

Configurazione dell'autenticazione TACACS+ sullo switch Arista con ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione TACACS+ su ISE](#)

[Configurazione switch Arista](#)

[Passaggio 1. Abilitare l'autenticazione TACACS+](#)

[Passaggio 2. Salvataggio della configurazione](#)

[Verifica](#)

[Recensione ISE](#)

[Risoluzione dei problemi](#)

[Problema 1](#)

[Possibili cause](#)

[Problema 2](#)

[Possibili cause](#)

[Soluzione](#)

Introduzione

In questo documento viene descritto come integrare Cisco ISE TACACS+ con uno switch Arista per un accesso AAA centralizzato di amministratore.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocollo Cisco ISE e TACACS+.
- Switch Arista

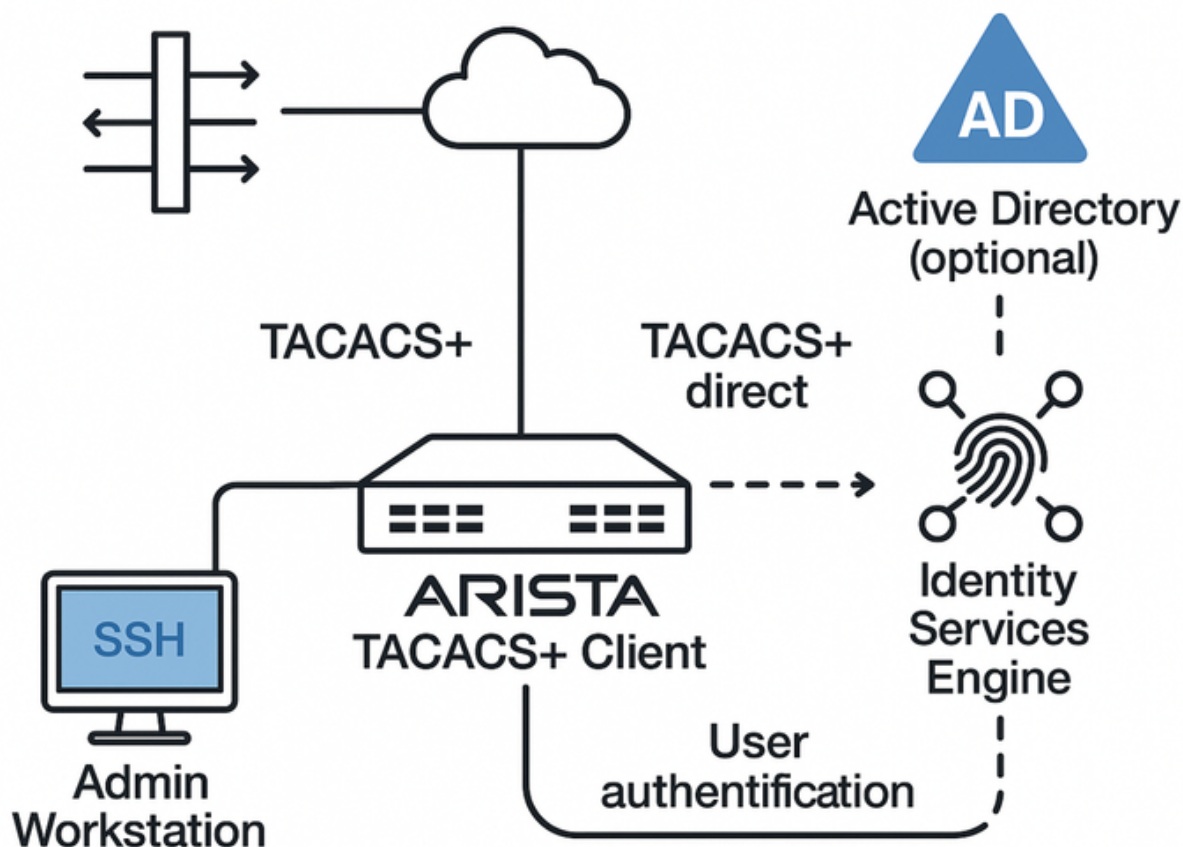
Componenti usati

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

- Versione immagine software switch Arista: 4.33.2F
- Patch 4 per Cisco Identity Services Engine (ISE) versione 3.3

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

Esempio di rete

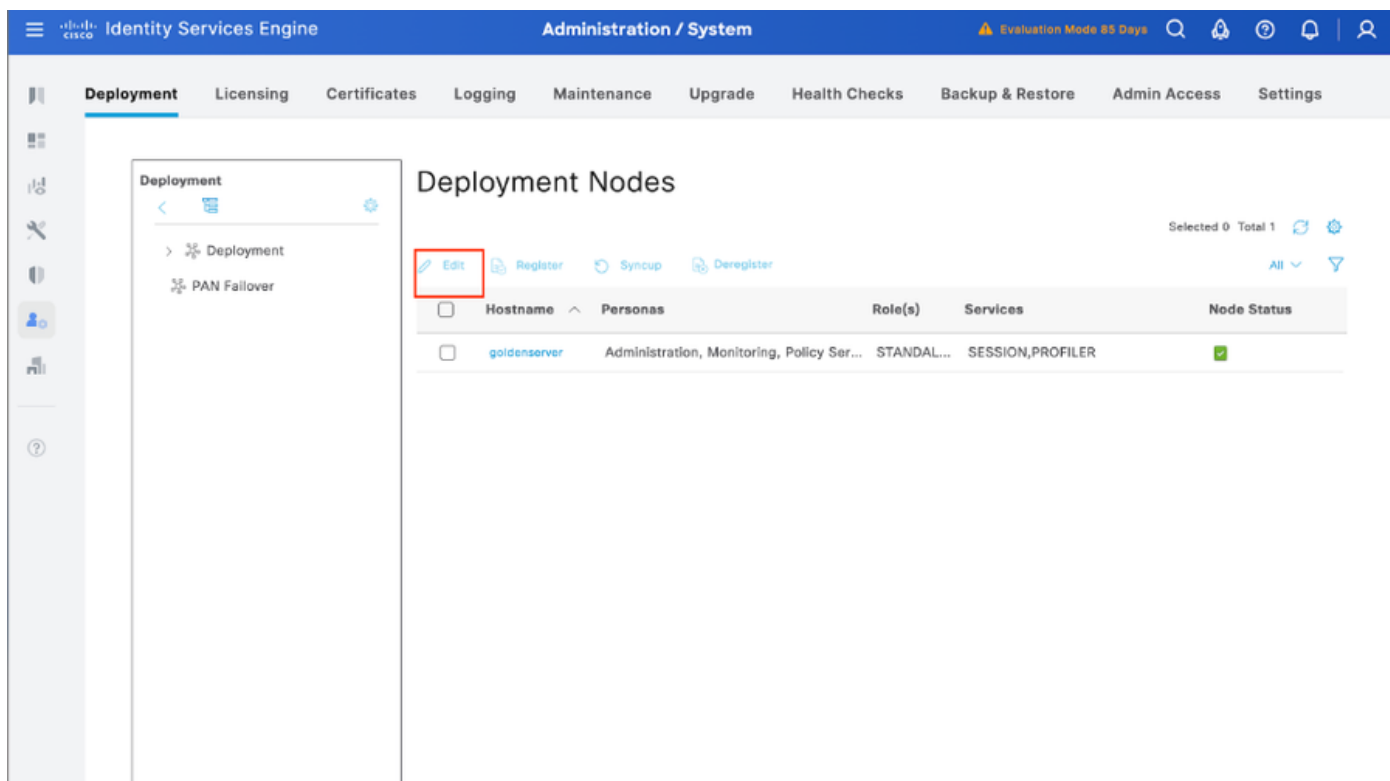


Configurazioni

Configurazione TACACS+ su ISE

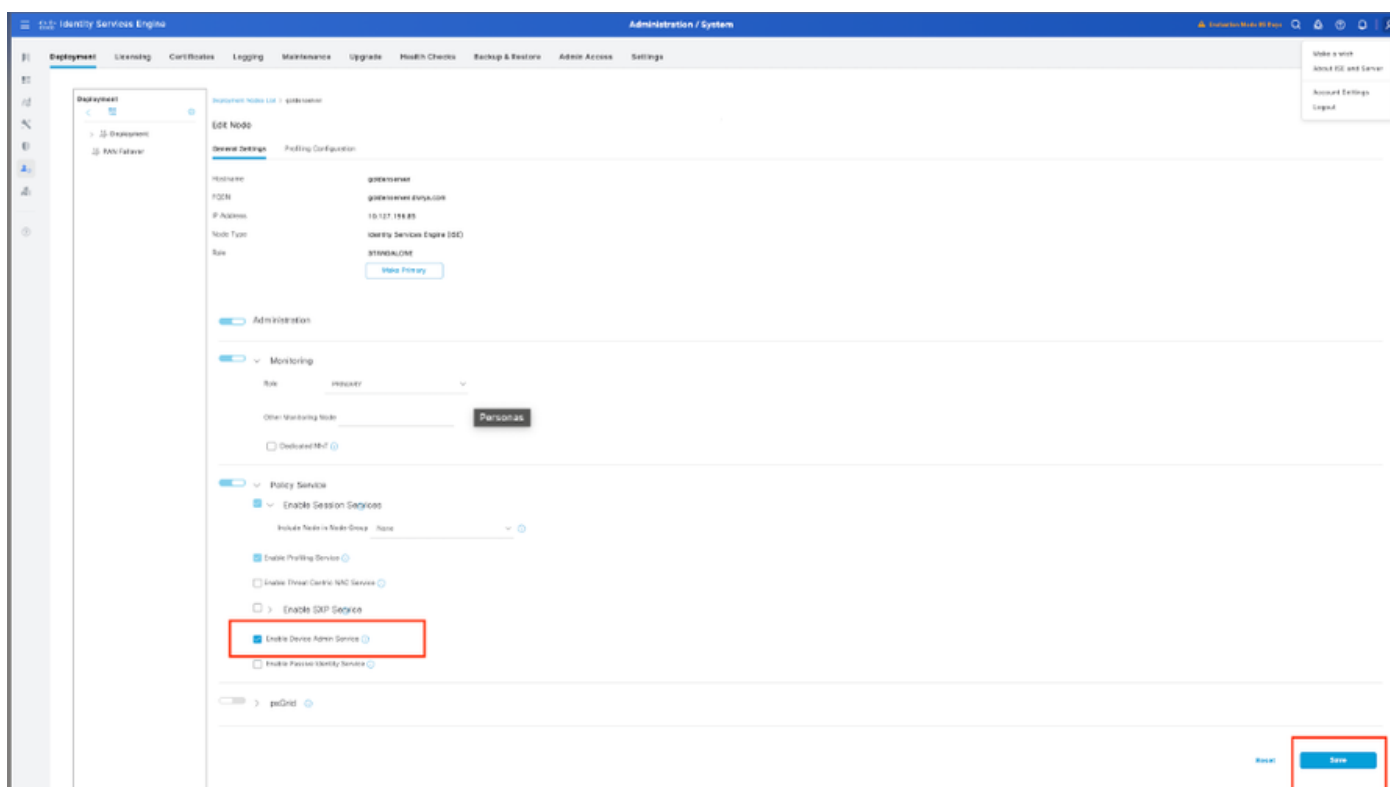
Passaggio 1. Il passaggio iniziale consiste nel verificare se Cisco ISE dispone delle funzionalità necessarie per gestire l'autenticazione TACACS+. A tale scopo, verificare che nel nodo PSN (Policy Service Node) desiderato sia attivata la funzionalità Servizio amministrazione dispositivi.

Passare a Amministrazione > Sistema > Distribuzione, selezionare il nodo appropriato in cui ISE elabora l'autenticazione TACACS+ e fare clic su Modifica per rivedere la configurazione.



Passaggio 2. Scorrere verso il basso per individuare la funzionalità Servizio di amministrazione del dispositivo. Notare che l'abilitazione di questa funzionalità richiede che la persona del servizio criteri sia attiva sul nodo, insieme alle licenze TACACS+ disponibili nella distribuzione.

Selezionare la casella di controllo per abilitare la funzionalità, quindi salvare la configurazione.

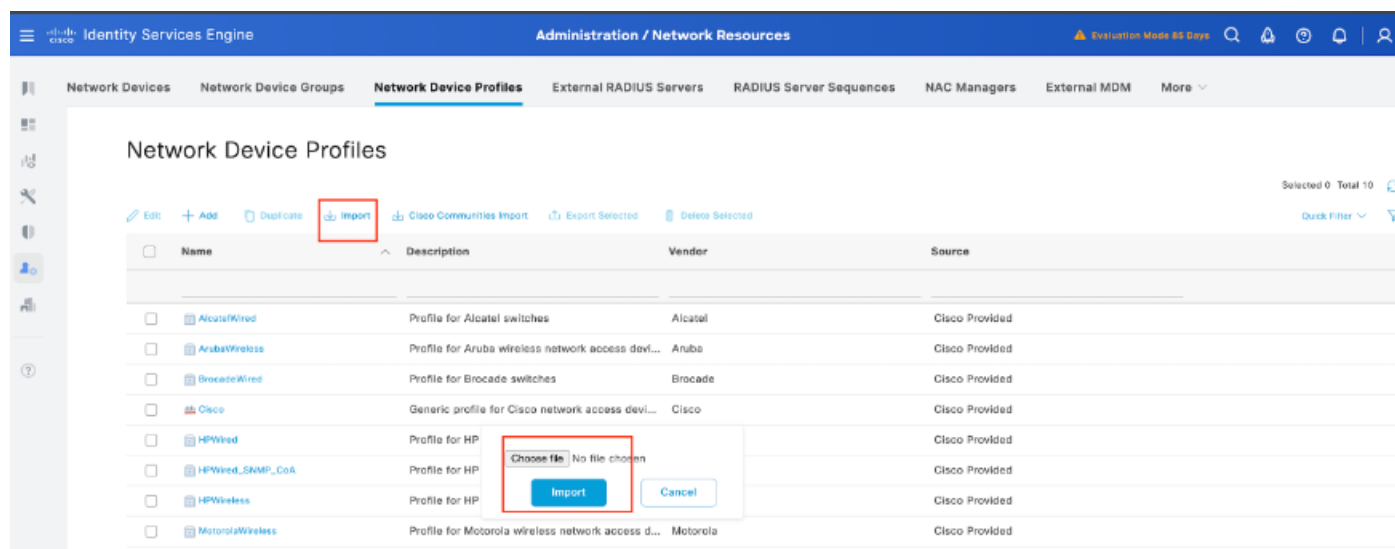


Passaggio 3. Come ottenere il profilo del dispositivo di rete Arista per Cisco ISE.

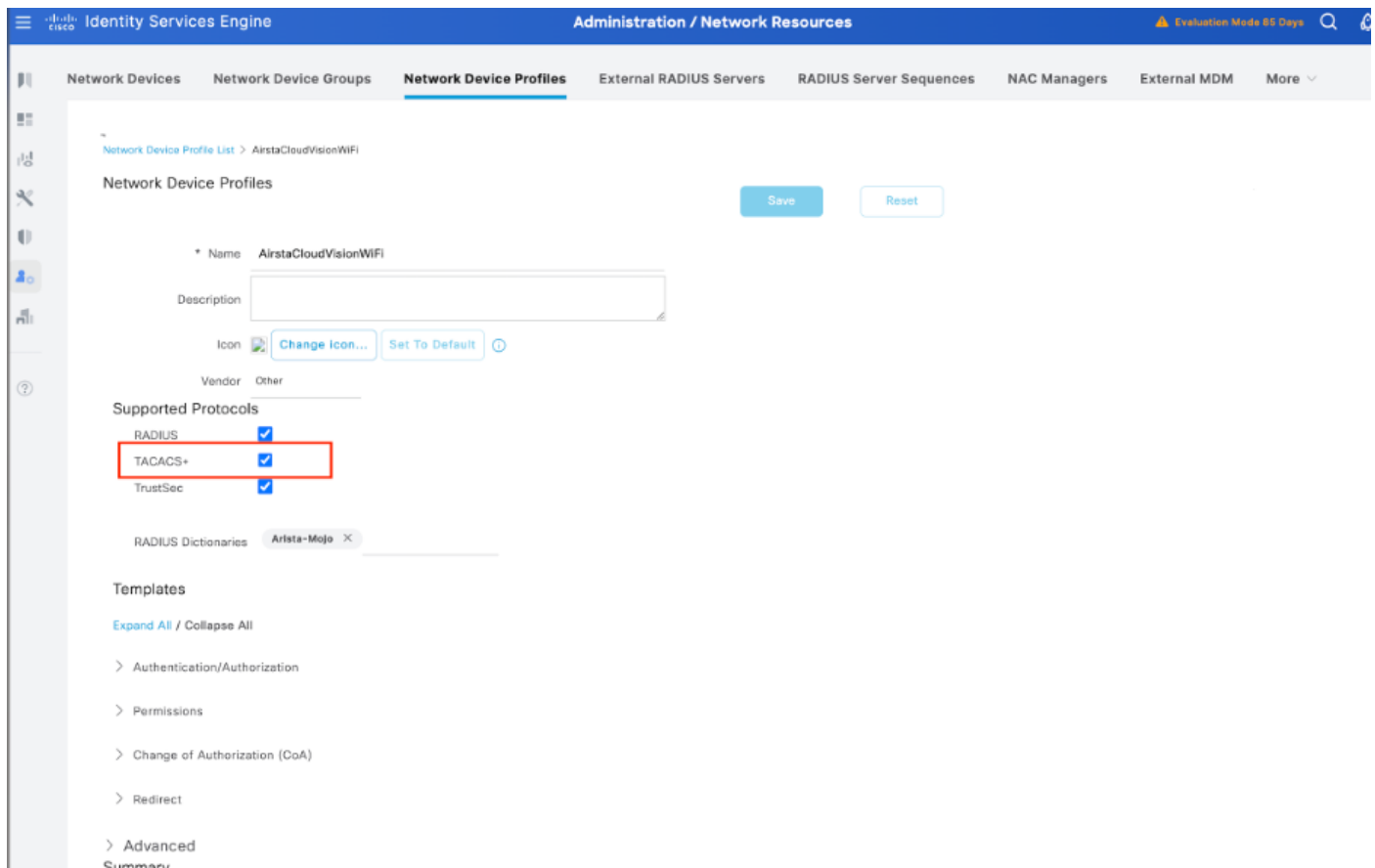
La Cisco Community ha condiviso un profilo NAD dedicato per i dispositivi Arista. Questo profilo, insieme ai file del dizionario necessari, è disponibile nell'articolo [Arista CloudVision WiFi Dictionary e NAD Profile for ISE Integration](#). Il download e l'importazione di questo profilo nella configurazione ISE semplifica l'integrazione

Procedura per importare il profilo Arista e AD in Cisco ISE:

1. Scarica il profilo:
 - Ottenere il profilo Arista NAD dal collegamento alla Cisco Community indicato sopra. [Cisco Community](#)
2. Access Cisco ISE:
 - Accedere alla console di amministrazione di Cisco ISE.
3. Importare il profilo NAD:
 - Selezionare Amministrazione > Risorse di rete > Profili dispositivi di rete.
 - Fare clic sul pulsante Importa.
 - Caricare il file di profilo Arista e AD scaricato.

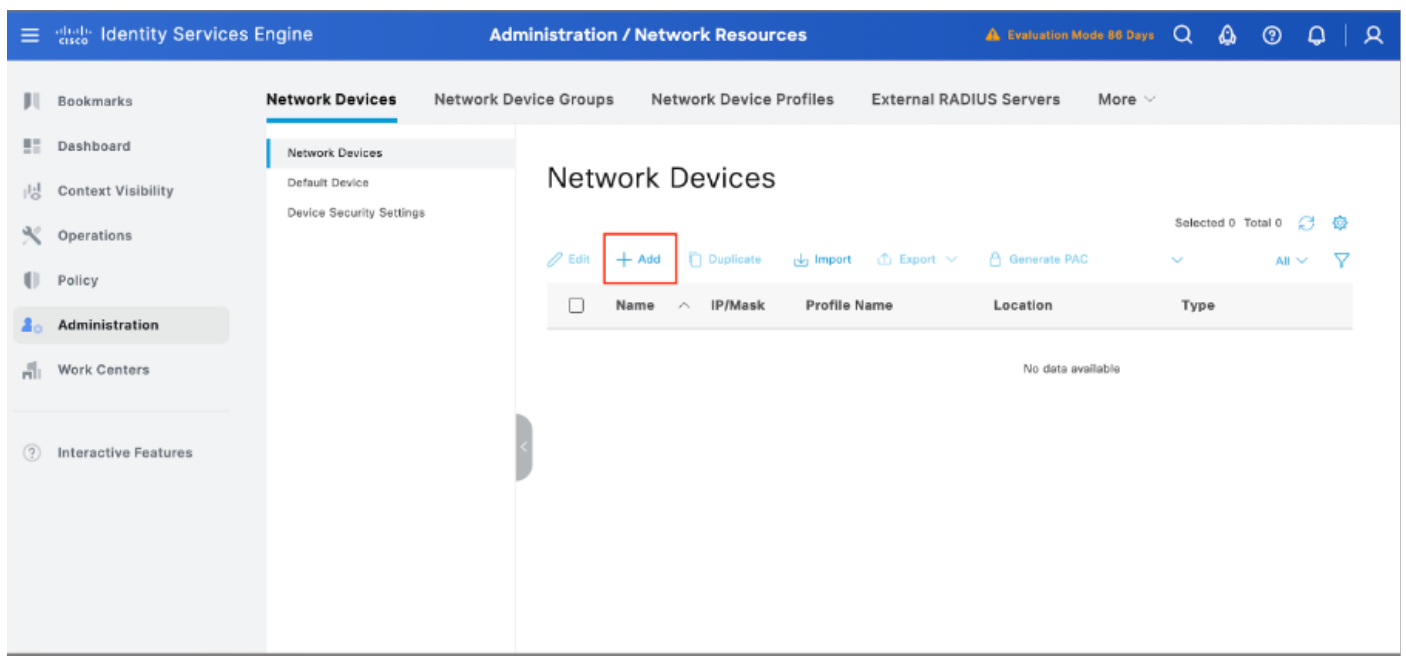


Al termine del caricamento, accedere all'opzione Edit e abilitare TACACS+ come protocollo supportato.



Passaggio 2: Aggiungere lo switch Arista come dispositivo di rete.

1. Selezionare Amministrazione > Risorse di rete > Dispositivi di rete> +Aggiungi:



2. Fare clic su Add (Aggiungi) e inserire i seguenti dati:

- Indirizzo IP: <IP switch>
- Tipo di dispositivo: Scegli altro cablato
- Profilo dispositivo di rete: selezionare AirstaCloudVisionWiFi.

- Impostazioni autenticazione RADIUS:
 - Abilita autenticazione RADIUS.
 - Immettere il segreto condiviso (deve corrispondere alla configurazione dello switch).

3. Fare clic su Salva:

The screenshot shows the 'Administration / Network Resources' page in the Cisco ISE console. The 'Network Devices' tab is selected. The configuration for 'Arista_switch' is displayed. The 'Name' field is 'Arista_switch'. The 'Description' is 'Arista_switch for device login TACACS and'. The 'IP Address' is '32'. The 'Device Profile' is 'AristaCloudVisionWiFi'. The 'Model Name' is empty. The 'Software Version' is '4-33-2F'. The 'Network Device Group' is 'All Locations'. The 'Location' is 'All Locations'. The 'IPSEC' is 'No'. The 'Device Type' is 'All Device Types'. The 'RADIUS Authentication Settings' section is expanded, showing 'Protocol' as 'RADIUS' and 'Shared Secret' as a redacted field. The 'Use Second Shared Secret' checkbox is unchecked.

Passaggio 3. Verificare che il nuovo dispositivo sia visualizzato in Dispositivi di rete:

The screenshot shows the 'Network Devices' list in the Cisco ISE console. The table contains one entry: 'Arista_switch'. The table has columns for Name, IP/Mask, Profile Name, Location, Type, and Description. The 'Arista_switch' entry has a profile name of 'AristaCloudVisionWiFi', location of 'All Locations', and type of 'All Device Types'.

Name	IP/Mask	Profile Name	Location	Type	Description
Arista_switch		AristaCloudVisionWiFi	All Locations	All Device Types	Arista_switch f

Passaggio 4. Configurare il profilo TACACS.

Creare un profilo TACACS, selezionare il menu Work Center > Device Administration > Policy Elements > Results > TACACS Profiles, quindi selezionare Add:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Device Administration'. The left sidebar contains various navigation options like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', and 'Interactive Features'. The main content area is titled 'TACACS Profiles' and displays a table of profiles. The 'Add' button is highlighted with a red box.

Name	Type	Description
Arista Profile Admin	Shell	
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
TAC_PROFILE_PRIV15	Shell	
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

Immettere un nome, selezionare la casella di controllo Privilegio predefinito e impostare il valore su 15. Selezionare inoltre Privilegio massimo, impostarne il valore su 15 e fare clic su Sottometti:

The screenshot shows the configuration page for the TACACS Profile 'TAC_PROFILE_PRIV15'. The 'Name' field is highlighted with a red box. Below the 'Name' field, there is a 'Description' field. The 'Task Attribute View' tab is selected, and the 'Common Tasks' section is visible. The 'Common Task Type' is set to 'Shell'. The 'Default Privilege' and 'Maximum Privilege' fields are highlighted with a red box, both set to 15. The 'Access Control List' field is set to 'Access Control List'. The 'Auto Command' field is set to 'Auto Command'. The 'No Escape' field is set to 'No Escape'. The 'Timeout' field is set to 60 minutes. The 'Idle Time' field is set to 15 minutes.

Passaggio 5. Creare un set di criteri di amministrazione del dispositivo da utilizzare per lo switch Arista, selezionare il menu Work Center > Device Administration > Device Admin Policy Sets, quindi selezionare l'icona del dispositivo da inserire nella riga precedente da un set di criteri esistente.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27	⋮	
+	Default	Tacacs Default policy set		Default Device Admin		⋮	

Context menu options: Insert new row above, Insert new row below, Duplicate above, Duplicate below, Delete.

Passaggio 6. Assegnare un nome al nuovo set di criteri, aggiungere le condizioni in base alle caratteristiche delle autenticazioni TACACS+ in corso sullo switch Arista e selezionare Protocolli consentiti > Amministrazione predefinita dispositivi, quindi salvare la configurazione.

Identity Services Engine Work Centers / Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27	⋮	
+	Default	Tacacs Default policy set				⋮	

Context menu options: Allowed Protocols (Default Device Admin, Default Network Access), Duplicate above, Duplicate below, Delete.

Passaggio 7. Selezionare nell'opzione > view, quindi nella sezione Authentication Policy (Criteri di autenticazione) selezionare l'origine identità esterna utilizzata da Cisco ISE per eseguire la query del nome utente e delle credenziali per l'autenticazione sullo switch Arista. Nell'esempio, le credenziali corrispondono a Internal Users memorizzato in ISE.

Identity Services Engine Work Centers / Device Administration

Policy Sets → Arista Switch Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	22	Options

Passaggio 8. Scorrere verso il basso fino a visualizzare la sezione Criteri di autorizzazione relativa ai criteri predefiniti, selezionare l'icona dell'ingranaggio, quindi inserire una regola.

Passaggio 9. Assegnare un nome alla nuova regola di autorizzazione, aggiungere le condizioni relative all'utente già autenticato come appartenenza al gruppo e, nella sezione Profili shell, aggiungere il profilo TACACS configurato in precedenza e salvare la configurazione.

Identity Services Engine Work Centers / Device Administration

Policy Sets → Arista Switch Access

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Arista Switch Access		DEVICE Device Type EQUALS All Device Types	Default Device Admin	27

Authorization Policy(2)

Status	Rule Name	Conditions	Results		Hits	Actions
			Command Sets	Shell Profiles		
✓	Arista_Switch	InternalUser-identityGroup EQUALS User Identity Groups:Employee	PermitAllCommands	TAC_PROFILE_PRIV15	10	
✓	Default		DenyAllCommands	Deny All Shell Profile	5	

Configurazione switch Arista

Passaggio 1. Abilitare l'autenticazione TACACS+

Accedere allo switch Arista e accedere alla modalità di configurazione:

configurazione

!

```
tacacs-server host <ISE-IP> chiave <TACACS-SECRET>
```

!

```
acs server di gruppo aaa+ ISE_TACACS
```

```
server <ISE-IP>
```

!

```
aaa authentication login default group ISE_TACACS local
```

```
aaa authorization exec default group ISE_TACACS local
```

```
comandi di accounting aaa 15 gruppo start-stop predefinito ISE_TACACS
```

!

```
End
```

Passaggio 2. Salvataggio della configurazione

Per salvare in modo permanente la configurazione dopo il riavvio:

```
# scrittura di memoria
```

```
O
```

```
# copy running-config startup-config
```

Verifica

Recensione ISE

Passaggio 1. Verificare che il servizio TACACS+ sia in esecuzione e che sia possibile archiviarlo:

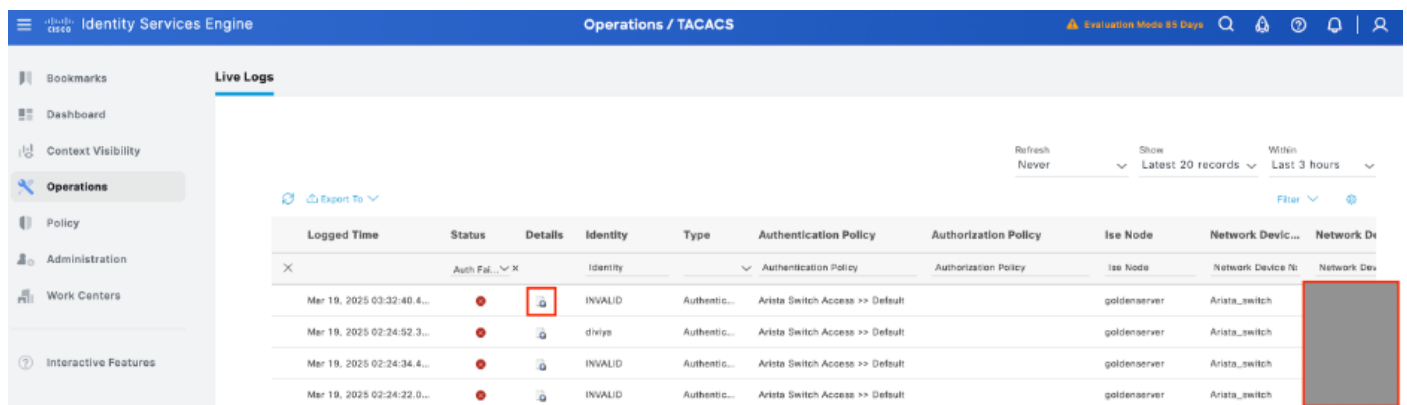
- GUI: Verificare se il nodo è elencato con il servizio DEVICE ADMIN in > Sistema > Distribuzione.
- CLI: Eseguire il comando `show ports | include 49` per confermare che la porta TCP contiene connessioni che appartengono a TACACS+

```
goldenserver/admin#show ports | include 49
```

```
tcp: [REDACTED]
```

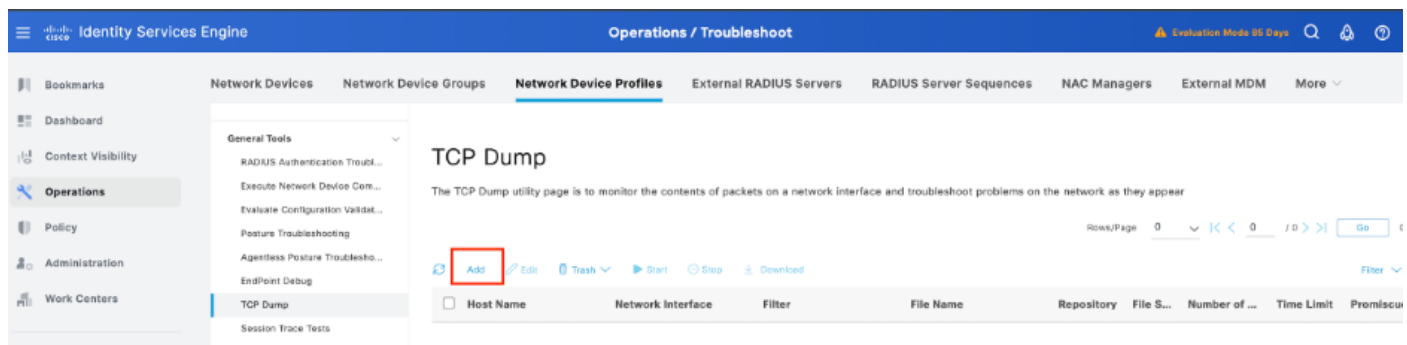
Passaggio 2. Conferma se sono presenti livellog relativi ai tentativi di autenticazione TACACS+: è possibile selezionare questa opzione nel menu Operazioni > TACACS > Live logs,

A seconda del motivo dell'errore, è possibile modificare la configurazione o risolvere la causa dell'errore.

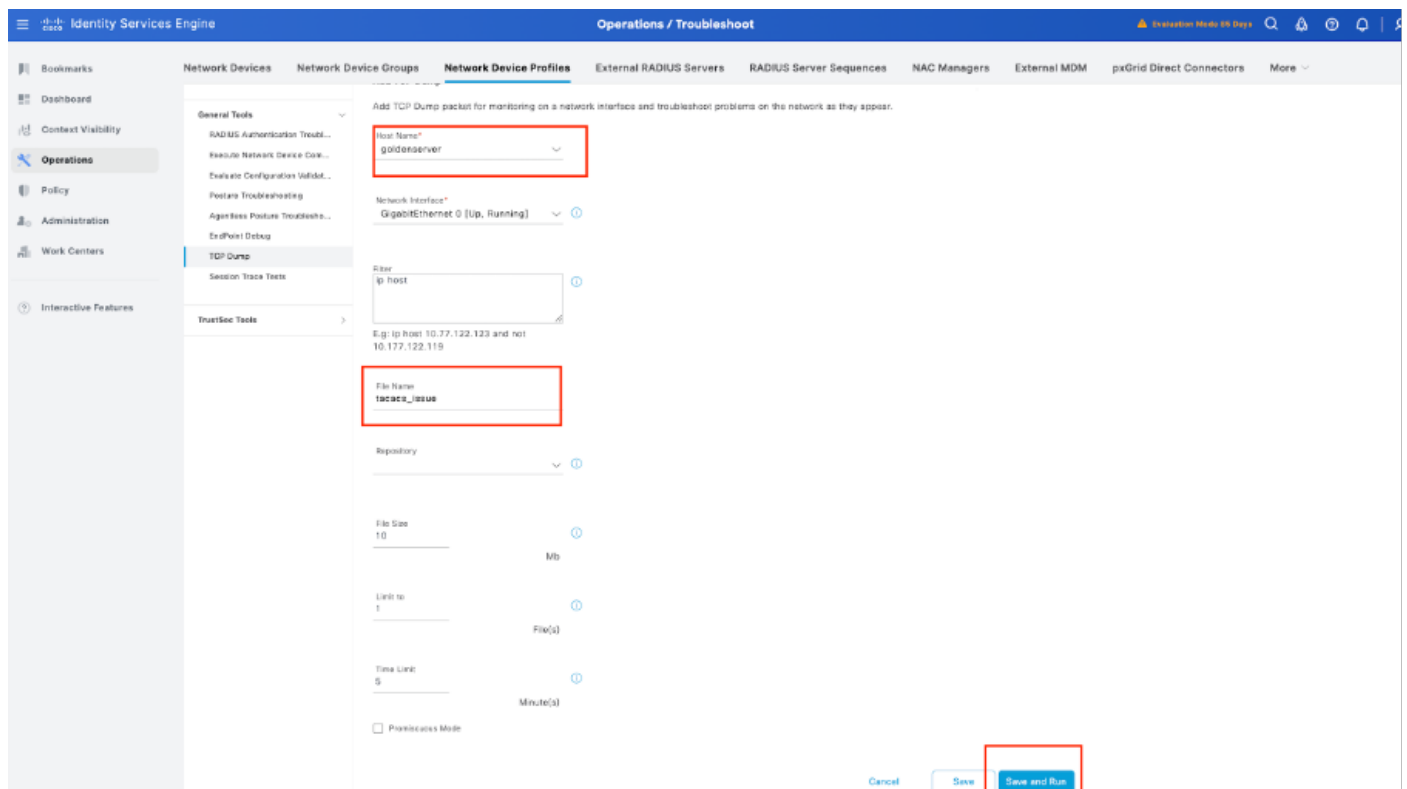


Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device...	Network De
Mar 19, 2025 03:32:40.4...	Auth Fail...	X	INVALID	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	
Mar 19, 2025 02:24:52.3...			diviya	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:24:34.4...			INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:24:22.0...			INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	

Passaggio 3. Se non viene visualizzato alcun catalogo, procedere all'acquisizione di un pacchetto. Passare al menu Operazioni > Risoluzione dei problemi > Strumenti diagnostici > Strumenti generali > TCP Dump , selezionare Aggiungi:



Host Name	Network Interface	Filter	File Name	Repository	File S...	Number of ...	Time Limit	Promiscu
-----------	-------------------	--------	-----------	------------	-----------	---------------	------------	----------



Host Name*
goldenserver

Network Interface*
GigabitEthernet 0 [Up, Running]

Filter
ip host

File Name
tacosca_issue

Repository

File Size
10 Mb

Limit to
1 File(s)

Time Limit
5 Minute(s)

☐ Promiscuous Mode

Cancel Save Save and Run

Passaggio 4. Abilitare il componente runtime-AAA nel debug nel PSN da cui viene eseguita

l'autenticazione in Operazioni > Risoluzione dei problemi > Debug guidato > Configurazione log di debug, selezionare il nodo PSN, quindi selezionare il pulsante Modifica:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Operations / Troubleshoot'. A sidebar on the left contains links to Bookmarks, Dashboard, Context Visibility, Operations (highlighted), Policy, Administration, Work Centers, and Interactive Features. The main content area is titled 'Debug Wizard' and has tabs for 'Diagnostic Tools' and 'Download Logs'. Under 'Diagnostic Tools', 'Debug Profile Configuration' and 'Debug Log Configuration' are listed. The 'Node List' is displayed, showing a table with columns 'Node Name' and 'Replication Role'. One node, 'goldenserver', is listed with a 'STANDALONE' role. Above the table are links for 'Edit' and 'Reset to Default'. A status bar at the top right indicates 'Evaluation Mode 85 Days'.

Node Name	Replication Role
goldenserver	STANDALONE

The screenshot shows the 'Debug Level Configuration' page in the Cisco Identity Services Engine (ISE) interface. The top navigation bar and sidebar are the same as in the previous screenshot. The main content area is titled 'Debug Level Configuration' and has tabs for 'Diagnostic Tools' and 'Download Logs'. Under 'Diagnostic Tools', 'Debug Profile Configuration' and 'Debug Log Configuration' are listed. The 'Debug Level Configuration' page shows a table with columns 'Component Name', 'Log Level', 'Description', 'Log file Name', and 'Log Filter'. The 'runtime-AAA' component is selected, and its log level is set to 'DEBUG'. The log filter is set to 'Disabled'. The log file name is 'prtt-server.log'. The description is 'AAA runtime messages (prtt)'. There are links for 'Edit', 'Reset to Default', 'Log Filter Enable', and 'Log Filter Disable'. A 'Quick Filter' dropdown is also present. A red box highlights the 'runtime-AAA' row. Below the table are 'Save' and 'Cancel' buttons.

Component Name	Log Level	Description	Log file Name	Log Filter
runtime-AAA	DEBUG	AAA runtime messages (prtt)	prtt-server.log	Disabled

Identificare il componente runtime-AAA, impostarne il livello di log per eseguire il debug, riprodurre il problema e analizzare i log per ulteriori informazioni.

Risoluzione dei problemi

Problema 1

L'autenticazione TACACS+ tra Cisco ISE e lo switch Arista (o un dispositivo di rete) non riesce con il messaggio di errore:

"13036 Selected Shell Profile is DenyAccess"

Overview		Steps	
Request Type	Authentication	13013	Received TACACS+ Authentication START Request
Status	Fail	15049	Evaluating Policy Group (🔍 Step latency=1ms)
Session Key	goldenserver/541265148/80	15008	Evaluating Service Selection Policy (🔍 Step latency=0ms)
Message Text	Failed-Attempt: Authentication failed	15048	Queried PIP - DEVICE.Device Type (🔍 Step latency=2ms)
Username	diviya	15041	Evaluating Identity Policy (🔍 Step latency=3ms)
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth	15048	Queried PIP - Network Access.Protocol (🔍 Step latency=2ms)
Selected Authorization Profile	Deny All Shell Profile	15013	Selected Identity Source - Internal Users (🔍 Step latency=2ms)
Authentication Details		24210	Looking up User in Internal Users IDStore (🔍 Step latency=0ms)
Generated Time	2025-07-27 16:06:30.094000 +05:30	24212	Found User in Internal Users IDStore (🔍 Step latency=37ms)
Logged Time	2025-07-27 16:06:30.094	13045	TACACS+ will use the password prompt from global TACACS+ configuration (🔍 Step latency=0ms)
Epoch Time (sec)	1753612590	13015	Returned TACACS+ Authentication Reply (🔍 Step latency=0ms)
ISE Node	goldenserver	13014	Received TACACS+ Authentication CONTINUE Request (🔍 Step latency=68ms)
Message Text	Failed-Attempt: Authentication failed	15041	Evaluating Identity Policy (🔍 Step latency=0ms)
Failure Reason	13036 Selected Shell Profile is DenyAccess	15013	Selected Identity Source - Internal Users (🔍 Step latency=4ms)
Resolution	Check whether the Device Administration Authorization Policy rules are correct	24210	Looking up User in Internal Users IDStore (🔍 Step latency=0ms)
Root Cause	Selected Shell Profile fails for this request	24212	Found User in Internal Users IDStore (🔍 Step latency=7ms)
Username	diviya	22037	Authentication Passed (🔍 Step latency=0ms)
		15036	Evaluating Authorization Policy (🔍 Step latency=0ms)
		15048	Queried PIP - Network Access.UserName (🔍 Step latency=4ms)

L'errore "13036 Selected Shell Profile is DenyAccess" in Cisco ISE in genere indica che, durante un tentativo di amministrazione di un dispositivo TACACS+, i criteri di autorizzazione corrispondono a un profilo della shell impostato su DenyAccess. Ciò non è in genere il risultato di un profilo della shell non configurato correttamente, ma indica piuttosto che nessuna delle regole di autorizzazione configurate corrisponde agli attributi utente in ingresso (ad esempio, appartenenza a gruppi, tipo di dispositivo o posizione). Di conseguenza, ISE torna a una regola predefinita o a una regola di negazione esplicita, che determina il rifiuto dell'accesso.

Possibili cause

- Rivedere le regole dei criteri di autorizzazione in ISE. Verificare che l'utente o il dispositivo corrisponda alla regola corretta che assegna il profilo di shell desiderato, ad esempio quella che consente l'accesso appropriato.
- Verificare che il mapping AD o del gruppo di utenti interno sia corretto e che le condizioni dei criteri, ad esempio l'appartenenza al gruppo di utenti, il tipo di dispositivo e il protocollo, siano specificate correttamente.
- Usare i log live ISE e i dettagli del tentativo non riuscito di vedere esattamente quale regola corrisponde e perché.

Problema 2

L'autenticazione TACACS+ tra Cisco ISE e lo switch Arista (o un dispositivo di rete) non riesce con il messaggio di errore:

"13017: ricevuto pacchetto TACACS+ da dispositivo di rete o client AAA sconosciuto"

 Cisco ISE

Overview

Request Type	Authentication
Status	Fail
Session Key	
Message Text	Failed-Attempt: TACACS+ Request dropped
Username	
Authentication Policy	
Selected Authorization Profile	

Steps

13017	Received TACACS+ packet from unknown Network Device or AAA Client
-------	---

Authentication Details

Generated Time	2025-07-27 17:50:17.705000 +05:30
Logged Time	2025-07-27 17:50:17.705
Epoch Time (sec)	1753618817
ISE Node	goldenserver
Message Text	Failed-Attempt: TACACS+ Request dropped
Failure Reason	13017 Received TACACS+ packet from unknown Network Device or AAA Client
Resolution	
Root Cause	
Username	

Possibili cause

- Il motivo più comune è che l'indirizzo IP dello switch non viene aggiunto come dispositivo di rete in ISE (in Amministrazione > Risorse di rete > Dispositivi di rete).
- Verificare che l'indirizzo IP o l'intervallo corrisponda esattamente all'indirizzo IP di origine usato dallo switch Arista per inviare i pacchetti TACACS+.
- Se lo switch usa un'interfaccia di gestione, verificare che l'IP esatto (non solo una subnet/intervallo) sia stato aggiunto in ISE.

Soluzione

- Selezionare Amministrazione > Risorse di rete > Dispositivi di rete nella GUI di ISE.
- Verificare che l'indirizzo IP di origine esatto sullo switch Arista sia in uso per la comunicazione TACACS+ (molto spesso l'IP dell'interfaccia di gestione).
- Specificare il segreto condiviso (deve corrispondere a quello impostato sullo switch Arista).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).