ACCESS CONTROL

2FA on connect

A second factor at the moment it matters: before a connection to a company device starts, not only at sign-in.

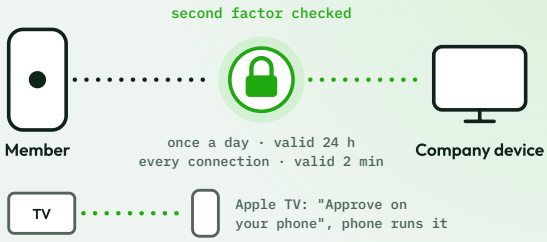
What it is

With 2FA on connect switched on, a member confirms a second factor before a connection to a company device begins. The check runs on the server, at session start and in the signalling service, so an app cannot skip it. Without a valid proof the connection is refused and written to the audit log. Admins choose how often: **once a day per device** or **every connection**.

Key capabilities

- **Checked on the server, per connection.** A proof is tied to the user and the device: valid 24 hours for "once a day", 2 minutes for "every connection".
- **Authenticator app (TOTP)** with 10 one-time recovery codes; works on every platform.
- **Your IdP's own step-up** via OpenID Connect, e.g. Entra MFA and Microsoft Authenticator, Okta Verify, Ping, OneLogin, JumpCloud. Accepted only with a fresh sign-in and a second factor reported by the IdP.
- **Duo Universal Prompt** and **passkeys / security keys** (YubiKey, Touch ID, Windows Hello, Android); passkeys work in the web app today, the native apps follow.
- **Apple TV approval.** The TV cannot ask for a code: it shows "Approve on your phone", and the member approves in the Awacino app on the phone.
- **Logged and alerted.** Every refusal is recorded with user, device, target, method and reason; 5 failed checks within 15 minutes alert all admins.

HOW IT WORKS



No valid proof, no connection: the refusal is written to the audit log.

Plan availability

PLAN	INCLUDED
Basic	Admin 2FA, step-up for critical changes, optional 2FA sign-in for every user. No 2FA on connect.
Standard	+ 2FA on connect: TOTP, passkeys, IdP step-up, Duo, Apple TV approval
Premium	As Standard, next to company sign-in (SSO)

Every plan limit is checked on the server. A downgrade stops 2FA on connect; settings are kept. The company version is rolled out in stages: ask us what is live for your plan.

Requirements

- Commercial Standard or Premium; switched on by a MAIN-ADMIN or ADMIN
- IdP method: an OIDC client at your IdP (issuer, client id, secret, optional `acr_values`); Google Workspace needs `acr_values`, or use TOTP or Duo
- Duo: a Universal Prompt application (client id, API hostname, secret)
- Secrets are kept in an encrypted vault and never shown again

Learn more

2FA on connect	www.awacino.com/commercial/technology/2fa-on-connect/
Company sign-in	www.awacino.com/commercial/technology/company-sign-in/
Plan features	www.awacino.com/commercial/pricing/#features
Security	www.awacino.com/commercial/technology/security/

Talk to us