Configure Time-Based TACACS+ Access for Network Devices with ISE

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Network Diagram
- Configure ISE
  - Step 1: Create Time and Date Condition
  - Step 2: Create a TACACS+ Command Set
  - Step 3: Create a TACACS+ Profile
  - Step 4: Create TACACS Authorization Policy
- Configure Switch
- Verify

Troubleshoot

- Debugs on ISE

Related Information

Frequently Asked Questions

Introduction

This document describes how to configure the Time and Date based authorization for Device Admin policy in Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of the Tacacs Protocol and Identity Services Engine (ISE) configuration.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalyst 9300 switch with softwareCisco IOS® XE 17.12.5 and later
- Cisco ISE, Release 3.3 and later

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. If your network is live, ensure

that you understand the potential impact of any command.

Background Information

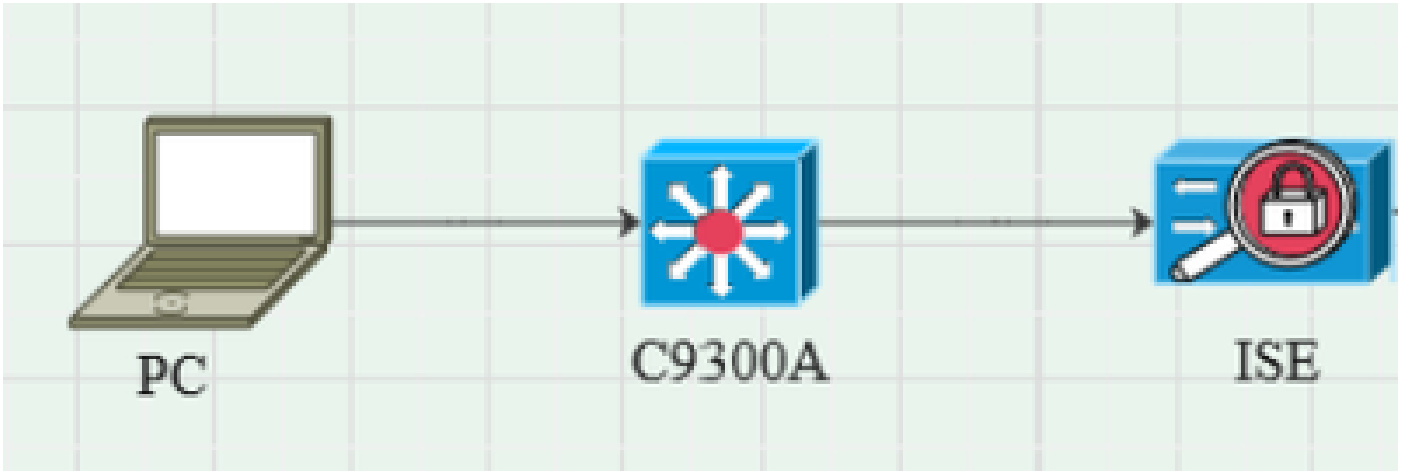
Authorization policies are a key component of Cisco Identity Services Engine (ISE), enabling you to define rules and configure authorization profiles for specific users or groups accessing network resources. These policies evaluate conditions to determine which profile to apply. When the conditions of a rule are met, the corresponding authorization profile is returned, granting appropriate network access.

Cisco ISE also supports Time and Date Conditions, which allow policies to be enforced only during specified times or days. This is particularly useful for applying access controls based on time-based business requirements.

This document outlines the configuration to allow TACACS+ administrative access to network devices only during business hours (Monday to Friday, 08:00–17:00) and to deny access outside of this time window.

Configure

Network Diagram



Configure ISE

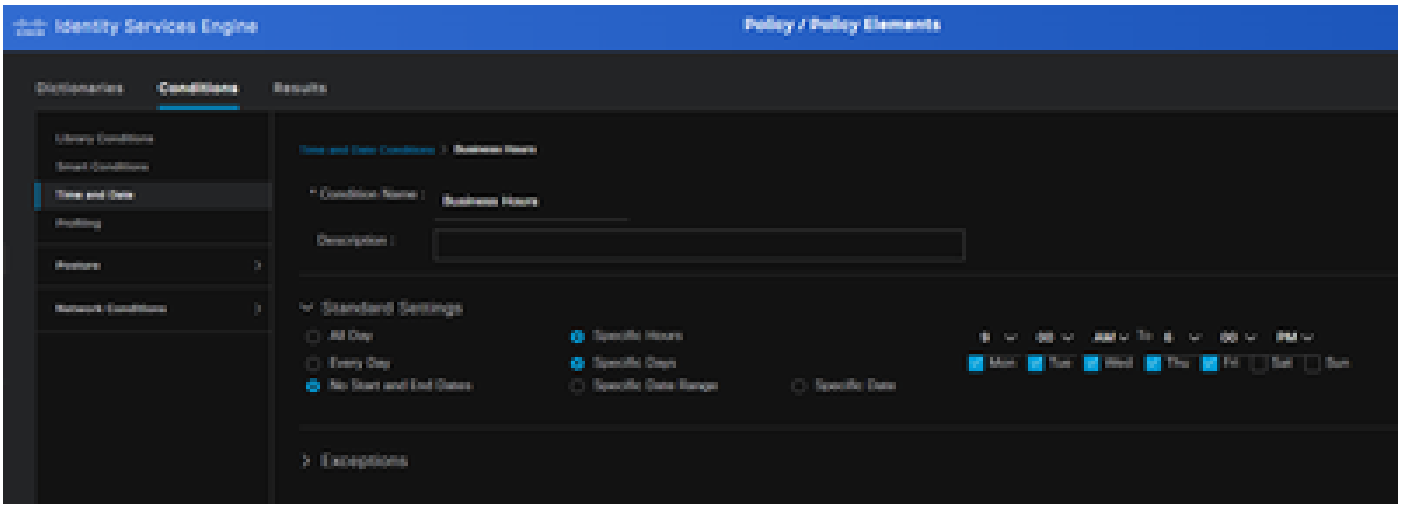
Step 1: Create Time and Date Condition

Navigate to Policy > Policy Elements > Conditions > Time and Date, click Add.

Condition Name: Business Hours

Set the Time Range Standard Settings > Specific Hours : 09:00 AM - 06:00 PM

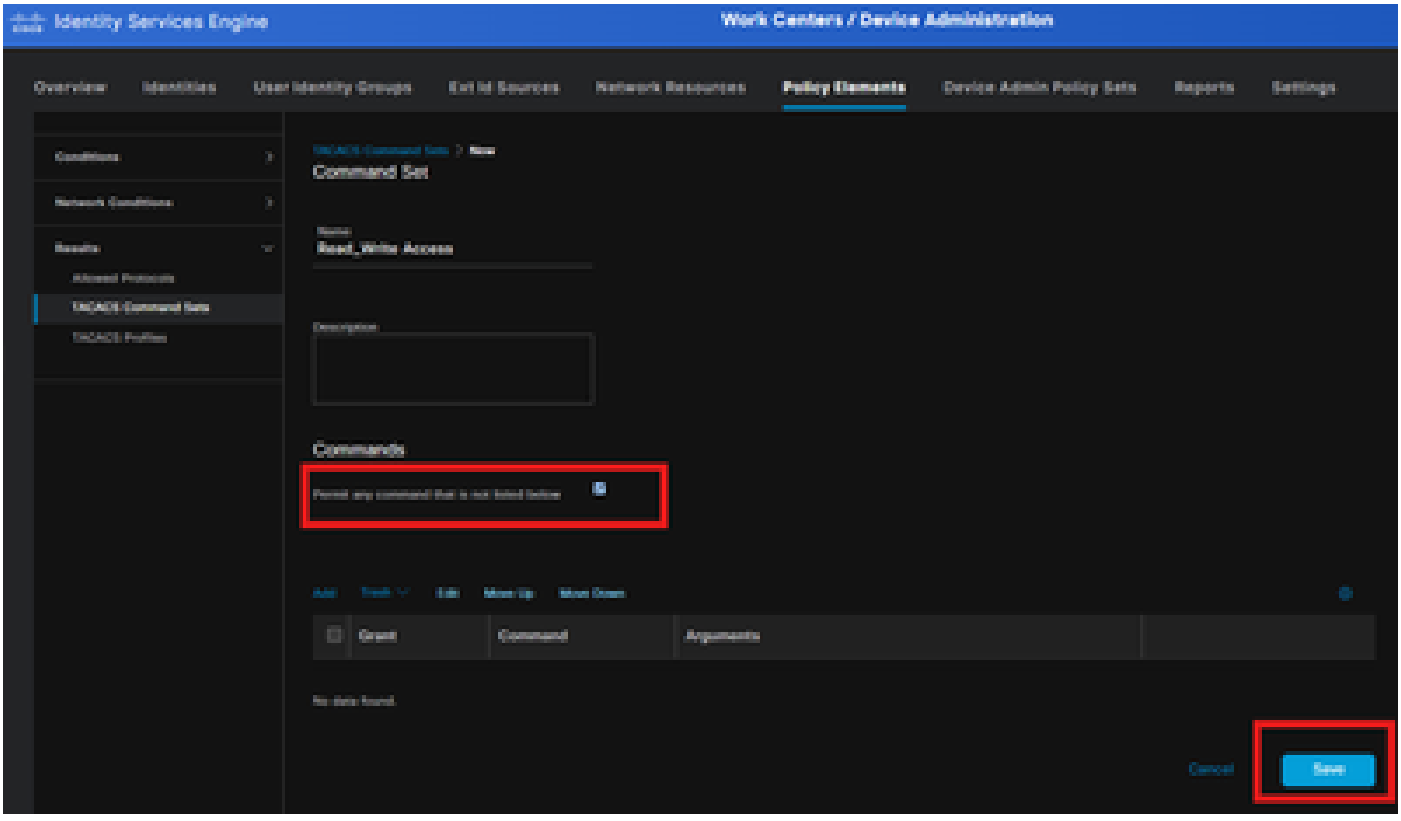
Specific Days: Monday to Friday



Step 2: Create a TACACS+ Command Set

Navigate to **Work Centers > Device Administration > Policy Elements > Results > Tacacs Command Sets**.

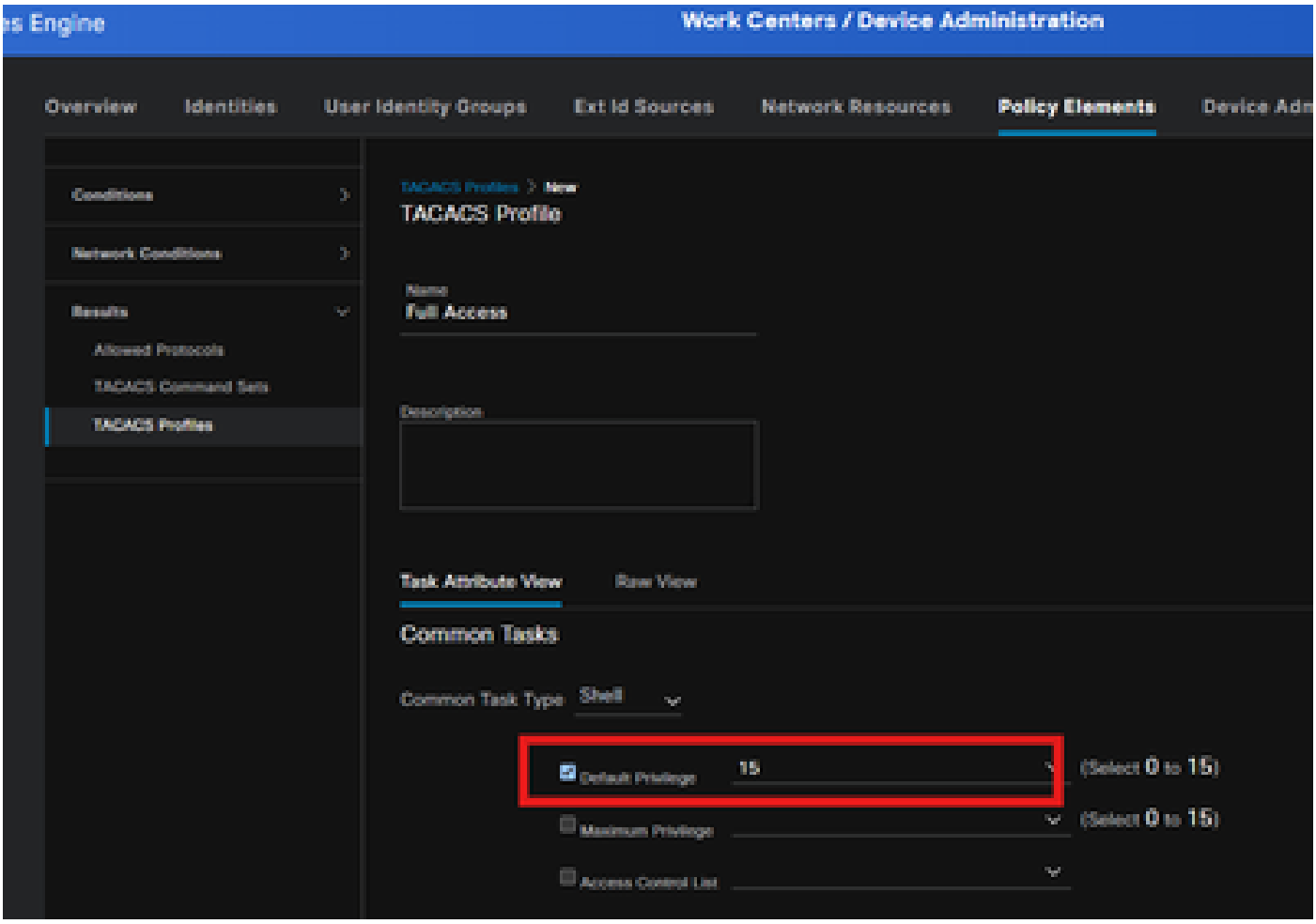
Create a command set by choosing the **Permit any command that is not listed below** checkbox and click **Submit** or add the Limited Commands if you want to restrict certain CLI commands.



Step 3: Create a TACACS+ Profile

Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles.** Click **Add.**

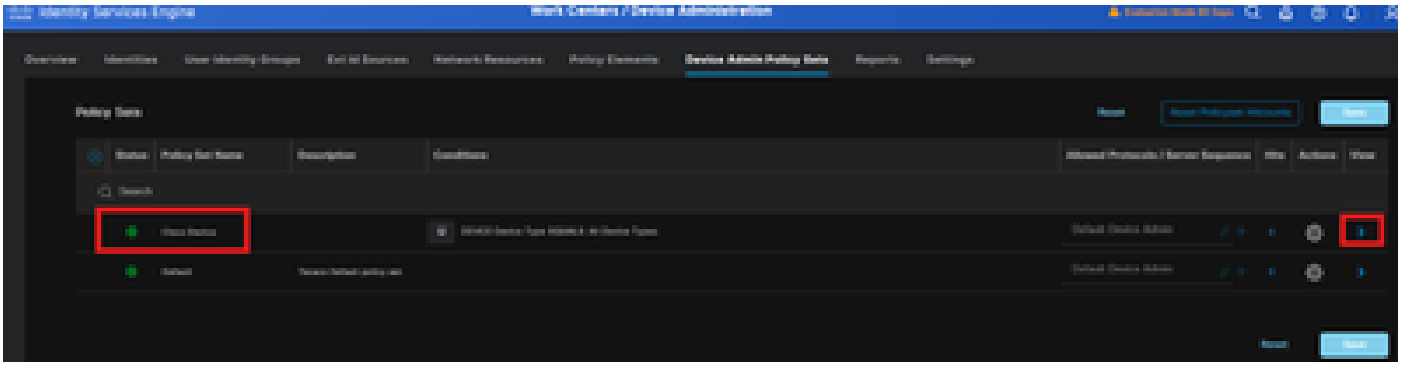
Select **Command Task Type** as **Shell**, then **Default Privilege** checkbox and enter the value of 15. Click **Submit.**



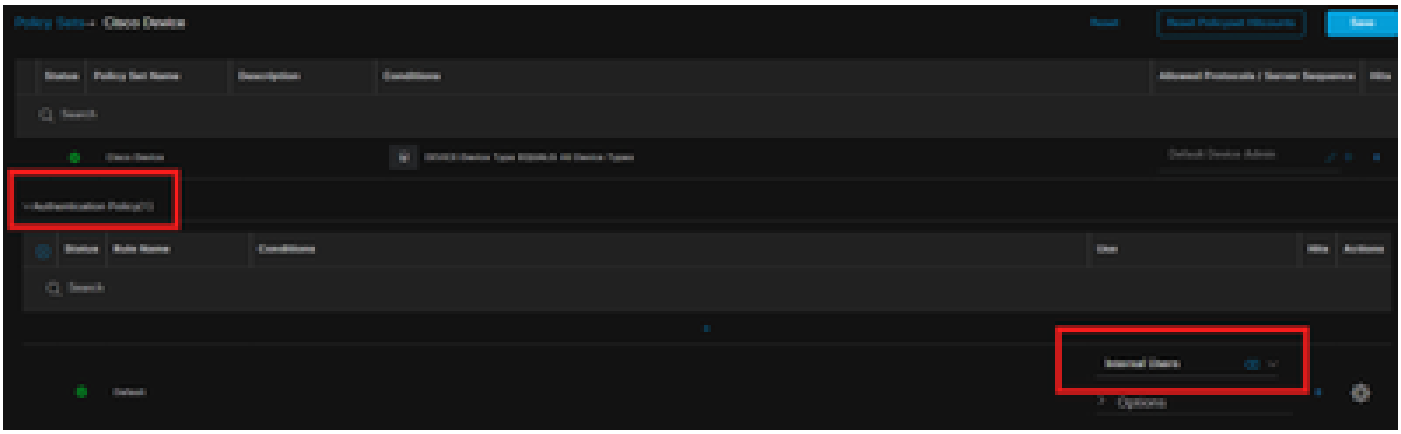
Step 4: Create TACACS Authorization Policy

Navigate to **Work Centers > Device Administration > Device Admin Policy Sets.**

Select your active **Policy Set**.



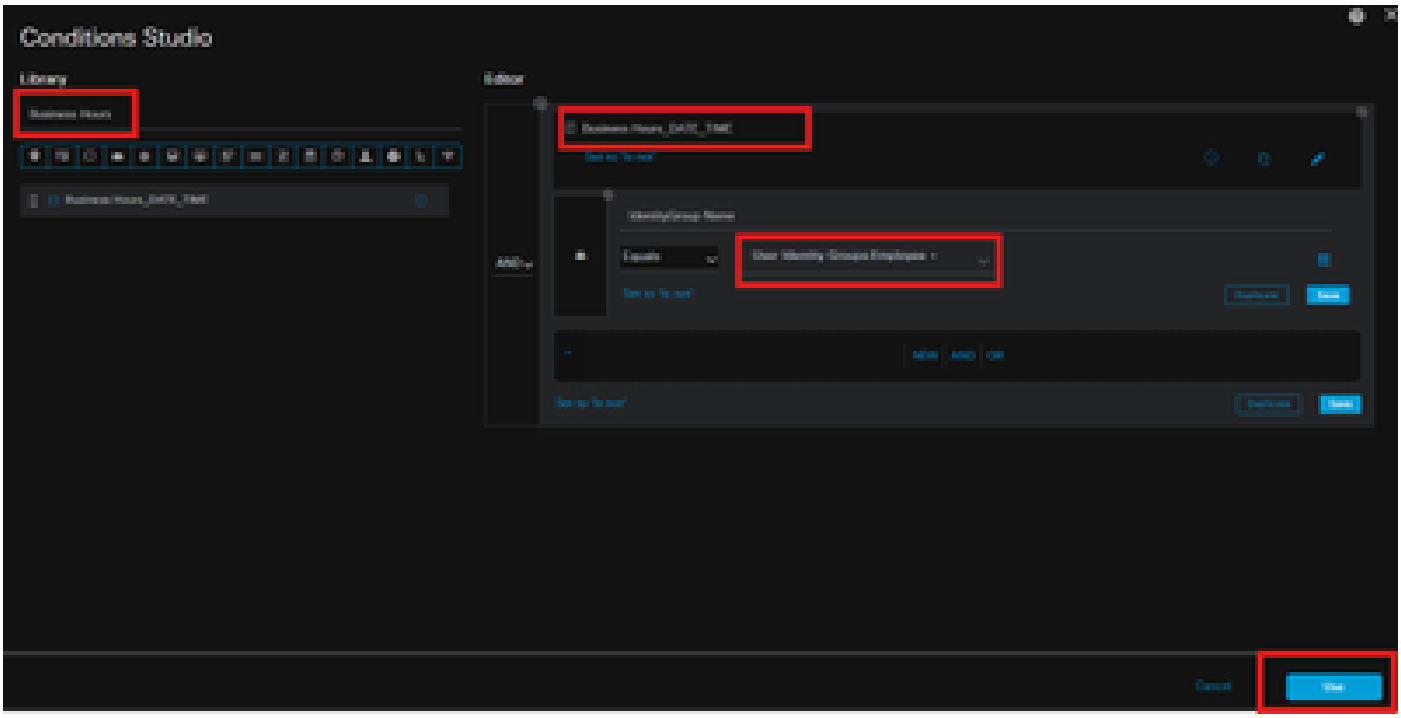
Configure the Authentication Policy based on the Internal or Active Directory users.



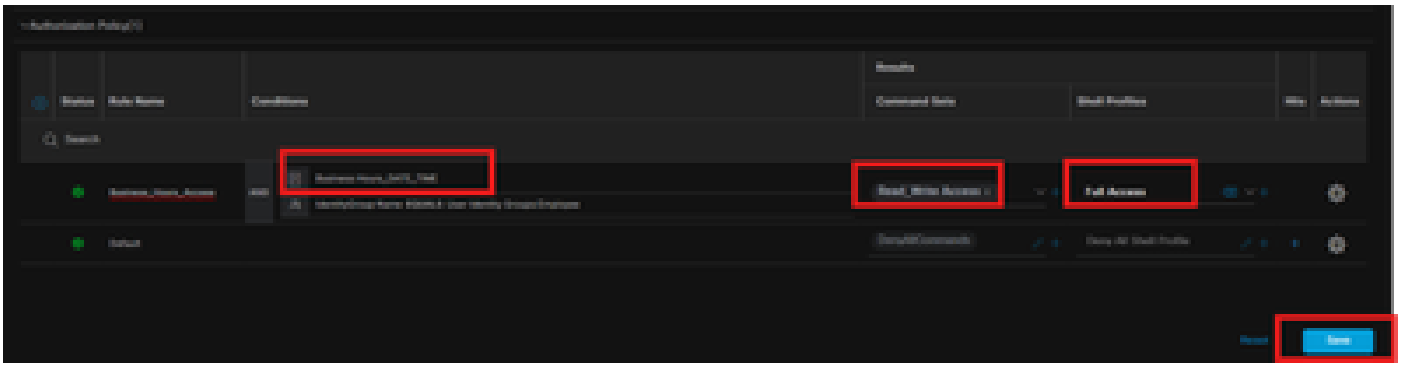
Under the **Authorization Policy** section, click **Add Rule** to provide the Rule Name and then Click + for adding authorization conditions.

A new **Condition Studio** window appears, in Search by Name field enter the name created in step 1 and drag it to the **Editor**.

Add additional conditions based on User Group and click **Save**.



In **Results**, select the Tacacs **Command Set** and **Shell Profile** created in step 2 and step 3 then click **Save**.



Configure Switch

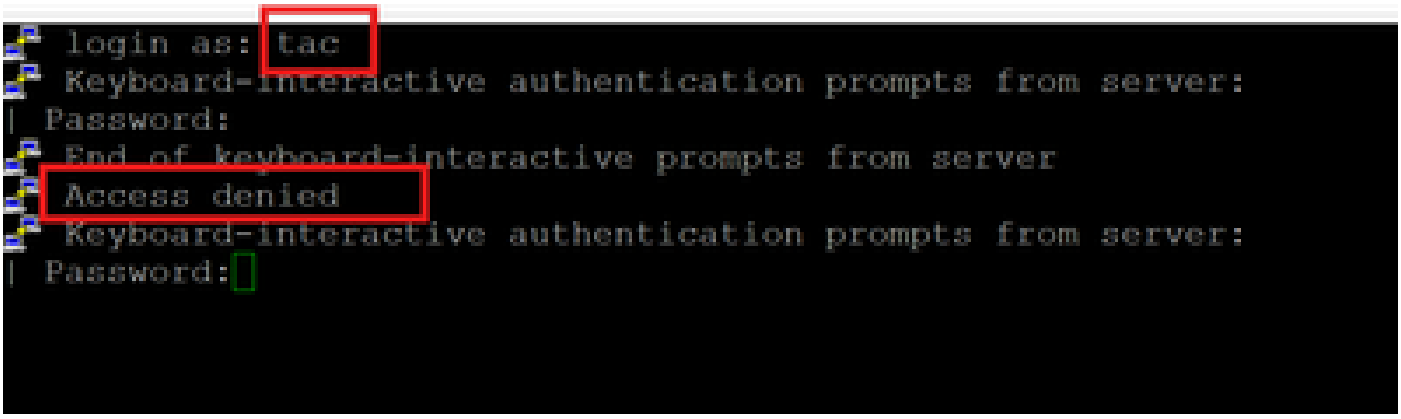
```
aaa new-model

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+

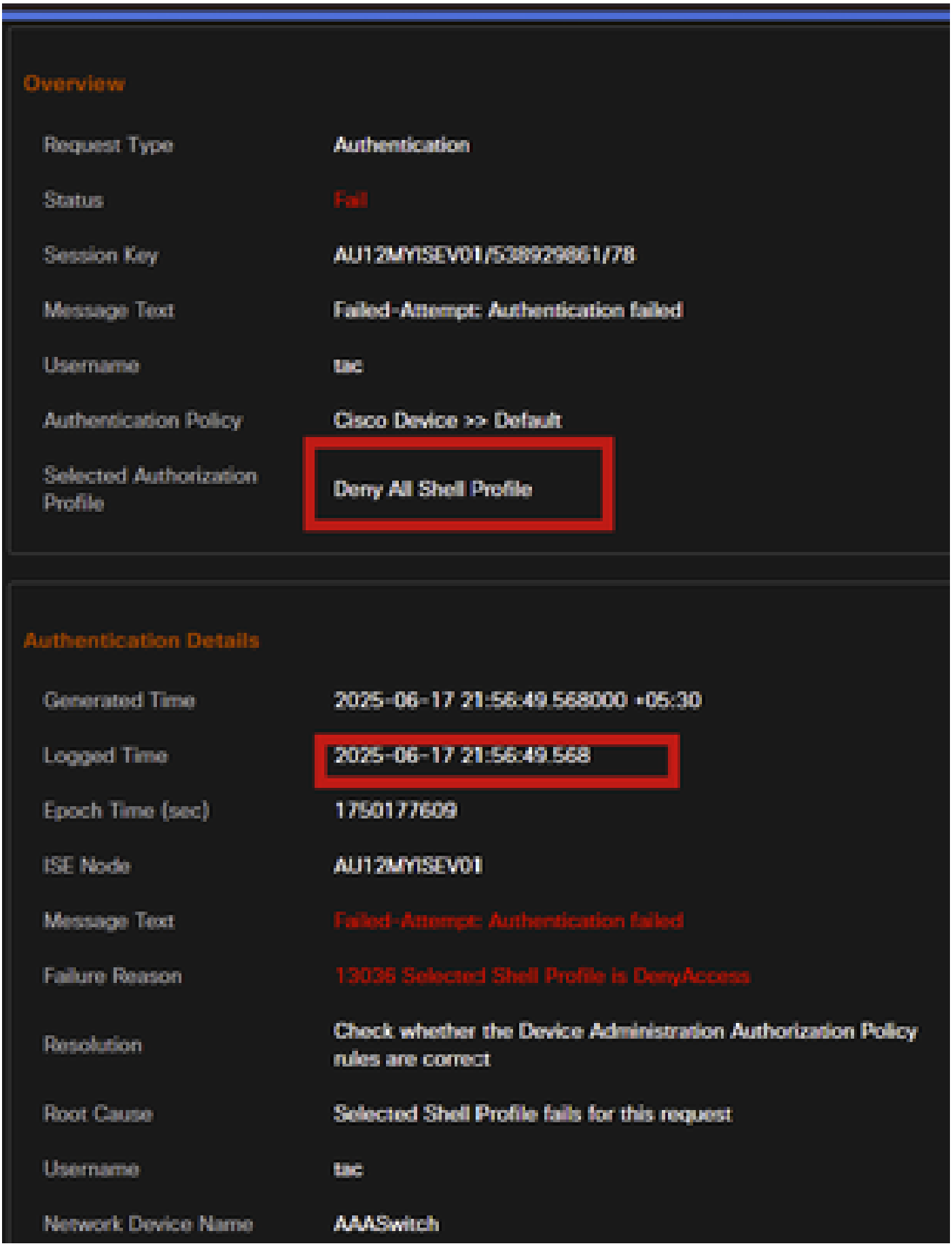
tacacs server ISE
address ipv4 10.127.197.53
key Qwerty123
```

Verify

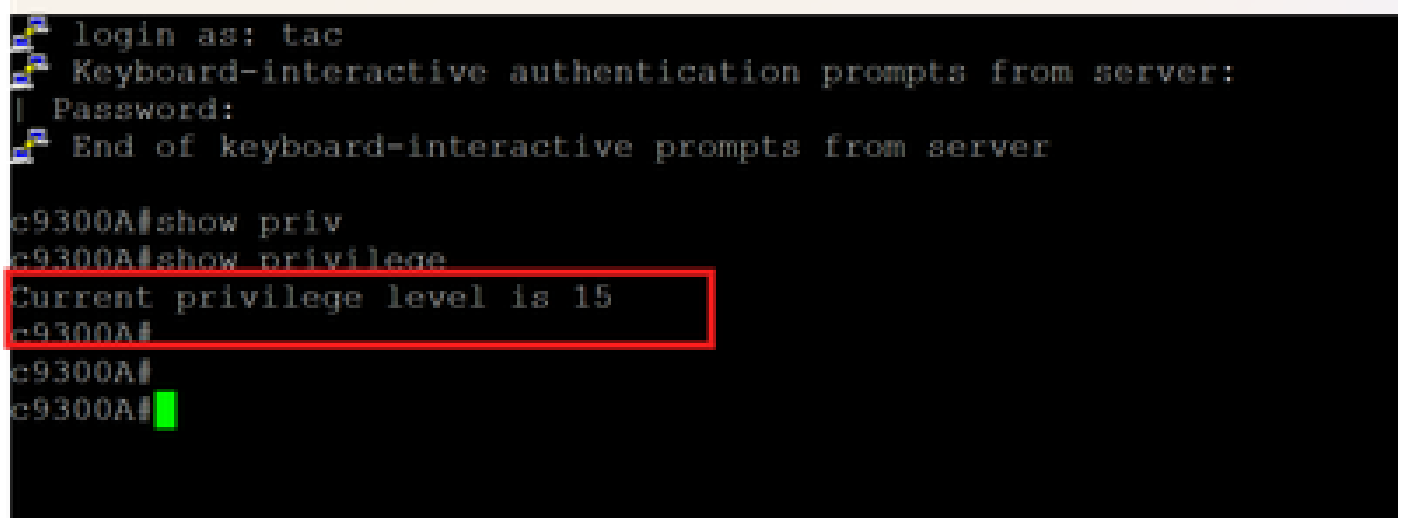
User attempting to SSH into the Switch Outside of Business Hours and got **Access denied** from ISE.



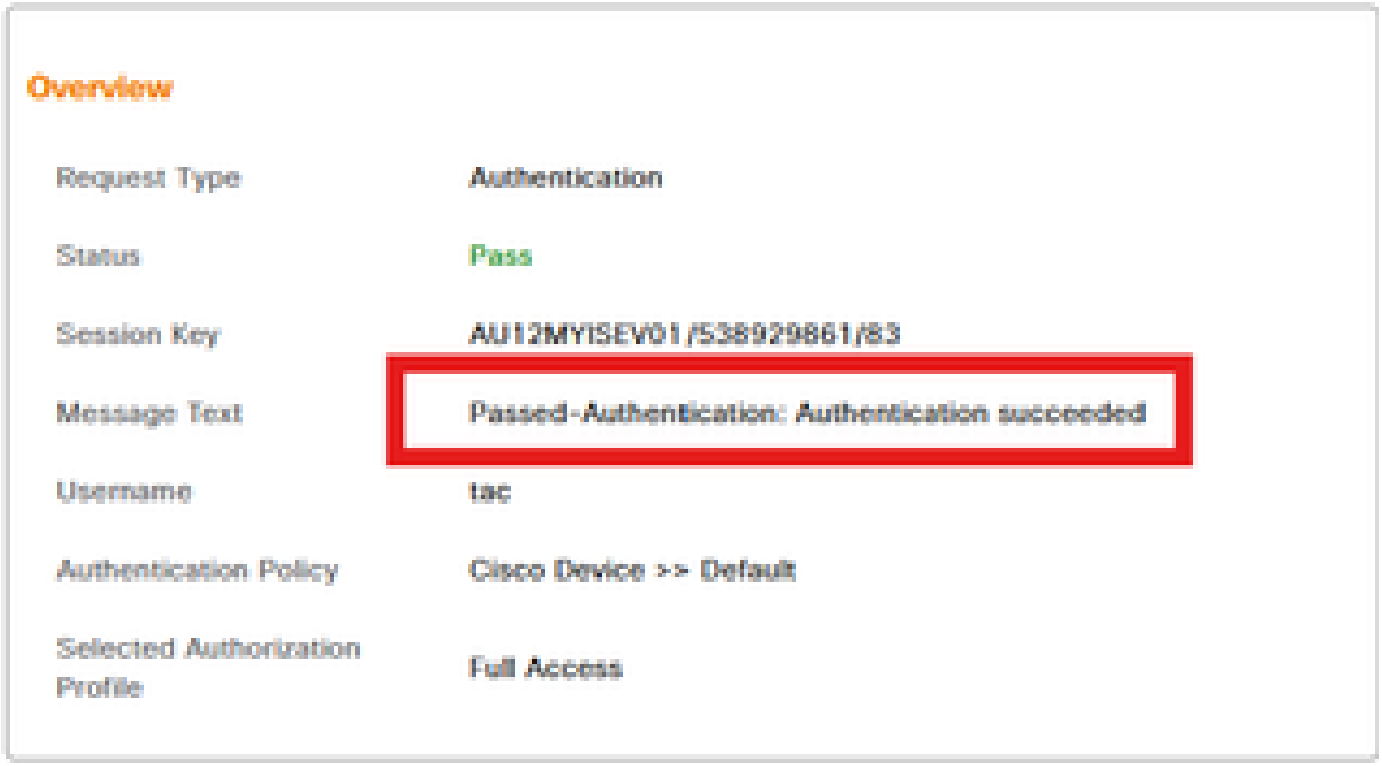
The ISE Live Logs indicate that authorization failed because the Time and Date condition in the authorization policy did not match, resulting in the session hitting the Default Deny Access rule.

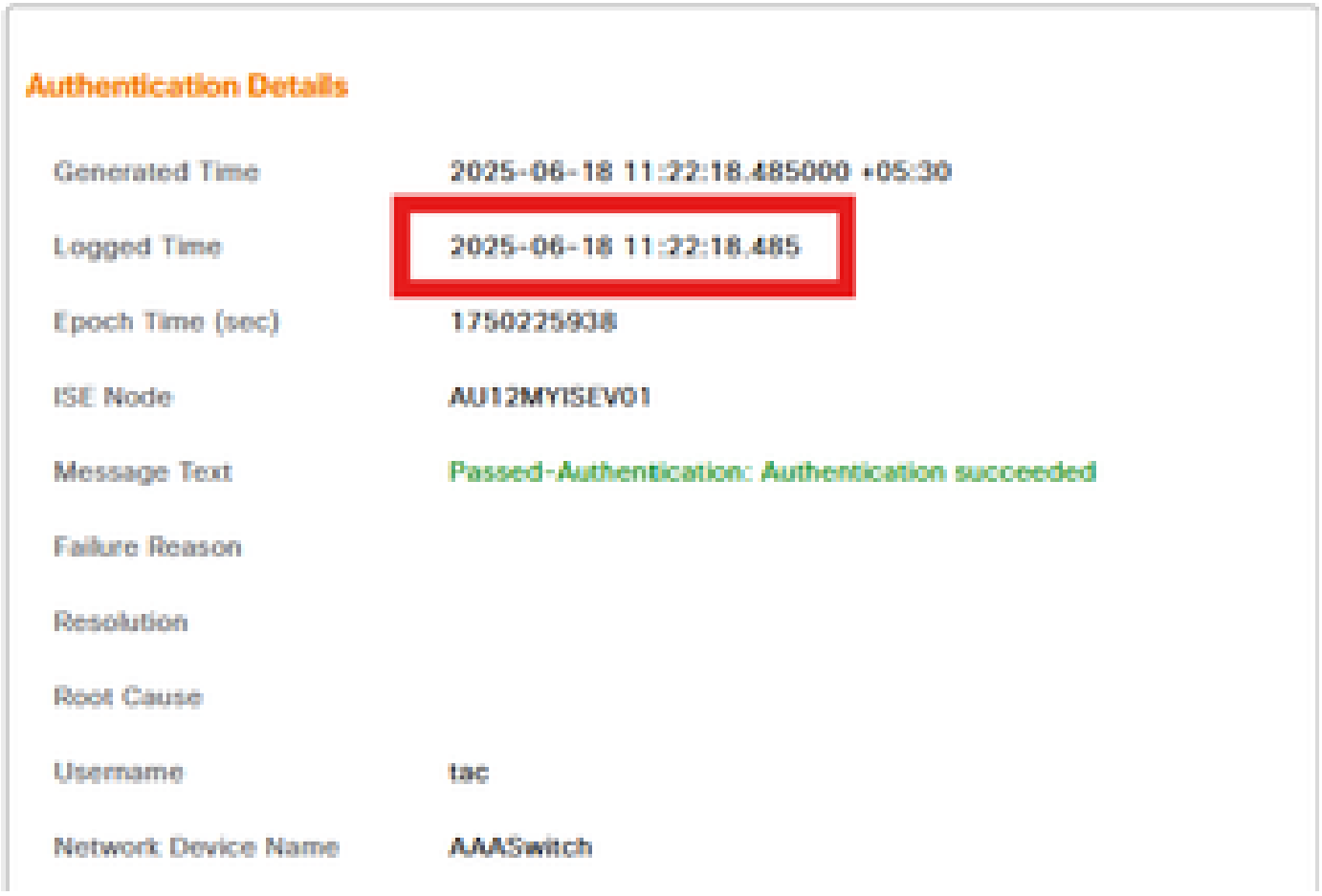


User attempting to SSH into switch during Business Hours and get Read Write Access:



The ISE Live Log indicates that login during Business Hours matched the Time and Date condition and hits correct Policy.





Troubleshoot

Debugs on ISE

Collect the ISE support bundle with these attribute to be set at the debug level:

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

When the User Attempting to SSH into the Switch Outside of Business Hours due to Time and Date Condition not matched with configured business hours.

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: Evaluating rule - <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: Evaluating Condition with 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 -::::- 360158683110.127.197.5449306Authentication3601586831: 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: Evaluation result for Condition - 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: Setting Result for Condition: 72483811-ba39-4cc2-bdac-90a38232b95e : **false**

When the User Attempting to SSH into the Switch during the Business Hours matched the Time and Date Condition.

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: Evaluating rule - <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: Evaluating Condition with 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 -::::- 181675991110.127.197.5414126Authentication1816759911: 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: Evaluation result for Condition - 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: Setting Result for Condition: 72483811-ba39-4cc2-bdac-90a38232b95e : **true**

Related Information

- Cisco ISE Device Administration Prescriptive Deployment Guide

Frequently Asked Questions

- **Can I apply different access levels based on time?**
  Yes. You can create different authorization policies and link them to time conditions.

  For example:
  Full access during business hours
  Read-only access after hours
  No access on weekends

- **What happens if the system time is incorrect or unsynchronized?**
  ISE can apply incorrect policies or fail to enforce time-based rules reliably. Ensure all devices and ISE nodes use a synchronized NTP source.

- **Can time-based policies be used in conjunction with other conditions (for example, user role, device type)?**
  Yes. Time conditions can be combined with other attributes in your policy rules to create granular and secure access controls.

- **Is Time-Based Access supported for both shell and command sets in TACACS+?**
  Yes. Time-based conditions can control access to the device shell or specific command sets, depending on how the authorization policy and profiles are structured.