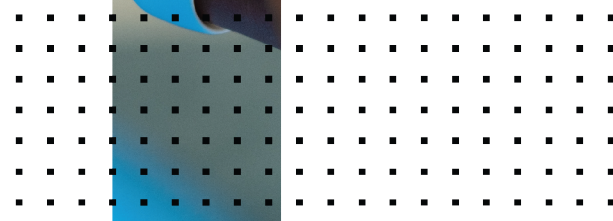


SD-WAN Configuration Migration

FortiManager 7.0.3



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



May 12, 2023

FortiManager 7.0.3 SD-WAN Configuration Migration

02-703-736464-20230512

TABLE OF CONTENTS

Change Log	4
Introduction	5
Procedure	7
Reviewing the SD-WAN configuration in FortiManager 6.4	7
Upgrading FortiManager firmware from 6.4 to 7.0	11
Creating meta fields to set gateway IP addresses	11
Adding meta fields to SD-WAN templates	15
Upgrading FortiOS from 6.4 to 7.0	20
Upgrading ADOM version 6.4 to 7.0	20
Installing policy changes with a workaround	20

Change Log

Date	Change Description
2022-06-09	Initial release.
2023-05-12	Updated Procedure on page 7 and Upgrading FortiOS from 6.4 to 7.0 on page 20 .

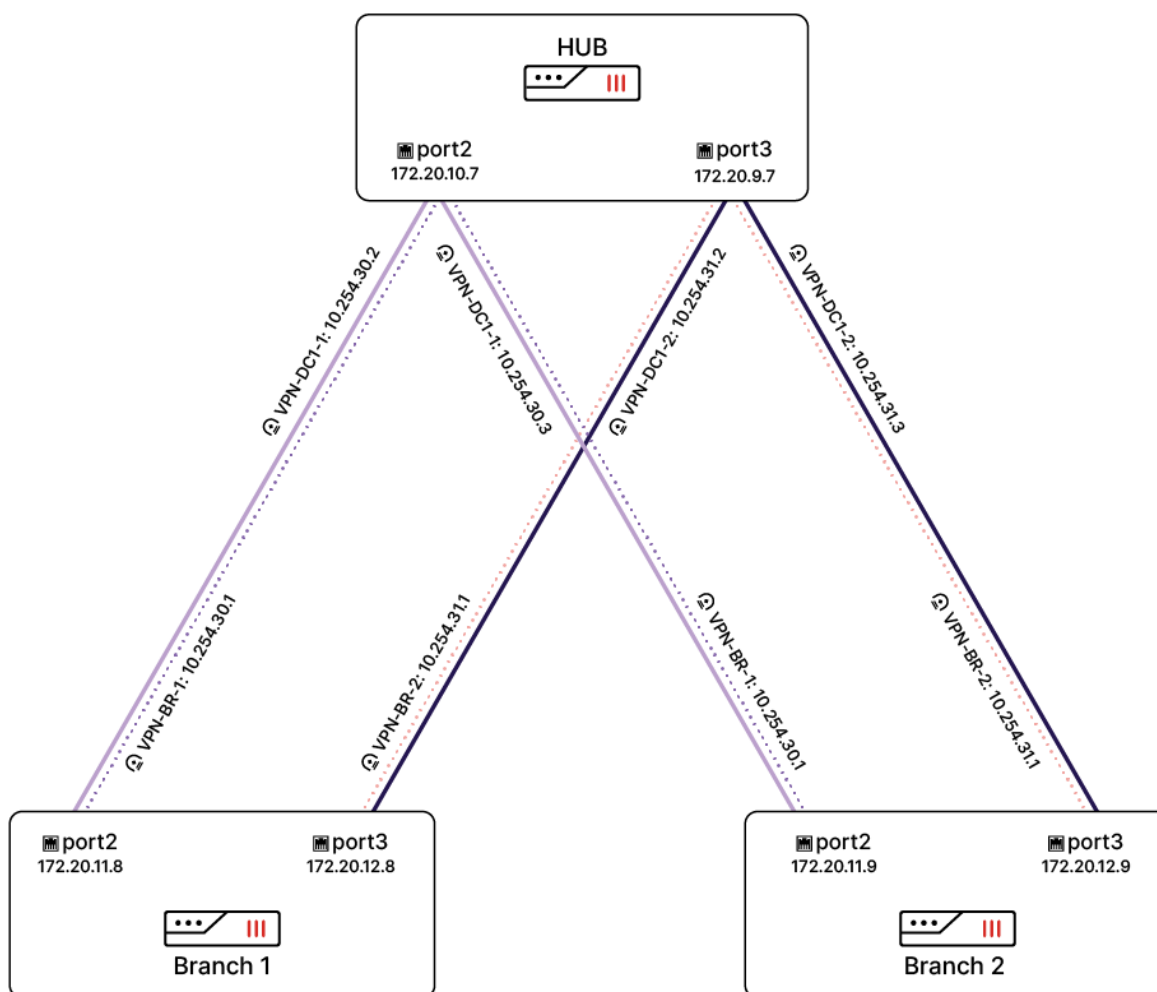
Introduction

This document describes how to navigate SD-WAN configuration changes during upgrade of FortiManager from 6.4 to 7.0. After upgrading FortiManager from 6.4 to 7.0, you must modify the centrally managed SD-WAN configuration before installing the configuration to FortiGates due to the following design improvements available with SD-WAN 7.0:

- *Normalized interfaces* used in the FortiManager 6.4 SD-WAN template have been replaced by *named interfaces* in the FortiManager 7.0 SD-WAN template.
- Named interfaces in FortiManager 7.0 support meta fields.
- Upgrade from FortiManager 6.4 to 7.0 clears the SD-WAN member interfaces from the SD-WAN template.

This guide describes how to upgrade FortiManager with an SD-WAN configuration from version 6.4.7 to version 7.0.3. In this example, the SD-WAN configuration is for the following managed FortiGates:

- One FortiGate device acting as a hub
- Two FortiGate devices acting as branches



As a design consideration, this document assumes an existing setup and initial state before upgrading FortiManager. After completing the upgrade of FortiManager to 7.0 and the process described in this document, the SD-WAN configuration is migrated and updated to the final state. Following is a summary of the initial and final states:

Before	After
<ul style="list-style-type: none">FortiManager version 6.4.7 / ADOM 6.4 and FortiOS 6.4.7/6.4.8SD-WAN central management mode is enabledSD-WAN configuration installed to FortiGates	<ul style="list-style-type: none">FortiManager version 7.0.3 / ADOM 7.0 and FortiOS 6.4.7/6.4.8 or 7.0.SD-WAN central management mode is enabledSD-WAN configuration installed to FortiGates

Following is a summary of SD-WAN changes between FortiManager 6.4 and 7.0:

Configuration	6.4	7.0
Gateway IP	Per-device mapping	Meta fields
Interfaces	Normalized Interface	Named Interface with meta field

Procedure

Following is an overview of the upgrade procedure:

1. Review before upgrade: [Reviewing the SD-WAN configuration in FortiManager 6.4 on page 7](#).
2. Upgrade FortiManager to 7.0: [Upgrading FortiManager firmware from 6.4 to 7.0 on page 11](#).
3. Create meta fields to use with interface members: [Creating meta fields to set gateway IP addresses on page 11](#).
4. Edit SD-WAN templates to use meta fields: [Adding meta fields to SD-WAN templates on page 15](#).
5. (Optional) Upgrade managed FortiGates: [Upgrading FortiOS from 6.4 to 7.0 on page 20](#).
Upgrade of FortiOS from 6.4 to 7.0 is recommended, but not required.
6. Upgrade the ADOM: [Upgrading ADOM version 6.4 to 7.0 on page 20](#).
7. Install policy changes: [Installing policy changes with a workaround on page 20](#).

Reviewing the SD-WAN configuration in FortiManager 6.4

This section describes what SD-WAN settings to review in FortiManager 6.4 before upgrading to FortiManager 7.0.

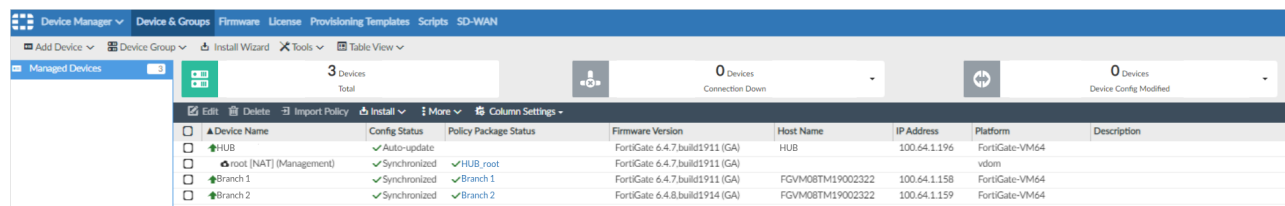
The interface members use per-device mapping.

To review SD-WAN settings in FortiManager 6.4:

1. Go to *Device Manager > Device & Groups*, and ensure all devices used for SD-WAN have been added to FortiManager and authorized, and the configuration is synchronized.

In the following example, all devices are visible:

- HUB
- Branch 1
- Branch 2



The screenshot shows the FortiManager 6.4 interface with the 'Managed Devices' tab selected. A table lists the following devices:

Device Name	Config Status	Policy Package Status	Firmware Version	Host Name	IP Address	Platform	Description
HUB	✓ Auto-update		FortiGate 6.4.7, build1911 (GA)	HUB	100.64.1.196	FortiGate-VM64	
root [NAT] (Management)	✓ Synchronized	✓ HUB_root	FortiGate 6.4.7, build1911 (GA)			vdcm	
Branch 1	✓ Synchronized	✓ Branch 1	FortiGate 6.4.7, build1911 (GA)	FGVM08TM19002322	100.64.1.158	FortiGate-VM64	
Branch 2	✓ Synchronized	✓ Branch 2	FortiGate 6.4.8, build1914 (GA)	FGVM08TM19002322	100.64.1.159	FortiGate-VM64	

2. In *Device Manager*, go to *SD-WAN > Interface Members*.

In this example, the following interfaces are displayed, and they are configured with per-device mappings:

- port2
- port3
- vpn_dc1-1
- vpn_dc1-2

Device Manager

Device & Groups
 Firmware
 License
 Provisioning Templates
 Scripts
 SD-WAN

Install Wizard

SD-WAN Templates

Create New
 Edit
 Delete
 Where Used
 Column Settings

Interface Members

Health-Check Servers

BGP Neighbors

Monitor

<input type="checkbox"/>	Interface Name	Per Device Mapping
<input type="checkbox"/>	port2	> 2 out of 3
<input type="checkbox"/>	port3	> 2 out of 3
<input type="checkbox"/>	vpn_dc1-1	> 2 out of 3
<input type="checkbox"/>	vpn_dc1-2	> 2 out of 3

3. Double-click each interface to display its details, and then click *Cancel* to close the pane. Notice that *Per-Device Mapping* is enabled for each interface.
For example, double-click the interface named *port2* to display its settings.

Device Manager ▾ | Device & Groups | Firmware | License | Provisioning Templates | Scripts | SD-WAN

Install Wizard

- SD-WAN Templates
- Interface Members**
- Health-Check Servers
- BGP Neighbors
- Monitor

Edit WAN Interface port2

Name	<input type="text" value="port2"/>
Description	<div style="border: 1px solid #ccc; height: 100px;"></div>
Normalized Interface	<input checked="" type="checkbox"/> port2 ▾
Gateway	<input type="text" value="0.0.0.0"/>
Weight	<input type="text" value="1"/>
Cost	<input type="text" value="0"/>
Volume Ratio	<input type="text" value="1"/>
Per-Device Mapping	<input checked="" type="checkbox"/> ON

+ Create New	Edit	Delete		Name	VDOM	Gateway	Weight	Cost	Volume Ratio
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Branch 1	root	172.20.11.8	80	1	1
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Branch 2	root	172.20.11.9	80	1	1

Advanced Options >

Following are the settings for the interface named *port3*.

Device Manager ▾ Device & Groups Firmware License Provisioning Templates Scripts **SD-WAN**

[Install Wizard](#)

SD-WAN Templates

- Interface Members**
- Health-Check Servers
- BGP Neighbors
- Monitor

Edit WAN Interface port3

Name:

Description:

Normalized Interface: ☒ port3

Gateway:

Weight:

Cost:

Volume Ratio:

Per-Device Mapping: ☒ ON

[+ Create New](#) [Edit](#) [Delete](#)

<input type="checkbox"/>	Name	VDOM	Gateway	Weight	Cost	Volume Ratio
<input type="checkbox"/>	Branch 1	root	172.20.12.8	20	1	1
<input type="checkbox"/>	Branch 2	root	172.20.12.9	20	1	1

[Advanced Options >](#)

Following are the settings for interface *vpn_dc1-1*.

Device Manager ▾ Device & Groups Firmware License Provisioning Templates Scripts **SD-WAN**

[Install Wizard](#)

SD-WAN Templates

- Interface Members**
- Health-Check Servers
- BGP Neighbors
- Monitor

Edit WAN Interface vpn_dc1-1

Name:

Description:

Normalized Interface: ☒ vpn_dc1-1

Gateway:

Weight:

Cost:

Volume Ratio:

Per-Device Mapping: ☒ ON

[+ Create New](#) [Edit](#) [Delete](#)

<input type="checkbox"/>	Name	VDOM	Gateway	Weight	Cost	Volume Ratio
<input type="checkbox"/>	Branch 1	root	10.254.30.2	1	1	1
<input type="checkbox"/>	Branch 2	root	10.254.30.3	1	1	1

[Advanced Options >](#)

Following are the settings for interface *vpn_dc1-2*.

The screenshot shows the 'Edit WAN Interface vpn_dc1-2' configuration page in FortiManager. The left sidebar contains a navigation menu with 'Interface Members' selected. The main area displays the following configuration fields:

- Name: vpn_dc1-2
- Description: (empty text area)
- Normalized Interface: vpn_dc1-2 (dropdown menu)
- Gateway: 0.0.0.0
- Weight: 1
- Cost: 0
- Volume Ratio: 1
- Per-Device Mapping: ON (toggle)

Below the fields is a table with columns: Name, VDOM, Gateway, Weight, Cost, and Volume Ratio. It lists two entries: 'Branch 1' and 'Branch 2', both with VDOM 'root' and Gateway '10.254.31.2' and '10.254.31.3' respectively.

- Click *Health-Check Servers* to ensure health-check servers are configured for SD-WAN. The following example uses several health-check servers.

The screenshot shows the 'Health-Check Servers' configuration page in FortiManager. The left sidebar has 'Health-Check Servers' selected. The main area displays a table with columns: Server Name, Detect Server, and Per Device Mapping.

Server Name	Detect Server	Per Device Mapping
http	10.200.1.10	> 0 out of 3
test_dc	10.200.1.1	> 0 out of 3
test_internet	10.201.1.1	> 0 out of 3

- Click *SD-WAN Templates* to review the SD-WAN template. The following example uses an SD-WAN template named *sdwan-branch*.

The screenshot shows the 'SD-WAN Templates' configuration page in FortiManager. The left sidebar has 'SD-WAN Templates' selected. The main area displays a table with columns: Name, Assigned to Devices, and Interfaces.

Name	Assigned to Devices	Interfaces
sdwan-branch	Branch 2 [root] Branch 1 [root]	port2 port3 vpn_dc1-1 vpn_dc1-2

6. Double-click the SD-WAN template to open it and review its settings.

The screenshot shows the FortiManager SD-WAN configuration window. The left sidebar contains navigation options: SD-WAN Templates, Interface Members, Health-Check Servers, BGP Neighbors, and Monitor. The main area is titled 'Edit sdwan-branch' and contains several sections:

- Interface Members:** A table with columns ID, Name, and Interface Member. It lists members like virtual-wan-link, 1, 2, vpn, 3, and 4, each mapped to a specific interface (port2, port3, vpn_dc1-1, vpn_dc1-2).
- Performance SLA:** A table with columns Name, Health-Check Server, Detect Protocol, Failure Threshold, and Recovery Threshold. It lists various default and custom SLAs like Default_AWS, Default_FortiGuard, Default_Gmail, Default_Google Search, Default_Office_365, http, test_dc, and test_internet.
- Neighbor:** A table with columns Neighbor, Interface Member, Performance SLA, and SLA. It currently shows 'No record found.'
- SD-WAN Rules:** A table with columns ID, Name, Source, Destination, Criteria, and Members. It lists rules like 1 (Critical-Business-Apps), 2 (Non-Business-Apps), and sd-wan.
- Advanced Options:** A link to expand more settings.

At the bottom, there are 'OK' and 'Cancel' buttons.

Upgrading FortiManager firmware from 6.4 to 7.0

After reviewing the SD-WAN settings in FortiManager 6.4, you are ready to upgrade FortiManager firmware from version 6.4.7 to version 7.0.3. For details, see the [FortiManager 7.0.3 Upgrade Guide](#).

After the FortiManager firmware upgrade completes, leave the managed FortiGates running FortiOS 6.4 in ADOM version 6.4. You will upgrade the FortiOS and ADOM versions later.

Creating meta fields to set gateway IP addresses

In FortiManager 6.4, SD-WAN interface members use per-device mappings to set the gateway IP address, weight, cost, and so on for each device.

After upgrading FortiManager to version 7.0, create meta fields to use with the SD-WAN template to define the gateway IP address for each device. By using meta fields, you can apply the template to many devices and use the meta fields to define unique IP addresses for devices.

This section describes how to create meta fields for the *Device VDOM* object, and set the importance of the meta field to *Optional*.

To create meta fields:

1. Go to *System Settings > Meta Fields*, and click *Create New*.
The *Create New Meta Fields* pane is displayed.
2. Set the following options to create a meta field named *gateway*, and click *OK*:
 - a. In the *Object List*, select *Device VDOM*.
 - b. In the *Name* box, type *gateway*.
 - c. Beside *Importance*, select *Optional*.



Be sure to set *Importance* to *Optional* to help prepare for upgrade to FortiManager 7.0 later.

- d. Leave the remaining defaults, and click *OK*.

Edit Meta Fields

Object

Device VDOM

Name

gateway

Length

20

Importance

☒ Optional ☐ Required

Status

☐ Disabled ☒ Enabled

Variable

\$(gateway)

Values

Create New

Edit

Delete


Column Settings

<input type="checkbox"/>	Device
<input type="checkbox"/>	Branch 1 [root]
<input type="checkbox"/>	Branch 2 [root]






The meta field is created.

3. Click *Create New*, and create another meta field named *vpn-dc* with the following settings:

Edit Meta Fields

Object	Device VDOM
Name	vpn_dc
Length	20
Importance	<input checked="" type="radio"/> Optional <input type="radio"/> Required
Status	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Variable	\$(vpn_dc) 

Values

 Create New  Edit  Delete  Column Settings 

<input type="checkbox"/>	▲ Device
<input type="checkbox"/>	▲ Branch 1 [root]
<input type="checkbox"/>	▲ Branch 2 [root]

The meta field are created.

System Settings

Dashboard

All ADOMs

Network

HA

Admin >

Certificates >

Event Log

Task Monitor

Advanced

SNMP

Mail Server

Syslog Server

Meta Fields

Advanced Settings

Create New

Edit

Delete

Collapse All

Expand All

Column Settings

<input type="checkbox"/>	Meta Fields	Length	Importance
Administrative Domain (0)			
Central NAT (0)			
Device (4)			
<input type="checkbox"/>	Address	150	Optional
<input type="checkbox"/>	Company/Organization	50	Optional
<input type="checkbox"/>	Contact Email	50	Optional
<input type="checkbox"/>	Contact Phone Number	50	Optional
Device Group (0)			
Device VDOM (2)			
<input type="checkbox"/>	gateway	20	Optional
<input type="checkbox"/>	vpn_dc	20	Optional
Firewall Address (0)			
Firewall Address Group (0)			
Firewall Policy (0)			
Firewall Service (0)			
Firewall Service Group (0)			
System Administrator (2)			
<input type="checkbox"/>	Contact Email	50	Optional
<input type="checkbox"/>	Contact Phone	50	Optional

Adding meta fields to SD-WAN templates

After you create meta fields, add the meta fields to the SD-WAN template for interfaces to use.

To add meta fields to SD-WAN templates:

1. Go to *Device Manager > Provisioning Templates > SD-WAN Templates*.

The SD-WAN template named *sdwan-branch* is displayed.

Device Manager

Device & Groups

Scripts

Provisioning Templates

Template Group

System Templates

IPsec Tunnel Templates

SD-WAN Templates

Static Route Templates

Install Wizard

Create New

Edit

Delete

Import

Assign to Devices/Groups

Column Settings

Name	Assigned to Devices	Interfaces
sdwan-branch	2 Devices in Total View Details >	<div>port2</div> <div>port3</div> <div>vpn_dc1-1</div> <div>vpn_dc1-2</div>
	<div>Branch 1 [root]</div> <div>Branch 2 [root]</div>	

2. Double-click the SD-WAN template to open it for editing.
In the *Interface Members* section, the interfaces are displayed.

Device Manager ▾ Install Wizard

Device & Groups ▸

Scripts

Provisioning Templates ▾

- Template Group
- System Templates
- IPsec Tunnel Templates
- SD-WAN Templates
- Static Route Templates
- BGP Templates
- Certificate Templates
- Threat Weight
- CLI Templates
- NSX-T Service Template

Firmware Templates

Edit SD-WAN Template CLI Configurations

Name: sdwan-branch

Description:

SD-WAN Status: ☒

Interface Members

ID	Interface Member	Status	Weight	Gateway
<input type="checkbox"/>	virtual-w			
<input checked="" type="checkbox"/>	1 port2	Enable	80	172.20.11.\$(gateway)
<input checked="" type="checkbox"/>	2 port3	Enable	20	172.20.12.\$(gateway)
<input type="checkbox"/>	vpn			
<input type="checkbox"/>	3 vpn_dc1-1	Enable	1	10.254.30.\$(vpn_dc)
<input type="checkbox"/>	4 vpn_dc1-2	Enable	1	10.254.31.\$(vpn_dc)

3. Add the $$(gateway)$ meta field to interfaces:

- Double-click the *port2* interface to open it for editing.
The *Edit SD-WAN Interface Member* dialog box is displayed.

Edit SD-WAN Interface Member

Sequence Number: 1

Interface Member: port2

SD-WAN Zone: virtual-wan-link ▾

Gateway IP: 172.20.11.\$(gateway)

Cost: 1

Status: ☒

Priority: 0

Weight: 80

Advanced Options >

OK Cancel

- In the *Gateway IP* box, select $$(gateway)$, and click *OK*.

- c. Repeat this procedure for port3.

Edit SD-WAN Interface Member

Sequence Number	<input type="text" value="2"/>
Interface Member	<input type="text" value="port3"/>
SD-WAN Zone	<input type="text" value="virtual-wan-link"/>
Gateway IP	<input type="text" value="172.20.12.\$(gateway)"/>
Cost	<input type="text" value="1"/>
Status	<input checked="" type="checkbox"/>
Priority	<input type="text" value="0"/>
Weight	<input type="text" value="20"/>
Advanced Options >	

4. Add the `$(vpn-dc)` meta field to interfaces:
- Double-click the `vpn-dc1-1` interface to open it for editing.
The *Edit SD-WAN Interface Member* dialog box is displayed.

Edit SD-WAN Interface Member

Sequence Number	<input type="text" value="3"/>
Interface Member	<input type="text" value="vpn_dc1-1"/>
SD-WAN Zone	<input type="text" value="vpn"/>
Gateway IP	<input type="text" value="10.254.30.\${vpn_dc}"/>
Cost	<input type="text" value="1"/>
Status	<input checked="" type="checkbox"/>
Priority	<input type="text" value="0"/>
Weight	<input type="text" value="1"/>
Advanced Options >	

- b.** In the *Gateway IP* box, select *\$(vpn-dc)*, and click *OK*.

- c. Repeat this procedure for *vpn-dc1-2*.

Edit SD-WAN Interface Member

Sequence Number	4
Interface Member	vpn_dc1-2
SD-WAN Zone	vpn
Gateway IP	10.254.31.\$(vpn_dc)
Cost	1
Status	<input checked="" type="checkbox"/>
Priority	0
Weight	1
Advanced Options >	

OK
Cancel

The interfaces now use meta fields to define gateway IP addresses.

Device Manager ▾ Install Wizard

Device & Groups ▸ Scripts Provisioning Templates ▾

- Template Group
- System Templates
- IPsec Tunnel Templates
- SD-WAN Templates**
- Static Route Templates
- BGP Templates
- Certificate Templates
- Threat Weight
- CLI Templates
- NSX-T Service Template
- Firmware Templates

Edit SD-WAN Template CLI Configurations

Name: sdwan-branch

Description:

SD-WAN Status: ☒

Interface Members

ID	Interface Member	Status	Weight	Gateway
<input type="checkbox"/>	virtual-w			
<input type="checkbox"/> 1	port2	✓ Enable	80	172.20.11.\$(gateway)
<input type="checkbox"/> 2	port3	✓ Enable	20	172.20.12.\$(gateway)
<input type="checkbox"/>	vpn			
<input type="checkbox"/> 3	vpn_dc1-1	✓ Enable	1	10.254.30.\$(vpn_dc)
<input type="checkbox"/> 4	vpn_dc1-2	✓ Enable	1	10.254.31.\$(vpn_dc)

5. Click **OK** to save the template.

6. Install the policy to the FortiGate devices.
The configuration should not change. You can review the installation preview before installing to confirm no configuration changes.

Upgrading FortiOS from 6.4 to 7.0

Upgrade of FortiOS from 6.4 to 7.0 is recommended, but not required.

To upgrade FortiOS on managed FortiGates:

1. In FortiManager, ensure you are in the correct ADOM.
2. Go to *Device Manager > Firmware Templates*, and create a new firmware template for FortiGate.
3. Assign the firmware template to the FortiGates.
4. Initiate the FortiOS upgrade.
The managed FortiGates are upgraded to FortiOS 7.0.

Upgrading ADOM version 6.4 to 7.0

If you are upgrading FortiOS to 7.0, finish upgrading all FortiGate devices in the SD-WAN network before upgrading the ADOM in FortiManager from version 6.4 to 7.0. See the [FortiManager 7.0.3 Administration Guide](#).

Installing policy changes with a workaround

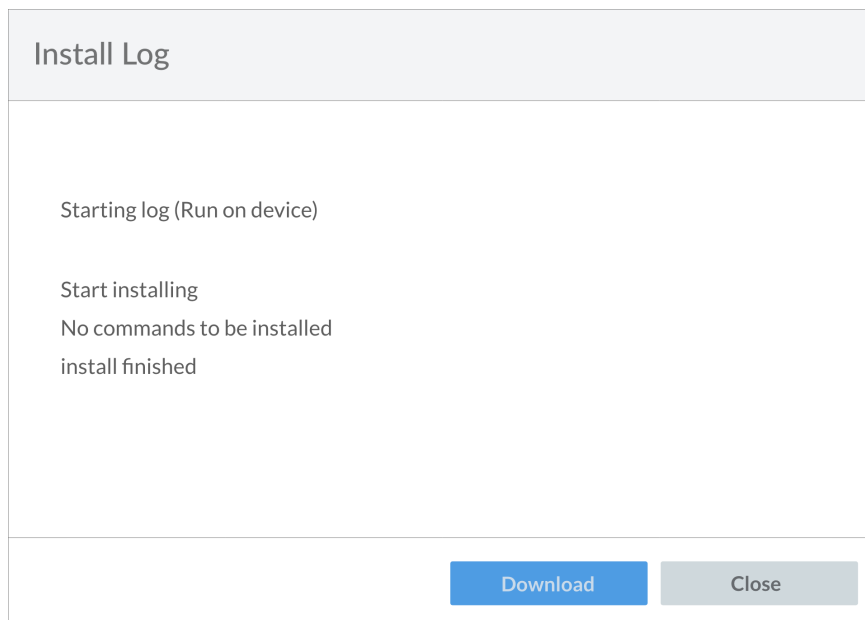
After the FortiManager ADOM is upgraded to 7.0, set the gateway IP address for the VPN interface to 0.0.0.0, and install the policy changes to the FortiGates.



This section assumes that meta fields are set to optional earlier in the process. See [Creating meta fields to set gateway IP addresses on page 11](#).

To install policy changes:

1. In *Device Manager*, go to *Provisioning Templates > SD-WAN Templates*, and double-click the SD-WAN template to open it for editing.
In the *Interface Members* section, the interfaces are displayed.
2. Double-click the VPN interface, set the *Gateway IP* to 0.0.0.0, and click *OK*.
The gateway IP address change is saved.
3. Click *OK* to save the SD-WAN template.
4. Click *Install Wizard* and install the policy changes.
The changes are installed. A *No command to be installed* message is displayed in the installation log file.



You can use the install preview to ensure that the configuration remains unchanged.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.