IBM Security Verify Identity
7.0

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

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The Password Synchronization Plug-in enables communication between the Identity server and the IBM Security Verify Access 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 Verify Identity
- IBM Security Verify Access
- IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access Plug-in for Web Server
- IBM Security Verify Identity Adapter for IBM Security Verify Access
- Password Synchronization Plug-in

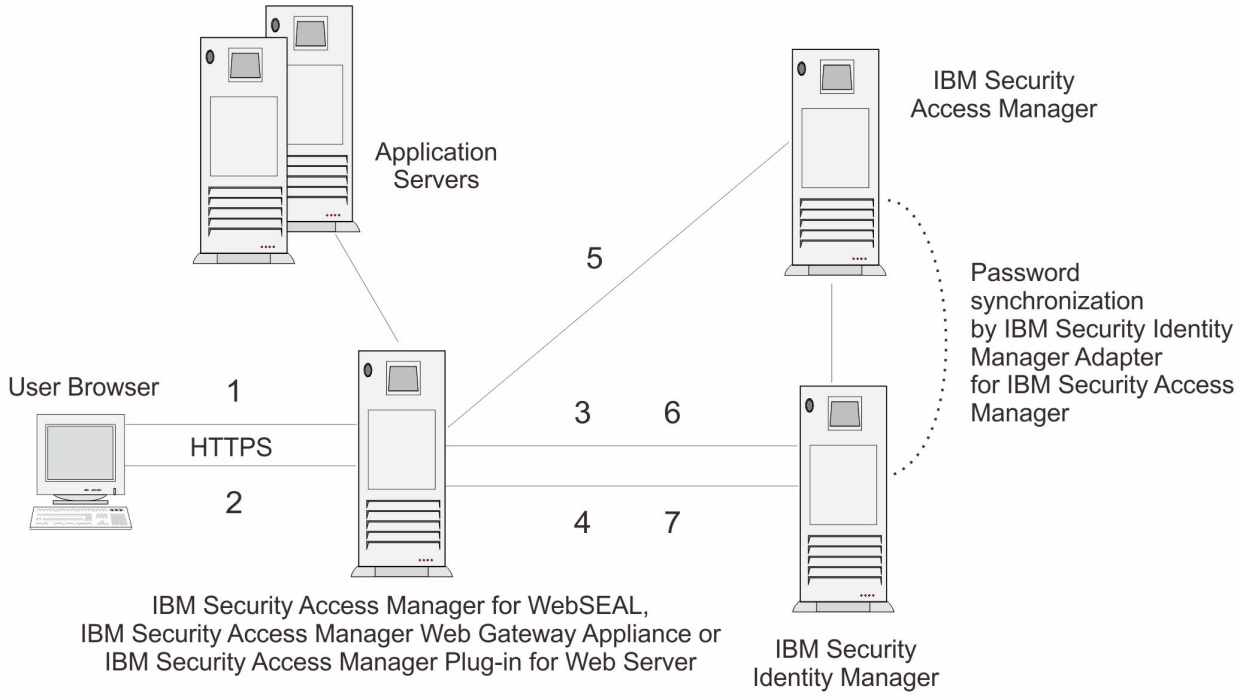

Figure 1. System architecture that shows password synchronization flow

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

1. A user submits a password change request to IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access Plug-in for Web Server.
2. IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access Plug-in for Web Server prompts the user to enter a new password.
3. IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access Plug-in for Web Server sends a request to IBM Security Verify Identity to check the new password against password policy for the specified service.

4. IBM Security Verify Identity responds to IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 Verify Access environment if the password check is successful.
6. WebSEAL or the Web Plug-in submits a second request to IBM Security Verify Identity to synchronize the new password for the specified user.
7. IBM Security Verify Identity returns a status to IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access Plug-in for Web Server that the password request is submitted.

Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

Use the Preinstallation roadmap to prepare the environment..

Table 1. Preinstallation roadmap

Task	For more information, see
Verify that your environment meets the software and hardware requirements for the adapter.	“Prerequisites” on page 3
Obtain the installation software.	“Software downloads” on page 4.
Obtain the necessary information for the installation and configuration.	“Installation worksheet” on page 5.

Use the Installation and configuration roadmap to complete the actual installation and configuration of the adapter.

Table 2. Installation and configuration 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 Verify Access for WebSEAL or IBM Security Verify Access Plug-in for Web Server” on page 11.
Verify the plug-in installation.	See “Verifying the installation” on page 17.

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 3. 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

Table 3. Prerequisites to install the plug-in (continued)	
Prerequisite	**Description**
System Administrator authority	The person who performs the plug-in installation procedure must have system administrator authority to complete the steps.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
IBM Security Verify Access	• IBM Security Verify Access 7.0 • Either of the following products: – IBM Security Verify Access WebSEAL 7.0 – IBM Security Verify Access Web Gateway Appliance 7.0 – IBM Security Verify Access Plug-in for Web Servers version 7.0

Software downloads

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

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Identity 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 4. 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**

Table 4. Distribution package contents (continued)	
Directory Name	**Description**

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

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 5. Required information to install the plug-in	
Required information	**Description**
An IBM Security Verify Identity Administrator Account.	To set password synchronization within the IBM Security Verify Identity you need access to an account with administration privileges.
An Administrator account on the server where IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access Plug-in for Web Server.

Chapter 3. Installing

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

1. Enable password synchronization on the IBM Security Verify Identity Server. See the online help or the IBM Security Verify Identity product documentation for specific instructions about IBM Security Verify Identity password synchronization.
2. Install the Password Synchronization Plug-in on the IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 3.
2. Obtain a copy of the installation software.
   See Software download.
3. Obtain system administrator authority.
4. Check the configuration.

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

   a. Log in to IBM Security Verify Identity 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 Verify Access 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 Verify Identity Policy and Organization Administration Guide*.

Related tasks

Enabling password synchronization in the IBM Security Verify Identity Server

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

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

Enabling password synchronization in the IBM Security Verify Identity Server

To enable password synchronization between accounts, you must configure the IBM Security Verify Identity password synchronization feature. These steps apply to IBM Security Verify Identity 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 Verify Identity server does not synchronize the IBM Security Verify Access password with the passwords for other accounts.

Procedure

1. Log in to IBM Security Verify Identity 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**.

Related tasks

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

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

Installing the Password Synchronization Plug-in

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

About this task

If you are configuring the Password Synchronization Plug-in on the IBM Security Verify Access Web Gateway Appliance, you can skip the following procedure because the plug-in is pre-installed on the appliance. Continue to Chapter 4, “Configuring,” 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 Verify Access WebSEAL
     WEBSEAL_HOME`/etc/webseald-`*`default`*`.conf`

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

IBM Security Verify Access 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
```

Related tasks

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

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

Chapter 4. Configuring

After you install the adapter, you must complete several other tasks. The tasks include configuring the adapter, setting up SSL, 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 Verify Identity Server. If IBM Security Verify Identity 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 Verify Access for WebSEAL or IBM Security Verify Access Plug-in for Web Server.
2. Configure the Password Synchronization Plug-in for IBM Security Verify Access Web Gateway Appliance.

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

The Password Synchronization Plug-in uses the HTTPS protocol. It must be configured to accept the corresponding IBM Security Verify Identity 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 Verify Access 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 Verify Access WebSEAL
   WEBSEAL_HOME`/etc/webseald-default.conf`

   IBM Security Verify Access 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 Verify Identity server that hosts the IBM Security Verify Identity Adapter for IBM Security Verify Access. 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 Verify Identity 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 Verify Identity manager account.

* This entry is mandatory.

principal-password
The password for the IBM Security Verify Identity 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 Verify Identity LDAP organization context, and the `erservicename` attribute of the IBM Security Verify Access service name, as defined in IBM Security Verify Identity. 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 Verify Access WebSEAL or IBM Security Verify Access Web Plug-in for Web Server.

Related concepts

Pseudo-distinguished name values

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

Related tasks

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

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

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

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

Procedure

1. Log in to the IBM Security Verify Access 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 Verify Access 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 Verify Access Web Gateway Appliance.

Table 6. Attributes (continued)	
Attributes	**Description**
`itim-server-name`	This entry is the host name or IP address of the IBM Security Verify Identity server that hosts the IBM Security Verify Access Adapter for IBM Security Verify Access. 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 Verify Access 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 Verify Access manager account. This entry is mandatory.
`principal-password`	The password for theIBM Security Verify Identity 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 Verify Access LDAP organization context, and • the `erservicename` attribute of the IBM Security Verify Access service name, as defined in IBM Security Verify Access. 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. 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 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`. c. `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 Verify Access 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 Verify Access 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**.

Related concepts

Pseudo-distinguished name values

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

Related tasks

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

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

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=
        00000000000000000000,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
```

Related tasks

Configuring the Password Synchronization Plug-in for IBM Security Verify Access for WebSEAL or IBM Security Verify Access Plug-in for Web Server
The Password Synchronization Plug-in uses the HTTPS protocol. It must be configured to accept the corresponding IBM Security Verify Identity service.

Configuring the Password Synchronization Plug-in for IBM Security Verify Access Web Gateway Appliance
The Password Synchronization Plug-in uses the HTTPS protocol. It must be configured to accept the corresponding IBM Security Verify Identity service.

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 Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 Verify Identity with the new password from the previous step.

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

Chapter 5. Troubleshooting

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. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

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 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 you start 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 operating system, or is it common across multiple 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 are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead 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 use 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 done?
- Is a certain sequence of events required 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 occur 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. 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?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Related concepts

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

Known issues

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

Trace level enablement

The Password Synchronization Plug-in for IBM Security Verify Access 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 Verify Access WebSEAL or IBM Security Verify Access for Web Plug-in log files.

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

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

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 Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access Plug-in for Web Server is unable to start after installation of the Password Synchronization Plug-in.	Review the IBM Security Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 Verify Access for WebSEAL, IBM Security Verify Access Web Gateway Appliance or IBM Security Verify Access 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 Verify Identity.
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.

Related concepts

Techniques for troubleshooting problems
Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

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

Chapter 6. Uninstalling

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 Verify Access 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 Verify Access WebSEAL
   - IBM Security Verify Access 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 Verify Access WebSEAL or the IBM Security Verify Access Web Plug-in for Web server.
6. Optional: If no longer required, disable password synchronization in IBM Security Verify Identity.

Chapter 7. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

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 Verify Access 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 Verify Access 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

Index

U

V