# Security Setup and Configuration

Copyright 2003-2023 OneVizion, Inc All Rights Reserved

# Security Set-Up and Configuration

OneVizion
Simply Smarter Information Management

## This Lesson will Cover ….

- The OneVizion Security System
  - Default Privileges
  - Security Groups/Tokens
  - Special Workplan Task Privileges
  - Lock/Unlock Privileges
  - Trackor Restrictions
  - Disciplines
  - Menu Applications
  - Global View and Filters
  - Global Portals
  - Rules
  - Imports
  - Reports and Report Delivery
  - Notifications and Notification Types
  - Assigned Users
  - Component Packages
  - Component Audit Log

# Security Best Practices, Topics and Recommendations

OneVizion
Simply Smarter Information Management

- The OneVizion Security Model is based upon Security Roles
- Security Roles control:
  - Access to information contained in the system
  - Privileges with regard to access (R-E-A-D or None)
  - Access to system functions (e.g., menus, admin tools, etc.)
- A good way to commence security set-up is to create an Administrative Superuser and a General User Security role.  Clone the General User Security Role and add or remove privileges based upon Job Function.
- In addition to an Admin Superuser, Security Roles can be created to grant limited administrative features to lower level admins (e.g., create reports or run imports)
- Security Privileges are generally controlled at the Role level, but, can be overridden at the individual User level

# Security Best Practices, Topics and Recommendations

OneVizion
Simply Smarter Information Management

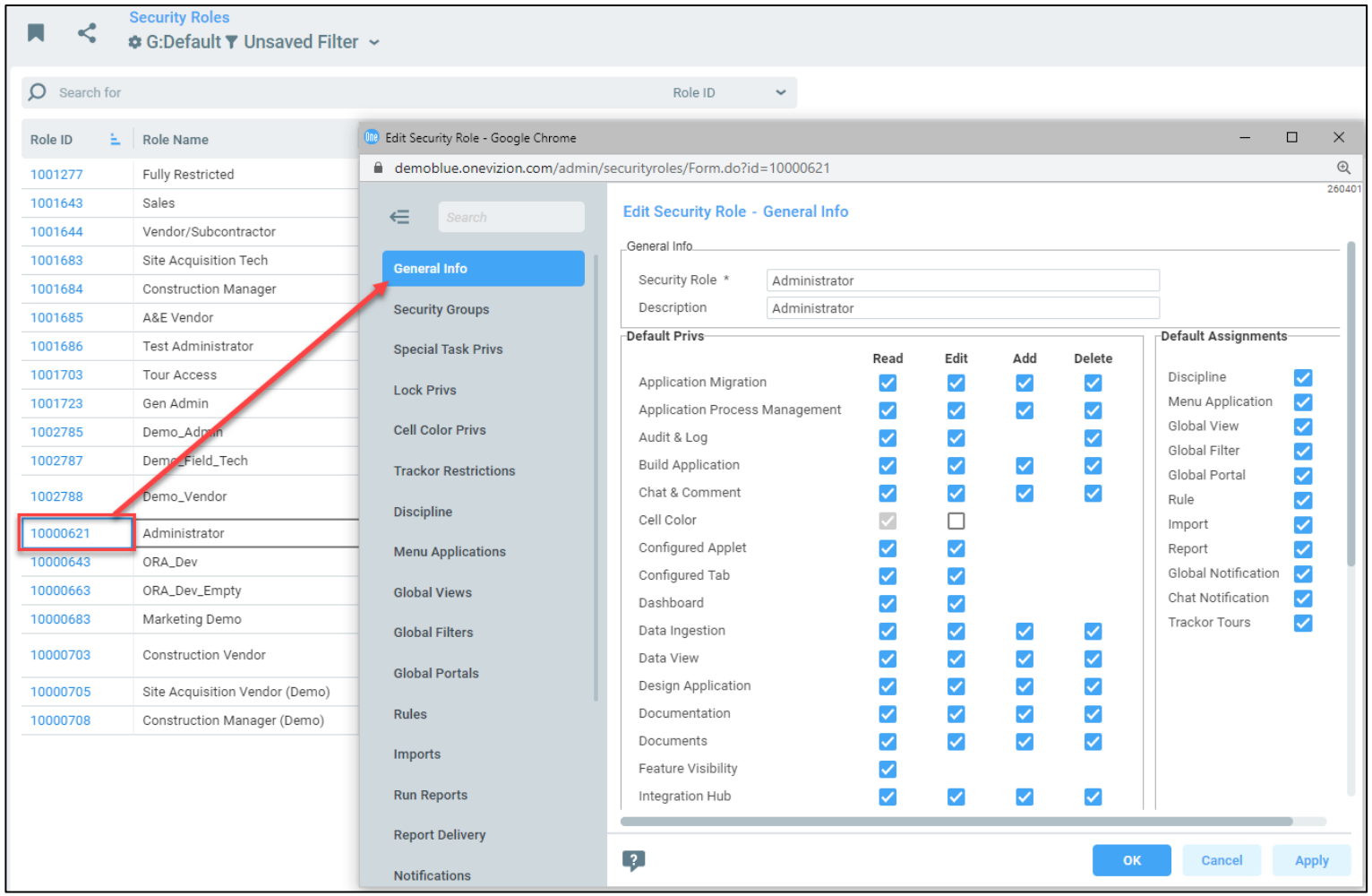
- Use Business Rules to enforce password requirements (e.g., expiration, format, etc.)
- Create a limited set of Global Views and Filters then let users modify the Global Views to create their own job-specific Local Views and Filters
- Use Security Roles to control access to data at the tab level and to control the ability to create relationships among Trackor Types
- Assign multiple Security Roles to a User(s) to grant a Union of all privileges. Use the “None” flag to remove a privilege.
- Security Roles can be augmented with Business Rules to further increase flexibility and granularity
- Use Trackor Restrictions to control access to records based upon Parent-Child relationships

# Security Best Practices, Topics and Recommendations

OneVizion
Simply Smarter Information Management

- Security Roles can be used in conjunction with Menu Applications to steer user behavior and limit access to data and system functionality.
- Security Role-based Task Privileges and Disciplines can be used to control R-E-A-D privileges to Workplan tasks – down to the individual task level
- Any Trackor Type in the system can be designated a OneVizion user – you are not limited to the User Trackor Type (e.g., Vendors, Customers)
- Use Security Roles to control access to Lock/Unlock functionality
- Use Security Roles to control access to Notifications and Notification Types
- Use Security Roles to control access to Global Portals
- Use Security Roles to control “default” privileges for new system objects

# Security – Default Privileges (General Info)



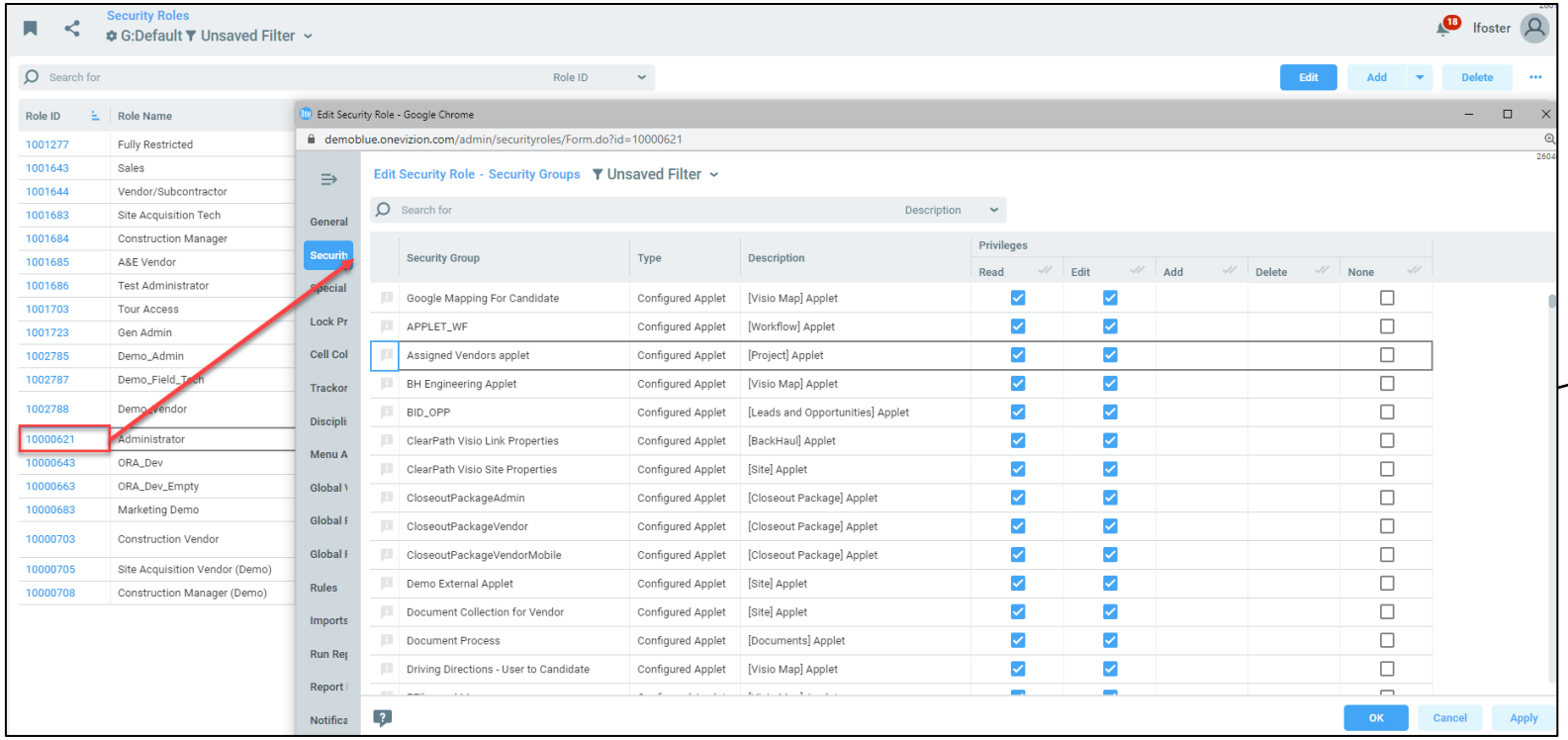

HINT: The "Login As" feature is extremely useful when testing system Security Settings. Another helpful approach is to login as a "test user" using one Browser (i.e., Chrome) while still being logged in as SysAdmin using a different Browser (i.e., Firefox)

The "inherited" privileges of new objects added to the Vizion Platform are controlled from the General Info tab

# Security – Security Groups

HINT: Quick Search to find tokens and
✓✓ to Select All in a Filtered Data Set

OneVizion
Simply Smarter Information Management




Use Security Tokens to set privileges for:

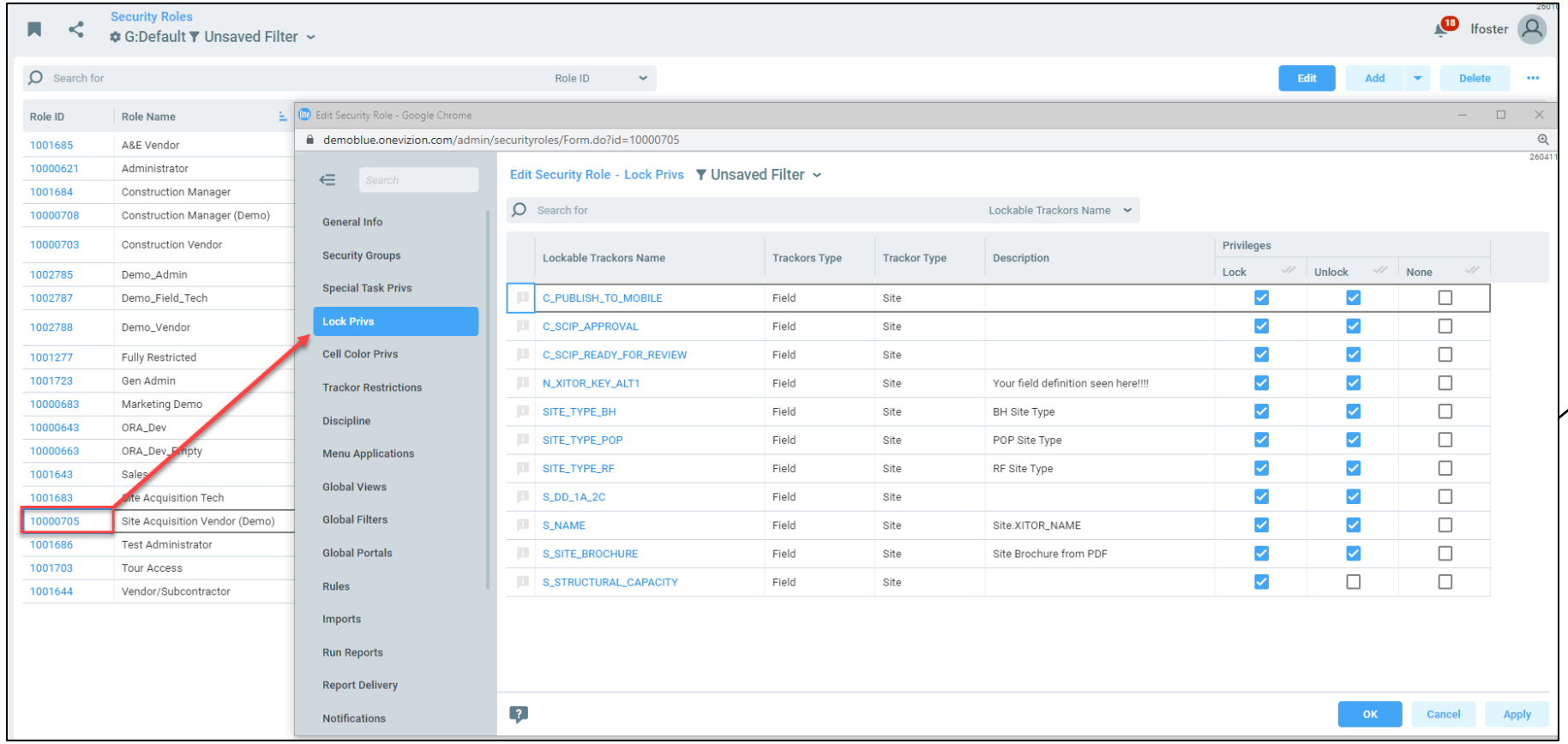
- Applets
- Configured Tabs
- Dashboards
- Trackor Relationships
- Super User Privileges
- Trackor Types
- Workplan Tasks

R=Read
E=Edit
A=Add
D=Delete
and, None

HINT: New Security Tokens are Automatically created as new components are added

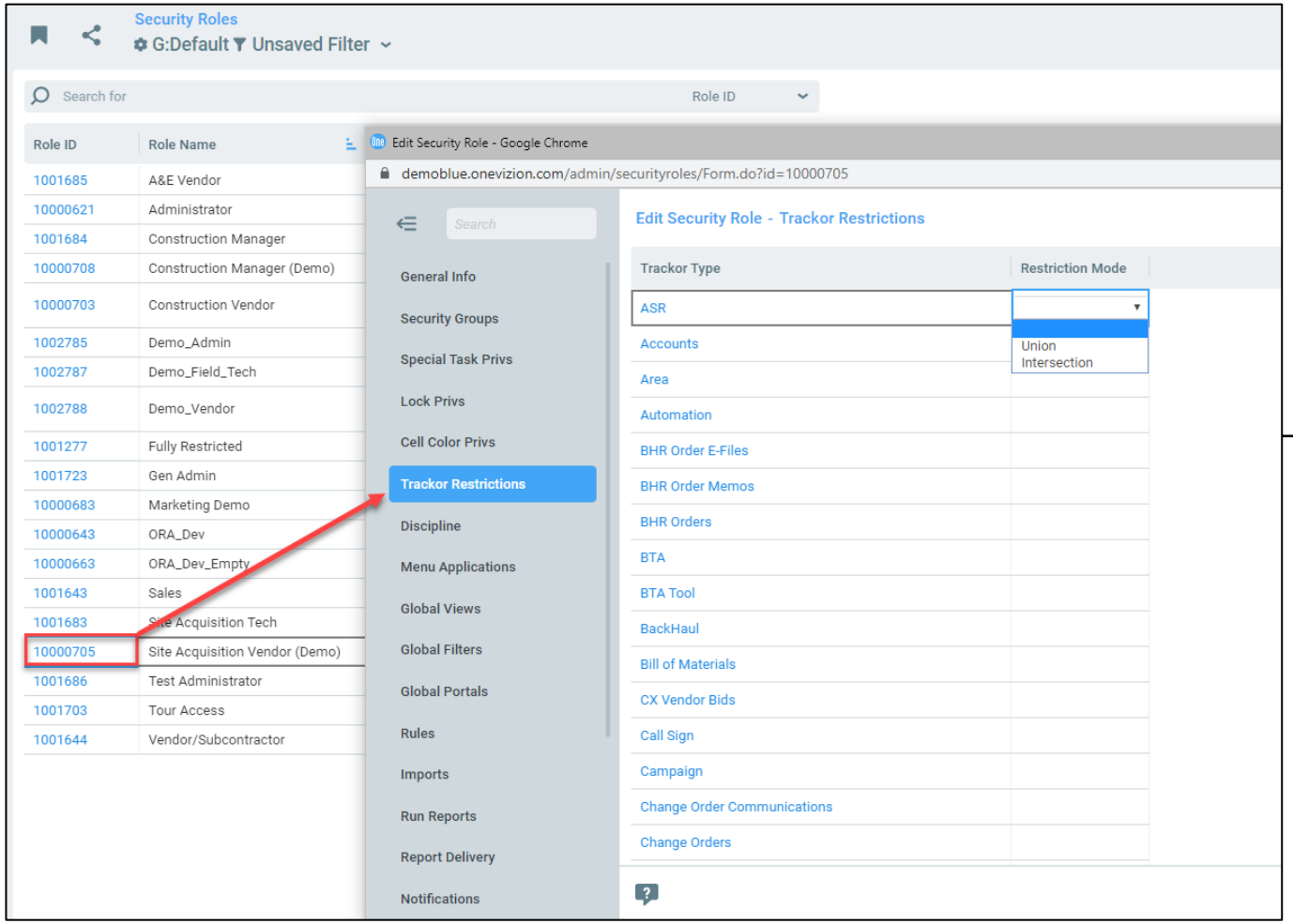
REMINDER – Adding a “None” Removes that Privilege

# Security – Lock Privileges




A list will be presented of all Configured Fields in the system that have the Lock flag set. SetLock/Unlock privileges for that Security Role.

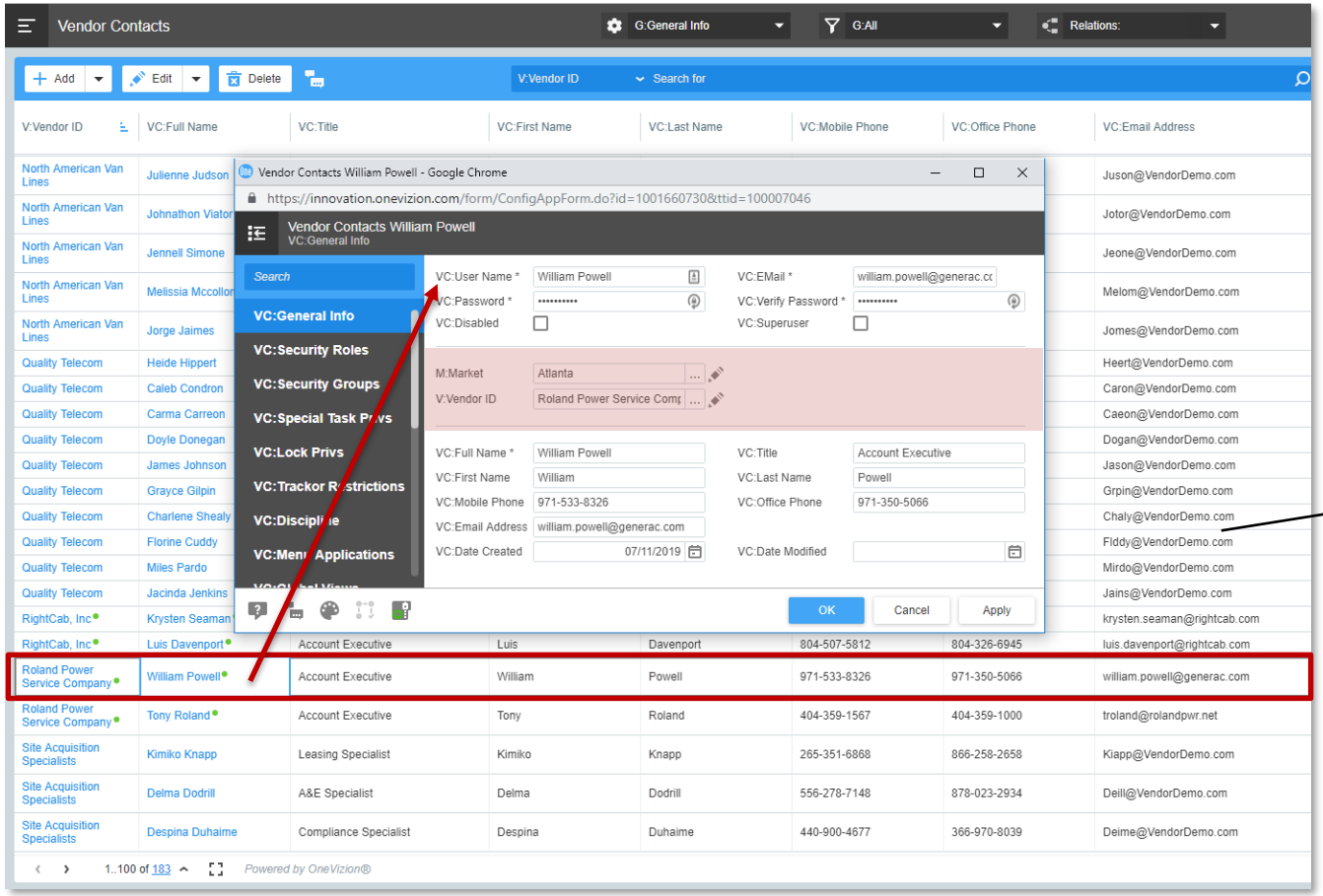
# Security – Trackor Restrictions




Trackor Restrictions are used to restrict which RECORDS a user can see.

1. Determine what Trackor Type(s) you wish to Restrict
2. Construct appropriate Parent-Child Relationships
3. Set Restriction Mode
4. Restrictions are applied to that Security Role only (e.g., Vendor)

# Security – Trackor Restrictions




We have made the Vendor Contact Trackor Type a User which allows us to assign User credentials AND restrict access to records for Vendor Contact users based upon Security Role Trackor Restrictions.

It is common practice to create separate Trackor Types for business partners such as Customers and Vendors and give them access to the system. These can be managed in their own user Trackors.

# Trackor Restrictions

| Vendor Contact | Vendor | Market |
|---|---|---|
| William Powell | Roland Power Service Company | Atlanta |
| Tony Roland | Roland Power Service Company | Los Angeles |

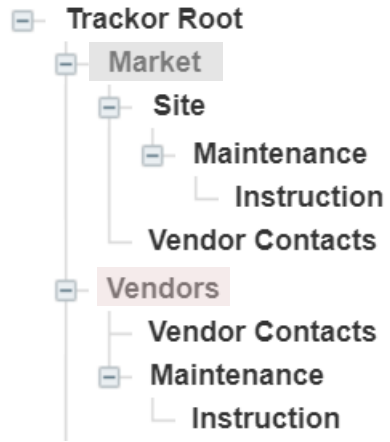
| Maint:Maintenance ID | M:Market | V:Vendor ID | Maint:Maintenance Class |
|---|---|---|---|
| AL13936-0000 | Atlanta | Southeast Generator Service, Inc. | Generator |
| AL13936-0001 | Atlanta | Coolray HVAC | HVAC |
| AL13936-0002 | Atlanta | Roland Power Service Company | Generator |
| AL13936-0003 | Atlanta | RightCab, Inc | Cabinet |
| AL13936-0004 | Atlanta | EIC Solutions | HVAC |
| AL13936-0005 | Atlanta | Heating and Air Unlimited | HVAC |
| AZ15042-0004 | Arizona | Roland Power Service Company | Generator |
| CA10018-0000 | Atlanta | Coolray HVAC | HVAC |
| CA10018-0001 | Atlanta | Roland Power Service Company | Generator |
| CA10036-0002 | Los Angeles | Roland Power Service Company | Generator |
| CA11007-0001 | Los Angeles | Roland Power Service Company | Generator |
| CA11007-0002 | Los Angeles | Roland Power Service Company | Generator |
| FL13815-10001 | South Florida | Roland Power Service Company | Generator |
| GA17837-10000 | Atlanta | Telecom Cabinet Inspection Services, LLC | Cabinet |
| MA20623-0000 | Boston | Roland Power Service Company | Generator |

1..15 of 15 Powered by OneVizion®

OneVizion
Simply Smarter Information Management

## Trackor Restrictions set on Maintenance and Instruction

- UNION – Vendor Contact User sees all records that are assigned to his Company OR in his Market



# Trackor Restrictions

| Vendor Contact | Vendor | Market |
|---|---|---|
| William Powell | Roland Power Service Company | Atlanta |
| Tony Roland | Roland Power Service Company | Los Angeles |

## Vendor Contact = William Powell

| Maint:Maintenance ID | M:Market | V:Vendor ID | Maint:Maintenance Class |
|---|---|---|---|
| AL13936-0002 | Atlanta | Roland Power Service Company | Generator |
| CA10018-0001 | Atlanta | Roland Power Service Company | Generator |

1..2 of 2 Powered by OneVizion®

## Vendor Contact = Tony Roland

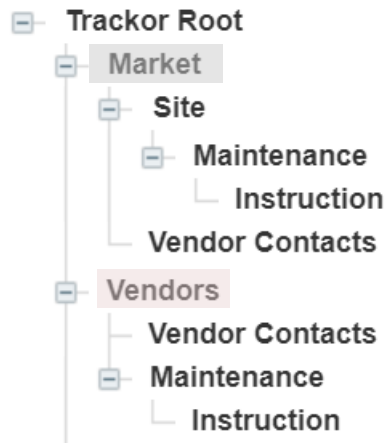
| Maint:Maintenance ID | M:Market | V:Vendor ID | Maint:Maintenance Class |
|---|---|---|---|
| CA10036-0002 | Los Angeles | Roland Power Service Company | Generator |
| CA11007-0001 | Los Angeles | Roland Power Service Company | Generator |
| CA11007-0002 | Los Angeles | Roland Power Service Company | Generator |

1..3 of 3 Powered by OneVizion®

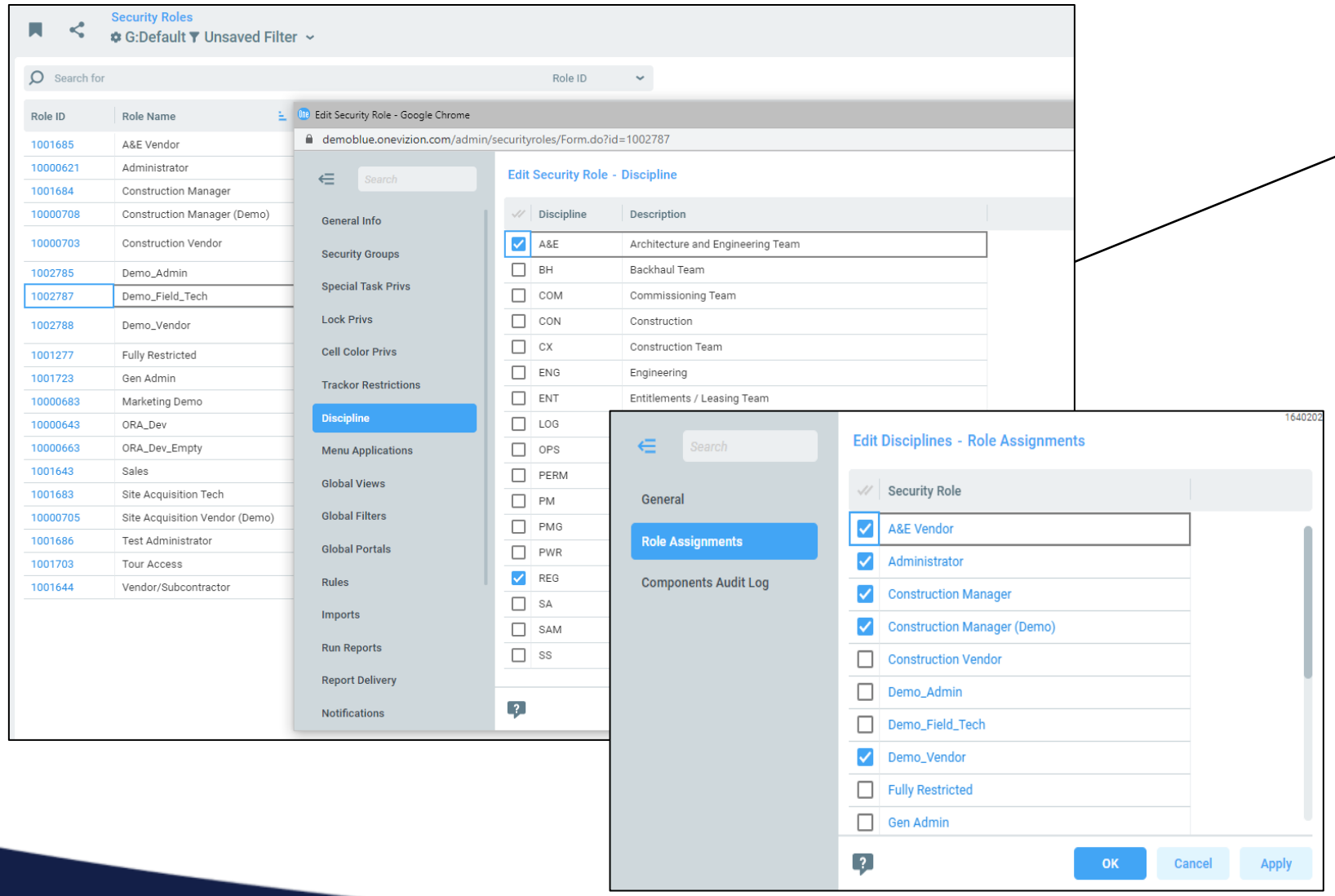
OneVizion
Simply Smarter Information Management

## Trackor Restrictions set on Maintenance and Instruction

- INTERSECTION – Vendor Contact User sees all records that are assigned to his Company AND are in his Market



# Security – Disciplines




Disciplines are another way of managing privileges related to Workplan Tasks. Workplan Tasks are assigned a Discipline and one or more Disciplines can be associated with a Security Role.

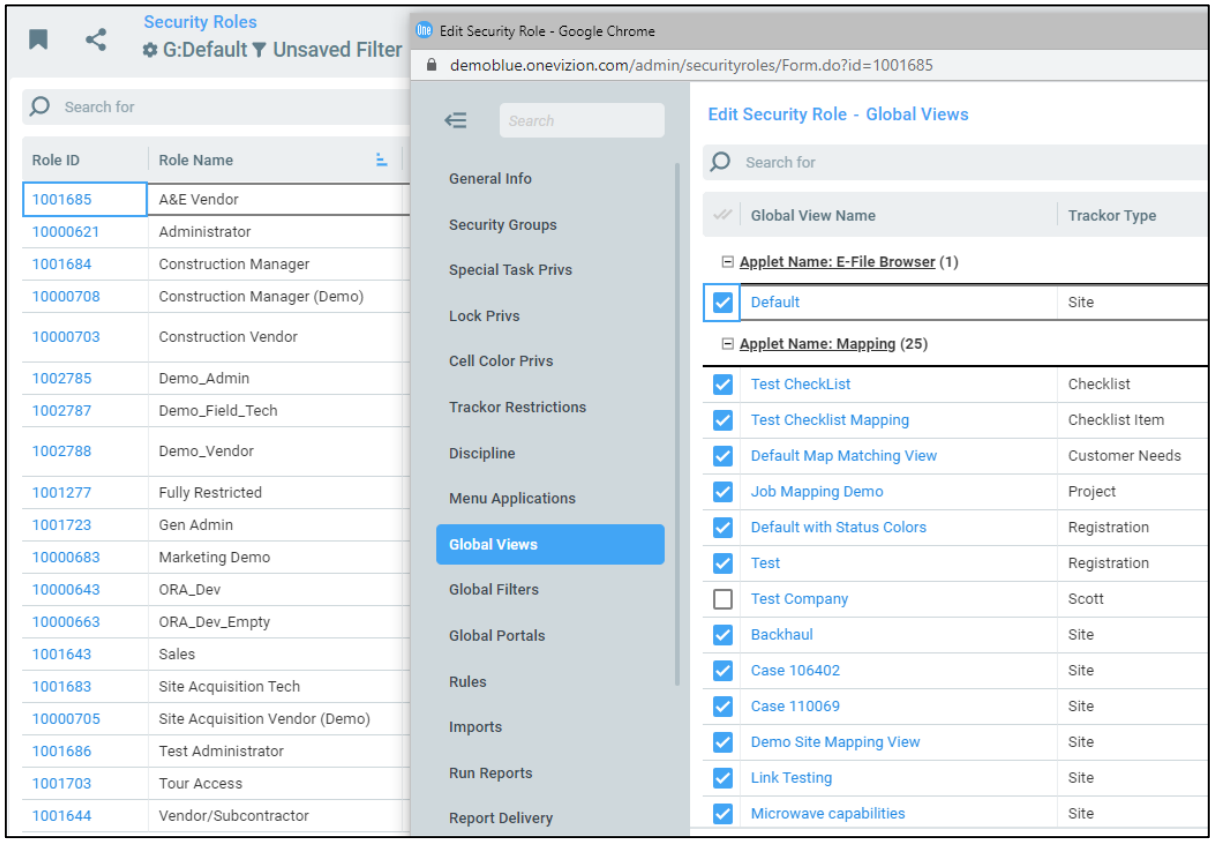
A user who is assigned a Security Role with a certain Discipline(s) can update Workplan Task Dates assigned to that Discipline.

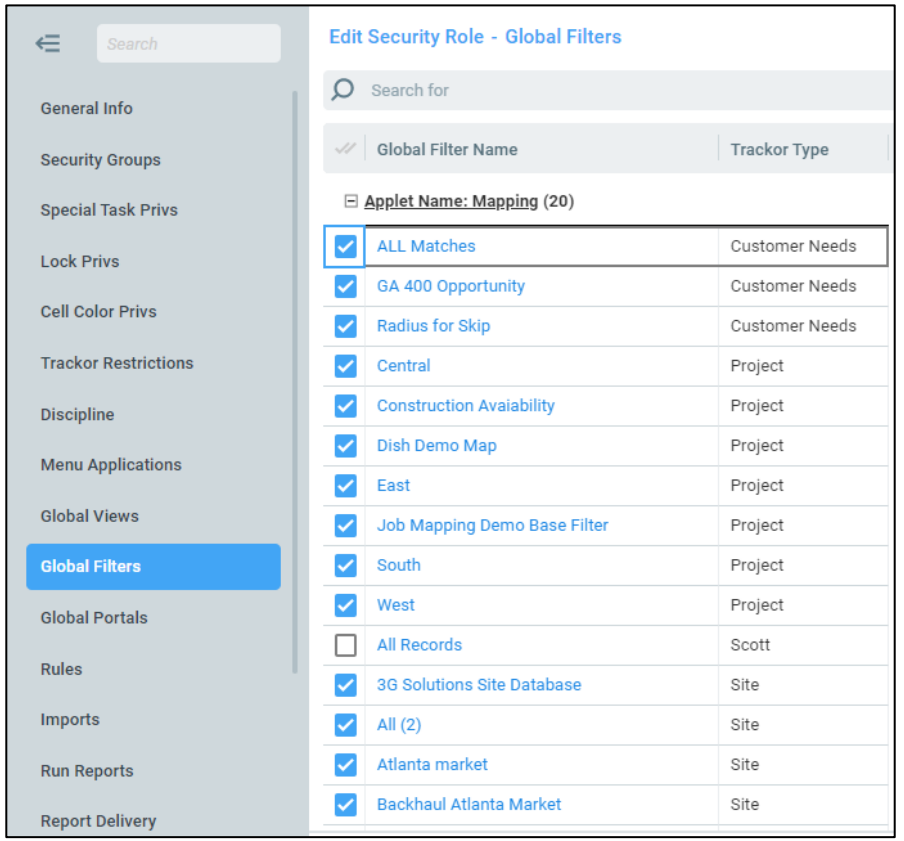
Special Workplan Task Privileges override Disciplines.

# Security – Global Views and Filters, Menus & Portal

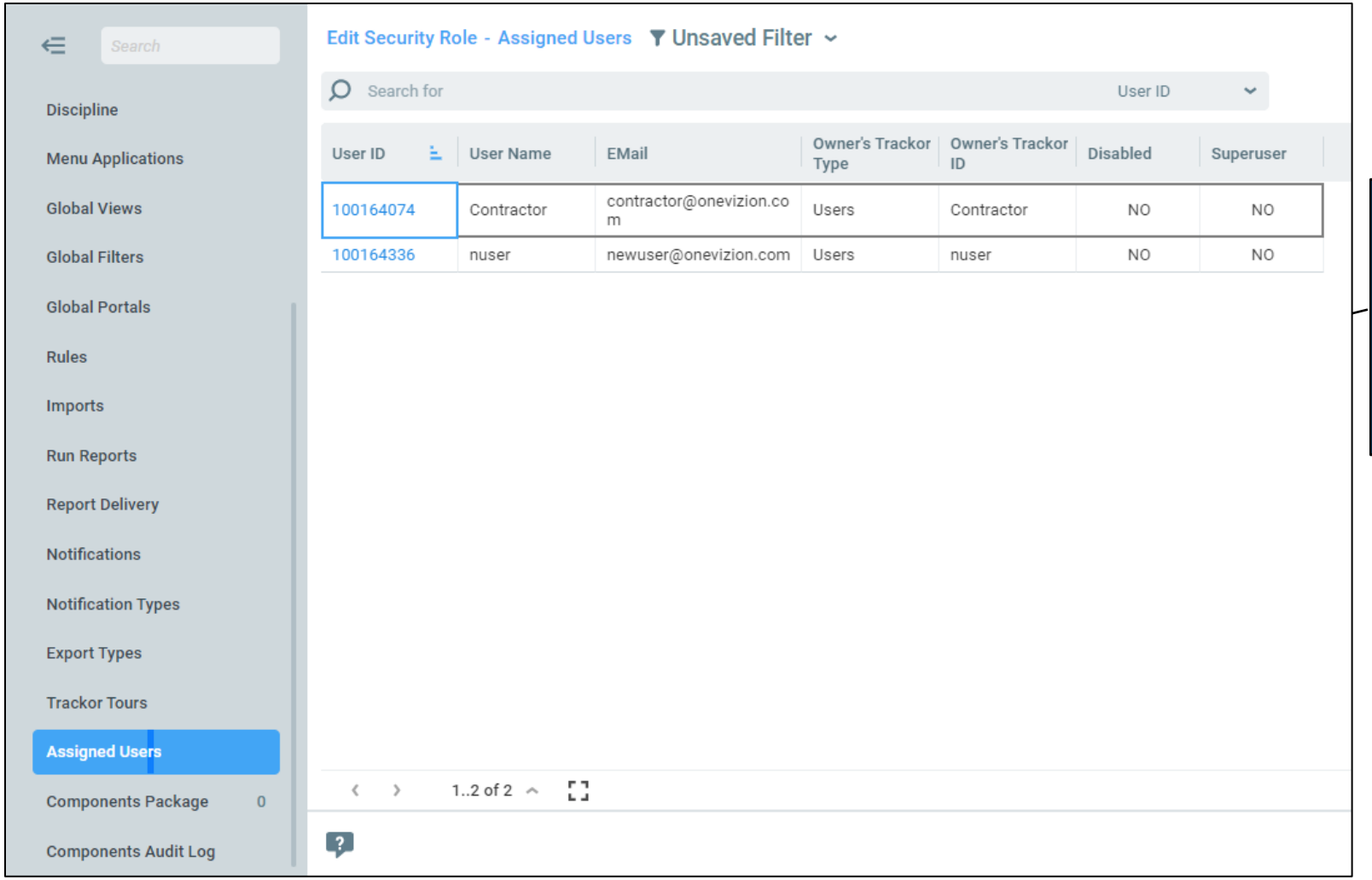
Simply Smarter Information Management

Security assignments for Global View and Filters, Menu Applications and Portals are simple and identical in concept.  Simply check the box for the appropriate item you wish to grant privileges to for the selected Security Role.



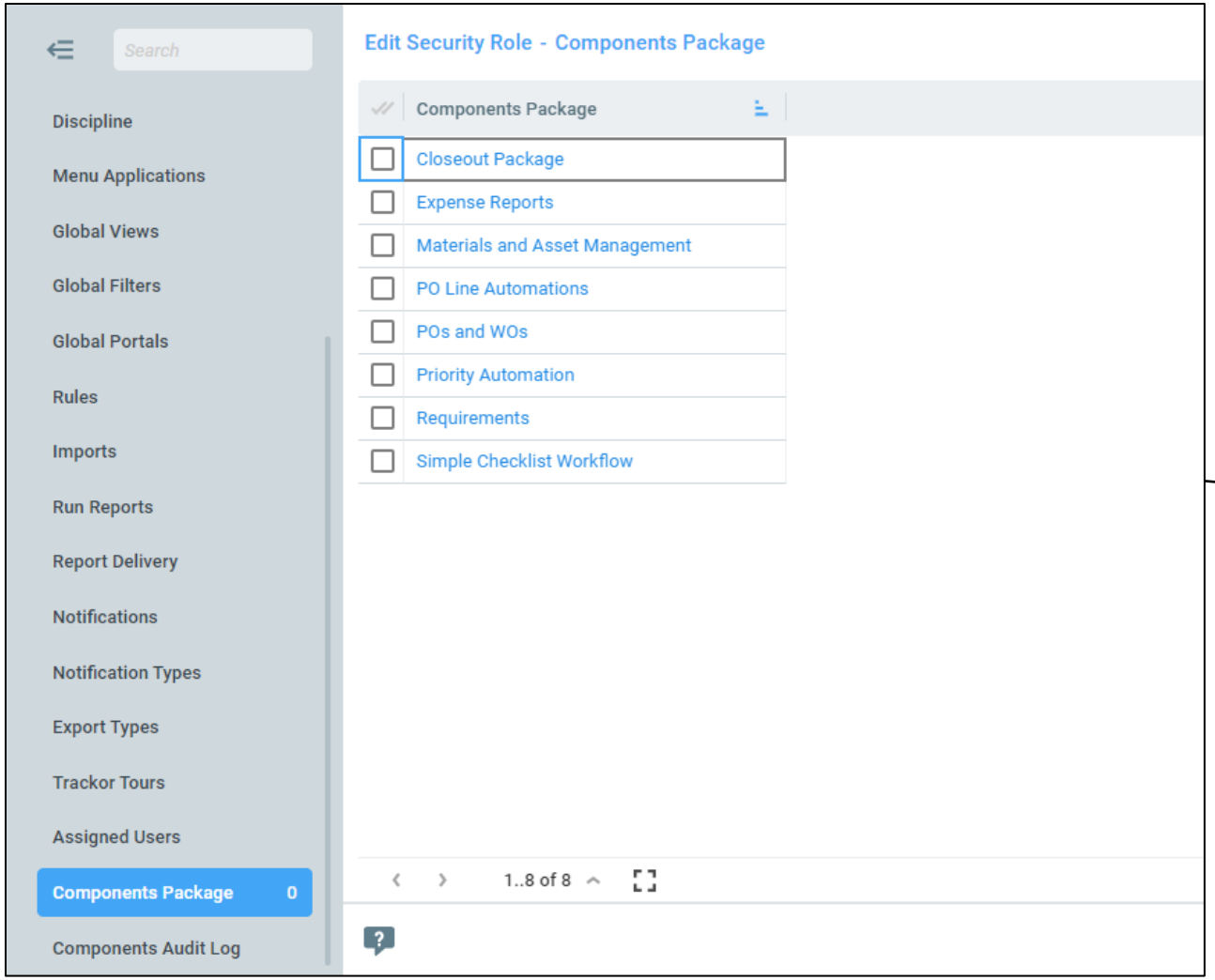



# Security – Assigned Users




The Assigned Users tab provides a list of all Users who are members of the selected Security Group.

# Security – Component Packages

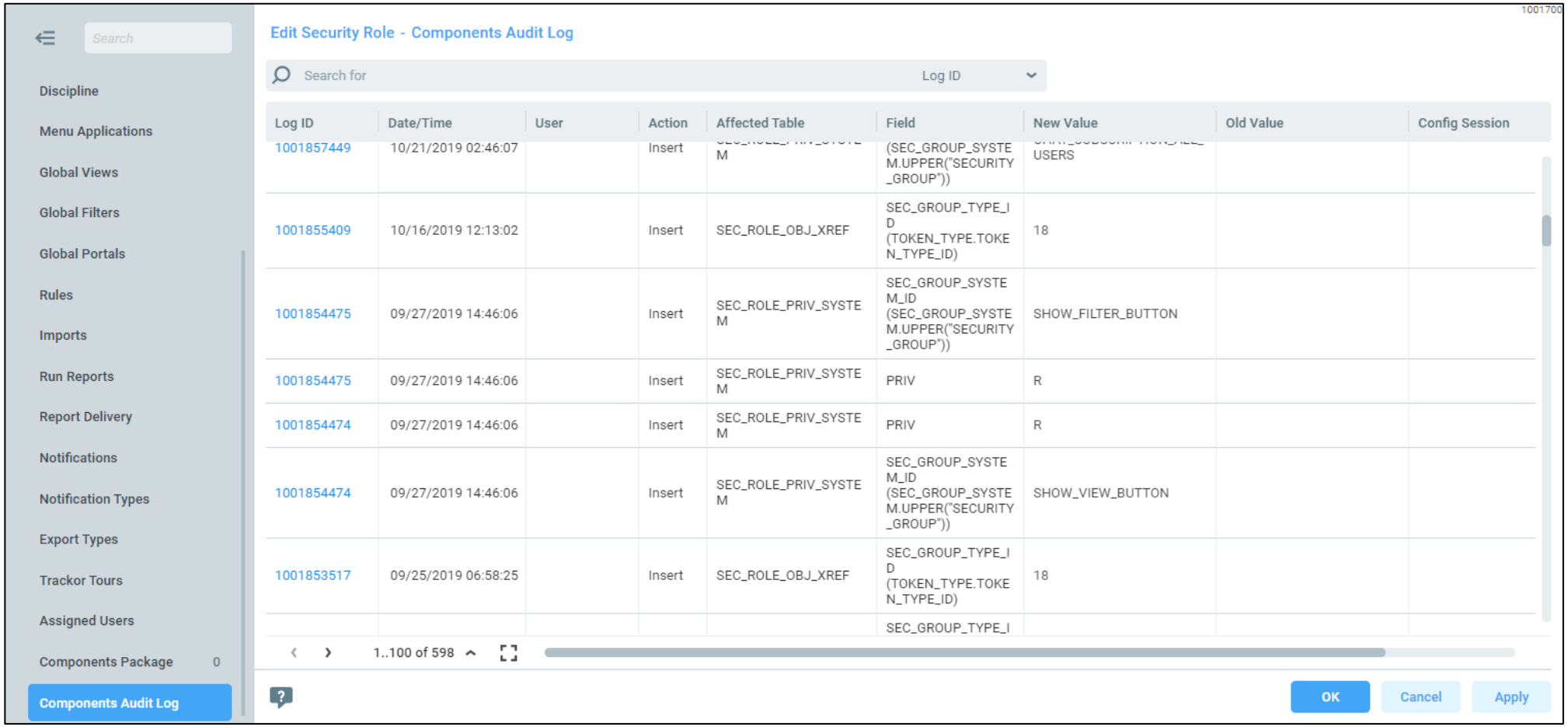



The Component Packages feature allows users to tag system components such as Trackor Types, Configured Fields, Tabs, Applets, Rules, Reports, etc. with a unique identifier. This effectively "groups" these components into a single package.

The Component Package tag can them be used to filter on all components that comprise that package when running the Components Export feature.

This provides users with a simple and easy way to manage the multiple components that might comprise a new application or applets.

# Security – Component Audit Log

The Security Component Audit Log tracks all additions, deletions and update made to a Security Role. The Component Audit Log tracks the Date/Time, the User making the transaction, the Action taken, the Field or Component acted upon, the Old Value and the Current Value. An optional Config Session ID can also be assigned.

OneVizion
Simply Smarter Information Management