Securing access from OS to apps with Okta Device Access

Today's speaker

Cynthia Luu
Principal Product Marketing Manager
Okta

Agenda

01	The Market: Why you need secure device access
02	The Solution: Okta Device Access is here to help (and what customers have to say)
03	The Vision: A secure device deployment journey & beyond

okta

Safe harbor

This presentation contains "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, long-term financial targets, product development, business strategy and plans, market trends and market size, opportunities, positioning and expected benefits that will be derived from the acquisition of Auth0, Inc. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as "expect," "anticipate," "should," "believe," "hope," "target," "project," "goals," "estimate," "potential," "predict," "may," "will," "might," "could," "intend," "shall" and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, the market for our products may develop more slowly than expected or than it has in the past; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; we may fail to successfully integrate any new business, including Auth0, Inc.; we may fail to realize anticipated benefits of any combined operations with Auth0, Inc.; we may experience unanticipated costs of integrating Auth0, Inc.; the potential impact of the acquisition on relationships with third parties, including employees, customers, partners and competitors; we may be unable to retain key personnel; global economic conditions could worsen; a network or data security incident that allows unauthorized access to our network or data or our customers' data could damage our reputation and cause us to incur significant costs; we could experience interruptions or performance problems associated with our technology, including a service outage; the impact of COVID-19 and variants of concern, related public health measures and any associated economic downturn on our business and results of operations may be more than we expect; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any unreleased products, features or functionality referenced in this presentation are not currently available and may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.

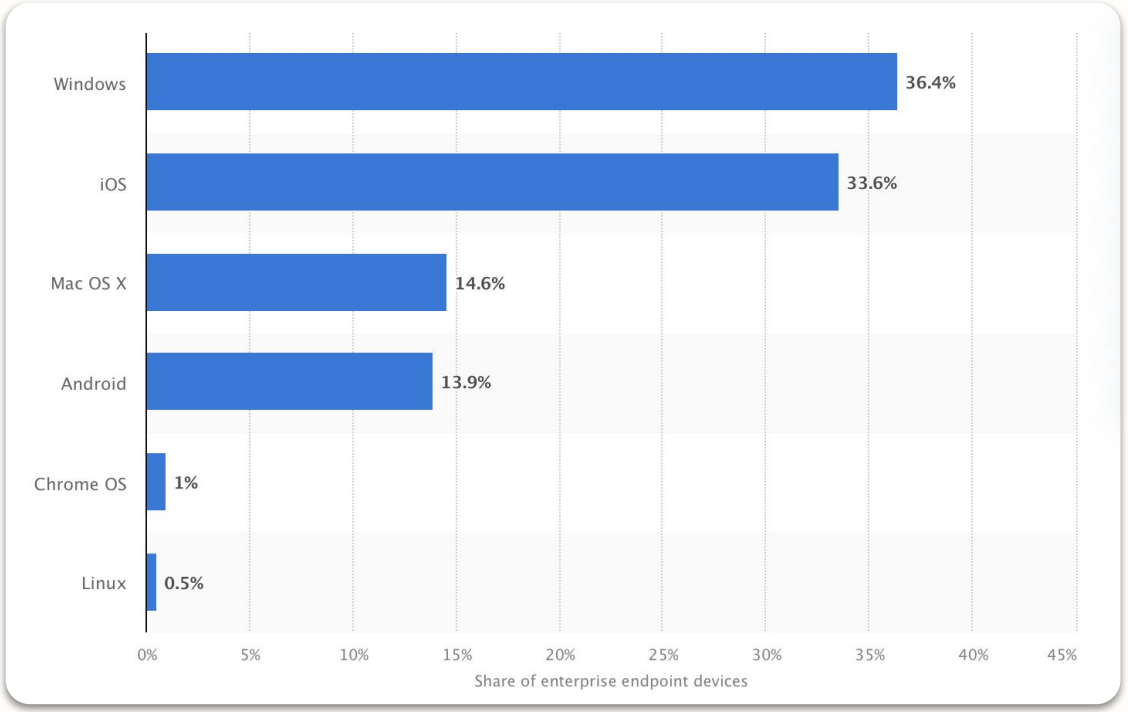
okta

Today, employees have a choice in where they work and what technology they work on

74%

of employers now offer hybrid work arrangements

Distribution of operating systems (OS) among enterprise endpoints in North America, Western Europe, and Asia Pacific as of 2022



Sources:

1. https://www.forbes.com/sites/joemckendrick/2022/12/28/hybrid-work-is-now-the-norm-for-the-year-aheadand-beyond/?sh=734160b8520b
2. https://www.statista.com/statistics/741497/worldwide-enterprise-endpoint-operating-system-distribution

okta

When your people and devices are not centrally located, security is critical

60% of security incidents associated with a lost or stolen asset include missing desktops and laptops – more than any other type of device, including mobile phones

65% of people reuse the same password for multiple or all their accounts – this makes laptops that are protected by only passwords a security risk

+$227K impact of lost or stolen devices on the average total cost of a data breach. Devices are often stolen, which can mean huge penalties for the business

Sources:

1. Verizon's 2022 Data Breach Investigation Report
2. https://services.google.com/fh/files/blogs/google_security_infographic.pdf
3. IBM Security Cost of a Data Breach Report 2022

okta

Devices are the front door to data, but are often neglected when it comes to securing access

Global average cost of a data breach reached an all-time high in 2023

$4.45M

Source: https://www.ibm.com/downloads/cas/E3G5JMBP

Increasingly more expensive and challenging to obtain and renew cyber insurance

+21%

forecast of compound annual growth for direct cyber insurance premiums until 2025

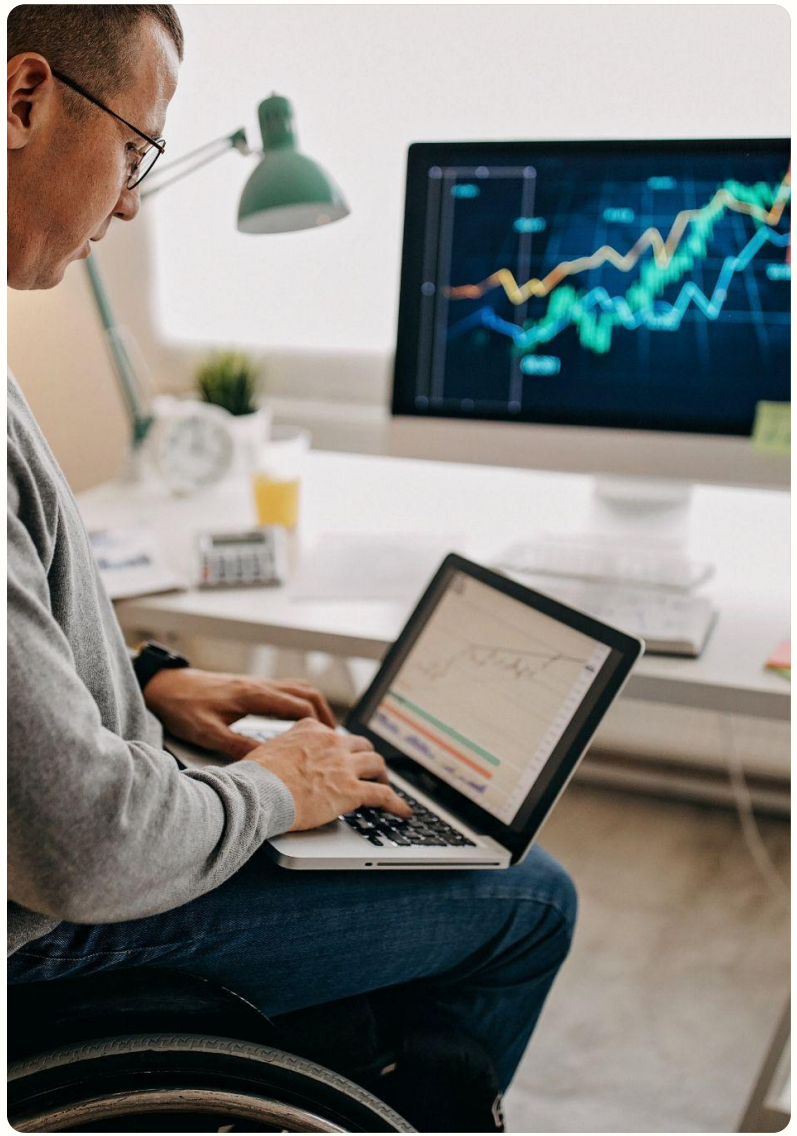
Source: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

PCI DSS 4.0 introduces greater security compliance requirements

Passwords must be at least 12 characters in length, and should change passwords every 90 days

All users, not just admins, requiring access to the cardholder data environment must now be challenged with MFA

MFA must be enforced for access to the cloud, hosted systems, on-premises apps, workstations, servers, etc.



Organizations must overcome these challenges

Securing access at all user touchpoints, across all their devices

Enabling employee efficiency with a great user experience

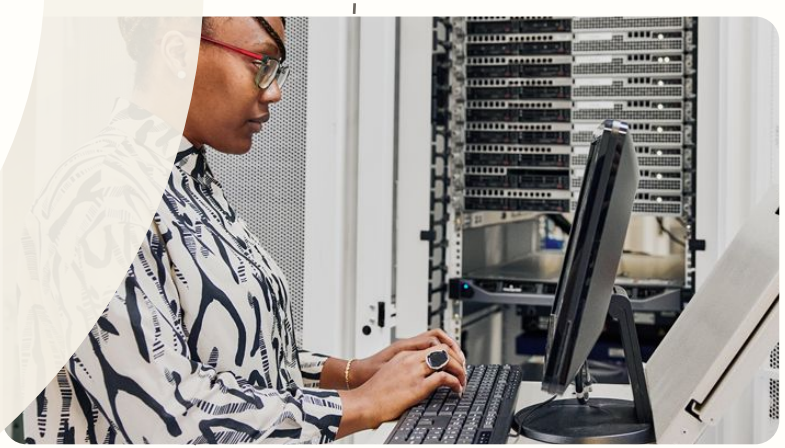
Scaling how you secure access to sustain a modern, digital business

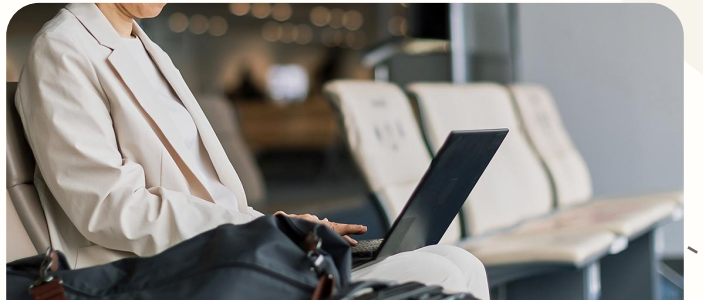
New release!

okta

Device Access

Unified Identity and Access Management,
from any device to all applications





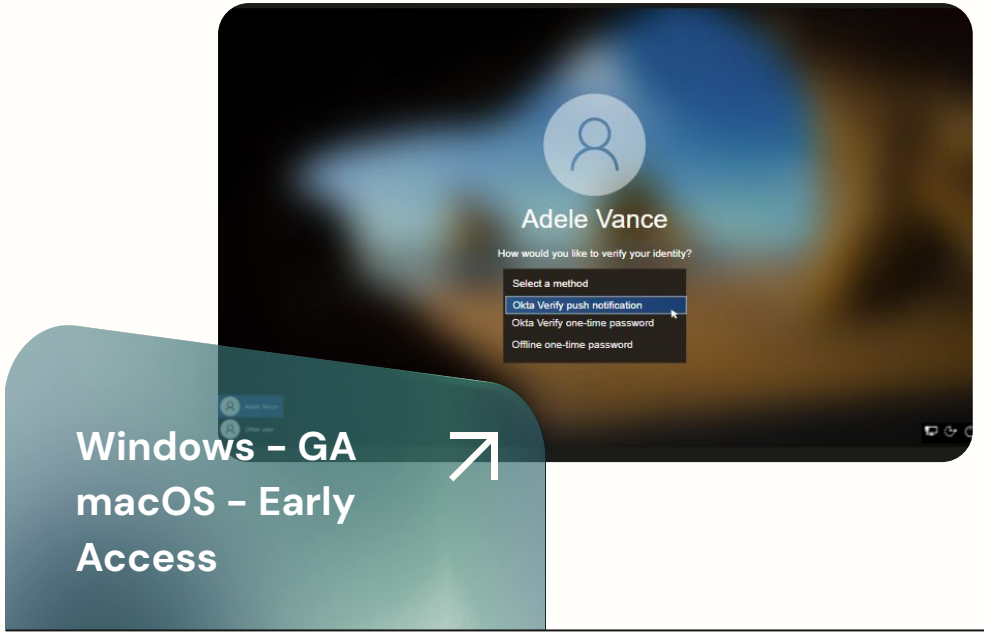
“Okta Device Access is a natural step on our zero trust journey by providing our employees with the seamless access they need to do their best work, while at the same time helping to protect the device.”

John McLeod

Chief Information Security Officer, NOV

okta

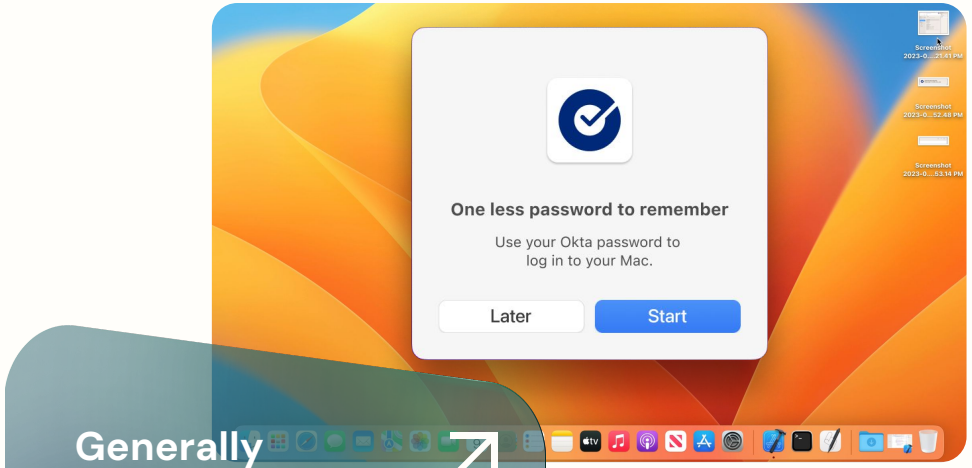
Secure the first vulnerable touchpoint - the device login – with Okta Device Access



Windows - GA
macOS - Early Access

Desktop MFA

Enforce MFA on top of passwords to login to your managed Windows or macOS device



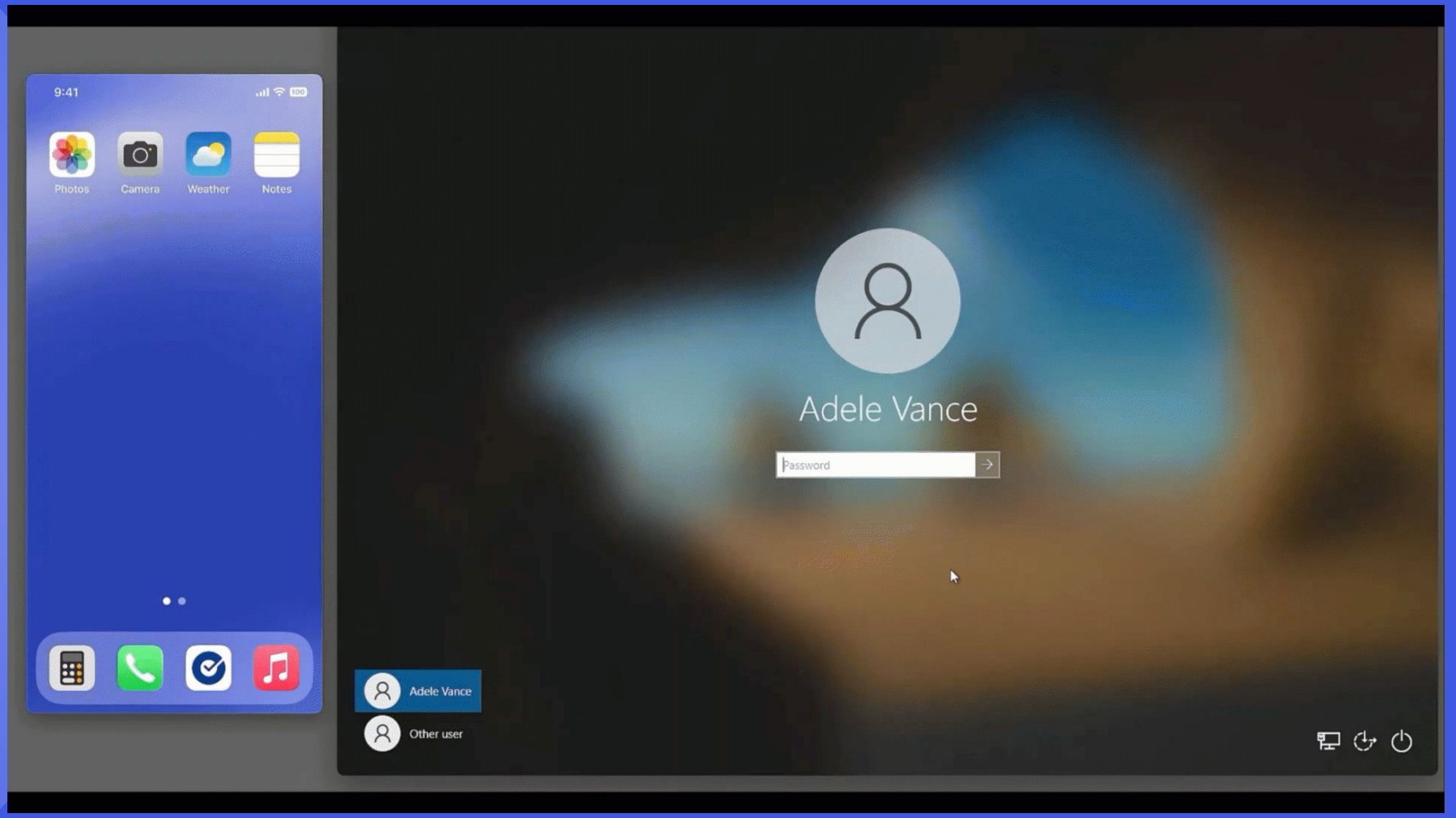
Generally available for macOS

Desktop Password Sync

Sign in to your macOS with your Okta password by syncing passwords

Desktop MFA for Windows

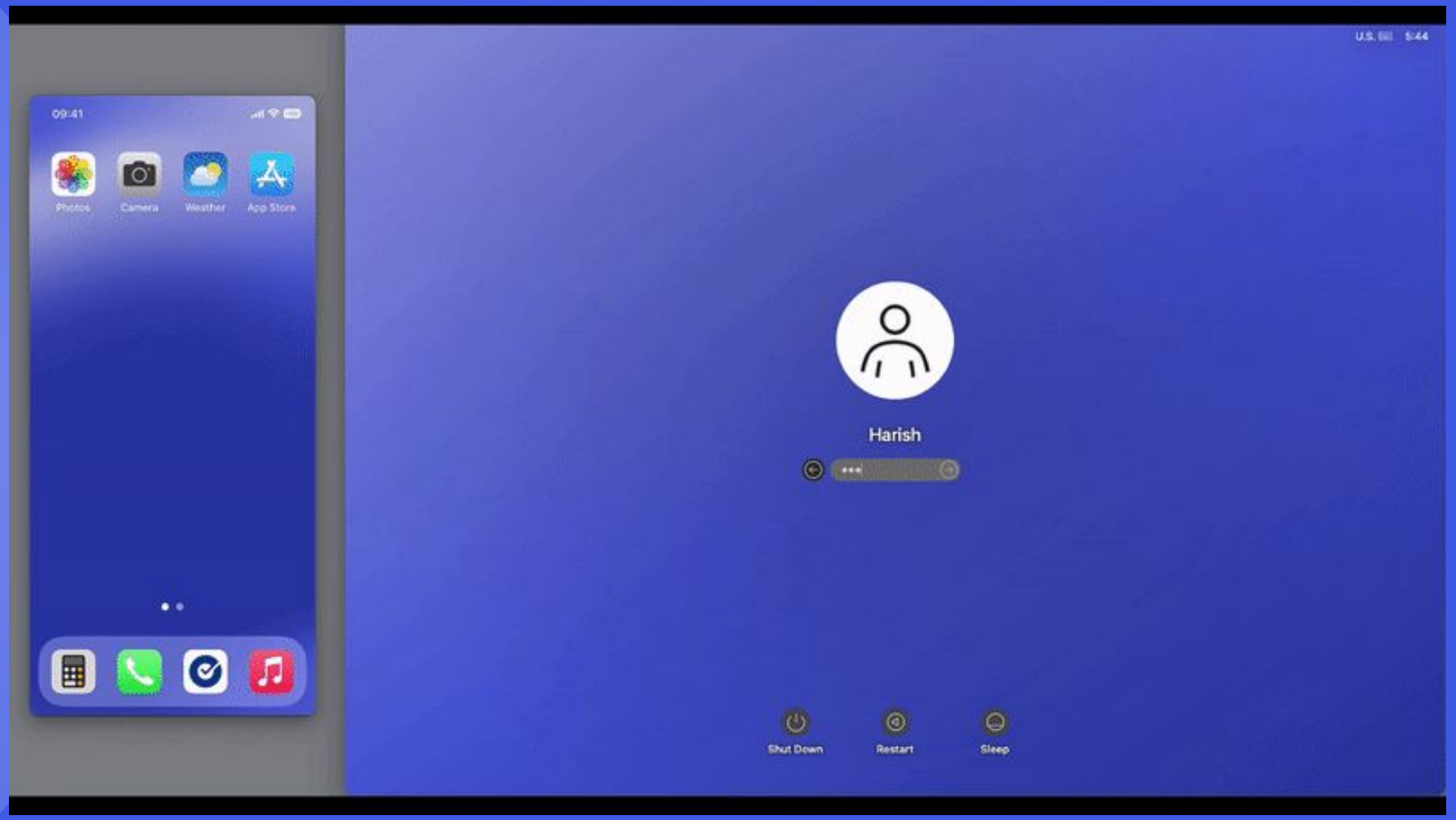
- Native UX
- Policies for enrollment, MFA challenge grace period
- Online factors: Okta Verify Push, TOTP
- Offline factors: TOTP, Yubikey OTP



https://www.crcgroup.com/Tools-Intel/post/multi-factor-authentication-a-must-have-for-cyber-coverage

Desktop MFA for macOS

- Native UX
- Inline offline factor setup
- Policies for enrollment
- Online factors: Okta Verify Push, TOTP
- Offline factors: TOTP



https://www.crcgroup.com/Tools-Intel/post/multi-factor-authentication-a-must-have-for-cyber-coverage

Desktop Password Sync for macOS

- Intuitive enrollment process
- Strong and consistent password policy from device to apps
- Secure, passwordless access to apps
- Phishing-resistance and adaptive policy checks

The Okta Advantage

Ease of use, ease of deployment

- Reduced time to value that Okta customers expect with all Okta solutions
- Friendly user experience that is well-integrated with Windows/macOS and flexibly supports online and offline scenarios

Neutral vendor that supports all devices

- Support for mixed OS deployments and the strongest integrations with best of breed technologies
- Freedom from vendor lock-in and lower TCO with vendor consolidation (Okta is an IdP and desktop access provider)

Integrated identity from device to apps

- Enforce consistent and comprehensive security access controls at scale, under a single, unified IAM platform
- Benefit from the stronger IAM capabilities of the market leading identity provider

What’s on deck for Okta Device Access

Passwordless

FIDO2 Yubikey

Device SSO

Okta Device Access Vision

When an Okta customer asks an OEM...

Meet “EverShip”, an Okta customer

1. I’d like 10,000 laptops, please!

3. Yes, a happy Okta customer.

5. Here’s my tenant ID...

Meet the OEM

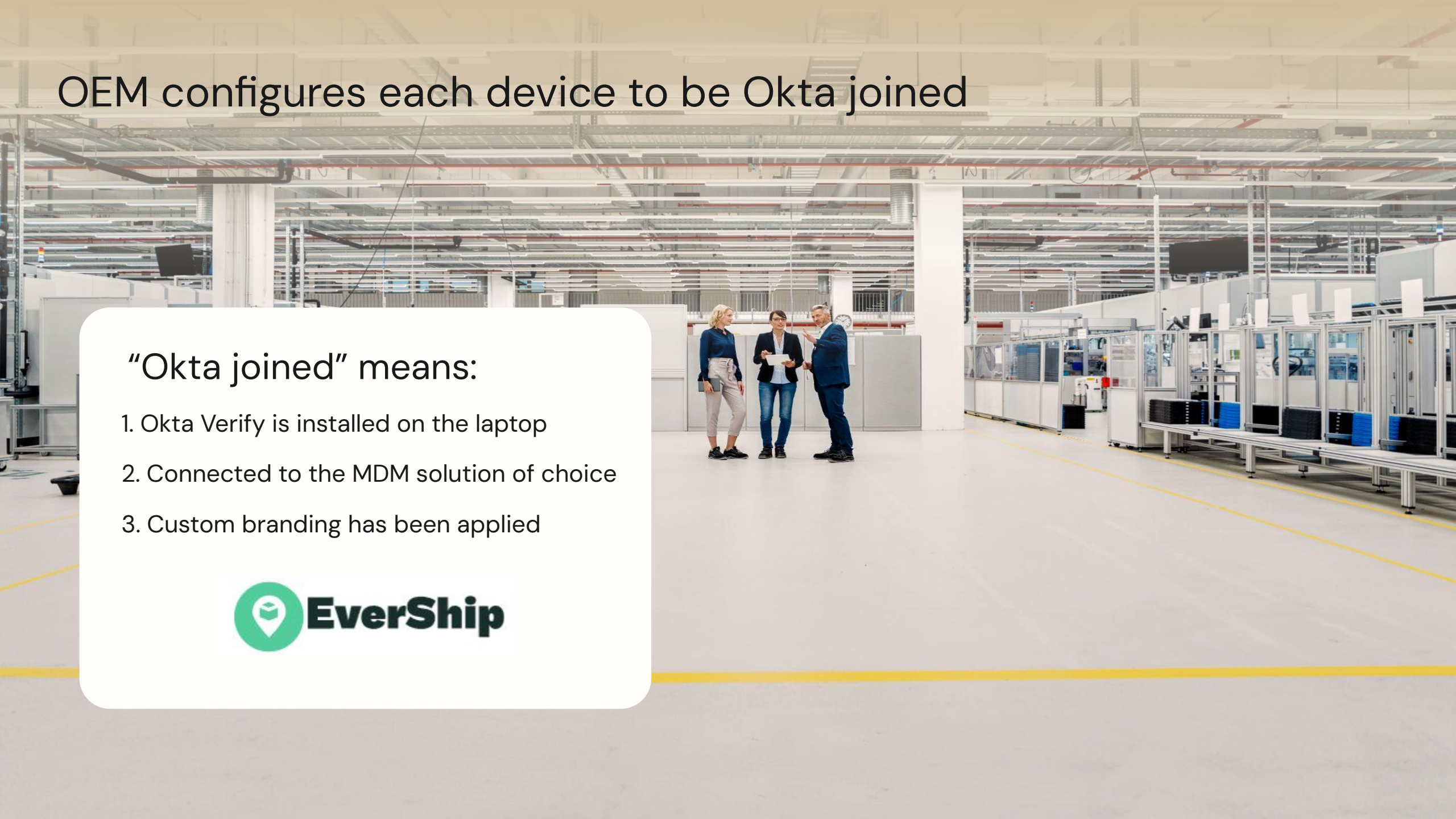
2. Our pleasure! Are you an Okta customer?

4. What are your tenants?

6. Great! We’ll take it from here...

okta

OEM configures each device to be Okta joined



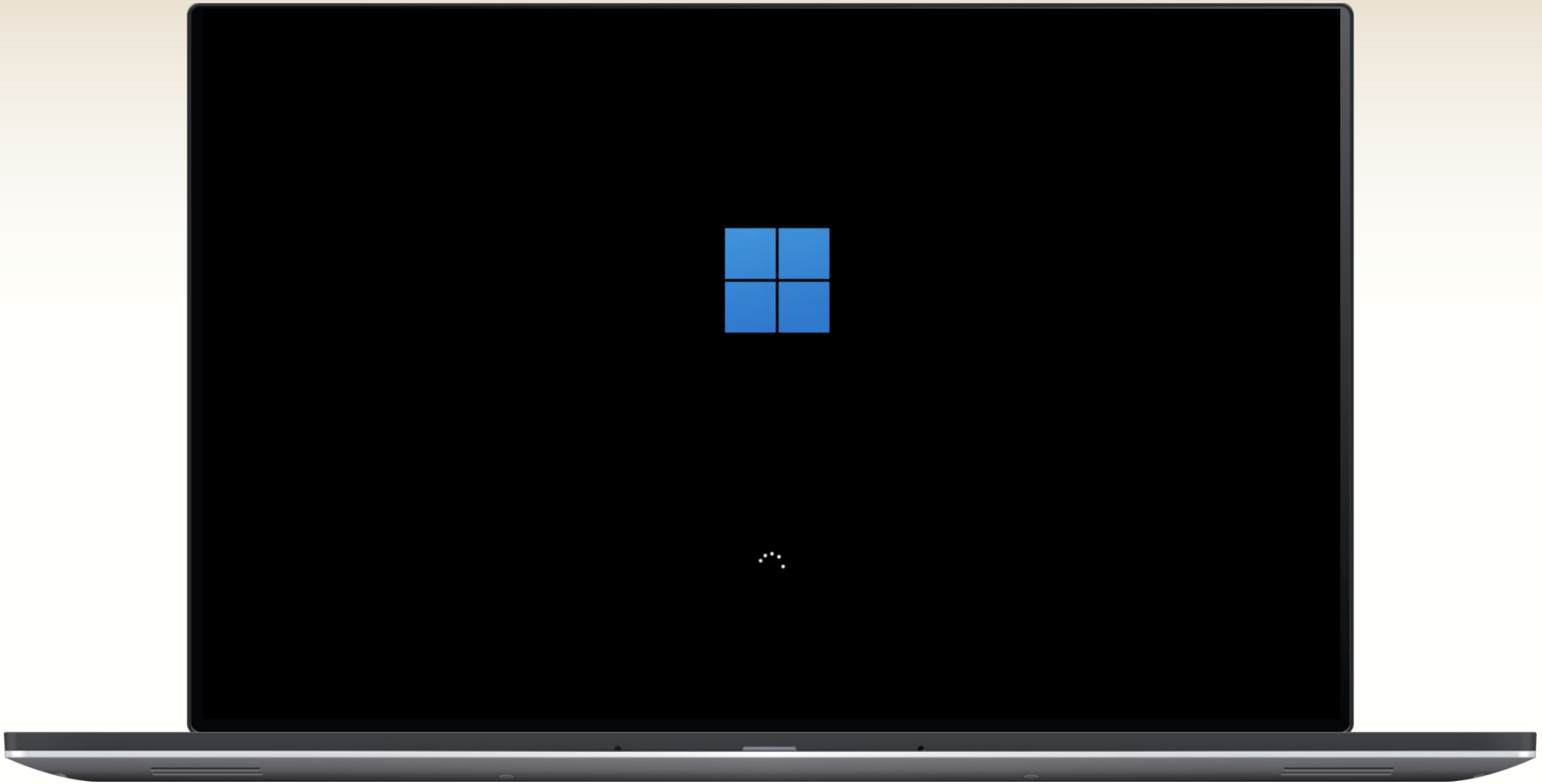
“Okta joined” means:

1. Okta Verify is installed on the laptop
2. Connected to the MDM solution of choice
3. Custom branding has been applied

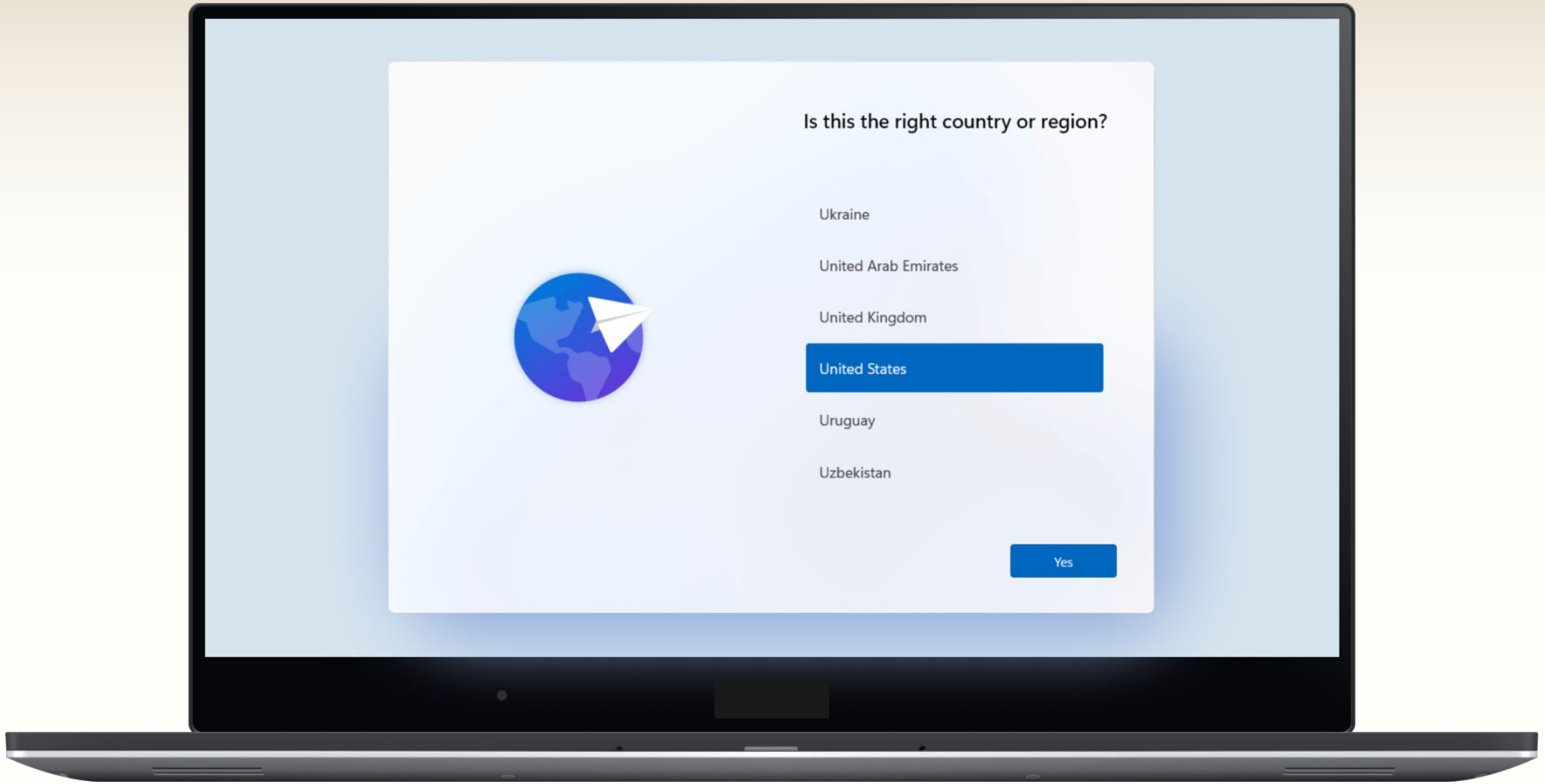
EverShip

A new EverShip employee receives an Okta-joined laptop

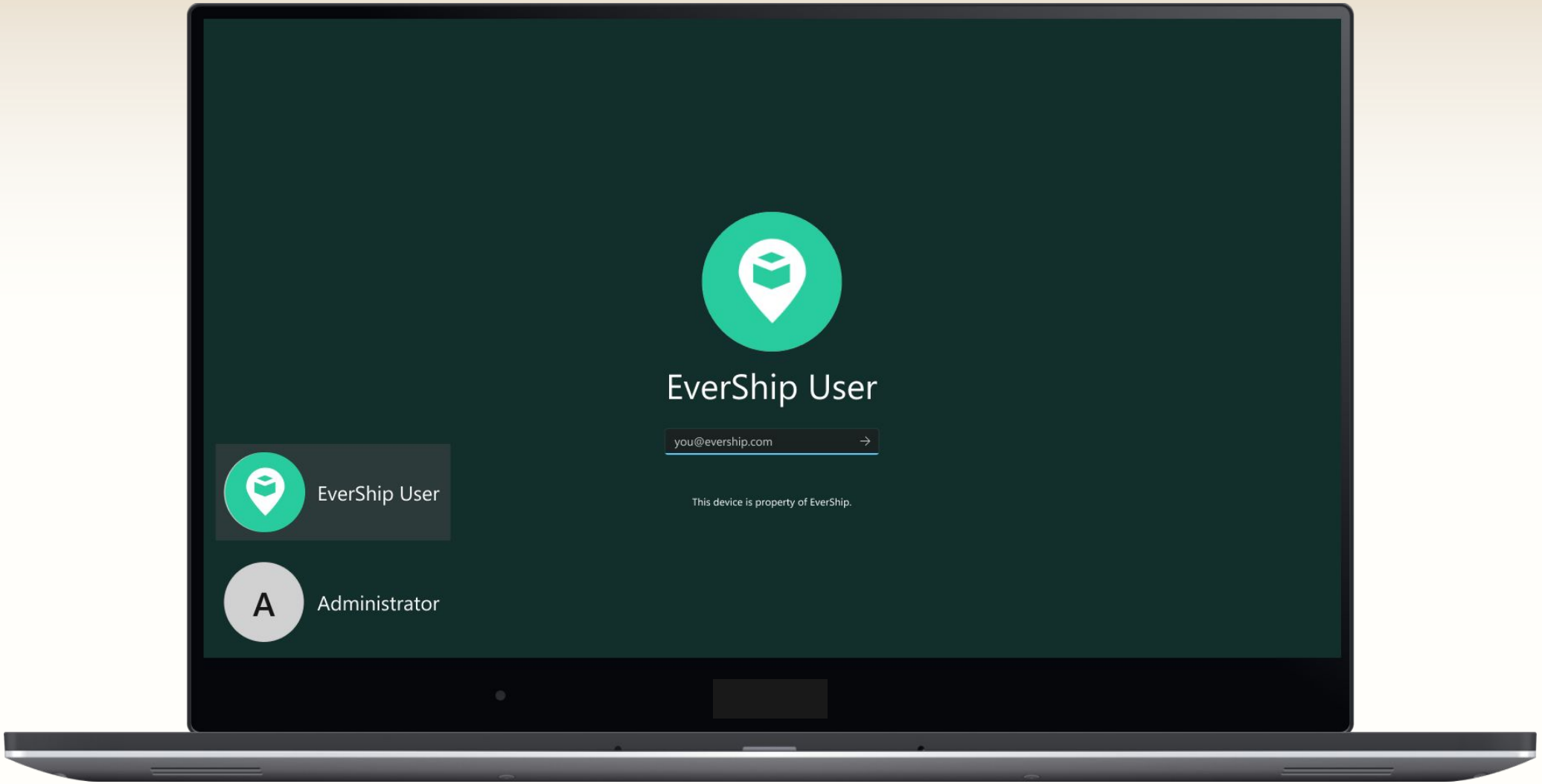
Laptop boots



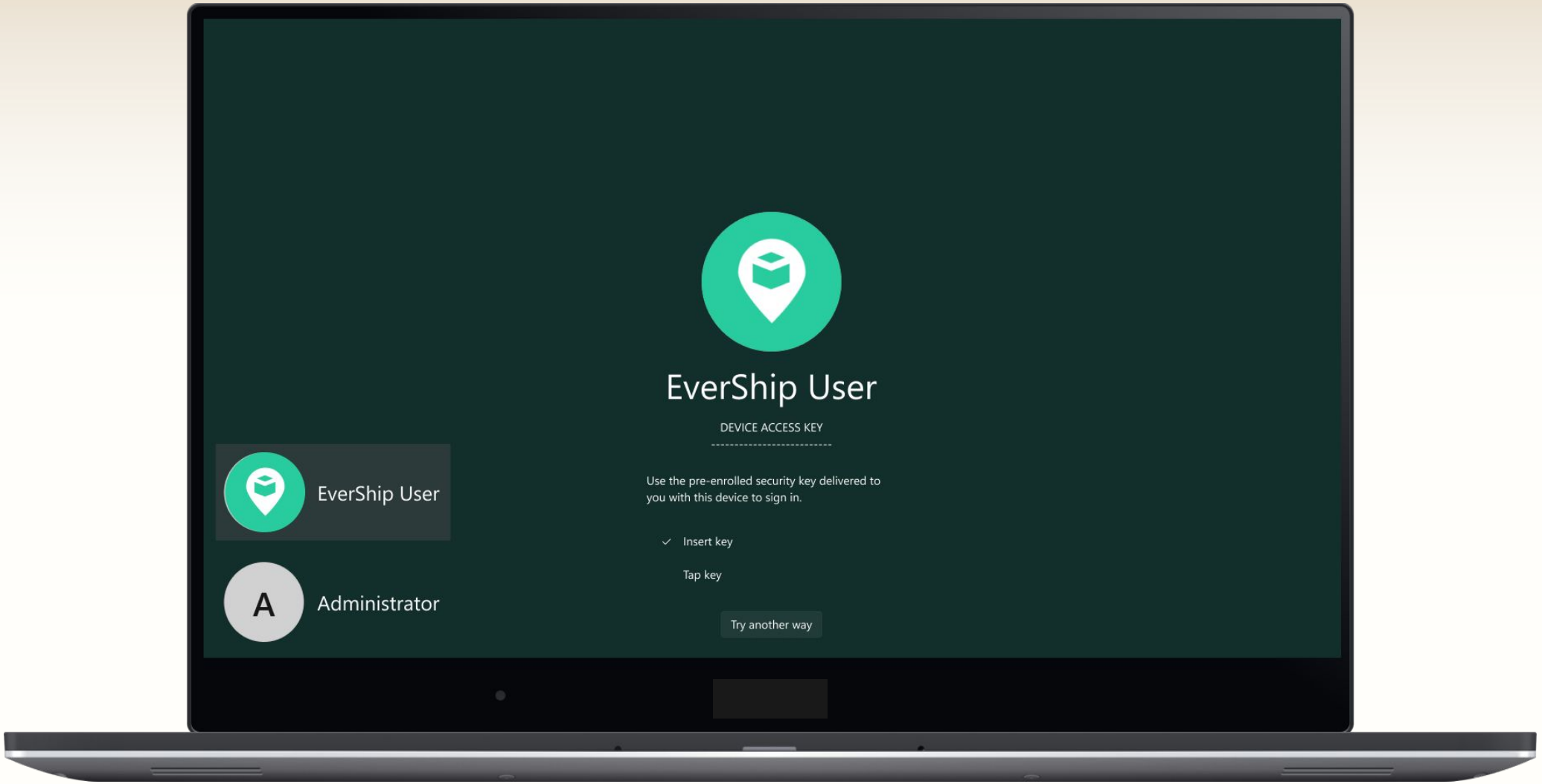
Out-of-the-box experience



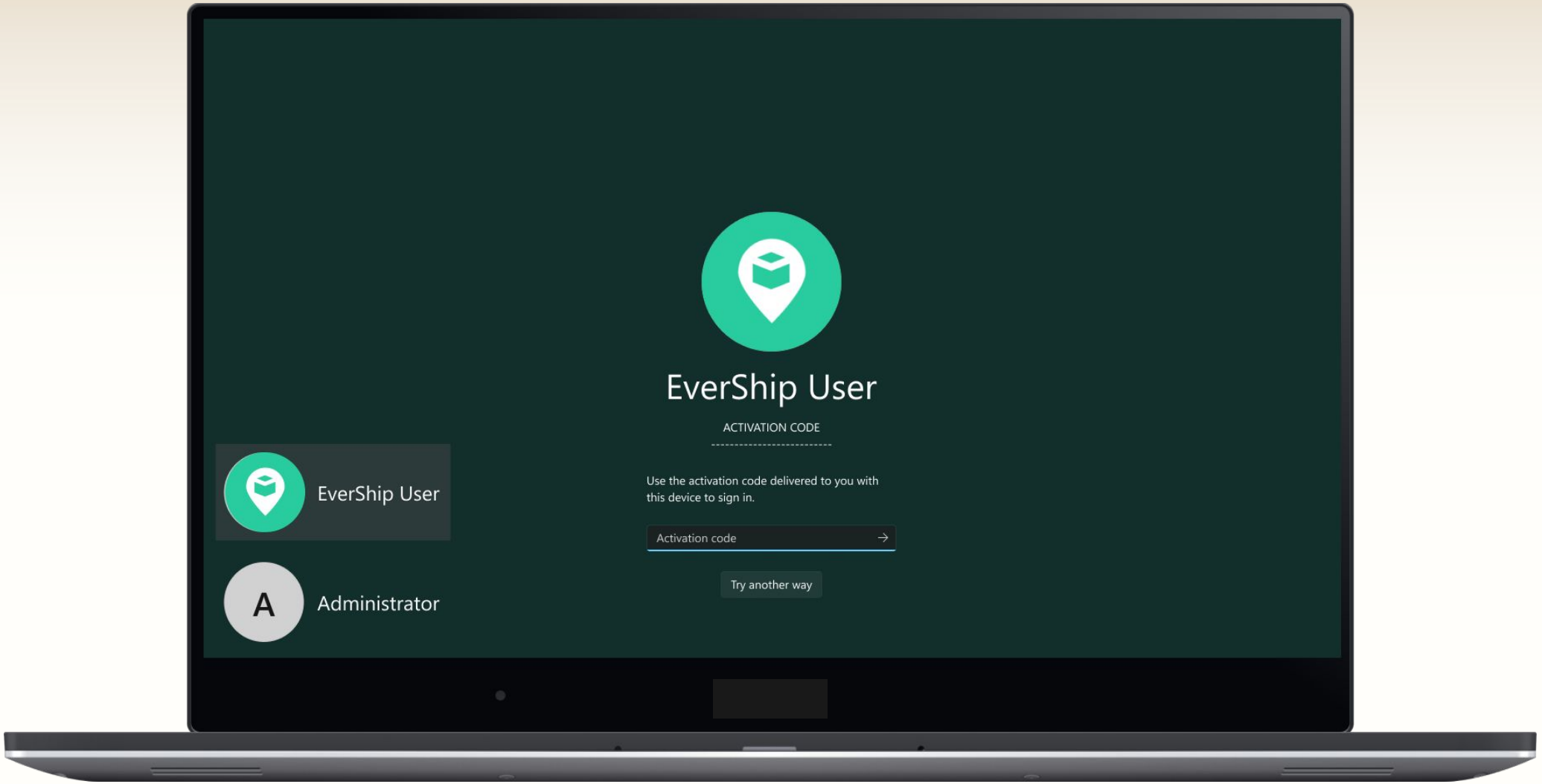
Onboard with branded login



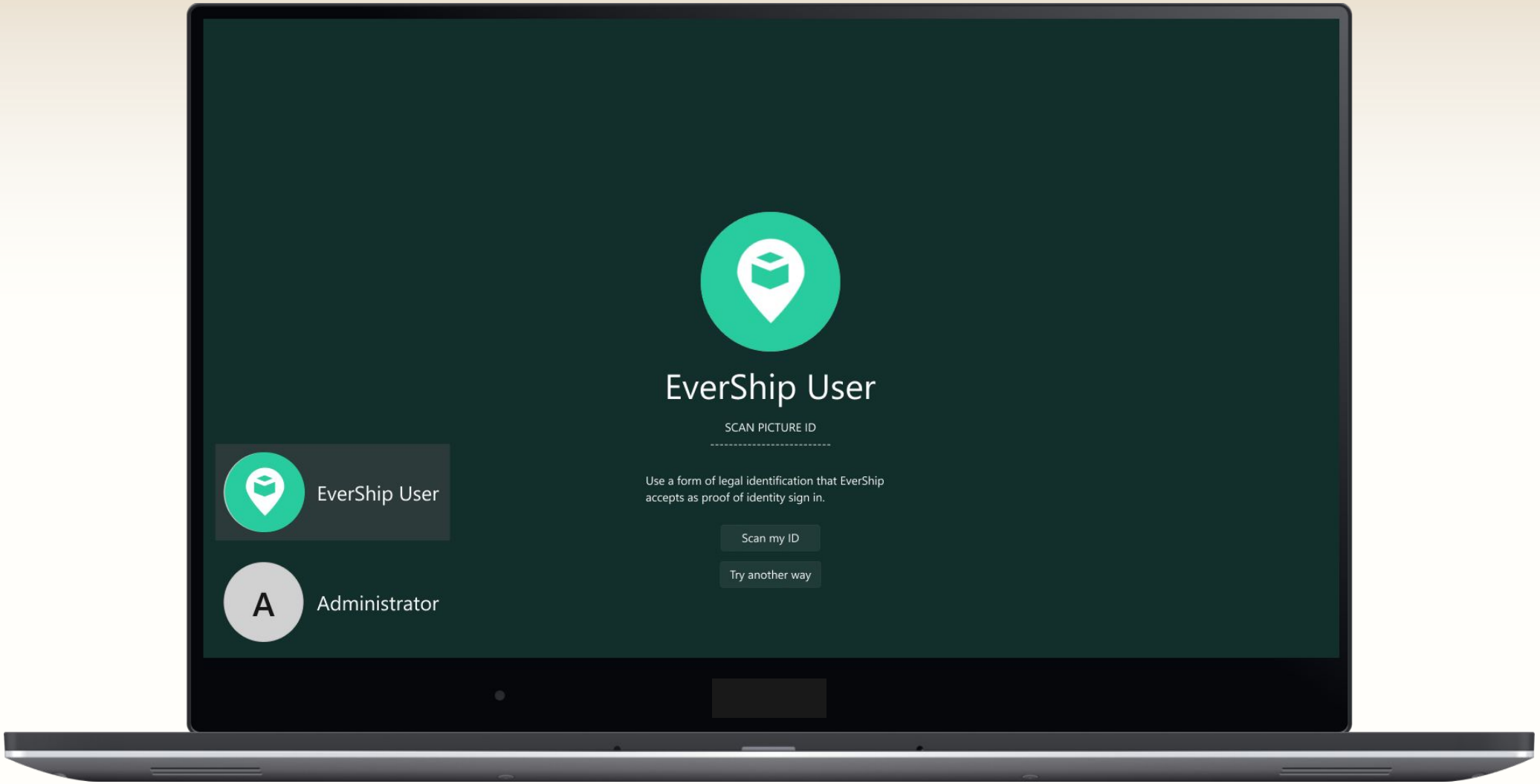
Option A: Pre-enrolled key



Option B: Activation code

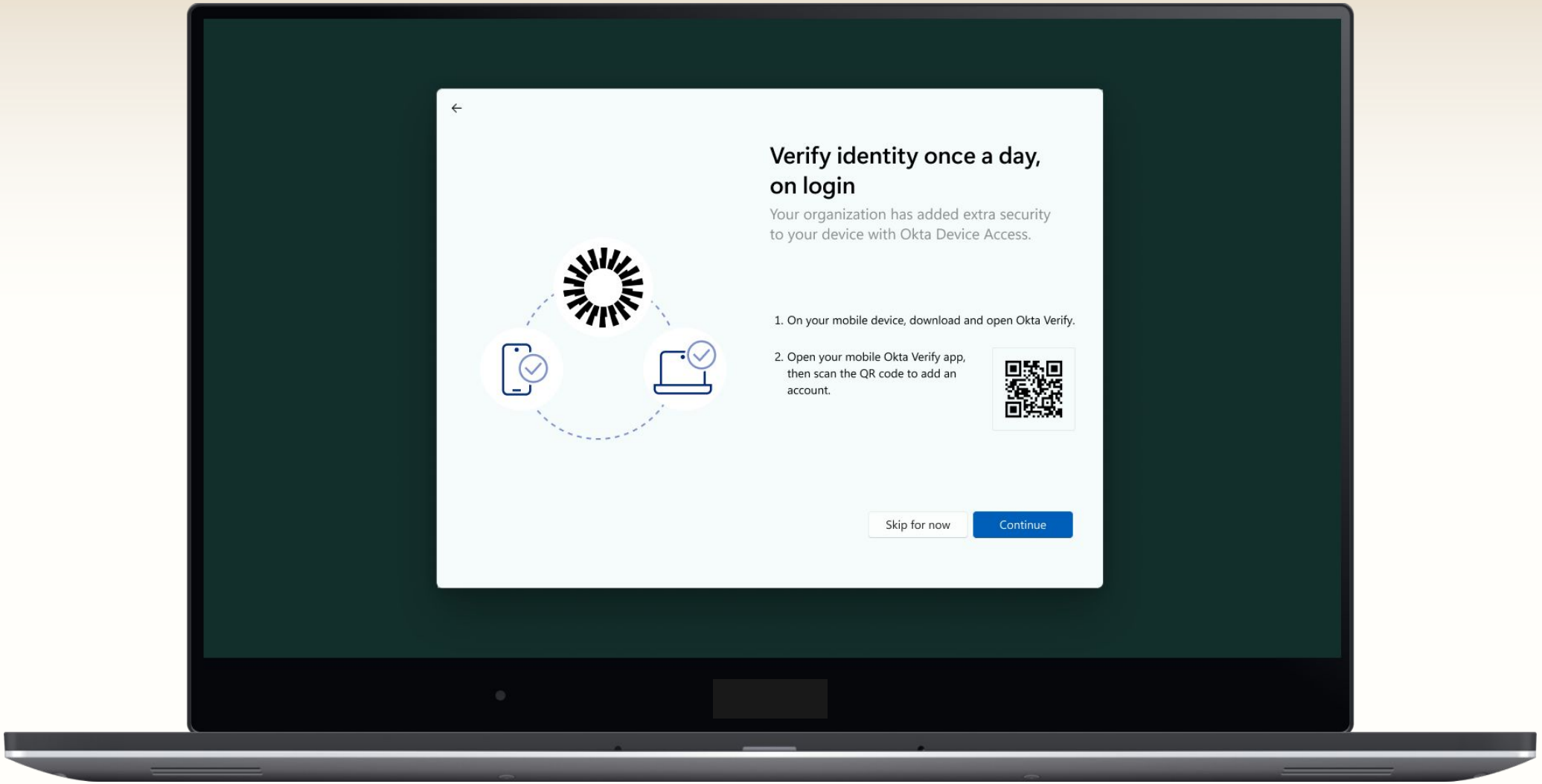


Option C: Identity verification 1 of 2



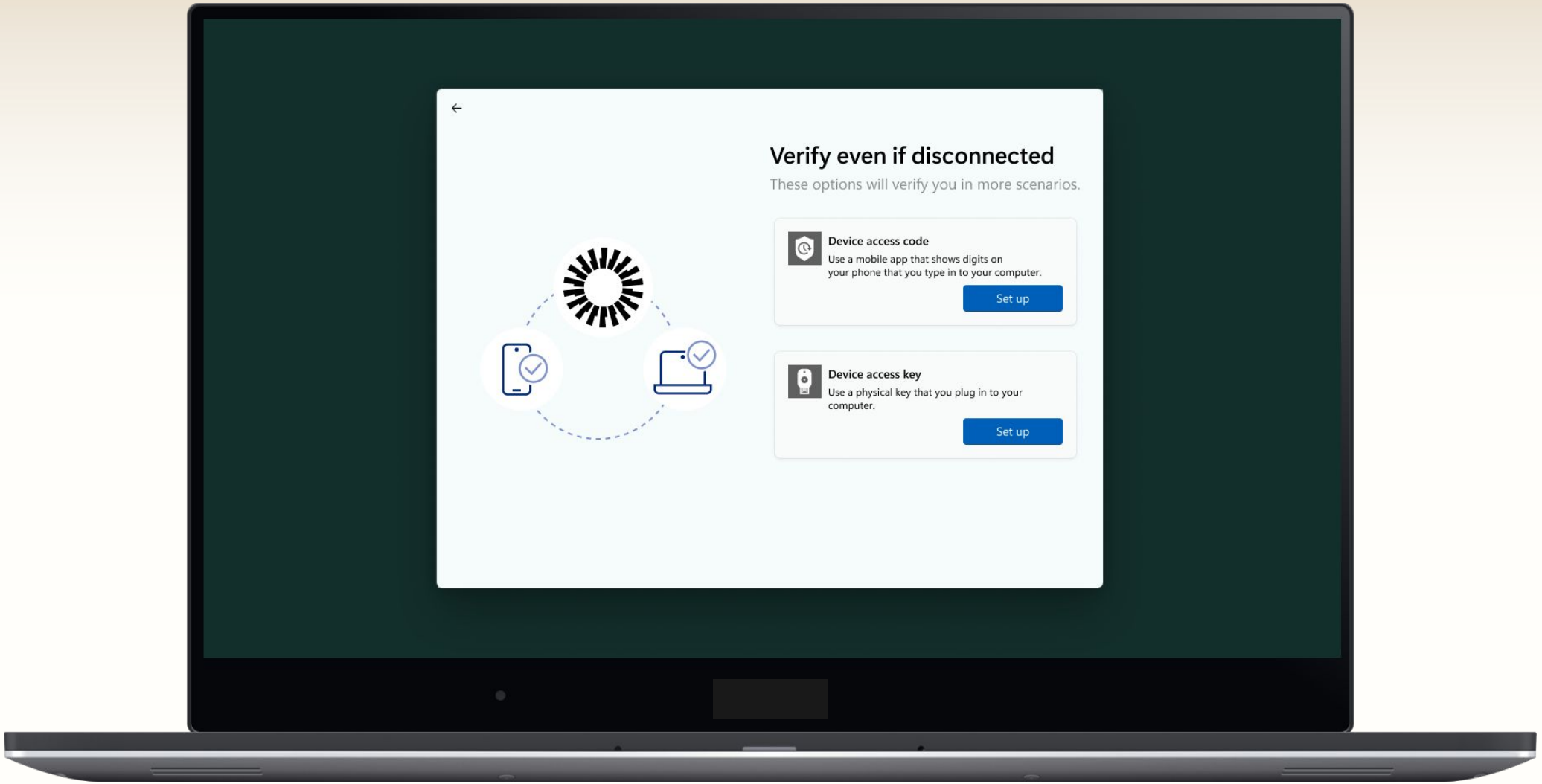
Option C: Identity verification 2 of 2

Enrollment 1 of 2



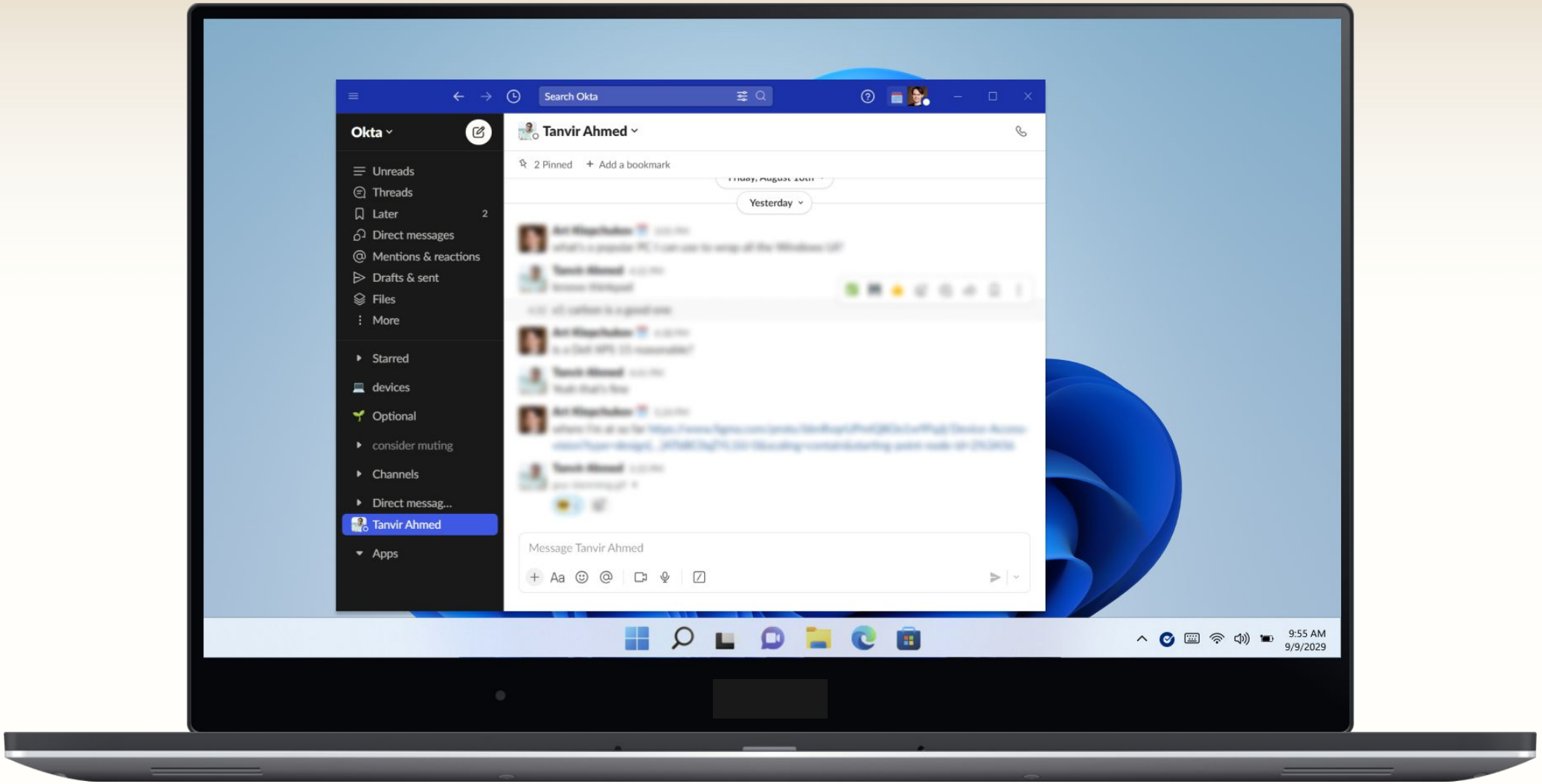
okta

Enrollment 2 of 2: Offline

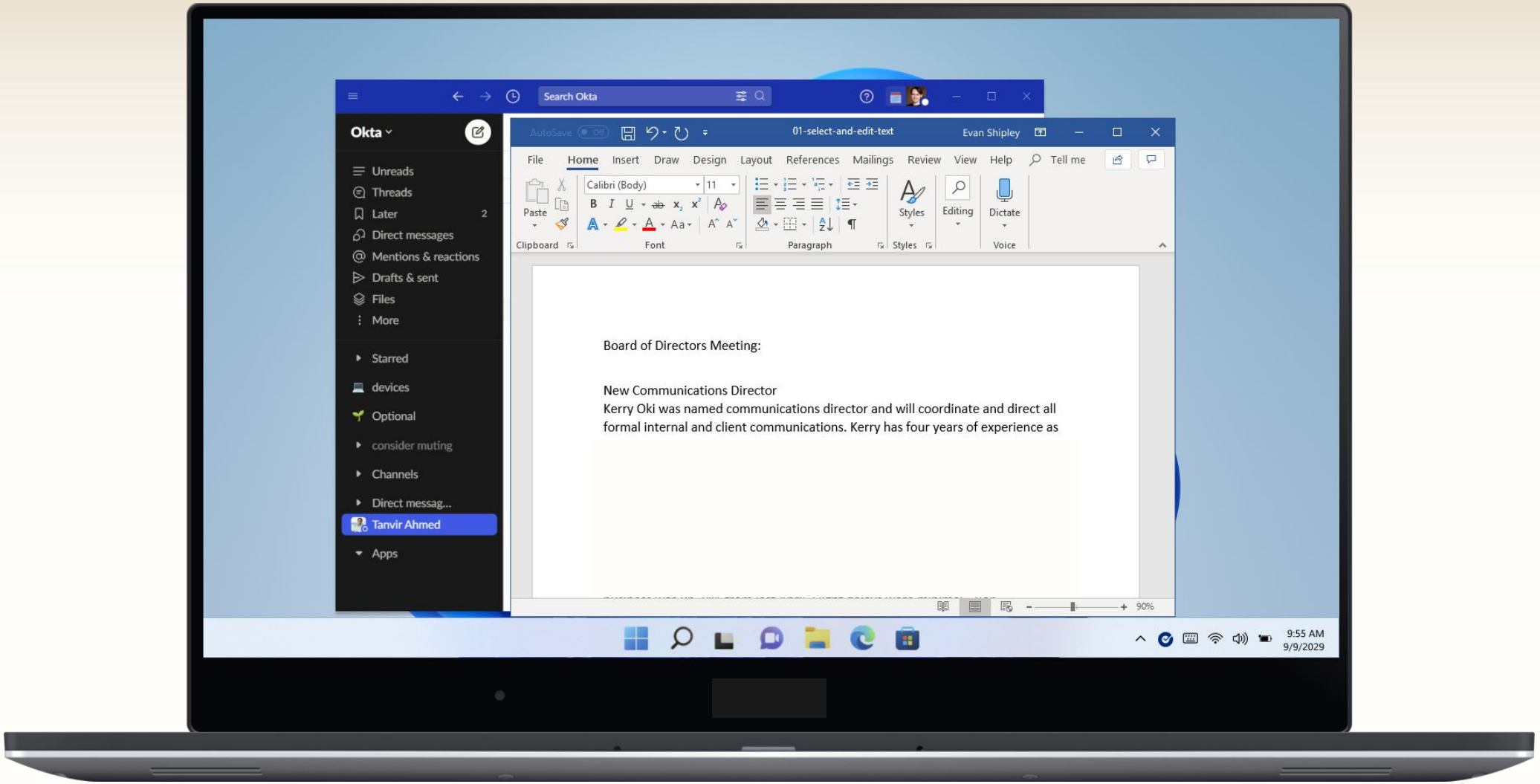


Logged in with Okta Verify running in the background

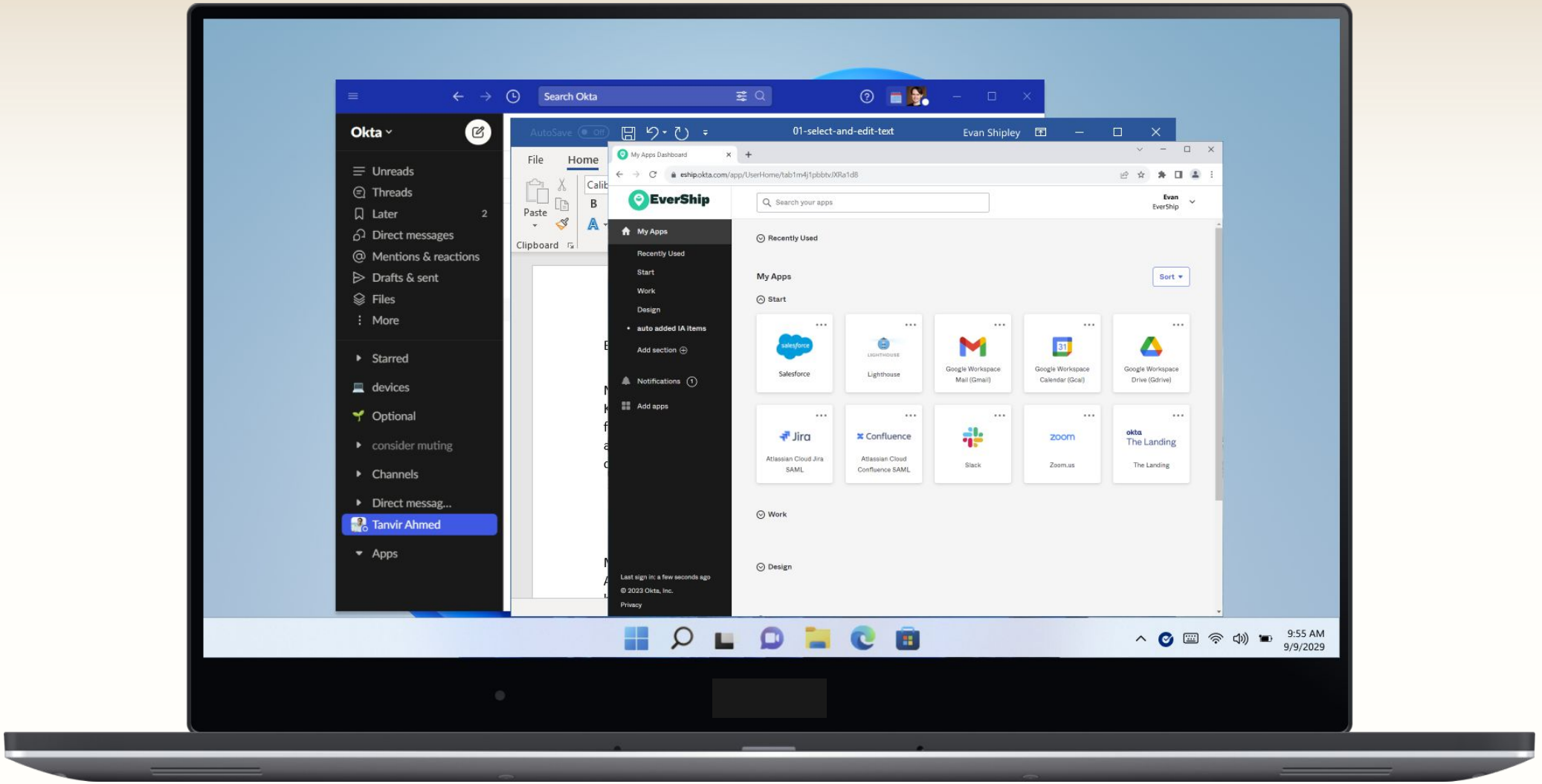
Already signed into Slack through Device Access



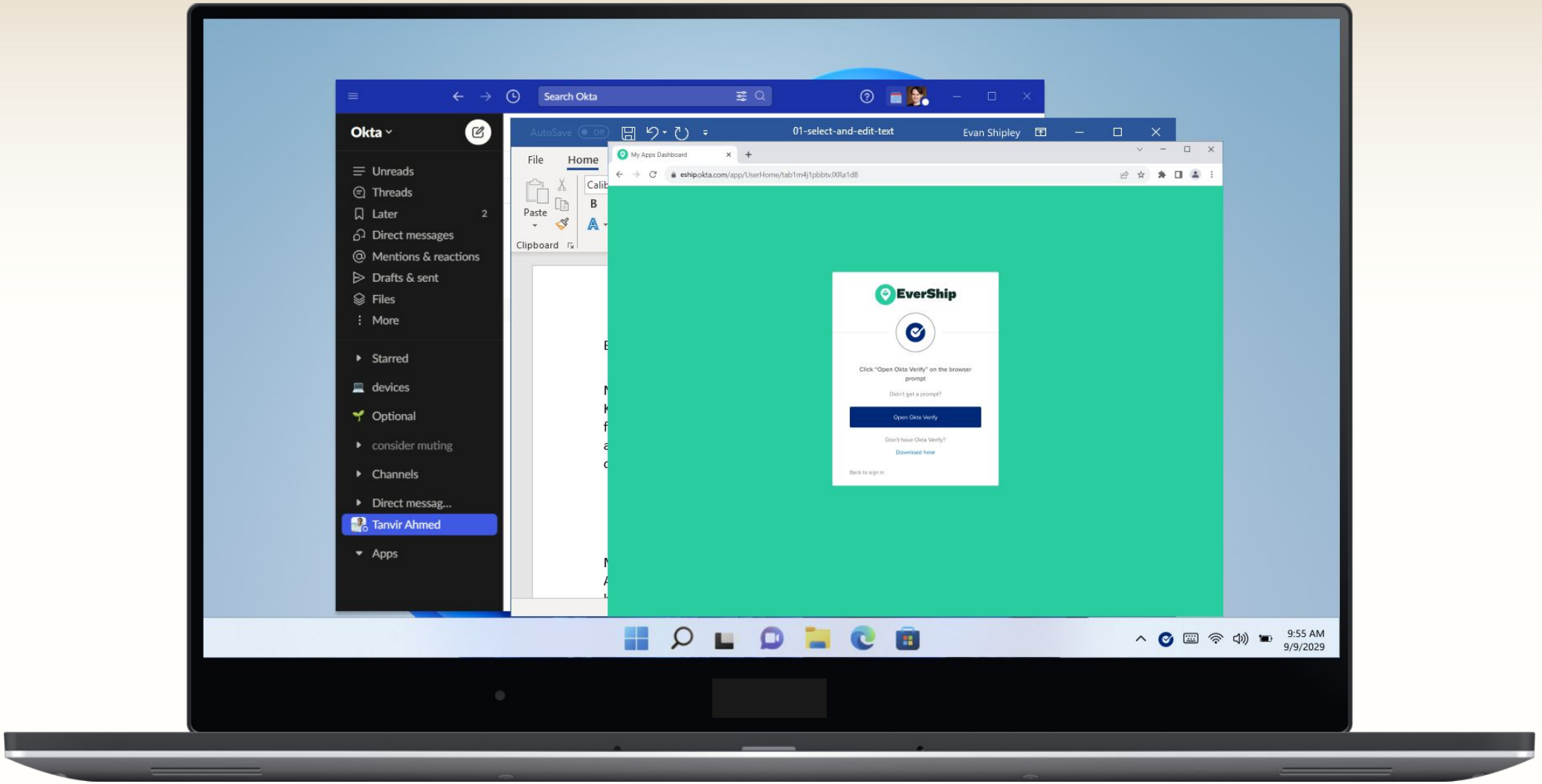
Already signed into Word through Device Access



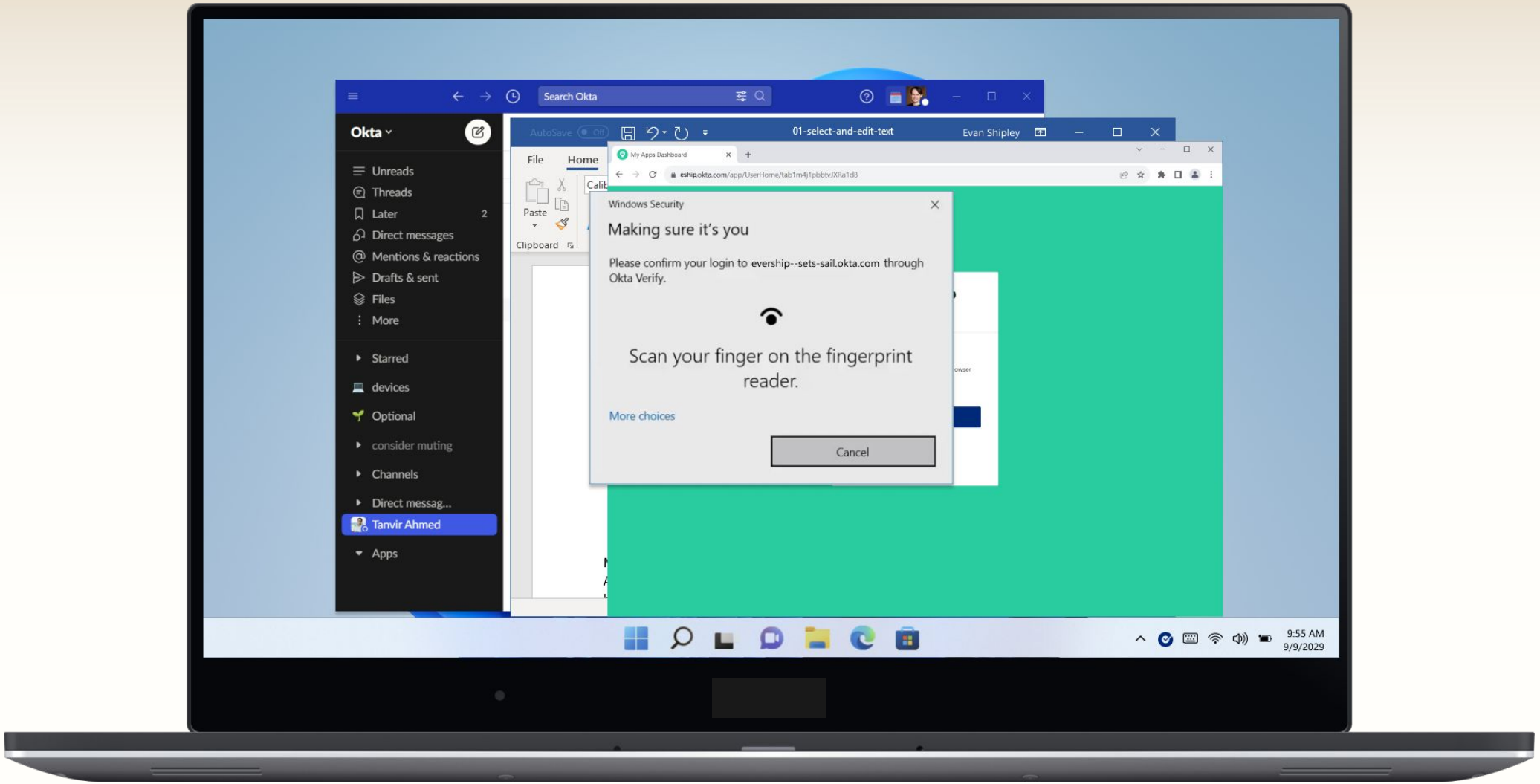
Already signed into browser through Device Access



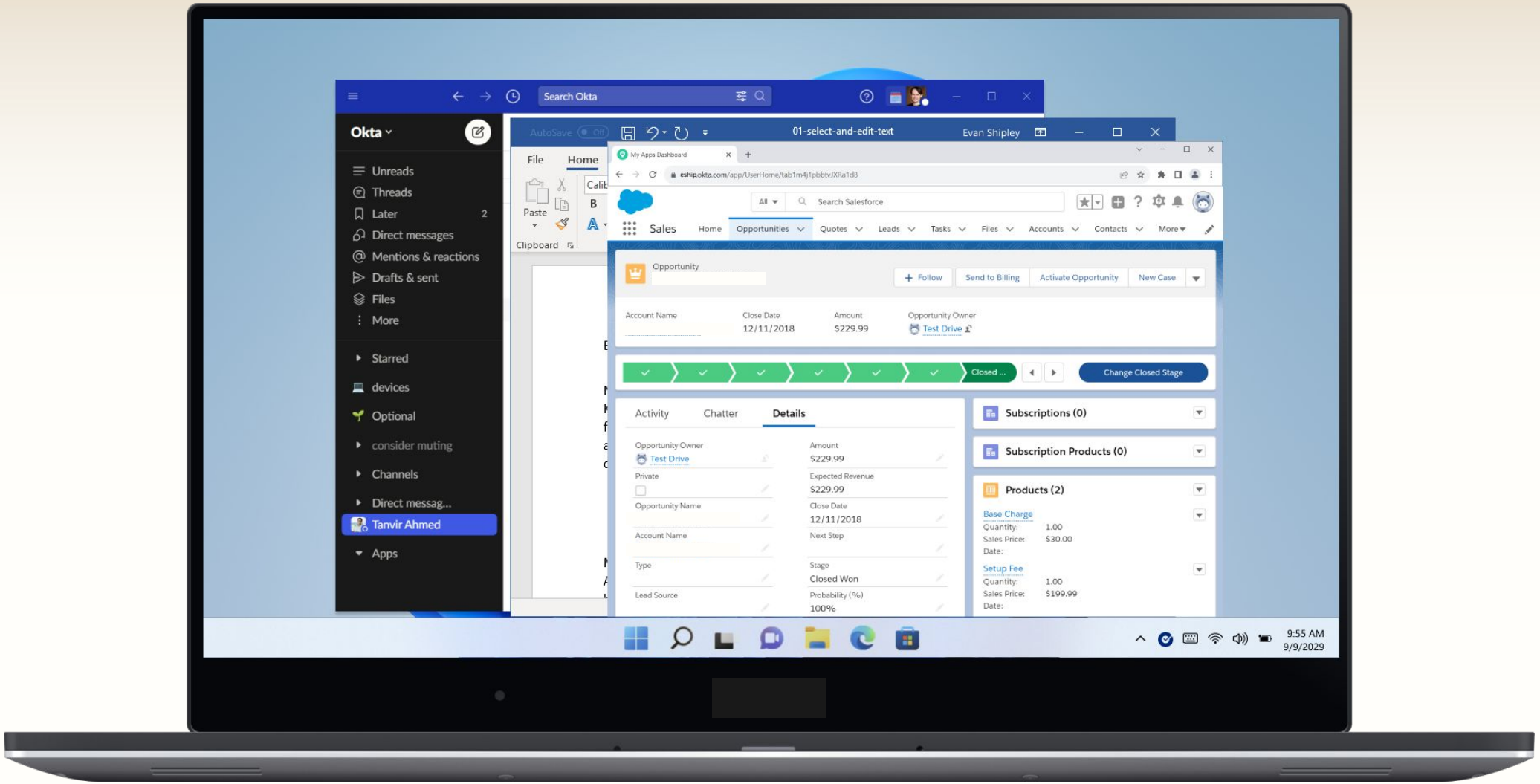
Salesforce triggers FastPass elevation



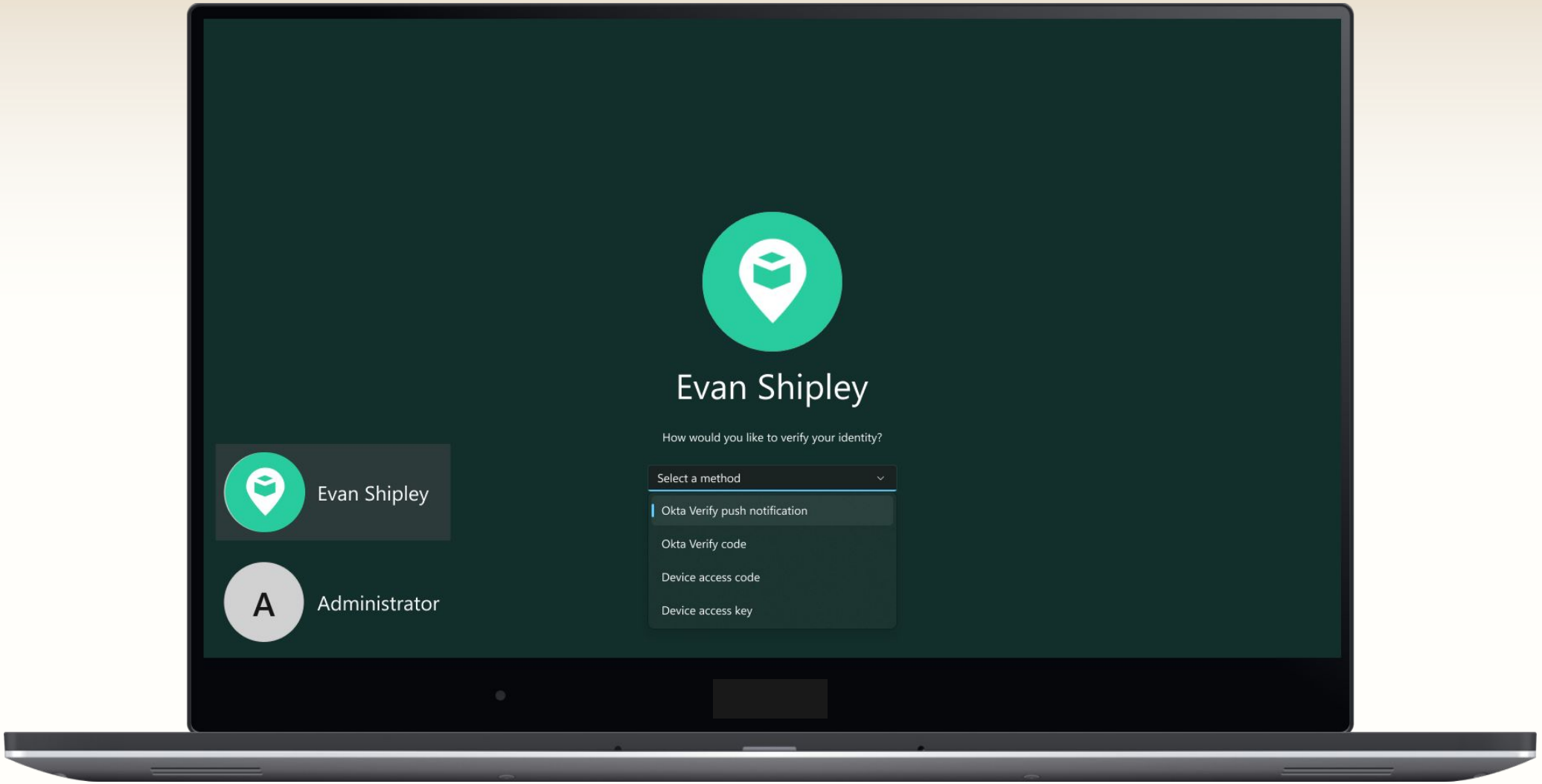
Provide biometrics with FastPass



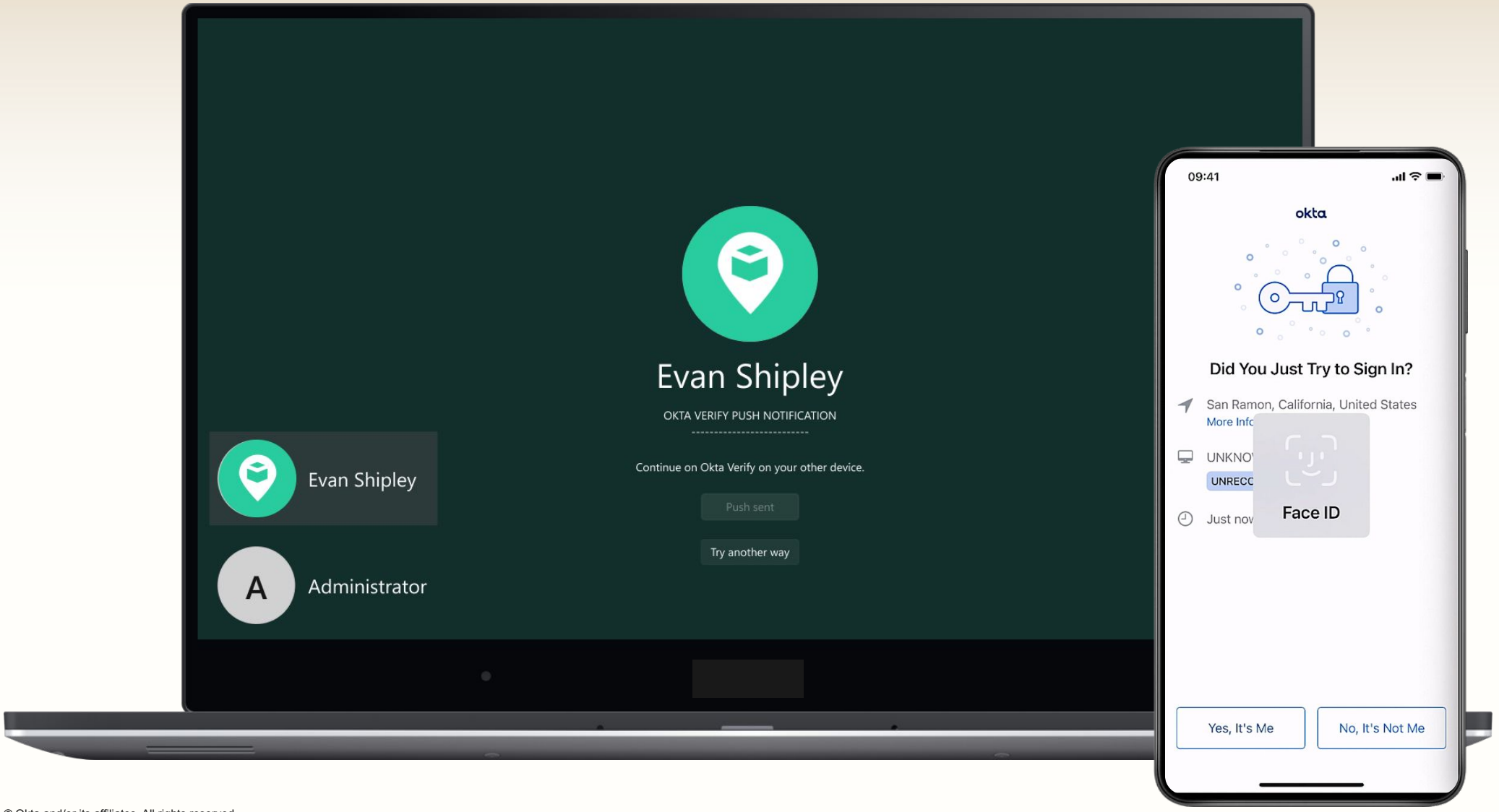
Signed into Salesforce



Daily login experience (even if offline)



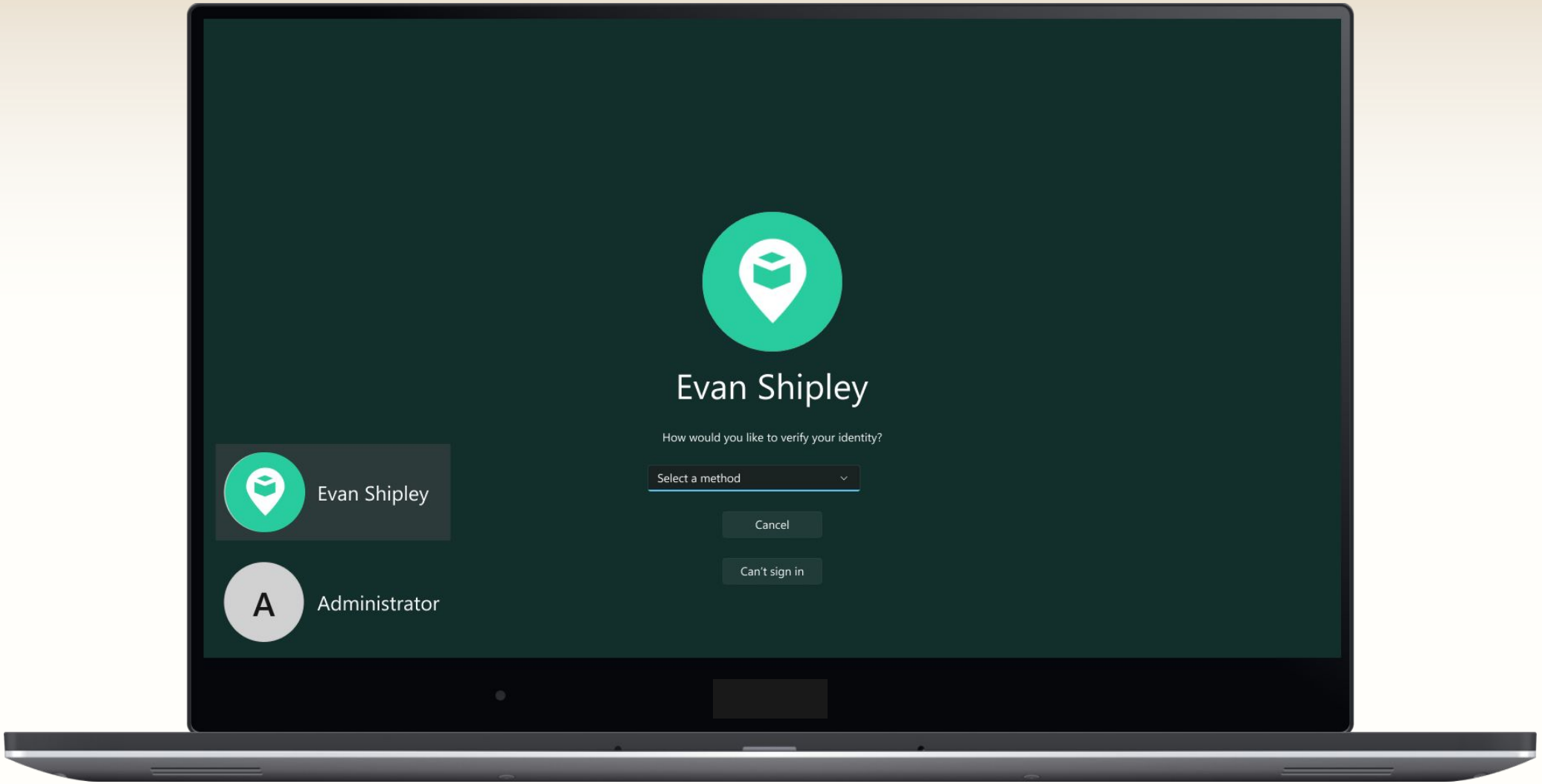
Daily login experience



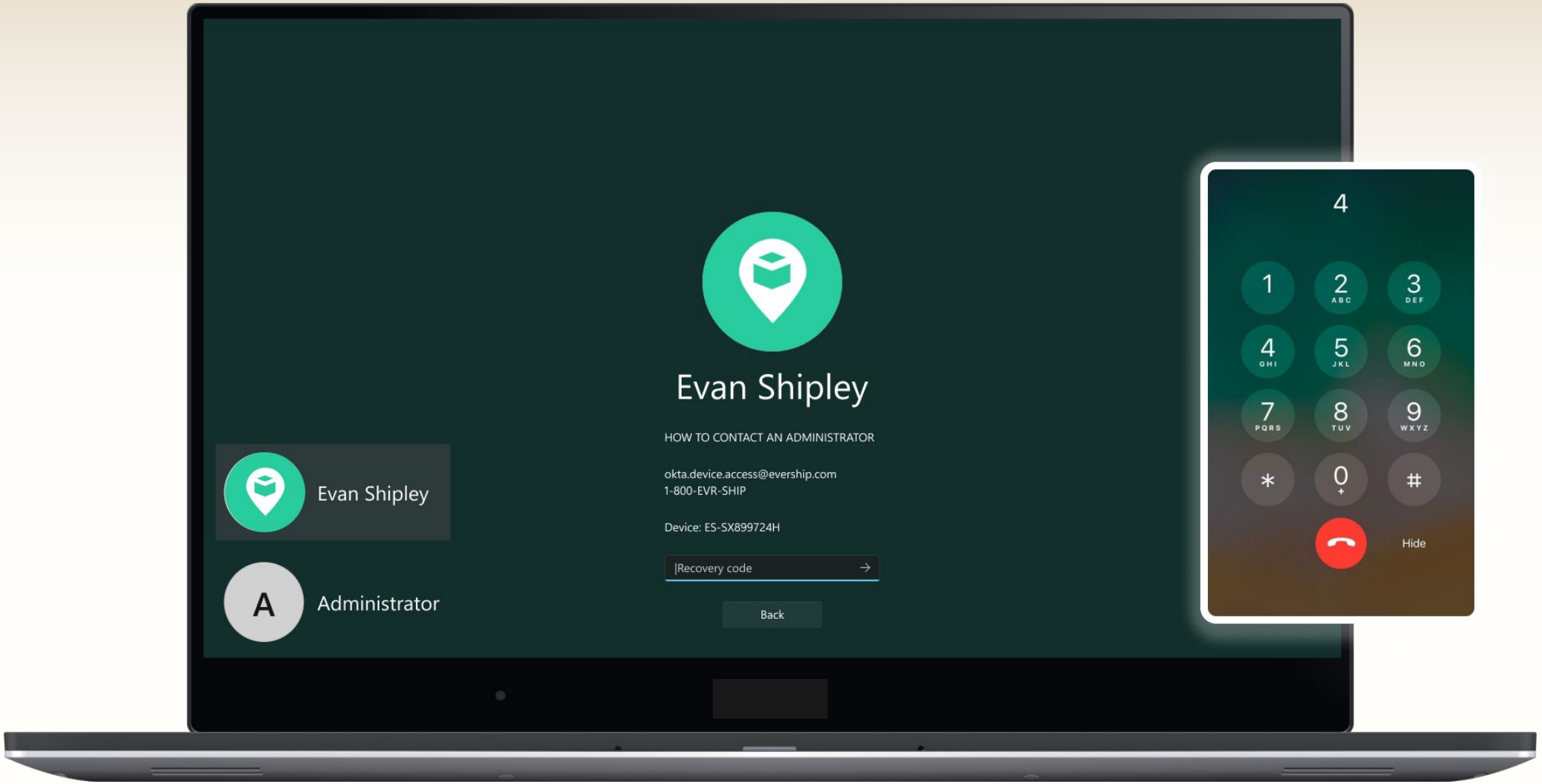
Logged in

okta

Recovery experience (even if offline)



Recovery experience: Contact admin

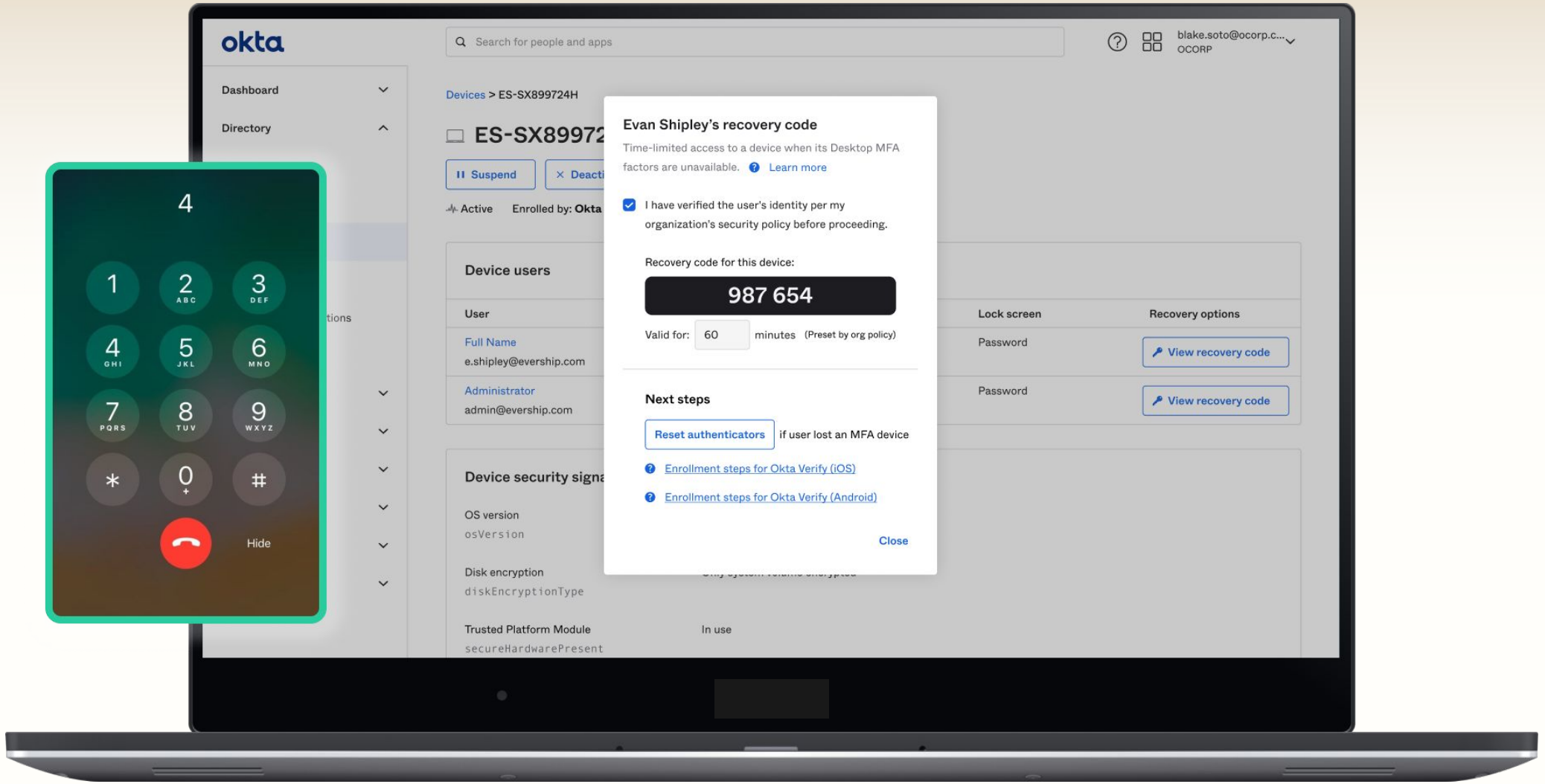


okta

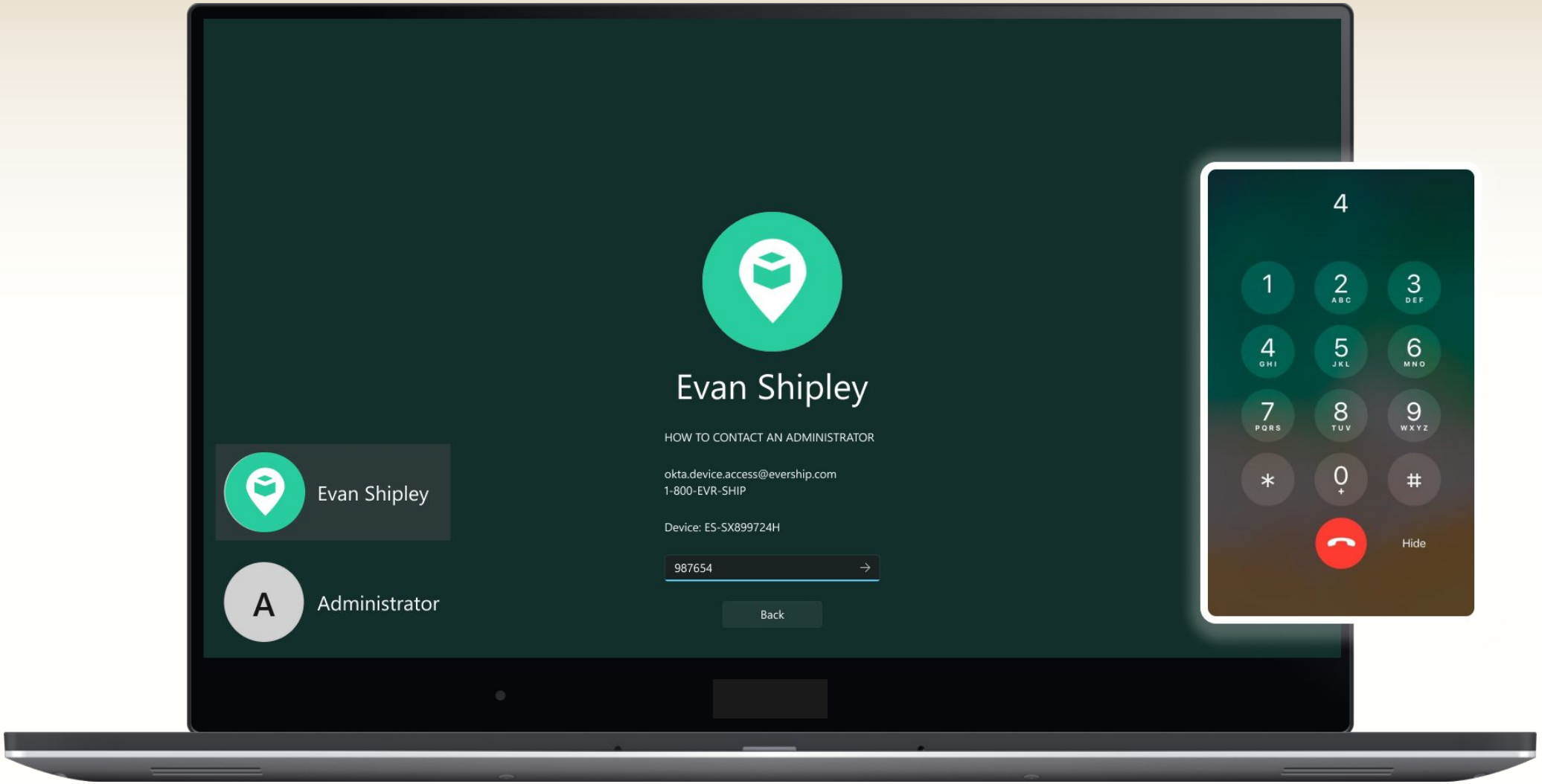
Recovery experience: Verify identity

okta

Recovery experience: Admin code



Recovery experience: Enter code



Logged in with recovery code

Learn more about Okta Device Access

Take a look at the Okta Device Access **solution brief**

Join the Okta Device Access **community group**

okta


okta