WHITE PAPER

vCenter Smart Card Authentication Configuration Guide

Version 7.0

vmware®

Contents

Overview 3
- Summary 3
- Requirements 3
- Browser Support 3
- ADFS Smart Card Support 3
- Future Smart Card Support 3
- vCenter 7.0 Update 2 FIPS Support 3

Smart Card Login Process Overview 4
Enabling Smart Card Authentication 4
- Configure the Reverse Proxy to Request Client Certificates 4
- Configure Smart Card Authentication from the UI 5

Advanced Configuration Options 8
- (Optional) Advanced OCSP/CRL Configuration 8
- (Optional) Add all DoD Trusted Certificates to the trust store 8
- (Optional) Restore password authentication 8

Frequently Asked Questions 9

Overview

Summary

The focus of this document is the configuration of certificate-based or Smart Card authentication in vCenter 7.0. This feature is biased towards Department of Defense Common Access Card (CAC) implementations but may fit other environments as well. This document will not describe how to implement PKI or ADFS, only how to integrate vCenter into an existing PKI environment.

Requirements

This deployment assumes that an enterprise PKI has been deployed. The end user is responsible for having the necessary tokens/cards and middleware so their certificate can be presented to the browser. The certificate selected by the user for authentication must meet the following requirements:

- The certificate will need to have a User Principal Name (UPN) in the Subject Alternative Name (SAN) extension. The UPN needs to correspond to an active directory account.
- The certificate will need to have "Client Authentication" as one of the "Application Policy" or "Enhanced Key Usage" purposes. If the certificate does not have this usage, then it will not be selected by the browser for authentication.
- Add an Active Directory identity source to vCenter Single Sign-On.

Browser Support

Supported browsers for certificate-based authentication.

- Google Chrome 75 or later
- Microsoft Edge 79 or later
- Firefox is not supported without additional plugins.

ADFS Smart Card Support

In addition to the built-in capability vCenter 7.0 now supports Identity Provider Federation which enables you to configure an external identity provider for federated authentication. In this configuration, the external identity provider interacts with the identity source on behalf of vCenter Server.

In this scenario, when a user logs in to vCenter Server, vCenter Server redirects the user login to the external identity provider. The user credentials are no longer provided to vCenter Server directly. Instead, the user provides credentials to the external identity provider. vCenter Server trusts the external identity provider to perform the authentication. In the federation model, users never provide credentials directly to any service or application but only to the identity provider. As a result, you "federate" your applications and services, such as vCenter Server, with your identity provider.

Currently only Active Directory Federation Services is supported with Identity Provider Federation, but other providers will be supported in the future.

As an alternative to configuring the native smart card support, meeting this requirement through ADFS when configured as the identity provider for vCenter is also acceptable.

Future Smart Card Support

In a future vSphere release, VMware plans to discontinue support for Windows Session Authentication (SSPI), Common Access Card (CAC), and RSA SecurID for vCenter Server. In place of SSPI, CAC, or RSA SecurID, users and administrators can configure and use Identity Federation with a supported Identity Provider to sign in to their vCenter Server system.

vCenter 7.0 Update 2 FIPS Support

Starting in vSphere 7.0 Update 2, you can enable FIPS on vCenter Server. RSA SecureID and CAC authentication are not supported when FIPS is enabled. Use external identity provider federation for MFA authentication.

Smart Card Login Process Overview

Users who log in to a vCenter Server system are prompted to authenticate with a smart card and PIN combination, as follows.

1. When a user inserts the smart card into the smart card reader, the browser reads the certificates on the card.
2. The browser prompts the user to select a certificate, then prompts the user for the PIN for that certificate.
3. vCenter Single Sign-On checks whether the certificate on the smart card is known. If revocation checking is turned on, vCenter Single Sign-On also checks whether the certificate is revoked.
4. If the certificate is known to vCenter Single Sign-On, and is not a revoked certificate, the user is authenticated and can perform tasks for which that the user has permissions.

Enabling Smart Card Authentication

The following steps configure the smart card feature inside of SSO. This change replicates across PSCs or linked vCenter instances and therefore only needs to be done in one place.

Configure the Reverse Proxy to Request Client Certificates

1. Login to the vCenter shell as the root user.
2. Create a trusted client CA store.

   This store contains the trusted issuing CA's certificates for client certificate. The client here is the browser from which the smart card process prompts the end user for information.

   The following example shows how you create a certificate store on the vCenter Server.

   Note the file clienttrustCA.pem does not exist by default and is created by running this command.

   To create this file the first time run the following command:

```
# openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

   To append another certificate to an already created file run the following command:

```
# openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

3. Make a backup of the /etc/vmware-rhttpproxy/config.xml file then open config.xml in a text editor.
4. Find the http section and make the following changes to and save the updated file.

Updated Configuration – Note - the comments have been removed for readability.

```
<http>
  <maxConnections> 2048 </maxConnections>
  <requestClientCertificate>true</requestClientCertificate>
  <clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
  <clientCertificateMaxSize>4096</clientCertificateMaxSize>
</http>
```

Default configuration in 7.0 U2

```
<http>
  <!-- Num of max proxy connections -->
  <maxConnections> 2048 </maxConnections>
  <!-- CA file, needed to scan all certificates in it and list them as acceptable CAs: -->
  <!-- <clientCAListFile>rootcerts.pem</clientCAListFile> -->
  <!-- Maximum size of a client certificate in case it is requested. -->
  <!-- <clientCertificateMaxSize>4096</clientCertificateMaxSize> -->
</http>
```

5. Restart the reverse proxy service by running the following command:

```
# /usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy
```

Configure Smart Card Authentication from the UI

1. Login to the vCenter Server UI as an administrative user.
2. Navigate to Menu > Administration > Single Sign On > Configuration > Identity Provider > Smart Card Authentication

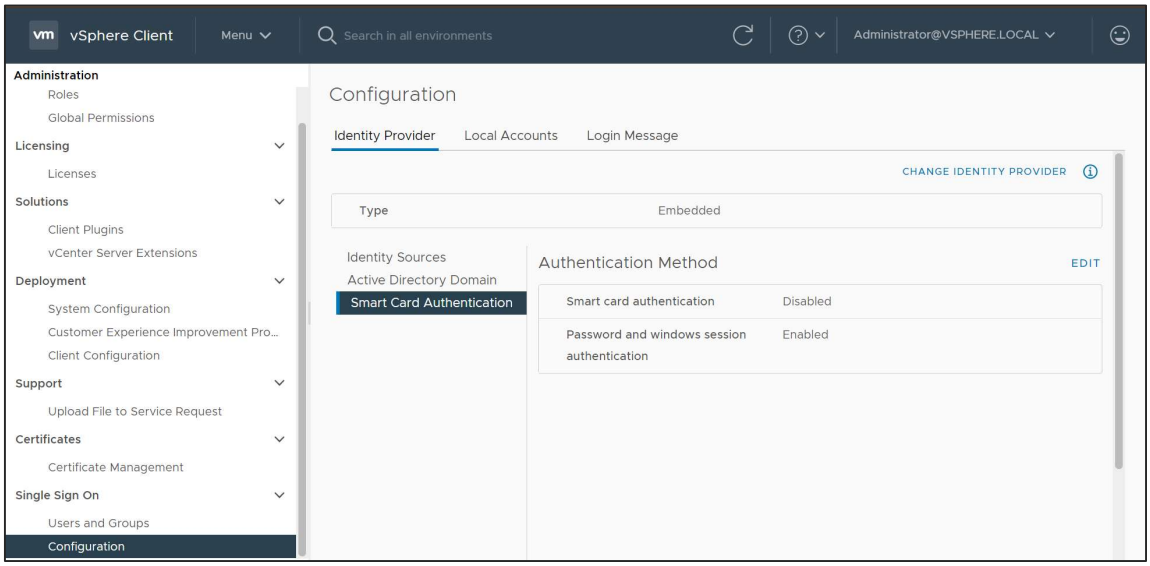

Figure 1: *UI Smart Card Configuration Menu*

3. Click the Edit button and select "Enable smart card authentication" to only allow smart card logins or "Enable both options" to allow smart card and username/password logins.

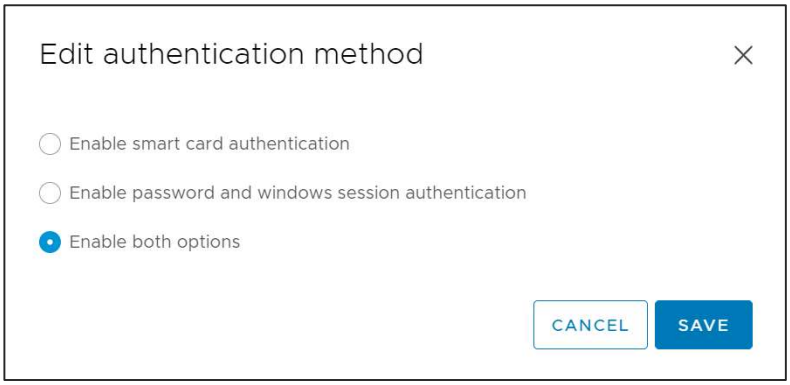

Figure 2: *Smart card enablement options*

4. Once enable additional options will now appear in the UI.

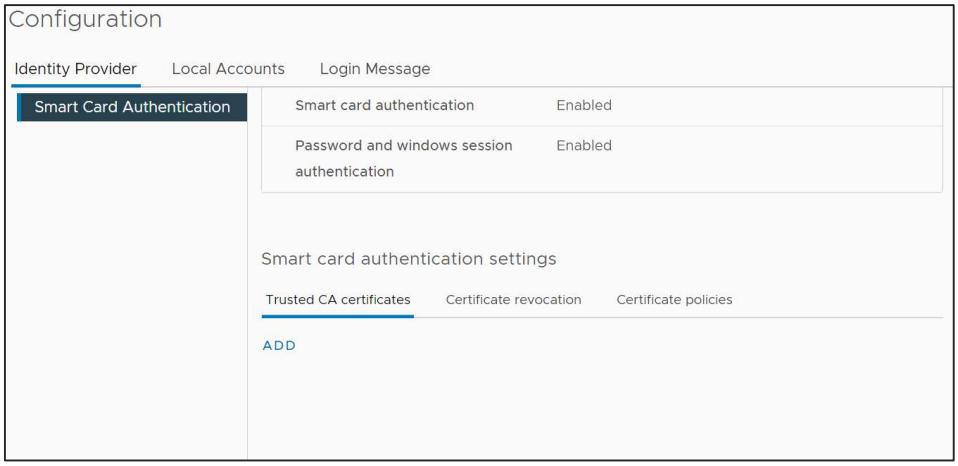

Figure 3: *Additional smart card options*

5. Add any trusted CA certificates here to include the entire chain for user issued certificates that will login to vCenter.
6. Configure certificate revocation by selecting the "Certificate Revocation" tab and clicking Edit. You can enable CRL or OCSP or both from the available options.

OCSP only
If the issuing CA supports an OCSP responder, enable OCSP and disable CRL as failover for OCSP.

CRL only
If the issuing CA does not support OSCP, enable CRL checking and disable OSCP checking.

Both OSCP and CRL
If the issuing CA supports both an OCSP responder and a CRL, vCenter Single Sign-On checks the OCSP responder first. If the responder returns an unknown status or is not available, vCenter Single Sign-On checks the CRL. For this case, enable both OCSP checking and CRL checking, and enable CRL as failover for OCSP.

Note – The UI does not let you specify an OCSP signing certificate or configure OCSP responders on a per-site basis in a multi-site deployment. This must be done from the command line and is shown in a later section.

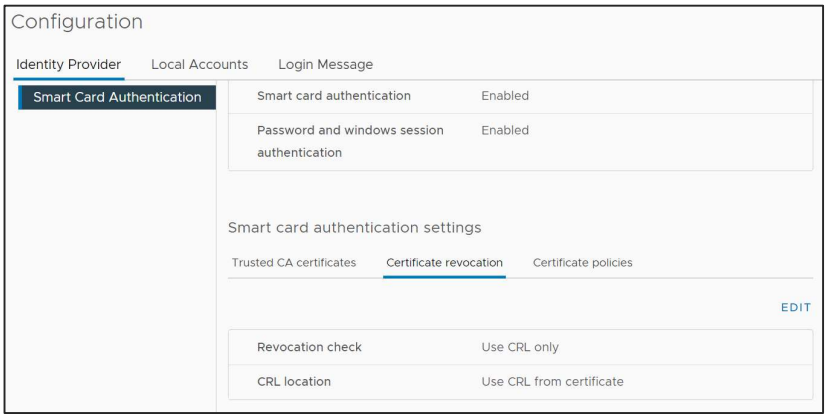

Figure 4: *Certificate revocation tab*

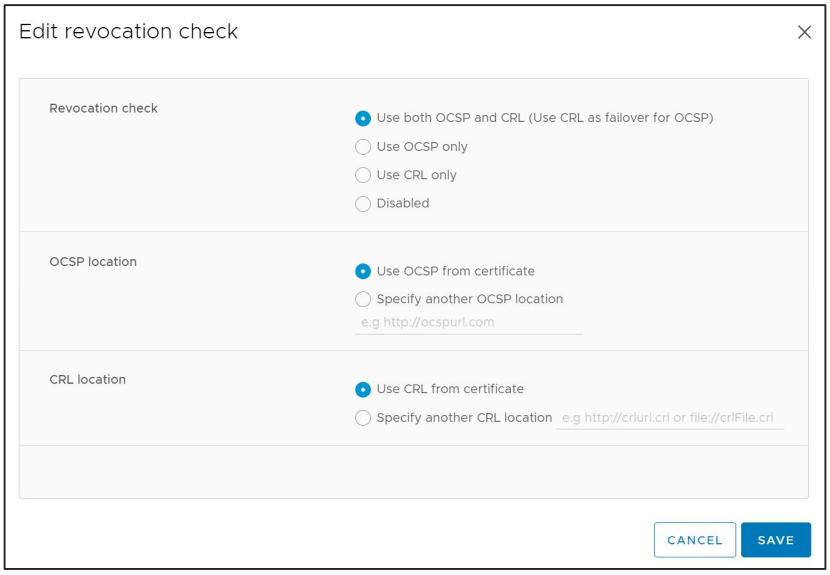

Figure 5: *Certificate revocation options*

7. Next configure the DoD login banner by going to the "Login Message" tab under Single Sign On > Configuration as shown in the screenshot.

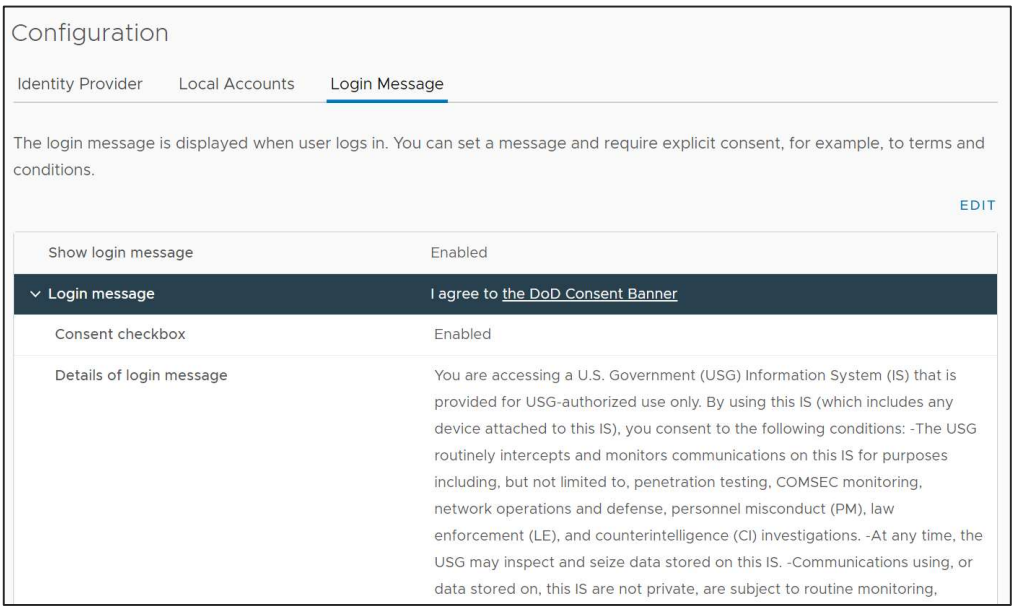

Figure 6: *Login Message Configuration*

Advanced Configuration Options

In this section we will highlight some advanced configuration options that some environments may need for optimal configuration.

(Optional) Advanced OCSP/CRL Configuration

Configure site specific OCSP responders for a multi-site scenario

It is recommended to configure alternate, local OCSP responders and CRL repositories to limit WAN traffic. Site ID is optional and will default to the default site. Responders can be configured to be site specific, for example to force your Boston site to use the Boston responder and your Seattle site to use the Seattle responder.

1. Login to the vCenter shell as the root user.
2. Run the following commands:

```
# /opt/vmware/bin/sso-config.sh -t vsphere.local -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl http://local.ocsp.url -ocspSigningCert /path/to/yourOCSPSigningCA.cer


# If you need to find the SiteID for a given PSC, run this command
# /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-guid --server-name PSC.FQDN.or.localhost
```

Note – ocspSigningCert is optional here.

Override the CRL URL with a local repository

1. Login to the vCenter shell as the root user.
2. Run the following commands:

```
# /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -useCertCrl false -crlUrl http://local.crl.url
```

(Optional) Add all DoD Trusted Certificates to the trust store

This would be in lieu of adding them through the UI.

1. Navigate to *https://public.cyber.mil/pki-pke/tools-configuration-files/*
2. Under “Configuration Files” download the PKI CA Certificate bundle for DOD PKI only. At the time of publication this was “PKI CA Certificate Bundles: PKCS#7 For DoD PKI Only - Version 5.7” for example.
3. Open the zip and extract the PEM p7b file. Certificates_PKCS7_v5.7_DoD.pem.p7b for this example
4. SCP the file to the vCenter appliance for example under /tmp
5. Import the DoD Certs by running the following command(s):

```
# cd /tmp
# openssl pkcs7 -inform PEM -print_certs -in ./Certificates_PKCS7_v5.6_DoD.pem.p7b | awk '/subject=/ {++n} {print > "dodcert" n ".cer"} END {print n " certificates split out"}'
# list="";for i in dodcert*.cer; do list="$list,$i";done;list=${list:1};/opt/vmware/bin/sso-config.sh -set_authn_policy -certAuthn true -cacerts "$list" -t vsphere.local
```

(Optional) Restore password authentication

If you have disabled password authentication and need to restore it you can turn it back on by following these steps.

1. Login to the vCenter shell as the root user.
2. Run the following commands:

```
# /opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn true -t vsphere.local
```

Frequently Asked Questions

QUESTION	ANSWER
Is the Enhanced Authentication Plugin (EAP) required for smart card authentication?	No. The documentation that says as such is incorrect. The EAP enables Windows Integration Authentication, it passes Windows Kerberos session credentials.
What is the format required for the trusted certificates?	Base64 / PEM
Does the order that the certificates are added via sso-config.sh or the VCSA UI matter?	No
Do I need to specify an OCSP URL?	No. By default the OCSP responder URL is pulled from the client certificate itself. If you have a local responder you can specify that local service with "-add_alt_ocsp" above and override the certificate fields.
Can I have username and password on with smart card authentication at the same time?	Yes
What if I mandated smart card authentication but I cannot login, how do I get access to vCenter?	Disable smart card authentication and re-enable username and password /opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn true -winAuthn false -certAuthn false -securIDAuthn false -t vsphere.local
I have multiple AD domains that I want to smart card authenticate to, how do I do pick my target domain? How do I know which one is being used by default?	You cannot currently specify the domain to target for smart card login. This will likely change in future releases. If you have multiple domains then SSO will start at the top of the list of identity sources and try each one until the user is found. SSO currently assumes a smart card user will be unique across domains. DoD users have the @mil domain in their UPN. For other types that may have "user@actual-domain.com" SSO will attempt to authenticate against "actual-domain.com" if that domain is configured or discovered through AD trust.
Where is the public documentation for this feature?	https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.authentication.doc/GUID-91CF824D-3C1A-403D-A680-1244F172F288.html
Where are the relevant logs on the VCSA?	/var/log/vmware/sso/vmware-sts-idmd.log /var/log/vmware/sso/ssoAdminServer.log

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com