Recipe 14 - Configuration Guide for Setting up Oblix ShareID 2.0 as an AA and CS

Table of Contents

1 Setup 1
1.1 Terms and Introduction 1
2 Partner Configuration 2
2.1.1 Configure a Partner AA 2
2.1.2 Configure a Partner CS 8

Version 2.0.0

1 Setup

1.1 Terms and Introduction

The SAML 1.0 is one of the adopted schemes within the E-Authentication architectural framework. This guide should help you setup SAML 1.0 and Oblix ShareID 2.0 as an Agency Application (AA) and Credential Service (CS). Remember that the Oblix setup screens are often the same, whether setting up an AA or a CS. After reviewing the terms, configure your scheme to handle SAML 1.0, starting at the login page shown in Figure 14-1.

Term	Definition
Agency Application (AA)	An online service provided by a government agency that requires an end user to be authenticated.
Credential Service (CS)	A service of a CSP that provides credentials to subscribers for use in electronic transactions. If a CSP offers more than one type of credential, then each one is considered a separate CS.
Credential Service Provider (CSP)	An organization that offers one or more CSs. Sometimes known as an Electronic Credential Provider (ECP).
Project Management Office (PMO)	The PMO is the organization that handles E-Authentication program management, administration, and operations.

2 Partner Configuration

2.1.1 Configure a Partner AA

Login

Open Oblix ShareID 2.0. Once the application has opened, the login screen will appear as shown in Figure 14-1. Enter a valid Username and Password and click the **Login** button.

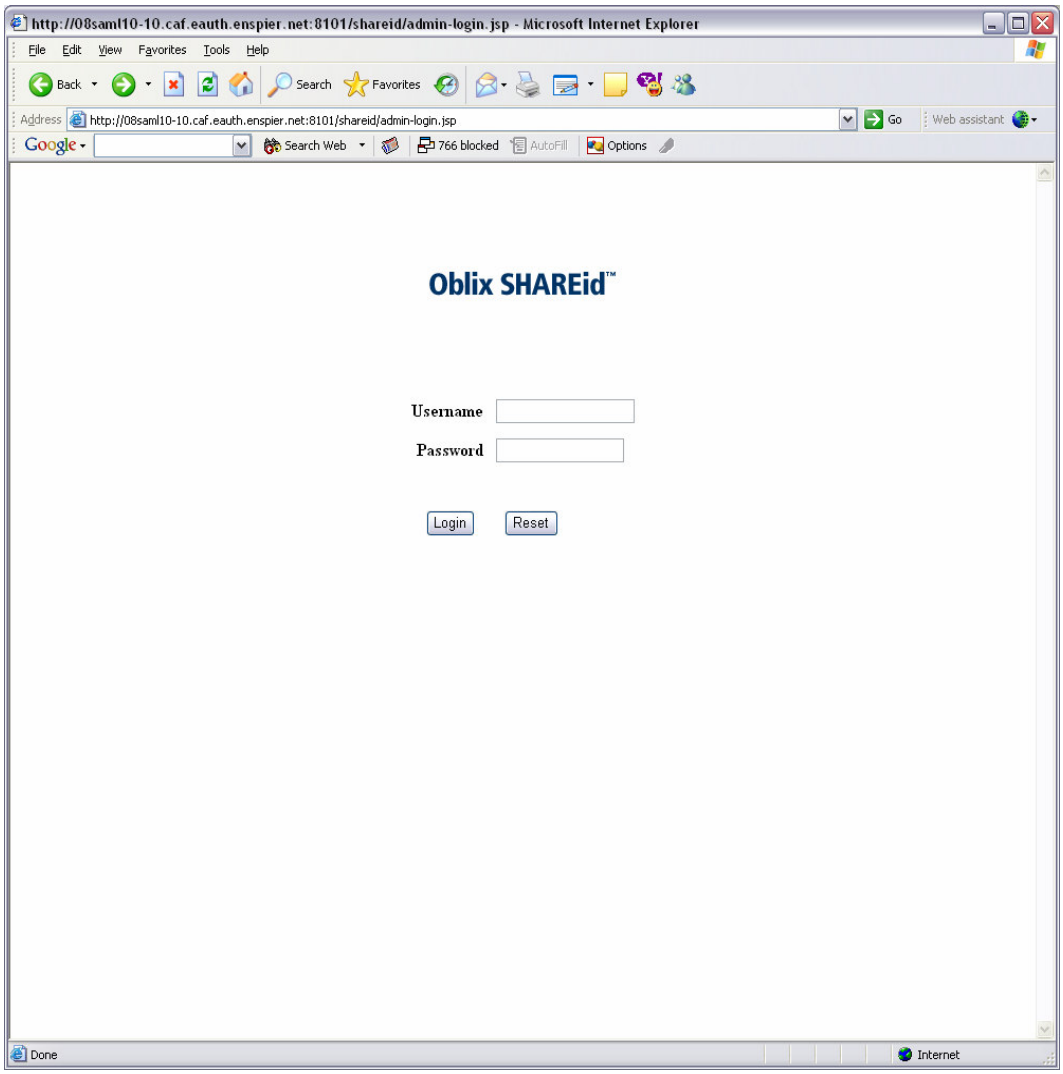

Figure 14-1

Once you have successfully logged into the application, the welcome screen will appear as shown in Figure 14-2.

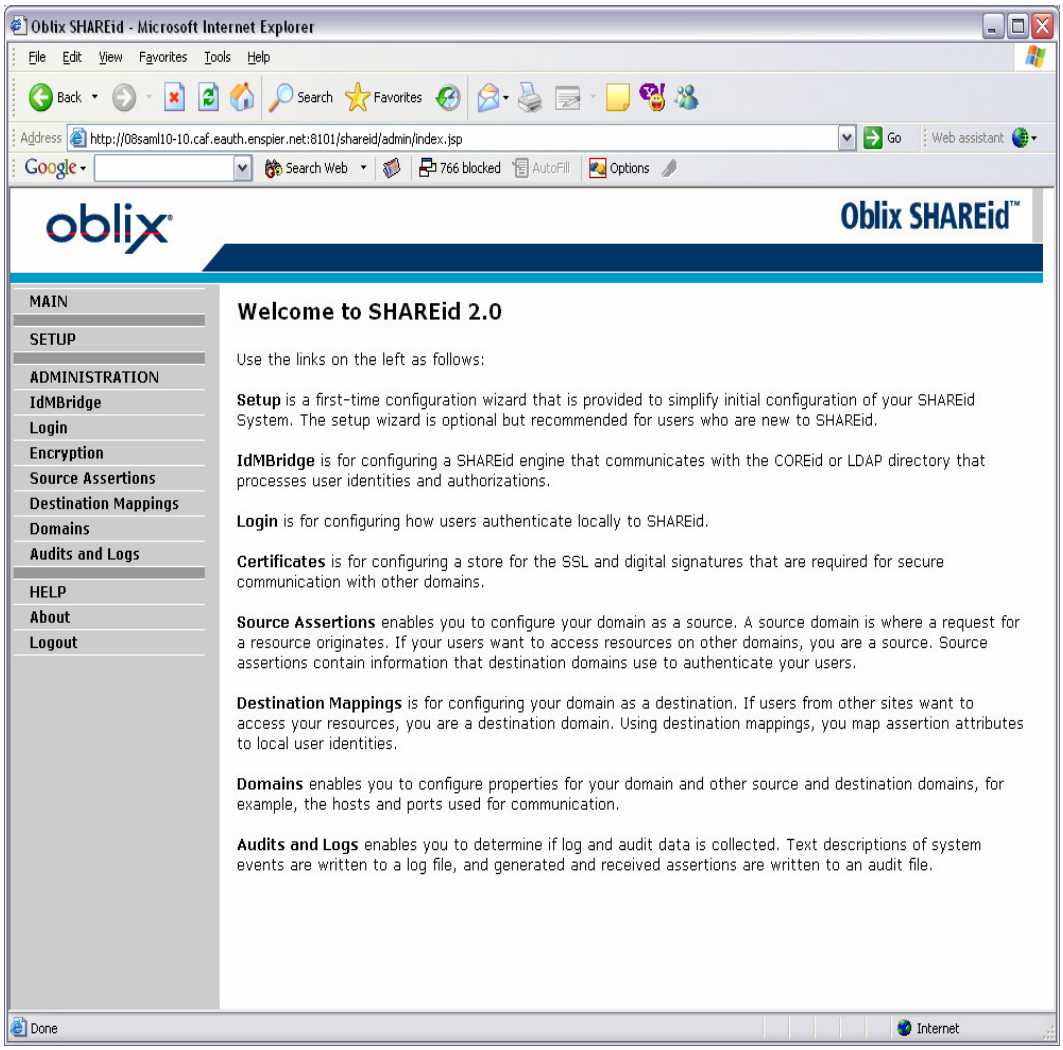

Figure 14-2

System Configuration for SSL

First, you must complete system configuration for SSL. This is completed by going to the menu bar on the left hand side of the screen and clicking on **Encryption > Certificates**. A screen will appear as shown in Figure 14-3. Enter all the appropriate information and click on the **Submit** button found at the bottom of the screen and restart ShareID.

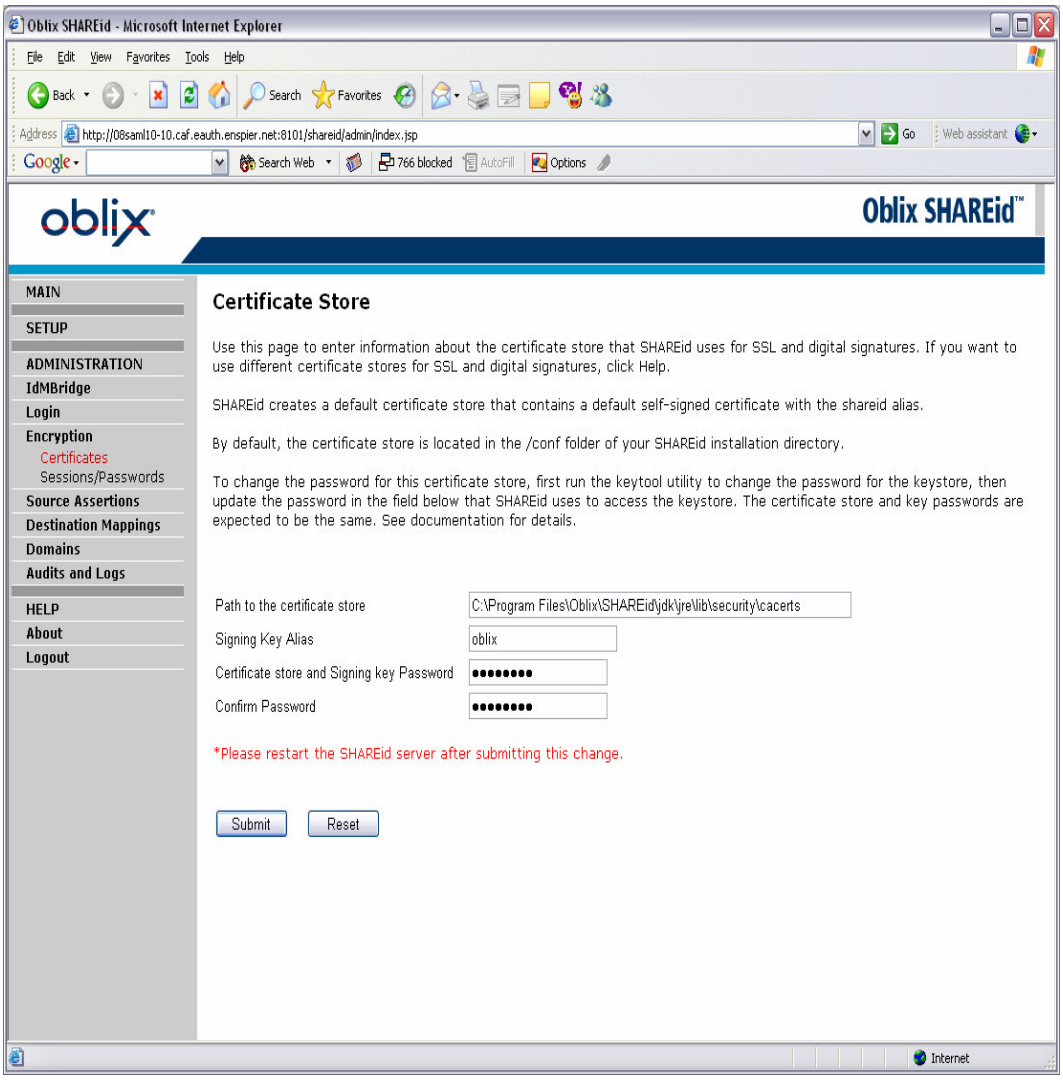

Figure 14-3

Note: The "Path to the certificate store" is the absolute path to the java keystore which contains your domain's client certificate to be used when partnering with CSs. The "Signing Key Alias" is the alias for that key in the keystore..

In our configuration we put our client cert in <shareid install dir>\jdk\jre\lib\security\cacerts. This keystore is installed by default with ShareID and contains CA certificates from all the major CAs. If you or your SAML partner's client certificate is not issued by one of the major CAs (i.e., verisign or thawte), you must add that CA's cert to this keystore.

Adding an Assertion Profile

Once you have restarted the application and logged in as previously described, the next step is to configure a partner AA. The first step involved in configuring a partner AA is to add an assertion profile (the attributes you want to include in your assertion). This can be completed by going to the menu bar on the left hand side of the screen and clicking on **Secure Assertions > Add Assertions**. A screen will appear as shown in Figure 14-4. Enter all appropriate information, check all boxes as shown in Figure 14-4, and then click the **Submit** button found at the bottom of the screen.

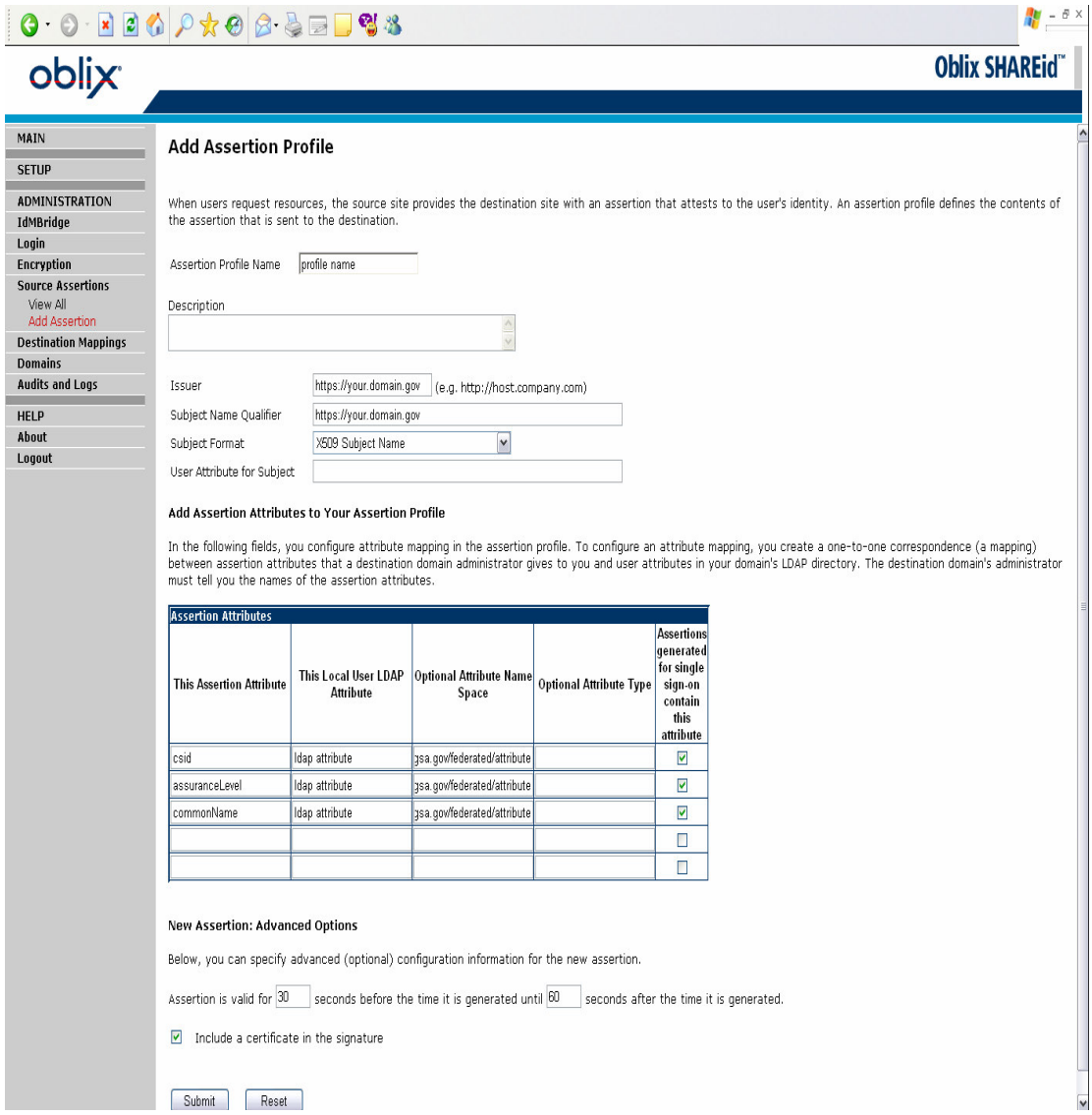

Figure 14-4

Note: Attribute Name Space = http://eauthentication.gsa.gov/federated/attribute
Required Attributes (as of 10/19/04) are csid, commonName, and assuranceLevel.

Adding a Partner Domain

The next step is enter information for your partner AA's Domain. This screen can be found by going to the menu bar on the left hand side of the screen and clicking on **Domains > Add Other Domains > Non-SHAREid**. A screen will appear as shown in Figure 14-5. Enter all required information as it pertains to your system and be sure to check all boxes as shown in Figure 14-5.

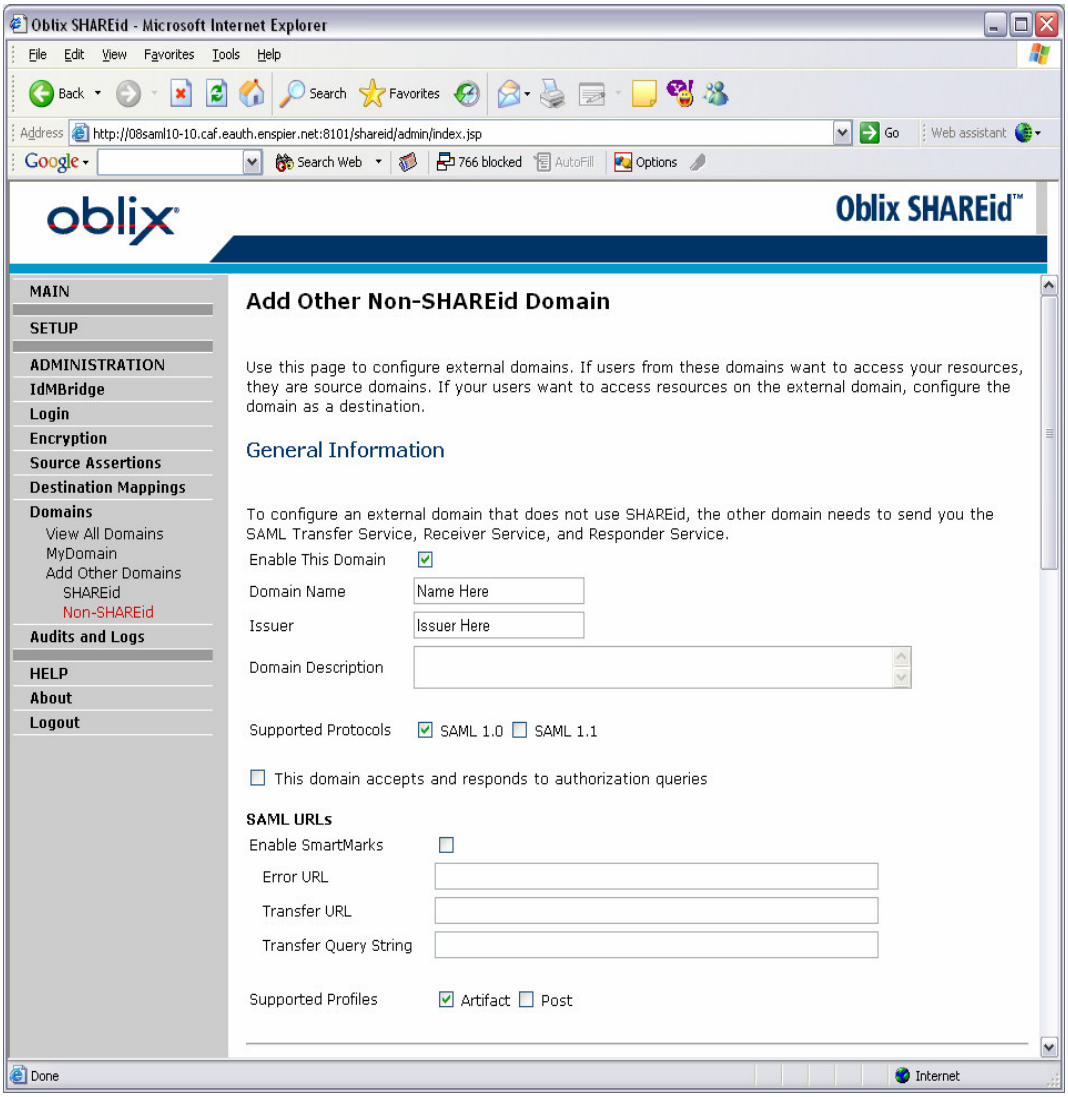

Figure 14-5

Next, scroll down to the **Configure This Domain as a Destination** section, which is shown in Figure 14-6 below. Enter all appropriate information. In the Assertion Profile pull down, select the assertion profile you created previously. Click on the X.509 radio button, and then click the **Submit** button found at the bottom of the screen.

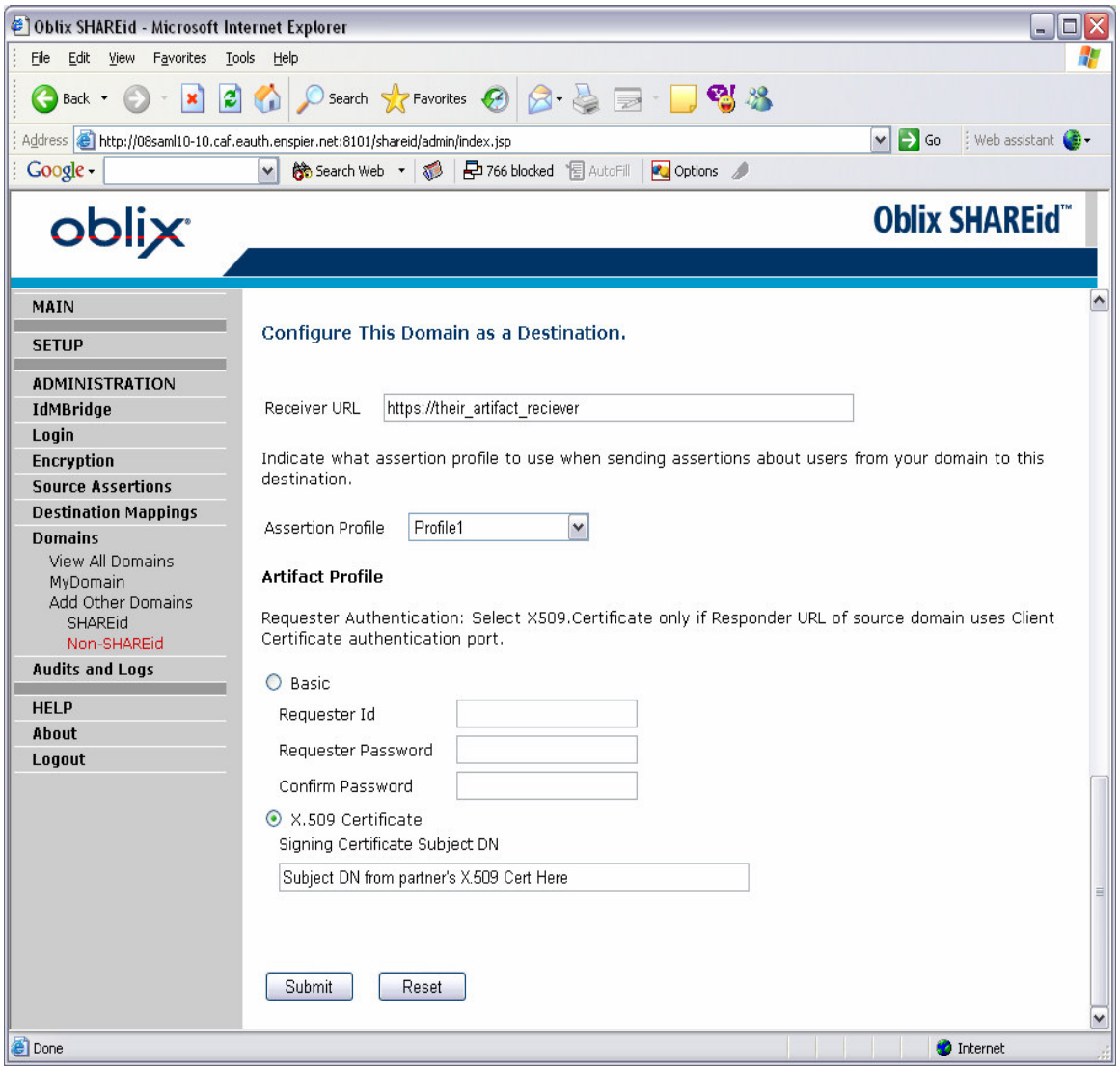

Figure 14-6

2.1.2 Configure a Partner CS

Login

Open Oblix ShareID 2.0. Once the application has opened, the login screen will appear as shown in Figure 14-7. Enter a valid Username and Password and click the **Login** button.

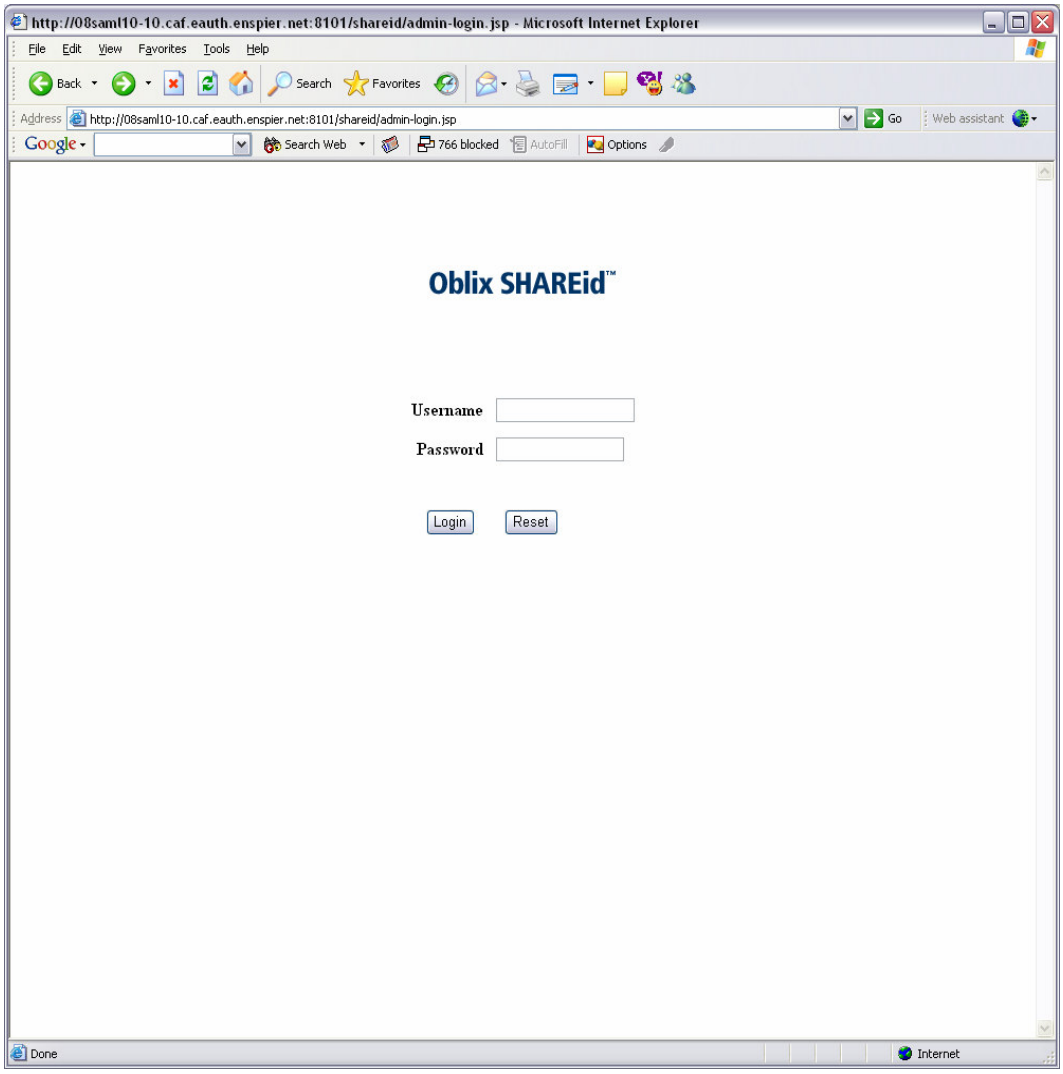

Figure 14-7

Once you have successfully logged into the application, the welcome screen will appear as shown in Figure 14-8.

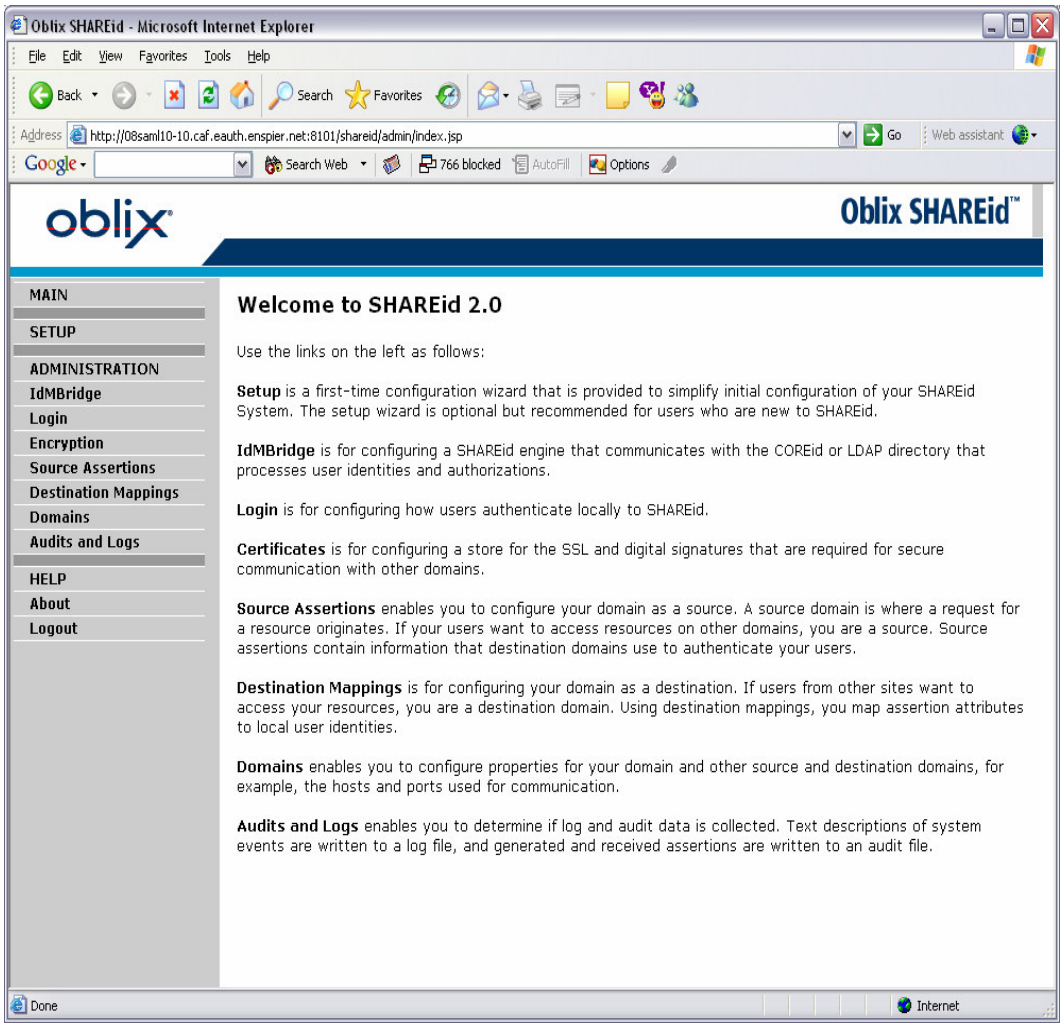

Figure 14-8

System Configuration for SSL

First, you must complete system configuration for SSL. This is completed by going to the menu bar on the left hand side of the screen and clicking on **Encryption > Certificates**. A screen will appear as shown in Figure 14-9. Enter all the appropriate information and click on the **Submit** button found at the bottom of the screen and restart ShareID.

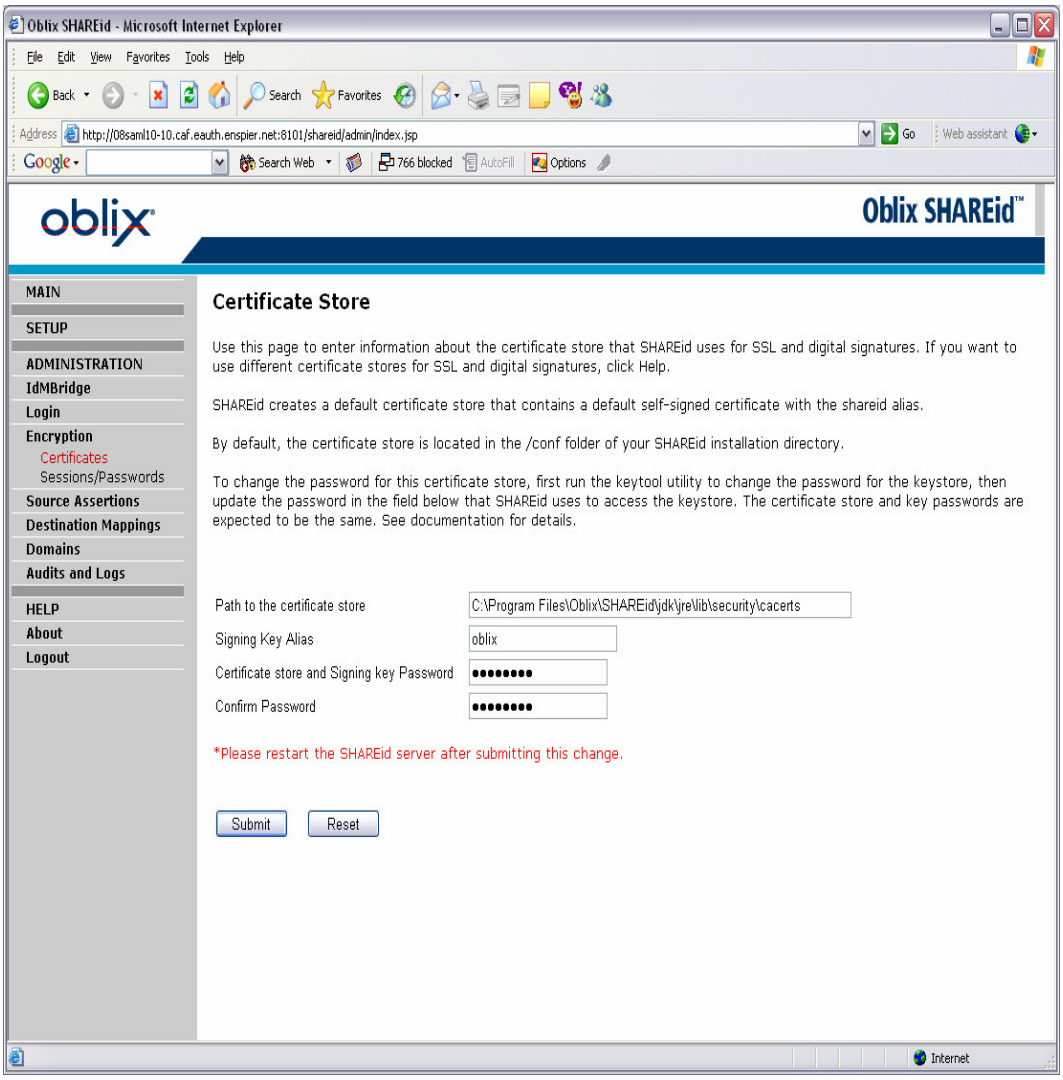

Figure 14-9

Note: The "Path to the certificate store" is the absolute path to the java keystore which contains your domain's client certificate to be used when partnering with CSs. The "Signing Key Alias" is the alias for that key in the keystore.

In our configuration we put our client cert in <shareid install dir>\jdk\jre\lib\security\cacerts. This keystore is installed by default with ShareID and contains CA certificates from all the major CAs. If YOU OR YOUR SAML PARTNER'S client cert is not issued by one of the major CAs (i.e., verisign or thawte), you must add that CA's cert to this keystore.

Assertion Mapping

Once you have restarted the application and logged in as previously described, the next step is to add an assertion to user mappings. This is completed by going to the menu bar on the left hand side of the screen and clicking on **Destination Mappings > Add Mappings**. A screen will appear as shown in Figure 14-10. Enter all appropriate information and then click on the **Submit** button found at the bottom of the screen.

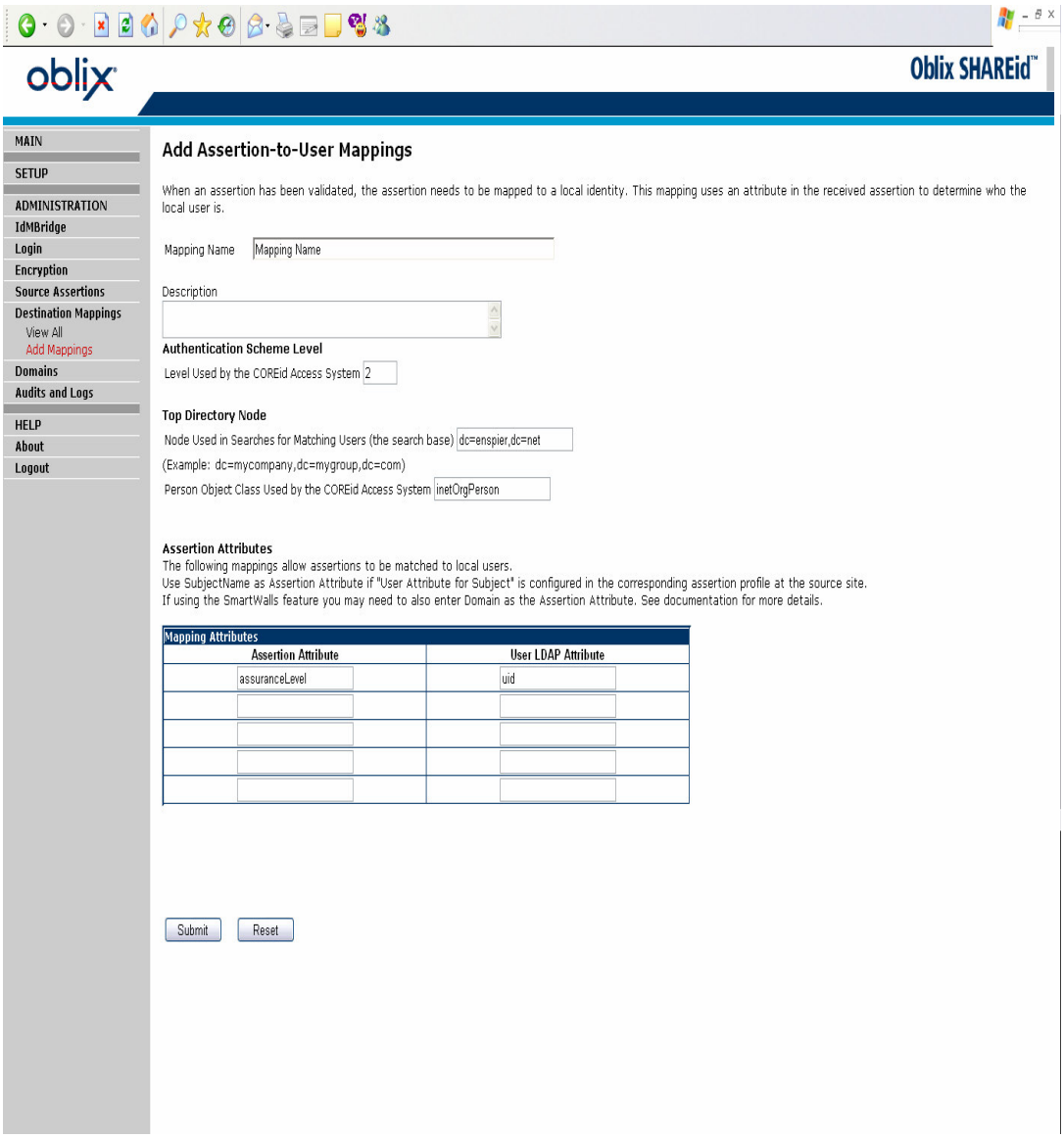

Figure 14-10

Note: dc=enspier,dc=net is our LDAP search base and inetOrgPerson is our LDAP user object. We have a many to one mapping for assertion users to local users. The assurancelevel attribute from the assertion is mapping to a local user whose uid is 2.

The next step is to configure a CS partner, which first requires entering general information. The general information page can be found by going to the menu bar on the left hand side of the screen and clicking on **Domains > Add Other Domains > Non-SHAREid**. A screen will appear as shown in Figure 14-11. Enter all required information as it pertains to your system and be sure to check all boxes as shown in Figure 14-11.

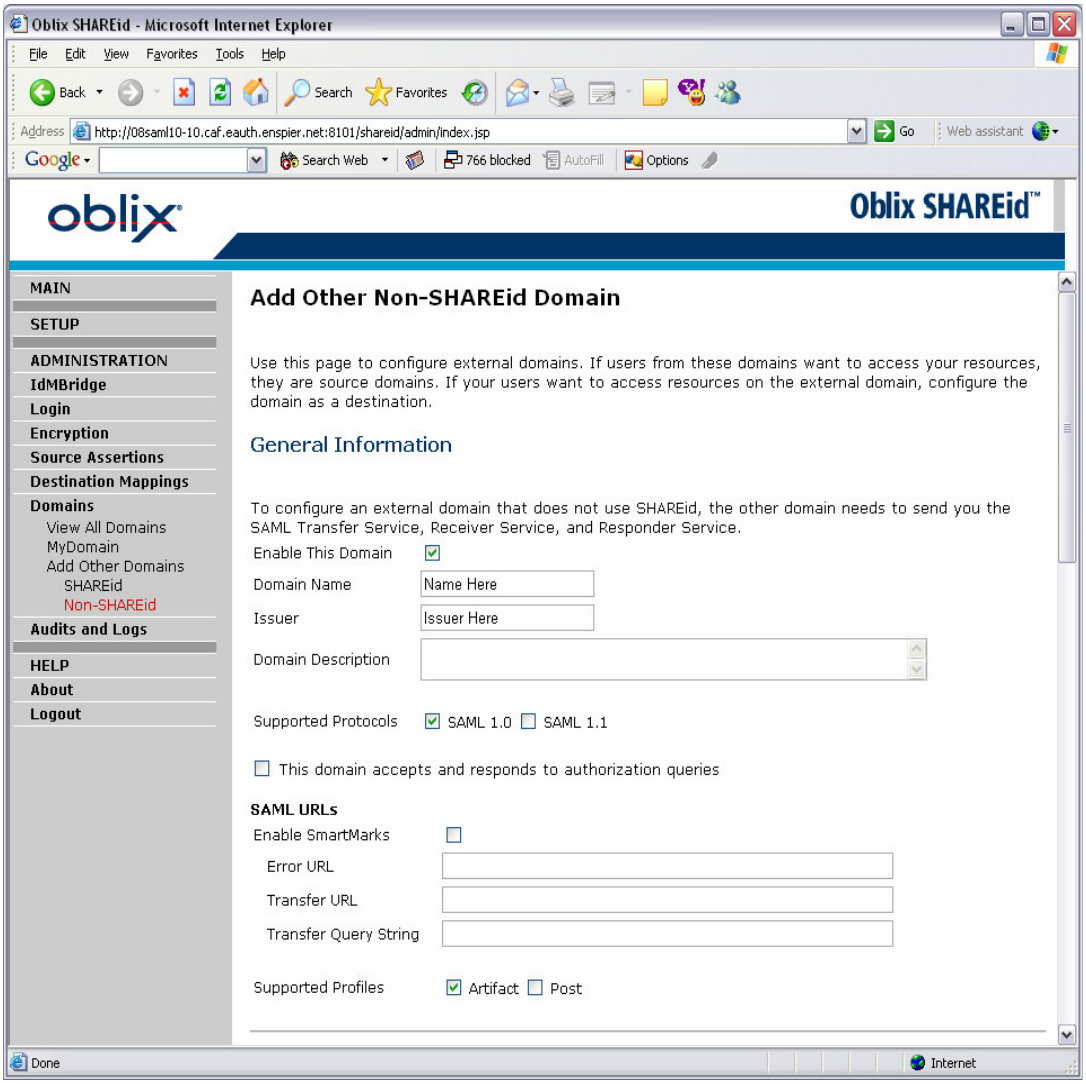

Figure 14-11

Next, scroll down to the **Configure This Domain as a Source** section, which is shown in Figure 14-12 below. Enter all appropriate information. In the Mapping Name pull down be sure to select the assertion mapping created in the previous step. When completed, click the **Submit** button found at the bottom of the screen.

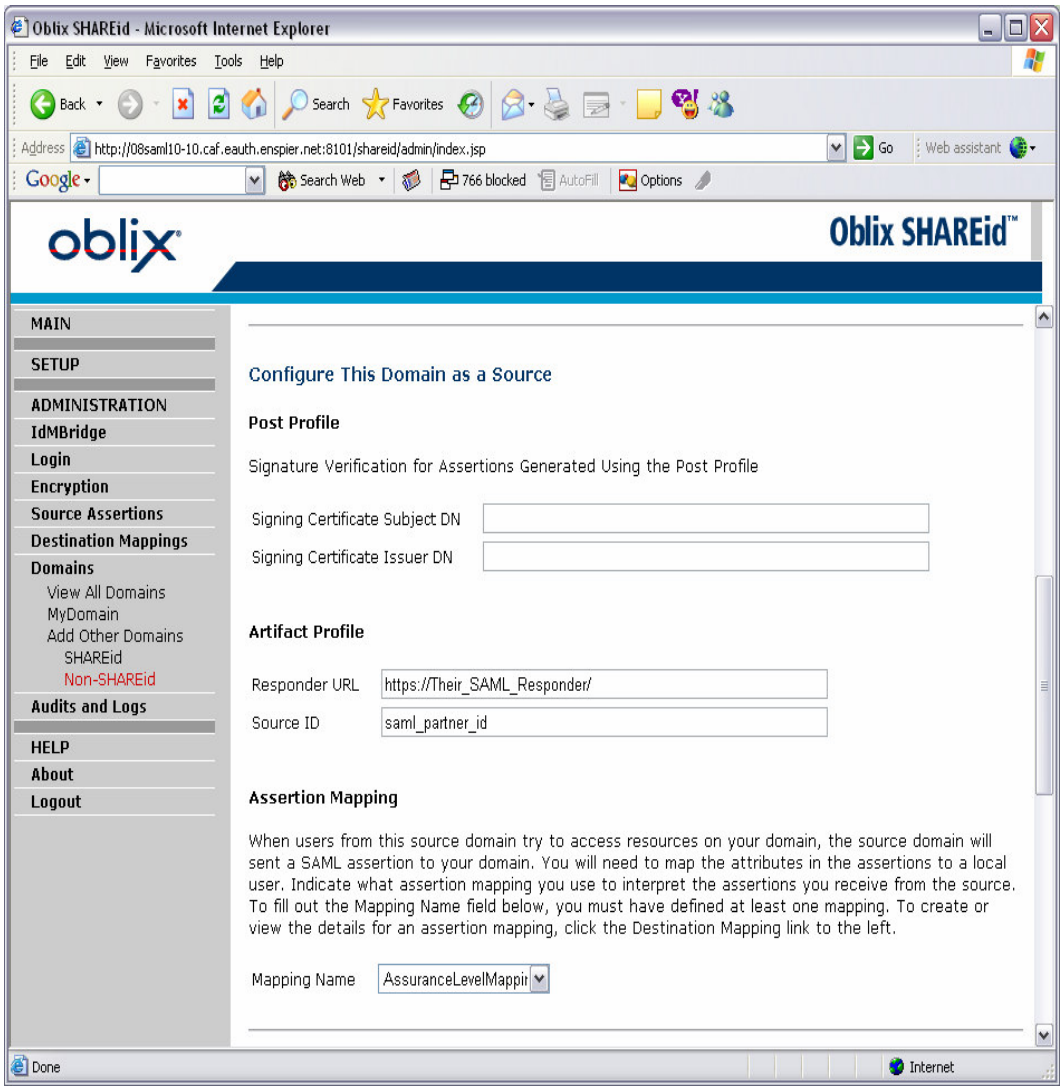

Figure 14-12