# Configurer VCS avec CAC et un lecteur de carte à puce

### Contenu

Introduction <u>Conditions préalables</u> <u>Conditions requises</u> <u>Components Used</u> <u>Informations générales</u> <u>Qu'est-ce qu'une carte à puce ?</u> <u>Configuration</u> <u>Vérification</u> Dépannage

## Introduction

Ce document décrit un guide détaillé pour installer et utiliser un lecteur de carte à puce et une carte d'accès commune pour une utilisation avec le serveur de communication vidéo Cisco (VCS) pour les entreprises qui ont besoin d'une authentification à deux facteurs pour l'environnement VCS, comme les banques, les hôpitaux ou les gouvernements disposant d'installations sécurisées.

### Conditions préalables

### **Conditions requises**

Aucune spécification déterminée n'est requise pour ce document.

### **Components Used**

Les informations de ce document sont basées sur 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

### Informations générales

Le CAC fournit l'authentification requise afin que " systèmes " savoir qui a obtenu l'accès à leur environnement et quelle partie de l'infrastructure, qu'elle soit physique ou électronique. Dans les environnements classifiés du gouvernement et dans d'autres réseaux sécurisés, les règles d'accès " moins privilégiés " ou " doivent savoir " prévaloir. Une connexion peut être utilisée par n'importe qui, l'authentification nécessite quelque chose que l'utilisateur a, par exemple, le CAC, également connu sous le nom de Common Access Card, est né en 2006, de sorte que l'individu

n'aurait pas besoin d'avoir plusieurs appareils, qu'il s'agisse de postes, de cartes d'identité ou de dongles pour accéder à son lieu de travail ou à ses systèmes.

## Qu'est-ce qu'une carte à puce ?

Les cartes à puce sont un composant clé de l'infrastructure à clé publique (PKI) que Microsoft utilise pour s'intégrer à la plate-forme Windows, car les cartes à puce améliorent les solutions logicielles uniquement, telles que l'authentification des clients, la connexion et la messagerie sécurisée. Les cartes à puce constituent un point de convergence pour les certificats de clé publique et les clés associées car elles :

- Fournir un stockage résistant aux altérations pour la protection des clés privées et d'autres formes d'informations personnelles.
- Isoler les calculs stratégiques en matière de sécurité, qui impliquent l'authentification, les signatures numériques et l'échange de clés à partir d'autres parties du système qui n'ont pas besoin de savoir.
- Permettre la portabilité des informations d'identification et autres informations privées entre les ordinateurs au travail, à la maison ou en déplacement.

La carte à puce fait désormais partie intégrante de la plate-forme Windows, car les cartes à puce offrent de nouvelles fonctionnalités souhaitables, révolutionnaires pour l'industrie informatique comme l'introduction de la souris ou du CD-ROM. Si vous n'avez pas d'infrastructure d'ICP interne pour le moment, vous devez d'abord vous assurer de le faire. Ce document ne couvre pas l'installation de ce rôle dans cet article particulier, mais des informations sur la façon de le mettre en oeuvre peuvent être trouvées ici : <u>http://technet.microsoft.com/en-us/library/hh831740.aspx.</u>

# Configuration

Ce TP suppose que vous avez déjà intégré LDAP à VCS et que vous avez des utilisateurs capables de se connecter avec des informations d'identification LDAP.

- 1. Équipement de laboratoire
- 2. Installer la carte à puce
- 3. Configurer les modèles d'autorité de certification
- 4. Inscrire le certificat d'agent d'inscription
- 5. S'inscrire au nom de...
- 6. Configuration de VCS pour la carte d'accès commune

Équipement requis :

Serveur de domaine Windows 2012R2 doté des rôles et du logiciel installé suivants :

- Autorité de certification
- Active Directory
- DNS
- PC Windows avec carte à puce connectée
- vSEC : Logiciel de gestion CMS série K pour gérer votre carte à puce :



#### Logiciel Versa Card Reader

#### Installer la carte à puce

Les lecteurs de cartes à puce contiennent généralement des instructions sur la façon de connecter les câbles nécessaires. Voici un exemple d'installation pour cette configuration.

#### Installation d'un pilote de périphérique de lecteur de carte à puce

Si le lecteur de carte à puce a été détecté et installé, l'écran d'ouverture de session Welcome to Windows le reconnaît. Dans le cas contraire :

- 1. Connectez votre carte à puce au port USB de votre ordinateur Windows
- 2. Suivez les instructions à l'écran pour installer le pilote de périphérique. Cela nécessite le support du pilote que le fabricant de la carte à puce ou le pilote est détecté dans Windows. Dans mon cas, j'ai utilisé le pilote de fabrication à partir de leur site de téléchargement. NE FAITES PAS CONFIANCE AUX FENÊTRES.
- 3. Cliquez avec le bouton droit de la souris sur l'icône **Poste de travail** de votre bureau et cliquez sur **Gérer** dans le sous-menu.

- 4. Développez le noeud Services et applications, puis cliquez sur Services.
- 5. Dans le volet droit, cliquez avec le bouton droit de la souris sur **Carte à puce**. Cliquez sur **Propriétés** dans le sous-menu.
- 6. Dans l'onglet **Général**, sélectionnez **Automatique** dans la liste déroulante **Type de démarrage**. Click OK.
- 7. Redémarrez votre machine si l'assistant Matériel vous le demande.

Configurer les modèles d'autorité de certification

- 1. Lancez l'autorité de certification MMC à partir des outils d'administration.
- 2. Cliquez ou sélectionnez le noeud Modèles de certificats et sélectionnez Gérer.
- 3. Cliquez avec le bouton droit de la souris ou sélectionnez le modèle de certificat **utilisateur Smartcard**, puis sélectionnez **Dupliquer** comme indiqué dans l'image.

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 Purpo	ses	-	Actions		
Certification Authority (Local)	Administrator 1 4.1						Certificate Templates (2012DC-AD iai		
Certificate Templates (2012DC-AD.jajanson.loc	Authenticated Session	1	3.1				Marchaliana		
	Basic EFS	1	3.1				More Actions		
	CA Exchange	2	106.0	Private Key Arch	hival		Smartcard User		
	CEP Encryption	1	4.1				More Actions		
	Code Signing	1	3.1						
	Computer	1	5.1						
	Cross Certification Authority	2	105.0						
	Directory Email Replication	2	115.0	Directory Servic	e Email Replication				
	Domain Controller	1	4.1						
	Domain Controller Authentication	2	110.0	Client Authentie	cation, Server Authentication, Smart Card Logon				
	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 Authentie	cation, Server Authentication, Smart Card Logon, KD				
	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 Authenti	cation, Server Authentication				
	Root Certification Authority	1	5.1						
	Router (Offline request)	1	4.1						
	Smartcard Logon	1	6.1						
	Smartcard User	1	11.1		Duplicate Template				
	Smartcard User_VCS	4	101.6	Secure Email	ogon	- 11			
	Subordinate Certification Authority	1	5.1		All Tasks				
	I Trust List Signing	1	3.1		Properties	- 11			
	@ User	1	3.1		Help	~			
< III >	<				>				

Modèles de certificats de contrôleur de domaine

4. Dans l'onglet **Compatibility**, sous **Certification Authority**, passez en revue la sélection et modifiez-la si nécessaire.

compatibilité des cartes à puce

- 5. Dans l'onglet Général :
- a. Spécifiez un nom, tel que Smartcard User\_VCS.
- b. Définissez la période de validité sur la valeur souhaitée. Cliquez sur Apply.

de début générale de la carte à puce

- 6. Dans l'onglet Gestion des demandes :
- a. Définissez la fonction sur Signature et connexion par carte à puce.
- b. Cliquez sur **Demander à l'utilisateur lors de l'inscription.** Cliquez sur Apply.

Pro	perties of New	/ Template	X					
Subject Name	Server	Issuance Requirements						
Superseded Templ	ates Ext	ensions	Security					
Compatibility General	Request Handling	Cryptography	Key Attestation					
Purpose: Signa	urpose: Signature and smartcard logon							
	ludo ammetrio plan	rithma allowed k	with a subject					
	sude symmetric algo	ntrims allowed t	by the subject					
	chive subject s encry	ption private Ke	ey					
Allow private key to	be exported							
Renew with the sar	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:								
<ul> <li>Enroll subject without requiring any user input</li> </ul>								
Prompt the user du	ing enrollment							
Prompt the user during enrollment and require user input when the private key is used								
* Control is disabled du	e to <u>compatibility se</u>	<u>tings.</u>						
ОК	Cancel	Apply	Help					

demandes de carte à puce

7. Dans l'onglet **Cryptographie**, définissez la taille de clé minimale sur 2048.

a. Cliquez sur **Demandes doivent utiliser l'un des fournisseurs suivants**, puis sélectionnez **Fournisseur de chiffrement de carte à puce Microsoft Base**.

b. Cliquez sur Apply.

Prop	perties of New	/ Template	X
Subject Name	Server	Issuance F	Requirements
Superseded Templa	tes Ext	ensions	Security
Compatibility General	Request Handling	Cryptography	Key Attestation
Provider Category:	Legacy Crypto	ographic Service	Provider v
Algorithm name:	Determined by	v CSP	~
Minimum key size:	2048		
Choose which cryptogra	aphic providers can ny provider availab	be used for requ	iests 's computer
<ul> <li>Requests must use of</li> </ul>	one of the following	providers:	e comparer
Providers:			
Microsoft Base Smar Microsoft DH SChan Microsoft Enhanced Microsoft Enhanced Microsoft Enhanced	t Card Crypto Provi nel Cryptographic F Cryptographic Prov DSS and Diffie-He RSA and AES Cryp	der Provider rider v 1.0 Ilman Cryptograph otographic Provid	hic Pr
Request hash:	Determined by	y CSP	~
Use alternate signati	ure format		
ОК	Cancel	Apply	Help

chiffrement du certificat

8. Dans l'onglet Sécurité, ajoutez le groupe de sécurité auquel vous souhaitez donner accès à l'option Inscription. Par exemple, si vous voulez donner accès à tous les utilisateurs, sélectionnez le groupe Utilisateurs authentifiés, puis sélectionnez Autorisations **d'inscription** pour eux.

	Prope	erties of Nev	v Template		x		
Compatibility G	eneral F	Request Handling	Cryptograph	y Key Attestati	ion		
Subject Nam	Name Server Issuance Requirements						
Superseded	Template	s B	tensions	Security			
Group or user na	ames:						
& Authentica	ted Users						
🔏 Administrat	or (Admin)	@jajanson.local)					
Section Advancements Advancemen	lmins (JAJ	ANSON\Domain	Admins)				
Kan Enterprise	Admins (J/	AJANSON\Enter	prise Admins)				
			Add	Remove			
			,				
Permissions for	Authentica	ted Users	Allow	Deny	_		
Full Control							
Read			$\checkmark$				
Write							
Enroll							
Autoenroll							
					J		
For special perm	nissions or	advanced settin	gs, click	Advanced	1		
Advanced.							
	ОК	Cancel	Apply	Help			
		m	odèles				

9. Cliquez sur **OK** afin de finaliser vos modifications et de créer le nouveau modèle. Votre nouveau modèle doit maintenant apparaître dans la liste des modèles de certificat.

🖀 Console1 - [Console Root\Certificate Templates (2012DC-AD.jajanson.local)]									
🖀 File Action View Favorites Window Hel	p					_ 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			Mare Actions A			
	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						
	R Exchange Enrollment Agent (Offline requ	1	4.1						
	Exchange Signature Only	1	6.1						
	R 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 >	<	ш							
36 certificate templates									

Modèle vu dans le contrôle de domaine

10. Dans le volet gauche du MMC, développez Autorité de certification (locale), puis développez votre Autorité de certification dans la liste Autorité de certification.

Cliquez avec le bouton droit sur Modèles de certificats, cliquez sur **Nouveau**, puis sur **Modèle de certificat** pour émettre. Choisissez ensuite le nouveau modèle de carte à puce.

<b>a</b>	Console1 - [Console Roo	t\Certification Authority (Local)\ja	janson-2012DC-AD-CA\Certificate Templates]		_ D X
🚡 File Action View Favorites Window Help					_ 8 ×
🗢 🔿 🙍 🖬 🖉 📷					
Console Root	Name	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		Mars Antions	
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 Kequests	Smartcard User_VCS	Secure Email, Client Authentication, Sm			
Failed Requests	VCS_Login_SMART	Smart Card Logon, Client Authentication			
Manage	: Agent	Certificate Request Agent			
Maria	mail Replication	Directory Service Email Replication			
New	ontroller Authentication	Client Authentication, Server Authentic			
View	<ul> <li>uthentication</li> </ul>	Client Authentication, Server Authentic			
New Window from H	Here try Agent	File Recovery			
New Taskpad View		Encrypting File System			
	ontroller	Client Authentication, Server Authentic			
Kefresh	r	Server Authentication			
Export List		Client Authentication, Server Authentic			
Help		Encrypting File System, Secure Email, Cl			
		<all></all>			
1	Administrator	Microsoft Trust List Signing, Encrypting			
				10	

Émettre un nouveau modèle

11. Une fois le modèle répliqué, dans MMC, cliquez avec le bouton droit de la souris ou sélectionnez la liste Autorité de certification, cliquez sur **Toutes les tâches**, puis cliquez sur **Arrêter le service**. Ensuite, cliquez à nouveau avec le bouton droit sur le nom de l'Autorité de certification, cliquez sur **Toutes les tâches**, puis sur **Démarrer le service**.



Arrêter puis démarrer les services de certificats

#### S'inscrire au certificat d'agent d'inscription

Il est recommandé d'effectuer cette opération sur un ordinateur client (bureau des administrateurs informatiques).

1. Lancer MMC choisissez **Certificates**, cliquez sur **Ajouter** puis certificats pour **Mon compte d'utilisateur**.



Ajouter des certificats

2. Cliquez avec le bouton droit de la souris ou sélectionnez le **noeud personnel**, sélectionnez **Toutes les tâches**, puis sélectionnez **Demander un nouveau certificat**.

Console1 - [Console Root\Certificates - Current User\Personal]	_ <b>D</b> X
File Action View Favorites Window Help	_ 5 ×
Console Root Object Type	Actions
△ 🛱 Certificates - Current User 📫 Certificates	Personal
▷ Pe ▷ Tr Find Certificates	More Actions
En All Tasks Find Certificates	
▶ Call Inf	
Import       Import	
▷ 🗍 Ur New Taskpad View Advanced Operations ▶	
N C Tr Refresh	
CI Export List	
⊳ 🛄 C∉ Help	
Certification Authority (Loc	
⊳ 🛃 jajanson-2012DC-AD-C/	
< III >	
Personal store contains 9 certificates.	

Demander de nouveaux certificats

3. Cliquez sur **Suivant** dans l'Assistant, puis sélectionnez **Stratégie d'inscription Active Directory**. Cliquez ensuite de nouveau sur **Suivant**.

	Concola 1 - [Concola Doot) Cartificator - Current Llear Darconall	
The Action View	📮 Certificate Enrollment	
Console Root  Certificates - Curren  Certificates - Curren  Final Personal  Final Trusted Root Certificate Certifi	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 Inal A Iore Actions
Active Directory	Configured by your administrator	
Trusted Publishe	Active Directory Enrollment Policy 🗸	
<ul> <li>Untrusted Certifi</li> <li>Third-Party Root</li> <li>Trusted People</li> <li>Client Authentic</li> <li>Certificate Enroll</li> <li>Smart Card Trust</li> <li>Certification Author</li> <li>jajanson-2012DC</li> </ul>	Configured by you Add New	
< 111	Next Cancel	
Personal store contains 9 cere	111.01(5).	

Inscription à Active Directory

4. Sélectionnez le **certificat d'agent d'inscription**, dans ce cas, **Smartcard User\_VCS** puis cliquez sur **S'inscrire**.



Agent de certificat d'inscription

Votre bureau Administrateurs IT est maintenant configuré en tant que poste d'inscription, ce qui vous permet d'inscrire de nouvelles cartes à puce au nom d'autres utilisateurs.

#### S'inscrire au nom de...

Pour que vous puissiez maintenant fournir aux employés des cartes à puce pour l'authentification, vous devez les inscrire et générer le certificat qui est ensuite importé sur la carte à puce.



S'inscrire au nom de

1. Lancez MMC et importez le **module Certificates et gérez** les certificats de mon compte d'utilisateur.

2. Cliquez avec le bouton droit de la souris ou sélectionnez **Personnel > Certificats** et sélectionnez **Toutes les tâches > Opérations avancées** et cliquez sur **S'inscrire au nom de...** 

3. Dans l'Assistant, sélectionnez la stratégie d'inscription Active Directory, puis cliquez sur **Suivant**.



#### S'inscrire au nom avancé

Console1 - [Console Root],Certificates - Current User/Personall,Certificates]									- 0 X
🖀 file Action View Favorites Window He	lp .								_ 0 ×
🗢 🔶 🙇 💼 🖬 💼									
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Cen	Actions	
a Personal	Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	«None»		Adr	Certificates	-
Cartificates	Administrator				- 0 X			More Actions	,
<ul> <li>Enterprise Trust</li> </ul>	Administrator	Certificate Encollment					Enro		
b Intermediate Certification Authorities	PIVKey 8094	Commence anomation			_		134		
<ul> <li>D III Trusted Publishers</li> </ul>	Scott Lang	Before You Begin					Sma		
b III Untrusted Certification Direct Party Root Certification Authorities	Scott Lang	The first second s					Sma		
p Trusted People		networks, protect content, establish identity	and do other security	related tasks.	nnect to wreeks				
<ul> <li>Dient Authentication Issuers</li> <li>Cartificate Envolment Requests</li> </ul>		Before requesting a certificate, verify the foll	owing						
5 11 Smart Card Trusted Roots		Your computer is connected to the network							
		You have credentials that can be used to ver	ify your right to obtain	the certificate					
					_				
				Next	t Cancel				
	-								
	-						_		
Personal store contains 9 certificates.	5						2		
							_	1	

4. Sélectionnez Stratégie d'inscription de certificat, puis cliquez sur Suivant.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]									- 🗆 X
Tile Action View Favorites Window Hel	lp .								_ 8 ×
(+ +) 2 🗊 🗓 🙆 🔂 🗊									
<ul> <li>File Action View Favorites Window Hel</li> <li>Console Root</li> </ul>	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.	<						>		

Stratégie d'inscription

5. Vous êtes maintenant invité à sélectionner le **certificat de signature**. Il s'agit du certificat d'inscription que vous avez demandé précédemment.

<b>ä</b>		Con	sole1 - [Console Root\Certific	ates - Current U	ser\Personal\Certifi	cates]				= 🗆 X	
File Action View Favorites Window He	lp									_ 8 ×	
Console Root	Issued To	•	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status C	Certi /	Actions		
a 🔛 Personal	Administrator	Administrator	jajanson-2012DC-AD-CA	10/12/2019 Cert	Microsoft Trust List	<none></none>	A	Adm	Certificates	-	
Certificates Trusted Root Certification Authorities	Administrator					_ 🗆 X			More Actions	,	
Enterprise Trust Intermediate Certification Authorities	jajanson-2012	📮 Certificate	Windo	ws Security	X			Enro			
Active Directory User Object	Scott Lang			ino occurrey			1.3.0	1.3.6 Sma	6		
<ul> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> </ul>	Scott Lang	Select I	Select a Certificate				s	Sma			
Third-Party Root Certification Authorities	Scott Lang	You need				her users. Click	S	Sma			
<ul> <li>Irusted People</li> <li>Client Authentication Issuers</li> </ul>		Browset	Administrato	12DC-AD-CA							
Certificate Enrollment Requests			Valid From: 10/14	/2017 to 10/14/2019							
p Smart Card Hosted Roots		Signing	Click here to view	cartificate		2					
			properties	B		Browse					
				Administrator	r						
			Issuer: jajanson-2	012DC-AD-CA							
			Valid From: 10/12	2/2017 to 10/12/2019							
				01	Cancel						
						Cancel					
						Cancer					
	<							>			
Personal store contains 9 certificates.											

Sélectionner un certificat de signature

6. Dans l'écran suivant, vous devez accéder au certificat que vous souhaitez demander et dans ce cas, c'est **Smartcard User\_VCS** qui est le modèle que vous avez créé précédemment.

<b>a</b>		Console1 - [Console Root\Certifie	cates - Current Us	ser\Personal\Certifi	cates]			_ <b>D</b> X
File Action View Favorites Window He	lp							_ & ×
<ul> <li>File Action View Favorites Window He</li> <li>Action View Favorites Window He</li> <li>Console Root</li> <li>Certificates - Current User</li> <li>Personal</li> <li>Certificates - Current User</li> <li>Intermediate Certification Authorities</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authorities</li> <li>Active Directory User Object</li> <li>Trusted Publishers</li> <li>Trusted Pool Certificates</li> <li>Trusted Pool Certificates</li> <li>Certificate Enrollment Requests</li> <li>Smart Card Trusted Roots</li> </ul>	Ip	Console1 - [Console Root\Certific Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA ertificate Enrollment Request Certificates You can request the following types of certific click Next. Cick Next. Cick Next. Cick Next. Cick Next. Cick Next. Cick Next. Cick Next. Cick Next. Show all templates	ates - Current Us Expiration Date In/14/2019 10/12/2018 tetes. Select the certific StartUS: Availat StartUS: Availat StartUS: Availat StartUS: Availat StartUS: Availat	ser/Personal/Certifi Intended Purposes Certificate Request Microsoft Trust List cates you want to reque cates you want to reque ole click here to configure ole click here to configure ole le	cates]	Status	Certi Actions Certificate: More Act I.3.6 Sma Sma Sma	ions i
	<		1				>	
Personal store contains 9 certificates.								

Choisir la carte à puce VCS

7. Ensuite, vous devez sélectionner l'utilisateur auquel vous souhaitez vous inscrire pour le compte de. Cliquez sur **Parcourir** et saisissez le nom d'utilisateur de l'employé que vous souhaitez inscrire. Dans ce cas, Scott Lang 'antman@jajanson.local account' est utilisé.

·		Console1 - [Console Root\Certi	ficates - Current U	ser\Personal\Certif	icates]				_ 🗆 X
Tile Action View Favorites Window He	lp								_ 8 ×
🗢 🔿 🙇 🖬 💷									
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
a 💭 Certificates - Current User	Administrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request	<none></none>		Enro	Certificates	
A Personal	Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	<none></none>		Adm	More Actions	•
Trusted Root Certification Authorities	Administrator				_ 🗆 X		Enro		
Enterprise Trust	jajanson-2012	Select User	×				Enito		
Active Directory User Object	PIVKey BD9A5	Calact this shiast type:					1.3.6	5	
Trusted Publishers	Scott Lang	User	Obi	ct Tunes			Sma		
Untrusted Certificates	Scott Lang	Error this location:	Cop	or types			Sma		
Find-Party Root Certification Authorities     Find People		jajanson Jocal	La	n name	of that user. For				
Client Authentication Issuers									
Certificate Enrollment Requests		Enter the object name to select (examples):		e needs t	o be installed is				
Smart Card Trusted Roots		Scott Long to an anticide state for the day	Che	ok Names					
		Advanced	ОК	Cancel	Browse				
				al	growsen				
					Cancel				
						_			
Personal store contains 9 certificates.							>		
· · · · · · · · · · · · · · · · · · ·									

Choisir l'utilisateur

8. Dans l'écran suivant, poursuivez l'inscription en cliquant sur **Inscription**. Maintenant, insérez une carte à puce dans votre lecteur.

		Console1 - [Console Root\Certif	cates - Current U	ser\Personal\Certifi	cates]				_ 🗆 X
Tile Action View Favorites Window Hel	lp								_ 8 ×
(* 🔿 🖄 🛅 📋 🙆 🔂 📆									
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
A Personal	Administrator	jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA	10/14/2019 10/12/2018	Certificate Request Microsoft Trust List	<none> <none></none></none>		Adm	Certificates	•
Certificates	Administrator	14			X			More Actions	•
<ul> <li>Frusted Root Certification Authorities</li> <li>Enterprise Trust</li> </ul>	Administrator	utificate Carolineant					Enro		
Intermediate Certification Authorities	PIVKey BD9A5	uncate enronment					1.3.6		
Finite Directory oser Object Finite Directory oser Object Finite Directory oser Object	Scott Lang	Select a user					Sma	a a	
Directory Control Certificates Directory Certification Authorities	Scott Lang	To request a certificate on hebalf of another u	rar anter the formal		of that user For		Sma		
Trusted People		To request a certificate on behait of another user, enter the formal name or domain name of that user. For example, Firstname Lastname, username, or domain\username.							
<ul> <li>Client Authentication Issuers</li> <li>Certificate Enrollment Requests</li> </ul>	Client Authentication Issuers Centificate Enrollment Requests Before enrolling for a certificate, make sure the device on which the user certificate needs to be installed is								
Smart Card Trusted Roots	4	attached.							
		JAJANSON\antman			Browse				
				Enrol	I Cancel				
	<						>		
Personal store contains 9 certificates.	11							•	

#### Inscrire

9. Une fois que vous avez inséré votre carte à puce, elle est détectée comme suit :

Reques		Windows Security	×		
The enrol	Enrolling for t Select a smart car	he user certificate. I device			
®1#		xalto Cryptoflex .NET multo USB Smart Card Reader 0 e smart card is ready for use.	Cancel		

10. Il vous est ensuite demandé de saisir un code PIN de carte à puce (code PIN par défaut : 0000).

<b>a</b>	Con	sole1 - [Console Root\Certific	ates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
File Action View Favorites Window Hel	lp							_ 8 ×
🗢 🔿 🙍 🔟 🔯 📾								
Centificates - Current User  Certificates - Current User  Certificates  Certificates  Certificates  D  Tusted Root Certification Authorities  D  Certificates	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	•
<ul> <li>Distance in the intermediate Certification Authorities</li> <li>Active Directory User Object</li> <li>Trusted Publishers</li> <li>Third-Party Root Certificates</li> <li>Third-Party Root Certification Authorities</li> <li>Third-Party Root Certificates</li> <li>Client Authentication Issuers</li> <li>Certificate Enrollment Requests</li> <li>Smart Card Trusted Roots</li> </ul>	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.								

Entrez la broche

11. Enfin, une fois que vous avez vu l'écran **Inscription réussie**, vous pouvez utiliser cette carte à puce pour vous connecter à un serveur joint au domaine, comme le serveur VCS avec seulement la carte et une broche connue. Cependant, il n'est pas fait oui, vous devez toujours préparer le VCS pour rediriger les demandes d'authentification vers la carte à puce et utiliser la carte d'accès commune pour libérer le certificat de carte à puce stocké sur la carte à puce pour l'authentification.

etificate Enrollment		_ <b>D</b> X
Certificate Installation Results		
Active Directory Services have been enrolle	d and initialied on this computer.	
® Valkundig Smartcard User	✓ STATUE: Succeeded	Details ¥
		Next user Oose

Configuration de VCS pour la carte d'accès commune

Téléchargez l'autorité de certification racine dans la liste des certificats de l'autorité de certification de confiance dans le VCS en accédant à **Maintenance > Security > Trusted CA Certificate.** 

2. Téléchargez la liste de révocation de certificats signée par l'autorité de certification racine dans le VCS. Accédez à **Maintenance > Security > CRL Management.** 

3. Testez votre certificat client par rapport à votre regex qui extrait le nom d'utilisateur du certificat à utiliser pour l'authentification contre l'utilisateur LDAP ou local. Le regex va correspondre avec l'**Objet** du certificat. Il peut s'agir de votre UPN, de votre e-mail, etc. Au cours de ces travaux pratiques, l'e-mail à comparer au certificat client pour le certificat client a été utilisé.

搹 Certificate	$\times$
General Details Certification Path	
Show: <all></all>	$\sim$
Field Signature hash algorithm Issuer Valid from	Value ^ sha512 jajanson-2012DC-AD-CA, jaja Tuesday, October 17, 2017 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

Objet du certificat client

4. Accédez à **Maintenance > Security > Client Certificate Testing**. Sélectionnez le certificat client à tester, dans Mon laboratoire c'était antman.pem, téléchargez-le dans la zone de test. Dans la section **Modèle d'authentification basé sur les certificats** sous **Regex pour correspondre au certificat** collez votre regex à tester. Ne modifiez pas le champ **Format du nom d'utilisateur**.

My Regex: /Subject:.*ema	ilAddress=(?.*)@jajanson.loc	al/m				
cift.iti CISCO Cisco TelePresence Video Communication Server Expressway		This system has a atoms				
Status System Configuration Applications Users Maintenance						
Client certificate testing		You are here: <u>Maintenance</u> · <u>Deputy</u> certificates · Che				
Client certificate						
Carificate source	This tests whether a client certificate is valid when checked against the VCI's current trusted CA lan [Uplicated test Tim (PEM format)] ()	and, if leaded, the revocation list				
Select the file you want to test	Brown, No file selected.					
Currently uploaded text file	antras par					
Centificate based authentication pattern						
	This section applies only if your certificate contains authentication oredentials and you want to use o the nominated certificate to see if the certificate's oredentials (the usename) can be exhacted.	enficiate-based authentication as your othert centificate-based security setting. It lets you test the outcome of applying topics and usemame format combinations to				
Repex to match agenal certificate	dutject."ematAddressr(%captureCommonNamen:")@pijanson.localim	<i>b</i>				
Gaenane format	*ceptureCommonName#	u (				
	Make these settings permanent					

Testez votre regex dans VCS



Résultats des tests

5. Si le test vous fournit les résultats souhaités, vous pouvez cliquer sur le bouton **Rendez ces modifications permanentes**. Cela modifie votre rég pour la **configuration de l'authentification basée sur les certificats** du serveur. Afin de vérifier la modification, accédez à cette configuration, **Maintenace > Security > Certificate-based authentication configuration.** 

6. Activez l'authentification basée sur le client en naviguant vers System > Administrator puis cliquez sur ou sélectionnez une zone déroulante pour sélectionner Client certificate-based security = Client-Based Authentication. Avec ce paramètre, l'utilisateur tape le nom de domaine complet du serveur VCS dans son navigateur et il est invité à choisir son compte client et à saisir la broche attribuée à sa carte d'accès commune. Le certificat est ensuite libéré et il est renvoyé à l'interface utilisateur graphique Web du serveur VCS et tout ce qu'il doit faire est de cliquer ou sélectionner le bouton Administrateur. Puis il est admis dans le serveur. Si les options Sécurité basée sur le certificat du client = Validation basée sur le client sont sélectionnées, le processus est le même, sauf lorsque l'utilisateur clique sur le bouton Administrateur, il a demandé à nouveau le mot de passe administrateur. Habituellement, ce dernier n'est pas ce que l'organisation essaie d'accomplir avec CVC.

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					

Activer l'authentification basée sur le client

Aide ! Je suis enfermé ! ! !

Si vous activez l'authentification basée sur le client et que le VCS rejette le certificat pour une raison quelconque, vous ne pourrez plus vous connecter à l'interface utilisateur graphique Web de manière traditionnelle. Mais ne vous inquiétez pas, il y a un moyen de revenir dans votre système. Le document ci-joint se trouve sur le site Web de Cisco et fournit des informations sur la façon de désactiver l'authentification basée sur le client à partir de l'accès racine.

### Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.