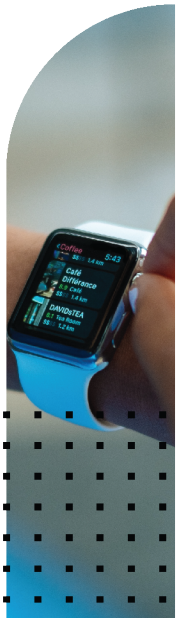
Administration Guide

Policy Analyzer MEA 1.0.0 Beta



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

FORTINET TRAINING 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

June 6, 2023
Policy Analyzer MEA 1.0.0 Beta Administration Guide
02-100-750937-20230606

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-10-20	Initial release of 1.0.0 Beta.
2021-10-22	Clarified the result of *Block malicious traffic* mode. Even though malicious traffic is leaned on a specific port, the policy block generated by Policy Analyzer MEA will block malicious traffic on all FortiGate interfaces. See Key concepts on page 5.
2022-03-31	Updated to support changes in FortiOS 7.2.0 and later. See Configuring FortiGate on page 9.
2023-06-06	Updated *JSON API Access* setting in FortiAnalyzer. See Configuring FortiAnalyzer on page 14.

Introduction

When enabled, Policy Analyzer MEA is installed on FortiManager. Policy Analyzer is a management extension application (MEA) that is released and signed by Fortinet to run on FortiManager.

You must be in ADOM version 7.0 or later to access Policy Analyzer MEA.

Policy Analyzer MEA is an automated tool with a wizard. It works with Security Policies in learn mode from a managed FortiGate to analyze logs sent to FortiAnalyzer. Based on the analyzed traffic, administrators can choose to automatically create a policy block to:

- Block malicious traffic
- Allowed learned traffic - permissive mode
- Allowed learned traffic - restricted mode

A policy block is automatically created and inserted in the policy package, and the policy package is installed to the target FortiGate.

Requirements

In order to use Policy Analyzer MEA, you must have the following products:

- FortiGate running FortiOS 7.0.2 or later
- FortiAnalyzer 7.0.2 or later
- FortiManager 7.0.2 or later
  - ADOM version 7.0 or later
  - FortiManager must manage FortiGate.
  - FortiManager must be able to communicate with FortiAnalyzer by its IP address, and the FortiManager administrator requires valid FortiAnalyzer credentials to authorize access to the logs.

Key concepts

This section describes the following key concepts for using Policy Analyzer MEA:

- Device and logging requirements on page 6
- Policy Analyzer wizard process on page 6
- Types of policies generated by Policy Analyzer wizard on page 6

Device and logging requirements

FortiGate must have NGFW set to policy-based and be configured to use a Security Policy with Learn Mode enabled. FortiGate must also send the logs to FortiAnalyzer. Allow the Security Policy to run for several days to generate traffic for analysis.

FortiGate must be managed by FortiManager in a version 7.0 or later ADOM, with a synchronized configuration status. FortiManager must have Policy Analyzer MEA enabled.

FortiManager must be able to communicate with FortiAnalyzer by its IP address, and the FortiManager administrator requires valid FortiAnalyzer credentials to authorize access to the logs.

Policy Analyzer wizard process

In Policy Analyzer MEA, you use a wizard to identify what FortiGate, FortiAnalyzer, and Security Policy to use for traffic analysis. Policy Analyzer MEA analyzes the traffic, and presents you with several options to handle the traffic. You choose an option, and Policy Analyzer MEA automatically creates a policy block. Policy Analyzer MEA also works with FortiManager to automatically insert the policy block into the Security Policy, and install the updated policy package to FortiGate.

You cannot edit the policy block in Policy Analyzer MEA. However after the policy block is automatically installed to the FortiGate, you can edit the policy block on the *FortiManager* > *Policy & Objects* pane, and then install the changes to FortiGate.

Types of policies generated by Policy Analyzer wizard

When using Policy Analyzer MEA wizard, you can choose one of the following modes:

- Block malicious traffic
- Allowed learned traffic - permissive mode
- Allowed learned traffic - restricted mode

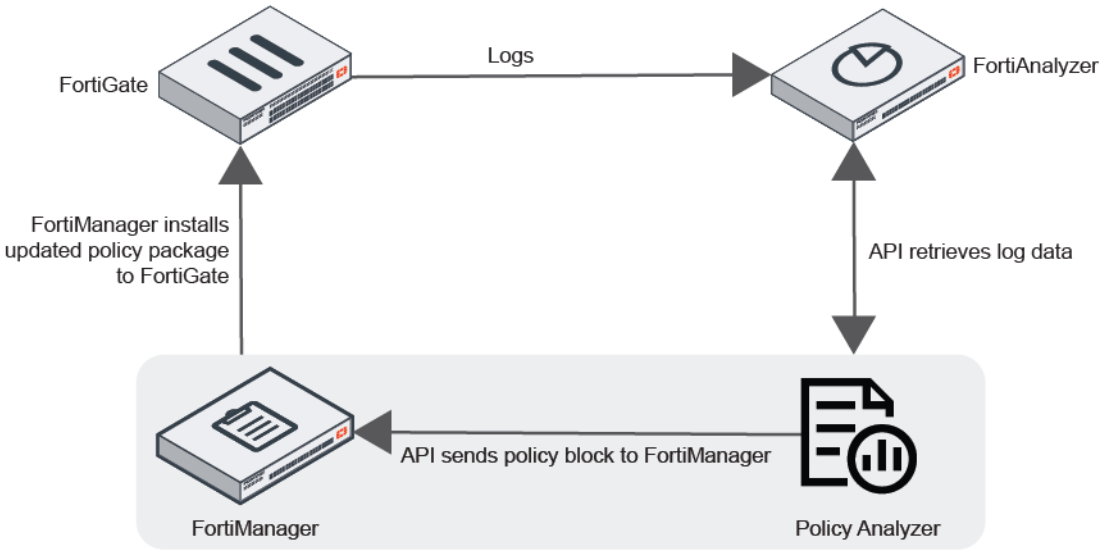
Both *Allow learned traffic* modes also generate an implicit policy, and you must specify whether the implicit policy accepts or denies all traffic.

After you choose a mode, Policy Analyzer MEA automatically generates policies based on the selected mode. The following table summarizes the modes:

Mode	Description	Implicit Policy Generated?
Block malicious traffic	When the Policy Analyzer MEA wizard detects malware and applications rated high-risk, you can select the *Block Malicious Traffic* mode to create a policy block that will block the traffic on the FortiGate. Even though malicious traffic is leaned on a specific port, the policy block generated by Policy Analyzer MEA will block malicious traffic on all FortiGate interfaces.	No
Allowed learned traffic - permissive mode	You can use the *Allow Learned Traffic - Permissive Mode* setting to combine and allow traffic learned from different users and their detected applications. This method is based on Least Common Multiple concept. The wizard automatically creates a policy block with one policy to allow this traffic, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.	Yes, and you choose whether the implicit policy denies or allows all traffic.
Allowed learned traffic - restricted mode	You can use the *Allow Learned Traffic - Restricted Mode* setting to allow the traffic learned for each user with their specific applications only. This method is based on Largest Common Denominator concept. The Policy Analyzer wizard automatically creates a policy block with one policy for each distinctive user, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.	Yes, and you choose whether the implicit policy denies or allows all traffic.

How Policy Analyzer MEA works with FortiManager

Once FortiGate, FortiAnalyzer, FortiManager, and Policy Analyzer MEA are configured, FortiGate sends logs to FortiAnalyzer. Policy Analyzer uses the API to retrieve log data from FortiAnalyzer, and to provide policy changes to FortiManager for installation on the FortiGate.



FortiManager with Policy Analyzer

Quick start

This section provides a summary of how to get started with Policy Analyzer MEA:

1. On FortiGate, configure FortiOS to provide logs for Policy Analyzer MEA to use. See Configuring FortiGate on page 9.
2. On FortiAnalyzer, configure an administrative account to use with Policy Analyzer MEA. See Configuring FortiAnalyzer on page 14.
   The administrative account must have JSON API set to a minimum of Read to enable API communication between the products.
3. On FortiManager, add FortiGate for management, and import policy packages. See Adding FortiGate to FortiManager on page 14.
4. On FortiManager, enable Policy Analyzer MEA. See Enabling Policy Analyzer MEA on page 15.
   Policy Analyzer MEA is downloaded from Fortinet Registry and installed on FortiManager.
5. Open Policy Analyzer MEA. See Opening Policy Analyzer MEA on page 15.
6. Use the Policy Analyzer wizard to analyze FortiGate traffic logs, and choose a mode for handling the traffic. See Policy Analyzer modes on page 17.
   Policy Analyzer MEA automatically generates a policy block, inserts the policy block into the policy, and initiates installation of the updated policy package to FortiGate.

Configuring FortiGate

FortiGate must be configured with a Security Policy that has Learn Mode enabled. The Security Policy allows all services from all source and destination ports and logs all traffic for analysis. Learn Mode uses a special prefix in the `policymode` and `profile` fields in traffic and UTM logs for use by FortiAnalyzer and Policy Analyzer MEA. After configuring FortiGate, allow the device to run for several days to capture traffic in logs.

The following FortiGate limitations apply when Learn Mode is enabled in a Security Policy:

- Only interfaces with `device-identification enable` can be used as source interfaces in a Security Policy with Learn Mode enabled.
- Incoming and outgoing interfaces do not support `any`.
- Internet service is not supported.
- NAT46 and NAT64 are not supported.
- Users and groups are not supported.
- Some negate options are not supported.

The logs are sent to FortiAnalyzer, and then used by Policy Analyzer MEA to learn about the traffic needs of the FortiGate.

Following is an overview of how to configure FortiGate:

1. Set NGFW to policy-based. See Setting NGFW to policy-based on page 10.
2. Configure a Security Policy with Learn Mode enabled.
   - For FortiOS 7.2.0 and later, see Configuring a Security Policy with Learn Mode enabled (7.2) on page 10.
   - For FortiOS 7.0.2 to 7.0.x, see Configuring a Security Policy with Learn Mode enabled (7.0) on page 11.

3. Enable logging to FortiAnalyzer. See Enabling logging to FortiAnalyzer on page 13.

Although this section describes how to use FortiOS to configure FortiGate, you can also use FortiManager to configure FortiGate for Policy Analyzer MEA.

Setting NGFW to policy-based

On the FortiGate, NGFW must be set to policy-based.

To set NGFW to policy-based:

1. Go to *System* > *Settings*.
2. Set *NGFW Mode* to *Policy-based*, and click *Apply*.

Configuring a Security Policy with Learn Mode enabled (7.2)

On the FortiGate, a Security Policy must be configured with Learn Mode enabled to provide the information that Policy Analyzer MEA requires to analyze traffic in logs.

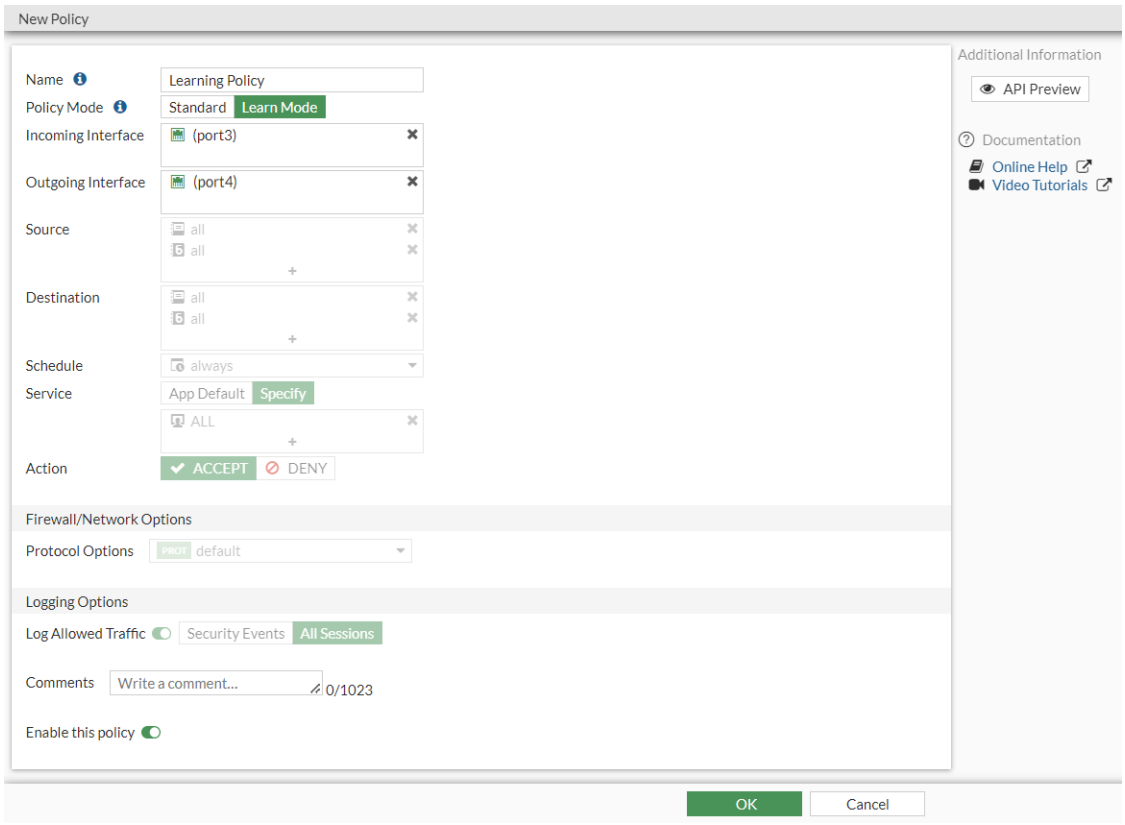
Starting with FortiOS 7.2.0, you can enable Learn Mode in the GUI. In earlier releases of FortiOS, you must use the CLI to enable `learning-mode` after creating a Security Profile.

```
config firewall security-policy
   edit <policy name>
   set learning-mode enable
end
```

To configure a Security Policy with Learn Mode enabled:

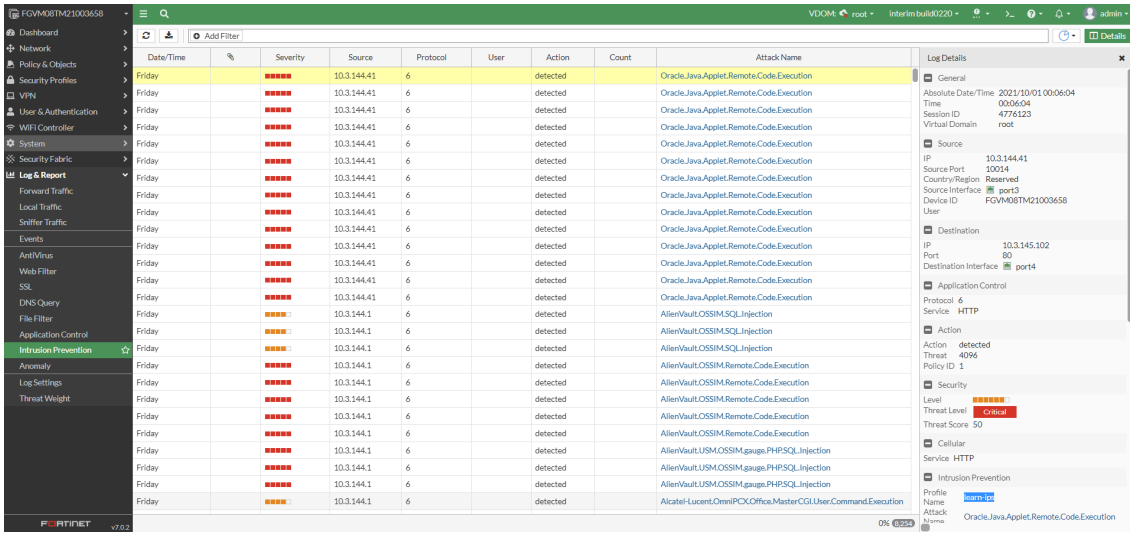
1. Enable advanced policy options.
   a. Go to *System* > *Feature Visibility*.
   b. In the *Additional Features* column, toggle on *Policy Advanced Options*, and click *Apply*.
   Advanced policy options are enabled.
2. Create a Security Policy.
   a. Go to *Policy & Objects* > *Security Policy*, and click *Create New*.
   b. Set the following options:

Name	Type a name, such as *Learning Policy*.
Policy Mode	Select *Learn Mode*.
Incoming Interface	Select a port.
Outgoing Interface	Select a port.



c. Click *OK*.
A Security Policy is created.

A Security Policy with Learn Mode enabled automatically sets the action for all Security Policies to *Monitor Only*.



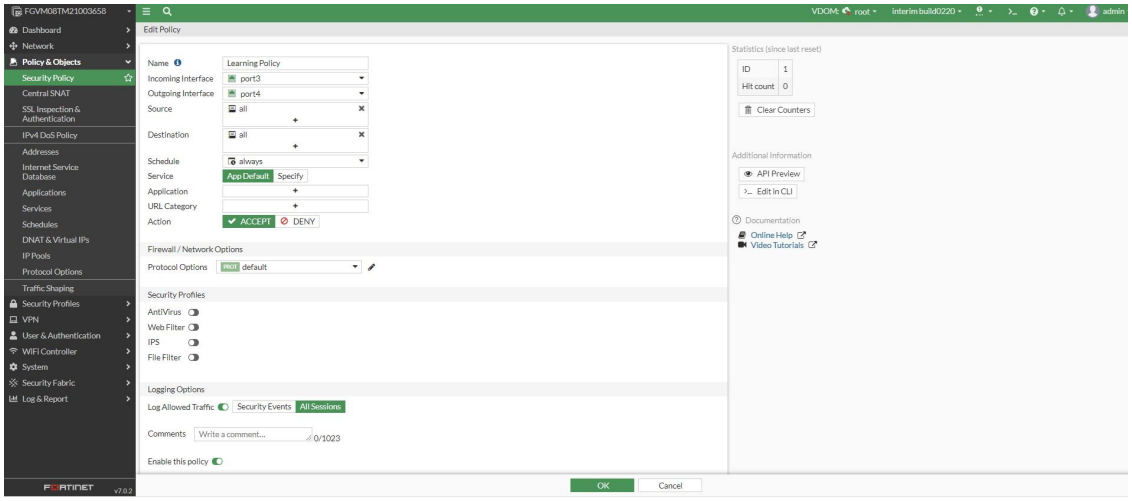
Configuring a Security Policy with Learn Mode enabled (7.0)

On the FortiGate, a Security Policy must be configured with Learn Mode enabled to provide the information that Policy Analyzer MEA requires to analyze traffic in logs.

To configure a Security Policy with Learn Mode enabled:

1. Enable advanced policy options.
   a. Go to *System* > *Feature Visibility*.
   b. In the *Additional Features* column, toggle on *Policy Advanced Options*, and click *Apply*.
   Advanced policy options are enabled.
2. Create a Security Policy.
   a. Go to *Policy & Objects* > *Security Policy*, and click *Create New*.
   b. Set the following options:

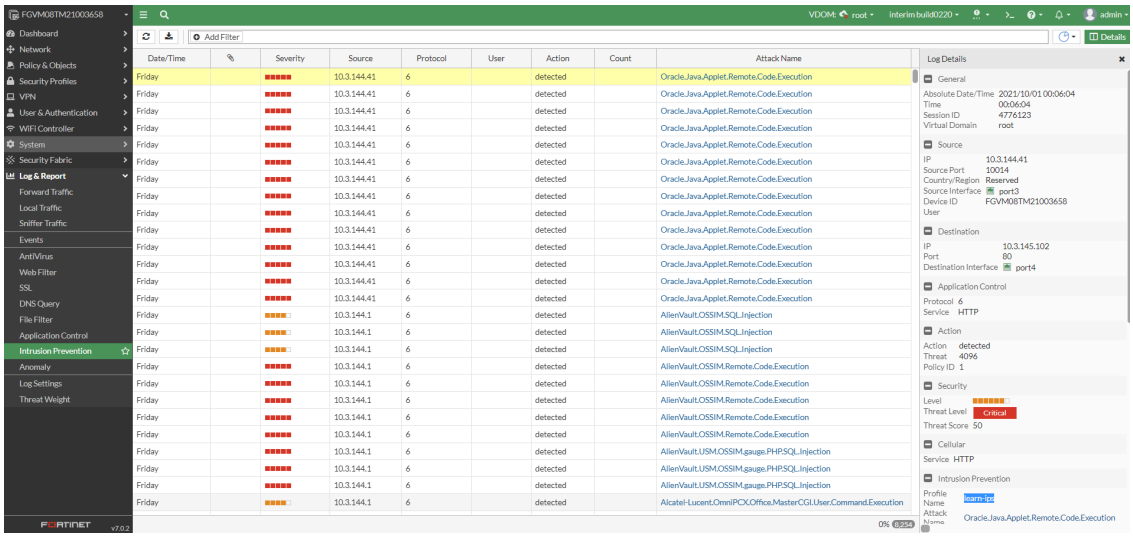
Name	Type a name, such as *Learning Policy*.
Incoming Interface	Select a port.
Outgoing Interface	Select a port.
Source	Select *all*.
Destination	Select *all*.



   c. Use the default settings for the remaining options, and click *OK*.
   A Security Policy is created.
3. Edit the Security Policy to enable `learning-mode` by using the CLI.

```
config firewall security-policy
   edit <policy name>
   set learning-mode enable
end
```

A Security Policy with Learn Mode enabled automatically sets the action for all Security Policies to *Monitor Only*.

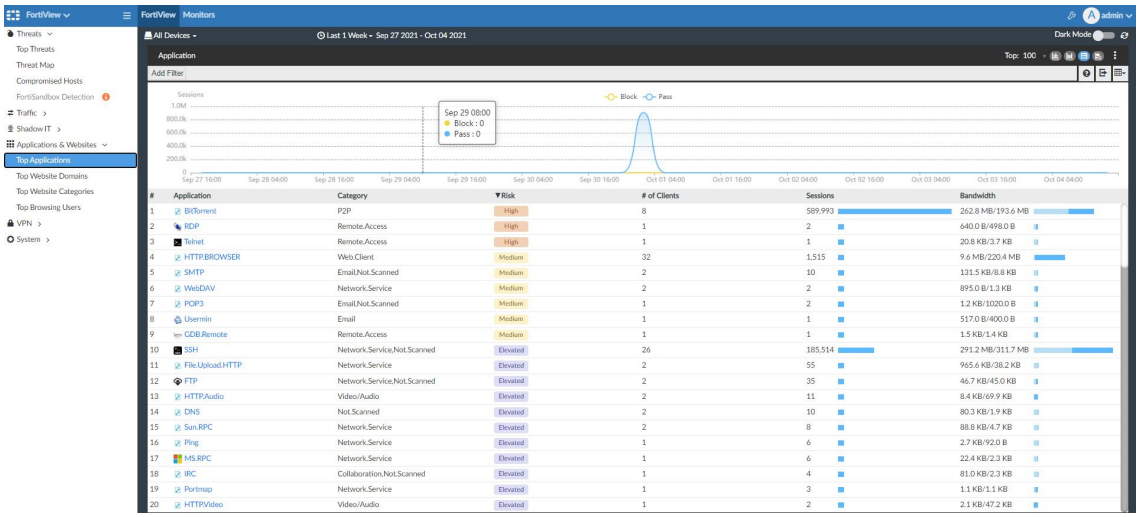


Enabling logging to FortiAnalyzer

FortiGate must be configured to send logs to FortiAnalyzer. Policy Analyzer MEA will retrieve log data from FortiAnalyzer.

To enable logging to FortiAnalyzer:

1. In FortiAnalyzer, configure the authorization address and port.
   a. Go to *System Settings* > *Admin* > *Admin Settings*.
   b. In the *Fabric Authorization* section, enter an *Authorization Address* and *Authorization Port*. FortiOS uses this information to access the FortiAnalyzer login screen.
2. In FortiOS, go to *Security Fabric* > *Fabric Connectors*, and double-click the *FortiAnalyzer Logging* card.
3. In the Server box, type the FortiAnalyzer IP, and click *OK*. The *FortiAnalyzer Status* (in the right-side gutter) is *Unauthorized*.
4. Click *Authorize*. You are redirected to a login screen.
5. Enter the username and password, and click *Login*.
6. Select *Approve*, and click *OK* to authorize the FortiGate.
7. In FortiOS, refresh the *FortiAnalyzer Logging* page. The *FortiAnalyzer Status* is *Authorized*.
8. In FortiAnalyzer, go to *FortiView* > *Applications & Websites* > *Top Applications* to view log details.
   The following example identifies top applications and whether the risk level for the application is *High*, *Medium*, or *Elevated*.



Configuring FortiAnalyzer

FortiGate is configured to send logs to FortiAnalyzer.

When using Policy Analyzer MEA, you must log in to FortiAnalyzer to authorize use of the logs, and the administrative account must have JSON API access set to Read-Write to enable API communication between the products.

This section describes how to configure an administrator account to use with Policy Analyzer MEA.

In Policy Analyzer MEA, you specify a date range of log data to analyze. It's recommended to check your log storage policies in FortiAnalyzer to ensure log data is available in the database for the timeframe you would like to analyze.

To configure FortiAnalyzer:

1. Go to *System Settings* > *Admin* > *Administrators*.
2. Double-click the administrator account to open it for editing.
   Alternately you can create a new account for use with Policy Analyzer MEA.
3. Beside *JSON API Access*, select *Read-Write*.
4. Configure the remaining options as desired, and click *OK*.

Adding FortiGate to FortiManager

FortiGate must be managed by FortiManager to work with Policy Analyzer MEA. You must also import policy packages from FortiOS to FortiManager. You can import policy packages as part of using the *Add Device* wizard. Alternately you can import policy packages after you complete the wizard.

Policy Analyzer MEA automatically adds a policy block to the Security Policy in the policy package, so you must import the policy package to enable updates to it by FortiManager and Policy Analyzer MEA.

FortiManager must be synchronized with FortiGate to work with Policy Analyzer MEA.

To add FortiGate to FortiManager:

1. In FortiOS, configure the authorization address and port by using the following commands.
```
config system global
   set management-ip
   set management-port
```
2. In FortiManager, ensure you are in a 7.0 or later ADOM.
   FortiGate must be running FortiOS 7.0.2 or later to work with Policy Analyzer MEA.
3. Go to *Device Manager* > *Device & Groups*, and click *Add Device*. The wizard opens.
4. Click *Discover Device*.
5. In the box, type the management port IP address for the device, and click *Next*.
6. Continue following the steps in the wizard, and select the *Import Policy Package* option when available.
7. Complete the wizard to finish adding the device.
   FortiGate is managed by FortiManager, and the policy package for the device is imported to FortiManager.

Enabling Policy Analyzer MEA

You must enable Policy Analyzer MEA before you can use it. FortiManager provides access to Policy Analyzer MEA that is released and signed by Fortinet.

Only administrators with a *Super_User* profile can enable management extension applications.

A CA certificate is required to install management extension applications on FortiManager.

To enable Policy Analyzer MEA in the GUI:

1. Ensure you are using a 7.0 or later ADOM.
2. Go to *Management Extensions*, and click the grayed out tile for Policy Analyzer to enable the application.
   Grayed out tiles represent disabled Fortinet management extension applications.
   A confirmation dialog box is displayed.
3. Click *OK* to confirm.
   Policy Analyzer MEA is installed and enabled. It may take some time to install the application.

To enable Policy Analyzer MEA in the CLI:

```
config system docker
   set policyanalyzer enable
end
```

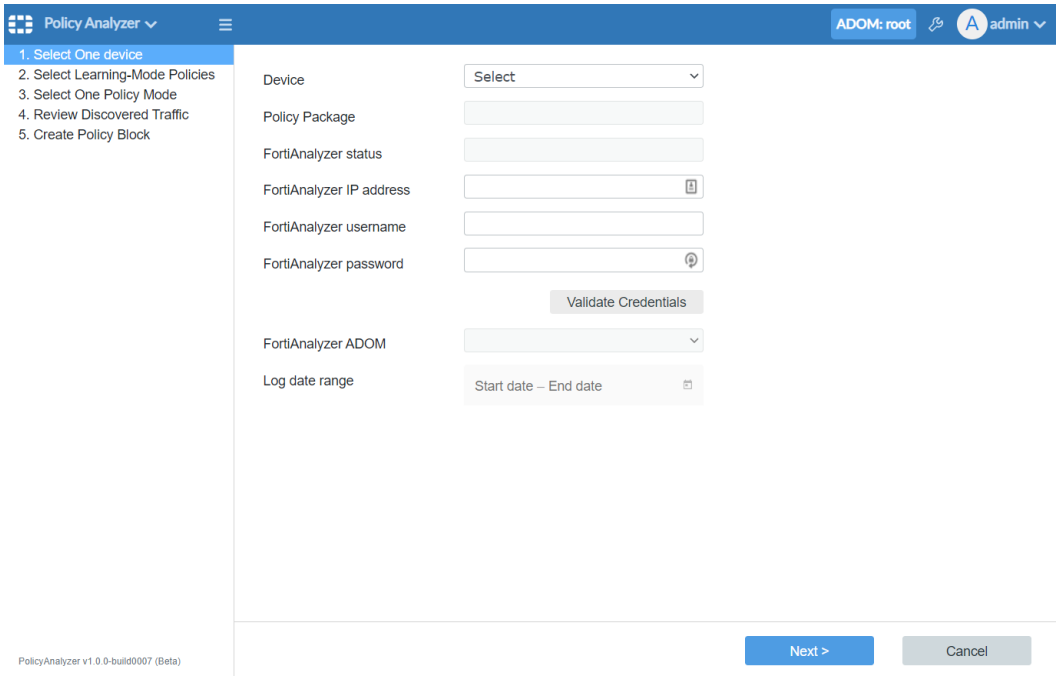
Opening Policy Analyzer MEA

After you enable Policy Analyzer MEA on FortiManager, you can open the MEA and use it.

To open Policy Analyzer MEA:

1. On FortiManager, ensure that Policy Analyzer MEA is enabled. See Enabling Policy Analyzer MEA on page 15.
2. If ADOMs are enabled, ensure you are in the correct ADOM.
   Policy Analyzer MEA requires ADOM version 7.0 or later.
3. In FortiManager, go to *Management Extensions*, and click *Policy Analyzer*.

Policy Analyzer opens.



4. Use the Policy Analyzer wizard to select one of the Policy Analyzer modes. See Policy Analyzer modes on page 17.

Policy Analyzer modes

This section provides examples of how to use the following Policy Analyzer MEA modes to create policies:

- Block malicious traffic. See Blocking malicious traffic on page 17.
- Allow learned traffic with permissive mode. See Allowing learned traffic with permissive mode on page 20.
- Allow learned traffic with restricted mode. See Allowing learned traffic with restrictive mode on page 23.

Blocking malicious traffic

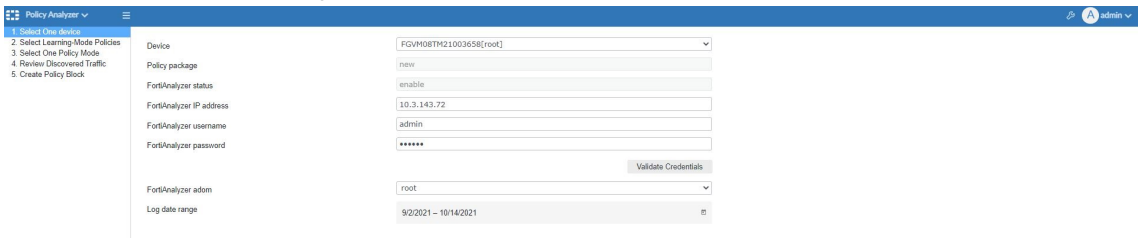
This example describes how to use Policy Analyzer MEA to create a policy block that blocks malicious traffic on FortiGates.

When the Policy Analyzer MEA wizard detects malware and applications rated high-risk, you can select the *Block Malicious Traffic* mode to create a policy block that will block the traffic on the FortiGate. Even though malicious traffic is leaned on a specific port, the policy block generated by Policy Analyzer MEA will block malicious traffic on all FortiGate interfaces.

For example, Policy Analyzer wizard can learn of a high-risk application on source port 1. When you select *Block Malicious Traffic* mode, Policy Analyzer creates a policy block that blocks high-risk applications for all ports. High-risk applications are not blocked only on the port used to learn traffic.

To block malicious traffic:

1. Open Policy Analyzer MEA to access the first step in the wizard.
   Policy Analyzer opens, and the first pane of the wizard is displayed. The name of the first pane is *1. Select One device*.
2. On the *1. Select One device* pane, select a FortiGate.



Option	Description
Device	Select a managed FortiGate that uses a Security Policy with Learn Mode enabled.
Policy package	After selecting a FortiGate, the policy package for the selected FortiGate is displayed.
FortiAnalyzer status	Displays whether logging from FortiGate to FortiAnalyzer is enabled.

Option	Description
FortiAnalyzer IP	After selecting a FortiGate, the IP address for the FortiAnalyzer that is receiving logs from the selected FortiGate is displayed.

3. On the *1. Select One device* pane, complete the following options to validate credentials for FortiAnalyzer and select a date range of logs to analyze, and then click *Next*.

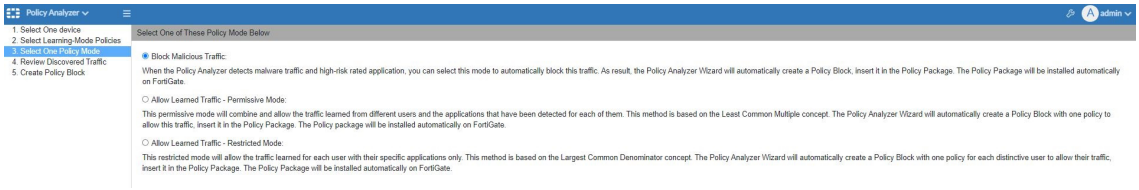
Option	Description
FortiAnalyzer username	Type the username for the administrator account for FortiAnalyzer. The administrator account must have JSON API set to a minimum of Read. See also Configuring FortiAnalyzer on page 14.
FortiAnalyzer password	Type the password for the administrator account.
Validate Credentials	After typing in the FortiAnalyzer username and password, click *Validate Credentials* to authenticate access to the logs on FortiAnalyzer.
FortiAnalyzer ADOM	Available after you validate the username and password for FortiAnalyzer. Select the ADOM on FortiAnalyzer that contains the logs for the selected FortiGate.
Log date range	Available after you validate the username and password for FortiAnalyzer. Click the calendar icon to select a date range of logs for analysis. Policy Analyzer MEA needs to access online logs indexed in the FortiAnalyzer SQL database. Policy Analyzer MEA cannot analyze archived logs. For more information, see the *FortiAnalyzer 7.0.2 Administration Guide*.

The *2. Select Learning-Mode Policies* pane is displayed.

4. On the *2. Select Learning-Mode Policies* pane, select a Security Policy with Learn Mode enabled, and click *Next*. Policies are available for selection when they have Learn Mode enabled and have hit counts.

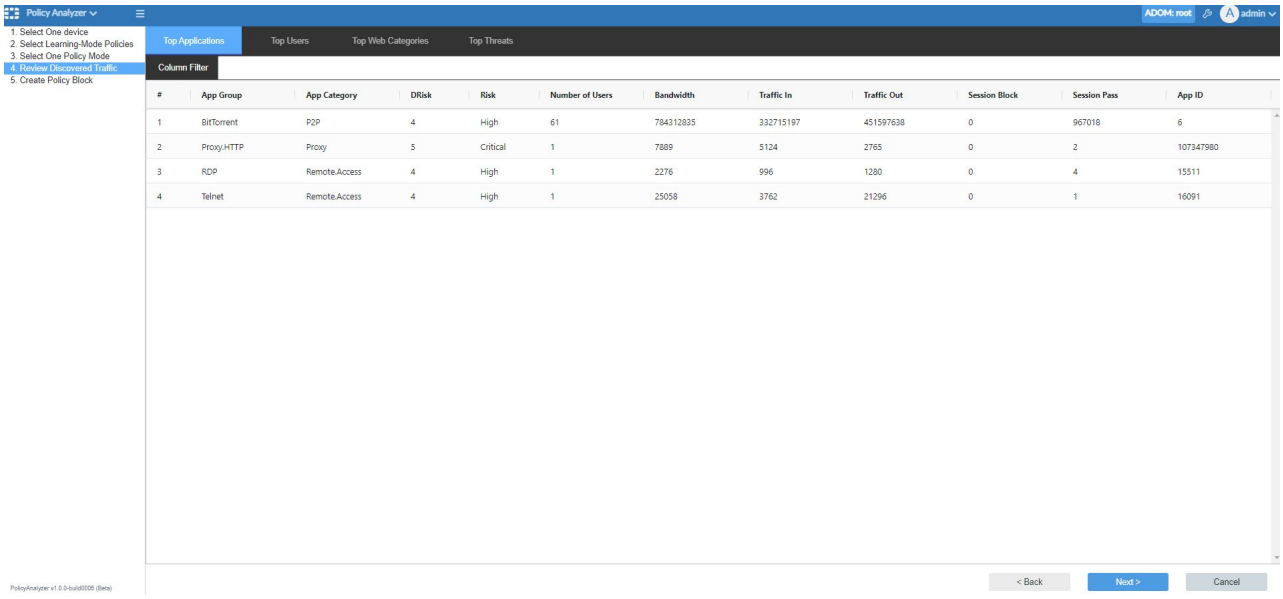
The *3. Select One Policy Mode* pane is displayed.

5. On the *3. Select One Policy Mode* pane, select *Block Malicious Traffic*, and click *Next*.

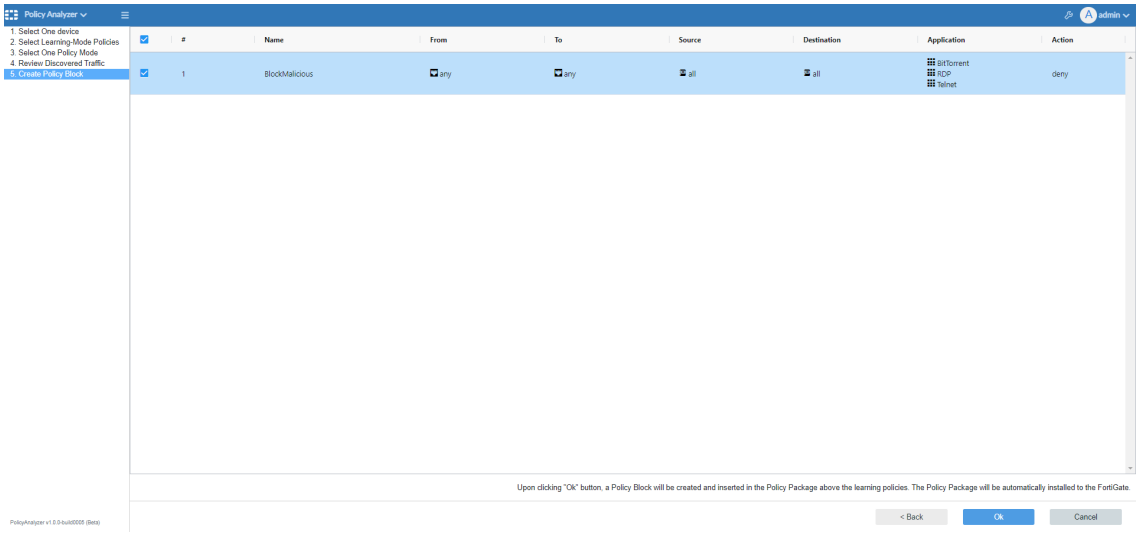


The *Review Discovered Traffic* pane is displayed.

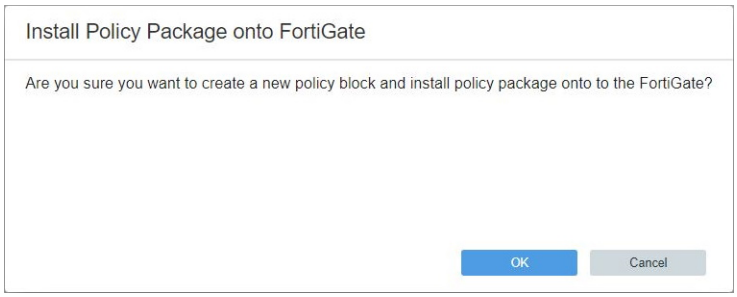
6. On the *Review Discovered Traffic* pane, review discovered traffic, and click *Next*.
In the following example, the *Top Applications* tab shows the high-risk applications in the logs. Click the *Top Users*, *Top Web Categories*, and *Top Threats* tabs to review traffic on those tabs. In the *Column Filter* box, type a string, and press *Enter* to filter results.



The *Create Policy Block* pane is displayed.



7. On the *Create Policy Block* pane, click *OK*.
   A confirmation dialog box is displayed.



8. In the confirmation dialog box, click *OK*.
   Policy Analyzer MEA automatically creates the policy block, inserts the policy block in to the policy package, and the policy package is installed to the FortiGate.

Allowing learned traffic with permissive mode

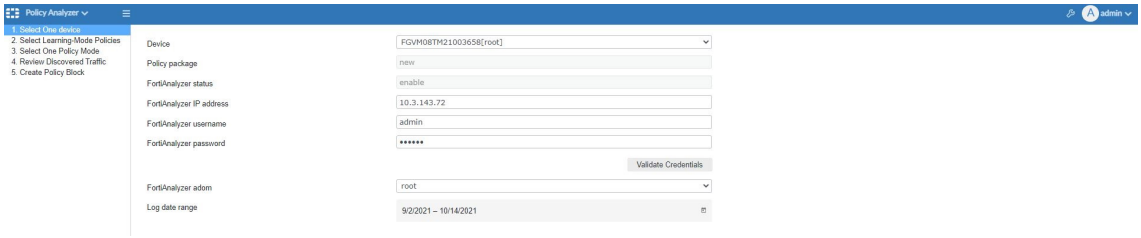
This example describes how to use the Policy Analyzer MEA wizard to create a policy block and an implicit policy. During the wizard, you must choose whether to configure the implicit policy to deny or allow all traffic.

You can use the *Allow Learned Traffic - Permissive Mode* setting to combine and allow traffic learned from different users and their detected applications. This method is based on Least Common Multiple concept. The wizard automatically creates a policy block with one policy to allow this traffic, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.

Only good, learned traffic is allowed. The malware and high-risk traffic is filtered out first.

To allow learned traffic with permissive mode:

1. Open Policy Analyzer MEA to access the first step in the wizard.
   Policy Analyzer opens, and the first pane of the wizard is displayed. The name of the first pane is *1. Select One device*.
2. On the *1. Select One device* pane, select a FortiGate.



Option	Description
Device	Select a managed FortiGate that uses a Security Policy with Learn Mode enabled.
Policy package	After selecting a FortiGate, the policy package for the selected FortiGate is displayed.
FortiAnalyzer status	Displays whether logging from FortiGate to FortiAnalyzer is enabled.
FortiAnalyzer IP	After selecting a FortiGate, the IP address for the FortiAnalyzer that is receiving logs from the selected FortiGate is displayed.

3. On the *1. Select One device* pane, complete the following options to validate credentials for FortiAnalyzer and select a date range of logs to analyze, and then click *Next*.

Option	Description
FortiAnalyzer username	Type the username for the administrator account for FortiAnalyzer. The administrator account must have JSON API set to a minimum of Read. See also Configuring FortiAnalyzer on page 14.

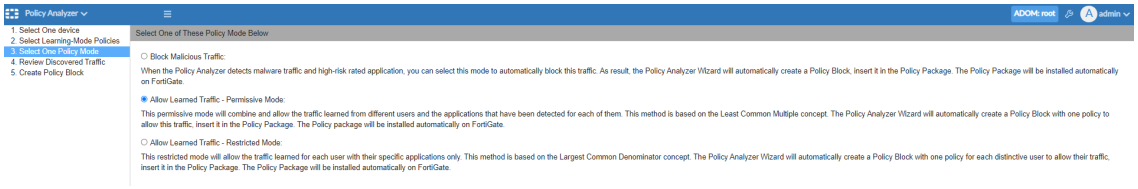
Option	Description
FortiAnalyzer password	Type the password for the administrator account.
Validate Credentials	After typing in the FortiAnalyzer username and password, click *Validate Credentials* to authenticate access to the logs on FortiAnalyzer.
FortiAnalyzer ADOM	Available after you validate the username and password for FortiAnalyzer. Select the ADOM on FortiAnalyzer that contains the logs for the selected FortiGate.
Log date range	Available after you validate the username and password for FortiAnalyzer. Click the calendar icon to select a date range of logs for analysis. Policy Analyzer MEA needs to access online logs indexed in the FortiAnalyzer SQL database. Policy Analyzer MEA cannot analyze archived logs. For more information, see the *FortiAnalyzer 7.0.2 Administration Guide*.

The *2. Select Learning-Mode Policies* pane is displayed.

4. On the *2. Select Learning-Mode Policies* pane, select a Security Policy with Learn Mode enabled, and click *Next*. Policies are available for selection when they have Learn Mode enabled and have hit counts.

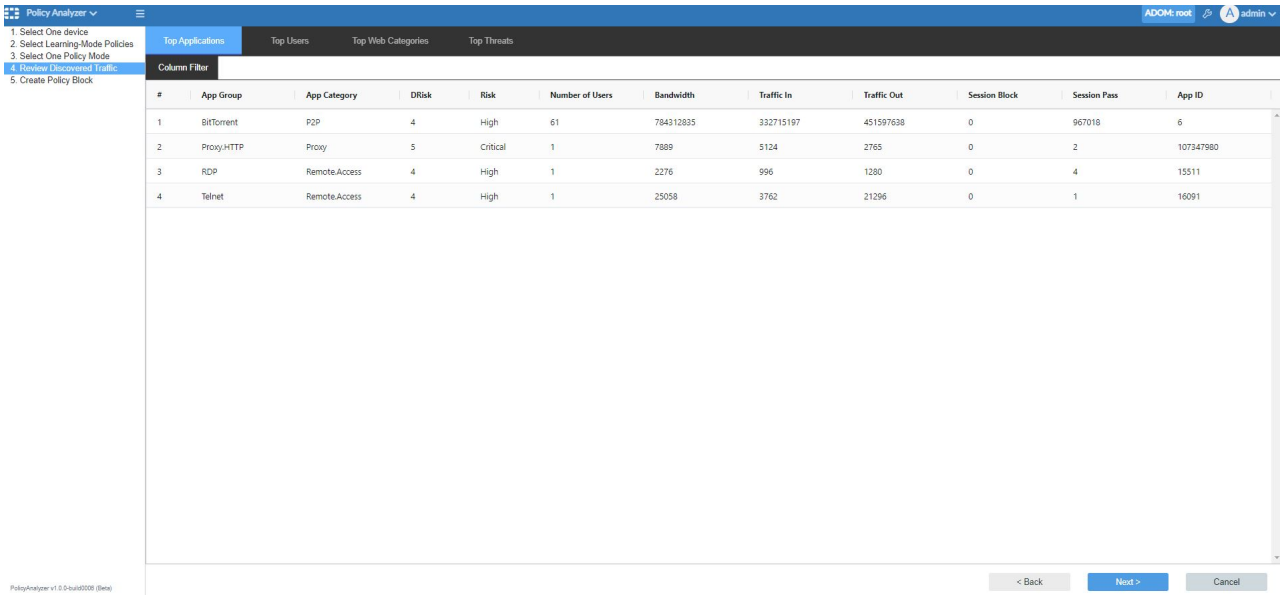
The *3. Select One Policy Mode* pane is displayed.

5. On the *3. Select One Policy Mode* pane, select *Allow Learned Traffic - Permissive Mode*, and click *Next*.

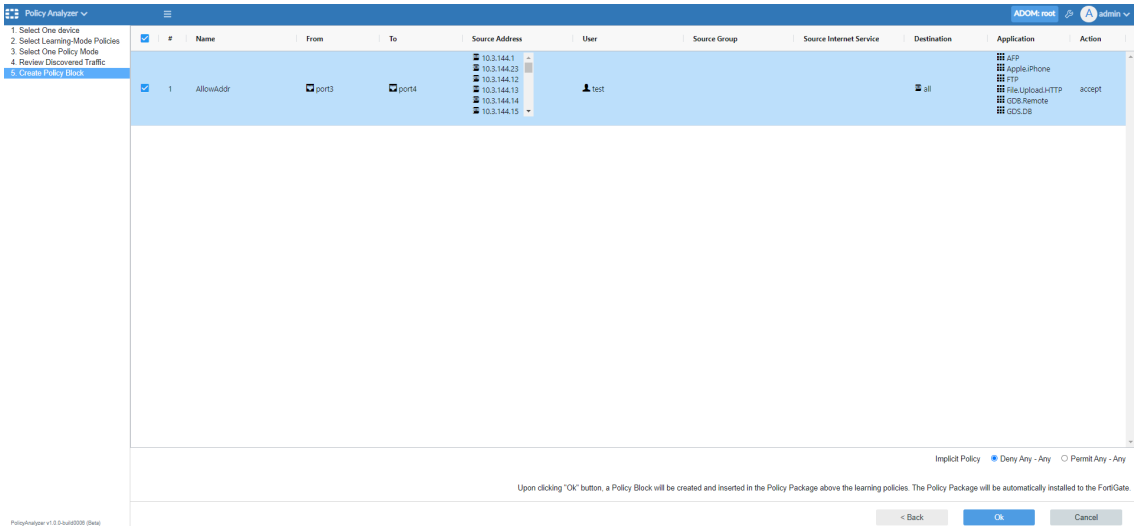


The *Review Discovered Traffic* pane is displayed.

6. On the *Review Discovered Traffic* pane, review discovered traffic, and then click *Next*.
In the following example, the *Top Applications* tab shows the high-risk applications in the logs. Click the *Top Users*, *Top Web Categories*, and *Top Threats* tabs to review traffic on each tab.



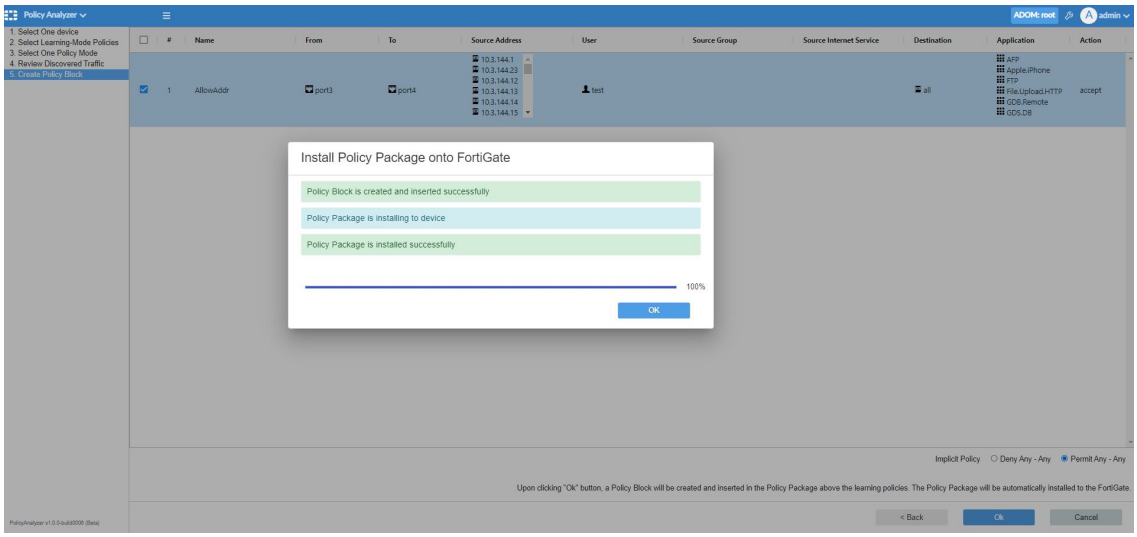
The *Create Policy Block* pane is displayed.



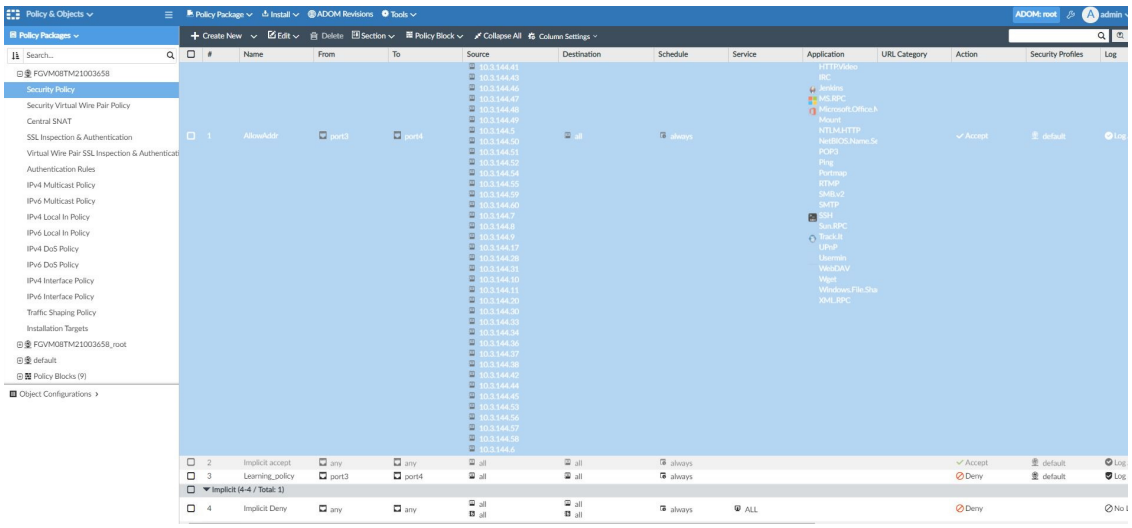
7. On the *Create Policy Block* pane, choose one of the following settings for the implicit policy, and click *OK*:

Option	Description
Deny Any - Any	Select to deny traffic on all source and destination ports.
Permit Any - Any	Select to permit traffic on all source and destination ports.

8. In the confirmation dialog box, click *OK*.
Policy Analyzer MEA automatically creates the policy block, inserts the policy block in to the policy package, and the policy package is installed to the FortiGate.



9. Go to *Policy & Objects* > *Policy Packages* > *Security Policy* to view the policy block created by Policy Analyzer MEA. The policy block and implicit policy are added above the rules in the policy package.



Allowing learned traffic with restrictive mode

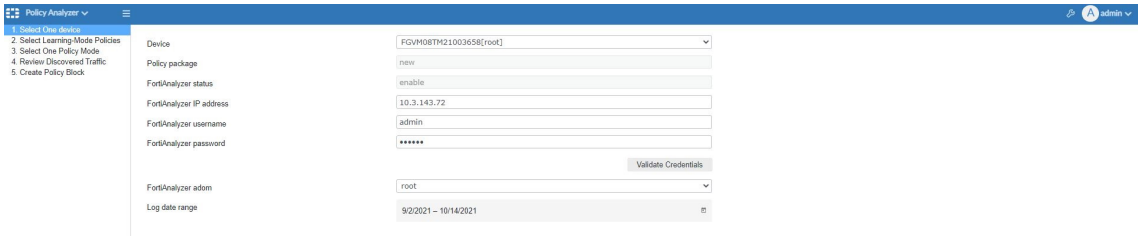
This example describes how to use the Policy Analyzer MEA wizard to create a policy block and an implicit policy. During the wizard, you must choose whether to configure the implicit policy to deny or allow all traffic.

You can use the *Allow Learned Traffic - Restricted Mode* setting to allow the traffic learned for each user with their specific applications only. This method is based on Largest Common Denominator concept. The Policy Analyzer wizard automatically creates a policy block with one policy for each distinctive user, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.

Only good, learned traffic is allowed. The malware and high-risk traffic is filtered out first.

To allow learned traffic with restrictive mode:

1. Open Policy Analyzer MEA to access the first step in the wizard.
   Policy Analyzer opens, and the first pane of the wizard is displayed. The name of the first pane is *1. Select One device*.
2. On the *1. Select One device* pane, select a FortiGate.



Option	Description
Device	Select a managed FortiGate that uses a Security Policy with Learn Mode enabled.
Policy package	After selecting a FortiGate, the policy package for the selected FortiGate is displayed.
FortiAnalyzer status	Displays whether logging from FortiGate to FortiAnalyzer is enabled.
FortiAnalyzer IP	After selecting a FortiGate, the IP address for the FortiAnalyzer that is receiving logs from the selected FortiGate is displayed.

3. On the *1. Select One device* pane, complete the following options to validate credentials for FortiAnalyzer and select a date range of logs to analyze, and then click *Next*.

Option	Description
FortiAnalyzer username	Type the username for the administrator account for FortiAnalyzer. The administrator account must have JSON API set to a minimum of Read. See also Configuring FortiAnalyzer on page 14.
FortiAnalyzer password	Type the password for the administrator account.
Validate Credentials	After typing in the FortiAnalyzer username and password, click *Validate Credentials* to authenticate access to the logs on FortiAnalyzer.
FortiAnalyzer ADOM	Available after you validate the username and password for FortiAnalyzer. Select the ADOM on FortiAnalyzer that contains the logs for the selected FortiGate.
Log date range	Available after you validate the username and password for FortiAnalyzer. Click the calendar icon to select a date range of logs for analysis.

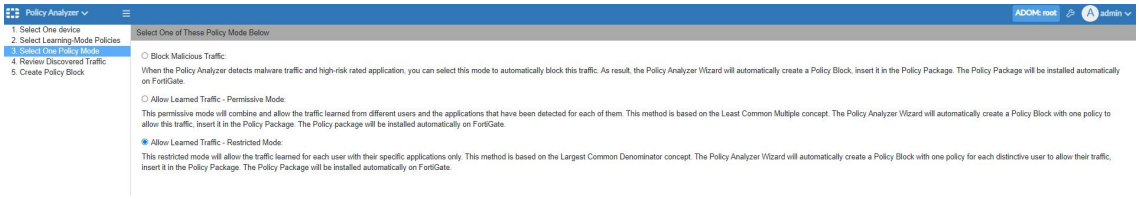
Option	Description
	Policy Analyzer MEA needs to access online logs indexed in the FortiAnalyzer SQL database. Policy Analyzer MEA cannot analyze archived logs. For more information, see the *FortiAnalyzer 7.0.2 Administration Guide*.

The *2. Select Learning-Mode Policies* pane is displayed.

4. On the *2. Select Learning-Mode Policies* pane, select a Security Policy with Learn Mode enabled, and click *Next*. Policies are available for selection when they have Learn Mode enabled and have hit counts.

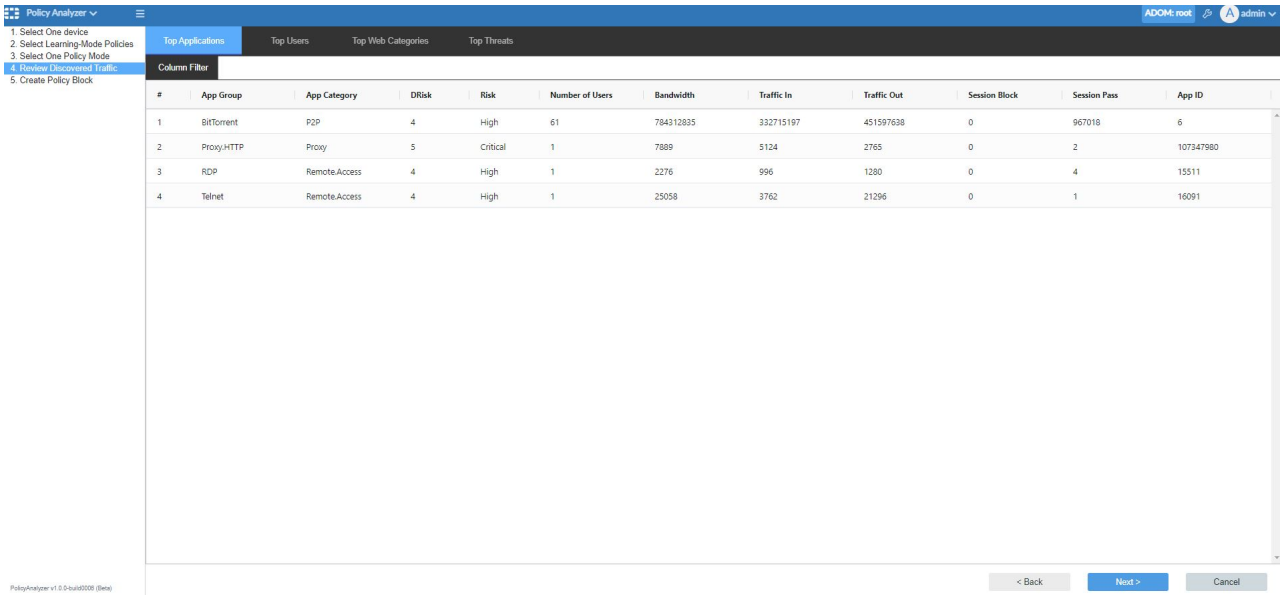
The *3. Select One Policy Mode* pane is displayed.

5. On the *3. Select One Policy Mode* pane, select *Allow Learned Traffic - Restricted Mode*, and click *Next*.

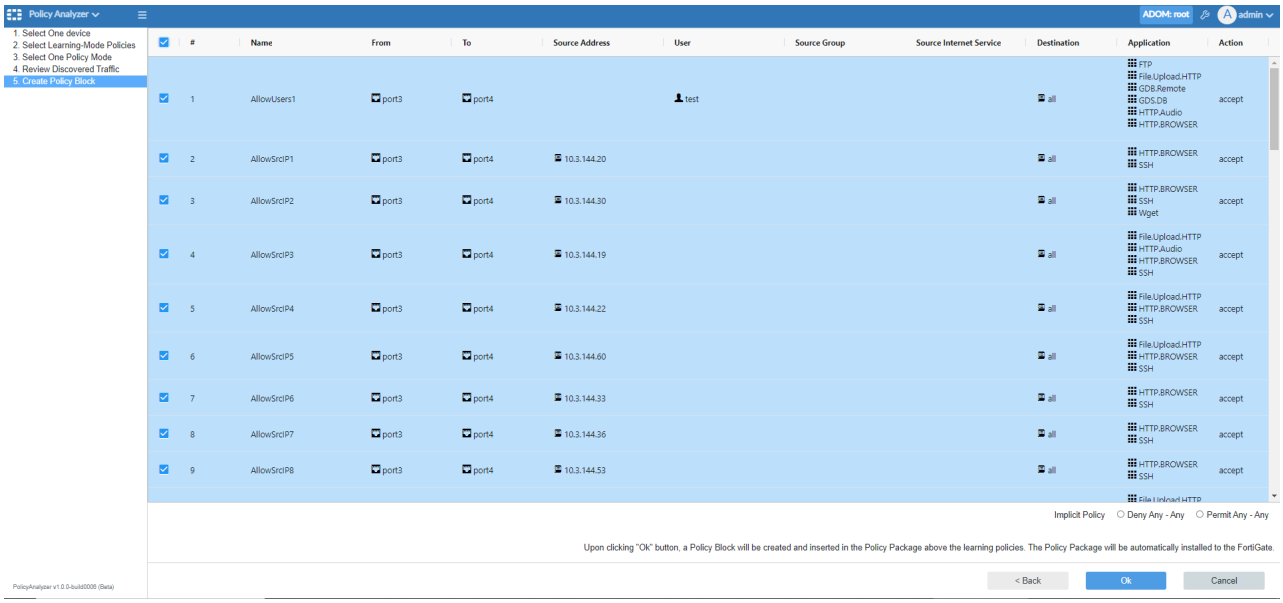


The *Review Discovered Traffic* pane is displayed.

6. On the *Review Discovered Traffic* pane, review discovered traffic, and then click *Next*.
In the following example, the *Top Applications* tab shows the high-risk applications in the logs. Click the *Top Users*, *Top Web Categories*, and *Top Threats* tabs to review traffic on those tabs.



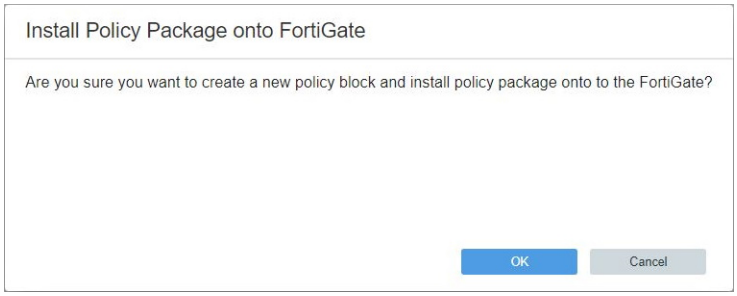
The *Create Policy Block* pane is displayed.



7. On the *Create Policy Block* pane, choose one of the following settings for the implicit policy, and click *OK*:

Option	Description
Deny Any - Any	Select to deny traffic on all source and destination ports.
Permit Any - Any	Select to permit traffic on all source and destination ports.

A confirmation dialog box is displayed.



8. In the confirmation dialog box, click *OK*.
   Policy Analyzer MEA automatically creates the policy block, inserts the policy block in to the policy package, and the policy package is installed to the FortiGate.
9. Go to *Policy & Objects* > *Policy Packages* > *Security Policy* to view the policy block created by Policy Analyzer MEA. The policy block and implicit policy are added above the rules in the policy package.

More information

Policy Analyzer is available as a management extension application with FortiManager. For information about Policy Analyzer MEA, see the FortiManager page on the Document Library.

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.