How-to Deploy

CIS Benchmark Tool

This is a guide to designed to help a Jamf Admin deploy the CIS Benchmark Tool for Ventura. This tool was built in April of 2023, on Jamf Pro version 10.45.0-t1678116779

Step 1

Download the CIS Benchmark Tool - Ventura v1.0.dmg. This dmg contains all the necessary files to deploy the tool to a new Jamf Server.

Step 2

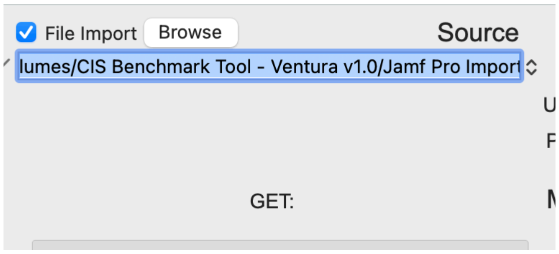
Open the .dmg.

Step 3

Launch the jamf-migrator.app. There is no need to move this to your Applications Folder

Step 4

Check the box for "File Import" and then select "Browse." Select the "raw" folder which is enclosed in the CIS Benchmark Tool - Ventura v1.0.dmg. It should look something like this:

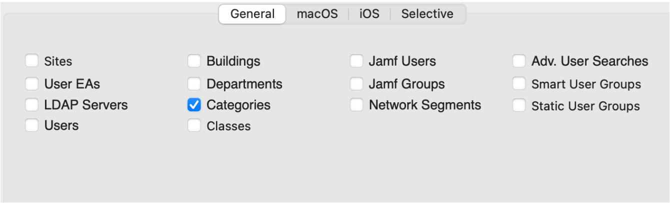


☑ File Import

lumes/CIS Benchmark Tool - Ventura v1.0/Jamf Pro Import

Step 5

Next, check the **Categories** checkbox underneath ***General*** and then check the **Extension Attributes, Scripts, Packages, Smart Groups, Config. Profiles, Adv. Comp. Searches and Policies** boxes under ***macOS***. *Note: Smart Groups and Adv. Comp. Searches are optional*

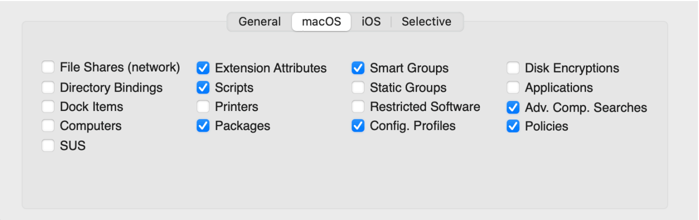


□ Sites
□ User EAs
□ LDAP Servers
□ Users

□ Buildings
□ Departments
☑ Categories
□ Classes

□ Jamf Users
□ Jamf Groups
□ Network Segments

□ Adv. User Searches
□ Smart User Groups
□ Static User Groups



□ File Shares (network)
□ Directory Bindings
□ Dock Items
□ Computers
□ SUS

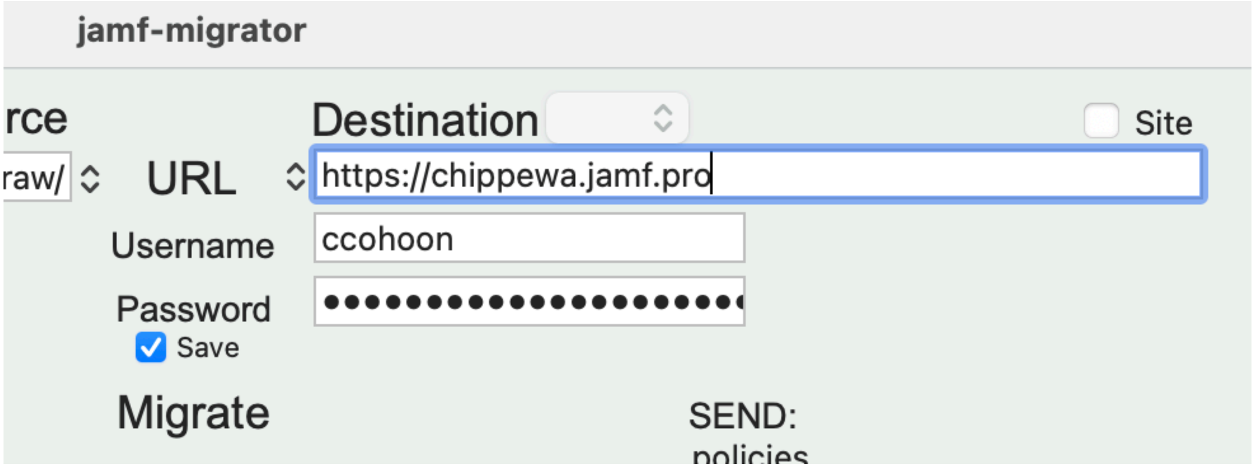
☑ Extension Attributes
☑ Scripts
□ Printers
☑ Packages

☑ Smart Groups
□ Static Groups
□ Restricted Software
☑ Config. Profiles

□ Disk Encryptions
□ Applications
☑ Adv. Comp. Searches
☑ Policies

Step 6

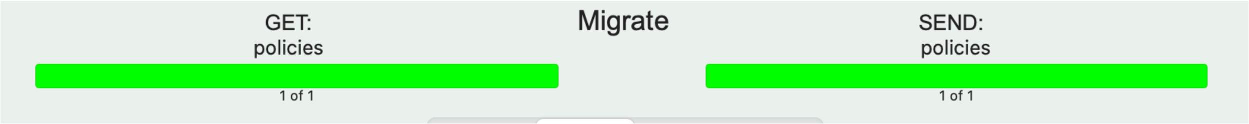
Now, populate the Destination with the Jamf Pro server that you'd like to install this on. Like this:



Destination
□ Site
URL https://chippewa.jamf.pro
Username ccohoon
Password ●●●●●●●●●●●●●●●●●●●●●●
☑ Save
SEND:
policies

Step 7

Execute the migration by clicking **Go** in the bottom right of the utility. You should see the progress bars progress as the items are uploaded to your Jamf Pro server.



GET:
policies
1 of 1

SEND:
policies
1 of 1

Step 8

Log into your destination Jamf Pro Server. Verify that you have the following:

Category	CIS Benchmark
Configuration Profiles	CIS Benchmark Enforcement | Cross-Site Tracking CIS Benchmark Enforcement | Firewall Auditing CIS Benchmark Enforcement | Login Window CIS Benchmark Enforcement | NEED TO CREATE FILEVAULT PROFILE CIS Benchmark Enforcement | Passcode CIS Benchmark Enforcement | Restrictions CIS Benchmark Enforcement | Screensaver 2 CIS Benchmark Enforcement | Screensaver Password Requirement CIS Benchmark Enforcement | Screensaver CIS Benchmark Enforcement | Security & Privacy CIS Benchmark Enforcement | Software Updates CIS Benchmark Enforcement | Terminal Full Disk Access CIS Benchmark Enforcement | Universal Control
Packages	CIS_v1.0.sh.pkg
Policies	CIS Scripts CIS Daily Audit
Computer Extension Attributes	CIS Benchmark | Applications CIS Benchmark | Logging & Auditing CIS Benchmark | Network Configurations CIS Benchmark | Software Updates CIS Benchmark | System Settings CIS | Overall
Scripts	CIS Daily Audit
Advanced Computer Searches (Optional)	CIS Benchmark | Compliant Macs - Ventura CIS Benchmark | Non Compliant Macs - Ventura
Smart Computer Groups (Optional)	CIS Benchmark Compliant Macs CIS Benchmark Non-Compliant Macs Ventura Macs

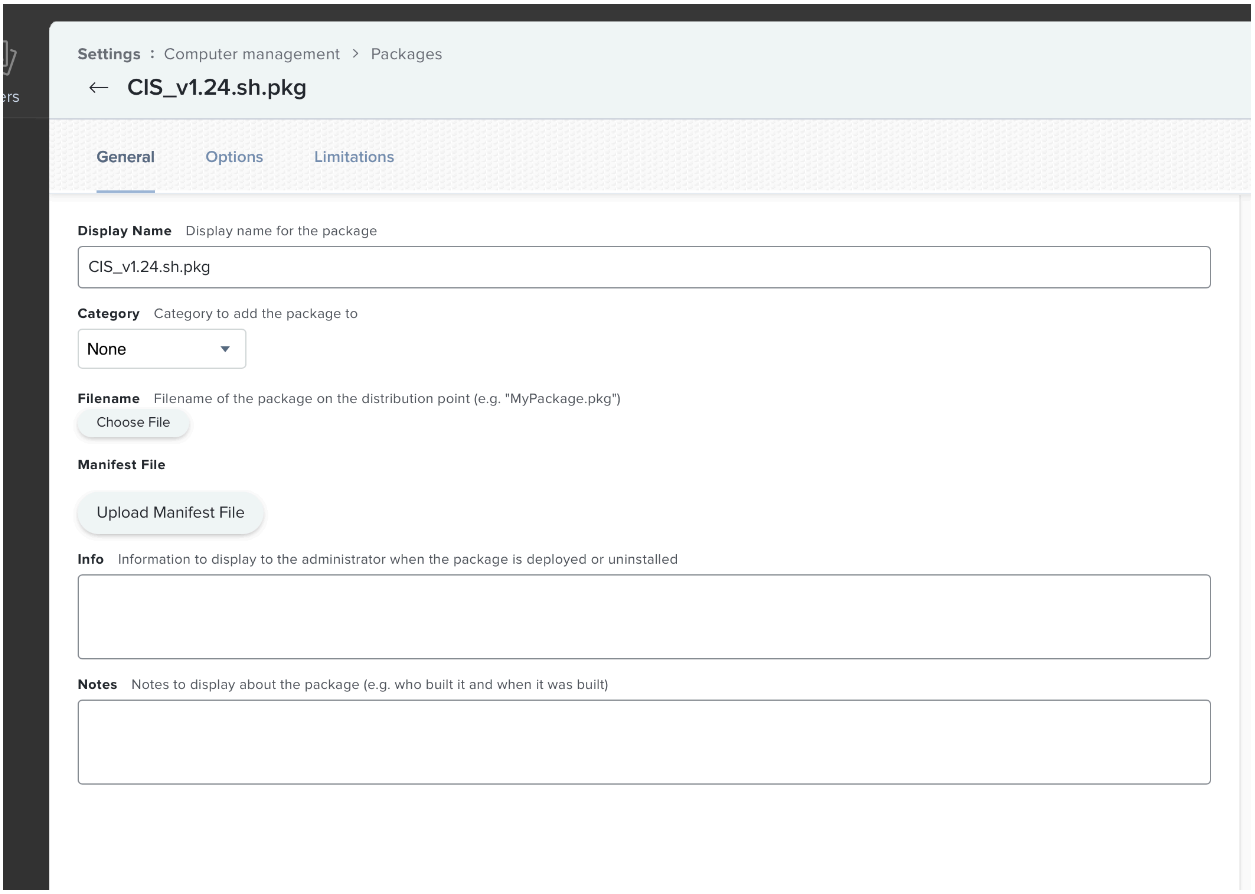
Step 9

Packages cannot be added through the Jamf Migrator utility - only their database record, so we need to navigate to our package record, and click edit. Then, click **Choose File** and upload the **CIS_v1.0.sh.pkg** which is located in the **CIS Benchmark Tool - Ventura v1.0.dmg.** Now, our package record has an actual package in the Distribution Point . This step assumes you're utilizing the JCDS. If you're utilizing another Distribution Point technology, follow the steps you typically would to upload your package.

Step 10

Navigate to the Configuration Profile titled **CIS Benchmark Enforcement | NEED TO CREATE FILEVAULT PROFILE.** Click **Edit** and rename this profile **CIS Benchmark Enforcement | FileVault.** Then, navigate to the Security & Privacy Payload - configure the FileVault section so that FileVault is enabled and the personal recovery keys are escrowed.

Step 11



Display Name Display name for the package: CIS_v1.24.sh.pkg

Category Category to add the package to: None

Filename Filename of the package on the distribution point (e.g. "MyPackage.pkg")

Manifest File

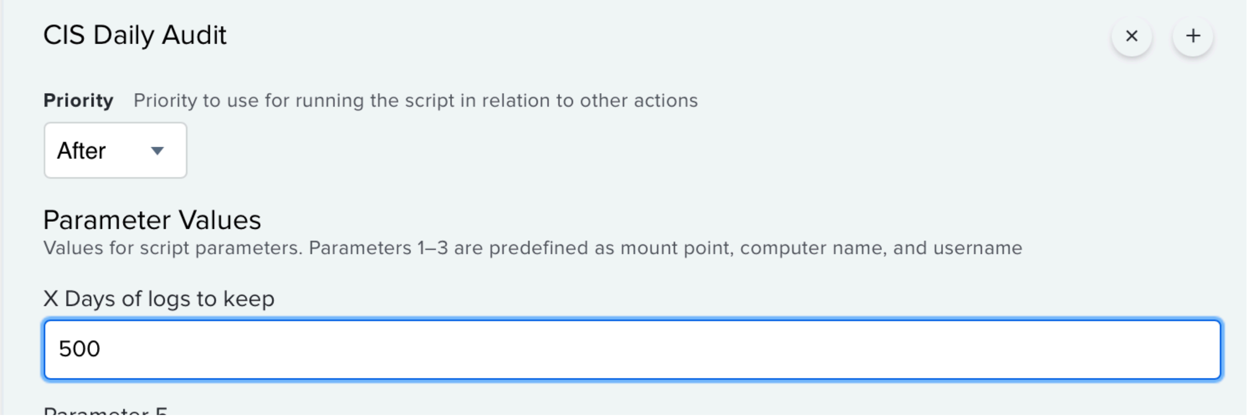
Info Information to display to the administrator when the package is deployed or uninstalled

Notes Notes to display about the package (e.g. who built it and when it was built)

Navigate to the policy named **CIS Scripts.** Set scope accordingly. Set Triggers to **Enrollment Complete** and **Recurring Check-in**. Set Frequency to **Once per Computer** and check the **Automatically re-run policy on failure box.** This will ensure all new and existing computers install the scripts.

Step 12

Navigate to the policy named **CIS Daily Audit.** Set scope accordingly. Configure this to run **once per day** with the **trigger Recurring Check-in**. If necessary, update the number of days you'd like to keep the CIS logs for. If you choose not to set a value in the script's parameters, the default is to store log files for 365 days. Each log is about 3.8 KB, which should only add up to about 1.4 MB each year. Retaining more logs will increase your forensic abilities if ever necessary.



CIS Daily Audit

Priority Priority to use for running the script in relation to other actions

After

Parameter Values

Values for script parameters. Parameters 1–3 are predefined as mount point, computer name, and username

X Days of logs to keep

500

Parameter 5

Step 13

That should be it. You now have all the components configured and installed on the Jamf Pro Server. Once the first policy runs and installs the scripts it will run a recon which should cause the machine to update the new extension attributes. The daily script will trigger new runs of the audit creating new log files which will be parsed by the subsequent recons. If it's needed -

Notes

- The policy CIS Scripts deploys two new directories onto the target Macs.

    1. /Library/Application Support/Security Audit

    2. /Private/etc/sudoers.d/

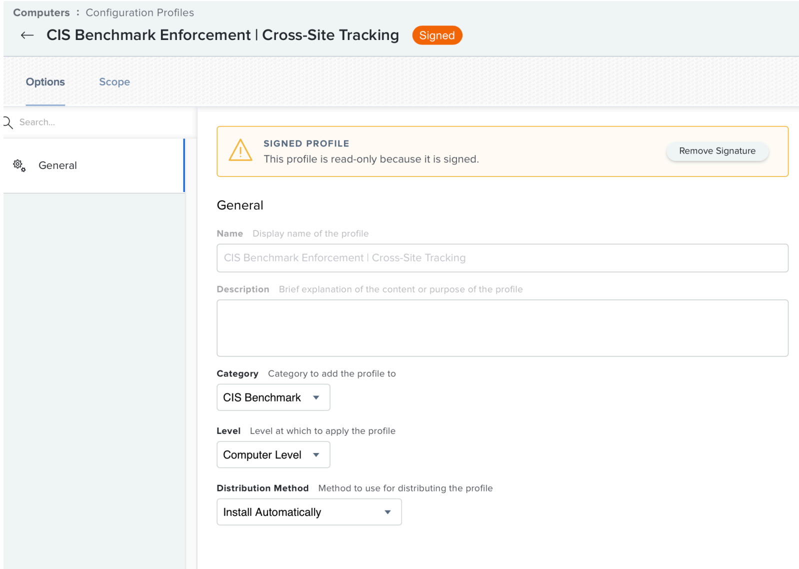
    - In these two directories we deploy a few files.

        1. In the Security Audit directory, we deploy two scripts. The first script is designed to bring a computer into compliance with the CIS Benchmark in ways that Configuration Profiles fail to do. The second script is designed to verify that both the compliance script + Configuration Profiles did their job in bringing the target computer up to compliance.

        2. In the sudeors.d file we deploy a custom configuration for Terminal.app. This was simply the best way to create the necessary file which is for item 5.5 in the Benchmark considering we're already deploying a package.

- The policy CIS Daily Audit simply runs a third script that is kept within Jamf Pro (not stored on the client locally). This script will remove old logs from previous runs, and then initiate a new run of the audit script which was deployed to the client in the CIS Scripts policy.

- I've created three Smart Groups and two advanced searches within the import files. These five objects could be considered optional. The "Ventura Macs" Smart Group is a little more necessary than the other four, as it is what the policies and Configuration Profiles are scoped to out of the box, but you could re-scope these as needed to any pre-existing smart group you may have already.



CIS Benchmark Enforcement | Cross-Site Tracking Signed

SIGNED PROFILE
This profile is read-only because it is signed.

General

Name Display name of the profile
CIS Benchmark Enforcement | Cross-Site Tracking

Description Brief explanation of the content or purpose of the profile

Category Category to add the profile to
CIS Benchmark

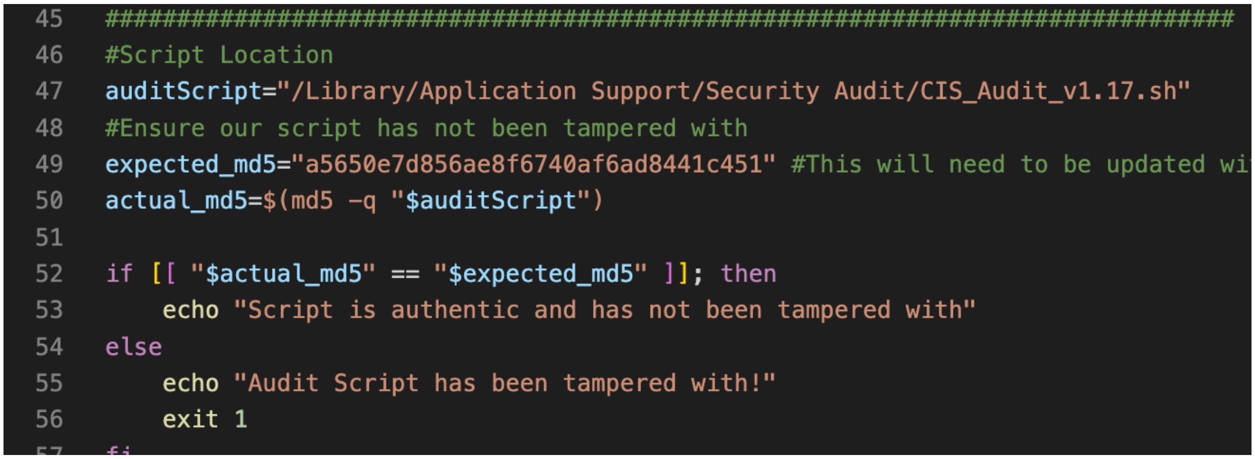
Level Level at which to apply the profile
Computer Level

Distribution Method Method to use for distributing the profile
Install Automatically

- Generally, its recommended to keep your Smart Groups to a minimum as they take a surprisingly large amount of resources within Jamf Pro. So, if you don't need them, don't import them.

- Many of the Configuration Profiles won't 'look right' within Jamf Pro. This is because many of them were constructed outside of Jamf Pro. This is because Jamf does not currently support the full MDM spec - only a subset of it. These profiles were created with another tool and signed in that tool. Its very important that these remain signed. If you click the Remove Signature button, Jamf Pro will have the capability to edit the profile. If that happens, it will remove any payloads it doesn't recognize. You can tell from the screenshot above, it doesn't recognize the payloads as it appears to only have "General" configured. The profile in the screenshot does however have the **Ad Tracking** payload configured - you just won't see it in Jamf Pro.

- The script within the CIS Daily Audit policy will verify the authenticity of the audit script via an MD5 hash. So, if you make any modifications to the Audit Script you must update the MD5 hash in the CIS Daily Audit script. You can generate a new hash by running this in Terminal: `md5 -q /path/to/script.sh`



```
##############################################################################
#Script Location
auditScript="/Library/Application Support/Security Audit/CIS_Audit_v1.17.sh"
#Ensure our script has not been tampered with
expected_md5="a5650e7d856ae8f6740af6ad8441c451" #This will need to be updated wi
actual_md5=$(md5 -q "$auditScript")

if [[ "$actual_md5" == "$expected_md5" ]]; then
    echo "Script is authentic and has not been tampered with"
else
    echo "Audit Script has been tampered with!"
    exit 1
fi
```