IBM Security Verify Identity
7.0

Password Synchronization for Active Directory Plug-in Installation and Configuration Guide

Contents

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The IBM® Security Verify Identity Password Synchronization plug-in enables connectivity between the IBM Security Verify Identity server and a system that runs the domain controller. This installation guide provides the basic information that you can use to install and configure the Password Synchronization plug-in.

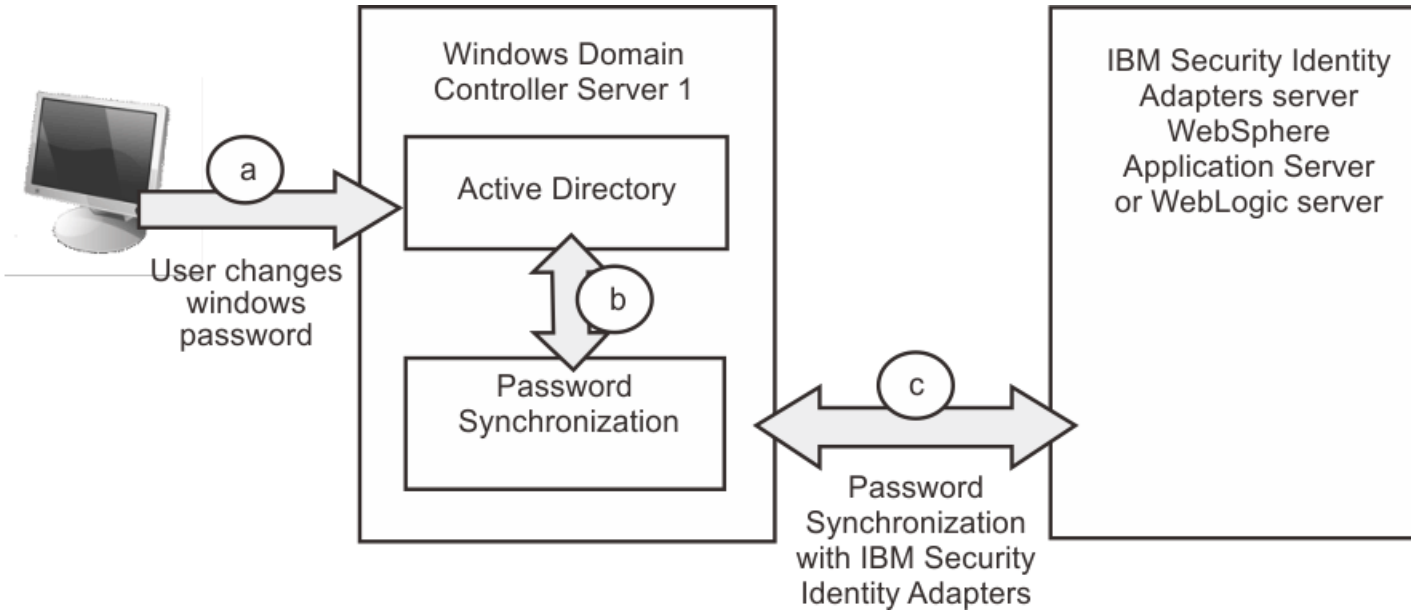
Features of the plug-in

The Password Synchronization plug-in intercepts the domain user password changes and communicates with IBM Security Verify Identity for password rules verification and synchronization.

The new password is synchronized with other accounts managed by IBM Security Verify Identity for the domain user.

Interaction among Active Directory, IBM Security Verify Identity, and the plug-in

The Active Directory and Password Synchronization plug-in work together for password change requests originating from IBM Security Verify Identity.



A client initiates the password change request directly to Active Directory, which is installed with the Password Synchronization plug-in on the domain controller. IBM Security Verify Identity is installed on a separate server.

Following is the sequence of the operations.

1. The user changes an account password by first selecting Ctrl + Alt + Delete and then clicking **Change Password**. The password change on the resource can also be initiated:
   a. On a domain controller workstation, select **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
   b. Browse to the appropriate container or organization unit. Select the user whose password is to be changed. Right click the user and click **Reset password**.

   See **a** in the illustration.

2. The Windows operating system captures the password change event. Before the password is changed on the resource, the Password Synchronization plug-in is started. The user ID and password are passed to the plug-in. See **b** in the illustration.
3. If 'Enable Password rules' is enabled for the Password Synchronization plug-in, the plug-in sends the password to IBM Security Verify Identity for rules verification. If the password matches the rules defined in IBM Security Verify Identity, then IBM Security Verify Identity sends success back to Password Synchronization plug-in. The plug-in notifies the Windows operating system that the password complies to the password rules and can proceed. The password is then changed on the resource.

   After the password change, the Windows operating system again invokes the Password Synchronization plug-in to indicate that the password change operation is successful. The Password Synchronization plug-in then sends SUCCESS to IBM Security Verify Identity for the password change operation. Upon receipt of success, IBM Security Verify Identity then synchronizes the password with rest of the accounts of the user. See **d** in the illustration.

Password recursion prevention is now controlled by IBM Security Verify Identity. See "Preventing recursion" on page 2

Preventing recursion

The password synchronization plug-in does not distinguish between password changes that are initiated by users, or password changes that are initiated by the Windows Active Directory adapter. You must modify the **enrole.passwordsynch.enabledonresource** property to prevent the IBM Security Verify Identity server from processing its own password change requests to the adapter as password synchronization requests.

Procedure

1. On the IBM Security Verify Identity, go to the *ISIM_HOME*/data directory.
2. Open theenRole.properties file with an editor.
3. Locate the entry enrole.passwordsynch.enabledonresource
4. Change the default value false to true.

```
################################################################################
## Below are the properties to Support Multiple Password-synch Agents
## An indication that a password change or restore request from ITIM may
## result in a reverse password synch\validation request from the plugin
## installed on resource. Default: false
enrole.passwordsynch.enabledonresource=true

## Specifies the maximum duration in seconds between a password change
## request sent from ITIM to remote agent, and recieving a reverse password
## synch request from the plugin installed on the remote resource.
## Default: 60 (sec)
enrole.passwordsynch.toleranceperiod=60

## Password synch transaction monitor settings (heartbeat is in HOURS).
## Default: 1 (hour)
enrole.PasswordSynchStoreMonitor.heartbeat=1
```

5. Save the enRole.properties file.

Chapter 2. Planning

Installing and configuring the Password synchronization plug-in involves several steps that you must complete in a specific sequence. As such, follow the roadmaps.

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 download" on page 3.
Obtain the necessary information for the installation and configuration.	"Installation worksheet" on page 4.

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, see**
Install the plug-in.	"Installing the Password Synchronization plug-in" on page 5
Verify the installation.	"Verifying the installation" on page 10.
Configure SSL communications.	"SSL authentication configuration for the plug-in" on page 15.

Prerequisites

Verify that all of the prerequisites are met before you install the Password Synchronization plug-in.

Table 3 on page 3 identifies installation prerequisites for this plug-in.

Table 3. Prerequisites to install the plug-in	
Prerequisite	**Description**
System	A Windows Server 2012 or Windows Server 2016 running Active Directory. Both 32-bit or 64-bit versions are supported **Note:** The Password Synchronization plug-in supports only x86 architecture, however, the Password Synchronization plug-in does not have Itanium support.
System Administrator Authority	The person who completes the Password Synchronization plug-in installation procedure must have system administrator authority to complete the steps in this chapter.
Identity server	Version 6.0

Software download

Download the adapter software from your account in IBM Passport Advantage Online.

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.

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 4. Information worksheet

Required information	**Description**
Installation directory	The location where the plug-in is installed. The default is `C:\Program Files\IBM\ISIM\Agents\PasswordSynch`
IBM Security Verify Identity Application server	IP address and SSL port
Target DN for the service	On the IBM Security Verify Identity server
IBM Security Verify Identity/> account	The account under which the requests are submitted.
IBM Security Verify Identity account password	The password for the IBM Security Verify Identity account under which the requests are submitted.

Chapter 3. Installing

Install the plug-in to achieve password synchronization.

Installing the Password Synchronization plug-in

You must install the plug-in on all the Windows Directory Domain Controllers in the domain. To install the plug-in on the Windows Core Server, use the **(-i console)** or the **(-i silent)** install option because a GUI based installer is not supported.

Before you begin

- Verify that your site meets all the prerequisite requirements. See "Prerequisites" on page 3.
- Obtain a copy of the installation software. See "Software download" on page 3.
- Obtain system administrator authority.

Procedure

1. If you downloaded the installation software from Passport Advantage, perform the following steps:
   a) Create a temporary directory on the computer on which you want to install the software.
   b) Extract the contents of the compressed file into the temporary directory.
2. Start the installation program with the `SetupPwdSynch.exe` file in the temporary directory.

   Note:

   - For Windows Core Server installation, use the following command:

     ```
     SetupPwdSynch.exe -i console
     ```

   - When you install the Windows Password Synchronization plug-in with the Windows Remote Desktop, ensure that you open the remote desktop connection by using the command **mstsc/ console**. If you do not do so, the following issue might occur:

     The Windows Password Synchronization plug-in is installed successfully. However, on restarting the domain controller the `TivoliPwdSync DLL` is not loaded and the `PwdSync.log` file is not created under the log directory of the plug-in.
3. Select a language and click **OK**.
4. On the Introduction window, click **Next**.
5. Specify where you want to install the adapter in the **Directory Name** field. Perform one of the following actions:
   - Click **Next** for the default location.
   - Click **Choose** and navigate to a different directory and click **Next**.
6. Choose the CA certificate file and click **Next**.

   For information about CA certificates installation after Password Synchronization plug-in installation, see "Installing CA certificates" on page 9.
7. Review the installation settings in the Pre-Installation Summary window and do one of the following actions:
   - Click **Previous** and return to a previous window to change any of these settings.
   - Click **Install** when you are ready to begin the installation.
8. Complete all of the text fields in the **PFConfig**window.

   Note:

- The **pfconfig** utility cannot be run on the Windows Core Server. It is included as a separate executable program in the adapter package and can be used to remotely configure the plug-in.
- For Windows Core Server installation:
  - Run the **pfconfig** utility after installation, on a machine that is a member of the domain hosted by the core machine. You need to be logged on with an account that has *read/write* access to the registry and *read* access to the system certificate store on the target server.
  - Click **Change Host** to select the remote host to configure and then complete the required information

The **PFConfig**window has the following fields:

Installation Path
Specifies the installation path for the Password Synchronization plug-in. The value specified must match with the installation directory value entered earlier in the installation process.

Host Name or IP
Specifies the IP address for the IBM Security Verify Identity server.

SSL Port Number
Specifies the SSL port for the IBM Security Verify Identity server. The default SSL port for WebSphere® Application Server is 9443 on a single server setup. If you have a WebSphere Application Server cluster, the IBM HTTP Server must be configured for SSL. The default port for HTTP SSL is 443. For example, `shreth.tivlab.austin.ibm.com:9443`

Note: For more information about configuring certificates, see "Installing CA certificates" on page 9.

Connection Timeout

This is the timeout value, in seconds, of the send and receive operations when communicating with the IBM Security Verify Identity server.

User Certificate

This field contains the serial number of the selected user certificate, which is used when the IBM Security Verify Identity server is configured for two-way SSL and requires a client certificate for the SSL handshake. Click the **Select** button to select a certificate from the system certificate store.

Validate CN of server certificate to host name

Select this option to verify that the CN of the subject name in the server certificate, received during the SSL handshake, is the same as the hostname of the IBM Security Verify Identity server.

Registered Certificate

Click this button to view details of the currently registered certificate, if any. The **Registered Certificate** dialog box includes options for registering and unregistering a certificate and for enabling verification of the registered certificate.

Unregister

Click this button to remove the currently registered certificate and to disable the registered certificate validation.

Register New Cert

Click this button to register a new certificate. A dialog box is displayed where you can select the certificate file. The file must contain a single certificate and must be in binary (der) format.

Note: When you register a new certificate, the previously registered certificate is automatically removed.

Enable Registered Cert Validation

Select this option to enable the validation of the registered certificate after the SSL handshake.

When you register a certificate, it is compared with the server certificate received in the SSL handshake. The certificates much match exactly. Only connections that have the registered certificate during the SSL handshake are allowed.

Service DN

At the Service DN field, click **Configure Target Services**. A list of configured target services is displayed.

Note: One copy of the Password Synchronization client can monitor multiple base points. Enter each of the points by using the Target Services window.

To edit a target service, click the service and click **Edit**. The Base Point and Service Target DN specifications are displayed. The base point in the Active Directory must match the Service Target DN on the IBM Security Verify Identity server.

Base Point

The base points specified must be identical to the base points configured in your Active Directory Adapter. The default base point is the root domain of the Active Directory.

Example 1

If the root of Active Directory is `Cascades.Irvine.IBM.com`, the Base Point must be specified as:

```
dc=Cascades,dc=Irvine,dc=IBM,dc=com
```

Example 2

If you installed the Windows Active Directory Adapter in an OU (organizational short name) of your Active Directory, **Users**, the Base Point is entered as:

```
cn=Users,dc=Cascades,dc=Irvine,dc=IBM,dc=com
```

Service Target DN

The format is:

```
erservicename=nameofservice,o=organizationname
ou=organizationshortname,dc=com
```

Note: Although DN formatting is used for the Service DN value, this DN is **not** the DN of the service that is being monitored. These values are parameter values to the Password Synchronization plug-in.

erservicename

Specifies the name of the target service used by the IBM Security Verify Identity server

o

Specifies the name of the organization on the IBM Security Verify Identity server

ou

Specifies the short name defined for the organization during installation and configuration of the IBM Security Verify Identity server. If this value is not known, it can be determined by opening the LDAP configuration tool for your product. Locate the new root suffix created during the IBM Security Verify Identity installation.

dc=*com*

Specifies the root of the directory tree.

For example, if you installed the IBM Security Verify Identity server in the root LDAP suffix called **ISIM** and your Windows Active Directory service is named **WinAD Corp Server** and is installed in an organization named **Finance Org**, the IBM Security Verify Identity organization chart looks similar to the following diagram:

- + ISIM Home
  - + Corporate Org
    + IT Org Unit
    + HR Org Unit
  - + Finance Org
    + Accounts Payable Org Unit

This Windows Active Directory Adapter example has the following Service DN value:

```
erservicename=WinAD Corp Server,o=Finance Org,
ou=ITIM,dc=com
```

Principal
Specifies the IBM Security Verify Identity account under which the password change requests are submitted. The account must have the proper authority to submit password change requests for the specified people. This authority is granted when you create the access control information (ACI) for the Principal account by granting read and write permissions to all the attributes that were listed.

At a minimum, the principal must be granted read and write permissions to perform the following tasks for password synchronization:

a. Search for the account that triggered the password synchronization
b. Search for the owner of that account.
c. Search for any accounts that are to have their passwords synchronized.
d. Modify those same accounts, with write access to their password attributes.

Create an account specifically for these types of requests.

Refer to the IBM Security Verify Identity Information Center for more information about creating accounts and privileges.

Password
Specifies the password for the IBM Security Verify Identity account under which the password change requests are submitted

Verify Password
Specifies the verification field for the IBM Security Verify Identity account password

Max Notify Thread Count
Specifies the maximum number of Password Change requests which can be processed by the plug-in at any one time. The plug-in processes password synchronization requests in a multi-threaded manner. This value limits the number of threads to be created, so that requests can be processed in parallel.

For example, if this value is specified as *15*, then the Password Synchronization plug-in processes only 15 parallel password change requests at any one time. The next password change request after 15 fails.

The default value for this parameter is **10**.

Enable Password Synchronization
Specifies whether to enable or disable password synchronization.

When password synchronization is enabled, all password change requests are sent to IBM Security Verify Identity to synchronize all passwords affected by the change request. When password synchronization is not enabled, the Password Synchronization plug-in ignores all password change requests on the managed resource.

Enable Password Rules Verification
Validates that the password complies with the password rules defined for the user.

When this option is selected, the new password is checked against the password policy rules that is defined in the account. The password must be valid for all accounts. Otherwise, the password change fails with an error that indicates that the new password does not meet specified password rules. Refer to the IBM Security Verify Identity Information Center for more information about setting IBM Security Verify Identity password policies.

Require Response
This option is enabled only if **Enable Password Rules Verification** is selected. When this option is selected, passwords cannot be changed on IBM Security Verify Identity when it is unavailable.When this option is enabled password changes fail if the Identity server is down. All attempts to change the password results in an error, that indicates the password did not meet the password rule requirements.

Enable Logging
Allows administrators to enable logging for password change requests, which are sent to the Active Directory server.

Number of log files

This value controls the number of log files that are maintained.

Max log file size

This value controls the maximum size of the log files (in KB).

9. In the **Install Complete** window, answer the question about restarting the system, and click **Done**.
10. Restart the Active Directory server.

Note:

a. The connection information can be modified at a later time by running the `pfconfig.exe` program. This program opens the IBM Security Verify Identity Password Change Notification Configuration page.
b. The Restart panel might not be displayed. For password synchronization to function correctly, you must install CA certificate and restart the system.
c. When you change in SSL configuration such as by adding or removing a certificate, you must restart the system.

What to do next

After you finish the installation, you must install CA certificates. See "Installing CA certificates" on page 9.

Installing CA certificates

To install the CA certificates after you install the Password Synchronization plug-in, follow the steps below.

Procedure

1. Go to **Start** > **Run** and type `mmc` and click **OK** or press **Enter**.
2. From the Console menu, select **Add/Remove Snap-in**.
3. From the Add/Remove Snap-in window, click **Add** to display the Add Standalone Snap-in window.
4. From the Add Standalone Snap-in window, select **Certificates** and click **Add**.
5. On the Certificates Snap-in window, select **Computer Account** and click **Next** to display the Select Computer window.
6. Select **Local computer** and click **Finish**, **Close**, and then **OK**.
7. Expand **Certificates (Local computer) > Trusted Root Certification Authorities** and select **Certificates**.
8. Right-click **Certificates** and select **All Tasks > Import** to display the Certificate Import Wizard and click **Next**.

9. Browse or type the name of the CA certificate for the IBM Security Verify Identity server and click **Next**.
10. Select **Place all certificates in the following store** option and click **Next** and then click **Finish**.

    You can also use the `CertMgr.exe` command line tool to install the CA certificates after the Password Synchronization plug-in installation.

    When you use the `CertMgr.exe` command line tool to install the CA certificates, run the following command:

    ```
    CertMgr -add -c certificate file -s -r localMachine root
    ```

    where *certificate file* is the full path to the certificate file.

Verifying the installation

You can take these steps to verify the installation.

Procedure

- Determine that the required directories are created.
  - bin
  - jre
  - license
  - log
  - Uninstall_Tivoli Windows Password Synch Plugin
- Determine that the following files were created in the system32 directory such as `C:\Windows\system32`.

Table 5. Operating system and file

Operating system	File
32-bit operating system	TivoliPwdSync.dll
64-bit operating system	TivoliPwdSync64.dll

- Review the installer log file for any errors.

  The log file `Tivoli_Windows_Password_Synch_Plugin_InstallLog.log` is located in the installation directory, for example, `C:\Program Files\IBM\PasswordSynch`.
- When you use `regedit.exe` or `regedt32.exe`, ensure that the Windows registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages` includes TivoliPwdSync for 32-bit operating systems and TivoliPwdSync64 for 64-bit operating systems.
- Ensure that your certificates are installed correctly. The SSL handshake fails when the certificate or the CA is not installed.

Installing and uninstalling in silent mode

Silent installation suppresses the adapter installation wizard and the Launcher User Interfaces (UIs). It does not display any information or require interaction.

You can use the –silent option to install or uninstall the adapter in silent mode.

Note:

- The plug-in installs runtime files from Microsoft. The installer for these runtime files shows some user interfaces and you cannot suppress these user interfaces.

- If you install the plug-in in silent mode, the uninstaller runs in silent mode irrespective of whether you are using the –silent option or not.

Installing the plug-in by using silent mode

Take these steps to install the plug-in in silent mode.

Procedure

- **Installing the plug-in with default options**

  To install the adapter with the –silent option:

  1. Navigate to the location where you stored the `SetupPwdSynch.exe`.
  2. Run the following command from command prompt:

     ```
     SetupPwdSynch.exe -i silent -DLICENSE_ACCEPTED=TRUE
     ```

  The adapter is installed in the adapter installation directory, `C:\Program Files\IBM \PasswordSynch`. A log file, `pwd_out.txt`, is created and the plug-in is installed with the default value, `%SYSTEM_DRIVE_ROOT%:\Tivoli\passwordsynch`.

  After you install the plug-in, you must:

  1. Run the `pfconfig.exe` (for the 32-bit version of the plug-in) and `pfconfig64.exe` (for the 64-bit version of the plug-in) from the `bin` directory and configure the plug-in.
  2. Install the CA certificates. For information about CA certificates installation, see “Installing CA certificates” on page 9.
  3. Restart the workstation.

- **Installing the plug-in with command-line options**

  You can specify the listed installation options from the command prompt when you install the plug-in by using the silent mode. For example, if you want to override the default installation directory path, run the following command:

  ```
  SetupPwdSynch.exe -i silent -DLICENSE_ACCEPTED=TRUE
  -DUSER_INSTALL_DIR="D:\Security\MyFolder"
  ```

  Note:

  – The `-D` option is followed by a variable and a value pair without any space after the `-D` option.

  – You must wrap arguments with quotation marks when the arguments contain spaces.

Table 6. Installation options

Option	Value
-DUSER_INSTALL_DIR=Value	Value overrides the default installation directory path. For example, *D*:\Tivoli*MyFolder*.
-DLICENSE_ACCEPTED=Value	Accept the IBM license for plug-in, the value must be TRUE. When you do not specify this option, the default value is FALSE.
-DUSER_CERT_FILE=Value	The name of the CA certificate file for your IBM Security Verify Identity server. For example, *My_CertfileName.cer*.
-DPATH_OF_CERT_FILE=Value	The full path of the CA certificate file (excluding the file name) for your IBM Security Verify Identity server. For example, *C:\CA_My_Folder*.

After you install the plug-in, you must:

1. Run `pfconfig.exe` (for the 32-bit version of the plug-in) and `pfconfig64.exe` (for the 64-bit version of the plug-in) from the `bin` directory and configure the plug-in.
2. Restart the workstation.

- **Installing the plug-in by using the response file**

  Generating the response file

  You can use a response file to provide inputs during silent installation. The response file can be generated by running the following command, which runs the installer in interactive mode and installs the plug-in.

  ```
  SetupPwdSync.exe –r "Full path of response file"
  ```

  For example:

  ```
  SetupPwdSync.exe –r "c:\temp\PwdSynResponse.txt"
  ```

  Note: If you run this command to generate only the response file, you must uninstall the plug-in by using the uninstaller.

  Creating the response file manually

  You can also manually create the response file with the following content:

  ```
  #Start of Response file

  #Choose Install Folder
  #---------------------
  USER_INSTALL_DIR=Value

  #Has the license been accepted
  #-----------------------------
  LICENSE_ACCEPTED=TRUE

  #Select CA Certificate file.
  #---------------------------
  USER_CERT_FILE=Value
  PATH_OF_CERT_FILE=Value

  #End of Response file
  ```

  After you create the response file, you can use it as:

  ```
  SetupPwdSynch.exe –i silent -f "Full path of response file"
  ```

  After you install the Password Synchronization plug-in, you must:

  1. Run pfconfig.exe (for the 32-bit version of the plug-in) and `pfconfig64.exe` (for the 64-bit version of the plug-in) from the `bin` directory and configure the plug-in.
  2. Reboot the workstation.

Uninstalling the plug-in by using silent mode

Run the following command from the command line to uninstall the Password Synchronization plug-in by using the –i silent option.

Procedure

1. Specify the full path when you are not running the command from `Uninstall_Tivoli Windows Password Synch Plugin` directory in the installation directory of the plug-in.

   ```
   "Uninstall Tivoli Windows Password Synch Plugin.exe" -i silent
   ```

   For example, `"C:\Program Files\IBM\ISIM\Agents\PasswordSynch\Uninstall_Tivoli Windows Password Synch Plugin\Uninstall Tivoli Windows Password Synch Plugin.exe" -i silent`.

2. Restart the workstation to completely remove the plug-in.

Chapter 4. Configuring

After you install the plug-in, configure it to function correctly and based on your requirements or preference.

SSL authentication configuration for the plug-in

You can establish a secure connection between IBM Security Verify Identity plug-in and IBM Security Verify Identity server.

You must configure the plug-in and the server to use the Secure Sockets Layer (SSL) authentication.

The IBM Security Password Synchronization plug-in sends sensitive password information over the network to the IBM Security Verify Identity server. For this reason, a Secure Sockets Layer (SSL) connection is required to communicate with the IBM Security Verify Identity server.

When configuring certificates for an SSL connection, there are two levels of validation. One-way SSL is achieved by the server that sends you its certificate and the software that verifies it is signed by a trusted Certificate Authority (CA). For additional security, the server can enforce two-way SSL and also request that the client provide a certificate to the server. It is validated the same way by ensuring it is signed by a trusted CA.

One-way SSL

At minimum, you must install the CA certificate that is the signer of the IBM Security Verify Identity server certificate to the local trust store. When a connection is requested, the server sends its certificate, which is verified, to be signed by a trusted CA. This is enough to establish a secure connection with the server.

Two-way SSL

For additional security, the IBM Security Verify Identity server can be configured to also request a certificate from the plug-in. This works the same as the server certificate, only in reverse. You must install a user certificate in the local certificate store and the CA certificate must be installed in the trust store on the IBM Security Verify Identity server. The extra security allows the IBM Security Verify Identity server to verify the source of the password change notification.

Additional SSL security options

It is important to ensure that the connection to the IBM Security Verify Identity server is secure because the password synchronization plugin sends password information. At minimum, the plugin requires an SSL connection. One-way SSL only verifies that the plugin trusts the signer of the certificate received in the handshake, and establishes an encrypted session. Two-way SSL is enforced by the target IBM Security Verify Identity server and it also just verifies that the signer of the client certificate is trusted.

The SSL handshake can be configured to verify that the CN of the subject in the server certificate, received in the handshake, matches the hostname of the server. You can enable this option in `pfconfig`. If the hostname does not match the CN, the connection is refused.

For additional security, the IBM Security Verify Identity server certificate can be registered with the password synchronization plugin. A binary copy of the certificate is stored by the plugin. Only those server connections that present the server certificate are accepted. This option ensures that only connections to the IBM Security Verify Identity server are allowed. The is configured in the Registered Certificate section of `pfconfig`.

Installing the IBM Security Verify Identity CA certificate

Since the Password Synchronization plug-in runs as a system extension, you must install the certificates in the system certificate store.

Procedure

1. Run the Microsoft Management Console.
2. Select **File** > **Add/Remove Snap-in**.
3. Under **Available snap-ins**, select **Certificates**, and click **Add**.
4. Select **Computer Account**, read the screen prompts, and click **Finish**.
5. Click **OK**.

   The Certificates Plug-in is loaded into the Microsoft Management Console.
6. Install the CA certificate from the IBM Security Verify Identity server:
   a) Browse to **Certificates/Trusted Root Certification Authorities**.
   b) Right-click **Certificates**, and select **All Tasks** > **Import**.
   c) Select the CA certificate file for the IBM Security Verify Identity server.

Setting user certificates for 2-way SSL

If the IBM Security Verify Identity server has been configured to use 2-Way SSL, you must specify a user certificate to present to the IBM Security Verify Identity server when connecting.

The plug-in runs as a system extension and uses the system certificate store to access certificates.

To uniquely identify a certificate you need the issuer and the serial number. The plug-in stores the issuer name as an X500 name string and the serial number as a hex string in the registry.

The easiest way to set these values is to use the `pfconfig` tool to select the certificate and the tool will update the registry with the issuer and serial number. You can also manually add the issuer name and serial number to the registry.

Using pfconfig to select user certificates

You can select the certificate for 2-way SSL by using the `pfconfig.exe` configuration tool.

1. Start the `pfconfig.exe` configuration tool.

   The **User Certificate Serial number** is displayed.
2. Open the **Select Certificate** dialog box.

   A list of user certificates in the system certificate store by name is displayed.
3. Click a certificate name to update the details display.

   This step ensures that you have selected the correct certificate. If the certificate you want to use is not in the list, you must first install the certificate in the system certificate store.
4. After you have selected the certificate, click **Select** to update the configuration.

Manually setting the user certificate

The user certificate is identified by the issuer name and serial number which are stored in the registry values `CertIssuerName` and `CertSerialNumber`. Use the Certificate snap-in in the Microsoft Management Console to get the issuer and serial number.

Procedure

1. In the Microsoft Management Console, open the certificate in the **Certificates** snap-in.
2. Select the **Details** tab.

3. To obtain the issuer name for the `CertIssuerName` registry value, complete the following steps:
   a) Locate the **Issuer** field and value. For example: `cdm-BALBOA-CA,cdm,newport,cm,example,com`
   b) In the lower panel, take note that the value for the **Issuer** field is represented in a different way, on multiple lines. For example:

```
CN = cdm-BALBOA-CA
DC = cdm
DC = newport
DC = cm
DC = example
DC = com
```

   c) Starting from the last line, combine each value into one line.

      Note: Do modify the certificate values in the **Details** tab.

      For example: `DC = com DC = example DC = cm DC = newport DC = cdm CN = cdm-BALBOA-CA`
   d) Remove the spaces surrounding the equal sign (=).
      For example: `DC=com DC=example DC=cm DC=newport DC=cdm CN=cdm-BALBOA-CA`
   e) Separate each item with a comma (,), and an empty space ( ).
      For example: `DC=com, DC=example, DC=cm, DC=newport, DC=cdm, CN=cdm-BALBOA-CA`
4. To get the serial number for the `CertSerialNumber` registry value, complete the following steps:
   a) Identify the **Serial number** field.
   b) Take note of the value.

      For example: `35 bc 7a f7 00 00 00 00 00 0f`
   c) Switch the order of the serial numbers, so that the numbers match the order with the certificate store.

      For example: `0f 00 00 00 00 f7 7a bc 35`

Overview of SSL and digital certificates

You can deploy IBM Security Verify Identity into an enterprise network. You must secure communication between the IBM Security Verify Identity server and the software products and components with which the server communicates.

The industry-standard SSL protocol, which uses signed digital certificates from a certificate authority (ca) for authentication, is used to secure communication in a IBM Security Verify Identity deployment. Additionally, SSL provides encryption of the data exchanged between the applications. Encryption makes data transmitted over the network intelligible only to the intended recipient.

Signed digital certificates enable two applications connecting in a network to authenticate each other's identity. An application acting as an SSL server presents its credentials in a signed digital certificate to verify to an SSL client that it is the entity it claims to be. An application acting as an SSL server can also be configured to require the application acting as an SSL client to present its credentials in a certificate, thereby completing a two-way exchange of certificates. Signed certificates are issued by a third-party certificate authority for a fee. Some utilities, such as those provided by OpenSSL, can also issue signed certificates.

A certificate-authority certificate (ca certificate) must be installed to verify the origin of a signed digital certificate. When an application receives another application's signed certificate, it uses a ca certificate to verify the originator of the certificate. A certificate authority can be well-known and widely used by other organizations, or it can be local to a specific region or company. Many applications, such as Web browsers, are configured with the ca certificates of well known certificate authorities to eliminate or reduce the task of distributing ca certificates throughout the security zones in a network.

Private keys, public keys, and digital certificates

Keys, digital certificates, and trusted certificate authorities are used to establish and verify the identities of applications.

SSL uses public key encryption technology for authentication. In public key encryption, a public key and a private key are generated for an application. Data encrypted with the public key can only be decrypted using the corresponding private key. Similarly, the data encrypted with the private key can only be decrypted using the corresponding public key. The private key is password-protected in a key database file so that only the owner can access the private key to decrypt messages that are encrypted using the corresponding public key.

A signed digital certificate is an industry-standard method of verifying the authenticity of an entity, such as a server, client, or application. In order to ensure maximum security, a certificate is issued by a third-party certificate authority (ca). A certificate contains the following information to verify the identity of an entity:

Organizational information
This section of the certificate contains information that uniquely identifies the owner of the certificate, such as organizational name and address. You supply this information when you generate a certificate using a certificate management utility.

Public key
The receiver of the certificate uses the public key to decipher encrypted text sent by the certificate owner to verify its identity. A public key has a corresponding private key that encrypts the text.

Certificate authority's distinguished name
The issuer of the certificate identifies itself with this information.

Digital signature
The issuer of the certificate signs it with a digital signature to verify its authenticity. This signature is compared to the signature on the corresponding ca certificate to verify that the certificate originated from a trusted certificate authority.

Web browsers, servers, and other SSL-enabled applications generally accept as genuine any digital certificate that is signed by a trusted Certificate Authority and is otherwise valid. For example, a digital certificate can be invalidated because it has expired or the ca certificate used to verify it has expired, or because the distinguished name in the digital certificate of the server does not match the distinguished name specified by the client.

Self-signed certificates

You can use self-signed certificates to test an SSL configuration before you create and install a signed certificate that is issued by a certificate authority.

A self-signed certificate contains a public key, information about the owner of the certificate, and the owner's signature. It has an associated private key, but it does not verify the origin of the certificate through a third-party certificate authority. Once you generate a self-signed certificate on an SSL server application, you must extract it and add it to the certificate registry of the SSL client application.

This procedure is the equivalent of installing a ca certificate that corresponds to a server certificate. However, you do not include the private key in the file when you extract a self-signed certificate to use as the equivalent of a ca certificate.

Use a key management utility to generate a self-signed certificate and private key, extract a self-signed certificate, and add a self-signed certificate.

Where and how you choose to use self-signed certificates depends on your security requirements. In order to achieve the highest level of authentication between critical software components, do not use self-signed certificates, or use them selectively. For example, you can choose to authenticate applications that protect server data with signed digital certificates, and use self-signed certificates to authenticate Web browsers or IBM Security Verify Identity plug-ins.

If you are using self-signed certificates, in the following procedures you can substitute a self-signed certificate for a certificate and ca certificate pair.

Certificate and key formats

Certificates and keys are stored in files with the following formats:

.pem format

A privacy-enhanced mail (.pem) format file begins and ends with the following lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

A .pem file format supports multiple digital certificates, including a certificate chain. If your organization uses certificate chaining, use this format to create ca certificates.

.arm format

An .arm file contains a base-64 encoded ASCII representation of a certificate, including its public key, but not its private key. An .arm file format is generated and used by the IBM Key Management utility.

.der format

A .der file contains binary data. A .der file can only be used for a single certificate, unlike a .pem file, which can contain multiple certificates.

.pfx format (PKCS12)

A PKCS12 file is a portable file that contains a certificate and a corresponding private key. This format is useful for converting from one type of SSL implementation to a different implementation.

Verifying that the adapter is working correctly

You must take several steps after you install and configure the adapter.

Procedure

1. Install the CA certificate if you have not installed it during plug-in installation.

   For information about CA certificates installation after Password Synchronization plug-in installation, see “Installing CA certificates” on page 9.
2. Restart the domain controller.

   Note: After you restart the domain controller, ensure that the `PwdSync.log` file is created in the log directory.

Chapter 5. Uninstalling

You must complete several steps to remove the Password synchronization plug-in.

Before you begin

Inform users that the resource will be unavailable prior to removing the client. If the server is taken offline, Password Synchronization plug-in requests that are not completed may not be recovered when the server is back online.

About this task

Complete the following procedure to remove the Password Synchronization plug-in and directories.

Procedure

1. From the Windows Control Panel, select **Add/Remove Programs** > **Tivoli Windows Password Synch Plugin**.
2. On the Introduction window, click **Uninstall**.
3. On the Uninstall Complete window, click **Done**.
4. Restart the workstation.

What to do next

- To ensure that the Password Synchronization plug-in directories, subdirectories, and files are removed from the system, view the directory tree.
- When you use `regedit.exe` or `regedt32.exe`, ensure that the Windows registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages` does not include the TivoliPwdSync for 32-bit operating systems and TivoliPwdSync64 for 64-bit operating systems.

Index

U

V

W