FatPipe
Auto Configuration

Objectives

Desired Functionality

- Centralised Management of all Appliances
- Pro-active monitoring of WAN Infrastructure
- Ability to analyze and raise alerts when thresholds in wan behavior are crossed.

Fatpipe Orchestration

Standalone or "On Device" Orchestrator
Manage all appliances from a "single window"
Key based branch appliance management
Templates based policy management
Intelligent separation of paths based on ISP Link Types
Mix Mesh or Hub and Spoke topologies based on requirements.
Auto-detection of changes in topology and re-calibrate the network.
Extensive reporting on the WAN.
Identify WAN bottlenecks before they become a major problem.

Types and Licensing

Feature	License string	Functionality	Menu and extra options in the UI
Orchestration	CM	Manage devices & templates.	Orchestration menu option Template Check box in VPN / MPSec Global Policy Routing Rules Global QoS
EnterpriseView Reporting	EV	Gather statistics and show reports	EnterpriseView menu option
HQ Device	HUB	HeadEnd device deployed at DC. Involved in actual routing	No extra options in the UI.
Branch	-	Edge device deployed at branches. Involved in actual routing.	No extra options in the UI.

Orchestration Device Type	Description
CONTROLLER	Work as a Orchestrator only. Will not participate in Routing. No IPSec/MPSec/PRR templates will be applied.
HQ	Work as a HeadEnd device. Participate in routing, download templates and apply them in the device. Able to create multiple key configurations to the same Orchestrator to support multiple topologies.
BRANCH	Work as an edge device. Participate in routing, download templates and apply them in the device. Can create only one key configuration to an Orchestrator .

Process Flow Information

•Node contacts the Orchestrator.

•Orchestrator validates the Contacting device.

•Node provides its Network information to the Orchestrator.

•Node asks for the templates. Orchestrator gives the templates based on the key.

•Node configures itself based on the templates.

•Orchestrator re-configures itself based on the Node details and hands over the node details to the other nodes when those nodes poll for new information.

•Network is auto-populated and connection established.

Deployment Options

Scenario 1 : Large Deployments

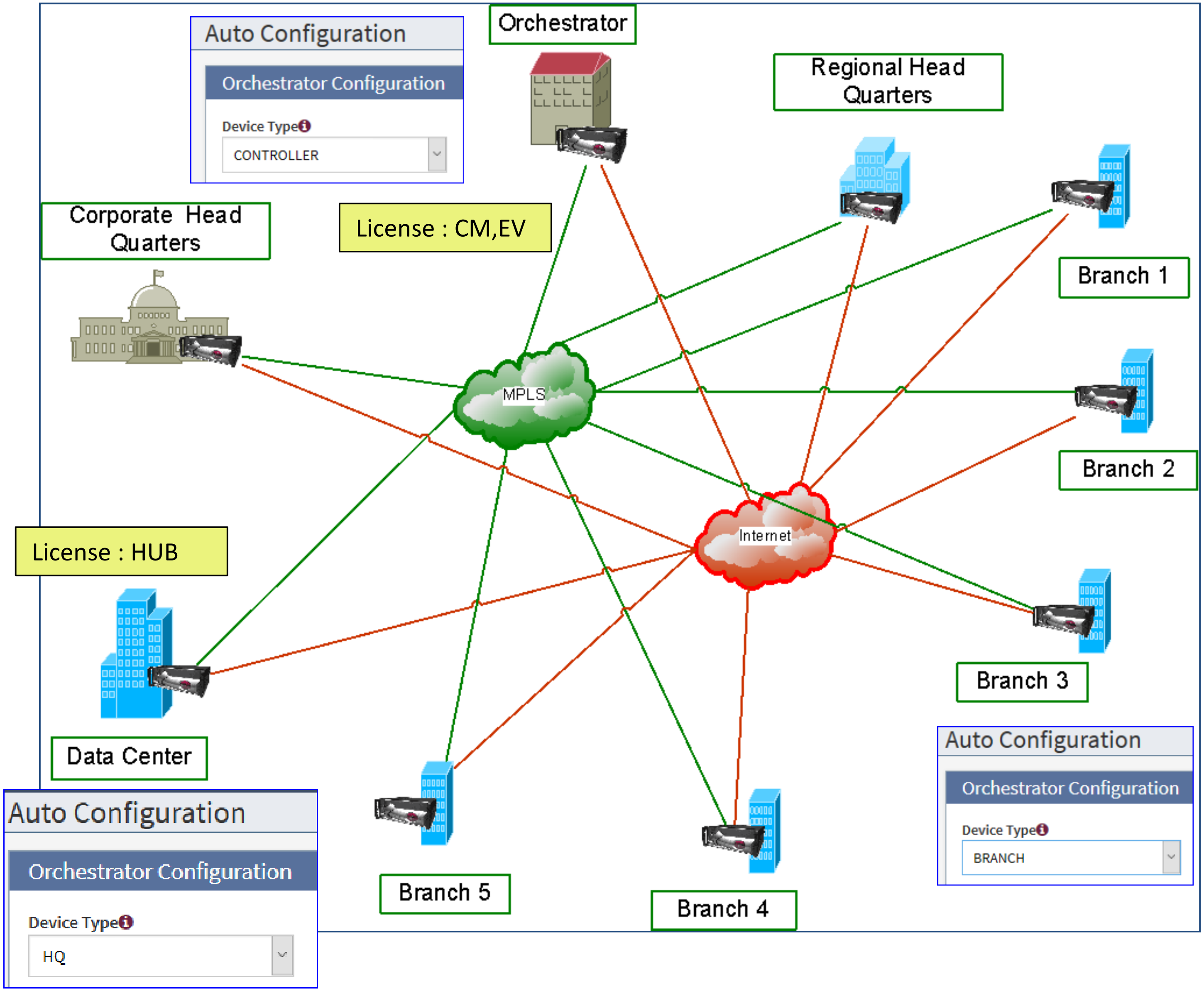
Orchestrator and EnterpriseView are deployed on a separate device.
HUBs are deployed at the DC/DR.
Branch is deployed at the edges

Scenario 2: Medium and Small Deployments

Orchestrator, EnterpriseView and HUB are deployed on the same device.
Branch is deployed at the edges

Featues can be clubbed on a single device or installed on separate devices depending on the requirement.

Scenario 1



Auto Configuration

Orchestrator Configuration

Device Type: CONTROLLER

Auto Configuration

Orchestrator Configuration

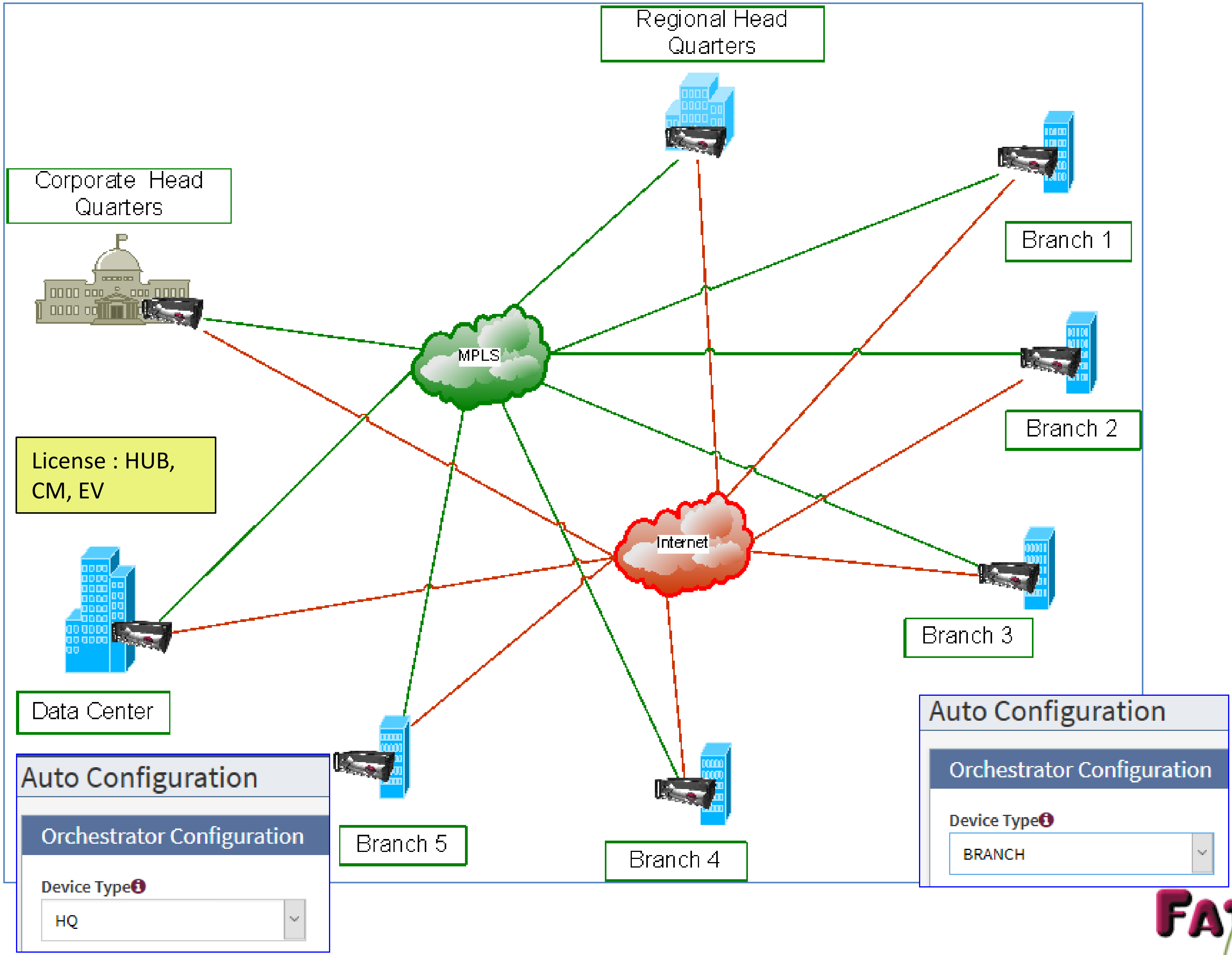
Device Type: BRANCH

Auto Configuration

Orchestrator Configuration

Device Type: HQ

Scenario 2



License : HUB, CM, EV

Auto Configuration

Orchestrator Configuration

Device Type: HQ

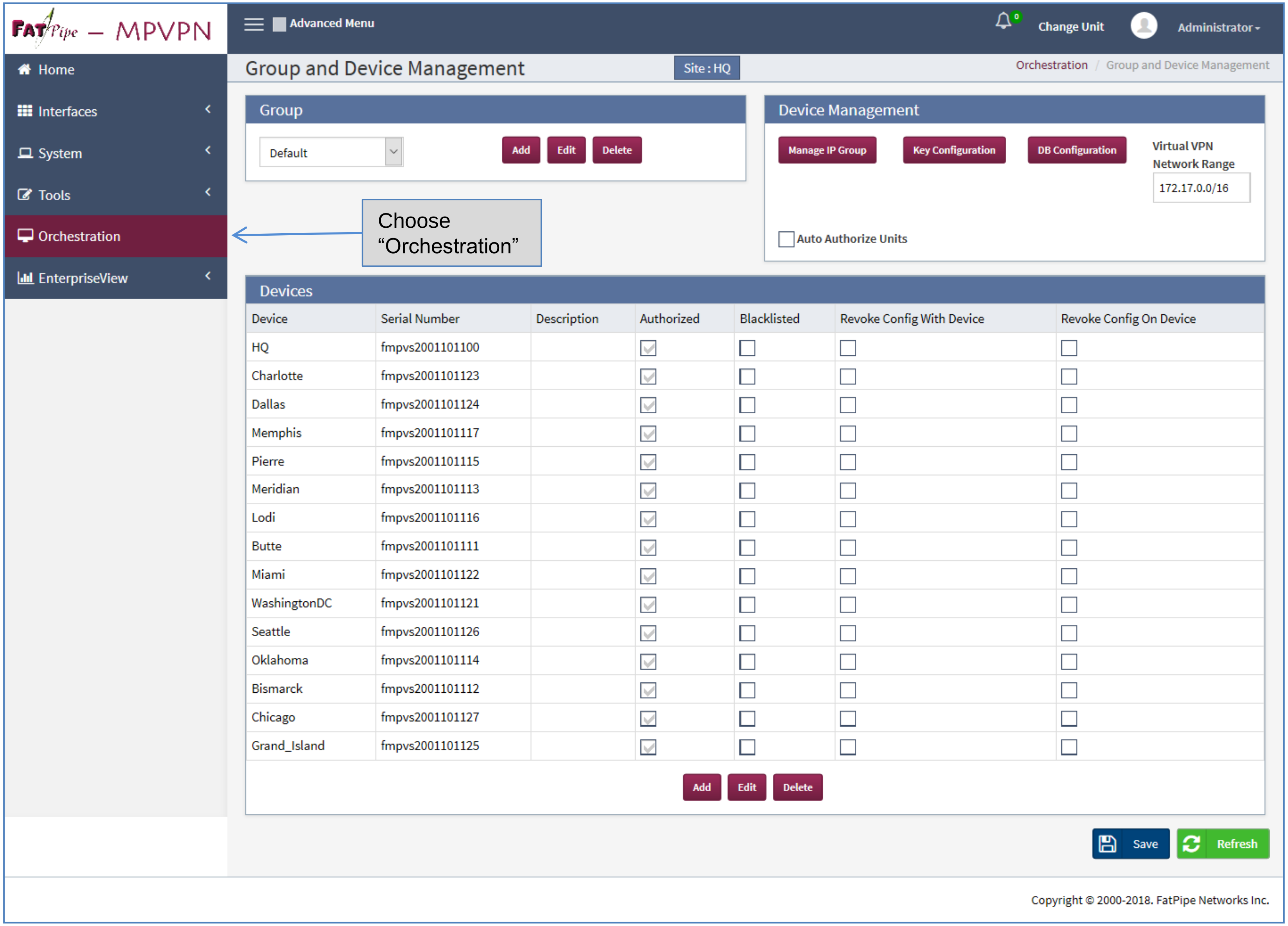
Auto Configuration

Orchestrator Configuration

Device Type: BRANCH

FAT Pipe

Orchestrator Configuration



Choose “Orchestration”

Group and Device Management

Group

Default

Device Management

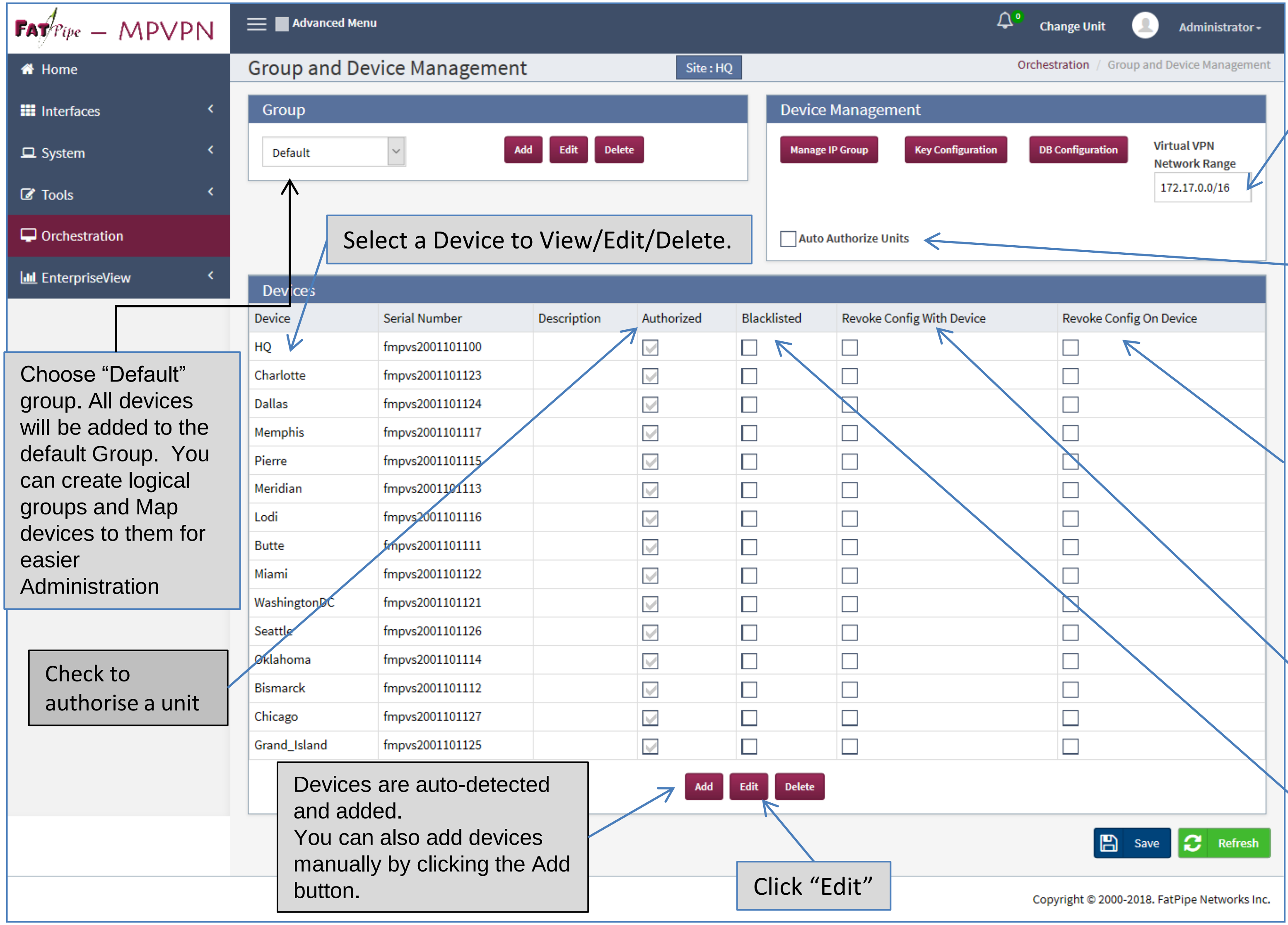
Virtual VPN Network Range: 172.17.0.0/16

□ Auto Authorize Units

Devices

Device	Serial Number	Description	Authorized	Blacklisted	Revoke Config With Device	Revoke Config On Device
HQ	fmpvs2001101100		☑	□	□	□
Charlotte	fmpvs2001101123		☑	□	□	□
Dallas	fmpvs2001101124		☑	□	□	□
Memphis	fmpvs2001101117		☑	□	□	□
Pierre	fmpvs2001101115		☑	□	□	□
Meridian	fmpvs2001101113		☑	□	□	□
Lodi	fmpvs2001101116		☑	□	□	□
Butte	fmpvs2001101111		☑	□	□	□
Miami	fmpvs2001101122		☑	□	□	□
WashingtonDC	fmpvs2001101121		☑	□	□	□
Seattle	fmpvs2001101126		☑	□	□	□
Oklahoma	fmpvs2001101114		☑	□	□	□
Bismarck	fmpvs2001101112		☑	□	□	□
Chicago	fmpvs2001101127		☑	□	□	□
Grand_Island	fmpvs2001101125		☑	□	□	□

Device Management



FATPipe – MPVPN

Group and Device Management

Site : HQ

Group

Default

Add | Edit | Delete

Device Management

Manage IP Group | Key Configuration | DB Configuration

Virtual VPN Network Range: 172.17.0.0/16

□ Auto Authorize Units

Devices

Device	Serial Number	Description	Authorized	Blacklisted	Revoke Config With Device	Revoke Config On Device
HQ	fmpvs2001101100		☑	□	□	□
Charlotte	fmpvs2001101123		☑	□	□	□
Dallas	fmpvs2001101124		☑	□	□	□
Memphis	fmpvs2001101117		☑	□	□	□
Pierre	fmpvs2001101115		☑	□	□	□
Meridian	fmpvs2001101113		☑	□	□	□
Lodi	fmpvs2001101116		☑	□	□	□
Butte	fmpvs2001101111		☑	□	□	□
Miami	fmpvs2001101122		☑	□	□	□
WashingtonDC	fmpvs2001101121		☑	□	□	□
Seattle	fmpvs2001101126		☑	□	□	□
Oklahoma	fmpvs2001101114		☑	□	□	□
Bismarck	fmpvs2001101112		☑	□	□	□
Chicago	fmpvs2001101127		☑	□	□	□
Grand_Island	fmpvs2001101125		☑	□	□	□

Add | Edit | Delete

Save | Refresh

Copyright © 2000-2018. FatPipe Networks Inc.

Select a Device to View/Edit/Delete.

Choose “Default” group. All devices will be added to the default Group. You can create logical groups and Map devices to them for easier Administration

Check to authorise a unit

Devices are auto-detected and added.
You can also add devices manually by clicking the Add button.

Click “Edit”

Virtual IP Subnet to be used for assigning 1 IP per Branch device. Assign virtual IP if you are using Dynamic IPs on any of your WANs

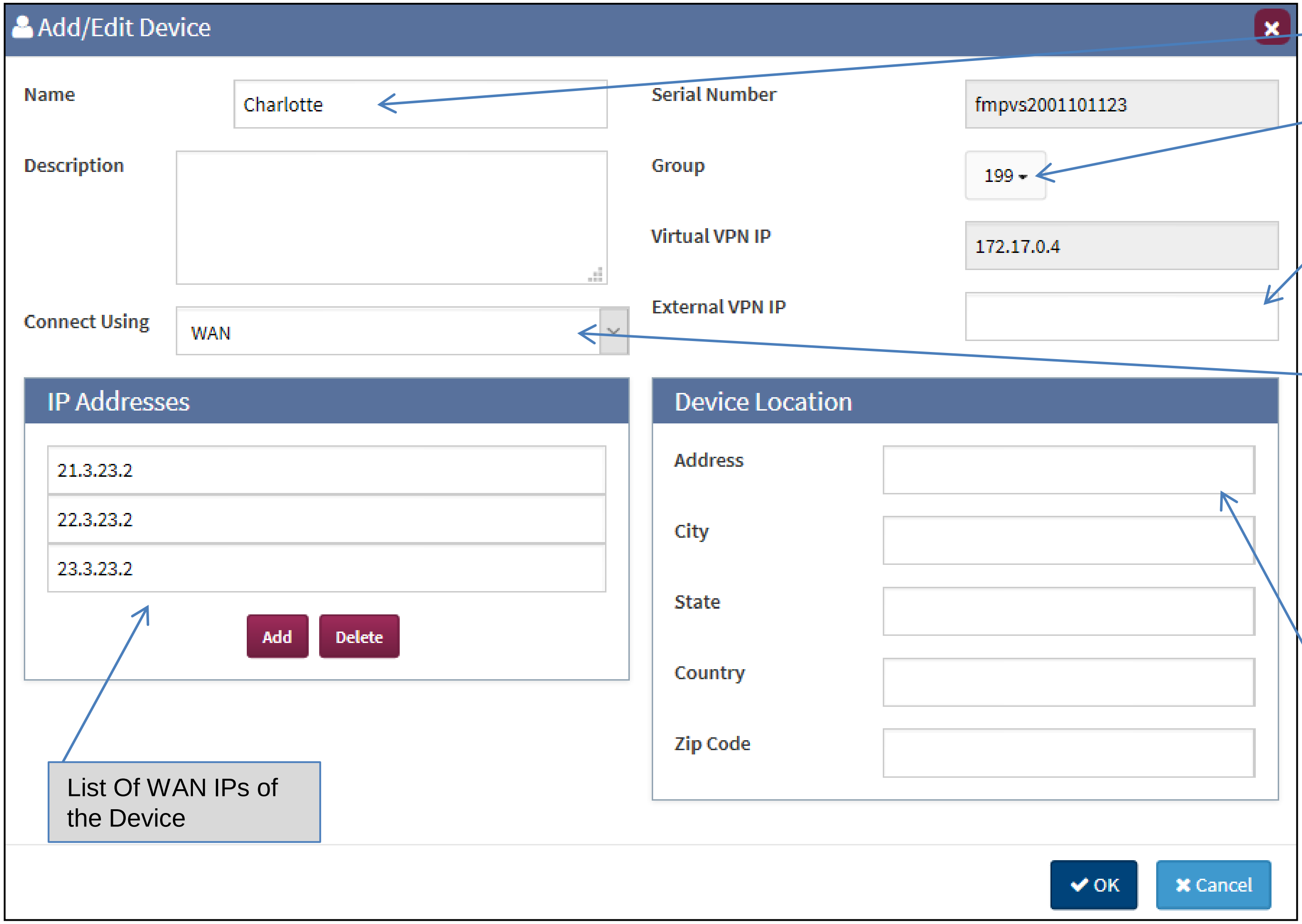
If checked all added units will be authorised automatically

Check to remove the config of a device on the orchestrator and restore defaults on the device

Check to remove the config of a device on the orchestrator

Check to blacklist a unit.

Device Management – Device configuration



Add/Edit Device

Name: Charlotte

Serial Number: fmpvs2001101123

Description:

Group: 199

Virtual VPN IP: 172.17.0.4

External VPN IP:

Connect Using: WAN

IP Addresses

21.3.23.2

22.3.23.2

23.3.23.2

Device Location

Address:

City:

State:

Country:

Zip Code:

List Of WAN IPs of the Device

Name of the Unit

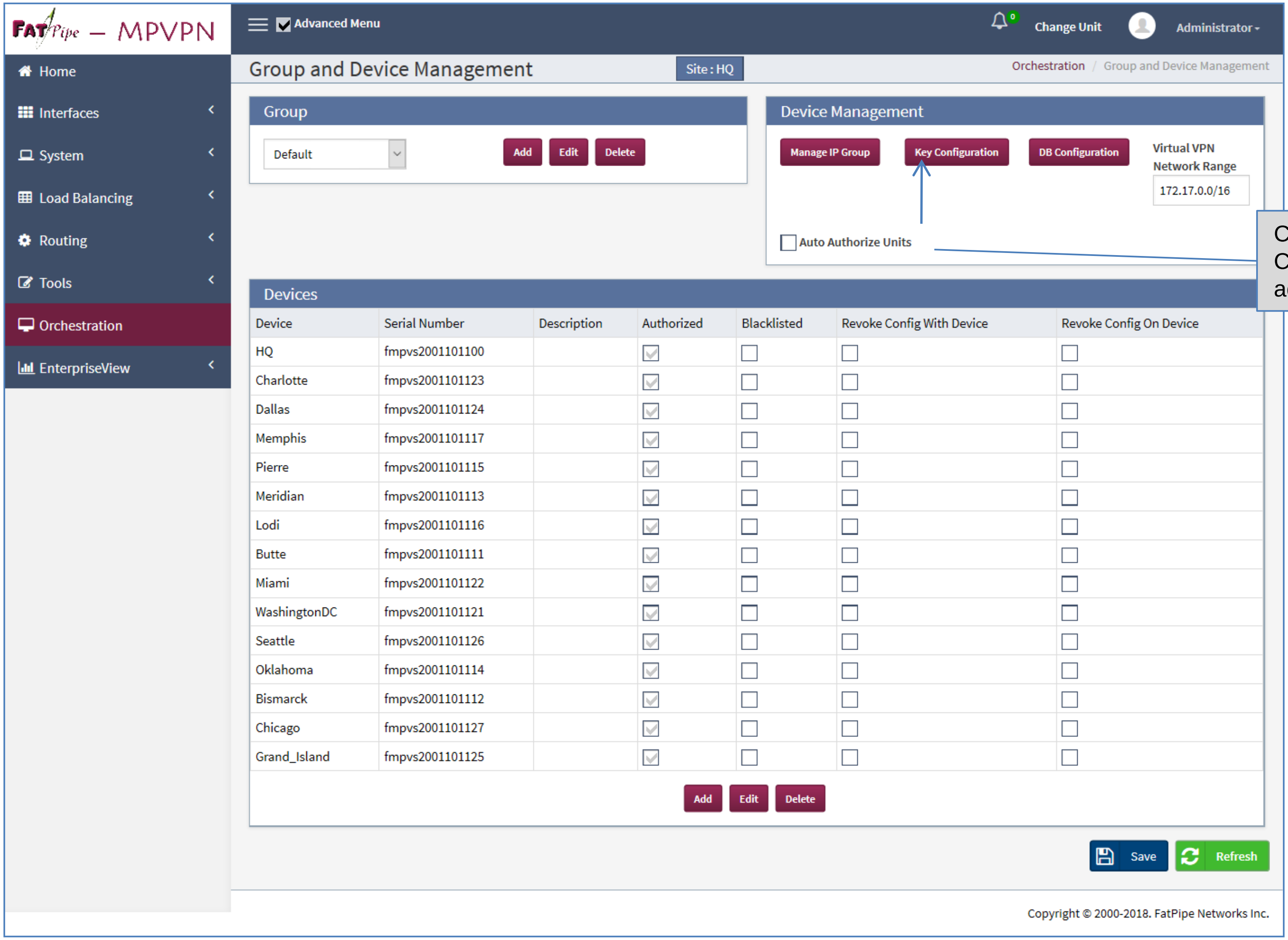
List of groups to which the device can be assigned.

If the VPN is configured on an external device, define the IP here.

WAN – Connect over WAN.
LAN – connect using LAN IP. Choose this to connect through VPN tunnel if you cannot reach the device over WAN IP
ALL – Connect using WAN first and if not reachable , use VPN to connect to the branch.

Physical Address where the device is deployed. This helps to plot the location in the Map.

Key Configuration



Group and Device Management

Site : HQ

Orchestration / Group and Device Management

Group

Default

Device Management

Virtual VPN Network Range: 172.17.0.0/16

□ Auto Authorize Units

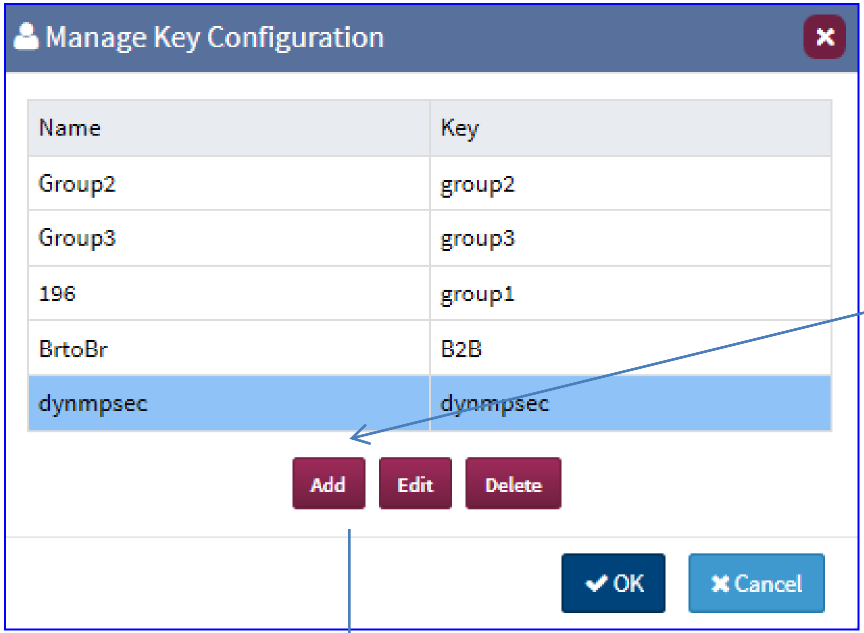
Devices

Device	Serial Number	Description	Authorized	Blacklisted	Revoke Config With Device	Revoke Config On Device
HQ	fmpvs2001101100		☑	□	□	□
Charlotte	fmpvs2001101123		☑	□	□	□
Dallas	fmpvs2001101124		☑	□	□	□
Memphis	fmpvs2001101117		☑	□	□	□
Pierre	fmpvs2001101115		☑	□	□	□
Meridian	fmpvs2001101113		☑	□	□	□
Lodi	fmpvs2001101116		☑	□	□	□
Butte	fmpvs2001101111		☑	□	□	□
Miami	fmpvs2001101122		☑	□	□	□
WashingtonDC	fmpvs2001101121		☑	□	□	□
Seattle	fmpvs2001101126		☑	□	□	□
Oklahoma	fmpvs2001101114		☑	□	□	□
Bismarck	fmpvs2001101112		☑	□	□	□
Chicago	fmpvs2001101127		☑	□	□	□
Grand_Island	fmpvs2001101125		☑	□	□	□

Copyright © 2000-2018. FatPipe Networks Inc.

Click Key Configuration to add new Keys

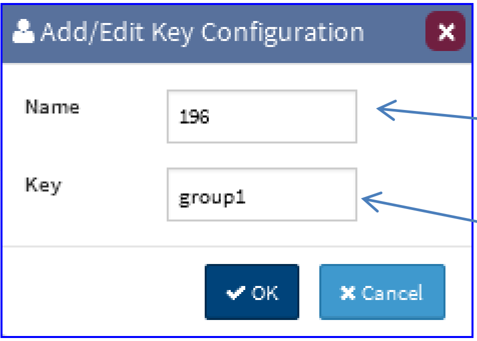
Key Configuration - Manage Keys



Manage Key Configuration

Name	Key
Group2	group2
Group3	group3
196	group1
BrtoBr	B2B
dynmpsec	dynmpsec

Click “Add” button



Add/Edit Key Configuration

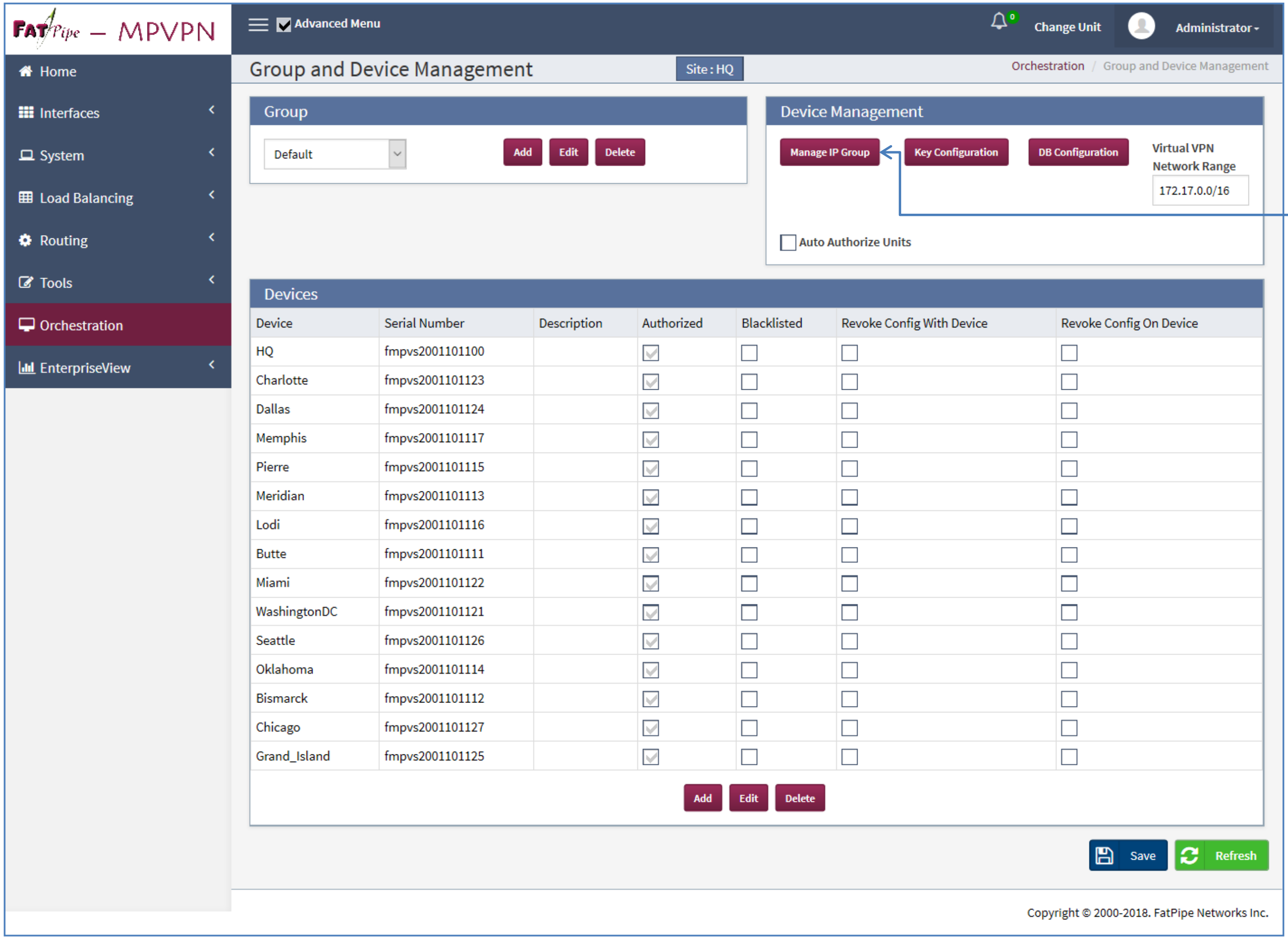
Name: 196

Key: group1

Give the key a Name for identification purposes

Configure the Key. This key will be used to identify the Templates and Devices

ISP Management



Group and Device Management

Site : HQ

Orchestration / Group and Device Management

Group

Default

Device Management

Virtual VPN Network Range: 172.17.0.0/16

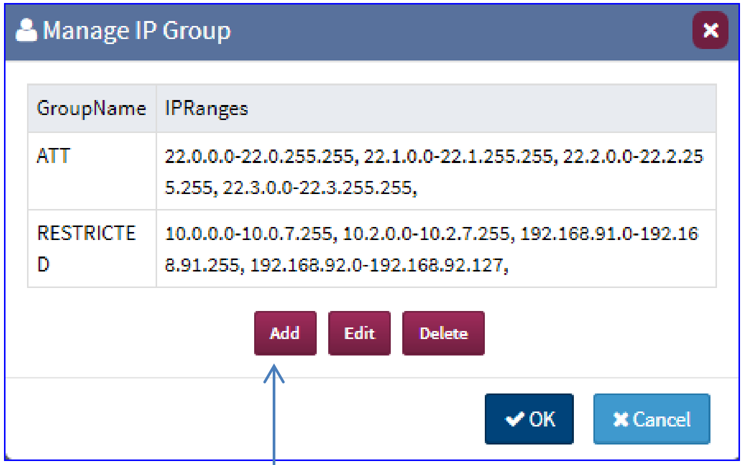
□ Auto Authorize Units

Devices

Device	Serial Number	Description	Authorized	Blacklisted	Revoke Config With Device	Revoke Config On Device
HQ	fmpvs2001101100		☑	□	□	□
Charlotte	fmpvs2001101123		☑	□	□	□
Dallas	fmpvs2001101124		☑	□	□	□
Memphis	fmpvs2001101117		☑	□	□	□
Pierre	fmpvs2001101115		☑	□	□	□
Meridian	fmpvs2001101113		☑	□	□	□
Lodi	fmpvs2001101116		☑	□	□	□
Butte	fmpvs2001101111		☑	□	□	□
Miami	fmpvs2001101122		☑	□	□	□
WashingtonDC	fmpvs2001101121		☑	□	□	□
Seattle	fmpvs2001101126		☑	□	□	□
Oklahoma	fmpvs2001101114		☑	□	□	□
Bismarck	fmpvs2001101112		☑	□	□	□
Chicago	fmpvs2001101127		☑	□	□	□
Grand_Island	fmpvs2001101125		☑	□	□	□

If we have private Links (MPLS), Click on “Manage IP Group” to isolate networks based on IP subnets. This ensures a mesh is not created between private links

ISP Management – Manage IP Groups



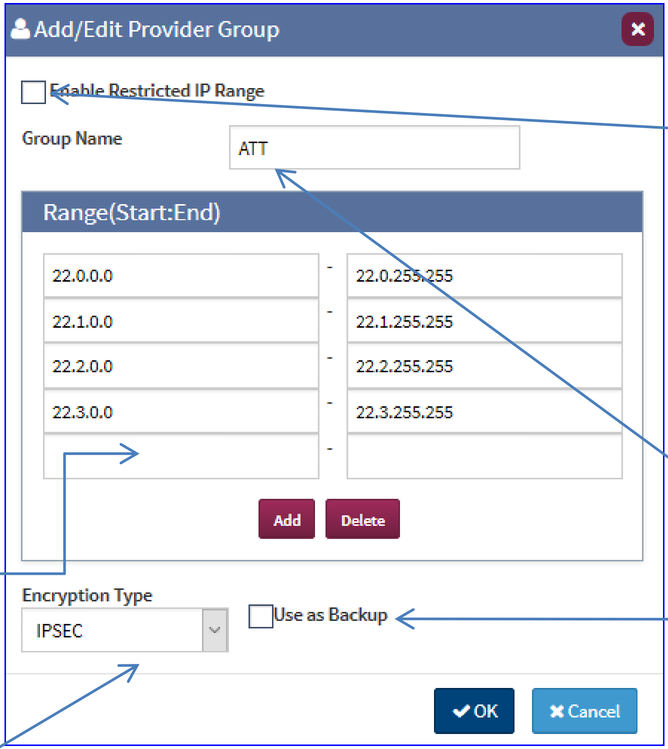
Manage IP Group

GroupName	IPRanges
ATT	22.0.0.0-22.0.255.255, 22.1.0.0-22.1.255.255, 22.2.0.0-22.2.255.255, 22.3.0.0-22.3.255.255,
RESTRICTED	10.0.0.0-10.0.7.255, 10.2.0.0-10.2.7.255, 192.168.91.0-192.168.91.255, 192.168.92.0-192.168.92.127,

Click “Add” button to add a new IP Group.

Configure the networks

Choose between IPSec / GRE or NONE



Add/Edit Provider Group

□ Enable Restricted IP Range

Group Name: ATT

Range(Start:End)		
22.0.0.0	-	22.0.255.255
22.1.0.0	-	22.1.255.255
22.2.0.0	-	22.2.255.255
22.3.0.0	-	22.3.255.255
	-	

Encryption Type: IPSEC

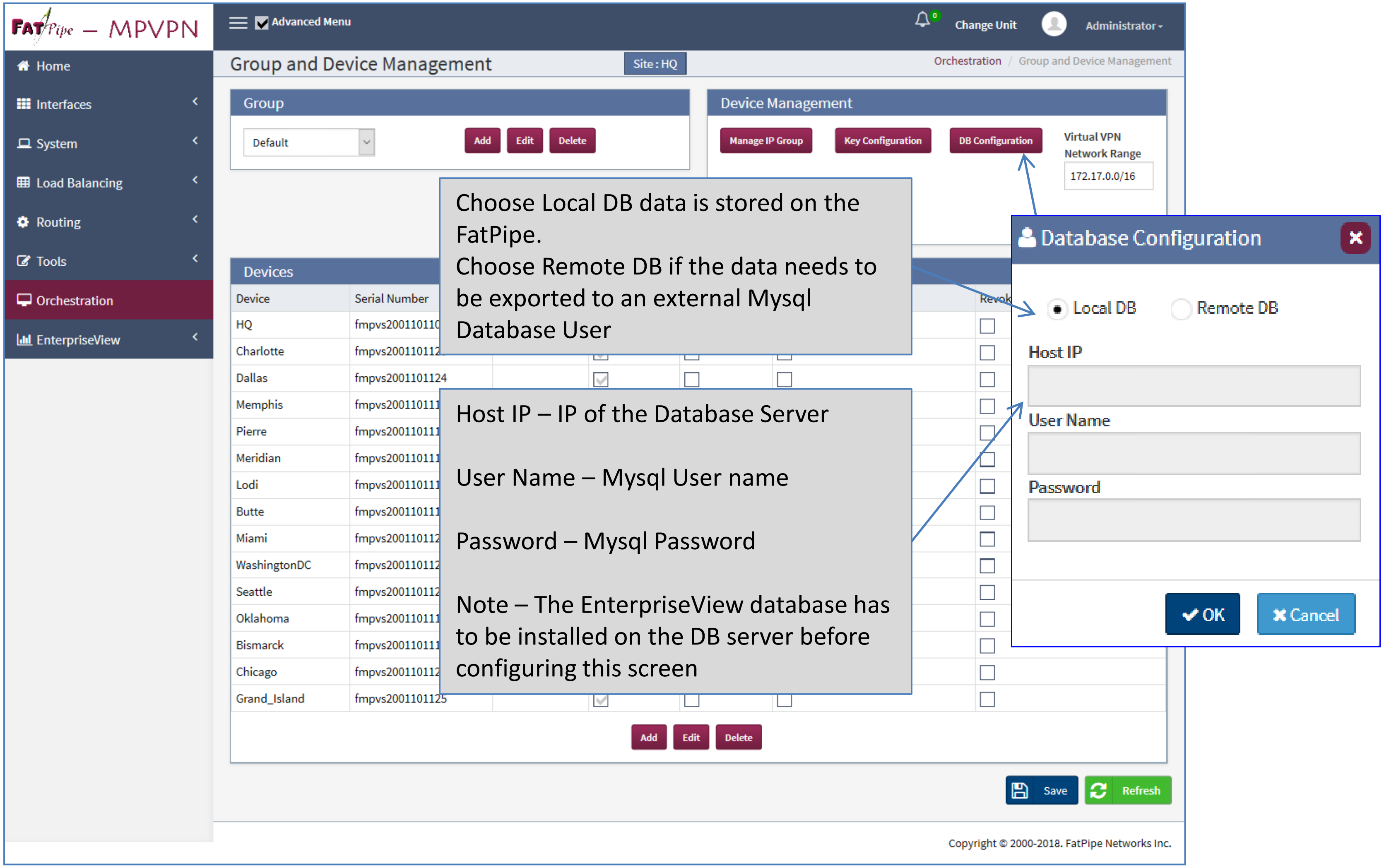
□ Use as Backup

Check this box if you DO NOT want the networks configured in this group to be part of IPSec /MPSec

Enter a group name preferably ISP Name

Check this box if you want to use paths with endpoints mapped to this group as Backup paths

Database Management



Group and Device Management

Site : HQ

Group: Default

Virtual VPN Network Range: 172.17.0.0/16

Device	Serial Number					Revok
HQ	fmpvs200110110					□
Charlotte	fmpvs200110112		☑	□	□	□
Dallas	fmpvs2001101124		☑	□	□	□
Memphis	fmpvs200110111					□
Pierre	fmpvs200110111					□
Meridian	fmpvs200110111					□
Lodi	fmpvs200110111					□
Butte	fmpvs200110111					□
Miami	fmpvs200110112					□
WashingtonDC	fmpvs200110112					□
Seattle	fmpvs200110112					□
Oklahoma	fmpvs200110111					□
Bismarck	fmpvs200110111					□
Chicago	fmpvs200110112					□
Grand_Island	fmpvs2001101125		☑	□	□	□

Copyright © 2000-2018. FatPipe Networks Inc.

Database Configuration ✖

● Local DB ○ Remote DB

Host IP:

User Name:

Password:

✔ OK ✖ Cancel

Choose Local DB data is stored on the FatPipe.
Choose Remote DB if the data needs to be exported to an external Mysql Database User

Host IP – IP of the Database Server

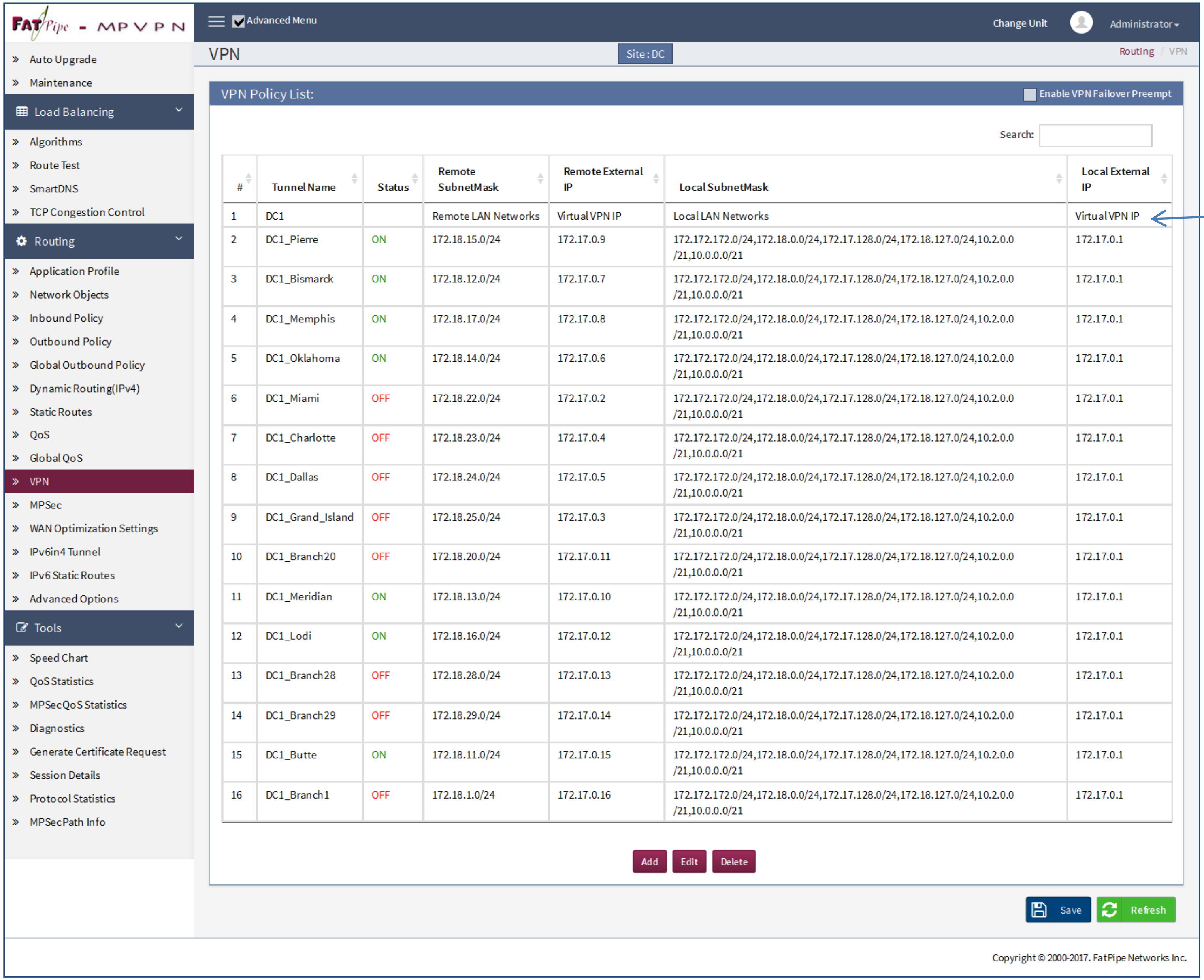
User Name – Mysql User name

Password – Mysql Password

Note – The EnterpriseView database has to be installed on the DB server before configuring this screen

Orchestration
Creating Templates

VPN Page



VPN

VPN Policy List:

☐ Enable VPN Failover Preempt

Search:

#	Tunnel Name	Status	Remote SubnetMask	Remote External IP	Local SubnetMask	Local External IP
1	DC1		Remote LAN Networks	Virtual VPN IP	Local LAN Networks	Virtual VPN IP
2	DC1_Pierre	ON	172.18.15.0/24	172.17.0.9	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
3	DC1_Bismarck	ON	172.18.12.0/24	172.17.0.7	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
4	DC1_Memphis	ON	172.18.17.0/24	172.17.0.8	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
5	DC1_Oklahoma	ON	172.18.14.0/24	172.17.0.6	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
6	DC1_Miami	OFF	172.18.22.0/24	172.17.0.2	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
7	DC1_Charlotte	OFF	172.18.23.0/24	172.17.0.4	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
8	DC1_Dallas	OFF	172.18.24.0/24	172.17.0.5	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
9	DC1_Grand_Island	OFF	172.18.25.0/24	172.17.0.3	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
10	DC1_Branch20	OFF	172.18.20.0/24	172.17.0.11	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
11	DC1_Meridian	ON	172.18.13.0/24	172.17.0.10	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
12	DC1_Lodi	ON	172.18.16.0/24	172.17.0.12	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
13	DC1_Branch28	OFF	172.18.28.0/24	172.17.0.13	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
14	DC1_Branch29	OFF	172.18.29.0/24	172.17.0.14	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
15	DC1_Butte	ON	172.18.11.0/24	172.17.0.15	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1
16	DC1_Branch1	OFF	172.18.1.0/24	172.17.0.16	172.172.172.0/24,172.18.0.0/24,172.17.128.0/24,172.18.127.0/24,10.2.0.0/21,10.0.0.0/21	172.17.0.1

Template

Auto-configured VPN Tunnels

VPN Template

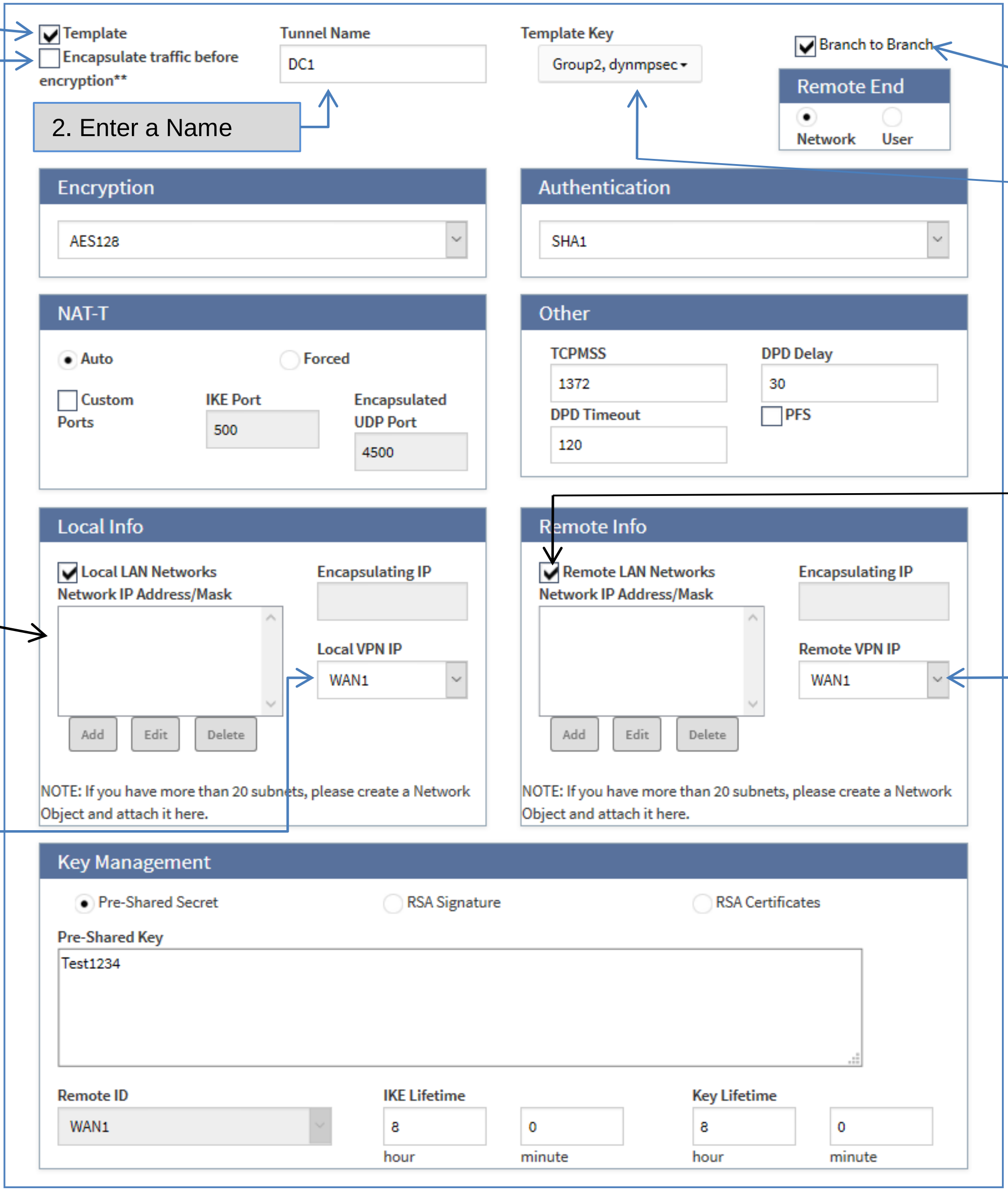
1. Check Template

Check this to create a single IPSec tunnel and encapsulate all matching traffic. This option is used when we have a large number of subnets that need to be encrypted.

5. Check this to use the LAN networks in the Local networks field.

Local Networks can be added if this is unchecked.

Choose an appropriate WAN as the VPN Local Endpoint.



☑ Template

□ Encapsulate traffic before encryption**

Tunnel Name: DC1

2. Enter a Name

Template Key: Group2, dynmpsec

☑ Branch to Branch

Remote End

● Network ○ User

Encryption

AES128

Authentication

SHA1

NAT-T

● Auto ○ Forced

□ Custom Ports

IKE Port: 500

Encapsulated UDP Port: 4500

Other

TCPMSS: 1372

DPD Delay: 30

DPD Timeout: 120

□ PFS

Local Info

☑ Local LAN Networks

Network IP Address/Mask

Encapsulating IP

Local VPN IP: WAN1

NOTE: If you have more than 20 subnets, please create a Network Object and attach it here.

Remote Info

☑ Remote LAN Networks

Network IP Address/Mask

Encapsulating IP

Remote VPN IP: WAN1

NOTE: If you have more than 20 subnets, please create a Network Object and attach it here.

Key Management

● Pre-Shared Secret ○ RSA Signature ○ RSA Certificates

Pre-Shared Key: Test1234

Remote ID: WAN1

IKE Lifetime: 8 hour 0 minute

Key Lifetime: 8 hour 0 minute

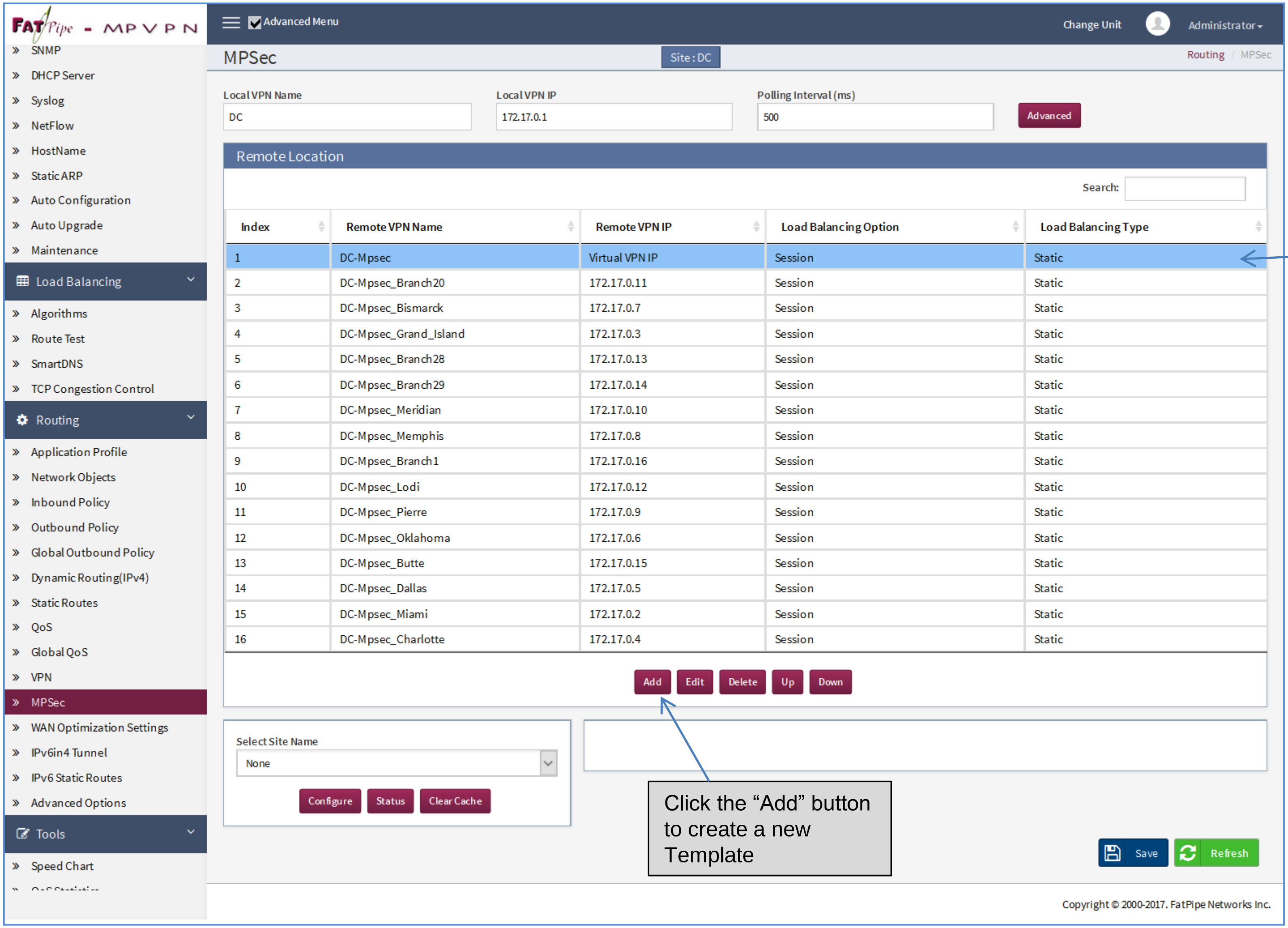
4. Hub and Spoke is the default topology Check this to create a Mesh topology.

3. Select the Template Keys

Check this to use the branch LAN networks in the remote networks field. Remote Networks can be added if this is unchecked.

Choose an appropriate WAN as the VPN Remote Endpoint.

MPSec Page



MPSec

Site : DC

Local VPN Name: DC

Local VPN IP: 172.17.0.1

Polling Interval (ms): 500

Remote Location

Index	Remote VPN Name	Remote VPN IP	Load Balancing Option	Load Balancing Type
1	DC-Mpsec	Virtual VPN IP	Session	Static
2	DC-Mpsec_Branch20	172.17.0.11	Session	Static
3	DC-Mpsec_Bismarck	172.17.0.7	Session	Static
4	DC-Mpsec_Grand_Island	172.17.0.3	Session	Static
5	DC-Mpsec_Branch28	172.17.0.13	Session	Static
6	DC-Mpsec_Branch29	172.17.0.14	Session	Static
7	DC-Mpsec_Meridian	172.17.0.10	Session	Static
8	DC-Mpsec_Memphis	172.17.0.8	Session	Static
9	DC-Mpsec_Branch1	172.17.0.16	Session	Static
10	DC-Mpsec_Lodi	172.17.0.12	Session	Static
11	DC-Mpsec_Pierre	172.17.0.9	Session	Static
12	DC-Mpsec_Oklahoma	172.17.0.6	Session	Static
13	DC-Mpsec_Butte	172.17.0.15	Session	Static
14	DC-Mpsec_Dallas	172.17.0.5	Session	Static
15	DC-Mpsec_Miami	172.17.0.2	Session	Static
16	DC-Mpsec_Charlotte	172.17.0.4	Session	Static

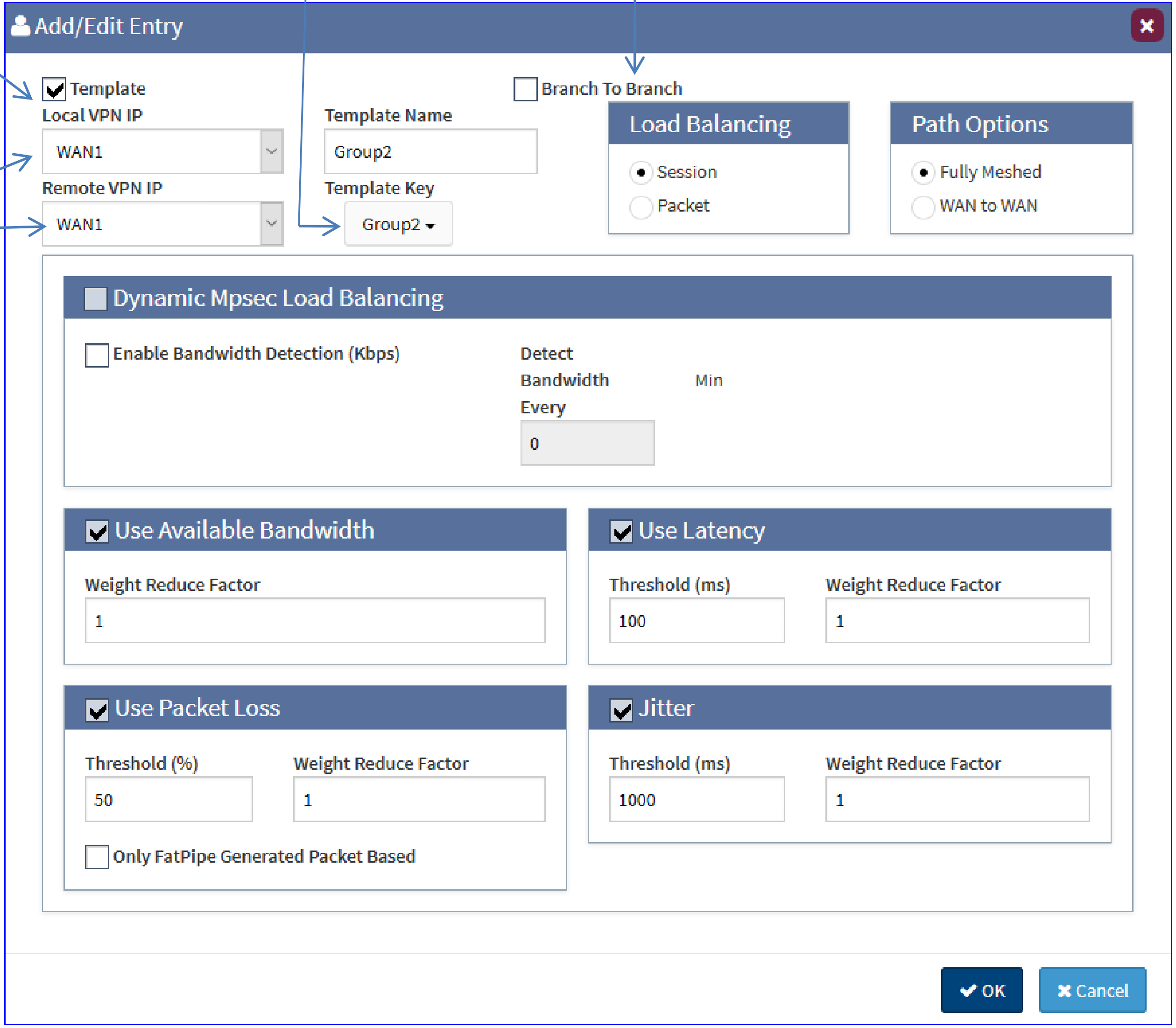
Select Site Name: None

Copyright © 2000-2017. FatPipe Networks Inc.

Template

Click the "Add" button to create a new Template

MPSec Template



1.Check Template

2.Select the Template Keys
You can choose more than 1 key.

3.Hub and Spoke is the default topology
Check this to create a Mesh topology.

4. Choose the appropriate VPN Endpoint. This should match the ones chosen in the VPN template

Add/Edit Entry

☑ Template

Local VPN IP: WAN1

Remote VPN IP: WAN1

Template Name: Group2

Template Key: Group2

□ Branch To Branch

Load Balancing

● Session
○ Packet

Path Options

● Fully Meshed
○ WAN to WAN

□ Dynamic Mpsec Load Balancing

□ Enable Bandwidth Detection (Kbps)

Detect Bandwidth Every: 0 Min

☑ Use Available Bandwidth

Weight Reduce Factor: 1

☑ Use Latency

Threshold (ms): 100
Weight Reduce Factor: 1

☑ Use Packet Loss

Threshold (%): 50
Weight Reduce Factor: 1

□ Only FatPipe Generated Packet Based

☑ Jitter

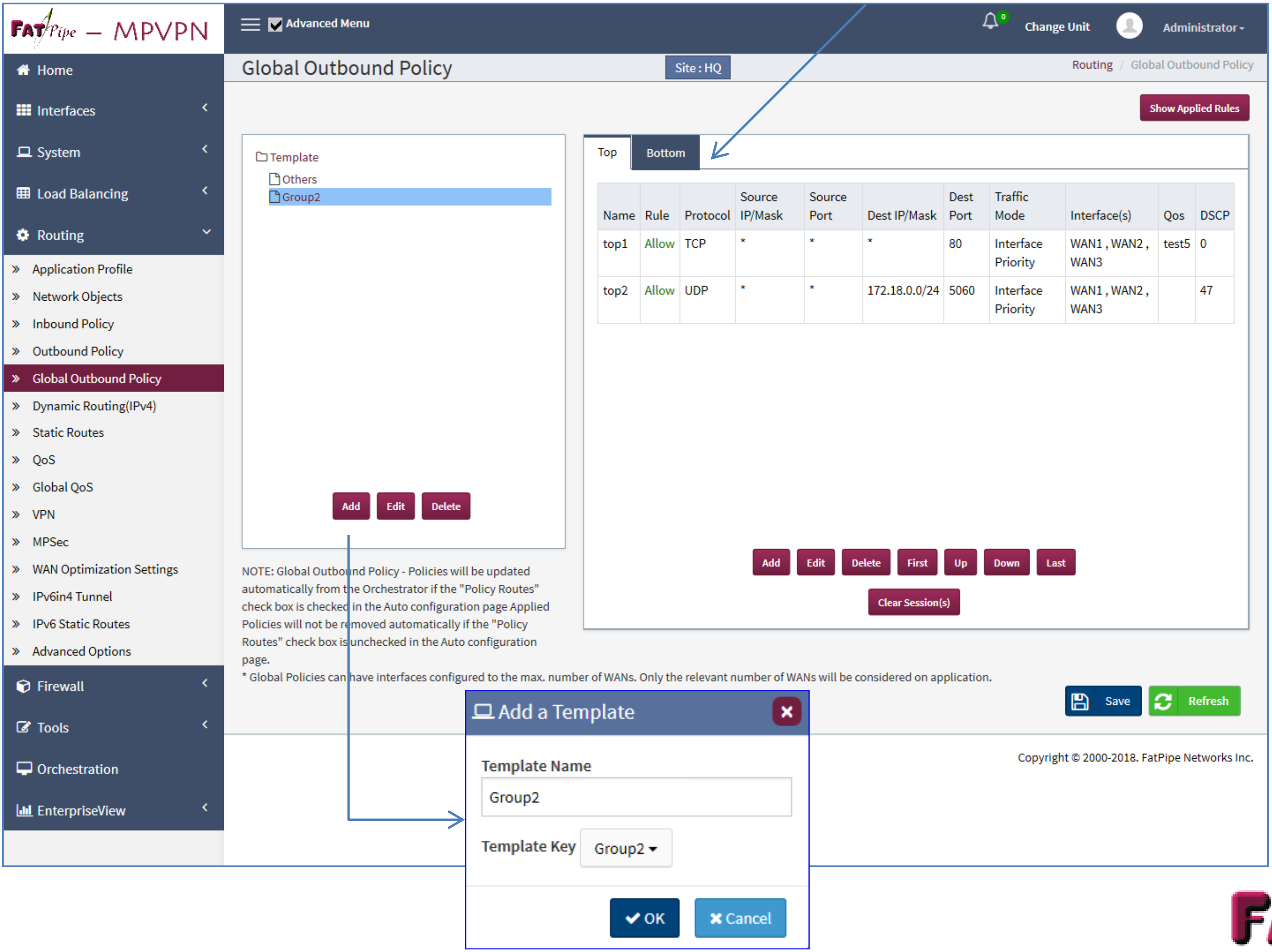
Threshold (ms): 1000
Weight Reduce Factor: 1

Global Outbound Policy Routing Rules - configuration

1.Create a Template

2. Assign Rules to the template

Top : Rules will be applied ABOVE all local rules.
Bottom : Rule will be applied BELOW all local rules.



Global Outbound Policy

Site : HQ

Name	Rule	Protocol	Source IP/Mask	Source Port	Dest IP/Mask	Dest Port	Traffic Mode	Interface(s)	Qos	DSCP
top1	Allow	TCP	*	*	*	80	Interface Priority	WAN1 , WAN2 , WAN3	test5	0
top2	Allow	UDP	*	*	172.18.0.0/24	5060	Interface Priority	WAN1 , WAN2 , WAN3		47

NOTE: Global Outbound Policy - Policies will be updated automatically from the Orchestrator if the "Policy Routes" check box is checked in the Auto configuration page Applied Policies will not be removed automatically if the "Policy Routes" check box is unchecked in the Auto configuration page.
* Global Policies can have interfaces configured to the max. number of WANs. Only the relevant number of WANs will be considered on application.

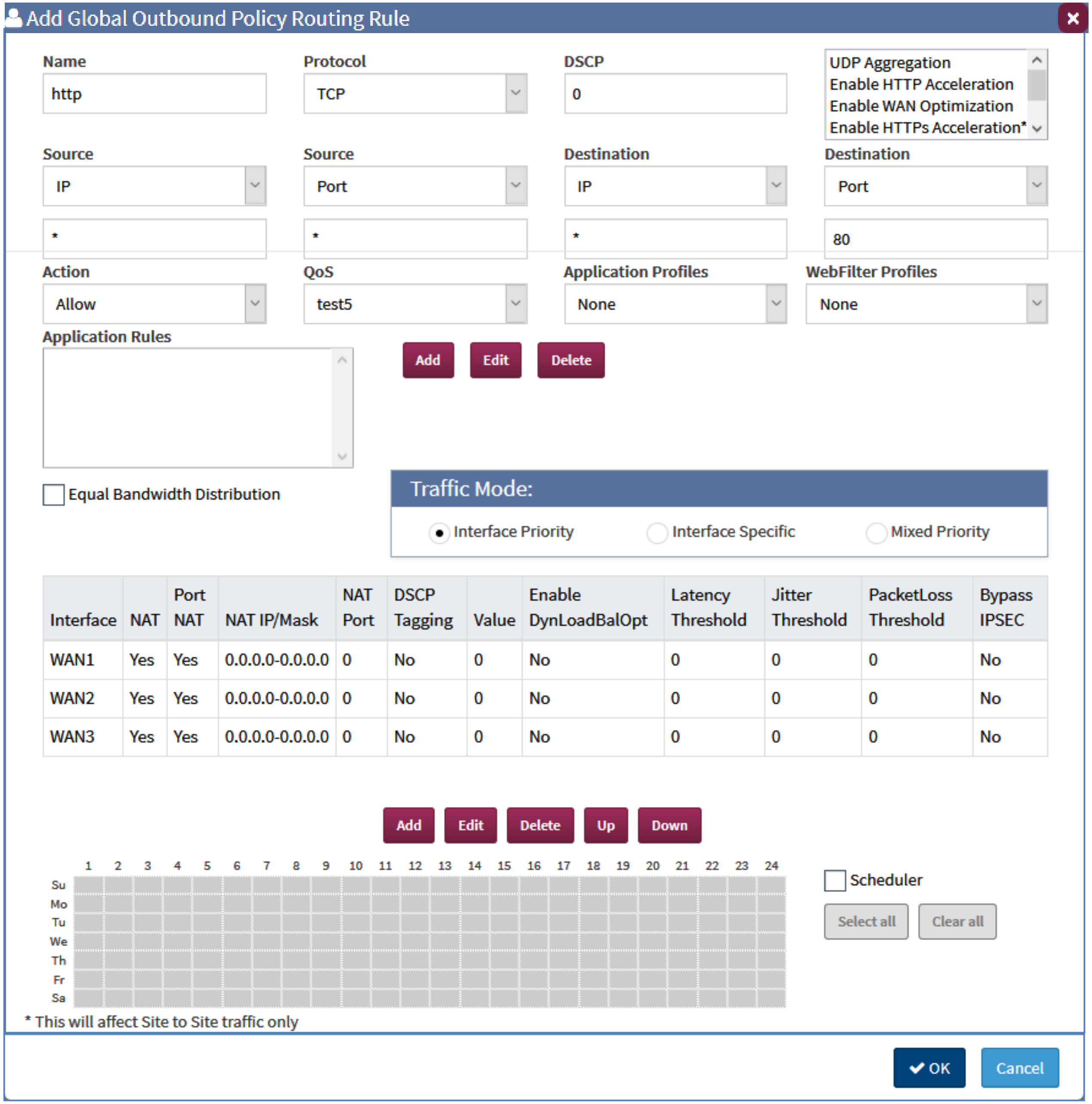
Copyright © 2000-2018. FatPipe Networks Inc.

Add a Template

Template Name: Group2

Template Key: Group2

Global Outbound Policy Routing Rules



Add Global Outbound Policy Routing Rule ×

Name	Protocol	DSCP	UDP Aggregation Enable HTTP Acceleration Enable WAN Optimization Enable HTTPs Acceleration*
http	TCP	0	
Source	Source	Destination	Destination
IP	Port	IP	Port
*	*	*	80
Action	QoS	Application Profiles	WebFilter Profiles
Allow	test5	None	None

Application Rules

Add Edit Delete

□ Equal Bandwidth Distribution

Traffic Mode:

● Interface Priority ○ Interface Specific ○ Mixed Priority

Interface	NAT	Port NAT	NAT IP/Mask	NAT Port	DSCP Tagging	Value	Enable DynLoadBalOpt	Latency Threshold	Jitter Threshold	PacketLoss Threshold	Bypass IPSEC
WAN1	Yes	Yes	0.0.0.0-0.0.0.0	0	No	0	No	0	0	0	No
WAN2	Yes	Yes	0.0.0.0-0.0.0.0	0	No	0	No	0	0	0	No
WAN3	Yes	Yes	0.0.0.0-0.0.0.0	0	No	0	No	0	0	0	No

Add Edit Delete Up Down

□ Scheduler

Select all Clear all

* This will affect Site to Site traffic only

✔ OK Cancel

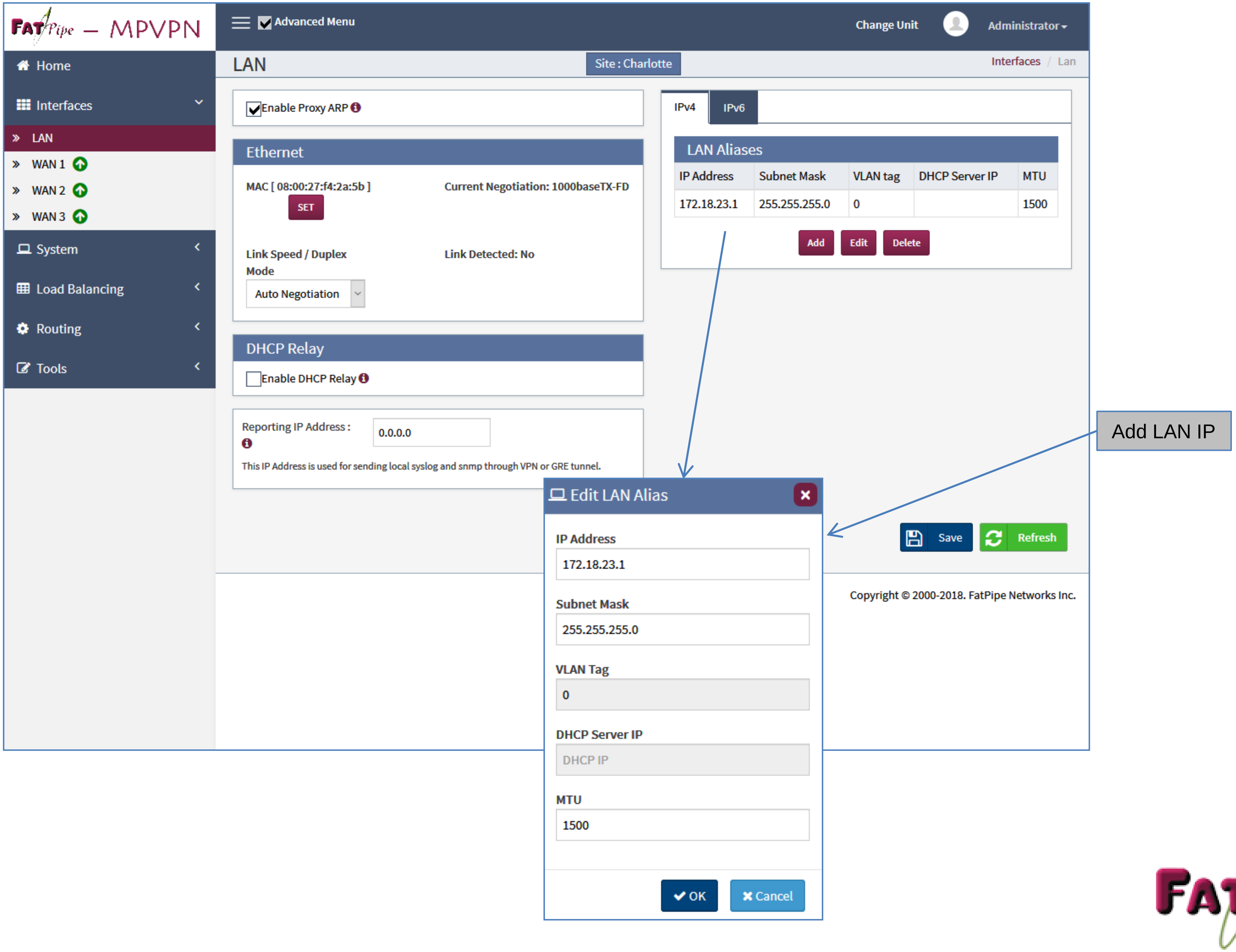
The PRR creation rules are the same as the regular Outbound Policy Routing Rules

Branch Configuration

1) Configure LAN IP
2) Configure WAN IP
3) Configure Orchestrator Information in Auto Configuration Page
4) Choose the modules that need to be auto configured.

Note : You can add only One Key Per Orchestrator

Branch Configuration – LAN Page



☑ Enable Proxy ARP

Ethernet

MAC [08:00:27:f4:2a:5b]

Current Negotiation: 1000baseTX-FD

Link Speed / Duplex Mode: Auto Negotiation

Link Detected: No

DHCP Relay

□ Enable DHCP Relay

Reporting IP Address : 0.0.0.0

This IP Address is used for sending local syslog and snmp through VPN or GRE tunnel.

LAN Aliases

IP Address	Subnet Mask	VLAN tag	DHCP Server IP	MTU
172.18.23.1	255.255.255.0	0		1500

Edit LAN Alias

IP Address: 172.18.23.1

Subnet Mask: 255.255.255.0

VLAN Tag: 0

DHCP Server IP: DHCP IP

MTU: 1500

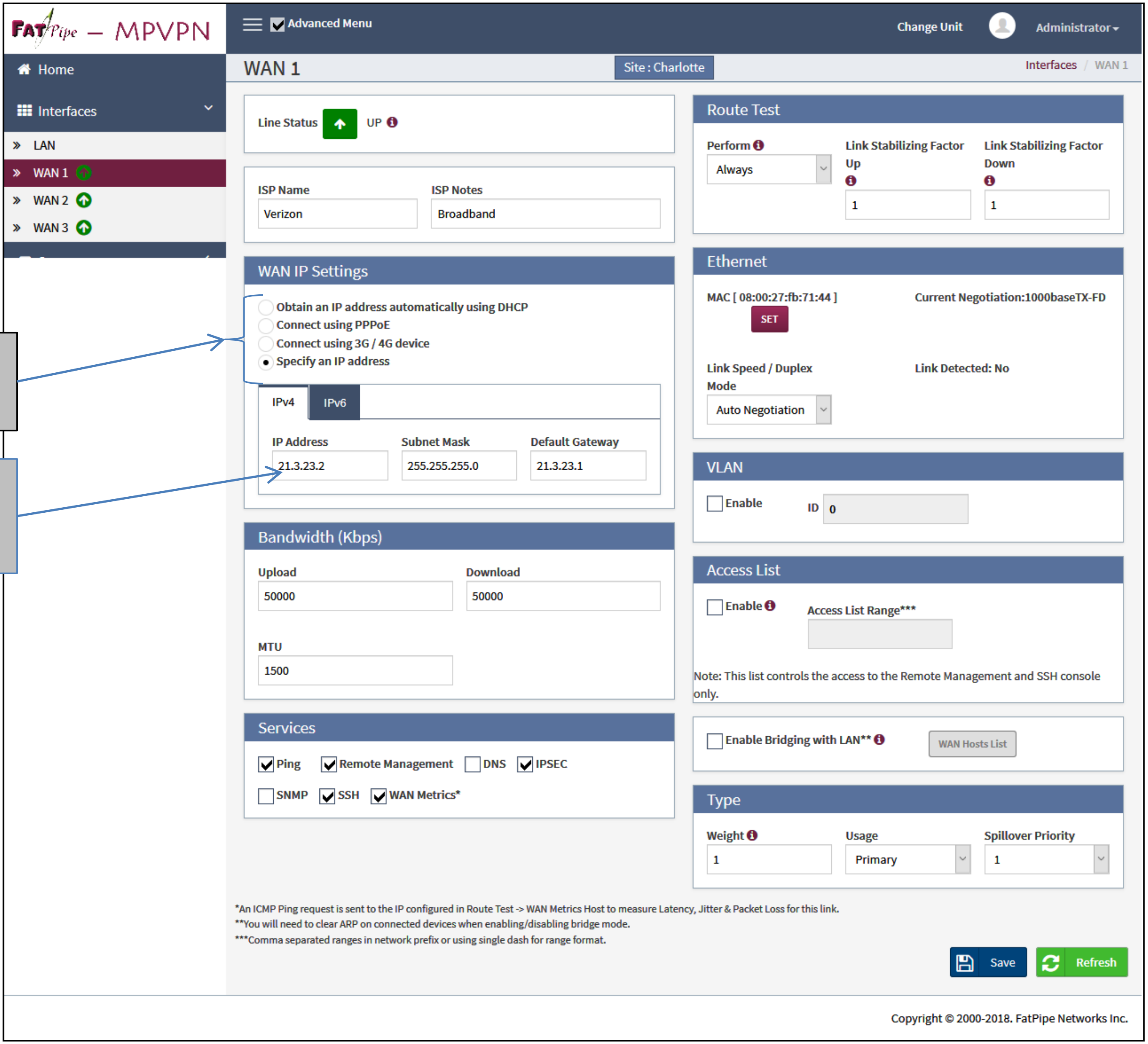
Copyright © 2000-2018. FatPipe Networks Inc.

Add LAN IP

Branch Configuration – WAN Page

Choose the ISP connection type

Configure WAN IP if the IP is Static.



WAN 1

Site : Charlotte

Line Status UP

ISP Name	ISP Notes
Verizon	Broadband

WAN IP Settings

○ Obtain an IP address automatically using DHCP
○ Connect using PPPoE
○ Connect using 3G / 4G device
● Specify an IP address

IPv4 | IPv6

IP Address	Subnet Mask	Default Gateway
21.3.23.2	255.255.255.0	21.3.23.1

Bandwidth (Kbps)

Upload	Download
50000	50000

MTU: 1500

Services

☑ Ping ☑ Remote Management □ DNS ☑ IPSEC
□ SNMP ☑ SSH ☑ WAN Metrics*

Route Test

Perform	Link Stabilizing Factor Up	Link Stabilizing Factor Down
Always	1	1

Ethernet

MAC [08:00:27:fb:71:44] SET

Current Negotiation:1000baseTX-FD

Link Speed / Duplex Mode: Auto Negotiation

Link Detected: No

VLAN

□ Enable ID 0

Access List

□ Enable

Access List Range***

Note: This list controls the access to the Remote Management and SSH console only.

□ Enable Bridging with LAN** WAN Hosts List

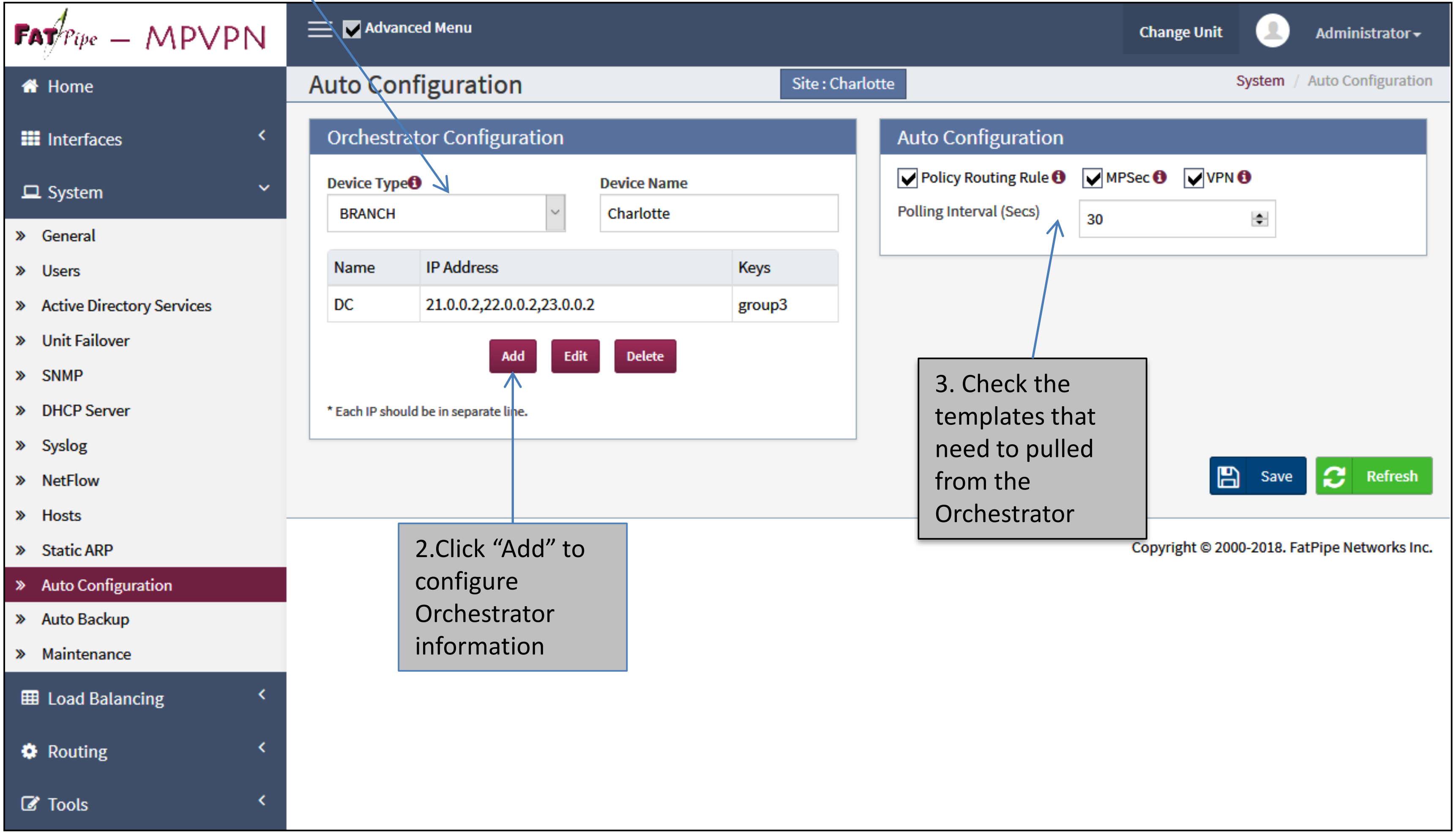
Type

Weight	Usage	Spillover Priority
1	Primary	1

*An ICMP Ping request is sent to the IP configured in Route Test -> WAN Metrics Host to measure Latency, Jitter & Packet Loss for this link.
**You will need to clear ARP on connected devices when enabling/disabling bridge mode.
***Comma separated ranges in network prefix or using single dash for range format.

Save Refresh

Branch - Auto Configuration Page



1.Choose Device type as Branch

2.Click “Add” to configure Orchestrator information

3. Check the templates that need to pulled from the Orchestrator

Auto Configuration

Orchestrator Configuration

Device Type: BRANCH

Device Name: Charlotte

Name	IP Address	Keys
DC	21.0.0.2,22.0.0.2,23.0.0.2	group3

* Each IP should be in separate line.

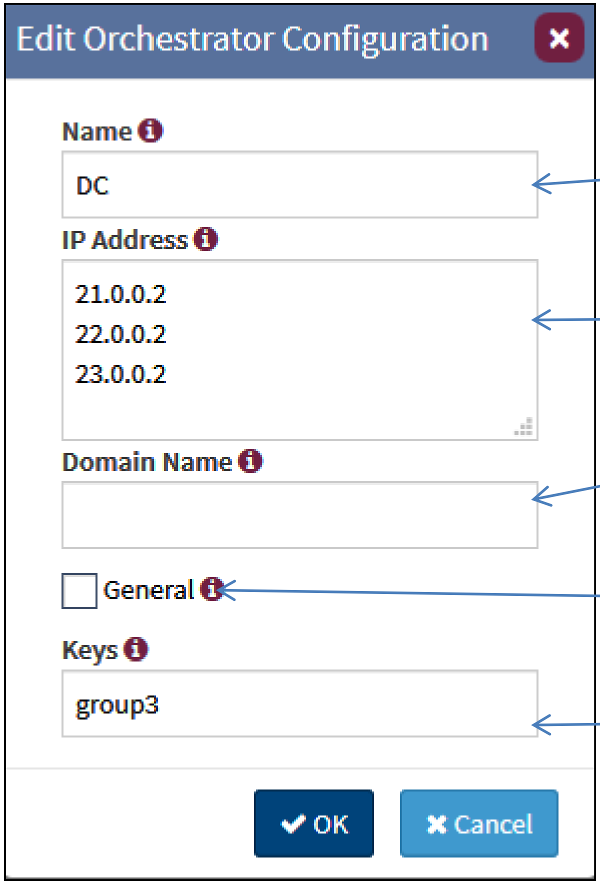
Auto Configuration

☑ Policy Routing Rule ☑ MPSec ☑ VPN

Polling Interval (Secs): 30

Copyright © 2000-2018. FatPipe Networks Inc.

Branch – Add Orchestrator Configuration



Edit Orchestrator Configuration

Name
DC

IP Address
21.0.0.2
22.0.0.2
23.0.0.2

Domain Name

□ General

Keys
group3

Provide a Name to identify the server

Add an IP of the Orchestrator.

You can add one or more IPs.

Enter the URI if you have one.
E.g. autoconfig.example.com

Check this to copy the General Settings from this orchestrator including NTP settings

Add the key configured on the Orchestrator.
This key will be used to identify the unit and hand out the respective templates.

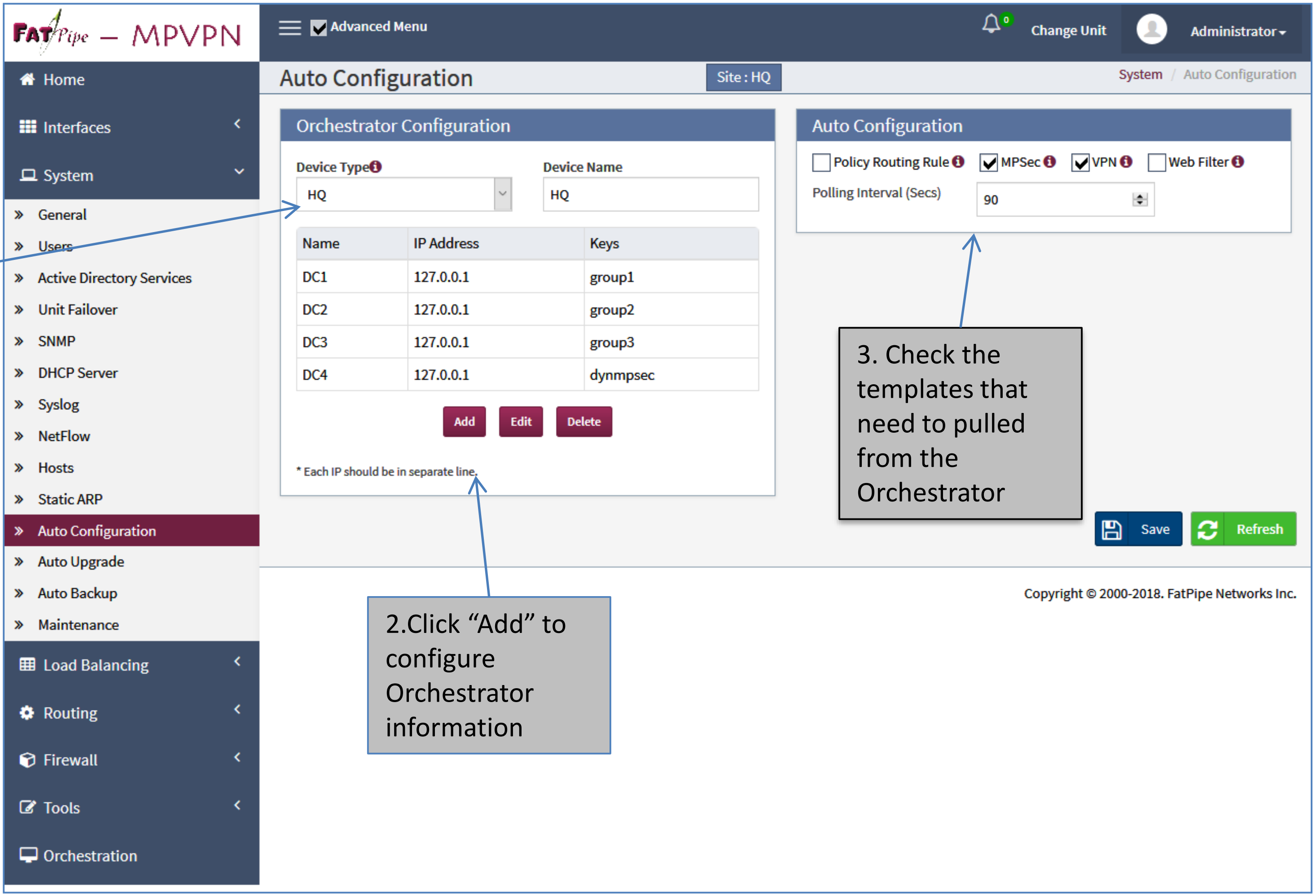
HQ Configuration

1) Configure LAN IP
2) Configure WAN IP
3) Configure Orchestrator Information in Auto Configuration Page
4) Choose HQ as the Device Type
5) Choose the modules that need to be auto configured.

Note : You can configure more than one key per orchestrator to facilitate the HQ/DC unit to talk to multiple Groups.

HQ Device Configuration – Auto Configuration Page

Choose "HQ" from the dropdown



Auto Configuration

Site : HQ

Orchestrator Configuration

Device Type: HQ

Device Name: HQ

Name	IP Address	Keys
DC1	127.0.0.1	group1
DC2	127.0.0.1	group2
DC3	127.0.0.1	group3
DC4	127.0.0.1	dynmpsec

* Each IP should be in separate line.

Auto Configuration

□ Policy Routing Rule ☑ MPSec ☑ VPN □ Web Filter

Polling Interval (Secs): 90

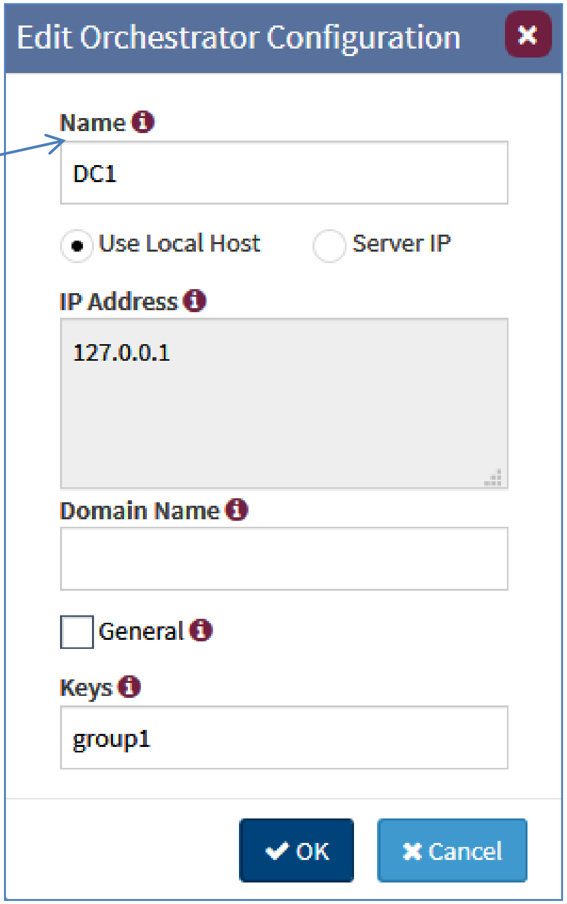
Copyright © 2000-2018. FatPipe Networks Inc.

2.Click "Add" to configure Orchestrator information

3. Check the templates that need to pulled from the Orchestrator

HQ Device Configuration – Add Orchestrator Configuration

1. Choose
 “Use Localhost”
If the orchestration is done on the HQ unit itself



Edit Orchestrator Configuration

Name: DC1

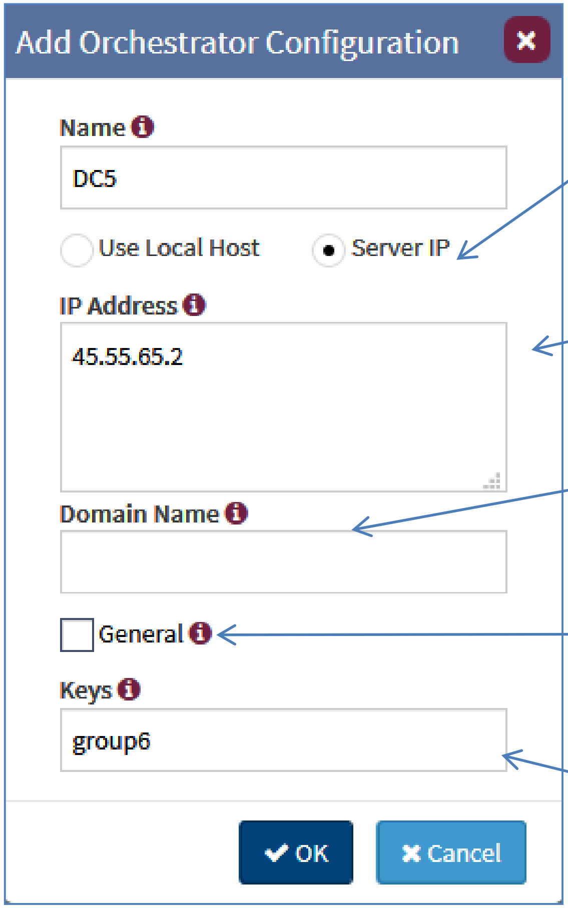
● Use Local Host ○ Server IP

IP Address: 127.0.0.1

Domain Name:

□ General

Keys: group1



Add Orchestrator Configuration

Name: DC5

○ Use Local Host ● Server IP

IP Address: 45.55.65.2

Domain Name:

□ General

Keys: group6

1. Choose
 “Server IP”
If the orchestrator is a separate device.

2. Configure the Orchestrator’s IP(s).
You can add multiple Ips.

Enter the URI if you have one. E.g. autoconfig.example.com

Check this to copy the General Settings from this orchestrator including NTP settings

Add the key configured on the Orchestrator. This key will be used to identify the unit and hand out the respective templates.

Thank You

FATPipe