Tivoli software

IBM

What's New in Maximo Security – Version 7.5

Colleen McCretton

Date of presentation: 8/2/2012

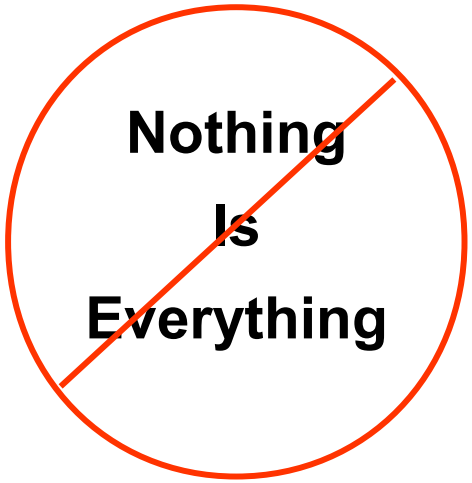
Contents of Presentation

- Overview
  - How Access is Determined
  - Profiles
  - Relationship with People and Labor
- Relevant Applications
  - Users
  - Security Groups
  - Conditional Expression Manager
- Integration
- Troubleshooting
- References

Overview

- Authentication
  - LDAP authentication via
    - WebSphere VMM
    - Microsoft Active Directory
    - Internal authentication disabled
  - Internal authentication
- Authorization
  - By Group
  - Authorizations to Maximo applications are managed in the Security Groups application
  - Architecture
    - Multi-site architecture
    - Site, Organization, Set and System levels
  - Independent and Combined Groups
  - Restrictions
- Other security Features

Access is Granted, not Assumed



How Access is Determined…

- When a User tries to access an application, the security objects will check to see what the maximum access is based on the combining of their group memberships
- Application access types
  - Read
  - Insert
  - Save
  - Delete
- In addition, their access to options (Actions) will be checked
- Access always has a site component
  - All sites
  - Specified Sites
  - No sites specified
- Database access, unless explicitly granted to a user, goes through the business objects and their rules

Example: Single organization with security groups that provide sufficient application, site and storeroom access and privileges for all users in XYZ company.

Worker and Management Groups for XYZ company

Worker Group

Sites	Inventory	Assets	Labor Reporting	Work Orders
✓ All sites	✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions
Storerooms ✓ All storerooms				

Management Group

Sites	Inventory	Work Orders	Labor Reporting
✓ All sites	✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions
Storerooms ✓ All storerooms			
Purchasing Limit ✓ $10,000	Assets ✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	Purchase Requisitions ✓ Read ✓ Insert ✓ Save ✓ All Actions	Financials ✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions

Security Profile for all Workers

All Workers →

Application Access

Inventory Assets	Work Orders Labor Reporting
✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions

Sites
✓ All sites

Storerooms
✓ All storerooms

Security Profile for all Management

All Management →

Application Access

Inventory Assets Financials	Work Orders Labor Reporting Purchase Requisitions
✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions

Sites
✓ All sites

Storerooms
✓ All storerooms

Purchasing Limit
✓ $10,000

Example: Single organization with a mix of non-independent security groups dedicated to individual group categories like application, site and storeroom access. Security profiles reflect functional areas within the company, like Maintenance and Purchasing, as you add users to groups that provide the required access and privileges needed to perform specific job responsibilities.

Mixed Non-Independent Security Groups for XYZ Company

Maintenance Application Group

Work Orders
Assets
Locations
✓ Read
✓ Insert
✓ Save
✓ Delete
✓ All Actions

Purchase Orders
✓ Read
✓ Insert
✓ Save
✓ All Actions

Inventory
✓ Read

Purchasing Application Group

Purchase Orders
✓ Read
✓ Insert
✓ Save
✓ All Actions

Work Orders
Inventory
✓ Read

Sites Group
✓ Bedford
✓ Nashua
✓ Needham

Storeooms Group
✓ Bedford
✓ Nashua
✓ Needham

Purchasing Approval Limits Group
PR $10,000
PO $10,000
Invoices $10,000

Security Profile for Mainenance Users

Maintenance users

Maintenance Application Access

Work Orders
Assets
Locations
✓ Read
✓ Insert
✓ Save
✓ Delete
✓ All Actions

Purchase Orders
✓ Read
✓ Insert
✓ Save
✓ All Actions

Inventory
✓ Read

Storerooms
✓ Bedford
✓ Nashua
✓ Needham

Sites
✓ Bedford
✓ Nashua
✓ Needham

Security Profile for Purchasing Users

Purchasing users

Purchasing Application Access

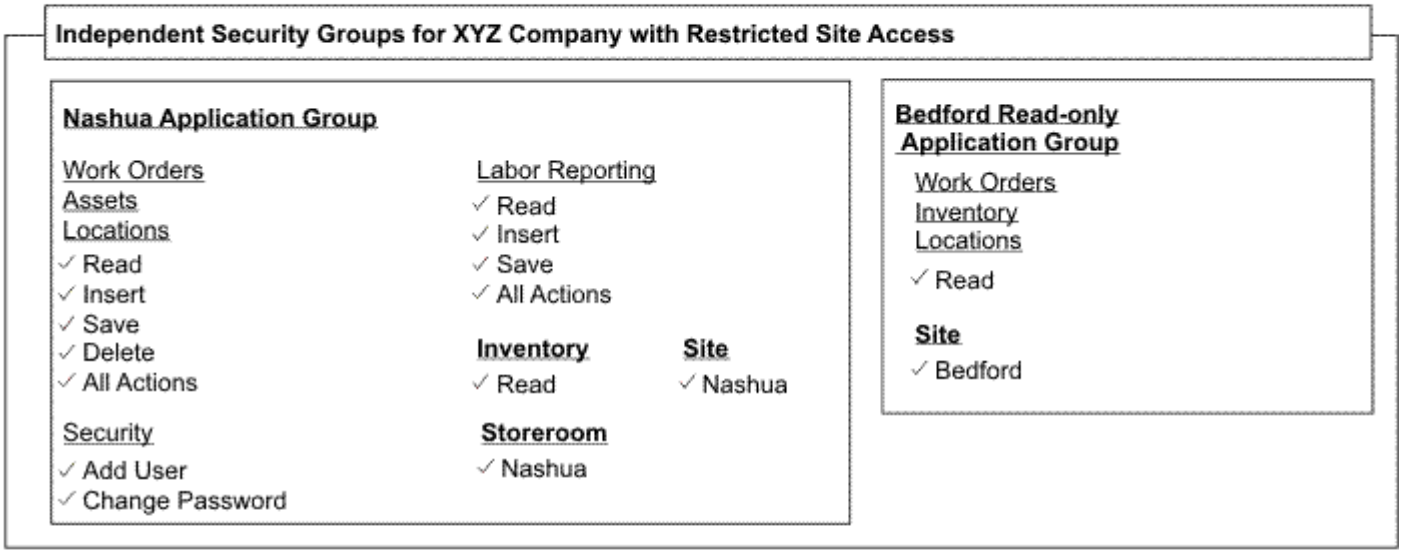
Purchase Orders
✓ Read
✓ Insert
✓ Save
✓ All Actions

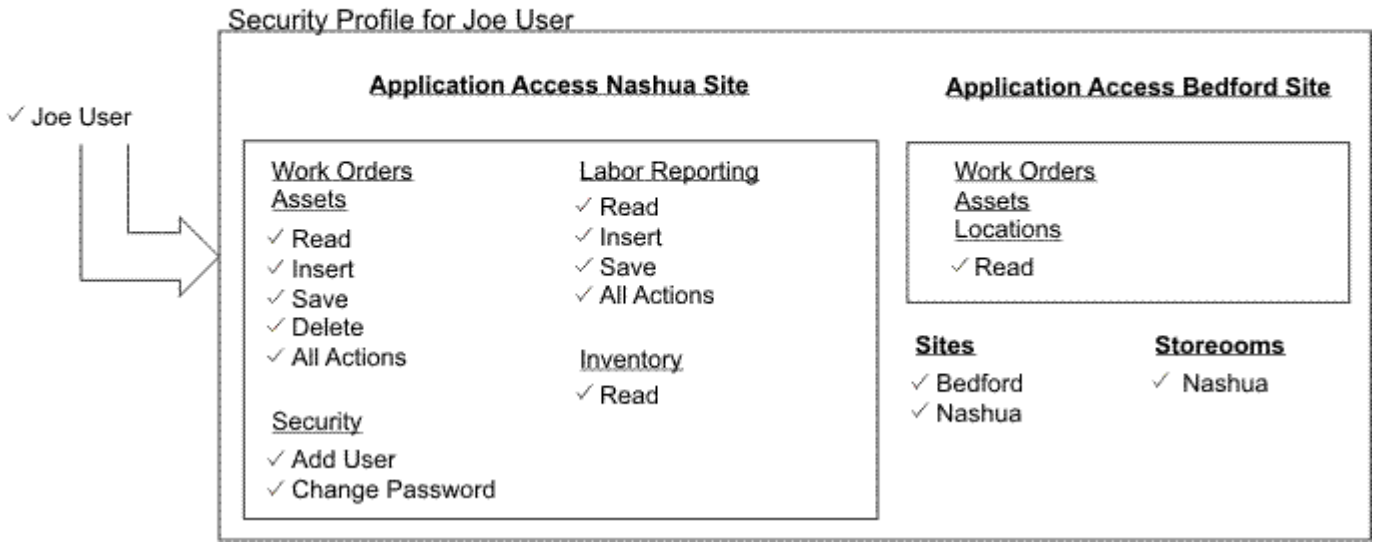
Work Orders
Inventory
✓ Read

Purchasing Approval Limits
PR $10,000
PO $10,000
Invoices $10,000

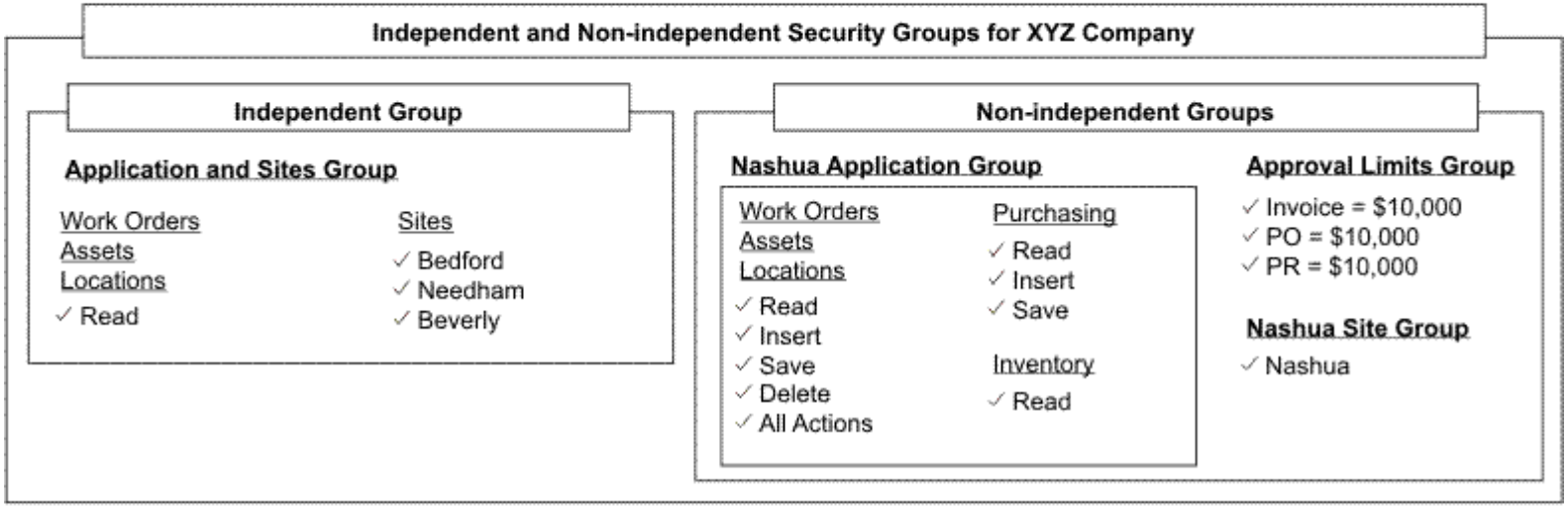
Sites
✓ Bedford
✓ Nashua
✓ Needham

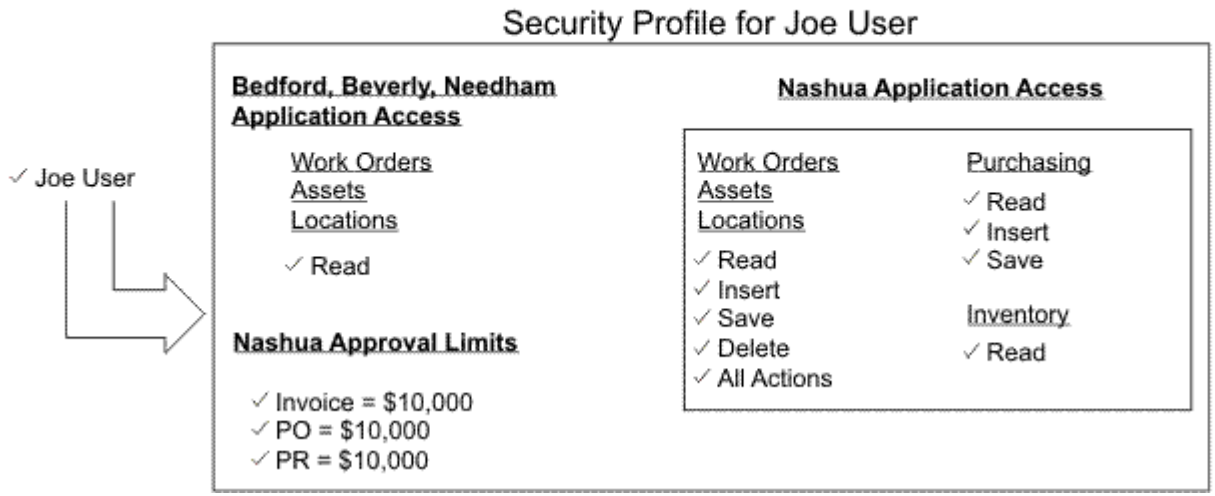
Example: Single organization that practices site administration with independent security groups. The application access groups are restricted to the Nashua and Bedford sites within the organization. The Nashua group provides the user with most of the application and storeroom access needed to perform his or her job. However, this user also requires Read-only access to several applications at the Bedford site. This example shows how to combine independent security groups so that a user has sufficient application access to perform his or her job responsibilities across sites.





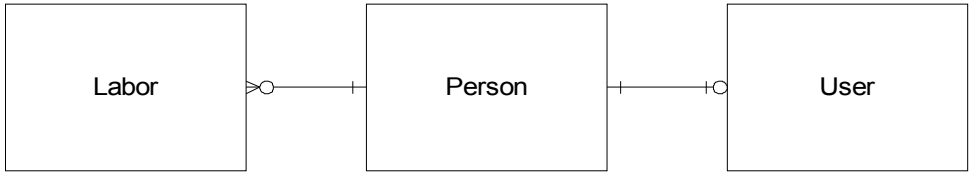
Example: Single organization that practices site administration with independent and non-independent security groups. The independent group provides the user with read-only application access at several remote sites. The non-independent groups provide the user with all the application access and approval limits he needs to perform his job responsibilities at his primary site.





People

- **Need to capture common personal information**
  - Labor
  - Users
  - Asset Custodians
  - Asset Owners
  - Help Desk Callers

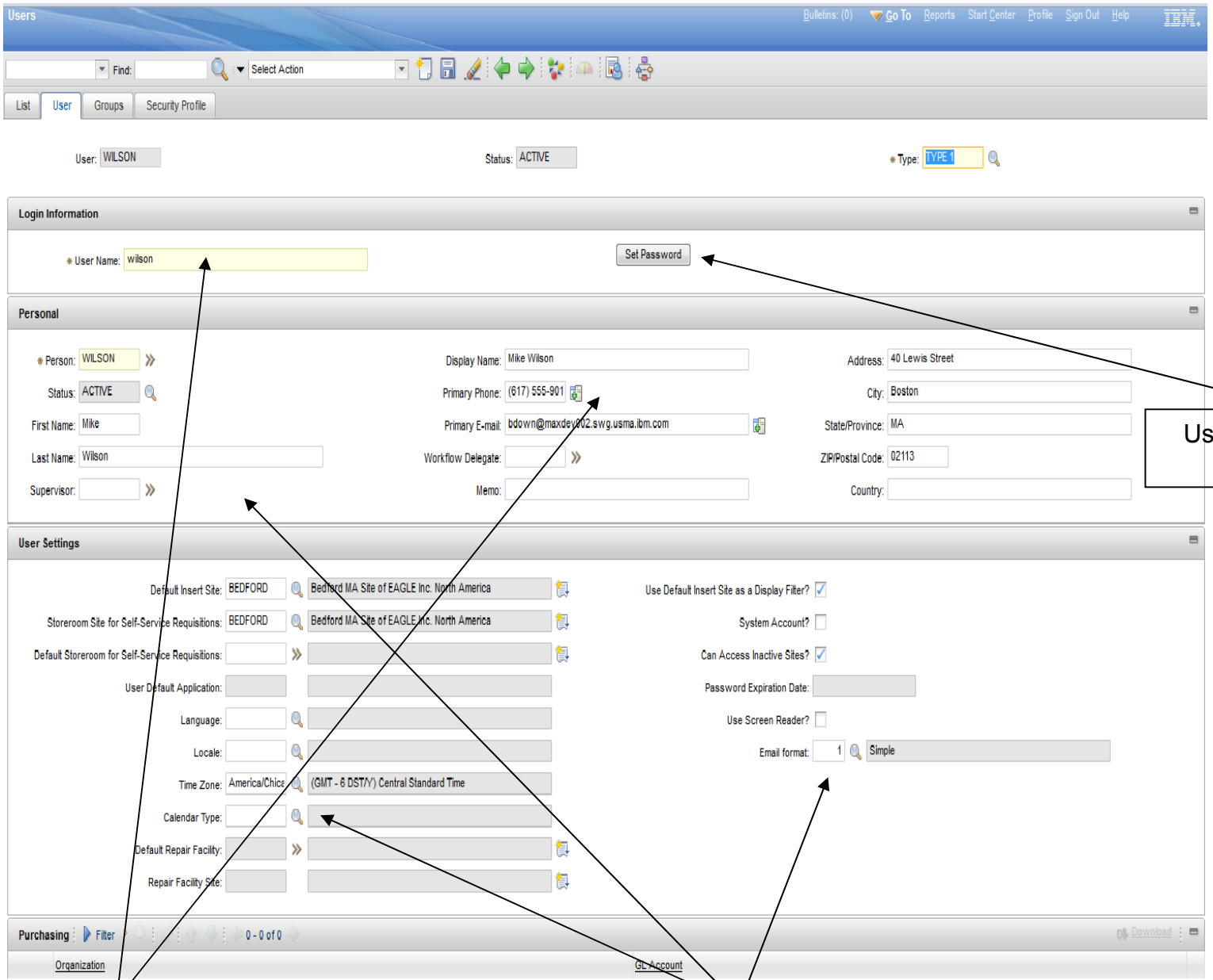


Users

- The Users application is located in the Security module
- Each user has a corresponding Person record that can be linked from the Users application
- The Groups tab allows a view of group memberships
- The Profile tab provides a view of a users access when all of their group access is combined
- Password management for internal authentication

Use

- Launch the Users application
- Locate a user record
- Specify a default insert site
- View their group membership and the resulting security profile
- Review the Actions menu items – most are not applicable to CCMDB

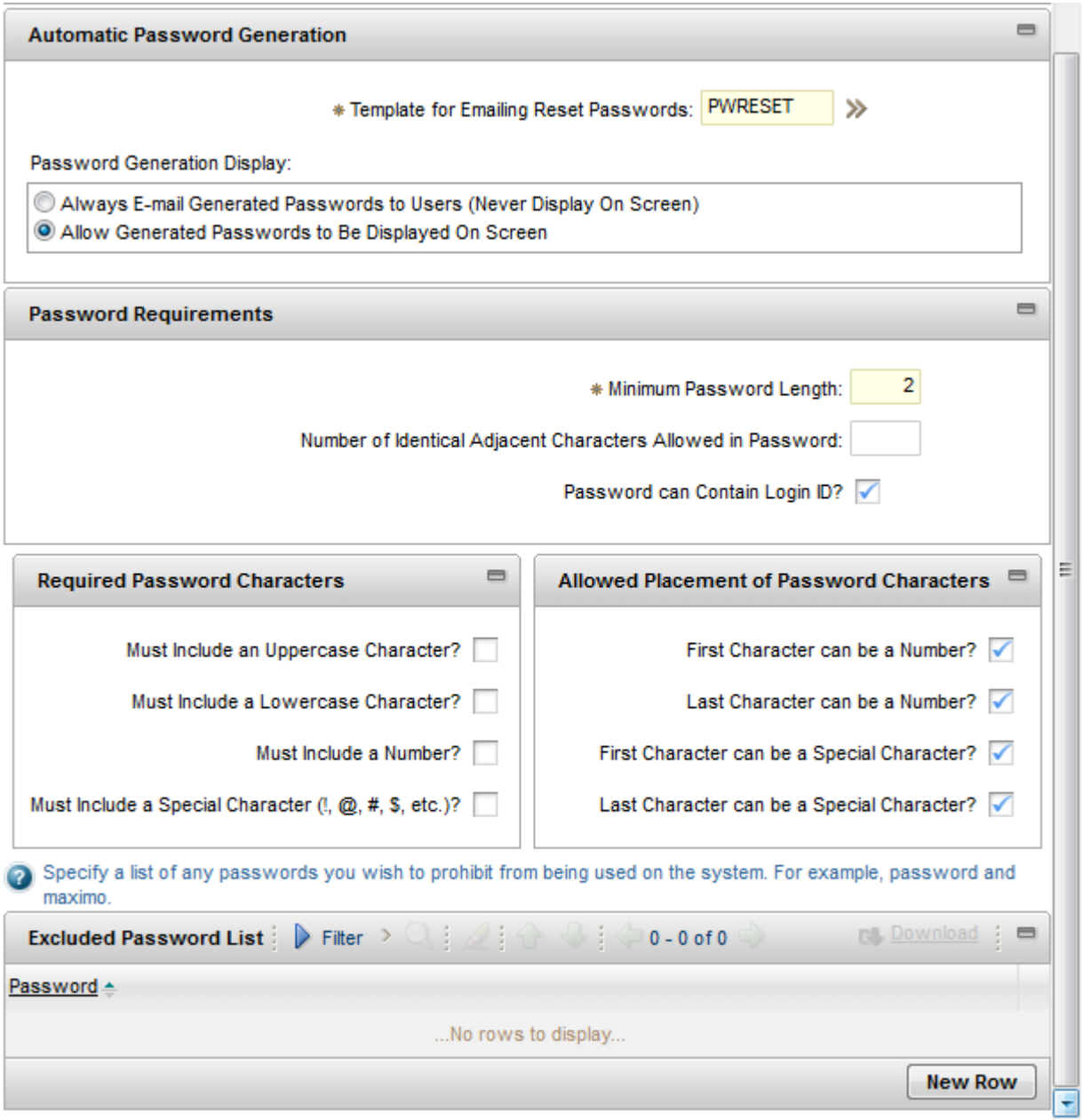


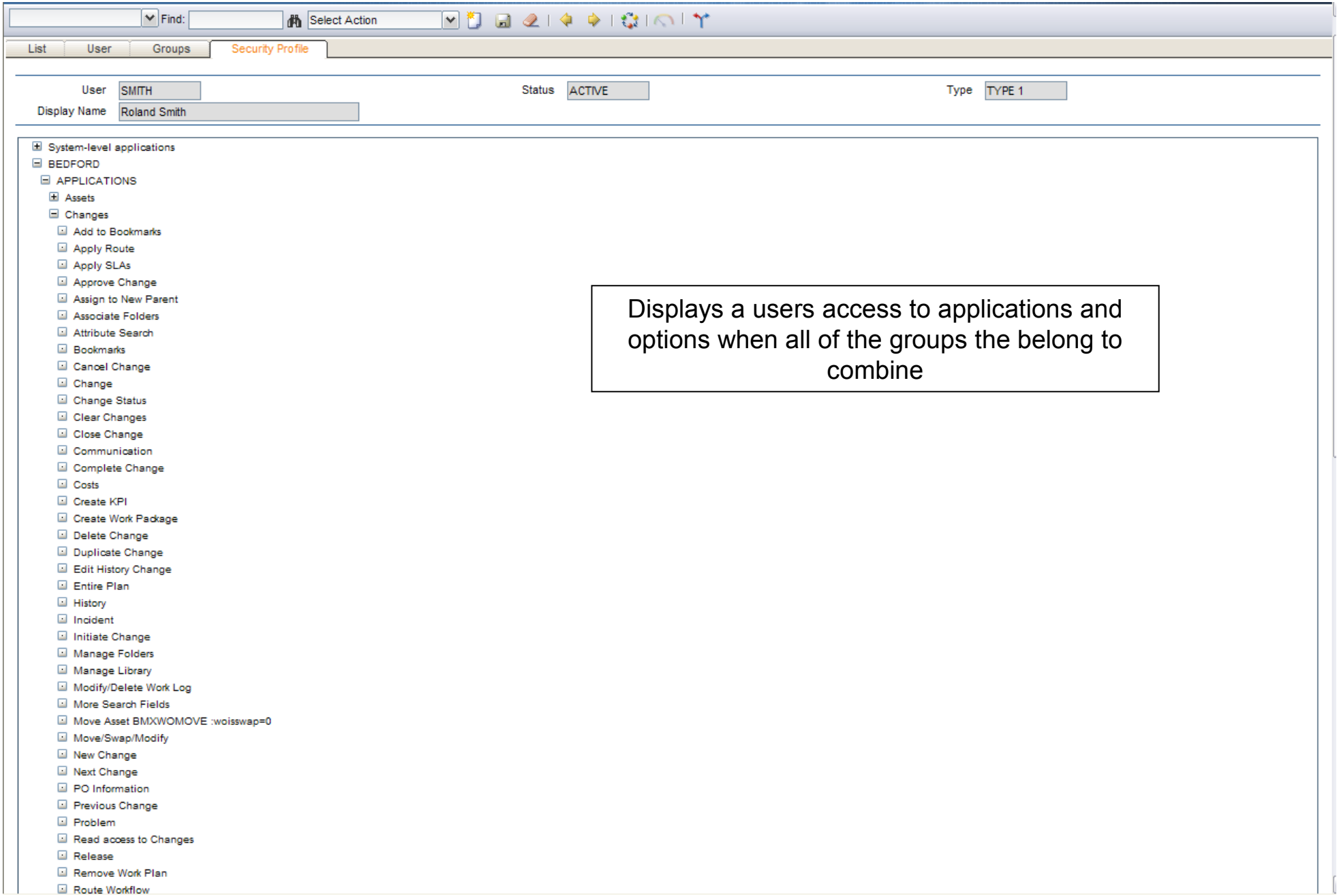
Used to manage password with internal authentication

Can be synchronized from the directory.

Entered in this system

Tivoli software Password Rules





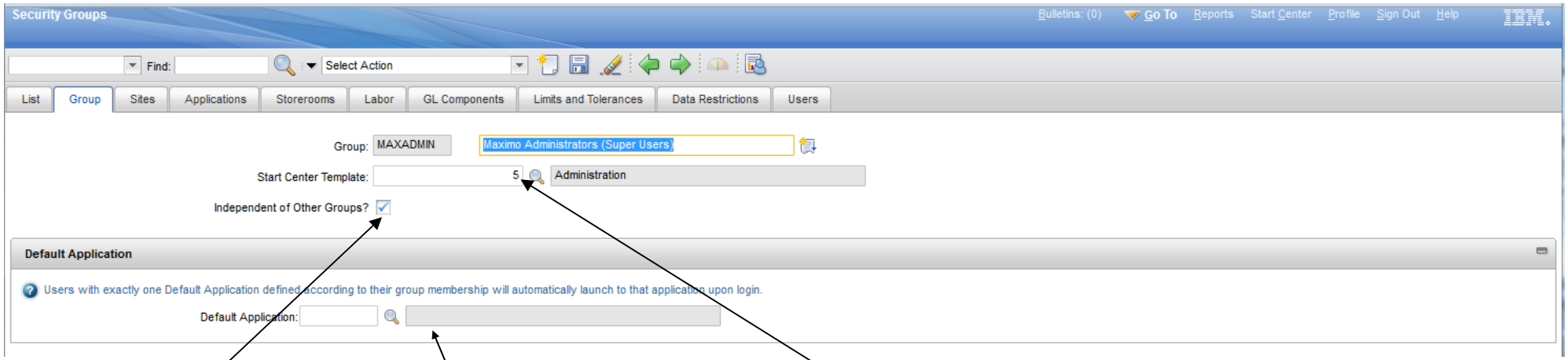
Displays a users access to applications and options when all of the groups the belong to combine

Security Groups

- Elements are secured by group, not user
  - Sites
  - Application Authorizations
  - Purchasing Limits
  - Invoice Tolerances
  - Start Centers
  - GL Component Authorizations
  - Labor Authorizations
  - Storeroom Authorizations
  - Data Restrictions
- A User can be a member of multiple Groups
  - If there is a conflict the ‘highest’ access ‘wins’
- Groups setting can be independent of other groups
  - Elements in a group stand alone
  - Need to have a site

Use

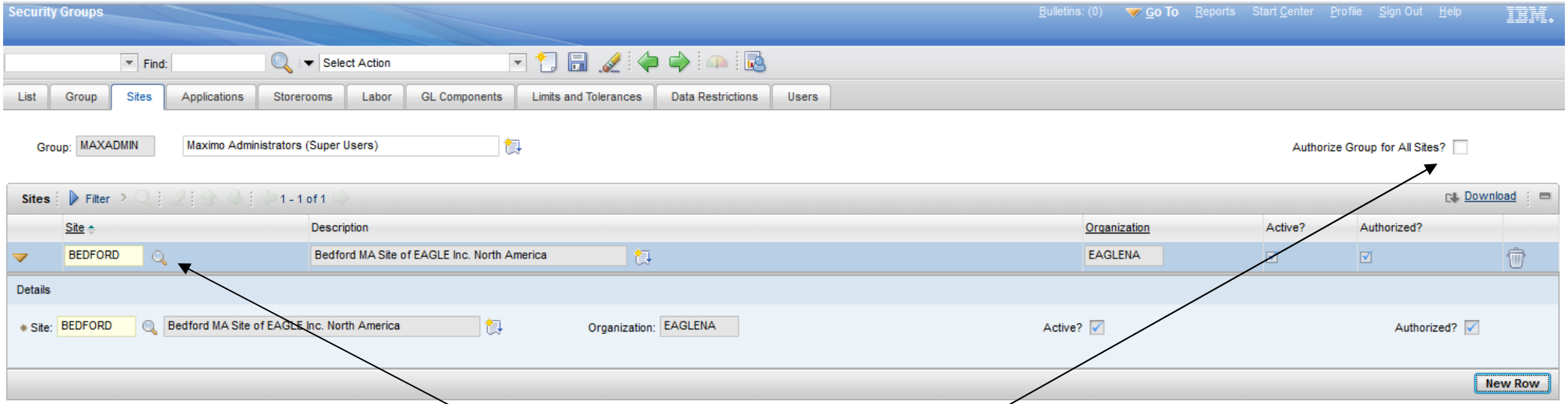
- Launch Security Groups application and navigate to a record that has been synchronized from the directory
- Specify Group Settings and Authorizations
  - Independent?
  - Start Center Template
  - Sites
  - Applications
  - Storerooms
  - Labor
  - GL Components
  - Limits & Tolerances
  - Data Restrictions
  - Users



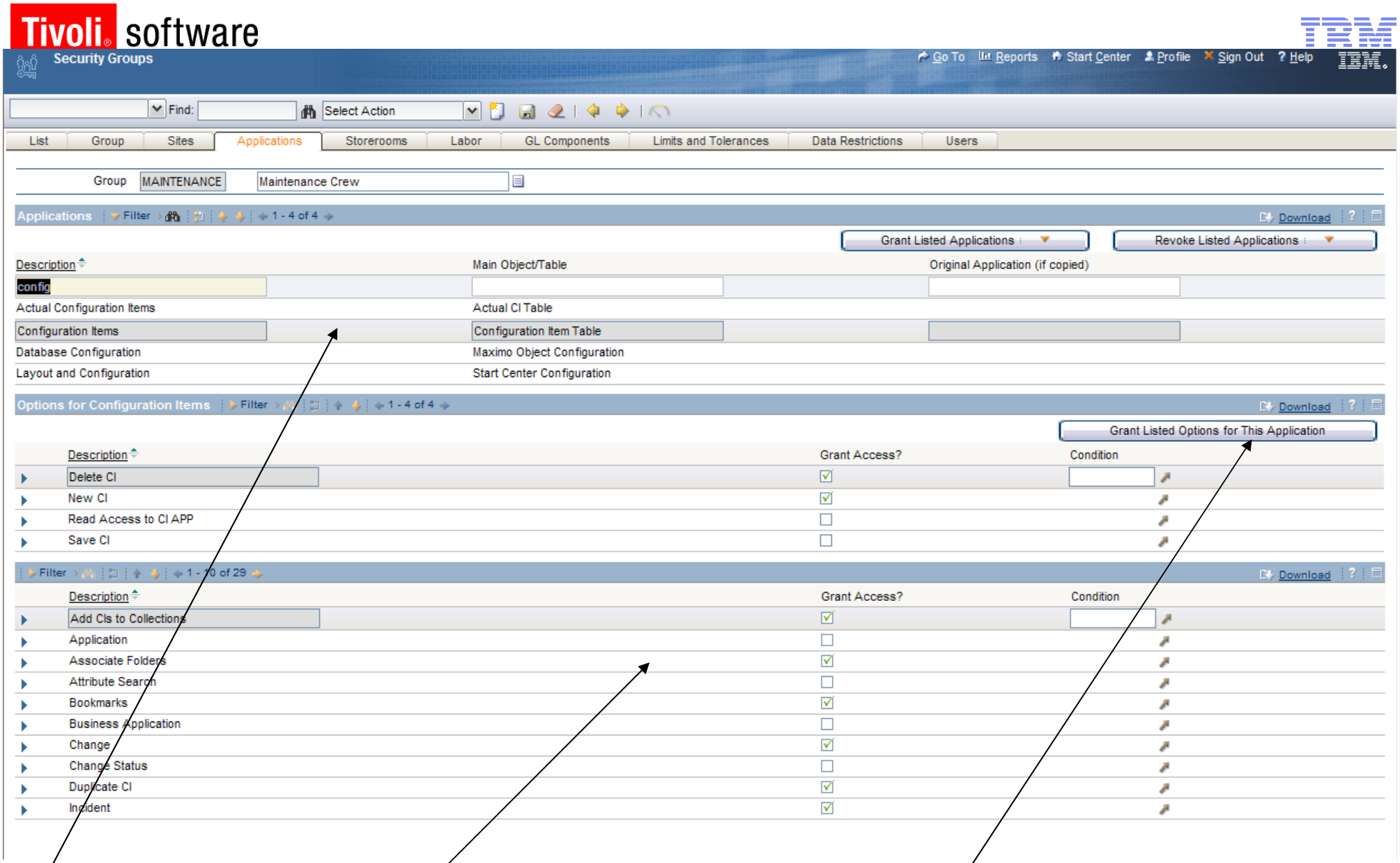
Indicates whether the authorizations in this group should combine with authorizations in other groups or be independent

Indicates the Start Center or 'dashboard' that will be presented for users in this group. A user in multiple groups can have multiple Start Centers and decide which one will be their default. Start Center templates are defined on the Start Center itself.

New in 7.5.0.2 groups can have a different start application.



A group can either have all sites or specific sites. Or no sites at all, unless it is an Independent group – then at least one site is required.



List of available Applications from MAXAPPS table

List of Options for application selected above from SIGOPTION table

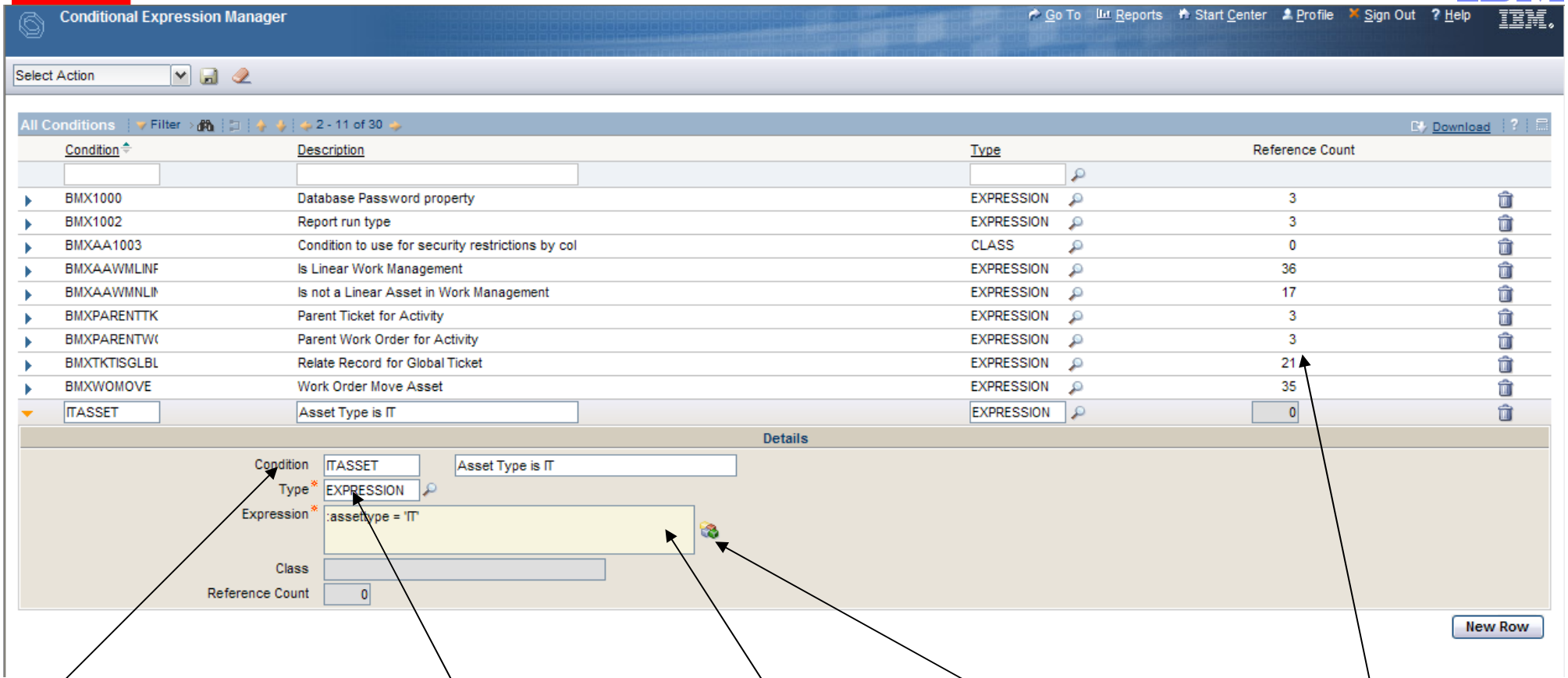
This button grants all of the options in the result set, even those on the next page. Use 'Filter' to reduce the list before granting, if desired. Granted options for the groups are stored in APPLICATIONAUTH table.

Conditional Expressions

- Library
  - Maximo expressions
  - Custom classes
- Reusable
  - Data Restrictions
  - Conditional option access
  - Conditional UI (control security/dynamic UI – Application Designer)
- Conditional Expression Manager application
  - Located in the Administration Module
  - Simple application for defining and managing conditions and seeing how many times they are used.

Use

- Open Conditional Expression Manager
- Click New Row to add a condition to the library
- Select a type
  - For Expressions, specify the syntax
    - Use the Expression Builder, if desired
    - See the System Administrator Guide for syntax tips
  - For Classes, specify the file name
- Save the record
- Each time the condition is used in the system the reference count will increment by one



The Condition ID will be auto-generated but you can change it to something more meaningful

The two types of conditions are EXPRESSION and CLASS

The same expression or class cannot be used more than once in the system.

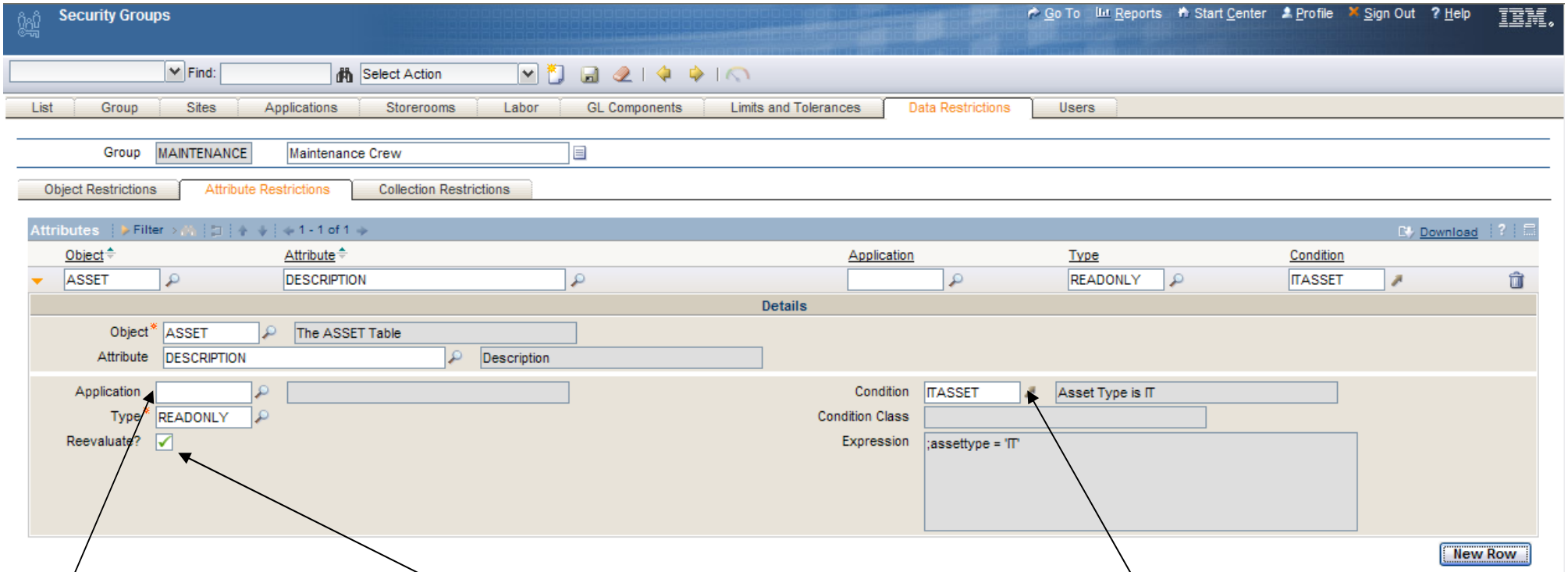
The Expression Builder can help you build your expression

The reference count will be increments by 1 each time the condition is used in the system

Data Restrictions (Row and Attribute Security)

- Configured in Security Groups application
- Globally (via an Action) or per security group (on the tab)
- Set conditions for access everywhere an object or attribute is used
- Objects can be
  - Hidden – when the condition is true, data will be masked
  - Read Only – when the condition is true no modifications will be allowed
  - Qualified – only records that meet the condition will be fetched from the database.
    - New in version 7.5 an 'Allow Qualified' property can be specified to allow the UI to use a Qualified data restriction for objects that are not 'main records'
- Attributes can be
  - Hidden – when the condition is true, the field will not be displayed
  - Read Only – when the condition is true no modifications will be allowed
  - Required – when the condition is true, the attribute is required
- Collection Restrictions
  - If there are no collection restrictions all CIs, Assets and Locations are allowed
  - If there are collection restrictions, only CIs, Assets and Locations in the collections are allowed
- Highest access 'wins'

- Launch Security Groups application and navigate to a record that has been synchronized from the directory
- Select the Data Restrictions tab
- Three tabs will appear for the different types of restrictions – Object, Attribute and Collection
  - On the Object or Attribute tab, select the entity you want to restrict, specify a condition and other applicable attributes
  - For Collection Restrictions, specify the collection the group is restricted to and a number of Object Data Restrictions will be created behind the scenes
    - You can view them on the Object Restriction tab but you cannot edit them.



You can create a Data Restriction that applies to only one application

Checking this box will set the system to re-evaluate the condition when a user tabs out of a field. If it is unchecked, the condition will be re-evaluated on save.

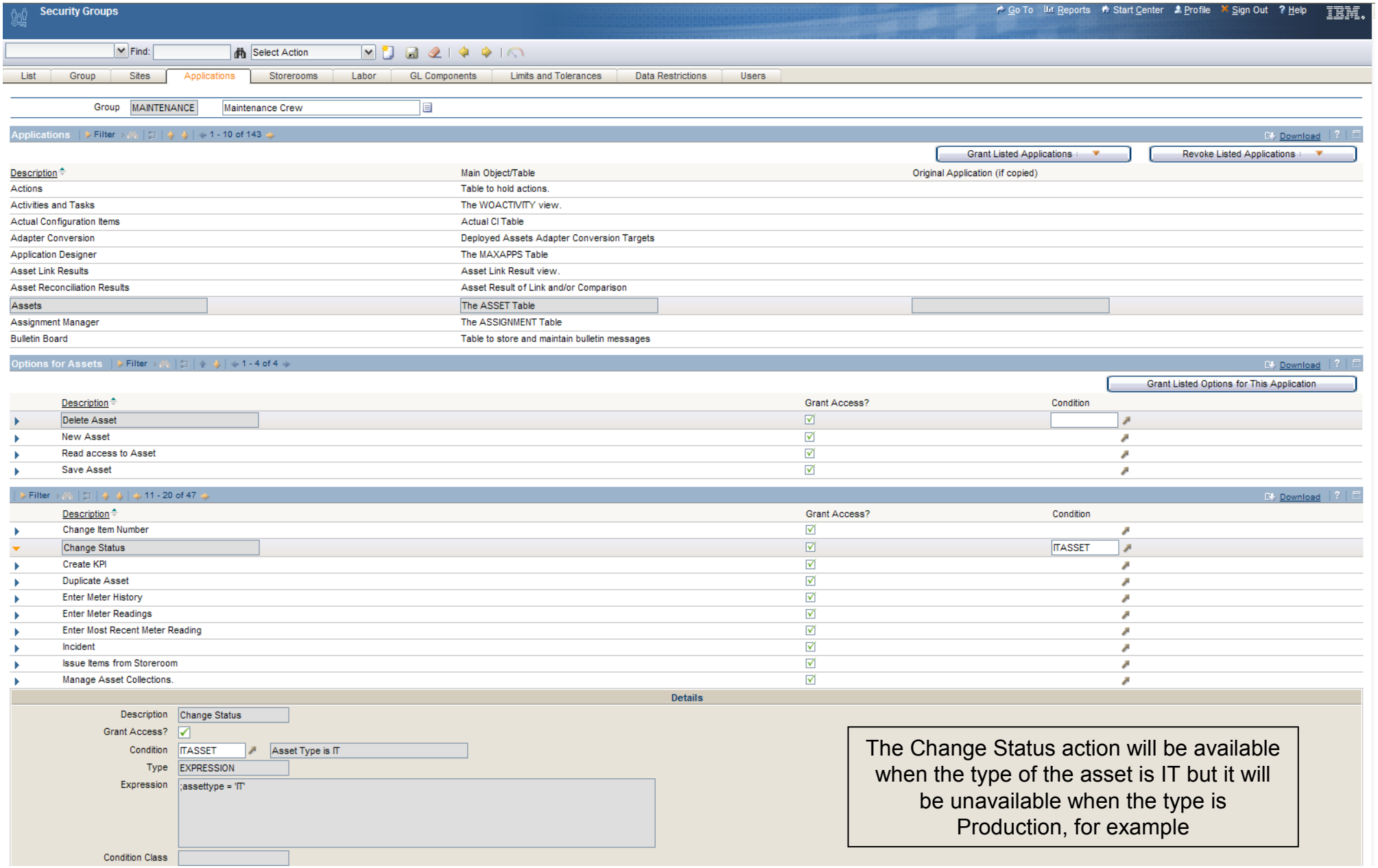
Select a existing condition or use the 'GOTO' to create on in Conditional Expression Manager

Conditional Option Access

- Determines when an application option (action) is available
- Set per security group
- Highest access ‘wins’

Use

- Launch Security Groups application and navigate to a record that has been synchronized from the directory
- Select the Applications tab
  - Select the application and option that you want to grant
  - Grant the option and specify an existing condition



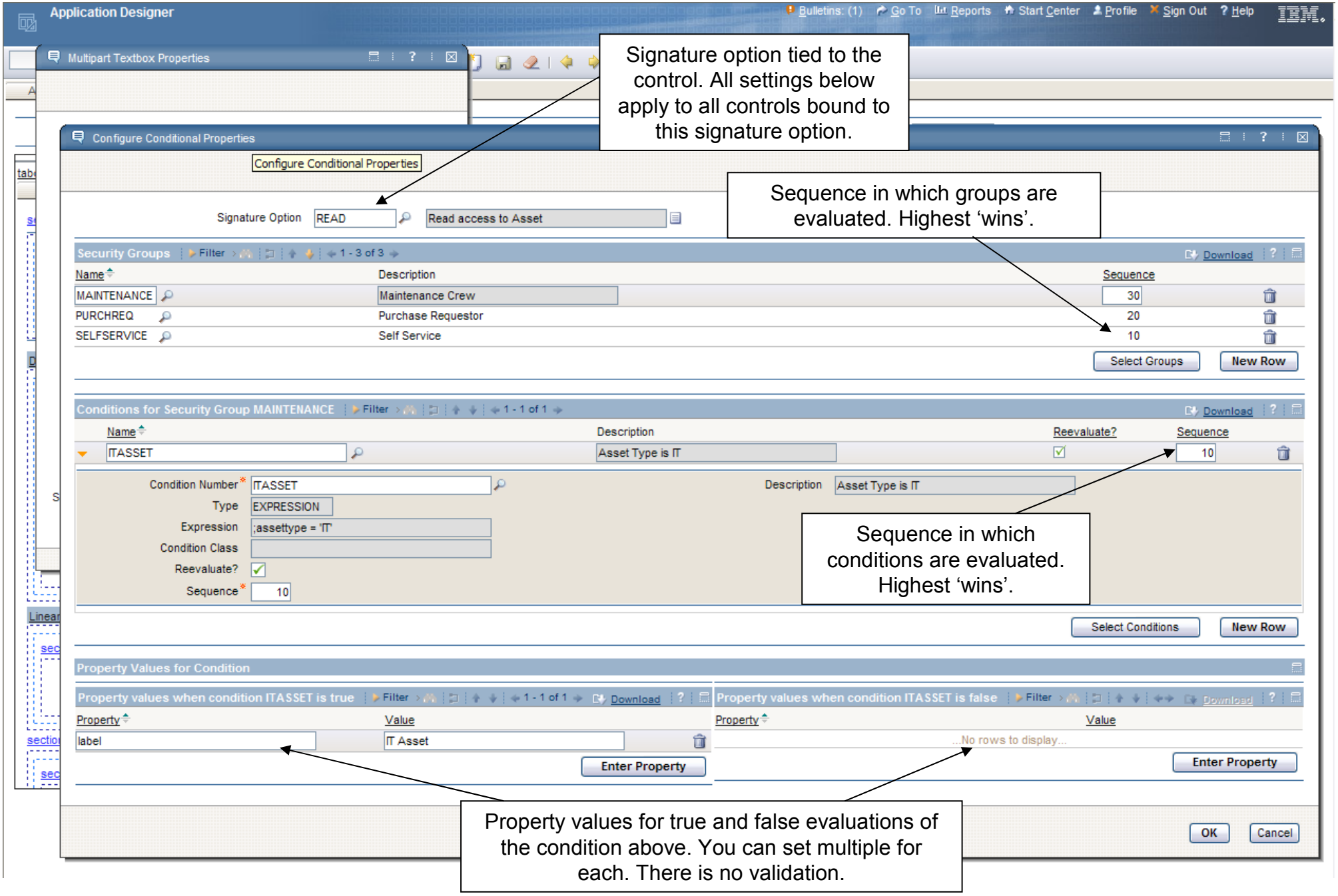
The Change Status action will be available when the type of the asset is IT but it will be unavailable when the type is Production, for example

Control Security & Conditional Properties

- In Application Designer Create a new Signature Option to grant a control or group of controls
- In Application Designer, choose your application and control(s)
  - Open the Control Properties Dialog for the control
  - Specify the Sig Option in the field in the bottom of the dialog
  - Save your changes
  - More than one Control can use the same Signature Option

Control Security & Conditional Properties

- Securing a Control
  - Open Application Designer and navigate to the application you want to configure
  - Add a signature option
  - Specify the data source of 'MAINRECORD' for most use cases
- Conditionally Controlling Properties
  - Open the Control Properties dialog for the control you want to configure
  - Specify the signature option (if not already specified)
  - Open the Configure Conditional Properties dialog
  - Specify the security groups, conditions, properties and values you want to configure
    - You must select existing security groups and conditions – you cannot create them in this application
    - Groups and Conditions are sequenced to resolve conflicts
      - Highest number is evaluated last and 'wins' in the case of a conflict
    - Settings apply to all controls that are tied to the signature option

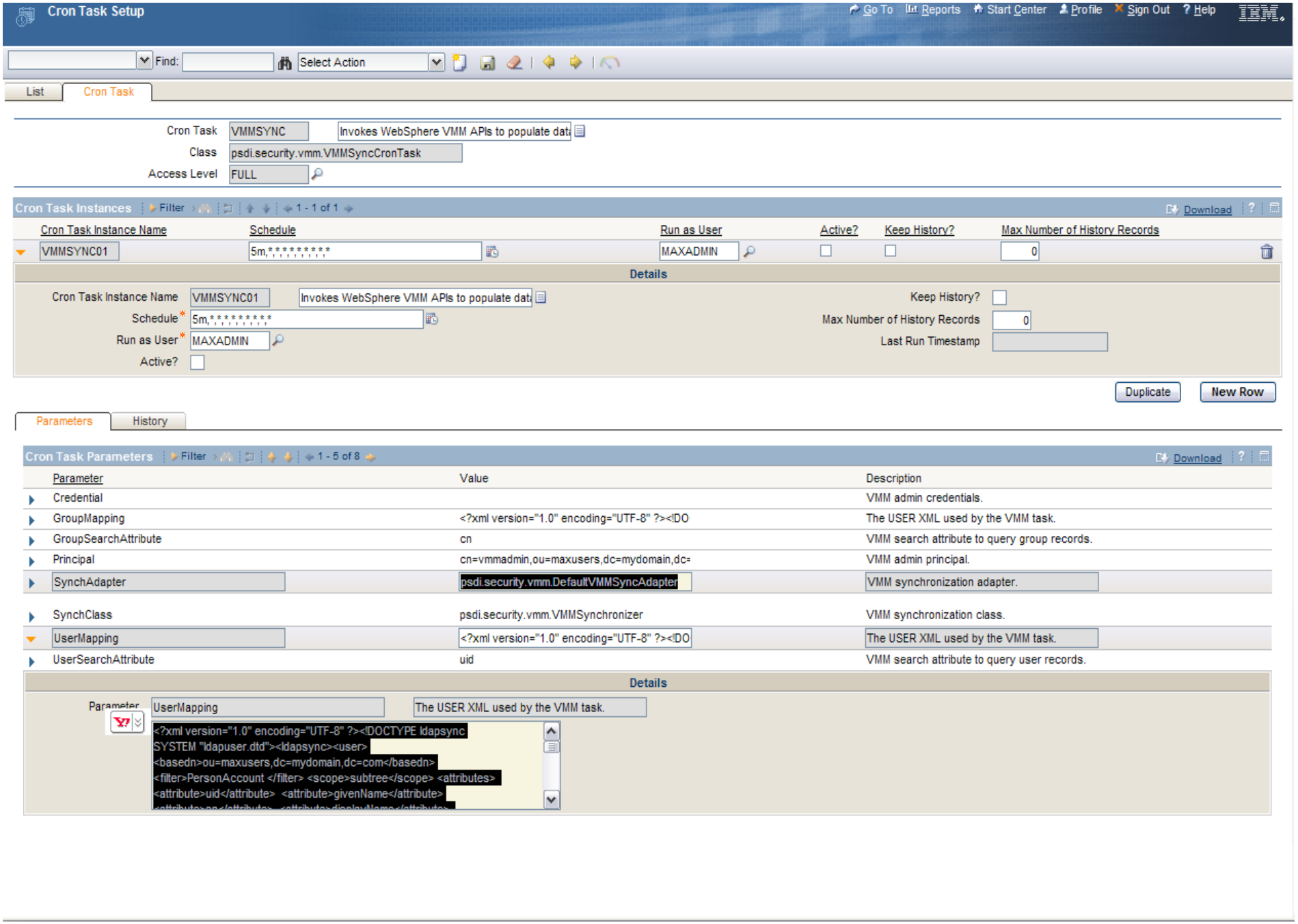


Known Issues

- Not all properties are supported for conditional properties
- No validation on properties or property values
- Property list in Control Properties dialog includes obsolete properties and is missing other new properties

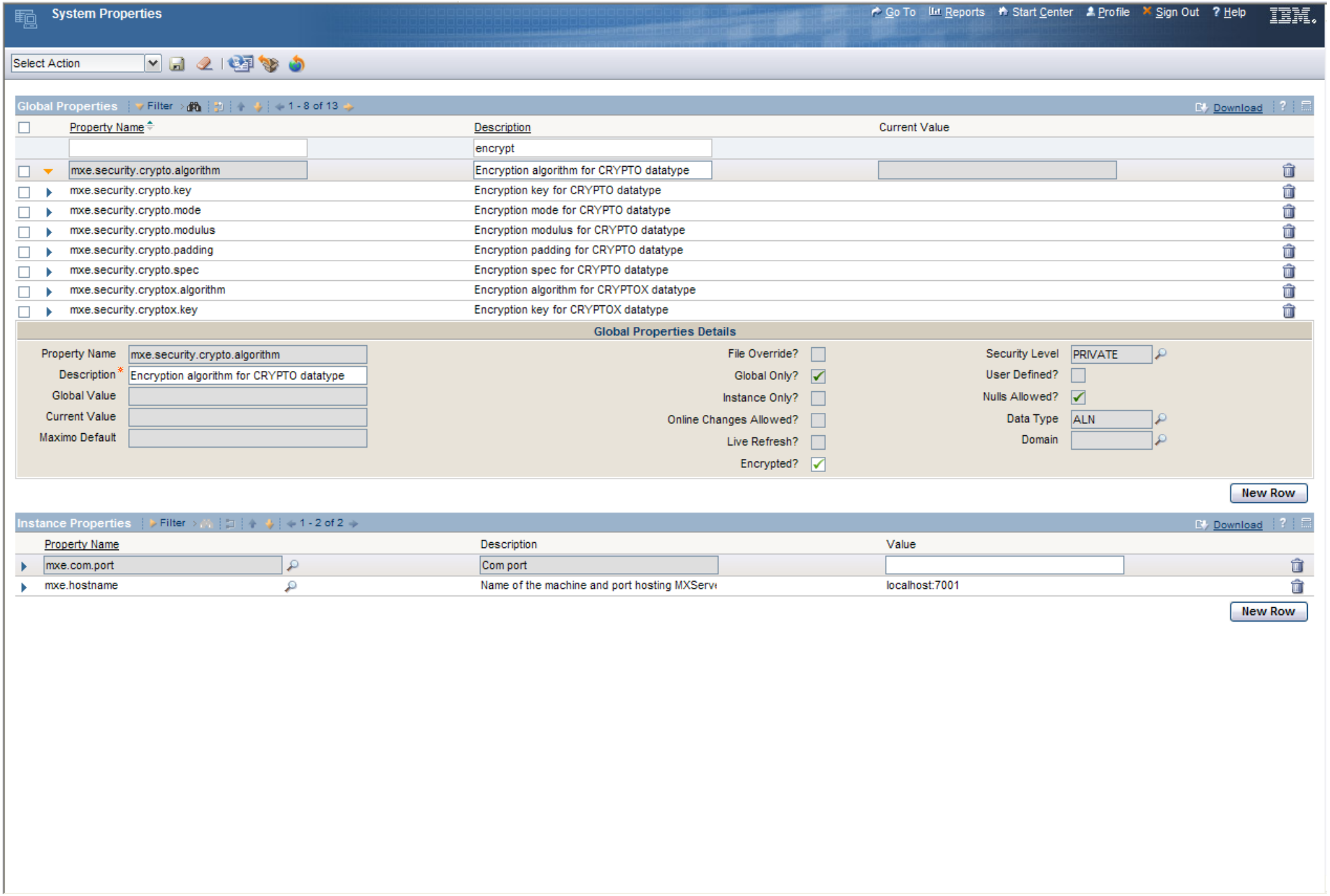
LDAP Integration

- Synchronization of data with Tivoli Directory Server (ITDS) and Microsoft Active Directory supported
  - Other directories can be supported through customizing a class file and creating an attribute mapping
- Parameters of the directory synchronization are configured in the Cron Task Setup application in the Platform Configuration module within the System Configuration module.
  - The cron task that handles the synchronization with is ITDS and Active Directory on WebSphere is‘VMMSYNC’
  - New in 7.5 – incremental sync supported with VMM
  - The cron task that handles the synchronization with Active Directory on WebSphere or WebLogic is‘LDAPSYNC’



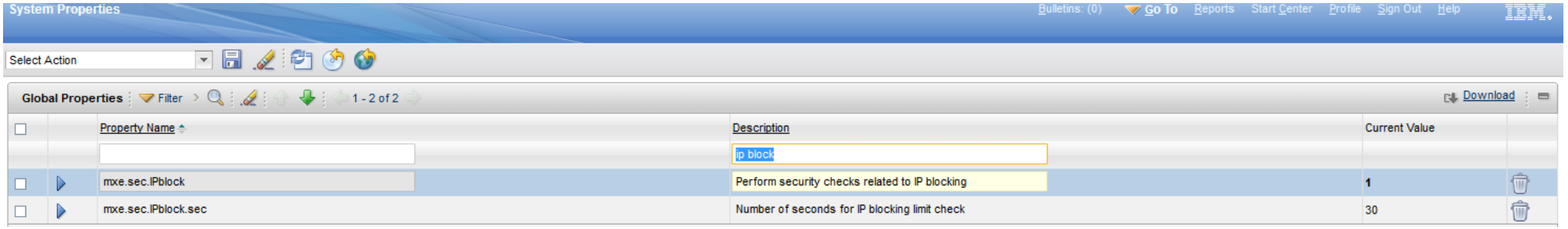
Encryption

- Any attribute can be encrypted using database configuration
  - CRYPTO – encrypted and decrypted for display
  - CRYPTOX – encrypted and used in the database in its encrypted format
- Decrypted data is ALN
- Properties can also be encrypted
  - File
  - Application
- Default encryption algorithm is DESEDE
  - Alternate can be specified
  - Additional Parameter can be specified



Misc Security Enhancements

- Password recovery function
  - 'Forgot Password'
  - Hint question and answer
  - Limit the number of 'Forgot Password' allowed
- Prevention of flooding a server with requests from unauthenticated users
  - Limit use of functions from the same IP address
    - Self-Registration
    - Forgot Password
  - Properties



  - Cross Site Scripting and SQL Injection protection
  - Filter
  - Property

License Compliance Tools

- Application Functionality
  - Persisting login information in the LOGINTRACKING table
  - Capturing IP addresses in the MAXSESSION and LOGINTRACKING tables
  - Addition of the Manage Session dialog to the Users application
- KPIs
  - Registered Users – By Type
  - Current User Sessions
  - Current Number of Logged In Users
- Start Centers
  - Addition of the KPIs above to the Administration start center in MAXDEMO
- Reports
  - User Session
  - Login History
  - User Type
- Configuration Required
  - Create the appropriate user types
  - Assign users to appropriate types

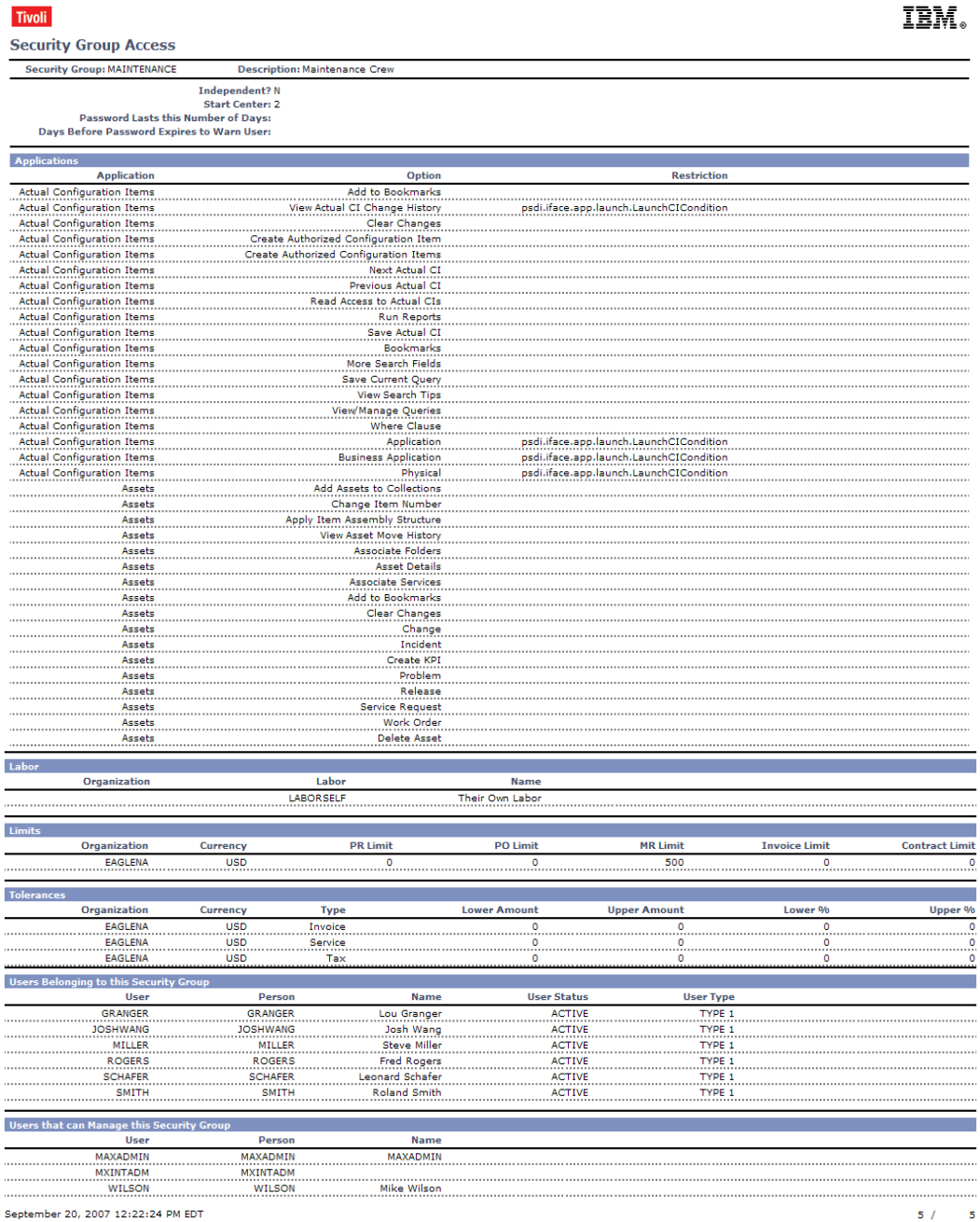
- New screens
- app scan enhancements

Troubleshooting

- **Don't 'x' out of a browser – always sign out**
  - 'X'ing out of a browser can leave hanging sessions and impact the implementation of security changes that take effect on the next login
  - To view and manage these sessions, use the 'Manage Sessions' action in the Users application
  - There is an action to end sessions
- **Check the 'Profile' tab in the Users application to see what access a user has**
  - This will show you all of the applications and options that a user has per site, including very basic information on restrictions
  - Useful for troubleshooting when you are getting unexpected results
- **When you are testing a configuration and experiencing unexpected results, try it with one group and one user**
  - Create a user that is in just one group
  - Put all of the configurations that you are trying to test in that one group
- **When configuring conditional behavior, create an 'alwaystrue' condition**

More Troubleshooting

- **A report is available in the Security Groups application that will show you all of the options configured for a specific group or all of the groups a user belongs to. This can help troubleshoot unexpected behavior as well.**



Tivoli IBM

Security Group Access

Security Group: MAINTENANCE **Description:** Maintenance Crew

Independent? N
Start Center: 2
Password Lasts this Number of Days:
Days Before Password Expires to Warn User:

Applications

Application	Option	Restriction
Actual Configuration Items	Add to Bookmarks	
Actual Configuration Items	View Actual CI Change History	psdi.iface.app.launch.LaunchCICondition
Actual Configuration Items	Clear Changes	
Actual Configuration Items	Create Authorized Configuration Item	
Actual Configuration Items	Create Authorized Configuration Items	
Actual Configuration Items	Next Actual CI	
Actual Configuration Items	Previous Actual CI	
Actual Configuration Items	Read Access to Actual CIs	
Actual Configuration Items	Run Reports	
Actual Configuration Items	Save Actual CI	
Actual Configuration Items	Bookmarks	
Actual Configuration Items	More Search Fields	
Actual Configuration Items	Save Current Query	
Actual Configuration Items	View Search Tips	
Actual Configuration Items	View/Manage Queries	
Actual Configuration Items	Where Clause	
Actual Configuration Items	Application	psdi.iface.app.launch.LaunchCICondition
Actual Configuration Items	Business Application	psdi.iface.app.launch.LaunchCICondition
Actual Configuration Items	Physical	psdi.iface.app.launch.LaunchCICondition
Assets	Add Assets to Collections	
Assets	Change Item Number	
Assets	Apply Item Assembly Structure	
Assets	View Asset Move History	
Assets	Associate Folders	
Assets	Asset Details	
Assets	Associate Services	
Assets	Add to Bookmarks	
Assets	Clear Changes	
Assets	Change	
Assets	Incident	
Assets	Create KPI	
Assets	Problem	
Assets	Release	
Assets	Service Request	
Assets	Work Order	
Assets	Delete Asset	

Labor

Organization	Labor	Name
	LABORSELF	Their Own Labor

Limits

Organization	Currency	PR Limit	PO Limit	MR Limit	Invoice Limit	Contract Limit
EAGLENA	USD	0	0	500	0	0

Tolerances

Organization	Currency	Type	Lower Amount	Upper Amount	Lower %	Upper %
EAGLENA	USD	Invoice	0	0	0	0
EAGLENA	USD	Service	0	0	0	0
EAGLENA	USD	Tax	0	0	0	0

Users Belonging to this Security Group

User	Person	Name	User Status	User Type
GRANGER	GRANGER	Lou Granger	ACTIVE	TYPE 1
JOSHWANG	JOSHWANG	Josh Wang	ACTIVE	TYPE 1
MILLER	MILLER	Steve Miller	ACTIVE	TYPE 1
ROGERS	ROGERS	Fred Rogers	ACTIVE	TYPE 1
SCHAFER	SCHAFER	Leonard Schafer	ACTIVE	TYPE 1
SMITH	SMITH	Roland Smith	ACTIVE	TYPE 1

Users that can Manage this Security Group

User	Person	Name
MAXADMIN	MAXADMIN	MAXADMIN
MXINTADM	MXINTADM	
WILSON	WILSON	Mike Wilson

September 20, 2007 12:22:24 PM EDT 5 / 5

Even More Troubleshooting

- **Do not change the encryption algorithm or properties after you have created data**
  - Encrypted data will no longer be usable
- **Re-sync of users and groups from external directory.**
  - Delete records from the LDAPSYNCPARAMS table. This will result in the application behaving as if it is synchronizing the records for the first time.
  - Note: Depending on the data within the tables, it may be desirable to remove records from the MAXUSER, PERSON, EMAIL, PHONE, MAXGROUP and GROUPUSER tables as well to avoid duplication of data.

QUESTIONS??