Using IKEv2 on Pulse Secure  Pulse Secure Access Appliance
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before we begin</td>
<td>3</td>
</tr>
<tr>
<td>Configuring IKEv2 on IVE</td>
<td>3</td>
</tr>
<tr>
<td>IKEv2 Client Side Configuration on Windows 7</td>
<td>9</td>
</tr>
<tr>
<td>Client Requirements</td>
<td>9</td>
</tr>
<tr>
<td>Before we begin</td>
<td>10</td>
</tr>
<tr>
<td>Client Side Configuration of IKEv2 on Windows 7</td>
<td>10</td>
</tr>
<tr>
<td>Connecting to 'VPN Connection’</td>
<td>15</td>
</tr>
<tr>
<td>Configuring IKEv2 VPN Client on Nokia Mobile Phones</td>
<td>18</td>
</tr>
<tr>
<td>Supported Mobile Phones</td>
<td>20</td>
</tr>
</tbody>
</table>
Before we begin:

- Make sure you have imported the valid Device Certificate to the IVE under Configuration > Certificates > Device Certificate
- Make sure a valid Device Certificate is bound to the port (internal or external) for IKEv2 traffic
- Make sure you have imported the Trusted Client CA certificate under Configuration > Certificates > Trusted Client CAs
- Make sure you have imported the Trusted Server Certificate under Configuration > Certificates > Trusted Server CAs
- Make sure you configure a valid VPN Tunneling profile to work with IKEv2

Configuring IKEv2 on IVE:

- Create a Role and enable IKEv2 in the role (as shown below). Roles specify the Secure Access session properties, including enabled access features, for users who are mapped to the role.

To enable the IKEv2 access feature:

1. Select Users > User Roles > Role Name > General > Overview from the admin console.
2. Under Access Features, check the IKEv2 (for 7.1 and below) or VPN Tunneling (for 7.2 and above)
3. Click Save Changes.

7.2 and above

![Access features](image-url)
7.1 and below

Create a Certificate Auth Server

**Name:** cert

**User Name Template:** `<certDN.CN>`

The template can contain textual characters as well as variables for substitution. Variables should be enclosed in brackets. Here are some examples:

- `<certDN.CN>`: First CN from the subject DN
- `<certAttr.serialNumber>`: Certificate serial number
- `<certAttr.altName.xxx>`: Where `xxx` can be:
  - `Email`: The Email alternate name
  - `UPN`: The Principal Name alternate name
  - `...`: etc
- `<certDNText>`: The complete subject DN
- `cert-<certDN.CN>`: The text `"cert-"` followed by the first CN from the subject DN

**User Record Synchronization**

- Enable User Record Synchronization

**Logical Auth Server Name:**
Create Realm and use the Certificate Authentication Server with the realm

IKE Realm

Name: IKE Realm
Description: IKE Realm

☐ When editing, start on the Role Mapping page

Servers

Specify the servers to use for authentication and authorization. To create or manage servers, see the Server.

Authentication: cert
Directory/Attribute: None
Accounting: None

☐ Additional authentication server

☐ Dynamic policy evaluation
Create the Role Mapping rule based on Custom Expression if UserAgent='IKEv2' then map the particular role created for IKEv2 Users.

a. To do this, click on User Realm > IKE Realm > Role Mapping > New Rule and choose Custom Expression under ‘Rule based on’ and click on ‘Update’.

b. Under the rule click on ‘Expression’. Now the Server Catalog page opens as shown in the screenshot above.

c. On the right hand side under Expression Dictionary scroll down to choose the expression “UserAgent= ‘*MSIE*’” and click on ‘Insert Expression’.

d. Modify the expression to ‘UserAgent= ‘IKEv2’ ’ and click on ‘Add Expression’ after giving the name for that Expression (Exp: IKEv2 Agent) and click on ‘Save Changes’.

e. Choose the ‘Expression’ and ‘Role ‘ under the Role Mapping rule and click on ‘Save Changes’ as shown in the screenshot below:
You can also create a role mapping role based on Username such as If Username = * then map the ‘IKE User role’. Both the rules can work independently since we are authenticating based on the certificate only and not based on Username.
Click on **Configuration>IKEv2** as shown in the screenshot below:

Under ‘User Realm’, select the port (internal or external) and realm where IKEv2 traffic will be sent to and click Add. Enter a DPD Timeout Value ranging from 400 to 3600 seconds and click Add. Once finalized, click ‘Save Changes’.
The configuration for IKEv2 is done. Once the user is successfully logged in, when you click on **System>Status>Active Users**, we can find the user logged in through IKEv2 Agent as shown below:

### IKEv2 Client Side Configuration on Windows 7

#### Client Requirements

Your IKEv2 client should support the following requirements in order to work with Secure Access:

- Ability to establish IPSec Security Associations in Tunnel mode (RFC 4301)
- Ability to utilize the AES 128-bit encryption function (RFC 3602)
- Ability to utilize the SHA-1 hashing function (RFC 2404)
- Ability to utilize Diffie-Hellman Perfect Forward Secrecy in “Group 2” mode (RFC 2409)
- Ability to utilize IPSec Dead Peer Detection (RFC 3706)
- Ability to utilize the MD5 hashing function (RFC 1321)
- Ability to handle Internal Address on a Remote Network utilizing CFG_REQUEST-CFG_REPLY exchange
Before we begin

- Import the client side certificate to the personal Certificate of the Windows 7 machine
- Import the certificate of the root CA to the trusted root Certificate Authority Store of Windows 7 machine

Client Side Configuration of IKEv2 on Windows 7

1. Right click on ‘Network’ and click on Properties
2. Now click on ‘Set up a new connection or network’ as shown below.
3. Click on ‘Connect to Work Place’ and click on ‘Next’.
4. Double Click on ‘Use my Internet Connection (VPN)’

5. Type the IP Address or the Host name of the IVE and type the name of the VPN Connection and click on ‘Next’.
6. Type the dummy username, password and Domain Name and click on Create.

7. Click on ‘Close’
8. Configuring the IKEv2 VPN Connection

a. To configure VPN Connection, go to Control Panel > Network and Internet > Network Connections. You will notice a new Network with the Network name ‘VPN Connection’.

![VPN Connection](image1)

b. Right click on ‘VPN Connection’ and click on Properties.

![Properties](image2)

c. Under the ‘General’ tab make sure you have entered the hostname of the Pulse Secure Access (SA) device. This name must match the hostname that is issued on the device certificate.

![Settings](image3)
d. Click on ‘Security’ tab. Under the Type of VPN, select ‘IKEv2’.

e. Under ‘Data Encryption’, select ‘Optional Encryption (Connect even if no encryption)’ [if 128bit encryption is configured on the Pulse Secure Access device]

f. Under ‘Authentication’, select ‘Use Machine Certificates’

g. Click ‘OK’
Connecting to 'VPN Connection’

1. Go to Control Panel>Network and Internet>Network Connections
2. Right click on 'VPN Connection’
3. Click on ‘Connect’
From the screenshot below of the IPCONFIG and ROUTE PRINT, we can notice the VPN Connection was successfully.
Under Status>Active Users, the administrator can configure the user is logged in successfully with the IKEv2 as the Agent Type.
Configuring IKEv2 VPN Client on Nokia Mobile Phones

1. Download the Nokia VPN Client software from the Nokia Web Page.
2. Install it on a Windows Machine
3. Start the Nokia Mobile VPN Client Policy Tool
4. Type the Policy Name
5. Type the IP address of the Pulse Secure Access under ‘VPN Gateway Address’
6. Under the IKE Section, choose IKEv2 as the IKE mode
7. Choose ‘RSA Signatures’ as the Authentication method
8. Leave the Identity type and Identity value blank
9. Under Certificate Authority, choose ‘BIN’ format and browse to the CA Root Certificate
10. Under PKCS#12, choose Client Certificate for the VPN client in P12 format

11. Click on View and ‘Advanced View’
12. Under IPSEC>SA, click on the Policy you created
13. Choose the encryption algorithm as ‘AES 128’ (Note: This should match the algorithm selected on the Pulse Secure Access device)

14. Under Hash algorithm, choose ‘SHA1’

15. On the left hand side, click on IKE>Proposals

16. In the ‘General’ tab, under Cert Store, choose ‘DEVICE’

17. On the left hand side, click on IKE>Proposal>ASE 128-CBC

18. Under the ‘IKE Proposal Parameters’, choose ‘3DES-CBC’ as the Encryption algorithm and SHA1 for the Hash algorithm

19. Click on ‘Generate VPN Policy’ to create a VPN policy file and upload this file to the Nokia mobile device.

On your Nokia mobile device, go to Office>VPN Management. Verify the policy file is properly imported and connect to the VPN using IKEv2

**Supported Mobile Phones**

IKE v2 should work on any mobile phones that support IKE v2 configuration. Pulse Secure has tested this using Nokia E63 Mobile Phone.