Configure VCS with CAC and a Smart Card Reader

Contents

Introduction Prerequisites Requirements Components Used Background Information What is a Smart Card? Configure Verify Troubleshoot

Introduction

This document describes a step-by-step guide to install and use a Smart Card Reader and Common Access Card log in for use with the Cisco Video Communication Server (VCS) for organizations who require two-factor authentication to the VCS environment like banks, hospitals, or governments with secure facilities.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Expressway Administrator (X14.0.2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The CAC provides required authentication so "systems" know who has gained access to their environment and what part of the infrastructure be it physical or electronic. Within the government classified environments, and other secure networks, the rules of "least privileged access" or "need to know" prevail. A log in could be used by anyone, authentication requires something which the user has, ergo the CAC, also known as the Common Access Card, came about in 2006 so that the individual would not need to have multiple devices, be they fobs, id cards or dongles to access their place of employment or systems.

What is a Smart Card?

Smart cards are a key component of the public key infrastructure (PKI) that Microsoft uses to integrate into the Windows platform because smart cards enhance software-only solutions, such as client authentication, logon, and secure email. Smart cards are a point of convergence for public key certificates and associated keys because they:

- Provide tamper-resistant storage for the protection of private keys and other forms of personal information.
- Isolate security-critical computations, which involves authentication, digital signatures, and key exchange from other parts of the system that don't have a need to know.
- Enable portability of credentials and other private information between computers at work, at home, or on the road.

The smart card has become an integral part of the Windows platform because smart cards provide new and desirable features as revolutionary to the computer industry as the introduction of the mouse or CD-ROM. If you do not have an Internal PKI Infrastructure at the moment then you need to ensure you do this first. This document does not cover the installation of this role in this particular article but information on how to implement this can be found here: http://technet.microsoft.com/en-us/library/hh831740.aspx.

Configure

This lab assumes you have already integrated LDAP with VCS and have users that can log in with LDAP credentials.

- 1. Lab Equipment
- 2. Install the Smart Card
- 3. Configure Certificate Authority Templates
- 4. Enroll the Enrollment Agent Certificate
- 5. Enroll on behalf of....
- 6. Configure the VCS for Common Access Card

Required Equipment:

Windows 2012R2 Domain server that has these roles/installed software:

- Certificate Authority
- Active Directory
- DNS
- Windows PC with Smart Card attached
- vSEC: CMS K-Series management software to manage your Smart Card:



Versa Card Reader Software

Install the Smart Card

Smart card readers generally come with instructions on how to connect any necessary cables. Here is an example of installation for this configuration.

How to Install a Smart Card Reader Device Driver

If the smart card reader has been detected and installed, the Welcome to Windows logon screen acknowledges this. If not:

- 1. Connect your Smart Card to the USB Port on your Windows PC
- Follow the on-screen directions for installing the device driver software. This requires the driver media that manufacturer of the smart card or the driver is discovered in Windows. In my case I used the manufactures driver from their download site. DON'T TRUST WINDOWS.
- 3. Right-click the **My Computer** icon on your desktop and click **Manage** on the submenu.
- 4. Expand the Services and Applications node, and click Services.

- 5. In the right pane, right-click **Smart Card**. Click **Properties** on the submenu.
- 6. On the General tab, select Automatic in the Startup Type drop-down list. Click OK.
- 7. Reboot your machine if the Hardware wizard instructs you to do so.

Configure Certificate Authority Templates

- 1. Launch Certificate Authority MMC from Administrative Tools.
- 2. Click or select the **Certificate Templates** node and select **Manage**.
- 3. Right-click or select the **Smartcard User** Certificate Template and then select **Duplicate** as shown in the image.

Console1 - [Console Root\Certificate Templates (2012DC-AD.jajanson.local)]									
http://www.com/action and the state of the s	P						_ 8 ×		
Console Root	Template Display Name	Schema Version	Versi	Intended Purpo	ises		Actions		
Certification Authority (Local)	@ Administrator	1	4.1						
Certificate Templates (2012DC-AD.jajanson.loc	Authenticated Session	1	3.1				Certificate Templates (2012DC-AD.jaj *		
	Basic EFS	1	3.1				More Actions •		
	CA Exchange	2	106.0	Private Key Arc	hival		Smartcard Liser		
	CEP Encryption	1	4.1	,			Sinarcard Oser -		
	Code Signing	1	3.1				More Actions •		
	@ Computer	1	5.1						
	Cross Certification Authority	2	105.0						
	Directory Email Replication	2	115.0	Directory Service	ce Email Replication				
	Domain Controller	1	4.1						
	Domain Controller Authentication	2	110.0	Client Authenti	cation, Server Authentication, Smart Card Logon				
	EFS Recovery Agent	1	6.1						
	Enrollment Agent	1	4.1			_			
	Enrollment Agent (Computer)	1	5.1			-			
	Rechange Enrollment Agent (Offline requ	1	4.1						
	Exchange Signature Only	1	6.1						
	Exchange User	1	7.1						
	@ IPSec	1	8.1						
	IPSec (Offline request)	1	7.1						
	Kerberos Authentication	2	110.0	Client Authenti	cation, Server Authentication, Smart Card Logon, KD				
	Key Recovery Agent	2	105.0	Key Recovery A	gent				
	OCSP Response Signing	3	101.0	OCSP Signing					
	RAS and IAS Server	2	101.0	Client Authenti	cation, Server Authentication				
	Root Certification Authority	1	5.1						
	Router (Offline request)	1	4.1						
	Real Smartcard Logon	1	6.1						
	Smartcard User	1	11.1		Duplicate Template	-1			
	Smartcard User_VCS	4	101.6	Secure Email	ogon	- 11			
	Subordinate Certification Authority	1	5.1		All Tasks	- 11			
	I Trust List Signing	1	3.1		Properties				
	@ User	1	3.1		Help	-			
< III >	<				>				

Domain controller Certificate Templates

4. On the **Compatibility** tab, under **Certification Authority**, review the selection and change it if needed.

Compatibility settings

- 5. On the General tab:
- a. Specify a name, such as **Smartcard User_VCS**.
- b. Set the validity period to the desired value. Click Apply.

Time Begin Expire

- 6. On the Request Handling tab:
- a. Set the Purpose to Signature and smartcard logon.
- b. Click Prompt the user during enrollment. Click Apply.

Properties of New Template									
Subject Name	Server	Issuance	Issuance Requirements						
Superseded Templa	ates	Extensions	tensions Security						
Compatibility General	Request Handli	ng Cryptograph	ny Key Attestatio						
Purpose: Signa	Purpose: Signature and smartcard logon Delete revoked or expired certificates (do not archive)								
	lude symmetric al	gorithms allowed	by the subject						
	hive subject's en	cryption private l	(ey						
Allow private key to	be exported								
Renew with the sam	ne key (*)								
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)									
Do the following when the subject is enrolled and when the private key associated with this certificate is used:									
C Enroll subject without	ut requiring any u	ser input							
Prompt the user duri	ing enrollment								
Prompt the user during enrollment and require user input when the private key is used									
* Control is disabled due	e to <u>compatibility</u>	settings.							
ОК	Cancel	Apply	Help						
	_								

Request Handling

7. On the **Cryptography** tab, set the minimum key size to 2048.

a. Click **Requests must use one of the following providers**, and then select **Microsoft Base Smart Card Crypto Provider**.

b. Click Apply.

	Proj	perties	of New	Template		X		
Subject N	lame	Ser	rver	Issuance I	Requiremen	its		
Supersec	ded Templa	ates	Exte	nsions Security Cryptography Key Attestation				
Compatibility	General	Request	t Handling	Cryptography	Key Atte	station		
Provider Ca	tegory:	Leg	acy Crypto	graphic Service	Provider	~		
Algorithm na	ime:	Det	ermined by	CSP		~		
Minimum kej	y size:	204	8					
Choose whic	ch cryptogr	aphic prov	viders can	be used for req	uests			
O Request	s can use a	any provid	ler availabl	e on the subject	t's compute	r		
Request	s must use	one of the	e following	providers:				
Providers:								
Microsoft	Base Sma	rt Card Cr	ypto Provid	ler	^			
Microsoft	DH SChar	nnel Crypt	ographic P	rovider	≡			
Microsoft	Enhanced		aphic Provi 1 Diffic Holl	ider v 1.0 Iman Countogran	bio Pr			
Microsoft	Enhanced	RSA and	J AES Cryp	tographic Provi	der 🖄	♣		
Request ha	sh:	Det	ermined by	CSP		\sim		
Use alternate signature format								
[ОК		Cancel	Apply	Н	elp		
				o <i>u</i> i				
				Settings				

8. On the Security tab, add the security group that you want to give Enroll access to. For example, if you want to give access to all users, select the Authenticated users group, and then select **Enroll** permissions for them.

		Prop	perties	of New	Template		x
Compat	tibility	General	Request	Handling	Cryptography	Key Attesta	tion
Su	ibject N	lame	Sen	ver	Issuance	Requirements	
Su	upersed	led Templa	tes	Exte	ensions	Security	
Group) or use	rnames:					
<u>82</u> /	Authent	ticated Use	rs				
88 F	Adminis Domain Enterpri	trator (Adm Admins (J se Admins	in@jajans AJANSON (JAJANSC	on.local) \Domain <i>I</i>)N\Enterp	Admins) ise Admins)		
Permi	ssions f	or Authent	icated Use	ers	Add Allow	Remove Deny	
Ful	Contro	bl					
Re	ad				~		
Wri	ite						
Enr	roll				<		
Aut	toenroll						
For sp Advar	ecial p nced.	emissions	or advanc	ed setting:	s, click	Advanced	
		ОК	(Cancel	Apply	Help	

9. Click **OK** in order to finalize your changes and create the new template. Your new template must now appear in the list of Certificate Templates.

Console1 - [Console Root\Certificate Templates (2012DC-AD,jajanson.local)]								
🜇 File Action View Favorites Window Help	,					_ 8 ×		
Console Root	Template Display Name	Schema Version	Versi	Intended Purposes	^	Actions		
Certification Authority (Local)	Code Signing	1	3.1			Certificate Templates (2012DC-AD iai		
Certificate Templates (2012DC-AD.jajanson.loc	Computer	1	5.1			certificate remplates (2012DC-ADijajiii =		
	Cross Certification Authority	2	105.0			More Actions		
	Directory Email Replication	2	115.0	Directory Service Email Replication		Smartcard User VCS		
	Domain Controller	1	4.1			Mara Astions		
	Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon		more Actions		
	EFS Recovery Agent	1	6.1					
	Enrollment Agent	1	4.1					
	Enrollment Agent (Computer)	1	5.1					
	Exchange Enrollment Agent (Offline requ	1	4.1					
	Exchange Signature Only	1	6.1					
	Exchange User	1	7.1					
	@ IPSec	1	8.1					
	IPSec (Offline request)	1	7.1					
	Kerberos Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon, K	D			
	Key Recovery Agent	2	105.0	Key Recovery Agent				
	OCSP Response Signing	3	101.0	OCSP Signing				
	RAS and IAS Server	2	101.0	Client Authentication, Server Authentication	=			
	Root Certification Authority	1	5.1					
	Router (Offline request)	1	4.1					
	Smartcard Logon	1	6.1					
	Smartcard User	1	11.1					
	Smartcard User_VCS	4	101.6	Secure Email, Client Authentication, Smart Card Logon				
	Subordinate Certification Authority	1	5.1					
	Trust List Signing	1	3.1					
	@ User	1	3.1					
	User Signature Only	1	4.1					
	VCS_Login_SMART	2	100.8	Smart Card Logon, Client Authentication				
	Web Server	1	4.1	-				
	Webclientandserver	2	100.4	Client Authentication, Server Authentication				
	Workstation Authentication	2	101.0	Client Authentication				
< III >	٢	ш						
36 certificate templates								

Template seen in domain controlling

10. In the left pane of the MMC, expand Certification Authority (Local), and then expand your CA within the Certification Authority list.

Right-click Certificate Templates, click **New** and then click **Certificate Template** to Issue. Then choose the newly created Smartcard template.

a	Console1 - [Console Roo	t\Certification Authority (Local)\jajanson-2012DC-AD-CA\Certificate Templates]		_ 🗆 X
Tile Action View Favorites Window Help				_ 8 ×
Console Root Na	me	Intended Purpose	Actions	
D Certificate Templates	Exchange Enrollment Agent (Offline r	Certificate Request Agent	Certificate Templates	
⊿ 🙀 Certification Authority (Local)	IPSec (Offline request)	IP security IKE intermediate	Mare Astiens	
a 👩 jajanson-2012DC-AD-CA	Webclientandserver	Client Authentication, Server Authentic	More Actions	
Revoked Certificates	Exchange Signature Only	Secure Email		
Issued Certificates	CEP Encryption	Certificate Request Agent		
Pending Requests	Smartcard User_VCS	Secure Email, Client Authentication, Sm		
Failed Requests	VCS_Login_SMART	Smart Card Logon, Client Authentication		
Manage	Agent	Certificate Request Agent		
	mail Replication	Directory Service Email Replication		
New	ontroller Authentication	Client Authentication, Server Authentic		
View	uthentication	Client Authentication, Server Authentic		
New Window from Here	ery Agent	File Recovery		
New Taskpad View		Encrypting File System		
	ontroller	Client Authentication, Server Authentic		
Refresh	7	Server Authentication		
Export List		Client Authentication, Server Authentic		
Help		Encrypting File System, Secure Email, Cl		
	www.www.e Certification Authority	<all></all>		
	Administrator	Microsoft Trust List Signing, Encrypting		
			1	

Issue New Template

11. After the template replicates, in the MMC, right-click or select the Certification Authority list, click **All Tasks**, and then click **Stop Service**. Then, right-click the name of the CA again, click **All Tasks**, and then click **Start Service**.



Stop then start certificate services

Enroll on the Enrollment Agent Certificate

It is recommended that you do this on a Client Machine (IT Administrators Desktop).

1. Launch MMC choose Certificates, click Add then certificates for My User Account.

·		Console	- [Console Root]			_ 🗆 X
File Action View Favorites Window Hel	lp					_ <i>6</i> ×
Console Root	Name				Actions	
		There are no it	tems to show in this view.		Console Root	•
		Add or I	Remove Snap-ins	x	More Actions	,
	You can select snap-in, y Available snap-ins, y Available snap-ins; Snap-in Active Directory i Active Directory i Active Directory i Active Directory i Active Directory i Active Directory Active Directory Component Service Component Service Component Service Disk Management Disk Manage	s for this console from those available ou can configure which extensions are of the second	n your computer and configure the selected set of sur mabled. Selected anap-ins: Console Root Ed Certificat This snap-in will always manage certificates for: My user account Service account Computer account	ap-ins. For It Extensions It Estensions Ites snap-in	Cancel	

Add certificates

2. Right-click or select the **Personal Node**, select **All Tasks** and then select **Request New Certificate**.

Console1 - [Console Root\Certificates - Current User\Personal]	_ □ X
 File Action View Favorites Window Help ← ←	_ 8 ×
Console Root △	Actions Personal
▷ Pe ▷ Tr Find Certificates	More Actions
Find Certificates	
Image: Second	
▶ 🛄 Ur New Taskpad View Advanced Operations ►	
▷ □ Tr Refresh ▷ □ Cl Export List	
▷ 🛄 Ce Help	
Certification Authority (Loc Jajanson-2012DC-AD-Ci ✓ Ⅲ >	
Personal store contains 9 certificates.	

Request new certificates

3. Click **Next** on the wizard, and then select **Active Directory Enrollment Policy**. Then click **Next** again.

—	Concolal (Concola Doot) Cartificatae Current Usar Darconal 🗕 🗖 🗙	_ 🗆 X
File Action View	Certificate Enrollment	_ & ×
Console Root Certificates - Curren Certificates - Curren Certificates - Curren Certificates - Curren Certificates - Certi	Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.	s nal A lore Actions
Active Directory	Configured by your administrator	
Trusted Publishe	Active Directory Enrollment Policy 🗸	
 Untrusted Certifi Third-Party Root Trusted People Client Authentic Certificate Enroll Certificate Enroll Smart Card Trust Certification Author Jajanson-2012DC 	Configured by you Add New	
< III Personal store contains 9 cer	Next Cancel	

Active Directory Enrollement

4. Select the Enrollment Agent Certificate, in this case, Smartcard User_VCS and then click Enroll.



Enrollment Certificate Agent

Your IT Administrators desktop is now set up as an Enrollment Station, this enables you to enroll new smartcards on behalf of other users.

Enroll on behalf of....

In order for you to now provide employees with smartcards for authentication, you need to enroll them and generate the certificate which then is imported onto the Smartcard.



Enroll on behalf of

1. Launch MMC and import the **Certificates Module & Manger** the certificates for My User Account.

2. Right-click or select **Personal > Certificates** and select **All Tasks > Advanced Operations** and click **Enroll on behalf of...**

3. On the wizard, and choose the Active Directory Enrollment Policy then click Next.



Enroll on behalf advanced

a		Console1 - (Console Root)/Certif	icates - Current U	ser\Personal\Certifi	cates)				= 0 X
🔚 File Action View Favorites Window He	lp .								- 0 ×
🗢 🌩 🙎 📰 🖨 🗟 🕞 📓 📰									
Coreole Root	Issued To	based By	Expiration Date	Intended Purposes	Friendly Nome	Status	Cent	Actions	
a Personal	Administrator	isjancon-2012DC-AD-CA	10/12/2018	Microsoft Trust List	«None»		Adr	Certificates	•
Cartificates	Administrator				- 0 X			More Actions	,
p iii Enterprise Trust	Sideministrato	Certificate Encollement					Enro		
 Intermediate Certification Authorities Artice Directory User Object 	PrvKey 80945	Contraste enterneen			_		13.6		
p III Trusted Publishers	Scott Long	Before You Begin					Sma		
 Detroited Certification Darty Root Certification Authorities 	Scott Long	The fall and a start will have any install and it	and an address of the local data	d conduction conductor			Sma		
b Trusted People		networks, protect content, establish identity,	and do other security-	related tasks.	need to wearen				
 Client Authentication Issuers Certificate Envolment Requests 		Before requesting a certificate, verify the folio	wing						
5 🛄 Smart Card Trusted Roots		Your computer is connected to the network							
		You have credentials that can be used to vari	y your right to obtain	the certificate					
				Next	Cancel				
	<								
Personal store contains 9 certificates.	n - 1								

4. Select Certificate Enrollment Policy then click Next.

2		Console1 - [Console Root\Certifica	ites - Current Us	er\Personal\Certifi	cates]				- 🗆 X
Tile Action View Favorites Window Hel	lp .								_ 8 ×
(+ +) 2 🗊 🗓 🙆 🔂 🗊									
 File Action View Favorites Window Hel Console Root 	p Issued To Administrator Administrator Administrator Administrator Solution So	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA ertificate Enrollment Select Certificate Enrollment Policy Certificate enrollment policy mables enrollment Certificate enrollment policy mables de cor Configured by your administrator Active Directory Enrollment Policy Configured by you	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Certificate Request Microsoft Trust List	Friendly Name <none> <none> ate templates. Add New Cancel</none></none>	Status	Certi / Adrr Enro 1.3.6 Sma Sma Sma	Actions Certificates More Actions	@ X
Personal store contains 9 certificates.	<						>		

Enrollment policy

5. You are now asked to select the **Signing Certificate**. This is the enrollment certificate you requested earlier.

ä		Cons	sole1 - [Console Root\Certific	ates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
File Action View Favorites Window Help									_ @ ×
Console Root	Issued To		Issued By	Expiration Date	Intended Purposes	Friendly Name	Status Cer	rti Actions	
A Personal	Administrator		jajanson-2012DC-AD-CA	10/12/2019	Microsoft Trust List	<none></none>	Ad	Certificates	-
Certificates	Administrator					_ 0 X		More Actions	•
Enterprise Trust	Administrator	Cortificate					Enr	ro	
Intermediate Certification Authorities	PIVKey BD9A5		Windo	Windows Security			1.3	.6	
 Active Directory User Object Trusted Publishers 	Scott Lang	ing Select I Select a Certificate					Sm	a	
Untrusted Certificates	Scott Lang						Sm	a	
Third-Party Root Certification Authorities Trusted People		You need Browse t	Administrato			her users. Click			
Client Authentication Issuers			Issuer: jajanson-2	12DC-AD-CA					
Certificate Enrollment Requests Smart Card Trusted Roots			Valid From: 10/14	/2017 to 10/14/2019					
		Signing	Click here to view	certificate		Browne			
			properties			biowse			
			Administrato						
			See Issuer jajanson-2	1200-40-04					
			Valid From: 10/12	/2017 to 10/12/2019					
				0	Cancel				
					curren				
						Cancel			
	"								
	<						3	>	
Personal store contains 9 certificates.									

Select Signing Certificate

6. On the next screen, you need to browse to the certificate you would like to request and in this instance, it is **Smartcard User_VCS** which is the template you created earlier.

Choose the VCS Smart Card

7. Next, You need to select the user you wish to enroll on behalf of. Click **browse** and type in the username of the employee you wish to enroll. In this instance, Scott Lang 'antman@jajanson.local account' is used.

E	Console1 - [Console Root\Certificates - Current User\Personal\Certificates]		_ 🗆 X
File Action View Favorites Window Help			_ 8 ×
(+ +) 2 🗊 🗓 🤉 🔛 🗊			
Console Root Console Root Certificates - Current User Certificates Certificate Enrollment Requests Certificate Enrollment Requests	Issued By Expiration Date Intended Purposes Friendly Name ator jajanson-2012DC-AD-CA 10/14/2019 Certificate Request	Aame Status Certi Erro Adrr More Actions Enro 1.3.6 Sma Sma Sma Sma ncel	,
	88		
	ni		

Choose the user

8. On the next screen, proceed with the enrollment by clicking on **Enroll**. Now, insert a smartcard into your reader.



Enroll

9. Once you have inserted your smartcard, it's detected as follows:

ques	Windows Security		
e envol	Enrolling for the user certificate. Select a smart card device	_	
EVan	Axaito Cryptoflex .NET Gemaito USB Smart Card Reader 0 The smart card is ready for use. OK Cancel		

10. You are then asked to type in a smartcard PIN number (Default Pin: 0000).

a	Con	sole1 - [Console Root\Certific	ates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
File Action View Favorites Window Hel	lp							_ 8 ×
🗢 🔿 🙍 🔟 🔯 📾								
Console Root Console Root Certificates - Current User Certificates Certificates Certificates Certificates Certification Authorities Certification A	Issued To Administrator	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Certificate Request Microsoft Trust List	Friendly Name <none> - X</none>	Status Ce En Ac	erti Actions reo Certificates More Actions reo	•
 Distance in the intermediate Certification Authorities Active Directory User Object Trusted Publishers Third-Party Root Certificates Third-Party Root Certification Authorities Third-Party Root Certificates Client Authentication Issuers Certificate Enrollment Requests Smart Card Trusted Roots 	Carliganson-2012 Certificate PUKkey B0945 Scott Lang Scott Lang Scott Lang Scott Lang Scott Lang	Enrollment Windo Enrolling for the user cert Plesse enter your authentication F PIN PIN PIN Click here for mo	In the second se	X Cancel	Cancel	1.3 Sn Sn	3.6 na na	
Descend store contains 0 contificator	(10					2	
Personal store contains 9 certificates.								

Enter the pin

11. Finally, once you have seen the **Enrollment Successful** screen, you can then use this smartcard to log on to a domain-joined server, like the VCS with only the card and a known pin. However, it is not done yes, you still need to prepare the VCS to redirect authentication requests to the Smart Card and use Common Access Card to release the smartcard certificate stored on the smartcard for authentication.

-	Certificate Enrollment		_ D X
Γ	Certificate Installation Results The following certificates have been en	rolled and installed on this-computer.	
	Active Directory Enrolment Policy		
	® Yakkundig Smartcard Uber	✓ STATUS: Succeeded	Detalis ¥
		D	Vext user Oose

Configure the VCS for Common Access Card

Upload the Root CA to the Trusted CA Certificate list in the VCS by navigating to **Maintenance > Security > Trusted CA Certificate.**

2. Upload the Certificate Revocation List signed by the Root CA to the VCS. Navigate to **Maintenance > Security > CRL Management.**

3. Test your client certificate against your regex which pulls the username from the certificate to use for authentication against the LDAP or local user. The regex is going to match against the **Subject** of the certificate. This can be your UPN, Email and so on. In this lab, the email to match against the client certificate for the client certificate was used.

搹 Certificate	×
General Details Certification Path	
Show: <all></all>	\sim
Field Signature hash algorithm Issuer Valid from Valid to	Value ^ sha512 jajanson-2012DC-AD-CA, jaja Tuesday, October 17, 2017 5: Thursday, October 17, 2019 5
Subject Public key Public key parameters Certificate Template Inform	antman@jajanson.local, Scott RSA (1024 Bits) 05 00 Template=1 3 6 1 4 1 311 21
E = antman@jajanson.local CN = Scott Lang OU = Heroes DC = jajanson DC = local	
Ed	it Properties Copy to File
	OK

Subject of Client Certificate

4. Navigate to **Maintenance > Security > Client Certificate Testing**. Select the client certificate to be tested, in My lab it was antman.pem, upload it to the test area. In the **Certificate-based authentication pattern** section under **Regex to match against certificate** paste your regex to be tested. Do not change the **Username format** field.

My Regex: /Subject:.*email	Address=(?.*)@jajanson.local/m				
CISCO Cisco TelePresence Video Communication Server Expressway		This system had a starms			
Status System Configuration Applications Users Maintenance					
Client certificate testing		You are here: <u>Mantemance</u> / <u>Deputhy certificates</u> + Clien			
Client certificate					
	This tests whether a client certificate is valid when checked against the VCII's current trusted CA list and, if loaded, the revocation list				
Centrate source Uplease test for (PDI formage)					
Select the file you want to test	ou want to feed Booses. No file selected.				
Currently sploaded text file	antman peri				
Cirtilicate-based authentication pattern					
	This section applies only if your certificants contains authentication condentals and you want to use certificate-based authentication as your client certificate-based security secting, the nominated certificate is see if the certificate's condentals (the usersme) can be instituted.	It lets you test the outcome of applying regex and username format combinations to			
Report to match against bertificate	(Subject: "enail/ddfessen("koaptureCommonNamen" 1)@pijanson localim				
Username format	Augus Connohime				
	Main these satings permanent				

Test your regex in VCS



Testing Results

5. If the testing is providing you with the desired results then you can click the button **Make these changes permanent**. This changes your regex for the **Certificate-based authentication configuration** of the server. In order to verify the change, navigate to that configuration, **Maintenace > Security > Certificate-based authentication configuration**.

6. Enable client-based authentication by navigating to **System > Administrator** and then click or select drop down box to choose **Client certificate-based security = Client-Based Authentication.** With this setting, the user types the FQDN of the VCS server in his browser and he is prompted to choose his client account and enter the pin assigned to his Common Access Card. Then the certificate is released and he gets returned the Web GUI of the VCS server and all he needs to do is click or select the Administrator button. Then he is admitted into the server. If the options **Client certificate-based security = Client-Based Validation** is selected, the process is the same with the exception when the user clicks the Administrator button, he has prompted again for the admin password. Usually, the latter is not what the organization is trying to accomplish with CAC. CISCO Cisco Expressway-E

Status	System	Configuration	Applications	Users	Maintenance	
System	n administ	ration				
Epheme	eral port range er	ıd				* 49999
Servic	es					
Serial p	ort / console					0n 🗸 (į)
SSH se	rvice					0n 🗸 (j)
Web int	terface (over HT	(PS)				
		·				
Sessio	on limits					
Seccio	n time out (minute	.0)				+ 30
Des ser		2				
Per-acc	count session iim	r.				* •
System	i session limit					* 0
Syster	n protection					
Automa	ated protection se	ervice				On 🗸 👔
Automa	atic discovery pro	otection				0n 🗸 (j)
Web s	erver configura	ation				
Redirec	t HTTP requests	to HTTPS				On 🗸 (į)
HTTP S	trict Transport S	ecurity (HSTS)				0n 🗸 (į)
Web ad	Iministrator port					443 V
Client c	ertificate-based	security				Not required V
Save						Drop down the above box and choose
						GITENC-Dased Authentication
Relate	d tasks					
Upload	a CA certificate	file for HTTPS				
Test cli	ent certificates					

Enable client based authentication

Help! I am locked out!!!

If you enable the Client Based Authentication and the VCS rejects the certificate for whatever reason, you are not going to be able to log in with to the web GUI in the traditional way anymore. But, do not fret there is a way to get back into your system. The attached document can be found on the Cisco website and provides information on how to disable Client Based Authentication from root access.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.