CAC 및 스마트 카드 리더로 VCS 구성

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>배경 정보</u> <u>스마트 카드란?</u> <u>구성</u> 다음을 확인합니다.</u> 문제 해결

소개

이 문서에서는 은행, 병원 또는 보안 시설이 있는 정부와 같은 VCS 환경에 2단계 인증을 필요로 하 는 조직을 위해 Cisco VCS(Video Communication Server)와 함께 사용할 수 있도록 스마트 카드 리 더와 공통 액세스 카드 로그인을 설치하고 사용하는 단계별 지침에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco Expressway 관리자(X14.0.2)을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

CAC는 필수 인증을 제공하므로 "시스템"은 환경에 대한 액세스 권한을 얻은 사람과 물리적 또는 전 자 인프라를 통해 인프라의 어느 부분을 파악합니다. 정부 기밀 환경 및 기타 보안 네트워크 내에서 "최소한의 특권 액세스" 또는 "알아야 할 사항"의 규칙이 우선합니다. 로그인은 누구나 사용할 수 있 으며, 인증에는 사용자가 가지고 있는 것을 필요로 하며, CAC(Common Access Card)라고도 하는 것이 2006년에 등장하여 직원이 직장 또는 시스템에 액세스하기 위해 포브, ID 카드 또는 동글처럼 여러 개의 장치를 가질 필요가 없도록 했습니다.

스마트 카드란?

스마트 카드는 클라이언트 인증, 로그온 및 보안 이메일과 같은 소프트웨어 전용 솔루션을 강화하 기 때문에 Microsoft가 Windows 플랫폼에 통합하기 위해 사용하는 PKI(공개 키 인프라)의 핵심 구 성 요소입니다. 스마트 카드는 다음과 같은 이유로 공개 키 인증서 및 관련 키를 통합합니다.

- 개인 키 및 기타 형태의 개인 정보 보호를 위해 변조 방지 스토리지를 제공합니다.
- 시스템 내 다른 부분으로부터 인증, 디지털 서명 및 키 교환이 포함되며 알 필요가 없는 보안 크 리티컬 컴퓨팅을 격리합니다.

• 직장, 가정 또는 이동 중에 컴퓨터 간에 자격 증명 및 기타 개인 정보의 이동성을 지원합니다. 스마트 카드는 마우스나 CD-ROM을 도입하는 것과 같이 컴퓨터 업계에 혁명적이고 바람직한 새로 운 기능을 제공하기 때문에 스마트 카드가 윈도우 플랫폼의 필수적인 부분이 되었다. 현재 내부 PKI 인프라가 없는 경우 먼저 이를 확인해야 합니다. 이 문서에서는 이 문서에서 이 역할의 설치에 대해 다루지 않지만, 이 역할의 구현 방법에 대한 자세한 내용은 여기에서 확인할 수 있습니다. http://technet.microsoft.com/en-us/library/hh831740.aspx

구성

이 실습에서는 LDAP를 VCS와 이미 통합했으며 LDAP 자격 증명으로 로그인할 수 있는 사용자가 있다고 가정합니다.

- 1. <u>랩 장비</u>
- 2. <u>스마트 카드 설치</u>
- 3. <u>인증 기관 템플릿 구성</u>
- 4. <u>등록 에이전트 인증서 등록</u>
- 5. <u>다음에 대한 등록...</u>
- 6. <u>공통 액세스 카드에 대한 VCS 구성</u>
- 필수 장비:

다음 역할/설치 소프트웨어가 있는 Windows 2012R2 도메인 서버:

- 인증 기관
- Active Directory
- DNS
- 스마트 카드가 연결된 Windows PC
- vSEC: 스마트 카드를 관리하는 CMS K-Series 관리 소프트웨어:



Versa Card Reader 소프트웨어

스마트 카드 설치

스마트 카드 리더는 일반적으로 필요한 케이블을 연결하는 방법에 대한 지침을 제공합니다. 다음은 이 구성에 대한 설치 예입니다.

스마트 카드 판독기 장치 드라이버 설치 방법

스마트 카드 판독기가 탐지되어 설치된 경우 Windows 로그온 시작 화면에서 이를 확인합니다. 그 렇지 않은 경우:

- 1. 스마트 카드를 Windows PC의 USB 포트에 연결
- 장치 드라이버 소프트웨어 설치에 대한 화면의 지침을 따릅니다. 이렇게 하려면 스마트 카드 또는 드라이버의 제조업체가 Windows에서 검색된 드라이버 미디어가 필요합니다. 내 경우에 는 다운로드 사이트에서 제조 드라이버를 사용했습니다. WINDOWS를 신뢰하지 마십시오.
- 바탕 화면에서 내 컴퓨터 아이콘을 마우스 오른쪽 단추로 클릭하고 하위 메뉴에서 관리를 클 릭합니다.
- 4. 서비스 및 애플리케이션 노드를 확장하고 서비스를 클릭합니다.

- 5. 오른쪽 창에서 **스마트 카드**를 마우스 오른쪽 단추로 클릭합니다. 하위 메뉴에서 속성을 클릭 합니다.
- 6. General 탭의 Startup Type 드롭다운 목록에서 Automatic을 선택합니다. 확인을 클릭합니다.
- 7. 하드웨어 마법사가 지시하면 시스템을 재부팅합니다.

인증 기관 템플릿 구성

- 1. 관리 도구에서 인증 기관 MMC를 시작합니다.
- 2. Certificate Templates(**인증서 템플릿**) 노드를 클릭하거나 선택하고 Manage(관리)를 **선택합니** 다.
- 3. 스마트 카드 **사용자** 인증서 템플릿을 마우스 오른쪽 단추로 클릭하거나 선택한 다음 이미지에 표시된 대로 복제를 선택합니다.

a	Console1 - [C	onsole Root\Certifie	cate Temp	lates (2012DC	-AD.jajanson.local)]		
File Action View Favorites Window Hele	· · · · · · · · · · · · · · · · · · ·						_ @ ×
Console Root	Template Display Name	Schema Version	Versi	Intended Purpos	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				Marchaticas
	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 Service	e Email Replication		
	Domain Controller	1	4.1				
	Domain Controller Authentication	2	110.0	Client Authentic	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 Authentic	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 Authentic	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		
	Subordinate Certification Authority	1	5.1		All Tasks		
	Trust List Signing	1	3.1		Properties		
	2 User	1	3.1		Help	-	
<	C Construction Cal.) (III)		

도메인 컨트롤러 인증서 템플릿

4. 호환성 탭의 인증 기관에서 선택 사항을 검토하고 필요한 경우 변경합니다.

Smar	tcard	User_VCS	Prop	perties	?	X
		_				
Subject Name		Estensions	Issuan	Ce Require	ements	
General Compatibility	Reque	et Handling	Count	ography	Key Att	erver
The template options ar versions set in Compatit	vailable pility Set nges	are based or tings.	the e	arliest oper	rating sys	stem
Windows Server 20 Certificate recipient	, 112 R2		*			
Windows 8.1 / Win	dows Se	erver 2012 R	: •			
These settings may not template.	prevent	earlier opera	iting sy	stems fron	n using tł	his
ОК		Cancel		Apply		lelp

설정

5. **일반** 탭

a. Smartcard **User_VCS**와 같은 이름**을 지정합니다**.

b. 유효 기간을 원하는 값으로 설정합니다. Apply를 **클릭합니다**.

	Smarto	ard User_VCS	Properties	? X						
	Subject Name Issuance Requirements									
Supers	seded Templates	Security	Server							
General	Compatibility Request Handling Cryptography Key Attestation									
Templa	te display name:									
Smartc	ard User_VCS									
Templa Smartc Validity 10	te name: ard User_VCS period: years v lish certificate in A Do not automatical Directory	Renewa 6 ctive Directory lly reenroll if a dupli	l period: weeks ✓	xists in Active						
	ОК	Cancel	Apply	Help						

간 만료

- 6. **요청 처리** 탭
- a. Purpose를 **Signature**(서명) **및 smartcard logon(스마트 카드 로그온)으로 설정합니다**.
- b. 등록 중에 사용자에게 프롬프트를 클릭합니다. Apply를 클릭합니다.

Proj	perties of New	/ Template		
Subject Name	Server	Issuance F	Requirements	
Superseded Templa	ites Ext	tensions	ensions Security	
Compatibility General	Request Handling	Cryptography	Key Attestation	
Purpose: Signa	ture and smartcard	logon	¥	
De	lete revoked or expi	ired certificates (do not archive)	
_ Inc	lude symmetric algo	rithms allowed by	y the subject	
Arc	hive subject's encry	yption private key	y	
Allow private key to	be exported			
Renew with the sam	ie key (*)			
For automatic renew	val of smart card cer	tificates, use the	existing key if a	
inew key cannot be	created (*)			
Do the following when t	he subject is enrolle	ed and when the	private key	
associated with this cer	tificate is used:			
 Enroll subject without 	it requiring any user	rinput		
Prompt the user duri	ng enrollment			
O Prompt the user duri private key is used	ng enrollment and r	equire user input	when the	
* Control is disabled due	e to <u>compatibility se</u>	ttings.		
ОК	Cancel	Apply	Help	
		-1		

7. Cryptography 탭에서 최소 키 크기를 2048로 설정합니다.

a. Requests must use **the following providers(요청에서 다음 공급자 중 하나를 사용해야 함)를** 클릭한 다음 **Microsoft Base Smart Card Crypto Provider를 선택합니다**.

b. 적용을 **클릭합니다**.

Subject Name Server Issuance Requirements Superseded Templates Extensions Security Compatibility General Request Handling Cryptography Key Attestation Provider Category: Legacy Cryptographic Service Provider ✓ Algorithm name: Determined by CSP ✓ Minimum key size: 2048 Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Microsoft Base Smart Card Crypto Provider Microsoft Enhanced Cryptographic Provider Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider Microsoft Enhanced RSA and AES Cryptographic Provider Microsoft Enhanced RSA and AES Cryptographic Provider Will be alternate signature format OK Cancel Apply Help	Prop	perties of New	/ Template	X		
Superseded Templates Extensions Security Compatibility General Request Handling Cryptography Key Attestation Provider Category: Legacy Cryptographic Service Provider ✓ Algorithm name: Determined by CSP ✓ Minimum key size: 2048 Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Image: Requests must use one of the following providers: Providers: Providers: Microsoft Base Smart Card Crypto Provider Image: Request Enhanced Cryptographic Provider V1.0 Microsoft Enhanced Cryptographic Provider V1.0 Image: Request Enhanced DSS and Diffie-Hellman Cryptographic Provider Microsoft Enhanced RSA and AES Cryptographic Provider Image: Request hash: Image: Determined by CSP Request hash: Determined by CSP Image: Request hash: Image: Determined by CSP Image: Request hash: OK Cancel Apply Help	Subject Name	Server	Issuance R	equirements		
Compatibility General Request Handling Cryptography Key Attestation Provider Category: Legacy Cryptographic Service Provider ✓ Algorithm name: Determined by CSP ✓ Minimum key size: 2048 Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Microsoft Base Smait Card Crypto Provider Microsoft Enhanced Cryptographic Provider Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr Microsoft Enhanced RSA and AES Cryptographic Provider Microsoft Enhanced RSA and AES Cryptographic Provider Wise alternate signature format OK Cancel Apply	Superseded Templa	tes Ext	ensions Security			
Provider Category: Legacy Cryptographic Service Provider Algorithm name: Determined by CSP Minimum key size: 2048 Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Image: Requests must use one of the following providers: Providers: Providers: Image: Requests function of the following provider via th	Compatibility General	Request Handling	Cryptography	Key Attestation		
Algorithm name: Determined by CSP ✓ Minimum key size: 2048 Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider v1.0 Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr Microsoft Enhanced RSA and AES Cryptographic Provider Request hash: Determined by CSP Use altemate signature format	Provider Category:	Legacy Crypto	ographic Service	Provider 🗸		
Minimum key size: 2048 Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider Microsoft Enhanced RSA and AES Cryptographic Provider Request hash: Determined by CSP Use alternate signature format OK Cancel Apply Help	Algorithm name:	Determined by	y CSP	~		
Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider v1.0 Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced RSA and AES Cryptographic Provider Request hash: Determined by CSP Wise alternate signature format OK Cancel Apply Help	Minimum key size:	2048				
○ Requests can use any provider available on the subject's computer ③ Requests must use one of the following providers: Providers: Providers: ○ Microsoft Base Smart Card Crypto Provider ○ Microsoft DH SChannel Cryptographic Provider ○ Microsoft Enhanced Cryptographic Provider v1.0 ○ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr ○ Microsoft Enhanced RSA and AES Cryptographic Provider ○ Use alternate signature format	Choose which cryptogr	aphic providers can	be used for requ	ests		
 Requests must use one of the following providers: Providers: Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr Microsoft Enhanced RSA and AES Cryptographic Provider Request hash: Determined by CSP Use alternate signature format 	Requests can use a	ny provider availab	le on the subject's	s computer		
Providers: Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider v1.0 Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced RSA and AES Cryptographic Provider Request hash: Determined by CSP Use alternate signature format	Requests must use	one of the following	providers:			
Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider v1.0 Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr Microsoft Enhanced RSA and AES Cryptographic Provider Request hash: Determined by CSP Use alternate signature format	Providers:					
Request hash: Determined by CSP Use alternate signature format OK Cancel Apply Help	Microsoft Base Sma Microsoft DH SChar Microsoft Enhanced Microsoft Enhanced Microsoft Enhanced	rt Card Crypto Provi anel Cryptographic Prov Cryptographic Prov DSS and Diffie-He RSA and AES Cryp	der Provider vider v1.0 Ilman Cryptograph otographic Provide	ic Pr er ⊻		
Use alternate signature format OK Cancel Apply Help	Request hash:	Determined by	y CSP	~		
OK Cancel Apply Help	Use alternate signat	ure format				
OK Cancel Apply Help						
	OK	Cancel	Apply	Help		

8. 보안 탭에서 등록 액세스 권한을 부여할 보안 그룹을 추가합니다. 예를 들어, 모든 사용자에게 액 세스 권한을 부여하려면 Authenticated users(인증된 사용자) 그룹을 선택한 다음 Enroll permissions(권한 등록)를 선택합니다.

	Proj	perties o	f New	Template		x
ompatibility	General	Request H	andling	Cryptography	Key Attesta	ation
Subject N	lame	Server Issuance Requirements				
Supersec	ded Templa	ites	Exte	ensions	Security	
Group or use	rnames:					
& Authent	ticated Use	IS				
🔏 Adminis	trator (Adm	in@jajansor	n.local)			
🍇 Domain	Admins (J.	AJANSON\[Domain A	Admins)		
용 Enterpri	ise Admins	(JAJANSON	I∖Enterpr	ise Admins)		
			Г	A	D	51
				Add	Remove	
Permissions	for Authent	icated Users	8	Allow	Deny	
Full Contro	bl					
Read				~		
Write						
Enroll						
Autoenroll						
For special p	emissions	or advance	d setting	s, click	Advanced	
Advanced.			-		Auvanced	
Γ	OK		neel	Analy	Lista	
				ADDIV	Help	

9. **확인**을 클릭하여 변경 사항을 완료하고 새 템플릿을 생성합니다. 이제 새 템플릿이 인증서 템플 릿 목록에 나타나야 합니다.

🖀	Console1 - [Console Root\Certi	ificate Templ	ates (2012DC-AD.jajanson.local)]		
🜇 File Action View Favorites Window Help					- 8 ×
← ⇒ 2 📷 🗙 🗈 🕞 🛛 📷					
Console Root Template Display Nante	e 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 Omputer	1	5.1			Certificate Templates (2012DC-ADijaj
Cross Certification A	uthority 2	105.0			More Actions
Directory Email Replication	ication 2	115.0	Directory Service Email Replication		Smartcard User VCS
Domain Controller	1	4.1			Marchatiana k
Domain Controller A	authentication 2	110.0	Client Authentication, Server Authentication, Smart Card Logon		More Actions
EFS Recovery Agent	1	6.1			
Enrollment Agent	1	4.1			
R Enrollment Agent (C	omputer) 1	5.1			
Exchange Enrollment	t Agent (Offline requ 1	4.1			
Exchange Signature	Only 1	6.1			
🗷 Exchange User	1	7.1			
@ IPSec	1	8.1			
IPSec (Offline request	it) 1	7.1			
Kerberos Authentica	tion 2	110.0	Client Authentication, Server Authentication, Smart Card Logon, KE		
Key Recovery Agent	2	105.0	Key Recovery Agent		
OCSP Response Sign	ing 3	101.0	OCSP Signing		
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication	Ξ.	
Root Certification Au	uthority 1	5.1			
Router (Offline requi	est) 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 Certifica	ation Authority 1	5.1			
Trust List Signing	1	3.1			
@ User	1	3.1			
User Signature Only	1	4.1			
2 VCS_Login_SMART	2	100.8	Smart Card Logon, Client Authentication		
Web Server	1	4.1			
2 Webclientandserver	2	100.4	Client Authentication, Server Authentication		
Workstation Authent	tication 2	101.0	Client Authentication		
с ш > с	ш		>	Ť	
36 certificate templates					

도메인 제어에 표시되는 템플릿

10. MMC의 왼쪽 창에서 인증 기관(로컬)을 확장한 다음 인증 기관 목록에서 CA를 확장합니다.

Certificate Templates(인증서 템플릿)를 마우스 오른쪽 버튼으로 클릭하고 New(새로 만들기)를 클 릭한 다음 Certificate Template to Issue(발급할 인증서 템플릿)를 클릭합니다. 그런 다음 새로 생성 된 스마트카드 템플릿을 선택합니다.

a		(Console1 - [Console Roo	ot\Certification Authority (Local)\ja	janson-2012DC-AD-CA\Certificate Templates]		_ 🗆 X
🚋 File Action View Fa	avorites 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 (Off	fline request)	IP security IKE intermediate		Mars Astiens	
a 🛃 jajanson-2012DC-A	AD-CA	🖉 Webclien	tandserver	Client Authentication, Server Authentic		More Actions	
Revoked Certifi	icates	🔄 🖾 Exchange	Signature Only	Secure Email			
Ssued Certifica	ites	CEP Encry	yption	Certificate Request Agent			
Pending Reque	ists	Smartcare	d User_VCS	Secure Email, Client Authentication, Sm			
Failed Kequests	s	VCS_Logi	n_SMART	Smart Card Logon, Client Authentication			
Certificate Ter	Manage		: Agent	Certificate Request Agent			
	Neu		mail Replication	Directory Service Email Replication			
	New	,	ontroller Authentication	Client Authentication, Server Authentic			
	View	•	uthentication	Client Authentication, Server Authentic			
	New Window fr	om Here	try Agent	File Recovery			
	New Technold V		-	Encrypting File System			
	ivew taskpad v	iew	ontroller	Client Authentication, Server Authentic			
	Refresh		r	Server Authentication			
	Export List			Client Authentication, Server Authentic			
	Help			Encrypting File System, Secure Email, Cl			
	- comp		te Certification Authority	<all></all>			
		🗟 Administ	rator	Microsoft Trust List Signing, Encrypting			

새 템플릿 문제

11. 템플릿이 복제되면 MMC에서 인증 기관 목록을 마우스 오른쪽 단추로 클릭하거나 선택한 다음 **모든 작업**을 클릭한 다음 **서비스 중지를** 클릭합니다. 그런 다음 CA의 이름을 다시 마우스 오른쪽 단 추로 클릭하고 **모든 작업**을 클릭한 다음 **서비스 시작 을** 클릭합니다.

-	Console1 - [Console Root\Certification Authority (Local)\jajanson-2012DC-AD-CA]	_ D X
🔚 File Action View Favorites Window Hel	p	_ @ ×
🗢 🔿 🙍 📰 🖾 🔒 📓 📰 🕨 🔳		
Console Root	Name	Actions
a Gertification Authority (Local)	Succed Certificates	jajanson-2012DC-AD-CA
All Tasks	Start Service	More Actions
View >	Stop Service	
New Window from Here New Taskpad View	Submit new request Back up CA	
Refresh	Restore CA	
Export List	Renew CA Certificate	
Properties		
Help		
Contains actions that can be performed on the item.		2

인증서 서비스 중지 후 시작

등록 에이전트 인증서에 등록

클라이언트 시스템(IT 관리자 데스크톱)에서 이 작업을 수행하는 것이 좋습니다.

 MMC를 실행하여 인증서를 선택하고 추가를 클릭한 다음 내 사용자 계정에 대한 인증서를 선 택합니다.



인증서 추가

2 . 마우스 오른쪽 단추를 클릭하거나 **개인 노드**를 선택하고 **모든 작업**을 선택한 다음 **새 인증서 요 청**을 <mark>선택합니다</mark>.

Console1 - [Console Root\Certificates - Current User\Personal]	_ D X
 File Action View Favorites Window Help ← ←	_ <i>6</i> ×
Console Root Object Type	Actions
Certificates - Current User	Personal
▷ Pe ▷ ^{Ch} Tr Find Certificates	More Actions
En All Tasks Find Certificates	
Comparison of the second	
b in the View with the View Advanced Occuptions	
The rest of t	
⊳ 🛅 Tr Refresh	
CI Export List	
∠ The control of	
▶ jajanson-2012DC-AD-C/	
Personal store contains 9 certificates.	

새 인증서 요청

3. 마법사에서 [다음]을 클릭한 다음 Active Directory 등록 정책을 선택합니다. 그런 다음 Next(다음)를 다시 클릭합니다.

	Concola1_[Concola_Doot\Cartificatoc_Current Ucor\Darconal]	
The Action View	📮 Certificate Enrollment	_ [=] ×
Console Root	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 v	
 ▶ □ Untrusted Certifi ▶ □ Third-Party Root ▶ □ Trusted People ▶ □ Client Authentic ▶ □ Client Authentid ▶ □ Smart Card Trust ▲ □ Certification Author ▶ □ jajanson-2012DC 	Configured by you Add New	
		-
< 111	Next Cancel	
Personal store contains 9 cer	incores.	

Active Directory 등록

4. 등록 **에이전트 인증서**(이 경우 Smartcard User_VCS)를 선택한 다음 등록을 **클릭합니다.**



등록 인증서 에이전트

이제 IT 관리자 데스크탑이 등록 스테이션으로 설정되어 있으므로 다른 사용자를 대신하여 새 스마 트 카드를 등록할 수 있습니다.

<u>다음에 대한 등록...</u>

이제 직원에게 인증을 위한 스마트카드를 제공하려면 이를 등록하고 인증서를 생성해야 합니다. 이 인증서는 스마트 카드로 가져옵니다.



1. MMC를 시작하고 인증서 모듈 및 관리자를 내 사용자 계정에 대한 인증서를 가져옵니다.

2. 마우스 오른쪽 단추를 누르거나 **개인 > 인증서**를 선택하고 **모든 태스크 > 고급 작업**을 선택하고 **등록**을 클릭합니다.

3. 마법사에서 Active Directory 등록 정책을 선택한 다음 **다음**을 클릭합니다.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]										
 File Action View Favorites Window He Image: Image: Im	elp							_ # ×		
Console Root Certificates - Current User Certificate - Current User Certificate Envolument Requests Certificate Envolument Requests Sonart Card Trusted Roots Certification Authority (Local)	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Iministrator anson-2012DC-AD-CA Create Custom Request Froli On Behalf Of Manage Enrollment Policies jajanson-2012DC-AD-CA	Expiration Date 10/14/2019 10/12/2018 5/20/2117 10/12/2019 -7/5/2027 -9 	Intended Purposes Certificate Request Microsoft Trust List File Recovery Certificate Request <all> 1.3.6.1.4.1.44986.1.9 Secure Email, Client Secure Email, Client</all>	Friendly Name <none> <none> <none> <none> <none> <none> <none> <none> <none> <none> <none></none></none></none></none></none></none></none></none></none></none></none>	Status Certi Enro Adm Enro 1.3.6 Sma Sma	Actions Certificates More Actions	,		

<u>고급 대신 등록</u>

a		Console1 - [Console Root\Certifi	cates - Current U	er/Personal/Certific	cates)				= 0 X
Tile Action View Favorites Window He	lp								- 0 ×
Conside Root Control Root Constant User Construction Control Control User Control Control User Control Control User Control Control Control User Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Control Contro Control Control Contro Control	Isseed To	tourd By jearnen-2012DC-AD-CA jearnen-2012DC-AD-CA entificate Entollment Before You Begin The fellowing steps will help you install certific returnisk, product context, establish identity, a Before requesting a certificate, verify the follow	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Certificate Request Microsoft Trust List I credentials used to correlated tasks.	Friendly Nome «None» «None» • O X meet to winders	Status	Certi A Inre Adar Enro 134 Sma Sma Sma	etions Certificates More Actions	, _ [-] -] -] -] -] -] -] -] -] -
 Certificate Envelopment Requests Smart Card Trusted Roots 		Your computer is connected to the network You have condentials that can be used to verify	rytvær right to olikain.	the certificate	Cancal				
Personal store contains 9 certificates.							12.1		

4. Certificate Enrollment Policy(인증서 등록 정책)를 선택한 다음 Next(다음)를 클릭합니다.

2		Console1 - [Console Root\Certifica	tes - Current U	ser\Personal\Certifi	cates]				- 🗆 X
🔚 File Action View Favorites Window H	elp								_ 8 ×
🗢 🔶 🙍 🖬 📋 🙆 🔒 📓 📷									
File Action View Favorites Window H File Action View Favorites Window H Console Root Console Root Console Root Console Root Certificates - Current User Certificates Difference Certification Authorities Difference Certification Susers Difference Certificate Enrollment Requests Difference Certificate Roots	elp Issued To Administrator Administrator Administrator Jajajanson-2012 Socott Lang Scott Lang Scott Lang	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA ertificate Enrollment Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment Configured by your administrator Active Directory Enrollment Policy Configured by you	Expiration Date 10/14/2019 10/12/2018 for certificates bas figured for you.	Intended Purposes Certificate Request Microsoft Trust List ed on predefined certific	Friendly Name <none> <none> cate templates. Add New Add New</none></none>	Status	Certi Enro Adrr Enro 1.3.6 Sma Sma Sma	Actions Certificates More Actions	X
Personal store contains 9 certificates.	<						>		

등록 정책

5. 이제 서명 인증서를 선택하라는 메시지가 표시됩니다. 이는 이전에 요청한 등록 인증서입니다.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]	x
File Action View Favorites Window Help	8 ×
Tratel Posities Centralizes Consoler Pool (Centralizes - Current Oser Versional (Centralizes) Centralizes - Current Use Consoler Pool (Centralizes - Current Use Centralizes - Current Use Centralizes - Current Use Centralizes Centrali	
Personal store contains 9 certificates.	

서명 인증서 선택

6. 다음 화면에서 요청하려는 인증서를 찾아보아야 하며, 이 경우에는 이전에 생성한 템플릿인 Smartcard User_VCS가 됩니다.

a		Console1 - [Console Root\Certific	ates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
🖀 File Action View Favorites Window Hel	p							_ 8 ×
File Action View Favorites Window Hel File Action View Favorites Window Hel Console Root Console Root Certificates - Current User Certificates Certifi	Administrator Administrator Administrator Administrator Administrator Parker banson-2012 Scott Lang Scott Lang Scott Lang	lissued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Certificate Enrollment Request Certificates You can request the following types of certificat click Net.	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Certificate Request Microsoft Trust List	Friendly Name <none> <none> st, and then</none></none>	Status Ce En Ac En 1.: Sn Sn Sn	rti To To To To S.6 Ana Ana Actions More Actions To To To To To To To To To To	
P Government Authentication Issuers Gertificate Enrollment Requests Smart Card Trusted Roots		You can request the following types of certificates. Select the certificates you want to request, and then click Next. Exchange Enrollment Agent (Offline ① STATUS: Available Details ~ request) More information is required to enroll for this certificate. Click here to configure settings. Exchange Signature Only ② STATUS: Available Details ~ More information is required to enroll for this certificate. Click here to configure settings. Smartcard User_VCS ③ STATUS: Available Details ~ User ③ STATUS: Available Details ~ Show all templates 						
Personal store contains 9 certificates	د	Ш		Next	Cancel		Σ	

VCS 스마트 카드 선택

7. 다음으로, 등록할 사용자를 선택해야 합니다. 찾아보기를 클릭하고 등록하려는 직원의 사용자 이 름을 입력합니다. 이 경우 Scott Lang 'antman@jajanson.local account'가 사용됩니다.

a		Console1 - [Console Root\Certif	ïcates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
Tile Action View Favorites Window Hel	P							_ 8 ×
(+ +) 2 🗊 🗓 🧟 🕞 📓 🗊								
Console Root Console Root Certificates - Current User Certificates Cer	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Select User Select this object type: User From this location: [ajanson local Enter the object name to select (examples): Scott Lans (extman@aianson local) Advanced	Expiration Date 10/14/2019 10/12/2018 00g 00g 00g 00g 00g 00g 00g 00g 00g 00	Intended Purposes Certificate Request Microsoft Trust List t Types en name of enceds to Cancel	Friendly Name <none> <none> f that user. For b be installed is Browse</none></none>	Status Cr Er Au Er Sr Sr Sr	Actions Certificates More Actions 3.6 ma ma ma	, ,
	<						>	
Personal store contains 9 certificates.								

사용자 선택

8. 다음 화면에서 **등록**을 클릭하여 등록을 진행합니다. 이제 판독기에 스마트 카드를 삽입합니다.



등록

9. 스마트 카드를 삽입하면 다음과 같이 탐지됩니다.

eques	Windows Security	×
ke envol Aribee D	Enrolling for the user certificate. Select a smart card device	
® vaki	Axaito Cryptoflex .NET Gemaito USB Smart Card Reader 0 The smart card is ready for use.	
		- 1

10. 그런 다음 스마트 카드 PIN 번호(기본 PIN: 0000).

8	Con	sole1 - [Console Root\Certif	cates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
Tile Action View Favorites Window Hel	p							_ <i>8</i> ×
	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Enrollment	Expiration Date 10/14/2019 10/12/2018	Intended Purposes Certificate Request Microsoft Trust List	Friendly Name <none> X</none>	Status Co Er Ar Er	ers Actions reo dar More Actions reo 3.6	•
Active Directory User Object Trusted Publishers Untrusted Publishers Third-Party Root Certification Authorities Trusted People Client Authentication Issuers Certificate Enrollment Requests Smart Card Trusted Roots	Scott Lang Scott Lang Scott Lang The enro Active ⊙ Sm	Vind Enrolling for the user cer Please enter your authentication PIN PIN Click here for m	In the second se	X Cancel	Cancel	Si Si Si	ma ma ma	
Personal store contains 9 certificates.								

핀 입력

11. Enrollment Successful(등록 성공) 화면이 표시되면 이 스마트 카드를 사용하여 VCS(예: 카드 및 알려진 핀)와 같은 도메인 가입 서버에 로그온할 수 있습니다. 그러나 이 작업은 "예"가 아닌 경우 에도 VCS를 준비하여 인증 요청을 스마트 카드로 리디렉션하고 일반 액세스 카드를 사용하여 인증 을 위해 스마트 카드에 저장된 스마트 카드 인증서를 릴리스해야 합니다.

		_ 0 X	
Sficate Enrollment			
rtificate Installation Results			
e following certificates have been en	oiled and installed on this computer.		
other Directory Enrolment Policy			
8 Vakkundig Smartcard User	STATUS: Succeeded	Details 🛩	
		Next user Oose	- =
			등폭

공통 액세스 카드에 대한 VCS 구성

Maintenance(**유지 관리**) > Security(보안) > Trusted CA Certificate(신뢰할 수 있는 CA 인증서)로 이 동하여 VCS의 Trusted CA Certificate(신뢰할 수 있는 CA 인증서) 목록**에 루트 CA를 업로드합니다.**

2. 루트 CA에서 서명한 인증서 해지 목록을 VCS에 업로드합니다. Maintenance(유지 관리) > Security(보안) > CRL Management(CRL 관리)로 이동합니다.

3. LDAP 또는 로컬 사용자에 대한 인증에 사용할 인증서에서 사용자 이름을 가져오는 regex에 대해 클라이언트 인증서를 테스트합니다. regex가 인증서의 **Subject**와 일치합니다. UPN, 이메일 등이 될 수 있습니다. 이 Lab에서는 클라이언트 인증서의 클라이언트 인증서와 매칭할 이메일이 사용되었 습니다.

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

클라이언트 인증서 주체

4. Maintenance(유지 관리) > Security(보안) > Client Certificate Testing(클라이언트 인증서 테스트)으로 이동합니다. 테스트할 클라이언트 인증서를 선택하고 My Lab에서 antman.pem을 테스트 영 역에 업로드합니다. Regex의 Certificate-based authentication pattern(인증서 기반 인증 패턴) 섹션 에서 테스트할 regex를 붙여넣습니다. Username 형식 필드를 변경하지 마십시오.

My Regex: /Subject:.*e	<pre>mailAddress=(?.*)@jajanson.loca</pre>	al/m				
CISCO Cisco TelePresence Video Communication Server Expressway		This system has a starmer				
Status System Configuration Applications Users Maintenance						
Client certificate testing		You are here: <u>Mantemanos</u> / <u>Departy certificates</u> / Clen				
Client certificate						
	This tests whether a client certificate is valid when checked against the VCIS's current trusted CA list s	nd. If loaded, the revocation list				
Certificate source	Uploaded test file (PEM formal) (j)					
Belect the file you want to test	Browse. No file selected.					
Currently uploaded text file	antman peri					
Certificate-based authentication pattern						
	This section applies only if your certificate contains authentication credentials and you want to use ce the nominated destificate to see if the certificate's ordentials (the usename) can be extracted.	infrate-based authentication as your client certificate-based security setting. It less you test the outcome of applying regax and usemame format combinations to				
Regex to match against bent/ficate	Rubject, "ematAddresen("ktapfureCommonNamen ;")@jajanson.lotailm	u u				
Username format	*captureCommonName#	<i>v</i>				
	Make these settings permanent					

VCS에서 regex 테스트

Check certificate									
Certificate test results									
Valid certificate:		0K							
Source: Filename: Test pattern (as entered above):		Uploaded test file (PEM format) antman pern	This is our test source client certificate and the regex we are testing. We see the resulting string username is antman which is in our Active Directory to be used with authentication. Actman was issued the marktard certificate on his DCC card.						
	Regex Template	/Subject. *emaiAddressn(?+captureCommonName*.*)@jajanson.localim #captureCommonName#	issoed the smartcard certificate on his CAC card.						
	Resucing string (username)	anordan							
Stored pattern (current VCS config	uration):								
	Regex	/Subject:.*CN+(? <capturecommonname>([*,\]((\.))*)/m</capturecommonname>							
	Template	#captureCommonName#							
	Resulting string (usernar	me) Regex Invalid							
Constant of part last	vocuncee	Certificate: Deal Deal Style 1 Note: Signature A (pertine: heiligitation): Signature A (pertine: heiligitation): Note: Note: Note: Signature A (pertine: heiligitation): Note: Signature A (pertine: heiligitation): Note: Signature A (pertine: heiligitation): Note: Signature A (pertine: heiligitation): Note: Signature A (pertine: heiligitation): Signature A (pertine: heiligitation): Signat	17:00:00:00:00:00:00:17 ns:on.,0C=1oca1 4:00:00:00:00:15:cc 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00 4:00:00:00:00:00:00 4:00:00:00:00:00:00 4:00:00:00:00:00:00 4:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00 4:00:00:00:00:00:00:00 4:00:00:00:00:00:00 4:00:00:00:00:00:00:00:00 4:00:00:00:00:00:00 4:00:00:00:00:00:00 4:00:00:00:00:00 4:00:00:00:00:00 4:00:00:00:00:00 4:00:00:00:00:00 4:00:00:00:00 4:00:00:00:00 4:00:00:00:00 4:00:00:00:00 4:00:00:00 4:00:00:00 4:00:00:00 4:00 4	ros Scialara, Scialara	\bigtriangledown	Here we see the uploaded certificate and the current configuration of the regex on the server. Once you have verified that the regex is working then you can permentantly change the Regex. So do not worry that this section shows a failure because this is the current configuration not your test configuration above.			

테스트 결과

5. 테스트를 통해 원하는 결과를 얻을 수 있는 경우 이러한 변경 사항을 영구적으로 만들기 버튼을 클릭할 수 있습니다. 이렇게 하면 서버의 인증서 기반 인증 컨피그레이션에 대한 regex가 변경됩니 다. 변경 사항을 확인하려면 해당 컨피그레이션, Maintenance(유지 관리) > Security(보안) > Certificate-based authentication configuration(인증서 기반 인증 컨피그레이션)으로 이동합니다.

6. System(시스템) > Administrator(관리자)로 이동하여 클라이언트 기반 인증을 활성화한 다음 드 롭다운 상자를 클릭하거나 선택하여 클라이언트 인증서 기반 보안 = Client-Based Authentication(클라이언트 기반 인증)을 선택합니다. 이 설정을 사용하면 사용자가 브라우저에 VCS 서버의 FQDN을 입력하면 클라이언트 계정을 선택하고 자신의 일반 액세스 카드에 할당된 핀 을 입력하라는 메시지가 표시됩니다. 그런 다음 인증서가 릴리스되고 VCS 서버의 웹 GUI가 반환되 며, Administrator 버튼을 클릭하거나 선택하면 됩니다. 그리고 나서 그는 서버에 들어갔다. Client certificate-based security = Client-Based Validation(클라이언트 인증서 기반 보안 = 클라이언트 기 반 검증) 옵션이 선택된 경우, 사용자가 Administrator(관리자) 버튼을 클릭할 때 프로세스가 예외와 동일하며 관리자 비밀번호를 다시 입력하라는 프롬프트가 표시됩니다. 일반적으로 후자는 조직이 CAC를 사용하여 성취하려고 하는 것이 아닙니다. CISCO Cisco Expressway-E

Status	System	Configuration	Applications	Users	Maintenance	
System Epheme	n administra ral port range end	ation				* 49999 <i>i</i>
Service	s					
Serial po	ort / console vice					On → ① On → ①
Web inte	erface (over HTT	PS)				On 🗸 (1)
Sessio	n limits					
Session	time out (minutes	;)				* 30
Per-acc	ount session limit					* 0
System	session limit					* 0
System	n protection					
Automat	ted protection ser	vice				On v i
Automat	tic discovery prot	ection				On 🗸 (1)
Web se	erver configura	tion				
Redirect	t HTTP requests t	0 HTTPS				On 🗸 i
HTTP St	rict Transport Se	curity (HSTS)				On 🗸 🛈
Web ad	ministrator port	_				443 🗸 👔
Client ce	ertificate-based s	ecurity				Not required 🗸
Save						Drop down the above box and choose Client-Based Authentication
Related	l tasks					
Upload a	a CA certificate fi nt certificates	le for HTTPS				

클라이언트 기반 인증 사용

도와주세요! 문이 잠겼어요!

Client Based Authentication(클라이언트 기반 인증)을 활성화하고 VCS가 어떤 이유로든 인증서를 거부하면 웹 GUI에 더 이상 기존의 방식으로 로그인할 수 없게 됩니다. 하지만 시스템을 다시 사용 할 수 있는 방법이 있다고 걱정하지 마십시오. 첨부된 문서는 Cisco 웹 사이트에서 찾을 수 있으며 루트 액세스에서 클라이언트 기반 인증을 비활성화하는 방법에 대한 정보를 제공합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.