

Configure FlexVPN IKEv2 for Windows Built-in Clients

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[CA Prerequisites](#)
[Network Diagram](#)
[Configurations](#)
[Configure a CA](#)
[Router as CA](#)
[OpenSSL as CA](#)
[Configure the Router IOS XE/IOS](#)
[Import the pkcs12 Certificate if OpenSSL](#)
[Request the Certificate with the Router as CA Server](#)
[Configure FlexVPN IKEv2 with Certificate Authentication](#)
[Configure the IKEv2 Windows Built-in Client](#)
[Windows 10 Built-In Client](#)
[Windows 11 Built-In Client](#)
[Obtain a Client Certificate](#)
[Windows PKCS12 Certificate Installation](#)
[Windows CA Certificate Installation](#)
[Important Details](#)
[Verify](#)
[Troubleshoot](#)

Introduction

This document describes the configuration steps to set up FlexVPN with a built-in client on Windows 10/11.

Prerequisites

Requirements

Cisco recommends you to have knowledge of these topics:

- Windows build-in VPN client
- Cisco IOS® XE FlexVPN configuration
- OpenSSL basic configuration

Components Used

The configuration guide is based on these hardware and software versions:

- Windows 10 and Windows 11

- Cisco IOS XE 16.12.4
- OpenSSL Certificate Authority (CA) v1.1.0g

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, ensure that you understand the potential impact of any command.

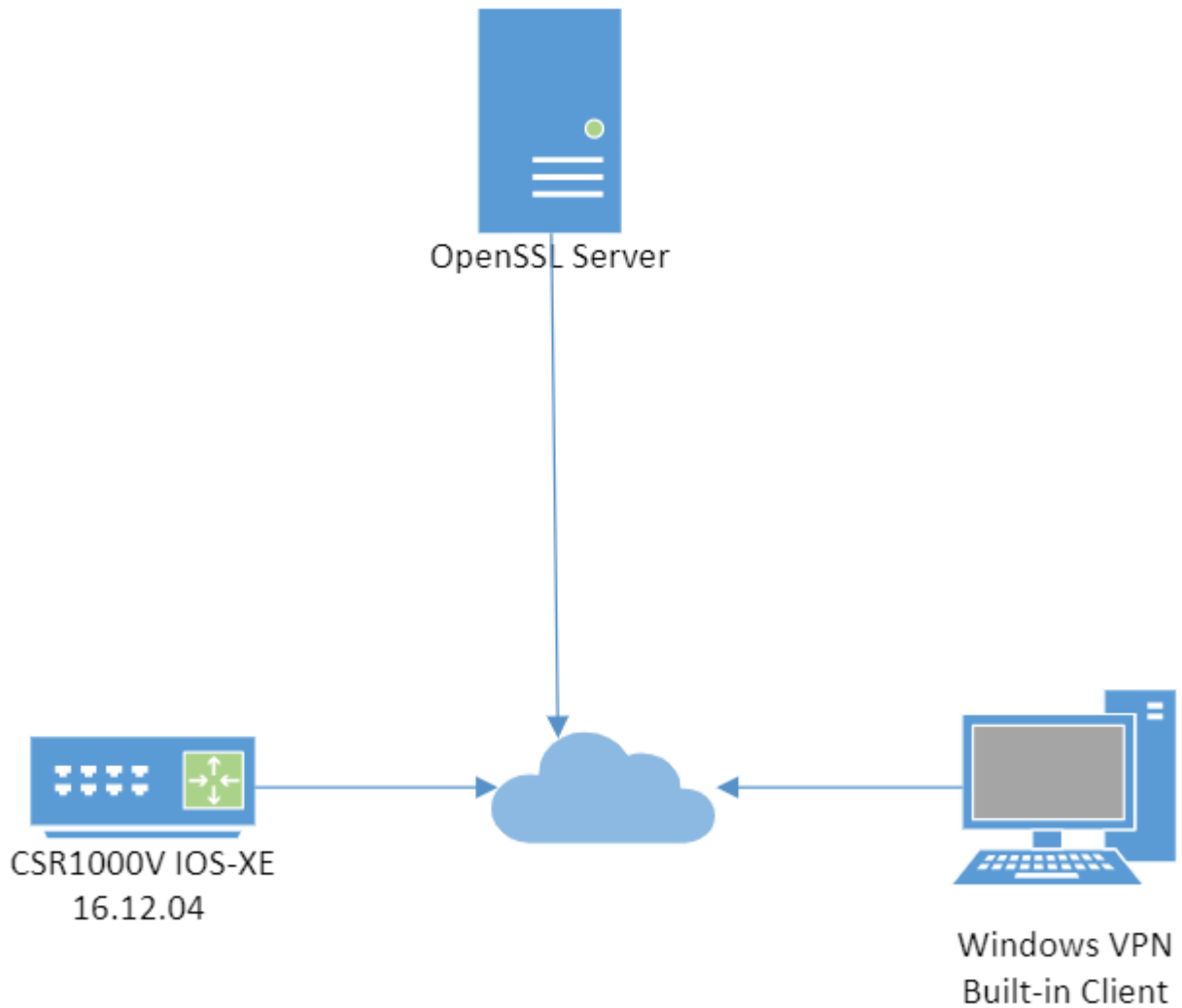
Configure

CA Prerequisites

The CA must allow you to embed the required Extended Key Usage (EKU) in the certificate. For example, on the IKEv2 server, `Server Auth EKU` is required, while the client certificate needs `Client Auth EKU`. Local deployments can make use of:

- Cisco IOS CA server - Self-signed certificates cannot be used because of Cisco bug ID [CSCuc82575](#).
- OpenSSL CA server - `openssl.cnf` must have the `extendedKeyUsage = serverAuth, clientAuth`, this file is normally located in the path `/etc/ssl/`.
- Microsoft CA server - In general, this is the preferred option because it can be configured to sign the certificate exactly as desired.

Network Diagram



Topology lab

Configurations

Configure a CA

Router as CA

If you use a Cisco IOS CA server, ensure you use the most recent Cisco IOS Software release, which assigns the ECU.

```
<#root>
```

```
IOS-CA# show run | section crypto pki
```

```
crypto pki server IOS-CA
```

```
    issuer-name cn=IOS-CA.cisco.com,ou=TAC,o=cisco
```

```
    grant auto
```

```
□
```

```
extendedKeyUsage = serverAuth, clientAuth
```

Configure the Router IOS XE/IOS

Import the pkcs12 Certificate if OpenSSL

The certificate must have the EKU fields set to 'Server Authentication' for Cisco IOS and 'Client Authentication' for the client. Typically, the same CA is used to sign both the client and server certificates. In this case, both 'Server Authentication' and 'Client Authentication' are seen on the server certificate and client certificate respectively, which is acceptable.

If the CA issues the certificates in Public-Key Cryptography Standards (PKCS) #12 format on the IKEv2 server to the clients and the server, and if the certificate revocation list (CRL) is not reachable or available, it must be configured:

```
<#root>
```

```
crypto pki trustpoint FlexRootCA
```

```
    revocation-check none
```

Enter this command in order to import the PKCS#12 certificate:

```
<#root>
```

```
copy ftp://user:***@OpenSSLServer/p12/FlexRootCA.p12* flash:/
```

```
crypto pki import FlexRootCA pkcs12 flash:/FlexRootCA.p12 password <password>
```

!! Note: FlexRootCA.p12 is a pkcs12 format certificate that has CA Certificate bundled in it.

You can also convert the pkcs12 to base64 in OpenSSL and import the certificate in the terminal:

```
openssl base64 -in ikev2.p12 -out ikev2.pem
```

```
cat ikev2.pem --> copy the base64 output
```

```
<#root>
```

```
crypto pki trustpoint FlexRootCA
```

```
enrollment terminal
```

```
revocation-check none
```

```
crypto pki import FlexRootCA pkcs12 terminal password <password>
```

```
***paste the base64 output from the cat ikev2.pem here***
```

```
quit --> when the paste ends you need to type quit to finish
```

Request the Certificate with the Router as CA Server

If a Cisco IOS CA server auto grants certificates, the IKEv2 server must be configured with the CA server URL in order to receive a certificate as shown in this example:

```
<#root>
```

```
crypto pki trustpoint FlexRootCA
```

```
enrollment url http://<CA_Server_IP>:80
```

```
subject-name cn=ikev2.cisco.com,ou=TAC,o=cisco
```

```
revocation-check none
```

```
eku server-auth client-auth
```

When the trustpoint is configured, you need to:

1. Authenticate the CA with this command:

```
<#root>
```

```
crypto pki authenticate FlexRootCA
```

2. Enrol the IKEv2 server with the CA with this command:

```
<#root>
```

```
crypto pki enroll FlexRootCA
```

Configure FlexVPN IKEv2 with Certificate Authentication

This is an example of an IKEv2 configuration:

```
<#root>
```

```
aaa authorization network winclient local
```

```
ip local pool mypool 172.16.0.101 172.16.0.250
```

```
!! Certificate MAP to match Remote Certificates, in our case the Windows Clients
```

```
crypto pki certificate map winclient_map 10
```

```
    subject-name co ou = tac
```

```
!! One of the proposals that Windows 10/11 Built-In Client Likes
```

```
crypto ikev2 proposal winclient
```

```
    encryption aes-cbc-256
```

```
    integrity sha1
```

```
    group 2
```

```
crypto ikev2 policy winclient
```

```
    proposal winclient
```

```
!! IKEv2 Local Authorization Policy. Split-Tunneling does not work, as was
```

```
!! the case in good old l2tp over IPSec.
```

```
crypto ikev2 authorization policy winclient_author
```

```
pool mypool
```

```
crypto ikev2 profile winclient-rsa
```

```
match certificate winclient_map
```

```
identity local fqdn ikev2.cisco.com
```

```
authentication local rsa-sig
```

```
authentication remote rsa-sig
```

```
pki trustpoint FlexRootCA
```

```
aaa authorization group cert list winclient winclient_author
```

```
virtual-template 1
```

```
crypto ipsec transform-set aes256-sha1 esp-aes 256 esp-sha-hmac
```

```
crypto ipsec profile winclient_ikev2
```

```
set transform-set aes256-sha1
```

```
set ikev2-profile winclient-rsa
```

```
interface Virtual-Templat1 type tunnel
```

```
ip unnumbered Loopback0
```

```
tunnel mode ipsec ipv4
```

```
tunnel protection ipsec profile winclient_ikev2
```

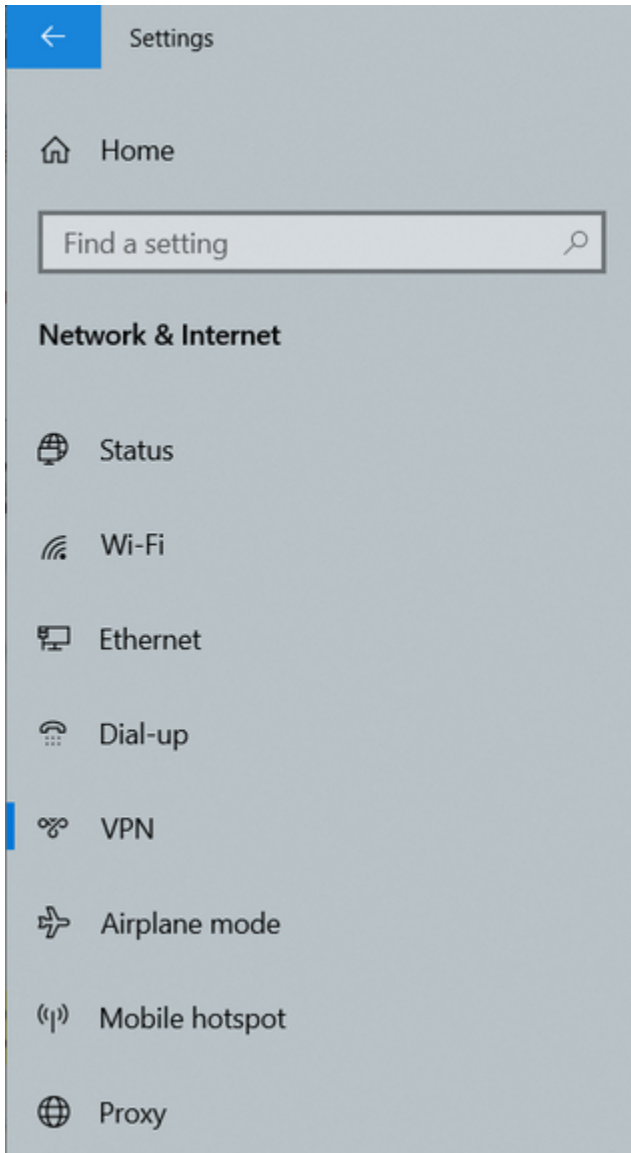
The IP unnumbered of the virtual template must be anything except the local-address used for the IPsec connection. (If you use a hardware client, you would exchange routing information via the IKEv2 configuration node and create a recursive routing issue on the hardware client).

Note: IOS XE version 17.06.01a Cisco bug ID [CSCwa76260](#) and Cisco bug ID [CSCwa80474](#) interfere with the proper functionality of the Windows built-in client since they use group2 as a default dh group. With an upgrade to a fixed release, you are notified about the future removal of deprecated cyphers but they can still work. Additional information:


Configure the IKEv2 Windows Built-in Client

Windows 10 Built-In Client

1. Navigate to Settings > Network & Internet > VPN , and click or select Add a VPN Connection as shown in the image:



VPN

 Add a VPN connection

Advanced Options

Allow VPN over metered networks

On

Allow VPN while roaming

On

Related settings

[Change adapter options](#)

[Change advanced sharing options](#)

[Network and Sharing Center](#)


[Windows Firewall](#)

Windows VPN settings

2. Configure the VPN provider as Windows (built-in), the Connection name, the Server name or address, the VPN type and the Type of sign-in info (authentication), then click **Save** as shown in the image.

Add a VPN connection

VPN provider

Windows (built-in) 

Connection name

FlexVPN-IOS

Server name or address

ikev2.cisco.com

- The IKEv2 server is a Windows 2008 server.
- There is more than one Server Authentication Certificate in use for IKEv2 connections. If this is true, either place both 'Server Authentication' EKU and 'IPSec IKE Intermediate' EKU on one certificate, or distribute these EKUs among the certificates. Ensure at least one certificate contains 'IPSec IKE Intermediate' EKU.

Refer to [Troubleshooting IKEv2 VPN Connections](#) for more information.

- In a FlexVPN deployment, do not use 'IPSec IKE Intermediate' in EKU. If you do, the IKEv2 client does not pick up the IKEv2 server certificate. As a result, they are not able to respond to CERTREQ from IOS in the IKE_SA_INIT response message and thus fail to connect with a 13806 Error ID.
- While the Subject Alternative Name (SAN) is not required, it is acceptable if the certificates have one.
- On the Windows 10/11 Client Certificate Store, ensure that the Machine-Trusted Root Certificate Authorities Store has the least number of certificates possible. If it has more than 50 or so, Cisco IOS might fail to read the entire Cert_Req payload, which contains the Certificate Distinguished Name (DN) of all the known CAs from the Windows 10/11 box. As a result, the negotiation fails and you see the connection time-out on the client.

Verify

Use this section in order to confirm that your configuration works properly.

```
<#root>
```

```
CSR1kv# show crypto ikev2 session detail
```

```
IPv4 Crypto IKEv2 Session
```

```
Session-id:6,
```

```
Status:UP-ACTIVE
```

```
, IKE count:1,
```

```
CHILD count:1
```

```
Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.3.1/4500 192.168.56.1/4500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/5s 7 sec
CE id: 1007, Session-id: 6
Status Description: Negotiation done
Local spi: 3A330D1951062E50 Remote spi: 222ED6C38002E26D
```

```
Local id: ikev2.cisco.com
```

```
Remote id: ou=TAC,o=Cisco,c=BE,cn=Winclient
```

```
Local req msg id: 0 Remote req msg id: 2
```

```
Local next msg id: 0 Remote next msg id: 2
```

```
Local req queued: 0 Remote req queued: 2
```

```
Local window: 5 Remote window: 1
```

```
DPD configured for 0 seconds, retry 0
```

```
NAT-T is not detected
```

```
Cisco Trust Security SGT is disabled
Assigned host addr: 172.16.0.105
Initiator of SA : No
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 172.16.0.105/0 - 172.16.0.105/65535
ESP spi in/out: 0xB01348F5/0x142CEC36
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

<#root>

CSR1Kv#

```
show crypto ipsec sa peer 192.168.56.1
```

```
interface: Virtual-Access1
```

```
  Crypto map tag: Virtual-Access1-head-0, local addr 10.0.3.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
remote ident (addr/mask/prot/port): (172.16.0.105/255.255.255.255/0/0)
```

```
current_peer 192.168.56.1 port 4500
```

```
  PERMIT, flags={origin_is_acl,}
```

```
#pkts encaps: 223, #pkts encrypt: 223, #pkts digest: 223
```

```
#pkts decaps: 315, #pkts decrypt: 315, #pkts verify: 315
```

```
#pkts compressed: 0, #pkts decompressed: 0
```

```
#pkts not compressed: 0, #pkts compr. failed: 0
```

```
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0
```

```
local crypto endpt.: 10.0.3.1, remote crypto endpt.: 192.168.56.1
```

```
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
```

```
current outbound spi: 0x142CEC36(338488374)
```

```
PFS (Y/N): N, DH group: none
```

```
inbound esp sas:
```

```
spi: 0xB01348F5(2954053877)
```

```
  transform: esp-aes esp-sha-hmac ,
```

```
  in use settings ={Tunnel, }
```

```
  conn id: 2017, flow_id: CSR:17, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-head-
```

```
  sa timing: remaining key lifetime (k/sec): (4607961/2461)
```

```
  IV size: 16 bytes
```

```
  replay detection support: Y
```

```
  Status: ACTIVE(ACTIVE)
```

```
inbound ah sas:
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0x142CEC36(338488374)
  transform: esp-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  conn id: 2018, flow_id: CSR:18, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-head
  sa timing: remaining key lifetime (k/sec): (4607987/2461)
  IV size: 16 bytes
  replay detection support: Y
  Status: ACTIVE(ACTIVE)
```

outbound ah sas:

outbound pcp sas:

Troubleshoot

You can troubleshoot the FlexVPN connection and certificate negotiation with these debugs:

```
debug crypto condition peer <remove client public ip>
debug crypto ikev2
```

```
debug cry pki messages
debug cry pki transactions
```

In the Windows client, you can check the Event Viewer under the Windows Logs and check the Application, the VPN connection events use the source RasClient. For example;

Event Viewer

File Action View Help

← → 📄 ? 📄

Event Viewer (Local)

- > Custom Views
- ▼ Windows Logs
 - Application
 - Security
 - Setup
 - System
 - Forwarded Events
- > Applications and Services Logs
 - Subscriptions

Application Number of events: 1,959

Level	Date and Time	Source
Information	3/29/2022 1:23:00 AM	RasClient
Information	3/29/2022 12:53:19 AM	RasClient

Event 20225, RasClient

General Details

Cold={3E68E360-42D9-0000-CE70-6F3ED942D801}: The user JP\JP has dialed a connection named F... Access Server which has successfully connected. The connection parameters are:
TunnellpAddress = 172.16.0.105
Tunnellpv6Address = None
Dial-in User = .

Windows eventviewer logs for RasClient