

Configure and Test AMP File Policy via FDM

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Instructions](#)

[Licensing](#)

[Configuration](#)

[Test](#)

[Troubleshooting](#)

Introduction

This document describes how to configure and test an Advanced Malware Protection (AMP) file policy via Firepower Device Manager (FDM).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Firepower Device Manager (FDM)
- Firepower Threat Defense (FTD)

Components Used

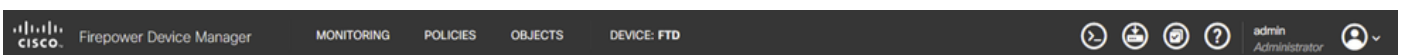
- Cisco virtual FTD version 7.0 managed via FDM
- Evaluation License (Evaluation license is used for demonstration purposes. Cisco recommendation is to acquire and utilize a valid license)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Instructions

Licensing

1. In order to enable the malware license, navigate to the **DEVICE** page on the FDM GUI.



2. Locate the box labeled **Smart License** and click **View Configuration**.

The screenshot displays a grid of configuration cards on the FDM Device Page. The 'Smart License' card is highlighted with a red border and shows 'Evaluation expires in 89 days' and a 'View Configuration' button. Other cards include 'Interface' (7 Enabled), 'Routing' (1 route), 'Updates', 'System Settings', 'Backup and Restore', 'Troubleshoot', 'Site to Site VPN', 'Remote Access VPN', 'Advanced Configuration', and 'Device Administration'. Each card has a 'View Configuration' button.

FDM Device Page

3. Enable the license labeled **Malware**.

The screenshot shows the 'Malware' license configuration page. The license is currently 'Enabled', indicated by a green checkmark. A 'DISABLE' button is visible in the top right corner. Below the status, there is a descriptive text: 'This License allows you to perform Cisco Advanced Malware Protection (AMP) with AMP for Firepower and AMP Threat Grid. You must have this license to apply file policies that detect and block malware in files transmitted over your network.' At the bottom, it lists 'Includes: File Policy'.

Malware License

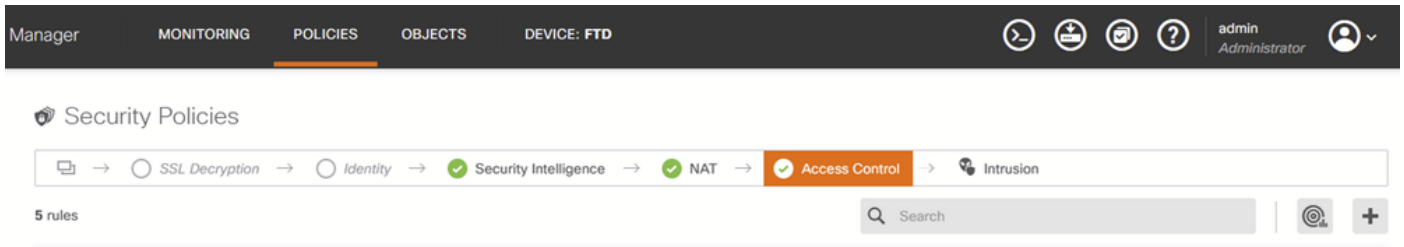
Configuration

1. Navigate to the **POLICIES** page on the FDM.

The screenshot shows the navigation bar of the Firepower Device Manager. The 'POLICIES' tab is selected and highlighted with an orange underline. Other tabs include 'MONITORING', 'OBJECTS', and 'DEVICE: FTD'. The Cisco logo and 'Firepower Device Manager' text are on the left.

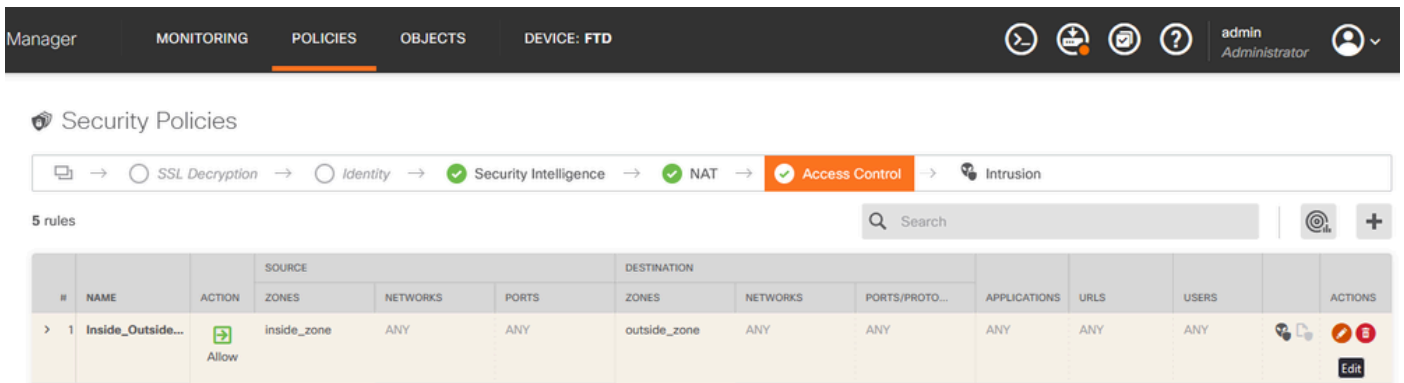
FDM Policies Tab

2. Under **Security Policies**, navigate to the **Access Control** section.



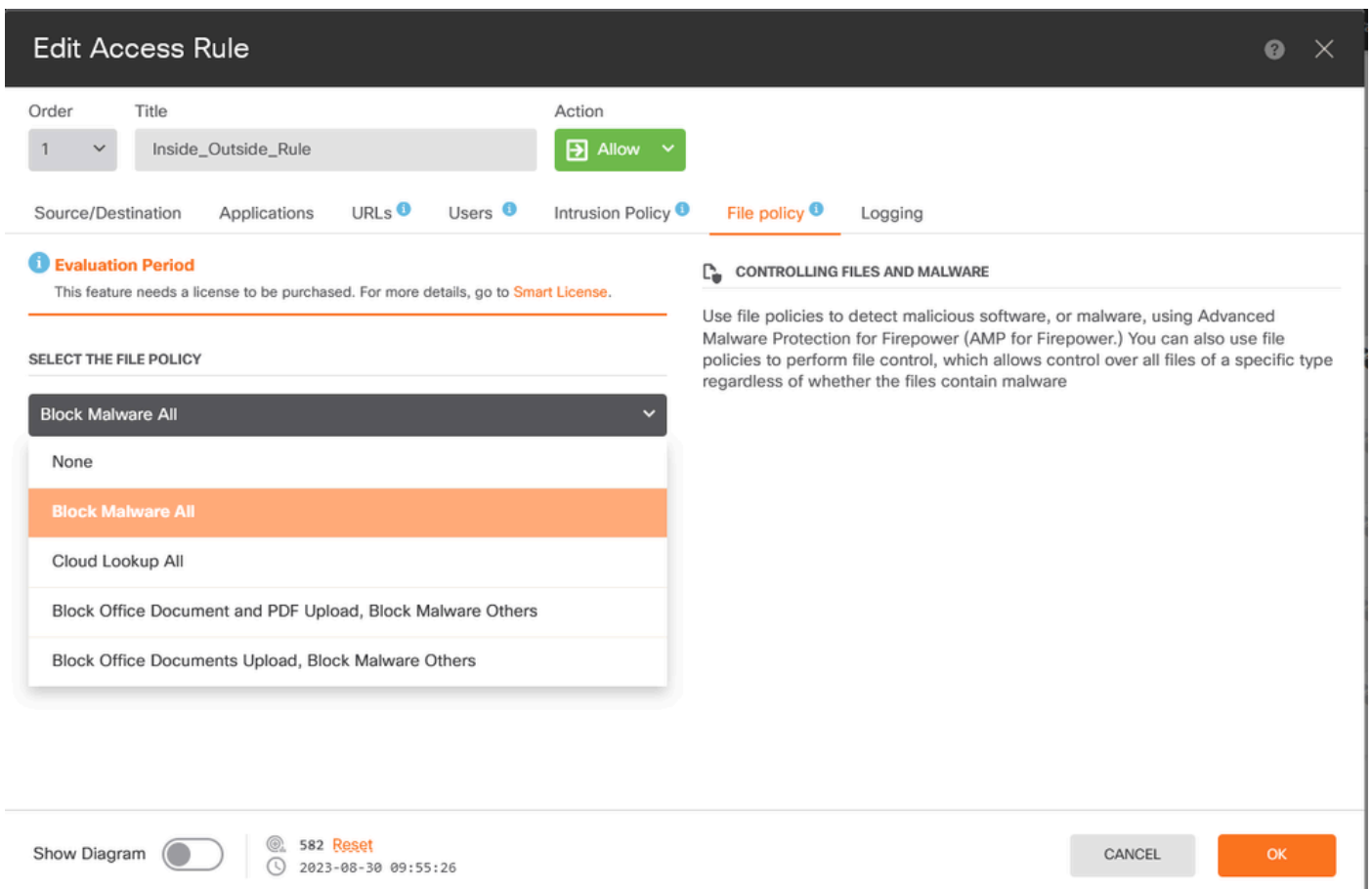
FDM Access Control Tab

3. Find or create an Access Rule to configure the **File Policy**. Click the **Access Rule** editor. For instructions on how to create an Access Rule, refer to the this [link](#).



FDM Access Control Rule

4. Click the **File Policy** section on the **Access Rule** and select the preferred **File Policy** option from the dropdown. Click **OK** to save the changes to the rule.



5. Confirm the **File Policy** has been applied to the Access Rule by checking if the **File Policy** icon is enabled.



File

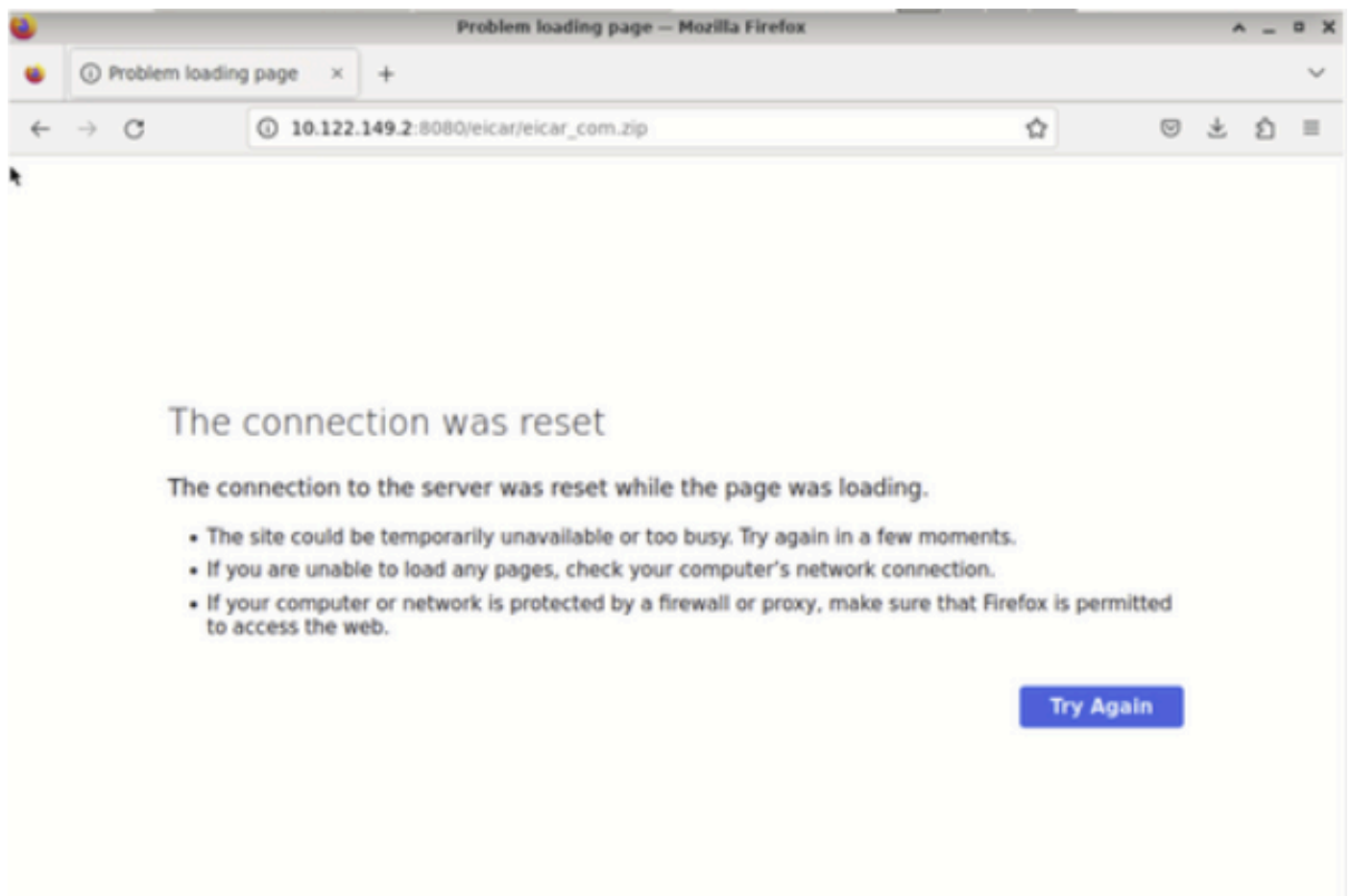
File Policy Icon Enabled

6. **Save** and **Deploy** the changes to the managed device.

Test

To verify the configured file policy for malware protection is working, use these testing scenario attempts to download a malware test file from the web browser of an end host.

As displayed in this screenshot, attempting to download a malware test file from the web browser is unsuccessful.



Browser Download Test

From the FTD CLI, system support trace shows the file download was blocked by file process. For instructions on how to run a system support trace via the FTD CLI, refer to this [link](#).

```
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict Reject and flags 0x00005A00 for 2546d
cffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad of instance 0
192.168.0.10-40016 > 10.122.149.2-8080 6 File Process: drop /eicar/eicar_com.zip
192.168.0.10-40016 > 10.122.149.2-8080 6 IPS Event: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File malware event for 2546dcffc5ad854d4ddc64fbf056871cd5a00
f2471cb7a5bfd4ac23b6e9eedad named eicar_com.zip with disposition Malware and action Block Malware
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 Archive child's been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort detect_drop: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 deleting firewall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST
192.168.0.10-40016 > 10.122.149.2-8080 6 ==> Blocked by File Process
Verdict reason is sent to DAG
```

System Support Trace Test

This confirms the file policy configuration was successful in blocking malware.

Troubleshooting

In case malware is not successfully blocked when using the previous configurations, refer to these troubleshooting suggestions:

1. Verify malware license is not expired.
2. Confirm access control rule is targeting correct traffic.
3. Confirm selected file policy option is correct for targeted traffic and wanted malware protection.

If issue is still not resolvable, contact Cisco TAC for additional support.