

# ISEアラームエラー“；プロファイラのSNMP要求失敗のトラブルシューティング：Server=NAD Address=エラーメッセージ=Request timed out”

## 内容

---

### [問題](#)

### [環境](#)

### [解決方法](#)

[ステップ1：影響を受けるNADを特定します。](#)

[ステップ2：該当するネットワークアクセスデバイス\(NAD\)クライアントでSNMPが実行されていることを確認します](#)

[ステップ3:NADとISEの両方で、SNMPバージョンとSNMPコミュニティストリングまたはSNMP認証/プライバシープロトコルパスワードが一致していることを確認します](#)

[ステップ4:ISE PSNとNADクライアント間の到達可能性および必要なUDPポート\(161、162\)を検証します。](#)

### [原因](#)

### [関連コンテンツ](#)

---

- [問題](#)
  - [環境](#)
  - [解決方法](#)
    - [ステップ1：影響を受けるNADを特定します。](#)
    - [ステップ2：該当するネットワークアクセスデバイス\(NAD\)クライアントでSNMPが実行されていることを確認します](#)
    - [ステップ3:NADとISEの両方で、SNMPバージョンとSNMPコミュニティストリングまたはSNMP認証/プライバシープロトコルパスワードが一致していることを確認します](#)
    - [ステップ4:ISE PSNとNADクライアント間の到達可能性および必要なUDPポート\(161、162\)を検証します。](#)
  - [原因](#)
  - [関連コンテンツ](#)
- 

## 問題

ISEでアラームを確認しているときに、次のSNMPプロファイラエラーが表示されます。

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

## 環境

- Cisco Identity Services Engine(ISE)バージョン3.0.0以降
- ISEプロファイリングサービスが有効
- SNMP通信用に設定されたネットワークアクセスデバイス(NAD)

## 解決方法

ステップ1：影響を受けるNADを特定します。

1. ダッシュボード>アラームに移動します
2. アラームの詳細を確認し、影響を受けるNADデバイス名またはIPをメモします。
3. 「Profiler SNMP Request Failure」エラーメッセージの「NAD Address」フィールドを参照すると、特定のNADクライアントのIPアドレスを確認できます。

ステップ2：該当するネットワークアクセスデバイス(NAD)クライアントでSNMPが実行されていることを確認します

NADクライアントのCLIにログインし、次のコマンドを実行してSNMP機能が有効になっているかどうかを確認します。

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

SNMP v3の例：

```
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
```

SNMP v2cの例

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

ステップ3:NADとISEの両方で、SNMPバージョンとSNMPコミュニティストリングまたはSNMP認証/プライバシープロトコルパスワードが一致していることを確認します

次の手順を使用して、SNMP v2cの設定を検証します。

1. NADクライアントCLIにログインし、コマンド「show snmp community」を実行します。

スイッチ出力：

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

2. ISEで、Administration > Network Resources > Network Devicesの順に移動します。
3. 特定されたNADエントリを編集し、SNMPコミュニティストリングおよびSNMPバージョンが「show snmp community」からの出力と一致することを確認します。

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) |
| <input checked="" type="checkbox"/> Link Trap Query |        |                                           |
| <input checked="" type="checkbox"/> MAC Trap Query  |        |                                           |
| Originating Policy Services Node                    | Auto   | ▼                                         |

スイッチは、SNMP v3認証/プライバシーパスワードをマスクします。これらのクレデンシャルが正確であることを確認するには、次の手順に従って再入力します。

1. ISE GUIにログインします。
2. [管理 ( Administration ) ] > [ネットワーク リソース ( Network Resources ) ] > [ネットワーク デバイス ( Network Devices ) ] に移動します。
3. 特定されたNADエントリを編集し、SNMP Settingsに移動します。Auth PasswordとPrivacy PasswordのShowをクリックします。そのパスワードを明らかにすることができます。

☒ **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) |
| <input checked="" type="checkbox"/> Link Trap Query |          |                                           |
| <input checked="" type="checkbox"/> MAC Trap Query  |          |                                           |
| Originating Policy Services Node                    | Auto     | ▼                                         |

#### 4. スイッチのCLIにログインします。

- configure terminalコマンドを実行します。
- その後、次のコマンドを実行して、スイッチのSNMP v3クレデンシャルを更新します。

スイッチ コマンド:

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

以下に例を挙げます。

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

ステップ4:ISE PSNとNADクライアント間の到達可能性および必要なUDPポート(161、162)を検証します。

1. Profiler対応PSNノードからNADクライアントにpingテストを実行します。
2. NADクライアントからPSNノードにpingテストを実行します。
3. PSNノードとNADの間でポート161および162が開いていることを確認します。
  - NADクライアントからProfiler対応ノードへのTelnetを使用してテストし、ポート161および162が開いていることを確認します。

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

## 原因

SNMP Request Failureアラームは、ISEがネットワークアクセスデバイスへのクエリに失敗すると発生します。これは通常、2台のデバイス間のSNMPコミュニティストリング、バージョン、またはv3クレデンシャルに関する設定の不一致が原因で発生します。さらに、ファイアウォールがUDPポート161または162をブロックしたり、NADでSNMPサーバ設定が欠落したりするなどのネットワークの問題が、正常な通信を妨げることがあります。

## 関連コンテンツ

[ネットワーク上で必要なISEポートとFQDNを許可する](#)

[ISEプロファイリング設計ガイド](#)

[SNMP コミュニティストリングの設定](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。