

Troubleshooting the ISE Alarm Error “Profiler SNMP Request Failure: Server= NAD Address= Error Message=Request timed out”

Contents

[Issue](#)

[Environment](#)

[Resolution](#)

[Step 1: Identify affected NAD.](#)

[Step 2: Ensure the SNMP is running on the affected Network Access Device NAD client](#)

[Step 3: Ensure the SNMP version and SNMP community string or SNMP Auth/Privacy Protocol Password match, on both the NAD and in ISE](#)

[Step 4: Validate reachability, and required UDP ports \(161,162\) between ISE PSN and NAD client](#)

[Cause](#)

[Related Content](#)

- [Issue](#)
 - [Environment](#)
 - [Resolution](#)
 - [Step 1: Identify affected NAD.](#)
 - [Step 2: Ensure the SNMP is running on the affected Network Access Device NAD client](#)
 - [Step 3: Ensure the SNMP version and SNMP community string or SNMP Auth/Privacy Protocol Password match, on both the NAD and in ISE](#)
 - [Step 4: Validate reachability, and required UDP ports \(161,162\) between ISE PSN and NAD client](#)
 - [Cause](#)
 - [Related Content](#)
-

Issue

While reviewing alarms in ISE you see this SNMP profiler error:

“Profiler SNMP Request Failure: Server= <NAD DEVICE Name> NAD Address=<x.x.x.x> Error Message=Request t

Environment

- Cisco Identity Services Engine (ISE) version 3.0.0 and later
- ISE Profiling service enabled
- Network Access Devices (NADs) configured for SNMP communication

Resolution

Step 1: Identify affected NAD.

1. Navigate to **Dashboard > Alarms**
2. Check alarm details and note the affected NAD device name or IP.
3. You can identify the specific NAD client IP address by referencing the "NAD Address" field within the "Profiler SNMP Request Failure" error message.

Step 2: Ensure the SNMP is running on the affected Network Access Device NAD client

Log into the CLI of the NAD client and run this command to check if the SNMP feature is enabled.

```
show running-config | include snmp
```

Example SNMP v3:

```
Switch#show running-config | include snmp
ip access-list standard snmp-access
snmp-server group my-snmp-group v3 priv read admin-view access snmp-access
snmp-server view admin-view iso included
```

Example SNMP v2c:

```
snmp-server community public R0
snmp-server community private RW
snmp-server host 192.168.1.100 version 2c public
```

Step 3: Ensure the SNMP version and SNMP community string or SNMP Auth/Privacy Protocol Password match, on both the NAD and in ISE

Validate your SNMP v2c configuration using the steps:

1. Login into the NAD client CLI and run the command “show snmp community”.

Switch Output:

```
Community name: public
Community Index: public
Community SecurityName: public
storage-type: nonvolatile          active
```

2. On ISE: Navigate to **Administration > Network Resources > Network Devices**.
3. Edit the identified NAD entry to ensure the SNMP community string and SNMP version matches with the output from “show snmp community”.

ISE SNMP v2c:

☒ SNMP Settings

SNMP Version

2c

▼

SNMP RO Community

public

Hide

SNMP Username

Security Level

▼

Auth Protocol

▼

Auth Password

Show

Privacy Protocol

▼

Privacy Password

Show

Polling Interval

28,800

seconds(Valid Range 600 to 86400 or zero)

☒ Link Trap Query

☒ MAC Trap Query

Originating Policy Services Node

Auto

▼

The switch masks SNMP v3 Auth/Privacy passwords. To ensure these credentials remain accurate, re-enter them using the steps :

1. Log into the ISE GUI.
2. Navigate to **Administration > Network Resources > Network Devices**.
3. Edit the identified NAD entry and go to the **SNMP Settings**. By clicking on the '**Show**' on the Auth Password and Privacy Password. You could reveal the password for it.

☒ **SNMP Settings**

SNMP Version	3	▼
SNMP RO Community		Show
SNMP Username	test	
Security Level	Priv	▼
Auth Protocol	SHA	▼
Auth Password	test@123	Hide
Privacy Protocol	AES128	▼
Privacy Password	test@123	Hide
Polling Interval	28,800	seconds(Valid Range 600 to 86400 or zero)
☒ Link Trap Query		
☒ MAC Trap Query		
Originating Policy Services Node	Auto	▼

4. Log into the Switch CLI.

- Run the command configure terminal.
- After that run this command to update the SNMP v3 credentials on the switch.

Switch Command :

```
snmp-server user <username> <groupname> v3 auth sha <auth-password> priv aes 128 <priv-password>
```

Example :

```
snmp-server user test snmpgroup v3 auth sha test@123 priv aes 128 test@123
```

Step 4: Validate reachability, and required UDP ports (161,162) between ISE PSN and NAD client

1. Perform a ping test from the Profiler-enabled PSN node to the NAD client.

2. Perform a ping test from the from the NAD client to the PSN node.
3. Ensure ports 161 and 162 are open between the PSN node and NAD.
 - Test using telnet from the NAD client to the Profiler-enabled node to confirm that ports 161 and 162 are open.

```
telnet <ISE IP-address> 161  
telnet <ISE IP-address> 162
```

Cause

The SNMP Request Failure alarm occurs when ISE fails to successfully query the Network Access Device. This is typically caused by configuration mismatches regarding SNMP community strings, versions, or v3 credentials between the two devices. Additionally, network issues such as firewalls blocking UDP ports 161 or 162, or missing SNMP server configurations on the NAD, frequently prevent successful communication.

Related Content

[Allow the required ISE ports and FQDNs on the network](#)

[ISE Profiling Design Guide](#)

[Configure SNMP Community Strings](#)