

L2L VPN Tunnel

Armor Knowledge Base

Topics Discussed

- [Create an L2L VPN tunnel with a new workload](#)
- [Edit an L2L VPN tunnel](#)
- [Enable, disable, or delete an L2L VPN tunnel](#)



To fully use this screen, you must have the following permissions assigned to your account:

- Read Network L2L
- Write Network L2L



If you are an upgraded user, then any L2L VPN tunnel that you created in Generation 3 (my.armor.com) will not be displayed in the Armor Management Portal (AMP). If you need to modify a Generation 3 L2L VPN tunnel, please contact Armor Support via a [support ticket](#).

Any L2L VPN tunnel that you create in AMP will be visible and configurable in AMP.

Create an L2L VPN tunnel with a new workload



To create an L2L VPN tunnel, you must have an existing workload with an existing virtual machine. To learn how to create a virtual machine, see [Create a virtual machine with a new workload](#).

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **L2L VPN**.
3. In the top menu, in the drop-down menu, select the data center where the virtual machine lives.
4. Click the plus (+) icon.
 - If you do not have any tunnels in that data center, then click **Create an L2L tunnel**.
5. In **Tunnel Name**, enter a descriptive name.
6. Use the slider to enable or disable the tunnel.
7. In **Pre-Shared Key**, enter a secure password.
 - You will use this key to securely connect to your local endpoint.
 - You can click **Generate New Key** to generate a password.
 - You can also create your own key. If you create your own key, the key must contain the following requirements:
 - 16 to 96 characters
 - One lower-case letter
 - One upper-case letter
 - One number
8. In **Internet Key Exchange Version (IKE Version)**, select the IKE version (**IKEV1** or **IKEV2**).
9. In **Digest Algorithms**, select an algorithm (**SHA1** or **SHA256**).
10. In **Encryption Mode**, select an encryption mode:
 - Advanced Encryption Standard (**AES-128**), (**AES-256-CBC**), or (**AES-256-GCM**).
11. Select a **Diffie-Hellman Group** option:
 - **DH-2**
 - MODP with a 1024-bit modulus
 - **DH-5**
 - MODP with a 1536-bit modulus
 - **DH-14**
 - **DH-15**
 - **DH-16**
12. Enable or disable **Perfect Forward Secrecy (PFS)**.
13. In **Remote Peer IP Address**, enter your VPN peer IP address.
14. In **Remote Host/Networks (CIDR)**, enter your LAN encryption domain, and then click the plus (+) sign.
15. In **Local Host/Networks (CIDR)**, enter the Armor LAN encryption domain, and then click the plus (+) sign.
 - This information is the same as your secure cloud server IP address at Armor.
16. Click **Save Changes**.



For the L2L VPN tunnel to properly function, your remote device must contain the following configurations:

| Attribute | Setting |
|------------------------------------|----------------|
| ISAKMP Mode | Main Mode |
| Authentication | Pre-Shared Key |
| Phase 1 Lifetime (Seconds) | 28800 |
| DPD/Keep Alive | Enabled |
| DPD/Keep Alive Retries | 2 |
| DPD/Keep Alive Threshold (Seconds) | 10 |
| SA Lifetime (Seconds) | 3600 |
| SA Lifetime (Kilobytes) | 4608000 |

Edit an L2L VPN tunnel

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **L2L VPN**.
3. If you have virtual machines in various data centers, then click the corresponding data center.
4. Locate and hover over the desired virtual machine.
5. Click the vertical ellipses.
6. Click **Edit**.
7. Make your desired changes, and then click **Save Changes**.

Enable, disable, or delete an L2L VPN tunnel

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **L2L VPN**.
3. If you have virtual machines in various data centers, then click the corresponding data center.
4. Locate and hover over the desired virtual machine.
5. Click the vertical ellipses.
6. Click **Enable**, **Disable**, or **Delete**.
7. Make your desired changes, and then click **Save Changes**.



Troubleshooting

If you do not see any data in the **L2L VPN** screen, consider that:

- An L2L VPN was never created.
- You do not have permission to view L2L VPN configurations.
 - You must have the **Read Network L2L** and **Write Network L2L** permissions enabled. Contact your account administrator to enable these permissions. To learn how to update your permissions, see [Roles and Permissions](#).

If you cannot save a new tunnel, consider that you have reached your limit of tunnels. When you are near your limit of tunnels, a warning message will appear. In this case, Armor recommends that you review existing tunnels to possibly consolidate or delete.



Was this helpful? *

Your Rating: 

Results:  5 rates