Configuration de l'accès TACACS+ basé sur le temps pour les périphériques réseau avec ISE

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Diagramme du réseau
  - Configuration d'ISE
    - Étape 1 : Créer une condition de date et heure
    - Étape 2 : Créer un jeu de commandes TACACS+
    - Étape 3 : Créer un profil TACACS+
    - Étape 4 : Créer une politique d'autorisation TACACS
  - Configurer le commutateur
  - Vérifier
- Dépannage
  - Débogages sur ISE
- Informations connexes
- Forum aux questions

Introduction

Ce document décrit comment configurer l'autorisation basée sur l'heure et la date pour la politique d'administration des périphériques dans Cisco Identity Services Engine (ISE).

Conditions préalables

Exigences

Cisco vous recommande de connaître le protocole Tacacs et la configuration ISE (Identity Services Engine).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateur Cisco Catalyst 9300 avec logicielCisco IOS® XE 17.12.5 et versions

ultérieures
- Cisco ISE, versions 3.3 et ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

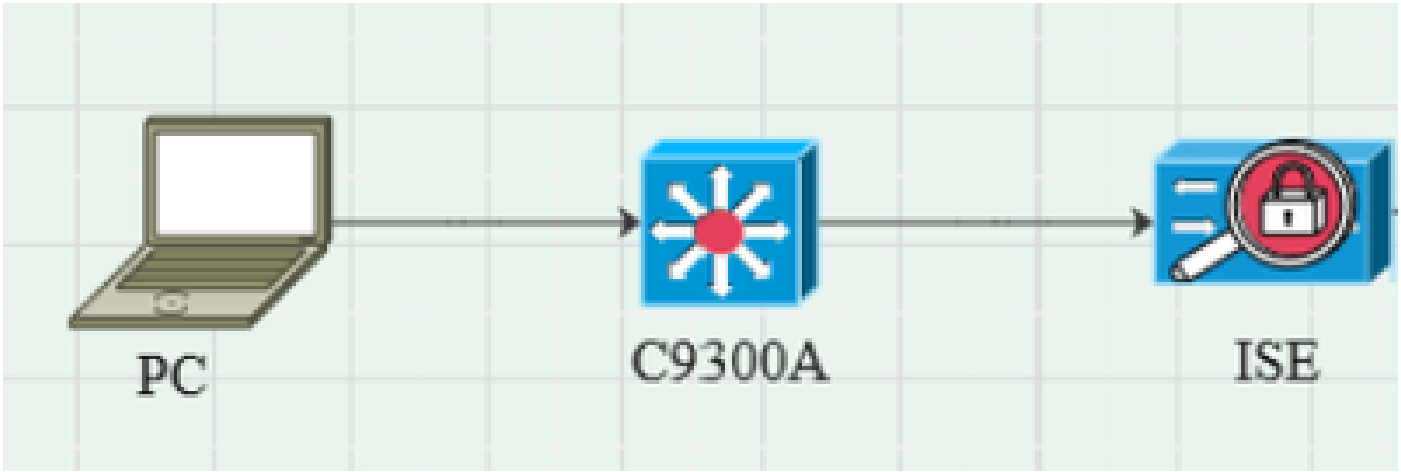
Les stratégies d'autorisation sont un composant clé de Cisco Identity Services Engine (ISE). Elles vous permettent de définir des règles et de configurer des profils d'autorisation pour des utilisateurs ou des groupes spécifiques accédant à des ressources réseau. Ces politiques évaluent les conditions pour déterminer le profil à appliquer. Lorsque les conditions d'une règle sont remplies, le profil d'autorisation correspondant est renvoyé, ce qui permet d'accorder l'accès au réseau approprié.

Cisco ISE prend également en charge les conditions d'heure et de date, qui permettent d'appliquer les politiques uniquement pendant des heures ou des jours spécifiés. Cela est particulièrement utile pour appliquer des contrôles d'accès basés sur des exigences métier basées sur le temps.

Ce document décrit la configuration permettant d'autoriser l'accès administratif TACACS+ aux périphériques réseau uniquement pendant les heures de bureau (du lundi au vendredi, de 8 h 00 à 17 h 00) et de refuser l'accès en dehors de cette fenêtre.

Configurer

Diagramme du réseau



Configuration d'ISE

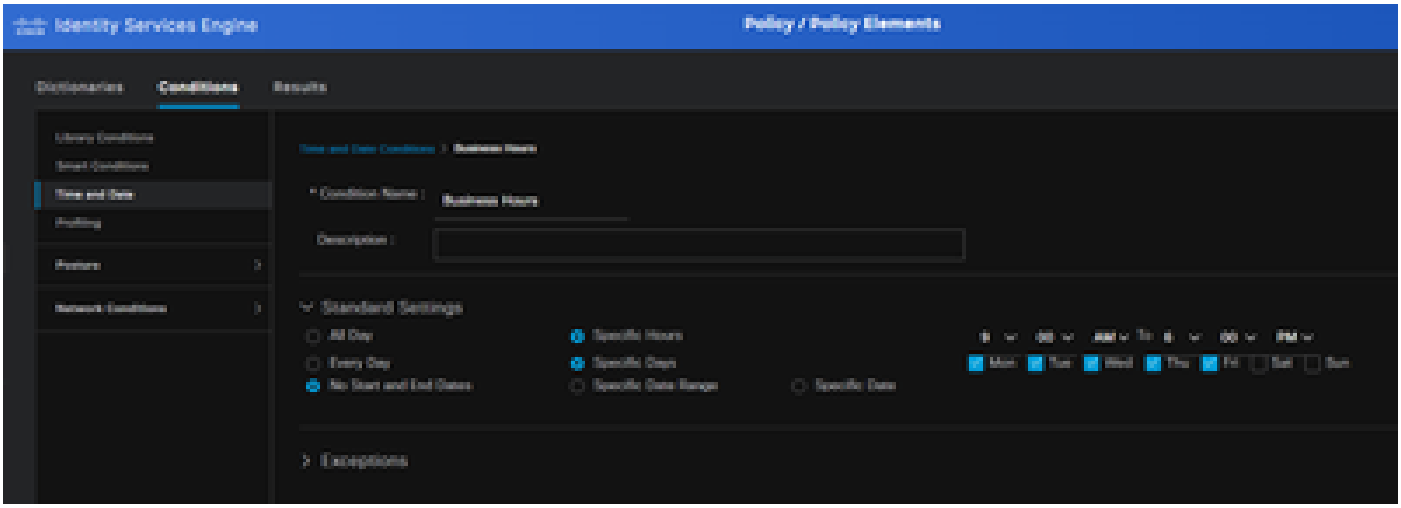
Étape 1 : Créer une condition de date et heure

Accédez à Policy > Policy Elements > Conditions > Time and Date, puis cliquez sur Add.

Nom de la condition : Heures ouvrables

Définissez la plage horaire Paramètres standard > Heures spécifiques : 09:00 AM - 06:00 PM

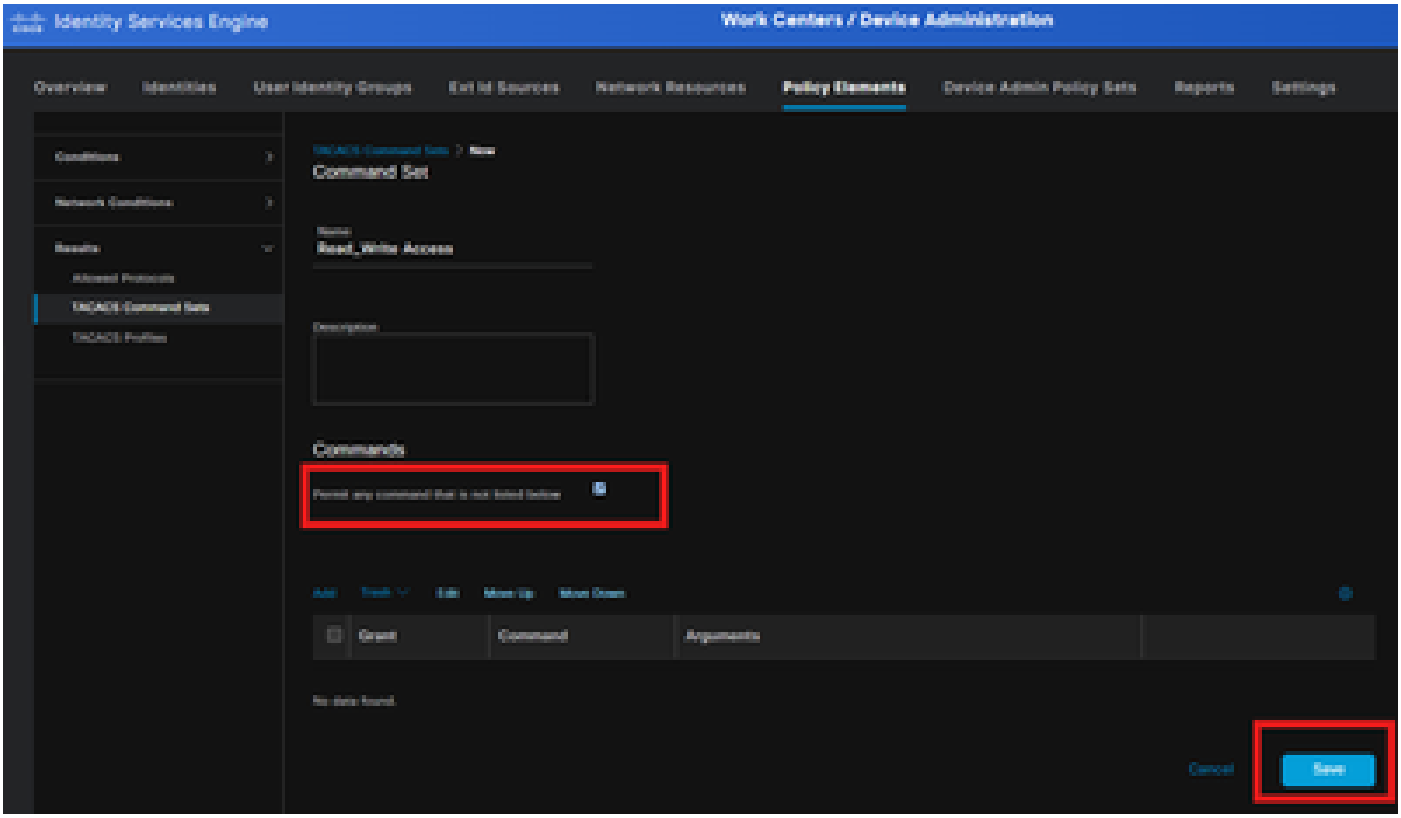
Jours spécifiques : Du lundi au vendredi



Étape 2 : Créer un jeu de commandes TACACS+

Accédez à Work Centers > Device Administration > Policy Elements > Results > Tacacs Command Sets.

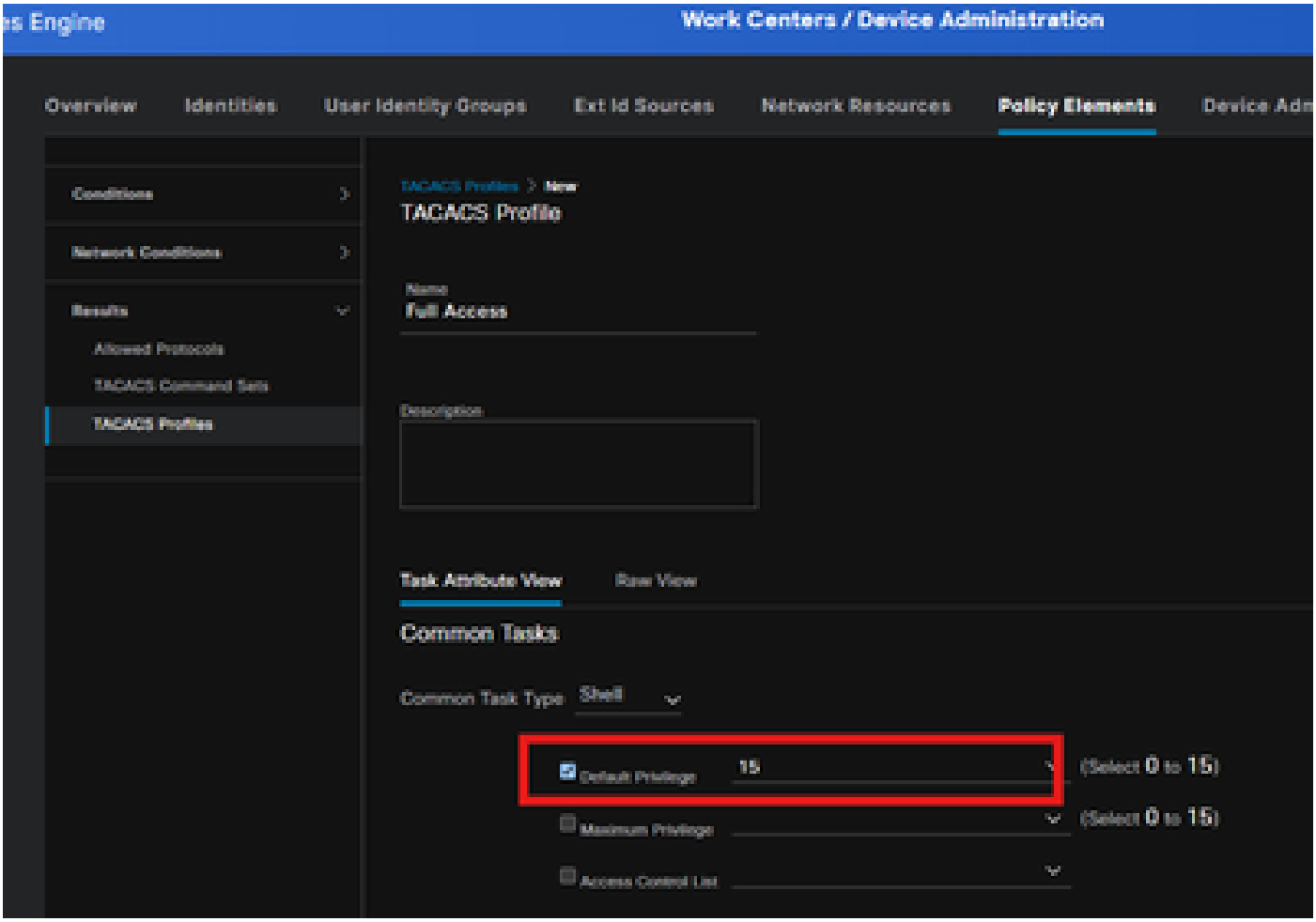
Créez un jeu de commandes en sélectionnant la case à cocher Autoriser toute commande qui n'est pas répertoriée ci-dessous et cliquez sur Envoyer ou ajoutez les commandes limitées si vous souhaitez restreindre certaines commandes CLI.



Étape 3 : Créer un profil TACACS+

Accédez à Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Cliquez sur Add.

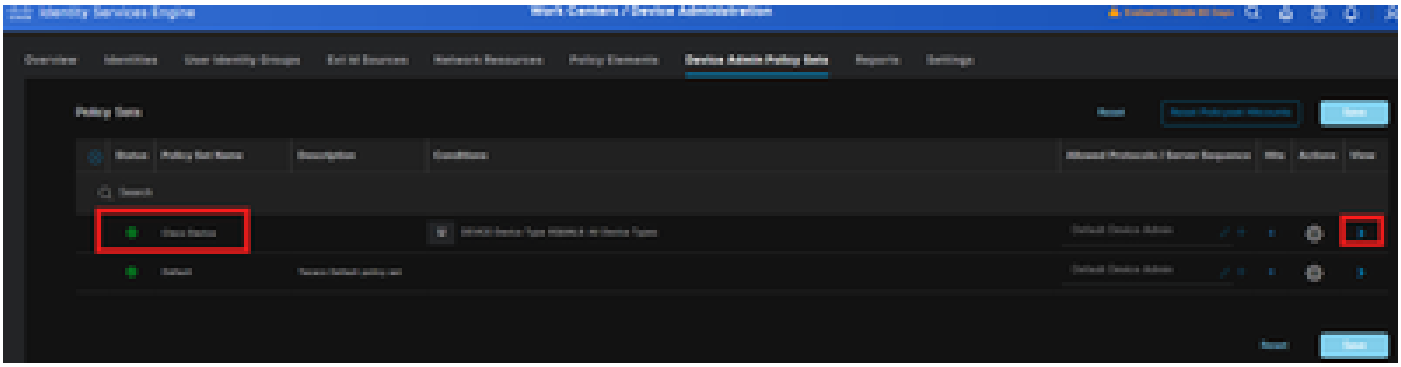
Sélectionnez Command Task Type comme Shell, puis la case à cocher Default Privilege et entrez la valeur 15. Cliquez sur Submit.



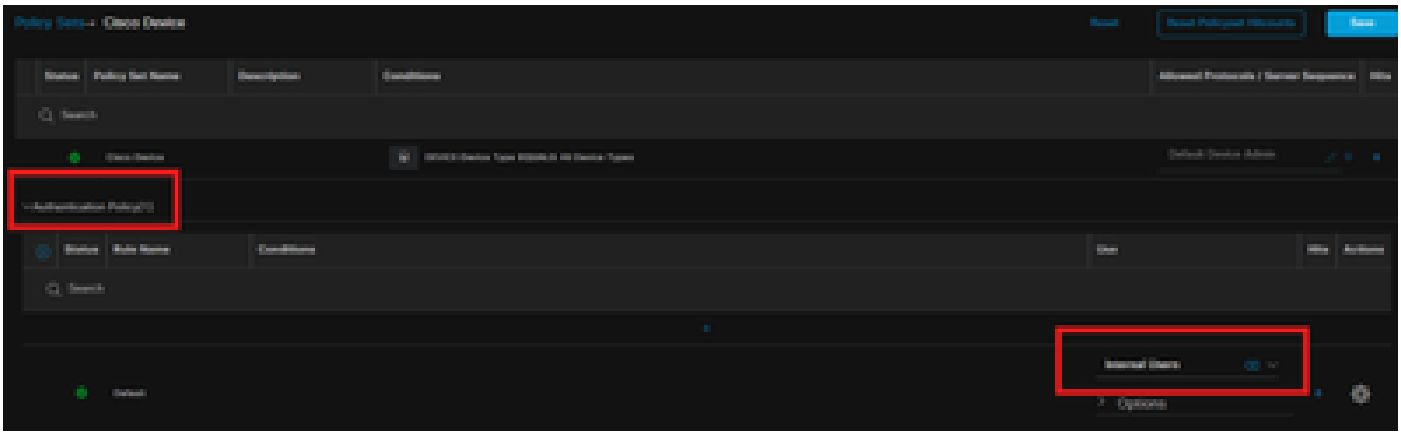
Étape 4 : Créer une politique d'autorisation TACACS

Accédez à Work Centers > Device Administration > Device Admin Policy Sets.

Sélectionnez votre jeu de stratégies actif.



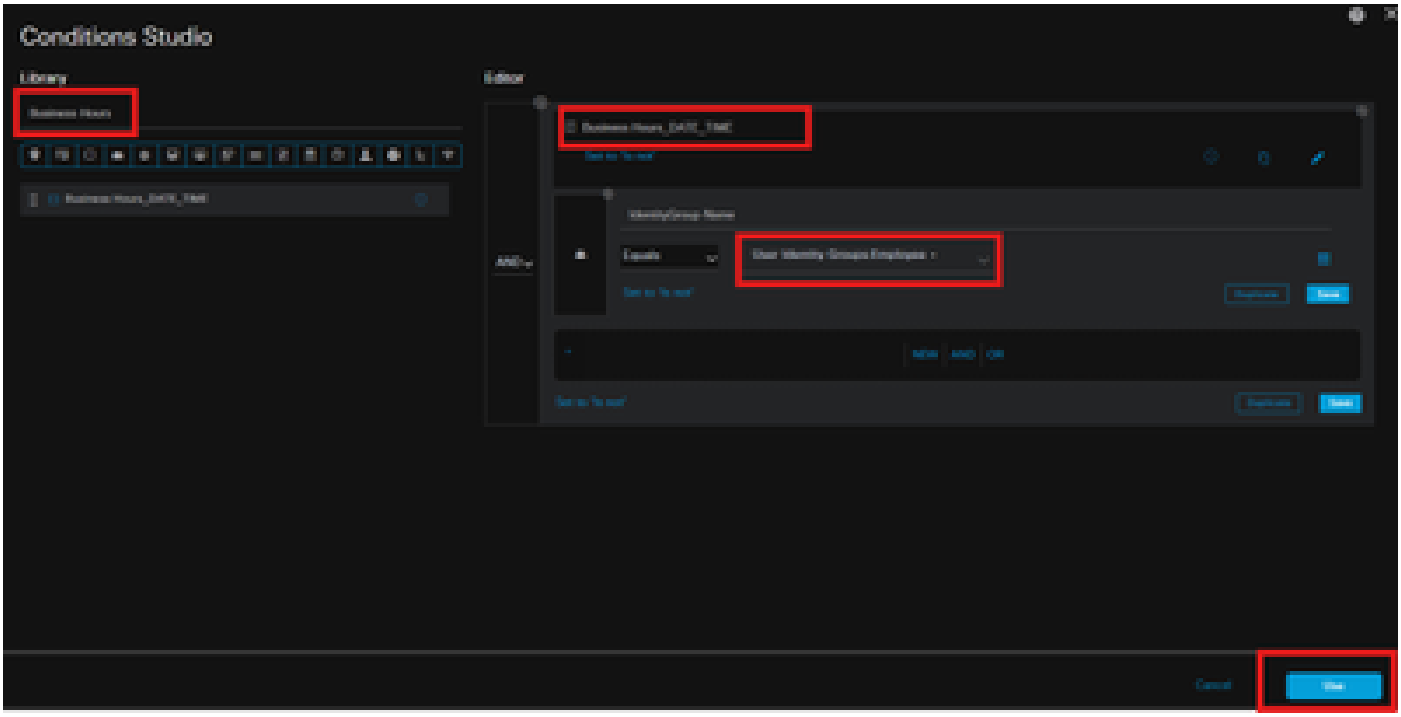
Configurez la stratégie d'authentification en fonction des utilisateurs internes ou Active Directory.



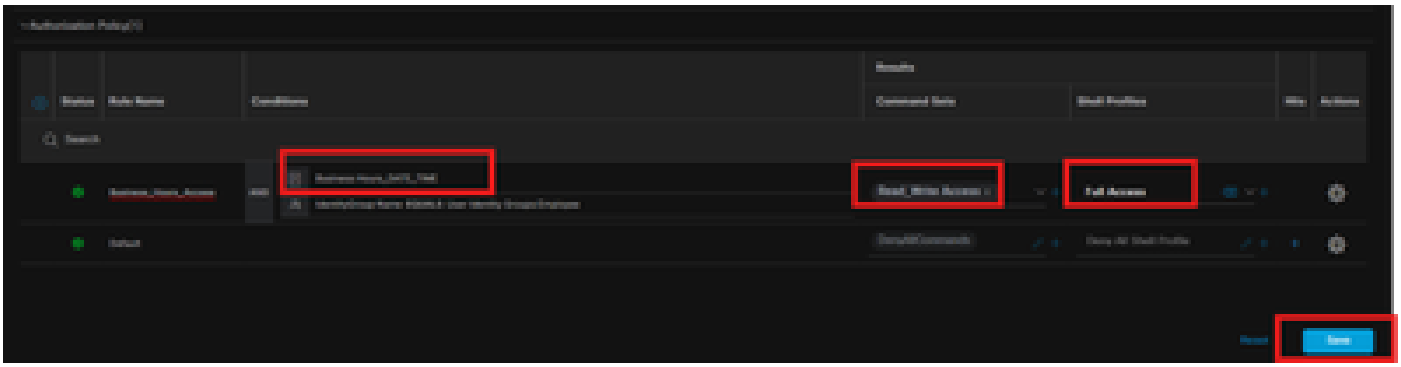
Dans la section Stratégie d'autorisation, cliquez sur Ajouter une règle pour fournir le nom de la règle, puis cliquez sur + pour ajouter des conditions d'autorisation.

Une nouvelle fenêtre Condition Studio s'affiche, dans le champ Search by Name, saisissez le nom créé à l'étape 1 et faites-le glisser vers l'éditeur.

Ajoutez des conditions supplémentaires basées sur le groupe d'utilisateurs et cliquez sur Enregistrer.



Dans Résultats, sélectionnez le jeu de commandes Tacacs et le profil de shell créés à l'étape 2 et à l'étape 3, puis cliquez sur Enregistrer.

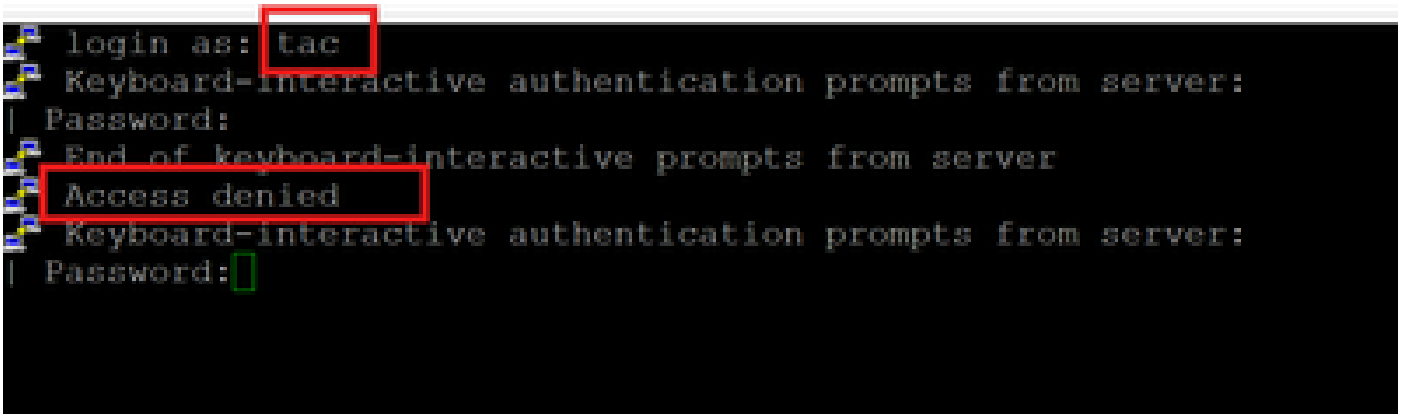


Configurer le commutateur

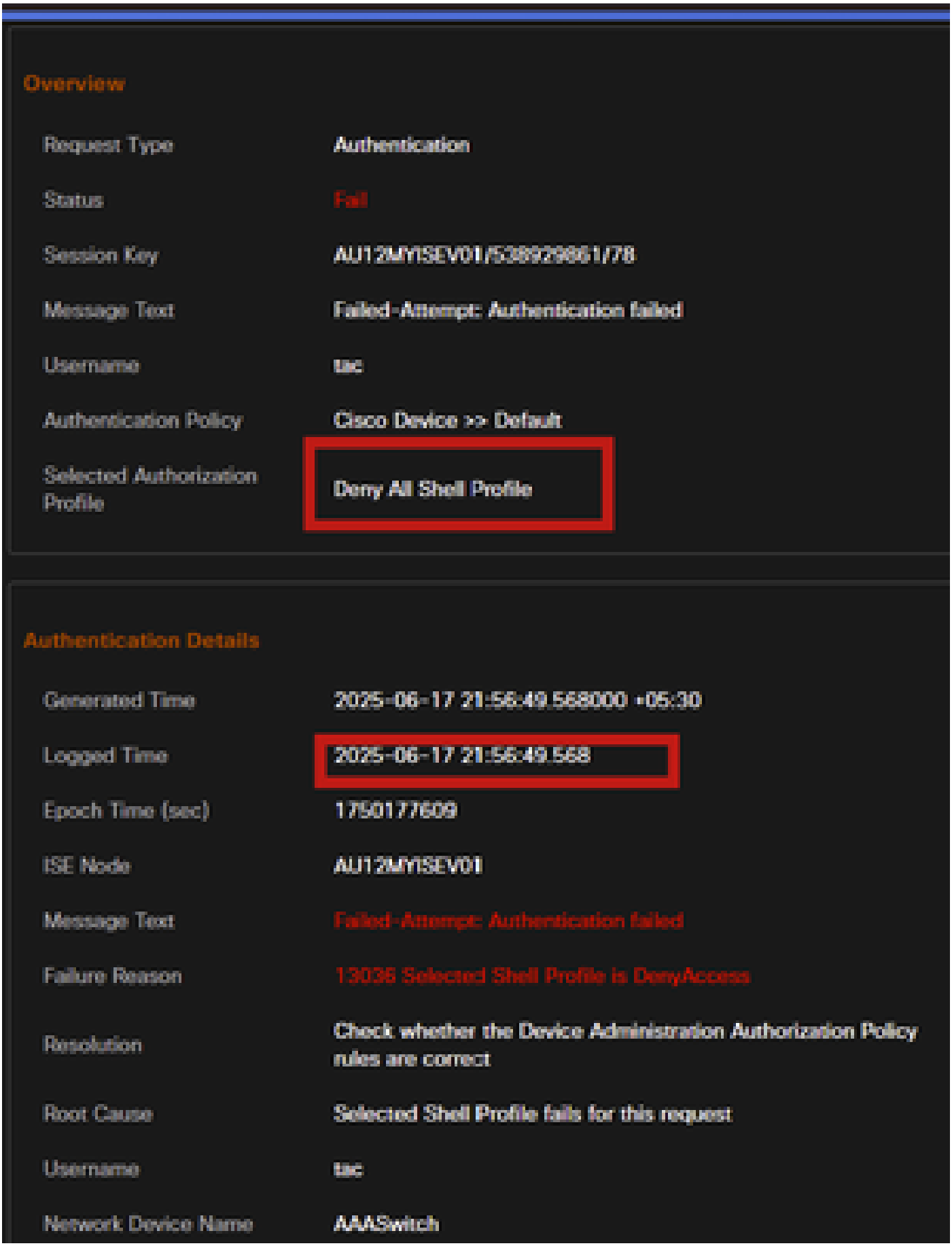
```
aaa new-model

aaa authentication login default local group tacacs+
aaa authentication enable default enable group tacacs+
aaa authorization config-commands
aaa authorization exec groupe local par défaut tacacs+
aaa authorization commandes 0 default local group tacacs+
aaa authorization, commandes 1 groupe local par défaut tacacs+
aaa authorization, commandes 15 groupe local par défaut tacacs+

serveur TACACS ISE
address ipv4 10.127.197.53
clé Qwerty123
```

Vérifier

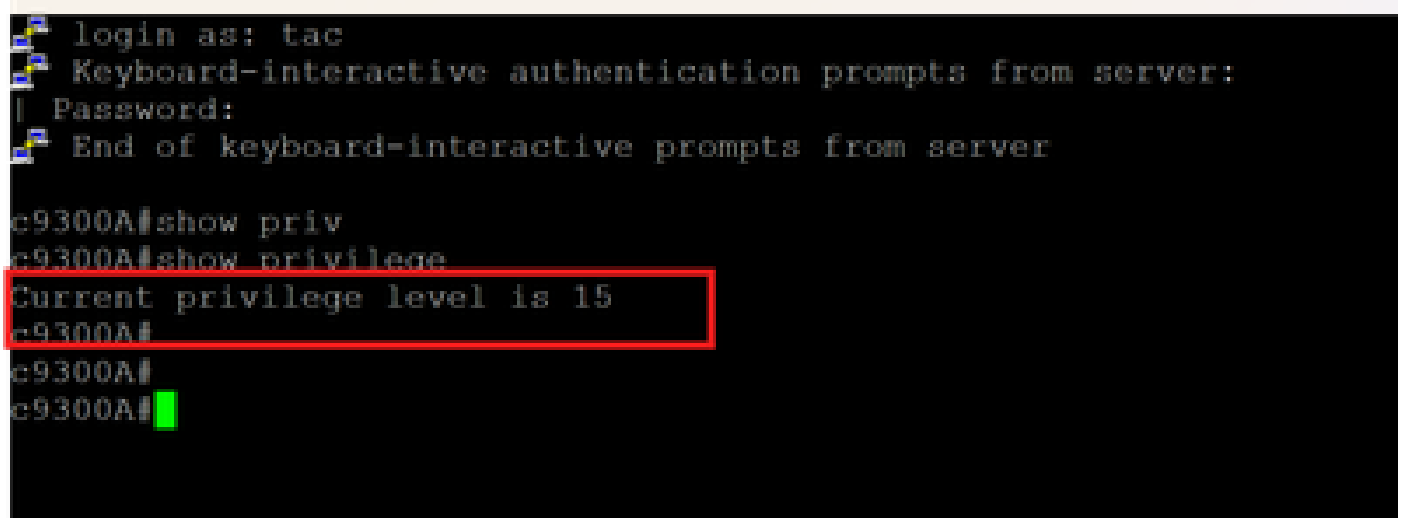
L'utilisateur qui tente d'établir une connexion SSH avec le commutateur en dehors des heures d'ouverture se voit refuser l'accès par ISE.



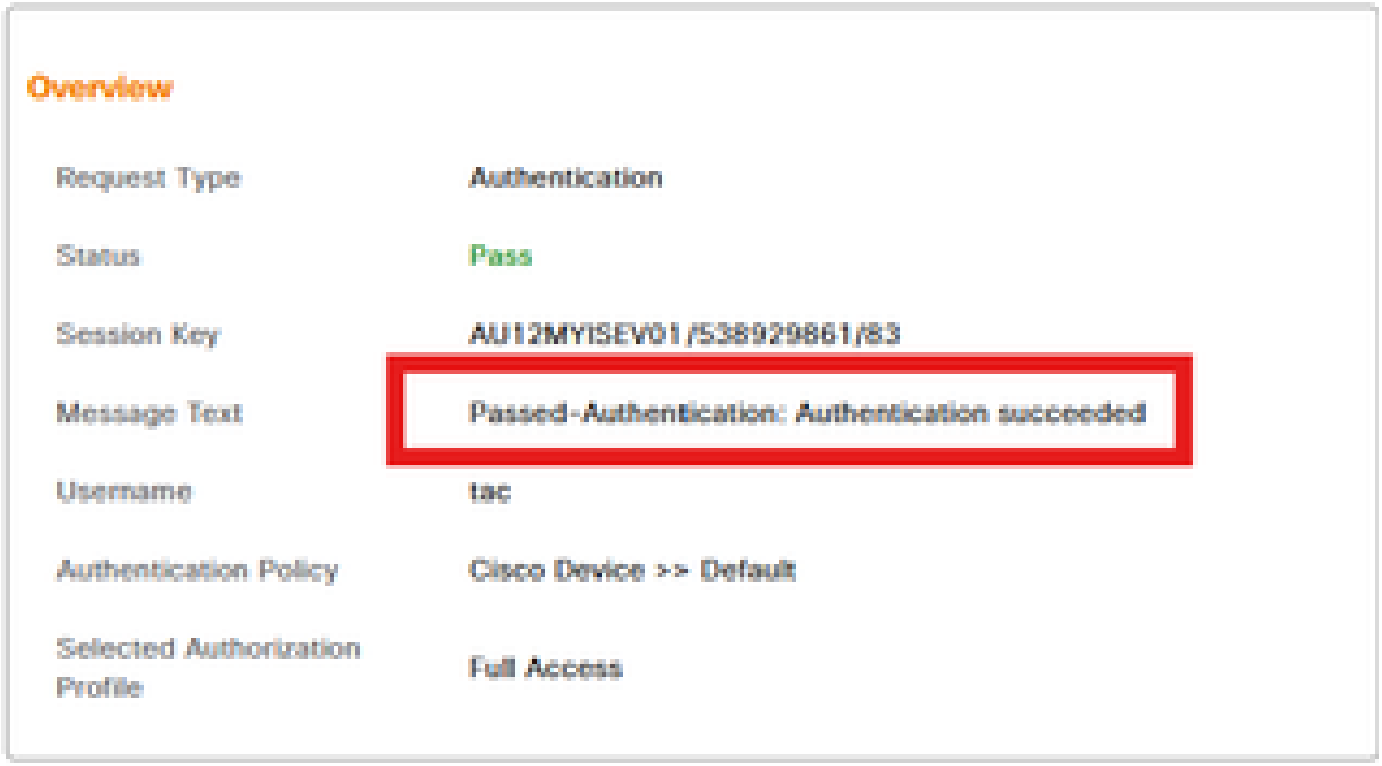
Les journaux en direct ISE indiquent que l'autorisation a échoué car la condition Heure et Date de la stratégie d'autorisation ne correspondait pas, ce qui a entraîné l'application de la règle Refuser l'accès par défaut à la session.

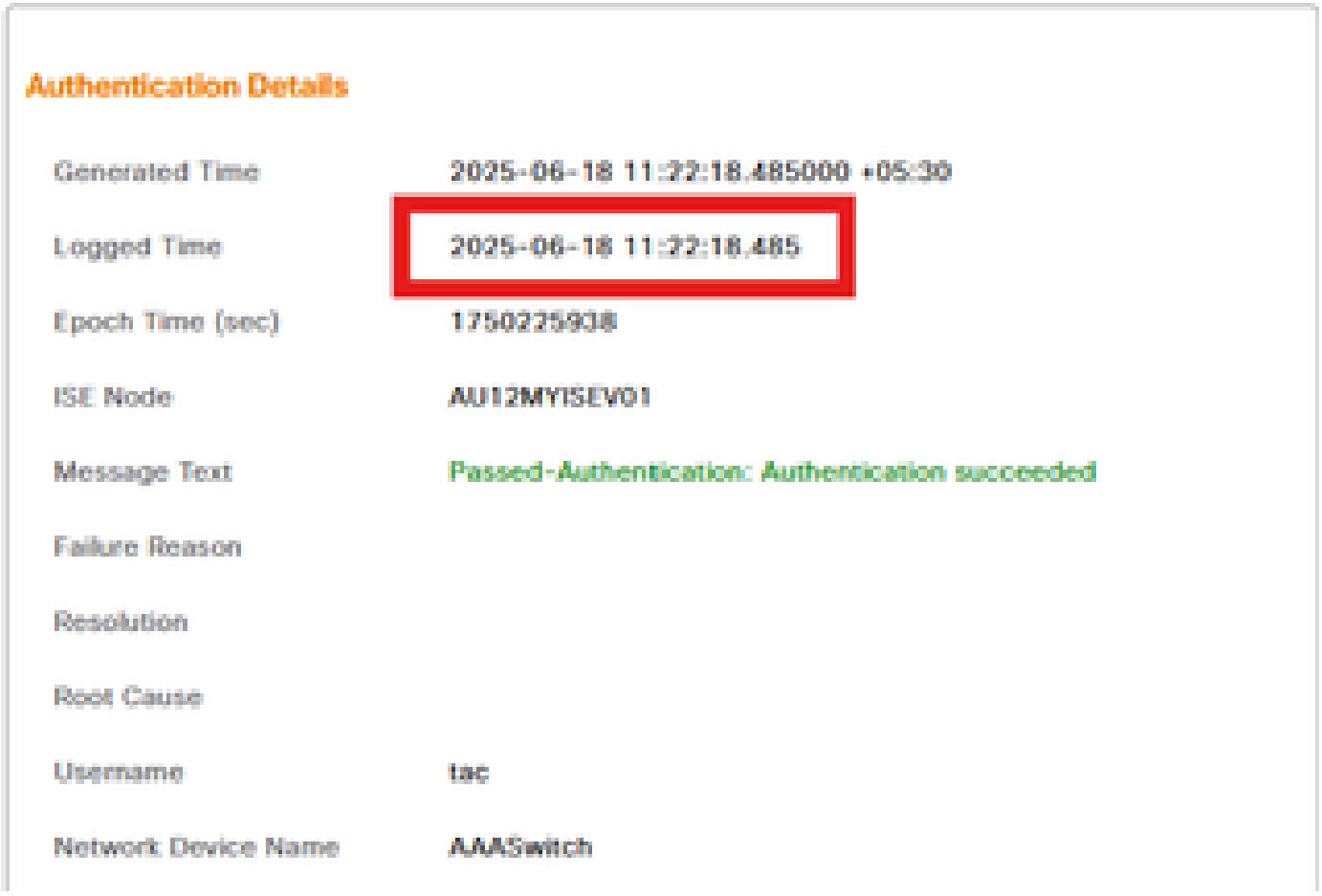


Utilisateur essayant d'établir une connexion SSH dans le commutateur pendant les heures ouvrées et d'obtenir un accès en lecture/écriture :



Le journal en direct d'ISE indique que la connexion pendant les heures d'ouverture correspond à la condition Heure et date et atteint la stratégie correcte.





Dépannage

Débogages sur ISE

Collectez le bundle de support ISE avec ces attributs à définir au niveau du débogage :

- RuleEngine-Policy-IDGroups
- RuleEngine-Attributes
- Policy-Engine
- epm-pdp
- epm-pip

Lorsque l'utilisateur tente d'établir une connexion SSH avec le commutateur en dehors des heures de bureau en raison de la condition d'heure et de date ne correspond pas aux heures de bureau configurées.

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 :
Évaluation de la règle - <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 :
Évaluation de la condition avec l'id - 72483811-ba39-4cc2-bdac-90a38232b95e - LHS operandId -
operandId, opérateur DATETIME_MATCHES, RHS operandId - rhsoperand
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.ConditionUtil -::::-
360158683110.127.197.5449306Authentication3601586831 : Condition 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 :
Résultat de l'évaluation pour Condition - 72483811-ba39-4cc2-bdac-90a38232b95e renvoyé -
false
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831 :
Définition du résultat pour la condition : 72483811-ba39-4cc2-bdac-90a38232b95e : falsifié
```

Lorsque l'utilisateur qui tente d'établir une connexion SSH avec le commutateur pendant les heures de bureau a respecté la condition d'heure et de date.

show logging application ise-psc.log

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911 :
Évaluation de la règle - <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 -::::- 181675991110.127.197.5414126Authentication1816759911 :
Évaluation de la condition avec l'id - 72483811-ba39-4cc2-bdac-90a38232b95e - LHS operandId -
operandId, opérateur DATETIME_MATCHES, RHS operandId - rhsoperand
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.ConditionUtil -::::-
181675991110.127.197.5414126Authentication1816759911 : Condition 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 -::::- 181675991110.127.197.5414126Authentication1816759911 :
Résultat de l'évaluation pour Condition - 72483811-ba39-4cc2-bdac-90a38232b95e renvoyé -
true
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911 :
Définition du résultat pour la condition : 72483811-ba39-4cc2-bdac-90a38232b95e : vrai
```

Informations connexes

- Guide de déploiement prescriptif de Cisco ISE Device Administration

Forum aux questions

- Puis-je appliquer différents niveaux d'accès en fonction du temps ?
  Oui. Vous pouvez créer différentes stratégies d'autorisation et les lier à des conditions horaires.

  Exemple :
  Accès total pendant les heures de bureau
  Accès en lecture seule en dehors des heures de bureau
  Aucun accès le week-end

- Que se passe-t-il si l'heure système est incorrecte ou non synchronisée ?
  ISE peut appliquer des stratégies incorrectes ou ne pas appliquer les règles basées sur le temps de manière fiable. Assurez-vous que tous les périphériques et les noeuds ISE utilisent une source NTP synchronisée.

- Les politiques basées sur le temps peuvent-elles être utilisées conjointement avec d'autres conditions (par exemple, rôle d'utilisateur, type de périphérique) ?
  Oui. Les conditions de temps peuvent être combinées avec d'autres attributs dans vos règles de stratégie pour créer des contrôles d'accès granulaires et sécurisés.

- L'accès basé sur le temps est-il pris en charge pour le shell et les jeux de commandes dans TACACS+?
  Oui. Les conditions basées sur le temps peuvent contrôler l’accès à l’interpréteur de commandes du périphérique ou à des jeux de commandes spécifiques, en fonction de la

structure de la stratégie d’autorisation et des profils.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.