為使用ISE的網路裝置配置基於時間的TACACS+訪問

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[背景資訊](#)

[設定](#)

- [網路圖表](#)
- [配置ISE](#)
  - [步驟 1:建立時間和日期條件](#)
  - [步驟 2:建立TACACS+命令集](#)
  - [步驟 3:建立TACACS+設定檔](#)
  - [步驟 4:建立TACACS授權策略](#)
- [配置交換機](#)
- [驗證](#)

[疑難排解](#)

- [ISE上的調試](#)

[相關資訊](#)

[常見問題](#)

簡介

本文檔介紹如何為思科身份服務引擎(ISE)中的裝置管理策略配置基於時間和日期的授權。

必要條件

需求

思科建議您瞭解Tacacs通訊協定和身分識別服務引擎(ISE)組態。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Catalyst 9300交換機，軟體Cisco IOS® XE 17.12.5及更高版本
- Cisco ISE 3.3版及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

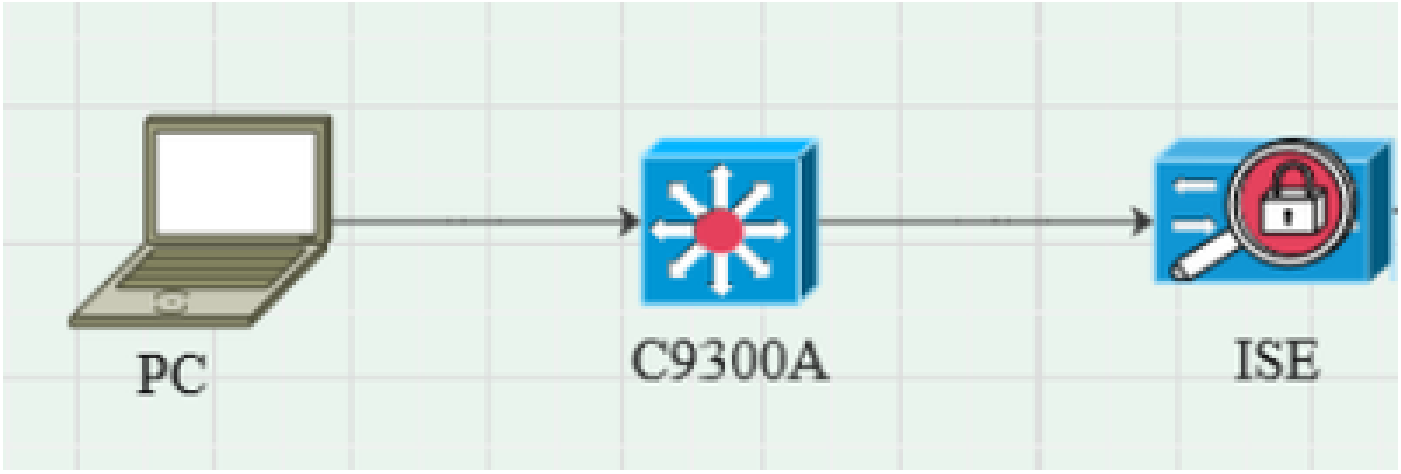
授權策略是思科身份服務引擎(ISE)的關鍵元件，允許您為訪問網路資源的特定使用者或組定義規則和配置授權配置檔案。這些策略評估條件以確定應用哪個配置檔案。當滿足規則的條件時，返回相應的授權配置檔案，授予適當的網路訪問許可權。

思科ISE還支援時間和日期條件，這些條件允許僅在指定的時間或天實施策略。這對於根據基於時間的業務要求應用訪問控制尤其有用。

本文檔概述了僅在工作時間（星期一至星期五，08:00-17:00）內允許TACACS+管理訪問網路裝置的配置，以及在此時間範圍之外拒絕訪問的配置。

設定

網路圖表



配置ISE

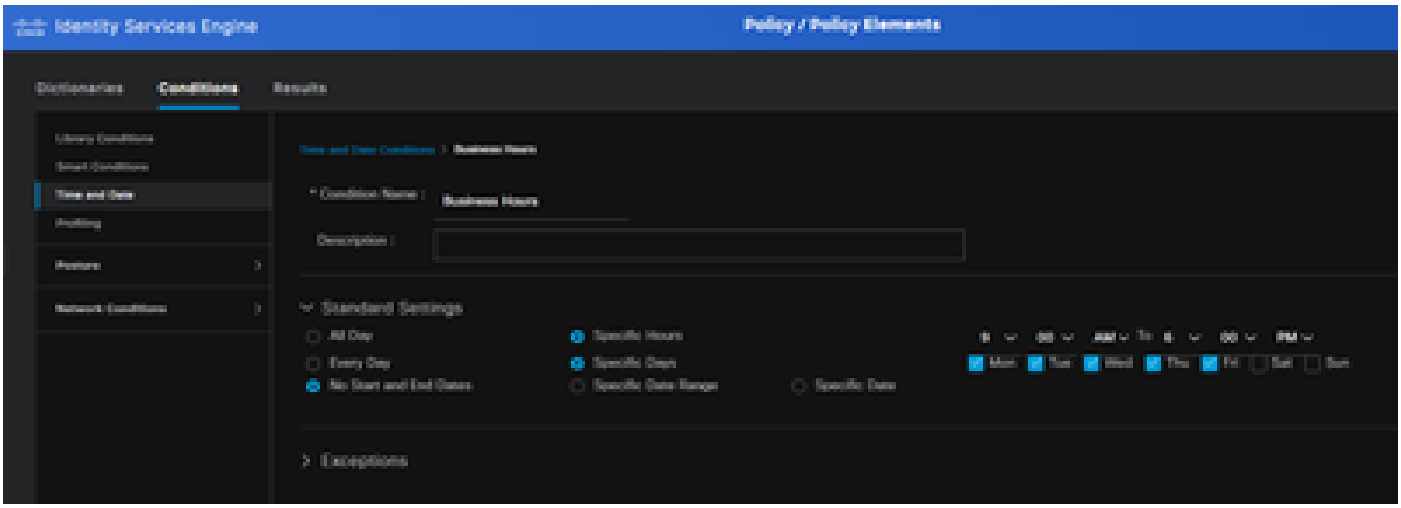
步驟 1:建立時間和日期條件

導航到Policy > Policy Elements > Conditions > Time and Date，點選Add。

條件名稱：工作時間

設定Time Range Standard Settings > Specific Hours: 09:00 AM - 06:00 PM

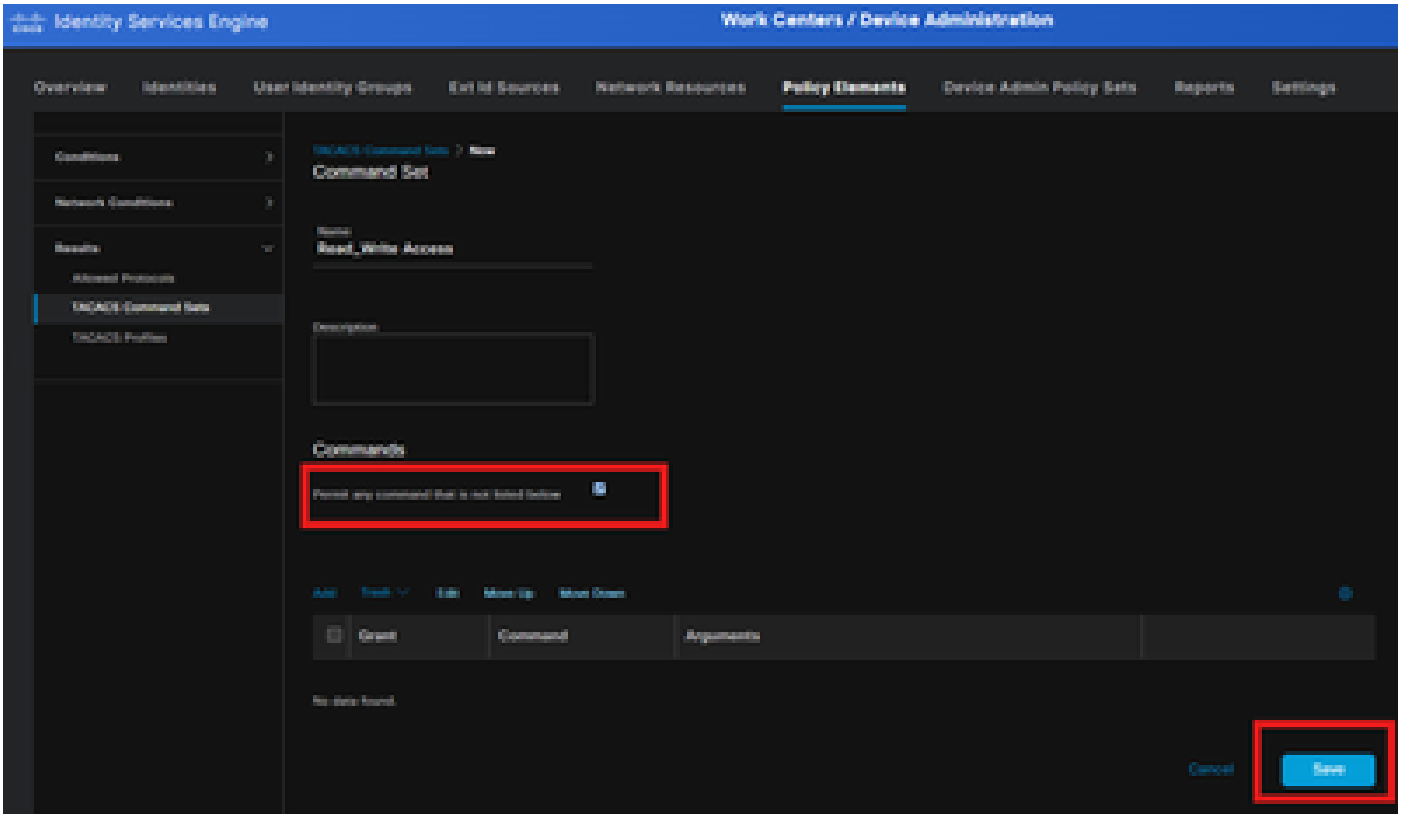
特定日期：星期一到星期五



步驟 2:建立TACACS+命令集

導航到工作中心(Work Centers)>裝置管理(Device Administration)>策略元素(Policy Elements)>結果(Results)> Tacacs命令集(Tacacs Command Sets)。

如果要限制某些CLI命令，請選中Permit any command that not listed below 覈取方塊，然後點選Submit 或新增Limited Commands。

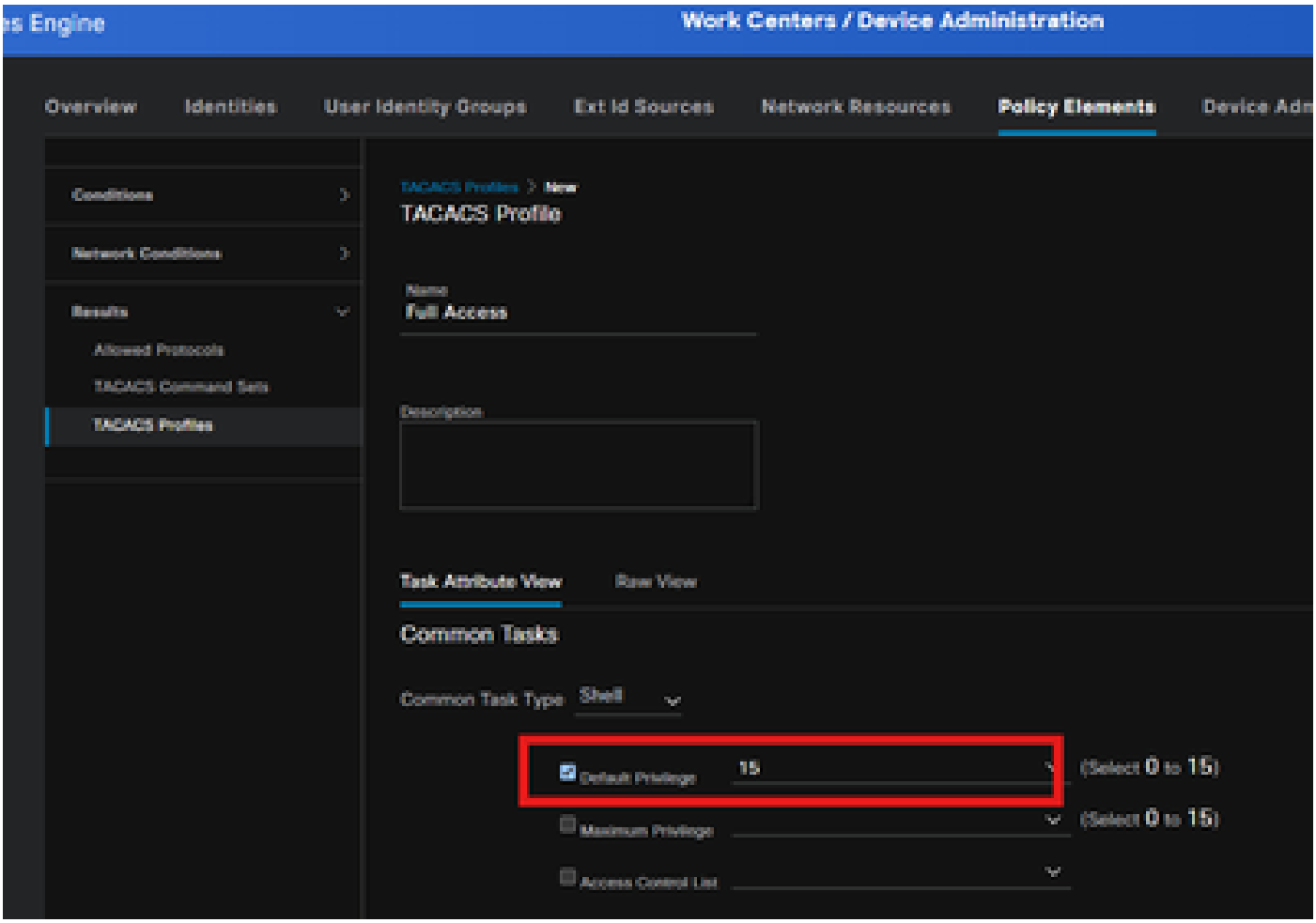


步驟 3:建立TACACS+設定檔

導航到工作中心(Work Centers)>裝置管理(Device Administration)>策略元素(Policy Elements)>結果(Results)> TACACS配置檔案(TACACS Profiles)。按一下「新增」。

選中Command Task Type（命令任務型別）作為Shell（外殼），然後選中Default Privilege（預設

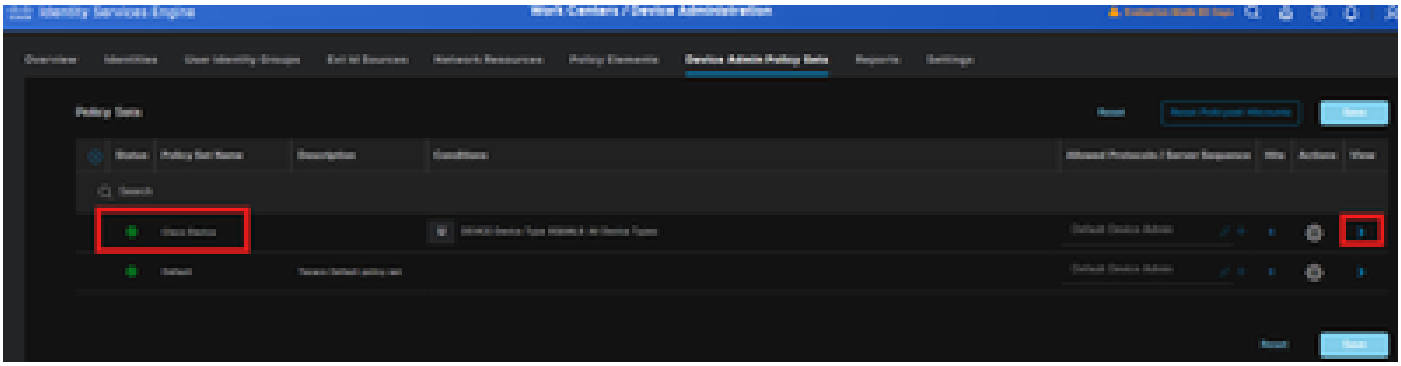
許可權）覈取方塊，並輸入值15。按一下Submit（提交）。



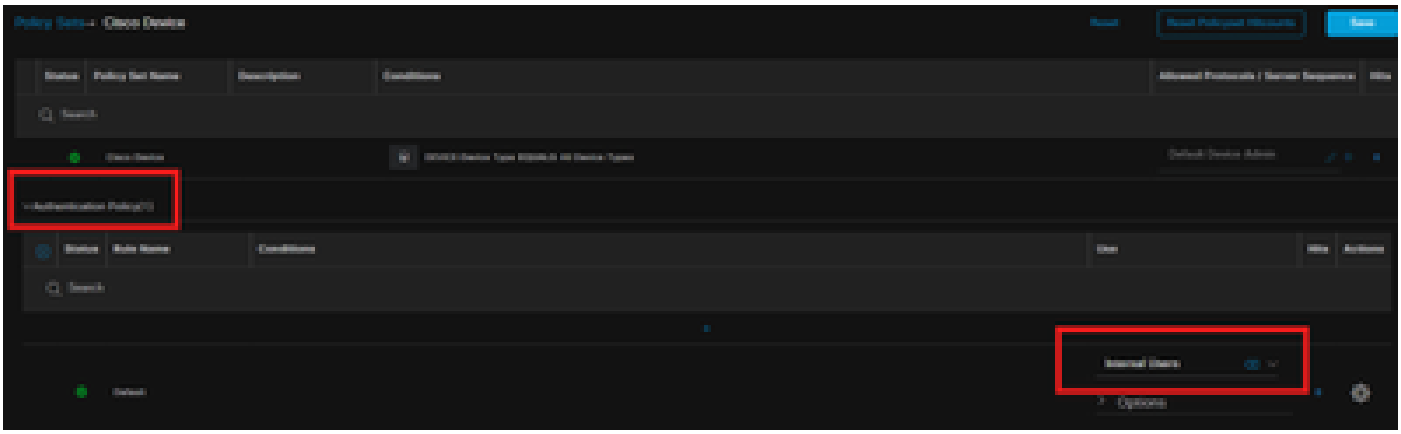
步驟 4：建立TACACS授權策略

導航至工作中心(Work Centers)>裝置管理(Device Administration)>裝置管理策略集(Device Admin Policy Sets)。

選擇活動策略集。



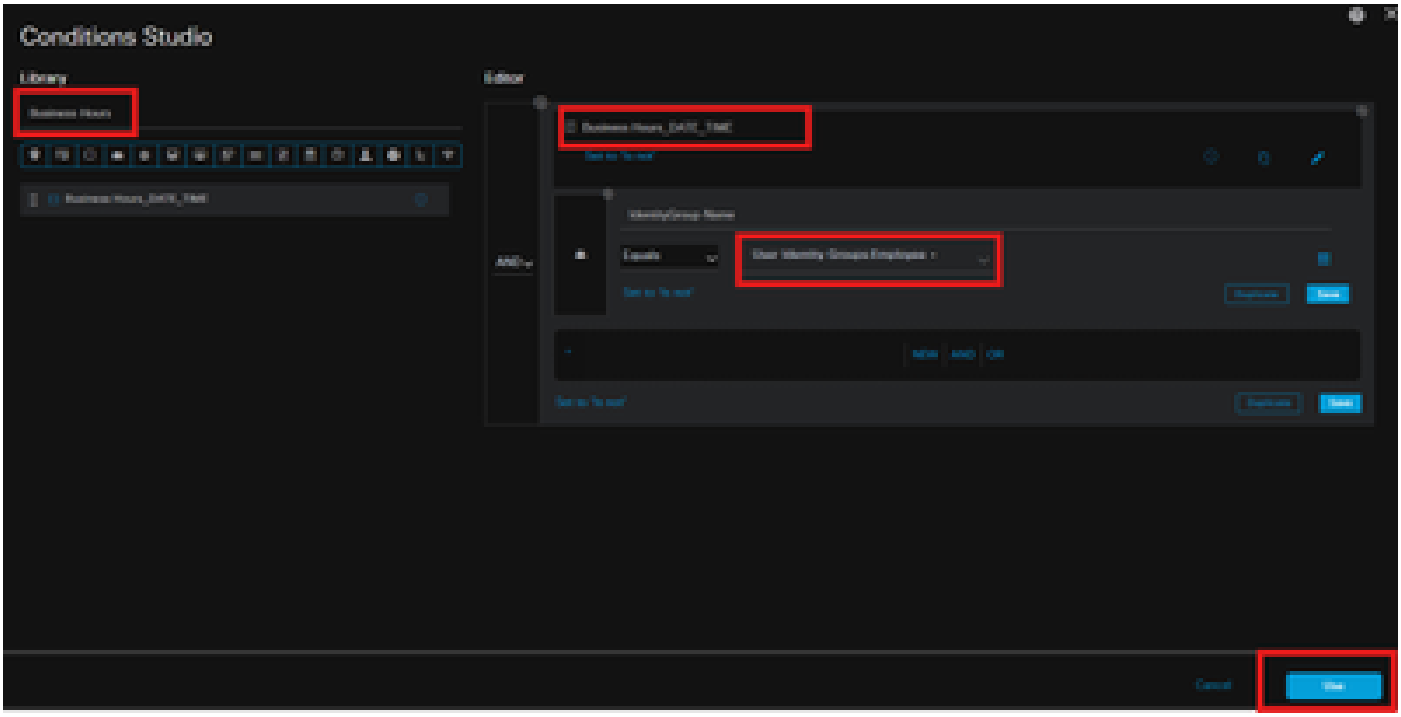
根據內部或Active Directory使用者配置身份驗證策略。



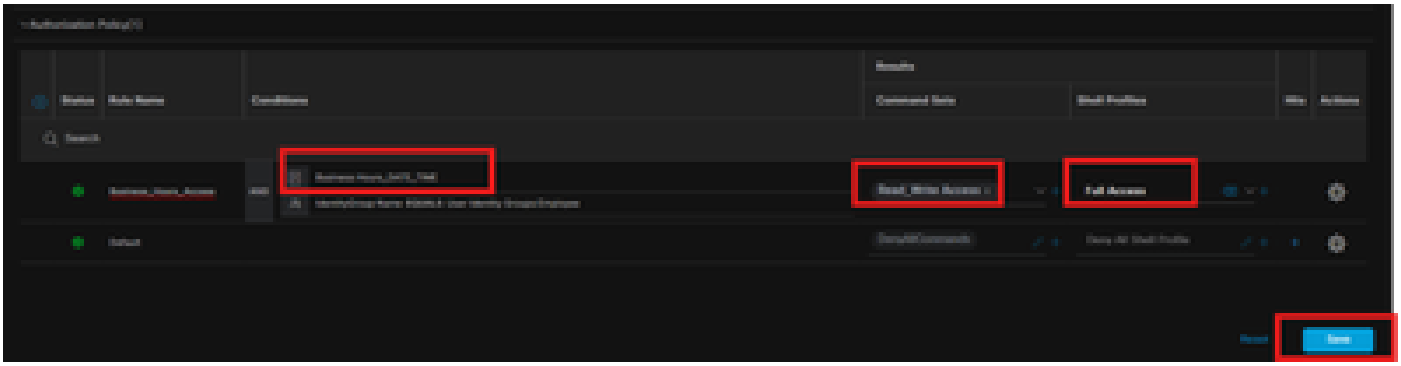
在Authorization Policy部分下，按一下Add Rule以提供Rule Name，然後按一下+新增授權條件。

將出現新的Condition Studio窗口，在Search by Name欄位中輸入在步驟1中建立的名稱並將其拖到編輯器。

根據使用者組新增其他條件，然後按一下儲存。



在Results中，選擇步驟2和步驟3中建立的Tacacs Command Set和Shell Profile，然後按一下Save。

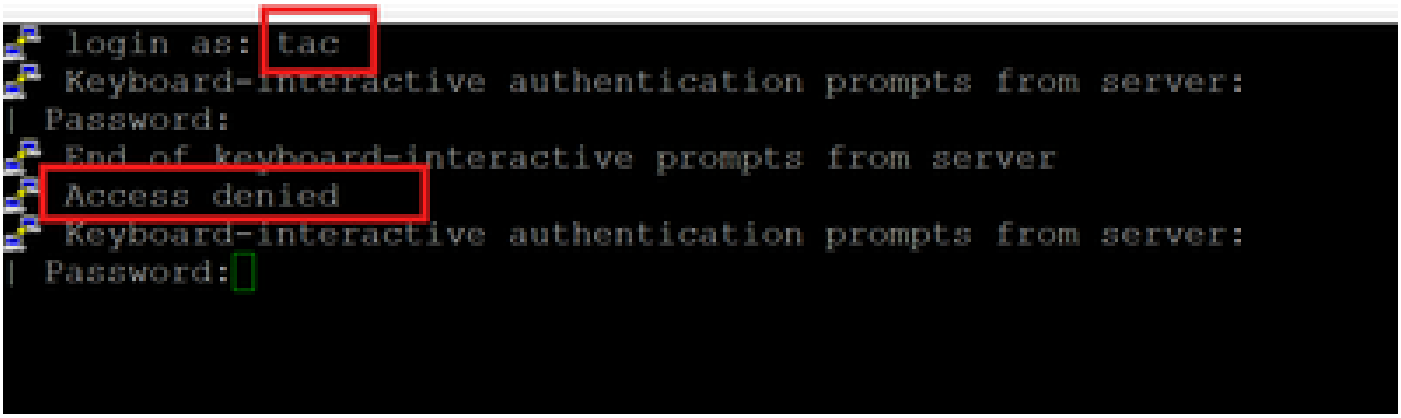


配置交換機

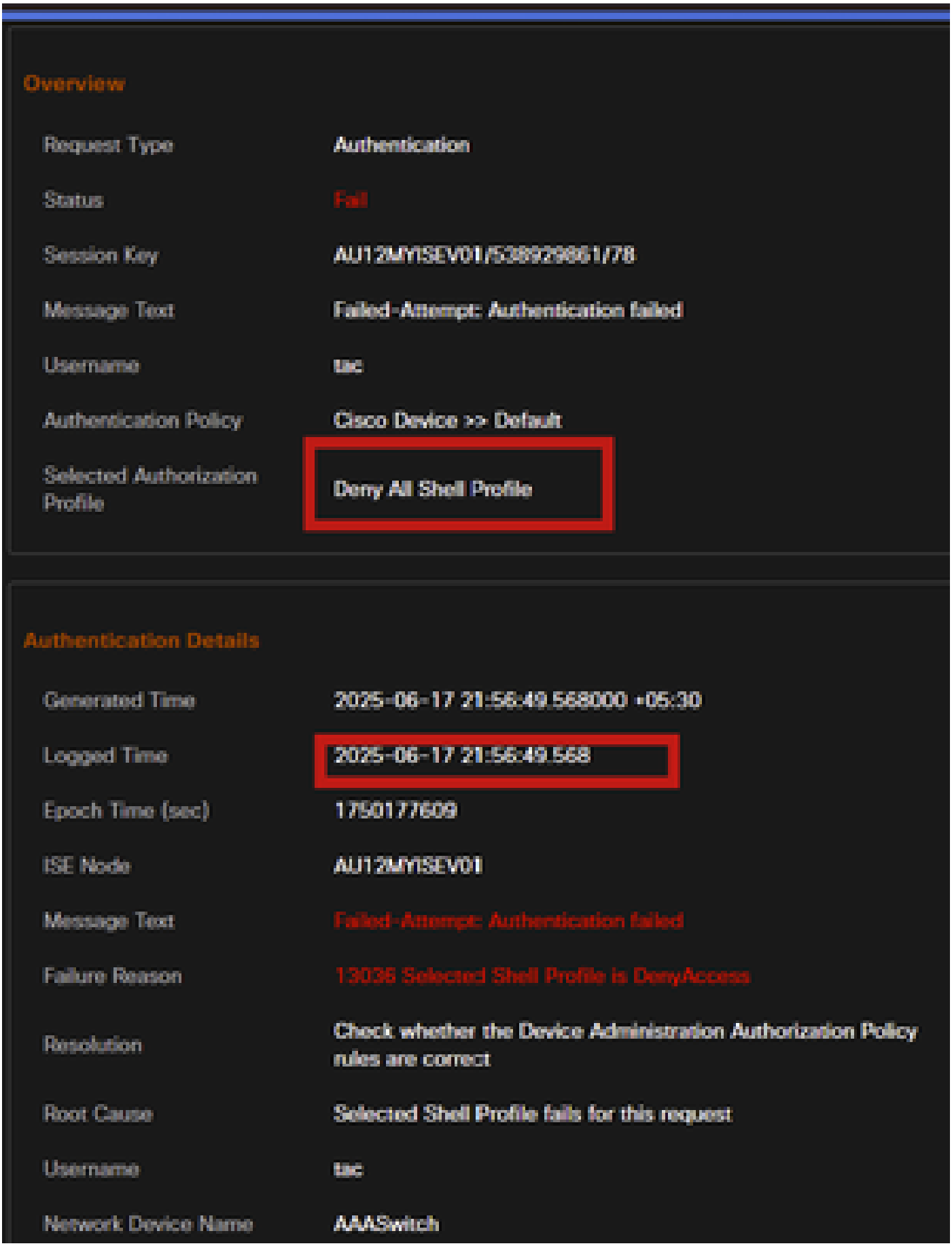
```
aaa new-model

aaa authentication login default local group tacacs+
aaa authentication enable default enable group tacacs+
aaa authorization config-commands
aaa authorization exec預設本地組tacacs+
aaa authorization commands 0 default local group tacacs+
aaa authorization commands 1 default local group tacacs+
aaa authorization commands 15 default local group tacacs+

tacacs伺服器ISE
地址ipv4 10.127.197.53
key Qwerty123
```

驗證

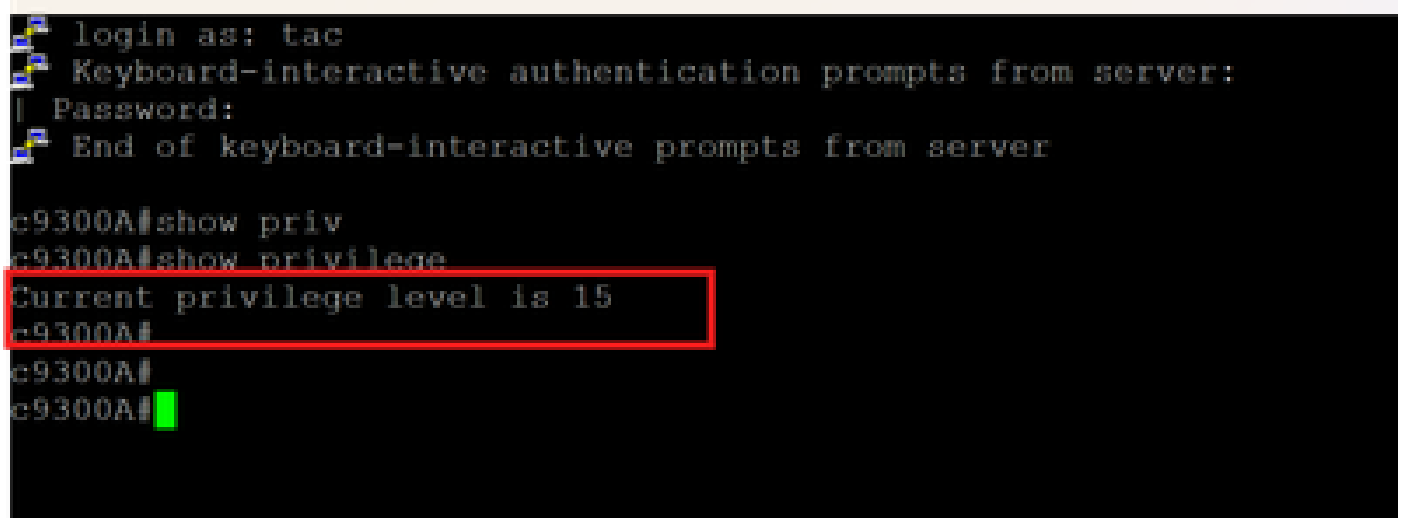
使用者嘗試在工作時間以外通過SSH連線到交換機，但從ISE獲得訪問拒絕。



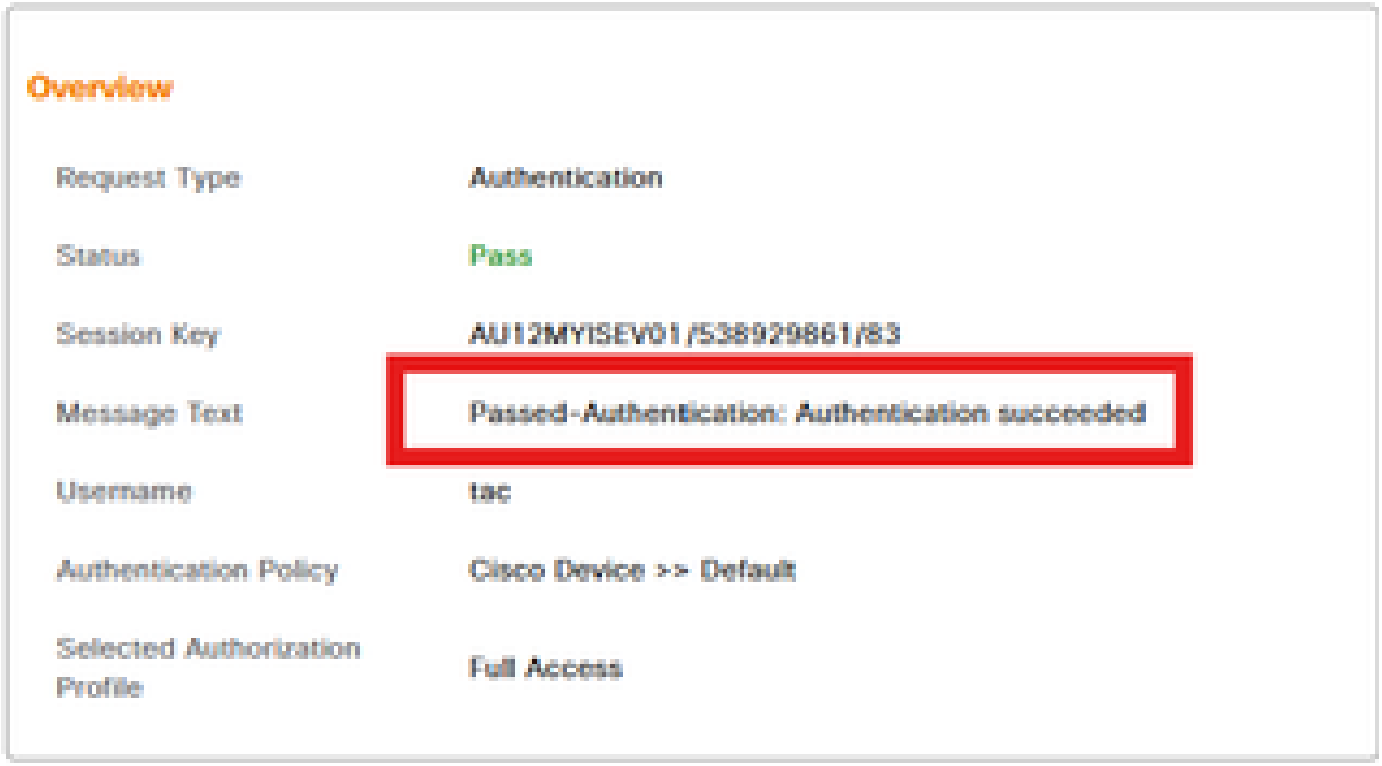
ISE即時日誌表示授權失敗，因為授權策略中的時間和日期條件不匹配，導致會話觸碰預設拒絕訪問規則。



在工作時間嘗試通過SSH連線到交換機並獲得讀寫訪問許可權的使用者：

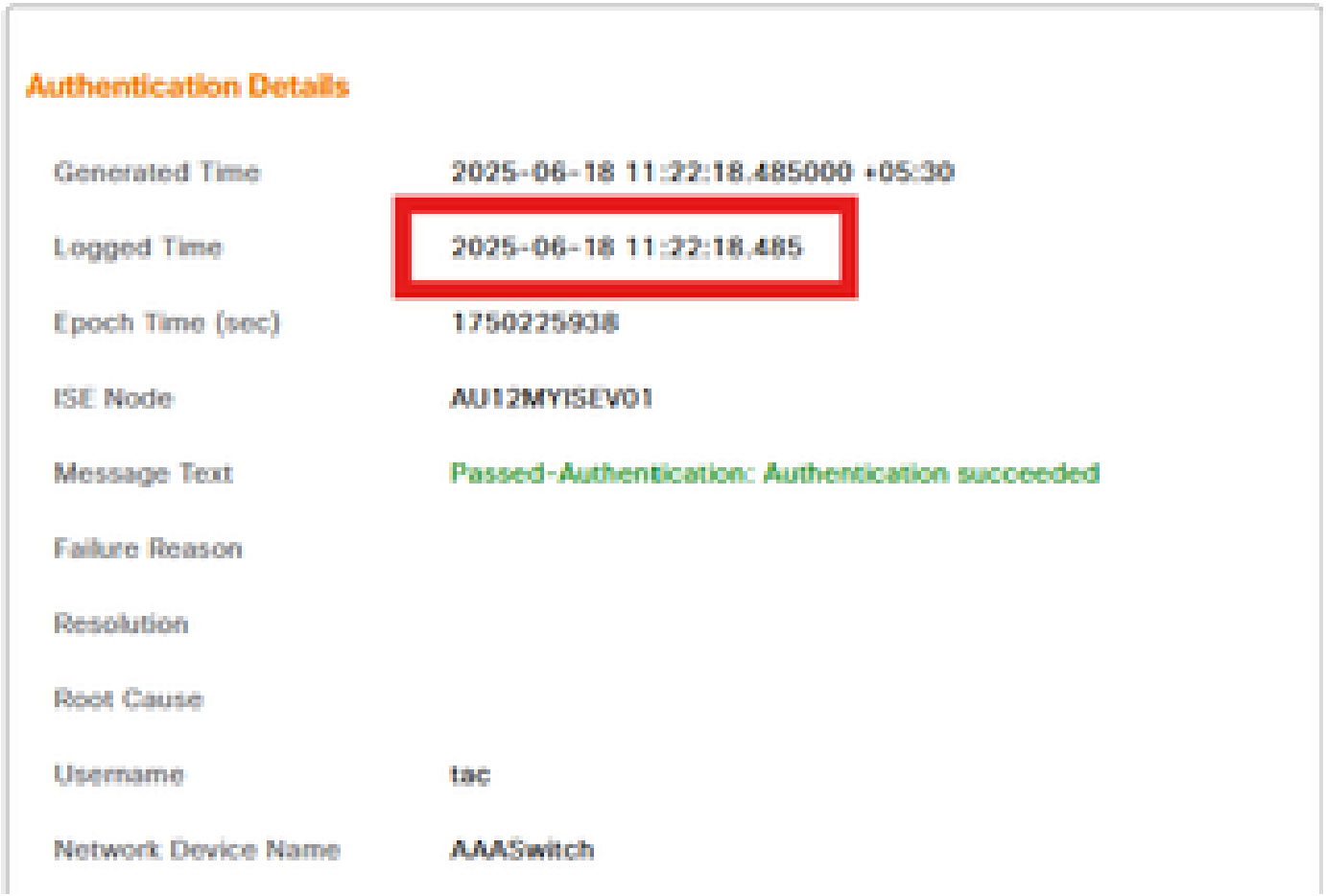


ISE即時日誌指示在營業時間登入與時間和日期條件相匹配，並達到正確的策略。



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

疑難排解

ISE上的調試

收集具有以下屬性的ISE支援捆綁包，以在調試級別設定：

- RuleEngine-Policy-IDGroups
- RuleEngine屬性
- 策略引擎
- epm-pdp
- epm-pip

當由於時間和日期條件而嘗試在營業時間以外通過SSH連線到交換機的使用者與配置的工作時間不匹配時。

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:正在評估規則 — <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<條件Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-operand="rhsproand"/>
</Rule>
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 360158683110.127.197.5449306Authentication3601586831:正在使用id - 72483811-ba39-4cc2-bdac-90a38232b95e - LHS運算元Id — 運算元Id、運算子DATETIME_MATCHES、RHS運算元Id - rhsperand評估條件
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.ConditionUtil -::::-
360158683110.127.197.5449306Authentication3601586831:Condition lhsperand Value -
com.cisco.cpm.policy.DTConstraint@6924136c, rhsperand 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:條件評估結果 — 72483811-ba39-4cc2-bdac-90a38232b95e返回 — false
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 360158683110.127.197.5449306Authentication3601586831:正在設定條件的結果：72483811-ba39-4cc2-bdac-90a38232b95e:假
```

當使用者在營業時間嘗試通過SSH連線到交換機時，符合Time and Date Condition（時間和日期條件）。

show logging application ise-psc.log

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 181675991110.127.197.5414126驗證1816759911:正在評估規則 — <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<條件Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-operand="rhsproand"/>
</Rule>

2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 181675991110.127.197.5414126驗證1816759911:正在使用id - 72483811-ba39-4cc2-bdac-90a38232b95e - LHS運算元Id — 運算元Id、運算子
```

```
DATETIME_MATCHES、RHS運算元Id - rhsperand評估條件
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.ConditionUtil -:::::- 181675991110.127.197.5414126驗證
1816759911:Condition lhsperand Value - com.cisco.cpm.policy.DTConstraint@4af10566,
rhsperand Value - com.cisco.cpm.policy.DTConstraint@2bdb62e9
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 181675991110.127.197.5414126驗證1816759911:條件評估結
果 — 72483811-ba39-4cc2-bdac-90a38232b95e返回 — true
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 181675991110.127.197.5414126驗證1816759911:正在設定條
件的結果：72483811-ba39-4cc2-bdac-90a38232b95e:true
```

相關資訊

- 思科ISE裝置管理規範部署指南

常見問題

- 是否可以根據時間應用不同的訪問級別？
  會。您可以建立不同的授權策略並將其連結到時間條件。

  舉例來說：
  在工作時間內完全訪問
  數小時後的只讀訪問
  週末不能訪問

- 如果系統時間不正確或不同步，會發生什麼情況？
  ISE可以應用不正確的策略或無法可靠地實施基於時間的規則。確保所有裝置和ISE節點使用同步的NTP源。

- 基於時間的策略是否可以與其他條件（例如，使用者角色、裝置型別）結合使用？
  會。時間條件可以與策略規則中的其他屬性結合使用，以建立精細且安全的訪問控制。

- TACACS中的shell和命令集是否支援基於時間的訪問+?
  會。基於時間的條件可以控制對裝置shell或特定命令集的訪問，具體取決於授權策略和配置檔案的構建方式。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。