

إلى ادانتسا هي بننتا لي غشت متيسو (Active Directory) م دختسم لوخد ليجست دنن
هن يوكت مت يذلا دلح

راذن إلى تاراركت بنجتل إلى دلح عميق نوكت نأ بجي، جات إلى مداخل ة بسنلاب: **ةظحال**
ةر يبال

هي بننتا تاداع | > ماظن > ةراد إلى لقتنا 1. ةوطخل

يف حضورم وه امك هي بننتا ةفاصل قوف رونا، هي بننتا لي كشت تحت 2. ةوطخل
ةروصل

Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
Posture
Profiling
Protocols
Endpoint Scripts
Proxy
SMTP Server
SMS Gateway
System Time
API Settings
Network Success Diagnostics
DHCP & DNS Services
Max Sessions

Alarm Settings

Alarm Configuration Alarm Notification

Selected 0 Total 228

Edit **+ Add** Delete

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	▲	✓	✗	

هي بننتا تاداع | - لي وختل جئاتن إلى ة دننتسم ال 3.1 ISE تاهي بننتا

يف حضورم وه امك هي بننتا ل مسا لخدأو لي وختل ة جيتنك هي بننتا ل عون دح 3. ةوطخل
ةروصل

Administration - System

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access **Settings**

Client Provisioning
FIPS Mode
Security Settings
Alarm Settings
Posture
Profiling
Protocols
Endpoint Scripts
Proxy
SMTP Server
SMS Gateway
System Time
API Settings
Network Success Diagnostics
DHCP & DNS Services
Max Sessions

Alarm Settings

Alarm Configuration Alarm Notification

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

Severity * WARNING

هي بننتا نيوكت - لي وختل جئاتن إلى ادانتسا 3.1 ISE تاهي بننتا

دلح ي ف اهن يوكت مت يتي ال ة نزل ةرتف ال ي ضي وفتل دح، دلح مسق ي ف 4. ةوطخل
ةر يفتل ل ماع مسق ي ف. ةر يفتل ل لوقحل او ة بتعل ة بسنابنم ال ميقل لخدأو لدسنم ال

ةروصللا يف حضوم وه امك هل هبنتلا لئغشت بجي يذلا لئوختلا لئفرت فلمب لصتا

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - System' and various settings tabs like 'Deployment', 'Licensing', 'Certificates', etc. The 'Settings' tab is active. On the left, there is a sidebar menu with categories 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 'Thresholds' and contains a form to define threshold conditions. The 'Thresholds' section is highlighted with a red box and includes fields for 'Threshold On' (Authorizations in configured time p...), 'Include data of last(minutes)' (60), 'Threshold Type' (Number), 'Threshold Operator' (Greater Than), 'Threshold Value' (5), and 'Run Every' (20 minutes). Below this, the 'Filters' section is also highlighted with a red box and shows a dropdown menu for 'Authorization Profile' with 'ad_user' selected.

هه بنتلا دح نيوكت - لئوختلا لئئاتن لئ ادانتسا ISE 3.1 تاهه بنت

> ةسايسلا تحت فرعم راذنلال مدختسملا لئوختلا صئصخت فلم نأ نم دكأت: ةظالم
لئوختلا صئصخت تافلم > لئوختلا > لئئاتنلا > ةسايسلا رصانع

ةحصللا نم ققحتلا

حئص لكشب نيوكتلا لمع دئكأتل مسقلا اذه مدختسا

يفي و RADIUS ةقداصم بلطل هه بنتلا لئوختلا صئصخت فلم ISE ةفدي ام دنع
ةحول يف دوجوملا راذنلال قلاطي هئاف، ءاصقتسالل لئوختلا لئوختلا صئصخت
نأ وه ad_user profile هه بنتلا لئوختلا صئصخت فلم ISE تامولعم
(ققحتلا لئوختلا) ةقيد 20 رخآ يف (دحلا ةمقي) تارم 5 نم رثكأ ةفدي صئصختلا

Live Logs Live Sessions

Misconfigured Suppliants 0

Misconfigured Network Devices 0

RADIUS Drops 0

Client Stopped Responding 0

Repeat Counter 0

0

0

0

0

0

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

Refresh Reset Repeat Counts Export To

Filter

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

ةرشابم ال ISE تالچس - لي وختالچئاتن لي اذانتسا ISE 3.1 تاهي بنت

هه بنتالذفان قوف رقناو ISE تامولعم ةحول لي لقتنا، هه بنتال نم ققحتلل 1. ةوطخل
 ح:ضوم وه امك ةديج بي و ةحفص حتف متسي:

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

هه بنتال مالع - لي وختالچئاتن لي اذانتسا ISE 3.1 تاهي بنت

ديزلما يطعيسو، هه بنتال دح، هه بنتال نع لي صافتال نم ديزم لي لوصحلل 2. ةوطخل
 هه بنتال لي نزلما عباطال او لغشمال لوح لي صافتال نم


```
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={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,17,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},
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]
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={65,108,97,114,109,32,116,111,32,109,111,110,105,116,111,114,32,97,117,116,104,111,114,105,122,97,116,105,111,110,32,114,101,115,17,108,116,115,32,97,110,100,32,97,99,116,105,118,101,32,115,101,115,115,105,111,110,115,46},
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},
```

0,121,37,50,48,100,105,115,99,114,101,112,97,110,99,105,101,115,46},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

نم ققحتت ف، لئوختت ل فئرت فلم عفد دعب ىت ح هئبنتت ل لئغشت متئ مل اذئ: **ةظحالم**
ل صافل دحل ةمئقو دحل لئغشت لماعو (قئاقد) رخآ تانائب نئمضت: لثم طورشل
هئبنتت لئف ةنوكم ل ققحتت ل تارتفو.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل