DO NOT REPRINT
© FORTINET

FortiSandbox
Lab Guide

for FortiSandbox 4.2

FORTINET
Training Institute

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

8/17/2022

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Brave-Dumps.com

TABLE OF CONTENTS

Network Topology 6
Lab 1: Attack Methodology 7
Exercise 1: SQL Injection Overview 8
SQL Overview 8
SQL Injection Overview 9
Exercise 2: Exploiting a SQL Injection Vulnerability 10
Exploit the Web Form 10
Navigate Using the Web Shell (Optional) 12
Remove the Web Shell 13
Lab 2: FortiSandbox Introduction 16
Exercise 1: Deploying FortiSandbox 17
Verify the Network Interfaces 17
Configure the System Settings 17
Configure the Guest VM Settings 21
Configure the Package Options 24
Configure Alert Emails 25
Disable the Uploading of Malicious Samples 26
Enable Verbose Logging 27
Lab 3: Diagnostics 29
Exercise 1: Running Diagnostics 30
Run Diagnostics 30
Gather System Information 31
Lab 4: Protecting the Edge 32
Exercise 1: Integrating FortiSandbox With FortiGate 33
Configure FortiGate System Time 33
Configure FortiSandbox Integration 33
Enable Sandboxing 36
Verify Sandbox Inspection 38
Exercise 2: Blocking URLs Based on FortiSandbox Threat Intelligence 46
Block URLs Based on FortiSandbox Threat Intelligence 46
Exercise 3: Using FortiGate Diagnostics 50
Restore a Configuration File on FortiGate 50
Verify FortiSandbox Communication 50

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Diagnose the Problem 52
Exercise 4: Using Inline Scanning 56
Configure Inline Scanning on FortiSandbox 56
Configure Inline Scanning on FortiGate 58
Verify Inline Scanning Inspection 59
Disable Inline Scanning 60
Lab 5: Email Network Protection 61
Exercise 1: Integrating FortiSandbox With FortiMail 62
Configure the FortiMail System Time 62
Configure FortiSandbox Integration 62
Configure FortiMail for Sandboxing 65
Verify Sandbox Inspection 68
Exercise 2: Configuring Quarantine Release Rescanning 74
Configure User Quarantine on FortiMail 74
Configure Quarantine Rescan 77
Exercise 3: Diagnosing FortiMail Submissions 80
Disable the Content Profile 80
Diagnose FortiMail Submissions 80
Lab 6: Protecting Web Applications 87
Exercise 1: Configuring Machine Learning for Advanced Threats 88
Configure the FortiWeb System Time 88
Configure Machine Learning 89
Configure the Sampling Limit 91
Generating HTTP Requests 92
Attacking the Web Server 94
Exercise 2: Integrating FortiSandbox With FortiWeb 97
Configure FortiSandbox Integration 97
Configure FortiWeb for Sandboxing 99
Verify Sandbox Inspection 101
Exercise 3: Diagnosing FortiWeb Submissions 104
Diagnose FortiWeb Submissions 104
Lab 7: Protecting End Users 106
Exercise 1: Integrating FortiSandbox With FortiClient 108
Configure FortiSandbox Integration 108
Verify Sandbox Inspection 110
Disable FortiSandbox Scanning on FortiClient 114
Lab 8: Protecting Third-Party Devices 116
Exercise 1: Configuring Network Share Scanning 117
Access the File Share 117
Configure Network Share Scanning 118
Verify Network Share Scanning 122

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

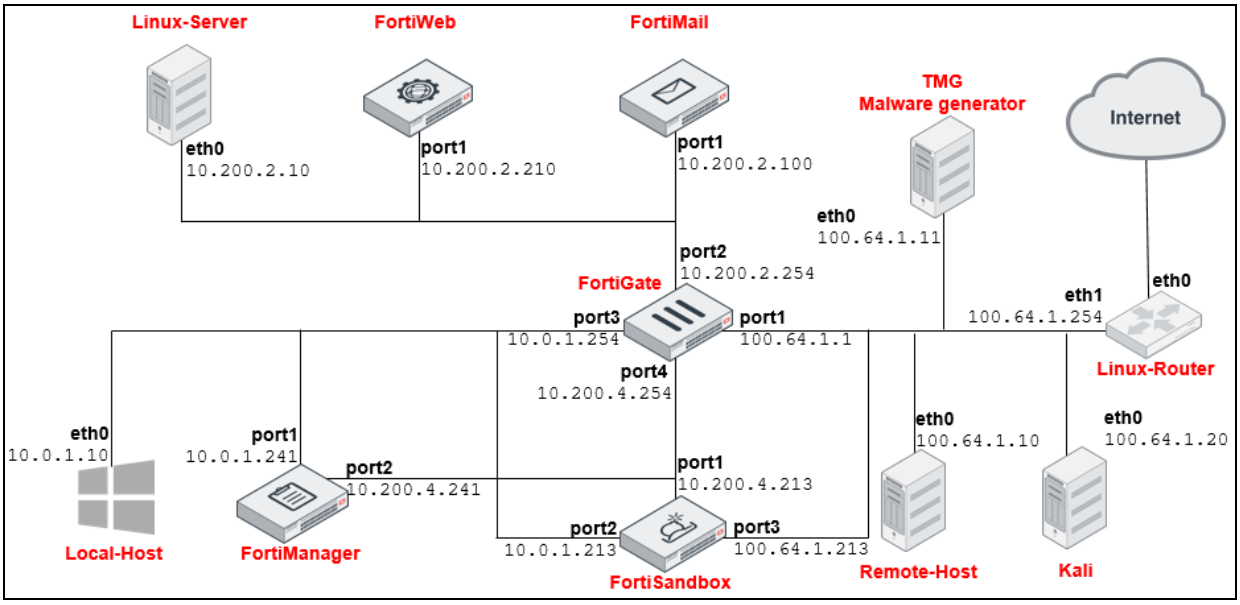
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Diagnosing Network Share Scanning **124**
Prepare the File Share 124
Diagnose Network Share Scanning 124
Lab 9: Analysis of Results **127**
Exercise 1: Analyzing a URL **128**
Access the Scan Job Report 128
Analyze the Created and Injected Process 130
Override a Verdict 135

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Network Topology



The TMG Malware Generator VM generates a new downloader (`fsa_downloader.exe`) malware every time a user generates a file download request from the Malware Sample Portal (hosted on Remote-Host IIS server).

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 1: Attack Methodology

In this lab, you will exploit a SQL injection vulnerability, and then you will upload a web shell to gain full access to the Linux-Server VM.

Objectives

- Exploit a SQL injection vulnerability
- Upload a backdoor web shell to the Acme Corp billing portal

Time to Complete

Estimated: 20 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: SQL Injection Overview

This exercise provides an overview of SQL and SQL injection attacks. If you are already familiar with SQL queries and SQL injection attacks, go to Exploiting a SQL Injection Vulnerability on page 10

SQL Overview

SQL is a language used to access and manipulate databases. Websites use SQL to store and retrieve data from a database. When a website uses a database to retrieve information, it typically uses user input from a web form to build the query.

The following example shows a website that queries a database table for product items, based on user input:

Product Search

Please Enter the Product ID number to search for

Product ID: 78923 Search

The HTML for this page looks like the following image:

```
17      <p>Product Search<br>
18      <p><br>
19      Please Enter the Product ID number to search for</p>
20      </center>
21      </center>
22      <form action="search.php" method="post">
23      <p> Product ID: <input type="text" name="ProductId" />
24      <input type="submit" value="Search" /></p>
25      </center>
```

The following image shows the product table:

ProdID	Description	QuantityOnHand	UnitPrice	SupplerID
78919	plastic bolt	0	9.95	234
78920	metal screw #5	12	14.95	416
78921	metal screw #4	8	7.95	613
78922	metal screw #3	7	3.95	234
78923	metal bolt	52	12.95	234

The user input, `78923`, when submitted to the server-side code, makes the following query to the products table in the database:

```
$sql = "SELECT Description, QuantityOnHand, UnitPrice FROM products WHERE
ProdID='".$_POST['ProductID']."';
```

After adding the user input, the SQL query looks like the following example:

```
SELECT Description, QuantityOnHand, UnitPrice FROM products WHERE ProdID =
'78923'
```

This query will return the description, quantity on hand, and unit price for the product with ID 78923.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

ProdID	Description	QuantityOnHand	UnitPrice	SupplerID
78919	plastic bolt	0	9.95	234
78920	metal screw #5	12	14.95	416
78921	metal screw #4	8	7.95	613
78922	metal screw #3	7	3.95	234
78923	metal bolt	52	12.95	234

SQL Injection Overview

SQL injection can occur when the user input is not validated and is used directly in a SQL query. When this happens, the logic of the query's originally intended action is changed.

If an attacker enters the following text in the **Product Search** form:

```
78923'; UPDATE products SET UnitPrice = '0.00' WHERE ProdID = 78923';--
mycomment
```

The server-side query will look like the following example:

```
SELECT Description, QuantityOnHand, UnitPrice FROM products where ProdID =
'78923'; UPDATE products SET UnitPrice = '0.00' WHERE ProdID = '78923';--
mycomment
```

This example query contains the following two commands:

- The first command, `SELECT Description, QuantityOnHand, UnitPrice FROM products where ProdID = '78923'`, queries the database for the product with an ID of 78923.
- The second command, `UPDATE products SET UnitPrice = '0.00' WHERE ProdID = '78923'`, updates the price of the product with an ID of 78923.

The attacker can use other commands to perform even more destructive actions, such as deleting entire tables, or displaying entries from the users' tables along with their passwords. This vulnerability exists when the input fields of the web application are not sanitized. Unsanitized input fields allow attackers to exploit the database using SQL meta characters, which are special characters that SQL interprets to perform specific functions, to alter the SQL query.

The following table lists some examples of SQL meta characters:

SQL meta character	Description
`'`	Single quotation marks are used as a delimiter to mark the beginning and end of a value. For example, `ProdID = '78923'`.
`.;`	A semicolon is used to end a SQL statement.
`--`	Double dashes are used for comments. All information after the double dashes is ignored. **Note**: For MySQL, the last dash must be followed by at least one white space or control character.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Exploiting a SQL Injection Vulnerability

The company you are going to breach is Acme Corp. During your reconnaissance, you discover a web application that Acme Corp uses for its billing portal. You determine that the web application is vulnerable to SQL injection. You will exploit this vulnerability to log in to the billing portal. After you gain access to the portal, you will upload a web shell. This web server can act as a pivot point that you can use to penetrate deeper into the organization.

Exploit the Web Form

You will use SQL meta characters to gain access to the Acme Corp billing portal.

To access the billing portal

1. On the Remote-Host VM, open a Google Chrome browser tab, and then navigate to the Acme Corp billing portal at `http://billings.acmecorp.net`.
2. In the **Username** field, type `'` (single quotation mark).
3. In the **Password** field, type `pass`.
4. Click **Logon**.

   The following error appears:

   ```
   You have an error in your SQL syntax; check the manual that corresponds to
   your MySQL server version for the right syntax to use near 'pass'' at line 1
   ```

If the server-side SQL query is `SELECT * FROM users WHERE username = '<user input>' and password = '<user input>'`, you can assume that after entering the username and password, the resulting SQL query will be `SELECT * FROM users WHERE username = ''' and password = 'pass'`.

The query will fail because the username value contains three single quotation marks (`'''`) in a row. The failure means that the web form inputs are not sanitized, and the web form is passing SQL meta characters into the query. An attacker can take advantage of the unsanitized web form by using the SQL meta characters to bypass username and password requirements.

To simplify this lab, you will use the username `jsmith` to gain access to the billing portal without a password.

To create the SQL injection

1. Modify the following SQL query with a `username` value that uses the SQL meta characters necessary to bypass password verification:

   ```
   SELECT * FROM users WHERE username = '__________' and password = '________'
   ```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

You learned that semicolons (`;`) are used to end a SQL statement and double dashes (`--`) are used to enter comments. So, if you enter `jsmith';--` for the username, and `pass` for the password, the resulting query will be `SELECT * FROM users WHERE username = 'jsmith';-- ' and password = 'pass';`.

When the query is executed, the SQL engine will ignore everything after the double dashes (`--`), which comments out the `password` portion of the query. The result is the following query:

```
SELECT * FROM users WHERE username = 'jsmith';
```

2. In the **Username** field, type `jsmith';--`. (Remember to add a space after the double dashes.)
3. In the **Password** field, type `pass`.
4. Click **Logon**.
   The login is successful.

This method of creating a SQL injection statement requires that the user `jsmith` already exists in the user table in the database. If the user does not exist, this SQL injection statement will not work.

To upload the web shell

1. Continuing on the Chrome browser tab, click **Choose File**.
2. Click **Desktop** > **Resources** > **Lab 1 - Attack Methodology** > `b374k.php`, and then click **Open**.
3. Click **Upload Invoice**.
4. The following confirmation appears:

```
The file b374k.php has been uploaded to our uploads directory. You, will be
redirected back to the mainpage in 10 seconds
```

You can see that the file is uploaded to the **uploads** directory. After the web page is redirected to the main page, you will use a URL to access the web shell.

To access the web shell

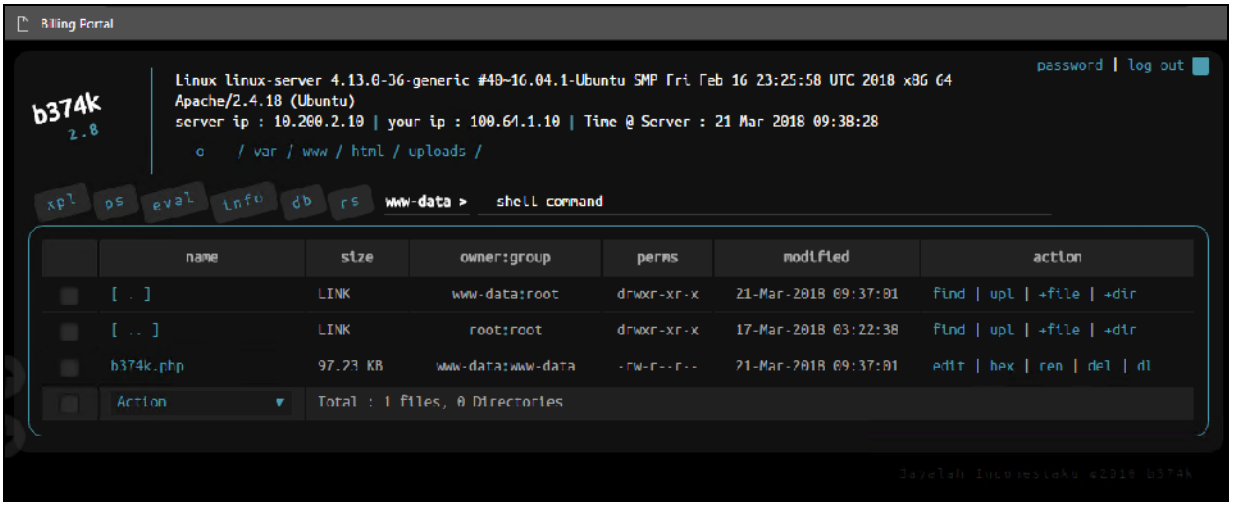
1. Open a new Chrome browser tab, and navigate to `http://billings.acmecorp.net/uploads/b374k.php`
   A password prompt opens.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

2. Type `b374k`.
3. Click **Go**.

   The web shell opens.



A web shell is a script that can be uploaded to a web server to enable remote administration. While it is useful for system administrators, it can also be used by an attacker to gain access to an organization's network, because the infected host can act as a pivot. Web shell features include:

- File manager (view, edit, rename, delete, upload, download)
- Command execution
- Script execution
- Shell access
- Database-management system connection
- SQL explorer
- Process list and task manager

After uploading the web shell, an attacker can use it to leverage other exploitation techniques to escalate privileges and issue commands remotely. The remote commands are directly linked to the privilege and functionality available to the web server and may include the ability to add, delete, and execute files, as well as the ability to run shell commands, other executables, or scripts.

Navigate Using the Web Shell (Optional)

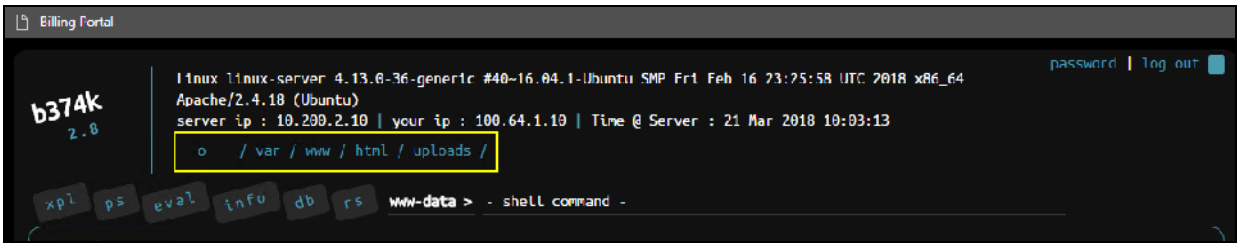
You will use the web shell to navigate the web server directories and determine the username and password used by the web form to connect to the MySQL database.

To navigate using the web shell

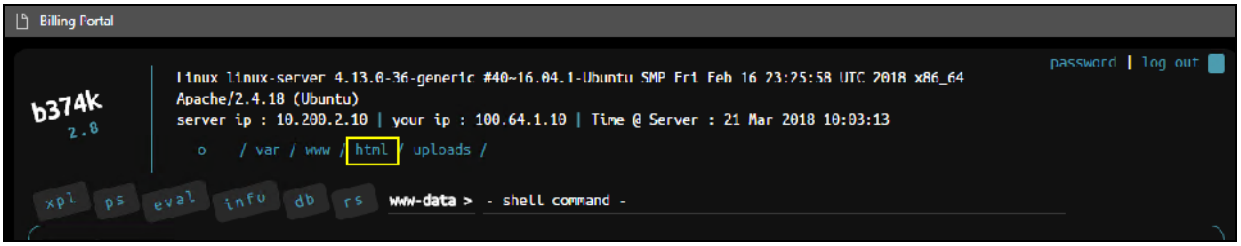
1. Note the navigation path. It contains links to navigate directories.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

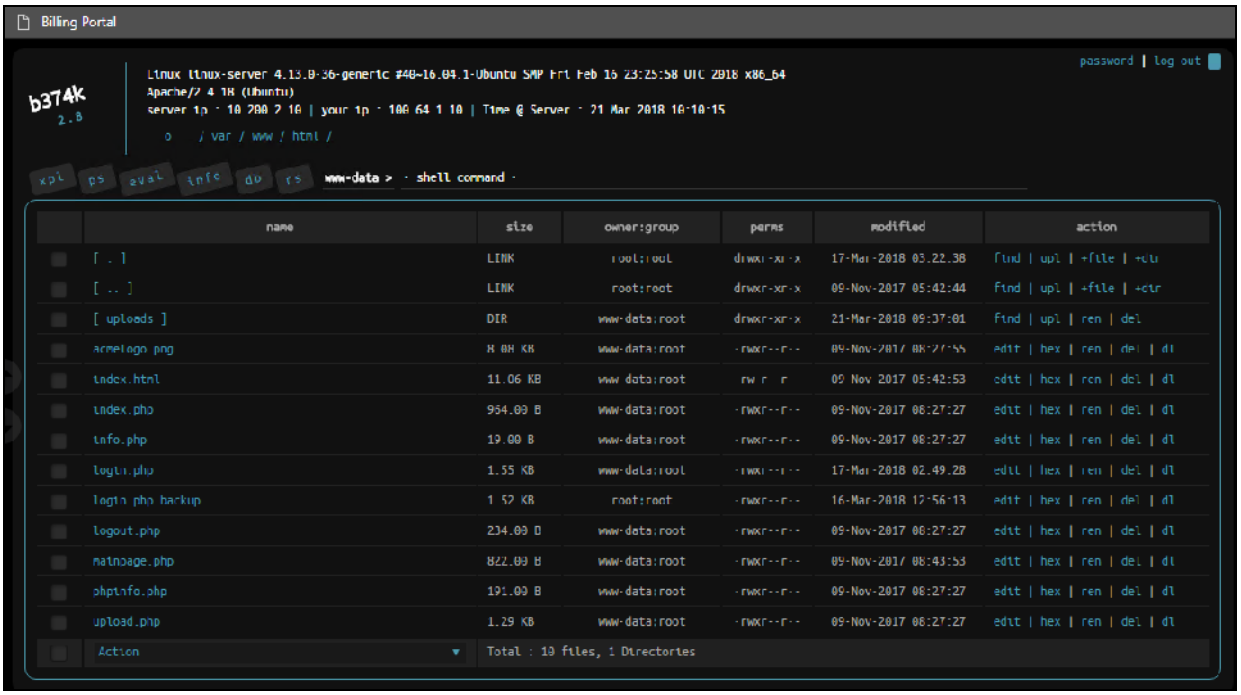
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



2. Click **html**.



The **html** folder contents appear.



3. Use the web shell to determine the username and password that the web form uses to connect to the MySQL database.

   Hint: Navigate to the **/var/www/html** directory, and view the **login.php** file.

Remove the Web Shell

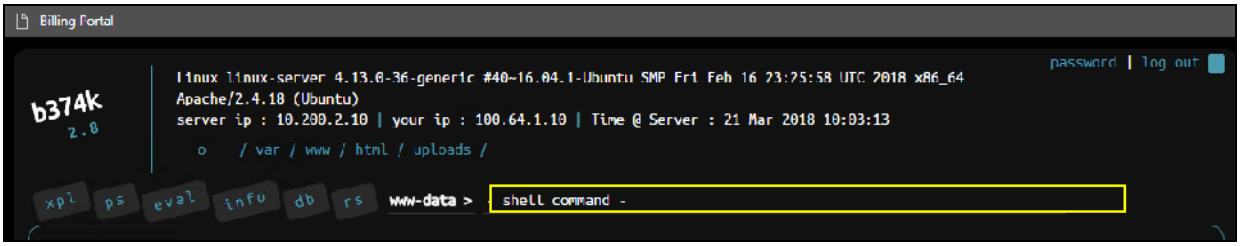
You will remove the web shell from the **uploads** directory.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

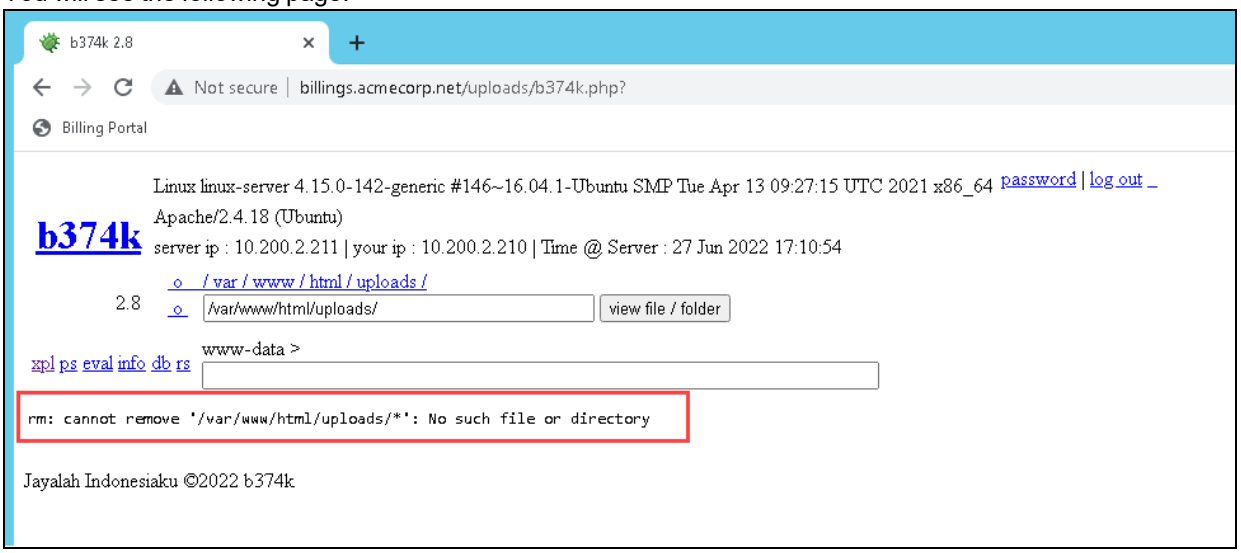
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To remove the web shell

1. Note the `shell command` field.

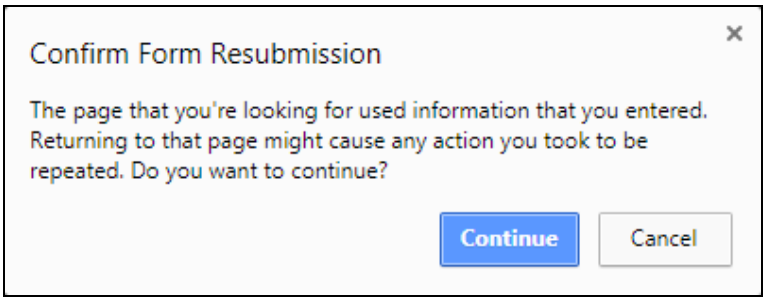


2. In the `shell command` field, type `rm /var/www/html/uploads/*`.
3. Press `Enter`.
4. You will see the following page:



5. Refresh the page.

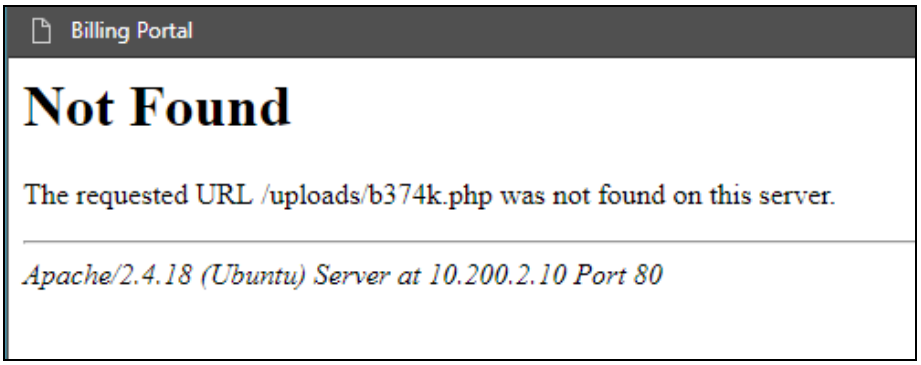
   A **Confirm Form Resubmission** prompt appears.



6. Click **Continue**.
7. An error message appears.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



The error message verifies that the `b374k.php` file has been removed from the **uploads** directory.

8. Close Chrome.
9. Close the Remote-Host VM browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 2: FortiSandbox Introduction

In this lab, you will perform the initial configuration tasks required to deploy FortiSandbox in the lab network.

Objectives

- Review the interface settings
- Configure the system time
- Configure the idle timeout
- Load the tracer and rating engine package
- Configure VM internet access
- Verify the guest VM images
- Configure the scan profile
- Configure the package options
- Configure alert emails
- Configure verbose logging
- Verify the installation using CLI commands

Time to Complete

Estimated: 30 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Deploying FortiSandbox

In this exercise, you will verify the network interfaces, and configure the system time and VM internet access on FortiSandbox. You will also load the tracer and rating engine package, and verify the guest VM images, configure the scan profile and malware package options, disable the uploading of any malicious samples to the Sandbox Community Cloud, and configure verbose logging.

Verify the Network Interfaces

You will verify the configured IP addresses and subnet masks, as well as the default gateway.

To verify the network interfaces

1. Open an SSH session to the FortiSandbox VM.
2. Enter the following CLI command to view the list of FortiSandbox interfaces and their preconfigured IP addresses:
   `show`
   The interface list should match the following example:

```
Configured parameters:
        port1    IPv4 IP: 10.200.4.213/24        MAC: 00:50:56:A1:74:C6
                 MTU: 1500
        port2    IPv4 IP: 10.0.1.213/24  MAC: 00:50:56:A1:E1:B3
                 MTU: 1500
        port3    IPv4 IP: 100.64.1.213/24        MAC: 00:50:56:A1:0C:74
                 MTU: 1500
        port4    IPv4 IP: 192.168.0.213/24       MAC: 00:50:56:A1:AA:40
                 MTU: 1500
        IPv4 Default Gateway: 10.200.4.254
        Administration interface(s): port1 port4
        API interface(s):
```

The `port4` interface does not appear in the network diagram. It is strictly used for management access from the NSE Training Institute environment.

3. Close the SSH session browser tab.

Configure the System Settings

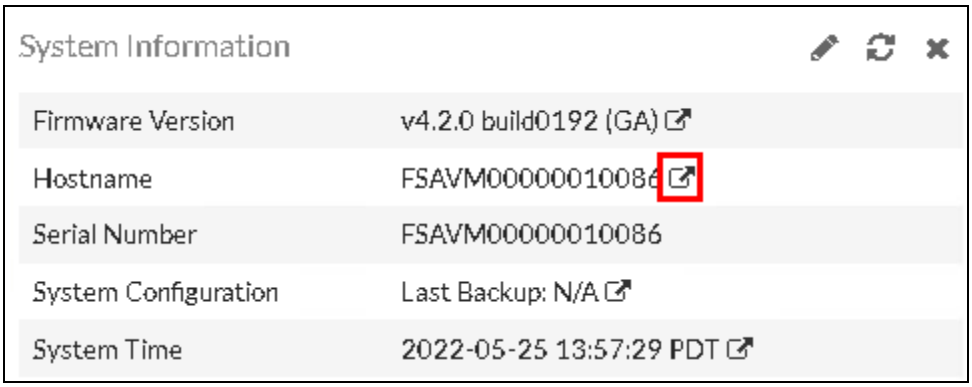
You will access the FortiSandbox GUI and configure the host name, system time, and idle timeout. You will also upload the sandbox engine package.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To configure the host name

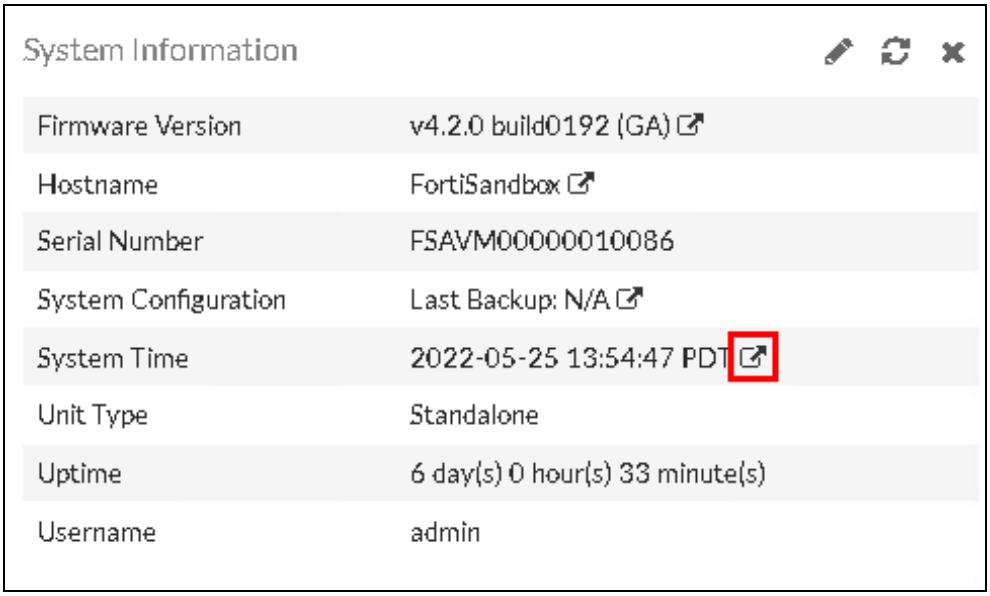
1. On the FortiSandbox GUI, log in with the username `admin` and password `password`.
2. Click **Dashboard** > **Status**.
3. On the **System Information** widget, in the **Hostname** field, click the edit icon.



4. In the **New Name** field, type `FortiSandbox`.
5. Click **Apply**.
6. Click **Back**.

To configure the system time

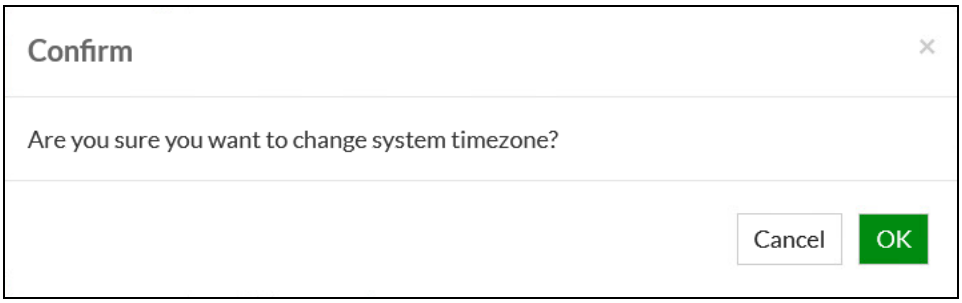
1. Continuing on the FortiSandbox GUI, on the **System Information** widget, in the **System Time** field, click the icon.



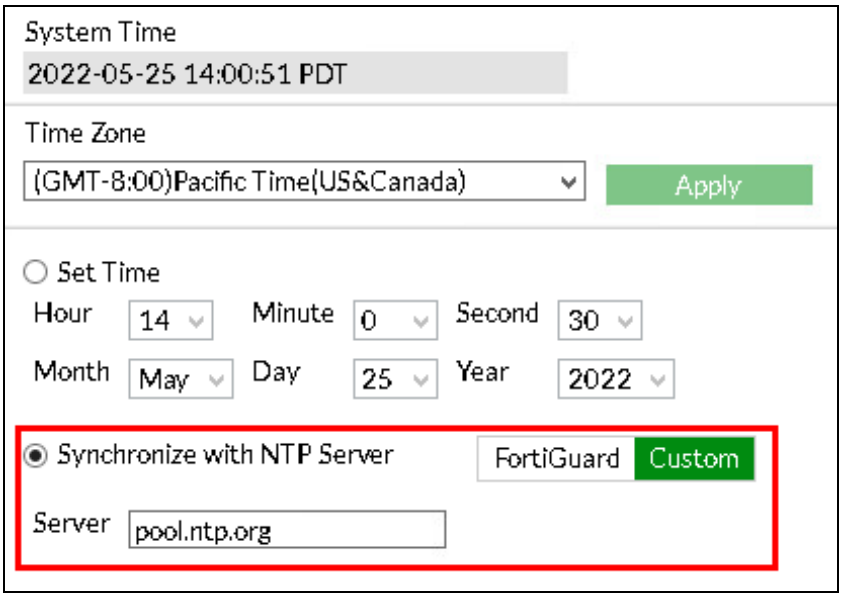
2. In the **Time Zone** drop-down list, select your local time zone.
3. Click **Apply**.
   A confirmation prompt appears.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

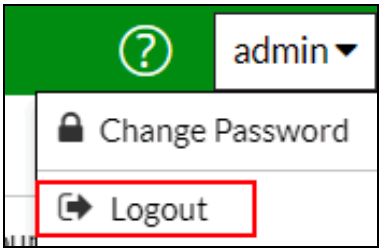


4. Click **OK**.
5. Click **Synchronize with NTP Server**.
6. Click **Custom**.
7. In the **Server** field, type `pool.ntp.org`.



8. Click **Apply**.
9. Wait for a confirmation.
   The system might log you out. If this occurs, go to step 11.

10. In the upper-right corner of the screen, click **admin**, and then click **Logout**.



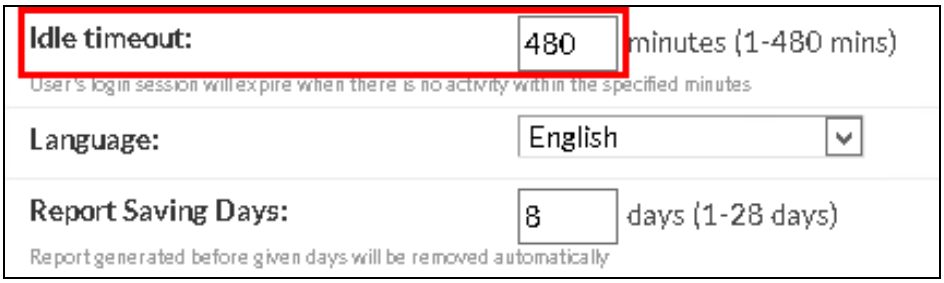
11. Log back in to the FortiSandbox GUI with the username `admin` and password `password`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To configure the system settings

1. Continuing on the FortiSandbox GUI, click the **System** > **Settings**.
2. In the **Idle Timeout** field, type `480`.



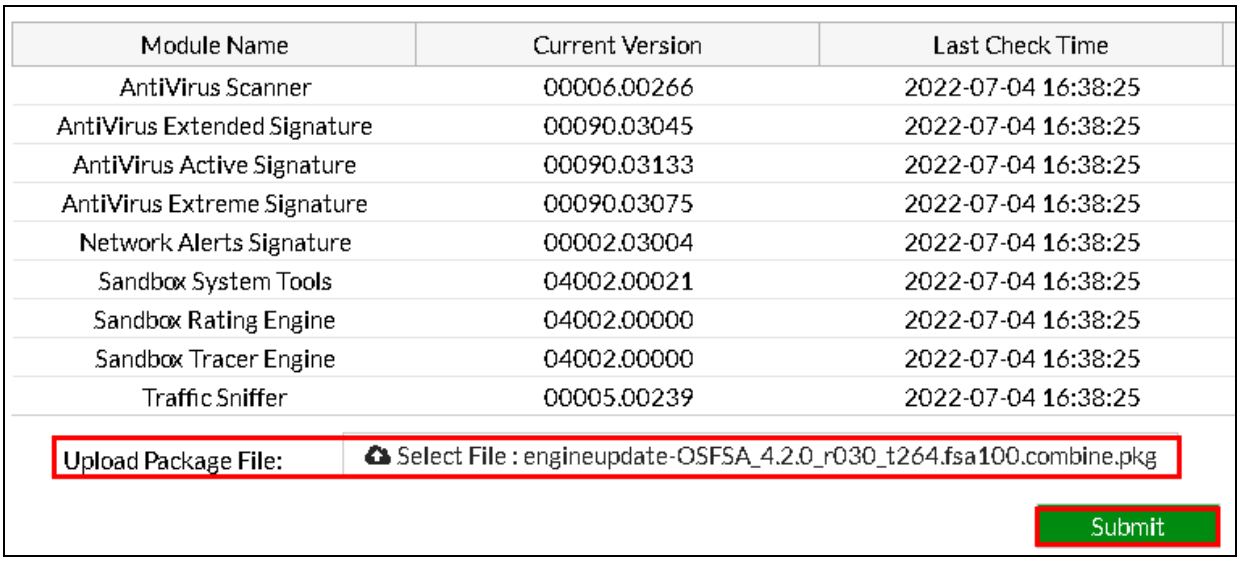
3. Click **OK**.

To load the sandbox engine package

1. Go to the Local-Host VM, open Firefox, and log in to the FortiSandbox GUI with the username `admin` and password `password`.

Firefox is preconfigured with bookmarks for all lab devices. The tracer and rating engine package is located in the **Resources** folder on the Local-Host VM.

1. Click **System** > **FortiGuard**.
2. In the **Upload Package File** section, click **Select File**.
3. Click **Desktop** > **Resources** > **Lab 2 - FortiSandbox Introduction** > `engineupdate-OSFSA_4.2.0_r030_t264.fsa100.combine.pkg`, and then click **Open**.
4. Click **Submit**.

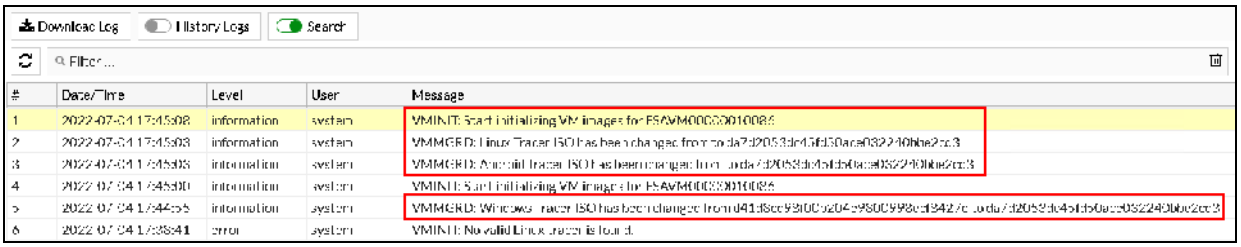


Module Name	Current Version	Last Check Time
AntiVirus Scanner	00006.00266	2022-07-04 16:38:25
AntiVirus Extended Signature	00090.03045	2022-07-04 16:38:25
AntiVirus Active Signature	00090.03133	2022-07-04 16:38:25
AntiVirus Extreme Signature	00090.03075	2022-07-04 16:38:25
Network Alerts Signature	00002.03004	2022-07-04 16:38:25
Sandbox System Tools	04002.00021	2022-07-04 16:38:25
Sandbox Rating Engine	04002.00000	2022-07-04 16:38:25
Sandbox Tracer Engine	04002.00000	2022-07-04 16:38:25
Traffic Sniffer	00005.00239	2022-07-04 16:38:25

5. Click **OK**.
   Wait until the package loads. This may take up to 10 minutes.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



6. Click **Log & Report** > **Events** > **System Events**.
7. Verify that the package is installed successfully:

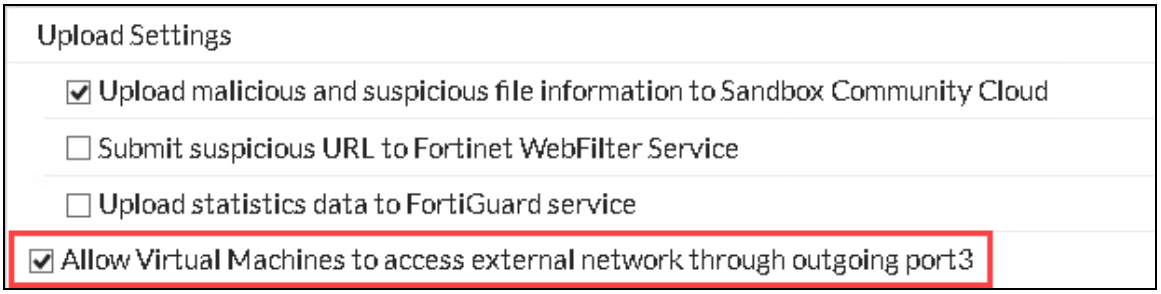
#	Date/Time	Level	User	Message
1	2022-07-04 17:44:59	information	admin	The new package file user submitted is successfully installed.
2	2022-07-04 17:44:59	information	system	Successfully installed Sandbox Tracer Engine, ver: 04002.00264
3	2022-07-04 17:44:57	information	system	FSA-ICAP is starting
4	2022-07-04 17:44:57	information	system	FSA-MTA: fsamta is starting
5	2022-07-04 17:44:57	information	system	FSA-BCC: fsabcc is starting
6	2022-07-04 17:44:57	information	system	Sandbox Tracer Engine is ready.
7	2022-07-04 17:43:36	information	system	Successfully installed Sandbox Rating Engine, ver: 04002.00030
8	2022-07-04 17:43:15	information	system	Sandbox Rating Engine is ready.
9	2022-07-04 17:38:07	information	admin	User successfully submitted a new package file.

Configure the Guest VM Settings

You will configure the port3 gateway and DNS settings to allow VM internet access. Then, you will verify the guest VM images, and configure the scan profile and malware package options.

To configure VM internet access

1. Continuing on the FortiSandbox GUI, click **Scan Policy and Object** > **General Settings**.
2. Select the **Allow Virtual Machines to access external network through outgoing port3** checkbox.



3. Configure the following settings:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

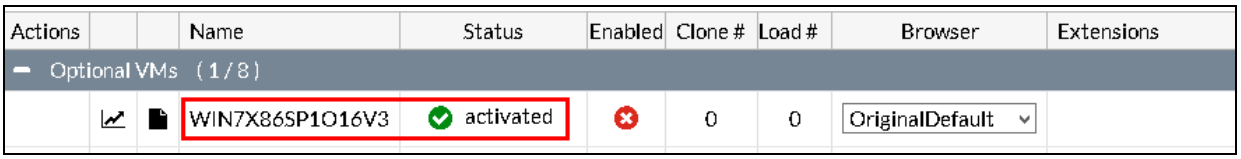
Field	Value
Gateway	100.64.1.254
DNS	10.200.2.10

4. Click **OK**.
5. Click **Dashboard** > **Status**.
6. In the **System Information Widget**, verify that the **VM Internet Access** icon is green.

7. If the **VM Internet Access** icon is still **red**, wait a few minutes, and then refresh the widget.

To activate the guest VM images

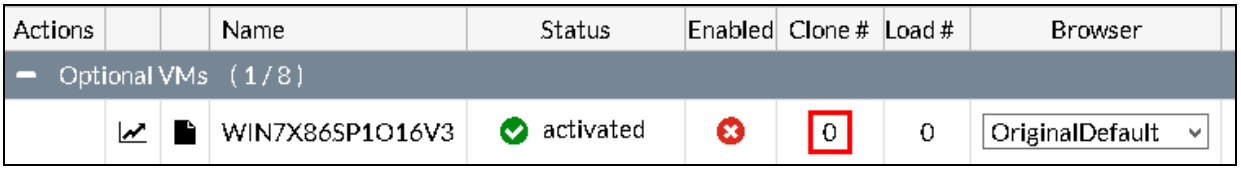
1. Continuing on the FortiSandbox GUI, click **Scan Policy and Object** > **VM Settings**.
2. Verify that there is a Windows 7 VM image.



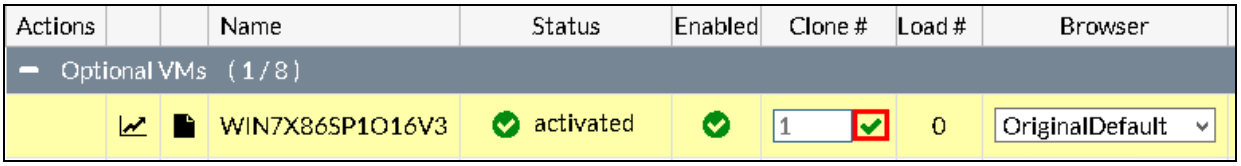
The FortiSandbox VM00 appliance does not include any preinstalled VM images. They must be downloaded and installed manually, which can take a significant amount of time. You can view the available images in the **Optional VMs** section.

To save time, the Windows 7 VM image has already been downloaded for the lab environment.

3. Double-click the **WIN7X86SP1O16V3** clone field:



4. In the text field, type `1`.
5. Click the check mark.



6. Scroll down to the bottom of the page, and click **Apply**.

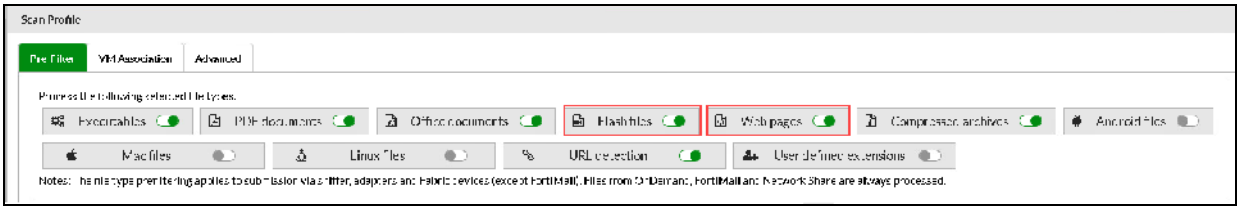
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

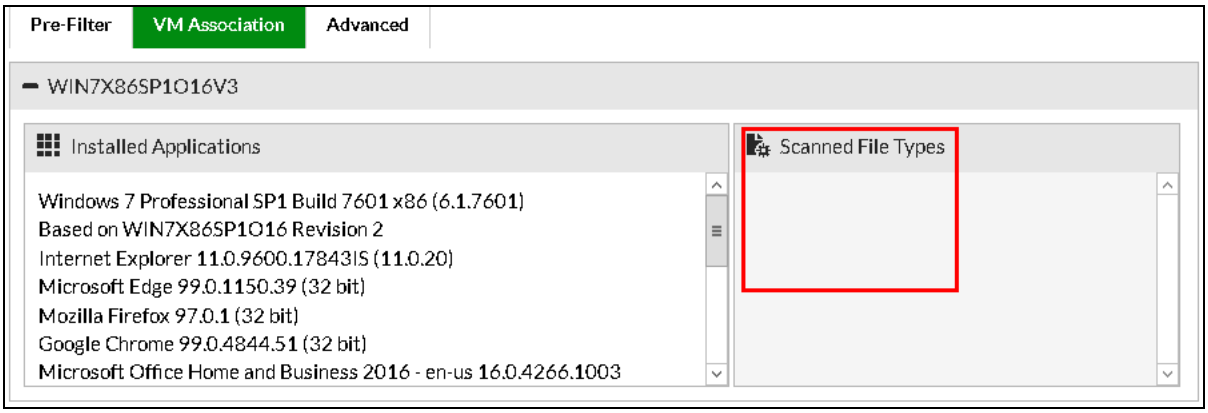
Note that currently, the guest VM image does not have any **Extensions** assigned. This is because you have not configured the scan profile.

To configure the scan profile

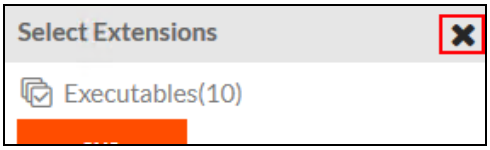
1. Continuing on the FortiSandbox GUI, click **Scan Policy and Object** > **Scan Profile**.
2. In the **Pre-Filter** section of the profile, enable **Flash files** and **Web pages**.



3. In the **Advanced** section, enable and change the **VM Scan timeout for non-executable file** value to `180` (3 minutes).
4. Enable and change the **VM Scan timeout for URL** value to `240` (4 minutes).
5. Click **Apply**.
6. Click the **VM Association** tab.
7. In the **Extensions** column, click the edit icon (✎).
8. In the **WIN7X86SP1O16V3** section, click the **Scanned File Types** section.



9. In the **Select Extensions** pane, select the following categories:
   - **Executables**
   - **PDF documents**
   - **Office documents**
   - **Flash files**
   - **Web pages**
   - **Compressed archives**
   - **URL detection**
10. Click **X** to close the **Select Extensions** pane.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

11. Click **Apply**.
12. Click **Scan Policy and Object** > **Scan profile** > **VM Association**.
13. The **Extensions** column should now match the following example:

Name	Extensions
WIN7X86SP1O16	WEBLink, bat, cmd, dll, doc, docm, docx, dot, dotm, dotx, eml, exe, htm, iqy, jar, js, jse, lnk, msg, msi, onetoc, pdf, pot, potm, potx, ppam, pps, ppsm, ppsx, ppt, pptm, pptx, ps1, rtf, scr, sldm, sldx, swf, thmx, upx, url, vbs, wsf, xlam, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, zip

After a scan profile configuration change, FortiSandbox reinitializes the guest VM images. This is why the **Status** column may show **installed** instead of **activated**.

14. Click **Log & Report** > **Events** > **VM Events**.
15. Verify that the scan profile was updated successfully.

#	Date/Time	Level	User	Message
1	2022-04-28 23:16:14	information	admin	Scan Profile was updated successfully.
2	2022-04-28 23:15:54	information	admin	Scan Profile was updated successfully.
3	2022-04-28 23:15:13	information	system	VMINIT: Start initializing VM images for FSAVM00000010086.
4	2022-04-28 23:15:08	information	system	VMMGRD: VM profile has been changed.

Configure the Package Options

You will configure the definitions that will be included in the antivirus and URL packages that FortiSandbox generates.

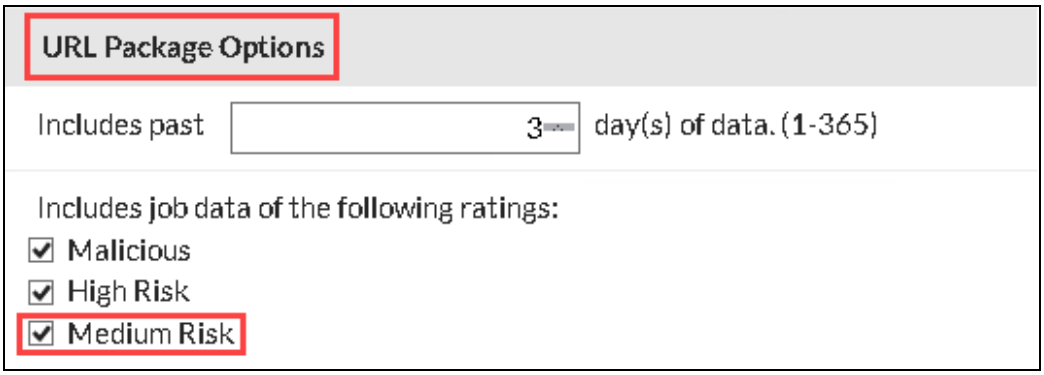
To configure the package options

1. Continuing on the FortiSandbox GUI, click **Scan Policy and Object** > **Threat Intelligence**.
2. In the **Malware Package Options** section, select the **Medium Risk** checkbox.

3. In the **URL Package Options** section, select the **Medium Risk** checkbox.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



4. Click **OK**.

Configure Alert Emails

You will configure and test alert emails.

To configure alert emails

1. Continuing on the FortiSandbox GUI, click **System** > **Mail Servers**.
2. Configure the following settings:

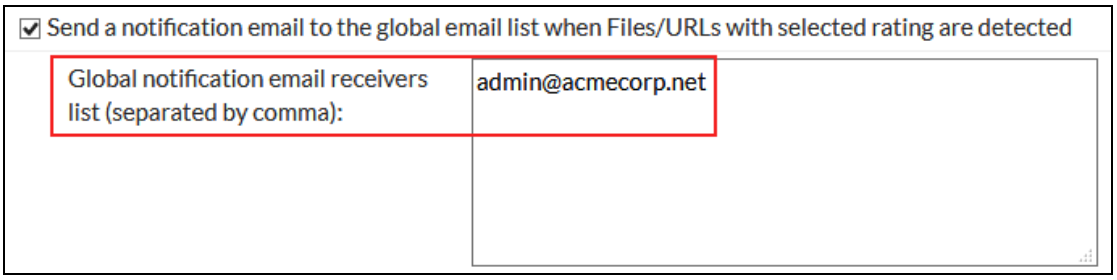
Field	Value
SMTP Server Address	10.200.2.100
Email Account	fsa@acmecorp.net
Login Account	fsa@acmecorp.net
Password	Fortinet1!
Confirm Password	Fortinet1!

The `10.200.2.100` host is the FortiMail located in the DMZ of the lab network. The fsa@acmecorp.net account has been preconfigured.

3. Select the **Send a notification email to the global email list when Files/URLs with selected ratings are detected** checkbox.
4. In the **Global notification email receivers list** field, type `admin@acmecorp.net`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



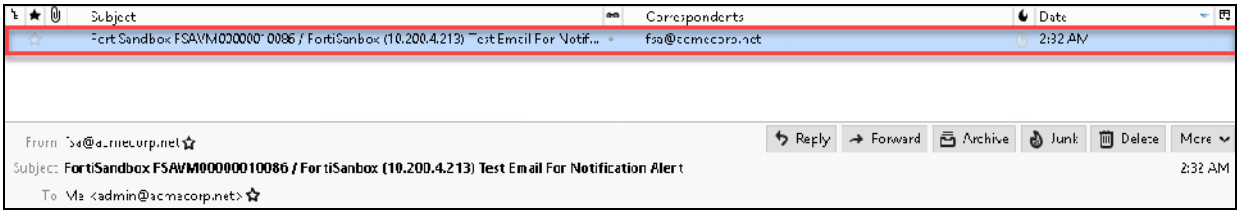
5. Click **OK**.
6. Click **Send Test Email**.
7. You should receive a success message that looks like the following example:

To view the test alert email

1. On the Local-Host VM, open Thunderbird.

Thunderbird has been preconfigured with the admin@acmecorp.net email account.

2. Click **admin@acmecorp.net** > **Inbox**.
3. Verify that you received the email.



4. Close Thunderbird.
5. Close the Local-Host VM browser tab.

Disable the Uploading of Malicious Samples

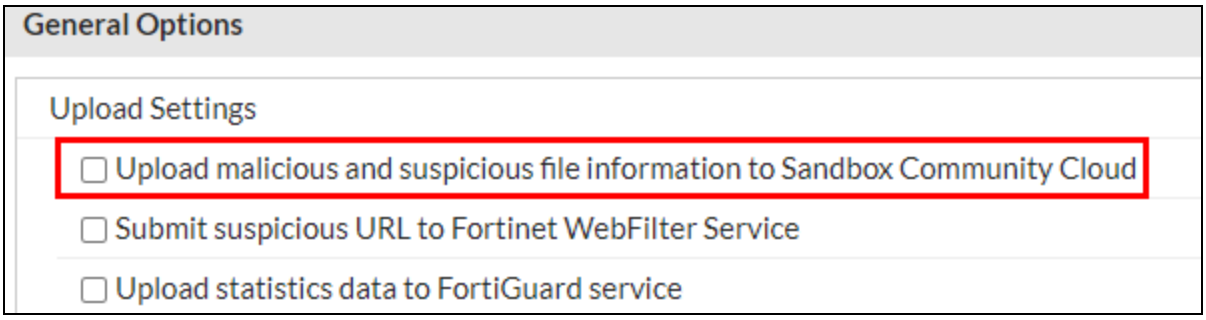
You will disable the uploading of the malware test samples to the Sandbox Community Cloud. You will do this to make sure that FortiSandbox does not upload any information related to the malware test samples to the community cloud.

To disable uploads to the Sandbox Community Cloud

1. Return to the FortiSandbox GUI, and then click **Scan Policy and Object** > **General Settings**.
2. In the **Upload Settings** section, clear the **Upload malicious and suspicious file information to Sandbox Community Cloud** checkbox to disable it.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



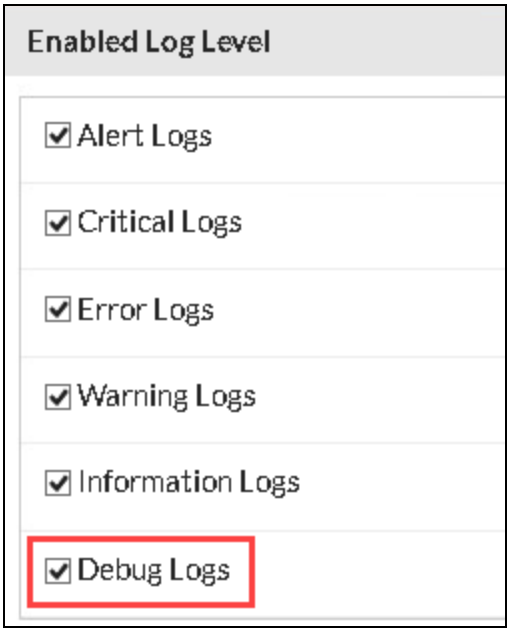
3. Click **OK**.

Enable Verbose Logging

You will enable verbose logging on FortiSandbox. This level of verbosity is useful for troubleshooting and lab environments, however, it is not recommended for day-to-day operations.

To enable debug level logging

1. Continuing on the FortiSandbox GUI, click **Log & Report** > **Log Settings**.
2. Select the **Debug Logs** checkbox to enable it.



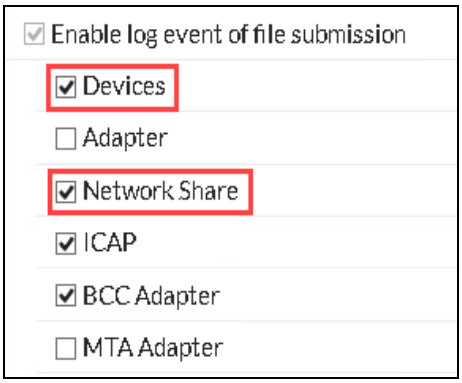
3. Click **Save**.

To enable different inputs for the event log

1. Continuing on the FortiSandbox GUI, click **Scan Policy and Object** > **General Settings**.
2. In the **Enable log event of file submission** section, select the **Devices** and **Network Share** checkboxes.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

Brave-Dumps.com
DO NOT REPRINT
© FORTINET



3. Click **OK**.
4. Log out of the FortiSandbox GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 3: Diagnostics

In this lab, you will run some very common diagnostic commands on FortiSandbox. These diagnostic commands are useful when you run into issues and need to troubleshoot the problem.

Objectives

- Review a list of commands
- Verify installation
- Gather system information

Time to Complete

Estimated: 15 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Running Diagnostics

You will run some diagnostic commands on FortiSandbox using the FortiSandbox CLI.

Run Diagnostics

You will access the FortiSandbox CLI, and run some diagnostic commands to verify your installation.

Take the Expert Challenge!

- Open an SSH connection to the FortiSandbox VM.
- Type `?`, and then press `Enter` to list the available CLI commands on FortiSandbox.
- Use appropriate CLI commands to answer the following questions:
  - How many different versions of Microsoft Office licenses are installed?
  - Which three FQDNs are used to test Wget speeds?
  - Which two URLs are used to validate the web filtering service?

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To navigate the CLI

1. Open an SSH connection to the FortiSandbox VM.
2. Type the following command to list the available CLI commands on FortiSandbox:
   `?`
3. Review the list of commands. They are grouped into the following three categories:
   - `System`
   - `Utilities`
   - `Diagnostics`

To verify the installation

1. Continuing on the FortiSandbox CLI, type the following command to list the installed Microsoft license keys:
   `vm-license -l` (lowercase L)

   Using the list of license keys, you can verify how many different versions of Windows and Microsoft Office your FortiSandbox can support in guest VM images.
2. Type the following command to run the network tests:
   `test-network`
3. Wait until all of the tests complete, and then review the information. Make a note of *all* the FQDNs used in all the tests.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

- `www.google.com` and `www.fortinet.com`: Used to validate general internet connectivity and web filtering service
- `fsavm.fortinet.com`: Used to validate connectivity to the FortiGuard VM image download server
- `go.microsoft.com`: Used to validate connectivity to the Microsoft license validation servers

4. Review the output for the web filtering service tests, and then make a note of the URLs used in the rating queries.

```
Testing Web Filtering service ++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Secure Web Filtering service: Disabled
Proxy: Disabled
Verify contract: Success
Rating 1=www.google.com 2=www.fortinet.comm via 10.200.4.241:53: Success
```

Gather System Information

You will use various CLI commands to gather system information.

To gather system information

1. Continuing on the FortiSandbox CLI, type the following command to display the system information:
   `status`
   From the output, you can view the following information:
   - Device serial number
   - Firmware image version
   - License status for VM appliances
   - Disk allocation and usage
   - Guest VM image initialization status
   - Guest VM internet access status
2. Type the following command to display hardware information:
   `hardware-info`
3. Answer the following questions:
   - How many CPUs are allocated to this VM?
   - How much RAM is allocated to this VM?
4. Type the following command to display the system performance information:
   `diagnose-sys-perf`
6. Type the following command to display the system's running processes:
   `diagnose-sys-top`

The `diagnose-sys-top` command generates an auto-refreshing output of the system's running processes, and their respective resource utilization values in real time. It is a quick way to determine which process is currently demanding the most CPU and RAM utilization.

7. Press `q` to stop the output.
8. Close the SSH session browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 4: Protecting the Edge

In this lab, you will configure FortiGate to submit files to FortiSandbox. You will verify your configuration using multiple malware samples. You will also run some FortiGate debug commands and analyze the output.

Objectives

- Configure FortiGate to submit files to FortiSandbox for inspection
- Block URLs based on FortiSandbox threat intelligence
- Monitor FortiSandbox inspection results and statistics for the inspected files
- Use Inline Scanning Configuration
- Troubleshoot connection issues between FortiSandbox and FortiGate

Time to Complete

Estimated: 90 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Integrating FortiSandbox With FortiGate

In this exercise, you will integrate FortiSandbox with FortiGate. You will configure an antivirus profile to offload files to FortiSandbox. You will then verify your configuration using multiple malware test samples and observe the behavior of FortiSandbox. Finally, you will configure block URLs that are reported as malicious by FortiSandbox.

Configure FortiGate System Time

You will configure the system time zone and enable synchronization with a custom NTP server on FortiGate.

To configure the system time zone

1. Open an SSH session to the FortiGate VM.
2. Type the following commands to see the time zone codes:
```
config system global
   set timezone ?
```
   The available time zone codes are displayed.
3. Determine your local time zone code, and then type the following commands to configure the time zone:
```
   set timezone <code>
end
```

To configure a custom NTP server

1. Continuing on the FortiGate CLI, type the following commands to configure a custom NTP server:
```
config system ntp
   set type custom
   config ntpserver
      edit 1
         set server pool.ntp.org
      next
   end
end
```
2. Close the FortiGate SSH session browser tab.

Configure FortiSandbox Integration

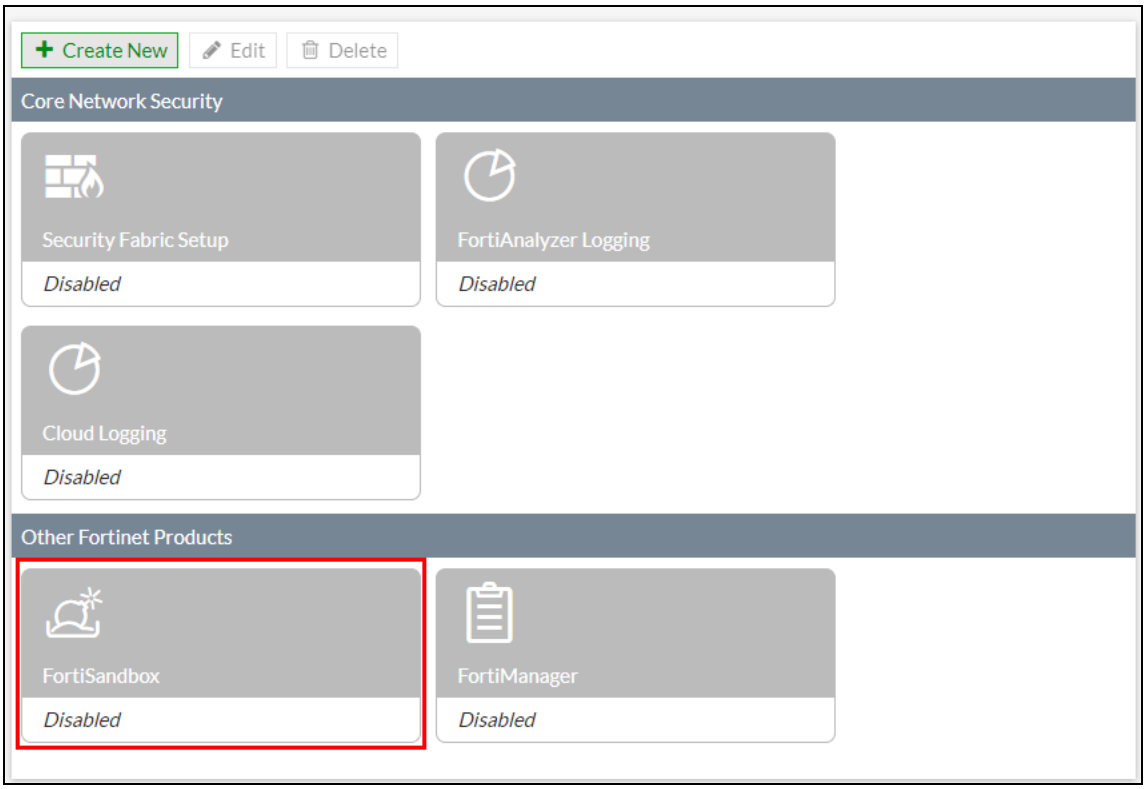
You will configure the settings required to integrate FortiGate with FortiSandbox. You will then authorize FortiGate on FortiSandbox, and then verify the connectivity between the two devices.

To configure the sandbox settings on FortiGate

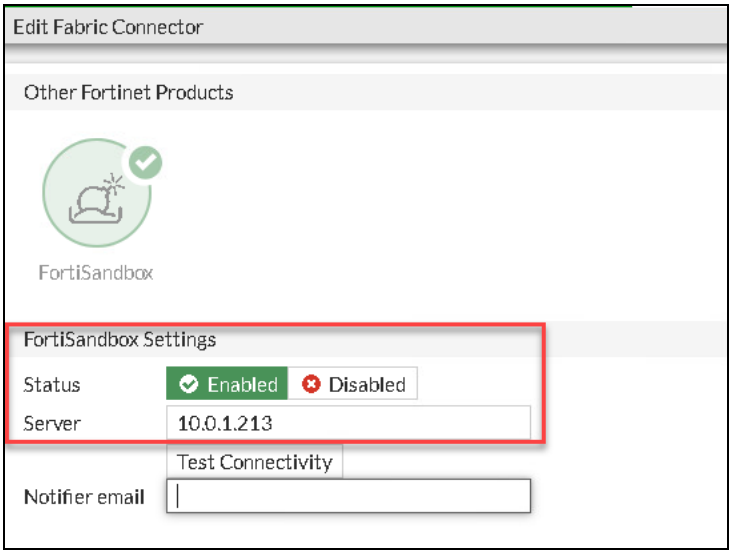
1. On the FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Fabric Connectors**.
3. Double-click **FortiSandbox**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



4. In the **Status** field, click **Enabled**.
5. In the **Server** field, type `10.0.1.213`.

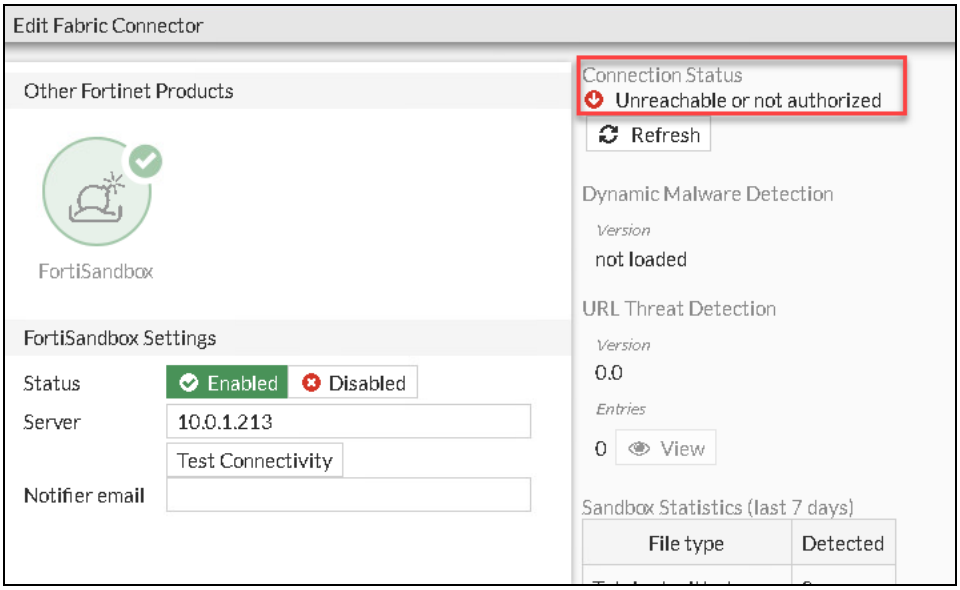


Because you already configured the alert email settings on FortiSandbox, you will not configure the **Notifier email** setting. Configuring this setting on FortiGate will duplicate the alert emails.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

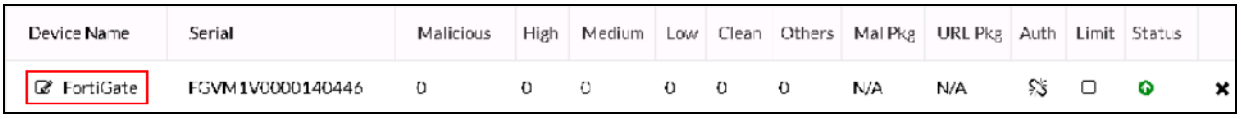
6. Click **OK**.
7. Double-click **FortiSandbox** again.
   The **Connection Status** field displays the following error:



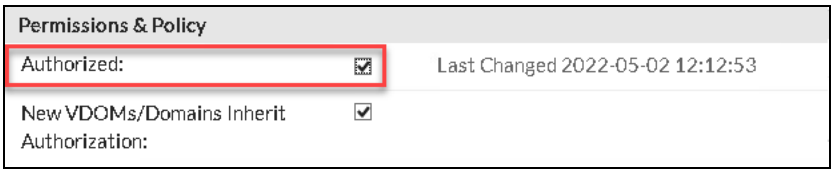
You must authorize FortiGate on FortiSandbox.

To authorize FortiGate on FortiSandbox

1. On the FortiSandbox GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Device**.
3. Click **FortiGate**.



4. In the **Permissions & Policy** section, select the **Authorized** checkbox.



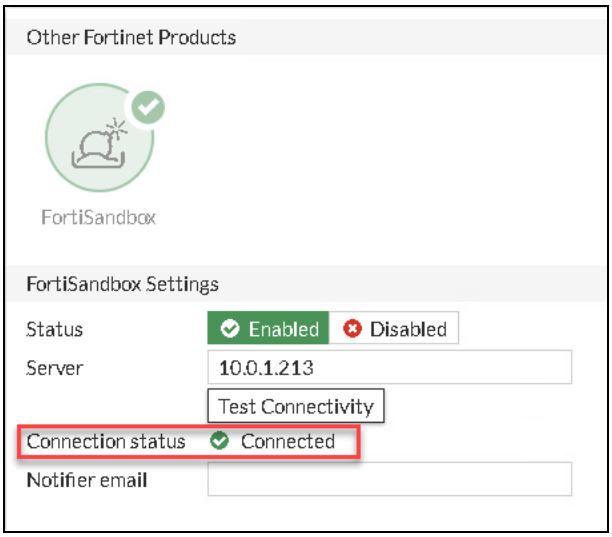
5. Click **OK**.
6. Click **OK** again because you already configured notifications for the global email list.

To verify connectivity between FortiGate and FortiSandbox

1. Return to the FortiGate GUI, and then click **Test Connectivity**.
   The **Connection status**displays **Connected**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



Enable Sandboxing

First, you will configure an antivirus profile to send all supported files to FortiSandbox, and then you will apply it to a firewall policy.

Take the Expert Challenge!

Create a new antivirus profile and name it `AV-AcmeCorp`.

For the antivirus profile configuration, confirm the following:

- **Feature Set** is set to **Proxy**.
- HTTP protocol scanning is enabled.
- Sandboxing is enabled for all supported files.
- FortiGate uses the FortiSandbox signature database to supplement its own antivirus signature database.

Enable the **AV-AcmeCorp** antivirus profile on the existing firewall policy that is configured to allow all traffic from port3 (LAN) to port1 (WAN), and then ensure that the inspection mode is set to **Proxy**.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify Sandbox Inspection on page 38

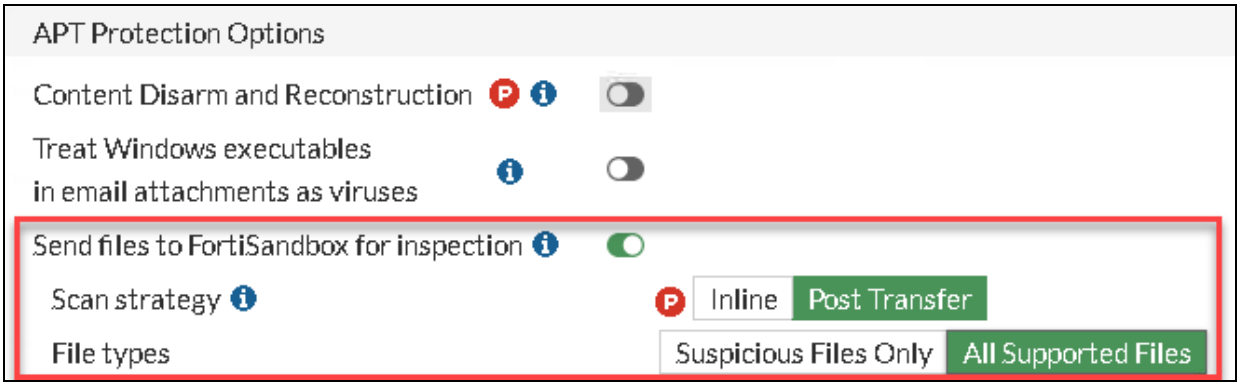
To configure an antivirus profile

1. Continuing on the FortiGate GUI, click **Security Profiles** > **AntiVirus**.
2. Click **Create New**.
3. In the **Name** field, type `AV-AcmeCorp`.
4. In the **Feature set** section, make sure **Proxy-based** is selected.

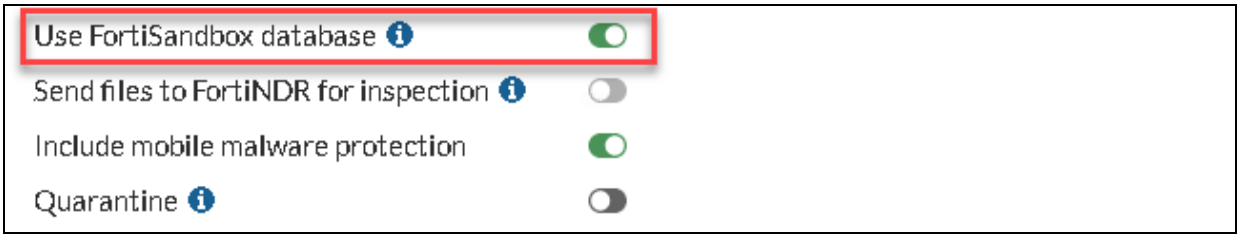
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

5. In the **Inspected Protocols** section, enable **HTTP**.
6. Enable **AntiVirus Scan**, and use the default value **Block**.
7. In the **APT Protection Options** section, enable **Send Files to FortiSandbox for Inspection**.
8. In the **Scan strategy**section, select **Post Transfer**.
9. In the **File Types**section, select **All Supported Files**.



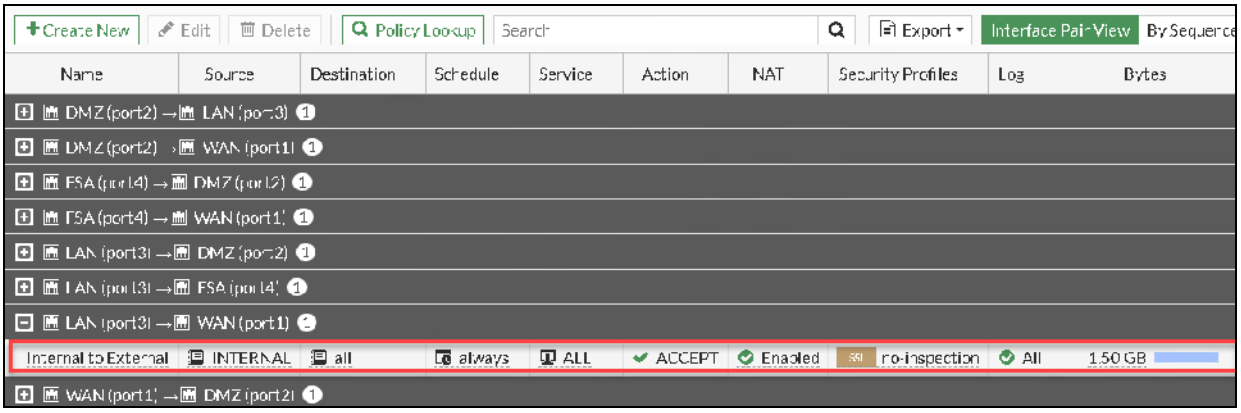
10. Turn on **Use FortiSandbox Database**.



11. Click **OK**.

To apply the antivirus profile to a firewall policy

1. Continuing on the FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.
2. Expand **LAN(port3)** → **WAN(port1)**.
3. Double-click the **Internal to External** firewall policy.

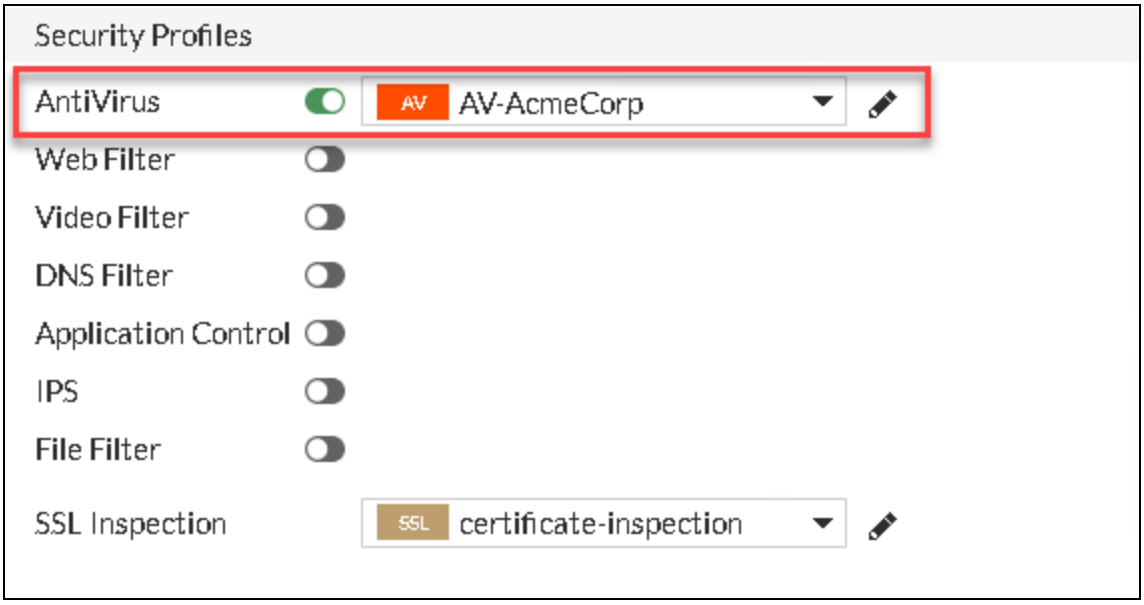


4. In the **Inspection Mode** section, select **Proxy-based**.
5. Turn on **AntiVirus**.
6. In the **AntiVirus** drop-down list, select **AV-AcmeCorp**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The **Security Profiles** section for the policy should match the following example:



7. Click **OK**.

Verify Sandbox Inspection

You will verify sandbox inspection using multiple malware samples.

To verify antivirus inspection with a known virus

1. On the Local-Host VM, open Google Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.

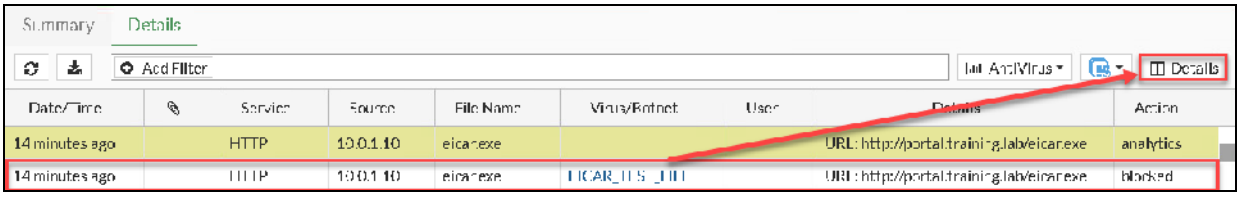
Chrome has been configured to automatically start in incognito mode. This is done to make sure that every time you open Chrome, it establishes a new session on FortiGate.

2. Click **EICAR**.
   A block message is displayed.

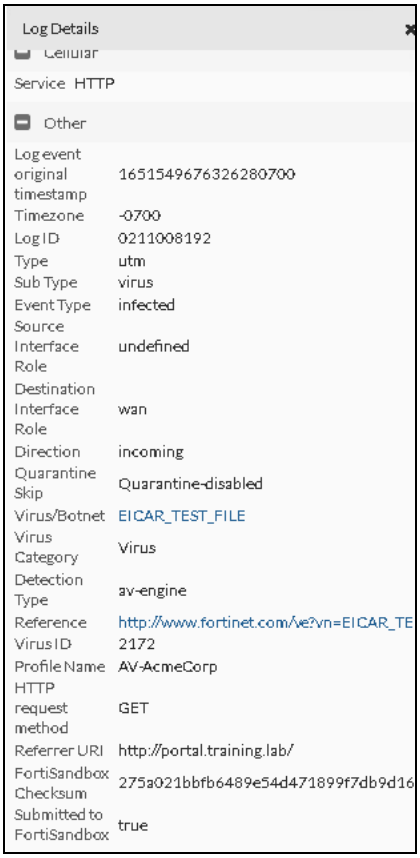
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

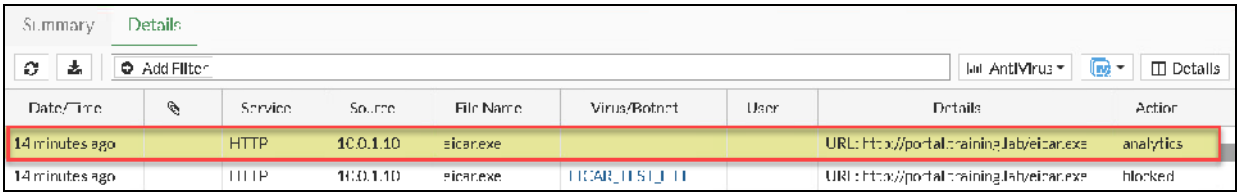
3. Close Chrome.
4. Return to the FortiGate GUI, and then click **Log & Report** > **Security Events**.
5. Under **Summary**, click the **AntiVirus**block log entry, select the log record, and then click **Details**.



6. In the **Details** pane, in the **Other** section, review the log information.



7. Review the antivirus analytics log entry.



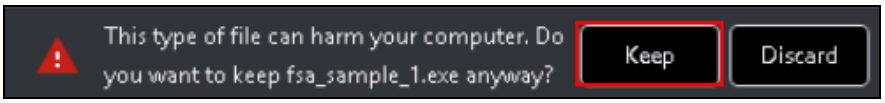
Even though the EICAR test file was detected using local antivirus scanning, FortiGate still shares the file and related information with FortiSandbox. This ensures that FortiSandbox acts as a complete central repository of all malware activity in your network.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

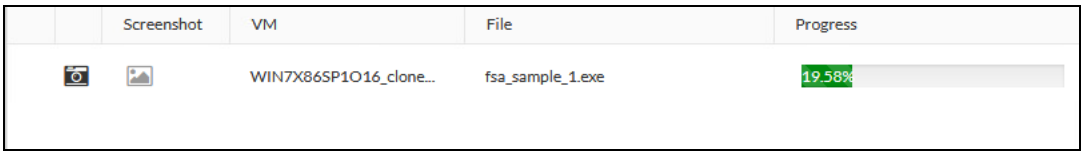
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To verify sandbox inspection with a clean sample

1. Return to the Local-Host VM, open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
2. Click **Clean Sample**.
   A security warning is displayed.

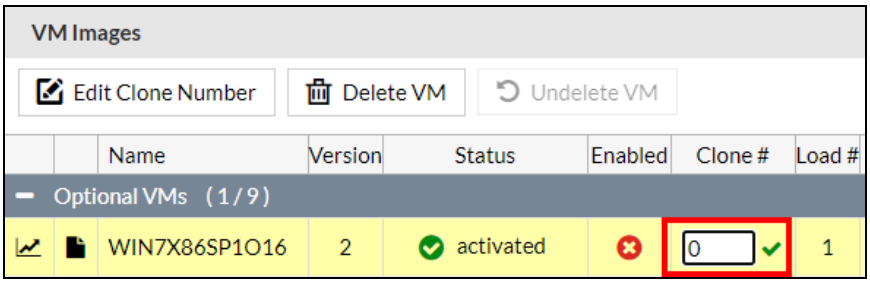


3. Click **Keep**.
4. Close Chrome.
5. Return to the FortiSandbox GUI, and then click **Scan Job** > **VM Jobs**.
   The VM scanning progress is displayed.

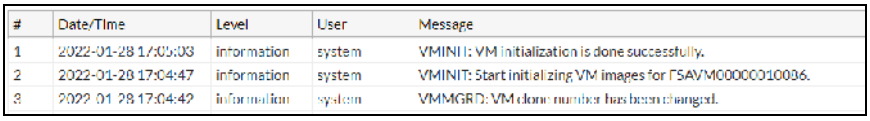


If FortiSandbox generates a verdict *without* displaying a VM scanning progress, then you *must* reinitialize the guest VM image. To reinitialize the guest VM, do the following:

1. Click **Scan Policy and Object** > **VM Settings**.
2. Double-click the **WIN7X86SP1O16** entry.
3. Change the **Clone #** value to `0`, and then click the check mark.



4. Click **Apply**.
5. Double-click the **WIN7X86SP1O16** entry again.
6. Change the **Clone #** value to `1`, then click the check mark.
7. Click **Apply**.
8. Click **Log & Report** > **Events** > **VM Events**.
9. Verify that the guest VM is successfully initialized before continuing:

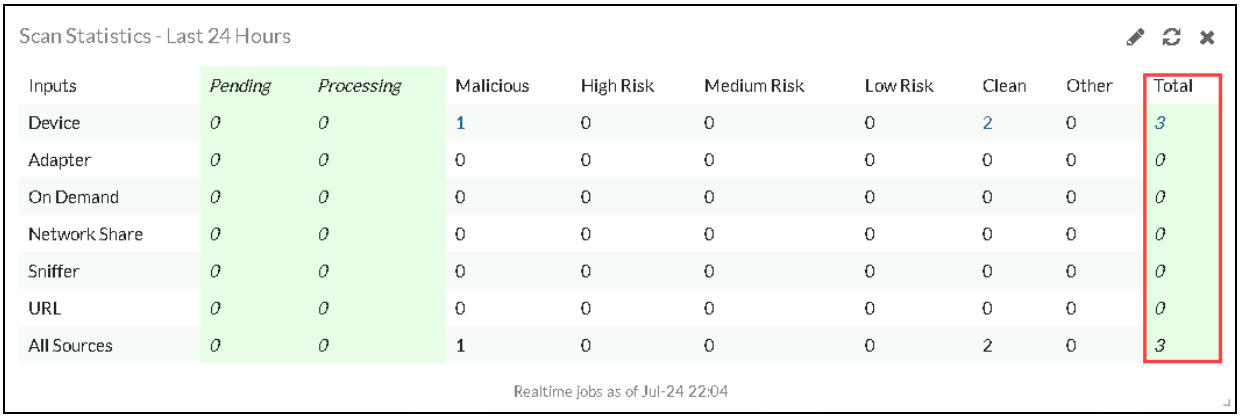


#	Date/Time	Level	User	Message
1	2022-01-28 17:05:03	information	system	VMINIT: VM initialization is done successfully.
2	2022-01-28 17:04:47	information	system	VMINIT: Start initializing VM images for FSAVM00000010006.
3	2022-01-28 17:04:42	information	system	VMMGRD: VM clone number has been changed.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

6. Wait for the scan to finish, and then click **Dashboard** > **Status**.
7. In the **Scanning Statistics** widget, review the **Device(s)** column.

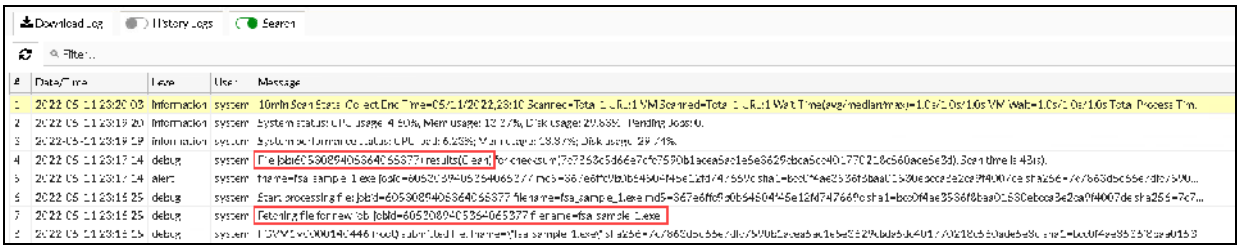


Scan Statistics - Last 24 Hours

Inputs	Pending	Processing	Malicious	High Risk	Medium Risk	Low Risk	Clean	Other	Total
Device	0	0	1	0	0	0	2	0	3
Adapter	0	0	0	0	0	0	0	0	0
On Demand	0	0	0	0	0	0	0	0	0
Network Share	0	0	0	0	0	0	0	0	0
Sniffer	0	0	0	0	0	0	0	0	0
URL	0	0	0	0	0	0	0	0	0
All Sources	0	0	1	0	0	0	2	0	3

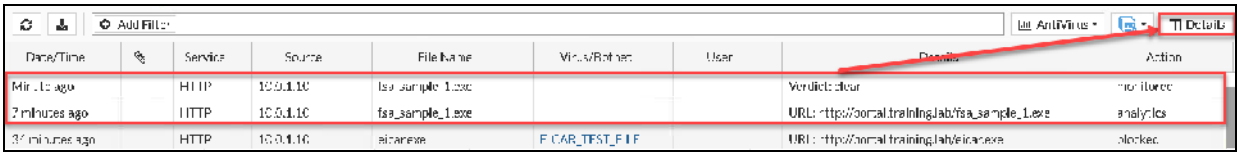
Realtime jobs as of Jul-24 22:04

8. Click **Log & Report** > **Events** > **Job Events**.
9. Review the logs for the `fsa_sample_1.exe` file.



The file generates a clean verdict.

10. Return to the FortiGate GUI, and then click **Log & Report** > **Security Events** > **AntiVirus**.
11. Review the log details for the `fsa_sample_1.exe` file.



Why are there two logs for the same file?

FortiGate generates the first log after the analytics engine determines that the file requires sandboxing. The second log is generated when FortiSandbox returns a verdict.

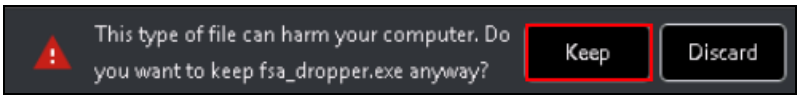
It can take up to five minutes after FortiSandbox has finished scanning the file for the verdict log to be generated. Click the refresh icon ( ) to refresh the log view.

To verify sandbox inspection with high-risk samples

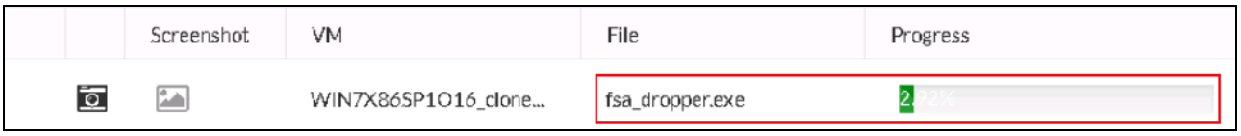
1. Return to the Local-Host VM, open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
2. Click **Dropper**.
   A security warning is displayed.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

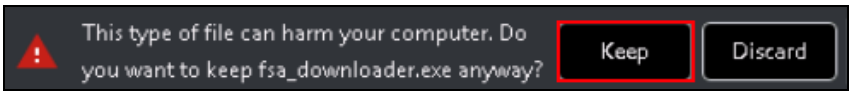


3. Click **Keep**.
4. Close Chrome.
5. Return to the FortiSandbox GUI, and then click **Scan Job** > **VM Jobs**.
   The VM scanning progress is displayed.

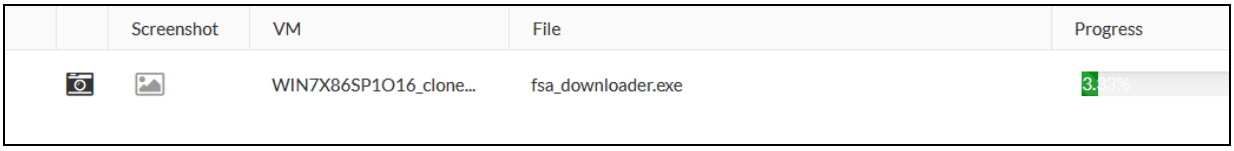


6. After the scanning is complete, click **Dashboard** > **Operation Center**.
7. Verify that the sample received a high risk verdict.

8. Return to the Local-Host VM, open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
9. Click **Downloader**.
   A security warning is displayed.



10. Click **Keep**.
11. Close Chrome.
12. Return to the FortiSandbox management GUI, and then click **Scan Job** > **VM Jobs**.
    The VM scanning progress is displayed.



13. Wait for the scan to complete, and then log out of the FortiSandbox management GUI.
14. Return to the Local-Host VM, and then open Thunderbird.
15. Click **admin@acmecorp.net** > **Inbox**.
16. Review the alert email for the `fsa_downloader.exe` file.
17. Click the URL in the alert email.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com


```
Source IP: 10.0.1.10
Destination IP: 100.64.1.10
Scan Start Time: 2022-05-02 22:00:41
Scan Finish Time: 2022-05-02 22:01:54
Scan Time: 73 (seconds)
SHA256: 47fec447f4b02512edd4144e3441b25577454c72e36452aa7b6aea112b8fe6fa
SHA1: e2959d157dee3c354dedfcf9364136eea760a467
MD5: c71c15dc8975cee77437a781cdf15806
URL: https://10.200.4.213/job-detail/?jid=6039652417501760889


Sent from FortiSandBox (FSAVM00000010086) (10.200.4.213)
```

18. Log in with the username `admin` and password `password`.
    The scan job report is displayed.
19. Review the report. Make a note of the value in the **Rated By** field.

High Risk Downloader

Basic Information

Job ID:	6039652417501760889
Status:	Done
Received:	May 02 2022 22:00:39-07:00
Started:	May 02 2022 22:00:41-07:00
Rated By:	Dynamic Scan
Submit Type:	FortiGate
Submission Protocol:	OFTP
Source IP:	10.0.1.10
Destination IP:	100.64.1.10
Digital Signature:	No
AI Mode:	ON
SIMNET:	OFF
Virus Total:	

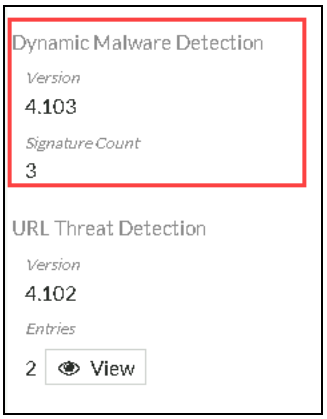
20. Close the scan job report browser tab.
21. Close Thunderbird.

To verify threat intelligence sharing

1. Return to the FortiGate GUI, and then click **Security Fabric** > **Fabric Connectors**.
2. Click **FortiSandbox**, and then click **Edit**.
3. Review the **Dynamic Malware Detection** and **URL Threat Detection** information.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



Why does the antivirus package (**Dynamic Malware Detection version**) loaded from FortiSandbox include only two signatures?

FortiSandbox includes signatures for only the files that generate malicious, high risk, and medium risk verdicts. So far, only the `fsa_downloader.exe` and `fsa_dropper.exe` files have generated a high risk verdict. A signature for the `fsa_sample_1.exe` file inspected by FortiSandbox is not included in this database because it generated a clean verdict. The `eicar.exe` file was detected locally by FortiGate, which is not part of the malware package.

To verify the FortiSandbox antivirus database

1. Return to the Local-Host VM.
2. Open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
3. Click **Dropper**.
   A block page is displayed.

4. Close Chrome.
5. Close the Local-Host VM browser tab.
6. Return to the FortiGate management GUI, and then click **Log & Report** > **Security Events** > **AntiVirus**.
7. View the log details for the `fsa_dropper.exe` file, and then review the information in the **Other** section.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Log Details

Other

Log event original timestamp	1651555179013252000
Timezone	-0700
Log ID	0211009234
Type	utm
Sub Type	virus
Event Type	infected
Source Interface Role	undefined
Destination Interface Role	wan
Direction	incoming
Quarantine Skip	Quarantine-disabled
Virus/Botnet	FSA/RISK_HIGH
Virus Category	Virus
Detection Type	fortisandbox
Reference	http://www.fortinet.com/ve?vn=FSA%2FRISI
Virus ID	8
Profile Name	AV-AcmeCorp
HTTP request method	GET
Referrer URI	http://portal.training.lab/
FortiSandbox Checksum	47fec447f4b02512edd4144e3441b25577
Submitted to FortiSandbox	true

The second attempt to download the `fsa_dropper.exe` file is blocked by FortiGate. FortiGate blocked the file using an antivirus signature (**FSA/RISK_HIGH**) that was generated by FortiSandbox as a result of scanning the file after the first download.

8. Log out of the FortiGate management GUI.
9. Close the FortiGate browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

Brave-Dumps.com

Exercise 2: Blocking URLs Based on FortiSandbox Threat Intelligence

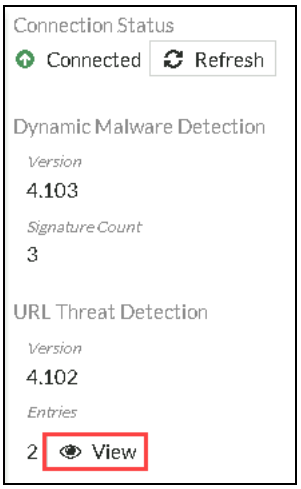
In this exercise, you will configure a web filter profile to block URLs that are reported as malicious by FortiSandbox.

Block URLs Based on FortiSandbox Threat Intelligence

First, you will verify the FortiSandbox URL package on FortiGate and the FortiGuard web filtering service. Then, you will configure a web filter profile and apply it to a firewall policy to block URLs that are reported as malicious by FortiSandbox.

To verify the FortiSandbox URL package on FortiGate

1. On the FortiGate management GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Fabric Connectors**.
3. Select **FortiSandbox**, and then click **Edit**.
4. In the **URL Threat Detection** section, click **View**.



The **Malicious URLs** pane is displayed.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

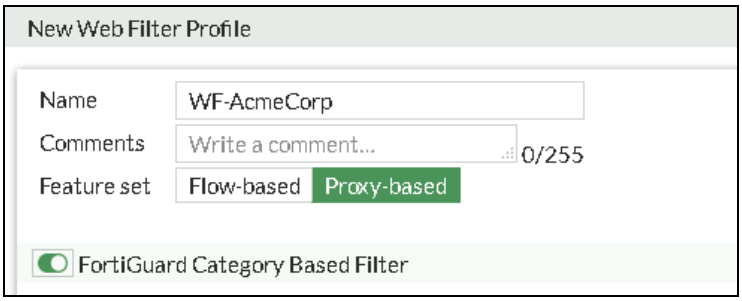
Brave-Dumps.com

These are the URLs that link directly to the `fsa_downloader.exe` and `fsa_dropper.exe` files that you downloaded in the previous exercise.

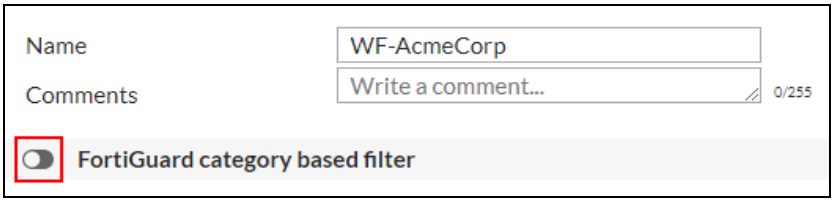
5. Click **X** to close the **Malicious URLs** pane.

To configure a web filter profile

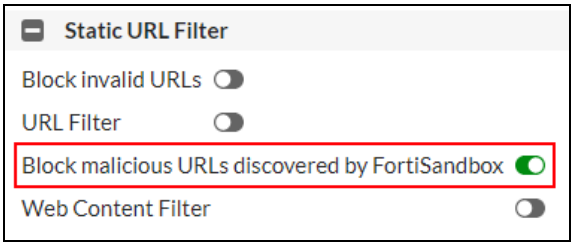
1. Continuing on the FortiGate management GUI, click **Security Profiles** > **Web Filter**.
2. Click **Create New**.
3. In the **Name** field, type `WF-AcmeCorp`.
4. In the **Feature set** section, make sure **Proxy-based** is selected.



5. Disable **FortiGuard category based filter**.



6. In the **Static URL Filter** section, enable **Block malicious URLs discovered by FortiSandbox**.



7. Click **OK**.

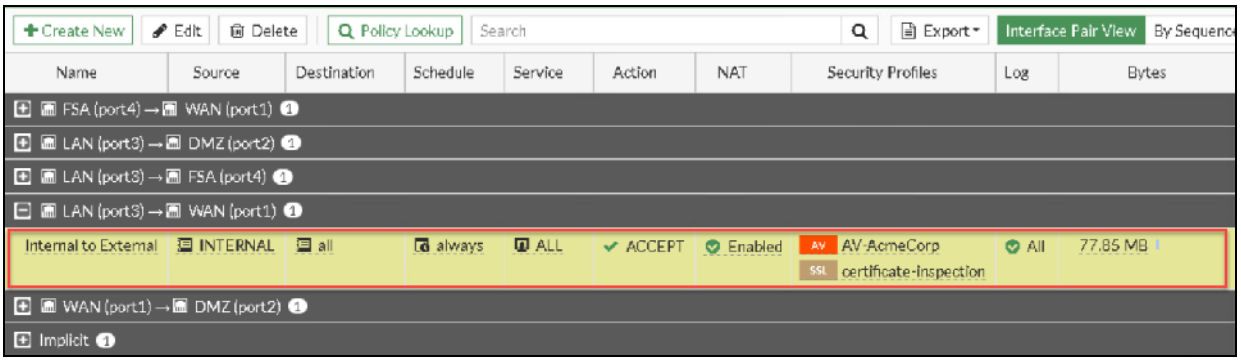
To apply the web filter profile to a firewall policy

1. Continuing on the FortiGate management GUI, click **Policy & Objects** > **Firewall Policy**.
2. In the **LAN(port3) - WAN(port1)** section, double-click the **Internal to External** firewall policy.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

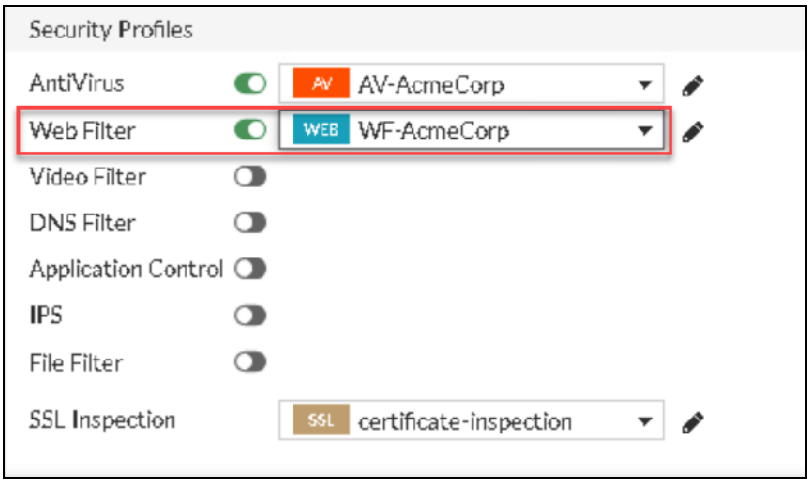
DO NOT REPRINT
© FORTINET

Brave-Dumps.com



3. Turn on **Web Filter**.
4. In the **Web Filter** drop-down list, select **WF-AcmeCorp**.

   The **Security Profiles** section for the policy should match the following example:

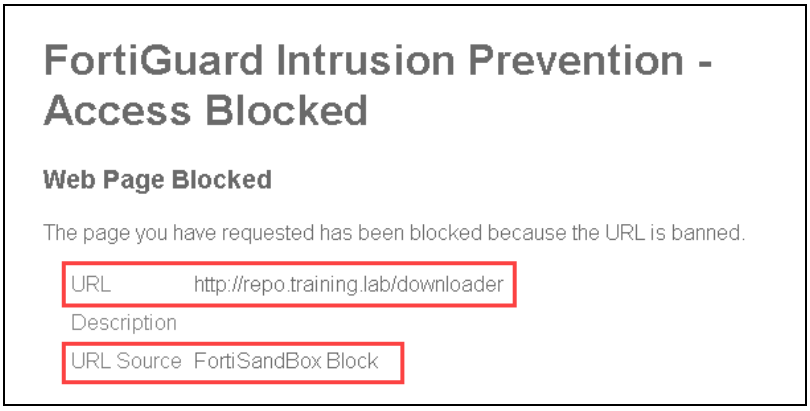


5. Click **OK**.

To verify malicious URL blocking

1. On the Local-Host VM, open a new Chrome browser tab, and then connect to `http://repo.training.lab/downloader`.

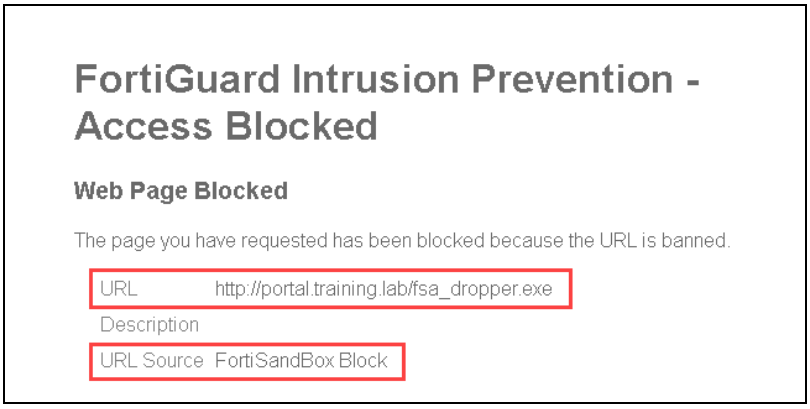
   A block page is displayed.



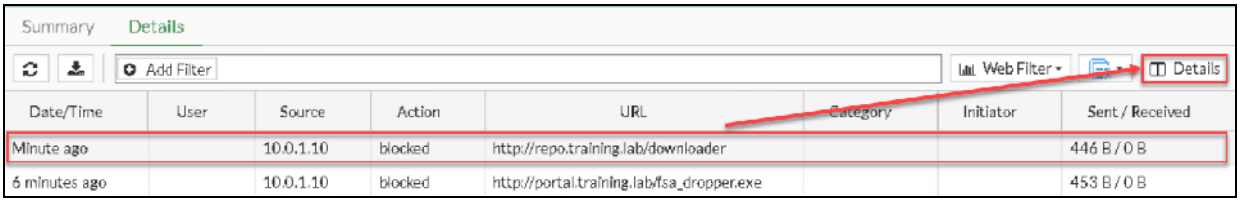
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

2. Continuing on Chrome browser, connect to `http://portal.training.lab/fsa_dropper.exe`. Another block page is displayed.



3. Close Chrome.
4. Close the Local-Host VM browser tab.
5. Return to the FortiGate management GUI, and then refresh the page.
6. Click **Log & Report** > **Security Events** > **Web Filter**.
7. Review the log details for the URL blocks.



8. Log out of the FortiGate management GUI.
9. Close the FortiGate browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 3: Using FortiGate Diagnostics

In this exercise, you will restore a configuration file on FortiGate, and then troubleshoot communication issues between FortiGate and FortiSandbox.

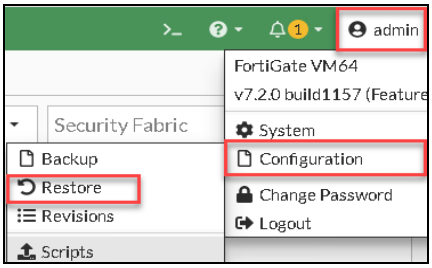
The configuration file introduces configuration issues on FortiGate. Use the troubleshooting methodology presented in this exercise to resolve the issues, instead of using the GUI to view the configuration.

Restore a Configuration File on FortiGate

You will restore a configuration file on FortiGate.

To restore the FortiGate configuration file

1. On the Local-Host VM, open a Firefox browser tab, and then log in to the FortiGate management GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Lab 4 - Protecting the Edge** > `Lab_4-3_FortiGate.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.
   Wait until the browser is redirected to the login page.
7. Close Firefox.

Verify FortiSandbox Communication

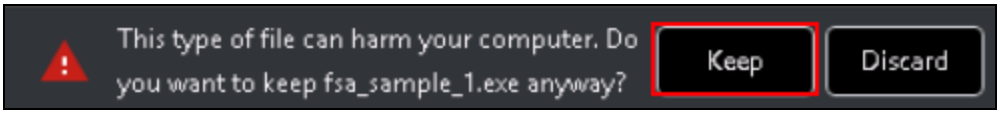
You will download a malware test sample that should be offloaded to FortiSandbox for inspection. Then, you will investigate whether or not the file was sent to FortiSandbox.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To download a malware sample

1. Open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
2. Click **Clean Sample**.
   A security warning is displayed.



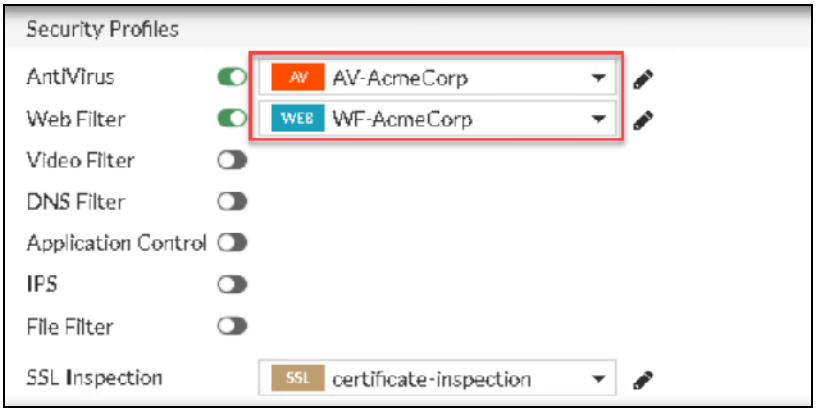
3. Click **Keep**.

In the last exercise, you verified that the `fsa_sample_1.exe` file generated a clean verdict. This means FortiSandbox will not include a signature for this file in its threat intelligence database. Therefore, FortiGate should send this file to FortiSandbox for analysis.

4. Close Chrome.

To verify FortiGate configuration

1. On the FortiGate management GUI, log in with the username `admin` and password `password`.
2. Click **Log & Report** > **Security Events** > **AntiVirus**.
   Do you see any new logs generated for the `fsa_sample_1.exe` file?
3. Click **Policy & Objects** > **Firewall Policy**.
4. Double-click the **Internal to External** policy.
5. Verify that the correct security profiles are applied to the policy.



To verify FortiSandbox configuration

1. On the FortiSandbox management GUI, log in with the username `admin` and password `password`.
2. Click **Log & Report** > **Events** > **Job Events**.
   There appear to be no scan jobs as a result of the `fsa_sample_1.exe` file download.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Diagnose the Problem

On the surface, it looks like the FortiGate configuration is correct. However, it also appears that FortiGate is not sending the `fsa_sample_1.exe` file to FortiSandbox. You must investigate further to diagnose the problem.

Take the Expert Challenge!

Use the following CLI debug commands to diagnose the connection and file transfer issue between FortiGate and FortiSandbox:

- Use `diagnose debug application quarantine -1` to debug connection issues.

Fix the configuration issues, and then verify your work by downloading the `fsa_sample_1.exe` file from the Malware Sample Portal (`http://portal.training.lab`). Then, review the FortiGate logs.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

To diagnose FortiGate file submission to FortiSandbox

1. Open an SSH connection to the FortiGate VM.
2. Type the following commands to enable debugging for the quarantine daemon:
```
diagnose debug application quarantine -1
diagnose debug enable
```
3. Wait a few seconds until the daemon debug output is displayed.
4. Type the following command to disable debugging:
```
di de di
```

FortiGate supports short forms for most CLI commands. These are especially useful when you are trying to type commands while a lot of debug output is scrolling by. The scrolling output might prevent you from seeing what you are typing. Using the short forms of the commands decreases the chances of making a mistake when you type CLI commands.

5. Review the debug messages.
```
__quar_start_connection()-908: start server fortisandbox-fsb3-10.1.0.213 in vdom-0
[104] __ssl_cert_ctx_load: Added cert /etc/cert/factory/root_Fortinet_Factory.cer, root ca Fortinet_CA, idx 0 (default)
[104] __ssl_cert_ctx_load: Added cert /etc/cert/factory/root_Fortinet_Factory_Backup.cer, root ca Fortinet_CA_Backup, idx 1
[552] ssl_ctx_create_new_ex: SSL CTX is created
[579] ssl_new: SSL object is created
[640] ssl_set_hostname: Set hostname 'fortinet-ca2.fortinet.com'
quar_monitor_connection_func()-982: monitoring dev fortisandbox-fsb4
quar_restart_connection()-1002: restart connection to server(fortisandbox-fsb4)
quar_stop_connection()-1010: close connection to server(fortisandbox-fsb4)
[194] __ssl_data_ctx_free: Done
[839] ssl_free: Done
```

It appears that FortiGate cannot establish a connection with FortiSandbox.

To resolve the connectivity issue

1. Continuing on the FortiGate CLI, type the following command to view the FortiSandbox integration settings:
```
show system fortisandbox
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

2. Review the configuration.

```
config system fortisandbox
    set status enable
    set server "10.1.0.213"
end
```

Can you identify the issue?

3. Type the following commands to fix the server IP address:

```
config system fortisandbox
   set server 10.0.1.213
end
```

Verify the fix

1. Continuing on the FortiGate CLI, type the following commands to re-enable debugging for the quarantine daemon:

```
diagnose debug enable
```

Wait until the following output is displayed:

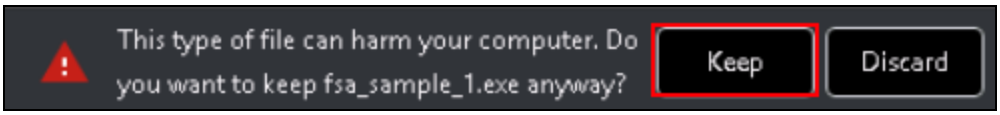
```
quar_monitor_connection_func()-982: monitoring dev fortisandbox-fsb1
quar_monitor_connection_func()-982: monitoring dev fortisandbox-fsb2
quar_monitor_connection_func()-982: monitoring dev fortisandbox-fsb3
quar_monitor_connection_func()-982: monitoring dev fortisandbox-fsb4
quar_monitor_connection_func()-982: monitoring dev fortisandbox-fsb5
quar_monitor_connection_func()-982: monitoring dev fortisandbox-fsb6
```

2. Type the following command to disable debugging for all daemons:

```
diagnose debug reset
```

3. Close the FortiGate SSH session browser tab.
4. Return to the Local-Host VM.
5. Open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
6. Click **Clean Sample**.

A security warning is displayed.



7. Click **Keep**.
8. Close Chrome.
9. Return to the FortiSandbox management GUI, and then click **Log & Report** > **Events** > **Job Events**.
10. Review the logs.

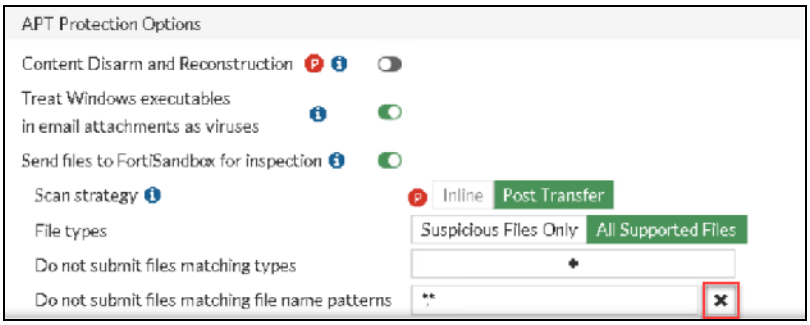
Are there any new logs related to the `fsa_sample_1.exe` file?

To fix the antivirus profile configuration

1. Return to the FortiGate management GUI, and then click **Security Profiles** > **AntiVirus**.
2. Double-click the **AV-AcmeCorp** profile.
3. In the **APT Protection Options** section, click **X** to remove the wildcard filename pattern.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

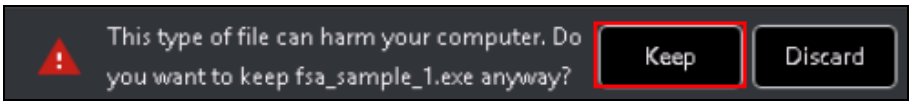
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



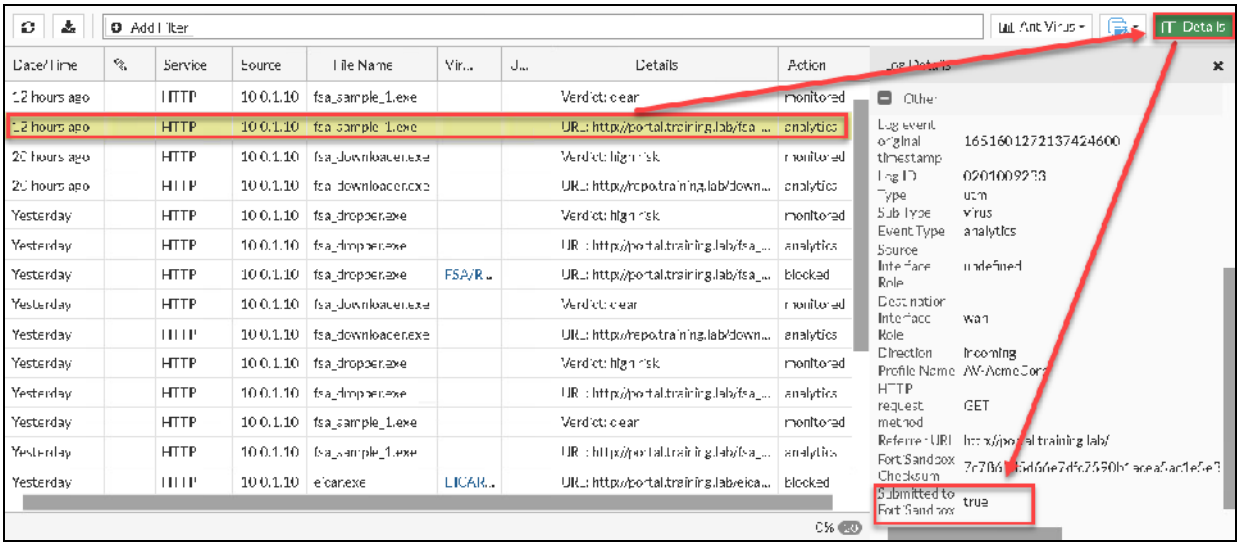
4. Click **OK**.

To verify the fix

1. Return to the Local-Host VM.
2. Open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
3. Click **Clean Sample**.
   A security warning is displayed.



4. Click **Keep**.
5. Close Chrome.
6. Return to the FortiGate management GUI, and then click **Log & Report** > **Security Events** > **AntiVirus**.
7. Review the latest logs generated for the `fsa_sample_1.exe` file, and then verify that the file was sent to FortiSandbox.



8. Log out of the FortiGate management GUI.
9. Return to the FortiSandbox management GUI, and then click **Log & Report** > **Events** > **Job Events**.
10. Verify that FortiSandbox received and started processing the file.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

#	Date/Time	Level	User	Message
11	2022-05-03 11:07:5...	debug	system	File job(6040463855756372588) results(Clean) for checksum(7c7863d5d66e7dfc7590b1acea5ac1e5e3629cbda5dc401...
12	2022-05-03 11:07:5...	alert	system	fname=fsa_sample_1.exe duplicated=true jobid=6040463855756372588 md5=367e6ffc9b0b64504f45e12fd747669c ...
13	2022-05-03 11:07:5...	debug	system	Start processing file: jobid=6040463855756372588 filename=fsa_sample_1.exe md5=367e6ffc9b0b64504f45e12fd7476...
14	2022-05-03 11:07:5...	debug	system	Fetching file for new job. jobid=6040463855756372588 filename=fsa_sample_1.exe
15	2022-05-03 11:07:5...	debug	system	FGVM1V0000140446 (root) submitted file. fname=\"fsa_sample_1.exe\" sha256=7c7863d5d66e7dfc7590b1acea5ac1e...

11. Log out of the FortiSandbox management GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 4: Using Inline Scanning

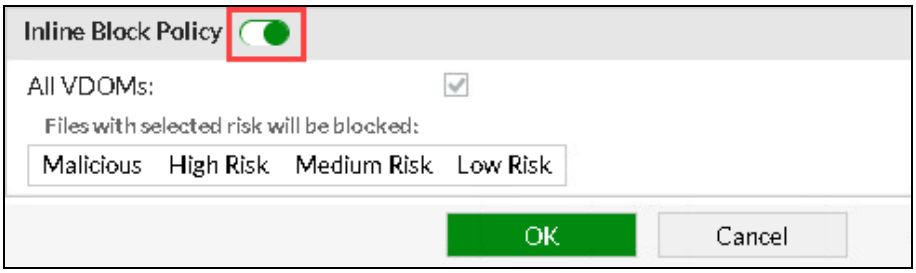
In this exercise, you will perform basic configuration on FortiGate and FortiSandbox to enable inline scanning. You will then verify your configuration using a clean file sample and observe the behavior of FortiSandbox.

Configure Inline Scanning on FortiSandbox

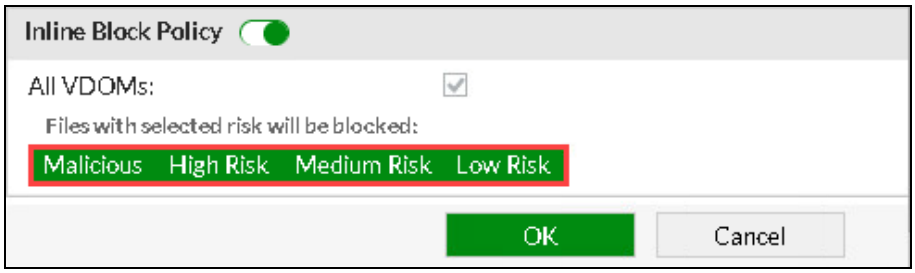
You will configure the settings to enable inline scanning on FortiSandbox.

To enable inline scanning on FortiSandbox

1. On the FortiSandbox GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Device**.
3. Click **FortiGate**.
4. Enable **Inline Block Policy**.



5. Select the risk levels that will be blocked: **Malicious**, **High Risk**,**Medium Risk**, and **Low Risk**.



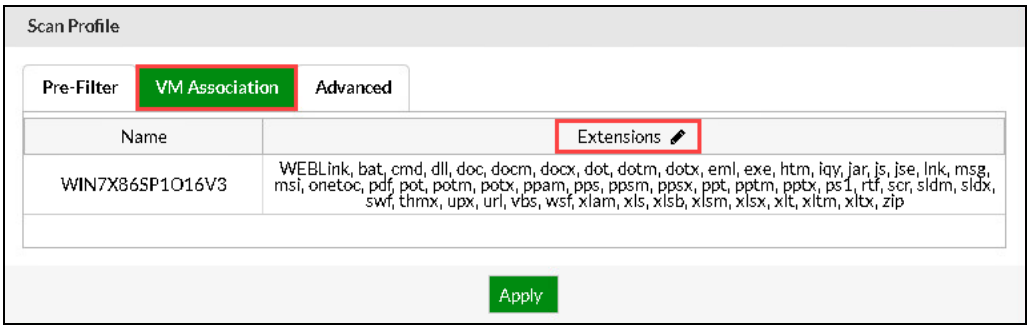
6. Click **OK**.

To modify the scan profile

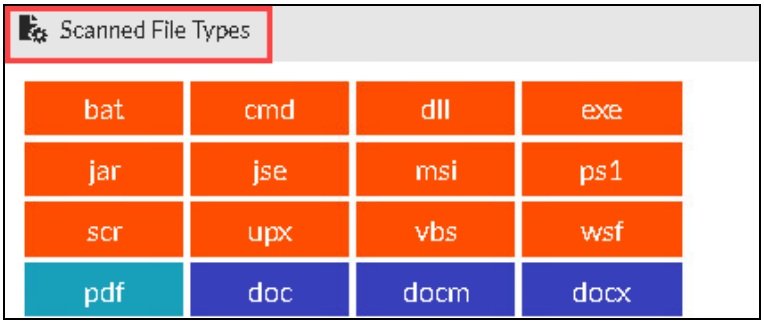
1. Continuing on the FortiSandbox GUI, click **Scan Policy and Object** > **Scan Profile**.
2. Click the **VM Association** tab and, in the **Extensions** column, click the edit icon (✎).

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

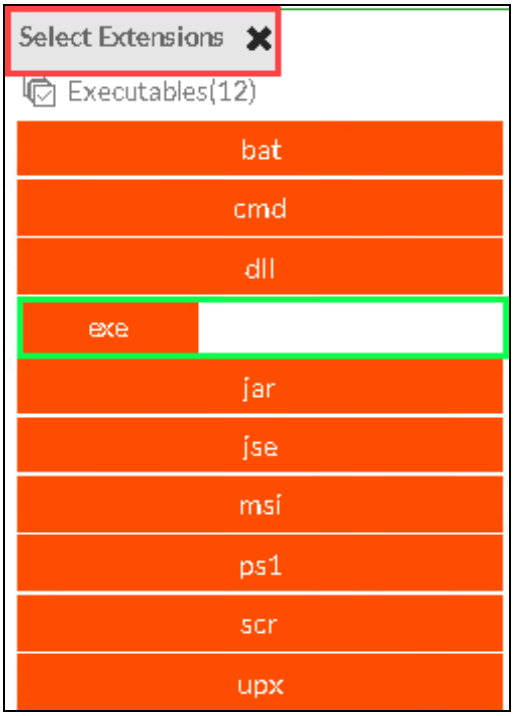
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. In the **WIN7X86SP1O16** section, click the **Scanned File Types** section.



4. In the **Select Extensions** pane, under the **Executables**category, disable **exe**.



5. Click **Apply**
6. Click **Log & Report** > **Events** > **VM Events**.
7. Verify that the scan profile was updated successfully.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

#	Date/Time	Level	User	Message
1	2022-04-28 23:16:14	information	admin	Scan Profile was updated successfully.
2	2022-04-28 23:15:54	information	admin	Scan Profile was updated successfully.
3	2022-04-28 23:15:13	information	system	VMINIT: Start initializing VM images for FSAVM00000010086.
4	2022-04-28 23:15:08	information	system	VMMGRD: VM profile has been changed.

Because of the inline scanning time out limit (maximum of 50 seconds), it's not recommended to submit files for VM inspection.

To grant access rights on FortiSandbox port2

1. Open an SSH session to the FortiSandbox VM.
2. Type the following commands to enable API access on **port2**:

```
set api-port port2
```

FortiGate and FortiSandbox communicate through port 4443. Management or API ports grant access through port 4443.

Configure Inline Scanning on FortiGate

You will configure the settings required to enable inline scanning on FortiGate.

To enable inline scanning on FortiGate

1. Open an SSH session to the FortiGate VM.
2. Type the following commands to enable Inline Scanning globally:

```
config system fortisandbox
   set inline-scan enable
end
```

To configure an antivirus profile for inline scanning

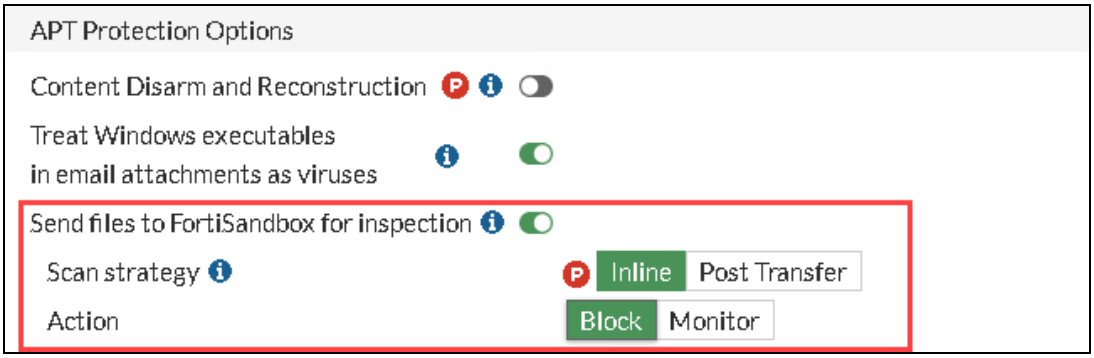
1. On the FortiGate GUI, log in with the username `admin` and password `password`.
2. Click **Security Profiles** > **Antivirus**.
3. Double-click **AV-AcmeCorp**
4. In the **APT Protection Options** section, under**Send files to FortiSandbox for inspection**, configure the following settings:

Field	Value
Scan strategy	Inline
Action	Block

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Your configuration should match the following example:



5. Click **OK**.

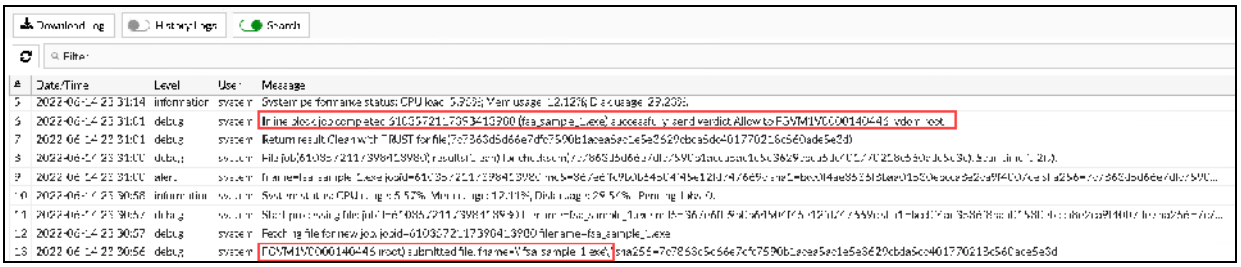
Verify Inline Scanning Inspection

You will verify inline scanning inspection using a file sample.

To verify inline scanning

1. Open an SSH session to the FortiSandbox VM.
2. Enter the following commands to enable inline scanning real-time debug:
   `diagnose-debug inline-block`
3. On the Local-Host VM, open Google Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
4. Click **Clean Sample**.
   A security warning appears.

5. Click **Keep**
6. Close Chrome.
7. Return to the FortiSandbox GUI, and then click **Log & Report** > **Events** > **Job Events**.
8. Review the logs generated by inline scanning.



Notice that FortiGate submitted the file `fsa_sample1.exe` and an inline block job was completed.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

9. Return to the FortiSandbox SSH session.
10. Review the debug output.

```
FortiSandbox> diagnose-debug inline-block
06/14 23:30:56 (.538) DEBUG [24750] main.cpp        :_get_size_limit:868 ;      File size limitation 300
06/14 23:30:56 (.538) DEBUG [24750] main.cpp        :scan_file      :777 ;      ===> scan_file
06/14 23:30:56 (.538) DEBUG [24750] main.cpp        :get_post_data  :307 ;      ---> get_post_data
06/14 23:30:56 (.538) DEBUG [24750] main.cpp        :get_post_data  :411 ;      <=== get_post_data 5597 saved 1
06/14 23:30:56 (.538) DEBUG [24750] main.cpp        :fetch_results  :651 ;      ---> fetch_result
06/14 23:30:56 (.538) DEBUG [24750] main.cpp        :_handle_commit_:465 ;      Save SID: 6103572117390413D80 to
meta file /drive0/private/temp/fgtpre/scnf/6103572117390413580.meta
06/14 23:30:56 (.539) DEBUG [24750] main.cpp        :_handle_commit_:469 ;      Save JID: 6103572117390413D80 to
meta file /drive0/private/temp/fgtpre/scnf/6103572117390413580.meta
06/14 23:30:56 (.539) DEBUG [24750] main.cpp        :_commit_file   :658 ;      fsa_sample1.exe file saved and ready for scan
06/14 23:30:56 (.539) DEBUG [24750] data_util.cpp   :get_verdict_rec:350 ;      ---> get_verdict_result_db
06/14 23:31:01 (.544) DEBUG [24750] utils.cpp       :_fsa_suspicious:536 ;      returns result with 0 for file(7c7563d5d65a7dfa
759Cb1aceaSac1eSe3529cbda5dc401770210c500adc5e3d), finish time: 2022-06-14 23:31:00, last update time: 2022-06-14 22:31:10
06/14 23:31:01 (.544) DEBUG [24750] data_util.cpp   : check_db       :345 ;      score=1,severity=Unknown
06/14 23:31:01 (.544) DEBUG [24750] main.cpp        :fetch_results  :765 ;      Verdict Result is(file_id:"7c7563d5d65a7dfa759
b1acca5ac1e5e3529cbda5dc401770210c500adc5e3d","virus_name":"N/A","severity":"Clean","verdict":"Allow","category":"Unknown","file_type":"exe")
06/14 23:31:01 (.544) DEBUG [24750] main.cpp        :scan_file      :826 ;      <=== scan_file
```

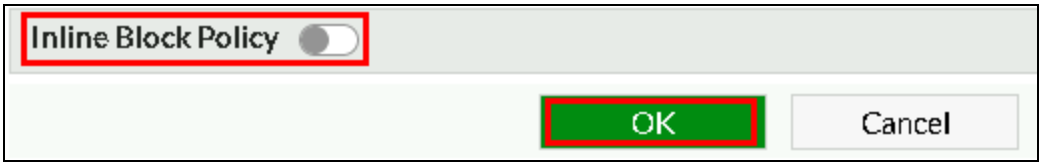
Notice that FortiSandbox received the file `fsa_sample1.exe` and generated a `Clean` verdict.

Disable Inline Scanning

You will disable inline scanning before proceeding to the next lab exercise.

To disable inline scanning on FortiSandbox

1. Continuing on the FortiSandbox GUI, click **Security Fabric** > **Device**
2. Click **FortiGate**.
3. Disable **Inline Block Policy**.
4. Click **OK**.



To restore the scan profile

1. Continuing on the FortiSandbox GUI, click **Scan Policy and Object** > **Scan Profile**.
2. Click the **VM Association** tab and, in the **Extensions** column, click the edit icon (✎).
3. In the **WIN7X86SP1O16** section, click the **Scanned File Types** section.
4. In the **Select Extensions** pane, under the **Executables**category, enable **exe**.
5. Click **Apply**
6. Log out of the FortiSandbox GUI.
7. Log out of the FortiGate GUI.
8. Close the FortiSandbox SSH session browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 5: Email Network Protection

In this lab, you will configure FortiMail to submit files to FortiSandbox. You will verify your configuration using multiple malware samples.

Objectives

- Configure FortiMail to submit files to FortiSandbox for inspection
- Configure quarantine release rescanning
- Monitor FortiSandbox inspection results and statistics for the inspected files

Time to Complete

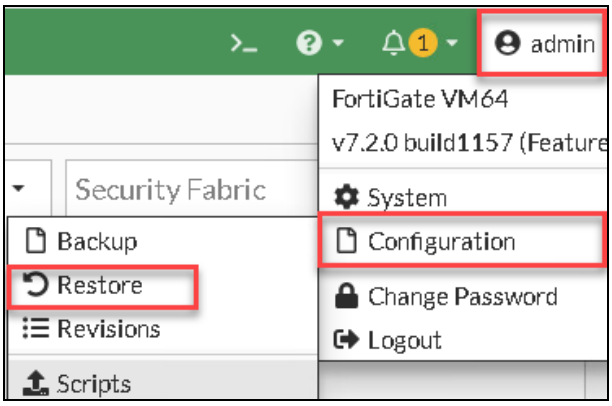
Estimated: 60 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file to FortiGate.

To restore the FortiGate configuration file

1. On the Local-Host VM, open a Firefox browser tab, and then log in to the FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Lab 5 - Protecting Email Networks** > `Lab_5_FortiGate.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.
   Wait until the browser is redirected to the login page.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Integrating FortiSandbox With FortiMail

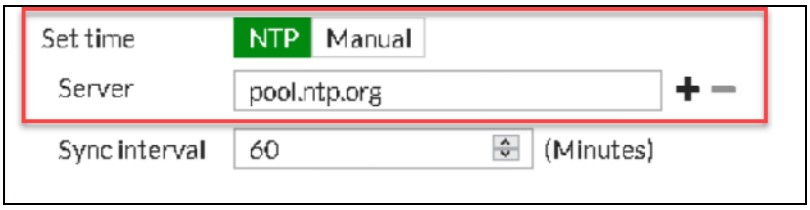
In this exercise, you will integrate FortiSandbox with FortiMail. You will configure FortiMail antivirus inspection to offload files and URLs to FortiSandbox. Then, you will verify your configuration using various malware samples.

Configure the FortiMail System Time

You will configure the system time zone and enable synchronization with a custom NTP server on FortiMail.

To configure the system time

1. On the FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Configuration**.
3. In the **Time zone** drop-down list, select your local time zone.
4. Click **NTP**.
5. Change the **Server** field to `pool.ntp.org`.



6. Click **Apply**.

As the FortiMail system time updates, you may be logged out of your existing browser session. If this happens, log back in with the username `admin` and password `password`.

Configure FortiSandbox Integration

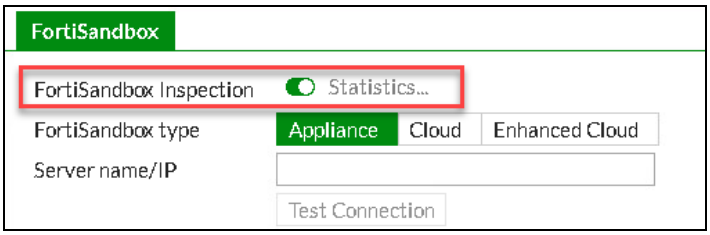
You will configure the settings required to integrate FortiMail with FortiSandbox. Then, you will authorize FortiMail on FortiSandbox and verify the connectivity between the two devices.

To configure FortiSandbox settings on FortiMail

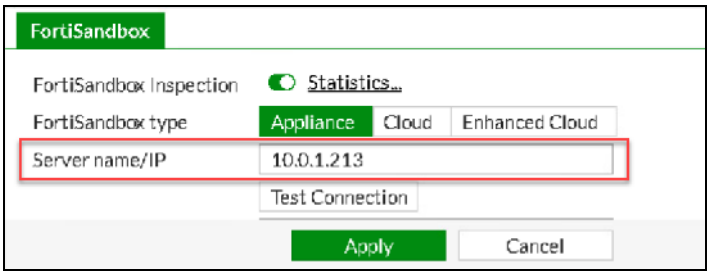
1. Continuing on the FortiMail management GUI, click **System** > **FortiSandbox**.
2. Turn on **FortiSandbox Inspection**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. In the **Server name/IP** field, type `10.0.1.213`.



Because you already configured the alert email settings on FortiSandbox, you will not configure the **Notification email** setting. Configuring this setting on FortiMail will duplicate the alert emails.

4. Click **Apply**.
5. Click **Test Connection**.

   An error message is displayed.

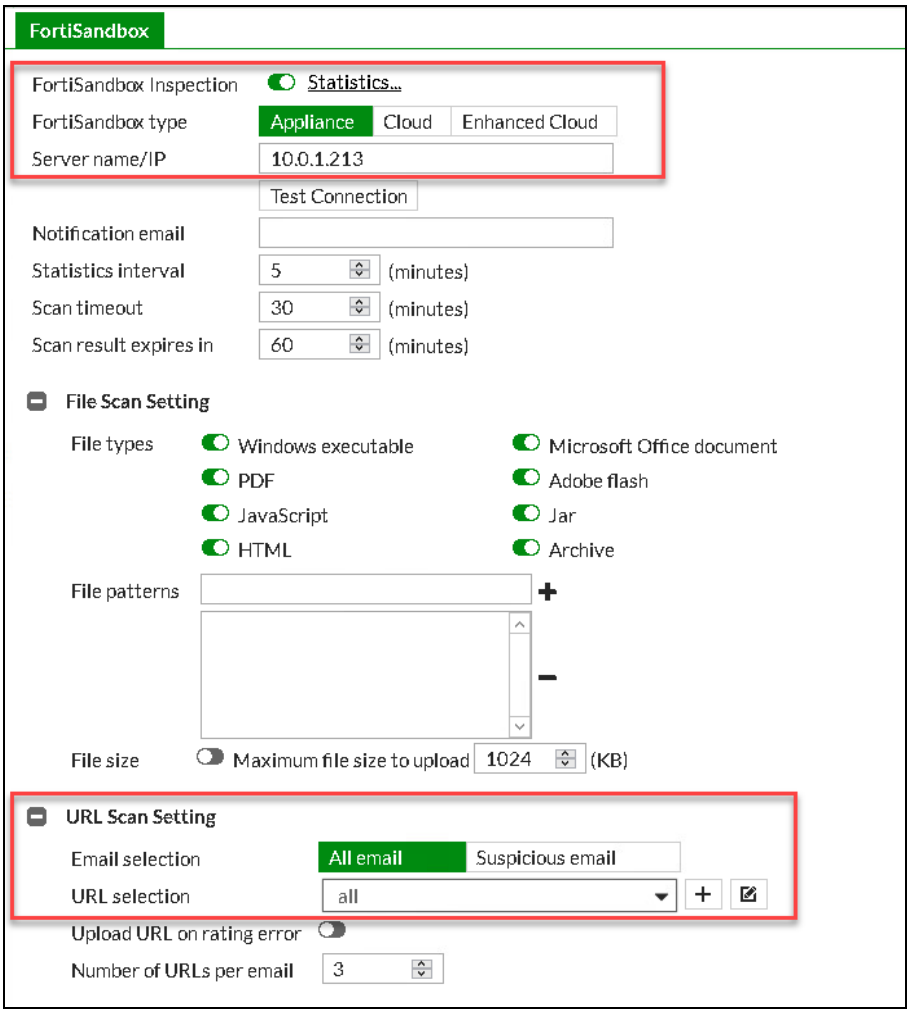
6. Click **OK**.
7. In the **URL Scan Settings** section, configure the following settings:

Field	Value
Email selection	All email
URL selection	all

8. Your configuration should match the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

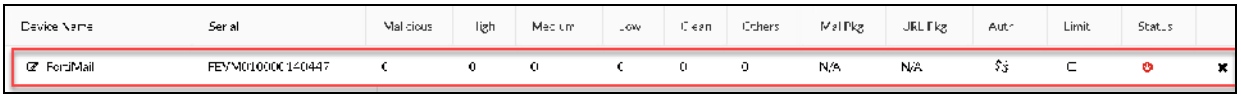
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



9. Click **Apply**.

To authorize FortiMail on FortiSandbox

1. On the FortiSandbox GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Device**.
3. Click **FortiMail**.

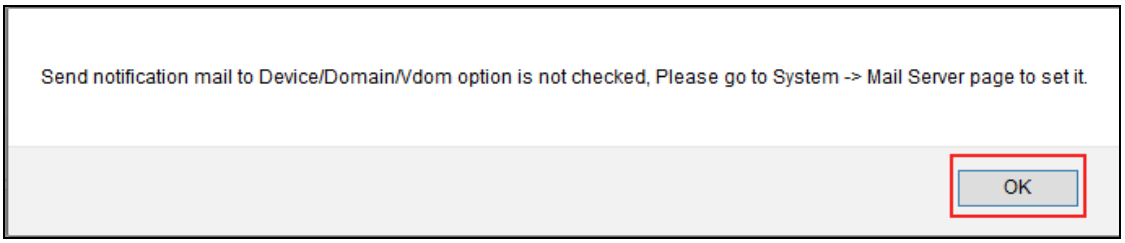


4. In the **Permissions & Policy** section, select the **Authorized** checkbox.

5. Click **OK** to accept the pop-up notification.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



6. Click **OK**.

To verify connectivity between FortiMail and FortiSandbox

1. Return to the FortiMail management GUI, and then click **Test Connection**.
   A success message is displayed.

2. Click **OK**.

Configure FortiMail for Sandboxing

To enable sandboxing, you will configure an antivirus profile, and then apply it to a recipient policy.

Take the Expert Challenge!

Create a new antivirus profile and name it `AV-AcmeCorp-Inbound`.

For the antivirus profile configuration, confirm the following:

- The profile is available for the **acmecorp.net** domain only.
- The profile uses the preconfigured **FSA-Replace** action profile.
- All FortiMail virus detection features are disabled.
- FortiSandbox attachment and URL analysis is enabled.
- Emails with malicious or high-risk verdicts are discarded.

Enable the **AV-AcmeCorp-Inbound** antivirus profile on the existing recipient policy that is configured for *all* `acmecorp.net` inbound emails.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

After you complete the challenge, see Verify Sandbox Inspection on page 68

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To configure an antivirus profile

1. Continuing on the FortiMail management GUI, click **Profile** > **AntiVirus**.
2. Click **New**.
3. Configure the following settings:

Field	Value
Domain	acmecorp.net
Profile name	AV-AcmeCorp-Inbound
Default action	FSA-Replace

The **FSA-Replace** action profile has been preconfigured to remove any malicious content in attachments or the body of an email before delivering the email to the recipient.

4. In the **Antivirus** section, configure the following settings:

Field	Value
Antivirus	disabled
Malware/virus outbreak	disabled
Heuristic	disabled
Grayware	disabled

5. In the **FortiSandbox** section, configure the following settings:

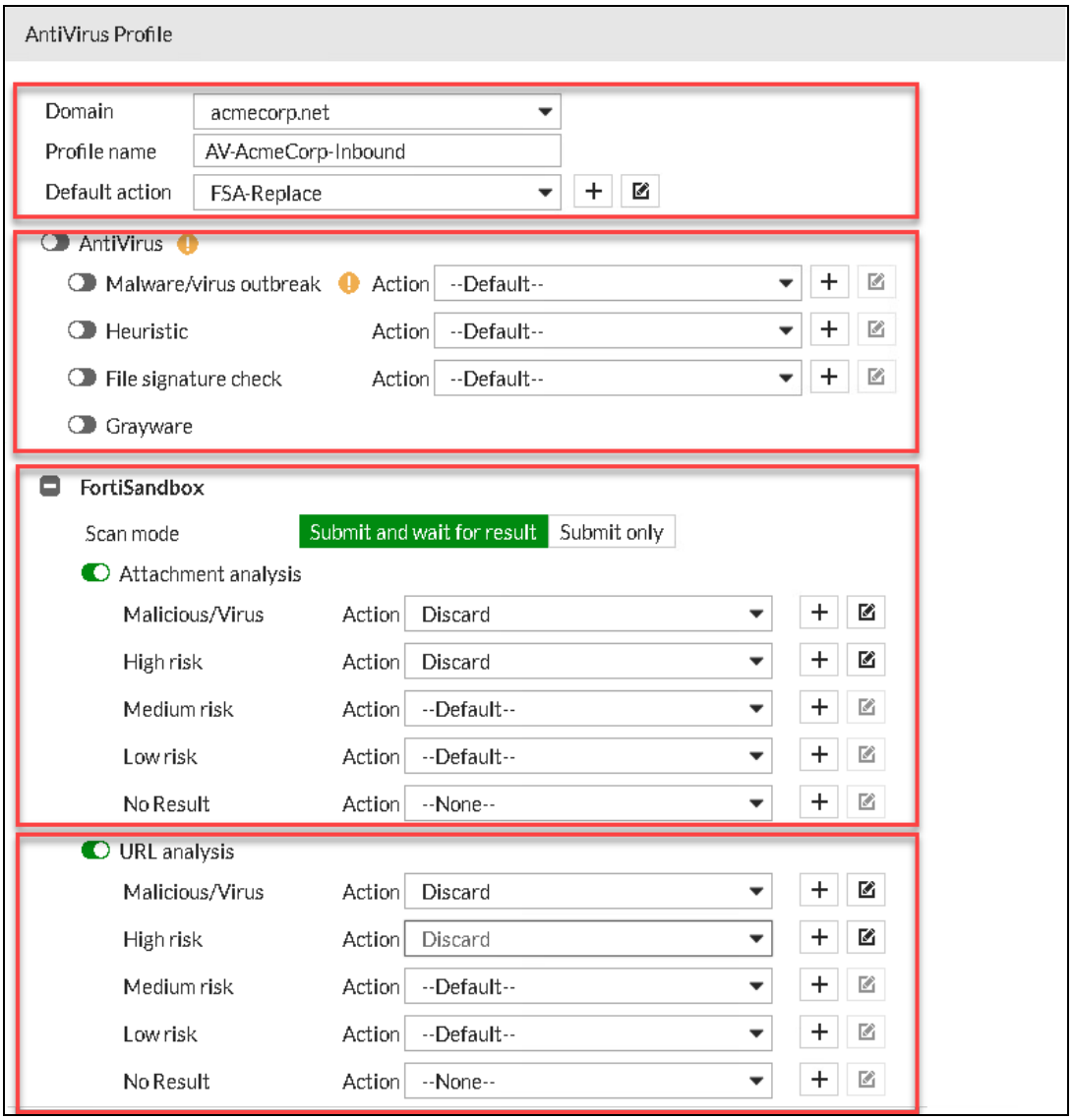
Field	Value
Attachment analysis	enabled
Malicious/Virus	Discard
High risk	Discard

Field	Value
URL analysis	enabled
Malicious/Virus	Discard
High risk	Discard

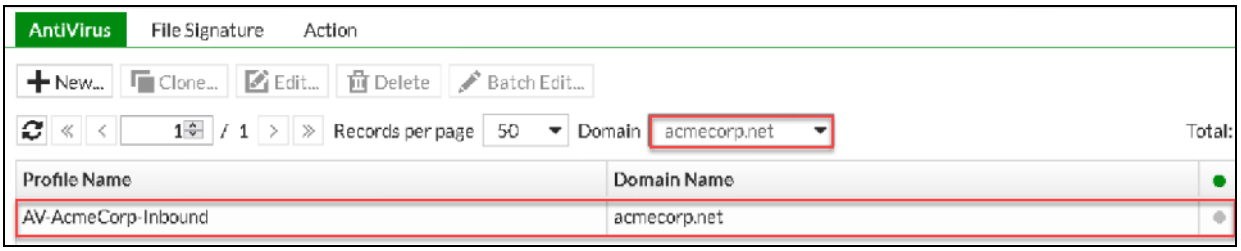
Your configuration should match the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



6. Click **Create**.
7. In the **Domain** drop-down list, select **acmecorp.net**.
8. Verify that the **AV-AcmeCorp-Inbound** antivirus profile is displayed.

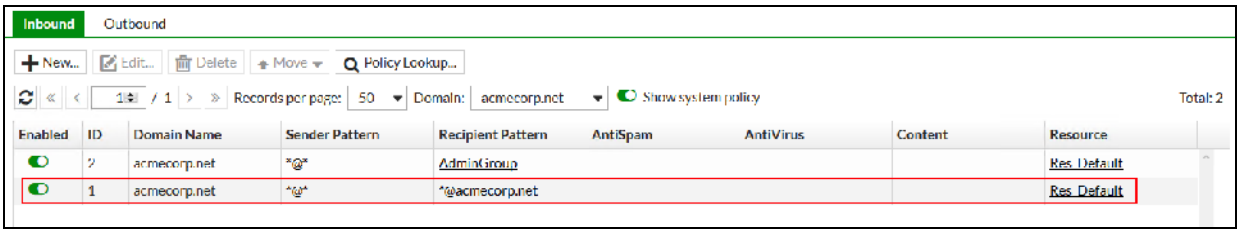


To apply the antivirus profile to a recipient policy

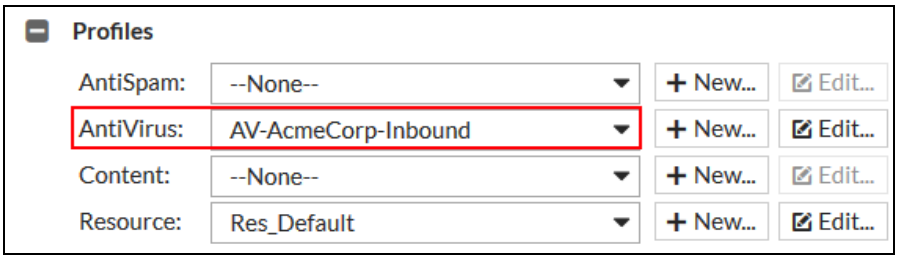
1. Continuing on the FortiMail management GUI, click **Policy** > **Recipient Policy**.
2. Double-click policy ID **1**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

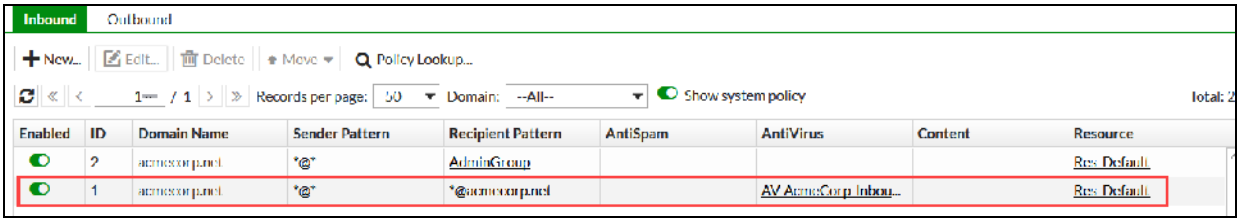
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. In the **Profiles** section, in the **AntiVirus** drop-down list, select **AV-AcmeCorp-Inbound**.



4. Click **OK**.
5. Your configuration should match the following example:



Verify Sandbox Inspection

You will verify sandbox inspection using various malware samples. You will also use the ATP Email Sender application, installed on Remote-Host, to generate emails containing a link to a malicious executable file.

To send an email with a high risk sample

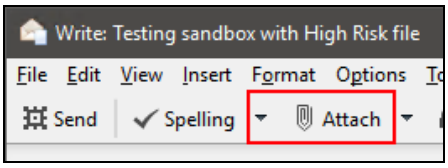
1. On the Local-Host VM, open Thunderbird.
2. Click **alice@acmecorp.net** > **Inbox**.
3. Click **Write**.
4. Compose a new email message using the following values:

Field	Value
To	bob@acmecorp.net
Subject	Testing sandbox with High Risk file
Message body	This email should be discarded.

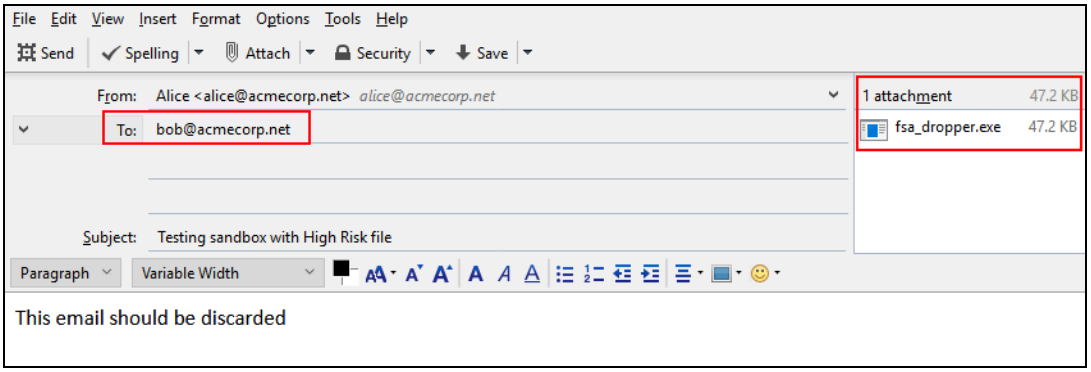
5. Click **Attach**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



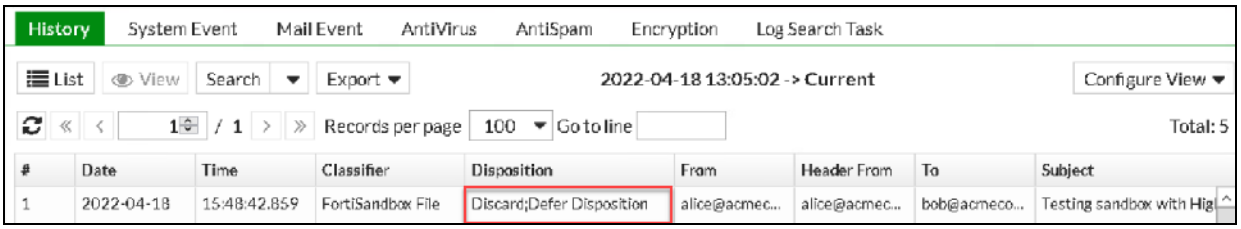
6. Click **Desktop** > **Resources** > **Lab 5 - Protecting Email Networks** > `fsa_dropper.exe`, and then click **Open**.
7. Your email should match the following example:



8. Click **Send**.
   Wait until the email is sent.
9. Close Thunderbird.

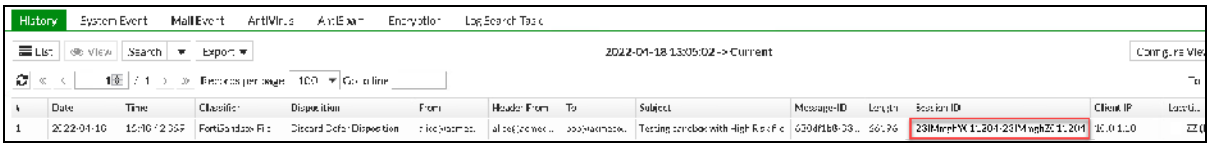
To validate sandbox inspection of a high-risk sample

1. Return the FortiMail management GUI, and then click **Monitor** > **Log**.
   Wait a few minutes for the log to appear.
2. Click the refresh icon (🔄) to force an update.
3. Review the **Disposition** column of the history log entry for the email.



The **Defer Disposition** action indicates that the mail was queued while FortiMail queried FortiSandbox. After FortiMail received the verdict from FortiSandbox, it applied the **Discard** action to the email.

4. Click the session ID.

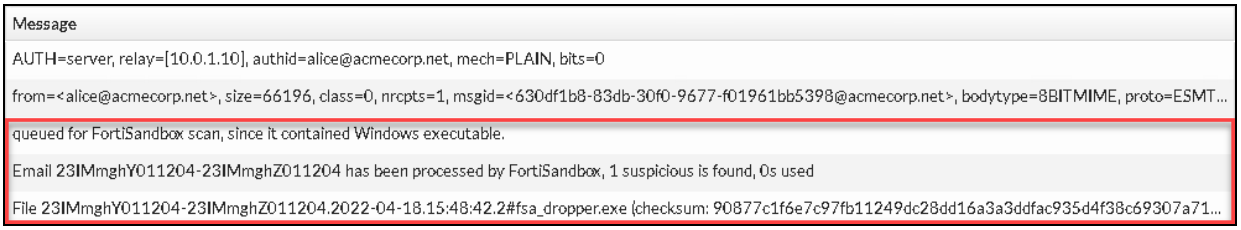


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The **Cross search result** tab appears.

5. On the **Cross search result** tab, review the **AntiVirus** logs.

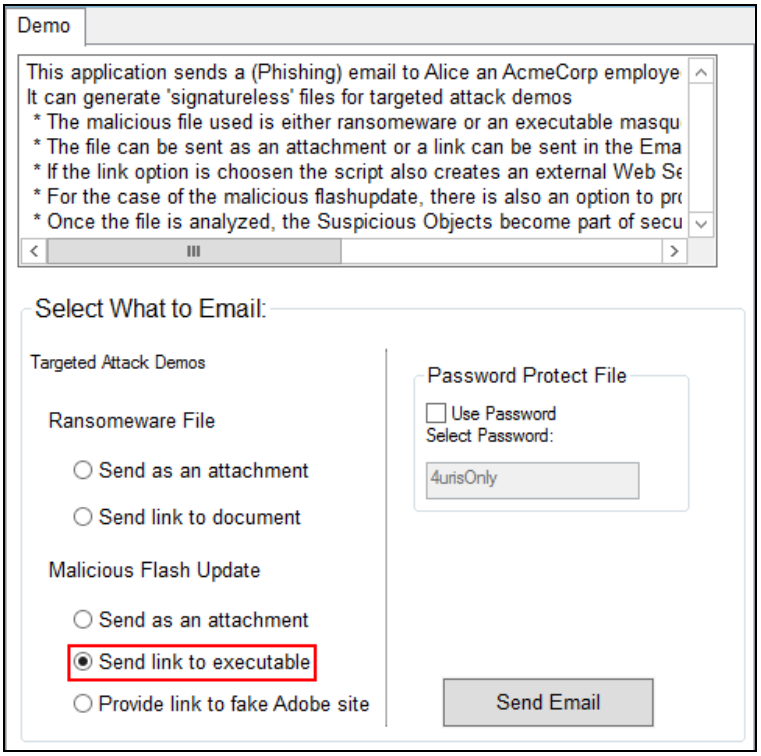


6. Double-click each antivirus log, review the log details, and then answer the following questions:
   - What rating did FortiSandbox return for the `fsa_dropper.exe` file?
   - How long did FortiMail take to process the email?
   - Did FortiMail send the `fsa_dropper.exe` file to FortiSandbox for analysis?

To verify the sandbox inspection of URLs

1. On the Remote-Host VM, on the desktop, double-click **ATP Email Sender**.

2. In the **Malicious Flash Update** section, select **Send link to executable**.

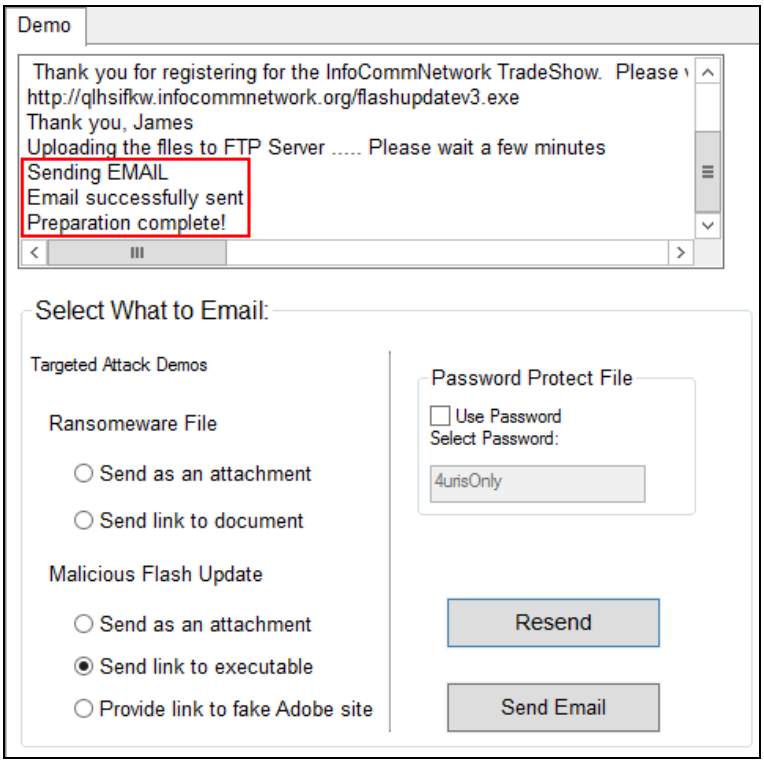


3. Click **Send Email**.

   The application status messages are displayed. Wait until the email is sent.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

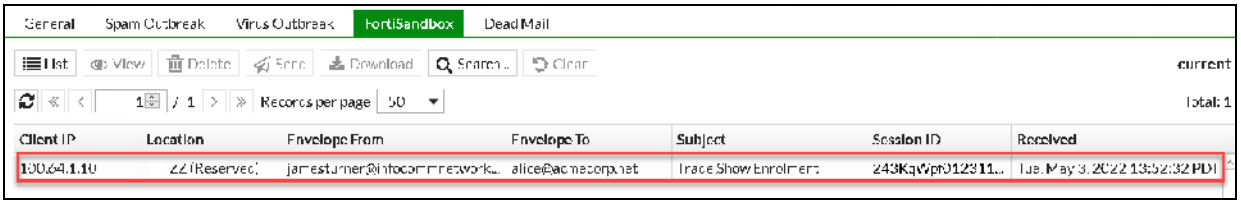
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



4. Close the application.
5. Close the Remote-Host VM browser tab.

To validate the sandbox inspection of URLs

1. Return to the FortiMail management GUI, and then click **Monitor** > **Mail Queue**.
2. Click the **FortiSandbox** tab.
3. Verify that the email is queued for sandboxing.



4. Return to the FortiSandbox GUI, and then click **Scan Job** > **VM Jobs**.
5. Wait until the VM scan job is complete.

The **File** column lists the full URL path that is being inspected inside the guest VM. Your URL will not match this example exactly. The ATP Email Sender application generates the URL randomly.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

6. Click **Log & Report** > **Events** > **Job Events**.
7. Review the log messages for the URL scan job.

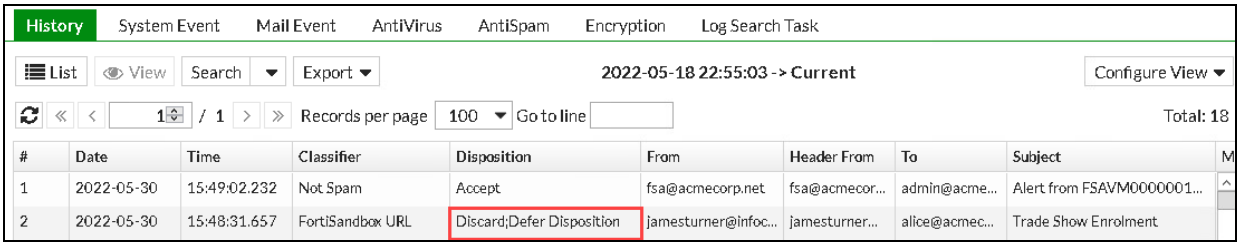
8. Click **Scan Job** > **URL Job Search**.
9. Click the view details (⧉) icon.

The scan job report is displayed.

10. Review the scan job report.
    - Which FortiSandbox component identified the threat?
11. Close the scan job report browser tab.
12. Log out of the FortiSandbox GUI.

To view FortiMail logs for a malicious URL

1. Return to the FortiMail management GUI, and then click **Monitor** > **Log**.
2. Locate the history log entry for the email, and then verify that the email was discarded as a result of sandboxing.



3. Click the session ID.
4. Review the log details for all **AntiVirus** logs in the **Cross search result** tab, and then answer the following questions:
    - What rating did FortiSandbox return for the URL?
    - How long did FortiMail take to process the email?
5. Log out of the FortiMail management GUI.
6. Close the FortiMail VM browser tab.

To validate sandboxing using alert emails

1. Return to the Local-Host VM, and then open Thunderbird.
2. Click **admin@acmecorp.com** > **Inbox**.
3. Review the alert email details.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

From fsa@acmecorp.net
Subject **Alert from FSAVM00000010086**
To Me <admin@acmecorp.net>

```
One suspicious or malicious file has been detected by FSAVM00000010086, please review detail via following URL:

Parent File Name:24UMgxmW020960-24UMgxmX020960
Parent SHA1:ca1343c9707dbaef5f5bae3421cfbbd7926e086b
Parent SHA256:876f04c676b74955fe9831ba9f6a6936194f769b1acde5cde5ecb69e700df2da
File Name: hxxp://ltyrentq.infocommnetwork.org/flashupdatev3.exe
File Type: WEBLink
File Size: 53
Rating: High Risk
Rated by: Dynamic Scan
Malware Name: N/A
Malware Type: Clean
Malware Info: N/A
Infected OS: WIN7X86SP1O16V3
Downloaded from: hxxp://ltyrentq.infocommnetwork.org/flashupdatev3.exe
Send Over: N/A
Device: FEVM010000140447(FortiMail:acmecorp.net)
Submit Time: 2022-05-30 15:42:59
Submit Type: URL via Device
Submit User: alice@acmecorp.net
Source IP: 0.0.0.0
Destination IP: 0.0.0.0
Scan Start Time: 2022-05-30 15:43:00
Scan Finish Time: 2022-05-30 15:48:23
Scan Time: 323 (seconds)
SHA256: 876f04c676b74955fe9831ba9f6a6936194f769b1acde5cde5ecb69e700df2da
SHA1: ca1343c9707dbaef5f5bae3421cfbbd7926e086b
MD5: 3bd8f2fe34dfd3483f36d585c576a27e
URL: https://10.200.4.213/job-detail/?jid=6080824677473642901
Email Sender: jamesturner@infocommnetwork.org
Email Receiver: alice@acmecorp.net
Subject: Trade Show Enrolment


Sent from FSAVM00000010086 (FSAVM00000010086) (10.200.4.213)
```

4. Close Thunderbird.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Configuring Quarantine Release Rescanning

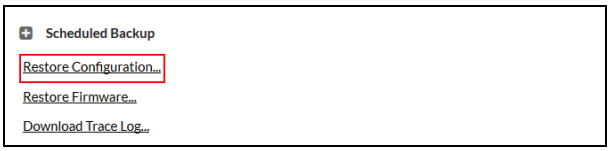
In this exercise, you will configure rescanning for emails that are released from FortiMail quarantine folders.

Configure User Quarantine on FortiMail

You will restore a configuration file to FortiMail that will apply a preconfigured content profile (CF-AcmeCorp-Inbound) to the inbound recipient policy for `acmecorp.net`. You will also validate the configuration by sending an email that contains a malicious attachment using the ATP Email Sender application from Remote-Host.

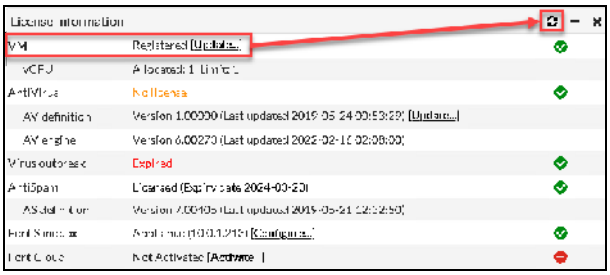
To restore the configuration file

1. On the Local-Host VM, open a Firefox browser tab, and then log in to the FortiMail management GUI at `https://10.200.2.100/admin` with the username `admin` and password `password`.
2. Click **System** > **Maintenance**.
3. Click **Restore Configuration**.



4. Click **Desktop** > **Resources** > **Lab 5 - Protecting Email Networks** > `Lab_5-2_FortiMail.cfg`, and then click **Open**.
5. Click **OK** to reboot.

   Wait until the browser is redirected to the FortiMail login page.
6. Log in with the username `admin` and password `password`.
7. In the **License Information** widget on the dashboard, if the **VM** status is **Waiting for communication**, click the refresh icon (🔄).



8. Close Firefox.

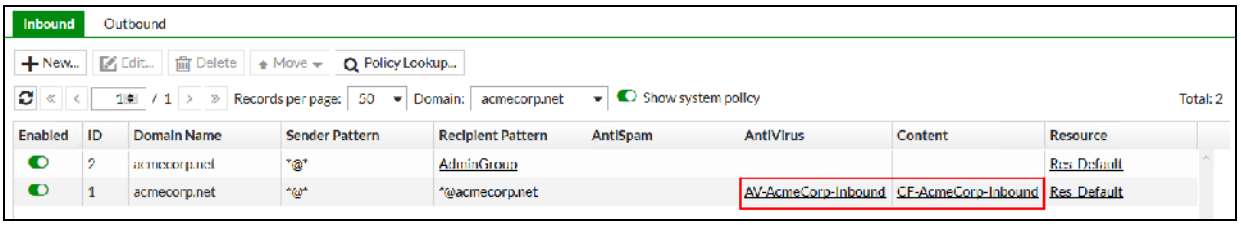
To verify the configuration

1. On the FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **Recipient Policy**.

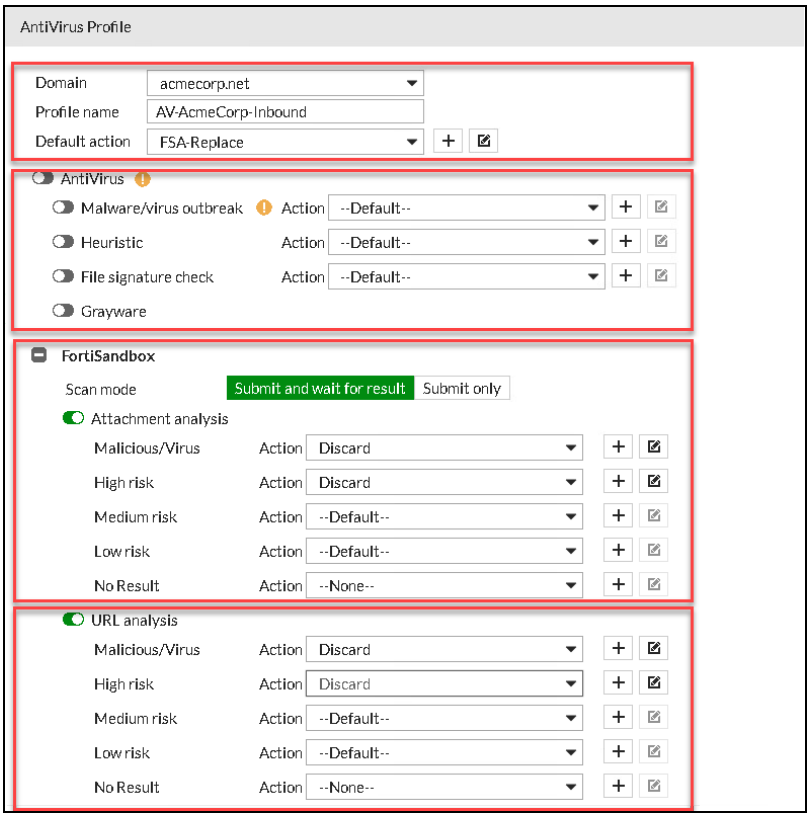
   The inbound recipient policy for `acmecorp.net` should match the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

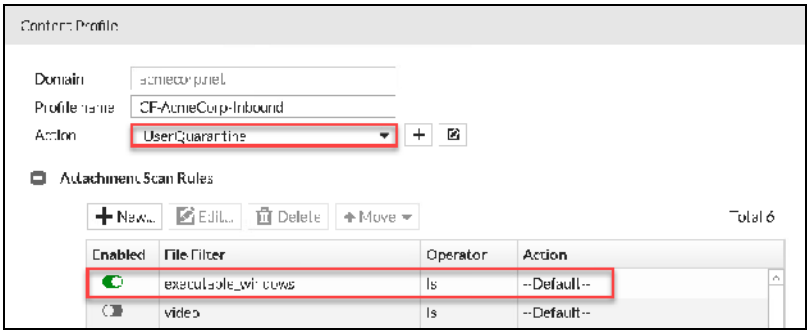
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. Click **AV-AcmeCorp-Inbound**.
4. Verify that the antivirus profile matches the following example:



5. Click **OK**.
6. Click **CF-AcmeCorp-Inbound**.
7. Verify that the content profile is configured to send emails containing executable attachments to user quarantine.



8. Click **OK**.

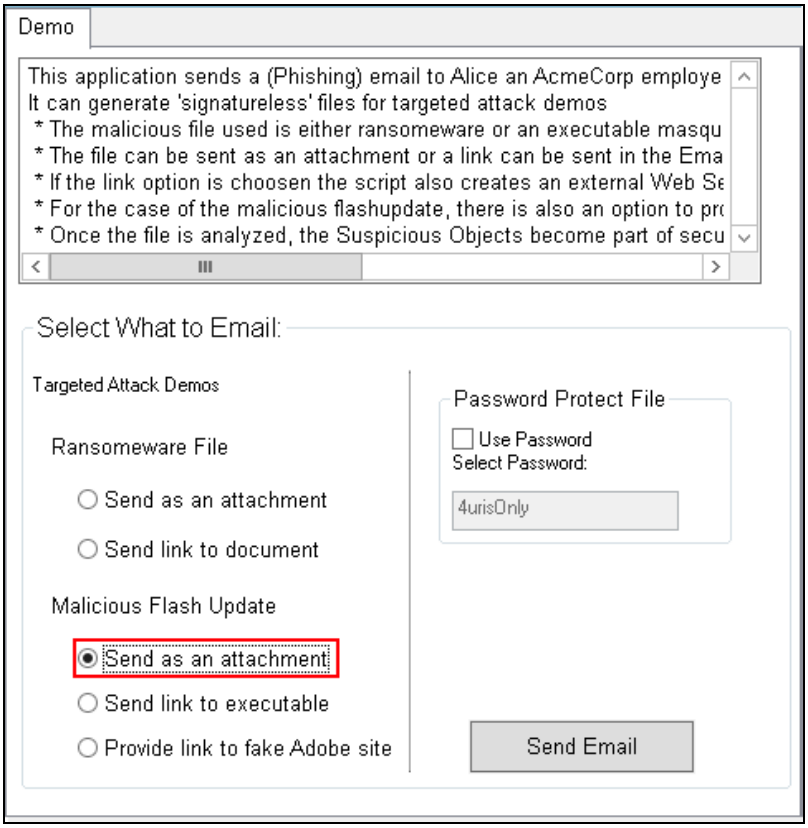
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To send a malicious email

1. On the Remote-Host VM, on the desktop, double-click **ATP Email Sender**.

2. In the **Malicious Flash Update** section, select **Send as an attachment**.



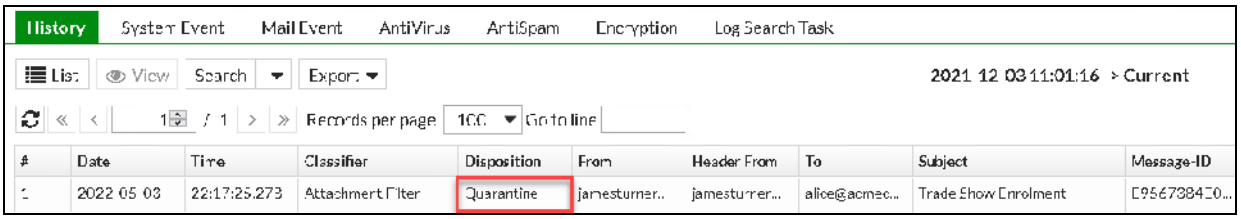
3. Click **Send Email**.
   The application status messages are displayed. Wait until the email is sent.
4. Close the application.
5. Close the Remote-Host VM browser tab.

To verify the quarantine action using FortiMail logs

1. Return to the FortiMail management GUI, and then click **Monitor** > **Log**.
2. Locate the history log entry for the email you just sent and then, in the **Disposition** column, confirm that the value listed is **Quarantine**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. Click the **Session ID**.
4. Review the **Message** column, and verify that the email was sent to user quarantine because of a content filter attachment scan rule.

Message	File name: flashupdatev3.exe, detected by Content Filter filetype application/x-ms-dos-executable, attachment scan rule: executable_windows

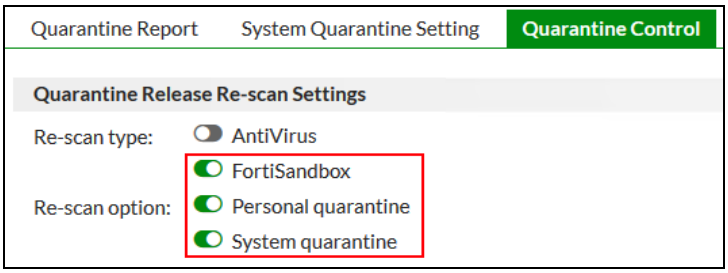
The default scan order is antispam, then content, and then FortiSandbox. Therefore, emails that are quarantined by the content filter will not be submitted to FortiSandbox, and emails that are potentially malicious could remain in FortiMail quarantine folders and be released to end users.

Configure Quarantine Rescan

You will configure quarantine release rescanning to make sure that FortiSandbox inspects quarantined emails before they are released to the end user. You will verify your configuration by releasing an email from user quarantine, and then monitoring the scan job on FortiSandbox.

To configure quarantine rescan

1. Continuing on the FortiMail management GUI, click **Security** > **Quarantine** > **Quarantine Control**.
2. In the **Re-scan type** section, enable **FortiSandbox**.
3. In the **Re-scan option** section, enable **Personal quarantine** and **System quarantine**.
   Your configuration should match the following example:



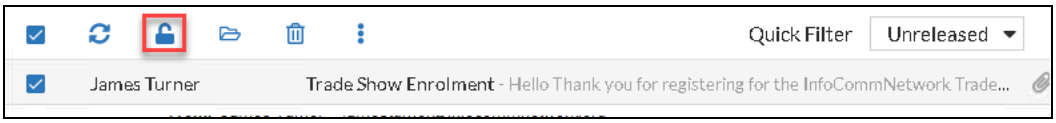
4. Click **Apply**.

To release an email from user quarantine

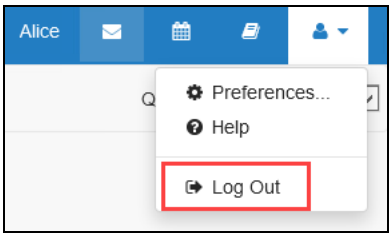
1. On the FortiMail webmail GUI, log in with the username `alice` and password `Fortinet1!`.
2. Click **Bulk**.
3. Click the quarantined email to open it.
4. Click **Release**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

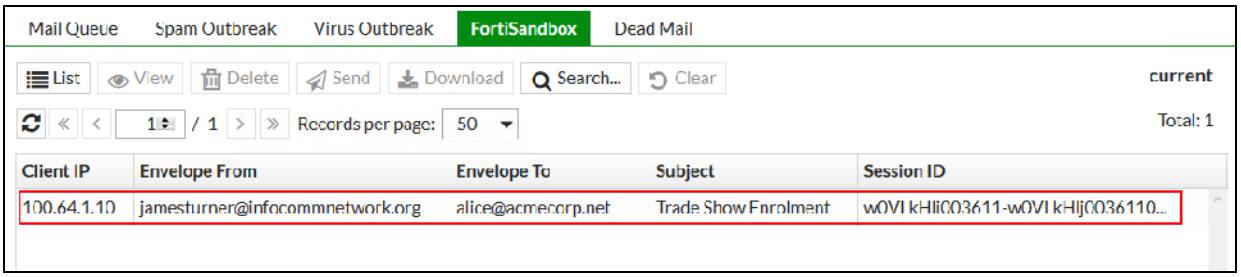


5. In the upper-right corner of the screen, click the drop-down list, and then click **Log Out**.



To verify the sandboxing of released email

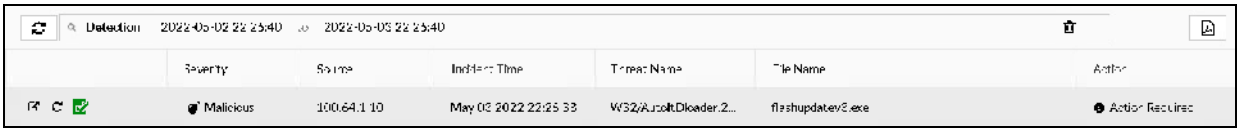
1. Return to the FortiMail management GUI, and then click **Monitor** > **Mail Queue** > **FortiSandbox**.
2. Verify that FortiMail has queued the released email for sandboxing.



If the email is not listed in the FortiSandbox queue, click the refresh icon ( ) a few times.

3. On the FortiSandbox GUI, log in with the username `admin` and password `password`.
4. Click **Scan Job** > **VM Jobs**.
5. Verify that the `flashupdatev3.exe` file from the released email is being scanned.

6. Wait for the scan job to finish.
7. Click **Dashboard** > **Operation Center**.
8. Verify that a verdict generated for the `flashupdatev3.exe` file.



9. Log out of the FortiSandbox GUI.

To verify the action taken on released email

1. Return to the FortiMail management GUI, and then click **Monitor** > **Log**.
2. Locate the history log entry for the released email, and then verify that the email was discarded.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

#	Date	Time	Classifier	Disposition	From	Header From	To	Subject
1	2022-05-03	22:25:08.625	FortiSandbox File	Discard;Defer Disposition	jamesturner@infos...	jamesturner..	alice@acmes..	Trace Show Environment

3. Log out of the FortiMail management GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 3: Diagnosing FortiMail Submissions

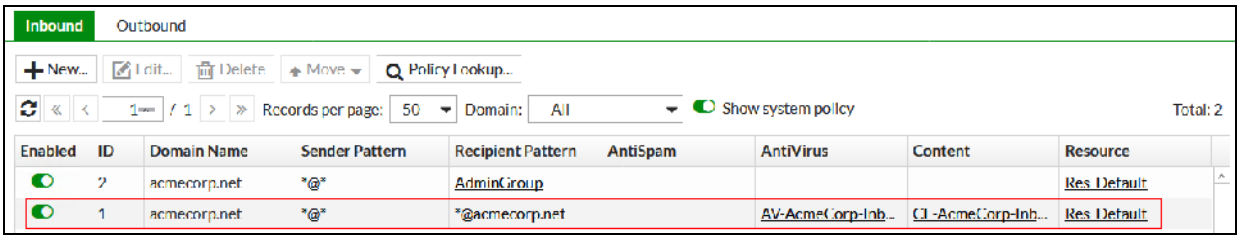
In this exercise, you will run some diagnostic commands on FortiMail and analyze the debug messages for file submissions.

Disable the Content Profile

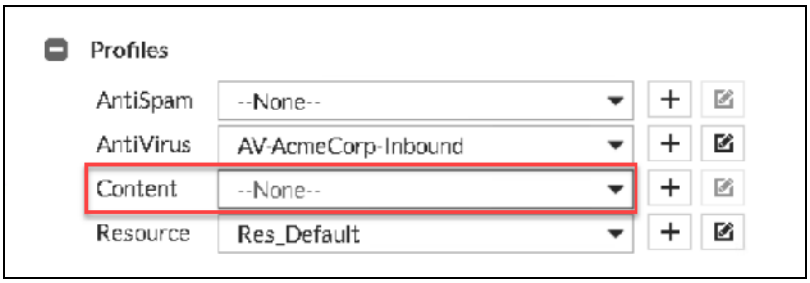
You will disable the content profile that you applied in the previous exercise.

To disable the content profile

1. On the FortiMail management GUI, log in with the username `admin` and password `password`.
2. Click **Policy** > **Recipient Policy**.
3. Double-click recipient policy ID **1**.



4. In the **Content** drop-down list, select **None**.



5. Click **OK**.
6. Log out of the FortiMail management GUI.

Diagnose FortiMail Submissions

You will run diagnostic commands on FortiMail and analyze the generated output for file submissions.

To enable debugging on FortiMail

1. Open an SSH connection to the FortiMail VM.
2. Enter the following command to view the available debug options for the `sandboxclid` daemon:

```
diagnose debug application sandboxclid ?
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

3. Review the `instant options` section.

```
FortiMail # diagnose debug application sandboxclid
-------- instant options --------
to-console                  print debugging information on console
to-file                     write debugging information to crashlog file
display                     follow crashlog file
clear                       clear debugging level and flags
```

If you use the `to-console` option, the debug messages will be printed to your SSH session. If you use the `to-file` option, you must then use the `display` option to display the debug messages from the crashlog file on your screen.

4. Review the `customized options` section.

```
-------- customized options --------
enable                      turn on debugging
disable                     turn off debugging
<level>                     debug level
        level is a number, add following values together
        1 - debug, 2 - verbose debug, 8 - low level debug
        32 - write debug to console, 64 - write debug to crashlog file
        65 is a good starting place
flags <level>               debug level
        level is a string, join the following values together
        C - to console, F - to crashlog file, S - to standard out
        d - debug, D - verbose debug, l - library level debug, L - verbose library debug
        v - very verbose debug, V - very verbose library debug
        p - print PID, t - add time stamp, s - add source file, f - add function, n - add line number
        Fdtsfn is a good starting place
persistent <level>          set persistent debug level for this applications
clear-persistent            clear persistent debug levels for ALL applications
```

There are two options to enable debugging: numerical `levels` or alphabetical `flags`.

If you use the numerical levels, add the numbers to combine various debug options. For example, to enable verbose debugging (`2`) and the saving of debug messages to the crashlog (`64`), you use `66`.

If you use the alphabetical flags, append each flag, as needed. For example, to enable verbose debugging (`D`), with function names (`f`) and timestamp (`t`), and print the output to the console (`C`), you use `CDtf`.

5. Enter the following commands to enable both `deferd` and `sandboxclid` debugging:

```
diagnose debug application sandboxclid 33
diagnose debug application deferd 33
diagnose debug enable
```

6. Leave the SSH session open.

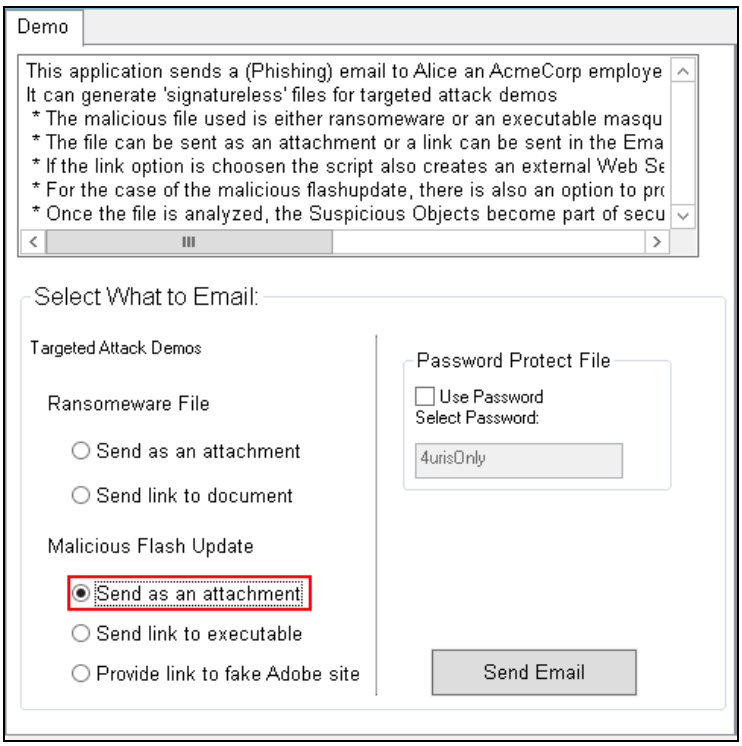
To send a malicious file attachment

1. On the Remote-Host VM, on the desktop, double-click **ATP Email Sender**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

2. In the **Malicious Flash Update** section, select **Send as an attachment**.



3. Click **Send Email**.
   The application status messages appear. Wait until the email is sent.
4. Close the application.
5. Close the Remote-Host VM browser tab.

To analyze the FortiMail debug output

1. Return to the FortiMail CLI, and then review the output.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com


```
sandboxclid:2022-04-19T12:26:10:SandboxScanJob.cpp:1087:UploadScanElements:file 23JJQ9bp016048-23JJQ9bq016048.2022-04-19.12:26:10.2#flashupdatev3.exe (checksum: cab3ec8db7190e64796393e
sandboxclid:2022-04-19T12:26:22:SandboxJob.cpp:165:process:use configured FortiSandbox server
sandboxclid:2022-04-19T12:26:22:Session.cpp:88:Connect0:connected
sandboxclid:2022-04-19T12:26:22:Connection.cpp:453:Read:ssl_read() failed, rc = 5, (error:00000000:lib(0):func(0):reason(0))
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:137:Receive:peer dropped connection
sandboxclid:2022-04-19T12:26:22:Connection.cpp:167:Connect:connecting to 10.0.1.213
sandboxclid:2022-04-19T12:26:22:Session.cpp:179:MakeConnection:connected to '10.0.1.213:514' successfully
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:220:Execute:server ack code: 0
sandboxclid:2022-04-19T12:26:22:Session.cpp:205:MakeConnection:logged in successfully
sandboxclid:2022-04-19T12:26:22:Session.cpp:88:Connect0:connected
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:220:Execute:server ack code: 0
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:569:ParseData:size of OFTP_OPT_DATA: 47, raw: 754974720
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:539:__parse_statistics_data:statistics data: field 1, size 1, value 1
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:539:  parse statistics data:statistics data: field 0, size 1, value 4
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:539:__parse_statistics_data:statistics data: field 2, size 1, value 0
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:539:__parse_statistics_data:statistics data: field 3, size 1, value 0
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:539:  parse statistics data:statistics data: field 4, size 1, value 0
sandboxclid:2022-04-19T12:26:22:RemoteCommand.cpp:539:__parse_statistics_data:statistics data: field 5, size 1, value 0
sandboxclid:2022-04-19T12:26:42:SandboxScanJob.cpp:1399:process:processing 23JJQ9bp016048-23JJQ9bq016048
sandboxclid:2022-04-19T12:26:42:Session.cpp:88:Connect0:connected
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:101:Prepare:checking cab3ec8db7190e64796393eb61b082c6e0e44698b1bd57358d8c98183bdeaaf
sandboxclid:2022-04-19T12:26:42:RemoteCommand.cpp:137:Receive:peer dropped connection
sandboxclid:2022-04-19T12:26:42:SandboxScanJob.cpp:1399:process:processing 23JJQ9bp016048-23JJQ9bq016048
sandboxclid:2022-04-19T12:26:42:Connection.cpp:167:Connect:connecting to 10.0.1.213
sandboxclid:2022-04-19T12:26:42:Session.cpp:179:MakeConnection:connected to '10.0.1.213:514' successfully
sandboxclid:2022-04-19T12:26:42:RemoteCommand.cpp:220:Execute:server ack code: 0
sandboxclid:2022-04-19T12:26:42:Session.cpp:205:MakeConnection:logged in successfully
sandboxclid:2022-04-19T12:26:42:Session.cpp:88:Connect0:connected
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:101:Prepare:checking cab3ec8db7190e64796393eb61b082c6e0e44698b1bd57358d8c98183bdeaaf
sandboxclid:2022-04-19T12:26:42:RemoteCommand.cpp:220:Execute:server ack code: 0
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:134:ParseData:size of OFTP_OPT_DATA: 67, raw: 1250291200
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:140:ParseData:verdict data returned: 01CA0300
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:142:ParseData:number of verdict returned: 1
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:167:ParseData:verdict_v2_t is used
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:173:ParseData:FSA empty: hash cab3ec8db7190e64796393eb61b082c6e0e44698b1bd57358d8c98183bdeaaf, score: 156, flags: 0, name: ''
```

2. The `deferd` daemon saves the email in the FortiSandbox queue folder, and also saves a copy of the email in the defer queue folder, using the email session ID as the identifier.

```
deferd:2022-04-19T12:26:10:TaskManager.cpp:230:qfind:runner 0 load 1

deferd:2022-04-19T12:26:10:Runner.cpp:322:hold:hold 8f23JJQ9bp016048-
23JJQ9bq016048 repost 0

deferd:2022-04-19T12:26:10:Runner.cpp:373:hold:sandbox scan qf
(/var/spool/deferd/temp2/new/8f23JJQ9bp016048-23JJQ9bq016048) df
(/var/spool/deferd/temp2/df/df23JJQ9bp016048-23JJQ9bq016048)
```

3. The `sandboxclid` daemon starts preparing the scan job, and extracts all attachments—the message body and executable file—from the copy in the defer queue folder. The executable file will be submitted, but the message body will not.

```
sandboxclid:2022-04-19T12:26:10:SandboxScanJob.cpp:147:SandboxScanJob_
_:ScanJob(23JJQ9bp016048-23JJQ9bq016048) is scheduled, will expire in 1785
sec

sandboxclid:2022-04-19T12:26:10:SandboxScanJob.cpp:1416:process:Email
8f23JJQ9bp016048-23JJQ9bq016048 is picked up from sandbox queue

sandboxclid:2022-04-
19T12:26:10:AttachmentExtractorQF.cpp:317:AttachmentExtractorImplQF:QF:
/var/spool/deferd/sbxqueue/in/8f23JJQ9bp016048-23JJQ9bq016048

sandboxclid:2022-04-
19T12:26:10:AttachmentExtractorQF.cpp:318:AttachmentExtractorImplQF:DF:
/var/spool/deferd/sbxqueue/in/df23JJQ9bp016048-23JJQ9bq016048

sandboxclid:2022-04-
19T12:26:10:AttachmentExtractorQF.cpp:219:ParseHeaders:attachments [2.0] will
be uploaded

sandboxclid:2022-04-
19T12:26:10:AttachmentExtractorQF.cpp:253:visitRfc822Msg:attachment 1 is
skipped
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com


```
sandboxclid:2022-04-19T12:26:10:SandboxScanJob.cpp:306:ExtractScanElements:1
elements will be scanned
```

4. The `sandboxclid` daemon performs a quick check on the file by sending the file checksum to FortiSandbox.

```
sandboxclid:2022-04-19T12:26:10:Session.cpp:89:Connect0:connected

sandboxclid:2022-04-19T12:26:10:FileVerdictCommand.cpp:101:Prepare:checking
cab3ec6db7190e64796393eb61b082c6e0ef44696b1bd57358d8c98183bdeaaf

...output omitted...

sandboxclid:2022-04-19T12:26:10:FileVerdictCommand.cpp:173:ParseData:FSA
reply: hash cab3ec6db7190e64796393eb61b082c6e0ef44696b1bd57358d8c98183bdeaaf,
score 156, flags 0, name ''
```

FortiSandbox does not return a verdict for the file checksum.

5. The `sandboxclid` daemon prepares a TGZ archive file. The archive filename contains the FortiMail serial number. FortiMail also supplies the email session ID inside the archive. The file is then transferred to FortiSandbox.

```
sandboxclid:2022-04-19T12:26:10:SandboxScanJob.cpp:887:UploadOneFile:upload
'23JJQ9bp016048-23JJQ9bq016048.2022-04-19.12:26:10.2#flashupdatev3.exe'

...omitted output...

sandboxclid:2022-04-19T12:26:10:AnalyticalCommand.cpp:229:Prepare:suspicous
file: 536491:1:969216:FEVM010000140447.3.tgz

...omitted outout...

sandboxclid:2022-04-
19T12:26:10:SandboxScanJob.cpp:1087:UploadScanElements:File 23JJQ9bp016048-
23JJQ9bq016048.2022-04-19.12:26:10.2#flashupdatev3.exe (checksum:
cab3ec6db7190e64796393eb61b082c6e0ef44696b1bd57358d8c98183bdeaaf) has been
sent to FortiSandbox
```

6. After the file is transferred, FortiMail queries FortiSandbox for the verdict every 30 seconds by sending the file checksum.

```
sandboxclid:2022-04-19T12:26:22:Session.cpp:89:Connect0:connected

sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:101:Prepare:checking
cab3ec6db7190e64796393eb61b082c6e0ef44696b1bd57358d8c98183bdeaaf

sandboxclid:2022-04-19T12:26:42:RemoteCommand.cpp:228:Execute:server ack
code: 0

sandboxclid:2020-09-23T18:33:46:FileVerdictCommand.cpp:132:ParseData:size of
OFTP_OPT_DATA: 67, raw: 1258291200

sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:140:ParseData:verdict
data returned: 01CAB3EC

sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:142:ParseData:number
of verdict returned: 1

sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:167:ParseData:verdict_
v2_t is used
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com


```
sandboxclid:2022-04-19T12:26:42:FileVerdictCommand.cpp:173:ParseData:FSA
reply: hash cab3ec6db7190e64796393eb61b082c6e0ef44696b1bd57358d8c98183bdeaaf,
score 156, flags 0, name ''
```

7. After FortiSandbox completes the scan, it responds with a verdict for the file checksum query.

```
sandboxclid:2022-04-19T18:36:46:Session.cpp:101:Connect0:connected

sandboxclid:2022-04-19T18:36:46:FileVerdictCommand.cpp:100:Prepare:checking
ac27cd204240c5d4c3612bd2d2f4bc4226dbc0906318004b767ec34bb3deefa3

sandboxclid:2022-04-19T18:36:46:RemoteCommand.cpp:225:Execute:server ack
code: 0

sandboxclid:2022-04-19T18:36:46:FileVerdictCommand.cpp:132:ParseData:size of
OFTP_OPT_DATA: 67, raw: 1258291200

sandboxclid:2022-04-19T18:36:46:FileVerdictCommand.cpp:138:ParseData:verdict
data returned: 01AC27CD

sandboxclid:2022-04-19T18:36:46:FileVerdictCommand.cpp:140:ParseData:number
of verdict returned: 1

sandboxclid:2022-04-19T18:36:46:FileVerdictCommand.cpp:165:ParseData:verdict_
v2_t is used

sandboxclid:2022-04-19T18:36:46:FileVerdictCommand.cpp:174:ParseData:FSA
reply: hash ac27cd204240c5d4c3612bd2d2f4bc4226dbc0906318004b767ec34bb3deefa3,
score 2, flags 0, name 'Downloader'
```

8. The `sandboxclid` daemon extracts the scan result and notifies the `deferd` daemon.

```
sandboxclid:2022-04-19T18:36:46:SandboxScanJob.cpp:408:FetchFileResults:File
08O1XFem007205-08O1XFen007205.2020-09-23.18:33:16.2#flashupdatev3.exe
(checksum ac27cd204240c5d4c3612bd2d2f4bc4226dbc0906318004b767ec34bb3deefa3)
has been scanned by FortiSandbox. Scan result: rating=SUSPICIOUS_HIGH
category=Downloader

sandboxclid:2022-04-19T18:36:46:ActiveRequestList.cpp:55:PostFileResult:File
(checksum ac27cd204240c5d4c3612bd2d2f4bc4226dbc0906318004b767ec34bb3deefa3)
has 1 jobs

sandboxclid:2022-04-19T18:36:46:SandboxScanJob.cpp:1511:post_process:Email
08O1XFem007205-08O1XFen007205 has been processed by FortiSandbox, 1
suspicious is found, 210s used

sandboxclid:2022-04-19T18:36:46:SandboxScanJob.cpp:59:notify:Notify deferd
(8f08O1XFem007205-08O1XFen007205) 1
```

9. The `deferd` daemon releases the email from the FortiSandbox queue folder.

```
deferd:2022-04-19T18:36:46:DatagramServer.cpp:79:handle_request:received
reqeust type 5 id 5519

deferd:2020-04-19T18:36:46:Service.cpp:30:process:sbx request
8f08O1XFem007205-08O1XFen007205 scan_result 0

deferd:2022-04-19T18:36:46:Service.cpp:36:process:sbx request
8f08O1XFem007205-08O1XFen007205 result: id=2 verdict=3 malware=Downloader
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

Brave-Dumps.com
DO NOT REPRINT
© FORTINET


```
hash=ac27cd204240c5d4c3612bd2d2f4bc4226dbc0906318004b767ec34bb3deefa3
name=08O1XFem007205-08O1XFen007205.2022-04-19.18:33:16.2#flashupdatev3.exe

deferd:2022-04-19T18:36:46:Deferd.cpp:269:sbxnotify:sbxnotify
8f08O1XFem007205-08O1XFen007205

deferd:2022-04-19T18:36:46:TaskManager.cpp:293:qfind:runner 0 load 1

deferd:2022-04-19T18:36:46:Runner.cpp:756:process:Sandbox Parts 2.0 for
08O1XFem007205-08O1XFen007205

deferd:2022-04-19T18:36:46:Runner.cpp:718:visitRfc822Msg:sandbox verdict for
2 is 3

sandboxclid:2022-04-19T18:36:46:SandboxScanJob.cpp:62:notify:Notify deferd
(8f08O1XFem007205-08O1XFen007205) successfully

deferd:2022-04-19T18:36:46:Runner.cpp:441:release:release qf
(/var/spool/deferd/mqueue/current/8f08O1XFem007205-08O1XFen007205) df
(/var/spool/deferd/mqueue/current/df/df08O1XFem007205-08O1XFen007205)
```

10. Enter the following commands to disable debugging:

```
diagnose debug disable
diagnose debug application sandboxclid clear
diagnose debug application deferd clear
```

11. Close the FortiMail SSH session browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 6: Protecting Web Applications

In this lab, you will configure FortiWeb to submit files to FortiSandbox. You will verify your configuration using multiple malware samples.

Objectives

- Configure machine learning on FortiWeb
- Configure FortiWeb to submit files to FortiSandbox for inspection
- Monitor FortiSandbox inspection results and statistics for the inspected files

Time to Complete

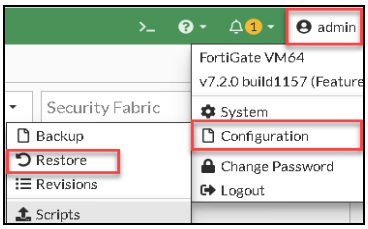
Estimated: 70 minutes

Prerequisites

Before beginning this lab, you must restore a configuration file to FortiGate.

To restore the FortiGate configuration file

1. On the Local-Host VM, open a Firefox browser tab, and then log in to the FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Lab 6 - Protecting Web Applications** > `Lab_6_FortiGate.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

   Wait until the browser is redirected to the login page.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Configuring Machine Learning for Advanced Threats

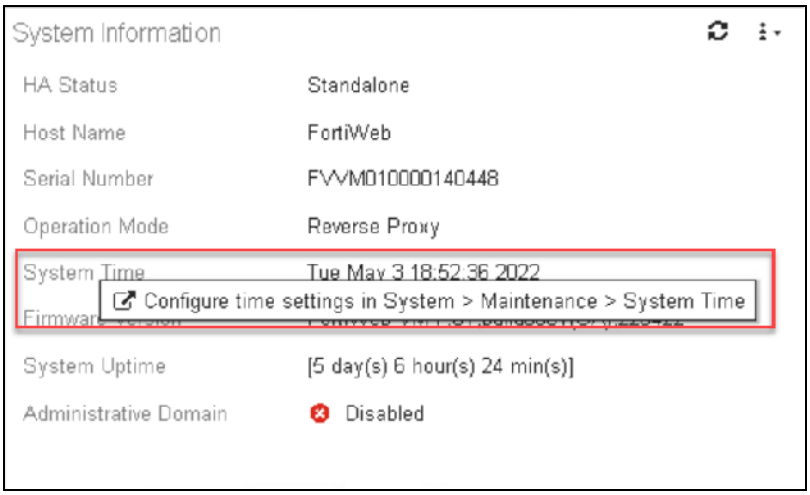
In this exercise, you will configure machine learning on FortiWeb, and generate samples to build the Hidden Markov Model (HMM). You will then verify your configuration using a SQL injection attack.

Configure the FortiWeb System Time

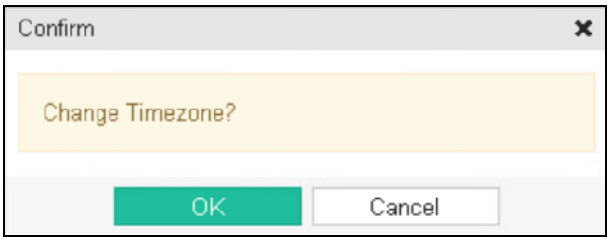
You will configure the system time zone, and enable synchronization with a custom NTP server on FortiWeb.

To configure the system time

1. On the FortiWeb GUI, log in with the username `admin` and password `password`.
2. In the **System Information** widget, click **System Time**.



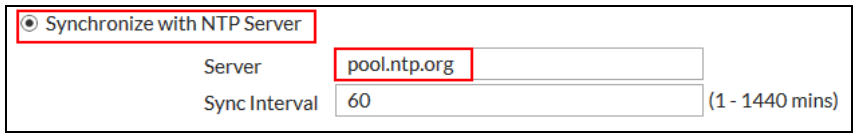
3. In the **Time Zone** drop-down list, select your local time zone.
   A confirmation prompt appears.



4. Click **OK**.
5. Click **Synchronize with NTP Server**, and then verify that **Server** is set to `pool.ntp.org`.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



If your local time zone observes daylight savings time, enable **Automatically adjust clock for daylight saving changes**.

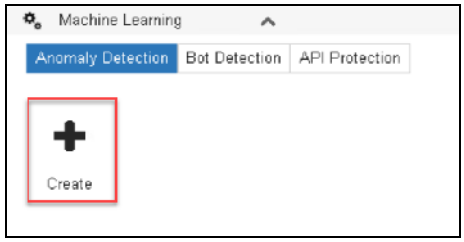
6. Click **OK**.

Configure Machine Learning

You will configure machine learning to detect anomalies in web traffic. FortiWeb employs two layers of machine learning to detect malicious attacks. The first layer uses the HMM, monitors access to the application, and collects data to build a mathematical model behind every parameter and HTTP method. After the first layer completes, FortiWeb verifies each request against the model to determine whether or not it is an anomaly.

To configure machine learning

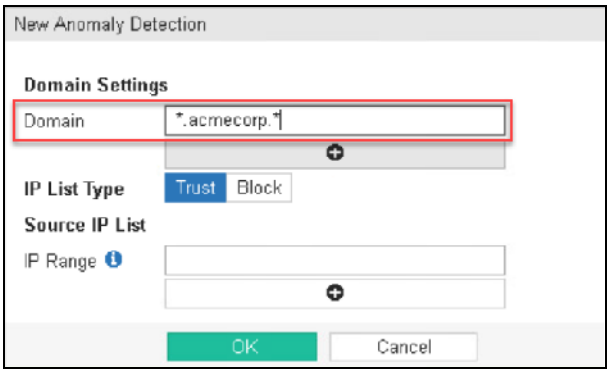
1. Continuing on the FortiWeb GUI, click **Policy** > **Server Policy**.
2. Double-click the **BillingPortalAccess** policy.
3. Scroll down to the **Machine Learning** section, expand the **Machine Learning** section, select **Anomaly Detection**, and then click **Create**.



4. In the **Domain** field, type `*.acmecorp.*`.

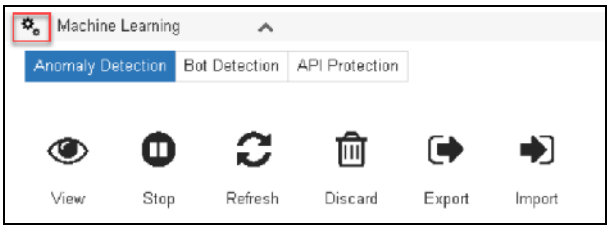
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



5. Click**OK**.

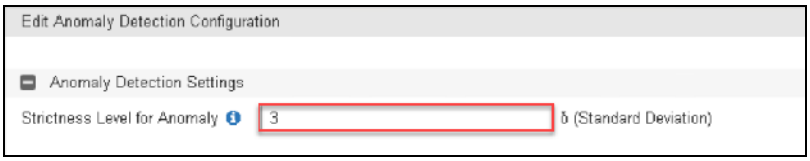
   Under the **Machine Learning** heading with the gears turning—the gears indicate that machine learning is now turned on—you should see the following icons:



6. Click **OK**.

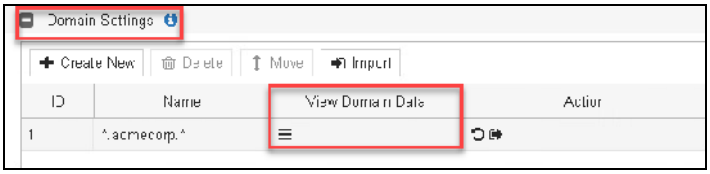
To review and edit the machine learning policy

1. Continuing on the FortiWeb GUI, click **Machine Learning** > **Anomaly Detection**.
2. Double-click the **BillingPortalAccess** policy.
3. In the **Anomaly Detection Settings** section, confirm that the value in the **Strictness Level for Anomaly** field is `3`.



The anomaly distribution model determines whether the functions of a parameter have changed. FortiWeb calculates deviations only after 500 inputs. You cannot change this number.

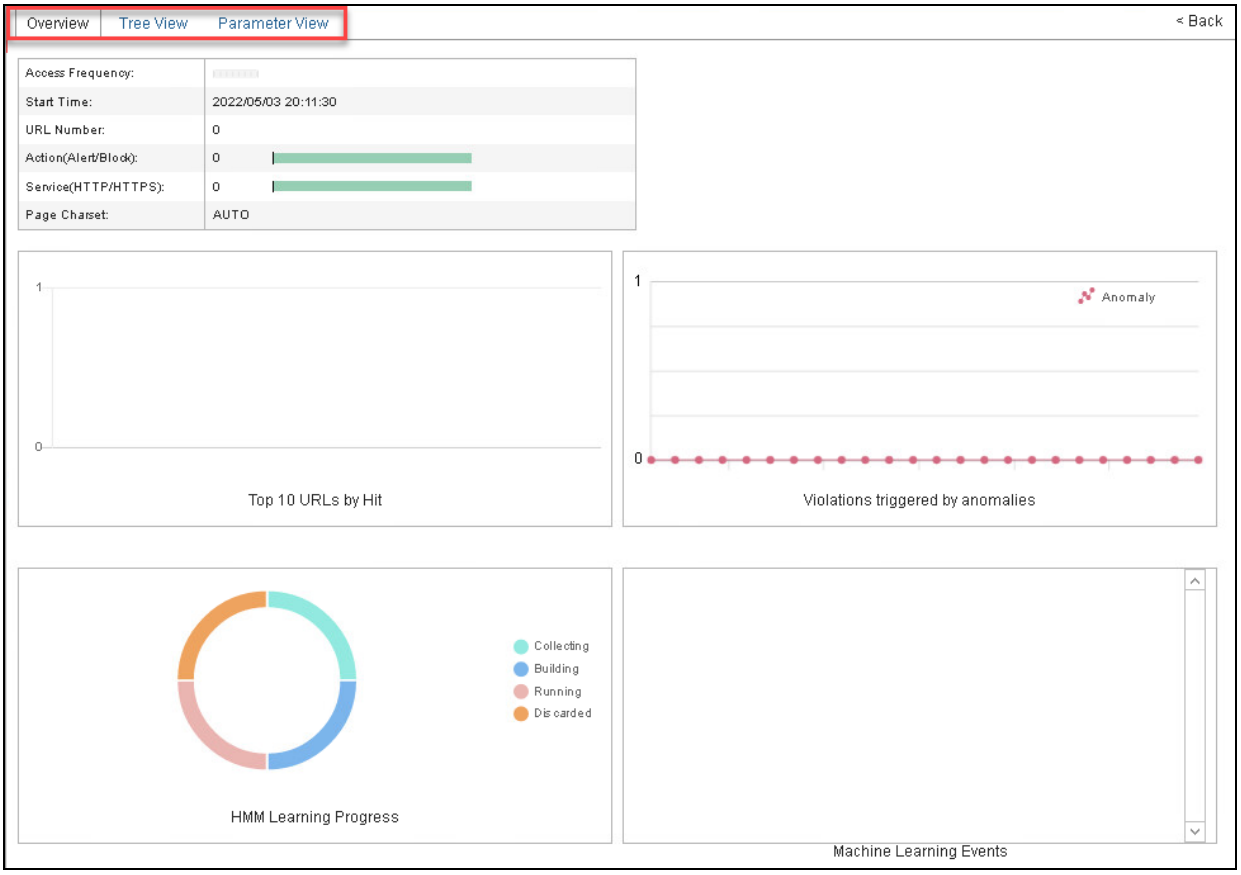
4. Click **OK**.
5. Double-click the **BillingPortalAccess** policy again.
6. In the **Domain Settings** section, click **View Domain Data**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The following three tabs appear: **Overview**, **Tree View**, and **Parameter View**. Click each one, and you will notice that no data was collected. This is because no HTTP requests are currently being sent to the web server.



7. Click **Tree View**.

Do not close this screen—you will return here after you start sending sample data from the Kali VM.

Configure the Sampling Limit

You will now change the machine learning policy to limit samples from one IP address, to facilitate the lab testing.

By default, when the machine learning is in the collecting phase, FortiWeb accepts only 30 requests from the same IP address. You can modify this in the CLI. For testing purposes, you will configure FortiWeb to accept unlimited samples from the same IP address (the Kali VM).

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To configure the sampling limit

1. Open an SSH session to the FortiWeb VM.
2. Enter the following commands:

```
config waf machine-learning-policy
   edit 1
      set sample-limit-by-ip 0
      set ip-expire-cnts 1
   next
end
```

3. Enter the following command to exit the PuTTY session:

```
exit
```

4. Close the FortiWeb SSH session browser tab.

Generating HTTP Requests

You will send HTTP requests to the web server to train the FortiWeb machine learning models.

To generate HTTP requests

1. Go to the Kali VM.
2. Open a terminal window.
3. Enter `pwd`, and then verify that you are in the `root` directory.
4. Enter the following command:

```
./wfuzz_ml.sh
```

This generates more than 2000 login attempts to the `http://billings.acmecorp.net/index.php` URL.

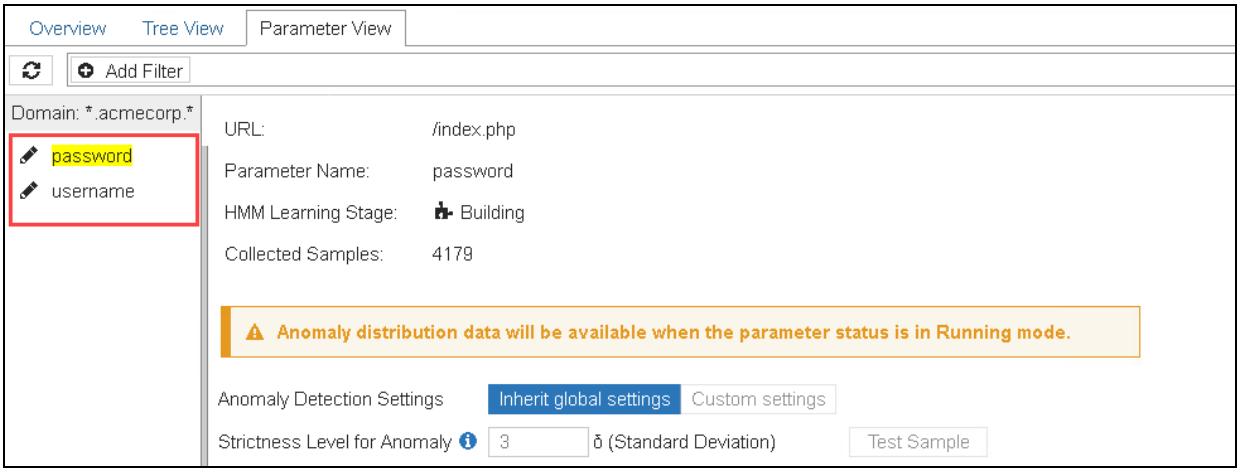
You should see the requests being sent to the web server, similar to the following example:

```
root@kali:~# ./wfuzz_ml.sh

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.3.4 - The Web Fuzzer                         *
********************************************************

Target: http://www.billings.acmecorp.net/index.php
Total requests: 12334000

=====================================================================
ID   Response   Lines      Word         Chars          Payload
=====================================================================

000001:  C=200     27 L       66 W          647 Ch        "NWARE3889 - 123456"
000002:  C=200     27 L       66 W          647 Ch        "NWARE3889 - password"
000003:  C=200     27 L       66 W          647 Ch        "NWARE3889 - 12345678"
000004:  C=200     27 L       66 W          647 Ch        "NWARE3889 - 1234"
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

5. Return to the FortiWeb GUI, and then click **Parameter View**.
6. Verify that the **username** and **password** parameters were added.

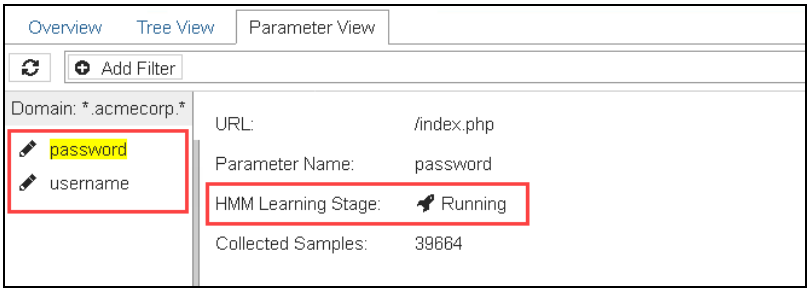


FortiWeb gathers this information during the collection stage by monitoring the HTTP requests. The collection stage must run for at least five minutes.

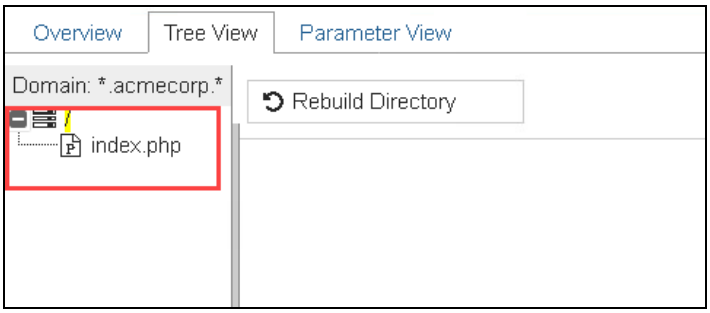
7. After five minutes, click the refresh icon (🔄) to update the progress of the **HMM Learning Stage**.

From the collecting stage, the **HMM Learning Stage** moves to the testing stage, and then to the running stage. You may not see the testing stage because FortiWeb moves very quickly from the testing stage to the running stage.

8. Verify that for both the **password** and **username** stages, the **HMM Learning Stage** field shows **Running**.



9. Return to the Kali VM, and then press `Ctrl` + `C` to end the wfuzz process.
10. Return to the FortiWeb GUI, and then click **Tree View**.
11. Expand the URL, and then click **index.php**.



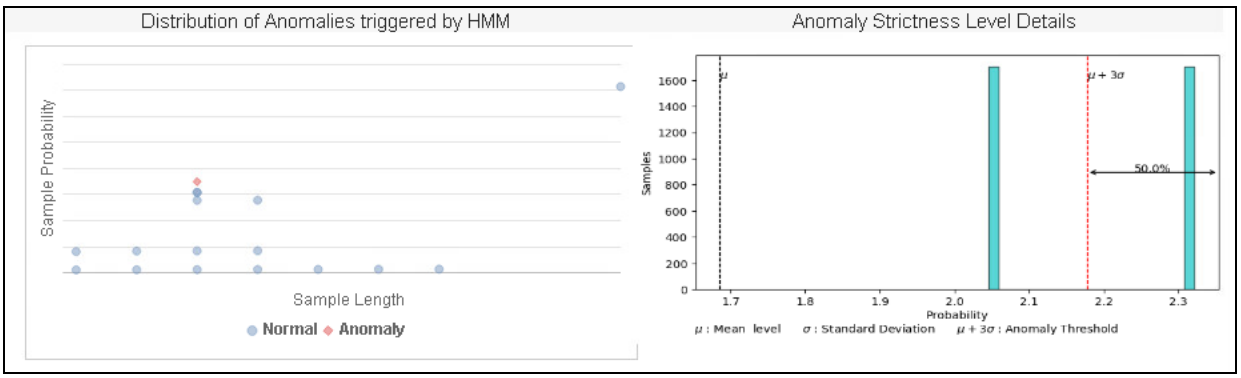
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

12. Observe the **password** and **username** parameters that FortiWeb learned and linked to the **index.php** page. You can also observe the **HMM Learning Stage** for each parameter.

13. Click **Parameter View** > **password**.

Examine the **Distribution of Anomalies triggered by HMM** graph. You can see which samples were considered anomalies when FortiWeb built the HMM model. All the samples matched the HMM model.



Attacking the Web Server

Now, you will run attacks on the web server. FortiWeb machine learning should identify the attacks as anomalous and block them.

To run attacks from Kali

1. Return to the Kali VM.
2. In the terminal window, enter the following command:

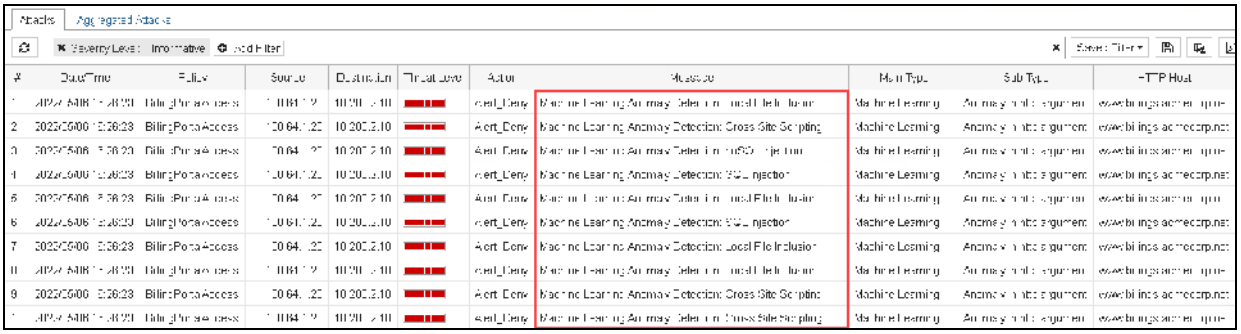
```
./wfuzz_attack.sh
```

The script sends 24 malicious requests to the password parameter for the web page.

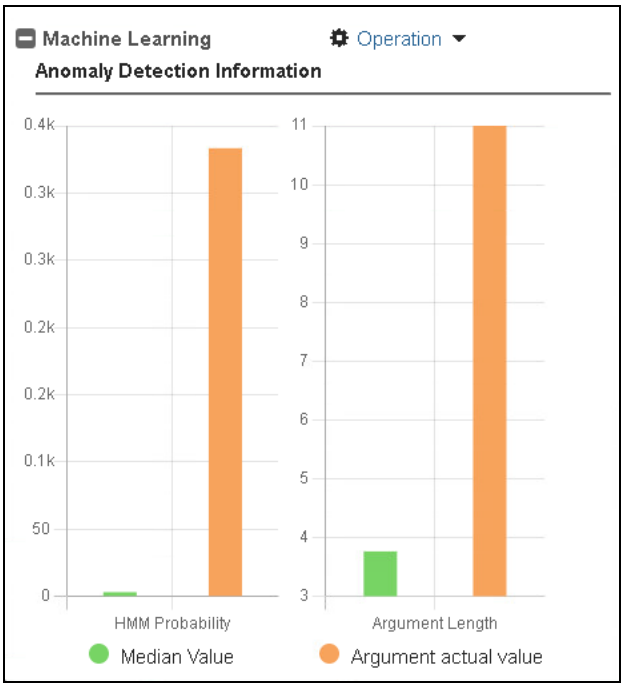
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

3. Close the terminal window.
4. Close the Kali VM browser tab.
5. Return to the FortiWeb GUI, and then click **Log&Report** > **Log Access** > **Attack**.
6. Verify that FortiWeb machine learning blocked the attacks.



7. Click the first log entry, and then scroll down to the **Machine Learning** section of the log details.

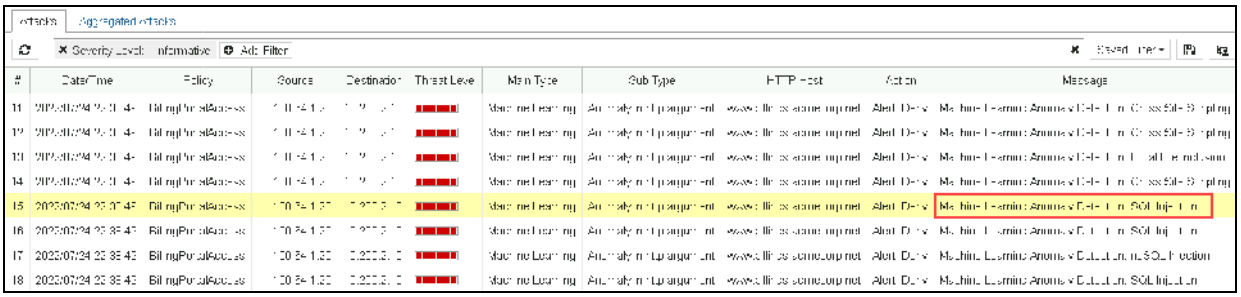


Observe the **Anomaly Detection information**. You can see the input from the attack (in orange), compared to both the **HMM probability** and **Argument Length** that was observed for the password parameter (in green). For the password, the **HMM Probability** is **5** and the **Argument Length** is **4**. In other words, FortiWeb expected only four digits for the password value, but this request used five digits, triggering an anomaly.

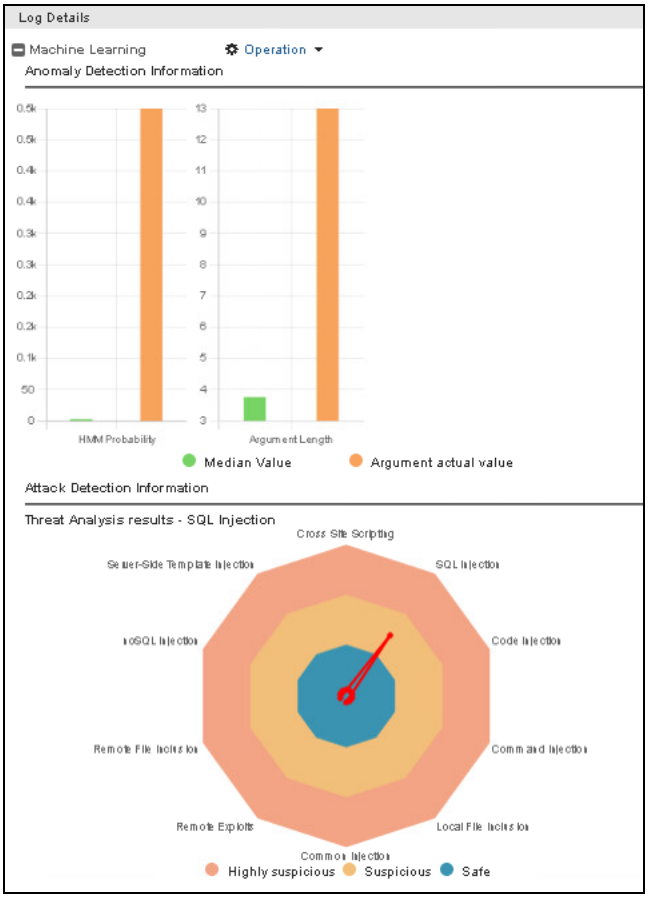
8. Find a SQL injection log entry.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



9. View the **Log Details**.



Here, you can see that the threat model describes this as a SQL injection attack based on the characteristics of the malicious input.

10. Log out of the FortiWeb GUI.
11. Close the FortiWeb GUI browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Integrating FortiSandbox With FortiWeb

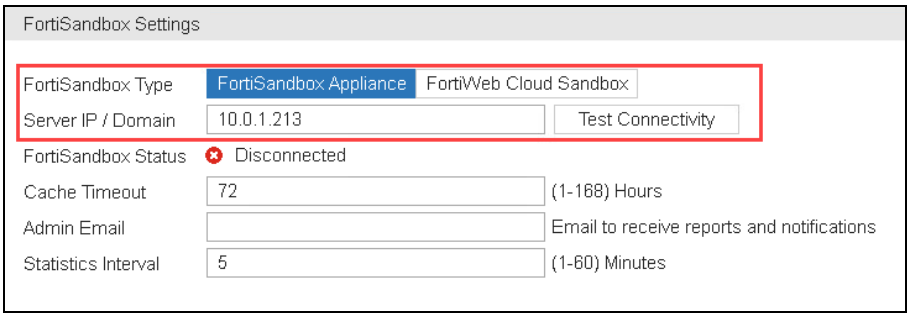
In this exercise, you will integrate FortiSandbox with FortiWeb. You will configure a FortiWeb file security policy to offload files to FortiSandbox. You will then verify your configuration using various malware samples.

Configure FortiSandbox Integration

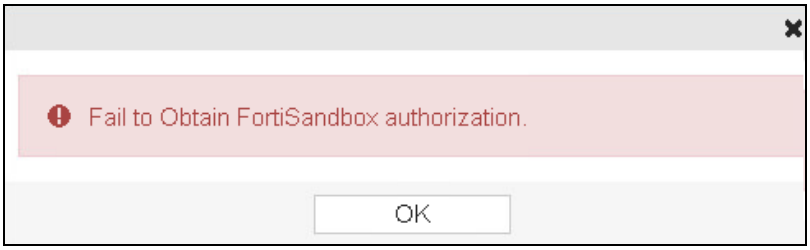
You will configure the settings required to integrate FortiWeb with FortiSandbox. You will then authorize FortiWeb on FortiSandbox, and verify the connectivity between the two devices. You will also configure FortiWeb to use the FortiSandbox malware signature database, and enable event logging for FortiSandbox file submissions.

To configure the sandbox settings on FortiWeb

1. On the FortiWeb GUI, log in with the username `admin` and password `password`.
2. Click **System** > **Config** > **FortiSandbox**.
3. In the **Server IP/ Domain** field, type `10.0.1.213`.



4. Click **Apply**.
5. Click **Test Connectivity**.
   An error message appears.



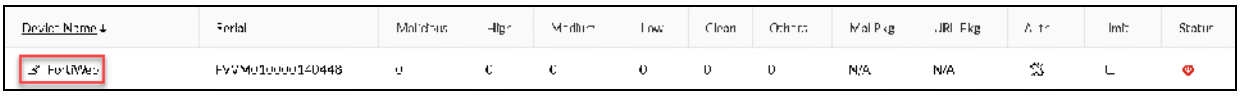
6. Click **OK**.

To authorize FortiWeb on FortiSandbox

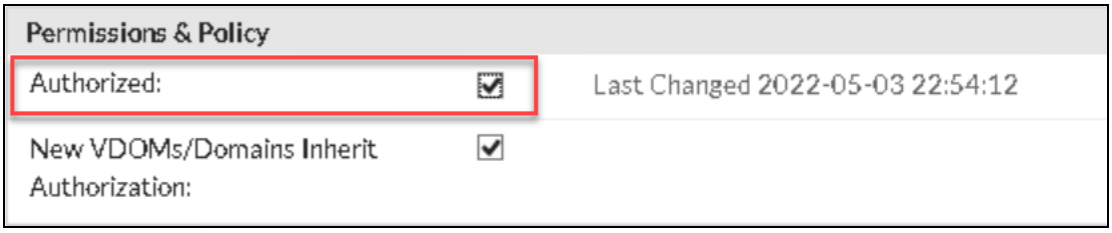
1. On the FortiSandbox GUI, log in with the username `admin` and password `password`.
2. Click **Security Fabric** > **Device**.
3. Click **FortiWeb**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



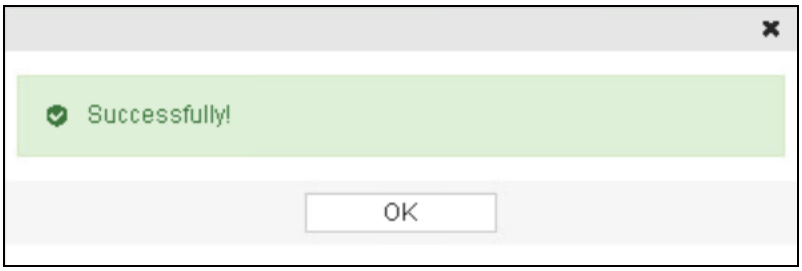
4. In the **Permissions & Policy** section, select the **Authorized** checkbox.



5. Click **OK** for the notification warning.
6. Click **OK**.

To verify connectivity between FortiWeb and FortiSandbox

1. Return to the FortiWeb GUI, and click **Test Connectivity**.
   A success message appears.



2. Click **OK**.

To enable the FortiSandbox malware signature database

1. Continuing on the FortiWeb GUI, click **System** > **Config** > **FortiGuard**.
2. Enable **Use FortiSandbox Malware Signature Database**.

3. Click **Apply**.
4. Refresh the page until you see that the database version is updated.

5. Return to the FortiSandbox GUI, and then click **Scan Policy and Object** > **Malware Package**.
6. Verify that the database version on FortiWeb matches the latest database version on FortiSandbox.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Version	Release Time
4.106	2022-05-03 22:39:01
4.105	2022-05-03 22:26:02
4.104	2022-05-03 13:45:02

To enable event logs for FortiSandbox file submissions

1. Open an SSH connection to the FortiWeb VM.
2. Enter the following commands to enable event logs of FortiSandbox file submissions:

```
config system fortisandbox
   set elog enable
end
```

3. Close the FortiWeb SSH session browser tab.

Configure FortiWeb for Sandboxing

To enable sandboxing, you will configure a file security policy. Then, you will enable the file security policy on a web protection profile, and apply it to a server policy.

To configure a file security policy

1. Return to the FortiWeb GUI, and then click **Web Protection** > **Input Validation** > **File Security**.
2. In the **File Security Policy** section, click **Create New**.
3. Configure the following settings:

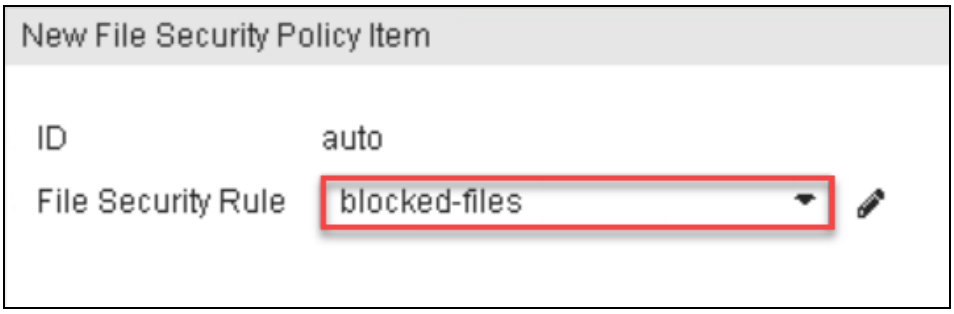
Field	Value
Name	FSA-Check
Action	Alert & Deny
Severity	High
Antivirus Scan	Enabled
Send Files to FortiSandbox	Enabled
Hold Session While Scanning File	Enabled

4. Click **OK**.
5. Scroll down to the bottom of the page, and in the **File Security Rule** section, click **Create New**.

6. In the **File Security Rule** drop-down list, select **blocked-files**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

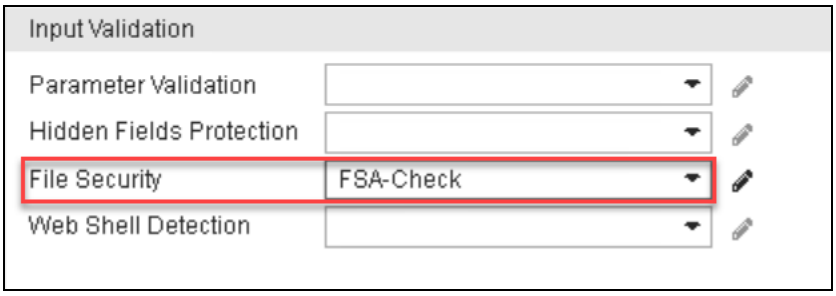


The **blocked-files** file security rule is preconfigured to *block all audio and video files* and *allow everything else*. You can click the pencil icon (✎) to review the configuration.

7. Click **OK**.

To configure the web protection profile

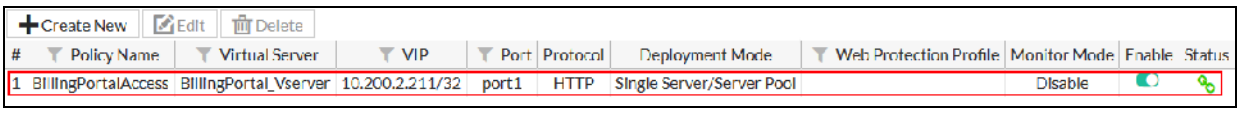
1. Continuing on the FortiWeb GUI, click **Policy** > **Web Protection Profile**.
2. Click **Create New**.
3. In the **Name** field, type `WPP-AcmeCorp`.
4. In the **Standard Protection** section, in the **Signatures** drop-down list, select **Signature_Alert&Deny**.
5. In the **Input Validation** section, in the **File Security** drop-down list, select **FSA-Check**.



6. Click **OK**.

To configure the server policy

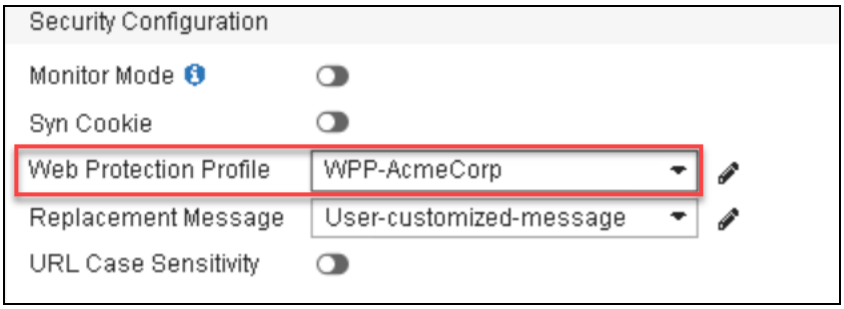
1. Continuing on the FortiWeb GUI, click **Policy** > **Server Policy**.
2. Double-click the existing **BillingPortalAccess** policy.



3. In the **Security Configuration** section, in the **Web Protection Profile** drop-down list, select **WPP-AcmeCorp**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



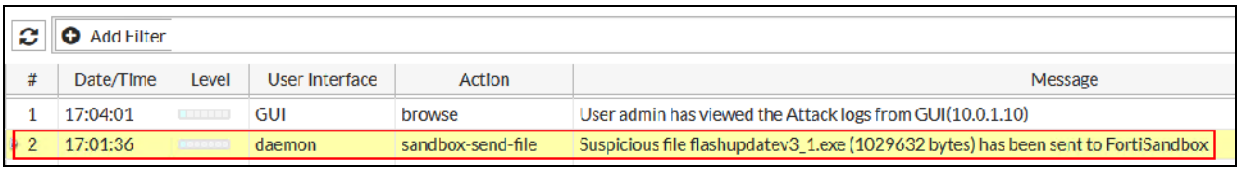
4. Click **OK**.

Verify Sandbox Inspection

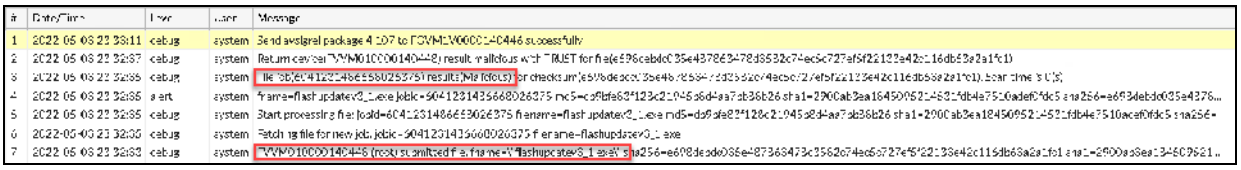
You will verify sandbox inspection using multiple malware samples.

To verify file submission to FortiSandbox for inspection

1. On the Remote-Host VM, open Chrome, and then connect to the Acme Corp Billing Portal at `http://billings.acmecorp.net`.
2. Log in with the username `jsmith` and password `jsmith01`.
3. Click **Choose File**.
4. Click **Desktop** > **Resources** > **Lab 6 - Protecting Web Applications** > `flashupdatev3_1.exe`, and then click **Open**.
5. Click **Upload Invoice**.
   FortiWeb holds the file upload session while waiting for a verdict from FortiSandbox.
6. Return to the FortiWeb GUI, and click **Log & Report** > **Log Access** > **Event**.
7. Verify that the file was sent to FortiSandbox.



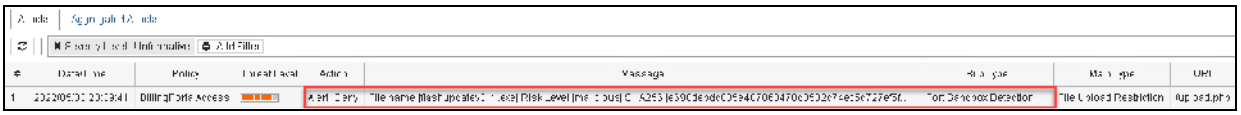
8. Return to the FortiSandbox management GUI, and click **Log & Report** > **Events** > **Job Events**.
9. Verify that FortiSandbox has scanned the file and generated a verdict



10. Log out of the FortiSandbox GUI.
11. Return to the FortiWeb GUI, and click **Log&Report** > **Log Access** > **Attack**.
12. Review the log details:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

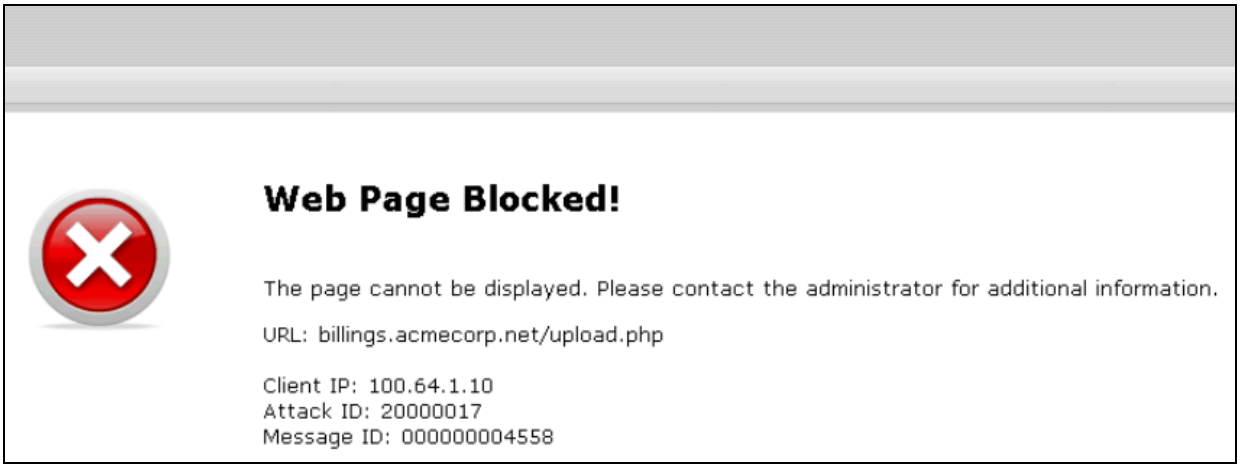
DO NOT REPRINT
© FORTINET
Brave-Dumps.com



If you don't see an attack log entry for the `flashupdatev3_1.exe` file, wait a few minutes, and then click the refresh icon ( ).

To verify antivirus inspection using the local cache

1. Return to the Remote-Host VM, and verify that the upload was blocked.



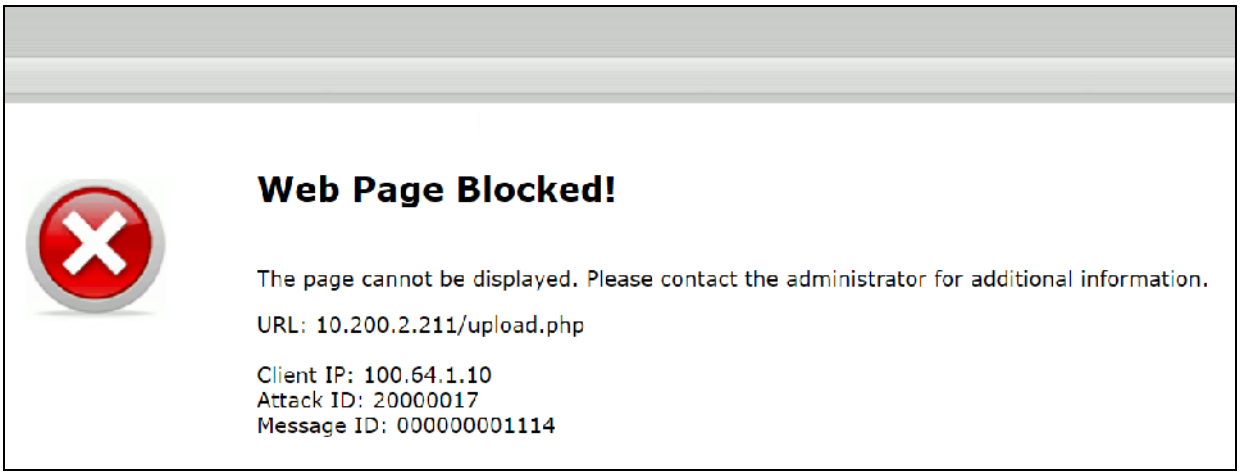
When you attempted to upload the `flashupdatev3_1.exe` file, FortiWeb held the session while it waited for FortiSandbox to finish scanning the file. After FortiSandbox supplied the verdict, FortiWeb blocked the upload. The file was never saved on the server storage.

2. Open another Chrome browser tab, and then connect to the Acme Corp Billing Portal at `http://billings.acmecorp.net`.
3. Click **Choose File**.
4. Click **Desktop** > **Resources** > **Lab 6 - Protecting Web Applications** > `flashupdatev3_2.exe`, and then click **Open**.
5. Click **Upload Invoice**.

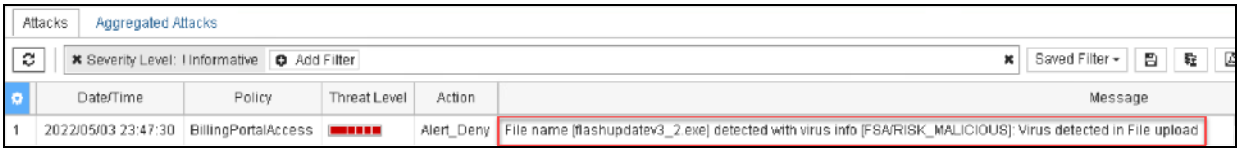
   A block page appears.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



6. Close Chrome.
7. Close the Remote-Host VM browser tab.
8. Return to the FortiWeb GUI, and then click **Log&Report** > **Log Access** > **Attack**.
9. Review the log details.



10. Click **Log&Report** > **Log Access** > **Event**.
    Was the `flashupdatev3_2.exe` file sent to FortiSandbox?

If you see a log entry with a `suspicious` verdict, wait a few more minutes, and then upload the `flashupdatev3_2.exe` file again. It may take a few minutes for FortiWeb to receive the malware database update from FortiSandbox.

11. Log out of the FortiWeb GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 3: Diagnosing FortiWeb Submissions

In this exercise, you will run some diagnostic commands on FortiSandbox and analyze the debug messages for FortiWeb submissions.

Diagnose FortiWeb Submissions

You will run diagnostic commands on FortiSandbox and analyze the generated output for files that FortiWeb submitted.

To enable debugging on FortiSandbox

1. Open an SSH session to the FortiSandbox VM.
2. Enter the following command to display the available options:
   `diagnose-debug -h`

You can use the `diagnose-debug` command to view real-time debug messages for file submissions and threat intelligence sharing with integrated devices.

3. Enter the following command to enable debugging for files that FortiWeb submitted:
   `diagnose-debug device FVVM010000140448`
4. Leave the SSH session open in the background.

To upload malware samples

1. On the Remote-Host VM, open Chrome, and then connect to the Acme Corp Billing Portal at `http://billings.acmecorp.net`.
2. Log in as `jsmith` with the password `jsmith01`.
3. Click **Choose File**.
4. Click **Desktop** > **Resources** > **Lab 6 - Protecting Web Applications** > `flashupdatev3_3.exe`, and then click **Open**.
5. Click **Upload Invoice**.

To analyze the debug output

1. Return to the FortiSandbox CLI.
2. Review the debug messages.
   FortiWeb sends the ADOM name, filename, source IP address, and destination IP address:

```
FVVM01000079329 VDOM: root
FVVM01000079329 File Name: flashupdatev3_3.exe
FVVM01000079329 Source IP: 100.64.1.10:1
FVVM01000079329 Destination IP: 10.200.2.10:1
```

   FortiSandbox stores received files in a temporary folder for scanning:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

Brave-Dumps.com
DO NOT REPRINT
© FORTINET


```
[store_pkg.c:294] FVVM01000079329 File name:1:1:1. Package size:1. Total file
    number:1. Total file size:1.
[store_pkg.c:424] FVVM01000079329 store first stage was successful
FVVM01000079329 Committed new file successfully /drive0/private/temp/fgtpre/tmp/oftp_
    ca_0hPzpx
```

3. Press `Ctrl` + `C` to disable debugging.
4. Close the FortiSandbox SSH session browser tab.
5. Close the Remote-Host VM browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 7: Protecting End Users

In this lab, you will configure FortiClient to submit files to FortiSandbox. Then, you will verify your configuration using multiple malware samples.

Objectives

- Configure FortiClient to submit files to FortiSandbox for inspection
- Monitor the FortiSandbox inspection results and statistics for the inspected files

Time to Complete

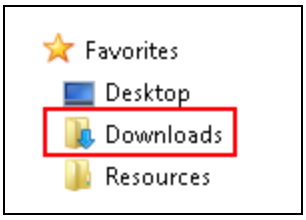
Estimated: 30 minutes

Prerequisites

Before beginning this lab, you must delete all samples from the **Downloads** folder. You must also restore a configuration file to FortiMail and FortiGate.

To delete files in the downloads folder

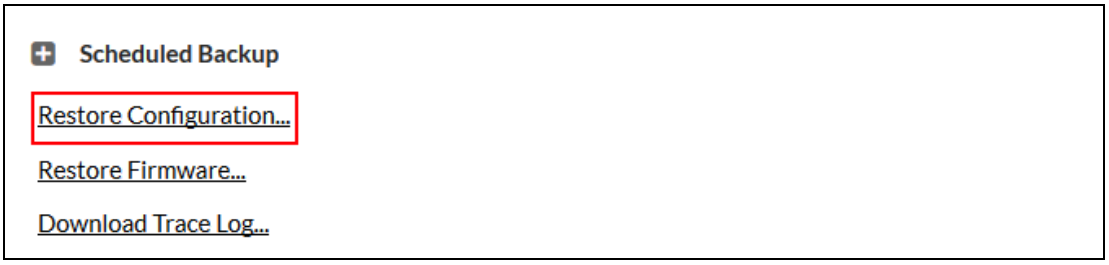
1. On the Local-Host VM desktop, double-click **Computer**.
2. On the navigation pane, click **Downloads**.



3. Press `Ctrl+A` to select all files.
4. Press `Shift+Delete` to delete the files.

To restore the FortiMail configuration file

1. Open a Firefox browser tab, and then log in to the FortiMail administrator GUI at `https://10.200.2.100/admin` with the username `admin` and password `password`.
2. Click **System** > **Maintenance**.
3. Click **Restore Configuration**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

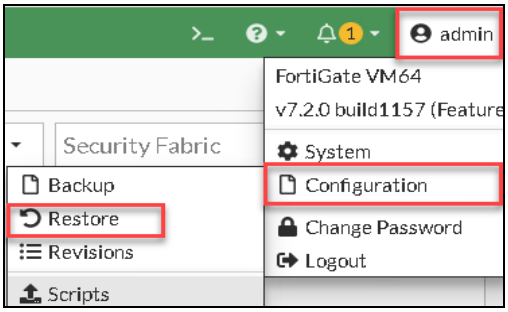
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

4. Click **Desktop** > **Resources** > **Lab 7 - Protecting End Users** > `Lab_7_FortiMail.cfg`, and then click **Open**.
5. Click **OK** to reboot.

   Wait until the browser is redirected to the FortiMail login page.

To restore the FortiGate configuration file

1. Continuing on the Local-Host VM, open a Firefox browser tab, and then log in to the FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Lab 7 - Protecting End Users** > `Lab_7_FortiGate.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

   Wait until the browser is redirected to the login page.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Integrating FortiSandbox With FortiClient

In this exercise, you will integrate FortiSandbox with FortiClient. You will configure FortiClient sandbox detection settings to offload files to FortiSandbox. Then, you will verify your configuration using various malware samples.

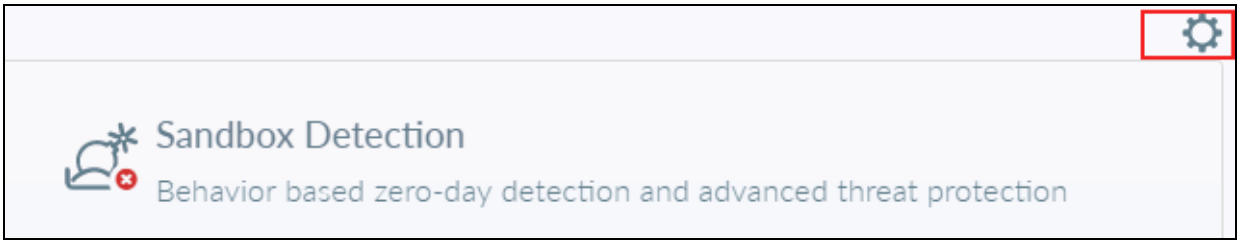
Configure FortiSandbox Integration

You will configure the required settings on FortiClient to integrate with FortiSandbox. You will then authorize FortiClient on FortiSandbox, and verify connectivity between the two devices.

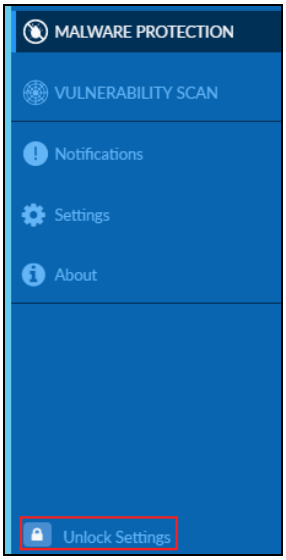
To configure the sandbox settings on FortiClient

1. Go to the Local-Host VM and, on the desktop, double-click FortiClient.
2. In the pane on the left side of the window, click **MALWARE PROTECTION**.
3. In the upper-right corner, click the **Settings** icon ( ).

   The configuration tab opens.



4. Click **Unlock Settings**.

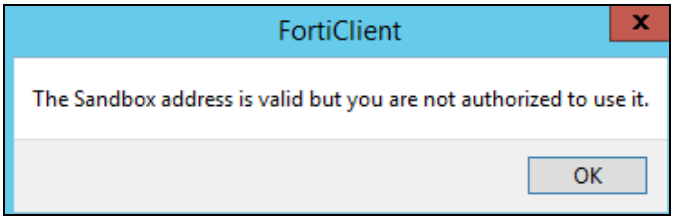


5. Enable **Sandbox Detection**.
6. In the **IP** field, type `10.0.1.213`.
7. Click **Test**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

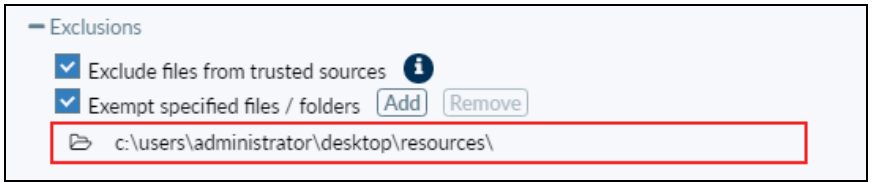
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

An error message appears.

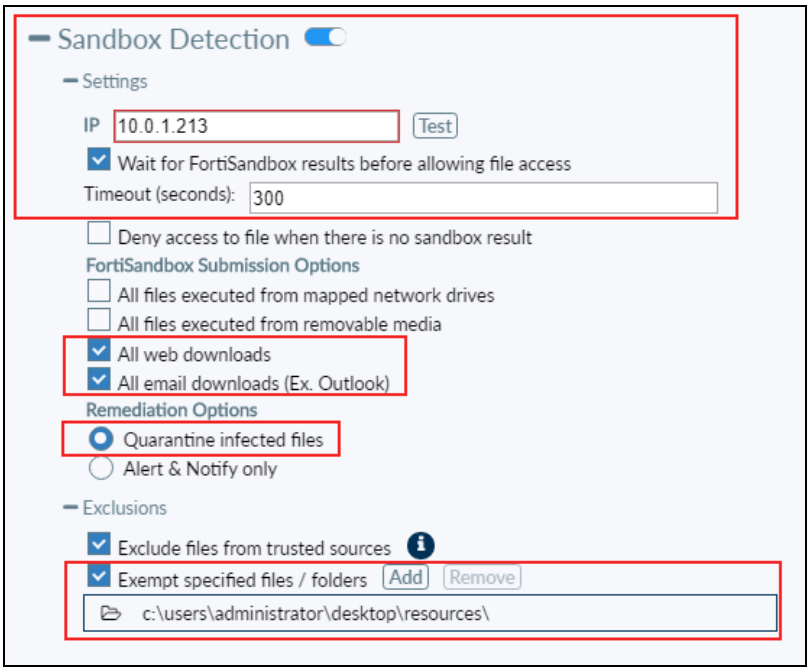


8. Click **OK**.
9. Select the **Wait for FortiSandbox results before allowing file access** checkbox.
10. In the **Timeout** field, type `300` (five minutes).
11. In the **FortiSandbox Submission Options** section, select the **All Email Downloads** checkbox.
12. In the **Exclusions** section, verify that **Exempt specified files / folders** is enabled.

FortiClient has been preconfigured to exempt the **Resources** folder.



Your configuration should match the following example:



To authorize FortiClient on FortiSandbox

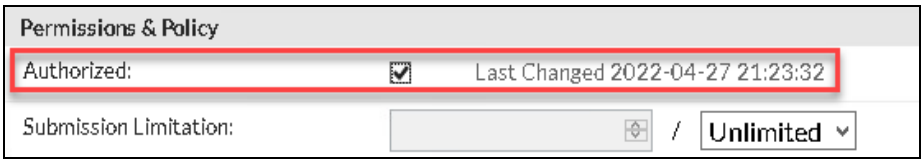
1. Log in to the FortiSandbox GUI with the username `admin` and password `password`.
2. Click **Security Fabric** > **FortiClient**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

3. Click the FortiClient entry.

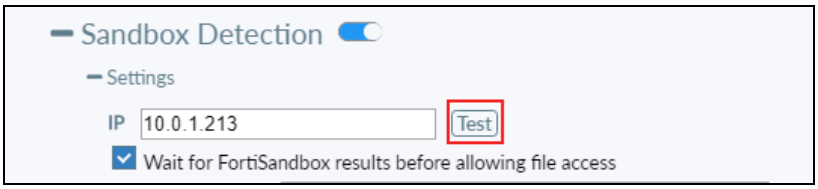
4. In the **Permissions & Policy** section, select the **Authorized** checkbox.



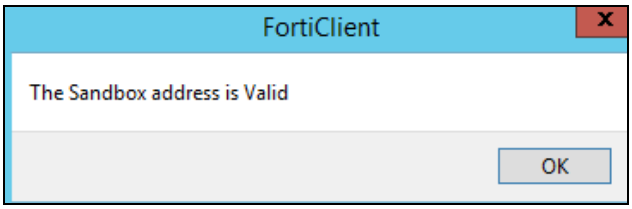
5. Click **OK**.

To verify connectivity between FortiClient and FortiSandbox

1. Return to the Local-Host VM and, in the FortiClient window, click **Test**.



2. A pop-up window opens to confirm that the sandbox address is valid.



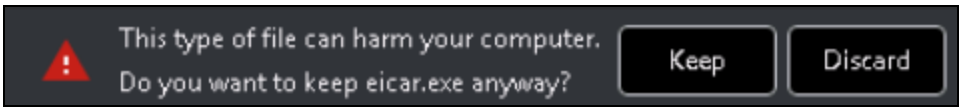
3. Click the close icon ( ).

Verify Sandbox Inspection

You will verify sandbox inspection using multiple malware samples.

To verify sandbox inspection with a known virus

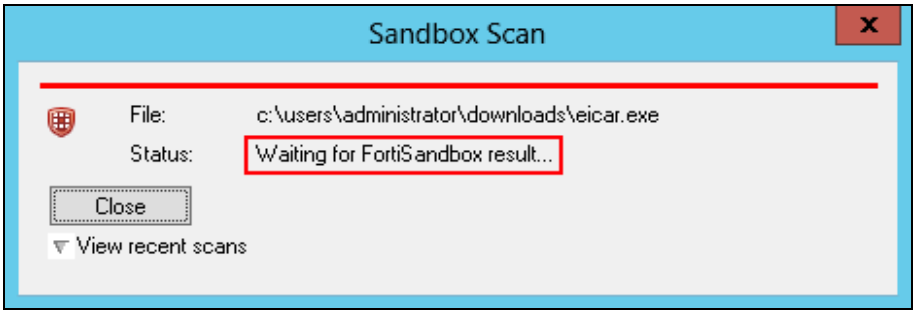
1. Continuing on the Local-Host VM, open Google Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
2. Click **EICAR**.
   A security warning appears.



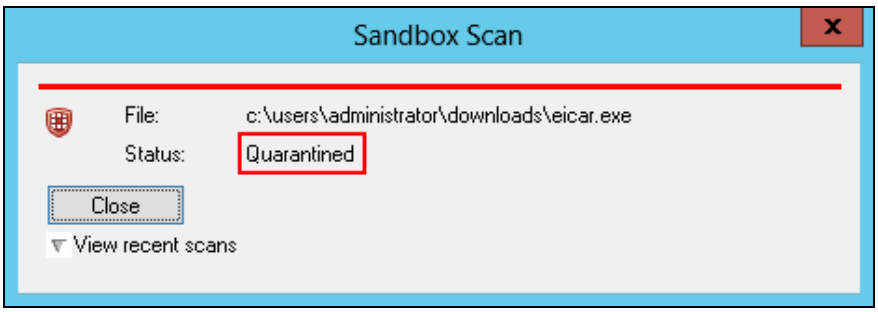
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

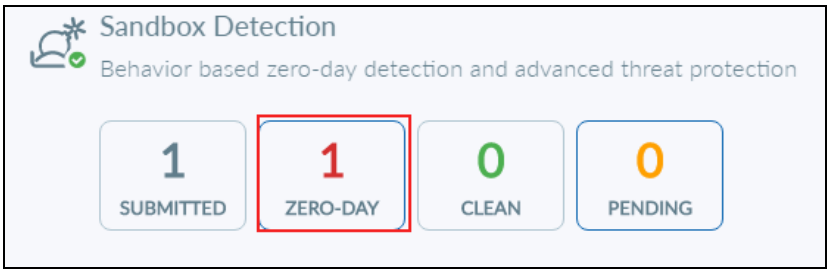
3. Click **Keep**.
   The **Sandbox Scan** window opens.



4. Close Chrome.
5. Return to the FortiClient **Sandbox Scan** window.
6. Wait for FortiClient to quarantine the file, and then click **Close**.



7. Return to the Local-Host VM, and in the FortiClient window, click **MALWARE PROTECTION**.
   You will notice that one file was submitted to the sandbox and that file was detected as zero-day malware.



EICAR is not zero-day malware. The reason that FortiClient identified EICAR as zero-day malware is because FortiClient has only the advanced persistent threat (APT) module installed, and therefore FortiClient is not performing any signature-based antivirus scanning.

8. Click **Close**.

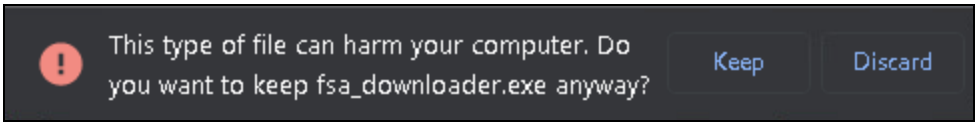
To verify sandbox inspection with a high-risk sample

1. Continuing on the Local-Host VM, open Chrome, and then connect to the Malware Sample Portal at `http://portal.training.lab`.
2. Click **Downloader**.

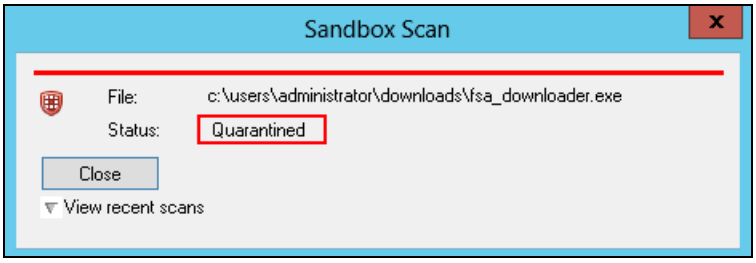
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

A security warning appears.



3. Click **Keep**.
4. Close Chrome.
5. Return to FortiClient, and then wait for the file to be quarantined.



6. Click **Close**.

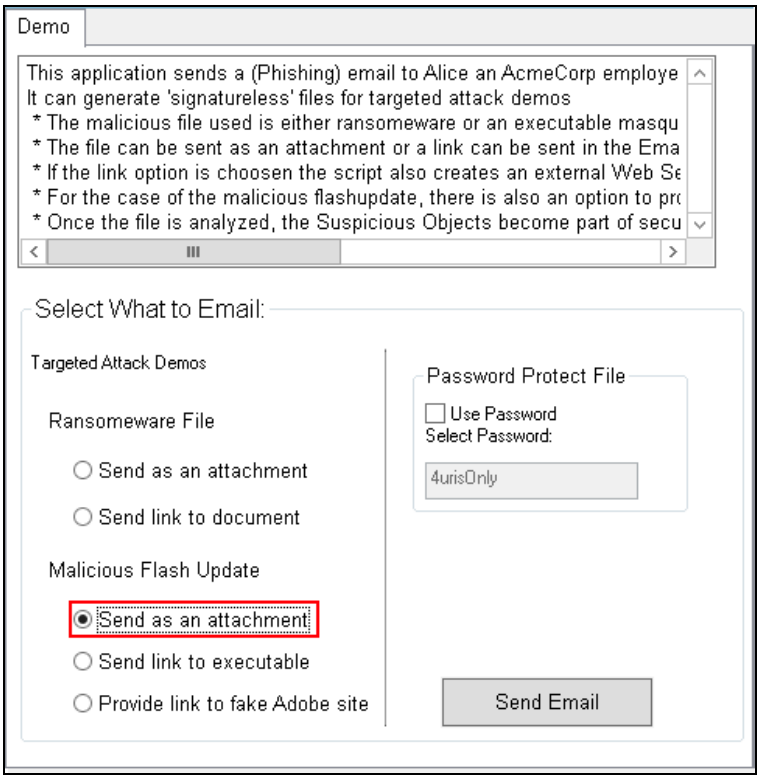
To verify sandbox inspection of email attachments

1. Go to the Remote-Host VM and, on the desktop, double-click **ATP Email Sender**.

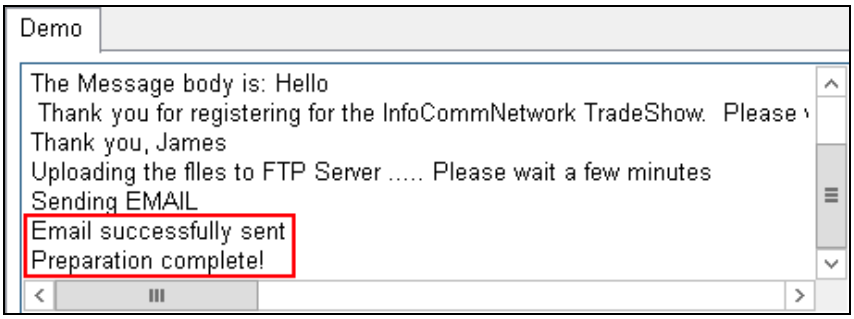
2. In the **Malicious Flash Update** section, select **Send as an attachment**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



3. Click **Send Email**.
   Wait until the email is sent.



4. Close the application.
5. Close the Remote-Host VM browser tab.
6. Return to the Local-Host VM, and open Thunderbird.
7. Click **alice@acmecorp.net** > **Inbox**.
8. Double-click the latest email in the inbox to open it.
9. Save the attachment.

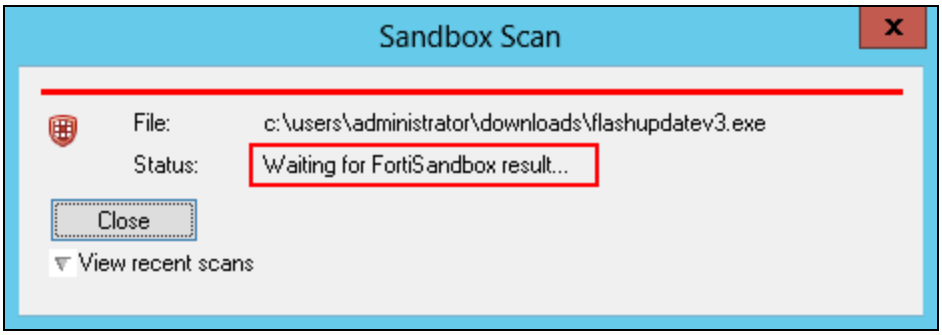
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The **Save Attachment** prompt appears.

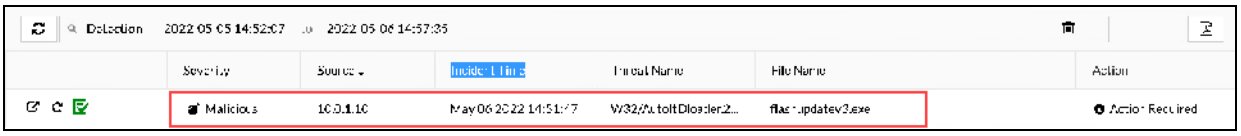
10. Click **Downloads**.
11. Click **Save**.
12. Close Thunderbird.
13. On the Local-Host VM desktop, double-click **Computer**.
14. Click **Downloads**.

    The **Sandbox Scan** window opens.



Wait until the file is quarantined.

15. Click **Close**.
16. Close Thunderbird.
17. Return to the FortiSandbox management GUI, and click **Dashboard** > **Operation Center**.
18. Verify the verdict for the file.



19. Log out of the FortiSandbox management GUI.

Disable FortiSandbox Scanning on FortiClient

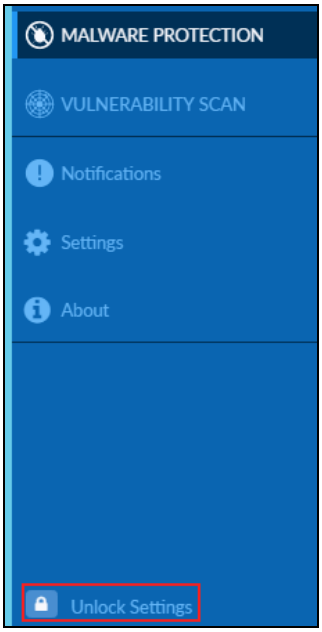
You will disable FortiSandbox scanning on FortiClient so FortiClient does not interfere with the next lab exercises.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

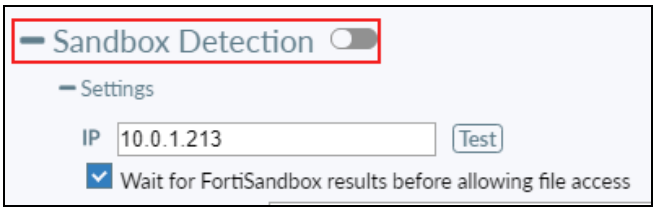
Brave-Dumps.com
DO NOT REPRINT
© FORTINET

To disable FortiSandbox scanning on FortiClient

1. Return to the Local-Host VM and, in the FortiClient window, click **MALWARE PROTECTION**.
2. Click the **Settings** icon ( ).
   The configuration tab appears.
3. Click **Unlock Settings**.



4. Disable **Sandbox Detection**.



5. Close FortiClient.
6. Close the Local-Host VM browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 8: Protecting Third-Party Devices

In this lab, you will configure network share scanning and sniffer mode inspection on FortiSandbox.

Objectives

- Configure network share scanning

Time to Complete

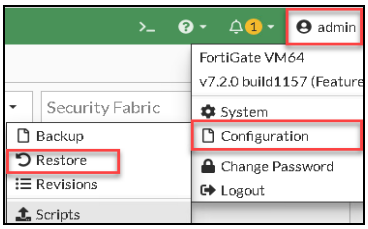
Estimated: 20 minutes

Prerequisites

You must restore a configuration file to FortiGate.

To restore the FortiGate configuration file

1. On the Local-Host VM, open a Firefox browser tab, and then log in to the FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **Lab 8 - Protecting Third Party Appliances** > `Lab_8_FortiGate.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot.

   Wait until the browser is redirected to the login page.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Configuring Network Share Scanning

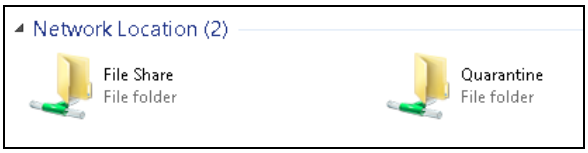
In this exercise, you will configure network share scanning on FortiSandbox.

Access the File Share

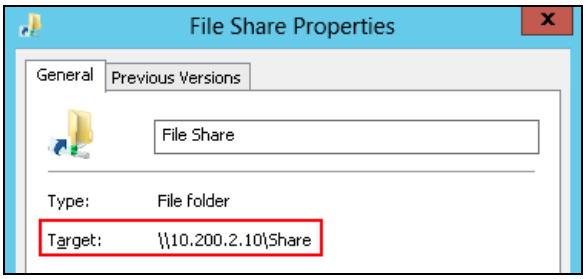
Two file shares have been created on the Linux-Server VM. The file shares are mounted as network folders on the Local-Host VM. You will save samples to the file shares.

To access the file share

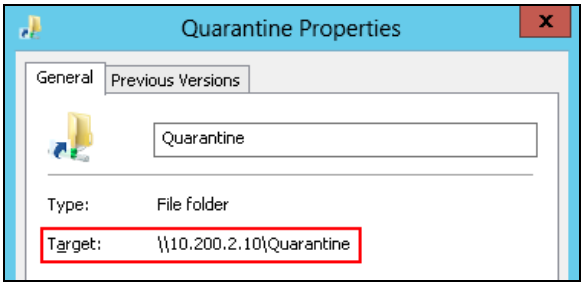
1. Go to the Local-Host VM and, on the desktop, double-click **Computer**.
2. Verify that there are two preconfigured network folders.



3. Right-click **File Share**, and then select **Properties**.
   The **File Share Properties** window opens.
4. Note the **Target** location for the **File Share** folder.



5. Click **OK**.
6. Right-click **Quarantine**, and then select **Properties**.
   The **Quarantine Properties** window opens.
7. Note the **Target** value for the **Quarantine** folder.



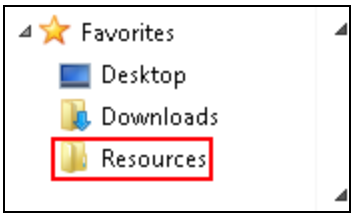
8. Click **OK**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

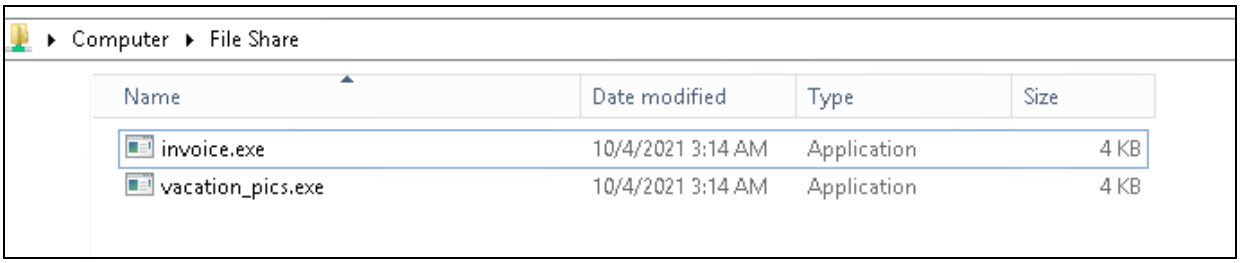
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

To save the samples to the file share

1. Continuing on Windows Explorer, in the navigation pane, click **Resources**.



2. Double-click **Lab 8 - Protecting Third Party Appliances**.
3. Copy `invoice.exe` and `vacation_pics.exe` to the **File Share** network folder.
4. Before you continue to the next step, verify that the `invoice.exe` and `vacation_pics.exe` files are in the **File Share** folder.



5. Close Windows Explorer.

Configure Network Share Scanning

You will configure network share scanning on FortiSandbox.

To configure the quarantine folder location

1. Log in to the FortiSandbox GUI with the username `admin` and password `password`.
2. Click **Security Fabric** > **Quarantine**.
3. Click **Create New**.
4. Configure the following values:

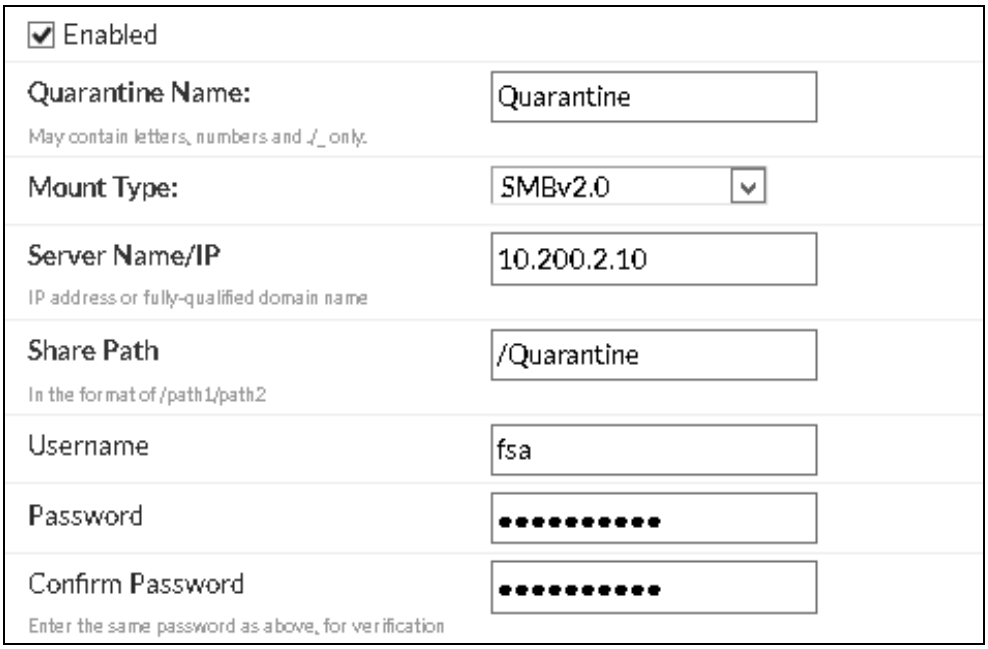
Field	Value
Quarantine Name	Quarantine
Server Name/IP	10.200.2.10
Share Path	/Quarantine
Username	fsa
Password	Fortinet1!

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

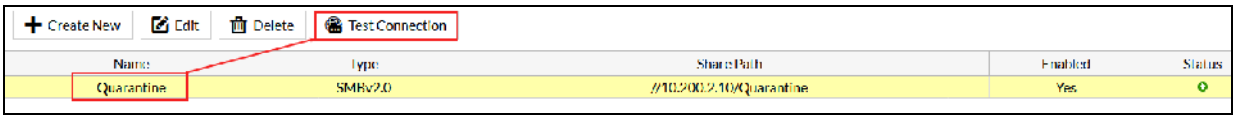
DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Field	Value
Confirm Password	Fortinet1!
Keep Original File At Source Location	Disabled

Your configuration should match the following example:



5. Click **OK**.
6. Click **Quarantine**, and then click **Test Connection**.



A success message appears.

To configure network share scanning

1. Continuing on the FortiSandbox GUI, click **Security Fabric** > **Network Share**.
2. Click **Create New**.
3. Configure the following values:

Field	Value
Network Share Name	Share

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

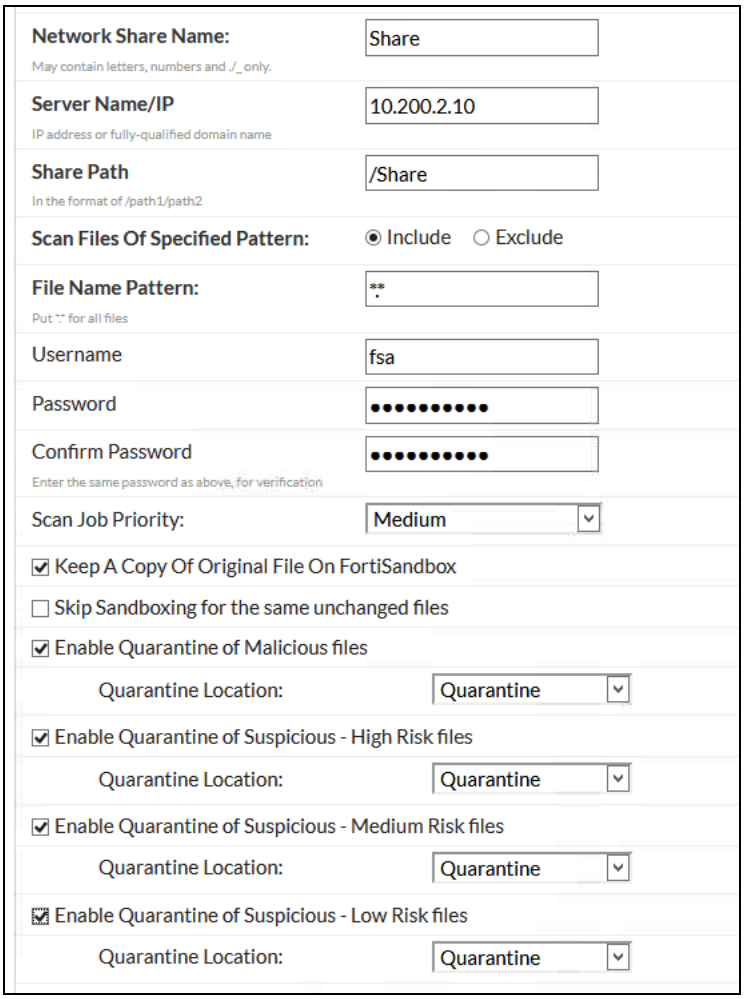
Brave-Dumps.com
DO NOT REPRINT
© FORTINET

Field	Value
Server Name/IP	10.200.2.10
Share Path	/Share
File Name Pattern	*.*
Username	fsa
Password	Fortinet1!
Confirm Password	Fortinet1!
Enable Quarantine of Malicious files	Enabled
Enable Quarantine of Suspicious - High Risk files	Enabled
Enable Quarantine of Suspicious - Medium Risk files	Enabled
Enable Quarantine of Suspicious - Low Risk files	Enabled

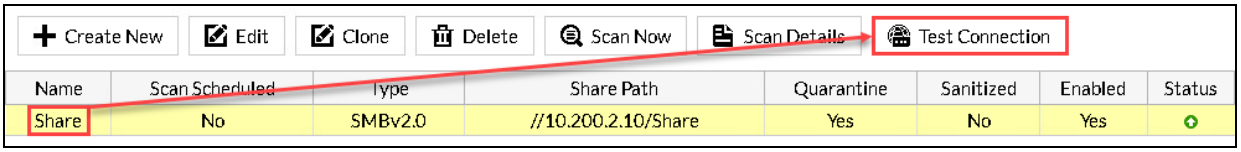
Your configuration should match the following example:

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



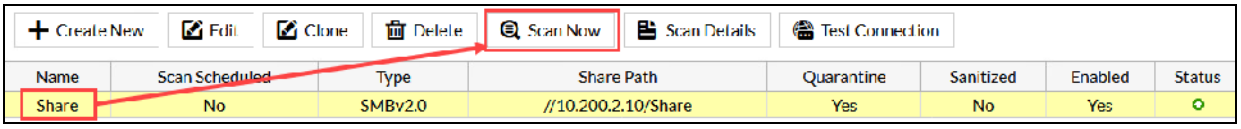
4. Click **OK**.
5. Click **Share**, and then click **Test Connection**.



A success message appears.

To scan samples in the network share

1. Continuing on the FortiSandbox GUI, click **Share**, and then click **Scan Now**.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

A success message appears.

2. Click **Scan Job** > **VM Jobs**.
3. Verify that the files are being scanned.

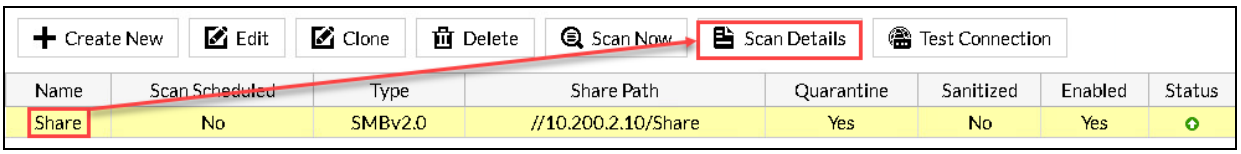
4. Before continuing to the next step, wait until the scan completes.

Verify Network Share Scanning

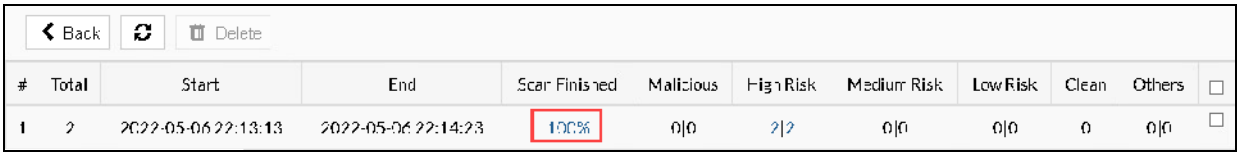
You will verify network share scanning on FortiSandbox. You will also view the **Quarantine** folder to verify that FortiSandbox has moved the high-risk samples from the original location.

To verify network share scanning on FortiSandbox

1. Continuing on the FortiSandbox GUI, click **Security Fabric** > **Network Share**.
2. Click **Share**, and then click **Scan Details**.



3. Click **100%**.



4. Verify that your scan results match the following example:

5. Log out of the FortiSandbox GUI.

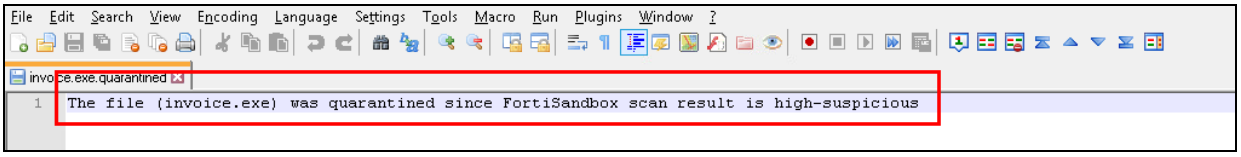
To verify quarantining of high-risk and malicious samples

1. Return to the Local-Host VM and, on the desktop, double-click **Computer**.
2. Double-click **File Share**.

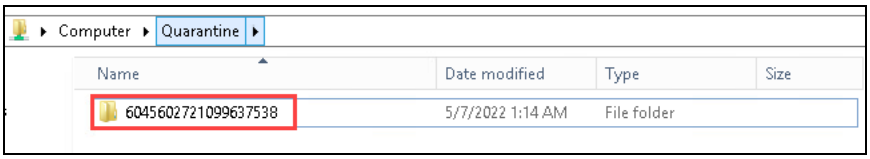
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

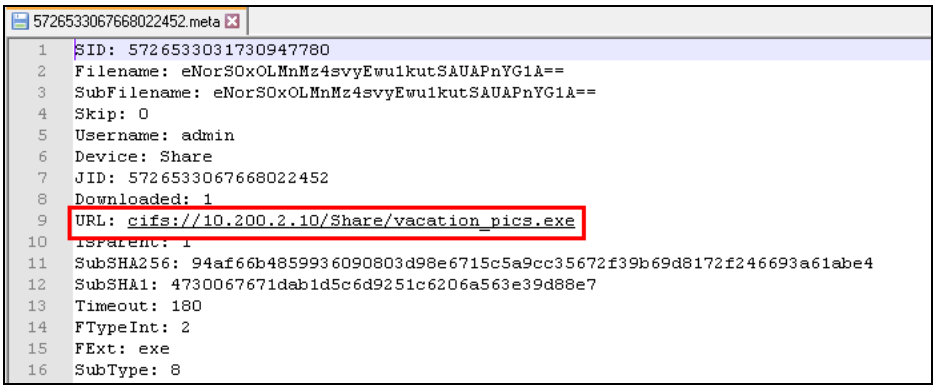
3. Right-click `invoice.exe.quarantined`, and then select **Edit with Notepad++**.
4. Verify that the original file has been quarantined.



5. Close Notepad++.
6. Return to Windows Explorer, and then click **Quarantine** in the navigation pane.
7. Double-click the quarantine folder. (**Note**: FortiSandbox autogenerates the folder name, so your folder name may not match the following example.)



8. Double-click **high_risk**.
9. Right-click the `.meta` file, and then select **Edit with Notepad++**.
10. Verify that FortiSandbox has quarantined the `invoice.exe` and `vacation_pics.exe` files.



11. Close Notepad++.
12. Close Windows Explorer.
13. Close the Local-Host VM browser tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 2: Diagnosing Network Share Scanning

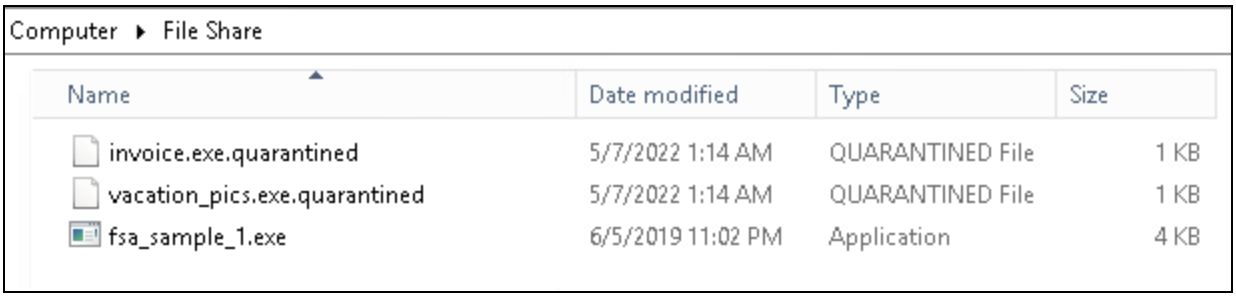
In this exercise, you will copy new samples to the **File Share** network folder, and then diagnose network share scanning on FortiSandbox.

Prepare the File Share

You will copy a new file to the **File Share** network folder.

To copy a new sample to the network share

1. Go to the Local-Host VM and, on the desktop, double-click **Resources**.
2. Double-click **Lab 8 - Protecting Third Party Appliances**.
3. Copy `fsa_sample_1.exe` to the **File Share** network folder.
4. Before you continue to the next step, verify that `fsa_sample_1.exe` is in the **File Share** folder.



5. Close Windows Explorer.

Diagnose Network Share Scanning

You will use FortiSandbox diagnostic commands to view the real-time debug messages of network share scanning.

To enable the real-time debug

1. On the Local-Host VM, open PuTTY, and then connect over SSH to the FORTISANDBOX saved session.
2. Log in with the username `admin` and password `password`.
3. Type the following command to display the available options:

```
diagnose-debug -h
```

You can use the `diagnose-debug` command to view real-time debug messages for file submissions from various sources, and threat intelligence sharing with integrated devices.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

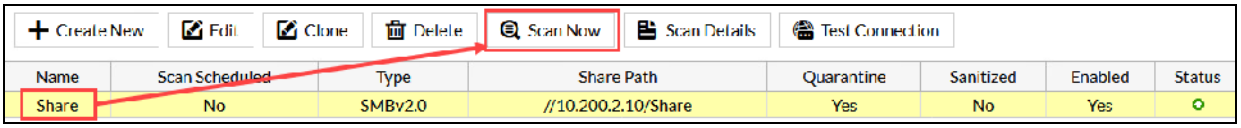
4. Type the following command to enable debugging for files that FortiWeb submits:

```
diagnose-debug netshare
```

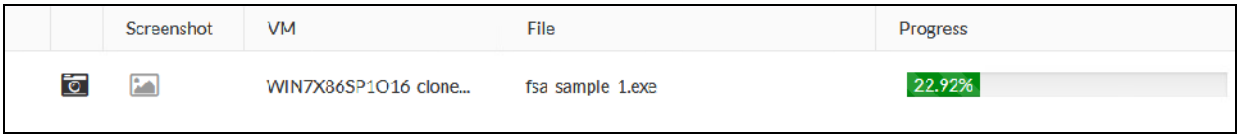
Maximize the PuTTY window, and leave it open in the background.

To start network share scanning

1. Go to the FortiSandbox management GUI.
2. Login with the username `admin` and password `password`.
3. Click **Security Fabric** > **Network Share**.
4. Click **Share**, and then click **Scan Now**.



5. Click **Scan Job** > **VM Jobs**.
6. Wait for the scan job to finish.



7. Close Firefox.

To view real-time debug messages

1. On the Local-Host VM, return to the PuTTY session.
2. Press `Ctrl` + `C` to disable debugging.
3. Review the debug messages.

```
08/20 16:21:09 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:09 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:09 DEBUG [1940 ] JOB->LOADING starting to load all network share files to DB for job (5118025667365269072).
08/20 16:21:09 DEBUG [1940 ] JOB->LOADING job (5118025667365269072) state from JOB_NEW to JOB_FILE_LOADED.
08/20 16:21:09 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) has medium priority, (100) ready submit files.
08/20 16:21:09 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) state from JOB_FILE_LOADED to JOB_RUNNING
08/20 16:21:09 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) starting to submit files ...
08/20 16:21:09 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:09 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:09 DEBUG [14223] JOB->LOADING job (5118025667365269072) completed.
08/20 16:21:09 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) has medium priority, (100) ready submit files.
08/20 16:21:09 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) starting to submit files ...
08/20 16:21:09 DEBUG [1940 ] SID: (5118825687528659879), Filename: (eNor50nOLMnMz4nvyEwulkut5NUrLE0nSawrycxLTQEAnc8Lnq==),
Skip: (0), Url: (cifs://10.200.2.10/Share/vacation_pics.exe.quarantined), Username: (admin)
08/20 16:21:09 DEBUG [1940 ] SID: (5118025607528661580), Filename: (eMpLR06HL07MLchOjYfU0611DQAlnQYc),
Skip: (0), Url: (cifs://10.200.2.10/Share/fsa_sample_1.exe), Username: (admin)
08/20 16:21:09 DEBUG [1940 ] SID: (5118025607528662049), Filename: (eNrLzCwLz0xO1Ut5NUrLE0nSawrycxLTQEAbW8JKA==),
Skip: (0), Url: (cifs://10.200.2.10/Share/invoice.exe.quarantined), Username: (admin)
08/20 16:21:09 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072), (3) files were submitted. The last file ID in DB is (3).
08/20 16:21:10 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:10 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:10 DEBUG [1940 ] JOB->PROCESSING: Pending jobs are (3).
08/20 16:21:10 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) has medium priority, (100) ready submit files.
08/20 16:21:10 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) starting to submit files ...
08/20 16:21:10 DEBUG [1940 ] JOB->SUBMIT job (5118025667365269072) all files were submitted, change state from JOB_RUNNING to JOB_COMPLETE.
08/20 16:21:11 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:11 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:11 DEBUG [1940 ] ARCHIVE->CLEAN_WORKER: 5118825687528659879,5118825693372940585
08/20 16:21:11 DEBUG [1940 ] ARCHIVE->CLEAN_WORKER: 5118025607528661580,5118025693406581996
08/20 16:21:11 DEBUG [1940 ] ARCHIVE->CLEAN_WORKER: 5118025607528662049,5118025693339134701
08/20 16:21:12 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:12 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:13 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:13 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:14 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:14 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:15 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:21:15 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:21:15 DEBUG [1940 ] RESULT->RETRIEVE: original file (5118025607528662049,5118025693339134701.1), SID (5118025607528662049), JID (5118025693339134701), score (1)
08/20 16:21:15 DEBUG [1940 ] RESULT->RETRIEVE: original file (5118825687528659879,5118825693372940585.1), SID (5118825687528659879), JID (5118825693372940585), score (1)
08/20 16:21:15 DEBUG [16724] RESULT->UPDATE: start update for /tmp/netshare_update_file_5118025790612103501
08/20 16:21:15 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:22:16 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:22:16 DEBUG [1940 ] RESULT->RETRIEVE: original file (5118025607528661580,5118025693406581996.1), SID (5118025607528661580), JID (5118025693406581996), score (1)
08/20 16:22:16 DEBUG [7095 ] RESULT->UPDATE: start update for /tmp/netshare_update_file_5118026038590652957
08/20 16:22:16 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:22:16 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:22:17 DEBUG [1940 ] JOB->RESULT job (5118025667365269072) change state from JOB_COMPLETE to JOB_UPDATED.
08/20 16:22:18 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
08/20 16:22:18 DEBUG [1940 ] SHARE->MOUNT starting to process shares...
08/20 16:22:19 DEBUG [1940 ] QUARANTINE->MOUNT starting to process quarantine...
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

4. FortiSandbox loads the files from the network share to its local database.

```
SHARE->MOUNT starting to process shares...

JOB->LOADING starting to load all network share files to DB for job
(3848068416176666943).

JOB->LOADING job (3848068416176666943) completed.

JOB->LOADING job (3848068416176666943) state from JOB_NEW to JOB_FILE_LOAED.
```

5. The file is copied to a temporary directory for inspection.

```
JOB->SUBMIT job (3848068416176666943) has medium priority, (100) ready submit
files.

JOB->SUBMIT job (3848068416176666943) state from JOB_FILE_LOADED to JOB_
RUNNING

JOB->SUBMIT job (3848068416176666943) starting to submit files ...

SID: (3848068478044497726), Filename: (eNpLK06ML07MLchJjTfUS61IBQA1nQYc),
Skip: (0), Url: (cifs://10.200.2.10/Share/fsa_sample_1.exe), Username:
(admin)
```

6. After inspection is complete, FortiSandbox generates a rating (`score (1)` is clean).

```
RESULT->RETRIEVE: original file (5118825687528662049.5118825693339134701.1),
SID (5118825687528662049), JID (5118825693339134701), score (1)
```

7. Type the following command to exit PuTTY:

```
exit
```


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Lab 9: Analysis of Results

In this lab, you will examine the verdicts that FortiSandbox generates for a URL scan.

Objectives

- Analyze the output of a URL linking to a suspicious executable
- Override a FortiSandbox verdict

Time to Complete

Estimated: 30 minutes

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

Exercise 1: Analyzing a URL

In this exercise, you will analyze the scan job report of the malicious URL that was sent to Alice in a previous lab.

Access the Scan Job Report

You will review the scan job report of the malicious URL that was sent to Alice.

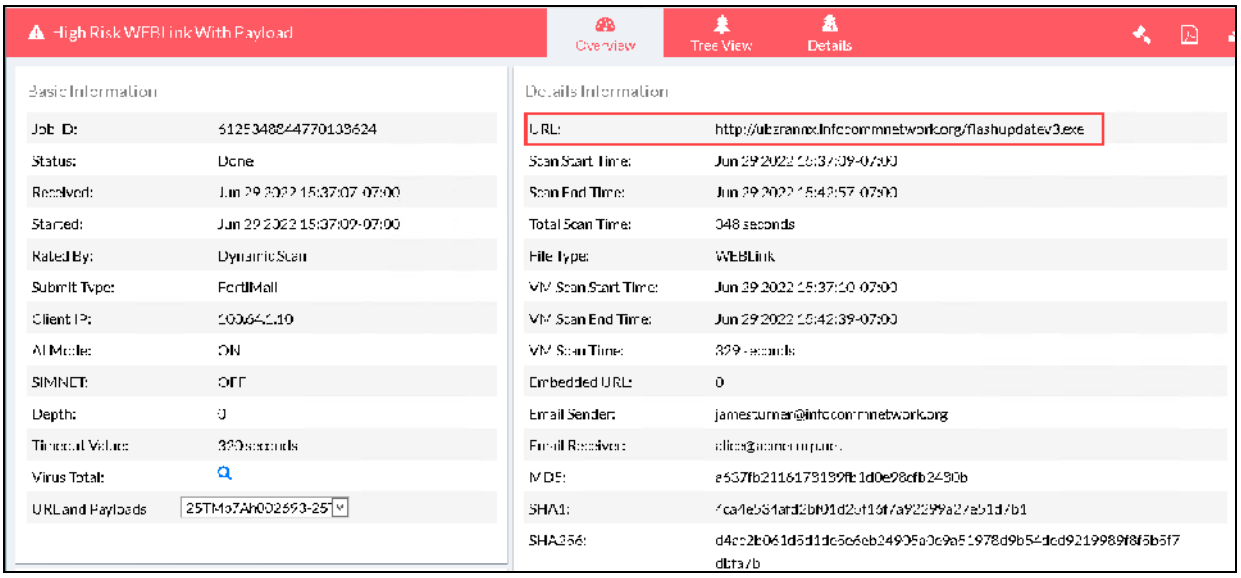
To access the URL scan job report

1. Log in to the FortiSandbox GUI with the username `admin` and password `password`.
2. Click **Scan Job** > **URL Job Search**.

There are multiple ways that you can access a scan job report. Other methods that you can use to access the reports include using the alert emails, the **Scanning Statistics** widget on the dashboard, or the various FortiView subsections.

3. Locate the `infocommnetwork.org` URL entry with a **High Risk** verdict, and then click the view details icon ( ).

The scan job report is displayed.



Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The left pane contains the **Basic Information** and **Indicators** sections. FortiSandbox used one VM to analyze this file. If FortiSandbox used other VMs, the summary would include information from all VMs.

The right pane contains the **Details Information** section, which displays the **File Type**, **URL**, **Submit Device**, and **Launched OS** rows. In this case, the file type is **WEBLink**, the file was submitted by **FortiMail**, and the OS that scanned it was a Windows 7 VM.

4. Review the URL in the **Details Information** section.

Details Information

URL:	http://ubzrannx.infocommnetwork.org/flashupdatev3.exe
Scan Start Time:	Jun 29 2022 15:37:09-07:00
Scan End Time:	Jun 29 2022 15:42:57-07:00
Total Scan Time:	348 seconds
File Type:	WEBLink

Your URL may not match the one that is shown in this example because the ATP Email Sender application randomly generates the URLs.

It is common for URLs to link to executable files, a tactic used by attackers to install malware.

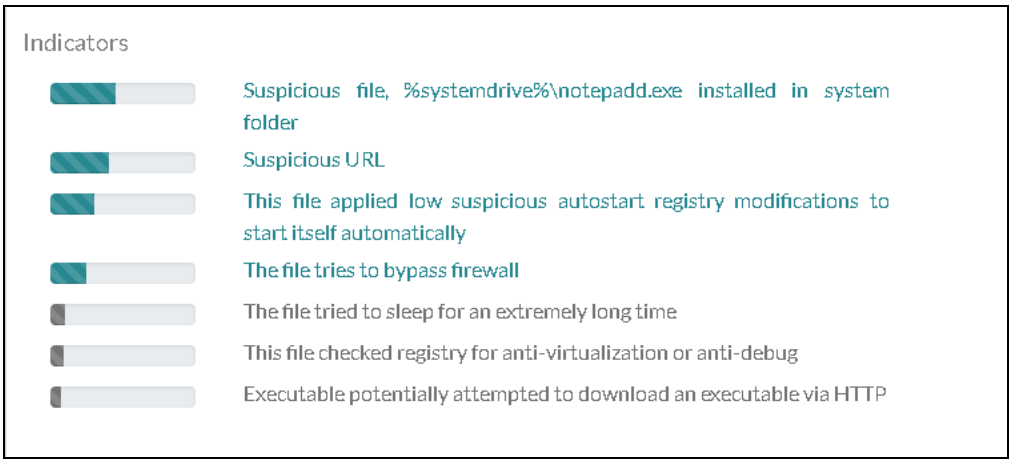
5. Review the information in the report, and then answer the following question:
Why might you want to use more than one VM to analyze a file?

Some viruses may affect some OSs, and not others.

6. Review the information in the **Indicators** section.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



The indicators are color-coded based on their severity, which is specified by the rating engine.

Analyze the Created and Injected Process

You will analyze the created and injected process from the tree view.

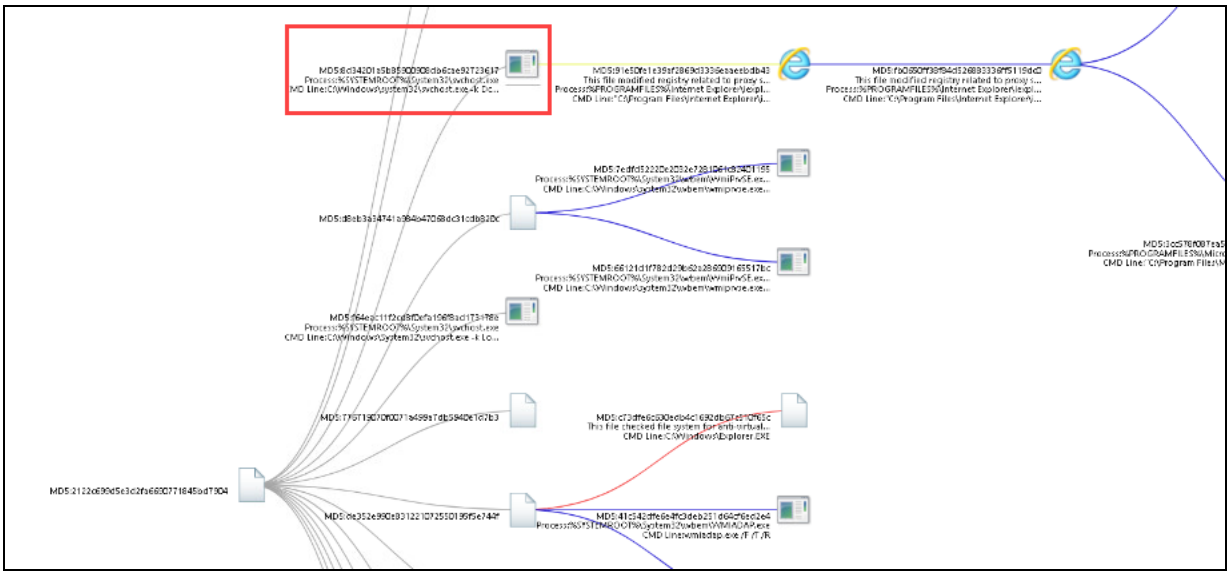
To analyze the process

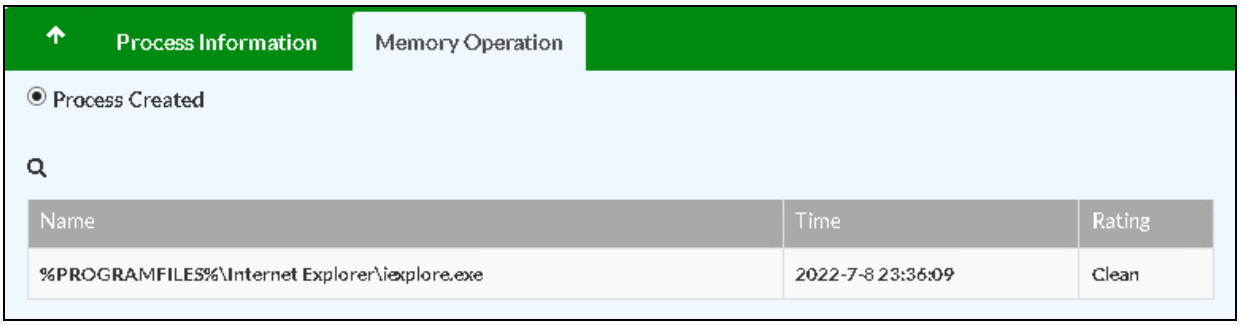
1. Click **Tree View**.

2. Click the first indicator process before the first **IE**is generated, and then review the **Memory Operation** tab.

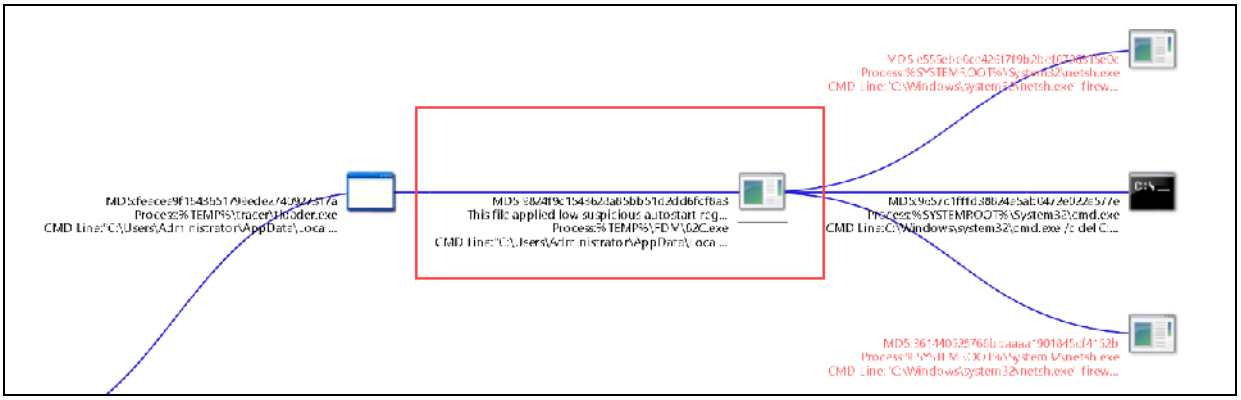
Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com





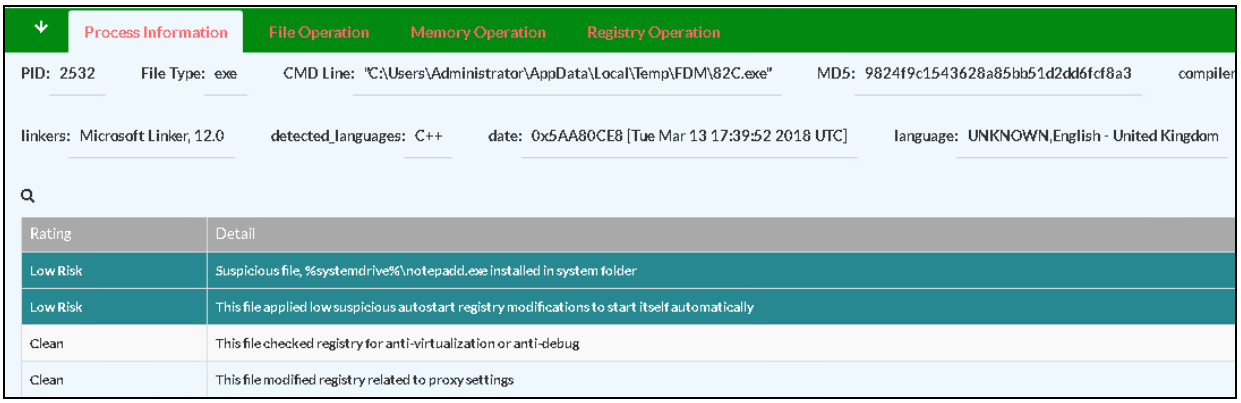
3. Click the last process that was created and injected.



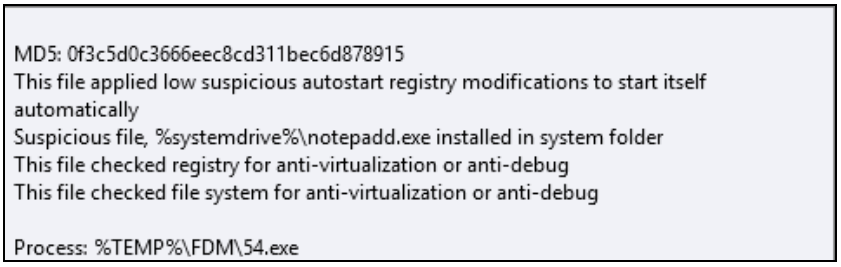
4. Review the **Process Information** tab.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



5. Hover your mouse cursor over the process to review more details.

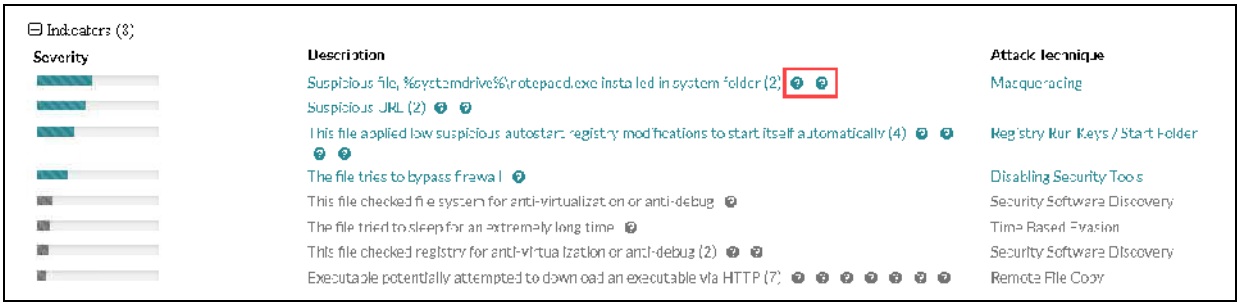


The suspicious file, `notepadd.exe`, was installed in the system folder. The file also modified the autostart registry to start itself automatically.

The sample displayed antivirtualization or antidebug behavior. This typically indicates that the malware is built to evade sandboxing.

6. Click **Details**.

7. Review the indicators.



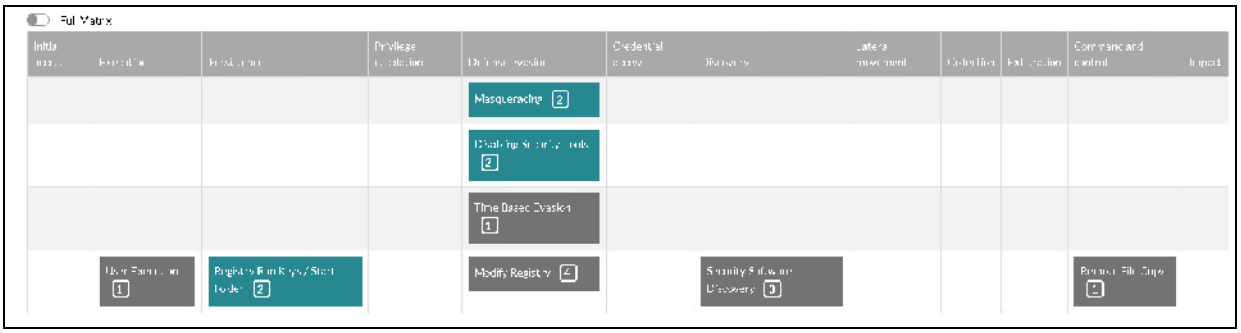
Click the **?** icon beside any of the indicators—this takes you to the appropriate operation.

What you observed in the tree view is displayed on the indicators as a summary.

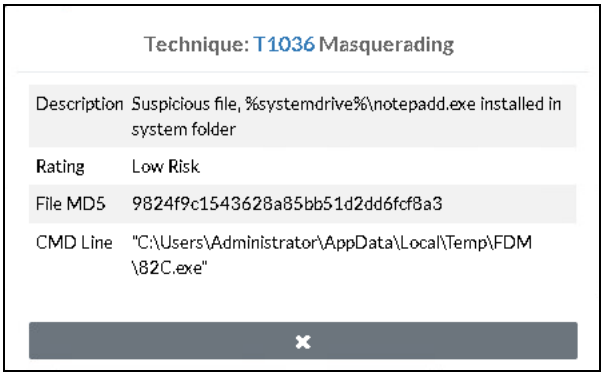
8. Expand the **MITRE ATT&CK MATRIX**.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

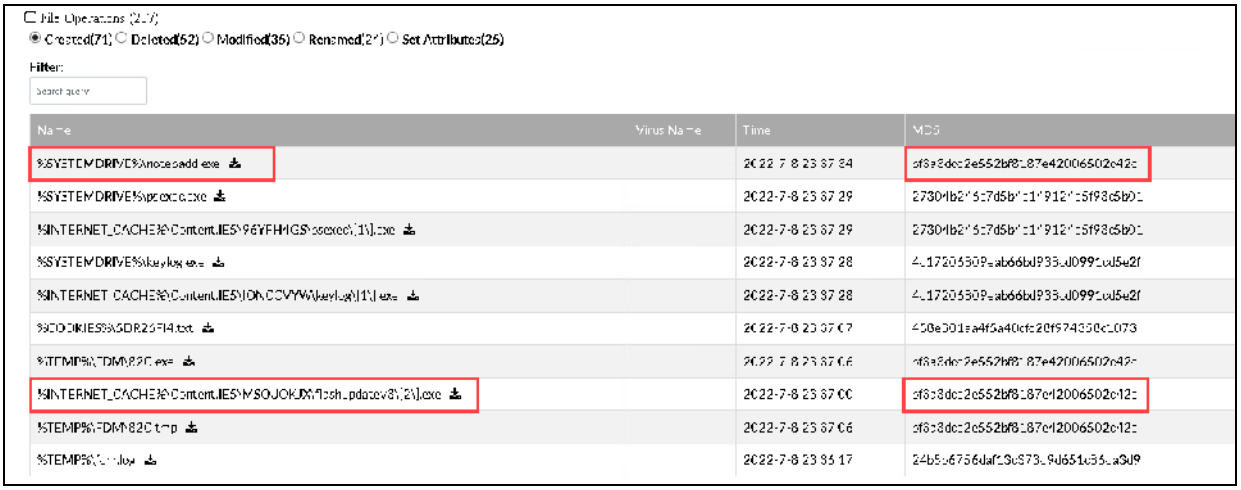


9. Click **2** beside **Masquerading** and then click the first **!**.



This shows the description, rating, and MD5 hashing algorithm of the attack technique.

10. Click **X** to close the **Masquerading** table details.
11. Expand the **File Operation** section of the report.
12. Verify that the process created a file named `notepadd.exe`.



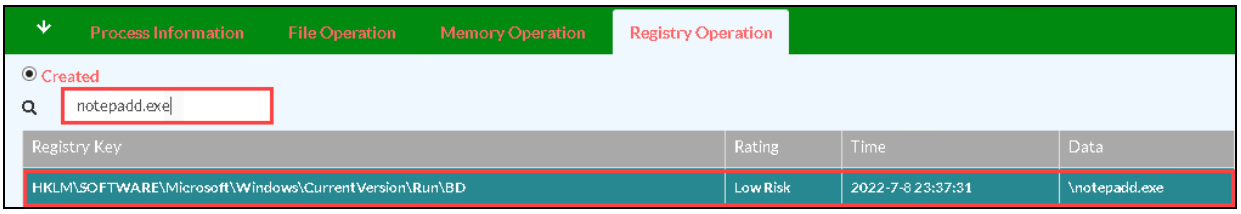
13. Review the information in the **Files Operation** section, and then answer the following question:
Are `notepadd.exe` and `flashupdatev3.exe` the same file? (**Hint**: Take a look at the MD5 checksums.)

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

The original URL pointed to a `flashupdatev3.exe` file, however, after the file ran, it wrote itself in the system32 directory under a different name.

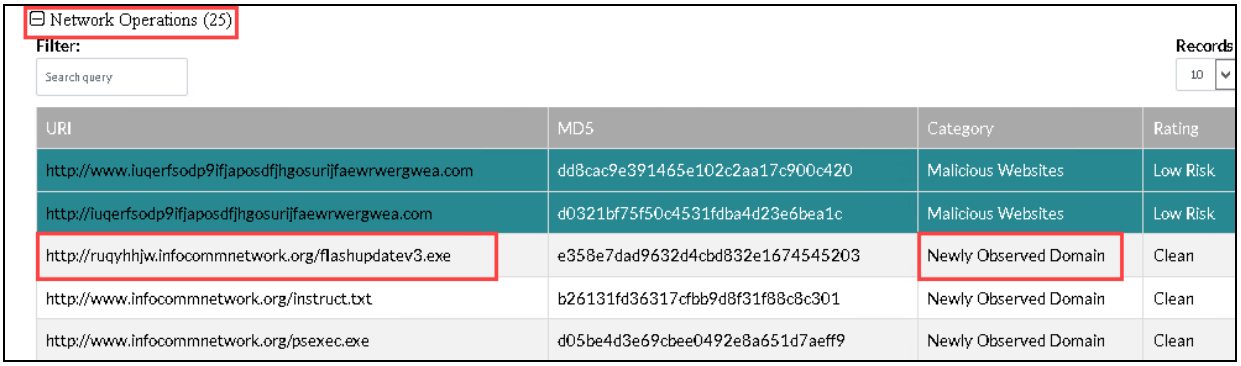
14. Return to the **Tree View** tab of the report, and click the last process that was created and injected.
15. Click **Registry Operation**.
16. Click the search icon (🔍), and then type `notepadd.exe`.



17. Review the registry changes, and then answer the following question:
    Will the `flashupdatev3.exe` executable run each time the system is rebooted?

The `HKLM\software\microsoft\windows\currentversion\run` registry is used to register programs that run each time the computer is started. This is one of many registry keys that can be used by malware to make itself persistent when the host is booted.

18. Return to the **Details** section of the report, and expand **Network Operations**.
    The **URI** column displays a list of the visited URIs.

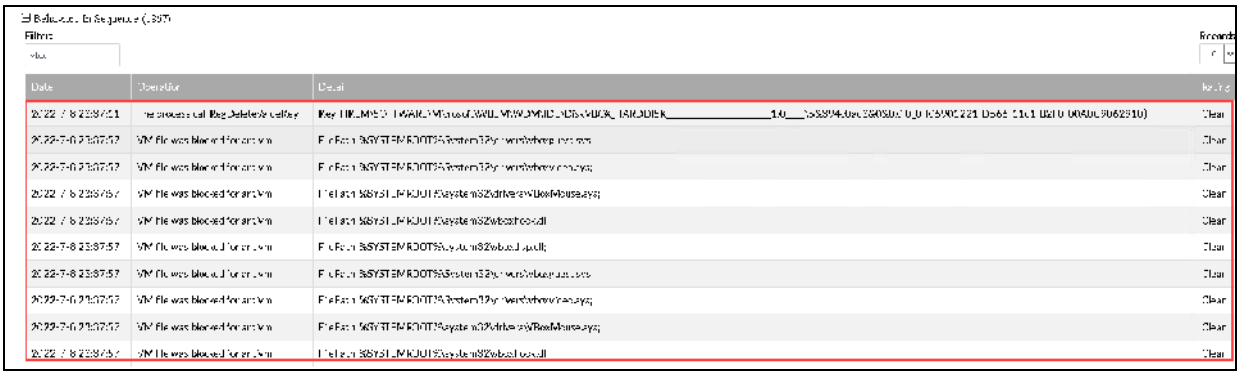


All files were downloaded from the same site. Because none of the URL callbacks made by the `flashupdatev3.exe` file are known malicious sites, the FortiGuard Web Filter does not block access to them.

19. Expand **Behaviors in Sequence**.
20. In the **Filter** field, type `vbox`.
21. Review the search results.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com



You can see some of the checks that the sample performed. It was searching for some common dynamic-link libraries (DLL) and drivers used by the virtual infrastructure providers. FortiSandbox intercepted those requests, so the sample cannot detect that it is running in a sandbox based on the existence of these files.

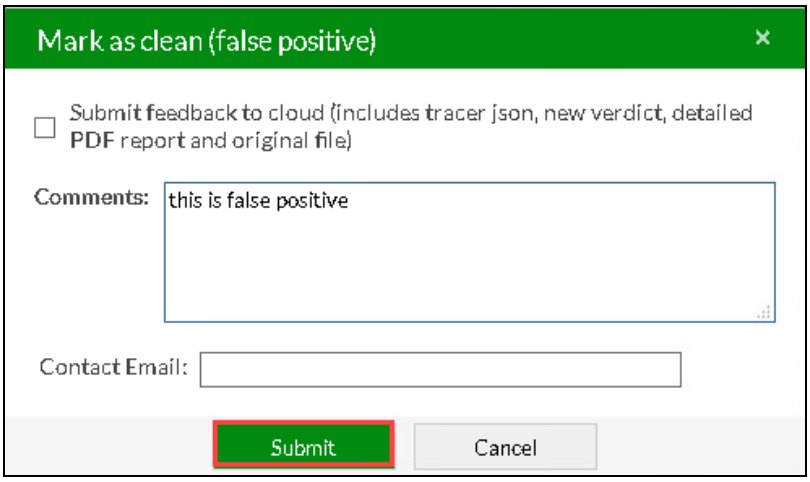
After reviewing the scan job report in depth, do you agree that this is a high-risk sample?

Override a Verdict

You will use the scan job report to override a FortiSandbox verdict. You will verify the override by viewing the overridden verdicts list and the URL package version.

To override a verdict

1. In the upper-right corner of the report, click **Mark as clean (false positive)**.
   The **Mark as clean (false positive)** window opens.
2. In the **Comments** field, type the reason that you think the verdict is not correct.

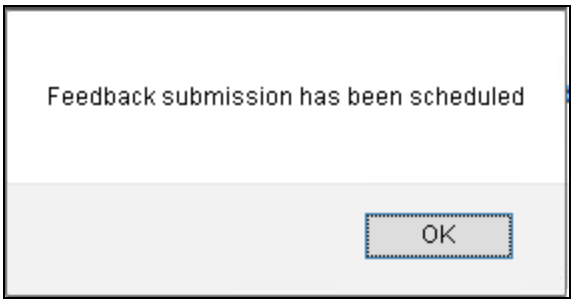


Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET
Brave-Dumps.com

You also have the option to send the feedback to the FortiSandbox Cloud Community. If the sample is found to be clean, any other FortiSandbox scanning the same sample will get a clean rating from the Cloud Community.

3. Click **Apply**.
   A confirmation window opens.



4. Click **OK**.
5. Close the scan job report browser tab.
   If the same URL is submitted to FortiSandbox again, at what stage will FortiSandbox stop analyzing it?
   a. File-filter stage
   b. Cache check stage
   c. Static analysis scan stage
   d. VM scan stage

FortiSandbox will apply the overridden verdict at the cache check stage.

5. Log out of the FortiSandbox GUI.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com

DO NOT REPRINT
© FORTINET

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 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.

Fortinet Vouchers & Dumps are Available on Brave-Dumps.com