Op tijd gebaseerde TACACS+-toegang configureren voor netwerkapparaten met ISE

Inhoud

Inleiding

In dit document wordt beschreven hoe u de op tijd en datum gebaseerde autorisatie voor apparaatbeheerbeleid kunt configureren in Cisco Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van de Tacacs Protocol and Identity Services Engine (ISE) configuratie.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Catalyst 9300 switch met softwareCisco IOS® XE 17.12.5 en hoger
- Cisco ISE, versie 3.3 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

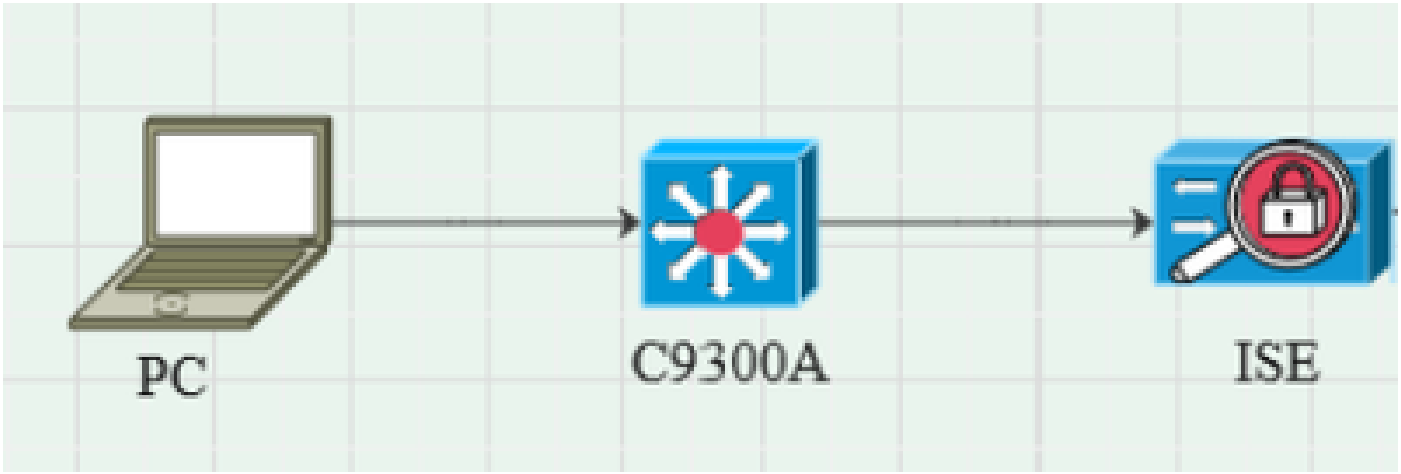
Autorisatiebeleid is een belangrijk onderdeel van Cisco Identity Services Engine (ISE), waarmee u regels kunt definiëren en autorisatieprofielen kunt configureren voor specifieke gebruikers of groepen die toegang hebben tot netwerkbronnen. Dit beleid evalueert voorwaarden om te bepalen welk profiel van toepassing is. Wanneer aan de voorwaarden van een regel is voldaan, wordt het bijbehorende machtigingsprofiel geretourneerd, waarbij passende netwerktoegang wordt verleend.

Cisco ISE ondersteunt ook de tijd- en datumvoorwaarden, waardoor beleid alleen kan worden afgedwongen tijdens bepaalde tijden of dagen. Dit is met name handig voor het toepassen van toegangscontroles op basis van zakelijke vereisten op basis van tijd.

Dit document schetst de configuratie om TACACS+ beheerderstoegang tot netwerkapparaten alleen toe te staan tijdens kantooruren (maandag tot en met vrijdag, 08:00-17:00) en om toegang buiten dit tijdvenster te weigeren.

Configureren

Netwerkdiagram



ISE configureren

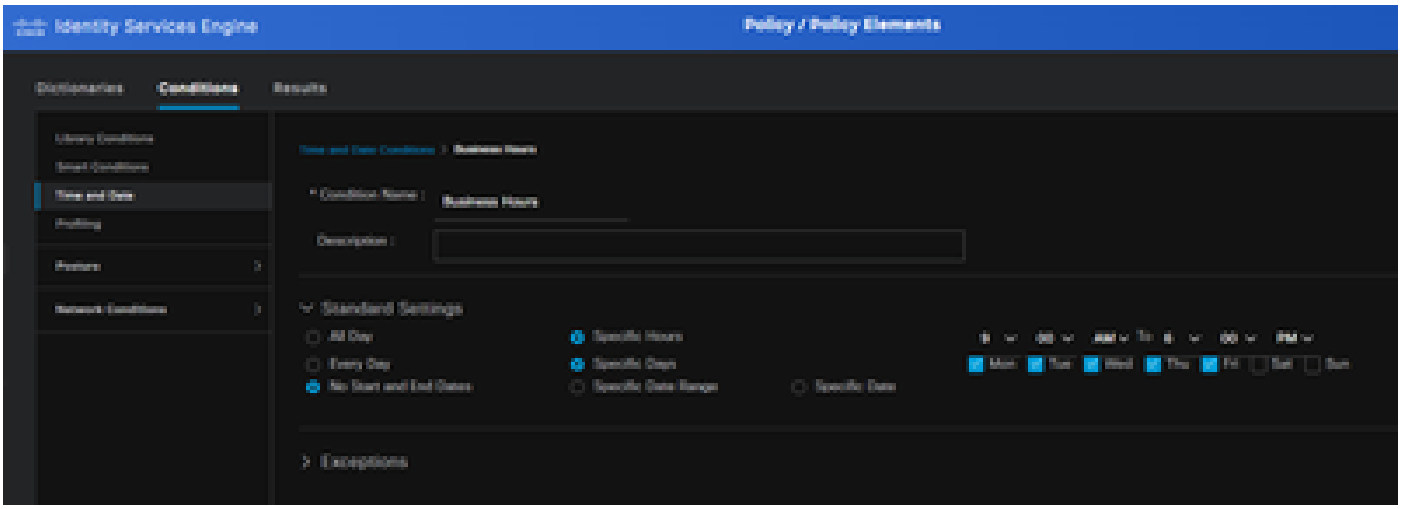
Stap 1: Tijd- en datumvoorwaarde maken

Navigeer naar Beleid > Beleidselementen > Voorwaarden > Tijd en datum en klik op Toevoegen.

Naam conditie: kantooruren

Stel het Tijdsbereik Standaardinstellingen in > Specifieke uren: 09:00 - 06:00 PM

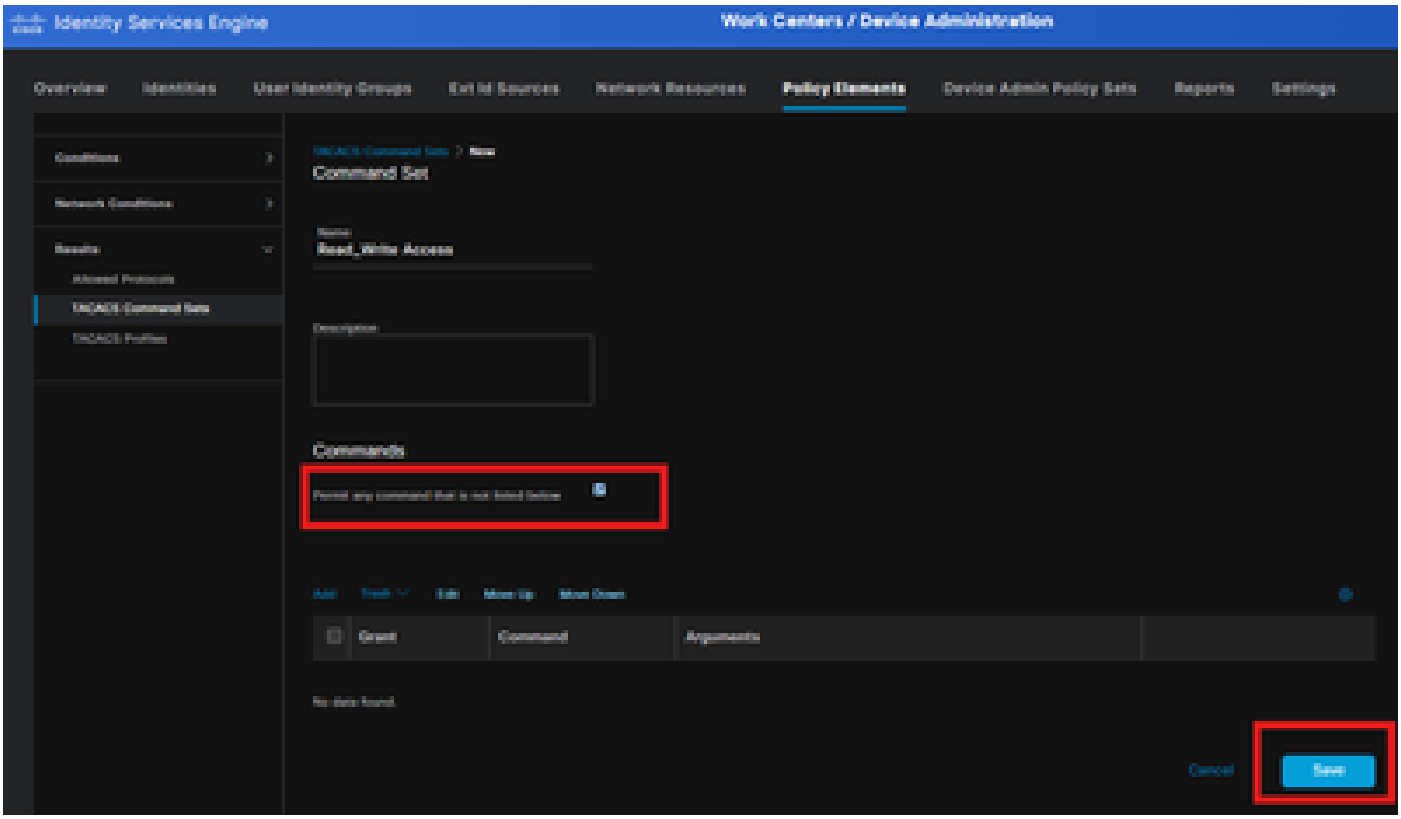
Specifieke dagen: van maandag tot vrijdag



Stap 2: Maak een TACACS+ Command Set

Navigeer naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > Tacacs-opdrachtsets.

Maak een opdrachtset door het selectievakje Opdrachten toestaan te kiezen die niet hieronder worden weergegeven en klik op Indienen of de Beperkte opdrachten toevoegen als u bepaalde CLI-opdrachten wilt beperken.

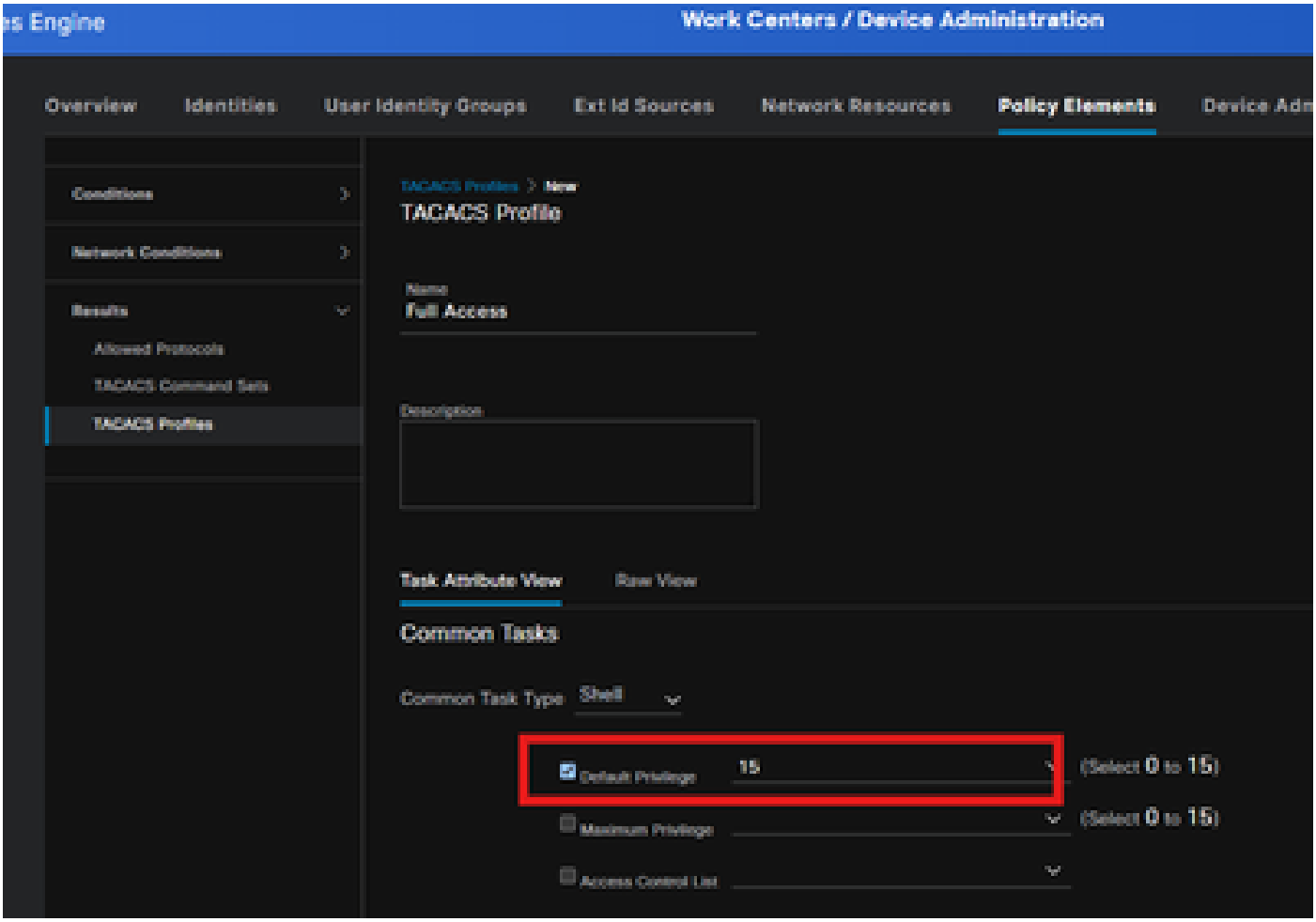


Stap 3: Maak een TACACS+ profiel aan

Navigeer naar Werkcentra > Apparaatbeheer > Beleidselementen > Resultaten > TACACS-

profielen. Klik op Add (Toevoegen).

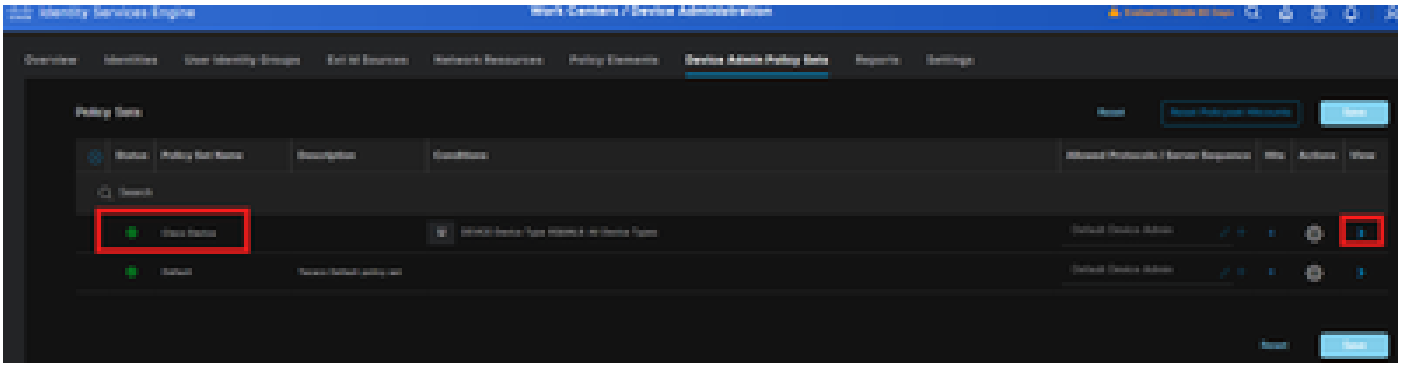
Selecteer Opdrachttaaktype als Shell, selecteer het selectievakje Standaardbevoegdheden en voer de waarde 15 in. Klik op Indienen.



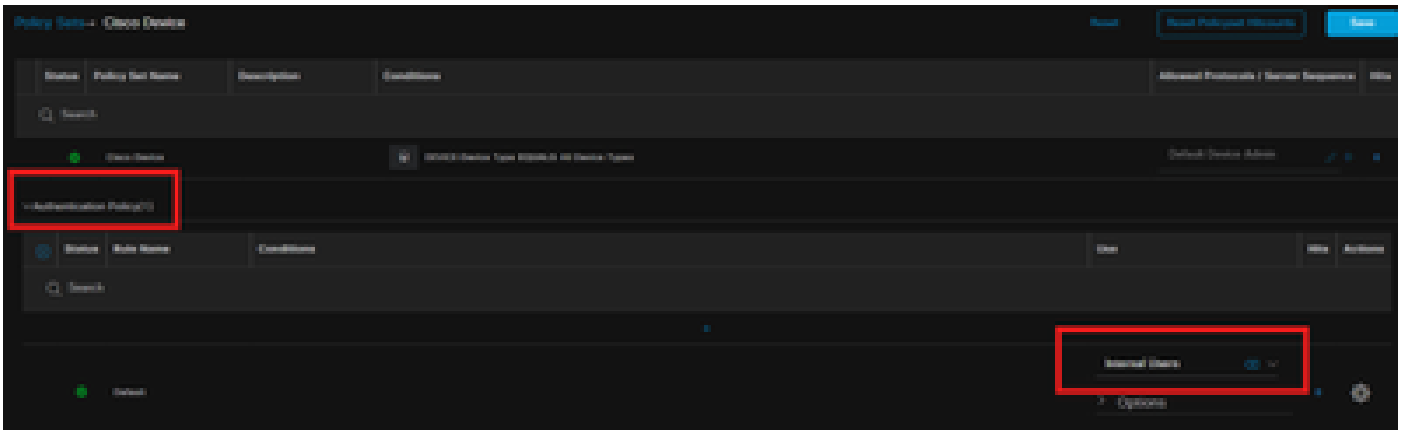
Stap 4: TACACS-autorisatiebeleid maken

Navigeer naar Werkcentra > Apparaatbeheer > Beleidssets apparaatbeheer.

Selecteer uw actieve beleidsset.



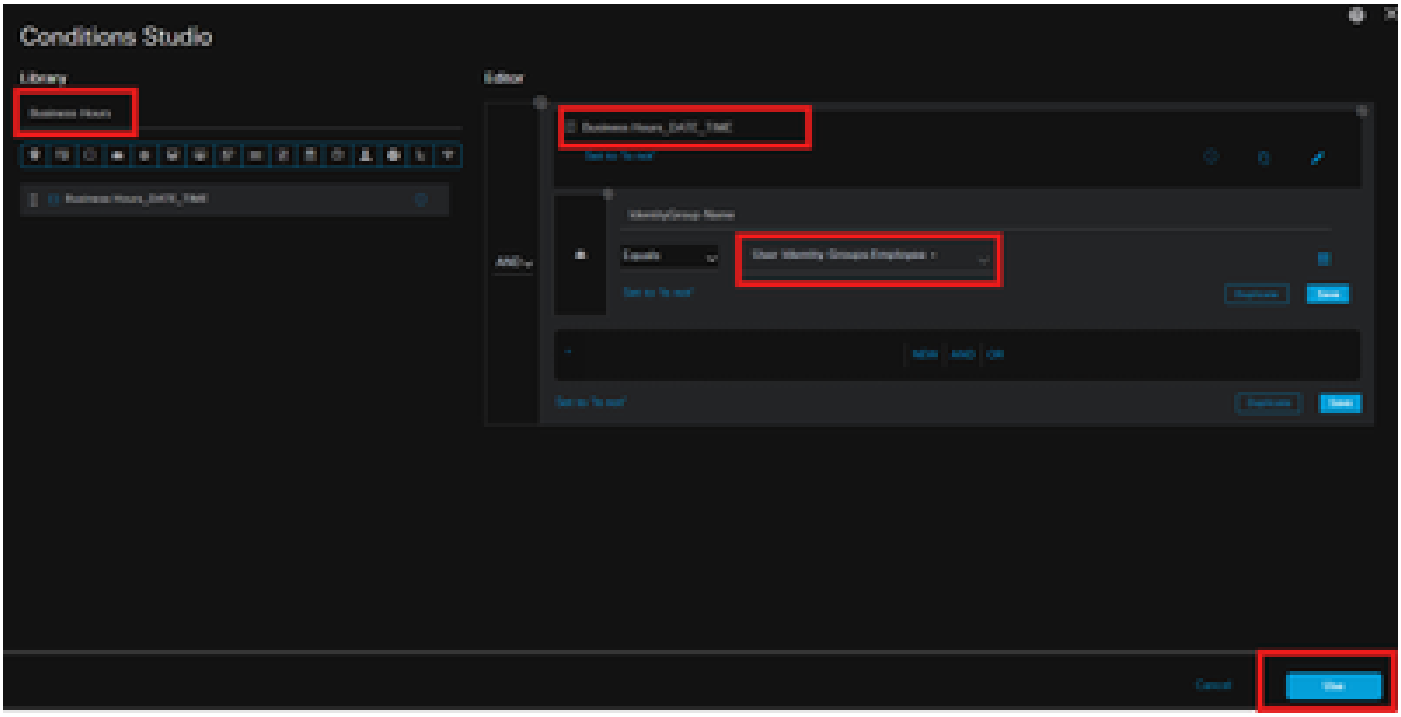
Configureer het verificatiebeleid op basis van de interne of Active Directory-gebruikers.



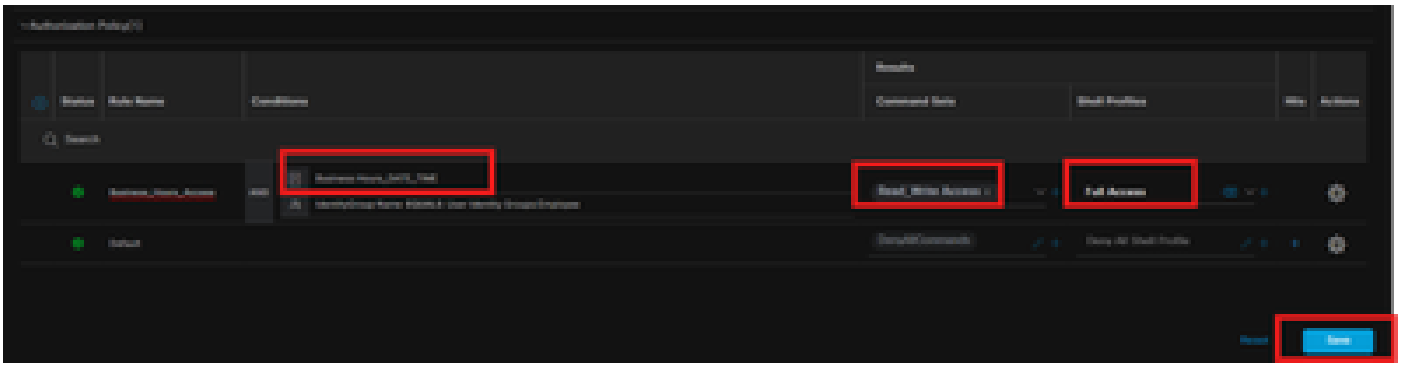
Klik in het gedeelte Autorisatiebeleid op Regel toevoegen om de naam van de regel op te geven en klik vervolgens op + voor het toevoegen van autorisatievoorwaarden.

Er verschijnt een nieuw venster Condition Studio, voer in het veld Zoeken op naam de naam in die is gemaakt in stap 1 en sleep deze naar de editor.

Voeg aanvullende voorwaarden toe op basis van de gebruikersgroep en klik op Opslaan.



Selecteer in Resultaten de Tacacs-opdrachtset en het Shell-profiel die in stap 2 zijn gemaakt en klik vervolgens op Opslaan.



Switch configureren

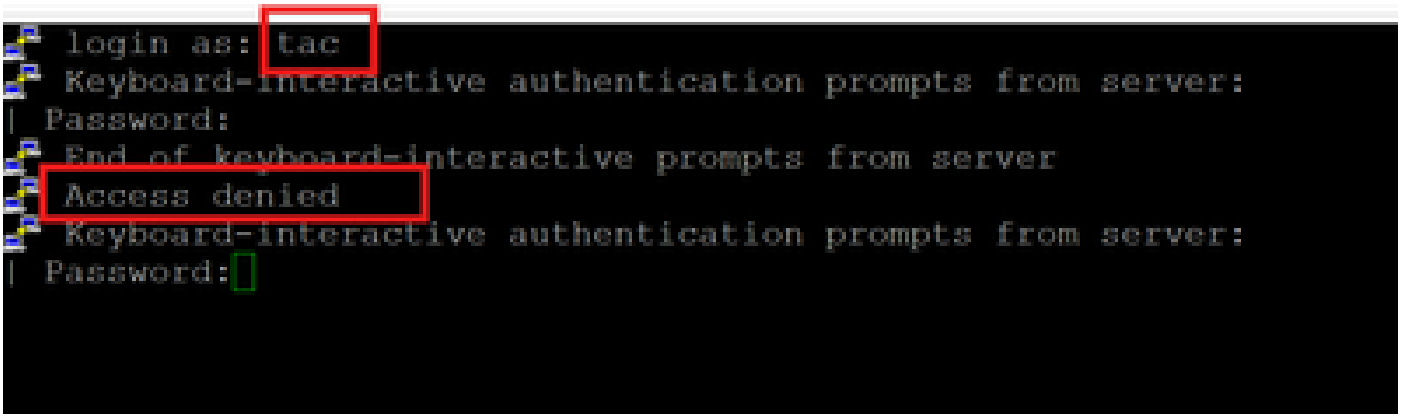
nieuw AAA-model

AAA-verificatie Aanmeldingsgegevens Standaard lokale groep TACACS+
AAA-verificatie Schakel standaard TACACS+-groep in
AAA-autorisatieconfig-opdrachten
AAA-autorisatie EXEC Standaard lokale groep TACACS+
AAA-autorisatieopdrachten 0 standaard lokale groep Tacacs+
AAA-autorisatieopdrachten 1 standaard lokale groep TACACS+
AAA-autorisatieopdrachten 15 standaard lokale groep Tacacs+

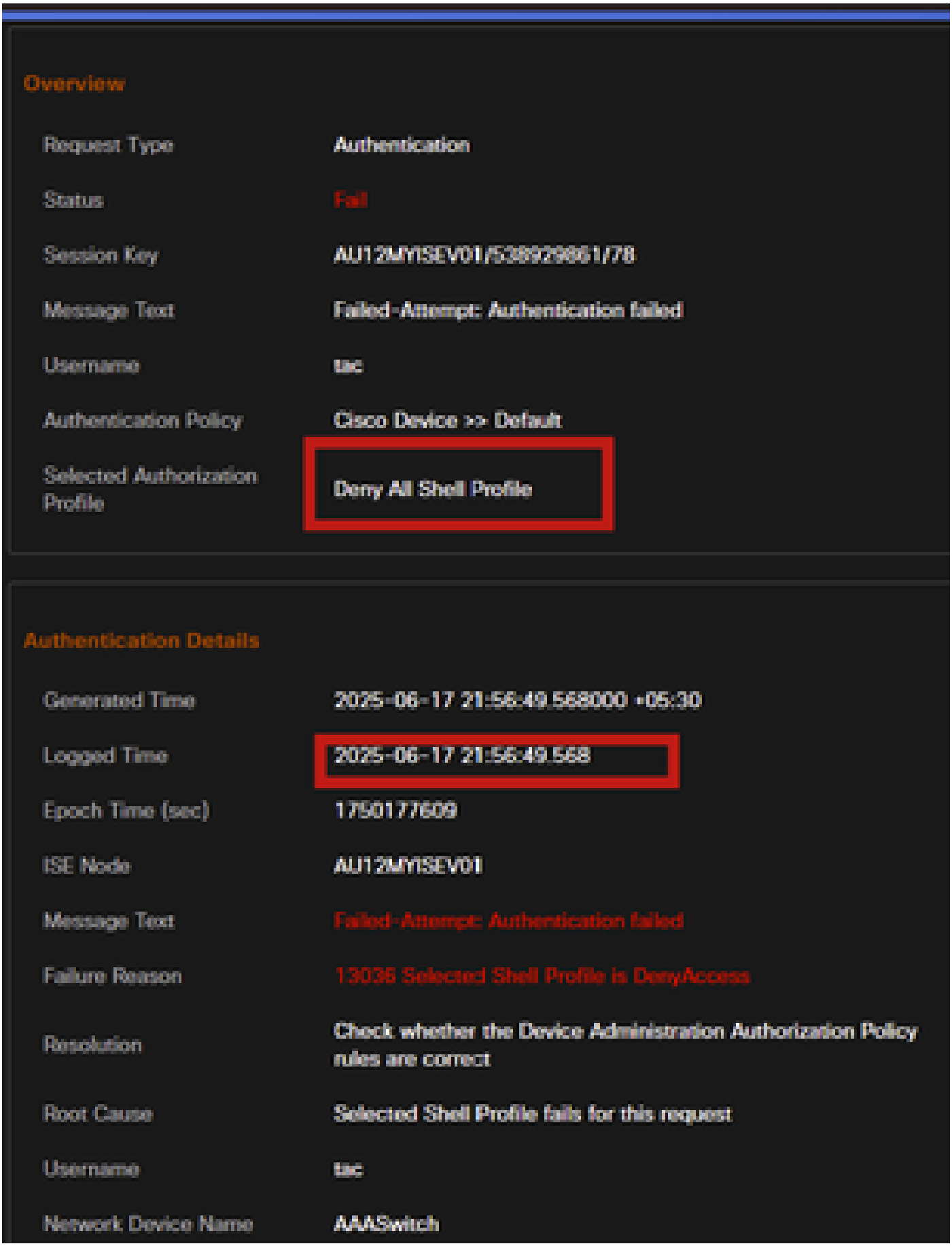
tacacs-server-ISE
Adres IPv4 10.127.197.53
key Qwerty123

Verifiëren

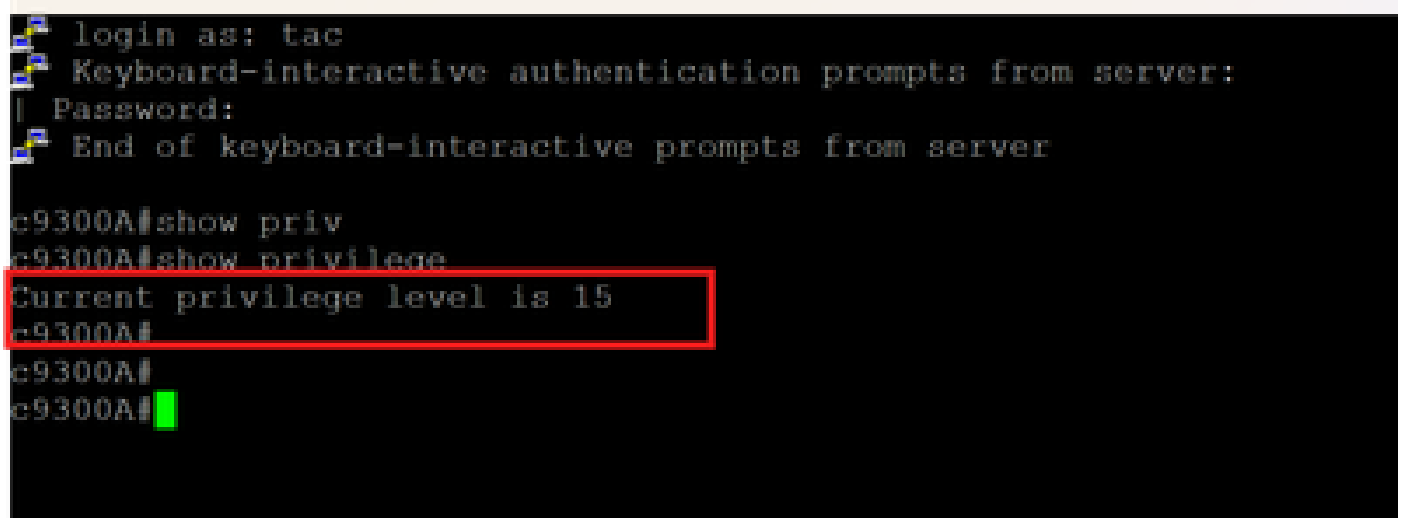
Gebruiker die probeert SSH in de Switch te krijgen buiten kantooruren en toegang kreeg geweigerd van ISE.



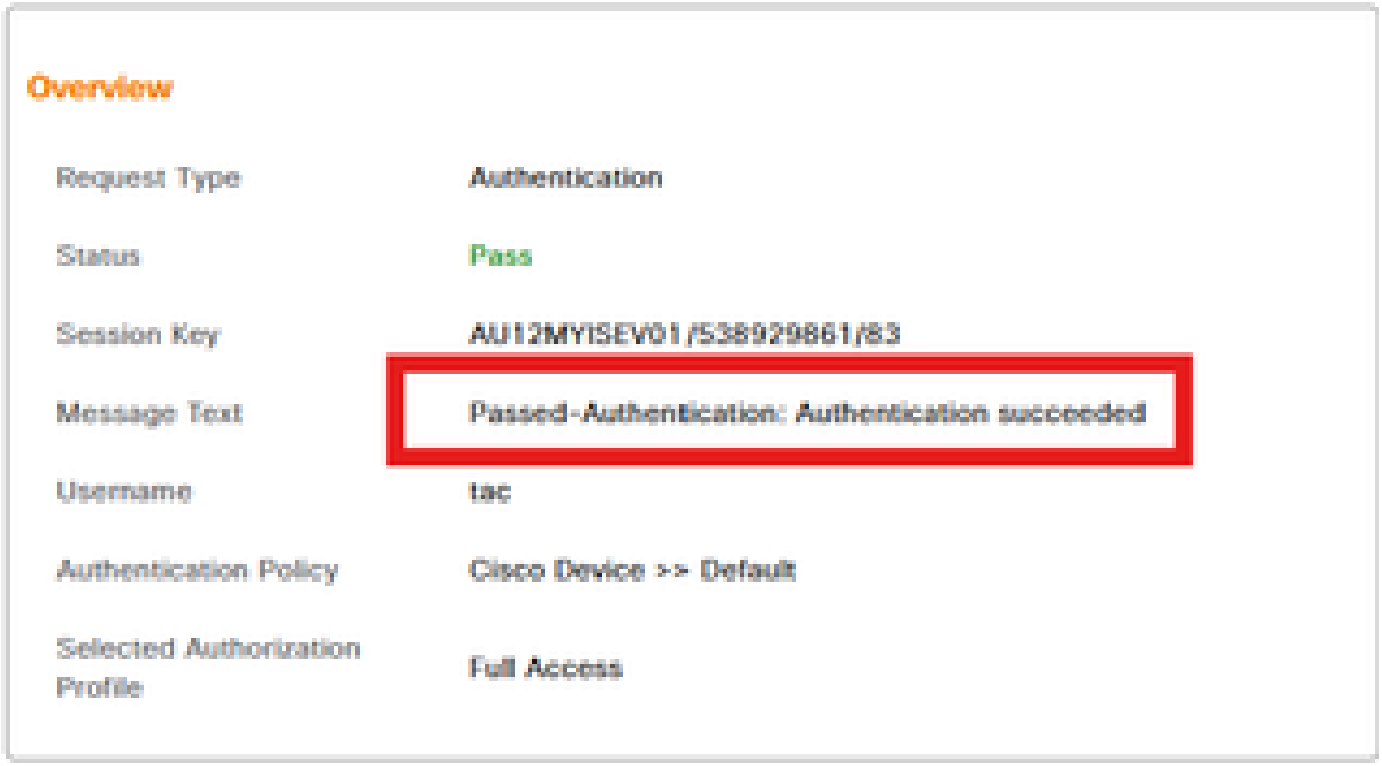
De ISE Live Logs geven aan dat de autorisatie is mislukt omdat de voorwaarde Tijd en Datum in het autorisatiebeleid niet overeenkwam, waardoor de sessie de regel Standaard toegang weigeren raakt.

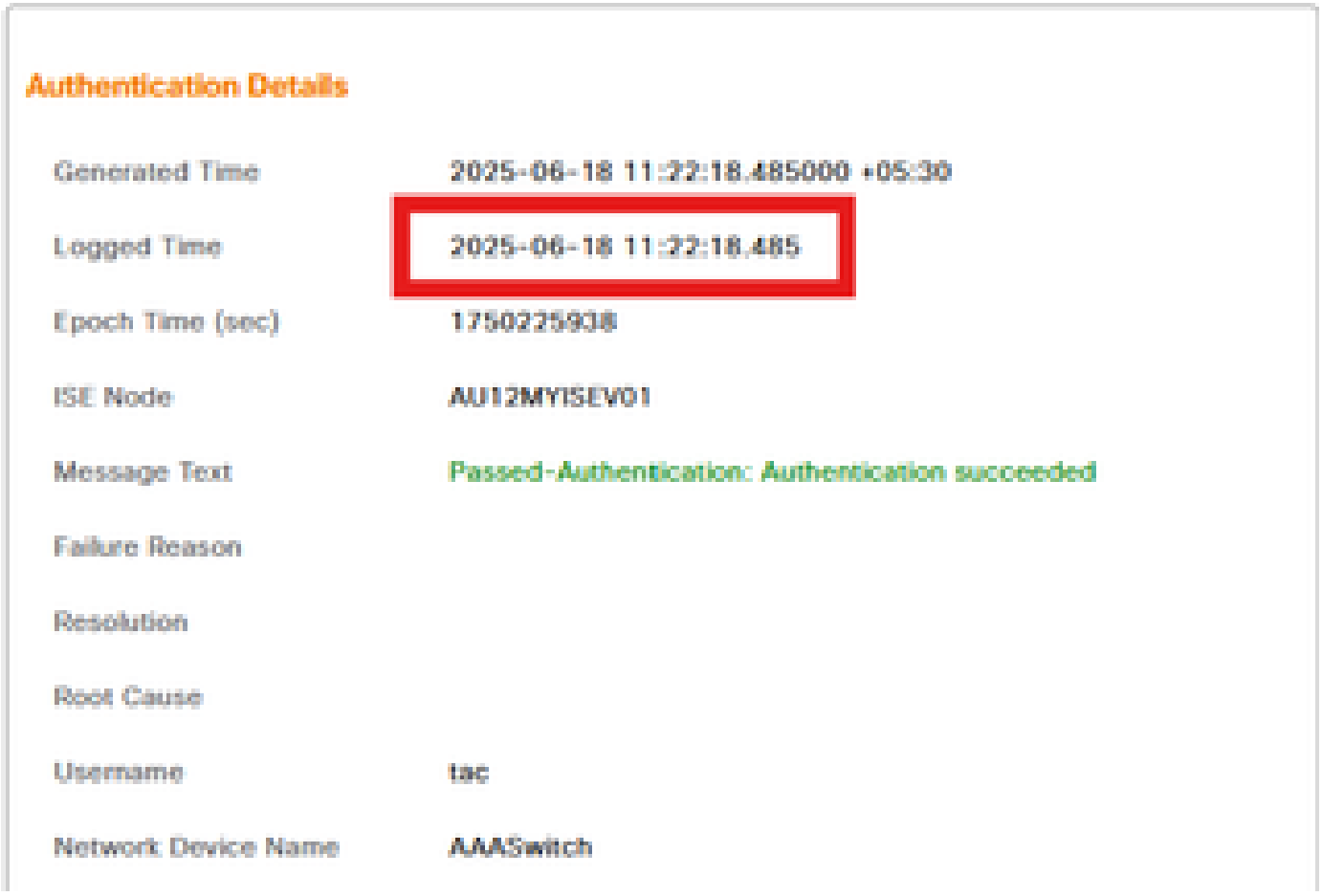


Gebruiker die tijdens kantooruren probeert om SSH in switch te plaatsen en toegang tot lezen en schrijven te krijgen:



Het ISE Live-logboek geeft aan dat de aanmelding tijdens kantooruren overeenkomt met de tijd- en datumvoorwaarde en het juiste beleid raakt.





Problemen oplossen

Foutopsporing op ISE

Verzamel de ISE-supportbundel met deze attributen die op het debug-niveau moeten worden ingesteld:

- RuleEngine-Policy-IDGroups
- regelEngine-attributen
- beleidsmotor
- EPM-PDP
- epm-pip

Wanneer de gebruiker probeert om SSH in de Switch te krijgen buiten kantooruren vanwege de tijd- en datumconditie die niet overeenkomt met de geconfigureerde kantooruren.

Logboekregistratietoepassing ise-psc.log weergeven

```
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::- 360158683110.127.197.5449306Authenticatie3601586831:
Evaluatieregel - <Regel ID="cdd4e295-6d1b-477b-8ae6-587131770585">
<Condition Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-
operand="rhsoperand"/>
</regel>
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::- 360158683110.127.197.5449306Authenticatie3601586831:
Conditie evalueren met 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 -:::- 360158683110.127.197.5449306Authenticatie3601586831:
Conditie lhsoperand Waarde - com.cisco.cpm.policy.DTConstraint@6924136c, rhsoperand -
com.cisco.cpm.policy.DTConstraint@3eeea825
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::- 360158683110.127.197.5449306Authenticatie3601586831:
Evaluatieresultaat voor conditie - 72483811-BA39-4CC2-BDAC-90A38232B95E geretourneerd -
FALSE
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::- 360158683110.127.197.5449306Authenticatie3601586831:
Resultaat instellen voor conditie: 72483811-BA39-4CC2-BDAC-90A38232B95E: FALSE
```

Wanneer de gebruiker die tijdens de kantooruren probeert SSH in de Switch in te voeren, overeenkomt met de tijd- en datumconditie.

Logboekregistratietoepassing ise-psc.log weergeven

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::- 181675991110.127.197.5414126Authenticatie1816759911:
Evaluatieregel - <Regel ID="cdd4e295-6d1b-477b-8ae6-587131770585">
<Condition Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-
operand="rhsoperand"/>
</regel>
```

```
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::- 181675991110.127.197.5414126Authenticatie1816759911:
Conditie evalueren met 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 -:::- 181675991110.127.197.5414126Authenticatie1816759911:
Conditie lhsoperand Value - com.cisco.cpm.policy.DTConstraint@4af10566 , rhoperand Value -
com.cisco.cpm.policy.DTConstraint@2bdb62e9
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::- 181675991110.127.197.5414126Authenticatie1816759911:
Evaluatieresultaat voor conditie - 72483811-BA39-4CC2-BDAC-90A38232B95E geretourneerd -
true
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::: - 181675991110.127.197.5414126Authenticatie1816759911:
Resultaat instellen voor conditie: 72483811-BA39-4CC2-BDAC-90A38232B95E: true
```

Gerelateerde informatie

- Cisco ISE Device Administration Prescriptive Deployment Guide

Veelgestelde vragen

- Kan ik verschillende toegangsniveaus toepassen op basis van tijd?
  Ja. U kunt verschillende autorisatiebeleidsregels maken en deze koppelen aan tijdsvoorwaarden.

  Voorbeeld:
  Volledige toegang tijdens kantooruren
  Alleen-lezen toegang na kantooruren
  Geen toegang in het weekend

- Wat gebeurt er als de systeemtijd onjuist of ongesynchroniseerd is?
  ISE kan onjuist beleid toepassen of nalaten om op tijd gebaseerde regels betrouwbaar af te dwingen. Zorg ervoor dat alle apparaten en ISE-knooppunten een gesynchroniseerde NTP-bron gebruiken.

- Kunnen tijdgebaseerde beleidsregels worden gebruikt in combinatie met andere voorwaarden (bijvoorbeeld gebruikersrol, apparaattype)?
  Ja. Tijdsvoorwaarden kunnen worden gecombineerd met andere kenmerken in uw beleidsregels om gedetailleerde en veilige toegangscontroles te maken.

- Wordt Time-Based Access ondersteund voor zowel shell- als opdrachtsets in TACACS+?
  Ja. Op tijd gebaseerde voorwaarden kunnen de toegang tot de shell van het apparaat of specifieke opdrachtsets regelen, afhankelijk van hoe het autorisatiebeleid en de profielen zijn gestructureerd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.