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

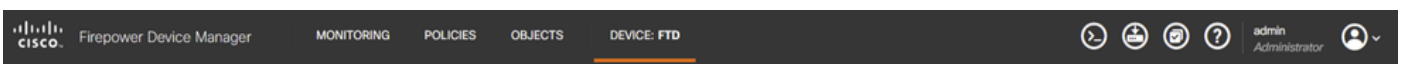
- Cisco virtual FTD version 7.0 managed via FDM
- Evaluation License (Evaluation license is used for demonstration purposes. Cisco recommendation is to acquire and utilize a valid license)

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

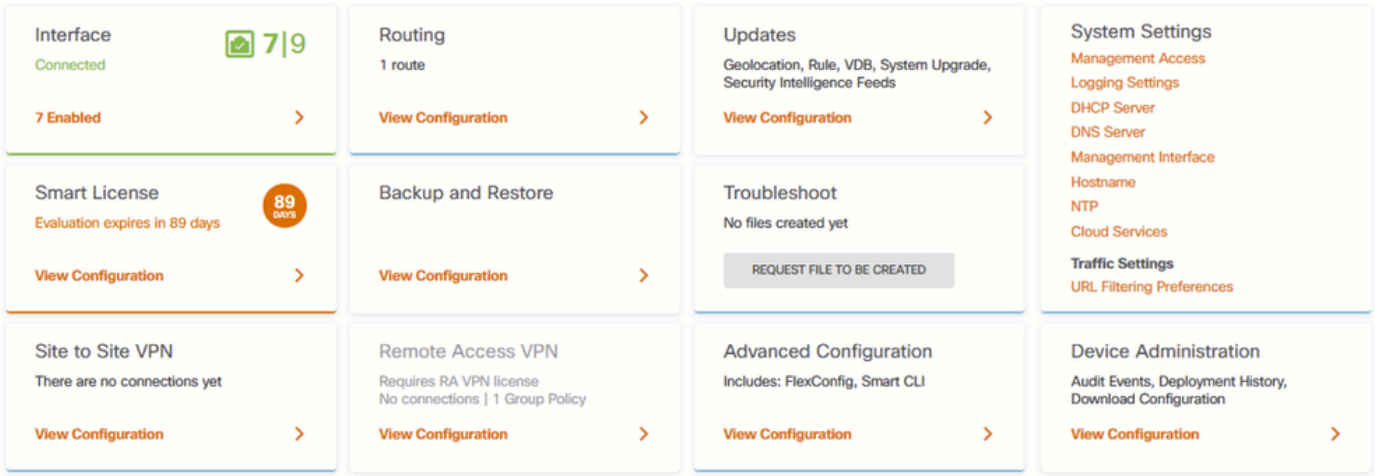
Licensing

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



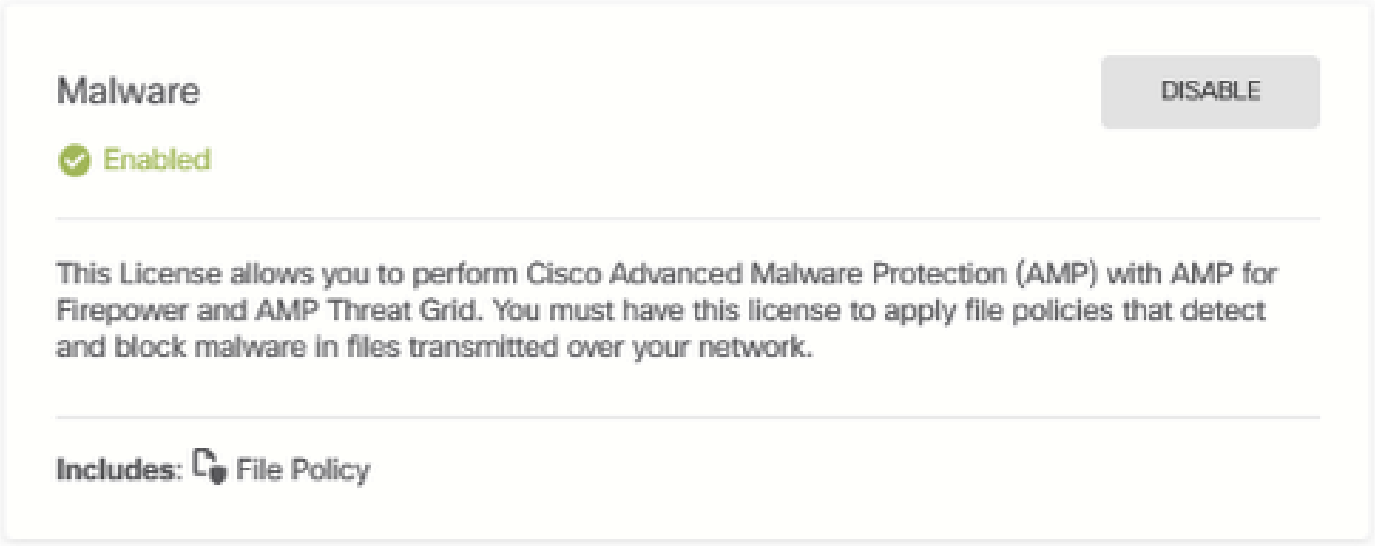
FDM Device Tab

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



FDM Device Page

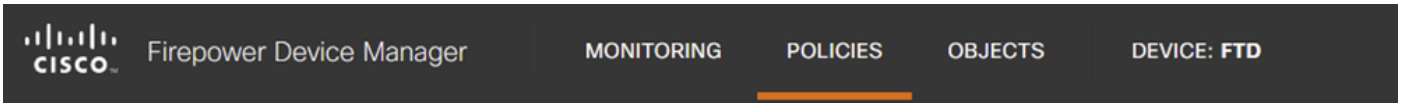
3. Enable the license labeled **Malware**.



Malware License

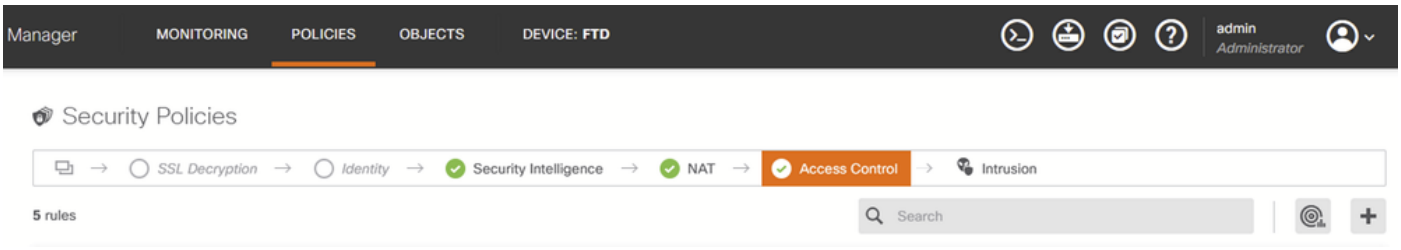
Configuration

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



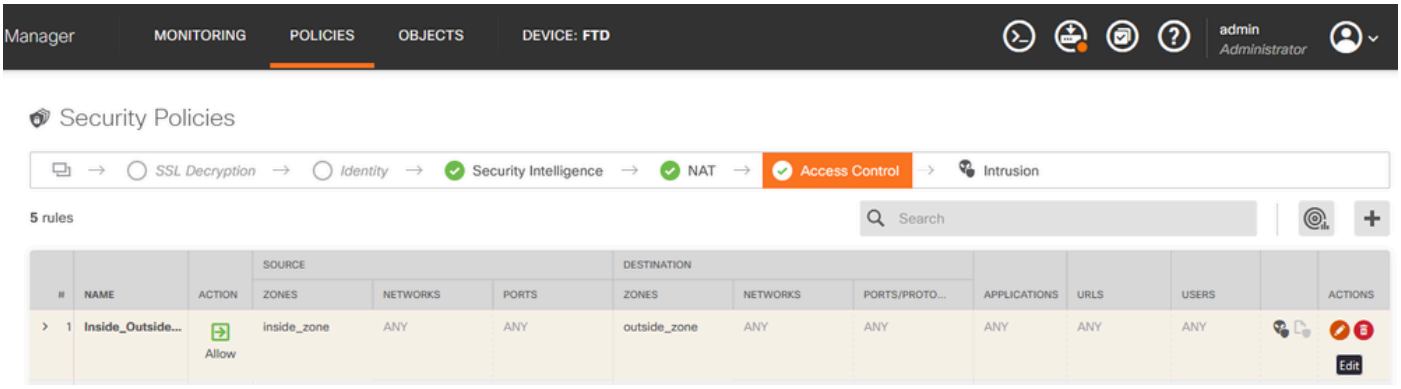
FDM Policies Tab

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



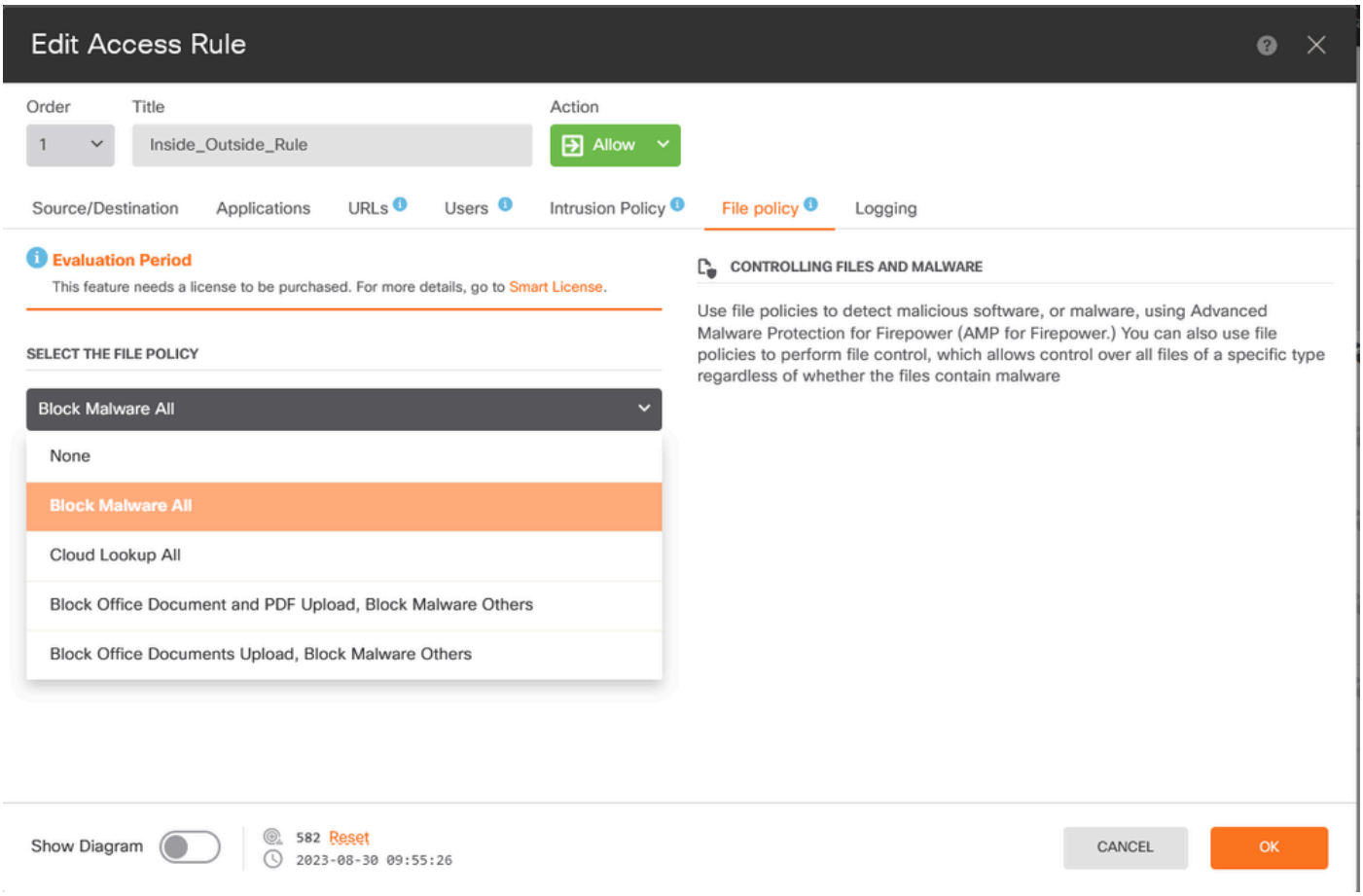
FDM Access Control Tab

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.]



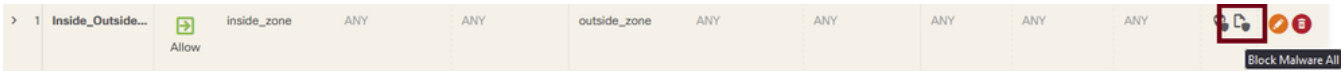
FDM Access Control Rule

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.



FDM Access Control Rule File Policy Tab

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

File 

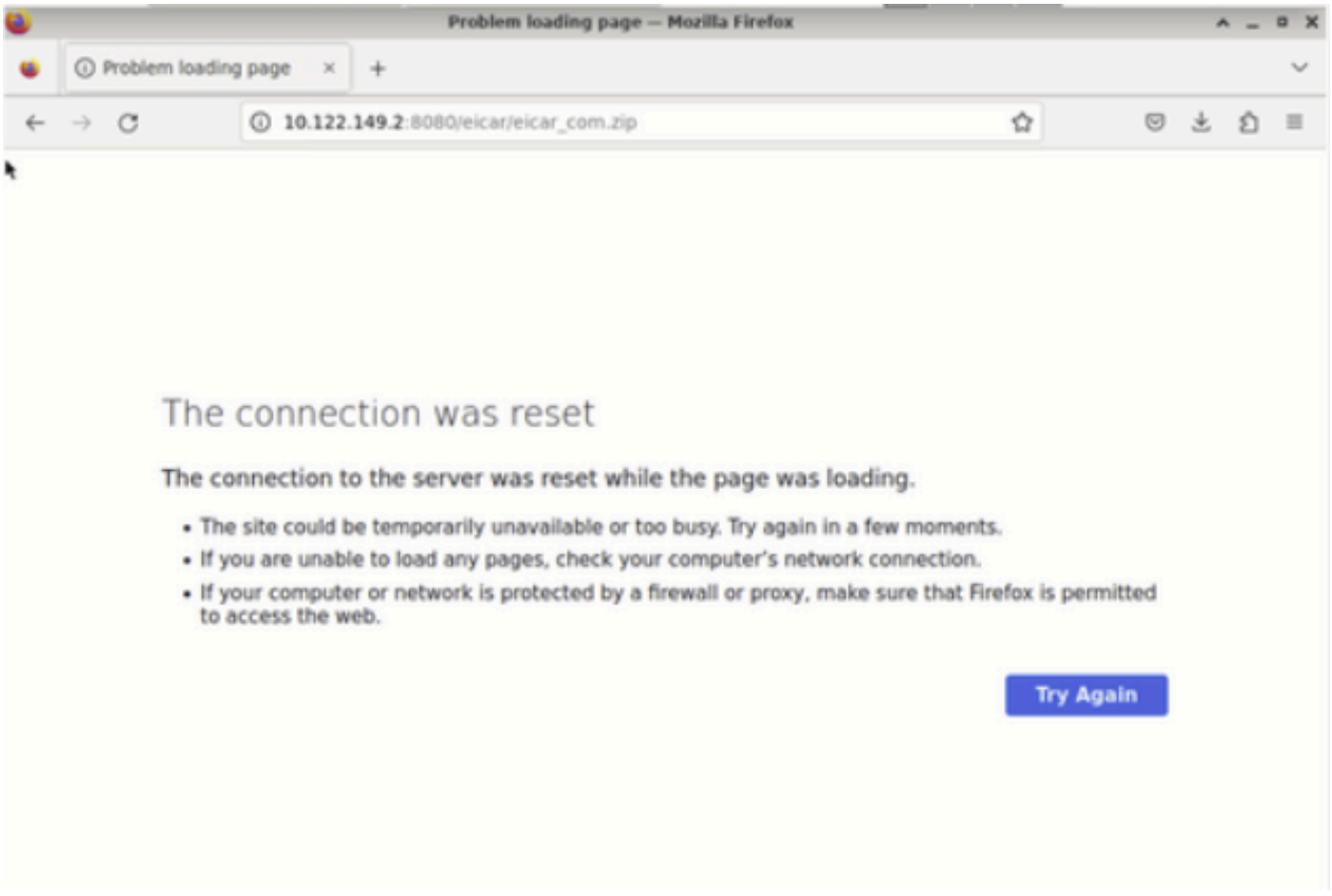
File Policy Icon Enabled

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

Test

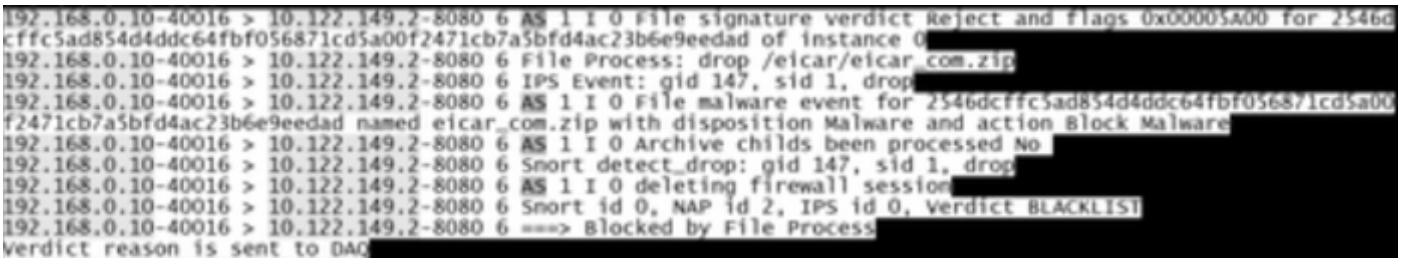
To verify the configured file policy for malware protection is working, use these testing scenario attempts to download a malware test file from the web browser of an end host.

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.



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.