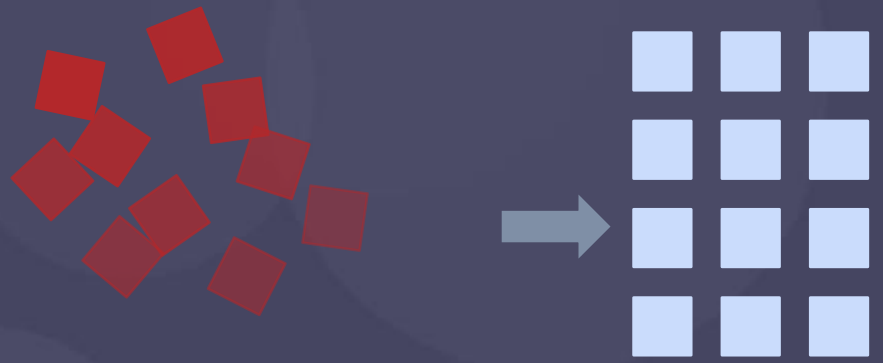
QUEST INFOCUS 2026 · JD EDWARDS TECHNICAL CONFERENCE

Kill the Chaos: A No-Nonsense JDE Security Overhaul

How we rebuilt JDE security with cleaner roles, stronger controls, and fewer surprises

Prinova
Melanee Melia · Program Manager

ERP Suites
Brian Connor · Director – JDE security



WHERE WE ARE GOING

Agenda

01 **Where we started**
Inherited security, and why it compounds

02 **Scope and guardrails**
What we chose to fix, and what we deferred

03 **Dual security tables**
The decision, the build, the promotion process

04 **Role and security cleanup**
Duplicate security, *PUBLIC

05 **Inactive user cleanup**
Two automated processes, 1,800 accounts to under 600

06 **Lessons learned**
What we would do differently, and what you can take with you

WHO IS TALKING

About Prinova and ERP Suites

P

THE CUSTOMER

Prinova

- Global supplier of ingredients, nutrient premixes, and contract manufacturing
- A NAGASE Group company; US operations headquarters in Illinois
- Runs JD Edwards EnterpriseOne as the system of record

E

THE PARTNER

ERP Suites

- JD Edwards consulting, managed services and CNC
- Headquartered in Cincinnati, Ohio; 20+ years with JDE
- Security, compliance and risk advisory practice

The engagement: a joint security overhaul beginning October 2025 - customer-owned, partner-guided, still running today.

WHERE WE STARTED

Nobody designed this. It accumulated.

Nine years of reasonable decisions, none of them revisited.

Roles multiplied	Every new requirement got a new role. No roles were ever retired.
Security was copied, not designed	New users cloned from whoever sat nearby. Mistakes inherited mistakes.
Implementation was an afterthought	Went live and then tried to apply security to roles without a master design of assignment
Two environments, one set of habits	Only the F00950 was split just before the project started - the process around it was not.

WHERE WE STARTED

What that actually cost us

Duplicate security

A change made in Non-Prod during testing may not make it to Prod, making it difficult to identify cause of environments behaving differently.

Manual dual maintenance

Every change keyed twice, by hand, in two environments.

Silent misses

Changes documented thru email communication. Some never made it to production.

Roles nobody owned

Roles were designed for job titles so sometimes granted more access than necessary

1,800+ user accounts

LDAP discontinued access, but they still showed as active users making it difficult to tell who needed analyzed for access.

Unusable SoD reporting

Runtimes and output volume large enough that results would not have been usable.

SCOPE

Define the project up front

The foundation of our success was bringing our teams together and agreeing on a clear plan with shared objectives.

1 IN SCOPE

- Install ALLOut Security at the current release
- Analyse existing security at the role level
- Remove duplicate security records
- Move common access to *PUBLIC
- Dual tables for UDO and change control
- Inactive user identification and removal

2 DELIVERABLES

- Annual user access review process
- Profile management policy
- Periodic profile and role review cycle
- Customer training and handover
- Department and job title on every active user

3 PARKING LOT

- Everything discovered mid-project that was real, but not this project
- Revisited at phase close, not in flight
- Kept the team from chasing every finding

FOUNDATION

Nail down the basics

1

Install ALLOut Security at the current release

We took the newest version available at project implementation. Later releases removed constraints we would otherwise have designed around - the web client fix for change control being the clearest example.

2

Analyse existing security at the role level

Cleaning up what was on the role level and removing duplication of security ensured we were looking at less lines when it came down to analyzing and designing a go-forward plan

3

Confirm the reporting you will use to prove progress

Security history was already enabled, which is what made the inactive-user work possible later. If it is not on in your environment, turn it on and then wait - you cannot analyse sign-on history you never collected.

FOUNDATION

Two cleanups that pay for themselves

Remove duplicate security records

- Run the duplicate security report to find records granting the same thing twice
- Validate every candidate against the role and the business requirement
- Object-level and version-level differences need a human decision, not a bulk delete

Move common access to *PUBLIC

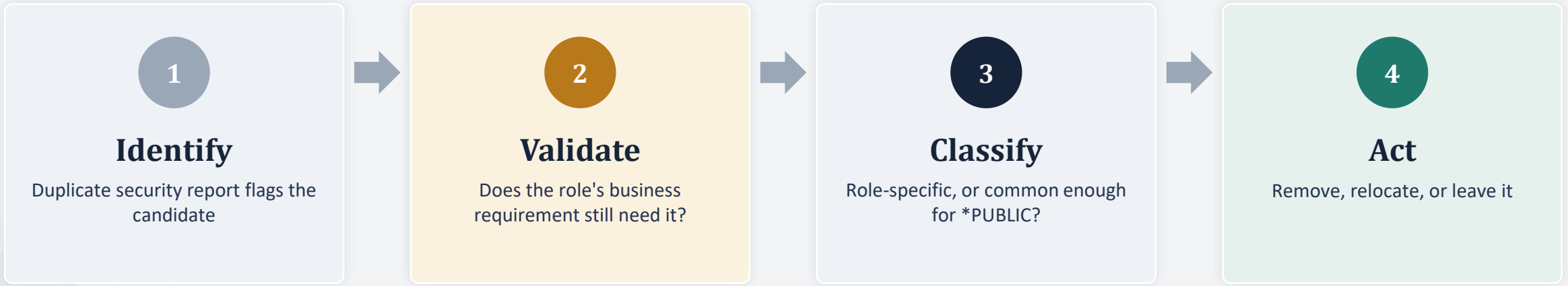
- Access every role needed anyway does not belong in every role
- Shrinks F00950 and shortens the list you have to reason about
- Directly reduces SoD report runtime and output volume

The payoff nobody advertises: smaller, cleaner security means role evaluation time is reduced and future SOD reports will run quicker and be easier to read.

FOUNDATION

How a security record earns its place

Every candidate record goes through the same four gates. Nothing gets deleted in bulk.



The gate that saves you

Gate 2. A report can tell you a record is redundant. Only the business can tell you the role still needs the access at the version level. Skipping validation is how a cleanup project becomes an outage.

01

SECTION ONE

Dual security tables

Why we split them, what it took, and how promotion works day to day.

F00950 · F00950W · AOS change control

THE DECISION

We had the split. We did not have the control.

Before

Split tables, manual everything

- F00950 already split between production and non-production
- Security maintained by hand in both - twice the work, twice the error surface
- Project-based work made the workload spike unmanageably
- Changes tracked in paper documentation, so some daily maintenance never reached production

The decision

Dual tables plus real change control

- Extend the split to UDO security so the same discipline covers both
- Use change control to cut the duplicate keying entirely
- Get a system-generated record of what changed, not a document someone remembered to update
- Make promotion an event with an approver, not a Tuesday habit

ARCHITECTURE

What the split actually looks like

NON-PRODUCTION

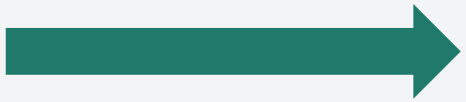
Where change happens

F00950 Application security

F00950W UDO security

+ partial PD path code installed so AOS can reach production

PROMOTE



delta only

PRODUCTION

Changes only arrive by promotion

F00950 Application security

F00950W UDO security

No direct maintenance. No exceptions.

How AOS decides what to move: it reads the security tables in both environments, computes the delta, and promotes only the differences from non-Production to Production, **or** from Production to non-Production.

THE BUILD

What it takes to get there

None of these are hard. All of them are easy to miss when you scope the work.

1

Split F00950W as well as F00950

AOS promotion covers UDO security, so the UDO table has to be split the same way. Splitting one and not the other leaves you half in change control and half in the old habit.

2

Install a partial PD path code on the non-production servers

AOS has to be able to connect to the production security setup from non-production. That connectivity is a CNC task, not a security task, and it belongs in your project plan early.

3

Get current on the ALLOut release

Change control initially required a fat client. That was addressed in AOS version 4.1.11 so it runs on the web. Confirm the version you are on before you design your process around a constraint that no longer exists.

THE BUILD

Configuring AOS change control

What the tool gives you

- Interactive screen drives promotion - you pick the scope
- Select an individual role, a range of roles, or all roles
- Output shows security settings before and after the promotion
- Proof mode reports the delta between environments without changing anything

What we made of it

- Promotion is by role, which keeps the blast radius legible
- The before/after output is the artefact your auditor wants
- Proof mode is not optional in our process - it is the first step every time
- Approvals gate what is allowed to move at all

PROMOTION

The promotion process, end to end

1. **Change made** — in non-production
2. **Test/Approved** — security change validated and approval recorded
3. **Proof run** — delta reported, nothing moved
4. **Review delta** — confirm you own every line
5. **Promote by role** — individual, range, or all
6. **Before/after output** — filed as evidence

Steps 3 and 4 are the whole safety model

Proof mode tells you what would move. Reviewing it tells you whether you meant to move it. If you skip either, promotion is just a faster way to make the same mistake in production.

Three common pitfalls to avoid

The demote button

The same screen that promotes can demote. It sits next to the option you want. Read the screen before you submit - every time, including the hundredth time.

Running wide open

You can promote all roles in one action. If you do, you own every change in that delta, including the ones a colleague made and did not tell you about. This is why we review and approve.

File the paper trail

The output is generated by the promotion. Keep the generated artefact and file it for future reference if a question arises.

Bonus Tip

Verify effected users have correct roles based on implemented changes to avoid a gap in access.

PROMOTION

Approvals: only approved changes move

- Security change approval is configured so unapproved changes are not eligible for promotion
- The gate sits in the tool, not in someone's memory of an email thread
- Approval and promotion are separate acts, performed by people who can be named afterwards
- The generated before/after output closes the loop: requested, approved, applied, evidenced

WHY THIS MATTERS

Error proof your process

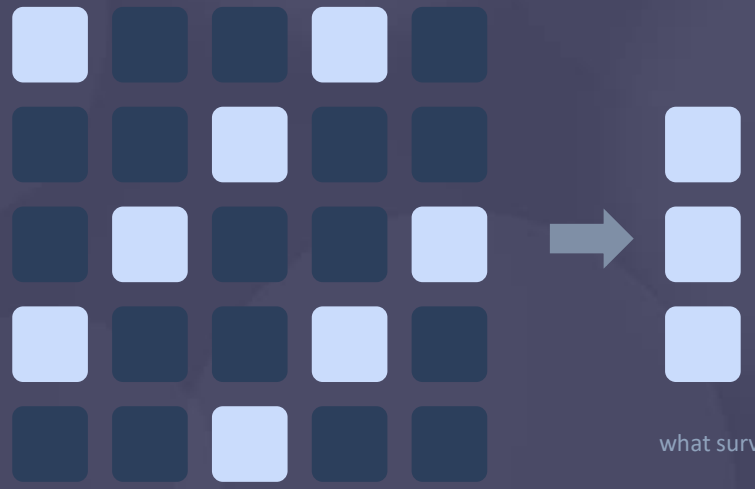
A control your tooling enforces, and evidences without being asked, is the one that survives an audit and a staff change.

02

SECTION TWO

Role and security cleanup

Finding what is redundant, what is unused, and what was quietly wrong all along.



25 roles reviewed

what survives review

ROLE CLEANUP

Validate before you delete

The duplicate security report finds candidates. It does not make decisions.

1	**Run the duplicate security report**	Identifies records that grant the same access more than once.
2	**Validate against role and business requirement**	The report cannot see intent. Someone who understands the job has to.
3	**Review object-level against version-level**	Same application, different versions is not a duplicate. This is where careless cleanups break things.
4	**Then remove**	With the business decision recorded, not assumed.

ROLE CLEANUP

The LDAP problem we found by accident

One bad source profile, propagated by a routine provisioning step, for an unknown length of time.

What was happening

- An administrator set up user security for a new account
- The new user signed in to complete LDAP provisioning
- The LDAP source had been assigned the wrong roles
- Those wrong roles were copied straight onto the new user
- Repeat, quietly, until somebody notices

The cost

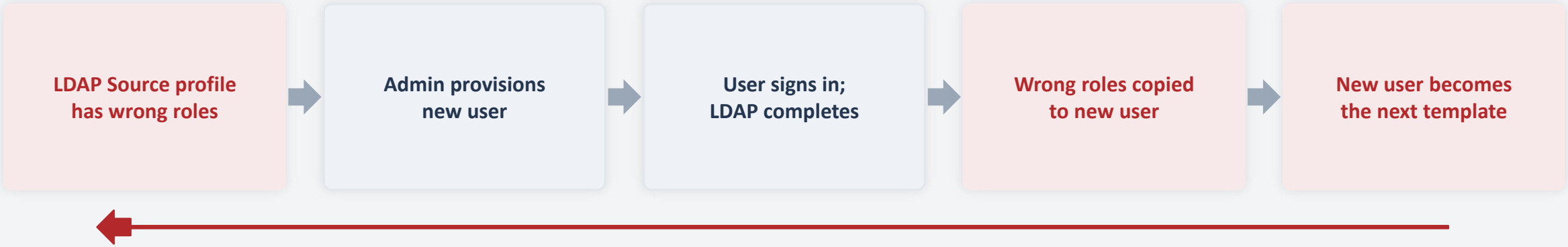
Extensive cleanup once discovered, across every account provisioned through the bad path.

The fix that lasts

A DAS report that alerts when wrong roles are assigned, so the next occurrence is caught in days rather than years.

ROLE CLEANUP

How one wrong profile becomes fifty



the loop: every bad account is a fresh source of bad accounts

DETECT

DAS alert fires when roles are assigned outside the expected set

CORRECT

Cleanup scoped to accounts provisioned through the bad path

PREVENT

Review roles assigned by LDAP based on a date after cleanup occurred should prove no additional roles have been assigned thru this method.

ROLE CLEANUP

Finding roles that no longer earn their keep

AOS WORKBENCH

Unused roles

- Identify roles with no meaningful assignment or use
- Removal candidates, validated with the business before deletion
- Fewer roles means role review becomes a task someone can finish

AOS ROLE COMPARISON

Redundant roles

- Compare similar roles against each other to expose overlap
- Decide which one survives and which gets folded in
- Comparison output is the evidence for the decision, not a suggestion to accept blindly

ROLE CLEANUP

Removing FastPath access for non technical users

One more level of buttoning up access

When this can be an issue

- A user could travel to an application/version not intended for their business process
- Users with *All in a particular category could explore applications outside their assigned duties
- If a menu path is updated to a new version, FastPath users will continue to travel to the prior version

Evaluate

- What roles still have FastPath
- Users with those roles

Team Communications

Users were notified of the upcoming change and advised to provide applications accessed by FastPath so it could be added to a menu path.

Why we could move fast on user cleanup

Three conditions were already true. Without them this work is much harder.

1

LDAP authentication

Users need a live network account to sign in. A stale JDE account with no network account is a licensing and hygiene problem, not an open door.

2

Security history enabled

Sign-on history was already being collected, so we had the data to identify who had genuinely stopped using the system.

3

An active-user report

AOS reporting surfaced accounts with no sign-on in over 270 days, which gave us a defensible starting list.

Be honest about this: if you have not enabled security history, you cannot do this work today. Turn it on and come back in nine months.

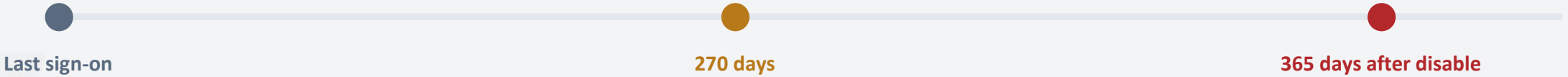
USER CLEANUP

Two processes, both with a proof mode

PROCESS 1

Disable after 270 days without sign-on

Runs in proof mode first, then final. Exceptions applied before final.



Why we keep the address book record

Historical transactions still reference it. Delete the address book record and you break the audit trail you spent the whole project building.

PROCESS 2

Delete disabled accounts after 365 days

Removes everything except the address book record. Proof mode, then final.

USER CLEANUP

Managing as we move forward

1 **Executives**

Sign on rarely, need the account when they do. On the exception list, reviewed rather than auto-disabled.

2 **DAS users**

Hold an active JDE account but never sign on to JDE. The active-user report flags them, so the output requires a human review pass for DAS access before anything is disabled.

3 **Leavers**

HR notifies, the account is disabled immediately. The 365-day delete process picks it up later without anyone having to remember.

RESULTS

Where the numbers landed

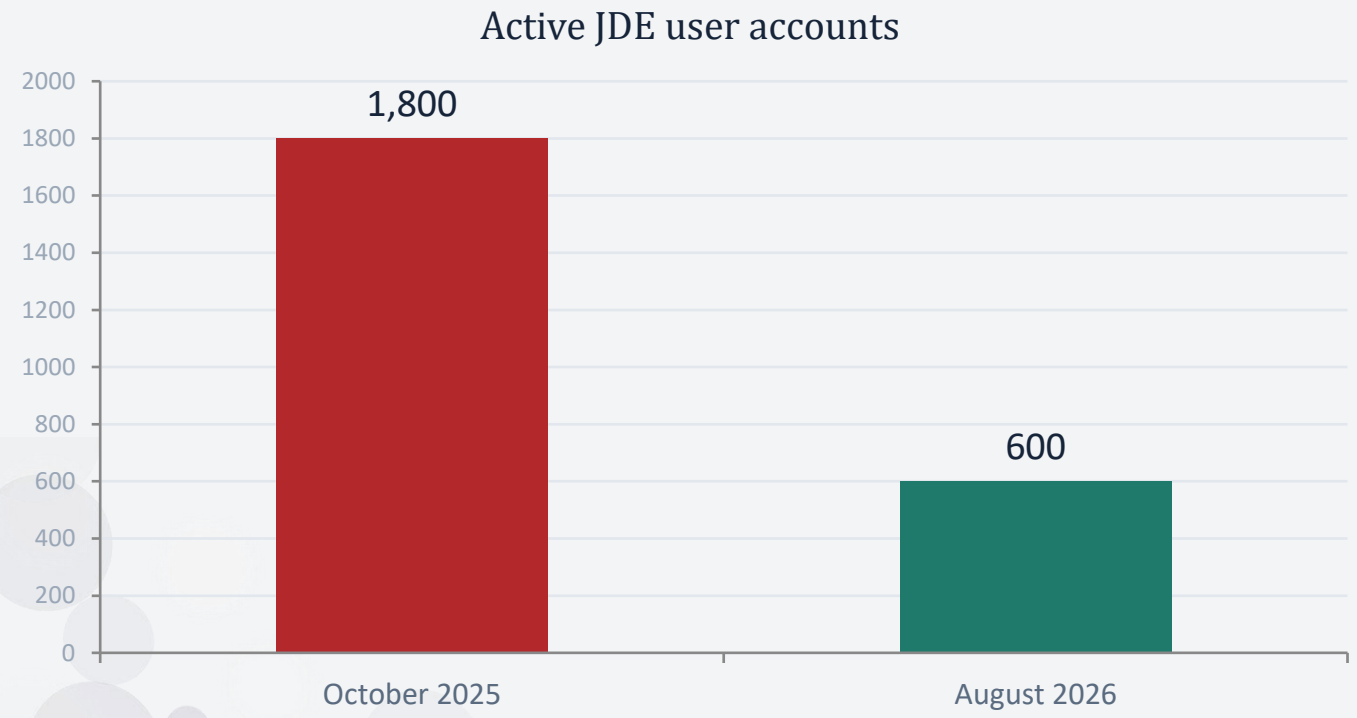


Chart values are the outline figures: 1,800+ accounts in October 2025, under 600 as of August 2026.

~67%

reduction in active accounts

270 / 365

day thresholds for disable and delete

100%

of current active users are verified thru HR

SUSTAINING IT

What keeps it clean after we leave

A cleanup without a cadence is a cleanup you will repeat in three years.

1

Annual user access review

Managers confirm their people still need what they have. Department and job title on every active user is what makes this reviewable.

2

Profile management policy

Written rules for how profiles are created, changed, and retired, so provisioning stops being folklore or inherited.

3

Periodic profile and role review

A scheduled cycle, not an event triggered by an auditor's email.

4

Customer training

The team that runs it day to day was trained during the project, not handed a document at the end.

The measure of the project is not what we removed. It is whether it stays removed.

LESSONS

What we would tell you to do differently

1. **Define the project up front**

   Write the scope down and keep the focus where it belongs. Everything else goes on the parking lot for a later date.

2. **Train before you start, not during**

   Go through the AOS Academy before the project begins. Focus on the areas you will actually use. You will make better decisions and ask better questions of your consulting team.

3. **Prioritise by business need**

   Not by what the report ranks highest, and not by what is easiest to fix.

4. **Fix *ALL access**

   Roles carrying *ALL were reviewed and corrected. These are the findings that make everything downstream look worse than it is.

5. **Expect the cleanup to find its own work**

   The LDAP issue was not on the plan. Budget review time for what is unknown to you at the start.

ONE MORE THING

The licensing conversation, handled carefully

What fewer accounts actually buys you

- A defensible account population you can explain line by line
- A smaller surface to reconcile if Oracle LMS ever asks
- Shorter SoD output and faster access reviews, which is where the real recurring saving is
- Removal of accounts that were never entitled in the first place
- For future projects, your reviewing active user access as you continue your journey

!

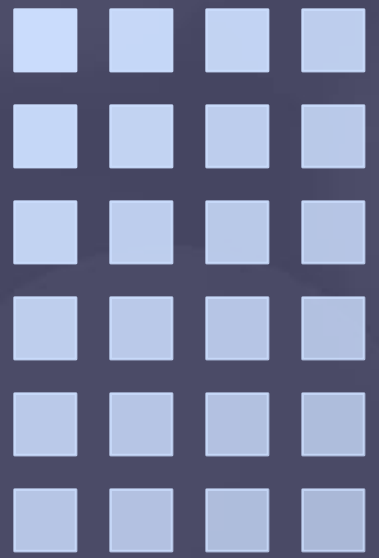
Do not promise a licence reduction

Oracle's standard user metrics count individuals authorised to use the software, not individuals who happen to use it. Frequency of sign-on is not a general exemption. What your agreement says governs, so check the contract before you put a number in front of a CFO.

TAKE THIS HOME

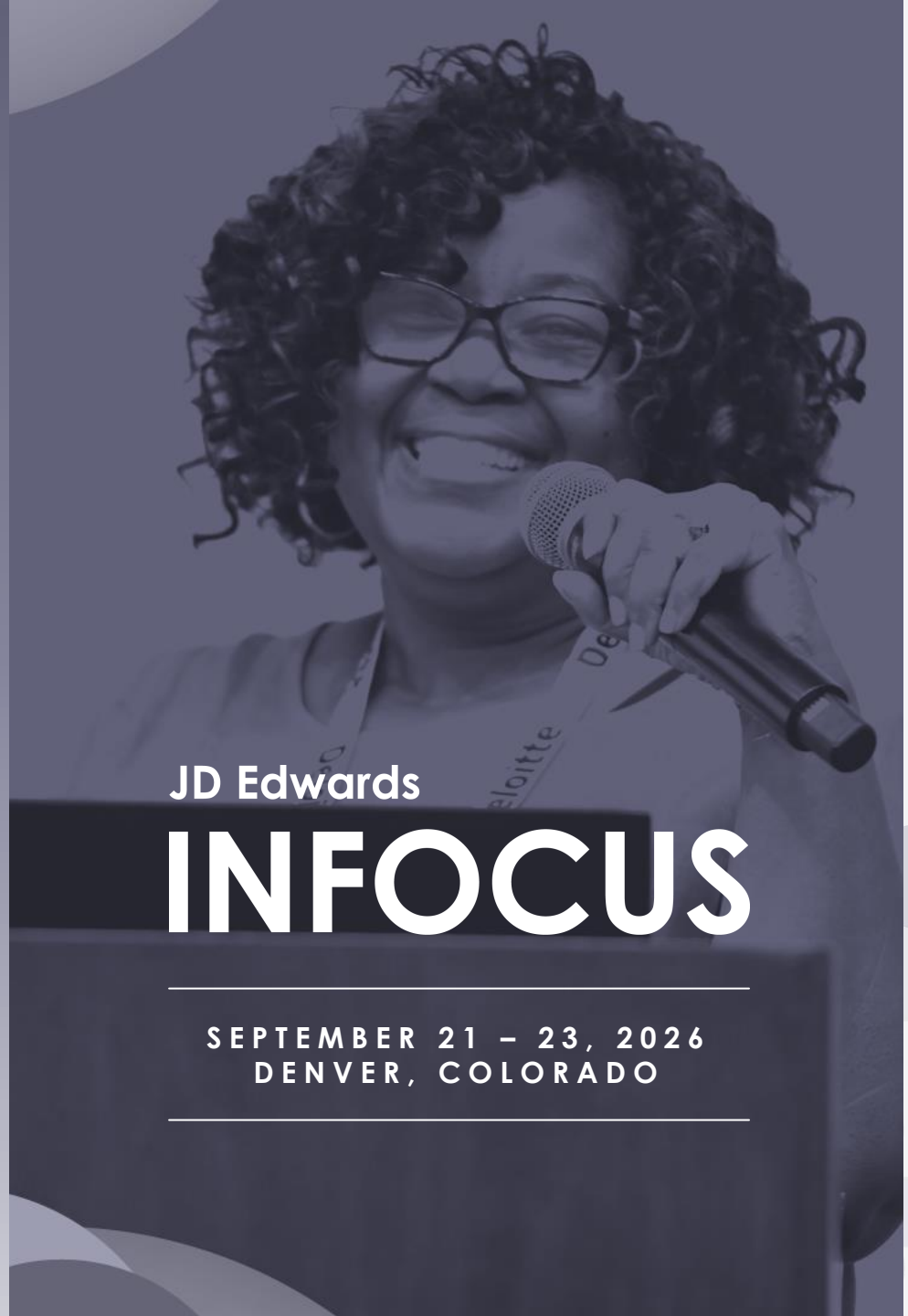
Five things you can start on Monday

1. Turn on security history today. You cannot analyse sign-on data you never collected.
2. Write down what the project is not. Defend that line harder than the scope itself.
3. Never provision a user by copying a live colleague. One bad profile reproduces itself.
4. Run proof mode every time, and read the delta before you promote.
5. Build the review cadence before you finish the cleanup, or you will do it all again.



Questions

Prinova · ERP Suites · Quest InFocus 2026



JD Edwards

INFOCUS

SEPTEMBER 21 – 23, 2026
DENVER, COLORADO

Q&A

Contact me:

Melanee Melia

Prinova · Program Manager

Melanee.Melia@PrinovaUSA.com

Brian Connor

ERP Suites · Director, JDE Security

BConnor@erpsuites.com

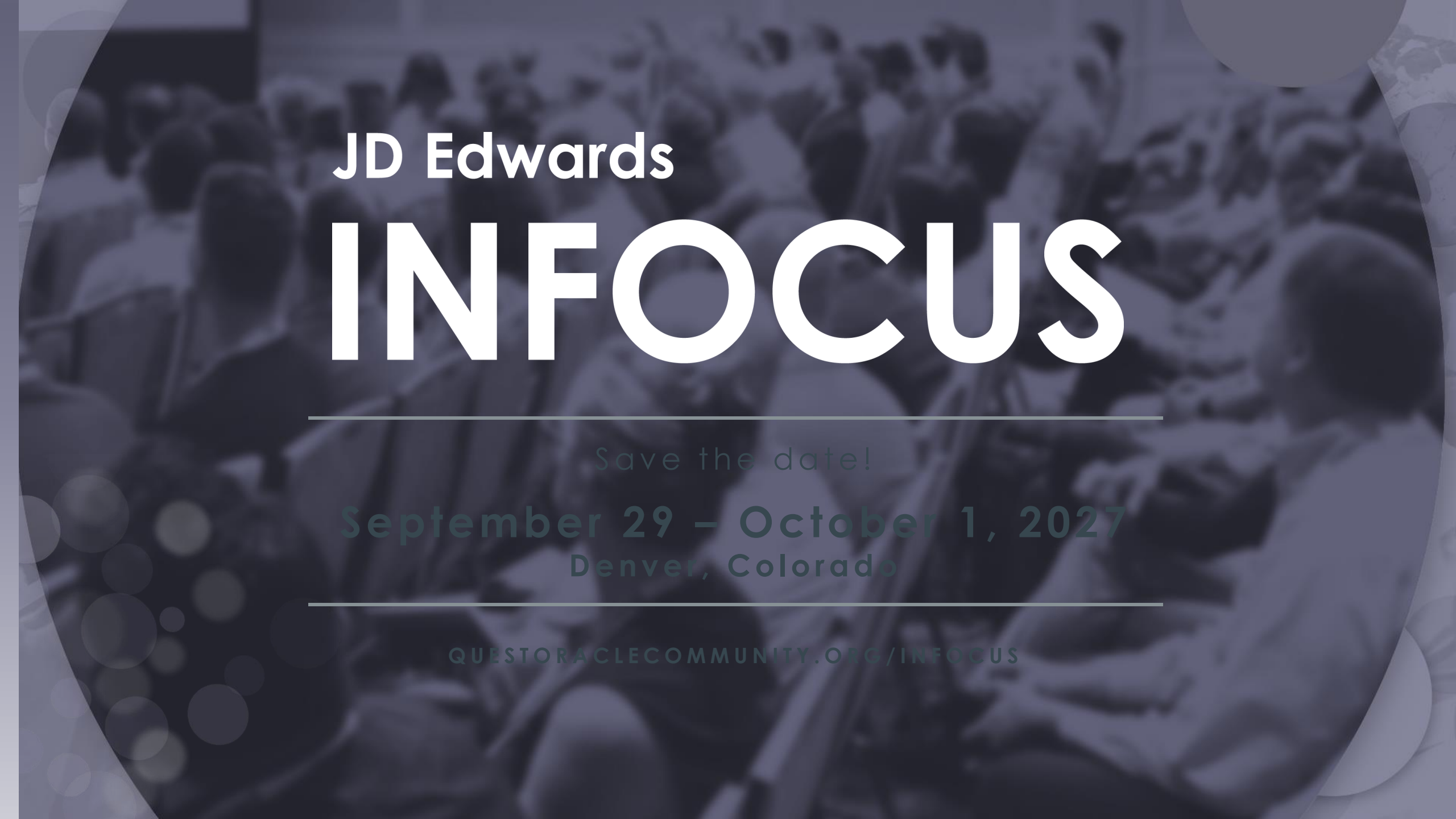
Session ID:

P-052757

Quest
JD Edwards
Community

LOVE THIS SESSION?

COMPLETE AT LEAST **3 SESSION SURVEYS** PER DAY AND GET ENTERED INTO THE DAILY DRAWINGS TO WIN A **$500** GIFT CARD!


JD Edwards
INFOCUS
Save the date!
September 29 – October 1, 2027
Denver, Colorado
QUESTORACLECOMMUNITY.ORG/INFOCUS