# Contents

**Figures** .............................................. v

**Tables** ............................................. vii

**Preface** ........................................... ix
About this publication ................................ ix
Access to publications and terminology ............ ix
Accessibility ............................................. x
Technical training ....................................... x
Support information ..................................... x
Statement of Good Security Practices ................. x

**Chapter 1. Overview of the plug-in** ............ 1
Features of the plug-in .................................. 1
Interaction among Active Directory, IBM Security
Identity Manager, and the plug-in ...................... 1
Preventing recursion .................................... 2

**Chapter 2. Plug-in installation planning** ...... 3
Preinstallation roadmap .................................. 3
Installation roadmap ..................................... 3
Prerequisites ............................................. 3
Information worksheet .................................. 4
Software download ....................................... 4

**Chapter 3. Installing the Password**
**Synchronization plug-in** ......................... 5
Installing CA certificates ............................... 9
Verifying the installation ............................... 9

**Chapter 4. Plug-in installation and**
**uninstallation by using silent mode** ............ 11
Installing the plug-in by using silent mode .......... 11
Uninstalling the plug-in by using silent mode ...... 13

**Chapter 5. SSL authentication**
**configuration for the plug-in** .................... 15
Overview of SSL and digital certificates .......... 15
Private keys, public keys, and digital certificates 16
Self-signed certificates ................................ 16
Certificate and key formats ........................... 17
Certificate configuration when the plug-in operates as an SSL client .. 17

**Chapter 6. Taking the first steps after**
**installation** ........................................ 19

**Chapter 7. Uninstalling the plug-in** .......... 21

**Appendix A. Support information** .............. 23
Searching knowledge bases ........................... 23
Obtaining a product fix ............................... 24
Contacting IBM Support ............................... 24

**Appendix B. Accessibility features for**
**IBM Security Identity Manager** ................. 27

**Notices** ............................................ 29

**Index** ............................................... 33

© Copyright IBM Corp. 2012, 2014
Figures

1. Plug-in operating as an SSL server and an SSL client. .......................... 18
Tables

1. Preinstallation road map ..................... 3
2. Installation road map ....................... 3
3. Prerequisites to install the plug-in ........ 3
4. Information worksheet ....................... 4
5. Operating system and file ................... 10
6. Installation options ......................... 12
Preface

About this publication

The Password Synchronization for Active Directory Plug-in Installation and Configuration Guide provides information about how to install and configure the Password Synchronization plug-in for Active Directory.

The IBM® Security Identity Manager provides the plug-in to process password change requests between an Active Directory domain controller and the IBM Security Identity Manager server.

Note: The program that is used to connect the managed resource to the IBM Security Identity Manager server is now called an adapter. The term adapter replaces the previously used term agent. The user interface that is used to configure the adapter still uses the term agent.

Access to publications and terminology

This section provides:

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

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation, see the online library http://www-01.ibm.com/support/knowledgecenter/SSRMWJ/welcome.

Online publications

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

IBM Security Identity Manager library

The product documentation site http://www-01.ibm.com/support/knowledgecenter/SSRMWJ/welcome displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central

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

IBM Publications Center

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


---

**Accessibility**

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

---

**Technical training**

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

---

**Support information**

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

Appendix A, “Support information,” on page 23 provides details about:

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

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

---

**Statement of Good Security Practices**

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.
Chapter 1. Overview of the plug-in

The IBM Security Identity Manager Password Synchronization plug-in enables connectivity between the IBM Security Identity Manager 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.

This chapter provides an overview of the plug-in and the features of the plug-in.

Features of the plug-in

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

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

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

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

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 Identity Manager 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 Identity Manager for rules verification. If the password matches the rules defined in IBM Security Identity Manager, then IBM Security Identity Manager 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 Identity Manager for the password change operation. Upon receipt of success, IBM Security Identity Manager 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 Identity Manager. See "Preventing recursion"

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 Identity Manager server from processing its own password change requests to the adapter as password synchronization requests.

Procedure

1. On the IBM Security Identity Manager, go to the ISIM_HOME/data directory.
2. Open the enRole.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. Plug-in installation planning

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

Preinstallation roadmap

You must prepare the environment before you can install the plug-in.

Table 1. Preinstallation road map

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain the installation software</td>
<td>Download the software from Passport Advantage®. See “Software download” on page 4.</td>
</tr>
<tr>
<td>Verify that the software and hardware requirements for the adapter that you want to install have been met.</td>
<td>See “Prerequisites.”</td>
</tr>
<tr>
<td>Collect the necessary information for the installation and configuration.</td>
<td>See “Information worksheet” on page 4.</td>
</tr>
</tbody>
</table>

Installation roadmap

You must complete the necessary steps to install the plug-in. The steps include completing post-installation configuration tasks and verifying the installation.

Table 2. Installation road map

<table>
<thead>
<tr>
<th>Task</th>
<th>For more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify the installation.</td>
<td>See “Verifying the installation” on page 9.</td>
</tr>
</tbody>
</table>

Prerequisites

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

Table 3 identifies installation prerequisites for this plug-in.

Table 3. Prerequisites to install the plug-in

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>A Windows 2008 Server running Active Directory. Both 32-bit or 64-bit versions are supported</td>
</tr>
<tr>
<td>Note: The Password Synchronization plug-in supports only x86 architecture, however, the Password Synchronization plug-in does not have Itanium support.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3. Prerequisites to install the plug-in (continued)

<table>
<thead>
<tr>
<th>Prerequisite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator Authority</td>
<td>The person who completes the Password Synchronization plug-in installation procedure must have system administrator authority to complete the steps in this chapter.</td>
</tr>
<tr>
<td>IBM Security Identity Manager server</td>
<td>Version 6.0</td>
</tr>
</tbody>
</table>

Information worksheet

Use the information in the following table to complete the installation of the plug-in. Gather this information before you start the installation process.

Table 4. Information worksheet

<table>
<thead>
<tr>
<th>Required information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation directory</td>
<td>The location where the plug-in is installed. The default is C:\Program Files\IBM\ISIM\Agents\PasswordSynch</td>
</tr>
<tr>
<td>IBM Security Identity Manager server</td>
<td>IP address and SSL port</td>
</tr>
<tr>
<td>Target DN for the service</td>
<td>On the IBM Security Identity Manager server</td>
</tr>
<tr>
<td>IBM Security Identity Manager account</td>
<td>The account under which the requests are submitted.</td>
</tr>
<tr>
<td>IBM Security Identity Manager account password</td>
<td>The password for the IBM Security Identity Manager account under which the requests are submitted.</td>
</tr>
</tbody>
</table>

Software download

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

Go to [IBM Passport Advantage](#)

See the [IBM Security Identity Manager Download Document](#) for instructions.

Note:

You can also obtain additional adapter information from IBM Support.
Chapter 3. Installing the Password Synchronization plug-in

You must install the plug-in on the Windows Directory Domain Controller.

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 4.
- 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: 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. In the PFConfig window, complete all of the text fields in the window. The following information describes the 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.
ISIM Host Name or IP
Specifies the IP address for the IBM Security Identity Manager server.

SSL Port Number
Specifies the SSL port for the IBM Security Identity Manager 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.

Service DN
Specifies the Target DN of the service that is being monitored. 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 Identity Manager 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=namelservice,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 Identity Manager server.
Specifies the name of the organization on the IBM Security Identity Manager server

Specifies the short name defined for the organization during installation and configuration of the IBM Security Identity Manager 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 Identity Manager installation.

dc=com

 Specifies the root of the directory tree.

For example, if you installed the IBM Security Identity Manager 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 Identity Manager 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

ISIM Principal

Specifies the IBM Security Identity Manager 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 Identity Manager Information Center for more information about creating accounts and privileges.

Password

Specifies the password for the IBM Security Identity Manager account under which the password change requests are submitted.
Verify Password
Specifies the verification field for the IBM Security Identity Manager 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 Identity Manager 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 defined for each account type to be synchronized. 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 Identity Manager Information Center for more information about setting IBM Security Identity Manager password policies.

Require ISIM 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 Identity Manager when it is unavailable.

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

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 Identity Manager 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."

Installing CA certificates

To install the CA certificates after you install the Password Synchronization plug-in, you must take several steps.

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 Identity Manager 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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>32-bit operating system</td>
<td>TivoliPwdSync.dll</td>
</tr>
<tr>
<td>64-bit operating system</td>
<td>TivoliPwdSync64.dll</td>
</tr>
</tbody>
</table>

- 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:\Tivoli\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.
Chapter 4. Plug-in installation and uninstallation by using 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 uninstalled 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 SetupPwdSync.exe.
  2. Run the following command from command prompt:

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

     The adapter is installed in the adapter installation directory, `C:\Program Files\IBM\ISIM\Agents\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

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

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 5. SSL authentication configuration for the plug-in

You can establish a secure connection between an IBM Security Identity Manager plug-in and the IBM Security Identity Manager server. You must configure the plug-in and the server to use the Secure Sockets Layer (SSL) authentication.

By configuring the plug-in for SSL, you ensure that the IBM Security Identity Manager server verifies the identity of the plug-in before a secure connection is established.

The Password Synchronization plug-in uses http with SSL to establish secure communications.

Note: In a production environment, you need to enable SSL security. For testing purposes you might want to disable SSL. However, if an external application that communicates with the plug-in (such as IBM Security Identity Manager server) is set to use server authentication, you must enable SSL on the plug-in to verify the certificate that the application presents.

You can configure SSL authentication for connections that originate from the IBM Security Identity Manager server or from the plug-in. Typically, the IBM Security Identity Manager server initiates a connection to the plug-in in order to set or retrieve the value of a managed attribute on the plug-in. However, depending on the security requirements of your environment, you might need to configure SSL authentication for connections that originate from the plug-in. For example, if the plug-in uses events to notify the IBM Security Identity Manager server of changes to attributes on the plug-in, 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 Identity Manager server.

Overview of SSL and digital certificates

You can deploy IBM Security Identity Manager into an enterprise network. You must secure communication between the IBM Security Identity Manager 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 an IBM Security Identity Manager 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 Identity Manager 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.

**Certificate configuration when the plug-in operates as an SSL client**

In this configuration, the plug-in operates as an SSL client. For example, the plug-in initiates the connection and the web server responds by presenting its certificate to the plug-in.
Figure 1 illustrates how an IBM Security Identity Manager plug-in operates as an SSL server and an SSL client. When communicating with the IBM Security Identity Manager server, the plug-in sends its certificate for authentication. When communicating with the Web server, the plug-in receives the certificate of the Web server.

If the Web Server is configured for two-way SSL authentication, it verifies the identity of the plug-in, which sends its signed certificate to the Web server (not shown in the illustration). In order to enable two-way SSL authentication between the plug-in and Web server, use the following procedure:

1. Configure the Web server to use client authentication.
2. Follow the procedure for creating and installing a signed certificate on the Web server.
3. Install the CA certificate on the plug-in.
4. Add the CA certificate corresponding to the signed certificate of the plug-in to the Web server.

For more information on configuring certificates when the plug-in initiates a connection to the Web server (used by the IBM Security Identity Manager server) to send a notification, see the IBM Security Identity Manager product documentation.
Chapter 6. Taking the first steps after installation

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 7. Uninstalling the plug-in

Use these procedures to uninstall 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.
Appendix A. Support information

You have several options to obtain support for IBM products.

- "Searching knowledge bases"
- "Obtaining a product fix" on page 24
- "Contacting IBM Support" on page 24

Searching knowledge bases

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

About this task

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

Procedure

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

1. Search for content by using the IBM Support Assistant (ISA).
   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the [ISA website](https://www.ibm.com/support/isa).

2. Find the content that you need by using the IBM Support Portal.
   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the [demo videos](https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports)
   - IBM Security Identity Manager Support website
   - IBM Redbooks®
   - IBM support communities (forums and newsgroups)

4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.

5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to
include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

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

---

**Obtaining a product fix**

A product fix might be available to resolve your problem.

**About this task**

You can get fixes by following these steps:

**Procedure**

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

---

**Contacting IBM Support**

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

**Before you begin**

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the [Support portfolio](http://www.ibm.com/software/support/isa/) topic in the “Software Support Handbook”.

**Procedure**

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the [Getting IBM support](http://www.ibm.com/software/support/isa/) topic in the Software Support Handbook.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     - Any data that has been collected can be attached to the service request.
     - Using ISA in this way can expedite the analysis and reduce the time to resolution.
     - b. Open ISA.
c. Click Collection and Send Data.
d. Click the Service Requests tab.
e. Click Open a New Service Request.

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

Results

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

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

Accessibility features

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

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

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

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

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

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

IBM and accessibility

See the [IBM Human Ability and Accessibility Center](https://www.ibm.com/able) for more information about the commitment that IBM has to accessibility.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

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

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

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

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

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

**Trademarks**

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

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

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

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

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

Index

A
accessibility x, 27
adapter
recursion, preventing 2
silent installation 11

C
CA certificate
authentication 15
installation 9, 19
secure communication 15
certificates
definition 15
key formats 17
overview 15
private keys and digital
certificates 16
self-signed 17
client validation, SSL 18

D
domain controller restart 19
download
online location 4
software 4

E
education x
encryption, SSL 15, 16

I
IBM
Software Support x
Support Assistant x
IBM Support Assistant 24
import, PKCS12 file 17
installation
CA certificate 9
domain controller 5
first steps following
CA certificate installation 19
domain controller restart 19
PwdSync.log file 19
plug-in 5
prerequisites
authority requirements 3
system requirements 3
roadmap 3
silent 11
verifying 9
worksheet 4
ISA 24

K
knowledge bases 23

N
notices 29

O
online
publications ix
terminology ix
overview
connectivity between servers 1
plug-in 1

P
passwords
change requests 1
client initiation 1
domain user changes 1
recursion prevention 1, 2
rules verification, synchronization 1
plug-in
change request processing ix
features
domain user password changes 1
password rules verification,
synchronization 1
installation
overview 1
planning 3
roadmaps 3
steps 5
overview ix, 1
silent
installation 11
uninstallation 13
uninstallation 21
preinstallation
requirements 3
roadmap 3
software download 3
prerequisites
authority requirements 3
system requirements 3
preventing recursion 2
private key, definition 15
problem-determination x
protocol, SSL
overview 15
two-way configuration 18
public key 16
publications
accessing online ix
list of ix
PwdSync.log file 19

R
recursion of passwords, preventing 2
roadmaps
installation 3
preinstallation 3
sequence of steps 3

S
Security Identity Manager Adapter
communication with the server 18
SSL communication 18
self-signed certificate 17
silent
installation
adapter 11
plug-in 11
uninstallation, plug-in 13
software
download 4
online location 4
SSL
certificate installation 15
encryption 15
key formats 17
overview 15
private keys and digital
certificates 16
self-signed certificates 17
two-way configuration 18
support contact information 24

T
terminology ix
training x
troubleshooting
contacting support 24
getting fixes 24
searching knowledge bases 23
support website x
two-way configuration
client and server 18
SSL 18

U
uninstallation
plug-in 21
using silent mode 13

V
verifying
installation 9
steps 9