Configurazione dell'accesso TACACS+ temporizzato per i dispositivi di rete con ISE

Sommario

Introduzione

In questo documento viene descritto come configurare l'autorizzazione basata su ora e data per il criterio Device Admin in Cisco Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza del protocollo Tacacs e della configurazione di Identity Services Engine (ISE).

Componenti usati

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

- Switch Cisco Catalyst 9300 con software Cisco IOS® XE 17.12.5 e versioni successive

- Cisco ISE versione 3.3 e successive

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

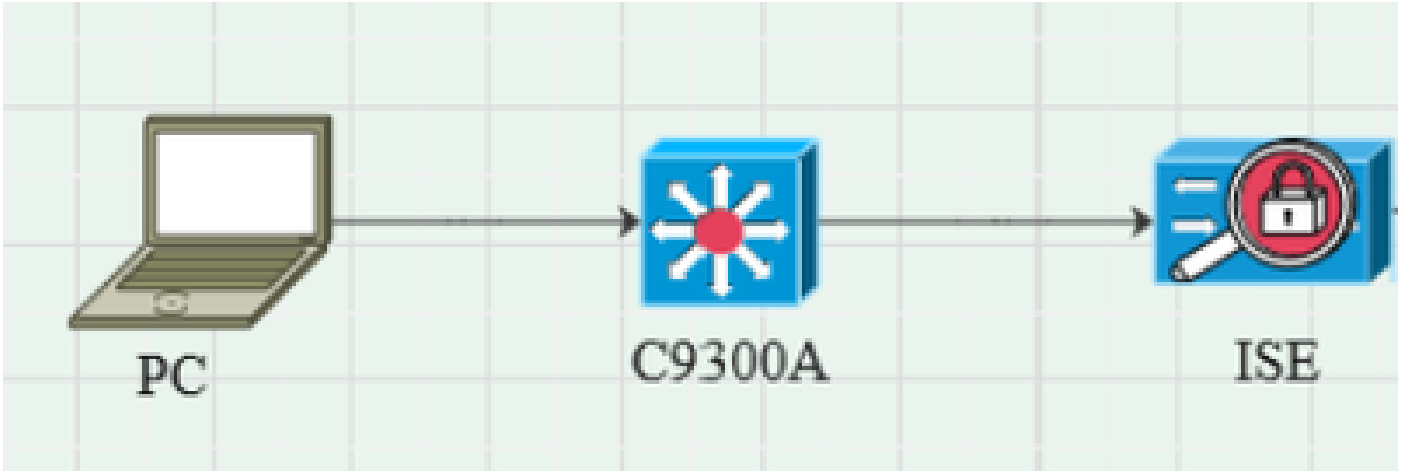
I criteri di autorizzazione sono un componente chiave di Cisco Identity Services Engine (ISE) e consentono di definire regole e configurare profili di autorizzazione per utenti o gruppi specifici che accedono alle risorse di rete. Questi criteri valutano le condizioni per determinare quale profilo applicare. Quando le condizioni di una regola sono soddisfatte, viene restituito il profilo di autorizzazione corrispondente, che consente l'accesso alla rete appropriato.

Cisco ISE supporta anche le condizioni di ora e data, che consentono di applicare le policy solo in determinati orari o giorni. Ciò è particolarmente utile per applicare controlli di accesso basati su requisiti aziendali temporizzati.

Questo documento descrive la configurazione per consentire l'accesso amministrativo TACACS+ ai dispositivi di rete solo durante l'orario di lavoro (dal lunedì al venerdì, 08:00-17:00) e per negare l'accesso al di fuori di questo intervallo di tempo.

Configurazione

Esempio di rete



Configurare ISE

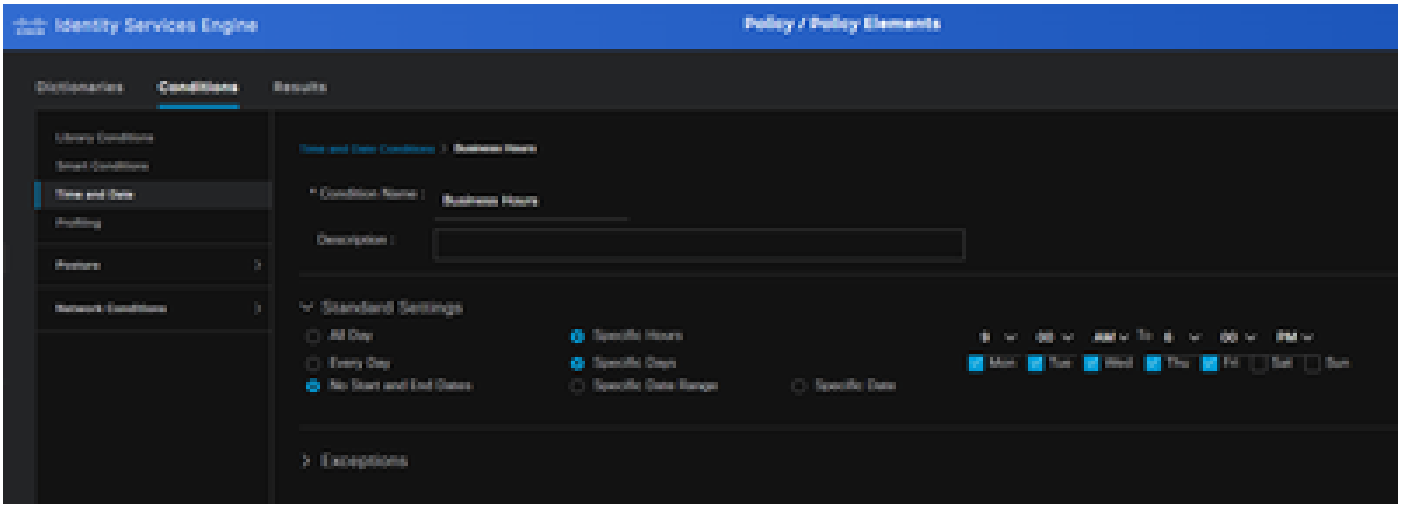
Passaggio 1: Crea condizione data e ora

Passare a Criterio > Elementi criterio > Condizioni > Ora e data, quindi fare clic su Aggiungi.

Nome condizione: Orario di ufficio

Imposta l'intervallo di tempo Impostazioni standard > Ore specifiche : 09:00 AM - 06:00 PM

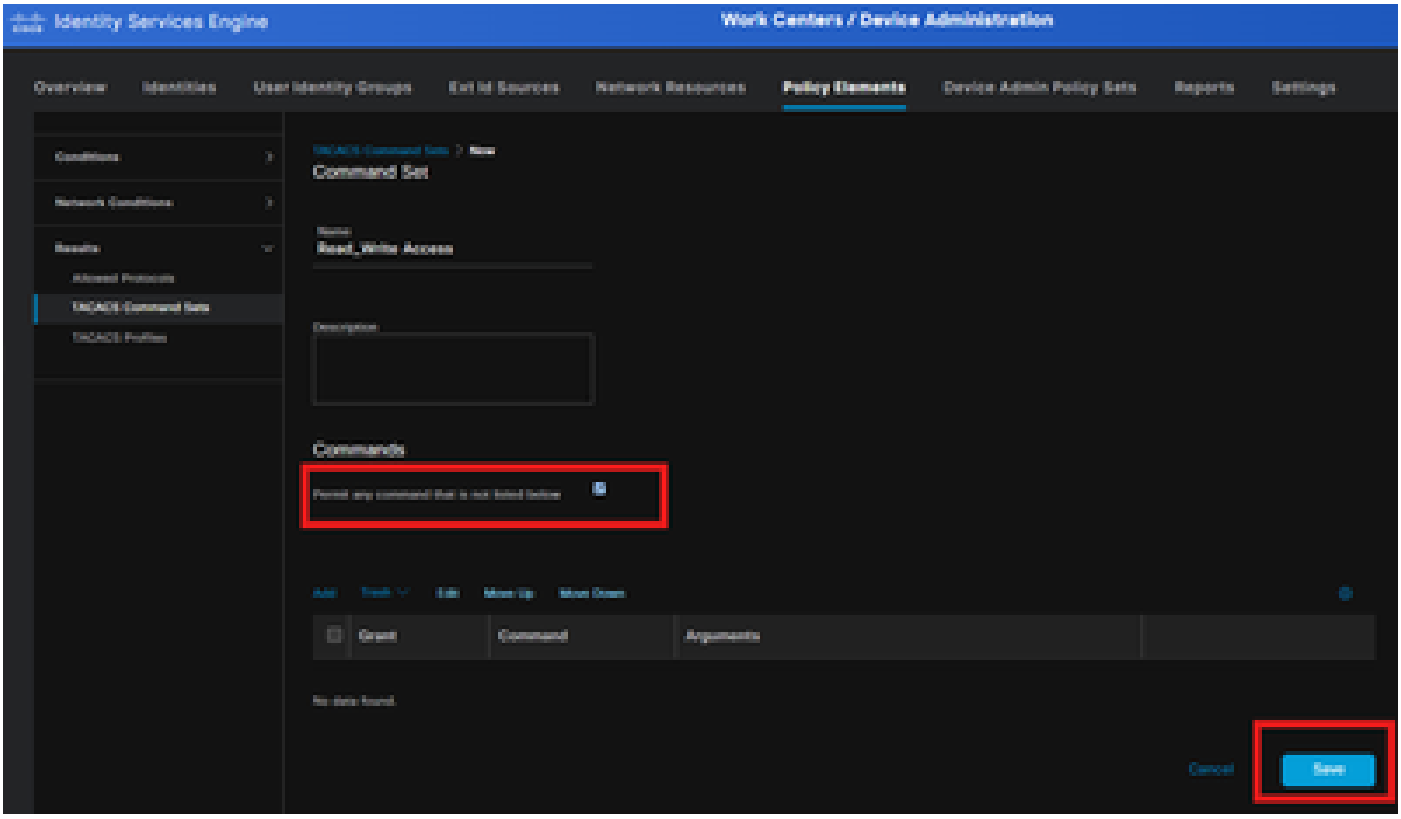
Giorni specifici: Da lunedì a venerdì



Passaggio 2: Creare un set di comandi TACACS+

Passare a Centri di lavoro > Amministrazione dispositivi > Elementi criteri > Risultati > Set di comandi TACACS.

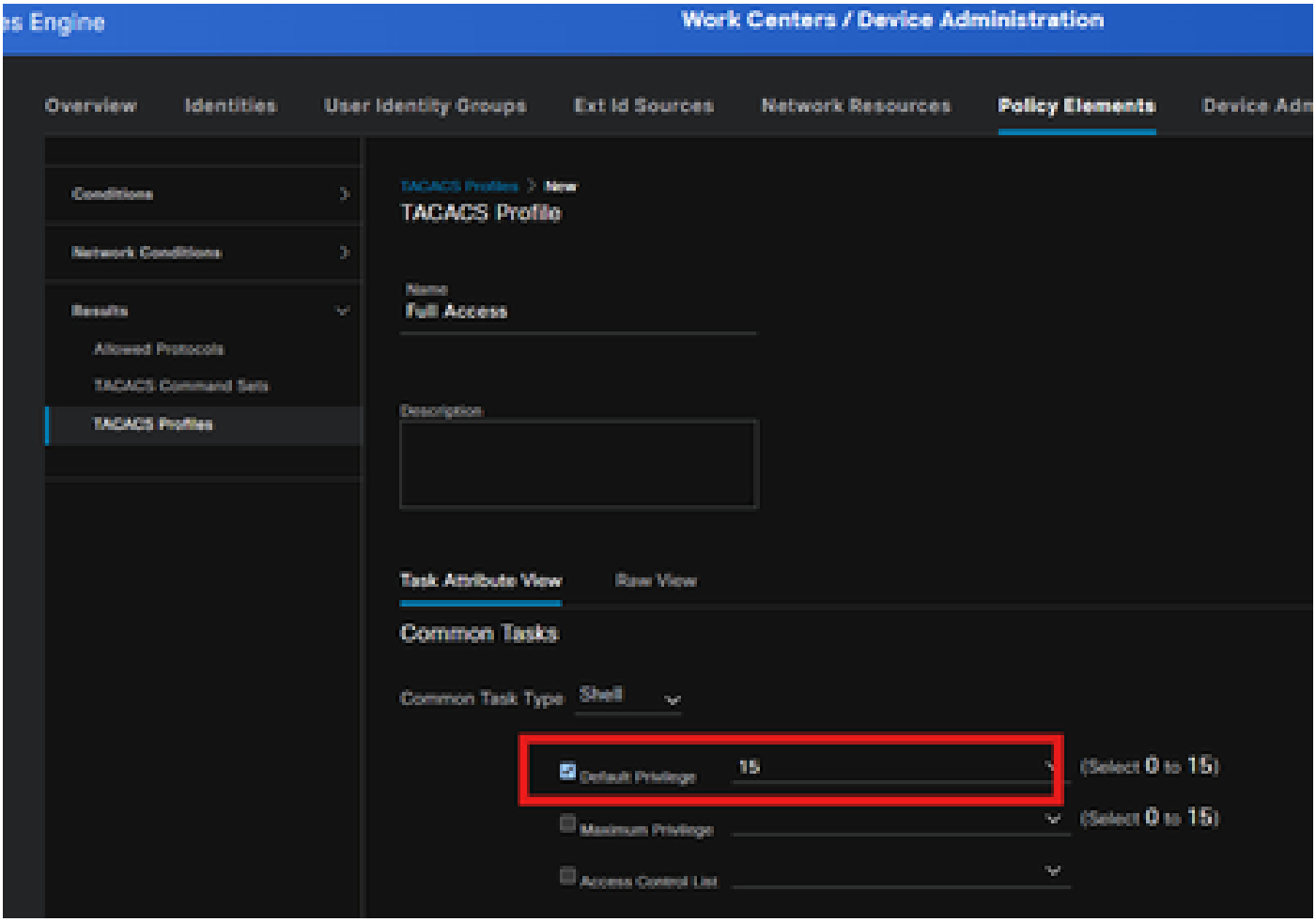
Creare un set di comandi selezionando la casella di controllo Consenti comandi non elencati di seguito e facendo clic su Invia o aggiungendo i Comandi limitati se si desidera limitare alcuni comandi CLI.



Passaggio 3: Crea un profilo TACACS+

Selezionare Centri di lavoro > Amministrazione dispositivi > Elementi della policy > Risultati > Profili TACACS. Fare clic su Add.

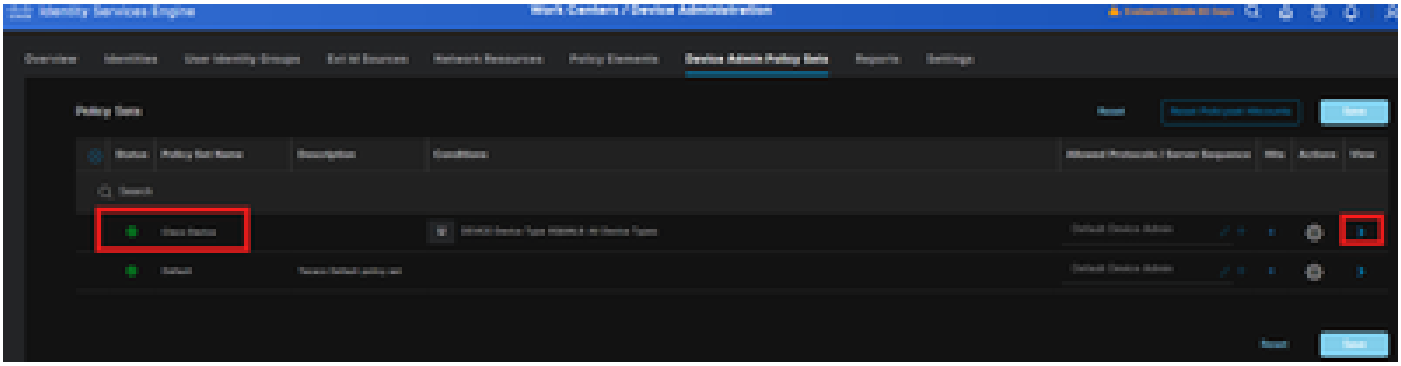
Selezionare Tipo task comando come shell, quindi casella di controllo Privilegio predefinito e immettere il valore 15. Fare clic su Invia.



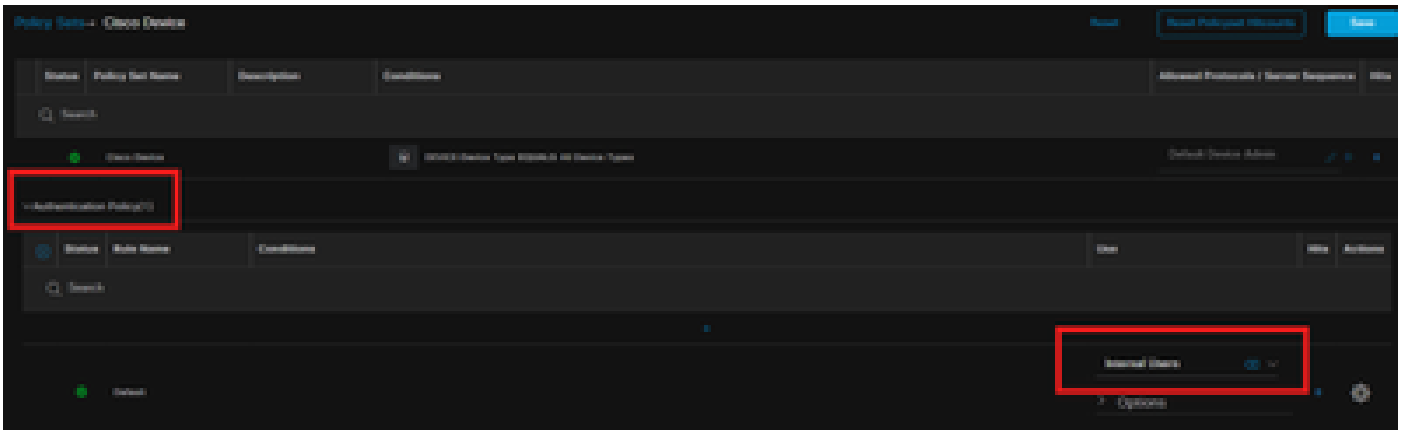
Passaggio 4: Crea criterio di autorizzazione TACACS

Passare a Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi.

Selezionare il set di criteri attivo.



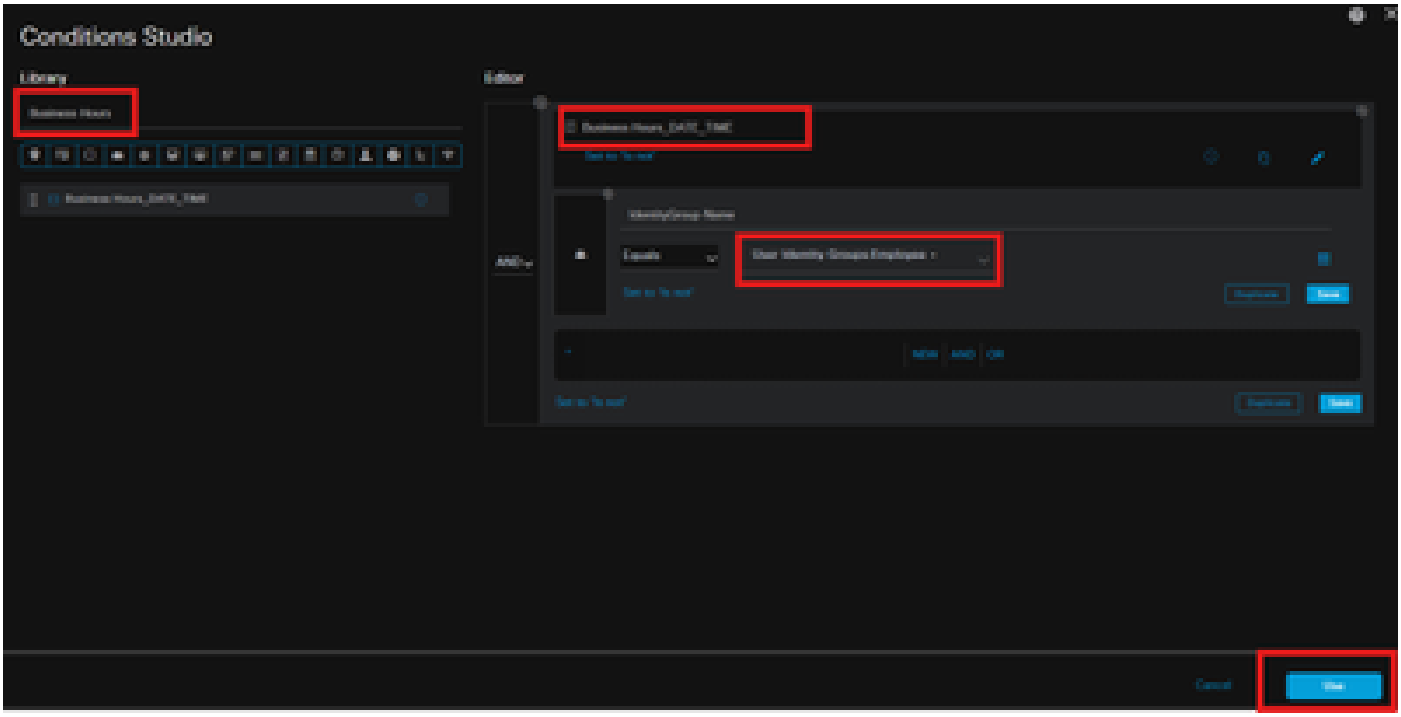
Configurare il criterio di autenticazione in base agli utenti interni o di Active Directory.



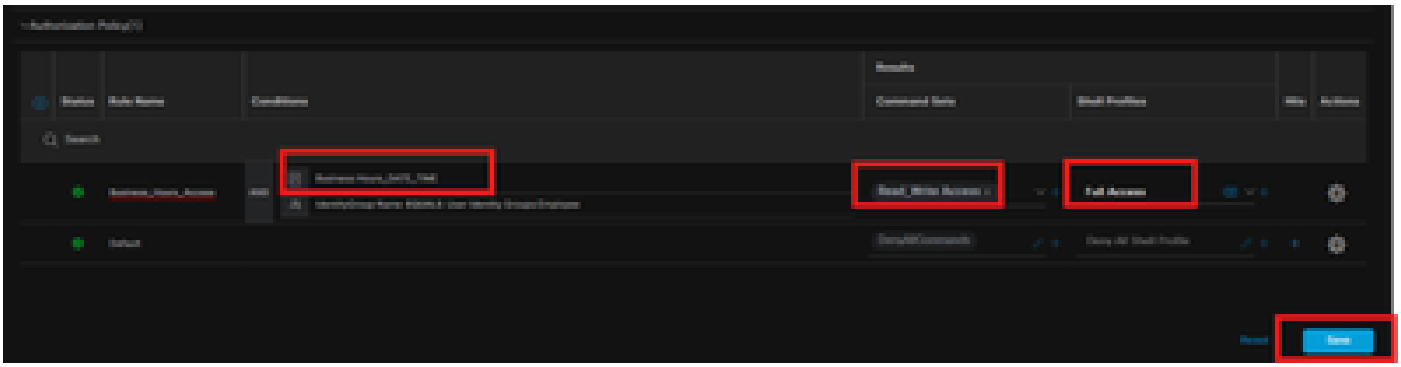
Nella sezione Criteri di autorizzazione fare clic su Aggiungi regola per specificare il nome della regola e quindi fare clic su + per aggiungere le condizioni di autorizzazione.

Viene visualizzata una nuova finestra di Condition Studio. Nel campo Cerca per nome immettere il nome creato nel passaggio 1 e trascinarlo nell'editor.

Aggiungere ulteriori condizioni in base al gruppo di utenti e fare clic su Salva.



In Risultati, selezionare il set di comandi TACACS e il profilo di shell creati al passaggio 2 e al passaggio 3, quindi fare clic su Salva.



Configura switch

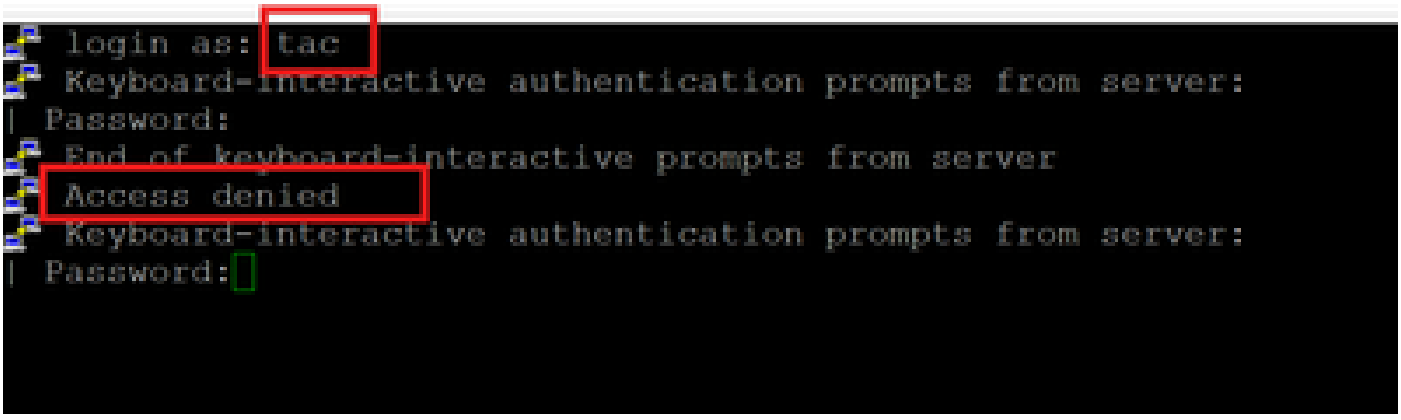
aaa new-model

tacacs+ gruppo locale predefinito per l'accesso con autenticazione aaa
autenticazione aaa abilitazione impostazione predefinita abilitazione gruppo tacacs+
comandi config di autorizzazione aaa
acs+ gruppo locale predefinito esecuzione autorizzazione aaa
comandi autorizzazione aaa 0 gruppo locale predefinito tacacs+
comandi di autorizzazione aaa 1 gruppo locale predefinito tacacs+
comandi di autorizzazione aaa 15 tacacs+ gruppo locale predefinito

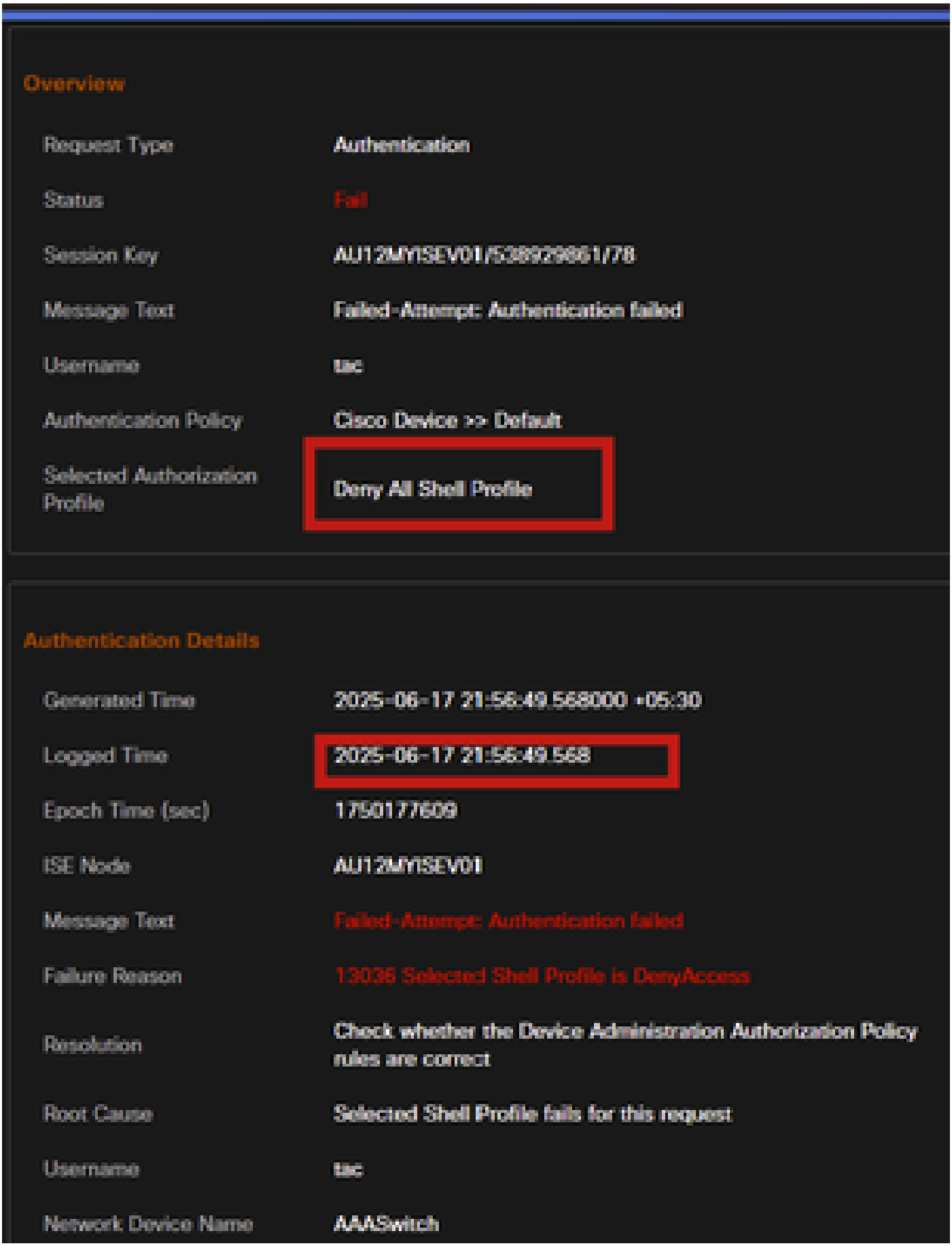
tacacs server ISE
indirizzo ipv4 10.127.197.53
QWERTY123

Verifica

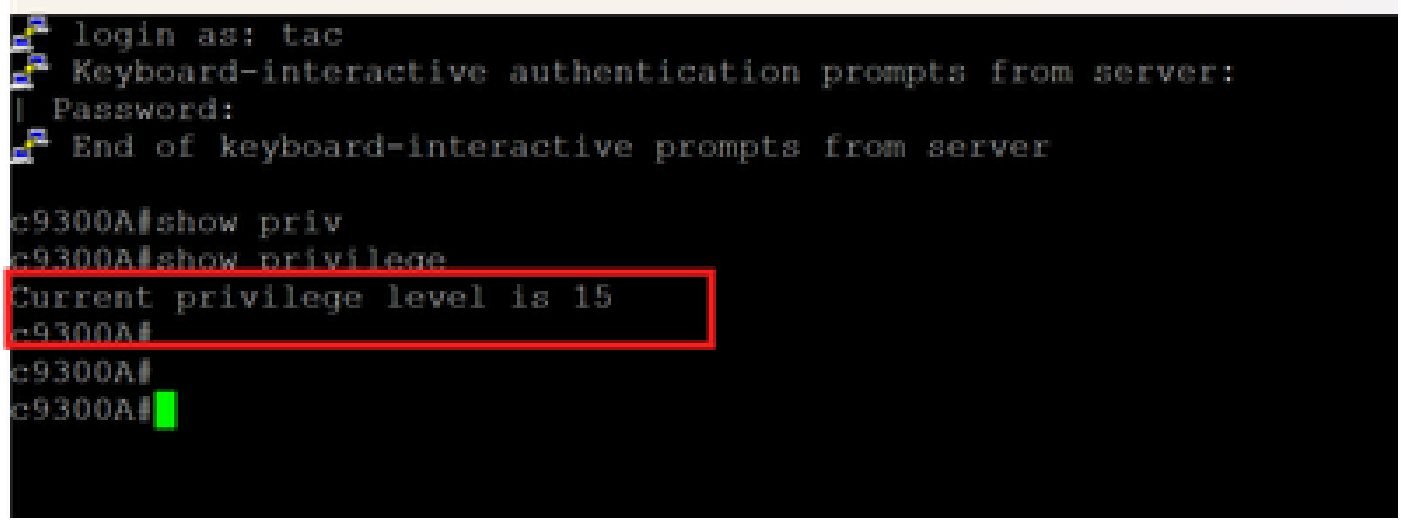
L'utente che sta tentando di usare il protocollo SSH sullo switch fuori dall'orario di lavoro ha ricevuto da ISE il rifiuto di accesso.



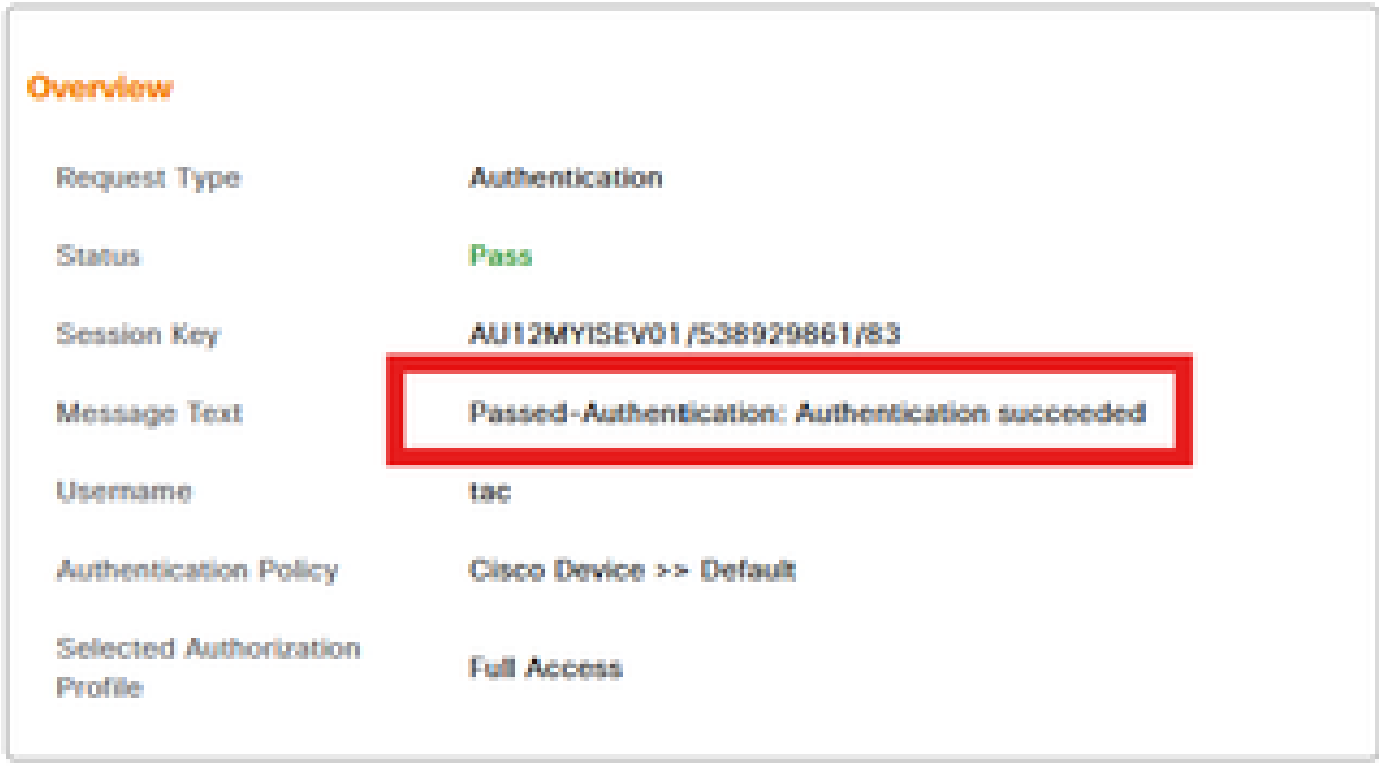
I log di ISE Live indicano che l'autorizzazione non è riuscita perché la condizione di data e ora nei criteri di autorizzazione non corrispondeva. Di conseguenza, la sessione ha raggiunto la regola di accesso negato predefinita.



L'utente sta tentando di usare il protocollo SSH nello switch durante l'orario di lavoro e di ottenere l'accesso in lettura/scrittura:

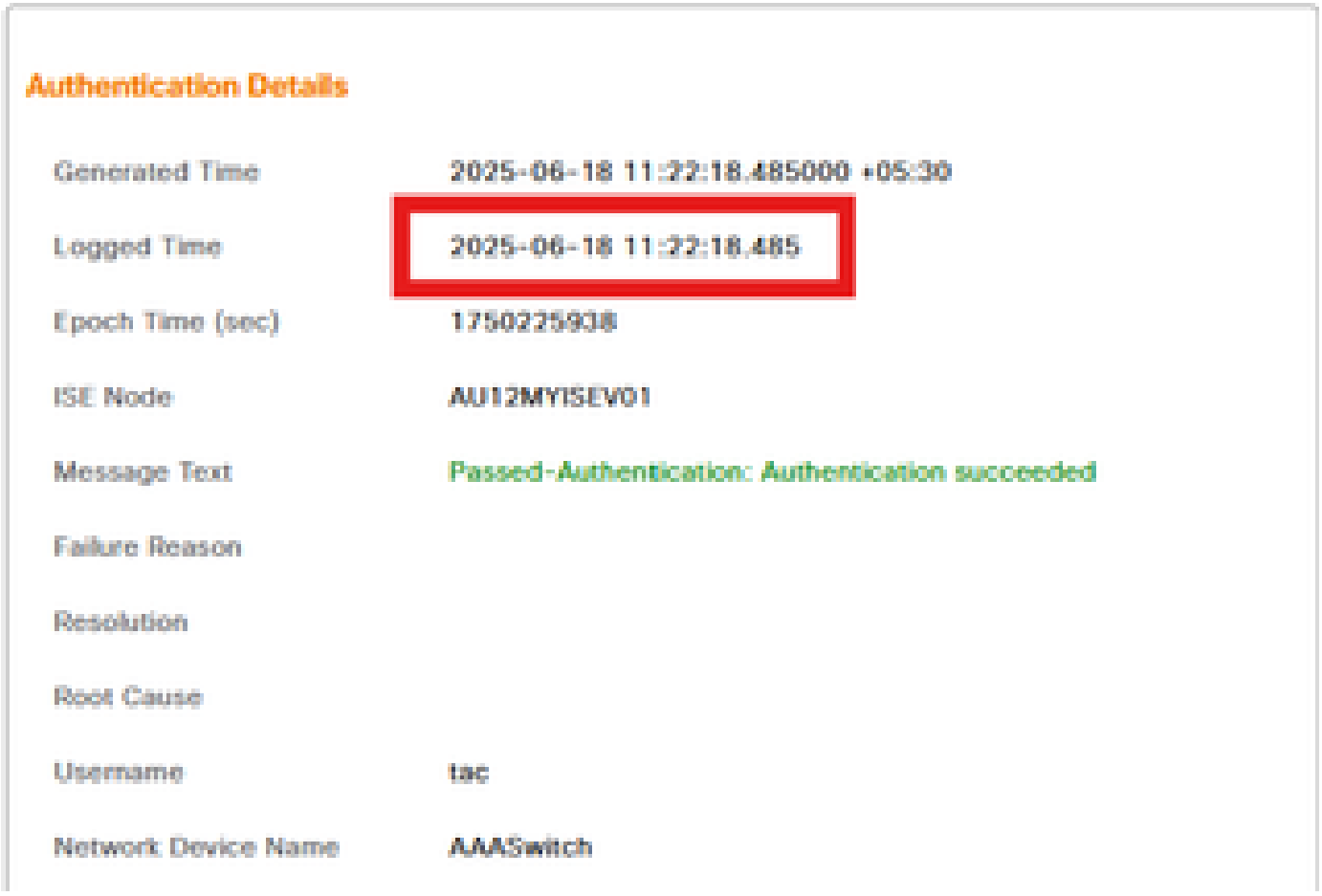


Il registro ISE Live indica che l'accesso durante l'orario di lavoro ha soddisfatto le condizioni di ora e data e ha soddisfatto la policy corretta.



Overview

Request Type	Authentication
Status	Pass
Session Key	AU12MYISEV01/538929861/83
Message Text	Passed-Authentication: Authentication succeeded
Username	tac
Authentication Policy	Cisco Device >> Default
Selected Authorization Profile	Full Access



Authentication Details

Generated Time	2025-06-18 11:22:18.485000 +05:30
Logged Time	2025-06-18 11:22:18.485
Epoch Time (sec)	1750225938
ISE Node	AU12MYISEV01
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	tac
Network Device Name	AAASwitch

Risoluzione dei problemi

Debug su ISE

Raccogliere il bundle di supporto ISE con questi attributi da impostare al livello di debug:

- RuleEngine-Policy-IDGroups
- Attributi Motore regole
- Policy-Engine
- epm-pdp
- epm-pip

Quando l'utente che tenta di connettersi al protocollo SSH al di fuori dell'orario di lavoro a causa di una condizione di data e ora non corrisponde all'orario di lavoro configurato.

show logging application ise-psc.log

```
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 360158683110.127.197.5449306Authentication3601586831:
Regola di valutazione - <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<Condition Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-
operand="rhsoperand"/>
</Rule>
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 360158683110.127.197.5449306Authentication3601586831:
Valutazione della condizione con ID - 72483811-ba39-4cc2-bdac-90a38232b95e - LHS operandId
- operandId, operator DATETIME_MATCHES, RHS operandId - rhsoperand
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.ConditionUtil -:::::-
360158683110.127.197.5449306Authentication3601586831: Condizione lhsoperand Value -
com.cisco.cpm.policy.DTConstraint@6924136c , rhsoperand Value -
com.cisco.cpm.policy.DTConstraint@3eeea825
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 360158683110.127.197.5449306Authentication3601586831:
Risultato della valutazione per Condition - 72483811-ba39-4cc2-bdac-90a38232b95e restituito -
false
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 360158683110.127.197.5449306Authentication3601586831:
Impostazione del risultato per la condizione: 72483811-ba39-4cc2-bdac-90a38232b95e : falso
```

Quando l'utente che ha tentato di passare al protocollo SSH durante l'orario di lavoro ha soddisfatto le condizioni di ora e data.

show logging application ise-psc.log

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 18167599110.127.197.5414126Authentication1816759911:
Regola di valutazione - <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<Condition Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-
operand="rhsoperand"/>
</Rule>
```

```
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 18167599110.127.197.5414126Authentication1816759911:
Valutazione della condizione con ID - 72483811-ba39-4cc2-bdac-90a38232b95e - LHS operandId
- operandId, operator DATETIME_MATCHES, RHS operandId - rhsoperand
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.ConditionUtil -:::::-
18167599110.127.197.5414126Authentication1816759911: Condizione lhsoperand Value -
com.cisco.cpm.policy.DTConstraint@4af10566 , rhsoperand Value -
com.cisco.cpm.policy.DTConstraint@2bdb62e9
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 18167599110.127.197.5414126Authentication1816759911:
Risultato della valutazione per la condizione - 72483811-ba39-4cc2-bdac-90a38232b95e
restituito - true
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 18167599110.127.197.5414126Authentication1816759911:
Impostazione del risultato per la condizione: 72483811-ba39-4cc2-bdac-90a38232b95e : vero
```

Informazioni correlate

- Guida all'implementazione prescrittiva di Cisco ISE Device Administration

Domande frequenti

- È possibile applicare diversi livelli di accesso in base al tempo?
  Sì. È possibile creare criteri di autorizzazione diversi e collegarli alle condizioni temporali.

  Ad esempio:
  Accesso completo durante l'orario di lavoro
  Accesso in sola lettura fuori orario
  Nessun accesso durante il fine settimana

- Cosa succede se l'ora di sistema non è corretta o non è sincronizzata?
  ISE può applicare policy errate o non applicare regole basate sul tempo in modo affidabile. Accertarsi che tutti i dispositivi e i nodi ISE utilizzino un'origine NTP sincronizzata.

- È possibile utilizzare i criteri basati sul tempo insieme ad altre condizioni, ad esempio il ruolo utente o il tipo di dispositivo?
  Sì. Le condizioni temporali possono essere combinate con altri attributi nelle regole dei criteri per creare controlli di accesso granulari e sicuri.

- L'accesso a tempo è supportato sia per la shell che per i set di comandi in TACACS+?
  Sì. Le condizioni basate sul tempo possono controllare l'accesso alla shell del dispositivo o a specifici set di comandi, a seconda della struttura dei profili e dei criteri di autorizzazione.

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).