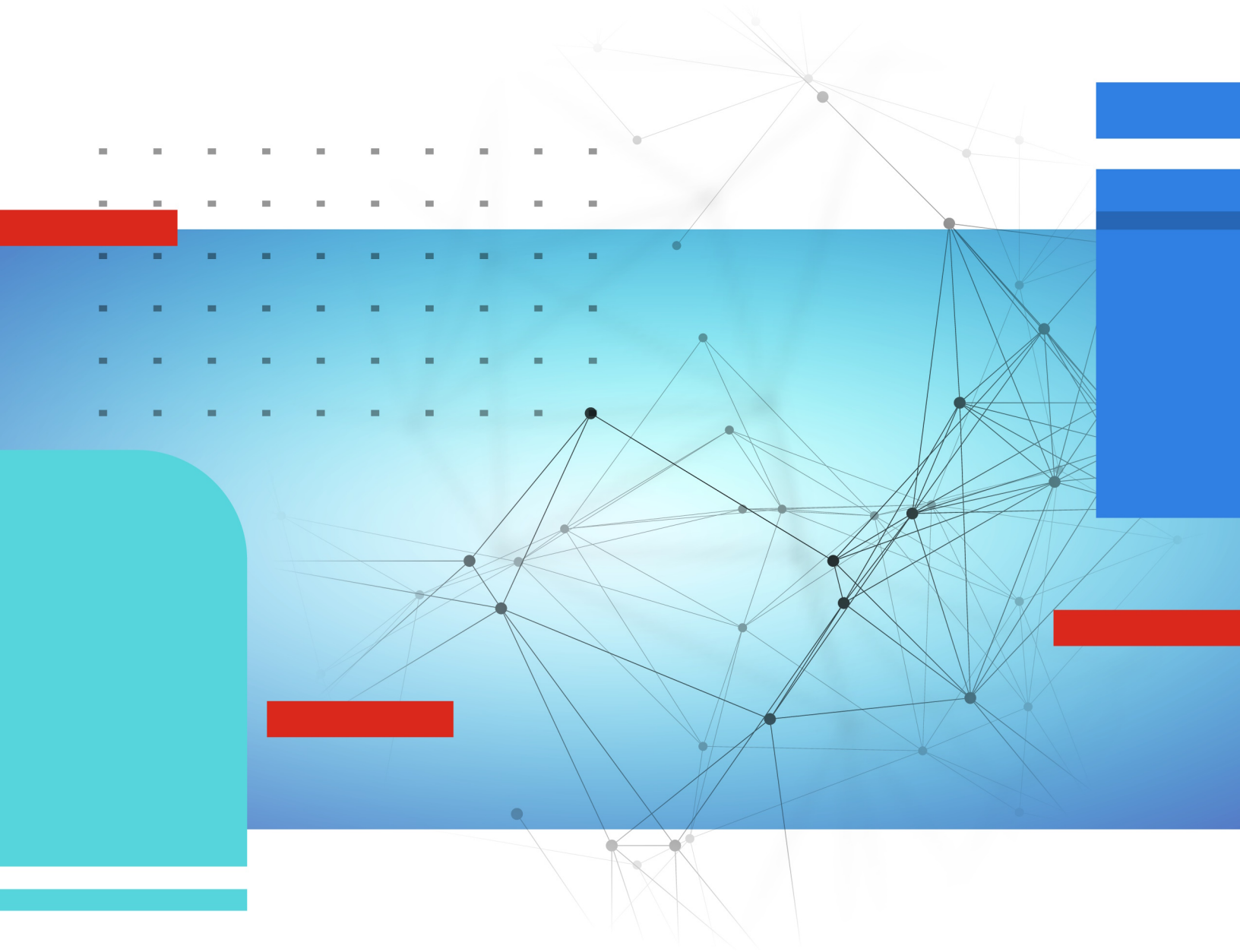
SSL VPN to IPsec VPN Migration

FortiOS 7.6.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 06, 2025
FortiOS 7.6.0 SSL VPN to IPsec VPN Migration
01-760-1018190-20251106

TABLE OF CONTENTS

Change Log

Date	Change Description
2024-07-25	Initial release.
2025-02-12	Updated for FOS 7.6.1.
2025-02-13	Added Split DNS and DNS suffix on page 11.
2025-05-02	Added steps to configure IPsec VPN using TCP as transport with port 443.
2025-08-26	Updated to note that IKEv1 is not supported on FortiClient 7.4.4 and later.
2025-09-26	Updated FortiClient endpoint configuration migration on page 33.
2025-11-06	Updated FortiClient endpoint configuration migration on page 33.

Introduction

Virtual Private Network (VPN) technology allows users, devices, and sites to securely connect to each other over the internet in an otherwise insecure medium. SSL VPN and IPsec VPN in particular are well used technologies that are easy to configure and deploy.

Each technology has its advantages and common use cases. SSL VPN, for example, is typically tailored towards secure remote access from individual users and endpoints. It is generally easy to set up, and because connections are secured over TLS on TCP/443, few ISPs will restrict SSL VPN connections. It also offers two modes (tunnel and web mode) that can be provisioned in agent and agentless deployments.

On the other hand, IPsec VPN is typically associated with site-to-site connections, and is especially convenient in multi-site hub and spoke deployments using ADVPN (Auto Discovery VPN). Complex multi-site deployments are simplified, as ADVPN incorporates automatic tunnel establishment between sites, dynamic routing, and mass provisioning using an orchestrator such as FortiManager.

On a smaller scale, IPsec VPN is just as capable of supporting remote users using dial-up VPN connections. Similar to SSL VPN, IPsec when configured to use IKE version 2 supports configuring TCP as its transport method using port 443 that enables IKE negotiation over TCP and encapsulates ESP packets inside TCP headers. Protocols, encryption algorithms, and authentication methods can all be customized to suit a company's needs.

Finally, as an alternative to VPN—and especially SSL VPN web-based VPN—ZTNA (Zero Trust Network Access) can also be used to secure remote access. ZTNA offers a seamless connection secured over TLS between the endpoints and Zero Trust Application Gateway. A Zero Trust approach assumes devices cannot be trusted until they have passed required security posture checks, such as client certificate verification and vulnerability scans. See the SSL VPN to ZTNA Migration Guide for more information.

This document explores SSL VPN and IPsec VPN a little deeper, as well as things to consider while migrating from SSL VPN to IPsec VPN. Additionally, we will review examples of common SSL VPN use cases and demonstrate steps to migrate these setups to IPsec VPN.

Customers are advised to move to remote access using IPsec VPN as an SSL VPN tunnel mode replacement before upgrading to FortiOS 7.6.3 and above.

Migration background

To understand how to migrate from SSL VPN to IPsec VPN, we first examine a few aspects of each VPN technology:

Security Comparison

SSL VPN offers security through TLS in the following ways:

- By encrypting the data transmitted between the client and the VPN gateway using cryptographic algorithms to ensure data in transit has not been tampered
- By providing an authentication mechanism for client and server to verify the identify of each other
- By using secure key exchanges such as Diffie-Hellman to establish shared secrets between client and server
- By using X.509 certificates to authenticate servers and optionally clients

IPsec offers security through the ISAKMP (Internet Security Association and Key Exchange Management Protocol) framework:

- By using the IKE (Internet Key Exchange) protocol to negotiate the parameters of secure communication, generate and manage keys, and establish SAs (Security Associations) between the communicating parties
- By encrypting data packets using symmetric encryption algorithms, such as AES, 3DES, CHACHA, that are negotiated by IKE with keys that are generated by IKE. See Phase 1 Configurations.
- By using HMAC (Hash-based Message Authentication Code) to verify the integrity of the message and ensure data in transit has not been tempered. See Phase 1 Configurations.
- By specifying key lifetimes and other security settings used in the SAs

IPsec offers flexibility in choosing the encryption and hashing algorithm as well as key lifetime intervals as opposed to SSL VPN, which negotiates the cipher suite between the client and server.

IKEv1 or IKEv2?

FortiGate supports IKEv1 and IKEv2, and both are configured similarly. The underlying protocol for IKEv2 is more streamlined, requiring fewer message exchanges to negotiate the SAs compared to IKEv1. The major difference is IKEv1 uses XAuth (Extended Authentication) for user authentication, and IKEv2 uses EAP (Extensible Authentication Protocol). IKEv2 also supports using TCP as transport enabling IPsec to negotiate over TCP, encapsulate ESP packets within TCP and operate on custom TCP port such as port 443.

IKEv1 is generally well used and well understood, with a more rigid protocol that is simpler to troubleshoot. Whereas IKEv2 offers more flexibility, resulting in more variations when troubleshooting.

However, starting with FortiClient 7.4.4, IKEv1 is no longer supported on the client. Therefore, plan accordingly when choosing your IKE version. Use IKEv2 if you plan on deploying FortiClient 7.4.4 and later.

Tunneling protocol and encapsulation

SSL VPN uses the TLS protocol for tunneling.

However, Fortinet's IPsec VPN offers the following options for tunneling and encapsulation:

- Native ESP
- UDP encapsulation
- TCP encapsulation with Fortinet proprietary extension
- TCP encapsulation using RFC 8229

When ESP is used without encapsulation, it connects directly over IP Protocol 50. When ESP is encapsulated within UDP, it uses UDP/500 and UDP/4500 for NAT traversal, which are the options for dialup IPsec VPN.

For remote access VPN tunnels, where FortiGate acts as dialup IPsec server for FortiClient endpoints, it is recommended to configure the IPsec tunnels using TCP as transport using a custom TCP port 443. This allows IPsec to encapsulate ESP packets within TCP and operate on TCP port 443, enabling ESP packets to traverse carrier networks where direct IPsec traffic is blocked or impeded by carrier-grade NAT. However, this feature requires using IKE version 2. See Dialup IPsec VPN using custom TCP port for more information. It also requires FortiClient 7.4.1 or later. For information on configuring custom TCP port on FortiClient, see IPsec VPN over TCP.

In IPsec site-to-site tunnels, the UDP port can be customized. See Configurable IKE port.

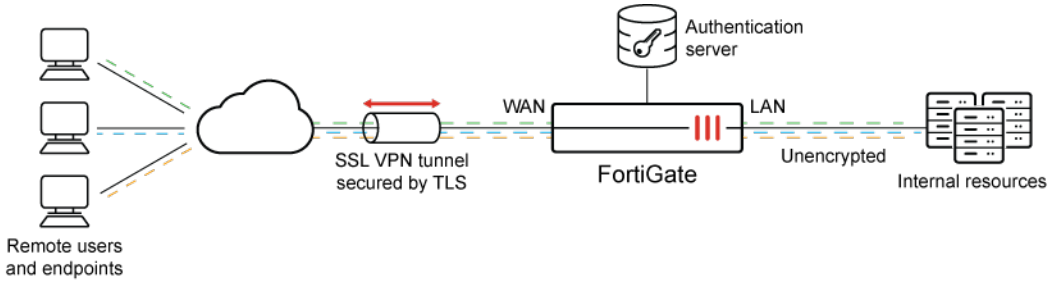
In IPsec site-to-site tunnels using IKEv2, the TCP port can also be customized. See Encapsulate ESP packets within TCP headers

Migration basics

Once you understand the differences between SSL VPN and IPsec VPN technologies, it is time to plan the migration. This section describes the following:

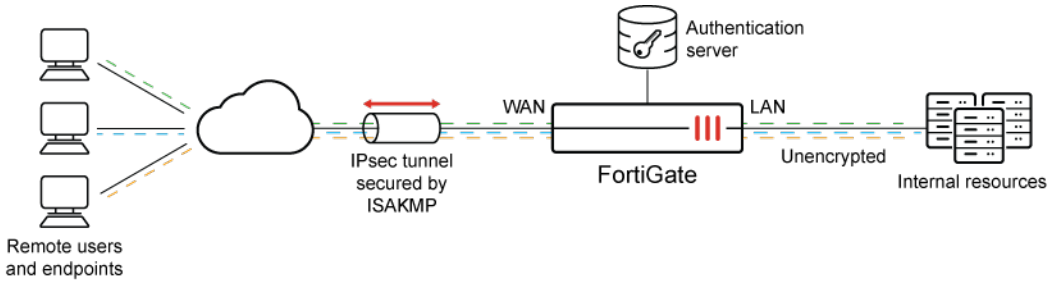
Design considerations

The following example diagram represents a common SSL VPN tunnel-mode topology:



Individual users connect from the internet to TCP port 443 on the WAN interface of the FortiGate for SSL VPN tunnel access. Each user must authenticate to be granted access and establish an SSL VPN tunnel. Once connected, traffic is encrypted and secured by TLS between the endpoint and the FortiGate WAN interface. Users can access internal resources based on the configured firewall policy for their user group.

In a dial-up IPsec VPN scenario, the topology will be generally the same.



Individual users connect from the internet to TCP port 443 on the WAN interface of the FortiGate for IPsec VPN access using IKE version 2 and will authenticate using the chosen method. IKE negotiation occur over TCP and the IKE port can be customized as needed. Once the IPsec tunnel is established, traffic is encrypted and secured by the ISAKMP protocol and ESP traffic is encapsulated within TCP header between the endpoint and the FortiGate WAN interface between the endpoint and the FortiGate WAN interface. Users can access internal resources based on the configured firewall policy for their user group.

In conclusion, no topology or port number changes are needed to migrate from SSL VPN to IPsec VPN and TCP port 443 can continue to be used.

Deciding on the IKE version is an important design consideration. In general, IKEv2 is recommended since TCP port 443 can be used.

In addition, starting with FortiClient 7.4.4, IKEv1 is no longer supported on the client. Therefore, use IKEv1 only if you do not require IKE over TCP, and you do not plan on deploying FortiClient 7.4.4 and later.

Also, FortiClient 7.4.4 does not support IPv6. Use FortiClient 7.4.6 or later.

Authentication method

In order to establish an SSL VPN tunnel, users must authenticate to a user group that is associated with SSL VPN in a user group to portal mapping. Authentication can be any of the following methods supported by the FortiGate:

SSL VPN Authentication Methods	Requirement
• PKI • Local • LDAP • RADIUS • SAML	Required to configure at least one of these user authentication methods
• Two-factor authentication	Optional

Two-factor authentication using FortiToken is also supported, and can work in combination with Local, LDAP, RADIUS or SAML authentication. Two-factor authentication with client certificate is also supported.

For IPsec tunnels, users can authenticate using pre-shared keys or certificates or through XAuth (Extended Authentication) in IKEv1 tunnels and EAP in IKEv2 tunnels. Authentication can be any of the following methods supported by the FortiGate:

Authentication Methods	IKE Version	Requirement
• Pre-shared key • PKI (Signature)	IKEv1 and IKEv2	Required to configure one of these user authentication methods
• LDAP	IKEv1 and IKEv2 (requires EAP-TTLS)	Optional user authentication methods. (IPsec IKEv1 uses XAUTH, and IPsec IKEv2 uses EAP for user authentication.)
• Local • RADIUS	IKEv1 and IKEv2	
• SAML	IKEv2	
• Two-factor authentication	IKEv1 and IKEv2	Optional

Pre-shared key and PKI authentication can be paired with any of the other user authentication methods. Two-factor authentication using FortiToken is also supported and can work in combination with Local, LDAP, RADIUS, or SAML authentication. Two-factor authentication with client certificate is also supported.

In conclusion, when migrating from SSL VPN to IPsec VPN, all authentication methods are supported and can be migrated. Users and user groups can be reused in the new IPsec configurations. Administrators must choose a pre-shared key or PKI certificate while configuring the IPsec tunnel as it is a required setting.

Multiple user groups

SSL VPN configurations use only one SSL VPN settings page and one SSL VPN interface. Multiple user groups can be configured and mapped to different portals, and granular access is controlled by the firewall policy.

In IPsec VPN, one dial-up VPN tunnel setting can accommodate one or more user groups by defining the group within the VPN settings or inheriting the groups from the firewall policy. See Using single or multiple user groups for user authentication for details. Unlike SSL VPN, administrators can also create individual dial-up VPN tunnels to accommodate the various feature your current SSL VPN tunnel mode web portals support for each user group(s).

When using multiple dial-up VPN tunnels, each tunnel with the same settings requires a unique peer ID in order for dial-up clients to engage the right tunnel when initiating a connection to the VPN gateway. In IKEv1, it is recommended to use aggressive mode to accommodate the peer ID field within the phase1 tunnel. Whereas for IKEv2, it is recommended to use Network ID field within Phase 1 tunnel. The Network ID setting cannot be configured on unmanaged or standalone FortiClient. For managed FortiClient, configuration of the Network ID is supported through FortiClient EMS starting with versions 7.2.6 and later or 7.4.1 and later.

When migrating from SSL VPN to IPsec VPN, use one of these methods to define your group settings.

Full tunneling versus split tunneling

Full tunneling forces all remote user traffic to go through the VPN; whereas, split tunneling allows administrators to specify the traffic destinations that go through VPN.

Both SSL VPN and IPsec VPN support split tunneling. By default, SSL VPN enables split tunneling based on the destination configured in the firewall policy. By default, IPsec disables split tunneling in custom configurations, but enables it in wizard configurations. When enabled, you must configure the network(s) to be included or excluded from routing through the tunnel.

Client address assignments

SSL VPN assigns addresses out of a pre-defined or custom IP range. Dialup IPsec VPN has many methods of address assignments. However, it is recommended to use `mode config` where the FortiGate acts as the IP addressing server. The `mode config` setting has many options for address assignments, ranging from manual IP address range to integration with a DHCP server.

Migrating from SSL VPN to IPsec VPN provides added flexibility in IP addressing. Use `mode config` and one of the addressing options that it provides.

Split DNS and DNS suffix

SSL VPN in tunnel mode supports the configuration of both split DNS and DNS suffix. For dial-up IPsec tunnels, the availability of these features depends on the IKE version in use.

- IKE version 1: Supports DNS suffix configuration but requires enabling unity-support in the Phase 1 configuration. See IPsec DNS Suffix.
- IKE version 2: Supports split DNS. See IPsec Split DNS.

When configuring your environment, consider reviewing the existing SSL VPN settings to determine the most suitable IKE version for your requirements.

Policy configurations

SSL VPN uses a single `ssl.root` tunnel interface as source within a firewall policy to control inbound access from endpoint clients. User groups must be defined within the policy to control user groups that are allowed access to the internal resources.

Conversely, IPsec VPN creates a virtual VPN interface using the name of each IPsec tunnel. The virtual tunnel interface(s) can be chosen as a source within a firewall policy to control inbound access from endpoint clients. User groups can be defined in the policy and inherited by the VPN tunnel configurations, or they can be defined individually in each tunnel configuration.

When migrating from SSL VPN to IPsec VPN, consider the changes to the firewall policies needed to accommodate user group configurations.

FortiClient or endpoint configurations

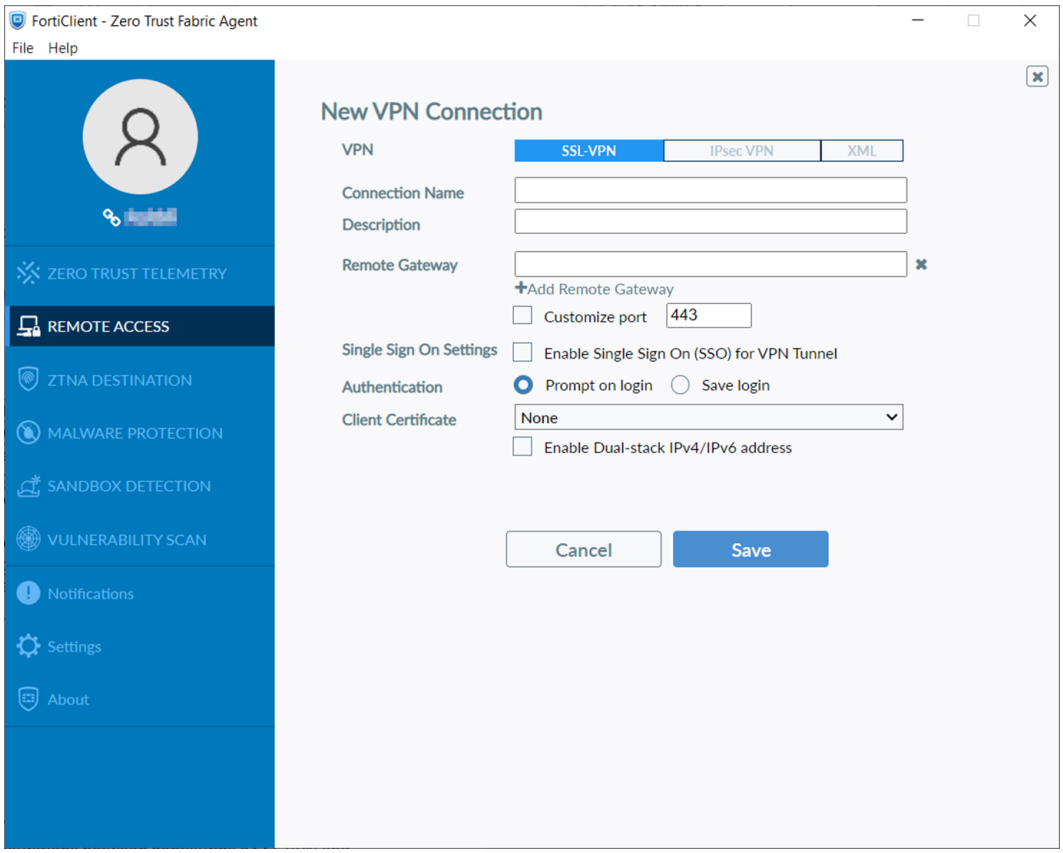
When connecting to SSL VPN in tunnel mode, endpoints must have FortiClient installed. Same is the case for IPsec tunnels.

FortiClient can be installed individually on endpoints or managed by FortiClient EMS. Using FortiClient EMS is preferred because it allows administrators to centrally manage their clients and easily scale their deployments. See FortiClient endpoint configuration migration on page 33 for more information.

A basic FortiClient SSL VPN configuration consists of:

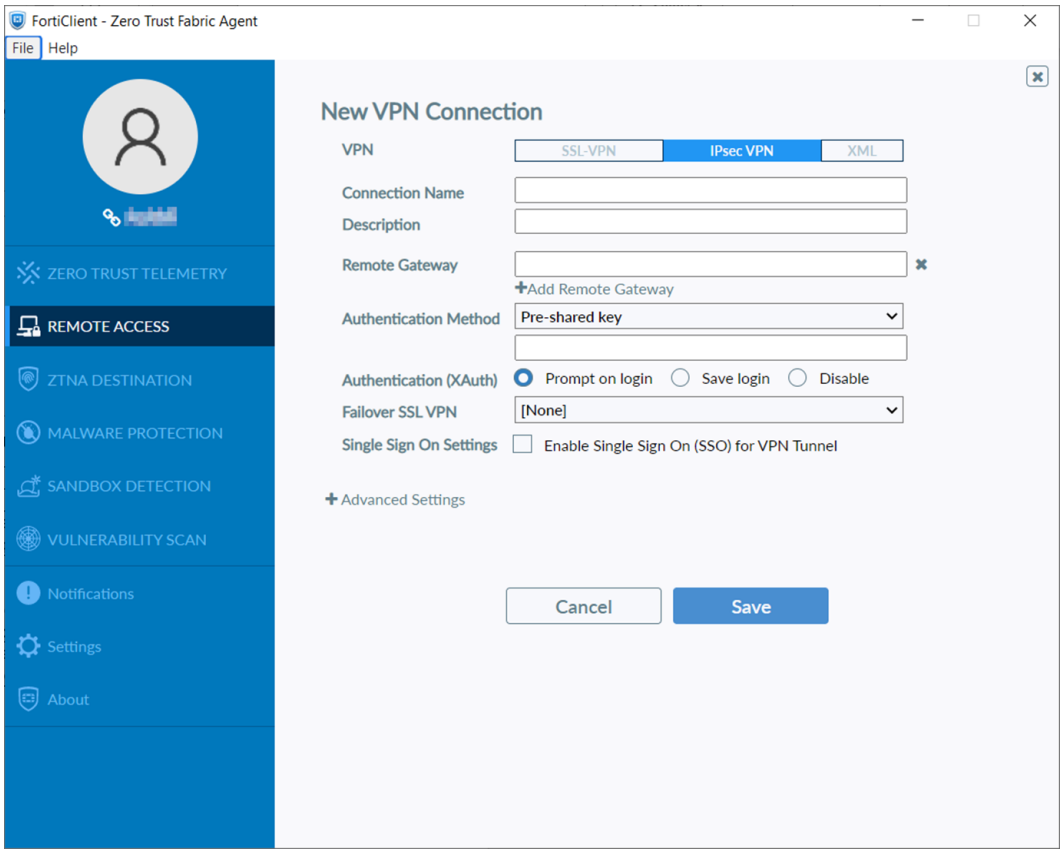
Connection name	Local name to identify the tunnel.
Remote Gateway	The address of the FortiGate SSL VPN interface.
Port	The listening port on the FortiGate. Defaults to TCP/443. Can be customized to another port.
Authentication	Supports manual entry of username/password each time to authenticate or a saved login. When single sign-on is enabled, users can perform SAML authentication using the embedded browser or through an external browser.

Client Certificate	When SSL VPN server requires a client certificate, FortiClient must supply the certificate to be used.



A basic FortiClient IPsec VPN configuration consists of:

Connection name	Local name to identify the tunnel.
Remote Gateway	The address of the FortiGate IPsec VPN gateway.
Authentication Method	Either a pre-shared key or X.509 client certificate.
Authentication (XAuth or EAP)	Supports manual entry of username/password each time to authenticate or a saved login.
Failover SSL VPN	Relevant only when using SSL VPN for redundancy. Set to *None* otherwise.
Single Sign On	Enable to use SAML authentication. This feature is available on FortiClient 7.2.4 and later.
Advanced Settings	Additional IPsec VPN settings such as: • IKE version • Main/Aggressive mode (for IKEv1) • Addressing mode • Phase1 options • Phase2 options



The *Advanced Settings* options include granular settings such as:

VPN Settings	• IKE version • Main/Aggressive mode (for IKEv1) • Encapsulation and IKE TCP port (for IKEv2) • Addressing mode • Phase1 options • Phase2 options
Phase 1	• IKE proposal – Encryption and Authentication algorithms • DH Group • Key Life • Local ID • Dead Peer Detection • NAT Traversal • Local LAN
Phase 2	• IKE proposal – Encryption and Authentication algorithms • Key Life • Replay Detection • Perfect Forward Secrecy (PFS) • DH Group

These settings must match the VPN settings configured on the FortiGate. For example, when multiple dial-up tunnels are configured on the FortiGate with peer ID enabled, the client must configure a local ID to match. On FortiClient, configure a local ID under *Phase 1* options.

VPN settings should be configured and centrally managed by FortiClient EMS and pushed to each endpoint when possible. From FortiClient EMS, create a new remote access profile for the IPsec tunnel to match the FortiGate tunnel setting. See FortiClient or endpoint configurations on page 11 for more information about IPsec configuration using FortiClient EMS.

Migrate VPNs before or after upgrade?

Deciding whether to migrate VPNs before or after an upgrade is a choice that administrators should make based on their company policies, best practices, and business impact. One consideration is to evaluate the potential downtime for remote users in either scenario.

Another factor to consider is whether the current firmware impacts security. If a security patch is critical, administrators may decide to upgrade before migrating their VPN.

Finally, it takes time to carefully assess the design considerations, create a plan, execute and test configurations in a controlled manner, and then deploy changes to users. Give yourself time to plan accordingly. Schedule your upgrade and maintenance only after you decide on an approach.

FortiOS SSL VPN to dial-up VPN migration

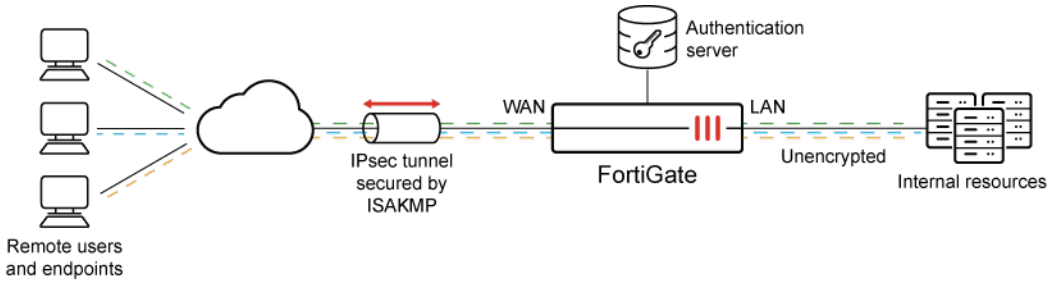
Once you understand the design considerations, you can migrate the configurations based on your preferences. We recommend taking a two-part approach:

- First, analyze the user authentication method(s) that are used in your current SSL VPN setup. Understand any conditions that may require you to choose between different IPsec VPN implementations.
- Next, configure your IPsec tunnel settings using the VPN wizard. Further customization may be needed to complete the configuration for specific setups.

The following sections will guide you through these steps:

Topology

The examples in this migration guide use the following topology:



It is assumed that SSL VPN is preconfigured on the WAN interface of the FortiGate using TCP/443, and the remote users connect to the WAN interface to access internal resources hosted behind the FortiGate's LAN interface.

This SSL VPN configuration will be migrated to IPsec using the same basic topology.

Part 1: Identifying user authentication methods

In Part 1, we identify the user authentication methods currently used in your SSL VPN configuration. For each method, we outline any restrictions and limitations related to using those methods for IPsec.

User authentication methods on FortiGate require configuration of either users or user groups. These user groups make use of different authentication servers, such as RADIUS, LDAP, and SAML inside their configuration. These preconfigured objects can generally be used in the IPsec VPN configurations without further modifications.

Follow these steps to identify the user authentication method currently used in your SSL VPN configuration. If you already know the authentication method, you can skip these steps and go to Next steps after identifying the authentication method on page 16.

To identify the user authentication method currently used in SSL VPN configurations:

1. Locate the user group(s) used in SSL VPN firewall policies:
   a. Go to *Policy & Object* > *Firewall Policy*.
   b. Edit the firewall policy that has SSL-VPN tunnel interface (*ssl.root*) in the *Incoming interface* field.
   c. Note the user groups used in the *Source* field inside the firewall policy.
   d. Perform the same step for all SSL VPN firewall policies to get a list of user groups used for SSL VPN user authentication.
2. Identify the configured authentication method for SSL VPN:
   a. Go to *User & Authentication* > *User Groups*, and edit the group(s).
   b. Use the following statements to help you identify the configured authentication method:

If the configuration shows	Your authentication method is
Local users configured under *Member* with no configuration under *Remote Groups* > *Remote Server*	Local user authentication
Remote Groups > *Remote Server*, uses *LDAP Server*	LDAP-based user authentication

If the configuration shows	Your authentication method is
Remote Groups > *Remote Server*, uses *RADIUS Server*	RADIUS-based user authentication
Remote Groups > *Remote Server*, uses *SAML SSO Server*	SAML-based user authentication
PKI users are configured under *Member*: • If *Remote Group* > *Remote Server* uses *LDAP Server*, then you are using Certificate-based user authentication with LDAP as two-factor authentication. • If *Remote Group* > *Remote Server* uses *RADIUS Server*, then you are using Certificate-based user authentication with RADIUS as two-factor authentication.	Certificate-based user authentication Note: This guide does not demonstrate how to migrate certificate-based user authentication. See IKEv1 and IKEv2 for more information.

Next steps after identifying the authentication method

Based on the identified authentication method, go to the following topics to find more information about migrating the authentication method to IPsec VPN as well as specific IPsec IKE version support requirements, if any:

- Local user authentication on page 16
- LDAP-based user authentication on page 17
- RADIUS-based user authentication on page 19
- SAML-based user authentication on page 20

After reviewing the authentication method, move to Part 2, which outlines configuring IPsec tunnel using VPN wizard and makes use of user groups discussed in Part 1.

Local user authentication

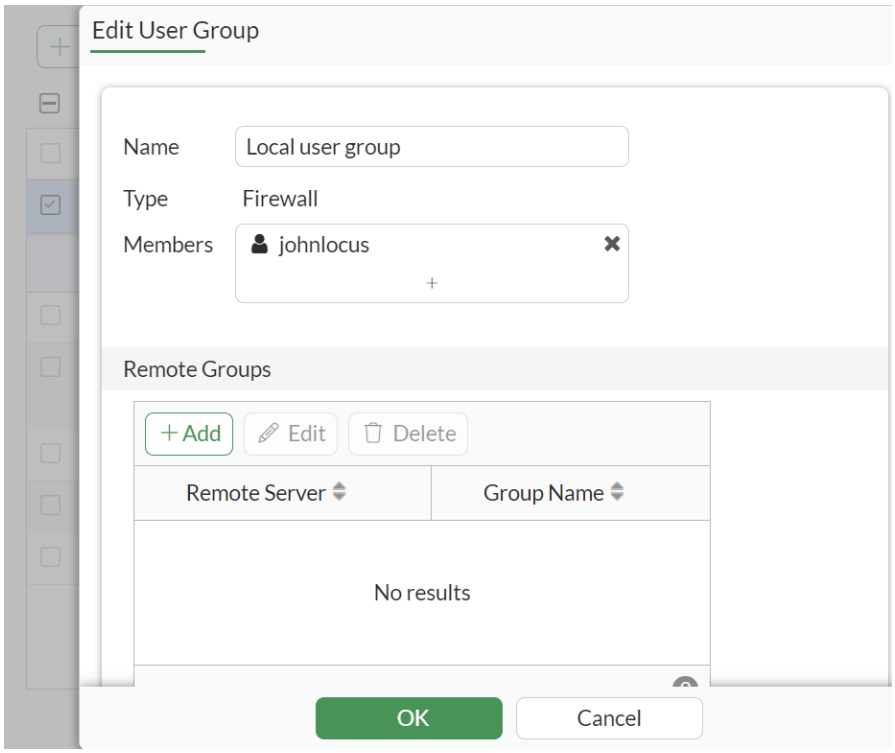
In local user authentication, username and password are configured locally on FortiGate for each user. You can then configure local user groups to contain multiple local users. See Users to configure a local user, and see User groups to configure user groups.

This example configuration shows a local user with username *johnlocus* added to local user group named *Local user group*.

To view the configuration in the GUI:

1. Go to *User & Authentication* > *User Groups*.
2. Find the user group that you previously identified in the policy configuration, and double-click to see the details.

   In this example, the member *johnlocus* is displayed.



To view the configuration in the CLI:

```
config user group
    edit "Local user group"
        set member "johnlocus"
    next
end
```

Applying the user group

The user group named *Local user group* can be used inside the IPsec tunnel configuration, if you have a single user group. If you have multiple user groups, they can be used inside firewall policies, after configuring *Inherit from policy* on the IPsec tunnel. See Part 2: Configuring IPsec tunnels using the VPN wizard on page 23.

LDAP-based user authentication

IPsec IKEv1 uses XAUTH for user authentication, and IPsec IKEv2 uses EAP for user authentication. Only EAP-TTLS is interoperable with LDAP. For LDAP based user authentication with IKE version 2, EAP-TTLS must be used. EAP-TTLS support is only supported on FortiClient EMS & FortiClient version 7.4.3 and later, see EAP-TTLS support for IPsec VPN.

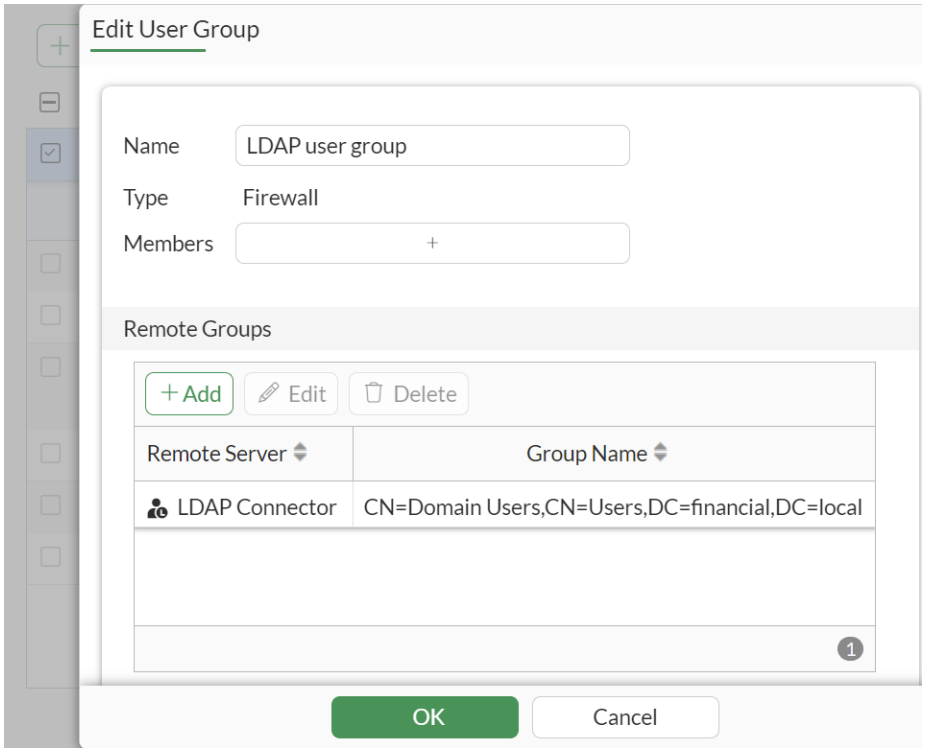
In LDAP-based user authentication, LDAP server acts as a centralized authentication server. Thus, usernames and passwords must be directly managed on the LDAP server. To use this authentication method for IPsec, FortiGate requires a configured LDAP server and user group that uses LDAP server. Optionally, to segregate user groups based on user's LDAP group membership to perform group matching, you can configure multiple user groups and use group name option.

See Configuring an LDAP server to configure an LDAP server. See Tracking users in each Active Directory LDAP group to configure group matching.

This example configuration shows an LDAP server named *LDAP Connector* that is used inside a user group named *LDAP user group*. The *Group Name* setting matches only users belonging to the LDAP group called *Domain Users* on the LDAP server. Only users belonging to *Domain Users* are allowed to connect to the IPsec tunnel.

To view the configuration in the GUI:

1. Go to *User & Authentication* > *User Groups*.
2. Find the user group that you previously identified in the policy configuration, and double-click to see the details.
   The *Remote Group* displays an LDAP server connector.



To view the configuration in the CLI:

```
config user group
    edit "LDAP user group"
        set member "LDAP Connector"
        config match
            edit 1
                set server-name "LDAP Connector"
                set group-name "CN=Domain Users,CN=Users,DC=financial,DC=local"
            next
        end
    next
end
```

Applying the user group

The user group named *LDAP user group* can be used inside the IPsec tunnel configuration, if you have a single user group. If you have multiple user groups, they can be used inside firewall policies, after configuring *Inherit from policy* on the IPsec tunnel. Be sure to change IKE version to version 2. See Part 2: Configuring IPsec tunnels using the VPN wizard on page 23.

RADIUS-based user authentication

In RADIUS-based user authentication, the RADIUS server is used as a centralized authentication server. Thus, usernames and passwords must directly be managed on the RADIUS server. To configure a RADIUS server on FortiGate, see Configuring a RADIUS server.

To use this authentication method for IPsec, FortiGate requires a configured RADIUS server and a user group that references the RADIUS server.

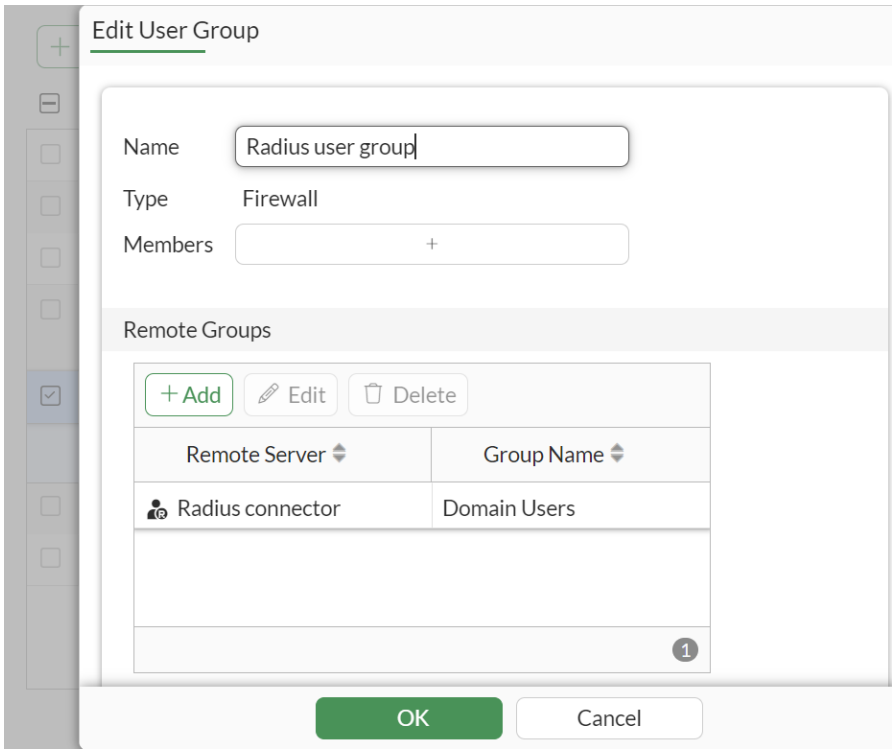
Optionally, to segregate user groups based on user's group membership on RADIUS server, you can use the *Group Name* option. FortiGate expects the RADIUS server to be configured correctly to return the correct RADIUS attribute (that is, Fortinet-Group-Name VSA) in RADIUS response packet. See Restricting RADIUS user groups to match selective users on the RADIUS server.

In this example configuration, FortiGate is configured with RADIUS server named *Radius Connector*, and a user group called *Radius user group* references the RADIUS server. The group name option is configured to only allow the user to connect to IPsec tunnel, if RADIUS server returns *Domain Users* in the RADIUS response packet to FortiGate.

To view the configuration in the GUI:

1. Go to *User & Authentication* > *User Groups*.
2. Find the user group that you previously identified in the policy configuration, and double-click to see the details.

   The *Remote Group* displays a RADIUS server connector.



To view the configuration in the CLI:

```
config user group
    edit "Radius user group"
        set member "Radius Connector"
        config match
            edit 1
                set server-name "Radius Connector"
                set group-name "Domain Users"
            next
        end
    next
end
```

Applying the user group

The user group named *Radius user group* can be used inside the IPsec tunnel configuration, if you have a single user group. If you have multiple user groups, they can be used inside firewall policies, after configuring *Inherit from policy* on IPsec tunnel. See Part 2: Configuring IPsec tunnels using the VPN wizard on page 23.

SAML-based user authentication

IPsec supports SAML-based user authentication on FortiClient version 7.2.4 and later. SAML authentication is only supported on IPsec IKEv2. IPsec IKEv1 is not supported.

Ensure to upgrade FortiClient to version 7.2.4 or later. See Deployment & Installers to upgrade FortiClient using FortiClient EMS.

Part 2 of this guide uses the VPN wizard to configure IPsec. By default, the VPN wizard configures IKE version 1. The configuration is then later customized to use IKE version 2 along with enabling EAP for user authentication.

For SAML to work with IPsec, it needs additional configuration of `auth-ike` SAML port, SAML sever certificate, and interface binding between interface used by IPsec VPN gateway and SAML server. For end-to-end configuration example on deploying SAML with IKEv2 using different IdPs, review SAML-based authentication for FortiClient remote access dialup IPsec VPN clients.

This example configuration demonstrates the additional SAML configurations needed. The configuration is based on using FortiAuthenticator as the SAML IdP.

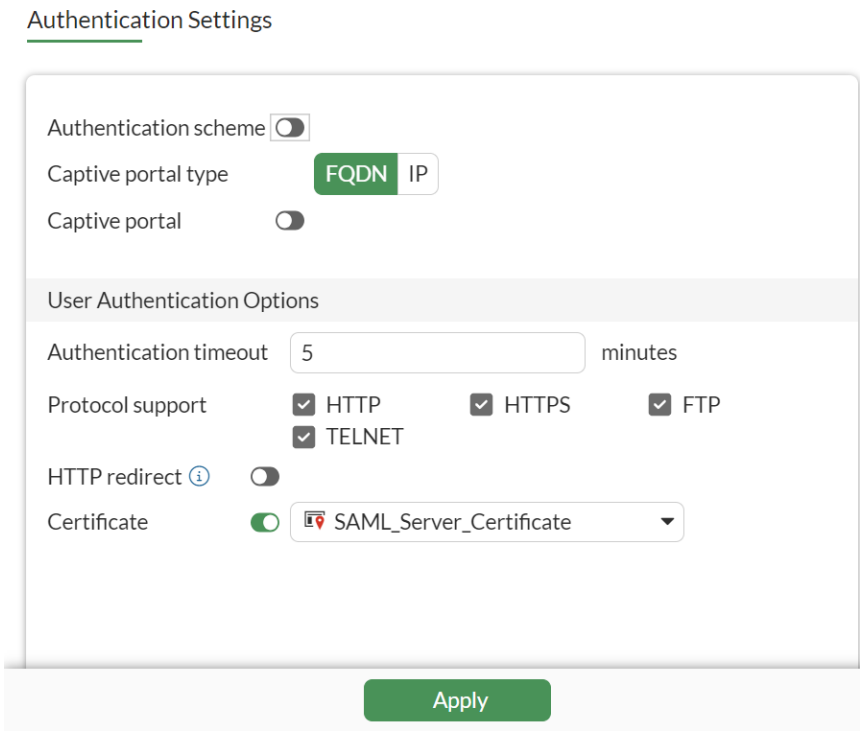
To configure and view the auth-ike-saml-port used for authentication in the CLI:

You can only configure and view this setting in the CLI.

```
config system global
    set auth-ike-saml-port 9443
end
```

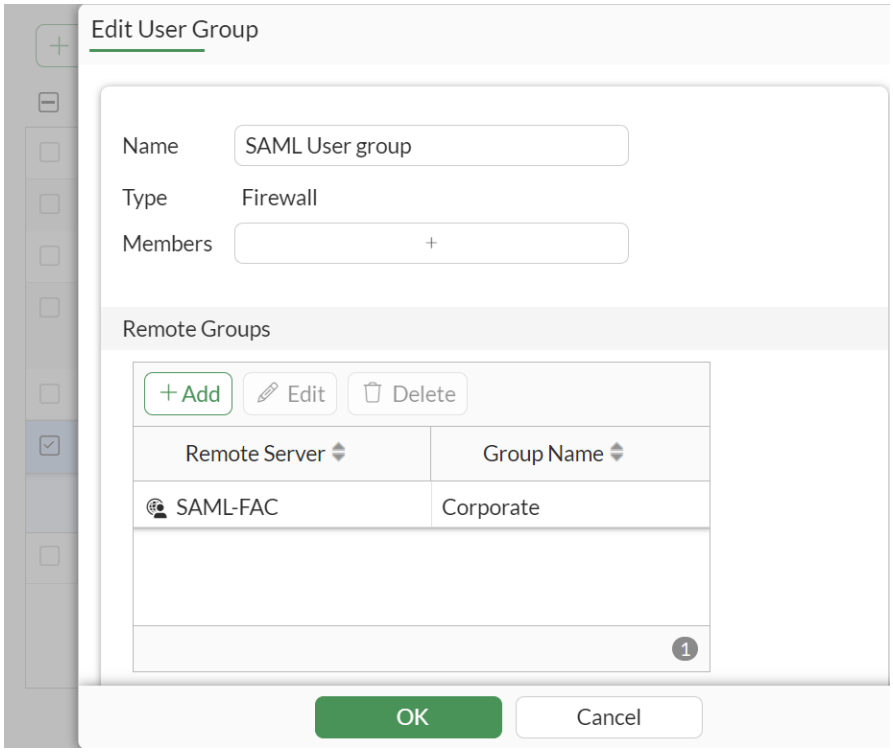
To configure and view the SAML certificate in the GUI:

1. View the SAML server certificated configured for use with SAML.
   a. Go to *User & Authentication* > *Authentication Settings*.
   b. Enable *Certificate*, and select your SAML server certificate.



To view the SAML User Group in the GUI:

1. Go to *User & Authentication* > *User Groups*.
2. Find the user group that you previously identified in the policy configuration, double-click to see the details. The *Remote Groups* display the SAML SSO server.



To configure and view the SAML configurations in the CLI:

1. View SAML server certificate uploaded as `SAML_Server_Certificate`.

```
config user setting
    set auth-cert "SAML_Server_Certificate"
end
```

2. View the SAML user group named `SAML User group` that uses the SAML SSO server named `SAML-FAC`.

```
config user group
    edit "SAML User group"
        set member "SAML-FAC"
        config match
            edit 1
                set server-name "SAML-FAC"
                set group-name "Corporate"
            next
        end
    next
end
```

To configure the binding between the SAML server and the interface on which IPsec gateway is configured:

1. Configure the binding between the SAML server and interface on which IPsec gateway is configured. This configuration can only be performed and viewed using the CLI.

```
config system interface
    edit "WAN"
        set ike-saml-server "SAML-FAC"
    next
end
```

Applying the user group

The user group named *SAML User group* can be used inside the IPsec tunnel configuration, if you have a single user group. If you have multiple user groups, they can be used inside firewall policies, after configuring *Inherit from policy* on IPsec tunnel. See Part 2: Configuring IPsec tunnels using the VPN wizard on page 23.

Part 2: Configuring IPsec tunnels using the VPN wizard

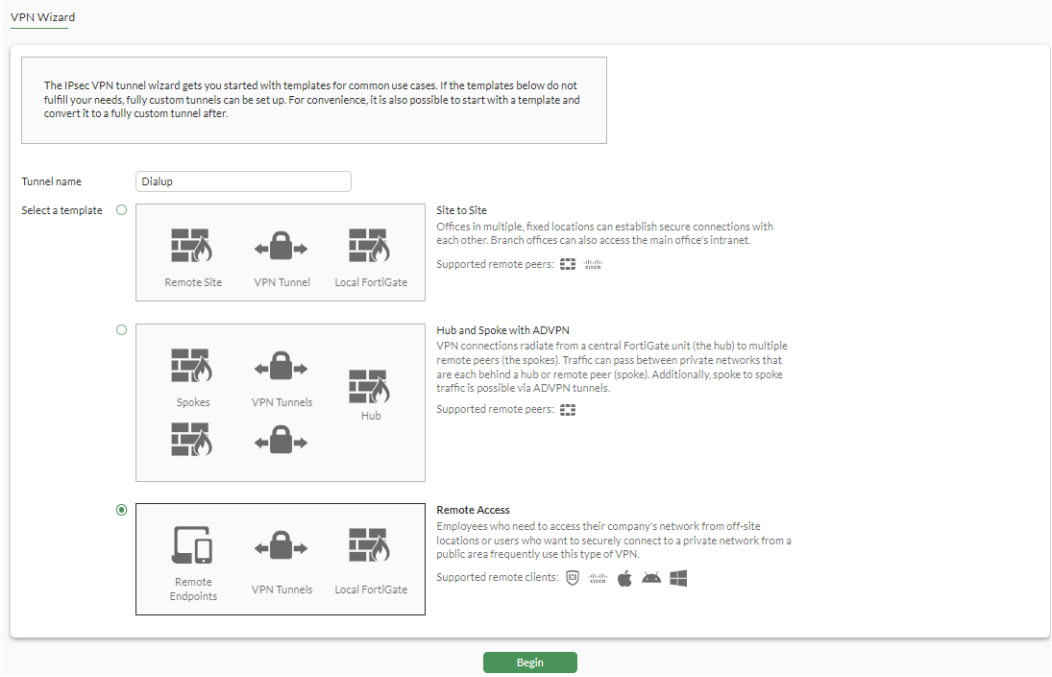
After reviewing user authentication methods used in your current SSL VPN configuration and comparing it with IPsec authentication methods discussed in Part 1: Identifying user authentication methods on page 15, you can now migrate SSL VPN to IPsec VPN.

IPsec tunnels can be configured using either the VPN wizard in the GUI, or a custom IPsec configuration in the GUI or CLI. In this guide, the VPN Wizard is used to configure IPsec tunnels. The settings specified in the VPN wizard for configuring the IPsec tunnel can also be customized later to modify the IKE version, the IKE mode, or to specify custom security associations (SAs) and other granular settings.

To configure IPsec using the VPN wizard:

1. On FortiGate, go to *VPN* > *VPN Wizard*. The *VPN Wizard* opens.
2. Set the following options, and click *Begin*:

Tunnel name	Enter a name for the VPN tunnel. The name can be a maximum of 15 characters.
Select a template	Select *Remote Access*.



3. In the *VPN tunnel* section, set the following options, and click *Next*:

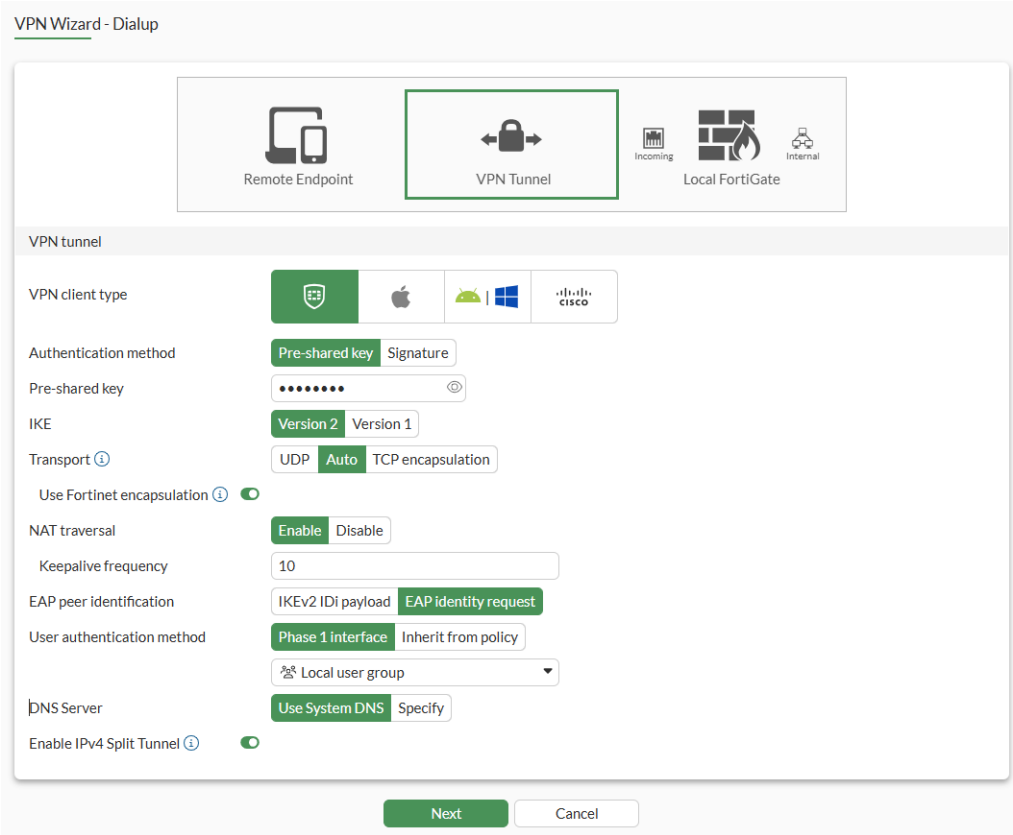
VPN client type	Select *FortiClient*. If you have other VPN clients installed on endpoints choose from: *iOS*, *Android/Windows*, and *Cisco*.

Authentication method	Choose between the following options:
	• *Pre-shared key*: create a unique pre-shared key. The key must be shared among all FortiClient endpoints to connect to VPN.
	• *Signature*: Used to authenticate remote users to IPsec gateway using their user certificates.
	  • Set *Certificate Name* to the server certificate used to identify the VPN Gateway.
	  • Set *Peer Certificate CA* to the CA certificate that signed certificates for FortiClient endpoints.
	  Both the server certificate (*Certificate name*) and peer CA (*Peer Certificate CA*) certificates must be uploaded to FortiGate.
	For more information about the certificates, see Importing the certificates from Dialup IPsec VPN with certificate authentication.

IKE	Select IKE version 2 or 1 based on your requirements. To enable using TCP as transport, set IKE version to 2. Note that the supported user authentication methods vary based on the IKE version, see Authentication method on page 9. Note also that starting with FortiClient 7.4.4, IKEv1 is no longer supported on the client.
Transport	Select from the following: • *UDP*: Use UDP transport for IKE.

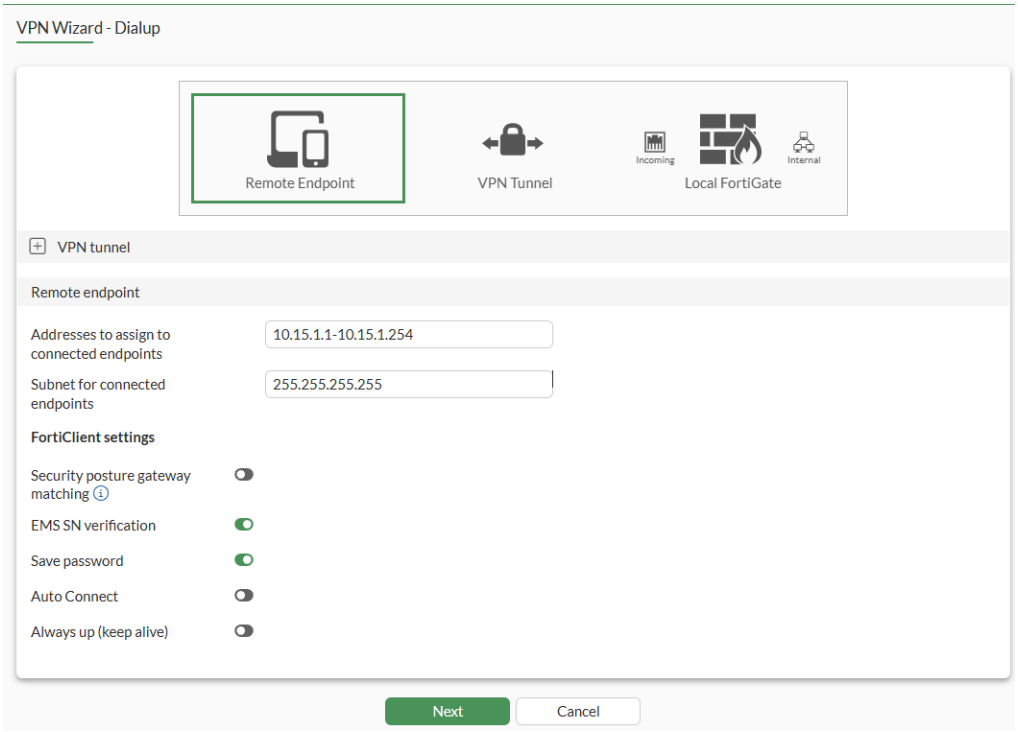
	• *Auto*: Use UDP transport for IKE, with fallback to TCP transport. • *TCP encapsulation*: Use TCP transport for IKE. This option is only available when using IKE version 2. For encapsulating traffic within TCP header, the option *TCP encapsulation* will be selected in later steps. For more information on using custom TCP ports when TCP is used as transport, see Using TCP as transport method on page 29.
Use Fortinet encapsulation	• Enabled: Enables Fortinet TCP encapsulation that is an alternative to and compliant with RFC 8229, allowing NP8 inline offload of IPsec traffic. • Disabled: Uses TCP encapsulation based on RFC 8229 as per configured transport setting. This option is only available when using IKE version 2 and *Transport* is set to *Auto* or *TCP encapsulation*. Keep this option *Disabled* as FortiClient does not support Fortinet Inc. encapsulation.
NAT traversal	• *Enable*: This option is used when there is a NAT device between FortiGate and VPN clients. It enables NAT-T Discovery and Traversal if NAT device is detected. • *Disable*: Disables NAT-T Discovery. • *Forced*: Enables NAT-T and forces to use UDP port 500 for ESP encapsulation. This option is only available when using IKE version 1.
Keepalive frequency	Keepalives keep the IPsec tunnel active by sending probes regularly per the configured frequency, but only if the IPsec tunnel is idle and no traffic is flowing through it. These probes prevent the NAT port session mappings on the intermediate NAT devices in the ISP network from timing out. It is set to 10 by default. This option is only available when *NAT traversal* is set to *Enabled* or *Forced*.
EAP peer identification	To perform user authentication using EAP, select *EAP identity request*. This option is only available when using IKE version 2.
User authentication method	When *Authentication* is set to *Pre-shared key*, select the user group to perform user authentication. Review the different types of user authentication methods available for IPsec: • Local user authentication on page 16 • LDAP-based user authentication on page 17 • RADIUS-based user authentication on page 19 • SAML-based user authentication on page 20 When using IKE version 1 and *Authentication method* is set to *Signature*, the *User authentication method* setting is optional. Select a user group if you want to perform username and password authentication along with certificate authentication.

	Single User groups: If your current SSL VPN Authentication/Portal Mapping uses a single user group for user authentication, select *Phase 1 interface* then select the user group from the drop-down. Multiple User groups: If your current SSL VPN Authentication/Portal Mapping uses multiple user groups for user authentication, select *Inherit from policy setting* then select the user groups. The specified user groups are automatically added under User/group fields in the respective IPsec firewall policies configured by the VPN Wizard.
DNS Server	Select either: • *Use System DNS*: enables FortiClient to use its own DNS server. • *Specify*: lets you specify a unique DNS server. Note: If split tunneling is enabled, and the specified DNS server is located behind FortiGate, ensure the DNS server is reachable through the *Local interface* and is part of *Local Address* field IP scope.
Enable IPv4 Split Tunnel	When enabled, only traffic configured in the *Local address* field will go through the tunnel (that is, split tunneling). When disabled, all traffic from remote users will go through the tunnel (that is, full tunneling).



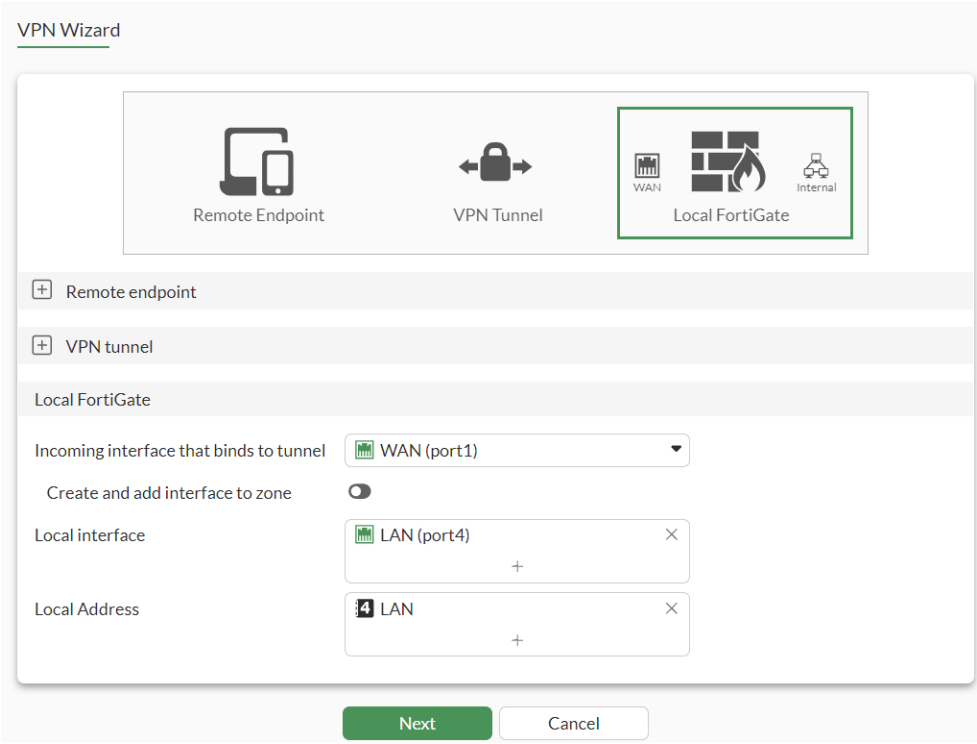
4. In the *Remote Endpoint* section, set the following options, and click *Next*:

Addresses to assign to connected endpoints	Enter the IP address range that you need to assign IP addresses from to the dialup clients that successfully connect to IPsec VPN. The VPN wizard only configures tunnels using `mode-config` and address range. To use other methods, you can customize the settings after the IPsec tunnel is configured by the VPN Wizard. See IKE Mode Config clients. (Optional) You can use different address ranges from your current SSL VPN configurations to avoid IP overlap.
Subnet for connected endpoints	255.255.255.255 Enter the subnet mask to be used by the clients. It is recommended to configure it as 255.255.255.255 since addresses are assigned to single clients.
FortiClient settings	
Security posture gateway matching	Enable and select the required *Security posture tags*. See Augmenting VPN security with ZTNA for more information.
Save Password	Enable saving XAuth username and password on the VPN clients. Enabled by default. CLI setting is `set save-password enable`.
Auto Connect	Allow the client to bring the tunnel up when there is no traffic. Disabled by default. CLI setting is `set client-auto-negotiate disable`.
Always up (keep alive)	Allow the client to keep the tunnel up when there is no traffic. Disabled by default. CLI setting is `set client-keep-alive disable`.



5. In the *Local FortiGate* section, set the following options, and click *Next*:

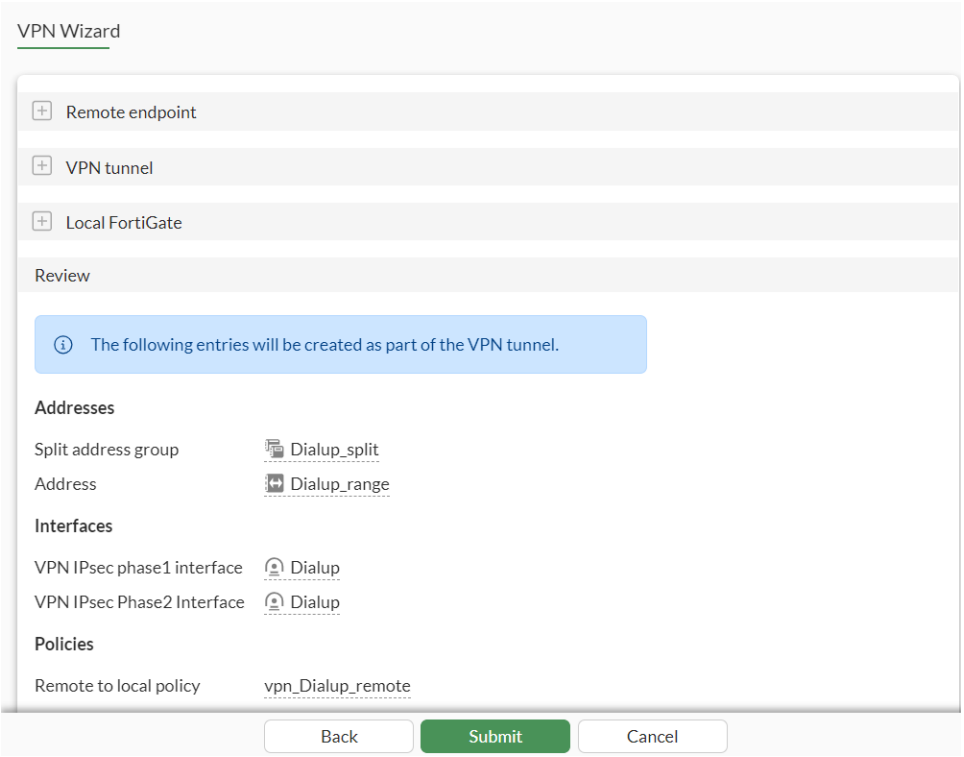
Incoming interface that binds to tunnel	This interface is the same *Listen on interface* as defined in your SSL VPN settings.
Create and add interface to zone	Enable if the requirement is to segregate incoming interfaces into different zones. See Zones. If not, disable.
Local interface	This is the internal interface(s) that will be accessed by VPN users. The equivalent SSL VPN configurations are the destination interface(s) in the ssl.root to <destination> firewall policies.
Local address	These are internal network(s) that are allowed to be accessed by VPN users. The equivalent SSL VPN configurations are the destination address(es) in the ssl.root to <destination> firewall policies. The subnet specified in the *Local Address field* is used for split tunneling if the setting *Enable IPv4 Split Tunnel* is enabled in the *VPN tunnel* section of the VPN Wizard.



6. In the *Review* section, review the configurations and objects, and then click *Submit*:

Addresses	
Split address group	Address group for the destination address(es) allowed by the tunnel. Used for split tunneling configurations.
Address	Firewall address for the range defined for VPN clients.

Interfaces	
VPN IPsec phase 1 interface	IPsec Phase 1 tunnel name and configuration.
VPN IPsec phase 2 interface	IPsec Phase 2 tunnel name and configuration.
Zone	Name of the zone created for IPsec tunnel, if *Zone* creation was enabled.
Policies	
Remote to local policies	Name of inbound firewall policy or policies.
Peer	Name of PKI user configured, if selected authentication method is *Signature*.



The VPN wizard generates all required configurations, objects, and policies. Go to *VPN > IPsec tunnels* to view the newly created IPsec tunnels.

Using TCP as transport method

Dialup IPsec VPN, traditionally reliant on UDP, can now operate over TCP using default port 443. This enhancement enables VPN traffic from FortiClient to traverse restrictive firewalls that permit only TCP-based traffic. This feature is only available if the IPsec tunnel is configured to use IKE version 2. FortiClient must be also configured to use TCP as its transport. The supported FortiClient version for this feature is FortiClient version 7.4.1 or later. For more information on configuring custom TCP port on FortiClient, see IPsec VPN over TCP.

To configure TCP as transport in the GUI:

1. Go to *VPN > IPsec Tunnels* and edit the respective IPsec tunnel.
2. Confirm that *IKE* is set to *Version 2*.
3. Set *Transport* to *TCP encapsulation*.
4. Click *OK*.

To configure TCP as transport in the CLI:

See Connecting to the CLI for information about connecting to the CLI.

```
config vpn ipsec phase1-interface
    edit <tunnel-name>
        set transport tcp
    next
end
```

To view and modify TCP port used by IKEv2 in the CLI:

1. Check the default TCP IKE port used by FortiGate:

```
# show full-configuration system settings | grep ike-tcp
    set ike-tcp-port 443
```

2. (Optional) To change the default TCP port to use a custom port, such as 5500:

```
config system settings
    set ike-tcp-port 5500
end
```

Variable	Description
`ike-tcp-port <port>`	Set the TCP port for IKE/IPsec traffic (1 - 65535, default = 443).

When using TCP port 443 for IKE/IPsec traffic, GUI access can be affected for interfaces that are bound to an IPsec tunnel when the GUI admin port is also using port 443. To ensure continued functionality, change either the IKE/IPsec port or the administrative access port.

To change the administrative access port:

```
config system global
    set admin-sport <port>
end
```

For port conflicts with ZTNA and SSL VPN, ZTNA and SSL VPN will take precedence. To avoid any port conflicts with other services, review the FortiOS Ports guide for other incoming ports used on the FortiGate.

Next steps

You may need to edit the IPsec tunnel settings created by the VPN wizard, depending on your requirements. For further customization, see Customizing IPsec tunnel settings on page 31.

Customizing IPsec tunnel settings

You may need to edit the IPsec tunnel settings created by the VPN wizard, depending on your requirements. This section includes the following optional procedures:

Using peer ID

If multiple dialup IPsec tunnels are configured on same physical (WAN) interface, FortiGate uses a peer ID or Network ID to differentiate between incoming IPsec connection attempts and to associate the connection to the correct IPsec tunnel. As such, it is important to configure a unique peer ID or Network ID for each IPsec tunnel.

The peer ID can be used to differentiate between multiple dialup IPsec tunnels when using IKE version 1 in *Aggressive* mode. Thus, for IKEv1, it is recommended to use aggressive mode to accommodate the peer ID field within the phase1 tunnel.

When using IKE version 1 in *Aggressive* mode, during the IPsec negotiation process, FortiClient transmits its configured local ID, which FortiGate matches against the defined peer IDs to identify the appropriate tunnel. Therefore, local ID configured on FortiClient must align with the corresponding peer ID set on FortiGate to successfully establish an IPsec tunnel.

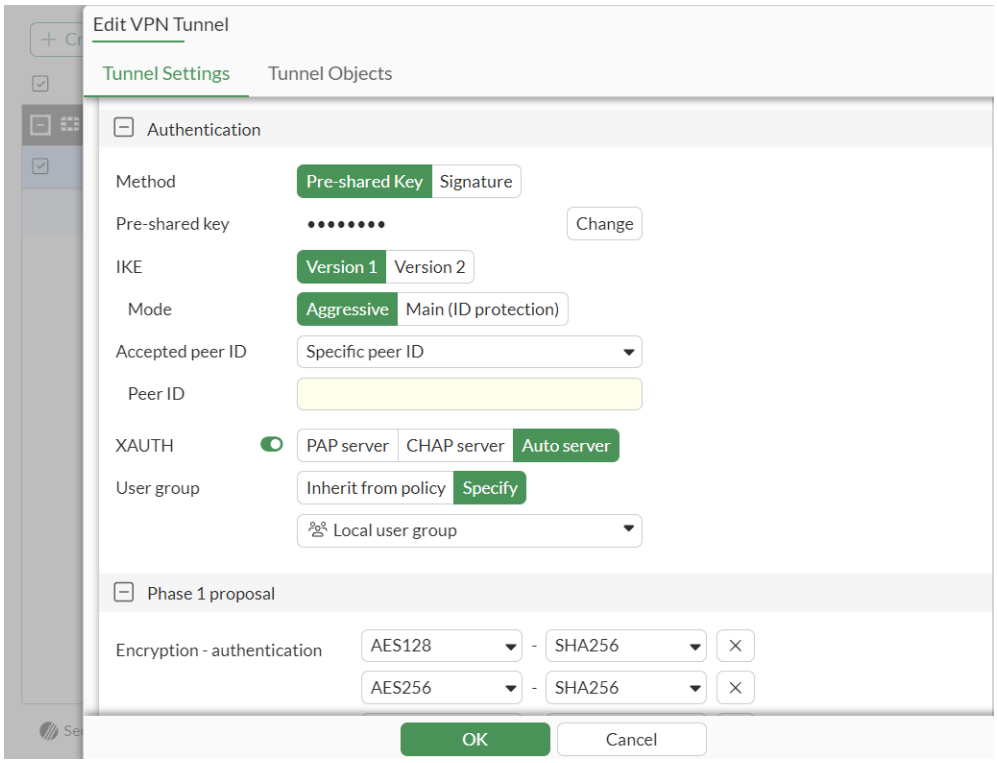
However, peer ID functionality is limited with IKE version 2 because the peer ID is not included in the initial IKE message. As a result, FortiGate as IPsec dialup server is unable to accurately match the correct phase 1 configuration among multiple dialup IPsec tunnel configurations. Thus, for IKEv2, it is recommended to instead use Network ID field within Phase 1 tunnel. The Network ID setting cannot be configured on unmanaged or standalone FortiClient. For managed FortiClient, configuration of the Network ID is supported through FortiClient EMS starting with versions 7.2.6 and later or 7.4.1 and later.

In IKE version 2, FortiGate utilizes Network ID as unique identifiers to distinguish between multiple dialup tunnels configured on the same WAN interface. During the IPsec negotiation process, FortiClient transmits its configured Network ID, which FortiGate matches against its defined Network IDs to identify the appropriate tunnel. The Network ID configured on FortiClient must align with the corresponding Network ID set on FortiGate to successfully establish an IPsec tunnel.

A unique peer ID or Network ID must be configured on different IPsec tunnels.

To configure a Peer ID or Netowkr ID on each IPsec tunnel for each user group:

1. Go to *VPN* > *IPsec Tunnels* and edit the respective IPsec tunnel.
2. Confirm that *IKE* is set to *Version 1* and *Mode* is set to *Aggressive*.
3. Under *Authentication*, change *Accept Peer ID* to *Specific peer ID*:



4. Set *Peer ID* to a unique peer ID of your choice.
5. Click *OK*.
6. Similarly, for IPsec tunnel configured with IKEv2, the Network ID can be configured via the CLI using following commands:

```
config vpn ipsec phase1-interface
    edit <vpn-tunnel-name>
        set network-overlay enable
        set network-id <ID>
    next
end
```

Changing Phase1 and Phase2 proposals

To change Security Associations in Phase 1 and Phase 2 of IPsec tunnel:

1. Go to *VPN* > *VPN Tunnels*, and edit the IPsec tunnel.
2. Under *Phase 1 proposal*, select required custom configuration.
3. Under *Phase 2 Selectors*, select the phase 2 tunnel, and click *Edit*.
4. Select the required custom configuration, and click *OK* to save the changes to the phase 2 selectors.
5. Click *OK* to save the changes on the IPsec tunnel.

FortiClient endpoint configuration migration

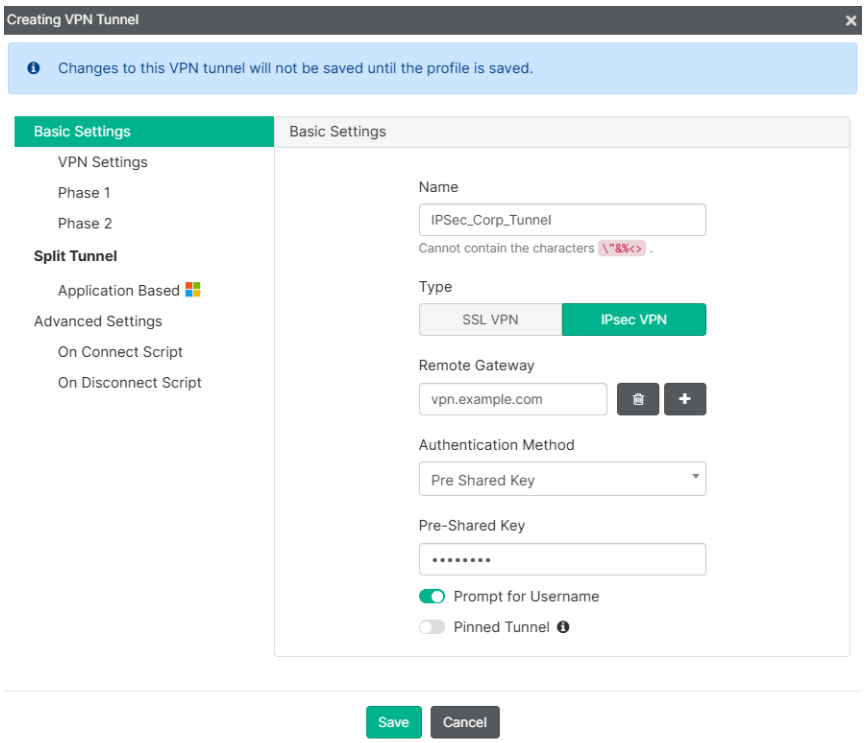
Migration from SSL VPN to IPsec on FortiClient EMS must be done in parallel with FortiGate configuration since IPsec settings have to be matched on both FortiGate (VPN server) and FortiClient (VPN client). On FortiClient EMS, VPN configuration is accomplished through the Remote Access endpoint profile, which enables setting up either SSL VPN or IPsec or both. See FortiClient EMS Remote Access documentation. This migration guide uses FortiClient EMS and FortiClient version 7.4.4 for demonstrating the steps.

To get started, add a remote access profile under the *Endpoint Profiles* section on FortiClient EMS. See Creating a new profile.

Once new Remote Access profile is added, add tunnel under the VPN Tunnels section within the same Remote Access profile context.

To migrate using a FortiClient EMS Remote Access endpoint profile:

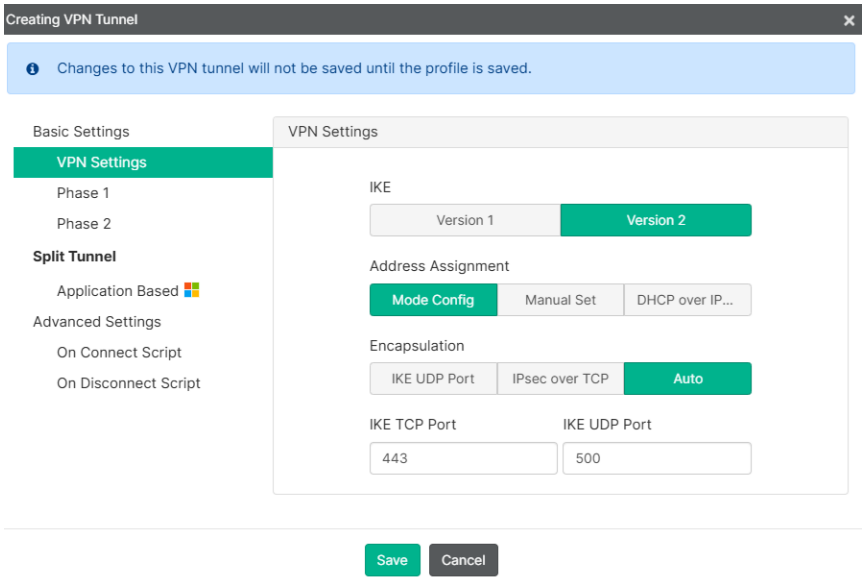
1. In FortiClient EMS, go to *Endpoint Profiles*.
2. Select the needed profile type, and click *Add*.
3. Click *Add Profile* to create a Windows, macOS, and Linux profile.
4. Under *VPN Tunnel*, click *Add Tunnel* > *Manual* and complete the options in the *Basic Settings* section to add a new connection:



Name	Name of the tunnel.
Type	Select *IPsec VPN*. On FortiClient EMS 7.4.3 and later. The type is IPsec by default.

Remote Gateway	IP address or FQDN that FortiClient uses to reach FortiGate for VPN connection. If you used FortiGate's VPN wizard, this setting corresponds to the address of the incoming interface configured during the wizard's *Authentication* step. Typically, this is the same address used for the SSL VPN remote gateway.
Authentication Method	Available options are *Local Certificate*, *Pre Shared Key*, *Smart Card Certificate*, and *Local Store Certificate*. The FortiGate VPN wizard permits either pre-shared key or signature. When the pre-shared key option is configured on the FortiGate, use the same value in the *Pre Shared Key* field in FortiClient EMS. If signature authentication method is preferred, select the certificate option suitable for your company requirements. Ensure that the certificate's CA matches the *Peer Certificate CA* configured during the *Authentication* step of the FortiGate VPN wizard.

5. Under *Basic Settings*, go to *VPN Settings* section, and configure the *IKE* version, *Mode*, and *Options*. These settings must match the ones configured on FortiGate.



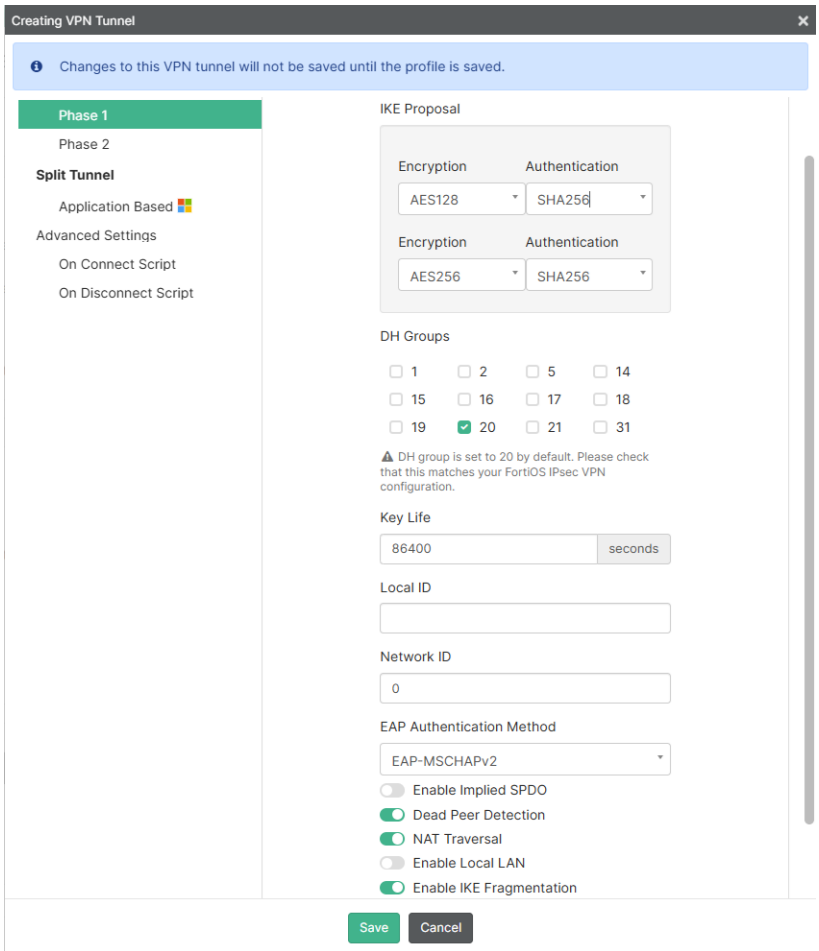
IKE	The FortiGate VPN wizard defaults to *Version 2*. In general, IKEv2 is recommended because TCP port 443 can be used. In addition, starting with FortiClient 7.4.4, IKEv1 is no longer supported on the client.
Address Mode (For IKEv1)	When IKE is set as Version 1 you see two options: *Aggressive* or *Main* mode.
Address Assignment	The *Mode Config* option is the default option and recommended. It's also the default mode configured on FortiGate with the IPsec wizard.

Encapsulation	Select *IKE UDP Port* or *IPsec over TCP* if you want to choose UDP or TCP only. *Auto* mode is recommended as it automatically falls back from UDP to TCP if a connection cannot be made over UDP.

6. Under *Basic Settings*, go to the *Phase 1* section and configure the option. FortiGate's VPN wizard automatically selects phase 1 parameters. You can check these parameters by running the following CLI commands on the FortiGate:

```
show full vpn ipsec phase1-interface <tunnel-name>
```

Ensure that you match phase 1 settings on FortiClient EMS to the phase 1 settings configured on FortiGate.



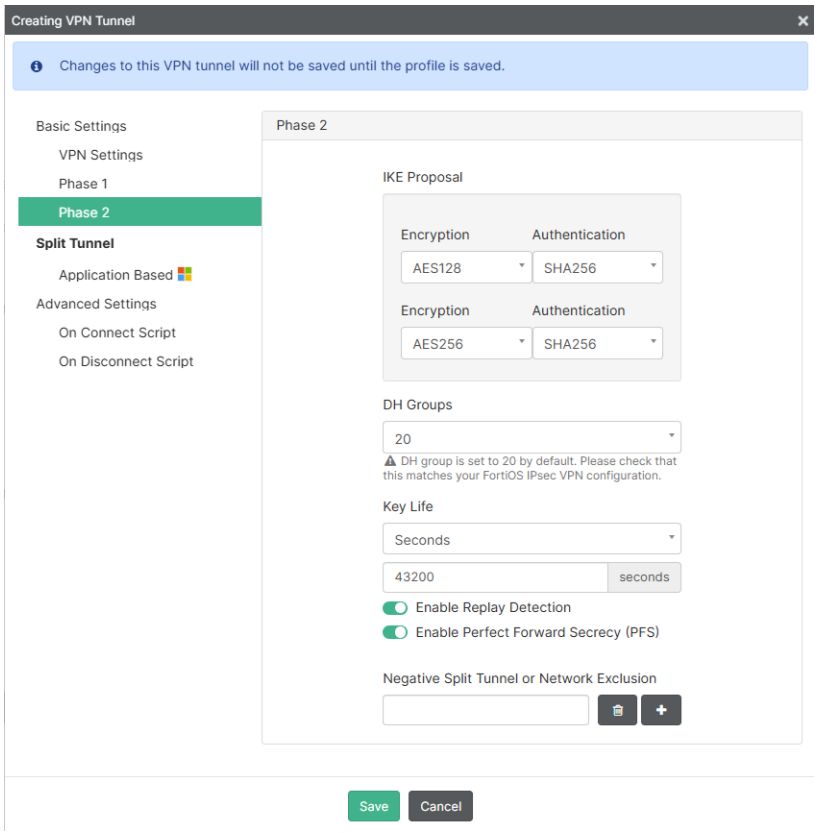
IKE Proposal	Select *Encryption* and *Authentication* algorithms used for generating keys to protect FortiClient and FortiGate negotiations. At least one of the selected encryption-authentication pairs must match to any of the ones configured on FortiGate. FortiGate's VPN wizard sets the following algorithms automatically: • AES128 - SHA256

	• AES256 - SHA256 • AES128 - SHA1 • AES256 - SHA1 Using SHA1 as the authentication algorithm is not recommended. Consider using SHA256.
DH Groups	Select a Diffie-Hellman (DH) group. It must match to one of the groups selected on FortiGate. Groups 5 and 14 are not recommended. Consider using 20 and 21.
Key Life	Enter the time (in seconds) that must pass before IKE encryption key expires. New key gets generated in real-time without interrupting the service. Key life can be configured within the range of 120 and 172,800 seconds. The default value for the FortiGate VPN wizard is 86400 seconds.
Local ID	Enter the *Local ID* that corresponds to the FortiGate VPN's peer ID. By default the FortiGate VPN wizard leaves this setting blank.
Network ID	Enter the *Network ID* corresponding to the FortiGate VPN's *Network ID* when *Network Overlay* is enabled.
EAP Authentication Method	Use EAP-MSCHAPv2 for RADIUS based authentication. Use EAP-TTLS for LDAP based authentication. This setting is new in FortiClient EMS 7.4.4.
Enable IKE Fragmentation	By enabling this setting, IKE messages that exceed the `fragmentation-mtu` threshold configured on the FortiGate will be fragmented and encrypted. This is recommended since IKE messages can exceed path MTU sizes when certificate authentication is used or an IKE message has many proposals or other parameters. See IKEv2 fragmentation for more information.

7. Configure the remaining *Phase 1* options as needed by your requirements. Refer to IPsec VPN documentation for details.

   Phase 1 configuration also allows configuring *Dead Peer Detection* (DPD) mechanism on both FortiClient and FortiGate. DPD configuration is not available in the GUI but is available in XML on FortiClient EMS. For more information regarding DPD and how to configure it on FortiGate, see Dead peer detection. The IKE Settings section describes FortiClient\EMS configuration of DPD with XML.
8. Under *Basic Settings*, go to the *Phase 2* section. The same concept applies for phase 2 settings, the settings on FortiClient EMS and FortiGate must match. As with phase 1, you can confirm what settings were automatically set by the FortiGate VPN wizard by running the following command on FortiGate:

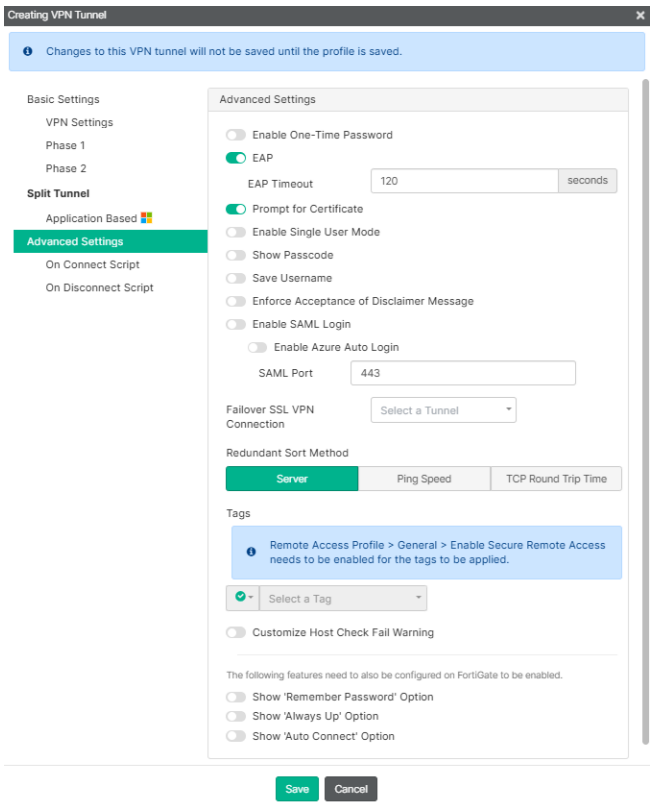
```
show full vpn ipsec phase2-interface <tunnel-name>
```



IKE Proposal	Select *Encryption* and *Authentication* algorithms used to protect the data transferred between the IPsec peers. At least a single pair must match on both FortiClient and FortiGate. The FortiGate VPN wizard configures the following settings by default: • AES128-SHA1 • AES256-SHA1 • AES128-SHA256 • AES256-SHA256 • AES128GCM • AES256GCM Using SHA1 as the authentication algorithm is not recommended. Consider using SHA256.
DH groups	Configure the DH groups to match on FortiGate. Groups 5 and 14 are not recommended. Consider using 20 or 21.
Key Life	Set the time until the phase 2 key expires. The default option is in seconds; however, you can also configure the key life in kilobytes (KBytes) or both. If both is selected, whichever limit gets exceeded first takes precedence. Default value is 43200 (seconds), which matches the value set by the FortiGate VPN wizard.

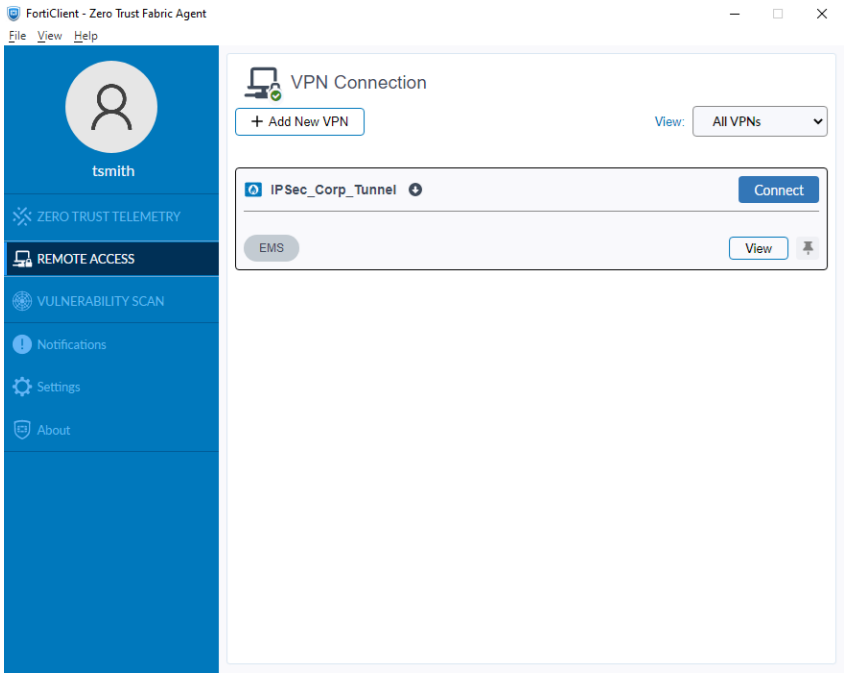
Replay Detection	When enabled, FortiGate checks for already- received packets and discards the ones that arrive out of order. Enabled by default on both FortiClient EMS and FortiGate.
PFS	PFS forces a new DH key exchange upon tunnel establishment and after phase 2 key expiration, causing a new key to be generated each time. Enabled by default on both FortiClient EMS and FortiGate.

9. Go to the *Advanced Settings* section to configure multiple options for IPsec connection including *Save Password*, *Auto-Connect*, and *Always Up*, which then appear on FortiClient GUI. They enable automatic connection to a VPN tunnel and its recovery from network disruption. If you decide to include these settings in your configuration, ensure that you also configure them in the *Client Options* step of FortiGate VPN wizard. For more information on the available options, refer to Remote Access IPsec documentation.



10. Click *Save* to save the changes.
11. Push the profile to FortiClient endpoints.
12. On an endpoint, open FortiClient, and go to the *Remote Access* tab to confirm the settings have been pushed to FortiClient.

The user must select *Save Password*, *Auto-Connect*, and *Always Up* to activate them.


FortiClient - Zero Trust Fabric Agent
File View Help
tsmith
ZERO TRUST TELEMETRY
REMOTE ACCESS
VULNERABILITY SCAN
Notifications
Settings
About
VPN Connection
+ Add New VPN
View:
All VPNs
IPSec_Corp_Tunnel
Connect
EMS
View

www.fortinet.com