ISEによるネットワークデバイスの時間ベースTACACS+アクセスの設定

内容

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)でデバイス管理ポリシーの日付と時刻に基づく認可を設定する方法について説明します。

前提条件

要件

Tacacsプロトコル(TACACS)およびIdentity Services Engine(ISE)の設定に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェアがインストールされたCisco Catalyst 9300スイッチCisco IOS® XE 17.12.5以降

- Cisco ISE リリース 3.3 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

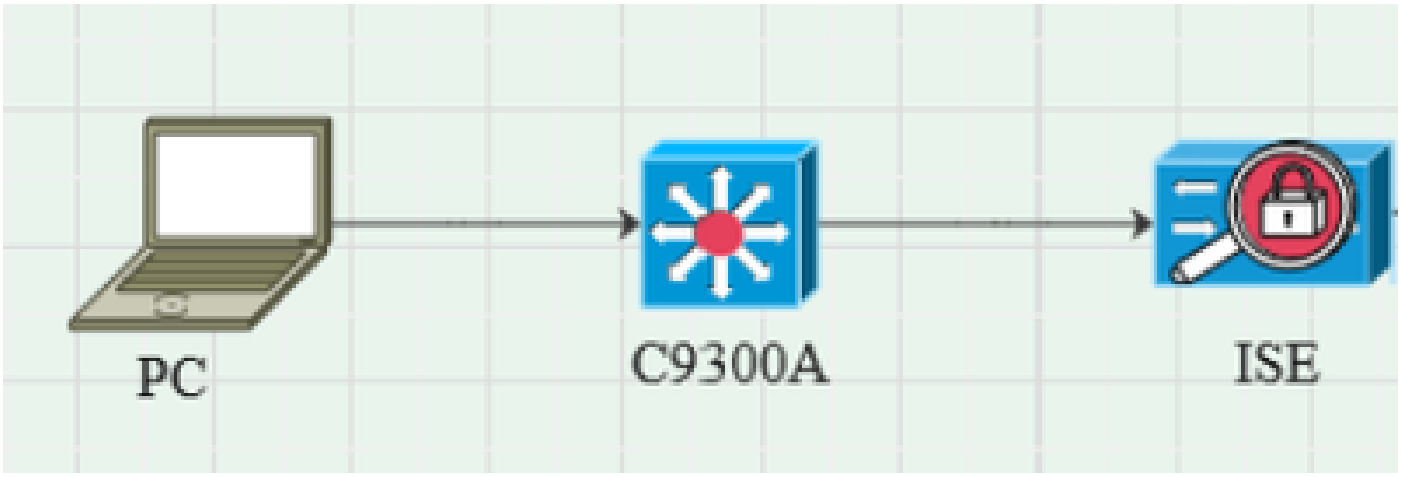
認可ポリシーは、Cisco Identity Services Engine(ISE)の主要コンポーネントであり、ネットワークリソースにアクセスする特定のユーザまたはグループのルールの定義と認可プロファイルの設定を可能にします。これらのポリシーは、条件を評価して、適用するプロファイルを決定します。ルールの条件が満たされると、対応する認可プロファイルが返され、適切なネットワークアクセスが付与されます。

また、Cisco ISEは日時条件もサポートします。日時条件を使用すると、指定した時間または日の間にのみポリシーを適用できます。これは、時間ベースのビジネス要件に基づいてアクセスコントロールを適用する場合に特に便利です。

このドキュメントでは、TACACS+管理アクセスを営業時間内（月曜日から金曜日の08:00 ~ 17:00）にのみ許可し、この時間枠外のアクセスを拒否する設定の概要について説明します。

設定

ネットワーク図



ISE の設定

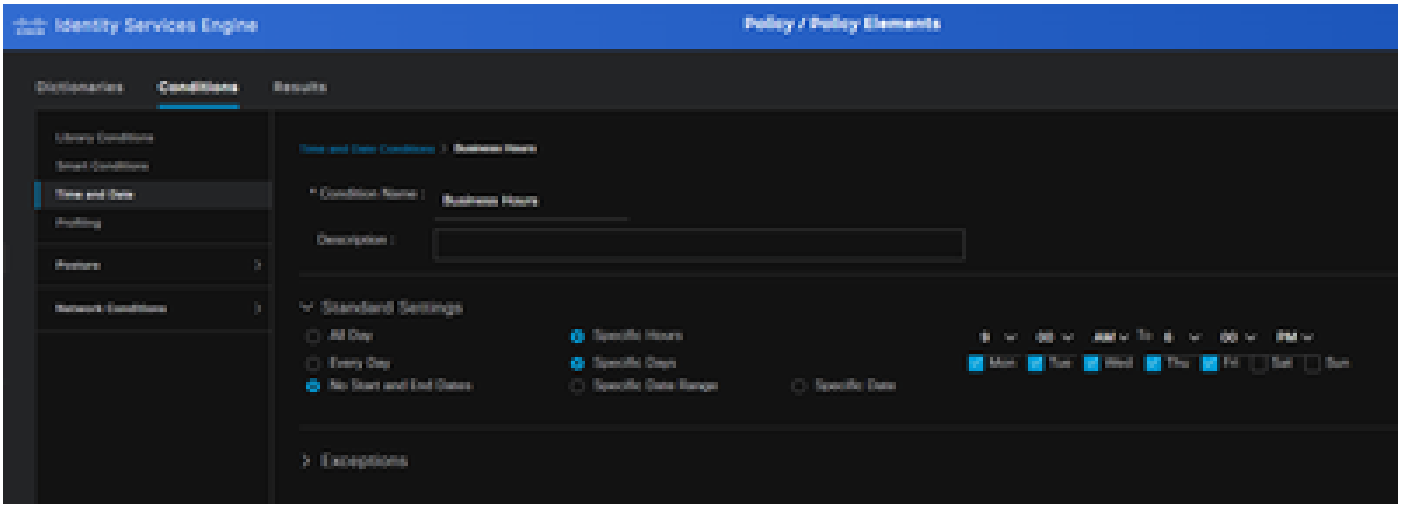
ステップ1：日時条件の作成

[ポリシー] > [ポリシー要素] > [条件] > [日付と時刻]に移動し、[追加]をクリックします。

条件名：営業時間

時間範囲の設定「標準設定」 > 「特定時間：09:00 AM - 06:00 PM」

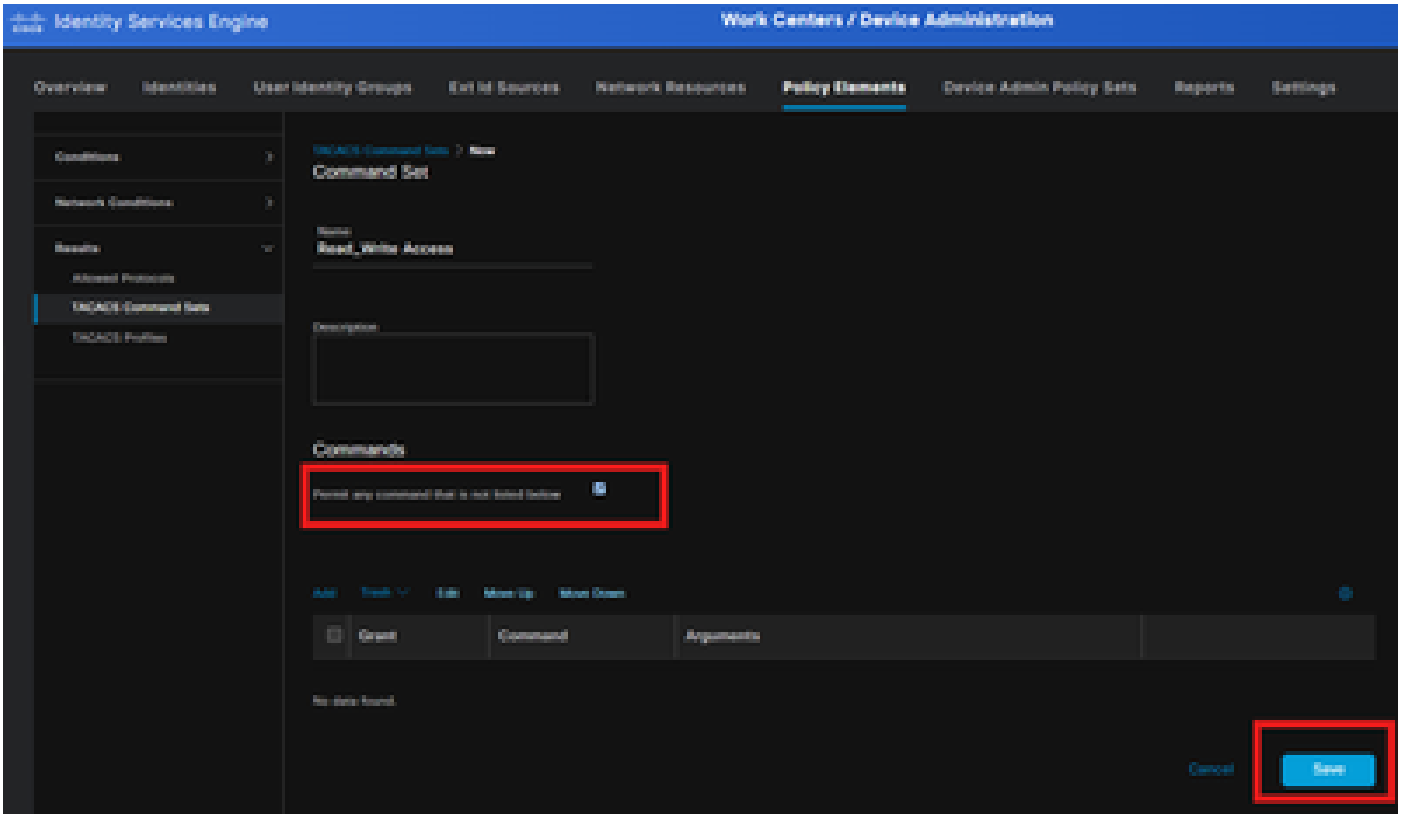
特定の日：月曜日から金曜日



ステップ2:TACACS+コマンドセットの作成

Work Centers > Device Administration > Policy Elements > Results > Tacacs Command Setsの順に移動します。

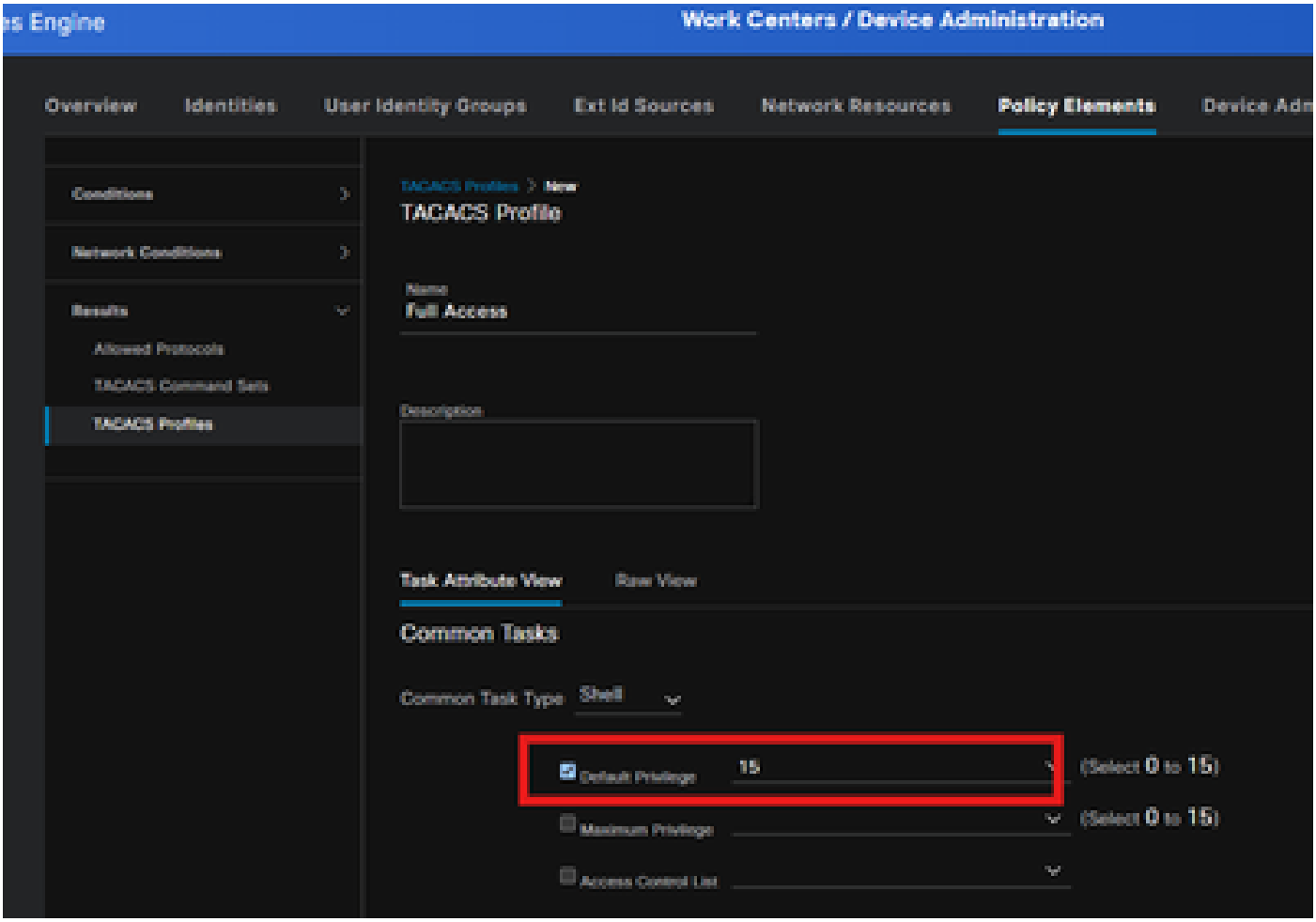
特定のCLIコマンドを制限する場合は、Permit any command that is not listed below チェックボックスを選択してコマンドセットを作成し、Submit をクリックするか、または制限されたコマンドを追加します。



ステップ3:TACACS+プロファイルの作成

Work Centers > Device Administration > Policy Elements > Results > TACACS Profilesの順に移動します。[Add] をクリックします。

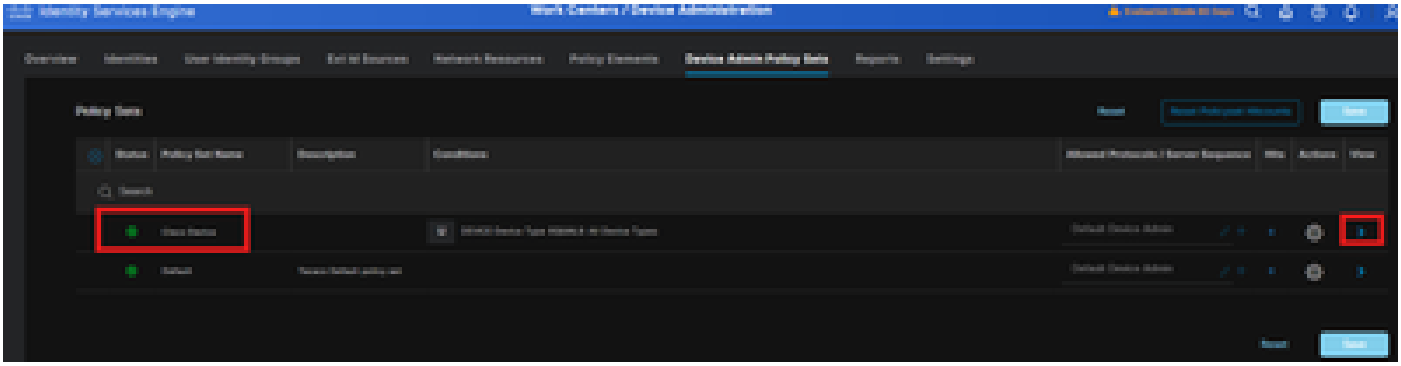
Command Task Type as Shell、Default Privilegeの順に選択して、値15を入力します。[Submit] をクリックします。



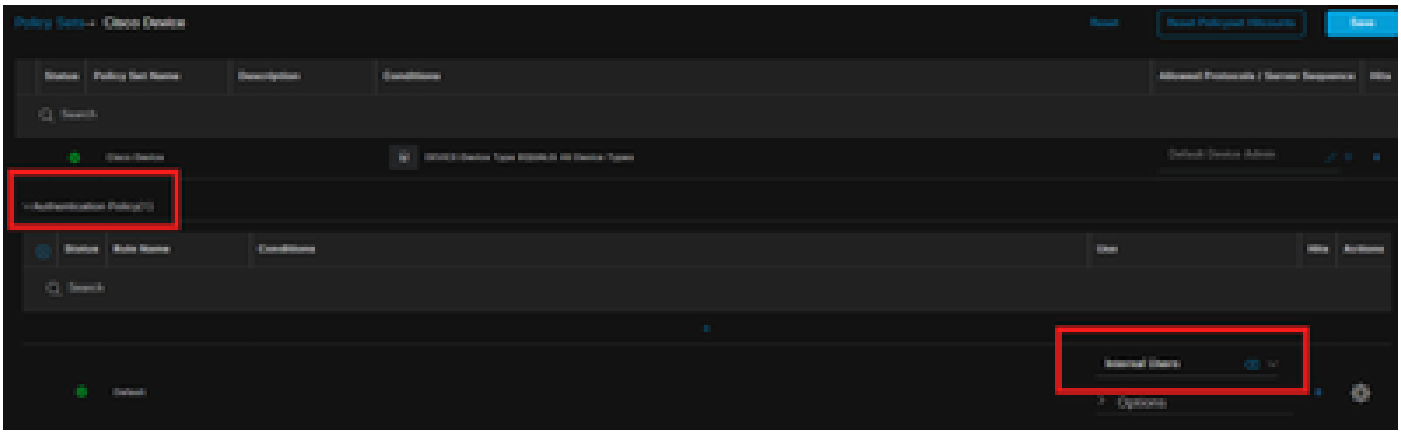
ステップ4:TACACS認可ポリシーの作成

Work Centers > Device Administration > Device Admin Policy Setsの順に移動します。

アクティブなポリシーセットを選択します。



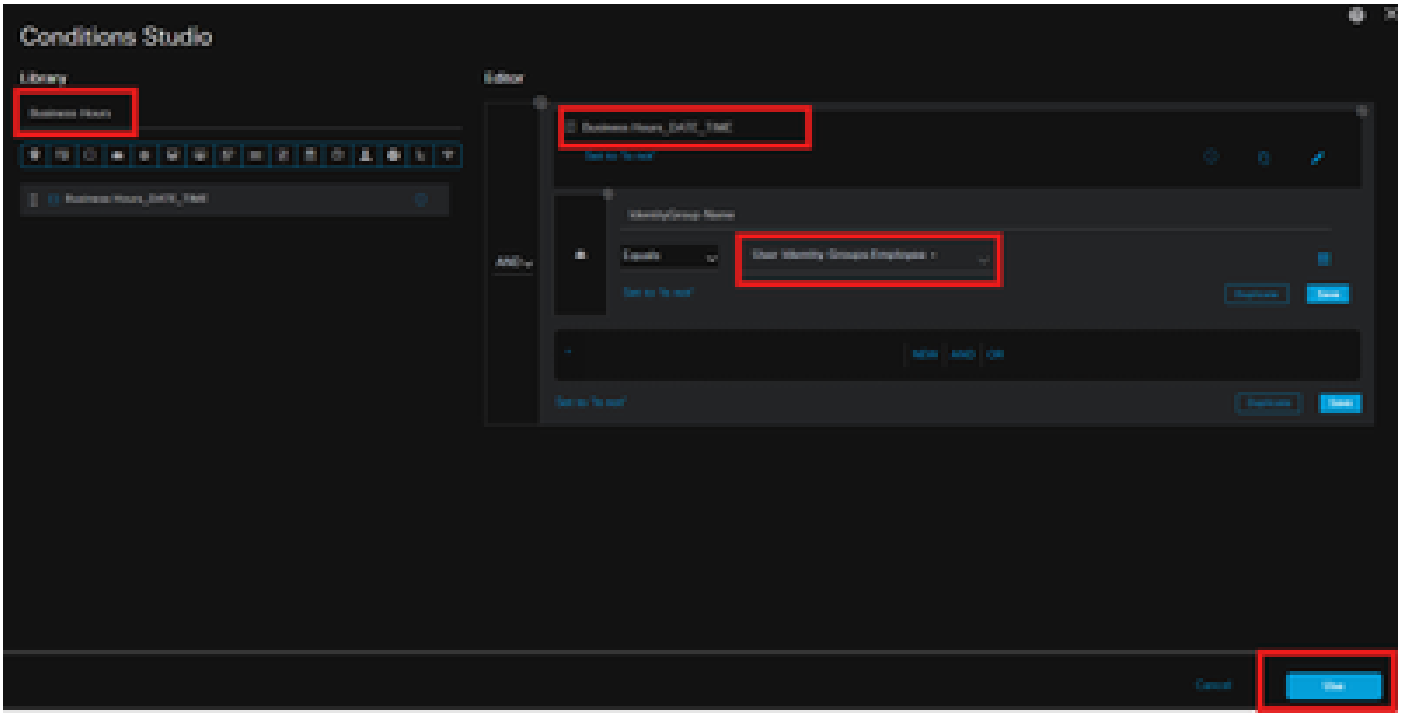
内部ユーザまたはActive Directoryユーザに基づいて認証ポリシーを設定します。



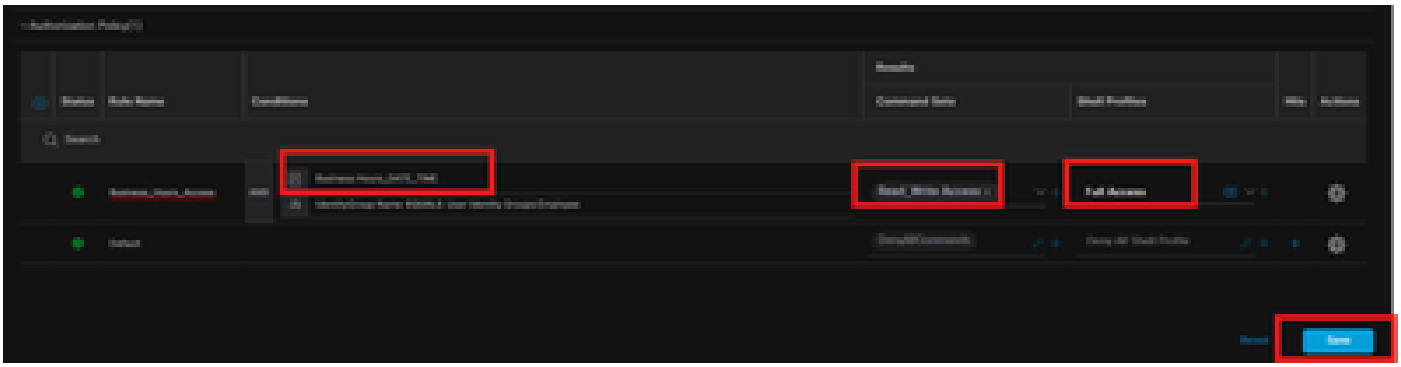
Authorization Policyセクションで、Add Ruleをクリックしてルール名を指定し、+をクリックして認可条件を追加します。

新しいCondition Studioウィンドウが表示されます。Search by Nameフィールドに、ステップ1で作成した名前を入力し、Editorにドラッグします。

ユーザグループに基づいて条件を追加し、Saveをクリックします。



Resultsで、ステップ2とステップ3で作成したTACACS Command SetとShell Profileを選択し、Saveをクリックします。



スイッチの設定

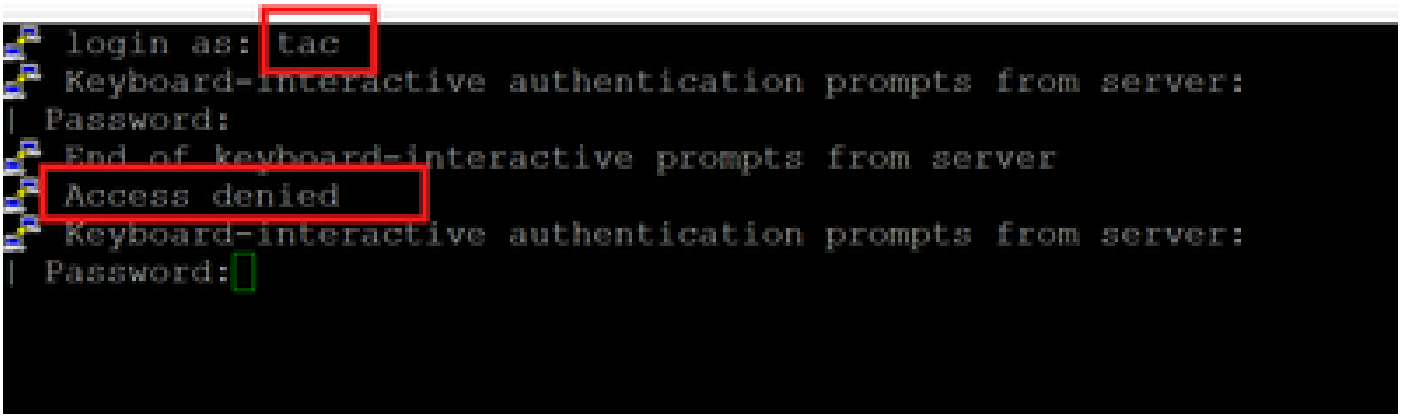
aaa new-model

aaa authentication login default local group tacacs+(aaa authentication login default local group tacacs+)
aaa authentication enable default enable group tacacs+(aaa authentication enable default enable group tacacs+)
aaa authorization configコマンド
aaa authorization exec default local group tacacs+ (aaa許可execデフォルトローカルグループ tacacs+)
aaa authorizationコマンド0 default local group tacacs+
aaa authorizationコマンド1 default local group tacacs+
aaa authorizationコマンド15 default local group tacacs+

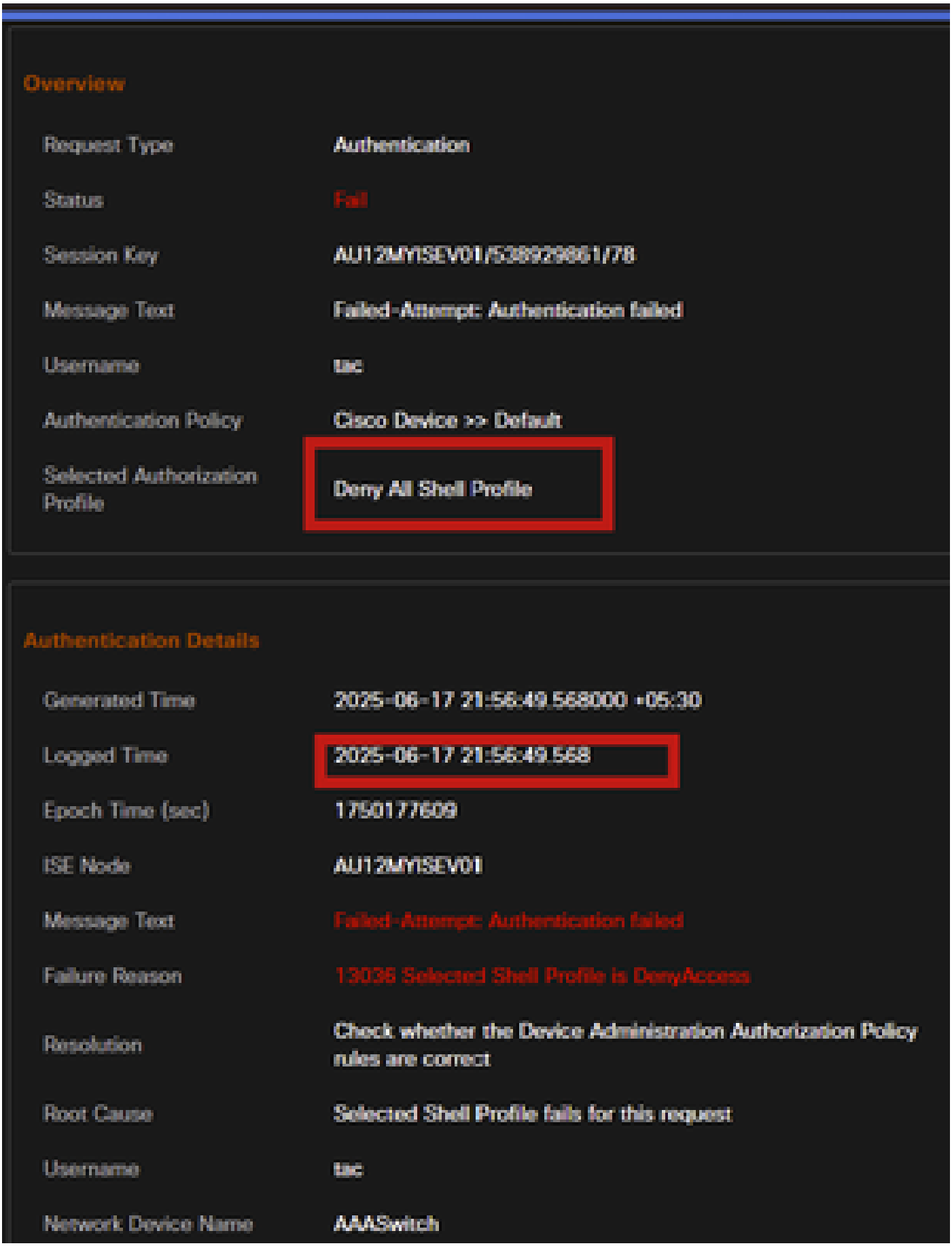
tacacsサーバISE
アドレスipv4 10.127.197.53
キーQwerty123

確認

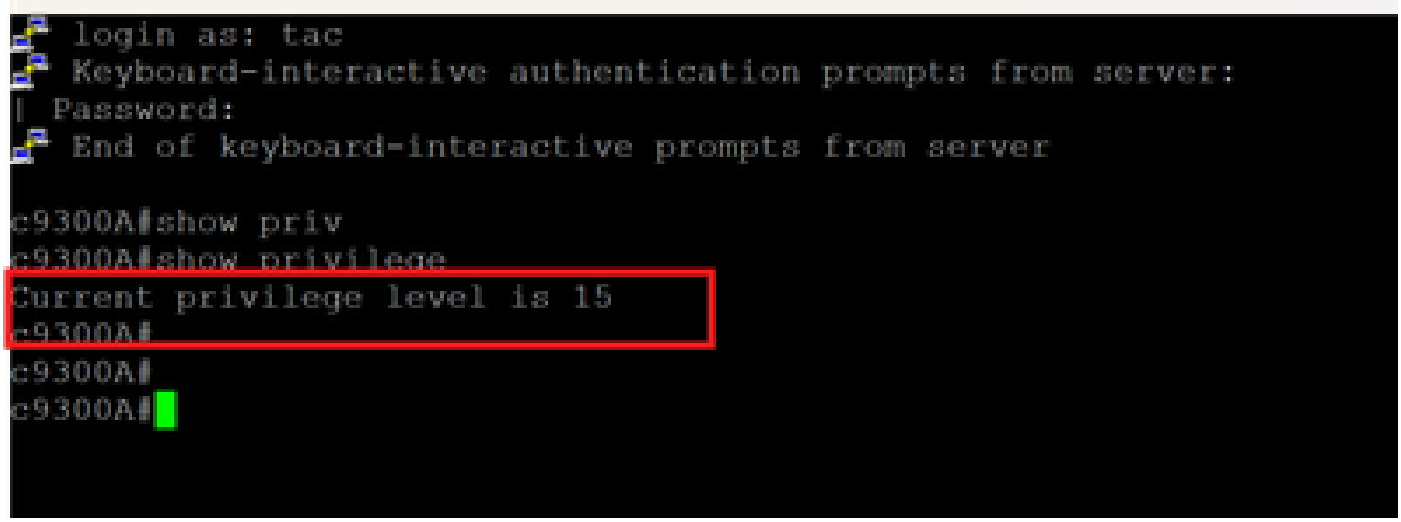
営業時間外にスイッチへのSSHを試行したユーザが、ISEからアクセス拒否を受け取りました。



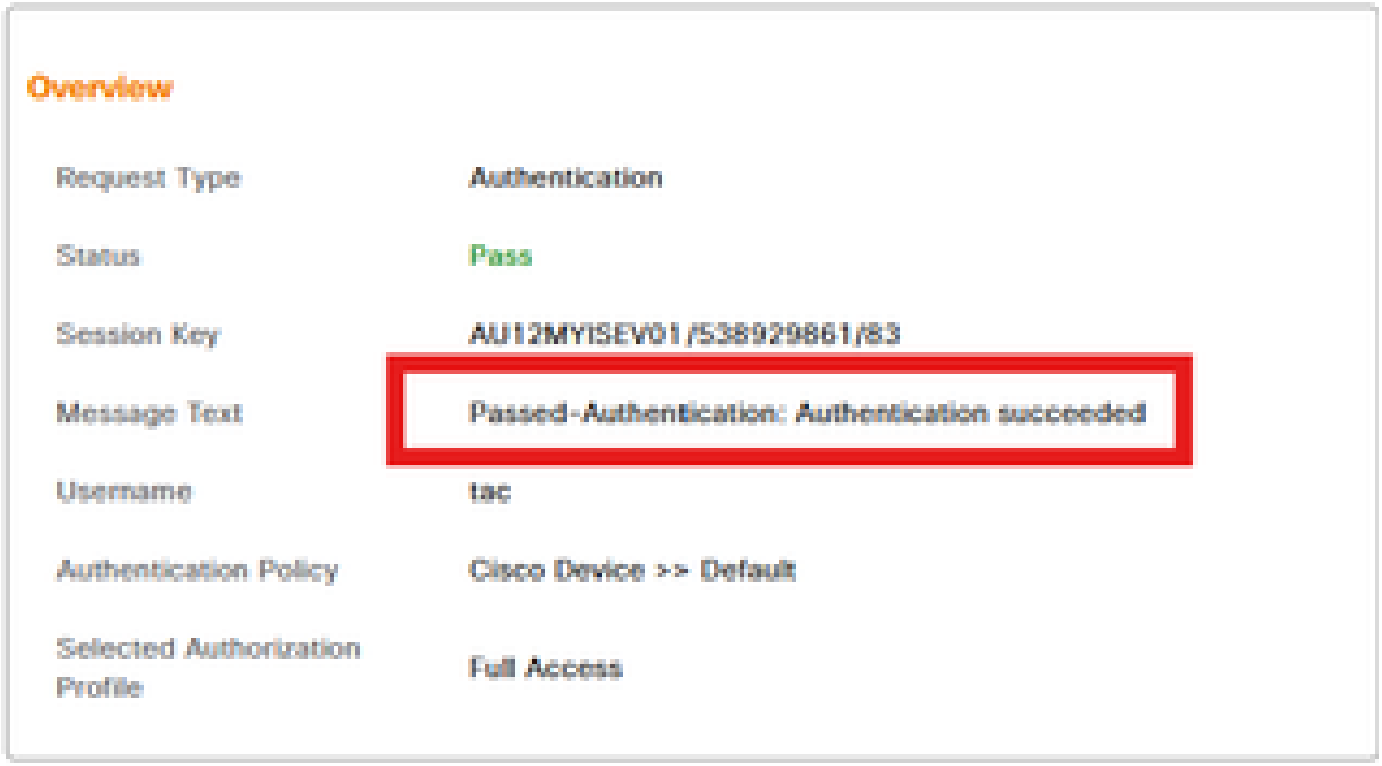
ISEライブログは、許可ポリシーの日時の条件が一致しなかったため許可に失敗し、その結果セッションがデフォルトの拒否アクセスルールに一致したことを示しています。



営業時間中にスイッチにSSH接続して、読み取り/書き込みアクセスを取得しようとしたユーザ：

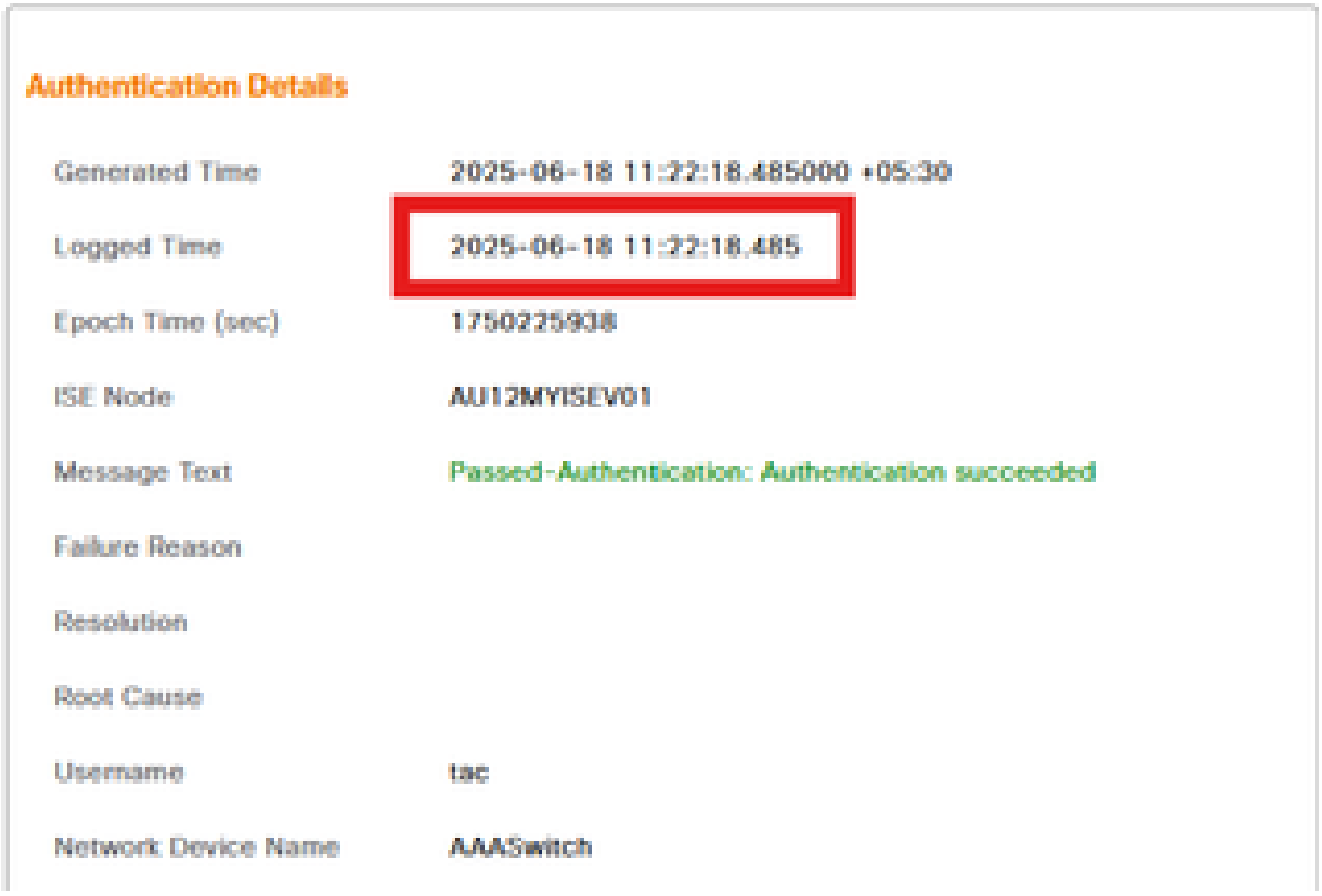


ISEライブログは、営業時間内のログインが日時の条件に一致し、正しいポリシーに一致したことを示しています。



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

トラブルシュート

ISE でのデバッグ

デバッグレベルで設定する次の属性を持つISEサポートバンドルを収集します。

- ルールエンジン – ポリシー – グループ
- ルールエンジン属性
- ポリシーエンジン
- EPM-PDP
- EPM-PIP

時刻と日付の条件が原因で営業時間外にスイッチへのSSHを試行するユーザが、設定された営業時間と一致しない場合。

show logging application ise-psc.log（隠しコマンド）

```
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][]
cpm.policy.eval.utils.RuleUtil -::::-
360158683110.127.197.5449306Authentication3601586831：評価ルール – <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 -::::- 360158683110.120
7.197.5449306Authentication3601586831：条件をid - 72483811-ba39-4cc2-bdac-90a38232b95e
- LHS operandId - operandId, operator DATETIME_MATCHES, RHS operandId - rhsoperandで評
価しています
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][]
cpm.policy.eval.utils.ConditionUtil -::::-
360158683110.127.197.5449306Authentication3601586831：条件lhsoperand値 –
com.cisco.cpm.policy.DTConstraint@6924136c , rhsoperand値 –
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：条件の評価結果 – 72483811-ba39-
4cc2-bdac-90a38232b95e returned - false
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][]]
cpm.policy.eval.utils.RuleUtil -::::-
360158683110.127.197.5449306Authentication3601586831：条件の結果の設定： 72483811-
ba39-4cc2-bdac-90a38232b95e : false
```

営業時間内にスイッチへのSSHを試行したユーザが、日時の条件に一致した日時。

show logging application ise-psc.log（隠しコマンド）

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]
cpm.policy.eval.utils.RuleUtil -:::-
181675991110.127.197.5414126Authentication1816759911：評価ルール – <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 -::::- 181675991110.12 7.197.5414126Authentication1816759911: id
- 72483811-ba39-4cc2-bdac-90a38232b95e - LHS operandId - operandId、operator
DATETIME_MATCHES、RHS operandId - rhsoperandで条件を評価しています
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]
cpm.policy.eval.utils.ConditionUtil -::::-
181675991110.127.197.5414126Authentication1816759911：条件lhsoperand値 –
com.cisco.cpm.policy.DTConstraint@4af10566 , rhsoperand値 –
com.cisco.cpm.policy.DTConstraint@2bdb62e9
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::-
181675991110.127.197.5414126Authentication1816759911：条件の評価結果 – 72483811-ba39-
4cc2-bdac-90a38232b95e returned - true
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::-
181675991110.127.197.5414126Authentication1816759911：条件の設定結果： 72483811-ba39-
4cc2-bdac-90a38232b95e : true
```

関連情報

- Cisco ISE Device Administration規範的導入ガイド

よく寄せられる質問（FAQ）

- 時間に基づいて異なるアクセスレベルを適用できますか。
  はい。異なる認可ポリシーを作成して、それらを時間条件にリンクできます。

  例：
  営業時間中のフルアクセス
  営業時間外の読み取り専用アクセス
  週末はアクセス不可

- システム時刻が不正確または同期されていない場合はどうなりますか。
  ISEは誤ったポリシーを適用したり、時間ベースのルールを確実に適用しなかったりします。すべてのデバイスとISEノードが同期されたNTPソースを使用していることを確認します。

- 時間ベースのポリシーを他の条件（ユーザロール、デバイスタイプなど）と組み合わせて使用できますか。
  はい。時間条件をポリシールール内の他の属性と組み合わせて、きめ細かく安全なアクセスコントロールを作成できます。

- TACACSのシェルセットとコマンドセットの両方で時間ベースアクセスがサポートされている+?

はい。時間ベースの条件により、認可ポリシーとプロファイルの構造に応じて、デバイスシェルまたは特定のコマンドセットへのアクセスを制御できます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。