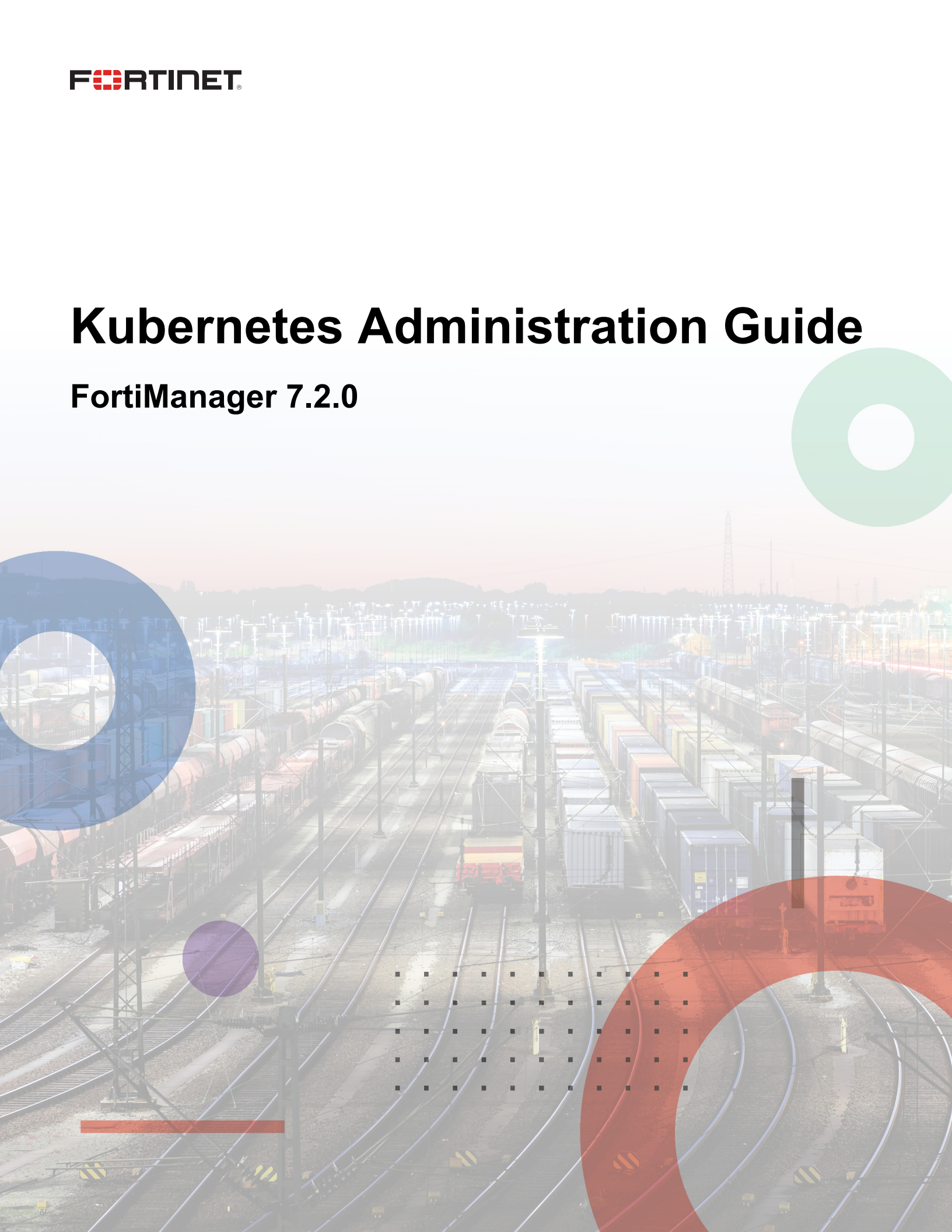


# Kubernetes Administration Guide

FortiManager 7.2.0



**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](mailto:techdoc@fortinet.com)



April 11, 2022

FortiManager 7.2.0 Kubernetes Administration Guide

02-720-794632-20220411

# TABLE OF CONTENTS

<b>Security Fabric connector integration with Kubernetes</b> .....	<b>4</b>
Creating a Fabric connector for Kubernetes .....	4
Importing address names to a Fabric connector .....	5
Creating an IP address policy .....	5
Installing a policy package .....	6
<b>Change log</b> .....	<b>8</b>

# Security Fabric connector integration with Kubernetes

You can use FortiManager to create Fabric connectors for Kubernetes, and then install the Fabric connectors to FortiOS.

The Fabric connectors in FortiManager define the type of connector and include information for FortiOS to communicate with and authenticate with the products. In some cases the FortiGate must communicate with products through the Fabric connector, and in other cases the FortiGate communicates directly with the products.

FortiOS works with the Fabric connector to communicate with Kubernetes.

For information about the Fabric connector, see the [Fortinet Document Library](#).



You cannot import a policy package for the Fabric connector from FortiOS to FortiManager.

---

Following is an overview of creating Fabric connectors for Kubernetes using FortiManager:

1. Create a Fabric connector. See [Creating a Fabric connector for Kubernetes on page 4](#).
2. Import address names from Kubernetes to the Fabric connector. See [Importing address names to a Fabric connector on page 5](#). FortiManager imports the address names and converts them to dynamic firewall address objects. The objects do not include IP addresses and display in *Firewall Objects > Addresses*.
3. In the policy package in which you are creating the new policy, create an IPv4 policy and include the firewall address objects for Kubernetes. See [Creating an IP address policy on page 5](#).
4. Install the policy package to FortiOS. See [Installing a policy package on page 6](#). FortiGate communicates with Kubernetes to dynamically populate the firewall address objects with IP addresses.

## Creating a Fabric connector for Kubernetes

With FortiManager, you can create a Fabric connector for Kubernetes and import address names from Kubernetes to automatically create dynamic objects that you can use in policies.

When you install the policies to one or more FortiGates, FortiOS uses the information and the Fabric connector to communicate with Kubernetes and dynamically populate the objects with IP addresses.

When you create a Fabric connector for Kubernetes, you specify how FortiOS can communicate with Kubernetes through the Fabric connector. As a result, you are configuring communication and authentication information for the Fabric connector.

If you have enabled ADOMs, you can create multiple Fabric connectors per ADOM. Each Fabric connector requires a unique IP address.

This configuration requires the following:

- FortiManager version 6.0 ADOM or later
- FortiManager is managing the FortiGate.

- You have configured the managed FortiGate to work with Kubernetes.

#### To create a Fabric connector object for Kubernetes:

- Go to *Fabric View > Fabric Connectors*.
- Click *Create New*. The *Create New Fabric Connector* wizard displays.
- Under *SDN*, select *Kubernetes*, and click *Next*.
- Configure the following options, then click *OK*:

<b>Name</b>	Enter the Fabric connector name.
<b>IP</b>	Enter the Fabric connector IP address.
<b>Port</b>	Identify the port used for the Fabric connector: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default port.</li> <li>Click <i>Specify</i> and type the port number.</li> </ul>
<b>Secret Token</b>	Specify a secret token for the Fabric connector.
<b>Update Interval(s)</b>	Specify the update interval for the Fabric connector: <ul style="list-style-type: none"> <li>Click <i>Use Default</i> to use the default port.</li> <li>Click <i>Specify</i> and type the port number.</li> </ul>
<b>Status</b>	Toggle <i>On</i> to enable the Fabric connector. Toggle <i>OFF</i> to disable the Fabric connector.

## Importing address names to a Fabric connector

After you configure a Fabric connector, you can import dynamic objects from cloud platforms, such as Kubernetes, to the Fabric connector, and dynamic firewall address objects are automatically created.

#### To import address names for Kubernetes:

- Go to *Policy & Objects > Object Configurations*.
- Go to *Security Fabric > Fabric Connectors*.
- In the content pane, right-click the Kubernetes Fabric connector, and select *Import*. The *Import SDN Connector* dialog displays.
- Select the address names, and click *Import*. FortiManager imports the address names and converts them to dynamic firewall address objects that display on the *Firewall Objects > Addresses* pane.

## Creating an IP address policy

The section describes how to create new IPv4 and IPv6 policies.

You can create an IPv6 security policy for an IPv6 network and a transitional network. A transitional network is a network that is transitioning to IPv6 but must still have access to the Internet or must connect over an IPv4 network. IPv6 policies allow for this specific type of traffic to travel between the IPv6 and IPv4 networks.



On the *Policy & Objects* tab, from the *Tools* menu, select *Display Options*. In the *Policy* section, select the *IPv6 Policy* checkbox to display this option.

**To create a new IPv4 or IPv6 policy:**

1. Ensure that you are in the correct ADOM.
2. Go to *Policy & Objects > Policy Packages*.
3. In the tree menu for the policy package in which you will be creating the new policy, select *IPv4 Policy* or *IPv6 Policy*. If you are in the Global Database ADOM, select *IPv4 Header Policy*, *IPv4 Footer Policy*, *IPv6 Header Policy*, or *IPv6 Footer Policy*.
4. Click *Create New*, or, from the *Create New* menu, select *Insert Above* or *Insert Below*. By default, policies will be added to the bottom of the list, but above the implicit policy. The *Create New Policy* pane opens.

**Create New IPv4 Policy**

Name	<input type="text"/>
Incoming Interface	<input type="text" value="any"/> <span style="float: right;">⊗</span>
Outgoing Interface	<input type="text" value="any"/> <span style="float: right;">⊗</span>
Source Internet Service	<input type="checkbox"/> OFF
Source Address	<input type="text" value="all"/> <span style="float: right;">⊗</span>
Source User	<input type="text" value="+"/>
Source User Group	<input type="text" value="+"/>
Source Device	<input type="text" value="+"/>
Destination Internet Service	<input type="checkbox"/> OFF
Destination Address	<input type="text" value="all"/> <span style="float: right;">⊗</span>
Service	<input type="text" value="ALL"/> <span style="float: right;">⊗</span>
Schedule	<input type="text" value="always"/> <span style="float: right;">⊗</span>
Action	<input checked="" type="radio"/> Deny <input type="radio"/> Accept <input type="radio"/> IPSEC
Log Traffic	<input checked="" type="checkbox"/> Log Violation Traffic
	<input type="checkbox"/> Generate Logs when Session Starts
Comments	<input style="width: 100%;" type="text"/>
Meta Fields >	
Advanced Options >	

5. Complete the options.
6. Click *OK* to create the policy.  
You can enable or disable the policy in the right-click menu. When disabled, a disabled icon displays in the *Seq.#* column to the left of the number.

## Installing a policy package

When installing a policy package, objects that the policy references are installed to the target device. Default or per-device mapping must exist or the installation fails.



Some objects that the policy does not directly reference are also installed to the target device, such as FSSO polling objects, address and profile groups, and CA certificates.

**To install a policy package to a target device:**

1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy package. You can install policy package and device settings or install the interface policy only.







[www.fortinet.com](http://www.fortinet.com)

Copyright© 2022 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.