Remediating Security Events with Jamf Pro, Jamf Connect, & Jamf Protect

virtual JNUC 2021

Catherine McKay

Consulting Engineer, Security

Sean Rabbitt

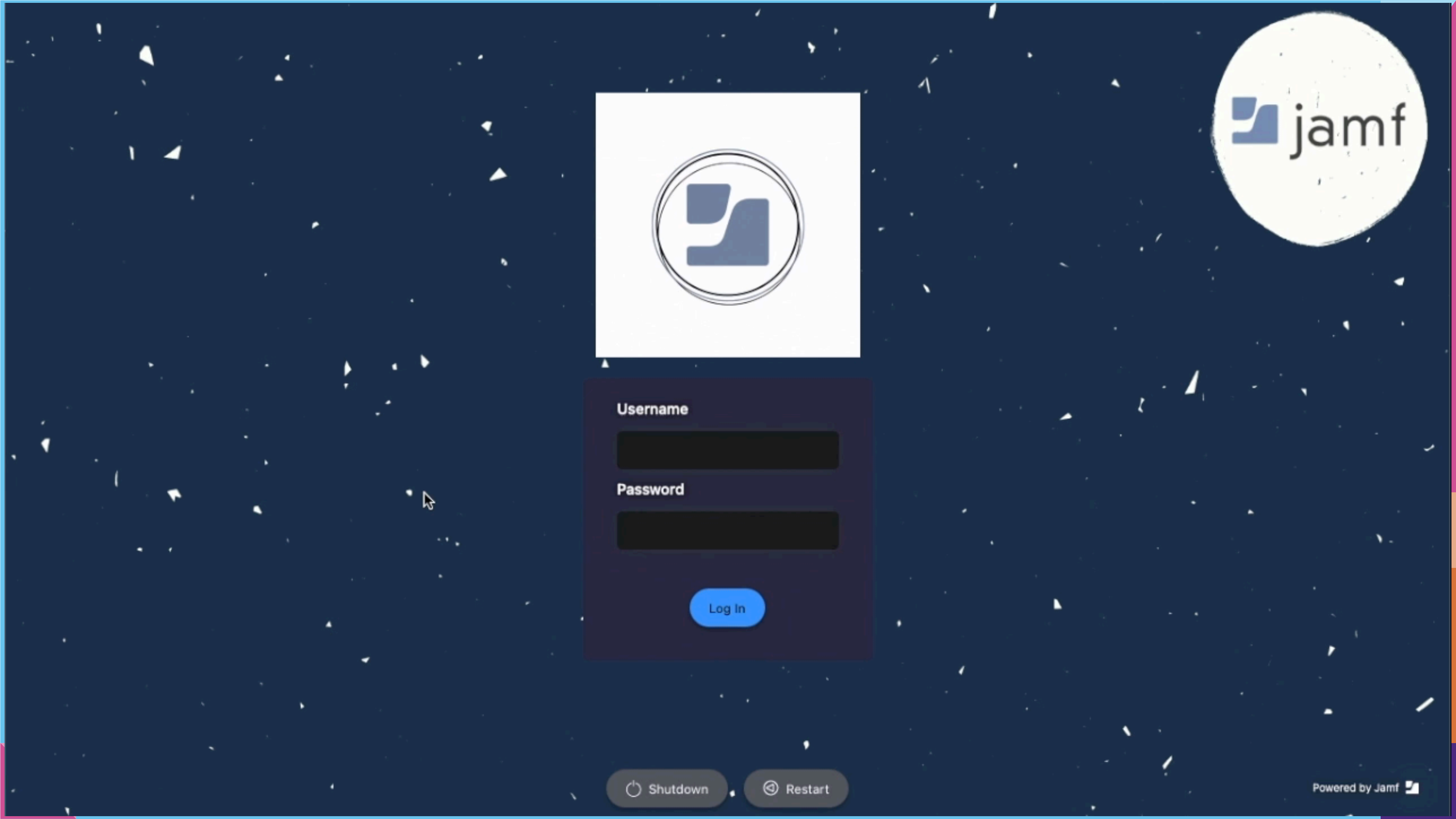
Sr. Consulting Engineer, Identity

Handouts for this Session will be available at

https://github.com/sean-rabbitt

Remediating Security Events with Jamf Pro, Jamf Connect, and Jamf Protect

- Overview of Pro, Connect, and Protect
- Flowchart of the Workflow
- Tools Needed
- Deployment Instructions


jamf
Username
Password
Log In
Shutdown
Restart
Powered by Jamf

Apple Enterprise Management Platform

Connect

- Zero-Touch Deployment
- Identity-Based Access
- Curated Resources On Demand

Manage

- App Lifecycle Management
- Device Management
- Inventory Management

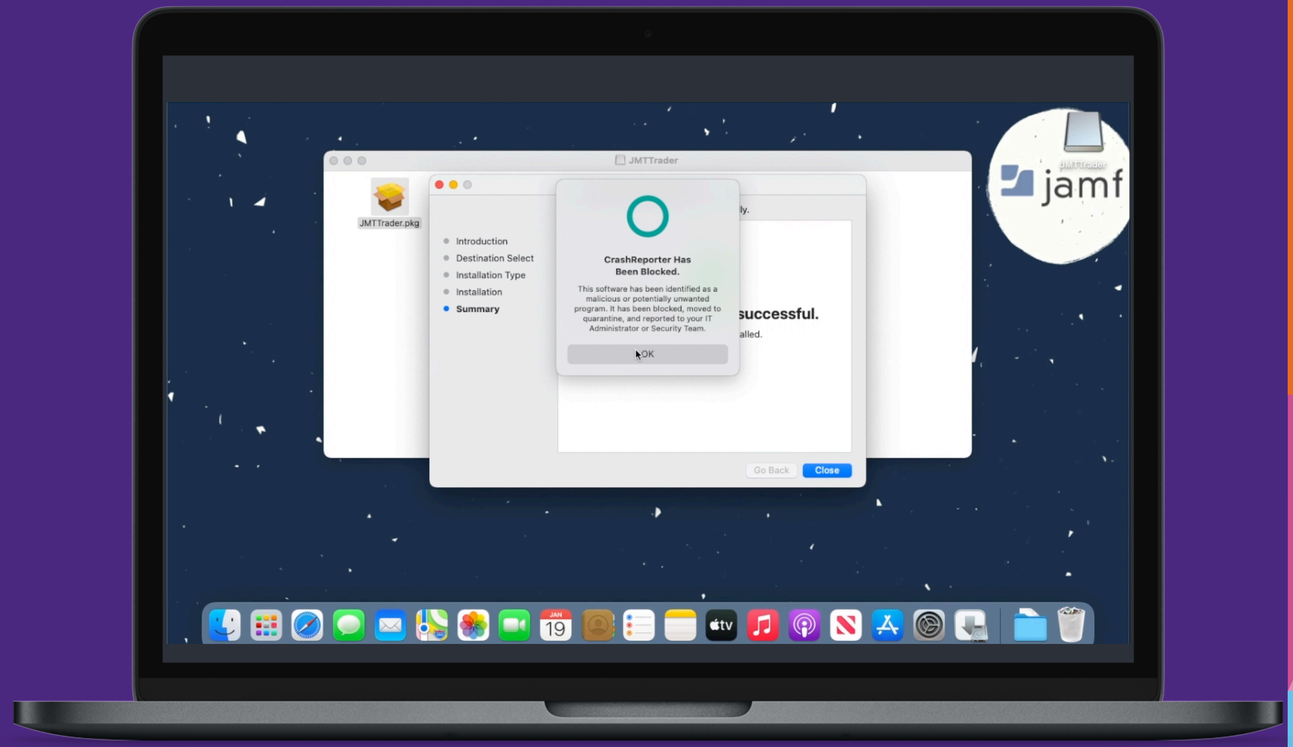
Protect

- Security Management
- Threat Prevention and Remediation
- APIs and Automation
- Industry Workflows

Visibility and Analytics

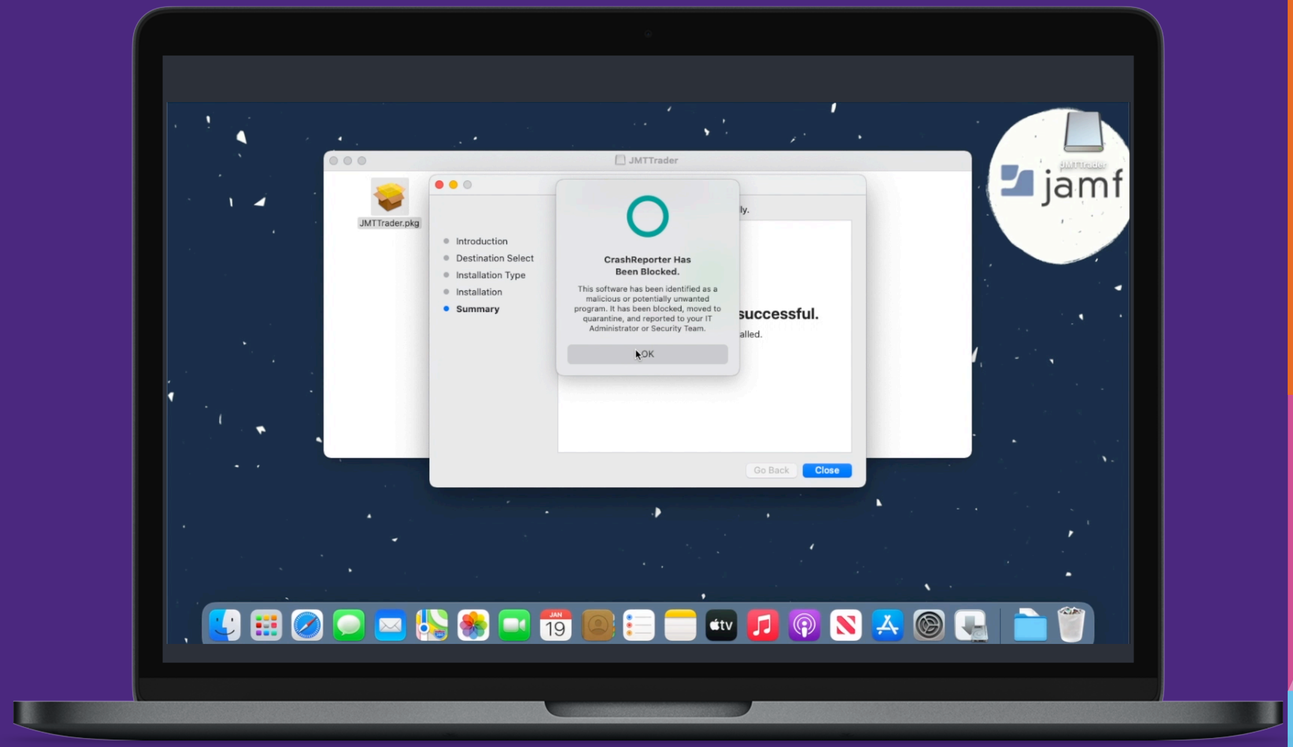
End-User Experience

Jamf’s Product Portfolio



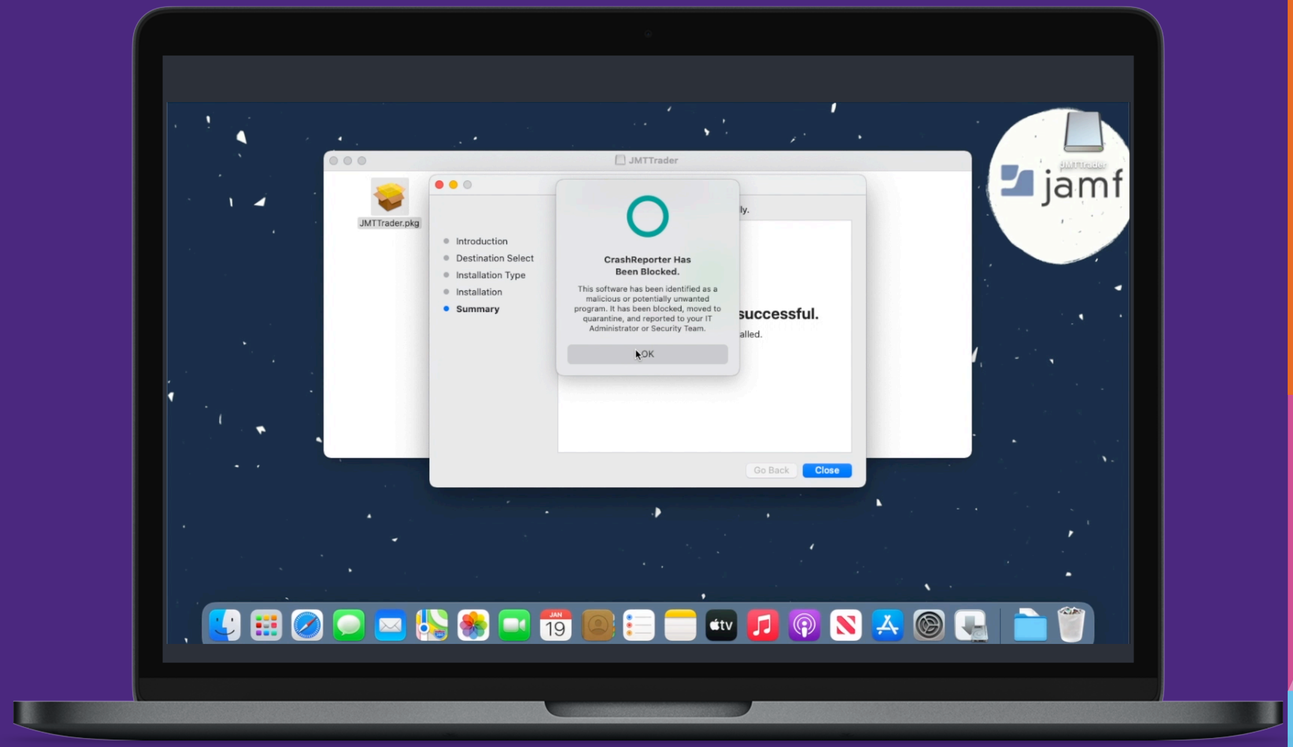
virtual JNUC 2021

jamf | PROTECT



virtual JNUC 2021

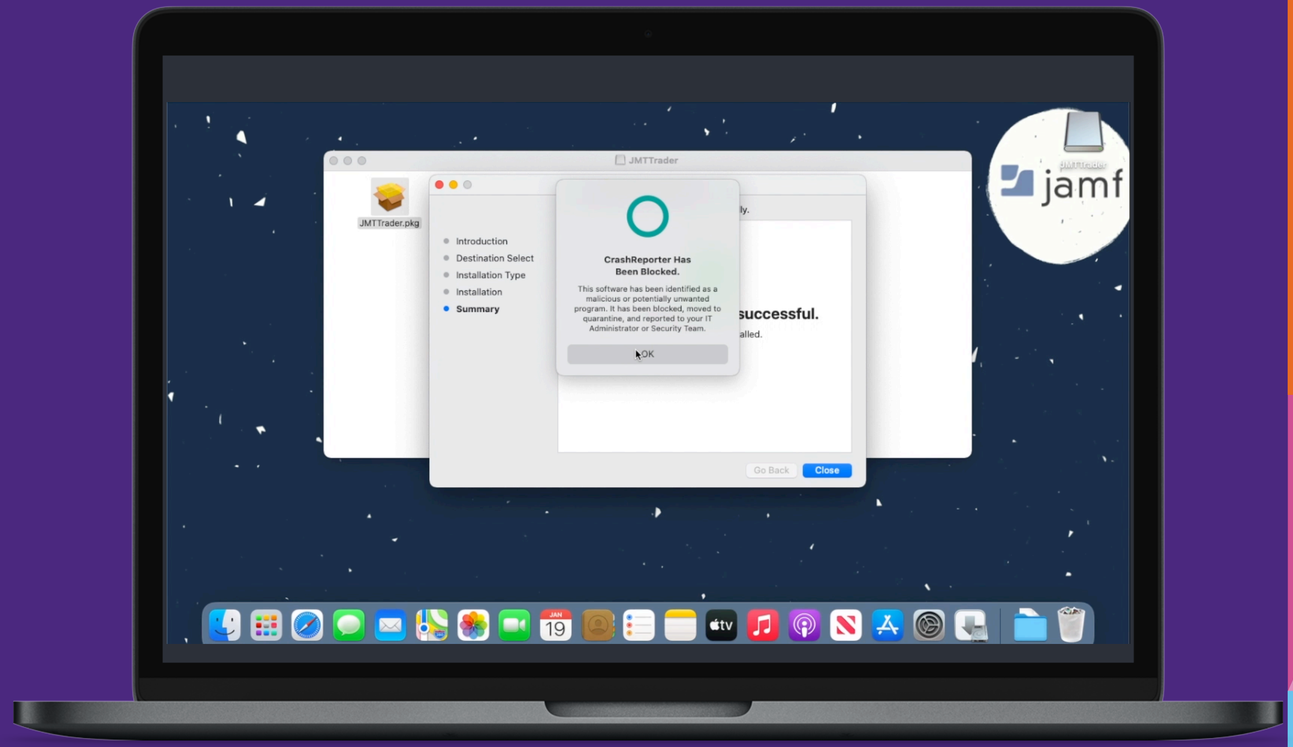
jamf | PROTECT



jamf | PRO

virtual JNUC 2021

jamf | PROTECT

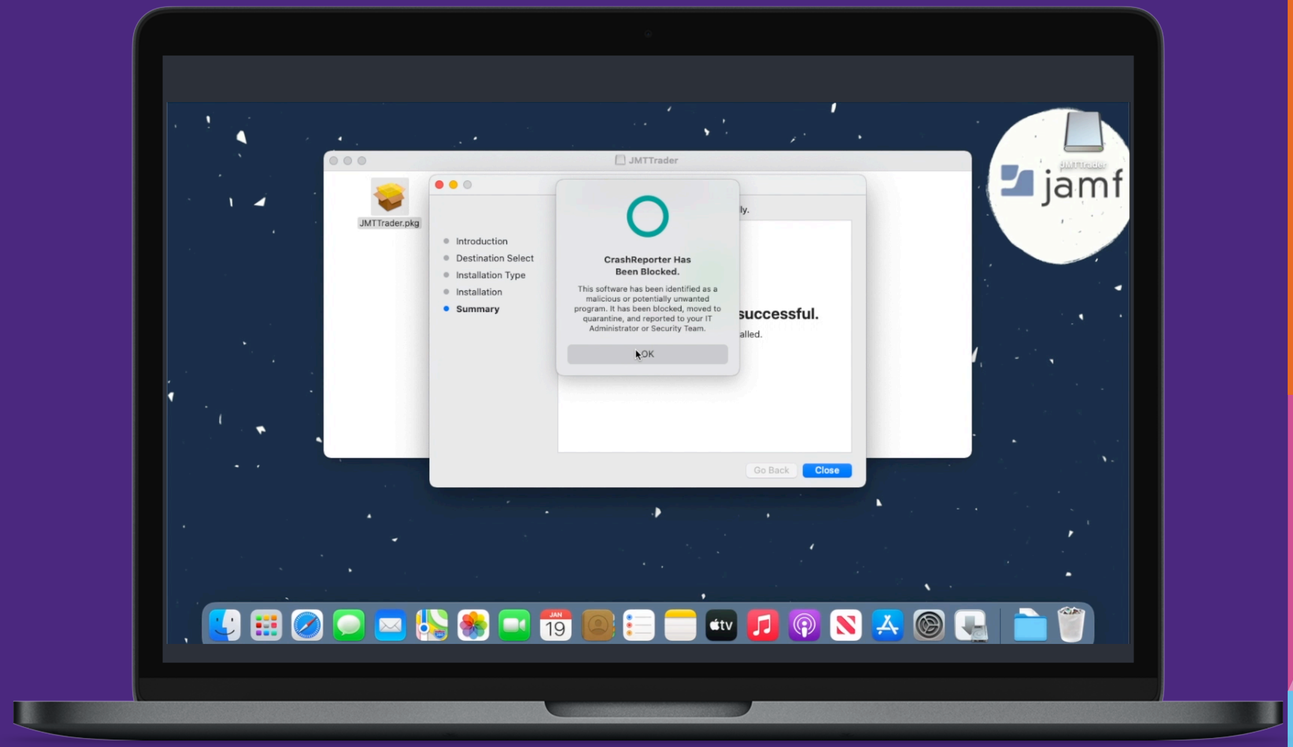


Inventory Information

jamf | PRO

virtual JNUC 2021

jamf | PROTECT



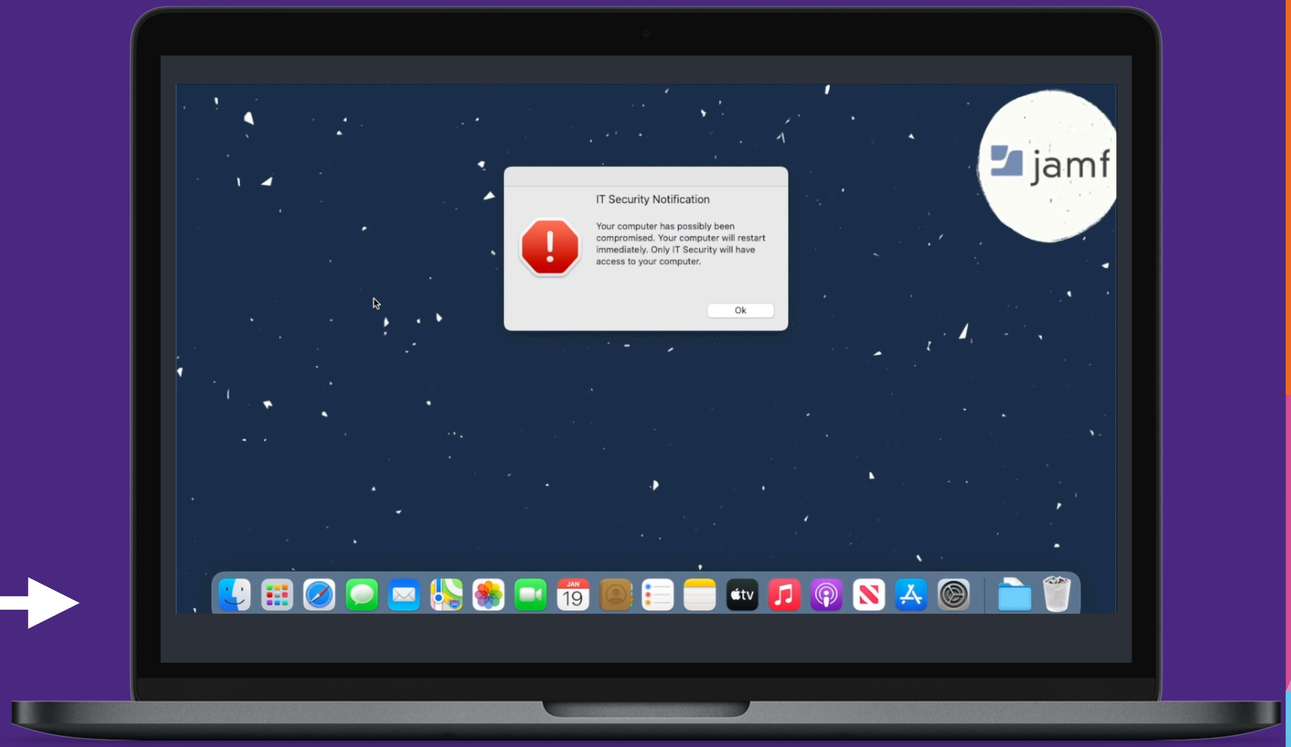
Smart Computer Group: Target device with new Config Profile

Inventory Information

jamf | PRO

virtual JNUC 2021

jamf | PROTECT



Smart Computer Group: Target device with new Config Profile

Execute Script

Update Config Profile

Inventory Information

jamf | PRO

virtual JNUC 2021

jamf | PROTECT

Smart Computer Group: Target device with new Config Profile

Execute Script

Update Config Profile

Inventory Information

jamf | PRO

virtual JNUC 2021

jamf | PROTECT

Smart Computer Group:
Target device with new
Config Profile

Execute Script

Update Config Profile

Inventory Information

jamf | PRO

virtual JNUC 2021

splunk>

Event Details

jamf | PROTECT

Smart Computer Group:
Target device with new
Config Profile

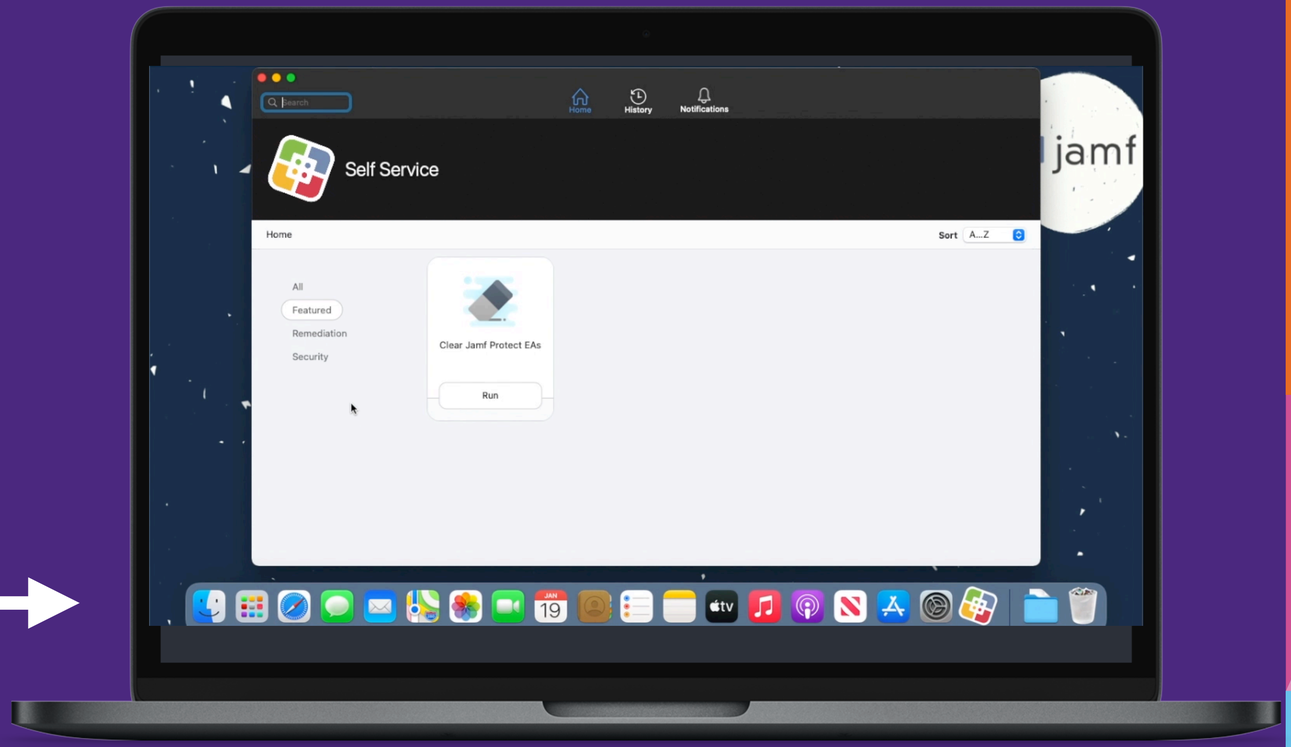
Execute Script

Update Config Profile

jamf | PRO

Inventory Information

virtual JNUC 2021



Execute Script

Self Service Command

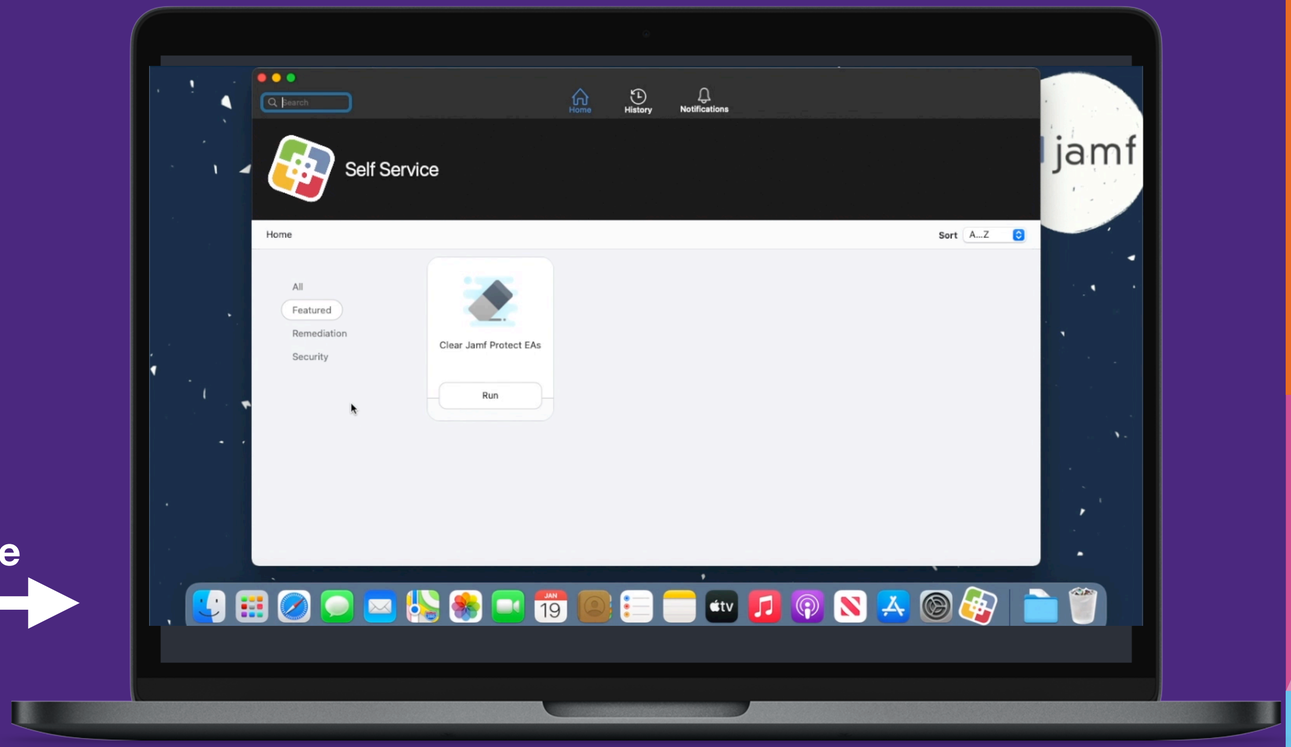
jamf | PRO

virtual JNUC 2021

Remove device from Smart Computer Group

Remove Configuration Profile

Add Configuration Profile

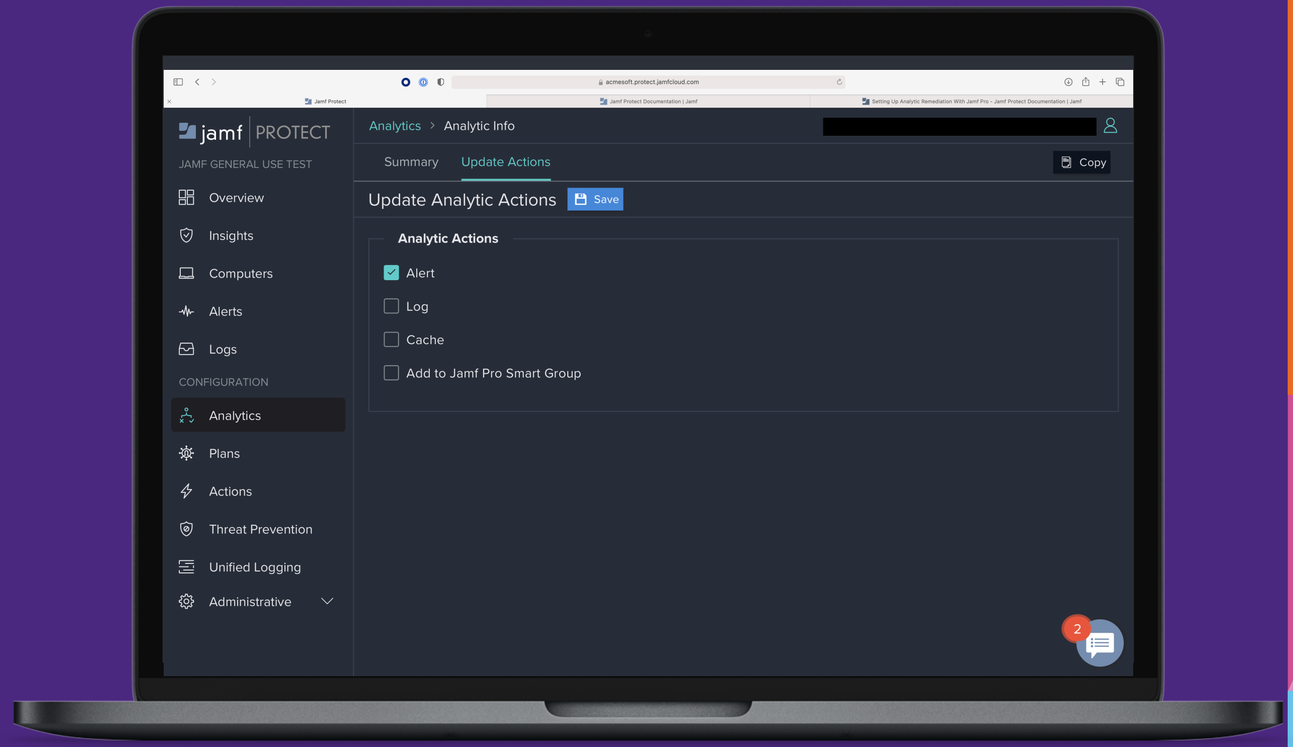


Updated Inventory

jamf | PRO

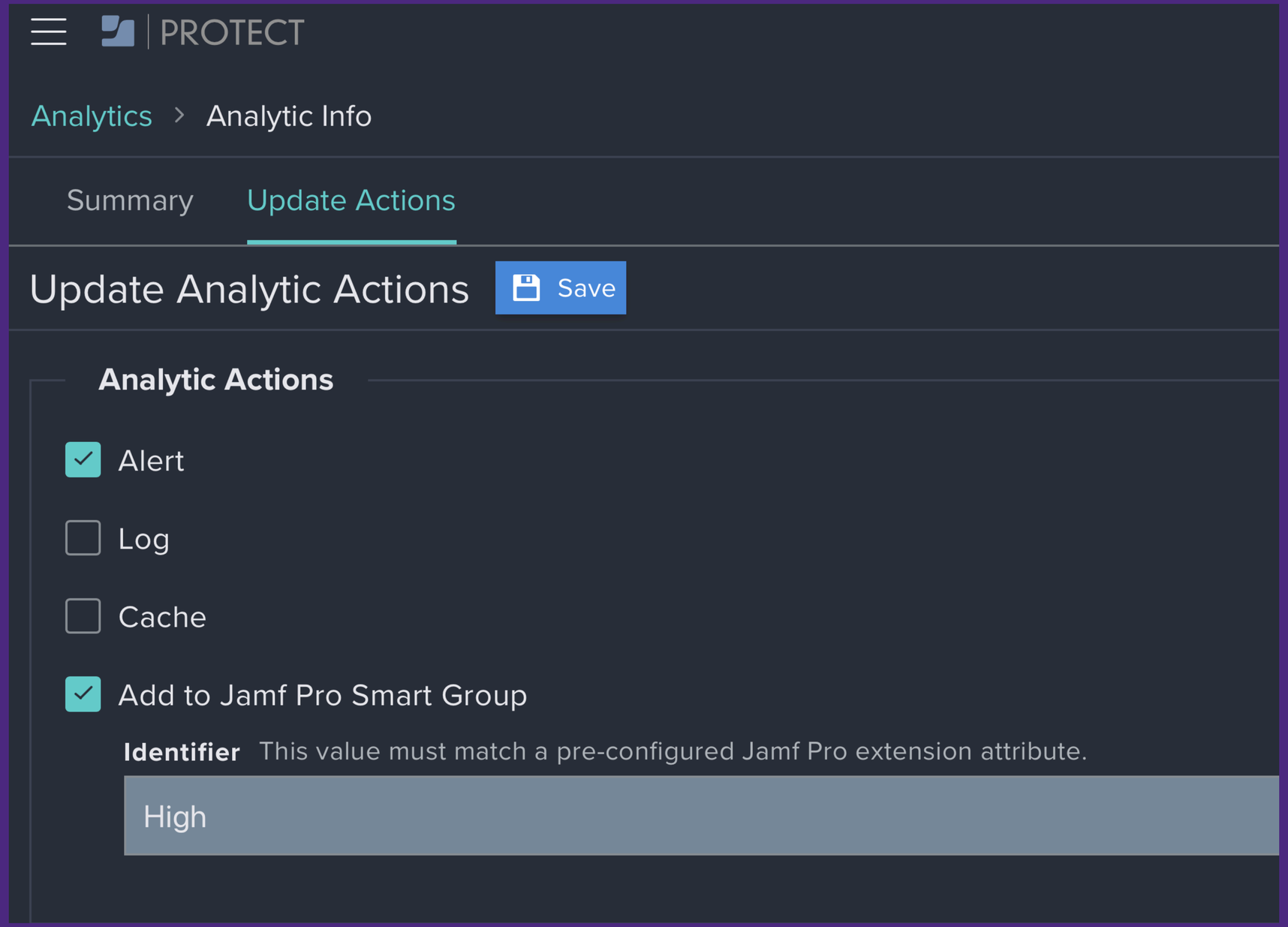
virtual JNUC 2021

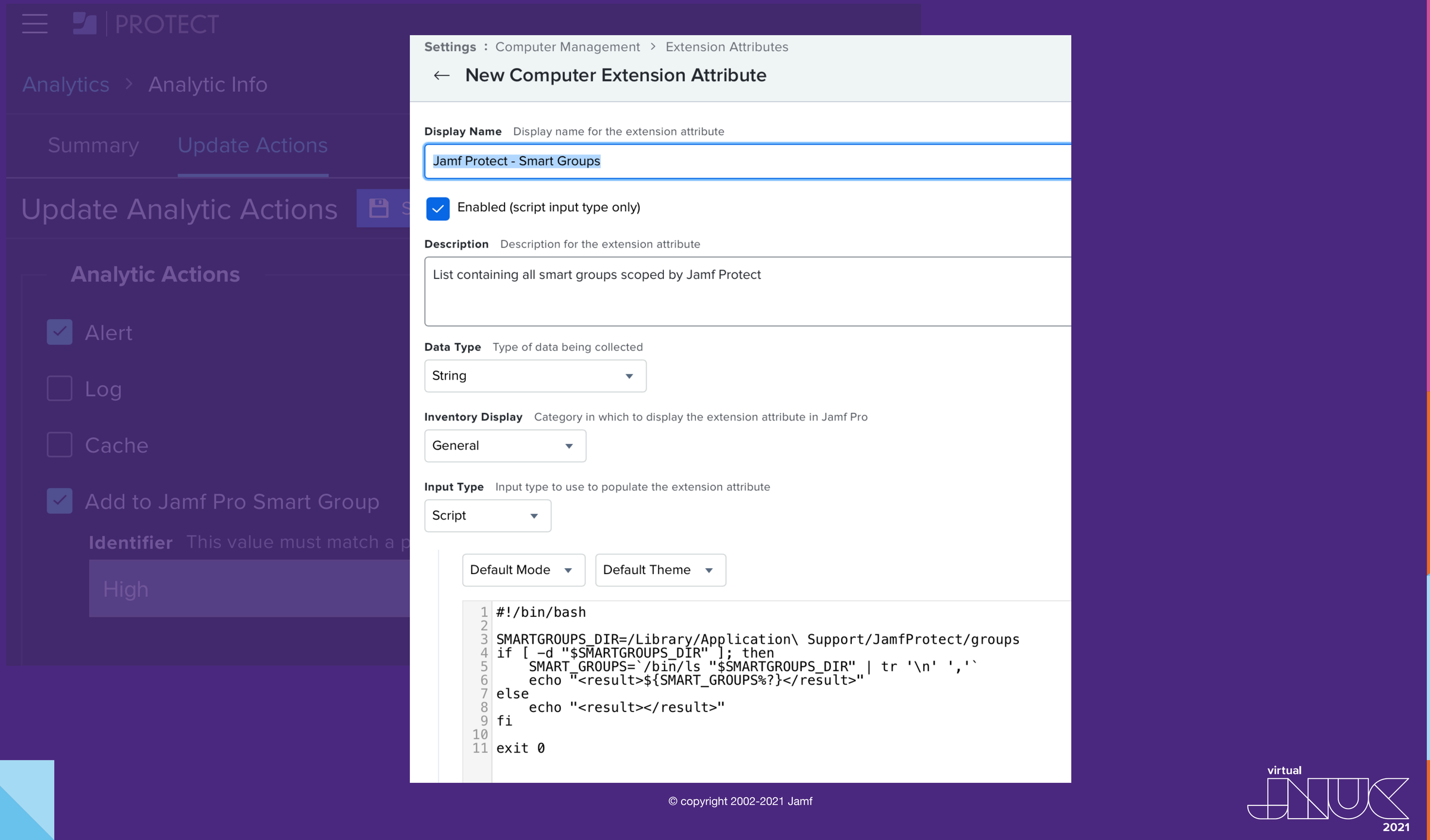
Analytic Remediation with Jamf Pro

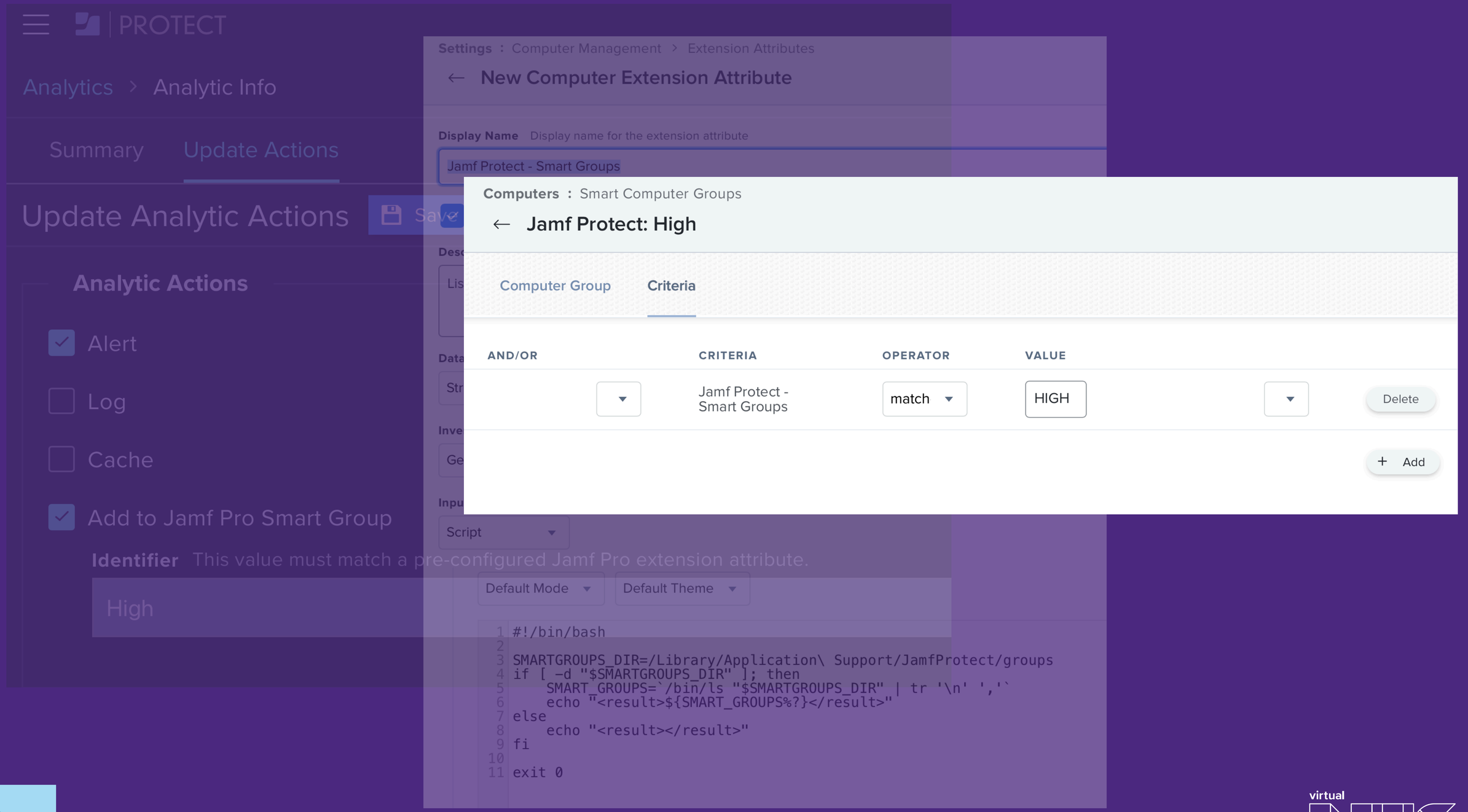


https://docs.jamf.com/jamf-protect/documentation/Setting_Up_Analytic_Remediation_With_Jamf_Pro.html

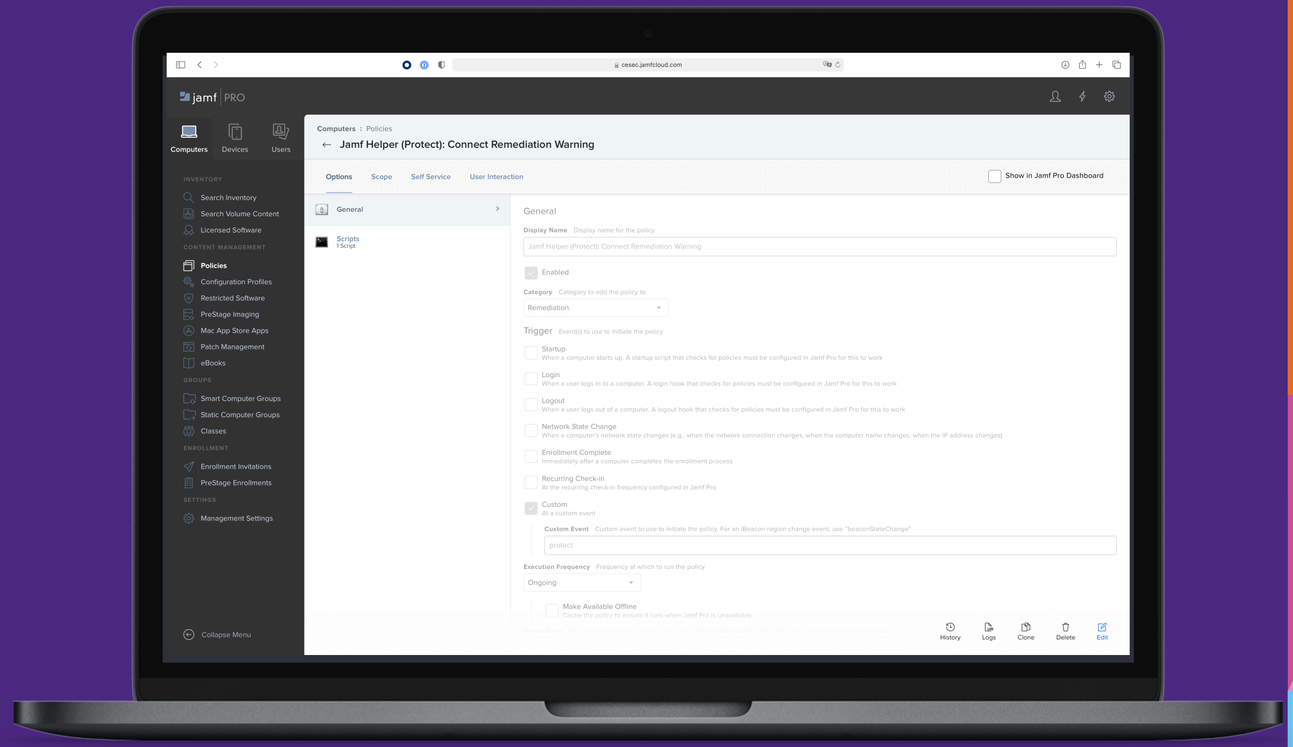
virtual JNUC 2021



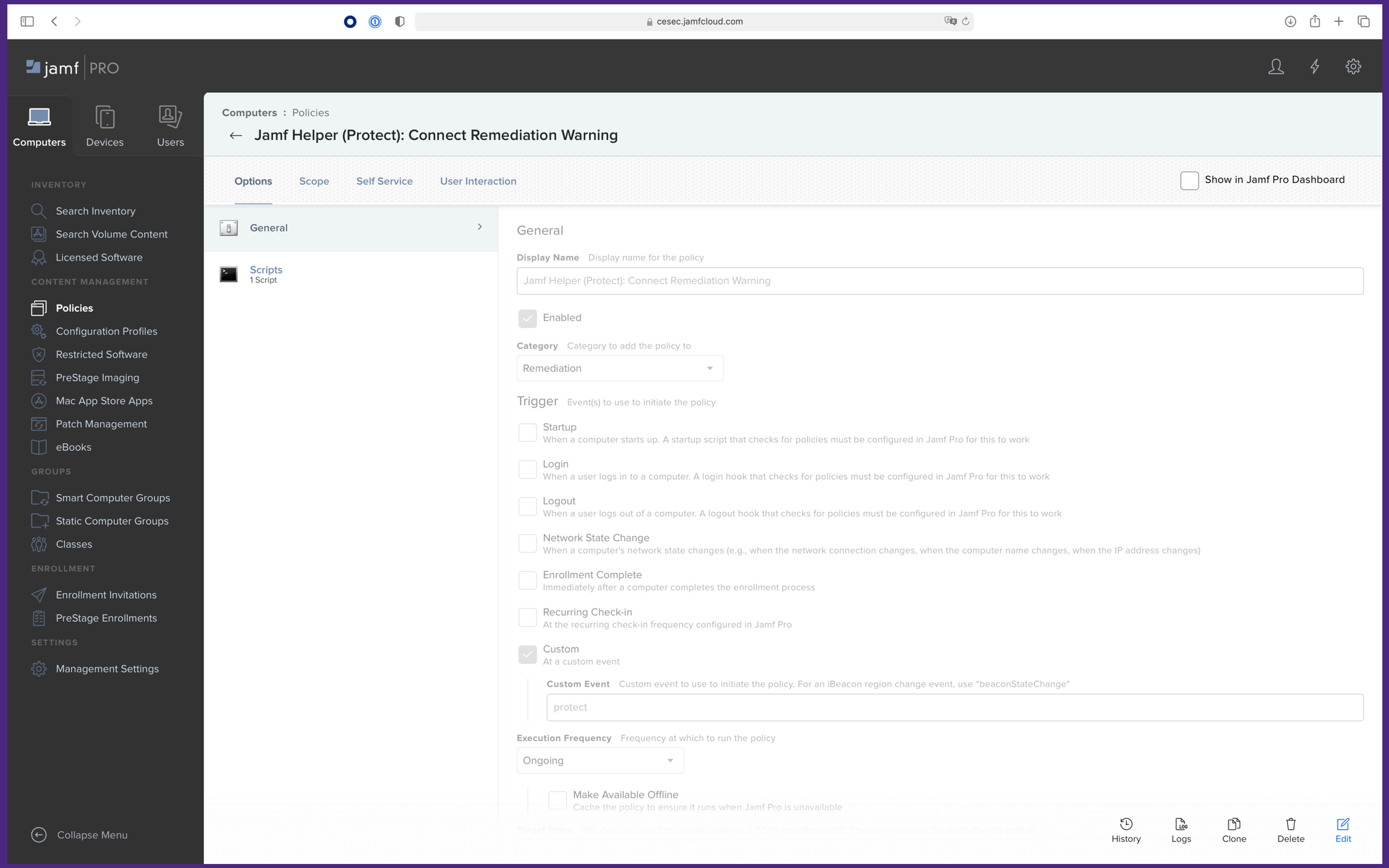




How to create a policy to run offline in Jamf Pro

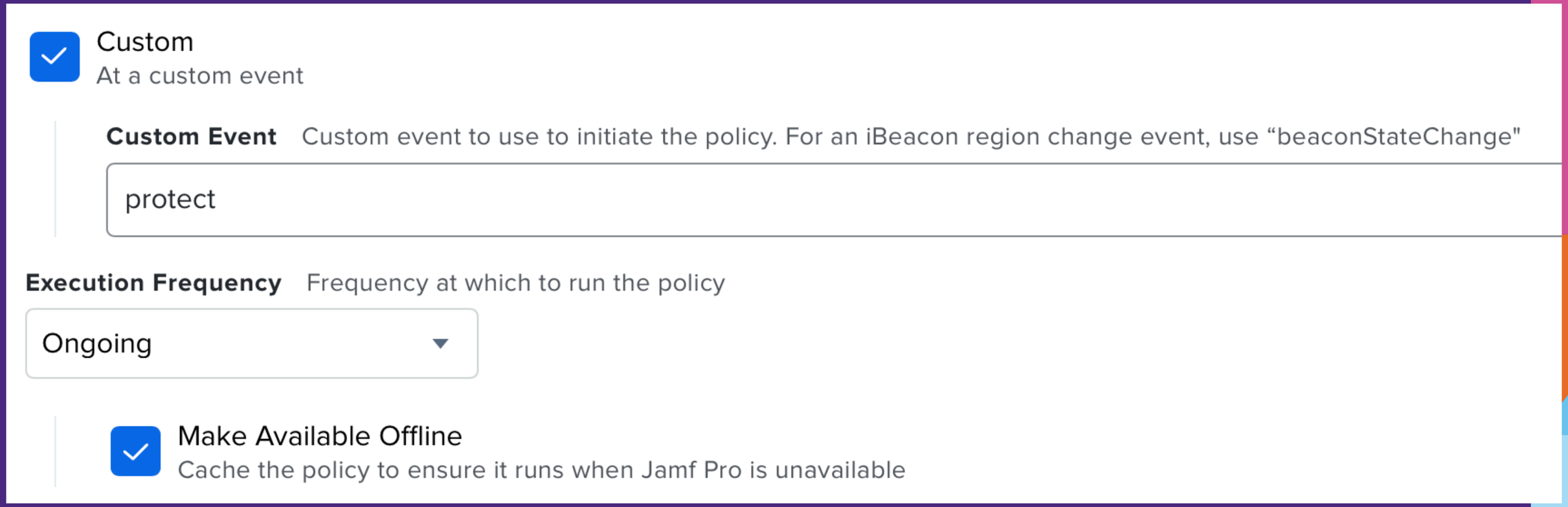


virtual JNUC 2021



virtual JNUC 2021

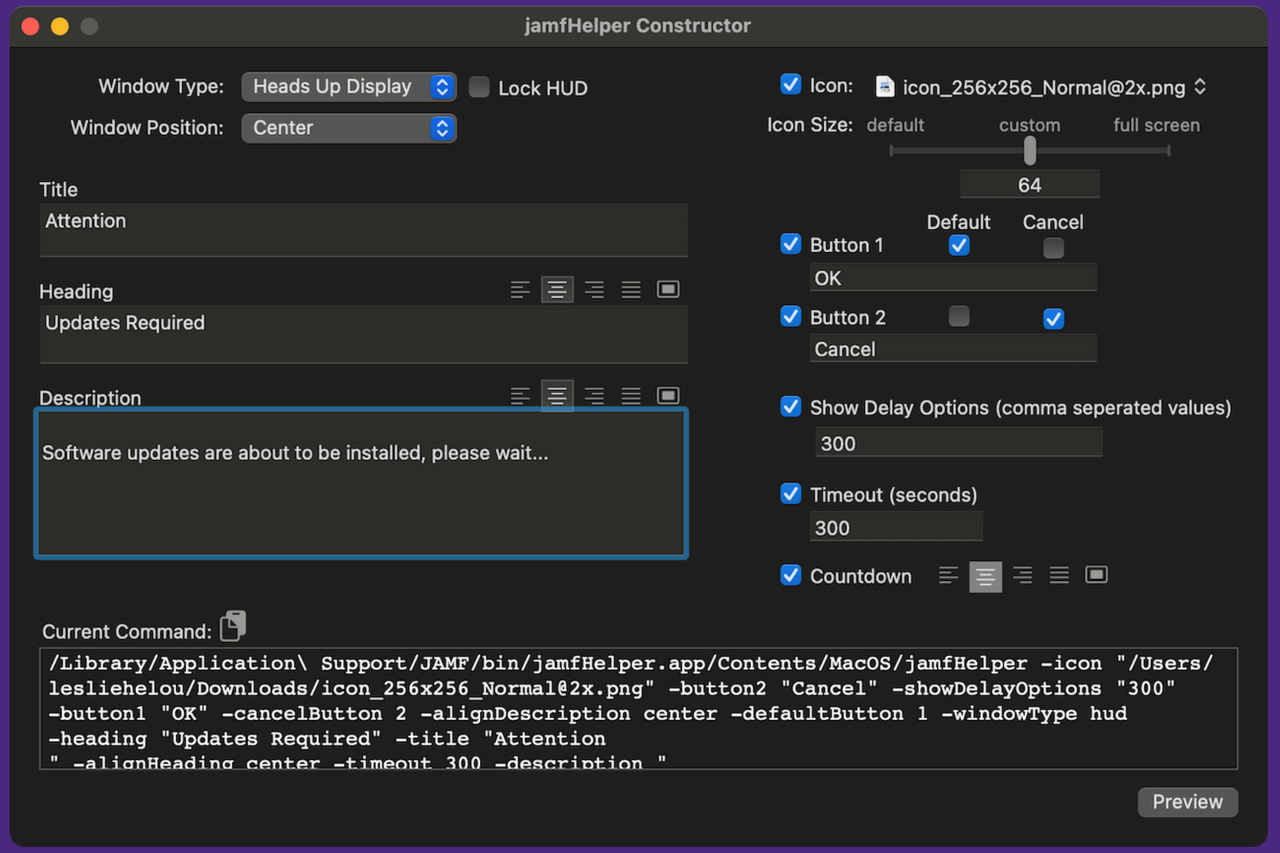
sudo jamf ~~magic~~ policy -event protect



Policy actions

```
jamfHelper="/Library/Application Support/JAMF/bin/jamfHelper.app/Contents/MacOS/jamfHelper"

#Header for Pop Up
heading="IT Security Notification"
#Description for Pop Up
description="Your computer has possibly been compromised. Your computer will restart immediately. Only IT Security will have access to your computer."
#Button Text
button1="Ok"
#Pixel Size for Pop Up
size=500
#Path for Icon Displayed
icon="/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/AlertStopIcon.icns"

userChoice=$("$jamfHelper" -windowType utility -heading "$heading" -description "$description" -button1 "$button1" -icon "$icon")

    if [[ $userChoice == 0 ]]; then
   echo "user clicked $button1"
   #Command to logout user
   shutdown -r now
fi
```

https://github.com/BIG-RAT/jhc

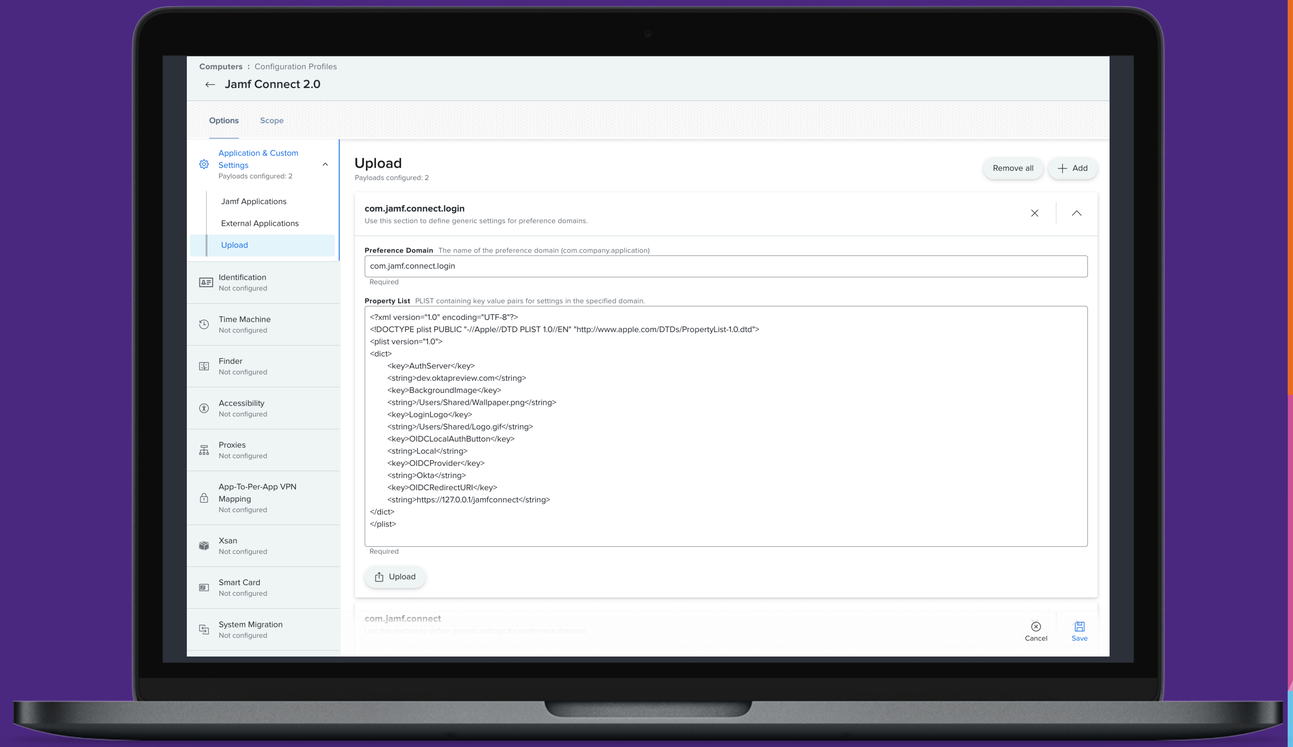


virtual JNUC 2021

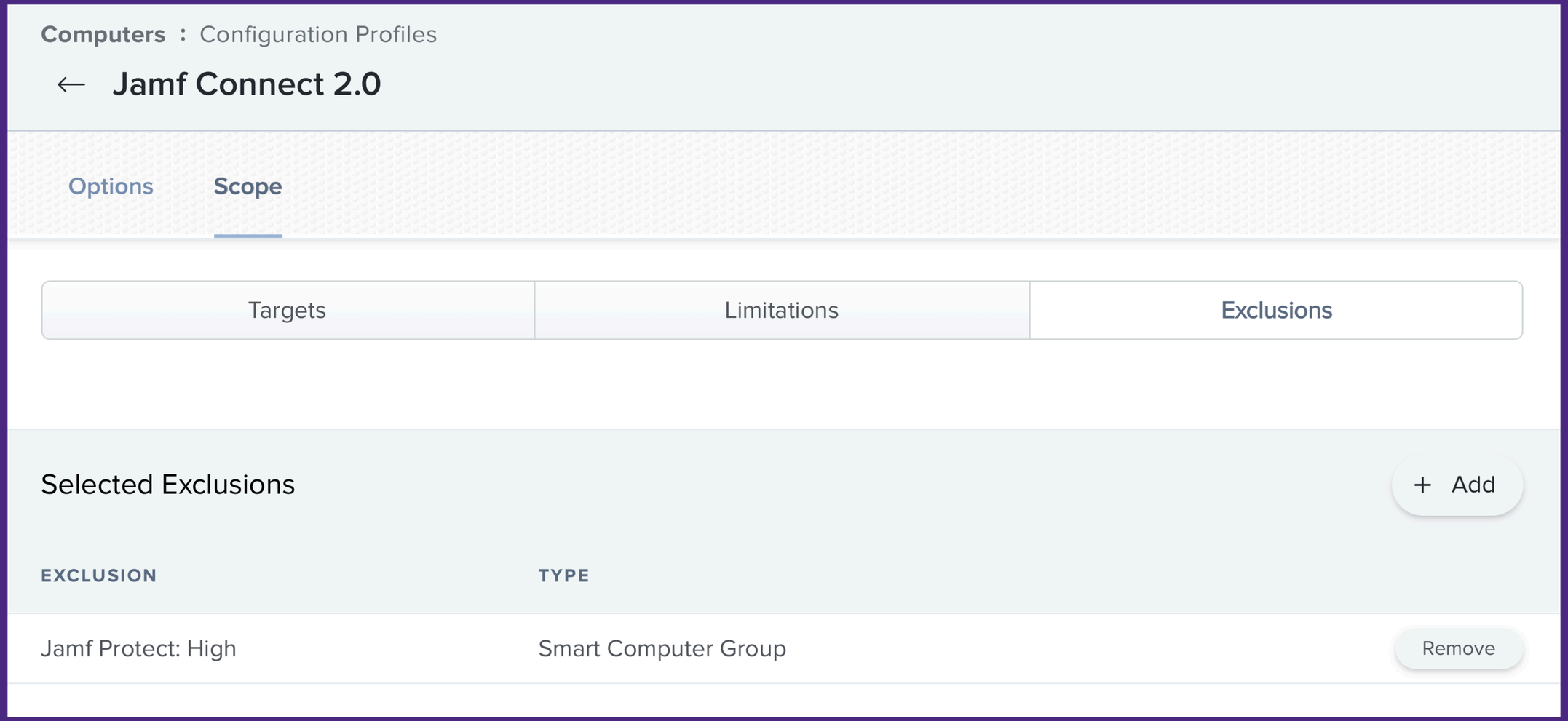
Policy actions - fancy mode

```
#!/bin/bash
# Version 1.0.0
#########################################################################################################
# Script by Sean Rabbitt, Jamf Senior Sales Engineer and Kelli Conlin, Jamf Security Solutions Specialist
#########################################################################################################
# DEP Notify for Jamf Protect

if [ -f "/Applications/Utilities/DEPNotify.app/Contents/MacOS/DEPNotify" ]; then
   /Applications/Utilities/DEPNotify.app/Contents/MacOS/DEPNotify -fullScreen &
else
echo "DEP Notify Not Present.. Exiting"
   exit 1;
fi

echo "Command: Image: /System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/AlertStopIcon.icns" >> /var/tmp/depnotify.log
echo "Command: MainTitle: Jamf Protect Remediation" >> /var/tmp/depnotify.log
echo "Command: MainText: Malicious activity on this computer has been detected by Jamf Protect.\nIf this screen appears for longer than 5 m
echo "Status: Isolating malicious software..." >> /var/tmp/depnotify.log
echo "Command: Determinate: 2" >> /var/tmp/depnotify.log

# Here's where you would put your Jamf policy command
jamf policy -event clearing
sleep 2

# Here's where you would put your Jamf policy command
#jamf policy -event collection
#sleep 2

echo "Status: The malicious software has been isolated." >> /var/tmp/depnotify.log
echo "Command: DeterminateManualStep" >> /var/tmp/depnotify.log
sleep 2 # Optional sleeps...

echo "Command: MainTitle: Remediation Complete" >> /var/tmp/depnotify.log
echo "Command: Image: /Library/Application Support/JamfProtect/JamfProtect.app/Contents/Resources/AppIcon.icns" >> /var/tmp/depnotify.log
echo "Command: MainText: The malicious software has been isolated. Reboot is recommended.\n \nSave your work and reboot your computer.\n\nF
echo "Command: DeterminateManualStep" >> /var/tmp/depnotify.log
echo "Status: " >> /var/tmp/depnotify.log
echo "Command: ContinueButton: Continue" >> /var/tmp/depnotify.log

# Alternative Command to force a restart:
#echo "Command: ContinueButtonRestart: Restart" >> /var/tmp/depnotify.log
```

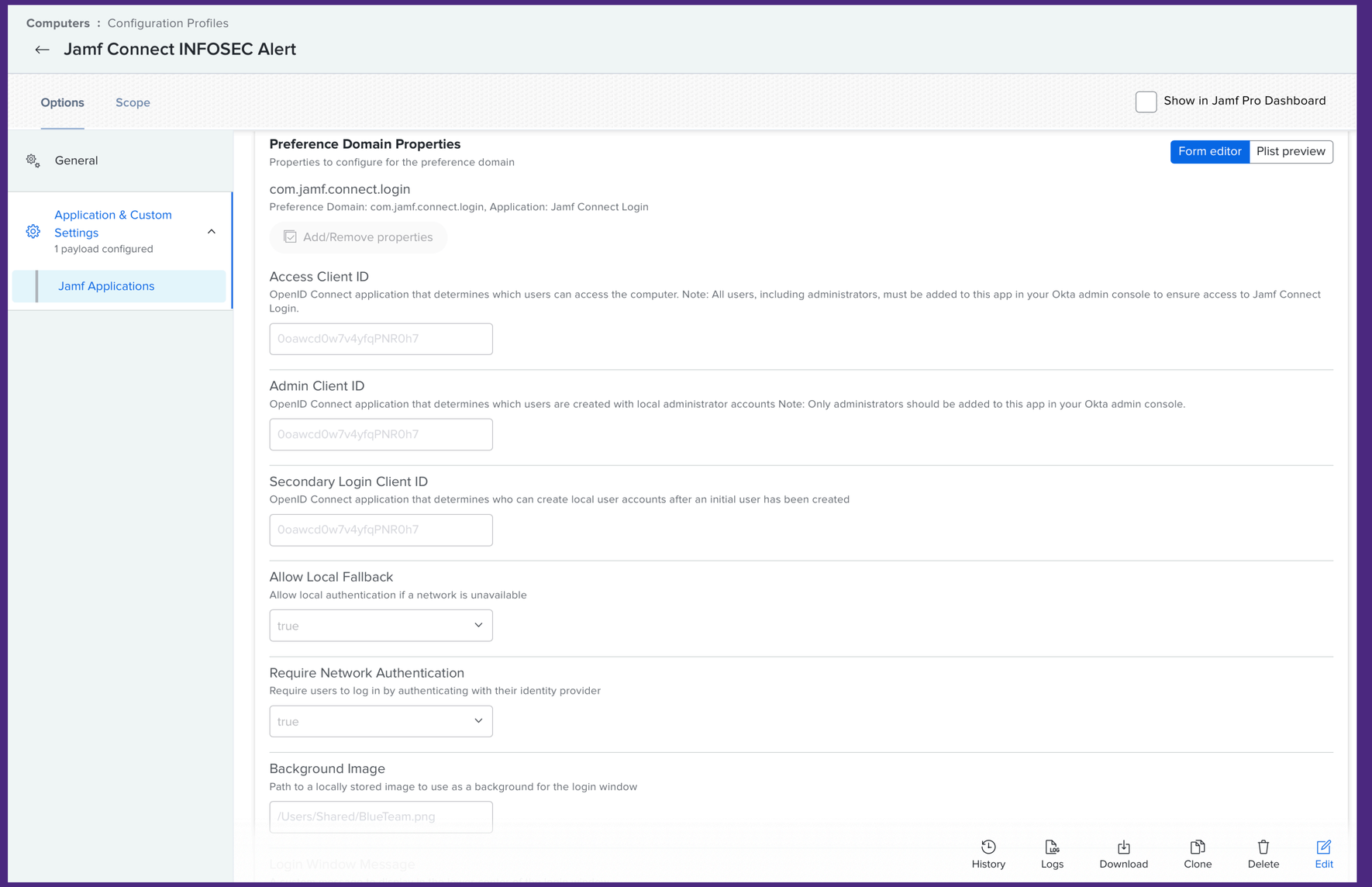
So.... remember those Smart Computer Groups?



Access Control Lists in IdP

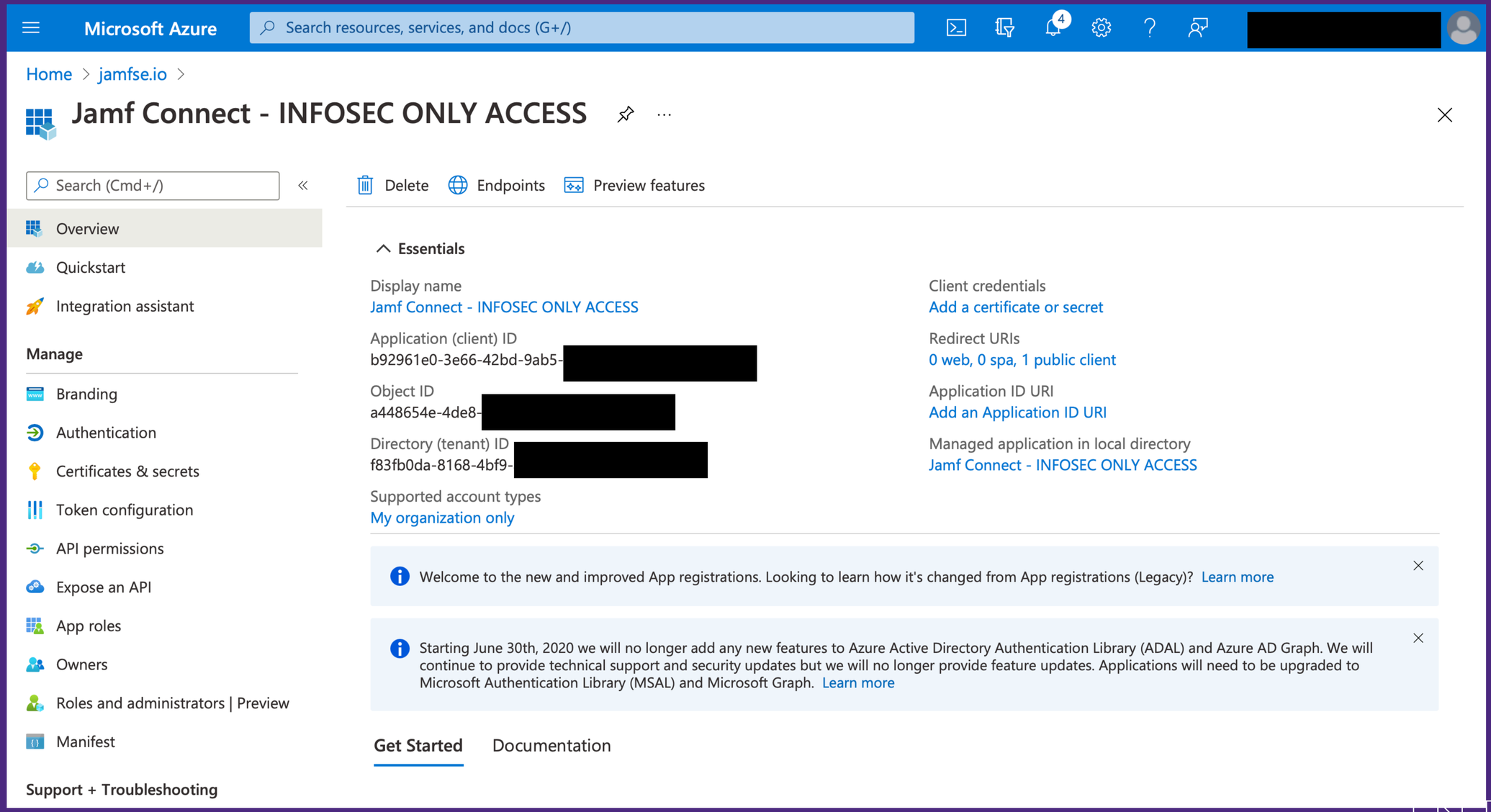


Access Control Lists in IdP

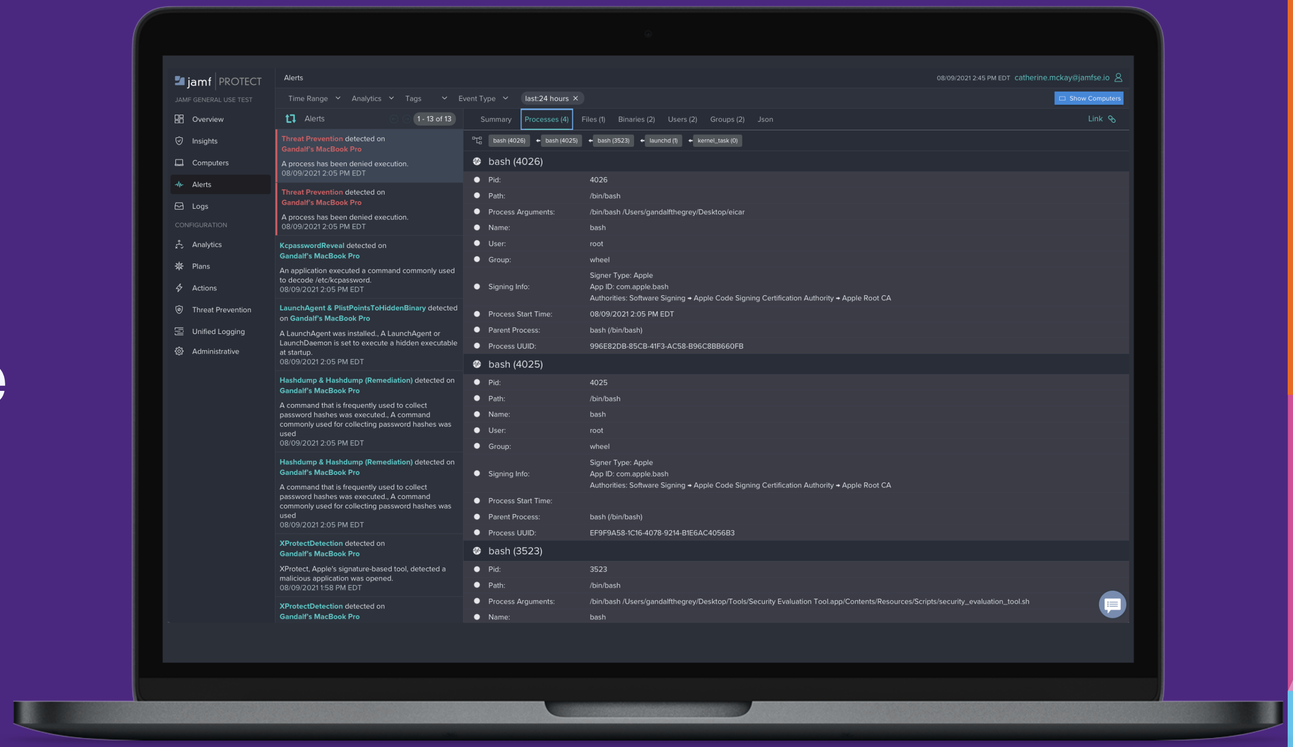


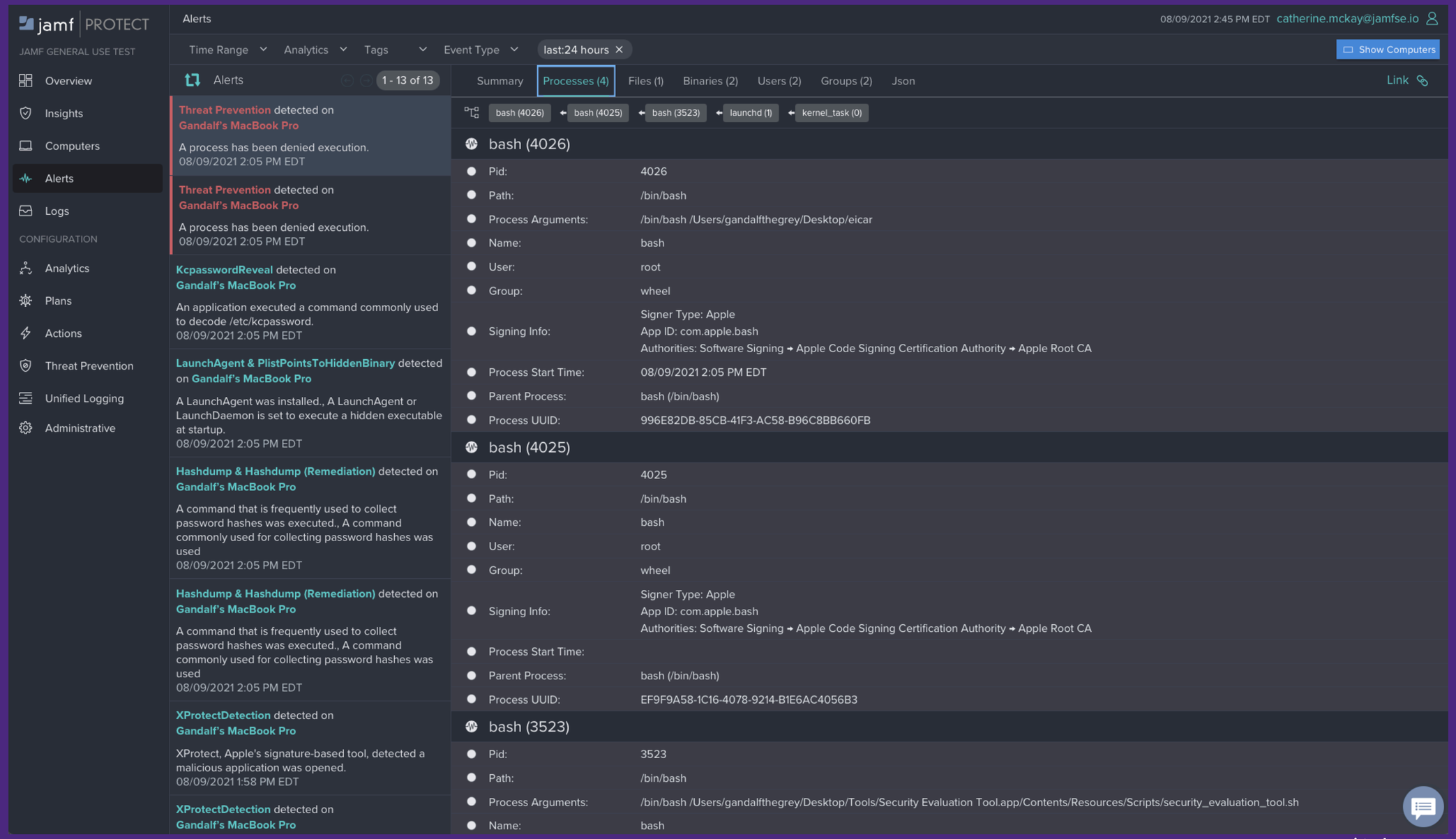
virtual JNUC 2021

Access Control Lists in IdP

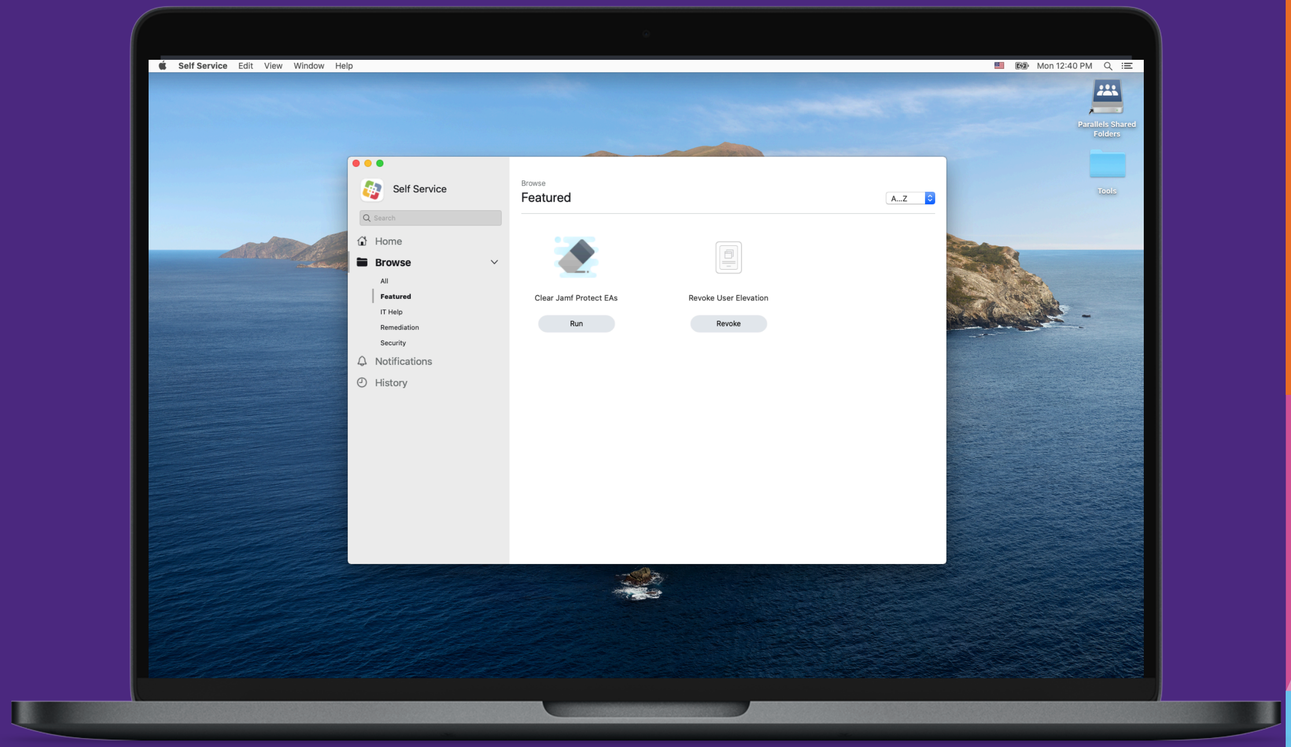


Sample screen of info about a security incident in the Jamf Protect console

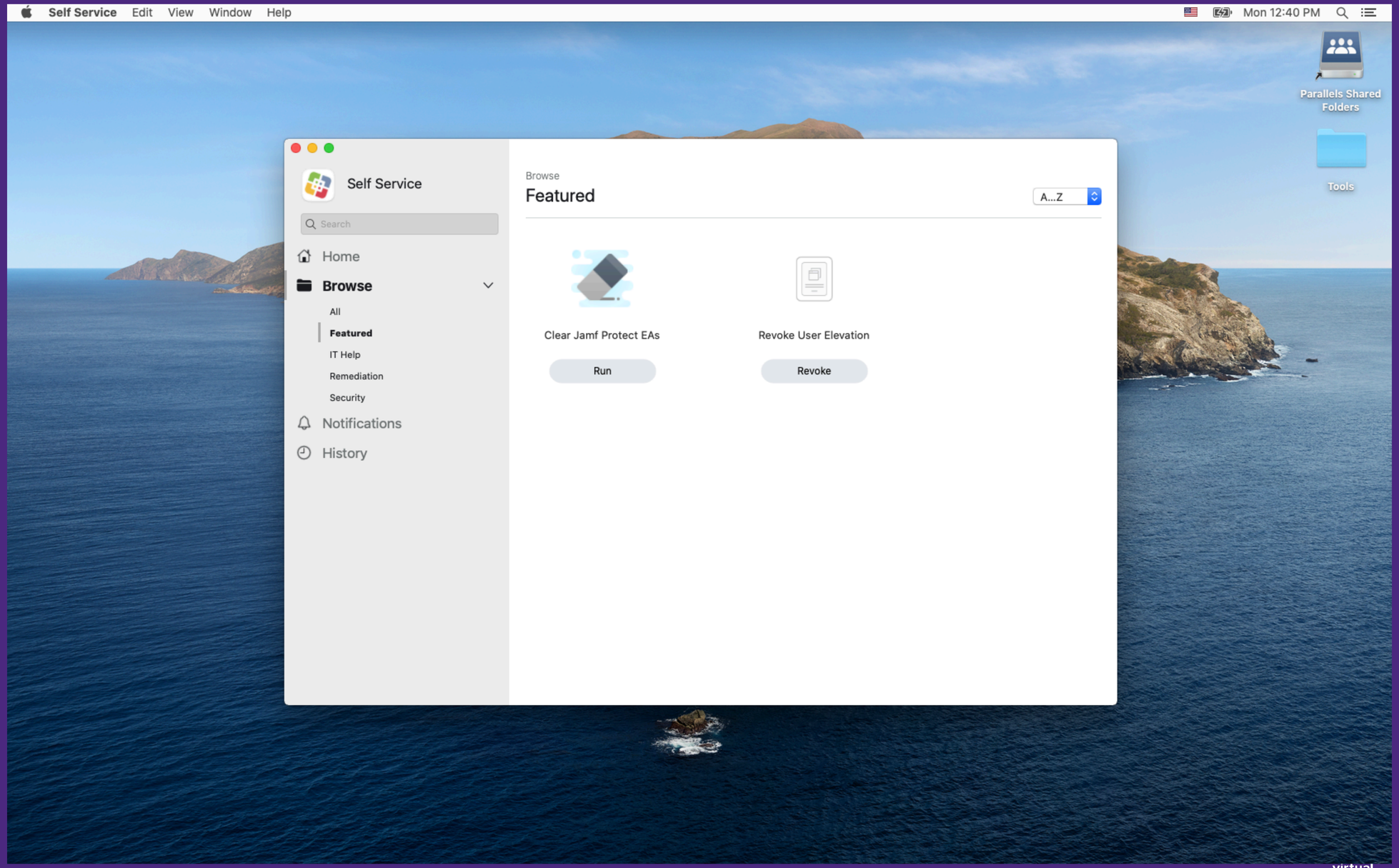




How to clear the EA with Self Service



virtual JNUC 2021




```
rm /Library/Application\ Support/JamfProtect/groups/*
```

Next Steps for Admins

- Determine analytic criticality
- Customize Jamf Helper message
- Educate your users on what to do
- Test your setup with an EICAR file

Handouts for this Session will be available at

https://github.com/sean-rabbitt

Jamf Support

support@jamf.com

Jamf Professional Services Team

info@jamf.com

Thank you for listening!