UP NEXT

To Bind or not to Bind: A guide in 2020

Session Start Time - End Time *(JNUC team will add this)*

JNUC

VIRTUAL

CONFERENCE

2020

Johan McGwire

Systems Engineer

Coinbase

Slack - @Yohan

Github - @Yohan460

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

To Bind or not to Bind: A guide in 2020

Presentation agenda:

- Define the deployment situations
- Evaluate different identity methods
- Discuss the security implications
- Random Topics
- Assess the transition away from binding

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Preface

- Views are my own
- Opinionated piece
- Very dynamic environment

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Deployment Requirements

1. Automated Device Enrollment
2. Externally Facing MDM
3. Centralized Identity Infrastructure
   - Cloud Identity
   - On Premise Identity

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

What Happened at WWDC

- Local accounts strongly recommended
- Leverage identity to your advantage

Sessions

- Leverage enterprise identity and authentication
- Deploy Apple devices using zero-touch

JNUC

VIRTUAL

CONFERENCE

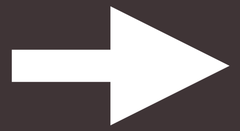
2020

coinbase

Identity Types

On Premise

- Active Directory
- Open Directory
- LDAP
- etc…



Cloud

- Azure
- Okta
- G Suite
- etc…

JNUC

VIRTUAL

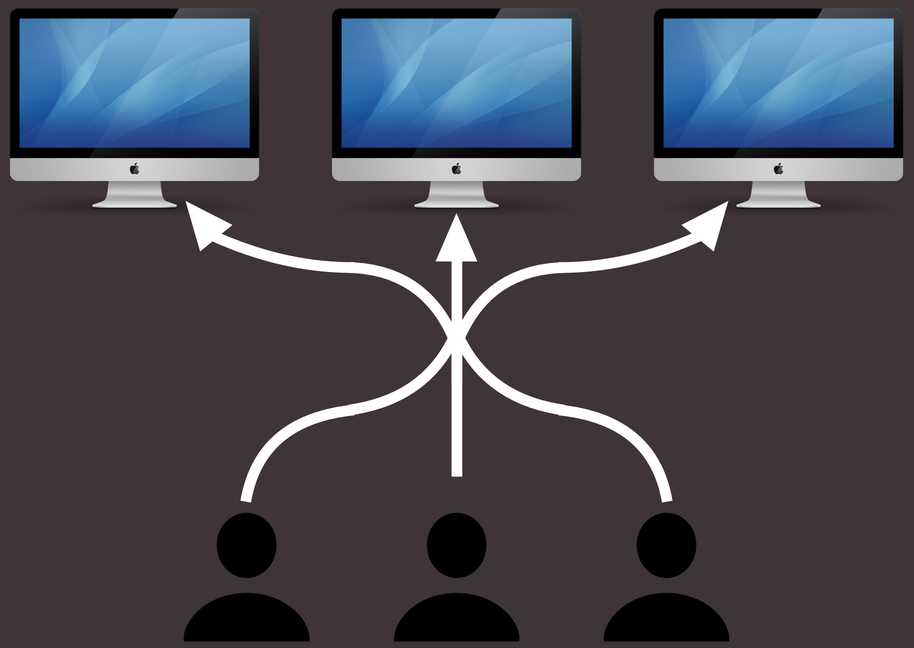
CONFERENCE

2020

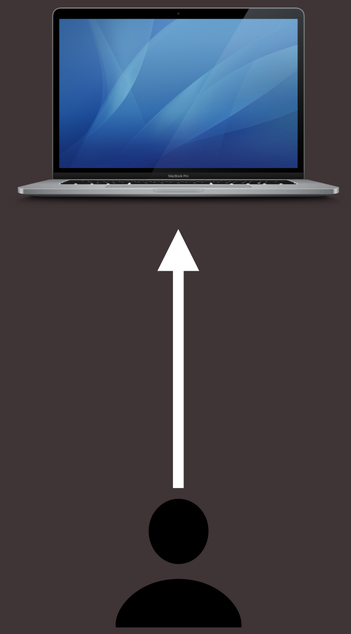
coinbase

Deployment Scenarios

Many to Many



One to One



JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Issues with Traditional Binding

- Keychain synchronization prompts
- Difficult health reporting

Remote Challenges

- FileVault password irrecoverability
- Password Synchronization at login

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Many to Many Options

On Premise idP → Traditional Bind

On Premise idP → NoMAD Login
- Local accounts
- Agent capabilities

Cloud idP → Jamf Connect
- Restrictions per idP
- Local accounts

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Realms of User Creation

Login Window

Traditional Bind

NoMAD Login

Jamf Connect

Etc…

Setup Assistant

Credential Auth

SSO Enrollment Customization

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Setup Assistant vs Login Window

- Authenticate before enrollment
  - No pre-loaded identifiable assets
  - No pre-installed programs
  - No organization specific settings
- Apple supported method

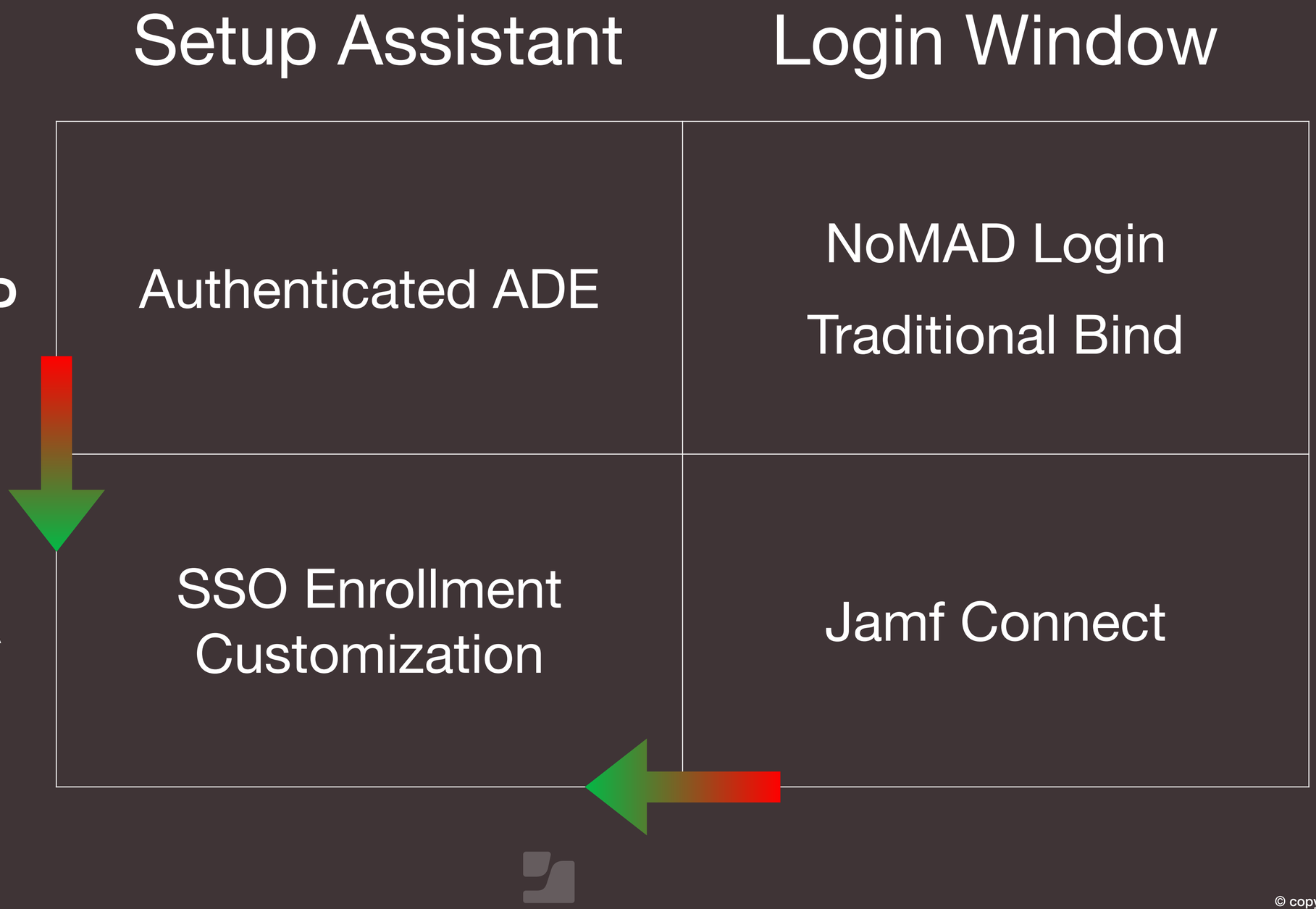
JNUC

VIRTUAL

CONFERENCE

2020

coinbase



JNUC

VIRTUAL

CONFERENCE

2020

coinbase

One to One - Login Window

NoMAD Login & Traditional Bind

- Password sync with on-premise idP
- Requires direct domain connectivity

Jamf Connect

- Password sync
- MFA capability

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

One to One - Setup Assistant

Credential Authenticated ADE

- Initial password sync with on-premise idP

SSO Enrollment Customization

- No password sync
- MFA capability

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Password Synchronization

- No direct security benefit
  - Some niche scenarios
- Enforce via MDM configuration profiles
- Password de-sync is more secure
  - Adds another hurdle for attacker

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Binding with Local Accounts

- DFS (Directory File Shares)
- 802.1X Certificates - **Many additional options**
  - Jamf ADCS Connector
  - SCEP Proxy

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

FileVault...

- Not advisable in Many to Many scenarios
- FileVault screen =/= Login window
  - Dual auth for LW replacements
    - Disable-able via recovery mode
    - Bad user experience

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Transitioning from the bind

- Scripted per account - **Hard**
- NoMAD Login Mechanism - **Easy**
  - NoLo v1.4
  - Automatic demobilization during login
    - FileVault or LoginWindow
    - SmartCard capabilities

JNUC

VIRTUAL

CONFERENCE

2020

NoLo Demobilization PostInstall

```
# Insert the Demobilization mechanism
authchanger -reset -demobilize

# Enabling the Demobiliztion
defaults write /Library/Preferences/menu.nomad.login.ad.plist DemobilizeUsers -bool true
```

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Smartcards

- Attribute Mapping predominantly used
  - Tied to unpreserved account attribute
  - Programmatically added for Local accounts
  - Preservation possible with demobilization

NoLo Demobilization PostInstall

```
# Saving the AltSecurityIdentites account attribute
defaults write /Library/Preferences/menu.nomad.login.ad.plist DemobilizeSaveAltSecurityIdentities -bool true
```

JNUC

VIRTUAL

CONFERENCE

2020

coinbase

Sources

- NoMAD Login Gitlab
- Apple MDM Guide
- Demobilization Script - rtrouton
- WWDC 2020

JNUC

VIRTUAL

CONFERENCE

2020

Thank you for listening!

Give us feedback by completing the 2-question session survey in the JNUC 2020 app.

UP NEXT

Session title *(JNUC team will add this)*

Session time (JNUC team will add this)