Change
3. Auditing What the Set Actually Covers
4. Clearing Exclusion Debt

Walkthroughs

Four cases reasoned end to end, including the policy that was enabled, correct, and evaluating nobody.

1. The Policy That Was Evaluating Nobody
2. The Lockout Report-Only Did Not Predict
3. The Sign-In Where MFA Was Satisfied
4. The Set Nobody Could Reason About

Playground

A free tenant, a policy set you build yourself, and the checks that make the practice real.

Operational Reference

Every portal path, Graph command, log query, specification and check from the Conditional Access Design course in one place, organized by task and linked back to the section that explains when not to use it.

1. Operational Reference

References & Further Reading

Where to check whether anything in this course has changed, what the live open questions are, which features are in preview, and the authoritative page for each class of fact.

Course Completion

Course Exam

Conditional Access Design end-of-course exam: a privileged sign-in the policy set was built to block, and a coverage figure that reported full protection while it happened.

1. Course Completion. Conditional Access Design

Generated 2026-09-01 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/conditional-access-design/