

Jamf Nation Roadshow

Security & Business Intelligence 101

Zentral Pro Services GmbH & Co. KG

About Me



Henry Stamerjohann
Client Platform Engineer
Zentral Pro Services GmbH & Co. KG

Zentral Pro Services

Jamf Integrator & Professional Services

Apple Platform Engineering (Consultancy)

Research & Development Partner (B2B, Enterprise)

www.zentral.pro

What do you use ?

Jamf Pro Cloud

Jamf Dashboard

Jamf Connect

Jamf API

Proposition - next steps



- 1.** Inventory overview > optimize
- 2.** Endpoint security > enhance
- 3.** Identity validation > extend

1. Inventory



Jamf Pro Inventar

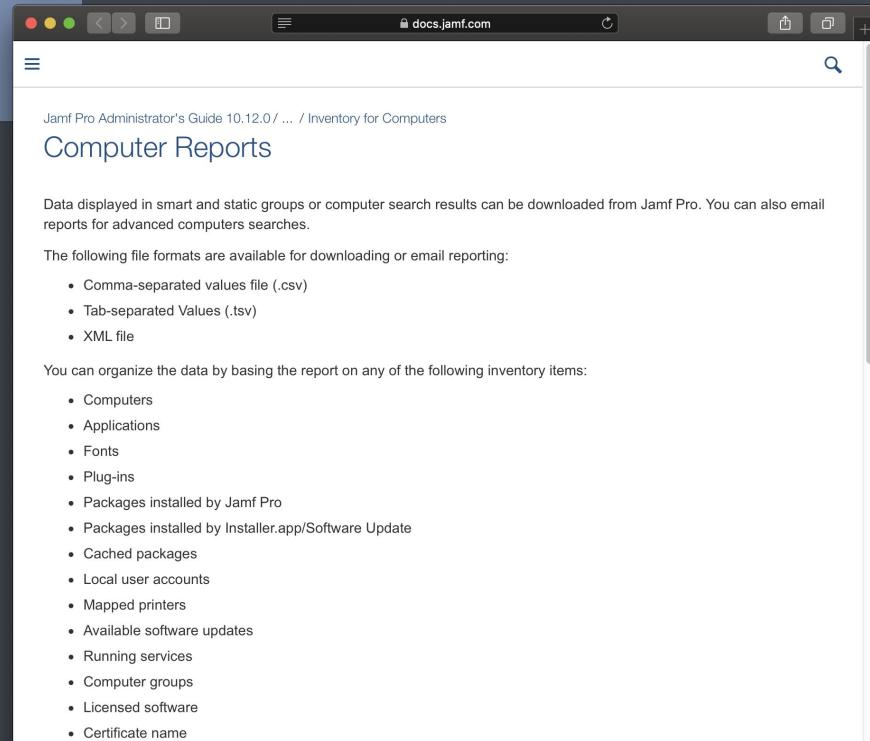


Current state

Search, Smart Groups

History (Jamf & MDM Events)

Reporting



The screenshot shows a web browser window displaying the Jamf Pro Administrator's Guide. The URL is docs.jamf.com. The page title is "Computer Reports". The content discusses data organization based on inventory items like Computers, Applications, Fonts, etc. It also mentions the ability to download data in CSV, TSV, or XML formats.

Inventory items:

- Computers
- Applications
- Fonts
- Plug-ins
- Packages installed by Jamf Pro
- Packages installed by Installer.app/Software Update
- Cached packages
- Local user accounts
- Mapped printers
- Available software updates
- Running services
- Computer groups
- Licensed software
- Certificate name

The data is displayed in alphanumeric order by the selected inventory item.

Creating Reports for Smart and Static Groups or Simple Computer Searches

1. Log in to Jamf Pro.
2. Click **Computers** at the top of the page.
3. Do one of the following:
 - View computer group memberships. For more information, see [Smart Groups or Static Groups](#)
 - View simple or advanced computer search results. For more information, see [Simple Computer Searches or Advanced Computer Searches](#)

Jamf Reports

1

Computers > Advanced Computer Search >

Inventory report

Search Criteria Display Reports

FILE FORMAT File format to export the report
Comma-Separated Values (.csv) ▾

INVENTORY ITEM Choose the inventory item on which to base your results
Computers

Download Report

Email Reporting

Configure Email Reports

2

Download Report

Email Reporting

EMAIL RECIPIENTS Email addresses, separated by commas or new lines. Required for sending email reports
client-platform-team@example.com

SUBJECT Subject line of email
Jamf Pro monthly

BODY Message to appear in the body of email
Hi, attached is the monthly inventory report (CSV format)

Send Email Report

Schedule automatic email reports

Jamf Reports

2

Download Report

Email Reporting

EMAIL RECIPIENTS Email addresses, separated by commas or new lines. Required for sending email reports

SUBJECT Subject line of email

BODY Message to appear in the body of email

Send Email Report

Schedule automatic email reports

3

BODY Message to appear in the body of email

Send Email Report

Schedule automatic email reports

FREQUENCY Frequency at which the reports are calculated and sent

Daily

Days per week

1st day of every month

1st Monday of every month

AT (i) Time is displayed in Coordinated Universal Time (UTC)

Report processing



Display (Inventory overview)

Share (Stakeholder)

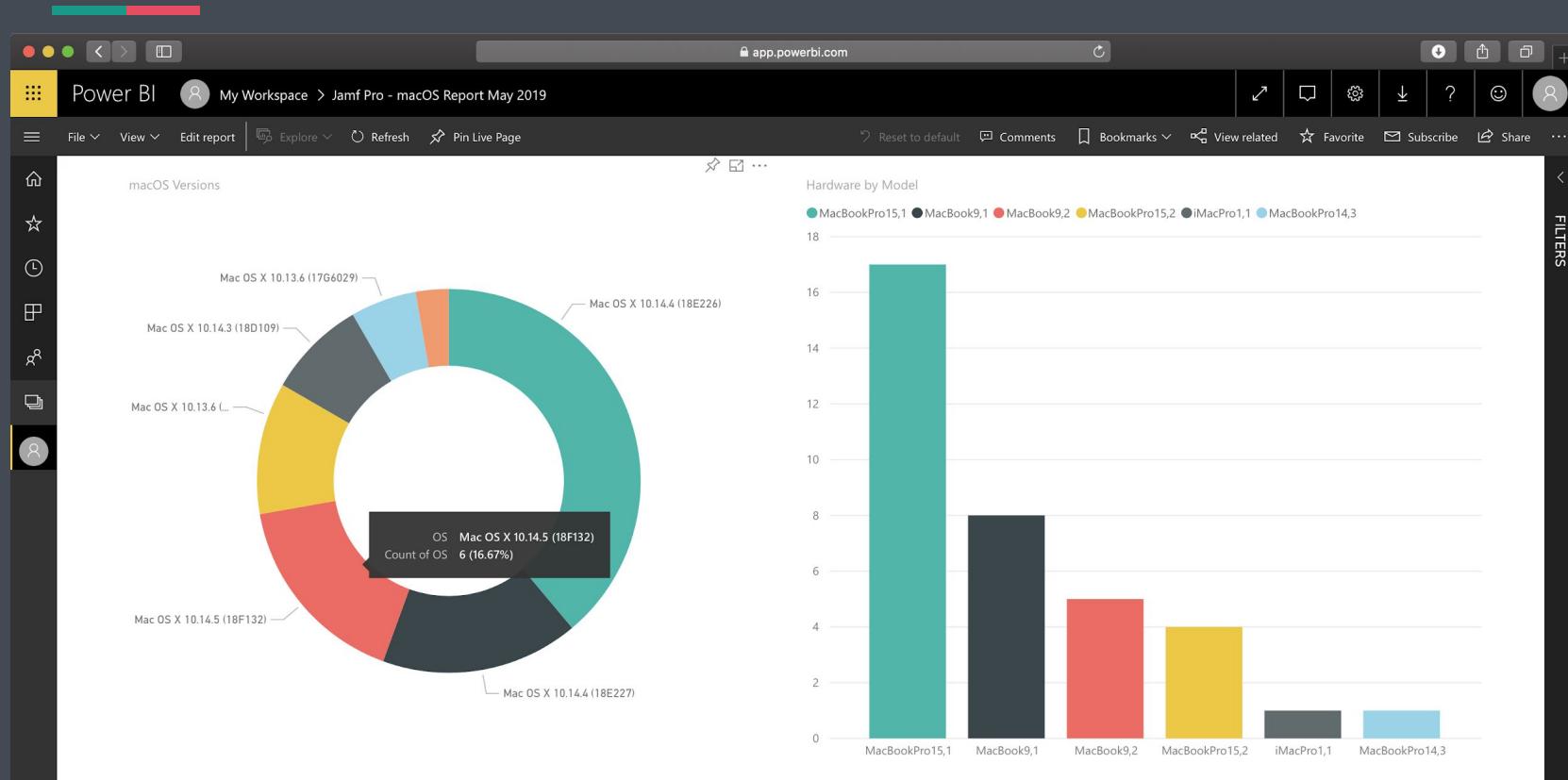
Visualize

Extended analyzation

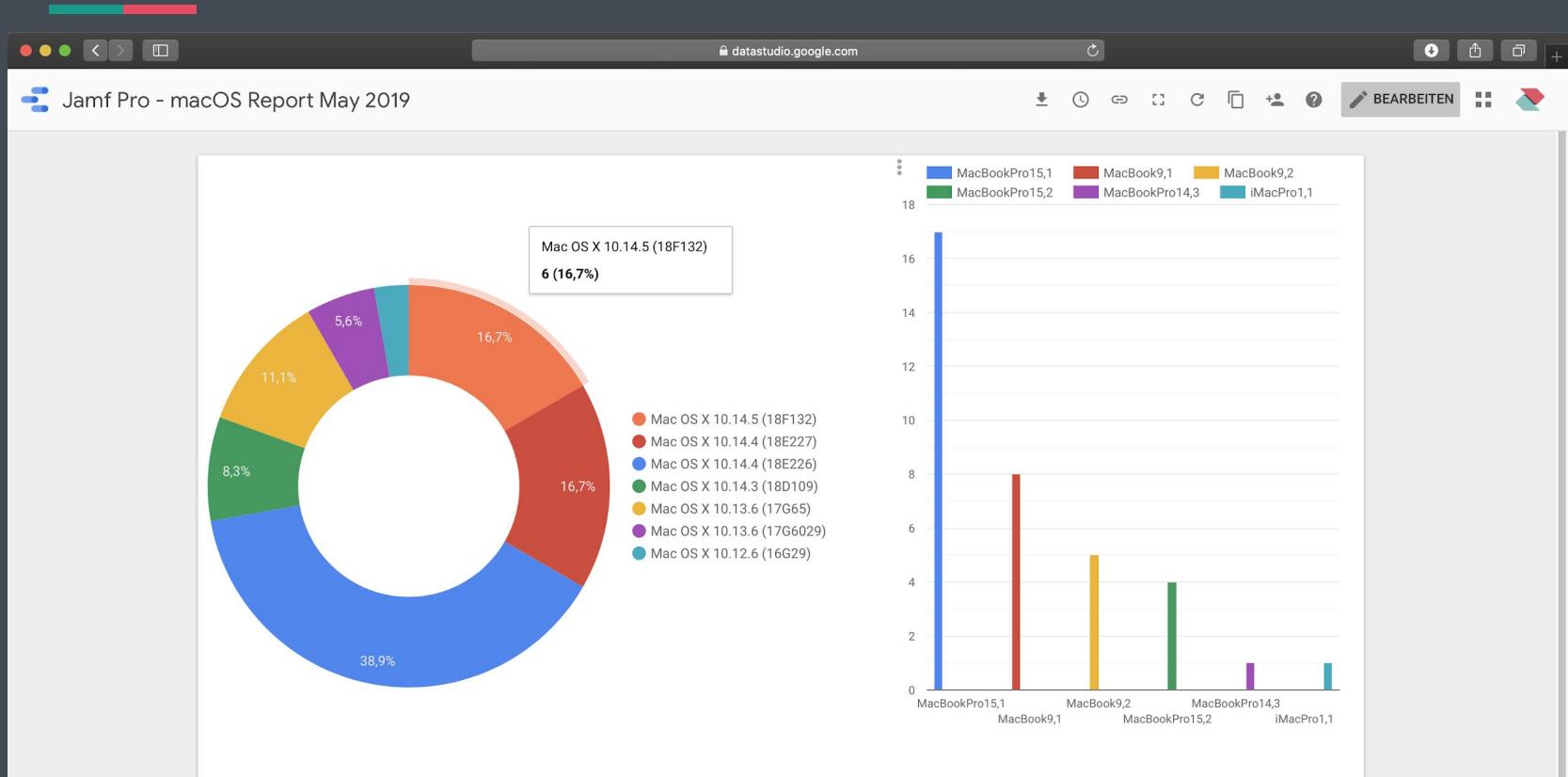
(Cloud services)



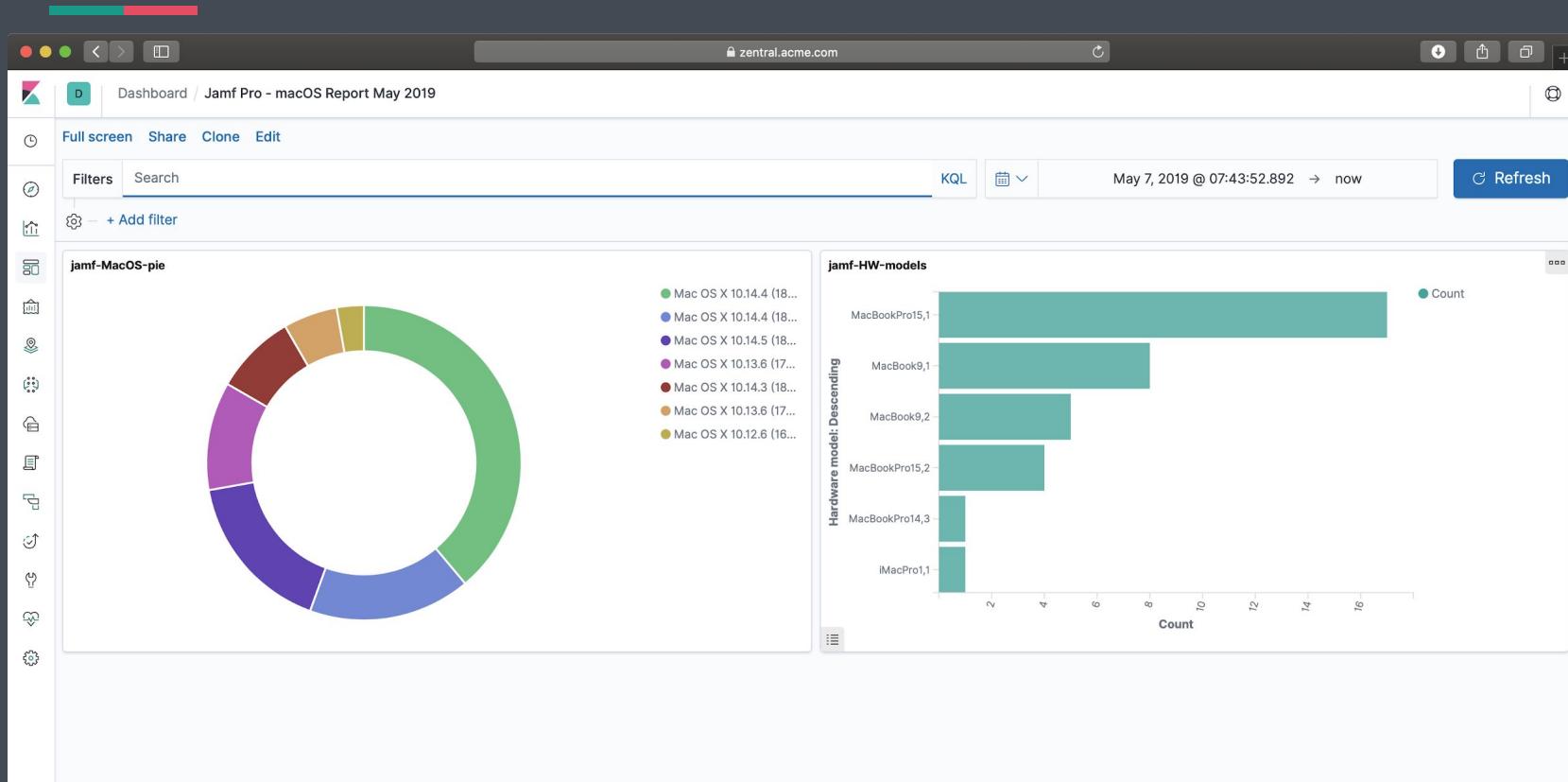
Microsoft Azure / Power BI



Google Data Studio



Elastic Stack Kibana (CSV import)



Jamf Pro API & Webhooks

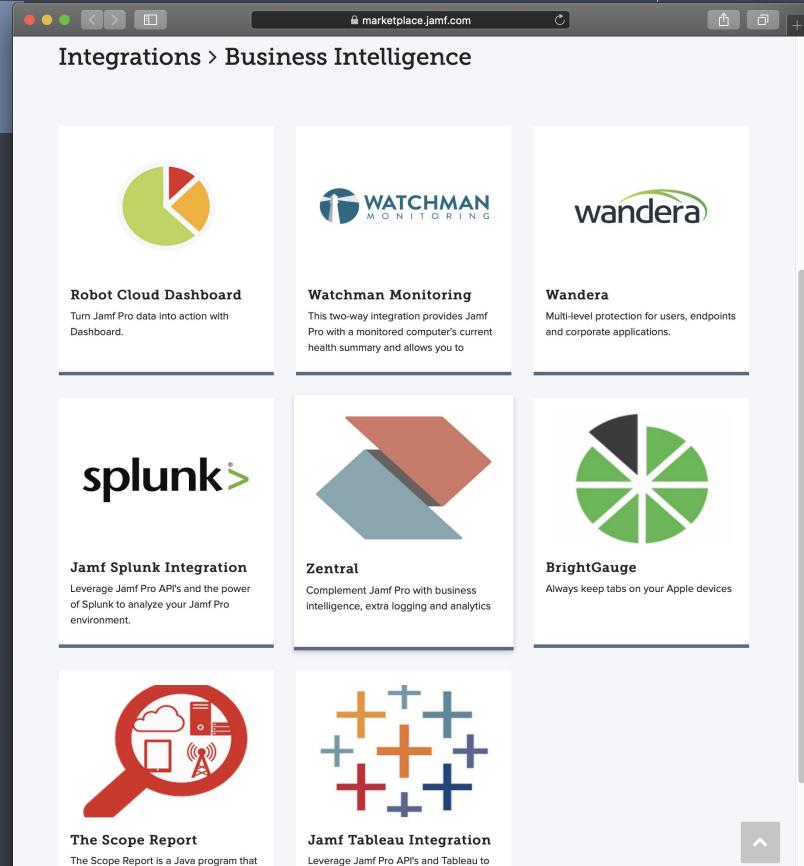


Query (REST API)

Jamf Events (Webhooks)

Filter

Analyse



The screenshot shows a web browser displaying the Jamf Marketplace at marketplace.jamf.com. The page is titled "Integrations > Business Intelligence". It features six integration cards arranged in two rows of three:

- Robot Cloud Dashboard**: Turn Jamf Pro data into action with Dashboard.
- Watchman Monitoring**: This two-way integration provides Jamf Pro with a monitored computer's current health summary and allows you to
- wandera**: Multi-level protection for users, endpoints and corporate applications.
- splunk®**: Jamf Splunk Integration. Leverage Jamf Pro API's and the power of Splunk to analyze your Jamf Pro environment.
- Zentral**: Complement Jamf Pro with business intelligence, extra logging and analytics.
- BrightGauge**: Always keep tabs on your Apple devices
- The Scope Report**: The Scope Report is a Java program that
- Jamf Tableau Integration**: Leverage Jamf Pro API's and Tableau to

<https://marketplace.jamf.com>

Data Warehouse (History)

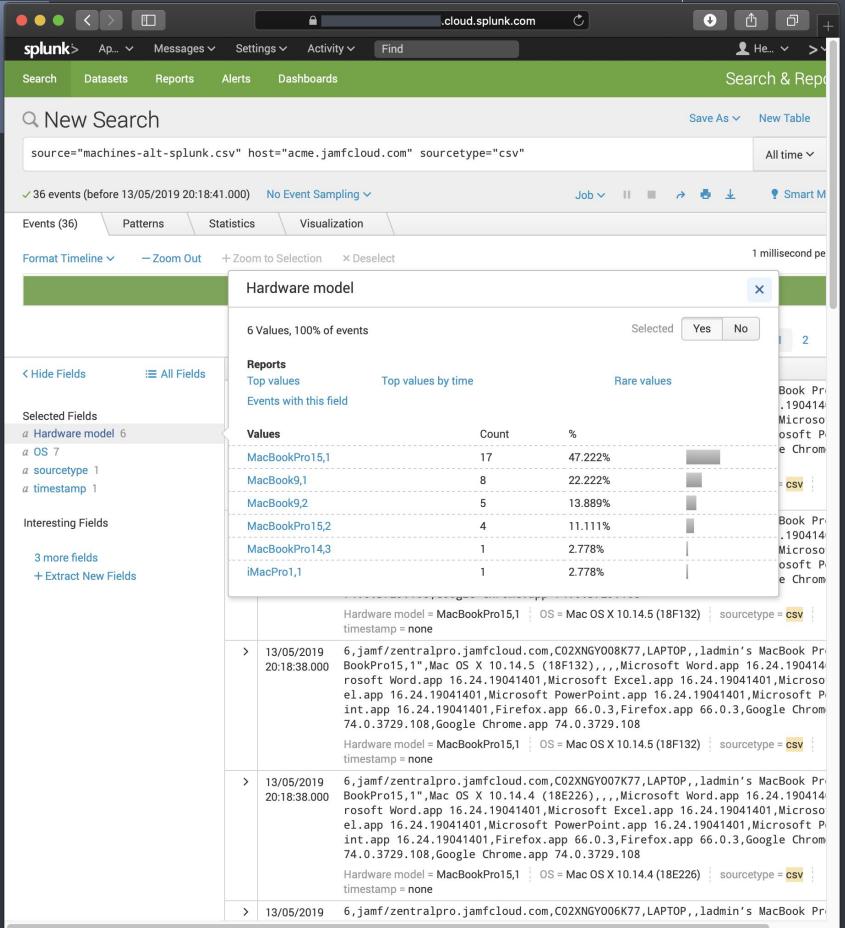


Data processing

Event-store

Examine

Historical analysis



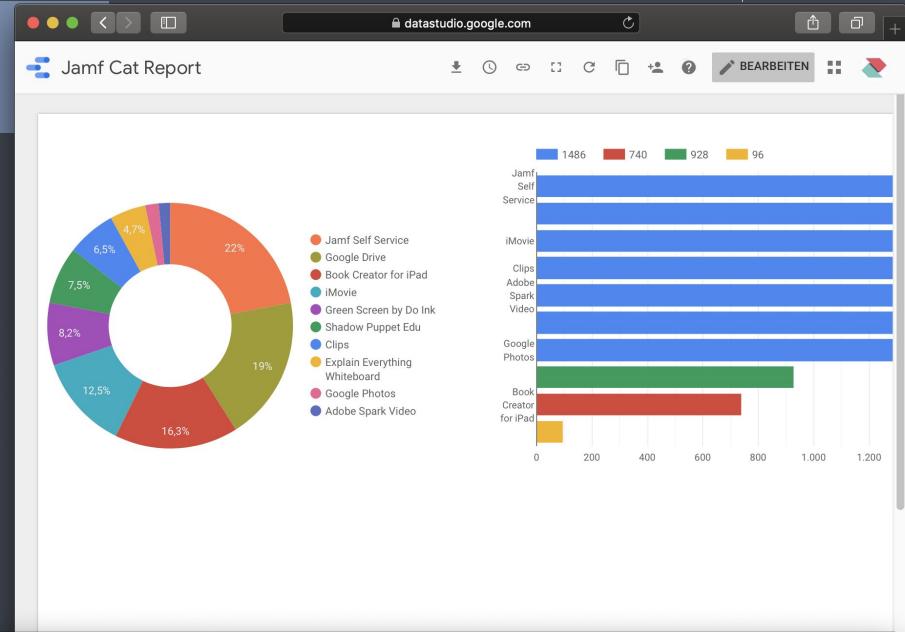
Example #1 (Cat Report for iOS)



Cat-Report (iOS catalog info)

Python tool

github.com/nstrauss/jamf-cat-report



example.csv															Open with Numbers	Import
id	name	main_category	self_service_cat1	self_service_cat2	self_service_cat3	self_service_cat4	self_service_cat5	featured	installed_count	used_licenses	remaining_licenses	total_licenses	price	latest_release	average_rating	bundle_id
786	Jamf Self Service	Productivity	Productivity	Utilities	None	None	None	FALSE	6588	6514	1486	8000	0	2018-11-16T20:41:15Z	2.5	com.jamfsoft.jamf-self-service
580	Google Drive	Productivity	3rd-5th Grade	6th-8th Grade	Productivity	None	None	TRUE	5699	6514	1486	8000	0	2019-04-22T14:50:59Z	5	com.google.drive
953	iMovie	Video Editing	3rd-5th Grade	6th-8th Grade	Early Childhood	K-2nd Grade	Video Editing	TRUE	3736	6514	1486	8000	0	2018-11-07T18:10:56Z	4	com.apple.imovie
955	Green Screen by Do Ink	Video Editing	3rd-5th Grade	6th-8th Grade	Early Childhood	K-2nd Grade	Video Editing	FALSE	2468	5642	928	6570	2.99	2019-01-24T19:30:03Z	3.5	com.doink.green-screen
1387	Clips	Video Editing	3rd-5th Grade	6th-8th Grade	Creativity	Early Childhood	K-2nd Grade	FALSE	1932	6514	1486	8000	0	2019-04-02T17:00:10Z	3.5	com.apple.clips
523	Adobe Spark Video	Video Editing	3rd-5th Grade	6th-8th Grade	Digital Storytelling	Video Editing	None	FALSE	447	6514	1486	8000	0	2019-04-09T21:50:55Z	4.5	com.adobe.spark-video
1016	Explain Everything Whiteboard	Digital Storytelling	3rd-5th Grade	6th-8th Grade	Digital Storytelling	Productivity	None	TRUE	1417	2579	96	2675	13.99	2019-05-01T07:27:43Z	4.5	com.morrisco.explain-everything
1007	Shadow Puppet Edu	Digital Storytelling	3rd-5th Grade	6th-8th Grade	Digital Storytelling	K-2nd Grade	Video Editing	FALSE	2260	6514	1486	8000	0	2019-01-14T17:23:45Z	4.5	com.shadowpuppet.educational
1169	Book Creator for iPad	Digital Storytelling	3rd-5th Grade	6th-8th Grade	Digital Storytelling	Early Childhood	K-2nd Grade	FALSE	4869	5830	740	6570	4.99	2019-04-04T20:08:14Z	4	com.redjumpe.book-creator-ipad
513	Google Photos	Photo Editing	3rd-5th Grade	6th-8th Grade	Photo Editing	Productivity	None	FALSE	533	6514	1486	8000	0	2019-05-01T18:03:42Z	5	com.google.photos

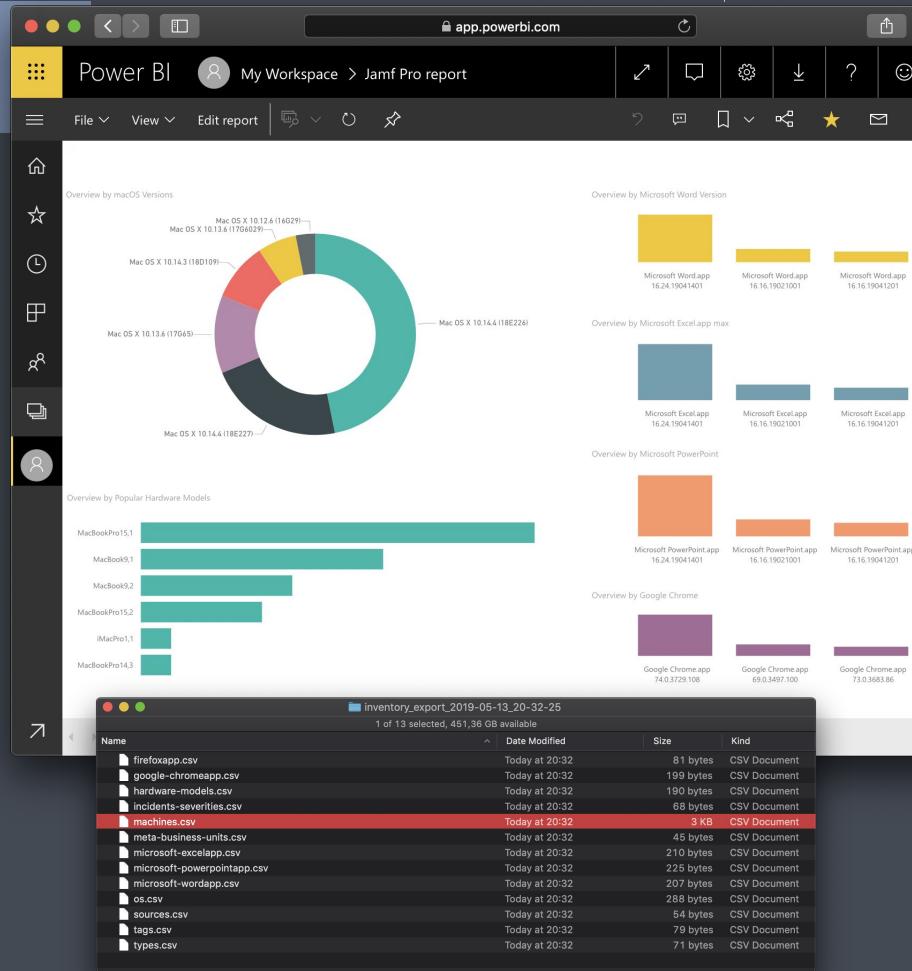
Example #2 (Zentral drilldown)

Report Builder^(advanced)

Web Service / API

CSV or XLSX

github.com/zentralopensource/zentral



Summary (Inventory overview)



Use automatic reports

Visualize inventory

Jamf Marketplace

Cloud services for sharing

2. Endpoint security



Apple (macOS Security)

FileVault, Gatekeeper, Xprotect, MRT

T2 Chip (SEP), System Integrity Protection (SIP)

MDM Kext Approval (UAKEL) / Whitelisting (MDM)

New in Mojave (10.14):

Privacy Preferences Policy Control (PPPC)

& Transparency Consent and Control (TCC)

macOS hardening (guides)



CIS (Apple OS Benchmark)

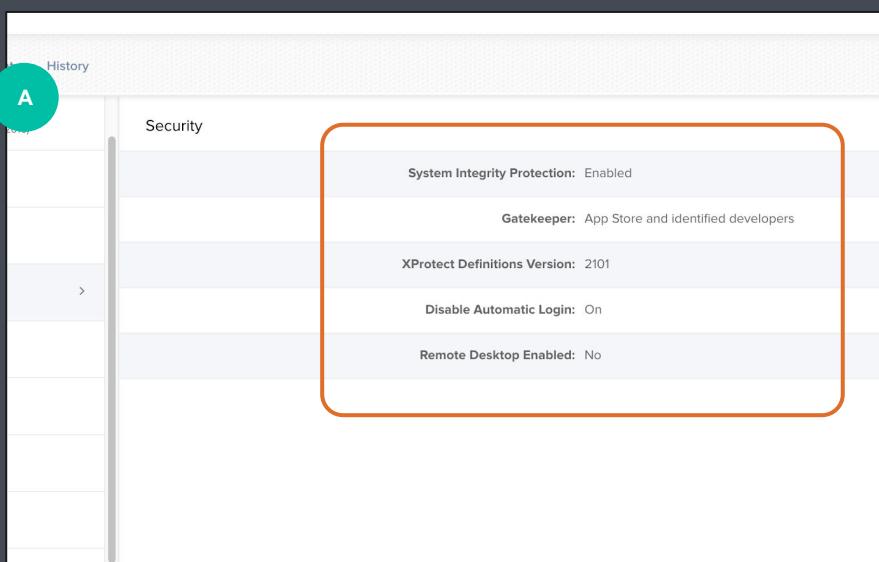
NIST (SP 800-179)

Community resources
github.com/drduh

Category	Setting Name	Description	Security Baseline		
			Standalone	Managed	SSLF
Access Control	all_files_in_a_users_home_dir_are_owned_by_the_user	Changes all files in a user's home directory and subdirectories to be owned by that user.	All files and folders belong to their respective users.	All files and folders belong to their respective users.	All files and folders belong to their respective users.
Access Control	check_system_integrity_protection_status	Checks to see if the System Integrity Protection (SIP) subsystem is enabled.	System Integrity Protection is enabled	System Integrity Protection is enabled	System Integrity Protection is enabled
Access Control	enable_gatekeeper	Enables the security assessment policy (Gatekeeper) subsystem.	Security assessment policy subsystem is enabled.	Security assessment policy subsystem is enabled.	Security assessment policy subsystem is enabled and allows software downloaded from the App Store.
Access Control	files_in_home_dir_group_owned_by_owners_group	Changes all files in a user's home directory and subdirectories to be part of a group that the user belongs to.	All files and folders belong to an appropriate group.	All files and folders belong to an appropriate group.	All files and folders belong to an appropriate group.
Access Control	set_umask	Prevents newly created files from being overly permissive.	Newly created files should only be writable by the owner. Non-group members should not have any access.	Newly created files should only be writable by the owner. Non-group members should not have any access.	Newly created files should only be writable by the owner. Non-group members should not have any access.
Access Control	user_home_directories_permissions	Sets permissions on all user home directories to 700.	Permissions for all user home directories are 700.	Permissions for all user home directories are 700.	Permissions for all user home directories are 700.
Auditing	audit_log_max_file_size	Sets a maximum file size for each log file.	In the "/etc/security/audit_control" file, the log file size property must be set to 80 Megabytes.	In the "/etc/security/audit_control" file, the log file size property must be set to 80 Megabytes.	In the "/etc/security/audit_control" file, the log file size property must be set to 80 Megabytes.
Auditing	audit_log_retention	Sets a maximum file age to ensure effective audit log retention.	In the "/etc/security/audit_control" file, audit log files must be set to expire after 30 days and 5 Gigabytes.	In the "/etc/security/audit_control" file, audit log files must be set to expire after 30 days and 5 Gigabytes.	In the "/etc/security/audit_control" file, audit log files must be set to expire after 30 days and 5 Gigabytes.
Auditing	do_not_send_diagnostic_info_to_apple	Disables automatic sending of diagnostic information to Apple.	Automatic diagnostic reporting is disabled.	Automatic diagnostic reporting is disabled.	Automatic diagnostic reporting is disabled.
Auditing	set_audit_control_flags	Sets a number of flags in the audit_control file to ensure effective auditing.	In the "/etc/security/audit_control" file, the flags property must be set to "lo.ad-all.fd.fm".	In the "/etc/security/audit_control" file, the flags property must be set to "lo.ad-all.fd.fm".	In the "/etc/security/audit_control" file, the flags property must be set to "lo.ad-all.fd.fm".

[License](#) [Baselines](#) [Unchanged Defaults](#) [Legend](#)

Jamf Pro (macOS Security)



A

History

Security

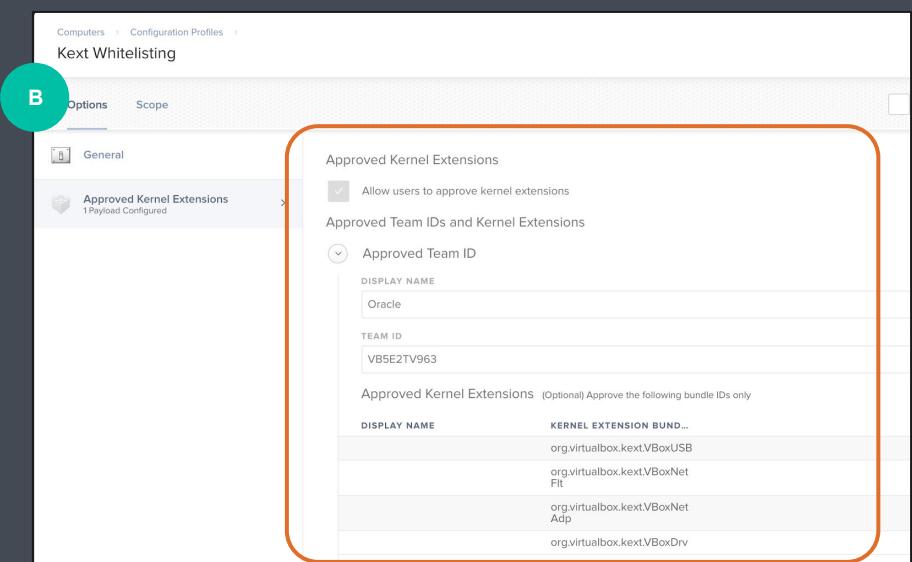
System Integrity Protection: Enabled

Gatekeeper: App Store and identified developers

XProtect Definitions Version: 2101

Disable Automatic Login: On

Remote Desktop Enabled: No



B

Computers > Configuration Profiles > Kext Whitelisting

General

Approved Kernel Extensions

Allow users to approve kernel extensions

Approved Team IDs and Kernel Extensions

Approved Team ID

DISPLAY NAME: Oracle

TEAM ID: VB5E2TV963

Approved Kernel Extensions (Optional) Approve the following bundle IDs only

DISPLAY NAME	KERNEL EXTENSION BUND...
org.virtualbox.kext.VBoxUSB	
org.virtualbox.kext.VBoxNet	
org.virtualbox.kext.VBoxNet	
org.virtualbox.kext.VBoxDrv	

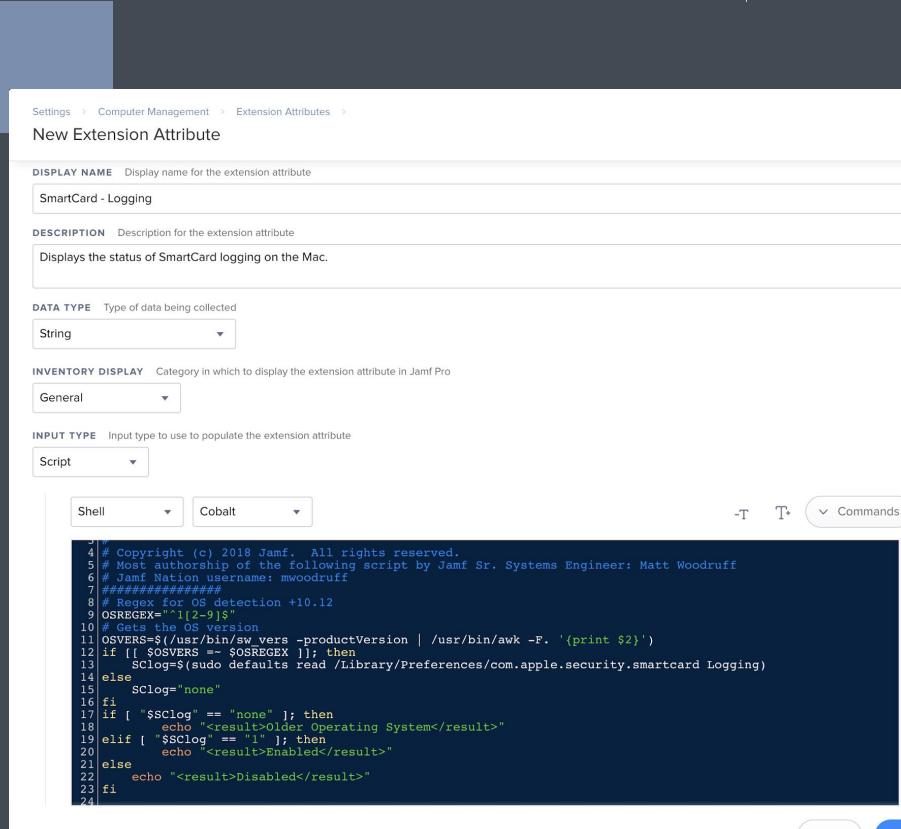
Extension Attributes

Extended collection

Change control (Script)

Smart groups

Extra source for report

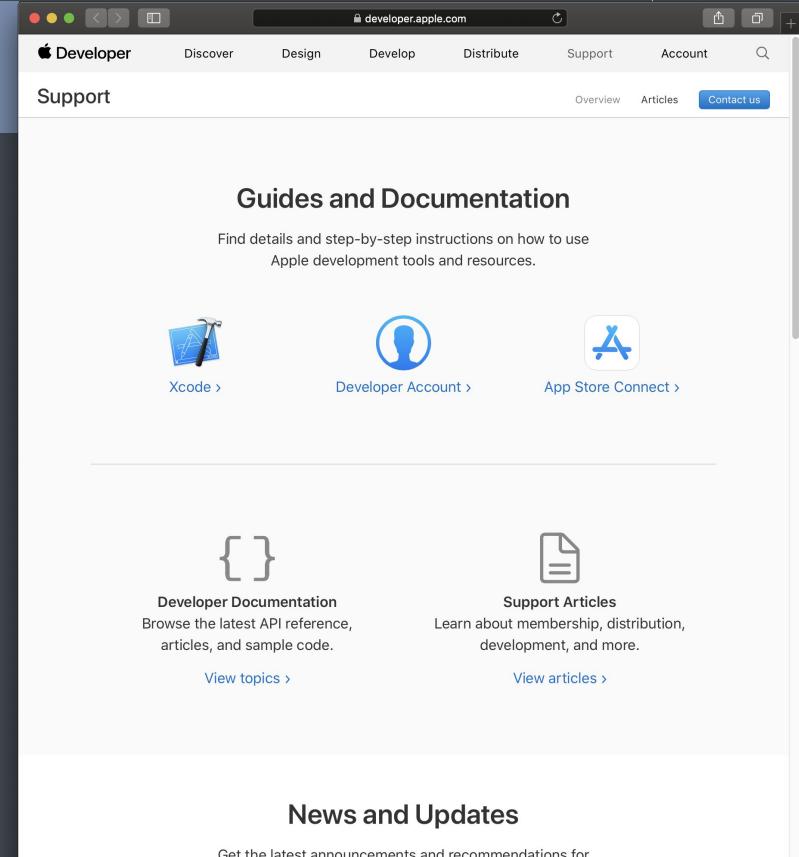


Apple Developer / Notarization

Apple Developer Account Code Signing

xcrun tool

Notarize & Stapling



The screenshot shows the Apple Developer Support page at developer.apple.com. At the top, there's a navigation bar with links for Apple Developer, Discover, Design, Develop, Distribute, Support, and Account. Below that is a "Support" section with links for Overview, Articles, and Contact us. The main content area features a "Guides and Documentation" section with a sub-section for Xcode, Developer Account, and App Store Connect. Below this is a "Developer Documentation" section with a sub-section for View topics. To the right is a "Support Articles" section with a sub-section for View articles. At the bottom is a "News and Updates" section with a sub-section for Get the latest announcements and recommendations for.

Guides and Documentation

Find details and step-by-step instructions on how to use Apple development tools and resources.

Xcode > Developer Account > App Store Connect >

Developer Documentation

Browse the latest API reference, articles, and sample code.

[View topics >](#)

Support Articles

Learn about membership, distribution, development, and more.

[View articles >](#)

News and Updates

Get the latest announcements and recommendations for

Notarization

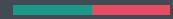
Trusted Developer ID-signed software



```
# notarize, upload App to Apple Notarization Service
xcrun altool --notarize-app --primary-bundle-id "com.example.application.name" -
--username "adc_appleid_here" --password "<adc_appleid_password_here>" --file
"/path/to/Application Name Here.zip"

# next step attach or staple the notarization to the App
xcrun stapler staple "/path/to/Application Name Here.app"
```

Client logs



Log stream



```
# log sudo failed attempts, send to syslog server

log stream --style syslog --predicate 'process == "sudo" and eventMessage
contains "incorrect password"' | openssl s_client -host <hostname> -port 514
```

Caveats: UDP (!), doesn't scale, etc...

Security agents

Modern AV tools (Commercial, Cloud backends)

open source projects (agents):

Osquery (Change detection)



Google Santa (Binary Black/Whitelisting)



Xnumon (auditd wrapper)



Security analytics

Elastic Stack, Splunk, LogRhythm (SaaS backends)



open source projects (control servers):

Kolide Fleet (Osquery)



Zentral Server (Elastic Stack, Osquery, Santa, etc.)



Summary (endpoint security)

Update macOS, iOS & Apps consistently

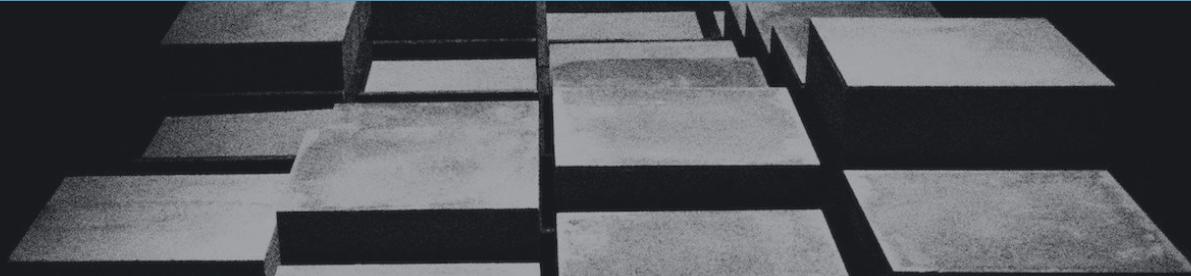
Apple Developer Account (Team account for € 99/y)

Extend Jamf Pro (search JamfNation, GitHub, Marketplace)

Evaluate security tools & analytics*

* we do consult on those topics ;-)

3. Authentication



Identity Provider (IdP)



Cloud Directory Service

Centralized access control (User / Group / Apps)

SAML / OpenID Connect (Web & Mobile Apps, Endpoints)

Optional: use conditional criteria

(Endpoint location, endpoint state)

MFA (IdP enforcement)

Mobile Apps

Push Notification (Mobile Apps)

TOTP (time based one time passcode)

Security Token

FIDO2, U2F (YubiKey, etc.)

SSO (Jamf Pro Server)

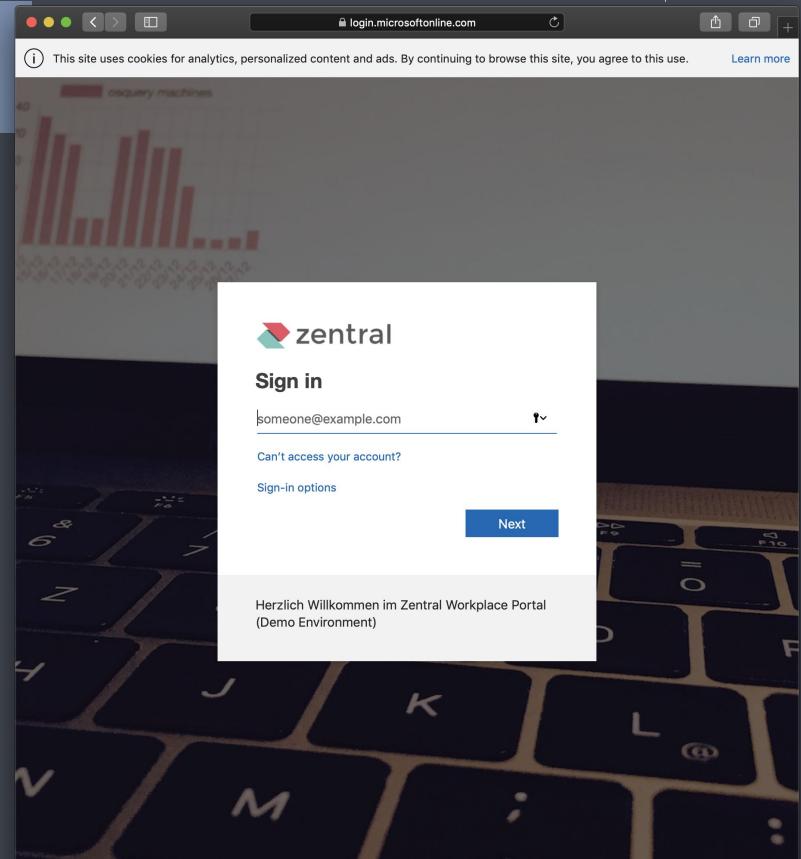
SAML Identity Provider

(AD FS, Azure, GSuite, Okta, ...)

Admin group mapping

MFA options

Audit trail (login success/fail, ...)



Jamf Connect (Endpoint)

macOS Authentication
OpenID Identity Provider
Local user account
Password sync check
Apple Enrollment ready (DEP)



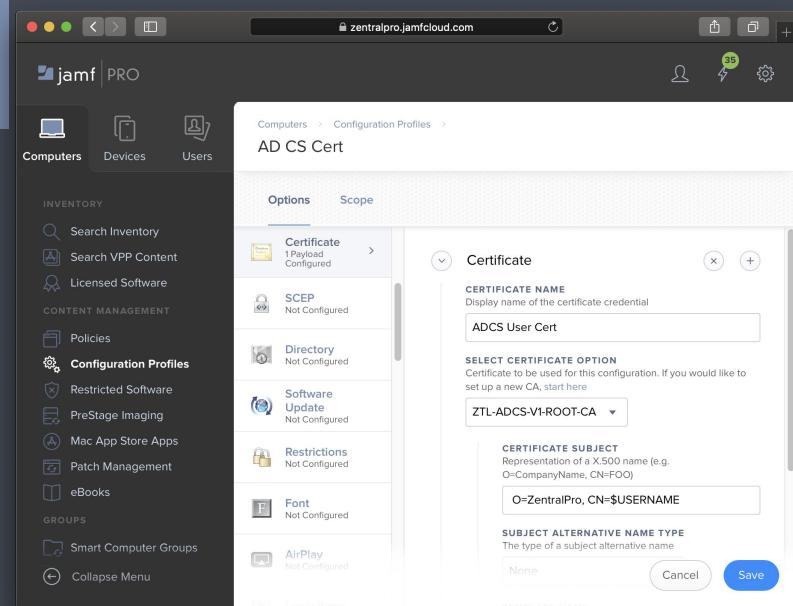
Jamf AD CS Connector

AD certificates (without AD bind)

Jamf Pro as proxy

Complementary to JamfConnect

alternatives: SCEP / NDES setup



Smart Cards

Identity Certificates (self-signed or PKI)

PIN Code (used as 2nd factor)

MFA locally, without IdP

Connect to user account

(direct or use Directory Service Attribute Matching)

MDM configurable



Summary (Authentication)

Use central directory services (Identity Provider)

Use SSO with Jamf Pro (On premises, Cloud)

Jamf Connect for endpoints (macOS, xx)

Use MFA everywhere

Info & links

Links:

<https://t1p.de/2twg>



Zentral Pro Services GmbH & Co. KG