

인증서를 사용하여 VPN 클라이언트와 통신하도록 VPN 3000 Concentrator 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[VPN 클라이언트용 VPN 3000 Concentrator 인증서](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에는 인증서를 사용하여 VPN 클라이언트를 사용하여 Cisco VPN 3000 Series Concentrator를 구성하는 방법에 대한 단계별 지침이 포함되어 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco VPN 3000 Concentrator 소프트웨어 버전 4.0.4A를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

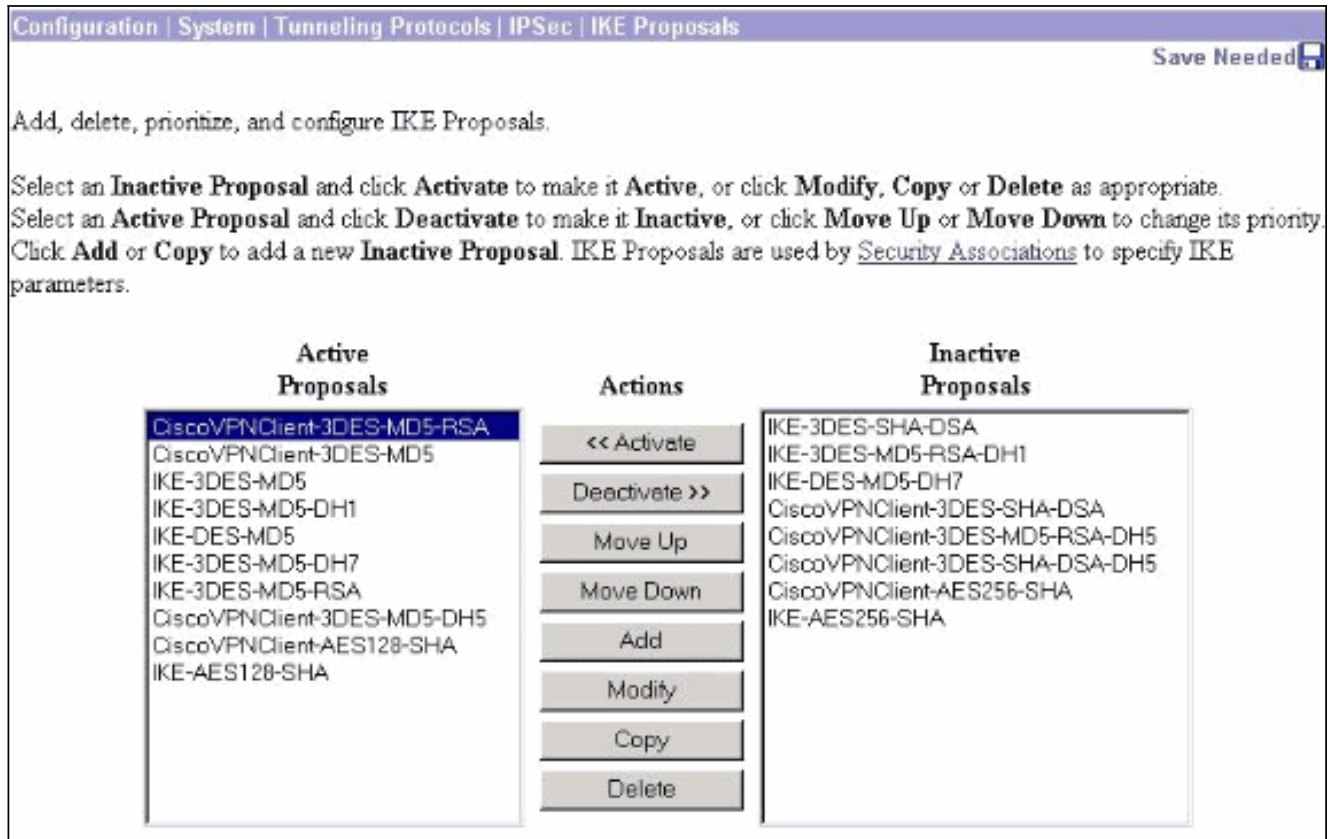
표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

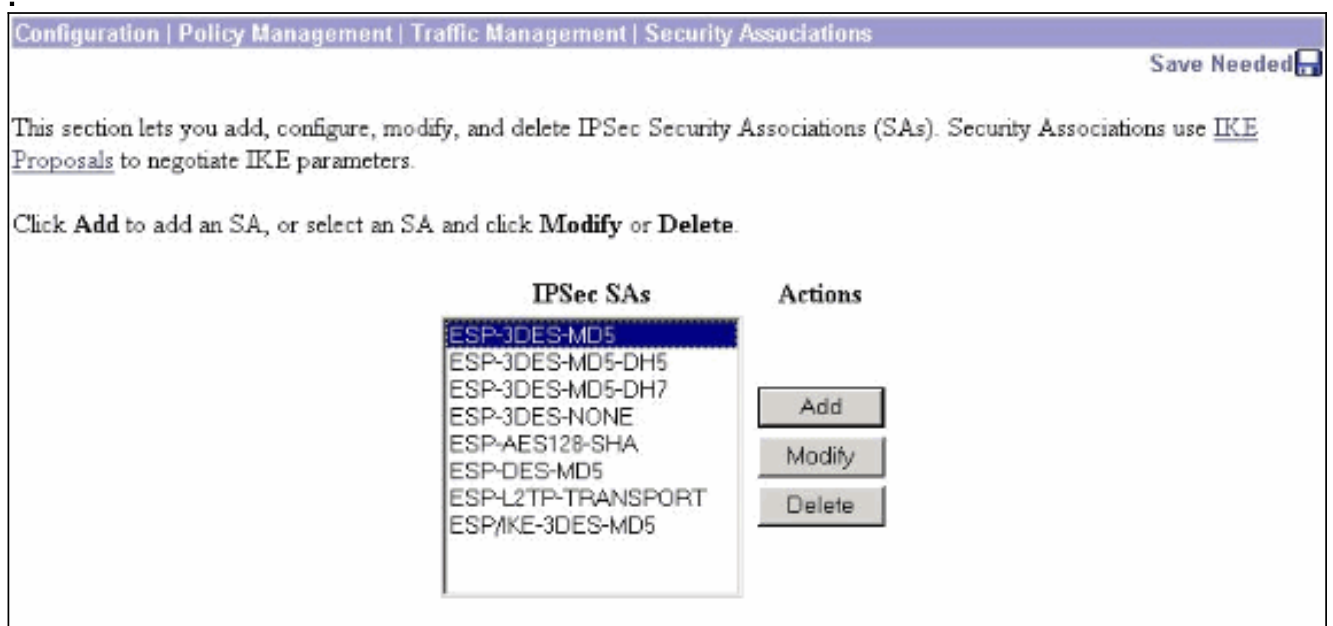
VPN 클라이언트용 VPN 3000 Concentrator 인증서

VPN 클라이언트에 대한 VPN 3000 Concentrator 인증서를 구성하려면 다음 단계를 완료하십시오.

- VPN 3000 Concentrator Series Manager에서 인증서를 사용하도록 IKE 정책을 구성해야 합니다. IKE 정책을 구성하려면 **Configuration(구성) > System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPsec > IKE Proposals(IKE 제안)**를 선택하고 **CiscoVPNClient-3DES-MD5-RSA**를 **Active Proposals**로 이동합니다



- 또한 인증서를 사용하도록 IPsec 정책을 구성해야 합니다. **Configuration(구성) > Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Security Associations(보안 연결)**를 선택하고 **ESP-3DES-MD5**를 선택한 다음 **Modify(수정)**를 클릭하여 IPsec 정책을 구성하여 IPsec 정책을 구성합니다



- Modify(수정)** 창의 **Digital Certificates(디지털 인증서)**에서 설치된 ID 인증서를 선택해야 합니다. IKE Proposal(IKE 제안)에서 **CiscoVPNClient-3DES-MD5-RSA**를 선택하고 **Apply(적용)**를 클릭합니다

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 그룹을 구성하려면 Configuration > User Management > Groups > Add를 선택하고 IPSECCERT라는 그룹을 추가합니다(IPSECCERT 그룹 이름이 ID 인증서의 OU(조직 단위)와 일치). 암호를 선택합니다.인증서를 사용하는 경우 이 비밀번호는 사용되지 않습니다. 이 예에서 "cisco123"은 비밀번호입니다

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="cisco123"/>	Enter the password for the group.
Verify	<input type="text" value="cisco123"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

5. 같은 페이지에서 General(일반) 탭을 클릭하고 IPsec을 Tunneling Protocol(터널링 프로토콜)으로 선택해야 합니다

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 탭을 클릭하고 IPsec SA 아래에서 구성된 IPsec SA(Security Association)가 선택되었는지 확인하고 Apply(적용)를 클릭합니다

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 Individual User Authentication .
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 Concentrator에서 IPsec 그룹을 구성하려면 **Configuration > User Management > Users > Add**를 선택하고 사용자 이름, 암호 및 그룹 이름을 지정한 다음 Add를 클릭합니다.이 예에서는 다음 필드가 사용됩니다. 사용자 이름 = cert_user비밀번호 = cisco123확인 = cisco123그룹 = 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 Concentrator에서 디버깅을 활성화하려면 **Configuration > System > Events > Classes**를 선택하고 다음 클래스를 추가합니다.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. 디버그를 보려면 > **Filterable Event Log**를 선택합니다

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes (dropdown menu with options: AUTH, AUTHDBG, AUTHDECODE)

Severities: ALL (dropdown menu with options: 1, 2, 3)

Client IP Address: 0.0.0.0

Events/Page: 100

Group: -All-

Direction: 0 dest to Newest

Buttons: <<<, <<, >>, >>>, Get Log, Save Log, Clear Log

Buttons: <<<, <<, >>, >>>

참고: IP 주소를 변경하려는 경우 새 IP 주소를 등록하고 발급된 인증서를 나중에 새 주소로 설치할 수 있습니다.

[다음을 확인합니다.](#)

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

[문제 해결](#)

자세한 문제 [해결 정보는 VPN 3000 Concentrator의 연결 문제 해결](#)을 참조하십시오.

[관련 정보](#)

- [Cisco VPN 3000 Series Concentrator](#)
- [Cisco VPN 3002 하드웨어 클라이언트](#)
- [IPSec 협상/IKE 프로토콜](#)
- [기술 지원 및 문서 - Cisco Systems](#)