

The background is a vibrant, multi-colored gradient. It features a diagonal split between a blue-purple gradient on the left and a yellow-orange gradient on the right. The text 'AWS re:Invent' is positioned on the left side, with 'AWS' in a smaller font above 're:Invent'.

AWS  
re:Invent

W P S 3 1 4

# Amazon WorkSpaces for regulated industries

## **Eric Jones**

Senior Product Manager  
Amazon WorkSpaces  
Amazon Web Services

## **Matt Juaiire**

EUC Specialty SA  
Worldwide Public Sector  
Amazon Web Services

# Agenda

## WorkSpaces capabilities for regulated industries

- Regulatory/Compliance availability

- Features for security posture

## Using Amazon WorkSpaces in the Worldwide Public Sector

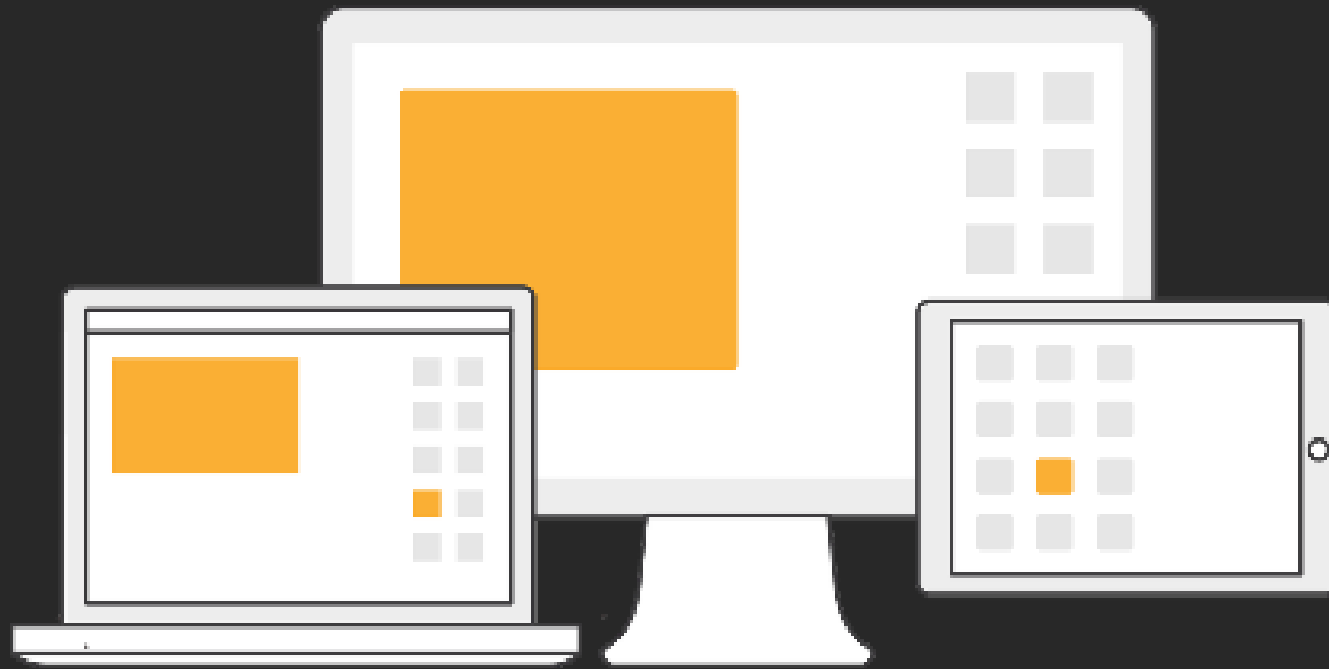
- Using Amazon WorkSpaces to help meet common government security requirements

# WorkSpaces capabilities for regulated industries



amazon  
**WorkSpaces**

A cost-effective, managed cloud desktop for flexible work styles



- Managed desktop as a service (DaaS) offering hosted in the AWS Cloud
- Secure access to the business desktop: Applications, documents, and corporate resources
- Fast, responsive user experience on any network
- Available on wide range of personal devices including iPads, Android tablets, Macs, PCs, laptops, and Chromebooks
- Cloud economics: Scale at your pace and only pay for what you use

# Included with Amazon WorkSpaces

- **Compliance**
  - Ongoing programs
  - Data sovereignty
- **Features and partner solutions**
  - Auditing
  - Security
  - Access controls

# Current compliance programs

- FedRAMP-Moderate
- ISO 27018
- IRAP
- DoD SRG IL2
- PCI
- SOC 1, 2, 3
- Infocomm Media Development Authority
- HIPAA
- GDPR
- ENS

# Amazon WorkSpaces security features: New in 2019

## AWS GovCloud (US-West) launch

- Amazon WorkSpaces is available in the ITAR-restricted AWS GovCloud (US-West) Region

## New compliance accreditations

- IRAP (Australia)
- FedRAMP Moderate & DoD SRG IL2 – N. Virginia and Oregon Regions

## WorkSpaces restore

- Gives customers the ability to restore both root and user volumes to meet data backup requirements for sensitive data



# Using Amazon WorkSpaces in the Worldwide Public Sector

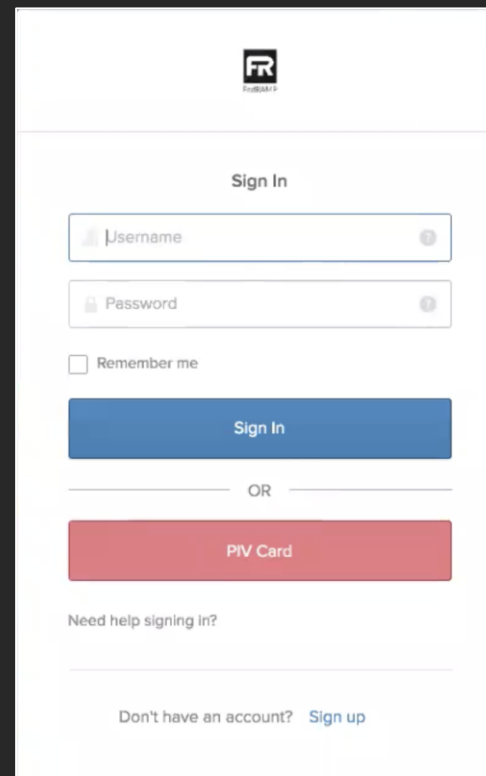
# Highly secure environments

- Secure endpoints
- Enforce AES-256 encryption
- Encryption at rest
- Multifactor authentication

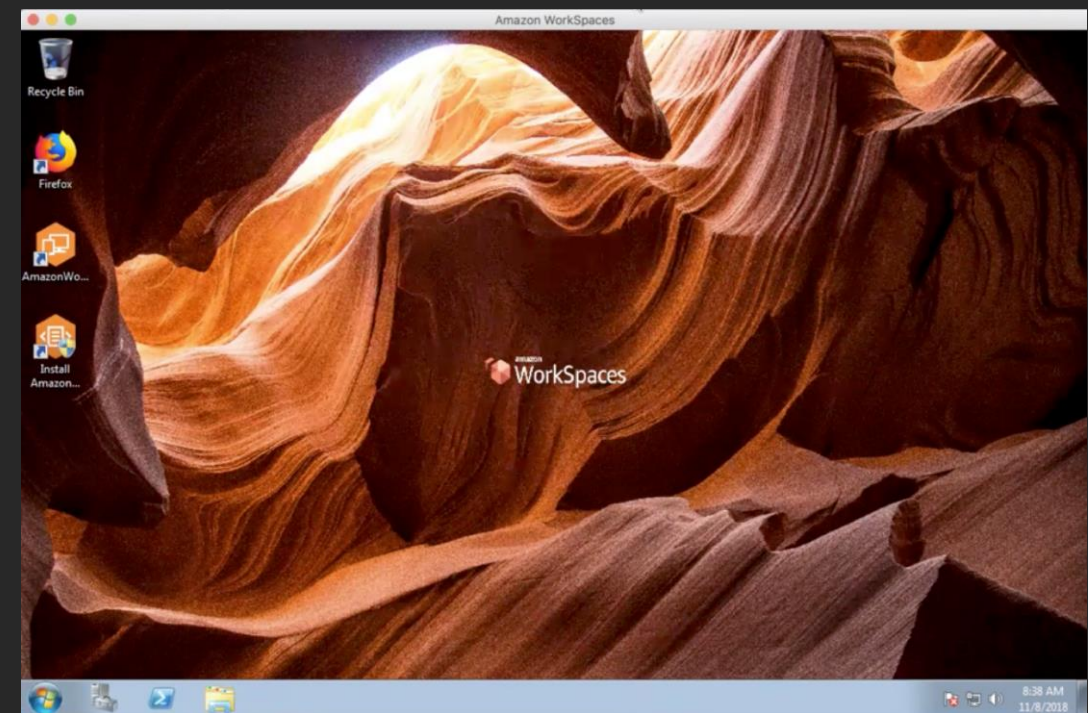
# Amazon WorkSpaces + Okta Federation/smart card use case: Meeting compliance VDI challenges

## Use case challenges

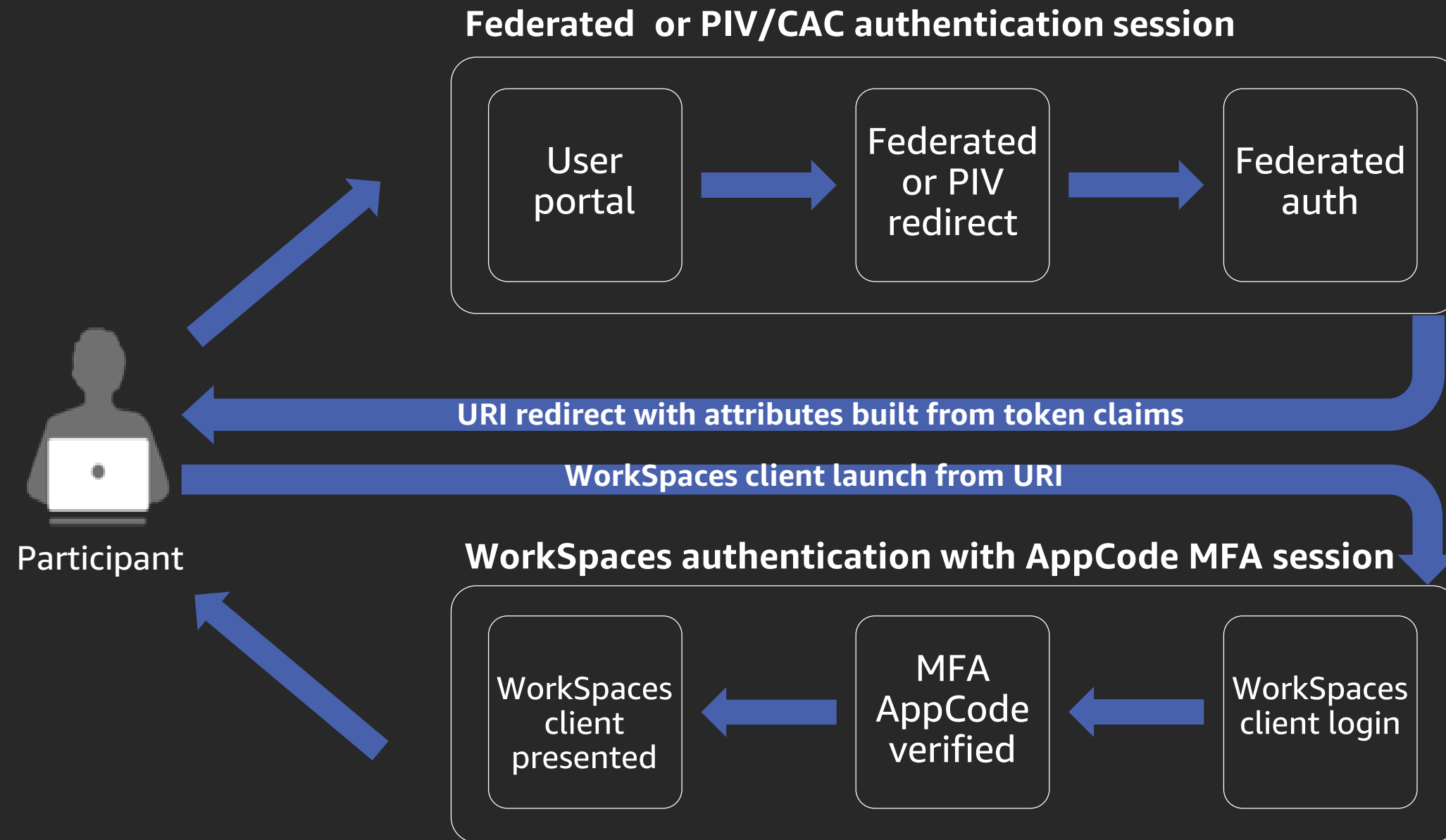
- High-compliance environments need to integrate federated authentication methods for applications, especially in high-security enclaves
- High-compliance environments still need to connect strong authentication from federated sources for virtual desktop
- Optimal customer experience demands to be able to use existing credentials where possible using federation



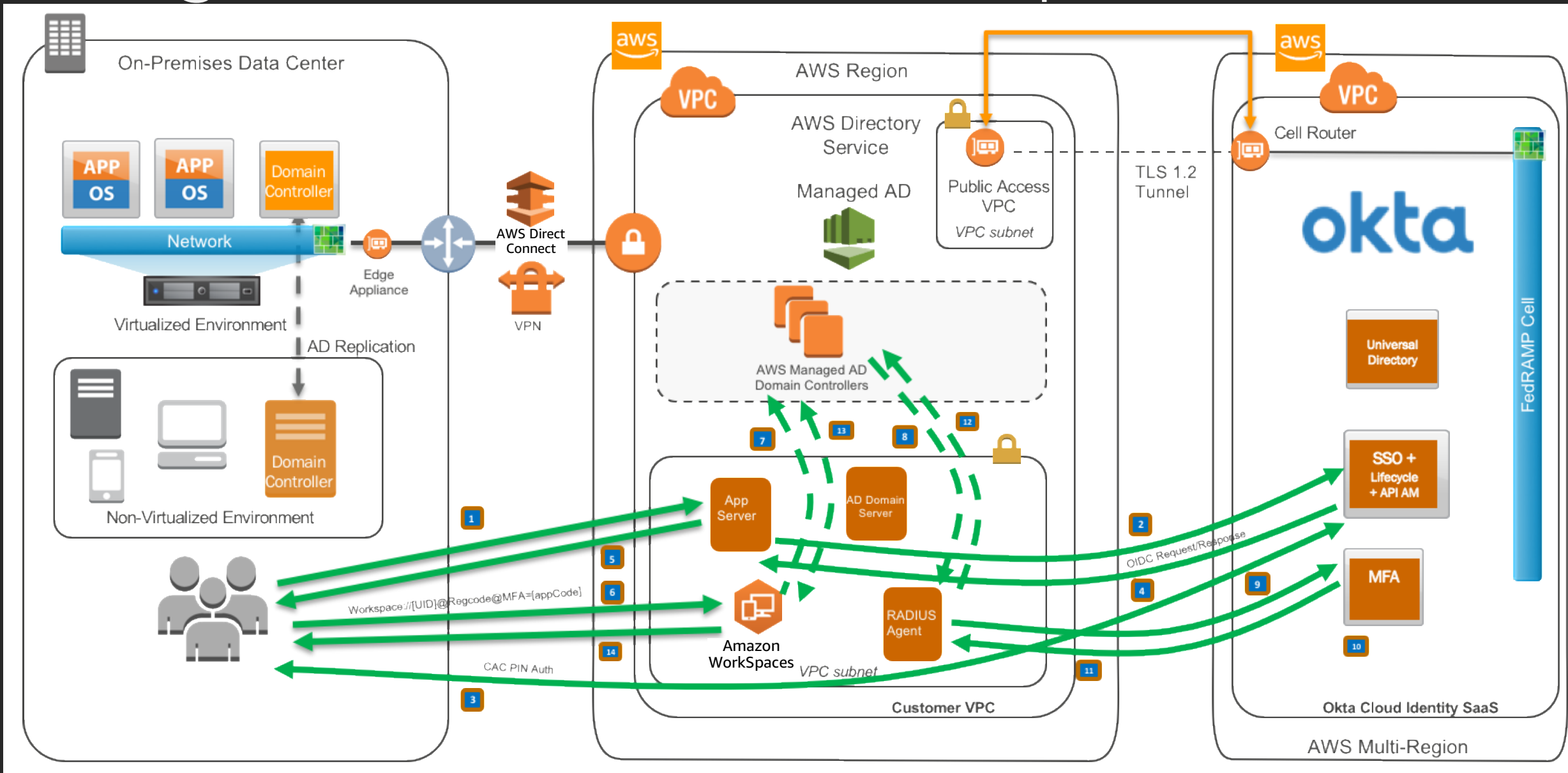
The image shows a web-based sign-in page for Okta. At the top is the Okta logo. Below it is the text "Sign In". There are two input fields: "Username" and "Password". Below the password field is a checkbox labeled "Remember me". A blue "Sign In" button is positioned below the checkbox. Below the button is the text "OR". Below "OR" is a red button labeled "PIV Card". At the bottom of the page, there is a link that says "Need help signing in?". At the very bottom, there is a link that says "Don't have an account? Sign up".



# Amazon WorkSpaces + Okta Federation/smart card high-level-solution user experience



# Amazon WorkSpaces + Okta Federation/smart card integration: User workflow experience



- 1 End user clicks on login app
- 2 OIDC auth request started
- 3 OIDC IdP auth complete with PIV/CAC Pin
- 4 OIDC response with ID token; login app decodes for IdP ID validation
- 5 Redirect from login app launches WorkSpaces app
- 6 WorkSpaces app launches with URI contents including Username, RegCode, and MFA app code
- 7 WorkSpaces authenticates to Managed AD directory
- 8 Managed AD calls to RADIUS agent for MFA and passes app code
- 9 RADIUS agent calls to Okta for MFA response
- 10 Okta MFA validates with app code provided in URI launch
- 11 Okta MFA returns MFA status to RADIUS agent
- 12 Okta RADIUS agent returns RADIUS accept or reject to Managed AD
- 13 Managed AD returns auth status to WorkSpaces
- 14 WorkSpaces completes auth and starts session

# Q&A

# Appendix: WorkSpaces features



# IP-based access controls

## Control WorkSpaces access

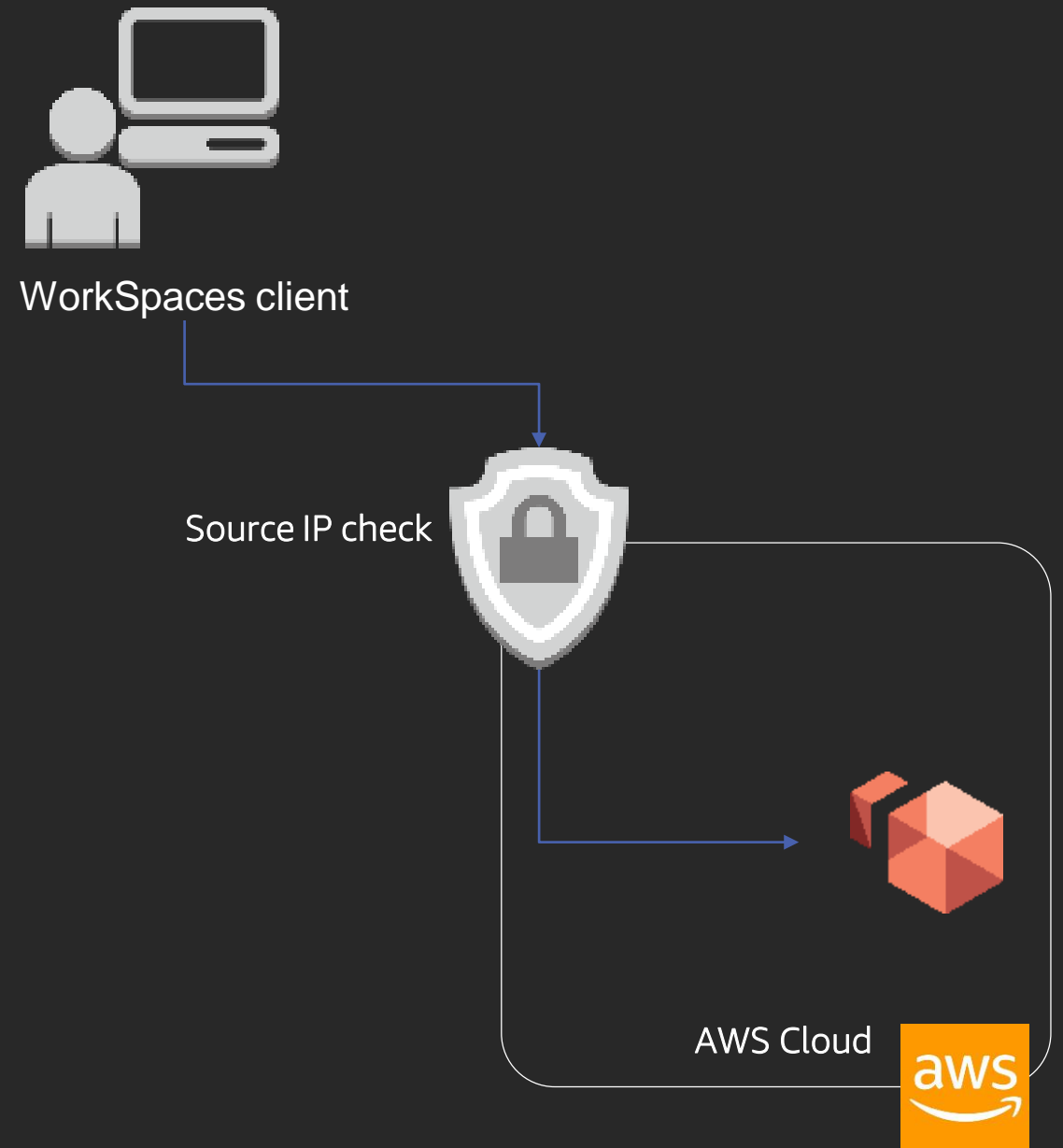
- Select IP addresses from which users can access WorkSpaces
- Create groups of custom rules specifying from which IP addresses users can access WorkSpaces

## Benefits

- Ensure that Amazon WorkSpaces is only accessed from trusted networks
- Groups can be applied at the individual directory level from the WorkSpaces console or through APIs

## Limitations

- Cannot be enabled for the Web Access client





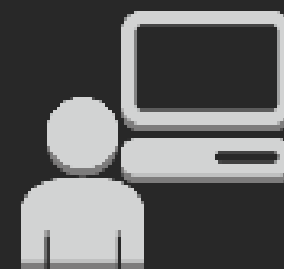
# Amazon CloudWatch Events on WorkSpaces access

## Identify WorkSpaces access

- View, search, download, archive, analyze, and respond to successful logins to your Amazon WorkSpaces
- Monitor client WAN IP addresses, operating system, WorkSpaces ID, and Directory ID information for users' logins to Amazon WorkSpaces

## Benefits

- Learn when, where, and how your users log into and access their Amazon WorkSpaces
- Monitor client WAN IP addresses, operating system, WorkSpaces ID, and Directory ID information for users' logins to Amazon WorkSpace
- Set up automated actions based on how a WorkSpace is accessed



WorkSpaces client

WorkSpaces access event  
(on login success)



CloudWatch Events



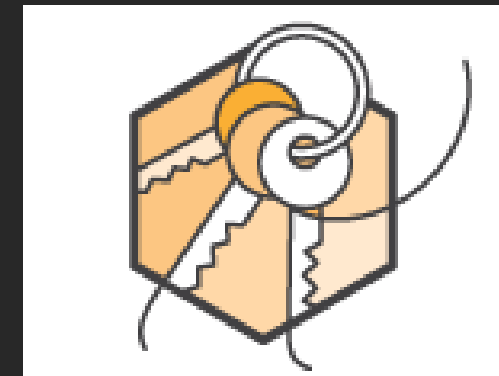
# Certificate authentication

## Benefits

- Access control based on the client device type and certificates
- Managed device authentication

## How does it work?

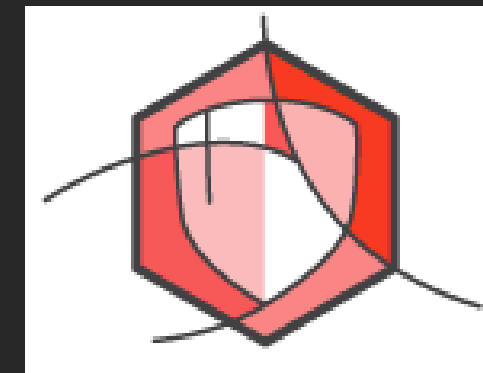
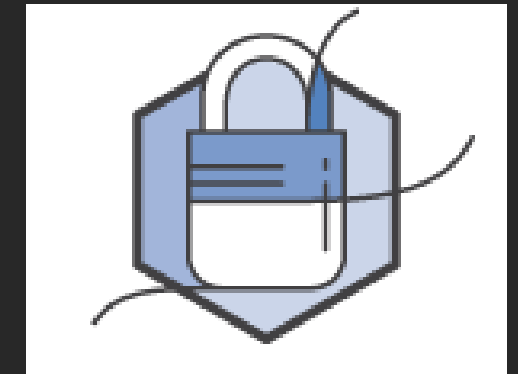
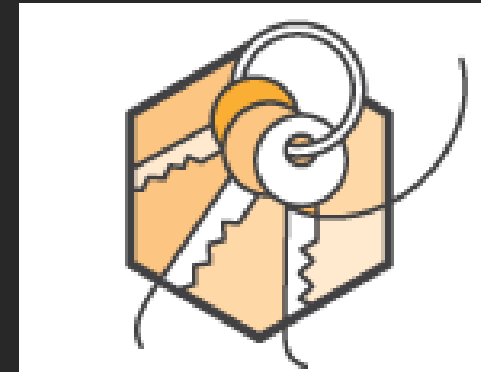
- Customers deploy device certificates to managed devices
- WorkSpaces service stores root certificate with public key only
- WorkSpaces application makes authentication request and the service returns a randomly generated nonce along with root certificate
- App locates device cert chaining to root authority of the certificate provided by the service
- App uses private key of the device certificate, signs the nonce provided by the service, and sends to service along with public key
- The service validates if the nonce is signed by device certificate and allows authentication to proceed



# Encryption

## Encrypt WorkSpaces volumes

- Data in transit and rest is encrypted using AES 256-bit encryption
- Integrates with the AWS Key Management Service (AWS KMS)
- Use your AWS KMS keys to encrypt Amazon WorkSpaces
- Encrypt up to 30 Amazon WorkSpaces with a single key
- Can encrypt both root and user volume
- No material performance impact
- **Pricing**
  - Pay for AWS KMS keys and Amazon WorkSpaces—no additional charge



# Partner Solutions

- Authentication portals
- Multifactor authentication
- Endpoint inspection
- Anti-virus protection
- Network inspection
- Web proxy

# Related sessions

## Wednesday, December 4<sup>th</sup>

EUC341: Why GE Renewable Energy and Multiview stream their desktop applications

9:15 am – 10:15 am | Bellagio, Monet 3

---

## Wednesday, December 4<sup>th</sup>

EUC331: Moving to SaaS? Deliver desktop apps as web apps with no rewrite

10:00 am – 11:00 am | Mirage, St. Thomas A

---

## Wednesday, December 4<sup>th</sup>

ENT314: How GE Power empowered its departments to manage & stream their desktop apps

1:45 pm – 2:45 pm | Bellagio, Grand Ballroom 1

---

## Wednesday, December 4<sup>th</sup>

EUC338: Why Carnival Cruise Line moved from on-premises VDI to Amazon WorkSpaces

4:00 pm – 5:00 pm | MGM, Level 3, Chairman's Ballroom 366

---

## Wednesday, December 4<sup>th</sup>

EUC404: How Facebook deployed Amazon WorkSpaces globally

5:30 pm – 6:30 pm | MGM, Level 1, Grand Ballroom 119

---

## Wednesday, December 4<sup>th</sup>

EUC405: Amazon WorkSpaces Streaming Protocol: Enable a consistent user experience

6:15 pm – 7:15 pm | Aria, Level 3 West, Ironwood 8

# Customer Reception

---

**Wednesday, December 4<sup>th</sup>**

**[eucappsreception.splashthat.com](http://eucappsreception.splashthat.com)**

6:00 pm – 8:00 pm | Canaletto Ristorante Veneto at the Venetian

---

# Thank you!

**Eric Jones**

[ejjonesa@amazon.com](mailto:ejjonesa@amazon.com)



Please complete the session survey in the mobile app.