Netsurion | EventTracker®

How to - forward Exchange Logs to EventTracker

EventTracker v9.x and above

Publication Date: May 12, 2020

Abstract

EventTracker allows you to effectively manage your systems and provides operational efficiencies – reducing IT costs and freeing resources for other duties that increase the business value of your organization. EventTracker's built-in knowledge base enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Scope

The configuration details in this guide are consistent with EventTracker version 9.x and later, and Microsoft Exchange Server 2010, 2013, 2016 and later.

Audience

EventTracker users, who want to monitor Microsoft Exchange Server.

Table of Contents

1. Introduction

Microsoft Exchange Server is Microsoft's email, calendaring, contact, scheduling and collaboration platform deployed on the Windows Server operating system for use within a business or larger enterprise.
Microsoft designed Exchange Server to give users access to the messaging platform on smartphones, tablets, desktops and web-based systems. Exchange users collaborate through calendar and document sharing. Storage and security features in the platform let organizations archive content, perform searches and execute compliance tasks.

With EventTracker you can monitor all your servers running Microsoft Exchange from a single view. EventTracker centrally consolidates all the event logs, SMTP logs and connectivity logs. Through consolidated logging you can monitor the performance, availability, and security of your Exchange servers. EventTracker can generate reports for mailbox access, mailbox changes, message tracking, audit activity, user permission and database changes by admin.

2. Prerequisites

- EventTracker Agent should be installed on the Exchange server.
- PowerShell version 5.0 or later should be installed.
- User with admin permission on Exchange Server.
- Enabling Message Tracking, Admin and mailbox auditing using Exchange Server.
- Enable remote PowerShell on user which integrator can use to fetch logs.

3. Enabling Message Trace, Mailbox audit and admin audit Logging on Exchange Server

1. Please contact EventTracker Support for script which will help to enabling logging on Exchange Server
2. Login to Exchange Server.
3. Open “Exchange Management Shell” in exchange Server.
4. Click **Start** > **Microsoft Exchange Server > Exchange Management Shell**.
5. Run downloaded script using following command
   `& “<Downloaded path>\EnableLogging.ps1”`
6. Once you run above script, it will ask for folder location where you want to store message tracking logs

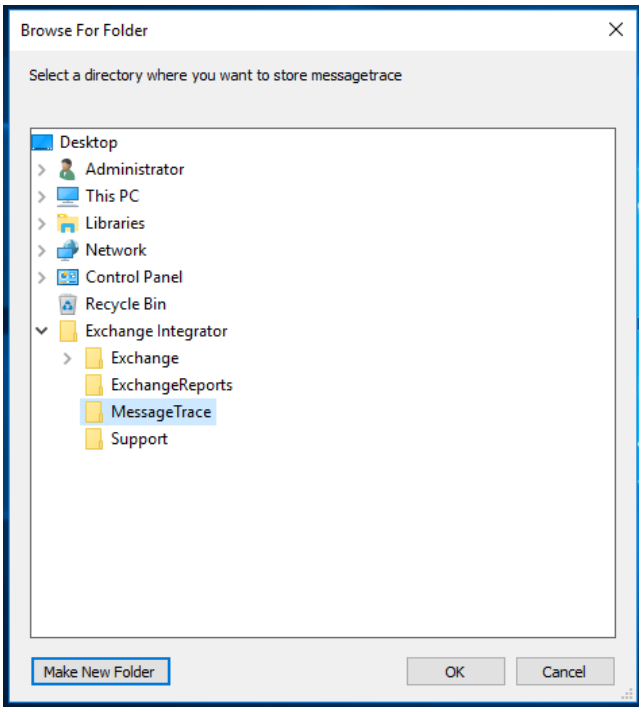

Figure 1

7. Select the folder or make new folder. Click **OK.**

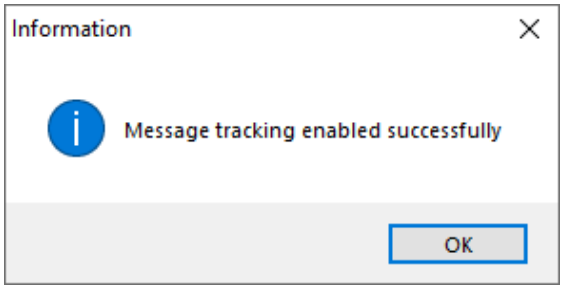

Figure 2

8. After message tracking is enabled, script will try to enable admin auditing on exchange sever. Once it's enabled, it will show following message

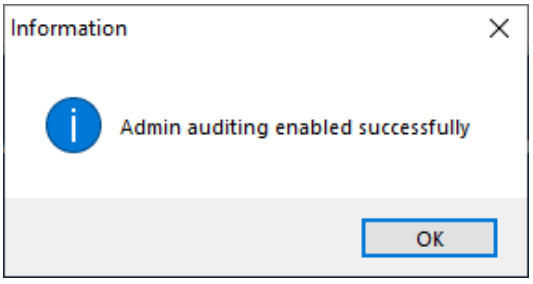

Figure 3

9. Now script will try to enable the mailbox auditing.
   By default, script will enable the mailbox auditing for all the user.

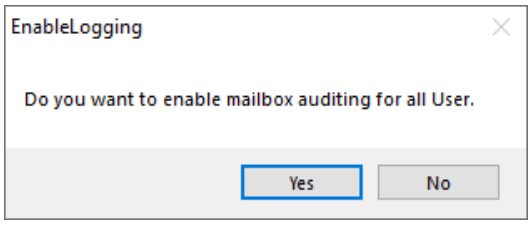

Figure 4

Once you click **Yes,** it will enable mailbox auditing for all the user.
If you don't want to enable mailbox auditing for all user. You can use following cmdlets in Exchange management shell for enabling mailbox auditing:

```
Set-Mailbox -Identity "Lahuara1" -AuditEnabled $true
```

You can also use CSV file of identity for enabling auditing logs. Following is the command set in Exchange management shell for enabling mailbox auditing using CSV

```
Import-Csv <path of CSV file> | %{
Set-Mailbox -Identity $_ -AuditEnabled $true
}
```

Above command will enable the auditing for users.

Now after doing above instruction, we are ready to integrate Exchange server to EventTracker

4. Integrating Exchange with EventTracker

Before running ExchangeIntegrator, we need to enable Remote PowerShell on one of the User which we can use to get logs from exchange sever. Following is the command used for enabling remote PowerShell in exchange server.

```
Set-user "Lahuara1" -RemotePowerShellEnabled $true
```

1. Run the integrator on any EventTracker agent machine.

Note: you can use Exchange Server also. Please install EventTracker agent on Exchange server.

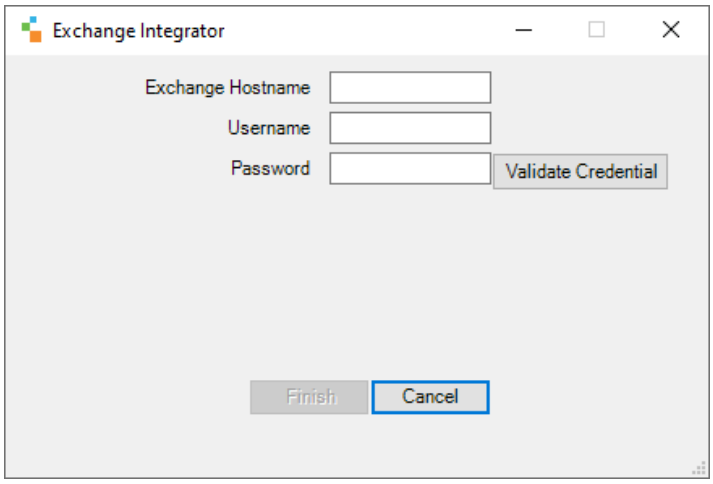

Figure 5

2. Provide the Exchange Server hostname, Username and password of identity on which remote PowerShell enabled.
3. Now, click on Validate credential to check the user.
4. If username/password is correct, it will enable the **Finish** button
5. Click **Finish** to complete the Integration.

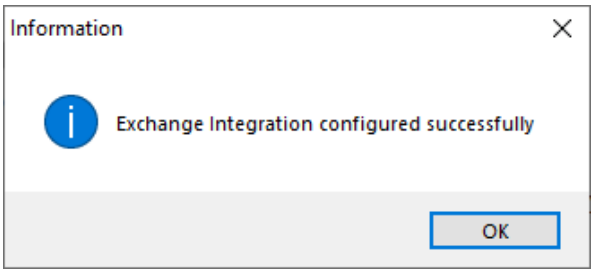

Figure 6