

# Configurazione dell'autorizzazione dei comandi di autenticazione TACACS+ per ISE 2.0

## Sommario

---

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione di ISE per l'autenticazione e l'autorizzazione](#)

[Partecipa ad ISE 2.0 e ad Active Directory](#)

[Aggiungi dispositivo di rete](#)

[Abilita servizio di amministrazione dispositivi](#)

[Configura set di comandi TACACS](#)

[Configura profilo TACACS](#)

[Configura criterio di autorizzazione TACACS](#)

[Configurazione del router Cisco IOS per l'autenticazione e l'autorizzazione](#)

[Verifica](#)

[Verifica router Cisco IOS](#)

[Verifica ISE 2.0](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come configurare l'autenticazione TACACS+ e l'autorizzazione dei comandi in base all'appartenenza al gruppo di Microsoft Active Directory (AD).

## Premesse

Per configurare l'autenticazione TACACS+ e l'autorizzazione dei comandi in base all'appartenenza al gruppo Microsoft Active Directory (AD) di un utente con Identity Service Engine (ISE) 2.0 e versioni successive, ISE utilizza AD come archivio identità esterno per archiviare risorse quali utenti, computer, gruppi e attributi.

## Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Il router Cisco IOS® è pienamente operativo
- Connettività tra router e ISE.
- Il server ISE è stato avviato ed è connesso a Microsoft AD

## Componenti usati

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

- Cisco Identity Service Engine 2.0
- Software Cisco IOS® versione 15.4(3)M3
- Microsoft Windows Server 2012 R2

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.

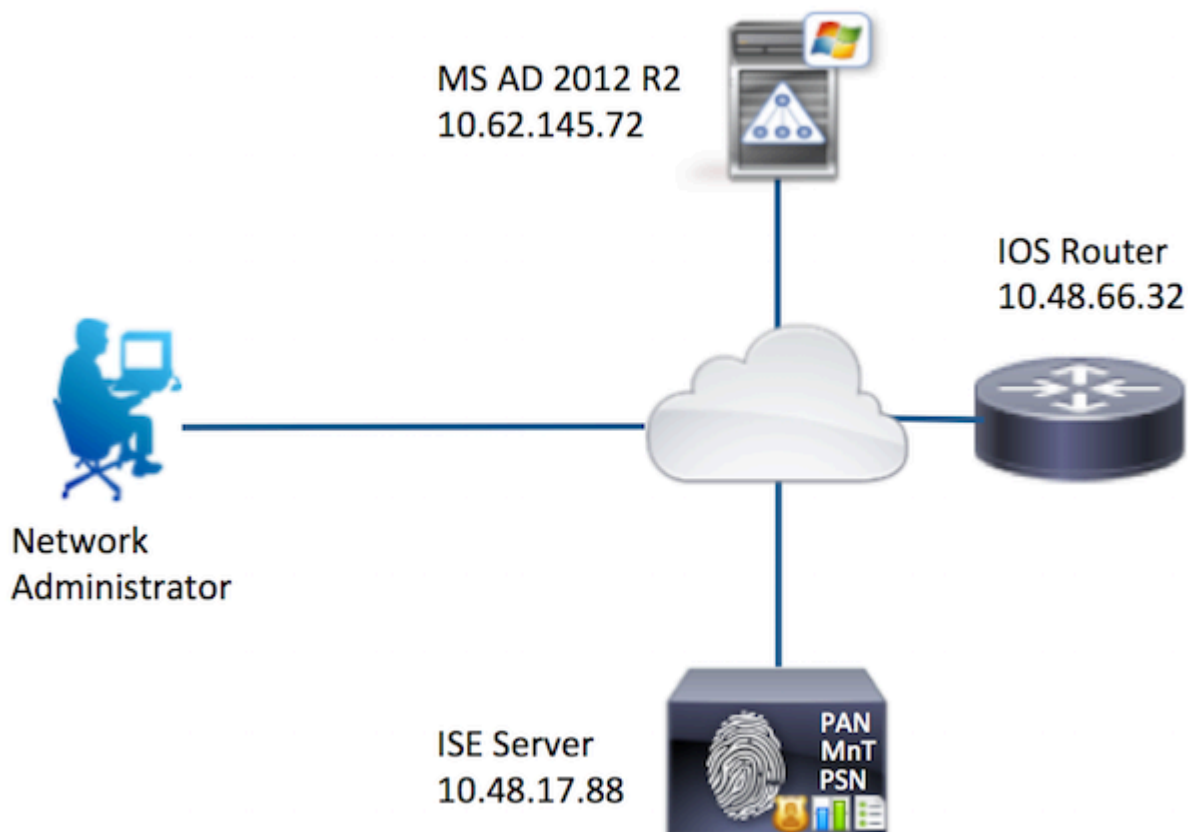
Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## Configurazione

La configurazione ha lo scopo di:

- Autentica utente telnet tramite AD
- Autorizzare l'utente telnet a passare in modalità di esecuzione privilegiata dopo l'accesso
- Controlla e invia ogni comando eseguito ad ISE per la verifica

## Esempio di rete



## Configurazioni

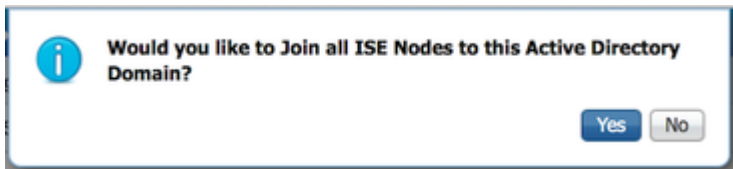
Configurazione di ISE per l'autenticazione e l'autorizzazione

Partecipa ad ISE 2.0 e ad Active Directory

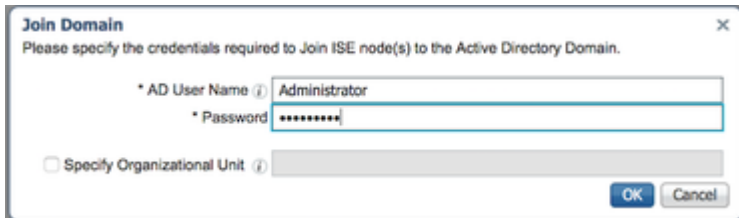
1. Passare a Amministrazione > Gestione delle identità > Archivi identità esterni > Active Directory > Aggiungi. Specificare il nome del punto di join, il dominio di Active Directory e fare clic su Invia.

The screenshot shows the ISE Administration console. The top navigation bar includes 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below this, a breadcrumb trail reads: 'sources > Device Portal Management > pxGrid Services > Feed Service > pxGrid Identity Mapping'. The main content area is titled 'Identity Source Sequences > Settings'. A 'Connection' tab is selected, and a form is displayed with the following fields: 'Join Point Name' (value: AD) and 'Active Directory Domain' (value: example.com). Both fields are highlighted with a red border. At the bottom of the form are 'Submit' and 'Cancel' buttons.

2. Quando viene richiesto di aggiungere tutti i nodi ISE a questo dominio Active Directory, fare clic su Sì.




3. Specificare il nome utente e la password di Active Directory, quindi fare clic su OK.



L'account AD richiesto per l'accesso al dominio in ISE può avere una delle seguenti caratteristiche:

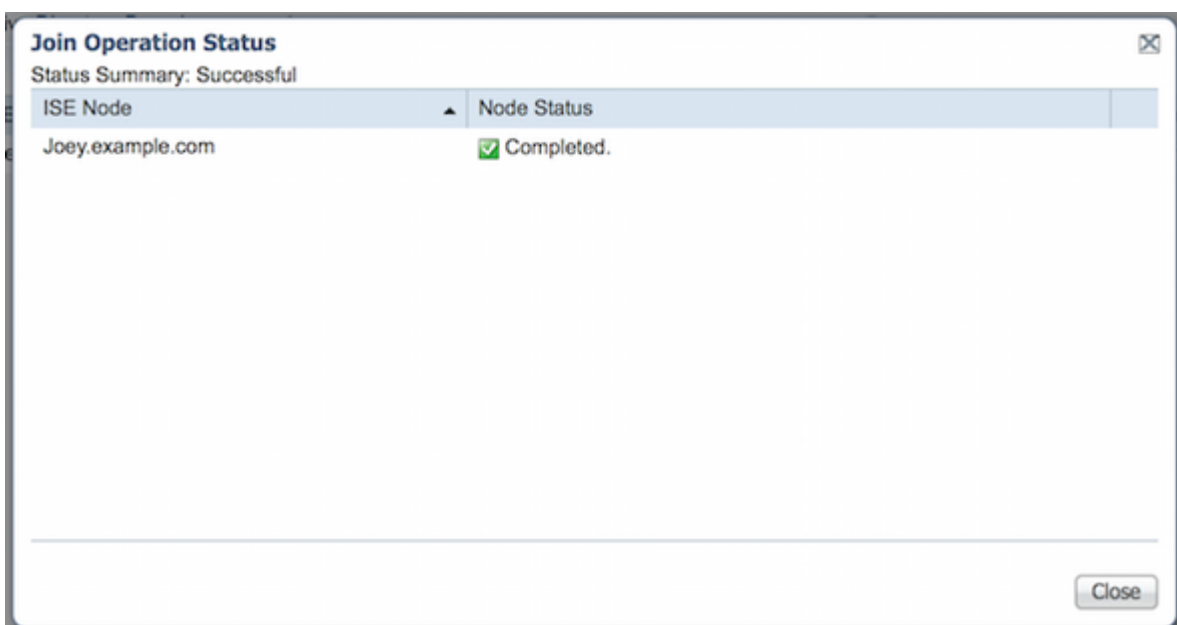
- Aggiunta di workstation al diritto utente del dominio nel rispettivo dominio
- Autorizzazione Creazione oggetti computer o Eliminazione oggetti computer nei rispettivi contenitori in cui viene creato l'account del computer ISE prima che il computer venga aggiunto al dominio

---

 **Nota:** Cisco consiglia di disabilitare il criterio di blocco per l'account ISE e configurare l'infrastruttura AD in modo che invii avvisi all'amministratore se per l'account viene utilizzata una password errata. Se viene immessa una password errata, ISE non crea né modifica il proprio account computer quando necessario e quindi probabilmente nega tutte le autenticazioni.

---

4. Esaminare lo stato dell'operazione. Lo stato del nodo deve essere impostato su Completato. Fare clic su Close (Chiudi).



5. Lo stato di AD è Operativo.

Operations   Policy   Guest Access   Administration   Work Centers

Resources   Device Portal Management   pxGrid Services   Feed Service   pxGrid Identity Source Sequences   Settings

---

Connection   Authentication Domains   Groups   Attributes

\* Join Point Name

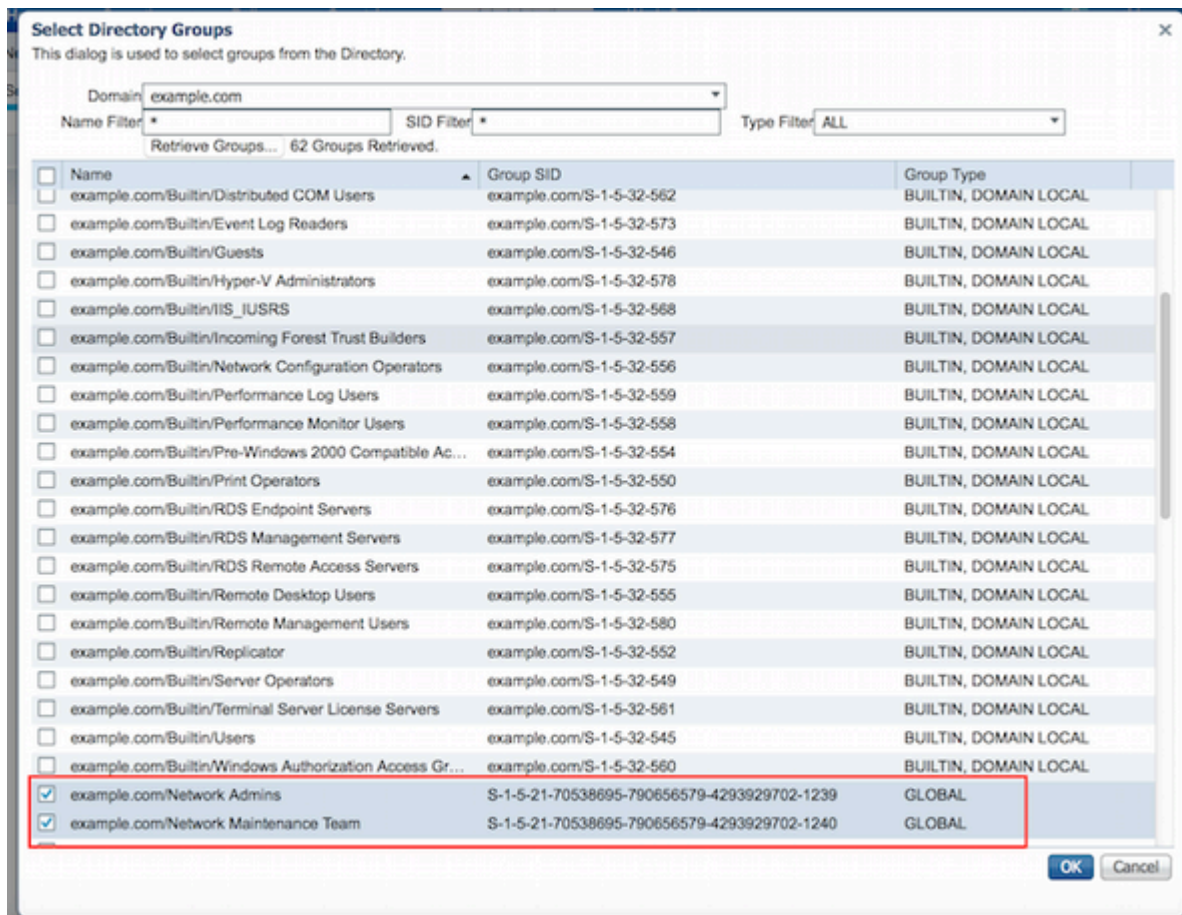
\* Active Directory Domain **example.com**

Join   Leave   Test User   Diagnostic Tool   Refresh Table

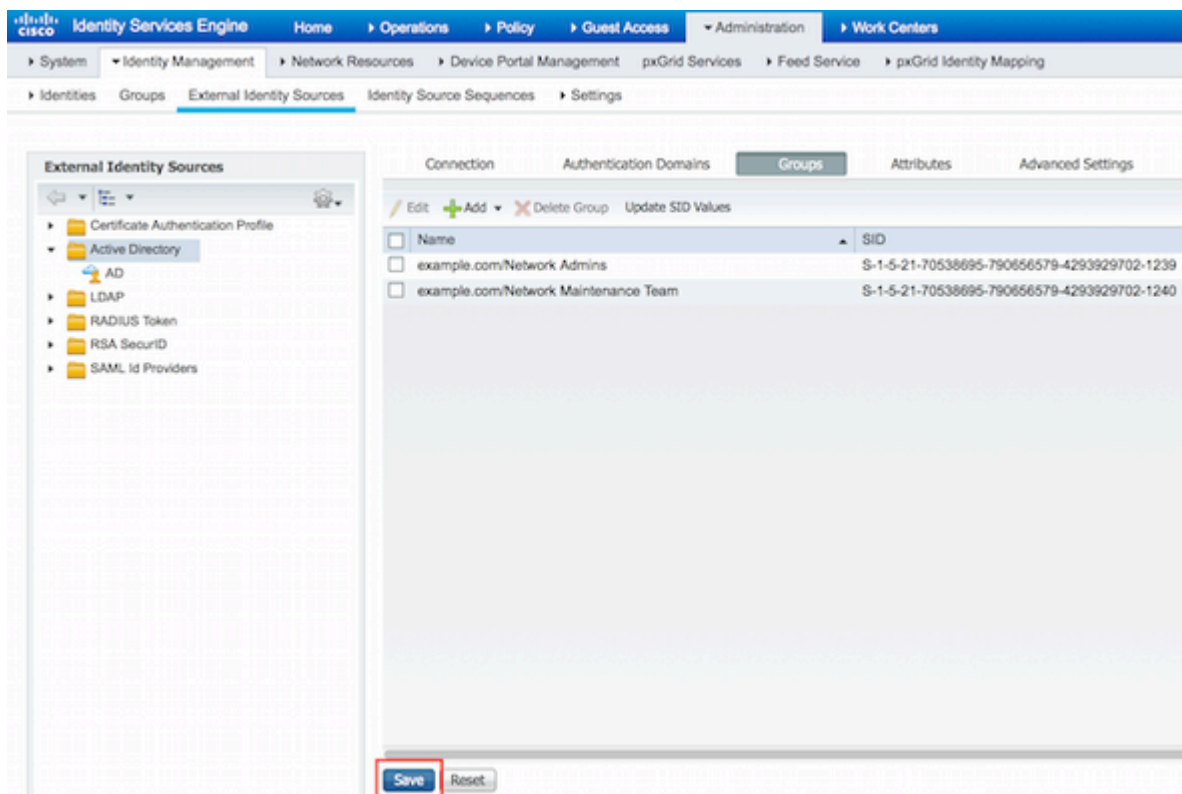
<input type="checkbox"/> ISE Node	ISE Node Role	Status
<input type="checkbox"/> Joey.example.com	STANDALONE	<input checked="" type="checkbox"/> Operational

6. Passare a Gruppi > Aggiungi > Seleziona gruppi da directory > Recupera gruppi. Selezionare le caselle di controllo Gruppo AD amministratori di rete e Gruppo AD team manutenzione di rete, come illustrato in questa immagine.

Nota: L'amministratore utente è membro del gruppo AD Amministratori di rete. L'utente dispone dei privilegi di accesso completo. L'utente è un membro del gruppo AD del team di manutenzione della rete. Questo utente è in grado di eseguire solo i comandi show.



7. Fare clic su Salva per salvare i gruppi AD recuperati.



Aggiungi dispositivo di rete

Passare a Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Dispositivi di rete. Fare clic su Add. Specificare il nome, l'indirizzo IP, selezionare la casella di controllo TACACS+ Authentication Settings (Impostazioni autenticazione TACACS+) e fornire la chiave segreta condivisa.

The screenshot displays the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is divided into several sections:

- Network Devices List > New Network Device**: The main heading.
- Network Devices**: A section containing the following fields:
  - Name**: A text input field with the value 'Router' (highlighted with a red box and labeled '1').
  - Description**: A text input field.
  - IP Address**: A text input field with the value '10.48.66.32 / 32' (highlighted with a red box and labeled '2').
  - Device Profile**: A dropdown menu with 'Cisco' selected.
  - Model Name**: A dropdown menu.
  - Software Version**: A dropdown menu.
  - Network Device Group**: A section with two dropdown menus: 'Location' (set to 'All Locations') and 'Device Type' (set to 'All Device Types').
- RADIUS Authentication Settings**: A section with a checkbox for 'TACACS+ Authentication Settings' (checked, highlighted with a red box and labeled '3').
- Shared Secret**: A text input field with masked characters '\*\*\*\*\*' and a 'Show' button.
- Enable Single Connect Mode**: A checkbox.

Abilita servizio di amministrazione dispositivi

Passare a Amministrazione > Sistema > Distribuzione. Scegliere il nodo richiesto. Selezionare la casella di controllo Abilita servizio di amministrazione del dispositivo e fare clic su Salva.



FQDN **Joey.example.com**  
 IP Address **10.48.17.88**  
 Node Type **Identity Services Engine (ISE)**

**Personas**

- ☒ Administration Role **STANDALONE** [Make Primary](#)
- ☒ Monitoring Role **PRIMARY** [Other Monitoring Node](#)
- ☒ Policy Service
  - ☒ Enable Session Services [i](#)  
Include Node in Node Group **None** [i](#)
  - ☒ Enable Profiling Service
  - ☐ Enable SXP Service
  - Use Interface **GigabitEthernet 0** [i](#)
  - 1** ☒ **Enable Device Admin Service** [i](#)
  - ☐ Enable Identity Mapping [i](#)
- ☐ pxGrid [i](#)

**2** [Save](#) [Reset](#)



Nota: Per TACACS è necessario avere licenze separate installate.

## Configura set di comandi TACACS

Sono configurati due set di comandi. First PermitAllCommands per l'amministratore utente che consente tutti i comandi sul dispositivo. Secondo PermitShowCommands per l'utente che consente solo comandi show.

1. Passare a Work Center > Device Administration > Policy Results > TACACS Command Sets. Fare clic su Add. Specificare il nome PermitAllCommands, selezionare la casella di controllo Permit any command non presente nell'elenco e fare clic su Submit (Invia).



Home ▶ Operations ▶ Policy ▶ Guest Access ▶ Administration ▶ Work Centers

Groups ▶ Network Resources ▶ Network Device Groups ▶ Policy Conditions ▶ Policy Results ▶ Policy Sets

TACACS Command Sets > New

**Command Set**

1 **Name \*** PermitAllCommands

Description

2 Permit any command that is not listed below ☒

+ Add Trash Edit Move Up Move Down

Grant	Command	Arguments
No data found.		

2. Passare a Work Center > Device Administration > Policy Results > TACACS Command Sets. Fare clic su Add. Fornire il nome PermitShowCommands, fare clic su Add e consentire i comandi show e exit. Se Argomenti viene lasciato vuoto per impostazione predefinita, verranno inclusi tutti gli argomenti. Fare clic su Invia.

Home ▶ Operations ▶ Policy ▶ Guest Access ▶ Administration ▶ Work Centers

Groups ▶ Network Resources ▶ Network Device Groups ▶ Policy Conditions ▶ Policy Results ▶ Policy Sets

TACACS Command Sets > New

**Command Set**

1 Name \* PermitShowCommands

Description

Permit any command that is not listed below ☐

0 Selected

2 + Add Trash Edit Move Up Move Down

Grant	Command	Arguments
<input type="checkbox"/>	PERMIT	show
<input type="checkbox"/>	PERMIT	exit

3

## Configura profilo TACACS

È configurato un singolo profilo TACACS. TACACS Profile è lo stesso concetto di Shell Profile su ACS. L'applicazione effettiva del comando viene eseguita tramite set di comandi. Selezionare Work Center > Device Administration > Policy Results > TACACS Profiles (Centri di lavoro > Amministrazione dispositivi > Risultati criteri > Profili TACACS). Fare clic su Add. Fornire il nome Profilo shell, selezionare la casella di controllo Privilegio predefinito e immettere il valore 15. Fare clic su Sottometti.

**TACACS Profile**

1 Name \* ShellProfile

Description

Task Attribute View Raw View

**Common Tasks**

2 ☒ Default Privilege 15 (Select 0 to 15)

☐ Maximum Privilege (Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape (Select true or false)

☐ Timeout

☐ Idle Time

## Configura criterio di autorizzazione TACACS

Per impostazione predefinita, il criterio di autenticazione punta a All\_User\_ID\_Stores, che include AD, pertanto non viene modificato.

Passare a Centri di lavoro > Amministrazione dispositivi > Set di criteri > Predefinito > Criteri di autorizzazione > Modifica > Inserisci nuova regola sopra.

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular ☒ Proxy Sequence ☐

**Authentication Policy**

**Authorization Policy**

**Exceptions (0)**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Tacacs_Default	If no matches, then	DenyAllCommands	

Sono configurate due regole di autorizzazione. La prima regola assegna il profilo TACACS ShellProfile e il comando Set PermitAllCommands in base all'appartenenza al gruppo AD degli amministratori di rete. La seconda regola assegna il profilo TACACS ShellProfile e il comando Set PermitShowCommands in base all'appartenenza al gruppo AD del team di manutenzione della rete.

Operations
Policy
Guest Access
Administration
Work Centers
0
License Warning

Network Resources
Network Device Groups
Policy Conditions
Policy Results
Policy Sets
Reports
Settings

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular
Proxy Sequence

Authentication Policy

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles	
<input checked="" type="checkbox"/>	PermitAllCommands	if AD:ExternalGroups EQUALS example.com/Network Admins	then PermitAllCommands AND ShellProfile		Edit   ▼
<input checked="" type="checkbox"/>	PermitShowCommands	if AD:ExternalGroups EQUALS example.com/Network Maintenance Team	then PermitShowCommands AND ShellProfile		Edit   ▼
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands		Edit   ▼

## Configurazione del router Cisco IOS per l'autenticazione e l'autorizzazione

Completare questa procedura per configurare il router Cisco IOS per l'autenticazione e l'autorizzazione.

1. Creare un utente locale con privilegi completi per il fallback utilizzando il comando username, come mostrato di seguito.

```
username cisco privilege 15 password cisco
```

2. Abilitare aaa new-model. Definire il server TACACS ISE e collocarlo nel gruppo ISE\_GROUP.

```
aaa new-model
```

```
tacacs server ISE
address ipv4 10.48.17.88
key cisco
aaa group server tacacs+ ISE_GROUP
server name ISE
```



Nota: La chiave del server corrisponde a quella definita in ISE Server precedente.

3. Verificare la raggiungibilità del server TACACS con il comando test aaa, come mostrato.

<#root>

Router#

```
test aaa group tacacs+ admin Krakow123 legacy
```

Attempting authentication test to server-group tacacs+ using tacacs+  
User was successfully authenticated.

L'output del comando precedente mostra che il server TACACS è raggiungibile e che l'utente è stato autenticato correttamente.

4. Configurare l'accesso e abilitare le autenticazioni, quindi utilizzare le autorizzazioni di esecuzione e di comando come mostrato.

```
aaa authentication login AAA group ISE_GROUP local  
aaa authentication enable default group ISE_GROUP enable  
aaa authorization exec AAA group ISE_GROUP local  
aaa authorization commands 0 AAA group ISE_GROUP local  
aaa authorization commands 1 AAA group ISE_GROUP local  
aaa authorization commands 15 AAA group ISE_GROUP local  
aaa authorization config-commands
```



Nota: L'elenco di metodi creato è denominato AAA, utilizzato in seguito, quando viene assegnato alla riga vty.

---

5. Assegnare gli elenchi dei metodi alla linea vty 0 4.

```
line vty 0 4  
authorization commands 0 AAA  
authorization commands 1 AAA  
authorization commands 15 AAA  
authorization exec AAA  
login authentication AAA
```

## Verifica

Verifica router Cisco IOS

1. Collegare in modalità Telnet il router Cisco IOS come amministratore che appartiene al gruppo di accesso completo in Active Directory. Il gruppo Network Admins è il gruppo in Active Directory mappato a ShellProfile e al comando PermitAllCommands impostato su ISE. Provare a eseguire qualsiasi comando per garantire l'accesso completo.

<#root>

Username:

admin

Password:

Router#

conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

crypto isakmp policy 10

Router(config-isakmp)#

encryption aes

Router(config-isakmp)#

exit

Router(config)#

exit

Router#

2. Collegare in modalità Telnet il router Cisco IOS come utente che appartiene al gruppo di accesso limitato in Active Directory. Il gruppo Team di manutenzione di rete è il gruppo in Active Directory mappato al comando ShellProfile e PermitShowCommands impostato sull'ISE. Provare a eseguire un comando qualsiasi per assicurarsi che sia possibile eseguire solo i comandi show.

<#root>

Username:

user

Password:

Router#

show ip interface brief | exclude unassigned

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.48.66.32	YES	NVRAM	up	up

Router#

ping 8.8.8.8

Command authorization failed.

Router#

```
configure terminal
```

Command authorization failed.

Router#

```
show running-config | include hostname
```

```
hostname Router
```

Router#

## Verifica ISE 2.0

1. Passare a Operazioni > TACACS Livelog. Accertarsi che i tentativi effettuati siano visibili.

Cisco

Identity Services Engine

Home

Operations

Policy

Guest Access

Administration

Work Centers

RADIUS Livelog

TACACS Livelog

Reports

Troubleshoot

Adaptive Network Control

Add or Remove Columns

Refresh

Refresh

Eve

Generated Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy
2015-08-18 14:28:12.011	<div></div>	<div></div>	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:28:05.11	<div></div>	<div></div>	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:55.408	<div></div>	<div></div>	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:53.013	<div></div>	<div></div>	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:47.387	<div></div>	<div></div>	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:41.034	<div></div>	<div></div>	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:40.415	<div></div>	<div></div>	user	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:24:43.715	<div></div>	<div></div>	admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:24:40.834	<div></div>	<div></div>	admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:24:40.213	<div></div>	<div></div>	admin	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:20:42.923	<div></div>	<div></div>	admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:20:42.762	<div></div>	<div></div>	admin	Authentication	Tacacs_Default >> Default >> Default	

2. Fare clic sui dettagli di uno dei rapporti rossi. Il comando non riuscito eseguito in precedenza può essere visualizzato.



## Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

## Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

## Risoluzione dei problemi

Errore: Il comando 13025 non corrisponde a una regola di autorizzazione

Controllare gli attributi SelectedCommandSet per verificare che i set di comandi previsti siano stati selezionati dal criterio di autorizzazione.

## Informazioni correlate

[Documentazione e supporto tecnico – Cisco Systems](#)

[Note sulla release di ISE 2.0](#)

[Guida all'installazione dell'hardware ISE 2.0](#)

[Guida all'aggiornamento a ISE 2.0](#)

[Guida allo strumento di migrazione da ACS ad ISE](#)

[Guida all'integrazione di ISE 2.0 Active Directory](#)

[Guida per l'amministratore di ISE 2.0 Engine](#)

### 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).