Configure o VCS com CAC e um leitor de Smart Card

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio O que é um Smart Card? Configurar Verificar Troubleshoot

Introduction

Este documento descreve um guia passo a passo para instalar e usar um leitor de Smart Card e um cartão de acesso comum para uso com o Cisco Video Communication Server (VCS) para organizações que exigem autenticação de dois fatores para o ambiente VCS, como bancos, hospitais ou governos com instalações seguras.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Expressway Administrator (X14.0.2).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O CAC fornece a autenticação necessária para que os "sistemas" saibam quem ganhou acesso ao seu ambiente e que parte da infraestrutura é física ou eletrônica. Nos ambientes classificados pelo governo e em outras redes seguras, prevalecem as regras do "acesso menos privilegiado" ou da "necessidade de saber". Um login pode ser usado por qualquer pessoa, a autenticação requer algo que o usuário tem, depois de remover o CAC, também conhecido como Cartão de Acesso Comum, lançado em 2006 para que o indivíduo não precise ter vários dispositivos, sejam eles fobs, cartões de identificação ou dongles para acessar seu local de trabalho ou sistemas.

O que é um Smart Card?

Os cartões inteligentes são um componente chave da infraestrutura de chave pública (PKI) que a Microsoft usa para integrar à plataforma Windows porque os cartões inteligentes aprimoram soluções somente de software, como autenticação de cliente, login e e-mail seguro. Os cartões inteligentes são um ponto de convergência para certificados de chave pública e chaves associadas porque:

- Fornece armazenamento resistente a adulterações para proteção de chaves privadas e outras formas de informações pessoais.
- Isole as computações críticas de segurança, que envolvem autenticação, assinaturas digitais e troca de chaves de outras partes do sistema que não precisam saber.
- Habilitar a portabilidade de credenciais e outras informações privadas entre computadores no trabalho, em casa ou em trânsito.

O cartão inteligente tornou-se parte integrante da plataforma Windows porque os cartões inteligentes fornecem recursos novos e desejáveis, tão revolucionários para a indústria de computadores como a introdução do mouse ou CD-ROM. Se você não tem uma infraestrutura interna de PKI no momento, é preciso garantir que faça isso primeiro. Este documento não aborda a instalação desta função neste artigo específico, mas informações sobre como implementá-la podem ser encontradas aqui: <u>http://technet.microsoft.com/en-us/library/hh831740.aspx.</u>

Configurar

Este laboratório pressupõe que você já tenha um LDAP integrado com VCS e que tenha usuários que possam fazer login com credenciais LDAP.

- 1. Equipamento de laboratório
- 2. Instale o Smart Card
- 3. Configurar modelos de autoridade de certificado
- 4. Inscreva o certificado do agente de inscrição
- 5. Inscrever-se em nome de...
- 6. Configure o VCS para a placa de acesso comum

Equipamento necessário:

Servidor de Domínio do Windows 2012R2 que tem estas funções/software instalado:

- Autoridade de certificação
- Ative Diretory
- DNS
- PC Windows com Smart Card conectado
- vSEC: Software de gerenciamento CMS K-Series para gerenciar seu Smart Card:



Software Versa Card Reader

Instale o Smart Card

Os leitores de Smart Card geralmente recebem instruções sobre como conectar os cabos necessários. Aqui está um exemplo de instalação para esta configuração.

Como instalar um driver de dispositivo do leitor de Smart Card

Se o leitor de cartão inteligente tiver sido detectado e instalado, a tela Bem-vindo ao login do Windows confirmará isso. Caso contrário:

- 1. Conecte seu Smart Card à porta USB no PC Windows
- 2. Siga as instruções na tela para instalar o software do driver do dispositivo. Isso exige a mídia do driver que o fabricante do smart card ou do driver foi descoberto no Windows. No meu caso, usei o driver de fabricação do site de download. **NÃO CONFIE EM JANELAS**.
- 3. Clique com o botão direito do mouse no ícone **Meu computador** na área de trabalho e clique em **Gerenciar** no submenu.
- 4. Expanda o nó Serviços e aplicativos e clique em Serviços.

- 5. No painel direito, clique com o botão direito do mouse em **Smart Card**. Clique em **Propriedades** no submenu.
- 6. Na guia Geral, selecione Automático na lista suspensa Tipo de inicialização. Click OK.
- 7. Reinicie a máquina se o Assistente de hardware instruir você a fazê-lo.

Configurar modelos de autoridade de certificado

- 1. Inicie a Autoridade de Certificação MMC a partir de Ferramentas Administrativas.
- 2. Clique ou selecione o nó Modelos de certificado e selecione Gerenciar.
- 3. Clique com o botão direito do mouse ou selecione **Smartcard User** Certificate Template e selecione **Duplicate** conforme mostrado na imagem.

Console1 - [Console Root\Certificate Templates (2012DC-AD.jajanson.local)]								
k File Action View Favorites Window Hel	P						- 8 ×	
Console Root	Template Display Name	Schema Version	Versi	Intended Purpose	8	_	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 Antinen	
	Basic EFS	1	3.1				More Actions	
	CA Exchange	2	106.0	Private Key Archi	val		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	Email Replication			
	Domain Controller	1	4.1					
	Domain Controller Authentication	ontroller Authentication 2 110.0 Client Authentication, Server Authentication, Smart Card Logon						
	EFS Recovery Agent	1	6.1					
	Enrollment Agent	1	4.1					
	Enrollment Agent (Computer)	1	5.1			=		
	Rechange Enrollment Agent (Offline requ	1	4.1					
	Exchange Signature Only	1 6.1						
	Exchange User	1	7.1					
	@ IPSec	1	8.1					
	IPSec (Offline request)	1	7.1					
	Kerberos Authentication	2	110.0	Client Authentica	tion, Server Authentication, Smart Card Logon, KD			
	Key Recovery Agent	2	105.0	Key Recovery Age	ent			
	OCSP Response Signing	3	101.0	OCSP Signing				
	RAS and IAS Server	2	101.0	Client Authentica	tion, Server Authentication			
	Root Certification Authority	1	5.1					
	Router (Offline request)	1	4.1					
	Smartcard Logon	1	6.1					
	Smartcard User		11.1		Dualizata Tamalata			
	Smartcard User_VCS	4	101.6	Secure Email	ogon ogon			
	Subordinate Certification Authority	1	5.1		All Tasks 🕨			
	Trust List Signing	1	3.1		Properties			
	🖉 User	1	3.1					
< III 5	Contraction Cali				нер	Ť		
· · · · · · · · · · · · · · · · · · ·			_		12			

Modelos de certificado do controlador de domínio

4. Na guia **Compatibilidade**, em **Autoridade de certificação**, revise a seleção e altere-a, se necessário.

Smarte	card User_VCS	Properties	? X
Subject Name	suance Require	ements	
Superseded Templates	Extensions	Security	Server
General Compatibility	Request Handling	Cryptography	Key Attestation
The template options ava versions set in Compatibi	ailable are based on lity Settings. ges	the earliest ope	rating system
Compatibility Settings			
Windows Server 201	2 R2	~	
Certificate recipient Windows 8.1 / Wind	ows Server 2012 R.	~	
These settings may not p template.	orevent earlier operat	ing systems fron	n using this
ОК	Cancel	Apply	Help

compatibilidade de Smart Card

- 5. Na guia Geral:
- a. Especifique um nome, como Smartcard User_VCS.
- b. Defina o período de validade para o valor desejado. Clique em Apply.

	Smart	tcard User_VCS	Properties	? X
(Subject Name		ssuance Require	ements
Superse	eded Templates	s Extensions	Security	Server
General	Compatibility	Request Handling	Cryptography	Key Attestation
Template	e display name:			
Smartca	rd User_VCS			
Template Smartca Validity p	e name: rd User_VCS eriod:	Renewal	period:	
10	years V	6	weeks 🗸	
Publis	sh certificate in o not automatic irectory	Active Directory ally reenroll if a duplic	ate certificate e	xists in Active
	ОК	Cancel	Apply	Help

cartão inteligente vencimento

- 6. Na guia Solicitar tratamento:
- a. Defina a Finalidade como Login de assinatura e cartão inteligente.
- b. Clique em Solicitar ao usuário durante a inscrição. Clique em Apply.

Prop	perties of Nev	v Template	X					
Subject Name	Server	Issuance Requirements						
Superseded Templa	tes E	tensions	Security					
Compatibility General	Request Handling	Cryptography	Key Attestation					
Purpose: Signature and smartcard logon								
Del	ete revoked or exp	vired certificates (do not archive)					
_ Inc	lude symmetric algo	orithms allowed by	y the subject					
Arc	hive subject's encr	yption private key	y					
Allow private key to	be exported							
Renew with the sam	e key (*)							
For automatic renew new key cannot be	ral of smart card ce created (*)	rtificates, use the	existing key if a					
Do the following when t associated with this cert	he subject is enroll tificate is used:	ed and when the	private key					
O Enroll subject without	t requiring any use	r input						
• Prompt the user duri	ng enrollment							
Prompt the user duri private key is used	ng enrollment and i	require user input	when the					
* Control is disabled due	e to <u>compatibility se</u>	ttings.						
ОК	Cancel	Apply	Help					

Solicitações de Cartão Inteligente

7. Na guia **Cryptography**, defina o tamanho mínimo da chave como 2048.

a. Clique em **Requests must use a um dos seguintes provedores** e selecione **Microsoft Base** Smart Card Crypto Provider.

b. Clique em Apply.

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:
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:
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: The service of the following providers: Providers:
Provider Category: Legacy Cryptographic Service Provider Algorithm name: Determined by CSP Minimum key size: 2048 Choose which cryptographic providers can be used for requests O Requests can use any provider available on the subject's computer Image: Providers:
Algorithm name: Determined by CSP v Minimum key size: 2048 Choose which cryptographic providers can be used for requests O Requests can use any provider available on the subject's computer Image: The sequest of the following providers: Providers:
Minimum key size: 2048 Choose which cryptographic providers can be used for requests O Requests can use any provider available on the subject's computer
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:
 Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers:
 Requests must use one of the following providers: Providers:
Providers:
Microsoft Base Smart Card Crypto Provider 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 Microsoft Enhanced RSA and AES Cryptographic Provider
Request hash: Determined by CSP v
Use alternate signature format
OK Cancel Apply Help

criptografia de certificado

8. Na guia Segurança, adicione o grupo de segurança ao qual deseja conceder acesso de Inscrição. Por exemplo, se quiser conceder acesso a todos os usuários, selecione o grupo de usuários autenticados e selecione **Inscrever** permissões para eles.

		. memer en	
Pro	perties of New	Template	X
Compatibility General	Request Handling	Cryptography	Key Attestation
Subject Name	Server	Issuance R	equirements
Superseded Templa	ates Ext	ensions	Security
Group or user names:			
& Authenticated Use	ers		
🤱 Administrator (Adm	iin@jajanson.local)		
Solution Admins (J.	AJANSON\Domain	Admins)	
Manual Enterprise Admins	(JAJANSON\Enterp	vrise Admins)	
	[Add	Remove
Permissions for Authent	icated Users	Allow	Deny
Full Control			
Read		∠	
Write			
Enroll			
Autoenroli			
-			
For special permissions Advanced	or advanced setting	js, click	Advanced
ОК	Cancel	Apply	Help
	rr	nodelo	

9. Clique em **OK** para finalizar suas alterações e criar o novo modelo. O novo modelo deve aparecer agora na lista de Modelos de certificado.

Console1 - [Console Root\Certificate Templates (2012DC-AD.jajanson.local)]									
🖀 File Action View Favorites Window Hel	p					- 8 ×			
🗢 🔿 🙍 🔀 🖾 😹 🔝 💼									
Console Root	Template Display Name	Schema Version	Versi	Intended Purposes	^	Actions			
Certification Authority (Local)	Code Signing	1	3.1			Certificate Templates (2012DC-AD iai			
Certificate Templates (2012DC-AD.jajanson.loc	Computer	1	5.1			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		more Actions			
	EFS Recovery Agent	1	6.1						
	Enrollment Agent	1	4.1						
	Enrollment Agent (Computer)	1	5.1						
	R Exchange Enrollment Agent (Offline requ	1	4.1						
	Exchange Signature Only	1	6.1						
	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, 8	D				
	Key Recovery Agent	2	105.0	Key Recovery Agent					
	OCSP Response Signing	3	101.0	OCSP Signing					
	RAS and IAS Server	2	101.0	Client Authentication, Server Authentication	=				
	Root Certification Authority	1	5.1						
	Router (Offline request)	1	4.1						
	Smartcard Logon	1	6.1						
	Smartcard User	1	11.1						
	Smartcard User_VCS	4	101.6	Secure Email, Client Authentication, Smart Card Logon					
	Subordinate Certification Authority	1	5.1						
	Trust List Signing	1	3.1						
	User	1	3.1						
	User Signature Only	1	4.1						
	VCS_Login_SMART	2	100.8	Smart Card Logon, Client Authentication					
	Web Server	1	4.1						
	Webclientandserver	2	100.4	Client Authentication, Server Authentication					
	Workstation Authentication	2	101.0	Client Authentication	~				
< III >	<	ш			>				
36 certificate templates									

Modelo visto no controle de domínio

10. No painel esquerdo do MMC, expanda Certification Authority (Local) e expanda sua CA na lista da Certification Authority.

Clique com o botão direito do mouse em Modelos de certificado, clique em **Novo** e em **Modelo de certificado** para problemas. Em seguida, escolha o modelo de Smartcard recém-criado.

a		C	onsole1 - [Console Roo	t\Certification Authority (Local)\jajanson-2012DC-AD-CA\Certificate Templates]		_ 🗆 X
Tile Action View Favorites W	Vindow Help					_ 8 ×
🗢 🔿 🙍 🖬 🖉 📷						,
Console Root	N	Name		Intended Purpose	Actions	
D Certificate Templates	3	Exchange E	nrollment Agent (Offline r	Certificate Request Agent	Certificate Templates	
a 🙀 Certification Authority (Local)	8	IPSec (Offli	ine request)	IP security IKE intermediate	Mare Astiens	
a jajanson-2012DC-AD-CA	8	Webclienta	indserver	Client Authentication, Server Authentic	More Actions	'
Revoked Certificates	3	Exchange S	ignature Only	Secure Email		
Issued Certificates	3	CEP Encryp	otion	Certificate Request Agent		
Pending Requests	3	Smartcard S	User_VCS	Secure Email, Client Authentication, Sm		
Catificate Templeter	3	🛛 VCS_Login	_SMART	Smart Card Logon, Client Authentication		
Manage Manag	ige		Agent	Certificate Request Agent		
Mari	-		mail Replication	Directory Service Email Replication		
New		•	ontroller Authentication	Client Authentication, Server Authentic		
View		•	uthentication	Client Authentication, Server Authentic		
New V	Window from He	ere	ny Agent	File Recovery		
Mary T	Taskoad View			Encrypting File System		
IVEW I	raskpau view		ontroller	Client Authentication, Server Authentic		
Refres	sh)	r	Server Authentication		
Export	t List			Client Authentication, Server Authentic		
Help				Encrypting File System, Secure Email, Cl		
nop			e Certification Authority	<all></all>		
	5	🗟 Administra	tor	Microsoft Trust List Signing, Encrypting		

Emitir novo modelo

11. Depois que o modelo for replicado, no MMC, clique com o botão direito do mouse ou selecione a lista Autoridade de certificação, clique em **Todas as tarefas** e, em seguida, clique em **Parar serviço**. Em seguida, clique com o botão direito do mouse no nome da AC novamente, clique em **Todas as tarefas** e, em seguida, clique em **Iniciar serviço**.



Parar e iniciar serviços de certificado

Inscreva-se no certificado do agente de inscrição

Érecomendável que você faça isso em uma máquina cliente (área de trabalho dos administradores de TI).

1. Inicie o MMC escolha **Certificados**, clique em **Adicionar** e depois em Certificados para a **Minha Conta de Usuário**.



Adicionar certificados

2. Clique com o botão direito do mouse ou selecione o **Nó pessoal**, selecione **Todas as tarefas** e selecione **Solicitar novo certificado**.

Console1 - [Console Root\Certificates - Current User\Personal]	_ D X
File Action View Favorites Window Help	_ & ×
 Console Root Certificates - Current User Certificates - Current User Certificates - Current User Certificates Find Certificates Find Certificates Request New Certificate New Window from Here New Taskpad View Advanced Operations Tr Refresh CI Export List Certification Authority (Loc Find Certification Authority (Loc Jajanson-2012DC-AD-Ci 	Actions Personal More Actions
III > Personal store contains 9 certificates.	

Solicitar novos certificados

3. Clique em **Next** no assistente e selecione **Ative Diretory Enrollment Policy**. Em seguida, clique em **Avançar** novamente.

	Concola 1 - [Concola Doot) Cartificator - Current Llear Darconall	
The Action View	📮 Certificate Enrollment	
Console Root Certificates - Curren Certificates - Curren Final Personal Final Trusted Root Certificate Certifi	Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Certificate enrollment policy may already be configured for you.	s Inal A Iore Actions
Active Directory	Configured by your administrator	
Trusted Publishe	Active Directory Enrollment Policy 🗸	
 Untrusted Certifi Third-Party Root Trusted People Client Authentic Certificate Enroll Smart Card Trust Certification Author jajanson-2012DC 	Configured by you Add New	
< 111	Next Cancel	
Personal store contains 9 cere	111.01(5).	

Inscrição no Ative Diretory

4. Selecione o **Certificado do agente de inscrição**, nesse caso, **Smartcard User_VCS** e clique em **Inscrever-se.**



Agente de certificado de inscrição

A área de trabalho dos Administradores de TI agora está configurada como uma Estação de Inscrição, permitindo que você inscreva novos smartcards em nome de outros usuários.

Inscrever-se em nome de...

Para que agora você forneça aos funcionários smartcards para autenticação, você precisa inscrevê-los e gerar o certificado que é importado para o Smartcard.



Inscrever-se em nome de

1. Inicie o MMC e importe o Módulo e o Gerente de Certificados para a Minha Conta de Usuário.

2. Clique com o botão direito do mouse ou selecione **Pessoal > Certificados** e selecione **Todas as Tarefas > Operações Avançadas** e clique em **Inscrever-se em nome de...**

3. No assistente, escolha a Política de Registro do Ative Diretory e clique em Avançar.



Inscreva-se em nome de

a		Console1 - [Console Root\Certif	icates - Current U	ser/Personal/Certifi	cates)				= 0 X
🖀 File Action View Favorites Window He	lp .								_ Ø ×
Console Root	Issued To	issued By	Expiration Date 10/14/2019	Intended Purposes Cartificate Request	Friendly Nome	Status	Cent	Actions	
a 🛄 Personal	Administrator	Jeanson-2012DC-AD-CA	10/12/2018	Microsoft Trust List	«None»		Adr	Certificates	-
 Certificates Trusted Root Certification Authorities 	Cadministrator				_ 0 X		Fore		
b Enterprise Trust	Sjøjarson-2012	Certificate Enrollment							
5 📫 Active Directory User Object	Scott Lang						1.3.6 Sma		
 D Trusted Publishers D Untrusted Certificates 	Scott Long	Before You Begin					Sme		
b Third-Party Root Certification Authorities	Scott Lang	The following steps will help you install certific outputs of a statute outputs and block identifies and the statute of the s	cates, which are digit	I credentials used to con	nnect to windex		Sma		
 D Intrast People D International Sector Sector		Rewond, protect concert, essential the fail	and do cone security	100000-00045					
b Cartificate Envolment Requests b Smart Card Trusted Roots		before requesting a certificate, verify the follo							
		Your computer is connected to the network. You have credentials that can be used to verify	y your right to obtain	the certificate					
	I L			Paul	Cancel				
	-								
	<						>		
Personal store contains 9 certificates.									

4. Selecione Política de registro de certificado e clique em Avançar.

-	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.									

Política de inscrição

5. Agora, é solicitado que você selecione o **certificado de assinatura**. Este é o certificado de inscrição solicitado anteriormente.

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]								_ 🗆 X	
File Action View Favorites Window Hel	lp								_ <i>8</i> ×
Console Root	Issued To		Issued By	Expiration Date	Intended Purposes	Friendly Name	Status Ce	rti Actions	
A Personal	Administrator Personal		jajanson-2012DC-AD-CA jajanson-2012DC-AD-CA	10/12/2019	Microsoft Trust List	<none></none>	Ad	Certificates	•
Certificates	Administrator					_ 🗆 X		More Actions	,
Finisted Root Certification Authorities Enterprise Trust	Administrator	ortificate					En	ro	
Intermediate Certification Authorities	PIVKey BD9A5	ertificate	Window	/s Security	×		1.3	.6	
 Active Directory User Object Trusted Publishers 	Scott Lang	Select I	Select a Certificate				Sm	ha	
Untrusted Certificates	Scott Lang						Sm	ma	
Inird-Party Koot Certification Authorities Inird-Party Koot Certification Authorities Inird-Party Koot Certification Authorities		You need Browse t	Administrator			her users. Click			
Client Authentication Issuers			Issuer: jajanson-201	2DC-AD-CA					
Certificate Enrollment Requests Smart Card Trusted Roots		Valid From: 10/14/2017 to 10/14/2019							
		Signing	Click here to view of	ertificate		Browse			
			properties						
			Administrator						
			Issuer jajanson-201	2DC-AD-CA					
			Valid From: 10/12/2	017 to 10/12/2019					
				ОК	Cancel				
						Cancel			
	<		III				1	>	
Personal store contains 9 cértificates.									

Selecionar certificado de assinatura

6. Na próxima tela, você precisa navegar até o certificado que gostaria de solicitar e, nesta instância, é o **Smartcard User_VCS** que é o modelo criado anteriormente.

a		Console1 - [Console Root\Certifie	ates - Current U	ser\Personal\Certifi	cates]				_ 🗆 X
The Action View Favorites Window He	lp								- 8 ×
🗢 🔿 📶 🛍 🖻 🛃 🗊									
Console Rot Certificates - Current User Certificates - Current User Certificates - Current User Certificates Certificates Certificates Certificates Certificates Certificates Current Quero Certification Authorities Current Quero Certification Authorities Crusted Publisher Circuited Publisher Certificate Encollment Requests Certificate Encollment Requests Smart Card Trusted Roots	Ssued To	Issued By jajanson-2012DC-AD-CA tificate Enrollment Request Certificates You can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (ou can request the following types of certificatick Next (out can request) (for the formation is required to endition (formation is required to endition (formation is required to endition (formation (form	Expiration Date 10/14/2019 10/12/2018 ttes. Select the certificate STATUS: Availal STATUS: Availal STATUS: Availal STATUS: Availal STATUS: Availal	Intended Purposes Certificate Request Microsoft Trust List cates you want to reque ble Click here to configure ble Click here to configure ble Click here to configure ble Next	Friendly Name <none> <none> st, and then Details ~ settings. Details ~ Details ~ Cancel</none></none>	Status	Certi Enro 1.3.6 Sma Sma Sma	Actions Certificates More Actions	,
Personal store contains 9 certificates.									

Escolha o cartão inteligente VCS

7. Em seguida, selecione o usuário que deseja inscrever em nome do. Clique em **Procurar** e digite o nome de usuário do funcionário que deseja inscrever. Neste caso, é usada a 'conta antman@jajanson.local' de Scott Lang.

10M									
Console1 - [Console Koot/Certificates - Current User/Personal/Certificates]									
File Action View Favorites Window Help									_ 8 ×
Console Root Issue	ued To 📍	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certi	Actions	
a 🗊 Certificates - Current User 😭 🖓	Administrator	jajanson-2012DC-AD-CA	10/14/2019	Certificate Request	<none></none>		Enro	Certificates	
A Personal Y A	Administrator	jajanson-2012DC-AD-CA	10/12/2018 Microsoft Trust List		List <none></none>		Adm	More Actions	•
Trusted Root Certification Authorities	Administrator				_ D X		Enro		
Enterprise Trust	jajanson-2012	Select User	X						
Description Authorities	PIVKey BD9A5						1.3.6		
p Trusted Publishers	Scott Lang	Select this object type:					Sma	5	
Untrusted Certificates	Scott Lang	User	Objec	t Types			Sma		
D Dirid-Party Root Certification Authorities		From this location:	n name of that user. For			Sma			
Client Authentication Issuers		ajarison Jocal	Loc	abons					
Certificate Enrollment Requests		Enter the object name to select (examples):		e needs to	be installed is				
Smart Card Trusted Roots		Scott Lang (antman@iajanson.local)	Chec	k Names					
		Advanced	OK	Cancel	Deserves				
		Autoroot		al	prowse				
					Cancel				
						_			
Personal store contains 9 certificates.									

Escolha o usuário

8. Na próxima tela, continue com a inscrição clicando em **Inscrever-se**. Agora, insira um smartcard em seu leitor.

		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 uple, 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.								

Inscrever-se

9. Depois de inserir seu smartcard, ele é detectado da seguinte forma:

eques	Windows Security	×
e enrol Ariter D	Enrolling for the user certificate. Select a smart card device	
⊛væ	Axaito Cryptoflex .NET Gemato USB Smart Card Reader 0 The smart card is ready for use.	
	un un	

10. Em seguida, é solicitado que você digite um número PIN do cartão inteligente (Pino padrão: 0000).

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]	D X
File Action View Favorites Window Help	- 8 ×
Console Action View Favorites Window Help Console Root \Certificates - Current User\Personal\Certificates - Current User\Personal\Certificates - Current User Console Root \Certificates - Current User Console Root \Certificate Enrollment Console Root \Certificates - Current User Console Root \Certificate Enrollment Console Root \Certificate Enrollment Console Root \Certificates - Current User Console Root \Certificate Enrollment Console Root \Certificate Enrollment Console Root \Certificate Enrollment Console Console Root \Certificate Enrollment Console Console Root \Certificate Enrollment Console Console Root \Certificate Root \Second \Certificate Enrollment \Certificate \Certificate \Certificate Enrollme	
C Berronal store contains 9 certificates	

Insira o pino

11. Por fim, depois de ver a tela **Enrollment Successful**, você poderá usar esse smartcard para fazer logon em um servidor associado a domínio, como o VCS com apenas a placa e um pin conhecido. No entanto, não é feito sim, você ainda precisa preparar o VCS para redirecionar as solicitações de autenticação para o Smart Card e usar o Common Access Card para liberar o certificado de smartcard armazenado no smartcard para autenticação.

Certificate Enrollment		_ D X	
Certificate Installation Results			
The following certificates have been env	olled and initialied on this computer.		
Wakkundig Smartcard User	✓ STATUS: Succeeded	Details 🛩	
		iest user Oose	Inscrição bem-suce

Configure o VCS para a placa de acesso comum

Carregue a CA raiz na lista de certificados CA confiáveis no VCS navegando para **Manutenção >** Segurança > Certificado CA confiável.

2. Carregue a lista de revogação de certificado assinada pela CA raiz no VCS. Navegue até Manutenção > Segurança > Gerenciamento de CRL.

3. Teste seu certificado de cliente em relação ao seu regex, que extrai o nome de usuário do certificado para usar para autenticação em relação ao LDAP ou usuário local. O regex vai corresponder ao **assunto** do certificado. Pode ser o seu UPN, e-mail e assim por diante. Neste laboratório, o e-mail para correspondência com o certificado do cliente para o certificado do cliente foi usado.

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: Thursday, October 17, 2019 5
Subject Public key Public key parameters Certificate Template Inform	antman@jajanson.local, Scott RSA (1024 Bits) 05 00 Template=1 3 6 1 4 1 311 21
E = antman@jajanson.local CN = Scott Lang OU = Heroes DC = jajanson DC = local	
Ed	it Properties Copy to File
	OK

Assunto do certificado do cliente

4. Navegue até Manutenção > Segurança > Teste de certificado do cliente. Selecione o certificado do cliente a ser testado, em Meu laboratório foi antman.pem, carregue-o na área de teste. Na seção Padrão de autenticação baseado em certificado em Regex para corresponder ao certificado cole seu regex para ser testado. Não altere o campo Formato do nome de usuário.

My Regex: /Subject:.*email#	ddress=(?.*)@jajanson.local/m				
clico Cisco TelePresence Video Communication Server Expressway		"Driv system bas & alarmo'			
Status System Configuration Applications Users Maintenance					
Client certificate testing		You are here: <u>Stantenance</u> / <u>Deputy certificates</u> - Clear			
Client contribute					
	This tests whether a client certificate is valid when checked against the VCIS's current trusted CA list and, if loaded, the	nevocation lat			
Certificate source	Upliaded test the (PEN format)				
Belect the file you sant to text					
Currently upstable set file advent gem					
Certificate-based authentication pattern					
	This section applies only if your certificate contains authentication oredentials and you want to use certificate-based aut the nominated certificate to see if the certificate's codentials (the username) can be extracted.	tentication as your client certificane-based security setting. It lets you test the outcome of applying regax and usemame format combinations to			
Repex to match against berifficate	dubject. "emailAddress+(? <capturecommonnamer -)@pipeson.localim<="" td=""><td></td></capturecommonnamer>				
Usernams format	#capureCommoName#				
	Make these settings permanent				

Teste seu regex no VCS



Resultados do teste

5. Se o teste fornecer os resultados desejados, clique no botão Torne essas alterações permanentes. Isso altera seu regex para a configuração de autenticação baseada em certificado do servidor. Para verificar a alteração, navegue até essa configuração, Manutenção > Segurança > configuração de autenticação baseada em certificado.

6. Ative a autenticação baseada em cliente navegando para Sistema > Administrador e clique ou selecione a caixa suspensa para escolher Segurança baseada em certificado do cliente = Autenticação baseada em cliente. Com essa configuração, o usuário digita o FQDN do servidor VCS em seu navegador e é solicitado que ele escolha sua conta de cliente e insira o pino atribuído a sua Placa de Acesso Comum. Em seguida, o certificado é liberado e ele retorna a GUI da Web do servidor VCS e tudo o que precisa fazer é clicar ou selecionar o botão Administrador. Então ele é admitido no servidor. Se as opções Segurança baseada em certificado do cliente = Validação baseada em cliente estiverem selecionadas, o processo será o mesmo, com exceção quando o usuário clicar no botão Administrador, ele terá solicitado novamente a senha do administrador. Normalmente, o último não é o que a organização está tentando realizar com o CAC.

CISCO Cisco Expressway-E

Status	System	Configuration	Applications	Users	Maintenance	
Syster	n adminis	tration				
Ephem	eral port range (end				* 49999
Servic	es					
Serial p	oort / console					On 🗸 (i)
SSH se	ervice					
Web in	tarfaca (over H	TTRE				
Web III	ternace (over n	(11-3)				
Sacci	on limite					
30330	Jii iii iii a					
Sessio	n time out (minu	tes)				* 30
Per-ac	count session li	mit				* 0
Systen	n session limit					* 0
System	m protection					
Autom	ated protection :	service				On 🗸 (i)
Autom	atic discovery p	rotection				
Web s	erver configu	ration				
Dedies						
Redire	ct HTTP request	S TO HITPS				
HTTP S	strict Transport	Security (HSTS)				
Web a	dministrator por					443 🧹 🤅
Client o	certificate-based	l security				Not required 🗸 🥡
						Drop down the above box and choose
Save						Client-Based Authentication
Dolate	d taaka					
Relate	utasks					
Upload Test of	a CA certificates	e file for HTTPS				
Test Cl	ent centricates					

Ativar autenticação baseada em cliente

Socorro! Estou trancado para fora!!

Se você habilitar a autenticação baseada em cliente e o VCS rejeitar o certificado por qualquer motivo, você não poderá mais fazer login com a GUI da Web da maneira tradicional. Mas, não se preocupe, há uma maneira de voltar ao seu sistema. O documento anexado pode ser encontrado no site da Cisco e fornece informações sobre como desativar a autenticação baseada em cliente do acesso raiz.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta

configuração.