SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Lieberman RED Identity Management

gemalto
security to be free

Document Number: 007-013981-001, Rev. A

Release Date: October 2017

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Lieberman RED Identity Management.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SAC enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering security for web access, network logon, email, and data. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

Lieberman RED – Rapid Enterprise Defense™ Identity Management, formerly known as Enterprise Random Password Manager, is a Proactive Cyber Defense Platform. It protects organizations against malicious insiders, advanced persistent threats (APTs) and other sophisticated cyber-attacks – on-premises, in the cloud and in hybrid environments.

An effective strong authentication solution must be able to address data breaches on the rise for companies to protect their information assets and comply with privacy regulations. Data encryption is a common technique used by enterprises today, but to be most effective, it must be accompanied by strong two factor user authentication to desktop, mobile, and laptop computer applications. Working together, encryption and authentication reduce risk and stop unauthorized access to sensitive data.

SafeNet smart card certificate-based tokens and secure USB certificate-based tokens are interoperable with Lieberman RED Identity Management, providing a solution for encryption and strong access control that prevents unauthorized access to sensitive data and stops information loss and exposure. The integrated solution delivers greater security, reduced operational costs, and improved compliance by adding smart card-based strong user authentication to Lieberman RED Identity Management.

Gemalto's X.509 certificate-based USB tokens and smart cards have been integrated with Lieberman RED Identity Management, providing two-factor authentication at both pre-boot and Microsoft Windows levels.

The Gemalto's X.509 certificate-based USB tokens and smart cards provide secure storage for the certificates needed for endpoint encryption for Lieberman RED Identity Management functionality to boot up. If Gemalto's X.509 certificate-based USB token or smart card is not inserted in the client machine, or if the certificates are deleted, revoked, or expired, the Lieberman RED Identity Management software will not boot up and the data on the laptop will stay encrypted and secure.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Lieberman RED Identity Management using Gemalto tokens or smart cards.

It is assumed that the Lieberman RED Identity Management environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Lieberman RED Identity Management can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode—** SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- **SafeNet Authentication Client (SAC) IDGo800 Compatible mode—** IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

  For more details about different SAC installation modes, please refer to the Customization section in SafeNet Authentication Client Administrator Guide.
- **Lieberman RED Identity Management**

Environment

The integration environment that was used in this document is based on the following software versions:

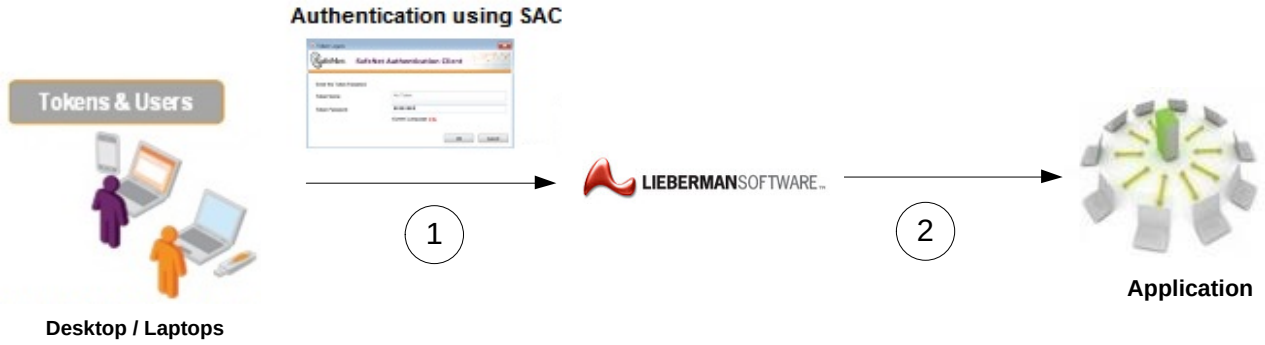
- **SafeNet Authentication Client (SAC)—** 10.4
- **Lieberman RED Identity Management—** 5.5.2.1

Audience

This document is targeted to system administrators who are familiar with Lieberman RED Identity Management, and are interested in adding multi-factor authentication capabilities during pre-boot using SafeNet tokens.

CBA Flow using SafeNet Authentication Client

1. The user attempts to connect to the Lieberman RED Identity Management server using a browser. The user inserts the SafeNet token, on which his certificate resides, and, when prompted, enters the token password.
2. After successful authentication, the user is allowed access to internal resources.



Prerequisites

To enable users to perform pre-boot authentication with Lieberman RED Identity Management using Gemalto tokens and smart cards, ensure the following:

- Users can authenticate through pre-boot from the Lieberman RED Identity Management environment with a static password before configuring the Lieberman RED Identity Management to use Gemalto tokens and smart cards.
- If SafeNet Authentication Manager (SAM) is used to manage the tokens, Token Policy Object (TPO) should be configured with MS CA connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users have a Gemalto token or smart card, enrolled with a valid certificate.
- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- SafeNet Authentication Client 10.4 must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client 10.4 supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830 rev B
- Gemalto IDPrime MD 840 rev B

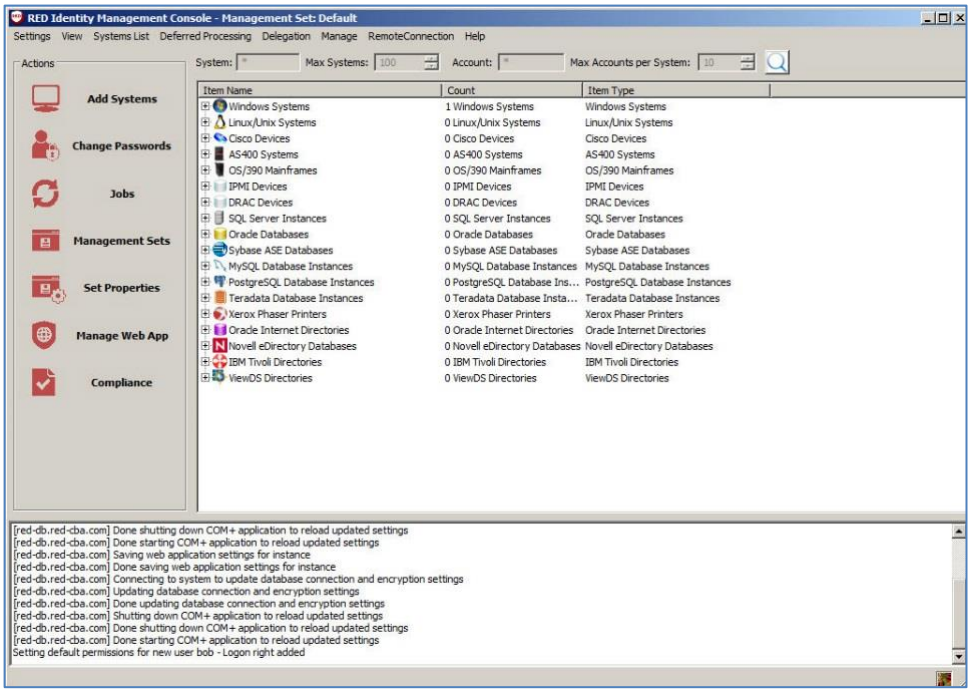
For a list of supported devices please refer to SafeNet Authentication Client Customer Release Notes.

Configuring Lieberman RED Identity Management

In our environment we used a Microsoft certificate authority. For a user to authenticate with a certificate, the certificate needs to be imported to the RED Identity management console.

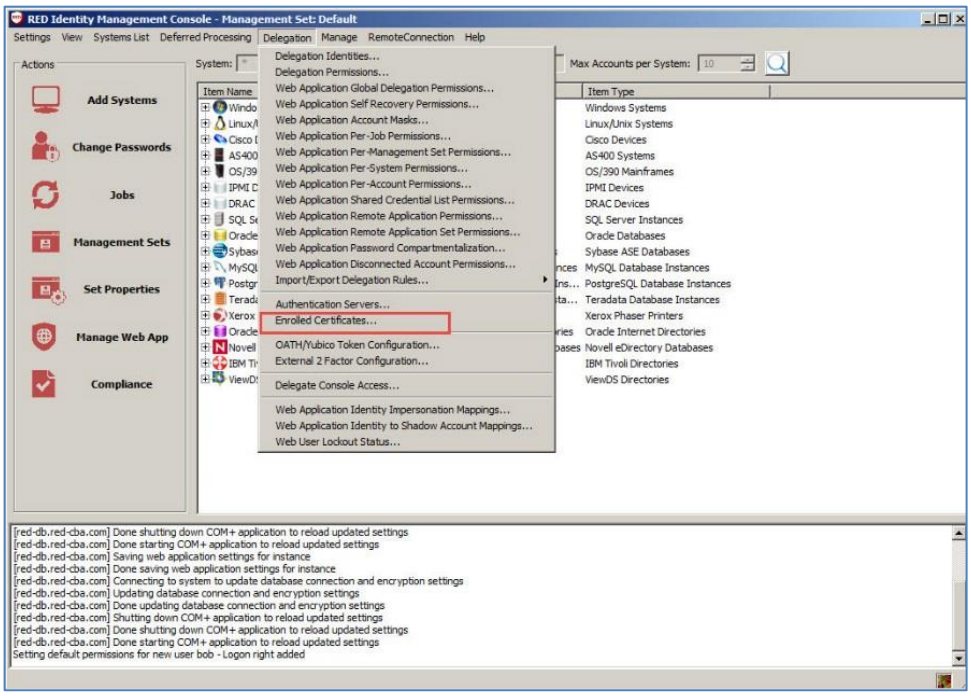
Importing User Certificate

1. Open the **RED Identity Management Console**.



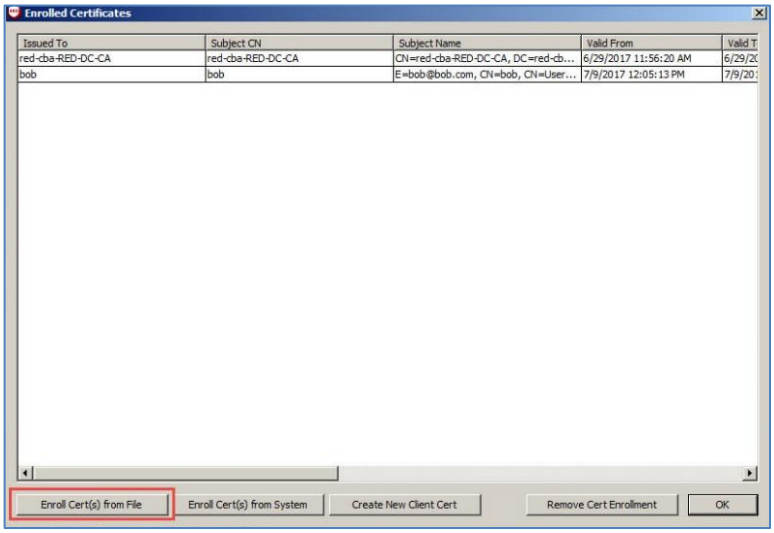
(The screen image above is from Lieberman Software Corporation®. Trademarks are the property of their respective owners).

2. Select **Delegation > Enrolled Certificates.**



(The screen image above is from Lieberman Software Corporation®. Trademarks are the property of their respective owners).

3. Click **Enroll Cert(s) from File.**

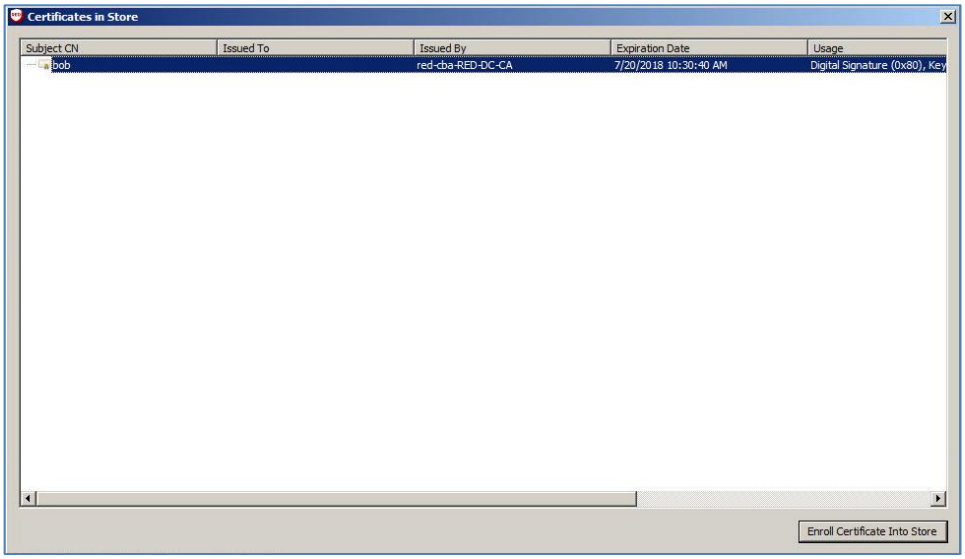


(The screen image above is from Lieberman Software Corporation®. Trademarks are the property of their respective owners).

4. Select the certificate file and click **Open**.

The certificate appears in the Certificate store window.

5. Click on the certificate and click **Enroll Certificate Into Store**.



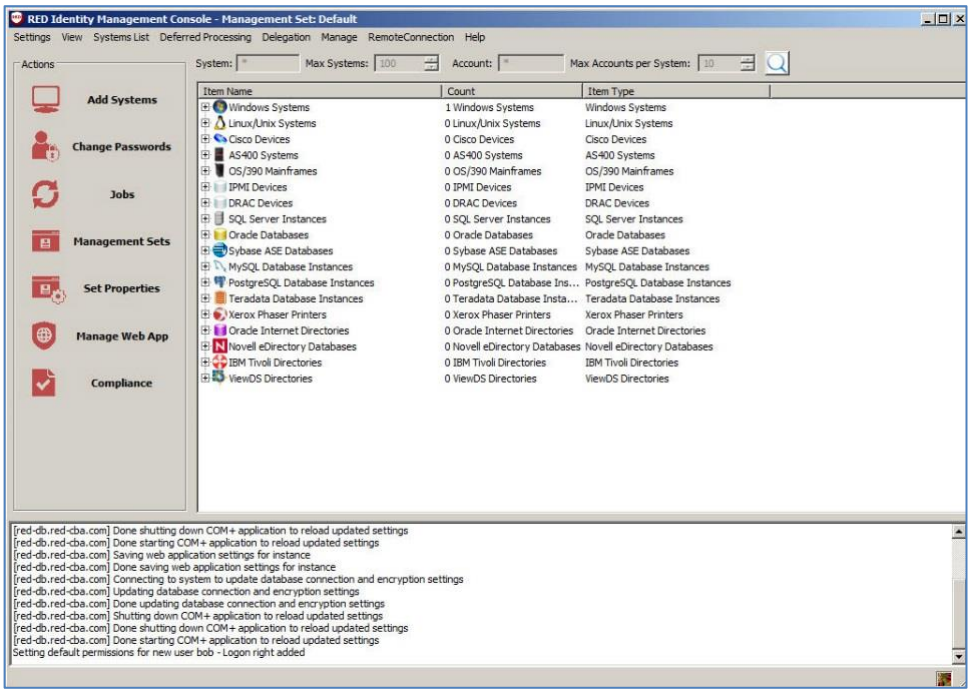
(The screen image above is from Lieberman Software Corporation®. Trademarks are the property of their respective owners).

6. Click **OK**.

Setting Delegation Identities

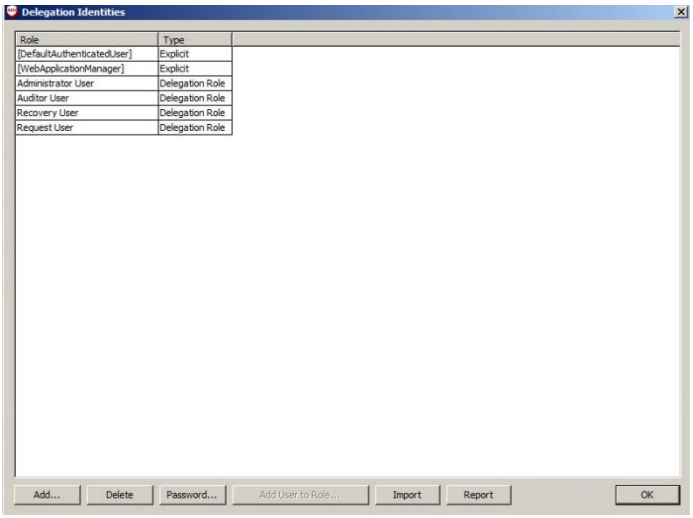
Next, we need to add the user to the delegation identities list to enable access the protected resource.

1. Open the **RED Identity Management Console.**



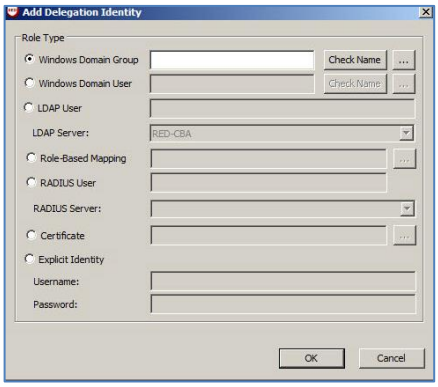
(The screen image above is from Lieberman Software Corporation®. Trademarks are the property of their respective owners).

2. Select **Delegation > Delegation Identities**.

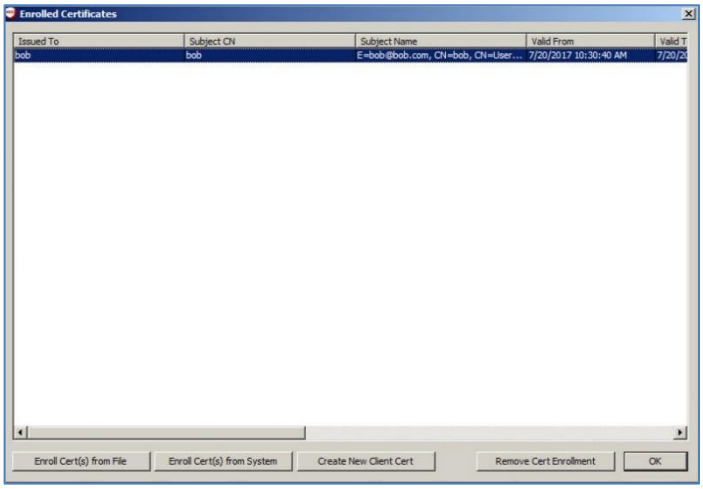


3. Click **Add**.

   The **Add Delegation Identity** window opens.



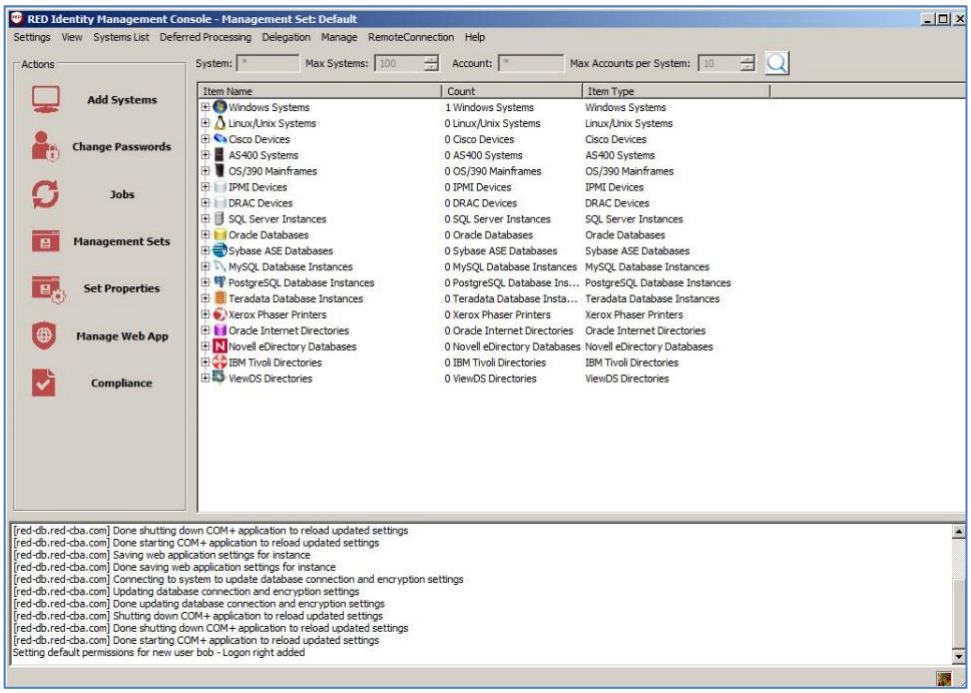
4. Select **Certificate** and click on the three dots button. The **Enrolled Certificates** window opens.
5. Select the user certificate and click **OK**.



6. On the **Add Delegation Identity** window click **OK,** and again, in the **Delegation Identities** window click **OK**.

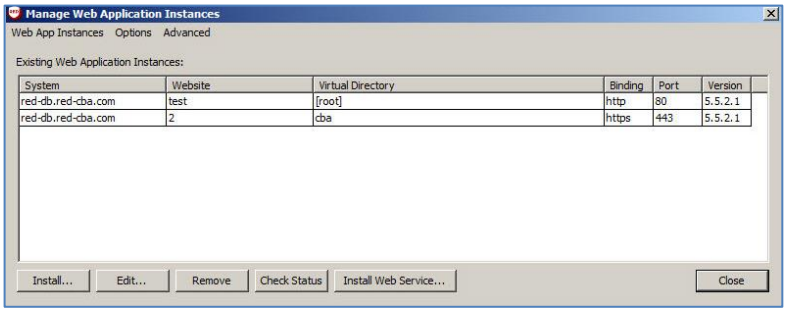
Configure Web Application for Certificate Authentication

1. Open the **RED Identity Management Console**.



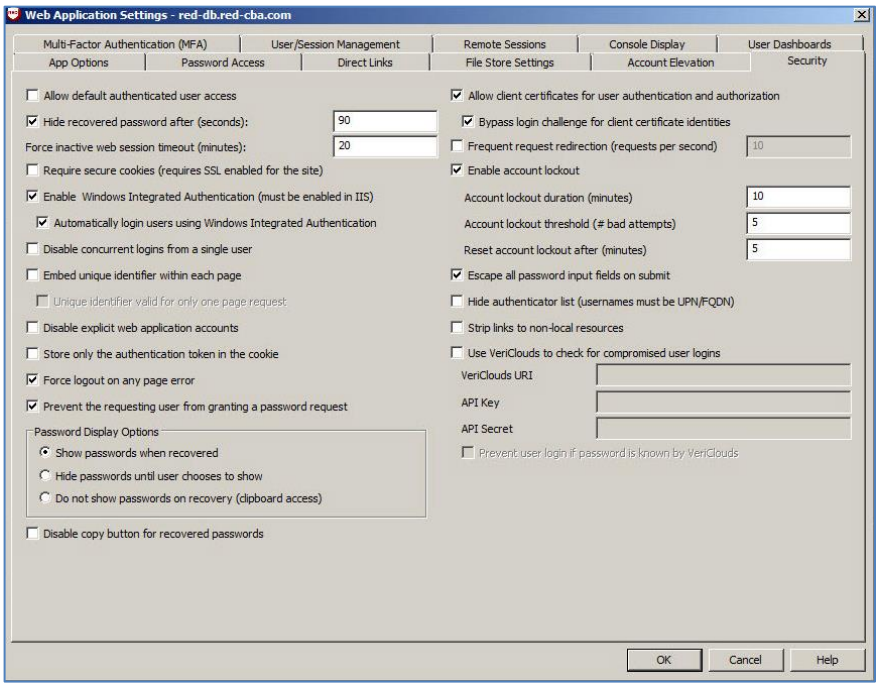
2. On the left pane, click **Manage Web App**.

   The **Manage Web Application Instances** window opens

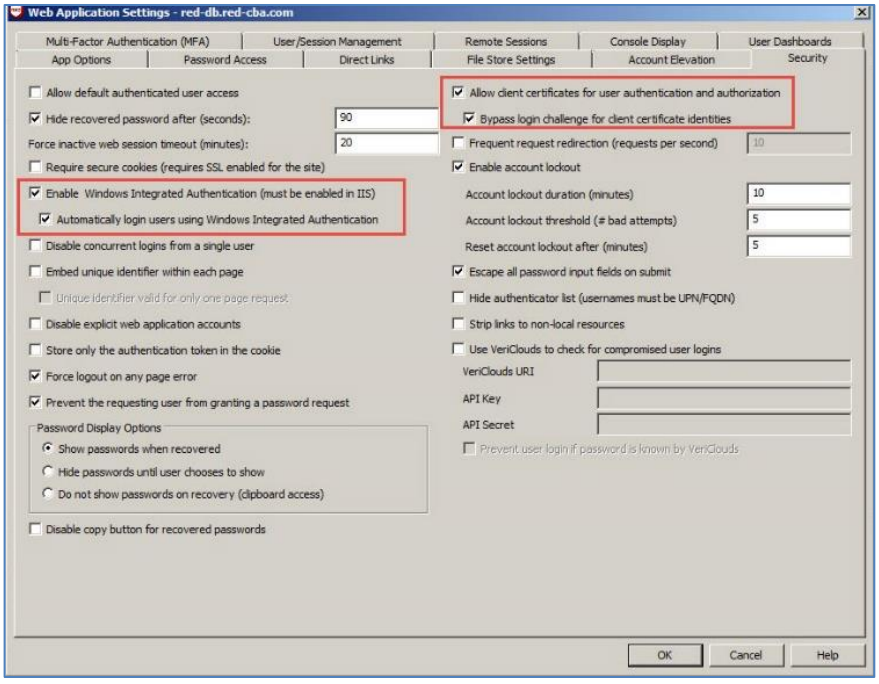


3. Select your web application instance and click **Edit.**

4. On the **Web Application Settings** window, select the **Security** tab.



5. Select the following options:
   a. **Enable Windows Integrated Authentication (must be enabled in IIS)**
   b. **Automatically login users using Windows Integrated Authentication**
   c. **Allow client certificates for user authentication and authorization**
   d. **Bypass login challenge for client certificate identities**



6. Click **OK.**
7. On the **Manage Web Application Instances** window, click **Close.**

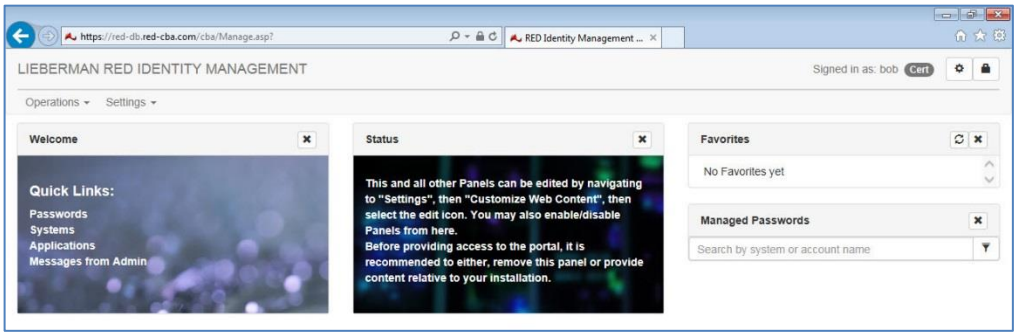
Running the Solution

In this section we will demonstrate certificate based authentication with SafeNet Authentication Client to a web app protected with Lieberman RED.

1. Start the client machine and insert the Gemalto token/smart card.
2. Open a web browser and access the protected web app. The **Confirm Certificate** window opens.
3. Select the certificate and click **OK**.

4. The **SafeNet Authentication Client Token Logon** window opens. Enter the token password and click **OK**.

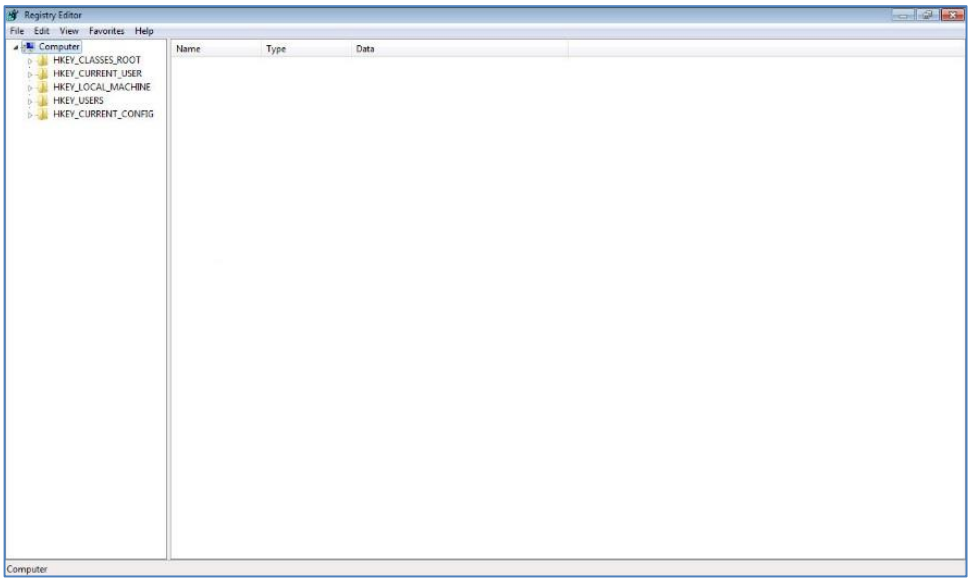
Upon successful authentication, the user is logged in to the protected resource.



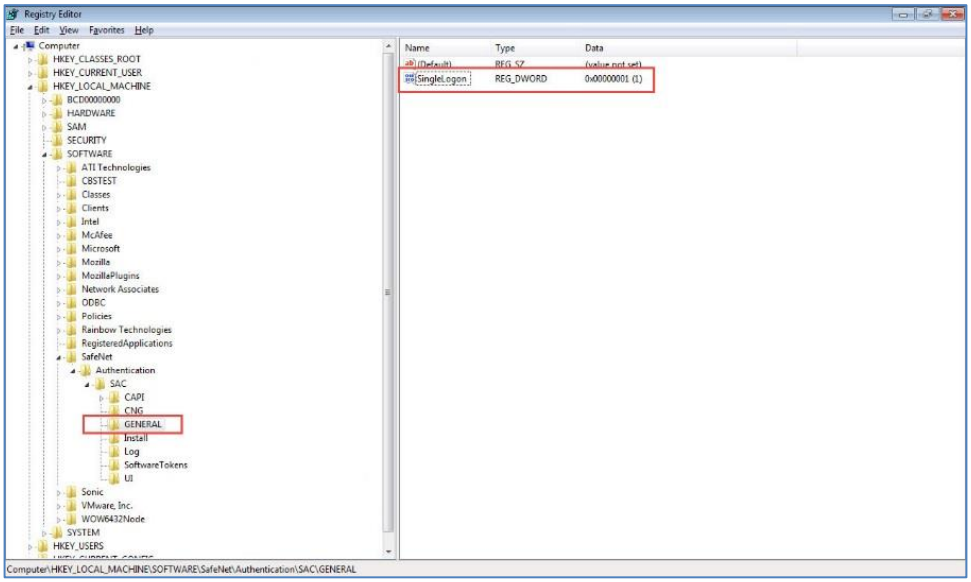
Configuring Smartcard Pass-through

To configure pass-through smart card authentication, configure the Registry Editor as follows.

1. Open the Registry editor: **regedit.exe** in **Administrator mode.**



2. On the left pane, go to: **HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC.**
3. Add a new Key: **General.**
4. Under **General** create a DWORD: **SingleLogon** with the value 1.



Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support.

Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.com, is a where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

NOTE: You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

Region	**Telephone number** (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Global	+1-410-931-7520
Australia	1800.020.183
China	North: 10800-713-1971 South: 10800-1301-932
France	0800-912-857
Germany	0800-181-6374
India	000.800.100.4290
Israel	180-931-5798
Italy	800-786-421
Japan	0066 3382 1699

Region	Telephone number (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
Korea	+82 2 3429 1055
Netherlands	0800.022.2996
New Zealand	0800.440.359
Portugal	800.863.499
Singapore	800.1302.029
Spain	900.938.717
Sweden	020.791.028
Switzerland	0800.564.849
United Kingdom	0800.056.3158
United States	(800) 545-6608