Implement Platform Settings for VPN Troubleshooting

Contents

Introduction

This document describes how to easily organize and identify VPN debug logs using Secure Firewall Management Center and Secure Firewall Threat Defense.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Firewall Threat Defense (FTD)
- Secure Firewall Management Center (FMC)

- Basic understanding of navigating the FMC GUI and FTD CLI
- Existing policy assignment for Platform Settings

Components Used

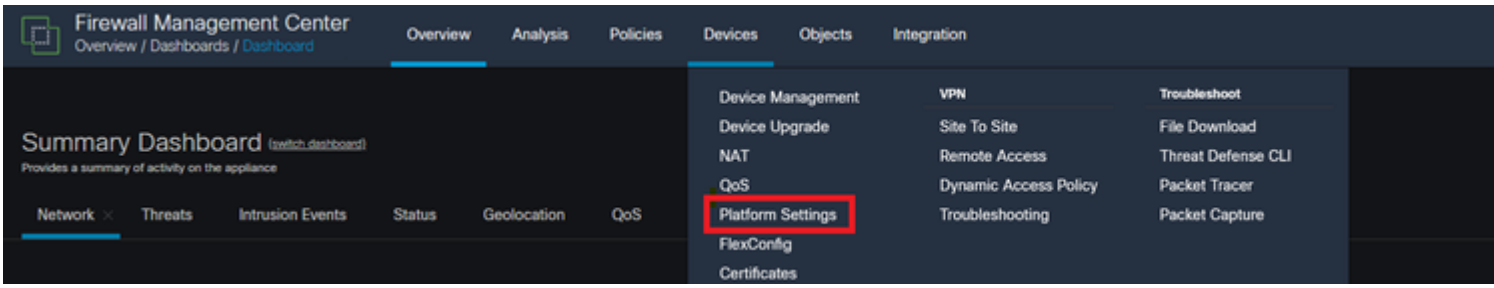
The information in this document is based on these software versions and hardware versions:

- Firewall Management Center version 7.3
- Firewall Threat Defense version 7.3

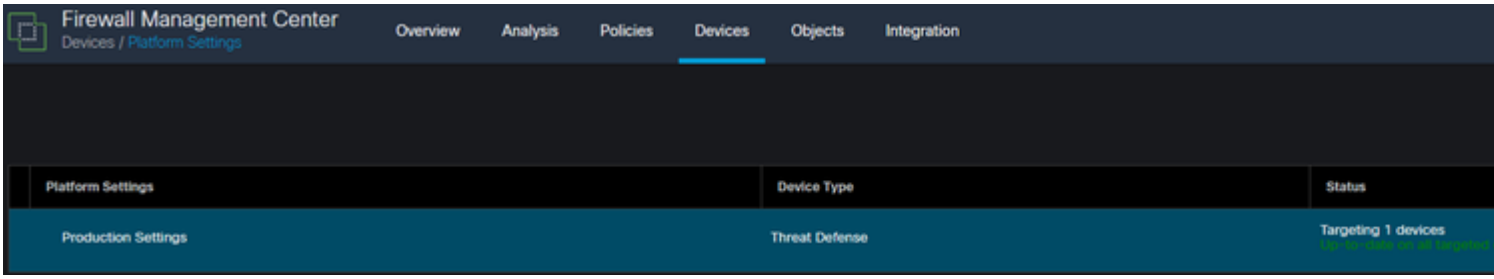
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Firewall Management Center

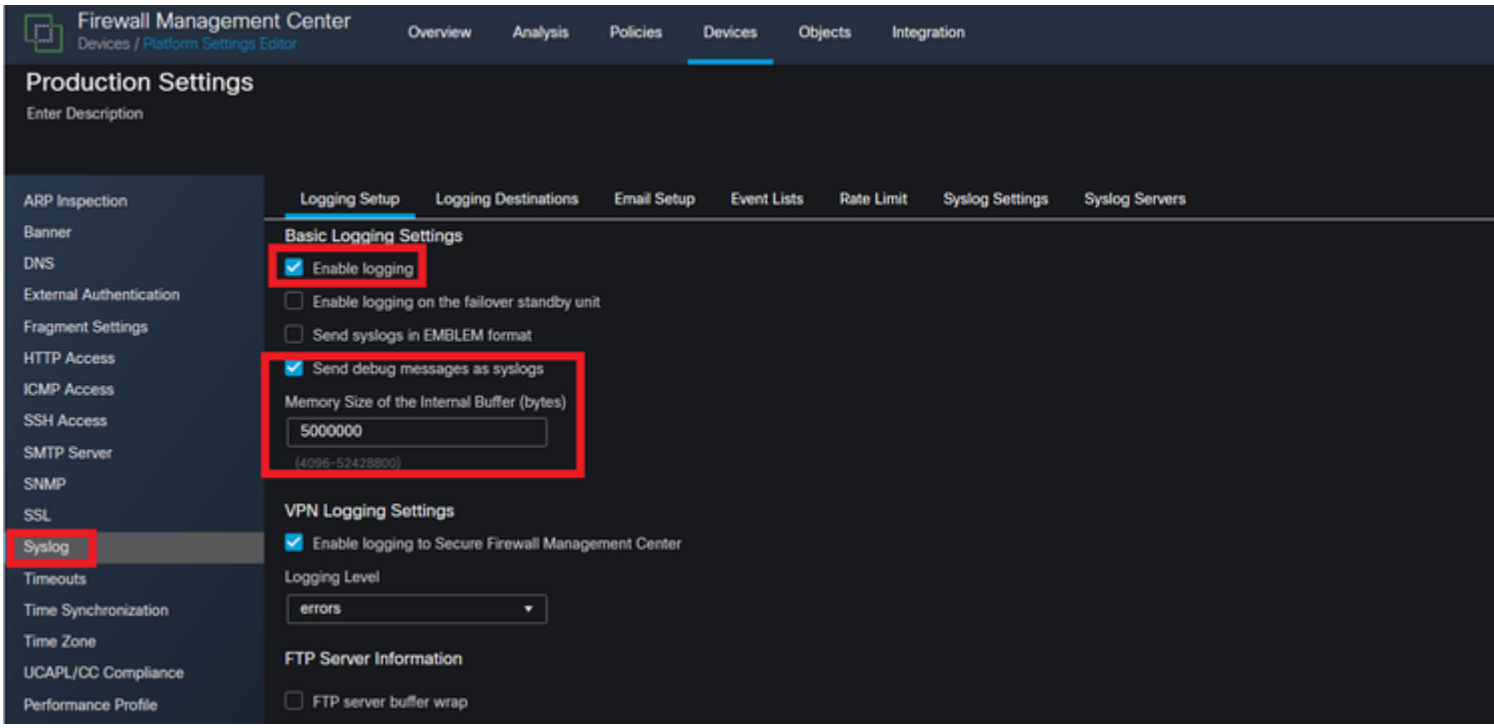
Navigate to Devices > Platform Settings.



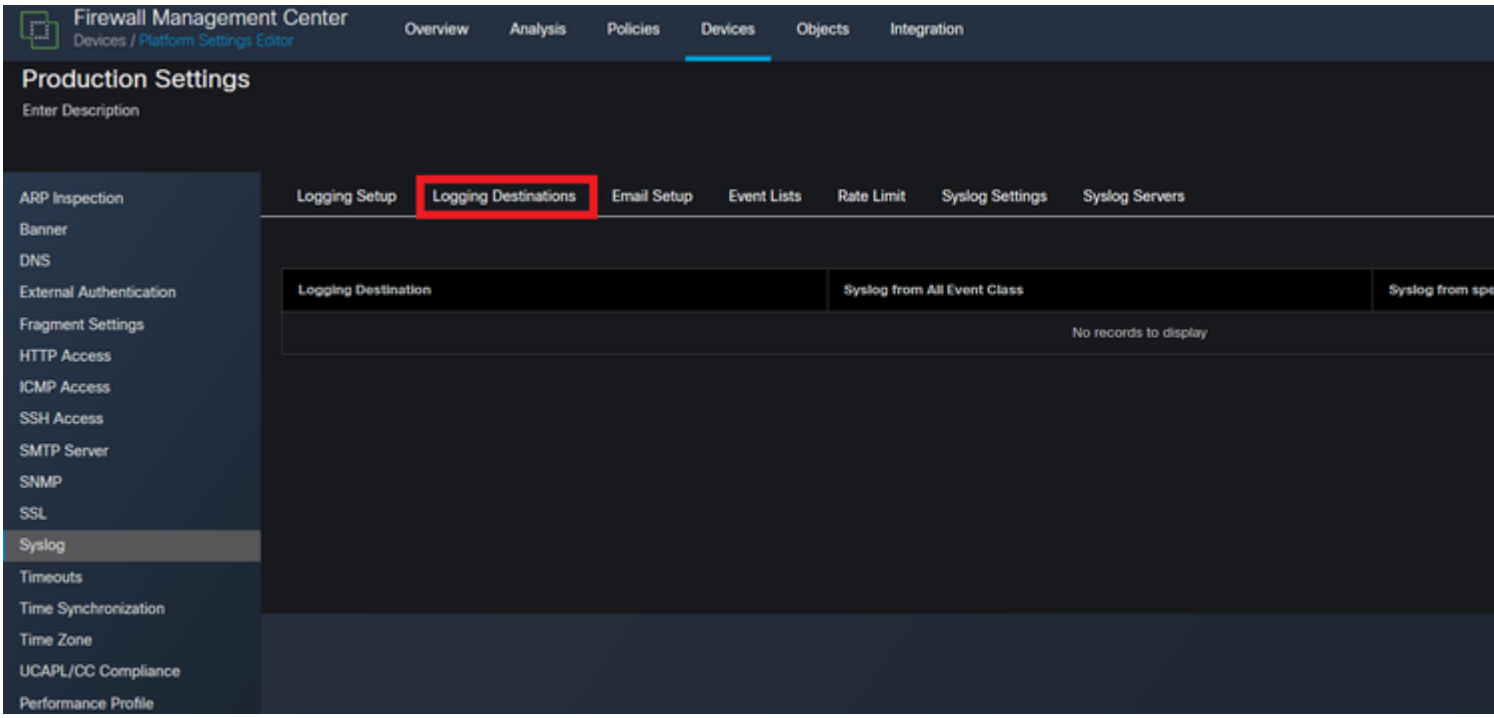
Click the **pencil** between the copy and delete icon.



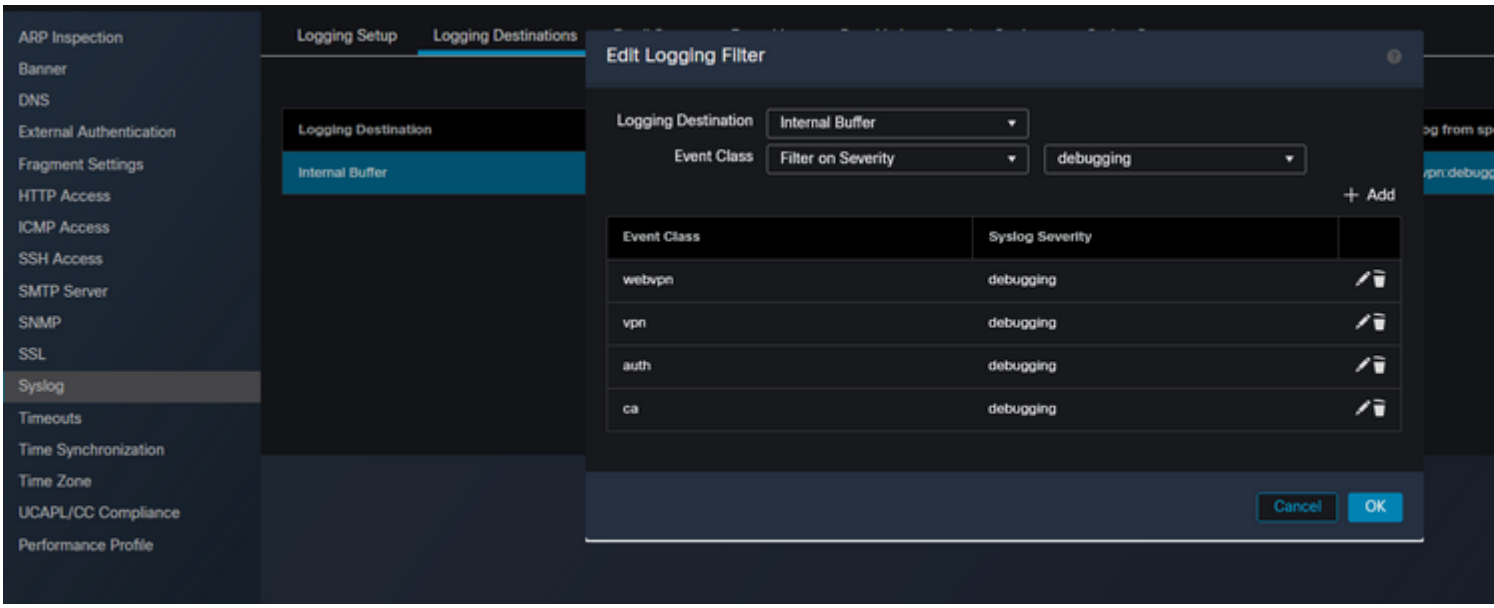
Navigate to Syslogin the left column of options and ensure **Enable Logging,** and **Send debug messages as syslog** are enabled. Additionally, ensure the Memory Size of the Internal Buffer is set with a value that is adequate for troubleshooting purposes.



Click **Logging Destinations** and then click **+Add**.



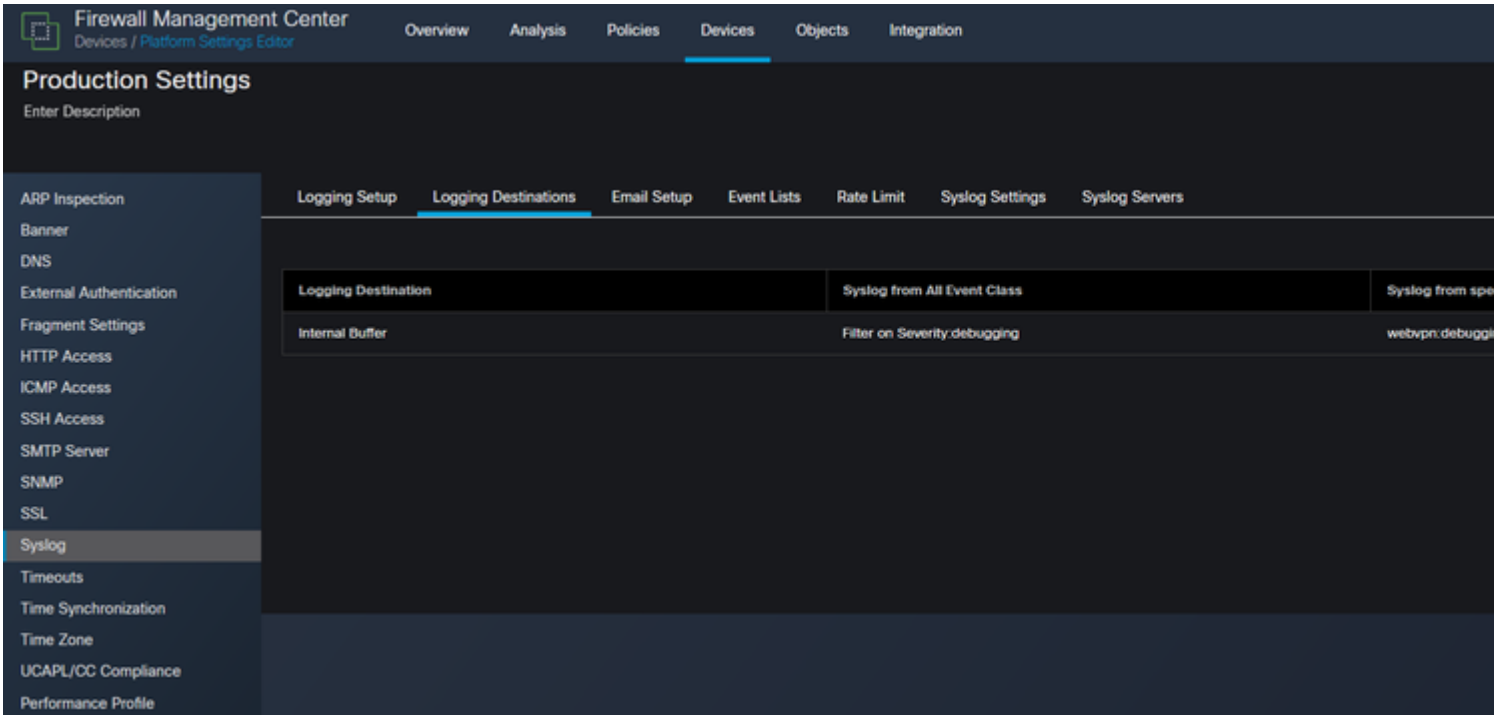
In this section, the logging destination is a preference of the administrator and **Internal Buffer** is used. Change **Event Class** to **Filter on Severity and debugging**. Once this is completed, click +Add and choose webvpn, vpn, auth, and caall with Syslog severity of debugging. This step allows the administrator to filter these debug outputs to a specific syslog message of 711001. These can be modified depending type of troubleshooting. However, the ones chosen in this example cover the most commonly encountered Site-to-Site, Remote Access, and AAA VPN-related issues.



Create event classes and filters for the debugs.

> **Warning**: This changes the Buffer Logging Level to debugging and logs debugging events for the classes specified to the internal buffer. It is recommended to use this logging method for troubleshooting purposes, and not for long-term use.

Choose Save in the top right, and then Deploythe configuration changes.



Firewall Threat Defense

Navigate to the FTD CLI and issue the command show logging setting. The settings here reflect the changes made on the FMC. Ensure the debug-trace logging is enabled, and the buffer logging matches the classes and logging level specified.

```
FTD72# show logging setting
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
```

is applied. This triggers a logging debug-trace notice, letting the administrator know that these debugs are redirected. In order to view these debugs, issue the command show log | in 711001. This syslog ID now only contains relevant VPN debugs as applied by the administrator. Existing logs can be cleared with a clear logging buffer.

```
FTD72# debug webvpn anyconnect 255
INFO: 'logging debug-trace' is enabled. All debug messages are currently being redirected to syslog:711001 and wi
INFO: debug webvpn anyconnect enabled at level 255.
FTD72# show log | in 711001
```

Shows all VPN debugs are being redirected to syslog 711001.