Table of Contents

Written and tested with FMG 7.0.3 and FGT 7.0.5

Create “FOUNDATION1” ADOM

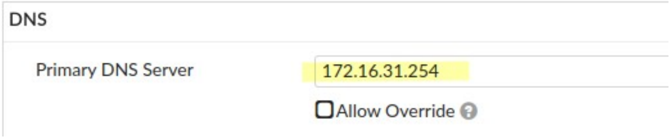
Create device groups

* WEST-DATACENTERS
* WEST-BRANCHES
* EAST-DATACENTERS
* EAST-BRANCHES

Provisioning templates

System template

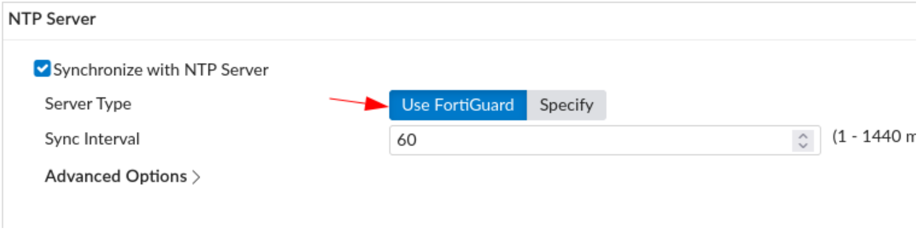
Configure the “default” system template:



DNS

Primary DNS Server: 172.16.31.254

□ Allow Override



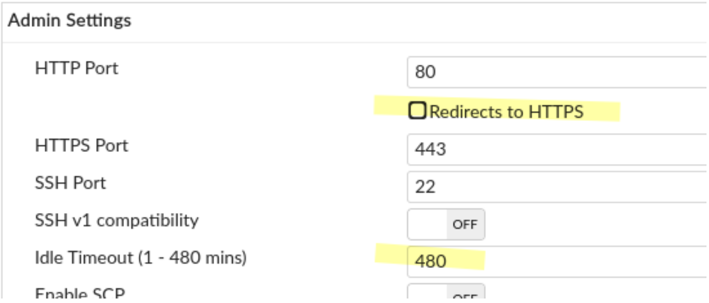
NTP Server

☑ Synchronize with NTP Server

Server Type: [✓ Use FortiGuard] Specify

Sync Interval: 60 (1 - 1440 m

Advanced Options >



Admin Settings

HTTP Port: 80

□ Redirects to HTTPS

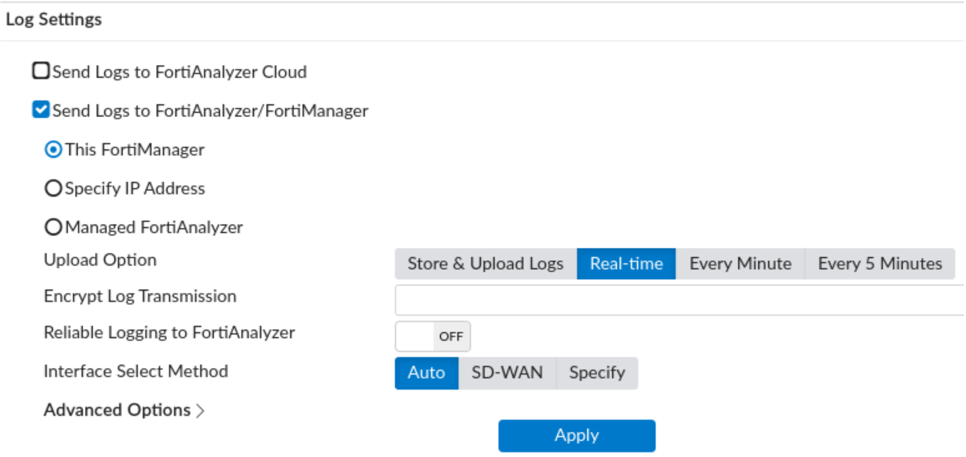
HTTPS Port: 443

SSH Port: 22

SSH v1 compatibility: OFF

Idle Timeout (1 - 480 mins): 480

Enable SCP: OFF



Log Settings

□ Send Logs to FortiAnalyzer Cloud

☑ Send Logs to FortiAnalyzer/FortiManager

● This FortiManager

○ Specify IP Address

○ Managed FortiAnalyzer

Upload Option: Store & Upload Logs [✓ Real-time] Every Minute Every 5 Minutes

Encrypt Log Transmission

Reliable Logging to FortiAnalyzer: OFF

Interface Select Method: [✓ Auto] SD-WAN Specify

Advanced Options >

Apply

System templates cannot be assigned to groups. It’s FMG bug which complains the groups do not have meta-data. Individual devices are therefore assigned to this template groups during on-boarding.

Pre-Run CLI Template

Models based off FGT-VM have a single interface.
Need to create a Jinja script Pre-Run CLI template which creates the 10 interfaces for our FGT-VM models.

```
{# EXAMPLE: Use this file as a Pre-Run CLI Template for FGT-VM Model Devices #}

{# Create physical interface from port1 to port10 #}
config system interface
   {% for i in range(1,11) %}
   edit "port{{i}}"
    set vdom "root"
    set type physical
   next
   {% endfor %}
end

{# Use this for successful onboarding, when your FGT is preconfigured (Low-Touch Provisioning) #}
config system admin
  edit "admin"
    set password fortinet
  next
end
```

Create the "SETTINGS.DEVICES" Post-Run jinja template

Import the jinja templates

Import the CLI jinja templates.

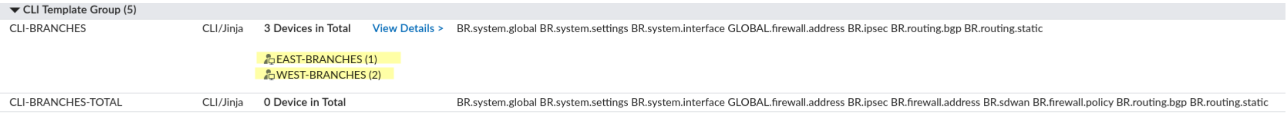
* Jinja files in BRANCHES and DATACENTERS folders of PoC6
Select "routing.objects1.conf" or "routing.objects2.conf" depending on context:
* cross-region shortcut allowed => objects1.conf
* no cross-region shortcut => objects2.conf

* firewall.address from BOOTSTRAP PoC

Make "FMG_FORTIGATE_ID" a *required* Device meta-field.
Keep all other meta fields as *Optional*.

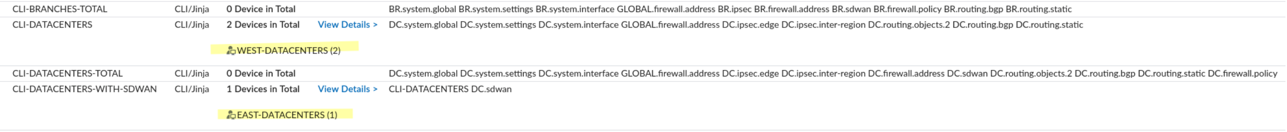
Create the template groups:

* Template groups for Branches



▼ CLI Template Group (5)				
CLI-BRANCHES	CLI/Jinja	**3 Devices in Total** EAST-BRANCHES (1) WEST-BRANCHES (2)	View Details >	BR.system.global BR.system.settings BR.system.interface GLOBAL.firewall.address BR.ipsec BR.routing.bgp BR.routing.static
CLI-BRANCHES-TOTAL	CLI/Jinja	**0 Device in Total**		BR.system.global BR.system.settings BR.system.interface GLOBAL.firewall.address BR.ipsec BR.firewall.address BR.sdwan BR.firewall.policy BR.routing.bgp BR.routing.static

* Template groups for Datacenters



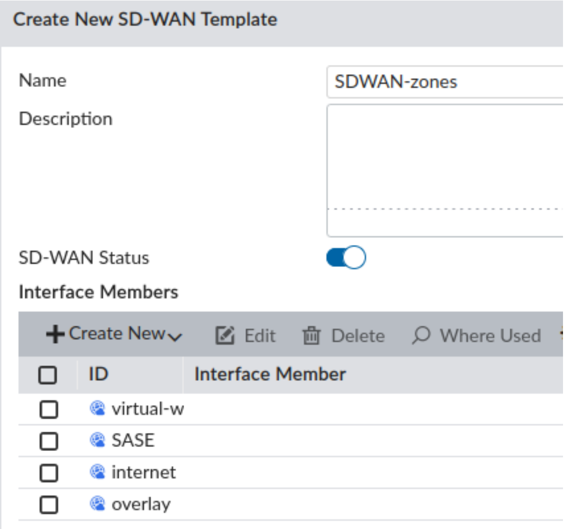
CLI-BRANCHES-TOTAL	CLI/Jinja	**0 Device in Total**		BR.system.global BR.system.settings BR.system.interface GLOBAL.firewall.address BR.ipsec BR.firewall.address BR.sdwan BR.firewall.policy BR.routing.bgp BR.routing.static
CLI-DATACENTERS	CLI/Jinja	**2 Devices in Total** WEST-DATACENTERS (2)	View Details >	DC.system.global DC.system.settings DC.system.interface GLOBAL.firewall.address DC.ipsec.edge DC.ipsec.inter-region DC.routing.objects.2 DC.routing.bgp DC.routing.static
CLI-DATACENTERS-TOTAL	CLI/Jinja	**0 Device in Total**		DC.system.global DC.system.settings DC.system.interface GLOBAL.firewall.address DC.ipsec.edge DC.ipsec.inter-region DC.firewall.address DC.sdwan DC.routing.objects.2 DC.routing.bgp DC.routing.static DC.firewall.policy
CLI-DATACENTERS-WITH-SDWAN	CLI/Jinja	**1 Devices in Total** EAST-DATACENTERS (1)	View Details >	CLI-DATACENTERS DC.sdwan

Assign the template groups to the corresponding device groups:

* CLI-DATACENTERS to device group "WEST-DATACENTERS"
* CLI-DATACENTERS-WITH-SDWAN to device group "EAST-DATACENTERS"
* "CLI-BRANCHES" to device groups "WEST-DATACENTERS" and "EAST-DATACENTERS"

Create an "SD-WAN-zones" template

Create empty zones "internet" and "overlay".



Name	SDWAN-zones
Description	
SD-WAN Status	●
Interface Members	

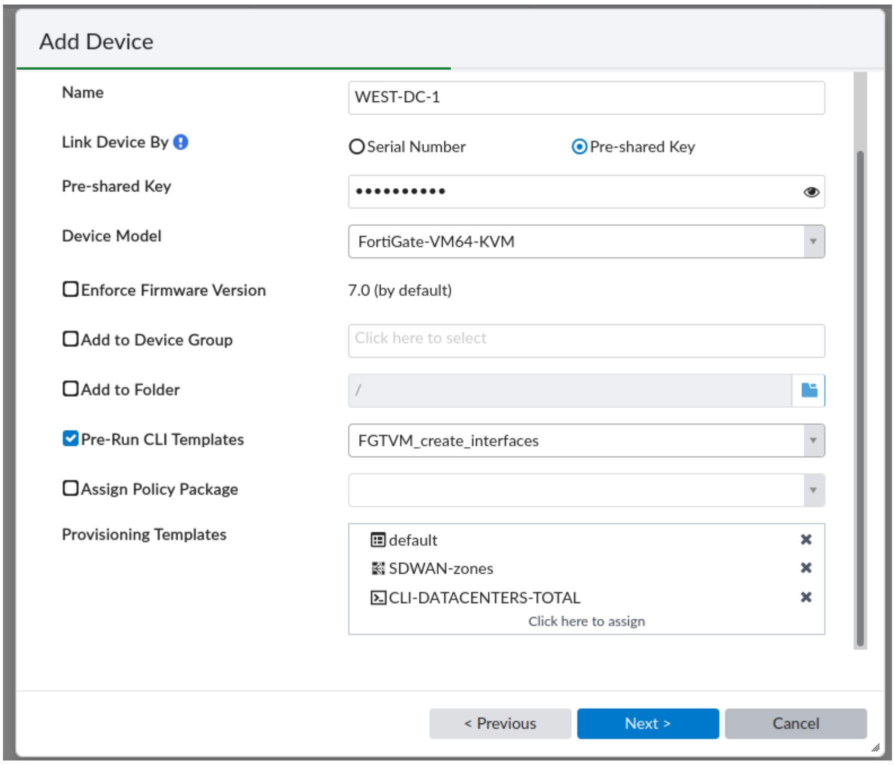
□	ID	Interface Member
□	virtual-w	
□	SASE	
□	internet	
□	overlay	

These zones are referenced in the SD-WAN default static routes.
So they are needed for the "routing.static" jinja template.

Provisioning WEST-DC-1

This device is a reference device which will be used to:
* create an SDWAN template from its SDWAN jinja file
* create a policy package from its fw-addr and fw-policy jinja files

Create a model device



Name	WEST-DC-1
Link Device By	○ Serial Number ● Pre-shared Key
Pre-shared Key	••••••••••
Device Model	FortiGate-VM64-KVM
□ Enforce Firmware Version	7.0 (by default)
□ Add to Device Group	Click here to select
□ Add to Folder	/
☑ Pre-Run CLI Templates	FGTVM_create_interfaces
□ Assign Policy Package	
Provisioning Templates	default SDWAN-zones CLI-DATACENTERS-TOTAL

No device group is specified.
No PP is specified since the firewall addresses and policies are pushed by Jinja templates.

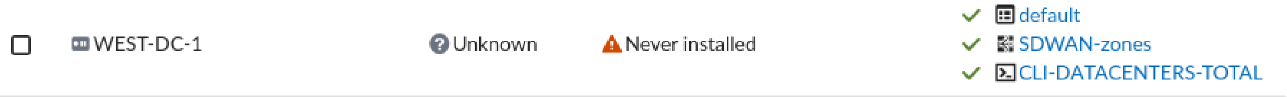
Fill meta-data and location

FMG_FORTIGATE_ID: FGT-W-DC1

dc_id: 1 will be used for the SD-WAN template to distinguish FGT-W-DC1 and FGT-W-DC2
location: Paris

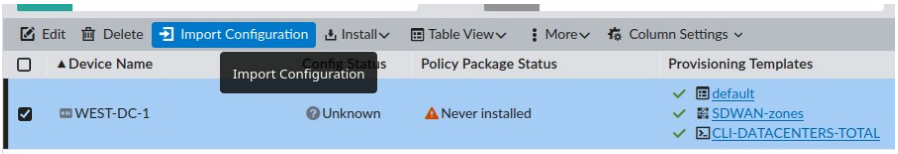
Install config on model device

install device-db settings with “Quick Install (Device DB)”

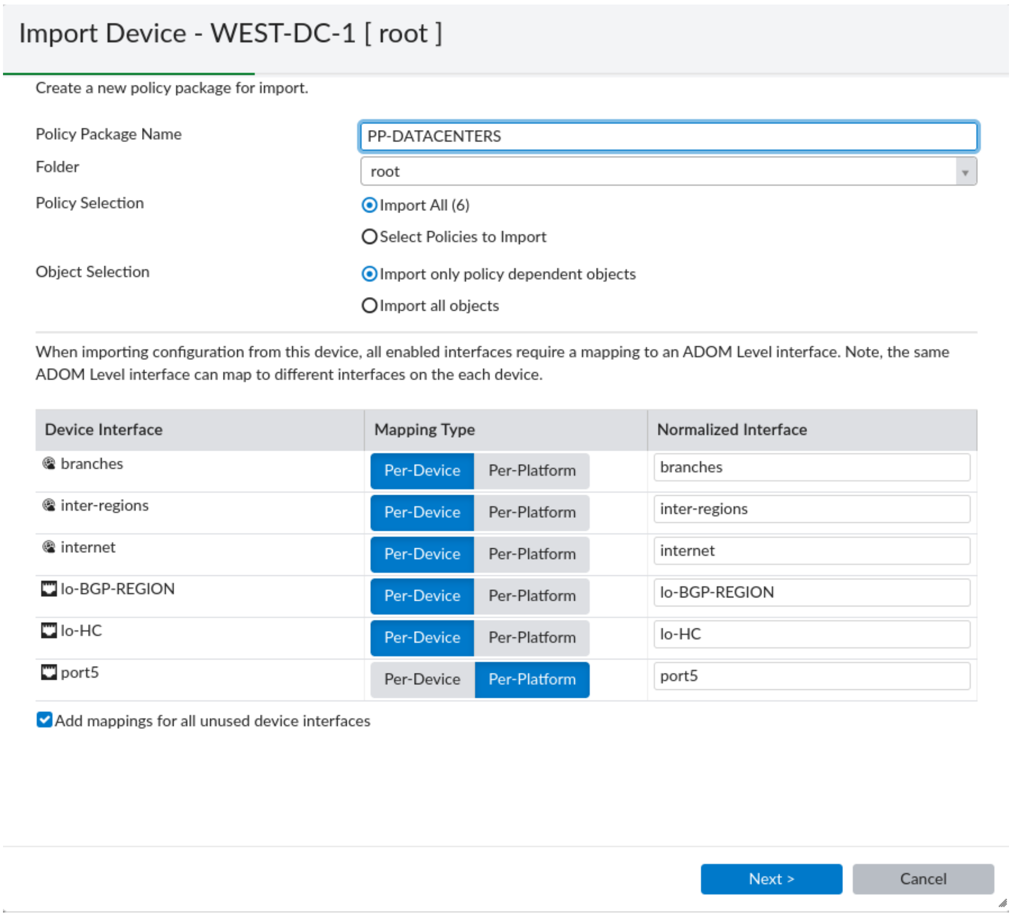


□	WEST-DC-1	Unknown	Never installed	✓ default ✓ SDWAN-zones ✓ CLI-DATACENTERS-TOTAL

Import policy-package from the device



□	Device Name	Config Status	Policy Package Status	Provisioning Templates
☑	WEST-DC-1	Unknown	Never installed	✓ default ✓ SDWAN-zones ✓ CLI-DATACENTERS-TOTAL



Import Device - WEST-DC-1 [root]

Create a new policy package for import.

Policy Package Name: PP-DATACENTERS

Folder: root

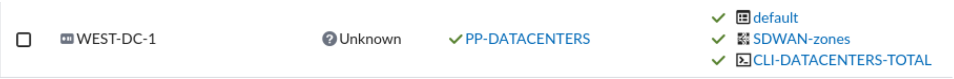
Policy Selection: ● Import All (6) ○ Select Policies to Import

Object Selection: ● Import only policy dependent objects ○ Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	Mapping Type	Normalized Interface
branches	[✓ Per-Device] Per-Platform	branches
inter-regions	[✓ Per-Device] Per-Platform	inter-regions
internet	[✓ Per-Device] Per-Platform	internet
lo-BGP-REGION	[✓ Per-Device] Per-Platform	lo-BGP-REGION
lo-HC	[✓ Per-Device] Per-Platform	lo-HC
port5	Per-Device [✓ Per-Platform]	port5

☑ Add mappings for all unused device interfaces



□	WEST-DC-1	Unknown	✓ PP-DATACENTERS	✓ default ✓ SDWAN-zones ✓ CLI-DATACENTERS-TOTAL

Go to the PP and change the “Installation Taget”

Remove “WEST-DC-1” and associate groups “WEST-DATACENTERS” and “EAST-DATACENTERS”

Import SD-WAN template from the device

Name= SDWAN-WEST-DATACENTERS

Assign this SDWAN template to the WEST-DATACENTERS device group

Edit the template to make it valid for both WEST-DC-1 and WEST-DC-2

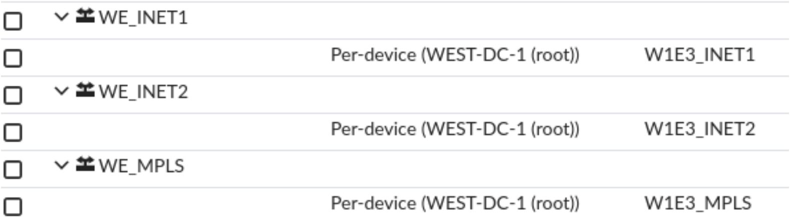
Change:

100.64.11.254	to	100.64.$(dc_id)1.254	Internet_1
100.64.12.254	to	100.64.$(dc_id)2.254	Internet_2
W1E3_INET1	to	W$(dc_id)E3_INET1	inter-region members **AND “input-device” in rule 7**
W1E3_INET2	to	W$(dc_id)E3_INET2	inter-region members **AND “input-device” in rule 8**
W1E3_MPLS	to	W$(dc_id)E3_MPLS	inter-region members **AND “input-device” in rule 9**

Rename some normalized interfaces

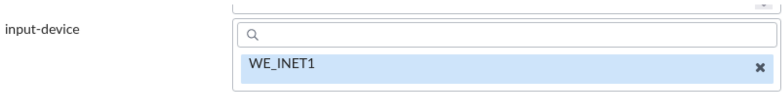
W1E3_INET1, W1E3_INET2 and W1E3_MPLS are used as “input-device” in sdwan rules 7,8,9
They must be normalized interfaces
We must make them generic name because they will be normalized for WEST-DC1 and WEST-DC2

Rename then WE_….



□	WE_INET1		
□		Per-device (WEST-DC-1 (root))	W1E3_INET1
□	WE_INET2		
□		Per-device (WEST-DC-1 (root))	W1E3_INET2
□	WE_MPLS		
□		Per-device (WEST-DC-1 (root))	W1E3_MPLS

The interface name is automatically changed in the “input-device” of rules 7,8,9:



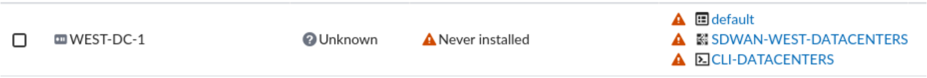
input-device: WE_INET1

Change the provisioning templates assignment for this device

Remove “SDWAN-zones”
Remove “CLI-DATACENTERS-TOTAL”

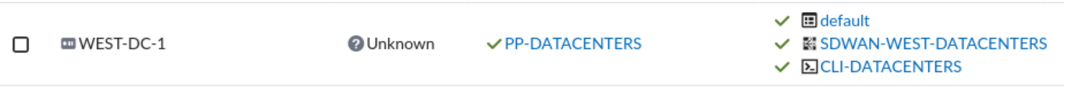
Assign this device to group “WEST-DATACENTERS”

WEST-DC-1 gets assigned the SD-WAN template, the PP and the CLI template from its group:



□	WEST-DC-1	Unknown	Never installed	default SDWAN-WEST-DATACENTERS CLI-DATACENTERS

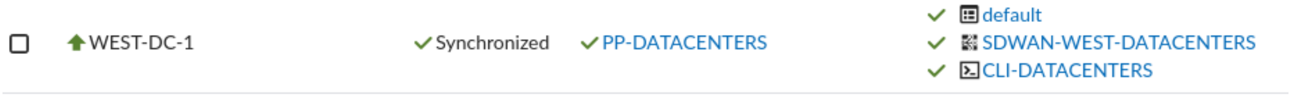
Install Wizard Policy Package “PP-DATACENTERS”



□	WEST-DC-1	Unknown	✓ PP-DATACENTERS	✓ default ✓ SDWAN-WEST-DATACENTERS ✓ CLI-DATACENTERS

On-board the real device (low-touch provisioning)

```
# exec central-mgmt register-device FMG-VM0A13000123 <psk-of-model-device>
```



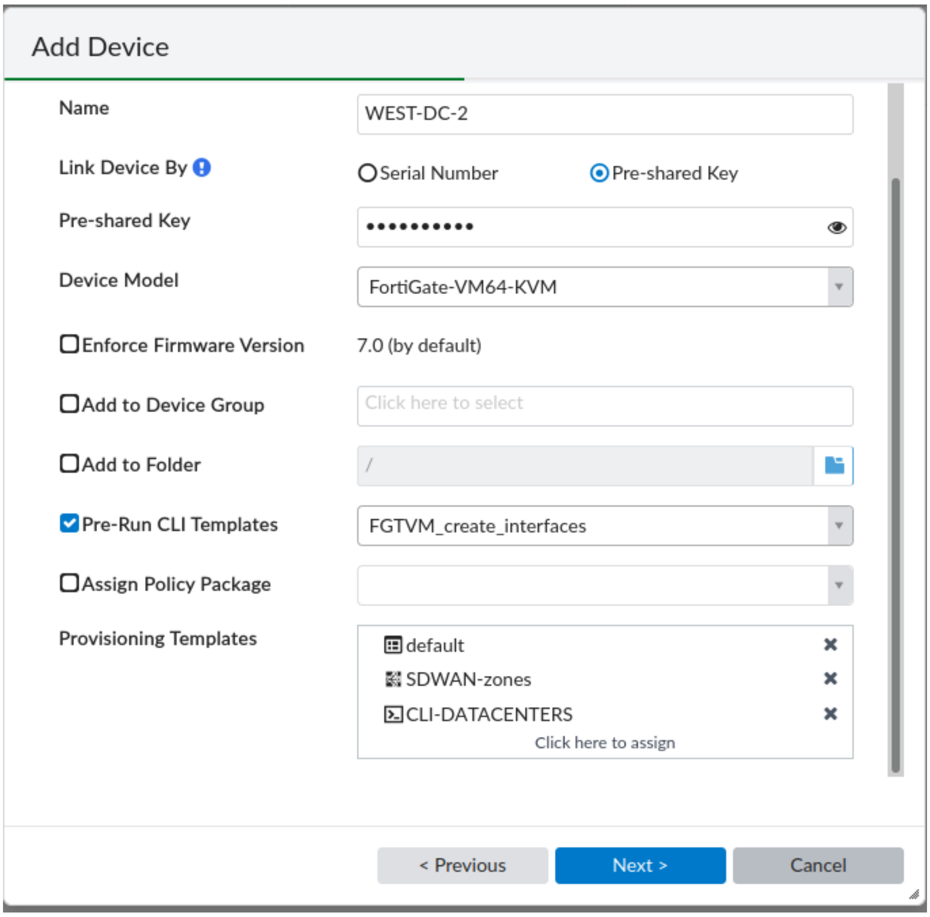
☐	⬆ WEST-DC-1	✓ Synchronized	✓ PP-DATACENTERS	✓ default ✓ SDWAN-WEST-DATACENTERS ✓ CLI-DATACENTERS

Provisioning WEST-DC-2

SDWAN-WEST-DATACENTERS has manual sdwan rules with “input-device” referencing interfaces.
These interfaces must be normalized interfaces :-(
It complicates the on-boarding since these normalized interfaces must be created. And to do so, they must exists in the device-db. And to do so, we must create the overlay interfaces on the model device.

Simplest approach I found is to model this device with almost the same logic as WEST-DC-1.
Except that, here, the CLI group is “CLI-DATACENTERS” which only contains underlay, overlay and routing. It does not contain SDWAN and FW-POLICIES (unlike “CLI-DATACENTERS-TOTAL”).
SDWAN and FW-policies will be associated to this device after it is assigned to its group.

Create a model device



Add Device

Name: WEST-DC-2

Link Device By: ○ Serial Number ● Pre-shared Key

Pre-shared Key: ••••••••••

Device Model: FortiGate-VM64-KVM

☐ Enforce Firmware Version: 7.0 (by default)

☐ Add to Device Group: Click here to select

☐ Add to Folder: /

☑ Pre-Run CLI Templates: FGTVM_create_interfaces

☐ Assign Policy Package:

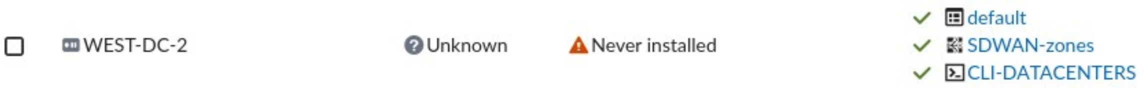
Provisioning Templates:
- default
- SDWAN-zones
- CLI-DATACENTERS

Fill meta-data and location

FMG_FORTIGATE_ID: FGT-W-DC2
dc_id: 2 will be used for the SD-WAN template to distinguish FGT-W-DC1 and FGT-W-DC2
location: Lyon

Install config on model device

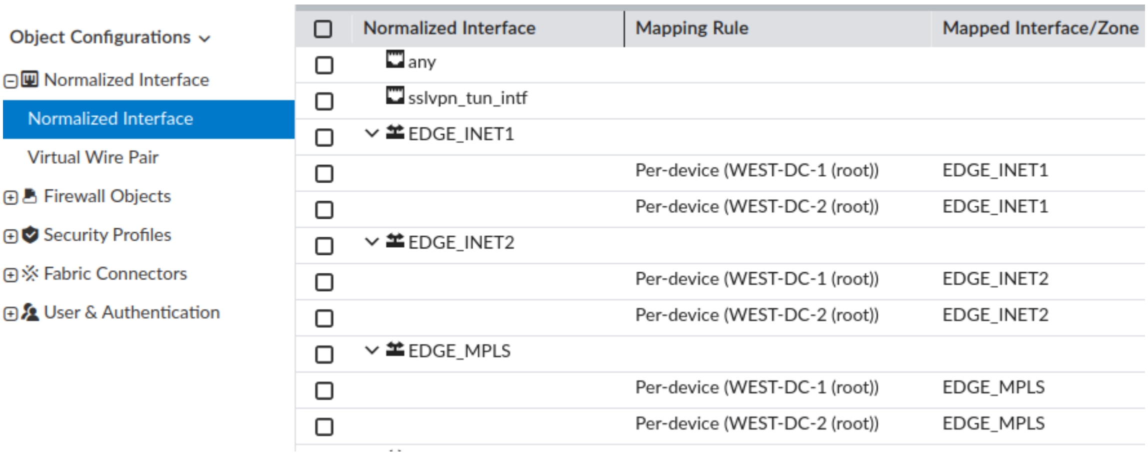
install device-db settings with “Quick Install (Device DB)”



□	WEST-DC-2	Unknown	Never installed	✓ default ✓ SDWAN-zones ✓ CLI-DATACENTERS

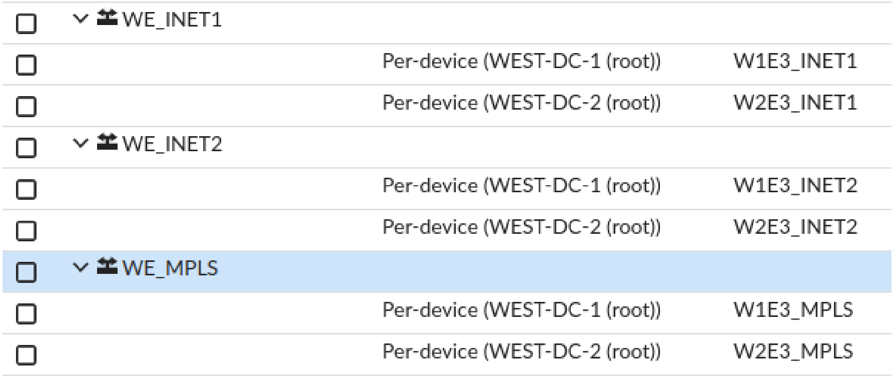
Normalize the interfaces used as “input-device” in SDWAN

EDGE_INET1, EDGE_INET2 and EDGE_MPLS are used as “input-device” in rules 1-6



□	Normalized Interface	Mapping Rule	Mapped Interface/Zone
□	any		
□	sslvpn_tun_intf		
□	EDGE_INET1		
□		Per-device (WEST-DC-1 (root))	EDGE_INET1
□		Per-device (WEST-DC-2 (root))	EDGE_INET1
□	EDGE_INET2		
□		Per-device (WEST-DC-1 (root))	EDGE_INET2
□		Per-device (WEST-DC-2 (root))	EDGE_INET2
□	EDGE_MPLS		
□		Per-device (WEST-DC-1 (root))	EDGE_MPLS
□		Per-device (WEST-DC-2 (root))	EDGE_MPLS

W2E3_INET1, W2E3_INET2, W2E3_MPLS are used as “input-device” in rules 7,8,9

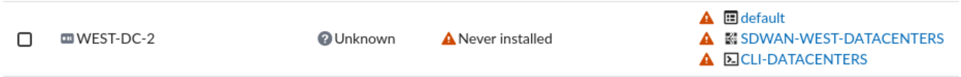


□	WE_INET1		
□		Per-device (WEST-DC-1 (root))	W1E3_INET1
□		Per-device (WEST-DC-2 (root))	W2E3_INET1
□	WE_INET2		
□		Per-device (WEST-DC-1 (root))	W1E3_INET2
□		Per-device (WEST-DC-2 (root))	W2E3_INET2
□	WE_MPLS		
□		Per-device (WEST-DC-1 (root))	W1E3_MPLS
□		Per-device (WEST-DC-2 (root))	W2E3_MPLS

Assign this device to group “WEST-DATACENTERS”

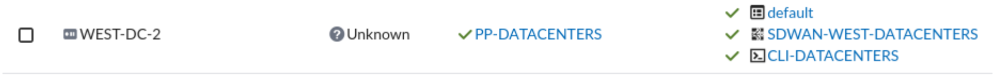
Remove “SDWAN-zones” and “CLI-DATACENTERS” as provisioning templates

Assign this device to its group “WEST-DATACENTERS” so that it gets assigned its SD-WAN template, its PP and its CLI template.



□	WEST-DC-2	Unknown	Never installed	⚠ default ⚠ SDWAN-WEST-DATACENTERS ⚠ CLI-DATACENTERS

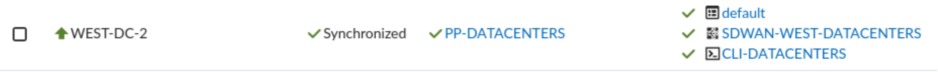
Install Wizard Policy Package “PP-DATACENTERS”



□	WEST-DC-2	Unknown	✓ PP-DATACENTERS	✓ default ✓ SDWAN-WEST-DATACENTERS ✓ CLI-DATACENTERS

On-board the real device (low-touch provisioning)

```
# exec central-mgmt register-device FMG-VM0A13000123 <psk-of-model-device>
```



□	WEST-DC-2	✓ Synchronized	✓ PP-DATACENTERS	✓ default ✓ SDWAN-WEST-DATACENTERS ✓ CLI-DATACENTERS

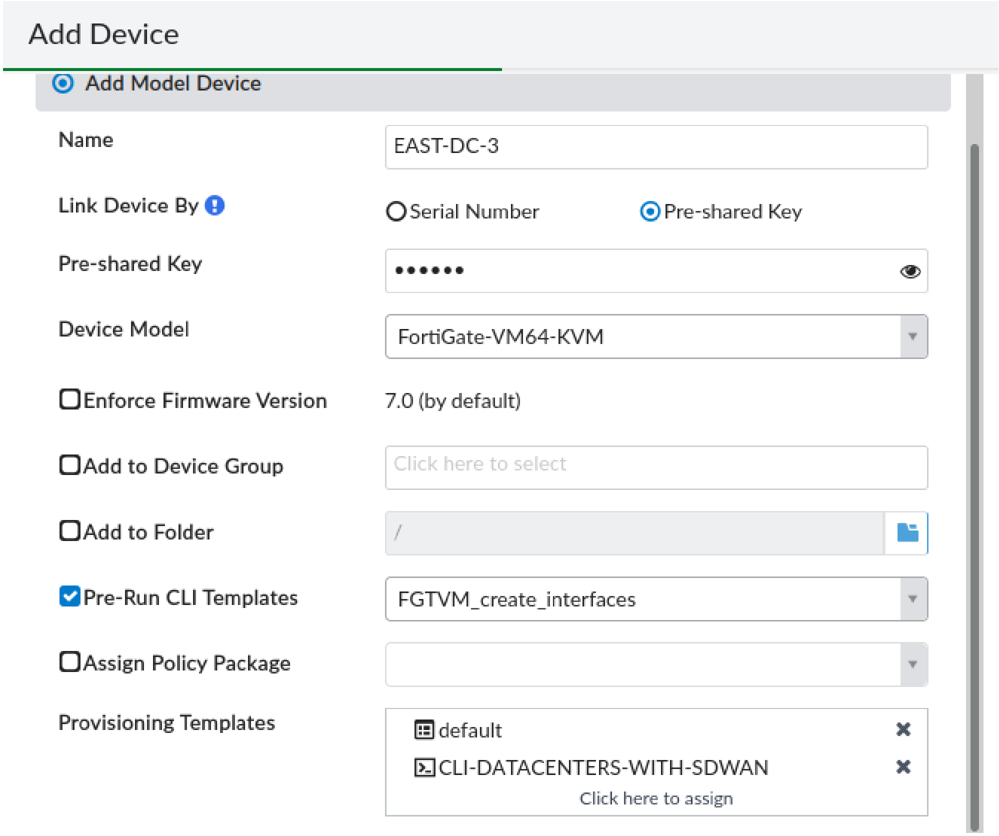
Provisioning EAST-DC-3

EAST-DC-3 has more SD-WAN rules than WEST-DC-{1,2}
As a consequence, this device cannot be provisioned with a simple on-boarding method (like BR2 and BR3 for e.g.).
Since there is no other DC in EAST region, I will not create an SDWAN template for this device, I will rely on the jinja sdwan template.
This is to avoid the complexity of having to define normalized interfaces for all the interfaces listed as “input-device”

EDGE_INET1, EDGE_INET2 and EDGE_MPLS are used as “input-device”
W1E3_INET1, W1E3_INET2 and W1E3_MPLS are used as “input-device”
W2E3_INET1, W2E3_INET2 and W2E3_MPLS are used as “input-device”

Create a model device

EAST-DC-3



Add Device

● Add Model Device

Name	EAST-DC-3
Link Device By	○ Serial Number ● Pre-shared Key
Pre-shared Key	••••••
Device Model	FortiGate-VM64-KVM
□ Enforce Firmware Version	7.0 (by default)
□ Add to Device Group	Click here to select
□ Add to Folder	/
☑ Pre-Run CLI Templates	FGTVM_create_interfaces
□ Assign Policy Package	
Provisioning Templates	default ✖ CLI-DATACENTERS-WITH-SDWAN ✖ Click here to assign

Fill meta-data and location

FMG_FORTIGATE_ID: FGT-E-DC3

dc_id: 3 *Not sure it is actually needed since there is no other DC in this region*

location: Prague

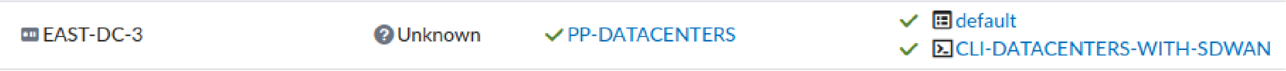
Install config on model device

install device-db settings with “Quick Install (Device DB)”

Assign this device to group “EAST-DATACENTERS”

Remove “CLI-DATACENTERS-WITH-SDWAN” as provisioning template
Assign this device to its group “EAST-DATACENTERS” so that it gets assigned its PP and its CLI template

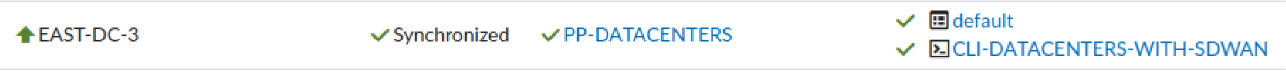
Install Wizard Policy Package “PP-DATACENTERS”



EAST-DC-3	Unknown	✓ PP-DATACENTERS	✓ default ✓ CLI-DATACENTERS-WITH-SDWAN

On-board the real device (low-touch provisioning)

```
# exec central-mgmt register-device FMG-VM0A13000123 <psk-of-model-device>
```

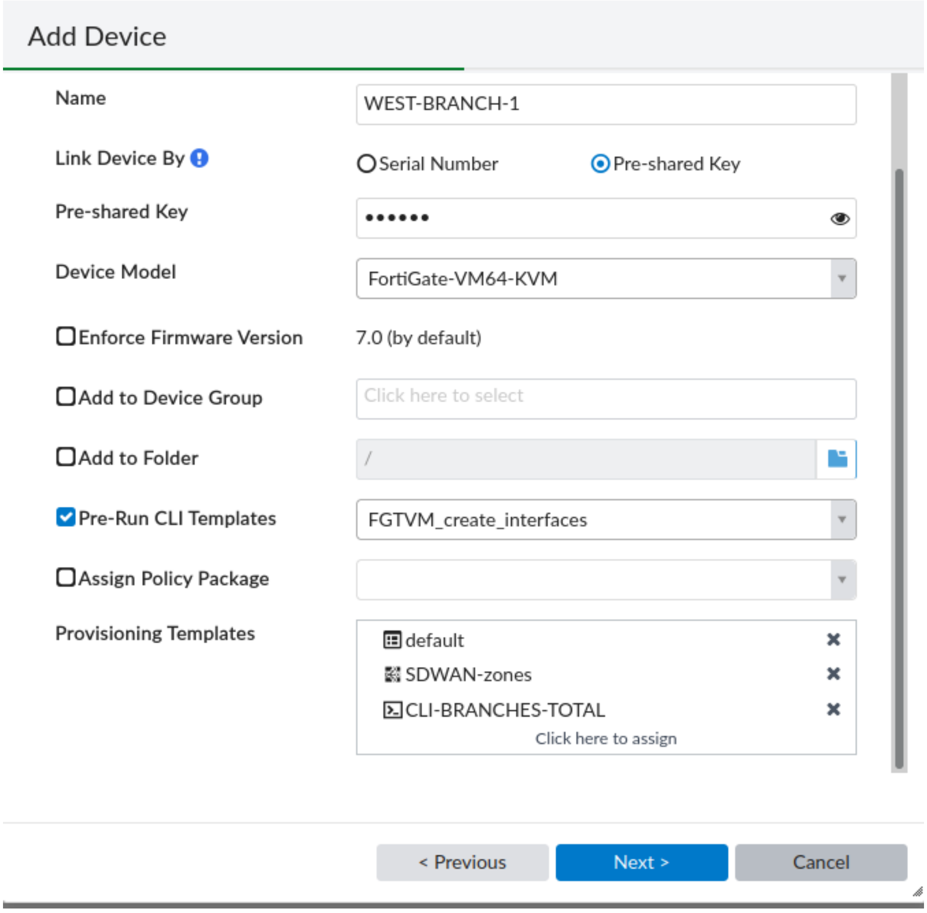


EAST-DC-3	✓ Synchronized	✓ PP-DATACENTERS	✓ default ✓ CLI-DATACENTERS-WITH-SDWAN

Provisioning WEST-BRANCH-1

This device is a reference device which will be used to:
* create an SDWAN template from its SDWAN jinja file
* create a policy package from its fw-addr and fw-policy jinja files

Create a model device



Add Device

Name	WEST-BRANCH-1
Link Device By	○ Serial Number ● Pre-shared Key
Pre-shared Key	••••••
Device Model	FortiGate-VM64-KVM
□ Enforce Firmware Version	7.0 (by default)
□ Add to Device Group	Click here to select
□ Add to Folder	/
☑ Pre-Run CLI Templates	FGTVM_create_interfaces
□ Assign Policy Package	
Provisioning Templates	default SDWAN-zones CLI-BRANCHES-TOTAL Click here to assign

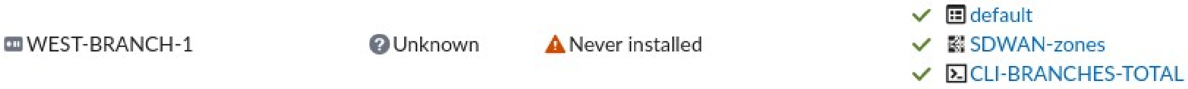
No device group is specified.
No PP is specified since the firewall addresses and policies are pushed by Jinja templates.

Fill meta-data and location

FMG_FORTIGATE_ID: FGT-W-BR1
branch_id: 1 will be used for the SD-WAN template to distinguish west/east branches
wan: 3 will be used for the underlay IP@ of the INET1/INET2 router
location: Bordeaux

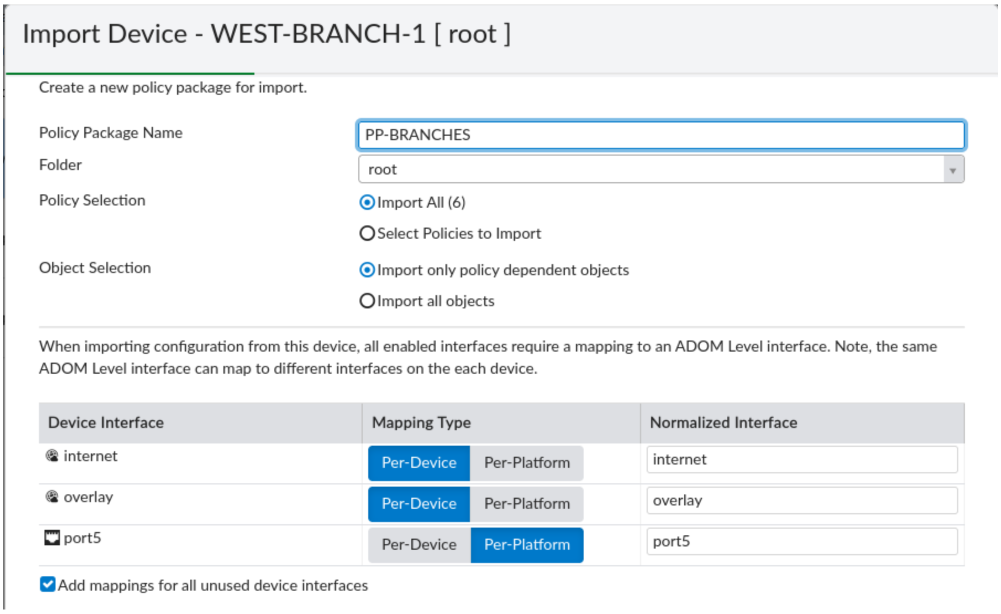
Install config on model device

install device-db settings with "Quick Install (Device DB)"



WEST-BRANCH-1	Unknown	Never installed	✓ default ✓ SDWAN-zones ✓ CLI-BRANCHES-TOTAL

Import policy-package from the device



Import Device - WEST-BRANCH-1 [root]

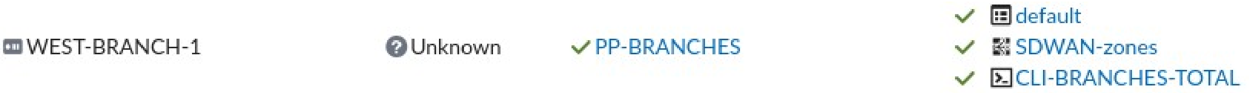
Create a new policy package for import.

Policy Package Name	PP-BRANCHES
Folder	root
Policy Selection	● Import All (6) ○ Select Policies to Import
Object Selection	● Import only policy dependent objects ○ Import all objects

When importing configuration from this device, all enabled interfaces require a mapping to an ADOM Level interface. Note, the same ADOM Level interface can map to different interfaces on the each device.

Device Interface	Mapping Type	Normalized Interface
internet	[✓ Per-Device] Per-Platform	internet
overlay	[✓ Per-Device] Per-Platform	overlay
port5	Per-Device [✓ Per-Platform]	port5

☑ Add mappings for all unused device interfaces

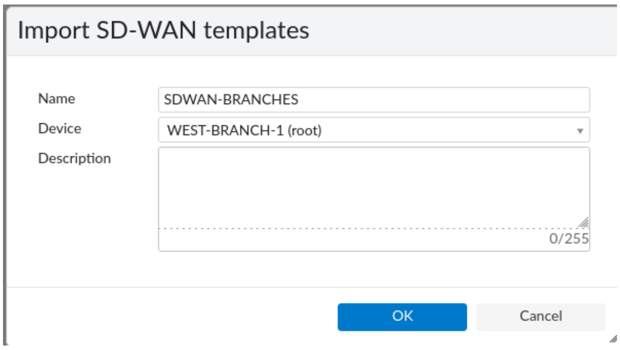


WEST-BRANCH-1	Unknown	✓ PP-BRANCHES	✓ default ✓ SDWAN-zones ✓ CLI-BRANCHES-TOTAL

Go to the PP and change the “Installation Taget”
Remove “WEST-BRANCH-1” and associate groups “WEST-BRANCHES” and “EAST-BRANCHES”

Import SD-WAN template from the device

Name= SDWAN-BRANCHES (used by both West and East regions)



Import SD-WAN templates

Name	SDWAN-BRANCHES
Device	WEST-BRANCH-1 (root)
Description	0/255

Assign this SDWAN template to the WEST-BRANCHES and EAST-BRANCHES device groups
Edit the template to make it valid for both WEST-BR-1/BR-1 and EAST-BR-3
Change:

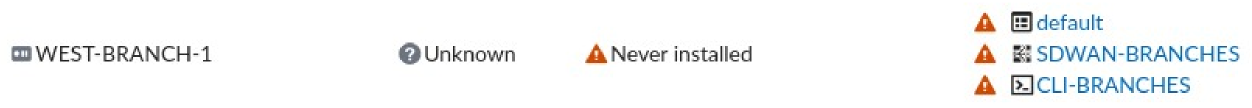
100.64.31.254	to	100.64.$(dc_id)1.254	Internet_1
100.64.32.254	to	100.64.$(dc_id)2.254	Internet_2

Change the provisioning templates assignment for this device

Remove “SDWAN-zones” and “CLI-DATACENTERS-TOTAL”

Assign this device to group “WEST-BRANCHES”

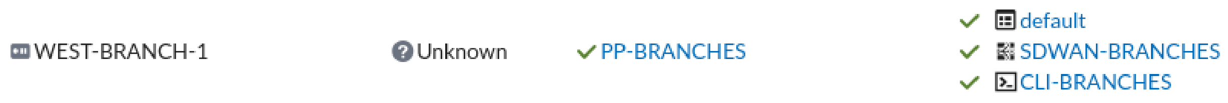
WEST-DC-1 gets assigned the SD-WAN template, the PP and the CLI template from its group:



WEST-BRANCH-1 Unknown ⚠ Never installed

⚠ default
⚠ SDWAN-BRANCHES
⚠ CLI-BRANCHES

Install Wizard Policy Package “PP-BRANCHES”

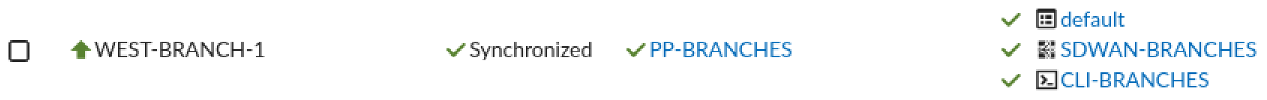


WEST-BRANCH-1 Unknown ✓ PP-BRANCHES

✓ default
✓ SDWAN-BRANCHES
✓ CLI-BRANCHES

On-board the real device (low-touch provisioning)

```
# exec central-mgmt register-device FMG-VM0A13000123 <psk-of-model-device>
```

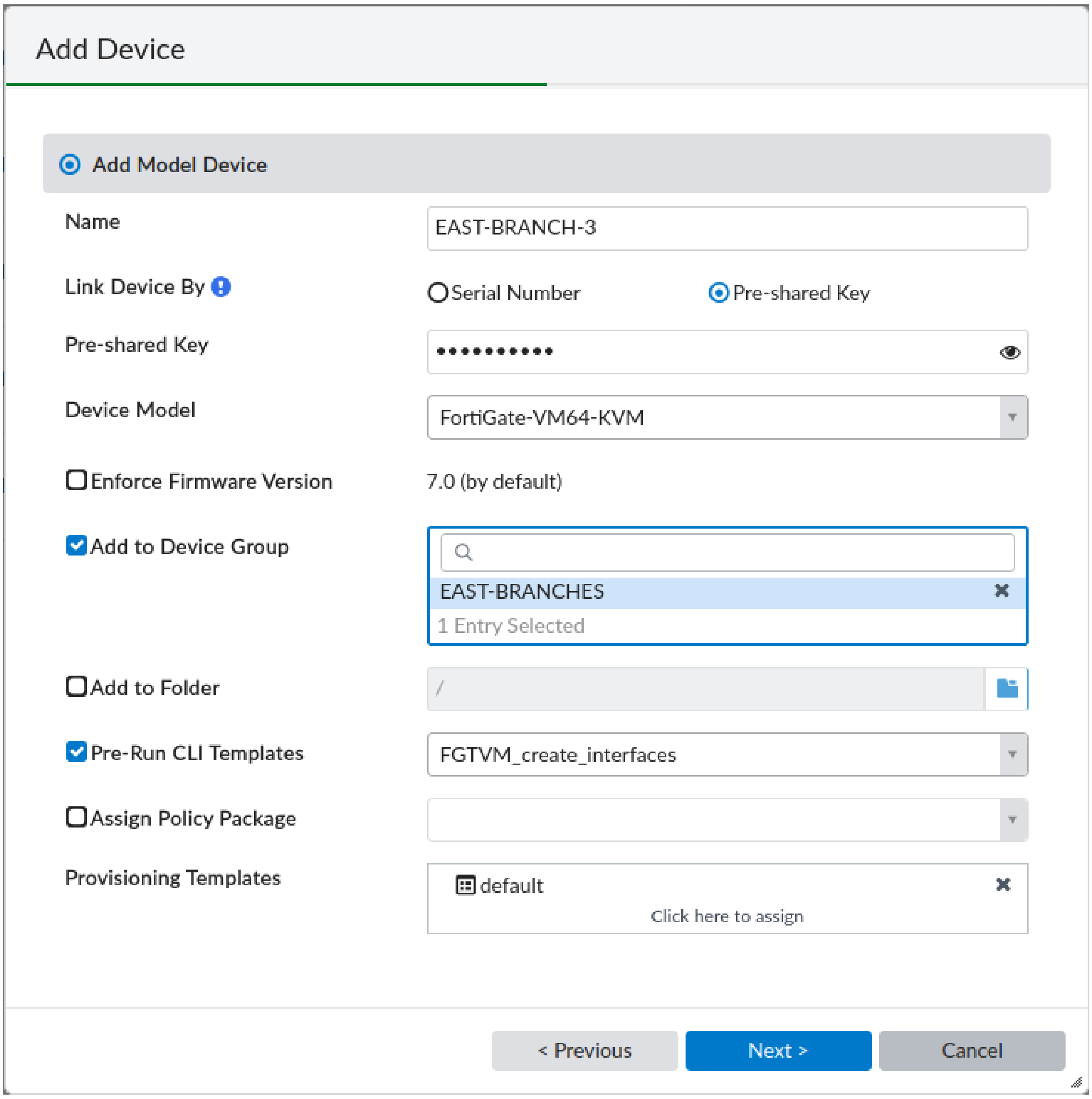


□ WEST-BRANCH-1 ✓ Synchronized ✓ PP-BRANCHES

✓ default
✓ SDWAN-BRANCHES
✓ CLI-BRANCHES

Low-touch Provisioning of WEST-BRANCH-2 and EAST-BRANCH-3

Create a model device

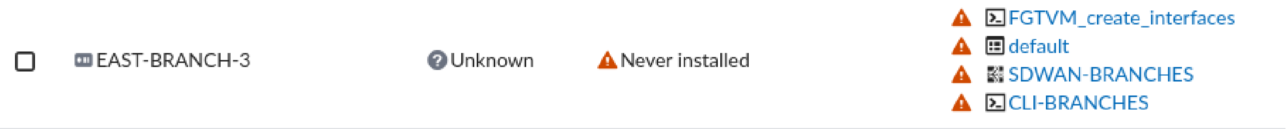


Add Device

● Add Model Device

Name	EAST-BRANCH-3
Link Device By	○ Serial Number ● Pre-shared Key
Pre-shared Key	•••••••••••
Device Model	FortiGate-VM64-KVM
□ Enforce Firmware Version	7.0 (by default)
☑ Add to Device Group	EAST-BRANCHES 1 Entry Selected
□ Add to Folder	/
☑ Pre-Run CLI Templates	FGTVM_create_interfaces
□ Assign Policy Package	
Provisioning Templates	default Click here to assign

The provisioning templates (SDWAN-BRANCHES, CLI-BRANCHES) and the policy package (PP-BRANCHES) are inherited from the device group.
Only add the “system default” template which configured logging to FMG.



□	EAST-BRANCH-3	Unknown	Never installed	FGTVM_create_interfaces default SDWAN-BRANCHES CLI-BRANCHES

Fill meta-data and location

Edit the device:

* Fill the meta-data:

- WEST-BRANCH-2: FMG_FORTIGATE_ID: FGT-W-BR2

wan: 4
- EAST-BRANCH-3: FMG_FORTIGATE_ID: FGT-E-BR3
wan: 4

The ‘wan’ meta-field digit is used for the ‘gateway’ IP of the INET1/INET2 sd-wan members

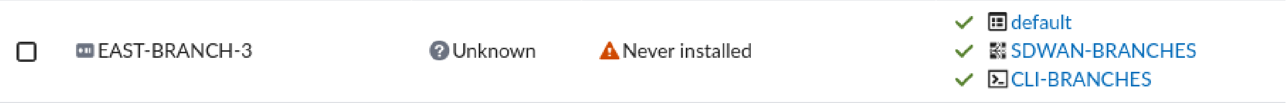
* Enter a location: e.g., W-BR2= Sophia-Antipolis ; E-BR3 = Budapest

Install config on model device

I tried to install full config (device-db settings + PP) at once but it failed.

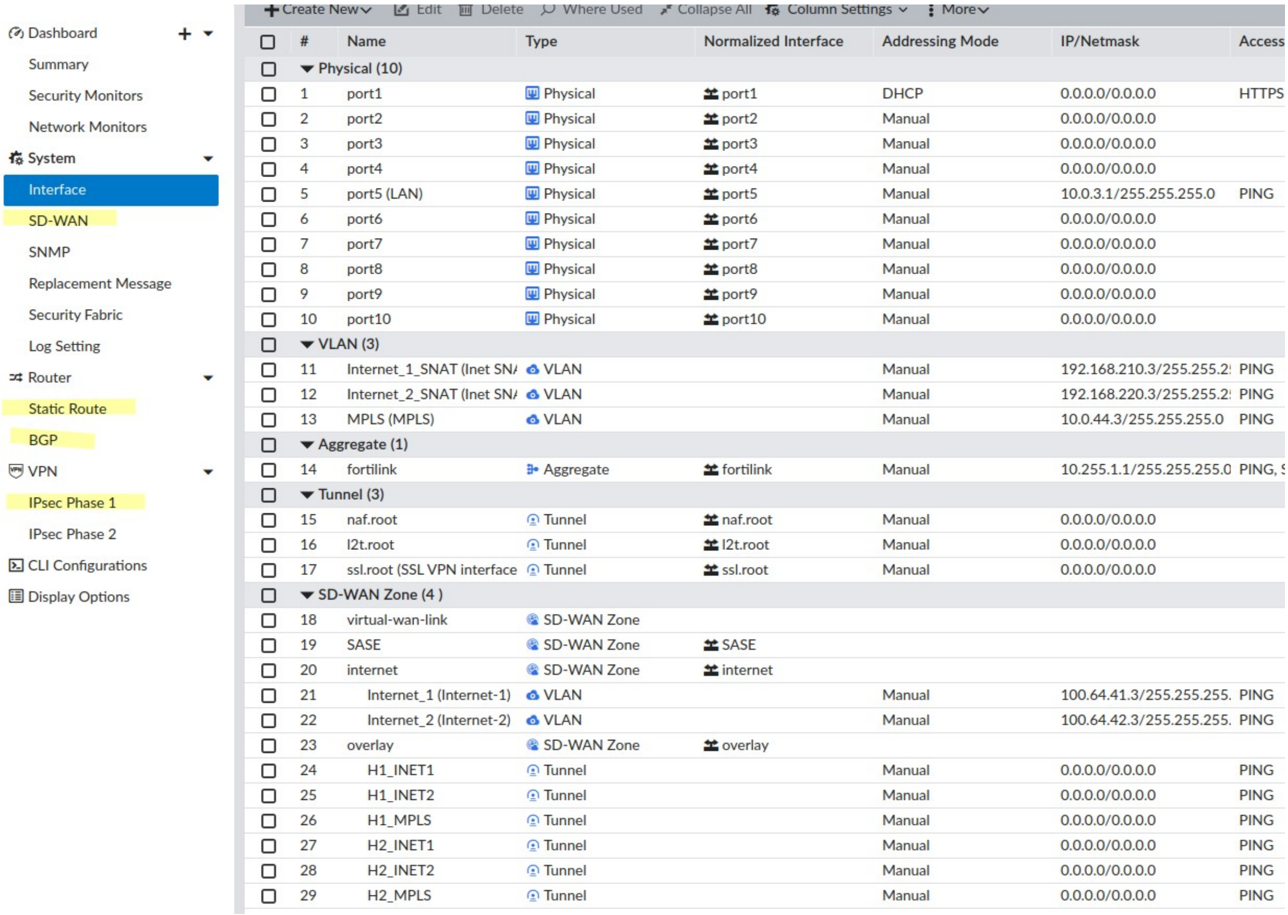
It works in a two steps process:
- 1st step: install device-db settings with “Quick Install (Device DB)”
- 2nd step: install PP

1st step: Install the settings with “Quick Install (Device DB)”



□	EAST-BRANCH-3	Unknown	⚠ Never installed	✓ default ✓ SDWAN-BRANCHES ✓ CLI-BRANCHES

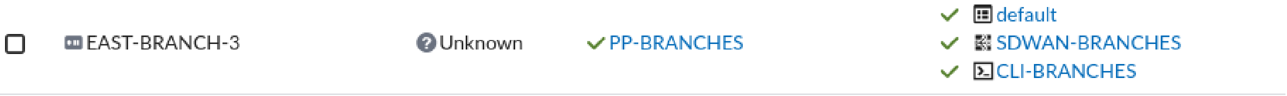
Check the device config: Underlay, Overlay, SD-WAN, Routing config is in the device DB.



□	#	Name	Type	Normalized Interface	Addressing Mode	IP/Netmask	Access
□	▼ Physical (10)						
□	1	port1	Physical	port1	DHCP	0.0.0.0/0.0.0.0	HTTPS
□	2	port2	Physical	port2	Manual	0.0.0.0/0.0.0.0	
□	3	port3	Physical	port3	Manual	0.0.0.0/0.0.0.0	
□	4	port4	Physical	port4	Manual	0.0.0.0/0.0.0.0	
□	5	port5 (LAN)	Physical	port5	Manual	10.0.3.1/255.255.255.0	PING
□	6	port6	Physical	port6	Manual	0.0.0.0/0.0.0.0	
□	7	port7	Physical	port7	Manual	0.0.0.0/0.0.0.0	
□	8	port8	Physical	port8	Manual	0.0.0.0/0.0.0.0	
□	9	port9	Physical	port9	Manual	0.0.0.0/0.0.0.0	
□	10	port10	Physical	port10	Manual	0.0.0.0/0.0.0.0	
□	▼ VLAN (3)						
□	11	Internet_1_SNAT (Inet SN/	VLAN		Manual	192.168.210.3/255.255.2!	PING
□	12	Internet_2_SNAT (Inet SN/	VLAN		Manual	192.168.220.3/255.255.2!	PING
□	13	MPLS (MPLS)	VLAN		Manual	10.0.44.3/255.255.255.0	PING
□	▼ Aggregate (1)						
□	14	fortilink	Aggregate	fortilink	Manual	10.255.1.1/255.255.255.0	PING, S
□	▼ Tunnel (3)						
□	15	naf.root	Tunnel	naf.root	Manual	0.0.0.0/0.0.0.0	
□	16	l2t.root	Tunnel	l2t.root	Manual	0.0.0.0/0.0.0.0	
□	17	ssl.root (SSL VPN interface	Tunnel	ssl.root	Manual	0.0.0.0/0.0.0.0	
□	▼ SD-WAN Zone (4)						
□	18	virtual-wan-link	SD-WAN Zone				
□	19	SASE	SD-WAN Zone	SASE			
□	20	internet	SD-WAN Zone	internet			
□	21	Internet_1 (Internet-1)	VLAN		Manual	100.64.41.3/255.255.255.	PING
□	22	Internet_2 (Internet-2)	VLAN		Manual	100.64.42.3/255.255.255.	PING
□	23	overlay	SD-WAN Zone	overlay			
□	24	H1_INET1	Tunnel		Manual	0.0.0.0/0.0.0.0	PING
□	25	H1_INET2	Tunnel		Manual	0.0.0.0/0.0.0.0	PING
□	26	H1_MPLS	Tunnel		Manual	0.0.0.0/0.0.0.0	PING
□	27	H2_INET1	Tunnel		Manual	0.0.0.0/0.0.0.0	PING
□	28	H2_INET2	Tunnel		Manual	0.0.0.0/0.0.0.0	PING
□	29	H2_MPLS	Tunnel		Manual	0.0.0.0/0.0.0.0	PING

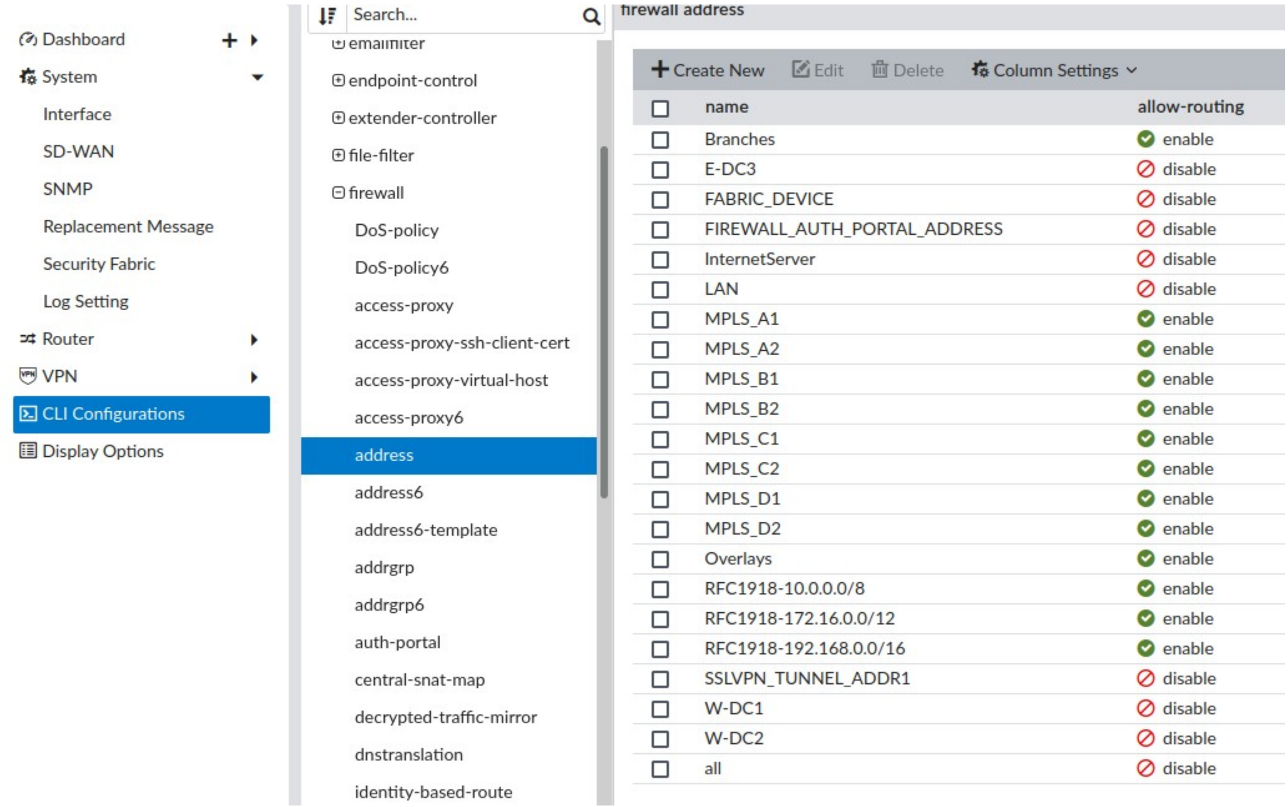
2nd step:

* In “policy & Objects”, **create a dynamic mapping for “LAN”** address: BR2= 10.0.2.0/24, BR3=10.0.3.0/24
* “Install Wizard” → “**Install Policy Package** & Device Settings” → choose “PP-BRANCHES”

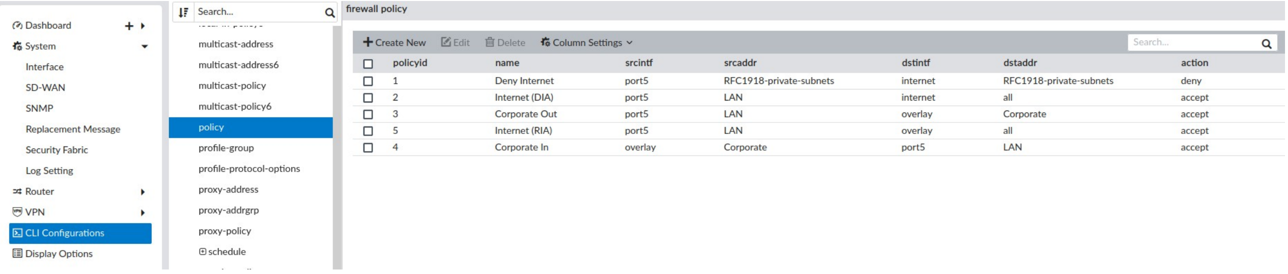


□	EAST-BRANCH-3	Unknown	✓ PP-BRANCHES	✓ default ✓ SDWAN-BRANCHES ✓ CLI-BRANCHES

Check that the policy were installed on model device:



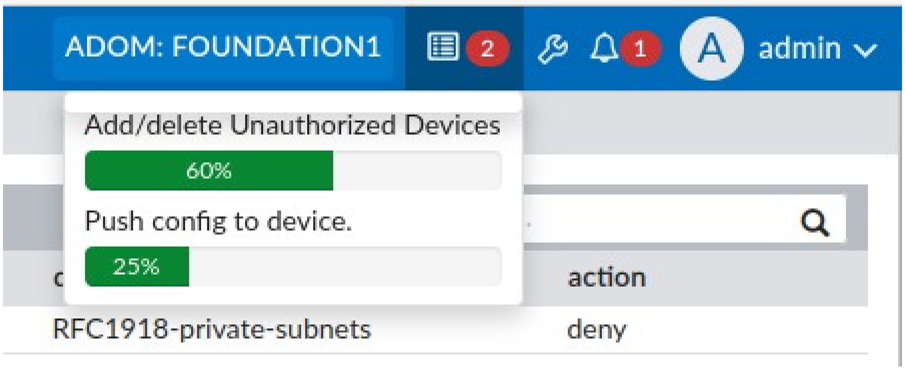
□	name	allow-routing
□	Branches	✓ enable
□	E-DC3	⊘ disable
□	FABRIC_DEVICE	⊘ disable
□	FIREWALL_AUTH_PORTAL_ADDRESS	⊘ disable
□	InternetServer	⊘ disable
□	LAN	⊘ disable
□	MPLS_A1	✓ enable
□	MPLS_A2	✓ enable
□	MPLS_B1	✓ enable
□	MPLS_B2	✓ enable
□	MPLS_C1	✓ enable
□	MPLS_C2	✓ enable
□	MPLS_D1	✓ enable
□	MPLS_D2	✓ enable
□	Overlays	✓ enable
□	RFC1918-10.0.0.0/8	✓ enable
□	RFC1918-172.16.0.0/12	✓ enable
□	RFC1918-192.168.0.0/16	✓ enable
□	SSLVPN_TUNNEL_ADDR1	⊘ disable
□	W-DC1	⊘ disable
□	W-DC2	⊘ disable
□	all	⊘ disable



□	policyid	name	srcintf	srcaddr	dstintf	dstaddr	action
□	1	Deny Internet	port5	RFC1918-private-subnets	internet	RFC1918-private-subnets	deny
□	2	Internet (DIA)	port5	LAN	internet	all	accept
□	3	Corporate Out	port5	LAN	overlay	Corporate	accept
□	5	Internet (RIA)	port5	LAN	overlay	all	accept
□	4	Corporate In	overlay	Corporate	port5	LAN	accept

On-board the real device (low-touch provisioning)

# exec central-mgmt register-device FMG-VM0A13000123 <psk-of-model-device>

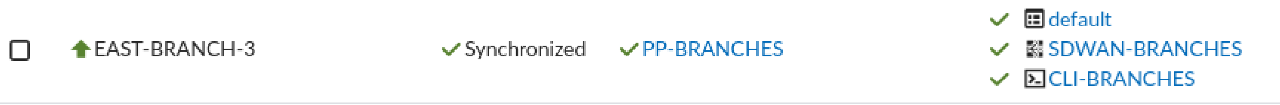


Add/delete Unauthorized Devices

60%

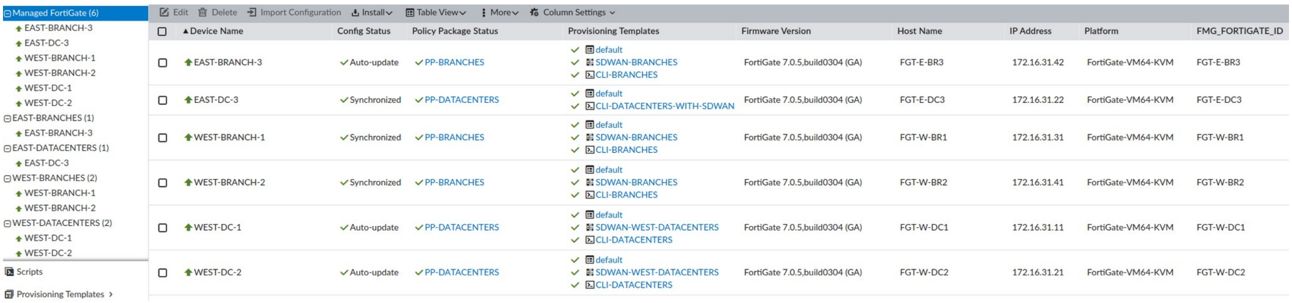
Push config to device.

25%



☐	EAST-BRANCH-3	✓ Synchronized	✓ PP-BRANCHES	✓ default ✓ SDWAN-BRANCHES ✓ CLI-BRANCHES

Final status



☐	▲Device Name	Config Status	Policy Package Status	Provisioning Templates	Firmware Version	Host Name	IP Address	Platform	FMG_FORTIGATE_ID
☐	EAST-BRANCH-3	✓ Auto-update	✓ PP-BRANCHES	✓ default ✓ SDWAN-BRANCHES ✓ CLI-BRANCHES	FortiGate 7.0.5,build0304 (GA)	FGT-E-BR3	172.16.31.42	FortiGate-VM64-KVM	FGT-E-BR3
☐	EAST-DC-3	✓ Synchronized	✓ PP-DATACENTERS	✓ default ✓ CLI-DATACENTERS-WITH-SDWAN	FortiGate 7.0.5,build0304 (GA)	FGT-E-DC3	172.16.31.22	FortiGate-VM64-KVM	FGT-E-DC3
☐	WEST-BRANCH-1	✓ Synchronized	✓ PP-BRANCHES	✓ default ✓ SDWAN-BRANCHES ✓ CLI-BRANCHES	FortiGate 7.0.5,build0304 (GA)	FGT-W-BR1	172.16.31.31	FortiGate-VM64-KVM	FGT-W-BR1
☐	WEST-BRANCH-2	✓ Synchronized	✓ PP-BRANCHES	✓ default ✓ SDWAN-BRANCHES ✓ CLI-BRANCHES	FortiGate 7.0.5,build0304 (GA)	FGT-W-BR2	172.16.31.41	FortiGate-VM64-KVM	FGT-W-BR2
☐	WEST-DC-1	✓ Auto-update	✓ PP-DATACENTERS	✓ default ✓ SDWAN-WEST-DATACENTERS ✓ CLI-DATACENTERS	FortiGate 7.0.5,build0304 (GA)	FGT-W-DC1	172.16.31.11	FortiGate-VM64-KVM	FGT-W-DC1
☐	WEST-DC-2	✓ Auto-update	✓ PP-DATACENTERS	✓ default ✓ SDWAN-WEST-DATACENTERS ✓ CLI-DATACENTERS	FortiGate 7.0.5,build0304 (GA)	FGT-W-DC2	172.16.31.21	FortiGate-VM64-KVM	FGT-W-DC2