



Jamf Connect: Deployment Planning

PRESENTING TO





Jamf Connect: Deployment Planning



Sean Rabbitt

Sr. Consulting Engineer,
Identity

Helping Organizations Succeed with Apple

From a seamless onboarding experience to empowering users to get the most up-to-date resources needed to be productive, apps are the crux of every step in a user's journey.

- ▶ The Standard for Apple Enterprise Management
- ▶ Large and Growing Addressable Market
- ▶ Strong and Predictable Financial Profile



43,000+

Active Jamf Customers

18,5MM+

Active Jamf Customers

100k

Jamf Nation Members

117%

Dollar-Based Net Retention

95%

Rate Jamf as a Great
Workplace

55+

2019 Net Promotor Score

Agenda

1 | What is Jamf Connect

2 | Jamf Connect Menu Bar Agent

3 | Jamf Connect Login

4 | Jamf Pro and Jamf Connect together

Or, how I learned to stop worrying and love the smart groups



What is Jamf Connect

What is Jamf Connect



Account provisioning

Create secure accounts that get users up and running from the moment they unbox their Mac, with a single cloud identity.



Modern Authentication

Employees accessing corporate information and resources from anywhere increases the ability for data to get into the wrong hands. That's why users must authenticate before they are given access to sensitive information.



Mac Password Sync

Sync Mac passwords across the device and all applications with a single cloud identity that unlocks the resources employees need to stay productive.



NoMAD



NoMAD
L O G I N

It makes **Local User Accounts**
It synchronizes **Local User Account Passwords**
It lets you pick who is a **Local Administrator**

Jamf Connect Menu Bar



Users & Groups

Search

Current User

User Connect
Standard

Other Users

Guest User
Off

Login Options

+ -

U User Connect

Change Password...

Contacts Card: Open...

☐ Allow user to administer this computer

Click the lock to make changes.

?

user.connect@jamfse.io

Password expires: 0 days

Connect...

Change password...

Unlock

Enable Unlock ☒

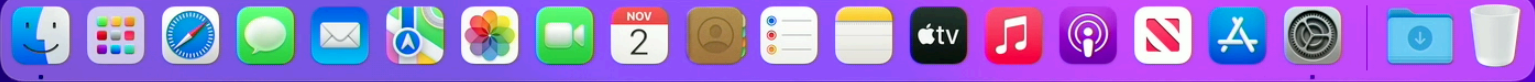
Paired Devices...

Get software

Get help

About...

Quit Jamf Connect



Jamf Connect menu bar

Lives in the menu bar dock

Silently checks identity provider for password changes every 60 minutes

com.jamf.connect domain

Can work completely independent of login window



Customize Jamf Connect

Hide

```
<key>HiddenMenuItems</key>
<array>
  <string>resetpassword</string>
</array>
```

Custom Actions

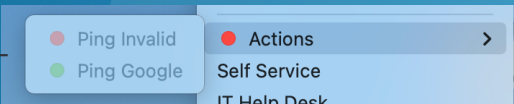
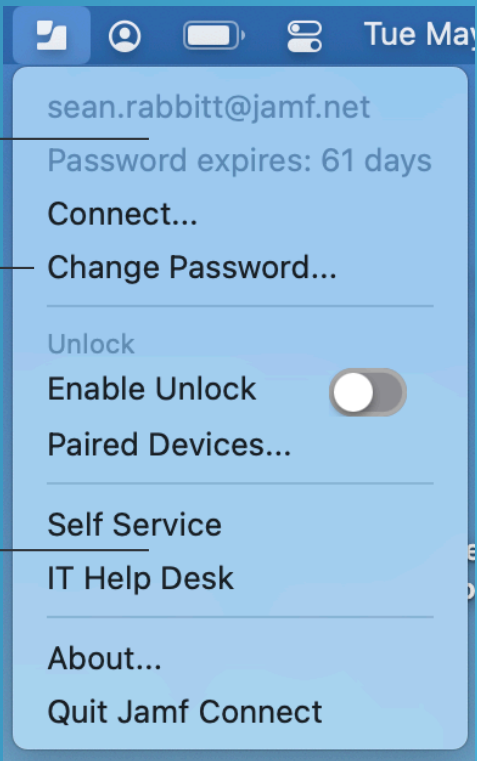
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Version</key>
  <string>1</string>
  <key>MenuItem</key>
  <true/>
  <key>Actions</key>
  <array>
    <dict>
      <key>Title</key>
      <dict>
        <key>Command</key>
        <string>ping</string>
        <key>CommandOptions</key>
        <string>domain.donna.exist.atall.bar</string>
      </dict>
      <key>ToolTip</key>
      <string>Pings a bad domain that doesn't exist</string>
      <key>Name</key>
      <string>Ping Invalid</string>
    </dict>
    <dict>
      <key>Title</key>
      <dict>
        <key>Command</key>
        <string>ping</string>
        <key>CommandOptions</key>
        <string>google.com</string>
      </dict>
      <key>ToolTip</key>
      <string>Pings google.com and returns a result of good or bad</string>
      <key>Name</key>
      <string>Ping Google</string>
    </dict>
  </array>
</dict>
</plist>
```

Get Kerberos Tickets

```
<key>Kerberos</key>
<dict>
  <key>AutoRenewTickets</key>
  <true/>
  <key>Realm</key>
  <string>JAMFSE.IO</string>
</dict>
```

Rename

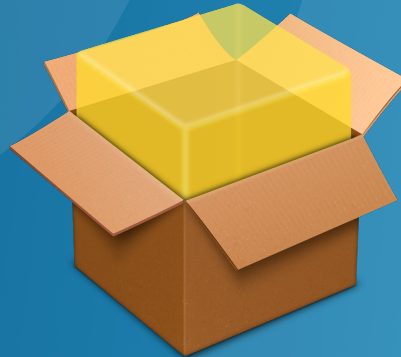
```
<key>CustomMenuItems</key>
<dict>
  <key>gethelp</key>
  <string>IT Help Desk</string>
  <key>getsoftware</key>
  <string>Self Service</string>
</dict>
```



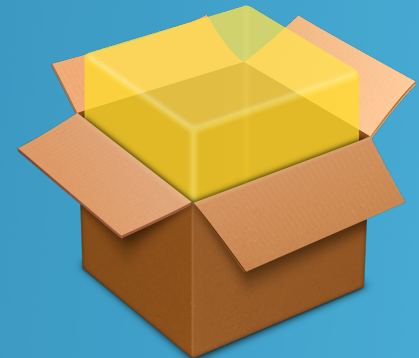
Deploy Jamf Connect menu bar



com.jamf.connect
configuration profile



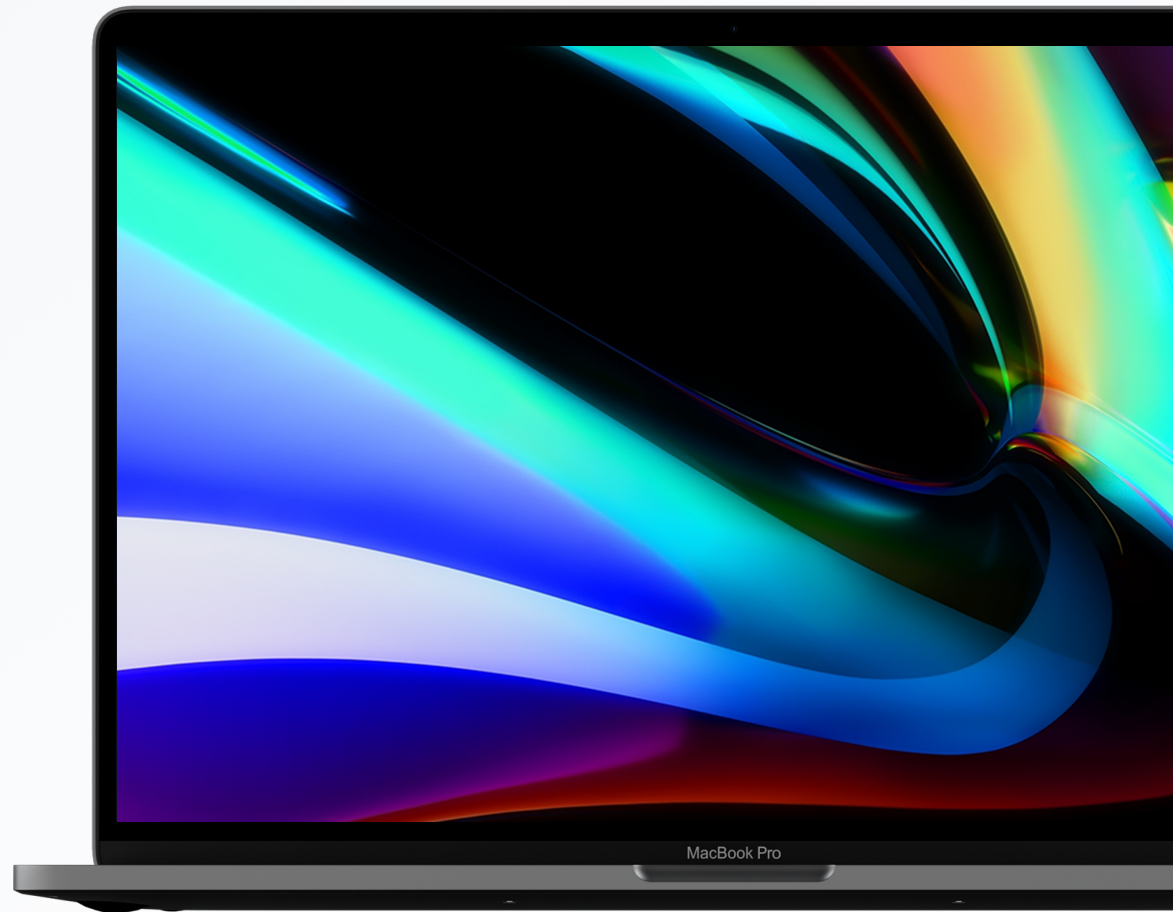
JamfConnect.pkg



JamfConnectLaunchAgent.pkg

Why just the **menu bar agent** by itself?

- Existing user accounts
- FileVault enabled
- Don't want additional accounts
- Centralized password complexity management
- 1:1 deployments




Jamf Connect Login



Authenticate

U.S.



 PARTNERS


Sign in

someone@example.com

Can't access your account?

Back

Next

 Sign-in options

Terms of use

Privacy & cookies

...

Shutdown

Restart

Local Login

Refresh

Help

Powered by Jamf

Jamf Connect login

Designed for Cloud

WiFi and Keyboard settings on login screen

OIDC or Okta

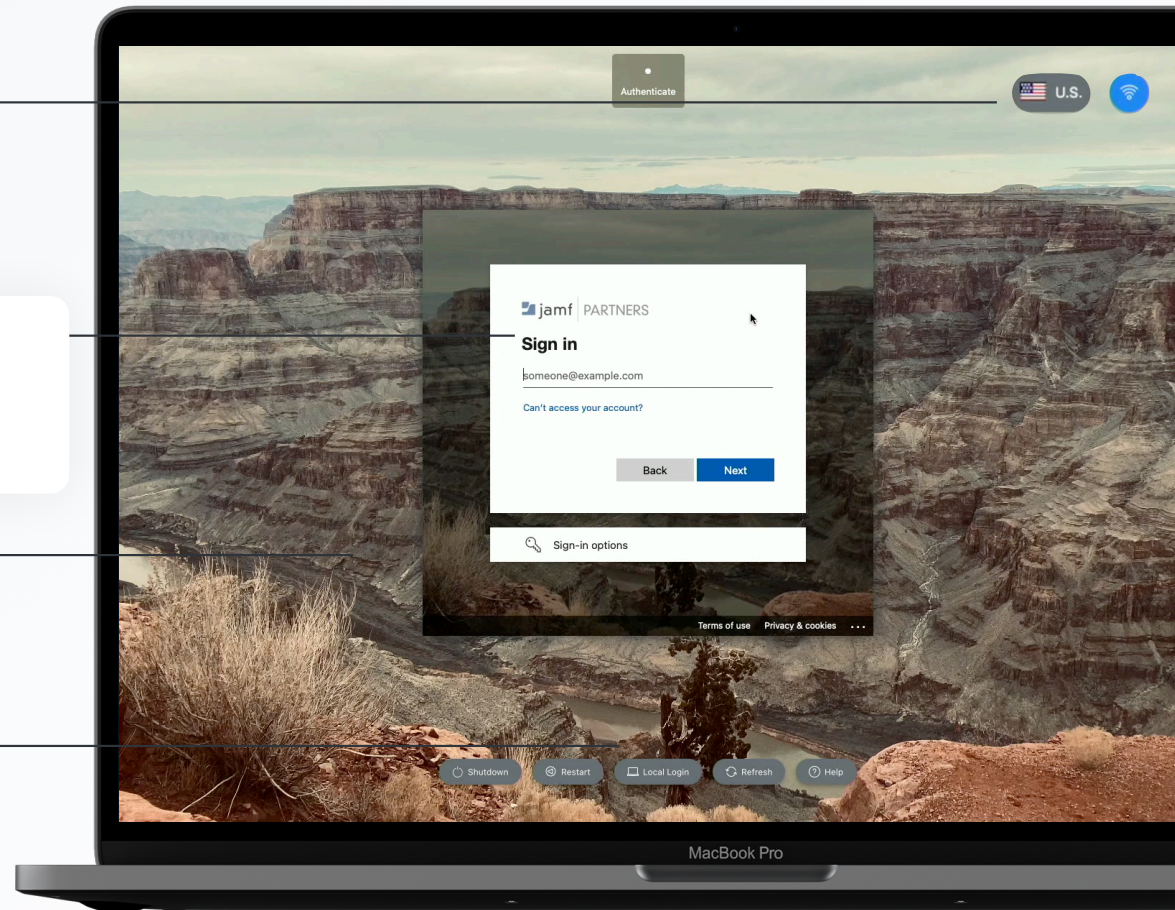
Client direct communication to your IDP - no extra servers

Branded for your organization

Select wallpapers, logos, help files, and your tenant login page

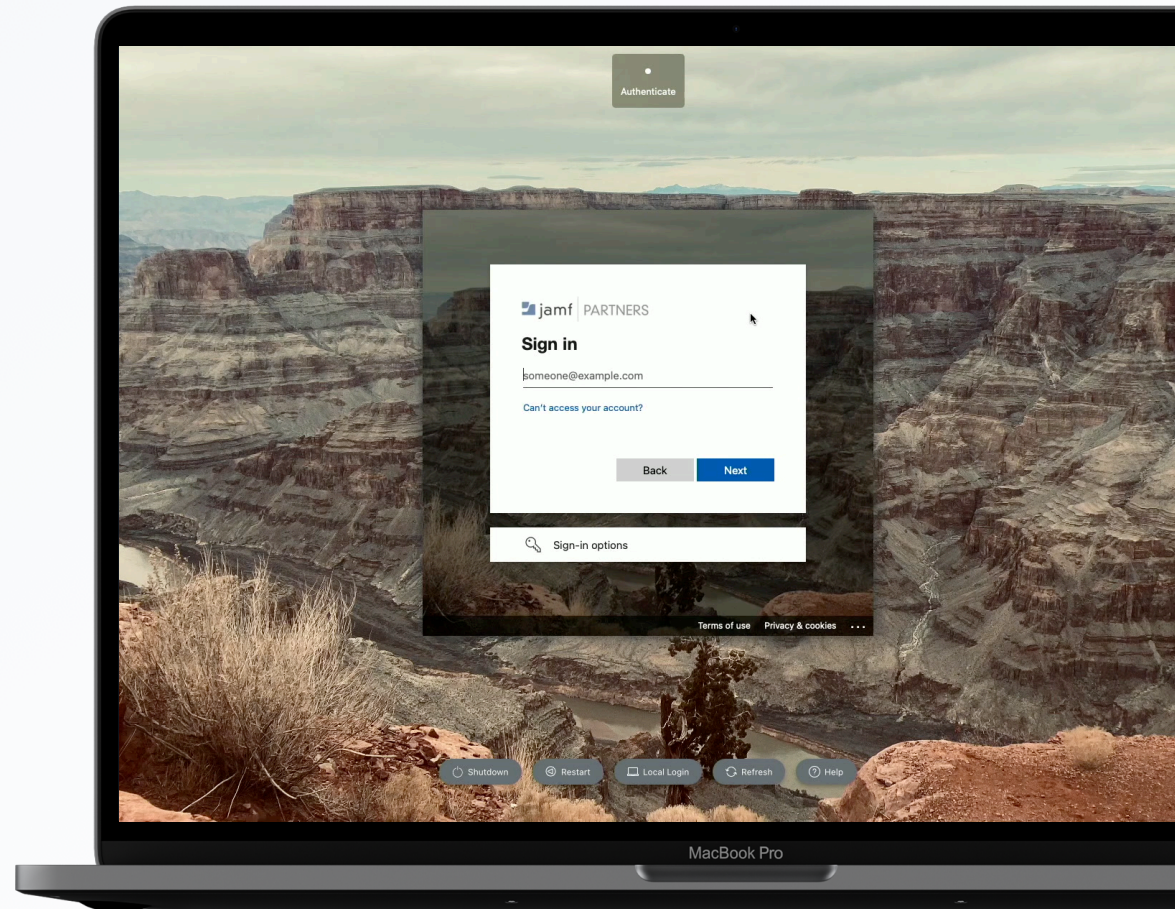
Secure and customized

Custom online and offline help files, local login override, familiar shutdown and restart options



Why just the **login screen** by itself?

- ▶ Lab environments - short term account life
- ▶ On-demand admin accounts
- ▶ Loaner computers
- ▶ Long term password sync not required
- ▶ Initial onboarding of new user



Better together.

- ▶ Zero touch deployment
- ▶ Use Jamf Connect Login for initial account creation
- ▶ Enable FileVault
- ▶ Menu bar agent for long term password sync
- ▶ Revert to macOS default login for password recovery scenarios
- ▶ Jamf Self Service policy to enable / disable
 - ▶ Admin account
 - ▶ Emergency loaners



```
#!/bin/bash

# REQUIRED VARIABLES
# Put the name of the management account created for Jamf in a prestage enrollment here
jamfManagementAccount=jamfManagement

# Declare variable for JamfConnectUsers
JamfConnectUserCount=0

# Get a list of all users on the machine who have a password. For each user check to see if
# the user is named after the Jamf Management Account or the _mbsetupuser

####NOTE: That second thing may not be required; my setup of Parallels might have given the
# _mbsetupuser a password when it really didn't need one...
####NOTE: You may want to modify this to add any additional programatically created
# local admin accounts you create in your environment.

for user in $(dscl . list /Users Password | awk '$2 != "*" {print $1}');do
  if [[ ("user" != "$jamfManagementAccount") && ("user" != "_mbsetupuser") ]]; then
    # Look in the dscl record for the user and see if there is an entry for OIDCProvider
    # Jamf Connect will add that to the user record when it is migrated or created
    MIGRATESTATUS=$(dscl . -read /Users/$user | grep "OIDCProvider: " | awk '{print $2}')
    # If we didn't get a result, the variable is empty. Thus that user hasn't been migrated.
    if [[ -z $MIGRATESTATUS ]];
    then
      # user is not a jamf connect user
      echo "$user is Not a Jamf Connect User"
    else
      echo "$user is a Jamf Connect user"
      JamfConnectUserCount=$((JamfConnectUserCount+1))
    fi
  fi
done

echo "<result>$JamfConnectUserCount</result>"

exit 0
```

<https://jamf.it/rabbitt-ea>

FileVault and Password Resets

FileVault happens at:

- Intel based processors: EFI Firmware level
- Apple Silicon based processors: macOS in READ ONLY mode

Thus:

- FileVault has no line of sight to a cloud IDP or a domain controller

To reset a forgotten password with FileVault (assuming 1:1 issued machine):

- **Intel and Apple Silicon:**

- After initial account creation, use EA to make Smart Computer Group to determine a Jamf Connect enabled account exists
- Use group to run policy to disable JC Login window
- Give FileVault Personal Recovery Key (PRK) to user to reset in recovery mode

- **Apple Silicon Only Alternative:**

- Use FileVault PRK to start macOS in read/write mode
- Use JC Login with another admin account to reset user password

Computers		
Policies		
▼	● Jamf Connect Login - Disable	Ongoing
1	Run Unix command '/usr/local/bin/authchanger -reset'	
▼	● Jamf Connect Login - Enable	Ongoing
1	Run Unix command '/usr/local/bin/authchanger -reset -JamfConnect'	

Zero Touch Deployment

- Prestage enrollment
 - Skip account creation
 - Config profiles: Login, Menu Bar, Authchanger
 - Enrollment package - JamfConnect.pkg and signed pkg with your branding assets
- Consider combining with Enrollment Customization for security and ease of login



<https://www.jamf.com/blog/zero-touch-deployment-with-jamf-pro-and-jamf-connect/>



English

jamf

Solutions Industries Pricing Resources Contact

Log in


Start Trial

Jamf Blog

January 27, 2021 by Sean Rabbitt

Zero-touch deployment with Jamf Pro and Jamf Connect

This document describes the steps to create a method of onboarding devices using Automated Device Enrollment from Apple (formerly DEP), Jamf Pro, and Jamf Connect to make a customized experience for end users.



Prerequisites: The administrator should follow the instructions in https://docs.jamf.com/jamf-connect/administrator-guide/Before_You_Begin.html to create an application in the organization identity provider and create configuration profiles for Jamf Connect. Administrators should be familiar with smart computer groups, scoping of policies and configuration profiles, and creating installer packages with Jamf Composer or a similar tool.

Before You Begin

Jamf Pro and Jamf Connect can provide a highly customizable user experience. By being highly customizable, administrators are advised to document the experience they want before building out the pieces. For example, administrators may consider:

- Enrollment Customization - On enrollment, end users can experience interactive elements like

SHARE

- f
- tw
- in
-

Remediating Security Events

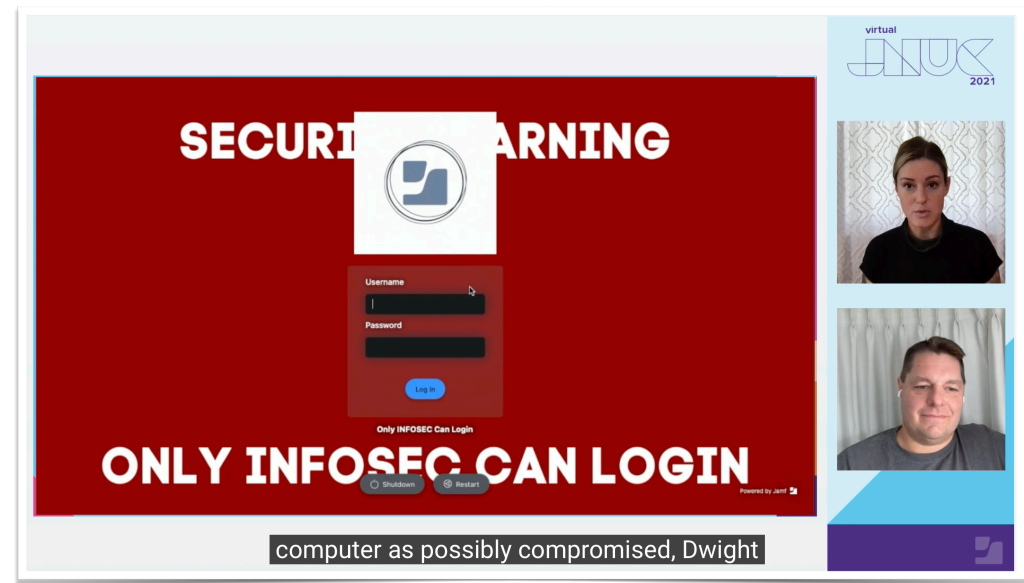
Use Jamf Connect, Jamf Pro, and Jamf Protect to lock down machines when security risks are detected:



<https://www.youtube.com/watch?v=5dQagP7y6Jw>



<https://www.jamf.com/blog/remediating-security-events-jamf-enterprise-management-jnuc2021/>





“But what about macOS Ventura
and the new Platform Single
sign-on (SSO) for macOS?”

Everyone watching the presentation

PITCHFORK ENTHUSIASTS



“We don’t talk about beta.”

But I guarantee more interesting discussions to come.



[Gage Skidmore](#) from Peoria, AZ, United States of America - [Lin-Manuel Miranda & James McAvoy](#)
Lin-Manuel Miranda and James McAvoy speaking at the 2019 San Diego Comic Con International, for "His Dark Materials", at the San Diego Convention Center in San Diego, California. Please attribute to Gage Skidmore if used elsewhere.



Summary

1 | What is Jamf Connect

2 | Jamf Connect Menu Bar Agent

3 | Jamf Connect Login

4 | Jamf Pro and Jamf Connect together

Or, how I learned to stop worrying and love the smart groups



**Join us at JNUC 2022, in
person or virtually**

<https://www.jamf.com/events/jamf-nation-user-conference/2022/>

