IBM Security Identity Manager
Version 6.0, 5.1

Password Synchronization Plug-in for IBM Security Access Manager 7.0 Installation and Configuration Guide

IBM Security Identity Manager
Version 6.0, 5.1

Password Synchronization Plug-in for IBM Security Access Manager 7.0 Installation and Configuration Guide

Note
Before using this information and the product it supports, read the information in "Notices" on page 33.

Edition notice

Note: This edition applies to version 6.0 of IBM Security Identity Manager (product number 5724-C34) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Preface

About this publication

This guide provides information about the procedures that are required to achieve password synchronization between IBM Security Access Manager and IBM® Security Identity Manager. IBM Security Access Manager was known previously as Tivoli® Access Manager. IBM Security Identity Manager was known previously as Tivoli Identity Manager.

The IBM Security Identity Manager Password Synchronization Plug-in for IBM Security Access Manager, referred to as the Password Synchronization Plug-in, provides password synchronization from IBM Security Access Manager to IBM Security Identity Manager.

This document assumes that the following components are already installed, configured, and running on the target system:

- IBM Security Access Manager
- IBM Security Identity Manager
- IBM Security Identity Manager Adapter for IBM Security Access Manager

This plug-in guide does not provide details on the installation and administration of these products.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Identity Manager library."
- Links to "Online publications."
- A link to the "IBM Terminology website" on page x.

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation, see the online library (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm).

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager library
The product documentation site (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center

The IBM Publications Center site (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Appendix A, "Support information," on page 27 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Overview of the plug-in

The Password Synchronization Plug-in enables communication between the IBM Security Identity Manager server and the IBM Security Access Manager server.

Architecture of the plug-in

You must install and configure several components to achieve password synchronization.

The following figure shows a typical system architecture that involves:

- IBM Security Identity Manager
- IBM Security Access Manager
- IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server
- IBM Security Identity Manager Adapter for IBM Security Access Manager
- Password Synchronization Plug-in

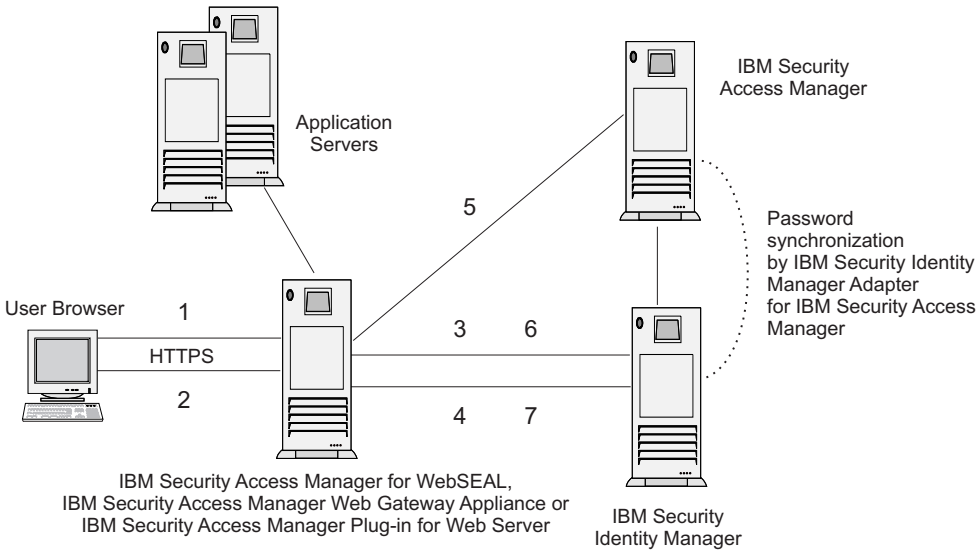

Figure 1. System architecture that shows password synchronization flow

The Password Synchronization Plug-in provides password synchronization through the following process:

1. A user submits a password change request to IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server.
2. IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server prompts the user to enter a new password.
3. IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server

sends a request to IBM Security Identity Manager to check the new password against password policy for the specified service.

4. IBM Security Identity Manager responds to IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server with a success or a failed result after the password check is performed.
5. Password is changed within the IBM Security Access Manager environment if the password check is successful.
6. WebSEAL or the Web Plug-in submits a second request to IBM Security Identity Manager to synchronize the new password for the specified user.
7. IBM Security Identity Manager returns a status to IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server that the password request is submitted.

Chapter 2. Plug-in installation planning

Installing and configuring the plug-in involves several steps that you must complete in an appropriate sequence. Review the roadmaps before you begin the installation process.

Software download

Download the software through your account at the IBM Passport Advantage® website.

Go to IBM Passport Advantage.

See the *IBM Security Identity Manager Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Distribution package contents

The contents of the distribution package vary slightly, depending on your operating system.

Table 1. Distribution package contents

Directory Name	**Description**
`amd64_linux_2`	Password Synchronization plug-in for Linux systems (64bit only)
`rios_64_aix_5`	Password Synchronization plug-in for AIX® systems (64bit only)
`s390_64_linux_2`	Password Synchronization plug-in for zLinux systems (64bit only)
`sparc_64_solaris_2`	Password Synchronization plug-in for Solaris on sparc systems (64bit only)
`x86_64_nt_4`	Password Synchronization plug-in for Microsoft Windows systems (64bit only)
File names in compressed files	**Descriptions**
Windows: `revpwdchk.dll` and `revpwdsyn.dll` **AIX:** `librevpwdchk.a` and `librevpwdsyn.a` **Solaris:** `librevpwdchk.so` and `librevpwdsyn.so` **Linux:** `librevpwdchk.so` and `librevpwdsyn.so` **zLinux:** `librevpwdchk.so` and `librevpwdsyn.so`	Dynamic libraries
Additional files	**Description**
`passwdsync.conf`	Configuration file template

Table 1. Distribution package contents (continued)

Directory Name	Description
`ReleaseNotes-TAMebPwdSync.html`	Release notes that outline the latest information about the plug-in

Prerequisites

Verify that your environment meets all the prerequisites before you install the plug-in.

The following table identifies the software and operating system prerequisites for the plug-in installation.

Table 2. Prerequisites to install the plug-in

Prerequisite	Description
System	• A minimum of 256 MB of memory. • At least 300 MB of free disk space.
Operating System	Installation packages are available for the following operating systems: • IBM AIX • Linux • Microsoft Windows • Sun Solaris • zLinux on S/390
Network Connectivity	TCP/IP network
System Administrator authority	The person who performs the plug-in installation procedure must have system administrator authority to complete the steps.
IBM Security Identity Manager	6.0, 5.1
IBM Security Access Manager	• IBM Security Access Manager 7.0 • Either of the following products: – IBM Security Access Manager WebSEAL 7.0 – IBM Security Access Manager Web Gateway Appliance 7.0 – IBM Security Access Manager Plug-in for Web Servers version 7.0

Preinstallation roadmap

Before you install the plug-in, you must prepare the environment.

Perform the tasks that are listed in Table 3.

Table 3. Preinstallation roadmap

Task	For more information
Obtain the installation software.	Download the software from Passport Advantage website. See "Software download" on page 3.
Verify that your environment meets the software and hardware requirements for the plug-in.	See "Prerequisites" on page 4.
Obtain the necessary information for the installation and configuration.	See "Installation worksheet for the plug-in."

Installation roadmap

To install the plug-in, you must complete several tasks.

Table 4. Installation roadmap

Task	For more information
Install the plug-in.	See "Installing the Password Synchronization Plug-in" on page 8.
Configure the plug-in.	See "Configuring the Password Synchronization Plug-in for IBM Security Access Manager for WebSEAL or IBM Security Access Manager Plug-in for Web Server" on page 11.
Verify the plug-in installation.	See "Verifying the installation" on page 17.

Installation worksheet for the plug-in

You need the information in this table before you install the plug-in.

Table 5. Required information to install the plug-in

Required information	Description
An IBM Security Identity Manager Administrator Account.	To set password synchronization within the IBM Security Identity Manager you need access to an account with administration privileges.
An Administrator account on the server where IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server is installed	Administrator access is required to install and configure the password synchronization plug-in. Additionally you must restart IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server.

Chapter 3. Plug-in installation

To install the Password Synchronization Plug-in, you must complete several steps.

1. Enable password synchronization on the IBM Security Identity Manager Server. See the online help or the IBM Security Identity Manager product documentation for specific instructions about IBM Security Identity Manager password synchronization.
2. Install the Password Synchronization Plug-in on the IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server.

These steps are described in more detail in the following sections.

Before you install

Before you install the Password Synchronization Plug-in, complete the preliminary steps.

Procedure

1. Verify prerequisite requirements. See "Prerequisites" on page 4.
2. Obtain a copy of the installation software. See "Software download" on page 3.
3. Obtain system administrator authority.
4. Check the configuration.

   As part of the adapter installation, you must configure the IBM Security Identity Manager server so that users can manage their IBM Security Access Manager account passwords.

   a. Log in to IBM Security Identity Manager as an administrator.
   b. Select **Set System Security**.
   c. Select **Manage Access Control Item**.
   d. Click **Search**.

   If the configuration is correct, a corresponding organizational Access Control Information (ACI) is set for the IBM Security Access Manager account. If so, you can proceed with the Password Synchronization Plug-in installation process. If not, continue with these steps to create an ACI.

   a. Select **Set System Security**.
   b. Select **Manage Access Control Item**.
   c. Select the **Account** category.
   d. Select **eritamaccount**.
   e. Enter the ACI name in the text field.
   f. Select **Grant** for the **Modify** operation. Click **Next**.
   g. Grant **Read** and **Write** permissions for the **Password** attribute.
   h. Click **Finish**.

   For more details on ACI, see the *IBM Security Identity Manager Policy and Organization Administration Guide*.

Enabling password synchronization in the IBM Security Identity Manager Server

To enable password synchronization between accounts, you must configure the IBM Security Identity Manager password synchronization feature. These steps apply to IBM Security Identity Manager versions 5.1 and 6.0.

About this task

Note: Without this step, the Password Synchronization Plug-in processes the password change. However, the IBM Security Identity Manager server does not synchronize the IBM Security Access Manager password with the passwords for other accounts.

Procedure

1. Log in to IBM Security Identity Manager as an administrator.
2. Select **Set System Security** and then the **Set System Properties** tab.
3. Select the **Enable Password Synchronization** check box.
4. Click **OK**.

Installing the Password Synchronization Plug-in

You must install the Password Synchronization Plug-in on your IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server.

About this task

If you are configuring the Password Synchronization Plug-in on the IBM Security Access Manager Web Gateway Appliance, you can skip the following procedure because the plug-in is pre-installed on the appliance. Continue to Chapter 4, “First steps after installation,” on page 11.

The steps that you take depend on the operating system of your server.

Procedure

- **UNIX and Linux:**
  1. Copy the dynamic libraries `librevpwdchk` and `librevpwdsyn` from the distribution package to the `/usr/lib/` directory.
  2. With a text editor, open the appropriate configuration file:

     IBM Security Access Manager WebSEAL
     WEBSEAL_HOME`/etc/webseald-`*default*`.conf`

     IBM Security Access Manager Web Plug-in for Web Server
     WEBPI_HOME`/etc/pdwebpi.conf`

     Where *default* indicates your default WebSEAL domain name.
  3. Modify the `[authentication-mechanisms]` stanza as follows (entered as two single lines):

     ```
     passwd-strength=/usr/lib/librevpwdchk.extension&WEBSEAL_HOME_or_
     WEBPI_HOME/etc/webseald-default.conf check
     post-pwdchg-process=/usr/lib/librevpwdsyn.extension&WEBSEAL_HOME_or_
     WEBPI_HOME/etc/webseald-default.conf synch
     ```

     For example, on a Solaris system this stanza is:

```
passwd-strength=/usr/lib/librevpwdchk.so&/opt/
  pdweb/etc/webseald-default.conf check
post-pwdchg-process=/usr/lib/librevpwdsyn.so&/opt/
  pdweb/etc/webseald-default.conf synch
```

- **Windows:**

  Note: On the Windows operating system, file and directory names might contain space characters. WebSEAL and the Web Plug-in expect additional arguments for any `passwd-strength` and `post-pwdchg-process` configuration lines that are separated by a space character. You must use the 8.3 convention for truncated long file names to avoid errors. For example, `C:\Progra~1\Tivoli\PdWeb\etc\passwdsync.conf`

  1. Copy the dynamic libraries `revpwdchk.dll` and `revpwdsyn.dll` from the distribution package to the *WEBSEAL_HOME*_or_*WEBPI_HOME*\bin\ directory.
  2. With a text editor, open the appropriate configuration file:

     IBM Security Access Manager WebSEAL
     WEBSEAL_HOME\etc\webseald-*default*.conf

     IBM Security Access Manager Web Plug-in for Web Server
     WEBPI_HOME\etc\pdwebpi.conf

     Where *default* indicates your default WebSEAL domain name.
  3. Modify the [authentication-mechanisms] stanza as follows (entered as two single lines):

```
passwd-strength=C:\Progra~1\Tivoli\pdweb\bin\
 revpwdchk.dll&WEBSEAL_HOME_or_
WEBPI_HOME\etc\webseald-default.conf check
post-pwdchg-process=C:\Progra~1\Tivoli\pdweb\bin\
 revpwdsyn.dll&WEBSEAL_HOME_or_
WEBPI_HOME\etc\webseald-default.conf synch
```

Chapter 4. First steps after installation

After you install the adapter, you must complete several other tasks. The tasks include configuring the adapter, setting up SSL, installing the language pack, and verifying the adapter works correctly.

Plug-in configuration

Several configuration steps are required to configure the Password Synchronization Plug-in.

Configure the Password Synchronization Plug-in to work with the IBM Security Identity Manager Server. If IBM Security Identity Manager Server is installed on a WebSphere® Application Server cluster, you must also configure SSL for IBM HTTP Server.

1. Configure the Password Synchronization Plug-in for IBM Security Access Manager for WebSEAL or IBM Security Access Manager Plug-in for Web Server.
2. Configure the Password Synchronization Plug-in for IBM Security Access Manager Web Gateway Appliance.

Configuring the Password Synchronization Plug-in for IBM Security Access Manager for WebSEAL or IBM Security Access Manager Plug-in for Web Server

The Password Synchronization Plug-in uses the HTTPS protocol. It must be configured to accept the corresponding IBM Security Identity Manager service.

Procedure

1. Create a Key Database file of type CMS for the Password Synchronization Plug-in. This task can be done by using the IBM **iKeyMan** or one of the GSKit command line tools.
2. Copy the `.kdb` file to the `keytabs` directory.

   UNIX: *WEBSEAL_HOME or WEBPI_HOME*`/keytab-`*default*

   Windows:
   WEBSEAL_HOME or WEBPI_HOME`\keytab-default`

   Note: This directory might not exist on some platforms for IBM Security Access Manager 6.0. If so, put the file in the following directory:
   WebSEAL_or_WebPI_install_dir`/etc`

   (where *default* indicates your default WebSEAL domain name).
3. With a text editor, open the appropriate configuration file:

   IBM Security Access Manager WebSEAL
   WEBSEAL_HOME`/etc/webseald-default.conf`

   IBM Security Access Manager Web Plug-in for Web Server
   WEBPI_HOME`\etc\pdwebpi.conf`
4. Edit the configuration file by adding an `[itim]` stanza and the additional attributes as outlined following

   is_enabled
   Enables or disables the Password Synchronization Plug-in.

- Set the attributes value to `true` to enable the plug-in.
- Set the value to `false` to disable the plug-in.

itim-server-name
This entry is the host name or IP address of the IBM Security Identity Manager server that hosts the IBM Security Identity Manager Adapter for IBM Security Access Manager. In a WebSphere Application Server cluster environment, you need to configure SSL for IBM HTTP Server. If you are using a WebSphere Application Server single-server environment, you do not need to configure SSL for IBM HTTP Server.

* This entry is mandatory.

servlet-port
The port that is associated with the `itim-server-name` URL. The default HTTPS port is 9443 for a single server configuration and 443 for an IBM Security Identity Manager cluster with HTTP SSL configured.

principal-name
An ID that has the necessary permissions to request the check and synchronization operations. The best practice is to create a separate account with appropriate permissions and use this account instead of the IBM Security Identity Manager manager account.

* This entry is mandatory.

principal-password
The password for the IBM Security Identity Manager Principal Name.

* This entry is mandatory.

service-source-dn, service-password-dn, service-token-card-dn
Each of these entries can hold the pseudo-distinguished names of the services or resources that issue the password synchronization request. This pseudo-distinguised name consists of the attributes o, ou, and dc from the IBM Security Identity Manager LDAP organization context, and the `erservicename` attribute of the IBM Security Access Manager service name, as defined in IBM Security Identity Manager. For assistance in determining these values, see "Pseudo-distinguished name values" on page 16.

If there are more than one pseudo-distinguished names that are specified, they must be separated with a semicolon (;) character. The plug-in iterates through the list of service names until an account is found for one of the services. If no account is found on the specified services, an error is reported.

a. **service-source-dn** is used to define the service pseudo-distinguished name for all authentication methods.
b. **service-password-dn** is used to define the service pseudo-distinguished name if it uses standard **password** as the authentication method. If this method is specified, it overrides the **password** authentication method that is defined under **service-source-dn**.
c. **service-token-card-dn** is used to define the service pseudo-distinguished name if it uses **token card** as the authentication method. If this method is specified, it overrides the **token card** authentication method that is defined under **service-source-dn**.

* It is mandatory to specify at least one of these entries.

keydatabase-file
The location and name of the Key Database file.

* This entry is mandatory.

keydatabase-password
The password for the Key Database file.

* This entry is mandatory.

servlet-context
The password synchronization context root on the application server.

* This entry is optional.

The following example shows a modified file for a UNIX system:

```
[itim]
is_enabled=true
itim-server-name=ITIM_host_name_or_IP_address
servlet-port=servlet_port
servlet-context=/passwordsynch/synch
principal-name=principal_login_name
principal-password=principal_password
service-source-dn=erservicename=TAM Employees Service,
o=IBM,ou=IBM,dc=com;erservicename=TAM Customers Service,
o=IBM,ou=IBM,dc=com
#service-password-dn=<service pseudo DN>
#service-token-card-dn=<service pseudo DN>
keydatabase-file=WebSEAL_dir/keytab-default/revpwdsync.kdb
keydatabase-password=password
```

5. Restart the IBM Security Access Manager WebSEAL or IBM Security Access Manager Web Plug-in for Web Server.

Configuring the Password Synchronization Plug-in for IBM Security Access Manager Web Gateway Appliance

The Password Synchronization Plug-in uses the HTTPS protocol. It must be configured to accept the corresponding IBM Security Identity Manager service.

Procedure

1. Log in to the IBM Security Access Manager Web Gateway Appliance administration console.
2. From the menu, select **Secure Reverse Proxy Settings** > **Reverse Proxy**. A list of currently configured reverse proxies is displayed.
3. Select the reverse proxy to use for the Password Synchronization Plug-in configuration.
4. From the submenu, select **Manage** > **Configuration** > **Edit Configuration File**. The reverse proxy configuration is displayed in an editable mode.
5. Search for the [itim] stanza in the configuration file. This stanza is added by default to the IBM Security Access Manager Web Gateway Appliance.
6. Update the [itim] stanza to reflect your environment settings. Use the following table to help you determine the appropriate value for each attribute.

Table 6. Attributes

Attributes	Description
`is_enabled`	Enables or disables the Password Synchronization Plug-in. • Set the attribute value to `true` to enable the plug-in. • Set the value to `false` to disable the plug-in. Set the attribute value to `true` to enable the Password Synchronization Plug-in on the IBM Security Access Manager Web Gateway Appliance.
`itim-server-name`	This entry is the host name or IP address of the IBM Security Identity Manager server that hosts the IBM Security Access Manager Adapter for IBM Security Access Manager. In a WebSphere Application Server cluster environment, configure the SSL for IBM HTTP Server. If you are using a WebSphere Application Server single-server environment, you do not need to configure SSL for IBM HTTP Server. This entry is mandatory.
`servlet-port`	The port that is associated with the `itim-server-name` URL. The default HTTPS port for: • a single-server configuration is 9443 • an IBM Security Access Manager cluster with HTTP SSL configured is 443
`principal-name`	An ID that has the necessary permissions to request the check and synchronization operations. The best practice is to create a separate account with appropriate permissions and use this account instead of the IBM Security Access Manager manager account. This entry is mandatory.
`principal-password`	The password for theIBM Security Identity Manager Principal Name. This entry is mandatory.

Table 6. Attributes (continued)

Attributes	Description
`service-source-dn, service-password-dn, service-token-card-dn`	Each of these entries can hold the pseudo-distinguished names of the services or resources that issue the password synchronization request. This pseudo-distinguished name consists of the attributes `o`, `ou`, and `dc` from: • the IBM Security Access Manager LDAP organization context, and • the `erservicename` attribute of the IBM Security Access Manager service name, as defined in IBM Security Access Manager. For assistance in determining these values, see "Pseudo-distinguished name values" on page 16. If there are more than one pseudo-distinguished names that are specified, separate them with a semicolon (;) character. The plug-in iterates through the list of service names until an account is found for one of the services. If no account is found on the specified services, an error is reported. 1. `service-source-dn` is used to define the service pseudo-distinguished name for all authentication methods. 2. `service-password-dn` is used to define the service pseudo-distinguished name when it uses standard password as the authentication method. If this method is specified, it overrides the password authentication method that is defined under `service-source-dn`. 3. `service-token-card-dn` is used to define the service pseudo-distinguished name when it uses token card as the authentication method. If this method is specified, it overrides the token card authentication method that is defined under `service-source-dn`. It is mandatory to specify at least one of these entries.
`keydatabase-file`	The location and name of the Key Database file. On the IBM Security Access Manager Web Gateway Appliance, the following default configuration can be used: `keydatabase-file = pdsrv.kdb` This entry is mandatory.

Table 6. Attributes (continued)

Attributes	Description
keydatabase-password	The password for the Key Database file. Either this entry, or the keydatabase-password-file entry is mandatory.
keydatabase-password-file	The passwords stash-file for the Key Database file. On the IBM Security Access Manager Web Gateway Appliance, the following default configuration can be used: keydatabase-file = pdsrv.sth Either this entry, or the keydatabase-password entry is mandatory.
servlet-context	The password synchronization context root on the application server. This entry is optional.

7. Click **Save** to confirm the changes. The following message is displayed:
   ```
   There is currently one undeployed change.
   Click here to review the changes or apply them to the system
   ```
8. Click the link as advised in the message.
9. To deploy the Password Synchronization Plug-in configuration, click **Deploy**. The following message is displayed:
   ```
   Successfully deployed all pending changes.
   The following reverse proxy instances need to be restarted
    for updates to take effect:

   <WebSEAL_instance_name>
   ```
10. Close the message.
11. Select the **<*WebSEAL_instance_name*>** from the reverse proxy list and select **Restart**.

Pseudo-distinguished name values

The **service-source-dn** entry holds the pseudo-distinguished name of the service that is issuing the password synchronization request.

To help determine the correct entries, this name might be considered to contain the following components, in the order **C+B+A**:

Component	Item	Description
A	ou, dc	The ou and dc parts of the service distinguished name.
B	o	The value of the o attribute of the organization to which the service belongs.
C	erServiceName	The value of the erServiceName attribute of the service.

For example, assume the service distinguished name is:

```
erglobalid=7311179187489369500,ou=services,erglobalid=
  0000000000000000000,ou=IBM,dc=com
```

Component A equals:

```
ou=IBM,dc=com
```

Component B equals the value of the `o` attribute for an organization entry with the distinguished name:

```
erglobalid=00000000000000000000,ou=IBM,dc=com
```

If the `o` attribute has the value International Business Machines, **Component B** would have the value:

```
o=International Business Machines
```

Component C equals the value of the `erServiceName` attribute of the service. If this attribute has the value `TAM Service`, the component would be:

```
erservicename=TAM Service
```

Thus, the complete pseudo-distinguished name is

```
erservicename=TAM Service, o=International Business Machines, ou=IBM,dc=com
```

Verifying the installation

Make sure that the Password Synchronization Plug-in is installed and working properly.

Procedure

1. Check that the Password Synchronization Plug-in is installed correctly. If IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server:
   - Starts, the Password Synchronization Plug-in is installed.
   - Does not start, the Password Synchronization Plug-in is not installed correctly.

     Review the IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server log files. Use the log files to identify the exact cause of the error. To enable the Password Synchronization Plug-in trace, see "Trace level enablement" on page 21.
2. Check that password synchronization is working correctly.
   a. Log in to IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server as a user.
   b. Go to the Password Change page. For example, if password authentication method is being used, go to the following page:

      `https://`*`WEBSEAL_HOSTNAME, WGA_HOSTNAME or WEBPI_HOSTNAME`*`:`*`port_number`*`/pkmspasswd`
   c. Change the user password.
   d. Log in to IBM Security Identity Manager with the new password from the previous step.

      If the login attempt is successful, the password synchronization is working correctly.

Language pack installation

The plug-in uses the same language package as the adapter and IBM Security Identity Manager and IBM Security Access Manager. Ensure that the products are using the same language pack.

See your IBM product documentation and search for information about installing language packs.

Chapter 5. Adapter error troubleshooting

Troubleshooting can help you determine why a product does not function properly.

You can use this information and techniques to identify and resolve problems with the adapter. The topics also provide information about troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?

- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix A, "Support information," on page 27.

Trace level enablement

The Password Synchronization Plug-in for IBM Security Access Manager traces messages to the NOTICE level. You must set the trace level to NOTICE.

Add the following line of code to the routing file in either the *WEBSEAL_HOME*/etc directory or the *WEBPI_HOME*/etc directory.

```
NOTICE:STDERR:-
```

All messages are traced to the standard IBM Security Access Manager WebSEAL or IBM Security Access Manager for Web Plug-in log files.

Known issues

A problem might occur because certain restrictions exist for the plug-in. The information identifies known issues that you might encounter.

Table 7. Known issues and solutions

Issue	Solution
IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server is unable to start after installation of the Password Synchronization Plug-in.	Review the IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server log files for detailed information.
HPDIA0201W `The client supplied invalid authentication information.`	Validate that the password that is being entered for the **Input old password** field is correct for the IBM Security Access Manager for WebSEAL or Web Plug-in user.
DPWCA0907E `Could not connect to socket (113)`	Validate in the passwordsync.conf file that the host name or IP address that is used for the **`itim-server-name`** attribute is correct and resolvable.

Table 7. Known issues and solutions (continued)

Issue	Solution
HPDIA0300W Password rejected due to policy violation.	Review the IBM Security Access Manager for WebSEAL, IBM Security Access Manager Web Gateway Appliance or IBM Security Access Manager Plug-in for Web Server log files for detailed information. Typically this error might require the validation of the following attributes in the passwordsync.conf file: • **principle-name** • **principle-password** • **service-source-dn** • **service-password-dn** • **service-token-dn** Additionally, validate that the password that is being entered complies with the specification of the password policy that is defined in IBM Security Identity Manager.
DPWCA0918I ITIM reply message: (The information used to login is not correct)	Validate that the **principle-name** and **principle-password** are defined correctly within the passwordsync.conf file.
DPWCA0918I ITIM reply message: (Invalid source: erServiceName=*service_dn* can not be found	Validate that the **erServiceName** is defined correctly within the passwordsync.conf file.
DPWCA0905W Function call, gsk_environment_init, failed error: 000000ca GSK_KEYRING_OPEN_ERROR-Keyring file did not open	Validate in the passwordsync.conf file that the key database file name and password is correctly configured for the **keydatabase-file** and **keydatabase-password** attributes.

Chapter 6. Uninstalling the plug-in

To remove the Password Synchronization Plug-in, you must complete several steps.

About this task

To unconfigure the Password Synchronization Plug-in from the IBM Security Access Manager Web Gateway Appliance, set the `is_enabled` attribute to `false`. There is no way to remove the Password Synchronization Plug-in from the appliance.

Procedure

1. Log on to the computer where either of these products is configured for password synchronization.
   - IBM Security Access Manager WebSEAL
   - IBM Security Access Manager Web Plug-in for Web server
2. Open the following file in the `etc` directory:
   - WebSEAL: `default-webseald.conf`
   - Web Plug-in: `pdwebpi.conf`
3. In the `[authentication-mechanisms]` stanza, comment out or delete the two lines added to remove the Password Synchronization Plug-in configuration:

   ```
   passwd-strength
   post-pwdchg-process
   ```
4. Delete files added during the installation process if required.
5. Restart the IBM Security Access Manager WebSEAL or the IBM Security Access Manager Web Plug-in for Web server.
6. Optional: If no longer required, disable password synchronization in IBM Security Identity Manager.

Chapter 7. Definitions for WEBSEAL_HOME and WEBPI_HOME directories

Typically, the WebSEAL and the WEB Plug-in products are installed in their default directories. The installation directories are called the home directories.

The IBM Security Access Manager WebSEAL home directory is *WEBSEAL_HOME*. The default locations depend on the operating system.

Windows systems
drive:\Program Files\Tivoli\PDWeb

UNIX systems
/opt/pdweb

The IBM Security Access Manager Web Plug-in for Web Server home directory is *WEBPI_HOME*. The default locations depend on the operating system.

The default locations for the home directories of these products are typically:

Windows systems
drive:\Program Files\Tivoli\PDWebPI

UNIX systems
/opt/pdwebpi

Appendix A. Support information

You have several options to obtain support for IBM products.

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).

   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
2. Find the content that you need by using the IBM Support Portal.

   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports).
   - IBM Security Identity Manager Support website.
   - IBM Redbooks®.
   - IBM support communities (forums and newsgroups).
4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.
5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to

include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Obtaining a product fix

A product fix might be available to resolve your problem.

About this task

You can get fixes by following these steps:

Procedure

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the *Fix Central Site*. See http://www.ibm.com/support/fixcentral/.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.

Contacting IBM Support

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):

     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.

     a. Download and install the ISA tool from the ISA website. See http://www.ibm.com/software/support/isa/.
     b. Open ISA.

c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.

- Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

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

Appendix B. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

IBM and accessibility

See the IBM Human Ability and Accessibility Center For more information about the commitment that IBM has to accessibility.

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:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 might 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 document 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 measurement 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 contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

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

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

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 http://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.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

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

Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, and to tailor interactions with the end user or for other purposes. In many cases, no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled "Cookies, Web Beacons and Other Technologies and Software Products and Software-as-a Service".

Index

Printed in USA