Making Apple Products First-Class Citizens

Managing Apple Devices at Scale

THE OHIO STATE UNIVERSITY

osu.edu

Who We Are

Marty Winders

Associate Director, Client Services and Engineering
The Ohio State University - Office of Technology and Digital Innovation

Ray DeMay

Senior Endpoint Engineer
The Ohio State University - Office of Technology and Digital Innovation

Daniel Patenaude

Senior Sales Engineer
Jamf

History

- Digital Flagship led to Shared Jamf
- Device Enrollment Program and Apple School Manager did not exist due to Apple’s Terms and Conditions

History

- 15 different Jamf servers
- ~6,000 Macs
- ~12,000 Mobile Devices
- Some units not managing with anything

Shared Jamf

- A site for each unit
- Three tiers of access:
  - Administrator
  - Limited (custom role with Create, Read, Update, but not Delete)
  - Auditor
- Self-service access management
  - InCommon Grouper
- API account(s)
- Single sign-on
- LDAP

Apple School Manager

To support the autonomy of the sites, admins also have ASM access

Each site has:

- an MDM token for ADE
- A location associated with a VPP token
- An admin with content manager and device enrollment manager roles
- Default Site/MDM Server
  - Enrollment customization in Jamf

Early challenges

Shared service didn’t have a lot of sharing

- Every site had the same kinds of config profiles and policies
- Package upload collisions
- No mechanism to share ideas
- Performance issues

Top Level Changes

To remove duplication and improve Jamf performance, many deployments were moved to the top of the instance

- Self Service applications
- Common configuration profiles
  - CrowdStrike
  - Microsoft
  - Cisco Secure Client
  - BeyondTrust Remote Support
  - Symantec DLP
  - Other common PPPC and system extension profiles

Using Your MDM to Its Fullest

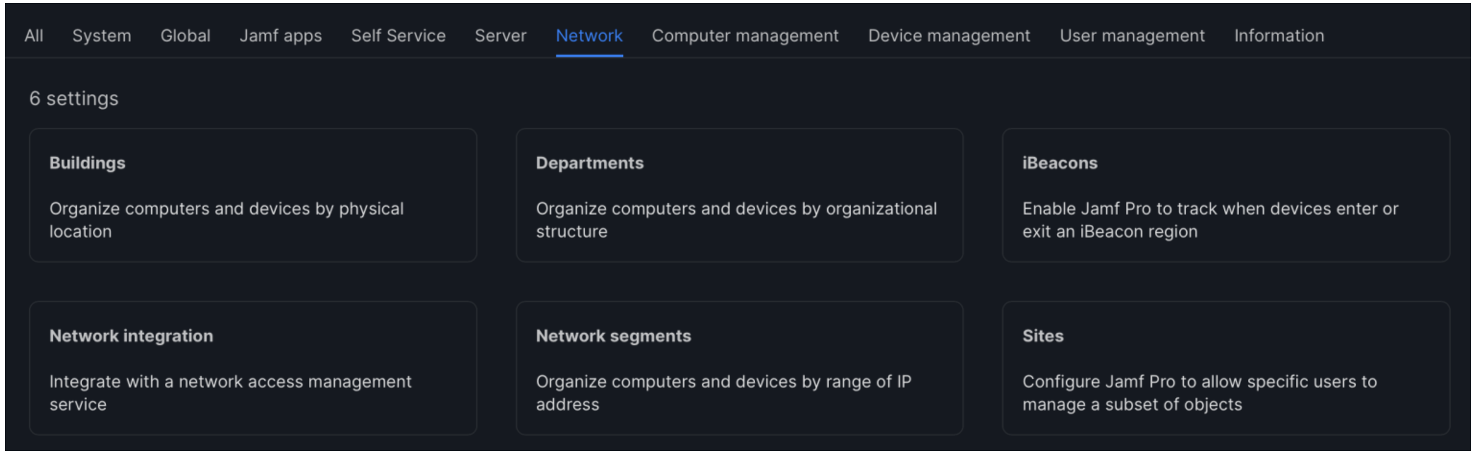
MDM-Agnostic Thoughts

- Don’t be afraid of trying new features
- Managing Macs isn’t like managing Windows
- Use the community
  - Admins in other departments
  - Macadmins Slack
  - Third-party/open-source tools

Jamf Sites

Sites are for *delegated access*. They are not to organize devices, but to control who can see and change them. Jamf has many other ways to organize devices.

- Buildings
- Departments
- Network segments
- Smart groups
  - Prestage enrollments
  - Extension attributes



6 settings

Buildings
Organize computers and devices by physical location

Departments
Organize computers and devices by organizational structure

iBeacons
Enable Jamf Pro to track when devices enter or exit an iBeacon region

Network integration
Integrate with a network access management service

Network segments
Organize computers and devices by range of IP address

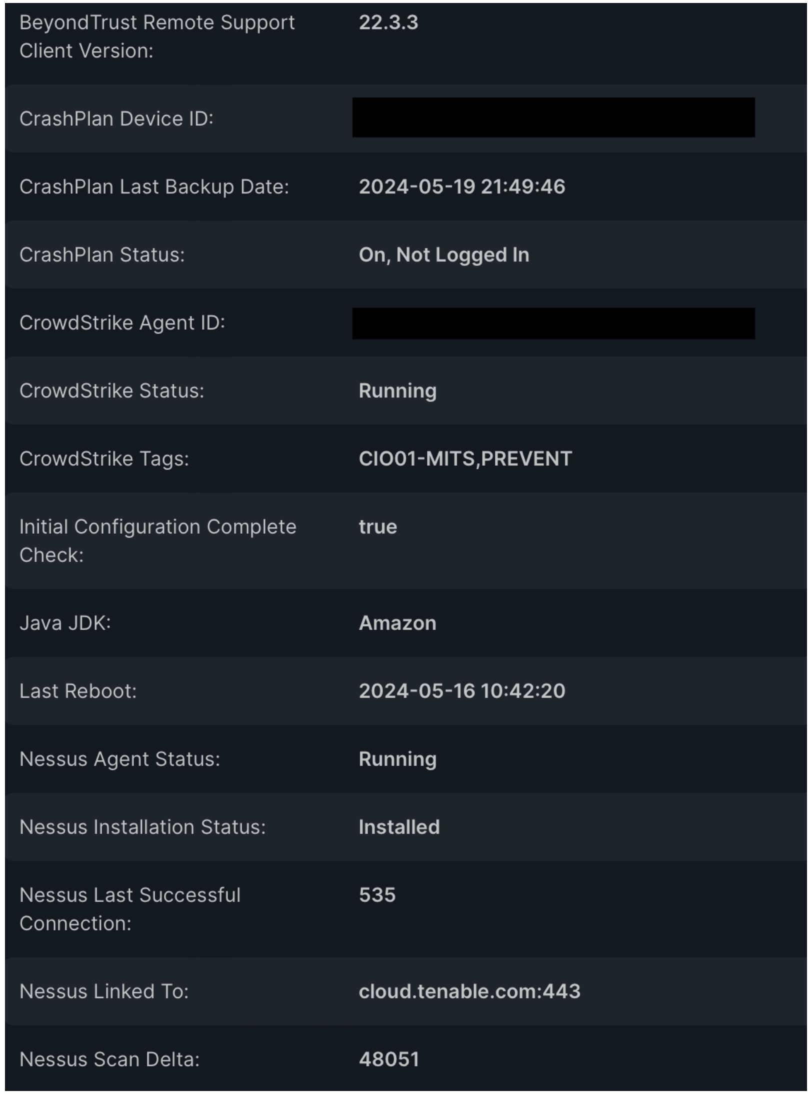
Sites
Configure Jamf Pro to allow specific users to manage a subset of objects

Site-level vs. Full Jamf Pro level

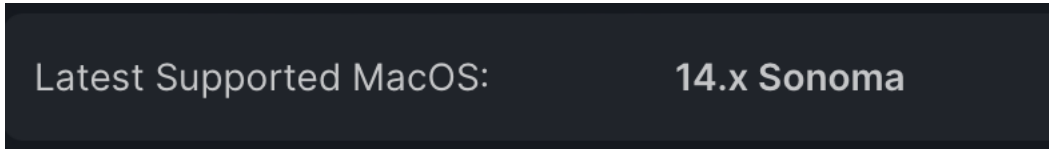
In our shared model, the site admins are basically given full reign over their site, but there are some considerations

- Configuration profiles used by everyone go to the top to lower total number of payloads
- Packages should be named with a unit prefix if nobody else should use it
- Don’t deploy bad policies (all computers, ongoing frequency)
- Extension attributes have to be approved and uploaded by service owner

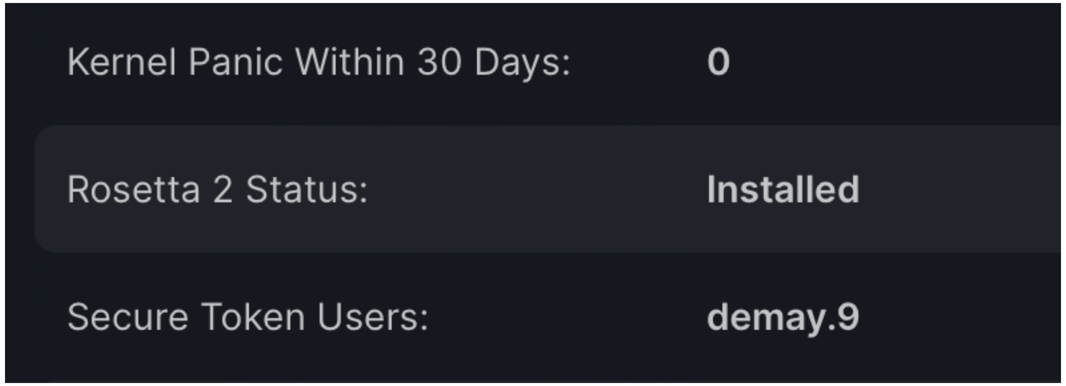
Extension Attributes



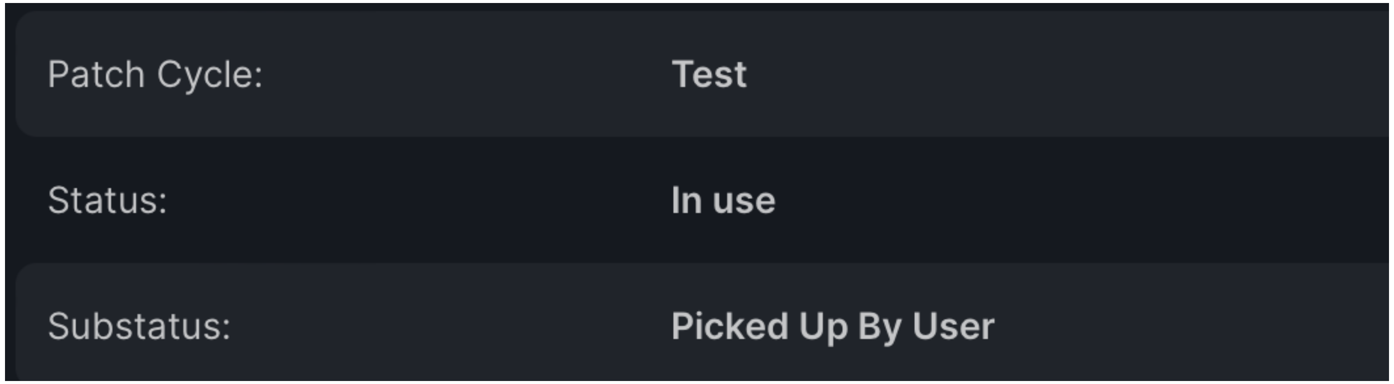
BeyondTrust Remote Support Client Version:	22.3.3
CrashPlan Device ID:	[redacted]
CrashPlan Last Backup Date:	2024-05-19 21:49:46
CrashPlan Status:	On, Not Logged In
CrowdStrike Agent ID:	[redacted]
CrowdStrike Status:	Running
CrowdStrike Tags:	CIO01-MITS,PREVENT
Initial Configuration Complete Check:	true
Java JDK:	Amazon
Last Reboot:	2024-05-16 10:42:20
Nessus Agent Status:	Running
Nessus Installation Status:	Installed
Nessus Last Successful Connection:	535
Nessus Linked To:	cloud.tenable.com:443
Nessus Scan Delta:	48051



Latest Supported MacOS:	14.x Sonoma



Kernel Panic Within 30 Days:	0
Rosetta 2 Status:	Installed
Secure Token Users:	demay.9



Patch Cycle:	Test
Status:	In use
Substatus:	Picked Up By User

MDM APIs

Don’t be afraid of using APIs, but be careful

- Inventory management/CMDB
- Extension attributes
- Integrations
- Security concerns with scripts
  - API proxy with Azure Functions or AWS Lambda
- Jamf recommendations
  - https://developer.jamf.com/developer-guide/docs/jamf-pro-api-scalability-best-practices

Additional Tools and Integrations

- ServiceNow
- Aruba ClearPass
- Autopkg(r)
- Microsoft Entra Device Compliance
- Webhooks
  - Teams and Slack

Don’t try to manage Apple devices like Windows devices

Active Directory

Macs can utilize AD resources without binding.

- Jamf ADCS Connector, SCEP
- NoMAD, Jamf Connect, XCreds
- Kerberos SSO Extension

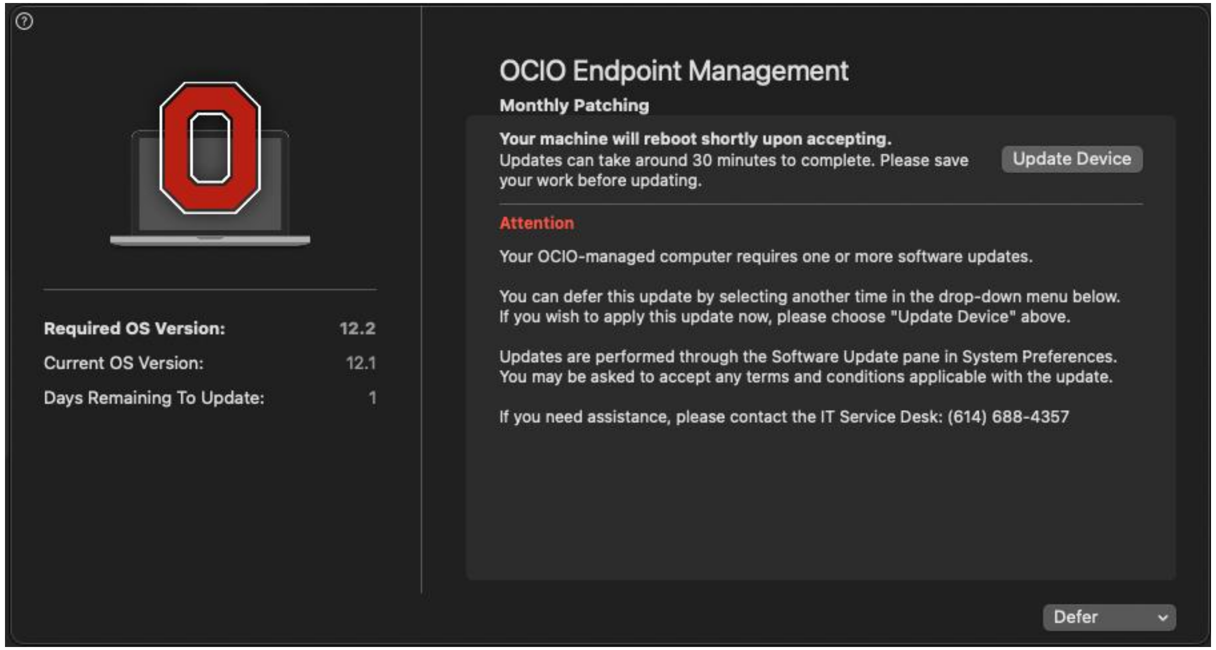
This includes computer labs!

OS Updates

Apple wants the user to be in charge, but management options are getting there.

- Declarative Device Management (MacOS 14/iOS 17)
- Nudge
  - https://github.com/macadmins/nudge
- super
  - https://github.com/Macjutsu/super
- erase-install
  - https://github.com/grahampugh/erase-install

Nudge



OCIO Endpoint Management

Monthly Patching

Your machine will reboot shortly upon accepting.
Updates can take around 30 minutes to complete. Please save your work before updating.

Attention

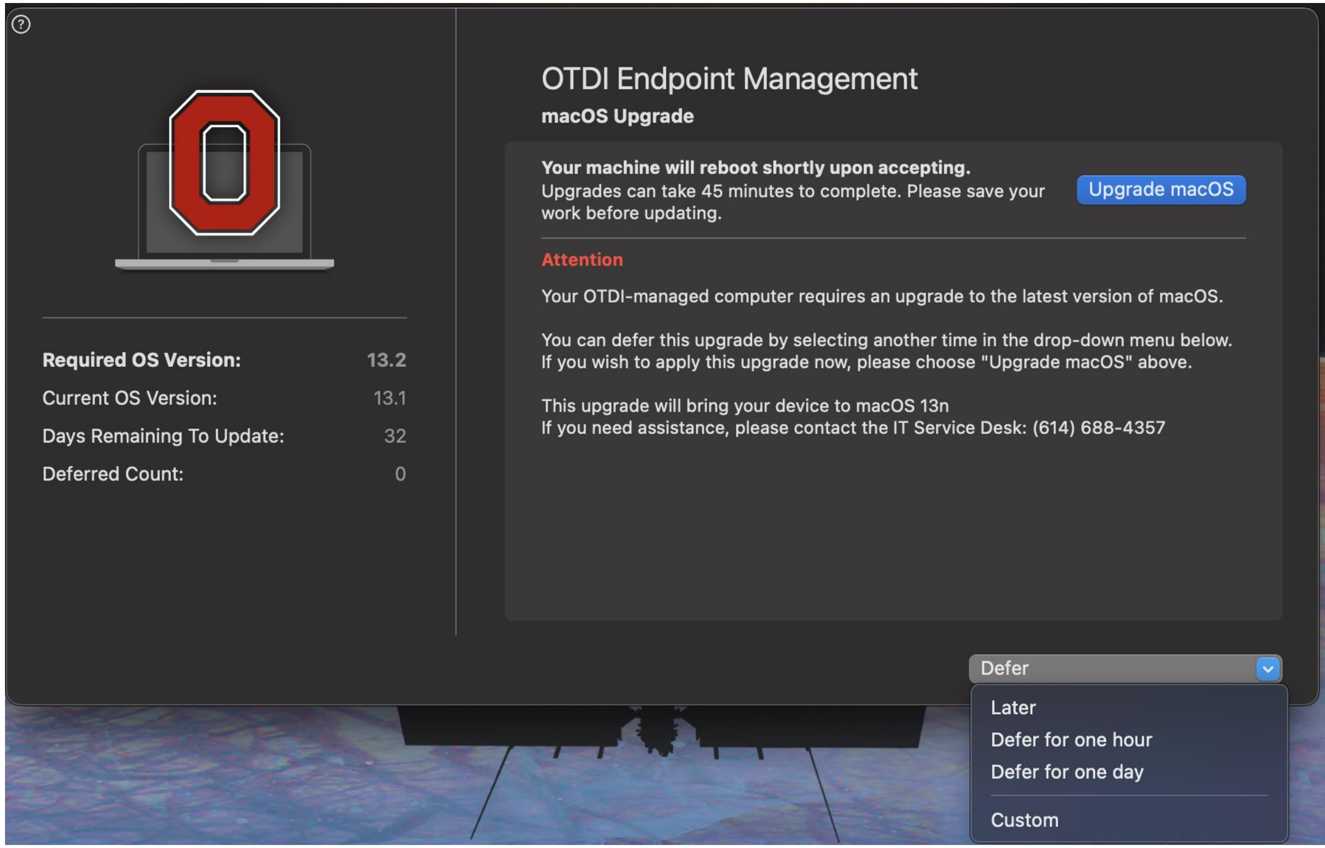
Your OCIO-managed computer requires one or more software updates.

You can defer this update by selecting another time in the drop-down menu below.
If you wish to apply this update now, please choose "Update Device" above.

Updates are performed through the Software Update pane in System Preferences.
You may be asked to accept any terms and conditions applicable with the update.

If you need assistance, please contact the IT Service Desk: (614) 688-4357

Required OS Version:	12.2
Current OS Version:	12.1
Days Remaining To Update:	1



OTDI Endpoint Management

macOS Upgrade

Your machine will reboot shortly upon accepting.
Upgrades can take 45 minutes to complete. Please save your work before updating.

Attention

Your OTDI-managed computer requires an upgrade to the latest version of macOS.

You can defer this upgrade by selecting another time in the drop-down menu below.
If you wish to apply this upgrade now, please choose "Upgrade macOS" above.

This upgrade will bring your device to macOS 13n
If you need assistance, please contact the IT Service Desk: (614) 688-4357

Required OS Version:	13.2
Current OS Version:	13.1
Days Remaining To Update:	32
Deferred Count:	0

Using `actionButtonPath` to call Jamf policy URI

OS Updates

- Don’t try to force a “patch Tuesday”
- Test/Pilot/Production waves
- Get non-IT early adopters for major upgrades
- Have a documented exception process

Mac Deployments

Don’t think in terms of “imaging” for Macs.

- Zero-touch enrollment
- Mature self-service catalog
- Friendly user setup
  - DEPNotify
  - Setup Your Mac
  - Jamf MacOS Onboarding
- Pre-provisioning (white glove) needed?
  - Secure token is the big concern

Future Ideas

Shared Jamf Improvements

- Package upload changes
- Smart group and policy auditing
- Better communication with partners
- Automation
- Jamf App Catalog

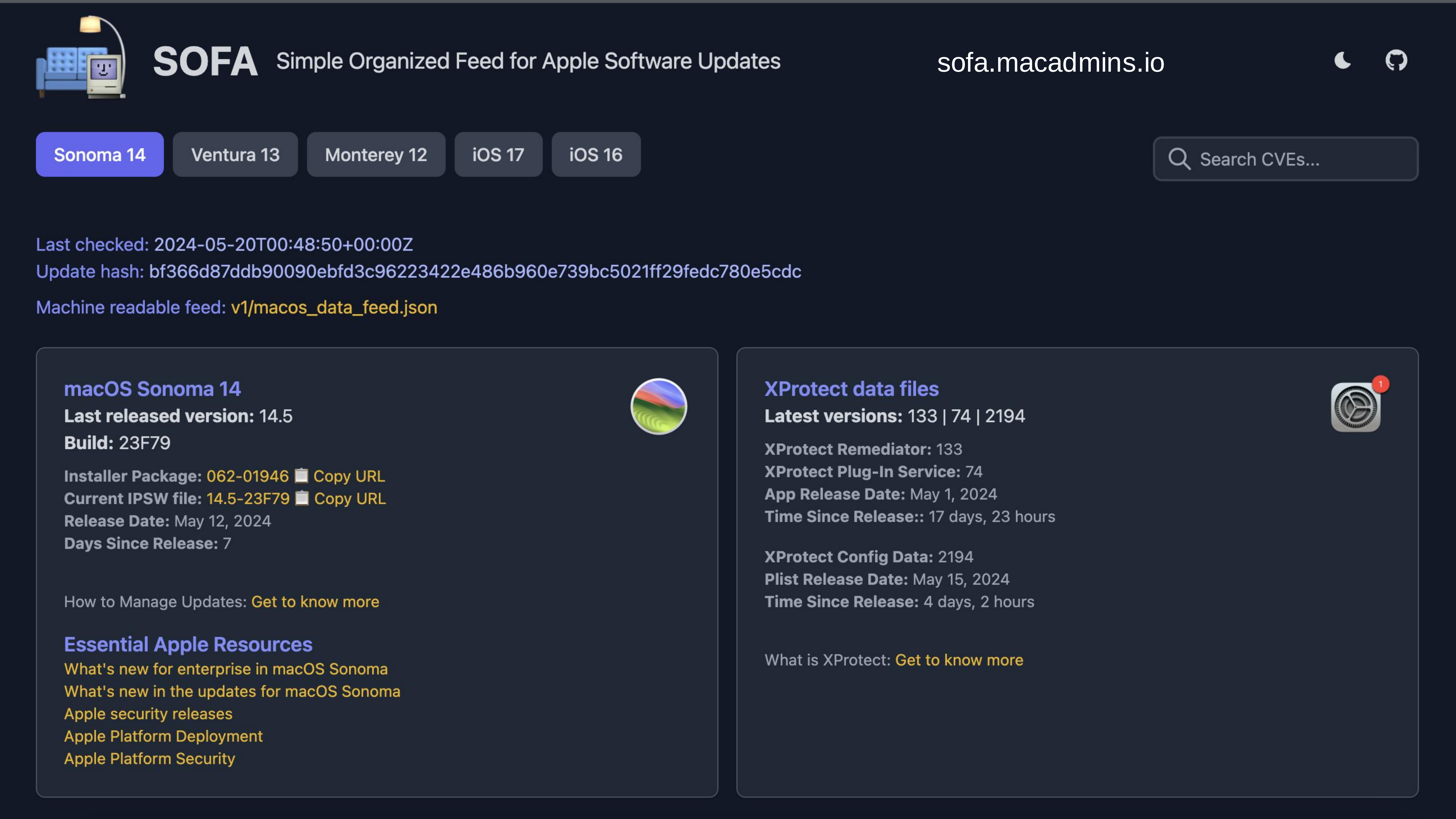
APIs and Automation

Jamf APIs + Azure Functions

Current work is automating Nudge deployments using remote JSON

Steal my ideas!

Ray’s GitHub



SOFA Simple Organized Feed for Apple Software Updates

sofa.macadmins.io

Last checked: 2024-05-20T00:48:50+00:00Z
Update hash: bf366d87ddb90090ebfd3c96223422e486b960e739bc5021ff29fedc780e5cdc

Machine readable feed: v1/macos_data_feed.json

macOS Sonoma 14

Last released version: 14.5
Build: 23F79

Installer Package: 062-01946 📋 Copy URL
Current IPSW file: 14.5-23F79 📋 Copy URL
Release Date: May 12, 2024
Days Since Release: 7

How to Manage Updates: Get to know more

Essential Apple Resources

What's new for enterprise in macOS Sonoma
What's new in the updates for macOS Sonoma
Apple security releases
Apple Platform Deployment
Apple Platform Security

XProtect data files

Latest versions: 133 | 74 | 2194

XProtect Remediator: 133
XProtect Plug-In Service: 74
App Release Date: May 1, 2024
Time Since Release:: 17 days, 23 hours

XProtect Config Data: 2194
Plist Release Date: May 15, 2024
Time Since Release: 4 days, 2 hours

What is XProtect: Get to know more

JNUC
Nashville
2024

Meet us in Music City!

The 15th Annual Jamf Nation User Conference (JNUC) is headed to Nashville, Tuesday, October 1 - Thursday, October 3, 2024.

Questions?