

alarmen configureren op basis van resultaten van autorisatie op ISE 3.1

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

In dit document worden de stappen beschreven die nodig zijn om de signaleringen aan te passen op basis van het autoriteitsresultaat voor een RADIUS-verificatieaanvraag bij Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- RADIUS-protocol
- ISE-beheertoegang

Gebruikte componenten

De informatie in dit document is gebaseerd op Identity Services Engine (ISE) 3.1.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

In dit voorbeeld zou een douanealarm worden ingesteld voor een specifiek vergunningsprofiel met een vastgestelde drempelwaarde en indien ISE de drempelwaarde van het beleid inzake de vergunning bereikt, zou het alarm in werking worden gesteld.

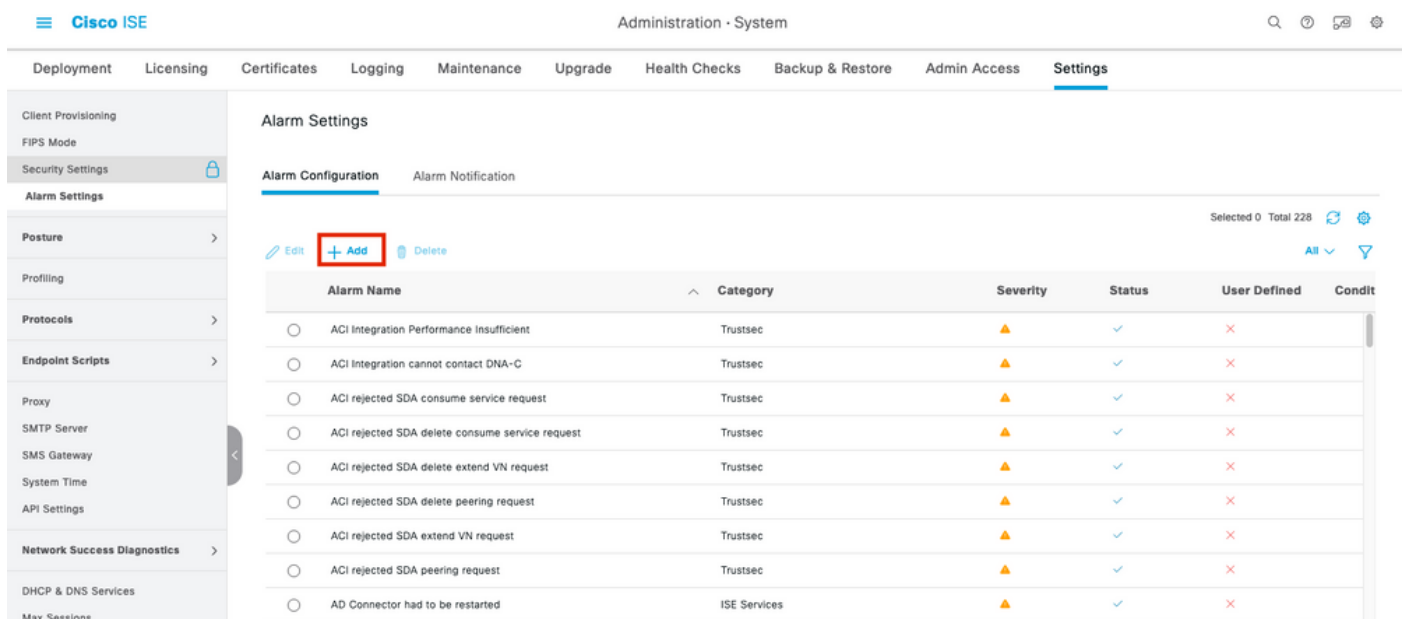
Configureren

In dit voorbeeld zullen we een alarm voor het autorisatieprofiel ("ad_user") aangezet creëren wanneer een Actieve Gebruiker van de Map (AD) inlogt en het alarm op basis van de geconfigureerde drempelwaarde wordt geactiveerd.

Opmerking: Voor een productieserver moet de drempel een hogere waarde zijn om grote voorvallen van het alarm te voorkomen.

Stap 1. Navigeer naar **Administratie > Systeem > Alarminstellingen**.

Stap 2. Klik onder Alarmconfiguratie op **Add** om een alarm te maken zoals in de afbeelding.

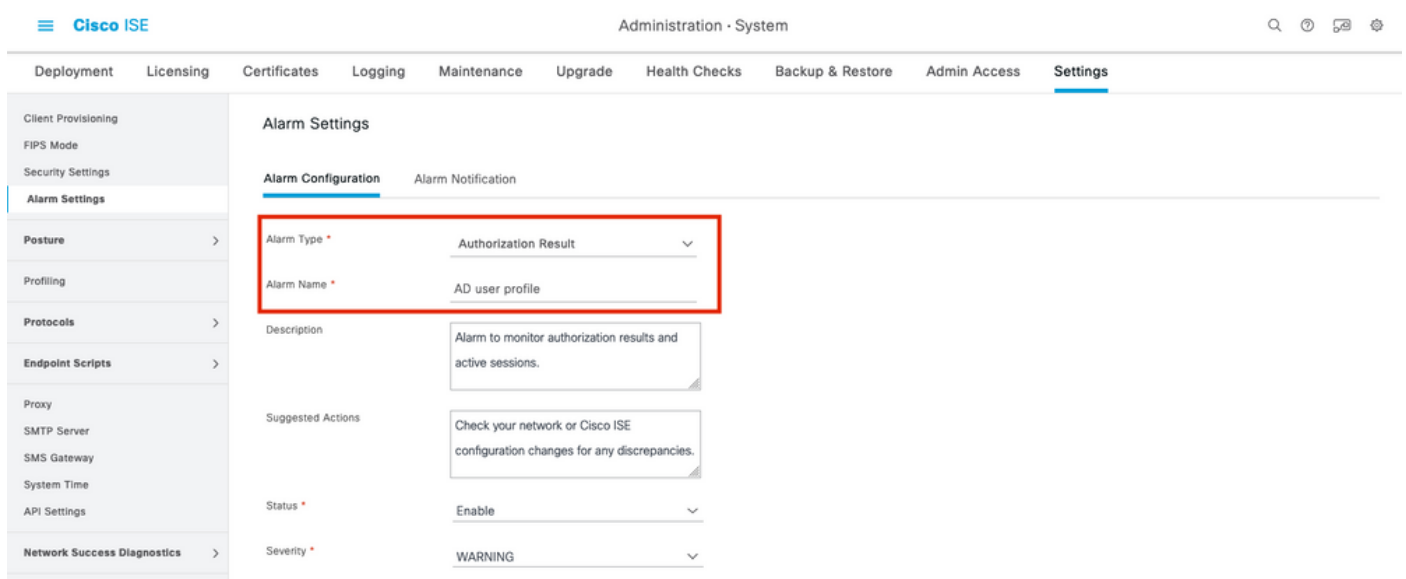


The screenshot shows the Cisco ISE Administration - System interface. The left sidebar contains navigation options like Client Provisioning, Security Settings, Alarm Settings, Posture, Profiling, Protocols, Endpoint Scripts, Proxy, SMTP Server, SMS Gateway, System Time, API Settings, Network Success Diagnostics, DHCP & DNS Services, and Max Sessions. The main content area is titled 'Alarm Settings' and has two tabs: 'Alarm Configuration' (selected) and 'Alarm Notification'. In the 'Alarm Configuration' tab, there is a '+ Add' button highlighted with a red box. Below it is a table of existing alarms.

Alarm Name	Category	Severity	Status	User Defined	Condit
ACI Integration Performance insufficient	Trustsec	▲	✓	×	
ACI Integration cannot contact DNA-C	Trustsec	▲	✓	×	
ACI rejected SDA consume service request	Trustsec	▲	✓	×	
ACI rejected SDA delete consume service request	Trustsec	▲	✓	×	
ACI rejected SDA delete extend VN request	Trustsec	▲	✓	×	
ACI rejected SDA delete peering request	Trustsec	▲	✓	×	
ACI rejected SDA extend VN request	Trustsec	▲	✓	×	
ACI rejected SDA peering request	Trustsec	▲	✓	×	
AD Connector had to be restarted	ISE Services	▲	✓	×	

ISE 3.1-alarmen gebaseerd op resultaten van de vergunning - alarminstellingen

Stap 3. Selecteer het Alarmtype als **gevolg van de autorisatie** en voer de alarmnaam in zoals in de afbeelding.



The screenshot shows the Cisco ISE Administration - System interface. The left sidebar is the same as in the previous image. The main content area is titled 'Alarm Settings' and has two tabs: 'Alarm Configuration' (selected) and 'Alarm Notification'. In the 'Alarm Configuration' tab, the 'Add' form is highlighted with a red box. The form fields are: Alarm Type (Authorization Result), Alarm Name (AD user profile), Description (Alarm to monitor authorization results and active sessions.), Suggested Actions (Check your network or Cisco ISE configuration changes for any discrepancies.), Status (Enable), and Severity (WARNING).

ISE 3.1-alarmen gebaseerd op de resultaten van de vergunning - alarminstallatie instellen

Stap 4. In het gedeelte **Drempelwaarde** selecteert u **Vergunning in een geconfigureerde tijdsperiode** in Drempel Bij de vervolkeuzelijst en voert u de juiste waarden voor Drempel en de verplichte velden in. Raadpleeg in het filtergedeelte het machtigingsprofiel waarvoor het alarm moet worden geactiveerd, zoals in de afbeelding.

The screenshot shows the Cisco ISE Administration System Settings page. The left sidebar contains navigation options like Client Provisioning, Security Settings, Alarm Settings, Posture, Profiling, Protocols, Endpoint Scripts, Proxy, Network Success Diagnostics, DHCP & DNS Services, Max Sessions, Light Data Distribution, and Interactive Help. The main content area is titled 'Settings' and contains two sections: 'Thresholds' and 'Filters'. The 'Thresholds' section is highlighted with a red box and contains the following configuration: Threshold On: Authorizations in configured time p...; Include data of last(minutes): 60; Threshold Type: Number; Threshold Operator: Greater Than; Threshold Value: 5 (0 - 999999); Run Every: 20 minutes. The 'Filters' section is also highlighted with a red box and contains the following configuration: Authorization Profile: ad_user *; SGT: (empty).

ISE 3.1-alarmen gebaseerd op resultaten van de vergunning - alarmdrempel instellen

Opmerking: Zorg ervoor dat het vergunningprofiel dat voor alarm wordt gebruikt, is gedefinieerd onder **Beleids-elementen > Resultaten > Vergunning > Verificatieprofielen**.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Wanneer ISE het vergunningsprofiel dat in het alarm voor de authenticatie van de RADIUS is genoemd, aandrukt en binnen het steminterval aan de drempelvoorwaarde voldoet, zou dit het alarm in het ISE-dashboard tweebrengen zoals in de afbeelding wordt getoond. De trigger voor het alarm ad_user profiel is dat het profiel meer dan vijf keer (Drempel Waarde) in de laatste 20 minuten (steminterval) wordt geduwd.

Live Logs Live Sessions

Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

Refresh Every 10 seconds v Show Latest 50 records v Within Last 3 hours v

Refresh Reset Repeat Counts Export To v

Filter v

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authenti...	Authoriz...	Authorization Profiles	IP Address	Network De...	Device
Oct 06, 2021 12:30:13.8...			0	test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user			GigabitE
Oct 06, 2021 12:30:13.8...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:51.2...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:35.8...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:29:22.5...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:58.5...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:46.3...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:28:33.5...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:01:09.9...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE
Oct 06, 2021 12:00:52.6...				test@nancy.com	B4:96:91:26:DD:...	Intel-Device	Default >>...	Default >>...	ad_user		labsw	GigabitE

ISE 3.1-alarmen gebaseerd op de resultaten van de vergunning - ISE-levende stammen

Stap 1. Als u het alarm wilt controleren, navigeer dan naar ISE Dashboard en klik op in het venster **ALARMS**. Er wordt een nieuwe webpagina geopend, zoals wordt getoond:

Cisco ISE

ALARMS

Severity	Name	Occ...	Last Occurred
	ISE Authentication In...	624	11 mins ago
	AD user profile	4	16 mins ago
	Configuration Changed	2750	28 mins ago
	No Configuration Bac...	8	56 mins ago

ISE 3.1-alarmen gebaseerd op de resultaten van de vergunning - Alarmmelding

Stap 2. Om meer details van het alarm te krijgen, selecteert u het alarm en geeft u meer details over de trigger en de tijdstempel van het alarm.

▲ Alarms: AD user profile

Description

Alarm to monitor authorization results and active sessions.

Suggested Actions

Check your network or Cisco ISE configuration changes for any discrepancies.

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

Rows/Page 4 | << 1 / 1 >> | Go 4 Total Rows

<input type="checkbox"/>	Time Stamp	Description	Details
<input type="checkbox"/>	Oct 06 2021 00:40:00.016 AM	The number of Authorizations in configured time period with Authorization Profile - [ad_user]; in the last 60 minutes is...	Details
<input type="checkbox"/>	Oct 02 2021 14:40:00.013 PM	The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min...	Details
<input type="checkbox"/>	Oct 02 2021 14:20:00.011 PM	The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min...	Details
<input type="checkbox"/>	Oct 02 2021 14:00:00.082 PM	The number of Authorizations in configured time period with Authorization Profile - [UDN; ad_user]; in the last 60 min...	Details

ISE 3.1 alarmen gebaseerd op de resultaten van de vergunning - alarmgegevens

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Om problemen met betrekking tot de oplossing van problemen met betrekking tot alarm op te lossen, moet de cisco-component op het bewakingsknooppunt (MnT) zijn ingeschakeld aangezien de alarmevaluatie op het MnT-knooppunt plaatsvindt. navigeren naar **bewerkingen > Probleemoplossing > Wizard Debug > Configuratie logbestand debug**. Selecteer het knooppunt waarop de bewakingsservices worden uitgevoerd en wijzig het logniveau in om te stoppen voor de naam van component zoals wordt weergegeven:

Cisco ISE Operations · Troubleshoot

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration
Debug Log Configuration

Node List > ise131.nancy.com

Debug Level Configuration

[Edit](#) [Reset to Default](#) [All](#) [Filter](#)

Component Name	Log Level	Description	Log file Name
<input type="radio"/> bootstrap-wizard	INFO	Bootstrap wizard messages	ise-psc.log
<input type="radio"/> ca-service	INFO	CA Service messages	caservice.log
<input type="radio"/> ca-service-cert	INFO	CA Service Cert messages	ise-psc.log
<input type="radio"/> CacheTracker	WARN	PSC cache related debug messages	tracking.log
<input type="radio"/> certprovisioningportal	INFO	Certificate Provisioning Portal debug messages	guest.log
<input type="radio"/> cisco-mnt	DEBUG	Debug M&T database access logging	ise-psc.log
<input type="radio"/> client-webapp	OFF	Client Provisioning admin server debug me	guest.log
<input type="radio"/> collector	FATAL	Debug collector on M&T nodes	collector.log
<input type="radio"/> cpm-clustering	ERROR	Node group runtime messages	ise-psc.log
<input type="radio"/> cpm-mnt	WARN	Debug M&T UI logging	ise-psc.log
<input type="radio"/> EDF	INFO	Entity Definition Framework logging	edf.log
<input type="radio"/> edf-remoting	DEBUG	EDF Remoting Framework	ise-psc.log
<input type="radio"/> edf2-persistence	TRACE	EDF2 Persistence Framework	ise-psc.log
<input type="radio"/> endpoint-analytics	INFO	EA-ISE Integration	ea.log

ISE 3.1-alarmen gebaseerd op de resultaten van de vergunning - ISE-configuratie

Log scherpen in als het alarm is geactiveerd.

```
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={65,108,97,114,109,32,116,111,32,1  
09,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,1  
17,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},  
  
suggestedAction={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107  
,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,1  
17,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,11  
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]  
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,filterCondi  
tionOperator=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,filterConditio  
nOperator=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={65,108,97,114,109,32,116,111,32,1  
09,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,1  
17,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},
```

suggestedAction={67,104,101,99,107,37,50,48,121,111,117,114,37,50,48,110,101,116,119,111,114,107,37,50,48,111,114,37,50,48,67,105,115,99,111,37,50,48,73,83,69,37,50,48,99,111,110,102,105,103,17,114,97,116,105,111,110,37,50,48,99,104,97,110,103,101,115,37,50,48,102,111,114,37,50,48,97,110,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},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} : 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

OPMERKING: Als het alarm niet wordt geactiveerd zelfs nadat het autorisatieprofiel is ingedrukt, controleert u de omstandigheden zoals: Omvat gegevens van laatste (minuten), Drempel operator, Drempel waarde en steminterval ingesteld in het alarm.