

Onboarding an Identity: Registration and Identity Proofing

Tue, Aug 4, 4:00 PM EDT · <https://scottslab.io/posts/registration-and-identity-proofing>



TL;DR

Registration should pass through four different people: request, approval, identity proofing, and credential issuance. That way no single insider can conjure an account out of nothing. Identity proofing (NIST's 800-63A grades ID evidence by strength, so lean on strong, independent government photo IDs) is where you earn the right to trust everything downstream. A flawless MFA setup on an account issued to the wrong person is a strong lock on a door you already opened.

Before anyone gets a username to type, someone has to decide they're real and that they belong. That's registration, and it's the step where a surprising amount of fraud gets stopped, or waved straight through, depending on how many different people actually touch it.

The clean version is four steps, and the whole point is that they're four *different* people. Someone requests the account, usually a hiring manager. Someone else approves it. It has to be someone else, because a request that approves itself isn't a control, it's a formality. A registration authority, often HR, does the identity proofing: actually confirming this person is who they claim to be. And then, ideally a fourth person, issues the credential. Spread across four roles, no single insider can conjure

an account out of nothing. Collapse it down to one busy admin doing all four, and you've rebuilt the exact gap fraudsters look for.



Identity proofing is the part that decides how much you should actually trust the claim. NIST's 800-63A framework (revised in 2025) grades identity evidence by *strength* (FAIR, STRONG, SUPERIOR) rather than simply counting IDs: the higher the assurance level you need, the stronger, and often the more numerous, the documents have to be. In practice that still means leaning on strong, independent government photo IDs, and "independent" is doing real work: two documents from the same source prove far less than one each from two. In the US that's the usual set: driver's license, passport, state ID, military ID. Higher-assurance environments layer on more, and fingerprinting is routine in government, with a criminal background check where the role warrants it.

None of this is glamorous, and it's tempting to file it under HR paperwork and move on. But every authentication control downstream is only as trustworthy as this step. A flawless MFA setup on an account that was issued to the wrong person is a very strong lock on a door you already let the intruder walk through. Proofing is where you earn the right to trust everything that comes after it.