

# SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for VMware vCenter Server 6.5  
vSphere Web Client

All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2018 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Number:** 007-014050-001, Rev. A

**Release Date:** January 2018

# Contents

Third-Party Software Acknowledgement .....	4
Description .....	4
Applicability .....	5
Environment.....	5
Audience .....	5
Authentication Flow.....	6
Prerequisites .....	6
Supported Tokens and Smart Cards in SafeNet Authentication Client .....	7
Configuring vCenter Server .....	7
Running the Solution .....	11
Support Contacts .....	15
Customer Support Portal.....	15
Telephone Support.....	15

# Third-Party Software Acknowledgement

---

This document is intended to help users of Gemalto products when working with third-party software. In this case, VMware vCenter Server 6.5 VSphere Web Client.

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.

An effective strong authentication solution must be able to address ever more frequent data breaches to enable 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 the risk of unauthorized access to sensitive data.

SafeNet smart card certificate-based tokens and secure USB certificate-based tokens are interoperable with VMware vCenter Server 6.5 VSphere Web Client, 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 VMware vCenter Server 6.5 VSphere Web Client.

Gemalto's X.509 certificate-based USB tokens and smart cards have been integrated with VMware vCenter Server 6.5 VSphere Web Client, 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 VMware vCenter Server 6.5 VSphere Web Client functionality to boot up. If Gemalto's X.509 certificate-based USB token or smart card is not inserted into the client machine, or if the certificates are deleted, revoked, or expired, the VMware vCenter Server 6.5 VSphere Web Client 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 VMware vCenter Server 6.5 VSphere Web Client using Gemalto tokens or smart cards.

It is assumed that the VMware vCenter Server 6.5 VSphere Web Client environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

VMware vCenter Server 6.5 VSphere Web Client 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, using Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards. For more details about different SAC installation modes, refer to the SafeNet Authentication Client Administration Guide.

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

## Environment

---

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

- **SafeNet Authentication Client (SAC)** - SAC 10.4 Post GA
- **VMware vCenter Server 6.5 Update 1b** – installed on Windows server 2012R2
- **Windows Server 2008R2** – installed with Active Directory, Certificate Authority.
- **Win 7 x32/x64** – Domain Joined using IE 11.

## Audience

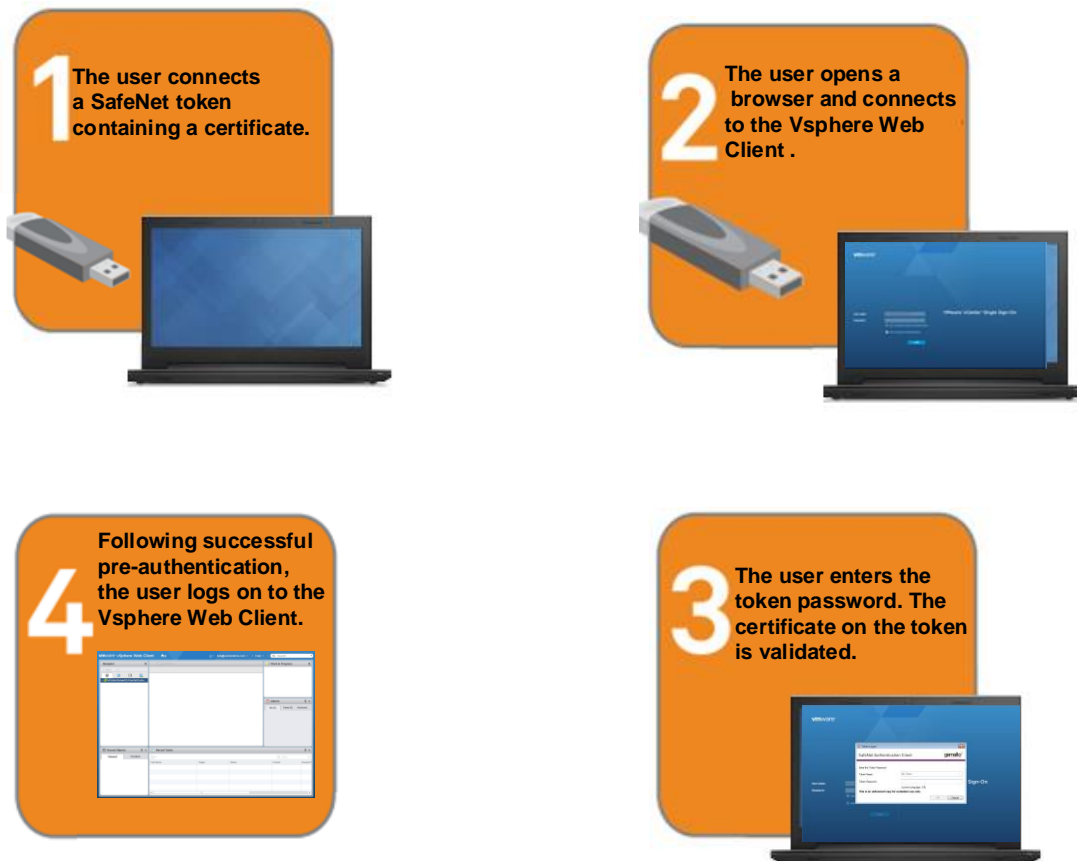
---

This document is targeted to system administrators who are familiar with VMware vCenter Server 6.5 VSphere Web Client, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

# Authentication Flow

---

The diagram below illustrates the flow of certificate-based authentication to vSphere Web Client:



## Prerequisites

---

To enable users to perform pre-boot authentication with VMware vCenter Server 6.5 vSphere Web Client using Gemalto tokens and smart cards, ensure the following:

- Users can authenticate the VMware vCenter Server 6.5 vSphere Web Client environment with a static password before configuring 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 valid certificate.
- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Any CA can be used. In this guide, integration is demonstrated using Microsoft CA.
- SafeNet Authentication Client (SAC 10.4) must be installed on all client machines.

# Supported Tokens and Smart Cards in SafeNet Authentication Client

---

SafeNet Authentication Client (SAC 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
- Gemalto IDPrime MD 840

For all supported devices please refer to *SafeNet Authentication Client Customer Release Notes*.

# Configuring vCenter Server

---

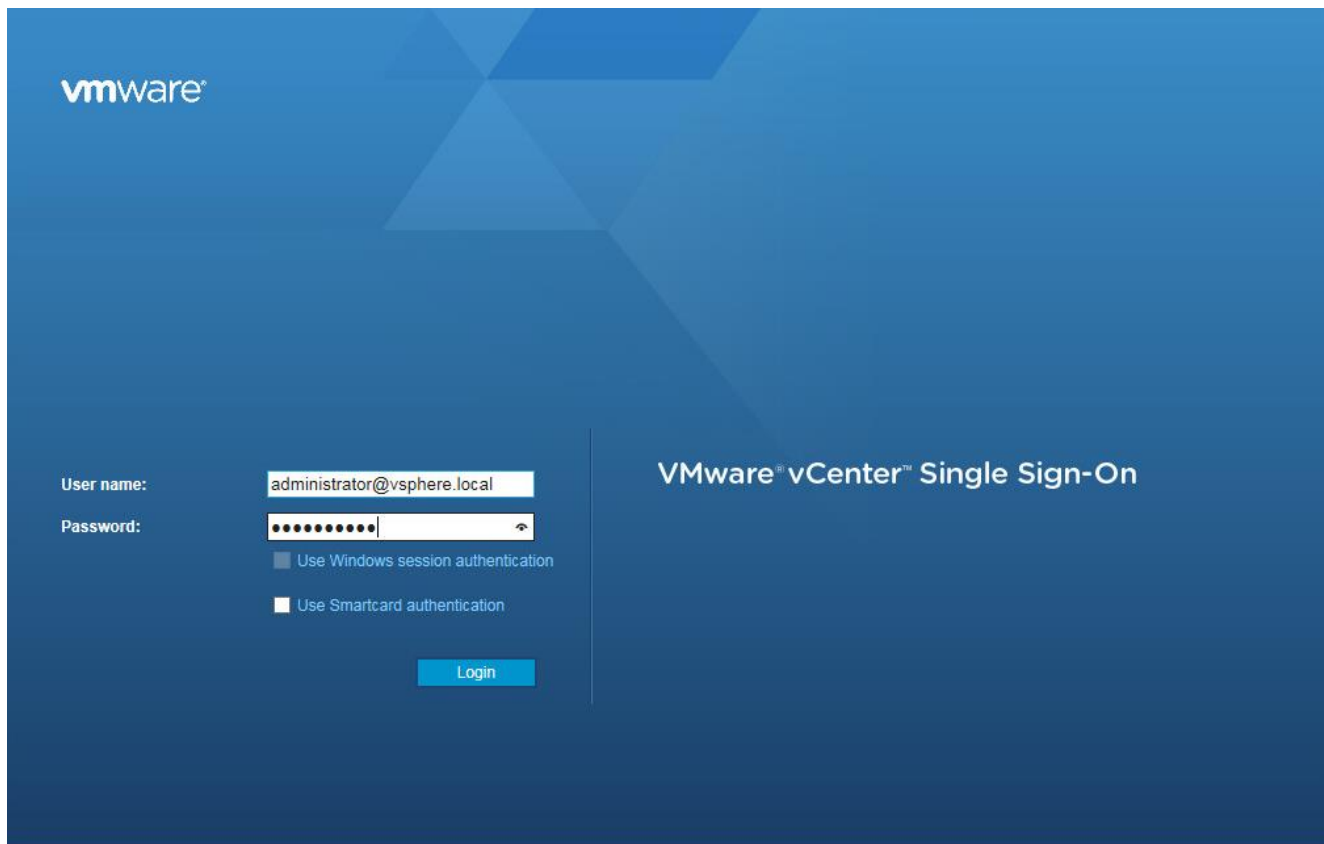
Complete the procedures in this section to configure CBA Authentication for two-factor authentication so users can authenticate using certificates on their smart cards or Tokens.

## Prerequisites:

- Platform Services Controller Web interface certificate is trusted by the end user's workstation
- Active Directory identity source is added to vCenter Single Sign-On as an identity source
- In the vCenter Server, assign the required role permissions to one or more users in the Active Directory identity source.

## Configure the Platform Services Controller

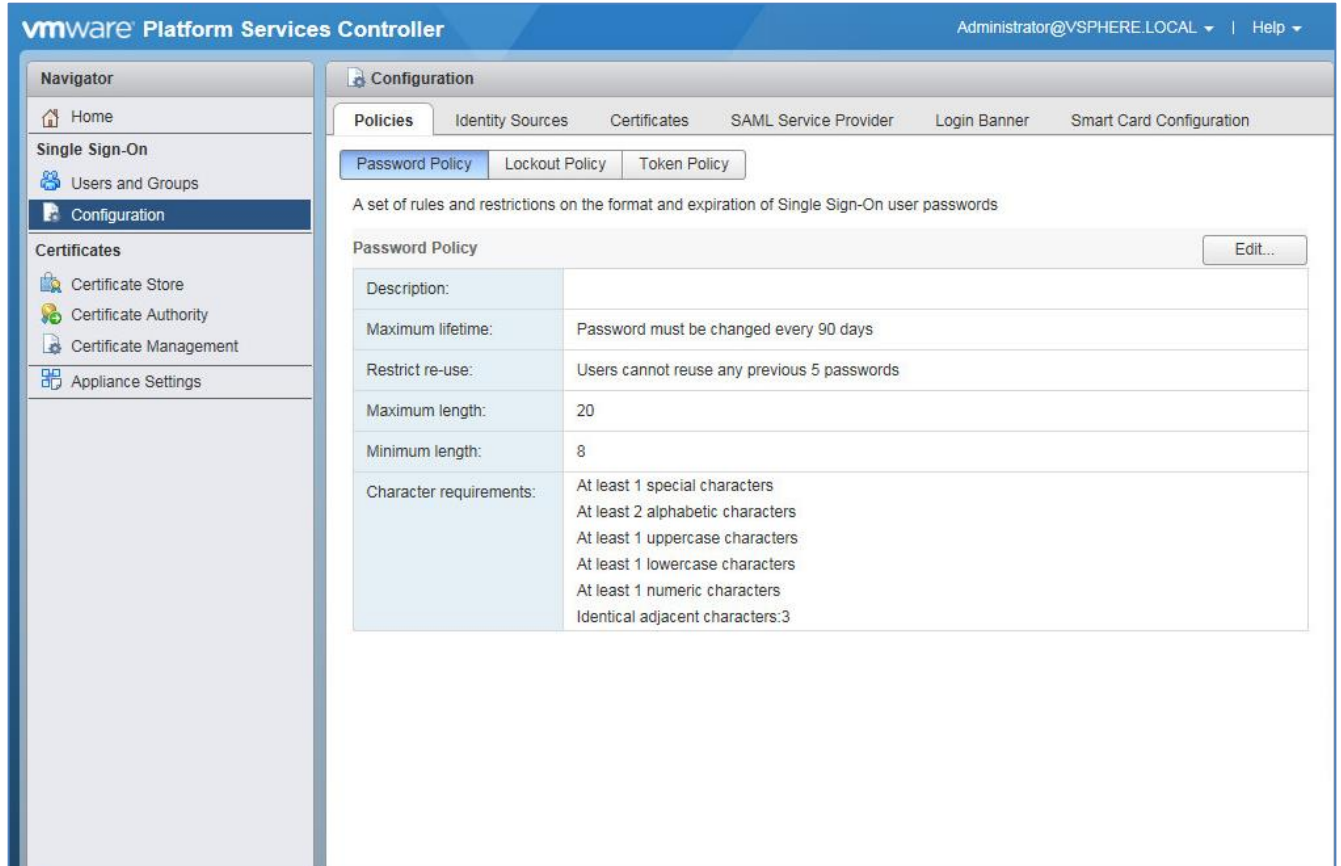
1. Open and login to the **Platform Services Controller** using web browser URL:  
**https://psc\_hostname\_or\_IP/psc**



*(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)*

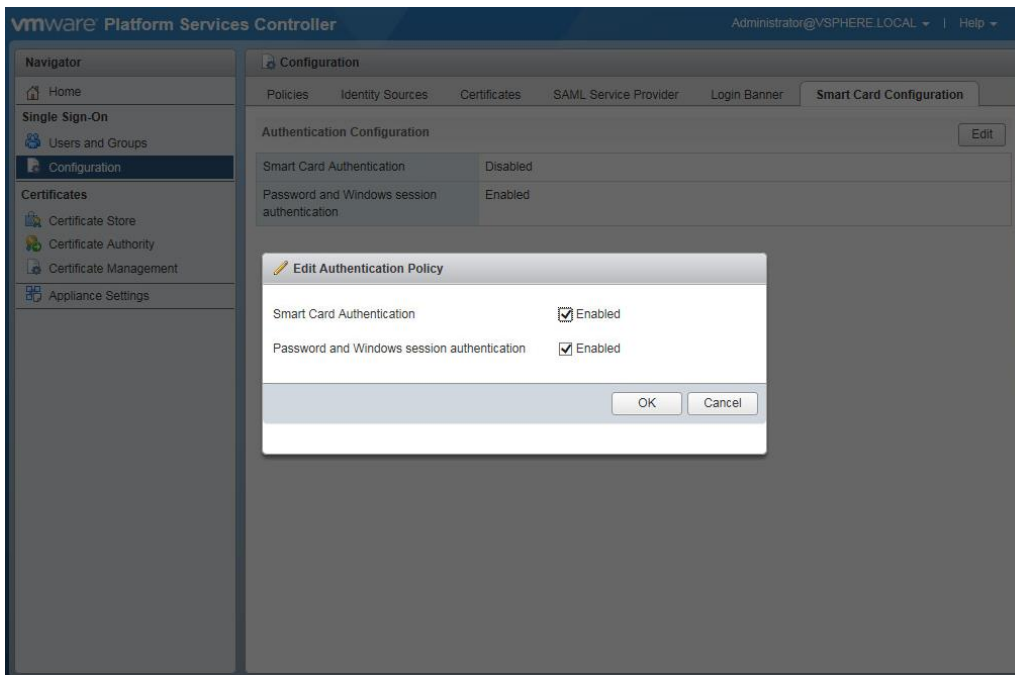


2. Navigate to **Single Sign-On > Configuration**.



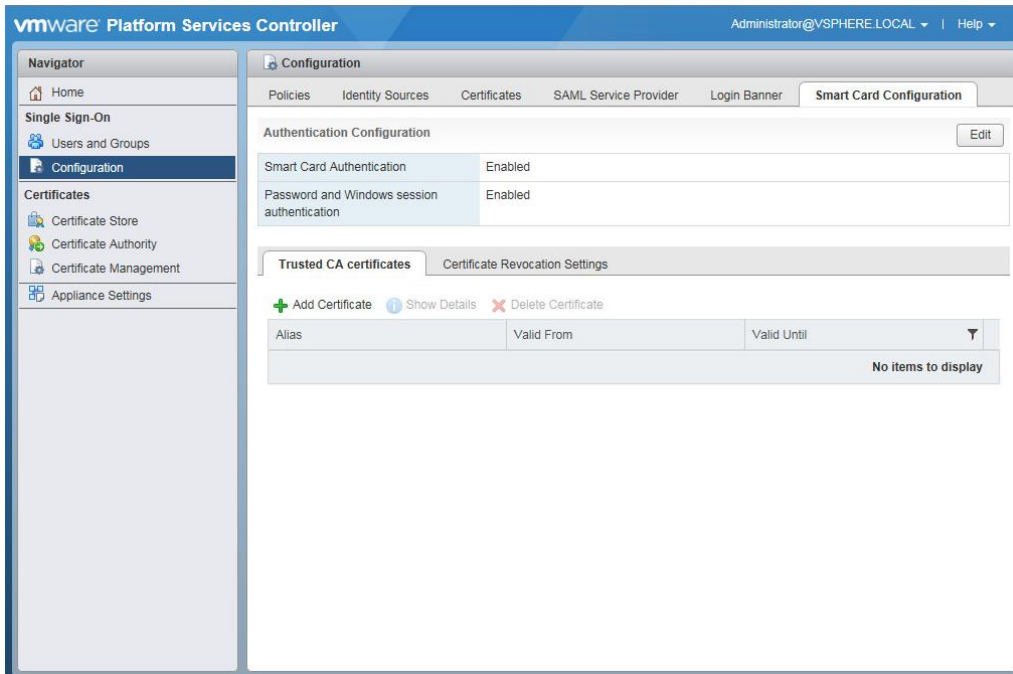
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

3. Select the **Smart Card Configuration** tab, click **Edit** and select **Smart Card Authentication Enabled**, then click **OK**.



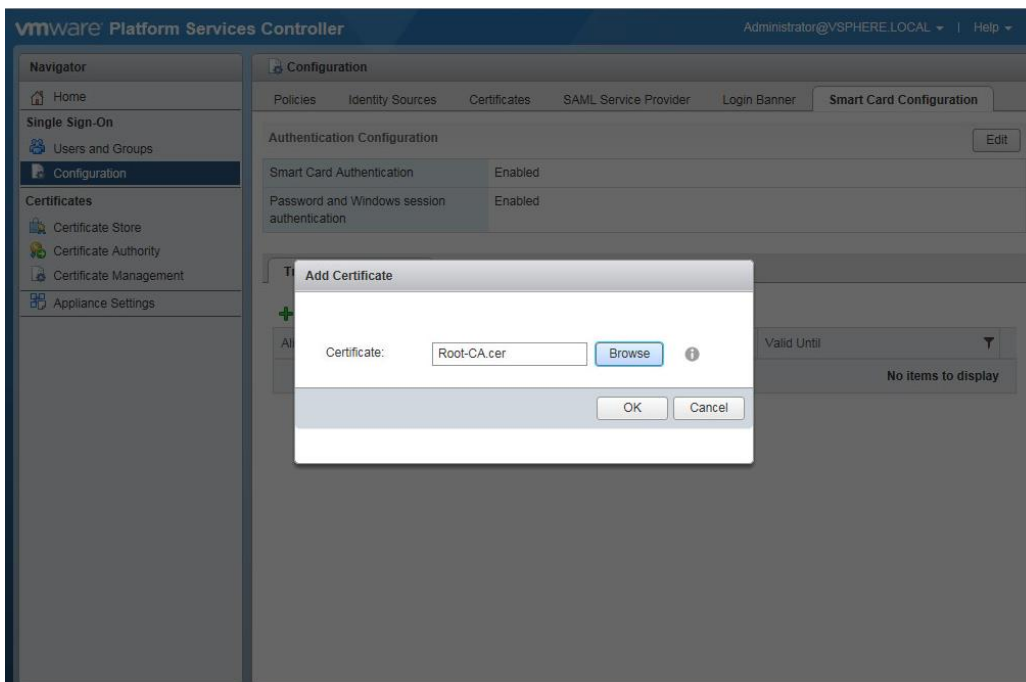
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

4. Select the **Trusted CA certificates** tab.



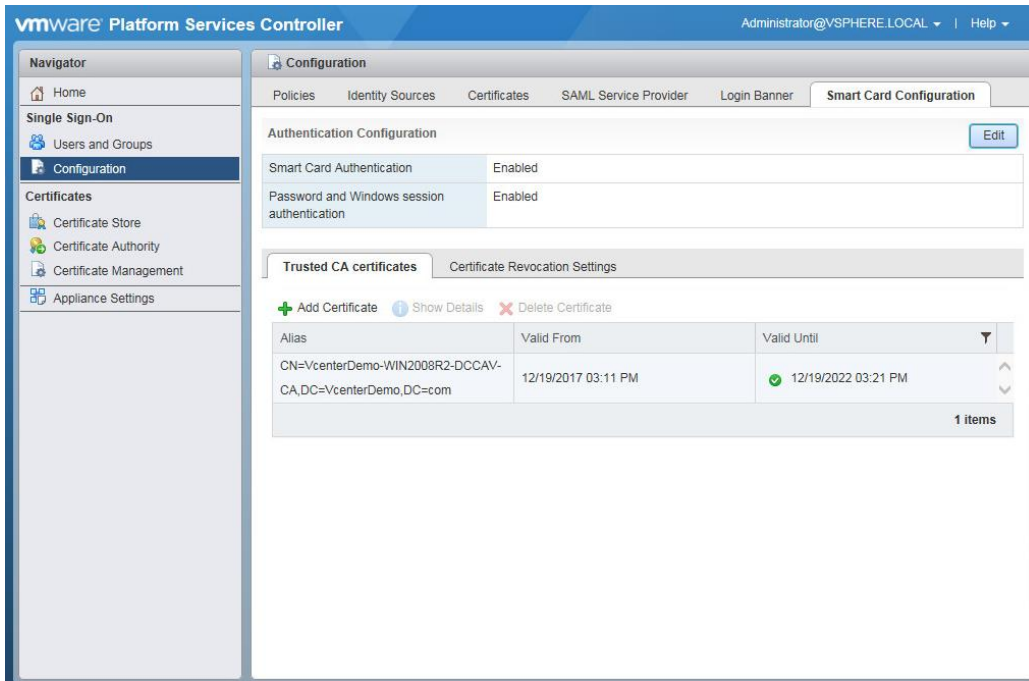
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

5. Click **Add Certificate**, click **Browse**, select a certificate from a trusted CA, and click **OK**.



(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

The trusted CA is added.



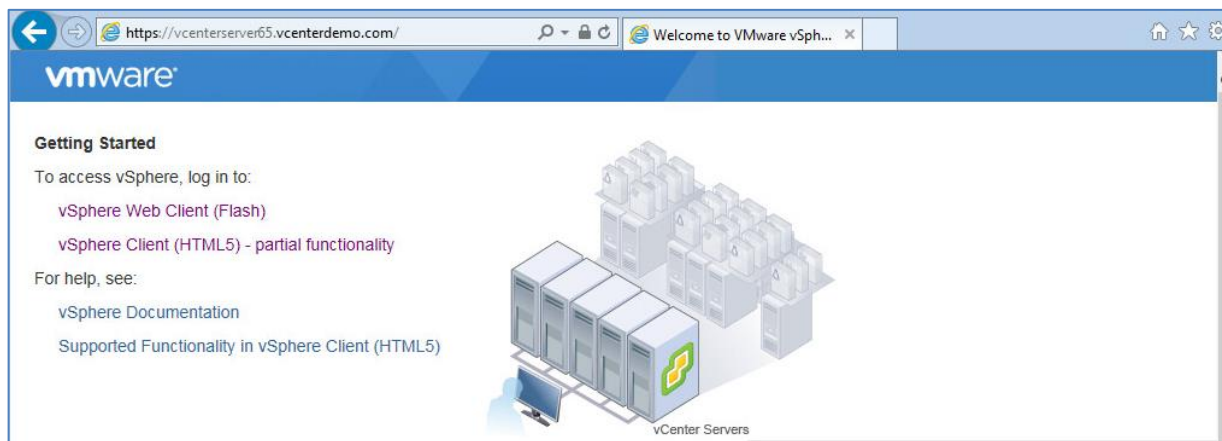
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

## Running the Solution

In this example Win 7x64 is demonstrated

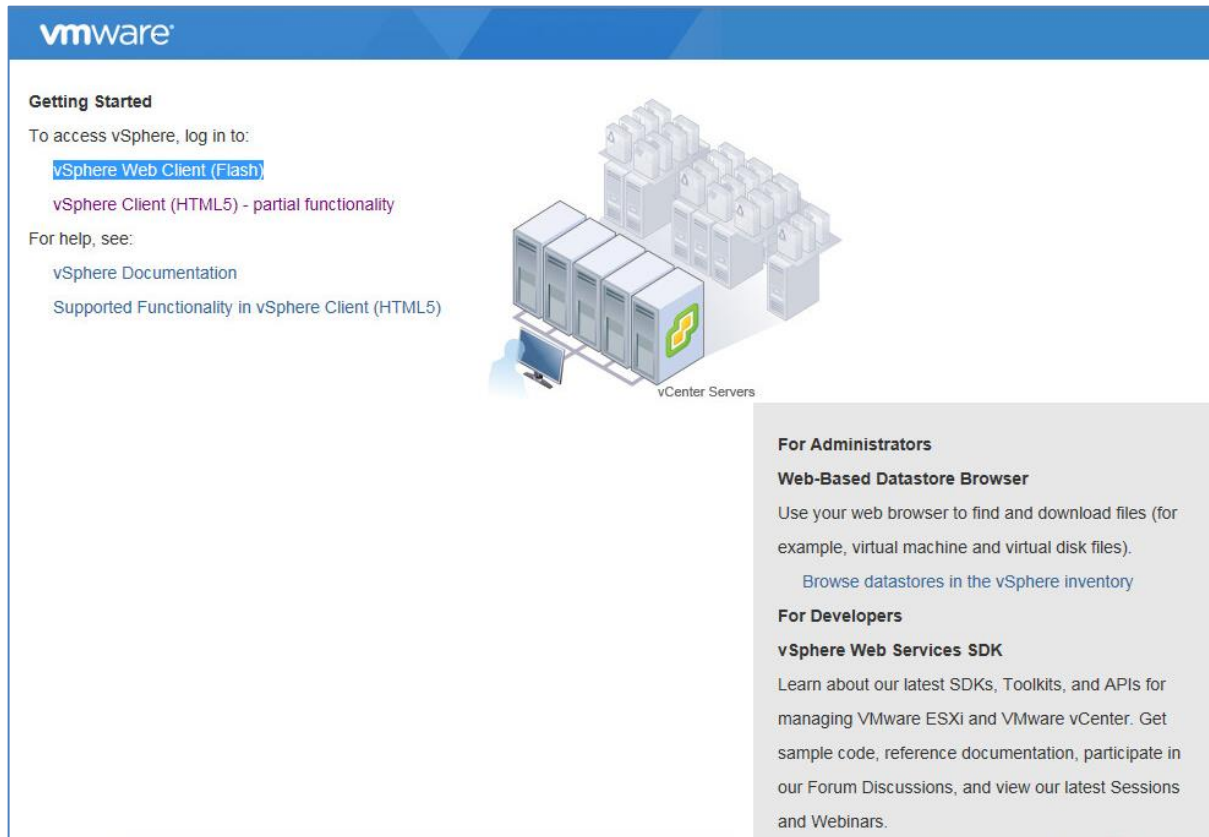
To enroll a Smartcard User certificate on the Smart Card/Token:

1. Connect the token.
2. Browse to the vSphere server web address



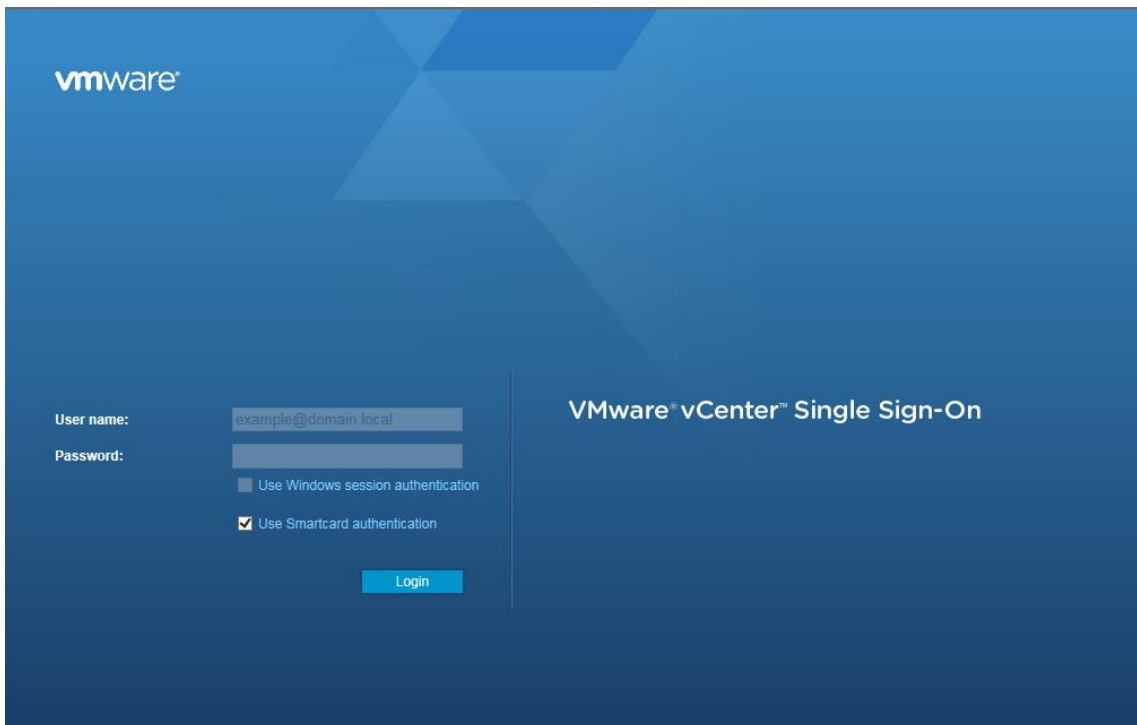
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

3. Click **VSphere Web Client**



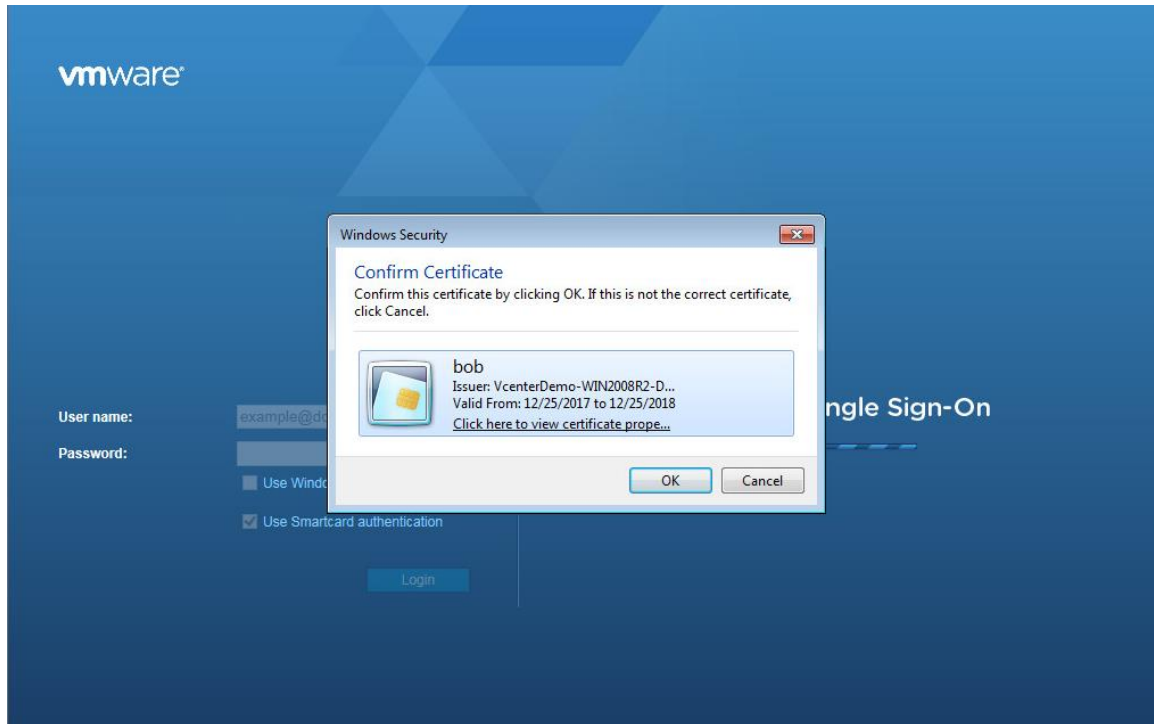
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

4. Select **Use Smartcard authentication** and click **Login**.



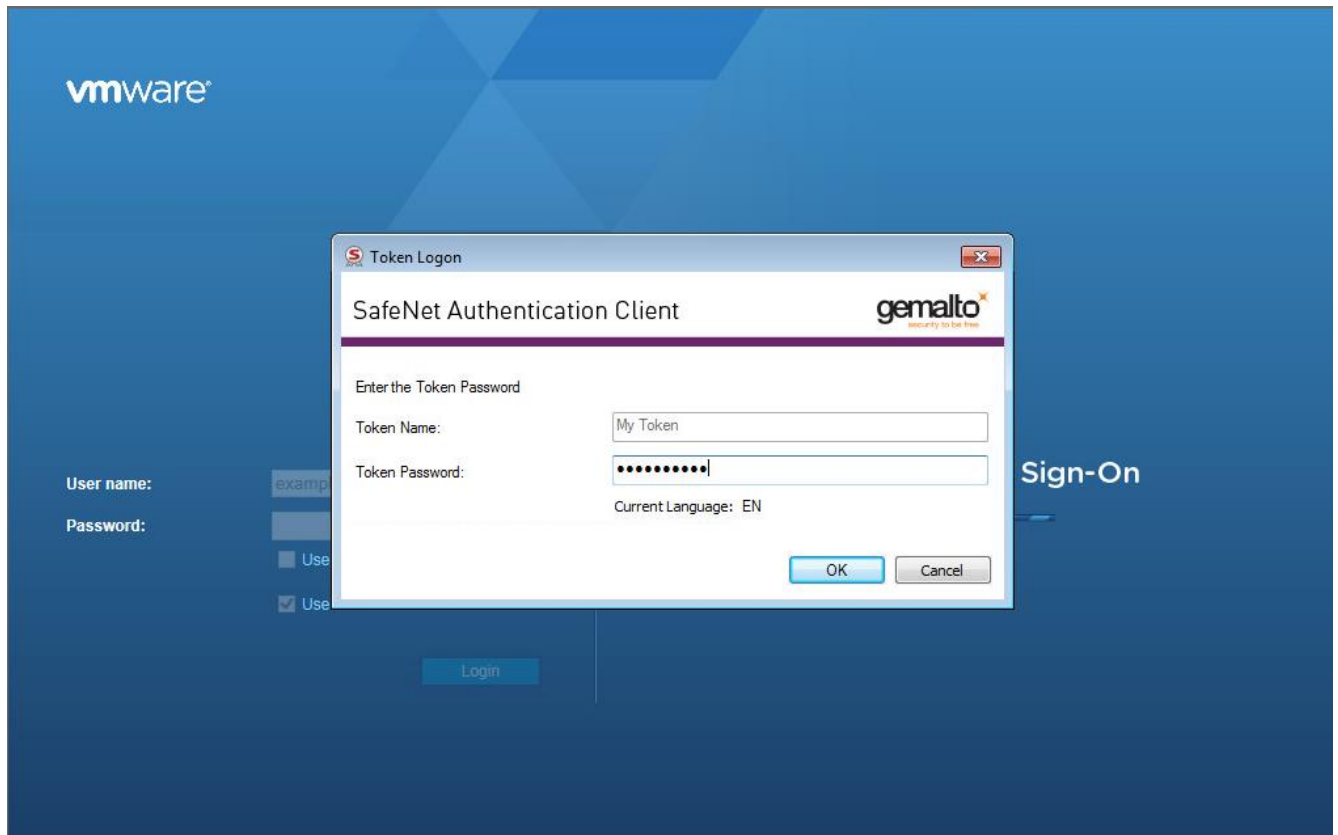
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

5. In the **Confirm Certificate** window, click **OK**.



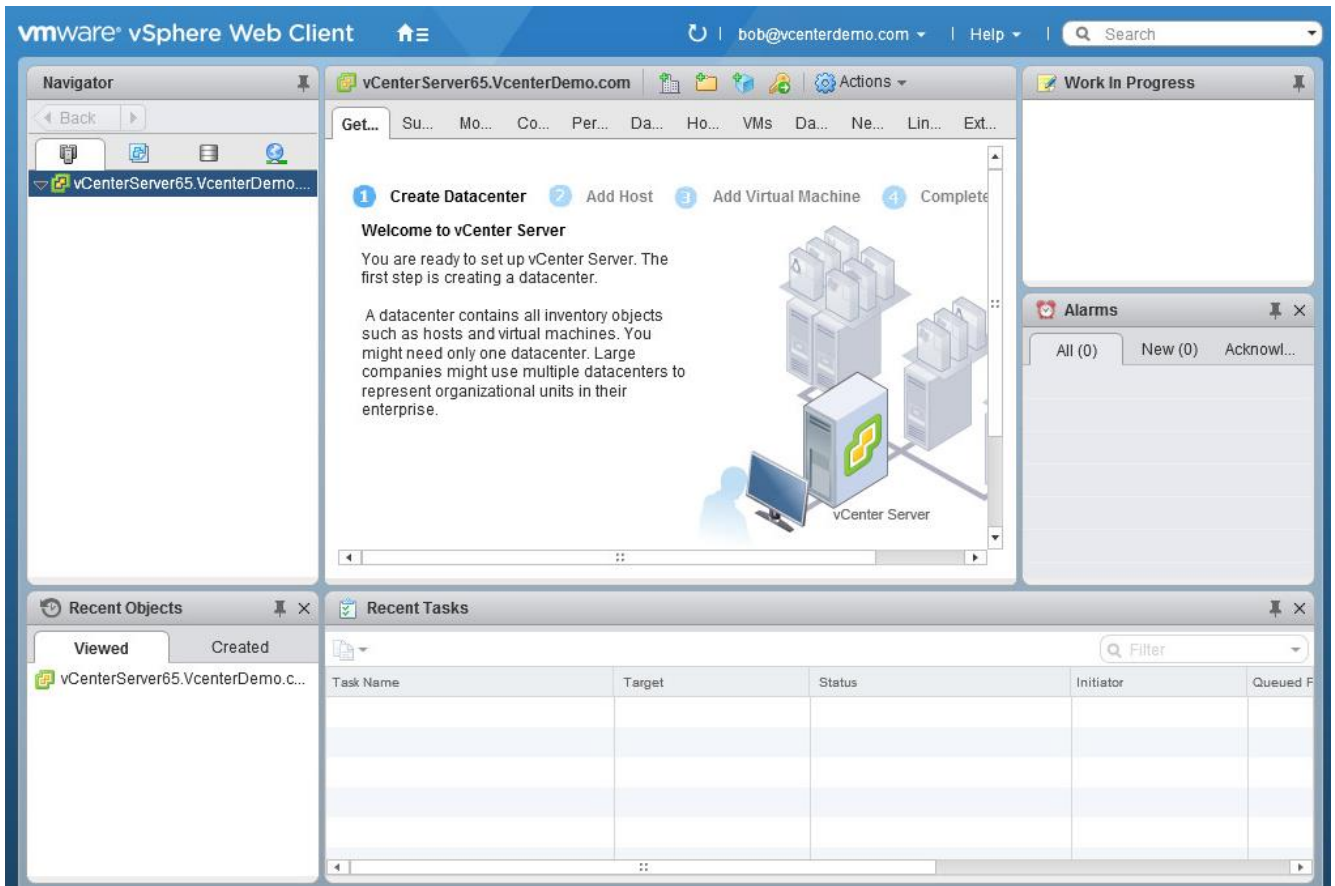
(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

6. In the **Token Logon** window, enter smart card credentials and click **OK**.



(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

The user is connected.



(The screen image above is from VMware® software. Trademarks are the property of their respective owners.)

# 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
Korea	+82 2 3429 1055

<b>Region</b>	<b>Telephone number</b> (Subject to change. An up-to-date list is maintained on the Customer Support Portal)
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