

## How To Setup VPN IPSec Autokey

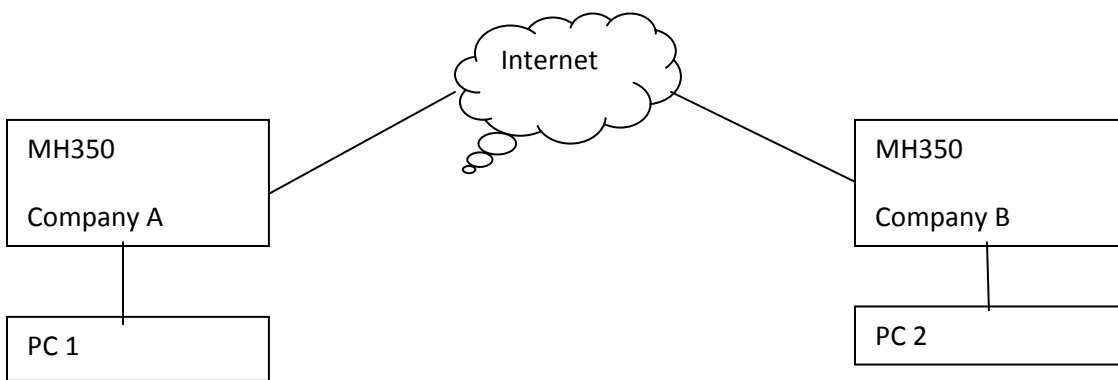
Example: to setup between two MH350s below

Company A **WAN IP: 61.11.11.11**

**LAN IP: 192.168.1.1**

Company B **WAN IP: 61.22.22.22**

**LAN IP: 192.168.2.1**



### At Company A

1. Log into **MH350**
2. **Policy Object** → **VPN** → **IPSec Autokey** setting
  - a) Click **New Entry**
  - b) Fill in Name with **VPN\_A**
  - c) At **To Destination**, select **Remote Gateway-Fixed IP or Domain Name**
  - d) Enter IP **61.22.22.22**
  - e) At **Authentication Method**, select **Preshare** and enter key **123456789** (max: 100bits)
  - f) At **ISAKMP Algorithm** → **Encapsulation**, choose the following:
    - 1) ENC Algorithm: **3DES**
    - 2) AUTH Algorithm: **MD5**
    - 3) Group: **Group1**
  - g) Select **Data Encryption + Authentication** and choose the following:
    - 1) ENC Algorithm: **3DES**
    - 2) AUTH Algorithm: **MD5**
  - h) On the **Optional Item**, choose:
    - 1) Perfect Forward Secrecy: **Group 1**
    - 2) ISAKMP Lifetime: **3600**
    - 3) IPSec Lifetime: **28800**

4) Mode: **Main Mode**

Necessary Item	
Name	VPN_A
WAN interface	<input checked="" type="radio"/> WAN 1 <input type="radio"/> WAN 2
To Destination	
<input checked="" type="radio"/> Remote Gateway -- Fixed IP or Domain Name	<input type="text" value="61.22.22.22"/> (Max. 99 characters)
<input type="radio"/> Remote Gateway or Client -- Dynamic IP	
Authentication Method	Preshare <input type="button" value="v"/>
Preshared Key	<input type="text" value="123456789"/> (Max. 103 characters)
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	3DES <input type="button" value="v"/>
AUTH Algorithm	MD5 <input type="button" value="v"/>
Group	GROUP 1 <input type="button" value="v"/>
IPSec Algorithm	
<input checked="" type="radio"/> Data Encryption + Authentication	
ENC Algorithm	3DES <input type="button" value="v"/>
AUTH Algorithm	MD5 <input type="button" value="v"/>
<input type="radio"/> Authentication Only	
Optional Item	
Perfect Forward Security	GROUP 1 <input type="button" value="v"/>
ISAKMP Lifetime	<input type="text" value="3600"/> Seconds ( Range: 1200 - 86400 )
IPSec Lifetime	<input type="text" value="28800"/> Seconds ( Range: 1200 - 86400 )

5) When saved, you should see the following under **Policy Object** → **VPN** → **IPSec Autokey**

i	Name	WAN	Gateway IP	IPSec Algorithm	Configure
	VPN_A	WAN1	61.22.22.22	3DES / MD5	<input type="button" value="In Use"/>

**New Entry**


3. **Policy Object → VPN → Tunnel** setting

- a) Click **New Entry**
- b) Fill in Name with **IPSec\_VPN\_Tunnel**
- c) From Source: select **LAN**
- d) From Source Subnet/Mask: enter IP **192.168.1.0 / 255.255.255.0**
- e) To Destination: select **To Destination Subnet/Mask**
- f) To Destination Subnet/Mask: enter IP **192.169.2.0 / 255.255.255.0**
- g) IPSec / PPTP Setting: select **VPN\_A**
- h) Place a check mark at **Show remote Network Neighborhood**

Modify IPSec_VPN_Tunnel Tunnel	
Name	IPSec_VPN_Tunnel
From Source	<input checked="" type="radio"/> LAN <input type="radio"/> DMZ
From Source Subnet / Mask	<input type="text" value="192.168.1.0"/> / <input type="text" value="255.255.255.0"/>
To Destination	<input checked="" type="radio"/> To Destination Subnet / Mask <input type="radio"/> Remote Client
	<input type="text" value="192.168.2.0"/> / <input type="text" value="255.255.255.0"/>
IPSec / PPTP Setting	VPN_A ▾
Keep alive IP :	<input type="text"/>
<input checked="" type="checkbox"/> Show remote Network Neighborhood	

**Cancel**

- i) When saved, you should see the following under **Policy Object → VPN → Tunnel**

i	Name	Source Subnet	Destination Subnet	IPSec / PPTP	Configure
	IPSec_VPN_Tu...	192.168.1.0	192.168.2.0	VPN_A	<b>In Use</b>

**New Entry**

- 4. **Policy** → **Outgoing Policy** setting
  - a) Click **New Entry**
  - b) At **Tunnel**, select **IPSec\_VPN\_Tunnel**
  - c) Click **OK** to save

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Inside_Any ▾
Destination Address	Outside_Any ▾
Service	ANY ▾
Schedule	None ▾
Authentication User	None ▾
Tunnel	IPSec_VPN_Tunnel ▾
Action, WAN Port	PERMIT ALL ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
Content Blocking	<input type="checkbox"/> Enable
IM / P2P Blocking	None ▾
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )

**OK** **Cancel**

5. **Policy** → **Incoming Policy** Setting

- a) Click **New Entry**
- b) At **Tunnel**, select **IPSec\_VPN\_Tunnel**
- c) Click **OK** to save

Comment :  (Max. 32 characters)

Modify Policy	
Source Address	Outside_Any ▾
Destination Address	Inside_Any ▾
Service	ANY ▾
Schedule	None ▾
Tunnel	IPSec_VPN_Tunnel ▾
Action	PERMIT ▾
Traffic Log	<input type="checkbox"/> Enable
Statistics	<input type="checkbox"/> Enable
QoS	None ▾
MAX. Bandwidth Per Source IP	Downstream <input type="text" value="0"/> Kbps Upstream <input type="text" value="0"/> Kbps ( 0: means unlimited )
MAX. Concurrent Sessions Per IP	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
MAX. Concurrent Sessions	<input type="text" value="0"/> ( Range: 1 - 99999, 0: means unlimited )
NAT	<input type="checkbox"/> Enable

At Company B

1. Repeat steps above, except change the following values:
  - Step 2 → d): enter **61.11.11.11**
  - Step 3 → d): enter **192.168.2.0 / 255.255.255.0**
  - Step 3 → f): enter **192.168.1.0 / 255.255.255.0**