



**N-Partner**

**N-REPORTER**

How do user manage Exchange  
Server message tracking audit log  
**V 1.1.4**

## Prefac

This document is mainly to introduce how N-Reporter users manage Exchange Server message tracking audit log. The first step is to deploy Exchange message tracking. Secondly, use the Open Source tool, NXLOG Community Edition, to convert the message tracking record into Syslog, and send to N-Reporter. Since there are some difference setting between Windows and Exchange, the deployment of Exchange Management Console(EMC) may be different. The deploy environment of this document is Windows server 2003 64bit with Exchange 2007, Windows server 2008 R2 with Exchange 2010 and Windows server 2012 with Exchange 2013.

Message tracking record is the detailed mail record of all the message transmission including Exchange server with Hub Transport server role, Mailbox server role or the computer with Edge Transport server role. The Exchange Server with Client Access server role or Unified messaging server role does not have message tracking record. The deployment of this document is for Exchange Server with Hub Transport server role or Edge Transport server role.

Note: Exchange Server enable message tracking logging by default.

## Contents:

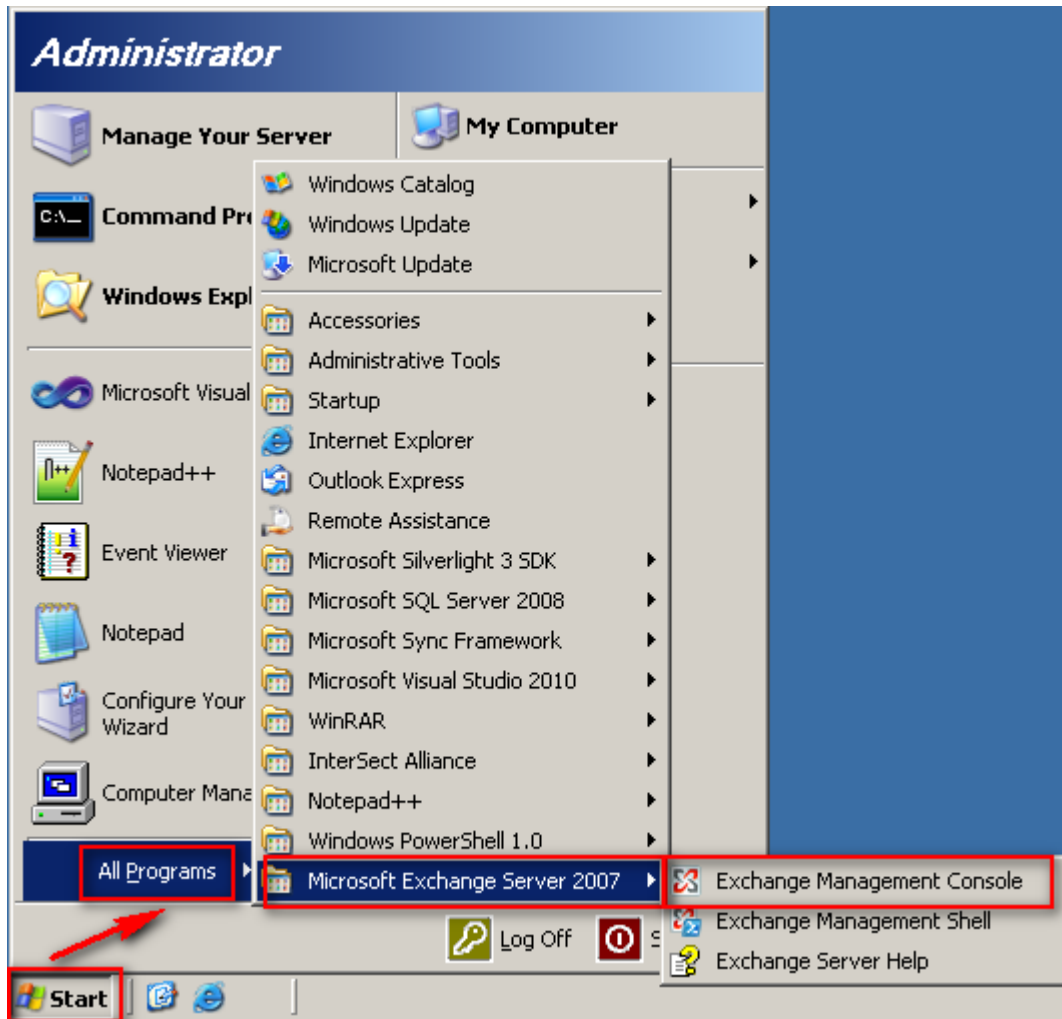
1 Set up Exchange Server 2007 message tracking log .....	2
2 Set up Exchange Server 2010 message tracking log .....	6
3 Set up Exchange Server 2013 message tracking log .....	9
4 Set up NXLOG .....	12

# 1 Set up Exchange Server 2007 message tracking log

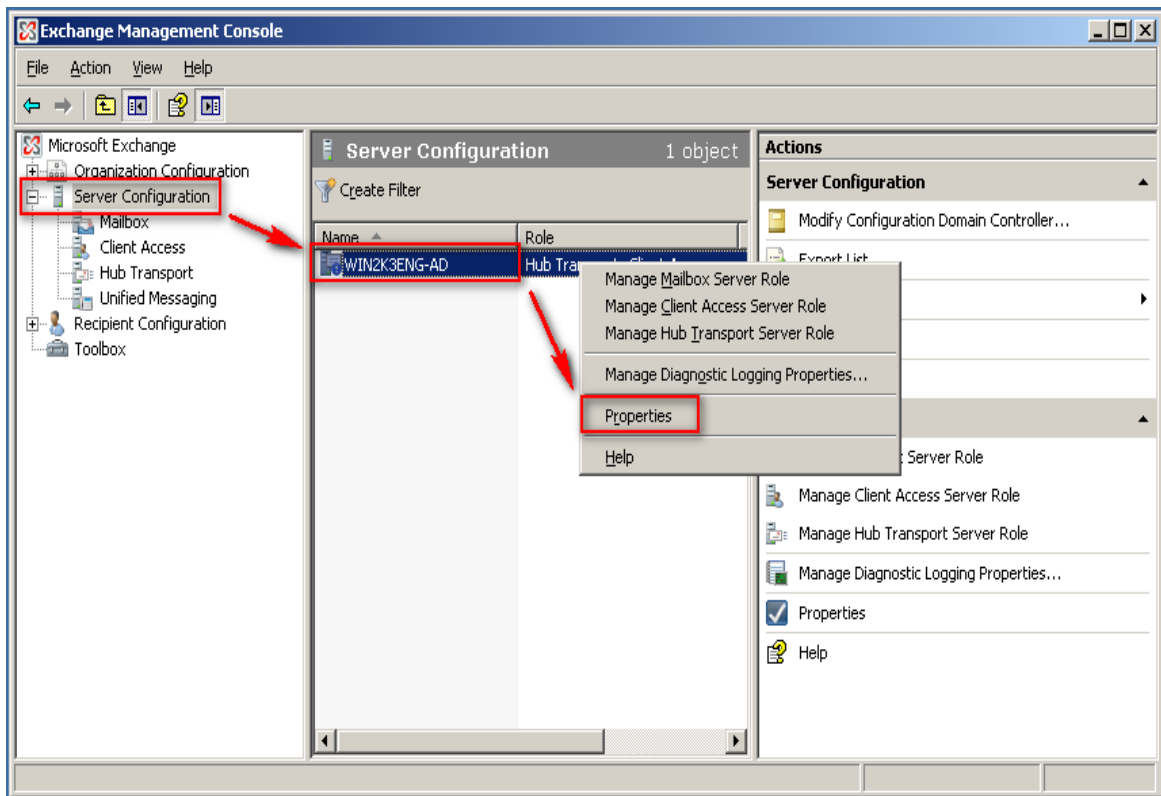
You can set up message tracking log file by either [Exchange Management Console] or [Exchange Management Shell].

## 1. Using Exchange Management Console

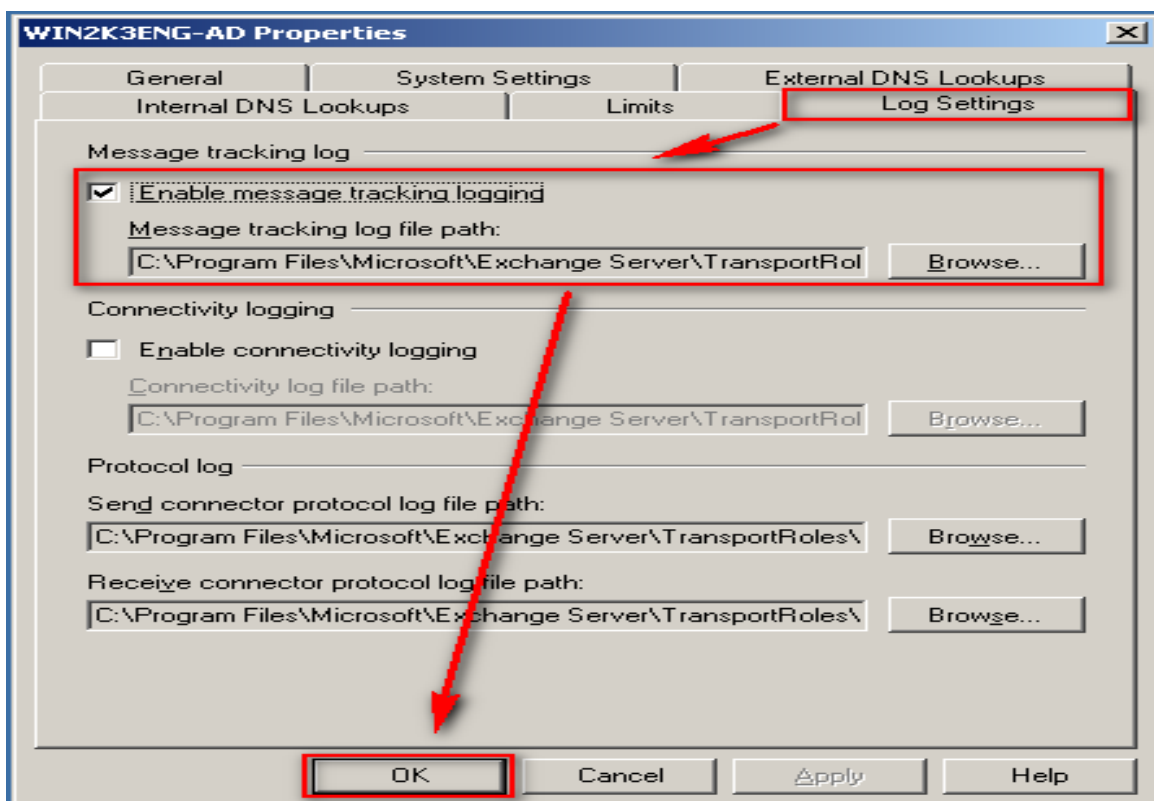
- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All programs] → [ Microsoft Exchange Server 2007 ]  
→ [ Exchange Management Console].



- (3) Click [Server Configuration] → [Exchange Server], here it is "WIN2K3ENG-AD" → Right click → Properties ◦

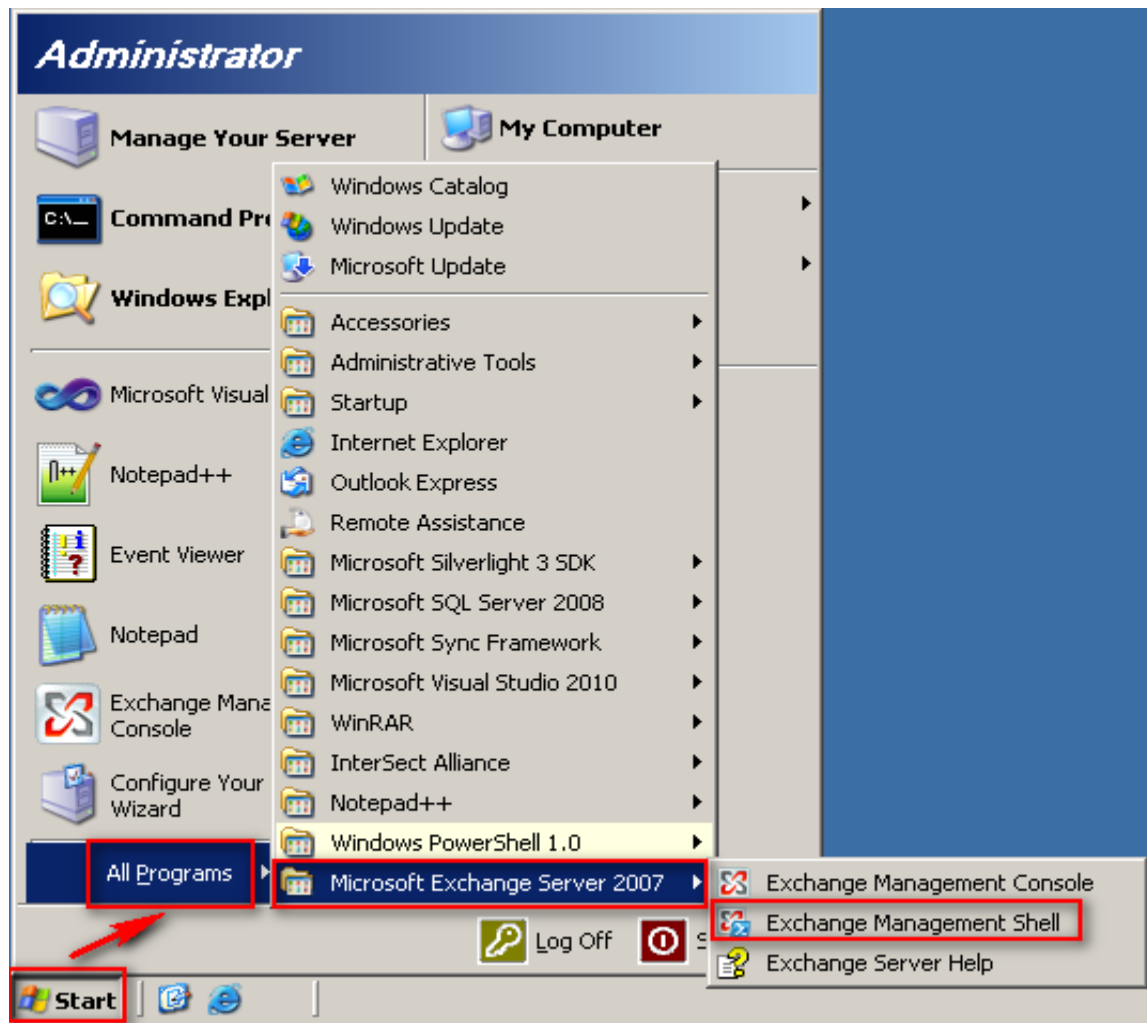


- (4) Click [Log settings] → Check [Enable message tracking logging] → Set the message tracking log file. Default setting is :  
 "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"  
 Click [ OK ], complete.



## 2. Using [ Exchange Management Shell ] To Set Up

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All Programs] → [ Microsoft Exchange Server 2007 ] → [ Exchange Management Shell ].



- (3) Enable message tracking. Type in program:

```
Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath
<LocalFilePath>
```

or

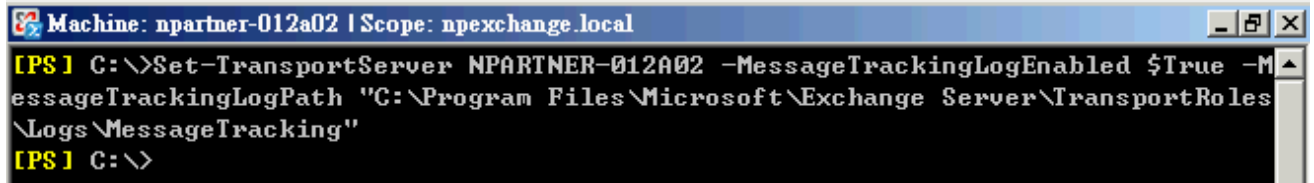
```
Set-MailboxServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath
<LocalFilePath>
```

<ServerIdentity> is the computer name of Exchange Serve, <LocalFilePath> is the path of message tracking,

Default setting is : "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"

In this example we type in:

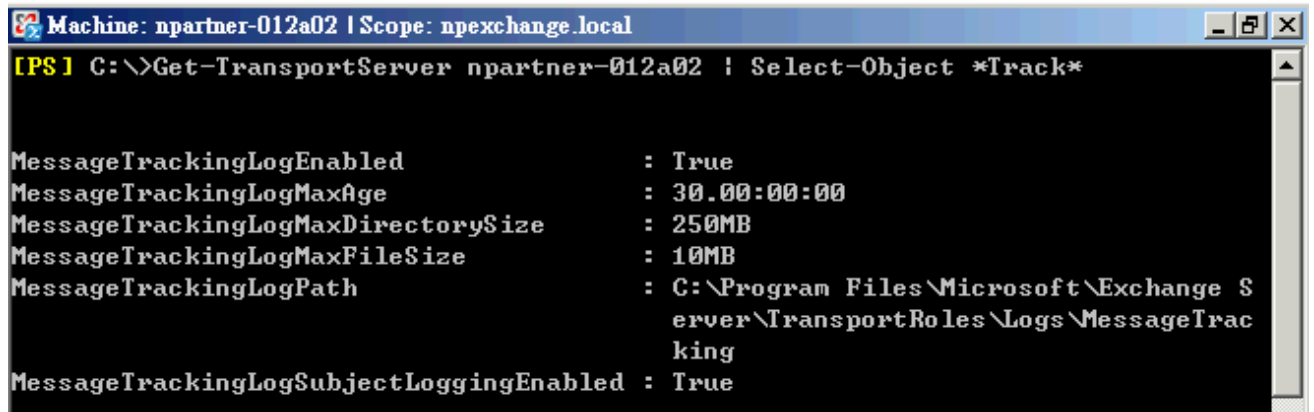
```
Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"
```



```
Machine: npartner-012a02 | Scope: npexchange.local
[PS] C:\>Set-TransportServer NPARTNER-012A02 -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking"
[PS] C:\>
```

(4) Check the setting of message tracking record. Type in program:

```
Get-TransportServer npartner-012a02 | Select-Object *Track*
```



```
Machine: npartner-012a02 | Scope: npexchange.local
[PS] C:\>Get-TransportServer npartner-012a02 | Select-Object *Track*

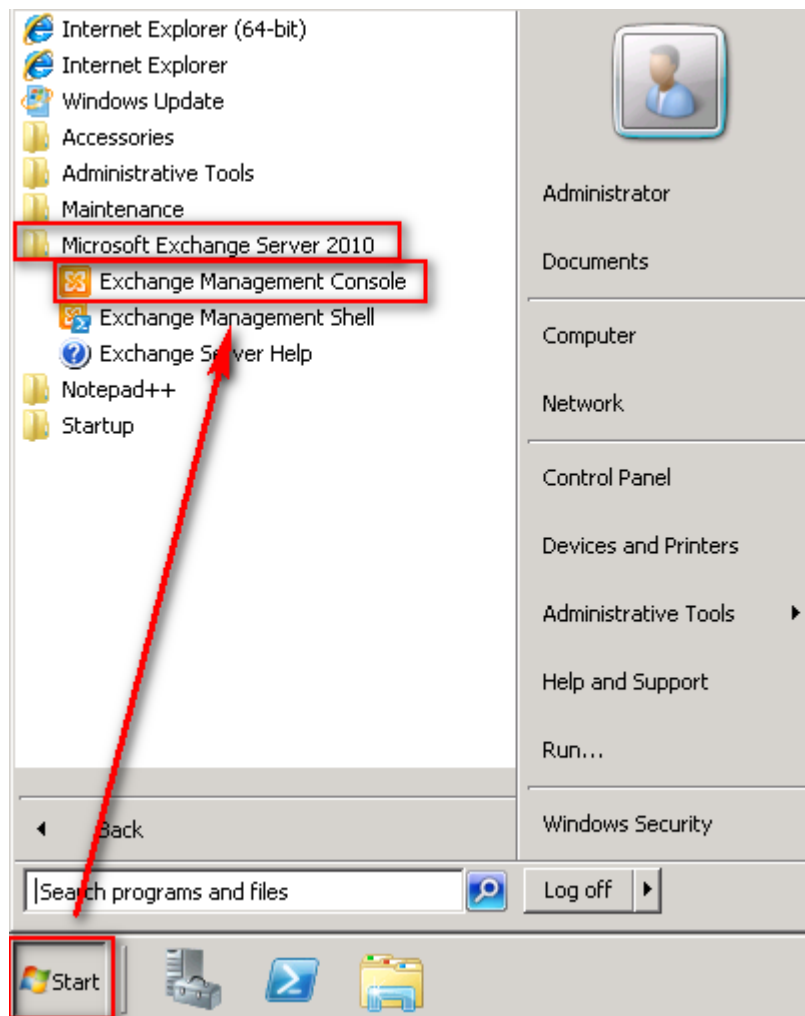
MessageTrackingLogEnabled           : True
MessageTrackingLogMaxAge             : 30.00:00:00
MessageTrackingLogMaxDirectorySize  : 250MB
MessageTrackingLogMaxFileSize       : 10MB
MessageTrackingLogPath               : C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True
```

## 2 Set up Exchange Server 2010 message tracking log

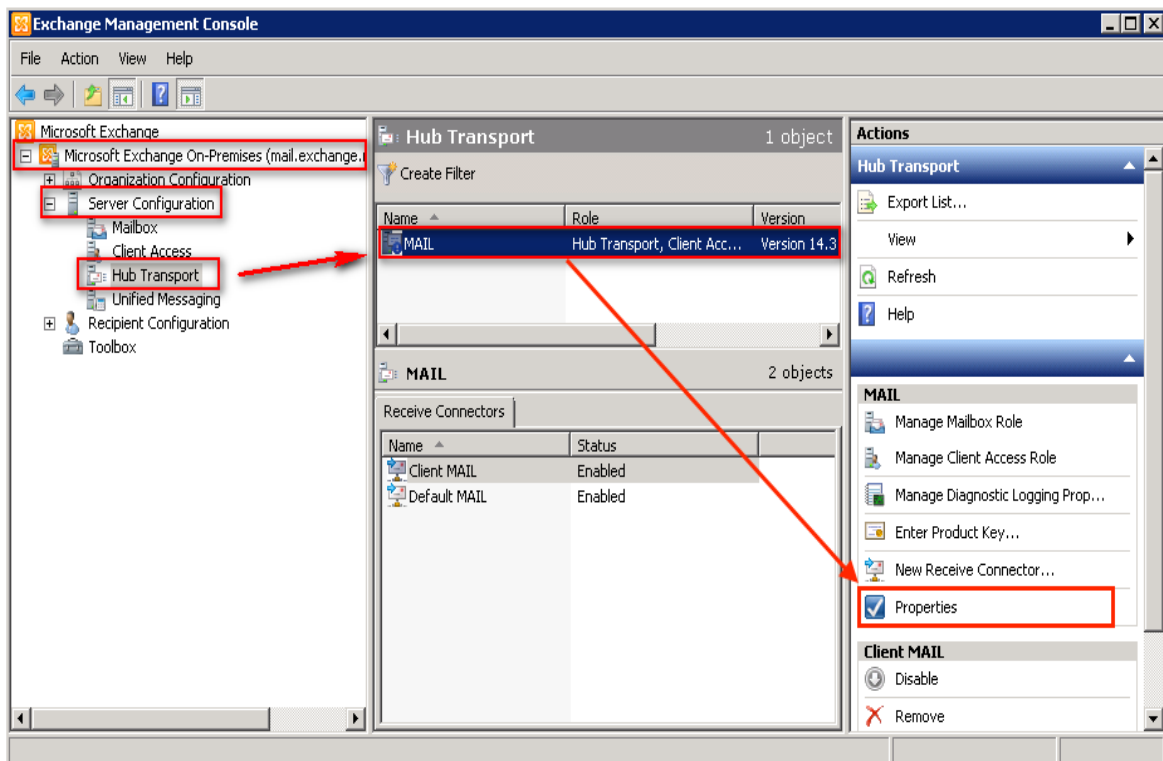
You can set up message tracking log file by either [Exchange Management Console] or [Exchange Management Shell].

### 1. Using Exchange Management Console:

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All programs] → [ Microsoft Exchange Server 2010 ] → [ Exchange Management Console ] ◦



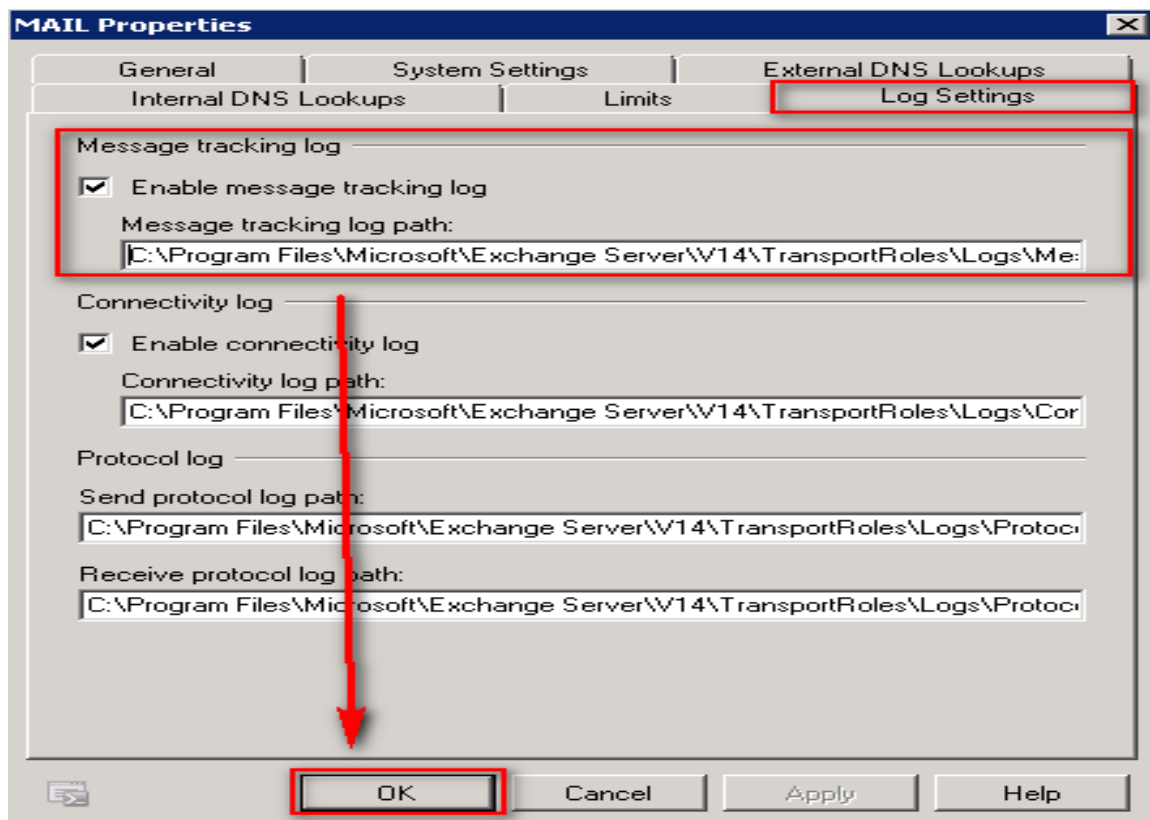
- (3) Click [ Microsoft Exchange On-Premises] → [Server Configuration] → [Hub Transport].  
Click [Exchange Server], here it is "MAIL." Then, click [Properties].



- (4) Click [Log Settings]. Check [Enable message tracking log], type in [Message tracking log path].

Default setting is "C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking".

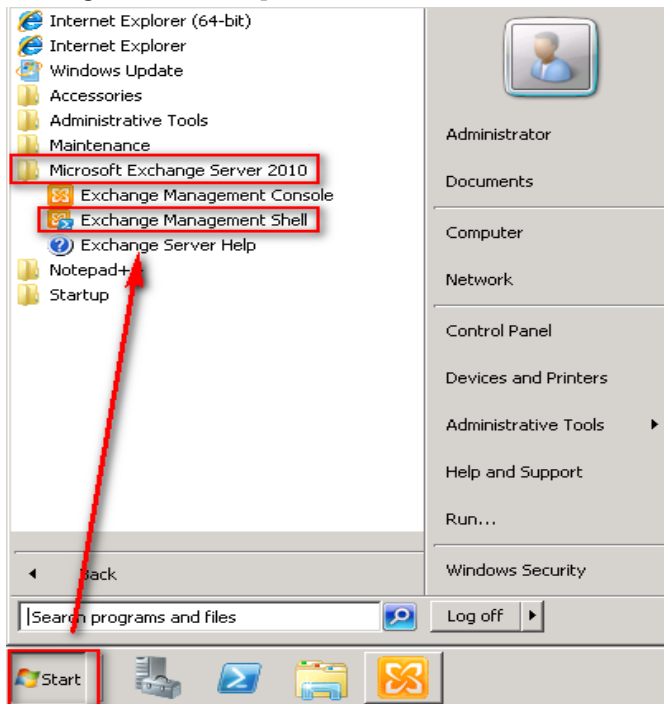
Click [OK], complete.





## 2. Using [Exchange Management Shell]:

- (1) Log in Exchange server as the administrator.
- (2) Click [Start] → [All programs] → [ Microsoft Exchange Server 2010 ] → [ Exchange Management Shell ].



- (3) Enable message tracking. Type in program:

```
Set-TransportServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath <LocalFilePath>
```

or

```
Set-MailboxServer <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath <LocalFilePath>
```

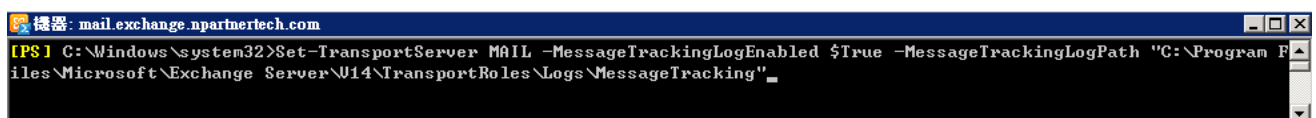
<ServerIdentity> is the computer name of Exchange Server. <LocalFilePath> is the path of message tracking, default setting is

"C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking".

In this example, we type in:

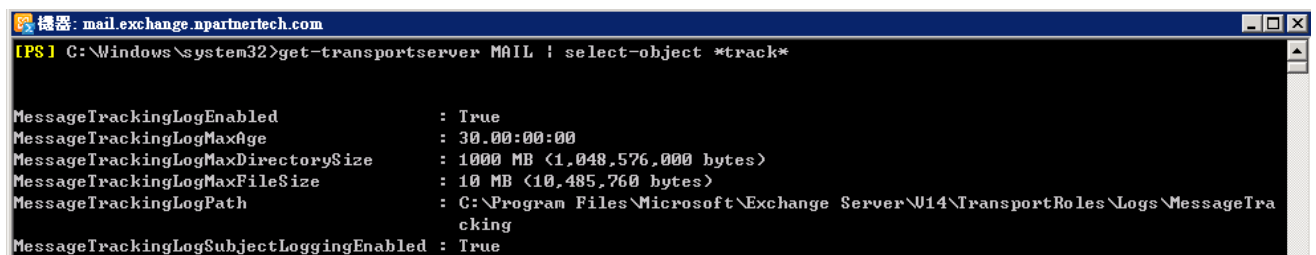
```
Set-TransportServer MAIL -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program
```

```
Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking"
```



- (4) Check the message tracking log deployment. Type in program:

```
Get-TransportServer MAIL | Select-Object *Track*
```



### 3 Set up Exchange Server 2013 message tracking log

You can set up message tracking log file by either [Exchange Admin Center/EAC] or [Exchange Management Shell]

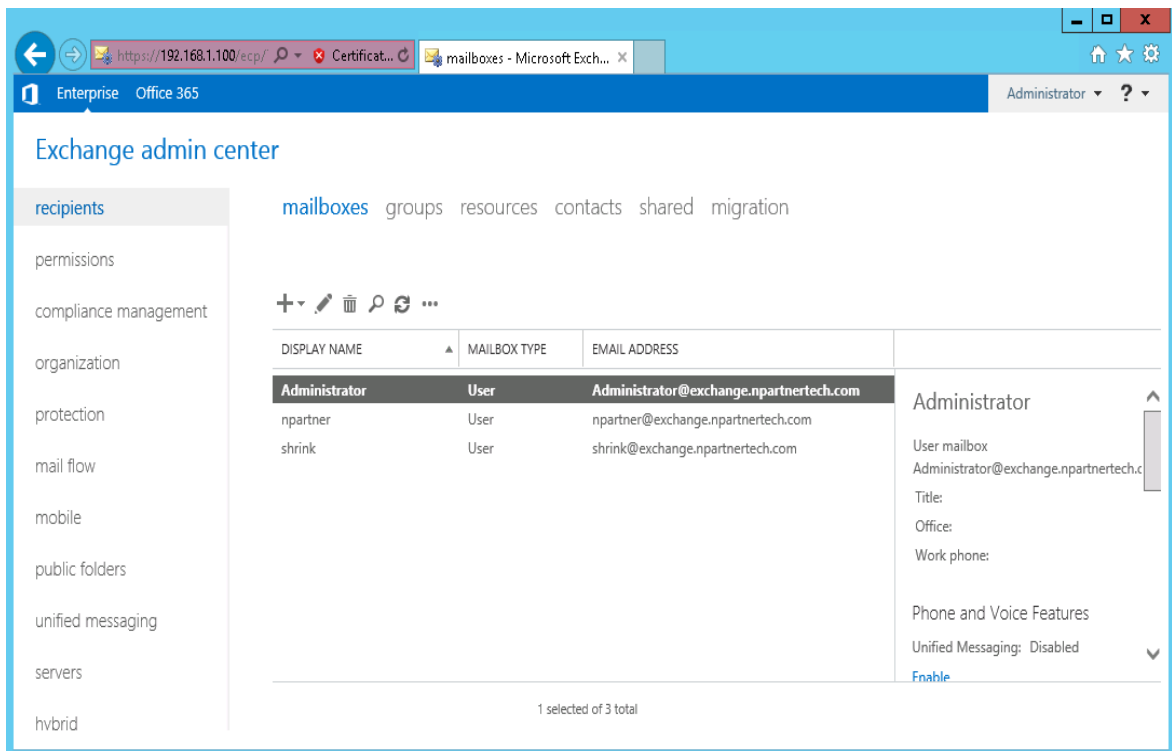
#### 1. Using [ Exchange Admin Center/EAC]:

(1) Start the server.

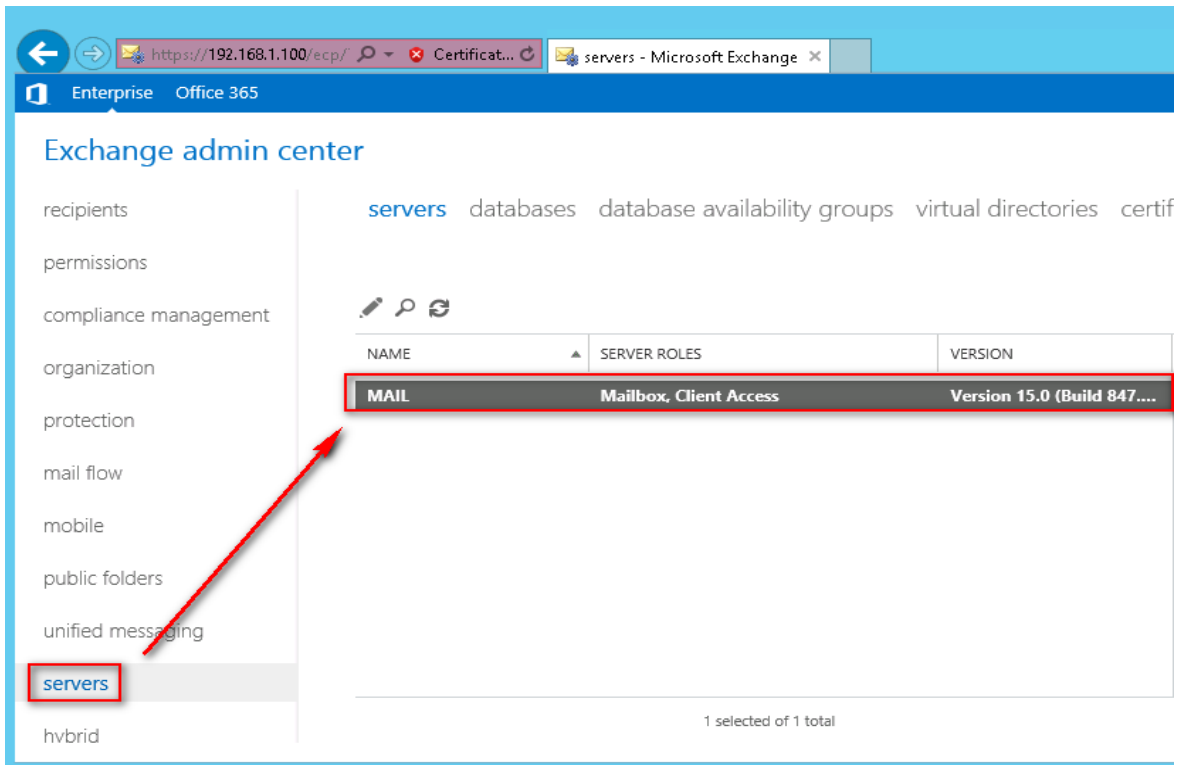
- ▶ Internal URL: “https://<CASServerName or private IP>/ecp”. The internal URL is to access EAC in the organization firewall.
- ▶ External URL: “https://<MailHostName or public IP>/ecp”. The external URL is to access EAC outside the organization firewall.

**Here we type in URL: “https://192.168.2.71/ecp”, to connect Exchange Admin Center.**

(2) Type in the Exchange Server administrator and password in the login webpage of Exchange Admin Center(EAC).



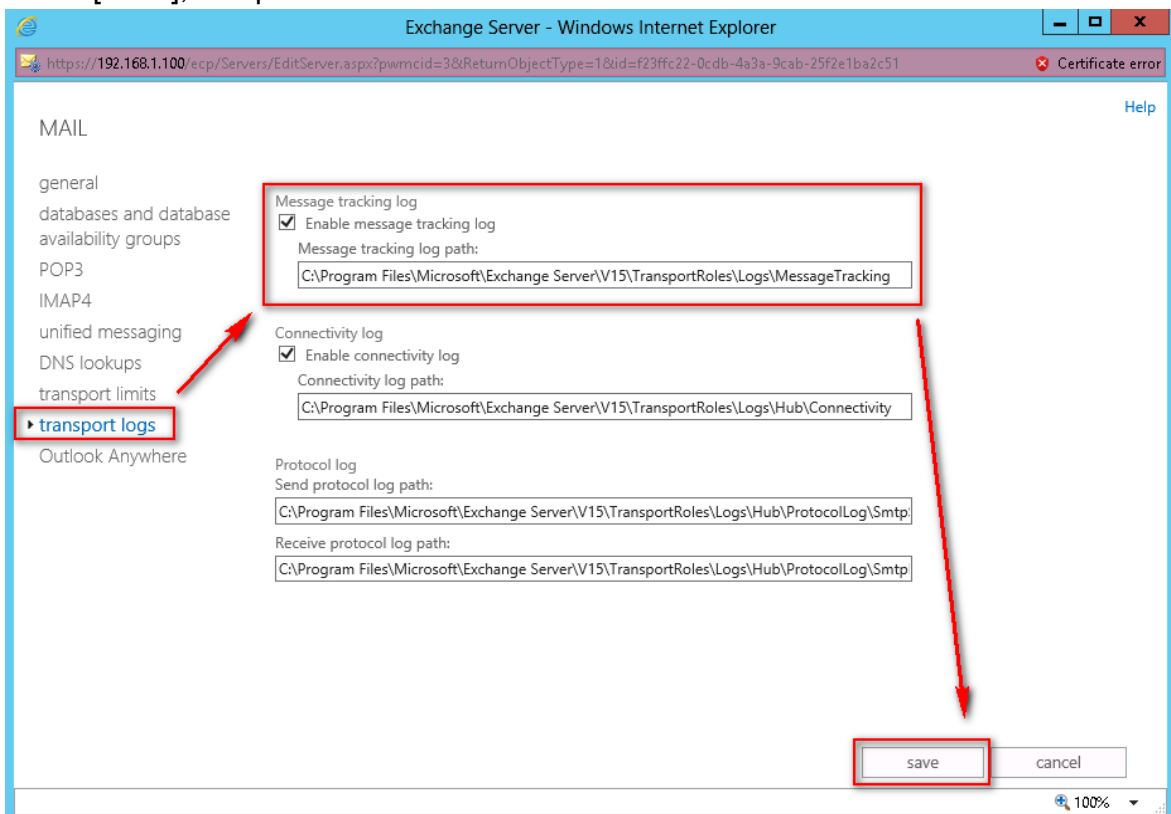
- (3) Click [Server]. Double click Exchange Server. Here we double click "MAIL".



- (4) Click [transport logs] → Check [Enable message tracking log]. Set the message tracking log path. Exchange 2013 default setting is

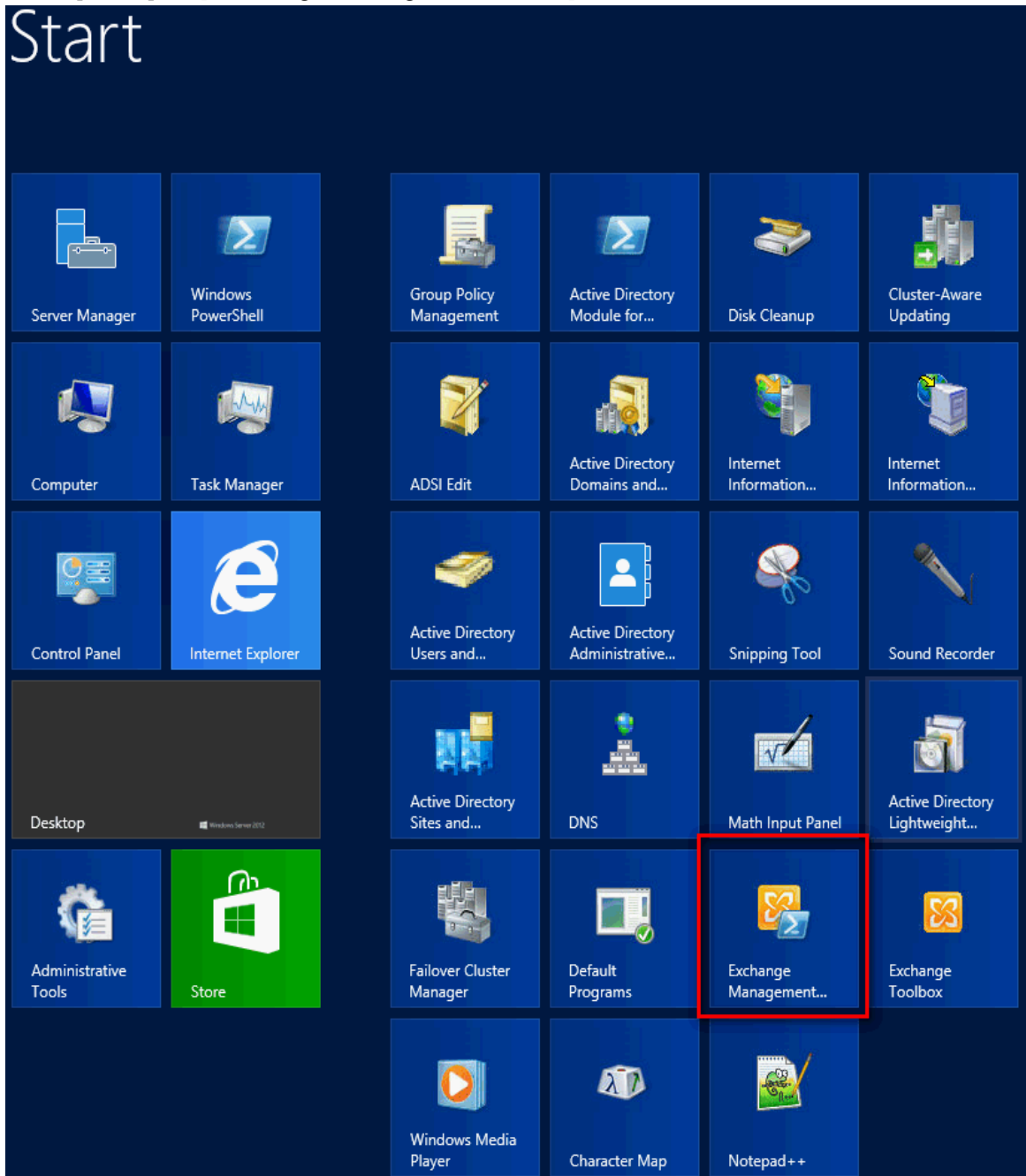
"C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking".

Click [Save], complete.



## 2. Using [ Exchange Management Shell]:

- (1) Log in Exchange server as the administrator.
- (2) Click [Start ] → [Exchange Management Shell ].



- (3) Enable message tracking. Type in program:

```
Set-TransportService <ServerIdentity> -MessageTrackingLogEnabled $True -MessageTrackingLogPath <LocalFilePath>
```

<ServerIdentity> is the computer name of Exchange Server. <LocalFilePath> is the message Tracking path, default setting is

"C:\Program Files\Microsoft\Exchange Server\ V15\TransportRoles \Logs\MessageTracking".

Here we type in:

```
Set-TransportService win2012ad -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking"
```

```
Machine: WIN2012AD.win2012cht.local
[PS] C:\Windows\system32>Set-TransportService win2012ad -MessageTrackingLogEnabled $True -MessageTrackingLogPath "C:\Program Files\Microsoft\Exchange Server\W15\TransportRoles\Logs\MessageTracking"
[PS] C:\Windows\system32>
Microsoft New Phonetic 𐄂 :
```

(4) Check the message tracking log setting.

Type in program:

```
Get-TransportService win2012ad | Select-Object *Track*
```

```
Machine: WIN2012AD.win2012cht.local
[PS] C:\Windows\system32>Get-TransportService win2012ad | select-object *Track*
MessageTrackingLogEnabled           : True
MessageTrackingLogMaxAge             : 30.00:00:00
MessageTrackingLogMaxDirectorySize  : 1000 MB (1,048,576,000 bytes)
MessageTrackingLogMaxFileSize       : 10 MB (10,485,760 bytes)
MessageTrackingLogPath               : C:\Program Files\Microsoft\Exchange Server\W15\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled : True
[PS] C:\Windows\system32>
Microsoft New Phonetic 𐄂 :
```

## 4 Set up NXLOG

(1) Log in Windows Server as Administrator.

(2) Download NXLOG: go to <http://sourceforge.net/projects/nxlog-ce/files/>, download {nxlog-ce-x.x.x.msi}.

(3) Install NXLOG: Click {nxlog-ce-x.x.x.msi}, install NXLOG.

Note:

Install NXLOG on 32 bit operating system at " C:\Program Files\nxlog\conf\nxlog.conf "

Install NXLOG on 64 bit operating system at "C:\Program Files (x86)\nxlog\conf\nxlog.conf "

#### (4) Set Up NXLOG:

- (a) Download NXLOG Exchange setting profile:

[http://www.npartnertech.com/download/tech/nxlog\\_exchange.conf](http://www.npartnertech.com/download/tech/nxlog_exchange.conf)

- (b) Edit NXLOG profile "C:\Program Files (x86)\nxlog\conf\nxlog.conf". Copy NXLOG Exchange setting profile contents: nxlog\_exchange.conf. Paste it and overwrite nxlog.conf.

```
#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log
<Extension syslog>
    Module      xm_syslog
</Extension>
define BASEDIR C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
<Input in_exchange>
    Module      im_file
    File        '%BASEDIR%\MSGTRK20??????.LOG'
    SavePos     TRUE
</Input>
<Output out_exchange>
    Module      om_udp
    Host        192.168.2.64
    Port        514
    Exec        $SyslogFacilityValue = 2;
    Exec        $SourceName = 'Exchange';
    Exec        to_syslog_bsd();
</Output>
<Route exchange>
    Path        in_exchange => out_exchange
</Route>
```

Please choose the correct install path of NXLOG about green words.

**The environment of this example is a 64 bit system.**

Choose "define ROOT C:\Program Files (x86)\nxlog".

About red words "define BASEDIR \$dir", please type in the message tracking log path of Exchange Server in \$dir.

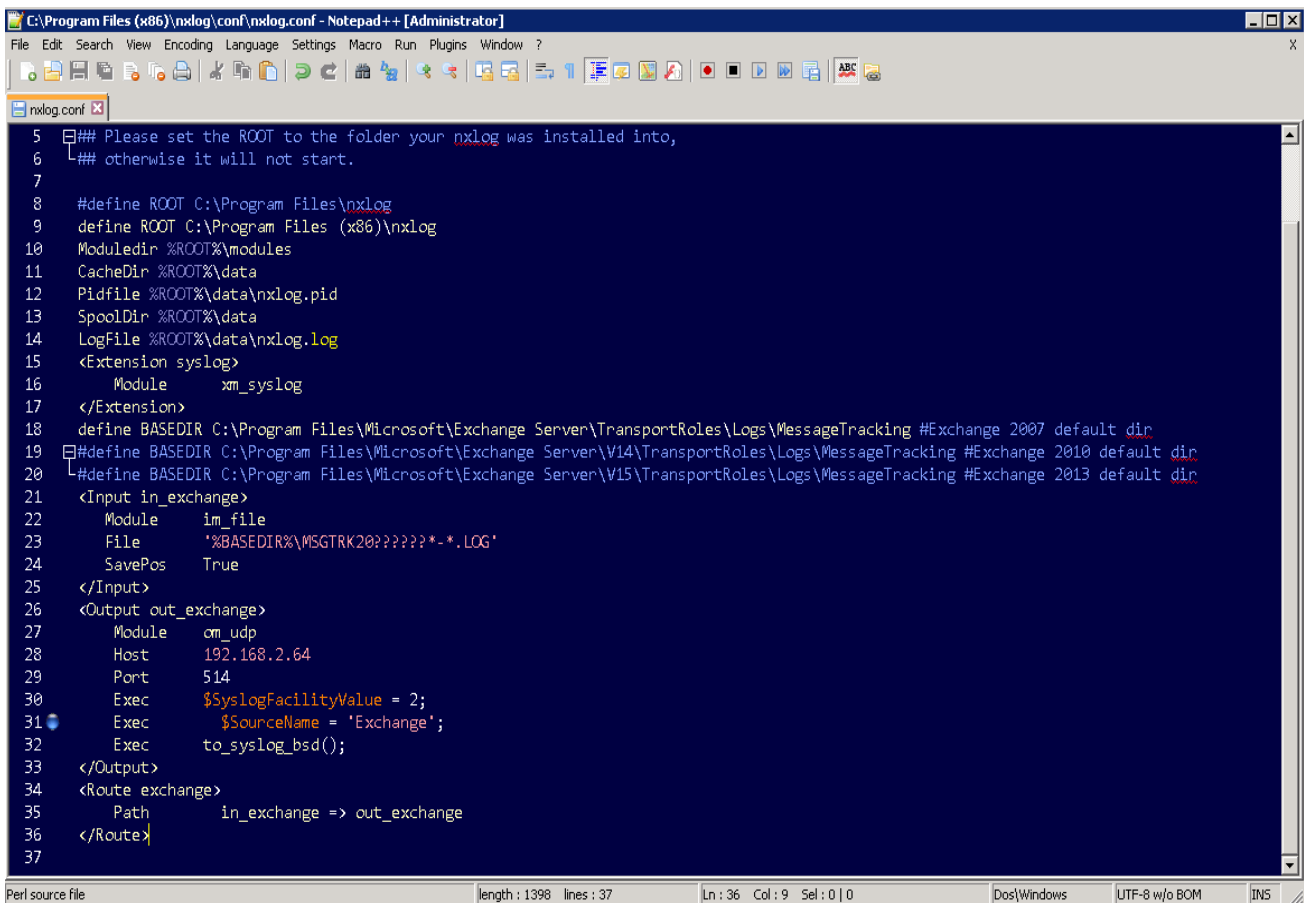
**This example we use Exchange 2007**

The default path is "C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking".

About red words "Host \$N\_Reporter\_IP", please setting '\$N-Reporter\_IP' to real N-Reporter IP.

In this example the IP is 192.168.2.64.

For example :



```

5  ### Please set the ROOT to the folder your nxlog was installed into,
6  ### otherwise it will not start.
7
8  #define ROOT C:\Program Files\nxlog
9  define ROOT C:\Program Files (x86)\nxlog
10 Moduledir %ROOT%\modules
11 CacheDir %ROOT%\data
12 Pidfile %ROOT%\data\nxlog.pid
13 SpoolDir %ROOT%\data
14 LogFile %ROOT%\data\nxlog.log
15 <Extension syslog>
16     Module      xm_syslog
17 </Extension>
18 define BASEDIR C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking #Exchange 2007 default dir
19 #define BASEDIR C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking #Exchange 2010 default dir
20 #define BASEDIR C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking #Exchange 2013 default dir
21 <Input in_exchange>
22     Module      im_file
23     File        '%BASEDIR%\MSGTRK20?????*.LOG'
24     SavePos     True
25 </Input>
26 <Output out_exchange>
27     Module      om_udp
28     Host        192.168.2.64
29     Port        514
30     Exec        $SyslogFacilityValue = 2;
31     Exec        $SourceName = 'Exchange';
32     Exec        to_syslog_bsd();
33 </Output>
34 <Route exchange>
35     Path        in_exchange => out_exchange
36 </Route>
37

```

### (3) Start NXLOG :

a. Start NXLOG by using [Command Prompt] or b. [Services]

a. Click [Start] → [All programs] → [Accessories] → Right click [Command Prompt] → Click [Run as administrator], run as system administrator.

Type in command prompt:

```
net stop nxlog
```

```
net start nxlog
```

b. Click [Start] → [All programs] → [Administrative Tools] → [Services], right click [ nxlog ] → Click [Start] or [Restart].

### (4) Check whether does NXLOG runs normally:

Check the log file of NXLOG "C:\Program Files (x86)\nxlog\data\nxlog.log". If it does not show Error, means it is running normally.

**Technical Support :**

Email: [support@npartnertech.com](mailto:support@npartnertech.com)

Skype : [support@npartnertech.com](mailto:support@npartnertech.com)

**Sales Information :**

Email: [sales@npartnertech.com](mailto:sales@npartnertech.com)

