IBM Security Verify Identity
7.0

IBM i Password Synchronization Plug-in Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The IBM i Password Synchronization Plug-in enables communication between the Identity server and an IBM i Password Synchronization system.

The IBM i Password Synchronization Plug-in is a plug-in that must be installed on the iSeries server. It must be installed before the Identity server can accept password changes from the iSeries Password Change user interface. You must also install a certificate for the client because Identity server relies on certificates to establish secure SSL communication with the IBM i Password Synchronization Plug-in.

This installation and configuration guide provides the basic information that you need to install and configure the IBM i Password Synchronization Plug-in. This section provides an overview of the plug-in and the features of the plug-in.

The IBM i Password Synchronization Plug-in intercepts the iSeries user password changes and communicates with IBM® Security Verify Identity for passwords rules verification and synchronization. If Password Synchronization is enabled in Identity server, it synchronizes the new password with other accounts of the user that are managed by IBM Security Verify Identity.

The IBM i Password Synchronization Plug-in uses the CHGPWD command to detect password changes. The CHGPWD command does not take user name as a parameter. The individual user must log in and use CHGPWD command to change user password.

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.	Plug-in downloads.
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, see**
Install the plugin.	Chapter 3, “Installing,” on page 7.
Verify the installation.	“Verifying the plug-in installation” on page 7.
Configure the adapter.	Chapter 4, “Configuring,” on page 9

Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

Table 3. Requirements to install the plugin

Prerequisite	**Description**

System	• A supported hardware system.
	  – i5/OS V5R4
	  – IBM i Password Synchronization V6R1
	  – IBM i Password Synchronization V7R1
	• A minimum of 16 MB of memory.
	• A minimum of at least 20 MB of free disk space.

Adapter compatibility	IBM Security Verify Identity IBM i Password Synchronization Plug-in 6.0, 7.0

Table 3. Requirements to install the plugin (continued)	
Software	**i5/OS V5R4** • 5722SS1, option 12 (Host Servers) • 5722JC1 (IBM Toolbox for Java™) The following software is required for secure connections: • 5722SS1, option 34 (Digital Certificate Manager) • 5722AC3 - V5R3 only (Crypto Access Provider 128-bit) • 5722DG1 (IBM HTTP Server) The following administrative tool is needed for the directory server: iSeries Navigator - included with iSeries Access EZSetup **IBM i Password Synchronization 7.1** • 5770SS1, option 12 (Host Servers) • 5761JV1 (IBM Developer Kit for Java) The following software packages are required for secure connections: • 5770SS1, option 34 (Digital Certificate Manager) • 5770SSI, option 35, (CCA Cryptographic Service Provider) • 5770DG1 (IBM HTTP Server for i) The following administrative tool is needed for IBM Directory server for i configuration and the Digital Certificate Manager: 5770XH2 - IBM Navigator for i (included in IBM i Access)
Network connectivity	The plug-in must be installed on a system that can communicate with the IBM Security Verify Identity service through the TCP/IP network.
System Administrator authority	The person, who installs the IBM i Password Synchronization Plug-in, must have IBM i QSecurity Officer (QSECOFR) authority.
User permissions	The user whose password is being changed must have access to the *SYSTEM certificate store.
Identity server	Identity server Version 10.0

Related concepts

Software downloads

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

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.

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.

Related concepts

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

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.

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. Required information to install the plug-in

Required information	**Description**
Installation directory	The location where the plug-in is installed. The default directory is `QITIM`.
IBM Security Verify Identity Application server	IP address and SSL port
Target DN for the service	On the 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.

Related concepts

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

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

Chapter 3. Installing

This task provides the necessary steps for installing the IBM i Password Synchronization Plug-in software.

About this task

Password synchronization has a client-side plug-in that is installed on the iSeries server. This plug-in must be installed before the Identity server can accept password changes from the IBM i Password Change user interface.

You must also install a certificate for the client. The Identity server uses certificates to establish secure SSL communication between itself and the plug-in.

Procedure

1. Use the **CRTSAVF** command to create a *SAVF file on the IBM i server.
2. Download the IBM i Password Synchronization Plug-in compressed file from Passport Advantage.
3. Use the FTP utility to copy the file to the IBM i server.
   Use the *SAVF file name that you created.
4. Create the QITIM library of type *PROD (cannot be updated in debug/test mode).
   Type `CRTLIB LIB(QITIM) TYPE(*PROD)` and press **Enter**.
5. Extract the IBM i Password Synchronization Plug-in program objects.
   Type `RSTLIB SAVLIB(QITIM) DEV(*SAVF) SAVF(`*`SaveFileName`*`)`, where *SaveFileName* is the name of the save file in step 1.
6. Add the QITIM library to the user portion of the library list.
   Type `ADDLIBLE QITIM`, and press **Enter**.
7. Display the library list.
   Type `DSPLIBL` and press **Enter**. Verify that the QITIM library is displayed.

What to do next

After you finish the installation, you must configure the plug-in and configure the Identity server. See “Configuring the plug-in” on page 9 and “Configuring the IBM Security Verify Identity server” on page 11.

Verifying the plug-in installation

After you install the plug-in, you must verify that the installation was successful.

If the plug-in is installed correctly, the following components exist in the QITIM library.

- QITIMPWSYN (*PGM)
- QITIMMSG (*MSGF)
- CHGITIMCFG (*CMD)

Chapter 4. Configuring

After you install the plug-in, you must perform several other tasks. The tasks include configuring the plug-in, setting up SSL, and verifying the plug-in works correctly.

Plug-in and server configuration

Before you can use the IBM i Password Synchronization Plug-in, you must configure both the plug-in and the IBM Security Verify Identity server.

Related concepts

Configuration of SSL communication for the plug-in

For secure connection between the adapter and the server, configure the plug-in and the server to use the Secure Sockets Layer (SSL) authentication with the GSKit communication protocol. By configuring the plug-in for SSL, the server can verify the identity of the adapter before establishing a secure connection.

Configuring the plug-in

Use this procedure to configure and verify the configuration of the IBM i Password Synchronization Plug-in.

Procedure

1. Set the system value `QRETSVRSEC = 1`.

   This system value is used to determine whether to store the encrypted data from the IBM Security Verify Identity server in the Validation List Entry. When set to 1, the encrypted data is stored when the Validation List Entry is added to or changed by either of these APIs:

   - QsyAddValidationLstEntry()
   - QsyChangeValidationLstEntry()

2. Set the system value `QPWDVLDPGM = *REGFAC`.

   This system value provides the ability for a user-written program (QITIMPWSYN in this case) to do additional validation on passwords. If the value of QPWDVLDPGM is set to any other value, the validate password exit programs are not called.

3. Make QITIMPWSYN an exit program for password validation.

   a) Run the **ADDEXITPGM** command to add the QITIMPWSYN program to the IBM i registration facility.

   b) Specify the following values:

   - `Exit Point = QIBM_QSY_VLD_PASSWRD`
   - `Exit Point Format = VLDP0100`
   - `Exit Program = QITIMPWSYN in Lib QITIM`

   c) Verify that the QITIMPWSYN program is registered.

   Run the **WRKREGINF EXITPNT(QIBM_QSY_VLD_PASSWRD)** command.

4. Run the **QITIM/CHGITIMCFG** command.

   (Press PF4 for the prompt.) Enter connection details about the IBM Security Verify Identity server that is to accept password changes from the IBM i Password Synchronization Plug-in. Specify the following details:

   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 selected people. This authority is granted when you create the access control information (ACI) for the Principal account. You must grant read and write permissions to all the attributes that are listed.

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

- Search for the account that triggered the password synchronization.
- Search for the owner of that account.
- Search for any accounts that need their passwords synchronized.
- Modify those same accounts, with write access to their password attributes.

You must create an account specifically for these types of requests.

For more information about creating accounts and privileges, see the IBM Security Verify Identity product documentation.

PASSWORD
Specify the password for the IBM Security Verify Identity server login ID.

HOSTNAME
Specify the IP address of the IBM Security Verify Identity server.

TARGETDN
Specify the DN of the IBM Security Verify Identity service that receives the password change synchronization requests.

PORT
Specify the IBM Security Verify Identity port.

CHKPWDRULE
Specify

- *YES to check whether the password conforms to password rules on IBM Security Verify Identity.
- *NO not to check whether the password conforms to password rules on IBM Security Verify Identity.

LOGGING
Specify

- *YES to enable logging.
- *NO not to enable logging.

ITIM Response
Specify

- *YES if the response from IBM Security Verify Identity is needed during password change.
- *NO if the response from IBM Security Verify Identity is not needed during password change.

5. Set permissions on the validation list (VLDL).

   After configuring RPS with the **CHGITIMCFG** command, a **QITIMCFG (*VLDL)** object is created in QITIM library. You must manually grant *PUBLIC *USE, *ADD, and *UPD authority to the validation list. If the permissions are not set correctly on the VLDL, the password synchronization plug-in cannot access the VLDL. Symptoms of incorrect permissions are:

   - RPS cannot access the VLDL.
   - The VLDL can be accessed, but the encrypted password cannot be retrieved and decrypted.

6. Verify that the configuration was successful.

   Ensure that:

   a) QITIMCFG (*VLDL) is available in the QITIM library.

   b) A log file is created in:

   `/qibm/userdata/tivoli/qpwdsync.log`

Related tasks
Configuring the IBM Security Verify Identity server

In addition to the IBM i Password Synchronization Plug-in, you must also configure IBM Security Verify Identity to use password synchronization.

Configuring the IBM Security Verify Identity server

In addition to the IBM i Password Synchronization Plug-in, you must also configure IBM Security Verify Identity to use password synchronization.

About this task

On the IBM Security Verify Identity, complete the following steps to enable the Password Synchronization option:

Procedure

1. On the IBM Security Verify Identity main menu, select **Set System Security**.
2. Select **Set Security Properties**.
3. Select the **Enable password synchronization** check box.
4. Click **OK**.

Related tasks

Configuring the plug-in
Use this procedure to configure and verify the configuration of the IBM i Password Synchronization Plug-in.

Configuration of SSL communication for the plug-in

For secure connection between the adapter and the server, configure the plug-in and the server to use the Secure Sockets Layer (SSL) authentication with the GSKit communication protocol. By configuring the plug-in for SSL, the server can verify the identity of the adapter before establishing a secure connection.

The plug-in notifies the IBM Security Verify Identity server of changes made to user passwords on the managed resource. You can configure SSL authentication for Web connections that originate from the plug-in to the Web server that is used by the IBM Security Verify Identity server.

In a production environment, you must enable SSL security. For testing purposes you might want to disable SSL. However, you must enable SSL on the plug-in to verify the certificate that the application presents, if these conditions exist:

- An external application communicates with the adapter (for example, the IBM Security Verify Identity server).
- The application uses server authentication.

Related concepts

Plug-in and server configuration
Before you can use the IBM i Password Synchronization Plug-in, you must configure both the plug-in and the IBM Security Verify Identity server.

Overview of SSL and digital certificates

In an enterprise network deployment, you must provide secure communication between the Identity server and the software products and components with which the server communicates.

SSL protocol uses signed digital certificates from a certificate authority (CA) for authentication. SSL secures communication in a configuration. SSL provides encryption of the data that is exchanged between the applications. Encryption makes data that is transmitted over the network intelligible only to the intended recipient.

Signed digital certificates enable two applications that connect in a network to authenticate their identity. An application that acts as an SSL server presents its credentials to verify to an SSL client. The SSL client

then verifies that the application is the entity it claims to be. You can configure an application that acts as an SSL server so that it requires the application that acts as an SSL client to present its credentials in a certificate. In this way, the two-way exchange of certificates is completed. A third-party certificate authority issues signed certificates for a fee. Some utilities, such as those provided by OpenSSL, can also provide signed certificates.

You must install a certificate authority certificate (CA certificate) to verify the origin of a signed digital certificate. When an application receives a signed certificate from another application, it uses a CA certificate to verify the certificate originator. A certificate authority can be:

- Well-known and widely used by other organizations.
- Local to a specific region or a company.

Many applications, such as web browsers, use the CA certificates of well-known certificate authorities. Using a well-known CA eliminates or reduces the task of distributing CA certificates throughout the security zones in a network.

Related concepts

CA certificates installation
The self-signed CA certificate from IBM Security Verify Identity must be installed on each of the target iSeries servers.

Related tasks

Configuring certificates when the plug-in operates as an SSL server and an SSL client
In this configuration, the plug-in operates as an SSL server and an SSL client.

Private keys, public keys, and digital certificates

Keys, digital certificates, and trusted certificate authorities 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. The data encrypted with the public key can be decrypted only with corresponding private key. Similarly, the data encrypted with the private key can be decrypted only by using the corresponding public key. The private key is password-protected in a key database file. Only the owner can access the private key to decrypt messages that are encrypted with the corresponding public key.

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

Organizational information
This certificate section 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 with a certificate management utility.

Public key
The receiver of the certificate uses the public key to decipher encrypted text that is 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. The corresponding CA certificate compares the signature to verify that the certificate is originated from a trusted certificate authority.

Web browsers, servers, and other SSL-enabled applications 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 for the following reasons:

- The digital certificate expired.
- The CA certificate that is used to verify that it is expired.
- The distinguished name in the digital certificate of the server does not match with 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 provided by a certificate authority.

A self-signed certificate contains a public key, information about the certificate owner, and the owner signature. It has an associated private key; however, it does not verify the origin of the certificate through a third-party certificate authority. After you generate a self-signed certificate on an SSL server application, you must:

1. Extract it.
2. Add it to the certificate registry of the SSL client application.

This procedure is equivalent to 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.
- Generate a private key.
- Extract a self-signed certificate.
- Add a self-signed certificate.

Usage of self-signed certificates depends on your security requirements. To obtain the highest level of authentication between critical software components, do not use self-signed certificates or use them selectively. You can authenticate applications that protect server data with signed digital certificates. You can use self-signed certificates to authenticate web browsers or adapters.

If you are using self-signed certificates, you can substitute a self-signed certificate for a certificate and CA certificate pair.

Certificate and key formats

Certificates and keys are stored in the files with various 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, not a private key. The `.arm` file format is generated and used by the IBM Key Management utility.

.der format

A `.der` file contains binary data. You can use a`.der` file 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. Use this format to convert from one type of SSL implementation to another. For example, you can create and export a PKCS12 file with the IBM Key Management utility. You can then import the file to another workstation with the certTool utility.

Configuring certificates when the plug-in operates as an SSL server and an SSL client

In this configuration, the plug-in operates as an SSL server and an SSL client.

About this task

The plug-in initiates the connection and the webserver responds by presenting its certificate to the plug-in.

Figure 1 on page 14 describes how the plug-in operates as an SSL server and an SSL client. When communicating with the IBM Security Verify Identity server, the adapter sends its certificate for authentication. When communicating with the web server, the adapter receives the certificate of the web server.

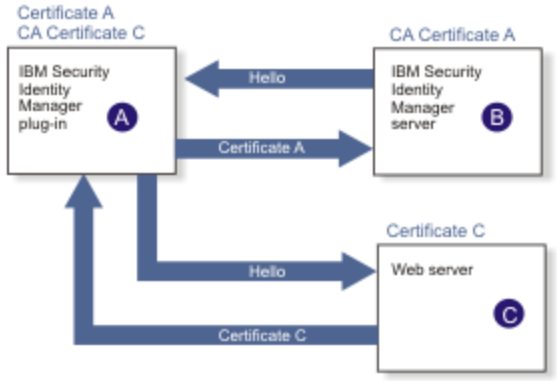

Figure 1. Plug-in operating as an SSL server and an SSL client

If the webserver is configured for two-way SSL authentication, it verifies the identity of the plug-in, which sends its signed certificate to the webserver. (Not shown in the illustration.) To enable two-way SSL authentication between the plug-in and webserver, use the following procedure:

Procedure

1. Configure the webserver to use client authentication.
2. Follow the procedure for creating and installing a signed certificate on the webserver.
3. Install the CA certificate on the adapter with a certification installation tool.
4. Add the CA certificate corresponding to the signed certificate of the adapter to the webserver.

What to do next

For more information about configuring certificates to send an event notification, when the plug-in initiates a connection to the webserver, see the IBM Security Verify Identity product documentation.

Note: The webserver is the one used by the IBM Security Verify Identity server.

Related concepts

Overview of SSL and digital certificates
In an enterprise network deployment, you must provide secure communication between the Identity server and the software products and components with which the server communicates.

CA certificates installation

The self-signed CA certificate from IBM Security Verify Identity must be installed on each of the target iSeries servers.

CA certificates installation

The self-signed CA certificate from IBM Security Verify Identity must be installed on each of the target iSeries servers.

To install the self-signed CA certificate you must:

- Extract the certificate from the IBM Security Verify Identity server.
- Transfer the file to the iSeries servers.
- Install the file on the iSeries servers

Related concepts

Overview of SSL and digital certificates

In an enterprise network deployment, you must provide secure communication between the Identity server and the software products and components with which the server communicates.

Related tasks

Configuring certificates when the plug-in operates as an SSL server and an SSL client

In this configuration, the plug-in operates as an SSL server and an SSL client.

Extracting and transferring the self-signed CA certificate from the Identity server

Perform this procedure to extract and transfer the CA certificate used by IBM Security Verify Identity for authentication with the iSeries server:

Procedure

1. Use a Web browser, for example Internet Explorer, to connect to IBM Security Verify Identity.

   Use the SSL protocol `https://`*`hostname:9443`*`/itim/console`.

   A dialog box is displayed requesting that you accept an untrusted certificate. Accept the certificate.

   Note: This dialog box is not displayed if the SSL certificate is signed by a well-known CA. In this situation, you must use a certificate tool such as ikeyman to extract the certificate.
2. Click **View Certificate**.
3. On the Details tab, click **Copy to File**.
4. Click **Next**.
5. Select to use DER encoded, type a file name in the field and click **Finish**.
6. Use the FTP utility to transfer the file to each of the iSeries servers.
   a) Type `ftp` *`targetmachinename`* and press **Enter**.
   b) Type your user name press **Enter**.
   c) Type the password associated with your user name and press **Enter**.
   d) Type `bin` and press **Enter**.
   e) Type `cd/tmp` and press **Enter**.
   f) Type `put` *`filename`* and press **Enter**.
   Filename is the certificate file that you extracted and copied in the previous steps.
   g) Type `quit` and press **Enter**.

Related tasks

Installing the CA certificate on an iSeries system

After transferring the certificate from IBM Security Verify Identity, you must install it on each of the target iSeries servers.

Verifying the plug-in
After you install and configure the plug-in, perform these tasks:

Installing the CA certificate on an iSeries system

After transferring the certificate from IBM Security Verify Identity, you must install it on each of the target iSeries servers.

About this task

Perform these steps to install the CA certificate:

Procedure

1. Open the web browser to `http://iSerieshostname:2001`.
   iSerieshostname is the host name of the iSeries server.
2. Enter your iSeries server user name and password, and click **OK**.
3. On the iSeries Tasks window, select *Digital Certificate Manager*.
4. On the Digital Certificate Manager window, select **Create a Certificate Authority (CA)**.
5. Type the information in the required fields.

   Note: The Certificate Authority (CA) name describes the name of the iSeries system.
6. Click **Continue**.
7. On the **Install Local CA Certificate** pane, click **Continue.**
   The local certificate does not need to be installed.
8. On the **Certificate Authority (CA) Policy Data** pane, accept the default settings and click **Continue**.
   On the Policy Data Accepted pane, a message `The policy data for the Certificate Authority (CA) was accepted.` is displayed.
9. Click **Continue** to create the default server certificate store, `*SYSTEM`, and a server certificate signed by your CA.
   If `*SYSTEM` exists, the certificate store is not created.
10. On the next Digital Certificate Manager window, type in the information for the required fields.

    Note: Specify a different name in the Certificate label field for the certificate store database, `*SYSTEM`. The fields in the Subject Alternative Name section can be left blank.
11. Click **Continue**.
    On the next Digital Certificate Manager window, a list of applications and certificates is displayed.
12. Click **Select All** then click **Continue**.
    On the Application Status pane, a message `The applications you selected will use this certificate.` is displayed.
13. Click **Cancel**.
    The creation of a signing certificate is optional.
14. On the Select a Certificate Store pane, select ***SYSTEM** and click **Continue**.
15. On the Certificate Store and Password pane, type the password for the *SYSTEM Certificate Store database and click **Continue**.
16. If not already extracted, extract the CA certificate from the IBM Security Verify Identity system and copy the file to the iSeries system.
    See “Extracting and transferring the self-signed CA certificate from the Identity server” on page 15.
17. On the next Digital Certificate Manager window in the Fast Path menu, click **Work with CA Certificates**.
    A list of certificates is displayed.

18. Click **Import**.
19. On the Import **Certificate Authority (CA) Certificate** pane, specify the path and the file name on the iSeries system of the certificate that you extracted from IBM Security Verify Identity. Specify the path in the **Import file:** field.

    For example, type: `/qibm/userdata/`*`psdserver.der`*. The value of *psdserver.der* is the name of the certificate you extracted from the IBM Security Verify Identity system.
20. Click **Continue**.
21. On the **Import Certificate Authority (CA) Certificate** pane, type a label name in the **CA certificate label:** field.

    For example: IBM Security Verify Identity, and click **Continue**.
22. In the **Fast Path** menu, select **Work with Client applications** and click **Continue**.
23. On the Applications registered to use certificates: pane, click **Add Application**.
24. On the next Digital Certificate Manager window in the **Application: ID** field, type `TIVOLI_PWD_SYNCH`.
    a) Select **Application description:** and type a description.

       For example, `Password Sync Exit Handler`.
    b) Click Add.

    On the Work with Client Applications pane, a message `The application has been added.` is displayed.
25. Select *Password Synch Exit Handler* (the description you gave the application) and click **Work with application**.
26. On the next Digital Certificate Manager window, click **Update Certificate Assignment**.
27. On the next Digital Certificate Manager window, select the certificate you created from the list and click **Assign New Certificate**.

    In the Update Certificate Assignment pane, the message `The certificate was assigned to the application.` is displayed.
28. In the **Fast Path** pane, click **Work with CA certificates**. Verify that IBM Security Verify Identity server is listed as enabled in the **Certificate Authority (CA)** list.

Related tasks

Extracting and transferring the self-signed CA certificate from the Identity server
Perform this procedure to extract and transfer the CA certificate used by IBM Security Verify Identity for authentication with the iSeries server:

Verifying the plug-in
After you install and configure the plug-in, perform these tasks:

Verifying the plug-in

After you install and configure the plug-in, perform these tasks:

Procedure

1. Use the **chgpwd** command to change the password for a user.
2. Verify that the plug-in was called by checking the log file:

   `/qibm/userdata/tivoli/qpwdsync.log`
3. Verify that the password synchronization was successful by checking the IBM Security Verify Identity logs.

Related tasks

Extracting and transferring the self-signed CA certificate from the Identity server
Perform this procedure to extract and transfer the CA certificate used by IBM Security Verify Identity for authentication with the iSeries server:

Installing the CA certificate on an iSeries system

After transferring the certificate from IBM Security Verify Identity, you must install it on each of the target iSeries servers.

Chapter 5. Uninstalling

You can take a series of steps to uninstall the plug-in.

Procedure

1. Set the system value `QPWDVLDPGM = *NONE`.
   When the value of QPWDVLDPGM is set to *NONE, the validate password exit program is not called.
2. Remove the installed QITIMPWSYN password validation exit program:
   a) Run the **`WRKREGINF`** command to display a list of exit points.
   b) Go to the QIBM_QSY_VLD_PASSWRD exit point and enter option 8 - **work with exit programs**.
   QITIMPWSYN program name is displayed.
   c) Enter option 4 - **remove exit program**.
3. After you finish removing exit points, stop and restart the FTP server.
4. Delete the PROD library QITIM and the objects it contains.

Index