# CACおよびスマートカードリーダーを使用した VCSの設定

### 内容

<u>概要</u>
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>スマートカードとは</u>
<u>設定</u>
<u>確認</u>
トラブルシュート

### 概要

このドキュメントでは、Cisco Video Communication Server(VCS)で使用するSmart Card ReaderおよびCommon Access Card(CCC)ログインをインストールして使用する手順を説明しま す。これは、銀行、病院、または政府機関などのVCS環境に2要素認証を必要とするとする組織 です。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco Expressway Administrator(X14.0.2)に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

### 背景説明

CACは必要な認証を提供するため、「システム」は環境にアクセスできるユーザと、インフラス トラクチャのどの部分が物理的または電子的であるかを認識します。政府が分類した環境、およ びその他のセキュアなネットワークでは、「最小特権アクセス」または「知る必要がある」とい うルールが優先されます。ログインは誰でも利用できます認証にはCACが持っているものを必要 としますCACは2006年に登場しました個人が複数のデバイスを持つ必要はありません例えばfobs, id card, donglesです

# スマートカードとは

スマートカードは、クライアント認証、ログオン、および安全な電子メールなどのソフトウェア のみのソリューションを強化するため、MicrosoftがWindowsプラットフォームに統合するために 使用する公開キーインフラストラクチャ(PKI)の主要コンポーネントです。スマートカードは、公 開キー証明書と関連キーを統合するポイントです。その理由は次のとおりです。

- 秘密鍵およびその他の個人情報を保護するための改ざん防止ストレージを提供します。
- セキュリティクリティカルな計算を切り分けます。この計算には、認証、デジタル署名、およびシステムの他の部分からのキー交換が含まれます。これらの情報を知る必要はありません。
- ・職場、自宅、または外出先のコンピュータ間で、クレデンシャルやその他のプライベート情報のポータビリティを有効にします。

スマートカードは、マウスやCD-ROMの導入と同様に、コンピュータ業界に画期的な新しい望ま しい機能を提供するため、Windowsプラットフォームの不可欠な要素となっています。 現時点 で内部PKIインフラストラクチャがない場合は、最初にこれを行う必要があります。このドキュ メントでは、この記事でこのロールをインストールする方法については説明しませんが、この機 能の実装方法については、次のリンクを参照してください。<u>http://technet.microsoft.com/en-</u> us/library/hh831740.aspx にアクセスしてください。

### 設定

この実習では、LDAPとVCSがすでに統合されており、LDAPクレデンシャルでログインできるユ ーザがいることを前提としています。

- 1. ラボ機器
- 2. スマートカードの取り付け
- 3. 認証局テンプレートの設定
- 4. 登録エージェント証明書の登録
- 5. <u>の代理で登録....</u>
- 6. <u>共通アクセスカード用のVCSの設定</u>

必要な機器:

次の役割またはインストールされたソフトウェアを持つWindows 2012R2ドメインサーバ:

- 認証局
- Active Directory
- DNS
- スマートカードが接続されたWindows PC
- •vSEC:スマートカードを管理するためのCMS Kシリーズ管理ソフトウェア:



Versa Card Readerソフトウェア

スマートカードの取り付け

通常、スマートカードリーダーには、必要なケーブルの接続方法に関する指示が記載されていま す。この設定のインストール例を次に示します。

スマートカードリーダーデバイスドライバのインストール方法

スマートカード読み取り装置が検出され、インストールされている場合は、[Windowsログオンへ ようこそ]画面で確認できます。そうでない場合:

- 1. スマートカードをWindows PCのUSBポートに接続します
- 2. 画面の指示に従って、デバイスドライバソフトウェアをインストールします。これには、ス マートカードまたはドライバの製造元がWindowsで検出されているドライバメディアが必要 です。私の場合、私は彼らのダウンロードサイトからメーカーのドライバを使用しました。 WINDOWSを信頼しないでください。
- 3. デスクトップの[マイコ**ンピュータ**]アイコンを右クリックし、サブメニューの[管理]をクリッ クします。

- 4.「サービスとアプリケー**ション」ノードを展開**し、「サービス」をクリ**ックします**。
- 5. 右側のペインで、[スマートカード]を右クリ**ックします**。サブメニュー**の「プロ**パティ」を クリックします。
- 6. [全般]タ**ブ**で、[スタートアップ**タイプ]**ドロップダウン**リストの[自動**]を選択します。[OK] を クリックします。

7. ハードウェアウィザードで指示された場合は、マシンを再起動します。

認証局テンプレートの設定

- 1. [管理ツール(Administrative Tools)]から認証局(CA)MMCを起動します。
- 2. [証明書テンプレート]ノードをクリックまたは選択し、[管理]を選択します。
- 3. 右クリックするか、[Smartcard User Certificate Template]を選択し、図のように [Duplicate]を選択します。

<b>a</b>	Console1 - [C	onsole Root\Certifie	ate Temp	lates (2012DC	-AD.jajanson.local)]		_ <b>D</b> X
🚟 File Action View Favorites Window Help	>						_ 8 ×
							<u></u>
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				Marchatiana
	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			- 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 A	gent		
	OCSP Response Signing	3	101.0	OCSP Signing			
	RAS and IAS Server	2	101.0	Client Authentie	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	- 11	
	Trust List Signing	1	3.1		Properties		
	2 User	1	3.1		Help	$\overline{}$	
< III >	<				)		

ドメインコントローラ証明書テンプレート

4. [Compatibility]タブの[Certification Authority]で、選択を確認して、必要に応じて変更します。

Smartca	ard User_VCS I	Properties	? X
Subject Name	ls	suance Require	ements
Superseded Templates	Extensions	Security	Server
General Compatibility Re	equest Handling	Cryptography	Key Attestation
The template options availate versions set in Compatibility	able are based on t y Settings. s	he earliest oper	ating system
Compatibility Settings			
Windows Server 2012	R2	~	
Certificate recipient Windows 8.1 / Windov	ws Server 2012 R.	×	
These settings may not pre template.	event earlier operati	ng systems from	1 using this

性の設定

5. [General]タブ**で次の**操作を行います。

a.名前を指定します(Smartcard User\_VCSなど)。

b.有効期間を目的の値に設定します。[Apply] をクリックします。

開始時間の有効期限

6. 「要求の処理」**タブで**は、次を行います。

a.[Purpose]を[Signature]および[smartcard logon]に設定します。

b.[登録時にユーザーにプロンプトを表示]をクリックします。[Apply] をクリックします。

	Prop	perties	of New	/ Template		
Subject I	Name	Sen	ver	Issuance	Requiren	nents
Superse	ded Templa	tes	Ext	ensions	Sec	curity
Compatibility	General	Request	Handling	Cryptography	y Key A	Attestation
Purpose:	Signat	ture and s	martcard	logon		¥
	Del	ete revok	ed or expi	red certificates	(do not a	rchive)
	_ Incl	lude symm	etric algo	rithms allowed l	by the sub	bject
	Arc	hive subje	ct's encry	ption private k	ey	
Allow priv	vate key to	be exporte	ed			
	محمد مطغ طقن	- Leev (*)				
	with the sam	le key ()				1
new key	cannot be (	created (*)	card cer	tificates, use th	e existing	кеуга
Do the follow	wing when t with this cert	he subject	t is enrolle ised:	ed and when th	e private	key
	hiect withou	t requiring	anv user	innut		
0 -	bjeet minoe	it requiring	any asor	npar		
<ul> <li>Prompt the</li> </ul>	he user duri	ng enrollm 	ent			
Prompt the private k	he user duri: ev is used	ng enrollm	ent and re	equire user inpu	t when th	he
	.,					
* Control is a	disabled due	e to <u>compa</u>	atibility set	tings.		
]	OK		Canad	Analy		Hele
l	UK		Jancei	Арріу		пер
				の処理		

7. [暗号化]タブで、最小キーサイズを2048に設定します。

a.[Requests must use **one the following providers]をクリックし、**[**Microsoft Base Smart Card Crypto Provider]を選択します**。

b. 「適用」をクリ**ックします**。

	Prop	perties	of New	Templat	te		X
Subject Na	ame	Sen	ver	Issuan	ce Req	uiremer	nts
Supersed	ed Templa	tes	Ext	ensions		Secur	ity
Compatibility	General	Request	Handling	Cryptogra	phy	Key Atte	estation
Provider Cate	egory:	Lega	acy Crypto	graphic Ser	vice Pr	ovider	~
Algorithm nar	ne:	Dete	ermined by	CSP			~
Minimum key	size:	2048	3				
Choose whicl	h cryptogra	aphic prov	iders can	be used for	reques	ts	
◯ Requests	can use a	ny provide	er availabl	e on the sub	ject's c	compute	er
Requests	must use (	one of the	following	providers:			
Providers:							
Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft Microsoft	Base Smar DH SChan Enhanced Enhanced Enhanced	t Card Cry nel Crypto Cryptogra DSS and RSA and	pto Provid ographic P phic Prov Diffie-Hel AES Cryp	der Irovider ider v1.0 Iman Cryptog tographic Pr	graphic rovider	^ ≡ Pr	
Request has	n:	Dete	ermined by	CSP			~
Use alternate signature format							
	_						
	OK	(	Cancel	Appl	y	H	lelp

証明書暗号化設定

8. [セキュリティ]タブで、登録アクセス権を付与するセキュリティグループを追加します。たと えば、すべてのユーザーにアクセス権を付与する場合は、[認証済みユーザー]グループを選択し、 そのグループに対して[登**録]権限**を選択します。

. Ar fight.	Proj	perties o	f New	Template	×	
Compatibility	General	Request H	landling	Cryptography	Key Attestation	
Subject N	lame	Serve	er	Issuance R	equirements	
Superse	ded Templa	ites	Exte	ensions	Security	
Group or use	er names:					
& Authen	ticated Use	ers				
🤱 Adminis	trator (Adm	in@jajansor	n.local)			
Section 2010	Admins (J.	AJANSON\I	Domain A	dmins)		
Ma Enterpr	ise Admins	(JAJANSON	N\Enterpr	ise Admins)		
			Γ	Add	Remove	
Permissions	for Authent	icated Users	8	Allow	Deny	
Full Contro	bl					
Read				✓		
Write						
Enroll				$\checkmark$		
Autoenrol						
For special p	emissions	or advance	d setting:	s, click	Advanced	
Advanced.					, aranood	
[	ОК	Ca	ancel	Apply	Help	

ユリティ

9. [**OK**]をクリックして、変更を確定し、新しいテンプレートを作成します。新しいテンプレート が[証明書テンプレート(Certificate Templates)]のリストに表示されます。

Sec. 1997	Console1 - [Console Root\Certifi	icate Templ	ates (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)	1	3.1			Certificate Templates (2012DC-AD.jaj +
Certificate Templates (2012DC-AD.jajanson.loc) Computer	1	5.1			More Actions
Cross Certification Authority	prity 2	105.0			indicación /
Directory Email Replicati	on 2	115.0	Directory Service Email Replication		Smartcard User_VCS
Domain Controller	1	4.1			More Actions
Domain Controller Authority	entication 2	110.0	Client Authentication, Server Authentication, Smart Card Logon		
EFS Recovery Agent	1	6.1			
R Enrollment Agent	1	4.1			
R Enrollment Agent (Com	puter) 1	5.1			
Exchange Enrollment Ag	ent (Offline requ 1	4.1			
R Exchange Signature Only	r 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, KE		
Rev 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 Autho	rity 1	5.1			
Router (Offline request)	1	4.1			
Smartcard Logon	1	6.1			
Smartcard User	1	11.1			
Smartcard User_VCS			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		
R Web Server	1	4.1			
Webclientandserver	2	100.4	Client Authentication, Server Authentication		
Workstation Authenticat	ion 2	101.0	Client Authentication	~	
< III > <	ш		>		
36 certificate templates					

ドメイン制御で表示されるテンプレート

10. MMCの左側のペインで、[Certification Authority (Local)]を展開し、[Certification Authority]リ スト内のCAを展開します。

[Certificate Templates]を右クリックし、[**New**]をクリック**し**、[**Certificate Template to** Issue]をク リックします。次に、新しく作成したスマートカードテンプレートを選択します。

<b>a</b>	Console1 - [Console Roo	ot\Certification Authority (Local)\jajanson-2012DC-AD-CA\Certificate Templates]		_ 🗆 X
Tile Action View Favorites Window He	lp			- 8 ×
◆ → <b>2</b> 🖬 Q 🕞 🖬 🖬				
Console Root	Name	Intended Purpose	Actions	
D Certificate Templates	Schange Enrollment Agent (Offline r	Certificate Request Agent	Certificate Templates	
Certification Authority (Local)	IPSec (Offline request)	IP security IKE intermediate	Mars Actions	
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		
New	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	Here try Agent	File Recovery		
New Taskend View		Encrypting File System		
INEW TASKPAG VIEW	ontroller	Client Authentication, Server Authentic		
Refresh	*	Server Authentication		
Export List		Client Authentication, Server Authentic		
Help		Encrypting File System, Secure Email, Cl		
Tieb		<all></all>		
	Administrator	Microsoft Trust List Signing, Encrypting		

新しいテンプレートの発行

11.テンプレートが複製された後、MMCで[証明機関]の一覧を右クリックまたは選択し、[すべて のタスク]をクリックして、[サービスの停止]をクリ**ックしま**す。次に、CAの名前を再度右クリッ クし、[すべてのタスク]をクリック**し、[サービ**スの開始]をクリ**ックします**。

	Console1 - [Console Root\Certification Authority (Local)\jajanson-2012DC-AD-CA]	_ <b>D</b> X
🖀 File Action View Favorites Window He	lp	_ 6 ×
◆ → 2 📷 🖾 ৫ 🕞 🛛 🖿 🕨		
🛗 Console Root	Name	Actions
Certificate Templates	Revoked Certificates	jajanson-2012DC-AD-CA
4 jainson 2012DC AD CA	lissued Certificates	More Actions
All Tasks +	Start Service	
View +	Stop Service	
New Window from Here	Submit new request	
New Taskpad View	Back up CA	
Refresh	Restore CA	
Export List	Renew CA Certificate	
Properties		
Help		
1		
1		
Contains actions that can be performed on the item.		

証明書サービスを停止してから開始する

### 登録エージェント証明書への登録

これは、クライアントマシン(IT Administrators Desktop)で行うことをお勧めします。

1. MMCを起動し、[証明書]を選**択し**、[追加]をクリックして、[マイユーザアカウント]の証明書 をクリックします。

<b></b>		Console1 - [Console Root]	_ 🗆 X
File Action View Favorites Window He	lp		_ <i>6</i> ×
	1		
Console Root	Name	Actions	
		There are no items to show in this view. Console Root	•
		Add or Remove Snap-ins X More Actions	,
		You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins:         You can select snap-in will always manage cetificates for:         You can select Templates         Morosoft Cor         You cerificates Templates         Morosoft Cor         You cerificates map-in allows you to browse the contents of the selected snap in allows you to browse the contents of the selected snap-in allows you to browse the contents of the selected snap-in allows you to browse the contents of the selected snap-in allows you to browse the contentselected snap-in allows you to browse the contentselec	
I			

証明書の追加

2. 右クリックするか、[個人ノード]を選択し、[すべてのタスク]を選択し、[新規証明書の要求]を 選択します。

Console1 - [Console Root\Certificates - Current User\Personal]	_ <b>D</b> X
Section View Favorites Window Help	_ & ×
Console Root Certificates - Current User Certificates Find Certificates	Actions Personal A More Actions
Image: Second state state       All Tasks       Find Certificates         Image: Second state state       View       Request New Certificate         Image: Second state       New Window from Here       Import         Image: Second state       New Taskpad View       Advanced Operations	
>     >     Tr       >     >     CI       Export List     >	
▷     □     Help       ▷     □     Snor-cura more transfer non-cura more transfer no	
Personal store contains 9 certificates.	

新しい証明書の要求

3.ウィザード**の[次**へ]をクリックし、[Active Directory Enrollment Policy]を選択します。次に、もう一度[次]をクリックします。

	Concola 1 (Concola Doot) Cartificator Current Llear) Dorconal 🗕 🗖 🗙	
File Action View	Certificate Enrollment	_ <u>-</u>
Console Root Certificates - Curren Certificates - Curren Personal Trusted Root Ce Enterprise Trust	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 mal ore Actions
Intermediate Certain State Certain State Certain State St	Configured by your administrator	
Trusted Publishe	Active Directory Enrollment Policy V	
<ul> <li>▷ □ Untrusted Certifi</li> <li>▷ □ Third-Party Roof</li> <li>▷ □ Trusted People</li> <li>▷ □ Client Authentic</li> <li>▷ □ Certificate Enroll</li> <li>▷ □ Smart Card Trus</li> <li>⊿ □ Certification Author</li> <li>▷ □ jajanson-2012DC</li> </ul>	Configured by you Add New	
< III Personal store contains 9 cer	Next Cancel	

Active Directory登録

4. [Enrollment Agent Certificate]を選択し、この場合は[Smartcard User\_VCS]を選択し、[Enroll]を クリックします。

<b>a</b>	Concolat Concola Doot/Cartificator Current Licen/Darconal	_ 🗆 X
🔚 File Action View		_ & ×
(† 🔿 🖄 🔁 👘	Certificate Enrollment	
Console Root  Certificates - Curren  Certificates - Curren  Personal  Trusted Root Cer  Certificates - Curren  Cer	Request Certificates You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.  Request More information is required to enroll for this certificate. Click here to configure settings.	s Inal A Iore Actions
▷ Intrusted Certifi▷ Intrusted Certifi▷ Intrusted Party Root▷ Intrusted People	□ Exchange Signature Only       ↓ STATUS: Available       Details ~         ▲       More information is required to enroll for this certificate. Click here to configure settings.	
Client Authentic Client Authentic Certificate Enroll	Smartcard User_VCS 🔅 STATUS: Available Details ~	
<ul> <li>▷ Smart Card Trust</li> <li>⊿ Certification Author</li> <li>▷ ∂ jajanson-2012DC</li> </ul>	□ User       ③ STATUS: Available       Details ~       ■         □ VCS_Login_SMART       ③ STATUS: Available       Details ~       ■         ▲ More information is required to enroll for this certificate. Click here to configure settings.       ✓         □ Show all templates       >	
< III Personal store contains 9 cer	<u>Enroll</u> Cancel	

登録証明書エージェント

IT管理者のデスクトップが登録ステーションとして設定されました。これにより、他のユーザに 代わって新しいスマートカードを登録できます。

#### <u>の代理で登録....</u>

認証のために従業員にスマートカードを提供するには、従業員を登録して証明書を生成する必要 があります。証明書はスマートカードにインポートされます。



1. MMCを起動し、**Certificates Module & Manager**をイ**ンポートし、マイユー**ザアカウントの証明 書をインポートします。

2.右クリックするか、「個人」>「証明書」を選択して、「すべてのタ**スク」>「詳細操作」を選** 択し、「**代理で登録」をクリックします。** 

3.ウィザードで、[Active Directory Enrollment Policy]を選択し、[Next]をクリックします。

<b>a</b>	Co	nsole1 - [Console Root\Certifica	ites - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
File Action View Favorites Window H	elp							_ 8 ×
Console Root Current User Console Root Current User Current User Current User Current User Current User Current View Current	Issued To Caldministrator Caldministrator Ca	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Iministrator anson-2012DC-AD-CA Create Custom Request Enroll On Behalf Of Manage Enrollment Policies jajanson-2012DC-AD-CA	Expiration Date 10/14/2019 10/12/2018 5/20/2117 10/12/2019 7/6/2027 9 9 10/24/2019	Intended Purposes Certificate Request Microsoft Trust List File Recovery Certificate Request <all> 1.3.6.1.4.1.44906.1.9 Secure Email, Client Secure Email, Client</all>	Friendly Name Stat <none> <none> <none> <none> <none> <none> <none> <none> <none> <none></none></none></none></none></none></none></none></none></none></none>	s Certi Enro Adm Enro 1.3.6 Sma Sma Sma	Actions Certificates More Actions	

### 代理登録の詳細設定

		Console1 - [Console Roof)/Certif	licates - Current U	ser/Personal/Certifi	icates)				= 0 X
🖀 File Action View Favorites Window Hel	lp .								_ Ø X
	Issued To	toued By jejansen-2012DC-AD-CA jejansen-2012DC-AD-CA	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Cartificate Request Microsoft Trust List	Friendly Nome «None»	Status	Cefi Erve Adr	Actions Certificates More Actions	
Drutted Root Cetification Authorities     Enterprise Trust     Drutted Root Cetification Authorities     Drutted Cetification Authorities     Drutted Publishers	Cadministration Cadmin	Certificate Enrollment Before You Begin			_ 0 X		Ervo 1.3.6 Sma		
D Untrasted Certificates     D Intra-Party Root Certification Authorities     Third-Party Root Certification Authorities     D Intrasted Paropia     D Intrasted Paropia     D Certificate Development Responses     D Send Certificate Reset	Cont Long	The following steps will help you install certif networks, protect content, establish identity, Before requesting a certificate, verify the follo	icates, which are digit and do other security- wing	el credentials used to co related tasks.	nnect to window		Sma		
		You have configured or compared on the send to veri	fy your right to obtain	the certificate					
				Next	t Cancal				
	c						>		
Personal store contains 9 certificates.									

4. [Certificate Enrollment Policy]を選択し、[**Next**]をクリ**ックします**。

<b>a</b>		Console1 - [Console Root\Certific	ates - Current U	ser\Personal\Certifi	cates]				_ 🗆 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 Personal	Administrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request	<none></none>		Enro	Certificates	
Certificates	Administrator	jajanson-2012DC-AD-CA	10/12/2016	MICrosoft Trust List	<ivone></ivone>		Adm	More Actions	+
Trusted Root Certification Authorities	Administrator						Enro		
D Intermediate Certification Authorities	El jajanson-2012 C	ertificate Enrollment					136		
Active Directory User Object	Scott Lang						Sma		
D Untrusted Publishers	Scott Lang	Select Certificate Enrollment Policy					Sma		
Third-Party Root Certification Authorities	E Scott Lang	Certificate enrollment policy enables enrollmen	for certificates bas	ed on predefined certific	ate templates.		Sma		
Figure 1		Certificate enrollment policy may already be co	ntigured for you.						
Certificate Enrollment Requests		Configured by your administrator							
Smart Card Trusted Roots		Active Directory Enrollment Policy			$\checkmark$				
		Configured by you		Next	Add New		2		
Personal store contains 9 certificates	<						2		
Contraction and a contraction of a contraction									

#### 登録ポリシー

### 5.署名証明書の選択を求められました。これは、以前に要求した登録証明書です。

<b>a</b>	Con	sole1 - [Console Root\Certifica	tes - Current Us	er\Personal\Certifi	cates]			- 🗆 X
File Action View Favorites Window He	lp							_ 8 ×
Console Root Console Root Certificates - Current User Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificate Inveloped Certificate Enrollment Requests Certificate Enrollment Requests Smart Card Trusted Roots	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Window Select a Certificate Administrator Issuer; jajanson-20 Valid From: 10/14/2 Click here to view of properties Administrator Issuer; jajanson-20 Valid From: 10/12/2	Expiration Date 10/14/2019 10/12/2018 vs Security 12DC-AD-CA 2017 to 10/14/2019 certificate. 12DC-AD-CA 2017 to 10/12/2019 0K	Intended Purposes Certificate Request Microsoft Trust List X Cancel	Friendly Name <none> - None&gt; - X her users. Click Browse</none>	Status Ce En Ad En Sm Sm Sm	tri Certificates More Actions 1.6 1.6 1.6 1.6 1.6 1.6 1.6 1.6	,
Personal store contains 9 certificates.								

### 署名証明書の選択

6.次の画面で、要求する証明書を参照する必要があります。この例では、以前に作成したテンプ レートであるSmartcard User\_VCSです。

<b>a</b>		Console1 - [Console Root\Certifi	cates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
🖀 File Action View Favorites Window He	slp							- 8 ×
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status C	erti Actions	
4 Personal	Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	<none></none>	A	dm Certificates	•
Certificates	Administrator				_ 0 X		More Actions	,
Finisted Root Certification Authorities	Administrator	Cortificato Enrollmont				Er	nro	
Intermediate Certification Authorities	PIVKey BD9A5	Certificate Enrollment				1.	3.6	
<ul> <li>Active Directory User Object</li> <li>Trusted Publishers</li> </ul>	Scott Lang	Request Certificates				Sr	ma	
Untrusted Certificates	Scott Lang	nequest certificates				Sr	ma	
D Third-Party Root Certification Authorities D Trusted People		You can request the following types of certific click Next.	ates. Select the certifi	cates you want to reque	st, and then			
Client Authentication Issuers								
Certificate Enrollment Requests     Smart Card Trusted Roots		Exchange Enrollment Agent (Offline	(i) STATUS: Availa	ale.	Details v			
		request)	coll for this cartificate	Click here to configure	settions			
				r enex nere to comigare	Jennigh			
		Exchange Signature Only	STATUS: Availab	ble	Details ~			
		More information is required to en	roll for this certificate	. Click here to configure	= settings.			
		Smartcard User_VCS	STATUS: Availal	ble	Details ~			
		⊖ User	STATUS: Available	ble	Details 🗸 🔔			
		Show all templates						
				Next	Cancel			
							_	
Personal store contains 9 certificates.							2	

VCSスマートカードの選択

7.次に、に代わって登録するユーザを選択する必要があります。[参**照]をクリック**し、登録する従 業員のユーザ名を入力します。この例では、Scott Lang 'antman@jajanson.local account'が使用 されます。

<b>a</b>		Console1 - [Console Root\Cer	tificates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
File Action View Favorites Window Hel	IP							_ 8 ×
◆ ⇒ ≥ 📷 🗓 🖻 💀 📓 🖬								
Console Root	Issued To	Issued By jajanson-2012DC-AD-CA	Expiration Date 10/14/2019	Intended Purposes Certificate Request	Friendly Name	Status C	Certi Actions	
Personal     Certificates	Administrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	<none></none>	4	Adm More Actions	,
<ul> <li>Trusted Root Certification Authorities</li> <li>Enterprise Trust</li> </ul>	Administrator	Select Use	er	×	_ O X	E	Enro	
Intermediate Certification Authorities     Active Directory User Object     Trusted Publisherr	PIVKey BD9A5	Select this object type:			_	1 S	1.3.6 Sma	
Untrusted Certificates     Third-Party Root Certification Authorities	Scott Lang	User From this location:	Obje	t Types	f that user. For	s	5ma 5ma	
Trusted People     Client Authentication Issuers		jajanson Jocal	Loc	ations				
Certificate Enrollment Requests     Smart Card Trusted Roots		Enter the object name to select ( <u>examples</u> ): Scott Lang (antman@iajanson.local)	Cher	e needs to k Names	be installed is			
		Advanced	OK	Cancel	Browse			
					Cancel			
	<		ш				>	
Personal store contains 9 certificates.								

ユーザの選択

8. 次の画面で、[登録]をクリックして登録を続行します。今すぐに、スマートカードをリーダー に挿入します。

		Console1 - [	Console Root\Cer	tificates - Current Us	er\Personal\Certifi	cates]				_ 🗆 X
Tile Action View Favorites Window Hel	lp									_ 8 ×
(+ +) 2 📰 📋 🍳 🕞 🔟 🗊										
Console Root	Issued To	Issued B	y .	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
4 🐺 Certificates - Current User	Administrator	jajansor	-2012DC-AD-CA	10/14/2019	Certificate Request	<none></none>		Enro	Certificates	
Personal     Castification	Administrator	jajansor	-2012DC-AD-CA	10/12/2018	Microsoft Trust List	<none></none>		Adm	More Actions	•
Trusted Root Certification Authorities	2 Administrator					_ <b>D</b> X		Enro		
Enterprise Trust	jajanson-2012	Certificate Enrollm	ent					Enito		
Intermediate Certification Authorities	PIVKey BD9A5							1.3.6		
Active Directory User Object Trusted Publishers	Scott Lang	Select a user						Sma		
Untrusted Certificates	Scott Lang	Derect d aber						Sma		
Third-Party Root Certification Authorities	- score cang	To request a certifica	ate on behalf of anothe	er user, enter the formal n	ame or domain name o	of that user. For		31110		
Client Authentication Issuers		example, riistname	Lastname, username, o	or domain/username.						
Certificate Enrollment Requests		Before enrolling for attached	a certificate, make sure	the device on which the	user certificate needs to	o be installed is				
Smart Card Trusted Roots		utuenea.								
		User name or alias:				Require				
		Moning our and the								
					Enrol	II Cancel				
	<			ш						
Personal store contains 9 certificates.							_			

#### 登録

### 9. スマートカードを挿入すると、次のように検出されます。

and the	CARTERIN.	
ques	Windows Security	
e ensol Alber D E Vaki	Errolling for the user certificate. Select a smart card device Axalto Cryptoflex .NET Genuto USB Smart Card Reader 0 The smart card is ready for use.	
	OK Generi	

10. 次に、スマートカードの暗証番号(デフォルトの暗証番号)を入力するように求められます 。:0000)。

·		Cons	ole1 - [Console Root\Certifi	cates - Current U	ser\Personal\Certifi	cates]				_ 🗆 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 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>		Enro	Certificates	•
Certificates	Administrator		,,,			_ 0 X			More Actions	•
<ul> <li>Trusted Root Certification Authorities</li> <li>Enterprise Trust</li> </ul>	Administrator	Cartificato	avallment					Enro		
Intermediate Certification Authorities	PIVKey BD9A5	e Certificate i	enroliment					1.3.6		
<ul> <li>Active Directory User Object</li> <li>Trusted Publishers</li> </ul>	Scott Lang	Reques	Wind	ows Security	×	Π		Sma		
Untrusted Certificates	Scott Lang			ons secondy				Sma		
<ul> <li>Inird-Party Root Certification Authorities</li> <li>Trusted People</li> </ul>		The enro	Enrolling for the user cer	tificate.						
Client Authentication Issuers		Active	rease enter your outrienteetion							
<ul> <li>Certificate Enformment Reduests</li> <li>Smart Card Trusted Roots</li> </ul>		Sm	PIN							
			Click here for m	ore information						
				0	Cancel					
						Cancel				
	-									
							_			
Personal store contains 9 certificates.	<								1	

#### ピンを入力します

11. [Enrollment Successful]画面が表示されたら、このスマートカードを使用して、ドメインに参加しているサーバ(カードと既知のPINのみを持つVCSなど)にログオンできます。ただし、 VCSを準備して認証要求をスマートカードにリダイレクトし、共通アクセスカードを使用してスマートカードに保存されているスマートカード証明書を認証のために解放する必要があります。

Certificate Enrollment		_ <b>0</b> X
Certificate Installation Results	and and included as this come day	
Active Directory Services at Policy	ones and material of the congress.	
®Vakkundig Smartcard User	✓ STATUS: Succeeded	Details 👻
		Next user Oose

### 共通アクセスカード用のVCSの設定

[**Maintenance**] > [**Security**] > [Trusted CA Certificate]の順に移動して、ルートCAをVCSの[Trusted CA Certificate]リストにアップロードします。

2.ルートCAによって署名された証明書失効リスト(CRL)をVCSにアップロードします。 [Maintenance] > [Security] > [CRL Management]に移動します。

3. LDAPまたはローカルユーザに対する認証に使用するユーザ名を証明書から取得する正規表現 に対してクライアント証明書をテストします。正規表現が証明書の件名と照合されます。これは 、UPN、電子メールなどになります。この実習では、クライアント証明書のクライアント証明書 と照合する電子メールを使用しました。

搹 Certificate	$\times$
General Details Certification Path	
Show: <all></all>	$\sim$
Field Signature hash algorithm Signature hash algorithm Suer Valid from	Value ^ sha512 jajanson-2012DC-AD-CA, jaja Tuesday, October 17, 2017 5:
Subject Public key Public key parameters	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

クライアント証明書の件名

4. [Maintenance] > [Security] > [Client Certificate Testing]に移動します。テスト対象のクライアン ト証明書を選択し、[My lab it was antman.pem]でテストエリアにアップロードします。[証明書ベ ースの認証パターン]セクションの[証明書と照合する正規表現]で、テスト対象の正規表現を貼り 付けます。[ユーザー名の形式]フィールドは変更しないでください。

My Regex: /Subject:.	*emailAddress=(?.*)@jajanson.local/m					
CISCO Cisco TelePresence Video Communication Server Expresso	ay .	This system has 6 atoms				
Status System Configuration Applications Users Maintenance						
Client certificate testing		You are here: <u>Mantenance</u> / <u>Departy certificates</u> / Clien				
Client certificate						
	This tests whether a client certificate is valid when checked against the VCIS's current trusted CA list and, if loaded, the revocation list					
Certificate source	Uploaded test file (PEM formal) [] ()	Copiesee test test (PED forwar) / //				
Belect the file you want to test	Browse. No file selected.	Browne. No file selected.				
Currently uphaded test file	anoman peri	antran gan				
Certificate-based authentication pattern						
	This section applies only if your testficane contains authentication credentals and you want to use certificate-based authentication as your the normanic destficate to see if the certificate's credentals (the username) can be extracted.	client certificate-based security setting. It lets you test the outcome of applying regax and username format combinations to				
Regex to match appliest certificate	Sulpot, "enal/kotesen/htopptureCommonNamen-t)@pareon.localm					
Usemane format	#captureCommoName#					
	Make these settings permanent					

VCSでの正規表現のテスト

Check certificate					
Centrificate text results Julid centrificate: Bourse: Flaname: Text pattern (as entered above): Passe:	OK Uplaade test file (PEM format) astman pen Sulaart "emalAddreasen"t cantur-CommoNames "«Balanses localim	This is our test a testing. We see th our Active Director issued the smartca	ource client certificate and the e resulting string username is a my to be used with authenticatio rd certificate on his CAC card.	client certificate and the regex we are ting string username is antmam which is in be used with authentication. Antman was ificate on his GC card.	
Template Resulting string (username)	#captureCommonName# antman				
Stand pamen (sument VCS configuration): Regists Template Resulting string (or Centificate in plain text:	/Subject."CNN(*capture/CommonName*(",Uj(,Uj')m Resput=CommonName*(",Uj(,Uj')m Resput=CommonName*(",Uj(,Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName*(",Uj')m resput=CommonName	17:00:00:00:00:00:12 rssm, SC+Tocal ( C. Chudeat T. Lang, Ounterood, SC-Tatansan, SC-Toc 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:01 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00 40:12:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00 40:12:00:00:00:00:00:00:00 40:12:00:00:00:00:00:00:00 40:12:00:00:00:00:00:00:00 40:12:00:00:00:00:00:00:00 40:12:00:00:00:00:00:00:00:00:00:00:00 40:12:00:00:00:00:00:00:00:00:00:00:00:00:00	- -	Here we see the uploaded certificate and the current configuration of the reges on the server. Once you have verified that the reges is working then you can permentantly change the Reges. So do not worry that this section shows a failure because this is the current configuration not your test configuration above.	

#### テスト結果

5.テストで目的の結果が得られる場合は、[Make these changes permanent]ボタンをクリックし てください。これにより、サーバの証明書ベースの認証設定の正規表現が変更されます。変更を 確認するには、[Maintenace] > [Security] > [Certificate-based authentication configuration]の設定 に移動します。

6. [System] > [Administrator]の順に移動し、ドロップダウンボックスをクリックまたは選択して Client certificate-based security = Client-Based Authenticationを選択し、クライアントベース認証 を有効にします。この設定を使用すると、ユーザはブラウザでVCSサーバのFQDNを入力し、ク ライアントアカウントを選択して共通アクセスカードに割り当てられたPINを入力するよう求め られます。その後、証明書がリリースされ、VCSサーバのWeb GUIが返されます。必要なのは、 [Administrator]ボタンをクリックするか選択するだけです。その後、彼はサーバに入ります。オプ ションClient certificate-based security = Client-Based Validationを選択した場合、ユーザが [Administrator]ボタンをクリックした場合を除き、管理者パスワードの入力を再度求めるメッセー ジが表示されます。通常、後者は組織がCACを使用して達成しようとしているわけではありませ ん。 Cisco Expressway-E

Status	System	Configuration	Applications	Users	Maintenance			
System	System administration							
Epheme	eral port range end	I.				* 49999		
Servic	es							
Serial p	ort / console					0n 🗸 (i)		
SSH se	ervice					0n 🗸 👔		
Web inf	terface (over HTTF	PS)				On 🗸 (i)		
Sessio	on limits							
Session	n time out (minutes	.)				* 30		
Per-acc	count session limit					* 0		
System	session limit					* 0		
System	n protection							
	in protootion							
Automa	ated protection ser	vice						
Automa	atic discovery prot	ection				On 🗸 (j)		
Web s	erver configurat	ion						
Redirec	t HTTP requests to	D HTTPS				On 🗸 ()		
HTTP S	trict Transport Sec	curity (HSTS)				On 🗸 (i)		
Web ad	dministrator port					443 🗸 👔		
Client c	ertificate-based s	ecurity				Not required V		
Save						Drop down the above box and choose Client-Based Authentication		
Relate	d tasks							
Upload	a CA certificate fil	e for HTTPS						
Test cli	ent certificates							

クライアントベースの認証を有効にする

このサイトについて!ロックアウト!!!

クライアントベース認証を有効にして、VCSが何らかの理由で証明書を拒否すると、従来の方法 でWeb GUIにログインできなくなります。しかし、システムに戻る方法があることを心配しない でください。添付のドキュメントはシスコのWebサイトにあり、クライアントベース認証をルー トアクセスから無効にする方法について説明しています。

確認

現在、この設定に使用できる確認手順はありません。

# トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。