Contact Information
Forescout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA
https://www.Forescout.com/support/
Toll-Free (US): 1.866.377.8771
Tel (Intl): 1.408.213.3191
Support: 1.708.237.6591

About the Documentation
- Refer to the Technical Documentation page on the Forescout website for additional documentation: https://www.Forescout.com/company/technical-documentation/
- Have feedback or questions? Write to us at documentation@forescout.com

Legal Notice
© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.Forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners.
Table of Contents

About the Fortinet Next-Generation Firewall Integration ............................. 5
  About Certification Compliance Mode ........................................................ 5
  Use Cases .................................................................................................. 5
  Additional Fortinet Documentation .......................................................... 6

Concepts, Components, and Considerations ............................................. 7
  Concepts .................................................................................................. 7
  Components ........................................................................................... 7
  Considerations ....................................................................................... 7

How it Works ............................................................................................... 8

What to Do .................................................................................................. 9

Requirements ............................................................................................. 10
  Forescout Software Requirements .......................................................... 10
  Fortinet Requirements ........................................................................... 10
  Forescout eyeExtend (Extended Module) Licensing Requirements ............. 10
    Per-Appliance Licensing Mode .............................................................. 11
    Flexx Licensing Mode ............................................................................ 12
    More License Information ...................................................................... 13

Install the Module ....................................................................................... 13

Configure the Module ................................................................................ 14
  Access REST API .................................................................................... 14
  Add a FortiManager Connection .............................................................. 14
  Edit a FortiManager Connection ............................................................ 18
  Test a FortiManager Connection ............................................................. 19
  Remove a FortiManager Connection ......................................................... 20
  Add a FortiGate Connection .................................................................... 20
  Sync a FortiGate Connection .................................................................... 24
  Edit a FortiGate Connection .................................................................... 24
  Test a FortiGate Connection .................................................................... 25
  Remove a FortiGate Connection .............................................................. 26

Create Custom Policies ............................................................................. 27
  Create a Custom Policy ........................................................................... 27
  Policy Properties .................................................................................... 31
  Policy Actions ......................................................................................... 33
    Manually Run FortiManager Action ....................................................... 37
    Manually Run FortiGate Action ............................................................ 40
    Set Action Thresholds .......................................................................... 42
    Remove an Action ............................................................................... 43
Policy Action Details................................................................. 44
Start or Stop a Custom Policy .................................................. 45

Best Practices .............................................................................. 46

Additional Forescout Documentation........................................... 46
  Documentation Downloads ....................................................... 47
  Documentation Portal ............................................................. 47
  Forescout Help Tools ............................................................. 48
About the Fortinet Next-Generation Firewall Integration

Forescout eyeExtend for Fortinet® Next-Generation Firewall (NGFW) integrates with FortiGate® and FortiManager® to magnify the power of the firewall. The integration:

- Implements dynamic network segmentation based on real-time device intelligence from the Forescout platform
- Supports Share Package, Address Group, or vDOM from the Forescout platform to enforce granular access policies within Fortinet NGFW
- Reduces your attack surface, prevents unauthorized access to sensitive resources, and minimizes the impact of data breaches

Support is provided for:

- Single FortiManager deployment
- Multiple FortiGate deployments
- IPv4 and IPv6 addresses
- Adding IP addresses to an address group or removing IP addresses from an address group based on policy

To use the module, you should have a solid understanding of Fortinet Next-Generation Firewall concepts, functionality, and terminology, and understand how Forescout policies and other basic features work.

About Certification Compliance Mode

Forescout eyeExtend for Fortinet NGFW supports Certification Compliance mode. For information about this mode, refer to the Forescout Installation Guide.

Use Cases

With the Fortinet NGFW integration:

- The Forescout platform automatically discovers, classifies, and assesses devices as they connect to the network.
- For devices that passed network compliance checks, the Forescout platform adds devices to the appropriate address group in a specific VDOM.
- The Fortinet NGFW leverages this information from the Forescout platform to apply granular context-aware security policies and enforce access controls.
The use case supported by Forescout eyeExtend for Fortinet is the dynamic addition of IPv4 or IPv6 addresses to pre-defined Fortinet object groups to FortiManager or directly to VDOM in FortiGate, providing dynamic network segmentation.

**Example Workflow**

The following is a scenario for network segmentation for different types of IoT devices. The workflow is as follows:

1. Different types of IoT devices connect to the network.
2. The Forescout platform automatically discovers, classifies, and assesses devices as they connect.
3. For devices that passed network compliance checks, the Forescout platform adds devices to the appropriate Fortinet virtual domains (VDOMs) and address group.
4. Fortinet NGFW leverages this information from the Forescout platform to provide access based on custom policies. Untrusted devices are blocked; IoT devices are limited to their functional needs only.

**Additional Fortinet Documentation**

Refer to the following online documentation for more information about the Fortinet Next-Generation Firewall solution:

- [https://docs.fortinet.com/fortigate/admin-guides](https://docs.fortinet.com/fortigate/admin-guides)
- [https://docs.fortinet.com/d/fortiauthenticator-rest-api-solution-guide](https://docs.fortinet.com/d/fortiauthenticator-rest-api-solution-guide)
Concepts, Components, and Considerations

The following sections provide an overview architecture of the Fortinet and Forescout eyeExtend for Fortinet platforms:

- **Concepts**
- **Components**
- **Considerations**

**Concepts**

The key concepts are as follows:

- **VDOM** – virtual domain, used for FortiGate only. A VDOM is a virtual instance of a firewall inside the firewall. It helps segregate networks by isolating traffic to specific VDOMs and not allowing them to talk to endpoints in other VDOMs.
- **Address group** – a group of IP addresses, leased from a Fortinet administrator. Fortinet provides you with address group names, such as addressgroup1, addressgroup2, addressgroup3.

**Components**

The Fortinet/Forescout eyeExtend for Fortinet architecture incorporates the following components:

- FortiGate Next-Generation Firewall (NGFW)
- FortiManager

**Considerations**

When deploying Fortinet/Forescout eyeExtend for Fortinet, consider the following:

- You cannot configure both FortiGate and FortiManager at the same time.
- The number of VDOMs supported by FortiGate is specified in the Fortinet license.
- The Forescout platform expects the default FortiManager Administrative Domain (ADOM) to be set to root.
- Address groups must be pre-defined in Fortinet.
- There are different address groups for IPv4 and IPv6 and you cannot mix them. For example, an IPv6 address has to match an IPv6 address group.
- If FortiManager is configured as a target connection, the address groups and the firewall rules must be synchronized between FortiManager and FortiGates at all times.
• In FortiGate, adding addresses to an address group that is currently at maximum capacity reports *Action Successful* on the Forescout platform. Despite this, no addresses are added to the group after the limit is reached. (FortiManager reports *Action Failed* for this.)

• You can use your own server certificate. For more information about certificates, refer to the *Forescout Administration Guide*.

**How it Works**

This section describes how the module communicates with one or more FortiGates or one FortiManager.

In the following diagram, each firewall is assigned to a connecting CounterACT® Appliance with which it communicates. Multiple firewalls can be assigned to a single CounterACT Appliance. The connecting CounterACT Appliance sends the action-related information to the relevant firewall.

The supported deployment architectures are as follows:

• One CounterACT Appliance to $M$ FortiGates (default)

• $M$ CounterACT Appliances to one FortiGate
• $M$ CounterACT Appliances to $M$ FortiGates (shown in figure above)
  where $M$ indicates Many

FortiGate supports either standalone or High Availability (HA) mode.
In the following diagram, each firewall is connected to FortiManager, which manages a distributed network of virtual or physical firewalls. One or more CounterACT Appliances communicate with FortiManager, which then communicates with the FortiGate firewalls.

The supported deployment architectures are as follows:
• One CounterACT Appliance to one FortiManager (shown in figure above)
• $M$ CounterACT Appliances to one FortiManager
  where $M$ indicates Many

**What to Do**

To set up your system for integration with Fortinet, perform the following steps:
1. Verify that the requirements are met. See Requirements.
2. Download and Install the Module.
3. Configure the Module.

Requirements

This section describes the system requirements, including:

- Forescout Software Requirements
- Fortinet Requirements
- Forescout eyeExtend (Extended Module) Licensing Requirements

Forescout Software Requirements

The module requires the following Forescout releases and other components:

- Forescout version 8.2.
- A module license for Forescout eyeExtend for Fortinet NGFW. See Forescout eyeExtend (Extended Module) Licensing Requirements.

Fortinet Requirements

Fortinet requires the following releases:

- FortiManager v6.0.2
- FortiGate v6.0.2
- For information about the vendor models (hardware/software) and versions (product/OS) that are validated for integration with this Forescout component, refer to the Forescout Compatibility Matrix.

Port 443/TCP must be open on enterprise firewalls to support HTTPS communication between the Forescout platform and FortiManager or FortiGate.

Forescout eyeExtend (Extended Module) Licensing Requirements

This Forescout eyeExtend product requires a valid license. Licensing requirements differ based on which licensing mode your deployment is operating in:

- Per-Appliance Licensing Mode
- Flexx Licensing Mode

To identify your licensing mode:

- From the Console, select Help > About Forescout.
Per-Appliance Licensing Mode

When installing the module, you are provided with a 90-day demo license.

If you would like to continue exploring the module before purchasing a permanent license, you can request a demo license extension. Consult with your Forescout representative before requesting the extension. You will receive email notification and alerts at the Console before the demo period expires.

To continue working with the module after the demo period expires, you must purchase a permanent module license.

Demo license extension requests and permanent license requests are made from the Console.

This module may have been previously packaged as a component of an Integration Module which contained additional modules. If you already installed this module as a component of an Integration Module, you can continue to use it as such. Refer to the section about module packaging in the Forescout Administration Guide for more information.

Requesting a License

When requesting a demo license extension or permanent license, you are asked to provide the device capacity requirements. This is the number of devices that you want this license to handle. You must define at least the number of devices currently detected by the Forescout platform. You can request a license that handles more to ensure that you are licensed for support on additional devices as your deployment grows.

Enter this number in the Devices pane of the Module License Request wizard, in the Console Modules pane.
To view the number of currently detected devices:

1. Select the **Home** tab.

2. In the Views pane, select the **All Hosts** folder. The number in parentheses displayed next to the **All Hosts** folder is the number of devices currently detected.

**Flexx Licensing Mode**

When you set up your Forescout deployment, you must activate a license file containing valid licenses for each feature you want to work with in your deployment, including eyeExtend products. After the initial license file has been activated, you can update the file to add additional eyeExtend licenses or change endpoint capacity for existing eyeExtend products. For more information on obtaining eyeExtend licenses, contact your Forescout sales representative.

- *No demo license is automatically installed during system installation.*

License entitlements are managed in the [Forescout Customer Portal](https://www.forescout.com). After an entitlement has been allocated to a deployment, you can activate or update the relevant licenses for the deployment in the Console.

Each eyeExtend license has an associated capacity, indicating the number of endpoints the license can handle. The capacity of each eyeExtend license varies by module but does not exceed the capacity of the Forescout eyeSight license.
Integration Modules, which package together groups of related licensed modules, are not supported when operating in Flexx Licensing Mode. Only eyeExtend products, packaging individual licensed modules are supported. The Open Integration Module is an eyeExtend product even though it packages more than one module.

More License Information

For more information on eyeExtend (Extended Module) licenses:

- **Per-Appliance Licensing.** Refer to the Forescout Administration Guide.
- **Flexx Licensing.** Refer to the Flexx Licensing How-to Guide.

You can also contact your Forescout sales representative for more information.

Install the Module

To install the module:

1. Navigate to one of the following Forescout download portals, depending on the licensing mode your deployment is using:
   - Product Updates Portal - **Per-Appliance Licensing Mode**
   - Customer Portal, Downloads Page - **Flexx Licensing Mode**

   To identify your licensing mode, select Help > About ForeScout from the Console.

2. Download the module .fpi file.

3. Save the file to the machine where the Console is installed.

4. Log into the Console and select Options from the Tools menu.

5. Select Modules. The Modules pane opens.

6. Select Install. The Open dialog box opens.

7. Browse to and select the saved module .fpi file.

8. Select Install. The Installation screen opens.

9. Select I agree to the License Agreement to confirm that you have read and agree to the terms of the License Agreement and select Install. The installation cannot proceed unless you agree to the license agreement.

   - The installation begins immediately after selecting Install and cannot be interrupted or canceled.

   - In modules that contain more than one component, the installation proceeds automatically one component at a time.

10. When the installation completes, select Close to close the window. The installed module is displayed in the Modules pane.

   - Some components are not automatically started following installation.
Configure the Module

Configure the module so that the Forescout platform can communicate with FortiManager and/or FortiGate.

You cannot configure both FortiGate and FortiManager at the same time. An error message is displayed if one is already configured and you try to configure the other.

For FortiManager, see the following sections:

- Access REST API
- Add a FortiManager Connection
- Edit a FortiManager Connection
- Test a FortiManager Connection
- Remove a FortiManager Connection

For FortiGate, see the following sections:

- Add a FortiGate Connection
- Sync a FortiGate Connection
- Edit a FortiGate Connection
- Test a FortiGate Connection
- Remove a FortiGate Connection

Access REST API

To allow the REST API to access FortiManager, set rpc-permit to read-write. Use the following CLI commands on FortiManager to enable rpc-permit for user ***.

```
FMG-1 # config system admin user
(user)# edit ***
(***)# set rpc-permit read-write
(***)# end
```

Add a FortiManager Connection

Define a connection to FortiManager, including login credentials.

**To add a FortiManager connection:**

1. In the Console, select **Options** from the **Tools** menu.
2. From the Options pane, select **Fortinet Next-Generation Firewall**.

![Options pane with Fortinet Next-Generation Firewall selected](image1.png)

3. Select the FortiManager tab and then select **Add**.

![Add FortiManager Connection](image2.png)

4. Define the FortiManager connection parameters as follows:

<table>
<thead>
<tr>
<th><strong>FortiManager FQDN or IP Address</strong></th>
<th>Enter the Fully Qualified Domain Name (FQDN) of FortiManager, or the IPv4 or IPv6 address. You must enter the FQDN if the <strong>Validate Server Certificate</strong> option is selected.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username used to access FortiManager. This is the same username granted read-write privilege for REST API access. See <a href="#">Access REST API</a>.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password used to access FortiManager.</td>
</tr>
<tr>
<td><strong>Verify Password</strong></td>
<td>Re-enter the password to verify it.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Enter text that describes the connection, such as a nickname.</td>
</tr>
</tbody>
</table>
**Validate Server Certificate**

Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:

- Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance
- Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance

Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the Forescout Administration Guide.

5. Select **Next**.

6. Assign CounterACT devices as follows:

**Enterprise Manager or IP address**

Select Enterprise Manager or an IP address of a connecting CounterACT Appliance to communicate with the targeted FortiManager instance, including requests by other CounterACT Appliances. Specific CounterACT Appliances assigned here cannot be assigned to another server elsewhere.
Assign specific devices | This CounterACT Appliance is assigned to a FortiManager, but it does not communicate with it directly. All communication between FortiManager and its assigned CounterACT Appliance is handled by the connecting CounterACT Appliance defined for the FortiManager. All the IP addresses handled by an assigned Appliance must also be handled by the FortiManager to which the Appliance is assigned.

Assign all devices by default | This is the connecting Appliance to which CounterACT Appliances are assigned by default, if they are not explicitly assigned to another connecting Appliance.

Select this option to make this connecting Appliance the middle man for all CounterACT Appliances not assigned to another connecting device.

If you do not assign specific devices, by default, all devices are assigned to one server. This server becomes known as the Default Server.

7. Select **Next**.

8. Define the Advanced Settings as follows:

   **Maximum number of queries and actions allowed at any given instance** | Select the rate limiting value as follows:

   - Use Default (50)
   - Specify a value from 10 to 200

   The Forescout platform limits the amount of actions sent to this FortiManager connection.

   For an $M$ to one configuration, consider reducing the rate limit assigned to each connection so that the sum of all rate limits for a FortiManager remains equal to the total rate limit.

9. Select **Finish**. The FortiManager is listed in the Fortinet Next-Generation Firewall pane. If there are multiple FortiManagers in a cluster, a starred icon in the **Default** column indicates the default focal Appliance.
10. In the Fortinet Next-Generation Firewall pane, select **Apply**.

The best practice is to perform a **Test** after setting up a connection. See Test a FortiManager Connection.

**Edit a FortiManager Connection**

You can edit the FortiManager connection.

**To edit a FortiManager connection:**

1. In the Fortinet Next-Generation Firewall pane, select the configured FortiManager.

2. Select **Edit**.
3. Edit the settings in the FortiManager Connection, Assign CounterACT Devices, and Advanced Settings tabs, as required.

4. Select OK.

**Test a FortiManager Connection**

Test the FortiManager connection and obtain information from FortiManager, such as its version and serial number.

To test a FortiManager connection:

1. In the Fortinet Next-Generation Firewall pane, select the configured FortiManager and select **Test**. The test results are displayed in the Testing dialog box.

> The test might fail if the connection times out due to an unreachable target or busy system. The best practice is to perform a test while there are not a lot of other actions executing.
2. Obtain the information you need and select **Close**.

**Remove a FortiManager Connection**

You can remove a FortiManager connection. If you remove a FortiManager connection, the connecting CounterACT Appliance assigned to that connection is re-assigned to the default connection.

**To remove a FortiManager connection:**

1. In the Fortinet Next-Generation Firewall pane, select the configured FortiManager and select **Remove**.
2. When prompted for confirmation, select **OK**.
3. In the Fortinet Next-Generation Firewall pane, select **Apply**.

**Add a FortiGate Connection**

Define a connection to FortiGate, including login credentials. Multiple FortiGates can be added.

**To add a FortiGate connection:**

1. In the Console, select **Options** from the **Tools** menu.

2. From the Options pane, select **Fortinet Next-Generation Firewall**.

3. Select the FortiGate tab and then select **Add**.
4. Define the FortiGate connection as follows:

<table>
<thead>
<tr>
<th><strong>FortiGate FQDN or IP Address</strong></th>
<th>Enter the FQDN of FortiGate, or the IPv4 or IPv6 address. You must enter the FQDN if the <strong>Validate Server Certificate</strong> option is selected.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>Enter the username used to access FortiGate.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the password used to access FortiGate.</td>
</tr>
<tr>
<td><strong>Verify Password</strong></td>
<td>Re-enter the password.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>(Optional) Enter text that describes the connection, such as a nickname.</td>
</tr>
</tbody>
</table>
| **Validate Server Certificate**  | Select this option to validate the identity of the third-party server before establishing a connection, when the eyeExtend product communicates as a client over SSL/TLS. To validate the server certificate, either of the following certificate(s) must be installed:  
  ▪ Self-signed server certificate – the server certificate must be installed on the CounterACT Appliance  
  ▪ Certificate Authority (CA) signed server certificate – the CA certificate chain (root and intermediate CA certificates) must be installed on the CounterACT Appliance  
  Use the Certificates > Trusted Certificates pane to add the server certificate to the Trusted Certificate list. For more information about certificates, refer to the appendix, "Configuring the Certificate Interface" in the *Forescout Administration Guide*. |

5. Select **Next**.
6. Assign CounterACT devices as follows:

| Enterprise Manager/IP address | Select Enterprise Manager or an IP address of a connecting CounterACT Appliance that will communicate with the targeted FortiGate instance, including requests by other CounterACT Appliances. Specific CounterACT Appliances assigned here cannot be assigned to another server elsewhere. |
| Assign specific devices | This CounterACT Appliance is assigned to a FortiGate, but it does not communicate with it directly. All communication between FortiGate and its assigned CounterACT Appliance is handled by the connecting CounterACT Appliance defined for the FortiGate. All IP addresses handled by an assigned Appliance must also be handled by the FortiGate to which the Appliance is assigned. |

- Select Available Devices and then select an item in the Available Devices list.
- Select Add. The selected device sends its requests to the FortiGate through the connecting Appliance.
Assign all devices by default

This is the connecting Appliance to which CounterACT Appliances are assigned by default, if not explicitly assigned to another connecting Appliance.

Select **Assign all devices by default** to make this connecting Appliance the middle man for all CounterACT Appliances not assigned to another connecting device.

If you do not assign specific devices, by default, all devices are assigned to one server. This server becomes known as the Default Server.

### 7. Select Next.

### 8. Define the Advanced Settings as follows:

<table>
<thead>
<tr>
<th>Maximum number of queries and actions allowed at any given instance</th>
<th>Select the rate limiting value as follows:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Use Default (100)</td>
</tr>
<tr>
<td></td>
<td>• Specify a value from 10 to 200</td>
</tr>
</tbody>
</table>

The Forescout platform limits the amount of actions sent to this FortiGate connection.

For an $M$ to one configuration, consider reducing the rate limit assigned to each connection so that the sum of all rate limits for a FortiGate remains equal to the total rate limit.

### 9. Select **Finish**. The FortiGate is listed in the Fortinet Next-Generation Firewall pane. A starred icon in the Fortinet Next-Generation Firewall pane indicates the default focal Appliance.

### 10. In the Fortinet Next-Generation Firewall pane, select **Apply**.
The best practice is to perform a Sync after setting up a FortiGate connection. See Sync a FortiGate Connection. Then perform a Test. See Test a FortiGate Connection.

**Sync a FortiGate Connection**

You can synchronize the connection and obtain information about VDOMs. The VDOM information is used when defining actions. See Policy Actions.

**To sync a FortiGate connection:**

1. In the Fortinet Next-Generation Firewall pane, select the configured FortiGate and select Sync. The sync results are displayed in the Syncing dialog box.

   ![Syncing dialog box](image)

   *Login successful*
   *List of vdoms: VDOM-E1, VDOM-E2, VDOM-E3, VDOM-QA, VDOM-RCD, root*
   *Fortigate retrieval of VDOM is successful*

2. Obtain the information you need and select Close.
3. In the Fortinet Next-Generation Firewall pane, select Apply to make the VDOM information available for use in a policy.

**Edit a FortiGate Connection**

You can edit a FortiGate connection.

**To edit a FortiGate connection:**

1. In the Fortinet Next-Generation Firewall pane, select the configured FortiGate.
2. Select **Edit**.

3. Edit the settings in the FortiGate Connection, Assign CounterACT Devices, and Advanced Settings tabs, as required.

4. Select **OK**.

**Test a FortiGate Connection**

Test the FortiGate connection and obtain information from FortiGate, such as its version and serial number. This information is used when defining an action.
To test a FortiGate connection:

1. In the Fortinet Next-Generation Firewall pane, select the configured FortiGate and select Test. The test results are displayed in the Testing dialog box, as well as the firewall deployment mode (standalone or HA).

   ![Testing dialog box]

   *The test might fail if the connection times out due to an unreachable target or busy system. The best practice is to perform a test while there are not a lot of other actions executing.*

2. Obtain the information you need and select Close.

Remove a FortiGate Connection

You can remove a FortiGate connection. If you remove a FortiGate connection, the connecting CounterACT Appliance assigned to that connection is re-assigned to the default connection.

To remove a FortiGate connection:

1. In the Fortinet Next-Generation Firewall pane, select the configured FortiGate and select Remove.
2. When prompted for confirmation, select OK.
3. In the Fortinet Next-Generation Firewall pane, select **Apply**.

## Create Custom Policies

Use custom policies on either FortiManager or FortiGate to create an **Add to Address Group** action. There are no default policy templates for FortiManager or FortiGate.

### Create a Custom Policy

This section describes how to create a custom policy for FortiManager or FortiGate.

**To create a custom policy:**

1. Log in to the Console and select **Policy**.

2. Select **Add**.
3. Select **Custom** and then select **Next**.
4. Enter a name for the policy. Optionally, enter a description. Select Next. Both the Scope pane and the IP Address Range dialog box open.

5. Use the IP Address Range dialog box to define which endpoints are inspected.

The following options are available:

- **All IPs**: Include all IP addresses in the Internal Network.
- **Segment**: Select a previously defined segment of the network. To specify multiple segments, select OK or Cancel to close this dialog box, and select Segments from the Scope pane.
- **Unknown IP addresses**: Apply the policy to endpoints whose IP addresses are not known. Endpoint detection is based on the endpoint MAC address.

6. Select OK. The added range is displayed in the Scope pane.
7. Select **Next**.

Policy rules instruct the Forescout platform how to detect and handle devices defined in the policy scope.

- Hosts that match the Main Rule are included in the policy inspection. **Hosts that do not match this rule are not inspected for this policy.** Sub-rules automatically follow up with hosts after initial detection and handling, streamlining separate detection and actions into one automated sequence.

- Sub-rules are performed in order until a match is found. When a match is found, the corresponding action is applied to the host. If the host does not match the requirements of the sub-rule, it is inspected by the next rule.
8. To add a condition, select **Add** in the Condition section. See Policy Properties.

9. To add an action, select **Add** in the Actions section. See Policy Actions.

10. In the Main Rule pane, select **Finish**.

11. In the Policy Manager, select **Apply**.

**Policy Properties**

Use policy properties to select appropriate conditions for the policy you are creating. For example, you can select devices classified with Windows 7 Operating System.

Conditions are optional, but are recommended to filter the policy scope. Many conditions are available for inclusion in a custom policy. There are no conditions specific to Fortinet.

**To access policy properties:**

1. Expand the Properties tree in the Policy Conditions dialog box.
2. In a custom policy, many conditions are available to select. For example, select devices classified with Windows 7 Operating System or another condition you want to use.

3. Select OK. The condition is displayed in the Policy Wizard.

Policy Actions

Use policy actions to perform an action for the policy you are creating. The procedure in this section is for FortiGate.

For more information on the FortiGate action, see Manually Run FortiGate Action.

For more information on the FortiManager action, see Manually Run FortiManager Action.

To access policy actions:

1. Expand the Fortinet Next-Generation Firewall folder in the Actions tree of the Policy Actions dialog box.
2. Select **Add to Address Group**.
3. In the Parameters tab of the Actions dialog box, define the parameters for the action as follows:

<table>
<thead>
<tr>
<th>Address Group</th>
<th>Enter the name of one or more address groups, obtained from Fortinet. Address group names are case-sensitive. Enter multiple address groups by separating them with a comma. For example: my_ipv4_addressgroup1,my_ipv4_addressgroup2. The same name of an address group, such as Test, can be under both IPv4 and IPv6, but they are treated as two separate address groups. IPv4 addresses are added to IPv4 address groups. IPv6 addresses are added to IPv6 address groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDOM</td>
<td>Select one VDOM for each action.</td>
</tr>
</tbody>
</table>
| Specify one or more Firewalls | Select one of the following:  
  • **Send to all firewalls** – Sends the action to all firewalls  
  • **Send to specific firewalls** – Sends the action to one or more selected firewalls |

4. If you selected **Send to specific firewalls**, the Specify one or more Firewalls dialog box opens. Otherwise, go to step 7.

5. Select one or more firewalls and select **OK**.

6. To schedule the action, select the Schedule tab in the Action dialog box.
7. For the Action Schedule, select one of the following:

<table>
<thead>
<tr>
<th>Start action when the endpoint matches a policy condition</th>
<th>Implements the policy when the policy condition(s) is met by the endpoint.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize action start time</td>
<td>Opens the Action Scheduler dialog box.</td>
</tr>
</tbody>
</table>

8. If you selected **Customize action start time**, the Action Scheduler dialog box opens. Otherwise, go to step 11.

9. Set the schedule parameters and select **OK**.
10. In the Main Rule pane, select **Finish**.
11. Select **Apply**.

**Manually Run FortiManager Action**

While a FortiManager action can be launched as part of a policy, you can also manually run an action.

**To manually run a FortiManager action:**

1. Log in to the Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, right-click an endpoint and select **Fortinet Next-Generation Firewall**, and then select an action.
3. Select the **Add to Address Group** action.

4. In the Parameters tab, configure the action as follows:

| **Address Group** | Enter the name of one or more address groups, obtained from Fortinet. Address group names are case-sensitive. Enter multiple address groups by separating them with a comma. For example, my_ipv4_addressgroup1,my_ipv4_addressgroup2. The same name of an address group, such as Test, can be under both IPv4 and IPv6, but they are treated as two separate address groups. IPv4 addresses are added to IPv4 address groups. IPv6 address are added to IPv6 address groups. |
| **Package**     |  |
Enter one package for each action. You need to obtain the package name from FortiManager. The package name is case-sensitive. Within the package is information about preconfigured address groups and installation targets.

To find a package in FortiManager, go to **Policy & Objects > Policy Packages** and select a package.

5. In the Specify Add to Address Group parameters dialog box, select **OK**. An action icon is displayed for an endpoint in the Policy Manager pane. Hover over the icon to view tooltip information, including the status of the action.

Note the following behaviors:

- The **Add to Address Group** action adds a `Forescout_Integration_Do_Not_Remove` object in the Details column in IPv4 and IPv6 address groups, deleting the `none` object (if it exists). In FortiManager, go to Policy & Objects > Object Configurations > Firewall Objects, and select Addresses.
By default, configuration from FortiManager to FortiGate is pushed at four-minute intervals. All policy packages containing address groups updated in the previous four minutes are pushed to their respective, pre-configured installation targets.

**Manually Run FortiGate Action**

While a FortiGate action can be launched as part of a policy, you can also manually run an action.

**To manually run a FortiGate action:**

1. Log in to the Console, select **Home**, and select **All Hosts**.

2. In the All Hosts pane, right-click an endpoint and select **Fortinet Next-Generation Firewall**, and then select an action.

3. Select the **Add to Address Group** action.
4. In the Parameters tab, configure the action, as follows:

<table>
<thead>
<tr>
<th><strong>Address Group</strong></th>
<th>Enter the name of one or more address groups, obtained from Fortinet. Address group names are case-sensitive. Enter multiple address groups by separating them with a comma. For example, my_ipv4_addressgroup1,my_ipv4_addressgroup2. The same name of an address group, such as Test, can be under both IPv4 and IPv6, but they are treated as two separate address groups. IPv4 addresses are added to IPv4 address groups. IPv6 address are added to IPv6 address groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VDOM</strong></td>
<td>Select one VDOM for each action. Use Sync to obtain VDOM information. See Sync a FortiGate Connection.</td>
</tr>
</tbody>
</table>
| **Specify one or more Firewalls** | Select one of the following:  
  - **Send to all firewalls** – Sends the action to all firewalls  
  - **Send to specific firewalls** – Sends the action to one or more selected firewalls |

To find a VDOM in FortiGate, select **Global** and select a VDOM.
5. In the Specify Add to Address Group parameters dialog box, select **OK**. An action icon is displayed for an endpoint in the Policy Manager pane. Hover over the icon to view tooltip information, including the status of the action.

Note the following behavior:

- The **Add to Address Group** action adds a Forescout_Integration_Do_Not_Remove object in the Details column in IPv4 and IPv6 address groups, deleting the **none** object (if it exists). In FortiGate, select a VDOM, select Policy & Objects, and select Addresses.

**Set Action Thresholds**

Action thresholds restrict the number of actions. They are designed to automatically implement safeguards. An action threshold is the maximum percentage of endpoints that can be controlled by a specific action type defined at a single device.
The **Add to Address Group** actions have a default 5% action threshold, which can be scaled up to 100%.

For information about action thresholds, refer to the *Forescout Administration Guide*.

**To change an action threshold:**

1. In the **Options** tree, expand **NAC** and select **Actions Thresholds**.

2. In Actions table, select **Add to Address Group**.

3. Below the Actions table, select the Configuration tab.

4. Select **Custom**, and enter a value in the field.

5. Select **Apply**.

**Remove an Action**

This section describes how to remove an action.

**To remove an action:**

1. In the Console, select **Home > All Hosts**.

2. In the All Hosts pane, right-click an endpoint that has a configured Fortinet action.
3. Select **Cancel Actions > Remove from Address Group** from the Actions menu.

4. When prompted for confirmation, select **Yes**.

**Policy Action Details**

This section describes how to view detailed information on a policy action. This information is helpful when an action fails and you want to determine the kind of address that failed, IPv4 or IPv6.

**To view details on a policy action:**

1. In the Console, select **Home**.
2. Under Views, locate the Fortinet policies.

3. Double-click an endpoint that has a configured Fortinet action. The Host Details pane opens.

4. In the Host Details pane, select the Policy Actions tab and view the Problems column. A red icon in the **Actions** column indicates an action failure.
The Policy Actions tab displays the result of the last action only. If there are multiple **Add to Address Group** actions on a single endpoint, the Problems column only displays the status of the last action.

5. Select **Close**.

**Start or Stop a Custom Policy**

This section describes how to start or stop a custom policy. There are also options to start or stop all policy actions.

**To start or stop a custom policy:**

1. In the Console, select **Home**.
2. In Views, locate the Fortinet policies.
3. To start a policy, right-click on a non-running policy and select **Start Policy**.

4. To stop a policy, right-click on a running policy and select **Stop Policy**.

5. To stop all policy actions, select **Stop Policy Actions**.

**Best Practices**

The best practices for Forescout eyeExtend for Fortinet NGFW are as follows:

- Define a user account on Fortinet with read-write privileges.
- Perform a **Sync** after setting up a FortiGate connection. See [Add a FortiGate Connection](#) and [Sync a FortiGate Connection](#).
- Perform a **Test** after setting up a connection. Also, perform a **Test** while there are not a lot of other actions executing. See [Test a FortiManager Connection](#) and [Test a FortiGate Connection](#).

**Additional Forescout Documentation**

For information about other Forescout features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [Forescout Help Tools](#)
Documentation Downloads

Documentation downloads can be accessed from the Forescout Technical Documentation Page, and one of two Forescout portals, depending on which licensing mode your deployment is using.

- Per-Appliance Licensing Mode – Product Updates Portal
- Flexx Licensing Mode – Customer Support Portal

Software downloads are also available from these portals.

To identify your licensing mode:
- From the Console, select Help > About Forescout.

Forescout Technical Documentation Page

The Forescout Technical Documentation Page provides access to a searchable, web-based Documentation Portal as well as PDF links to the full range of technical documentation.

To access the Technical Documentation Page:
- Go to https://www.Forescout.com/company/technical-documentation/

Product Updates Portal

The Product Updates Portal provides links to Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:
- Go to https://updates.forescout.com/support/index.php?url=counteract and select the version you want to discover.

Customer Support Portal

The Downloads page on the Forescout Customer Support Portal provides links to purchased Forescout version releases, Base and Content Modules, and eyeExtend products, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software.

To access documentation on the Customer Support Portal:
- Go to https://Forescout.force.com/support/ and select Downloads.

Documentation Portal

The Forescout Documentation Portal is a searchable, web-based library containing information about Forescout tools, features, functionality, and integrations.

To access the Documentation Portal:
- Go to https://updates.forescout.com/support/files/counteract/docs_portal/
**Forescout Help Tools**
Access information directly from the Console.

**Console Help Buttons**
Use context sensitive Help buttons to quickly access information about the tasks and topics you are working with.

**Forescout Administration Guide**
- Select **Administration Guide** from the Help menu.

**Plugin Help Files**
- After the plugin is installed, select **Tools > Options > Modules**, select the plugin and then select Help.

**Documentation Portal**
- Select **Documentation Portal** from the Help menu to access the Documentation Portal.