ISE 2.0: Esempio di configurazione dell'autenticazione e dell'autorizzazione dei comandi TACACS+ ASA CLI

Sommario

Introduzione

In questo documento viene descritto come configurare l'autenticazione TACACS+ e l'autorizzazione dei comandi su Cisco Adaptive Security Appliance (ASA) con Identity Service Engine (ISE) 2.0 e versioni successive. ISE utilizza un archivio identità locale per archiviare risorse come utenti, gruppi ed endpoint.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Il firewall ASA è completamente operativo

- Connettività tra ASA e ISE
- Il server ISE è stato avviato

Componenti usati

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

- Cisco Identity Service Engine 2.0
- Software Cisco ASA release 9.5(1)

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.

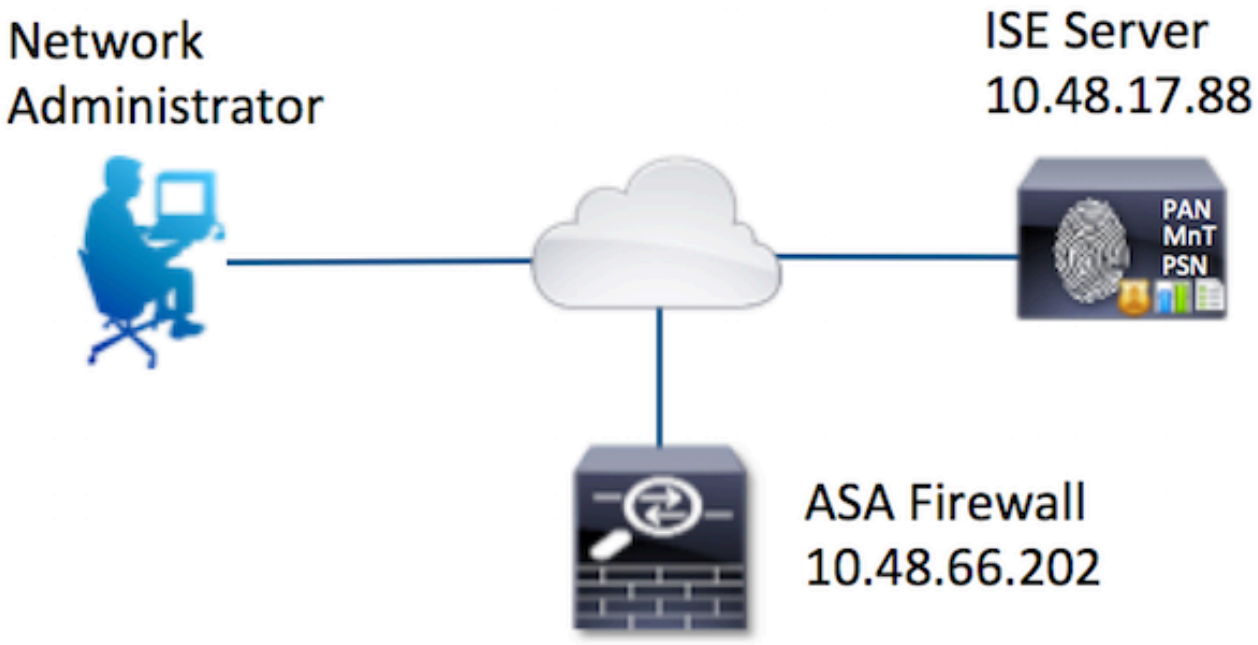
Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

La configurazione ha lo scopo di:

- Autenticazione utente ssh tramite archivio identità interno
- Autorizzare l'utente ssh a passare in modalità di esecuzione privilegiata dopo l'accesso
- Verifica e invia ogni comando eseguito ad ISE

Esempio di rete



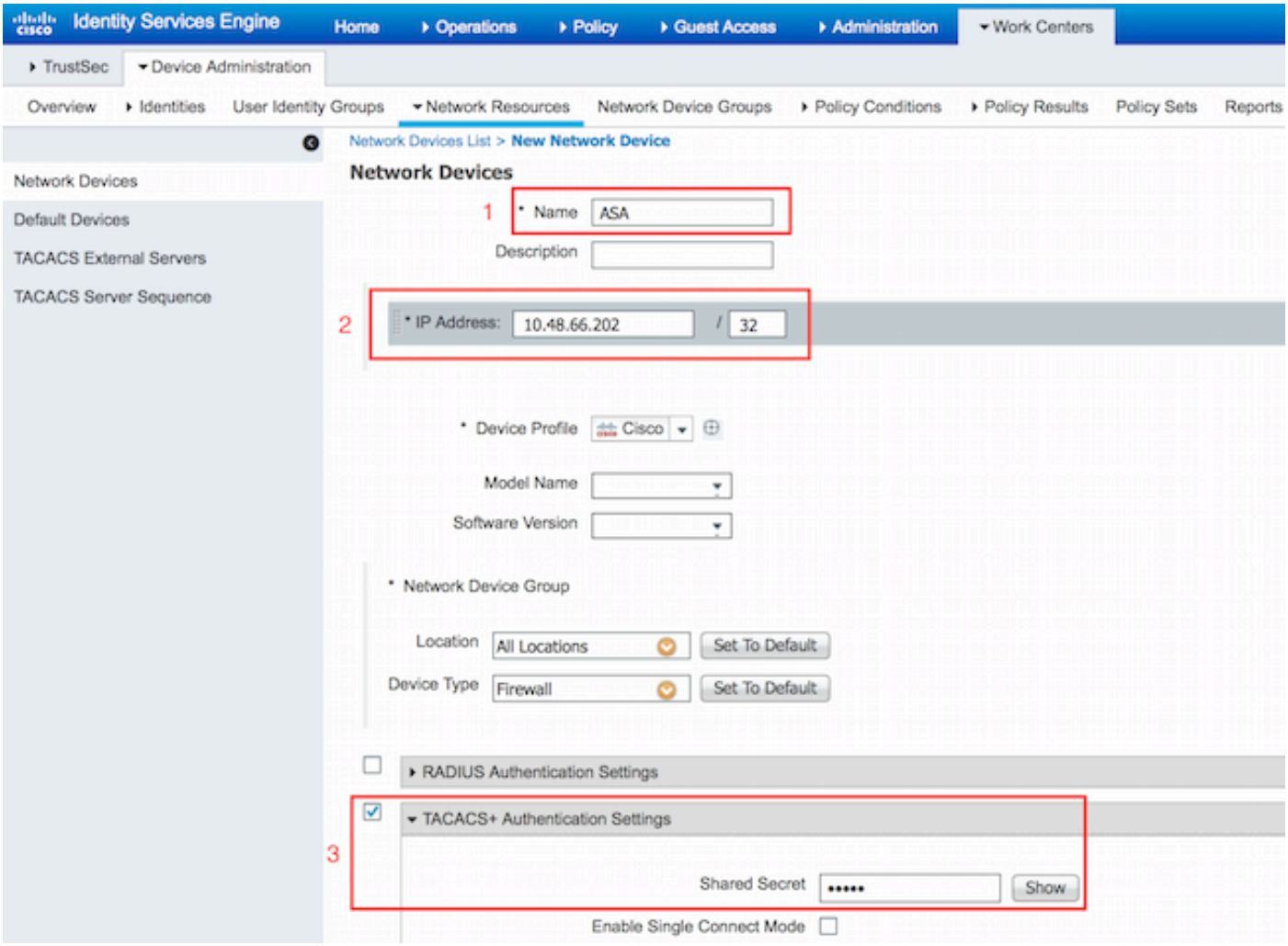
Configurazioni

Configurazione di ISE per l'autenticazione e l'autorizzazione

Vengono creati due utenti. User **administrator** fa parte del gruppo di identità locale **Network Admins** su ISE. L'utente dispone di privilegi CLI completi. L'utente **user** fa parte del **Network Maintenance Team** local Identity Group on ISE. Questo utente può solo visualizzare i comandi e il ping.

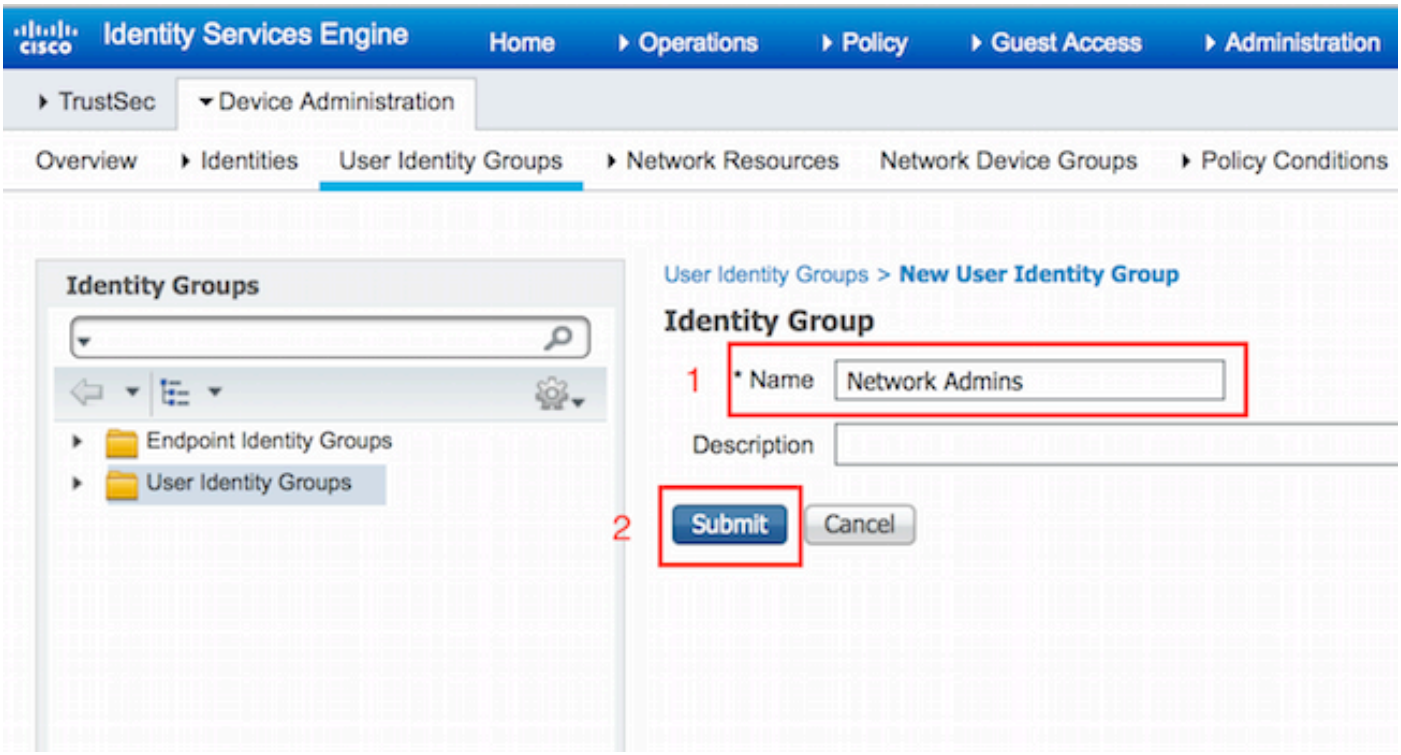
Aggiungi dispositivo di rete

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 e fornire la chiave **Shared Secret**. Facoltativamente, è possibile specificare il tipo/percorso del dispositivo.



Configurazione dei gruppi di identità utente

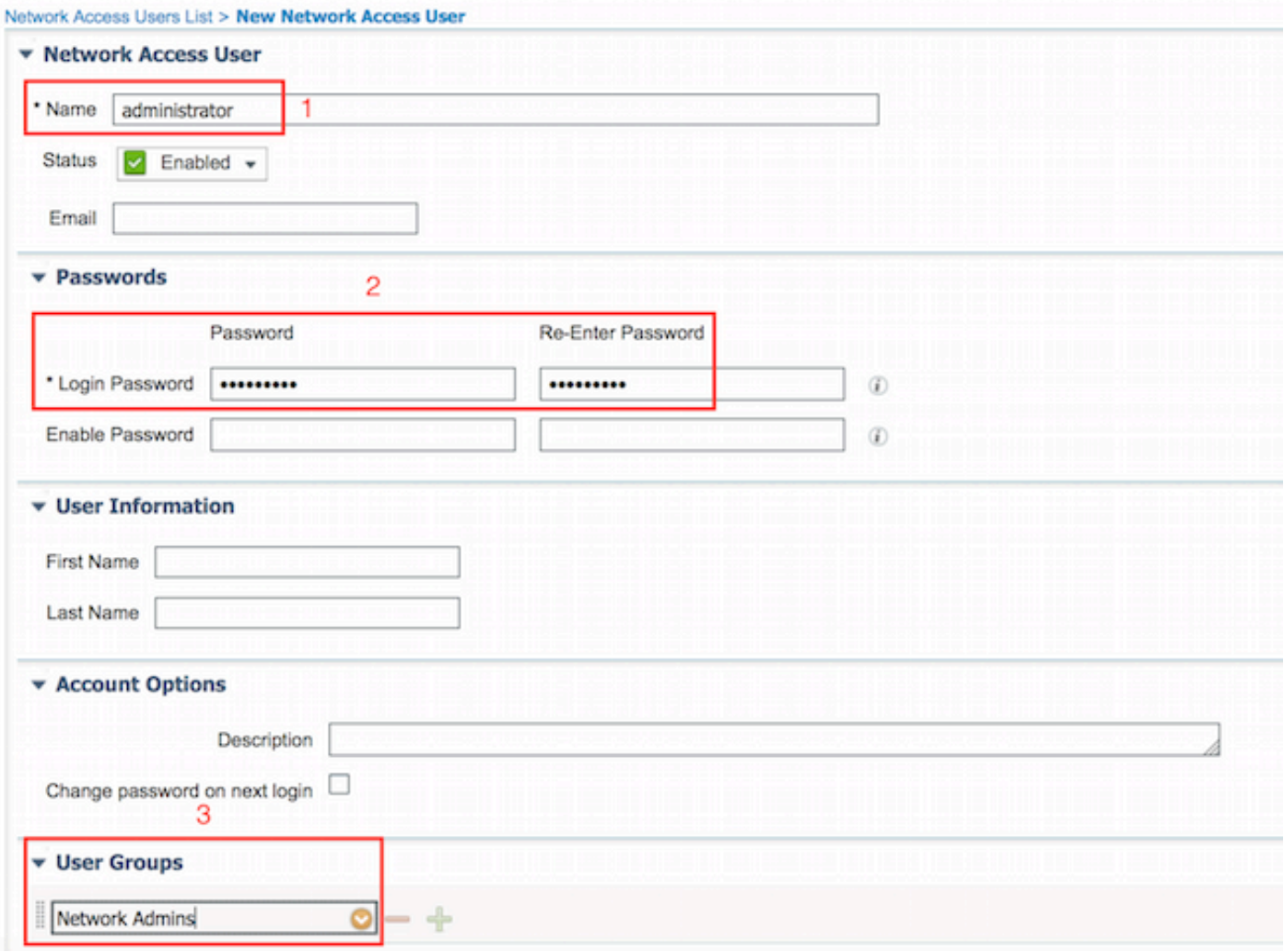
Passare a **Centri di lavoro > Amministrazione dispositivi > Gruppi di identità utente.** Fare clic su **Add.** Specificare il nome e fare clic su **Invia.**



Ripetere lo stesso passaggio per configurare il gruppo di identità utente del **team di manutenzione della rete**.

Configurazione degli utenti

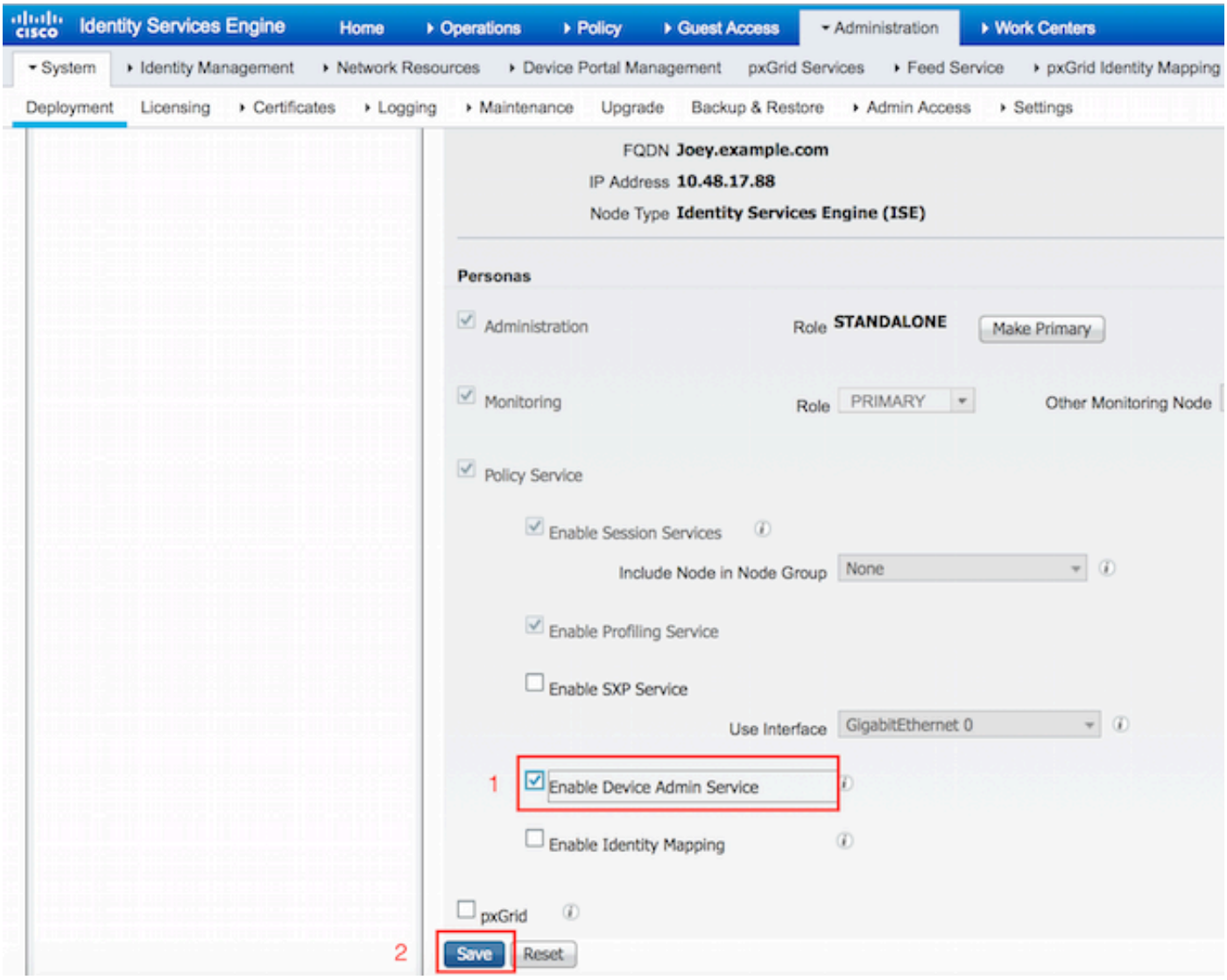
Passare a **Centri di lavoro > Amministrazione dispositivi > Identità > Utenti.** Fare clic su **Add.** Specificare il nome e la password di accesso, quindi fare clic su **Invia**.



Ripetere i passaggi per configurare l'**utente** e assegnare il gruppo di identità utente del **team di manutenzione della rete**.

Abilita servizio di amministrazione dispositivi

Selezionare **Amministrazione > Sistema > Distribuzione.** Selezionare il nodo richiesto. Selezionare la casella di controllo **Enable Device Admin Service** (Abilita servizio di amministrazione dispositivi) e fare clic su **Save (Salva).**

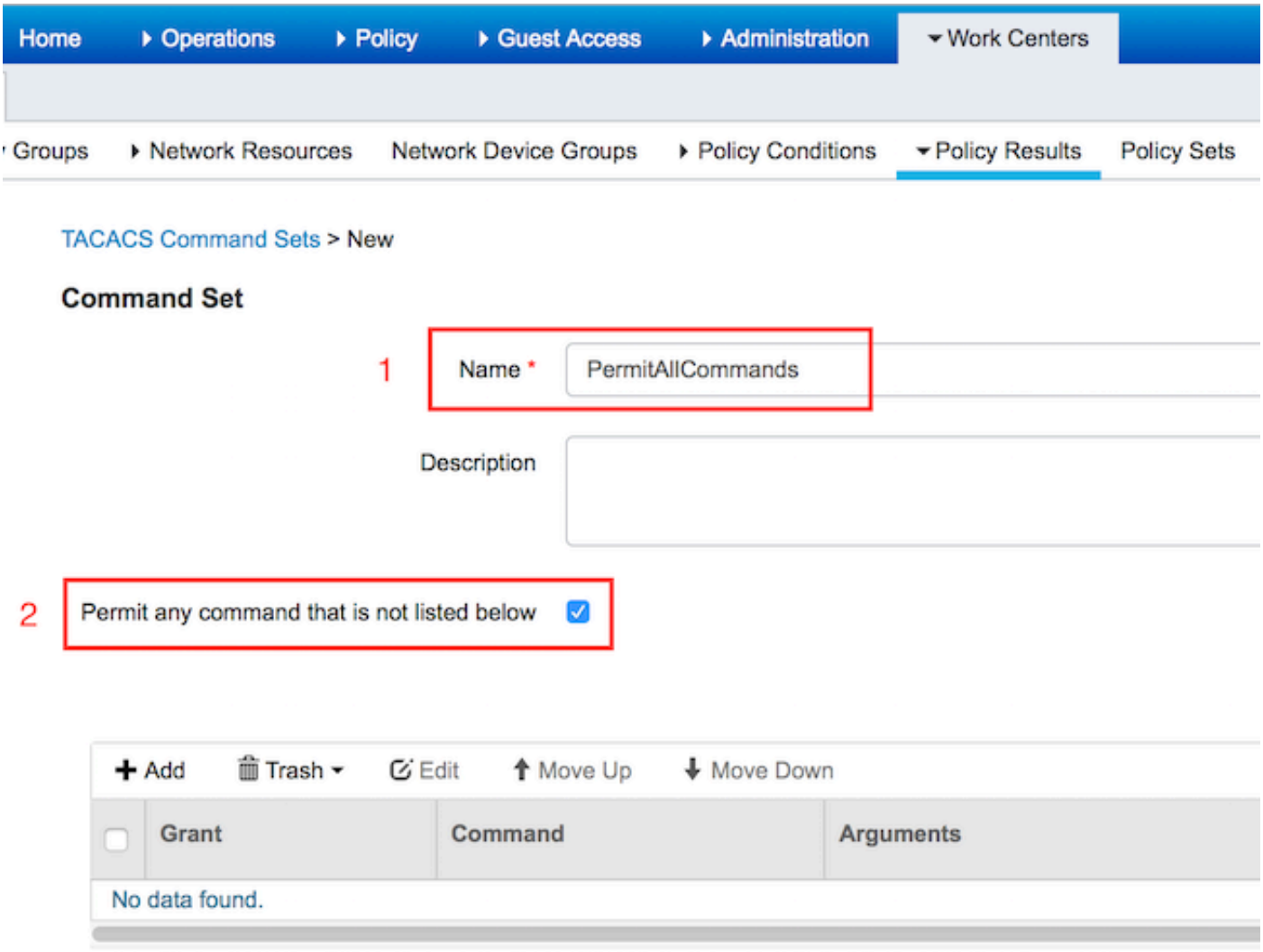


Nota: Per TACACS è necessario avere una licenza separata installata.

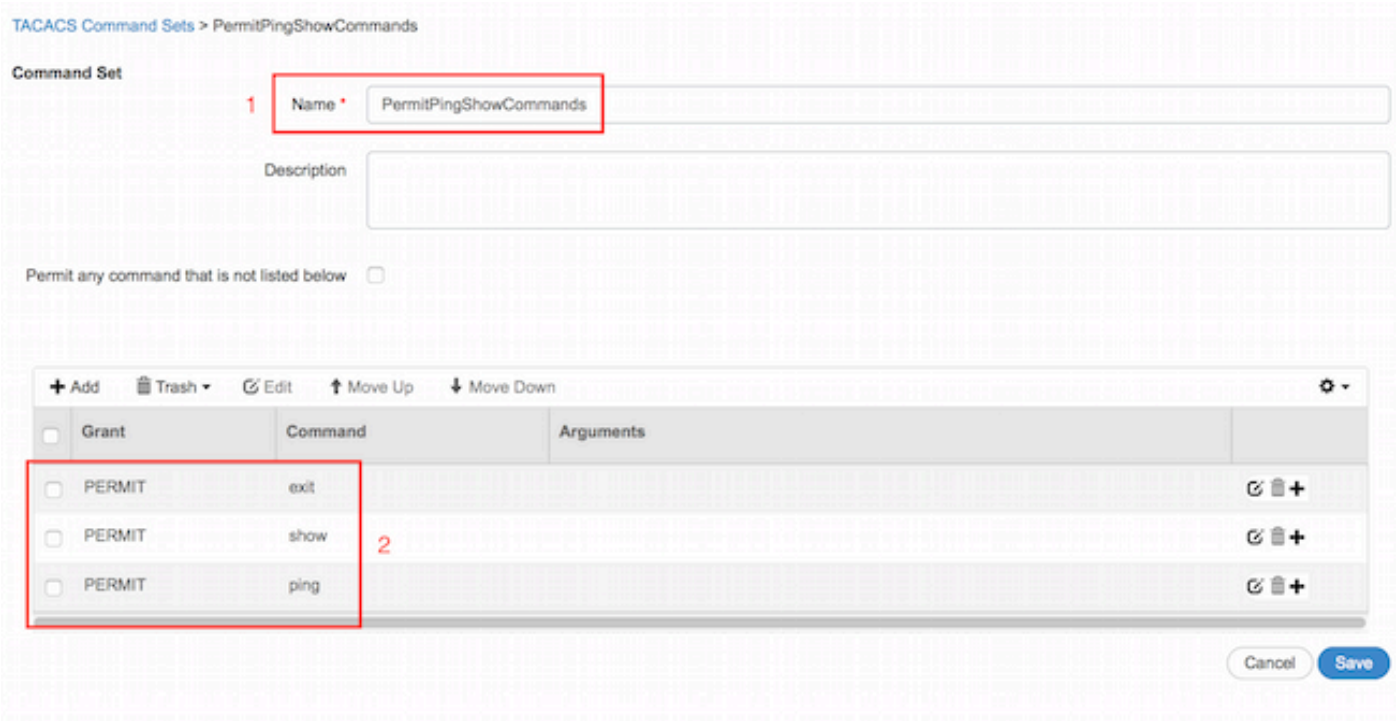
Configurazione dei set di comandi TACACS

Sono configurati due set di comandi. Innanzitutto, **PermitAllCommands** per l'utente **amministratore** che consente tutti i comandi sul dispositivo. Secondo **PermitPingShowCommands** per l'**utente** che consente solo i comandi show e ping.

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 that is not list below** e fare clic su **Submit.**

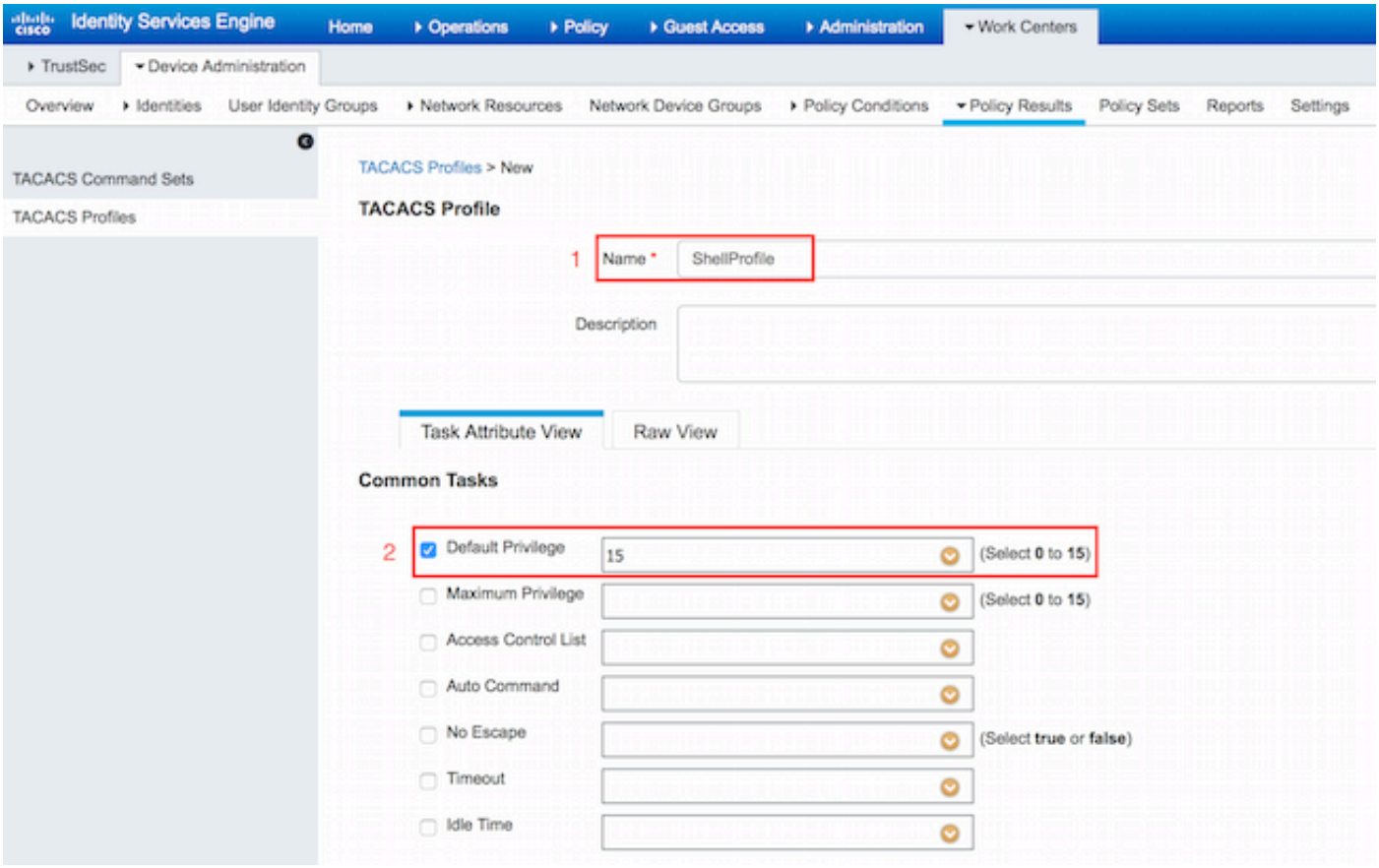


2. Passare a **Work Center > Device Administration > Policy Results > TACACS Command Sets.** Fare clic su **Add.** Fornire il nome **PermitPingShowCommands,** fare clic su **Add** e consentire **i comandi show, ping** e **exit**. Per impostazione predefinita, se gli argomenti vengono lasciati vuoti, vengono inclusi tutti gli argomenti. Fare clic su **Invia.**



Configurazione del profilo TACACS

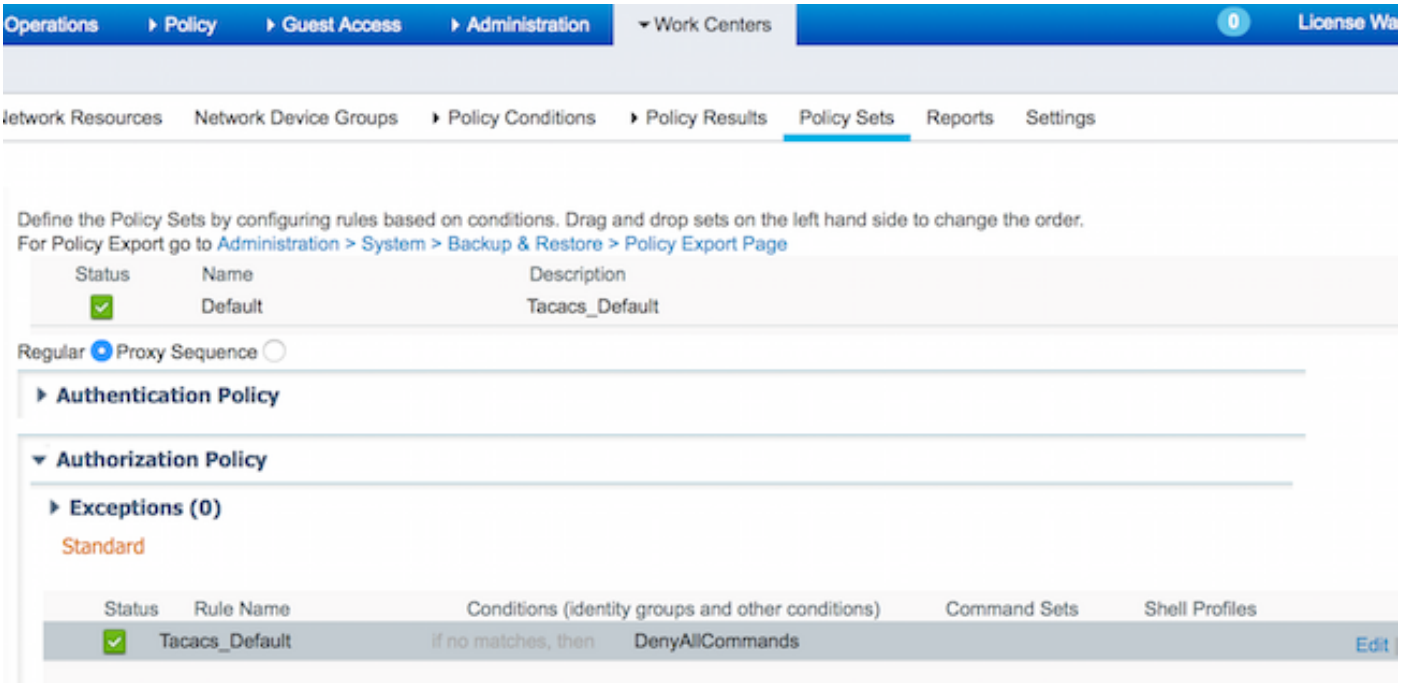
Verrà configurato un singolo profilo TACACS. L'applicazione effettiva del comando verrà eseguita tramite set di comandi. Selezionare **Work Center > Device Administration > Policy Results > TACACS Profiles.** Fare clic su **Add.** Fornire il nome **ShellProfile,** selezionare la casella di controllo **Privilegio predefinito** e immettere il valore 15. Fare clic su **Sottometti**.



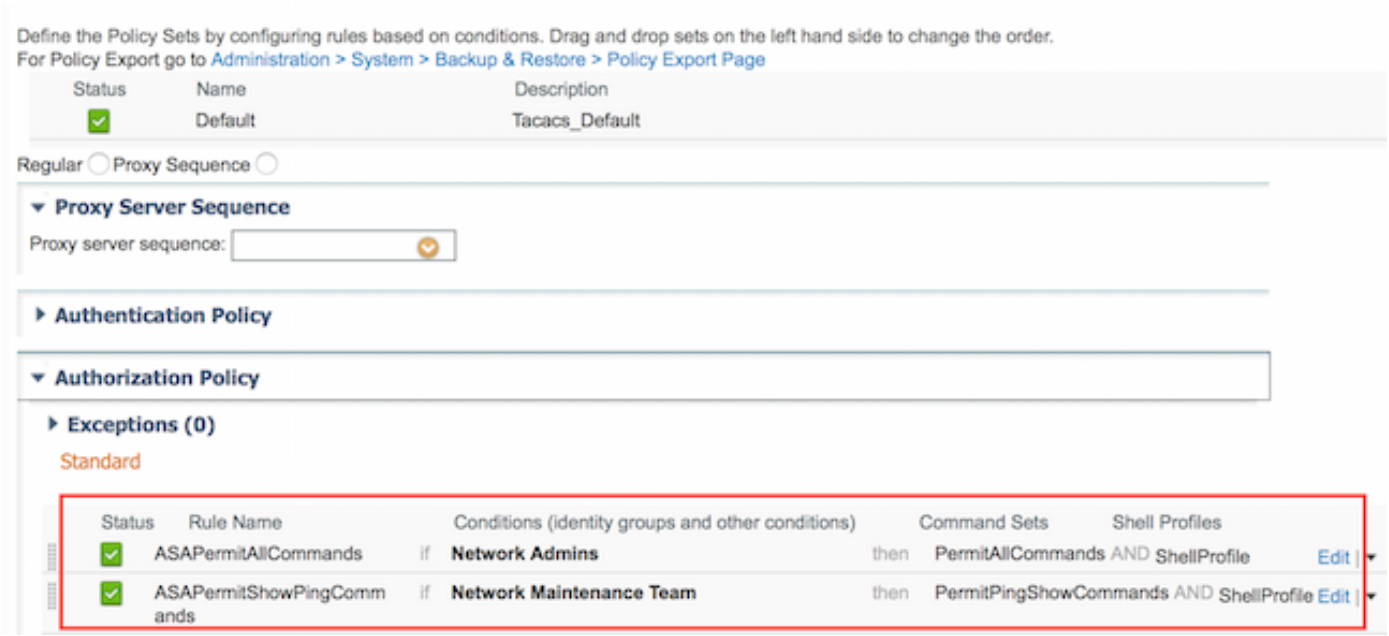
Configurazione del criterio di autorizzazione TACACS

Per impostazione predefinita, il criterio di autenticazione punta a All_User_ID_Stores, che include anche l'archivio locale, pertanto non viene modificato.

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



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 di identità utente **Network Admins**. La seconda regola assegna il profilo TACACS **ShellProfile** e il comando Set **PermitPingShowCommands** in base all'appartenenza al gruppo di identità utente del **team di manutenzione della rete**.



Configurazione di Cisco ASA Firewall per l'autenticazione e l'autorizzazione

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

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. Definire il server TACACS ISE, specificare l'interfaccia, l'indirizzo IP del protocollo e la chiave TACACS.

```
aaa-server ISE protocol tacacs+
aaa-server ISE (mgmt) host 10.48.17.88
 key cisco
```

Nota: La chiave del server deve corrispondere a quella definita in precedenza su ISE Server.

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

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

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

4. Configurare l'autenticazione per le autorizzazioni ssh, exec e dei comandi come mostrato di seguito. Se si esegue l'abilitazione automatica dell'autenticazione del server di autorizzazione aaa, l'utente viene posto automaticamente in modalità di esecuzione privilegiata.

```
aaa authentication ssh console ISE
aaa authorization command ISE
aaa authorization exec authentication-server auto-enable
```

Nota: Con i comandi sopra descritti, l'autenticazione viene effettuata su ISE, l'utente viene posto direttamente in modalità privilegiata e viene eseguita l'autorizzazione del comando.

5. Consentire shh sull'interfaccia di gestione.

```
ssh 0.0.0.0 0.0.0.0 mgmt
```

Verifica

Verifica firewall Cisco ASA

1. Eseguire il servizio Ssh sul firewall ASA come amministratore che appartiene al gruppo di identità degli utenti con accesso completo. Il gruppo Network Admins è mappato al comando ShellProfile e PermitAllCommands impostato sull'ISE. Provare a eseguire qualsiasi comando per garantire l'accesso completo.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
```

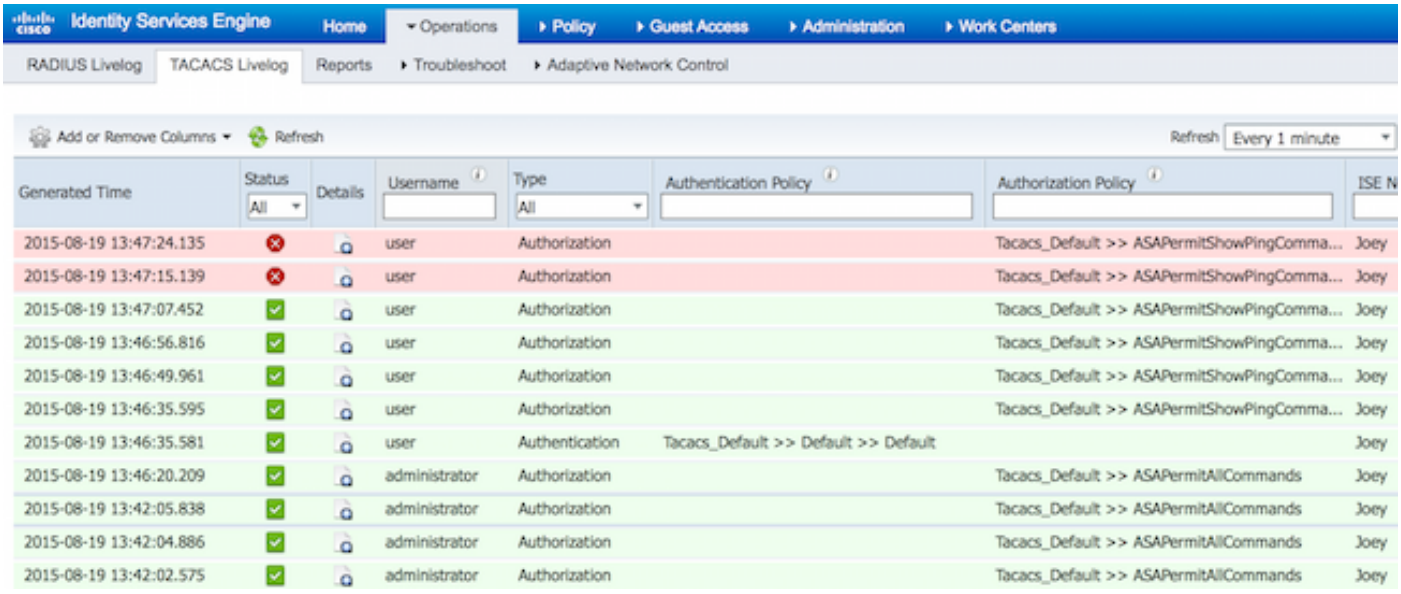
```
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

2. Eseguire il Ssh al firewall ASA come **utente** che appartiene al gruppo di identità degli utenti con accesso limitato. Il gruppo **Network Maintenance** è mappato al comando **ShellProfile** e **PermitPingShowCommands** impostato sull'ISE. Provare a eseguire un comando qualsiasi per assicurarsi che sia possibile eseguire solo i comandi show e ping.

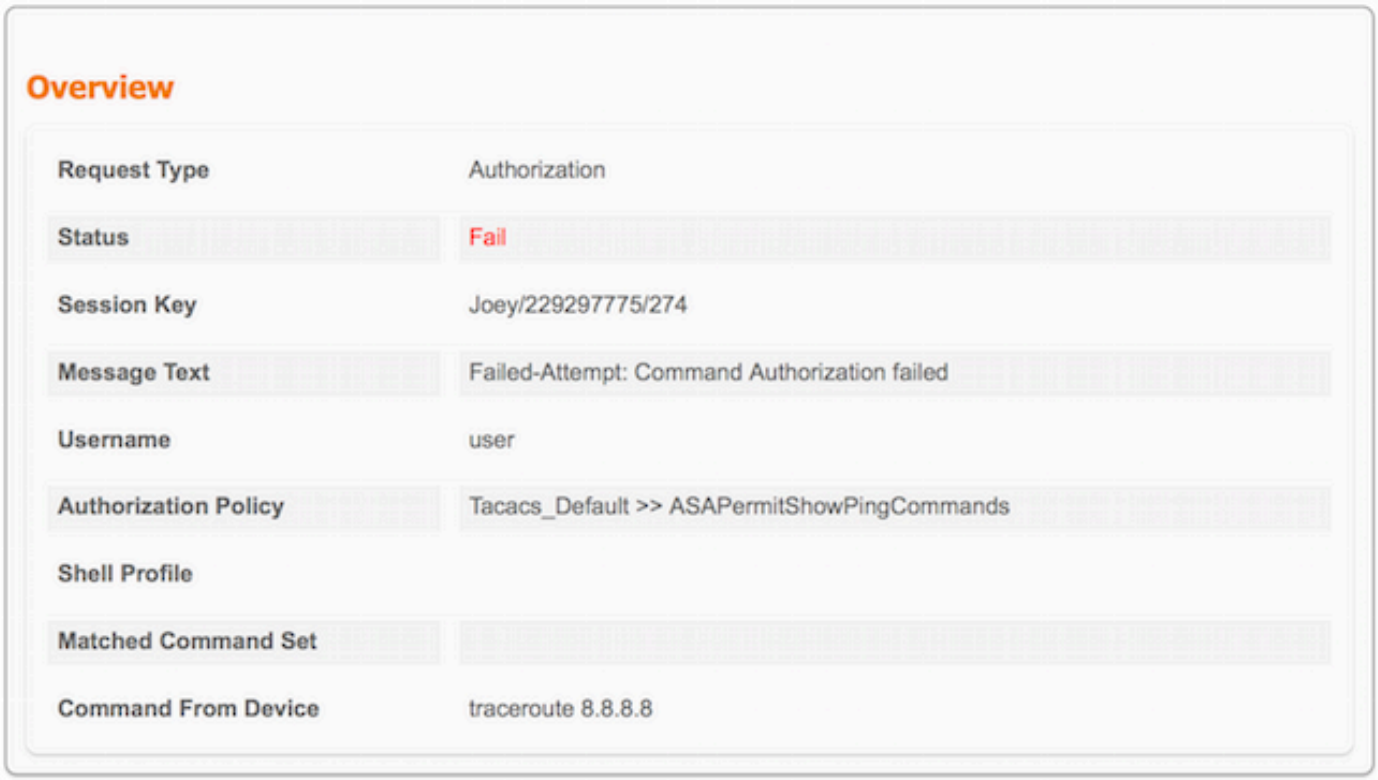
```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

Verifica ISE 2.0

1. Passare a **Operazioni > TACACS Livelog.** Accertarsi che i tentativi eseguiti in precedenza siano visibili.



2. Fare clic sui dettagli di uno dei report rossi. È possibile visualizzare il comando non riuscito eseguito in precedenza.



Risoluzione dei problemi

Errore: Tentativo non riuscito: Autorizzazione del comando non riuscita

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