Release Notes

IBM® Tivoli® Identity Manager

IBM Security Access Manager for Enterprise Single Sign-On Adapter

for Tivoli Directory Integrator

Version 5.1.13

First Edition (Sep 12, 2014)

This edition applies to version 5.1 of Tivoli Identity Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Table of Contents

Preface

Welcome to the IBM® Tivoli Identity Manager IBM Security Access Manager® for Enterprise Single Sign-On Adapter.

These Release Notes contain information for the following products that was not available when the IBM Tivoli Identity Manager manuals were printed:

- Tivoli Access Manager E-SSO Adapter Installation and Configuration Guide

Adapter Features and Purpose

The IBM Security Access Manager for Enterprise Single Sign-On (ISAM ESSO) Adapter is designed to create and manage User Accounts on the ISAM ESSO platform. The adapter runs in “agentless” mode and communicates using HTTPS and LDAP protocol.

IBM recommends the installation of this Adapter (and the prerequisite Tivoli Directory Integrator) on each node of an Identity Manager WAS cluster. A single copy of the adapter can handle multiple Tivoli Identity Manager Services. The optimum deployment configuration is based, in part, on the topology of your network domain, but the primary factor is the planned structure of your Identity Manager Provisioning Policies and Approval Workflow process. Please refer to the Identity Manager Information Center for a discussion of these topics.

The Identity Manager Adapters are powerful tools that require Administrator Level authority. Adapters operate much like a human system administrator, creating accounts, permissions and home directories. Operations requested from the Identity Manager server will fail if the Adapter is not given sufficient authority to perform the requested task. IBM recommends that this Adapter run with administrative (root) permissions.

Service Groups Management

The ability to manage service groups is a new feature introduced in Tivoli Identity Manager 5.1. By service groups, Tivoli Identity Manager is referring to any logical entity that can group accounts together on the managed resource.

Managing service groups implies the following:

Create service groups on the managed resource.
Modify attribute of a service group.
Delete a service group.

Note that service group name change is not supported in Tivoli Identity Manager 5.1 release.

The ISAM ESSO Adapter does not support service groups management.

Contents of this Release

Adapter Version

Component	Version
Release Date	September 12, 2014
Adapter Version	5.1.13
Component Versions	Adapter Build: 015 Profile: 5.1.13.18 AL version: 5.1.13.18 Dispatcher: 5.722 or higher (packaged separately)
Documentation	Directory Integrator-Based Tivoli Access Manager E-SSO Adapter Installation and Configuration Guide (SC23-9665-00)

New Features

Enhancement #	Description
	Items included in current release
52663	Using service attribute as third attribute in TAM ESSO adapter
53477	User lookup and filtered reconciliation
Internal	New workflow extension method to prevent multiple IMS accounts from being created for a user
Internal	Support for IBM Security Access Manager for Enterprise Single Sign-On v8.2.1 and v8.2.2
	Items included in v5.1.12
INTERNAL	Improved error handling support
	Items included in v5.1.10
MR0617096010	Support for suspend and restore operation.
	Items included in v5.1.9
MR020711269	Support for 3 and 4 data items in Account Data Templates with ISAM ESSO v8.2 IMS
INTERNAL	Support for IBM Security Access Manager for Enterprise Single Sign-On v8.2
INTERNAL	Support for IBM Tivoli Directory Integrator v7.1

Closed Issues

APAR#	PMR# / Description
	Items closed in current version
IV53748	Single field credentials are unsupported
Internal	Handle the Pre-provision IMS User and Create Wallet as a single atomic operation
	Items closed in v5.1.12
IV44611	ISAMESSO Adapter not functioning correctly with IMS cluster
	Items closed in v5.1.11
N/A	Documentation update for Workflow Extension configuration.
	Items closed in v5.1.10
IV19868	Shared Account Workflow must support retry mechanism in ITIM
	Items closed in v5.1.9
N/A	Support for TAM E-SSO 8.1
N/A	Support password change operation (INT00030)
N/A	Support Web Service for reconciliation operation (INT00009)
IV02385	Workflow extension does not use service defined port number for IMS Bridge
IZ79618	Issue with sessionid handling of TAM ESSO adapter
IZ61714	TAM ESSO Adapter (tamessowfe.jar) is not compatible with JDK on TIM 4.6
IZ65335	Fail to manage credential if user name is uid@domain format

IV11276	Adapter v5.1.7 incompatible with TDI v6.1.1

Known Issues

APAR# / MR# / Reference #	PMR# / Description
N/A	When AD sync in enabled on IMS server, then the AD account must exist before the TAMESSO account can be provisioned.
MR0204114026	IMS Bridge Name in TIM Service Form is case sensitive.
N/A	Some users present in the IMS server are not processed by TIM. When performing reconciliation, when the "Strip domain name from user ID during reconciliation" option is not selected, the reconciliation gives the following warning message: "CTGIMD014I reconciliation entries were not processed for the following entries: eruid=<full domain name>\\<ims user name>". This problem is caused by TIM "invalid escape sequence" exception. To overcome this issue, perform the COMMON TASKS section of the TIM 5.1 FP3 documentation 5.1.0.3-TIV-TIM-FP0003.README.
N/A	IMS MAc-only users can not be deleted using the adapter
N/A	Case sensitivity issue when using filtered reconciliation for TAM E-SSO accounts. When performing a filtered reconciliation of TAM E-SSO accounts, it is case sensitive. That is, if performing a reconciliation with filter (eruid=K*) in TIM then TAM E-SSO accounts that start with a capital letter 'K' will be returned, but those starting with lower case letter 'k' will be removed and vice versa. To overcome this issue, the filters used should take case sensitivity into account. That is, it is advised that filters such as the following should be used: (|(eruid=k*)(eruid=K*)).
N/A	After ITIM upgraded, workflow extension xml and jar file are deleted. Refer to User Guide to configure workflow extension again.
N/A	Dynamic TAM ESSO Profiles are not supported
N/A	If more than one Group Sharing Role are assigned to a person only one email will be sent to the owner of first role. Owner of second role will not be notified.
N/A	Non-direct TAM ESSO Profiles are not supported
1613299	eruid Format for provisioning TAM ESSO Account to IMS 8.2 Server

Installation and Configuration Notes

See the IBM Tivoli Identity Manager Adapter Installation Guide for detailed instructions.

Deprecation Notice

The Group Sharing Account feature in this version of IBM Security Access Manager for Enterprise Single Sign-On Adapter will not be supported beginning with IBM Security Identity Manager v6.0. The Privileged Identity Management feature is recommended as a replacement for the Group Sharing Account feature.

Additions to Installation Guide

The following additions to the Installation Guide apply to this release.

The adapter files has been renamed as follows:
TAMESSOConnector.jar → SAMESSOConnector.jar
TAMESSOWfe.jar → SAMESSOWfe.jar

Configuration Notes

The following configuration notes apply to this release:

AccessAgent cache wallets

Users MUST cache their wallets on the client machines in order for AccessAgent to process their credentials.

Active Directory password sync in IMS

Prior to TAMESSO v8.1, if IMS is configured for Enterprise Directory password sync AND if an IMSAccount is provisioned before the AD account, the IMSAccount ID must include the domain (example: ibm.com\alblair). Beginning with TAMESSO v8.1, if IMS is configured for Enterprise Directory password sync the AD account must exist before the TAMESSO account can be provisioned.

Support for up to 4 items in Account Data Templates

Beginning with ISAM ESSO v8.2, support for account data templates has been expanded to include up to 4 data items in the credentials. To configure an ITIM service for the additional data templates, perform the following pre-requisite steps:

1. Perform the installation steps as detailed in the Installation Guide. Replace any occurrence of:
   a) **TAMESSOConnector.jar** with **SAMESSOConnector.jar**
   b) **TAMESSOWfe.jar** with **SAMESSOWfe.jar**
2. Stop the Websphere Application Server Enterprise Application for TIM.
3. Extract the **subforms.zip** archive into a temporary folder.
4. Copy the folder and the files in **subforms\samesso** to the appropriate directory:
   ```
   WEBSPHERE_HOME\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME\I
   TIM.ear\itim_console.war\subforms\samesso
   ```
5. Restart the Websphere Application Server Enterprise Application for TIM.

To setup a specific TIM Service for ISAM ESSO credential management, perform the following steps:

1. Ensure an existing ISAM ESSO service has already been setup and configured, as detailed in the Installation Guide.
2. Logon to the TIM Administrator Console
3. Select **Configure System** and then **Design Forms**.
4. Double-click **Service** and then double-click the specific service .
5. From the Attribute List, double-click the **erservicessomapping** attribute, which then appears under the service Tab on the design form.
6. From the **Properties** menu, change the **Label** for this attribute to be **ISAM ESSO Authentication Service**.
7. Click on the $**erservicessomapping** attribute on the main panel to select it.
8. Click on the menu **Attribute** then **Change To** then **Subform**.
9. The **Subform Editor** window will appear. Enter the value **samesso/samesso.jsp** for the **customServletURI** attribute.
10. Click **OK** to close the **Subform Editor**.
11. Click **OK** and then save the design form.
12. On the TIM navigation pane, select **Manage Services**.
13. Find the service that requires ISAM ESSO integration and click on it to show the **Change Service** form.
14. Click on the **Details** button for the **ISAM ESSO Authentication Service** label to display the **SAMESSO Authentication Service Information** Subform popup.
15. Fill in the authentication service ID under the **Authentication Service ID** field and select the appropriate **Account Data Template** for that authentication service.

    Hint: To obtain details about the authentication service ID, login to the **IMS Configuration Utility** and select **Authentication Services** from the **Basic Settings** menu to show a list of available authentication services. Select the appropriate authentication service to view the authentication service ID and the account data template.
16. If necessary, complete the Second Key attribute mapping and Second Secret attribute mapping with the attribute name from the ITIM service or account schema. The attribute value from the service or account is saved as the second key or second secret in IBM Security Access Manager for Enterprise Single Sign-On. If the Second Key or Second Secret is a constant value, then add the prefix '@' in the text. For example: @sampleConstantValue

    Hint: To get the attribute name from the service or account schema:

    a) Click **Configure System** > **Manage Service Types**.
    b) Select the service type corresponding to the service being integrated.
    c) Select the **Service** tab for the service schema or **Account** tab for account schema.
    d) Click the attribute to view its schema name. Use the schema name for the attribute mapping field.
17. Click **OK** to save the configuration in the subform and close it.

Usage Note: When an account attribute is modified, the changes are not automatically propagated to ISAM ESSO server. This is because there is no workflow extension to trigger the ISAM ESSO Adapter. Therefore, when a second key or second secret value is changed, an explicit password change operation for the corresponding account must be performed.

Limitation: If a data template with second key attribute is specified then the account must contain a value for the corresponding attribute when performing an add, change password or delete operation.

Configuring Workflow Extensions

The Workflow Extension (SAMESSOWfe.jar) has been changed. To use the new Workflow Extension, the ITIM Workflow must be configured according to the following instructions.

The following instructions supersedes the instructions in the Install Guide Chapter 2 “Configuring Tivoli Access Manager E-SSO workflow extensions: Defining workflows with extensions” and “Configuring Group Sharing Account workflow extensions: Defining workflows with extensions”.

Defining workflows with extensions

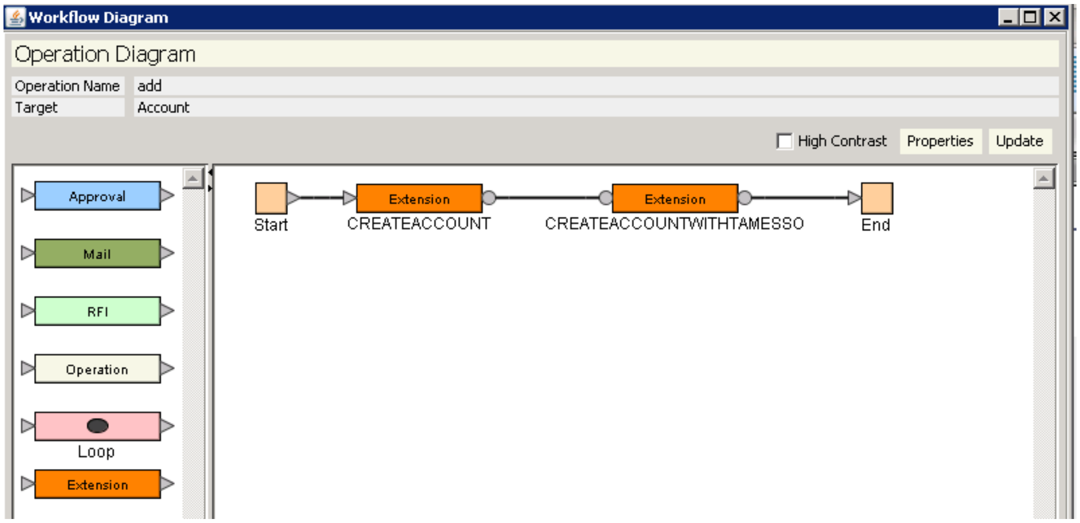
1. Log on to Tivoli Identity Manager.
   a) Select **Configure System** then **Manage Operations.**
   b) For the **Operation Level**, select **Entity level**.

   *Note: If all Account types are to be integrated with the IBM Security Access Manager ESSO service, select **Entity type level** as the Operation Level.*

   c) Select **Account** as the **Entity type**.
   d) Select the type of account to be integrated with the IBM Security Access Manager ESSO service.

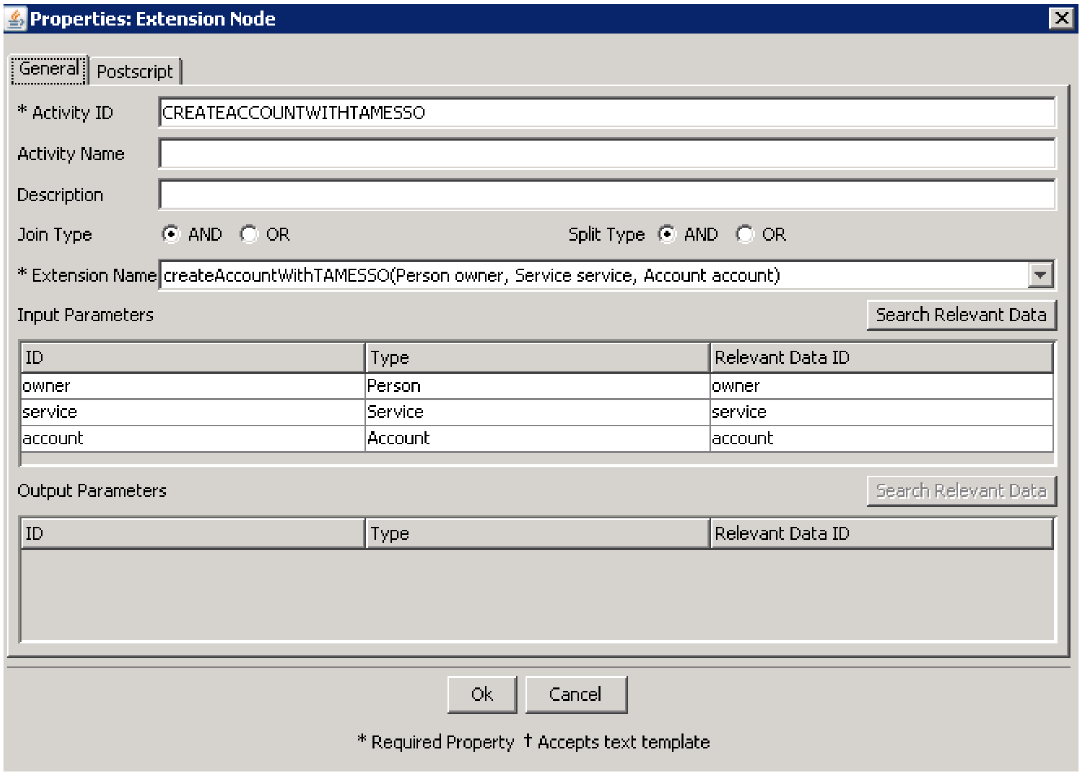
   *Note: If you want to integrate the ITIM Account with the service, select **Identity Manager User** as the **Entity type**.*

2. Click **Add** to create an add operation if it does not exist. The operation diagram is displayed.



Operation Name add
Target Account

3. Remove the transition from **CREATEACCOUNT** to **End**.
4. Add an extension node between **CREATEACCOUNT** and **End**.
5. Double-click on the new **Extension** node. A pop-up window displays all the extensions registered using workflowextensions.xml.
6. In the **Activity ID** field type **CREATEACCOUNTWITHTAMESSO**.
7. Select **createAccountWithTAMESSO** as the **Extension Name**.



Properties: Extension Node

* Activity ID: CREATEACCOUNTWITHTAMESSO

Activity Name:

Description:

Join Type ● AND ○ OR   Split Type ● AND ○ OR

* Extension Name: createAccountWithTAMESSO(Person owner, Service service, Account account)

Input Parameters

ID	Type	Relevant Data ID
owner	Person	owner
service	Service	service
account	Account	account

Output Parameters

ID	Type	Relevant Data ID

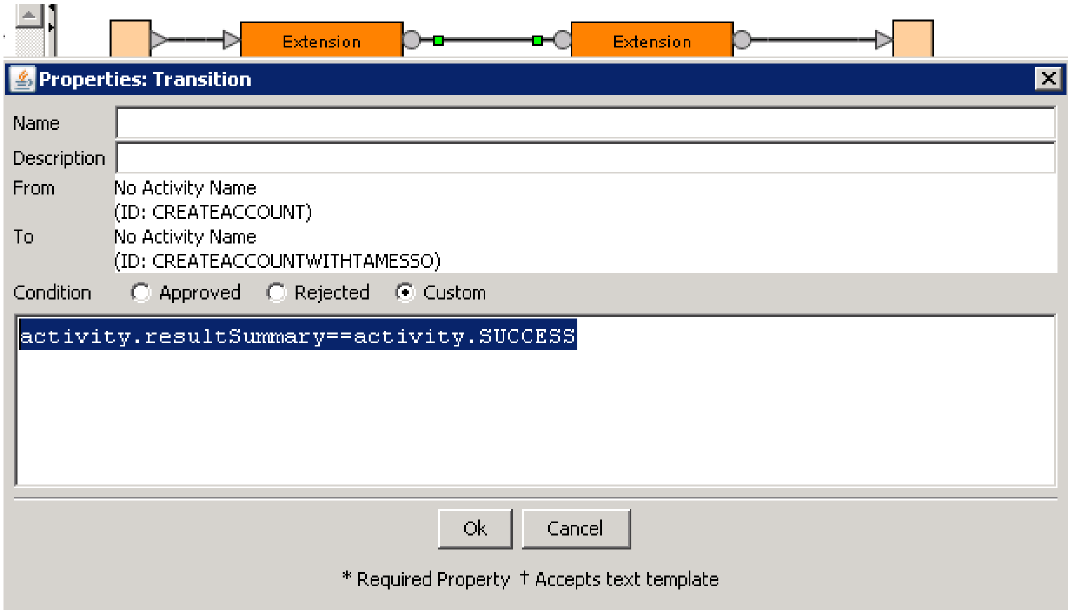
* Required Property † Accepts text template

8. Click **Ok** and attach the transitions to the newly-added extension.

9. Double click on the transition from **CREATEACCOUNT** to **CREATEACCOUNTWITHTAMESSO** to edit the properties.

10. Click **Custom** and type the following code:

```
activity.resultSummary==activity.SUCCESS
```



Properties: Transition

Name:

Description:

From: No Activity Name
(ID: CREATEACCOUNT)

To: No Activity Name
(ID: CREATEACCOUNTWITHTAMESSO)

Condition ○ Approved ○ Rejected ● Custom

```
activity.resultSummary==activity.SUCCESS
```

* Required Property † Accepts text template

11. Click **Ok** to close the property window.

12. Click **Update** and then click **OK**.
13. Click **Close** to close the Operations window.
14. Repeat Steps 2 to 13 for **changePassword** and **delete** operations, or the **add** operation for ITIM account.

Note: When configuring the properties of the new extension nodes (see step 6) for these operations, the following values can be used:

Entity	Operation	ActivityID	Extension Name
Account	changePassword	CHANGEPASSWORDWITHTAMESSO	changePasswordWithTAMESSO
Account	delete	DELETEACCOUNTWITHTAMESSO	DeleteAccountWithTAMESSO
ITIM account	add	CREATEACCOUNTWITHTAMESSO	createITIMAccountWithTAMESSO

Redefining IBM Security Access Manager Enterprise Single Sign-On account add operation

You must redefine the IBM Security Access Manager Enterprise Single Sign-On account add operation to prevent duplicate accounts from being created.

1. Select **Configure System** then **Manage Operations**.
2. Select **Entity level** as the **Operation Level**.
3. Select **Account** as the **Entity type**.
4. Select **ISAM ESSO Account** for **Entity**.
5. Click the **Refresh** button to get a list of operation changes from default.
6. Take one of the following actions:
   - If the add operation is not on the list, click **Add** and define the **Operation Name** as `add`. Click **Continue** to modify the workflow.
   - If the **add** operation is on the list, click the operation to modify the workflow.
7. Modify the operation workflow:

   a) Add an Extension node between **Start** and **CREATEACCOUNT**.

   b) Configure the extension node to use Extension Name **noExistingSSOAccount** and provide an Activity ID, for example NOEXISTINGSSOACCOUNT. Set the Split Type to **OR**.

   c) Double-click the transition from **NOEXISTINGSSOACCOUNT** to **CREATEACCOUNT** to edit the properties.

   d) Click **Custom** and type the following code:

   ```
   activity.resultSummary==activity.SUCCESS
   ```

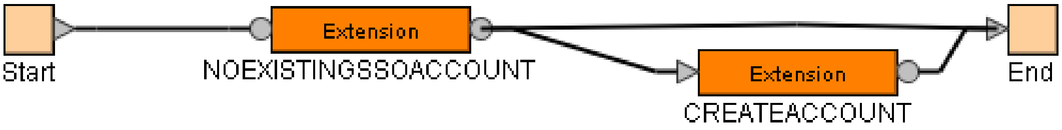
   e) Create a transition from the **NOEXISTINGSSOACCOUNT** node to the **End** node.

   f) Double-click the transition from **NOEXISTINGSSOACCOUNT** node to **End** node to edit the properties.

   g) Click Custom and type the following code:

   ```
   if(activity.resultSummary==activity.FAILED){
       WorkflowRuntimeContext.setProcessResult(process.FAILED);
       return true;
   }
   ```

2. Click **Update**. The workflow is displayed.



3. Click on **OK**.
4. Click **Close** to close the Operations window.

Configuring Group Sharing Account workflow extensions: Defining workflows with extensions

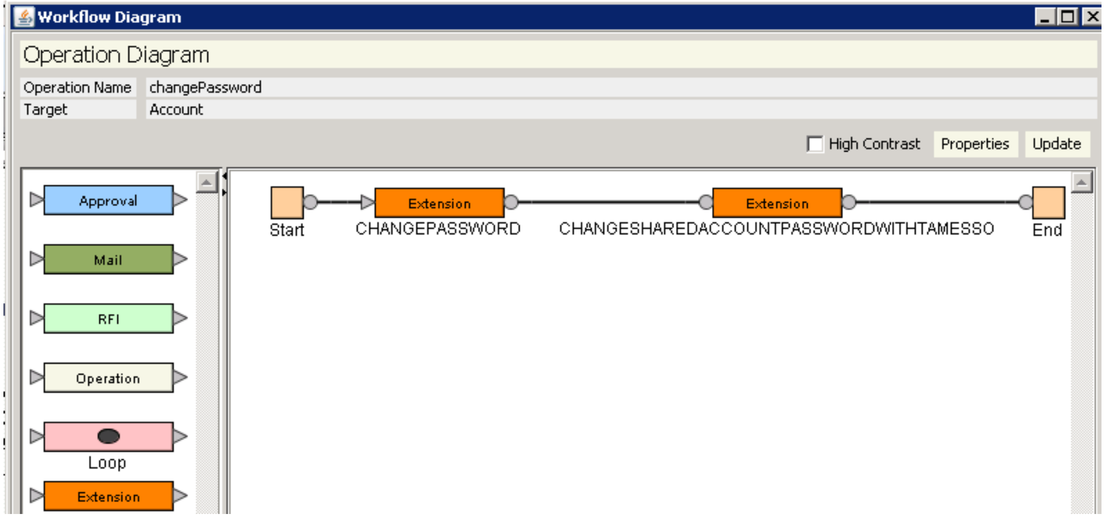
1. Log on to Tivoli Identity Manager.
   a) Select **Configure System** then **Manage Operations.**
   b) For the **Operation Level**, select **Entity level**.

   *Note: If all Account types are to be integrated with the IBM Security Access Manager ESSO service, select **Entity type level** as the **Operation Level**.*

   c) Select **Account** as the **Entity** type.
   d) Select the type of account to be integrated with the IBM Security Access Manager ESSO service.

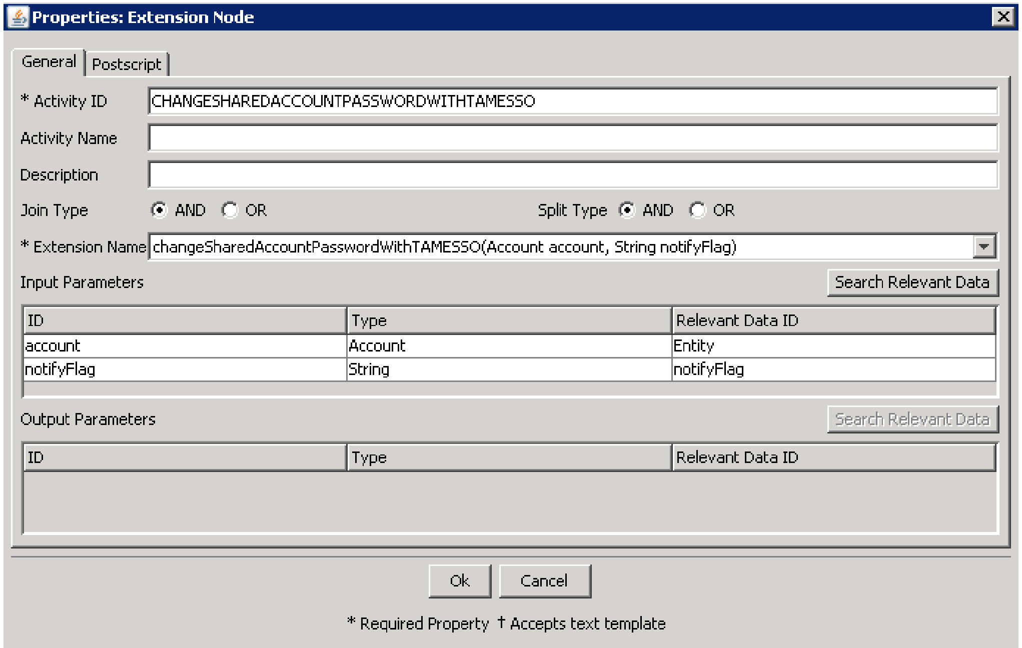
   *Note: If the **ITIM Account** is to be integrated with the IBM Security Access Manager ESSO service, select **Identity Manager User** as the **Entity type**.*

2. Click the Add button to create a **changePassword** operation if it does not already exist. The operation diagram is displayed. Provide the same changes shown in the following screen capture.



Operation Name changePassword
Target Account

3. Remove the transition from **CHANGEPASSWORD** to **End**.
4. Add a new extension node between **CHANGEPASSWORD** and **End**.
5. Double-click on the new **Extension** node. A pop-up window displays all the extensions registered using workflowextensions.xml.
6. Select the Extension Name as **changeSharedAccountPasswordWithTAMESSO** and fill in the Activity ID with **CHANGESHAREDACCOUNTPASSWORDWITHTAMESSO**



* Activity ID: CHANGESHAREDACCOUNTPASSWORDWITHTAMESSO

Activity Name:

Description:

Join Type: ● AND ○ OR Split Type: ● AND ○ OR

* Extension Name: changeSharedAccountPasswordWithTAMESSO(Account account, String notifyFlag)

Input Parameters

ID	Type	Relevant Data ID
account	Account	Entity
notifyFlag	String	notifyFlag

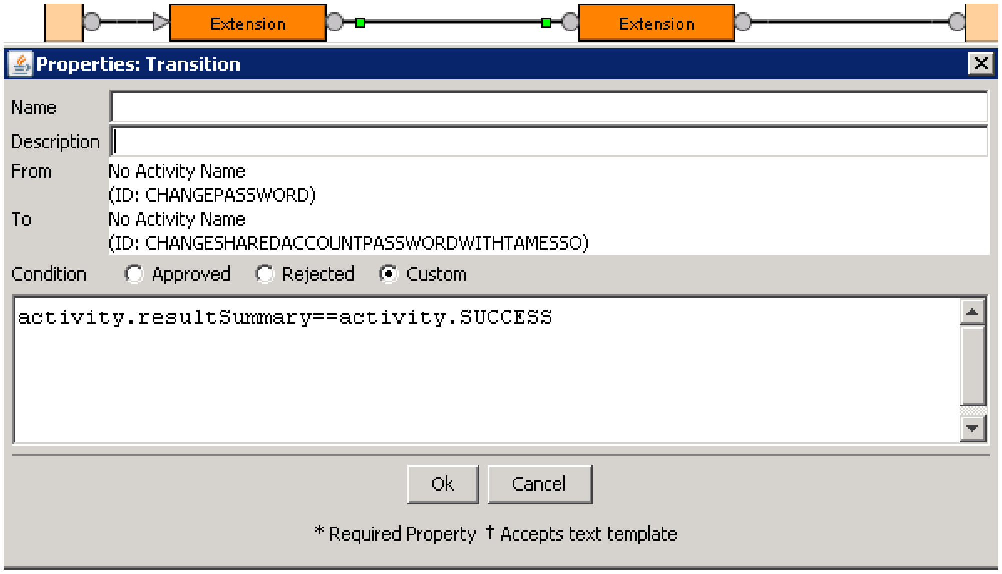
Output Parameters

ID	Type	Relevant Data ID

* Required Property † Accepts text template

7. Click **Ok** and attach the transitions to the newly-added extension.
8. Double click on the transition from **CHANGEPASSWORD** to **CHANGESHAREDACCOUNTPASSWORDWITHTAMESSO** to edit the properties.
9. Select the **custom** radio button and insert the following code:

```
activity.resultSummary==activity.SUCCESS
```



Name:

Description:

From: No Activity Name (ID: CHANGEPASSWORD)

To: No Activity Name (ID: CHANGESHAREDACCOUNTPASSWORDWITHTAMESSO)

Condition: ○ Approved ○ Rejected ● Custom

```
activity.resultSummary==activity.SUCCESS
```

* Required Property † Accepts text template

10. Click **Ok** to close the property window.
11. Click **Update** and then click **OK** at the bottom of the screen.
12. Click **Close** to close the Operations window.

You may need to define a workflow extension for the modify operation for Person. Refer to the **Directory Integrator-Based Tivoli Access Manager E-SSO Adapter Installation and Configuration Guide (SC23-9665-00)** page 22, under the section **Configuring Group Sharing Account workflow**

extensions: Defining workflows with extensions for instructions on defining a workflow extension for modify operation for Person.

Upgrading

This section provides information upgrading from previous adapter versions.

Upgrading From Adapter Version 5.1.9

If you have applied workflow extensions from Adapter version 5.1.9 or older, you must change the operations defined in ITIM according to the steps from the "Workflow Extensions" section in this document.

If you are upgrading from Adapter version 5.1.8 or older, please refer to the following section for additional upgrade steps.

Upgrading From Adapter Version 5.1.8 or older

If you have Adapter version prior to v5.1.8, you must perform an upgrade to v5.1.8 first before attempting the following upgrade instructions.

The adapter files has been renamed as follows starting from v5.1.9:
TAMESSOConnector.jar → SAMESSOConnector.jar
TAMESSOWfe.jar → SAMESSOWfe.jar

In addition, the archive subforms.zip is included in the installation package. The files in this archive consists of:

1. subforms\samesso\samesso.css
2. subforms\samesso\samesso.js
3. subforms\samesso\samesso.jsp
4. subforms\samesso\samesso_utils.jspf

To upgrade from v5.1.8 of the Adapter, perform the following steps:

1. Stop the Tivoli Directory Integrator RMI Dispatcher service that is used by the Adapter.
2. Copy **SAMESSOConnector.jar** to the *TDI_HOME*\jars\connectors folder.
3. Restart the Tivoli Directory Integrator RMI Dispatcher service that is used by the Adapter.
4. Stop the Websphere Application Server Enterprise Application for TIM.
5. Copy **SAMESSOWfe.jar** from the installation package to the appropriate directory:

   ```
   WEBSPHERE_HOME\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME\I
   TIM.ear\app_web.war\WEB-INF\lib
   ```

6. In the same directory as the previous step, delete the file **TAMESSOWfe.jar**
7. Copy the folder and the files extracted from **subforms.zip** to the appropriate directory:

   ```
   WEBSPHERE_HOME\AppServer\profiles\SERVER_NAME\installedApps\NODE_NAME\I
   TIM.ear\itim_console.war\subforms\samesso\
   ```

8. Restart the Websphere Application Server Enterprise Application for TIM.
9. Perform the steps in the section **Importing the adapter profile into the Tivoli Identity Manager Server** under **Chapter 3** of the Installation Guide.

Customizing or Extending Adapter Features

The Identity Manager adapters may be customized and/or extended. The type and method of this customization may vary from adapter to adapter.

Getting Started

Customizing and extending adapters requires a number of additional skills. The developer must be familiar with the following concepts and skills prior to beginning the modifications:

- Tivoli Identity Manager administration
- Tivoli Directory Integrator management
- Tivoli Directory Integrations assemblyline development
- LDAP schema management
- Working knowledge of Java scripting language
- Working knowledge of LDAP object classes and attributes
- Working knowledge of XML document structure

Note: If the customization requires a new Tivoli Directory Integrator connector, the developer must also be familiar with Tivoli Directory Integrator connector development and working knowledge of Java programming language.

Tivoli Identity Manager Resources:

Check the “Learn” section of the Tivoli Identity Manager Support web site for links to training, publications, and demos.

Tivoli Directory Integrator Resources:

Check the “Learn” section of the Tivoli Directory Integrator Support web site for links to training, publications, and demos.

Tivoli Identity Manager Adapter Development:

Adapter Development Tool

The Adapter Development Tool, ADT, is a tool used by IBM Tivoli Identity Manager (ITIM) customers and consultants to create custom Tivoli Identity Manager adapters. It reduces adapter delivery time by about 50% and it helps in the development of custom adapters. The Adapter development tool is available on the IBM Open Process Automation Library (OPAL).

Support for Customized Adapters

The integration to the Identity Manager server – the adapter framework – is supported. However, IBM does not support the customizations, scripts, or other modifications. If you experience a problem with a customized adapter, IBM Support may require the problem to be demonstrated on the GA version of the adapter before a PMR is opened.

Supported Configurations

Installation Platform

The IBM Tivoli Identity Manager Adapter was built and tested on the following product versions.

Adapter Installation Platform:

This adapter installs into Tivoli Directory Integrator (TDI) and may be installed on any platform supported by the TDI product and supported by the target system libraries or client, where applicable. IBM recommends installing TDI on each node of the Tivoli Identity Manager WAS Cluster and then installing this adapter on each instance of TDI. Supported TDI versions include:

Tivoli Directory Integrator 6.1.1 with Fix Pack 5 or higher
Tivoli Directory Integrator 7.0 with Fix Pack 1 or higher
Tivoli Directory Integrator 7.1

Managed Resource:

Tivoli Access Manager for Enterprise Single Sign-On v8.1
IBM Security Access Manager for Enterprise Single Sign-On v8.2
IBM Security Access Manager for Enterprise Single Sign-On v8.2.1
IBM Security Access Manager for Enterprise Single Sign-On v8.2.2

IBM Tivoli Identity Manager:

Identity Manager v5.1

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 give 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged should contact:

IBM Corporation
2ZA4/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

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.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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

End of Release Notes