



FortiManager - Fabric Connectors for Nuage

Version 6.0.3

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 COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com



October 26, 2018

FortiManager 6.0.3 Fabric Connectors for Nuage

02-600-00000-20181026

TABLE OF CONTENTS

Creating fabric connectors for Nuage	4
Configuring dynamic firewall addresses for fabric connectors	5
Creating IP policies	6
Installing policy packages	7
Change Log	8

Creating fabric connectors for Nuage

You can use FortiManager to create SDN fabric connectors for Nuage Virtualized Services Platform, and then install the fabric connectors to FortiGates.

The fabric connectors in FortiManager define the type of connector and include information for FortiGate to communicate with and authenticate with the products. In some cases FortiGate units must communicate with products through the Fortinet SDN Connector, and in other cases FortiGate units communicate directly with the products.

FortiGate works with Fortinet SDN Connector to communicate with Nuage Virtualized Services Platform.

For more information about Fortinet SDN Connector, see the [Fortinet Document Library](#).



You cannot import a policy package for Fortinet SDN Connector from FortiGate to FortiManager.

Following is an overview of how to create fabric connectors for Nuage by using FortiManager:

1. Create a fabric connector object for Nuage. See [Creating fabric connector objects for Nuage on page 4](#).
2. Create dynamic firewall address objects. See [Configuring dynamic firewall addresses for fabric connectors on page 5](#).
You cannot import address names from Nuage Virtualized Services Platform to FortiManager.
3. In the policy package in which you will be creating the new policy, create an IPv4 policy and include the firewall address objects for Nuage Virtualized Services Platform. See [Creating IP policies on page 6](#).
4. Install the policy package to FortiGate. See [Installing policy packages on page 7](#).
FortiGate communicates with Nuage Virtualized Services Platform to dynamically populate the firewall address objects with IP addresses.

Creating fabric connector objects for Nuage

With FortiManager, you can create a fabric connector for Nuage Virtualized Services Platform. You cannot import address names from Nuage Virtualized Services Platform to the fabric connector. Instead you must manually create dynamic firewall objects that you can use in policies. When you install the policies to one or more FortiGate units, FortiGate uses the information and Fortinet SDN Connector to communicate with Nuage Virtualized Services Platform and dynamically populate the objects with IP addresses.

When you create a fabric connector for Nuage Virtualized Services Plan, you are specifying how FortiGate can communicate with Nuage through Fortinet SDN Connector. As a result, you are configuring communication and authentication information for Fortinet SDN Connector.

If ADOMs are enabled, you can create multiple fabric connectors per ADOM; however, each fabric connector requires a unique IP address.

Requirements:

- FortiManager version 6.0 ADOM or later
- FortiGate is managed by FortiManager.
- The managed FortiGate unit is configured to work with Nuage Virtualized Services Platform.

To create a fabric connector object for Nuage:

1. Go to *Fabric View > Fabric Connectors*.
2. Click *Create New*. The *Create New Fabric Connector* wizard is displayed.
3. Under *SDN*, select *Nuage*, and click *Next*.
4. Configure the following options, and then click *OK*:

Name	Type a name for the fabric connector object.
Type	Displays Nuage Virtualized Services Platform.
IP	Type the IP address for Fortinet SDN Connector.
Port	Identify the port used for Fortinet SDN Connector. Perform one of the following options: <ul style="list-style-type: none"> • Click <i>Use Default</i> to use the default port. • Click <i>Specify</i> and type the port number.
User Name	Type the user name for Fortinet SDN Connector.
Password	Type the password for Fortinet SDN Connector.
Status	Toggle <i>On</i> to enable the fabric connector object. Toggle <i>OFF</i> to disable the fabric connector object.

Configuring dynamic firewall addresses for fabric connectors

You cannot import address names to fabric connectors created for Microsoft Azure and Nuage Virtualized Services Platform. Instead you must create dynamic firewall objects that can be dynamically populated when FortiGate communicates with Microsoft Azure and Nuage Virtualized Services Platform.

To configure dynamic firewall addresses for Microsoft Azure fabric connectors:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Firewall Objects > Addresses*.
3. In the content pane, click *Create New* and select *Address*.
4. Complete the following options for Microsoft Azure fabric connectors:

Address Name	Type a name for the firewall address object.
Type	Select <i>Fabric Connector Address</i> .
SDN	Select the Microsoft Azure fabric connector.
Filter	Type the name of the filter for the AWS instance.

5. Set the remaining options as required, and click *OK*

To configure dynamic firewall addresses for Nuage fabric connectors:

1. Go to *Policy & Objects > Object Configurations*.
2. In the tree menu, go to *Firewall Objects > Addresses*.
3. In the content pane, click *Create New* and select *Address*.
4. Complete the following options for Nuage fabric connectors:

Address Name	Type a name for the firewall address object.
Type	Select <i>Fabric Connector Address</i> .
SDN	Select the Nuage Virtualized Services Platform fabric connector.
Organization	Type the name of the organization for the Nuage Virtualized Services Platform.
Subnet Name	Type the name of the subnet for the Nuage Virtualized Services Platform.
Policy Group	Type the name of the policy group for the Nuage Virtualized Services Platform.

5. Set the remaining options as required, and click *OK*

Creating IP policies

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

IPv6 security policies are created both for an IPv6 network and a transitional network. A transitional network is a network that is transitioning over 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"/> ✕
Outgoing Interface	<input type="text" value="any"/> ✕
Source Internet Service	<input type="checkbox"/> OFF
Source Address	<input type="text" value="all"/> ✕
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"/> ✕
Service	<input type="text" value="ALL"/> ✕
Schedule	<input type="text" value="always"/> ✕
Action	<input type="button" value="Deny"/> <input type="button" value="Accept"/> <input type="button" value="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 select to enable or disable the policy in the right-click menu. When disabled, a disabled icon will be displayed in the *Seq.#* column to the left of the number.

Installing policy packages

When installing a policy package, objects that are referenced in the policy will be installed to the target device. Default or per-device mapping must exist or the installation will fail.



Some objects that are not directly referenced in the policy will also be 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:

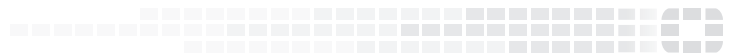
1. Ensure you are in the ADOM that contains the policy package.
2. Go to *Policy & Objects > Policy Packages*.
3. Select a policy package and from the *Install* menu or right-click menu select *Install Wizard*. The *Install Wizard* opens.
4. Follow the steps in the install wizard to install the policy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

Change Log

Date	Change Description
2018-	Initial release.



FORTINET[®]



Copyright© 2018 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.