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

Document ID: 4102

Contents

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.

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

2. 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.

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

3. 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  ESP-3DES-MD5              Specify the name of this Security Association (SA).
        Inheritance  From Rule ▼              Select the granularity of this SA.

IPSec Parameters
  Authentication Algorithm  ESP/MD5/HMAC-128 ▼   Select the packet authentication algorithm to use.
     Encryption Algorithm  3DES-168 ▼            Select the ESP encryption algorithm to use.
      Encapsulation Mode  Tunnel    ▼            Select the Encapsulation Mode for this SA.
    Perfect Forward Secrecy  Disabled        ▼   Select the use of Perfect Forward Secrecy.
    Lifetime Measurement  Time ▼                 Select the lifetime measurement of the IPSec keys.
          Data Lifetime  10000                   Specify the data lifetime in kilobytes (KB).
          Time Lifetime  28800                   Specify the time lifetime in seconds.

IKE Parameters
             IKE Peer  0.0.0.0                    Specify the IKE Peer for a LAN-to-LAN IPSec connection.
       Negotiation Mode  Main        ▼           Select the IKE Negotiation mode to use.
      Digital Certificate  OZ3000          ▼     Select the Digital Certificate to use.
                           ○ Entire certificate chain
   Certificate Transmission                      Choose how to send the digital certificate to the IKE peer.
                           ● Identity certificate only
          IKE Proposal  IKE-3DES-MD5         ▼   Select the IKE Proposal to use as IKE initiator.
    Apply     Cancel
```

4. 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      IPSECCERT        Enter a unique name for the group.
 Name
 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. On the same page, click the General tab and make sure that you select **IPsec** as the Tunneling Protocol.

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions- ▼	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	--None-- ▼	☑	Enter the filter assigned to this group.
Primary DNS		☑	Enter the IP address of the primary DNS server.
Secondary DNS		☑	Enter the IP address of the secondary DNS server.
Primary WINS		☑	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	☐	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**.

IPSec Parameters

Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5 ▼	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate ▼	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Confidence Interval	300	☑	(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 ▼	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.

Remote Access Parameters

Attribute	Value	Inherit?	Description
Group Lock	☐	☑	Lock users into this group.
Authentication	Internal ▼	☐	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
Authorization Type	None ▼	☑	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	☐	☑	Check to require successful authorization.
DN Field	CN otherwise OU ▼	☑	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	☐	☑	Check to require successful authorization.
DN Field	CN otherwise OU ▼	☑	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 ▼	☑	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	☑	☑	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	•••••••	Enter the user's password. The password must satisfy the group password requirements.
Verify	•••••••	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
- ♦ IPSECDBG 1–10
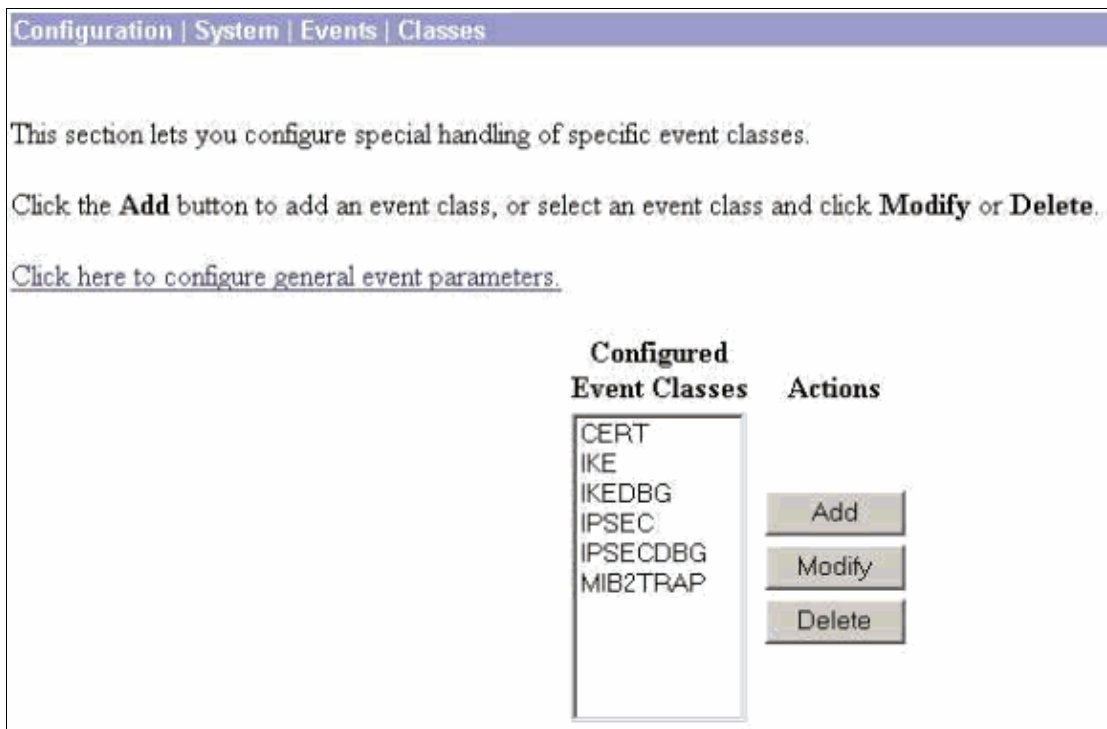
9. Select **Monitoring** > **Filterable Event Log** in order to view the debugs.
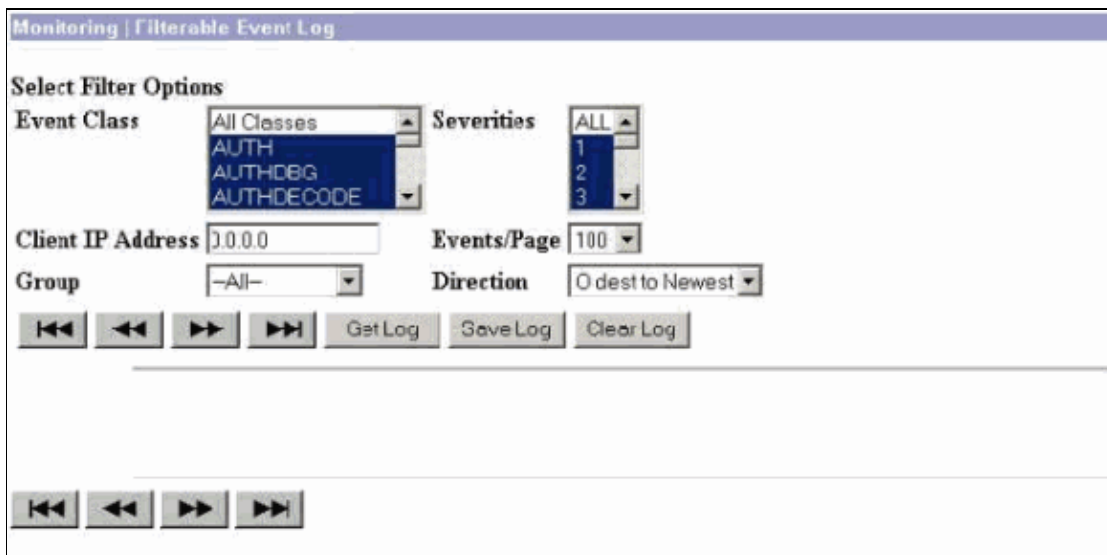
Note: If you decide to change the IP addresses, you can make an enrollment of the new IP addresses and install the issued certificate later with those new addresses.

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**

Updated: Apr 24, 2006   Document ID: 4102