IBM Security Access Manager 7.0

INTEGRATION GUIDE

Protecting IBM ISAM Security Web Gateway 7.0 Using Certificate-based Authentication

Contents

Description

This document provides guidance for deploying multi-factor user authentication to IBM ISAM 7.0 using any of SafeNet's certificate-based authenticators. It is intended for IT administrators or technical personnel familiar with the IBM ISAM environment and who are responsible for the implementation of strong authentication within an enterprise. It provides basic information on how to implement two-factor authentication and integrate certificate-based authentication solutions to enhance network security.

IBM® Security Access Manager for Web provides an integrated security management platform for authentication services, access control, authorization services, identity mapping, web single sign-on, entitlements, and audit services across enterprise resources. The solution also provides integrated, policy-based security management for the extended enterprise that enables customers, business partners, employees, suppliers, and distributors to securely access enterprise resources in a trusted manner. The Information Center maintains data on the Security Access Manager for Web components.

Organizations using IBM ISAM to protect their resources can now implement a certificate-based authentication solution for powerful two-factor authentication.

As users connect remotely to the reverse proxy, multi-factor authentication is a fundamental requirement. SafeNet's certificate-based authenticators provide secure remote access, as well as other advanced functions, including digital signing, password management, network logon, and combined physical/logical access in a single authenticator. The authenticators come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). SafeNet Authentication Client manages SafeNet's extensive portfolio of certificate-based authenticators, ensuring complete support for all currently deployed eToken and iKey devices.

Administrator Prerequisites

To successfully implement the SafeNet certificate-based authentication solution, the administrator should be familiar with the following:

- Certificate Authority (CA)—In order to use a PKI solution, there is a need to have a CA installed that is able to issue digital certificates. In this guide, Microsoft CA is used to enroll client certificates.
- IBM Security Access Manager (IBM ISAM 7.0)
- SafeNet Authentication Client 8.2

Integration System Requirements

This section details the requirements needed to install and configure the certificate-based authentication (CBA) solution for IBM ISAM 7.0.

NOTE: This guide assumes that an IBM ISAM 7.0 environment is fully installed and properly configured prior to the CBA integration. In addition, fully functional ISAM explicit authentication (user/password) must be implemented.

The following diagram shows the environment required to implement an IBM ISAM 7.0 solution using SafeNet's certificate-based authentication:

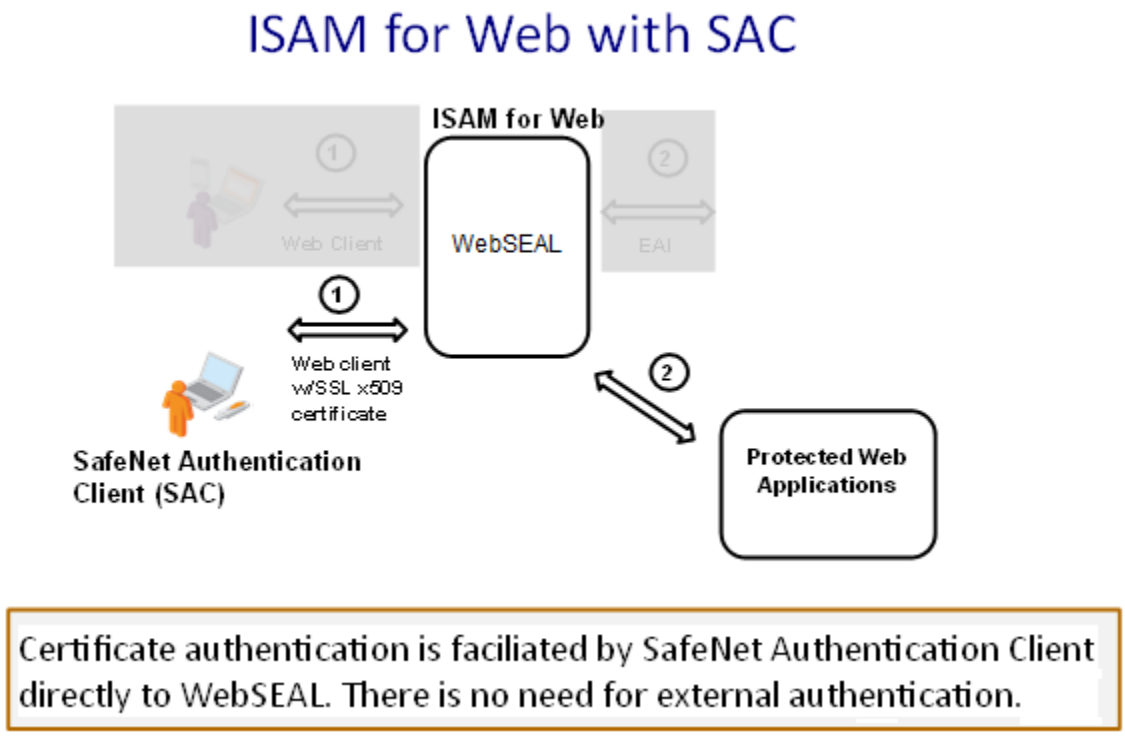

Figure 1: SafeNet Authentication for ISAM 7.0

1. In this example, a user connects a SafeNet CBA token to the Windows client computer.

   The user opens a web browser and connects to the ISAM WebSEAL-protected resource.

   The user is prompted to enter the token password.
2. Upon successful authentication, the user is directed to the protected web application.

The environment components are:

- Microsoft Enterprise CA
- IBM ISAM 7.0
- SafeNet Authentication Client (SAC) 8.2
- SafeNet eToken 5100

Product Prerequisites

IBM ISAM 7.0

Ensure the following:

- All prerequisites are fulfilled: http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.isam.doc_80/ameb_install_guide/concept/con_istl_preq_prod.html
- IBM ISAM 7.0 is installed
- SafeNet Authentication Client (SAC) 8.2 is installed on the server with default settings

For more information on SAC, or to receive the download link, contact SafeNet support:

http://www.safenet-inc.com/request-information/

Clients

Ensure the following:

- Clients are running Windows XP or Microsoft Windows 7
- SafeNet Authentication Client (SAC) 8.2 is installed on all clients

IBM ISAM 7.0 Configuration for CBA Support

This section explains how client authentication works, and provides the steps needed to install and implement SAC 8.2 for IBM ISAM 7.0.

How Client Authentication Works

A user is provided with a smart card containing a user certificate and a private key. In order to access the private key stored on the smart card, the user must provide the correct PIN. Any website or virtual directory served by IIS can be configured to accept or require client certificates.

Once the client certificate has been validated and sent to IIS, the web server communicates with an Active Directory domain controller to map the certificate to a domain user account. This step requires that **Active Directory Client Certificate Authentication** be enabled in the **WWW Service Master Properties** dialog box in the Internet Services Manager. IIS authenticates the user and enumerates applications using a list of group SIDs. Thereafter, IIS impersonates the user's domain account for script access.

Installing and Configuring SAC 8.2

SafeNet Authentication Client (SAC) 8.2 includes all the files and drivers needed to support SafeNet smart card integration. SAC 8.2 must be installed on each computer where smart card authentication will be required, including the XenApp 6.5 server machine.

IBM ISAM 7.0 Configuration

This section provides the steps needed to configure IBM ISAM 7.0 so that the user can log on to the protected web application using a smart card.

Basic Configuration

IBM ISAM 7.0 is configured with default options. This section describes the initial configuration steps required to create a basic environment.

To set up basic configuration:

1. Log in to the **Security Web Gateway Appliance** console.

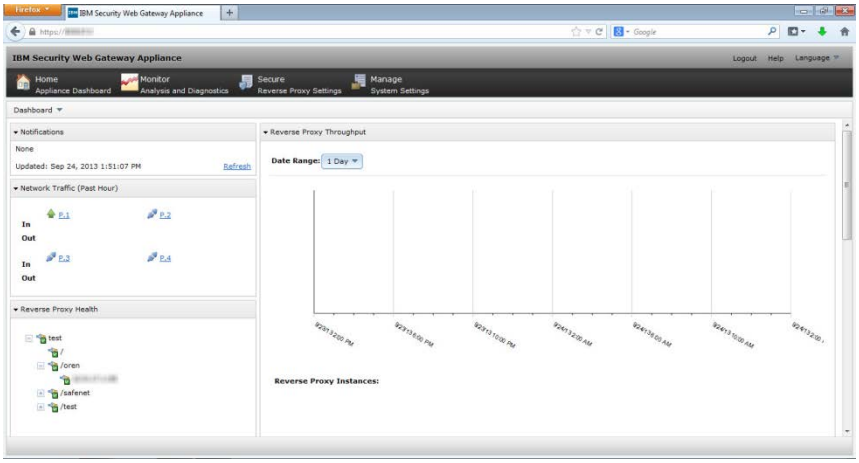

Figure 2: Security Web Gateway Appliance console

2. Go to **Secure > Reverse Proxy**. Ensure that you have a reverse proxy instance.

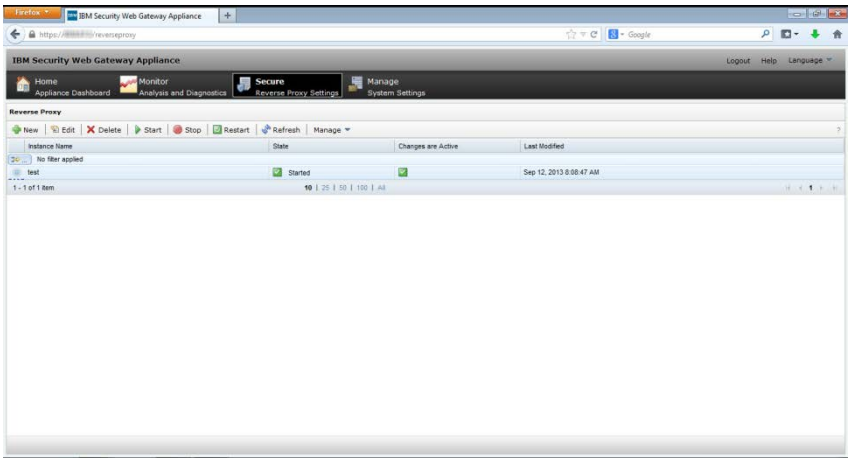

Figure 3: Security Web Gateway Appliance Reverse Proxy

3. Click the reverse proxy entry and then click **Manage > Junction Management**.

   Ensure that a junction is configured (the web application that will be protected by WebSEAL). In the examples below, the safenet-inc.com website is configured to be the protected web application.

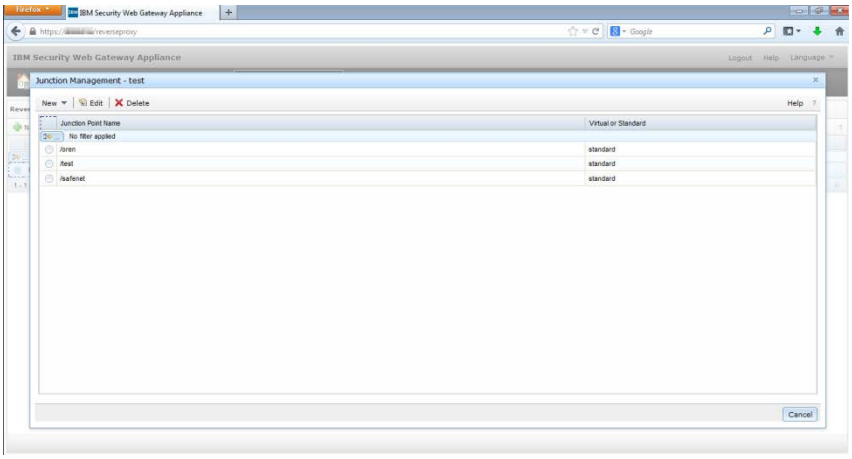

Figure 4: Junction Management

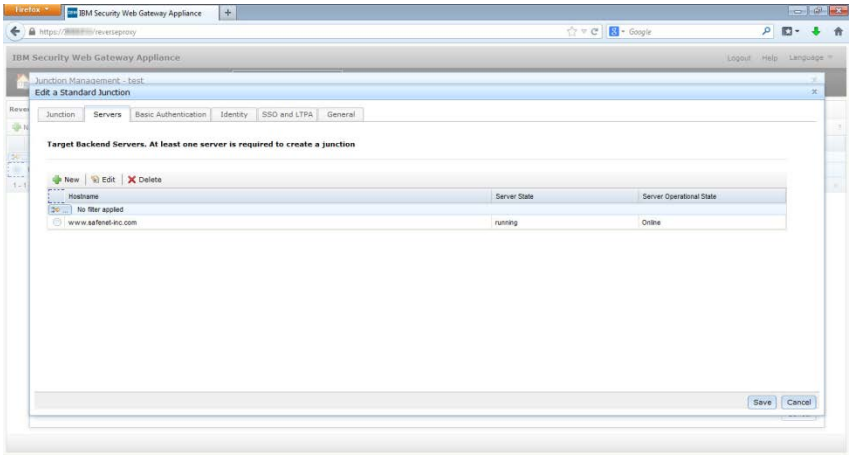

Figure 5: SafeNet Junction

4. Log in to the junction under the reverse proxy you created and make certain you have a username and password to access WebSEAL.

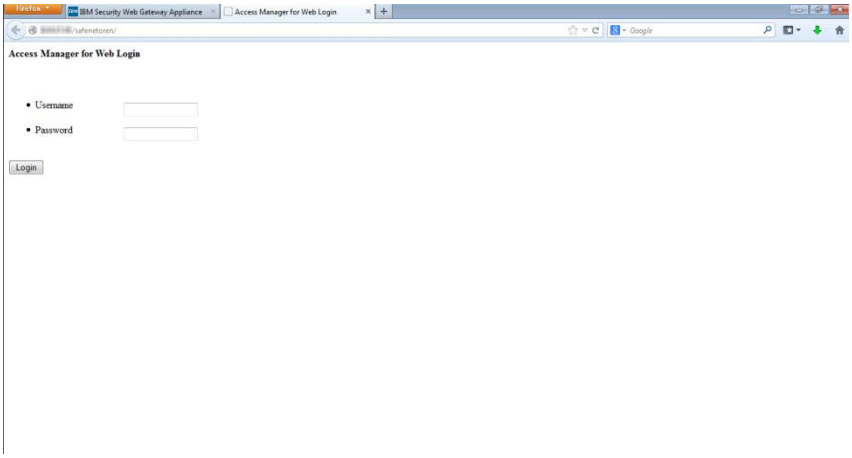

Figure 6: WebSeal username/password login

Configuring Reverse Proxy for CBA

To use CBA in IBM ISAM 7.0:

1. Click **Secure > Reverse Proxy**.
2. Select the reverse proxy you created and click **Edit**. On the **Server** tab, under **Client Connection**, verify that the **HTTPS** check box is selected.

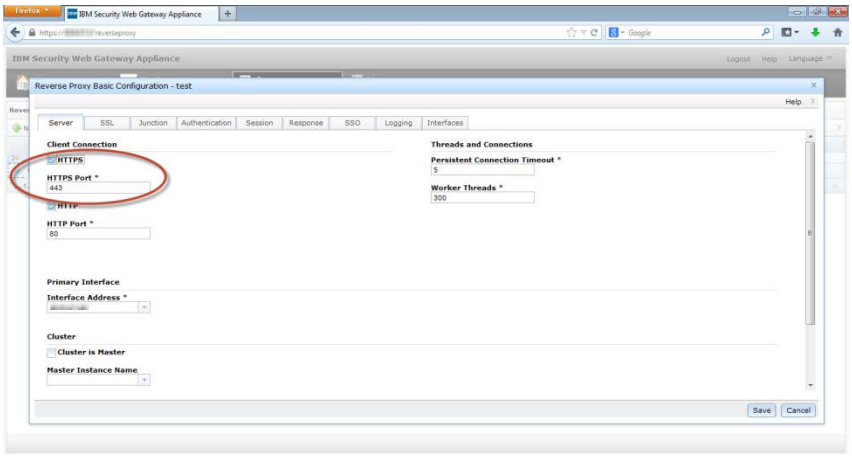

Figure 7: HTTPS connection configuration

3. Click the **Authentication** tab. Under **Client Certificates,** in the **Accept Client Certificates** field, select **Required**.

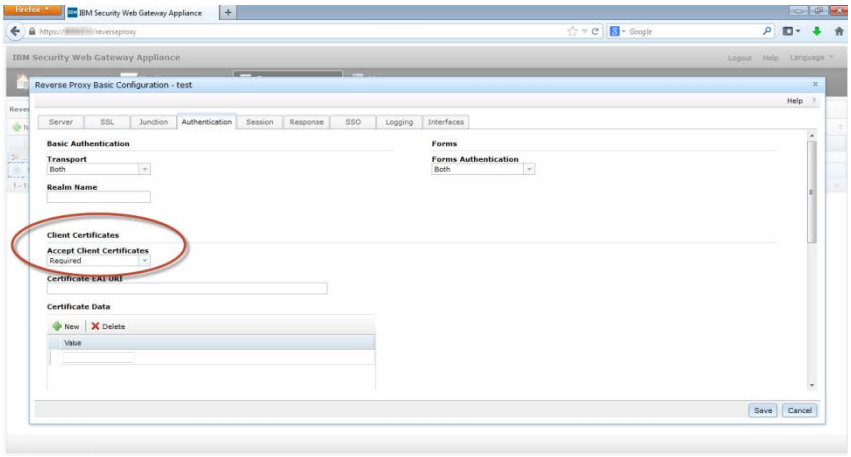

Figure 8: Reverse proxy authentication

4. Click **Save**.
5. When prompted, click the link to deploy and restart the reverse proxy.

Configuring the Client Certificate Mapping File

WebSEAL uses the Cross Domain Authentication Service (CDAS) to authenticate a user and provide a Security Access Manager user identity.

The client certificate user-mapping CDAS provides a mechanism by which WebSEAL can use the details of a client certificate to determine the corresponding Security Access Manager user identity. The rules that govern the mapping of the client certificate are defined in XSL style notation.

The CDAS supports all user registries that Security Access Manager supports.

The rule evaluation can return an LDAP search string. This string representation of the LDAP search filter must be in accordance with the format described in RFC 2254.

For more information on user mapping rules, refer to the following link:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.isam.doc_80%2Fameb_appl_guide%2Freference%2Fref_eg_usr_map.html

To configure the client certificate mapping file:

1. Go to **Secure > Client Certificate Mapping**. Click **New** to create a new CDAS file.

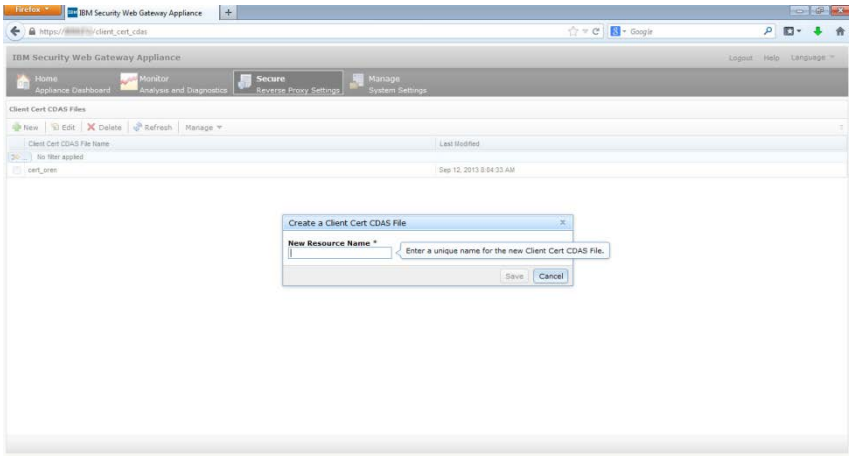

Figure 9: Creating a new CDAS file

2. Enter a name for the mapping file and then click **Save**.
3. Select the CDAS filename that you created and click **Edit** on the top menu bar. The CDAS file content is displayed.

4. Scroll to the end of the file and change “SubjectDN” to “SubjectCN”. In this case, the xslt rule will extract the **CN** data field from the certificate and compare it to the **CN** data field in the ISAM user store.

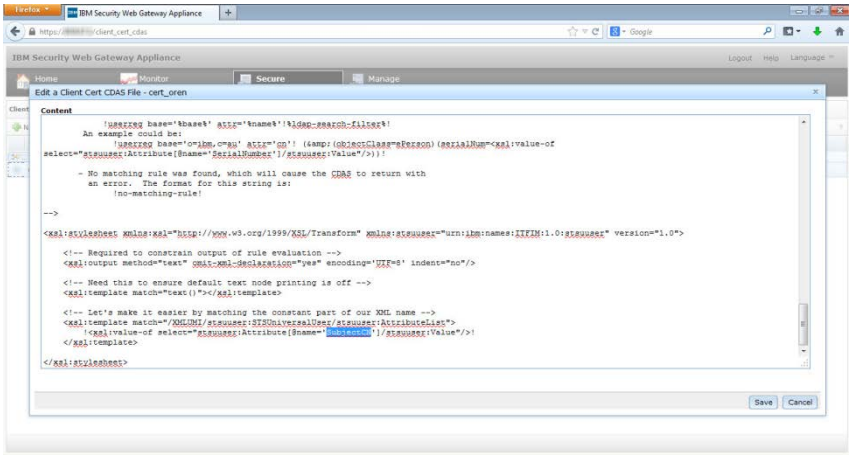

Figure 10: Changing the xslt rule

5. Click **Save** to deploy the file.
6. Click **Secure > Reverse proxy**. Select the reverse proxy and click **Manage > Configuration > Edit Configuration File**.

   Verify that in the **[cert-map-authn]** stanza, the **rules-file** key is set to the certificate mapping file you created.

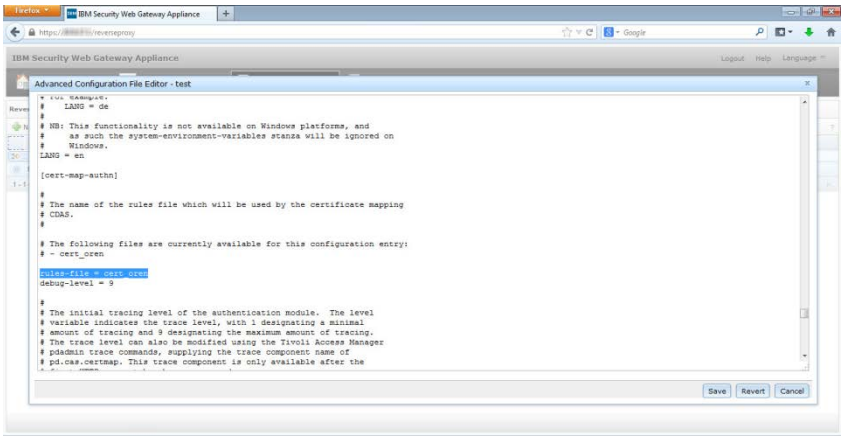

Figure 11: Certificate mapping file configured in the reverse proxy

7. Click **Save**.
8. When prompted, click the link to deploy and restart the reverse proxy.

Configuring SSL Certificates

In order for ISAM to use a certificate that was created with an external Root CA, it must have the Root CA signer certificate in its database. By default, an SSL certificate database, **pdsrv**, is created when installing ISAM 7.0. The database contains known signer certificates (for example, Verisign).

For more information on managing signer certificates in a certificate database, refer to the following link:

http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.isam.doc_80%2Fameb_webseal_appl_guide%2Ftask%2Ftsk_lmi_signer_cert_mng.html

To add your local Root CA signer certificate:

1. Click **Secure > Global keys > SSL Certificates**.

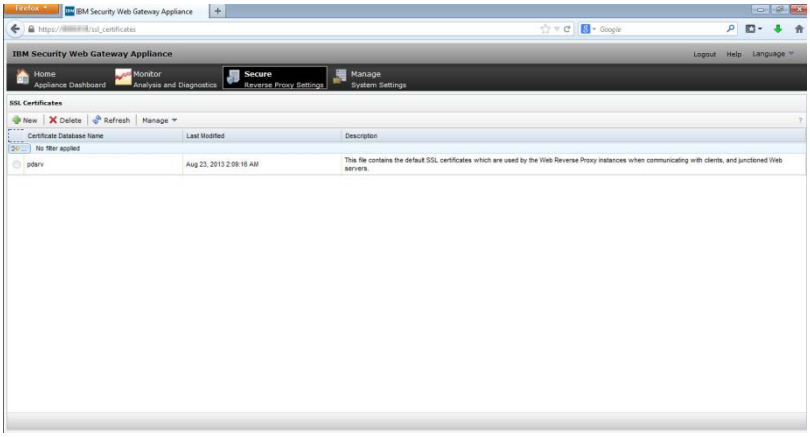

Figure 12: SSL Certificates main page

2. Select the file **pdsrv** and click **Manage > Edit SSL Certificate Database**.
3. To import the Root CA signer certificate to the database, on the **Signer Certificates** tab, click **Manage > Import**.

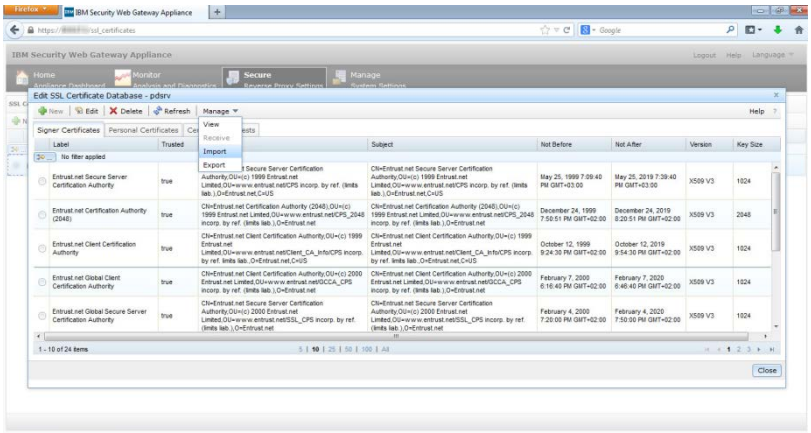

Figure 13: Importing the Root CA signer certificate

4. Click **Save**.

The configuration can now be deployed.

Running the Solution

After configuration is completed, the user can browse to the configured WebSEAL junction and authenticate using a certificate.

To authenticate to a protected web application:

1. Log in to the WebSEAL junction using SSL protocol. The **SAC Token Logon** dialog box opens.

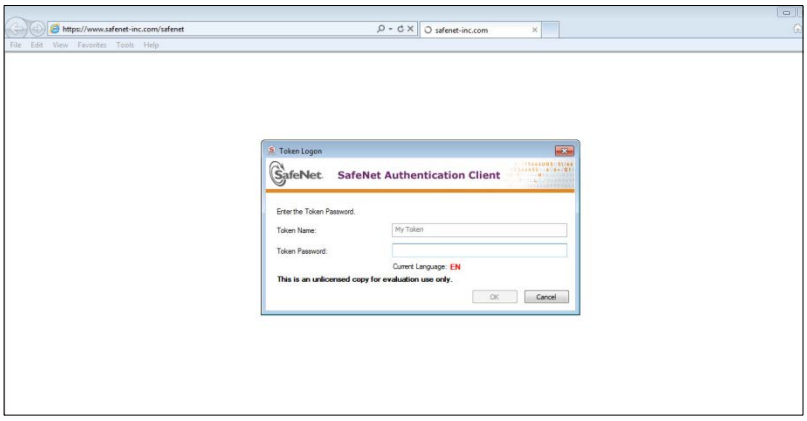

Figure 14: SAC Token Logon dialog box

2. Enter the token password. The user will authenticate to the protected web application.

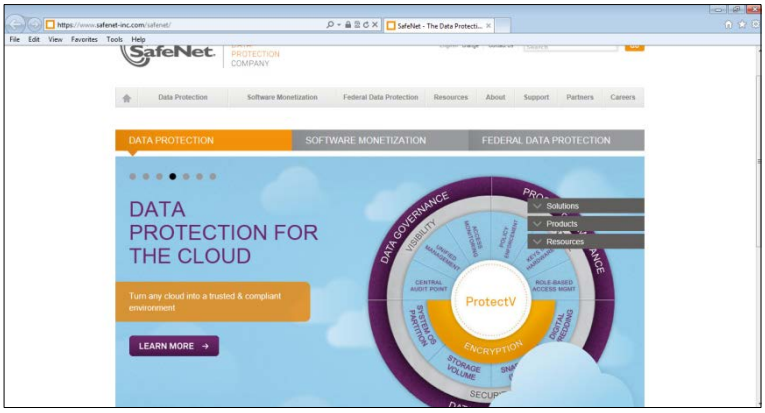

Figure 15: Protected web application after CBA