

Email Authentication and DMARC Enforcement

ARC405

Take a domain from unknown to enforced. Read a receiver's verdict from the message itself, find every system sending as you, get your platforms signing as your domain, and publish a policy that stops exact-domain spoofing without breaking legitimate mail. Built on the 2026 DMARC standard.

Modules	14
Lessons	56
Phases	5
Free preview	Course Orientation

The method

SPF, DKIM and DMARC are three records that produce one decision at the receiving mail server. This course runs the same loop for each of them, because most estates have all three published and none of them enforcing.

1. Read what the receiver actually does. The decision is made by somebody else's server against your published record. Reason from their evaluation, not from your intent.
2. Publish the record and read it back. An SPF record costing eleven DNS lookups against a limit of ten is broken with no mail flowing and no error anywhere.
3. Turn on reporting before enforcement. DMARC aggregate reports tell you who is sending as you. Moving to reject without reading them is how a legitimate sender gets blocked on a Monday morning.
4. Move the policy one step at a time. None to quarantine to reject, rehearsed first with the test flag the 2026 standard added and scoped by name rather than by percentage, with a reason to move recorded rather than a calendar date.
5. Operate it as configuration that drifts. A supplier restructures an include, a department buys a tool, a contract ends with the keys still published, and the record that was correct last quarter now authorizes something nobody told you about. A monthly diff and a ledger catch it; a ten-minute audit reads any other domain the same way.

What this course assumes

No minimum experience and no prerequisite course. DNS records, mail flow and the difference between the envelope sender and the visible From address are explained where they first matter.

What makes it go faster: access to your own DNS and a mailbox you can send test mail from. Neither is required, and every record in the course can be inspected against public domains.

What this course does not cover: mail server administration, spam filtering, and phishing investigation. This is the authentication layer and the policy decision on top of it.

Full syllabus

Course Orientation

Course Orientation [FREE PREVIEW](#)

What Email Authentication and DMARC Enforcement teaches: how a receiver reaches a verdict on a message, what SPF and DKIM each actually claim, why alignment decides whether either claim counts, and how to take a domain to enforcement without breaking legitimate mail.

Phase 1: The Decision

The Authentication Decision

How a receiver reaches a verdict on a message.

1. 1.1 Envelope and Header Sender Identities
2. 1.2 SPF, DKIM and DMARC: What Each Check Proves
3. 1.3 The Authentication-Results Header
4. 1.4 Identifier Alignment
5. 1.5 Policy Values and Receiver Handling
6. 1.6 Coverage Limits and Complementary Controls
7. Module Summary and Knowledge Check

Phase 2: The Two Claims

SPF: Authorizing Your Senders

The record that authorizes servers to send using your domain.

1. 2.1 SPF Record Syntax and Evaluation Order
2. 2.2 The DNS Lookup Limit
3. 2.3 Include Chains and Inherited Senders
4. 2.4 Record Design from a Sender Inventory
5. 2.5 Publishing and Verification
6. 2.6 SPF Coverage Limits
7. Module Summary and Knowledge Check

DKIM: The Signature That Travels

The record that travels with the message, built and operated: a signature dissected and verified by hand, keys generated and published, Microsoft 365 and Google signing as your domain end to end, a real failure diagnosed to its owner, rotation with the commands, and the replay case worked.

1. 3.1 What a Signature Commits To
2. 3.2 Selectors and Keys
3. 3.3 Getting Your Platforms to Sign as You
4. 3.4 What Breaks a Signature
5. 3.5 Key Rotation
6. 3.6 Replay, and Where DKIM Ends
7. Module Summary and Knowledge Check

Phase 3: The Policy

DMARC: Policy and Evidence

The record that ties the other two together and the reports that finally show what your domain sends.

1. 4.1 The Record and Its Tags
2. 4.2 Policy Discovery
3. 4.3 Publishing Your First Record
4. 4.4 Reading Aggregate Reports
5. 4.5 Failure Reports
6. 4.6 From Reports to Decisions
7. Module Summary and Knowledge Check

Phase 4: Enforcement and Operations

Reaching Enforcement

Taking a domain from monitoring to an enforcing policy without losing legitimate mail.

1. 5.1 The Sequence
2. 5.2 The Rehearsal
3. 5.3 Making the Move
4. 5.4 Subdomains and the Senders That Cannot Authenticate
5. 5.5 Forwarding and Mailing Lists
6. 5.6 When It Goes Wrong
7. Module Summary and Knowledge Check

Operate and Audit

Keeping an enforcing domain enforcing. The drift that arrives without anybody making a change, reading reports as a monthly operation, the domain audit as a repeatable deliverable, the transport security records in the same zone, BIML, and an honest account of where the standards are heading.

1. 6.1 Drift
2. 6.2 Reading Reports as an Operation
3. 6.3 The Domain Audit
4. 6.4 Transport Security
5. 6.5 BIML
6. 6.6 The Honest Edge
7. Module Summary and Knowledge Check

Phase 0: Course Resources

Cheatsheets

What each check proves, the record syntax and its limits, reading a report, and the failures that are not yours.

1. What Each Check Actually Proves
2. The Records You Publish
3. DMARC, Reports and Reaching Enforcement
4. Operating It, and the Failures That Are Not Yours

Cookbooks

Ordered procedures for inventorying senders, reaching enforcement, onboarding a platform, and diagnosing a delivery failure.

1. Inventorying Who Sends as You
2. Getting to Reject
3. Onboarding a New Sending Platform
4. Diagnosing Mail That Stopped Arriving

Walkthroughs

Four cases reasoned end to end, including the forgery that passed every check and the outage nobody had changed anything to cause.

1. The Invoice That Passed Every Check
2. The Outage Nobody Had Caused
3. The Sender That Only Mails in January
4. The Signature a Security Tool Broke

Playground

A domain you control, a few DNS records, and the checks that make the practice real.

Operational Reference

Every record format, query, command, tag value and check from the Email Authentication and DMARC Enforcement 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, the standards that were rewritten in 2026, the drafts still in motion, and the authoritative source for each class of fact.

Course Completion

Course Exam

Email Authentication and DMARC Enforcement end-of-course exam: invoice fraud where SPF, DKIM and DMARC all passed correctly, a supplier about to be wrongly accused, and what the investigation reveals about your own outbound posture.

1. Course Completion. Email Authentication and DMARC Enforcement

Generated 2026-09-22 from the published course. The current syllabus is always at ridgelinecyber.com/training/courses/email-authentication/