

# Configuration Management

## Capability Brief

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through SEWP V; NNG15SC03B and NNG15SC27B, ITES-SW2 Contract W52P1J-20-D-0042, NASPO ValuePoint Master Agreement #AR2472, TIPS Contract #220105 and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Acsense, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit [carahsoft.com](https://carahsoft.com)



Explore More Resources:  
[carah.io/learn](https://carah.io/learn)



Join Events & Webinars:  
[carah.io/acsenseevents](https://carah.io/acsenseevents)



Discover Technology Solutions:  
[carah.io/acsense](https://carah.io/acsense)



Learn About Procurement:  
[carah.io/acsensecontracts](https://carah.io/acsensecontracts)



Connect With Our Team:  
[acsense@carahsoft.com](mailto:acsense@carahsoft.com)  
857-499-4514

# Configuration Management

Continuous change tracking, drift detection, and one-click rollback for your IAM tenant. Know exactly what changed, when, and why, across every configuration.

Identity is Tier-0 infrastructure. Every employee, application, partner, and AI agent authenticates through it. When configurations drift, accumulate undocumented changes, or break silently, the consequences cascade. Authentication failures. Compliance gaps. Security blind spots.

Identity providers log events, but they do not manage configurations. There is no native way to track every change across tenants, detect drift from a known-good baseline, or roll back a configuration change without manual reconstruction.

Acsense Configuration Management closes the gap. Continuous change tracking across every IAM object, automated drift detection, dependency mapping, and one-click rollback to any prior state.

One platform. Any IDP. Tenant-level configuration management from a single change to a full cross-tenant promotion, without per-IDP tooling or manual change logs.

**≤ 10 min**

Drift detection across every config

**One-Click**

Rollback to any prior state

**IDP-Agnostic**

Tenant-level management, any IDP

Drift Detection

Baselines

Change Tracking

Rollback

Policy States

Attribute Differ...

**CONTINUOUS**  
**Configuration Control**

Cross-Tenant

Promote Chan...

Dependency M...

Bi-directional I...

Tenant Compare

Version Control

*"Identity providers guarantee their own uptime, not your ability to manage or recover your tenant configuration. The configuration visibility gap is the single most overlooked operational risk in enterprise IAM."*

Reflecting the [AWS Shared Responsibility Model](#)

**22%** of breaches start with stolen credentials. Credential-based breaches take **246 days** on average to identify and contain. Identity attacks rose **32%** in H1 2025.

SOURCES: VERIZON DBIR 2025 · IBM COST OF A DATA BREACH 2025 · MICROSOFT DIGITAL DEFENSE REPORT 2025

## Managing IAM configuration takes more than an audit log

IAM environments change constantly. Admins update policies, onboard apps, rotate roles, push workflows. AI agents and service principals add thousands of non-human identities, each with its own bindings and tokens. Without continuous tracking, small changes accumulate into large, undocumented drift from the intended configuration baseline.

Identity providers give you a record of what happened. Acsense gives you the operational layer to act on it: a change promotion workflow, a test-and-validate path, dependency mapping, and one-click rollback. The complete configuration management stack your IAM team needs, in one platform.

## How Acsense Configuration Management works



### STAGE 1

#### Clone + Establish Testing Environment

Clone your production tenant to create a testing environment that mirrors production.  
Validate changes before anything touches production.



### STAGE 2

#### Test, Approve & Promote

Test in a production-consistent environment. Compare sandbox against production state.  
Request CAB approvals and promote validated configurations with full dependency checks.



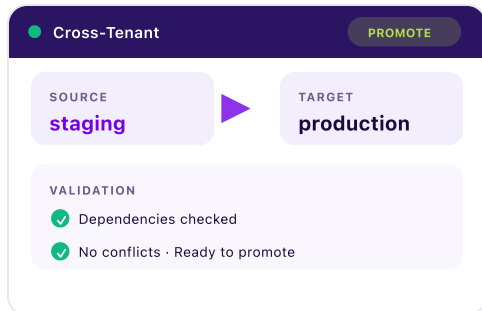
### STAGE 3

#### Track, Sync & Deploy

Every configuration change tracked with full context. Bi-directional ITSM integration keeps changes and tickets in sync automatically or on a defined schedule.

# Manage every change, across every tenant

Acsense Configuration Management operates at the granularity the change actually requires. Clone a tenant environment for safe testing. Compare your sandbox against production state. Roll back a policy. Promote a validated configuration across tenants. Each action is dependency-aware so relationships stay intact.



**Cross-Tenant** PROMOTE

SOURCE: **staging** → TARGET: **production**

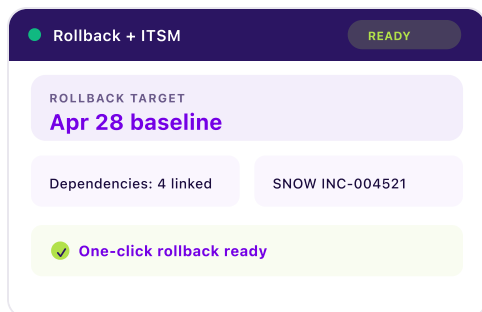
VALIDATION

- ✓ Dependencies checked
- ✓ No conflicts - Ready to promote

## Tenant Cloning + Testing Environment

Getting your sandbox to match production is the first problem every IAM team has to solve. Acsense clones your entire tenant configuration: policies, apps, groups, roles, MFA rules, and all their dependencies into an isolated testing environment. The clone is a one-time infrastructure setup step; once your testing environment is in place, validated changes promote in minutes and your RTO and RPO targets are set from there. Test new features, policy changes, and onboarding workflows in an environment consistent with production. No surprises when you promote.

Production-consistent clone    Isolated test env    Full dependency copy



**Rollback + ITSM** READY

ROLLBACK TARGET: **Apr 28 baseline**

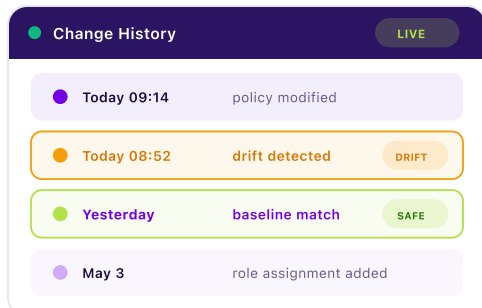
Dependencies: 4 linked    SNOW INC-004521

✓ One-click rollback ready

## Multi-Tenant Management + Cross-Tenant Promotion

Manage configurations across multiple tenants from a single console. Build and maintain a Dev, Test, and Production environment structure with consistent configuration across all three. Promote validated configuration changes across tenants with full dependency checks intact. Full Tenant Replication makes standing up new environments fast, accurate, and repeatable.

Cross-tenant promotion    Tenant replication    Single console



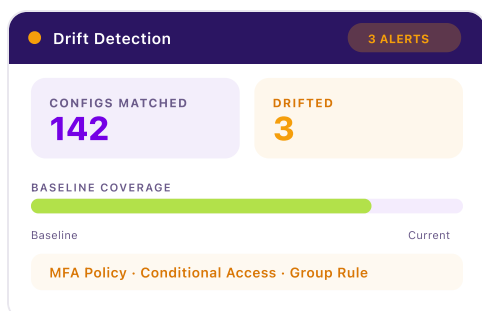
**Change History** LIVE

- Today 09:14 policy modified
- Today 08:52 drift detected DRIFT
- Yesterday baseline match SAFE
- May 3 role assignment added

## Bi-Directional ITSM Integration + CAB Approval

Every IAM configuration change linked to an ITSM ticket. Every approved ticket triggering the right IAM change. Bi-directional integration with ServiceNow and Jira keeps changes and tickets in sync automatically or on a defined schedule. CAB approval workflows built in: request approval, get the sign-off, deploy with confidence. Change management compliance without the manual overhead.

ServiceNow    Jira    CAB approval    Auto-sync



**Drift Detection** 3 ALERTS

CONFIGS MATCHED: **142**    DRIFTED: **3**

BASELINE COVERAGE

Baseline Current

MFA Policy · Conditional Access · Group Rule

## Configuration Change History + One-Click Rollback

Every IAM configuration change tracked with full context: who changed what, when, and exactly how the state differs from before. Built for operational visibility, audit evidence, and incident investigation. Roll back any configuration change to any prior state with one click. Dependency-aware rollback means Acsense understands the relationships between objects (a group referenced by a policy, an app binding tied to a role, a token scoped to a service principal) and restores them together. No broken dependencies, no manual reconstruction.

Full change log    Before/after diff    One-click rollback    Dependency-aware

## Real scenarios. Real control.

Configuration Management operates at the granularity the change actually requires. Four scenarios from real IAM environments. Each at the tenant level, regardless of which IDP is running underneath.

### WHEN THIS HAPPENS

#### New config needs to go from staging to production

**Acsense:** Full Tenant Replication clones the production tenant into an isolated test environment. Changes are validated before anything touches production.

Test confidently. No production risk.

### WHEN THIS HAPPENS

#### Team needs a safe environment to test policy changes

**Acsense:** Cross-Tenant Change Promotion validates the config in staging, checks dependencies, and pushes to production with an audit trail.

No manual replication. No copy-paste errors.

### WHEN THIS HAPPENS

#### Change requires CAB approval before going to production

**Acsense:** ITSM integration creates the ticket automatically. CAB reviews and approves. Acsense promotes the configuration on approval with dependency checks and a full audit trail.

Change management compliance built in.

### WHEN THIS HAPPENS

#### Auditor asks who changed what, when, and why

**Acsense:** Configuration Change History produces the full change record: before/after state, timestamp, actor, and ITSM ticket reference.

Audit evidence on demand. No log archaeology.

## Why Acsense for Configuration Management



### Purpose-built for cloud IAM

Architected from the ground up for cloud-native IAM. Every capability built around how Okta and Entra ID actually work, optimized for cloud identity infrastructure from the ground up.



### Bi-directional ITSM integration

Changes and tickets stay in sync automatically or on schedule. ServiceNow and Jira. Change management compliance without the manual overhead.



### One-click rollback, dependency-aware

Roll back any change with full dependency context. Relationships between objects come back intact, no manual reconstruction.



### NHI & AI agent coverage

Service principals, API tokens, and agent bindings are tracked, diffed, and rollback-ready alongside human identity configurations.



### Clone, Test & Promote

Clone your production tenant into a consistent testing environment. Validate changes before anything touches production. Promote with full dependency checks, no ad hoc copy-paste, no configuration surprises.



### Dependency-aware change promotion

Promote validated configurations across tenants with full object relationship checks. Groups, policies, app bindings, and role assignments move together. No broken dependencies, no manual reconstruction.



### IDP-agnostic by design

Acsense manages your tenant configuration the same way regardless of which IDP runs it. One process, one console, one change history.

## Ready to manage every IAM configuration change?

See Acsense Configuration Management in action on your IAM tenant.

[Request a demo](#)

# Built for the IAM admin, and everyone who depends on identity

Configuration Management is the operational backbone. The platform serves the people who keep IAM running every day, and the leaders who carry the risk when it doesn't.



### IAM Administrators

You own IAM configuration. Every change goes through you. Acsense gives you the operational layer to do it properly: clone environments for safe testing, track every change with full context, promote to production with dependency checks, and roll back anything with one click. Works alongside your existing IaC tooling. Acsense tracks all configuration changes in Okta regardless of how they were made, IaC-driven or otherwise, so your baseline stays accurate. Stop reconstructing change sequences from raw logs.



### IT & Operations Leaders

Multi-tenant management from a single console. Cross-tenant promotion with dependency checks. Configuration consistency across staging, production, and DR environments.



### Security & CISO

Complete change history for audit and incident response. Every configuration change tied to an actor, a timestamp, and an ITSM ticket. Drift detection as an early warning for unauthorized changes.



### AI & ML Leaders

Service principals, API tokens, and agent bindings are tracked, diffed, and rollback-ready alongside human identity configurations. As your NHI surface grows, configuration management scales with it.

#### ABOUT ACSENSE

Acsense is the IAM Resilience Platform that protects, recovers, and continuously validates enterprise identity infrastructure at scale. The platform delivers Backup & Recovery, Configuration Management, Disaster Recovery, and Compliance & Assurance across Okta and Microsoft Entra ID, from a single purpose-built product. Acsense serves security-first enterprises and federal agencies across financial services, healthcare, critical infrastructure, public sector, and technology globally. Learn more at [acsense.com](https://acsense.com).