

What's New in Maximo Security – Version 7.5

Colleen McCretton

Date of presentation: 8/2/2012



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

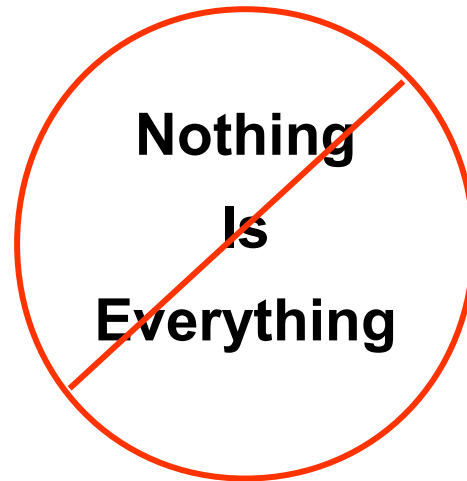
Overview

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

All Workers →

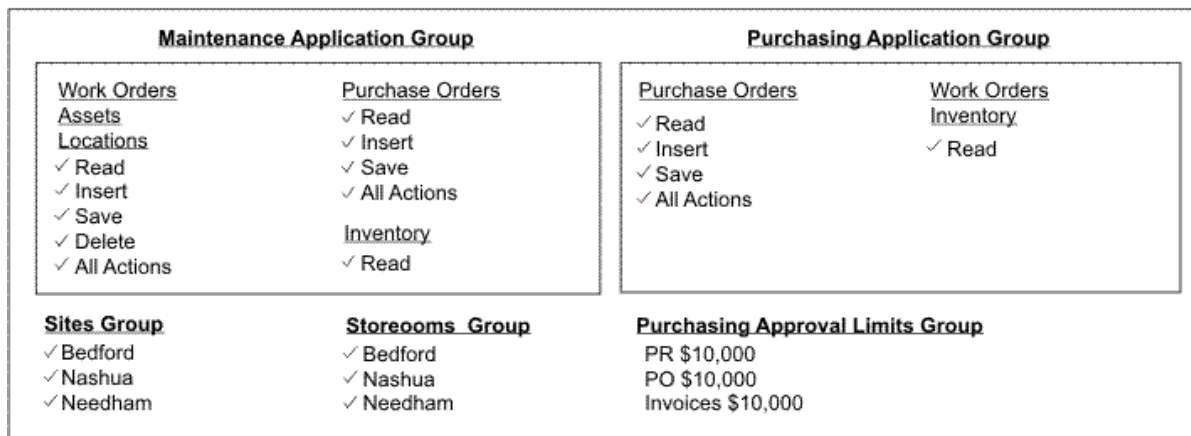
Security Profile for all Workers		
Application Access		Sites
Inventory Assets	Work Orders Labor Reporting	✓ All sites
✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions	Storerooms ✓ All storerooms

All Management →

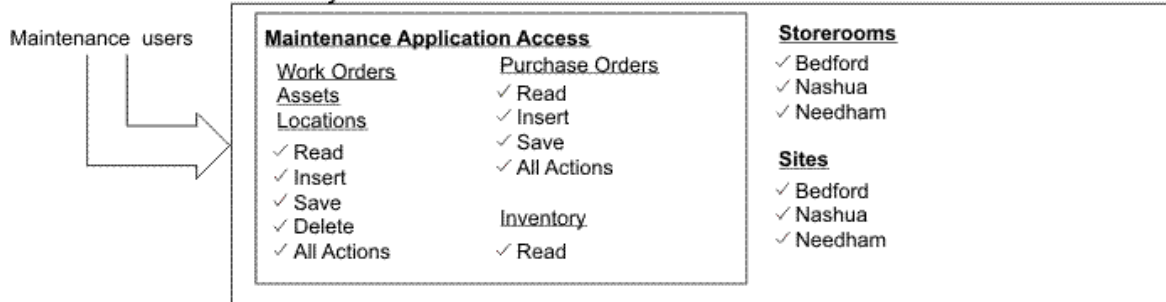
Security Profile for all Management		
Application Access		Sites
Inventory Assets Financials	Work Orders Labor Reporting Purchase Requisitions	✓ All sites
✓ Read ✓ Insert ✓ Save ✓ Delete ✓ All Actions	✓ Read ✓ Insert ✓ Save ✓ All Actions	Storerooms ✓ All storerooms
		Purchasing Limit ✓ \$10,000

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.

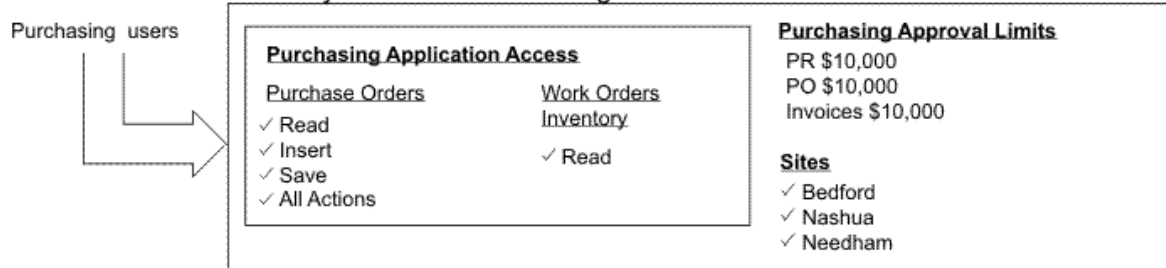
Mixed Non-Independent Security Groups for XYZ Company



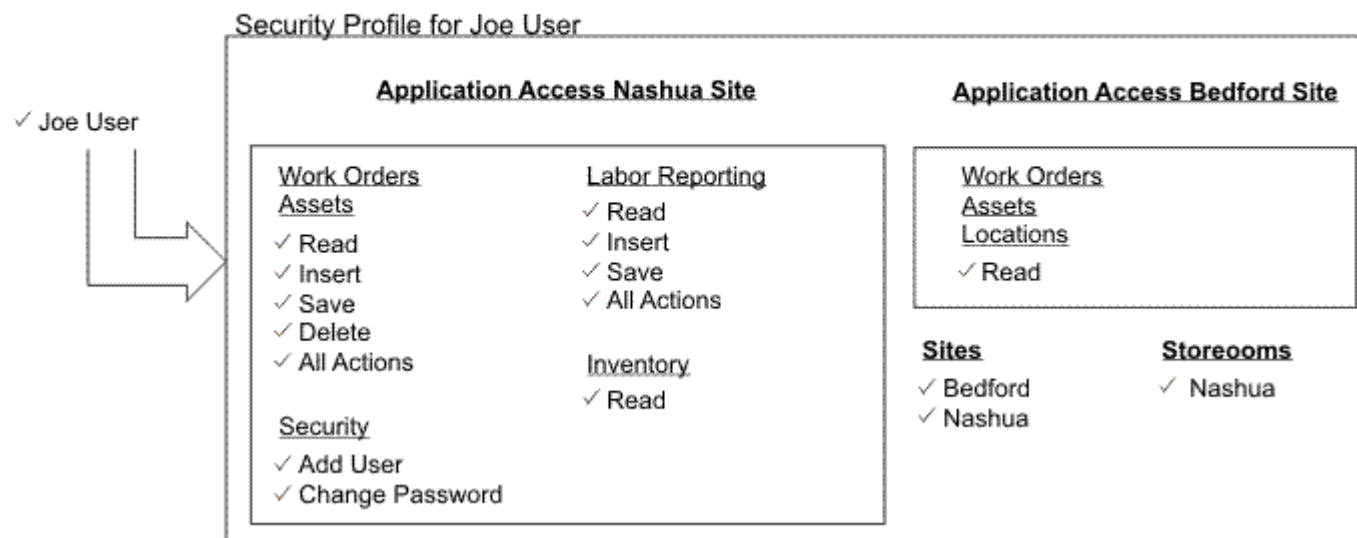
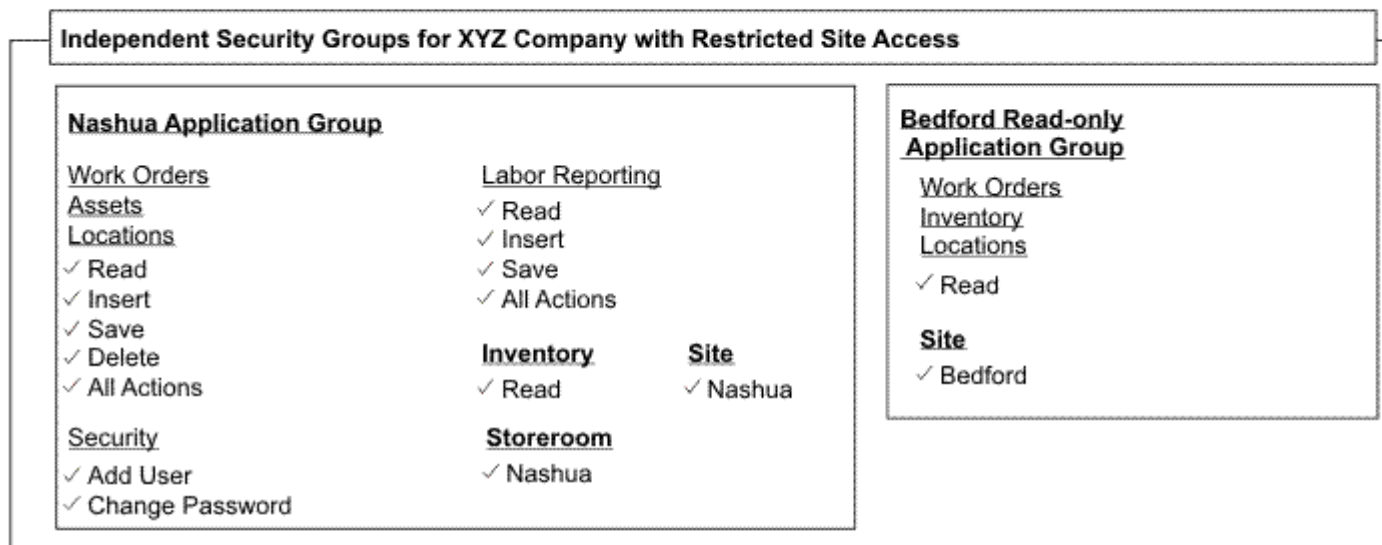
Security Profile for Maintenance Users



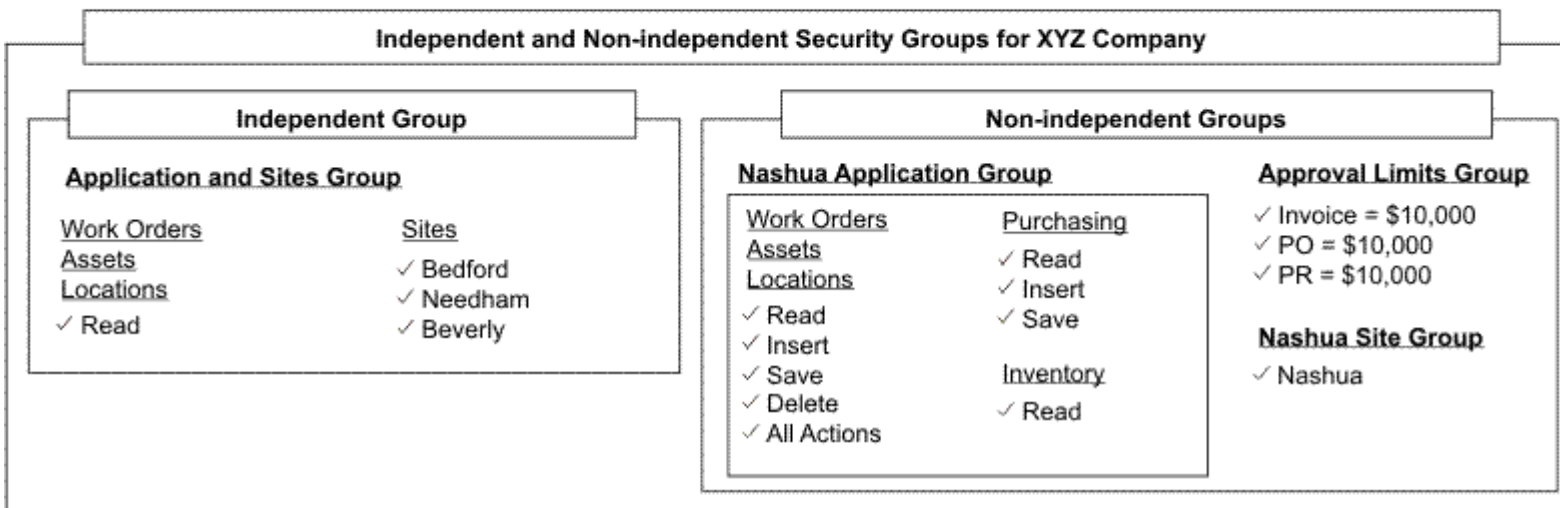
Security Profile for Purchasing Users



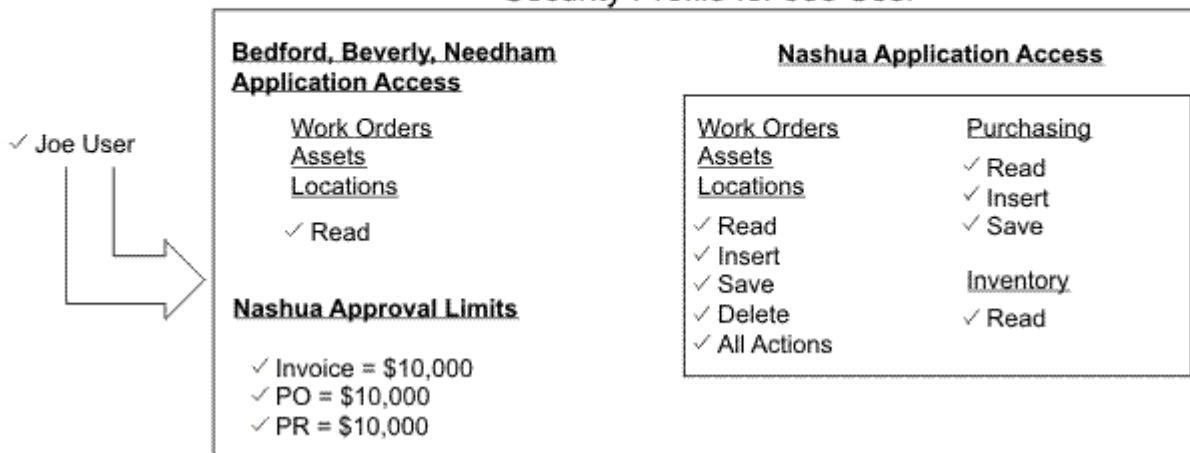
Example: Single organization that practices site administration with independent security groups. The application access groups are restricted to the Nashua and Bedford sites within the organization. The Nashua group provides the user with most of the application and storeroom access needed to perform 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.

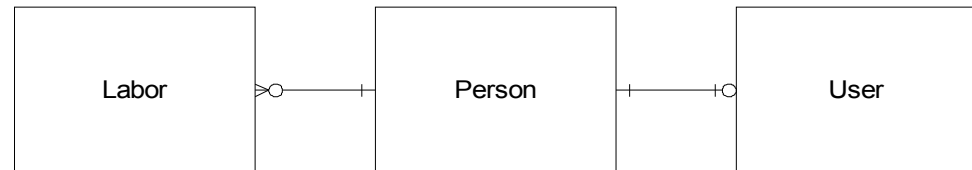


Security Profile for Joe User



People

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



- 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

- 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

The screenshot shows the 'Users' management interface. At the top, there's a navigation bar with 'Users', 'Bullets: (0)', 'Go To', 'Reports', 'Start Center', 'Profile', 'Sign Out', and 'Help'. Below this is a search bar with 'Find:' and 'Select Action' dropdowns, and a toolbar with various icons. The main content area is divided into sections: 'Login Information', 'Personal', and 'User Settings'.
- **Login Information:** Shows 'User Name: wilson' and a 'Set Password' button.
- **Personal:** Shows 'Person: WILSON', 'Status: ACTIVE', 'Display Name: Mike Wilson', 'Address: 40 Lewis Street', 'City: Boston', 'State/Province: MA', 'ZIP/Postal Code: 02113', 'Primary Phone: (617) 555-901', 'Primary E-mail: bdown@maxdev02.svg.usma.ibm.com', 'Workflow Delegate', and 'Memo'.
- **User Settings:** Includes 'Default Insert Site: BEDFORD', 'Storeroom Site for Self-Service Requisitions: BEDFORD', 'Default Storeroom for Self-Service Requisitions', 'User Default Application', 'Language', 'Locale', 'Time Zone: America/Chicago (GMT - 6 DST/Y) Central Standard Time', 'Calendar Type', 'Default Repair Facility', 'Repair Facility Site', 'Use Default Insert Site as a Display Filter? [checked]', 'System Account? [unchecked]', 'Can Access Inactive Sites? [checked]', 'Password Expiration Date', 'Use Screen Reader? [unchecked]', and 'Email format: 1 Simple'.
At the bottom, there's a 'Purchasing' section with 'Filter', '0 - 0 of 0', and 'Download' options, and an 'Organization' section with 'GL Account'.

Used to manage password with internal authentication

Can be synchronized from the directory.

Entered in this system

Automatic Password Generation

* Template for Emailing Reset Passwords: >>

Password Generation Display:

Always E-mail Generated Passwords to Users (Never Display On Screen)

Allow Generated Passwords to Be Displayed On Screen

Password Requirements

* Minimum Password Length:

Number of Identical Adjacent Characters Allowed in Password:

Password can Contain Login ID?

Required Password Characters

Must Include an Uppercase Character?

Must Include a Lowercase Character?

Must Include a Number?

Must Include a Special Character (!, @, #, \$, etc.)?

Allowed Placement of Password Characters

First Character can be a Number?

Last Character can be a Number?

First Character can be a Special Character?

Last Character can be a Special Character?

? Specify a list of any passwords you wish to prohibit from being used on the system. For example, password and maximo.

Excluded Password List

Filter > 0 - 0 of 0

Password
...No rows to display...

Find: Select Action

List User Groups **Security Profile**

User Status Type

Display Name

- System-level applications
 - BEDFORD
 - APPLICATIONS
 - Assets
 - Changes
 - Add to Bookmarks
 - Apply Route
 - Apply SLAs
 - Approve Change
 - Assign to New Parent
 - Associate Folders
 - Attribute Search
 - Bookmarks
 - Cancel Change
 - Change
 - Change Status
 - Clear Changes
 - Close Change
 - Communication
 - Complete Change
 - Costs
 - Create KPI
 - Create Work Package
 - Delete Change
 - Duplicate Change
 - Edit History Change
 - Entire Plan
 - History
 - Incident
 - Initiate Change
 - Manage Folders
 - Manage Library
 - Modify/Delete Work Log
 - More Search Fields
 - Move Asset BMXWOMOVE :woisswap=0
 - Move/Swap/Modify
 - New Change
 - Next Change
 - PO Information
 - Previous Change
 - Problem
 - Read access to Changes
 - Release
 - Remove Work Plan
 - Route Workflow

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

- 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

- 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

New in 7.5.0.2 groups can have a different start application.

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.

Security Groups

Bulletins: (0) Go To Reports Start Center Profile Sign Out Help

Find: Select Action

List Group Sites Applications Storerooms Labor GL Components Limits and Tolerances Data Restrictions Users

Group: MAXADMIN Maximo Administrators (Super Users) Authorize Group for All Sites?

Site	Description	Organization	Active?	Authorized?
BEDFORD	Bedford MA Site of EAGLE Inc. North America	EAGLENA	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Details

* Site: BEDFORD Bedford MA Site of EAGLE Inc. North America Organization: EAGLENA Active? Authorized?

New Row

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.

Applications Download ?

Grant Listed Applications: Revoke Listed Applications:

Description	Main Object/Table	Original Application (if copied)
config		
Actual Configuration Items	Actual CI Table	
Configuration Items	Configuration Item Table	
Database Configuration	Maximo Object Configuration	
Layout and Configuration	Start Center Configuration	

Options for Configuration Items Download ?

Grant Listed Options for This Application

Description	Grant Access?	Condition
Delete CI	<input checked="" type="checkbox"/>	<input type="text"/>
New CI	<input checked="" type="checkbox"/>	<input type="text"/>
Read Access to CI APP	<input type="checkbox"/>	<input type="text"/>
Save CI	<input type="checkbox"/>	<input type="text"/>

Filter Download ?

Description	Grant Access?	Condition
Add CIs to Collections	<input checked="" type="checkbox"/>	<input type="text"/>
Application	<input type="checkbox"/>	<input type="text"/>
Associate Folders	<input checked="" type="checkbox"/>	<input type="text"/>
Attribute Search	<input type="checkbox"/>	<input type="text"/>
Bookmarks	<input checked="" type="checkbox"/>	<input type="text"/>
Business Application	<input type="checkbox"/>	<input type="text"/>
Change	<input checked="" type="checkbox"/>	<input type="text"/>
Change Status	<input type="checkbox"/>	<input type="text"/>
Duplicate CI	<input checked="" type="checkbox"/>	<input type="text"/>
Incident	<input checked="" type="checkbox"/>	<input type="text"/>

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.

- **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.

- 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

Select Action

All Conditions Filter 2 - 11 of 30

Condition	Description	Type	Reference Count
BMX1000	Database Password property	EXPRESSION	3
BMX1002	Report run type	EXPRESSION	3
BMXAA1003	Condition to use for security restrictions by col	CLASS	0
BMXAAWMLINF	Is Linear Work Management	EXPRESSION	36
BMXAAWMLNLI	Is not a Linear Asset in Work Management	EXPRESSION	17
BMXPARENTTK	Parent Ticket for Activity	EXPRESSION	3
BMXPARENTWK	Parent Work Order for Activity	EXPRESSION	3
BMXTKTISGLBL	Relate Record for Global Ticket	EXPRESSION	21
BMXWOMOVE	Work Order Move Asset	EXPRESSION	35
ITASSET	Asset Type is IT	EXPRESSION	0

Details

Condition: ITASSET Description: Asset Type is IT

Type: EXPRESSION

Expression: :assettype = 'IT'

Class: [Empty]

Reference Count: 0

New Row

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

- 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.

Security Groups Go To | Reports | Start Center | Profile | Sign Out | Help

Find: [] Select Action []

List | Group | Sites | Applications | Storerooms | Labor | GL Components | Limits and Tolerances | **Data Restrictions** | Users

Group: MAINTENANCE Maintenance Crew

Object Restrictions | **Attribute Restrictions** | Collection Restrictions

Attributes Filter 1 - 1 of 1 Download

Object	Attribute	Application	Type	Condition
ASSET	DESCRIPTION		READONLY	ITASSET

Details

Object: ASSET The ASSET Table

Attribute: DESCRIPTION Description

Application: []

Type: READONLY

Reevaluate?

Condition: ITASSET Asset Type is IT

Condition Class: []

Expression: ;assettype = 'IT'

New Row

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

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

- 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

Description	Main Object/Table	Original Application (if copied)
Actions	Table to hold actions.	
Activities and Tasks	The WOACTIVITY view.	
Actual Configuration Items	Actual CI Table	
Adapter Conversion	Deployed Assets Adapter Conversion Targets	
Application Designer	The MAXAPPS Table	
Asset Link Results	Asset Link Result view.	
Asset Reconciliation Results	Asset Result of Link and/or Comparison	
Assets	The ASSET Table	
Assignment Manager	The ASSIGNMENT Table	
Bulletin Board	Table to store and maintain bulletin messages	

Description	Grant Access?	Condition
Delete Asset	<input checked="" type="checkbox"/>	
New Asset	<input checked="" type="checkbox"/>	
Read access to Asset	<input checked="" type="checkbox"/>	
Save Asset	<input checked="" type="checkbox"/>	

Description	Grant Access?	Condition
Change Item Number	<input checked="" type="checkbox"/>	
Change Status	<input checked="" type="checkbox"/>	ITASSET
Create KPI	<input checked="" type="checkbox"/>	
Duplicate Asset	<input checked="" type="checkbox"/>	
Enter Meter History	<input checked="" type="checkbox"/>	
Enter Meter Readings	<input checked="" type="checkbox"/>	
Enter Most Recent Meter Reading	<input checked="" type="checkbox"/>	
Incident	<input checked="" type="checkbox"/>	
Issue Items from Storeroom	<input checked="" type="checkbox"/>	
Manage Asset Collections.	<input checked="" type="checkbox"/>	

Details

Description:

Grant Access?:

Condition:

Type:

Expression:

Condition Class:

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

- 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

- 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

Application Designer

Bulletins: (1) Go To Reports Start Center Profile Sign Out Help

Multipart Textbox Properties

Configure Conditional Properties

Signature Option READ Read access to Asset

Signature option tied to the control. All settings below apply to all controls bound to this signature option.

Sequence in which groups are evaluated. Highest 'wins'.

Name	Description	Sequence
MAINTENANCE	Maintenance Crew	30
PURCHREQ	Purchase Requestor	20
SELFSERVICE	Self Service	10

Conditions for Security Group MAINTENANCE

Name	Description	Reevaluate?	Sequence
ITASSET	Asset Type is IT	<input checked="" type="checkbox"/>	10

Sequence in which conditions are evaluated. Highest 'wins'.

Property Values for Condition

Property	Value
label	IT Asset

Property values when condition ITASSET is true

Property	Value
label	IT Asset

Property values when condition ITASSET is false

...No rows to display...

Property values for true and false evaluations of the condition above. You can set multiple for each. There is no validation.

OK Cancel

- 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

- 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 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'

Find: Select Action [Icons]

List **Cron Task**

Cron Task: **VMMSYNC** Invokes WebSphere VMM APIs to populate data
 Class: **psdi.security.vmm.VMMSyncCronTask**
 Access Level: **FULL**

Cron Task Instances Download

Cron Task Instance Name	Schedule	Run as User	Active?	Keep History?	Max Number of History Records
VMMSYNC01	5m,*****	MAXADMIN	<input type="checkbox"/>	<input type="checkbox"/>	0

Details

Cron Task Instance Name: **VMMSYNC01** Invokes WebSphere VMM APIs to populate data
 Schedule*: **5m,*******
 Run as User*: **MAXADMIN**
 Active?

Keep History?
 Max Number of History Records:
 Last Run Timestamp:

[Duplicate](#) [New Row](#)

Parameters History

Cron Task Parameters Download

Parameter	Value	Description
Credential		VMM admin credentials.
GroupMapping	<?xml version="1.0" encoding="UTF-8" ?><IDO	The USER XML used by the VMM task.
GroupSearchAttribute	cn	VMM search attribute to query group records.
Principal	cn=vmmadmin,ou=maxusers,dc=mydomain,dc-	VMM admin principal.
SynchAdapter	psdi.security.vmm.DefaultVMMSyncAdapter	VMM synchronization adapter.
SynchClass	psdi.security.vmm.VMMSynchronizer	VMM synchronization class.
UserMapping	<?xml version="1.0" encoding="UTF-8" ?><IDO	The USER XML used by the VMM task.
UserSearchAttribute	uid	VMM search attribute to query user records.

Details

Parameter: **UserMapping** The USER XML used by the VMM task.

```
<?xml version="1.0" encoding="UTF-8" ?><!DOCTYPE Idapsync
SYSTEM "ldapuser.dtd"><ldapsync><user>
<basedn>ou=maxusers,dc=mydomain,dc=com</basedn>
<filter>PersonAccount </filter> <scope>subtree</scope> <attributes>
<attribute>uid</attribute> <attribute>givenName</attribute>
<attribute>sn</attribute> <attribute>displayname</attribute>
```

- 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

Select Action

Global Properties Download ?

Property Name	Description	Current Value
	encrypt	
<input type="checkbox"/> mx.e.security.crypto.algorithm	Encryption algorithm for CRYPTO datatype	
<input type="checkbox"/> mx.e.security.crypto.key	Encryption key for CRYPTO datatype	
<input type="checkbox"/> mx.e.security.crypto.mode	Encryption mode for CRYPTO datatype	
<input type="checkbox"/> mx.e.security.crypto.modulus	Encryption modulus for CRYPTO datatype	
<input type="checkbox"/> mx.e.security.crypto.padding	Encryption padding for CRYPTO datatype	
<input type="checkbox"/> mx.e.security.crypto.spec	Encryption spec for CRYPTO datatype	
<input type="checkbox"/> mx.e.security.cryptox.algorithm	Encryption algorithm for CRYPTOX datatype	
<input type="checkbox"/> mx.e.security.cryptox.key	Encryption key for CRYPTOX datatype	

Global Properties Details

Property Name: <input type="text" value="mx.e.security.crypto.algorithm"/>	File Override? <input type="checkbox"/>	Security Level: <input type="text" value="PRIVATE"/>
Description: <input type="text" value="Encryption algorithm for CRYPTO datatype"/>	Global Only? <input checked="" type="checkbox"/>	User Defined? <input type="checkbox"/>
Global Value: <input type="text"/>	Instance Only? <input type="checkbox"/>	Nulls Allowed? <input checked="" type="checkbox"/>
Current Value: <input type="text"/>	Online Changes Allowed? <input type="checkbox"/>	Data Type: <input type="text" value="ALN"/>
Maximo Default: <input type="text"/>	Live Refresh? <input type="checkbox"/>	Domain: <input type="text"/>
	Encrypted? <input checked="" type="checkbox"/>	

[New Row](#)

Instance Properties Download ?

Property Name	Description	Value
<input type="checkbox"/> mx.e.com.port	Com port	
<input type="checkbox"/> mx.e.hostname	Name of the machine and port hosting MXServ	localhost:7001

[New Row](#)

- 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

The screenshot shows the 'System Properties' interface with a table of global properties. The table has columns for 'Property Name', 'Description', and 'Current Value'. Two properties are listed: 'mxs.sec.IPblock' with a value of '1' and 'mxs.sec.IPblock.sec' with a value of '30'. The 'ip_block' text is highlighted in the search field.

Property Name	Description	Current Value
mxs.sec.IPblock	Perform security checks related to IP blocking	1
mxs.sec.IPblock.sec	Number of seconds for IP blocking limit check	30

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

- **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

- **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**

- 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.**

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		

Organization	Labor	Name
	LABORSELF	Their Own Labor

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

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

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 Schaffer	ACTIVE	TYPE 1
SMITH	SMITH	Roland Smith	ACTIVE	TYPE 1

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??