ISE를 사용하여 네트워크 디바이스에 대한 시간 기반 TACACS+ 액세스 구성

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)에서 디바이스 관리 정책에 대한 시간 및 날짜 기반 권한 부여를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 Tacacs 프로토콜 및 ISE(Identity Services Engine) 컨피그레이션에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 포함 Cisco Catalyst 9300 스위치Cisco IOS® XE 17.12.5 이상
- Cisco ISE, 릴리스 3.3 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

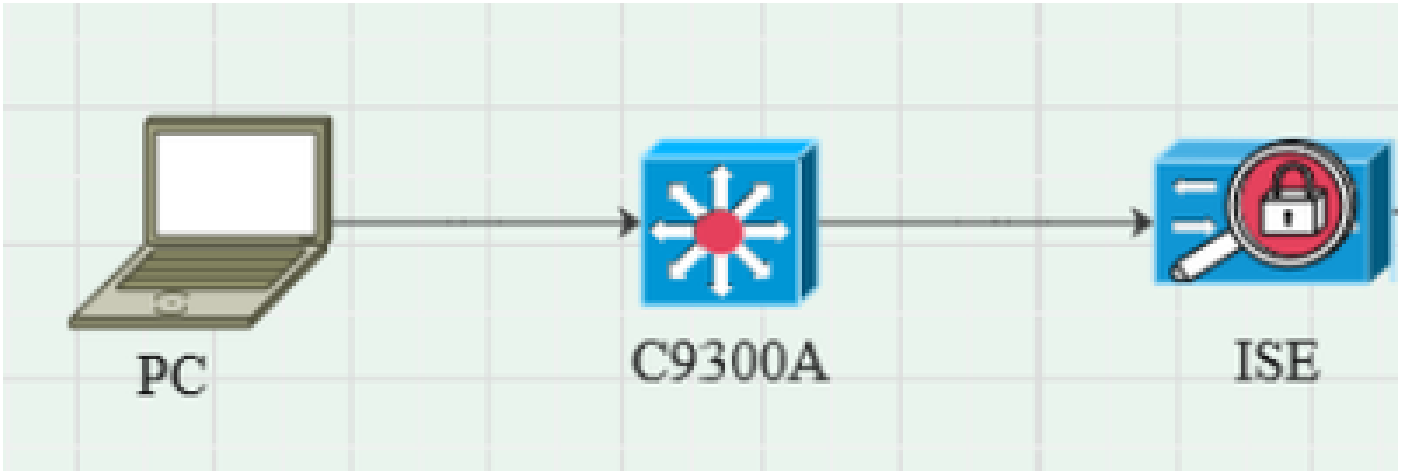
권한 부여 정책은 Cisco ISE(Identity Services Engine)의 주요 구성 요소로, 네트워크 리소스에 액세스하는 특정 사용자 또는 그룹에 대한 규칙을 정의하고 권한 부여 프로파일을 구성할 수 있습니다. 이러한 정책은 조건을 평가하여 적용할 프로필을 결정합니다. 규칙의 조건이 충족되면 해당 권한 부여 프로파일이 반환되어 적절한 네트워크 액세스를 허용합니다.

Cisco ISE는 또한 지정 된 시간 또는 일 동안만 정책을 적용 할 수 있는 시간 및 날짜 조건을 지원 합니다. 이는 시간 기반 비즈니스 요구 사항에 따라 액세스 제어를 적용하는 데 특히 유용합니다.

이 문서에서는 업무 시간(월~금, 08:00~17:00) 동안에만 TACACS+ 관리자가 네트워크 디바이스에 액세스할 수 있도록 하고 이 시간 창을 벗어난 시간에는 액세스를 거부하도록 하는 컨피그레이션에 대해 설명합니다.

구성

네트워크 다이어그램



ISE 구성

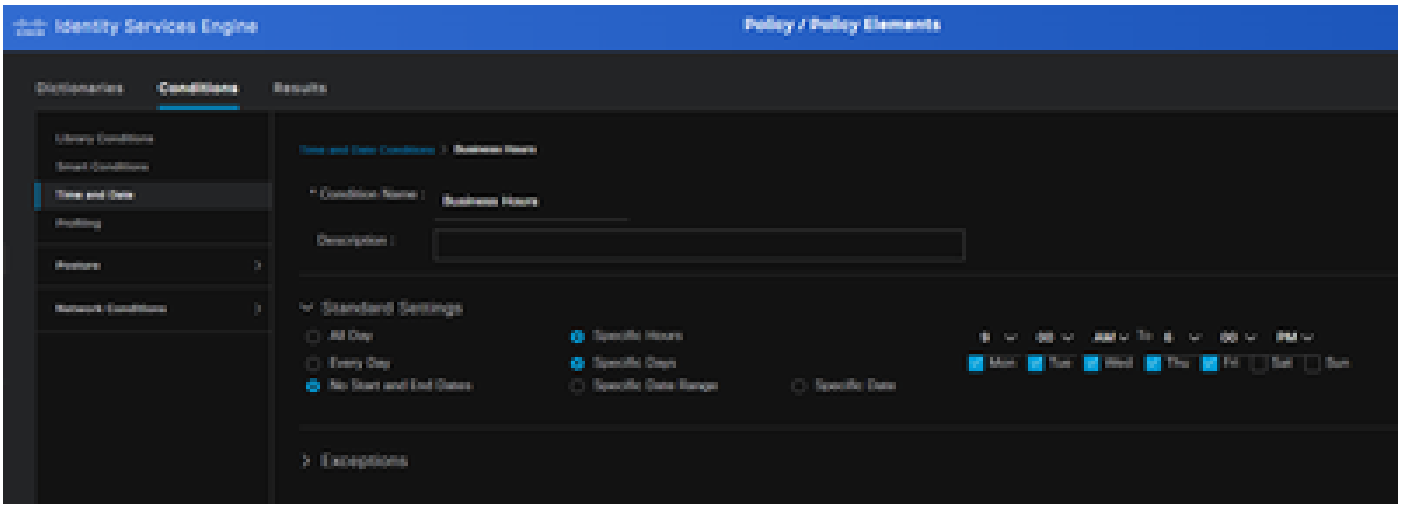
1단계: 시간 및 날짜 조건 생성

Policy(정책) > Policy Elements(정책 요소) > Conditions(조건) > Time and Date(시간 및 날짜)로 이동하고 Add(추가)를 클릭합니다.

조건 이름: 업무 시간

시간 범위 표준 설정 > 특정 시간 설정: 오전 9:00 - 오후 6:00

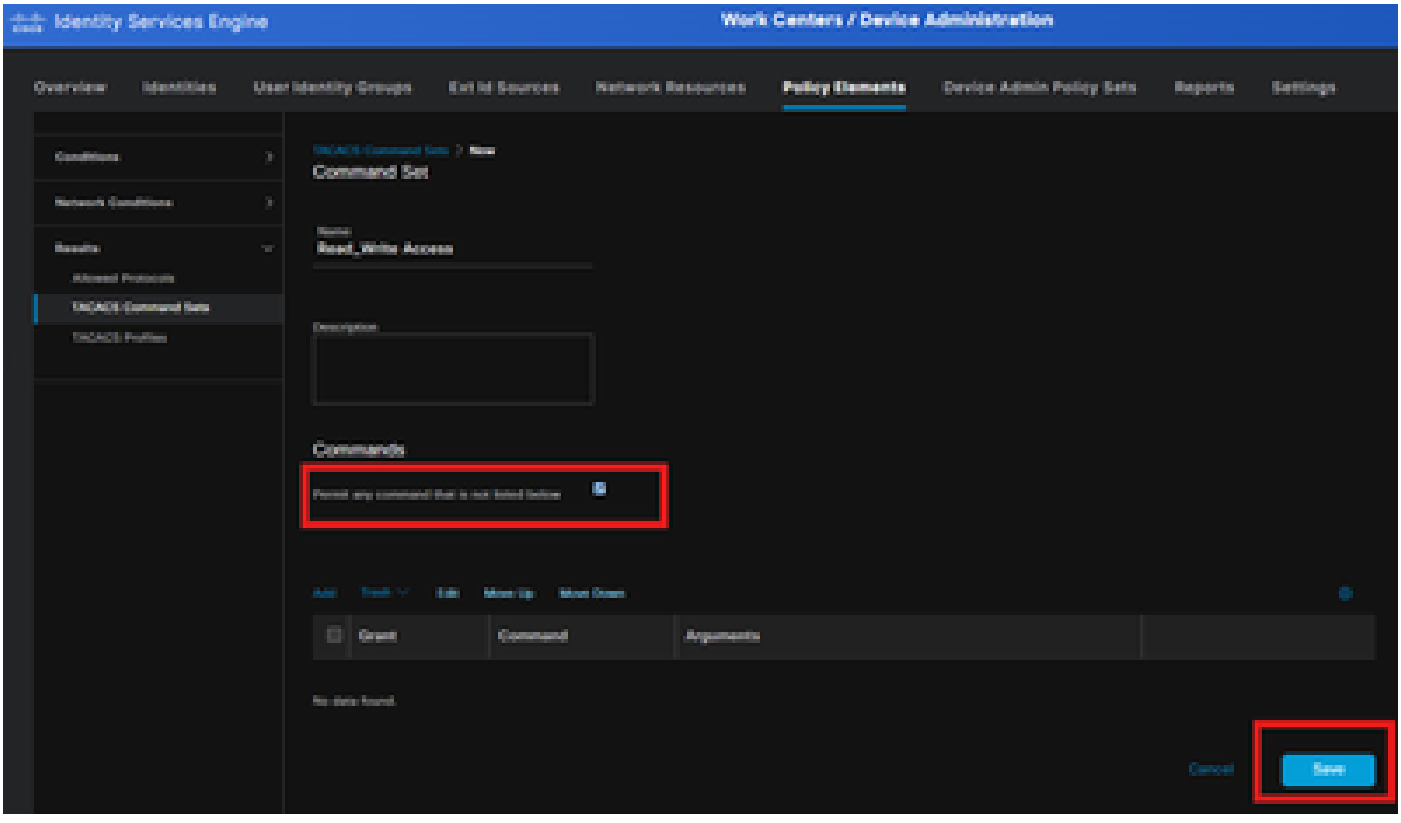
특정 날짜: 월~금



2단계: TACACS+ 명령 집합 생성

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > Tacacs Command Sets(Tacacs 명령 집합)로 이동합니다.

아래 나열되지 않은 모든 명령 허용 확인란을 선택하여 명령 집합을 만들고 특정 CLI 명령을 제한하려면 Submit(제출)을 클릭하거나 Limited Commands(제한된 명령)를 추가합니다.

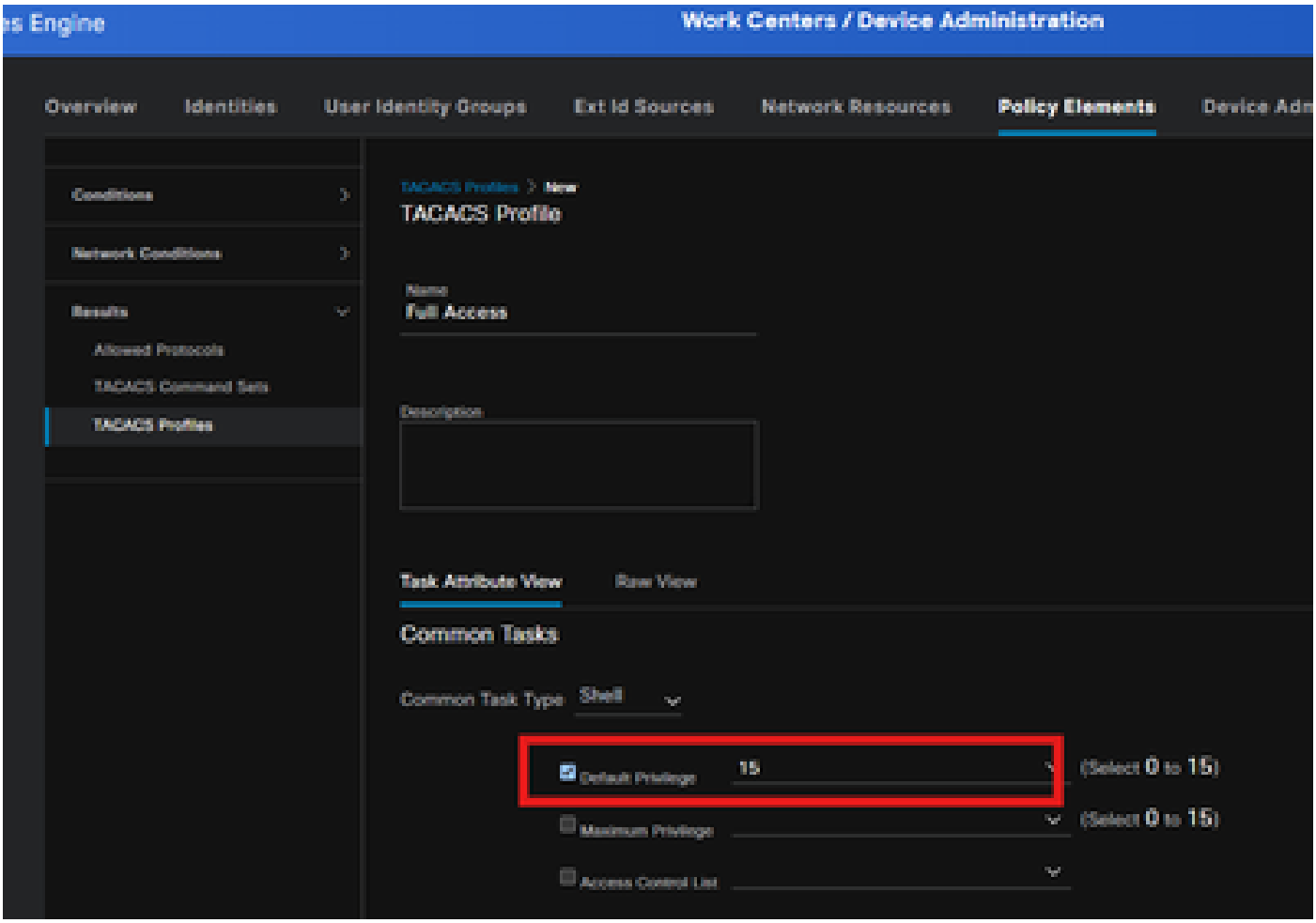


3단계: TACACS+ 프로파일 생성

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Policy Elements(정책 요소) > Results(결과) > TACACS Profiles(TACACS 프로파일)로 이동합니다. Add(추가)를 클릭합니다.

셸로 명령 작업 유형을 선택한 다음 기본 권한 확인란을 선택하고 값 15를 입력합니다. 제출을 누릅

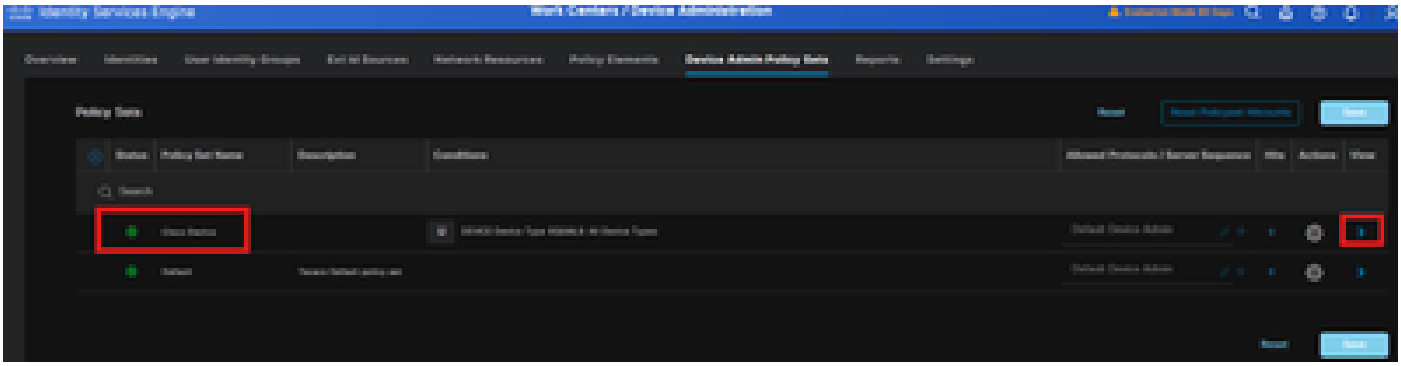
니다.



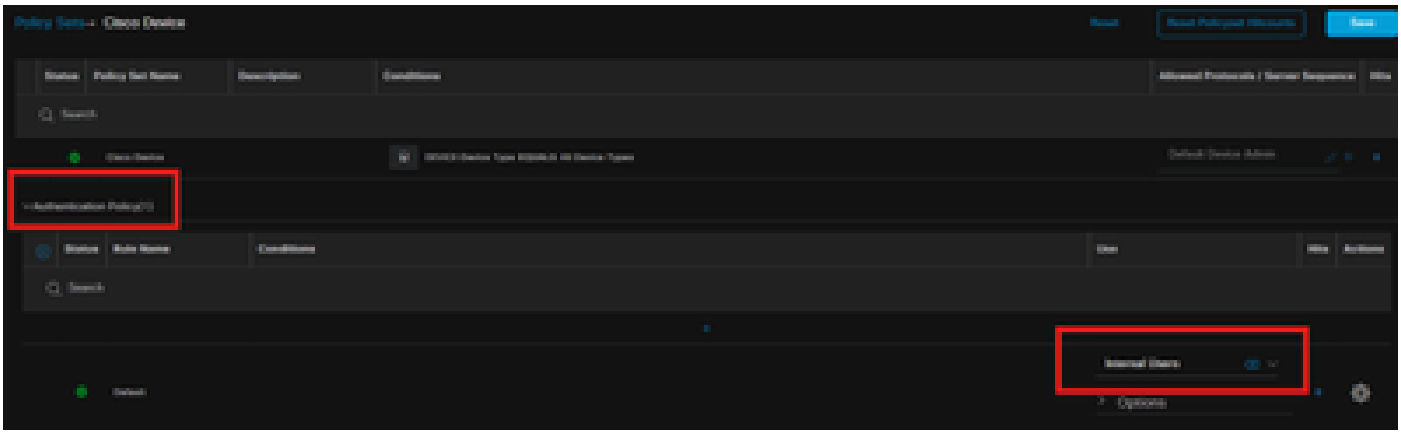
4단계: TACACS 권한 부여 정책 생성

Work Centers(작업 센터) > Device Administration(디바이스 관리) > Device Admin Policy Sets(디바이스 관리 정책 집합)로 이동합니다.

활성 정책 집합을 선택합니다.



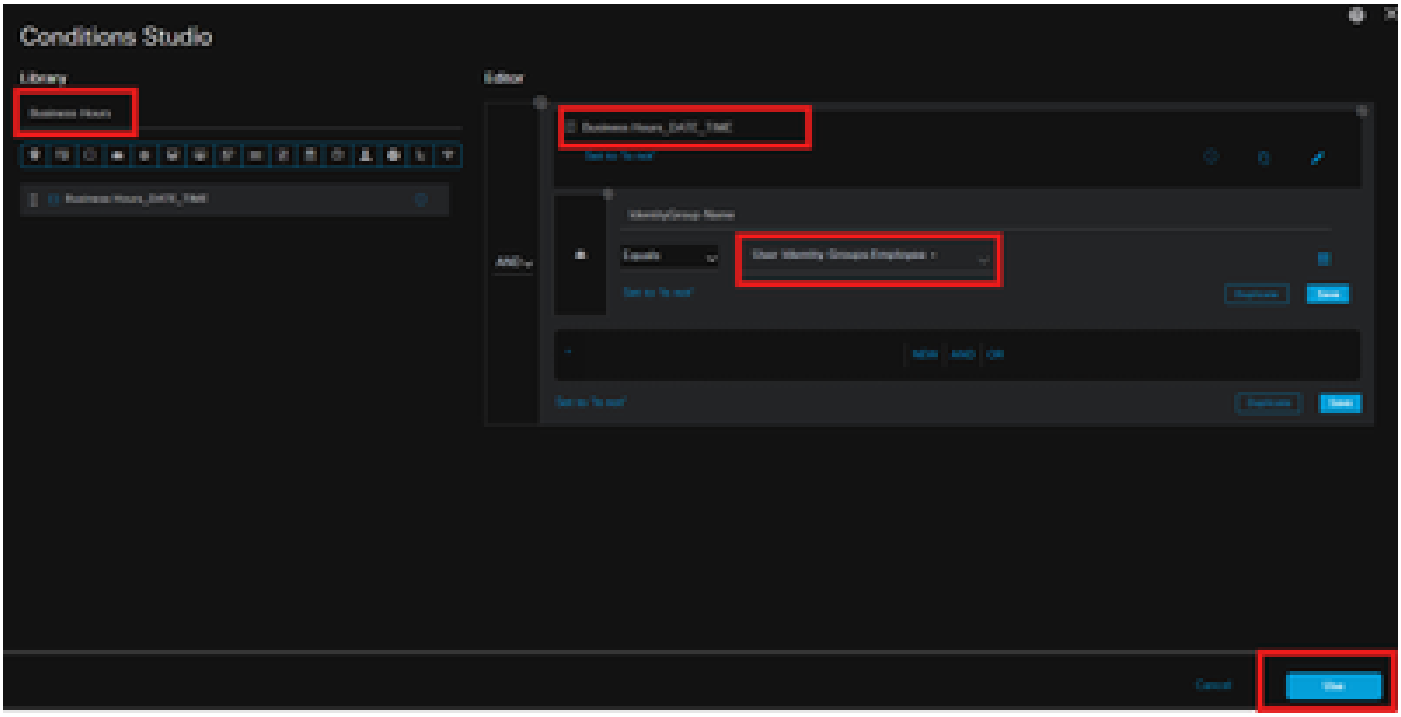
내부 또는 Active Directory 사용자를 기반으로 인증 정책을 구성합니다.



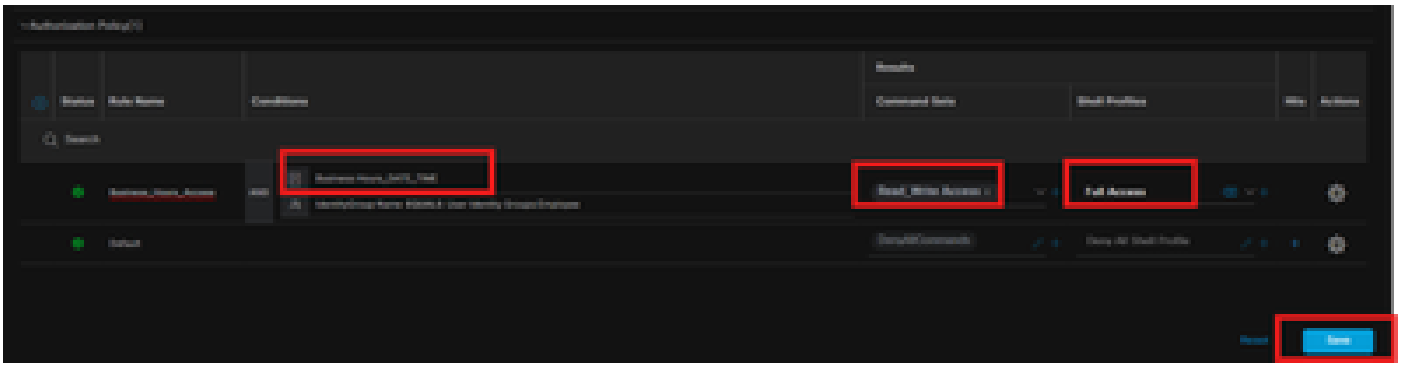
Authorization Policy(권한 부여 정책) 섹션에서 Add Rule(규칙 추가)을 클릭하여 규칙 이름을 제공한 다음 +를 클릭하여 권한 부여 조건을 추가합니다.

새 Condition Studio 창이 나타납니다. Search by Name 필드에 1단계에서 만든 이름을 입력하고 편집기로 끕니다.

User Group(사용자 그룹)에 따라 조건을 추가하고 Save(저장)를 클릭합니다.



Results(결과)에서 2단계와 3단계에서 생성한 Tacacs Command Set and Shell Profile(Tacacs 명령 집합 및 셸 프로파일)을 선택한 다음 Save(저장)를 클릭합니다.

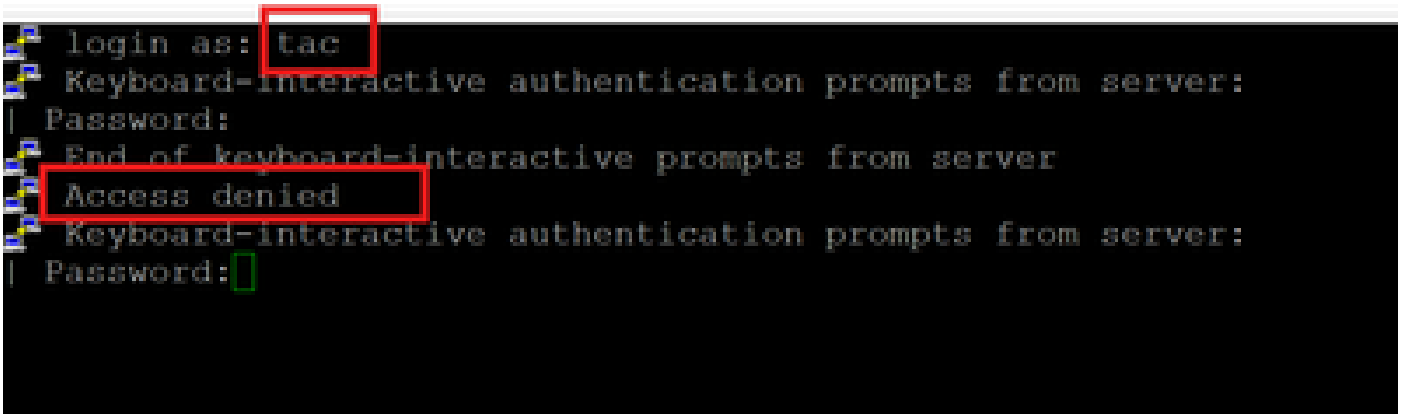


스위치 구성

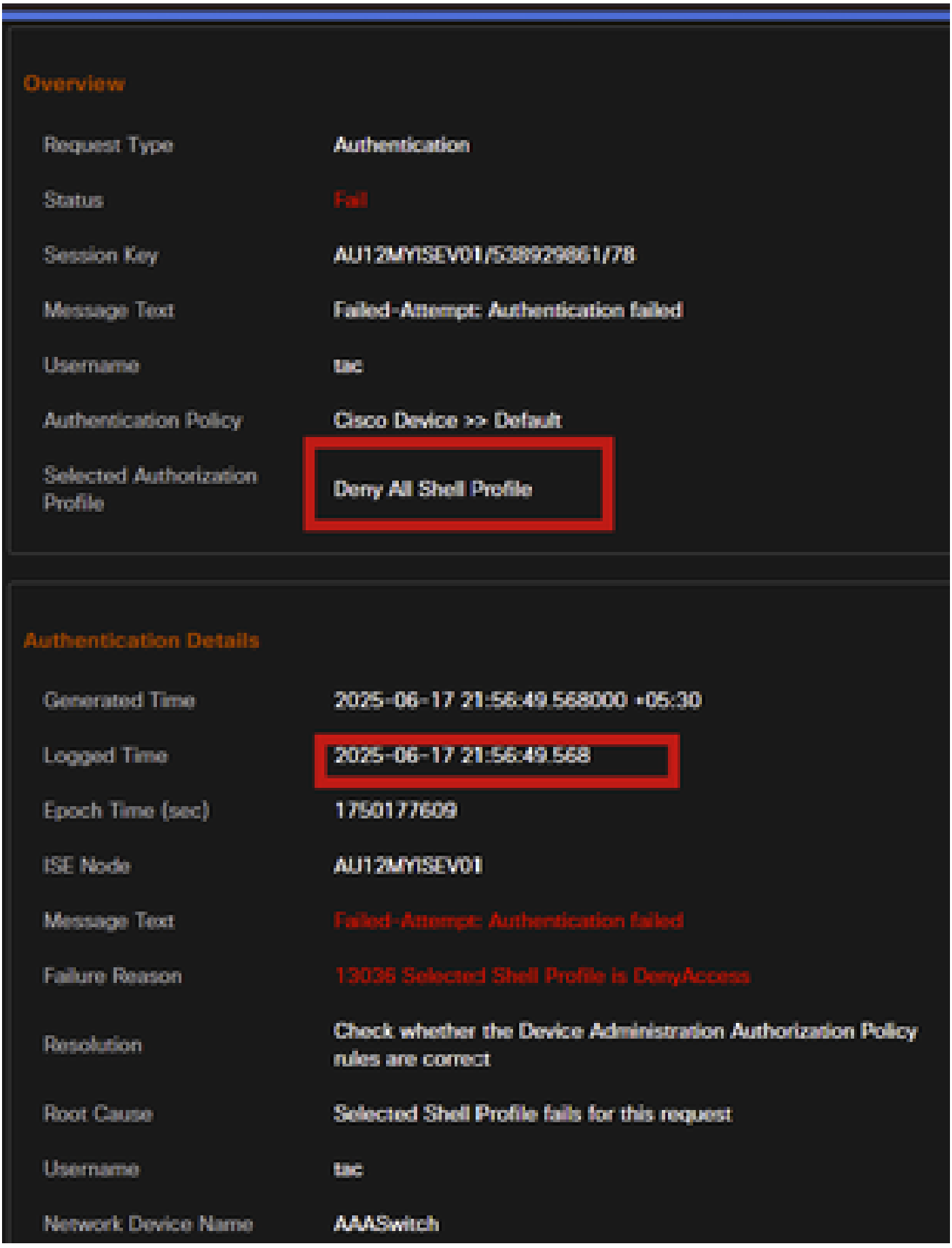
```
aaa 새 모델

aaa 인증 로그인 기본 로컬 그룹 tacacs+
aaa 인증 enable default enable group tacacs+
aaa authorization config-명령
aaa authorization exec 기본 로컬 그룹 tacacs+
aaa authorization 명령 0 기본 로컬 그룹 tacacs+
aaa authorization 명령 1 기본 로컬 그룹 tacacs+
aaa authorization 명령 15 기본 로컬 그룹 tacacs+

tacacs 서버 ISE
주소 ipv4 10.127.197.53
키 Qwerty123
```

다음을 확인합니다.

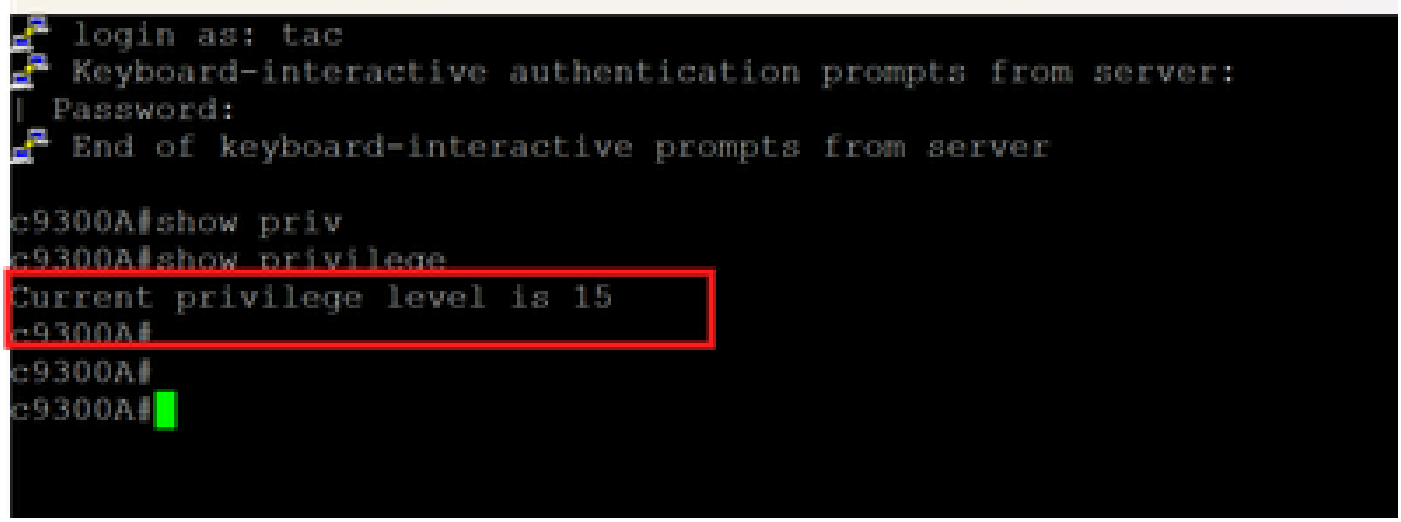
업무 시간 외에 스위치로 SSH를 시도한 사용자가 ISE에서 액세스를 거부했습니다.



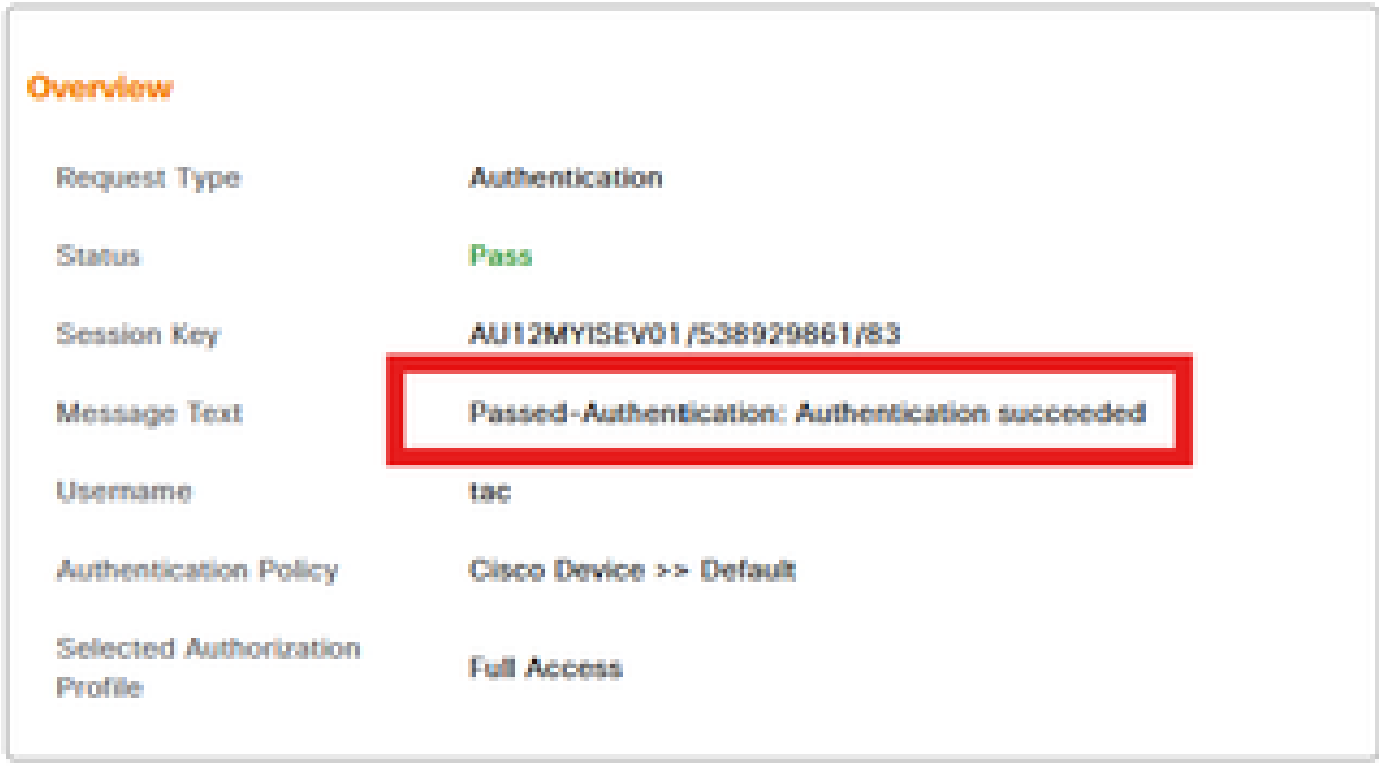
ISE 라이브 로그는 권한 부여 정책의 시간 및 날짜 조건이 일치하지 않아 세션이 기본 액세스 거부 규칙을 적중했기 때문에 권한 부여가 실패했음을 나타냅니다.

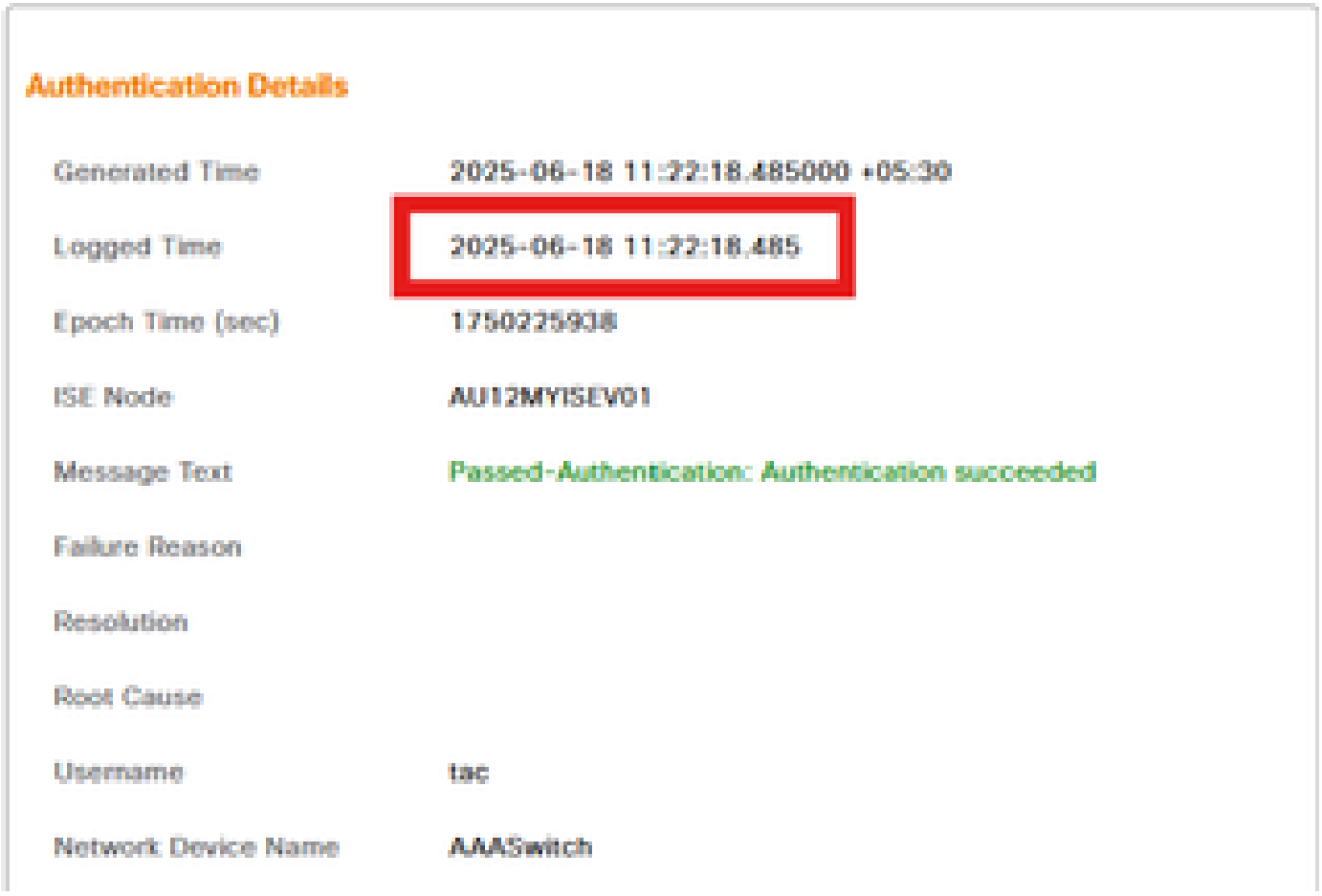


업무 시간 중에 스위치에 SSH를 적용하고 읽기/쓰기 액세스를 시도하는 사용자:



ISE Live Log(ISE 라이브 로그)는 업무 시간 동안 로그인이 Time and Date(시간 및 날짜) 조건과 일치하며 올바른 Policy(정책)에 도달했음을 나타냅니다.





문제 해결

ISE에서 디버깅

디버그 레벨에서 설정할 이러한 특성으로 ISE 지원 번들을 수집합니다.

- RuleEngine-Policy-IDGroups
- RuleEngine 특성
- 정책 엔진
- epm-pdp
- epm-pip

시간 및 날짜 조건이 구성된 업무 시간과 일치하지 않아 사용자가 업무 시간 외에 스위치에 SSH를 시도하는 경우.

show logging application ise-psc.log

```
2025-06-17 21:56:49,560 디버그 [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831: 규칙 평가 중 - <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<조건 Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-operand="rhsoperand"/>
</Rule>
2025-06-17 21:56:49,560 디버그 [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831: ID가 72483811-ba39-4cc2-bdac-90a38232b95e - LHS 피연산자 ID - 피연산자 ID, 연산자 DATETIME_MATCHES, RHS 피연산자 ID - rhsoperand인 조건 평가
2025-06-17 21:56:49,560 디버그 [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.ConditionUtil -::::-
360158683110.127.197.5449306Authentication3601586831: 조건 lhsoperand 값 -
com.cisco.cpm.policy.DTConstraint@6924136c , rhsoperand 값 -
com.cisco.cpm.policy.DTConstraint@3eeea825
2025-06-17 21:56:49,560 디버그 [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831: 조건 - 72483811-ba39-4cc2-bdac-90a38232b95e에 대한 평가 결과가 반환됨 - false
2025-06-17 21:56:49,560 디버그 [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831: 조건에 대한 설정 결과: 72483811-ba39-4cc2-bdac-90a38232b95e : 틀려
```

업무 시간 중에 사용자가 스위치에 SSH를 시도하면 시간 및 날짜 조건이 일치합니다.

show logging application ise-psc.log

```
2025-06-18 11:22:18,473 디버그 [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911: 규칙 평가 중 - <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<조건 Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-operand="rhsoperand"/>
</Rule>

2025-06-18 11:22:18,474 디버그 [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911:
```

ID가 72483811-ba39-4cc2-bdac-90a38232b95e - LHS 피연산자 ID - 피연산자 ID, 연산자 DATETIME_MATCHES, RHS 피연산자 ID - rhsoperand인 조건 평가
2025-06-18 11:22:18,474 디버그 [PolicyEngineEvaluationThread-11][[]] cpm.policy.eval.utils.ConditionUtil -::::- 181675991110.127.197.5414126Authentication1816759911: 조건 lhsoperand 값 - com.cisco.cpm.policy.DTConstraint@4af10566 , rhsoperand 값 - com.cisco.cpm.policy.DTConstraint@2bdb62e9
2025-06-18 11:22:18,474 디버그 [PolicyEngineEvaluationThread-11][[]] cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911: 조건 - 72483811-ba39-4cc2-bdac-90a38232b95e에 대한 평가 결과가 반환되었습니다. - true
2025-06-18 11:22:18,474 디버그 [PolicyEngineEvaluationThread-11][[]] cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911: 조건에 대한 설정 결과: 72483811-ba39-4cc2-bdac-90a38232b95e : 참

관련 정보

- Cisco ISE Device Administration 규범적 구축 설명서

자주 묻는 질문(FAQ)

- 시간에 따라 다른 액세스 레벨을 적용할 수 있습니까?
  예. 서로 다른 권한 부여 정책을 생성하고 시간 조건에 연결할 수 있습니다.

  예를 들면 다음과 같습니다.
  업무 시간 동안 전체 액세스
  몇 시간 후 읽기 전용 액세스
  주말에는 액세스 불가

- 시스템 시간이 잘못되었거나 동기화되지 않은 경우 어떻게 됩니까?
  ISE는 잘못된 정책을 적용하거나 시간 기반 규칙을 안정적으로 적용하지 못할 수 있습니다. 모든 디바이스 및 ISE 노드가 동기화된 NTP 소스를 사용하는지 확인합니다.

- 시간 기반 정책을 다른 조건(예: 사용자 역할, 장치 유형)과 함께 사용할 수 있습니까?
  예. 시간 조건을 정책 규칙의 다른 특성과 결합하여 세분화되고 안전한 액세스 제어를 생성할 수 있습니다.

- TACACS의 셸 및 명령 집합 모두에 대해 시간 기반 액세스가 지원됩니까+?
  예. 시간 기반 조건은 권한 부여 정책 및 프로필의 구조에 따라 디바이스 셸 또는 특정 명령 집합에 대한 액세스를 제어할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.