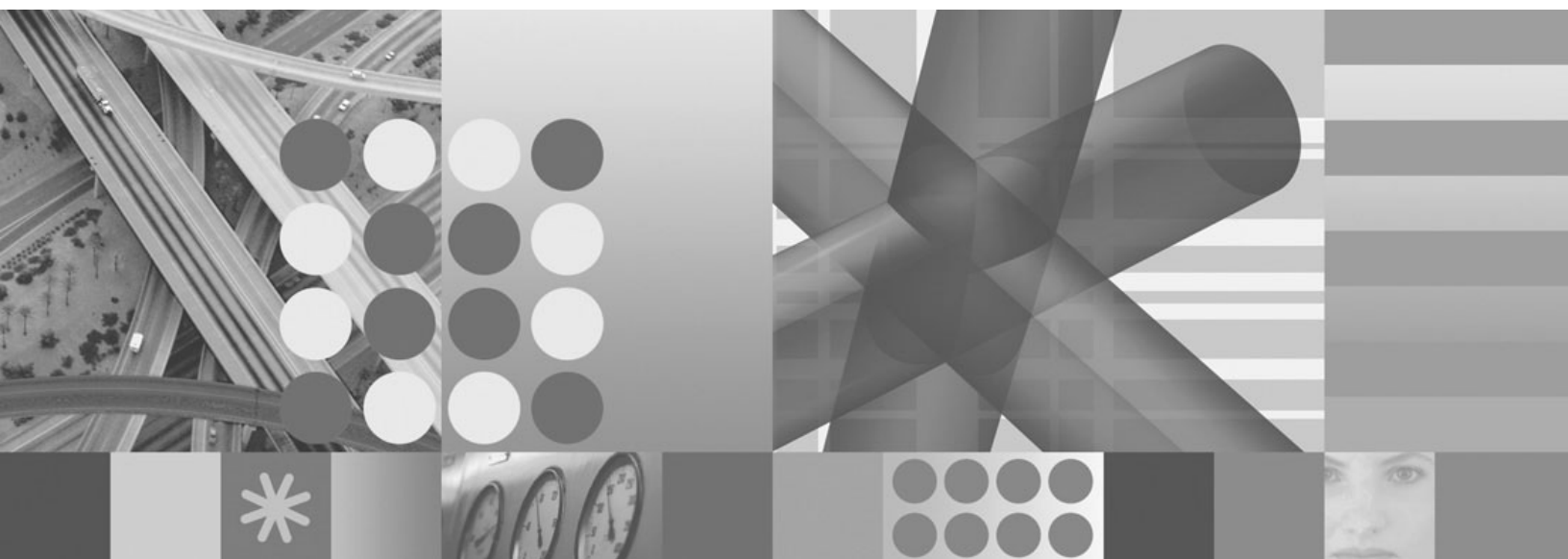


for Versions 4.1 and 5.1



**GSO/Active Directory Password Synchronization
using Tivoli Directory Integrator**

for Versions 4.1 and 5.1



**GSO/Active Directory Password Synchronization
using Tivoli Directory Integrator**

Note

Before using this information and the product it supports, read the information in Appendix B, “Notices,” on page 25

Third Edition (November 2004)

This edition applies to version 2.0.04 of the Tivoli Access Manager/GSO/Active Directory Password Synchronization integration using IBM Tivoli Directory Integrator, and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces previous versions.

© Copyright International Business Machines Corporation 2004. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	v
Who should read this book	v
Publications	v
Base Information	v
WebSEAL Information	v
Tivoli Directory Integrator Information	vi
Accessing Publications Online	vi
Contacting Software Support.	vi
Tivoli technical training	vi
Conventions Used in this Book.	vii
 Chapter 1. Introducing Password Synchronization with IBM Tivoli Directory Integrator. . .	1
Introduction	1
Before You Start	1
Integration Product Version Information	3
Integration Package Contents	3
 Chapter 2. Setup and Planning	5
Overview	5
Environment Setup	6
Single or Bi-Directional Mode Options.	6
Active Directory server	8
IBM Directory Server	8
IBM Tivoli Directory Integrator	8
Assembly Line Connectors Overview	11
Eventhandlers	11
Connectors	11
 Chapter 3. Configuring and Installing the Assembly Line	13
Configuring the External Properties File	13
Configuring the Assembly Line.	15
Running the Assembly Line	15
Running the Assembly Line from the Configuration Editor	16
Running the Assembly Line from the Command Line	16
Checking Installation and Configuration Success	17
Uninstallation	17
 Chapter 4. Troubleshooting and Issues.	19
Troubleshooting	19
Known Problems and Issues.	19
Expected Behavior	20
 Appendix A. IBM Software Support	21
Determine the business impact of your problem	21
Describe your problem and gather background information	22
Submit your problem to IBM Software Support	22
Searching knowledge bases	22
Search the information center on your local system or network	23
Search the Internet	23
Obtaining fixes	23
 Appendix B. Notices	25
Trademarks	27

Preface

This guide details a password synchronization solution that uses an IBM® Tivoli® Directory Integrator Assembly Line, combined with password change capture plug-ins, to synchronize passwords in real time between Microsoft® Active Directory®, IBM Directory Server and IBM Tivoli Access Manager GSO credentials.

Who should read this book

This guide is for those responsible for the installation, deployment and administration of IBM Tivoli Access Manager. The reader should be familiar with the administration of Tivoli Access Manager, including Tivoli Access Manager WebSEAL.

Readers should also be familiar with the following products, systems and concepts:

- IBM Tivoli Directory Integrator
- IBM Directory Server
- IBM Java® Runtime Environment (JRE)
- Microsoft Active Directory
- PC and UNIX® operating systems,
- Security management,
- Internet protocols, including HTTP, HTTPS and TCP/IP,
- Lightweight Directory Access Protocol (LDAP) and directory services,
- A supported user registry,
- Authentication and authorization.

Publications

The following publications complement the information contained in this guide:

Base Information

- *IBM Tivoli Access Manager Base Installation Guide*
Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.
- *IBM Tivoli Access Manager Base Administrator's Guide*
Describes the concepts and procedures for using Access Manager services. Provides instructions for performing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Tivoli Access Manager WebSEAL Installation Guide*
Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Tivoli Access Manager WebSEAL Administrator's Guide*
Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Tivoli Access Manager WebSEAL Developer's Reference*
Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Tivoli Directory Integrator Information

- *IBM Tivoli Directory Integrator 5.2 Administrator Interface*
An overview of Tivoli Directory Integrator, including explanations of Tivoli Directory Integrator concepts.
- *IBM Tivoli Directory Integrator 5.2 Reference Guide*
An in-depth guide to developing solutions with Tivoli Directory Integrator.
- *IBM Tivoli Directory Integrator 5.2 Users Guide*
Provides information on administering Tivoli Directory Integrator.

Accessing Publications Online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli software library:

<http://www.ibm.com/software/tivoli/library>

To locate product publications in the library, click the **Product manuals** link on the left side of the page. Then, locate and click the name of the product on the Tivoli Software Information Center page.

Product publications include release notes, installation guides, user's guides, administrator's guides, and developer's references.

Note: To ensure proper printing of PDF publications, select the **Fit to page** drop-down menu in the Adobe Acrobat Print window (which is available when you click **File ▶ Print**).

Contacting Software Support

Contact IBM Software Support by using the methods described in the *IBM Software Support Guide* at the following Web site:

<http://techsupport.services.ibm.com/guides/handbook.html>

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Telephone numbers, depending on the country in which you are located
- A list of information you should gather before contacting customer support

For more information, see Appendix A, "IBM Software Support," on page 21.

Tivoli technical training

For Tivoli technical training information, refer to the IBM Tivoli Education Web site: <http://www.ibm.com/software/tivoli/education>.

Conventions Used in this Book

The following typeface conventions are used in this book:

Bold Lowercase commands or mixed case commands that are difficult to distinguish from surrounding text, keywords, parameters, options, names of Java[®] classes, and objects are in **bold**.

Italic Variables, titles of publications, and special words or phrases that are emphasized are in *italic*.

Monospace

Code examples, command lines, screen output, file and directory names that are difficult to distinguish from surrounding text, system messages, text that the user must type, and values for arguments or command options are in monospace.

Chapter 1. Introducing Password Synchronization with IBM Tivoli Directory Integrator

This chapter has the following sections:

- “Introduction”
- “Before You Start”
- “Integration Product Version Information” on page 3
- “Integration Package Contents” on page 3

Introduction

This solution uses an IBM Tivoli Directory Integrator Assembly Line combined with password change capture plug-ins to synchronize passwords in real time between Microsoft Active Directory®, IBM Directory Server and Tivoli Access Manager GSO credentials.

Passwords are captured at the time of change, before they are encrypted and added to the directory.

For example, consider a Microsoft Exchange® server deployed behind WebSEAL. Single Sign On is achieved using a GSO junction to the Exchange server. When the user signs on to WebSEAL, and is authenticated, their GSO credentials for the junctioned resource are passed to the backend server, achieving seamless Single Sign On to the Exchange server.

If the user were to change their Active Directory password through their desktop, SSO would no longer be achieved, as an administrator would be needed to change the user's Access Manager GSO credentials for the Exchange server.

To overcome this, the assembly line monitors both the directories for password changes and propagates any password changes to the other directory and the Tivoli Access Manager GSO credentials of the user. This ensures that the user has one password for all resources, and reduces the administrative effort involved in changing passwords.

Before You Start

This document assumes there is an existing environment that makes use of at least one Tivoli Access Manager WebSEAL GSO junction to a resource hosted on Microsoft IIS (with Active Directory installed). Although WebSEAL is not a prerequisite for password synchronization, it is required for verification of password change results.

Users must have a valid account on both Active Directory and Tivoli Access Manager (TAM). The TAM account must be enabled for GSO so that GSO credentials can be created and updated. To sign on to a resource running on IIS, the user authenticates to WebSEAL. Then, using a GSO junction and the user's GSO credentials for that particular resource, WebSEAL signs the user onto the requested resource.

This integration requires that password policies on Active Directory and Tivoli Access Manager specify the same (or as close as possible) constraints on user passwords. Failure to enforce this requirement may result in errors in the Assembly Line.

This document does not instruct the reader on creating GSO junctions or administering GSO credentials for users. For further information on these topics, refer to the appropriate Tivoli Access Manager documentation.

Integration Product Version Information

The information provided in this guide is designed for the following product versions:

- IBM Tivoli Directory Integrator 5.2 Fix Pack 8 (plus Password change capture plug-ins for Active Directory and IBM Directory Server)
- Microsoft Active Directory (provided with Windows 2000 Advanced Server)
- Either:
 - IBM Tivoli Access Manager 4.1 with IBM Directory Server 4.1, or
 - IBM Tivoli Access Manager 5.1 with IBM Directory Server 5.2

Integration Package Contents

The integration package contains the following files:

File Name	Description
am_msADPwdSync_int_guide.pdf	This document.
am_msADPwdSync.xml	Assembly line configuration file
am_msADPwdSync.props	Assembly Line properties file.

Chapter 2. Setup and Planning

This chapter contains the following sections:

- “Overview”
- “Environment Setup” on page 6
- “Assembly Line Connectors Overview” on page 11

Overview

IBM Tivoli Directory Integrator Assembly Lines are designed and optimized to work on one item at a time. As users change their passwords, these password changes are added to a queue as password change objects. The Tivoli Directory Integrator Assembly Line retrieves one change item at a time, then propagates the change to the other directory and the Tivoli Access Manager GSO credentials of the user.

The user must have an account in both Active Directory (AD) and IBM Directory Server (IDS). Furthermore, the **sAMAccountName** for their AD account must match the **uid** of their IDS account in order to provide a mapping between the two directories.

Other attributes can be used to provide a mapping between the two directories, for example a new attribute called **SAMAccountName** could be created in the IBM Directory Server (however, this option is beyond the scope of this document and is not documented here).

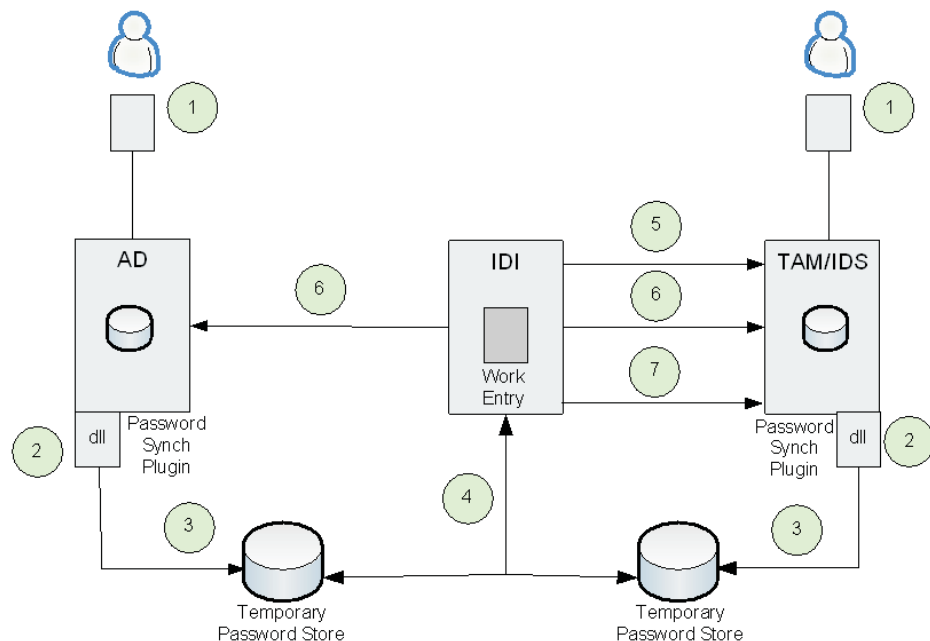


Figure 1. Password Synchronization architecture and event flow

The diagram above shows an overview of the architecture, where the following events occur:

1. User changes password on either Active Directory (AD) or IBM Directory Server (IDS).
2. IBM Tivoli Directory Integrator password capture plug-in intercepts password change before password is encrypted in the directory.
3. The plug-in stores the password change object in a temporary password store (MQe).
4. The MQ password store connector in the Tivoli Directory Integrator Assembly Line monitors the password stores for password change objects. When a password change object is detected, a work entry is built and passed to the next connector in the assembly line.
5. In bi-directional mode, the Assembly Line sets a flag in the user's LDAP entry to prevent further password change propagations occurring when the opposing plug-in captures this password change.

Note: With password capture plug-ins installed on both directories and the Assembly Line operating in bi-directional mode, a password change propagated to the opposing directory will trigger the password change capture plug-in on that directory. The result is an endless ping-pong effect. To counter this, the Assembly Line uses a flag in the user's IDS account (any unused LDAP attribute can be chosen) to detect and abort the second password change.

6. If the password change came from IDS, then the AD password is updated. If the password change came from AD, then the IDS/TAM password is updated.
7. The user's Tivoli Access Manager GSO credentials (if any) that are configured in the external properties file are updated to reflect the password change.

Environment Setup

The components of this scenario utilize three logical servers:

- Active Directory,
- Tivoli Access Manager (with IBM Directory Server),
- IBM Tivoli Directory Integrator.

Physically, Tivoli Directory Integrator can reside on the Active Directory machine, the Tivoli Access Manager machine or a stand alone machine. For best performance, and easier configuration changes, Tivoli Directory Integrator should be installed on a stand alone server. The software and services that must be installed and configured on each of the machines is described in the following sections.

In the following steps, only install the password capture plug-ins on the machines where password changes need to be intercepted. If operating in a single direction then only one directory server will have a plug-in installed. For bi-directional, install password capture plug-ins on both directories.

Single or Bi-Directional Mode Options

The Assembly Line can be run in either bi-directional or single directional mode. Bi-directional means password changes on either the Active Directory or IBM Directory Server machines are captured and propagated to the opposing directory

and the TAM GSO credentials of the user. Running in this mode requires installing password capture plug-ins on both machines and setting the `Single.Direction` entry in the properties file to *no*.

In single direction mode, a password capture plug-in is only installed on the directory where password changes are to be captured. For example, if password changes need to be propagated from Active Directory to IBM Directory Server and TAM GSO, then the password capture plug-in is only installed on the Active Directory machine. The `Single.Direction` option in the external properties file must be set to *yes*.

Setting the Assembly Line to single direction effectively skips those connectors responsible for setting and checking the flag.

To change from bi-directional to single directional mode, follow the steps below.

Note: If IBM Tivoli Directory Integrator is installed on a machine hosting one of the directories, uninstalling the password capture plug-ins from this machine may cause errors in the Assembly Line on startup. This is because installing the plug-in also removes the MQ queue manager component that the MQ password store connector uses for password notifications. Installation of IBM Tivoli Directory Integrator on a standalone machine is recommended.

To disable or remove the plug-in from IBM Directory Server:

1. Locate the IBM LDAP configuration file. In a typical installation this is found at:
`c:\Program Files\IBM\LDAP\etc\ibmslapd.conf`
2. Open the file with a text editor and locate the line (or similar, as the path may differ) that was added in configuring the plug-in:
`ibm-slapdPlugin: preoperation "C:\Program Files\IBM\DiPlugins\IDS\pwsync.dll"
PWSyncInit "C:\Program Files\IBM\DiPlugins\IDS\idspwconfigWin.props"`
3. Comment out the line with a hash symbol (#). For example:
`#ibm-slapdPlugin: preoperation "C:\Program Files\IBM\DiPlugins\IDS\pwsync.dll"
#PWSyncInit "C:\Program Files\IBM\DiPlugins\IDS\idspwconfigWin.props"`
4. Restart IBM Directory Server.
5. If desired, use the **Add/Remove Programs** feature to remove the plug-in.
6. Change the **Single.Direction** attribute in the properties file to *yes*.

To disable or remove the plug-in on Active Directory, the password synchronization plug-in must be uninstalled using **Add/Remove Programs** (you cannot disable it).

To change from single to bi-directional mode, configure the plug-in on the required machine and change the **Single.Direction** property to *no*.

In either bi-directional or single direction mode, changing the GSO password of a user's credentials does not update the directory passwords.

It is also worth noting, that at this stage, GSO credentials cannot be updated on their own without first updating a directory password. This feature may be incorporated in a future enhancement.

Active Directory server

Install the IBM Tivoli Directory Integrator password capture plug-in. After launching the installer, choose **IBM Tivoli Directory Integrator Password Synchronization plug-in for Windows NT/2000** and select **WebSphere MQ Everyplace** for the storage method.

After installation, follow the steps outlined in the following documents, which are located in the install directory of the plug-in:

readme_winpwsync_ismp.htm
readme_mqepwstore_ismp.htm

These documents provide all the steps necessary to configure the plug-in and the password store.

To update passwords on AD, the assembly line connector to Active Directory must use SSL. Install Certificate Services in the Active Directory Domain (ensure that IIS is already installed, and choose **Enterprise root CA** when installing Certificate Services)

IBM Directory Server

Install the IBM Tivoli Directory Integrator password capture plug-in. After launching the installer, choose **IBM Password Synchronization plug-in for IBM Directory Server** and select **WebSphere MQ Everyplace** for the storage method.

After installation, follow the steps outlined in the following documents, which are located in the install directory of the plug-in:

readme_idspwsync_ismp.htm
readme_mqepwstore_ismp.htm

These documents provide all the steps necessary to configure the plug-in and the password store.

Note: If you are using IBM Directory Server 4.1, these documents will contain minor differences because they are aimed at IBM Directory Server 5.1 or 5.2. However, these differences are minor and translate easily to IBM Directory Server 4.1.

After changing the IBM Directory Server configuration file, the IBM Directory Server must be restarted for the changes to take effect and the password changes to be captured.

IBM Tivoli Directory Integrator

For IBM Tivoli Directory Integrator to be able to communicate with Tivoli Access Manager, the Tivoli Access Manager Java Runtime is required. Perform the following steps to configure IBM Tivoli Directory Integrator:

1. Ensure the Tivoli Access Manager Java Runtime is installed on the IBM Tivoli Directory Integrator machine, and that the system variable Path contains the correct path to Java.exe on the machine. If the default installation location for IBM Tivoli Directory Integrator is used, then the required path is:
c:\progra~1\IBM\IBMDirectoryIntegrator_jvm\bin
2. Configure Tivoli Access Manager Java Runtime to use IBM Tivoli Directory Integrator Java Runtime. To do this, open a command window and enter the following commands:

```
cd c:\progra~1\tivoli\policy~1\sbin
```

```
pdjrtecfg -action config -java_home IDI_Java_dir
```

Note: When using Access Manager 5.1 the command will be (entered as one line):

```
pdjrtecfg -action config -host TAM_hostname -port 7135  
-java_home IDI_Java_dir
```

where:

- *IDI_Java_dir* is the Java Directory of IBM Tivoli Directory Integrator. In a typical install, this would be:
c:\progra~1\IBM\IBMDirectoryIntegrator_jvm
- *TAM_hostname* is the Fully Qualified Domain Name of the Tivoli Access Manager server.

3. Configure Tivoli Access Manager Java Runtime to the Tivoli Access Manager Policy Server and Authorization Server. To do this, open a command window and enter the following command (as one line):

```
c:\progra~1\IBM\IBMDirectoryIntegrator\_jvm\bin\java  
com.tivoli.pd.jcfg.SvrSslCfg -action config -admin_id  
sec_master -admin_pwd password -appsvr_id appsvr -mode remote  
-port 999 -policysvr policy_svr:7135:1 -authzsvr  
auth_svr:7136:1 -cfg_file cfg_file_name -key_file  
keyfile_name -cfg_action create
```

The following table describes the available variables:

Variable	Description
admin_id	A Tivoli Access Manager user with administrative privileges.
admin_pwd	Password associated with the Tivoli Access Manager administrative user specified.
appsvr_id	The name of the application server. For example: iditam
mode	Indicates whether the application server processes requests remotely or locally.
port	The TCP/IP port which the application server listens to for policy server notifications.
policysvr	A list of Tivoli Access Manager policy servers to which the application server can communicate. Formatted as: host_name:TCP/IP port number:rank Multiple servers can be specified by separating them with commas. For example: am.example.com:7135:1
authzsvr	A list of Tivoli Access Manager authorizations to which the application server can communicate. Formatted as: host_name:TCP/IP port number:rank Multiple servers can be specified by separating them with commas. For example: am.example.com:7136:1

Variable	Description
cfg_file	Fully qualified name of the configuration file on the application server. For example: C:\idi\tamConfigFile.conf This file will be created during execution of the SvrSslCfg command. Ensure the specified directory exists.
key_file	Fully qualified name of the keystore file on the application server. For example: C:\idi\tamKeyFile.ks This file will be created during execution of the SvrSslCfg command. Ensure the specified directory exists.
cfg_action	Indicates whether the configuration and keystore files should be created on the application server or replaced.

For further information on configuring the Tivoli Access Manager Java Runtime, refer to the *Tivoli Access Manager Authorization Java Classes Developer Reference*.

4. Finally, set up Tivoli Directory Integrator to use SSL with Active Directory as follows:
 - a. Open a Web browser and retrieve the CA certificate from the active directory machine to the local file system:
`http://active_directoryserver/certsrv/`
 - b. Use the **keytool** utility located in the IBM Tivoli Directory Integrator subdirectory to store the certificate just downloaded into a certificate store. Execute the following command (entered as one line):

```
IDI_home_dir\jvm\bin\keytool -import -file certificate_file_name
-keystore key_store_name.jks -storepass password
-alias key_alias_name
```

where:

 - *certificate_file_name* is the full path to the certificate retrieved in the previous step,
 - *key_store_name* is the name that will be given to the keystore that is created,
 - *password* is the password that will be used to protect the keystore being created, and
 - *alias* is an alias that can be used to refer to the keystore being created.

For example:

```
c:\progra~1\IBM\IBMDIRECTORYINTEGRATOR\jvm\bin\keytool -import -file
c:\idi\cert.cer -keystore c:\example\idi.jks -storepass pass
-alias keyAlias
```
 - c. Enter **yes** when prompted to **Trust This Certificate**.
 - d. Edit the Tivoli Directory Integrator properties file to enable Tivoli Directory Integrator to use the new keystore:
 - 1) Open the `global.properties` file located in the IBM Tivoli Directory Integrator root directory.

- 2) Find the sections # server authentication and # client authentication, and modify the values for the keystore file location, the keystore file password and the keystore file type. For example:

```
# server authentication
# example
# javax.net.ssl.trustStore=d:\test\KeyRings\namtp2.jks
# javax.net.ssl.trustStorePassword=secret
# javax.net.ssl.trustStoreType=jks

javax.net.ssl.trustStore=C:\example\idi.jks
javax.net.ssl.trustStorePassword=xxxx
javax.net.ssl.trustStoreType=jks

# client authentication
# example
# javax.net.ssl.keyStore=d:\test\KeyRings\namtp2.jks
# javax.net.ssl.keyStorePassword=secret
# javax.net.ssl.keyStoreType=jks

javax.net.ssl.keyStore=C:\example\idi.jks
javax.net.ssl.keyStorePassword=xxxx
javax.net.ssl.keyStoreType=jks
```

- 3) Restart IBM Tivoli Directory Integrator, if required.

Assembly Line Connectors Overview

This section provides an overview of the **Eventhandlers** and **Connectors** that make up the password synchronization Assembly Line.

Eventhandlers

am_msADPwdSync

The Assembly Line is started from this Event Handler. If the Assembly Line stops for some reason, this component restarts it.

Connectors

MQPwdStore

This connector retrieves password changes from both the queue on the Active Directory machine, as well as the Tivoli Access Manager Machine (with IBM Directory Server). Password change objects in the queues have the following attributes:

- **UserId**
- **UpdateType**
- **Passwords**
- **PasswordCount**

If the password change came from Active Directory, the **UserId** attribute will contain the user's **sAMAccountName**, which must match the user's **uid** in IBM Directory Server. If the password change came from IBM Directory Server (IDS), the **UserId** attribute will contain the user's full Distinguished name (DN) as it appears in IDS. The Password store connector populates the work entry with **UserId**, **UpdateType** and **Passwords** from the queue. It also introduces another attribute called **origin**, which stores either the value *AD* or *IDS*, depending on where the password change came from.

RedirectAL

Depending on whether the password change came from Active Directory

or IBM Directory Server, this component redirects the work entry to a different path through the Assembly Line. This component determines where the password change came from and directs the work entry to the next appropriate connector.

GetUID

This connector is invoked if the password change came from IBM Directory Server; in this case the **UserId** attribute in the work entry contains the user's full Distinguished Name (DN). To make processing the password change easier, this connector retrieves the user's **uid** (which will be the same as the Active Directory **sAMAccountName**) and replaces the DN in the work entry with this value. This helps simplify the logic in consecutive connectors, alleviating the need for connectors to treat the work entry differently, based on what value is in the **UserId**.

CheckADUser

If the password change came from IDS, then this connector checks that a corresponding account is found in AD for this user. If a match is not found, then processing is stopped, and no passwords are changed. If a match is found, processing continues. Note that for a password change from AD, there is no dedicated connector to check for a corresponding account in IDS. This is because this is handled by the **CheckFlag** connector, which establishes a connection to IDS early in the Assembly Line.

CheckFlag

The **CheckFlag** connector is only called if the Assembly Line is operated in bi-directional mode. Its function is to check the flag in the LDAP (IDS) for the current user, and determine whether the password change should be propagated to the other directory or dropped.

UpdateFlag

This connector's purpose is to either add or remove a flag from the LDAP attribute nominated in the external properties file. A flag is added if this is the first password change, and removed when a flag is detected.

UpdateIDSPassword

This LDAP connector is only activated if the password change came from Active Directory. It operates in **update** mode to update the **userPassword** attribute in IBM Directory Server with the value taken from the Active Directory password change.

UpdateADPassword

This LDAP connector to Active Directory is only activated if the password change came from IBM Directory Server. It updates the user's Active Directory password, based on the value retrieved from the IDS password change. This connector must use SSL to update the AD password. For details, refer to the section "Environment Setup" on page 6.

UpdateGSO

This script component uses the Tivoli Access Manager Java Administration API to update the user's Global Sign-On (GSO) credentials, updating the password to reflect the password change propagated from either directory. The GSO credentials to update are listed in the External Properties file. Another option in the properties file is **TAM.AddCreds**, which (when set to *yes*) allows creation of TAM GSO credentials if the current user is a GSO user and does not possess credentials for the resources listed in the properties file.

Chapter 3. Configuring and Installing the Assembly Line

This chapter contains the following sections:

- “Configuring the External Properties File”
- “Configuring the Assembly Line” on page 15
- “Running the Assembly Line” on page 15
- “Checking Installation and Configuration Success” on page 17

Configuring the External Properties File

The External Properties file, `am_msADPwdSync.props` (contained in the distribution package `.tar` file), is used to store configuration information for the Assembly Line. It contains both component parameters and specific options that effect how the Assembly Line works.

To achieve password synchronization, you must supply the required details for the property file. Edit the External Properties file using either a text editor or Tivoli Directory Integrator. The following table provides a description of the configurable parameters. Save the file when finished.

Name	Description
AD.AutoMapPwd	Used by the UpdateADPassword connector, leave as <i>true</i> .
AD.Username	DN of administrative user for Active Directory. For example <code>cn=Administrator,cn=users,dc=example,dc=com</code>
AD.Password	Password for the administrative user specified in AD.Username
AD.SearchBase	Search base for AD. For example <code>cn=users,dc=example,dc=com</code>
AD.URL	URL to the Active Directory machine, this parameter is used by the CheckADUser connector. For example: <code>ldap://ad.example.com:389</code>
AD.SSL.URL	URL to the Active Directory machine, this parameter is used by the UpdateADPassword connector. For example: <code>ldap://ad.example.com:636</code>
AD.UseSSL	Used by the UpdateADPassword connector, leave as <i>true</i> (ensure SSL has been setup between Tivoli Directory Integrator and AD)
IDS.Username	Username that the Assembly Line uses to bind to IBM Directory Server with administrative privileges. For example: <code>cn=root</code>
IDS.Password	Password for the administrative user specified in IDS.Username
IDS.SearchBase	Where in the LDAP directory the connector should start the search. For example: <code>o=example,c=au</code>

Name	Description
IDS.URL	The URL to the IBM Directory Server machine. For example: ldap://ids.example.com:389
IDS.Flag.Attribute	The Attribute to use on the LDAP server to store the flag. It can be any unused attribute within the user object. For example: mail
MQ.Server	This is the name and the port of the machine where the QueueManager resides. This will be the machine where Tivoli Directory Integrator is installed. For example: localhost:41002
MQ.Timeout	This value must be -1
MQ.ini.File	This is the path to the pwstore_server.ini file. For example: C:\Program Files\IBM\IBMDirectoryIntegrator\MQePWStore\pwstore_server.ini
Single.Direction	A <i>yes</i> here forces the Assembly line to run in a single direction. A <i>no</i> forces the Assembly Line to run in Bi-Directional mode.
TAM.Version	The version of Tivoli Access Manager that is being used. Valid values here are 4.1 or 5.1.
TAM.Username	Tivoli Access Manager administrative user. For example: sec_master
TAM.Password	The password for the Tivoli Access Manager administrative user.
TAM.Domain	If using Tivoli Access Manager 5.1, specify the appropriate domain. Use <i>default</i> if you are using the default Tivoli Access Manager 5.1 domain.
TAM.ConfigFile	The Tivoli Access Manager config file created when configuring the Java runtime using the SvrSslCfg class. This must be specified using the protocol file:/// . For example: file:///C:\IDI\configFile
TAM.GSOResources	A list of GSO resources that the Assembly Line should update. Each resource should be listed by name, followed by a comma and followed by the type. Multiple resources should be separated by a semicolon. A valid entry would look like this (on one line): msExchangeRsrc,Web Resource;msSharepointRsrc, Group Resource;msIISRsrc,Web Resource Note that spaces between the delimiters are not valid. Refer to the Tivoli Access Manager documentation for details of administering GSO credentials.
TAM.AddCreds	Whether the Assembly Line is to add resource credentials for users that don't possess them in their Tivoli Access Manager Account (user must be a GSO user). A <i>yes</i> forces the Assembly Line to create credentials. A <i>no</i> entered here will cause the Assembly Line to skip updating GSO credentials that the user does not possess.

Name	Description
ERROR.File	An error file that will log error messages from the Assembly Line. This file will be created if it does not exist. For example: C:\IDI\errFile.txt
Sleep.Interval	The interval (in seconds) that the system should sleep before restarting the Assembly Line after stopping.

Configuring the Assembly Line

The Assembly Line must be configured to use the External Properties file. The LDAP attribute for the **flag** component must be manually configured.

Configure the Assembly Line to use the external properties file:

1. Open the Tivoli Directory Integrator Configuration Editor.
2. Select **File** then **Open**.
3. Select the `am_msADPwdsync.xml` file and click **Open**.
4. Click on the **External Properties** branch in the object tree on the left hand side.
5. Click on the **Select External Properties File** symbol (this text is displayed as a tool tip) in the top right corner of the window that is displayed.
6. Click the **Select...** button.
7. Locate and select the `am_msADPwdsync.props` file and click **Open**.
8. Note that the External Properties file can be encrypted to protect the sensitive information in this file. Select this option if required.
9. Click **OK**.

If you have previously modified the External Properties File to reflect your environment, all the name value pair should be entered. If not, refer to the section “Configuring the External Properties File” on page 13.

Configure the LDAP attribute for the flag in the assembly line:

1. Expand **Assembly Lines** in the left pane.
2. Select **am_msADPwdsync**.
3. Select the **UpdateFlag** connector in the Connectors pane.
4. Select the **Output Map** tab.
5. Enter the name of the Attribute that you have selected in the **connector attribute** field (by default, this is *mail*: this should match the **IDS.Flag.Attribute** entry in the External Properties file).
6. Save the Assembly Line.

Running the Assembly Line

The Assembly Line can be run from either the Tivoli Directory Integrator Configuration Editor or from the command line. In the first instance, run it from the Configuration Editor in order to ensure that all items entered in the properties file are correct. The Configuration Editor provides greater feedback than when running the Assembly Line from the command line.

Running the Assembly Line from the Configuration Editor

With the eventhandler **am_msADPwdSyncEH** open in the Tivoli Directory Integrator Configuration Editor, select the **Run** button to launch the assembly line. The following output should be displayed:

```
11:18:20 Version           : Version 5.2 - 2004-11-04
11:18:20 OS Name            : Windows 2000
11:18:20 Java Runtime           : IBM Corporation, 1.4.1
11:18:20 Java Library            : C:\Program Files\IBM\IBMDirectoryIntegrator\_jvm\bin
11:18:20 Java Extensions        :
C:\Program Files\IBM\IBMDirectoryIntegrator\_jvm\lib\ext
11:18:20 Working directory      : C:\Program Files\IBM\IBMDirectoryIntegrator
11:18:20 Configuration File: <stdin>
11:18:20 ---
11:18:20 Loading system templates
11:18:24 Loading configuration from <stdin>
11:18:29 Starting EventHandler: EventHandlers/PwdEH
11:18:30 EventHandler EventHandlers/PwdEH has started
11:18:30 Wait for completion of EventHandler: EventHandlers/PwdEH
11:18:31 Generic Thread Started
11:18:31 BEGIN Include Script Library
11:18:32 END Include Script Library
11:18:37 AssemblyLine PwdSync started
11:18:38 AssemblyLine PwdSync started
11:18:41 [MQPwdStore] JMS Queue Session established successfully.
11:18:41 [MQPwdStore] The Storage Component is successfully notified for the
Connector startup.
11:18:44 [UpdateADPassword] Using LDAP SSL connection - make sure TCP port
number is changed accordingly
11:18:47 BEGIN prolog
11:18:47 Using Tivoli Access Manager 5.1
11:18:56 --- TAM Java AdminAPI initialized
11:18:56 END prolog
11:18:56 BEGIN Iteration
```

At this stage the Assembly Line is monitoring the queues for password changes. When a user changes a password on Active Directory, a message should be displayed that is similar to the following (a change from IBM Directory Server will result in a similar message):

```
14:31:34 Password change from AD detected for user: exampleUser
14:31:35 IDS Password updated successfully
14:31:37 ExampleRes, GSO credentials updated for user: exampleUser
14:31:39 Password change from IDS detected for user: CN=EXAMPLEUSER,O=EXAMPLE,C=AU
14:31:39 Dumping work entry for user: exampleUser
```

The first three lines reflect the true password change and the Assembly Line successfully completing the password update. The next two lines reflect the countering of the ping-pong effect, as mentioned earlier in the document.

Running the Assembly Line from the Command Line

To run the Assembly Line from the command line:

1. Open a command window.
2. Navigate to the Tivoli Directory Integrator install directory (typically C:\Program Files\IBM\IBMDirectoryIntegrator).
3. Start the Assembly Line (more specifically the **eventhandler**) with the following command:

```
ibmdisrv -c"path_to_config_file" -t"am_msADPwdSyncEH" -l"path_to_log_file"
```

where:

- *path_to_config_file* is the fully qualified path to the XML file for the Assembly Line. For example: C:\example\am_msADPwSync.xml
 - *path_to_log_file* is a fully qualified path to a log file for the Assembly line. For example: C:\example\iditam.log. The file will be created if it does not exist.
4. The log file specified above provides very little information on the normal operation of the Assembly Line. For details on setting up logging using Tivoli Directory Integrator, refer to the *Tivoli Directory Integrator Administrators Guide*.

The command prompt from which the Assembly Line is launched provides no information on the startup or running of the Assembly Line. The only way to really know that the Assembly Line has finished its startup procedure is to watch the CPU load or monitor the log file. When CPU load minimizes, the Assembly Line is running and monitoring for password changes. Until you are certain that all the values in the properties file are correct, always launch the Assembly Line from the Tivoli Directory Integrator Configuration Editor.

For details of other options that are available when running the Assembly Line from the command line, refer to the *IBM Tivoli Directory Integrator Users Guide*, particularly *Chapter 5: Tivoli Directory Integrator command line options*. This is especially relevant if the Assembly Line is using an encrypted properties file.

Checking Installation and Configuration Success

The following steps describe a simple test to ensure the Assembly Line is working correctly.

1. Ensure that you have a GSO junction setup from WebSEAL to IIS and that SSO is working.
2. Create a simple HTML page on the IIS server (in wwwroot). The content of this page is unimportant, it is simply used to demonstrate access control.
3. Create a GSO user in Tivoli Access Manager (ensure you make the account valid).
4. Create a corresponding account in Active Directory. Ensure that the User Logon Name (**sAMAccountName**) is the same as the Tivoli Access Manager user's Login ID. Specify the same password as you specified for the Tivoli Access Manager user.
5. Use **pdadmin** to create Resource Credentials for the Tivoli Access Manager user. When specifying the **rsrcuser** and **rsrcpwd** entries, use the Active Directory user's **User Logon Name** and **password**.
6. Run the Assembly Line.
7. Launch a Web browser and access the sample page through WebSEAL:
`http://webseal_server_name/gso_junction_name/sample_html_page.html`
8. Authenticate with the new Tivoli Access Manager user (created in step 2 above). The page should be displayed successfully.
9. Now change the user's password in either Tivoli Access Manager or Active Directory. Notice the password change captured in Tivoli Directory Integrator.
10. Repeat steps seven and eight, using the user's new password. This successfully demonstrates the Assembly Line propagating password changes to AD/TAM/GSO.

Uninstallation

As the Assembly Line consists of only the configuration (XML) file and the properties file, no uninstallation is required.

For uninstallation instructions for the other components, refer to the relevant product documentation.

Chapter 4. Troubleshooting and Issues

This chapter contains the following sections:

- “Troubleshooting”
- “Known Problems and Issues”
- “Expected Behavior” on page 20

Troubleshooting

Most errors are inevitably going to stem from incorrect entries in the External Properties file. Ensure that all values in the file are populated correctly. For example entries, refer to the section “Configuring the External Properties File” on page 13.

Known Problems and Issues

- During development, it was noticed that on occasions when the Assembly Line was not shut down cleanly, and was subsequently run again from the Configuration Editor, it failed to pick up password changes from the directories. This is due to an issue with the MQ QueueManager. Tivoli Directory Integrator must be restarted for password changes to be captured again.

- If inactive for a period of time, the Active Directory connectors may timeout. The output is similar to the following:

```
11:58:09 Password change from IDS detected for user: CN=EXAMPLEUSER,  
O=EXAMPLE,C=AU  
11:58:10 -----Active Directory connection timed out for CheckADUser  
Connector-----  
11:58:12 Jumping to CheckADUser  
11:58:12 -----Active Directory connection timed out for UpdateADPassword  
Connector-----  
11:58:12 [UpdateADPassword] Using LDAP SSL connection - make sure TCP port  
number is changed accordingly  
11:58:14 Jumping to UpdateADPassword  
11:58:14 AD password updated successfully  
11:58:15 IDIRes, GSO credentials updated for user: exampleUser  
11:58:15 Password change from AD detected for user: exampleUser  
11:58:15 Dumping work entry for user: exampleUser
```

It is normal to see entries like this in the log. When the Assembly Line detects that the Active Directory connector has timed out, it re-initializes the connector.

- If the Administrator logs off the Tivoli Directory Integrator machine after executing the Assembly Line and subsequently logs back on, then launches the Assembly Line, an error message may be generated advising that the Assembly Line cannot connect to the password store. To rectify this problem, the Tivoli Directory Integrator machine must be restarted.
- If the Assembly Line fails for some reason to fully propagate a password change, and the flag remains set in the user’s LDAP entry, then the Assembly Line will detect this flag the next time the user changes their password, dump the password change and clear the flag. In this case, the user will need to change their password again.

- The Tivoli Directory Integrator password capture plug-in is not officially supported on IBM Directory Server 4.1. Tivoli Access Manager 5.1 and IBM Directory Server 5.2 are recommended, although the plug-in will work with IBM Directory Server 4.1.
- It is highly recommended that password policies in Active Directory and Tivoli Access Manager should match. This will ensure that users adhere to password policy guidelines when changing passwords in either Active Directory or Tivoli Access Manager.
- If uninstalling the password capture plug-in from IBM Directory Server, remember to either comment out or remove the line that was added to the LDAP configuration file during configuration of the password store. See “Single or Bi-Directional Mode Options” on page 6.

Expected Behavior

The following table shows the behavior expected in various situations where password synchronization has been implemented.

Situation	Description
Password change for a user without GSO credentials and TAM.AddCreds property set to <i>no</i> .	If the password was changed in Active Directory then the IBM Directory Server password will be changed, but GSO credentials will not be changed. If the password was changed on IBM Directory Server, then the Active Directory password will be changed but GSO credentials will not be changed. GSO credentials will not be created for the resources listed in the properties file.
Password change for a non-GSO enabled user.	In this solution, only the user's directory passwords will be updated.
Password change for a user that has Account-valid set to <i>no</i> in Tivoli Access Manager.	The password will be changed regardless of the invalidated account. However, the user will still not be able to login through WebSEAL.
User exists in IBM Directory Server but not in Active Directory. Will GSO credentials be updated or created when the password is changed on IBM Directory Server?	With this integration applied, the users must have an account in both directories for passwords to be synchronized. When a password change is detected, a check is made to verify that the user exists in the other directory. If not, the password change is aborted without updating any passwords.

Appendix A. IBM Software Support

IBM Software Support provides assistance with product defects.

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus, and Rational products, as well as DB2 and WebSphere products that run on Windows or UNIX operating systems), enroll in Passport Advantage in one of the following ways:
 - **Online:** Go to the following Passport Advantage Web page and click **How to Enroll**:
http://www.lotus.com/services/passport.nsf/WebDocs/Passport_Advantage_Home
 - **By phone:** For the phone number to call in your country, go to the IBM Software Support Web site (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region.
- For IBM eServer software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web page (<http://www.ibm.com/servers/eserver/techsupport.html>).

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States or, from other countries, go to the contacts page of the IBM Software Support Handbook on the Web (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region for phone numbers of people who provide support for your location.

Follow the steps in this topic to contact IBM Software Support:

1. "Determine the business impact of your problem"
2. "Describe your problem and gather background information" on page 22
3. "Submit your problem to IBM Software Support" on page 22

Determine the business impact of your problem

When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem you are reporting. Use the following criteria:

Severity 1	Critical business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
Severity 2	Significant business impact: The program is usable but is severely limited.

Severity 3	Some business impact: The program is usable with less significant features (not critical to operations) unavailable.
Severity 4	Minimal business impact: The problem causes little impact on operations, or a reasonable circumvention to the problem has been implemented.

Describe your problem and gather background information

When explaining a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- What software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can the problem be recreated? If so, what steps led to the failure?
- Have any changes been made to the system? (For example, hardware, operating system, networking software, and so on.)
- Are you currently using a workaround for this problem? If so, please be prepared to explain it when you report the problem.

Submit your problem to IBM Software Support

You can submit your problem in one of two ways:

- **Online:** Go to the "Submit and track problems" page on the IBM Software Support site (<http://www.ibm.com/software/support/probsub.html>). Enter your information into the appropriate problem submission tool.
- **By phone:** For the phone number to call in your country, go to the contacts page of the IBM Software Support Handbook on the Web (<http://techsupport.services.ibm.com/guides/contacts.html>) and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround for you to implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM product support Web pages daily, so that other users who experience the same problem can benefit from the same resolutions.

For more information about problem resolution, see "Searching knowledge bases" and "Obtaining fixes" on page 23.

Searching knowledge bases

If you have a problem with your IBM software, you want it resolved quickly. Begin by searching the available knowledge bases to determine whether the resolution to your problem is already documented.

Search the information center on your local system or network

IBM provides extensive documentation that can be installed on your local machine or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

Search the Internet

If you cannot find an answer to your question in the information center, search the Internet for the latest, most complete information that might help you resolve your problem. To search multiple Internet resources for your product, expand the product folder in the navigation frame to the left and select **Support on the Web**. From this topic, you can search a variety of resources including:

- IBM technotes
- IBM downloads
- IBM Redbooks
- IBM DeveloperWorks
- Forums and newsgroups
- Google

Obtaining fixes

A product fix might be available to resolve your problem. You can determine what fixes are available for your IBM software product by checking the product support Web site:

1. Go to the IBM Software Support Web site (<http://www.ibm.com/software/support>).
2. Under **Products A - Z**, select your product name. This opens a product-specific support site.
3. Under **Self help**, follow the link to **All Updates**, where you will find a list of fixes, fix packs, and other service updates for your product. For tips on refining your search, click **Search tips**.
4. Click the name of a fix to read the description and optionally download the fix.

To receive weekly e-mail notifications about fixes and other news about IBM products, follow these steps:

1. From the support page for any IBM product, click **My support** in the upper-right corner of the page.
2. If you have already registered, skip to the next step. If you have not registered, click register in the upper-right corner of the support page to establish your user ID and password.
3. Sign in to **My support**.
4. On the My support page, click **Edit profiles** in the left navigation pane, and scroll to **Select Mail Preferences**. Select a product family and check the appropriate boxes for the type of information you want.
5. Click **Submit**.
6. For e-mail notification for other products, repeat Steps 4 and 5.

For more information about types of fixes, see the *Software Support Handbook* (<http://techsupport.services.ibm.com/guides/handbook.html>).

Appendix B. 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
2Z4A/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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 illustrates 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. 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 IBM's application programming interfaces.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

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

AIX
DB2
IBM
IBM(logo)
SecureWay
Tivoli
Tivoli (logo)
Universal Database
WebSphere

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries, or both.

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

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



Printed in USA