

# Resolución de problemas del error de alarma de ISE “Profiler SNMP Request Failure: Server=NAD Address= Mensaje de error=La solicitud ha agotado el tiempo de espera”

## Contenido

---

[Problema](#)

[Entorno](#)

[Resolución](#)

[Paso 1: Identifique el NAD afectado.](#)

[Paso 2: Asegúrese de que el SNMP se esté ejecutando en el dispositivo y cliente de acceso a la red afectados](#)

[Paso 3: Asegúrese de que la versión de SNMP y la cadena de comunidad SNMP o la contraseña del protocolo de autenticación/privacidad SNMP coincidan, tanto en NAD como en ISE](#)

[Paso 4: Validar la disponibilidad y los puertos UDP necesarios \(161 162\) entre ISE PSN y el cliente NAD](#)

[Causa](#)

[Contenido relacionado](#)

---

- [Problema](#)
  - [Entorno](#)
  - [Resolución](#)
    - [Paso 1: Identifique el NAD afectado.](#)
    - [Paso 2: Asegúrese de que el SNMP se esté ejecutando en el dispositivo y cliente de acceso a la red afectados](#)
    - [Paso 3: Asegúrese de que la versión de SNMP y la cadena de comunidad SNMP o la contraseña del protocolo de autenticación/privacidad SNMP coincidan, tanto en NAD como en ISE](#)
    - [Paso 4: Validar la disponibilidad y los puertos UDP necesarios \(161 162\) entre ISE PSN y el cliente NAD](#)
  - [Causa](#)
  - [Contenido relacionado](#)
- 

## Problema

Mientras revisa las alarmas en ISE, observa este error del perfilador SNMP:

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

## Entorno

- Cisco Identity Services Engine (ISE) versión 3.0.0 y posteriores
- Servicio de definición de perfiles ISE habilitado
- Dispositivos de acceso a la red (NAD) configurados para la comunicación SNMP

## Resolución

### Paso 1: Identifique el NAD afectado.

1. Vaya a Panel > Alarmas
2. Compruebe los detalles de la alarma y anote el nombre del dispositivo NAD o IP afectado.
3. Puede identificar la dirección IP específica del cliente NAD haciendo referencia al campo "NAD Address" dentro del mensaje de error "Profiler SNMP Request Failure".

### Paso 2: Asegúrese de que el SNMP se esté ejecutando en el dispositivo y cliente de acceso a la red afectados

Inicie sesión en la CLI del cliente NAD y ejecute este comando para verificar si la función SNMP está habilitada.

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

Ejemplo de 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
```

Ejemplo de SNMP v2c:

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

Paso 3: Asegúrese de que la versión de SNMP y la cadena de comunidad SNMP o la contraseña del protocolo de autenticación/privacidad SNMP coincidan, tanto en NAD como en ISE

Valide la configuración de SNMP v2c siguiendo estos pasos:

1. Inicie sesión en la CLI del cliente NAD y ejecute el comando "show snmp community".

Salida de conmutador:

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

2. En ISE: Vaya a Administration > Network Resources > Network Devices.
3. Edite la entrada NAD identificada para asegurarse de que la cadena de comunidad SNMP y la versión SNMP coincidan con la salida de "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

▼

El switch enmascara las contraseñas de autenticación/privacidad SNMP v3. Para asegurarse de que estas credenciales siguen siendo exactas, vuelva a introducirlas mediante los pasos siguientes:

1. Inicie sesión en la GUI de ISE.
2. Vaya a Administration > Network Resources > Network Devices.
3. Edite la entrada NAD identificada y vaya a SNMP Settings. Haciendo clic en "Show" en la contraseña de autenticación y la contraseña de privacidad. Podría revelar la contraseña para ello.

☒ **SNMP Settings**

|                                                     |                 |                                           |
|-----------------------------------------------------|-----------------|-------------------------------------------|
| SNMP Version                                        | <b>3</b>        | ▼                                         |
| SNMP RO Community                                   |                 | <a href="#">Show</a>                      |
| SNMP Username                                       | <b>test</b>     |                                           |
| Security Level                                      | <b>Priv</b>     | ▼                                         |
| Auth Protocol                                       | <b>SHA</b>      | ▼                                         |
| Auth Password                                       | <b>test@123</b> | <a href="#">Hide</a>                      |
| Privacy Protocol                                    | <b>AES128</b>   | ▼                                         |
| Privacy Password                                    | <b>test@123</b> | <a href="#">Hide</a>                      |
| Polling Interval                                    | <b>28,800</b>   | seconds(Valid Range 600 to 86400 or zero) |
| <input checked="" type="checkbox"/> Link Trap Query |                 |                                           |
| <input checked="" type="checkbox"/> MAC Trap Query  |                 |                                           |
| Originating Policy Services Node                    | <b>Auto</b>     | ▼                                         |

4. Inicie sesión en la CLI del switch.

- Ejecute el comando configure terminal.
- Después de esto, ejecute este comando para actualizar las credenciales SNMP v3 en el switch.

Comando del switch:

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

Ejemplo:

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

Paso 4: Validar la disponibilidad y los puertos UDP necesarios (161 162) entre ISE PSN y el cliente NAD

1. Realice una prueba de ping desde el nodo PSN activado por el analizador al cliente NAD.
2. Realice una prueba de ping desde el cliente NAD al nodo PSN.
3. Asegúrese de que los puertos 161 y 162 estén abiertos entre el nodo PSN y NAD.
  - Pruebe usando telnet desde el cliente NAD hasta el nodo habilitado para Profiler para confirmar que los puertos 161 y 162 están abiertos.

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

## Causa

La alarma SNMP Request Failure se produce cuando ISE no puede consultar correctamente el dispositivo de acceso a la red. Esto se debe normalmente a discrepancias de configuración con respecto a las cadenas de comunidad SNMP, versiones o credenciales v3 entre los dos dispositivos. Además, los problemas de red, como los firewalls que bloquean los puertos UDP 161 o 162, o la falta de configuraciones de servidor SNMP en el NAD, suelen impedir que la comunicación se realice correctamente.

## Contenido relacionado

[Permitir los puertos ISE y FQDN necesarios en la red](#)

[Guía de diseño de perfiles de ISE](#)

[Configuración de cadenas de comunidad del protocolo SNMP](#)

#### Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).