Configure Alarms Based on Authorization Results on ISE 3.1

Contents

Introduction

This document describes the steps required to configure alarms based on the authorization result for a RADIUS authentication request on Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- RADIUS protocol
- ISE admin access

Components Used

The information in this document is based on Identity Services Engine (ISE) 3.1.

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

In this example, a custom alarm would be configured for a specific authorization profile with a threshold limit defined and if ISE reaches the threshold limit on the configured authorization policy, the alarm would be triggered.

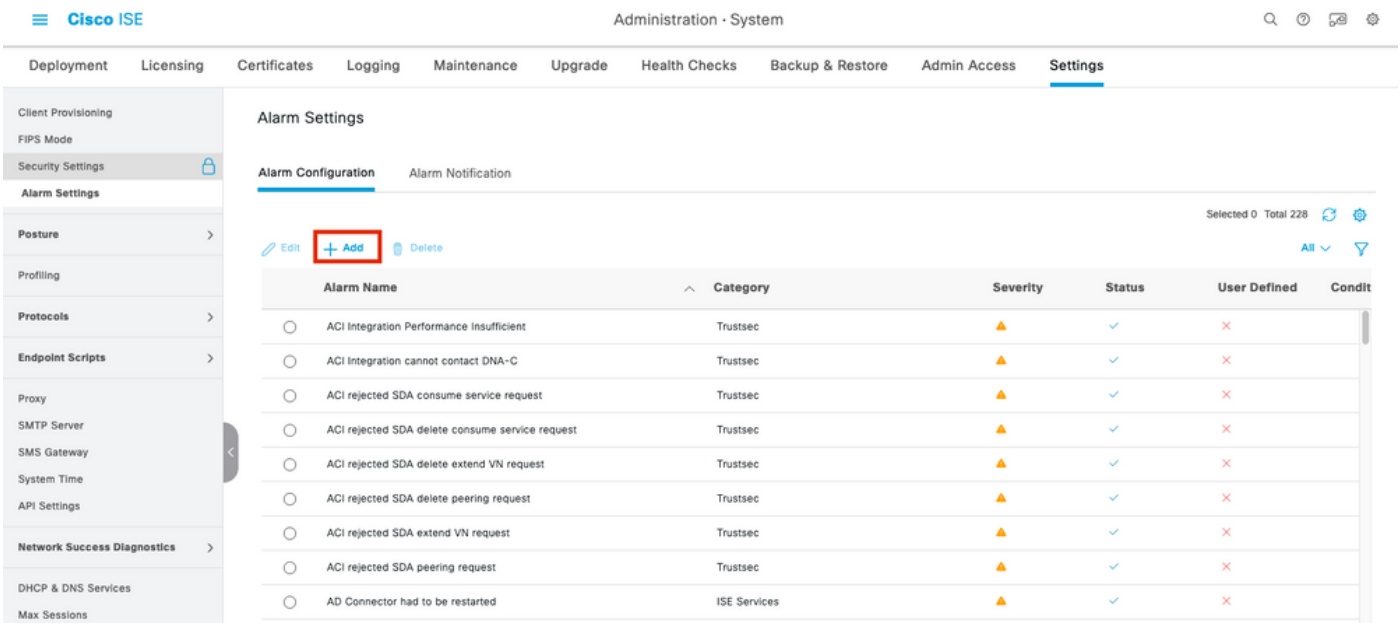
Configure

In this example, we will create an alarm for the authorization profile ("ad_user") pushed when an Active Directory (AD) user logs in and the alarm would be triggered based on the threshold configured.

> **Note**: For a production server, the threshold must be a higher value to avoid large occurrences of the alarm.

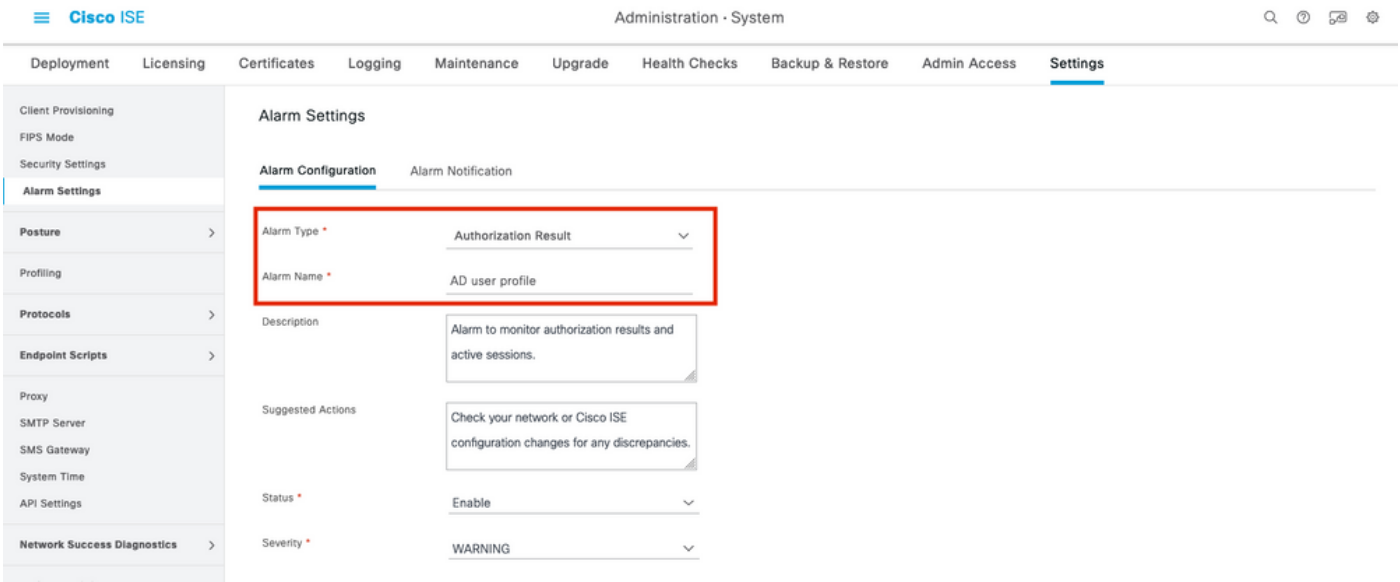
Step 1. Navigate to **Administration > System > Alarm Settings**.

Step 2. Under Alarm Configuration, click **Add** to create an Alarm as shown in the image.



ISE 3.1 alarms based on authorization results - Alarm settings

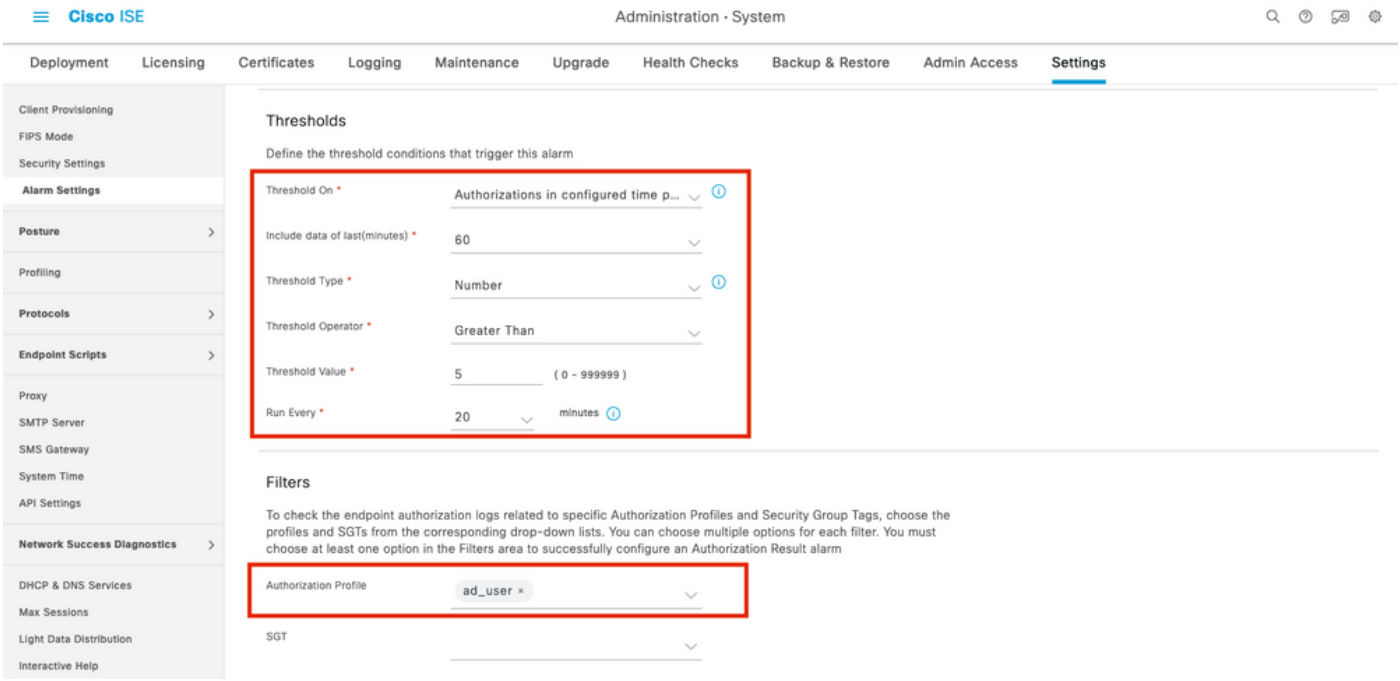
Step 3. Select the Alarm Type as **Authorization Result** and enter the alarm name as shown in the image.



ISE 3.1 alarms based on authorization results - Configure alarm

Step 4. In the **Threshold** section, select **Authorization in configured time period** in Threshold On drop-down and enter appropriate values for Threshold and the mandatory fields. In the filter

section, call the Authorization Profile for which the alarm must be triggered as shown in the image.



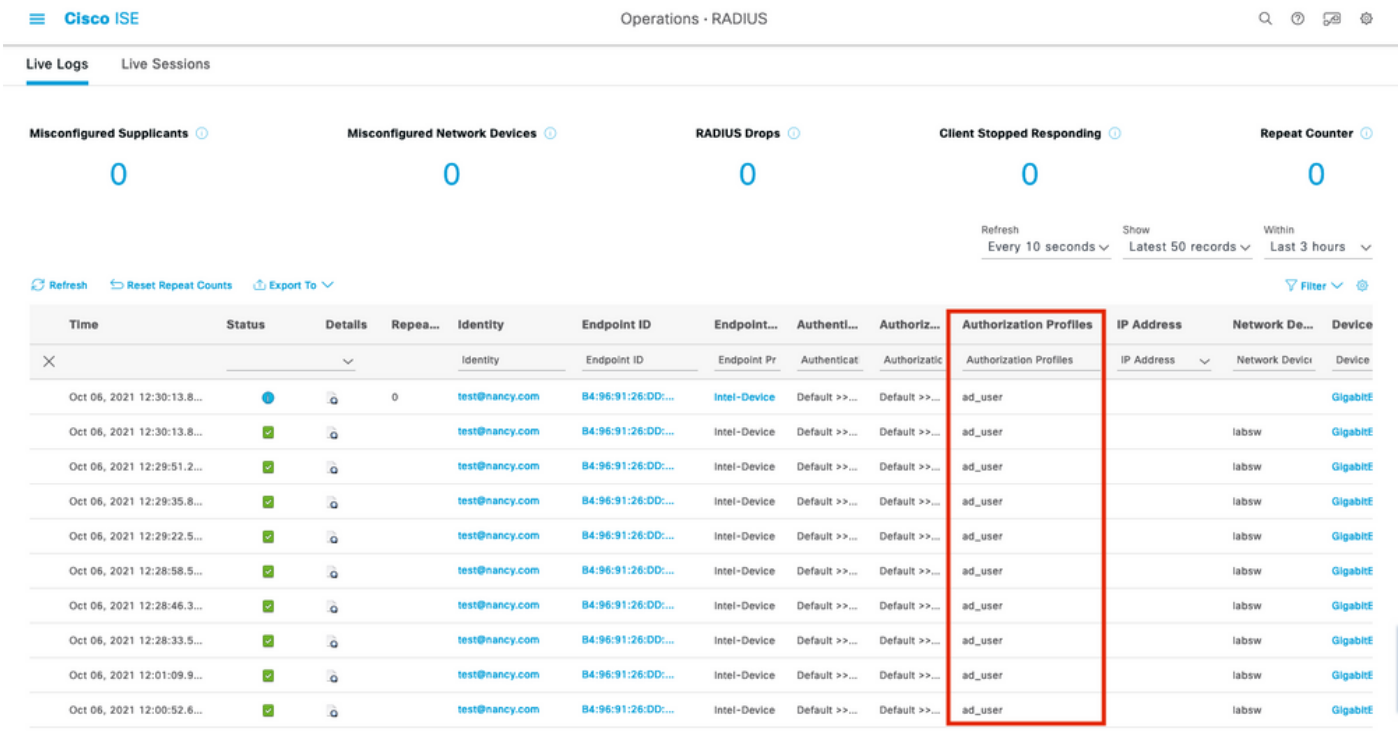
ISE 3.1 alarms based on authorization results - Configure alarm threshold

> **Note**: Ensure the authorization profile used for alarm is defined under **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

Verify

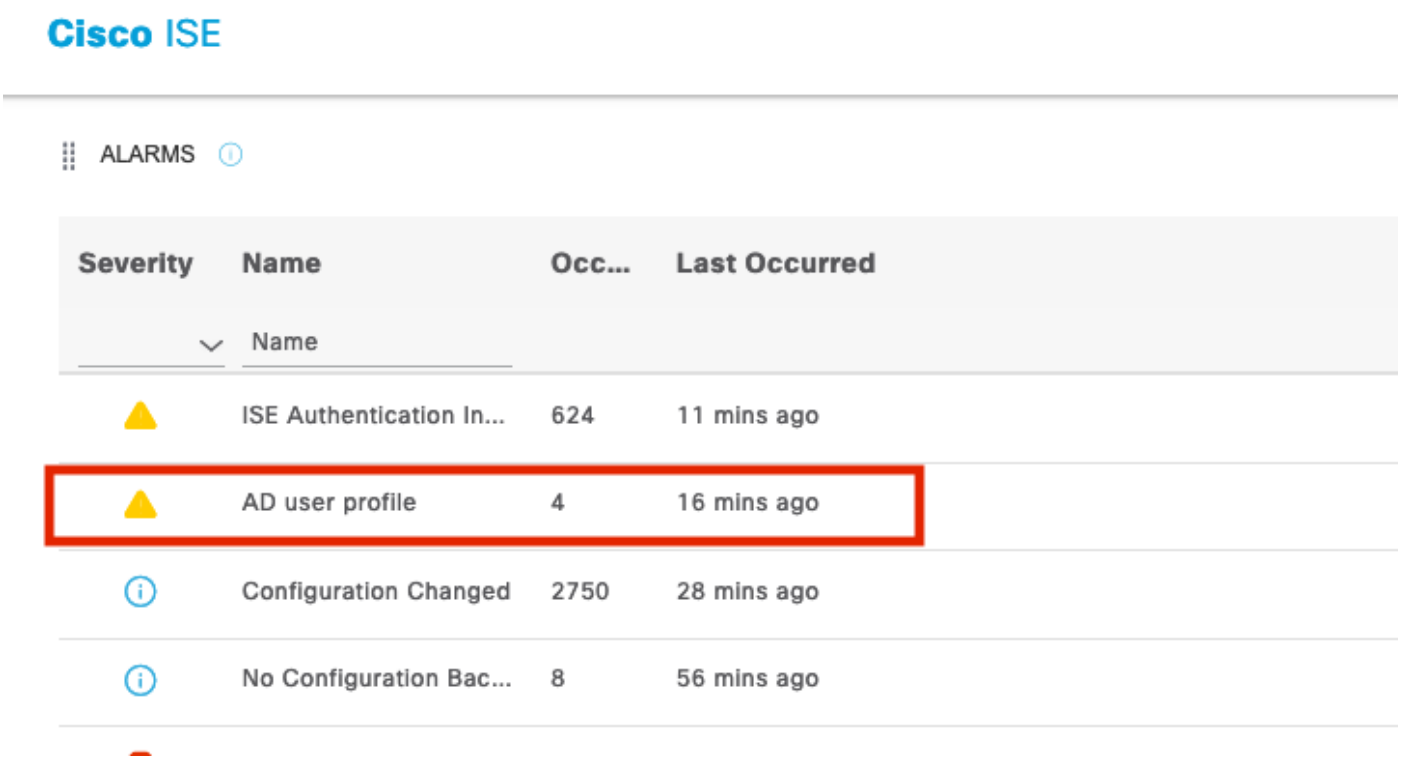
Use this section in order to confirm that your configuration works properly.

When ISE pushes the authorization profile called in the alarm for RADIUS authentication request and meets the threshold condition within the polling interval, it would trigger the alarm seen in the ISE Dashboard as shown in the image. The trigger for alarm ad_user profile is that the profile is pushed more than 5 times (Threshold Value) in the last 20 minutes (polling interval).



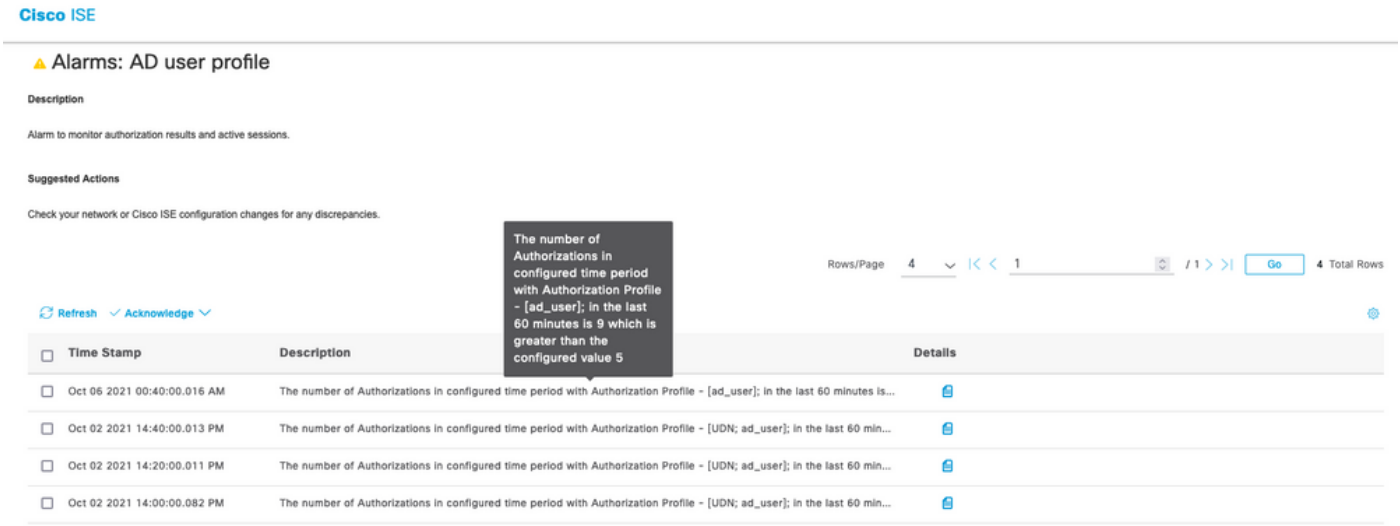
ISE 3.1 alarms based on authorization results - ISE live logs

Step 1. To check the alarm, navigate to ISE Dashboard and click on the **ALARMS** window. A new web page will open as shown:



ISE 3.1 alarms based on authorization results - Alarm notification

Step 2. To get more details of the alarm, select the alarm and it will give more details about the trigger and timestamp of the alarm.

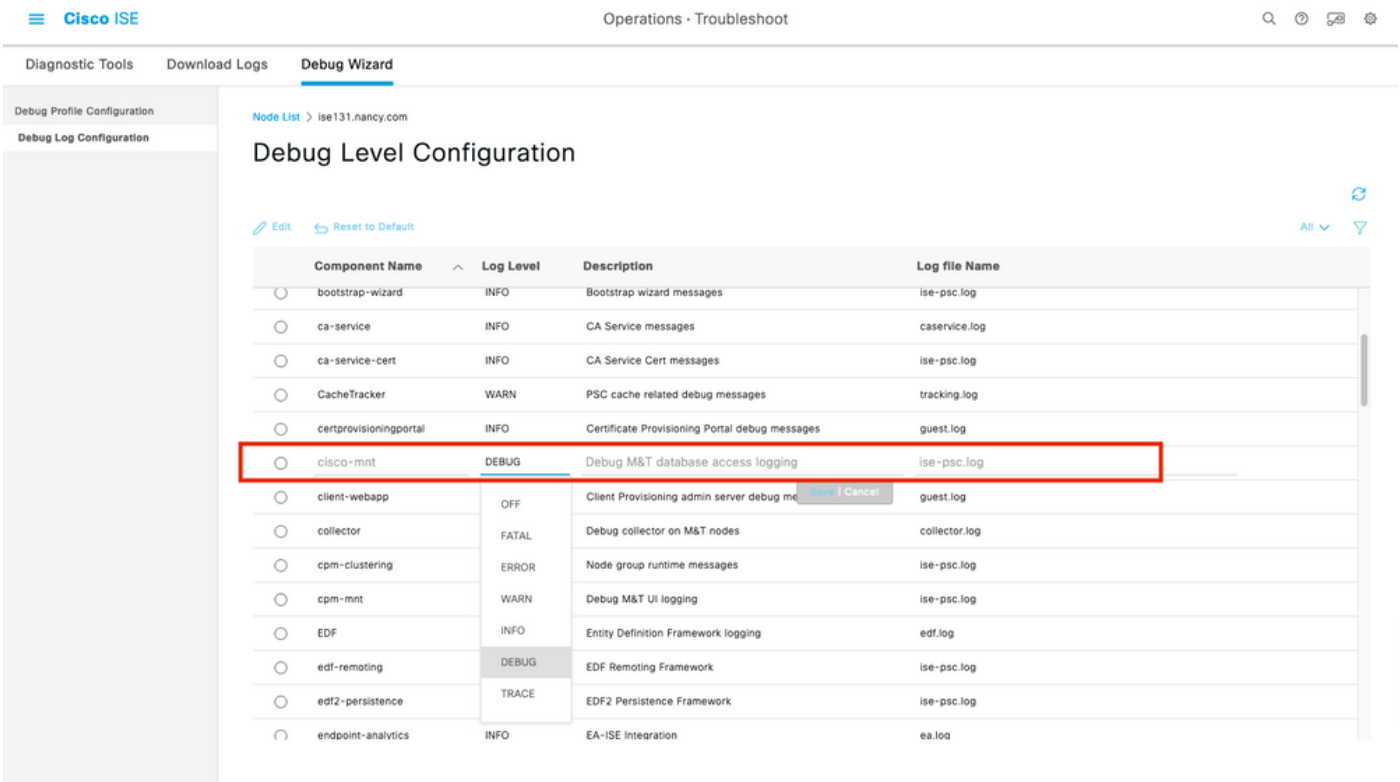


ISE 3.1 alarms based on authorization results - Alarm details

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

To troubleshoot issues related to alarm, the cisco-mnt component on the Monitoring node (MnT) must be enabled as the alarm evaluation happens on the MnT node. Navigate to **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**. Select the node on which Monitoring services are running and change the Log Level to Debug for Component Name cisco-mnt as shown:



ISE 3.1 alarms based on authorization results - ISE Debug configuration

Log Snippets when the alarm is triggered.

```
2021-10-06 00:40:00,001 DEBUG  [MnT-TimerAlarms-Threadpool-4][]
```

mnt.common.alarms.schedule.AlarmTaskRunner -::::- **Running task for rule: AlarmRule[id=df861461-89d5-485b-b3e4-68e61d1d82fc,name=AD user profile**,severity=2,isMandatory=false,enabled=true,description={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,117,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},

suggestedAction={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,117,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,110,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},detailsLink=#pageId=page_reports_details&pullOutId=authorizationResultAlarmDetails&definition=/Diagnostics/Authorization-Result-Alarm-Details.xml,

alarmTypeId=1065,isUserDefined=true,categoryId=1,enabledSyslog=true,emailAddress=[],customEmailText={},idConnectorNode=false]
2021-10-06 00:40:00,001 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- **Running custom alarm task for rule: AD user profile**
2021-10-06 00:40:00,010 INFO   [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Getting scoped alarm conditions
2021-10-06 00:40:00,011 INFO   [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Building attribute definitions based on Alarm Conditions
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Alarm Condition is:
AlarmCondition[id=bb811233-0688-42a6-a756-2f3903440feb,filterConditionType=STRING(2),filterConditionName=selected_azn_profiles,filterConditionOperator=LIKE(5),filterConditionValue=,filterConditionValues=[ad_user],filterId=]
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Alarm Condition is:
AlarmCondition[id=eff11b02-ae7d-4289-bae5-13936f3cdb21,filterConditionType=INTEGER(1),filterConditionName=ACSVIEW_TIMESTAMP,filterConditionOperator=GREATER_THAN(2),filterConditionValue=60,filterConditionValues=[],filterId=]
2021-10-06 00:40:00,011 INFO   [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Attribute definition modified and already added to list
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Query to be run is SELECT COUNT(*) AS COUNT FROM RADIUS_AUTH_48_LIVE where (selected_azn_profiles like '%,ad_user,%' OR selected_azn_profiles like 'ad_user' OR selected_azn_profiles like '%,ad_user' OR selected_azn_profiles like 'ad_user,%') AND (ACSVIEW_TIMESTAMP > SYSDATE - NUMTODSINTERVAL(60, 'MINUTE')) AND (ACSVIEW_TIMESTAMP < SYSDATE)
2021-10-06 00:40:00,011 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.dbms.timesten.DbConnection -::::- in DbConnection - getConnectionWithEncryPassword call
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- Threshold Operator is: Greater Than
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
common.alarms.schedule.tasks.ScopedAlarmTask -::::- **Alarm Condition met: true**
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.common.alarms.AlarmWorker -::::- df861461-89d5-485b-b3e4-68e61d1d82fc -> Enabled : true
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.common.alarms.AlarmWorker -::::- Active MNT -> true : false
2021-10-06 00:40:00,015 DEBUG [MnT-TimerAlarms-Threadpool-4][]
cisco.mnt.common.alarms.AlarmWorker -::::- trip() : AlarmRule[id=df861461-89d5-485b-b3e4-68e61d1d82fc,**name=AD user profile**,severity=2,isMandatory=false,enabled=true,description={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,117,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},

suggestedAction={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,117,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,11

```
0,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},detailsLink=#pageId=page_rep
orts_details&pullOutId=authorizationResultAlarmDetails&definition=/Diagnostics/Authorization-
Result-Alarm-Details.xml,

alarmTypeId=1065,isUserDefined=true,categoryId=1,enabledSyslog=true,emailAddress=[],customEmailT
ext={},idConnectorNode=false] : 2 : The number of Authorizations in configured time period with
Authorization Profile - [ad_user]; in the last 60 minutes is 9 which is greater than the
configured value 5
```

NOTE: If the alarm is not triggered even after the authorization profile is pushed, check conditions like: Include data of last (minutes), Threshold Operator, Threshold Value and polling interval configured in the alarm.