# Firewall & Anti-Virus Exclusion Migrator: User Guide

Contents

[Firewall & Anti-Virus Exclusion Migrator: User Guide 1](#_Toc83388277)

[Introduction 2](#_Toc83388278)

[What is Firewall and Anti-Virus Exclusion Migrator (FAVE)? 2](#_Toc83388279)

[Migration tasks that Firewall and Anti-Virus Exclusion Migrator (FAVE) performs 2](#_Toc83388280)

[How does Firewall and Anti-Virus Exclusion Migrator (FAVE) work? 3](#_Toc83388281)

[Firewall Rule Migration 3](#_Toc83388282)

[Antivirus Exclusion Extraction 4](#_Toc83388283)

[Before You Start 5](#_Toc83388284)

[A. Have Appropriate User Role & Privileges 5](#_Toc83388285)

[B. Export McAfee or Symantec Endpoint Protection policies 5](#_Toc83388286)

[C. Install FAVE 5](#_Toc83388287)

[Start Migration 8](#_Toc83388288)

[Part A: Firewall Migration 8](#_Toc83388289)

[Part B: Antivirus Exclusion 8](#_Toc83388290)

[Step 1: Log into your account 9](#_Toc83388291)

[Step 2: Select your Firewall Rules file 10](#_Toc83388292)

[Part A: Firewall Exclusion 12](#_Toc83388293)

[Step 3: Update Configurations 12](#_Toc83388294)

[Step 4: Review & Import 16](#_Toc83388295)

[Post Migration: Firewall Rules 19](#_Toc83388296)

[Part B: Antivirus Exclusions 22](#_Toc83388297)

[Step 3: Update Configurations 22](#_Toc83388298)

[Step 4: Review & Import 24](#_Toc83388299)

[Post Migration: Antivirus Exclusions 26](#_Toc83388300)

## Introduction

Welcome to the User Guide for Firewall and Anti-Virus Exclusion (FAVE) Migrator. Here you will find all details about the Firewall and Anti-Virus Exclusion Migrator tool along with step-by-step instructions on using Firewall and Anti-Virus Exclusion Migrator to migrate your policies to Microsoft’s Defender Platform.

### What is Firewall and Anti-Virus Exclusion Migrator (FAVE)?

The Firewall and Anti-Virus Exclusion Migrator tool is a Windows based desktop application that will migrate your Firewall rules and anti-virus exclusions from other Endpoint Protection platforms (EPP) to our Defender platform.

Our tool takes you through a simple three-step migration process. It accepts McAfee as well as Symantec Endpoint Protection (SEP) XML exports, performs mapping, and creates:

* Equivalent firewall rules through PowerShell scripts.
* List of anti-virus exclusions.

Once the rules are migrated using Firewall and Anti-Virus Exclusion Migrator to the requisite machine, they can be deployed organization-wide through Intune easily.

### Migration tasks that Firewall and Anti-Virus Exclusion Migrator (FAVE) performs

Firewall and Anti-Virus Exclusion Migrator takes over many of the difficult or tedious tasks involved in a DLP migration project:

* In a traditional migration scenario, you need to perform feasibility analysis between source & target EPP platforms, map features, migrate rules manually, and test and tweak rules. Your migrated rules can be up and running within minutes with Firewall and Anti-Virus Exclusion Migrator.
* With FAVE, you can scale up your migration project quickly from moving a single firewall rule or antivirus exclusion manually to multiple rules at the same time.
* FAVE automatically identifies firewall rules in source policies and creates firewall rules on your local machine in a few clicks.
* FAVE detects which antivirus exclusions are currently defined in source policies and automatically creates a list of all exclusions.
* FAVE provides you with a detailed migration report with rule-level migration status.
* FAVE supports firewall rule migration as well as antivirus exclusion extraction from McAfee Symantec Data Loss Prevention 15.7 or earlier.

## How does Firewall and Anti-Virus Exclusion Migrator (FAVE) work?

### Firewall Rule Migration

The following diagram illustrates the FAVE firewall migration process.

Graphical user interface, application

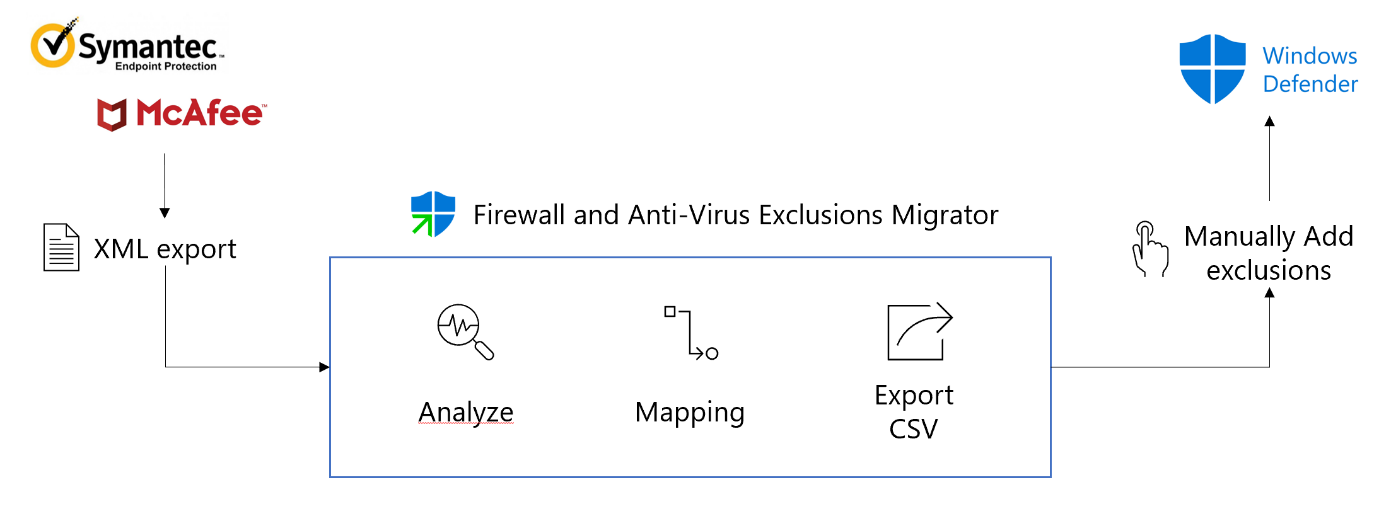
Description automatically generated

During a given instance of migration, Firewall and Anti-Virus Exclusion Migrator works in five phases:

1. Input  
   *FAVE ingests a McAfee or Symantec Endpoint Protection (SEP) firewall rule policy XML file.*
2. Analyze   
   *FAVE interprets the input file & identifies firewall rule policy constructs.*
3. Rationalize  
   *FAVE maps the identified firewall rule policy constructs to Windows Defender firewall capabilities. It performs validations for Windows Defender platform limitations.*
4. Migrate  
   *FAVE prepares & executes PowerShell scripts for the firewall rules identified & supported by the Windows Defender platform.*
5. Reporting  
   *FAVE provides the user with a detailed HTML migration report about which firewall rules were migrated successfully or not.*

### Antivirus Exclusion Extraction

The following diagram illustrates the FAVE antivirus exclusion extraction process.



During a given instance of antivirus exclusion extraction, FAVE works in five phases:

1. Input  
   *FAVE ingests a McAfee or Symantec Endpoint Protection (SEP) antivirus exclusion XML file.*
2. Analyze   
   *FAVE interprets the input file & identifies antivirus exclusion policy constructs.*
3. Rationalize  
   *FAVE maps the identified antivirus exclusion policy constructs to appropriate format. It performs validations for valid antivirus exclusion definition.*
4. Export  
   *FAVE prepares & exports a list of antivirus exclusions.*

## Before You Start

Before you use FAVE for the first time, complete the following pre-requisite tasks:

1. Verify your role & privileges
2. Export policy XMLs from McAfee or Symantec Endpoint Protection
3. Install FAVE

### Have Appropriate User Role & Privileges

You need to have *Local* *Administrator* privileges on the machine you are running FAVE to be able to import firewall rules on the local machine.

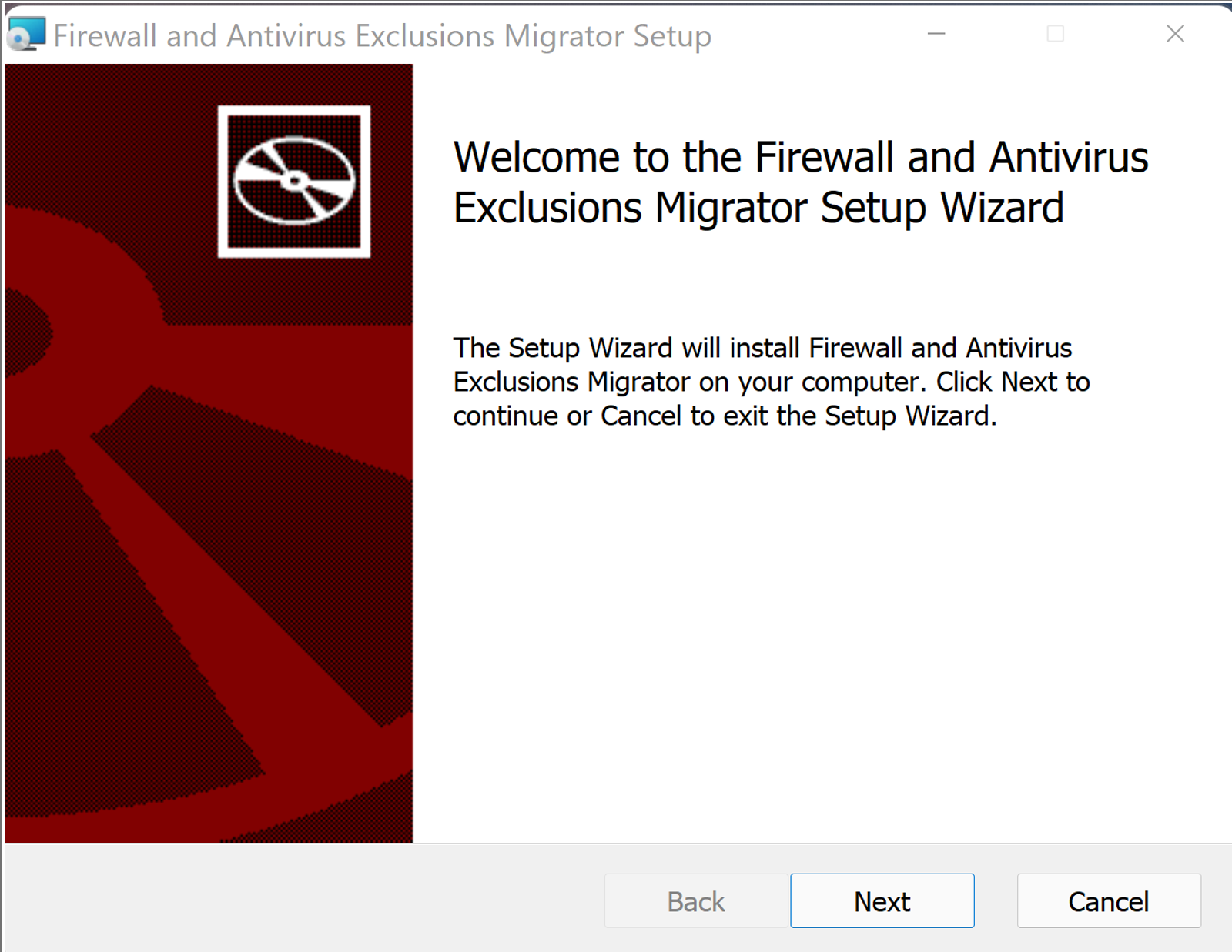
### Export McAfee or Symantec Endpoint Protection policies

Also, before you begin the migration process with FAVE, you will also need XML exports of your existing policies either from McAfee or Symantec Endpoint Protection platforms.

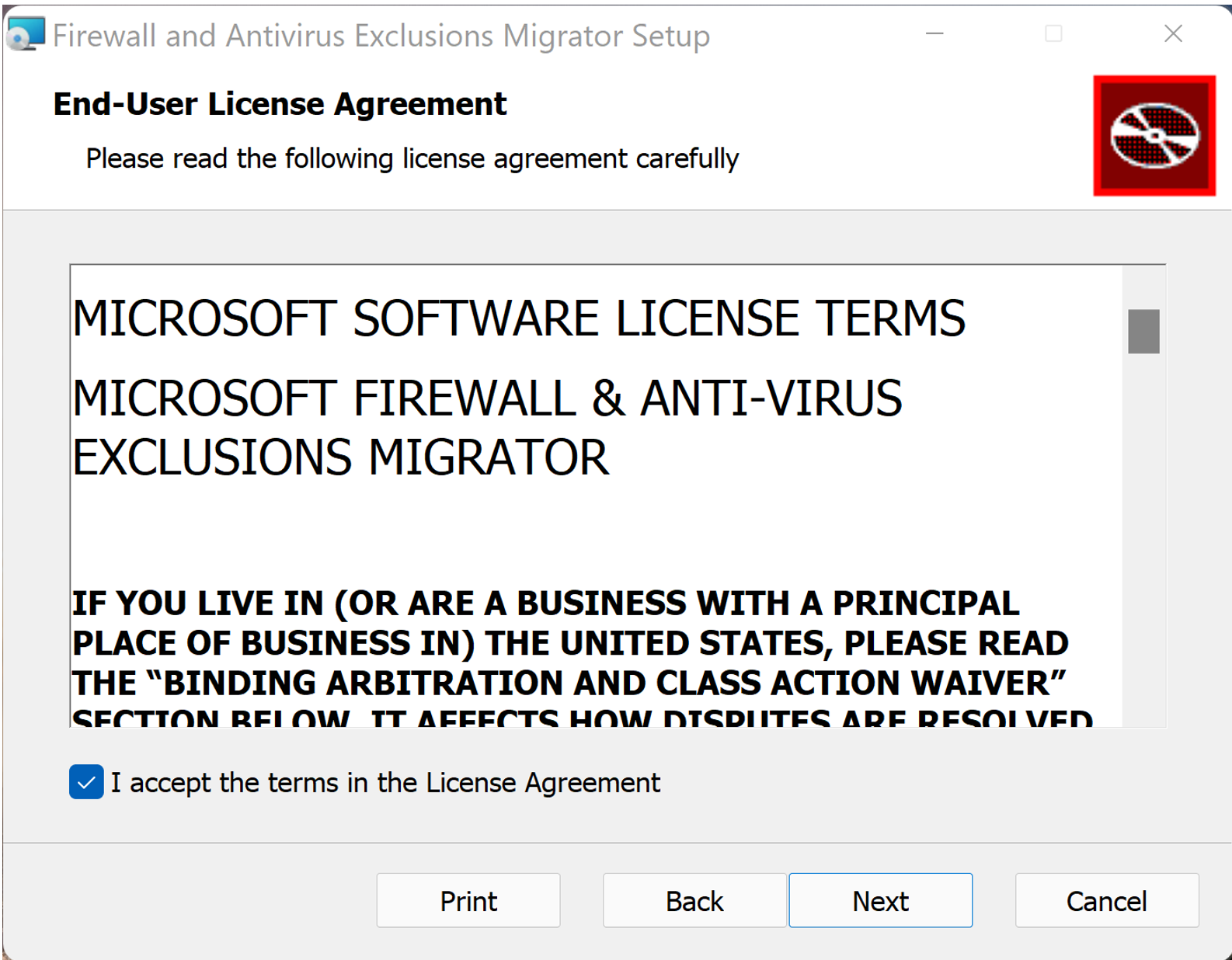
### Install FAVE

We strongly recommend that you install FAVE on a *non-production* reference Windows 10 virtual machine. Please follow the steps given to install Firewall and Antivirus Exclusions Migrator (FAVE).

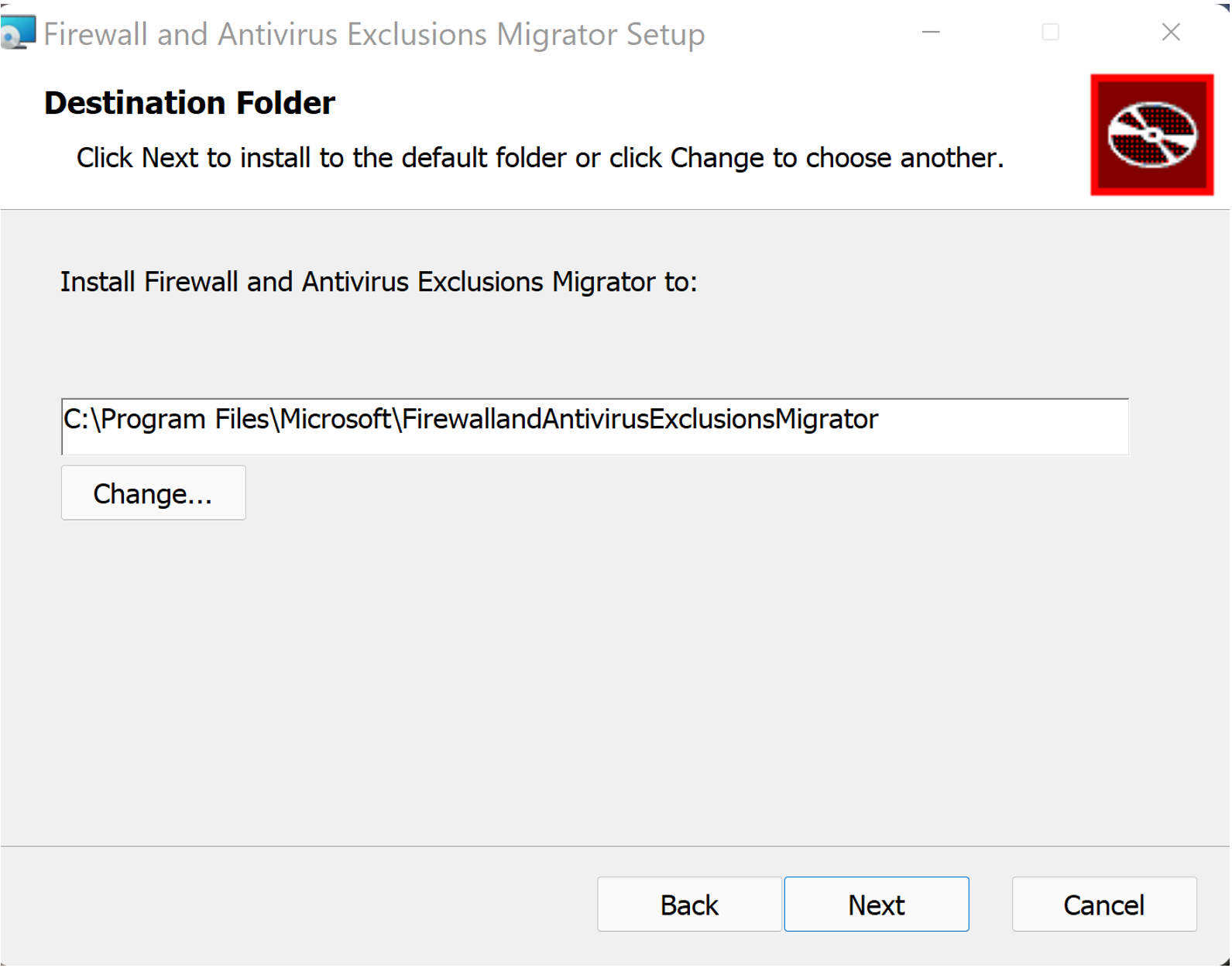
1. Download and launch **FAVESetup.msi** file.
2. The following dialog box will open. Click ‘Next’.



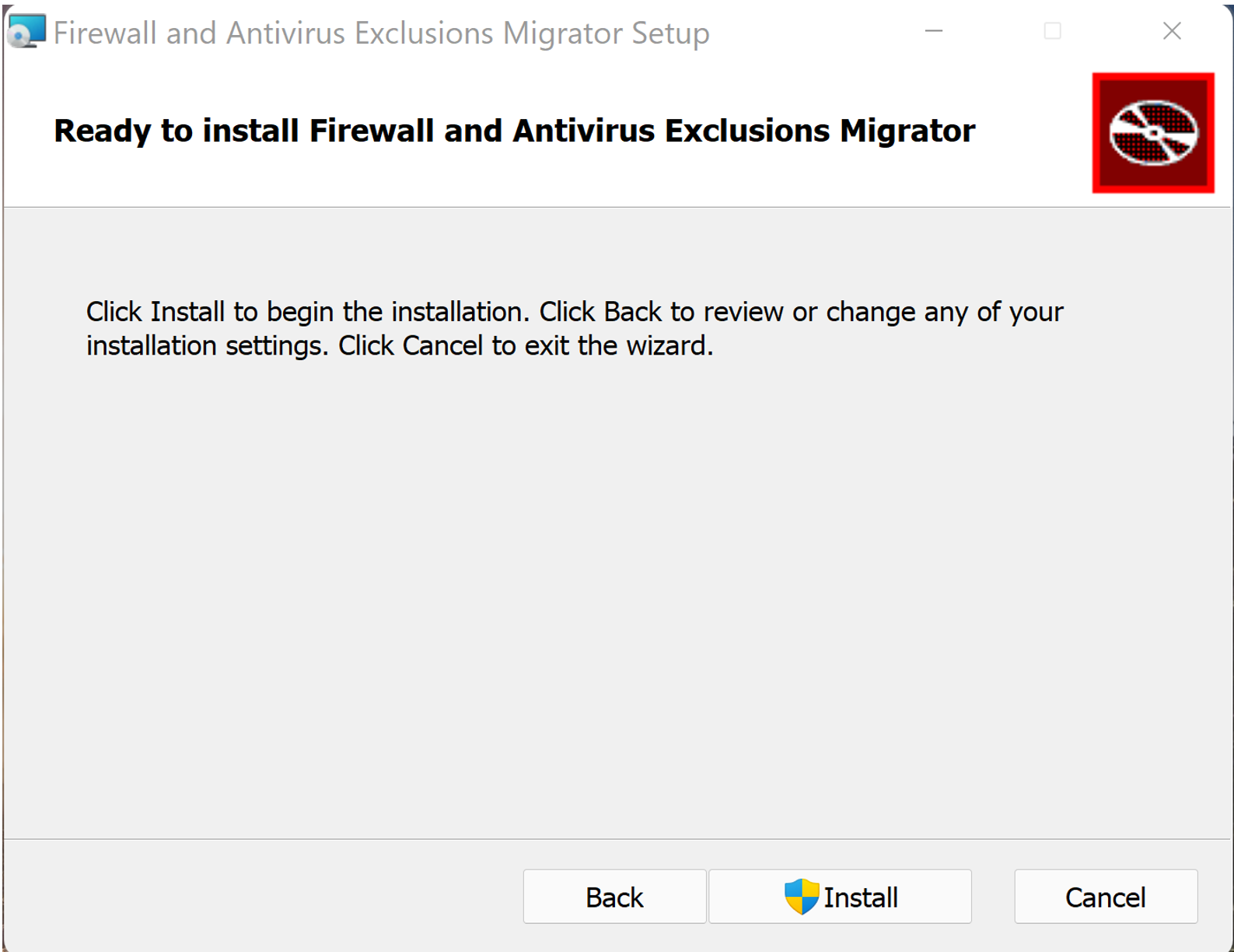
1. Read and agree to the End-User License Agreement (EULA) to proceed further.



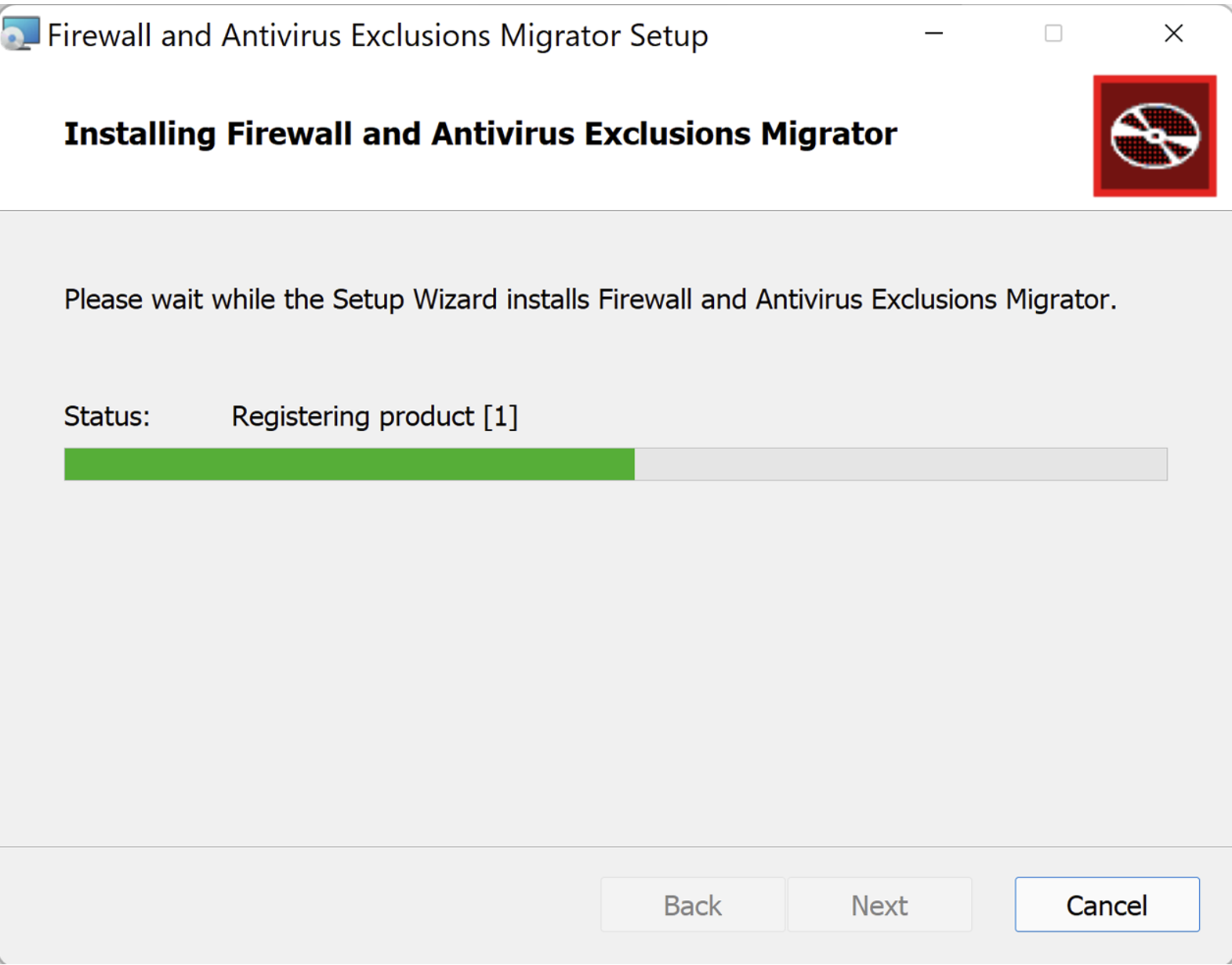
1. Please select the location where you want to install FAVE and click ‘Next’.



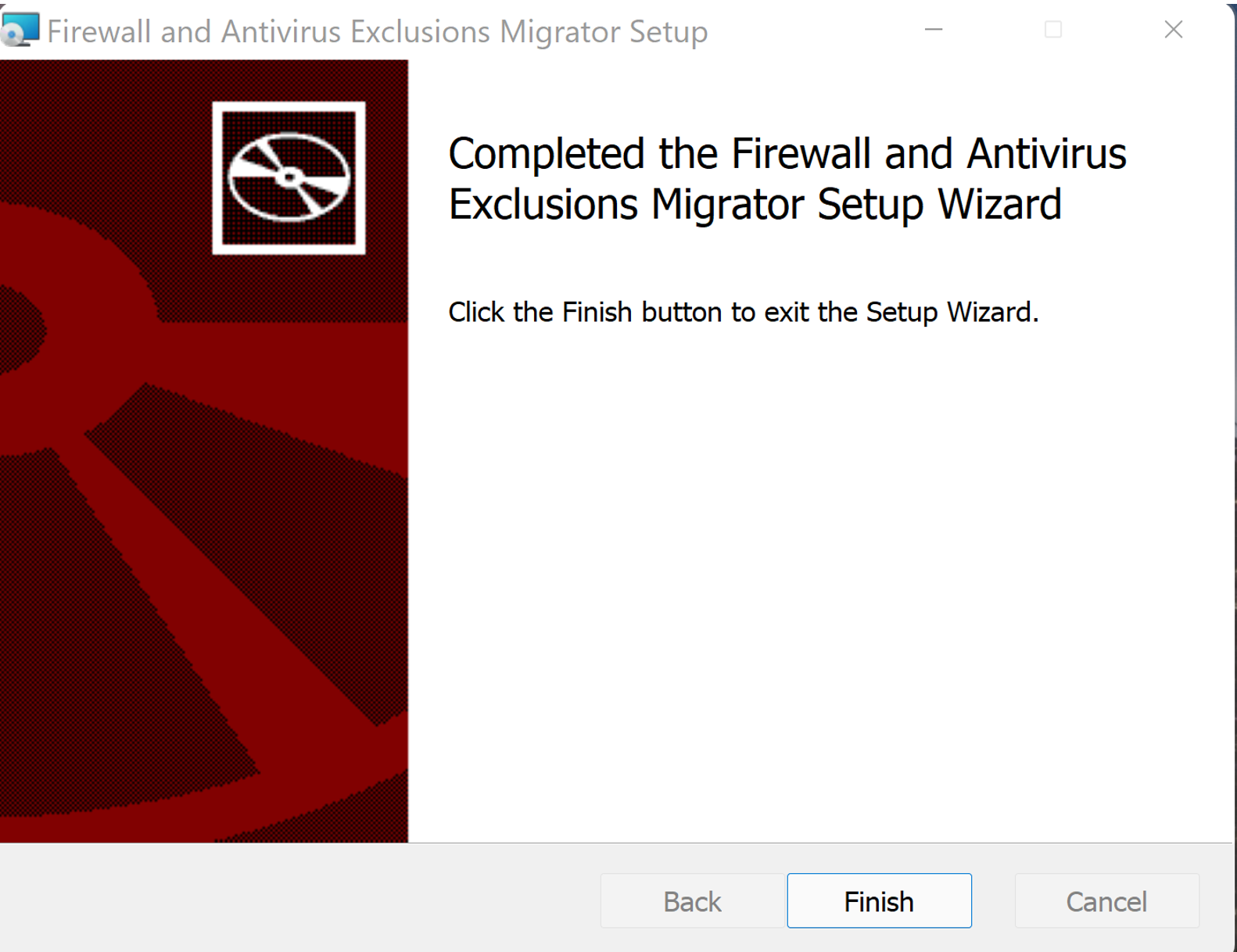
1. Click on ‘Install’ to begin installation.



1. Please wait while FAVE is being installed and then click ‘Next’.



1. Once FAVE is installed, you can click on Finish which will close the dialog box.



## Start Migration

To initiate migration, you do the following:

* Complete the steps in the [Before You Start](#_Before_You_Start) section.
* You input XML files of your policies exported from McAfee or Symantec Endpoint Protection.
* You make selections and/or tweaks to your rules as required.
* You create new rules on your local machine equivalent to your input policy.

Thereafter, you test your rules, make any further changes required & deploy it to your entire organization.

You can follow the following steps to perform migration:

* Step 1: Log into your account
* Step 2: Select your Firewall Rules file

### Part A: Firewall Migration

* Step 3: Update Configurations
* Step 4: Review & Import
* Post Migration: Firewall Rules

### Part B: Antivirus Exclusion

* Step 3: Update Configurations
* Step 4: Review & Import
* Post Migration: Antivirus Exclusion

### Step 1: Log into your account

After you have installed & launched FAVE, the first thing that you need to do is to login.

1. You will be greeted with a Welcome screen. Here, you can then click the Get Started button to start.

Graphical user interface, application

Description automatically generated

### Step 2: Select your Firewall Rules file

Next, you need to select your source platform (McAfee or Symantec) and Firewall DLP policy export which will act as an input for FAVE. The files you select will be the ones that will be migrated to the Windows Defender Firewall platform.

1. First, you need to select the source platform from which you want to migrate your firewall rules. You can choose between McAfee & Symantec from the drop-down menu.

Graphical user interface, text, application

Description automatically generated

1. Next, you need to click on ‘Browse files’ button.
2. Please select the required policy files in the File Explorer pop-up window and click ‘Open’.   
   1. You can select only one XML file to migrate at a time.
   2. Ensure that the XML files you upload are from the Source Platform selected and no other kind of XML. In such a scenario, the migration process will fail, and you will have to restart it from Step 1.

Graphical user interface, text, application

Description automatically generated

1. The tool will show the filename of your selected input policy file.
   1. If you wish to deselect a previously selected policy file, you can click the ‘Browse Files’ button again.

Graphical user interface, application

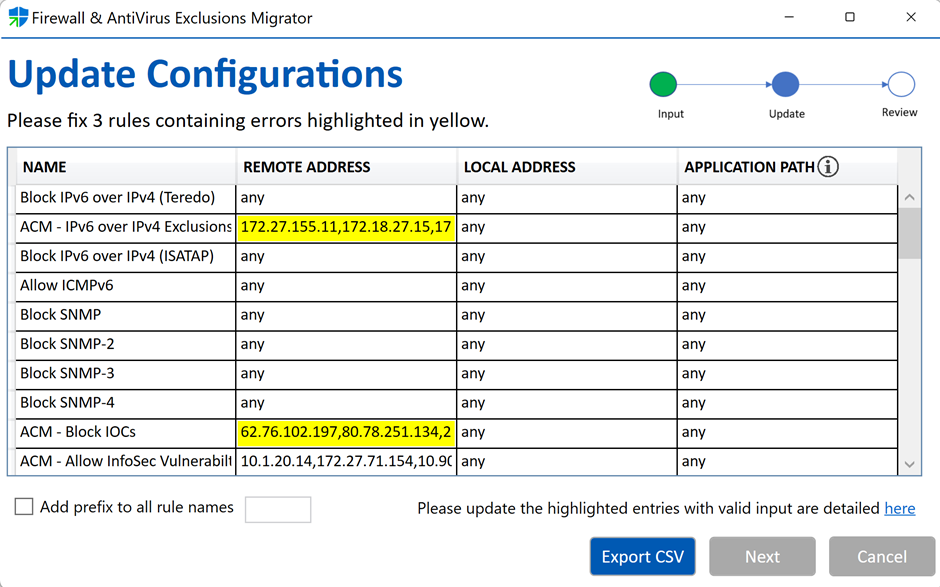
Description automatically generated

1. Once you have completed selection of the policy file you wish to migrate, you can click ‘Next’ and move to the next step.

## Part A: Firewall Migration

### Step 3: Update Configurations

Once you input the policy you want to migrate, FAVE will process those files to identify what kind of firewall rules you are trying to create.

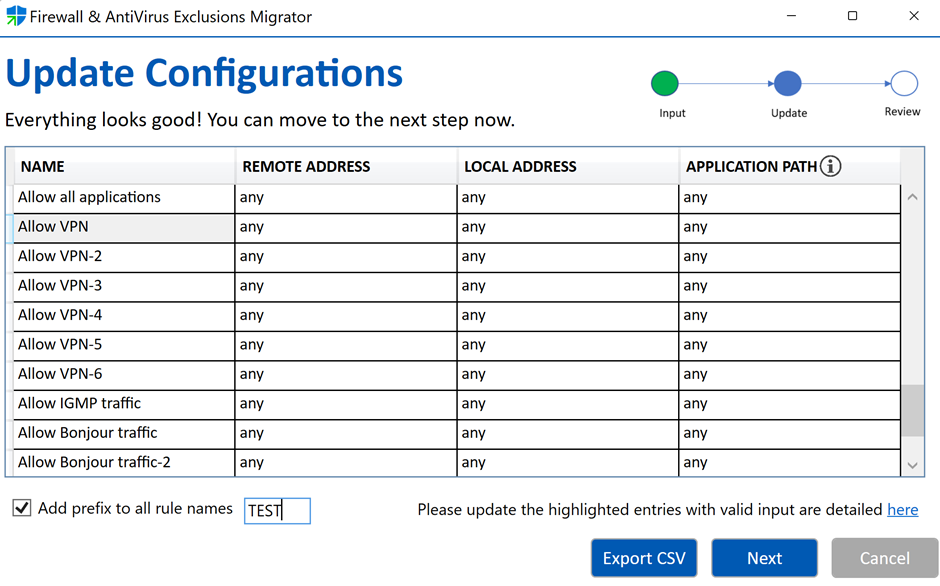


1. You will be able to see a list of all the firewall rules from the file you selected.

These lists are represented as a table with four columns:

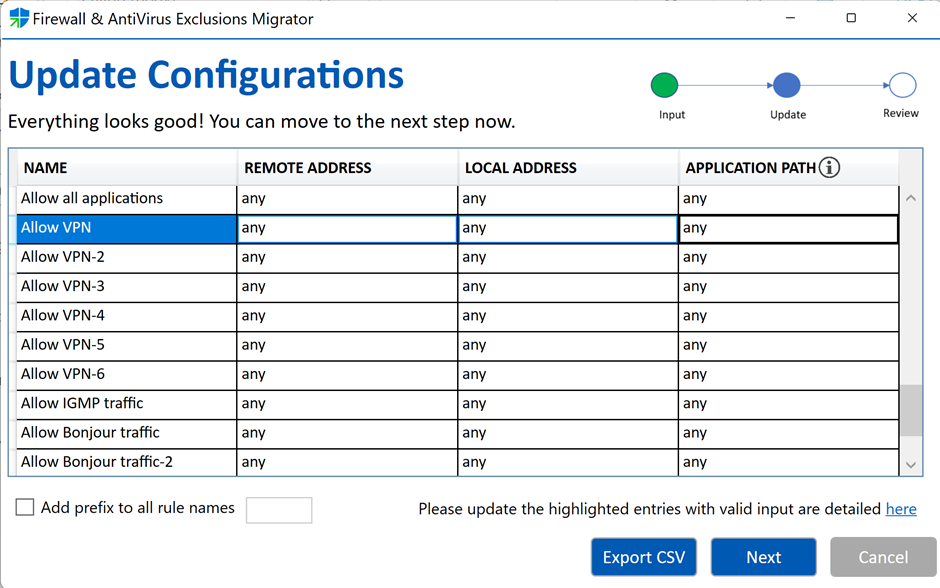
* Name: Specifies that only matching firewall rules of the indicated display name are created.
* Remote Address: Specifies that network packets with matching IP addresses match this rule. This parameter value is an IPv4 or IPv6 address, subnet, range, or keyword.
* Local Address: Specifies that network packets with matching IP addresses match this rule. This parameter value is the first end point of an IPsec rule and specifies the computers that are subject to the requirements of this rule. This parameter value is an IPv4 or IPv6 address, hostname, subnet, range, or the following keyword: Any.
* Application Path: Specifies the path and file name of the program for which the rule allows traffic. This is specified as the full path to an application file.

1. You may have some rules which will be highlighted in yellow. These are rules where you need to fix one of the above four values to an acceptable format.
   1. The count of number of rules that need to be fixed will be displayed above the table.
2. You can also click the ‘Export CSV’ button to export a CSV file with all the rules.
3. You can manually change any of the cell values if you wish by double-clicking on the corresponding cell.
   1. These details can be edited later using Windows Defender Firewall application after the policy is migrated.
   2. You can also choose to add an optional prefix at the beginning of all rule names by clicking on the ‘Add prefix to all rule names’ checkbox.



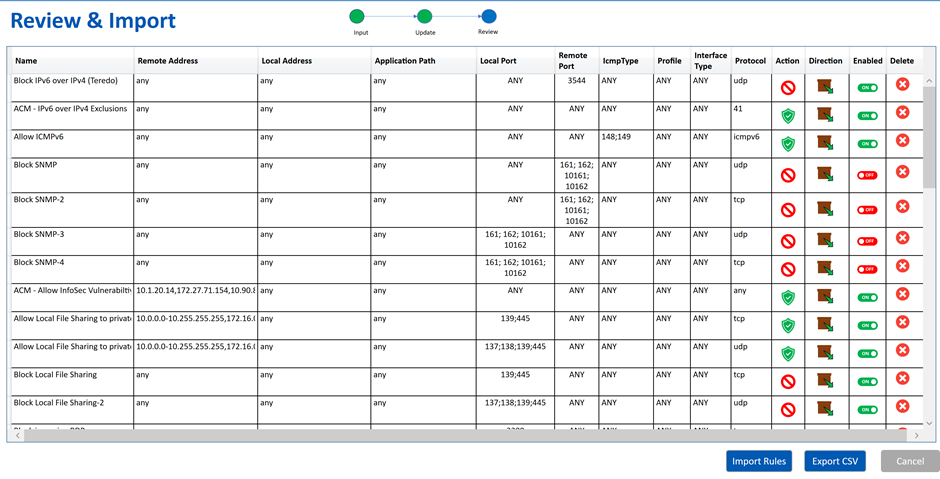
**Recommendation:** We highly recommend you spend a little extra time to review all the highlighted as well as non-highlighted rules and edit them as required. Learn more about [creating new firewall rule and acceptable formats](https://docs.microsoft.com/en-us/powershell/module/netsecurity/new-netfirewallrule?view=windowsserver2019-ps&viewFallbackFrom=win10-ps).

1. After you have reviewed and fixed all the rules following the above steps, you can click ‘Next’ and move to next step.

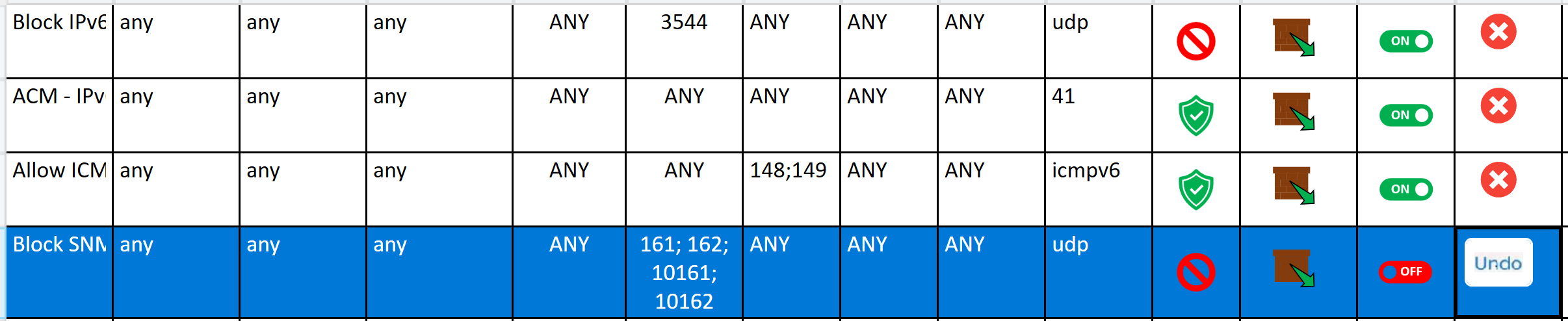


### Step 4: Review & Import

Finally, after you completed all the previous steps, your Firewall Rules are ready to be imported to Windows Defender Firewall.



1. You can have a look at all the rules and all additional parameters for each of them before migration.
   1. Each rule has a ‘Delete’ button which you can use to not migrate that rule.
   2. In case you accidentally click the ‘Delete’ button, you can use the ‘Undo’ option.



1. You can now click the ‘Import Rules’ button to migrate rules to Windows Defender Firewall or hit the ‘Export CSV’ button to export a CSV file with all the rules.

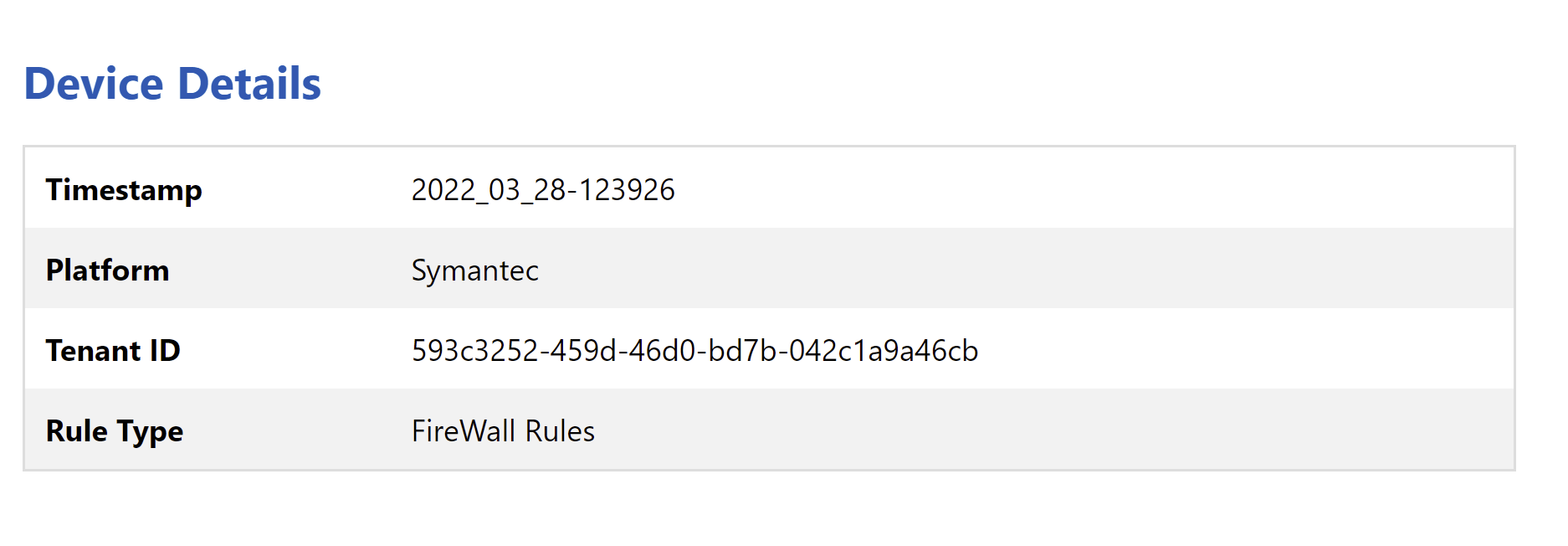
#### Import Rules

When you click ‘Import Rules’ button, a PowerShell window will open. PowerShell scripts will be executed to create the firewall rules in Windows Defender Firewall.

After the scripts complete executing, an HTML report is generated.



* Device Details: General information about your tenant, source platform, type of rules and timestamp.



* Migration Summary: Overview of the entire migration process.



* Success Report: List of all the rules that were migrated successfully.
* Failure Report: List of all rules that were not migrated successfully.
* Rules Deleted: List of all rules that were not part of final selection and were not migrated.

A picture containing text, screenshot, indoor

Description automatically generated

#### Export CSV

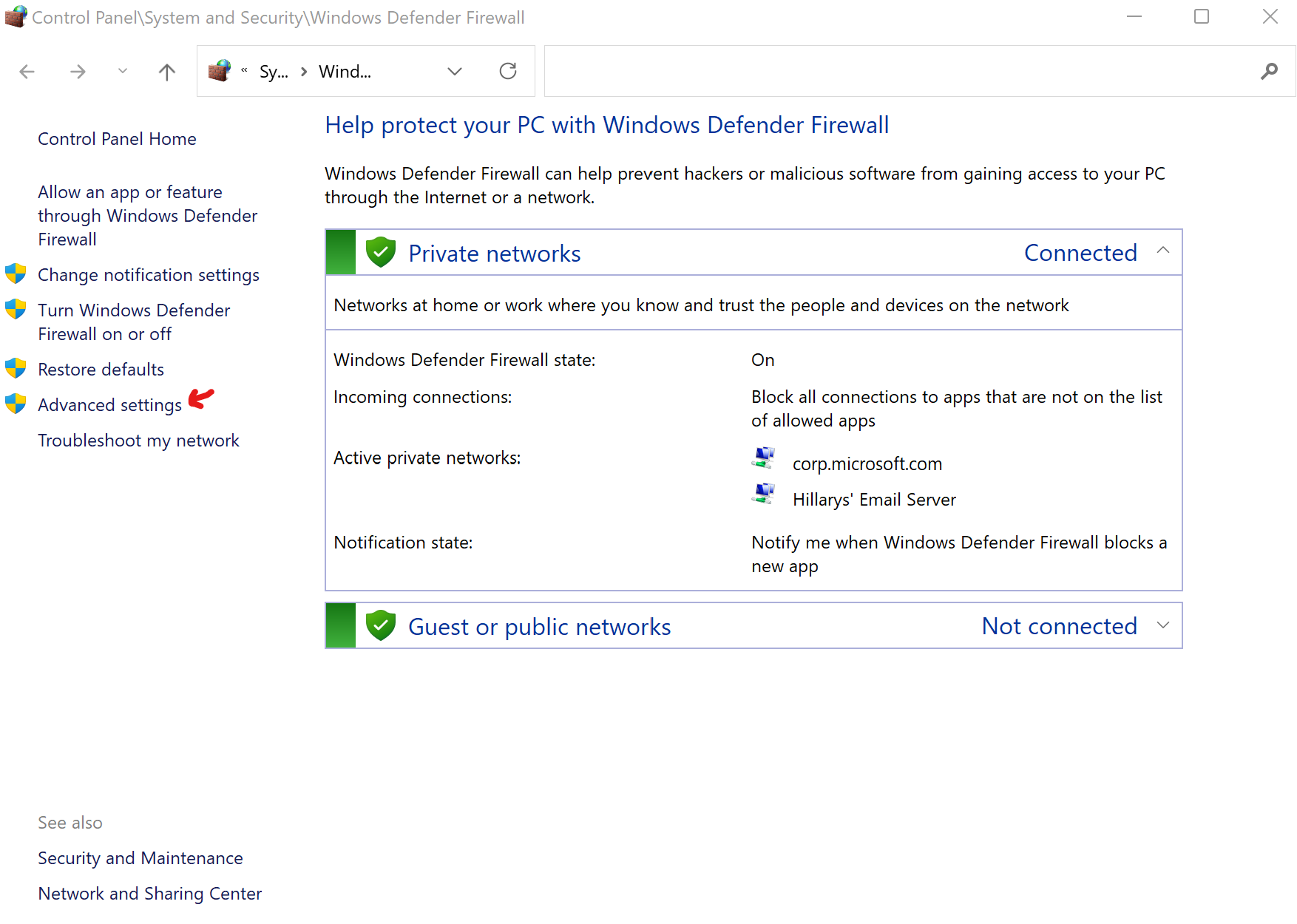
With the ‘Export CSV’ option, you can export all your rules in a CSV file locally for your reference or bulk edit them as required.

A picture containing text, electronics, computer, screenshot

Description automatically generated

### Post Migration: Firewall Rules

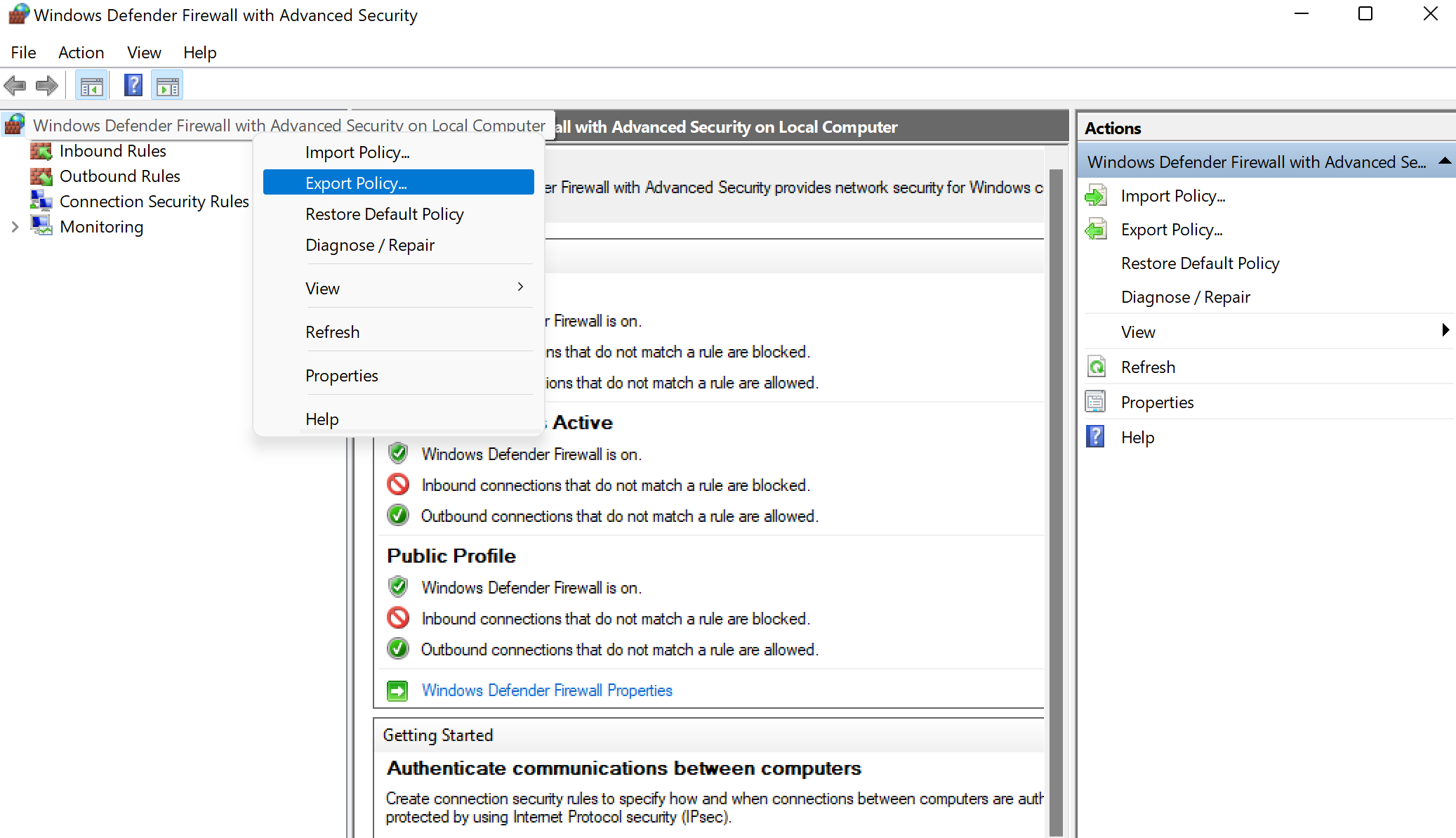
Once FAVE has imported all the firewall rules into Windows, you can open the firewall control panel applet (firewall.cpl) and click Advanced Settings to view the rules.



Review your imported rules in the inbound and outbound sections and make any changes you may need. This is where it is helpful to use the rule name prefix for the display name of the firewall rule as it helps you easily identify the imported rules.

#### Migrate Firewall rules to GPO

In the Advanced settings left pane right click on “***Windows Defender Firewall with Advanced Security***” and click “***Export Policy***”



Save the export as a \*.wfw file. You can now create a domain-based group policy object and import the firewall rules into it for testing and deployment.

1. Open the Group Policy Management Editor (GPMC) with an active directory account that has permission to create and edit domain-based GPOs
2. Create and edit a new group policy object
3. Navigate to **Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security**
4. In the left pane of the group policy editor right click on “***Windows Defender Firewall with Advanced Security***” and click “***Import Policy...***”
5. In the browse dialog box open the \*.wfw file that you exported from the referenced machine
6. The firewall rules are then imported into the GPO
7. Go into the inbound and outbound rules section and remove any firewall rules that do not have the prepended prefix that was specified (this ensures only your custom migrated rules are in the policy)
8. Close the GPO and link it to an OU where you want to apply the Firewall rules to Windows 10 devices.

#### Migrate Firewall Rules to Intune

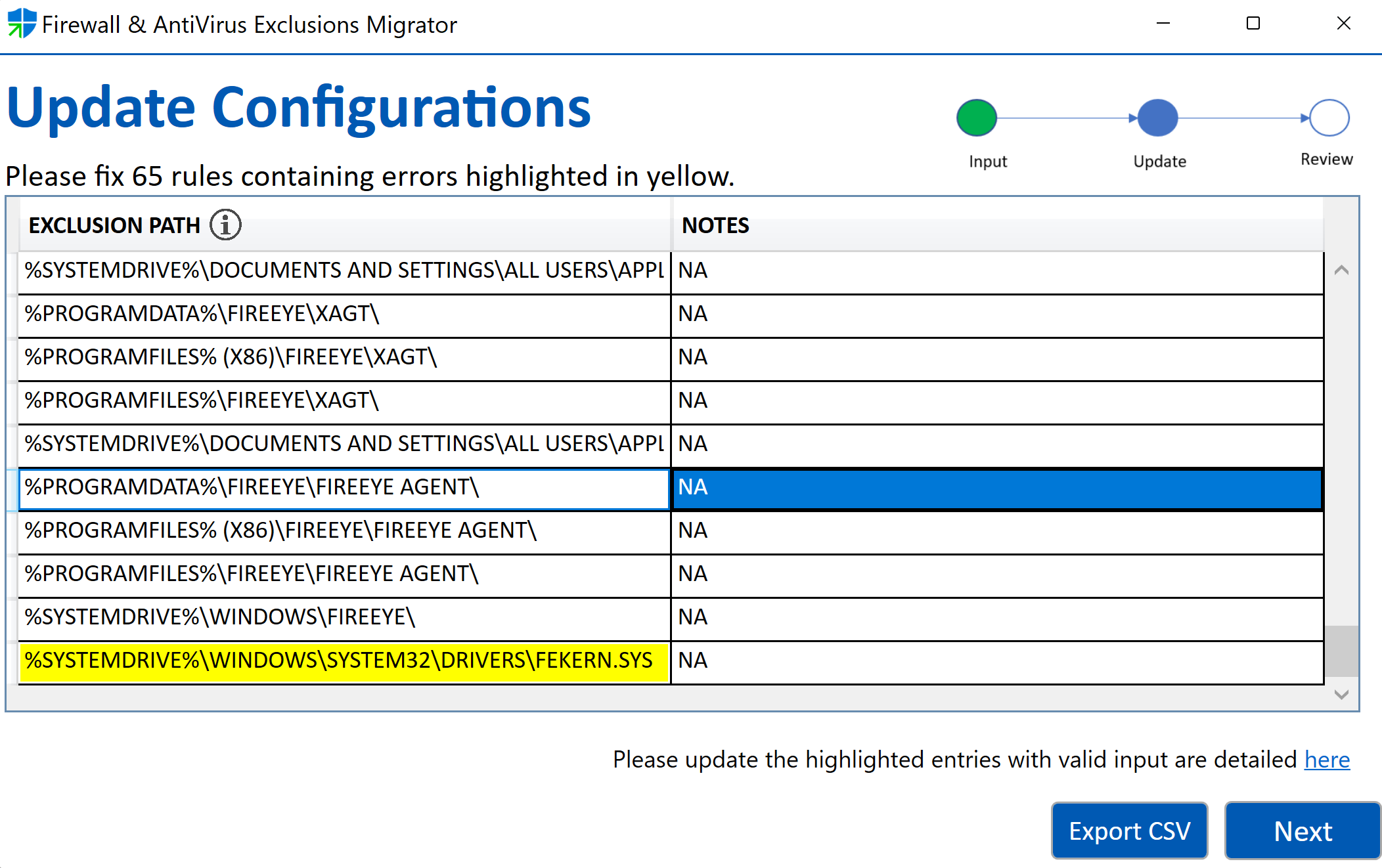
Perform the following steps to migrate your firewall rules to Endpoint Manager/Intune. You will need to perform the previous section “Migrate firewall rules to GPO” as a pre-requisite to this section, proceed with the following steps after you have completed the previous section.

1. Delete all inbound and outbound migrated FW rules from the reference VM (again they are easy to identify if you use the custom rule name prefix)
2. Deploy the migrated firewall rules to the reference machine via domain-based GPO
   1. This step is required as the Intune tool only migrates firewall rules that are applied by GPO
3. Download and run the [Endpoint Security Firewall Migration tool](https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-security-firewall-rule-tool) to import your migrated firewall rules into Endpoint Manager.

## Part B: Antivirus Exclusions

### Step 3: Update Configurations

Once you input the policy you want to migrate, FAVE will process those files to identify what kind of antivirus exclusions you are trying to create.



1. You will be able to see a list of all the antivirus exclusions from the file you selected.

These lists are represented as a table with two columns:

* Exclusion Path: Specifies the path of the folder which need to be excluded by the antivirus.
* Notes: Specifies any descriptive text found in the input xml (typically found only in McAfee xml files).

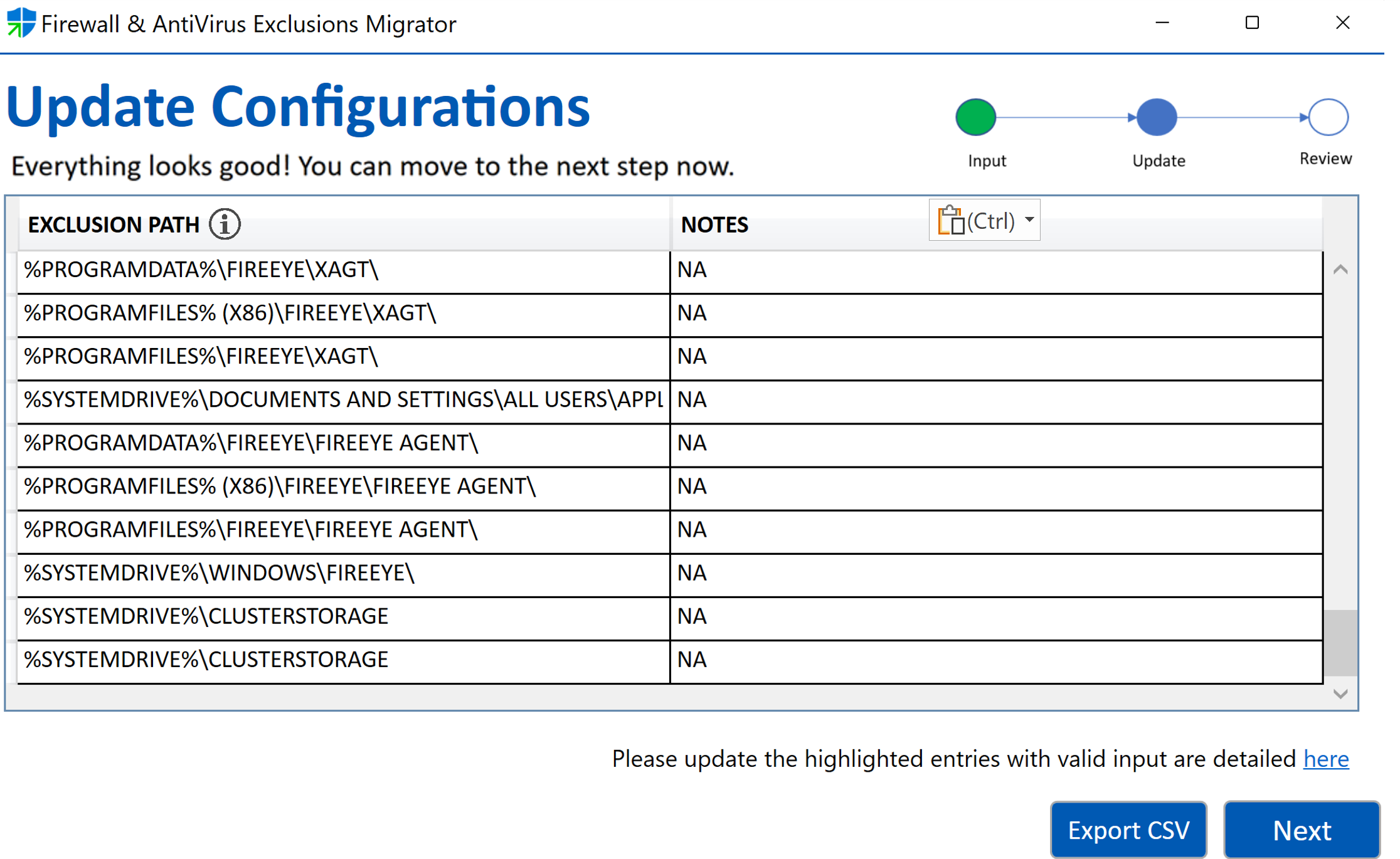
1. You may have some rows which will be highlighted in yellow. These are rows where you need to fix the exclusion path to an acceptable format.
   1. The count of number of rows that need to be fixed will be displayed above the table.
2. You can also click the ‘Export CSV’ button to export a CSV file with all the exclusions.
3. You can manually change any of the cell values if you wish by double-clicking on the corresponding cell.
   1. These details can be edited later using a CSV editor application after the tool has closed.
4. Alternatively, you can choose to skip fixing the highlighted rows. In which case, the invalid highlighted entries will be deleted (i.e., not exported).

Graphical user interface, text, application

Description automatically generated

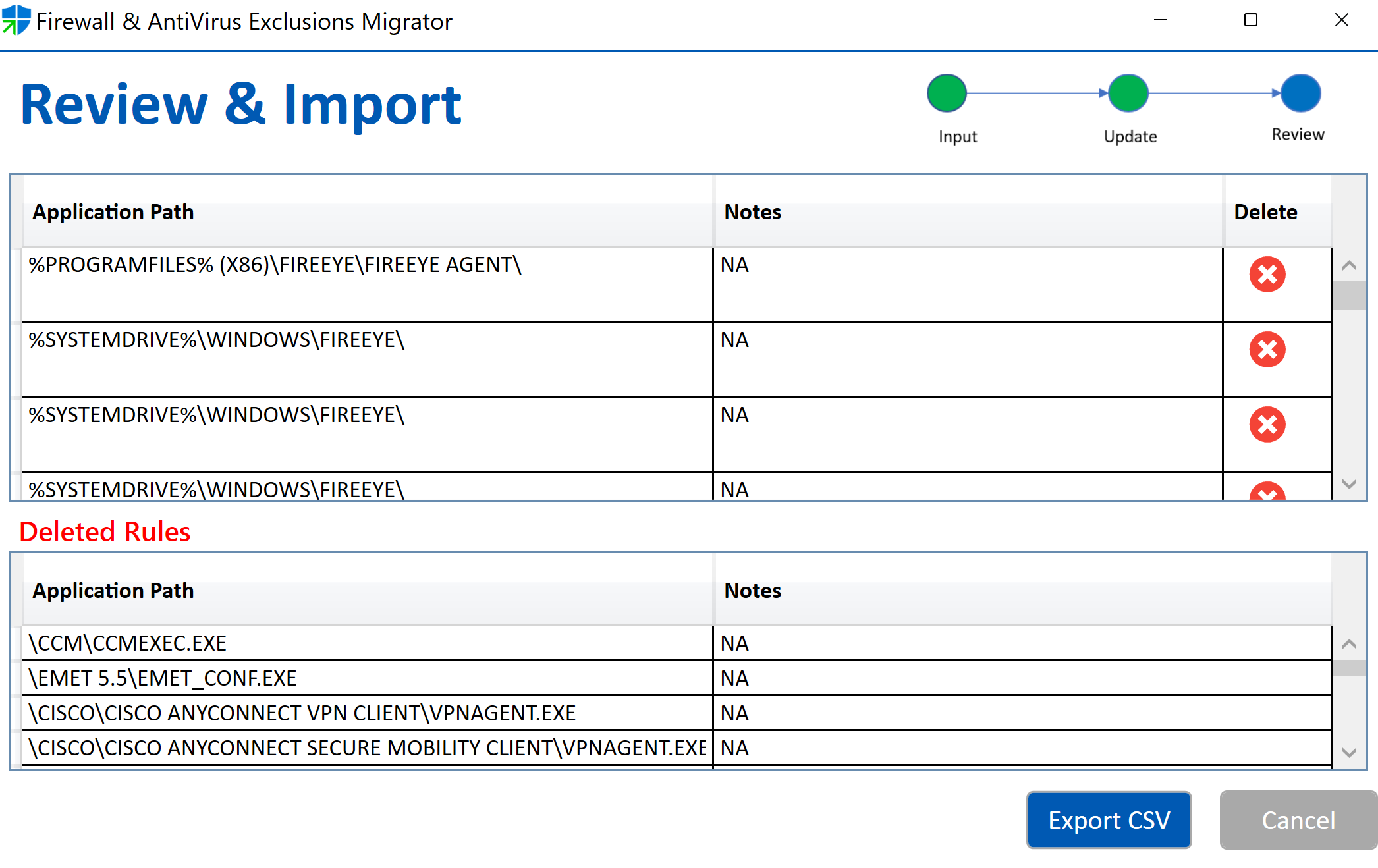
**Recommendation:** We highly recommend you spend a little extra time to review all the highlighted as well as non-highlighted rows and edit them as required.

1. After you have reviewed and fixed all the rows following the above steps, you can click ‘Next’ and move to next step.



### Step 4: Review & Import

Finally, after you completed all the previous steps, your Antivirus Exclusions are ready to be exported.



1. You can have a look at all the paths and any notes for each exclusion before exporting.
   1. Each row has a ‘Delete’ button which you can use to not export that exclusion.
   2. In case you accidentally click the ‘Delete’ button, you can use the ‘Undo’ option.
2. Also, you may be able to see a *Deleted Rules* section if you didn’t fix all the invalid entries in the previous step.   
   1. This section gives a list of all the exclusions that were found in the input file but will not be migrated because of errors in the exclusion path.
3. You can now click the ‘Export CSV’ button to export a CSV file with all the exclusions.

Graphical user interface, text, application

Description automatically generated

### Post Migration: Antivirus Exclusions

Once antivirus exclusions have been exported, please evaluate the exclusions, and remove or add any as required. Generally, Defender AV exclusions aren’t needed, and Defender AV includes many automatic exclusions based on known operating system behaviors and typical management files, such as those used in enterprise management, database management, and other enterprise scenarios and situations.

Please follow the [Defender AV exclusion guidance](https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-exclusions-microsoft-defender-antivirus?view=o365-worldwide). Once you have the exclusions you would like to deploy, you can deploy them using SCCM, Domain based group policy, or Endpoint Manager/Intune.