Smart Cloud Enterprise Tivoli Service Automation Manager Security Guide

Tivoli Service Automation Manager Server security setup

Maximo ID management

General security procedures in a cloud environment

Ira Chavis

Redpaper

ibm.com/redbooks

International Technical Support Organization

SmartCloud Enterprise Tivoli Service Automation Manager Security Guide

November 2012

REDP-4907-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (November 2012)

This edition applies to Version1 Release 7 of Tivoli Service Automation Manager.

This document was created or updated on November 16, 2012.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

DB2®
IBM®
Maximo®
Redbooks®
Redbooks (logo) ®
Tivoli®
WebSphere®

The following terms are trademarks of other companies:

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

The security for Tivoli® Service Automation Manager primarily relies on the underlying components of IBM® DB2®, WebSphere® Application Server, and IBM Tivoli Directory Server. The configuration steps to enable and manage security for Tivoli Service Automation Manager and the operational procedures to manage the environment after it is set up are described in this guide. It assumed that the Tivoli Service Automation Manager server is installed and operational. The security best practices that are used in this guide are based on real scenarios that are used in the IBM SmartCloud Enterprise (SCE). We also provide some sample scripts that were developed to help simply the tasks for creating and managing Maximo® administrators and users.

This IBM® Redpaper™ is intended for IT personnel who install and configure security for Tivoli Service Automation Manager.

The team who wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Ira Chavis is a Certified Consulting IT Specialist in the IBM GTS Services Delivery Offerings. In his role as Delivery Global Provisioning team leader for Smart Cloud Enterprise (SCE) and Smart Cloud Enterprise+ (SCE+), he leads the provisioning engineering practice for IBM's latest Cloud offerings. He has over 32 years of diversified software engineering and IT experience. Before working at IBM, Ira worked at Digital Equipment Corporation in various assignments.

Thanks to following people for their contributions to this guide:

- Deepak Vanjani
- Sunil Agrawal
- Jaidev Karanth

  Persistent Systems

- Chris Calzetoni, IBM Rochester
- Naveen Deshwal, IBM Research Triangle Park
- Mark Leitch, IBM Toronto
- Hendrik Wagner, IBM Boeblingen
- Chris Wheeler, IBM Poughkeepsie

- Mike Ebbers

  International Technical Support Organization, Poughkeepsie Center

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

http://ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  http://www.ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter at:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds at:

  http://www.redbooks.ibm.com/rss.html

1

Introduction

This Redpaper introduces the need for security when a cloud is used for provisioning.

This chapter provides an overview of security and is intended for executives, architects, and administrators.

1.1 Executive overview

With the increasing popularity of cloud computing and its capabilities of dynamic provisioning, the need for security in the provisioning process is greater than ever. But productivity is also an important concern.

The goal of security in IBM provisioning software (such as Tivoli® Provisioning Manager) is to protect the resources in the data model with a minimum of administrative support. The provisioning server uses two types of security to protect the data model: authentication and authorization. After the identity of the user is verified through authentication, authorization determines what the user can do with the product.

1.1.1 Business problem

When a multi-component cloud infrastructure is implemented, the security of the provisioning infrastructure is not integrated. Therefore, often the default role for IT staff is that of privileged user, which is a security exposure. In real-world scenarios, the support staff of the provisioning environment has multiple roles, such as privileged administrator, operator, or read-only operator. It is important to create a proper roles-based model that supports the security model of cloud provider and integrates into other elements of the cloud providers' security infrastructure. In some cases, the smaller business might have a single instance of an environment server that handles their entire provisioning infrastructure. For larger enterprises, many instances might exist that comprise the cloud-wide environment. In either case, we are faced with similar issues of leveraging the user directory for cloud-wide authentication and authorization requirements.

1.1.2 Business solution

This exposure is eliminated by using the proper security configuration with IBM Tivoli Service Automation Manager. The purpose of this IBM Redbooks publication is to describe the configuration steps that are used to enable and manage security with Tivoli Service Automation Manager. The operational procedures that are used to manage the environment after it is set up also are described.

1.2 Technical overview

The security for Tivoli Service Automation Manager security primarily relies on its underlying components of WebSphere Application Server and IBM Tivoli Directory Server. It assumes that the Tivoli Service Automation Manager server is installed and operational. The best practices of security that is used in this guide are based on real scenarios that are used in the IBM SmartCloud Enterprise. We also provide some sample scripts developed to help simplify the tasks for creating and managing Maximo administrators and users.

Tivoli Service Automation Manager provides a provisioning infrastructure that is built on the following IBM software components:

- IBM Tivoli Provisioning Manager
- IBM DB2
- IBM WebSphere Application Server
- IBM Tivoli Directory Server

Figure 1-1 shows the logical component architecture of Tivoli Service Automation Manager.

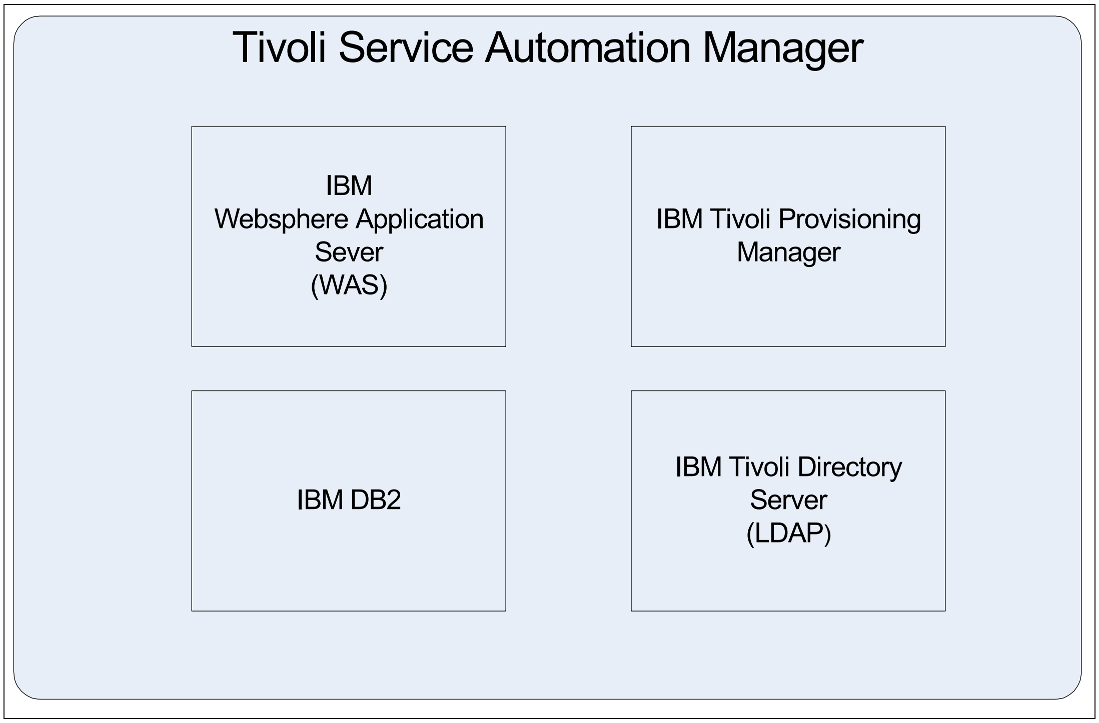


Figure 1-1 Tivoli Service Automation Manager logical architecture

The content of this guide is based on the following software levels:

- Operating System: RHEL 5.6 x64 Linux
- Tivoli Service Automation Manager: 7.2.0.3
- Tivoli Provisioning Manager: 7.1.1.6
- WebSphere Application Server: 6.1.0.23
- DB2: 9.5 FP9
- IBM Tivoli Directory Server: 6.2.0.21

1.2.1 Deployment patterns

Depending on your business and infrastructure requirements, the following deployment patterns are available for installing Tivoli Service Automation Manager and IBM Tivoli Directory Server:

- Single Tivoli Service Automation Manager Server and IBM Tivoli Directory Server (LDAP) instance
- Single Tivoli Service Automation Manager Server with IBM Tivoli Directory Server/DB2 Server
- Multiple Tivoli Service Automation Manager Servers with centralized remote LDAP Server

Single Tivoli Service Automation Manager Server and IBM Tivoli Directory Server instance

This deployment pattern provides all of the Tivoli Service Automation Manager components that are installed on a single physical server or virtual machine image. This environment is good for development and test purposes, but is not recommended for production installations. Here, all LDAP communications are local. The technical solution that is provided in this publication supports this deployment pattern, as shown in Figure 1-2.

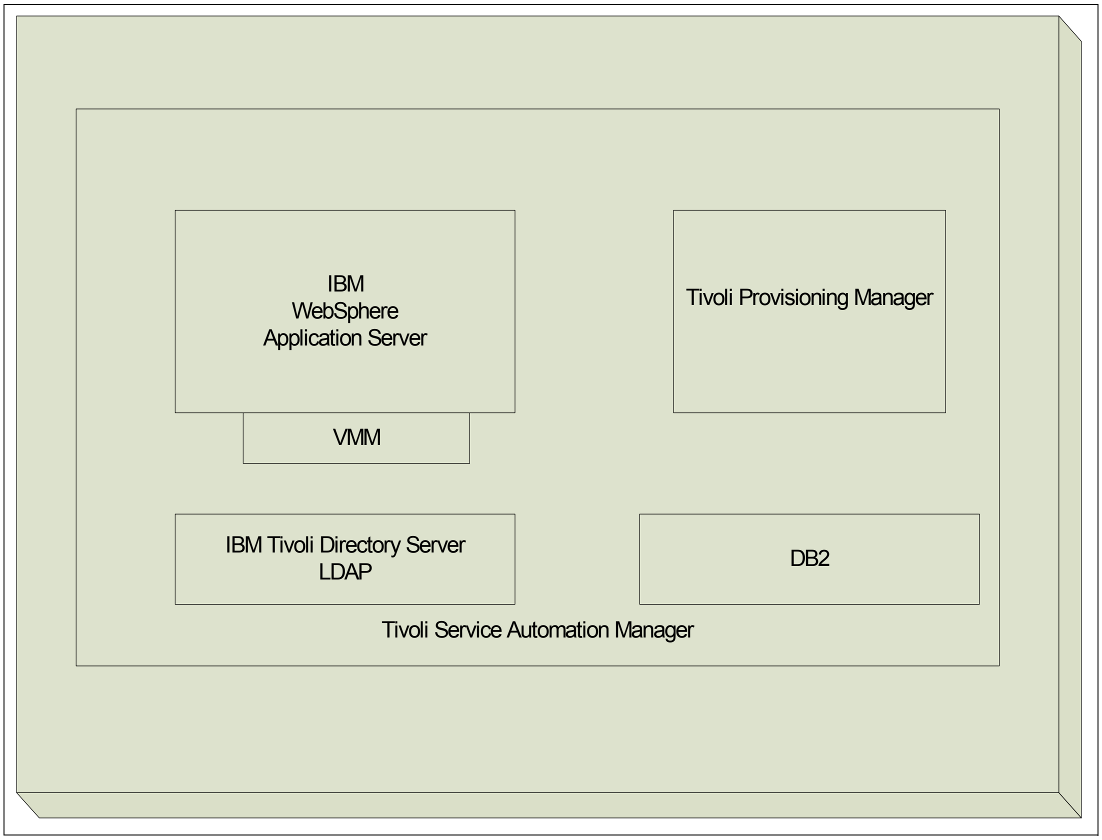

IBM
WebSphere
Application Server
Tivoli Provisioning Manager
VMM
IBM Tivoli Directory Server
LDAP
DB2
Tivoli Service Automation Manager

Figure 1-2 Single server with LDAP

Single Tivoli Service Automation Manager Server with IBM Tivoli Directory Server/DB2 Server

This deployment pattern involves placing DB2 and IBM Tivoli Directory Server on one physical server or virtual machine image and the Tivoli Service Automation Manager Management Server on another. This architecture allows for performance-oriented deployments. The LDAP communications from Tivoli Service Automation Manager to the LDAP server are done via a network connection. This pattern may be repeated for each Tivoli Service Automation Manager site but does not provide for centralized LDAP management. The technical solution that is provided in this publication supports this deployment pattern, as shown in Figure 1-3 on page 5.

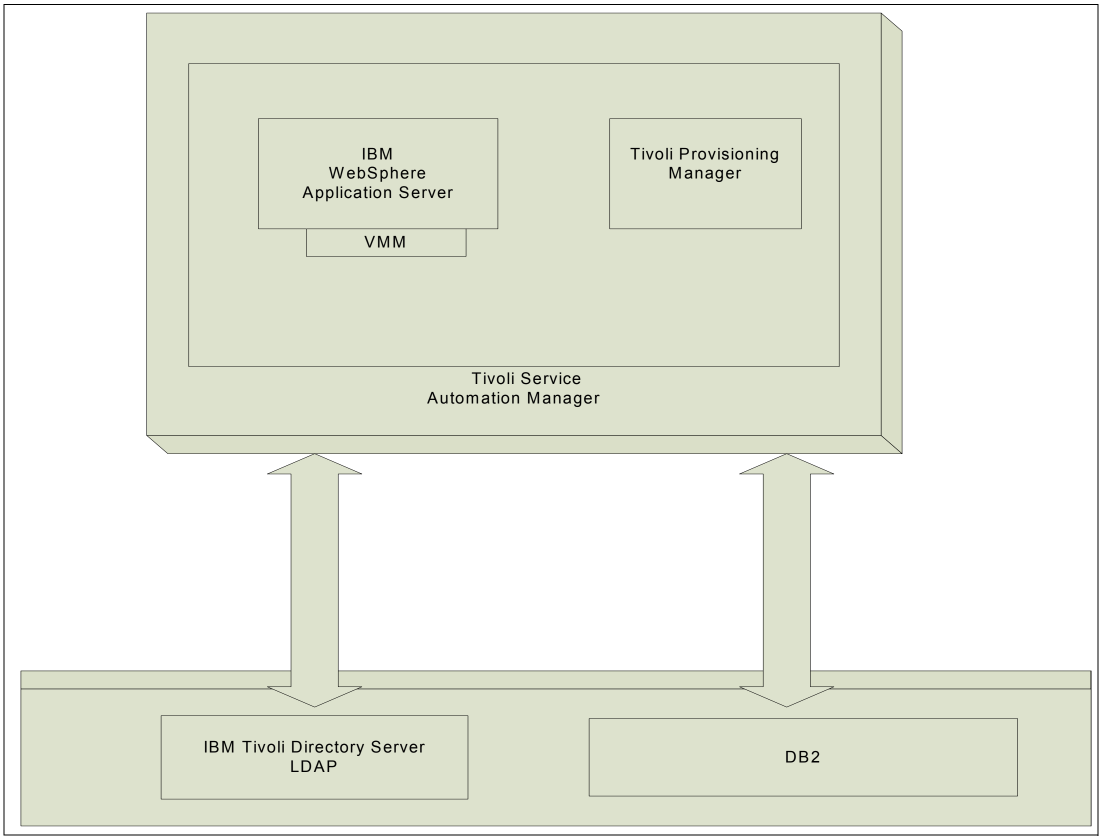


Figure 1-3 Single server with IBM Tivoli Directory Server and DB2

Multiple Tivoli Service Automation Manager instances with centralized remote LDAP server

This deployment pattern involves a centralized IBM Tivoli Directory Server LDAP server with multiple Tivoli Service Automation Manager servers. This deployment allows for centralized management of LDAP user and group credentials across multiple Tivoli Service Automation Manager server instances. This architecture is targeted towards large multi-site deployment patterns with the greatest scalability and flexibility, as shown in Figure 1-4 on page 6. Although the concepts presented in this publication apply to this pattern, it is beyond the scope of the solution that is provided here.

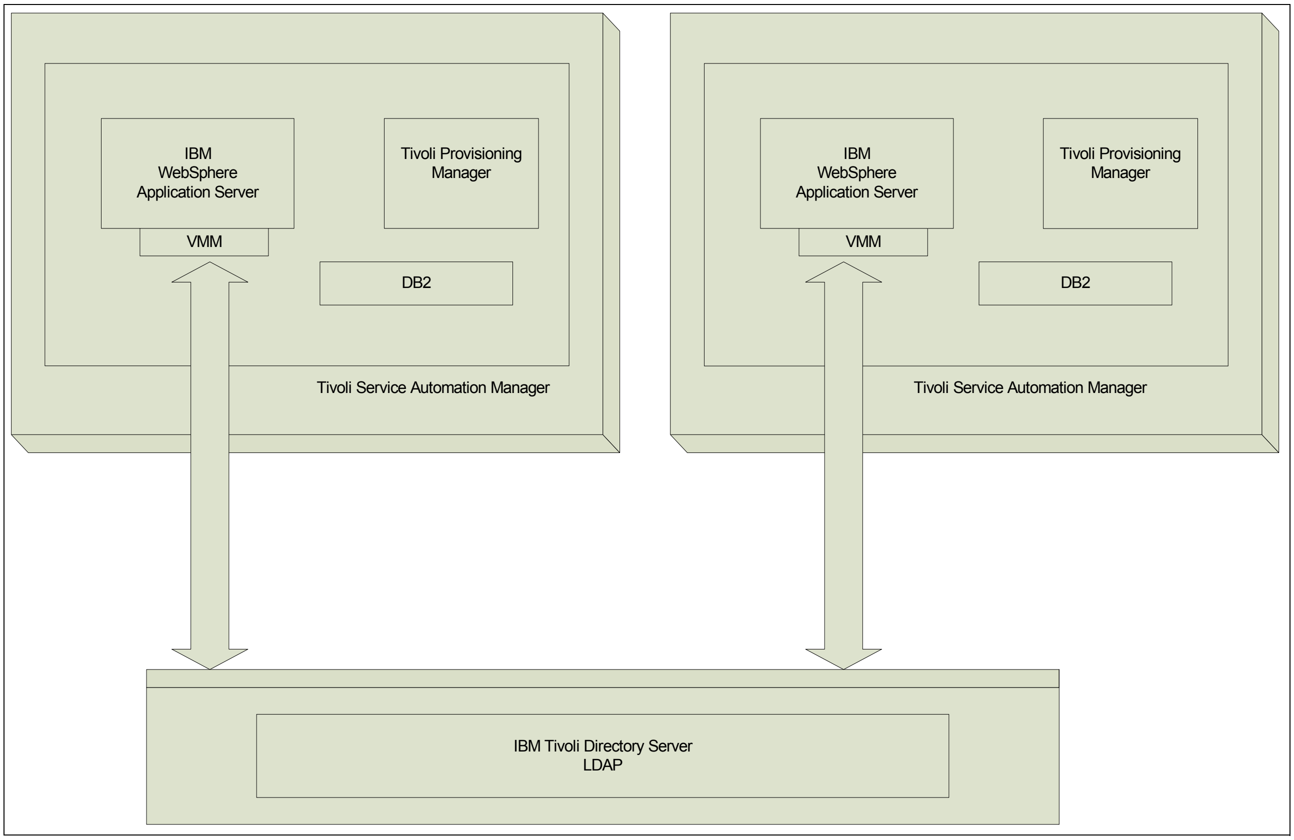


Figure 1-4 Multiple Tivoli Service Automation Manager servers with central LDAP server

1.3 Tivoli Service Automation Manager security overview

Most IT organizations require varying roles for their staff to enable or restrict the features of provisioning infrastructure of Tivoli Service Automation Manager. This manager, which is based on the Maximo security model, provides a wealth of security roles and can be adopted to any organization's requirements. In the IBM SmartCloud enterprise infrastructure, the team had two clear roles: the cloud administrator (CCMPADMIN) and the cloud operator (CCMPOP). The CCMPADMIN requires full access to all of the features of Tivoli Service Automation Manager in a read and write mode. The CCMPOP needs to access the features, but requires only read-only access. For example, the CCMPADMIN role needs to run TPM work flows and monitor work flow results. If the work flow fails, the CCMPADMIN may need to act on the workflow. The CCMPOP may need to view only the work flow execution history under the Maximo user interface.

1.3.1 Security model

For the IBM SmartCloud Enterprise environment, we are using two security groups to demonstrate the roles that are required to support our Tivoli Service Automation Manager configuration. CCMPADMIN and CCMPOP are created under the LDAP distinguished name (dn) ou=groups,ou=SWG,o=IBM,c=US object hierarchy.

CCMPADMIN

CCMPADMIN includes the following features:

- LDAP DN = cn=CCMPADMIN,ou=groups,ou=SWG,o=IBM,c=US
- The equivalent of MAXADMIN who has full admin authority in Tivoli Service Automation Manager

CCMPOP

CCMPOP includes the following features:

- Group that has full read only access to Tivoli Service Automation Manager.
- LDAP DN = cn=CCMPOP,ou=groups,ou=SWG,o=IBM,c=US

Figure 1-5 shows the LDAP distinguished name (dn) hierarchy for this model.

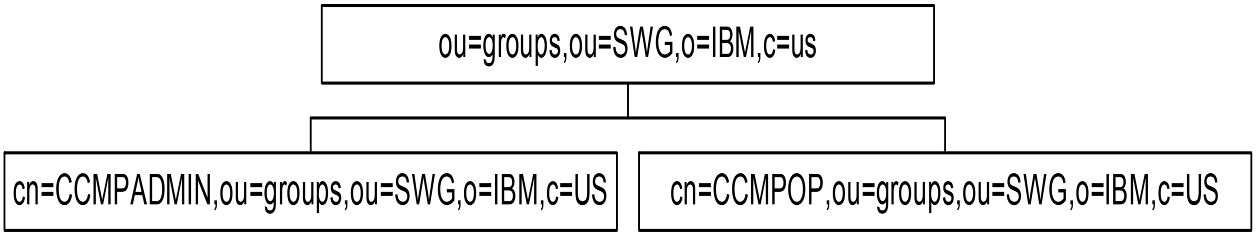

ou=groups,ou=SWG,o=IBM,c=us
cn=CCMPADMIN,ou=groups,ou=SWG,o=IBM,c=US
cn=CCMPOP,ou=groups,ou=SWG,o=IBM,c=US

Figure 1-5 LDAP distinguished name (dn) hierarchy and schema

In our examples, we apply password policies via ACLs to the CCMPADMIN and CCMPOP groups through the cn=group_pwd_policy,cn=ibmPolicies distinguished name.

2

Tivoli Service Automation Manager management server security setup

In this chapter, we describe the process that is used to configure the security policy, including passwords.

2.1 Activating the LDAP policy

Complete the following steps to activate the LDAP policy:

1. Create an LDIF file that is named `activatepolicy.ldif` and contains the following LDAP policies:

   ```
   dn: cn=pwdpolicy,cn=ibmPolicies
   ibm-pwdpolicy:true
   ibm-pwdGroupAndIndividualEnabled:true
   ```

2. Run the following command to apply this policy:

   ```
   /opt/ibm/ldap/V6.2/bin/idsldapmodify -D cn=root -w ? -p  -k –i
   activatepolicy.ldif
   ```

2.2 Adding group password policy to LDAP

Complete the following steps to add the group password policy to LDAP:

1. Create an LDIF file that is named `group_password_policy.ldif` and contains the following LDAP policies:

   ```
   dn:cn=group_pwd_policy,cn=ibmPolicies
   objectclass: container
   objectclass: pwdPolicy
   objectclass: ibm-pwdPolicyExt
   objectclass: top
   cn:group_pwd_policy
   pwdAttribute: userPassword
   ibm-pwdpolicy:true
   pwdInHistory: 8
   pwdCheckSyntax: 2
   pwdMinAge: 86400
   pwdMinLength: 8
   passwordMinOtherChars: 2
   pwdMaxAge: 7776000
   pwdExpireWarning: 604800
   ```

2. Run the following command to apply this policy

   ```
   /opt/ibm/ldap/V6.2/bin/idsldapadd -D cn=root  -w ? -k -i
   group_password_policy.ldif
   ```

2.3 Enable LDAP auditing

Complete the following steps to enable LDAP auditing:

1. Create an LDIF file that is named `ldapaudit.ldif` and contains the following LDAP policies:

   ```
   dn: cn=Audit, cn=Log Management, cn=Configuration
   changetype: modify
   replace: ibm-audit
   ibm-audit: true
   ```

```
replace: ibm-auditadd
ibm-auditadd: false

replace: ibm-auditAttributesonGroupEvalOp
ibm-auditAttributesonGroupEvalOp: false

replace: ibm-auditBind
ibm-auditBind: true

replace: ibm-auditCompare
ibm-auditCompare: false

replace: ibm-auditBind
ibm-auditBind: true

replace: ibm-auditCompare
ibm-auditCompare: false

replace: ibm-auditDelete
ibm-auditDelete: false

replace: ibm-auditExtOp
ibm-auditExtOp: false

replace: ibm-auditExtOPEvent
ibm-auditExtOPEvent: false

replace: ibm-auditFailedOPonly
ibm-auditFailedOPonly: true

replace: ibm-auditGroupsOnGroupControl
ibm-auditGroupsOnGroupControl: false

replace: ibm-auditModify
ibm-auditModify: false

replace: ibm-auditModifyDN
ibm-auditModifyDN: false

replace: ibm-auditSearch
ibm-auditSearch: false

replace: ibm-auditUnbind
ibm-auditUnbind: true
```

2. Run the following command to apply this policy:

```
/opt/ibm/ldap/V6.2/bin/idsldapmodify -D cn=root -w ? -k -i ldapaudit.ldif
```

2.4 Adding group policy to CCMPADMIN group

Complete the following steps to add a group policy to the CCMPADMIN group:

1. Create an LDIF file that is named `applypolicytoadmin.ldif` and contains the following LDAP policies that apply the group policy to the CCMPADMIN group:

   ```
   dn:cn=CCMPADMIN,ou=groups,ou=SWG,o=IBM,c=US
   changetype:modify
   add:ibm-pwdGroupPolicyDN
   ibm-pwdGroupPolicyDN:cn=group_pwd_policy,cn=ibmPolicies
   ```

2. Run the following command to apply this policy:

   ```
   /opt/ibm/ldap/V6.2/bin/idsldapmodify -D cn=root -w ? -k -i
   applypolicytoadmin.ldif
   ```

2.5 Adding group policy to CCMPOP group

Complete the following steps to add a group policy to the CCMPOP group:

1. Create an LDIF file that is named `applypolicytooperator.ldif` and contains the following LDAP ACL that applies the group policy to the CCMPOP group:

   ```
   dn:cn=CCMPOP,ou=groups,ou=SWG,o=IBM,c=US
   changetype:modify
   add:ibm-pwdGroupPolicyDN
   ibm-pwdGroupPolicyDN:cn=group_pwd_policy,cn=ibmPolicies
   ```

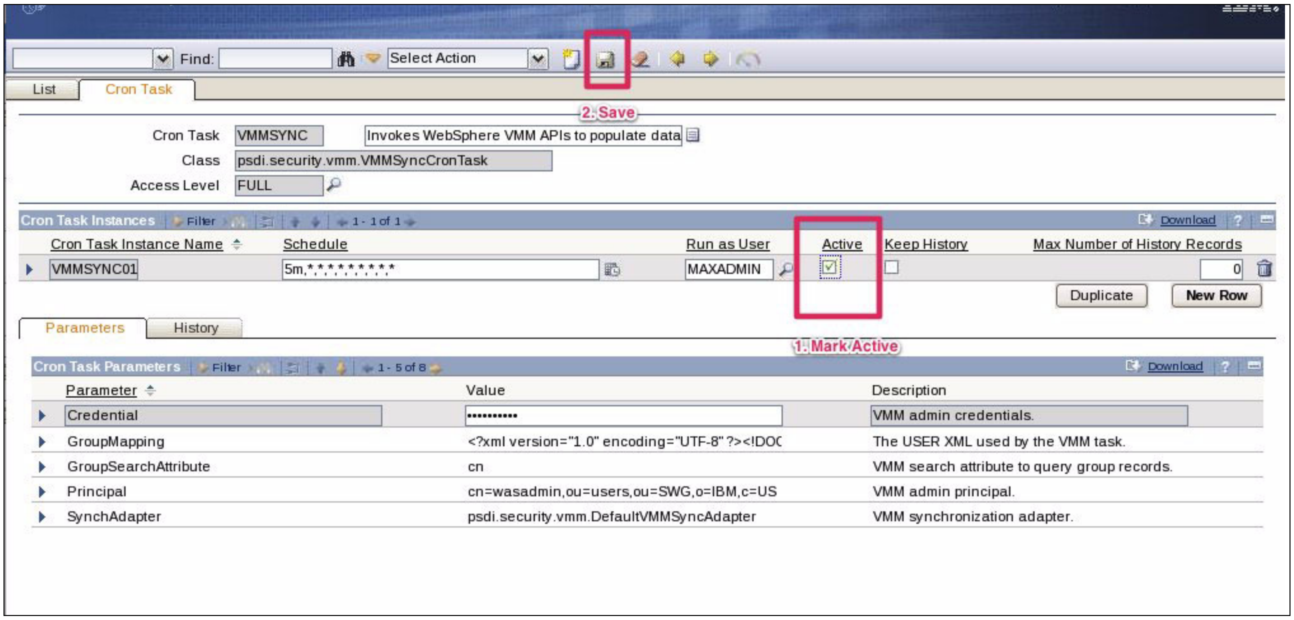
2. Run the following command to apply this policy:

   ```
   /opt/ibm/ldap/V6.2/bin/idsldapmodify -D cn=root -w ? -k -i
   applypolicytooperator.ldif
   ```

2.6 Activating the Cron task for VMMSync

Complete the following steps to activate the Cron Task for VMMSync:

1. Open the Maximo interface in a web browser and use the IP address of the Tivoli Service Automation Manager Management Server where security is configured.
2. Click **System Configuration** → **Platform Configuration** → **Cron Task Setup**.
3. Locate VMMSync Cron Task by searching in the Filter.
4. Enable the VMMSync Cron tab job in Maximo, as shown in Figure 2-1 on page 13.



2. Save

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

Cron Task Instances

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

1. Mark Active

Cron Task Parameters

Parameter	Value	Description
Credential	••••••••••	VMM admin credentials.
GroupMapping	<?xml version="1.0" encoding="UTF-8" ?><!DOC	The USER XML used by the VMM task.
GroupSearchAttribute	cn	VMM search attribute to query group records.
Principal	cn=wasadmin,ou=users,ou=SWG,o=IBM,c=US	VMM admin principal.
SynchAdapter	psdi.security.vmm.DefaultVMMSyncAdapter	VMM synchronization adapter.

Figure 2-1 Enabling the VMMSync Cron tab job

5. In the Cron Task Instances section, click **Active**, as shown in Figure 2-1.
6. Click the Save icon, as shown in Figure 2-1.

2.7 Setting password policy

Complete the following steps to set the password policy:

1. Create an LDIF file that is named `pwdpolicy.ldif` and contains the following LDAP policies:

```
dn: o=IBM,c=US
changetype: modify
replace: aclentry
aclentry: group:CN=ANYBODY:normal:rsc:system:rsc:restricted:rsc

add: aclentry
aclentry:
access-id:CN=THIS:normal:rsc:system:rsc:restricted:rsc:at.userPassword:rwsc
```

2. Run the following command to apply this policy:

```
/opt/ibm/ldap/V6.2/bin/idsldapmodify -D cn=root -w ? -k -i pwdpolicy.ldif
```

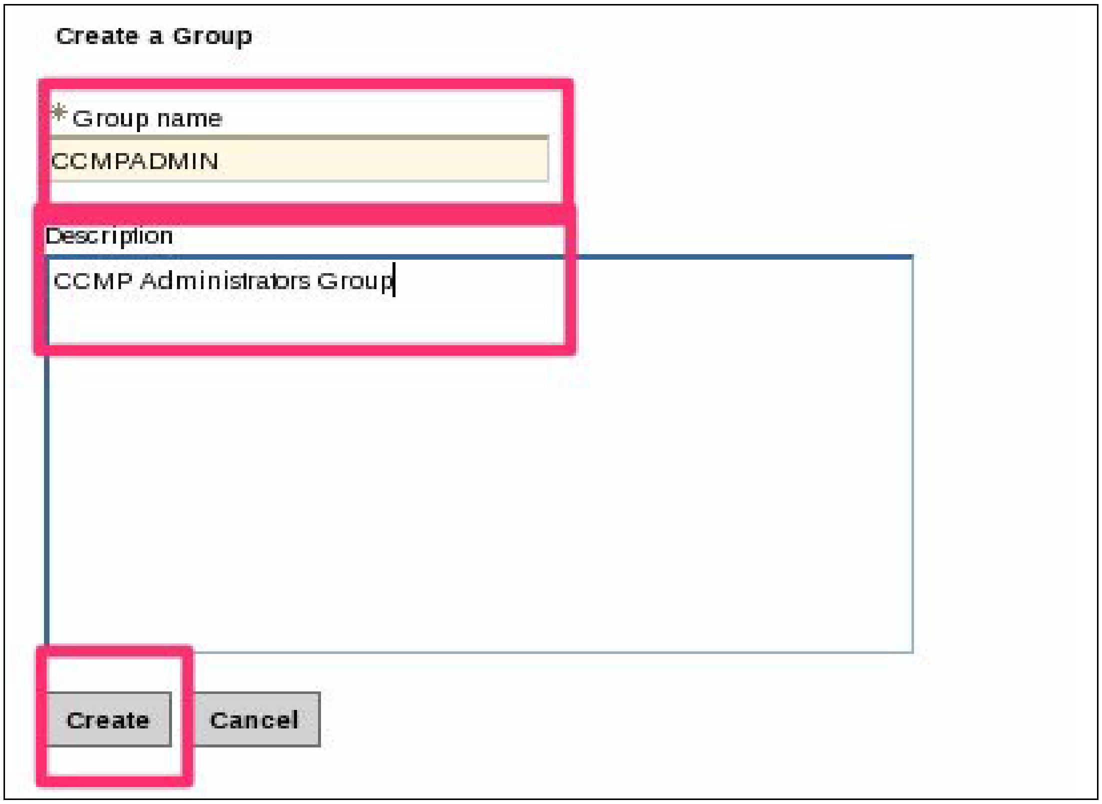
2.8 Creating the CCMPADMIN security group

Complete the following steps to create the CCMPADMIN security group in WebSphere Application Server:

1. Log in to the WebSphere Application Server console by using the WebSphere Application Server administrative ID and password at this website:

   `https://TSAM_SERVER_IP:9043/ibm/console/logon.jsp`

2. Open the **Users and Groups** → **Manage Groups** task.
3. Click **Create**.
4. In the **Create a Group** window, enter the following parameters:
   - Group Name: **CCMPADMIN**
   - Description: **CCMP Administrator Group**
5. Click **Create**, as shown in Figure 2-2.



Create a Group

*Group name

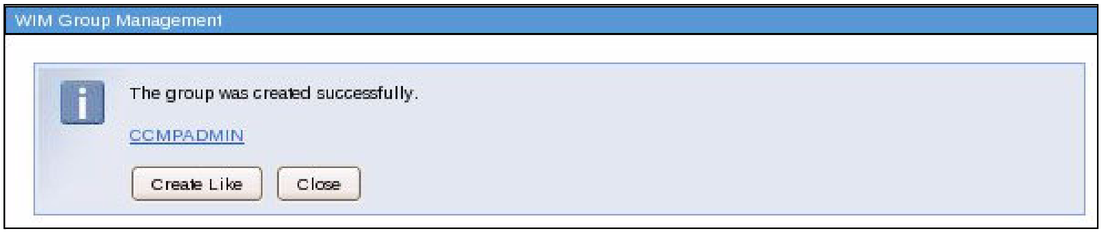
CCMPADMIN

Description

CCMP Administrators Group

Figure 2-2 Creating a group

6. A message is shown that indicates the group was created, as shown in Figure 2-3 on page 15. Click **Close**. Log out of WebSphere Application Server.



The group was created successfully.

CCMPADMIN

Figure 2-3 Successful creation message

It might take up to 5 minutes for the VMMSync cron task job to transfer the new group to Maximo.

2.9 Applying the password policy to the CCMPADMIN group

Apply the password policy to the CCMPADMIN group by creating an LDIF file that is named `applypolicytoadmin.ldif` and contains the following LDAP policies:

```
dn:cn=CCMPADMIN,ou=groups,ou=SWG,o=IBM,c=US
changetype:modify
add:ibm-pwdGroupPolicyDN
ibm-pwdGroupPolicyDN:cn=group_pwd_policy,cn=ibmPolicies
```

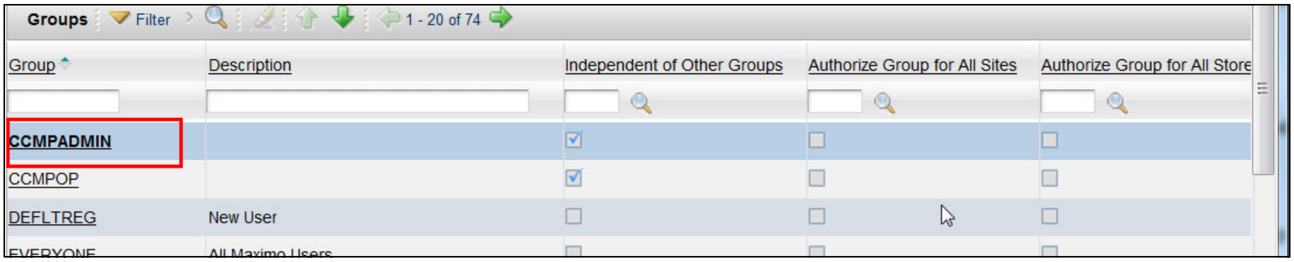
2.10 Configuring the CCMPAdmin group in Maximo

Complete the following steps to configure the CCMPAdmin group in Maximo (it might take up to 5 minutes for the VMMSync cron tab task to replicate the VMM contents from WebSphere Application Server to Maximo):

1. Log in to Maximo as **maxadmin** at this website:

   `https://TSAM_SERVER_IP:9043/ibm/console/logon.jsp`

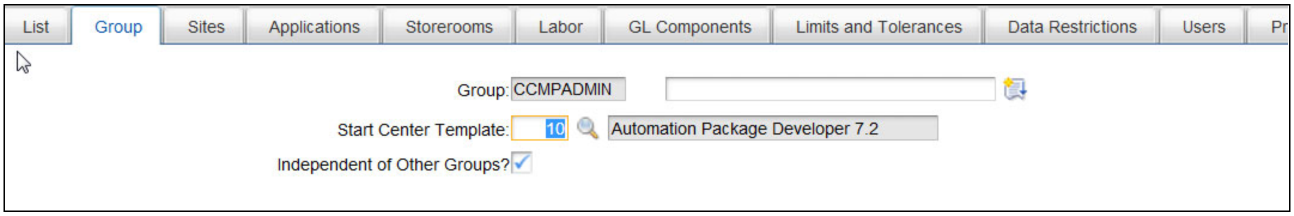
2. Click **Goto** → **Security** → **Security Groups**.
3. The list of Groups is displayed. Select the **CCMPADMIN** group, as shown in Figure 2-4.



Group	Description	Independent of Other Groups	Authorize Group for All Sites	Authorize Group for All Store
CCMPADMIN		☑	□	□
CCMPOP		☑	□	□
DEFLTREG	New User	□	□	□
EVERYONE	All Maximo Users	□	□	□

Figure 2-4 Selecting the CCMPADMIN group

4. Click the **Group** tab, as shown in Figure 2-5 on page 16.



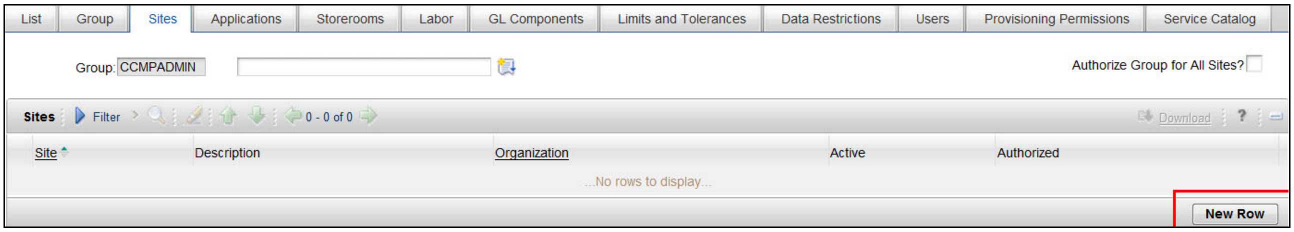
Group: CCMPADMIN

Start Center Template: 10 Automation Package Developer 7.2

Independent of Other Groups? ☑

Figure 2-5 Selecting the group tab

5. Enter the following values for the CCMPADMIN Group:
   - Start Center Template: 10
   - Independent of Other Groups: Y
6. Click the **Sites** tab and click **New Row** to add the default insert site, as shown in Figure 2-6.



Group: CCMPADMIN

Authorize Group for All Sites? □

Site	Description	Organization	Active	Authorized

...No rows to display...

Figure 2-6 Clicking the Sites tab and the New Row box

7. Click the search icon next to the site input box, as shown in Figure 2-7.

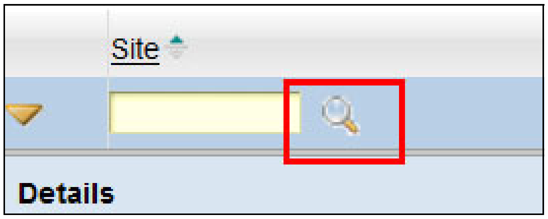
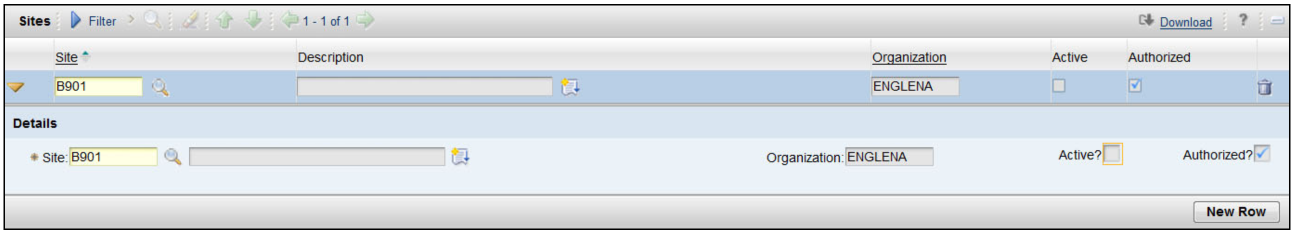


Figure 2-7 Clicking the search icon

8. From the Site list, select the site that you defined during your installation of Tivoli Service Automation Manager, as shown in Figure 2-8.



Site	Description	Organization	Active	Authorized
B901		ENGLENA	□	☑

Site: B901 Organization: ENGLENA Active? □ Authorized? ☑

Figure 2-8 Selecting your site

9. Click the Save icon to save your changes.

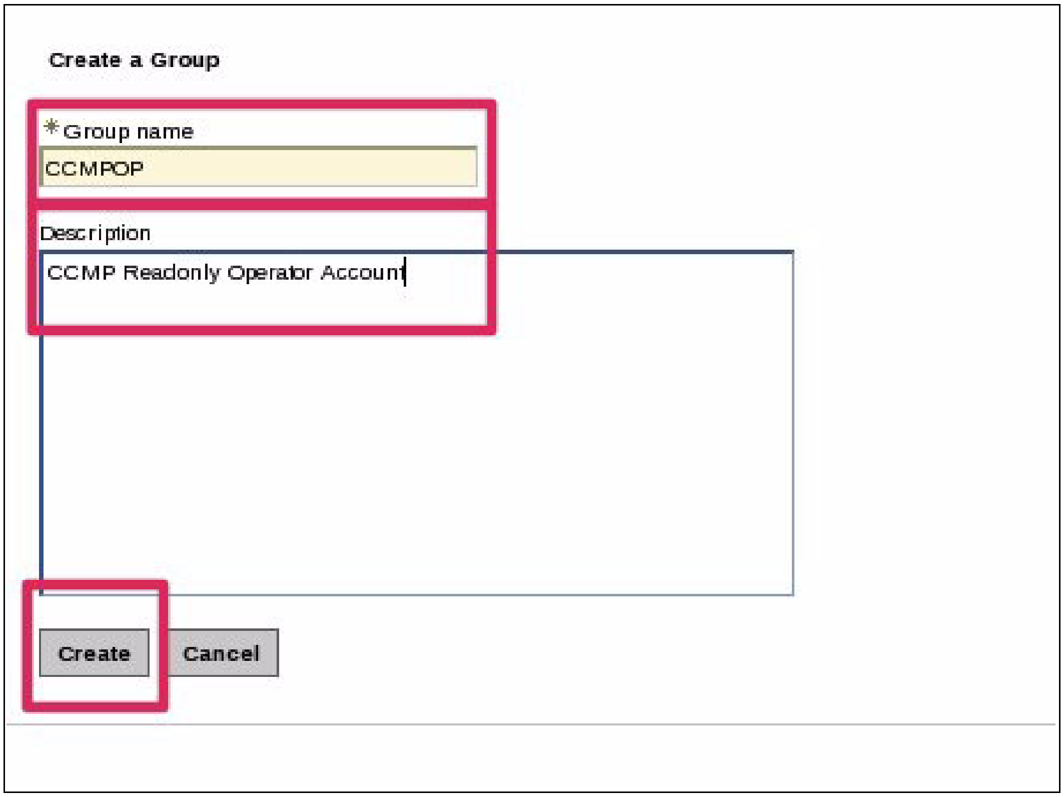
2.11 Creating the CCMPOP Security Group in WebSphere Application Server

Complete the following steps to create the CCMPOP Security Group in WebSphere Application Server:

1. Log in to the WebSphere Application Server console by using a WebSphere Application Server administrative ID and password at this website:

   `https://TSAM_SERVER:9043/ibm/console/logon.jsp`

2. Click **Users and Groups** → **Manage Groups**.
3. Click **Create**.
4. Enter the following parameters in the **Create a Group** window, as shown in Figure 2-9:
   - Group Name: CCMPOP
   - Description: CCMP Operator Group



Create a Group

*Group name: CCMPOP

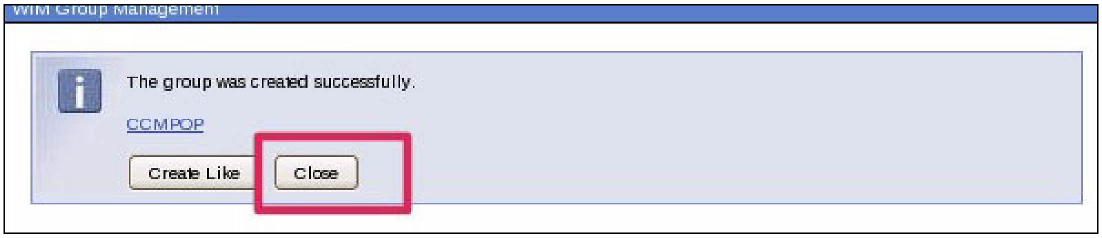
Description: CCMP Readonly Operator Account

Figure 2-9 Enter the group name

5. Click **Create**.

   A message appears that indicates the group was created.

6. Click **Close**, as shown in Figure 2-10 on page 18. Log out of WebSphere Application Server.



The group was created successfully.

CCMPOP

Figure 2-10 Successful creation message

7. You must wait up to 5 minutes for the VMMSync cron task job to transfer the new group to Maximo.

2.12 Applying the password policy to the CCMPOP group

Complete the following steps to apply the password policy to the CCMPOP group:

1. Create an LDIF file named `applypolicytooperator.ldif` that contains the following LDAP policies:

```
dn:cn=CCMPOPER,ou=groups,ou=SWG,o=IBM,c=US
changetype:modify
add:ibm-pwdGroupPolicyDN
ibm-pwdGroupPolicyDN:cn=group_pwd_policy,cn=ibmPolicies
```

2. Run the following command to apply this policy:

```
/opt/ibm/ldap/V6.2/bin/idsldapmodify -D cn=root -w ? -k
-applypolicytooperator.ldif
```

2.13 Configuring the CCMPOP Group in Maximo

Complete the following steps to configure the CCMPOP group in Maximo (it might take up to 5 minutes for the VMMSync cron tab task to replicate the VMM contents from WebSphere Application Server to Maximo):

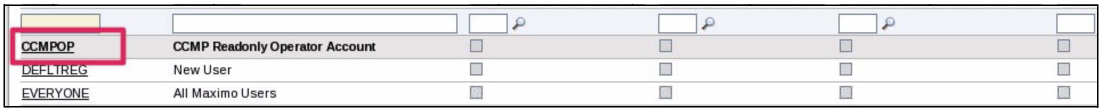
1. Log in to Maximo as **maxadmin** at this website:

   `https://TSAM_SERVER_IP:9043/ibm/console/logon.jsp`

2. Select **Goto** → **Security** → **Security Groups**.

   The list of Groups is displayed.

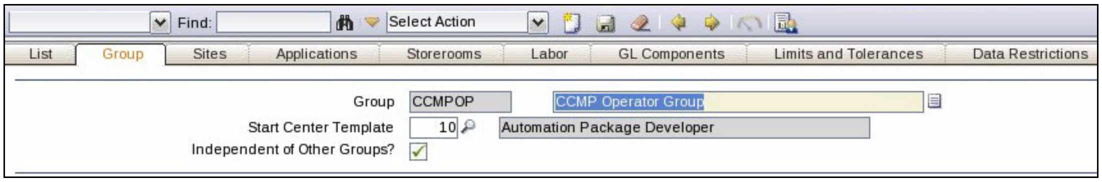
3. Click the **CCMPOP** group, as shown in Figure 2-11.



CCMPOP	CCMP Readonly Operator Account	□	□	□	□
DEFLTREG	New User	□	□	□	□
EVERYONE	All Maximo Users	□	□	□	□

Figure 2-11 Select the CCMPOP group

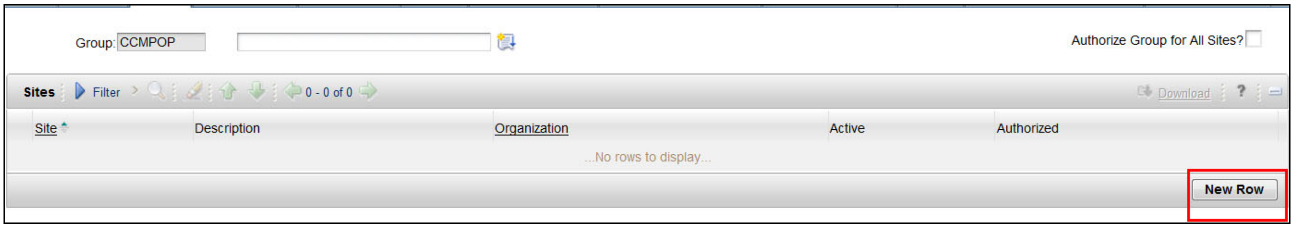
4. Click the **Group** tab, as shown in Figure 2-12 on page 19.



Group: CCMPOP — CCMP Operator Group
Start Center Template: 10 — Automation Package Developer
Independent of Other Groups? ☑

Figure 2-12 Select the group tab

5. Enter the following values for the CCMPOP Group:
   - Start Center Template: 10
   - Independent of Other Groups: Y
6. Click the **Sites** tab then click **New Row** to add the default insert site, as shown in Figure 2-13.



Group: CCMPOP
Authorize Group for All Sites? □

Site	Description	Organization	Active	Authorized

...No rows to display...

Figure 2-13 Selecting Sites tab and New Row button

7. Click the search icon that is next to the site input box, as shown in Figure 2-14.

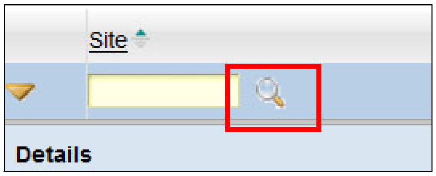
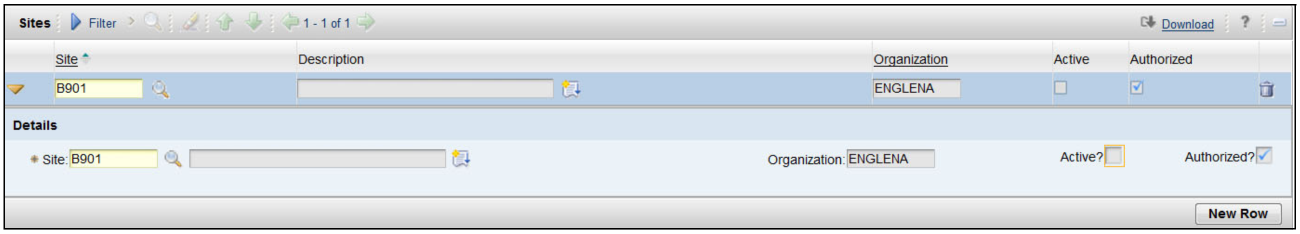


Figure 2-14 Select the search icon

8. From the Site list, select the site that you defined during your installation of Tivoli Service Automation Manager, as shown in Figure 2-15.



Site	Description	Organization	Active	Authorized
B901		ENGLENA	□	☑

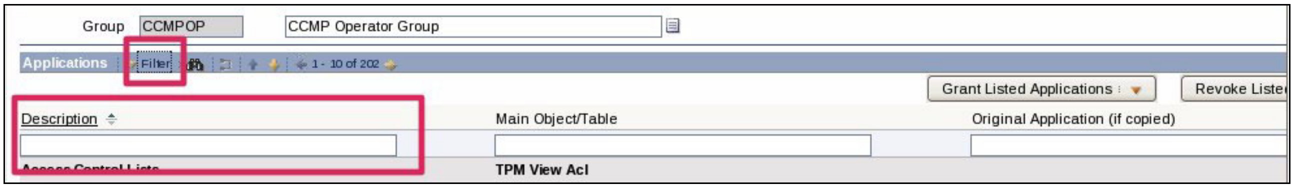
Site: B901
Organization: ENGLENA
Active? □
Authorized? ☑

Figure 2-15 Select your site

9. Click the Save icon to save your changes.

10. Click the **Applications** tab.

11. Click **Filter** to enter find the application names quickly, as shown in Figure 2-16.



Group: CCMPOP — CCMP Operator Group

Applications — 1 - 10 of 202

Figure 2-16 Select Filter

Table 2-1 lists all of the applications in Tivoli Service Automation Manager and their associated security settings, which are used to create the CCMPOP role.

Table 2-1 Application security settings

Application name	**Security setting**
Provisioning Workflow status	- Read Access to Workflow Status - Export - Refresh
Service Requests	Read Access to Service Requests
Provisioning Computers	Read Access to Computers
Service Deployment Instance	Read Access to Service Deployment Instances
Resource Allocation for Service Deployment Instances	- Read Access to Resource Allocation for Service Deployment Instances - View Workflow Assignments - View Workflow History
View Service Requests	Read Access to View Service Requests
Provisioning Task Tracking	Read Access to Tasks
Provisioning Workflows	Read Access to Workflows
View Catalog requests	- READ - Show Catalog Order Status History tab - Status
Subnetworks	Read Access to Subnetwork
Resource Pools	Read Access to Resource Pool
Favorite Applications Setup	Read/Modify access to Favorite Application Setup
Inbox/Assignments Setup	Read/Modify access to Inbox Assignment
KPI Graph Setup	Read/Modify access to the KPI Graph Setup
Images	Read Access to TPIMAGE
IT Topology Work Order	- Read Access to Work Order Tracking - New Work Order - Apply Route - Save Work Order
Escalations	Read Access to Escalation Application
KPI List Setup	Read Modify Access to KPI List Setup
Result Set Setup	Read Modify Access to Results Set Setup
Quick Insert Setup	Read Modify Access to Quick Insert Setup
Layout and Configuration	Read Modify Access to Layout and Configuration
Start Center Bulletin Board	- Read/Modify access to the Start Center - Can Update Start Center - Default Information - Personal Information

12. The following portlets can be hidden by using a security setting to Hide Portlet (ensure that the Hide Portlet is not selected):

    - Favorite Applications Setup
    - Inbox/Assignments Setup
    - KPI Graph Setup
    - KPI List Setup
    - Result Set Setup
    - Quick Insert Setup

13. Click **Save** to save the group changes.

2.14 Deactivating the LDAP password policies

Complete the following steps to de-active the LDAP password policies:

1. Create an LDIF file that is named `deactivatepolicy.ldif` and contains the following LDAP policies:

   ```
   deactivatepolicy.ldif
   dn: cn=pwdpolicy,cn=ibmPolicies
   ibm-pwdpolicy:false
   ibm-pwdGroupAndIndividualEnabled:false
   ```

2. Run the following command to apply this policy:

   ```
   /opt/ibm/ldap/V6.2/bin/idsldapmodify -D cn=root -w ? -k -deactivatepolicy.ldif
   ```

3

Maximo Identification management

In this chapter, some of the common tasks that are used to administer Maximo user identifications (IDs) are described.

3.1 Creating a Maximo admin account ID

Complete the following steps to create a Tivoli Service Automation Manager Maximo administrator ID for a user:

1. Log in to the Tivoli Service Automation Manager Management server as **tioadmin**.
2. Change the directory (by using the `cd` command) to the `/home/tioadmin/scripts/security` directory.
3. Run the `addmaxoper.sh` script to create the `joesmith` account. (For an example of this script, see Chapter 5, “Sample scripts” on page 43). Use the following syntax to run the script:

   ```
   usage: addmaxadmin.sh -w ldap_bind_password -u user_name -F first_name -L
   last_name -p password -e email
   ```

   For example:

   ```
   ./ usage: addadmin.sh: -w <LDAP_PASSWORD> -u joesmith -F Joe -L Smith -p
   joespassword -e joesmith@us.ibm.com
   ```

   Important: Ensure that each user has a unique email address specified. Otherwise, VMMSync will not synchronize the email addresses.

4. After the Maximo administrator ID is created, you might have to wait up to 5 minutes for the VMMSync cron tab task to run and synchronize the LDAP contents between WebSphere Application Server and Maximo.
5. Add the WebSphere Application Server administrator role to the Tivoli Service Automation Manager Maximo administration account section.
6. Grant the User Access to Inbox Content section by using the new ID and next available sequence number.

Adding the WebSphere Application Server administrator role to the Tivoli Service Automation Manager Maximo Administration account

After the user is added in Maximo, we must provide the user with the WebSphere Application Server administrative role. We show two methods for adding the WebSphere administrative role to the Maximo administrator and the command line and via the WebSphere Integrated Services Console (ISC).

Adding the WebSphere Application Server administrator role: Command line

Complete the following steps to add the WebSphere Application Server administrator role to the Tivoli Service Automation Manager Maximo Administrator account by using the command line:

1. Log in to the Tivoli Service Automation Manager Management server as **tioadmin**.
2. Change the directory (cd) to the `/home/tioadmin/scripts/security` directory.
3. Run the `addwasadmin.sh` script to add the Maximo Administrator to the WebSphere Application Server administrative role. (For an example of this script, see Chapter 5, “Sample scripts” on page 43). Use the following syntax to run this script:

   ```
   usage:addwasadmin.sh  usage: addwasadmin.sh: -u user_name -[s] [-a wasdamin_id]
   [-p wasadmin_pwd]
   ```

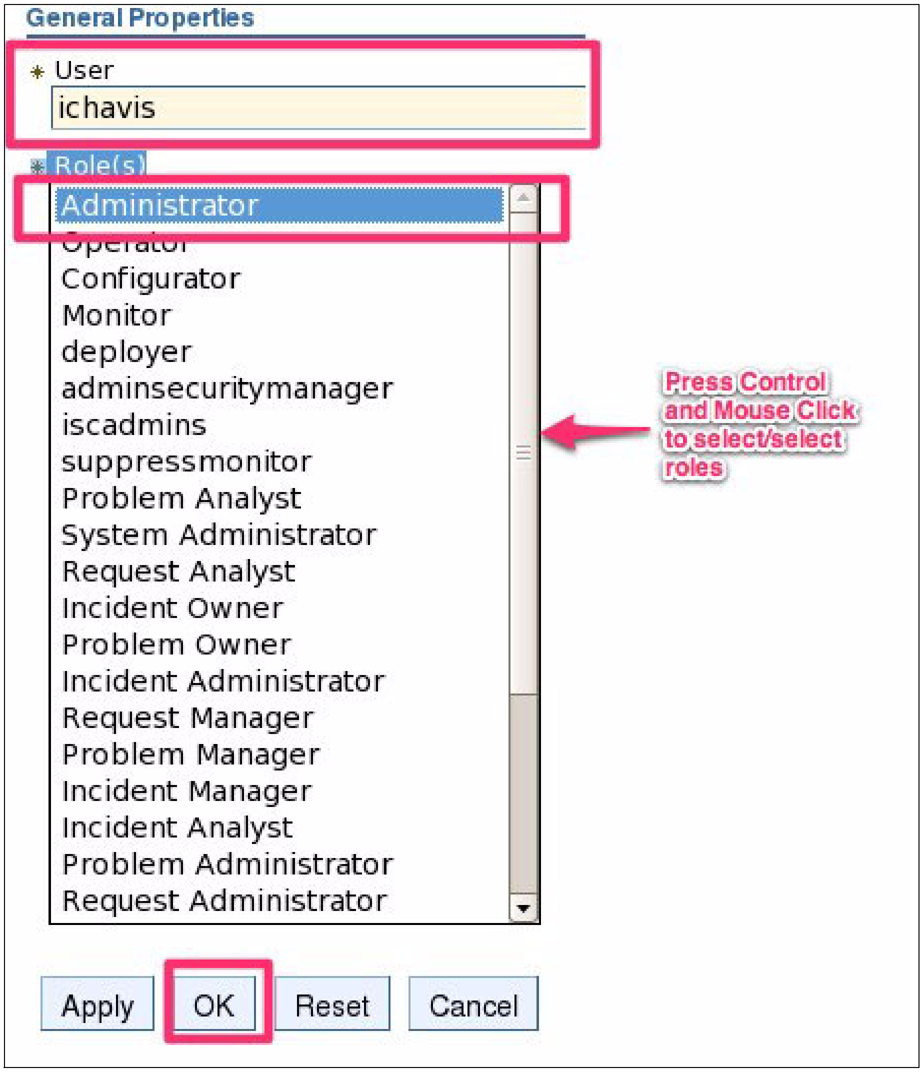
Adding the WebSphere Application Server administrator role: Integrated services console

Complete the following steps to add the WebSphere Application Server administrator role to the Tivoli Service Automation Manager Maximo Administrator account by using the WebSphere Integrated Services Console (ISC):

1. Open the WebSphere ISC by using the following site URL (include the Tivoli Service Automation Manager servers IP address in the actual URL):

   ```
   https://TSAM_SERVER:9043/ibm/console/logon.jsp
   ```

2. Log in to the WebSphere Application Server ISC by using the user ID that has WebSphere administrative rights.
3. Select **System and Groups** → **Administrative User Role**.
4. Click **Add**.
5. Click **Administrative User Role Screen** → **User Screen**.
6. Enter the following user information:
   - User: user ID added
   - Roles: Add the following roles by pressing Ctrl+Left Mouse button (see Figure 3-1 on page 26):
     - Administrator
     - adminsecuritymanager (grant this role to ID and security administrators only)



General Properties

* User

ichavis

* Role(s)

- Administrator
- Operator
- Configurator
- Monitor
- deployer
- adminsecuritymanager
- iscadmins
- suppressmonitor
- Problem Analyst
- System Administrator
- Request Analyst
- Incident Owner
- Problem Owner
- Incident Administrator
- Request Manager
- Problem Manager
- Incident Manager
- Incident Analyst
- Problem Administrator
- Request Administrator

Press Control and Mouse Click to select/select roles

Figure 3-1 Adding roles

7. Click **OK**.
8. To permanently save these changes, select the **Save directly to the master configuration** option.
9. Repeat these steps for all of the Maximo administrator IDs that need to be granted the WebSphere Application Server administrative role.

3.2 Creating a Tivoli Service Automation Manager operator account ID

Complete the following steps to create a Tivoli Service Automation Manager Operator account `tsamoper`:

1. Log in to the Tivoli Service Automation Manager Management server as **tioadmin**.
2. Change the directory (cd) to the `/home/tioadmin/scripts/security` directory.
3. Run the `addmaxoper.sh` script to create the TSAMOPER account by using the following syntax (for an example of this script, see Chapter 5, “Sample scripts” on page 43):

   ```
   usage: addmaxoper.sh: -w ldap_bind_password -u user_name -F first_name -L
   last_name -p password -e email
   ```

   For example:

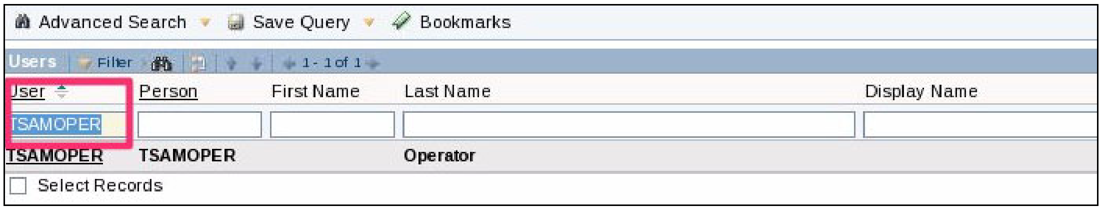
   ```
   ./ usage: addmaxoper.sh: -w <LDAP_PASSWORD> -u tsamoper -F TSAM -L Operator -p
   tsamoper -e tsamoper@void.com

   Adding:tsamoper to LDAP
   Operation 0 adding new entry uid=tsamoper,ou=users,ou=SWG,o=IBM,c=US
   Adding:tsamoper to MAXIMOUSERS LDAP Group
   Operation 0 modifying entry cn=MAXIMOUSERS,ou=groups,ou=SWG,o=IBM,c=US
   Adding:tsamoper to CCMPOP LDAP Group
   Operation 0 modifying entry cn=CCMPOP,ou=groups,ou=SWG,o=IBM,c=US
   ```

   In this example, we use an invalid email because the user does not have a valid email address. You must ensure that each user has a unique email address that is specified or VMMSync will not synchronize the email addresses.
4. After the `tsamoper` ID is created, you may have to wait for up to 5 minutes for the VMMSync cron tab task to run and synchronize the LDAP contents between WebSphere Application Server and Maximo.

3.3 Customizing the Tivoli Service Automation Manager OPER user

1. After waiting up to 5 minutes after the tsamoper account is created, log in to Maximo by using the maxadmin account.
2. From the Maximo Start Center, select **Goto** → **Security** → **Users**.
3. Find the new `tsamoper` account by entering **tsamoper** in the User field and clicking **Enter**, as shown in Figure 3-2.



User	Person	First Name	Last Name	Display Name
TSAMOPER				
TSAMOPER	TSAMOPER		Operator	

Figure 3-2 Finding teamoper

4. Click the **tsamoper** account.

5. Set the following parameters:
   - Display Name: TSAM Operator
   - Default Insert Site: PMSCRTP
   - Storeroom Site for Self-Service Requisitions: PMSCRTP
6. Click the **Save** icon to save the settings.
7. Log off and log back in to Maximo before you continue. Logging out of Maximo requires that you close all of your browser windows.

3.4 Customizing the TSAMOPER start center

After the tamoper account has been created, we must customize the Maximo Start Center to build the proper list of favorite applications and portlets. Complete the following steps to customize the Maximo Start Center:

1. After waiting up to 5 minutes after the `tsamoper` account has been created, log in to Maximo by using the **tsamoper** user ID and **tsamoper** password.
2. The Maximo Start Center window opens. First, we build the list of Favorite applications by clicking the small pencil icon on the Favorite Applications portlet (**Automation Development Applications**) title bar, as shown in Figure 3-3.

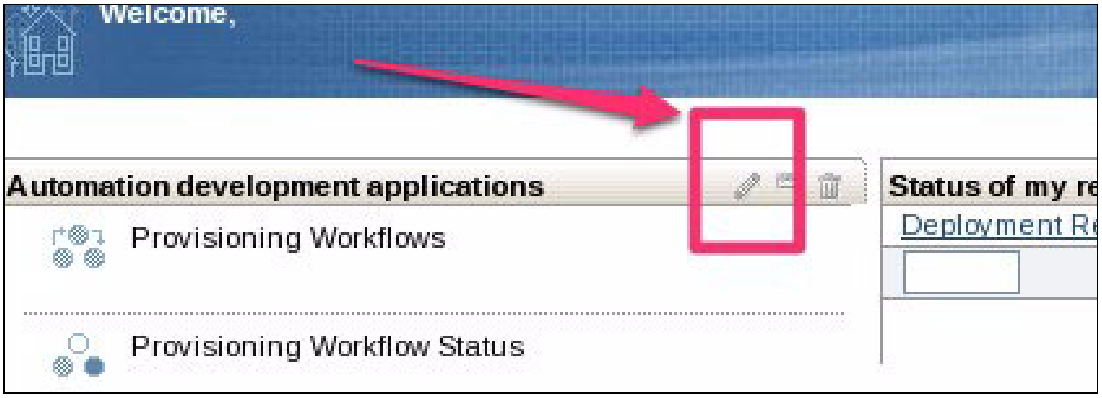

Welcome,
Automation development applications
Provisioning Workflows
Provisioning Workflow Status
Status of my re
Deployment Re

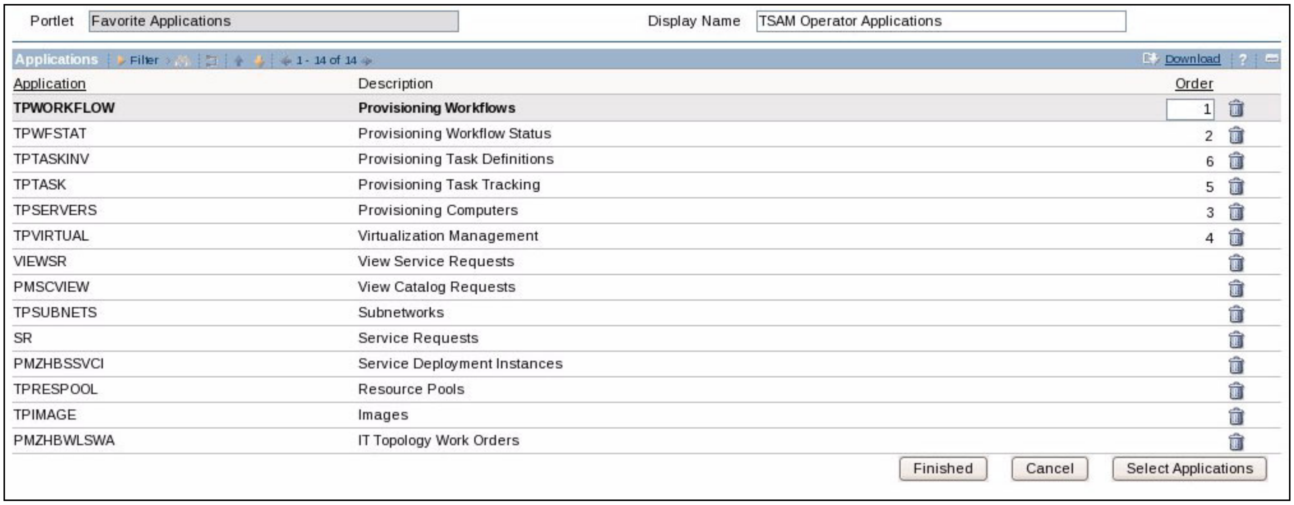
Figure 3-3 Building a list of favorite applications

3. Click **Select Applications** on the lower, left corner of the window. The Select Application list is shown. From the list of applications, select the check box for the following applications (you may need to scroll through several pages of choices to see all of the available applications):
   - Provisioning Workflows
   - Provisioning Workflow Status
   - Provisioning Task Definitions
   - Provisioning Task Tracking
   - Provisioning Computers
   - Virtualization Management
   - View Service Requests
   - View Catalog Requests
   - Sub Networks
   - Service Requests
   - Service Deployment Instances
   - Resource Pools
   - Images

- IT Topology Work Orders

When all of the applications are selected, click **OK**.

4. The **Favorite Application** setup window now includes the list of selected applications, as shown in Figure 3-4.

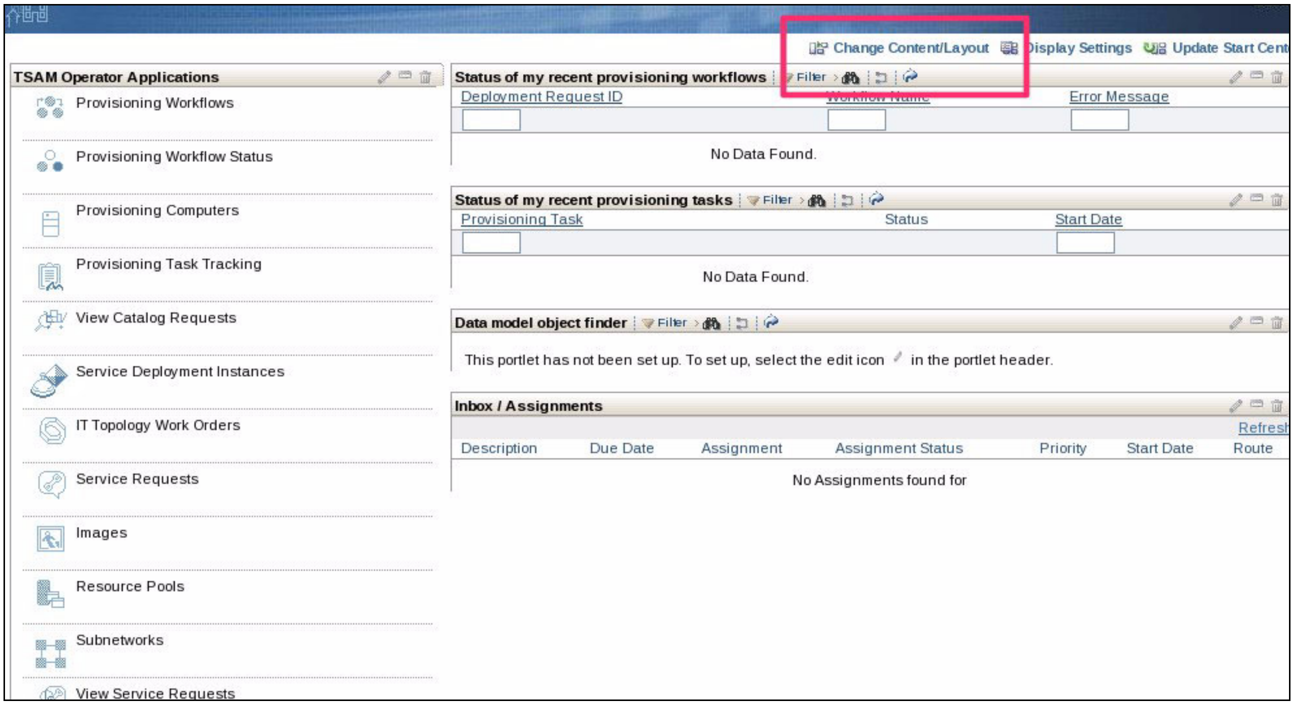


Portlet: Favorite Applications   Display Name: TSAM Operator Applications

Application	Description	Order
TPWORKFLOW	Provisioning Workflows	1
TPWFSTAT	Provisioning Workflow Status	2
TPTASKINV	Provisioning Task Definitions	6
TPTASK	Provisioning Task Tracking	5
TPSERVERS	Provisioning Computers	3
TPVIRTUAL	Virtualization Management	4
VIEWSR	View Service Requests	
PMSCVIEW	View Catalog Requests	
TPSUBNETS	Subnetworks	
SR	Service Requests	
PMZHBSSVCI	Service Deployment Instances	
TPRESPOOL	Resource Pools	
TPIMAGE	Images	
PMZHBWLSWA	IT Topology Work Orders	

Figure 3-4 List of favorite applications

5. Set the Favorite Application title to **TSAM Operator Applications**. Click **Finish** to complete the Favorite Application setup.
6. The updated Maximo Start Center that shows the new Favorite Applications is displayed.
7. Next, we need to change the Start Center layout to include the Inbox/Assignments to the portlet. On the Start Center, click **Change Content/Layout**, as shown in Figure 3-5.



TSAM Operator Applications
- Provisioning Workflows
- Provisioning Workflow Status
- Provisioning Computers
- Provisioning Task Tracking
- View Catalog Requests
- Service Deployment Instances
- IT Topology Work Orders
- Service Requests
- Images
- Resource Pools
- Subnetworks
- View Service Requests

Status of my recent provisioning workflows

Deployment Request ID	Workflow Name	Error Message

No Data Found.

Status of my recent provisioning tasks

Provisioning Task	Status	Start Date

No Data Found.

Data model object finder

This portlet has not been set up. To set up, select the edit icon in the portlet header.

Inbox / Assignments

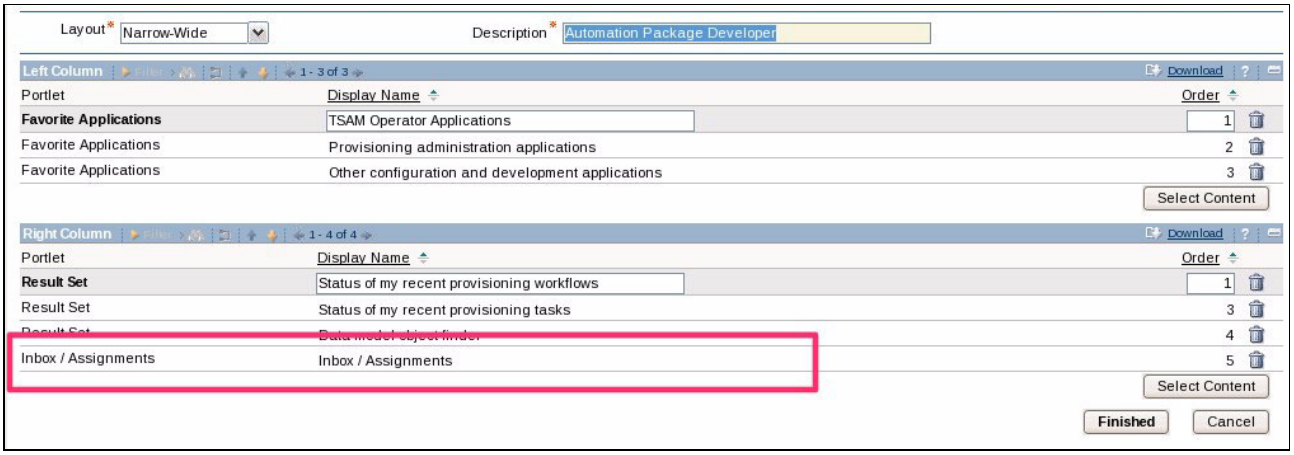
Description	Due Date	Assignment	Assignment Status	Priority	Start Date	Route

No Assignments found for

Figure 3-5 Changing the layout

8. The Layout and Configuration window opens. Click **Select Content** for the Right Column that is in the lower left part of the window.

9. Select **Inbox/Assignments** from the list of Available Portlets by selecting the check box next to the portlet name, as shown in Figure 3-6. You have to scroll though the pages of available portlets to find this portlet. Click **OK**.



Layout* Narrow-Wide

Description* Automation Package Developer

Left Column 1 - 3 of 3 Download

Portlet	Display Name	Order
Favorite Applications	TSAM Operator Applications	1
Favorite Applications	Provisioning administration applications	2
Favorite Applications	Other configuration and development applications	3

Select Content

Right Column 1 - 4 of 4 Download

Portlet	Display Name	Order
Result Set	Status of my recent provisioning workflows	1
Result Set	Status of my recent provisioning tasks	3
Result Set	Data model object finder	4
Inbox / Assignments	Inbox / Assignments	5

Select Content

Finished Cancel

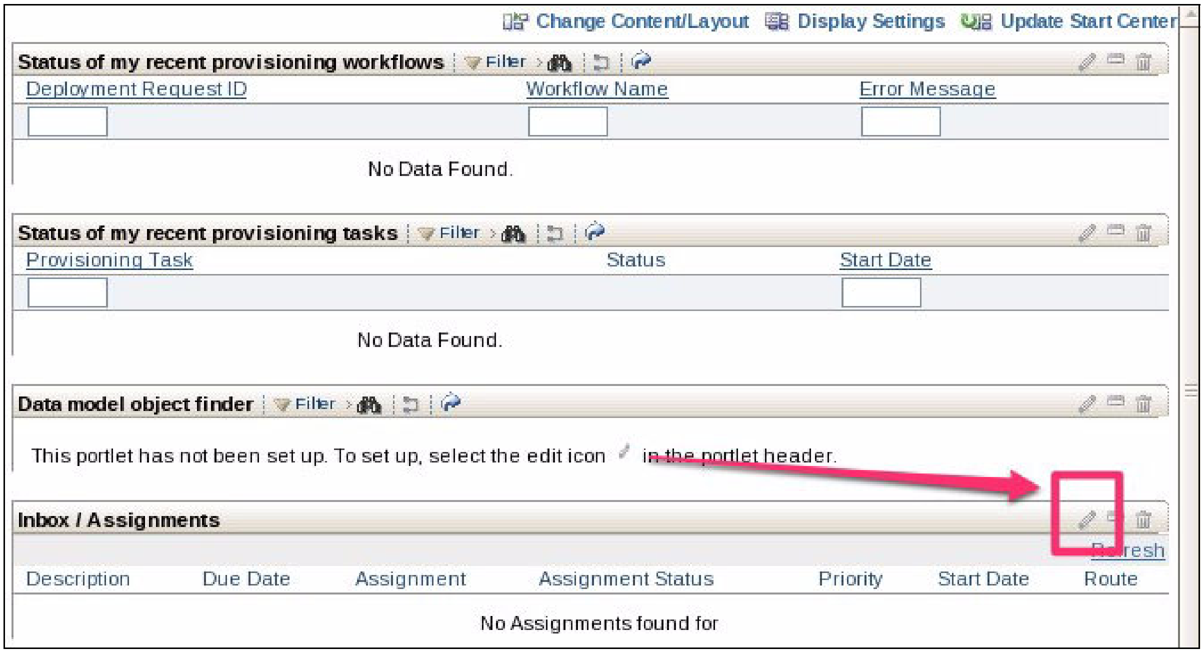
Figure 3-6 Selecting Inbox/Assignments

The Inbox/Assignments has been added to the list of right Column portlets.

10. Finally, we need to set the Description for the portlet to Tivoli Service Automation Manager Operator.

11. Click **Finished**. You are returned to the Maximo Start Center.

12. We need to set up the columns from the Inbox/Assignment portal by clicking the pencil Icon that is on the Inbox/Assignment portal title bar, as shown in Figure 3-7.



Change Content/Layout Display Settings Update Start Center

Status of my recent provisioning workflows Filter

Deployment Request ID	Workflow Name	Error Message

No Data Found.

Status of my recent provisioning tasks Filter

Provisioning Task	Status	Start Date

No Data Found.

Data model object finder Filter

This portlet has not been set up. To set up, select the edit icon in the portlet header.

Inbox / Assignments

Refresh

Description	Due Date	Assignment	Assignment Status	Priority	Start Date	Route

No Assignments found for

Figure 3-7 Setting up the columns

The Inbox/Assignment Setup page is shown. From the following list of available Column names, select the **Display** check box:

- DUEDATE
- ASSIGNID
- ASSIGNSTATUS
- PRIORITY
- STARTDATE

You might have to scroll through several pages to choices to see all of the column names.

13. When all of the Column names have been selected, you must update the Order Column for the first Column DUEDATE to the value of **-1**.
14. Click **Finished**.

    The Tivoli Service Automation Manager Operator Start center is now ready for use.
15. Log off and log back in to Maximo before you continue. Logging out of Maximo requires that you close all of your browser windows.

3.5 Granting the user access to the inbox content

Complete the following steps to grant user access to the inbox content:

1. Log in to the Maximo console by using a Maximo administrator ID.
2. The **Maximo Start Center** window opens. Go to Favorite applications by clicking the small pencil icon on the Favorite Applications portlet (Automation Development Applications) title bar, as highlighted in Figure 3-8.

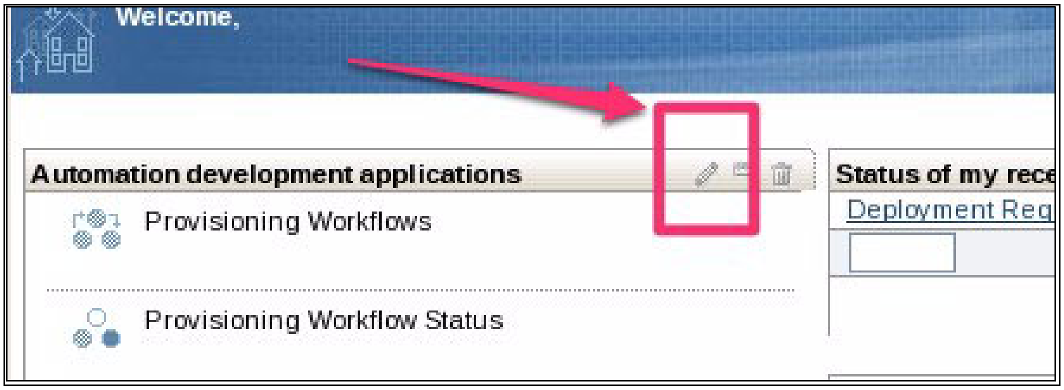
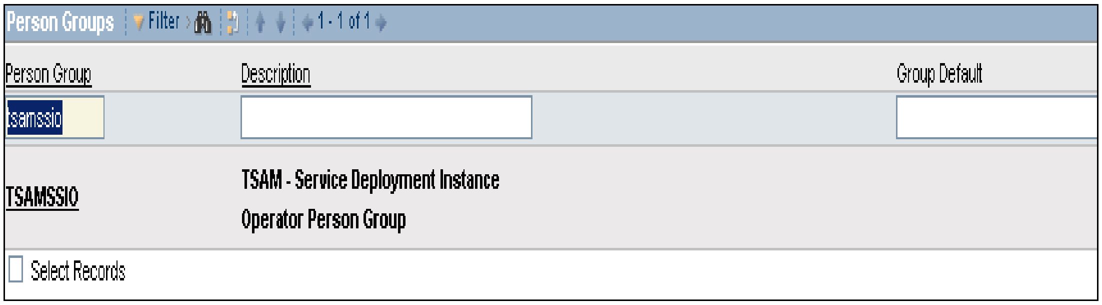

Welcome,
Automation development applications
Provisioning Workflows
Provisioning Workflow Status
Status of my rece
Deployment Req

Figure 3-8 Accessing favorite applications

3. Click the **Select Applications** menu button on the lower, left corner of the screen. The Select Application list is displayed. From the list of applications, select the check box for **Person Groups**. You can find this group by filtering the list of application with “person” search criteria. Click **OK**.
4. Click the **Person Groups** application from the list of favorite applications on the Start Center.
5. Search for **TSAMSSIO** person group, as shown in Figure 3-9 on page 32.



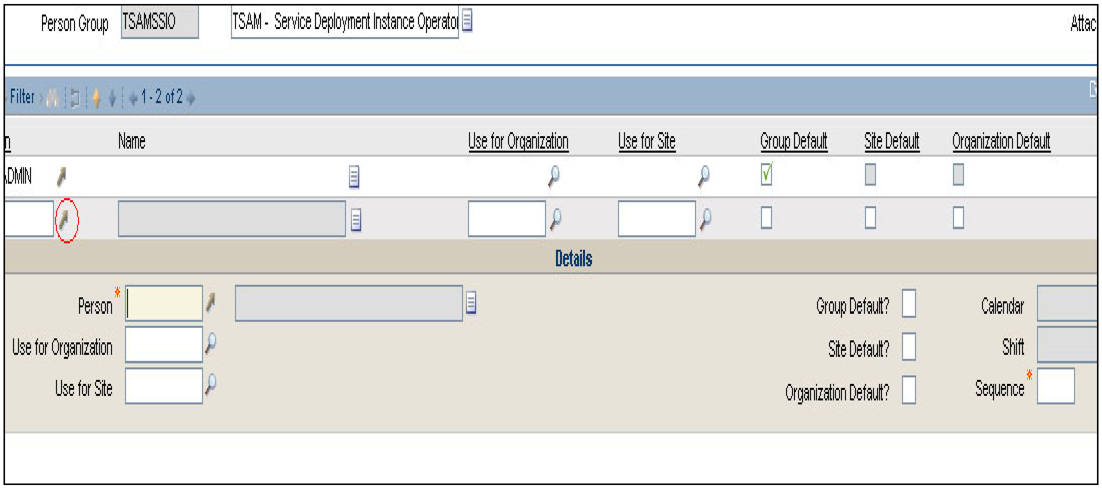
Person Groups | Filter > | 1 - 1 of 1

Person Group	Description	Group Default
tsamssio		
TSAMSSIO	TSAM - Service Deployment Instance Operator Person Group	

□ Select Records

Figure 3-9 Finding the TSAMSSIO person group

6. Add the **TSAMOPER** user to this person group by clicking **New Row** and search for the **TSAMOPER** user from the person group, as shown in Figure 3-10.



Person Group TSAMSSIO TSAM - Service Deployment Instance Operato

Filter > | 1 - 2 of 2

n	Name	Use for Organization	Use for Site	Group Default	Site Default	Organization Default
DMIN				☑	□	□
				□	□	□

Details

Person *

Use for Organization

Use for Site

Group Default? □

Site Default? □

Organization Default? □

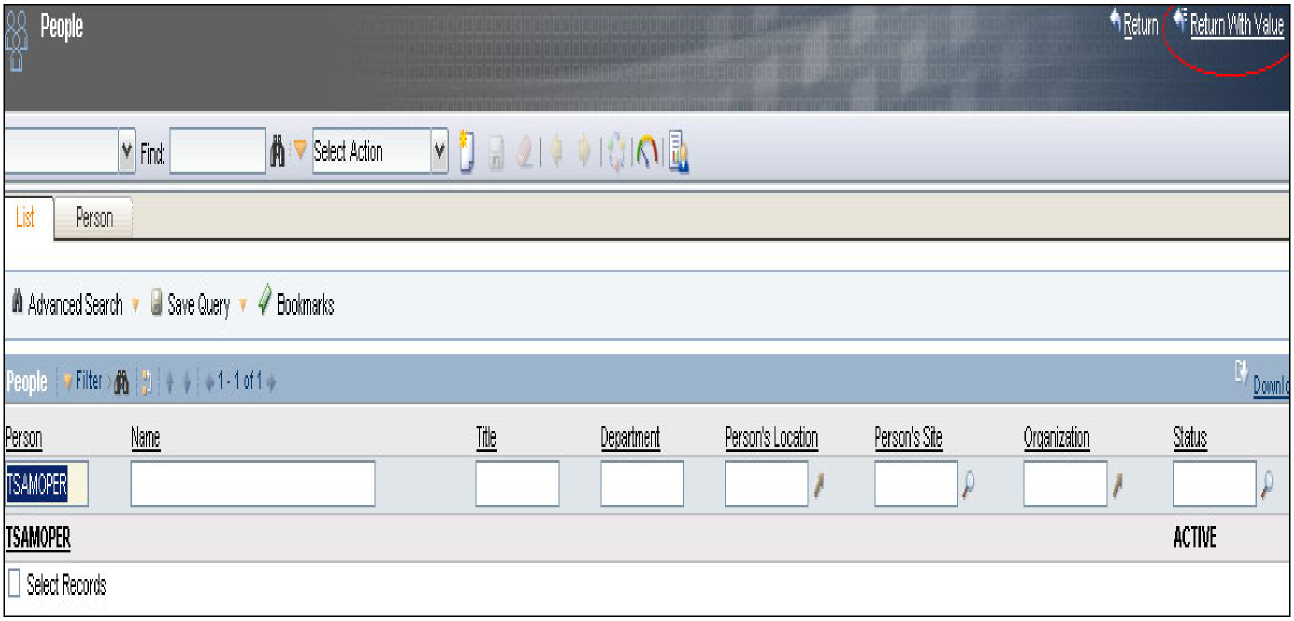
Calendar

Shift

Sequence *

Figure 3-10 Adding the TSAMOPER user ID

7. Click the **small arrow symbol** and select **Go To People** option from the menu that opens. Filter for **TSAMOPER** user and select **Return with Value**, as shown in Figure 3-11 on page 33.

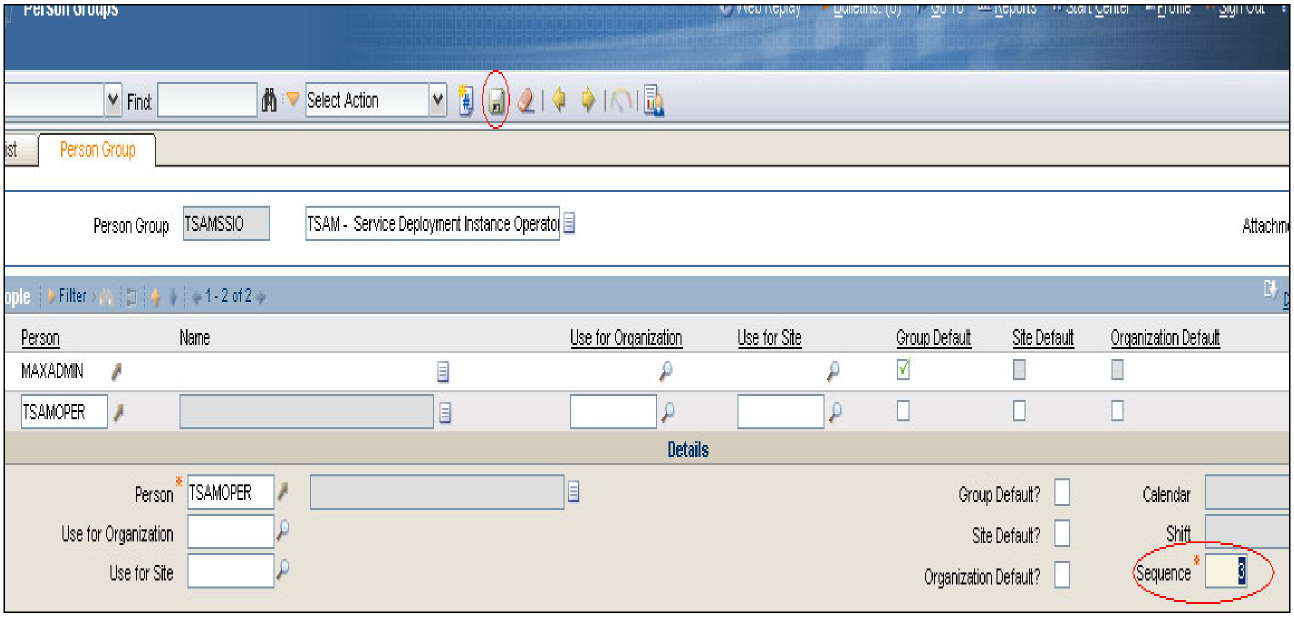


Person	Name	Title	Department	Person's Location	Person's Site	Organization	Status
TSAMOPER							
TSAMOPER							ACTIVE

□ Select Records

Figure 3-11 Selecting Return with Value option

8. TSAMOPER is added to the **TSAMSSIO** person group. Specify the sequence value as **3**, as shown in Figure 3-12. Select the **Group Default** check box for maxadmin user and save the changes.



Person Group: TSAMSSIO TSAM - Service Deployment Instance Operatoi

Person	Name	Use for Organization	Use for Site	Group Default	Site Default	Organization Default
MAXADMIN				☑	□	□
TSAMOPER				□	□	□

Details

Person * TSAMOPER

Use for Organization

Use for Site

Group Default? □

Site Default? □

Organization Default? □

Calendar

Shift

Sequence * 3

Figure 3-12 Saving the changes

All of the subsequent assignments will be redirected to all of the members of TSAMSSIO person group.

3.6 Changing a Maximo administrator or user password

Complete the following steps to change a Maximo administrator or user password:

1. Log in to the Server via Secure Shell (SSH) by using your administrator user ID and password.
2. Change your Maximo password by entering the following command. You will need to provide your actual Maximo user ID. (The sampleuser here is provided as an example. You need to substitute your actual ID after ou=.):

   ```
   /opt/ibm/ldap/V6.2/bin/idsldapchangepwd -D "uid=
   sampleuser,ou=users,ou=SWG,o=IBM,c=US" -w ? -n ?
   ```

3.7 Checking for the expiration of an LDAP users password

To pre-notify LDAP users of pending expirations of their passwords, a regular check of the user repository is required. Tivoli Service Automation Manager or any of its underlying components does not provide any capability. The `checkLdapPwdExpiration.sh` script is run via the Linux crontab scheduler to perform this daily check. Any users that may have a password that is about to expire according to the `pwdExpireWarning` settings are notified by email.

Complete the following steps to check for expirations of an LDAP users' password:

1. Log in to the Tivoli Service Automation Manager Management server via a user account.
2. Run `checkLdapPwdExpiration.sh` script to report any LDAP user IDs which might expire within the `pwdExpireWarning` (currently, it is seven days) setting on the ACL for your LDAP group. (For an example of this script, see Chapter 5, "Sample scripts" on page 43.)
3. To automate the execution of the `checkLdapPwdExpiration.sh` script, add the following line to your user account crontab:

   ```
   crontab -e
   ```

   Add the following line that changes the directory in which your script is located:

   ```
   30 00  * * *  /home/user/checkLdapPwdExpiration.sh 1>result.log 2>audit.log
   ```

4. Save the file.

When this script runs via crontab, the daily results of the LDAP password expiration check are placed into the `audit.log` file. Users also are automatically notified starting at the value of `pwdExpireWarning`.

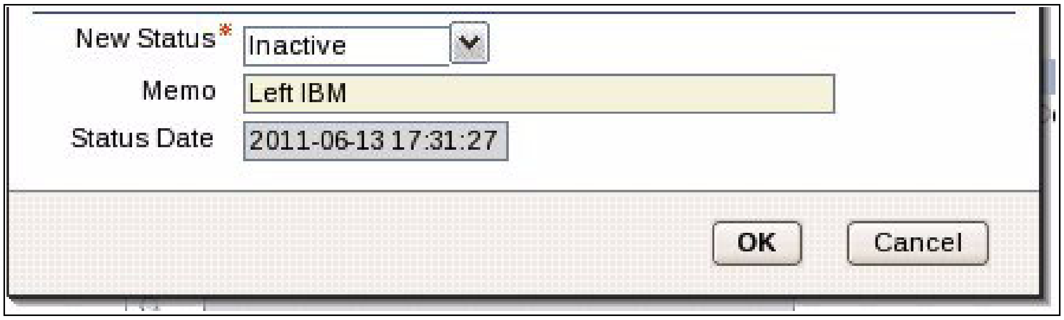
3.8 Account deactivation procedures

When a Maximo account owner no longer requires access or leaves the company, the owner's account ID must be deactivated, removed, or deleted.

3.8.1 Deactivating an administrator or user account

An administrator or user account must be deactivated from Maximo if the administrator or user is terminated or transferred to another job role. Complete the following steps to de-activate the account:

1. Log in to the Maximo application by using an Maximo administrator ID.
2. By using the Maximo Start Center, select **Security** → **Users**.
3. Enter the user name that is to be deactivated in the User field and click **Enter**.
4. Select the user's name from the users list by clicking the name.
5. From the Select Actions pull-down list, choose the **Change Status** option. The Change Status window opens.
6. Set the following parameters in the Change Status window:
   a. New Status: **Inactive** (select this parameter from the pull-down menu).
   b. Memo: Add the reason or change ticket number for the removal of the ID, as shown in Figure 3-13.



New Status* Inactive

Memo Left IBM

Status Date 2011-06-13 17:31:27

Figure 3-13 Choosing a status and entering a reason

7. Click **OK**.
8. The Status field on the user window should now read INACTIVE.
9. In the users window, click **Save** to finish the account deactivation.

3.8.2 Removing the administrative role

Important: This procedure is used only for the Tivoli Service Automation Manager Maximo administrator.

1. Open the WebSphere Integrated Services Console (ISC) by using the following site URL (include the Tivoli Service Automation Manager servers IP address in the actual URL):

   ```
   https://TSAM_SERVER:9043/ibm/console/logon.jsp
   ```

2. By using the user ID that includes the WebSphere administrative rights, log in to the WebSphere Application Server ISC.
3. Select **System and Groups** → **Administrative User Role**.
4. Find the account ID to be removed from the Administrative user role and click **Remove**.
5. To permanently save these changes, select the **Save directly to the master configuration** option.

3.8.3 Delete Maximo administrator or operator IDs

Complete the following steps to remove users from the Tivoli Provisioning Manager database:

1. Click **Go To** → **Security** → **Security Group**.
2. Click **Select Action** → **Security Controls**.
3. Check whether login tracking is enabled. Enable login tracking if it is not enabled. Information about how to enable login tracking is available in the Maximo online help. The Maximo help is accessed by clicking on the **Help** menu item in the Maximo Welcome window or by using the pressing Alt+H.
4. Stop Tivoli Provisioning Manager.
5. Enter the following SQL command:

   ```
   UPDATE MAXIMO.MAXPROPVALUE SET PROPVALUE='0' WHERE PROPNAME =
   'mxe.LDAPUserMgmt'
   ```

6. Start Tivoli Provisioning Manager.
7. Ensure that the user is removed from the LDAP server.
8. Click **Go To** → **Security** → **Users**.
9. Click the user that you want to remove.
10. Click **Select Action** → **Delete User**.
11. Enter the following SQL command:

    ```
    UPDATE MAXIMO.MAXPROPVALUE SET PROPVALUE='1' WHERE PROPNAME =
    'mxe.LDAPUserMgmt'
    ```

12. Restart Tivoli Provisioning Manager.

4

General security procedures

Several security-enhancing techniques are described in this chapter.

4.1 Removing root access to IBM Tivoli Directory Server

In this section, we describe an operating system security tip.

During the Tivoli Service Automation Manager middleware installation process, IBM Tivoli Directory Server is installed to provide authentication to various components, such as WebSphere. During the installation process, the `idsldap` ID is placed into the `root` group. The root user is given access to the `idsldap` group. This configuration creates a security exposure which must be remedied after the initial system is built.

Complete the following steps to remove root access from IBM Tivoli Directory:

1. Log in to your IBM Tivoli Directory Server.
2. Change to the root user (`sudo su -`).
3. Edit the `/etc/groups`.
4. Search for the `idsldap` user in the `root` group and remove the `idsldap` user by using the following command:

   ```
   root:x:0:root,idsldap (remove idsldap here)
   ```

5. Search for the root user in the `idsldap` group and remove the root user by using the following command:

   ```
   idsldap:x:505:idsldap,root,idsccmdb (remove root here)
   ```

6. Save the file.
7. To ensure that there are no issues with LDAP authentications, you should restart the IBM Tivoli Directory Server.

4.2 Limiting remote logins to Tivoli Service Automation Manager component user IDs

Remote login to several of the user IDs created by Tivoli Service Automation Manager presents a security exposure. Therefore, after your Tivoli Service Automation Manager environment is built, the ability to remotely log in to these user IDs should be eliminated.

To disable the ability to remotely log in to Tivoli Service Automation Manager component software user IDs, you must disable the login shell for those ids as follows:

1. Establish a Secure Shell (SSH) session to your Tivoli Service Automation Manager server
2. Place the root user in superuser mode and issue the `usermod` command for the following IDs to limit remote login shell:

   ```
   usermod -s /sbin/nologin ctginst1
   usermod -s /sbin/nologin dasusr1
   usermod -s /sbin/nologin db2fenc1
   usermod -s /sbin/nologin db2inst1
   usermod -s /sbin/nologin idsldap
   usermod -s /sbin/nologin idsccmdb
   usermod -s /sbin/nologin maximo
   ```

3. Because the remote shell is disabled, you may choose to eliminate the password age and expirations for those accounts by using the following commands (this step is optional):

   ```
   chage -M -1 -E -1 ctginst1
   ```

```
chage -M -1 -E -1 dasusr1
chage -M -1 -E -1 db2fenc1
chage -M -1 -E -1 db2inst1
chage -M -1 -E -1 idsccmdb
chage -M -1 -E -1 tioadmin
chage -M -1 -E -1 maximo
```

4.3 Limiting remote log in to tioadmin

In this section, we provide several suggestions for tioadmin security.

4.3.1 Perform key exchange for tioadmin

Complete the following steps to perform a key exchange for tioadmin:

1. Log in to Tivoli Service Automation Manager with the `tioadmin` user ID.
2. Run following command:

   ```
   cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
   ```

   This command ensures that the public key of `tioadmin` is added to its `authorized_keys` file. This configuration can be verified by establishing an SSH session to the Tivoli Service Automation Manager server with tioadmin by running the following command:

   ```
   ssh tioadmin@<<TSAM_HOST>>
   ```

4.3.2 Change SAP credentials within Trivoli Provisioning Manager

Complete the following steps to change the SAP credentials with Tivoli Provisioning Manager:

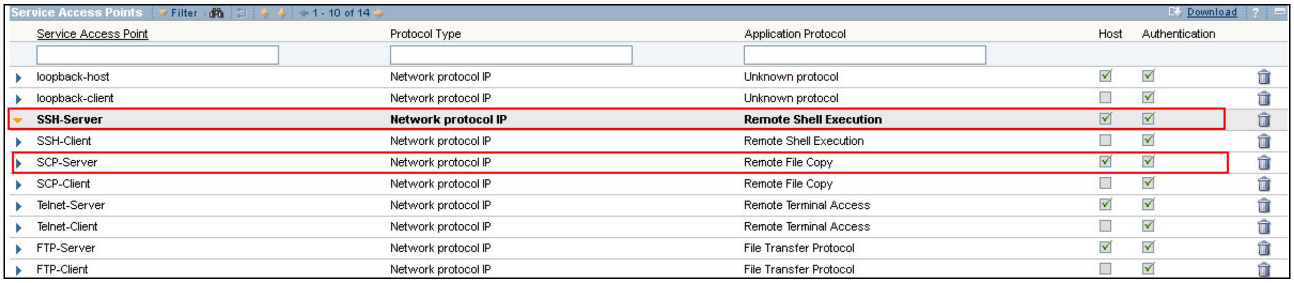
1. Open Start Center that is found at this website:

   https://TSAM_SERVER:9443/maximo

2. Open the Provisioning Computers Application by clicking **Go To → IT Infrastructure → Provisioning Inventory → Provisioning Computers**

   Search for Tivoli Service Automation Manager server.

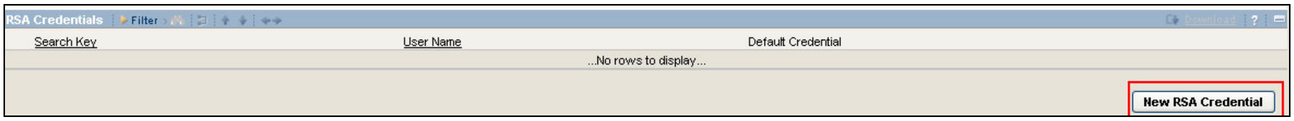
3. At the Credentials tab, complete the following steps to configure the SSH-Server and SCP-Server service access points (SAPs) of Tivoli Service Automation Manager server, as shown in Figure 4-1:



Service Access Point	Protocol Type	Application Protocol	Host	Authentication
loopback-host	Network protocol IP	Unknown protocol	☑	☑
loopback-client	Network protocol IP	Unknown protocol	□	☑
SSH-Server	**Network protocol IP**	**Remote Shell Execution**	☑	☑
SSH-Client	Network protocol IP	Remote Shell Execution	□	☑
SCP-Server	Network protocol IP	Remote File Copy	☑	☑
SCP-Client	Network protocol IP	Remote File Copy	□	☑
Telnet-Server	Network protocol IP	Remote Terminal Access	☑	☑
Telnet-Client	Network protocol IP	Remote Terminal Access	□	☑
FTP-Server	Network protocol IP	File Transfer Protocol	☑	☑
FTP-Client	Network protocol IP	File Transfer Protocol	□	☑

Figure 4-1 Tivoli Service Automation Manager SAPs

i. Select the SAP. Click **New RSA Credentials**, as shown in Figure 4-2.



Search Key	User Name	Default Credential
...No rows to display...		

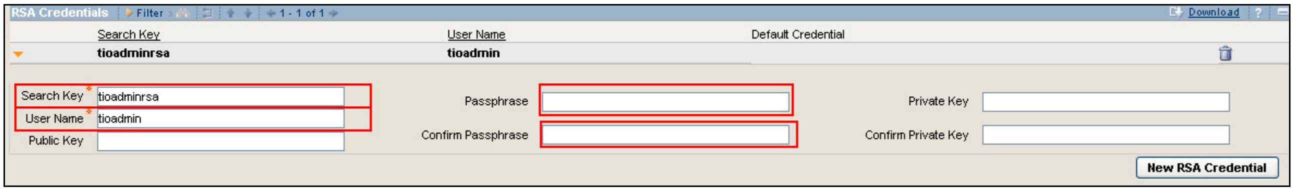
Figure 4-2 Selecting New RSA Credentials

ii. Enter the values that are shown in Table 4-1.

Table 4-1 RSA credentials

Search Key	tioadminrsa (only to keep the name constant; any unique name can be used)
User Name	tioadmin

iii. Enter and confirm the passphrase that is used for generating the SSH key of `tioadmin`, as shown in Figure 4-3.



Search Key	User Name	Default Credential
tioadminrsa	tioadmin	

Search Key * tioadminrsa

User Name * tioadmin

Public Key

Passphrase

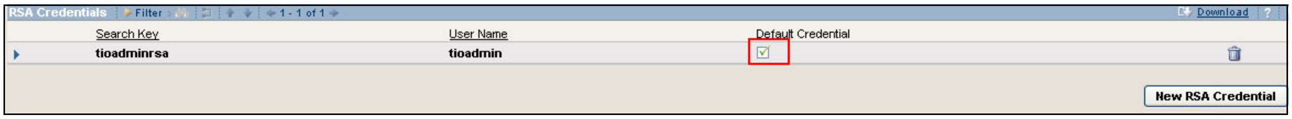
Confirm Passphrase

Private Key

Confirm Private Key

Figure 4-3 Entering the passphrase

iv. Save the computer record. Select the SAP and confirm that the RSA credentials are the default credentials, as shown in Figure 4-4.



Search Key	User Name	Default Credential
tioadminrsa	tioadmin	☑

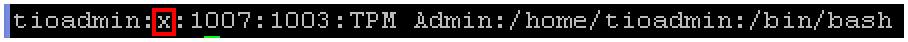
Figure 4-4 Making the credentials to be the defaults

v. Save the computer record.

4.3.3 Remove password for tioadmin

Complete the following steps to remove the password for tioadmin:

1. Log in to Tivoli Service Automation Manager server with Putty by using root credentials.
2. Create a backup of the `/etc/passwd` file.
3. Edit the `/etc/passwd` file. Search for **tioadmin** and remove '**x**' in the following tioadmin:

   ```
   tioadmin:x:1007:1003:TPM Admin:/home/tioadmin:/bin/bash
   ```

4. Save the `/etc/passwd` file. The password is removed.

4.4 Remove root user from Tivoli Service Automation Manager database tables

DB2 is installed during the Tivoli Service Automation Manager middleware installation process. During the initial build, the root user is given access to Tivoli Service Automation Managers-related databases. After the initial build is done, users are advised to remove root access from the MAXDB71 instance to minimize the security exposure of including root ID associated with database.

Complete the following steps to remove root user from Tivoli Service Automation Manager database tables:

1. Log in to Tivoli Service Automation Manager db2 server as **ctginst1.**
2. Run the following commands to remove the root user ID from the MAXDB71 database:

```
db2 connect to maxdb71
db2 revoke bindadd on database from user root
db2 revoke connect on database from user root
db2 revoke createtab on database from user root
db2 revoke create_external_routine on database from user root
db2 revoke create_not_fenced_routine on database from user root
db2 revoke implicit_schema on database from user root
db2 revoke dbadm on database from user root
db2 revoke load on database from user root
db2 revoke quiesce_connect on database from user root
db2 revoke secadm on database from user root
db2 connect reset
```

5

Sample scripts

In this chapter, several sample scripts are provided that might be helpful when the scripts are adapted to your system.

5.1 addmaxadmin.sh

The following script is a sample of the `addmaxadmin.sh` script:

```
#!/bin/bash
#
# addmaxadmin.sh ldap_bind_password user_name email
#
#
#
# this script is used to add a user to LDAP for TSAM and then update the correct
# LDAP groups so they can have correct admin groups memberships:
# - <arg1> Bind password
# - <arg2> user_name
# - <arg3> first_name
# - <arg4> last_name
# - <arg5> password
# - <arg6> email
#
#
# CHANGE these per your deployment
ldap_path="/opt/IBM/ldap/V6.2/bin/"
ldap_user_dn="ou=users,ou=SWG,o=IBM,c=US"
ldap_group_dn="ou=groups,ou=SWG,o=IBM,c=US"

LDAPPWD=""
USERNAME=""
FNAME=""
LNAME=""
EMAIL=""
PASSWD=""
USAGE="usage: addmaxadmin.sh: -w ldap_bind_password -u user_name -F first_name -L
last_name -p password -e email"

while getopts 'w:p:u:n:F:L:e:h?' OPTION
   do
     case $OPTION in
     w)            LDAPPWD="$OPTARG"
         ;;
     u)  USERNAME="$OPTARG"
         ;;

          L)            LNAME="$OPTARG"
                        ;;

          F)            FNAME="$OPTARG"
                        ;;
     e)            EMAIL="$OPTARG"
         ;;

         p)             PASSWD="$OPTARG"
                        ;;
   h)    echo $USAGE
         exit 1
         ;;
   ?)
         echo $USAGE
         exit 1
         ;;
     esac
   done

if [ $# -ne  12 ]
then
        echo $USAGE
   exit 1
fi

rm ldapcmd.ldif

echo 'dn: uid='$USERNAME','$ldap_user_dn > ldapcmd.ldif
echo 'objectClass: inetorgperson' >> ldapcmd.ldif
echo 'objectClass: organizationalPerson'  >> ldapcmd.ldif
echo 'objectClass: person' >> ldapcmd.ldif
echo 'objectClass: top' >> ldapcmd.ldif
echo 'uid: '$USERNAME >> ldapcmd.ldif
echo 'userPassword: '$PASSWD >> ldapcmd.ldif
echo 'sn: '$LNAME >> ldapcmd.ldif
echo 'cn: '$FNAME >> ldapcmd.ldif
echo 'mail: '$EMAIL >> ldapcmd.ldif
echo 'displayName: ' $FNAME $LNAME >> ldapcmd.ldif
ldap_binddn="cn=root"
ldap_bindpwd=$LDAPPWD
ldap_cmd="${ldap_path}/idsldapadd -D ${ldap_binddn} -w ${ldap_bindpwd} -f
ldapcmd.ldif"
echo 'Adding:'$USERNAME' to LDAP'
result=$(${ldap_cmd})

if [ "${result}" != "" ]; then
        result=$(echo ${result} | sed -e 's/^.*: //')
        echo ${result}
fi

declare -a TSAMGROUPS=("MAXADMIN" "CCMPADMIN"  "PMREQUESTER" "TPADMIN"
"TPCOMPLIANCEANALYST" "TPCONFIGURATIONLIBRARIAN" "TPDEPLOYMENTSPECIALIST"
"TPDEVELOPER" "TPWEBSERVICEUSER" "PMRDPCA" "PMRDPCLOUDPOLICY" )

for TSAMGROUP in ${TSAMGROUPS[@]}
do
   echo 'Adding:'$USERNAME' to '$TSAMGROUP' LDAP Group'
   rm ldapcmd.ldif
   echo 'dn: cn='$TSAMGROUP','$ldap_group_dn > ldapcmd.ldif
   echo 'changetype: modify' >> ldapcmd.ldif
   echo 'add: member' >> ldapcmd.ldif
   echo 'member: uid='$USERNAME','$ldap_user_dn >> ldapcmd.ldif

   ldap_cmd="${ldap_path}/idsldapmodify -D ${ldap_binddn} -w ${ldap_bindpwd} -f
ldapcmd.ldif"

 #  echo ${ldap_cmd}
```

```
   result=$(${ldap_cmd})

   if [ "${result}" != "" ]; then
        result=$(echo ${result} | sed -e 's/^.*: //')
        echo ${result}
   fi


done
```

5.2 addmaxoper.sh

The following script is a sample of the `addmaxoper.sh` script:

```
#!/bin/bash
#
# addmaxoper.sh ldap_bind_password user_name email
#
# this script is used to add a user to LDAP for TSAM and then update the correct
# LDAP groups so they can have correct admin groups memberships:
# - <arg1> Bind password
# - <arg2> user_name
# - <arg3> first_name
# - <arg4> last_name
# - <arg5> password
# - <arg6> email
#
# CHANGE these per your deployment
ldap_path="/opt/IBM/ldap/V6.2/bin"
ldap_user_dn="ou=users,ou=SWG,o=IBM,c=US"
ldap_group_dn="ou=groups,ou=SWG,o=IBM,c=US"

# Variables
LDAPPWD=""
USERNAME=""
FNAME=""
LNAME=""
EMAIL=""
PASSWD=""
USAGE="usage: addmaxoper.sh: -w ldap_bind_password -u user_name -F first_name -L
last_name -p password -e email"

while getopts 'w:p:u:n:F:L:e:h?' OPTION
   do
     case $OPTION in
     w)             LDAPPWD="$OPTARG"
         ;;
     u)  USERNAME="$OPTARG"
         ;;

          L)             LNAME="$OPTARG"
                         ;;

          F)             FNAME="$OPTARG"
```

```
                        ;;
     e)            EMAIL="$OPTARG"
         ;;

         p)             PASSWD="$OPTARG"
                        ;;
   h)    echo $USAGE
         exit 1
         ;;
   ?)
         echo $USAGE
         exit 1
         ;;
     esac
   done

if [ $# -ne  12 ]
then
        echo $USAGE
   exit 1
fi

rm ldapcmd.ldif

echo 'dn: uid='$USERNAME','$ldap_user_dn > ldapcmd.ldif
echo 'objectClass: inetorgperson' >> ldapcmd.ldif
echo 'objectClass: organizationalPerson'  >> ldapcmd.ldif
echo 'objectClass: person' >> ldapcmd.ldif
echo 'objectClass: top' >> ldapcmd.ldif
echo 'uid: '$USERNAME >> ldapcmd.ldif
echo 'userPassword: '$PASSWD >> ldapcmd.ldif
echo 'sn: '$LNAME >> ldapcmd.ldif
echo 'cn: '$FNAME >> ldapcmd.ldif
echo 'mail: '$EMAIL >> ldapcmd.ldif
echo 'displayName: ' $FNAME $LNAME >> ldapcmd.ldif

ldap_binddn="cn=root"
ldap_bindpwd=$LDAPPWD
ldap_cmd="${ldap_path}/idsldapadd -D ${ldap_binddn} -w ${ldap_bindpwd} -f
ldapcmd.ldif"
echo 'Adding:'$USERNAME' to LDAP'
 result=$(${ldap_cmd})

if [ "${result}" != "" ]; then
        result=$(echo ${result} | sed -e 's/^.*: //')
        echo ${result}
fi

declare -a TSAMGROUPS=("MAXIMOUSERS" "CCMPOP")

for TSAMGROUP in ${TSAMGROUPS[@]}
do
   echo 'Adding:'$USERNAME' to '$TSAMGROUP' LDAP Group'
   rm ldapcmd.ldif
   echo 'dn: cn='$TSAMGROUP','$ldap_group_dn > ldapcmd.ldif
   echo 'changetype: modify' >> ldapcmd.ldif
   echo 'add: member' >> ldapcmd.ldif
   echo 'member: uid='$USERNAME','$ldap_user_dn >> ldapcmd.ldif

   ldap_cmd="${ldap_path}/idsldapmodify -D ${ldap_binddn} -w ${ldap_bindpwd} -f
ldapcmd.ldif"

   echo ${ldap_cmd}
   result=$(${ldap_cmd})

   if [ "${result}" != "" ]; then
        result=$(echo ${result} | sed -e 's/^.*: //')
       echo ${result}
   fi


done
```

5.3 addwasadmin.sh

The following script is a sample of the `addwasadmin.sh` script:

```
#!/bin/bash

WASADMUSR=""
WASADMPWD=""
USERNAME=""
# SECID=""

# USAGE="usage: addwasadmin.sh: -u user_name -[s] [-a wasdamin_id] [-p wasadmin_
pwd]"
USAGE="usage: addwasadmin.sh: -u user_name [-a wasdamin_id] [-p wasadmin_pwd]"

while getopts 'a:p:s:u:h?' OPTION
# while getopts 'a:p:s:u:h?' OPTION
        do
          case $OPTION in
          a)           WASADMUSR="$OPTARG"
                        ;;
         p)            WASADMPWD="$OPTARG"
                        ;;
#         s)            SECID="1"
#                        ;;
         u)            USERNAME="$OPTARG"
                        ;;
        h)              echo $USAGE
                        exit 1
                        ;;
        ?)
                        echo $USAGE
                        exit 1
                        ;;
          esac
        done
```

```
if [ -z  $USERNAME ]; then
        echo $USAGE
        exit 1
fi

if [ -z $WASADMUSR ]; then
        echo "Enter the id for WAS administrative user :  $WASADMUSR"
        stty -echo; read WASADMUSR; stty echo; echo
fi

if [ -z $WASADMPWD ]; then
        echo "Enter the password for WAS administrative user :  $WASADMPWD"
        stty -echo; read WASADMPWD; stty echo; echo
fi

echo "Adding $USERNAME to WebSphere adminisrative group role"
/opt/IBM/WebSphere/AppServer/profiles/ctgAppSrv01/bin/wsadmin.sh -lang jython -u
ser ${WASADMUSR} -password ${WASADMPWD} -c "AdminTask.mapUsersToAdminRole('-user
ids [${USERNAME} ] -roleName administrator]') "
```

5.4 checkLdapPwdExpiration.sh

The following script is a sample of the `checkLdapPwdExpiration.sh` script:

> **Important:** This sample script is an open source script that was modified to work in the SmartCloud Enterprise environment and was not developed by IBM.

```
#!/bin/bash

#====================================================================
# Script for OpenLDAP with ppolicy overlay
#
# Does searches on LDAP directory to determine which user passwords
# came to expiration. If so, sends mails to concerned users.
#
# Tested on :
#   - GNU/Linux platform ;
#   - SunOS 8.5 platform ;
#
# Dependences :
#   - gawk
#   - ldapsearch
#
# Copyright (C) 2008 Clement OUDOT
# Copyright (C) 2007 Thomas CHEMINEAU
# Copyright (C) 2009 LTB-project.org
#
# This program is free software; you can redistribute it and/or
# modify it under the terms of the GNU General Public License
# as published by the Free Software Foundation; either version 2
# of the License, or (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# GPL License: http://www.gnu.org/licenses/gpl.txt
#
#====================================================================

#====================================================================
# Changelog
#====================================================================
# Version 0.2 (08/2008):
# - Use zulu time (GMT) for currentTime
# - Split mail command parameters (binary and subject)
# - Add script statitics to STDOUT
# - Add debug info to STDERR
# - Use ppolicy warning time for mail delay if provided
# - Manage no default ppolicy case (just per-user ppolicies)
# - LDAP user attributes are now configurable
# - Jump to next user if no password change date or no ppolicy
# LIMIT: multi-lined DN causes errors
# TODO: use GMT time for SunOS and test the script for this OS
# Author: Clement OUDOT (LINAGORA)
#
# Version 0.1 (2007):
# - First version
# Author: Thomas CHEMINEAU (LINAGORA)
#====================================================================


#====================================================================
# Configuration
#====================================================================
source /home/ctginst1/ccmpDefs.sh
#
# LDAP host URI
# eg: ldap://localhost:389
#
MY_LDAP_HOSTURI="ldap://localhost:389"

#
# LDAP root DN (optional)
#
MY_LDAP_ROOTDN="cn=root"

#
# LDAP root password (optional)
#
MY_LDAP_ROOTPW="PUT YOUR PWD HERE IF NEEDED"

#
# LDAP default password policy DN
# eg: ou=defaultPasswordPolicy,dc=example,dc=com
# If commented, we suppose there are no default, and only per-user policies
#
MY_LDAP_DEFAULTPWDPOLICYDN="cn=group_pwd_policy,cn=ibmPolicies"

#
# LDAP search base for users
# eg: ou=People,dc=example,dc=com
#
MY_LDAP_SEARCHBASE="ou=users,ou=SWG,o=IBM,c=US"

#
# LDAP search filter to use to get all users
#
#MY_LDAP_SEARCHFILTER="(&(uid=*)(objectClass=inetOrgPerson))"
MY_LDAP_SEARCHFILTER="(objectclass=*)"

#
# Path to LDAP search binary
#
MY_LDAP_SEARCHBIN="/opt/ibm/ldap/V6.2/bin/idsldapsearch"

#
# Delay to begin sending adverts
# Comment to use the pwdExpireWarning value of the user's Password Policy
#
MY_MAIL_DELAY=624800

#
# LDAP attributes storing user's information
#   NAME: Display name of the user
#   LOGIN: Account ID of the user
#   MAIL: Email of the user
#
MY_LDAP_NAME_ATTR=cn
MY_LDAP_LOGIN_ATTR=uid
MY_LDAP_MAIL_ATTR=mail

#
# Mail body message, with particular variables :
#   %name : user name
#   %login : user login
#
MY_MAIL_BODY="*****THIS IS A MACHINE GENERATED MESSAGE*****DO NOT REPLY TO THIS 
NOTIFICATION****\n\n \
Hello %name,\n\n \
Your TSAM LDAP password for ${site_id} is about to expire\n \
Please follow these steps\n \
1) Log into the $site_id TSAM Server via SSH using your account\n \
2) Immediately change your Maximo password by entering the following command\n \
/opt/ibm/ldap/V6.2/bin/idsldapchangepwd -D 
\"uid=%login,ou=users,ou=SWG,o=IBM,c=US\" -w ? -n ?\n\n \
You will be prompted for your current (reset) and new passwords\n \
PLEASE NOTE:  Each TSAM server has its own Maximo user registry so you will need 
to change each password that gets reset"
```

```
#
# Mail subject
#
MY_MAIL_SUBJECT="Your TSAM LDAP account in ${site_id} will expire soon"

#
# Mail command binary
# Replace mailx by mail for RedHat
#
MY_MAIL_BIN="mail"

#
# Log header format
# Could include unix commands
#
MY_LOG_HEADER="`date +\"%b %e %T\"` `hostname` $0[$$]:"

#
# Path to GAWK (GNU awk) binary
#
MY_GAWK_BIN="/usr/bin/gawk"

#=====================================================================
# Functions
#=====================================================================

#
# Retrieves date in seconds.
# This function could take one parameter, a time returned by the command
# `date +"%Y %m %d %H %M %S"`. Without parameter, it returns GMT time.
#
getTimeInSeconds() {
   date=0
   os=`uname -s`

   if [ "$1" ]; then
      date=`${MY_GAWK_BIN} 'BEGIN  { \
         if (ARGC == 2) { \
              print mktime(ARGV[1]) \
         } \
         exit 0 }' "$1"`
   else
      if [ "${os}" = "SunOS" ]; then
         # Under Sun Solaris, there is no simple way to
         # retrieve epoch time.
         # TODO: manage zulu time (GMT)
         date=`/usr/bin/truss /usr/bin/date 2>&1 | nawk -F= \
            '/^time\(\)/ {gsub(/ /,"",$2);print $2}'`
      else
         now=`date +"%Y %m %d %H %M %S" -u`
         date=`getTimeInSeconds "$now"`
      fi
   fi

   echo ${date}
}

#=====================================================================
# Script
#=====================================================================

## Variables initialization
tmp_dir="/tmp/$$.checkldap.tmp"
result_file="${tmp_dir}/res.tmp.1"
buffer_file="${tmp_dir}/buf.tmp.1"
# ldap_param="-LLL -H ${MY_LDAP_HOSTURI} -x"
ldap_param="-L"
nb_users=0
nb_expired_users=0
nb_warning_users=0

## Some tests
if [ -d ${tmp_dir} ]; then
   echo "Error : temporary directory exists (${tmp_dir})"
   exit 1
fi
mkdir ${tmp_dir}

if [ ${MY_LDAP_ROOTDN} ]; then
   ldap_param="${ldap_param} -D ${MY_LDAP_ROOTDN} -w ${MY_LDAP_ROOTPW}"
fi

## Performs global search

${MY_LDAP_SEARCHBIN} ${ldap_param} -s one -b "${MY_LDAP_SEARCHBASE}" \
   "${MY_LDAP_SEARCHFILTER}" "dn" > ${result_file}

## Loops on results
while read dnStr
do
   # Do not use blank lines
   if [ ! "${dnStr}" ]; then
      continue
   fi

   # Process ldap search
   dn=`echo ${dnStr} | cut -d : -f 2`
   # Increment users counter
   nb_users=`expr ${nb_users} + 1`

        ${MY_LDAP_SEARCHBIN} ${ldap_param} -b "$dn" -s base
"$MY_LDAP_SEARCHFILTER"  $MY_LDAP_NAME_ATTR $MY_LDAP_LOGIN_ATTR $MY_LDAP_MAIL_ATTR
pwdChangedTime +ibmpwdpolicy  > $buffer_file
   login=`grep -w "${MY_LDAP_LOGIN_ATTR}:" ${buffer_file} | cut -d : -f 2 \
      | sed "s/^ *//;s/ *$//"`
   name=`grep -w "${MY_LDAP_NAME_ATTR}:" ${buffer_file} | cut -d : -f 2\
      | sed "s/^ *//;s/ *$//"`
   mail=`grep -w "${MY_LDAP_MAIL_ATTR}:" ${buffer_file} | cut -d : -f 2 \
      | sed "s/^ *//;s/ *$//"`
   pwdChangedTime=`grep -w "pwdChangedTime:" ${buffer_file} \
      | cut -d : -f 2 | cut -c 0-15 | sed "s/^ *//;s/ *$//"`
   pwdPolicySubentry=`grep -w "pwdPolicySubentry" ${buffer_file} \
      | cut -d : -f 2 | sed "s/^ *//;s/ *$//"`
   # Go to next entry if no pwdChangedTime
   if [ ! "${pwdChangedTime}" ]; then
      echo "${MY_LOG_HEADER} No password change date for ${login}" >&2
      continue
   fi

   # Go to next entry if no pwdPolicySubEntry and no default policy
   if [ ! "${pwdPolicySubentry}" -a ! "${MY_LDAP_DEFAULTPWDPOLICYDN}" ]; then
      echo "${MY_LOG_HEADER} No password policy for ${login}" >&2
      continue
    fi
   # Retrieves user policy pwdMaxAge and pwdExpireWarning attributes
   ldap_search="${MY_LDAP_SEARCHBIN} ${ldap_param} -s base"
   if [ "${pwdPolicySubentry}" ]; then
      ldap_search="${ldap_search} -b ${pwdPolicySubentry}"
   else
      ldap_search="${ldap_search} -b ${MY_LDAP_DEFAULTPWDPOLICYDN}"
   fi
   ldap_search="$ldap_search objectclass=* pwdMaxAge pwdExpireWarning"
   pwdMaxAge=`${ldap_search} | grep -w "pwdMaxAge:" | cut -d : -f 2 \
      | sed "s/^ *//;s/ *$//"`
   pwdExpireWarning=`${ldap_search} | grep -w "pwdExpireWarning:" | cut -d : -f 2
\
      | sed "s/^ *//;s/ *$//"`

   # Replace MAIL_DELAY by pwdExpireWarning if exists
   MY_MAIL_DELAY=${MY_MAIL_DELAY:=$pwdExpireWarning}
   # Retrieves time difference between today and last change.
   if [ "${pwdChangedTime}" ]; then
      s=`echo ${pwdChangedTime} | cut -c 13-14`
      m=`echo ${pwdChangedTime} | cut -c 11-12`
      h=`echo ${pwdChangedTime} | cut -c 9-10`
      d=`echo ${pwdChangedTime} | cut -c 7-8`
      M=`echo ${pwdChangedTime} | cut -c 5-6`
      y=`echo ${pwdChangedTime} | cut -c 0-4`
      currentTime=`getTimeInSeconds`
      pwdChangedTime=`getTimeInSeconds "$y $M $d $h $m $s"`
      diffTime=`expr ${currentTime} - ${pwdChangedTime}`
   fi
   # Go to next user if password already expired
   expireTime=`expr ${pwdChangedTime} + ${pwdMaxAge}`
        # echo $name $pwdChangedTime $pwdMaxAge $currentTime $expireTime
   if [ ${currentTime} -gt ${expireTime} ]; then
      nb_expired_users=`expr ${nb_expired_users} + 1`
      echo "${MY_LOG_HEADER} Password expired for ${login}" >&2
      continue
   fi
   # ALL LDAP attributes should be there, else continue to next user
   if [ "${mail}" -a "${name}" \
      -a "${login}" -a "${diffTime}" -a "${pwdMaxAge}" ]
   then
      # Ajusts time with delay
      diffTime=`expr ${diffTime} + ${MY_MAIL_DELAY}`
                if [ ${diffTime} -gt ${pwdMaxAge} ]; then
         logmsg="${MY_MAIL_BODY}"
         logmsg=`echo ${logmsg} | sed "s/%name/${name}/; \
            s/%login/${login}/"`

         # Sending mail...
         echo "${logmsg}" | ${MY_MAIL_BIN} -s "${MY_MAIL_SUBJECT}" ${mail} >&2

         # Print debug information on STDERR
         echo "${MY_LOG_HEADER} Mail sent to user ${login} (${mail})" >&2

         # Increment warning counter
         nb_warning_users=`expr ${nb_warning_users} + 1`
      fi
   fi

done < ${result_file}

# Print statistics on STDOUT
echo "${MY_LOG_HEADER} --- Statistics ---"
echo "${MY_LOG_HEADER} Users checked: ${nb_users}"
echo "${MY_LOG_HEADER} Account expired: ${nb_expired_users}"
echo "${MY_LOG_HEADER} Account in warning: ${nb_warning_users}"

# Delete temporary files
rm -rf ${tmp_dir}

# Exit
exit 0
```

Smart Cloud Enterprise Tivoli Service Automation Manager Security Guide

Redpaper™

TSAM Server security setup

Maximo ID management

General security procedures in a cloud environment

The security for Tivoli Service Automation Manager primarily relies on the underlying components of IBM DB2, WebSphere Application Server, and IBM Tivoli Directory Server. The configuration steps to enable and manage security for Tivoli Service Automation Manager and the operational procedures to manage the environment after it is set up are described in this guide. It assumed that the Tivoli Service Automation Manager server is installed and operational. The security best practices that are used in this guide are based on real scenarios that are used in the IBM SmartCloud Enterprise. We also provide some sample scripts that were developed to help simply the tasks for creating and managing Maximo administrators and users.

This IBM Redpaper is intended for IT personnel who install and configure security for Tivoli Service Automation Manager.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks