Konfigurieren von zeitbasiertem TACACS+-Zugriff für Netzwerkgeräte mit der ISE

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die zeit- und datumsbasierte Autorisierungsrichtlinie für die Geräteadministration in der Cisco Identity Services Engine (ISE) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit der Konfiguration des TACACS-Protokolls und der Identity Services Engine (ISE) vertraut sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Switch der Serie 9300 mit SoftwareCisco IOS® XE 17.12.5 und höher
- Cisco ISE, Version 3.3 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

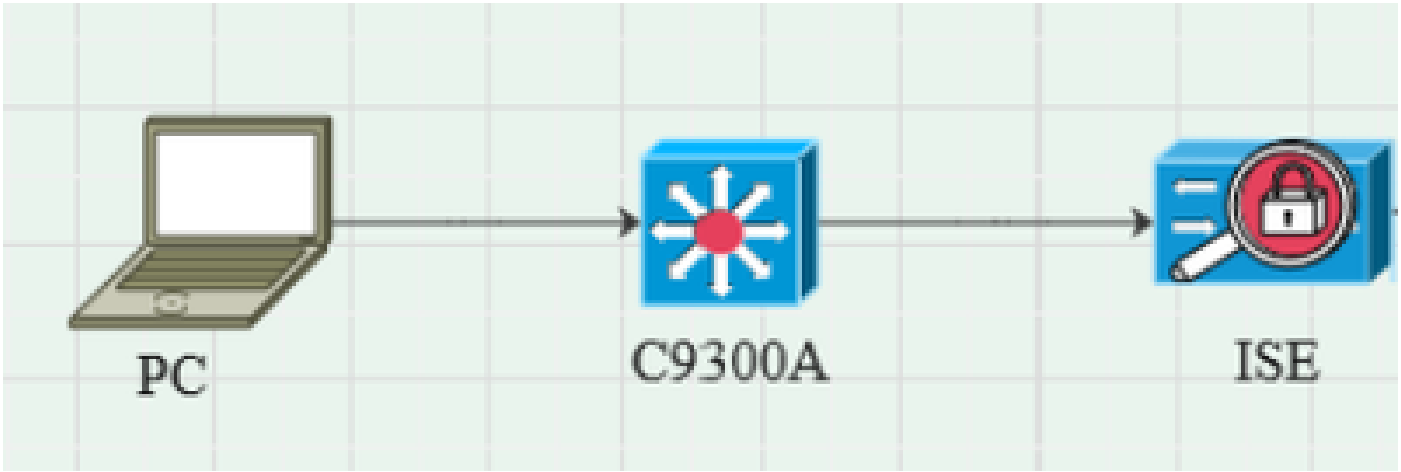
Autorisierungsrichtlinien sind eine Schlüsselkomponente der Cisco Identity Services Engine (ISE) und ermöglichen das Definieren von Regeln und das Konfigurieren von Autorisierungsprofilen für bestimmte Benutzer oder Gruppen, die auf Netzwerkressourcen zugreifen. Diese Richtlinien bewerten die Bedingungen, um zu bestimmen, welches Profil angewendet werden soll. Wenn die Bedingungen einer Regel erfüllt sind, wird das entsprechende Autorisierungsprofil zurückgegeben, das einen entsprechenden Netzwerkzugriff gewährt.

Die Cisco ISE unterstützt außerdem die Bedingungen für Uhrzeit und Datum, sodass Richtlinien nur zu bestimmten Zeiten oder Tagen durchgesetzt werden können. Dies ist besonders bei der Anwendung von Zugriffskontrollen auf Basis zeitbasierter geschäftlicher Anforderungen hilfreich.

In diesem Dokument wird die Konfiguration beschrieben, nach der der administrative TACACS+-Zugriff auf Netzwerkgeräte nur während der Geschäftszeiten (Montag bis Freitag von 08:00 bis 17:00 Uhr) zugelassen wird und der Zugriff außerhalb dieses Zeitfensters verweigert wird.

Konfigurieren

Netzwerkdiagramm



Konfigurieren der ISE

Schritt 1: Zeit- und Datumsbedingung erstellen

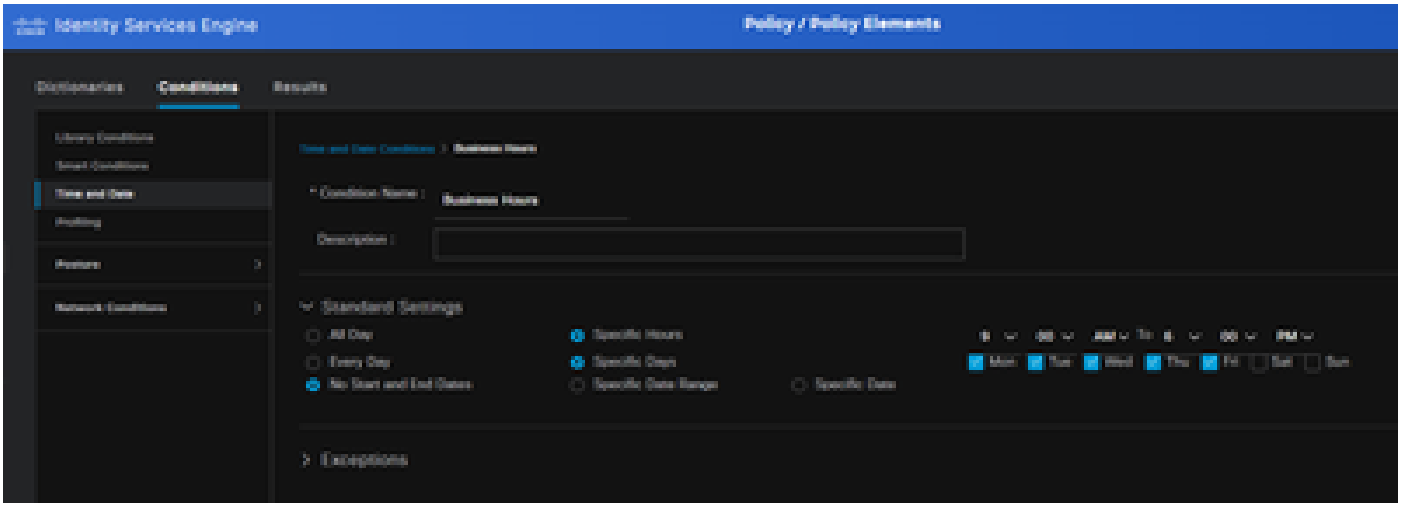
Navigieren Sie zu Policy > Policy Elements > Conditions > Time and Date, und klicken Sie auf

Add.

Bedingungsname: Geschäftszeiten

Legen Sie die Standardeinstellungen für den Zeitbereich > Bestimmte Stunden fest: 09:00 Uhr - 18:00 Uhr

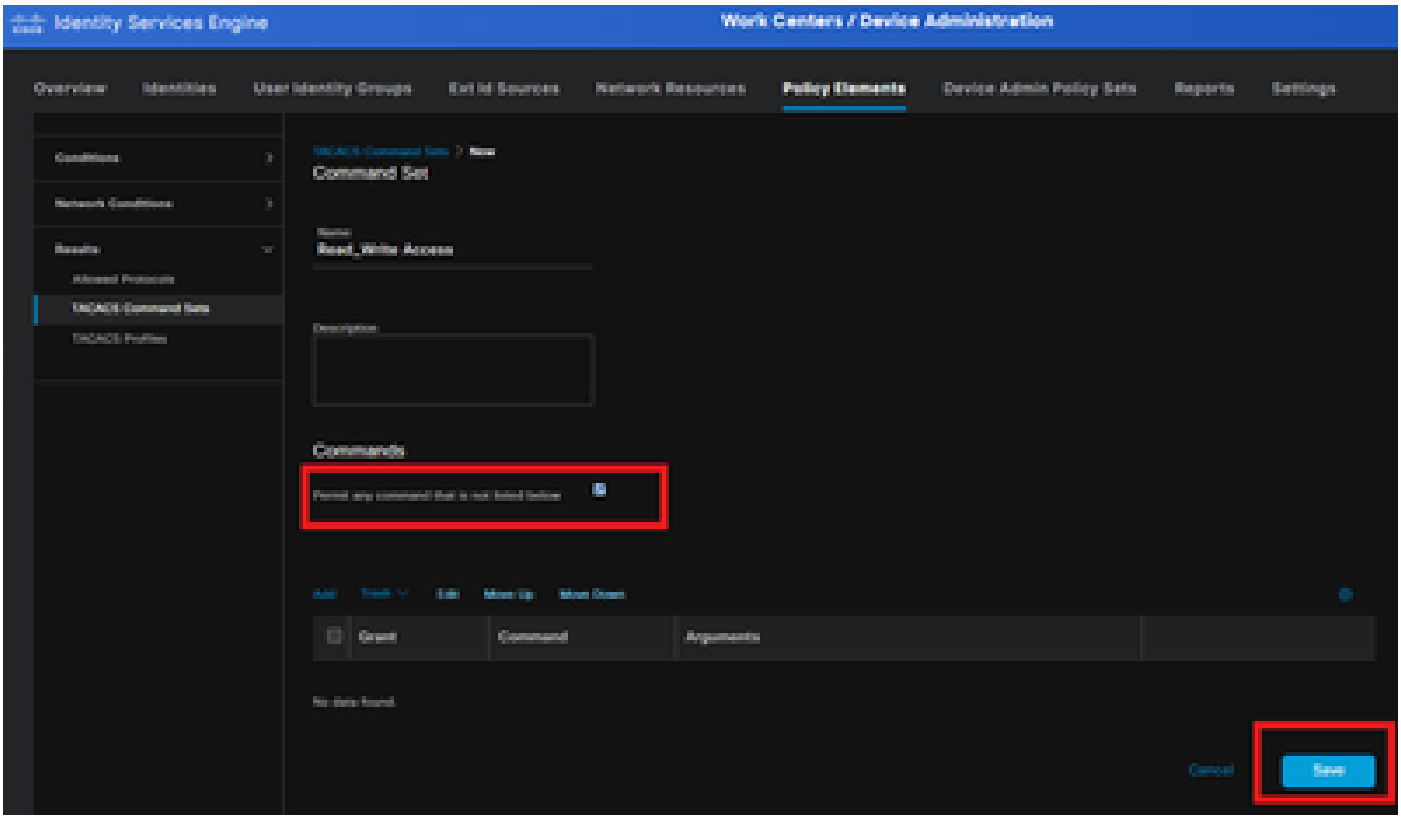
Bestimmte Tage: Montag bis Freitag



Phase 2: Erstellen eines TACACS+-Befehlssatzes

Navigieren Sie zu Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets.

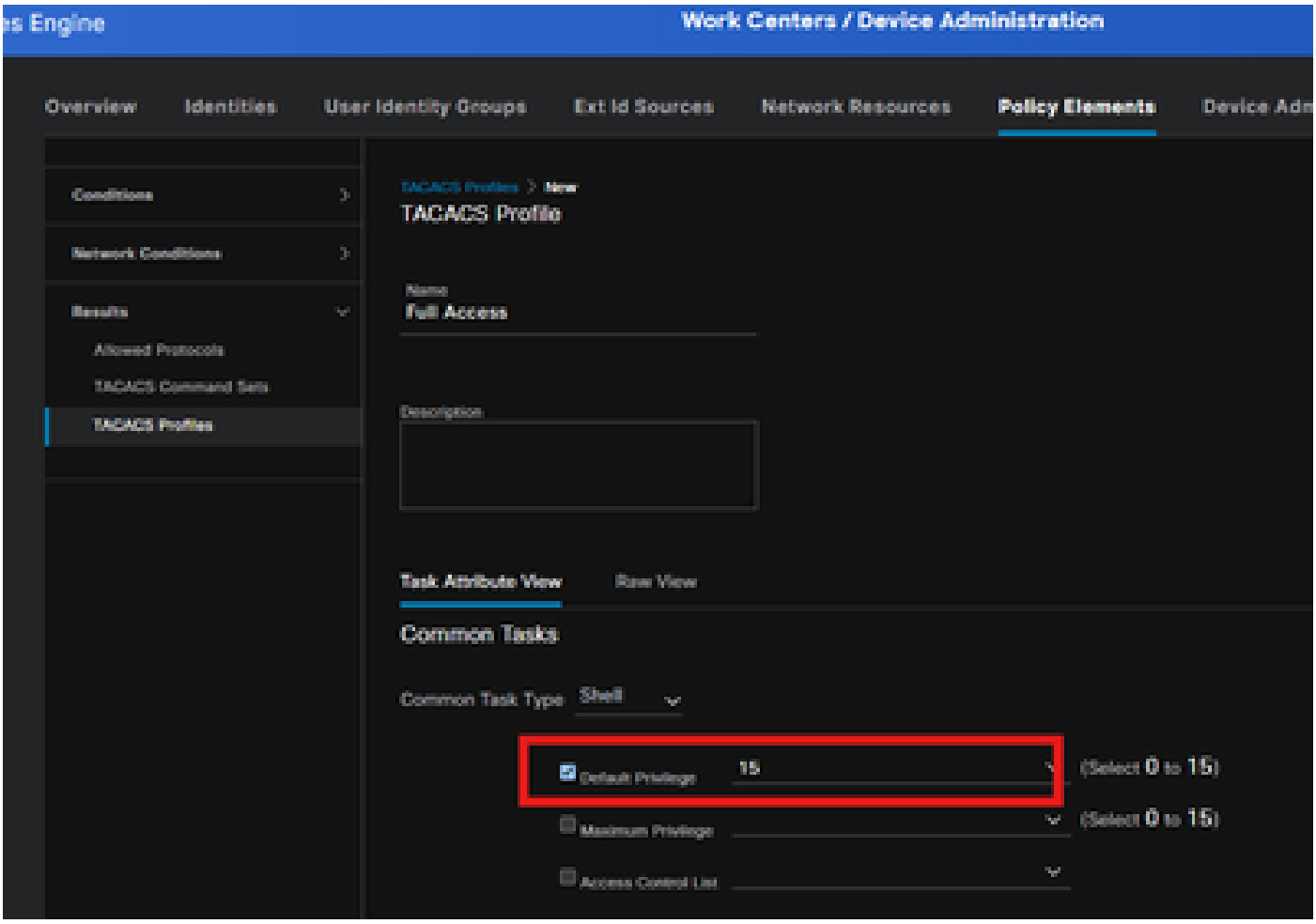
Erstellen Sie einen Befehlssatz, indem Sie das Kontrollkästchen Befehle zulassen, die unten nicht aufgeführt sind, aktivieren, und klicken Sie auf Senden oder fügen Sie die eingeschränkten Befehle hinzu, wenn Sie bestimmte CLI-Befehle einschränken möchten.



Schritt 3: Erstellen eines TACACS+-Profils

Navigieren Sie zu Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles. Klicken Sie auf Hinzufügen.

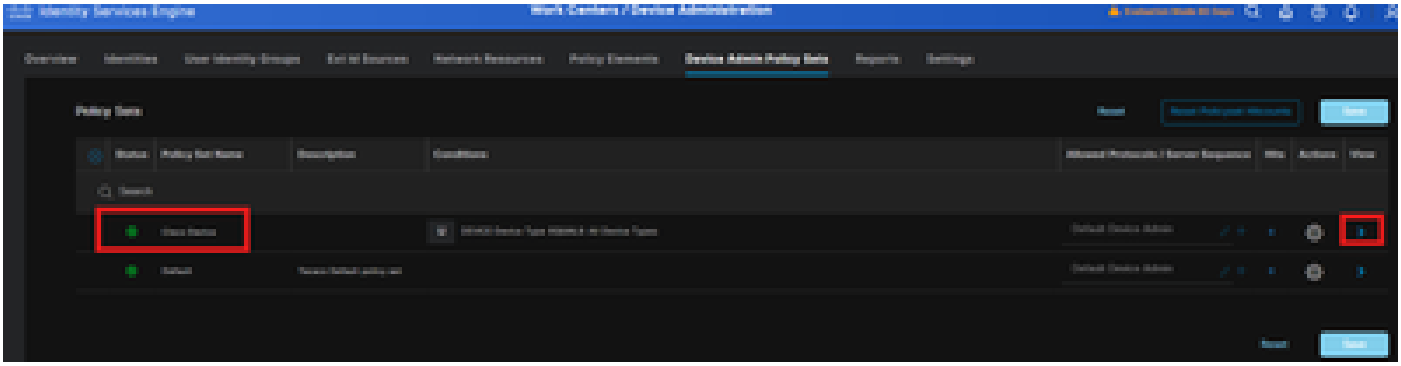
Wählen Sie Befehlsaufgabentyp als Shell, dann Standardberechtigung aus, und geben Sie den Wert 15 ein. Klicken Sie auf Senden.



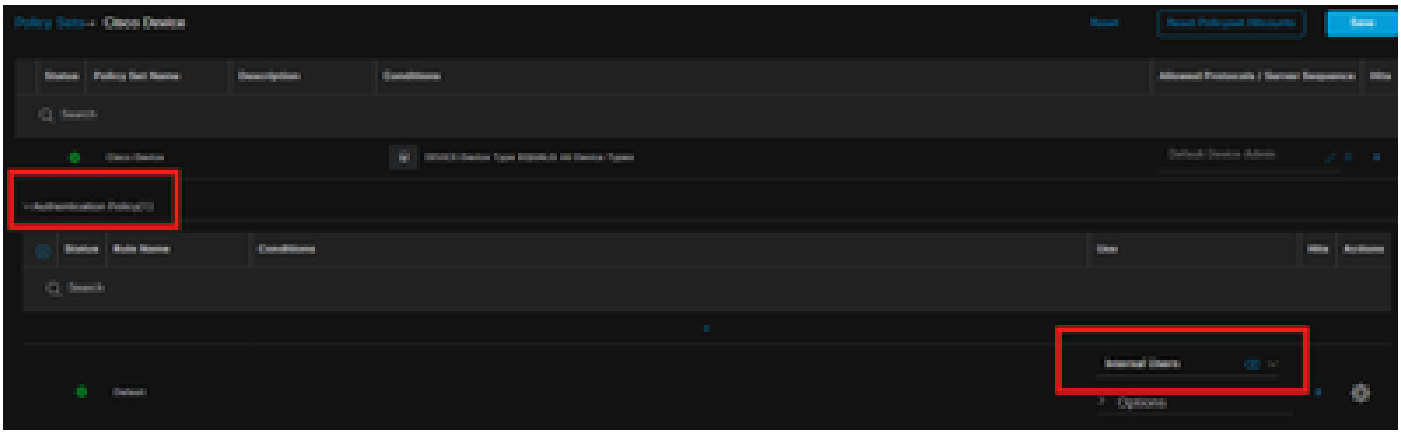
Schritt 4: Erstellen einer TACACS-Autorisierungsrichtlinie

Navigieren Sie zu Work Centers > Device Administration > Device Admin Policy Sets.

Wählen Sie Ihren aktiven Richtliniensatz aus.



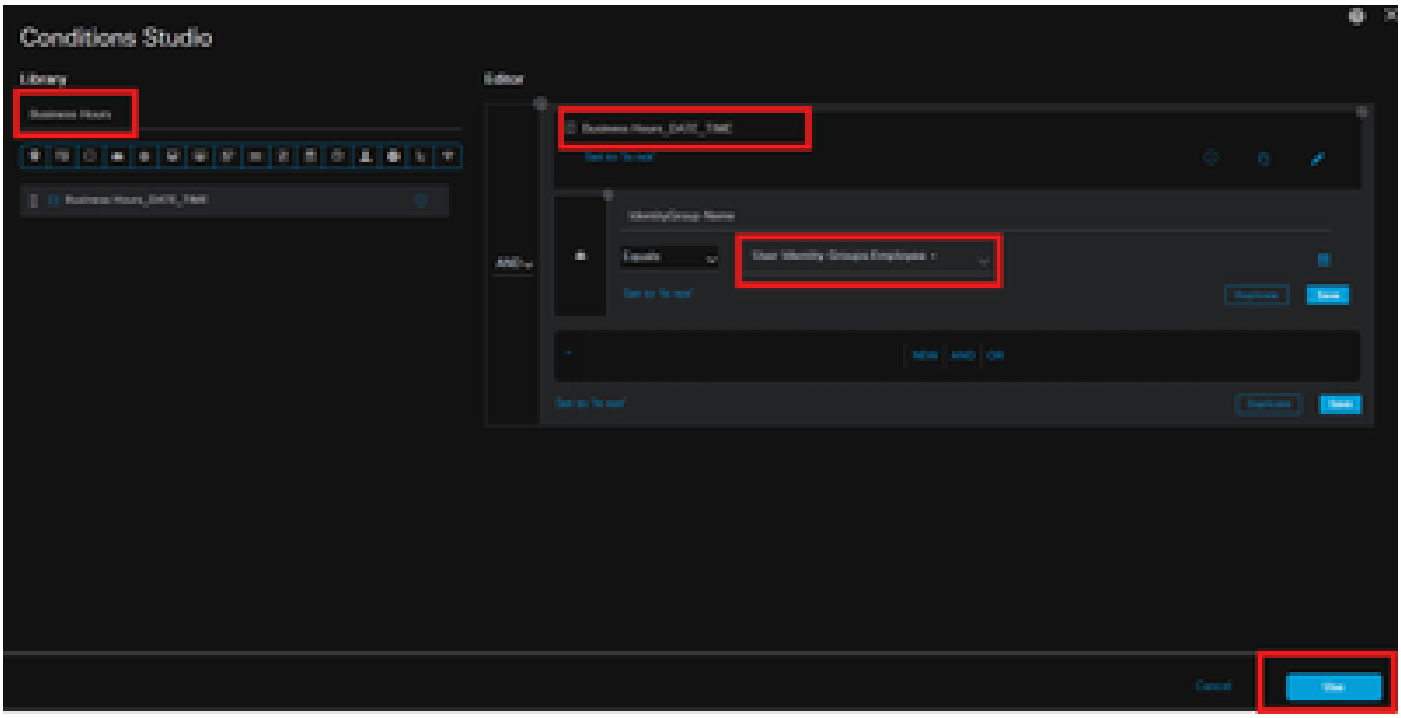
Konfigurieren Sie die Authentifizierungsrichtlinie auf Basis der internen oder der Active Directory-Benutzer.



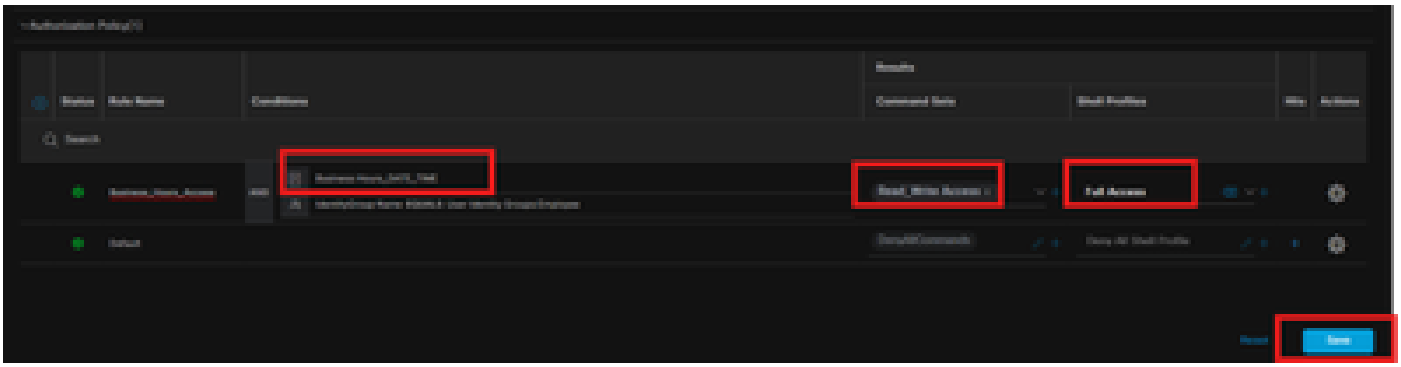
Klicken Sie im Abschnitt "Autorisierungsrichtlinie" auf Regel hinzufügen, um den Regelnamen anzugeben, und klicken Sie dann auf +, um Autorisierungsbedingungen hinzuzufügen.

Ein neues Condition Studio-Fenster wird angezeigt. Geben Sie im Feld Nach Namen suchen den in Schritt 1 erstellten Namen ein, und ziehen Sie ihn in den Editor.

Fügen Sie zusätzliche Bedingungen basierend auf der Benutzergruppe hinzu, und klicken Sie auf Speichern.



Wählen Sie in Results (Ergebnisse) den in Schritt 2 und Schritt 3 erstellten TACACS-Befehlssatz und das Shell-Profil aus, und klicken Sie dann auf Save.



Switch konfigurieren

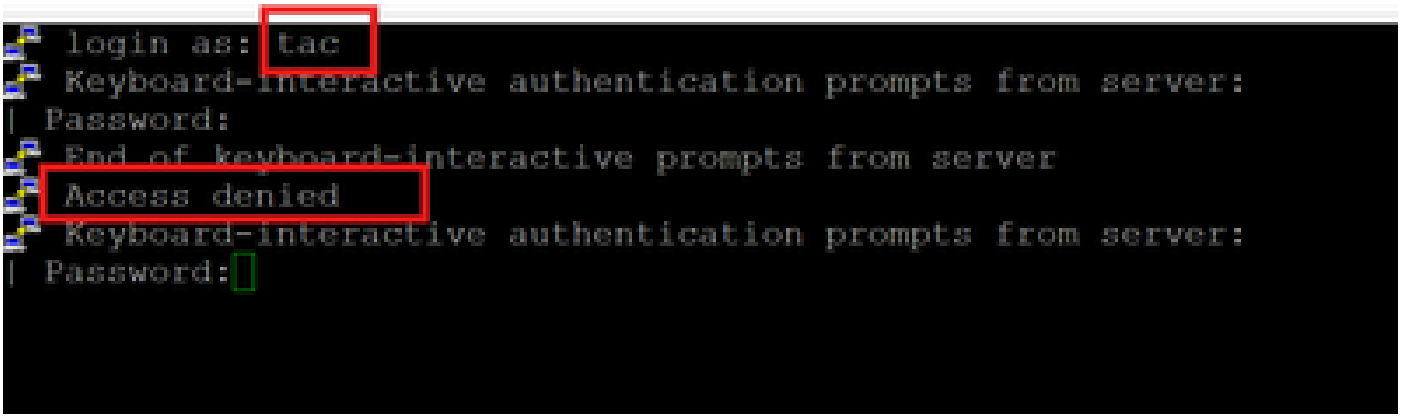
aaa neues Modell

aaa Authentifizierung Anmeldung lokale Standardgruppe TACACS+
aaa authentication default enable group tacacs+ aktivieren
aaa, Autorisierungskonfigurationsbefehle
aaa, Autorisierung exec, lokale Standardgruppentaktacs+
aaa, Autorisierungsbefehle 0 default local group tacacs+
aaa, Autorisierungsbefehle 1 standardmäßige lokale Gruppentacacs+
aaa, Autorisierungsbefehle 15 lokale Standardgruppentaketen+

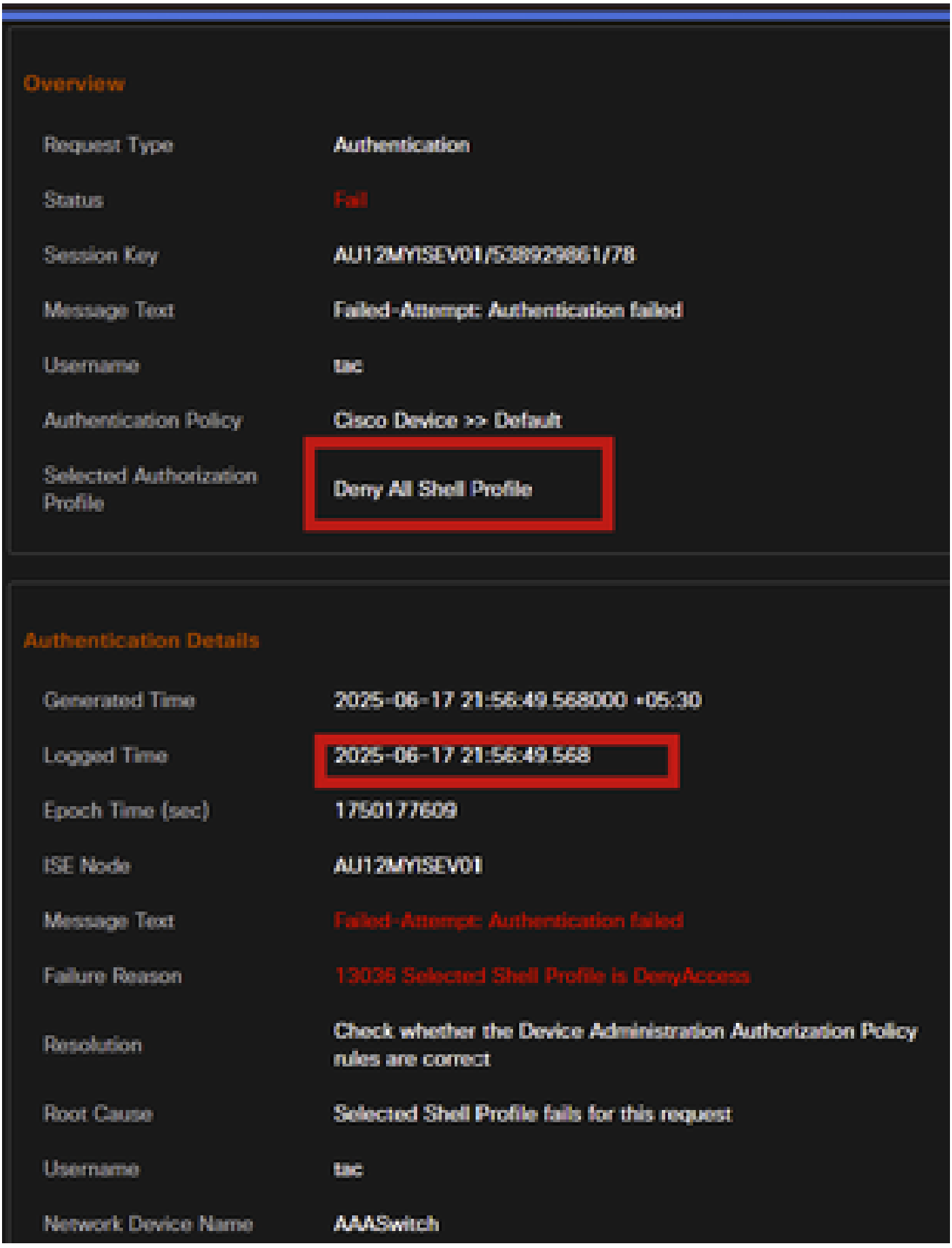
TACACS-Server ISE
address ipv4 10,127.197,53
Taste Qwerty123

Überprüfung

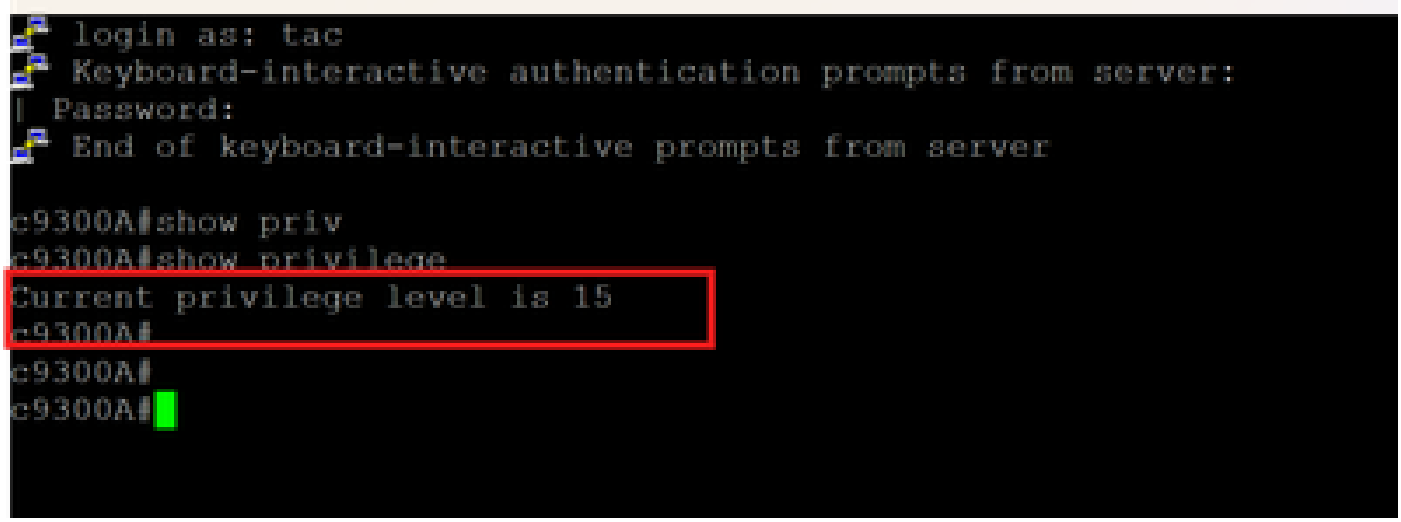
Benutzer, der versucht, eine SSH-Verbindung zum Switch außerhalb der Geschäftszeiten herzustellen, und der Zugriff von der ISE wurde verweigert.



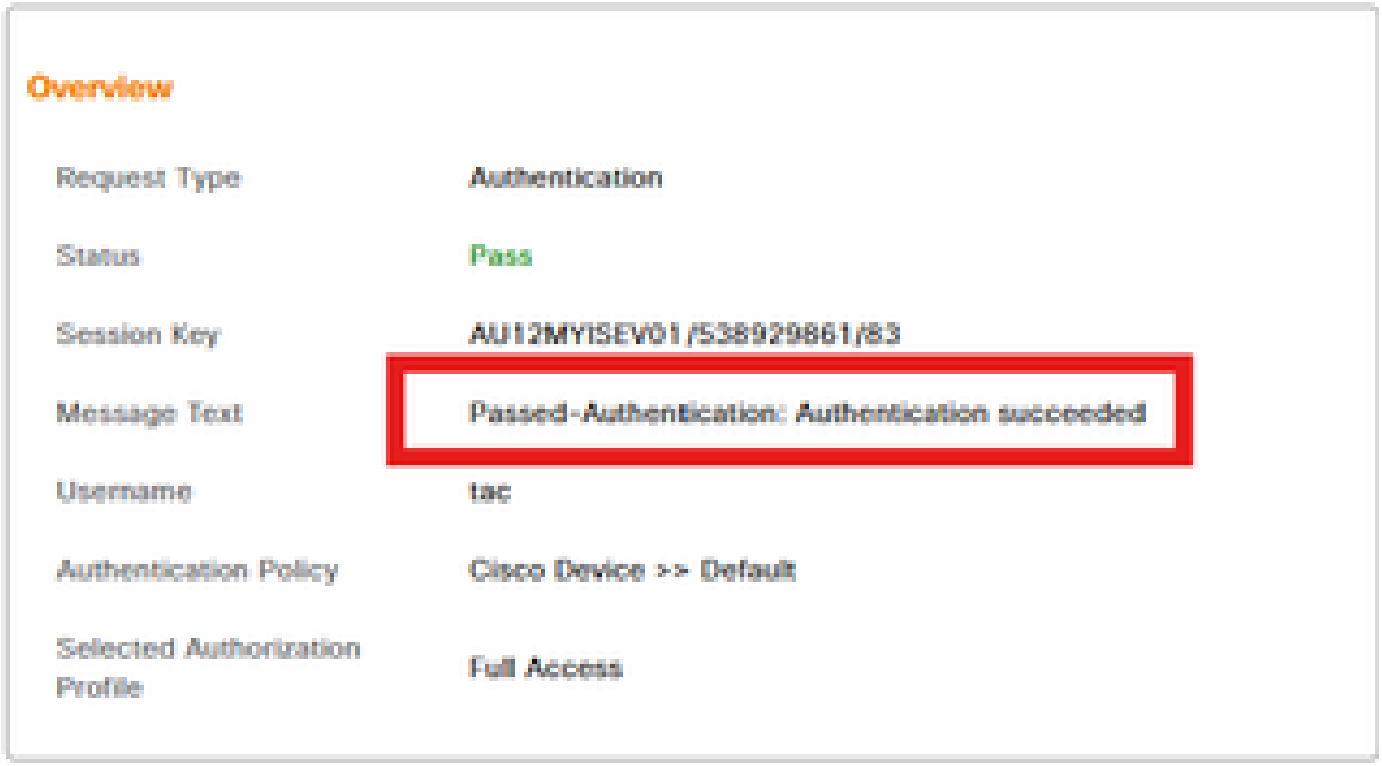
Die ISE-Live-Protokolle weisen darauf hin, dass die Autorisierung fehlschlug, weil die Zeit- und Datumsbedingung in der Autorisierungsrichtlinie nicht übereinstimmten, was dazu führte, dass die Sitzung die Standardregel für den verweigerten Zugriff erreichte.

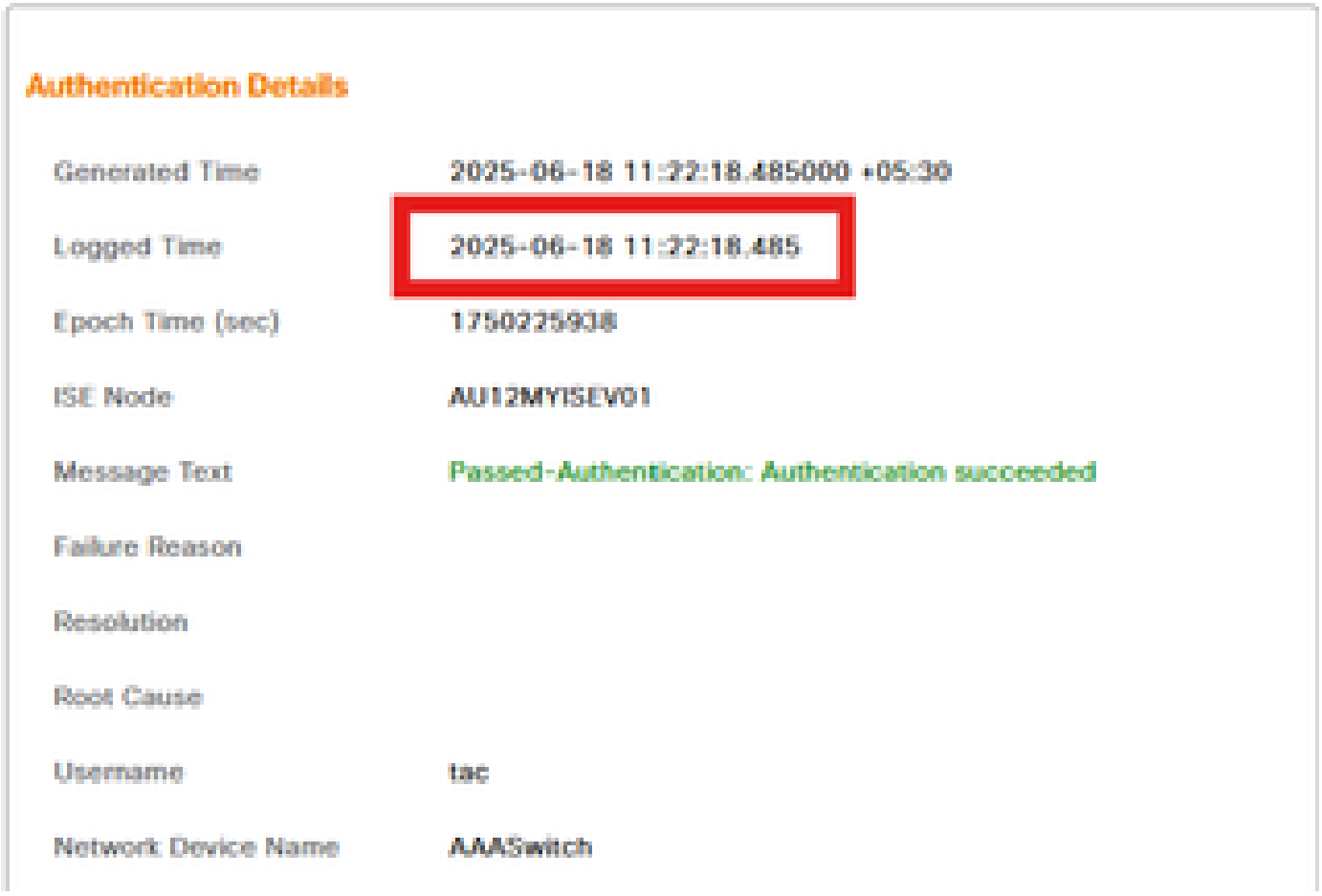


Benutzer, der während der Geschäftszeiten versucht, per SSH auf den Switch zuzugreifen und Lese-/Schreibzugriff zu erhalten:



Das ISE-Live-Protokoll gibt an, dass die Anmeldung während der Geschäftszeiten mit der Zeit- und Datumsbedingung übereinstimmt und die richtige Richtlinie trifft.





Fehlerbehebung

Debuggen auf der ISE

Sammeln Sie das ISE-Support-Paket mit den folgenden Attributen, die auf Debugebene festgelegt werden sollen:

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

Wenn der Benutzer, der versucht, außerhalb der Geschäftszeiten SSH-Verbindungen zum Switch herzustellen (aufgrund von Uhrzeit und Datum), nicht mit den konfigurierten Geschäftszeiten übereinstimmt.

show logging-Anwendung ise-psc.log

```
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::- 360158683110.127.197.5449306Authentication3601586831:
Regel wird ausgewertet - <Rule 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 -:::- 360158683110.127.197.5449306Authentication3601586831:
Bedingung mit ID auswerten - 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 -:::-
360158683110.127.197.5449306Authentifizierung3601586831: 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:
Testergebnis für Zustand - 72483811-ba39-4cc2-bdac-90a38232b95e ergibt - falsch
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -:::- 360158683110.127.197.5449306Authentication3601586831:
Ergebnis für Bedingung festlegen: 72483811-ba39-4cc2-bdac-90a38232b95e : falsch
```

Wenn der Benutzer, der während der Geschäftszeiten SSH-Verbindungen zum Switch herstellen möchte, mit der Zeit- und Datumsbedingung übereinstimmt.

show logging-Anwendung ise-psc.log

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::- 181675991110.127.197.5414126Authentication1816759911:
Regel wird ausgewertet - <Rule 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 -:::- 181675991110.127.197.5414126Authentication1816759911:
Bedingung mit ID auswerten - 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 -:::-
181675991110.127.197.5414126Authentication1816759911: 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:
Testergebnis für Zustand - 72483811-ba39-4cc2-bdac-90a38232b95e ergibt - wahr
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::- 181675991110.127.197.5414126Authentication1816759911:
Ergebnis für Bedingung festlegen: 72483811-ba39-4cc2-bdac-90a38232b95e : wahr
```

Zugehörige Informationen

- Cisco ISE Device Administration - Leitfaden zur Bereitstellung

Häufig gestellte Fragen

- Kann ich je nach Zeit unterschiedliche Zugriffsebenen anwenden?
  Ja. Sie können verschiedene Autorisierungsrichtlinien erstellen und diese mit den Zeitbedingungen verknüpfen.

  Beispiele:
  Vollständiger Zugriff während der Geschäftszeiten
  Schreibgeschützter Zugriff nach Geschäftsschluss
  Kein Zugriff am Wochenende

- Was passiert, wenn die Systemzeit falsch oder nicht synchronisiert ist?
  Die ISE kann inkorrekte Richtlinien anwenden oder zeitbasierte Regeln nicht zuverlässig durchsetzen. Stellen Sie sicher, dass alle Geräte und ISE-Knoten eine synchronisierte NTP-Quelle verwenden.

- Können zeitbasierte Richtlinien in Verbindung mit anderen Bedingungen (z. B. Benutzerrolle, Gerätetyp) verwendet werden?
  Ja. Die Zeitbedingungen können mit anderen Attributen in den Richtlinienregeln kombiniert werden, um präzise und sichere Zugriffskontrollen zu erstellen.

- Wird zeitbasierter Zugriff für Shell- und Befehlssätze in TACACS+? unterstützt?
  Ja. Zeitbasierte Bedingungen können den Zugriff auf die Geräte-Shell oder bestimmte Befehlssätze steuern, je nachdem, wie die Autorisierungsrichtlinien und -profile strukturiert sind.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.