

# Caller verification for human and AI service desks

Proofcall brings Microsoft-backed caller verification into the support conversation. Give your engineer or AI agent a defined way to check the expected account before a sensitive request.

## The verification workflow

- 01 Select the caller.** Your handler identifies the organisation and expected Microsoft account.
- 02 Authenticate with Microsoft.** The caller opens a link and uses their organisation's existing authentication.
- 03 Read back the Proofcall code.** After authentication, the caller receives a separate code and reads it to the handler.
- 04 Review the result.** The handler submits the code. Proofcall records the result, identity evidence and handler attribution.

## A process for the whole desk

Human engineers use the console. Compatible automated agents use the HTTP API or MCP tools. MSPs can work across connected client tenants.

## Evidence behind the result

Review the account, tenant, authentication time and available method information. The record distinguishes direct verification from a colleague authenticating and vouching for the caller.

## Evaluate against your own workflow

Start a 14-day trial at [proofcall.io/signup](https://proofcall.io/signup). No card required. Begin with one tenant and a test caller.

# Deployment fit and verification boundaries

| Capability         | What it provides                                                                                           |
|--------------------|------------------------------------------------------------------------------------------------------------|
| Microsoft Entra ID | Authentication context and expected tenant/account checks.                                                 |
| Engineer console   | Directory lookup, verification handling and history.                                                       |
| API and MCP        | Interfaces for compatible integrations and credentialed agents. Agent features depend on the account plan. |
| Audit export       | Verification evidence for review and CSV export. Retention depends on deployment settings.                 |
| Approver workflow  | A separate attestation path, clearly distinguished from direct verification.                               |
| PSA integration    | Evaluate ConnectWise writeback within an integration pilot.                                                |

## Prerequisites

Microsoft Entra ID P1, administrator-led tenant setup and a caller with a usable authentication method. Configure and test the Conditional Access authentication context.

## What the check establishes

Direct verification establishes control of the expected account and successful submission of the separate Proofcall code. It does not prove legal identity or identify synthetic speech. The consuming workflow must authorise the requested action.

## Recovery and caller guidance

Plan an approved recovery route when authentication is unavailable. Ask only for the code on the Proofcall page after authentication. Never ask for a Microsoft sign-in code, password or Authenticator code.