

# Configure an Internet Protocol Security (IPSec) Profile on an RV34x Series Router

## Objective

Internet Protocol Security (IPSec) provides secure tunnels between two peers, such as two routers. Packets that are considered sensitive and should be sent through these secure tunnels, as well as the parameters that should be used to protect these sensitive packets should be defined by specifying the characteristics of these tunnels. Then, when the IPsec peer sees such a sensitive packet, it sets up the appropriate secure tunnel and sends the packet through this tunnel to the remote peer.

When IPsec is implemented in a firewall or a router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

The objective of this document is to show you how to configure the IPSec Profile on an RV34x Series Router.

## Applicable Devices

- RV34x Series

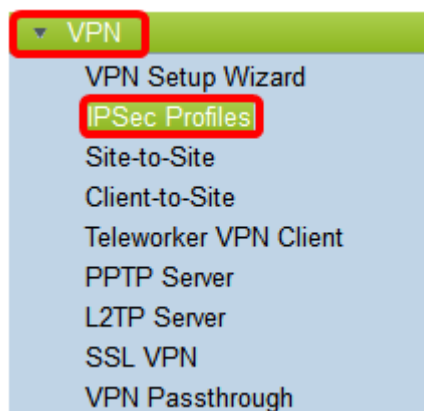
## Software Version

- 1.0.1.16

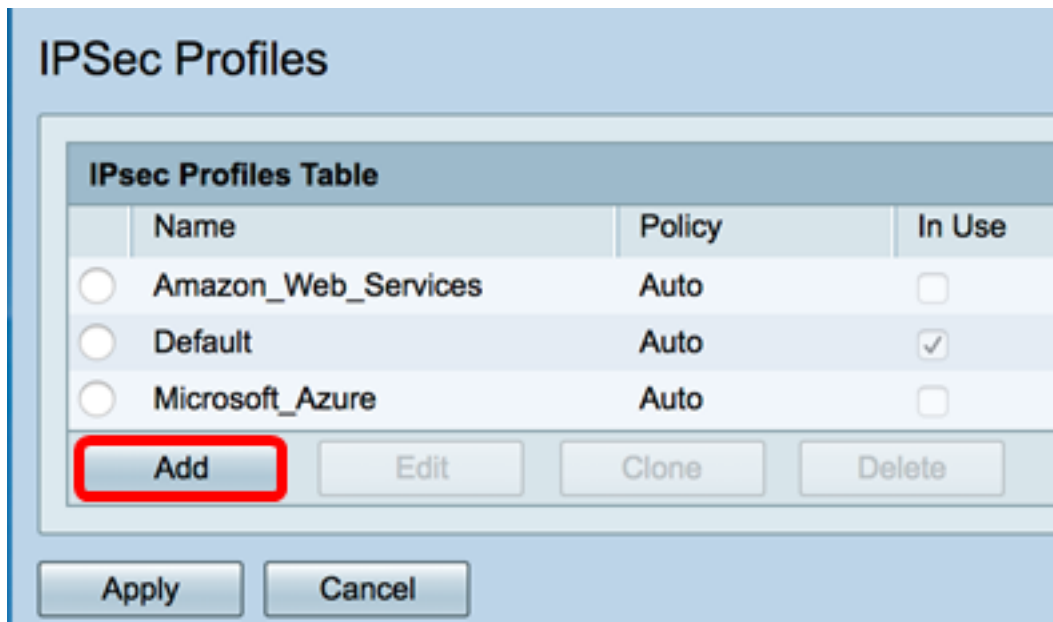
## Configure IPSec Profile

### Create an IPSec Profile

Step 1. Log in to the web-based utility of the router and choose **VPN > IPSec Profiles**.

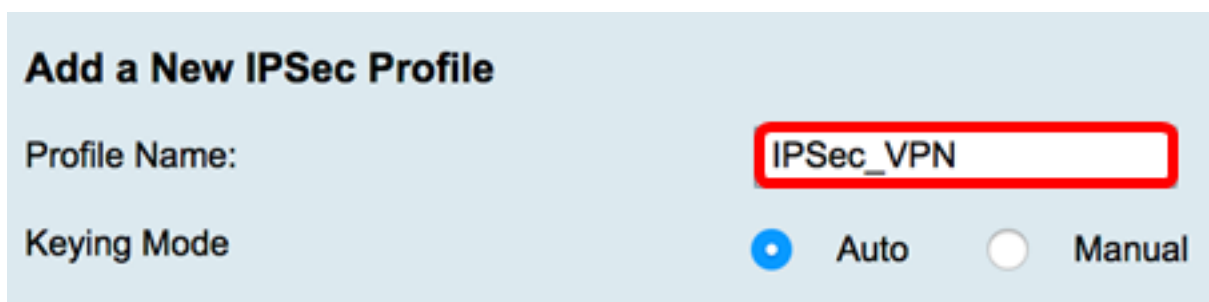


Step 2. The IPSec Profiles Table shows the existing profiles. Click **Add** to create a new profile.



Step 3. Create a name for the profile in the *Profile Name* field. The profile name must contain only alphanumeric characters and an underscore ( `_` ) for special characters.

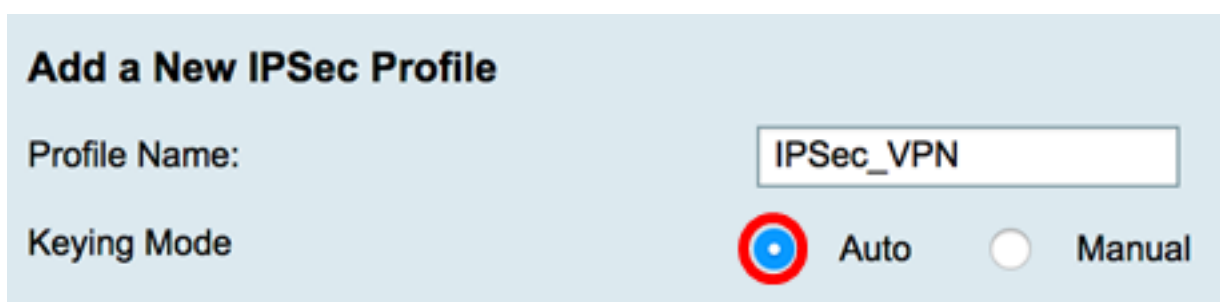
**Note:** In this example, IPsec\_VPN is used as the IPsec profile name.



Step 4. Click a radio button to determine the key exchange method the profile will use to authenticate. The options are:

- Auto — Policy parameters are set automatically. This option uses an Internet Key Exchange (IKE) policy for data integrity and encryption key exchanges. If this is chosen, the configuration settings under the Auto Policy Parameters area are enabled. Click [here](#) to configure the Auto settings.
- Manual — This option allows you to manually configure the keys for data encryption and integrity for the Virtual Private Network (VPN) tunnel. If this is chosen, the configuration settings under the Manual Policy Parameters area are enabled. Click [here](#) to configure the Manual settings.

**Note:** For this example, Auto was chosen.



## Configure the Auto Settings

Step 1. In the Phase 1 Options area, choose the appropriate Diffie-Hellman (DH) group to be used with the key in Phase 1 from the DH Group drop-down list. Diffie-Hellman is a cryptographic key exchange protocol which is used in the connection to exchange pre-shared key sets. The strength of the algorithm is determined by bits. The options are:

- Group2 - 1024 bit — Computes the key slower, but is more secure than Group1.
- Group5 - 1536-bit — Computes the key the slowest, but is the most secure.

**Note:** In this example, Group2-1024 bit is chosen.



Step 2. From the Encryption drop-down list, choose the appropriate encryption method to encrypt and decrypt Encapsulating Security Payload (ESP) and Internet Security Association and Key Management Protocol (ISAKMP). The options are:

- 3DES — Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard uses a 128-bit key.
- AES-192 — Advanced Encryption Standard uses a 192-bit key.
- AES-256 — Advanced Encryption Standard uses a 256-bit key.

**Note:** AES is the standard method of encryption over DES and 3DES for its greater performance and security. Lengthening the AES key will increase security with a drop-in performance. For this example, AES-256 is chosen.



Step 3. From the Authentication drop-down menu, choose an authentication method that will determine how ESP and ISAKMP are authenticated. The options are:

- MD5 — Message Digest Algorithm has a 128-bit hash value.
- SHA-1 — Secure Hash Algorithm has a 160-bit hash value.
- SHA2-256 — Secure Hash Algorithm with a 256-bit hash value.

**Note:** MD5 and SHA are both cryptographic hash functions. They take a piece of data, compact it, and create a unique hexadecimal output that is typically not reproducible. In this example, SHA2-256 is chosen.

DH Group: Group2 - 1024 bit

Encryption: MD5

Authentication:  SHA2-256

Step 4. In the *SA Lifetime* field, enter a value ranging between 120 to 86400. This is the length of time the Internet Key Exchange (IKE) Security Association (SA) will remain active in this phase. The default value is 28800.

**Note:** In this example, 28801 is used.

Authentication: SHA2-256

SA Lifetime: 28801

Perfect Forward Secrecy:  Enable

Step 5. (Optional) Check the **Enable Perfect Forward Secrecy** check box to generate a new key for IPsec traffic encryption and authentication.

Authentication: SHA2-256

SA Lifetime: 28801

Perfect Forward Secrecy:  Enable

Step 6. From the Protocol Selection drop-down menu in the Phase II Options area, choose a protocol type to apply to the second phase of the negotiation. The options are:

- ESP — If this is chosen, skip to [Step 7](#) to choose an encryption method on how the ESP packets will be encrypted and decrypted. A security protocol which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.
- AH — Authentication Header (AH) is a security protocol which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram). Skip to [Step 8](#) if this was chosen.

**Phase II Options**

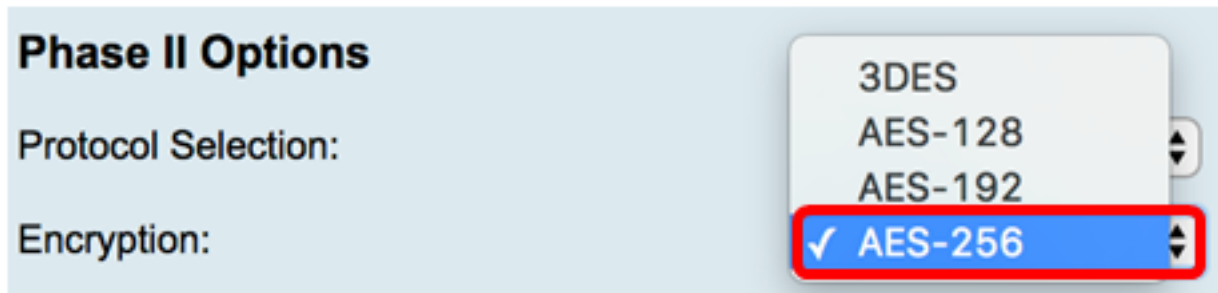
Protocol Selection:  ESP

Encryption: AH

[Step 7](#). If ESP was chosen in Step 6, choose the appropriate encryption method to encrypt and decrypt ESP and ISAKMP from the Encryption drop-down list. The options are:

- 3DES — Triple Data Encryption Standard.
- AES-128 — Advanced Encryption Standard uses a 128-bit key.
- AES-192 — Advanced Encryption Standard uses a 192-bit key.
- AES-256 — Advanced Encryption Standard uses a 256-bit key.

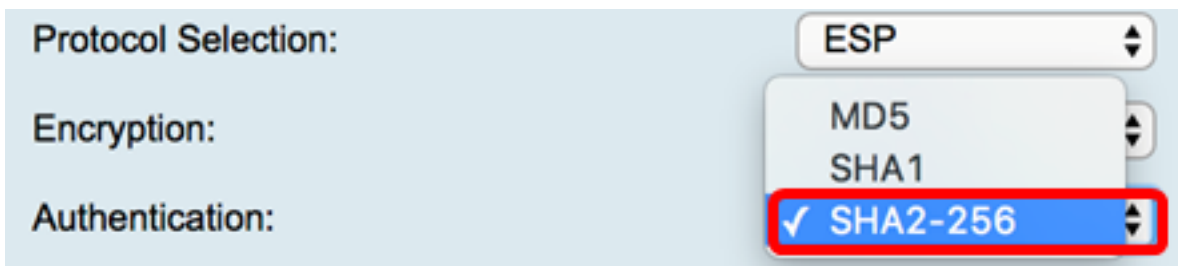
**Note:** In this example, AES-256 is chosen.



[Step 8](#). From the Authentication drop-down menu, choose an authentication method that will determine how ESP and ISAKMP are authenticated. The options are:

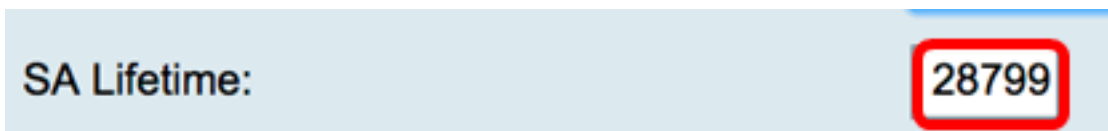
- MD5 — Message Digest Algorithm has a 128-bit hash value.
- SHA-1 — Secure Hash Algorithm has a 160-bit hash value.
- SHA2-256 — Secure Hash Algorithm with a 256-bit hash value.

**Note:** In this example, SHA2-256 is used.



Step 9. In the *SA Lifetime* field, enter a value ranging between 120 to 28800. This is the length of time the IKE SA will remain active in this phase. The default value is 3600.

**Note:** In this example, 28799 is used.



Step 10. From the DH Group drop-down list, choose the appropriate Diffie-Hellman (DH) group to be used with the key in Phase 2. The options are:

- Group2 – 1024 bit — Computes the key slower, but is more secure than Group1.
- Group5 – 1536 bit — Computes the key the slowest, but is the most secure.

**Note:** In this example, Group5 – 1536 bit is chosen.

SA Lifetime: 28700

DH Group: Group5 - 1536 bit

Step 11. Click .

**Note:** You will be taken back to the IPSec Profiles Table and the newly-created IPSec profile should now appear.

**IPSec Profiles**

Success. To permanently save the configuration, go to [Configuration Management](#) page or click Save icon.

IPsec Profiles Table			
	Name	Policy	In Use
<input type="radio"/>	Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>
<input type="radio"/>	Default	Auto	<input checked="" type="checkbox"/>
<input type="radio"/>	Microsoft_Azure	Auto	<input type="checkbox"/>
<input type="radio"/>	IPSec_Vpn	Auto	<input type="checkbox"/>

Step 12. (Optional) To save the configuration permanently, go to the Copy/Save Configuration page or click the  icon at the upper portion of the page.

You should now have successfully configured an Auto IPSec Profile on an RV34x Series Router.

## Configure the Manual Settings

Step 1. In the *SPI-Incoming* field, enter a hexadecimal number ranging from 100 to FFFFFFFF for the Security Parameter Index (SPI) tag for incoming traffic on the VPN connection. The SPI tag is used to distinguish the traffic of one session from the traffic of other sessions.

**Note:** For this example, 0xABCD is used.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Step 2. In the *SPI-Outgoing* field, enter a hexadecimal number ranging from 100 to FFFFFFFF for the SPI tag for outgoing traffic on the VPN connection.

**Note:** For this example, 0x1234 is used.

SPI-Incoming: 0xABCD  
SPI-Outgoing: 0x1234

**Step 3.** Choose an option from the Encryption drop-down list. The options are 3DES, AES-128, AES-192, and AES-256.

**Note:** In this example, AES-256 is chosen.

SPI Incoming: [ ]  
SPI Outgoing: [ ]  
Encryption:  AES-256

**Step 4.** In the *Key-In* field, enter a key for the inbound policy. The key length depends on the algorithm chosen in [Step 3](#).

- 3DES uses a 48-character key.
- AES-128 uses a 32-character key.
- AES-192 uses a 48-character key.
- AES-256 uses a 64-character key.

**Note:** In this example, 123456789123456789123... is used.

Key-In: 123456789123456789123  
Key-Out: 1a1a1a1a1a1a1a1a1212121

**Step 5.** In the *Key-Out* field, enter a key for the outgoing policy. The key length depends on the algorithm chosen in Step 3.

**Note:** In this example, 1a1a1a1a1a1a1a1a121212... is used.

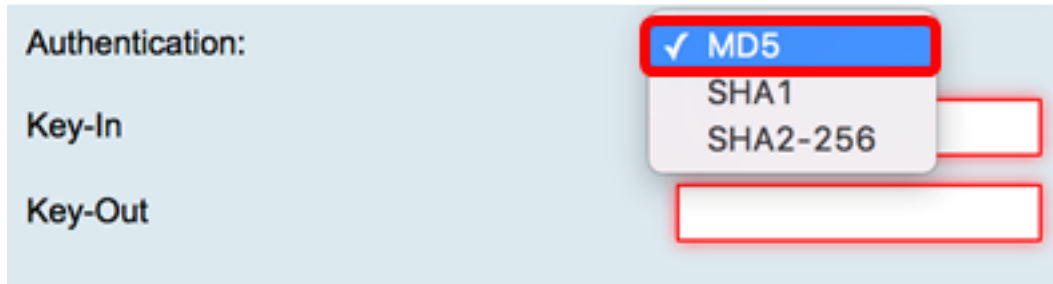
Key-In: 123456789123456789123  
Key-Out: 1a1a1a1a1a1a1a1a1212121

**Step 6.** Choose an option from the Manual Integrity Algorithm drop-down list.

- MD5 — Uses a 128-bit hash value for data integrity. MD5 is less secure but faster than SHA-1 and SHA2-256.
- SHA-1 — Uses a 160-bit hash value for data integrity. SHA-1 is slower but more secure than MD5, and SHA-1 is faster but less secure than SHA2-256.
- SHA2-256 — Uses a 256-bit hash value for data integrity. SHA2-256 is slower but secure than MD5 and SHA-1.



**Note:** In this example, MD5 is chosen.

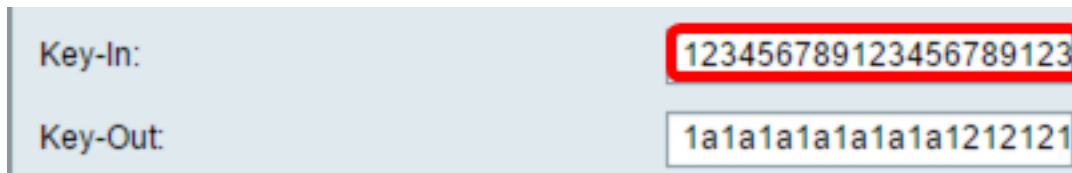


A screenshot of a configuration interface showing authentication options. The 'Authentication:' label is on the left. To its right is a dropdown menu with three options: 'MD5' (selected with a checkmark and highlighted in blue), 'SHA1', and 'SHA2-256'. Below the dropdown are two empty text input fields, one for 'Key-In' and one for 'Key-Out'. Red boxes highlight the 'MD5' option and the 'Key-In' and 'Key-Out' fields.

Step 7. In the *Key-In field*, enter a key for the inbound policy. The key length depends on the algorithm chosen in [Step 6](#).

- MD5 uses a 32-character key.
- SHA-1 uses a 40-character key.
- SHA2-256 uses a 64-character key.

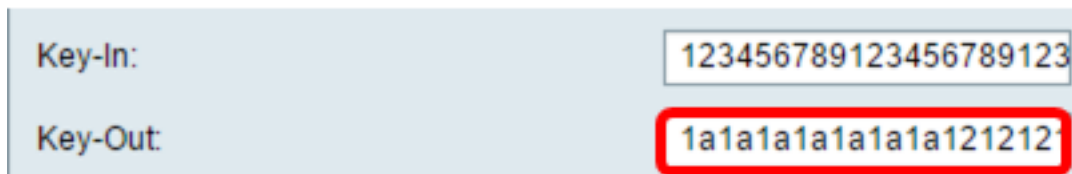
**Note:** In this example, 123456789123456789123... is used.



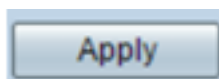
A screenshot of a configuration interface showing two text input fields. The 'Key-In:' field contains the text '123456789123456789123' and is highlighted with a red box. The 'Key-Out:' field contains the text '1a1a1a1a1a1a1a1a1212121'.

Step 8. In the *Key-Out field*, enter a key for the outgoing policy. The key length depends on the algorithm chosen in [Step 6](#).

**Note:** In this example, 1a1a1a1a1a1a1a1a121212... is used.



A screenshot of a configuration interface showing two text input fields. The 'Key-In:' field contains the text '123456789123456789123'. The 'Key-Out:' field contains the text '1a1a1a1a1a1a1a1a121212' and is highlighted with a red box.




Step 9. Click .

**Note:** You will be taken back to the IPSec Profiles Table and the newly-created IPSec profile should now appear.



## IPSec Profiles

 Success. To permanently save the configuration, Go to [Configuration Management page](#) or click Save icon.

IPsec Profiles Table			
	Name	Policy	In Use
<input type="radio"/>	Amazon_Web_Services	Auto	<input checked="" type="checkbox"/>
<input type="radio"/>	Default	Auto	<input checked="" type="checkbox"/>
<input type="radio"/>	Microsoft_Azure	Auto	<input type="checkbox"/>
<input type="radio"/>	IPSec_Vpn	Manual	<input type="checkbox"/>

Step 10. (Optional) To save the configuration permanently, go to the Copy/Save Configuration page or click the  icon at the upper portion of the page.

You should now have successfully configured a Manual IPSec Profile on an RV34x Series Router.