



[Knowledgebase](#) > [mCloud](#) > [How to configure IPSec VPN connections to endpoints outside mCloud](#)

How to configure IPSec VPN connections to endpoints outside mCloud

Vincent (Vinnie) Curle - 2025-01-17 - [mCloud](#)

This article provides a general guide for establishing functional IPSec VPN connections to endpoints outside of mCloud. Please note that specific endpoints, such as routers or other cloud providers, may have additional requirements or unique configurations not covered in this guide.

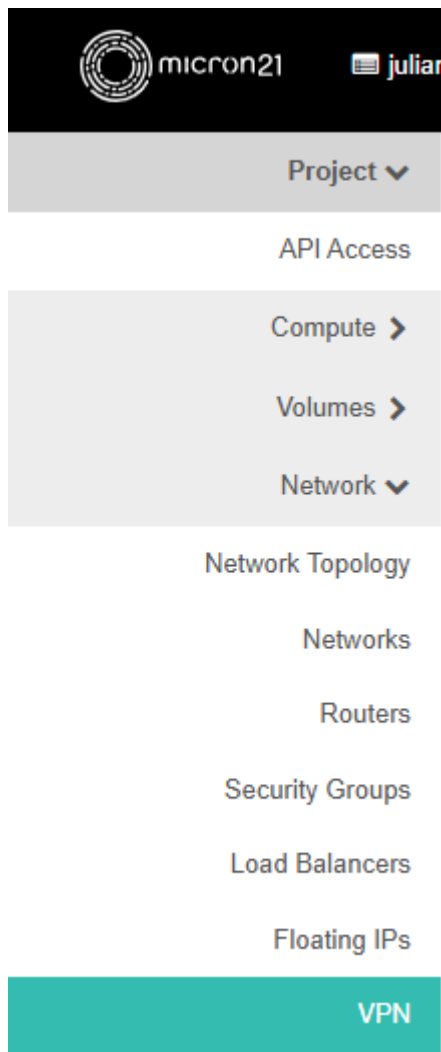
Prerequisites:

This article assumes the following is already configured and functional within your mCloud Dashboard:

- mCloud project
- mCloud internal subnet
- mCloud router
- Remote endpoint capable of IPSec tunnels

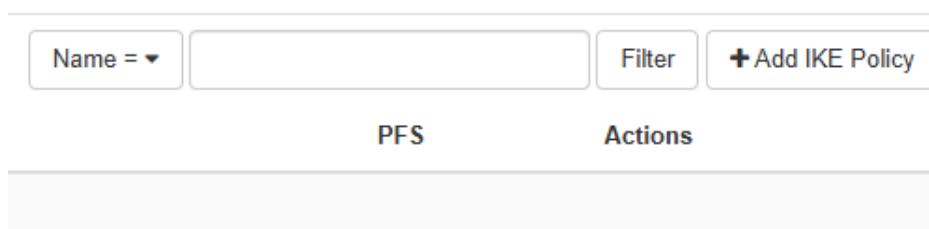
Method:

1. Log into mCloud at <https://mcloud.micron21.com/>
2. Go to Project > Network > VPN



1.

3. Click on "+Add IKE Policy"



1.

4. Fill out the desired settings and click Add

1. This policy can roughly be described as "Phase 1" on other network devices. Keep this in mind when setting up IPSec connections, any mismatch in these settings between endpoints will cause errors.

Add IKE Policy



<p>Name</p> <input type="text" value="IKEv2-Policy"/>	<p>Create IKE policy for current project.</p> <p>An IKE policy is an association of the following attributes:</p>
<p>Description</p> <input type="text"/>	<p>Authorization algorithm</p> <p>Valid algorithms are sha1, sha256, sha384 and sha512.</p>
<p>Authorization algorithm</p> <input type="text" value="sha512"/>	<p>Encryption algorithm</p> <p>Valid algorithms are 3des, aes-128, aes-192 and aes-256.</p>
<p>Encryption algorithm</p> <input type="text" value="aes-256"/>	<p>IKE version</p> <p>The type of version (v1/v2) that needs to be filtered.</p>
<p>IKE version</p> <input type="text" value="v2"/>	<p>Lifetime</p> <p>Life time consists of units and value. Units in 'seconds' and the default value is 3600.</p>
<p>Lifetime units for IKE keys</p> <input type="text" value="seconds"/>	<p>Perfect Forward Secrecy</p> <p>PFS limited to using Diffie-Hellman groups 2, 5 (default) and 14.</p>
<p>Lifetime value for IKE keys ?</p> <input type="text" value="28800"/>	<p>IKE Phase 1 negotiation mode</p> <p>Phase 1 negotiation mode limited to using 'main' and 'aggressive'.</p>
<p>Perfect Forward Secrecy</p> <input type="text" value="group14"/>	<p>All fields are optional.</p>
<p>IKE Phase1 negotiation mode</p> <input type="text" value="main"/>	

Cancel

Add

2.

5. Click on the "IPsec Policies" tab and click "+Add IPsec Policy".

	Filter	+ Add IPsec Policy
--	--------	--------------------

PFS

Actions

1.

6. Fill out the desired settings and click Add

1. This policy is roughly equivalent to "Phase 2" on other network devices.

Add IPsec Policy



Name

Description

Authorization algorithm

Encapsulation mode

Encryption algorithm

Lifetime units

Lifetime value for IKE keys ⓘ

Perfect Forward Secrecy

Transform Protocol

Create IPsec policy for current project.

An IPsec policy is an association of the following attributes

Authorization algorithm

Valid algorithms are sha1, sha256, sha384 and sha512.

Encapsulation mode

The type of IPsec tunnel (tunnel/transport) to be used.

Encryption algorithm

Valid algorithms are 3des, aes-128, aes-192 and aes-256.

Lifetime

Life time consists of units and value. Units in 'seconds' and the default value is 3600.

Perfect Forward Secrecy

PFS limited to using Diffie-Hellman groups 2, 5 (default) and 14.

Transform Protocol

The type of protocol (esp, ah, ah-esp) used in IPsec policy.

All fields are optional.

2.

7. Click on the "VPN Services" tab

8. Click on "+Add VPN Service"

1.

Name = ▼	<input type="text"/>	Filter	+ Add VPN Service
Status	Actions		

9. Enter a name, and select a router. Don't select a subnet at this time, then Click Add

Add VPN Service



Name

Create VPN service for current project.

Description

The VPN service is attached to a router and references to endpoint group or a single subnet to push to a remote site.

Router *

Specify a name, description, router, and subnet (optional) for the VPN service.

Admin State is enabled by default.

The router and admin state fields require to be enabled. All others are optional.

Subnet ?

Note: The recommended way to specify local subnets is to use endpoint groups in IPsec site connection. It is deprecated to specify subnet in VPN service. For a new VPN service or IPsec site connection, using endpoint group is recommended.

☒ Enable Admin State ?

Cancel

Add

1.

10. Click on the "Endpoint Groups" Tab. We'll need to add two endpoint groups here, for internal and remote.

1. Click "+Add Endpoint Group" and add a local subnet for our internal network

Add Endpoint Group



Name

Create endpoint group for current project.

Description

Type *

Local System Subnets ?

☐ 111.223.236.192/26

☐ 111.223.238.96/29

☐ 172.31.0.0/22

☒ 192.168.4.0/22

Cancel

Add

1.

2. Click "+Add Endpoint Group" and add an external subnet for our remote network

Add Endpoint Group



Name

Remote

Create endpoint group for current project.

Description

Type 

CIDR (for external systems) ▼

External System CIDRs 

192.168.207.0/24

Cancel

Add

1.

11. Click on the "IPsec Site Connections" tab and click "+Add IPsec Site Connection".
12. Enter the required details for the configuration we have done to this point, the remote peer details, and a pre-shared key.

Add IPsec Site Connection



Add New IPsec Site Connection *

Optional Parameters

Name

Remote

Create IPsec site connection for current project. Assign a name and description for the IPsec site connection. All fields in this tab are required.

Description

VPN service associated with this connection *

TestVPN

Endpoint group for local subnet(s) ?

Local

IKE policy associated with this connection *

IKEv2-Policy

IPsec policy associated with this connection *

IPsec-Policy

Peer gateway public IPv4/IPv6 Address or FQDN * ?

27.131.108.112

Peer router identity for authentication (Peer ID) * ?

27.131.108.112

Endpoint group for remote peer CIDR(s) ?

Remote

Remote peer subnet(s) ?

Pre-Shared Key (PSK) string * ?

Cancel

Add

1.

13. Configure the remote site VPN, matching the settings added above, and confirm both sides are connected. From here you can test traversing the firewall between sites.