kinsey™
WHEN EXPERIENCE MATTERS

Security Well-Check

for Infor/Lawson

Insight

FOR MORE informative DECISIONS

Agenda

- About Us
- Vulnerabilities
- Other Considerations
- Other Services
- Complimentary Solutions

About Us

- Founded in 1983, Kinsey has provided software sales, implementation, support and development for 34 years.
- Lawson reseller and implementation partner since 1997.
- Lawson certified systems integrator partner.
- Lawson complementary software partner.
- Lawson’s “Go to” implementation partner for public sector.
- Provide complementary Lawson software products.

Vulnerabilities

- Securing Drill Around and Selects
- Securing Critical Fields
- Elements and Element Groups
- Resolving Conflicting Form Access
- Over-Provisioned Form Access
- Securable Types
- Self-Service Considerations
- Segregation of Duties

Securing Drill Arounds and Selects

Requirement

- Providing access to tables is required in order to see data in Drill Arounds and Selects, which allows users to select records from drop-down selection lists, and allows drilling from various screens into detailed data.

Vulnerabilities

- It’s easy to grant access to tables, but that can also allow users to drill to inappropriate data such as SSNs and executive salaries. These need to be secured at the table level.

Common Error

- Securing the Pay tab in HR11 prevents the obvious method for viewing pay, but users may still be able to drill into pay history, quarterly pay amounts, see benefits based on pay, etc.
- Improper viewing of Inventory data
- Access to Banking information

AR

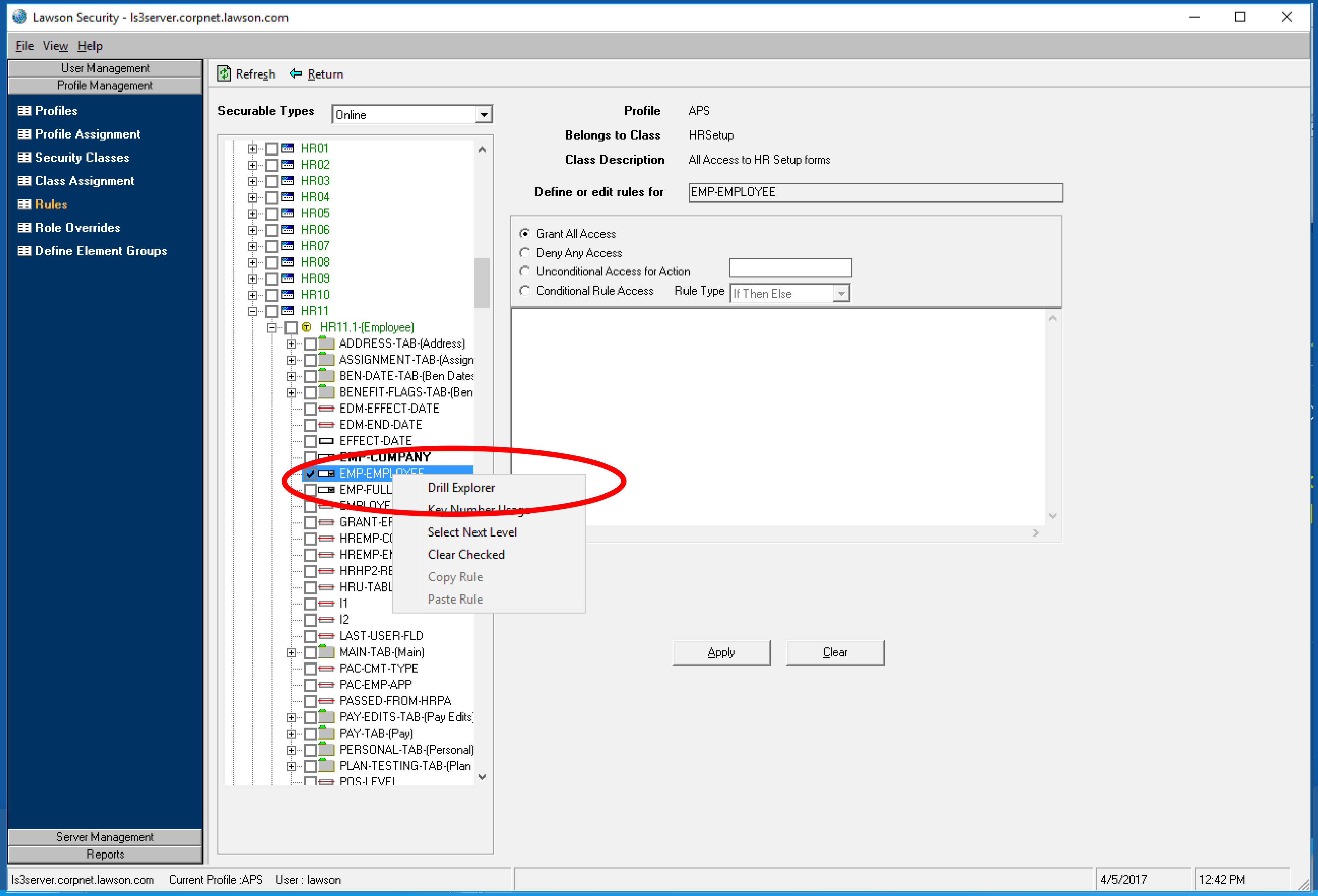
Securing Drill Arounds and Selects

Advantages

- When you have properly secured sensitive data, then users cannot view it through screens, via experimental drilling around or by downloading data through Microsoft Add-Ins!

What we are looking for

Identify the tables supporting the form in question with drill explorer is LSA.



Lawson Security - ls3server.corpnet.lawson.com

Securable Types: Online

Profile: APS

Belongs to Class: HRSetup

Class Description: All Access to HR Setup forms

Define or edit rules for: EMP-EMPLOYEE

● Grant All Access
○ Deny Any Access
○ Unconditional Access for Action
○ Conditional Rule Access Rule Type: If Then Else

ls3server.corpnet.lawson.com Current Profile :APS User : lawson 4/5/2017 12:42 PM

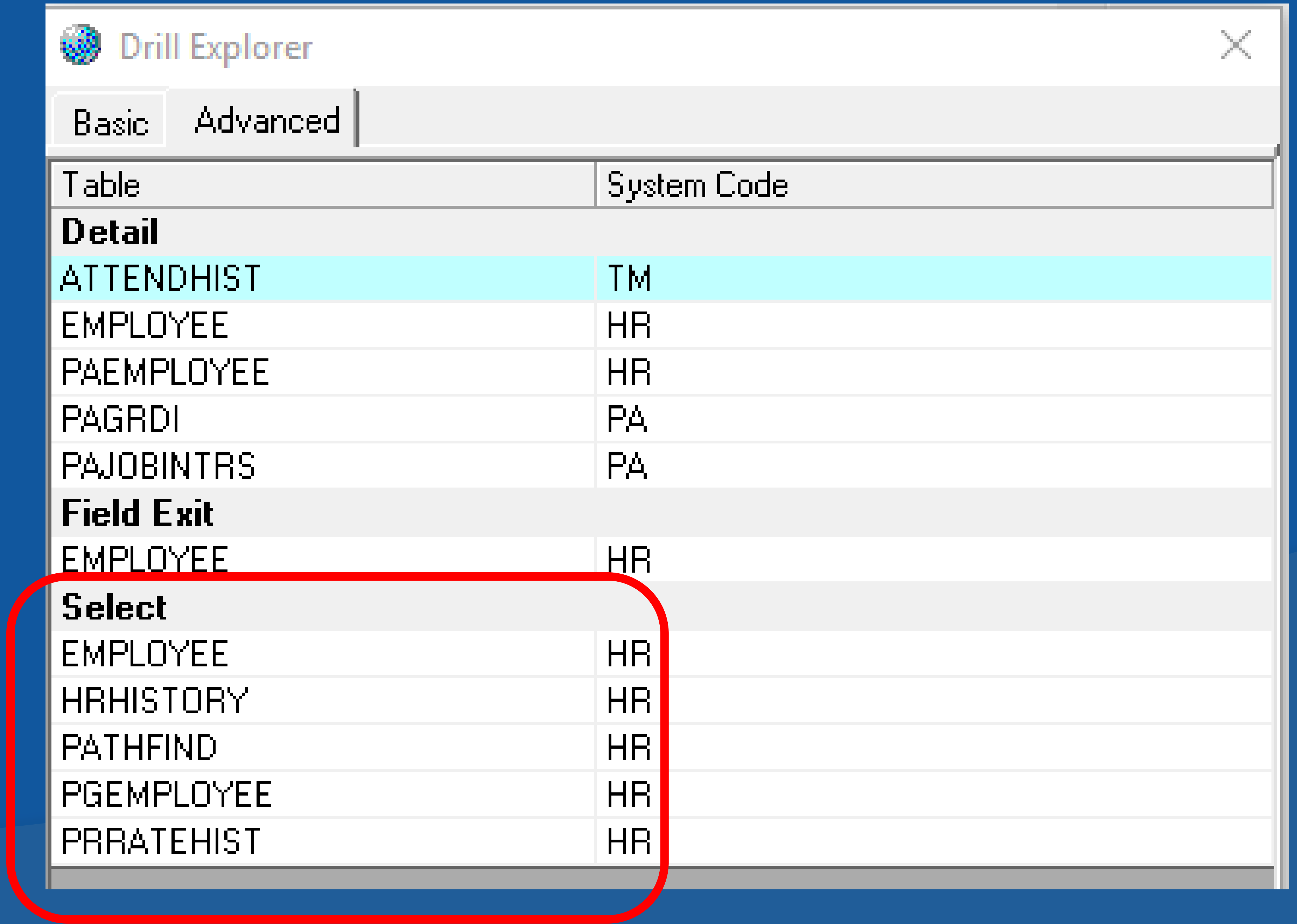


Table	System Code
Detail	
ATTENDHIST	TM
EMPLOYEE	HR
PAEMPLOYEE	HR
PAGRDI	PA
PAJOBINTRS	PA
Field Exit	
EMPLOYEE	HR
Select	
EMPLOYEE	HR
HRHISTORY	HR
PATHFIND	HR
PGEMPLOYEE	HR
PRRATEHIST	HR

Securing Drill Arounds and Selects

Then…

- Use the *Kinsey Reports* to determine who has access to the specific tables of interest (such as COMPHIST, PRRATEHIST, PAYMASTR, PRCHECK, etc. for pay amounts).

- Ensure that critical tables have rules on them to prevent inappropriate access.

- If in doubt, check the .or (object rules) and .sr (screen rules) files that contain the rules for drills and selects.

Securing Critical Fields

Vulnerabilities

- User’s may have access to sensitive PHI/PII information.
  - Can users view the Name, Address, SSN, Salary, D.O.B, Handicaps, etc., through an AGS or DME call via Portal, Ming.le, LSO, Addin, etc?
  - Frequently, users are sufficiently secured in screens, but they can drill to inappropriate data?

Common Errors/Problems

- Lack of effective communication/documentation of PII and PHI data items.
- Rash/Reactive efforts to secure these fields may make the security design top heavy with unnecessary rules. This lack of proactive planning could potentially prohibit extra-departmental staff from suppling requests for an increase in resources in a timely manor.

Our Approach

- Work with staff early to design a robust model based on all disclosed PHI and PII restriction needs.

AR

Elements and Element Groups

Definition

While elements (ELM) are global definitions of a field, element groups (ELG) are securable objects themselves and defined by more than one element. User defined element groups are not delivered by Infor/Lawson and must be called by specific functions from forms and/or files. However, Lawson defined element groups can provide a solid foundation in the creation data level security for your business. Lawson defined element groups allow you to balance your security efforts in single point of access. Meaning, both forms and files data are secured based on the conditions of the Lawson defined element group rule.

Element example:

- Company
- Process-Level

Element Group example:

- PROCLEVEL (Lawson Defined)
  - Company
  - Process-Level

Elements and Element Groups

Vulnerabilities

- Batch Forms are the specific vulnerability (only were Lawson defined ELGs are concerned)
- If you don’t use PROCLEVEL, you have to be certain you have identified all forms and or files needing to be secured for the Role.

Common Issues

- Be careful in overlapping efforts to security data
  - Rules on the form/file to secure data vs. leveraging the ELG securable object to secure data.
- Streamline (minimize) data level rules – You do not want to overlap ELG rules of the same type.
- Not understanding the system code and element dependencies.

Advantages

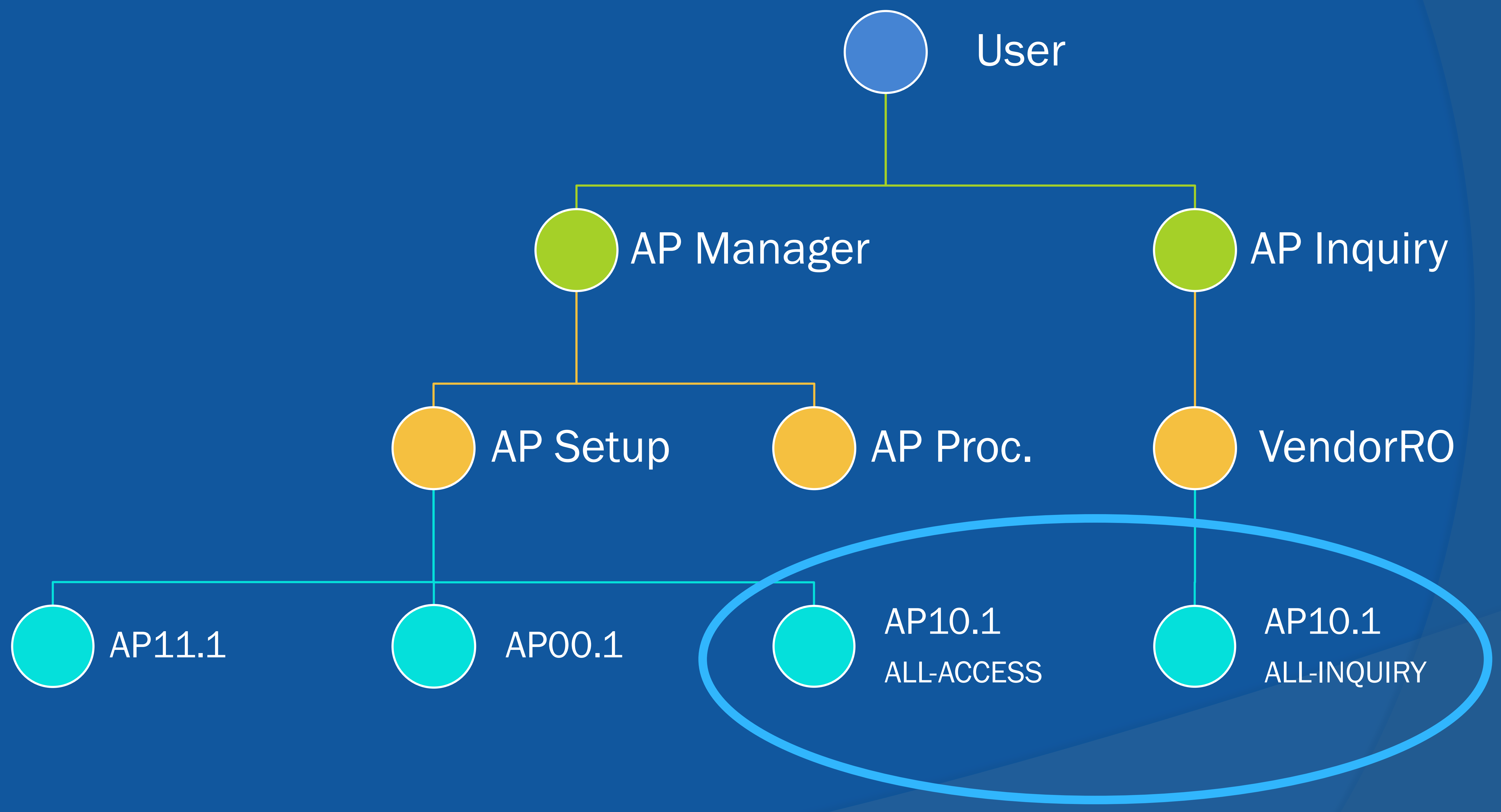
- Using Lawson delivered ELG in your security strategy is the most efficient way to secure data for online, batch and file access.

AR

Resolving Conflicting Form Access

Definition

- The common problem of a user having access to a form through more than one Role or Security Class.



Resolving Conflicting Form Access

Vulnerabilities

- Potential for users to have more functionality on a form than desired (i.e. A,C,D versus Inquiry only)

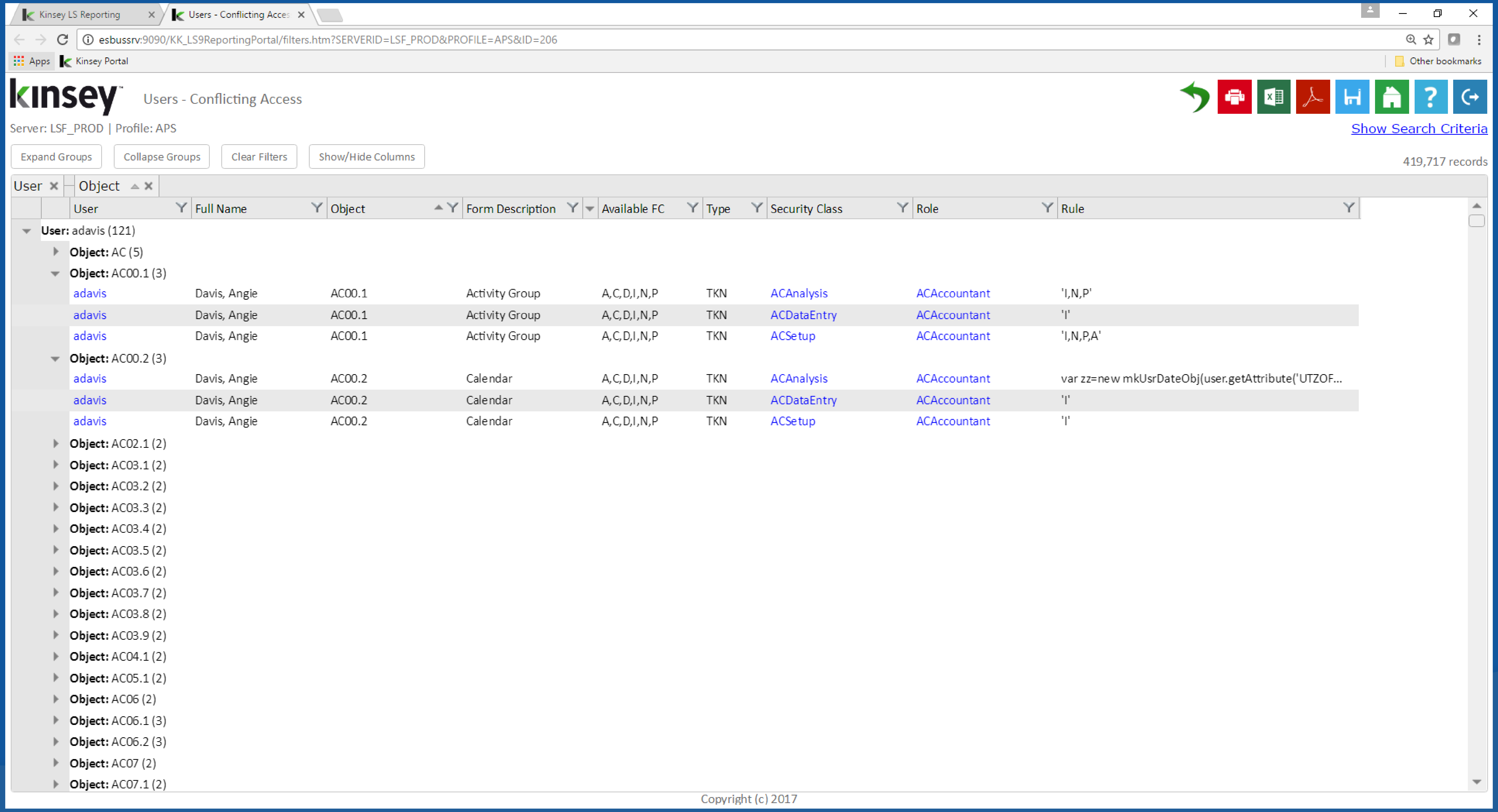
Common Issues

- Not realizing that a user has access to a form through more than one path.
- Not understanding how Lawson resolves "least restrictive" access to an object.
- Attempting to change access for one user snowballs into many changes affecting lots of users. Small changes quickly become impossible to complete.

Resolving Conflicting Form Access

Our Process/Solution

- We will identify the duplicates, determine which are the most crucial, and work with your team to resolve them.



Kinsey LS Reporting | Users - Conflicting Acce:

esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=206

Apps | Kinsey Portal | Other bookmarks

Users - Conflicting Access

Server: LSF_PROD | Profile: APS

Show Search Criteria

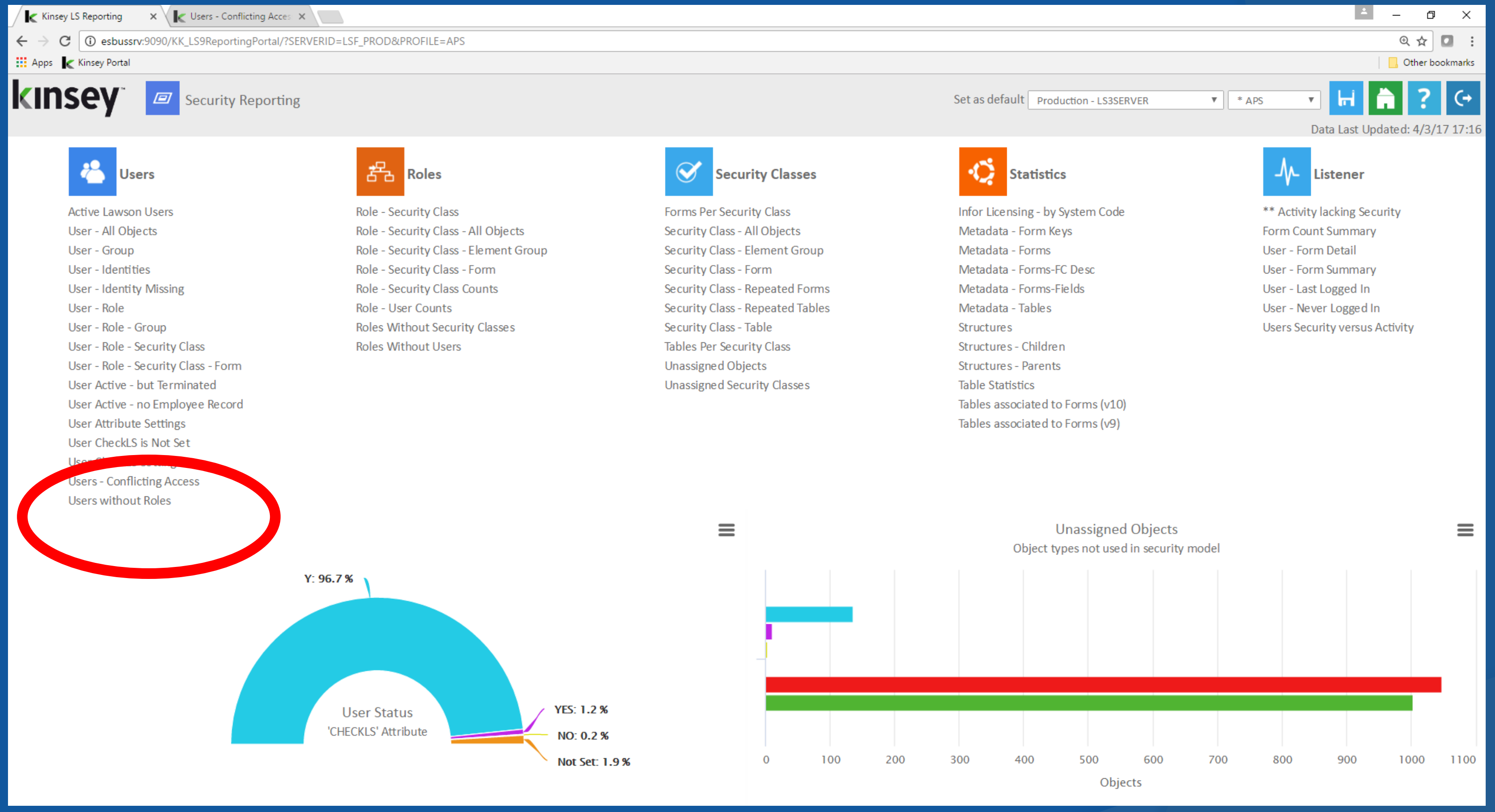
Expand Groups | Collapse Groups | Clear Filters | Show/Hide Columns

419,717 records

User × | Object ▲ ×

User	Full Name	Object	Form Description	Available FC	Type	Security Class	Role	Rule
User: adavis (121)								
Object: AC (5)								
Object: AC00.1 (3)								
adavis	Davis, Angie	AC00.1	Activity Group	A,C,D,I,N,P	TKN	ACAnalysis	ACAccountant	'I,N,P'
adavis	Davis, Angie	AC00.1	Activity Group	A,C,D,I,N,P	TKN	ACDataEntry	ACAccountant	'I'
adavis	Davis, Angie	AC00.1	Activity Group	A,C,D,I,N,P	TKN	ACSetup	ACAccountant	'I,N,P,A'
Object: AC00.2 (3)								
adavis	Davis, Angie	AC00.2	Calendar	A,C,D,I,N,P	TKN	ACAnalysis	ACAccountant	var zz=new mkUsrDateObj(user.getAttribute('UTZOF...
adavis	Davis, Angie	AC00.2	Calendar	A,C,D,I,N,P	TKN	ACDataEntry	ACAccountant	'I'
adavis	Davis, Angie	AC00.2	Calendar	A,C,D,I,N,P	TKN	ACSetup	ACAccountant	'I'
Object: AC02.1 (2)								
Object: AC03.1 (2)								
Object: AC03.2 (2)								
Object: AC03.3 (2)								
Object: AC03.4 (2)								
Object: AC03.5 (2)								
Object: AC03.6 (2)								
Object: AC03.7 (2)								
Object: AC03.8 (2)								
Object: AC03.9 (2)								
Object: AC04.1 (2)								
Object: AC05.1 (2)								
Object: AC06 (2)								
Object: AC06.1 (3)								
Object: AC06.2 (3)								
Object: AC07 (2)								
Object: AC07.1 (2)								

Copyright (c) 2017



Kinsey LS Reporting | Users - Conflicting Acce:

esbussrv:9090/KK_LS9ReportingPortal/?SERVERID=LSF_PROD&PROFILE=APS

Apps | Kinsey Portal | Other bookmarks

Security Reporting

Set as default: Production - LS3SERVER | * APS

Data Last Updated: 4/3/17 17:16

Users

Active Lawson Users
User - All Objects
User - Group
User - Identities
User - Identity Missing
User - Role
User - Role - Group
User - Role - Security Class
User - Role - Security Class - Form
User Active - but Terminated
User Active - no Employee Record
User Attribute Settings
User CheckLS is Not Set
Users - Conflicting Access
Users without Roles

Roles

Role - Security Class
Role - Security Class - All Objects
Role - Security Class - Element Group
Role - Security Class - Form
Role - Security Class Counts
Role - User Counts
Roles Without Security Classes
Roles Without Users

Security Classes

Forms Per Security Class
Security Class - All Objects
Security Class - Element Group
Security Class - Form
Security Class - Repeated Forms
Security Class - Repeated Tables
Security Class - Table
Tables Per Security Class
Unassigned Objects
Unassigned Security Classes

Statistics

Infor Licensing - by System Code
Metadata - Form Keys
Metadata - Forms
Metadata - Forms-FC Desc
Metadata - Forms-Fields
Metadata - Tables
Structures
Structures - Children
Structures - Parents
Table Statistics
Tables associated to Forms (v10)
Tables associated to Forms (v9)

Listener

** Activity lacking Security
Form Count Summary
User - Form Detail
User - Form Summary
User - Last Logged In
User - Never Logged In
Users Security versus Activity

Over-Provisioned Form Access

Vulnerabilities

- User's may have access to forms that violate SoD policies or with critical information not related their job.

Common Issues

- Not having a good understanding of exactly what forms a user requires to do their job.
- Your technical staff has WAY too much access (according to auditors). What can you do?
  - We'll configure Kinsey Activity Monitor reports for auditors showing exactly which screens tech users have been using to view or change data, including whether changes were made at all.
  - We will help create a configuration that prevents tech users from changing data without following your proper methodology (user involvement, documentation).

DA

Over-Provisioned Form Access

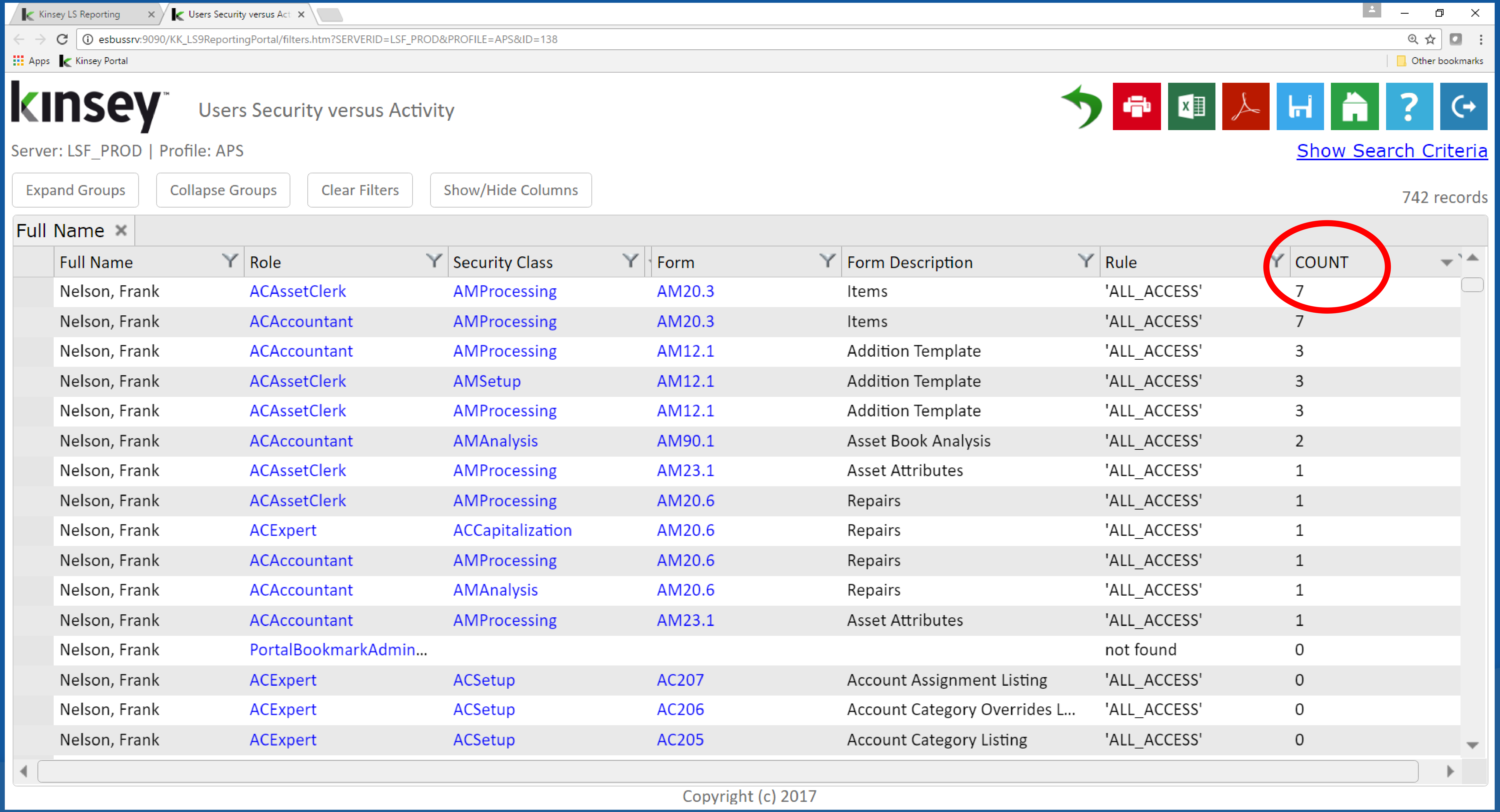
Our Approach

- We’ll use Kinsey Reports to determine exactly what users have access to and how to quickly restrict that access.
- Did they go “off the rails” and use inappropriate screens?
- We’ll show how to use Kinsey’s Activity Monitor to quickly determine what screens they used and if they simply inquired or made changes.

Over-Provisioned Form Access

Reporting

- User Activity
- User Activity versus Security



Kinsey LS Reporting | Users Security versus Act

esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=138

Apps | Kinsey Portal | Other bookmarks

Users Security versus Activity

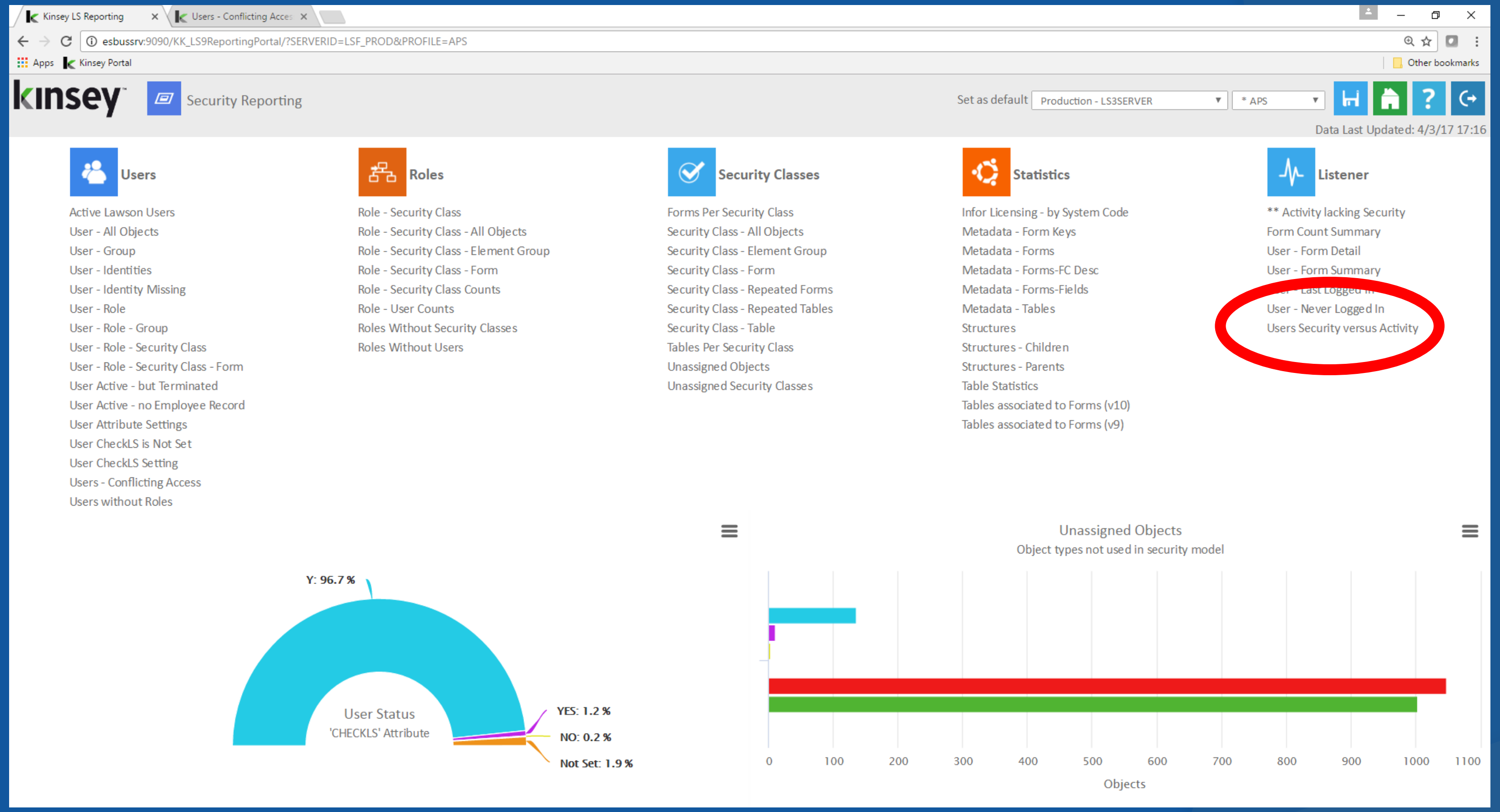
Server: LSF_PROD | Profile: APS

742 records

Full Name ✕

Full Name	Role	Security Class	Form	Form Description	Rule	COUNT
Nelson, Frank	ACAssetClerk	AMProcessing	AM20.3	Items	'ALL_ACCESS'	7
Nelson, Frank	ACAccountant	AMProcessing	AM20.3	Items	'ALL_ACCESS'	7
Nelson, Frank	ACAccountant	AMProcessing	AM12.1	Addition Template	'ALL_ACCESS'	3
Nelson, Frank	ACAssetClerk	AMSetup	AM12.1	Addition Template	'ALL_ACCESS'	3
Nelson, Frank	ACAssetClerk	AMProcessing	AM12.1	Addition Template	'ALL_ACCESS'	3
Nelson, Frank	ACAccountant	AMAnalysis	AM90.1	Asset Book Analysis	'ALL_ACCESS'	2
Nelson, Frank	ACAssetClerk	AMProcessing	AM23.1	Asset Attributes	'ALL_ACCESS'	1
Nelson, Frank	ACAssetClerk	AMProcessing	AM20.6	Repairs	'ALL_ACCESS'	1
Nelson, Frank	ACExpert	ACCapitalization	AM20.6	Repairs	'ALL_ACCESS'	1
Nelson, Frank	ACAccountant	AMProcessing	AM20.6	Repairs	'ALL_ACCESS'	1
Nelson, Frank	ACAccountant	AMAnalysis	AM20.6	Repairs	'ALL_ACCESS'	1
Nelson, Frank	ACAccountant	AMProcessing	AM23.1	Asset Attributes	'ALL_ACCESS'	1
Nelson, Frank	PortalBookmarkAdmin...				not found	0
Nelson, Frank	ACExpert	ACSetup	AC207	Account Assignment Listing	'ALL_ACCESS'	0
Nelson, Frank	ACExpert	ACSetup	AC206	Account Category Overrides L...	'ALL_ACCESS'	0
Nelson, Frank	ACExpert	ACSetup	AC205	Account Category Listing	'ALL_ACCESS'	0

Copyright (c) 2017



Kinsey LS Reporting | Users - Conflicting Acces

esbussrv:9090/KK_LS9ReportingPortal/?SERVERID=LSF_PROD&PROFILE=APS

Apps | Kinsey Portal | Other bookmarks

Security Reporting

Set as default: Production - LS3SERVER | * APS

Data Last Updated: 4/3/17 17:16

Users

- Active Lawson Users
- User - All Objects
- User - Group
- User - Identities
- User - Identity Missing
- User - Role
- User - Role - Group
- User - Role - Security Class
- User - Role - Security Class - Form
- User Active - but Terminated
- User Active - no Employee Record
- User Attribute Settings
- User CheckLS is Not Set
- User CheckLS Setting
- Users - Conflicting Access
- Users without Roles

Roles

- Role - Security Class
- Role - Security Class - All Objects
- Role - Security Class - Element Group
- Role - Security Class - Form
- Role - Security Class Counts
- Role - User Counts
- Roles Without Security Classes
- Roles Without Users

Security Classes

- Forms Per Security Class
- Security Class - All Objects
- Security Class - Element Group
- Security Class - Form
- Security Class - Repeated Forms
- Security Class - Repeated Tables
- Security Class - Table
- Tables Per Security Class
- Unassigned Objects
- Unassigned Security Classes

Statistics

- Infor Licensing - by System Code
- Metadata - Form Keys
- Metadata - Forms
- Metadata - Forms-FC Desc
- Metadata - Forms-Fields
- Metadata - Tables
- Structures
- Structures - Children
- Structures - Parents
- Table Statistics
- Tables associated to Forms (v10)
- Tables associated to Forms (v9)

Listener

- ** Activity lacking Security
- Form Count Summary
- User - Form Detail
- User - Form Summary
- User - Last Logged In
- User - Never Logged In
- Users Security versus Activity

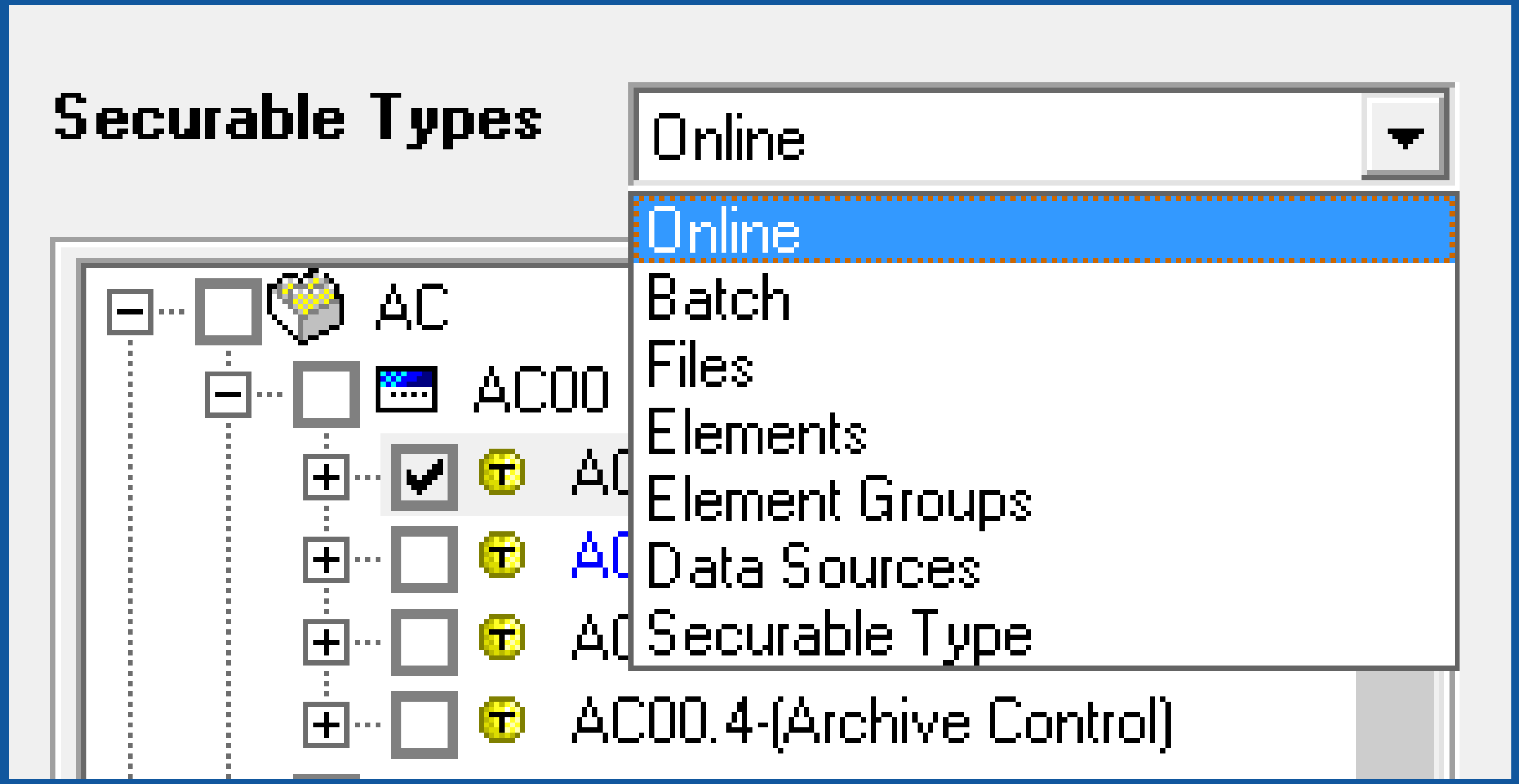
Object Type - Securable Types

Definition

- Provides global access to forms or files.

Vulnerabilities

- Overrides any user specific object rule for Form (online and batch) and Files.
- Improper provisioning of Securable Type object inadvertently provides too much access.



Securable Types: Online

Object Type - Securable Types

Common Misunderstandings

- Not realizing that Securable Types object rules have been assigned.
- That Data level rules will still be adhered to.

Advantages

- Can quickly provide full access to someone who needs it (i.e. Security Admin)

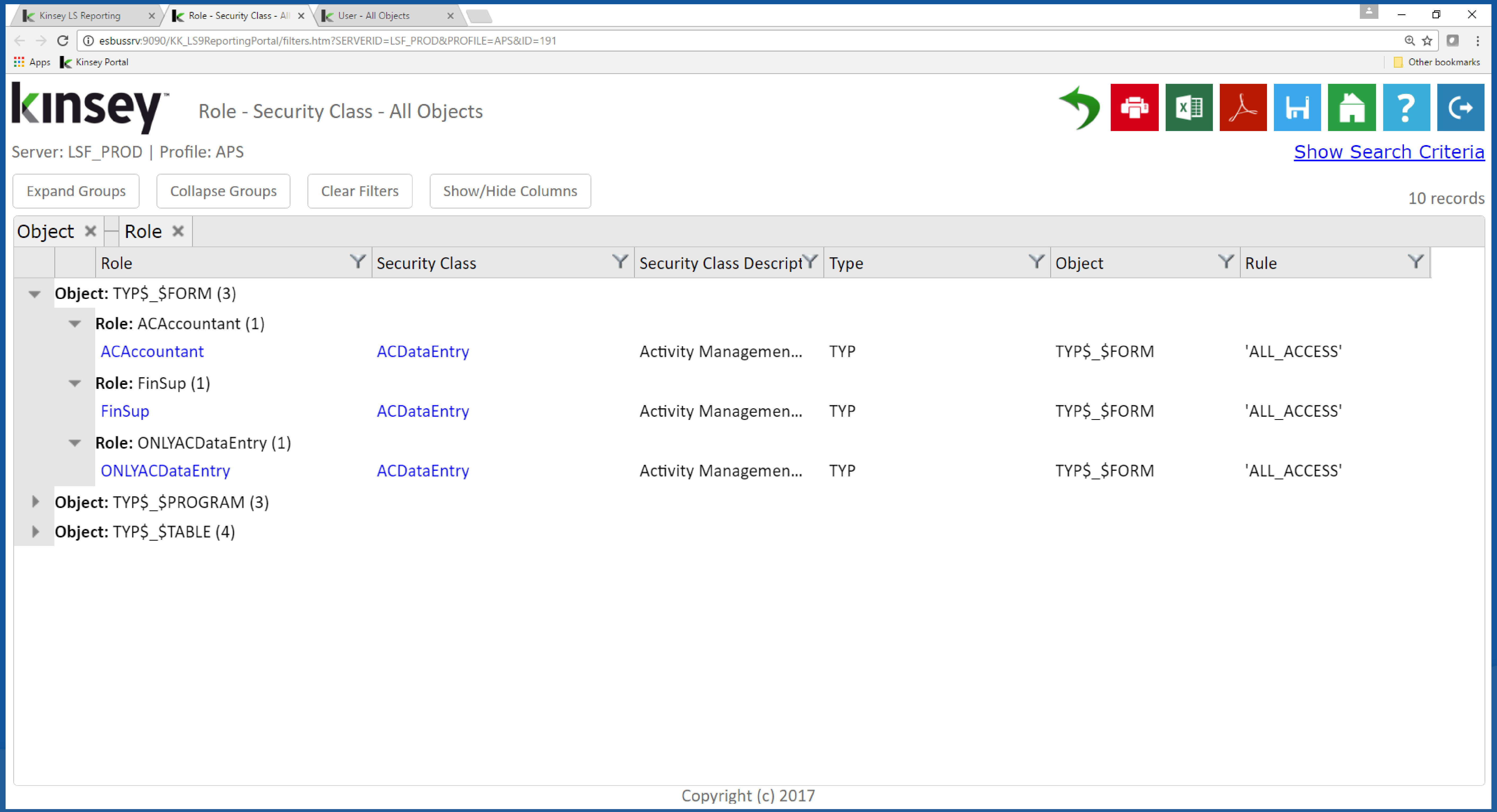
What you need to check in Security Administrator

- Validate access to securable type of TYP.

Object Type - Securable Types

Reporting

- User All Objects Report
- Role – Security Class All Object Report
- Security Class All Object Report



esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=191

Role - Security Class - All Objects

Server: LSF_PROD | Profile: APS

Show Search Criteria

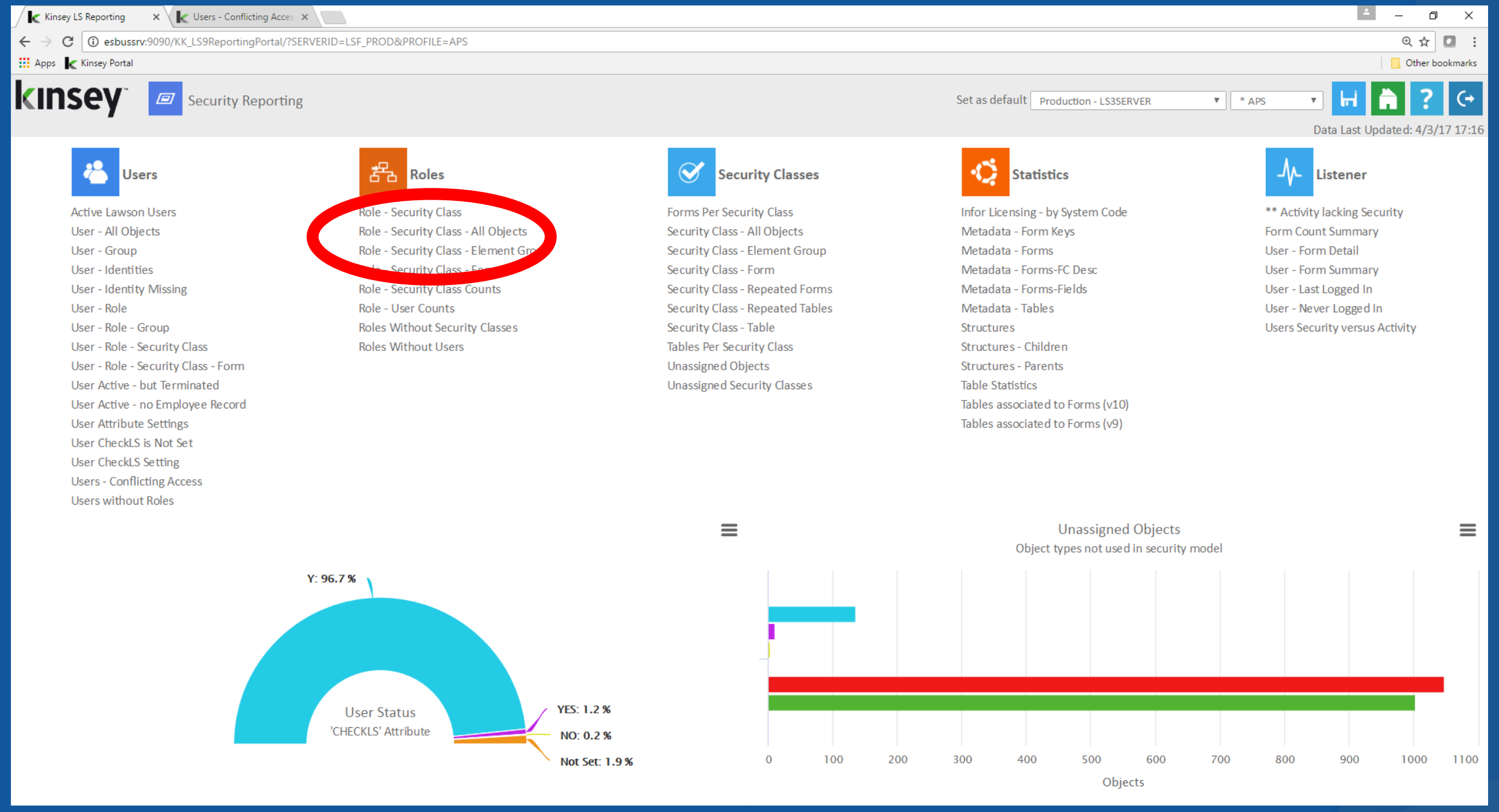
Expand Groups | Collapse Groups | Clear Filters | Show/Hide Columns

10 records

Object ✕ — Role ✕

Role	Security Class	Security Class Descript	Type	Object	Rule
Object: TYP$_$FORM (3)					
Role: ACAccountant (1)					
ACAccountant	ACDataEntry	Activity Managemen...	TYP	TYP$_$FORM	'ALL_ACCESS'
Role: FinSup (1)					
FinSup	ACDataEntry	Activity Managemen...	TYP	TYP$_$FORM	'ALL_ACCESS'
Role: ONLYACDataEntry (1)					
ONLYACDataEntry	ACDataEntry	Activity Managemen...	TYP	TYP$_$FORM	'ALL_ACCESS'
Object: TYP$_$PROGRAM (3)					
Object: TYP$_$TABLE (4)					

Copyright (c) 2017



esbussrv:9090/KK_LS9ReportingPortal/?SERVERID=LSF_PROD&PROFILE=APS

Set as default: Production - LS3SERVER | * APS

Data Last Updated: 4/3/17 17:16

Users
Active Lawson Users
User - All Objects
User - Group
User - Identities
User - Identity Missing
User - Role
User - Role - Group
User - Role - Security Class
User - Role - Security Class - Form
User Active - but Terminated
User Active - no Employee Record
User Attribute Settings
User CheckLS is Not Set
User CheckLS Setting
Users - Conflicting Access
Users without Roles

Roles
Role - Security Class
Role - Security Class - All Objects
Role - Security Class - Element Gro
Role - Security Class - For
Role - Security Class Counts
Role - User Counts
Roles Without Security Classes
Roles Without Users

Security Classes
Forms Per Security Class
Security Class - All Objects
Security Class - Element Group
Security Class - Form
Security Class - Repeated Forms
Security Class - Repeated Tables
Security Class - Table
Tables Per Security Class
Unassigned Objects
Unassigned Security Classes

Statistics
Infor Licensing - by System Code
Metadata - Form Keys
Metadata - Forms
Metadata - Forms-FC Desc
Metadata - Forms-Fields
Metadata - Tables
Structures
Structures - Children
Structures - Parents
Table Statistics
Tables associated to Forms (v10)
Tables associated to Forms (v9)

Listener
** Activity lacking Security
Form Count Summary
User - Form Detail
User - Form Summary
User - Last Logged In
User - Never Logged In
Users Security versus Activity

ESS/MSS Considerations

Definition

- ESS/MSS – Employee and Manager Self Service are a set of “self evident” applications or bookmarks that allow you to inquire or update HR, LP, BN, PA, or PR data in Lawson as the employee identified on the Employee Service.

Vulnerabilities

- The risks of not setting the EMG rules and corresponding forms up correctly is exposure of PII/PHI or employment related data to users other than themselves.

ESS/MSS Considerations

Common Errors

- Leaving HR Data Item or HR Record Security active.
- Supplying ALL USERS a ENV Identity. Not necessary for ONLINE users.
- Not setting up your Privileged User/Identity correctly.
- Not understanding the symbiotic relationship between the user defined EMSS ELG and EMSS forms/files.
- Unnecessarily leaving batch forms in your EMSS security class.
- Not communicating actual tasks your organization uses in EMSS.
- Not testing customizations created for EMSS or evaluating where antiquated technology can be retired.

EMSS Considerations

Our Process

- Review your EMSS task and tailor the security class(es) to your organization’s needs.
- Review the EMSS security class for the appropriate conditional rules.
- Review your Privileged Users and User Setups.
- Review EMSS forms that may provide access to sensitive data (outside of the required access of EMSS). i.e. PA52.x
- Review the drill right of the Manager. What PHI or PII data is accessible to them for their direct reports (outside of the scope of their managerial tasks).
- Review your current setup for HR Record level or Data level security setup within the HR application

Segregation of Duties

Definition

- Segregation of Duties (SoD) validates that you have the proper checks and balances in place to prevent fraudulent activity.

Vulnerabilities

- Exposure to a number inappropriate financial transactions including check processing, asset retirement, closing procedures, inventory transactions or journal transactions.

Common Issue

- The process of developing a list of policies and appropriate rules and then checking user security against those rules can be a daunting task. Most customer’s find it very difficult to even start this process manually.
- Validating user security against those rules.

Segregation of Duties

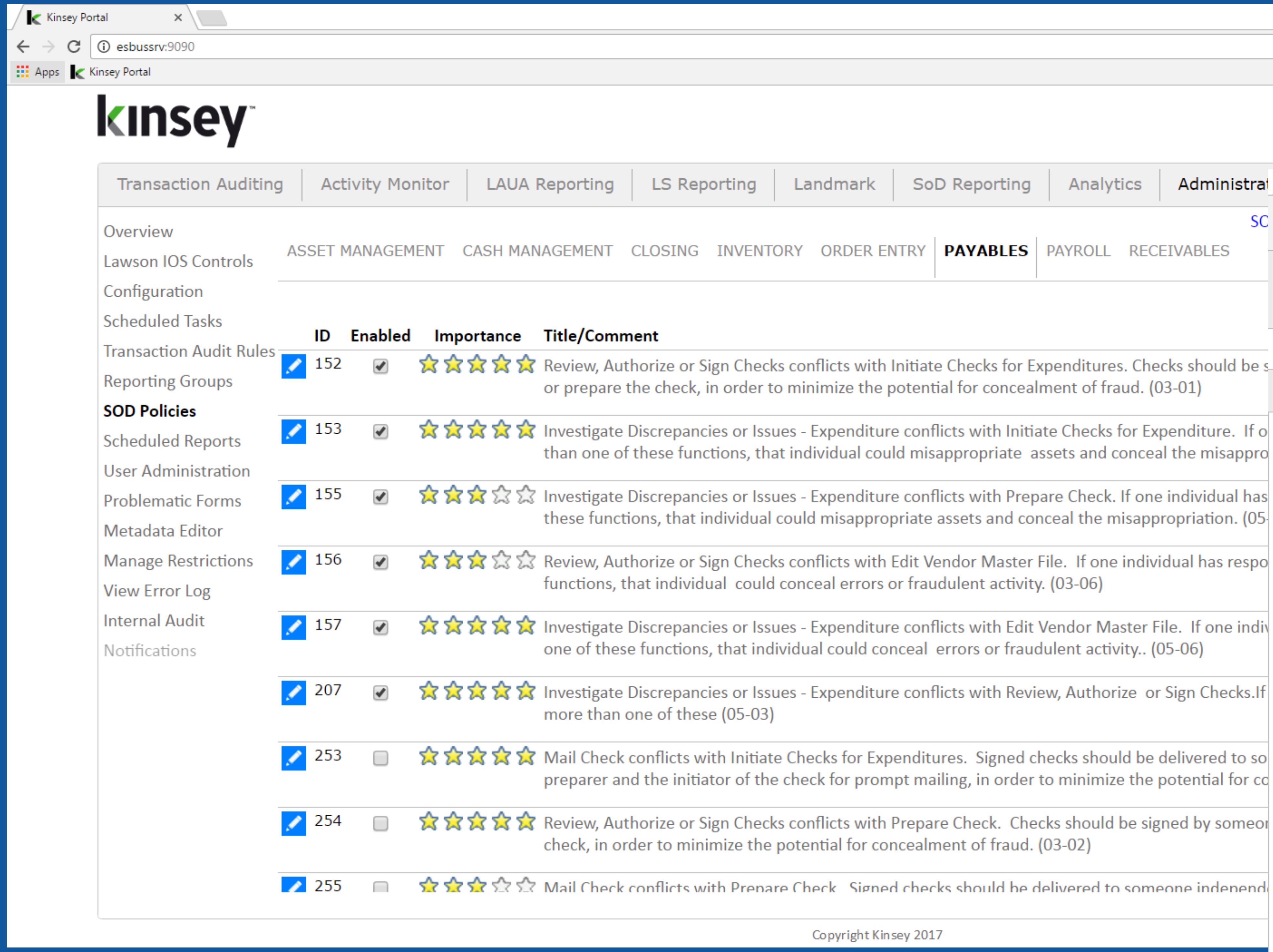
Our Process

- We start by reviewing with your team the 240 policies delivered with the application.

  Asset Management, Cash Management, Closing, Inventory, Order Entry, Payables, Receivables, and Payroll
- We then add any of your policies to our library.
- Using over 2,200 rules our SoD report will identify any user that violates a policy and the reason for the violation.
- Identify the users and policies that present the highest degree of risk.
- Modify security to mitigate the risk.

Segregation of Duties

Our Policies and Reports



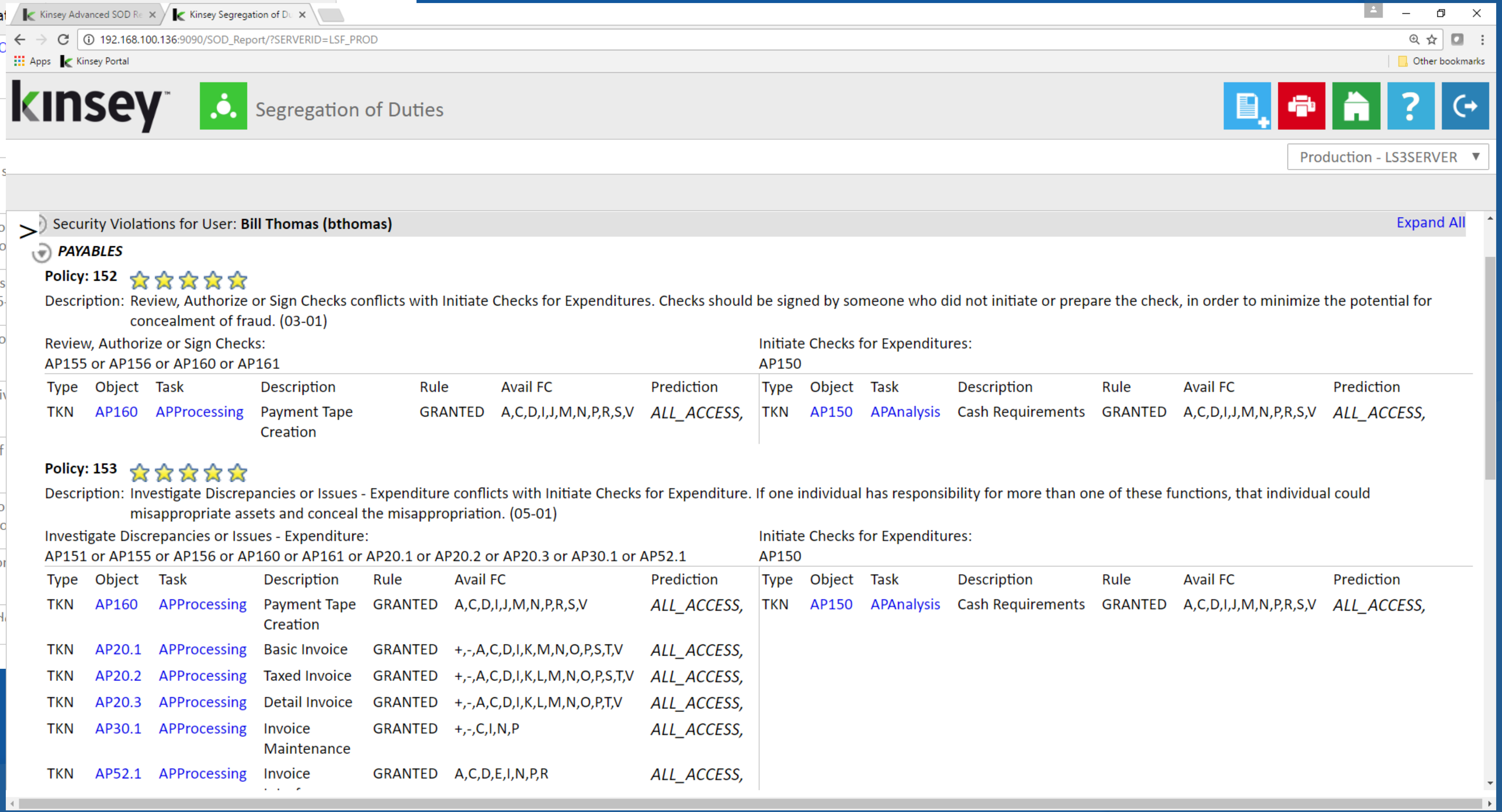
Kinsey Portal

esbussrv:9090

Logged in as: **admin**

ID	Enabled	Importance	Title/Comment
152	☑	★★★★★	Review, Authorize or Sign Checks conflicts with Initiate Checks for Expenditures. Checks should be s or prepare the check, in order to minimize the potential for concealment of fraud. (03-01)
153	☑	★★★★★	Investigate Discrepancies or Issues - Expenditure conflicts with Initiate Checks for Expenditure. If o than one of these functions, that individual could misappropriate assets and conceal the misappro
155	☑	★★★☆☆	Investigate Discrepancies or Issues - Expenditure conflicts with Prepare Check. If one individual has these functions, that individual could misappropriate assets and conceal the misappropriation. (05
156	☑	★★★☆☆	Review, Authorize or Sign Checks conflicts with Edit Vendor Master File. If one individual has respo functions, that individual could conceal errors or fraudulent activity. (03-06)
157	☑	★★★★★	Investigate Discrepancies or Issues - Expenditure conflicts with Edit Vendor Master File. If one indiv one of these functions, that individual could conceal errors or fraudulent activity.. (05-06)
207	☑	★★★★★	Investigate Discrepancies or Issues - Expenditure conflicts with Review, Authorize or Sign Checks.If more than one of these (05-03)
253	☐	★★★★★	Mail Check conflicts with Initiate Checks for Expenditures. Signed checks should be delivered to so preparer and the initiator of the check for prompt mailing, in order to minimize the potential for co
254	☐	★★★★★	Review, Authorize or Sign Checks conflicts with Prepare Check. Checks should be signed by someo check, in order to minimize the potential for concealment of fraud. (03-02)
255	☐	★★★☆☆	Mail Check conflicts with Prepare Check. Signed checks should be delivered to someone independ

Copyright Kinsey 2017



192.168.100.136:9090/SOD_Report/?SERVERID=LSF_PROD

Segregation of Duties

Production - LS3SERVER ▼

Security Violations for User: **Bill Thomas (bthomas)**

Expand All

PAYABLES

Policy: 152 ★★★★★

Description: Review, Authorize or Sign Checks conflicts with Initiate Checks for Expenditures. Checks should be signed by someone who did not initiate or prepare the check, in order to minimize the potential for concealment of fraud. (03-01)

Review, Authorize or Sign Checks:
AP155 or AP156 or AP160 or AP161

Type	Object	Task	Description	Rule	Avail FC	Prediction
TKN	AP160	APProcessing	Payment Tape Creation	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS,*

Initiate Checks for Expenditures:
AP150

Type	Object	Task	Description	Rule	Avail FC	Prediction
TKN	AP150	APAnalysis	Cash Requirements	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS,*

Policy: 153 ★★★★★

Description: Investigate Discrepancies or Issues - Expenditure conflicts with Initiate Checks for Expenditure. If one individual has responsibility for more than one of these functions, that individual could misappropriate assets and conceal the misappropriation. (05-01)

Investigate Discrepancies or Issues - Expenditure:
AP151 or AP155 or AP156 or AP160 or AP161 or AP20.1 or AP20.2 or AP20.3 or AP30.1 or AP52.1

Type	Object	Task	Description	Rule	Avail FC	Prediction
TKN	AP160	APProcessing	Payment Tape Creation	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS,*
TKN	AP20.1	APProcessing	Basic Invoice	GRANTED	+,-,A,C,D,I,K,M,N,O,P,S,T,V	*ALL_ACCESS,*
TKN	AP20.2	APProcessing	Taxed Invoice	GRANTED	+,-,A,C,D,I,K,L,M,N,O,P,S,T,V	*ALL_ACCESS,*
TKN	AP20.3	APProcessing	Detail Invoice	GRANTED	+,-,A,C,D,I,K,L,M,N,O,P,T,V	*ALL_ACCESS,*
TKN	AP30.1	APProcessing	Invoice Maintenance	GRANTED	+,-,C,I,N,P	*ALL_ACCESS,*
TKN	AP52.1	APProcessing	Invoice	GRANTED	A,C,D,E,I,N,P,R	*ALL_ACCESS,*

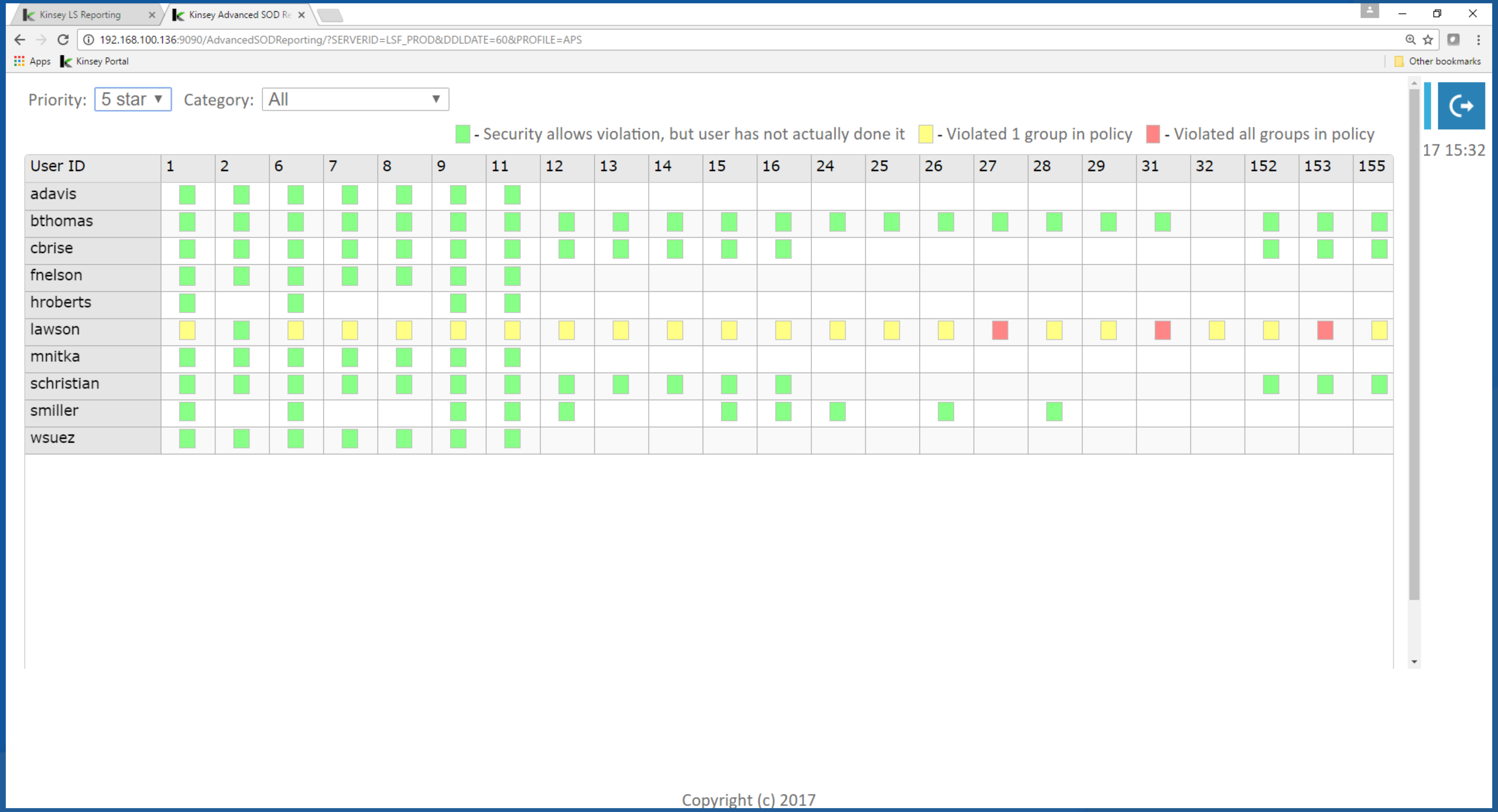
Initiate Checks for Expenditures:
AP150

Type	Object	Task	Description	Rule	Avail FC	Prediction
TKN	AP150	APAnalysis	Cash Requirements	GRANTED	A,C,D,I,J,M,N,P,R,S,V	*ALL_ACCESS,*

Segregation of Duties

Remediation Process

- By merging user activity with the violation results we can identity the policies that present the most immediate risk.



Kinsey LS Reporting
Kinsey Advanced SOD Re
192.168.100.136:9090/AdvancedSODReporting/?SERVERID=LSF_PROD&DDLDATE=60&PROFILE=APS
Apps
Kinsey Portal
Other bookmarks

Priority: 5 star ▾ Category: All ▾

🟩 - Security allows violation, but user has not actually done it 🟨 - Violated 1 group in policy 🟥 - Violated all groups in policy

17 15:32

User ID	1	2	6	7	8	9	11	12	13	14	15	16	24	25	26	27	28	29	31	32	152	153	155
adavis	🟩	🟩	🟩	🟩	🟩	🟩	🟩																
bthomas	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩
cbrise	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩									🟩	🟩	🟩
fnelson	🟩	🟩	🟩	🟩	🟩	🟩	🟩																
hroberts	🟩		🟩			🟩	🟩																
lawson	🟨	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟥	🟨	🟨	🟥	🟨	🟨	🟥	🟨
mnitka	🟩	🟩	🟩	🟩	🟩	🟩	🟩																
schristian	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩									🟩	🟩	🟩
smiller	🟩		🟩			🟩	🟩	🟩			🟩	🟩	🟩		🟩		🟩						
wsuez	🟩	🟩	🟩	🟩	🟩	🟩	🟩																

Copyright (c) 2017

Requires activation of Activity Monitor

Other Considerations

- Building Inquiry-only Roles
- Cleaning Up Menu Access and Invoked Programs
- Eliminating Duplicate Roles and Security Classes
- Standardizing Roles
- Synchronizing Your Test and Production Environments

Building Inquiry-only Roles

Definition

- The ability to easily grant inquiry-only access to all screens and all reports.

Vulnerabilities

- Users are often provided more access than they need to perform their day to day task. Inquiry only Roles resolve potential SoD violations and can prevent fraudulent transactions.

Common Errors/Problems

- *Some Roles or Security Classes may have names such as APInquiry, but include update-access to certain forms. This is misleading, or even dangerous.*

Building Inquiry-only Roles

Advantages

- This lets you confidently give access to auditors or others with no concerns about them being able to make any changes in the system.

Options

- Manually build inquiry-only configurations.
- Export Lawson Security Roles or Security Classes, adjust the XML to use ALL_INQUIRES in the place of A,C,D,I,N,P and load into new Roles/SecClasses
- Kinsey has utilities that allow us to build inquiry-only configurations that match your environment, including custom programs.

Cleaning up Menu Access and Invoked Programs

Why we do this

- Menu's and Invoked Programs tend to land in various Security Classes and create a "can't see the forest for the trees" situation. It's much cleaner and easier to control this with a well-organized solution.

Common Problems

- Not having proper access to a critical invoked program can impact your job related task.

Our Process

- Review and cleanup the usual mishmash of Invoked Program access.
- Clean up menu token access.
- Use innovative concepts to eliminate the forest of SysCodes and Programs that make the true screens harder to view and analyze.

DA

Eliminating Duplicate Roles & Security Classes

Why we do this

- Makes the security model easier to maintain and less prone to error.

Vulnerabilities

- Easy to lose track of all the paths to a critical object. (i.e. Employee Master HR11.x)

Our Process

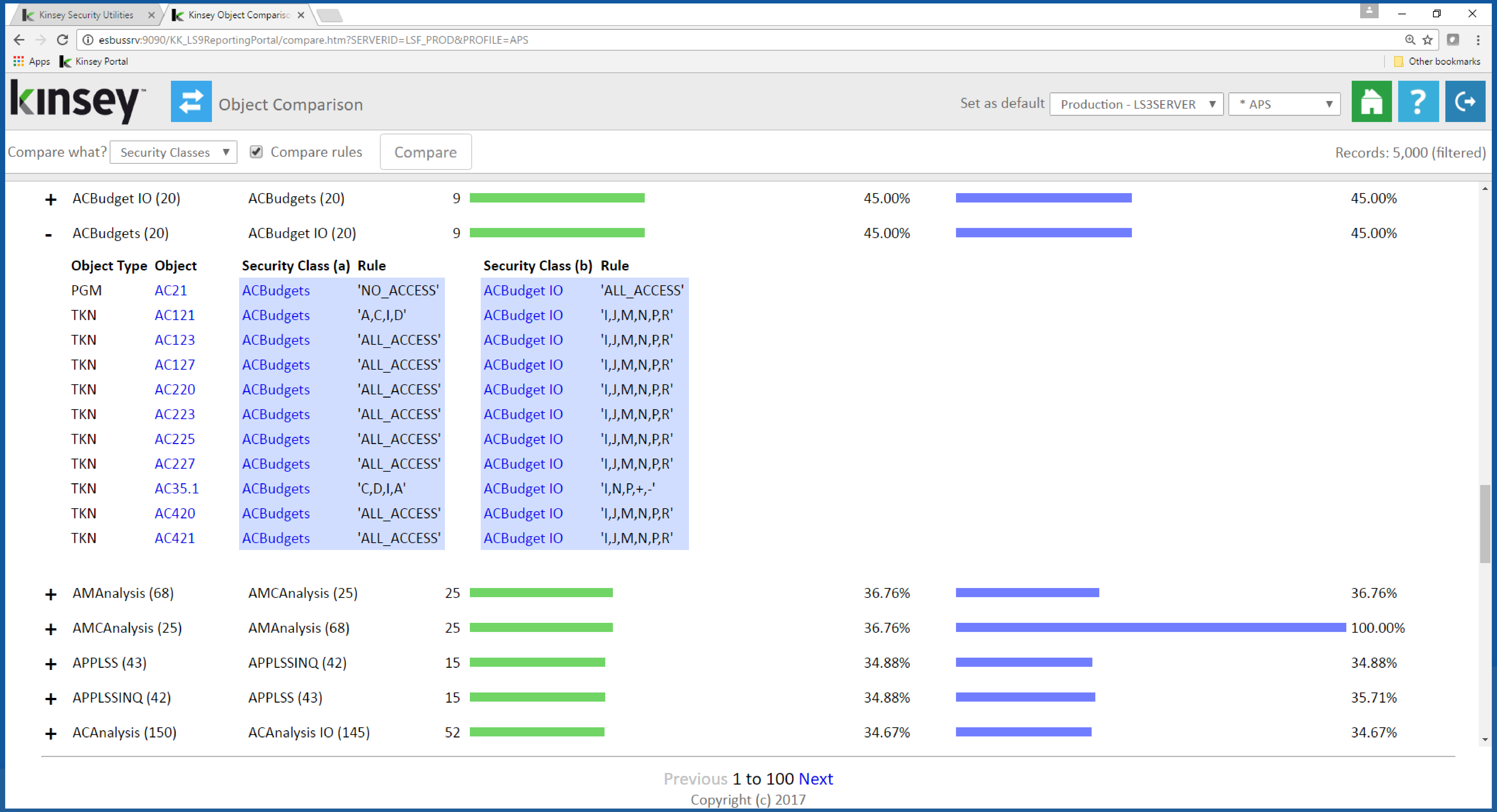
- Eliminate the duplicates which always cause maintenance nightmares.
- Compare and consolidate Roles and Security Classes.

DA

Eliminating Duplicate Roles & Security Classes

Reports

Role & Security Class Comparisons



Kinsey Security Utilities
Kinsey Object Comparis…
esbussrv:9090/KK_LS9ReportingPortal/compare.htm?SERVERID=LSF_PROD&PROFILE=APS
Apps
Kinsey Portal
Other bookmarks
kinsey
Object Comparison

Set as default: Production - LS3SERVER ▾ | * APS ▾

Compare what? Security Classes ▾ ☑ Compare rules [Compare]

Records: 5,000 (filtered)

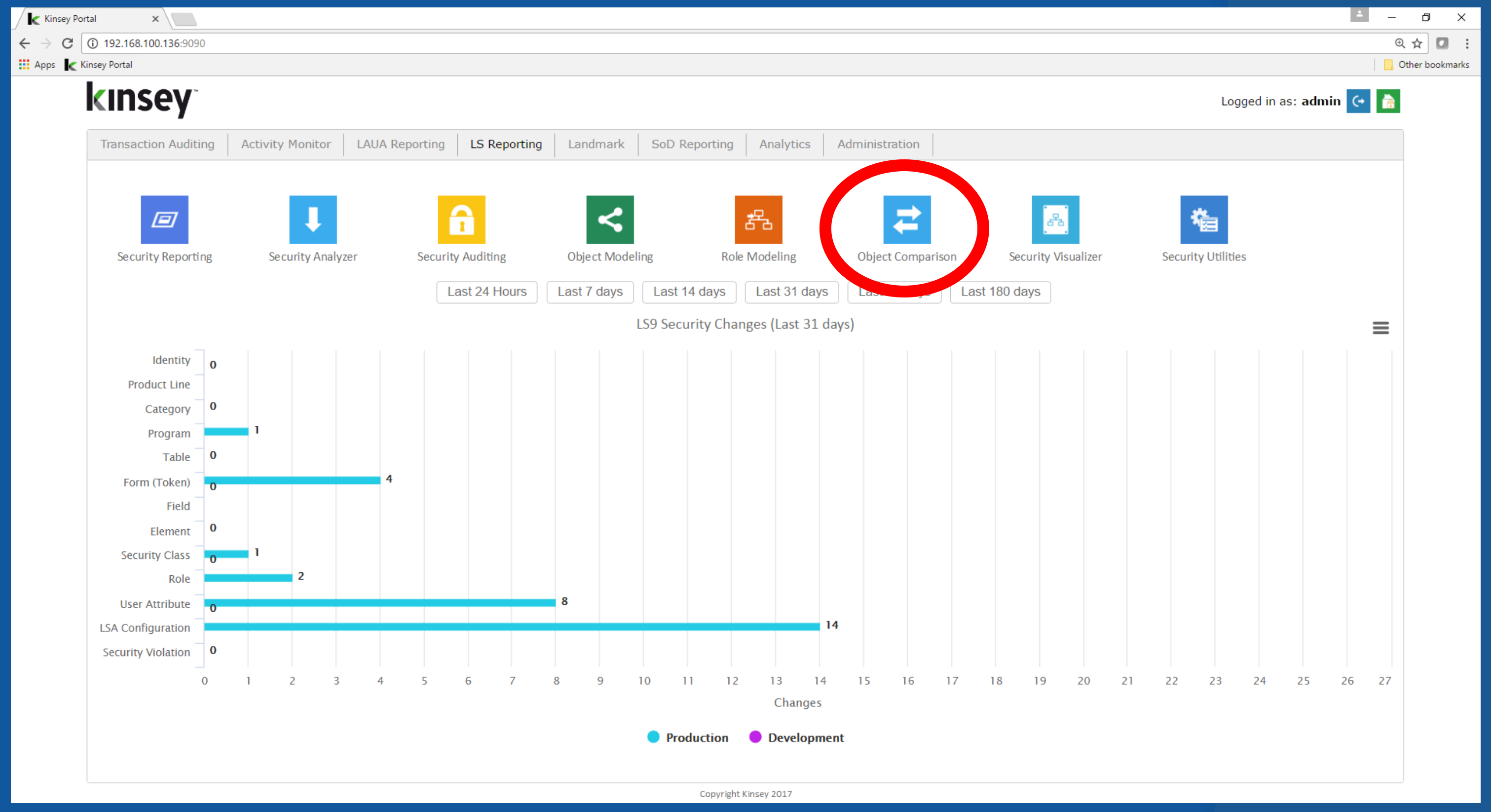
+	ACBudget IO (20)	ACBudgets (20)	9	45.00%	45.00%
-	ACBudgets (20)	ACBudget IO (20)	9	45.00%	45.00%

Object Type	Object	Security Class (a)	Rule	Security Class (b)	Rule
PGM	AC21	ACBudgets	'NO_ACCESS'	ACBudget IO	'ALL_ACCESS'
TKN	AC121	ACBudgets	'A,C,I,D'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC123	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC127	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC220	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC223	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC225	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC227	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC35.1	ACBudgets	'C,D,I,A'	ACBudget IO	'I,N,P,+,-'
TKN	AC420	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'
TKN	AC421	ACBudgets	'ALL_ACCESS'	ACBudget IO	'I,J,M,N,P,R'

+	AMAnalysis (68)	AMCAnalysis (25)	25	36.76%	36.76%
+	AMCAnalysis (25)	AMAnalysis (68)	25	36.76%	100.00%
+	APPLSS (43)	APPLSSINQ (42)	15	34.88%	34.88%
+	APPLSSINQ (42)	APPLSS (43)	15	34.88%	35.71%
+	ACAnalysis (150)	ACAnalysis IO (145)	52	34.67%	34.67%

Previous 1 to 100 Next

Copyright (c) 2017



DA

Standardizing Roles

Why we do this

- Makes the security model easier to maintain and less prone to error.

Our Recommendation

Put all of the standard Roles…

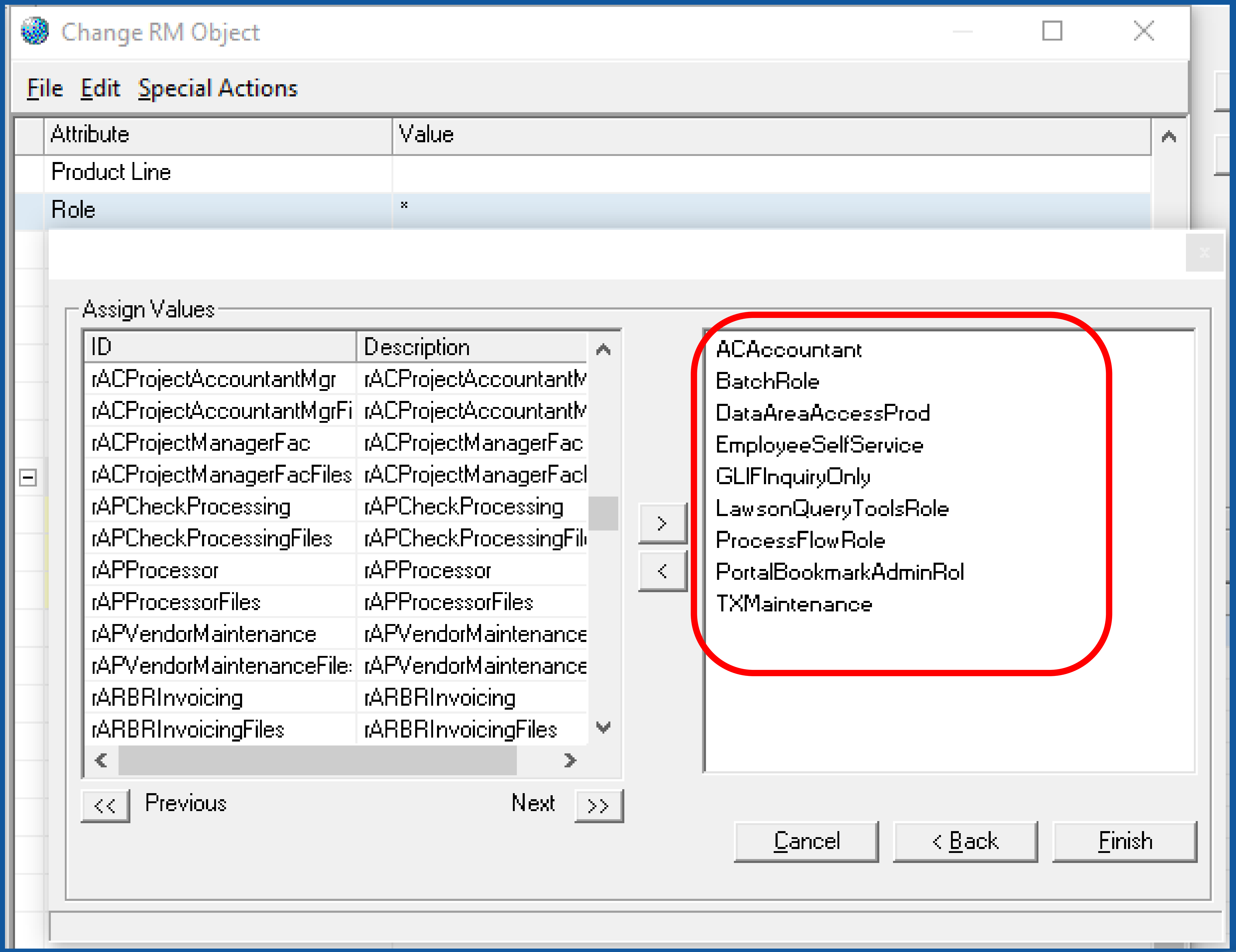
BatchRole; LawsonQueryToolsRole; ProcessFlowRole; PortalBookmarkAdminRole; Data Area Access Role

…into ONE single Role named something like:

- 1KinseyALL (starting with 1 so it always sorts to the top to be quickly assigned to users).
- Give 1KinseyALL to every new/changed user and forget about those other Roles.

Standardizing Roles

Typical Setup

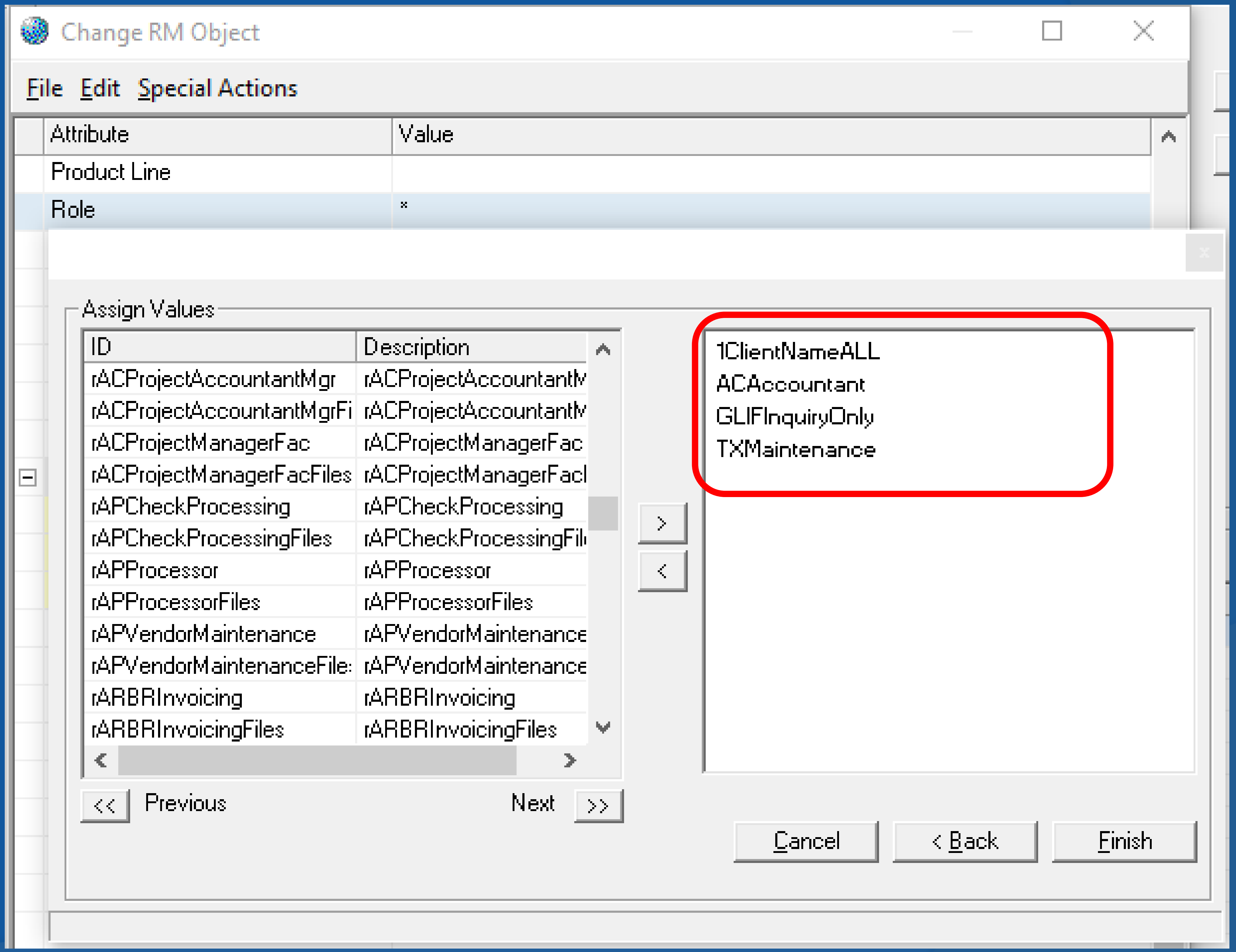


Attribute	Value
Product Line	
Role	*

ID	Description
rACProjectAccountantMgr	rACProjectAccountantM
rACProjectAccountantMgrFi	rACProjectAccountantM
rACProjectManagerFac	rACProjectManagerFac
rACProjectManagerFacFiles	rACProjectManagerFacl
rAPCheckProcessing	rAPCheckProcessing
rAPCheckProcessingFiles	rAPCheckProcessingFil
rAPProcessor	rAPProcessor
rAPProcessorFiles	rAPProcessorFiles
rAPVendorMaintenance	rAPVendorMaintenance
rAPVendorMaintenanceFile:	rAPVendorMaintenance
rARBRInvoicing	rARBRInvoicing
rARBRInvoicingFiles	rARBRInvoicingFiles

ACAccountant
BatchRole
DataAreaAccessProd
EmployeeSelfService
GLIFInquiryOnly
LawsonQueryToolsRole
ProcessFlowRole
PortalBookmarkAdminRol
TXMaintenance

Optional Setup



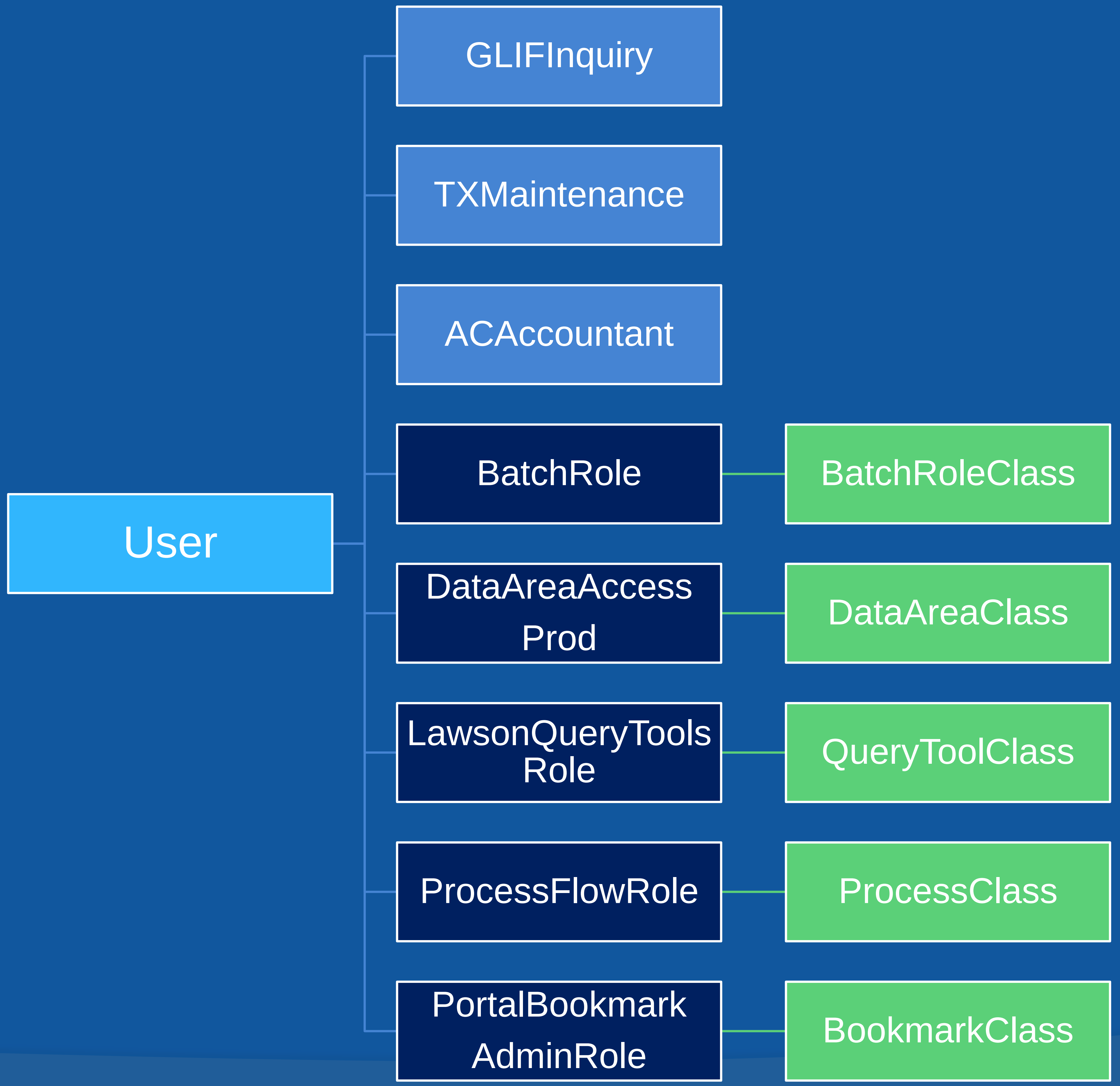
Attribute	Value
Product Line	
Role	*

ID	Description
rACProjectAccountantMgr	rACProjectAccountantM
rACProjectAccountantMgrFi	rACProjectAccountantM
rACProjectManagerFac	rACProjectManagerFac
rACProjectManagerFacFiles	rACProjectManagerFacl
rAPCheckProcessing	rAPCheckProcessing
rAPCheckProcessingFiles	rAPCheckProcessingFil
rAPProcessor	rAPProcessor
rAPProcessorFiles	rAPProcessorFiles
rAPVendorMaintenance	rAPVendorMaintenance
rAPVendorMaintenanceFile:	rAPVendorMaintenance
rARBRInvoicing	rARBRInvoicing
rARBRInvoicingFiles	rARBRInvoicingFiles

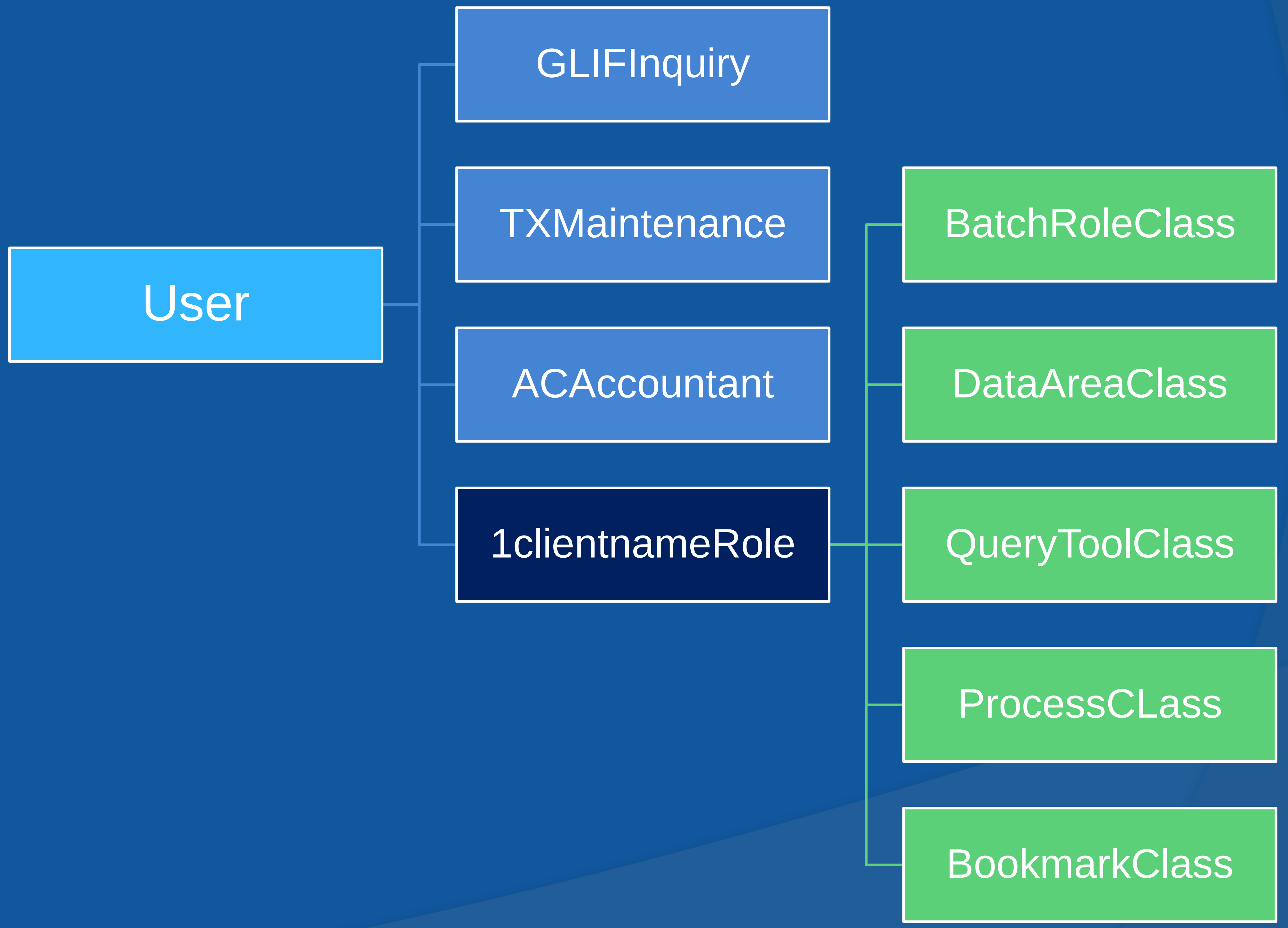
1ClientNameALL
ACAccountant
GLIFInquiryOnly
TXMaintenance

Standardizing Roles

Typical Setup



Optional Setup



Synchronizing your Environments

Why it's important

Many companies have moved well-tested patches or modifications from TEST to PROD, only to have them fail in PROD! Now what do you do?

- You have crucial tests underway in TEST – you can't risk those by simply copying PROD security onto TEST.
- And you have security rules in TEST that you're testing – you can't lose those!
- You could endeavor to ferret out everything that's different, if you only had lots of time for that.

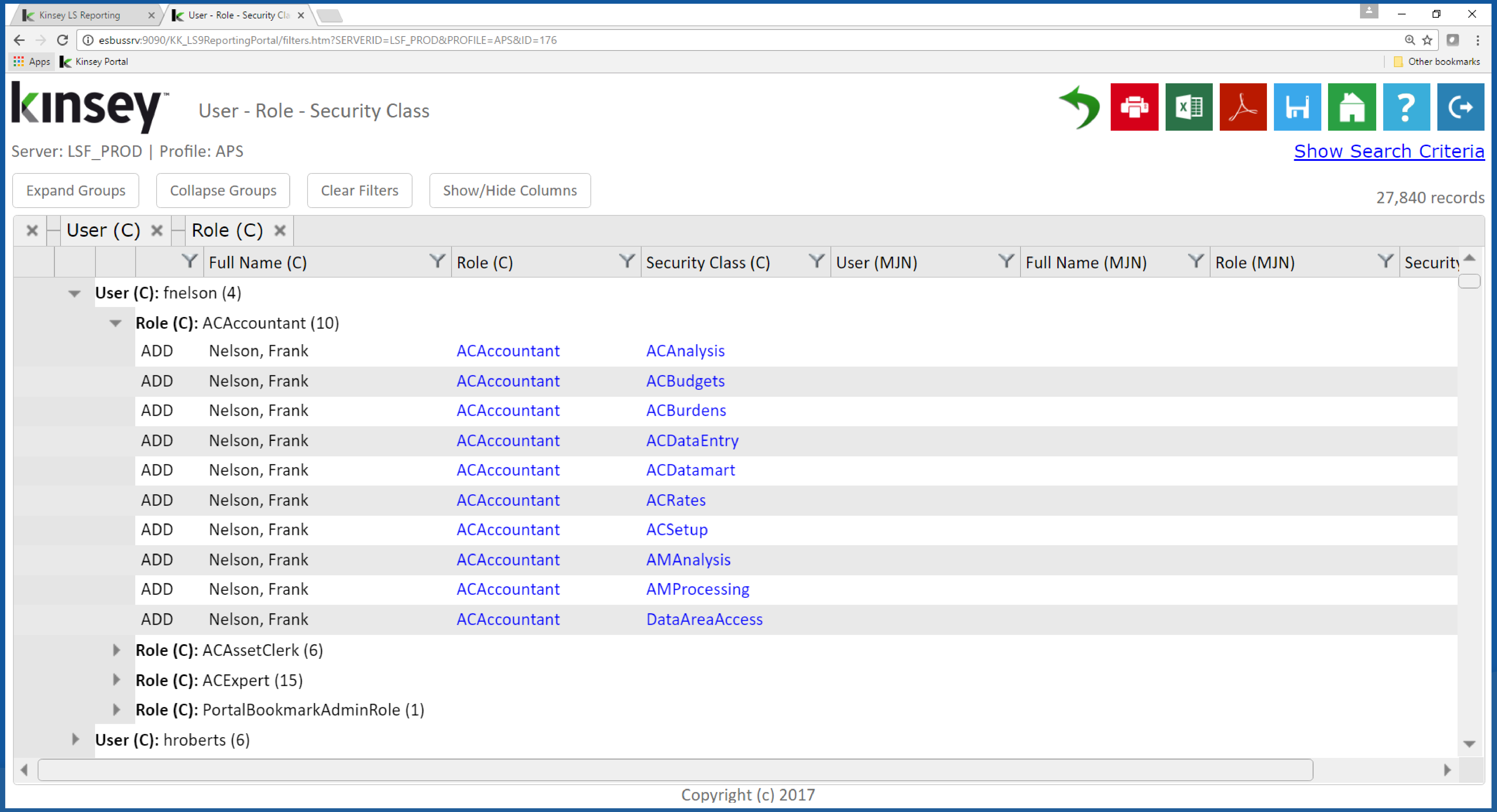
Our Solution

- We'll do a comprehensive comparison of security between the TEST and PROD, determine the significance of differences, and synchronize the two in the most effective manner.

Synchronizing your Environments

Our Reports

- Environment and Profile Security Comparisons



Kinsey LS Reporting
User - Role - Security Cla
esbussrv:9090/KK_LS9ReportingPortal/filters.htm?SERVERID=LSF_PROD&PROFILE=APS&ID=176
Apps
Kinsey Portal
Other bookmarks
kinsey

User - Role - Security Class

Server: LSF_PROD | Profile: APS

Show Search Criteria

Expand Groups | Collapse Groups | Clear Filters | Show/Hide Columns

27,840 records

× User (C) × Role (C) ×

User (C): fnelson (4)

Role (C): ACAccountant (10)

	Full Name (C)	Role (C)	Security Class (C)	User (MJN)	Full Name (MJN)	Role (MJN)	Security
ADD	Nelson, Frank	ACAccountant	ACAnalysis				
ADD	Nelson, Frank	ACAccountant	ACBudgets				
ADD	Nelson, Frank	ACAccountant	ACBurdens				
ADD	Nelson, Frank	ACAccountant	ACDataEntry				
ADD	Nelson, Frank	ACAccountant	ACDatamart				
ADD	Nelson, Frank	ACAccountant	ACRates				
ADD	Nelson, Frank	ACAccountant	ACSetup				
ADD	Nelson, Frank	ACAccountant	AMAnalysis				
ADD	Nelson, Frank	ACAccountant	AMProcessing				
ADD	Nelson, Frank	ACAccountant	DataAreaAccess				

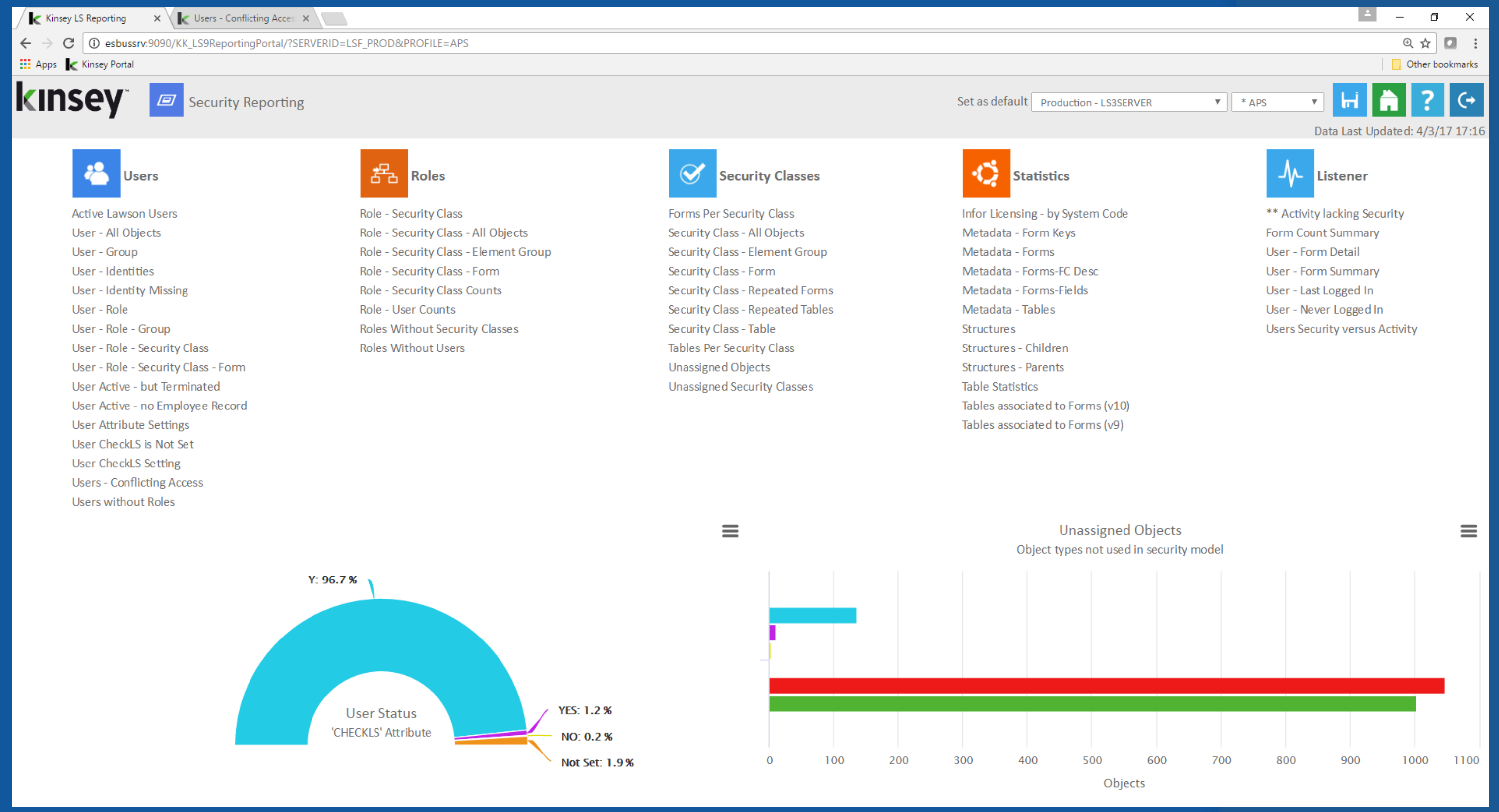
Role (C): ACAssetClerk (6)

Role (C): ACExpert (15)

Role (C): PortalBookmarkAdminRole (1)

User (C): hroberts (6)

Copyright (c) 2017



Set as default: Production - LS3SERVER | * APS

Data Last Updated: 4/3/17 17:16

Users

- Active Lawson Users
- User - All Objects
- User - Group
- User - Identities
- User - Identity Missing
- User - Role
- User - Role - Group
- User - Role - Security Class
- User - Role - Security Class - Form
- User Active - but Terminated
- User Active - no Employee Record
- User Attribute Settings
- User CheckLS is Not Set
- User CheckLS Setting
- Users - Conflicting Access
- Users without Roles

Roles

- Role - Security Class
- Role - Security Class - All Objects
- Role - Security Class - Element Group
- Role - Security Class - Form
- Role - Security Class Counts
- Role - User Counts
- Roles Without Security Classes
- Roles Without Users

Security Classes

- Forms Per Security Class
- Security Class - All Objects
- Security Class - Element Group
- Security Class - Form
- Security Class - Repeated Forms
- Security Class - Repeated Tables
- Security Class - Table
- Tables Per Security Class
- Unassigned Objects
- Unassigned Security Classes

Statistics

- Infor Licensing - by System Code
- Metadata - Form Keys
- Metadata - Forms
- Metadata - Forms-FC Desc
- Metadata - Forms-Fields
- Metadata - Tables
- Structures
- Structures - Children
- Structures - Parents
- Table Statistics
- Tables associated to Forms (v10)
- Tables associated to Forms (v9)

Listener

- ** Activity lacking Security
- Form Count Summary
- User - Form Detail
- User - Form Summary
- User - Last Logged In
- User - Never Logged In
- Users Security versus Activity

Other Security Services

- Reviewing the Organization’s Onboarding Process and Automating Procedures.
- Landmark Security Review
- Environment Identities - what is required based on Online or Batch user?
- What are your Privileged Identities and when are they used?
- PHI/PII Security Review
- Demonstrate features of ISS and assist with the sync.
- Any other issues you are currently experiencing.

Complimentary Solutions

Security Reporting

- User
- Role
- Security Class
- Usage Comparison

SOD Reporting

- 200+ Prebuilt Policies
- Violation Reports
- Email Notifications

Security Auditing

- Audit all object changes
- Email Notifications

Transaction Auditing

- Selectively audit over 6500 Lawson Forms

Activity Monitor

- Audit
- Security Tuning
- Unauthorized Access

SOD Remediation

- Risk Analysis Grid
- Security Modeling

Security Modeling

- Build What-if scenarios for Users, Roles, Forms

Landmark Reporting

- Actor
- Role
- Security Class
- Lawson LPL Detail

Security Well-Check

Security Review

Our team of security consultants will review your existing configuration and make recommendations on potential changes.

Security Consulting

Our analysis will include a Statement of Work for our consultants to assist you with implementing any changes.

Applications

During the review process you will have full use of Kinsey's Security and SoD Reporting tools at no charge.

Contact Us

Kinsey & Kinsey, Inc.
26 North Park Boulevard
Glen Ellyn, IL. 60137
630-858-4866

✉ g.henson@kinsey.com

call 757-621-8236

www.kinsey.com

Thank you for attending!

We hope you found it helpful!