

Configurazione di VPN 3000 Concentrator per comunicare con il client VPN utilizzando i certificati

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Certificati VPN 3000 Concentrator per client VPN](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento include istruzioni dettagliate su come configurare i Cisco VPN serie 3000 concentrator con client VPN con l'uso di certificati.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il software Cisco VPN 3000 Concentrator versione 4.0.4A.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

Certificati VPN 3000 Concentrator per client VPN

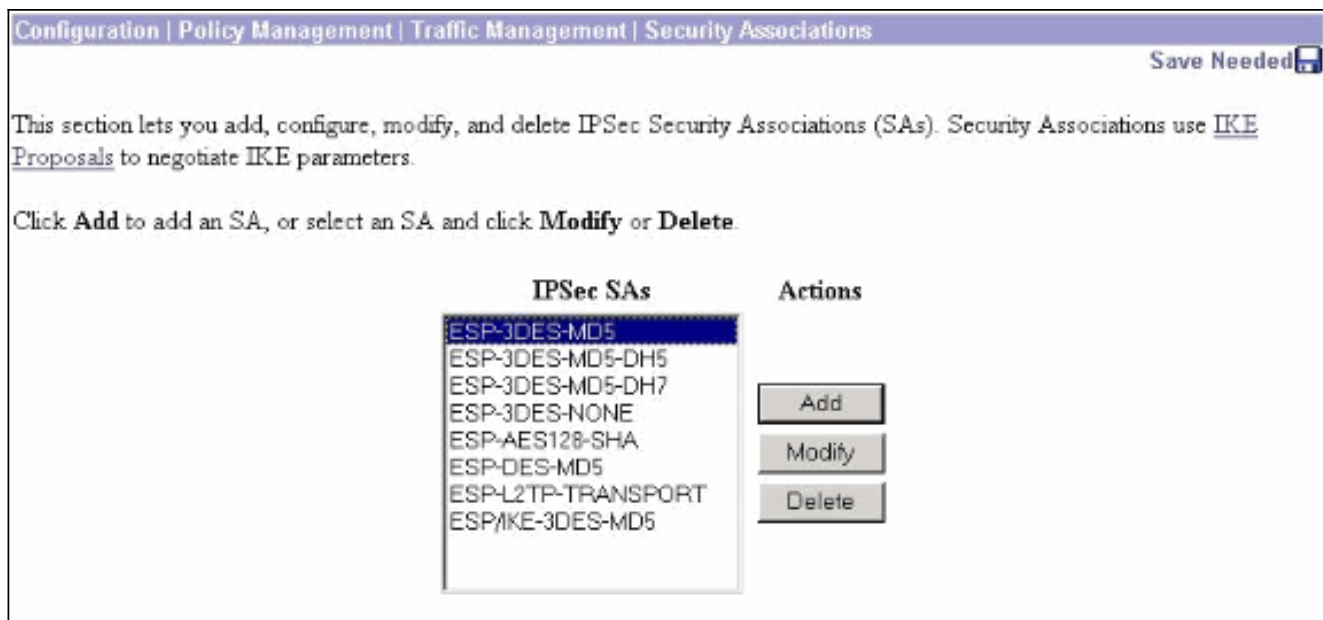
Completare questa procedura per configurare i certificati VPN 3000 Concentrator per i client VPN.

1. È necessario configurare il criterio IKE per l'utilizzo di certificati su VPN 3000 Concentrator Series Manager. Per configurare la policy IKE, selezionare Configurazione > Sistema > Protocolli di tunneling > IPsec > **Proposte IKE**, quindi spostare **CiscoVPNClient-3DES-MD5-RSA** nelle proposte attive.

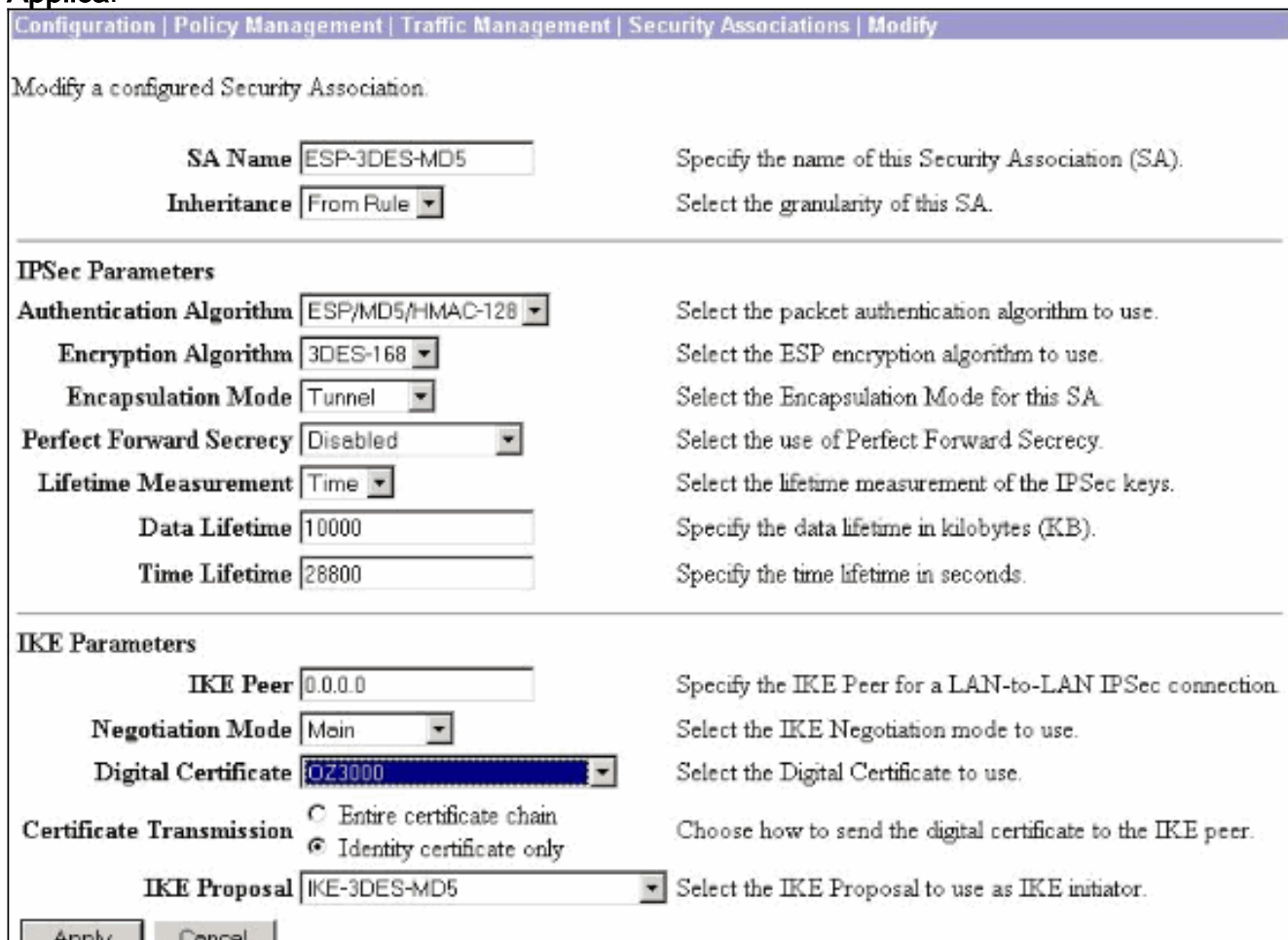
The screenshot shows the 'IKE Proposals' configuration page in the Cisco VPN 3000 Concentrator Series Manager. The breadcrumb trail is 'Configuration | System | Tunneling Protocols | IPsec | IKE Proposals'. A 'Save Needed' button is visible in the top right corner. Below the breadcrumb trail, there is a description: 'Add, delete, prioritize, and configure IKE Proposals.' and instructions: '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. È inoltre necessario configurare il criterio IPsec per l'utilizzo dei certificati. Selezionare Configurazione > Gestione criteri > Gestione traffico > **Associazioni di sicurezza**, evidenziare **ESP-3DES-MD5** e fare clic su **Modifica** per configurare il criterio IPsec per configurare il criterio IPsec.



3. Nella finestra Modifica, in Certificati digitali, assicurarsi di selezionare il certificato di identità installato. In Proposta IKE selezionare **CiscoVPNClient-3DES-MD5-RSA** e fare clic su **Applica**.



4. Per configurare un gruppo IPsec, selezionare Configurazione > **Gestione utenti > Gruppi > Aggiungi**, aggiungere un gruppo denominato **IPSECCERT** (il nome del gruppo IPSECCERT corrisponde all'unità organizzativa nel certificato di identità) e selezionare una password. Questa password non viene utilizzata in alcun modo se si utilizzano certificati. Nell'esempio, "cisco123" è la 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	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. Nella stessa pagina, fare clic sulla scheda General (Generale) e verificare di aver selezionato IPsec come protocollo di tunneling.

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. Fare clic sulla scheda IPsec e verificare che l'associazione di protezione (SA) IPsec configurata sia selezionata in SA IPsec e fare clic su **Applica**.

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. Per configurare un gruppo IPSec nel concentratore VPN 3000, selezionare Configurazione > Gestione utenti > Utenti > Aggiungi, specificare un nome utente, una password e il nome del gruppo, quindi fare clic su **Aggiungi**. Nell'esempio vengono utilizzati i campi seguenti: Nome utente = cert_user Password = cisco123 Verifica = 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. Per abilitare il debug su VPN 3000 Concentrator, selezionare **Configurazione > Sistema > Eventi > Classi** e aggiungere le seguenti classi: CERTIFICATO 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. Per visualizzare i debug, selezionare **Monitoraggio > Registro eventi filtrabili**.

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

Nota: se si decide di modificare gli indirizzi IP, è possibile effettuare la registrazione dei nuovi indirizzi IP e installare il certificato rilasciato in un secondo momento con questi nuovi indirizzi.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Per ulteriori informazioni sulla risoluzione dei problemi, fare riferimento a [Risoluzione dei problemi di connessione su VPN 3000 Concentrator](#).

Informazioni correlate

- [Cisco VPN serie 3000 concentrator](#)
- [Client hardware Cisco VPN 3002](#)
- [Negoziazione IPSec/protocolli IKE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)