

Evidence Packet Walkthrough: MFA Example

A sample evidence packet for turning a vague claim into defensible proof.

North Star Security

This is a simulated example for learning and portfolio practice. It is not from a real customer environment.

Scenario

A learner is practicing how to turn a vague security claim into a defensible evidence note.

Question: What evidence would support an MFA-related security claim?

Practice area: Identity and access management evidence

Status: Partially supported in this sample

Evidence type: Policy screenshot, admin settings export, user coverage report, limitation note

Weak claim

> MFA is enabled.

This claim is weak because it does not explain scope, evidence, limitations, or what still needs validation.

Stronger evidence note

- > MFA appears enabled for the reviewed identity platform and administrative
- > accounts in this simulated scope. Evidence includes an MFA settings
- > screenshot, an administrative user export, and a user coverage report captured
- > during the review period. Any excluded users, service accounts, or unsupported
- > systems should be documented as limitations and validated separately.

Evidence packet contents

Evidence item	What it proves	Notes
MFA policy screenshot	MFA is configured in the identity platform	Include date captured
Admin user export	Admin accounts are in scope	Include source
User coverage report	Shows enabled/disabled status	Watch for service accounts
Limitation note	Known gaps are documented	Explain what is not proven
Review note	Explains scope and limitation	Avoid overclaiming

Evidence note template

This evidence supports [claim/question] for [scope]. It was captured on [date] from [system/source]. The evidence shows [what is enabled or observed]. Current limitations are [unknowns/assumptions], and the next validation step is [action].

Evidence Packet Walkthrough: MFA Example

A sample evidence packet for turning a vague claim into defensible proof.

What to check before making the claim

- Does MFA apply to all users or only certain groups?
- Are administrators covered?
- Are service accounts excluded?
- Are third-party apps or legacy protocols bypassing MFA?
- Is there a policy, report, or screenshot with a date?
- Are limitations documented honestly?

Final evidence summary

MFA appears enabled for the reviewed identity platform and administrative accounts in this simulated scope, based on the sample settings screenshot and user coverage export. The claim should be documented as scoped evidence, not a blanket statement about every system. Any excluded accounts, unsupported systems, or unknown coverage areas should be listed as limitations and validated separately.

LinkedIn lesson

The difference between a weak and strong portfolio artifact is not fancy wording. It is scope, evidence, limitations, and a clear next step.

North Star standard

Proof of work needs evidence - not vibes. A good answer says what is true, what proves it, and what is still incomplete.