Social Voting for Santa

Henry Stamerjohann - Zentral

zentral

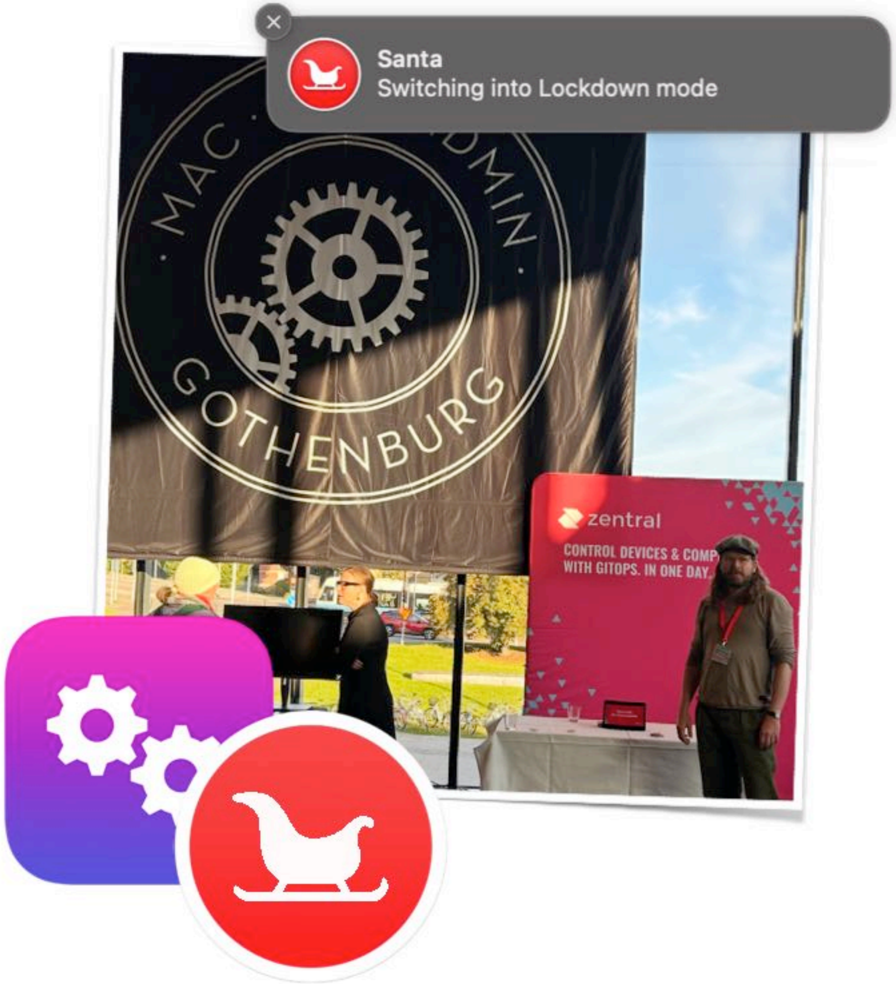
Hello Gothenburg

First time sponsor!

Zentral is a MDM

..that makes best open source tools easy to use

...so you don't have to build your own stack



Santa
Switching into Lockdown mode

zentral

MacSysAdmin 2023

We ❤️ GitOps because its transparent

You need transparency for compliance

Mixed reviews:

Not sure they'll get significant market for this

Very technical

Bit messy at times

Cool stuff [...] but why?!?!

Not feasible in the real IT world..

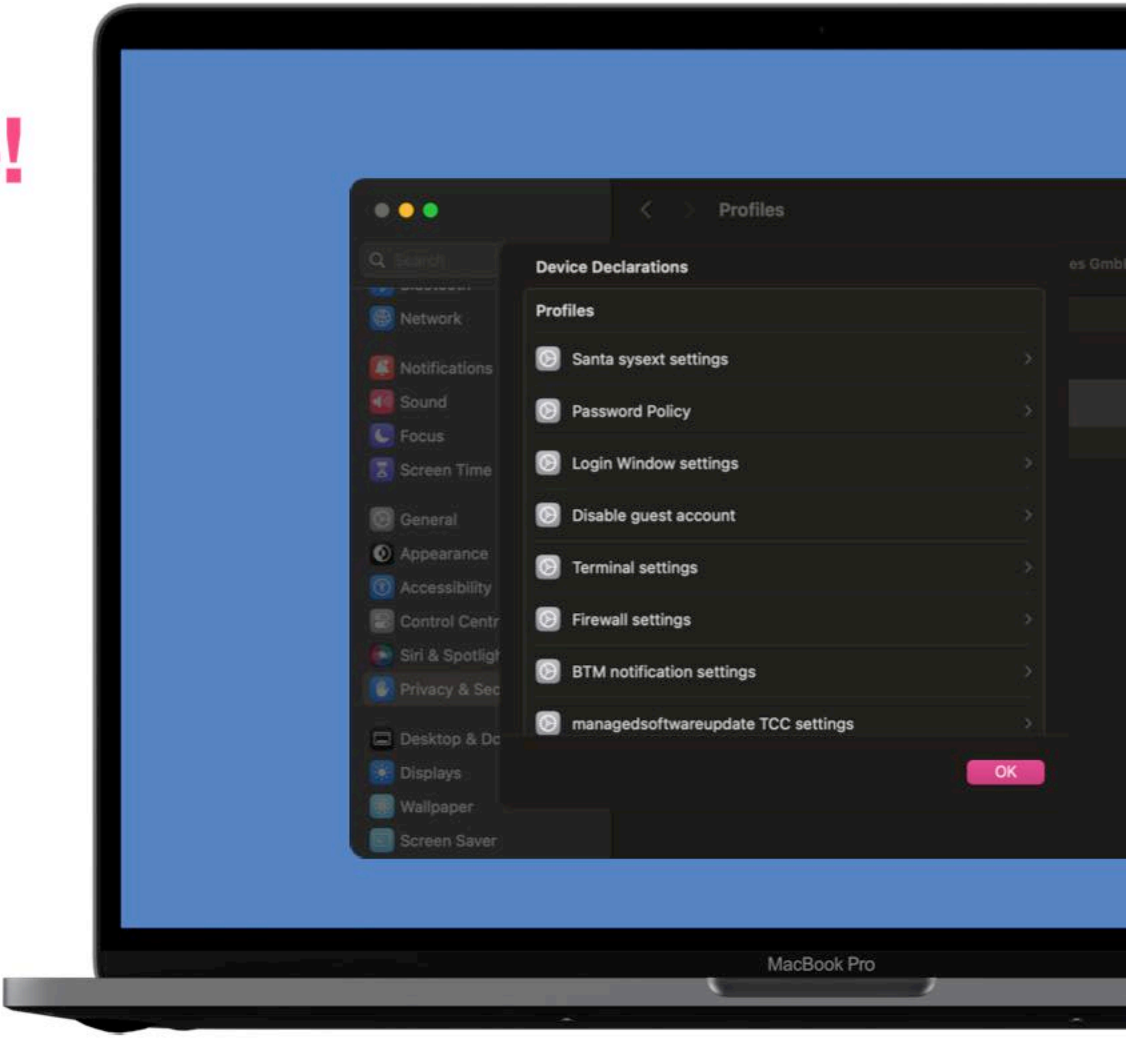
BACK TO THE FUTURE

Marty McFly

I guess you guys aren't ready for that yet. But your kids are gonna love it.

zentral

GitOps made accessible!



Device Declarations

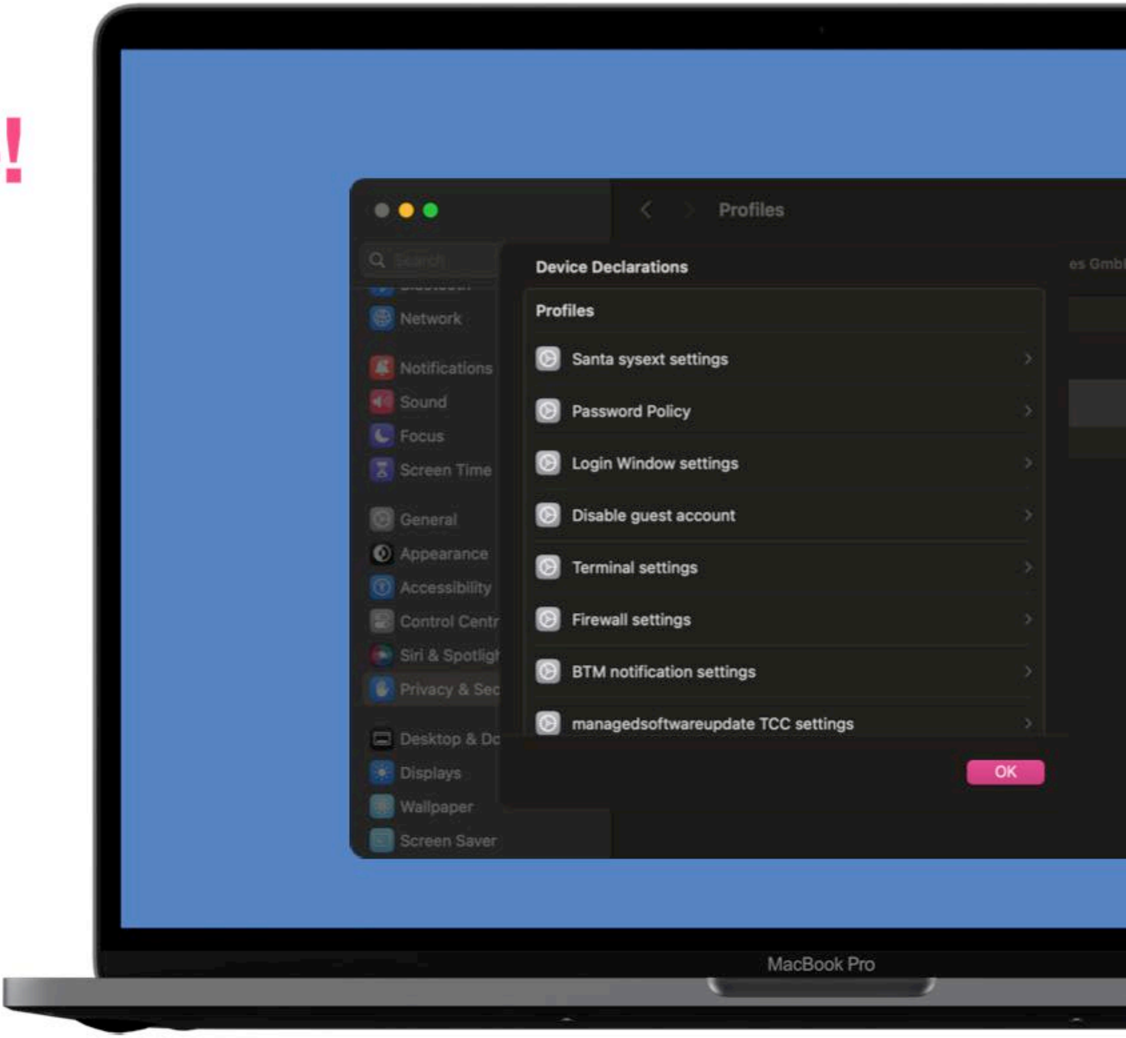
Profiles

- Santa sysext settings
- Password Policy
- Login Window settings
- Disable guest account
- Terminal settings
- Firewall settings
- BTM notification settings
- managedsoftwareupdate TCC settings

zentral

GitOps made accessible!

- 🎯 Framework & Playbook
- 💻 Pre-populated with Standard Client
- 🔒 Available as SaaS with SOC2
- 🚀 Hit the ground running!



Device Declarations

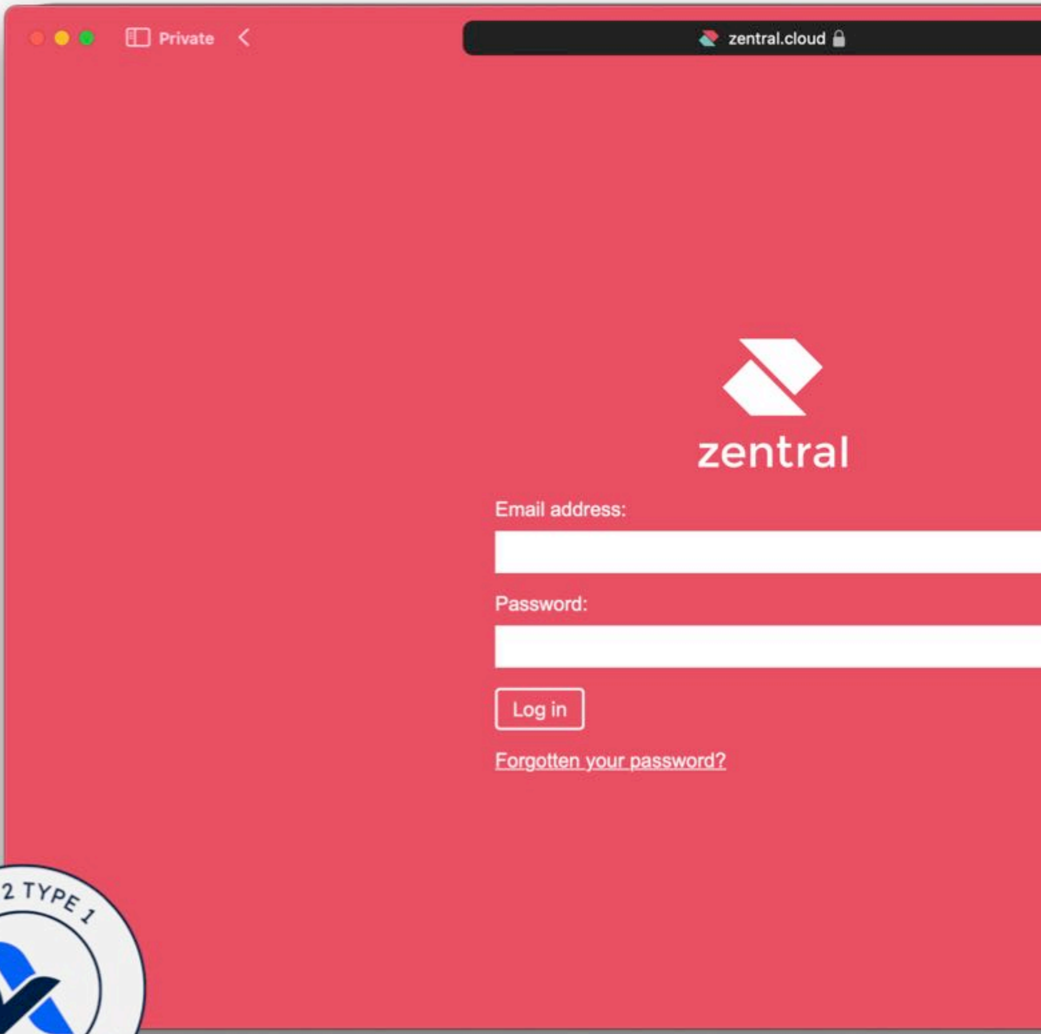
Profiles

- Santa sysext settings
- Password Policy
- Login Window settings
- Disable guest account
- Terminal settings
- Firewall settings
- BTM notification settings
- managedsoftwareupdate TCC settings

zentral

GitOps made accessible!

- 🎯 Framework & Playbook
- 💻 Pre-populated with Standard Client
- 🔒 Available as SaaS with SOC2
- 🚀 Hit the ground running!



zentral

Email address:

Password:

Log in

Forgotten your password?

SOC 2 TYPE 1

VERIFIED BY ASSURANCELAB

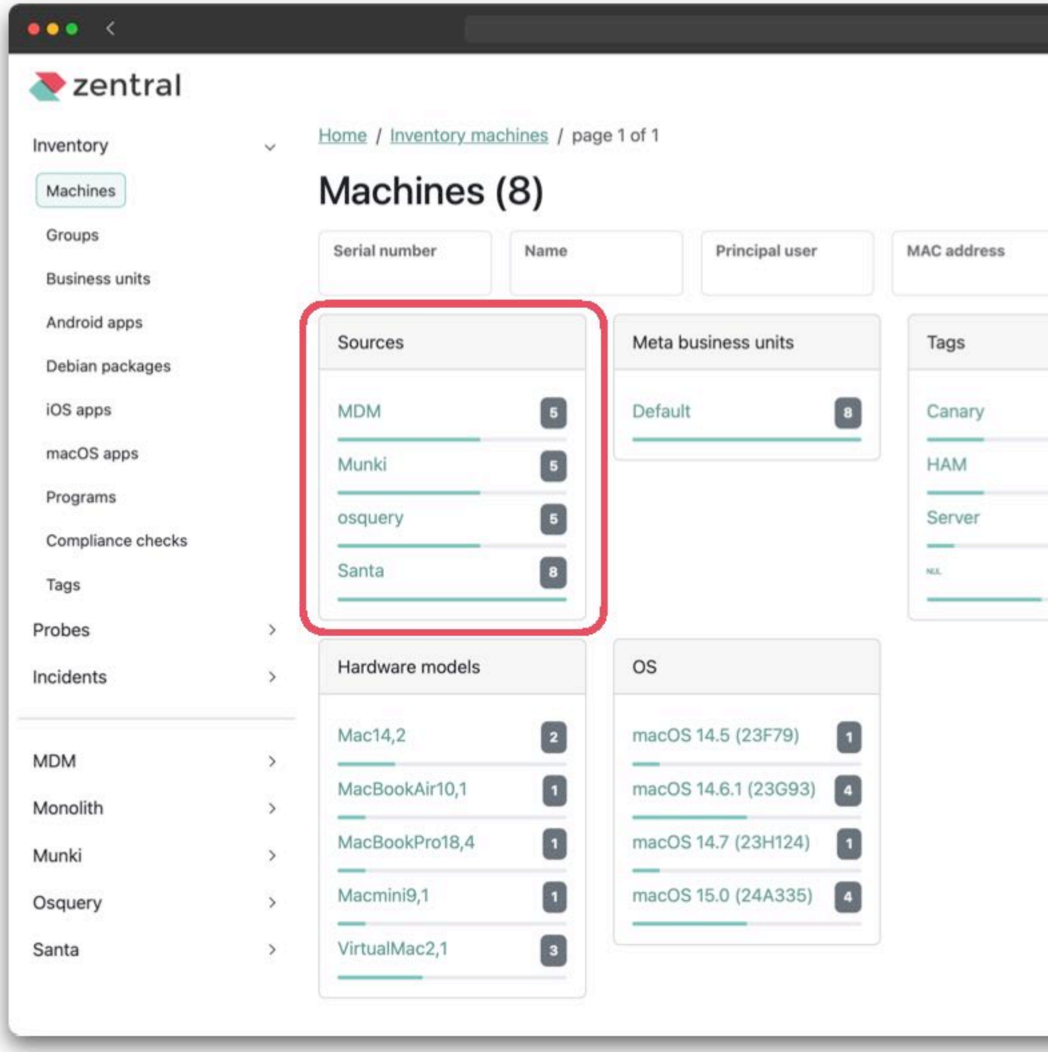
zentral

Pillars of Zentral

✨ Go with the Flow:
Stay true to the source

✨ Integrations:
Quality of life improvements where possible

✨ Visibility:
Events, Audit Trails and Logs, Feedback Loops for Compliance



Machines (8)

Sources	
MDM	5
Munki	5
osquery	5
Santa	8

Meta business units	
Default	8

Tags
Canary
HAM
Server

Hardware models	
Mac14,2	2
MacBookAir10,1	1
MacBookPro18,4	1
Macmini9,1	1
VirtualMac2,1	3

OS	
macOS 14.5 (23F79)	1
macOS 14.6.1 (23G93)	4
macOS 14.7 (23H124)	1
macOS 15.0 (24A335)	4

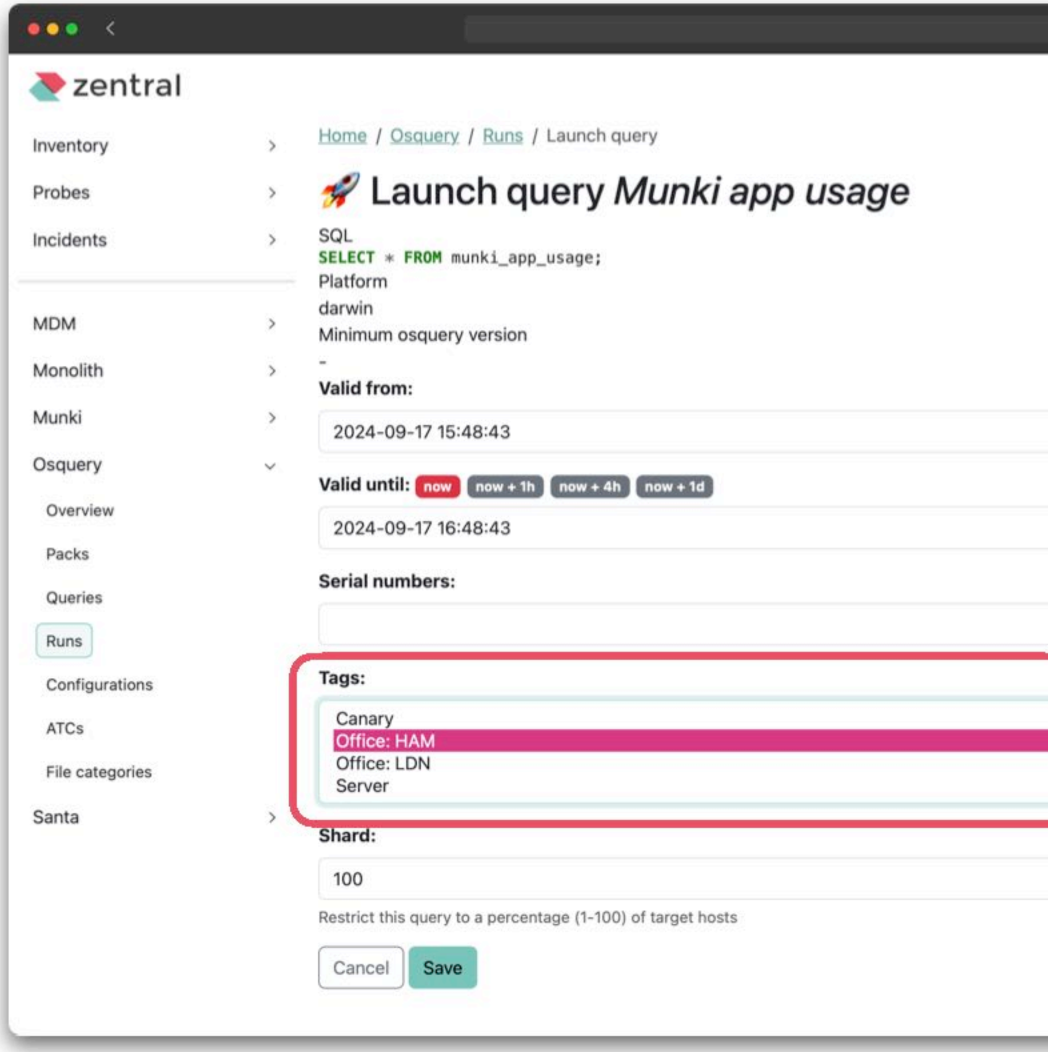
zentral

Pillars of Zentral

✨ Go with the Flow:
Stay true to the source

✨ Integrations:
Quality of life improvements where possible

✨ Visibility:
Events, Audit Trails and Logs, Feedback Loops for Compliance



Home / Osquery / Runs / Launch query

🚀 Launch query *Munki app usage*

SQL

```
SELECT * FROM munki_app_usage;
```

Platform

darwin

Minimum osquery version

-

Valid from: 2024-09-17 15:48:43

Valid until: now | now + 1h | now + 4h | now + 1d

2024-09-17 16:48:43

Serial numbers:

Tags:
Canary
Office: HAM
Office: LDN
Server

Shard: 100

Restrict this query to a percentage (1-100) of target hosts

Cancel | Save

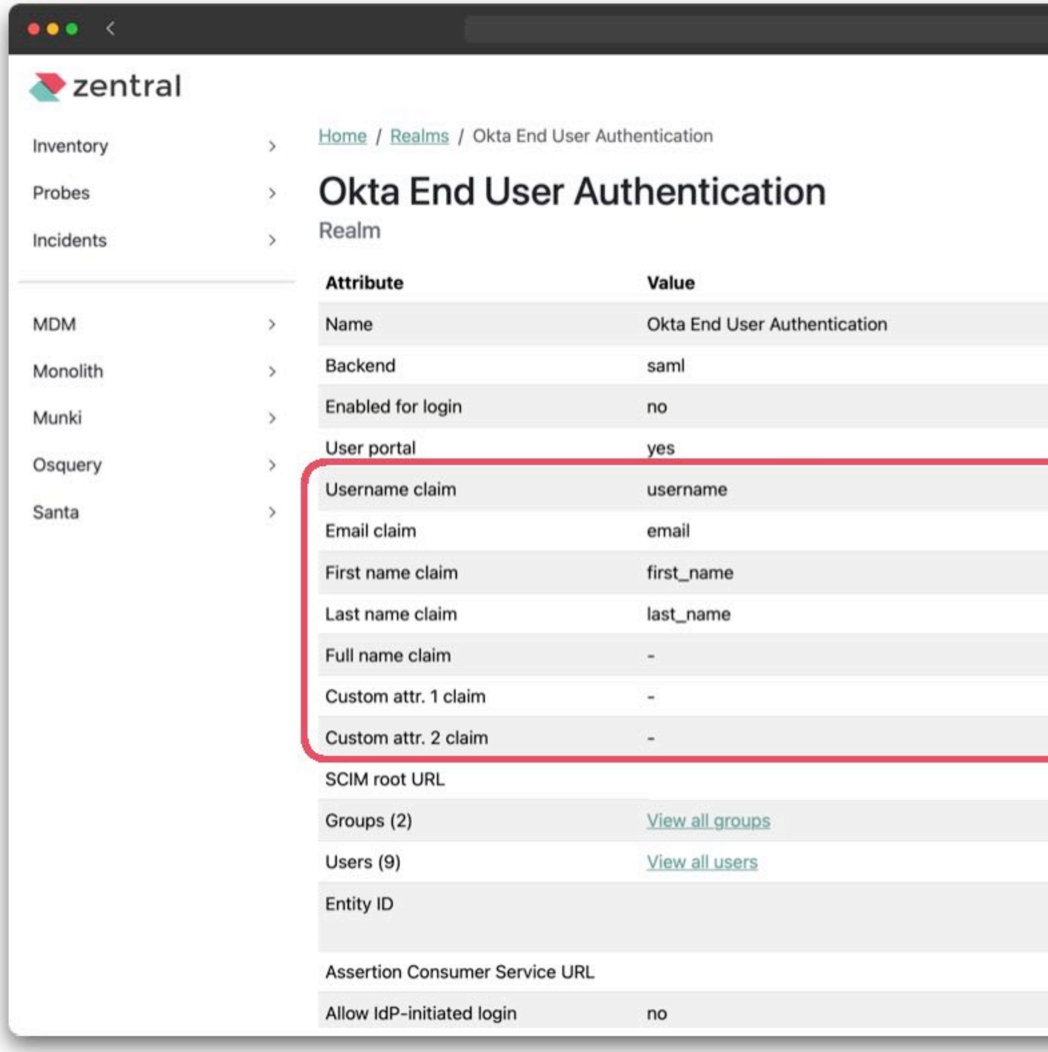
zentral

Pillars of Zentral

✨ Go with the Flow:
Stay true to the source

✨ Integrations:
Quality of life improvements where possible

✨ Visibility:
Events, Audit Trails and Logs, Feedback Loops for Compliance



Home / Realms / Okta End User Authentication

Okta End User Authentication

Realm

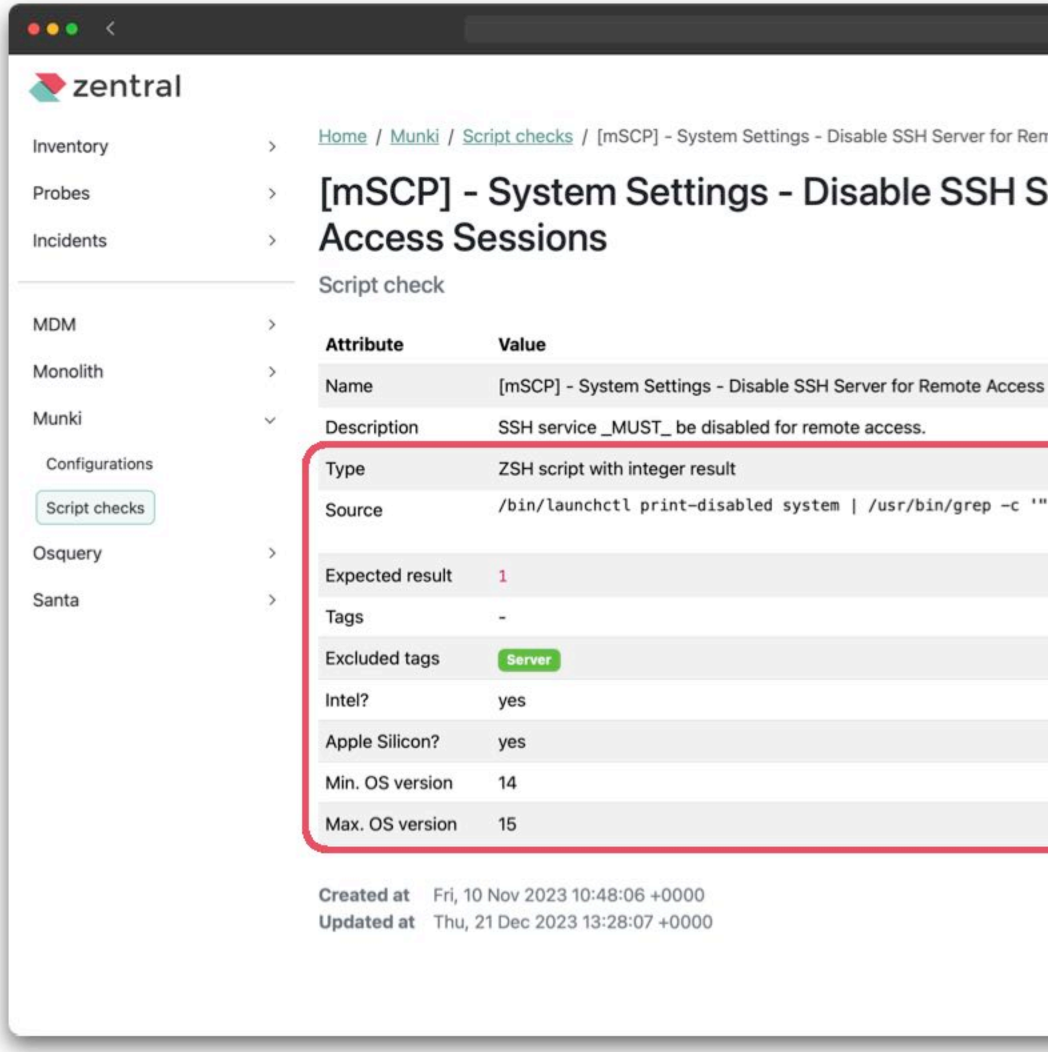
Attribute	Value
Name	Okta End User Authentication
Backend	saml
Enabled for login	no
User portal	yes
Username claim	username
Email claim	email
First name claim	first_name
Last name claim	last_name
Full name claim	-
Custom attr. 1 claim	-
Custom attr. 2 claim	-
SCIM root URL	
Groups (2)	View all groups
Users (9)	View all users
Entity ID	
Assertion Consumer Service URL	
Allow IdP-initiated login	no

Pillars of Zentral

✨ Go with the Flow:
Stay true to the source

✨ Integrations:
Quality of life improvements where possible

✨ Visibility:
Events, Audit Trails and Logs, Feedback Loops for Compliance



Home / Munki / Script checks / [mSCP] - System Settings - Disable SSH Server for Rem

[mSCP] - System Settings - Disable SSH S Access Sessions

Script check

Attribute	Value
Name	[mSCP] - System Settings - Disable SSH Server for Remote Access
Description	SSH service _MUST_ be disabled for remote access.
Type	ZSH script with integer result
Source	`/bin/launchctl print-disabled system | /usr/bin/grep -c '"`
Expected result	1
Tags	-
Excluded tags	Server
Intel?	yes
Apple Silicon?	yes
Min. OS version	14
Max. OS version	15

Created at Fri, 10 Nov 2023 10:48:06 +0000
Updated at Thu, 21 Dec 2023 13:28:07 +0000

zentral

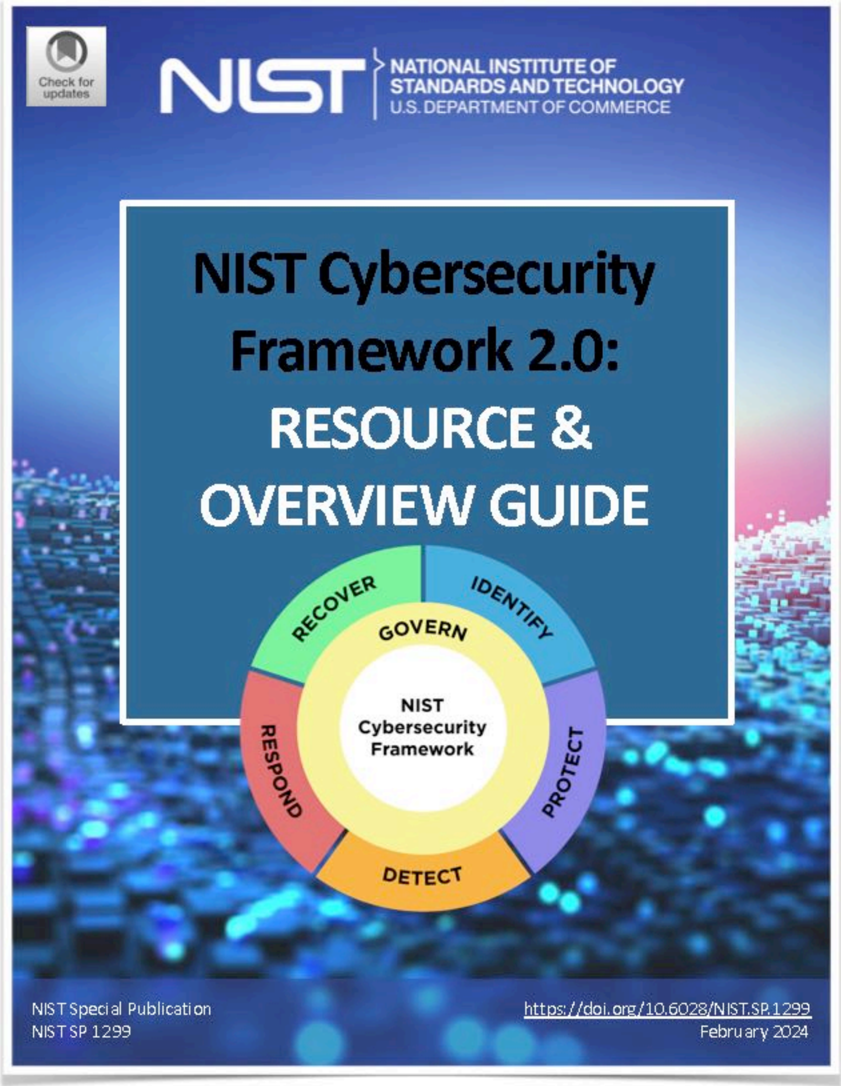
Security Posture

🔒 Fundamentals:
Identify, Detect, Protect

✅ Allowlisting:
“Protect” best practice

🎱 Challenges:

How to get to a quality custom Allowlist?
Best way to handle user-bound exceptions?



Check for updates

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Framework 2.0: RESOURCE & OVERVIEW GUIDE

NIST Special Publication
NIST SP 1299

https://doi.org/10.6028/NIST.SP.1299
February 2024

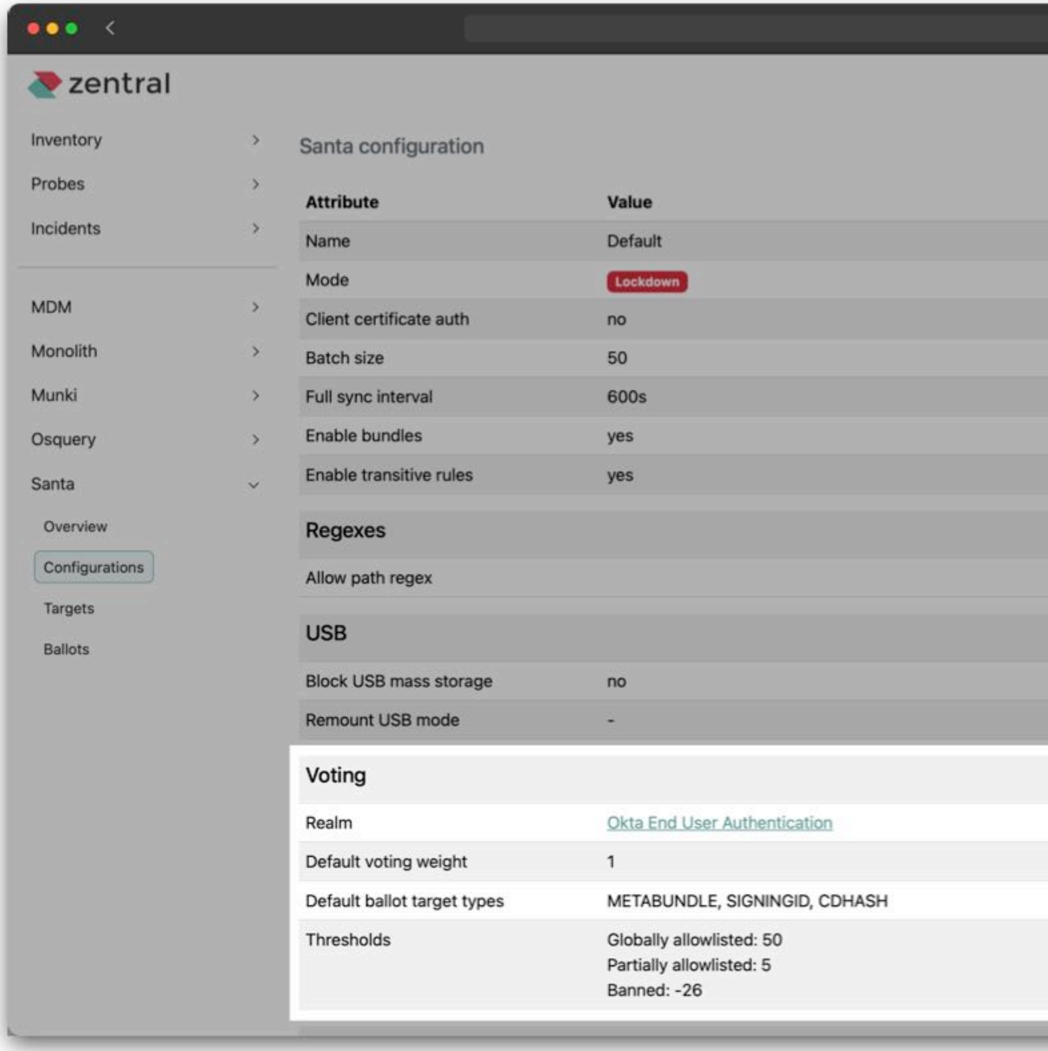
zentral

Upvote Reimagined

👍 Upvote:

Scores apps with user votes

Handles rule creation based on thresholds



Santa configuration

Attribute	Value
Name	Default
Mode	Lockdown
Client certificate auth	no
Batch size	50
Full sync interval	600s
Enable bundles	yes
Enable transitive rules	yes

Regexes

Allow path regex	

USB

Block USB mass storage	no
Remount USB mode	-

Voting

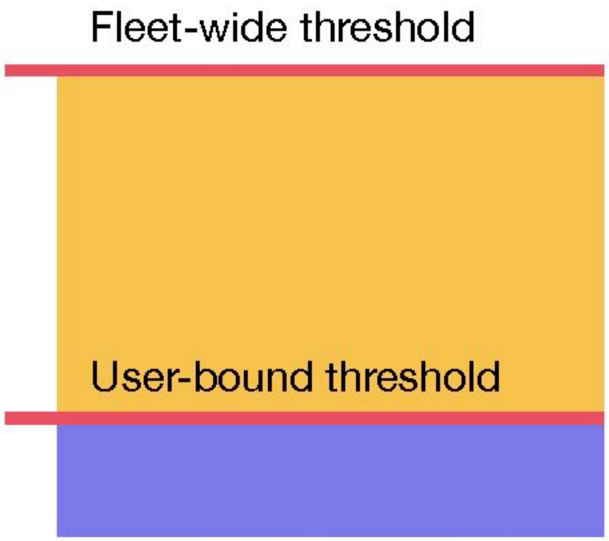
Realm	Okta End User Authentication
Default voting weight	1
Default ballot target types	METABUNDLE, SIGNINGID, CDHASH
Thresholds	Globally allowlisted: 50 Partially allowlisted: 5 Banned: -26

Upvote Reimagined

👍 Upvote:

Scores apps with user votes

Handles rule creation based on thresholds



Fleet-wide threshold

User-bound threshold

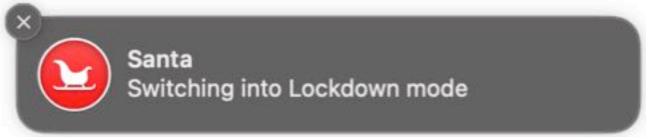
zentral

Social Voting

👍 Upvote the app

🔒 Partially allowlisted

🌎 Globally allowlisted



Santa
Switching into Lockdown mode

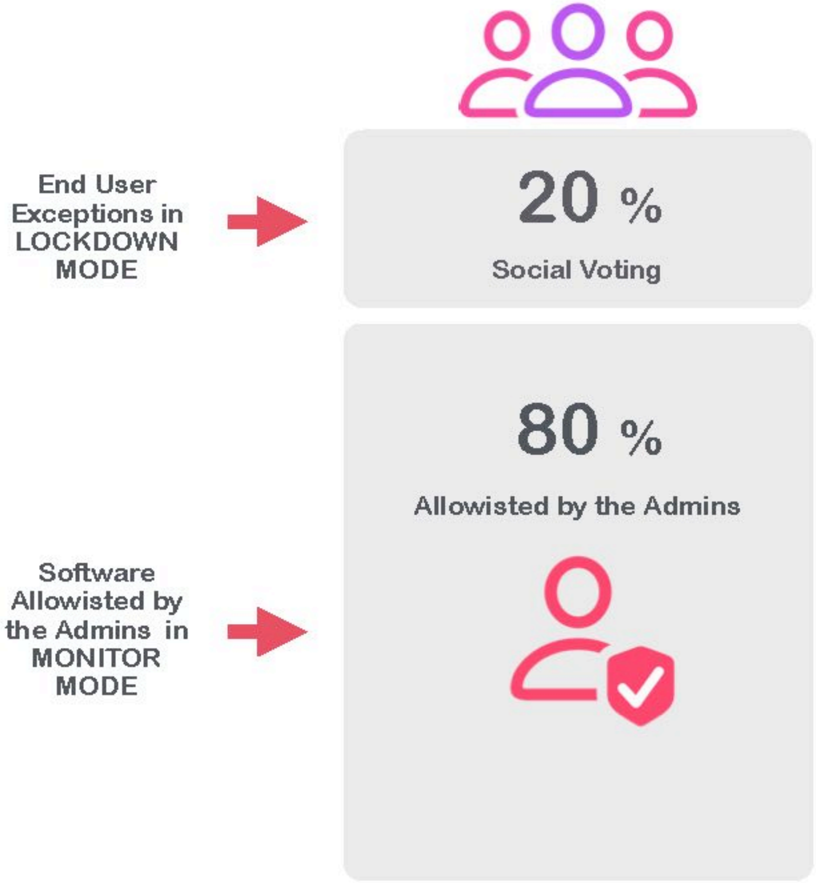
zentral

Social Voting

🚶 Walk before you run:
Monitor Mode

✅ Admin task:
Allowlist most important Apps

👍 Social Voting:
Users can cast a vote for App



End User Exceptions in LOCKDOWN MODE

20 %

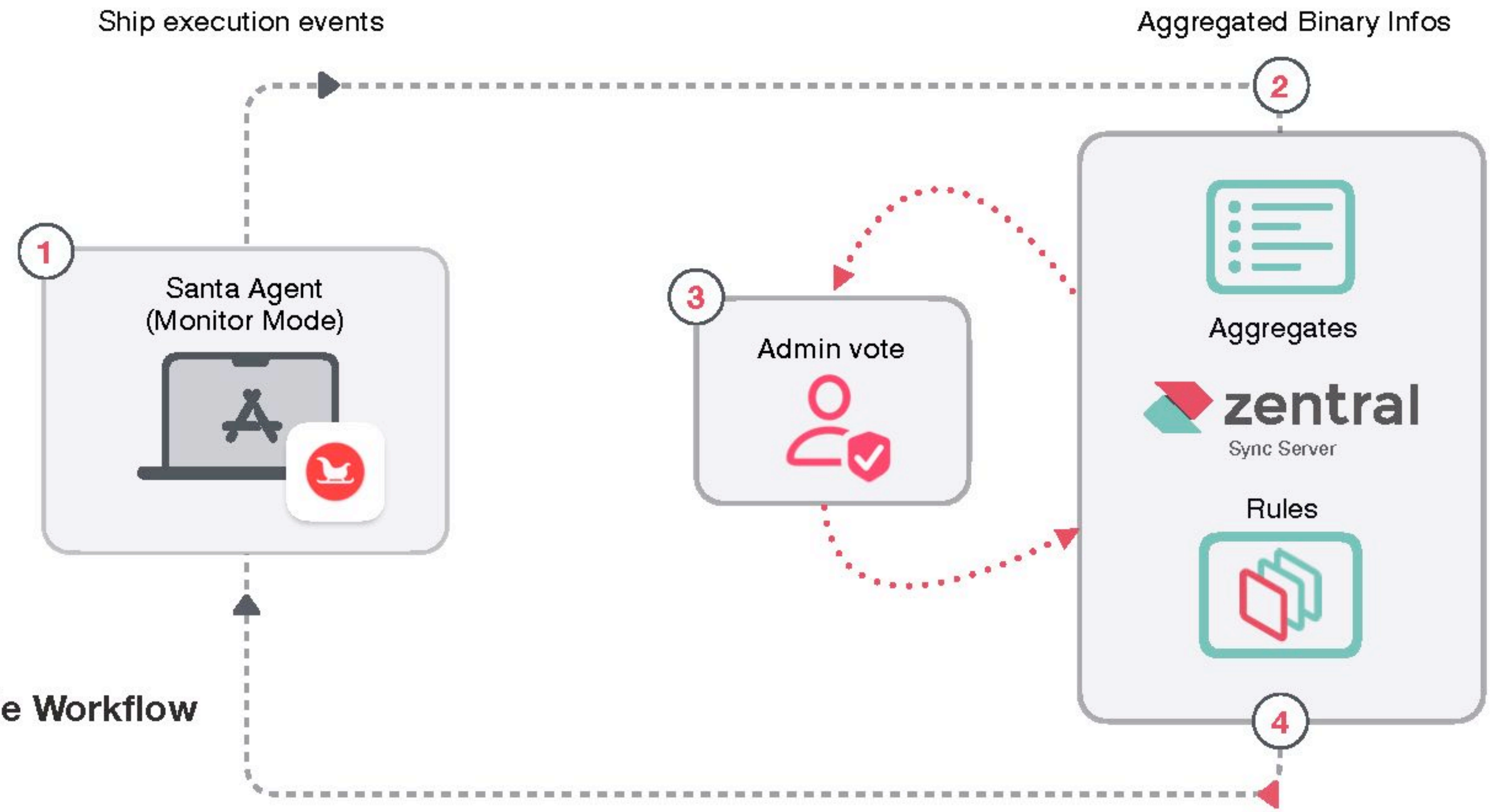
Social Voting

Software Allowisted by the Admins in MONITOR MODE

80 %

Allowisted by the Admins

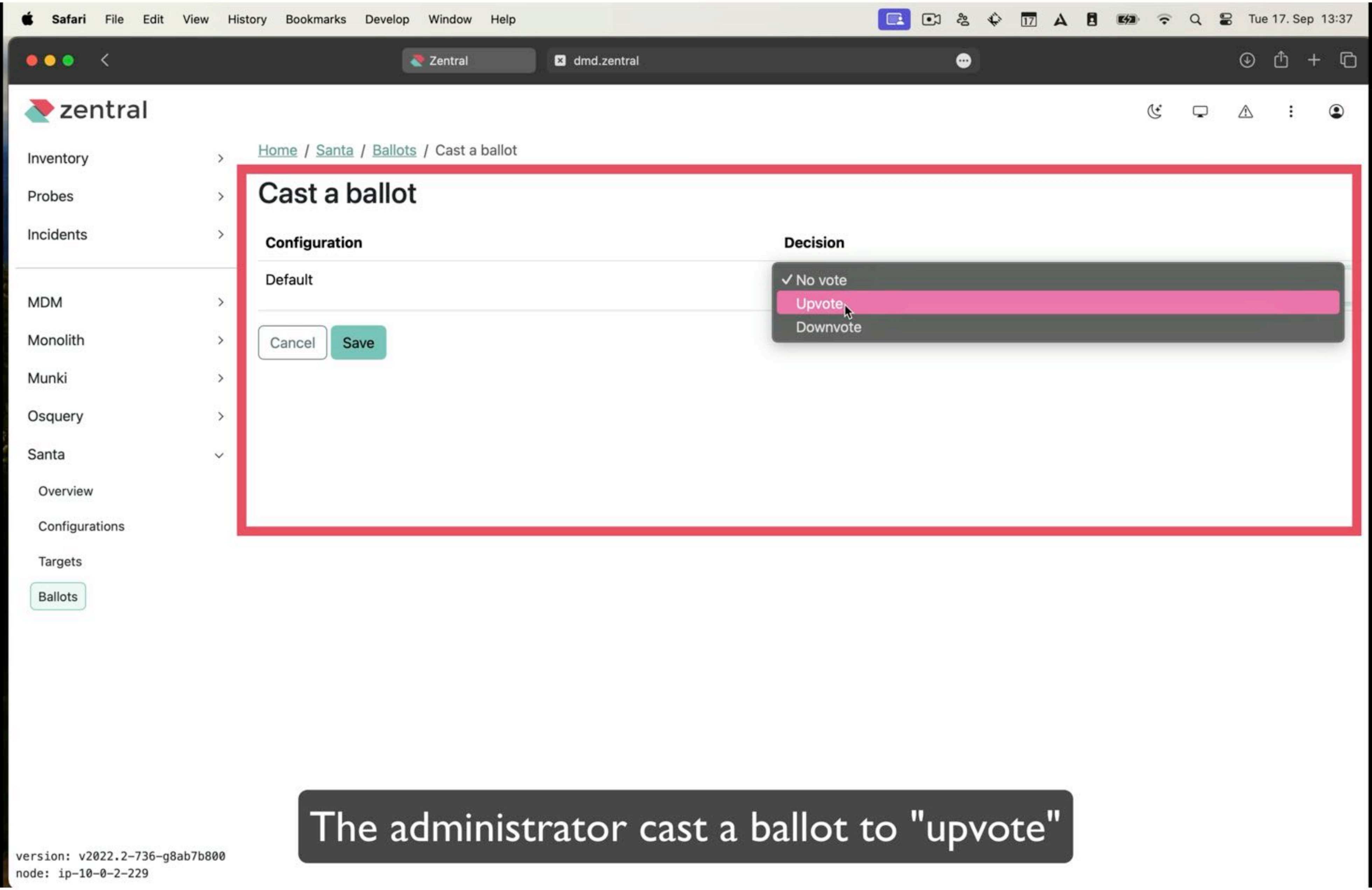
Preparing Your Allowlist



Monitor Mode Workflow

zentral

MONITOR MODE: Building the Allowlist

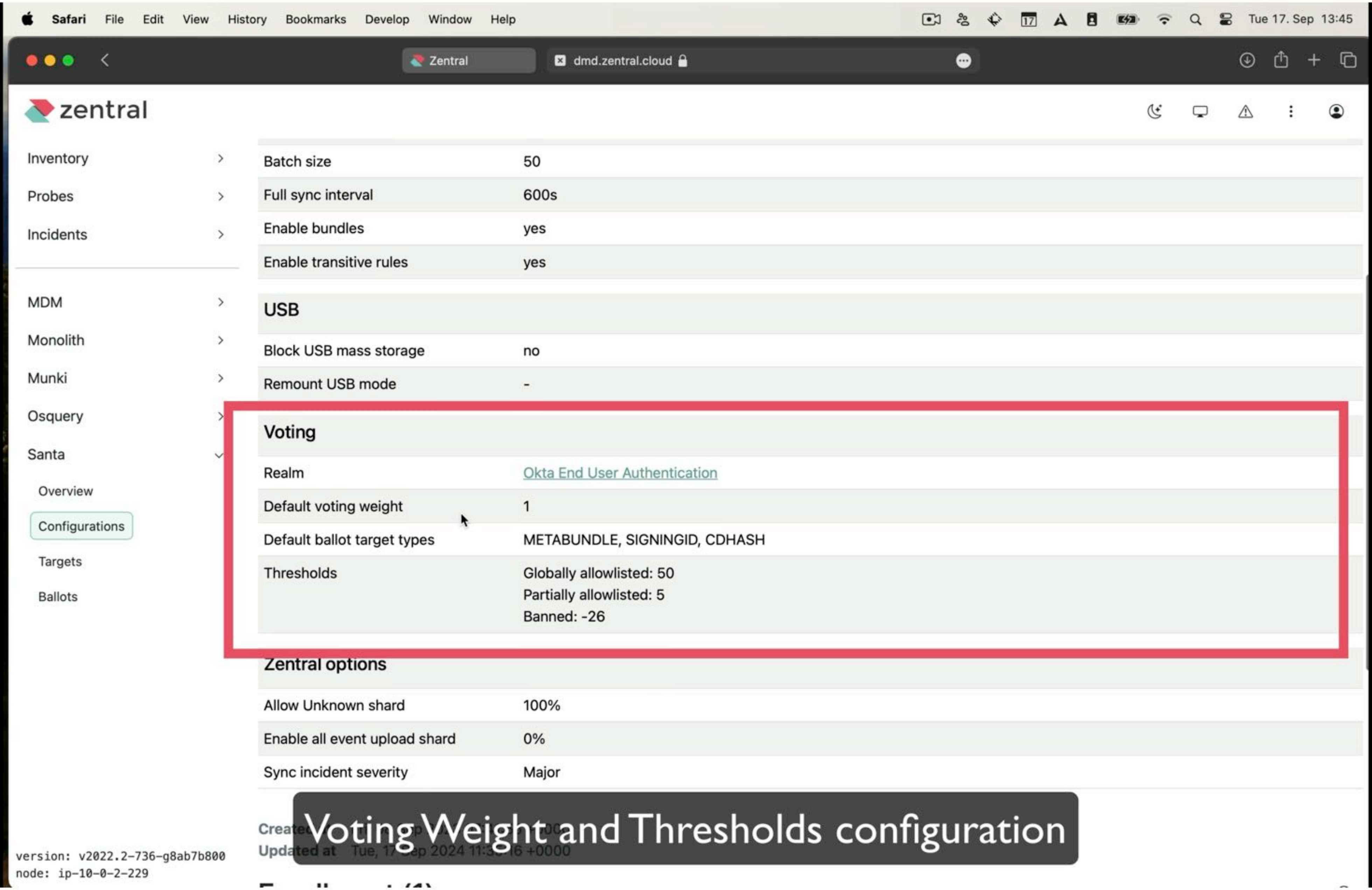


Cast a ballot

Configuration	Decision
Default	✓ No vote Upvote Downvote

```
version: v2022.2-736-g8ab7b800
node: ip-10-0-2-229
```

The administrator cast a ballot to "upvote"



Batch size	50
Full sync interval	600s
Enable bundles	yes
Enable transitive rules	yes

USB

Block USB mass storage	no
Remount USB mode	-

Voting

Realm	Okta End User Authentication
Default voting weight	1
Default ballot target types	METABUNDLE, SIGNINGID, CDHASH
Thresholds	Globally allowlisted: 50 Partially allowlisted: 5 Banned: -26

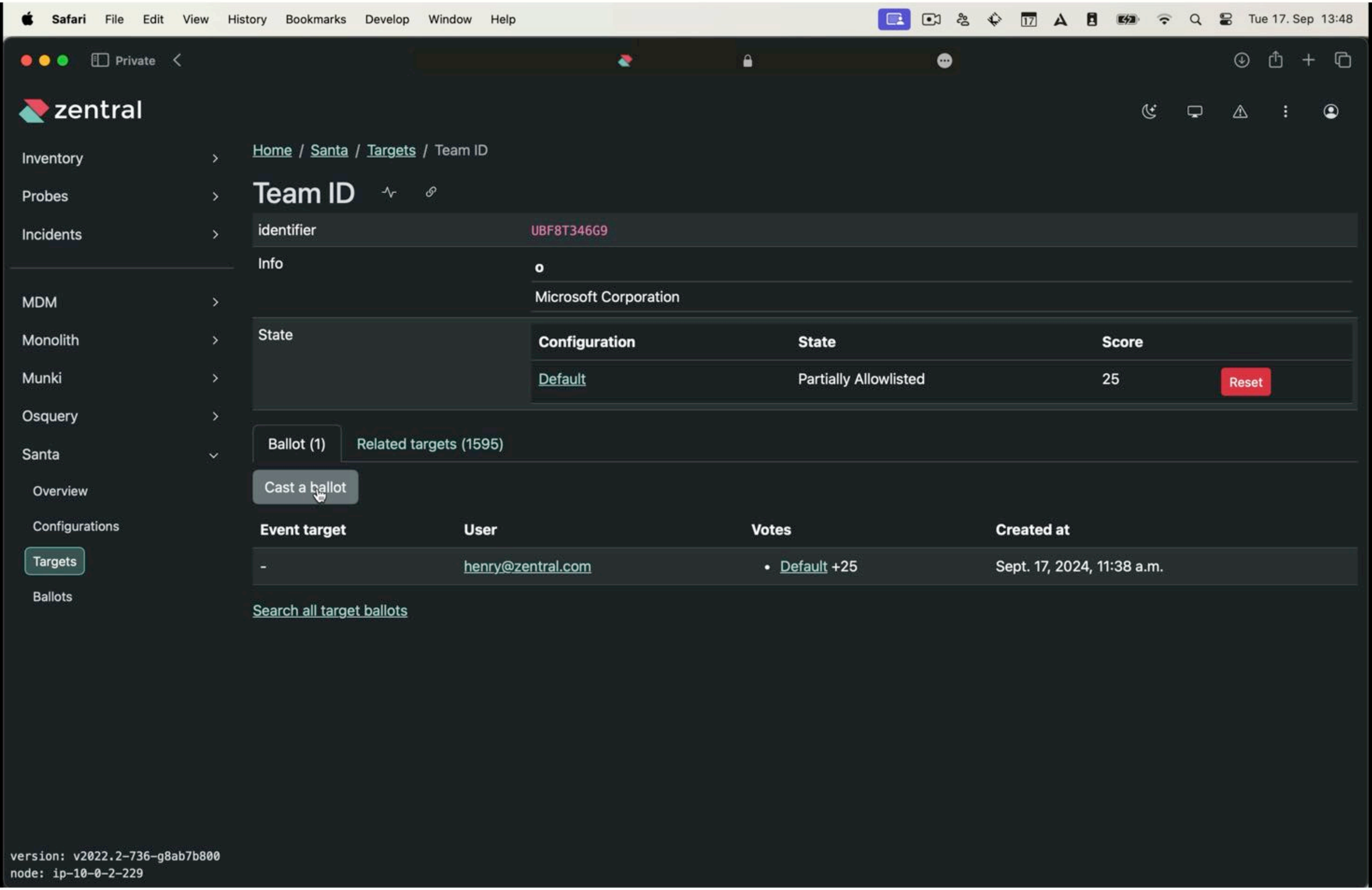
Zentral options

Allow Unknown shard	100%
Enable all event upload shard	0%
Sync incident severity	Major

Created [illegible]
Updated at Tue, 17 Sep 2024 11:30:16 +0000

```
version: v2022.2-736-g8ab7b800
node: ip-10-0-2-229
```

Voting Weight and Thresholds configuration



Home / Santa / Targets / Team ID

Team ID

identifier	UBF8T346G9
Info	o Microsoft Corporation

State

Configuration	State	Score	
Default	Partially Allowlisted	25	Reset

Event target	User	Votes	Created at
-	henry@zentral.com	• Default +25	Sept. 17, 2024, 11:38 a.m.

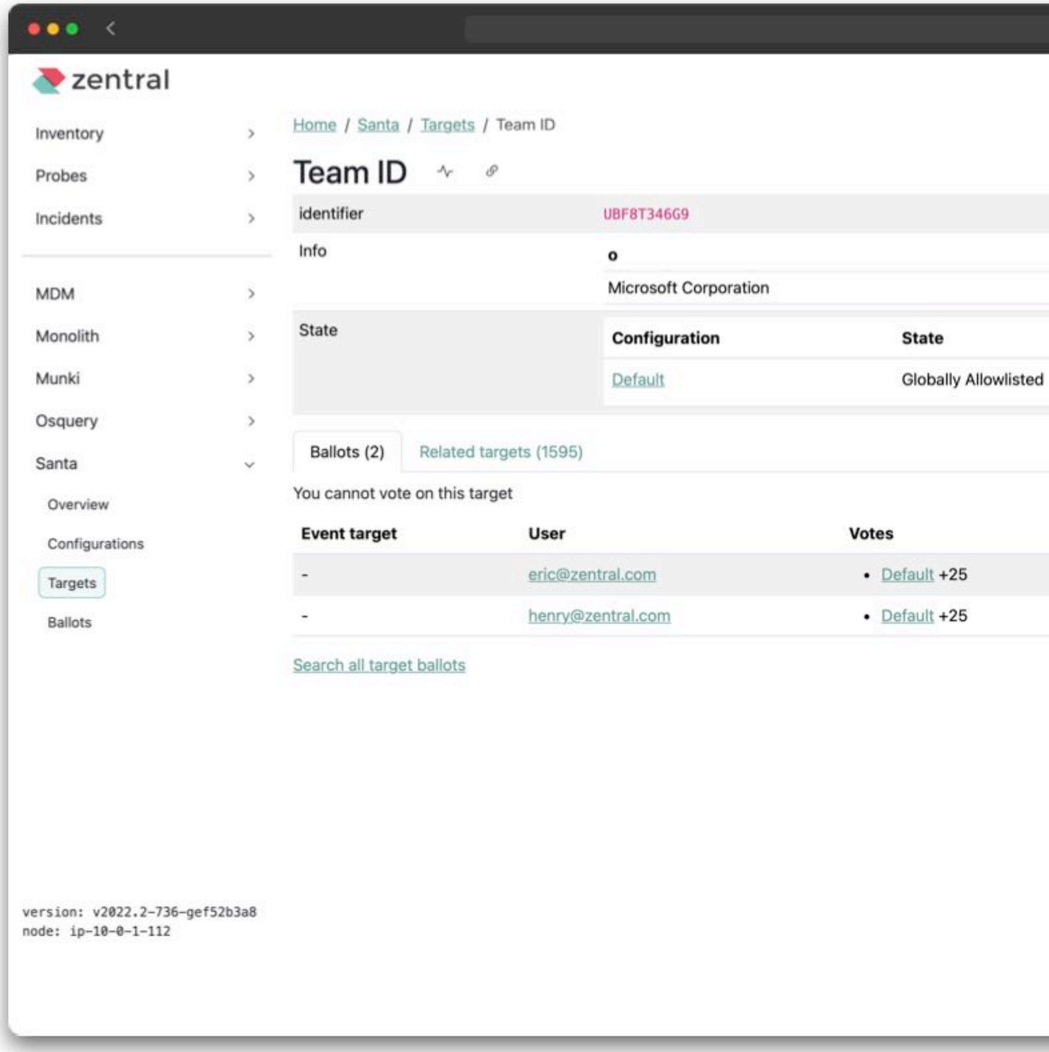
Search all target ballots

```
version: v2022.2-736-g8ab7b800
node: ip-10-0-2-229
```

zentral

Key takeaways:

- 🔨 Aggregates are for impact
- ✨ Stable identifiers are for lasting impact
- 👷 Flexible weights allow peer review



Home / Santa / Targets / Team ID

Team ID

identifier	UBF8T346G9
Info	o Microsoft Corporation
State	

Configuration	State
Default	Globally Allowlisted

Ballots (2) Related targets (1595)

You cannot vote on this target

Event target	User	Votes
-	eric@zentral.com	• Default +25
-	henry@zentral.com	• Default +25

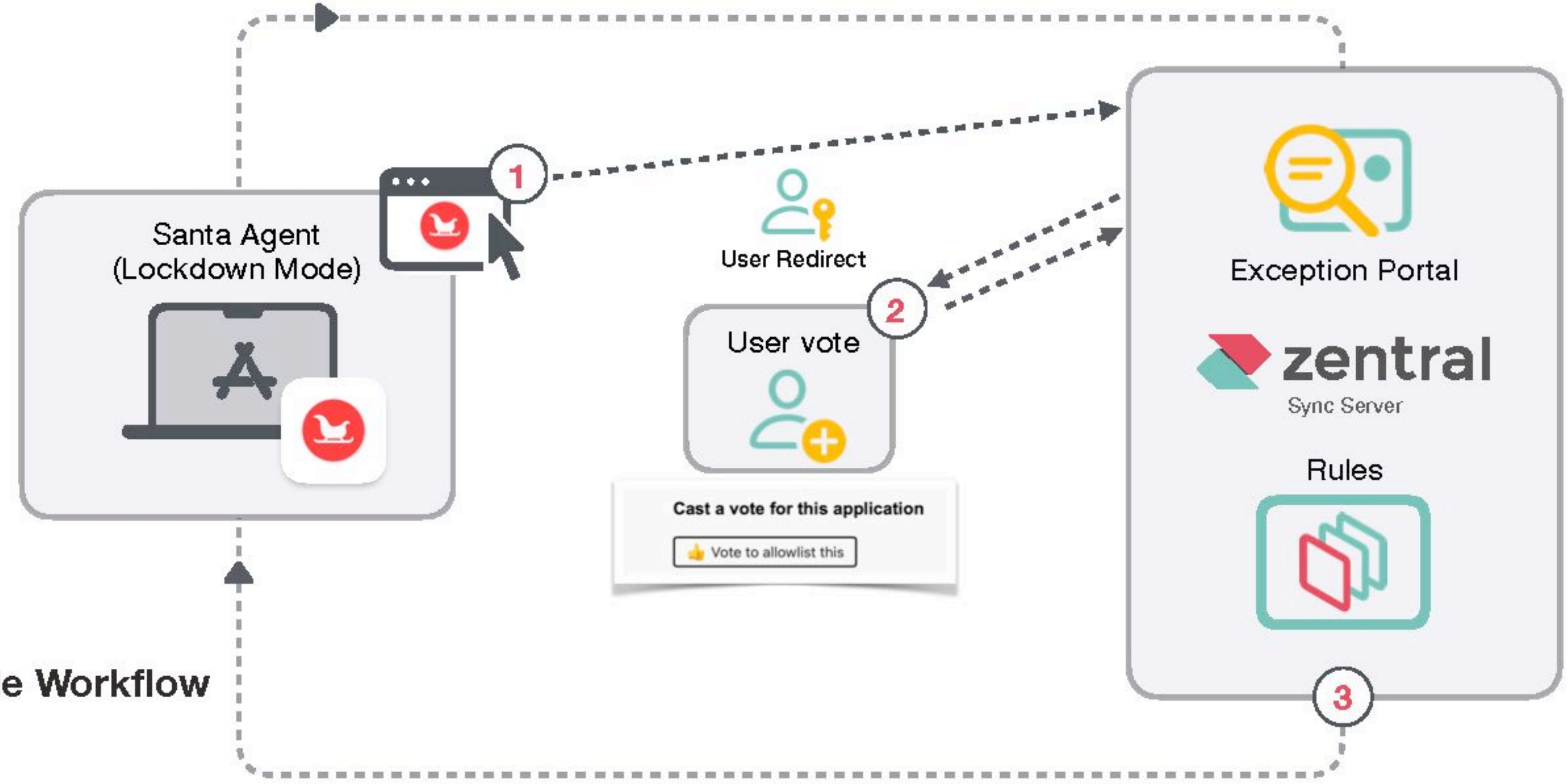
Search all target ballots

```
version: v2022.2-736-gef52b3a8
node: ip-10-0-1-112
```

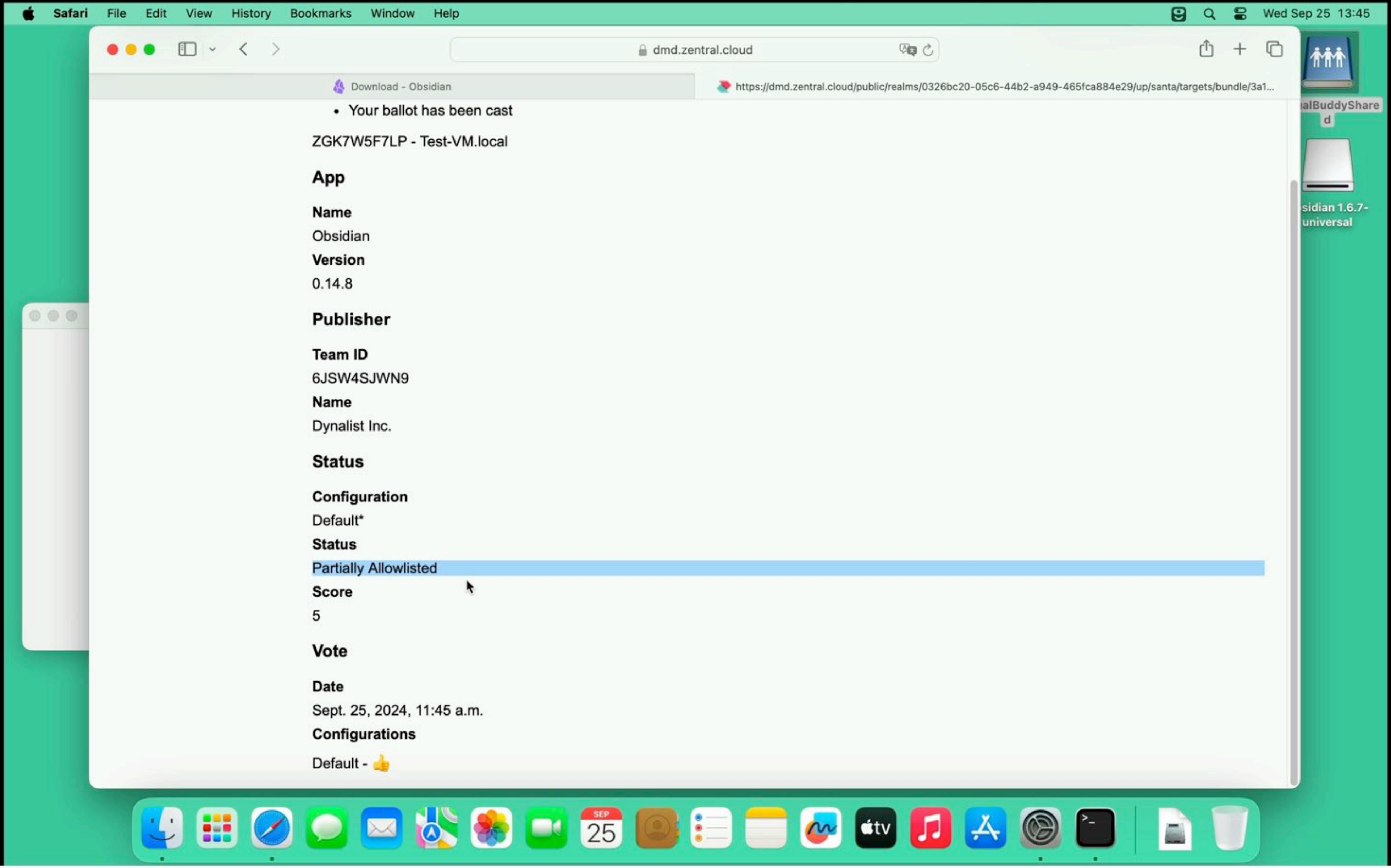
zentral

LOCKDOWN MODE:
Social-Voting System

zentral Managing Exceptions for Users



Lockdown Mode Workflow



- Your ballot has been cast

ZGK7W5F7LP - Test-VM.local

App

Name

Obsidian

Version

0.14.8

Publisher

Team ID

6JSW4SJWN9

Name

Dynalist Inc.

Status

Configuration

Default*

Status

Partially Allowlisted

Score

5

Vote

Date

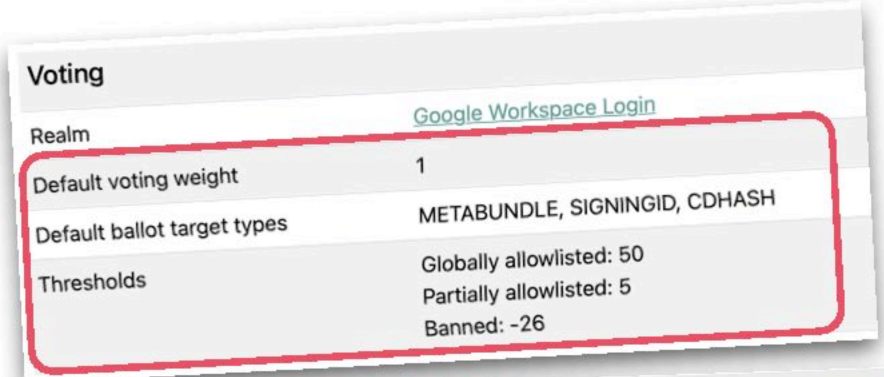
Sept. 25, 2024, 11:45 a.m.

Configurations

Default - 👍

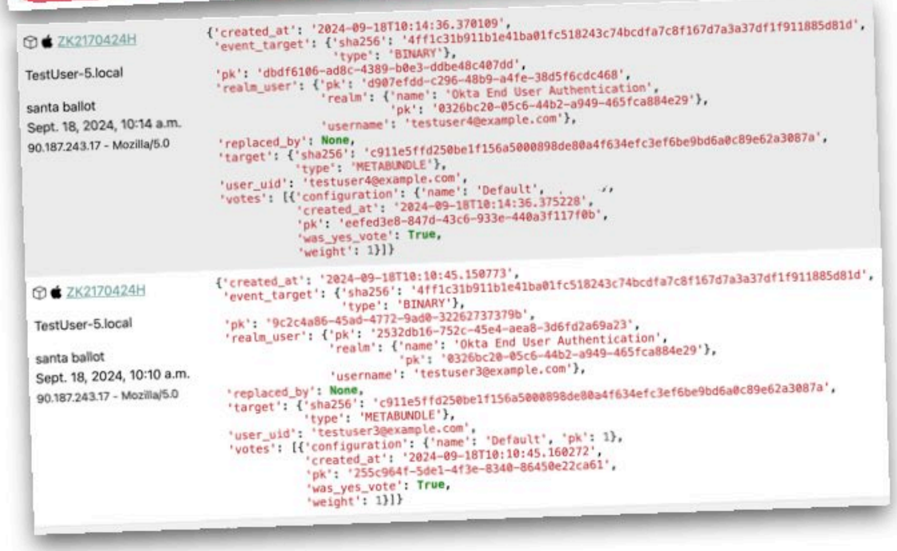
Key takeaways:

- 🔨 Social Voting
- ✨ Metabundles are persistent identifiers
- 🌟 Complete audit trail of events



Voting

Realm	Google Workspace Login
Default voting weight	1
Default ballot target types	METABUNDLE, SIGNINGID, CDHASH
Thresholds	Globally allowlisted: 50 Partially allowlisted: 5 Banned: -26



ZK2170424H

TestUser-5.local

santa ballot
Sept. 18, 2024, 10:14 a.m.
90.187.243.17 - Mozilla/5.0

```
{'created_at': '2024-09-18T10:14:36.370109',
 'event_target': {'sha256': '4ff1c31b911b1e41ba01fc518243c74bcdfa7c8f167d7a3a37df1f911885d81d',
                  'type': 'BINARY'},
 'pk': 'dbdf6106-ad8c-4389-b0e3-ddbe48c407dd',
 'realm_user': {'pk': 'd907efdd-c296-48b9-a4fe-38d5f6cdc468',
                'realm': {'name': 'Okta End User Authentication',
                          'pk': '0326bc20-05c6-44b2-a949-465fca884e29'},
                'username': 'testuser4@example.com'},
 'replaced_by': None,
 'target': {'sha256': 'c911e5ffd250be1f156a5000898de80a4f634efc3ef6be9bd6a0c89e62a3087a',
            'type': 'METABUNDLE'},
 'user_uid': 'testuser4@example.com',
 'votes': [{'configuration': {'name': 'Default', [illegible]
            'created_at': '2024-09-18T10:14:36.375228',
            'pk': 'eefed3e8-847d-43c6-933e-440a3f117f0b',
            'was_yes_vote': True,
            'weight': 1}]}
```

ZK2170424H

TestUser-5.local

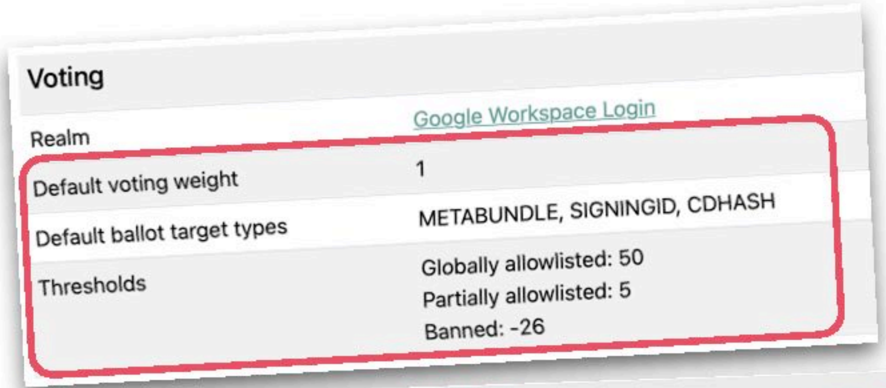
santa ballot
Sept. 18, 2024, 10:10 a.m.
90.187.243.17 - Mozilla/5.0

```
{'created_at': '2024-09-18T10:10:45.150773',
 'event_target': {'sha256': '4ff1c31b911b1e41ba01fc518243c74bcdfa7c8f167d7a3a37df1f911885d81d',
                  'type': 'BINARY'},
 'pk': '9c2c4a86-45ad-4772-9ad0-32262737379b',
 'realm_user': {'pk': '2532db16-752c-45e4-aea8-3d6fd2a69a23',
                'realm': {'name': 'Okta End User Authentication',
                          'pk': '0326bc20-05c6-44b2-a949-465fca884e29'},
                'username': 'testuser3@example.com'},
 'replaced_by': None,
 'target': {'sha256': 'c911e5ffd250be1f156a5000898de80a4f634efc3ef6be9bd6a0c89e62a3087a',
            'type': 'METABUNDLE'},
 'user_uid': 'testuser3@example.com',
 'votes': [{'configuration': {'name': 'Default', 'pk': 1},
            'created_at': '2024-09-18T10:10:45.160272',
            'pk': '255c964f-5de1-4f3e-8340-86450e22ca61',
            'was_yes_vote': True,
            'weight': 1}]}
```

zentral

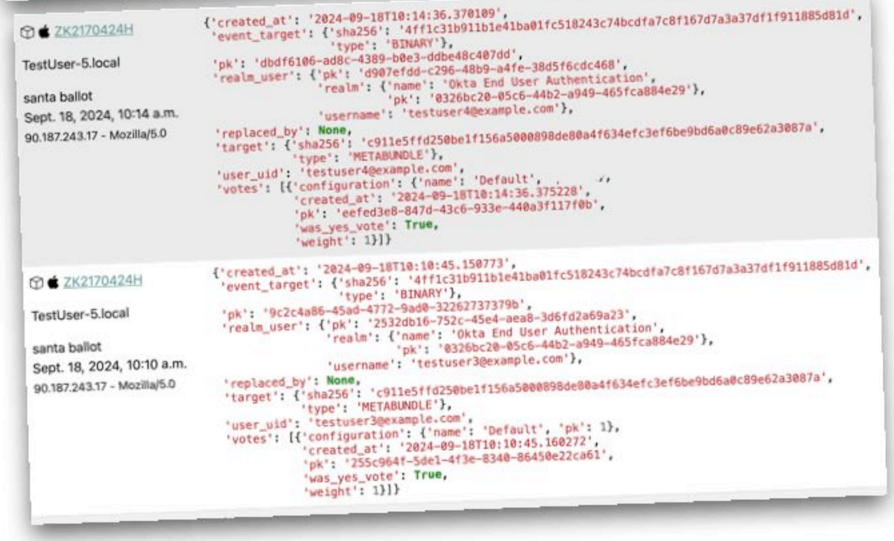
Summary

- ✅ Process from no allowlist to user voting
- 💫 What's next?
- 🚀 Zentral MDM + Zentral Santa (SaaS)



Voting

Realm	Google Workspace Login
Default voting weight	1
Default ballot target types	METABUNDLE, SIGNINGID, CDHASH
Thresholds	Globally allowlisted: 50 Partially allowlisted: 5 Banned: -26



ZK2170424H

TestUser-5.local

santa ballot
Sept. 18, 2024, 10:14 a.m.
90.187.243.17 - Mozilla/5.0

```
{'created_at': '2024-09-18T10:14:36.370109',
 'event_target': {'sha256': '4ff1c31b911b1e41ba01fc518243c74bcdfa7c8f167d7a3a37df1f911885d81d',
                  'type': 'BINARY'},
 'pk': 'dbdf6106-ad8c-4389-b0e3-ddbe48c407dd',
 'realm_user': {'pk': 'd907efdd-c296-48b9-a4fe-38d5f6cdc468',
                'realm': {'name': 'Okta End User Authentication',
                          'pk': '0326bc20-05c6-44b2-a949-465fca884e29'},
                'username': 'testuser4@example.com'},
 'replaced_by': None,
 'target': {'sha256': 'c911e5ffd250be1f156a5000898de80a4f634efc3ef6be9bd6a0c89e62a3087a',
            'type': 'METABUNDLE'},
 'user_uid': 'testuser4@example.com',
 'votes': [{'configuration': {'name': 'Default',
            'created_at': '2024-09-18T10:14:36.375228',
            'pk': 'eefed3e8-847d-43c6-933e-440a3f117f0b',
            'was_yes_vote': True,
            'weight': 1}]}
```

ZK2170424H

TestUser-5.local

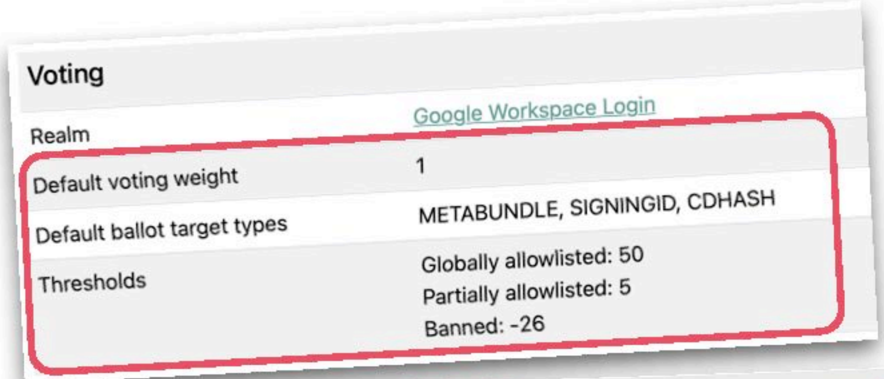
santa ballot
Sept. 18, 2024, 10:10 a.m.
90.187.243.17 - Mozilla/5.0

```
{'created_at': '2024-09-18T10:10:45.150773',
 'event_target': {'sha256': '4ff1c31b911b1e41ba01fc518243c74bcdfa7c8f167d7a3a37df1f911885d81d',
                  'type': 'BINARY'},
 'pk': '9c2c4a86-45ad-4772-9ad0-32262737379b',
 'realm_user': {'pk': '2532db16-752c-45e4-aea8-3d6fd2a69a23',
                'realm': {'name': 'Okta End User Authentication',
                          'pk': '0326bc20-05c6-44b2-a949-465fca884e29'},
                'username': 'testuser3@example.com'},
 'replaced_by': None,
 'target': {'sha256': 'c911e5ffd250be1f156a5000898de80a4f634efc3ef6be9bd6a0c89e62a3087a',
            'type': 'METABUNDLE'},
 'user_uid': 'testuser3@example.com',
 'votes': [{'configuration': {'name': 'Default', 'pk': 1},
            'created_at': '2024-09-18T10:10:45.160272',
            'pk': '255c964f-5de1-4f3e-8340-86450e22ca61',
            'was_yes_vote': True,
            'weight': 1}]}
```

zentral

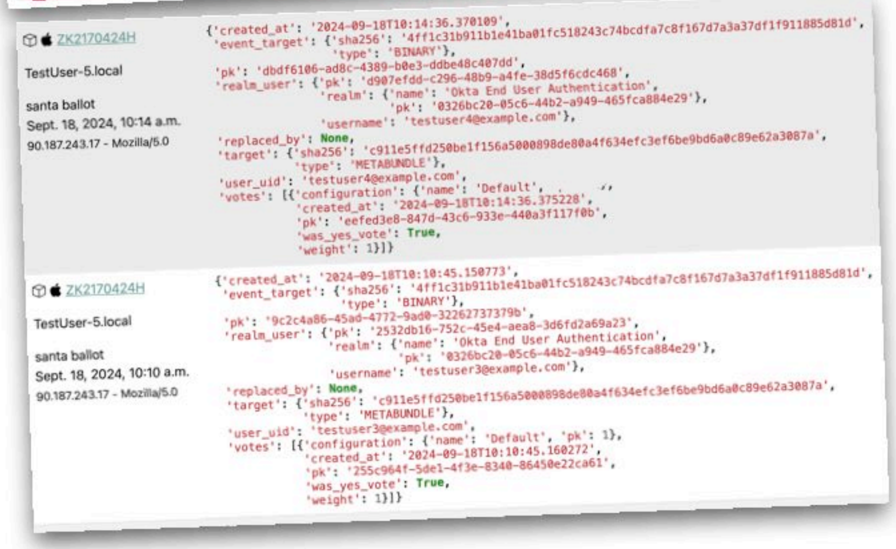
Summary

- ✅ Process from no allowlist to user voting
- 💫 What's next?
- 🚀 Zentral MDM + Zentral Santa (SaaS)



Voting

Realm	Google Workspace Login
Default voting weight	1
Default ballot target types	METABUNDLE, SIGNINGID, CDHASH
Thresholds	Globally allowlisted: 50 Partially allowlisted: 5 Banned: -26



ZK2170424H
TestUser-5.local
santa ballot
Sept. 18, 2024, 10:14 a.m.
90.187.243.17 - Mozilla/5.0

```
{'created_at': '2024-09-18T10:14:36.370109',
 'event_target': {'sha256': '4ff1c31b911b1e41ba01fc518243c74bcdfa7c8f167d7a3a37df1f911885d81d',
                  'type': 'BINARY'},
 'pk': 'dbdf6106-ad8c-4389-b0e3-ddbe48c407dd',
 'realm_user': {'pk': 'd907efdd-c296-48b9-a4fe-38d5f6cdc468',
                'realm': {'name': 'Okta End User Authentication',
                          'pk': '0326bc20-05c6-44b2-a949-465fca884e29'},
                'username': 'testuser4@example.com'},
 'replaced_by': None,
 'target': {'sha256': 'c911e5ffd250be1f156a5000898de80a4f634efc3ef6be9bd6a0c89e62a3087a',
            'type': 'METABUNDLE'},
 'user_uid': 'testuser4@example.com',
 'votes': [{'configuration': {'name': 'Default',
            'created_at': '2024-09-18T10:14:36.375228',
            'pk': 'eefed3e8-847d-43c6-933e-440a3f117f0b',
            'was_yes_vote': True,
            'weight': 1}]}
```

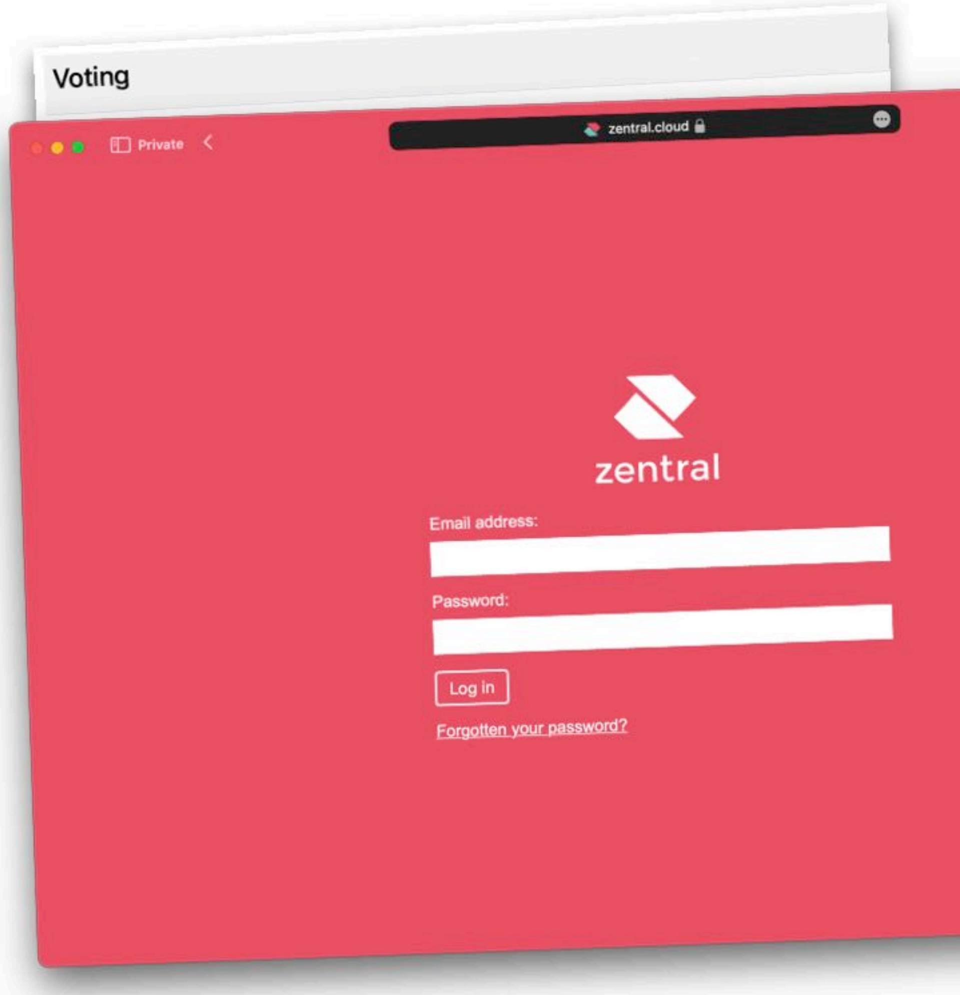
ZK2170424H
TestUser-5.local
santa ballot
Sept. 18, 2024, 10:10 a.m.
90.187.243.17 - Mozilla/5.0

```
{'created_at': '2024-09-18T10:10:45.150773',
 'event_target': {'sha256': '4ff1c31b911b1e41ba01fc518243c74bcdfa7c8f167d7a3a37df1f911885d81d',
                  'type': 'BINARY'},
 'pk': '9c2c4a86-45ad-4772-9ad0-32262737379b',
 'realm_user': {'pk': '2532db16-752c-45e4-aea8-3d6fd2a69a23',
                'realm': {'name': 'Okta End User Authentication',
                          'pk': '0326bc20-05c6-44b2-a949-465fca884e29'},
                'username': 'testuser3@example.com'},
 'replaced_by': None,
 'target': {'sha256': 'c911e5ffd250be1f156a5000898de80a4f634efc3ef6be9bd6a0c89e62a3087a',
            'type': 'METABUNDLE'},
 'user_uid': 'testuser3@example.com',
 'votes': [{'configuration': {'name': 'Default', 'pk': 1},
            'created_at': '2024-09-18T10:10:45.160272',
            'pk': '255c964f-5de1-4f3e-8340-86450e22ca61',
            'was_yes_vote': True,
            'weight': 1}]}
```

zentral

Summary

- ✅ Process from no allowlist to user voting
- 💫 What's next?
- 🚀 Zentral MDM + Zentral Santa (SaaS)



zentral

· MAC · SYS · ADMIN ·
GOTHENBURG

✨ Thank You ! ✨

www.zentral.com