

SMART CARD AUTHENTICATION

Table of Contents

[vCenter 6.5 Smart Card Authentication Configuration](#)

[vCenter 6.0 Update 2 Smart Card Authentication Configuration](#)

Smart Card Authentication

vCenter 6.5 Smart Card Authentication Configuration

vCenter 6.5 Smart Card Authentication Configuration Guide

Prepared by

Lincoln Porter
Staff Systems Engineer
lporter@vmware.com

Ryan Lakey
Senior Consultant
rlakey@vmware.com

vCenter 6.5 Smart Card Authentication Configuration Guide

Version History

Date	Ver.	Author	Description	Reviewers
20 MAR 2017	1.0	Lincoln Porter	Initial release forking from 6.0 version	Ryan Lakey

© 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

© 2015 VMware, Inc. All rights reserved.

Page 2 of 17

Contents

Version History	2
Contents	3
1. Overview	4
1.1 Summary	4
1.2 System requirements	4
1.3 Browser support	5
1.4 Browser plugins	5
2. Enabling smart card authentication	6
2.1 Configure the reverse proxy	6
2.2 Option 1 : Configure smart card authentication from the command line	8
2.3 Option 2 : Configure smart card authentication from the PSC web interface	11
2.4 Individual Configuration Items	13
2.4.1 Enable password authentication	13
2.4.2 Get a summary of the current configuration	13
2.4.3 Enable or disable revocation checking	13
2.4.4 Enable or disable OCSP	13
2.4.5 Set OCSP responder override	14
2.4.6 Enable or disable CRL failover after OCSP fails	14
2.4.7 Set logon banner from the command line	14
3. FAQ	15
4. Troubleshooting	17

1. Overview

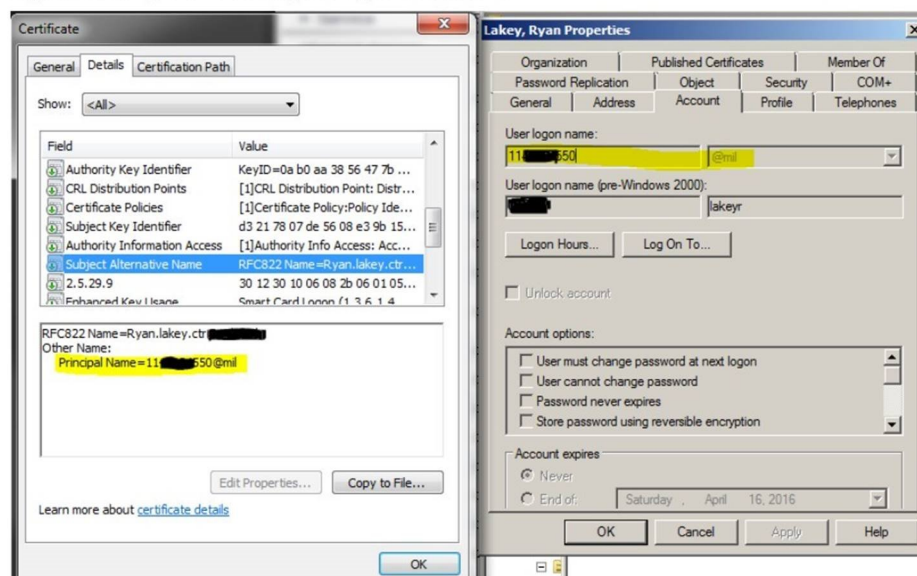
1.1 Summary

The Platform Services Controller (PSC) that was released as part of Single Sign-On (SSO) in vSphere 6.0GA only supported username/password for authentication. 6.0 Update 2 and later allows the configuration of a PSC to support multiple new forms of authentication. The focus of this document is the configuration of certificate-based authentication in vSphere 6.5 as the configuration is distinctly different from the 6.0 branch, there is a separate document for that version. This feature is biased towards Department of Defense Common Access Card (CAC) implementations but may fit other environments as well. This document will not tell you how to implement PKI, only how to integrate vSphere SSO into an existing PKI.

1.2 System requirements

1. 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:
 - a. 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.

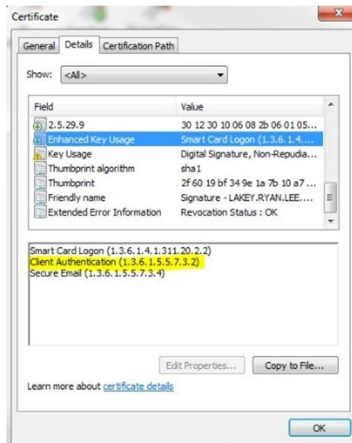
Figure 1. Example SAN corresponding to AD account



- b. 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.

vCenter 6.5 Smart Card Authentication Configuration Guide

Figure 2. Example Key Usage in Certificate



- Smart card authentication must be backed by Active Directory and as such an AD identity source must be configured in SSO. Both native and AD over LDAP are supported, neither is better than the other. This must be done manually by the SSO administrator.
- The enterprise PKI is configured so that the PSC is able to contact the OCSP and/or CRL servers specified in the certificate or optionally overridden by the SSO administrator.
- All PSCs and vCenters are assumed to be on the same build of 6.5. This guide is not intended for a mixed environment of 6.0 and 6.5 PSCs and vCenters.

1.3 Browser support

- Internet Explorer and Chrome are supported.
- Firefox does not work with smart card authentication.
- Safari is untested.

1.4 Browser plugins

The Enhanced Authentication Plugin (EAP) is not required for smart card authentication. This feature is enabled by the browser's native certificate capabilities and the SSO reverse proxy. The EAP enables logging in to vCenter with your Windows session credentials.

2. Enabling smart card authentication

The following steps will guide you through enabling smart card authentication. This involves two general steps.

1. Configure the reverse proxy on each PSC to request client certificates.
2. Configure SSO itself using either the GUI or the command line.

The Windows PSC is not included at this time. The configuration is nearly identical to the appliance but it is not documented here for simplicity's sake. You should move to the VCSA for 6.5 if you have not done so already. Windows vCenter deprecation is looming and all new features are being implemented in the appliance.

2.1 Configure the reverse proxy

This first step configures the reverse proxy to prompt for client side certificates and must be run locally on each PSC, there is no GUI for this step and it is mandatory.

1. SSH or log on to the console of the PSC.
2. Skip this step if the default shell has already been changed. SCP will not work with the default root shell. Enable SCP by changing the shell for root from "/bin/appliancesh" to "/bin/bash" by running the following commands:

```
a. shell
b. chsh -s /bin/bash root
```

3. The reverse proxy can optionally send a whitelist of issuing certificates for the client browser to filter available client certificates.
 - a. If the trusted root store is empty then all personal certs on the client side will be available for selection.
 - b. If there is at least one certificate in the store then the whitelist is enforced and only certificates issued by those authorities will be presented by the browser.
 - c. Providing root certificates covers all issued intermediates. This makes providing intermediates and roots redundant but not harmful.
 - d. Providing intermediates without roots is supported.
 - e. Providing only root certificates is the most future-proof. Until a new root is published any new intermediates will be covered.
4. Depending on your choice of certificates to white list, SCP them to /tmp then concatenate them into one file. Certificates must be in PEM/Base64 format. For the first command:

```
a. openssl x509 -inform PEM -in /tmp/ca_cert1.cer > /usr/lib/vmware-ss0/vmware-
sts/conf/clienttrustCA.pem
```

vCenter 6.5 Smart Card Authentication Configuration Guide

5. For subsequent certificates:

```
a. openssl x509 -inform PEM -in /tmp/ca_cert2.cer >> /usr/lib/vmware-
sso/vmware-sts/conf/clienttrustCA.pem
```

6. Alternatively, for DoD specifically, you can just dump the DISA issued bundle right into the store. This may be overkill as described in step 3c but it eliminates some manual work.

- <http://iase.disa.mil/pki-pke/Pages/tools.aspx>
- Click the 'Trust Store' tab
- Scroll to the bottom until you see "PKI CA Certificate Bundles: PKCS#7"
- Click the download link that says "For DoD PKI Only - Version X.X"
- Open the zip, extract the PEM p7b file, in our case Certificates_PKCS7_v5.0u1_DoD.pem.p7b, SCP to /tmp on the PSC

```
f. openssl pkcs7 -print_certs -in /tmp/Certificates_PKCS7_v5.0u1_DoD.pem.p7b |
egrep -v "subject|issuer" > /usr/lib/vmware-sso/vmware-
sts/conf/clienttrustCA.pem
```

7. To make sure you have the certificates you want in the store run the following command:

```
a. keytool -printcert -v -file /usr/lib/vmware-sso/vmware-
sts/conf/clienttrustCA.pem | grep "Owner" | sort
```

8. Now that we have built the certificate store we need to configure the reverse proxy to prompt for client certs using this store as a whitelist. Make a copy of the reverse proxy default configuration

```
a. cp /etc/vmware-rhttpproxy/config.xml /etc/vmware-rhttpproxy/config.xml.bak
```

9. Open /etc/vmware-rhttpproxy/config.xml in your editor of choice and make the following changes in the <http> block:

- Uncomment the 'clientCertificateMaxSize' line

```
i. <clientCertificateMaxSize>4096</clientCertificateMaxSize>
```

- Add

```
i. <requestClientCertificate>true</requestClientCertificate>
```


vCenter 6.5 Smart Card Authentication Configuration Guide

- c. Uncomment 'clientCAListFile' and change 'rootcerts.pem' to /usr/lib/vmware-ssso/vmware-sts/conf/clienttrustCA.pem .

```
i. <clientCAListFile>/usr/lib/vmware-ssso/vmware-
    sts/conf/clienttrustCA.pem</clientCAListFile>
```

- d. Check that the <http> block looks like this

```
i. <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>/usr/lib/vmware-ssso/vmware-
    sts/conf/clienttrustCA.pem</clientCAListFile>
    <!-- Maximum size of a client certificate in case it is requested. -
    ->
    <clientCertificateMaxSize>4096</clientCertificateMaxSize>
    <requestClientCertificate>true</requestClientCertificate>
</http>
```

- 10. Restart the rhttpproxy service.

```
a. /usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy
```

2.2 Option 1 : Configure smart card authentication from the command line

This second step configures the smart card feature inside of SSO and can be done from the CLI or the GUI. This change replicates across the PSCs and therefore only needs to be done in one place.

- 1. SSH or log on to the console of the PSC.
- 2. Skip this step if the default shell has already been changed. SCP will not work with the default root shell. Enable SCP by changing the shell for root from "/bin/appliancecsh" to "/bin/bash" by running the following commands:

```
a. shell
b. chsh -s /bin/bash root
```

- 3. Option 1 : To add all DoD root certs easily:
 - a. Navigate to <http://iase.disa.mil/pki-pke/Pages/tools.aspx>

© 2015 VMware, Inc. All rights reserved.

Page 8 of 17

vCenter 6.5 Smart Card Authentication Configuration Guide

- b. Click the 'Trust Store' tab
- c. Scroll to the bottom until you see "PKI CA Certificate Bundles: PKCS#7"
- d. Click the download link that says "For DoD PKI Only - Version X.X"
- e. Open the zip, extract the PEM p7b file, in our case
Certificates_PKCS7_v5.0u1_DoD.pem.p7b
- f. SCP the p7b file to /tmp on the PSC

```
g. cd /tmp

h. openssl pkcs7 -inform PEM -print_certs -in
  ./Certificates_PKCS7_v5.0u1_DoD.pem.p7b | awk '/subject=/ {++n} {print >
  "dodcert" n ".cer"} END {print n " certificates split out"}'

i. 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
```

4. Option 2 : Upload the desired certificates individually.

- a. SCP your PEM/Base64 trusted root certificates to /tmp on the PSC.
- b. Run the following command to add the trusted roots to SSO. This command is not additive, all certificates must be specified at once.

```
i. /opt/vmware/bin/sso-config.sh -set_authn_policy -certAuthn true -
  cacerts "/tmp/MySmartCA1.cer,/tmp/MySmartCA2.cer" -t
  vsphere.local
```

5. Turn off Integrated Windows Authentication and SecurID.

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -winAuthn false -
  securIDAuthn false -t vsphere.local
```

6. Add your smart card enabled AD account to the SSO Administrators group.

7. Make sure that logins are working correctly before continuing.

- a. Disable revocation checking (on by default) to make sure logins work without checks.

```
i. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -
  revocationCheck false
```

- b. When logins are working turn revocation checking on and continue configuration.

vCenter 6.5 Smart Card Authentication Configuration Guide

```
i. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -
    revocationCheck true
```

8. **(Optional)** Turn off password authentication and mandate smart card authentication. This includes vsphere.local accounts but it can easily be re-enabled.

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn false -t
    vsphere.local
```

9. By default OCSP is off and CRL from the distribution points on the certificate is used. It is recommend to turn on OCSP and use CRL as fallback but this will depend on your environment.

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -useOcsp
    true

b. /opt/vmware/bin/sso-config.sh -set_authn_policy -t vsphere.local -
    failoverToCrl true
```

10. **(Optional)** It is further 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. Once this again this is user choice and will depend on your environment.

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

b. If you need to find the SiteID for a given PSC, run this command
```

```
i. /usr/lib/vmware-vmafd/bin/vmafd-cli get-site-name --server-name
    PSC.FQDN.or.localhost
```

11. **(Optional)** Now we override the CRL URL with a local repository.

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

12. **(Optional)** Set the login banner.

© 2015 VMware, Inc. All rights reserved.

Page 10 of 17

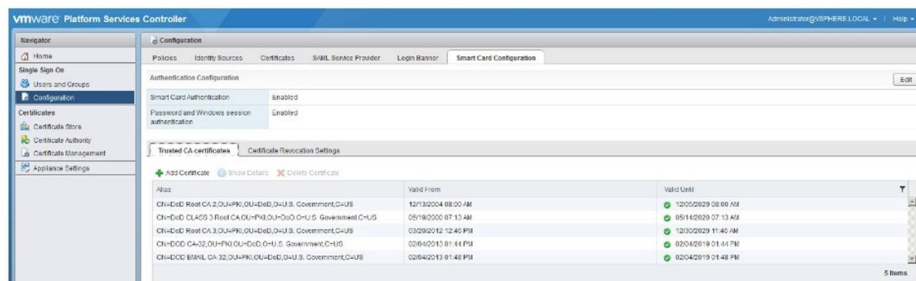

```
a. /opt/vmware/bin/sso-config.sh -set_logon_banner -title "Banner title" -
enable_checkbox Y <path-to-banner-file>
```

2.3 Option 2 : Configure smart card authentication from the PSC web interface

This second step configures the smart card feature inside of SSO using the PSC GUI. The GUI does not let you specify an OCSP signing cert or configure responders on a per-site basis, this must be done through the command line in section 2.2.

1. Login to the PSC web interface with administrator@vsphere.local from
https://<FQDN or IP of PSC>/psc
In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.
If you specified a different SSO domain during installation, log in as administrator@mydomain.
2. Browse to Single Sign-On > Configuration.
3. Click Smart Card Configuration, select "Edit" next to "Authentication Configuration", check the box next to "Smart Card Authentication".
4. In this same window if you uncheck "Password and Windows session authentication" then smart card login will be mandated and no user/pass logins will be allowed including vsphere.local. This can be rolled back via CLI in section 2.4 if access to vCenter via smart card is somehow lost.
5. On the same page, select the Trusted CA certificates tab.
6. To add one or more trusted certificates, click "Add Certificate", click "Browse" and select a certificate, and click "OK".

Figure 3. PSC Admin Console Smart Card Configuration



7. To change certificate revocation settings click on the "Certificate Revocation Settings" tab and enable/disable revocation checking and CRL/OCSP settings per your environment.
8. By default CRL checking using the certificates distribution point is enabled and OCSP is disabled. We recommend turning on OCSP and using CRL as fallback. We further recommend, optionally,

vCenter 6.5 Smart Card Authentication Configuration Guide

configuring alternate, local OSCP responders and CRL repos to further limit WAN traffic. Per-site OSCP responders can only be configured through the CLI.

Figure 4. PSC Admin Console Smart Card Certificate Revocation Settings

The screenshot shows the 'Smart Card Configuration' tab in the PSC Admin Console. Under 'Trusted CA certificates', the 'Certificate Revocation Settings' sub-tab is active. It displays the following settings:

- Certificate Revocation Settings:**
 - Revocation Check: Disabled (with an 'Enable Revocation Check' button)
- Certificate Revocation List Settings:**
 - Use CRL from certificates: Disabled
 - CRL Location: (empty field)
- OCSP Revocation:**
 - OCSP Revocation: Disabled
 - Use CRL in case of OCSP failure: Disabled
 - OCSP URL: (empty field)
- Certificate policies accepted:**
 - Buttons: + Add, - Remove
 - Certificate policy: (empty field)

At the bottom, it states 'No items to display'.

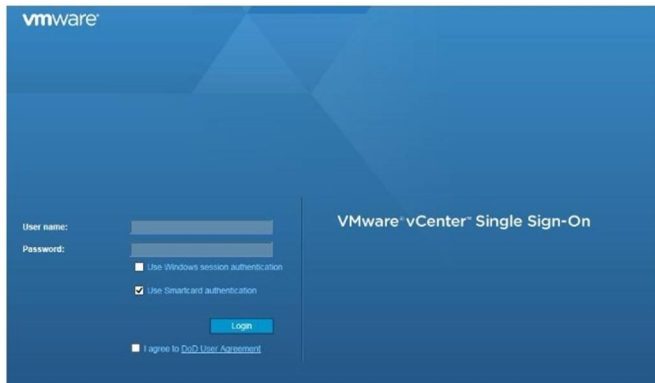
9. Configure the login banner according to your requirements.

Figure 5. Logon banner configuration

The screenshot shows the 'Login Banner' configuration page. It displays the following settings:

- Status:** Enabled
- Checkbox Consent:** Enabled
- Title:** DoD User Agreement
- Message:** You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests - not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

vCenter 6.5 Smart Card Authentication Configuration Guide

Figure 6. vCenter Web Client Login Page after Smart Card Authentication is Enabled.

2.4 Individual Configuration Items

2.4.1 Enable password authentication

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

2.4.2 Get a summary of the current configuration

```
b. /opt/vmware/bin/sso-config.sh -get_authn_policy -t vsphere.local
```

2.4.3 Enable or disable revocation checking

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -revocationCheck <true/false> -t  
vsphere.local
```

2.4.4 Enable or disable OCSP

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -useOcsp <true/false> -t  
vsphere.local
```

vCenter 6.5 Smart Card Authentication Configuration Guide

2.4.5 Set OCSP responder override

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -ocspUrl  
"http://responder.FQDN.or.IP" -t vsphere.local
```

2.4.6 Enable or disable CRL failover after OCSP fails

```
a. /opt/vmware/bin/sso-config.sh -set_authn_policy -failoverToCrl <true/false> -t  
vsphere.local
```

2.4.7 Set logon banner from the command line

```
a. /opt/vmware/bin/sso-config.sh -set_logon_banner -title "Banner title" -  
enable_checkbox Y <path-to-banner-file>
```

3. FAQ

1. Is the Enhanced Authentication Plugin (EAP) required for smart card authentication?
 - a. No. The documentation that says as such is incorrect. The EAP enables Windows Integration Authentication, it passes Windows Kerberos session credentials.
2. What is the format required for the trusted certificates?
 - a. Base64 / PEM
3. Does the order that the certificates are added via sso-config.sh or the PSC UI matter?
 - a. No
4. Do I need to specify an OCSP URL?
 - a. 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 “-ocspUrl” above and override the certificate fields.
5. Can I have username and password on with smart card authentication at the same time?
 - a. Yes
6. What if I mandated smart card authentication but I cannot login, how do I get access to vCenter?
 - a. 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
```

7. Why are we specifying certificates two times?
 - a. There are two components that need to be configured for smart card authentication to function, the reverse proxy and SSO itself. The reverse proxy sits in front of a number of vCenter/PSC services and its configuration is not currently exposed by API, all modifications must be made by hand. The certs for the reverse proxy are to aide the browser in client cert selection by providing an acceptable white list. The certs configured in SSO via GUI or sso-config.sh are for the verifying that client cert are issued by one of the specified trusted roots.
8. I want to go back to the stock configuration, how do I do that?
 - a. Set the authentication policy back to windows and username/password.

```
i. /opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn true -
winAuthn true -certAuthn false -securIDAuthn false -t vsphere.local
```

- b. Open /etc/vmware-rhttpproxy/config.xml in your editor of choice and replace the <requestClientCertificate> block with:

vCenter 6.5 Smart Card Authentication Configuration Guide

```
i. <!-- <requestClientCertificate>true</requestClientCertificate> -->
```

c. Restart the service:

```
i. /usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy
```

9. I have multiple AD domains that I want to smart card authenticate to, how do I pick my target domain? How do I know which one is being used by default?
 - a. You cannot currently specify the domain to target for smart card login. This will likely change in future releases.
 - b. 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.
 - c. 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.
10. If I mandate smart card authentication on the web client can't I bypass this with the C# client?
 - a. The authentication methods allowed by AD come in to play here. Generally speaking, accounts that are smart card enabled should not have a user-defined password. The C# client is fully deprecated in vSphere 6.5.
11. I have multiple PSCs linked in the same SSO domain, can I configure CAC authentication on one and have it replicate to the rest?
 - a. Partially. The reverse proxy must be configured on each PSC manually. All other changes through the PSC GUI or using sso-config.sh are replicated via vmdir and only need to be done on one PSC.
12. Where is the public documentation for this feature?
 - a. <https://pubs.vmware.com/vsphere-65/topic/com.vmware.psc.doc/GUID-08DF3B90-85C6-4CBB-B87C-CEF380844B95.html>
13. Where are the relevant logs on the PSC?
 - a. /var/log/vmware/sso/vmware-sts-idmd.log
 - b. /var/log/vmware/sso/ssoAdminServer.log

4. Troubleshooting

Issue: You get an error "Make sure the smart card is inserted properly" when trying to login to the vSphere Web Client with smart card authentication and are not prompted to choose a certificate.

Resolution: This error indicates a problem with the reverse proxy configuration. This must be done from the command line as described in section 2.1. If you have done that and is still throws that error and does not prompt for certificates make sure the trusted CA whitelist in `clienttrustCA.pem` is correct, that `config.xml` has been modified and that the service has been restarted as described in section 2.1. Optionally empty out the `clienttrustCA.pem` file, restart the service and retry.

Issue: You get an error "Unable to validate the submitted credential" when trying to login to the vSphere Web Client with Smart Card authentication.

Resolution: All root and intermediate certificates in the chain must be specified.

Check the logs under `/var/log/vmware/sso/vmware-sts-idmd.log` for

"com.vmware.identity.idm.CertificateRevocationCheckException: CertPath building failed. unable to find valid certification path to requested target"

You are probably missing a certificate in the path of the user's certificate. There are many DoD root and intermediate CAs so verify the path on the user's certificate and add any missing from the chain.

Resolution: This error can also indicate a problem after the raw certificate validation, an issue finding the user in AD. For example, it could be that a certificate without a subject alternative name was selected, resulting in the following logs entries:

Check the logs under `/var/log/vmware/sso/vmware-sts-idmd.log` for

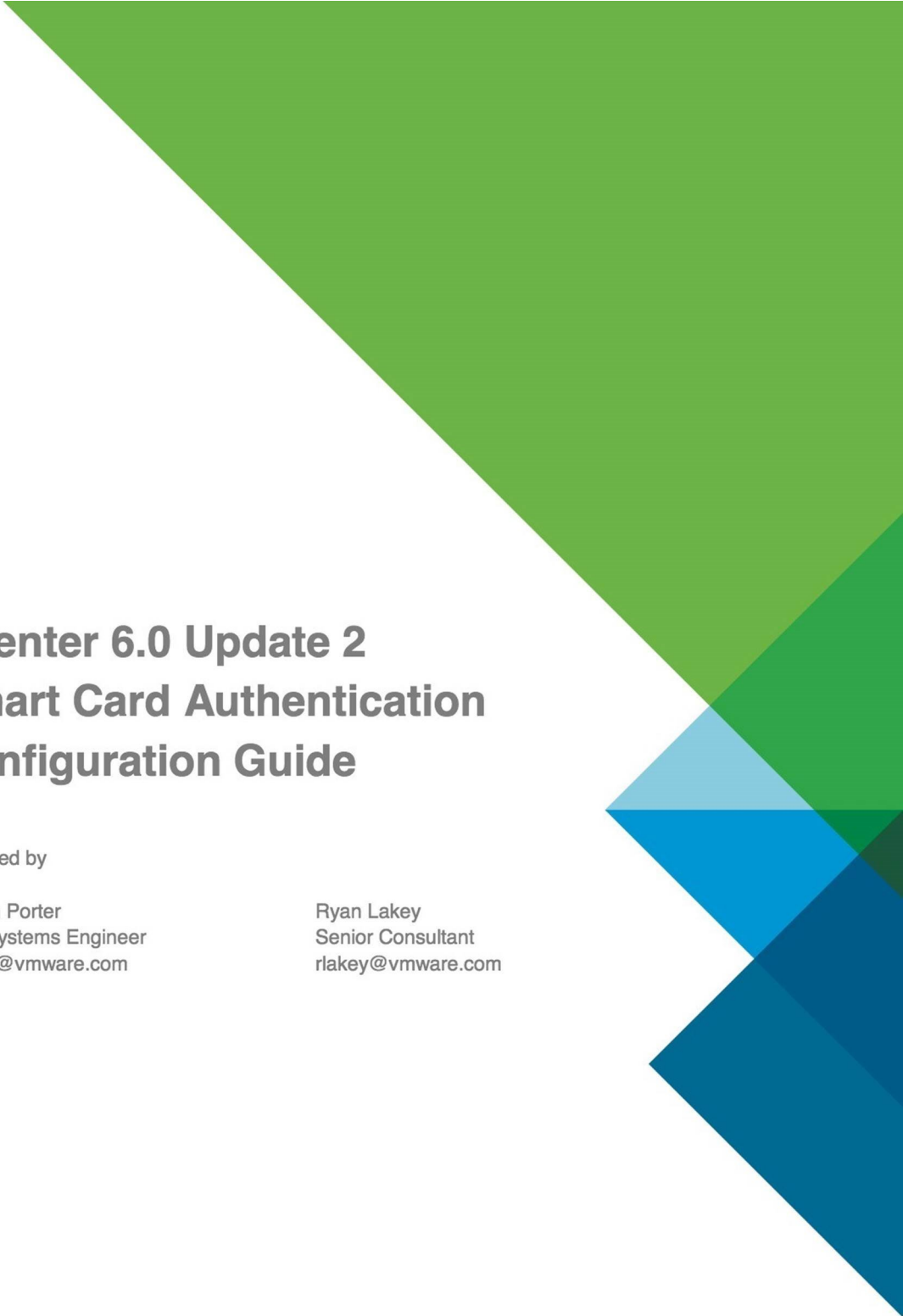
"ERROR] [IdmClientCertificateValidator] No subject alternative name found in the cert."

Or

"ERROR] [ServerUtils] Exception 'com.vmware.identity.idm.IdmClientCertificateParsingException: Empty Subject Alternative Names"

Resolution: Look at `/var/log/vmware/sso/vmware-sts-idmd.log` for details on where the authentication is failing. Otherwise, generally make sure that the AD identity source is working, that the base DNs are correct and that the user exists. The Web Client login is actually an LDAP lookup by the PSC (after certificate validation) so it must be able to find and read the user account or the login will fail. In the case of integrated authentication if the user is located in a trusted domain make sure that the machine account is able to enumerate that other domain.

vCenter 6.0 Update 2 Smart Card Authentication Configuration



vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

Prepared by

Lincoln Porter
Staff Systems Engineer
lporter@vmware.com

Ryan Lakey
Senior Consultant
rlakey@vmware.com

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

Version History

Date	Ver.	Author	Description	Reviewers
07/06/2016	1.2	Lincoln Porter	Command line clarifications	Ryan Lakey
04/08/2016	1.1	Lincoln Porter	Syntax corrections, clarified commands for multi-master deployments	Ryan Lakey
03/16/2016	1.0	Lincoln Porter	Initial Release	Ryan Lakey

© 2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. This product is covered by one or more patents listed at <http://www.vmware.com/download/patents.html>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

© 2015 VMware, Inc. All rights reserved.

Page 2 of 16

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304
www.vmware.com

© 2015 VMware, Inc. All rights reserved.

Page 3 of 16

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

Contents

1. Overview	5
1.1 Summary.....	5
1.2 System Requirements	5
1.3 PSC Support for Smart Card in a Highly Available Configuration.....	6
2. Configuring Smart Card Authentication	8
2.1 Enabling Smart Card from the command line	8
2.2 Enabling Smart Card from the Admin Console	9
2.3 Advanced Configuration Items	12
3. FAQ.....	14
4. Troubleshooting.....	16

List of Figures

Figure 1. Example SAN corresponding to AD account	5
Figure 2. Example Key Usage in Certificate.....	6
Figure 3. PSC Admin Console Smart Card Configuration.....	11
Figure 4. PSC Admin Console Smart Card Certificate Revocation Settings	11
Figure 5. vCenter Web Client Login Page after Smart Card Authentication is Enabled.	11
Figure 6. Logon banner configuration.....	13

1. Overview

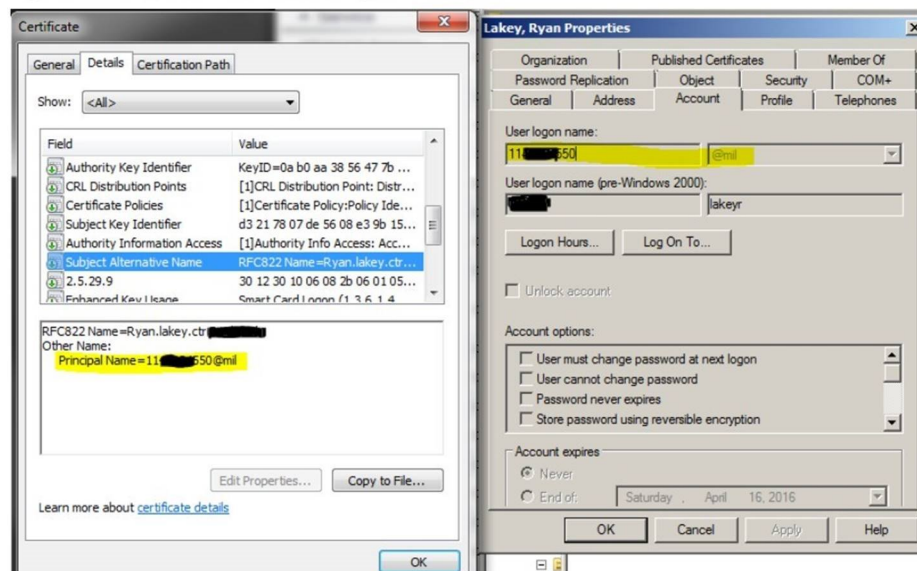
1.1 Summary

The Platform Services Controller (PSC) that was released as part of Single Sign-On (SSO) in vSphere 6 only supported username/password for authentication. Since then we have received numerous requests from customers with high governance requirement that we implement industry standard two factor authentication mechanisms. Update 2 allows the configuration of a PSC to support multiple new forms of authentication. The focus of this document is the configuration of certificate-based authentication to include but not specifically limited to smart cards.

1.2 System Requirements

1. 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:
 - a. 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.

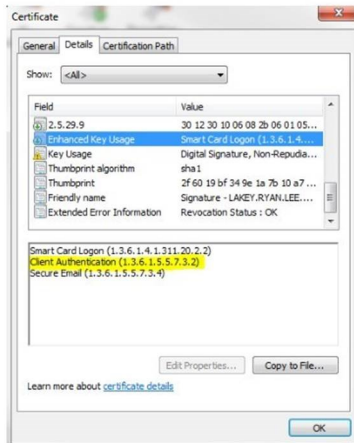
Figure 1. Example SAN corresponding to AD account



- b. 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.

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

Figure 2. Example Key Usage in Certificate



- Smart card authentication must be backed by Active Directory and as such an Active Directory identity source must be configured in SSO. This must be done manually by the SSO administrator.
- The enterprise PKI is configured so that the PSC is able to contact the OCSP and/or CRL servers specified in the certificate itself or optionally overridden by the SSO administrator.
- The PSC webssso certificate must be trusted by the end user's workstation. Failure to do so will prevent mutual TLS and authentication will not be attempted by the browser.
- In vSphere 5.5 port 7444 was used for vCenter communication with the SSO server. In 6.0 U2 we use the port 7444 to negotiate mutual TLS and obtain the client authentication certificate from the SSO server. Therefore before enabling smart card authentication any vCenter 5.5 servers that use the 6.0 PSC will need to be upgraded to 6.0.
- Root and intermediate certificates should be added to the PSC in base-64 format.

1.3 Browser Support

- Internet Explorer and Chrome are supported.
- Firefox does not work with smart card authentication.

1.4 PSC Support for Smart Card in a Highly Available Configuration

!! Warning !!

There is a known issue with Smart Card authentication and PSCs in an HA configuration and is not working at this time. See the following in the release notes.

http://pubs.vmware.com/Release_Notes/en/vsphere/60/vsphere-vcenter-server-60u2-release-notes.html#securityissues

!! Warning !!

This section is only applicable if you plan to deploy the 6.0 U2 PSC in a HA configuration.

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

1. If the 6.0 U2 PSC is set up in a HA configuration then port 7444 must be opened on the load balancer and configured as HTTPS, similar to port 443 in the HA configuration guide.
2. In the original PSC HA configuration scripts the PSC was configured in an SSL bridge where the SSL traffic from the vCenter server terminated at the load balancer and the load balancer set up a second SSL connection to the backend PSC server. However this will not be sufficient for CAC since the load balancer will need to pass the client authentication certificate directly to the backend PSC. Therefore you will need to use the updated scripts for PSC HA that will configure the PSC in a pass through configuration.
3. The HA scripts configures the certificate that will be used for SSL by the PSC. As part of the configuration of CAC it will configure port 7444 with the SSL certificate used by port 443. Therefore the CAC configuration will need to be performed after the HA configuration. Alternatively if the CAC configuration step was already performed then you will need to run the CAC configuration command `sso-config.bat` or `sso-config.sh` again so that the SSL certificate configuration is applied again. See the following section for file locations.

2. Configuring Smart Card Authentication

2.1 Enabling Smart Card from the command line

The following steps will guide you through enabling Smart Card authentication from the command line from a PSC.

1. If the PSC is to be configured for HA set that up before configuring smart card authentication. See Step 3 under section 1.3.
2. Upgrade your PSC to 6.0 U2 or start with a green-field deployment of 6.0 Update 2.
3. Configure the PSC to enable client certificate authentication via the following:
 - a. If using a Windows PSC:
 - i. Open an administrator command prompt and navigate to
 - ii. %PROGRAMFILES%\VMware\VMware Identity Service
 - iii. Replace <sso-config> referenced from here on with the batch file **sso-config.bat**
 - iv. Make sure all necessary root and intermediate issuing certificates are locally accessible to the sso-config.bat utility. Obtain and copy the certificates to a folder on the PSC machine.
 - b. If using a PSC virtual appliance:
 - i. SSH or log on to the console of the PSC
 - ii. SCP will not work with the default root shell. Enable SCP by changing the shell for root from "/bin/appliancesh" to "/bin/bash" by running the following commands:

```
1. shell.set --enabled True
2. shell
3. chsh -s /bin/bash root
```

- iii. Use WinSCP or similar utility to copy over all necessary root and intermediate issuing certificates to the PSC.
- iv. Optionally disable SCP and return to the default shell

```
1. chsh -s /bin/appliancesh root
```

- v. Replace <sso-config> referenced from here on with the shell script **/opt/vmware/bin/sso-config.sh**

- c. Run the following commands:

```
1. <sso-config> -set_to_cert_authn -switch true -cacerts
"pathtotrustedCAone.cer,pathtotrustedCATwo.cer,..." -t vsphere.local
```


vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

```
2. "service-control --stop vmware-std" and "service-control --start vmware-std"

3. <sso-config> -set_authn_policy -certAuthn true -cacerts
"pathtotrustedCAone.cer,pathtotrustedCAtwo.cer,..." -t vsphere.local
```

- d. Steps three will replicate across PSCs but step one and two must be run on each PSC in the SSO domain individually.
- e. Run the following command to verify the settings are configured correctly:

```
<sso-config> -get_authn_policy -t vsphere.local
```

Output should read as:

- IsPasswordAuthEnabled:true
- IsWindowsAuthEnabled:true
- IsTLSClientCertAuthnEnabled:true
- revocationCheckEnabled:true
- useOCSP:false
- sendOCSPNonce:false
- useCRLAsFailOver:false
- OCSPResponderSigningCert:UndefinedConfig
- OCSPUrl:UndefinedConfig
- useCertCRL:true
- CRL CacheSize:512
- CRLUrl:UndefinedConfig
- trustedCA:<Subject name of first CA certificate>
- trustedCA:<Subject name of second CA certificate>

2.2 Enabling Smart Card from the Admin Console

Some configuration can be done through the PSC Admin Console to enable Smart Card authentication except the tomcat server configuration above.

You can enable and disable smart card authentication, customize the login banner, and set up the revocation policy from the Platform Services Controller Web interface.

You can configure smart card authentication from the command line or by using the Platform Services Controller Web interface.

- Configure Tomcat from the command line and restart the Tomcat service for each Platform Services Controller, as shown in the steps below.
- Perform all other configuration either with the sso-config script or the Platform Services Controller. Configuration of supported authentication types and revocation settings is stored in

© 2015 VMware, Inc. All rights reserved.

Page 9 of 16

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

VMware Directory Service and replicated across all Platform Services Controller instances in a vCenter Single Sign-On domain.

The following steps will guide you through enabling Smart Card authentication from the admin console from a PSC.

1. Follow the steps in the command line section to configure the tomcat service on the PSC. For deployments with multiple PSCs this command must be run on each PSC individually. All other configuration can be done from the admin console of the PSC.
 - a. Only these commands need to be ran from the command line in this scenario

```
1. <sso-config> -set_tc_cert_authn -switch true -cacerts
   "pathtotrustedCAone.cer,pathtotrustedCATwo.cer,..." -t vsphere.local

2. "service-control --stop vmware-std" and "service-control --start vmware-
   std"
```

2. Login to the PSC admin console with administrator@vsphere.local from

https://<fqdn or ip of PSC>/psc

In an embedded deployment, the Platform Services Controller host name or IP address is the same as the vCenter Server host name or IP address.

If you specified a different domain during installation, log in as administrator@mydomain.

3. Browse to Single Sign-On > Configuration.
4. Click Smart Card Configuration, and select the Trusted CA certificates tab.
5. To add one or more trusted certificates, click Add Certificate, click Browse and select a certificate, and click OK.
6. To specify the authentication policy, click Edit next to Authentication Configuration and select or unselect authentication methods.

You cannot enable or disable RSA SecurID authentication from this Web interface. However, if RSA SecurID has been enabled from the command line, the status shows in the Web interface.

7. To change certificate revocation settings click on the Certificate Revocation Settings tab and enable/disable revocation checking and CRL/OCSP settings per your customer's environment.

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

Figure 3. PSC Admin Console Smart Card Configuration

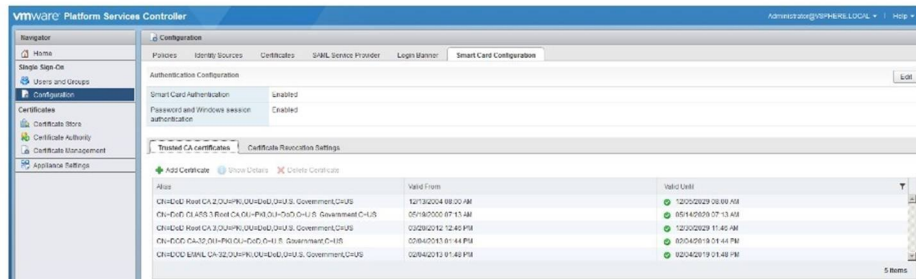


Figure 4. PSC Admin Console Smart Card Certificate Revocation Settings

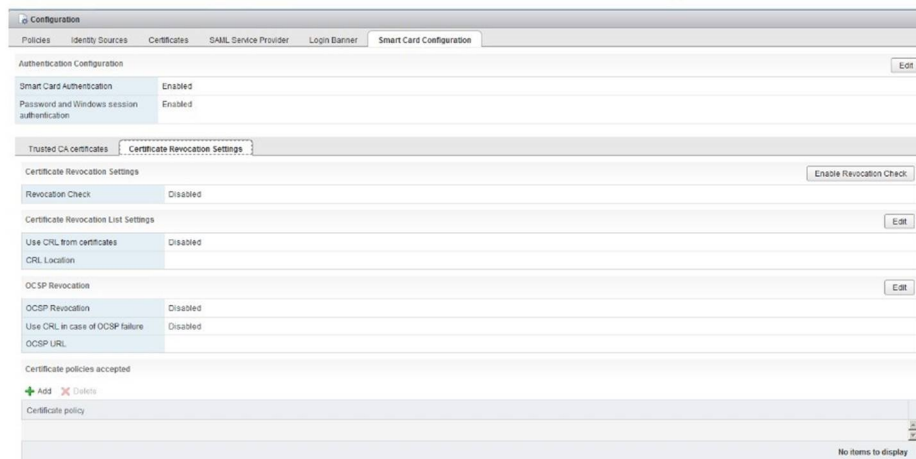
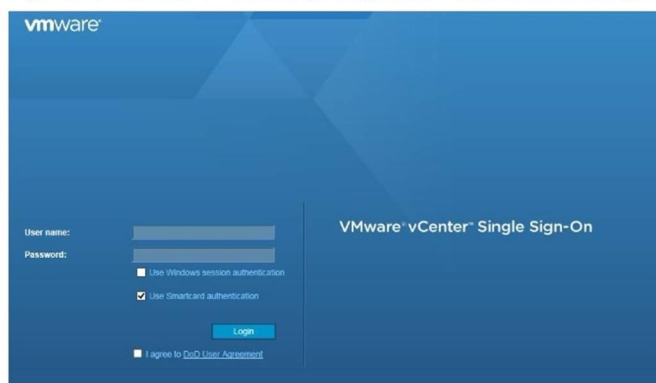


Figure 5. vCenter Web Client Login Page after Smart Card Authentication is Enabled.



2.3 Advanced Configuration Items

2.3.1 Configuration steps to mandate smart card authentication

In order to lock down vCenter so that smart card is the only accepted form of authentication the following steps must be performed.

1. Add an AD account that is smart card enabled to the SSO Administrators group. The administrator@vsphere.local account will not be able to login once smart card authentication is mandated. Adding this account ensures initial access to vCenter.
2. Configure smart card as the only accepted authentication method with the following:

```
<sso-config> -set_authn_policy -pwdAuthn false -winAuthn false -securIDAuthn
false -t vsphere.local
```

2.3.2 Advanced Configuration

2.3.2.1. Enable or disable revocation checking

```
<sso-config> -set_authn_policy -revocationCheck <true/false> -t vsphere.local
```

2.3.2.2. Enable OCSP

```
<sso-config> -set_authn_policy -useOcsp true -t vsphere.local
```

2.3.2.3. Set OCSP responder override

```
<sso-config> -set_authn_policy -ocspUrl "http://responder.FQDN.or.IP" -t vsphere.local
```

2.3.2.4. Set CRL failover if OCSP fails

```
<sso-config> -set_authn_policy -failoverToCrl true -t vsphere.local
```

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

2.3.2.5. Set logon banner from the PSC Admin Console

Figure 6. Logon banner configuration

The logon banner is displayed when a user logs in. You can set a message, and you can require explicit consent, for example, to Terms and Conditions.

login banner	
Status	Enabled
Checkbox Consent	Enabled
Title	DoD User Agreement
Message	You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

2.3.2.6. Set logon banner from the command line

```
<sso-config> -set_logon_banner -title "Banner title" -enable_checkbox Y <path-to-banner-file>
```

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

3. FAQ

1. What is the format required for the trusted certificates?
 - a. Base-64 .cer
2. Does the order that the certificates are added via sso-config matter?
 - a. No
3. Do I need to specify an OCSP URL?
 - a. 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 "-ocspUri" above and override the certificate fields.
4. Can I have username and password on with smart card auth at the same time?
 - a. Yes
5. What if I mandated smart card auth but I cannot login, how do I get access to vCenter?
 - a. Disable smart card auth and re-enable username and password

```
<sso-config> -set_authn_policy -pwdAuthn true -winAuthn false -certAuthn false -
securIDAuthn false -t vsphere.local
```

6. How do I set an OCSP signing cert, I see it in the policy description?
 - a. This feature is not implemented yet.
7. Why are we specifying certificates two times, one with "-set_tc_cert_authn -cacerts" and once with "-set_authn_policy -cacerts" ?
 - a. "-set_tc_cert_authn -cacerts" sets a whitelist for issuing certificates on the client side. This is not for certificate trust, it is a filter on the tomcat front end for allowed or expected issuing certs on the client side.
 - b. "-set_authn_policy -cacerts" sets the trusted certificates for the PSC application itself.
8. I want to go back to the stock configuration, how do I do that?
 - a. Set the authentication policy back to windows and username/password.

```
<sso-config> -set_authn_policy -pwdAuthn true -winAuthn true -certAuthn false -
securIDAuthn false -t vsphere.local
```

- b. Below commands disable the tomcat cert whitelist and restart the service. They have no practical effect on operation after the above command is run. Run these commands on each PSC in the SSO domain.

vCenter 6.0 Update 2 Smart Card Authentication Configuration Guide

```
1. <sso-config> -set_tc_cert_authn -switch false -t vsphere.local
2. "service-control --stop vmware-std" and "service-control --start vmware-std"
```

9. 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?
 - a. Currently only one AD identity source is supported for smart card login. If you have multiple domains then the first domain added as an identity source will be used for smart card authentication. Multiple domain support is on the roadmap for future versions.
10. If I mandate smart card authentication on the web client can't I bypass this with the C# client?
 - a. The authentication methods allowed by AD come in to play here. Generally speaking, accounts that are smart card enabled should not have a user-defined password. There are no plans to add smart card authentication to the C# client.
11. I am have multiple PSCs linked in the same SSO domain, can I configure CACauthentication on one and have it replicate to the rest?
 - a. Partially. The "-set_tc_cert_authn" command and subsequent vmware-std service restart must be on each PSC manually. All other changes are replicated via vmdir and only need to be done on one PSC.

4. Troubleshooting

Issue: You get an error "Make sure the smart card is inserted properly" when trying to login to the vSphere Web Client with Smart Card authentication.

Resolution: If you configured Smart Card authentication only through the PSC admin console it does not configure tomcat which must be done from the command line. If you have done that the vmware-stds service must be restarted on the PSC after configuration.

Issue: The vmware-stds service will not start after smart card configuration on the PSC.

Resolution: If you do not specify any certificates when running the sso-config commands the certificate store for tomcat will be deleted and the service will fail to start.

Check the logs under /var/log/vmware/sso/utils for errors relating to a missing key store.

To fix rerun the sso-config commands and specify certificates.

Issue: You get an error "Unable to validate the submitted credential" when trying to login to the vSphere Web Client with Smart Card authentication.

Resolution: All root and intermediate certificates in the chain may not be specified.

Check the logs under /var/log/vmware/sso/vmware-sts-idmd.log for

"com.vmware.identity.idm.CertificateRevocationCheckException: CertPath building failed, unable to find valid certification path to requested target"

You are probably missing a certificate in the path of the user's certificate. There are many DoD root and intermediate CAs so verify the path on the user's certificate and add any missing from the chain.

Issue: You get an error "Unable to validate the submitted credential" when trying to login to the vSphere Web Client with Smart Card authentication.

Resolution: A certificate without a subject alternative name was selected. Select the certificate when prompted that contains the user's AD name in the SAN field and that has Client Authentication extended key usage.

Check the logs under /var/log/vmware/sso/vmware-sts-idmd.log for

"ERROR] [IdmClientCertificateValidator] No subject alternative name found in the cert."

Or

"ERROR] [ServerUtils] Exception 'com.vmware.identity.idm.IdmClientCertificateParsingException: Empty Subject Alternative Names'"



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

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.