



# Quick Note 51

---

**Common Passwords/ID errors in IPsec VPN  
negotiation for TransPort WR routers**

Digi Support

## Contents

1	Introduction .....	4
1.1	Outline .....	4
1.2	Assumptions .....	4
1.3	Corrections .....	4
1.4	Version .....	4
2	How to Troubleshoot an IKE/IPsec VPN negotiation.....	5
2.1	Eventlog.....	5
2.2	Analyser IKE Trace.....	6
3	“No Password Available” error .....	7
3.1	What Eventlog shows .....	7
3.2	What to check & Solution.....	7
3.3	Deep analysis: What in the IKE trace .....	10
4	“Login failure by <responder ID>”/ “Bad Packet” Errors.....	11
4.1	What Eventlog shows .....	11
4.2	What to check & Solution.....	11
4.3	Deep analysis: What in the IKE trace .....	13
5	“Invalid ID Information,RX”/ “Login failure by <Initiator ID>” Errors.....	14
5.1	What Eventlog shows .....	14
5.1.1	Main Mode .....	14
5.1.2	Aggressive Mode.....	14
5.2	What to check & Solution.....	15
5.2.1	Main Mode .....	15
5.2.2	Aggressive Mode.....	16
5.3	Deep analysis: What in the IKE trace .....	18
5.3.1	Main Mode .....	18
5.3.2	Aggressive Mode.....	21
6	“Rx ID Failed”/ “Bad Packet” Errors .....	23

## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

6.1.1	Main Mode .....	23
6.1.2	Aggressive Mode.....	23
6.2	What to check & Solution.....	24
6.2.1	Main Mode .....	24
6.2.2	Aggressive Mode.....	26
6.3	Deep analysis: What in the IKE trace .....	28
6.3.1	Main Mode .....	28
6.3.2	Aggressive Mode.....	29

# 1 INTRODUCTION

## 1.1 Outline

When configuring an IPsec VPN on a TransPort WR router, users can experience issues in the negotiation phases related to Password/ID errors. This document provides a summary of the most common ones, with description, how to recognize them and what to check in order to solve them.

## 1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

**Preconditions:** This guide assumes that the Digi TransPort has IPsec features

**Models shown:** Digi TransPort WR44

**Other Compatible Models:** All other Digi TransPort products with IPsec features

**Firmware versions:** All Versions

**Configuration:** This Quick Note assumes that the devices are configured with an IPsec VPN using the Preshared Key authentication Method

## 1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: [tech.support@digi.com](mailto:tech.support@digi.com)

Requests for new application notes can be sent to the same address.

## 1.4 Version

Version Number	Status
1.0	Published
1.1	Update branding and WEB UI. Overall revision and fixes

## 2 HOW TO TROUBLESHOOT AN IKE/IPSEC VPN NEGOTIATION

In order to troubleshoot a VPN negotiation that is failing, two tools can be used on TransPort routers to see what is happening: Eventlog and Anlyser IKE trace.

### 2.1 Eventlog

First of all, when a user sees that the configured VPN doesn't go UP, the first thing to do is to look in the eventlog section of the TransPort, where are shown the main events occurring in the device, so also the main phases of the VPN negotiation.

#### MANAGEMENT - EVENT LOG:

```
Management - Event Log
12:56:33, 21 Sep 2017, PPP 1 down, LL disconnect
12:56:47, 21 Sep 2017, (273) New Phase 1 IKE Session 192.168.1.20, Initiator
12:56:47, 21 Sep 2017, IKE Request Received From Eroute 0
12:56:47, 21 Sep 2017, (272) IKE SA Removed. Peer: ,Negotiation Failure
12:56:47, 21 Sep 2017, (272) IKE Negotiation Failed. Peer: ,Retries Exceeded
12:56:43, 21 Sep 2017, PPP 1 down, LL disconnect
12:56:37, 21 Sep 2017, IKE Request Received From Eroute 0
12:56:33, 21 Sep 2017, PPP 1 down, LL disconnect
12:56:27, 21 Sep 2017, IKE Request Received From Eroute 0
12:56:23, 21 Sep 2017, PPP 1 down, LL disconnect
12:56:17, 21 Sep 2017, (272) New Phase 1 IKE Session 192.168.1.20, Initiator
12:56:17, 21 Sep 2017, IKE Request Received From Eroute 0
12:56:17, 21 Sep 2017, (271) IKE SA Removed. Peer: ,Negotiation Failure
12:56:17, 21 Sep 2017, (271) IKE Negotiation Failed. Peer: ,Retries Exceeded
12:56:13, 21 Sep 2017, PPP 1 down, LL disconnect
12:56:07, 21 Sep 2017, IKE Request Received From Eroute 0
12:56:03, 21 Sep 2017, PPP 1 down, LL disconnect
12:55:57, 21 Sep 2017, IKE Request Received From Eroute 0
12:55:53, 21 Sep 2017, PPP 1 down, LL disconnect
12:55:47, 21 Sep 2017, (271) New Phase 1 IKE Session 192.168.1.20, Initiator
12:55:47, 21 Sep 2017, IKE Request Received From Eroute 0
12:55:47, 21 Sep 2017, (270) IKE SA Removed. Peer: ,Negotiation Failure
12:55:47, 21 Sep 2017, (270) IKE Negotiation Failed. Peer: ,Retries Exceeded
12:55:43, 21 Sep 2017, PPP 1 down, LL disconnect
12:55:37, 21 Sep 2017, IKE Request Received From Eroute 0
12:55:33, 21 Sep 2017, PPP 1 down, LL disconnect

Refresh Clear Log Open in New Window
```

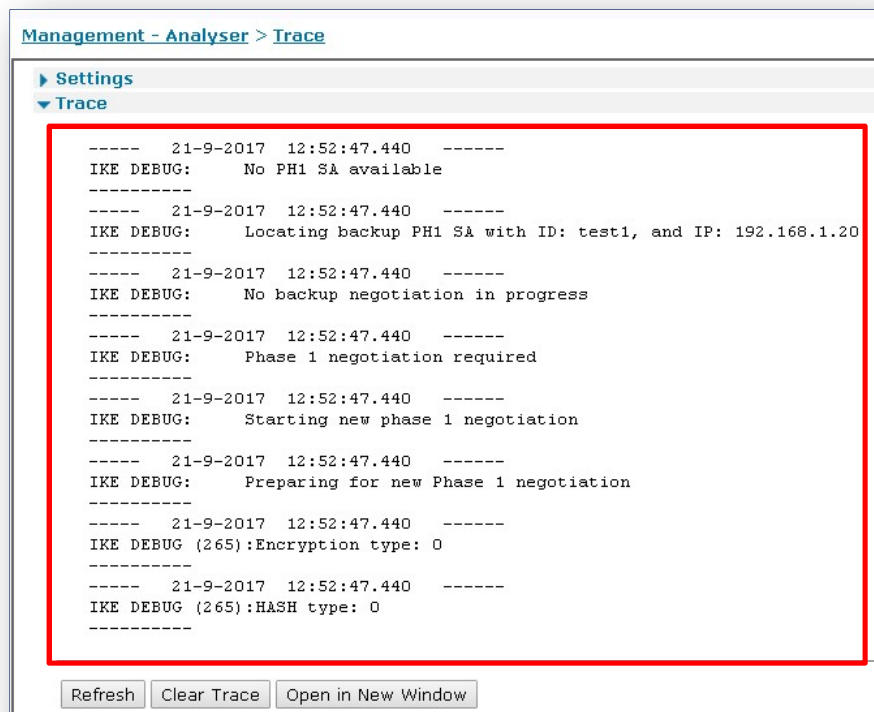
Figure 2.1-1: Eventlog Section Example

## 2.2 Analyser IKE Trace

If the messages found in the eventlog section are not enough to understand what is wrong in the setup, an IKE Trace needs to be configured, for this, please see instructions on: [QN45 - How To Get IKE/IPsec trace on TransPort Routers](#).

Following a screenshot of an example of what can be seen in the analyser trace when IKE debug is configured.

### MANAGEMENT - ANALYSER > TRACE:



```
Management - Analyser > Trace
  Settings
  Trace
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG:    No PH1 SA available
  -----
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG:    Locating backup PH1 SA with ID: test1, and IP: 192.168.1.20
  -----
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG:    No backup negotiation in progress
  -----
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG:    Phase 1 negotiation required
  -----
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG:    Starting new phase 1 negotiation
  -----
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG:    Preparing for new Phase 1 negotiation
  -----
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG (265):Encryption type: 0
  -----
  ----- 21-9-2017 12:52:47.440 -----
  IKE DEBUG (265):HASH type: 0
  -----
  Refresh Clear Trace Open in New Window
```

Figure 2.2-3: Analyser with IKE trace

Please note that each of the following sections is named as the errors that the user can easily see in the eventlog section. Anyway, it will be also explained what is shown in the Analyser IKE trace to better understand the issue in case of doubts.

### 3 “NO PASSWORD AVAILABLE” ERROR

This error appears on the Initiator when **Main Mode** is used and in the Initiator the “Remote peer’s IP” in the tunnel configuration has not a matching user in Security configuration.

No logs will be showed at responder side in this case, because the VPN doesn’t start at all from the Initiator due to this error.

#### 3.1 What Eventlog shows

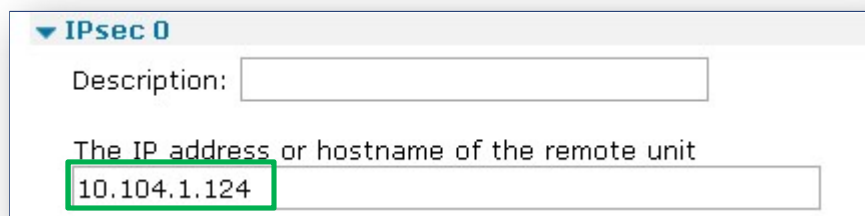
The error described in this section is shown in the eventlog section of a TransPort acting as Initiator of the VPN, and appear similar to the following:

```
15:40:39, 18 Feb 2015,(7) IKE SA Removed. Peer: ,Negotiation Failure
15:40:39, 18 Feb 2015,(7) IKE Negotiation Failed. Peer: ,No Password Available
15:40:39, 18 Feb 2015,IKE Request Received From Eroute 0
```

#### 3.2 What to check & Solution

On the Initiator:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**



The Remote Peer’s IP field is the IP address to which the Initiator connects in order to establish the VPN.

**CONFIGURATION - SECURITY > USERS:**



The User configured with the Preshared Key to identify the remote peer has not the “Remote Peer’s IP” as username.

**Solution:**

Basing on RFC 2409, Main Mode with pre-shared key authentication requires knowledge of the peer's pre-shared key prior to the knowledge of the peers’ identity. Therefore, Main Mode with pre-shared keys can only be used when the IP address of the peer is the identifier of the peer.

This is the reason why, in this case, the Pre-shared key user must have the username as the “Remote Peer’s IP”.

Change the configuration in order to have a user with the “Remote Peer’s IP” as username:



## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

### CONFIGURATION - SECURITY > USERS:

▼ Users

- ▶ User 0 - 9
- ▼ User 10 - 14
  - ▼ User 10

Username:

Password:

Confirm Password:

Access Level:

▶ Advanced

**Note:** if the environment doesn't allow using IP address to identify the peer, the only solution is to use Aggressive Mode:

### CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IKE > IKE 0

▼ IKE

- ▶ IKE Debug
- ▼ IKE 0

Use the following settings for negotiation

Encryption:  None  DES  3DES  AES (128 bit)  AES (192 bit)  AES (256 bit)

Authentication:  None  MD5  SHA1  SHA256

Mode:  Main  Aggressive

MODP Group for Phase 1:

MODP Group for Phase 2:

Renegotiate after  hrs  mins  secs

▶ Advanced

### 3.3 Deep analysis: What in the IKE trace

On the Initiator (an extract of the whole trace is reported), the IKE trace shows that the Phase 1 negotiation cannot be started due to an error in retrieving password:

```
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: IKE received SA request from eroute 0
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: New IKE request
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Start new IKE negotiation
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Locating PH1 SA with ID: initiator, and IP: 10.104.1.114
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: No PH1 SA available
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Locating backup PH1 SA with ID: initiator, and IP: 10.104.1.114
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: No backup negotiation in progress
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Phase 1 negotiation required
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Starting new phase 1 negotiation
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Preparing for new Phase 1 negotiation
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG (7): Encryption type: 2
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG (7): Key length: 128 bits
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG (7): HASH type: 1
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG (7): DH group: 2
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG (7): No password available
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Error starting new phase 1 negotiation
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG: Unable to process SA request
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG (7): Resetting IKE context 0
-----
----- 18-2-2015 15:40:39.110 -----
IKE DEBUG (7): Removing IKE SA
```

## 4 “LOGIN FAILURE BY <RESPONDER ID>”/ “BAD PACKET” ERRORS

This error appears on the Initiator/Responder when **Aggressive Mode** is used and on the Initiator there is NO correspondence between “Remote ID” in the tunnel configuration and a User in Security configuration.

### 4.1 What Eventlog shows

The eventlog on the Initiator will show:

```
13:14:01, 24 Feb 2015,(40) IKE SA Removed. Peer: responder,Negotiation Failure
13:14:01, 24 Feb 2015,(40) IKE Negotiation Failed. Peer: ,Rx SA Failed
13:14:01, 24 Feb 2015,Login failure by responder: IKE,IKE
13:14:01, 24 Feb 2015,(40) New Phase 1 IKE Session 10.104.1.124,Initiator
13:14:01, 24 Feb 2015,IKE Request Received From Eroute 0
```

The eventlog on the Responder will show:

```
22:23:22, 06 Jan 2000,(41) IKE Negotiation Failed. Peer: ,Bad Packet
22:23:22, 06 Jan 2000,(40) IKE Keys Negotiated. Peer: initiator
22:23:22, 06 Jan 2000,(40) New Phase 1 IKE Session 10.104.34.110,Responder
```

### 4.2 What to check & Solution

On the Initiator & Responder:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration page for IPsec 0. The description is "Test VPN - Initiator". The remote unit IP address is 10.104.1.124. The Local LAN settings are: IP Address 172.16.1.0, Mask 255.255.255.0, and Use interface PPP. The Remote LAN settings are: IP Address 192.168.1.0, Mask 255.255.255.0, and Remote Subnet ID. The security options are: Off, Preshared Keys, XAUTH Init Preshared Keys, RSA Signatures, and XAUTH Init RSA. The Our ID is initiator, and the Remote ID is responder.

## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

**IPsec 0**

Description:

The IP address or hostname of the remote unit

Use  as a backup unit

Local LAN	Remote LAN
<input checked="" type="radio"/> Use these settings for the local LAN	<input checked="" type="radio"/> Use these settings for the remote LAN
IP Address: <input type="text" value="192.168.1.0"/>	IP Address: <input type="text" value="172.16.1.0"/>
Mask: <input type="text" value="255.255.255.0"/>	Mask: <input type="text" value="255.255.255.0"/>
<input type="radio"/> Use interface <input type="text" value="PPP"/> <input type="text" value="0"/>	<input type="radio"/> Remote Subnet ID: <input type="text"/>

Use the following security on this tunnel

Off  Preshared Keys  XAUTH Init Preshared Keys  RSA Signatures  XAUTH Init RSA

Our ID:

Our ID type:  IKE ID  FQDN  User FQDN  IPv4 Address

Remote ID:

On the Initiator:

### CONFIGURATION - SECURITY > USERS

**User 10**

Username:

Password:

Confirm Password:

Access Level:

[Advanced](#)

Solution: Configure on the Initiator a user matching the ID of the responder

### CONFIGURATION - SECURITY > USERS

**User 10**

Username:

Password:

Confirm Password:

Access Level:

### 4.3 Deep analysis: What in the IKE trace

On the Initiator (an extract of the whole trace is reported):

```
IKE DEBUG (40):Processing ID payload
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Decoding ID type 11 Key ID
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Decoded ID is responder
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Peer ID matches eroute
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Retrieving password
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Decoding ID type 11 Key ID
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Decoded ID is responder
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Unable to locate password for ID responder
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):Error processing aggressive mode SA message
-----
----- 24-2-2015 13:14:01.760 -----
IKE DEBUG (40):IKE aggressive mode result 0
IKE DEBUG (40):Processing ID payload
-----
```

This trace confirms that the received Responder ID is “responder” and on the Initiator is not possible to retrieve a password for it as there is no matching user configured.

## 5 “INVALID ID INFORMATION,RX”/ “LOGIN FAILURE BY <INITIATOR ID>” ERRORS

This error appears on the Initiator/Responder when either Main Mode or Aggressive Mode is used, and on the Responder there is no User that matches with the ID sent by Initiator. Please note that in Main Mode case, <initiator ID> will be the IP address of the Initiator.

### 5.1 What Eventlog shows

#### 5.1.1 Main Mode

In the eventlog section of the Initiator, when Main Mode is used, the eventlog will show lines as the following:

```
10:35:32, 20 Feb 2015,(23) IKE Negotiation Failed. Peer: ,Bad Packet
10:35:32, 20 Feb 2015,(21) IKE SA Removed. Peer: ,Successful Negotiation
10:35:32, 20 Feb 2015,(21) IKE Notification: Invalid ID Information,RX
10:35:32, 20 Feb 2015,(21) New Phase 1 IKE Session 10.104.1.124,Initiator
10:35:32, 20 Feb 2015,IKE Request Received From Eroute 0
```

On the responder:

```
19:45:03, 02 Jan 2000,(9) IKE Negotiation Failed. Peer: ,Bad Packet
19:45:03, 02 Jan 2000,(7) IKE SA Removed. Peer: ,Negotiation Failure
19:45:03, 02 Jan 2000,(7) IKE Notification: Invalid ID Information,TX
19:45:03, 02 Jan 2000,Login failure by 10.104.34.108: IKE,IKE
19:45:03, 02 Jan 2000,(7) New Phase 1 IKE Session 10.104.34.108,Responder
```

#### 5.1.2 Aggressive Mode

In the eventlog section of the Initiator, when Aggressive Mode is used, the eventlog will show lines as the following:

```
15:25:47, 23 Feb 2015,(39) IKE Negotiation Failed. Peer: ,Bad Packet
15:25:47, 23 Feb 2015,(37) IKE SA Removed. Peer: ,Successful Negotiation
15:25:47, 23 Feb 2015,(37) IKE Notification: Invalid ID Information,RX
15:25:47, 23 Feb 2015,(37) New Phase 1 IKE Session 10.104.1.124,Initiator
15:25:47, 23 Feb 2015,IKE Request Received From Eroute 0
```

On the responder:

```
00:35:09, 06 Jan 2000,(39) IKE Negotiation Failed. Peer: ,Bad Packet
00:35:09, 06 Jan 2000,(37) IKE SA Removed. Peer: initiator,Negotiation Failure
00:35:09, 06 Jan 2000,(37) IKE Notification: Invalid ID Information,TX
00:35:09, 06 Jan 2000,Login failure by initiator: IKE,IKE
00:35:09, 06 Jan 2000,(37) New Phase 1 IKE Session 10.104.34.110,Responder
```

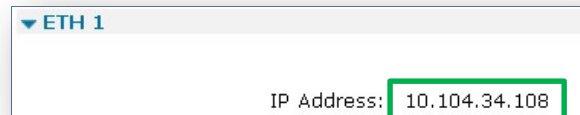
## 5.2 What to check & Solution

### 5.2.1 Main Mode

#### Initiator:

Check the WAN address of the Initiator. How to check it depends on the WAN interface type. In this example, the WAN is ETH 1.

**MANAGEMENT - NETWORK STATUS > INTERFACES > ETHERNET > ETH 1**



If there are doubts on the address sent from the Initiator as ID for the VPN, this can be checked looking at the IKE trace (see section 5.3).

#### Responder:

**CONFIGURATION - SECURITY > USERS**



#### Solution:

**RESPONDER: CONFIGURATION - SECURITY > USERS**



On the Responder must be configured a user matching the Initiator IP address.

## 5.2.2 Aggressive Mode

Initiator:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration page for an IPsec tunnel named "Test VPN - Initiator". The "Our ID" field is highlighted with a green box and contains the value "initiator".

**IPsec Tunnels**  
▼ **IPsec 0 - Test VPN - Initiator**

Description: Test VPN - Initiator

The IP address or hostname of the remote unit  
10.104.1.124

Use \_\_\_\_\_ as a backup unit

Local LAN	Remote LAN
<input checked="" type="radio"/> Use these settings for the local LAN	<input checked="" type="radio"/> Use these settings for the remote LAN
IP Address: 172.16.1.0	IP Address: 192.168.1.0
Mask: 255.255.255.0	Mask: 255.255.255.0
<input type="radio"/> Use interface PPP 0	<input type="radio"/> Remote Subnet ID: _____

Use the following security on this tunnel

Off  Preshared Keys  XAUTH Init Preshared Keys  RSA Signatures  XAUTH Init RSA

Our ID: initiator

Our ID type:  IKE ID  FQDN  User FQDN  IPv4 Address

Remote ID: responder

The "Our ID field" configured in the Tunnel section, when Aggressive Mode is used, must match with a User in the Responder Security configuration.

Responder:

**CONFIGURATION - SECURITY > USERS**

The screenshot shows the configuration page for a user named "User 10". The "Username" field is highlighted with a red box and contains the value "init".

**User 10**

Username: init

Password: ••••••

Confirm Password: \_\_\_\_\_

Access Level: None ▼

▶ **Advanced**

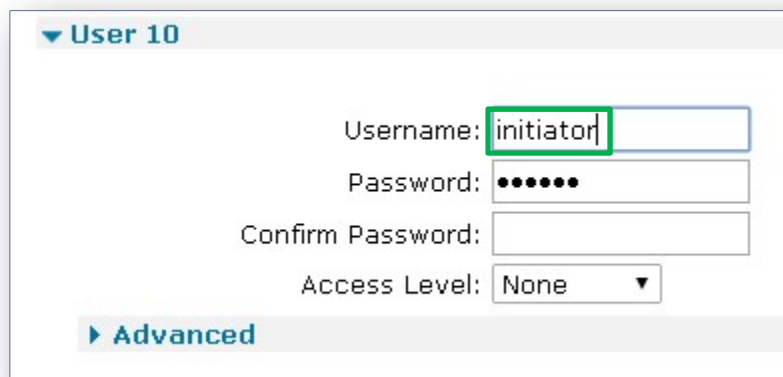


## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

### Solution:

The “Our ID” field on the Initiator Tunnel configuration and the Pre-shared key User on the Responder must match:

### **RESPONDER: CONFIGURATION - SECURITY > USERS**



The screenshot displays the configuration interface for a user named "User 10". The fields are as follows:

- Username:** A text input field containing the text "initiator".
- Password:** A text input field containing six black dots, indicating a masked password.
- Confirm Password:** An empty text input field.
- Access Level:** A dropdown menu currently set to "None".

At the bottom of the configuration area, there is a link labeled "Advanced" with a right-pointing arrow.

## 5.3 Deep analysis: What in the IKE trace

### 5.3.1 Main Mode

On the Initiator (an extract of the whole trace is reported), the IKE trace shows that the Responder has sent an Info Packet containing a notify payload with “Message type 18” that correspond to the “INVALID-ID-INFORMATION” error.

```

----- 20-2-2015 10:35:32.720 -----
IKE DEBUG (21):Changing IKE SA state from PH1 sent SA to PH1 sent KE
-----
----- 20-2-2015 10:35:32.720 -----
IKE DEBUG:      Handling IKE packet
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG:      Locating IKE context
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG:      Packet for existing negotiation
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Located SA for existing phase 1 negotiation
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):IKE context located. Local session ID: 0x21
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Checking packet
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Got unencrypted INFO packet
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Validating payloads
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Checking payload (11) Notify
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Packet payloads check out OK
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Packet type (5) Informational
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):IKE role Initiator
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Handling INFO packet
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):Got INFO exchange
-----
----- 20-2-2015 10:35:32.730 -----
IKE DEBUG (21):1 notify payload
-----

```

## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

```
----- 20-2-2015 10:35:32.730 -----  
IKE DEBUG (21):Handling NOTIFY payload with message type 18  
-----  
----- 20-2-2015 10:35:32.730 -----  
IKE DEBUG (21):Resetting IKE context 0
```

On the Responder (an extract of the whole trace is reported), the IKE trace shows that the responder is not able to retrieve a password for the Remote IP that is used as ID, and so the “Invalid ID information” notification is sent to the Initiator:

```
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG: Handling IKE packet  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG: Locating IKE context  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG: Packet for existing negotiation  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Located SA for existing phase 1 negotiation  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): IKE context located. Local session ID: 0x7  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Checking packet  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Validating payloads  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Checking payload (4) Key Ex  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Checking payload (10) Nonce  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Checking payload (20) NATD (RFC)  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Checking payload (20) NATD (RFC)  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Packet payloads check out OK  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Packet type (2) Main mode  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): IKE role Responder  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Handling main mode packet and SA state is (2) PH1 sent SA
```

## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

```
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Processing KE and NONCE payloads  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Processing RFC NATD payloads  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): HASH's same, we are not behind a NAT box  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Remote peer is not behind a NAT box  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): DH g_x length: 128  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Retrieving password  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Using remote IP (10.104.34.108) as ID  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Unable to locate password for ID 10.104.34.108  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Sending IKE phase 1 notification  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG (7): Notification type (18) Invalid ID Information  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG:      Handling IKE packet  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG:      Locating IKE context  
-----  
----- 2-1-2000 19:45:03.640 -----  
IKE DEBUG:      Packet for existing negotiation
```

### 5.3.2 Aggressive Mode

On the Initiator (an extract of the whole trace is reported), the IKE trace shows that the Responder has sent an Info Packet containing a notify payload with “Message type 18” that correspond to the “INVALID-ID-INFORMATION” error.

```

----- 23-2-2015 15:25:47.580 -----
IKE DEBUG:      Handling IKE packet
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG:      Locating IKE context
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG:      Packet for existing negotiation
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Located SA for existing phase 1 negotiation
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):IKE context located. Local session ID: 0x37
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Checking packet
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Got unencrypted INFO packet
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Validating payloads
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Checking payload (11) Notify
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Packet payloads check out OK
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Packet type (5) Informational
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):IKE role Initiator
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Handling INFO packet
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Got INFO exchange
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):1 notify payload
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Handling NOTIFY payload with message type 18
-----
----- 23-2-2015 15:25:47.580 -----
IKE DEBUG (37):Resetting IKE context 0
-----

```

## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

On the responder (an extract of the whole trace is reported), the IKE trace shows that the responder is not able to retrieve a password for the ID sent by the Initiator, and so the “Invalid ID information” notification is sent to the Initiator:

```
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Retrieving password  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Decoding ID type 11 Key ID  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Decoded ID is initiator  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Unable to locate password for ID initiator  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Sending IKE phase 1 notification  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Notification type (18) Invalid ID Information  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Transmit IKE packet  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Transmit to peer 10.104.34.110  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):IKE notification sent Invalid ID Information  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Error processing SA message  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):IKE aggressive mode result 0  
-----  
----- 6-1-2000 00:35:09.600 -----  
IKE DEBUG (37):Resetting IKE context 0
```

## 6 “RX ID FAILED”/ “BAD PACKET” ERRORS

This error appears on the Initiator/Responder when Main Mode or Aggressive Mode is used and, on the Initiator, the “Remote ID” on Tunnel configuration, doesn’t match with the ID sent by the responder. Please note that in Main Mode case this sent ID is the responder IP address, instead in Aggressive Mode this will be the “our ID” field in responder’s Tunnel configuration.

### 6.1.1 Main Mode

In the eventlog section of the Initiator, when Main Mode is used, the eventlog will show lines as the following:

```
15:54:42, 24 Feb 2015,(88) IKE SA Removed. Peer: 10.104.1.124,Negotiation Failure
15:54:42, 24 Feb 2015,(88) IKE Notification: Invalid ID Information,TX
15:54:42, 24 Feb 2015,(88) IKE Negotiation Failed. Peer: ,Rx ID Failed
15:54:42, 24 Feb 2015,(88) IKE Keys Negotiated. Peer:
15:54:42, 24 Feb 2015,(88) New Phase 1 IKE Session 10.104.1.124,Initiator
15:54:42, 24 Feb 2015,IKE Request Received From Eroute 0
```

On the responder:

```
15:54:42, 24 Feb 2015,(90) IKE Negotiation Failed. Peer: ,Bad Packet
15:54:42, 24 Feb 2015,(88) IKE Keys Negotiated. Peer:
15:54:42, 24 Feb 2015,(88) New Phase 1 IKE Session 10.104.34.110,Responder
```

### 6.1.2 Aggressive Mode

In the eventlog section of the Initiator, when Aggressive Mode is used, the eventlog will show lines as the following:

```
13:28:12, 24 Feb 2015,(79) IKE SA Removed. Peer: responder,Negotiation Failure
13:28:12, 24 Feb 2015,(79) IKE Negotiation Failed. Peer: ,Rx SA Failed
13:28:12, 24 Feb 2015,(79) IKE Negotiation Failed. Peer: ,Rx ID Failed
13:28:12, 24 Feb 2015,(79) New Phase 1 IKE Session 10.104.1.124,Initiator
13:28:12, 24 Feb 2015,IKE Request Received From Eroute 0
```

On the responder:

```
22:37:32, 06 Jan 2000,(80) IKE Negotiation Failed. Peer: ,Bad Packet
22:37:32, 06 Jan 2000,(79) IKE Keys Negotiated. Peer: initiator
22:37:32, 06 Jan 2000,(79) New Phase 1 IKE Session 10.104.34.110,Responder
```

## 6.2 What to check & Solution

### 6.2.1 Main Mode

Initiator:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration page for an IPsec tunnel. The 'Description' is 'Test VPN - Initiator'. The 'Remote IP address or hostname' is '10.104.1.124'. Under 'Local LAN', the 'IP Address' is '172.16.1.0' and the 'Mask' is '255.255.255.0'. Under 'Remote LAN', the 'IP Address' is '192.168.1.0' and the 'Mask' is '255.255.255.0'. The 'Security' section is set to 'Preshared Keys'. The 'Our ID' is 'initiator' and the 'Our ID type' is 'IKE ID'. The 'Remote ID' is 'responder'.

Responder:

Check the WAN address of the Responder. How to check it depends on the WAN interface type. In this example, the WAN is ETH 1:

**MANAGEMENT - NETWORK STATUS > INTERFACES > ETHERNET > ETH 1**

The screenshot shows the configuration page for the 'ETH 1' interface. The 'IP Address' is '10.104.1.124'.

If there are doubts on the address used from the Initiator as ID for the VPN, this can be checked looking at the IKE trace (see section 6.3).



## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

Solution:

**INITIATOR: CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration page for an IPsec Tunnel in an Initiator role. The tunnel is named "Test VPN - Initiator". The configuration is divided into two main sections: "Local LAN" and "Remote LAN".

**Local LAN:**

- Use these settings for the local LAN
- IP Address: 172.16.1.0
- Mask: 255.255.255.0
- Use interface: PPP, 0

**Remote LAN:**

- Use these settings for the remote LAN
- IP Address: 192.168.1.0
- Mask: 255.255.255.0
- Remote Subnet ID: [Empty]

**Security:**

Use the following security on this tunnel

- Off
- Preshared Keys
- XAUTH Init Preshared Keys
- RSA Signatures
- XAUTH Init RSA

Our ID: initiator

Our ID type:  IKE ID,  FQDN,  User FQDN,  IPv4 Address

Remote ID: 10.104.1.124

On the Initiator, in the Tunnel configuration, the Remote ID must be changed to match the Responder IP address.

## 6.2.2 Aggressive Mode

Initiator:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration for an IPsec tunnel named "Test VPN - Initiator". The description is "Test VPN - Initiator". There are fields for the remote unit's IP address and a backup unit. The Local LAN settings are: IP Address: 172.16.1.0, Mask: 255.255.255.0, and interface PPP 0. The Remote LAN settings are: IP Address: 192.168.1.0, Mask: 255.255.255.0, and Remote Subnet ID. Security options include Off, Preshared Keys (selected), XAUTH Init Preshared Keys, RSA Signatures, and XAUTH Init RSA. The "Our ID" is "initiator", "Our ID type" is "IKE ID" (selected), and "Remote ID" is "resp", which is highlighted with a red box.

Responder:

**CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration for an IPsec tunnel named "Test VPN - Responder". The description is "Test VPN - Responder". There are fields for the remote unit's IP address and a backup unit. The Local LAN settings are: IP Address: 192.168.1.0, Mask: 255.255.255.0, and interface PPP 0. The Remote LAN settings are: IP Address: 172.16.1.0, Mask: 255.255.255.0, and Remote Subnet ID. Security options include Off, Preshared Keys (selected), XAUTH Init Preshared Keys, RSA Signatures, and XAUTH Init RSA. The "Our ID" is "responder", which is highlighted with a red box, "Our ID type" is "IKE ID" (selected), and "Remote ID" is "initiator".

## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

### Solution:

The “Remote ID” field on the Initiator Tunnel configuration and the “Our ID field” on the Responder configuration must match:

**INITIATOR: CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration for an IPsec tunnel on the Initiator side. The tunnel is named "IPsec 0 - Test VPN - Initiator". The remote unit IP address is set to 10.104.1.124. The Local LAN settings are: IP Address 172.16.1.0, Mask 255.255.255.0, and Interface PPP 0. The Remote LAN settings are: IP Address 192.168.1.0, Mask 255.255.255.0, and Remote Subnet ID is empty. The security settings are: Off, Preshared Keys, XAUTH Init Preshared Keys, RSA Signatures, and XAUTH Init RSA. The "Our ID" is set to "initiator", "Our ID type" is IKE ID, and "Remote ID" is set to "responder".

**RESPONDER: CONFIGURATION - NETWORK > VIRTUAL PRIVATE NETWORKING (VPN) > IPSEC > IPSEC TUNNELS > IPSEC N**

The screenshot shows the configuration for an IPsec tunnel on the Responder side. The tunnel is named "IPsec 0 - Test VPN - Responder". The remote unit IP address is empty. The Local LAN settings are: IP Address 192.168.1.0, Mask 255.255.255.0, and Interface PPP 0. The Remote LAN settings are: IP Address 172.16.1.0, Mask 255.255.255.0, and Remote Subnet ID is empty. The security settings are: Off, Preshared Keys, XAUTH Init Preshared Keys, RSA Signatures, and XAUTH Init RSA. The "Our ID" is set to "responder", "Our ID type" is IKE ID, and "Remote ID" is set to "initiator".

## 6.3 Deep analysis: What in the IKE trace

### 6.3.1 Main Mode

On the Initiator (an extract of the whole trace is reported), the IKE trace shows that the Responder IP doesn't match with the configured eroute, this cause an error and the Initiator sent an "Invalid ID information" message:

```

----- 24-2-2015 15:54:42.810 -----
IKE DEBUG:      Handling IKE packet
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG:      Locating IKE context
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG:      Packet for existing negotiation
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Located SA for existing phase 1 negotiation
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):IKE context located. Local session ID: 0x88
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Checking packet
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):IKE decrypting packet
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Validating payloads
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Checking payload (5) ID
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Checking payload (8) Hash
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Packet payloads check out OK
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Packet type (2) Main mode
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):IKE role Initiator
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Handling main mode packet and SA state is (4) PH1 sent hash
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Processing ID payload
-----
----- 24-2-2015 15:54:42.810 -----
IKE DEBUG (88):Decoding ID type 1 IP V4 address
-----

```

## Common Passwords/ID errors in IPsec VPN negotiation for transport routers

```
----- 24-2-2015 15:54:42.810 -----  
IKE DEBUG (88):Decoded ID is 10.104.1.124  
-----  
----- 24-2-2015 15:54:42.810 -----  
IKE DEBUG (88):Peer ID doesn't match eroute  
-----  
----- 24-2-2015 15:54:42.810 -----  
IKE DEBUG (88):Error processing ID payload  
-----  
----- 24-2-2015 15:54:42.810 -----  
IKE DEBUG (88):Sending IKE phase 1 notification  
-----  
----- 24-2-2015 15:54:42.810 -----  
IKE DEBUG (88):Notification type (18) Invalid ID Information  
-----
```

### 6.3.2 Aggressive Mode

On the Initiator (an extract of the whole trace is reported), the IKE trace shows:

```
----- 24-2-2015 13:28:12.300 -----  
IKE DEBUG (79):Processing ID payload  
-----  
----- 24-2-2015 13:28:12.300 -----  
IKE DEBUG (79):Decoding ID type 11 Key ID  
-----  
----- 24-2-2015 13:28:12.300 -----  
IKE DEBUG (79):Decoded ID is responder  
-----  
----- 24-2-2015 13:28:12.300 -----  
IKE DEBUG (79):Peer ID doesn't match eroute  
-----  
----- 24-2-2015 13:28:12.300 -----  
IKE DEBUG (79):Error processing ID payload  
-----  
----- 24-2-2015 13:28:12.300 -----  
IKE DEBUG (79):Error processing aggressive mode SA message  
-----  
----- 24-2-2015 13:28:12.300 -----  
IKE DEBUG (79):IKE aggressive mode result 0
```

So, also in this case, the responder ID doesn't match with the configured eroute, this cause an error in processing the payload.