oktane

September 22-24, 2026 | Caesars Forum | Las Vegas, NV

Call for Speakers | Example of a winning submission

Proposed title
Lessons from the Login Screen: Deploying Desktop MFA at Okta

Proposed abstract
As organizations embrace Zero Trust, securing the device itself—starting at the login screen—is no longer optional. Okta Device Access (ODA) extends the power of Okta to macOS and Windows logins, enforcing strong authentication at the first point of contact. But what does real world deployment actually look like?

Hear directly from Okta's Client Platform Engineering (CPE) team as they walk through their own internal deployment of Desktop MFA. Learn what worked, what broke, and what got better through iteration. From configuration to communication, and recovery flows to real-time user feedback, this talk goes beyond the docs to give you a tactical playbook for rolling out Desktop MFA in your own organization. Okta's internal deployment from kickoff to completion was achieved in under six weeks. You'll walk away with concrete lessons, battle-tested workflows, and insights into how this partnership between product, platform, and end-user shaped a better login experience for everyone.

Please explain why this session would be compelling to our Oktane audience
Device login is a critical, but often overlooked part of enterprise security. Okta Device Access (ODA) secures device login with Desktop MFA, and interest in ODA is increasing among security, IT, and IAM teams.

This session offers something unique: a behind-the-scenes look at Okta's own internal rollout of ODA on macOS and Windows. You'll hear how the Client Platform Engineering (CPE) team worked with product and engineering to test, iterate, and improve the experience. This is a practitioner's guide to ODA: what to plan for, how to recover from

issues, and how to drive user adoption. It’s not just theory—it’s hard-won insight, straight from the login screen. Why attend? Get an unparalleled insider's view of Okta's own large-scale internal ODA deployment. We'll share actionable lessons: what worked, what didn't. Attendees will leave with practical strategies, deployment insights, and a clear understanding of how Desktop MFA strengthens your security posture right from the login screen.

How do you plan on engaging the audience in your breakout session?

- **Live Demos:**
  Showcase of a real login experience and common issues - *on/off line mode, recovery PINS) … Desktop MFA login experience, common issues and how to resolve
- **Polls / questions from the presenters:**
  Use live polls to gauge the room's deployment status, blockers, and concerns—help tailor the conversation in real time … e.g. how many are deploying DMFA, how many thinking about it, biggest challenges, what concerns have stopped you from proceeding
- **Live Q&A:**
  Questions from the audience and moderated live Q&A with time reserved for deep technical queries.