# Maximo LDAP Authentication

Colleen McCretton
Designer & Architect, Maximo

# Agenda

- LDAP Overview
- Maximo integration with LDAP
- Authentication
- Synchronization
- SSO

# What is LDAP?

- Lightweight Directory Access Protocol
- Connects to central repository of users, passwords, and information
- Hierarchical
- Based on open standard X.500 directory services

# Why use an LDAP Directory?

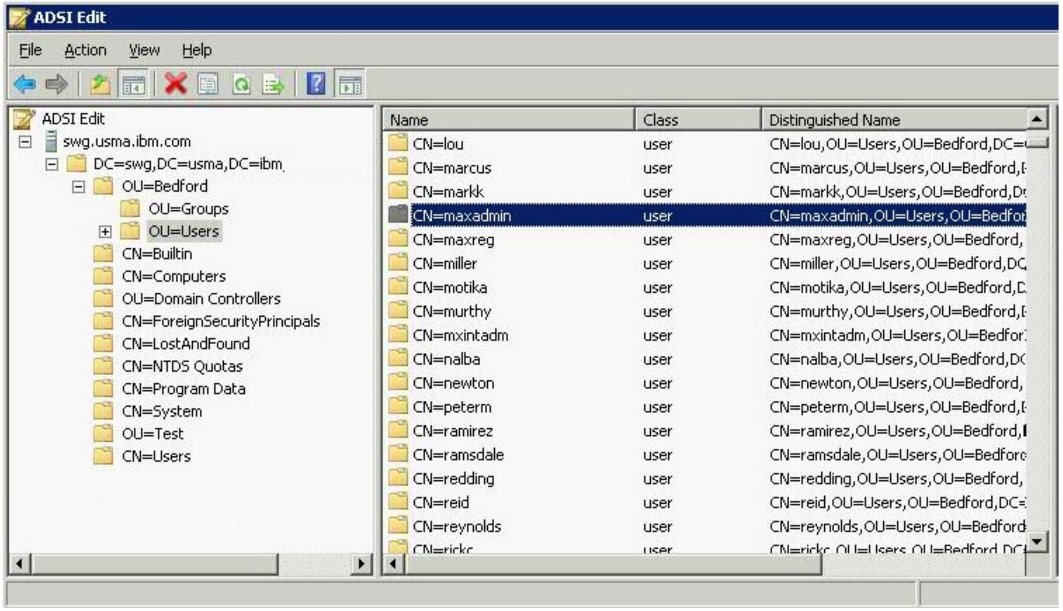
- **Centralized user and group administration**
- **Integration with other application authentication**
- **Streamline logins**
- **Users manage passwords in Windows**
- **Offload Maximo user administration to Windows**

# LDAP Directory Software

- **IBM Tivoli Directory Server**
- **Microsoft Active Directory**
- **Apple Open Directory**
- **Novell eDirectory**
- **OpenLDAP**
- **Oracle Internet Directory**
- **Sun Java System Directory Server**

# LDAP Conventions

- **Components**
  - CN-Common Name
  - DC-Domain Component
  - DN-Distinguished Name
  - OU-Organizational Unit
  - Root



- ADSI Edit
  - swg.usma.ibm.com
    - DC=swg,DC=usma,DC=ibm
      - OU=Bedford
        - OU=Groups
        - OU=Users
      - CN=Builtin
      - CN=Computers
      - OU=Domain Controllers
      - CN=ForeignSecurityPrincipals
      - CN=LostAndFound
      - CN=NTDS Quotas
      - CN=Program Data
      - CN=System
      - OU=Test
      - CN=Users

| Name | Class | Distinguished Name |
|---|---|---|
| CN=lou | user | CN=lou,OU=Users,OU=Bedford,DC= |
| CN=marcus | user | CN=marcus,OU=Users,OU=Bedford, |
| CN=markk | user | CN=markk,OU=Users,OU=Bedford,D |
| CN=maxadmin | user | CN=maxadmin,OU=Users,OU=Bedfor |
| CN=maxreg | user | CN=maxreg,OU=Users,OU=Bedford, |
| CN=miller | user | CN=miller,OU=Users,OU=Bedford,DC |
| CN=motika | user | CN=motika,OU=Users,OU=Bedford,D |
| CN=murthy | user | CN=murthy,OU=Users,OU=Bedford, |
| CN=mxintadm | user | CN=mxintadm,OU=Users,OU=Bedfor |
| CN=nalba | user | CN=nalba,OU=Users,OU=Bedford,D |
| CN=newton | user | CN=newton,OU=Users,OU=Bedford, |
| CN=peterm | user | CN=peterm,OU=Users,OU=Bedford, |
| CN=ramirez | user | CN=ramirez,OU=Users,OU=Bedford, |
| CN=ramsdale | user | CN=ramsdale,OU=Users,OU=Bedford |
| CN=redding | user | CN=redding,OU=Users,OU=Bedford, |
| CN=reid | user | CN=reid,OU=Users,OU=Bedford,DC= |
| CN=reynolds | user | CN=reynolds,OU=Users,OU=Bedford |
| CN=rickc | user | CN=rickc,OU=Users,OU=Bedford,DC |

# Distinguished Name

- **Read from “bottom up”**
- **Includes all parent folders**

```
cn=maxadmin,ou=users groups,ou=Bedford,dc=swg,dc=ibm,dc=com
```

# Active Directory (AD)

- **Microsoft’s LDAP software**
- **Most popular since Windows 2000**
- **Several major differences between other LDAP software**

# AD Specific Conventions – Users & Groups

- **sAMAccountName**
  - sAM=Security Accounts Manager
  - loginid
- **Domain Users**
  - Global group
  - CN=Domain Users,CN=Users,DC=company,DC=com
- **Groups**
  - Groups can be nested in AD
  - Groups are CN's not OU's

# AD Server Conventions

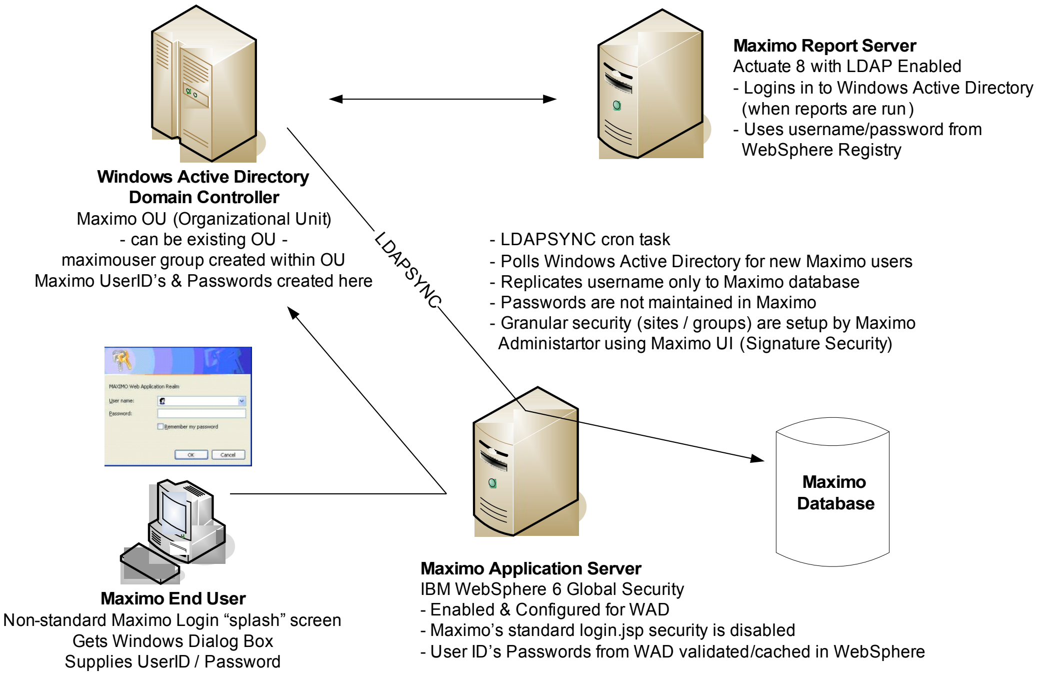
- **Servers**
  - Domain Controller (DC)
    - Contains AD information
  - Global Catalog (GC)
    - Extension of DC
    - Contains partial information of DC
    - Faster
- **Domain**
  - Branch of a “tree”
- **Forest**
  - Root
  - Can contain multiple domains

# LDAP and Maximo

- **Application Server Authentication**
  - Connect to an LDAP directory via application server
  - Directory ‘owns’ users, passwords
  - Information required for authorizations is synched into Maximo (optional)
  - Property available to allow managing information in the directory and Maximo
    - mxe.LDAPUserMgmt
      - When set to 1, ser information can only be managed in the directory
      - When set to 0 user information can be managed in Maximo too
- **Application server is the ‘authenticator’ for the Maximo deployment**

# Architecture (cont’d)

**IBM Maximo 6 – Standard LDAP Configuration for Microsoft Windows Active Directory**



**Windows Active Directory Domain Controller**
Maximo OU (Organizational Unit)
- can be existing OU -
maximouser group created within OU
Maximo UserID’s & Passwords created here

**Maximo Report Server**
Actuate 8 with LDAP Enabled
- Logins in to Windows Active Directory (when reports are run)
- Uses username/password from WebSphere Registry

- LDAPSYNC cron task
- Polls Windows Active Directory for new Maximo users
- Replicates username only to Maximo database
- Passwords are not maintained in Maximo
- Granular security (sites / groups) are setup by Maximo Administartor using Maximo UI (Signature Security)

**Maximo Database**

**Maximo End User**
Non-standard Maximo Login “splash” screen
Gets Windows Dialog Box
Supplies UserID / Password

**Maximo Application Server**
IBM WebSphere 6 Global Security
- Enabled & Configured for WAD
- Maximo’s standard login.jsp security is disabled
- User ID’s Passwords from WAD validated/cached in WebSphere

The maximouser group does not have to exist in the same OU as the users . Maximo users can exist in any OU , as long as we are looking at a parent that can traverse down all the children . This means that we can go up as long as the number of children do not exceed 1000. This is an artificial limit set by AD, which can be changed

# Authentication vs. Authorization

- **Authentication**
  - Access to resources
  - WebSphere sees all of Maximo as a sigle resource

- **Authorization**
  - Group membership
  - Permissions
  - Maximo application authorization

# When Application Server Security is Enabled for Maximo

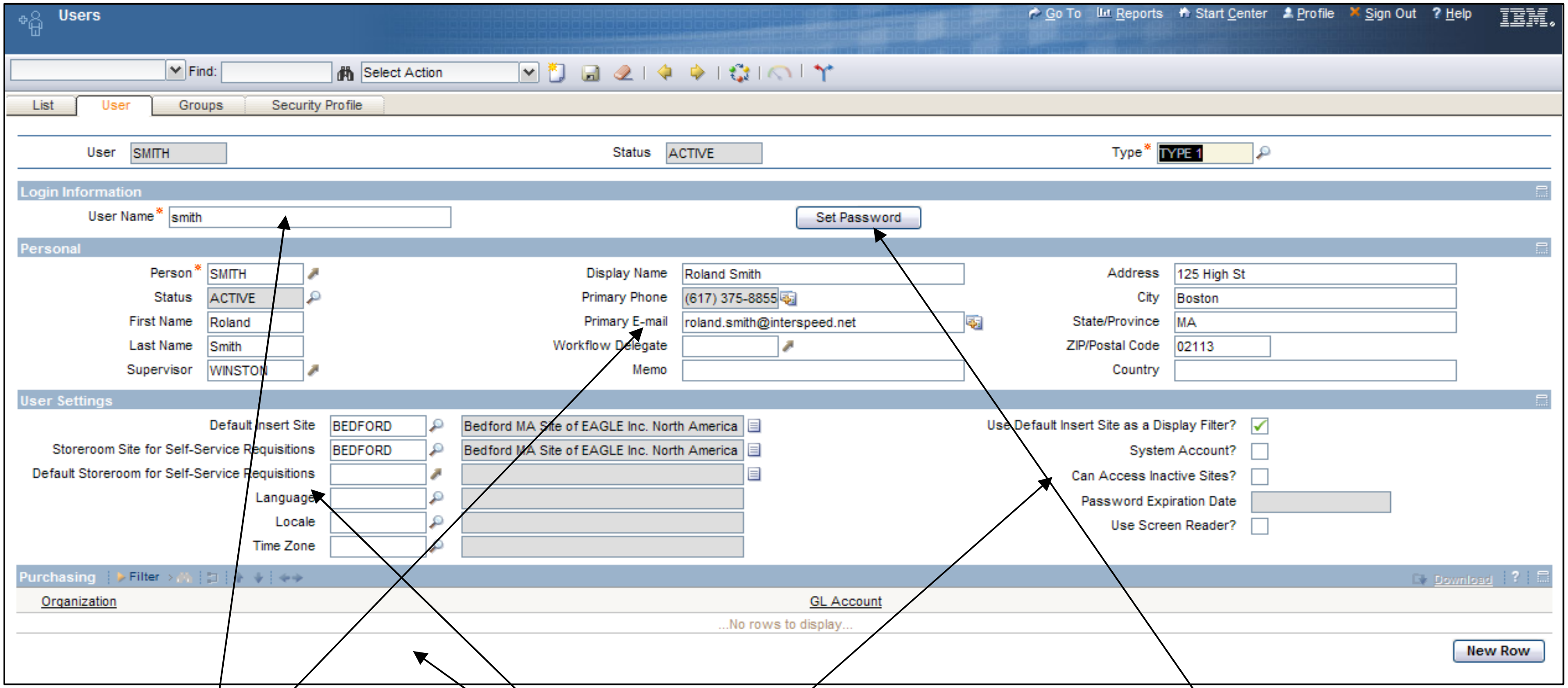
- **When a user tries to access the Maximo URL Maximo asks the app server to authenticate the user**
- **A ‘basic’ login box from the app server or a custom ‘form’ can be used – FORMS is advised as it is more secure**
- **The app server authenticates the user and passes back an LTPA token to Maximo**
  - Token must contain an id that can be resolved to a loginid in the MAXUSER table

## Important things to know about Maximo and LDAP Directories

- **All users must have unique logins across org**
  - Important with multiple forests or LDAP servers
- **Only one maxadmin ID can exist**
  - Any Maximo instance using LDAP uses same maxadmin
  - Cannot have both a group and a user named maxadmin
  - Copy current MAXADMIN group in Maximo to new MAXADMIN group *before* LDAP
- **No support for nested groups**

# Synchronization from and LDAP Directory

- **Enable Application Server Authentication**
  - Information required for authorizations can be synched from
    - User ID, Group Memberships, addresses and phone numbers, etc. the directory managed in Maximo
    - Never passwords – always in directory
  - Property settings for who ‘owns’ what information
- **Synchronizes users and groups from directory to Maximo**
- **One way only directory → Maximo**
- **Populates EMAIL, GROUPUSER, MAXGROUP, MAXUSER, PERSON, PHONE**
  - Cron task manages synchronization
    - LDAPSYNC
    - VMMSYNC
  - Parameters of the cron task contain xml for attribute mapping
    - Can populate other tables, *e.g.* LABOR
    - Can change default attribute mappings



| | | | | | |
|---|---|---|---|---|---|
| User | SMITH | Status | ACTIVE | Type* | TYPE 1 |

**Login Information**

User Name* smith

Set Password

**Personal**

| | | | | | |
|---|---|---|---|---|---|
| Person* | SMITH | Display Name | Roland Smith | Address | 125 High St |
| Status | ACTIVE | Primary Phone | (617) 375-8855 | City | Boston |
| First Name | Roland | Primary E-mail | roland.smith@interspeed.net | State/Province | MA |
| Last Name | Smith | Workflow Delegate | | ZIP/Postal Code | 02113 |
| Supervisor | WINSTON | Memo | | Country | |

**User Settings**

| | | | | |
|---|---|---|---|---|
| Default Insert Site | BEDFORD | Bedford MA Site of EAGLE Inc. North America | Use Default Insert Site as a Display Filter? | ☑ |
| Storeroom Site for Self-Service Requisitions | BEDFORD | Bedford MA Site of EAGLE Inc. North America | System Account? | ☐ |
| Default Storeroom for Self-Service Requisitions | | | Can Access Inactive Sites? | ☐ |
| Language | | | Password Expiration Date | |
| Locale | | | Use Screen Reader? | ☐ |
| Time Zone | | | | |

**Purchasing** Filter Download

| Organization | GL Account |
|---|---|

...No rows to display...

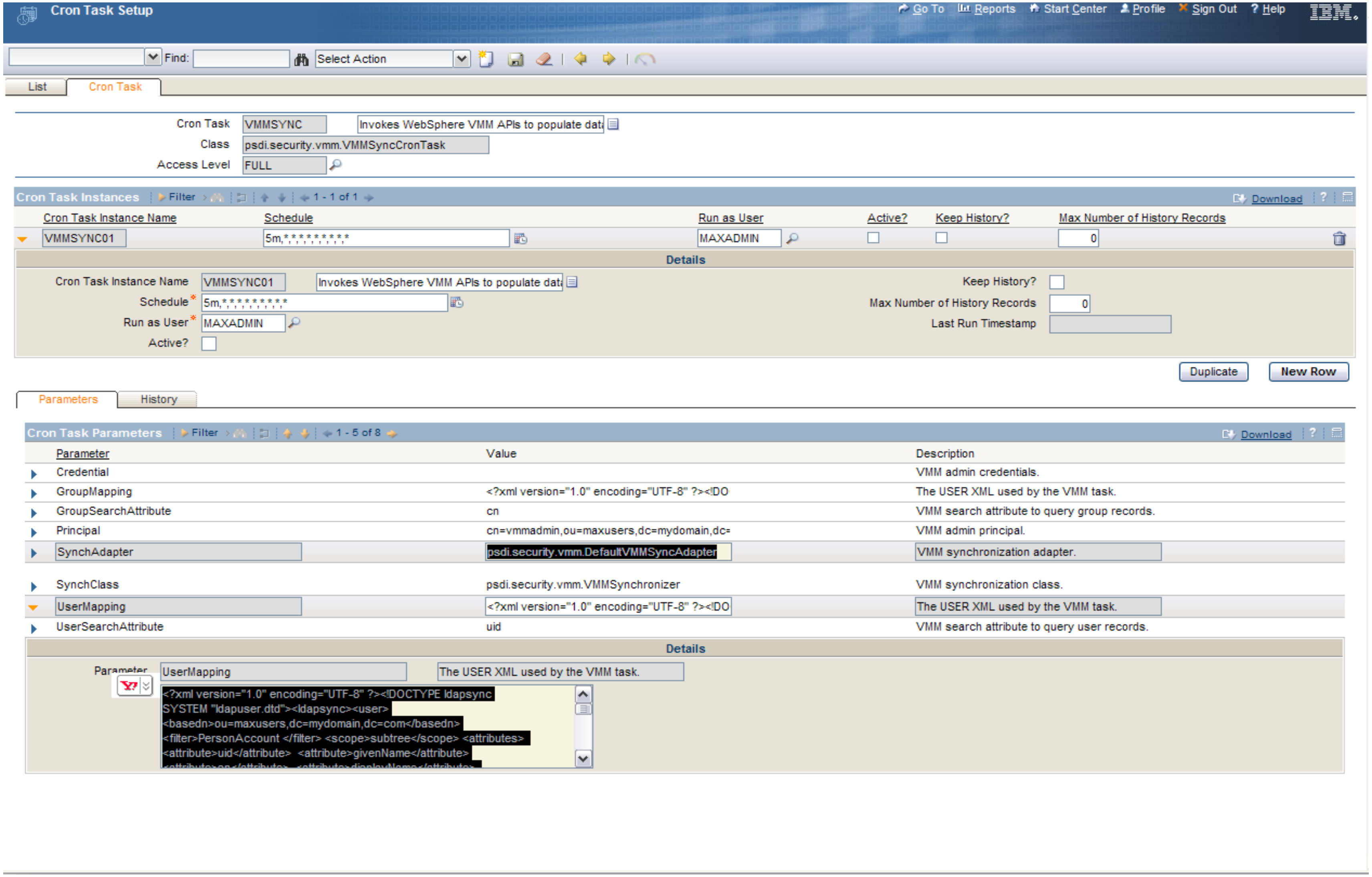
New Row

Synchronized from the directory.

Entered in this system

Irrelevant if the external directory (LDAP) handles password management

# Maximo LDAP Authentication



| | | |
|---|---|---|
| Cron Task | VMMSYNC | Invokes WebSphere VMM APIs to populate dat |
| Class | psdi.security.vmm.VMMSyncCronTask | |
| Access Level | FULL | |

| Cron Task Instance Name | Schedule | Run as User | Active? | Keep History? | Max Number of History Records |
|---|---|---|---|---|---|
| VMMSYNC01 | 5m,*,*,*,*,*,*,*,*,* | MAXADMIN | □ | □ | 0 |

**Details**

| | | | |
|---|---|---|---|
| Cron Task Instance Name | VMMSYNC01 Invokes WebSphere VMM APIs to populate dat | Keep History? | □ |
| Schedule* | 5m,*,*,*,*,*,*,*,*,* | Max Number of History Records | 0 |
| Run as User* | MAXADMIN | Last Run Timestamp | |
| Active? | □ | | |

| Parameter | Value | Description |
|---|---|---|
| Credential | | VMM admin credentials. |
| GroupMapping | <?xml version="1.0" encoding="UTF-8" ?><!DO | 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" ?><!DO | 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 ldapsync
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>cn</attribute>  <attribute>displayName</attribute>
```

# LDAP Sync Considerations

- **Who will be synchronized?**
  - Use filters to sync a subset of users.
  - Based on OU, role or group or meet a standard query.
  - If you have a registered user license, any user in the system must be licensed if they are in an ‘Active’ status.
- **What if we need to sync users from multiple places?**
  - use multiple instances of the sync process to ‘grab’ different OUs, for example.
- **Which sync process will we use?**
  - LDAPSYNC
    - only for Microsoft Active Directory.
    - WebSphere or WebLogic
    - after the initial sync only changes in the directory will be sync’d improving performance
  - VMMSYNC
    - WebSphere only
    - can bring together information from multiple directories
    - Microsoft Active Directory (AD) and/or IBM Tivoli Directory Server(ITDS)
    - performs a full sync each time it is run
    - enhancement to add incremental sync to this process coming end of 2011
- **What if I use a directory other that Microsoft Active Directory or IBM Tivoli Directory Server?**
  - These are the only supported directories
  - By modifying a class file and the xml mappings in the cron task instance integration with other directories such as Oracle, Sun and Siemens has been implemented through services and partners at several customer locations.
  - no current roadmap for extending support to additional directory platforms.

# Things to know about user synchronization

- **Cannot recycle users with Maximo**
  - Mike Lee (mlee) leaves Mary Lee (mlee) joins
  - Each user must be unique, *e.g.*, mlee, mlee2
- **Disabled users in the directory are not disabled in Maximo**
  - Create trigger in database to disable
- **Changing username in the directory will not change in Maximo**
  - Creates new user
  - One way replication (directory → Maximo)
- **Users deleted in  the directory will not delete in Maximo**
- **Users sync with NULL password in MAXUSER**
- **Existing users do not have password overwritten**
- **Case for loginid must be configured correctly**

# MiXeD cAsE

- **LOGINID field in Maximo *is* case sensitive**
- **Field used for LOGINID may be MiXeD CaSe**
- **Can force to UPPER case in ldapsync.xml**

```
<table name="MAXUSER">
    <keycolumn name="USERID" type="UPPER">sAMAccountName</keycolumn>
    <column name="LOGINID" type="UPPER">sAMAccountName</column>
    <column name="PERSONID" type="UPPER">sAMAccountName</column>
    <column name="STATUS" type="UPPER">{ACTIVE}</column>
    <column name="TYPE" type="UPPER">{PRIMARY}</column>
    <column name="QUERYWITHSITE" type="YORN">{1}</column>
    <column name="FORCEEXPIRATION" type="YORN">{0}</column>
    <column name="FAILEDLOGINS" type="YORN">{0}</column>
    <column name="PASSWORD" type="CRYPTO">{0}</column>
    <column name="MAXUSERID" type="INTEGER">{:uniqueid}</column>
    <column name="SYSUSER" type="YORN">{0}</column>
    <column name="SCREENREADER" type="YORN">{0}</column>
</table>
```

# Things to know about group synchronization

- **Group membership in directory replicates to Maximo**
  - Manage group membership in directory or Maximo
- **Renaming group in directory does not rename it Maximo**
  - Creates new group
- **Deleting group in directory does not delete it in Maximo**
- **All security Maximo application authorization handled in Maximo**

# Use LDAP Filters to sync only the right data

- **<user>**

```
<user>
   <basedn>ou=allmaximousers,dc=mydomain,dc=com</basedn>
   <filter>(&amp;(objectCategory=person)(objectClass=user))</filter>

<user>
   <basedn>OU=Accounts,DC=mydomain,DC=com</basedn>

   <filter>(memberOf=cn=MAXIMOUSER,OU=Groups,OU=Accounts,DC=mydomain,DC=com)</filter>
```

- **<group>**

```
<group>
   <basedn>ou=allmaximogroups,dc=mydomain,dc=com</basedn>
   <filter>(&amp;(objectCategory=Group)(objectClass=group))</filter>

<group>
   <basedn>OU=Groups,OU=Accounts,DC=mydomain,DC=com</basedn>
   <filter>(cn=MAX*)</filter>
```

# Example of what a filter can do…

- Bring all users over, but mixed with conference rooms, computers, resources
- AND

```
 <filter>(&amp;(objectCategory=person)(objectClass=user)((cn=Emp*))</filter>
```

- NOT

```
<filter>(&amp;(objectCategory=person)(objectClass=user)(!(cn=Conf*))(!
   (cn=thinkpad*))(!(cn=projector*)))</filter>
```

- OR

```
<filter>(&amp;(objectCategory=person)(objectClass=user)(|(cn=Conf*))(|
   (cn=thinkpad*))(|(cn=projector*)))</filter>
```

# If you need to re-sync from directory

- **Re-sync of users and groups from external directory.**
  - Delete records from the LDAPSYNCPARAMS table
    - Used with LDAPSYNC not VMMSYNC
    - Initiates a full sync
  - Deleting records from the MAXUSER, PERSON, EMAIL, PHONE, MAXGROUP and GROUPUSER tables may be desirable to avoid duplication of data
- **Only supported for LDAPSYNC cron task**

# Secure Sockets Layer (SSL)

- **SSL offers security between Maximo and LDAP**
- **SSL encrypts traffic**
- **Self-signed or public certificates**
- **SSL and ldapsync.xml**
  - Edit ldapsync.xml or Port Parameter of the cron task and change the port to 636

```
<host>myldapserverhost</host>
<port>636</port>
<sslenabled>true</sslenabled>
```

# Single Sign On (SSO)

- **Not prompted for credentials**
- **Third party software not supplied by IBM**
- **Dependent on what the application server supports**
- **Application Server Security must be enabled in Maximo**
- **All other configuration in app server**

# Questions