

# 認証を使用した VPN クライアントと通信するための VPN 3000 コンセントレータの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[VPN クライアントのVPN 3000 Concentrator 証明](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、証明書を使用した Cisco VPN 3000 シリーズ コンセントレータと VPN クライアントの設定方法の段階的な手順について説明します。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Cisco VPN 3000 コンセントレータソフトウェアバージョン 4.0.4A に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

### 表記法

ドキュメント表記の詳細については、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

# VPN クライアントのVPN 3000 Concentrator 証明

VPN ClientのVPN 3000コンセントレータ証明書を設定するには、次の手順を実行します。

1. VPN 3000コンセントレータシリーズマネージャで証明書を使用するようにIKEポリシーを設定する必要があります。IKEポリシーを設定するには、[Configuration] > [System] > [Tunneling Protocols] > [IPsec] > [IKE Proposals] の順に選択し、CiscoVPNClient-3DES-MD5-RSAを[Active Proposals]に移動します。

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
CiscoVPNClient-3DES-MD5-RSA	<< Activate	IKE-3DES-SHA-DSA
CiscoVPNClient-3DES-MD5	Deactivate >>	IKE-3DES-MD5-RSA-DH1
IKE-3DES-MD5	Move Up	IKE-DES-MD5-DH7
IKE-3DES-MD5-DH1	Move Down	CiscoVPNClient-3DES-SHA-DSA
IKE-DES-MD5	Add	CiscoVPNClient-3DES-MD5-RSA-DH5
IKE-3DES-MD5-DH7	Modify	CiscoVPNClient-3DES-SHA-DSA-DH5
IKE-3DES-MD5-RSA	Copy	CiscoVPNClient-AES256-SHA
CiscoVPNClient-3DES-MD5-DH5	Delete	IKE-AES256-SHA
CiscoVPNClient-AES128-SHA		
IKE-AES128-SHA		

2. 証明書を使用するようにIPsecポリシーを設定する必要もあります。[Configuration] > [Policy Management] > [Traffic Management] > [Security Associations]を選択し、ESP-3DES-MD5を強調表示し、[Modify]をクリックしてIPSecポリシーを設定します。

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
ESP-3DES-MD5	Add
ESP-3DES-MD5-DH5	Modify
ESP-3DES-MD5-DH7	Delete
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	

3. [Modify]ウィンドウの[Digital Certificates]で、インストールされているID証明書を選択します。[IKE Proposal]で[CiscoVPNClient-3DES-MD5-RSA]を選択し、[Apply]をクリックします。

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 Secrecy  Select the use of Perfect Forward Secrecy.

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.

4. IPsecグループを設定するには、[Configuration] > [User Management] > [Groups] > [Add] を選択し、ID証明書のOrganizational Unit(OU)に一致するIPSECCERTグループ名を追加して、パスワードを選択します。証明書を使用している場合、このパスワードは使用されません。この例では、「cisco123」がパスワードです。

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="text" value="*****"/>	Enter the password for the group.
Verify	<input type="text" value="*****"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

5. 同じページで、[General]タブをクリックし、トンネリングプロトコルとして[IPsec]を選択していることを確認します。

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. [IPsec]タブをクリックし、[IPsec SA]で設定済みのIPsec Security Association (SA)が選択されていることを確認し、[Apply]をクリックします。

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.
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.
IPComp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	<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.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>			

7. VPN 3000コンソントレータでIPsecグループを設定するには、[Configuration] > [User Management] > [Users] > [Add]の順に選択し、ユーザ名、パスワード、およびグループ名を指定し、[Add]をクリックします。この例では、次のフィールドを使用します。ユーザ名=cert\_userパスワード：cisco123確認=cisco123グループ=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. VPN 3000コンソントレータでデバッグを有効にするには、**Configuration > System > Events > Classes**の順に選択し、次のクラスを追加します。CERT 1-13IKE 1-6IKEDBG 1-10IPSEC 1-6IPSECDBG 1-10

Configuration | System | Events | Classes

This section lets you configure special handling of specific event classes.

Click the **Add** button to add an event class, or select an event class and click **Modify** or **Delete**.

[Click here to configure general event parameters.](#)

Configured Event Classes	Actions
CERT IKE IKEDBG IPSEC IPSECDBG MIB2TRAP	Add Modify Delete

9. [Monitoring] > [Filterable Event Log] を選択して、デバッグを表示します。

注：IPアドレスを変更する場合は、新しいIPアドレスを登録し、発行された証明書を後で新しいアドレスにインストールできます。

## 確認

現在、この設定に使用できる確認手順はありません。

## トラブルシューティング

トラブルシューティングの詳細については、[『VPN 3000コンセントレータの接続に関する問題のトラブルシューティング』](#)を参照してください。

## 関連情報

- [Cisco VPN 3000 シリーズ コンセントレータ](#)
- [Cisco VPN 3002 Hardware Client](#)
- [IPSec ネゴシエーション/IKE プロトコル](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)