



SD-WAN Orchestrator MEA - Release Notes

Version 6.4.1 r2

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/support-and-training/training.html>

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



August 13, 2020

SD-WAN Orchestrator MEA 6.4.1 r2 Release Notes

02-641r2-657247-20200813

TABLE OF CONTENTS

Change Log	4
SD-WAN Orchestrator MEA 6.4.1 r2 Release	5
Supported FortiManager host models	5
What's new	5
Support for additional FortiGate models	5
Support for more business rule options	5
Special Notices	7
FortiManager upgraded before SD-WAN Orchestrator MEA	7
FortiSwitch profiles	7
AP profiles	8
Upgrade Information	9
Upgrading SD-WAN Orchestrator MEA before FortiManager	9
Upgrading SD-WAN Orchestrator MEA after FortiManager	9
Product Integration and Support	11
Supported FortiManager and FortiOS versions	11
Supported FortiGate models	11
Resolved Issues	12
Known Issues	14
SD-WAN Orchestrator MEA	14
FortiManager and FortiOS	14
FortiSwitch and FortiAP	15

Change Log

Date	Change Description
2020-08-13	Initial release of 6.4.1 r2.

SD-WAN Orchestrator MEA 6.4.1 r2 Release

This document provides information about SD-WAN Orchestrator MEA version 6.4.1 r2 build 0314. SD-WAN Orchestrator MEA management extension application (MEA) is available with some FortiManager models.

This section includes the following topics:

- [Supported FortiManager host models on page 5](#)
- [What's new on page 5](#)

Supported FortiManager host models

For a list of FortiManager models that can host SD-WAN Orchestrator MEA 6.4.1 r2 management extension application and minimum system requirements, see the [FortiManager 6.4.2 Release Notes](#).

What's new

This section identifies new features and enhancements available with SD-WAN Orchestrator MEA 6.4.1 r2.

For information about what's new in FortiManager 6.4, see the [FortiManager 6.4 New Features Guide](#).

Support for additional FortiGate models

SD-WAN Orchestrator MEA 6.4.1 r2 adds support for the following FortiGate models:

- FortiGate 60F
- FortiGate 61F
- FortiGate 100F
- FortiGate 101F
- FortiGate 2200E
- FortiGate 2201E
- FortiGate 3300E
- FortiGate 3301E

Support for more business rule options

The options available when creating business rules depend on whether you are creating a business rule for a hub or edge device.

For hub devices, the following new options are now available when creating business rules:

- Set the *Group Type* to *Underlay*, and a *Manual* option is now available for *Load Policy*.
- Set the *Group Type* to *Overlay*, and a *Backhaul to Group* option is now available.

For edge devices, the following new option is now available when creating business rules:

- Set the *Group Type* to *All*.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in SD-WAN Orchestrator MEA 6.4.1 r2.

- [FortiManager upgraded before SD-WAN Orchestrator MEA on page 7](#)
- [FortiSwitch profiles on page 7](#)
- [AP profiles on page 8](#)

FortiManager upgraded before SD-WAN Orchestrator MEA

If SD-WAN Orchestrator was enabled in FortiManager 6.4.1, you can no longer access it in the FortiManager GUI if you upgrade FortiManager to 6.4.2 before you upgrade SD-WAN Orchestrator MEA to 6.4.1 r2.

To workaround this issue, run the following CLI command to manually trigger an update of SD-WAN Orchestrator MEA to 6.4.1 r2:

```
diagnose docker upgrade sdwancontroller
```

See also [Upgrading SD-WAN Orchestrator MEA after FortiManager on page 9](#).

FortiSwitch profiles

If SD-WAN Orchestrator MEA prompts an exception when changing the profile of a device as reported in issue 064530, check if the two profiles meet the following conditions:

1. Compare VLANs in interface FortiLink with these two profiles, and check if there are VLANs that own same VLAN ID.
2. Compare VLANs in same interface (except interface FortiLink) with these two profiles, and check if there are VLANs that own same name, but have different VLAN IDs.
3. Compare VLANs in different interfaces (except interface FortiLink) with these two profiles, and check if there are VLANs that own same name.

Workaround:

1. Make sure the device is synchronized, and then enable the *override device LAN* setting.
2. Release resources (for example, IP pool, DHCP server, and so on) used by VLANs (except default, video, voice, rspan, onboarding, quarantine) in interface FortiLink.
3. Release resources used by VLANs that meet condition 2 above, and then delete these VLANs.
4. Release resources used by VLANs that meet condition 3 above, and then delete these VLANs.
5. Disable Switch/AP configuration in *Device LAN setting* page.
6. Wait 5-10 minutes until device's configuration state becomes *Modified*, and then trigger a manual deployment.
7. When device is synchronized, change profile.
8. After changing the profile, disable *override device LAN* setting.

AP profiles

When you cannot re-assign or change AP profiles as described in 0644640 and 0644875 in the *Known Issues* section of the release notes, use the following workaround.

Workaround:

1. In SD-WAN Orchestrator MEA, edit the profile and toggle off *Switch/AP Configuration*, and install the configuration to the device.
SD-WAN Orchestrator MEA synchronizes the configuration to FortiGate with a default AP profile in which SSID is empty.
2. In FortiManager, install the policy package changes to the device, and ensure that the status is *Synchronized*.
3. In SD-WAN Orchestrator MEA, open the AP profile for editing to find the name of the profile in FortiManager (for example, *swnc-1*), and then click *Cancel* to close the profile without saving any changes.
4. In *FortiManager > AP Manager*, open the profile for editing, and change every radio mode from *access point* to *disabled*.
5. In SD-WAN Orchestrator MEA, edit the profile and toggle on *Switch/AP Configuration*, and wait for SD-WAN Orchestrator MEA to discover and bind the AP.
6. In *FortiManager > AP Manager*, open the profile for editing, and change every radio mode from *disabled* to *access point*.
7. In SD-WAN Orchestrator MEA, click the *sync* button.

Upgrade Information

Upgrade of SD-WAN Orchestrator MEA 6.4.1 to 6.4.1 r2 is supported. How you upgrade SD-WAN Orchestrator MEA depends on whether you have already upgraded FortiManager to 6.4.2.



SD-WAN Orchestrator MEA 6.4.1 r2 requires FortiManager 6.4.1 or later, and you must be in a 6.4 ADOM to access SD-WAN Orchestrator MEA.

This section covers the following upgrade scenarios:

- [Upgrading SD-WAN Orchestrator MEA before FortiManager on page 9](#)
- [Upgrading SD-WAN Orchestrator MEA after FortiManager on page 9](#)

Upgrading SD-WAN Orchestrator MEA before FortiManager

If you have not yet upgraded FortiManager to 6.4.2, you can upgrade SD-WAN Orchestrator MEA by using the GUI.

In this scenario, you are starting the upgrade with the following items:

- FortiManager 6.4.1
- SD-WAN Orchestrator MEA 6.4.1

To upgrade SD-WAN Orchestrator MEA by using the GUI:

1. Upgrade SD-WAN Orchestrator MEA from 6.4.1 to 6.4.1 r2 by using the GUI.
 - a. If ADOMs are enabled in FortiManager, ensure you are in the root ADOM to access the *Maintenance* tab in SD-WAN Orchestrator MEA.
 - b. In SD-WAN Orchestrator MEA, go to *Maintenance > Upgrade*, and click *Check for updates*.
SD-WAN Orchestrator MEA is upgraded to 6.4.1 r2.
2. Upgrade FortiManager from 6.4.1 to 6.4.2.
For details about upgrading FortiManager, see the [FortiManager 6.4.2 Upgrade Guide](#).
FortiManager is upgraded to 6.4.2.

Upgrading SD-WAN Orchestrator MEA after FortiManager

If you have already upgraded FortiManager to 6.4.2, you can upgrade SD-WAN Orchestrator MEA by using the CLI. You cannot use the SD-WAN Orchestrator MEA GUI for this upgrade scenario.

In this scenario, you are starting the upgrade with the following items:

- FortiManager 6.4.2
- SD-WAN Orchestrator MEA 6.4.1

To upgrade SD-WAN Orchestrator MEA by using the CLI:

1. Ensure that FortiManager has been upgraded to 6.4.2.
2. In the FortiManager banner, click the *CLI console* button located in the top-right corner.
The *CLI Console* opens.
3. Run the following command:

```
diagnose docker upgrade sdwancontroller
```


SD-WAN Orchestrator MEA is upgraded to 6.4.1 r2.

Product Integration and Support

This section lists SD-WAN Orchestrator MEA 6.4.1 r2 support of other Fortinet products. It contains the following topics:

- [Supported FortiManager and FortiOS versions on page 11](#)
- [Supported FortiGate models on page 11](#)

Supported FortiManager and FortiOS versions

This section identifies SD-WAN Orchestrator MEA 6.4.1 r2 product integration and support information:

FortiManager	• 6.4.1 - 6.4.2
FortiOS	• 6.4.1 - 6.4.2

Supported FortiGate models

SD-WAN Orchestrator MEA supports the following FortiGate models:

Model	Firmware Version
FortiGate: FortiGate-60F, FortiGate-61F, FortiGate-100F, FortiGate-101F, FortiGate-60E, FortiGate-61E, FortiGate-60E-POE, FortiGate-80E, FortiGate-81E, FortiGate-80E-POE, FortiGate-81E-POE, FortiGate-100E, FortiGate-100EF, FortiGate-101E, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-201E, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-401E, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-601E, FortiGate-1100E, FortiGate-1101E, FortiGate-2000E, FortiGate-2500E, FortiGate-3400E, FortiGate-3401E, FortiGate-3600E, FortiGate-3601E, FortiGate-3960E, FortiGate-3980E, FortiGate-300D, FortiGate-400D, FortiGate-500D, FortiGate-600D, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-2200E, FortiGate-2201E, FortiGate-3000D, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3800D, FortiGate-3980E; FortiGate-VM: Same support as FortiManager 6.4.1. See the FortiManager 6.4.1 Release Notes on the Document Library.	6.4

For a list of FortiManager models that support SD-WAN Orchestrator MEA, see [Supported FortiManager host models on page 5](#).

Resolved Issues

The following issues have been fixed in 6.4.1 r2. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
640693	Onos login page still displays during SD-WAN Orchestrator MEA startup.
638366	[Project_6.4.0] Remove the <i>Edit</i> icon for SD-WAN Orchestrator MEA generated <i>address/addrgroup</i> when adding a business rule.
644134	[Project_6.4.0] Business rule <i>config service</i> is always included in script, even if no changes in it.
637886	[Project_6.4.0_Stress env] Devices already added to the region can be added again.
656873	[Project_6.4.1] Change manual path from Internet link to MPLS link, and IPsec between two MPLS ports goes down.
643323	[Project_6.4.0] Show detail at hub is slow in stress test environment.
652323	[Project_6.4.1] Set <code>add-route disable</code> for IPsec tunnels when ADVPN is enabled.
652361	[Project_6.4.1] Suggest to set lower priority for MPLS WAN port in SD-WAN zone.
653415	[Project_6.4.0] If the FortiLink has members, SD-WAN Orchestrator MEA won't generate default switch VLANs.
654083	[Project_6.4.1] Cannot create and edit <i>address/user/service/isdb</i> objects in Business rule configuration page.
630303	[Project_6.4.0] When log content is too long, the CVS entry is disordered with Excel2016.
644377	FortiGate 60F added by <i>Model device</i> can't show sync details.
631226	[Project_6.4.0] If an SSID security mode is set to <i>WPA3_SAE</i> , and then set to <i>OPEN</i> or <i>WPA2_PERSONAL</i> a conflict occurs.
645045	[Project_6.4.0] Change the security mode from <i>WPA3_SAE</i> to <i>WPA2_Personal</i> causes a conflict.
645928	[Project_6.4.0] Conflict occurs when ISDB in FortiManager is not consistent with FortiGate.
645942	[Project_6.4.0] Enhance the procedure to deploy FortiSwitch to FortiGate, especially when they are already connected.
645633	[Project_6.4.0] If SD-WAN Orchestrator MEA is started, creating or upgrading an ADOM results in lost policy blocks.
644900	[Project_6.4.0] While creating an IP pool, the subnet conflict with FortiLink's default VLAN subnet causes an exception.

Bug ID	Description
629620	[Project_6.4.0] Many <i>src</i> and <i>dst</i> address objects in business rules cannot be edited via the <i>Edit</i> icon followed.
634193	[Project_6.4.0] The device name that was last searched is always displayed in the <i>Search</i> box.
632887	[Project_6.4.0] Change a profile for a region, the FortiGate will be offline and online, but there is no log print offline or online record.
645347	[Project_6.4.0] While disabling <i>sw/ap config override</i> , if the FortiSwitch VLAN assign IP by IP Pool, it is unable to override.
644070	[Project_6.4.0] Generate FortiLink default switch VLAN while creating new profile.
645656	[Project_6.4.0] Devices are added to FMG and SD-WAN Orchestrator MEA via JSON API while sync failed, and also cannot be listed when adding devices to SD-WAN Orchestrator MEA.

Known Issues

The following issues have been identified in 6.4.1 r2. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

SD-WAN Orchestrator MEA

Bug ID	Description
641221	FortiGate-500E does not show up in <i>Available Devices</i> list.
618409	In FortiGate 800-device test bed, not all devices are completely synchronized each time. Workaround: Install configuration again.
657823	Conflict reported as <code>java.lang.NullPointerException</code> when disabling a WAN port and installing config when it's referenced in <i>MANUAL</i> . Workaround: Remove and re-configure the business rule.
654540	Memory usage slowly increasing. Workaround: Use the FortiManager CLI to set <code>sdwancontroller disable</code> and then <code>enable</code> .
656872	When <i>Load Policy</i> is <i>MANUAL</i> and <i>Manual Path</i> is a <i>MPLS link</i> , business rule will fail to be deployed to FortiGate.

FortiManager and FortiOS

Bug ID	Description
643825	SLA in IPsec tunnels sometimes fails due to not sending out SLA probe packets. Workaround: Reboot the FortiGate.
0640431/0641740	When changing ISP link of WAN port from <i>MPLS</i> to <i>Internet</i> or reversely, conflict may occur.
0628750/0630007	When <i>Service Access</i> is enabled on FortiManager interface, SD-WAN Orchestrator MEA fails to start up.
0625980/0625978	Adding FortiGate 300E and FortiGate 600E by <i>Add Model Device</i> will get a conflict and deployment process gets stuck.
0598603/0598895	Sometimes FortiGate 30E warns conflict as <code>execute script:Response has no task attribute!</code> .
0572485/0632946	Once the name of address object changed, the address referred in business rule & firewall policy does not change.

FortiSwitch and FortiAP

Bug ID	Description
0578622/0586763	Installation fails when creating FortiLink interface. Workaround: Deploy FortiLink-related configuration before connecting FortiSwitch to FortiGate.
645946	Conflict reported as delete <code>'fortivoice.fortilink'</code> when FortiSwitch first comes online. Workaround: Use SD-WAN Orchestrator MEA to install configuration to FortiGate again. If it still fails, authorize FortiSwitch on FortiManager or FortiGate, and try to install configuration again.
0618165/0587742	Changing subnet of hard switch interface will cause FMG and FGT conflict.
645236	It will cause conflict if manual create VLAN on FGT but controller did not has this VLAN.
645309	Change the FortiSwitch profile to operate smoothly. For a workaround, see FortiSwitch profiles on page 7 .
0644640/0644875	Cannot re-assign or change AP profile of manually selected tunnel SSID. For a workaround, see AP profiles on page 8 .



FORTINET



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.