

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



Catherine McKay

Consulting Engineer, Security



Sean Rabbitt

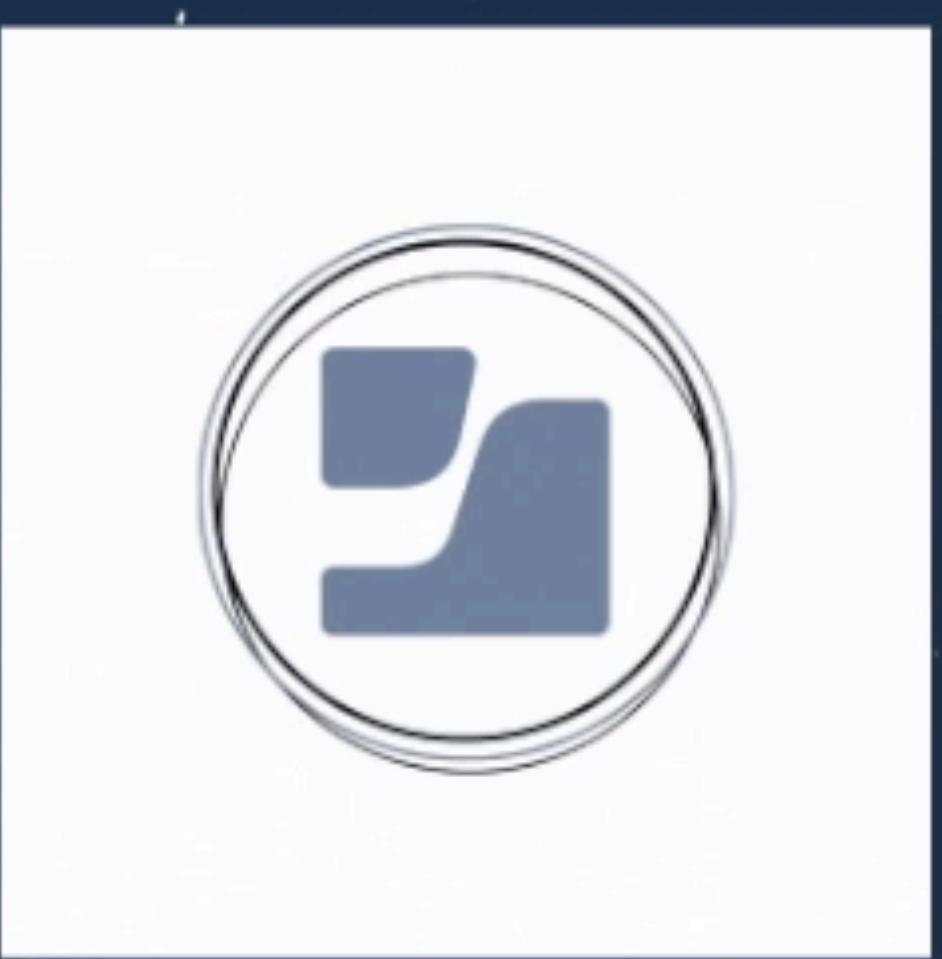
Sr. Consulting Engineer, Identity

**Handouts for this Session will be
available at**

<https://github.com/sean-rabbit>

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



Username

Password

Log In

Shutdown

Restart

Powered by Jamf

Apple Enterprise Management Platform

Connect



Zero-Touch
Deployment



Identity-
Based Access



Curated
Resources On
Demand



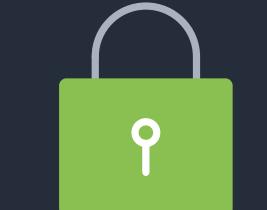
App Lifecycle
Management



Device
Management



Inventory
Management



Security
Management



Threat Prevention
and Remediation



APIs and
Automation



Industry Workflows

Manage

Protect



Visibility and Analytics



End-User Experience

Jamf's Product Portfolio



Streamlined Mac authentication and identity management.



Streamlined device management.
No IT required.



The Apple management standard.
Built for IT pros.



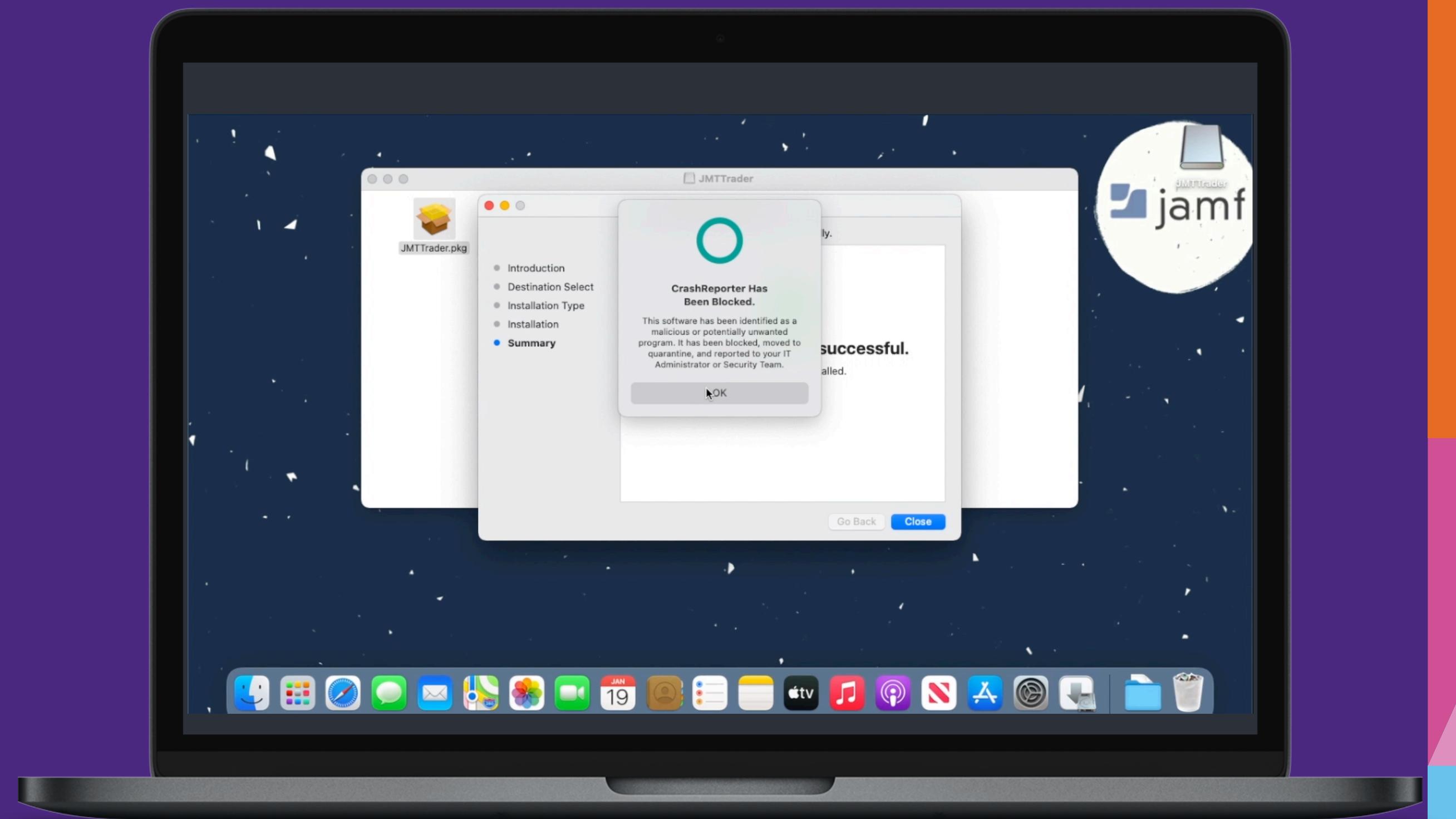
Empowering educators with
efficient Apple management.



Enterprise endpoint protection purpose-built for Mac.



100,000+ fellow Apple administrators.

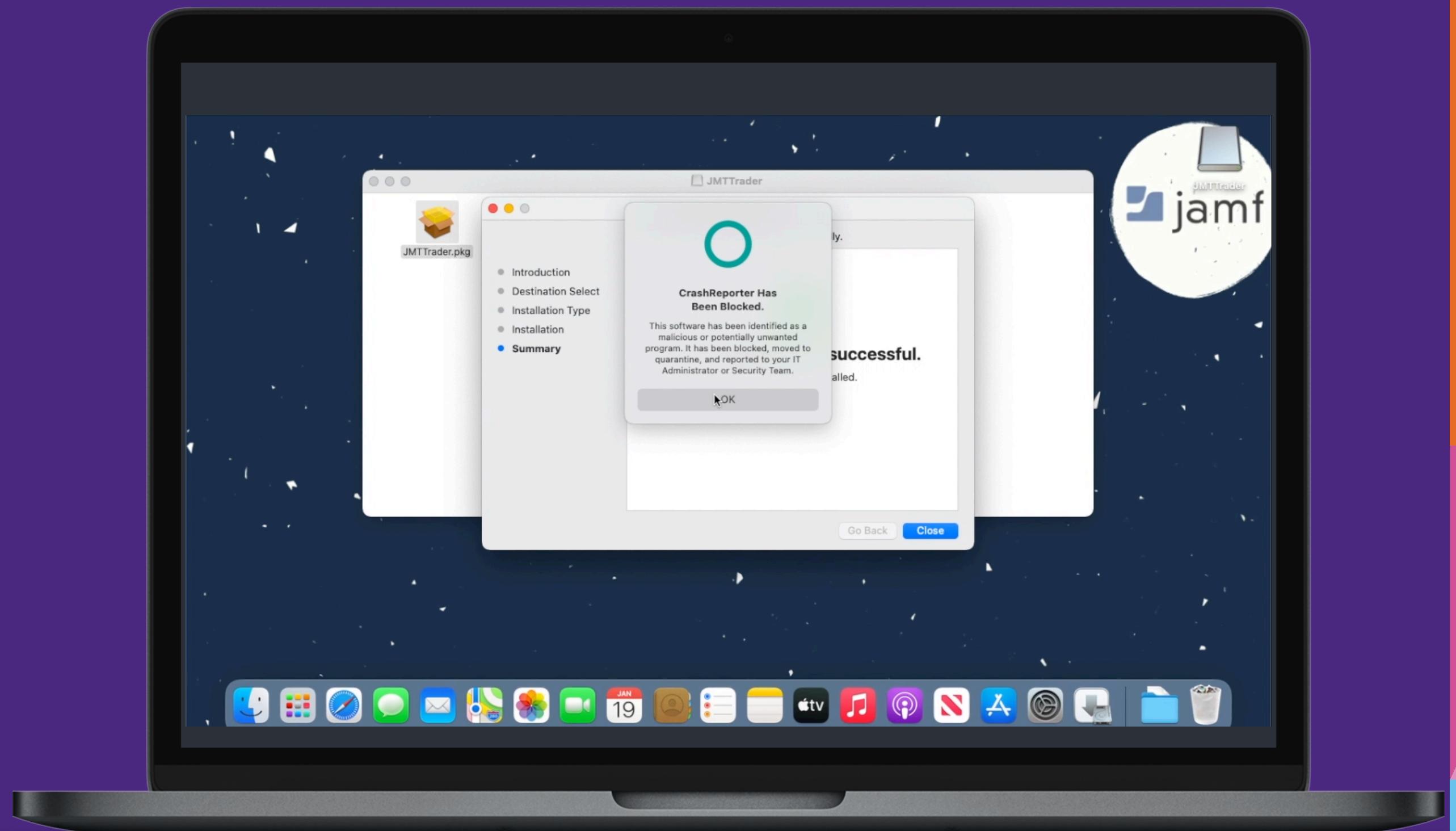


© copyright 2002-2021 Jamf

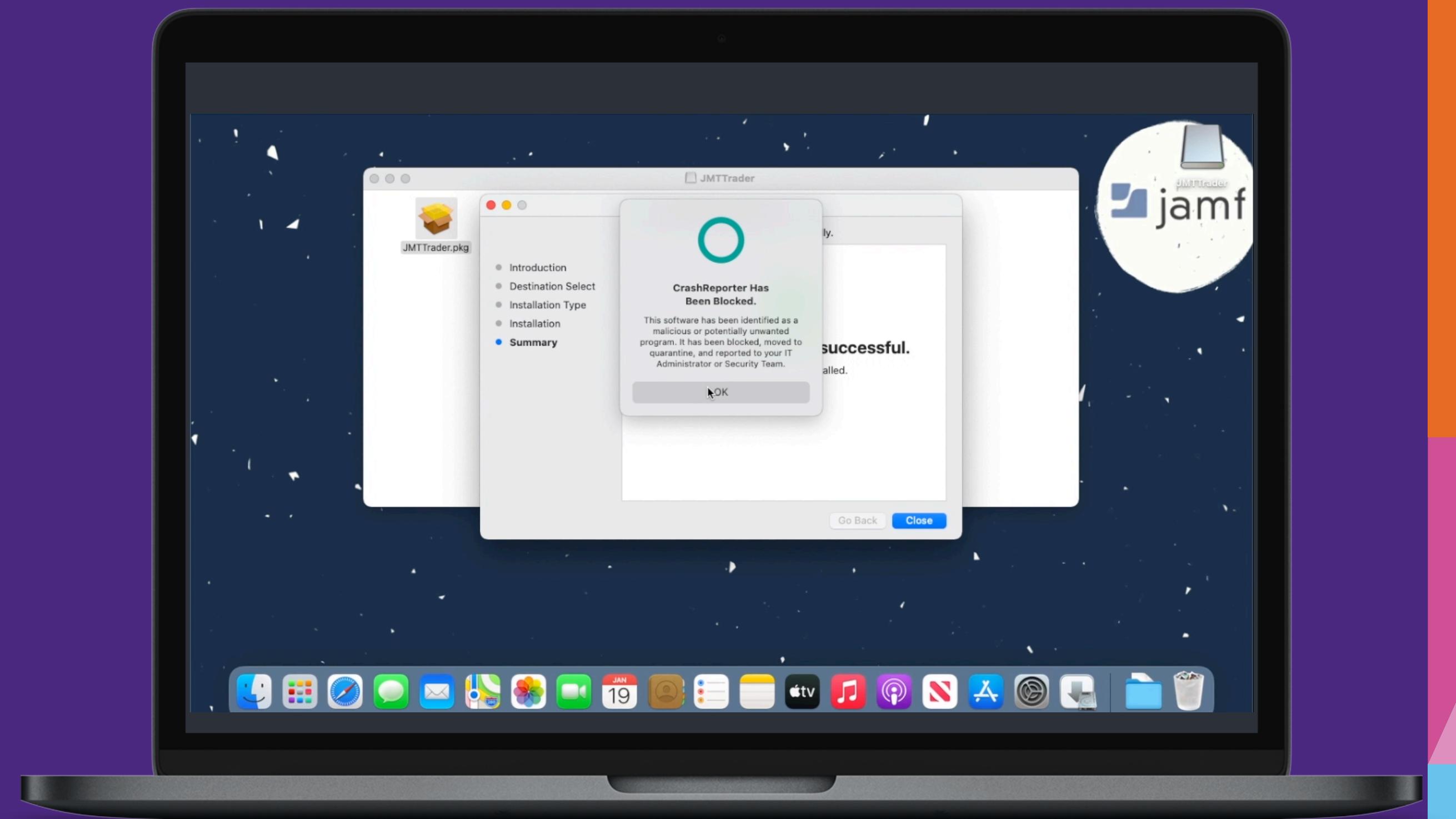
virtual
JNUK
2021



PROTECT



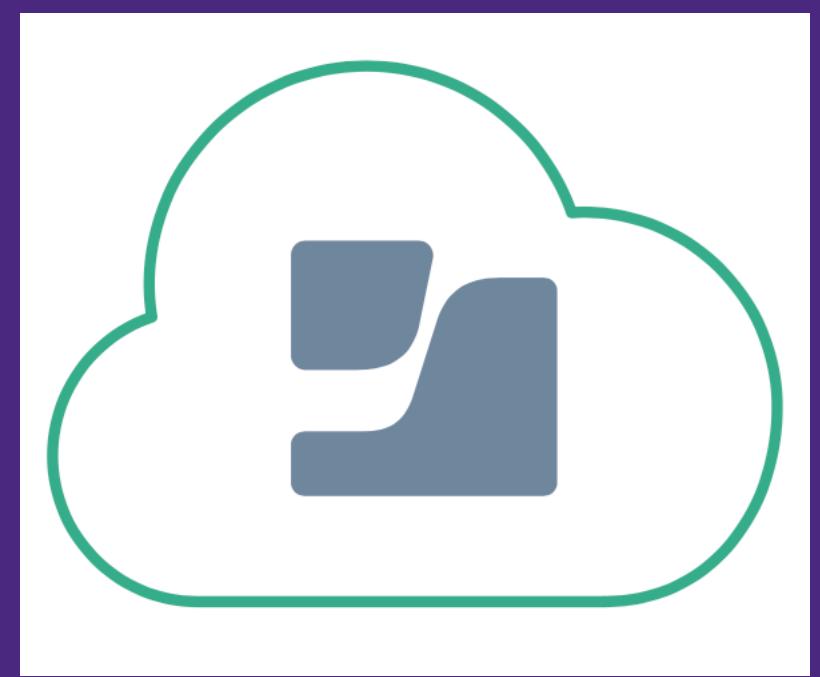
jamf | PROTECT



jamf | PRO



jamf | PROTECT



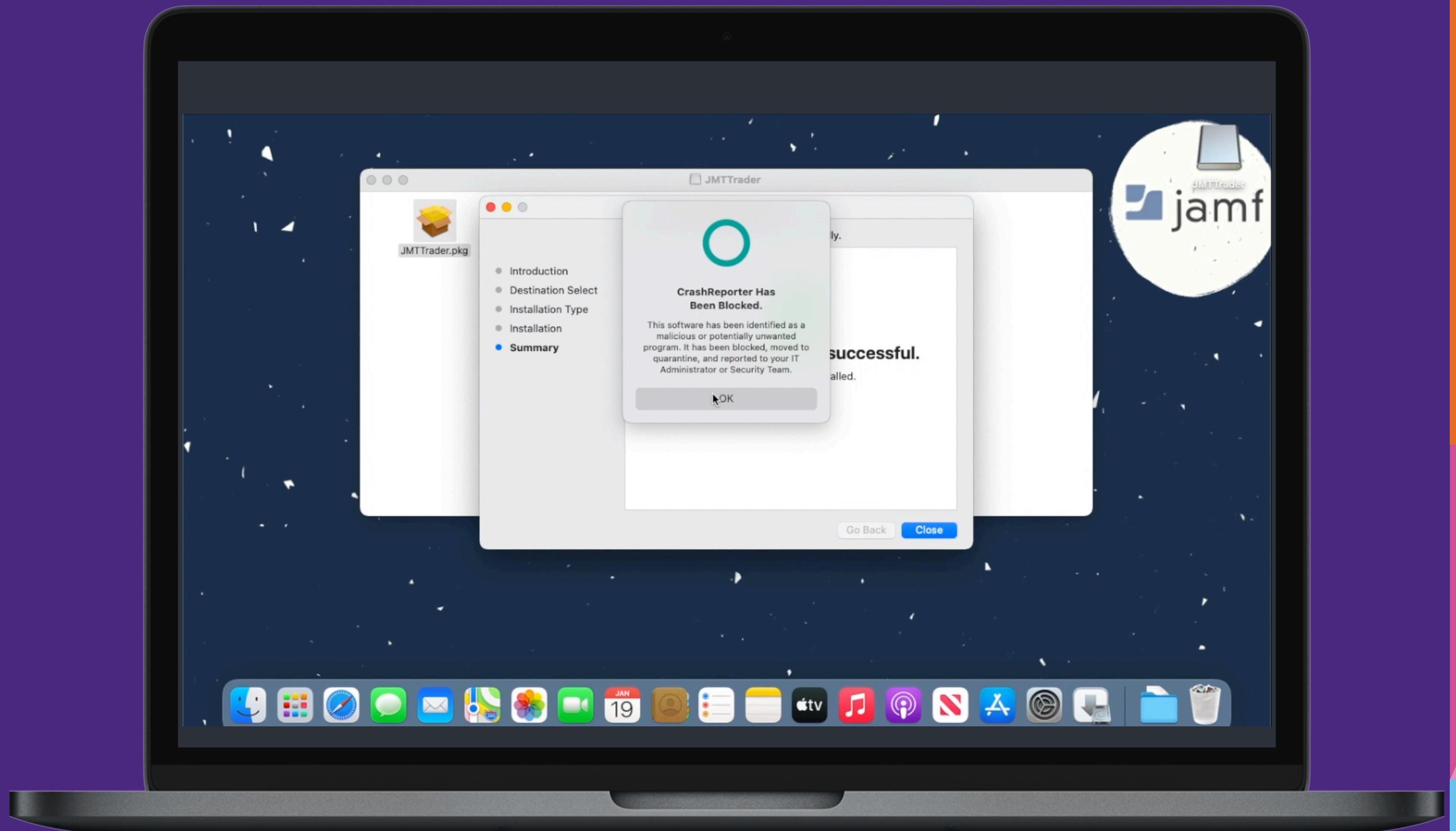
Inventory Information



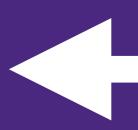
jamf | PRO



PROTECT



**Smart Computer Group:
Target device with new
Config Profile**



Inventory Information

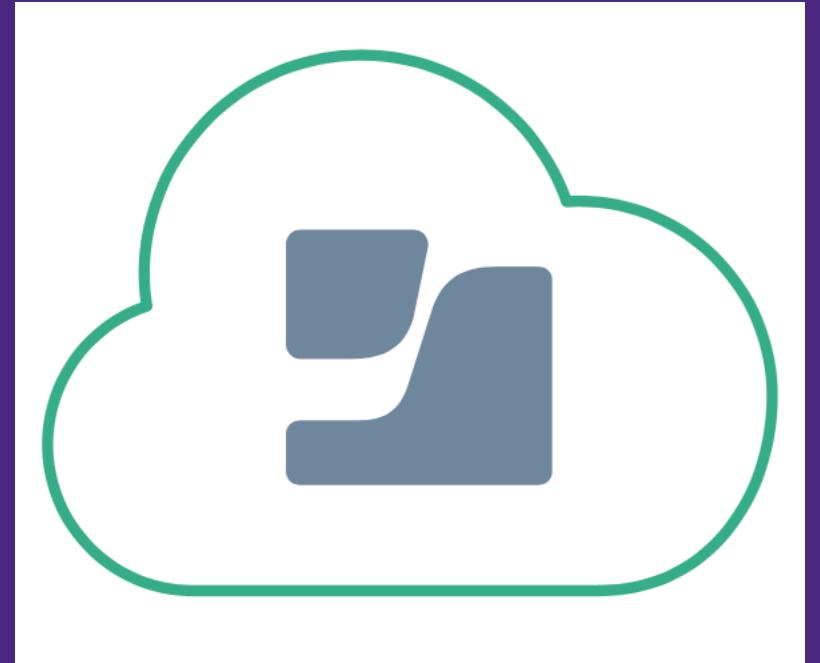


jamf | PRO



jamf | PROTECT

Smart Computer Group:
Target device with new
Config Profile



Execute Script

Update Config Profile



Inventory Information



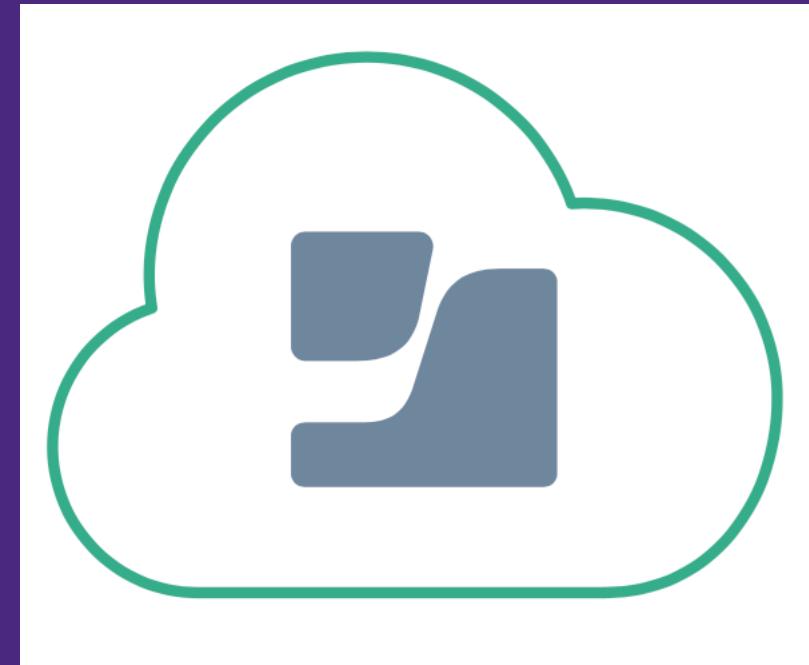
jamf | PRO





jamf | PROTECT

Smart Computer Group:
Target device with new
Config Profile



Execute Script

Update Config Profile

Inventory Information



jamf | PRO





jamf | PROTECT

Smart Computer Group:
Target device with new
Config Profile



Execute Script

Update Config Profile

Inventory Information



jamf | PRO





Smart Computer Group:
Target device with new
Config Profile



Event Details

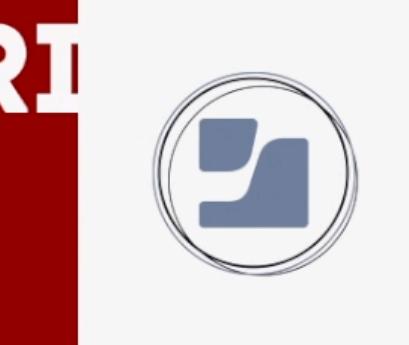
Execute Script

Update Config Profile

Inventory Information

jamf | PROTECT

SECURITY WARNING



Username

Password

Log In

Only INFOSEC Can Login

ONLY INFOSEC CAN LOGIN

Powered by Jamf

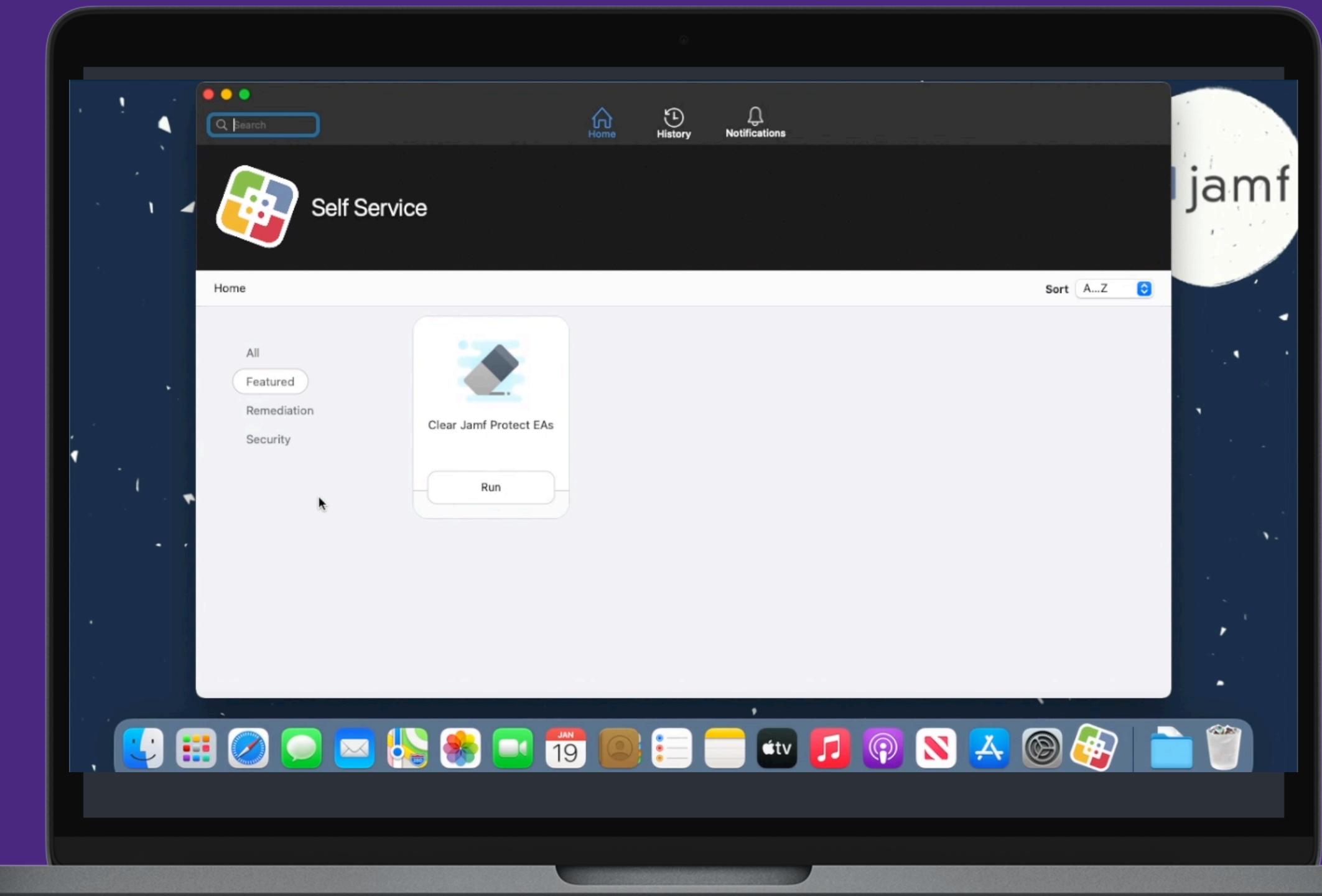
jamf | PRO



Execute Script



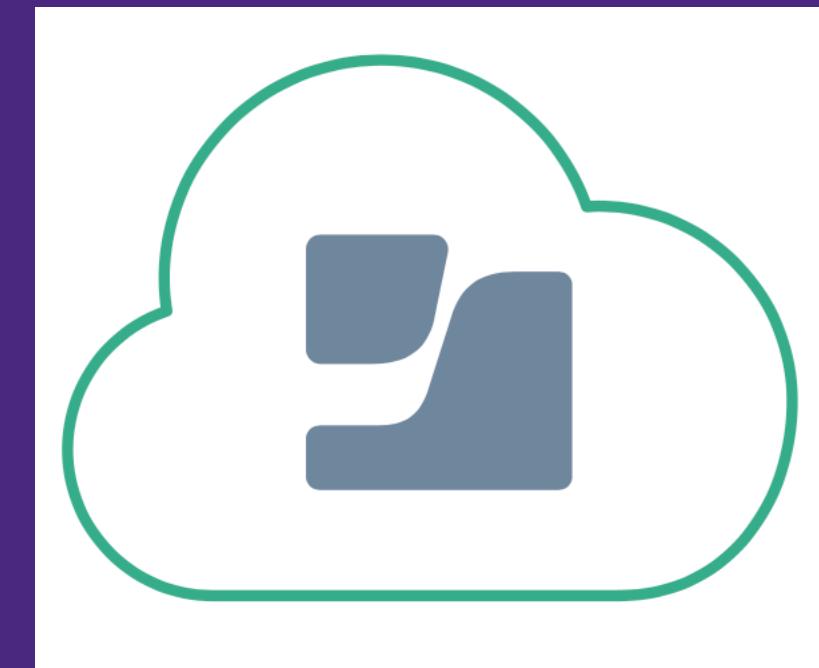
Self Service Command



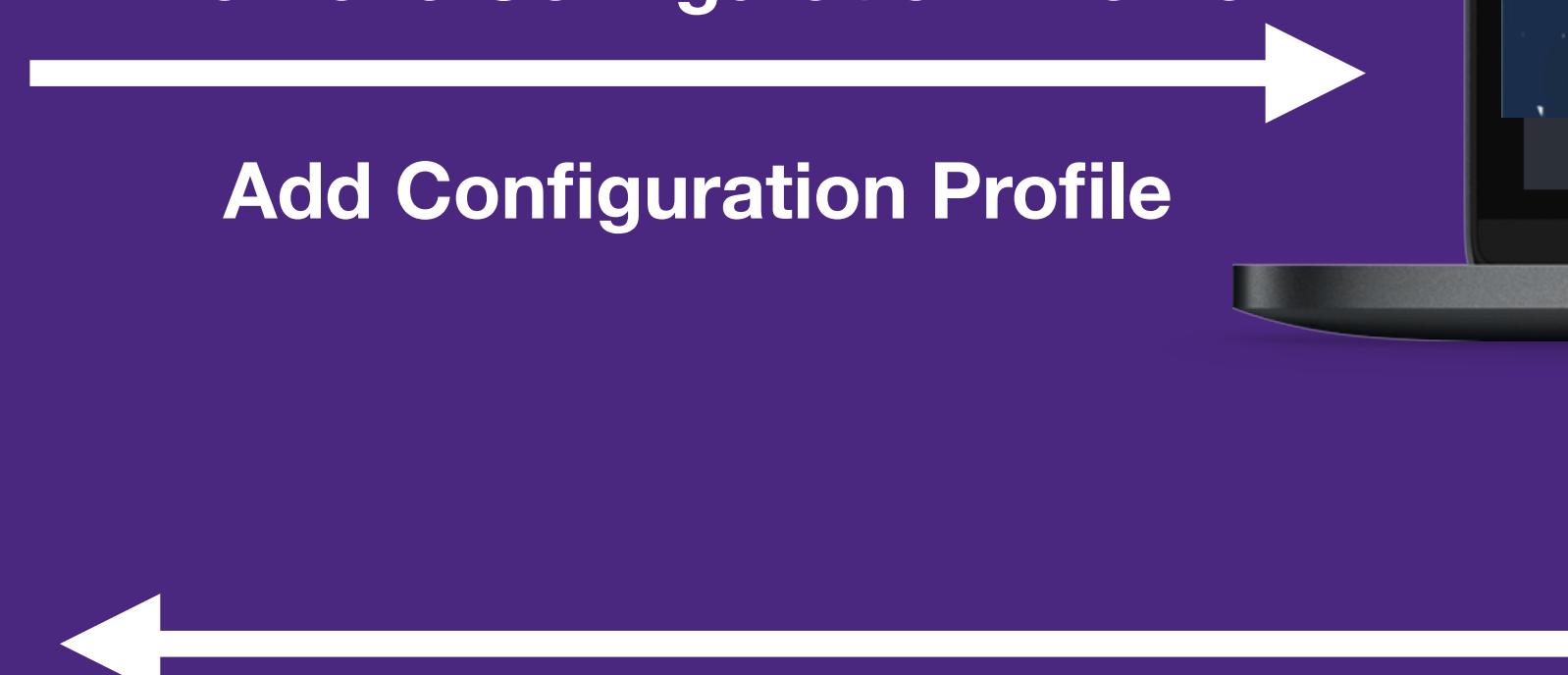
jamf | PRO



**Remove device from
Smart Computer Group**

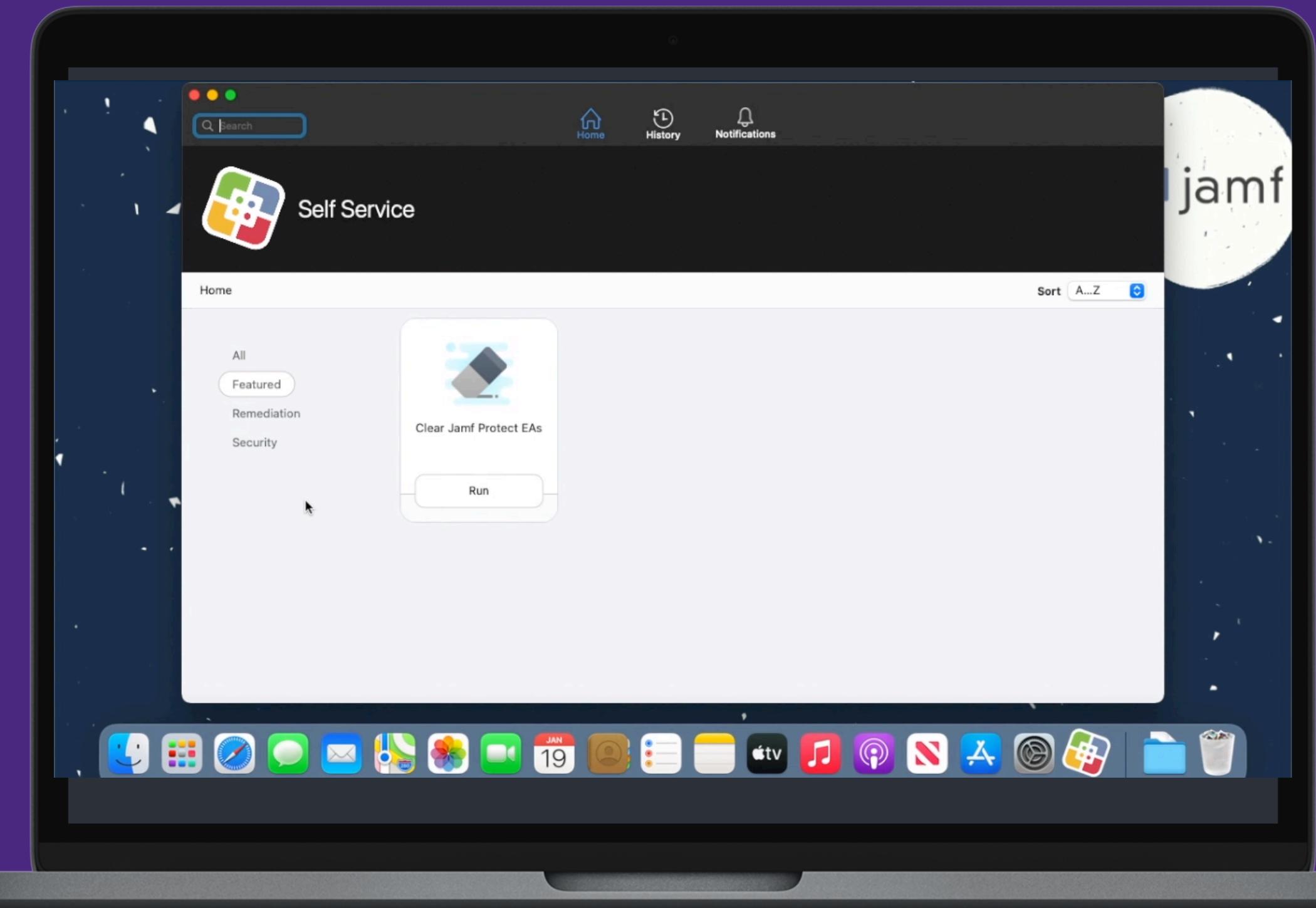


Remove Configuration Profile



Add Configuration Profile

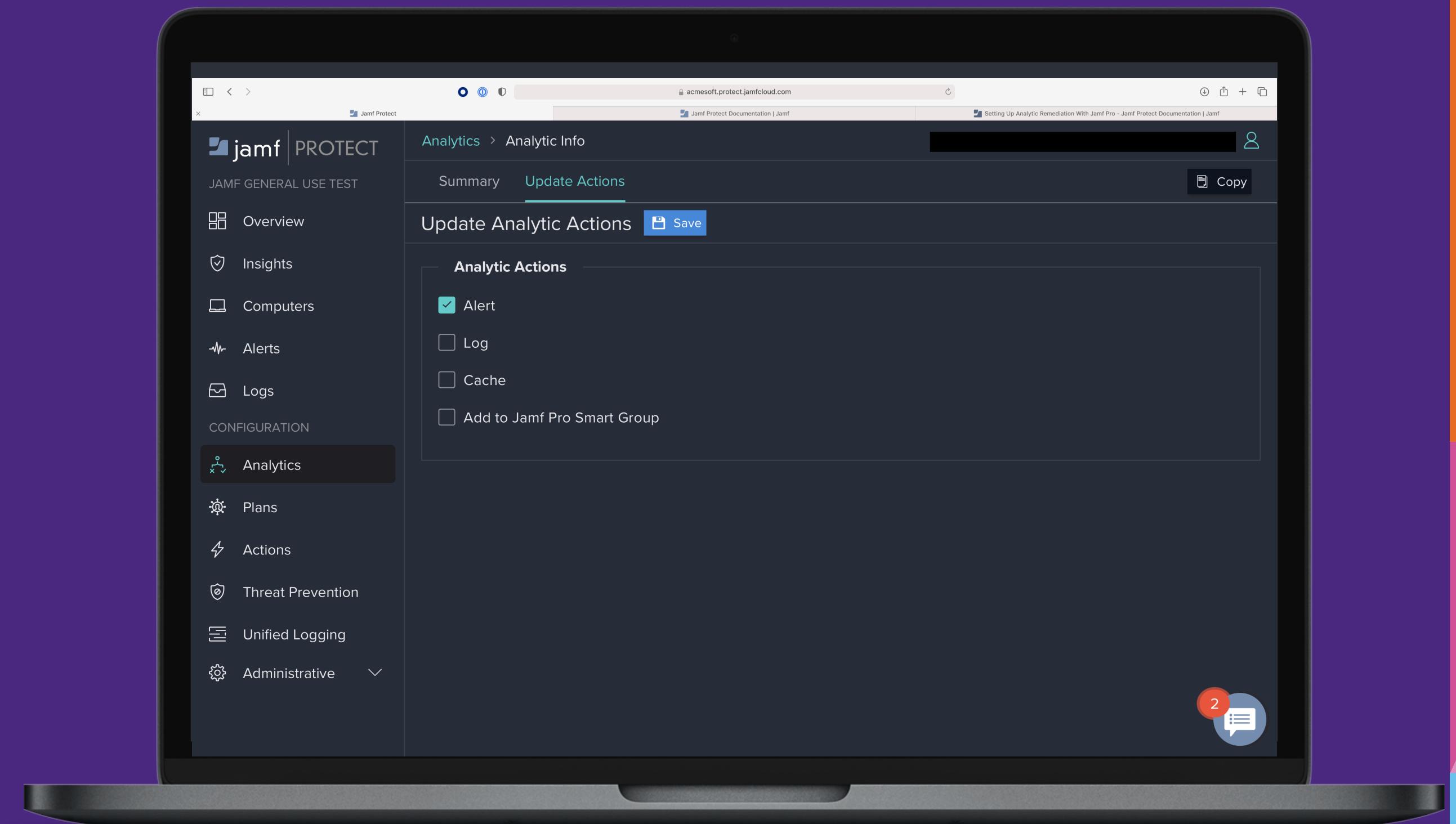
Updated Inventory



jamf | PRO



Analytic Remediation with Jamf Pro



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



Analytics > Analytic Info

Summary Update Actions

Update Analytic Actions

 Save

Analytic Actions

Alert

Log

Cache

Add to Jamf Pro Smart Group

Identifier This value must match a pre-configured Jamf Pro extension attribute.

High

Update Analytic Actions



S

Analytic Actions

 Alert Log Cache Add to Jamf Pro Smart Group**Identifier** This value must match a p

High

← New Computer Extension Attribute

Display Name Display name for the extension attribute

Jamf Protect - Smart Groups

 Enabled (script input type only)**Description** Description for the extension attribute

List containing all smart groups scoped by Jamf Protect

Data Type Type of data being collected

String

Inventory Display Category in which to display the extension attribute in Jamf Pro

General

Input Type Input type to use to populate the extension attribute

Script

Default Mode

Default Theme

```
1#!/bin/bash
2
3SMARTGROUPS_DIR=/Library/Application\ Support/JamfProtect/groups
4if [ -d "$SMARTGROUPS_DIR" ]; then
5    SMART_GROUPS=`/bin/ls "$SMARTGROUPS_DIR" | tr '\n' ','`
6    echo "<result>${SMART_GROUPS%?}</result>"
7else
8    echo "<result></result>"
9fi
10
11exit 0
```

Summary Update Actions

Update Analytic Actions



Analytic Actions

 Alert Log Cache Add to Jamf Pro Smart Group**Identifier** This value must match a pre-configured Jamf Pro extension attribute.

High

Settings : Computer Management > Extension Attributes

← New Computer Extension Attribute

Display Name Display name for the extension attribute

Jamf Protect - Smart Groups

Computers : Smart Computer Groups

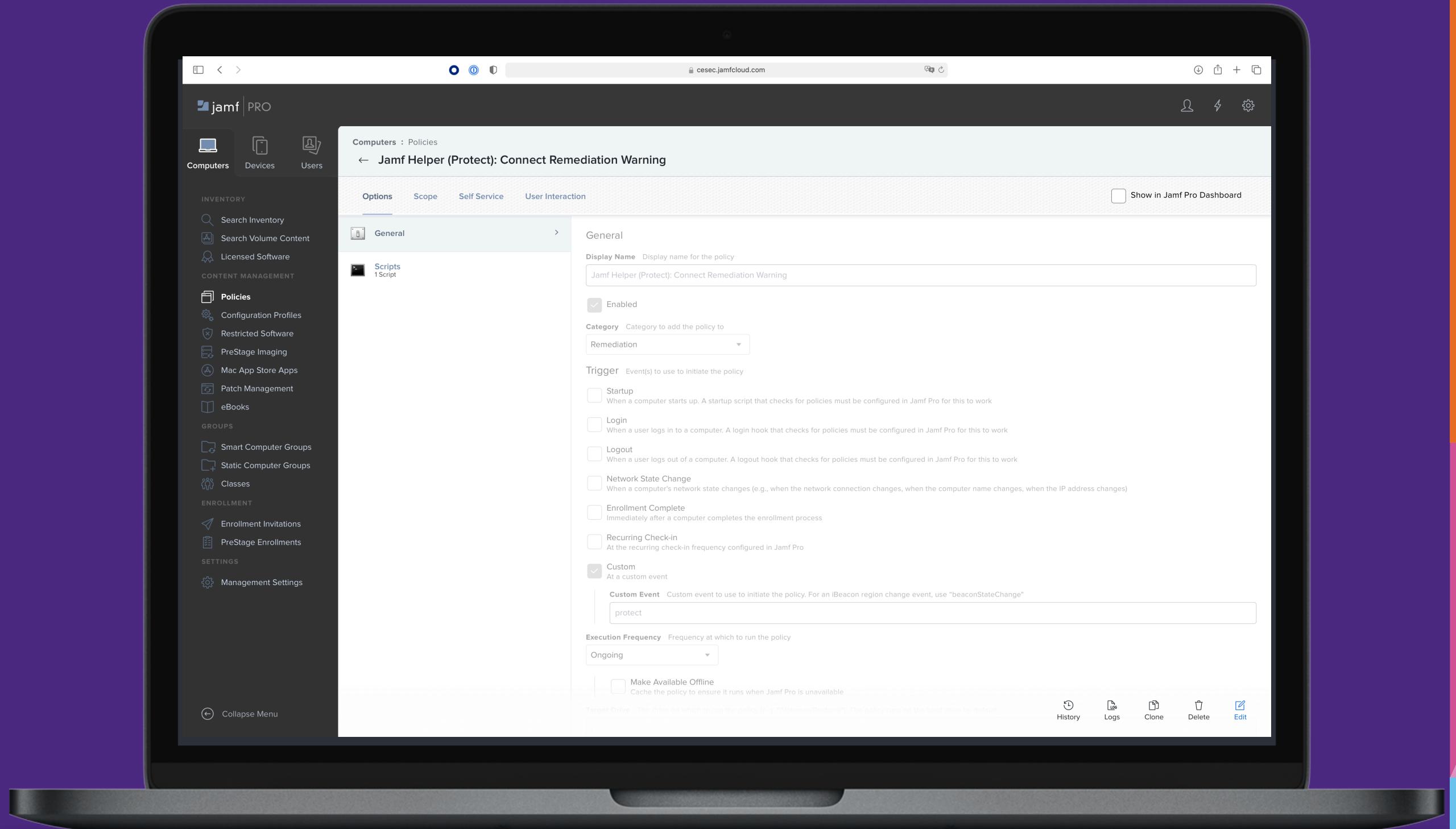
← Jamf Protect: High

Computer Group	Criteria
AND/OR	CRITERIA OPERATOR VALUE
Str	▼ Jamf Protect - Smart Groups match HIGH
Inve	▼
Ge	▼
Input	▼

Script

```
1 #!/bin/bash
2
3 SMARTGROUPS_DIR=/Library/Application\ Support/JamfProtect/groups
4 if [ -d "$SMARTGROUPS_DIR" ]; then
5     SMART_GROUPS=`/bin/ls "$SMARTGROUPS_DIR" | tr '\n' ','`
6     echo "<result>${SMART_GROUPS%?}</result>"
7 else
8     echo "<result></result>"
9 fi
10
11 exit 0
```

How to create a policy to run offline in Jamf Pro



jamf PRO

cesec.jamfcloud.com

Computers : Policies

← Jamf Helper (Protect): Connect Remediation Warning

Options Scope Self Service User Interaction Show in Jamf Pro Dashboard

General Scripts 1 Script

General

Display Name Display name for the policy
Jamf Helper (Protect): Connect Remediation Warning

Enabled

Category Category to add the policy to
Remediation

Trigger Event(s) to use to initiate the policy

Startup When a computer starts up. A startup script that checks for policies must be configured in Jamf Pro for this to work

Login When a user logs in to a computer. A login hook that checks for policies must be configured in Jamf Pro for this to work

Logout When a user logs out of a computer. A logout hook that checks for policies must be configured in Jamf Pro for this to work

Network State Change When a computer's network state changes (e.g., when the network connection changes, when the computer name changes, when the IP address changes)

Enrollment Complete Immediately after a computer completes the enrollment process

Recurring Check-in At the recurring check-in frequency configured in Jamf Pro

Custom At a custom event

Custom Event Custom event to use to initiate the policy. For an iBeacon region change event, use "beaconStateChange"
protect

Execution Frequency Frequency at which to run the policy
Ongoing

Make Available Offline Cache the policy to ensure it runs when Jamf Pro is unavailable

Target Drive The drive on which to run the policy (e.g. "/Volumes/Bootcamp"). The policy runs on the boot drive by default

History Logs Clone Delete Edit

Collapse Menu

`sudo jamf magic policy -event protect`



Custom

At a custom event

Custom Event Custom event to use to initiate the policy. For an iBeacon region change event, use “beaconStateChange”

protect

Execution Frequency Frequency at which to run the policy

Ongoing



Make Available Offline

Cache the policy to ensure it runs when Jamf Pro is unavailable

Policy actions

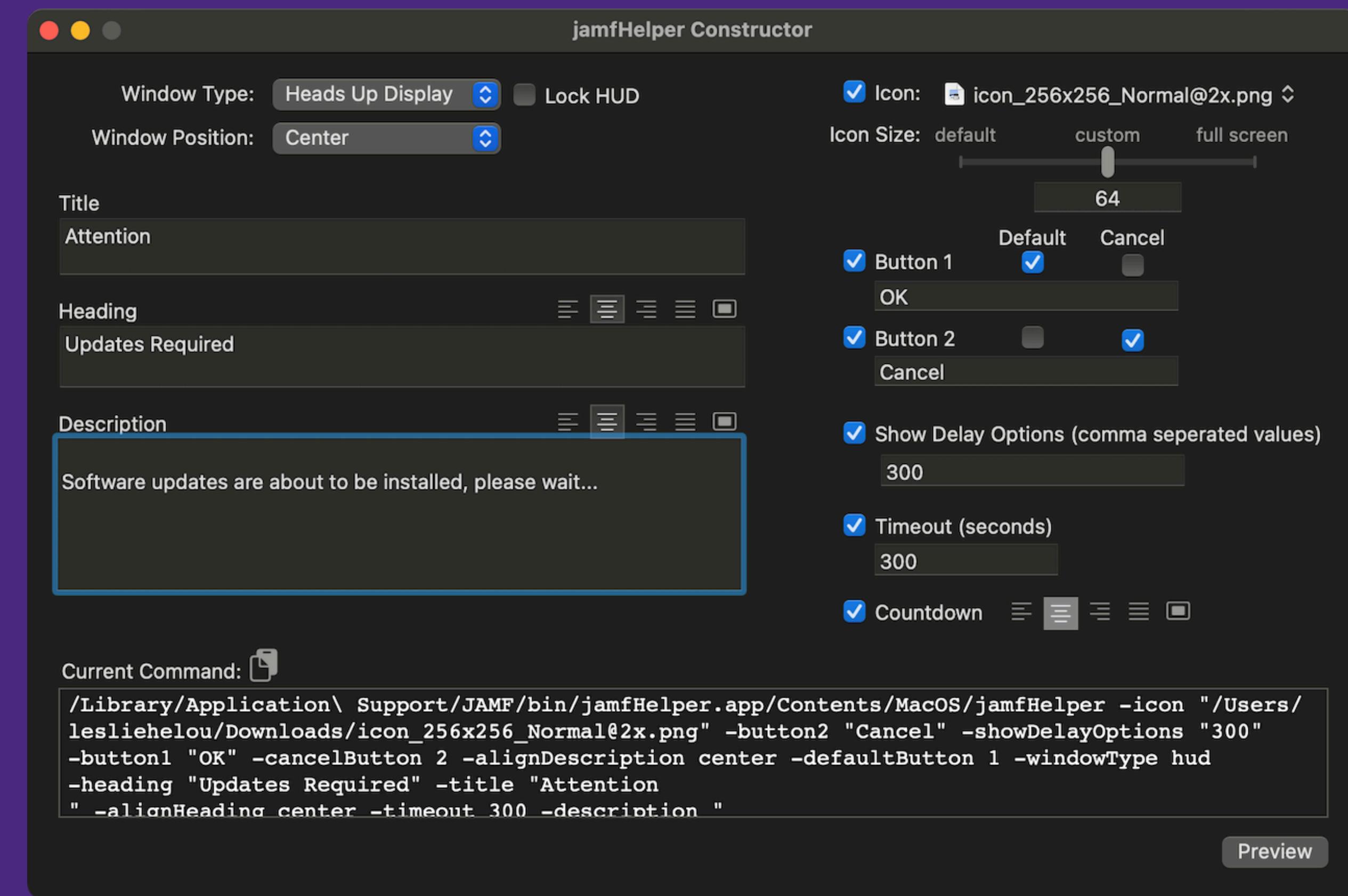
```
jamfHelper="/Library/Application Support/JAMF/bin/jamfHelper.app/Contents/MacOS/jamfHelper"

#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>



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/deponotify.log
echo "Command: MainTitle: Jamf Protect Remediation" >> /var/tmp/deponotify.log
echo "Command: MainText: Malicious activity on this computer has been detected by Jamf Protect.\nIf this screen appears for longer than 5 m" >> /var/tmp/deponotify.log
echo "Status: Isolating malicious software..." >> /var/tmp/deponotify.log
echo "Command: Determinate: 2" >> /var/tmp/deponotify.log

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

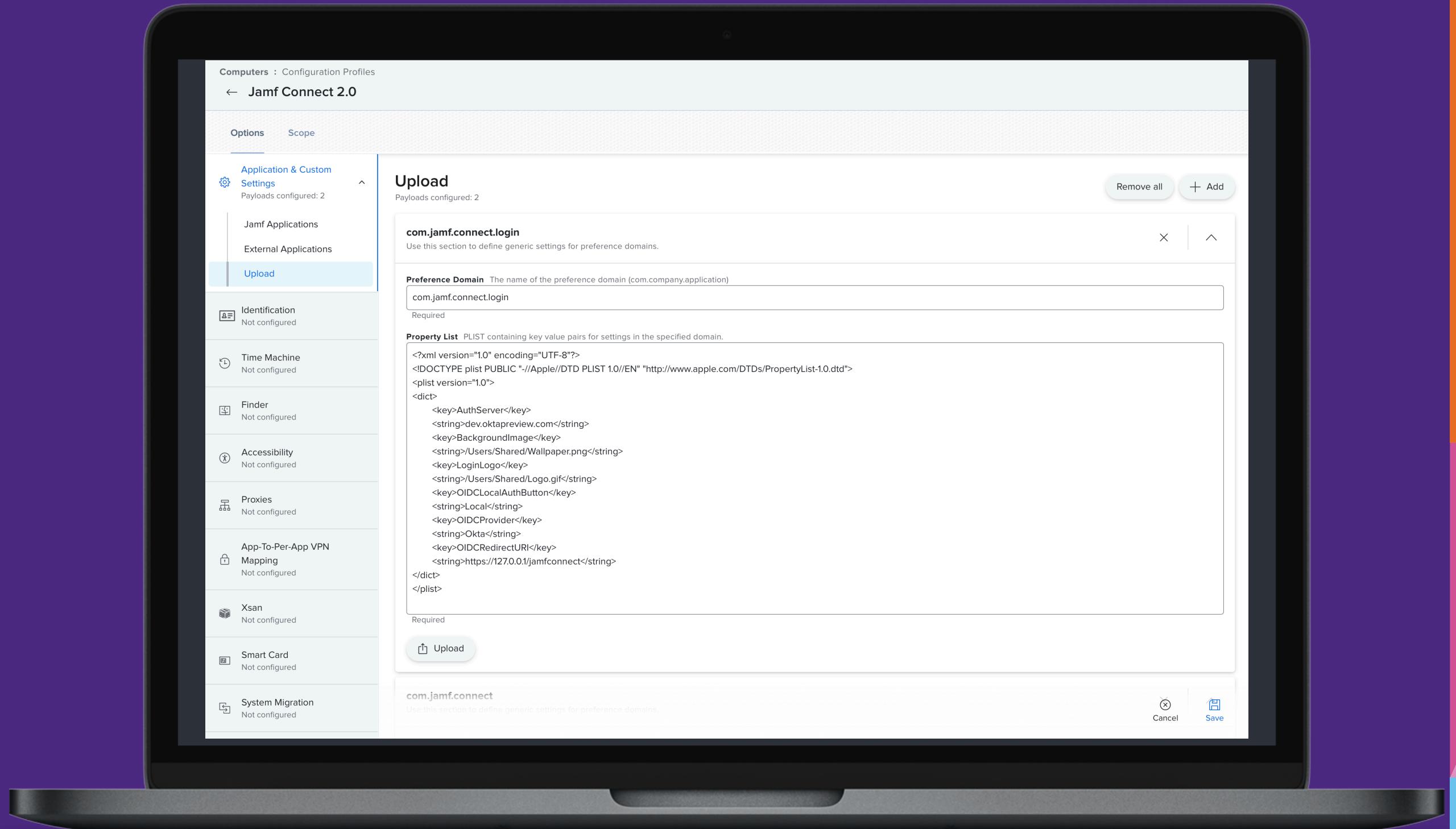
# Here's where you would put your Jamf policy command
#jamf policy -event collection
#sleep 2

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

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

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

So.... remember those Smart Computer Groups?



Access Control Lists in IdP

Computers : Configuration Profiles

← Jamf Connect 2.0

Options Scope

Targets Limitations Exclusions

Selected Exclusions + Add

EXCLUSION	TYPE	
Jamf Protect: High	Smart Computer Group	Remove

© copyright 2002-2021 Jamf

Access Control Lists in IdP

Computers : Configuration Profiles

← Jamf Connect INFOSEC Alert

Options Scope Show in Jamf Pro Dashboard

General Add/Remove properties

Application & Custom Settings 1 payload configured

Jamf Applications

Preference Domain Properties
Properties to configure for the preference domain
com.jamf.connect.login
Preference Domain: com.jamf.connect.login, Application: Jamf Connect Login

Access Client ID
OpenID Connect application that determines which users can access the computer. Note: All users, including administrators, must be added to this app in your Okta admin console to ensure access to Jamf Connect Login.
Ooawcd0w7v4yfqPNR0h7

Admin Client ID
OpenID Connect application that determines which users are created with local administrator accounts Note: Only administrators should be added to this app in your Okta admin console.
Ooawcd0w7v4yfqPNR0h7

Secondary Login Client ID
OpenID Connect application that determines who can create local user accounts after an initial user has been created
Ooawcd0w7v4yfqPNR0h7

Allow Local Fallback
Allow local authentication if a network is unavailable
true

Require Network Authentication
Require users to log in by authenticating with their identity provider
true

Background Image
Path to a locally stored image to use as a background for the login window
/Users/Shared/BlueTeam.png

Login Window Message

History Logs Download Clone Delete Edit

© copyright 2002-2021 Jamf

Access Control Lists in IdP

Microsoft Azure Search resources, services, and docs (G+/-) 4 ? User icon

Home > jamfse.io >

Jamf Connect - INFOSEC ONLY ACCESS

Search (Cmd+/) Delete Endpoints Preview features

Overview Quickstart Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners
- Roles and administrators | Preview
- Manifest

Get Started Documentation

Essentials

Display name: Jamf Connect - INFOSEC ONLY ACCESS

Application (client) ID: b92961e0-3e66-42bd-9ab5-[REDACTED]

Object ID: a448654e-4de8-[REDACTED]

Directory (tenant) ID: f83fb0da-8168-4bf9-[REDACTED]

Supported account types: My organization only

Client credentials: Add a certificate or secret

Redirect URIs: 0 web, 0 spa, 1 public client

Application ID URI: Add an Application ID URI

Managed application in local directory: Jamf Connect - INFOSEC ONLY ACCESS

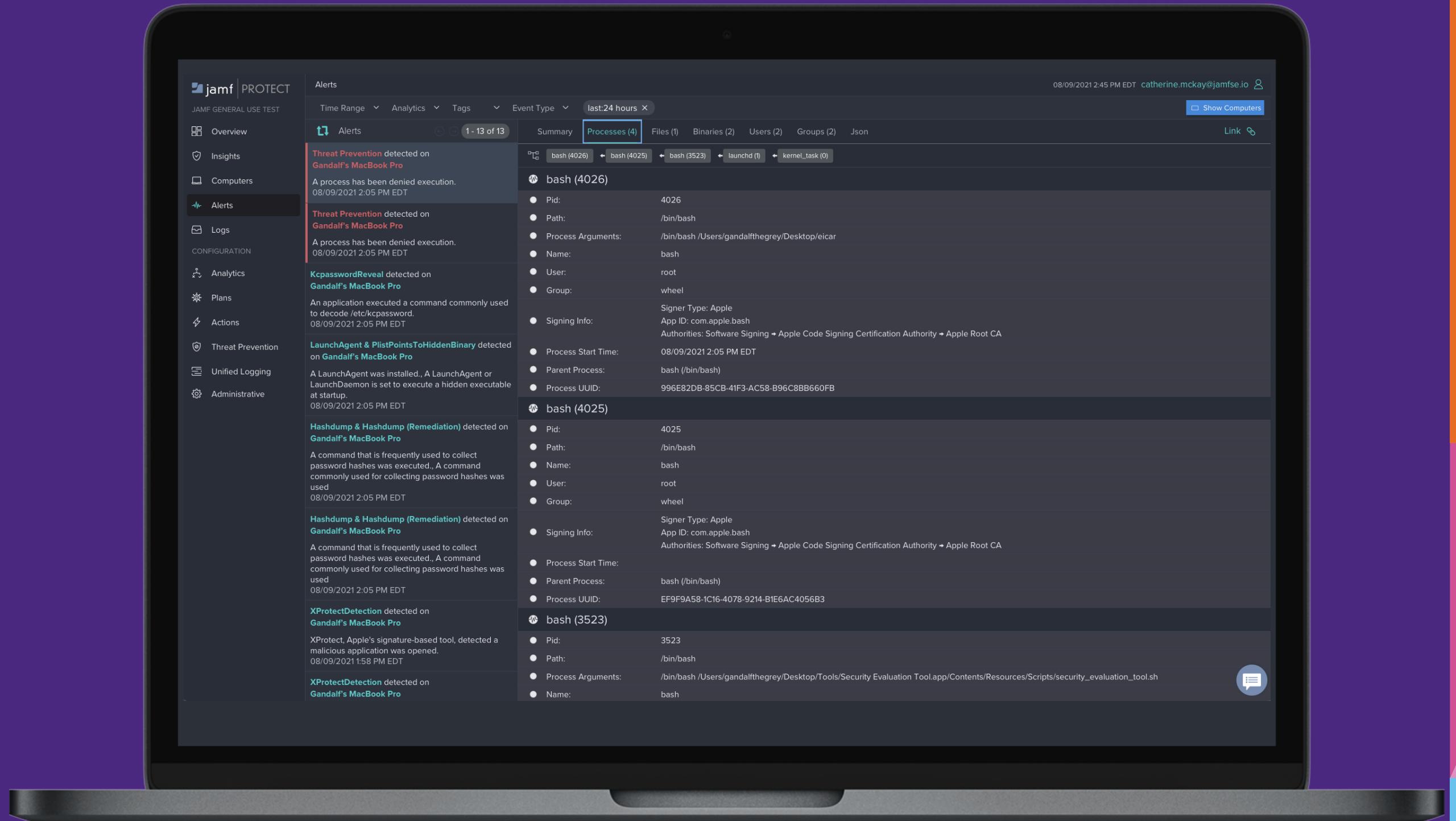
Information

i Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)

i Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

Support + Troubleshooting

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



jamf PROTECT

JAMF GENERAL USE TEST

Time Range ▾ Analytics ▾ Tags ▾ Event Type ▾ last:24 hours ×

Show Computers

Link

Alerts

1 - 13 of 13

Processes (4)

Summary Processes (4) Files (1) Binaries (2) Users (2) Groups (2) Json

Threat Prevention detected on Gandalf's MacBook Pro

A process has been denied execution.

08/09/2021 2:05 PM EDT

KcpasswordReveal detected on Gandalf's MacBook Pro

An application executed a command commonly used to decode /etc/kcpASSWORD.

08/09/2021 2:05 PM EDT

LaunchAgent & PlistPointsToHiddenBinary detected on Gandalf's MacBook Pro

A LaunchAgent was installed., A LaunchAgent or LaunchDaemon is set to execute a hidden executable at startup.

08/09/2021 2:05 PM EDT

Hashdump & Hashdump (Remediation) detected on Gandalf's MacBook Pro

A command that is frequently used to collect password hashes was executed., A command commonly used for collecting password hashes was used

08/09/2021 2:05 PM EDT

Hashdump & Hashdump (Remediation) detected on Gandalf's MacBook Pro

A command that is frequently used to collect password hashes was executed., A command commonly used for collecting password hashes was used

08/09/2021 2:05 PM EDT

XProtectDetection detected on Gandalf's MacBook Pro

XProtect, Apple's signature-based tool, detected a malicious application was opened.

08/09/2021 1:58 PM EDT

XProtectDetection detected on Gandalf's MacBook Pro

Process Tree:

- bash (4026) → bash (4025) → bash (3523) → launchd (1) → kernel_task (0)

bash (4026)

- Pid: 4026
- Path: /bin/bash
- Process Arguments: /bin/bash /Users/gandalfthegrey/Desktop/eicar
- Name: bash
- User: root
- Group: wheel
- Signer Info: Signer Type: Apple
App ID: com.apple.bash
Authorities: Software Signing → Apple Code Signing Certification Authority → Apple Root CA
- Process Start Time: 08/09/2021 2:05 PM EDT
- Parent Process: bash (/bin/bash)
- Process UUID: 996E82DB-85CB-41F3-AC58-B96C8BB660FB

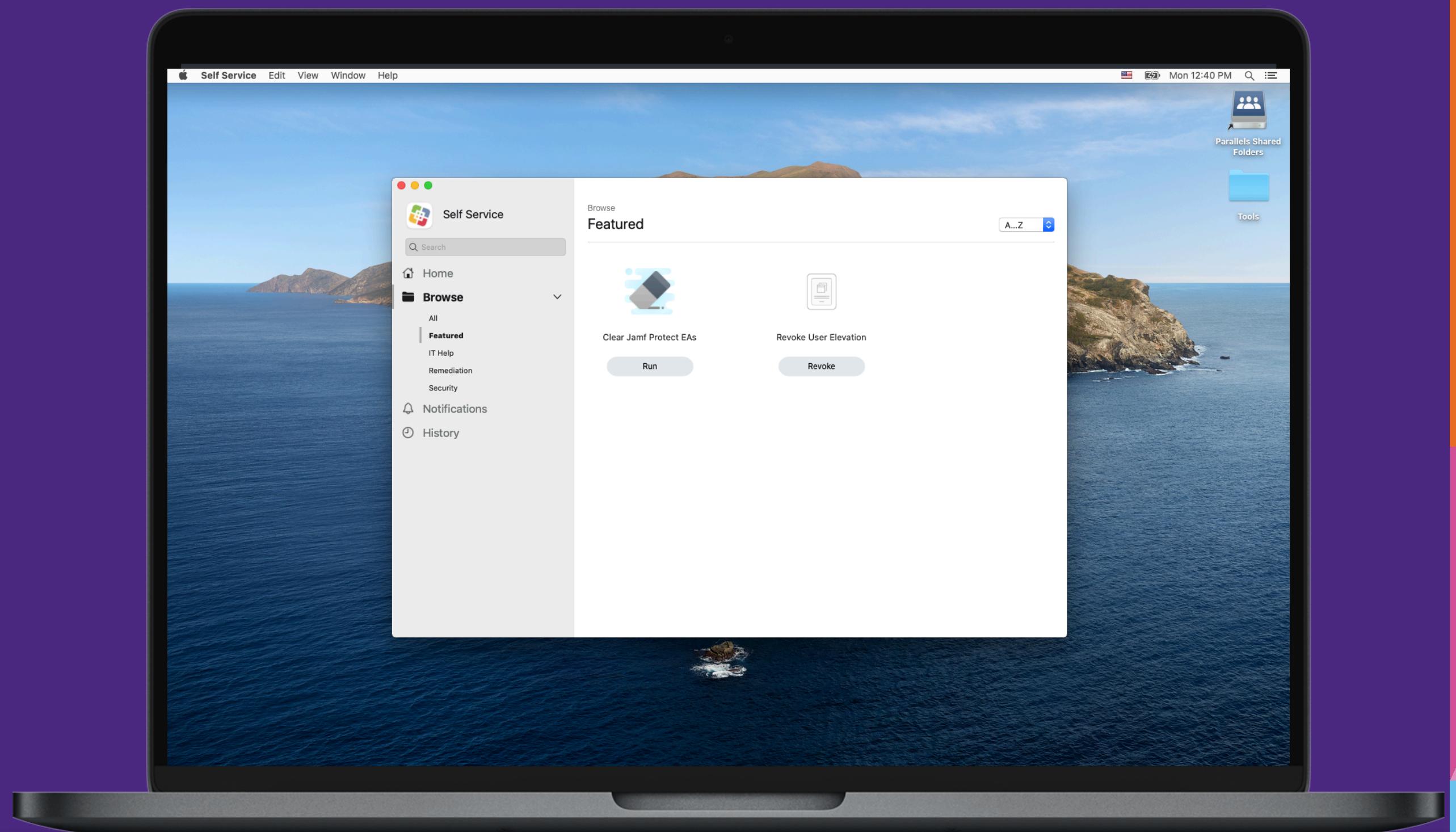
bash (4025)

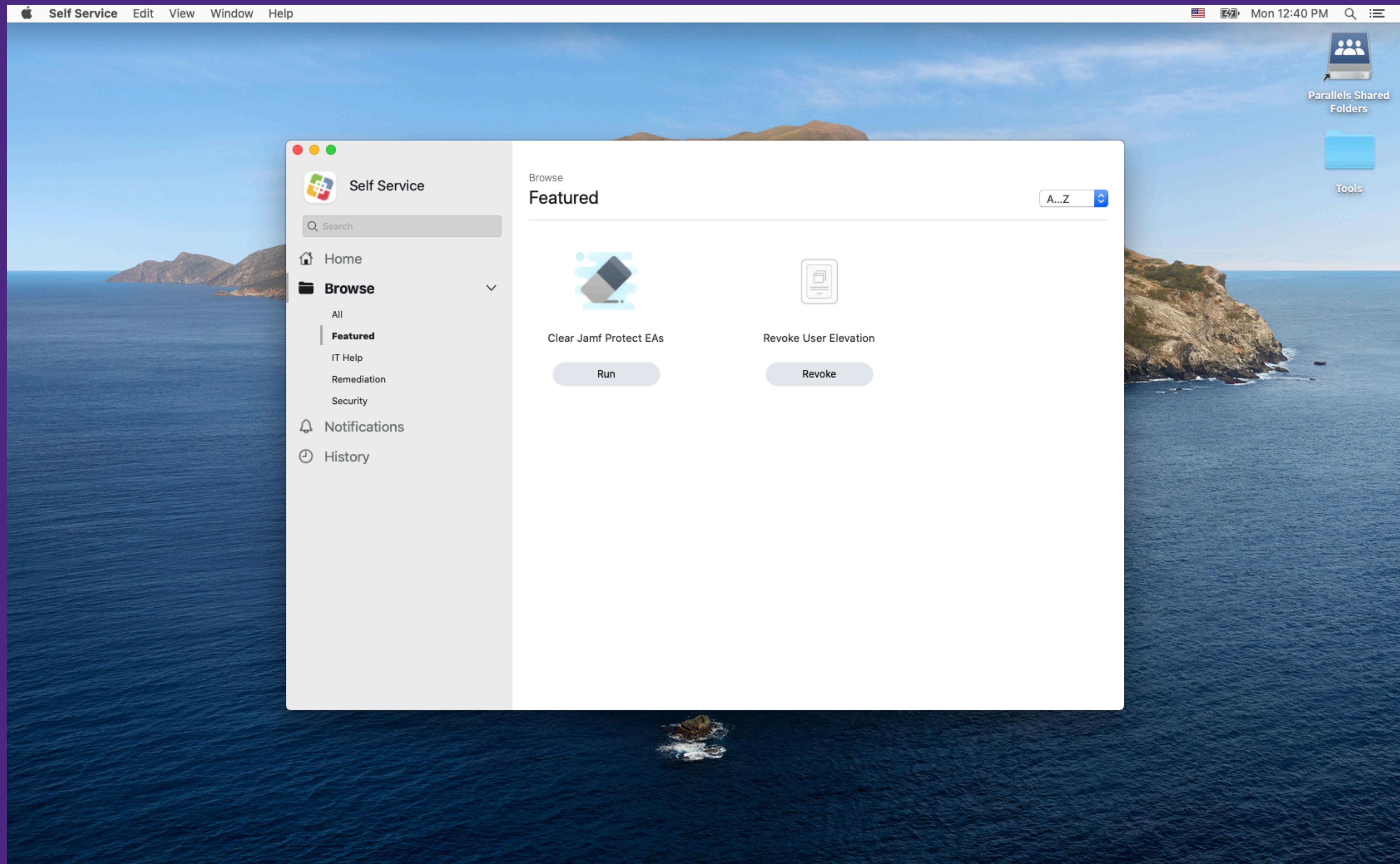
- Pid: 4025
- Path: /bin/bash
- Name: bash
- User: root
- Group: wheel
- Signer Info: Signer Type: Apple
App ID: com.apple.bash
Authorities: Software Signing → Apple Code Signing Certification Authority → Apple Root CA
- Process Start Time: 08/09/2021 2:05 PM EDT
- Parent Process: bash (/bin/bash)
- Process UUID: EF9F9A58-1C16-4078-9214-B1E6AC4056B3

bash (3523)

- Pid: 3523
- Path: /bin/bash
- Process Arguments: /bin/bash /Users/gandalfthegrey/Desktop/Tools/Security Evaluation Tool.app/Contents/Resources/Scripts/security_evaluation_tool.sh
- Name: bash

How to clear the EA with Self Service





▼ Clear Jamf Protect EAs

Ongoing

Self Service

- 1  Run Unix command 'rm /Library/Application\ Support/JamfProtect/groups/*'
- 2  Update Inventory

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-rabbit>

Jamf Support

support@jamf.com

Jamf Professional Services Team

info@jamf.com

Thank you for listening!