WHITE PAPER–AUGUST 2020

vCenter Smart Card Authentication Configuration Guide

Version 6.7

vmware®

Contents

Overview

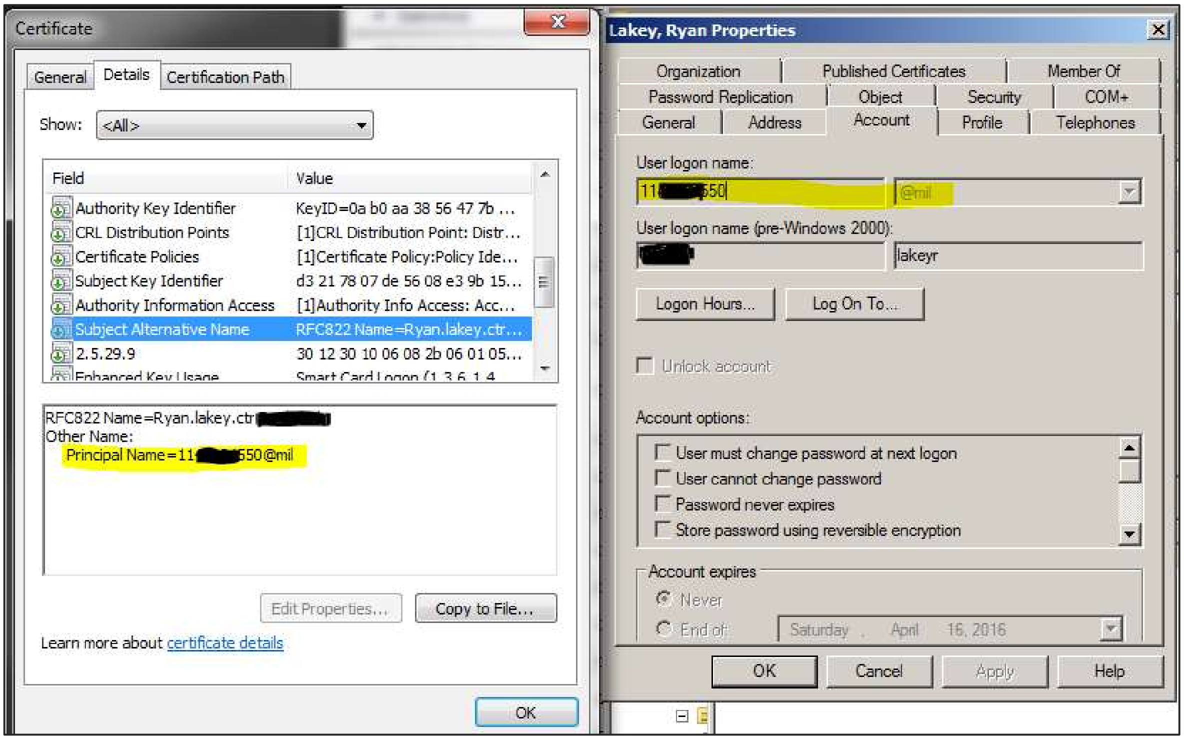
Summary

The Platform Services Controller (PSC) that was released as part of Single Sign-On (SSO) in vSphere 6.0 GA 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 6.7 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.

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.



Show: <All>

Field	Value
Authority Key Identifier	KeyID=0a b0 aa 38 56 47 7b ...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Subject Key Identifier	d3 21 78 07 de 56 08 e3 9b 15...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	RFC822 Name=Ryan.lakey.ctr...
2.5.29.9	30 12 30 10 06 08 2b 06 01 05...
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4

RFC822 Name=Ryan.lakey.ctr[redacted]
Other Name:
Principal Name=11[redacted]550@mil

Learn more about certificate details

User logon name:
11[redacted]550 @mil

User logon name (pre-Windows 2000):
[redacted] lakeyr

□ Unlock account

Account options:
□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Saturday , April 16, 2016

FIGURE 1: Example Certificate and Active Directory Account

Browser Support

For certificate-based authentication

- Chrome, Internet Explorer, Microsoft Edge
- Firefox is not supported without additional plugins

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. The EAP enables logging in to vCenter with your Windows session credentials.

Enabling Smart Card Authentication

The following steps configure the smart card feature inside of SSO. This change replicates across the PSCs and therefore only needs to be done in one place. Method 1, the GUI method, is applicable to both appliance and Windows deployment models. Method 2, the CLI method, is applicable to both models but with different paths and script locations.

If you are on still on a Windows vCenter, please consider moving to the appliance in your next version upgrade. Windows vCenter deprecation has been announced and all new features are being implemented in the vCenter Server Appliance.

Method 1: Configue Smart Card authentication from the vCenter web interface

1. Login to the vCenter web interface as “administrator@vsphere.local” or another user that is part of the SSO group SystemConfiguration.Administrators group in vCenter.
2. Click on Menu >> Administration >> 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 2.3 if access to vCenter via smart card is somehow lost.
5. Choose to Enable only smart card authentication or to enable both smart card and password authentication.
6. Select the Trusted CA Certificates tab. To add one or more trusted certificates, click “Add Certificate”, click “Browse” and select a certificate, and click “OK”.
   You will need to add all Trusted Root, Intermediate, and Subordinate CA certificates that are in the certificate chain of your smart card or token certificate chain.
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.

   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 that section.

8. If the login banner needs to be changed that can also optionally be updated from the Login Banner tab to reflect your organizations banner.

Method 2: Configue Smart Card authentication from the command line on the PSC/VCSA

1. SSH or log into the console of the PSC if external or VCSA if embedded.
2. Enable the bash shell to allow SCP to work for copying ceritificates to the appliance. If the default shell has already been changed skip this step.

```
# shell

# chsh -s /bin/bash root
```

3. Option 1: Add all DoD certificates to the trust store
   a. Navigate to https://public.cyber.mil/pki-pke/tools-configuration-files/
   b. 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 5.6” for example.
   c. Open the zip and extract the PEM p7b file
      i. Certificates_PKCS7_v5.6_DoD.pem.p7b for this example
   d. SCP the file to the PSC.VCSA for example under /tmp
   e. Import the DoD Certs by running the following commands

```
# 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
```

4. Option 2: Add individual certificates to the trust store
   a. SCP your PEM encoded trusted root certificates to /tmp on the PSC/VCSA
   b. Run the following command to add the trusted roots to SSO. This command is not additive, all certificates must be added at once.

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

5. Add your smart card enabled AD account to vCenters' permissions if not done already.
6. Test logins without revocation checking (optional)
   a. Run the following command to disable revocation checking

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

   b. When logins are working you can turn revocation checking back on

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

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

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

8. By default OCSP is off and the CRL from the disitrbuted points in the certificate are used. It is recommended to turn on OCSP if one is available and use CRL as a fall back. Run the follow commands to turn on OCSP

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

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

9. **(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 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
```

10. **(Optional)** Override the CRL URL with a local repository by running the following command.

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

11. **(Optional)** Set the login banner by running the following command.

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

Additional Configuration Options

Enable password authentication

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

Get current configuration

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

Enable or disable OCSP

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

Set OCSP Responder per site or OCSP signing cert

```
# /opt/vmware/bin/sso-config.sh -t vsphere.local -add_alt_ocsp [-siteID yourPSCClusterID] -ocspUrl
http://responder.FDQN.or.IP -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
```

Show OCSP responder configuration

```
# /opt/vmware/bin/sso-config.sh -t vsphere.local -get_alt_ocsp [-siteID yourPSCClusterID]
```

Remove OCSP responder site configuration

```
# /opt/vmware/bin/sso-config.sh -t vsphere.local -delete_alt_ocsp [-allSite] [-siteID
yourPSCClusterID]
```

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 PSC 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/6.7/com.vmware.psc.doc/GUID-08DF3B90-85C6-4CBB-B87C-CEF380844B95.html*
Where are the relevant logs on the PSC?	/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