

De VPN 3000 Concentrator configureren om met de VPN-client te communiceren met behulp van certificaten

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[VPN 3000 Concentrator-certificaten voor VPN-clients](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document bevat stap-voor-stap instructies over de manier waarop u Cisco VPN 3000 Series Concentrators met VPN-clients kunt configureren met gebruik van certificaten.

[Voorwaarden](#)

[Vereisten](#)

Er zijn geen specifieke vereisten van toepassing op dit document.

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op Cisco VPN 3000 Concentrator softwareversie 4.0.4A.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

[Conventies](#)

Raadpleeg de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

VPN 3000 Concentrator-certificaten voor VPN-clients

Voltooi deze stappen om VPN 3000 Concentrator-certificaten voor VPN-clients te configureren.

1. Het IKE-beleid moet worden geconfigureerd om certificaten te gebruiken in VPN 3000 Concentrator Series Manager. Om het IKE-beleid te configureren selecteert u **Configuration > System > Tunneling Protocols > IPsec > IKE-voorstellen** en zet **Cisco VPN-client-3DES-MD5-RSA** in op de actieve voorstellen.

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. U moet ook het IPsec-beleid configureren om certificaten te gebruiken. Selecteer **Configuration > Policy Management > Traffic Management > Security Associations**, toets **ESP-3DES-MD5** en klik vervolgens op **Wijzigen** om het IPsec-beleid te configureren om het IPsec-beleid te configureren.

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	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
ESP-3DES-MD5-DH5	
ESP-3DES-MD5-DH7	
ESP-3DES-NONE	
ESP-AES128-SHA	
ESP-DES-MD5	
ESP-L2TP-TRANSPORT	
ESP/IKE-3DES-MD5	

3. Zorg er in het venster Wijzigen onder Digitale Certificaten voor dat u het geïnstalleerde identiteitsbewijs selecteert. Selecteer onder IKE Proposal Cisco VPN,client-3DES-MD5-RSA en klik op **Toepassen**.

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. Om een IPsec-groep te configureren selecteert u **Configuration > User Management > Group > Add**, voegt u een groep IPSECCERT (de IPSECCERT-groepsnaam komt overeen met de Organisatorische eenheid (OU) in het identiteitsbewijs) en selecteert u een wachtwoord. Dit wachtwoord wordt nergens gebruikt als u certificaten gebruikt. In dit voorbeeld is "cisco123" het wachtwoord.

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	IPSECCERT	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	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.

Add Cancel

5. Klik op het tabblad Algemeen en zorg ervoor dat u IPsec selecteert als het 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. Klik op het tabblad IPsec en zorg ervoor dat uw geconfigureerde IPsec Security Association (SA) is geselecteerd onder IPsec SA en klik op Toepassen.

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. Om een IPSec-groep te configureren in het VPN 3000-centrator, selecteert u **Configuration > User Management > Gebruikers > Add**, specificert u een gebruikersnaam, wachtwoord en de naam van de groep en vervolgens klikt u op **Add**. In het voorbeeld worden deze velden gebruikt: Gebruikersnaam = cert_user Wachtwoord = cisco123 Controleer = cisco123 Groep = 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. Zo selecteert u het foutoptreden op de VPN 3000 Concentrator **Configuration > System > Events > Classes** en voegt u deze klassen toe: 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	Add Modify Delete
IKE	
IKEDBG	
IPSEC	
IPSECDBG	
MIB2TRAP	

9. Selecteer **Monitoring > Filterable Event Log** om de beelden te bekijken.

Monitoring | Filterable Event Log

Select Filter Options

Event Class: All Classes, AUTH, AUTHDBG, AUTHDECODE

Severities: ALL, 1, 2, 3

Client IP Address: 0.0.0.0

Events/Page: 100

Group: -All-

Direction: 0 dest to Newest

Get Log, Save Log, Clear Log

N.B.: Als u de IP-adressen wilt wijzigen, kunt u de nieuwe IP-adressen inschrijven en het afgegeven certificaat later met deze nieuwe adressen installeren.

[Verifiëren](#)

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

[Problemen oplossen](#)

Raadpleeg [verbindingproblemen met probleemoplossing in de VPN 3000-concentratie](#) voor meer informatie over probleemoplossing.

[Gerelateerde informatie](#)

- [Cisco VPN 3000 Series Concentrators](#)
- [Cisco VPN 3002 hardwareclients](#)
- [IPsec-onderhandeling/IKE-protocollen](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)