Integrating Microsoft Forefront Threat Management Gateway (TMG)

EventTracker v7.x
Abstract

This guide provides instructions to configure Microsoft Forefront Threat Management Gateway (TMG) 2010 to send events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later, and Microsoft Forefront Threat Management Gateway 2010 and later.

Audience

Microsoft Forefront Threat Management Gateway users, who wish to forward events to EventTracker Manager.
Table of Contents

Abstract ........................................................................................................................................................ 1
Scope ........................................................................................................................................................ 1
Audience ................................................................................................................................................... 1
Overview ....................................................................................................................................................... 3
Pre-requisite ................................................................................................................................................ 3
Integration of EventTracker with Forefront Threat Management Gateway ........................................... 3
EventTracker Knowledge Pack (KP) ........................................................................................................... 4
Categories ................................................................................................................................................ 4
Alerts ........................................................................................................................................................ 7
Import TMG Knowledge pack into EventTracker .................................................................................... 10
To import Category ................................................................................................................................ 10
To import Alerts ..................................................................................................................................... 11
Verify TMG knowledge pack in EventTracker .......................................................................................... 12
Verify Forefront Threat Management Gateway Categories ...................................................................... 12
Verify Forefront Threat Management Gateway Alerts ............................................................................. 13
Overview

Forefront Threat Management Gateway (TMG) 2010 is a multi-layered perimeter defense system. An enterprise-class firewall with advanced web protection features such as URL filtering, gateway-integrated virus and malicious software scanning, network intrusion detection and prevention, and outbound HTTPS inspection, Forefront TMG provides exceptional protection from advanced, persistent threats. It also provides secure remote access to internal networks and applications and can serve as a consolidated secure mail relay.

Pre-requisite

Prior to configuring Forefront Threat Management Gateway and the EventTracker Enterprise, ensure that you meet the following prerequisites:

- EventTracker V 7.x should be installed.
- Forefront Threat Management Gateway 2010 should be installed and proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.

Integration of EventTracker with Forefront Threat Management Gateway

To configure Forefront Threat Management Gateway Firewall to forward the log to EventTracker Enterprise, deploy EventTracker Agent.
EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker V 7.x to support Forefront Threat Management Gateway (TMG) monitoring:

Categories

- **Forefront TMG: Accumulation folder created** - This category based report provides information when an accumulation folder is created.
- **Forefront TMG: Accumulation folder failed to create** - This category based report provides information when the creation of an accumulation folder is failed.
- **Forefront TMG: All events** - This category based report provides information related to all events.
- **Forefront TMG: Authentication failed** - This category based report provides information about the failed authentications.
- **Forefront TMG: Authentication success** - This category based report provides information related to the successful authentications.
- **Forefront TMG: Cache container initialization error** - This category based report provides information related to cache container initialization error.
- **Forefront TMG: Cache file resize failure** - This category based report provides information related to cache file resize failure.
- **Forefront TMG: Cache initialization failure** - This category based report provides information related to cache initialization failure.
- **Forefront TMG: Cache permissions insufficient** - This category based report provides information related to insufficient cache permissions.
- **Forefront TMG: Cache restoration completed** - This category based report provides information related to the completed cache restoration processes.
- **Forefront TMG: Cache write error** - This category based report provides information related to cache write errors.
• Forefront TMG: Cached object discarded - This category based report provides information related to the discarded cached objects.

• Forefront TMG: Certificate expired - This category based report provides information related to the expired certificates.

• Forefront TMG: Certificate expiring soon - This category based report provides information, if the certificate is expiring soon.

• Forefront TMG: Certificate imported successfully - This category based report provides information, if the certificate is imported successfully.

• Forefront TMG: Certificate invalid - This category based report provides information if the certificate is invalid.

• Forefront TMG: Certificate issuer not trusted - This category based report provides information if the certificate issuer is not trusted.

• Forefront TMG: Certificate revoked - This category based report provides information related to the revoked certificates.

• Forefront TMG: Certificates cannot be initialized - This category based report provides information related to certificates that cannot be initialized.

• Forefront TMG: Client disk space limit exceeded - This category based report provides information, if the client disk space limit exceeds.

• Forefront TMG: Content download timed out - This category based report provides information if the content download is timed out.

• Forefront TMG: Content theft detected - This category based report provides information if content theft is detected.

• Forefront TMG: Database error - This category based report provides information related to database error.

• Forefront TMG: Definitions loaded - This category based report provides information related to definitions loaded.

• Forefront TMG: Definitions not loaded - This category based report provides information related to definitions not loaded.

• Forefront TMG: Definitions outdated - This category based report provides information related to definitions outdated.
- **Forefront TMG: Deletion of outdated definitions failed** - This category based report provides information related to deletion of outdated definitions failed.

- **Forefront TMG: DHCP anti-poisoning intrusion detection** - This category based report provides information related to DHCP anti-poisoning intrusion detection.

- **Forefront TMG: DNS intrusion** - This category based report provides information related to DNS intrusion.

- **Forefront TMG: Firewall configuration changes** - This category based report provides information related to firewall configuration changes.

- **Forefront TMG: Firewall policy changes** - This category based report provides information related to firewall policy changes.

- **Forefront TMG: Flood mitigation attack** - This category based report provides information related to flood mitigation attack.

- **Forefront TMG: Imported SSL certificate cannot access** - This category based report provides information related to imported SSL certificate cannot access.

- **Forefront TMG: Intrusion detection** - This category based report provides information related to intrusion detection.

- **Forefront TMG: License expired** - This category based report provides information related to license expired.

- **Forefront TMG: Malware detected** - This category based report provides information related to malware detected.

- **Forefront TMG: Malware inspection disabled** - This category based report provides information related to malware inspection disabled.

- **Forefront TMG: Notification template not loaded** - This category based report provides information related to notification template not loaded.

- **Forefront TMG: POP intrusion** - This category based report provides information related to POP intrusion.

- **Forefront TMG: Requested new pin** - This category based report provides information related to requested new pin.

- **Forefront TMG: Server incompatible** - This category based report provides information related to server incompatible.
• **Forefront TMG: Server rejected passcode** - This category based report provides information related to server rejected passcode.

• **Forefront TMG: Service stopped** - This category based report provides information related to service stopped.

• **Forefront TMG: Traffic allowed** - This category based report provides information related to traffic allowed.

• **Forefront TMG: Traffic denied** - This category based report provides information related to traffic denied.

• **Forefront TMG: Update failed** - This category based report provides information related to update failed.

• **Forefront TMG: Update successfully** - This category based report provides information related to update successfully.

• **Forefront TMG: VPN connection failure** - This category based report provides information related to VPN connection failure.

• **Forefront TMG: Web publishing rules created** - This category based report provides information related to web publishing rules created.

• **Forefront TMG: Web request allowed** - This category based report provides information related to web request allowed.

• **Forefront TMG: Web request denied** - This category based report provides information related to web request denied.

**Alerts**

• **Forefront TMG: Accumulation folder failed to create** - This alert is generated when accumulation folder failed to create.

• **Forefront TMG: Alert action failure** - This alert is generated when alert action failure occurs.

• **Forefront TMG: Authentication failed** - This alert is generated when authentication failed.

• **Forefront TMG: Cache container initialization error** - This alert is generated when cache container initialization error.

• **Forefront TMG: Cache file resize failure** - This alert is generated when cache file resize failure occurs.
EventTracker: Integrating Microsoft Forefront Threat Management Gateway

- **Forefront TMG: Cache initialization failure** - This alert is generated when cache initialization failure occurs.

- **Forefront TMG: Cache permissions insufficient** - This alert is generated when cache permissions insufficient event occurs.

- **Forefront TMG: Cache restoration completed** - This alert is generated when cache restoration completed.

- **Forefront TMG: Cache write error** - This alert is generated when cache write error occurs.

- **Forefront TMG: Cached object discarded** - This alert is generated when cached object discarded.

- **Forefront TMG: Certificate expired** - This alert is generated when certificate expired.

- **Forefront TMG: Certificate expiring soon** - This alert is generated when certificate expiring soon event occurs.

- **Forefront TMG: Certificate imported successfully** - This alert is generated when certificate imported successfully event occurs.

- **Forefront TMG: Certificate invalid** - This alert is generated when certificate invalid.

- **Forefront TMG: Certificate issuer not trusted** - This alert is generated when certificate issuer not trusted.

- **Forefront TMG: Certificate revoked** - This alert is generated when certificate revoked.

- **Forefront TMG: Certificates cannot be initialized** - This alert is generated when certificates cannot be initialized.

- **Forefront TMG: Client disk space limit exceeded** - This alert is generated when client disk space limit exceeded.

- **Forefront TMG: Definitions loaded** - This alert is generated when definitions loaded.

- **Forefront TMG: Definitions not loaded** - This alert is generated when definitions not loaded.

- **Forefront TMG: Definitions outdated** - This alert is generated when definitions outdated.

- **Forefront TMG: Deletion of outdated definitions failed** - This alert is generated when deletion of outdated definitions failed.
- **Forefront TMG: DHCP anti-poisoning intrusion detection** - This alert is generated when DHCP anti-poisoning intrusion detection event occurs.

- **Forefront TMG: DNS Intrusion** - This alert is generated when DNS Intrusion event occurs.

- **Forefront TMG: E-Mail Policy configuration failure** - This alert is generated when E-Mail Policy configuration failure event occurs.

- **Forefront TMG: E-Mail Policy configuration reapplied** - This alert is generated when E-Mail Policy configuration reapplied.

- **Forefront TMG: E-Mail Policy required products not installed** - This alert is generated when E-Mail Policy required products not installed.

- **Forefront TMG: E-Mail policy required service not started** - This alert is generated when E-Mail policy required service not started.

- **Forefront TMG: Event Log Deletion Failure** - This alert is generated when event Log Deletion Failure occurs.

- **Forefront TMG: Flood mitigation attack** - This alert is generated when flood mitigation attack occurs.

- **Forefront TMG: Imported SSL certificate cannot access** - This alert is generated when imported SSL certificate cannot access event occurs.

- **Forefront TMG: Intrusion detection** - This alert is generated when intrusion detection event occurs.

- **Forefront TMG: LDAP server unavailable** - This alert is generated when LDAP server unavailable event occurs.

- **Forefront TMG: License expired** - This alert is generated when license expired.

- **Forefront TMG: Malware detected** - This alert is generated when malware detected.

- **Forefront TMG: POP intrusion** - This alert is generated when POP intrusion event occurs.

- **Forefront TMG: Server publishing failure** - This alert is generated when server publishing failure event occurs.

- **Forefront TMG: Service stopped** - This alert is generated when service stopped.

- **Forefront TMG: Traffic denied** - This alert is generated when traffic denied.

- **Forefront TMG: Web request denied** - This alert is generated when web request denied.
Import TMG Knowledge pack into EventTracker

1. Launch EventTracker Control Panel.

2. Double click Import Export Utility. Click the Import tab. Import Category and Alert as given below.

To import Category

1. Click Category option, and then click the browse button.

2. Locate the All TMG group of Categories.iscat file, and then click the Open button.

Figure 1
3. Click the **Import** button to import the categories.

EventTracker displays success message.

![Figure 2](image)

4. Click the **OK** button. Click the **Close** button.

To import Alerts

1. Click **Alert** option, and then click the browse button.

![Figure 3](image)
2. Locate the **All TMG group of Alerts.isalt** file, and then click the **Open** button.

3. Click the **Import** button to import the alerts.

   EventTracker displays success message.

   ![Figure 4](image)

4. Click the **OK** button. Click the **Close** button.

**Verify TMG knowledge pack in EventTracker**

**Verify Forefront Threat Management Gateway Categories**

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** dropdown, and then click **Categories**.

3. In the **Category Tree**, expand Microsoft Forefront group folder under this Threat Management Gateway to see the imported categories.
Verify Forefront Threat Management Gateway Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin dropdown, and then click Alerts.
3. In the Search field, type Forefront TMG, and then click the Go button.

Alert Management page will display all the imported Forefront Threat Management Gateway alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Message from webpage](image)

**Figure 7**

5. Click the **OK** button, and then click the **Activate now** button.

**NOTE**: You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.