DEP - The Right Way

O&G

ORCHARD & GROVE

Joel Rennich

Chief Instigator

Joel Rennich

NoMAD Creator

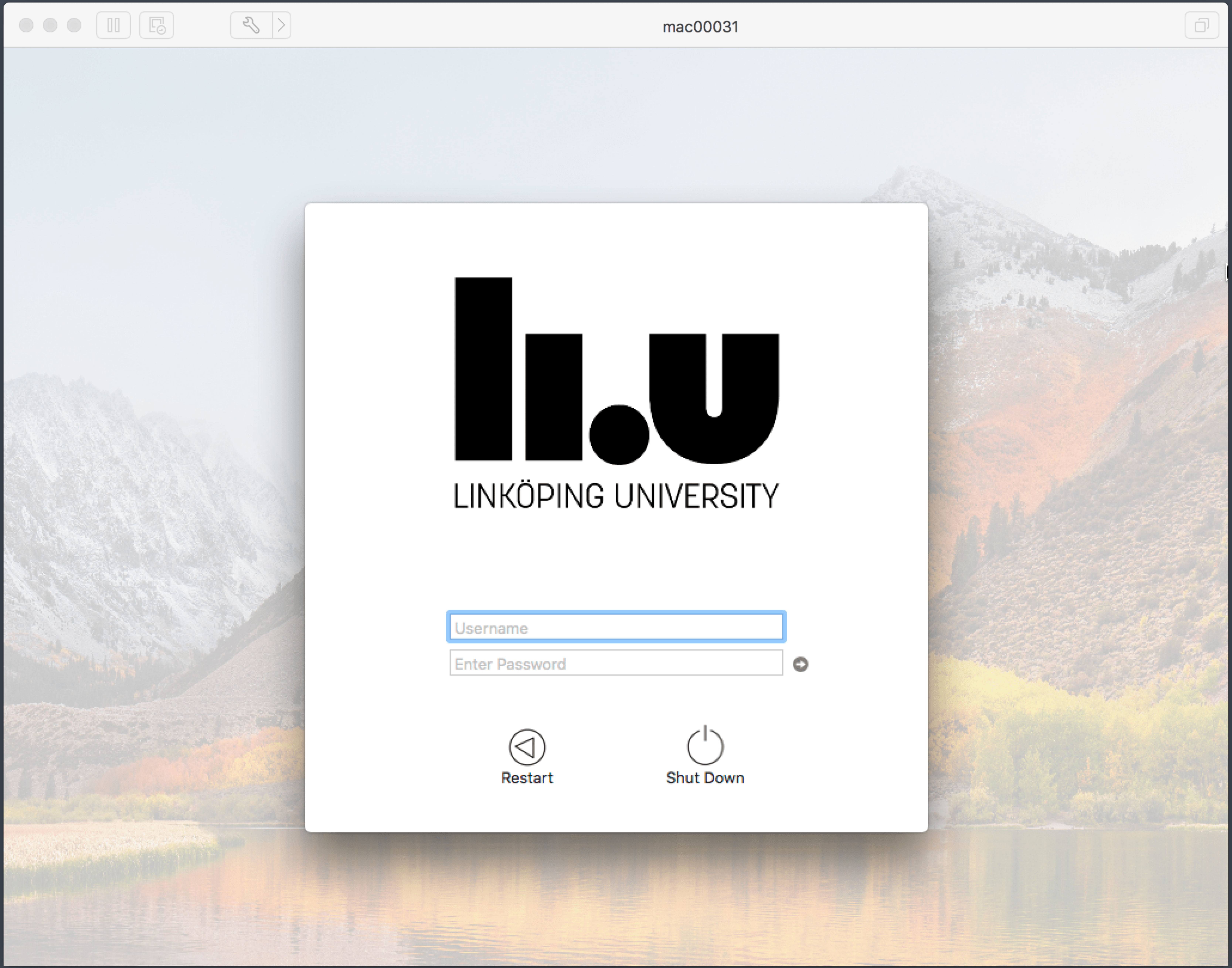
Product Director, Jamf

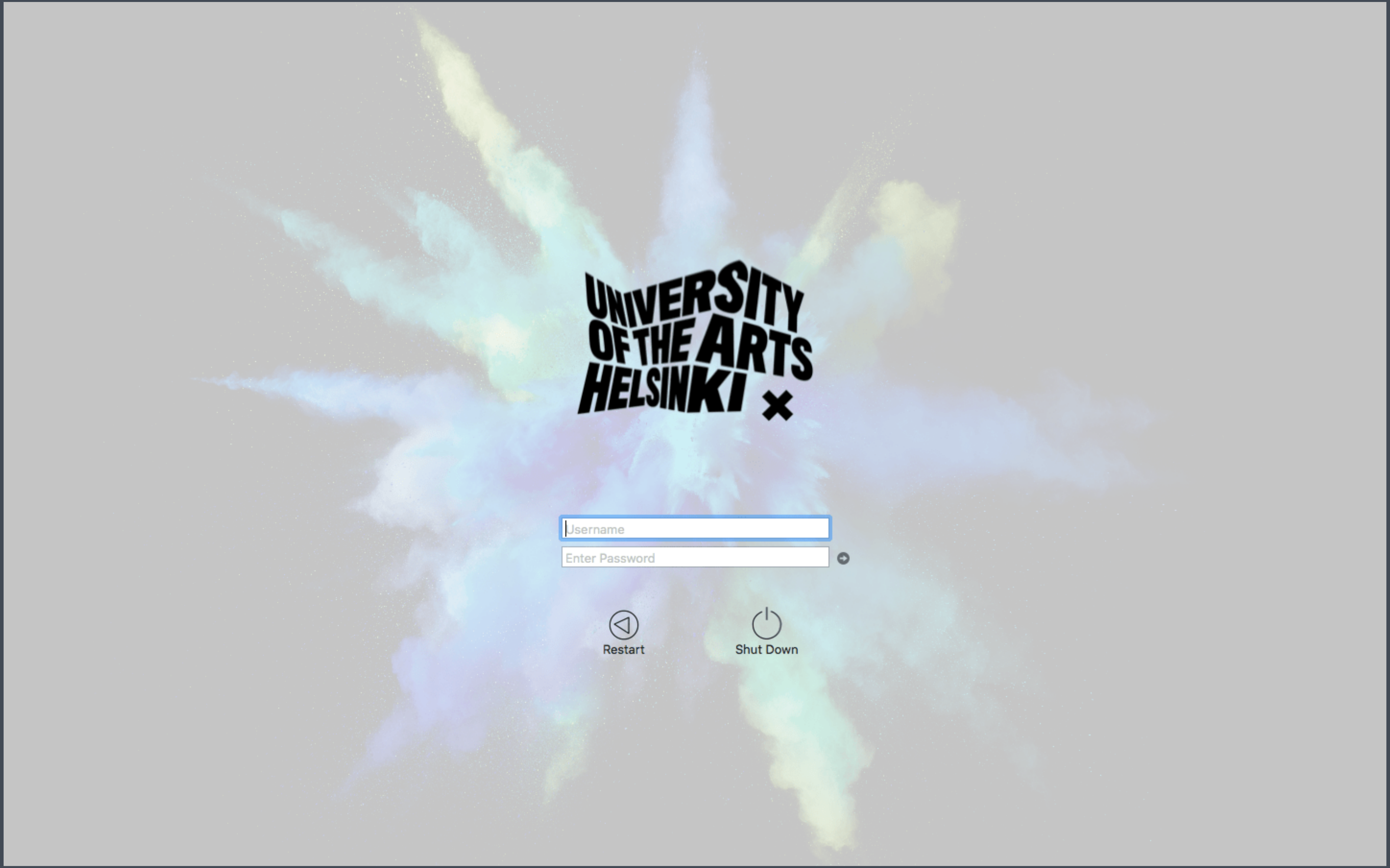
Sér ei skáldið skip á öldu
skautum búið að landi snúa?
er ei þys við þorskakasir?
þóttast ekki búðadróttir?
Harður byr að hafnavörum
húna- rekur -jóinn lúna,
glatt er lið á götustéttum,
glápa sperrtir búðaslápar.

Skipkoma, 1830 - Jónas Hallgrímsson

GOTHENBURG

NoMAD
LOGIN

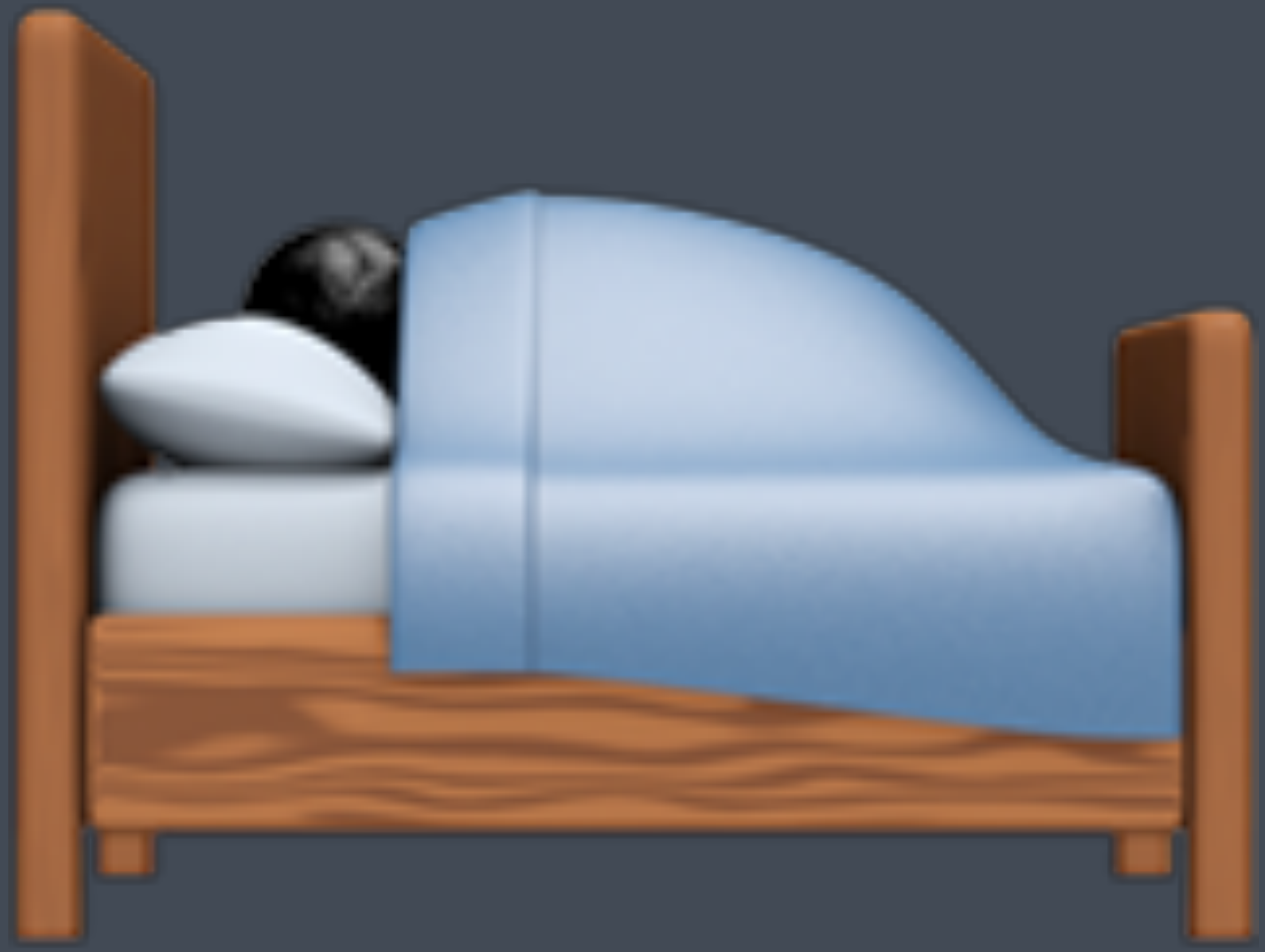

mac00031
LINKÖPING UNIVERSITY
Username
Enter Password
Restart
Shut Down



UNIVERSITY OF THE ARTS HELSINKI
Username
Enter Password
Restart
Shut Down

Enrollment is the beginning

Enrollment is the beginning



Ordinary meaning

Dreaming of a single banana [redacted] dream of a banana, [redacted] about [redacted] either you’re too affectionate towards others or maybe you’re not affectionate at all. Eating bananas in the dream states a new beginning in business affairs.

Decaying banana dreams indicate a business disagreement. Such a dream is related to the non-productive behavior. Dreaming of eating a banana is related to working hard but unable to achieve the goal. If you generally don’t like having a banana, it states that you’ll surely not enjoy the process that is needed to reach the goal.

- http://dreamatico.com/banana.html

Enrollment is the beginning

Use MDM to get a loginwindow or other bits on the disk, then do more from there

Enrollment is the beginning

DEP Workflow Components

1. Validation
2. Authentication
3. Information
4. Configuration
5. Notification

DEP Workflow Imperatives

1. Before the Finder
2. Only ask for the password once
3. Modular
4. Extensible

Step 1: Validation

Validation

- Ensure host has the correct security posture
- Remediate any issues, or block the login process
- Use Notify mechanism to show any UI to the users

Requirements

- Able to use any update system
- Can block the login process if posture check fails
- Outside of the user space, needs to be root

Step 2: Authentication

Authentication

- Authenticate user against AD, Okta, cloud identity provider
- Ideally using MFA
- Just in time user creation
- Verify user should have access, is an admin, other rights

Requirements

- If SAML, get auth token and refresh token
- Read in user record to create account or other things
- Rules-based access
- Demobilize users at login

Step 3: Information

Information

- Gather information from the user
- Can then be used to determine later configurations or other actions

Requirements

- Dynamic amount of text fields
- Dynamic amount of pull down menus
- Store information in a configurable location
- Positively agree to EULA

Step 4: Configuration

Configuration

- Process running as root
- Call Jamf policies, Chef, Munki, home made service, other MDM, etc…
- Ability to show UI

Requirements

- Enable FileVault
- Change wireless networks
- Local key escrow to add additional users to FileVault

Step 5: Notification

Notification

- Dynamic feedback to the user as to what’s going on
- Notification if you need to take remedial action
- Able to run multiple times within the login process

Login Window basics

Loginwindow

- Works linearly through mechanisms
- Can run as SecurityAgent or root
- Use SecurityAgent for UI
- All mechanisms must agree before login

```
<string>builtin:policy-banner</string>
<string>loginwindow:login</string>
<string>builtin:login-begin</string>
<string>builtin:reset-password,privileged</string>
<string>builtin:forward-login,privileged</string>
<string>builtin:auto-login,privileged</string>
<string>builtin:authenticate,privileged</string>
<string>PKINITMechanism:auth,privileged</string>
<string>builtin:login-success</string>
<string>loginwindow:success</string>
<string>loginwindow:FDESupport,privileged</string>
<string>HomeDirMechanism:login,privileged</string>
<string>HomeDirMechanism:status</string>
<string>MCXMechanism:login</string>
<string>CryptoTokenKit:login</string>
<string>loginwindow:done</string>
```

```
<string>builtin:policy-banner</string>
<string>NoMADLogin:CheckAD</string>
<string>NoMADLogin:CreateUser</string>
<string>builtin:login-begin</string>
<string>builtin:reset-password,privileged</string>
<string>builtin:forward-login,privileged</string>
<string>builtin:auto-login,privileged</string>
<string>builtin:authenticate,privileged</string>
<string>PKINITMechanism:auth,privileged</string>
<string>builtin:login-success</string>
<string>loginwindow:success</string>
<string>loginwindow:FDESupport,privileged</string>
<string>HomeDirMechanism:login,privileged</string>
<string>HomeDirMechanism:status</string>
<string>MCXMechanism:login</string>
<string>CryptoTokenKit:login</string>
<string>loginwindow:done</string>
```

NoMAD Login UI

EULA

RunScript

Notify

User Create

System Auth

User Setup

AwaitConfiguration

Shut up and show us!!

Demo

```
security authorize
system.login.console
```

Bonus Demo

All the mechs

Check AD

UserInput

Notify

EULA

KeychainAdd

Check Okta

CreateUser

EnableFDE

DeMobilize

RunScript

HTTPS://GITLAB.COM/
ORCHARDANDGROVE-OSS/
NoMADLogin-AD

Thanks!