Configuración del acceso TACACS+ basado en tiempo para dispositivos de red con ISE

Contenido

Introducción

Este documento describe cómo configurar la autorización basada en fecha y hora para la política Device Admin en Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recomienda que conozca la configuración de Tacacs Protocol e Identity Services Engine (ISE).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switch Cisco Catalyst 9300 con softwareCisco IOS® XE 17.12.5 y versiones posteriores

- Cisco ISE, versión 3.3 y posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

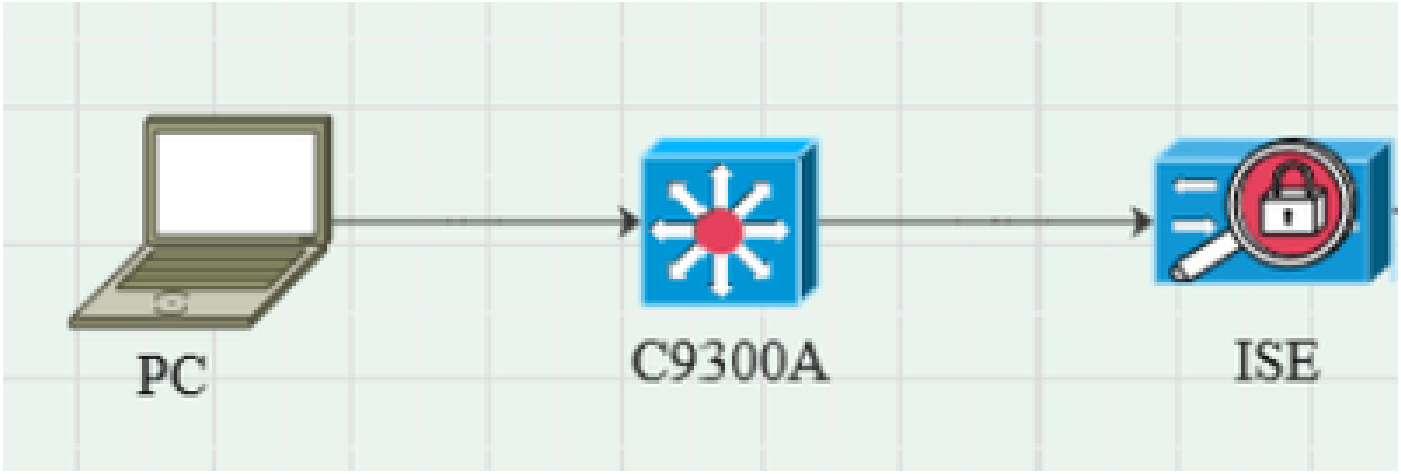
Las políticas de autorización son un componente clave de Cisco Identity Services Engine (ISE), que le permite definir reglas y configurar perfiles de autorización para usuarios o grupos específicos que acceden a los recursos de red. Estas políticas evalúan las condiciones para determinar qué perfil aplicar. Cuando se cumplen las condiciones de una regla, se devuelve el perfil de autorización correspondiente y se concede el acceso a la red adecuado.

Cisco ISE también es compatible con las condiciones de fecha y hora, que permiten que las políticas se apliquen solo durante horas o días específicos. Esto resulta especialmente útil para aplicar controles de acceso basados en requisitos empresariales basados en el tiempo.

Este documento describe la configuración para permitir el acceso administrativo de TACACS+ a los dispositivos de red solamente durante el horario comercial (de lunes a viernes, de 08:00 a 17:00) y para denegar el acceso fuera de esta ventana de tiempo.

Configurar

Diagrama de la red



Configuración de ISE

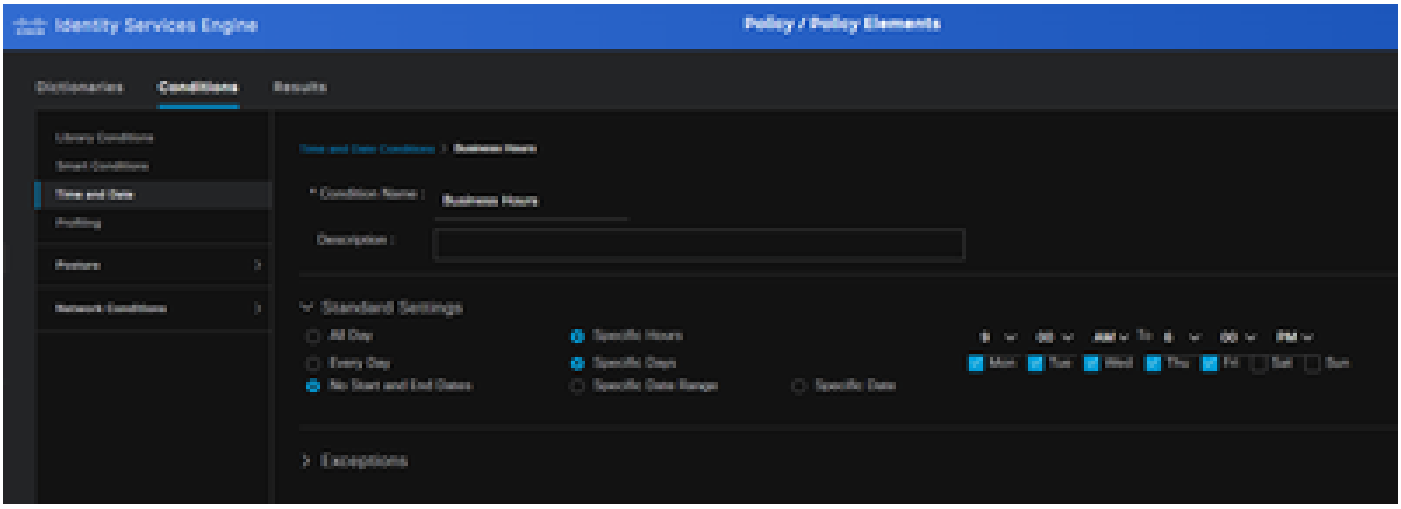
Paso 1: Crear condición de fecha y hora

Vaya a Directiva > Elementos de directiva > Condiciones > Fecha y hora y haga clic en Agregar.

Nombre de condición: Horario comercial

Ajuste el rango de tiempo Configuración estándar > Horas específicas: 09:00 AM - 06:00 PM

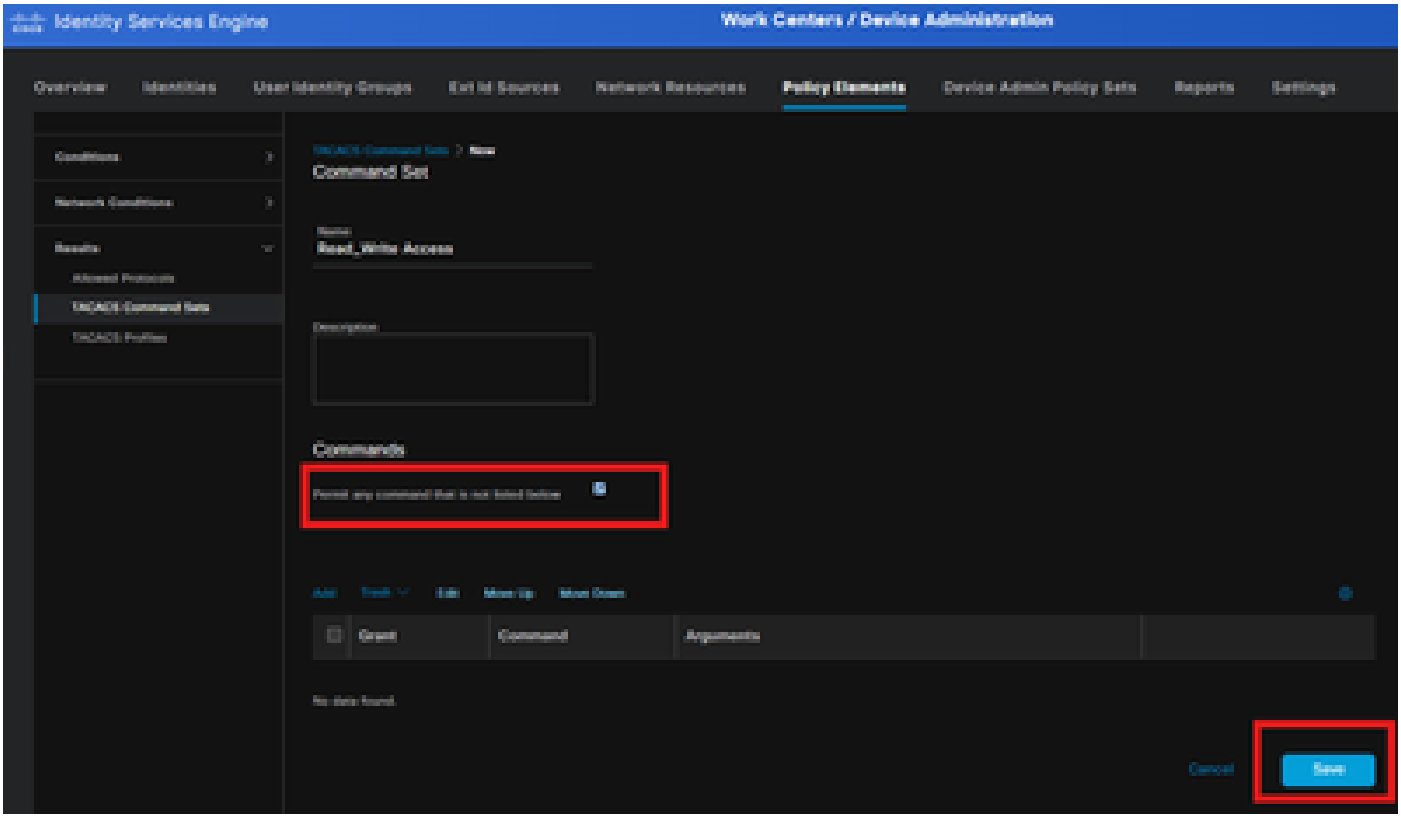
Días específicos: De lunes a viernes



Paso 2: Crear un conjunto de comandos TACACS+

Vaya a Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Conjuntos de comandos Tacacs.

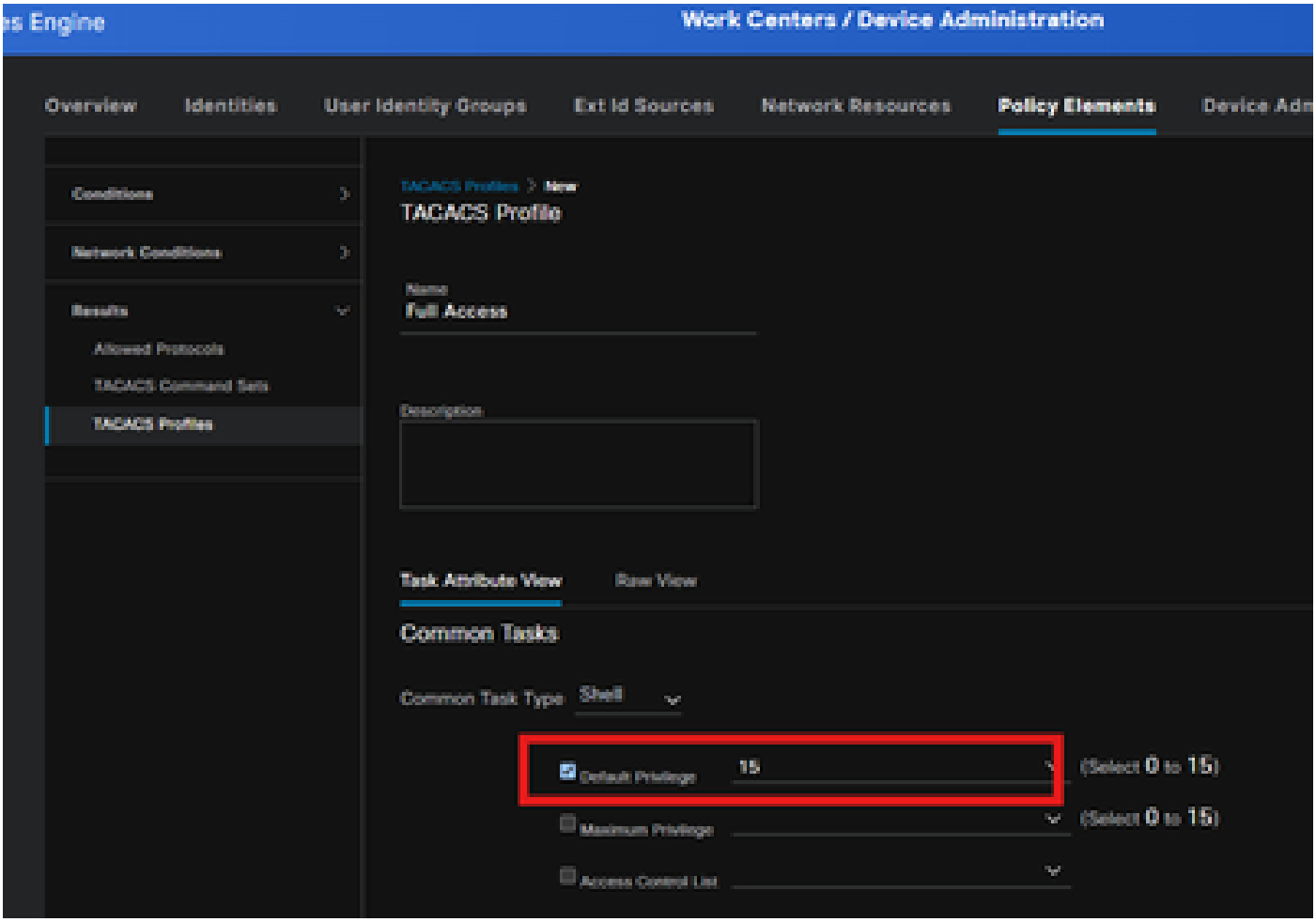
Cree un conjunto de comandos seleccionando la casilla de verificación Permitir cualquier comando que no aparezca debajo y haga clic en Enviar o agregue los comandos limitados si desea restringir ciertos comandos de CLI.



Paso 3: Crear un perfil TACACS+

Vaya a Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS. Haga clic en Add (Agregar).

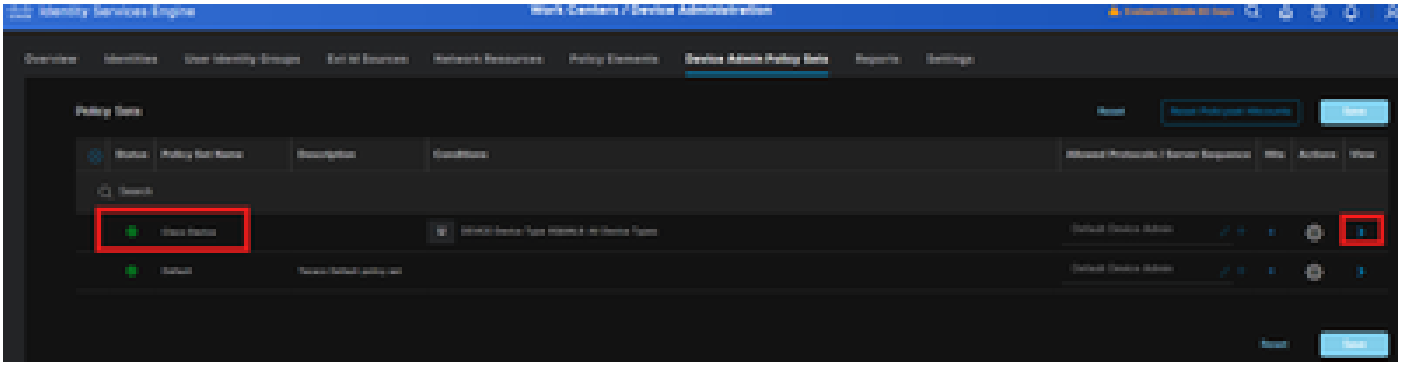
Seleccione Tipo de Tarea de Comando como Shell y, a continuación, la casilla de control Privilegio por Defecto e introduzca el valor de 15. Haga clic en Enviar.



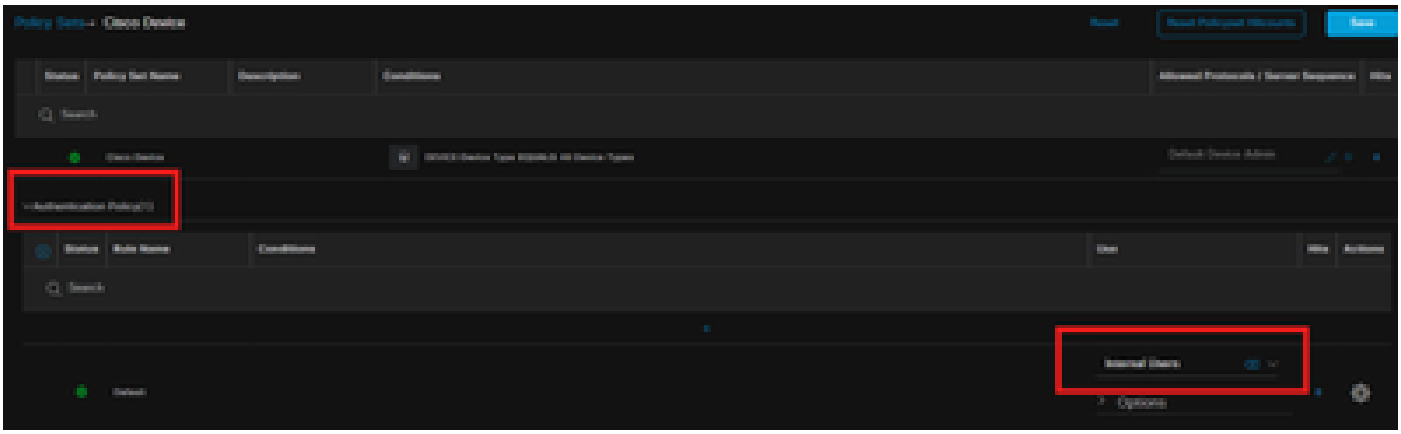
Paso 4: Crear política de autorización TACACS

Vaya a Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos.

Seleccione el conjunto de políticas activo.



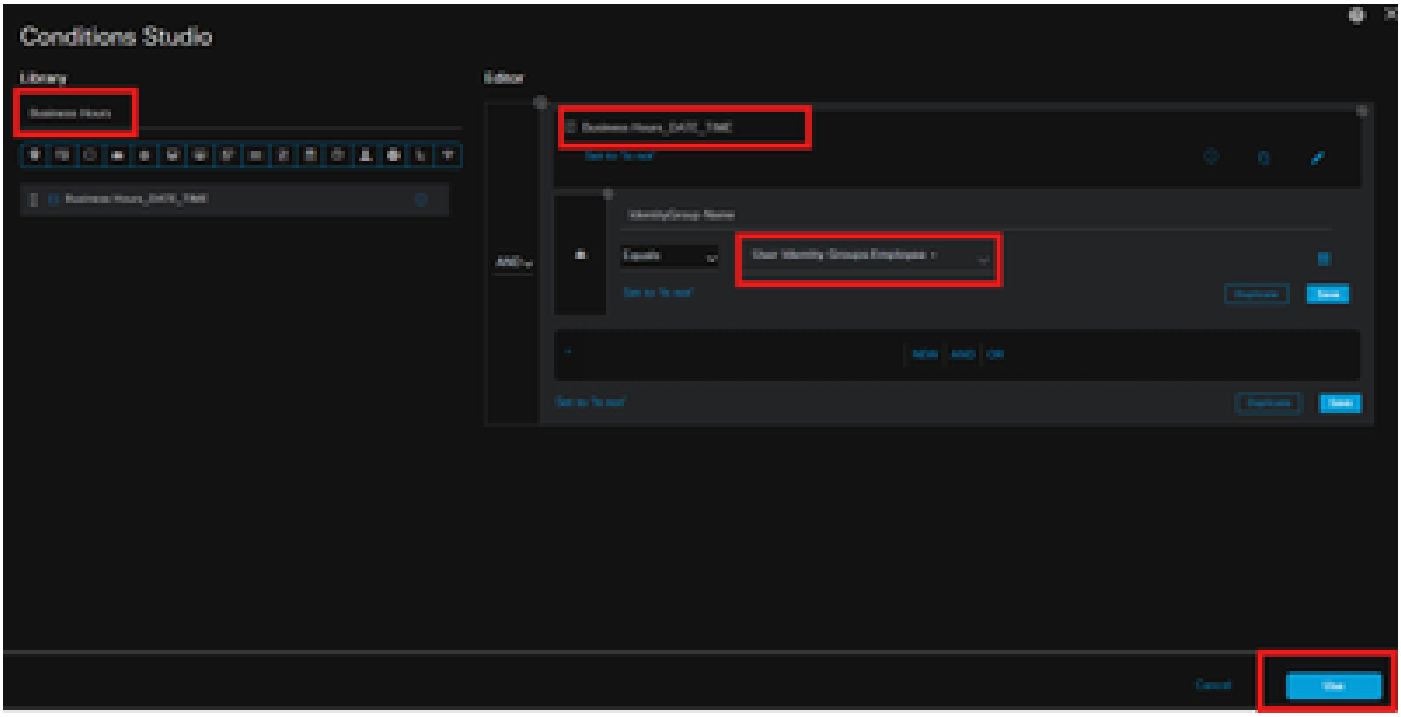
Configure la directiva de autenticación basada en los usuarios internos o de Active Directory.



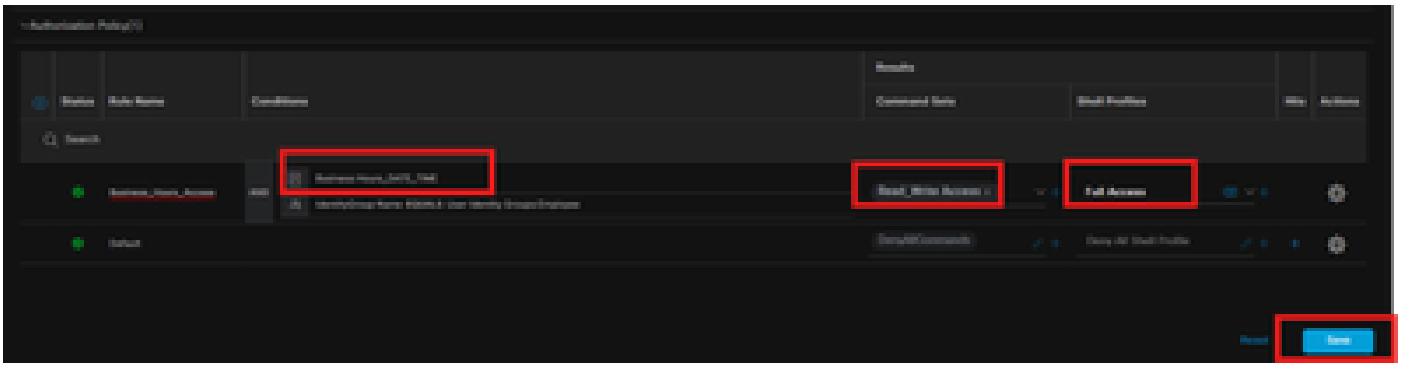
En la sección Directiva de autorización, haga clic en Agregar regla para proporcionar el nombre de la regla y, a continuación, haga clic en + para agregar condiciones de autorización.

Aparece una nueva ventana Condition Studio, en el campo Search by Name, ingrese el nombre creado en el paso 1 y arrástrelo al Editor.

Agregue condiciones adicionales según el grupo de usuarios y haga clic en Guardar.



En Results, seleccione el Command Set de Tacacs y el Shell Profile creados en los pasos 2 y 3, luego haga clic en Save.

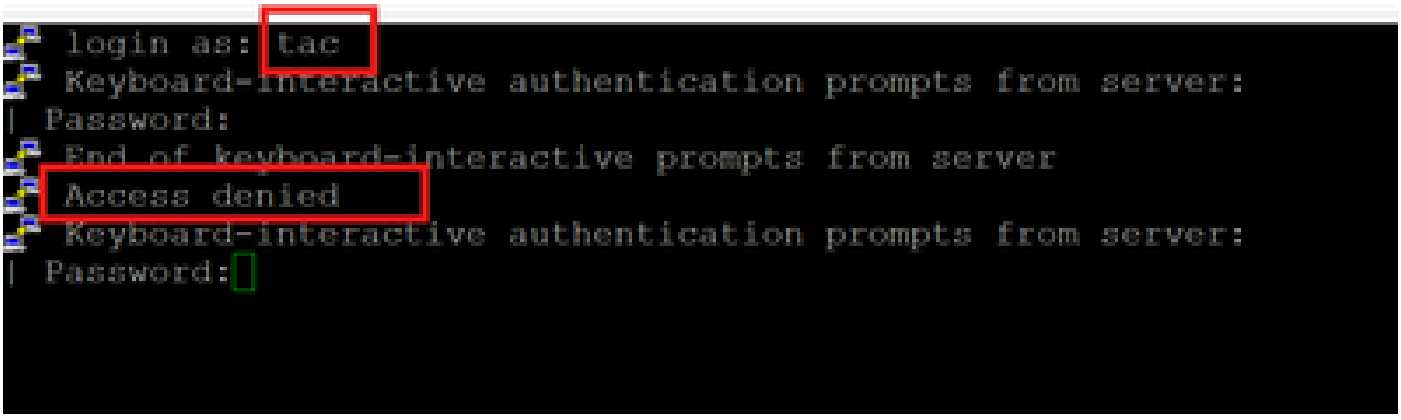


Configurar switch

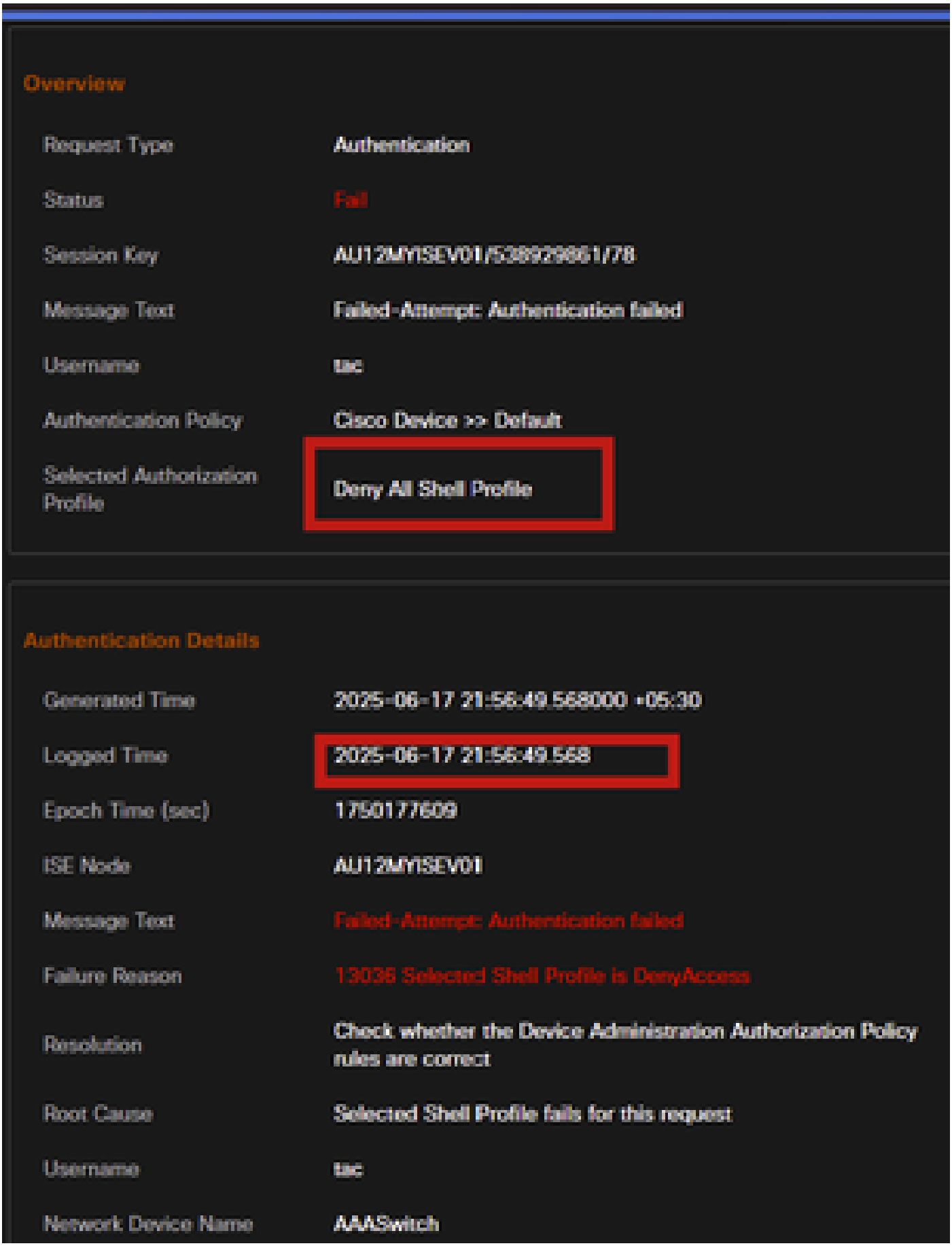
```
aaa new-model

aaa authentication login default local group tacacs+
aaa authentication enable default enable group tacacs+
aaa authorization config-commands
aaa authorization exec default local group 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+

ISE del servidor TACACS
address ipv4 10.127.197.53
clave Qwerty123
```

Verificación

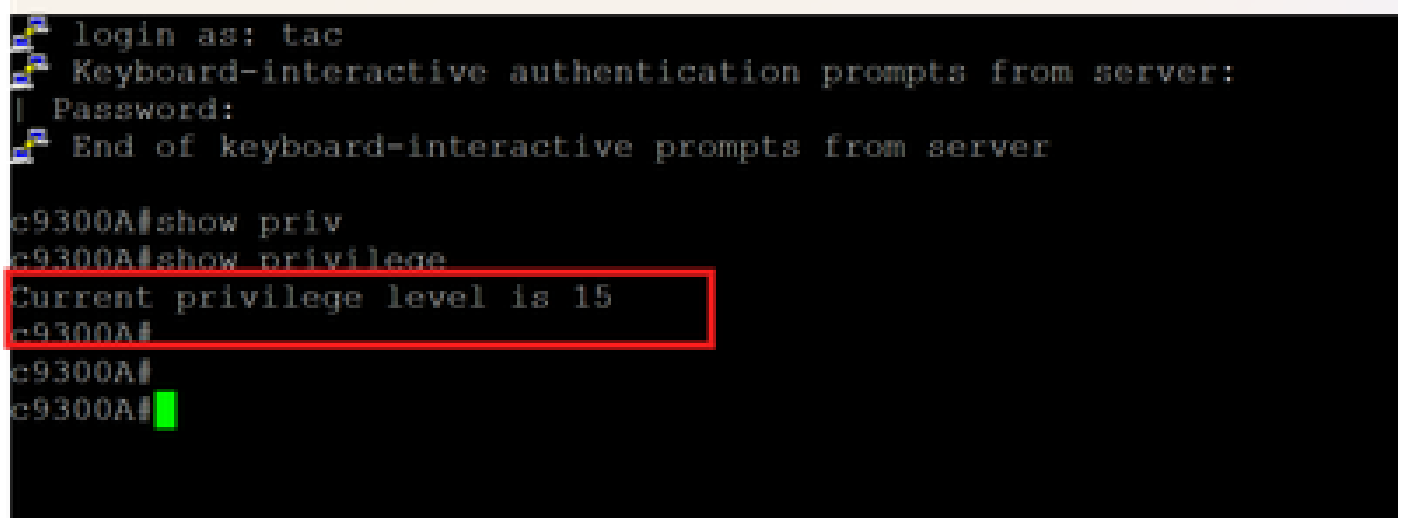
El usuario está intentando introducir SSH en el switch fuera del horario laboral y se le denegó el acceso desde ISE.



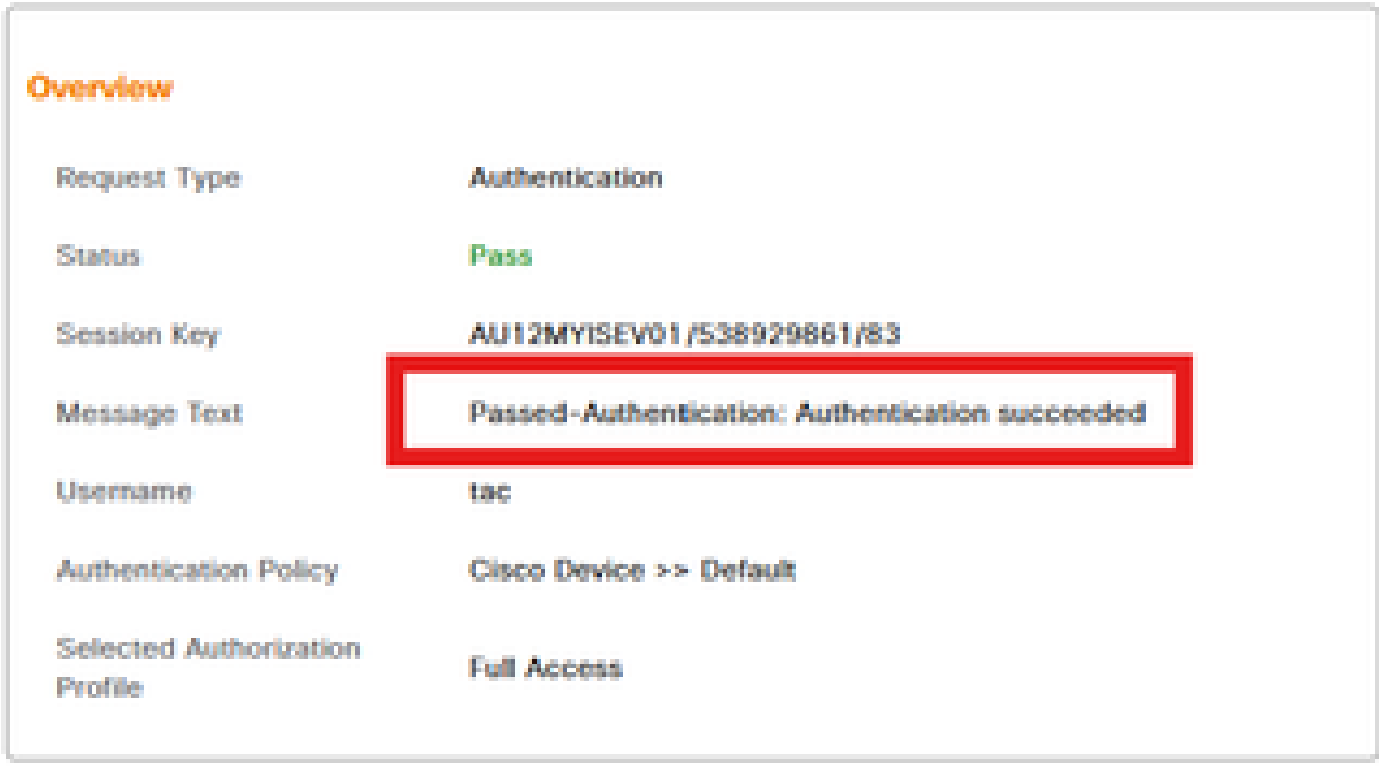
Los Live Logs de ISE indican que se produjo un error en la autorización porque la condición de fecha y hora de la política de autorización no coincidía, por lo que la sesión alcanzó la regla de denegación de acceso predeterminada.



El usuario está intentando introducir SSH en el switch durante el horario comercial y obtener acceso de lectura y escritura:

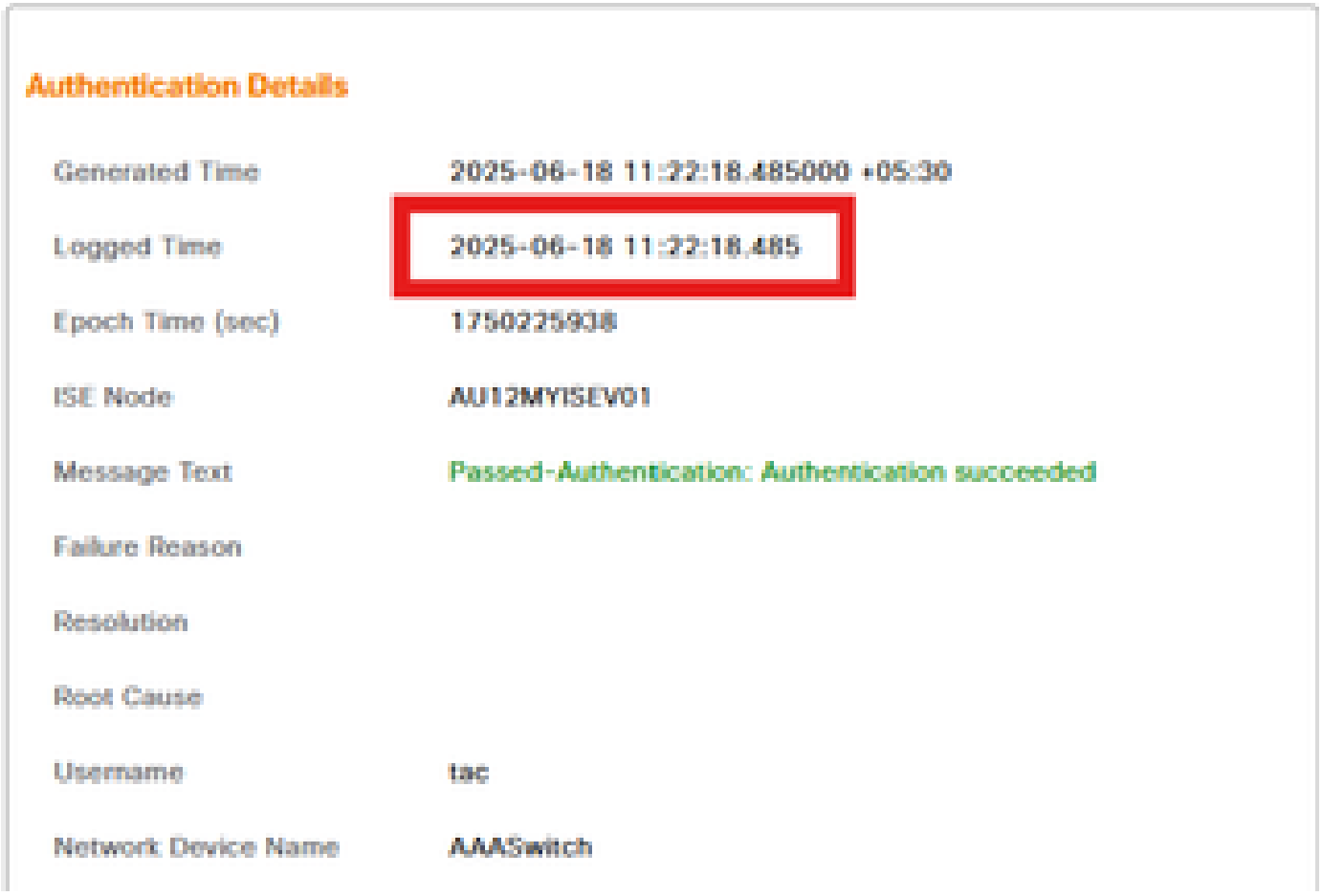


El registro en directo de ISE indica que el inicio de sesión durante el horario laborable coincide con la condición de fecha y hora y cumple la política correcta.



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

Troubleshoot

Depuraciones en ISE

Recopile el paquete de soporte de ISE con estos atributos para configurarlos en el nivel de depuración:

- RuleEngine-Policy-IDGgroups
- Atributos de RuleEngine
- Policy-Engine
- epm-pdp
- epm-pip

Cuando el usuario intenta introducir SSH en el switch fuera del horario comercial debido a que la condición de fecha y hora no coincide con el horario comercial configurado.

show logging application ise-psc.log

```
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Autenticación3601586831:
Regla de evaluación - <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 -::::- 360158683110.127.197.5449306Autenticación3601586831:
Evaluación de la condición con 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 -:::-
360158683110.127.197.5449306Autenticación3601586831: Condición lhsoperand Valor -
com.cisco.cpm.policy.DTConstraint@6924136c , rhsoperand Valor -
com.cisco.cpm.policy.DTConstraint@3eeea825
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Autenticación3601586831:
Resultado de la evaluación de la condición - 72483811-ba39-4cc2-bdac-90a38232b95e devuelto
- false
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Autenticación3601586831:
Establecimiento del resultado para la condición: 72483811-ba39-4cc2-bdac-90a38232b95e :
falso
```

Cuando el usuario que intentó conectarse a SSH en el switch durante el horario comercial coincidió con la condición de fecha y hora.

show logging application ise-psc.log

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Autenticación1816759911:
Regla de evaluación - <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 -::::- 181675991110.127.197.5414126Autenticación1816759911:
Evaluación de la condición con 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 -::::-
181675991110.127.197.5414126Autenticación1816759911: Condición lhsoperand Valor -
com.cisco.cpm.policy.DTConstraint@4af10566 , rhsoperand Valor -
com.cisco.cpm.policy.DTConstraint@2bdb62e9
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Autenticación1816759911:
Resultado de la evaluación de la condición - 72483811-ba39-4cc2-bdac-90a38232b95e devuelto
- true
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Autenticación1816759911:
Establecimiento del resultado para la condición: 72483811-ba39-4cc2-bdac-90a38232b95e :
verdadero
```

Información Relacionada

- Guía de implementación prescriptiva de Cisco ISE Device Administration

Preguntas Frecuentes

- ¿Puedo aplicar diferentes niveles de acceso en función del tiempo?
  Yes. Puede crear diferentes directivas de autorización y vincularlas a condiciones de tiempo.

  Por ejemplo:
  Acceso completo en horario comercial
  Acceso de solo lectura fuera del horario laboral
  Sin acceso los fines de semana

- ¿Qué sucede si la hora del sistema es incorrecta o no está sincronizada?
  ISE puede aplicar políticas incorrectas o no aplicar reglas basadas en tiempo de forma fiable. Asegúrese de que todos los dispositivos y nodos ISE utilizan un origen NTP sincronizado.

- ¿Se pueden utilizar políticas basadas en tiempo junto con otras condiciones (por ejemplo, función de usuario, tipo de dispositivo)?
  Yes. Las condiciones de tiempo se pueden combinar con otros atributos de las reglas de política para crear controles de acceso granulares y seguros.

- ¿Es compatible el acceso basado en tiempo para el shell y los conjuntos de comandos en TACACS+??
  Yes. Las condiciones basadas en tiempo pueden controlar el acceso al shell del dispositivo

o a conjuntos de comandos específicos, en función de cómo estén estructurados los perfiles y la política de autorización.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).