Client Authentication using Certificates

Contents

- 1 Client Authentication using Certificates during SSO
 - ♦ 1.1 Overview
 - 1.2 Pre-requisites
 - 1.2 Frefeguistes
 1.3 Setup a Server-Side Client Authentication keystore (truststore)
 \$ 1.3.1 Create a new Java keystore
 \$ 1.3.2 Import your CA certificate(s)
 \$ 1.4 Modify the Apache Tomcat server.xml

 - 1.5 Define the points within AuthControl Sentry SSO
 - 1.6 Establishing a Client-Side Certificate
 - 1.7 Enabling Certificate Revocation List checking ◊ 1.7.1 Create a job to download your CRL file(s)
 - 1.7.2 Modify the Apache Tomcat server.xml
 - ♦ 1.8 Troubleshooting

Client Authentication using Certificates during SSO

Overview

This article describes how to setup and configure Certificate authentication using AuthControl Sentry SSO. Some Linux knowledge and experience with certificates is recommended as this involves command line work and preparation of certificates from the CA within your enterprise. To establish Client Authentication with certificates in AuthControl Sentry, a Java keystore should be created with a certificate that is signed by your Enterprise CA. Changes then need to be made to the Apache Tomcat application server configuration, on the webapps2 connector entry in the server.xml configuration file.

Pre-requisites

- Certificate Authority within your organisation for signing certificates
 Creation of user certificate for ?Client Authentication? purposes with Private Key
- Keystore Explorer (freeware) installed on your workstation, to create and view Java Keystore files
- Command line access to the Swivel Secure appliance
- Some experience with the *vi* Linux command for file editing purposes

Setup a Server-Side Client Authentication keystore (truststore)

An easy method to create a new Java Keystore is by using a free third-party application called Keystore Explorer. The alternative method would be to take a copy of the keystore associated with the Apache Tomcat connectors (providing https to users connecting to ports 8080 and 8443) and modify it.

Create a new Java keystore

Create a new keystore e.g. auth.jks Import your Root CA certificate Import any intermediary CA certificates (especially if the certificate on the device was signed by those Intermediaries)



Click File -> Save As. You will first be prompted for a Keystore password. Enter the password as ???lockbox???

A Untitled-1	* - KeyStore Explo	rer 5.0.1			- 🗆 X	
File Edit View	Took Framina					
The cuit view	Tools examine			D D D LO		- 主要接近台省自然性于目
	AAA					ani in the second se
United-1 8 8						A second in the second second second
5113959 3						dia 3 - 10 martine rais
	Entry Name	Algorithm	Key Size	Cartificate Expiry	Last Modified	
		Set KeyStore Passw	brav	×		
		-				
		Palan Manu Baan	wath analysis			
		CITICET MEW Pass	MIGNES: 0000000			
		Can San May 8200	and a second			
		SETTI THE PRES	Millio 000000			
		1				
			CK	Cancel		
			hannann	20100 0		
						States and Marked Collins and Street
						CALMERT PLANTER WORK WORKS and a size of the second
						ставителя на сласти по ставителя ставителя ставителя с общество ставителя с общество с тавителя общ О тавителя общество с тавителя обществ О тавителя общество с тавителя о О тавителя общество с тавителя общество с тавителя общество с тавителя от тавителя от тавителя от тавителя от т О тави
KeyStore Type: 1	KS. Size: O Entries.	Path: Untilled-1				
ustame they	al area a punied	1 3 4 11 ST 1 4 5 9 4				

Save the file as auth.jks

A Untitled-1 * - Ke	yStore Explorer	5.0.1			- 🛛	Х	And and a
File Edit View Tool	ls Examine H	elp					
	XID	# 2 R 1	2 = O A G				
Uniitled-1 * 🗶							
📋 🚺 🖪 Ent	r <mark>y Name</mark>	Algorithm	Key Size	Cartificate Expiry	Last Modified		
A Save KeyStor	re As					X	
Save in:	keystares			· 686			
Recent Items Cesktop Documents							
Metwork	File name: Files of type:	auth.jks Keyštore Files (*	.ks;*.keystore;*.jks;	*.jæks;*.bks;*.ubær) 🗸	Save Cencel		
KeyStore Type: JKS, Si	ze: O Entries, Pai	h: Uniited-t'					

Import your CA certificate(s)

Next, import your Intermediate AND/OR your Root CA certificates into the keystore, so that any client certificates generated by your PKI can be validated during RBA using this keystore.

To import your CA trusted certificates, goto Tools -> Import Trusted Certificate.

Locate and select the certificate, then click Import.

🍌 auth.jks - KeyStore	Explorer 5.0.1				– 🗆 X	S.M. D. Comp. 1
File Edit View Tools	Examine Hel	p				an ana an an 120 Can And Can Strategy (1997) Managan Strategy (1997)
	XNB	R & R 1				No. of South Control Public
auth.jks 🗶						CAREFORNIN FRAMEWORK
📋 🚺 🗄 Brity P	Name	Algorithm	Key Size	Certificate Expiry	Last Medified	
Mimport Trust	ed Certificate	ecccentreccentere			Х	
Lockin:	keystore	3		· • • • •		
Recent Iters Desktop Documents	auth.jks					
	File nome:	root.crt			Import	STRATISSIN BRURNER CONTRACTOR
Network	Files of type:	All Fles		Y	Cancel	
KeyStore Type: JKS, Size:	0 Entries, Path	: 'C: (Users)daroj		umento/keystcres/quitu.jks		

You may receive this warning, where you will be prompted to trust the certificate you have imported:



Click OK and follow the onscreen prompts to review and accept the certificate as trusted.

A auth.jks - KeyStore Explorer	5.0.1	8 <u>22</u> 8		
				recorde recorder construction of March 2010 and 2010
File Edit View Tools Examine	e Help			
auh.jks 🗶				
Certificate Details for	File 'root.crt'		X	
1 6			đ	
Carlifeata Harawhee				
小人 机管门机 部分部件				
				1805 W 200 a start in an
Contract of Contra				An Al-West of the second
Version:	3			
Subject	CN=AddTrust External CA Root, OU=AddTrust External TTP Netwo			
				the second part of the second se
læver	CN=AddTrust External CA Root.OU=AddTrust External TTP Netwo	13		Sale and served the rest of the served served and the served serve
		Tib		The second
Seviel Musham	Part			
SCIENTING S	0.4.1			
Malid Beara	3728 85-050 11-49-28 95T			
VEDU FTSHIS	20/1493/5060 7.2-19/20 021			A DECEMBER OF DE
Webial LineSch	20.04-0020 11-030-08 PT			
VERO STUG	2016.61450 7.22.9226 221			
a.lk.k.	221 22 12 12 H			
PUDIC KEYS	RSA 2048 018			
0.0000000000000000000000000000000000000				
Signature Algorithm:	SHA-1 with RSA			
			-	
Fingerprints	SHA-1 v 02:FA:F3:E2:91:43:54:68:60:78:57:69:4D:F5:E	1. 0		Sec. 143, 50, 50, 50, 70, 70, 80, 80, 80, 80, 80, 80, 80, 80, 80, 8
	Extensions PEM	ASN.1		
			6	
1			_	
		ΟX	III	
		mmm	1111	
KeyStore Type: JKS, Size: O Entries	, Path: "C:/Users)dcroft.SWIVELSECURE/Documents/keystores/auth.jk	G		

🍌 auth.jks - KeyStore Explorer 5.0.1	[- 0	X	
File Edit View Tools Examine He	lp					
auh.jks ×						
👔 👔 📴 Entry Name	Algorithm	Key Size	Certificate Expiry	Last Medified		
Impor	t Trusted Certifica	ite	X			
THE	Do you want	to accept the certif	icate as trusted?			
VEL						
	Ύε	s No				

Enter a meaningful alias for the new CA certificate as it will appear in the keystore:





Save your changes, using the File -> Save menu option.

Modify the Apache Tomcat server.xml

On the Swivel Secure appliance, take a backup of the /usr/local/tomcat/conf/server.xml file, prior to making the necessary changes.

For the 8443 connector entry, add the following parameters:

```
clientAuth="want"
truststoreFile="/home/swivel/.swivel/auth.jks"
truststoreType="JKS"
truststorePass="lockbox"
```

So that it looks like this ...

Before:

<Service name="webapps2"> <Connector SSLEnabled="true" acceptCount="100" address="0.0.0.0" ciphers="TLS_ECDHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_ECDSA_WITH_AES_128 <Engine defaultHost="localhost" name="webapps2"> <Host appBase="webapps2" autoDeploy="true" name="localhost" unpackWARs="true">

```
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" pattern="common" prefix="webapps2" rotatable="false"
</Host>
</Engine>
</Service>
```

After:

```
<Service name="webapps2">

<Connector SSLEnabled="true" acceptCount="100" address="0.0.0.0" ciphers="TLS_ECDHE_DSS_WITH_AES_128_GCM_SHA256,TLS_DHE_ECDSA_WITH_AES_128

<Engine defaultHost="localhost" name="webapps2">

<Host appBase="webapps2" autoDeploy="true" name="localhost" unpackWARs="true">

<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs" pattern="common" prefix="webapps2" rotatable="false"

</Host>

</Host>

</Host>

</Host>

</Host>
```

Define the points within AuthControl Sentry SSO

Login to the AuthControl Sentry SSO Administration Portal. Goto Rules. Against Certificate, click ?View Rules?:

Stort Poge Rules	Rules		
Applications Authentication Methods	Rules	Number Of Rules	
View IdP Metodoto Keus	IP Range	0	QI
Usera Active Sessions	Time Range	0	QI
User History Log Vitewar	Certificate	0	Q



Add a new Certificate Rule. You can give any arbitrary name and assign the points you wish to award a user if they present a valid client authentication certificate during authentication:

Start Page Rules	Certificate Rule	
Applications	<i>v</i>	
Authenticotion Methods		
View to P Metao ata	Name	Truststore client authentication valid
(eye		
Users Advive Sessions	Score When Valid	50
Jeer History		
Log Viewer		
General Configuration		Sove
Application I mages		
	© 2018 Swivel Secure. All rights reserved.	
	1	

Establishing a Client-Side Certificate

- Ensure that your Client-Side certificate is PKCS#12 with a private key exported;
- The Client-Side certificate should be signed by your CA or Intermediate CA;
 Import this signed PKCS#12 certificate into the personal or computer trust store so that it is visible in the Settings -> Certificates panel of your Web Browser;

Enabling Certificate Revocation List checking

It's possible to enable CRL checks to establish a stronger chain of trust. Enabling this feature will enhance security by checking to see if an issued certificate has been revoked by the Certificate Authority.

Note: This feature relies upon an Outbound Internet connection and DNS to be configured. If not configured properly it may cause performance issues

Note: This feature relies upon restarting tomcat every time the CRL is updated

Create a job to download your CRL file(s)

```
#!/bin/bash
wget http://url1/crlfile1.crl -0 /home/swive1/crl.crl
if [ $? -ne 0 ]; then
exit
fi
openssl crl -inform DER -in /home/swivel/crl.crl -outform PEM -out /home/swivel/.swivel/crl.pem rm /home/swivel/crl.crl service tomcat restart
```

If you have more than one crl, you can concatenate them in one file:

```
#!/bin/bash
wget http://urll/crlfilel.crl -0 /home/swivel/crla.crl
if [ $? -ne 0 ]; then
exit
fi
wget http://url2/crlfile2.crl -0 /home/swivel/crlb.crl
if [ $? -ne 0 ]; then
exit
fi
openssl crl -inform DER -in /home/swivel/crla.crl -outform PEM -out /home/swivel/crla.pem
openssl crl -inform DER -in /home/swivel/crlb.crl -outform PEM -out /home/swivel/crlb.pem
cat /home/swivel/crla.crl
rm /home/swivel/crlb.crl
rm /home/swivel/crlb.crl
rm /home/swivel/crlb.crl
service tomcat restart
```

save the script as /home/swivel/.swivel/getCRLs.sh and create a cron job to run the script in "/etc/crontab". This example runs every day at midnight:

0 0 * * * swivel /home/swivel/.swivel/getCRLs.sh

Modify the Apache Tomcat server.xml

On the Swivel Secure appliance, take a backup of the /usr/local/tomcat/conf/server.xml file, prior to making the necessary changes.

For the 8443 connector entry, add the following parameter:

crlFile="/home/swivel/.swivel/crl.pem"

So that it looks like this...

Before:

After:

Troubleshooting

- If the Client-Side certificate is signed by the Root CA, then ensure that the Root CA trusted cert is imported into the server-side trust store. Likewise, if it is signed by an Intermediate CA, ensure that both the Root CA trusted cert AND the Intermediate CA trusted cert are BOTH imported into the server-side trust store;
- An Apache Tomcat restart is required, for the Server-Side changes to the server.xml to take effect;
- If you've just imported the Client Authentication PKCS#12 certificate into your device then you may need to completely close and re-open your Web Browser for it to become available;
- Ensure that the truststore password in the server.xml matches what was set in the KeyStore Explorer application. Re-apply the password under the Tools -> Set Password option on the KeyStore Explorer application if necessary.
- Check file permissions on the truststore file, so that they match those permissions of the existing keystore file being used for secure HTTP.
- Further clues about successfully loading the truststore keystore during startup can be found in /var/log/tomcat/catalina.out;
- View the AuthControl Sentry SSO logs for client authentication troubleshooting once your Server-side setup is established;
- If performance issues are encountered with CRL checking enabled, check to ensure that your Outbound Internet connection or DNS is still in place. Try to telnet the CRL URL hostname using telnet in the CMI Tools menu, or on the command line.
- ERR_BAD_SSL_CLIENT_AUTH_CERT (chrome), SSL_ERROR_CERTIFICATE_UNKNOWN_ALERT (firefox) or "Cannot securely connect to this page" (IE) means that the Client certificate is not valid or that the CRL file is not valid