

# Configuring the VPN 3000 Concentrator to Communicate with the VPN Client Using Certificates

Document ID: 4102

---

**Introduction**

**Prerequisites**

Requirements

Components Used

Conventions

**VPN 3000 Concentrator Certificates for VPN Clients**

**Verify**

**Troubleshoot**

**Related Information**

---

## Introduction

This document includes step-by-step instructions on how to configure the Cisco VPN 3000 Series Concentrators with VPN Clients with the use of certificates.

## Prerequisites

### Requirements

There are no specific requirements for this document.

### Components Used

The information in this document is based on Cisco VPN 3000 Concentrator software version 4.0.4A.

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## VPN 3000 Concentrator Certificates for VPN Clients

Complete these steps in order to configure VPN 3000 Concentrator certificates for VPN Clients.

1. The IKE policy must be configured to use certificates on the VPN 3000 Concentrator Series Manager. In order to configure the IKE policy, select **Configuration > System > Tunneling Protocols > IPsec > IKE Proposals**, and move **CiscoVPNClient-3DES-MD5-RSA** to the Active Proposals.

Configuration | System | Tunneling Protocols | IPsec | IKE Proposals Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate. Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority. Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by [Security Associations](#) to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
<ul style="list-style-type: none"> <li>CiscoVPNClient-3DES-MD5-RSA</li> <li>CiscoVPNClient-3DES-MD5</li> <li>IKE-3DES-MD5</li> <li>IKE-3DES-MD5-DH1</li> <li>IKE-DES-MD5</li> <li>IKE-3DES-MD5-DH7</li> <li>IKE-3DES-MD5-RSA</li> <li>CiscoVPNClient-3DES-MD5-DH5</li> <li>CiscoVPNClient-AES128-SHA</li> <li>IKE-AES128-SHA</li> </ul>	<ul style="list-style-type: none"> <li>&lt;&lt; Activate</li> <li>Deactivate &gt;&gt;</li> <li>Move Up</li> <li>Move Down</li> <li>Add</li> <li>Modify</li> <li>Copy</li> <li>Delete</li> </ul>	<ul style="list-style-type: none"> <li>IKE-3DES-SHA-DSA</li> <li>IKE-3DES-MD5-RSA-DH1</li> <li>IKE-DES-MD5-DH7</li> <li>CiscoVPNClient-3DES-SHA-DSA</li> <li>CiscoVPNClient-3DES-MD5-RSA-DH5</li> <li>CiscoVPNClient-3DES-SHA-DSA-DH5</li> <li>CiscoVPNClient-AES256-SHA</li> <li>IKE-AES256-SHA</li> </ul>

- You must also configure the IPsec policy to use certificates. Select **Configuration > Policy Management > Traffic Management > Security Associations**, highlight **ESP-3DES-MD5** and then click **Modify** to configure the IPsec policy to configure the IPsec policy.

Configuration | Policy Management | Traffic Management | Security Associations Save Needed

This section lets you add, configure, modify, and delete IPsec Security Associations (SAs). Security Associations use [IKE Proposals](#) to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPsec SAs	Actions
<ul style="list-style-type: none"> <li>ESP-3DES-MD5</li> <li>ESP-3DES-MD5-DH5</li> <li>ESP-3DES-MD5-DH7</li> <li>ESP-3DES-NONE</li> <li>ESP-AES128-SHA</li> <li>ESP-DES-MD5</li> <li>ESP-L2TP-TRANSPORT</li> <li>ESP/IKE-3DES-MD5</li> </ul>	<ul style="list-style-type: none"> <li>Add</li> <li>Modify</li> <li>Delete</li> </ul>

- On the Modify window, under Digital Certificates, make sure to select your installed identity certificate. Under IKE Proposal, select **CiscoVPNClient-3DES-MD5-RSA** and click **Apply**.

Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

SA Name  Specify the name of this Security Association (SA).

Inheritance  Select the granularity of this SA.

---

**IPSec Parameters**

Authentication Algorithm  Select the packet authentication algorithm to use.

Encryption Algorithm  Select the ESP encryption algorithm to use.

Encapsulation Mode  Select the Encapsulation Mode for this SA.

Perfect Forward Security  Select the use of Perfect Forward Security.

Lifetime Measurement  Select the lifetime measurement of the IPSec keys.

Data Lifetime  Specify the data lifetime in kilobytes (KB).

Time Lifetime  Specify the time lifetime in seconds.

---

**IKE Parameters**

IKE Peer  Specify the IKE Peer for a LAN-to-LAN IPSec connection.

Negotiation Mode  Select the IKE Negotiation mode to use.

Digital Certificate  Select the Digital Certificate to use.

Certificate Transmission  Entire certificate chain  
 Identity certificate only Choose how to send the digital certificate to the IKE peer.

IKE Proposal  Select the IKE Proposal to use as IKE initiator.

- In order to configure an IPsec group, select **Configuration > User Management > Groups > Add**, add a group called **IPSECCERT** (the IPSECCERT group name matches the Organizational Unit (OU) in the identity certificate), and select a password.

This password is not used anywhere if you use certificates. In this example, "cisco123" is the password.

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

**Identity** | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Group Name	<input type="text" value="IPSECCERT"/>	Enter a unique name for the group.
Password	<input type="password" value=""/>	Enter the password for the group.
Verify	<input type="password" value=""/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

- On the same page, click the General tab and make sure that you select **IPsec** as the Tunneling Protocol.

Identity   General   IPsec   Client Config   Client FW   HW Client   PPTP/L2TP			
General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	--None--	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS		<input checked="" type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input type="checkbox"/>	Select the tunneling protocols this group can connect with.

6. Click the IPsec tab and make sure that your configured IPsec Security Association (SA) is selected under IPsec SA and click **Apply**.

Identity   General   IPsec   Client Config   Client FW   HW Client   PPTP/L2TP			
IPsec Parameters			
Attribute	Value	Inherit?	Description
IPsec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPsec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to idle before the VPN Concentrator checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to <b>Individual User Authentication</b> .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorization in addition to authentication, select an authorization method. If you configure this field, you must also configure an Authorization Server.
Authorization Required	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
DN Field	CN otherwise OU	<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.

<b>Authorization Required</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require successful authorization.
<b>DN Field</b>	CN otherwise OU	<input checked="" type="checkbox"/>	For certificate-based users, select the subject Distinguished Name (DN) field that is used as the username. This field is used for user Authorization.
<b>IPComp</b>	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
<b>Reauthentication on Rekey</b>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
<b>Mode Configuration</b>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

Add Cancel

7. In order to configure an IPsec group on the VPN 3000 Concentrator, select **Configuration > User Management > Users > Add**, specify a User Name, Password, and the Group name, and then click **Add**.

In the example, these fields are used:

- ◆ User Name = cert\_user
- ◆ Password = cisco123
- ◆ Verify = cisco123
- ◆ Group = IPSECCERT

Configuration | User Management | Users | Add

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

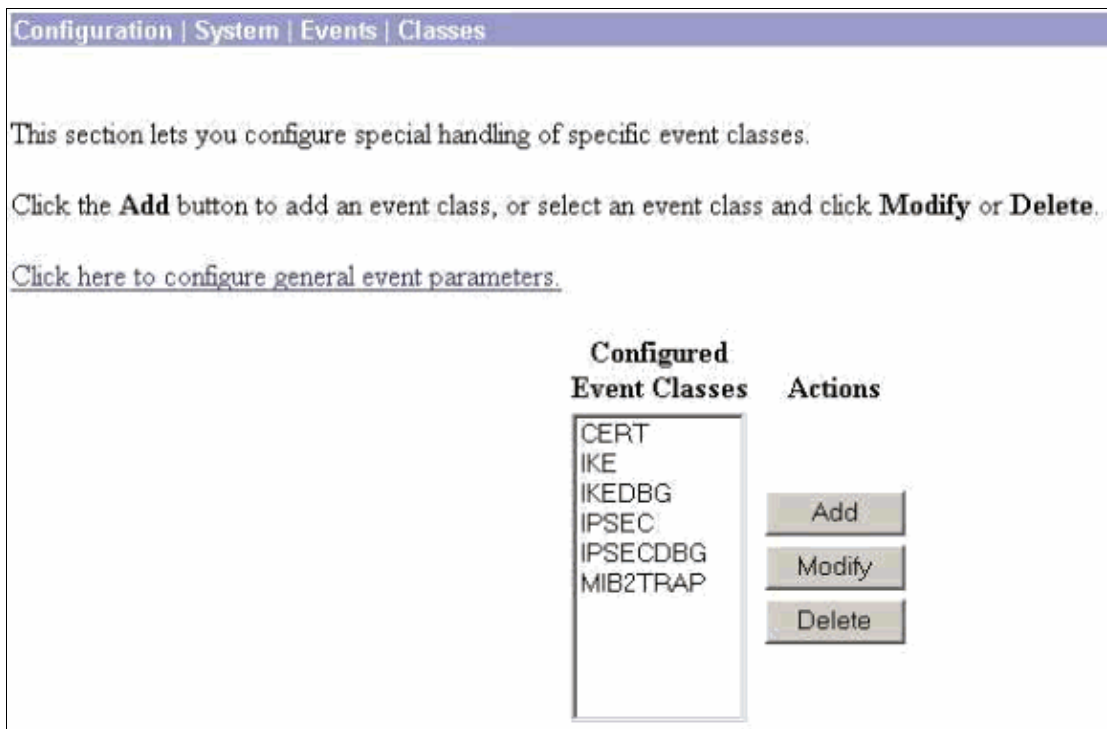
Identity General IPsec PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Username	cert_user	Enter a unique username.
Password	XXXXXXXXXX	Enter the user's password. The password must satisfy the group password requirements.
Verify	XXXXXXXXXX	Verify the user's password.
Group	IPSECCERT	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

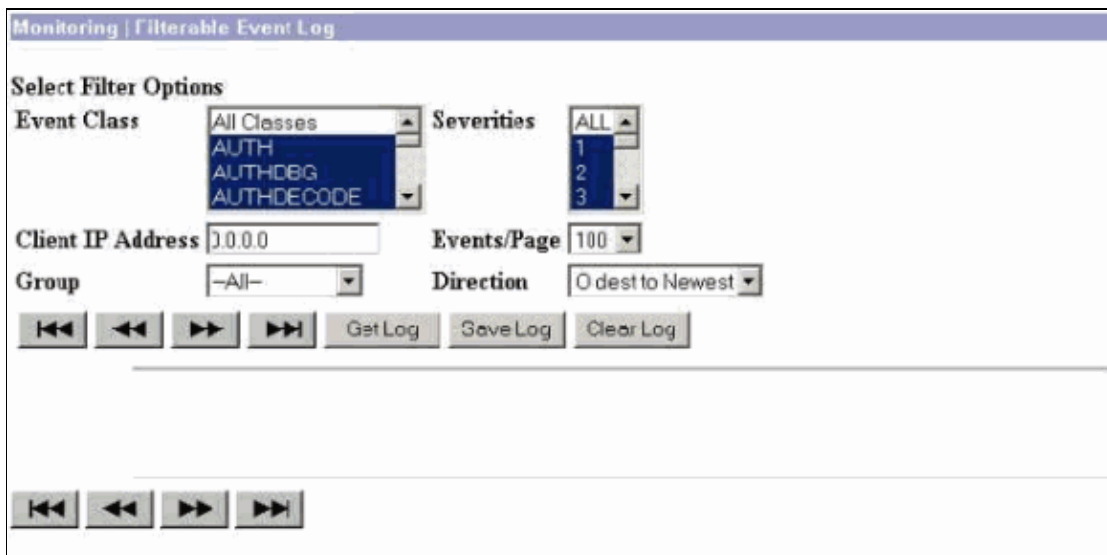
Add Cancel

8. In order to enable debugging on the VPN 3000 Concentrator select **Configuration > System > Events > Classes** and add these classes:

- ◆ CERT 1–13
- ◆ IKE 1–6
- ◆ IKEDBG 1–10
- ◆ IPSEC 1–6
- ◆ IPSECCDBG 1–10



9. Select **Monitoring > Filterable Event Log** in order to view the debugs.



**Note:** If you decide to change the IP addresses, you can make an enrollment of the new IP addresses and install the issued certificate later with those new addresses.

## Verify

There is currently no verification procedure available for this configuration.

## Troubleshoot

Refer to Troubleshooting Connection Problems on the VPN 3000 Concentrator for further troubleshooting information.

## Related Information

- **Cisco VPN 3000 Series Concentrators**
  - **Cisco VPN 3002 Hardware Clients**
  - **IPsec Negotiation/IKE Protocols**
  - **Technical Support & Documentation – Cisco Systems**
- 

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Apr 24, 2006

Document ID: 4102

---