Set up a VPN to your OutSystems Cloud

This topic details how you can set up a site-to-site VPN connection that allows secure communication between your on-premises network and OutSystems Cloud.

VPN and Your OutSystems Cloud

Your OutSystems Cloud environments are hosted on Amazon Web Services (AWS) and protected inside a virtual private cloud (VPC), which is logically isolated from the Internet and from other virtual networks in the AWS cloud. To establish a secure connection between your on-premises network and the OutSystems Cloud you can request the creation of a site-to-site virtual private network (VPN) connection using Internet Protocol security (IPSec).

The following diagram shows a single VPN connection, with your OutSystems Cloud, hosted on AWS, shown in the left side, and your on-premises network shown on the right side:

The VPN tunnels are anchored to a virtual private gateway on the OutSystems Cloud side, and to your VPN gateway on the on-premises network side.

The VPN connection consists of two VPN tunnels. If your VPN gateway supports asymmetric routing and if the first VPN tunnel is temporarily disabled, the VPN connection automatically switches over to the second VPN tunnel so that your access isn't interrupted.
VPN Specifications

Initiating the VPN

The VPN connection must be initiated and kept alive by generating constant network traffic from the on-premises network; the VPN tunnel cannot be initiated by the OutSystems Cloud. If your Site-to-Site VPN connection experiences a period of idle time (usually 10 seconds, depending on your configuration), the tunnel may go down. To initiate the VPN connection and keep it operating, you can use one of the following options:

- Use your VPN gateway to generate network traffic by using features such as service-level agreement (SLA) monitor or by running constant Internet Control Message Protocol (ICMP) pings to an environment in the OutSystems Cloud.

or

- Configure a permanent ICMP ping from a set of servers in the on-premises network to an environment in the OutSystems Cloud.

Redundancy

If your VPN gateway supports asymmetric routing, you should configure the two VPN tunnels to ensure high-availability of the VPN connection. Amazon performs routine maintenance on the virtual private gateways, which can disable one of the VPN tunnels for a brief period. Having two VPN tunnels configured ensures the failover to the second VPN tunnel if the first VPN tunnel goes down.

Please note that Cisco ASA devices will only establish a single connection with first configured peer whereas second peer IP is kept down (‘standby’ - connected only in case peer no.1 is unreachable).

Virtual private gateway device

The VPN Hardware Manufacturer for the virtual private gateway device is defined by AWS as "Amazon AWS VPC with VPN Service".

Limitation

The site-to-site VPN currently does not support IPv6 traffic.

Set up the First VPN to Your OutSystems Cloud
Before You Begin

Before you begin setting up your VPN, make sure you understand and comply with the following requirements:

**Check the VPN Gateway Requirements**

Your VPN gateway can be a physical or software device. Check this [list](https://success.outsystems.com/Support/Enterprise_Customers/Maintenance_and_Operations/Set_Up_a_VPN_to_your_OutSystems_Cloud) to know if your VPN gateway has been tested by AWS with the site-to-site VPN.

If your VPN gateway is not on the previous list, it must meet the following requirements:

- Maintain the same static public IP address.
- Establish IKE v1 or IKE v2 Security Association using pre-shared keys.
- Establish IPSec Security Associations in Tunnel mode.
- Use IPsec Dead Peer Detection (DPD).
- Use AES128-bit or AES256-bit encryption function.
- Use the SHA-1 or SHA-256 hashing function.
- Use the Diffie-Hellman Perfect Forward Secrecy in groups 2 (1024 bit), 5 (1536 bit), 14-18 (2048 bit), 22, 23, or 24 (2048 bit).

**Gather Necessary Information**

Before requesting a VPN connection, make sure you have the following information:

- The public IP of your VPN gateway. If your VPN gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device.
- The brand, model, and software version of your VPN gateway.
- The internal IP range of the on-premises network that will access to the VPN.
- The type of routing that your VPN gateway supports: if the gateway supports Border Gateway Protocol (BGP), use dynamic routing, otherwise use static routing.

**Check On-Premises Network**

Your on-premises network internal IP address range mustn't overlap with the internal IP address range of your OutSystems Cloud. Check out how to [find out internal IP address range of your OutSystems Cloud](https://success.outsystems.com/Support/Enterprise_Customers/Maintenance_and_Operations/Set_Up_a_VPN_to_your_OutSystems_Cloud).

---


Updated: Fri, 05 Jun 2020 17:07:49 GMT
Make Sure You Have the Necessary Permissions

To request a VPN you must have the **Administrator role** in LifeTime.

The VPN request must be approved by an **Infrastructure Administrator** in the Support Portal.

Setup Overview

Make sure you read the previous section before you continue.

Step 1. Request the First VPN

To request the first VPN to your OutSystems Cloud follow these steps:

1. **Open LifeTime** by accessing `https://<lifetime_environment>/lifetime`, where `<lifetime_environment>` is the address of your LifeTime environment.

2. Select the **Environments** tab, open **Options** and select **Activate VPN**.
1. Fill in the form by entering the values for each field:
   - Your email address.
   - The email address of the Network Engineer. If you are the Network Engineer enter your email.
   - The public IP of your VPN gateway. If your VPN gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device.
   - The internal IP range of the on-premises network that will access to the VPN.
   - The brand, model, and software version of your VPN gateway.
   - The type of Routing that your VPN gateway supports. If your VPN gateway supports Border Gateway Protocol (BGP), select Dynamic routing, otherwise select Static routing.

2. To send your request for a VPN, select Activate VPN Service. This creates a support ticket with the information you provided in the form.

Step 2. OutSystems Creates the VPN Connection and Contacts You

Once all the required information has been validated, OutSystems creates the VPN connection on your OutSystems Cloud, sends you the VPN Peer Address and the information needed to configure the VPN gateway on your on-premises network, including a configuration file created by AWS.

The type of configuration file you receive depends on your VPN gateway:

- If your device is on the list of VPN gateways tested by AWS, your configuration file contains a step by step guide on how to configure your device. Check an example configuration from AWS for a Cisco IOS Device without BGP.
• If your device is not on the previous list, your configuration file contains a generic guide on what to configure in your VPN device. Check an example configuration from AWS for a generic VPN gateway using BGP.

Step 3. Configure Your VPN Gateway

This step must be performed by your Network Engineer.

After receiving the required information to set up your VPN connection, complete the configuration of your VPN gateway by following the instructions in the communication sent by the OutSystems Support and in the configuration file.

During the VPN gateway configuration you should use the values provided in the configuration file. Otherwise, you must make sure your VPN gateway configuration values respect the following AWS requirements:

<table>
<thead>
<tr>
<th>Phase 1 Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>IKE v1 or IKE v2</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Pre-shared Key</td>
</tr>
<tr>
<td>Protocol Communications</td>
<td>Encapsulated UDP port 500, NAT-T (UDP port 4500)</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES-128, AES-256</td>
</tr>
<tr>
<td>Diffie-Hellman Group</td>
<td>2 (1024 bit), 14-18 (2048 bit), 22, 23, and 24 (2048 bit)</td>
</tr>
<tr>
<td>Perfect Forward Secrecy (PFS)</td>
<td>Yes</td>
</tr>
<tr>
<td>Hashing Algorithm for Integrity</td>
<td>SHA-1, SHA-256</td>
</tr>
<tr>
<td>Re-negotiation time</td>
<td>28800 seconds</td>
</tr>
<tr>
<td>Mode</td>
<td>Main</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Phase 2 Parameters</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>IKE Phase II (IPSEC SA)</td>
</tr>
<tr>
<td>IPSec Protocol</td>
<td>ESP; UDP port 500; NAT-T is supported on your side.</td>
</tr>
<tr>
<td>Encryption Algorithm</td>
<td>AES-128, AES-256</td>
</tr>
<tr>
<td>Encryption Mode</td>
<td>Tunnel</td>
</tr>
</tbody>
</table>
### Phase 2 Parameters

<table>
<thead>
<tr>
<th>Diffie-Hellman Group</th>
<th>2 (1024 bit), 5 (1536 bit), 14-18 (2048 bit), 22, 23, and 24 (2048 bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashing Algorithm for Integrity</td>
<td>SHA-1, SHA-256</td>
</tr>
<tr>
<td>Lifetime Measurement</td>
<td>Time</td>
</tr>
<tr>
<td>Time Lifetime</td>
<td>3600 seconds</td>
</tr>
</tbody>
</table>

### Step 4. Configure Your Firewall

**This step must be performed by your Network Engineer.**

If your on-premises network includes a firewall between the Internet and your VPN gateway, implement the following rules in the firewall:

- **Allow UDP traffic on port 500** between your VPN gateway and each of the VPN tunnels to the OutSystems Cloud to enable the transmission of IKE packets. There should be four rules: a pair of inbound and outbound rules for each VPN tunnel.

- **Allow IP 50 Encapsulating Security Payload (ESP) traffic** between your VPN gateway and each of the VPN tunnels to the OutSystems Cloud to enable the transmission of IPSec packets containing the encrypted network traffic. There should be four rules: a pair of inbound and outbound rules for each VPN tunnel.

- If your OutSystems Cloud needs to access systems on your on-premises network add other inbound and outbound firewall rules. Make sure to create inbound and outbound rules for each of the VPN tunnels.
  
  For example, to access a SQL Server database allow **TCP traffic on port 1433**, and to access an Oracle database allow **TCP traffic on port 1521**.

- If you are using **NAT-T** on your VPN gateway, allow **UDP traffic on port 4500**. Add outbound and inbound firewall rules.
Requesting Additional VPN Connections to Your OutSystems Cloud

If you need additional VPN connections, contact your Account Manager to obtain more information.

Troubleshooting

Check the [VPN connectivity and troubleshooting guide](https://success.outsystems.com/Support/Enterprise_Customers/Maintenance_and_Operations/Set_Up_a_VPN_to_your_Out...)

Updated: Fri, 05 Jun 2020 17:07:49 GMT