
SIFWorks® ZIS™ HTTPS Administration Guide

Version 3.5

January 2011



PEARSON

Data Solutions
9815 S. Monroe St.,
Ste. 400
Sandy, UT 84070
1.877.790.1261

www.pearsondatasolutions.com

*Copyright © 2011 Pearson Education, Inc. All rights reserved.
This document is provided to Data Solutions customers and partners and may not be reproduced—in part or whole—in any form without the express written permission of NCS Pearson, Inc. Information provided herein is subject to change without notice.
SIFWorks and Data Solutions are registered trademarks of NCS Pearson, Inc.
SIF and Schools Interoperability Framework are registered trademarks of the Schools Interoperability Framework Association.
All other trademarks mentioned herein are the property of their respective owners.*

Contents

1. SIFWorks ZIS HTTPS Administration Overview	4
How It Works	4
2. Certificate Management	6
Server Certificates	7
Agent Certificates	10
Transports	12
Certificate Format Details	14
3. Agent Administration	15
Creating Agent Keys and Certificates	15
Setting the Agent's Key Store	19
Importing the ZIS Certificate into the Agent	20
4. Other Certificate Scenarios	22
Importing Key Pairs from PFX Files	22
5. Index	28

1. SIFWorks ZIS HTTPS Administration Overview

The HTTPS Transports option allows you to configure and create keys and certificates for the ZIS to communicate via a secure connection. With the HTTPS option, you can administer your HTTPS transports, create private keys, or import trusted certificates directly in the SIFWorks® ZIS console. The major changes to the HTTPS Administration of the SIFWorks ZIS are as follows:

- The ZIS no longer uses an external tool for basic management
- Advanced tasks still require external tools such as Portecle and Keytool
- Self-signed certificates can now be created within the ZIS
- Public head certificate files can now be exported directly from the ZIS web console

How It Works

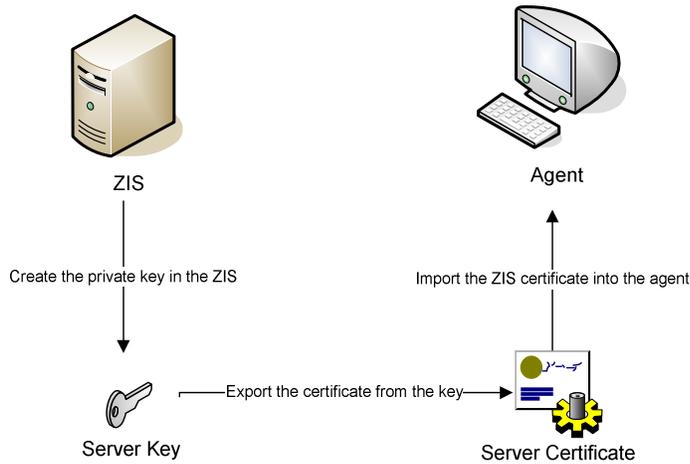
For HTTPS transports to work, both the ZIS and the agent need to have their own private keys and both need to exchange their public certificates. (The only exception to this is if the agent is running in pull mode without Client Authentication. If this is the case, the agent does not need a key and the ZIS does not need a certificate from the agent.) The creation of private keys and the importing/exporting of public certificates can all be done within the ZIS application.

On the agent side, for agents developed by Data Solutions, importing the ZIS's certificate into the agent can be done from the agent itself. However, the creation of the agent's private key and the exporting of the agent's public certificate must be done from a third-party program. For other agents, check the vendor's documentation.

From the ZIS to the Agent

From within the ZIS, you create a private key and export the associated public certificate (see [Server Certificates](#)). After the certificate is exported, you import the certificate into the agent (see [Importing the ZIS Certificate into the Agent](#)). The following diagram illustrates this process:

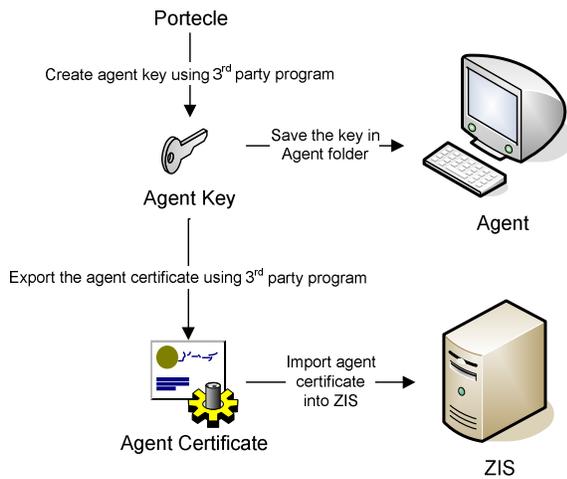
Diagram #1 – From the ZIS to the Agent



From the Agent to the ZIS

With current Data Solutions agents, you cannot create an agent's key nor export the security certificate from the agent itself. There are various tools that allow you to create keys and export certificates; however, Data Solutions recommends using Portecle, a free tool for creating keys and exporting certificates (see [Creating Agent Keys and Certificates](#)). The following diagram illustrates this process:

Diagram #2 – From the Agent to the ZIS



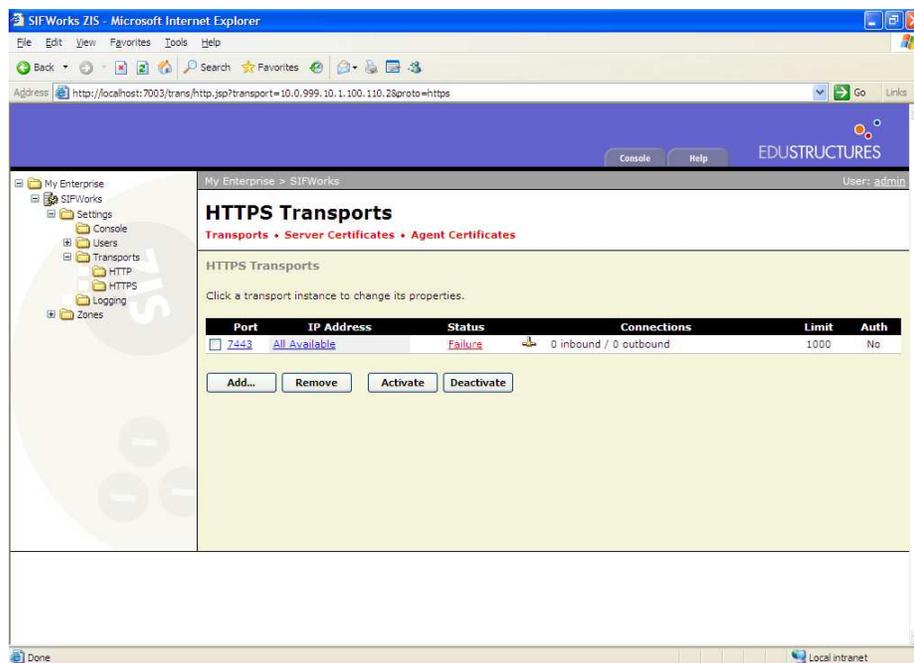
2. Certificate Management

HTTPS keys and certificates for the ZIS can now be configured directly in the ZIS. Previously, you were required to create keys and certificates in a third-party application. All HTTPS management is controlled in the **Settings > Transports > HTTPS** screen.

Note: Certificate changes will not take effect until HTTPS transports are disabled and re-enabled (see [Transports](#) for information on disabling and re-enabling transports).

To access the HTTPS screen:

1. Open the ZIS Console.
2. From the left menu pane, click **My Enterprise > SIFWorks > Settings > Transports > HTTPS**.



There are three options in the ZIS: Transports, Server Certificates, and Agent Certificates. To access any of the three options, click the category links located below the screen's title. For the purpose of this document, Server Certificates and Agent Certificates will be discussed first.

Note: Typically, there is only one transport used for HTTPS. Although transport configuration is discussed later in this document, you should use the default HTTPS transport; you do not need to add additional transports to the ZIS.

Server Certificates

The Server Certificates option allows you to create certificates (each with its accompanying keys), export a certificate with its accompanying keys, and view a certificate's details.

Creating Server Certificates

To create a server certificate:

1. Click the Server Certificates link located below the screen title.
2. Click **Create**.

Create Server Certificate

[Transports](#) • [Server Certificates](#) • [Agent Certificates](#)

Create Private Key and Self-Signed Certificate

In the following form you will enter information to create a private key for SSL, along with a self-signed certificate for that key.

Mandatory Fields

Key Algorithm: *

Alias: *

Validity (Days): *

Suggested Fields

In order to achieve SIF_AuthenticationLevel 3, the Common Name field must be defined as the host name or IP address of the ZIS as agents will recognize it. If, for example, the ZIS resides behind a firewall, in most cases the IP or host name will be that of the firewall and not that of the actual server hosting the ZIS.

Common Name (CN):

Optional Fields

Organizational Unit (OU):

Organization (O):

Locality Name (L):

State Name (ST):

Country Code (C):

E-Mail Address (E):

Create

Cancel

3. Complete the Server Certificate fields as follows:

Server Certificate Options

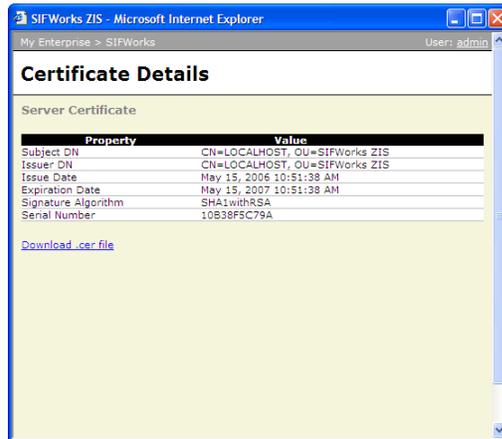
Field	Description
Key Algorithm	Mandatory Field —Select the category of encryption ciphers to support with this certificate. RSA ciphers are generally more secure and more broadly used while DSA is available to support some legacy applications
Alias	Mandatory Field — Enter any Alphanumeric name that describes the server certificate. The Alias can be anything that describes the certificate for you and your users.
Validity (Days)	Mandatory Field — Enter the number of days that the certificate will be valid. The ZIS will automatically calculate the expiration date from this field's entry and the creation date.
Common Name (CN)	Suggested Field — Enter the server hostname or IP for the ZIS zone. This is typically the host name located in the Zone URL.
Organizational Unit (OU)	Optional Fields — Enter the requested information in the appropriate fields. This information is used for identification purposes when users see certificate warnings or as requested by the application or browser.
Organization (O)	
Locality Name (L)	
State Name (ST)	
Country Code (C)	
E-Mail Address (E)	

4. Click **Create**.

Managing Certificates

Once the certificate is created, you can view its details or export the certificate. It is now easier than ever to export certificates for an agent's use.

To view a certificate's details, click that certificate's Alias link.



To export a certificate:

1. Click the icon for the certificate you want to export. The icon is located in the "Certificate" column.
2. Click **Save**.
3. Navigate to the location where you want to save your certificate file, and click **Save**.

Note: To import a Server Certificate into your agent, you must first export the Server Certificate from the ZIS.

Agent Certificates

In the Agent Certificates screen (SIFWorks ZIS > Server Settings > Transports > HTTPS > Agent Certificates), you can import agent certificates that identify trusted agents. Agent certificates are created by third-party tools (see Private Keys and Certificates in the Agent Administration section of this document).

Note: You can now retrieve a previously imported certificate.

Importing Agent Certificates

To import an Agent Certificate:

1. From the SIFWorks ZIS navigation pane, click on Server Settings > Transports > HTTPS > Agent Certificates.
2. The Agent Certificates page is displayed.

Alias	Certificate	Organizational Unit	Common Name	Expiration Date
<input type="checkbox"/> va-slf		null	SANUTWL-CY1SPJ1.PEEROT.COM	Jun 23, 2011 1:52:57 PM

3. Click **Import**.
4. The Add Agent Certificate page is displayed.

Alias: *

Certificate File:

5. Type a name in the Alias field. (The Alias is a unique name that you provide. It serves as an identifier for imported certificate, but does not affect functionality.)

6. Type the path and file name to the certificate you are importing (see *Exporting Agent Certificates using Portecle*) in the Certificate File field, or click **Browse** and navigate to the certificate file.

Note: Certificate files have the “*.cer” extension.

7. Click **Import**.
8. Validate the certificate’s details and click **Confirm**. Click **Cancel** to abort the process of adding an agent certificate.

Managing Agent Certificates

From the Agent Certificates screen (SIFWorks ZIS > Server Settings > Transports > Agent Certificates), you can view an agent certificate’s details, download the certificate, and/or delete an imported certificate from the ZIS.

SIFWorks ZIS

Agent Certificates

Transports > Server Certificates > Agent Certificates

Agent Certificates

Click an alias to view its details or click the icon to download the certificate.

Alias	Certificate	Organizational Unit	Common Name	Expiration Date
<input type="checkbox"/> va-slf	SANUTWL-CY1SPJ1.PEEROT.COM	null	SANUTWL-CY1SPJ1.PEEROT.COM	Jun 23, 2011 1:52:57 PM

To view an agent certificate’s details, click the certificate’s Alias link.

To download the certificate,

1. Click the red ribbon icon in the Certificate column.
2. Click **Save**.
3. Navigate to the location to which you want to save the certificate file.
4. Click **Save**.

To delete an agent certificate from the ZIS, select the certificate’s checkbox, click **Delete**, and confirm the deletion.

Note: When trusted certificate imports are disabled, the **Import** button on the Agent Certificate screen will be disabled.

Transports

The Transports screen allows you to configure the transport for your HTTP protocol. The HTTPS Transports screen is the default screen when you first open the **Settings > Transports > HTTPS** screen. From the HTTPS Transports screen, you can add, remove, activate or deactivate transports.

The screenshot shows the 'HTTPS Transports' management page. At the top, there is a breadcrumb trail: 'Transports > Server Certificates > Agent Certificates'. Below this, the page title is 'HTTPS Transports' with a subtitle 'Click a transport instance to change its properties.' A table lists the current transport instance:

Port	IP Address	Status	Connections	Limit	Auth
<input type="checkbox"/> 7443	All Available	Active	0 inbound / 0 outbound	1000	Yes

Below the table are four buttons: 'Add...', 'Remove', 'Activate', and 'Deactivate'.

To add an HTTPS Transport:

1. Click **Add**.
2. The HTTPS Transports > Add Transport page is displayed.

The screenshot shows the 'Add Transport' configuration form. It includes a checkbox for 'Activate this transport on startup' which is checked. Below this are three input fields: 'Server Port:', 'Server Address:', and 'Limit to: 1000 concurrent connections'. There is also a 'Require Client Authentication:' checkbox which is unchecked. At the bottom of the form are 'Save' and 'Cancel' buttons.

3. Select whether or not you want to activate this transport on startup.
4. Enter the Server Port and Server Address.
5. Enter the number of connections to limit with this transport. The default is 1000.

-
6. Select the **Require Client Authentication** to force client authentication through this transport.
 7. Click **Save**.

Note: Certificate changes will not take effect until HTTPS transports are disabled and re-enabled.

To remove an HTTPS Transport:

1. Select the left checkbox next to Transport(s) you want to remove.
2. Click **Remove**.
3. Click **OK** on the warning screen to remove the selected transport. Click **Cancel** to cancel the deletion.

To edit a transport, click either the Port link or IP Address link of the desired transport. The options are the same as the **Add Screen**.

To activate or deactivate transport(s):

1. Select the left checkbox next to the Transport(s) you want to Activate or Deactivate.
2. Click either **Activate** or **Deactivate**. (On a deactivation, you will be prompted to continue. Click **OK** to continue.)

The status displays "*Inactive*" for deactivated transports. For active transports that do not have a certificate, the status displays as "*Failure*."

Certificate Format Details

The following details are listed for your information:

- a. Exported certificates are X.509 DER encoded files;
- b. Signatures use SHA1withRSA encryption;
- c. Keystores are the standard JKS format;
- d. Private keys are 1024 bit RSA format.

3. Agent Administration

When configuring HTTPS, there are three tasks you need to perform from the agent's perspective: creating an agent key; exporting an agent certificate; and importing the ZIS certificate into the agent.

Private keys and certificates are required for most transfer configurations. (The only time an agent does not require a key and certificate is when that agent is configured to use Pull mode without Client Authentication enabled. All other configurations require a key and certificate.) Most agents have the ability to import server certificates from the ZIS.

Creating Agent Keys and Certificates

In order to create private keys and certificates for a SIF Agent, you need to use a third-party tool. Keytool has the ability to accomplish the required steps in creating private keys and certificates (see the Java documentation for details). However, Data Solutions recommends a third-party tool called Portecle (visit <http://portecle.sf.net/> for download instructions and documentation). The following process is described using Portecle to create agent keys and export agent certificates.

Creating an agent key using Portecle

Before you can create a key in Portecle, you must have a Keystore open.

To open a Keystore:

1. Open Portecle.
2. Click `File > Open Keystore File`.
3. Navigate to the Keystore file you want to open, highlight the file, and click `Open`.
4. Enter the password for the Keystore. The default password is "changeit".

Note: The recommended file name for a Keystore file is "Agent.ks".

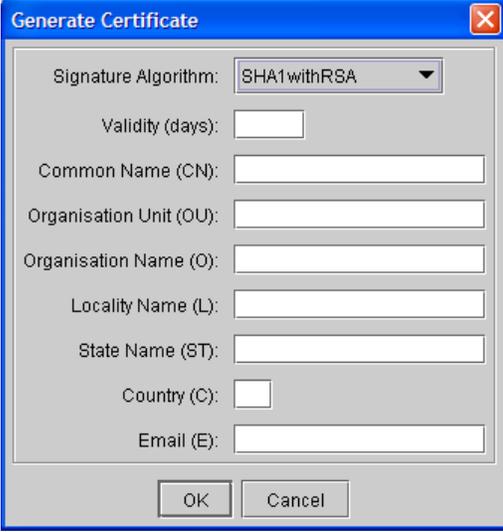
If there is no Keystore file, you must create a new Keystore File. To create a Keystore file:

1. Click `File > New Keystore`.
2. Verify that JKS is selected and click `OK`.

The new Keystore is created. You will need to save the Keystore after you are finished creating the agent key.

To create the agent key:

1. Click **Tools** > **Generate Key Pair**.
2. Select **RSA**, verify that 1024 is the **Key Size**, and click **OK**.



3. Enter the **Validity** of the agent key in days.
4. Enter a **Common Name (CN)**. The **Common Name** should be the same as the IP address of the computer where the agent resides.
5. Enter an **Organizational Unit (OU)** name. This name can be anything you want. However, a descriptive name would be best in that this is how the key name displays when the key is imported into the agent.
6. Complete the other fields as desired and click **OK**.

Note: Only **Validity** is a required field. However, adding a **Common Name** and **Organizational Unit** is **HIGHLY** recommended and will make the importing/exporting process easier.

7. Enter an **Alias** name. The default will be whatever you entered in the **CN** field. However, you can name the agent key whatever you want.
8. Click **OK**.
9. Enter a password for the new key. This needs to be the same password as entered in the **HTTPS** section of the agent. The default password in the agent is "changeit". (This password is case-sensitive.) Data Solutions recommends using the default password, "changeit". If you use a different password and forget or lose it, you will need to create a new key and follow the **HTTPS** configuration process anew.
10. Reenter the password and click **OK**.
11. Click **OK** to complete the task.

Saving the Keystore

After you have added the client key to the Keystore, you need to save the Keystore.

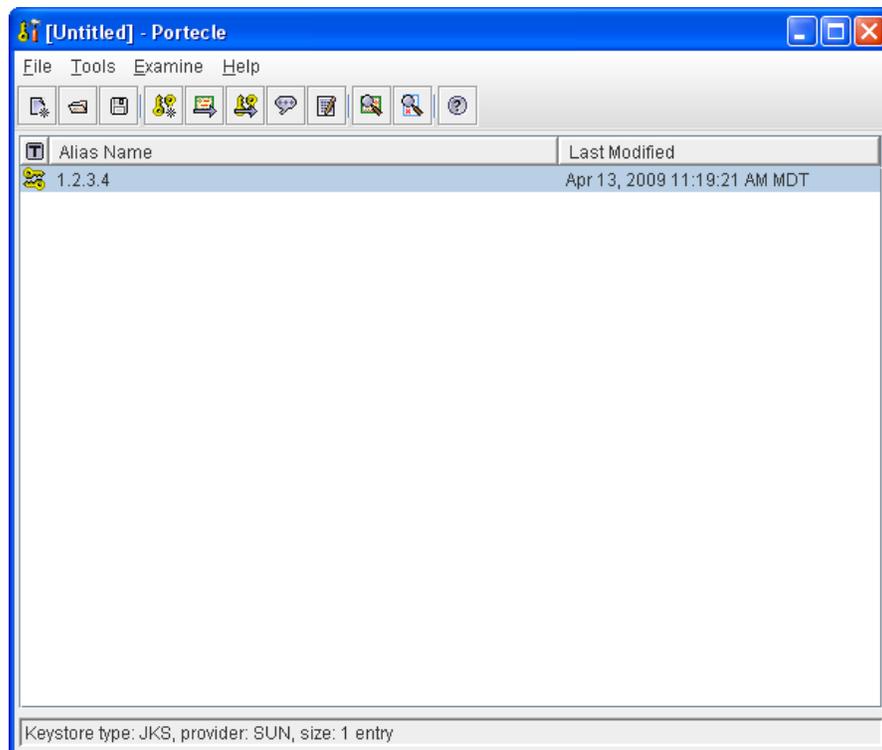
To save the Keystore:

1. Click **File > Save Keystore**.
2. Enter and reenter the password. This password needs to be the same as the password for the key you just created (i.e., “changeit”)
3. Navigate to the folder of the agent for which you are creating the key.
4. Enter “Agent.ks” as the name of the Keystore in the File Name field.
5. Click **Save**. (You will use the key store created in this process, in the subsection [Setting the Agent’s Key Store](#).)

Exporting Agent Certificates using Portecle

After you have created the agent key, you must export the agent certificate. This is the agent certificate that will be imported into the ZIS (see the subsection earlier in this document on [Importing Agent Certificates](#)).

To export the agent certificate:



1. Right-click the key you want to export.
2. Click **Export**.

-
3. Verify that Head Certificate and DER Encoder are selected and click **OK**.
 4. Navigate to the agent's directory. (This is the same directory where you saved the Keystore.)
 5. Enter a certificate name in the File Name field. This can be any name you want. However, naming the key something descriptive (e.g., the name of the agent) will help you later.

Note: When entering the certificate name, you need to enter the **complete certificate name** including the extension. For example, if you want to name the certificate "SLF", you would enter "SLF.cer" into the File Name field.

6. Click **Export**.
7. Click **OK**.

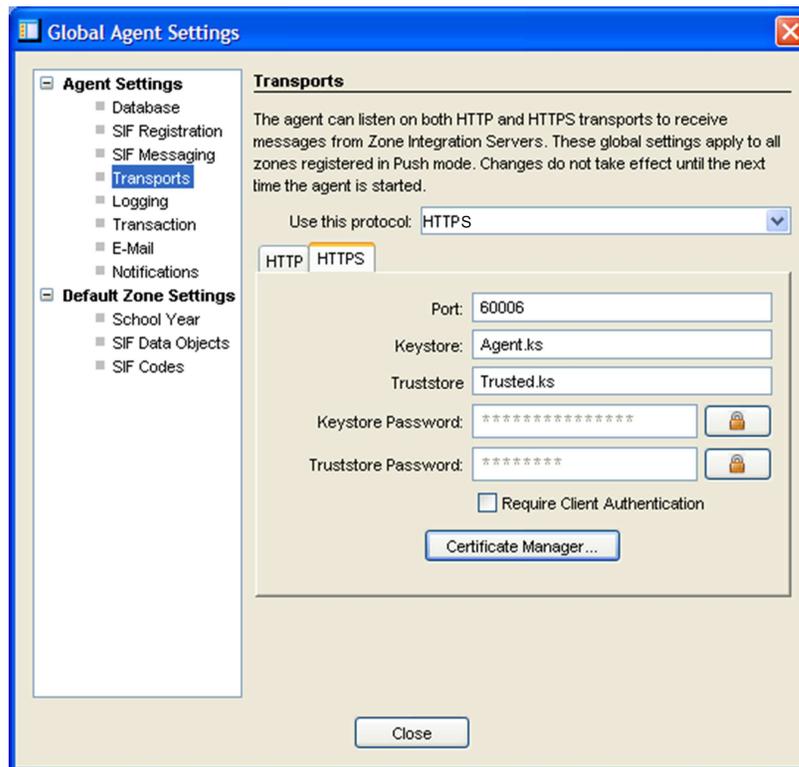
After you have exported the agent's certificate, you can import it into the ZIS (see [Importing Agent Certificates](#)).

Setting the Agent's Key Store

Previously in this document ([Creating Agent Keys and Certificates](#)), you created a key store named "Agent.ks" for the Agent. Now, you need to set the Agent's key store in the Agent through the agent's interface in the HTTPS tab. In most Data Solutions agents with a Java console, the HTTPS tab is located in the Settings section under **Agent > Transports**.

To set the Agent's key store:

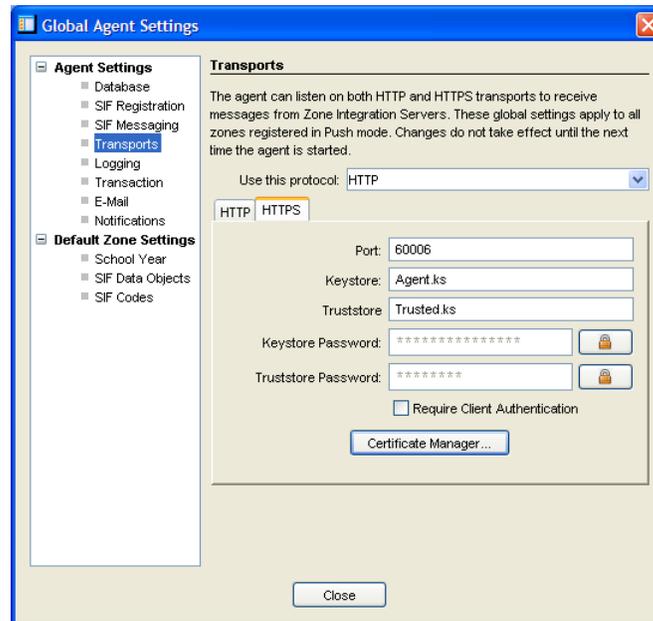
1. Open the agent.
2. Open Settings > Agent > Transports > HTTPS tab.
3. Enter the key store path in the box labeled "Keystore."
4. Enter the key store password in the box labeled "Keystore Password."



The key store is now in the Agent.

Importing the ZIS Certificate into the Agent

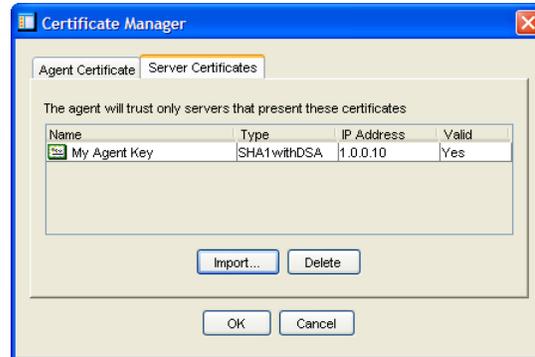
In a previous section of this document ([Creating Server Certificates](#)), you exported a certificate from the ZIS. Now, you need to import the ZIS public certificates into the Agent through the agent's interface in the HTTPS tab. In most Data Solutions agents with a Java console, the HTTPS tab is located in the Settings section under **Agent > Transports**.



To import ZIS certificates:

1. Open the agent.
2. Open Settings > Agent > Transports > HTTPS tab.
3. Click **Certificate Manager**.
4. Select the **Server Certificates** tab and click **Import...**
5. Navigate to the *.cer file that you exported from the ZIS, highlight the file, and click **Open**.

The name is the “Organizational” Unit name entered when the key was created in the ZIS. The IP address is the Common Name entered when the key was created in the ZIS.



6. Click **OK**. (Note: if you click **Cancel**, your import will not be saved.)

After you have imported the ZIS key, stop and restart the Agent so that the ZIS certificate will be recognized in the agent.

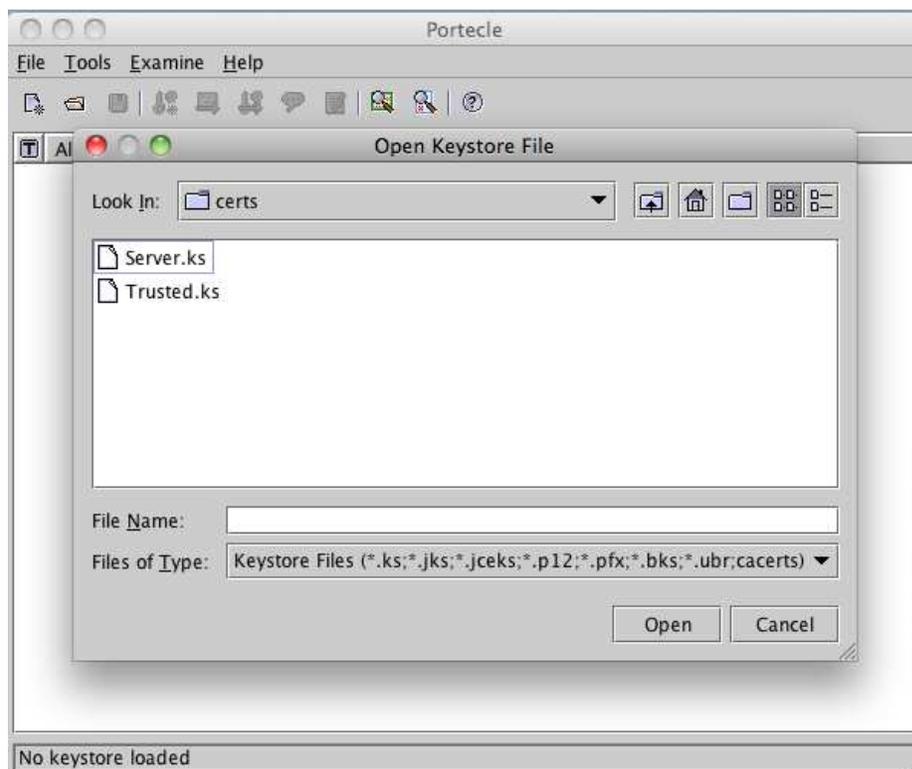
4. Other Certificate Scenarios

Importing Key Pairs from PFX Files

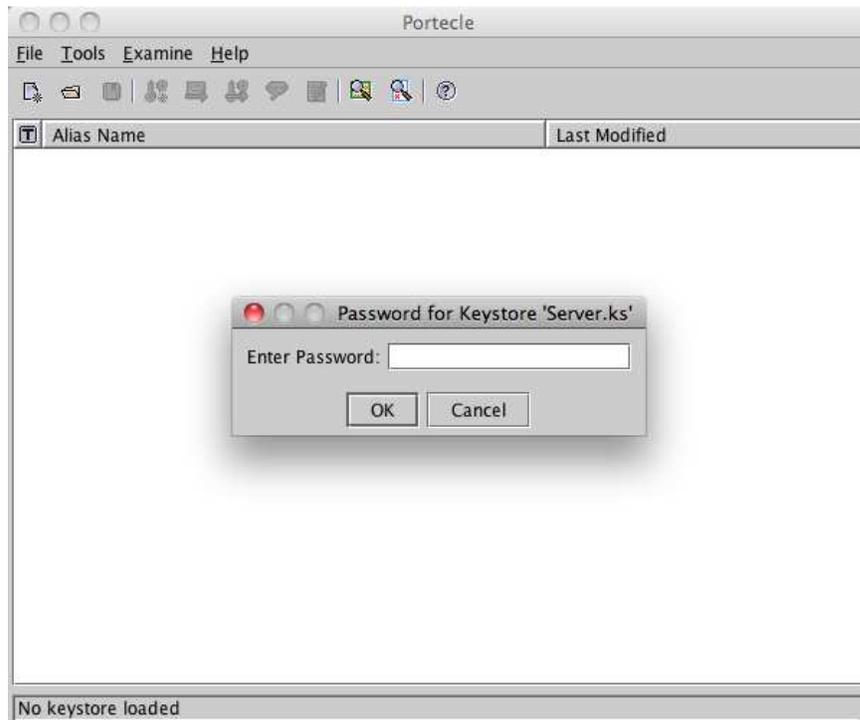
Following are instructions for importing key pairs from PFX files into the ZIS Server keystore for use as the ZIS's server key and certificate.

To import PFX files:

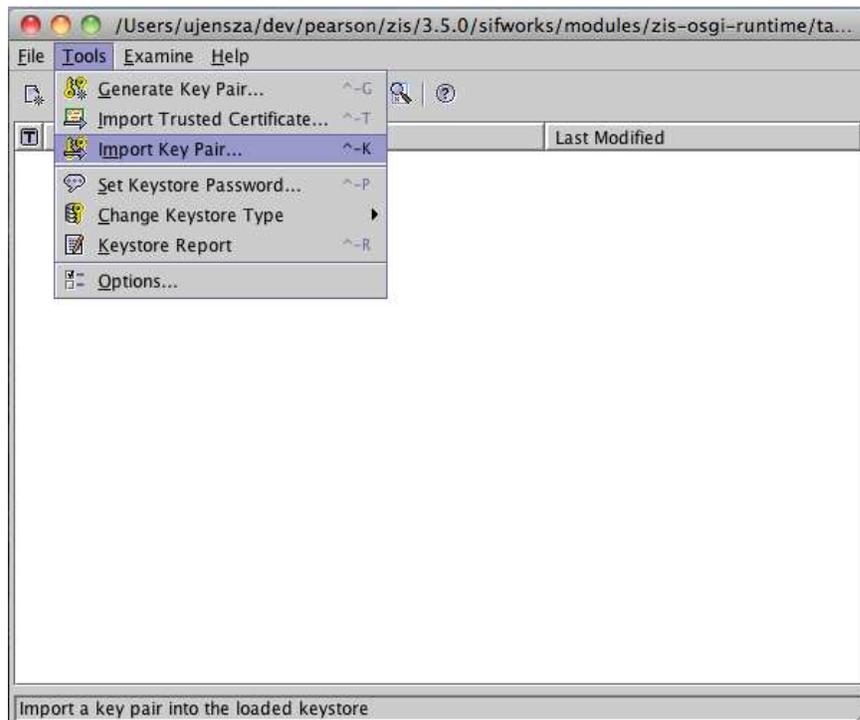
1. Shut down the ZIS.
2. Open the Server.ks file with Portecle, it's located in the certs directory where the ZIS is installed and has a default password of "changeit".



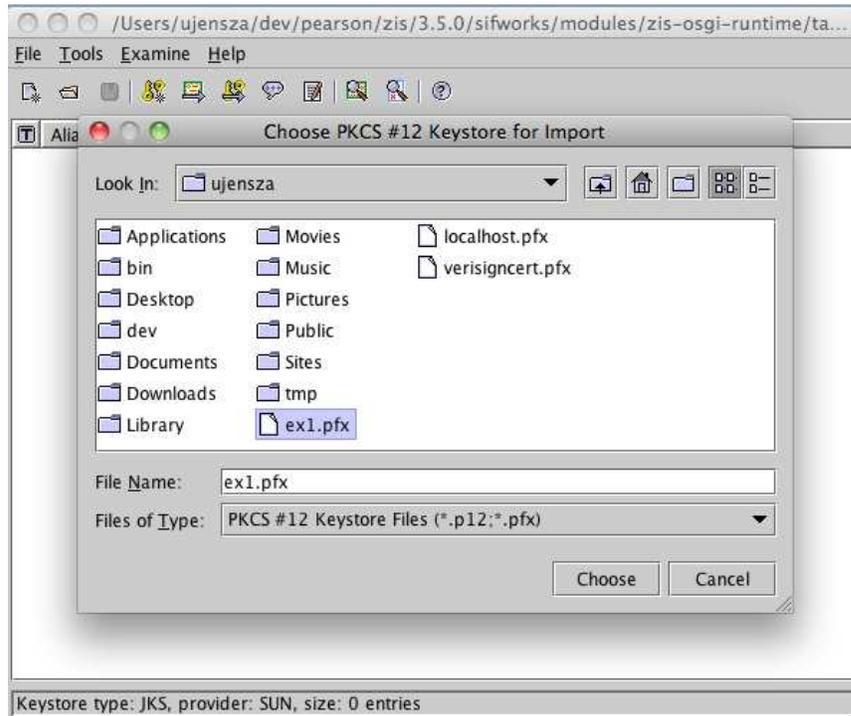
3. Enter the password for the keystore server.



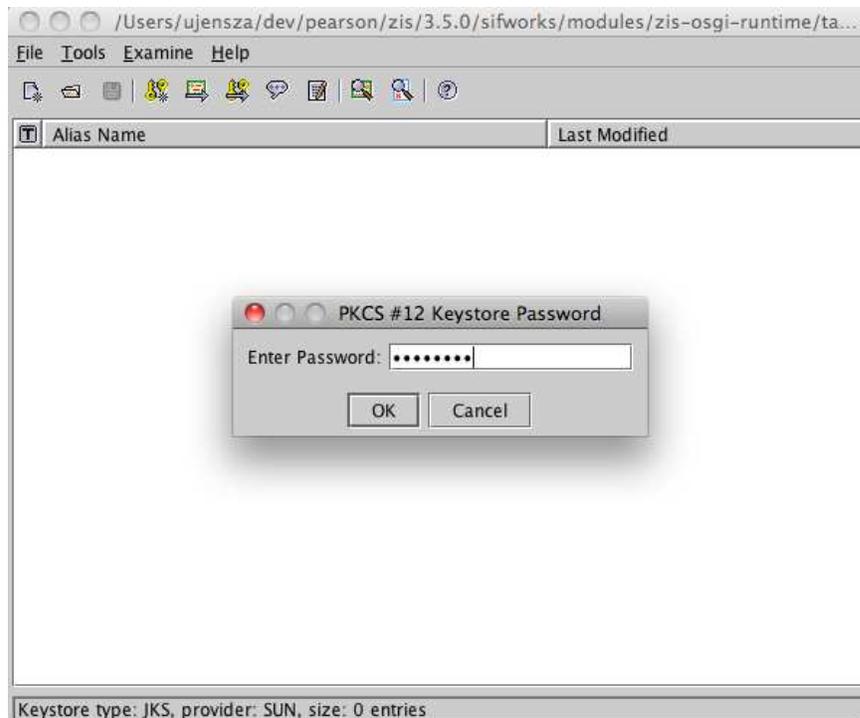
4. Click Tools then Import Key Pair.



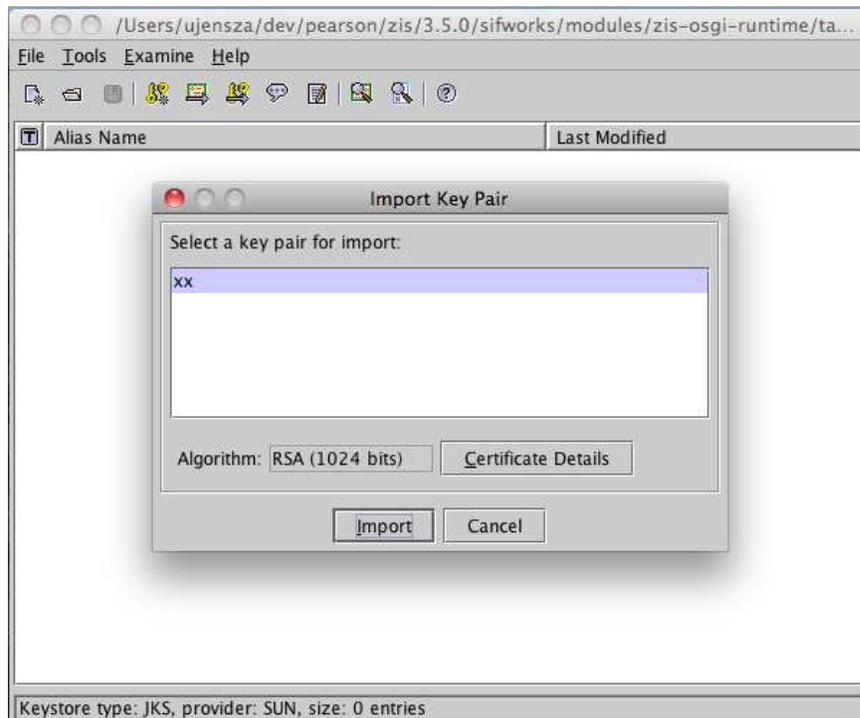
5. Select the PFX file from which you wish to import the key pair.



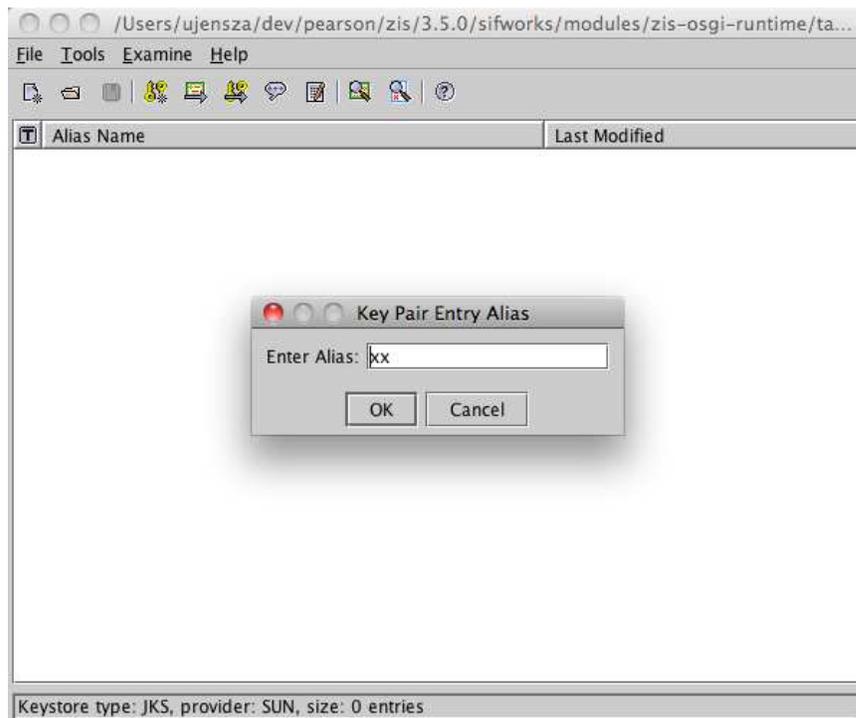
6. Enter the password (if any) for this PFX file.



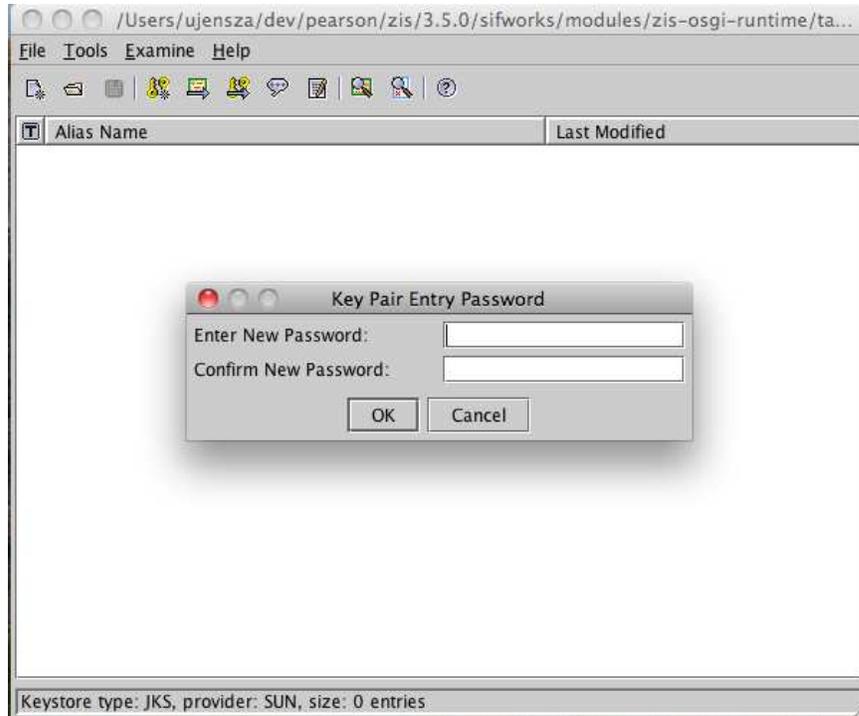
7. Select the pair you wish to import; there is usually only one.



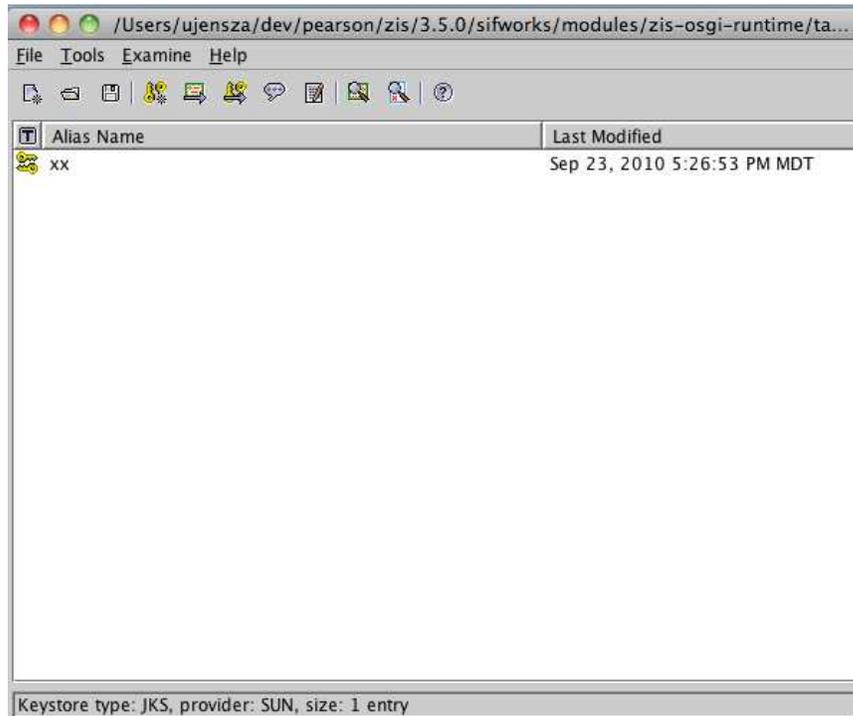
8. Choose an alias. (The alias is informative for the administrator; no special name is required.)



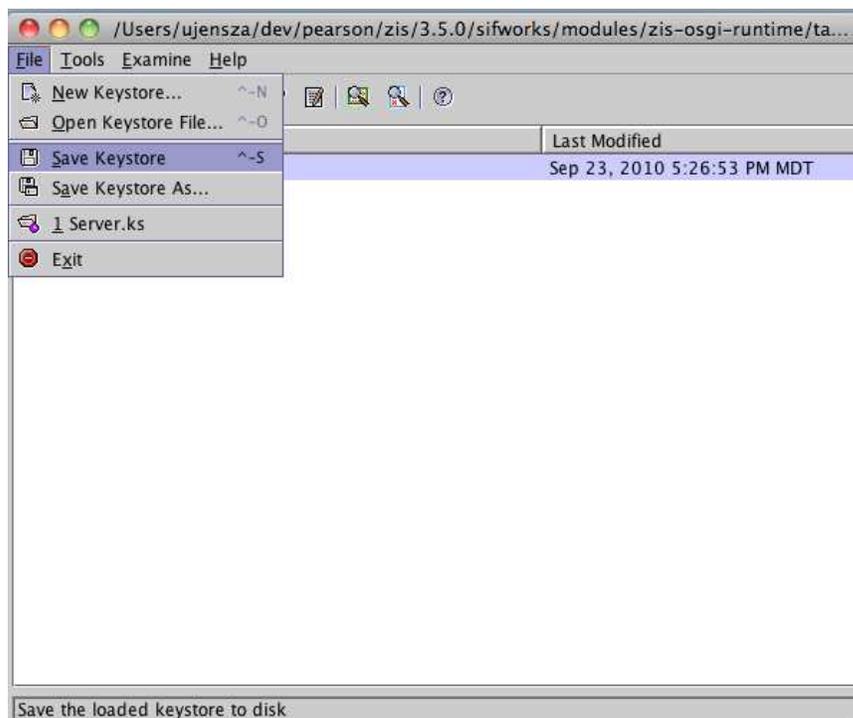
9. You must assign the same password you used to open your keystore (unless you have manually overridden this in the `zis.xml` file, which is unusual—in that case, use the appropriate password as configured).



10. You have now imported a key pair from a PFX file.



11. Save the keystore, or your changes will be lost.



12. Exit Portecle, and restart the ZIS.

5. Index

A

activate or deactivate transport(s):, 14
add an HTTPS Transport, 12
Agent Administration, 15, 22
Agent Certificates, 10
Agent Keys and Certificates, 15

C

Certificate Format Details, 14
Certificate Management, 6
create a Keystore file, 15
create the agent key, 15
Creating an agent key using Portecle, 15
Creating Server Certificates, 7

E

export the agent certificate, 17
Exporting Agent Certificates using Portecle, 17

F

From the Agent to the ZIS, 5
From the ZIS to the Agent, 4

H

How It Works, 4

I

Importing Agent Certificates, 10
Importing Key Pairs from PFX Files, 22
Importing the ZIS Certificate into the Agent, 20

K

Key Store, 19

M

Managing Agent Certificates, 11
Managing Certificates, 9

O

open a Keystore, 15
Other Certificate Scenarios, 22
Overview, 4

P

PFX Files, 22
Portecle, 15, 17

S

Saving the Keystore, 17
Server Certificate Options, 8
Server Certificates, 7

T

Transports, 12