# Integrazione CSM TACACS con ISE

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Premesse Configurazione Esempio di rete Procedura di autenticazione Configurazione di ISE Configurazione CSM Verifica Risoluzione dei problemi

### Introduzione

Questo documento descrive la procedura per integrare Cisco Security Manager (CSM) con Identity Services Engine (ISE) per autenticare gli utenti amministratori con il protocollo TACACS+.

### Prerequisiti

#### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Security Manager (CSM).
- Identity Services Engine (ISE).
- Protocollo TACACS.

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CSM Server versione 4.2
- ISE versione 3.0

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

Per impostazione predefinita, Cisco Security Manager (CSM) utilizza una modalità di autenticazione chiamata Ciscoworks per autenticare e autorizzare gli utenti a livello locale, in modo da avere un metodo di autenticazione centralizzato che è possibile utilizzare Cisco Identity Service Engine tramite il protocollo TACACS.

## Configurazione

### Esempio di rete



#### Procedura di autenticazione

Passaggio 1. Accedere all'applicazione CSM con le credenziali dell'utente amministratore.

Passaggio 2. Il processo di autenticazione attiva e ISE convalida le credenziali localmente o tramite Active Directory.

Passaggio 3. Una volta completata l'autenticazione, ISE invia un pacchetto di autorizzazione per autorizzare l'accesso al CSM.

Passaggio 4. CSM esegue il mapping del nome utente con l'assegnazione del ruolo utente locale.

Passaggio 5. ISE mostra un log live di autenticazione completato.

#### Configurazione di ISE

Passaggio 1. Selezionare l'icona a tre righenell'angolo superiore sinistro e selezionareAmministrazione > Risorse di rete > Dispositivi di rete.

E Cisco ISE			Admi	nistration - Network Resourc	6S		
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Services
Network Devices Default Device	Networ	k Devices					
Device Security Settings	/ tot + A	dd 🚺 Duplicate 🕁 Import	ය Export ~ ලි Generate PM	0 Delete V			
	Nam	e A IP/Mask Profile N	lame Location	Туре	Description		

**Passaggio 2.** Selezionare il pulsante **+Add** e immettere i valori corretti per Network Access Device Name e IP Address, quindi verificare la casella di controllo **TACACS Authentication Settings** e definire un segreto condiviso. Selezionare il pulsante **Invia**.

	Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services	
17	National Devices	Release Devices List > New Yorkers Device	
	lefault Device	Network Devices	
4	levice Security Settings		
		- same C55432	
		Description	
		E #A4046 v <sup>1</sup> P1 1085243.42 / 32 @v	
		* Device Profile	
		Nuodi Name V	
		Software Version	
		* Network Device Group	
		Location All Locations v Set To Detaut	
		1950 Is IPSRO Device v Set To Default	
		Every fuel Al Device Types v Set To Default	
		RADUS Authentication Settings	
		<ul> <li>TACACS Authentication Settings</li> </ul>	
		Shared Social Down	
		C Lapery Cass Device	
		<ul> <li>InCACS that Conjutative Single Contract Surgert</li> </ul>	
		SNMP Settings	
		Advanced TrustSec Settings	
			-
		Bulleton (Construction)	Cancel

Passaggio 3. Selezionare l'icona delle tre lineenell'angolo superiore sinistro eselezionare Amministrazione > Gestione delle identità > Gruppi.

E Cisco ISE		Administration • Identity	Management
dentities Groups Externa	Identity Sources	Identity Source Sequence	es Settings
Identity Groups	User	Identity Groups	
Endpoint Identity Groups	/ Edit	+ Add 👩 Delete 🗸 🕁 Imj	port 🏦 Export 🗸
>  User Identity Groups		Name	∧ Description
		ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
		A Employee	Default Employee User Group
		GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
		GuestType_Contractor (default)	Identity group mirroring the guest type
		A GuestType_Daily (default)	Identity group mirroring the guest type
		A GuestType_SocialLogin (default)	Identity group mirroring the guest type
		EuestType_Weekly (default)	Identity group mirroring the guest type
		MOWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

**Passaggio 4.** Passare alla cartella **Gruppi di identità utente** e selezionare il pulsante **+Aggiungi**. Definire un nome e selezionare il pulsante **Invia**.

dentities Groups External Iden	ty Sources Identity Source Sequences Settings	
Identity Groups ∃Q	User Identity Groups	
< 8 Ø		Selected 0 Total 10 💋 🚳
> 🗅 Endpoint Identity Groups	🖉 Edit 🕂 Add 🌘 Delete 🗸 🕁 Import 🏠 Export 🗸	NII $\sim$ $\nabla$
> 🛅 User Identity Groups	Name   Description	
	ALL_ACCOUNTS (defauit)     Defauit ALL_ACCOUNTS (defauit) User Group	
	CSM Admin	
	CSM Oper	

Nota: In questo esempio vengono creati i gruppi CSM Admin e CSM Oper Identity. È possibile ripetere il passaggio 4 per ogni tipo di utente Admin su CSM

Passaggio 5. Selezionare l'icona a tre righe e selezionare Amministrazione > Gestione delle identità > Identità. Selezionare il pulsante +Aggiungi e definire il nome utente e la password, quindi selezionare il gruppo a cui appartiene l'utente. In questo esempio vengono creati gli utenti csmadmin e csmoper, assegnati rispettivamente ai gruppi CSM Admin e CSM Oper.

textilies Owners Fr	namal Mantha Rauras - Mantha Raura Ranasas - Rations	
Croups D	carrier carriery actives intensity active antiperiodes anticings	
n Manual National Scient Res.	Newsex Access Unam Unit > considering	
	V Network Access User	
	* Name CSINADINA	
	Second Employ of	
	[nal	
	✓ Passwords	
	Paravel Tuor Internations	
	Pressent De. Jone Tamavet	
	filing Desert	
	trade Password Generate Password	] @
	V User Information	
	First Norm	
	Last Name	
	V Account Options	
	Description	
	Charge passwerd on hot togen	
	V Account Disable Policy	
	Double account if data access 2021-00-16 (type-mm-bb)	
	V User Groups	
	E CSM Admin v - +	

Identities Groups	External Identity Sources	Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network A	Access Users	
			Selected 0 Total 2 🧭 🧔
	🖉 Edik 🕂 Add	🛠 Change Status \vee 🕁 Import 🔥 Export 👻 🏮 Delete \vee 🍈 Duplicate	$\sim \gamma$
	Status	Name	User Identity Grou Ad
	Enabled	1 csmadmin	CSM Admin
	Enabled	1 camoper	CSM Oper

Passaggio 6. Selezionaree selezionare Amministrazione > Sistema > Distribuzione.Selezionare il nodo hostname e abilitare il servizio Device Admin

=



**Nota:** In caso di distribuzione distribuita, selezionare il nodo PSN che gestisce le richieste TACACS

Passaggio 7. Selezionare l'icona a tre righe e passare ad Amministrazione > Amministrazione dispositivi > Elementi della policy. Passare a Risultati > Set di comandi TACACS. Selezionare +Pulsante Aggiungi, definire un nome per il set di comandi e attivare la casella di controllo Consenti qualsiasi comando non elencato sotto la casella di controllo. Selezionare Sottometti.

	ŝ	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets	More $\backsim$	
onditions	>	TACACS Command Sets Command Set	> New					
etwork Conditions	~	Name Permit all						
TACACS Command Sets		Description						
		Commands Permit any command the	at is not listed below	5				
		+ Add 🛛 🗍 Trash 🗸	CEdit 🔷 Move Up	Move Down				

Passaggio 8. Selezionare l'icona a tre righe nell'angolo superiore sinistro e selezionare

Amministrazione->Amministrazione dispositivi->Set di criteri di amministrazione dispositivi.

Seleziona situato sotto il titolo Set di criteri, definire un nome e selezionare il pulsante + al centro per aggiungere una nuova condizione.

Policy Set	ts				Reset	et Policyset Hit	counts		Save
🕂 Stat	tus	Policy Set Name	Description	Conditions	Allowed Protocols / Ser	ver Sequence	Hits	Actions	View
Q Se	arch								
•	•	CSM Administrators		+	Select from list	~+		 (2) 	•
e		Default	Tacacs Default policy set		Default Device Admin	∞ ~+	0	<u>ل</u>	•

**Passaggio 9.** Nella finestra Condizione, selezionare Aggiungi attributo, quindi selezionare Icona **periferica di rete** seguito da Indirizzo IP periferica di accesso alla rete. Selezionare **Attribute Value** (Valore attributo) e aggiungere l'indirizzo IP del CSM. Selezionare **Use** once done (Usa al termine).

Library Search by Name Concentrations found - reset filters:	Conditions Studio							0
Search by Name       Image: Comparison of Comp	Library	Editor						-
Image: Constraint of the second o	Search by Name		Network Access-D	evice IP Address	5			
No conditions found - reset filters.		Ð	Equals 🗸	10.88.243.	42			
NEW AND OR	No conditions found - reset filters.		Set to 'Is not'				Duplicate	Save
				NEW	AND	OR		
Close Use							Close	Use

Passaggio 10. In Consenti protocolli, sezione, selezionare Device Default Admin. Selezionare Salva

Policy Sets						Reset	Reset Policyset Hi	tcounts		Save
🕂 Status	Policy Set Name	Description	Co	nditions		Allowed Protoco	ls / Server Sequence	Hits	Actions	View
Q Search										
٢	CSM 4.22		₽	Network Access-Device IP Address EQUALS 10.88.243.42	2	Default Device /	Admin 🛚 🛛 🔶 🕂	0	<u>ن</u>	•

**Passaggio 11.** Selezionare la freccia destra criteri di autenticazione e autorizzazione

icona del set di criteri per la definizione dei

**Passaggio 12.** Selezionare situato sotto il titolo del criterio di autenticazione, definire un nome e selezionare il segno + al centro per aggiungere una nuova condizione. Nella finestra Condizione selezionare Aggiungi attributo, quindi **Icona periferica di rete** seguito da Indirizzo IP periferica di accesso alla rete. Selezionare **Attribute Value** (Valore attributo) e aggiungere l'indirizzo IP del CSM. Selezionare **Use** once done (Usa al termine)

Passaggio 13. Selezionare gli utenti interni nell'archivio identità e selezionare Salva

Status         Rule Name         Conditions         Use         Hits         Actions           Q         Search         Image: Search <th>✓ Authent</th> <th>ntication</th> <th>Policy (1)</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	✓ Authent	ntication	Policy (1)						
Q Search	🕣 St	Status	Rule Name	Cor	ditions	Use		Hits	Actions
	Qs	Search							
Internal Users 🗷 🗸						Internal Users	<b>a</b> ~		
O       CSM Authentication       ₽       Network Access-Device IP Address EQUALS 10.88.243.42       > Options		0	CSM Authentication		Network Access-Device IP Address EQUALS 10.88.243.42	> Options			 (\$}

**Nota:** È possibile modificare l'archivio identità in archivio AD se ISE è aggiunto a un Active Directory.

	_	-	
-		_	
	_		
	_	_	
ς.			
-	_		

**Passaggio 14.** Selezionare sotto il titolo del criterio di autorizzazione, definire un nome e selezionare il pulsante + al centro per aggiungere una nuova condizione. Nella finestra Condizione selezionare Aggiungi attributo, quindi selezionare l'icona Gruppo di identità seguita da Utente interno: Gruppo di identità. Selezionare il gruppo CSM Admin e Usa.

Jiary		Editor				
earch by Name			InternalUser-Identity	Group		
	E C 1 C t 🕈	4	Equals 🗸	User Identity Groups:CSM Ad	imin × 🗸 🗸	
EAP-MSCHAPv2	0		Set to 'Is not'		Duplicate	Save
EAP-TLS	٥			NEW AND OR		
Guest_Flow	0					
Network_Access_Authent Passed	ication_ ()					

**Passaggio 15.** In Set di comandi selezionare Consenti tutti i set di comandi creati nel passaggio 7, quindi selezionare **Salva** 

Ripetere i passaggi 14 e 15 per il gruppo Oper CSM

- Auth	orization	Policy (3)								
					Results					
۲	Status	Rule Name	Con	ditions	Command Sets		Shell Profiles		Hits	Actions
0	Search									
	٥	CSM Oper	я	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	$\left  \text{Permit all} \times \right $	~+	Select from list	~+	0	(2)
	۲	CSM. Admin	8	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	$\text{Permit all} \times$	~+	Select from list	~+	0	{ĝ}
	۲	Default			$DenyAllCommands \times$	~+	Deny All Shell Profile	<u>a ~</u> +	0	(2)

**Passaggio 16 (facoltativo).** Selezionare l'icona a tre righe nell'angolo superiore sinistro e Selezionare **Amministrazione>Sistema>Manutenzione>Repository**, selezionare **+Aggiungi** per aggiungere un repository utilizzato per memorizzare il file di dump TCP per la risoluzione dei problemi.

**Passaggio 17 (facoltativo).** Definire un nome repository, un protocollo, un nome server, un percorso e le credenziali. Al termine, selezionare **Invia**.

Deployment	Licensing	Certificates L	ogging	Maintenance	Upgrade	Health Checks	Backup	Click here to do visibility setup Do not show this again.
Patch Management		Repository List > Ad	dd Repository					
Repository		Repository Co	nfiguration					
Operational Data Pur	ging							
		* Repository Name	WMReposit	ory				
		* Protocol	FTP 🗸					
		Location						
		* Server Name	10.122.11	2.137				
		* Path	1					
		Credentials						
		* User Name	cisco					
		* Password						

### Configurazione CSM

**Passaggio 1.** Accedere all'applicazione client Cisco Security Manager con l'account admin locale. Dal menu passare a **Strumenti > Amministrazione di Security Manager** 

					S
		Cisco Version 4	Security Manager		
		Server Name Username Password Default View	10.88.243.42       admin       •••••••       Image:	>     >	
L	© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco its affiliates in the U.S. and certain other countries.	) logo are registe	red trademarks of Cisco Systems, Inc. and/or		ılı.ılı. cısco



Passaggio 2. Selezionare la casella in Parametri RBAC nativo. Selezionare Salva e chiudi

5	Cisco Security Manager - Administration	_ <b>_</b> X
API     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     AutoLink     Configuration Archive     Configuration Archive     Configuration Archive     Configuration Archive     Customae Desistop     Customae Desistop     Customae Desistop     Device Computation     Policy Management     Policy Management     Policy Coglects     Policy Coglects     Policy Security     Rule Expension     Rule Expension     Rule Expension     Device Security	Server Security         Use the buttors below to cross launch the Server Security Tools within Common Services.         AAA Setup         Certificate Setup         Single Sign On         Local User Setup         System Identity Setup         Native RBAC Parameters         W Blow logon for user do not available in Local User Database	Save Restore Defaults

Passaggio 3. Dal menu selezionare File > Sottometti. File > Invia (Submit).

**Nota:** Tutte le modifiche devono essere salvate e, in caso di modifiche alla configurazione, devono essere inviate e distribuite.

Passaggio 4. Passare all'interfaccia utente di gestione CSM, digitare <u>https://<enter\_CSM\_IP\_Address</u> e selezionare Amministrazione server.



**Nota:** I passaggi da 4 a 7 mostrano la procedura per definire il ruolo predefinito per tutti gli amministratori che non sono definiti su ISE. Questi passaggi sono facoltativi.

**Passaggio 5.** Verificare che la modalità di autenticazione sia impostata su **CiscoWorks Local** e **Online** userID è l'account amministratore locale creato su CSM.

cisco Cis	co Security Mana	ger						edmin Logost About Feedback
Home Server • 1	Software Center •							
								17 Apr 2021, 14:11 F
Common Services	Home							
Auto Refresh		Version: 4.2.2						Last Updated: Sat Apr 17 14:11:20 PDT 2021 📀
	Security		Backup			Recent	ly Completed Jobs	
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job ki	Job Type	Status	Description	Completed At
				1001.1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 17 05:01:56 PDT 2021
uthorization Mode	CiscoWorks Local	Last Backup Completed at	Not found or unable to detect	1001.1369	SystemCheckUtility	Succeeded	SysCheckTest	Fri Apr 16 05:00:58 PDT 2021
inste Siss-on Mode	Standalone			1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
age age of acces		Recent Backup Status	Not found or unable to detect	1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021
				1001.1366	SystemCheckUtility	Succeeded	SysCheckTest	Tue Apr 13 05:00:54 PDT 2021
				1001.1365	SystemCheckUtility	Succeeded	SysCheckTest	Mon Apr 12 05:00:56 PDT 2021
				1001.1364	SystemCheckUtility	Succeeded	SysCheckTest	Sun Apr 11 05:00:55 PDT 2021
				1001.1363	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 10 05:00:56 PDT 2021
								More
	System Taska		Doline Users		Management Tax	ka l		Reports
ocal User Setup				Schedule Back	kup		Permission Rep	ot
Auto-Server Trust Manage	sment	Number of Online upors		Check for Soft	ware Updates		Log File Status	
onfigure Single Sign-On		Hander of Crime Gabra		Check for Dev	ice Updates		Process Status	
AA Mode Setup				Collect Server	Information		System Audit L	
			admin					
		Online User Id(s)	Sand Massage					

Passaggio 6. Passare a Server e selezionare Gestione server singolo

ciso	cisco Cisco Security Manager			
Home	Server V Software Center V			
	Security			
Commo	Single-Server Management			
🗹 Auto R	Multi-Server Trust Management			
	Cisco.com Connection Management			
Authentica	AAA Mode Setup	·		
Authorizat	Admin	,		
Single Sig	Processes			
Single Sig	Backup	2		
	Log Rotation			
	Collect Server information			
	Selfest			
	Notity Users			
	Besource Browser			
	System Preferences			
Local Use	CS Log Configurations			
Multi-Serv	DiskWatcher Configuration			
Configure	Disk taking comgaration			
AAA Mode	e Setuo II			

**Passaggio 7.** Selezionare Impostazione gestione ruoli e selezionare il privilegio predefinito che tutti gli utenti amministratori ricevono al momento dell'autenticazione. Nell'esempio viene utilizzato Amministratore di rete. Una volta selezionato, selezionare **Imposta come predefinito.** 

cisco Cisco Security Ma	anager		
Home Server * Software Center *			
Navigator Browser-Server Security mode setup	Role Management Setup		Showing 8 records
Local User Policy Setup Role Management Setup	1. Approver	Approver Role	Default Roles
Certificate Setup	2. Help Desk	Help Desk Role	
	3. Network Administrator	Network Administrator Role	R
	4. Network Operator	Network Operator Role	
	6. Security Administrator	Security Administrator Role	
	7. Super Admin	Super Admin Role	
	6. System Administrator	System Administrator Role	
	Add Edit Delete Copy I Exp	on Import I Set as default Clear defa	ut

Passaggio 8. Selezionare Server>Ruolo di installazione della modalità AAA, quindi selezionare l'opzione TACACS+ e infine selezionare change per aggiungere informazioni ISE.



cisco Cisco Security Manager
Home Server ▼ Software Center ▼
Authentication Mode Setup
AAA Mode Setup Select a Type: ACS O Local RBAC
Current I anis Made: I and Authoritation
Current Login Mode: Local Autentication
Available Login Modules
2 Local NT System
3 MS Active Directory
4 RADIUS
5 O TACACS+
Change

**Passaggio 9.** Definire l'indirizzo IP e la chiave ISE. Facoltativamente, è possibile selezionare l'opzione che consente a tutti gli utenti con autenticazione locale o a un solo utente se l'accesso non riesce. Per questo esempio, come metodo di fallback è consentito l'utilizzo dell'opzione Solo utente amministratore. Selezionare **OK** per salvare le modifiche.

Login Module Options		
Selected Login Module:	TACACS+	
Description:	Cisco Prime TACACS+ login module	
Server:	10.122.112.4	
Port:	49	
SecondaryServer:		
SecondaryPort:	49	
TertiaryServer:		
TertiaryPort:	49	
Key:		
Debug:	True O False	
	<ul> <li>Allow all Local Authentication users to fal Authentication login.</li> </ul>	lback to the Local
Login fallback options:	Only allow the following user(s) to fallbac Authentication login if preceding login fails:	k to the Local
	admin	(comma separated)
	Allow no fallbacks to the Local Authentica	ation login.
		OK Cancel



Passaggio 10. Selezionare Server> Gestione server singolo, quindi selezionare Configurazione utente locale e selezionare Aggiungi.

iliii cisc	Cisco Security Manager	
Home	Server V Software Center V	
Commo	Single Server Management	
Auto R	Multi-Server Trust Management	
	Cisco com Connection Management	i
	AAA Mode Setup	
Authentica		,
Authorizat	Admin	,
	Processes	
Single Sig	Backup	,
	Log Rotation	-
	Collect Server information	
	Selftest	
	Notify Users	
	Job Browser	
	Resource Browser	
Local Lise	System Preferences	
Multi-Serv	CS Log Configurations	
Configure	DiskWatcher Configuration	
AAA Mada	Patua	

cisco Cisco Security	v Manager
Home Server * Software Center *	manager
Navigator	Local User Setup
Browser-Server Security mode setup	Showing 206 records
Local User Policy Setup	
Local User Setup Role Management Setup	2. Advantacen
Certificate Setup	3 Addient Richards
	4. abchenstein
	5. Aida Agullar
	6. Alaric Castain
	7. alem.weldehimanot
	8. allen spiegel
	9. Andrew.OConnor
	10. Anwar.Khan
	11. armand.smith
	12. Bernard Alaton
	13. bhess
	14. DBILMason
	15. Dil.nash
	16. Billy Vaughan
	17. 🗋 bplotnik
	18 Broter Issue
	*Select items then take an Import Users Export Users Edit Delete Add Modify My Profile

**Passaggio 11.** Definire lo stesso nome utente e la stessa password creati per ISE nel passaggio 5 nella sezione Configurazione ISE. In questo esempio vengono utilizzati i **ruoli di autorizzazione delle attività csmoper** e **Help Desk**. Per salvare l'utente amministratore, selezionare **OK**.

ername: csmoper				
assword:			Verify Password:	
mail:				
uthorization Type				
elect an option: Full A	uthorization 💿 En	able Task Au	thorization C Enable Device Authori	rization
Roles		Device	level Authorization	
Help Desk		Not Ap	plicable	
Approver				
Network Operator				
Network Administrator	·			
System Administrator				
Super Admin				
Security Administrator				
Coounty Auministration				
Security Approver				
OK Cancel				

### Verifica

#### Interfaccia utente client di Cisco Security Manager

**Passaggio 1.** Aprire una nuova finestra del browser e digitare <u>https://<enter\_CSM\_IP\_Address</u>, utilizzare il nome utente e la password **csmadmin** creati nel passaggio 5 della sezione di configurazione ISE.



#### Sui log live ISE TACACS è possibile verificare l'esito del log nel tentativo

E Cisco ISE	Cisco ISE Operations · TA						Evaluation Mode 39 Days	0.00.00
Live Logs								
🖉 Refresh 🕁 Export To 🗸						Refresh Sho Every 3 seconds V La	w test 20 records 🗸	Within Last 3 hours → ⊽Filter → ⊕
Logged Time	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
×		~	Identity		Authentication Policy	Authorization Policy	ise Node	Network Device N
Apr 17, 2021 02:34:54.1		ia.	csmadmin	Authentic	CSM 4.22 >> Default		ise30	C5M422
Last Updated: Sat Apr 17 2021	09:37:58 0	MT-0500 (C	entral Daylight T	lime)				Records Shown: 1

#### Applicazione client Cisco Security Manager

**Passaggio 1.** Accedere all'applicazione client Cisco Security Manager con l'account di amministratore dell'helpdesk.

		3
	Cisco Security Manager Version 4.22.0 Service Pack 1	
	Server Name 10.88.243.42 V Username csmoper Password •••••• Default View Configuration Manager	
© 2020 Cisco Systems, Inc. Cisco, Cisco Systems an Its affiliates in the U.S. and certain other countries.	Login <u>Help</u> nd Cisco logo are registered trademarks of Cisco Systems, Inc. and/or cisco	

Sui log live ISE TACACS è possibile verificare l'esito del log nel tentativo

/e Logs								
						Refresh Every 3 seconds 🗸	Show Latest 20 records 🗸	Within Last 3 hours
C Refresh 🖞 Export To 🗸								V Filter V
C Refresh 🖞 Export To 🗸	Status	Details	Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	V Filter V
C Refresh the Expert To V Logged Time X	Status	Details	Identity Identity	Туре	Authentication Policy	Authorization Policy	Ise Node	Vetwork Device

**Passaggio 2.** Dal menu dell'applicazione client CSM selezionare **Strumenti > Amministrazione Security Manager**, deve essere visualizzato un messaggio di errore che indica la mancanza di privilegi.

🍮 Device 🗵 Nas 🔅 Pokcy 🙀	sky Bundle	Device Properties	6	6 🖗 🖗	Q % I					9,0	iearch All Categories	CISCO
Devkes 💽 🖗	Healt	Healt Facket Capture Witerd Prog.TaceBaste and Millockup Pintelligence			Dept	loyment P Fail 0 0	fenager Fending E - O	Paan: 0		Orvice State Octical 3 O Warring 3 O Korn	*1	
* J Lacator	0 a 1	Pinteligence								LeetUpdet	e Time: 17 Apr 2021 07	LIB PM PDT   B
* (34		Show Containment Inventory Status Catalyst Survmary Info Apply IPS Update		Alerta O	Connection 0	Sala 0	Deployment Qa •	Additional Information	P Address 199, 134, 215, 3 199, 139, 210, 3	reat Donain gwli etus vanto 3 uste gov gwli etus vanto 3 uste gov	Target 05 Herston 9.9(2) 9.9(2)	Running CS/ 5.9(2)40 5.9(2)40
P & Peniev Carl P Backup.	Preview Configuration Backup Security Manager Disonactics		-	:	0	8. 8.		199, 139, 210, 9 199, 139, 210, 30 199, 139, 215, 4	gin Links varies FLLinks ge gin Links varies FLLinks ge gin Links varies FLLinks gev	19.900 19.900 9.900	5.9(2)40 5.9(2)40 5.9(2)40	
- • no device selected	9 00	Security Manager Administration Security Manager Administration Onton volves Conference 0 Security Manager 0	0	:	:	0	9. 9. 9.		1998, 1298, 238, 4 1998, 1294, 215, 5 1999, 1299, 210, 5	igui) atus usrke il usta giri gui) atus usrk-ilunda giri gui) atus usrke il usta giri	9.9(2) 9.9(2) 9.9(2)	8.9(2)40 8.9(2)40 8.9(2)40
				Error	r - Ins	suffic	cient P	rivileges				x
You do r Please o If your If your	ontact y AA mod AA mod	sufficient privileges to p our system administrato e is ACS, privileges are e is non-ACS, privileges	perfor or and grant are (	m this of have t ted via of granted	operati hem gr ACS co I via "C	ion. rant y nfigur iscoW	ou additi ation. orks Hon	onal privileges. Jepage > Serve	er > Single-S	erver Management > L	ocal User Se	tup".

**Passaggio 3.** Ripetere i passaggi da 1 a 3 con l'account **csmadmin** per verificare che all'utente siano state fornite le autorizzazioni appropriate.

### Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Convalida della comunicazione con lo strumento TCP Dump su ISE

**Passaggio 1.** Accedere ad ISE e selezionare l'icona con le tre righe nell'angolo superiore sinistro, quindi selezionare **Operations>Troubleshoot>Diagnostic Tools.** 

Passaggio 2. In Strumenti generali selezionare TCP Dump, quindi selezionare Add+. Selezionare Nome host, Nome file interfaccia di rete, Repository e, facoltativamente, un filtro per raccogliere solo il flusso di comunicazione dell'indirizzo IP del CSM. Selezionare Salva ed esegui

#### Cisco ISE

Operations · Troubleshoot

<ul> <li>ACCOMPARIENT NOT NATION AND AND AND AND AND AND AND AND AND AN</li></ul>	Diagnostic Tools Dov	vnload Logs Debug V	Wizard	
data total   Add DDP Dump packet for monitoring on a network interface and troubleshoot problems on the network is they appear.   Rucha Automatic Configuration Values.   Rucha Troublashout   Rucha Troublashou		Add TCP Dump		
Automicitation Trouble         Discrete Rivers On	General Tools	V Add TCD Dump out	hat for monitorian on a m	natural interface and travidischoot problems on the actuarty of their appear
Bit Rank   Barling Root Rank   Partice Root Root Root Root   Agentess Porture TrootReton   Barling Root Root Root   Sasian Frace Tens     Far   By host 10.88.243.42   By host 10.88.243.42   By host 10.77.122.123 and not   10.77.122.123 and not <th>RADIUS Authentication TroubI</th> <th>Add for damp pad</th> <th>Net for monitoring on a re</th> <th>internet internete and observation problems on the network as only appres.</th>	RADIUS Authentication TroubI	Add for damp pad	Net for monitoring on a re	internet internete and observation problems on the network as only appres.
Waters Configeration Waters       im 30         Partices Finderston       im 30         Section Trace Tests       im 30         Top Duop       im 10         Section Trace Tests       im 10         Top Section Trace Tests       im 10         Image: Section Test Tests       im 10         Iman	Execute Network Device Com	Host Name *		
Particle Troublembourie   Carbine Oracle   Tor Dom   Session Trees Tests   Tor Stee Tools     The Time   Cist   Tor Stee Tools     The Time   Cist   Cist   Time Time   Cist   Time Time   Cist   Time Time   Cist   Time Linet   Second Model   Time Linet   Second Model     Time Linet   Second Model     Time Linet   Second Model     Time Linet   Second Model     Time Linet   Second Model     Time Linet   Second Model	Evaluate Configuration Validat	ise30	~	
Agendess Posters Troublesham   Breadward Delang   Bassian Trees Tests     Tractises Totols     Fig Dost 10.88.24.3.42   By Dost 10.77.122.123 and not   Durities Totol     Fig Dost 10.77.122.123 and not   Durities Totol     Fig Dost 10.77.122.123 and not     Durities Totol     Fig Dost 10.77.122.123 and not     Durities Totol     Fig Dost 10.77.122.109        Fig Dost 10.77.122.109        Fig Dost 10.77.122.109        Fig Dost 10.77.122.109           Fig Dost 10.77.122.109	Posture Troubleshooting			
Bigsbill Defreque       Gigsbill Defreque       Image: Construction of the co	Agentiess Posture Troublesho	Network Interface *		
Tor During         Session Tree Tests         Treetile Tool         Tor During         Cip (post 10.27.122.123 and not 10.77.122.123 and not 10.77.122.	EndPoint Debug	GigabitEthernet (	• ~	<ul> <li>Ø</li> </ul>
Transient Transient     Transient Tools     Transient Tools     Environ   Environ   Environ   WRRepository     Environ   WRRepository     Environ	TCP Dump			
Twettiee Tools       >         Pret:       Ip bots 10.88.243.42         Ip bots 10.88.243.42       Ip         Eg: (p hots 10.77.122.123 and not 10.77.122.123 and not 10.777.122.130         Hots 10.77.122.130         File size         C3M_TSHOOL         File size         100         Model(s)         100	Session Trace Tests			
Tractise Tools       Image: Dool 10.000,403.42         Image: Dool 10.000,403.42       Image: Dool 10.000,403.42         Image:		Filter	10	0
Trackset total       Cancel	Tourse and Toulo	10 nost 10.88.243	1.42	×
Eg: (p host 10.77.122.123 and not 10.777.122.119 File Name CSM_Tahnot	Trustaec tools	2	li.	
10.77.122.119 File Name CSM_Tishoot Recontory VMRepository ○		E.g: ip host 10.77.1	22.123 and not	
Fit same         Repository         WRepository         Fit Size         100         Mb         Limit 50         1         Fit (size)         Time Limit         5         Muste(s)         Muste(s)         Image: Promission Mode		10.177.122.119		
Fie Name CSM_TBinOC Recontary VMRepository VMRepository Pie Sire 10 0 Mb 0 1 Fie (s) Time Limit 5 0 Minuto(s) Minuto(s) 0 Minuto(s) 1 Premiscuous Mode				
Recontary         VMRepository         File Size         100         Mb         Mb         Mb         Imme to         1       Imme on         File(s)         File(s)         Minute(s)         Minute(s)         Promiseuous Mode		File Name CSM_Tshoot		
Resistory       Image: Size state stat				
Repository VMRepository Fie Size 10 0 Mb 0 Fie(s) Fie(s) Time Limit 5 0 Minute(s) Promiscuous Mode Cancel Save Save and Run				
WRepository       V         File Size       Image: Size         100       Image: Size         1       Image: Size         Image: Size       Image: Size         Image: Size       Image: Size         Image: Size       Image: Size         Image: Size       Size		Repository		
File Stree       Image: Stree Street St		VMRepository	~	2 0
Fie Size 10 Mb Limit to 1 Fie(s) Fie(s) Time Limit 5 Minute(s) Promiscuous Mode Limit to 1 Difference Minute(s) Cancel Save and Run				
100     Image: Cancel       100     Image: Cancel		File Size		
Mb Limit to 1		100	0	0
Limit to 1 I I I File(s) Time Limit 5 I I Minute(s) Promiscuous Mode Limit Save and Run			Mb	
Limit to 1 I I I I I I I I I I I I I I I I I I I				
1 File(s) Time Limit 5 Minute(s) Promiscuous Mode Cancel Save and Run		Limit to		
File(s) Time Limit 5 O Minute(s) Promiscuous Mode Cancel Save and Run		1	0	U
Time Limit     Image: Save and Run       5     Image: Save and Run			File(s)	
Time Limit 5 O Minute(s) Promiscuous Mode Cancel Save Save and Run				
Minute(s) Promiscuous Mode Cancel Save and Run		Time Limit 5	0	0
Promiscuous Mode  Cancel Save and Run		-	Minute(s)	
Cancel Save and Run				7
Cancel Save and Run		U Promiscuous Mode		
Cancel Save and Run				
				Cancel Save Save and Run

**Passaggio 3.** Accedere all'applicazione client CSM o all'interfaccia utente client e digitare le credenziali dell'amministratore.

**Passaggio 4.** Su ISE, selezionare **il** pulsante **Stop** e verificare che il file pcap sia stato inviato al repository definito.

₿ Re	fresh + Add	0 Edit	🔋 Trash 🗸 🕨 Start	$\odot$ Stop 😃 Downloa	ad		$\nabla$	Filter 🗸 🐵
	Host Name		Network Interface	Filter	File Name	Repository	File S	Number o
	ise30.ciscoise.lab		GigabitEthernet 0	ip host 10.88.24	3.42 CSM_Tshoot	VMReposit	100	1

File Commands Tools Favorites Options Help	Comment SFX
Add Extract To Test View Delete Find Wizard Info VirusScan	Comment SFX
CSM_Tshoot.zip - ZIP archive, unpacked size 1,166 bytes	
Name Size Packed Type Modified CRC	RC32
File folder	
CSM_Tshoot.pcap 1,166 556 PCAP File 4/17/2021 3:29 8A27	A 27900D

Passaggio 5. Aprire il file pcap per verificare la corretta comunicazione tra CSM e ISE.

•	•				CSM_Tshoot.pcap
	📕 🙋 🤅	S 🛛 🗋 📹 🤇	९ 🗰 🗯 警	Ŧ 🗶 🗔	📃 Q Q Q II
A N	oply a display filt	er<%/>			Expression +
No.	Time	Source	Destination	Protocol	Lengt? Info
100	1 0.000000	10.88.243.42	10.122.112.4	TCP	66 55740 → 49 [SYN, ECN, CMR] Seq=0 Win=8192 Len=0 MSS=1300 WS=256 SACK_PERM=1
	2 0.000130	10.122.112.4	10.88.243.42	TCP	66 49 → 55740 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
	3 0.065688	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [ACK] Seq=1 Ack=1 Win=66048 Len=0
	4 0.101272	10.88.243.42	10.122.112.4	TACACS+	97 Q: Authentication
	5 0.101362	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [ACK] Seq=1 Ack=44 Win=29312 Len=0
	6 0.107185	10.122.112.4	10.88.243.42	TACACS+	81 R: Authentication
	7 0.203012	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [ACK] Seq=44 Ack=28 Win=66048 Len=0
	8 0.220350	10.88.243.42	10.122.112.4	TACACS+	80 Q: Authentication
	9 0.259963	10.122.112.4	10.88.243.42	TCP	54 49 → 55740 [ACK] Seq=28 Ack=70 Win=29312 Len=0
	10 0.311136	10.122.112.4	10.88.243.42	TACACS+	72 R: Authentication
	11 0.311193	10.122.112.4	10.88.243.42	TCP	54 49 - 55740 [FIN, ACK] Seq=46 Ack=70 Win=29312 Len=0
	12 0.375973	10.88.243.42	10.122.112.4	TCP	60 55740 → 49 [ACK] Seq=70 Ack=47 Win=66048 Len=0
	13 8.488651	10.88.243.42	10.122.112.4	TCP	60 55740 + 49 [FIN, ACK] Seq=70 Ack+47 Win=66048 Len=0
> F	rame 6: 81 by	tes on wire (648 bits),	, 81 bytes captured (6	48 bits)	
> E	thernet II, S	rc: Vmware_a4:0d:c6 (0)	0:50:56:a4:0d:c6), Dst	: Cisco_1f:21:4	15 (00:14:6a:1f:21:45)
> 1	nternet Proto	col Version 4, Src: 10.	122.112.4, Dst: 10.88	.243.42	
⇒ T ⊽ T,	ransmission C ACACS+	ontrol Protocol, Src Po	ort: 49, Dst Port: 557	40, Seq: 1, Ac)	<: 44, Len: 27
	Major versio	on: TACACS+			
	Minor version Type: Auther	nt: 0 htication (1)			
>	Flags: 0x00 Session ID:	(Encrypted payload, Mu 3819957939	ltiple Connections)		
	Darket least	h. 15			
000	00 14 6a 1	f 21 45 00 50 56 a4 0	d c6 88 88 45 88 ···	j · ! E · P V · · · · E	
0	CSM_Tshoot	рсар			Packets: 14 - Displayed: 14 (100.0%)     Profile: Default
_	_				

Se nel file pcap non sono visualizzate voci, verificare quanto segue:

- 1. Il servizio Amministrazione dispositivi è abilitato sul nodo ISE
- 2. L'indirizzo IP ISE destro è stato aggiunto alla configurazione CSM
- 3. Se il firewall si trova nella parte centrale, verificare che la porta 49 (TACACS) sia autorizzata.