Configurazione di VCS con CAC e lettore di smart card

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Che cos'è una smart card? Configurazione Verifica Risoluzione dei problemi

Introduzione

Questo documento descrive una guida dettagliata all'installazione e all'utilizzo di un lettore di smart card e di una scheda di accesso comune da utilizzare con Cisco Video Communication Server (VCS) per le organizzazioni che richiedono l'autenticazione a due fattori per l'ambiente VCS, ad esempio banche, ospedali o enti pubblici con strutture protette.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco Expressway Administrator (X14.0.2).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il CAC fornisce l'autenticazione necessaria in modo che i "sistemi" sappiano chi ha avuto accesso al proprio ambiente e quale parte dell'infrastruttura sia fisica o elettronica. Negli ambienti governativi classificati, e in altre reti sicure, prevalgono le regole dell'"accesso meno privilegiato" o della "necessità di sapere". Un accesso può essere utilizzato da chiunque, l'autenticazione richiede qualcosa che l'utente ha, ergo il CAC, anche noto come Common Access Card, è nato nel 2006 in modo che l'individuo non ha bisogno di avere più dispositivi, che siano i piedini, carte d'identità o dongle per accedere al loro luogo di lavoro o sistemi.

Che cos'è una smart card?

Le smart card sono un componente chiave dell'infrastruttura a chiave pubblica (PKI, Public Key Infrastructure) utilizzata da Microsoft per l'integrazione nella piattaforma Windows, in quanto le smart card consentono di migliorare le soluzioni basate esclusivamente su software, ad esempio l'autenticazione dei client, l'accesso e la protezione della posta elettronica. Le smart card rappresentano un punto di convergenza per i certificati a chiave pubblica e le chiavi associate in quanto:

- Archiviazione a prova di manomissione per la protezione di chiavi private e altre forme di informazioni personali.
- Isolare i calcoli critici per la sicurezza, che implicano l'autenticazione, le firme digitali e lo scambio di chiavi da altre parti del sistema che non hanno necessità di conoscere.
- Consente la portabilità delle credenziali e di altre informazioni private tra computer al lavoro, a casa o in viaggio.

La smart card è diventata parte integrante della piattaforma Windows, in quanto offre funzionalità nuove e interessanti, rivoluzionarie per il settore informatico come l'introduzione del mouse o del CD-ROM. Se al momento non si dispone di un'infrastruttura PKI interna, è necessario assicurarsi di eseguire questa operazione. Il presente documento non descrive l'installazione di questo ruolo in questo particolare articolo, ma per informazioni su come implementarlo, fare clic qui: <u>http://technet.microsoft.com/en-us/library/hh831740.aspx.</u>

Configurazione

In questa esercitazione si presume che il protocollo LDAP sia già stato integrato con VCS e che gli utenti possano eseguire l'accesso con le credenziali LDAP.

- 1. Apparecchiature di laboratorio
- 2. Installazione della smart card
- 3. Configura modelli Autorità di certificazione
- 4. Registra il certificato Agente di registrazione
- 5. Registra per conto di....
- 6. Configurazione di VCS per Common Access Card

Attrezzatura richiesta:

Server di dominio Windows 2012R2 con i seguenti ruoli/software installato:

- Autorità di certificazione
- Active Directory
- DNS
- PC Windows con smart card collegata
- vSEC Software di gestione CMS serie K per la gestione della smart card:



Software Versa Card Reader

Installazione della smart card

I lettori di smart card in genere includono istruzioni su come collegare i cavi necessari. Di seguito è riportato un esempio di installazione per questa configurazione.

Installazione del driver di un lettore di smart card

Se il lettore di smart card è stato rilevato e installato, la schermata di accesso di Windows riconosce questa condizione. In caso contrario:

- 1. Collegare la smart card alla porta USB del PC Windows
- Seguire le istruzioni visualizzate sullo schermo per l'installazione del driver di periferica. È quindi necessario che il supporto del driver utilizzato dal produttore della smart card o del driver sia individuato in Windows. Nel mio caso ho utilizzato il driver di Manufactures dal loro sito di download. NON CONSIDERARE ATTENDIBILE WINDOWS.
- 3. Fare clic con il pulsante destro del mouse sull'icona **Risorse del computer** sul desktop e scegliere **Gestisci** dal sottomenu.

- 4. Espandere il nodo Servizi e applicazioni e fare clic su Servizi.
- 5. Nel riquadro destro fare clic con il pulsante destro del mouse su **Smart Card**. Scegliere **Proprietà** dal sottomenu.
- 6. Nella scheda **General** (Generale), selezionare **Automatic** (Automatico) nell'elenco a discesa **Startup Type** (Tipo di avvio). Fare clic su **OK**.
- 7. Riavviare il computer se richiesto dall'Installazione guidata hardware.

Configura modelli Autorità di certificazione

- 1. Avviare MMC Autorità di certificazione da Strumenti di amministrazione.
- 2. Fare clic sul nodo Modelli di certificato o selezionarlo e selezionare Gestisci.
- 3. Fare clic con il pulsante destro del mouse o selezionare il modello di certificato **utente smart card** e quindi selezionare **Duplica** come illustrato nell'immagine.

a	Console1 - [C	onsole Root\Certifi	cate Temp	lates (2012DC	-AD.jajanson.local)]		_ D X
🚟 File Action View Favorites Window Hel	p						_ 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				Man Asting
	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 Authentio	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 Authentio	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 Authentio	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	$\overline{}$	
< III >	<				>		

Modelli di certificato controller di dominio

4. Nella scheda **Compatibilità**, in **Autorità di certificazione**, rivedere la selezione e modificarla se necessario.

compatibilità smart card

- 5. Nella scheda Generale:
- r. Specificare un nome, ad esempio User_VCS della smart card.
- b. Impostare il periodo di validità sul valore desiderato. Fare clic su Apply (Applica).

Subject Name Issuance Requirements Superseded Templates Extensions Security Server erral Compatibility Request Handling Cryptography Key Attestation emplate display name: martcard User_VCS emplate name: matcard User_VCS didity period: Renewal period: Iverant Iverant 6 weeks v Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory	Smartcare	d User_VCS Properties	? X						
Auperseded Templates Extensions Security Server errai Compatibility Request Handling Cryptography Key Attestation emplate display name: martcard User_VCS emplate name: martcard User_VCS and User_VCS and User_VCS Alidity period: Renewal period: Imatcard User_VCS Alidity period: Renewal period: Imatcard User_VCS Indity period: Renewal period: Imatcard User_VCS Alidity period: Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory Directory	Subject Name	Subject Name Issuance Requirements							
Image: Compatibility Request Handling Cryptography Key Attestation emplate display name: martcard User_VCS emplate name: martcard User_VCS didity period: Renewal period: Image: Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory	Superseded Templates	Extensions Security Server							
emplate display name: martcard User_VCS emplate name: martcard User_VCS didity period: Renewal period: Jyears 6 weeks Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory Directory	General Compatibility Requ	uest Handling Cryptography	Key Attestation						
martcard User_VCS emplate name: martcard User_VCS Midity period: Renewal period: Verificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory	Template display name:								
emplate name: martcard User_VCS Midity period: Renewal period: years v 6 weeks v Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory Directory	Smartcard User_VCS								
Publish certificate in Active Directory ☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory Directory	Template name: Smartcard User_VCS Validity period:	Renewal period:							
Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory	🔟 years 🗸	6 weeks V							
	Publish certificate in Active Do not automatically re Directory	e Directory enroll if a duplicate certificate ex	ists in Active						
OK Cancel Apply Help	OK	Cancel Apply	Help						

generale smart card

- 6. Nella scheda Gestione richieste:
- r. Impostare Scopo su Firma e accesso smart card.
- b. Fare clic su Chiedi conferma all'utente durante la registrazione. Fare clic su Apply (Applica).

	Prop	perties	of New	Template		
Subject Na	me	Sen	ver	Issuance	Requ	uirements
Supersede	d Templa	tes	Exte	ensions		Security
Compatibility (General	Request	Handling	Cryptograph	ıy K	Key Attestation
Purpose:	Signat	ture and s	martcard lo	ogon		¥
	Del	ete revok	ed or expir	ed certificates	(do n	ot archive)
	Inc	ude symm	netric algori	ithms allowed	by the	e subject
	Arc	hive subje	ect's encry	ption private k	ey	
Allow priva	te key to	be exporte	ed			
Renew wit	h the sam	e key (*)				
For automa	atic renew	al of smar created (*	t card certi)	ificates, use th	ne exis	sting key if a
Do the followir associated wit	ng when t h this cer	he subject tificate is u	t is enrolle used:	d and when th	e priv	rate key
🔿 Enroll subje	ect withou	t requiring) any useri	input		
Prompt the	user duri	ng enrollm	ent			
O Prompt the private key	user duri is used	ng enrollm	ient and re	quire user inpo	ut whe	en the
* Control is dis	abled due	e to <u>compa</u>	atibility sett	ings.		
	OK	(Cancel	Apply		Help
			s	mart card		

7. Nella scheda Crittografia impostare le dimensioni minime della chiave su 2048.

r. Fare clic su **Le richieste devono utilizzare uno dei provider seguenti**, quindi selezionare **Microsoft Base Smart Card Crypto Provider**.

b. Fare clic su Apply (Applica).

Prope	erties of New	Template	X				
Subject Name	Server	Server Issuance Requirements					
Superseded Template	es Ext	Extensions Security					
Compatibility General F	Request Handling	Cryptography	Key Attestation				
Provider Category:	Legacy Crypto	graphic Service	Provider v				
Algorithm name:	Determined by	CSP	~				
Minimum key size:	2048						
Choose which cryptograp	bhic providers can	be used for requ	ests				
Requests can use any	y provider availabl	e on the subject's	s computer				
Requests must use or	ne of the following	providers:					
Providers:							
Microsoft Base Smart Microsoft DH SChann Microsoft Enhanced C Microsoft Enhanced D Microsoft Enhanced F	Card Crypto Providuel Cryptographic P Cryptographic Prov OSS and Diffie-Hel RSA and AES Cryp	der Provider ider v1.0 Iman Cryptograph tographic Provid	nic Pr er ⊻				
Request hash:	Determined by	CSP	~				
Use alternate signatur	re format						
ОК	Cancel	Apply	Help				

crittografia certificato

8. Nella scheda Protezione aggiungere il gruppo di protezione a cui si desidera concedere l'accesso Registrazione. Ad esempio, se si desidera concedere l'accesso a tutti gli utenti, selezionare il gruppo Utenti autenticati e quindi selezionare **Registra** autorizzazioni per tali utenti.

. Strients						
	Pro	perties	of New	Template		x
Compatibility	General	Request	Handling	Cryptography	Key Attest	ation
Subject N	lame	Sen	ver	Issuance	Requirements	;
Supersec	ded Templa	ites	Ext	ensions	Security	
Group or use	rnames:					
& Authent	ticated Use	rs				
🔏 Adminis	trator (Adm	in@jajans	on.local)			
🍇 Domain	Admins (J	AJANSON	\Domain	Admins)		
👫 Enterpri	ise Admins	(JAJANSC	N\Enterp	orise Admins)		
			Γ	L L L	Demous	
			l	Add	Remove	
Permissions f	for Authent	icated Use	ers	Allow	Deny	
Full Contro	bl					
Read				~		
Write						
Enroll						
Autoenroll						
For special p	emissions	or advanc	ed setting	js, click	Advanced	
Advanced.					Auvanceu	
Γ	OK		Cancel	Apply	Hel	0
L	UN		Janoor	7469		P

9. Fare clic su **OK** per finalizzare le modifiche e creare il nuovo modello. Il nuovo modello deve essere visualizzato nell'elenco dei modelli di certificato.

E	Console1 - [C	onsole Root\Certifica	te Templ	ates (2012DC-AD.jajanson.local)]		
🜇 File Action View Favorites Window Hel	P					_ @ ×
🗢 🔿 🙍 🔀 🖾 🛣 🔛						
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			Man Astissa
	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			More Actions
	Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Smart Card Logon		indicacións y
	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			
	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, R	D	
	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 Authority	1	5.1			
	Router (Offline request)	1	4.1			
	Real 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			
	Region SMART	2	100.8	Smart Card Logon, Client Authentication		
	I Web Server	1	4.1			
	2 Webclientandserver	2	100.4	Client Authentication, Server Authentication		
	Workstation Authentication	2	101.0	Client Authentication	×	
< III >	<	ш			>	
36 certificate templates						

Modello visualizzato nel controllo del dominio

10. Nel riquadro sinistro di MMC espandere Autorità di certificazione (locale), quindi l'Autorità di certificazione nell'elenco Autorità di certificazione.

Fare clic con il pulsante destro del mouse su Modelli di certificato, scegliere **Nuovo** e quindi fare clic su **Modello di certificato** da rilasciare. Scegliere quindi il modello di smart card appena creato.

a	Console1 - [Console Roo	ot\Certification Authority (Local)\jajanson-2012DC-AD-CA\Certificate Templates]		_ 🗆 X
Tile Action View Favorites Window Help				_ 8 ×
🗢 🔿 🙍 💽 🔒 📓 🗊				
Console Root Name		Intended Purpose	Actions	
D Certificate Templates Exchange	e Enrollment Agent (Offline r	Certificate Request Agent	Certificate Templates	
a 🙀 Certification Authority (Local) 🖉 IPSec (O	fline request)	IP security IKE intermediate	Mars Astians	
a 🛃 jajanson-2012DC-AD-CA 🛛 😨 Webclie	tandserver	Client Authentication, Server Authentic	More Actions	
Revoked Certificates Schang	e Signature Only	Secure Email		
Ssued Certificates CEP Enc	yption	Certificate Request Agent		
Smartca	d User_VCS	Secure Email, Client Authentication, Sm		
Catificate Terralities	in_SMART	Smart Card Logon, Client Authentication		
Manage	: Agent	Certificate Request Agent		
Nev	mail Replication	Directory Service Email Replication		
New	ontroller Authentication	Client Authentication, Server Authentic		
View	uthentication	Client Authentication, Server Authentic		
New Window from Here	try Agent	File Recovery		
New Taskpad View		Encrypting File System		
	ontroller	Client Authentication, Server Authentic		
Refresh	r	Server Authentication		
Export List		Client Authentication, Server Authentic		
Help		Encrypting File System, Secure Email, Cl		
	ate Certification Authority	<all></all>		
a Adminis	rator	Microsoft Trust List Signing, Encrypting		

Rilascia nuovo modello

11. Una volta replicato il modello, in MMC fare clic con il pulsante destro del mouse o selezionare l'elenco Autorità di certificazione, scegliere **Tutte le attività**, quindi **Arresta servizio**. Fare quindi nuovamente clic con il pulsante destro del mouse sul nome della CA, scegliere **Tutte le attività**, quindi **Avvia servizio**.



Arresta e avvia i servizi certificati

Registra nel certificato Agente di registrazione

Si consiglia di eseguire questa operazione su un computer client (desktop amministratori IT).

1. Avviare MMC. Scegliere **Certificati**, fare clic su **Aggiungi**, quindi su Certificati per **Account utente**.



Aggiungi certificati

2. Fare clic con il pulsante destro del mouse o selezionare il **nodo personale**, selezionare **Tutte le attività** e quindi **Richiedi nuovo certificato**.

Co	nsole1 - [Console Root\Certificates - Current User\Personal]	_ □ X
🚡 File Action View Favorites Window He	lp	_ <u></u> 5 ×
Console Root Object Type		Actions
△ 💭 Certificates - Current User 📔 Certificates		Personal
▷ Pe ▷ □ Tr Find Certificates		More Actions
En All Tasks	Find Certificates	
▷ Int ▷ Ac New Window from Here	Request New Certificate Import	
▷ 📋 Ur New Taskpad View	Advanced Operations	
 ▷ □ Ir ▷ □ Tr ▷ □ CI Export List 		
⊳ Ce Help		
 Sharcer riscer riscer too Gertification Authority (Loc jajanson-2012DC-AD-Ci 		
Personal store contains 9 certificates.		

Richiedi nuovi certificati

3. Fare clic su **Avanti** nella procedura guidata e quindi selezionare **Criteri di registrazione di Active Directory**. Quindi fare di nuovo clic su **Avanti**.

	Concolo 1 - IConcolo Doot/Cartificator - Current Usor/Dorconall	
File Action View		X
Console Root Certificates - Curren Personal Pi Trusted Root Certificates - Curren Certi	Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.	s mal A ore Actions
Intermediate Cer Active Directory	Configured by your administrator	
Trusted Publishe	Active Directory Enrollment Policy 🗸	
 ▷ □ Untrusted Certifi ▷ □ Third-Party Root ▷ □ Trusted People ▷ □ Client Authentic ▷ □ Certificate Enroll ▷ □ Smart Card Trust ⊿ □ Certification Author ▷ □ jajanson-2012DC 	Configured by you Add New	
< III Personal store contains 9 cer	Next Cancel	

Registrazione Active Directory

4. Selezionare il **certificato Agente di registrazione**, in questo caso **Smart Card User_VCS**, quindi fare clic su **Registra.**



Agente certificato di registrazione

Il desktop degli amministratori IT è ora configurato come stazione di registrazione, consentendo di registrare nuove smart card per conto di altri utenti.

Registra per conto di....

Per fornire ai dipendenti le smart card per l'autenticazione, è necessario registrarle e generare il certificato che verrà quindi importato nella smart card.



1. Avviare MMC e importare i certificati Modulo certificati e manager per II mio account utente.

2. Fare clic con il pulsante destro del mouse o selezionare **Personale > Certificati** e selezionare **Tutte le attività > Operazioni avanzate** e fare clic su **Registra per conto di...**

3. Nella procedura guidata, scegliere il criterio di registrazione di Active Directory, quindi fare clic su **Avanti**.



Registrazione per conto di utenti avanzati

file Action View Forum Window Help			Console1 - [Console Root\Certif	icates - Current U	ier/Personal/Certifi	cates)				= 0 X
Constant Note Constant Note Constants : Current Var Conficiant Conficiant	🖀 File Action View Favorites Window Hel	p								_ 0 ×
General Name Based 18			lan san							
Persond Ortification Ortifi	Console Root a (2) Certificates - Current User	Sound To	isiamon-2012DC-AD-CA	Expiration Date 10/14/2019	Entended Purposes Cartificate Request	Friendly Nome (None)	Status	Cetti	Actions	
Linking Transfer Linking Extension Linking Extension Extension Linking Extension Extension <	a 🛄 Personal	Administrator	Jejanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	«None»		Adr	Certificates Mon Actions	
Entreprise Truet Intermediate Configuration Authorities Intermediate Configuration Authorities<	Certification Authorities	Administrator				- 0 X		Fore		-
> Active Direction Constraints Another the Direction Autiversity Since Large 1.34 > Constraints Another the Direction Autiversity Before You Begin 5.35 > Trusted Partials Provide Configuration Autiversity Before You Begin 5.36 > Constraints Another the Direction Autiversity Before You Begin 5.36 > Constraints Another the Direction Autiversity Before You Begin 5.36 > Constraints Another Scale The Direction Autiversity Before You Begin 5.36 > Constraints Another Scale The Direction Autiversity Before You Begin 5.36 > Constraints Another Scale The Direction Autiversity Before You Begin 5.36 > Constraints Another Scale The Direction Autiversity Before You Begin 5.36 > Serves Card Trusted Reverse Before requesting a conflicted to the network Your constraint the used to verify your right to obtain the centificate 5.36 Yes Another Card Trusted Reverse Net Cancel 5.36 Yes Another Card Trusted Reverse Net Cancel	p 🛄 Enterprise Trust	injarson-2012	Certificate Enrollment							
Image: Transfer T	p 🛄 Active Directory User Object	Soft Leng						13.6 Sma		
Inited-Party Rate Certification Authonitian Image: Control and Starting and Transfer Reports Image: Control and Starting and S	p 11 Trusted Publishers b 12 Untrusted Cartificates	Scott Long	Before You Begin					Sme		
Institud Program Institud Program Image: Control Content, establish Identity, and 00 other security-resided tasks. Image: Control Content, establish Identity, and 00 other security-resided tasks. Image: Control Content, establish Identity, and 00 other security-resided tasks. Image: Control Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Identity, and 00 other security-resided tasks. Image: Content Content, establish Ident Identide tasks. Im	D Third-Party Root Certification Authorities	Scott Lang	The following steps will help you install certifi	cates, which are digit	I credentials used to co	nect to window		Sma		
b Certificate Evolution Requests b Small Card Trusted Roots Vour computer is connected to the network You have credentials that can be used to varify your right to obtain the certificate	 D Trusted People Client Authentication Issuers 		networks, protect content, establish identity, i	and do other security-	related tasks.					
Vour computer is connected to the network Yeu have credentials that can be used to verify your right to obtain the certificate Next	b Certificate Envolment Requests		Before requesting a certificate, verify the follo	wing						
Net Cancel	p Smert Card Trusted Roots		Your computer is connected to the network You have credentials that can be used to varif	y your right to obtain	the certificate					
Net Cancel										
Net Cancel										
Net Cancal										
Next Cancal										
Next Cancal										
Next Cancal										
Net Cancel										
					Next	Cancel				
Among the contribut Contributer	Parasoni strea contains 9 centification	¢						>		

4. Selezionare Criteri di registrazione certificati, quindi fare clic su Avanti.

-	C	onsole1 - [Console Root\Certifica	ites - Current Us	er\Personal\Certific	ates]				- 🗆 X
Tile Action View Favorites Window Help									_ 8 ×
(+ +) 🖄 🖬 🛄 🔍 🕞 📓 📷									
Console Root Issued	d To 📍	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
a 💭 Certificates - Current User	dministrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request	<none></none>		Enro	Certificates	•
Certificates	dministrator dministrator	jajanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	<none></none>		Adm	More Actions	•
D Interview Trusted Root Certification Authorities 2 Adress Adres Adress Adres Adress Adres Adress Adress Adress Adress Adress Adress Adress Adres Adress Adress Adress Adress Adres Adres Adres Adres Adres Adre	dministrator						Enro		
Enterprise Trust Intermediate Certification Authorities	janson-2012 🔜 Certifica	te Enrollment					126		
Active Directory User Object Sco	ott Lang						Sma		
D Intrusted Publishers Untrusted Certificates	ott Lang Selec	t Certificate Enrollment Policy					Sma		
Third-Party Root Certification Authorities	cott Lang Certific	ate enrollment policy enables enrollment	for certificates base	d on predefined certific	ate templates.		Sma		
b I Trusted People b I Client Authentication Issuers	Certifi	cate enrollment policy may already be con	figured for you.						
Certificate Enrollment Requests	Confi	gured by your administrator							
D Smart Card Trusted Roots	Activ	ve Directory Enrollment Policy			v				
	Confi	gured by you			Add New				
				Next	Cancel				
					_				
<.							>		
Personal store contains 9 certificates.									

Criteri di registrazione

5. Verrà richiesto di selezionare il **certificato di firma**. Si tratta del certificato di registrazione richiesto in precedenza.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]								
File Action View Favorites Window He	elp							_ 8 ×
🗢 🔿 🙍 🗊 📋 🙆 😹 🔝								
Console Root Certificates - Current User Certificates - Current User Certificates Certificates Certificates	Issued To	Issued By Expiration Date Inten jajanson-2012DC-AD-CA 10/14/2019 Certi jajanson-2012DC-AD-CA 10/12/2018 Micr		Intended Purposes Certificate Request Microsoft Trust List	Friendly Name Status C , <none> E , <none> A - □ X</none></none>		Certi Actions Enro Adrr Enro Enro Enro Enro Enro Enro Enro En	•
 Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Active Directory User Object Trusted Publishess Thusted Publishess Thusted Publishess Thusted Publishess Thusted People Client Authentication Issuers Certificate Enrollment Requests Smart Card Trusted Roots 	Administrato Ad	Window Select a Certificate Administrator Issue: jajanson-20 Valid From: 10/14/ Click here to view. properties Administrator Issue: jajanson-20 Valid From: 10/12/	vs Security 12DC-AD-CA 2017 to 10/14/2019 certificate. 12DC-AD-CA 2017 to 10/12/2019 OK	Cancel	her users. Click Browse Cancel	Enro 1.3.6 Sma Sma Sma		
Personal store contains 9 certificates.	<	ш				>		

Seleziona certificato di firma

6. Nella schermata successiva, è necessario selezionare il certificato che si desidera richiedere e, in questo caso, è **Smartcard User_VCS** il modello creato in precedenza.

a		Console1 - [Console Root\Certif	icates - Current U	er\Personal\Certifi	cates]				_ 🗆 X
File Action View Favorites Window He	lp								- 8 ×
File Action View Favorites Window He File Action View Favorites Window He File Certificates - Current User Certificates - Current User Certificates - Certification Authorities Certificates Certification Authorities Certificates Certification Authorities Certificates - Current User Object Certificates - Certification Authorities Certificate Certification Authorities Certificate Roote Certificate Income Certification Authorities Sector Certificates - Certification Authorities Certificate Enclower Certification Authorities Certificate Enclower Certification Authorities Certificate Enclower Certification Success Certificate Certificates - Certificates - Certification Success Certificate - Certificates - Certification Success Certificate - Certificates - Certification Success Certificate - Certificates - C	Ap	Console1 - [Console Root\Certif	Expiration Date 10/14/2019 10/12/2018 idea and a second	er\Personal\Certifi Intended Purposes Certificate Request Microsoft Trust List Cates you want to reque cates you want to reque cates click here to configure cates click here to co	cates]	Status	Certi Enro Adrr Enro 1.3.6 Sma Sma Sma	Actions Certificates More Actions	
	<						>		
Personal store contains 9 certificates.									

Scelta della smart card VCS

7. Quindi, è necessario selezionare l'utente che si desidera iscrivere per conto di. Fare clic su **Sfoglia** e digitare il nome utente del dipendente che si desidera iscrivere. In questo caso viene utilizzato l'account 'antman@jajanson.local' di Scott Lang.

· 🖀		Console1 - [Console Root\Certif	ïcates - Current U	ser\Personal\Certifi	icates]				_ 🗆 X
Tile Action View Favorites Window He	IP								_ @ ×
◆ ⇒ 2 🗊 🗓 🛛 💀 🛛 🗊									
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 Involution Certificates Certificate Enrollment Requests Certificate Enrollment Requests Certificate Authentication Susers Certificate Certificate Roots	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Select User Select this object type: User From this location: jajanson local Enter the object name to select (cosmoles): Scott Lana (antman@ajanson local) Advanced	Ехрігаtion Date 10/14/2019 10/12/2018 Спе ОК Спе	Intended Purposes Certificate Request Microsoft Trust List et Types ations ck Names cancel	Friendly Name <none> <none> T T T T T T T T T T T T T T T T T T T</none></none>	Status C E E 1 S S S S	Certi Actions inro ddm 3.3.6 ima ima ima	s icates ore Actions	,
	<		Ш				>		
Personal store contains 9 certificates.									

Scegli l'utente

8. Nella schermata successiva, procedere con la registrazione facendo clic su **Enroll**. Inserire una smart card nel lettore.

		Console1 - [Console Root\Certifi	cates - Current U	ser\Personal\Certifi	cates]			_ 🗆 X
Tile Action View Favorites Window He	lp.							_ <i>6</i> ×
(+ +) 2 🗊 🗓 🍳 🕞 🔟 🗊								
 File Action View Favorites Window He File Action View Favorites Window He Console Root Certificates - Current User Certificates - Current User Certificates - Certification Authorities Enterprise Trust Enterprise Trust Intermediate Certification Authorities Active Directory User Object Trusted Poublishers Untrusted Certificate Certification Authorities Cirtificate Root Trusted People Client Authentication Issuers Smart Card Trusted Roots 	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA cate Enrollment ct a user equest a certificate on behalf of another u pple, Firstname Lastname, username, or d re enrolling for a certificate, make sure the hed.	Expiration Date 10/14/2019 10/12/2018 see, enter the formal omain\username. e device on which the	Intended Purposes Certificate Request Microsoft Trust List name or domain name of e user certificate needs to the user certificate needs to Enrol	Friendly Name <none> (None> f that user. For b be installed is Browse</none>	Status CC En Ar 11 Sn Sn Sn	rti Actions Certificates irri More Actions 1.6 1.6 1.6 1.6 1.6 1.6 1.6 1.6	_ @ X
	<		1				>	
Personal store contains 9 certificates.								

Registrati

9. Una volta inserita la smart card, viene rilevata come segue:

leques	Windows Security	
he enrol Adhe D	Enrolling for the user certificate. Select a smart card device	
®Yan	Axaito Cryptoflex .NET Gemulto USB Smart Card Reader 0 The smart card is ready for use.	

10. Viene quindi richiesto di immettere un numero PIN della smart card (PIN predefinito: 0000).

Texted Forder Status Certificates Status Certificates Sontal Certificates Certificates Certificates Certificates Certificates Certificates Sontal Certificates Sontal Certificates Certificates Sontal Certificates Certificates Sontal Certificates Certificates Sontal Certificates Sontal Certificates Certificates Sontal Certificates Sontal Certificates Certificates Sontal Certificates Certificates Sontal Certificates Sontal Certificates Certificates Sontal Certificates Certificates Sontal Certificates Sontal Certificates Sontal Certificates Certificates Certificates Sontal Certificates Certificates Certificates Certificates Certificat	a	Cons	sole1 - [Console Root\Certific	ates - Current Us	er\Personal\Certifi	cates]			_ 🗆 X
Concise Real C	Tile Action View Favorites Window Hel	p							_ 8 ×
Issued By Expression Statue By Expression Statue Size Certificaties Image: Statue Size Firstonia Turited Root Certification Authonities None Actions More Actions More Actions Certificaties More Actions More Actions <td>🗢 🔿 🙍 🗊 📋 🖉 📷</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	🗢 🔿 🙍 🗊 📋 🖉 📷								
	Console Root Certificates - Current User Certificates Certificate Certification Authorities Certificate People Cient Authentication Issuers Certificate Enrollment Requests Smart Card Trusted Roots	Issued To	Issued By jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA Enrolling for the user certi Please enter your authentication P PIN PIN Elick here for most	Expiration Date 10/14/2019 10/12/2018 ws Security ficate. IN. te information OK	Intended Purposes Certificate Request Microsoft Trust List X Cencel	Friendly Name <none></none>	Status Cr Er Ai Er 11 Sr Sr Sr	erti Certificates More Actions 3.6 ma ma ma ma	•
Internet dates contained and finates									
AF FINDING STOLE STOLEGY AND A S	Personal store contains 9 certificates.	<						>	

Immettere il pin

11. Infine, una volta visualizzata la schermata **Iscrizione riuscita**, è possibile utilizzare questa smart card per accedere a un server aggiunto al dominio, come il VCS con solo la scheda e un pin noto. Tuttavia, non è stato fatto sì, è comunque necessario preparare il VCS per reindirizzare le richieste di autenticazione alla smart card e utilizzare la smart card Common Access Card per rilasciare il certificato della smart card archiviato nella smart card per l'autenticazione.

🖵 Cer	tificate Enrollment		_ 0 X
0	ertificate Installation Results te following certificates have been en	olled and initialied on this computer.	
E.	Active Directory Enrolment Policy		
	Wakkundig Smartcard Uter	✓ STATUS: Succeeded	Details ¥
			Next user Cose

Configurazione di VCS per Common Access Card

Caricare la CA radice nell'elenco dei certificati CA attendibili nel software VCS selezionando Manutenzione > Sicurezza > Certificato CA attendibile.

2. Caricare nel software VCS l'elenco di revoche di certificati firmato dalla CA radice. Passare a Manutenzione > Sicurezza > Gestione CRL.

3. Verificare il certificato client con il regex che estrae il nome utente dal certificato da utilizzare per l'autenticazione con il protocollo LDAP o l'utente locale. Il regex verrà confrontato con il **soggetto** del certificato. Può essere il tuo UPN, email e così via. In questa esercitazione è stato utilizzato il messaggio di posta elettronica corrispondente al certificato client per il certificato client.

搹 Certificate	×
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

Oggetto del certificato client

4. Passare a **Manutenzione > Sicurezza > Test certificati client**. Selezionare il certificato client da testare, in My lab era antman.pem, caricarlo nell'area di test. Nella sezione **Modello di autenticazione basato su certificato** in **Regex** incollare il regex da verificare. Non modificare il campo **Formato nome utente**.

My Regex: /Subject:.*emai	llAddress=(?.*)@jajanson.local/m
CISCO Cisco TelePresence Video Communication Server Expressway	This system fact 4 aleman
Status System Configuration Applications Users Maintenance	
Client certificate testing	You are here: Harmonice - Electric confidence - Cite
Citerif contificate	
	The tests whether a client certificate is valid when checked against the VCD's current trusted CA. Ist and, if baded, the twococition list
Certificate source	Uploaded test file (PEM format) J/
Belect the file you want to test	Browse. No file selected.
Currently uphraded text file	alterna para
Certificate-based authentication pattern	
	This sector applies only if your certificate contains antimetration condentials and your want to use certificate/assed authentitation as your client certificate/assed security secting. It less you test the outcome of applying regax and usemanie format contributions to the nominal certificate asset.
Regex to metch agenus certificate	Column - Heraldonian (- Stagenet Connectioner - 1000eces Column
Usernams format	RayuntunnoNanet J
	Main these satings personent

Prova regex in VCS



Risultati test

5. Se il test fornisce i risultati desiderati, è possibile fare clic sul pulsante **Rendi permanenti le modifiche**. In questo modo viene modificato il regex per la **configurazione dell'autenticazione basata su certificati** del server. Per verificare la modifica, passare alla configurazione **Manutenzione > Protezione > Autenticazione basata su certificati**.

6. Abilitare l'autenticazione basata su client passando a Sistema > Amministratore e quindi selezionare o fare clic sulla casella a discesa per scegliere Protezione basata su certificati client = Autenticazione basata su client. Con questa impostazione, l'utente digita il nome di dominio completo (FQDN) del server VCS nel browser e gli viene richiesto di scegliere l'account client e immettere il PIN assegnato alla scheda di accesso comune. Il certificato viene quindi rilasciato e l'utente riceve la GUI Web del server VCS e deve solo fare clic o selezionare il pulsante Administrator (Amministratore). Poi viene ammesso nel server. Se si seleziona l'opzione Protezione basata su certificati client = Convalida basata su client, il processo è lo stesso, con l'eccezione che quando l'utente fa clic sul pulsante Amministratore, ha richiesto nuovamente la password amministratore. Di solito, quest'ultimo non è quello che l'organizzazione sta cercando di ottenere con CAC.

CISCO Cisco Expressway-E

Status	System	Configuration	Applications	Users	Maintenance	
System	n administ	ration				
Epheme	eral port range er	d				* 49999
Servic	es					
Serial p	ort / console					0n 🗸 (1)
SSH se	rvice					On 🗸 👔
Web int	erface (over HT	TPS)				On 🗸 👔
Sessio	on limits					
Session	n time out (minute	s)				* 30
Per-acc	count session lim	t				* 0
System	session limit					* 0
System	n protection					
Automa	ited protection se	rvice				0n 🗸 (1)
Automa	tic discovery pro	tection				On 🗸 (i)
Web s	erver configura	ition				
Redirec	t HTTP requests	to HTTPS				0n 🗸 (i)
HTTP S	trict Transport Se	ecurity (HSTS)				On 🗸 (1)
Web ad	Iministrator port					443 🗸 👔
Client c	ertificate-based	security				Not required 🗸
Save						Drop down the above box and choose Client-Based Authentication
Relate	d tasks					
Upload	a CA certificate	file for HTTPS				
Test clie	ent certificates					

Abilita autenticazione basata su client

Aiuto! Sono bloccato!!!

Se si abilita l'autenticazione basata sul client e il VCS rifiuta il certificato per qualsiasi motivo, non sarà più possibile accedere alla GUI Web nel modo tradizionale. Ma, non preoccuparti, c'è un modo per tornare nel tuo sistema. Il documento allegato è disponibile sul sito Web Cisco e fornisce informazioni su come disabilitare l'autenticazione basata su client dall'accesso alla radice.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.