

Configuring the Cisco VPN 5000 Client to the Cisco VPN 5000 Concentrator with SDI Authentication

Document ID: 10134

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, refer to the End-of-Sales Announcement.

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations
- SDI Client Configuration

Verify

- SDI Log
- VPN 5000

Troubleshoot

- Node Verification Failed
- Server Unreachable
- Bad Username on VPN 5000
- Bad Username/Token on SDI

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document demonstrates how to configure the Cisco VPN 5000 Concentrator to authenticate Cisco VPN 5000 clients with native Security Dynamics International (SDI) (UDP 5500). This document assumes that local authentication works prior to the addition of SDI authentication (hence, the user *localuser* in group *ciscolocal*). Authentication to SDI is then added.

There are two ways to use SDI:

- Usernames can be enumerated on the VPN 5000 Concentrator. The user enters a VPN 5000 Concentrator username and password once and the VPN 5000 Concentrator passes the same username to the SDI server (in this example, user *vpnuser* in group *listuser* with password *vpnuser*). The user is prompted for an SDI token. On the VPN 5000 Concentrator, this requires:

```
SecurIDUserName = Off
```

- Usernames can be non-enumerated on the VPN 5000 Concentrator, but all users assigned a very generic username/password/group (in our example, user *catchall* in group *catchall* with password *catchall*). Once the user enters the VPN 5000 Concentrator username/password, the user is prompted for an SDI username and token. On the VPN 5000 Concentrator, this requires:

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- SDI 3.3
- VPN 5000 Concentrator 5.2.16.0005
- VPN 5000 Client 4.2.7

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

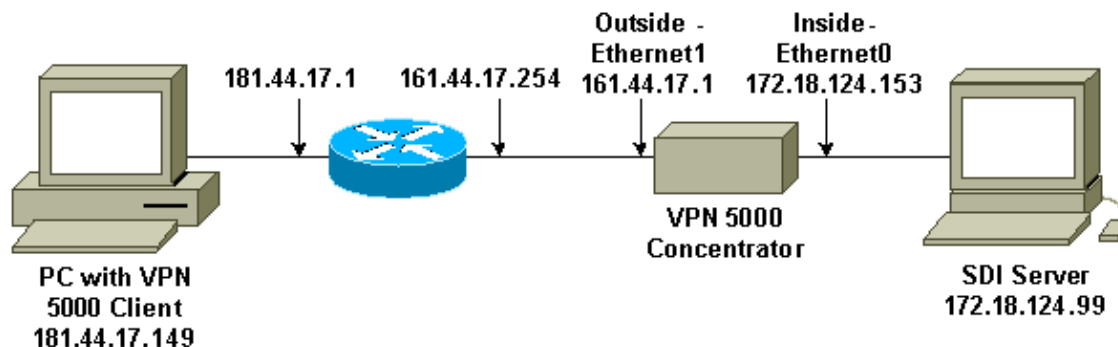
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only).

Network Diagram

This document uses this network setup:



Configurations

This document uses these configurations:

- VPN 5000 Concentrator
- VPN 5000 Client

```

VPN 5000 Concentrator
[ IP Ethernet 0 ]
IPAddress          = 172.18.124.153
SubnetMask         = 255.255.255.0
Mode               = Routed

[ IP Ethernet 1 ]
Mode               = Routed
IPAddress          = 161.44.17.1
SubnetMask         = 255.255.255.0

[ VPN Group "catchall" ]
SecurIDUserName    = On
SecurIDRequired    = On
IPNet              = 172.18.124.0/24
StartIPAddress     = 172.18.124.250
Transform          = esp(md5,des)
BindTo             = "ethernet0"
MaxConnections     = 2

[ SecurID ]
Enabled            = On
  EncryptMethod    = DES
BindTo             = "ethernet 0"
PrimaryServer      = 172.18.124.99

[ General ]
EthernetAddress    = 00:00:a5:f0:c9:00
DeviceType         = VPN 5001 Concentrator
ConfiguredOn       = Timeserver not configured
ConfiguredFrom     = Command Line, from Console
IPSecGateway       = 161.44.17.254

[ Logging ]
Level              = 7
Enabled            = On
LogToAuxPort       = On
LogToSysLog        = On
SyslogIPAddress    = 172.18.124.114
SyslogFacility     = Local5

[ VPN Group "localusers" ]
SecurIDRequired    = Off
IPNet              = 172.18.124.0/24

Transform          = esp(md5,des)
StartIPAddress     = 172.18.124.252
MaxConnections     = 2
BindTo             = "ethernet0"

[ VPN Users ]
catchall Config="catchall" SharedKey="catchall"
vpnuser Config="listuser" SharedKey="vpnuser"
localuser Config="localusers" SharedKey="localike"

[ IKE Policy ]
Protection         = MD5_DES_G1

```

```

[ VPN Group "listuser" ]
SecurIDUserName      = Off
SecurIDRequired      = On
BindTo               = "ethernet 0"
MaxConnections       = 2
StartIPAddress       = 172.18.124.248
Transform             = esp(md5,des)
IPNet                = 172.18.124.0/24

```

Note: In this configuration, none of the defaults are changed. Three users are added and the appropriate passwords entered when prompted after you click **Connect**.

| VPN 5000 Client | | | |
|-----------------|-----------------|--------------|--------------|
| username (5000) | password (5000) | SDI_username | SDI_password |
| ----- | ----- | ----- | ----- |
| localuser | localike | N/A | |
| catchall | catchall | 37297304 | token |
| vpnuser | vpnuser | vpnuser | token |

SDI Client Configuration

Follow this procedure to configure the SDI client.

1. Before configuring the SDI client, issue the following commands on the VPN 5000 Concentrator:

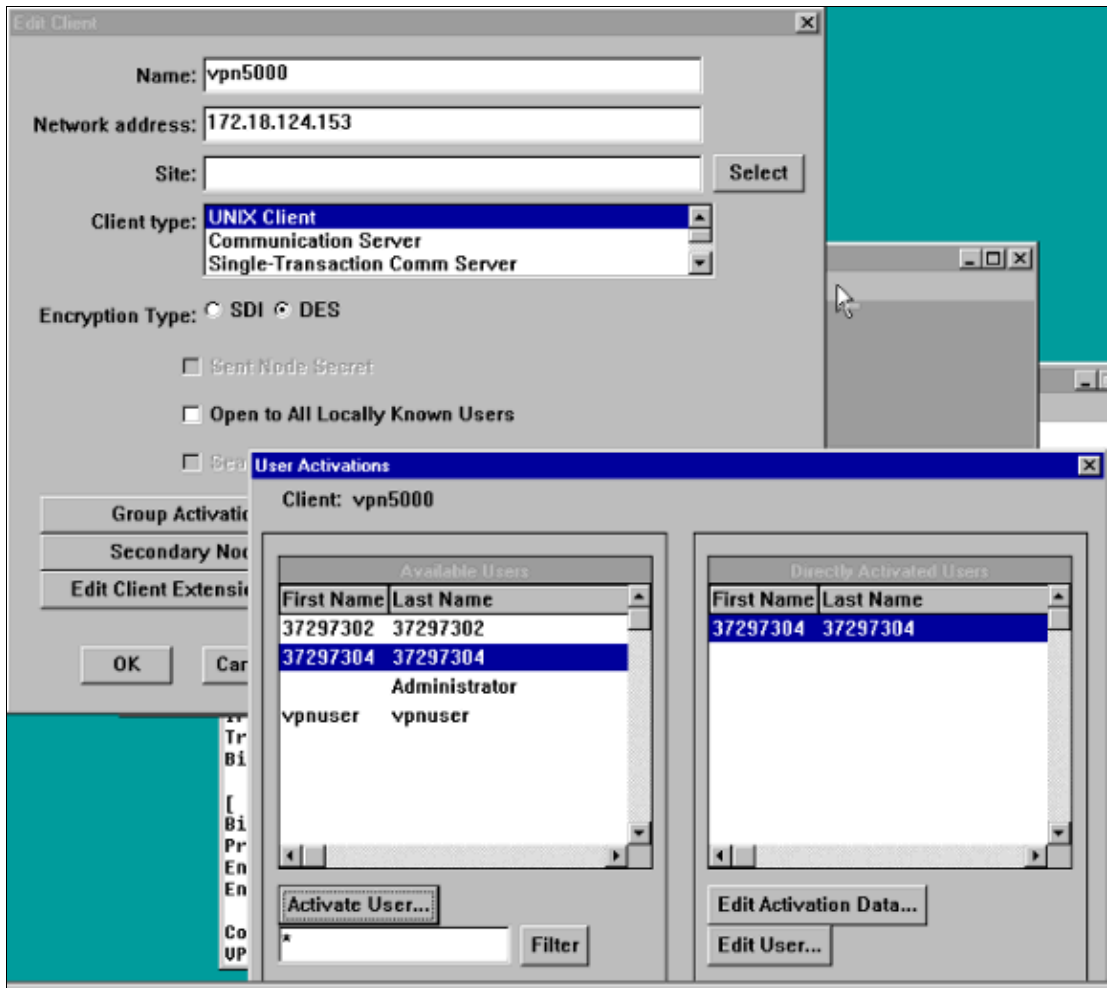
```

reset securid secret all
apply
write

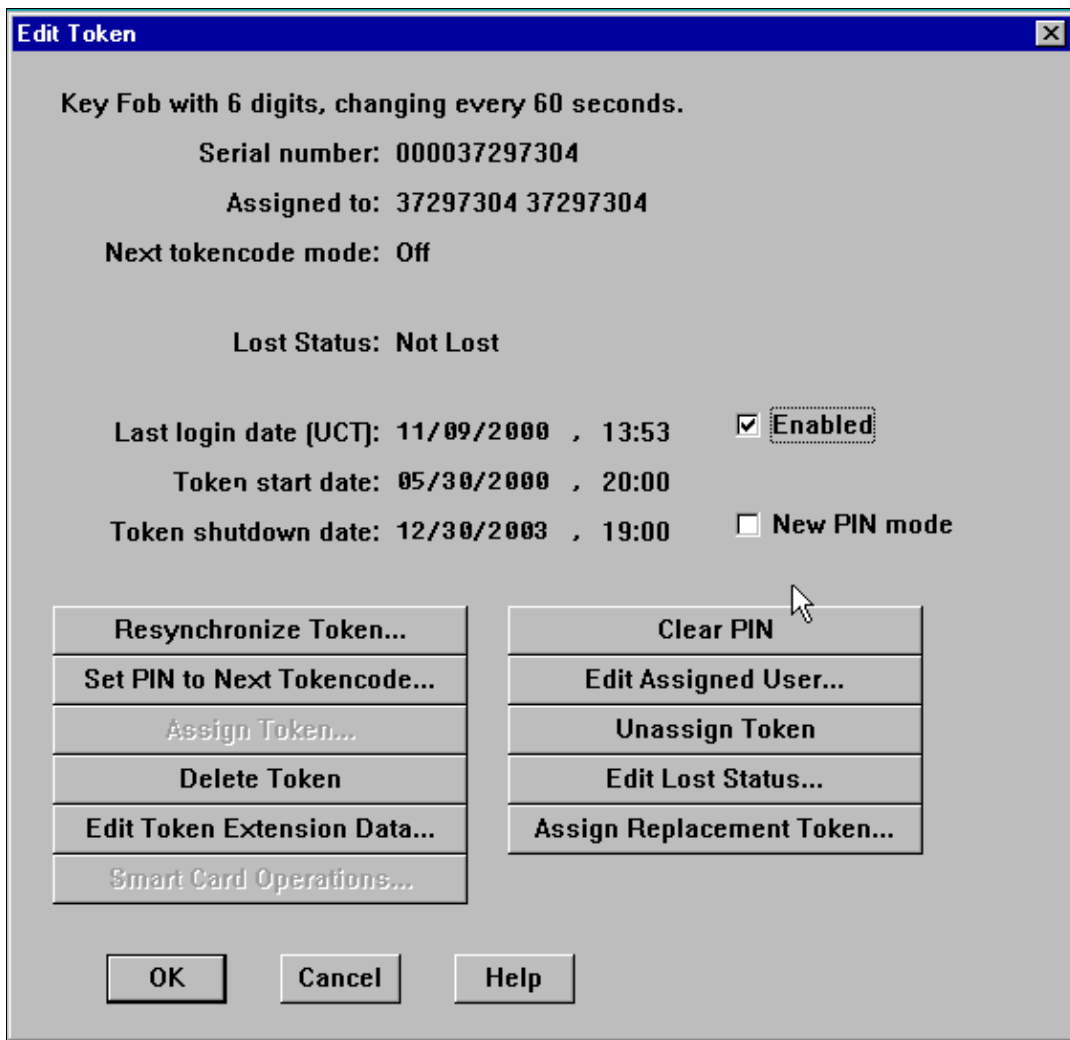
```

This removes the node-secret file on the VPN 5000, if one exists.

2. Configure the SDI server to speak to the Concentrator in the Client Configuration screen.



3. Click **Set PIN to Next Tokencode**. Select the **Enabled** check box, and then click **Resynchronize Token**.



4. Verify that the token is assigned to the user and the VPN 5000 is in the **Client Activations**.

Edit User [X]

First and last name:

Default login:

Default shell:

Local User Remote User

| Serial Number | Type | Status |
|---------------|---------|---------|
| 000037297304 | Key Fob | Enabled |

0: Original token R: Replacement for previous token

Role: <none>

Assigned Profile:

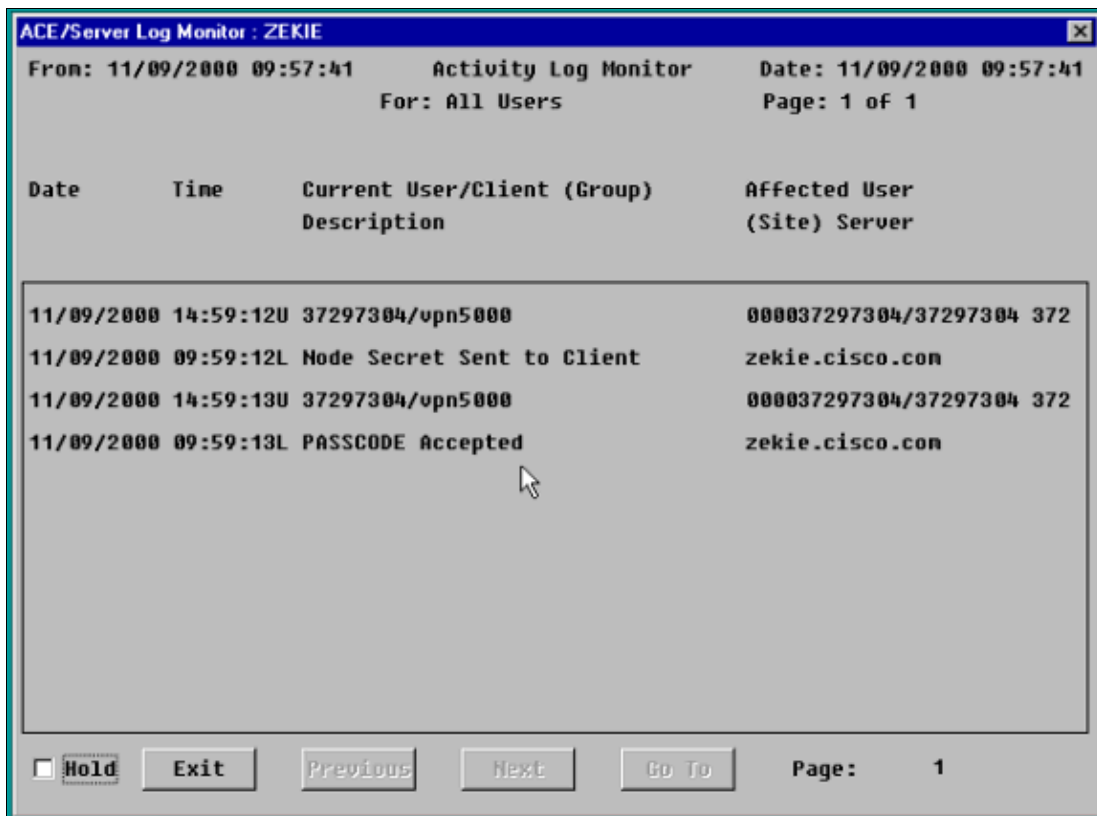
Temporary user
 Start date: 12/31/1985 , 19:00 End date: 12/31/1985 , 19:00

Allowed to create a PIN Required to create a PIN

| | | |
|-----------------------------|---------------------------|-----------------------------|
| Assign Token... | Edit Assigned Token... | Administrative Role... |
| Group Memberships... | Client Activations... | Edit User Extension Data... |
| Set/Change User Password... | Remove User Password | Edit Access Times... |
| Assign Profile... | Remove Profile Assignment | Delete User |

OK Cancel Apply L/S Changes Set All L/S Help

5. View the Log Monitor screen to debug transactions.



Note: The **Node Secret Sent to Client** message is displayed only at the time of first authentication/communication with the VPN 5000. Subsequent successes should only show **PASSCODE Accepted**.

Verify

This section provides information you can use to confirm your configuration is working properly.

SDI Log

```
11/13/2000 14:59:34U 37297304/vpn5000 000037297304/3727304 372
11/13/2000 09:59:34L PASSCODE Accepted zekie.cisco.com
```

VPN 5000

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **show sys log buffer**

```
show sys log buffer
```

```
!--- These were two different users.
```

```
Notice 115.42 seconds New IKE connection: [181.44.17.149]:1062:catchall
Info 135.24 seconds SecurID access request from 37297304 (catchall) granted
Notice 135.26 seconds VPN 0 opened for catchall from 181.44.17.149.
Debug 135.29 seconds Client's local broadcast address = 181.44.17.255
```

```

Notice    135.32 seconds User assigned IP address 172.18.124.250

Notice    234.6 seconds New IKE connection: [181.44.17.149]:1064:vpnuser
Info      248.0 seconds SecurID access request from vpnuser granted
Notice    248.2 seconds VPN 0 opened for vpnuser from 181.44.17.149.
Debug     248.4 seconds Client's local broadcast address = 181.44.17.255
Notice    248.8 seconds User assigned IP address 172.18.124.248

```

• **vpn trace dump all**

```
vpn trace dump all
```

```
!--- This was for user catchall.
```

```

6 seconds -- stepmngtr trace enabled --
  new script: ISAKMP primary responder script for (start)
manage @ 115 seconds :: [181.44.17.149]:1062 (start)
  115 seconds doing irpri_new_conn, (0 @ 0)
  115 seconds doing irpri_pkt_1_recvd, (0 @ 0)
  new script: ISAKMP Resp Aggr Shared Secret script for [181.44.17.149]:1062
(start)
  115 seconds doing irsass_process_pkt_1, (0 @ 0)
  115 seconds doing irsass_build_pkt_2, (0 @ 0)
  115 seconds doing irsass_send_pkt_2, (0 @ 0)
manage @ 115 seconds :: [181.44.17.149]:1062 (done)
manage @ 116 seconds :: [181.44.17.149]:1062:catchall (start)
  116 seconds doing irsass_check_timeout, (0 @ 0)
  116 seconds doing irsass_check_hash, (0 @ 0)
  116 seconds doing irsass_last_op, (0 @ 0)
  end script: ISAKMP Resp Aggr Shared Secret script for [181.44.17.149]:1062:
catchall, (0 @ 0)
  next script: ISAKMP primary responder script for [181.44.17.149]:1062:catchal
l, (0 @ 0)
  116 seconds doing irpri_phase1_done, (0 @ 0)
  116 seconds doing irpri_phase1_done, (0 @ 0)
  new script: SecurID initiator for [181.44.17.149]:1062:catchall (start)
  116 seconds doing start_securid, (0 @ 0)
manage @ 116 seconds :: [181.44.17.149]:1062:catchall (done)
manage @ 126 seconds :: [181.44.17.149]:1062:catchall (start)
  126 seconds doing rpkt_getusername, (0 @ 0)
  126 seconds doing send_challenge, (0 @ 0)
manage @ 126 seconds :: [181.44.17.149]:1062:catchall (done)
manage @ 134 seconds :: [181.44.17.149]:1062:catchall (start)
  134 seconds doing rpkt_sid_check, (0 @ 0)
manage @ 134 seconds :: [181.44.17.149]:1062:catchall (done)
manage @ 135 seconds :: [181.44.17.149]:1062:catchall (start)
  135 seconds doing recv_ace_msg, (0 @ 0)
  135 seconds doing send_access, (0 @ 0)
  135 seconds doing isid_last_op, (0 @ 0)
  end script: SecurID initiator for [181.44.17.149]:1062:catchall, (0 @ 0)
  next script: ISAKMP primary responder script for [181.44.17.149]:1062:catchal
l, (0 @ 0)
  135 seconds doing irpri_phase1_done, (0 @ 0)
135 seconds doing irpri_start_phase2, (0 @ 0)
  new script: phase 2 initiator for [181.44.17.149]:1062:catchall (start)
  135 seconds doing iph2_init, (0 @ 0)
  135 seconds doing iph2_build_pkt_1, (0 @ 0)
  135 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 135 seconds :: [181.44.17.149]:1062:catchall (done)
manage @ 135 seconds :: [181.44.17.149]:1062:catchall (start)
  135 seconds doing iph2_pkt_2_wait, (0 @ 0)
  135 seconds doing ihp2_process_pkt_2, (0 @ 0)
  135 seconds doing iph2_build_pkt_3, (0 @ 0)
  135 seconds doing iph2_config_SAs, (0 @ 0)

```

```
135 seconds doing iph2_send_pkt_3, (0 @ 0)
135 seconds doing iph2_last_op, (0 @ 0)
end script: phase 2 initiator for [181.44.17.149]:1062:catchall, (0 @ 0)
next script: ISAKMP primary responder script for [181.44.17.149]:1062:catchal
1, (0 @ 0)
135 seconds doing irpri_open_tunnel, (0 @ 0)
135 seconds doing irpri_start_i_maint, (0 @ 0)
new script: initiator maintenance for [181.44.17.149]:1062:catchall (start)
135 seconds doing imnt_init, (0 @ 0)
manage @ 135 seconds :: [181.44.17.149]:1062:catchall (done)
```

Troubleshoot

Note: Before issuing **debug** commands, refer to Important Information on Debug Commands.

Node Verification Failed

Before initial communication with the VPN 5000 Concentrator, the **Sent Node Secret** box in the SDI client configuration is unchecked and the 5000 should not have a *node secret*. Certain conditions, including an IP address change of the 5000 or SDI server, cause the Node Verification Failed error. To get rid of this error, issue these commands on the VPN 5000:

```
reset securid secret all
apply
write
```

On the SDI server, uncheck **Sent Node Secret** in the SDI client configuration. The node secret is re-sent at the time of first authentication.

VPN 5000 debug:

```
Notice 2467137.32 seconds -- reason: S_SECURID_FAILURE (254@2318)
```

SDI Log:

```
11/13/2000 14:04:06U -----/vpn5000 ---->/
11/13/2000 09:04:06L Node Verification Failed zekie.cisco.com
```

Server Unreachable

VPN 5000 debug:

```
Notice 247488.32 seconds -- reason: S_SECURID_FAILURE (254@2318)
```

SDI Log:

No indication that the request arrived.

What the user sees:

```
IKE ERROR: SecurID Authentication Failed.
```

Bad Username on VPN 5000

VPN 5000 Debug:

```
Notice 250157.18 seconds New IKE connection: [181.44.17.149]:1039:junkuser
Notice 250157.20 seconds Invalid user configuration for junkuser
Notice 250157.22 seconds no <ifp> (junkuser) reset -- user is unknown/invalid.
```

SDI Log:

Shows nothing because the VPN 5000 does not forward.

What the user sees:

```
VPN Server Error (6): Bad user configuration on IntraPort server.
```

Bad Username/Token on SDI

VPN 5000 Debug:

```
Notice 250280.20 seconds -- reason: S_SECURID_FAILURE (254@2318)
```

SDI Log:

```
user non-existent:
11/13/2000 15:03:09U notonsdi/vpn5000 ---->/
11/13/2000 10:03:09L User Not on Client zekie.cisco.com
passcode bad:
11/13/2000 15:08:54U 37297304/vpn50000 000037297304/37297304 372
11/13/2000 10:08:54L ACCESS DENIED< PASSCODE Incorrect zekie.cisco.com
```

What the user sees:

```
IKE ERROR: SecurID Authentication Failed
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

| |
|---|
| NetPro Discussion Forums – Featured Conversations for VPN |
| Service Providers: VPN Service Architectures |
| Service Providers: Network Management |
| Virtual Private Networks: General |

Related Information

- [Cisco VPN 5000 Series Concentrators End-of-Sales Announcement](#)
- [Cisco VPN 5000 Concentrator Support Page](#)
- [Cisco VPN 5000 Client Support Page](#)

- **IPSec Support Page**
 - **Technical Support – Cisco Systems**
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 23, 2007

Document ID: 10134
