N-Partner

How to Configure MS Exchange Message Tracking Logs

V020

2025/09/18

N-Reporter N-Cloud N-Probe N-Robot

Copyright Declaration

N- Copyright © N-Partner Technologies Co. All Rights reserved. Without written authorization from N-Partner Technologies Co., anyone may not in any way copy, plagiarize or translate this manual. The system is keeping upgraded; therefore, N-Partner reserves the right to revise it without informing.

Registered Trademark

All company products, names and trademarks mentioned in this manual belongs to their legally registered organizations.

Contents

Preface

This document describes how N-Reporter users can configure MS exchange message tracking logs using the open-source tool NXLog.

NXLog converts MS exchange message tracking logs into syslog format and forwards them to N-Reporter for normalization, auditing, and analysis.

This document applies to MS Exchange Server 2007, 2010, 2013, 2016 and 2019.

References

Message Tracking Logs in Exchange Server:

https://docs.microsoft.com/en-us/exchange/mail-flow/transport-logs/message-tracking?view=exchserver-2019

Mailbox Audit Logging in Exchange Server:

https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mailbox-audit-logging/mailbox-audit-logging?view=exchserver-2019

Audit Policy Recommendations:

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

W3C Logging:

https://docs.microsoft.com/en-us/windows/win32/http/w3c-logging

Note: This document is provided solely as a reference for configuring log output. It is recommended that you contact the device or software vendor for assistance with the appropriate log export methods.

1. NXLog

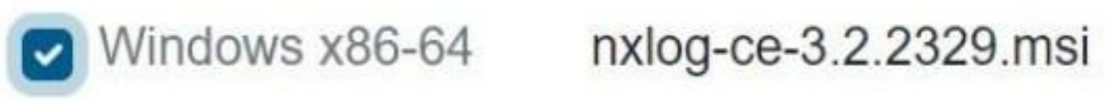
1.1 NXLog Installation

(1) Download NXLog CE (Community Edition)

Please go to: https://nxlog.co/products/nxlog-community-edition/download

Download the latest version of nxlog-ce-x.x.xxxx.msi.

Example Here: **nxlog-ce-3.2.2329.msi**



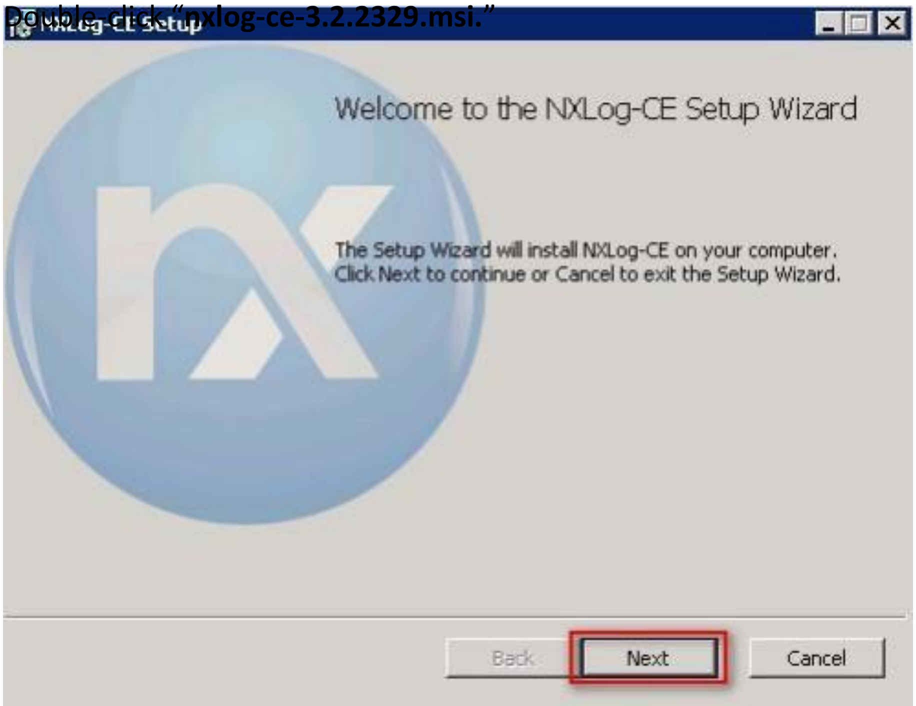
☑ Windows x86-64 nxlog-ce-3.2.2329.msi

Note: If you require the 32-bit version of NXLog, please contact our support team.

(2) Install NXLog

<2.1> For Windows Server **2008** or later:

Double-click "**nxlog-ce-3.2.2329.msi.**"

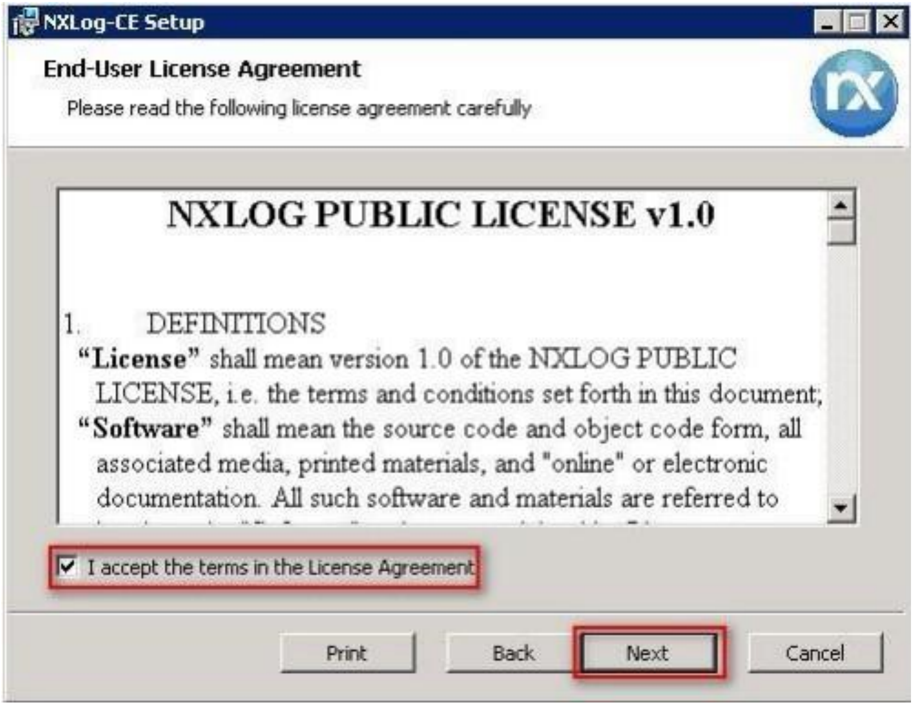


NXLog-CE Setup

Welcome to the NXLog-CE Setup Wizard

The Setup Wizard will install NXLog-CE on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

(3) Select "I accept the terms in the License Agreement," then click "Next."



NXLog-CE Setup

End-User License Agreement

Please read the following license agreement carefully

NXLOG PUBLIC LICENSE v1.0

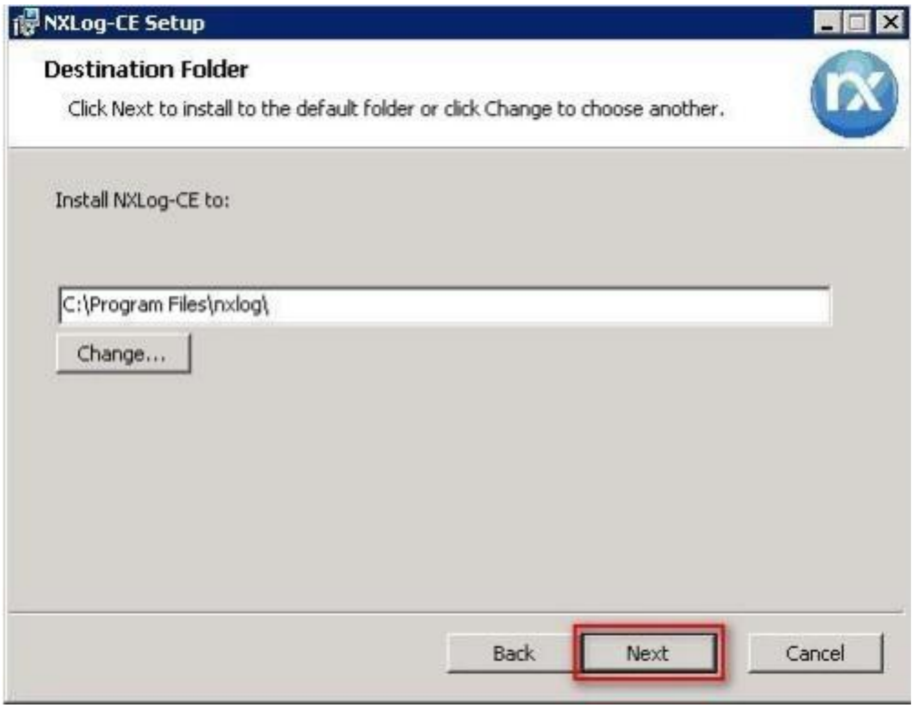
1. DEFINITIONS

"**License**" shall mean version 1.0 of the NXLOG PUBLIC LICENSE, i.e. the terms and conditions set forth in this document;

"**Software**" shall mean the source code and object code form, all associated media, printed materials, and "online" or electronic documentation. All such software and materials are referred to

☑ I accept the terms in the License Agreement

(4) Click "Next." (The default installation path is (C:\Program Files\nxlog\).



NXLog-CE Setup

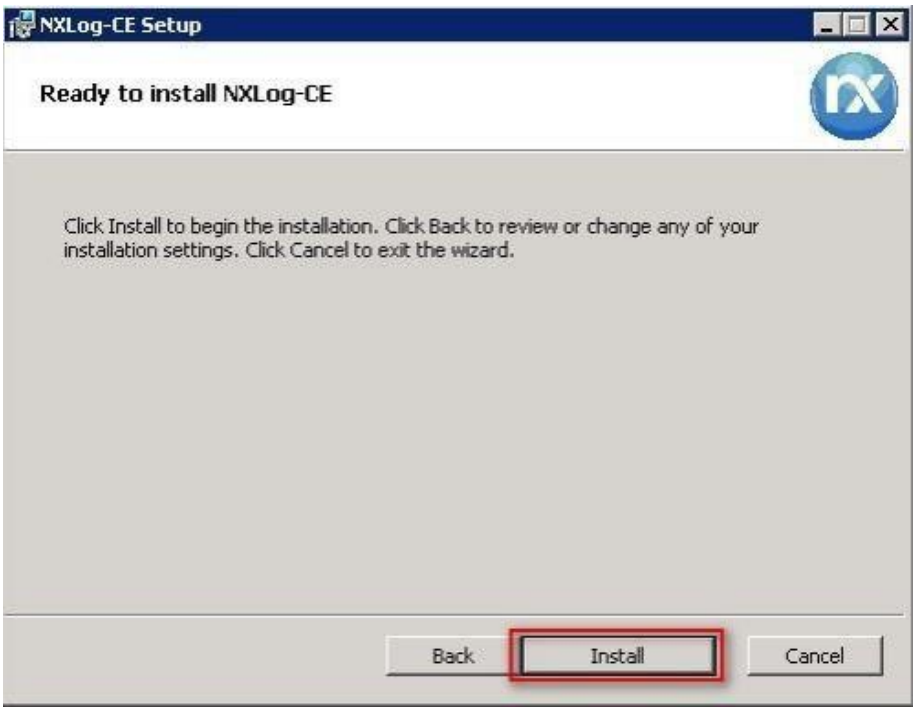
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install NXLog-CE to:

C:\Program Files\nxlog\

(5) Click “Install.”

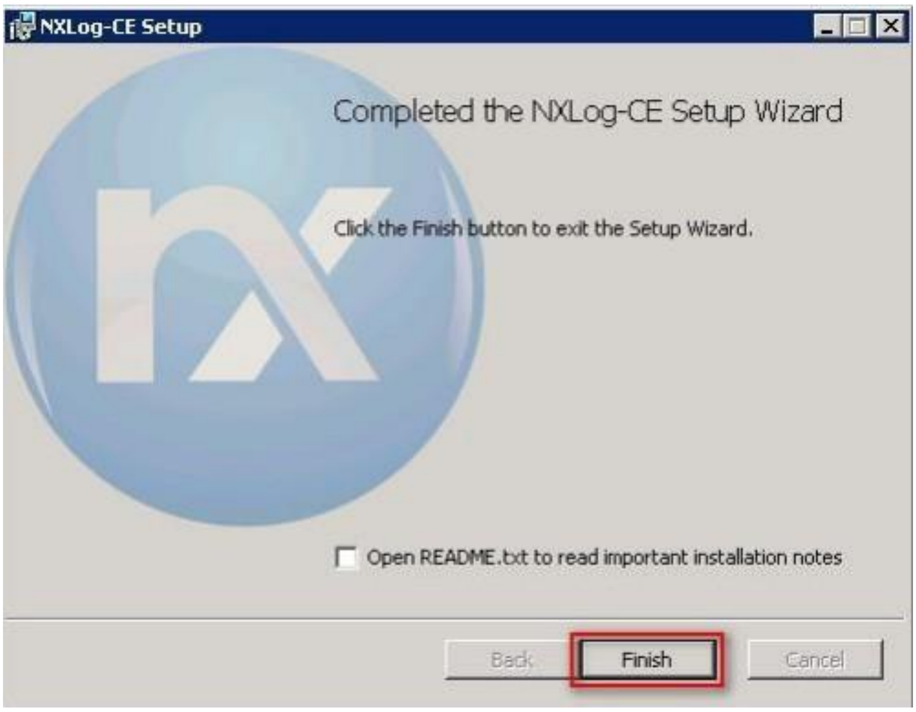


NXLog-CE Setup

Ready to install NXLog-CE

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

(6) Click “Finish.”



NXLog-CE Setup

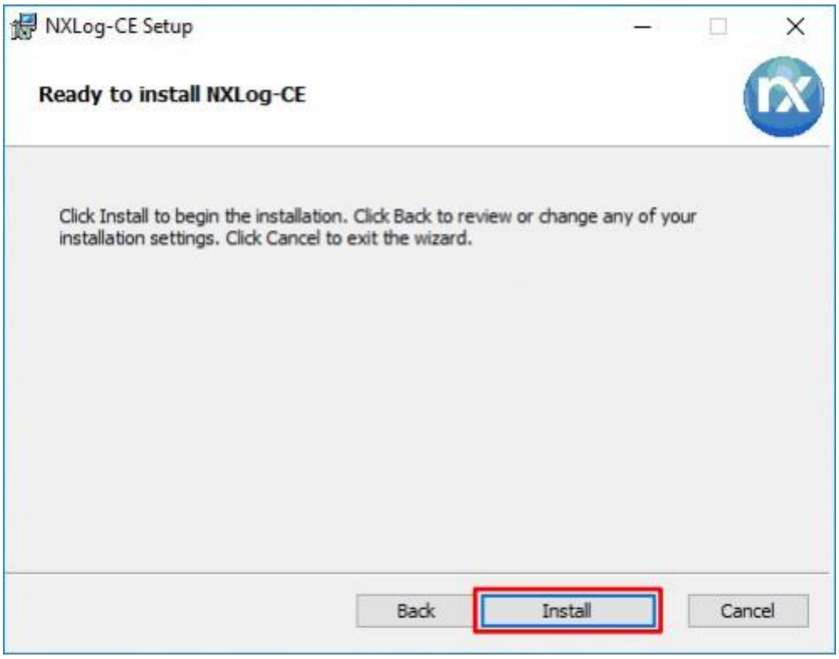
Completed the NXLog-CE Setup Wizard

Click the Finish button to exit the Setup Wizard.

□ Open README.txt to read important installation notes

<2.2> For Windows Server **2003**:

Download File: **nxlog-ce-3.2.2329.msi.** → Select “Install” and proceed until the installation completes. → Click “Finish” to exit.



Ready to install NXLog-CE

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

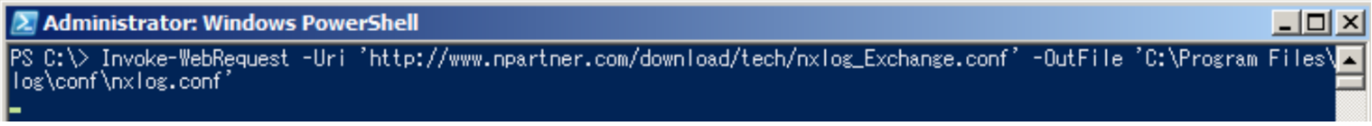
1.2 Download NXLog Configuration File

(1) Open “Command Prompt.”

(2) Download the “NXLog Windows 2003 File” and overwrite the existing NXLog configuration file in the Windows system.

Download link: https://www.npartner.com/download/tech/nxlog_Exchange.conf

```
PS C:\> Invoke-WebRequest -Uri'http://www.npartner.com/download/tech/nxlog_Exchange.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'
```



```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_Exchange.conf' -OutFile 'C:\Program Files\
log\conf\nxlog.conf'
```

Note: The example above is for a 64-bit operating system. For a 32-bit operating system, replace the highlighted text with: 'C:**\ Program Files (x86)**\nxlog\conf\nxlog.conf'

1.3 NXLog Configuration

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
define IISLog C:\inetpub\logs\LogFiles
define ROOT C:\Program Files\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR    %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile    %LOGFILE%

Moduledir %ROOT%\modules
CacheDir    %ROOT%\data
Pidfile      %ROOT%\data\nxlog.pid
SpoolDir    %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
    Module xm_syslog
</Extension>

## For Exchange Message Tracking log file use the following:
<Input in_maillog>
    Module im_file
    File '%MailLog%\MSGTRK*.LOG'
    ReadFromLast TRUE
    SavePos TRUE
</Input>

<Output out_maillog>
    Module om_udp
    Host %NCloud%
    Port 514
    Exec $SyslogFacilityValue = 2;
```

```
        Exec $SourceName = 'Exchange';

        Exec to_syslog_bsd();

    </Output>


    <Route maillog>

        Path in_maillog => out_maillog

    </Route>


    ## For Windows Event log use the following:

    <Input in_eventlog>

        Module im_msvistalog

        ReadFromLast TRUE

        SavePos TRUE

        Query    <QueryList> \

                        <Query Id="0"> \

                                <Select Path="Security">*[System[(EventID=4624 or EventID=4625 or EventID=4626 or EventID=4627 or
EventID=4634 or EventID=4646 or EventID=4647 or EventID=4648 or EventID=4649 or EventID=4672 or EventID=4675)]]</Select> \

                                <Select Path="Security">*[System[(EventID=4778 or EventID=4779 or EventID=4800 or EventID=4801 or
EventID=4802 or EventID=4803 or EventID=4964 or EventID=4976 or EventID=5378 or EventID=5632 or EventID=5633)]]</Select> \

                                <Select Path="Security">*[System[(EventID=4768 or EventID=4769 or EventID=4770 or EventID=4771 or
EventID=4772 or EventID=4773 or EventID=4774 or EventID=4775 or EventID=4776 or EventID=4777 or EventID=4820)]]</Select> \

                                <Select Path="Security">*[System[(EventID=4720 or EventID=4722 or EventID=4723 or EventID=4724 or
EventID=4725 or EventID=4726 or EventID=4727 or EventID=4731 or EventID=4732 or EventID=4733 or EventID=4734)]]</Select> \

                                <Select Path="Security">*[System[(EventID=4735 or EventID=4738 or EventID=4739 or EventID=4740 or
EventID=4749 or EventID=4750 or EventID=4751 or EventID=4752 or EventID=4753 or EventID=4764 or EventID=4765)]]</Select> \

                                <Select Path="Security">*[System[(EventID=4766 or EventID=4767 or EventID=4780 or EventID=4781 or
EventID=4782 or EventID=4793 or EventID=4794 or EventID=4797 or EventID=4798 or EventID=4799 or EventID=5376 or
EventID=5377)]]</Select> \

                                <Select Path="Security">*[System[(EventID=4608 or EventID=4610 or EventID=4611 or EventID=4612 or
EventID=4614 or EventID=4615 or EventID=4616 or EventID=4618 or EventID=4621 or EventID=4622 or EventID=4697)]]</Select> \

                                <Select Path="Security">*[System[(EventID=5024 or EventID=5025 or EventID=5027 or EventID=5028 or
EventID=5029 or EventID=5030 or EventID=5032 or EventID=5033 or EventID=5034 or EventID=5035 or EventID=5037)]]</Select> \

                                <Select Path="Security">*[System[(EventID=5038 or EventID=5056 or EventID=5058 or EventID=5059 or
EventID=5061 or EventID=5890 or EventID=6281 or EventID=6400 or EventID=6401 or EventID=6402 or EventID=6403)]]</Select> \

                                <Select Path="Security">*[System[(EventID=6404 or EventID=6405 or EventID=6406 or EventID=6407 or
EventID=6408 or EventID=6409 or EventID=6410)]]</Select> \
                        </Query> \
                    </QueryList>
    </Input>

    <Output out_eventlog>
        Module om_udp
        Host %NCloud%
        Port 514
        Exec $SyslogFacilityValue = 17;
        Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
        Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
                        else if ($EventType == 'WARNING')    { $SyslogSeverityValue = 4; } \
                        else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')    { $SyslogSeverityValue = 5; }
        Exec to_syslog_bsd();
    </Output>

    <Route eventlog>
        Path in_eventlog => out_eventlog
    </Route>

    ## For Microsoft IIS(Internet Information Server) log file use the following:
    <Input in_iislog>
        Module im_file
        File '%IISLog%\u_ex*.log'
        ReadFromLast TRUE
        Recursive TRUE
        SavePos TRUE
    </Input>

    <Output out_iislog>
        Module om_udp
        Host %NCloud%
        Port 514
        Exec $SyslogFacilityValue = 22;
        Exec $raw_event = "IIS [info]: " + $raw_event ;
        Exec to_syslog_bsd();
```

```
</Output>


<Route iislog>
    Path in_iislog => out_iislog
</Route>
```

Enter the N-Cloud system IP address in the blue text section.

```
define NCloud 192.168.8.4
```

This example is based on a 64-bit operating system.

For a 32-bit operating system, use the following setting instead:

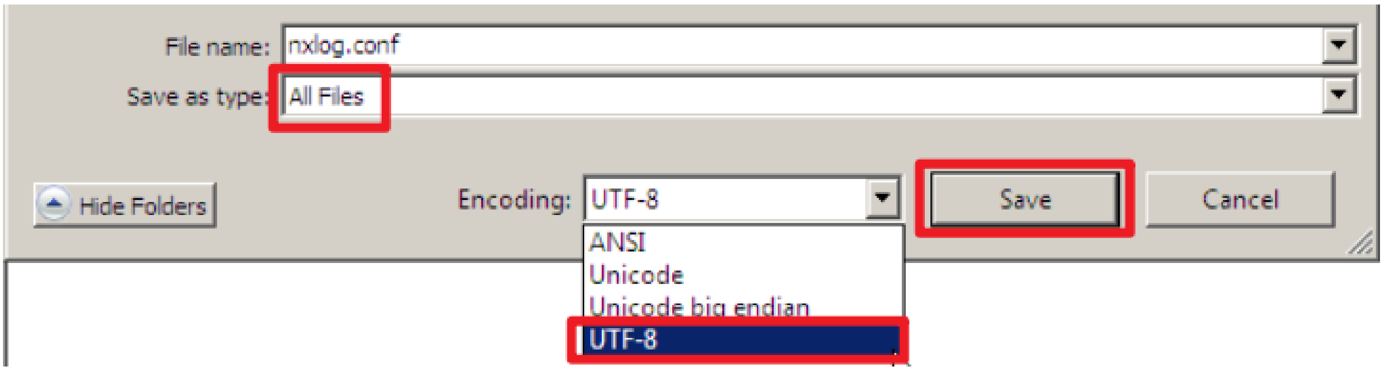
```
define ROOT C:\Program Files (x86)\nxlog
```

Enter the exchange message tracking log paths in blue text section:

```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

Enter the IIS (W3C) log paths in blue text section:

```
define IISpath C:\inetpub\logs\LogFiles
```



File name: nxlog.conf

Save as type: All Files

Encoding: UTF-8

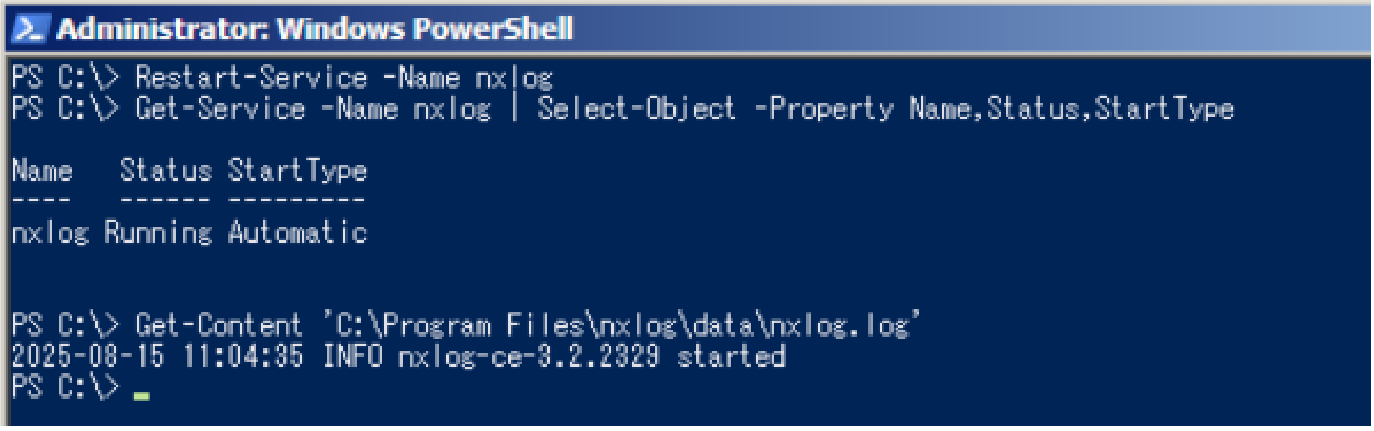
Note: After modifying the configuration file, save it as a new file to overwrite the original. For Save as type, select “All Files (*.*)”. For Encoding, select UTF-8 to avoid encoding errors that could prevent the service from starting.

1.4 Starting the NXLog Service

(1) Open “Windows Powershell.”

(2) Restart the NXLog service, verify that it is running, and ensure there are no error messages:

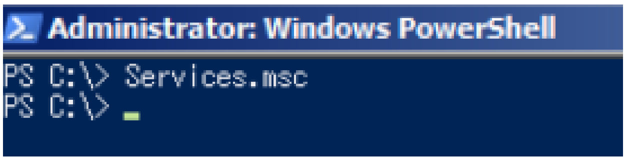
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\ Program Files\ nxlog\data\nxlog.log'
```



```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

Name   Status  StartType
----   ------  ---------
nxlog  Running Automatic


PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
2025-08-15 11:04:35 INFO nxlog-ce-3.2.2329 started
PS C:\> _
```

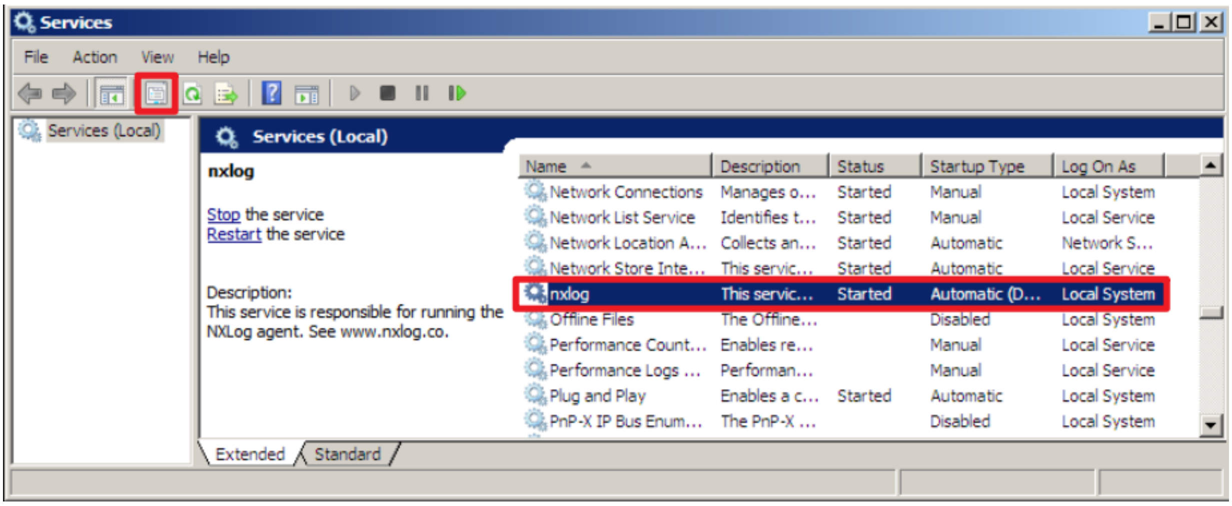
(3) Enter the command below to open the **Services** console:

```
PS C:\> Services.msc
```



```
PS C:\> Services.msc
PS C:\> _
```

(4) Open the NXLog service properties: select “NXLog” →Click “Properties.”



Services (Local)

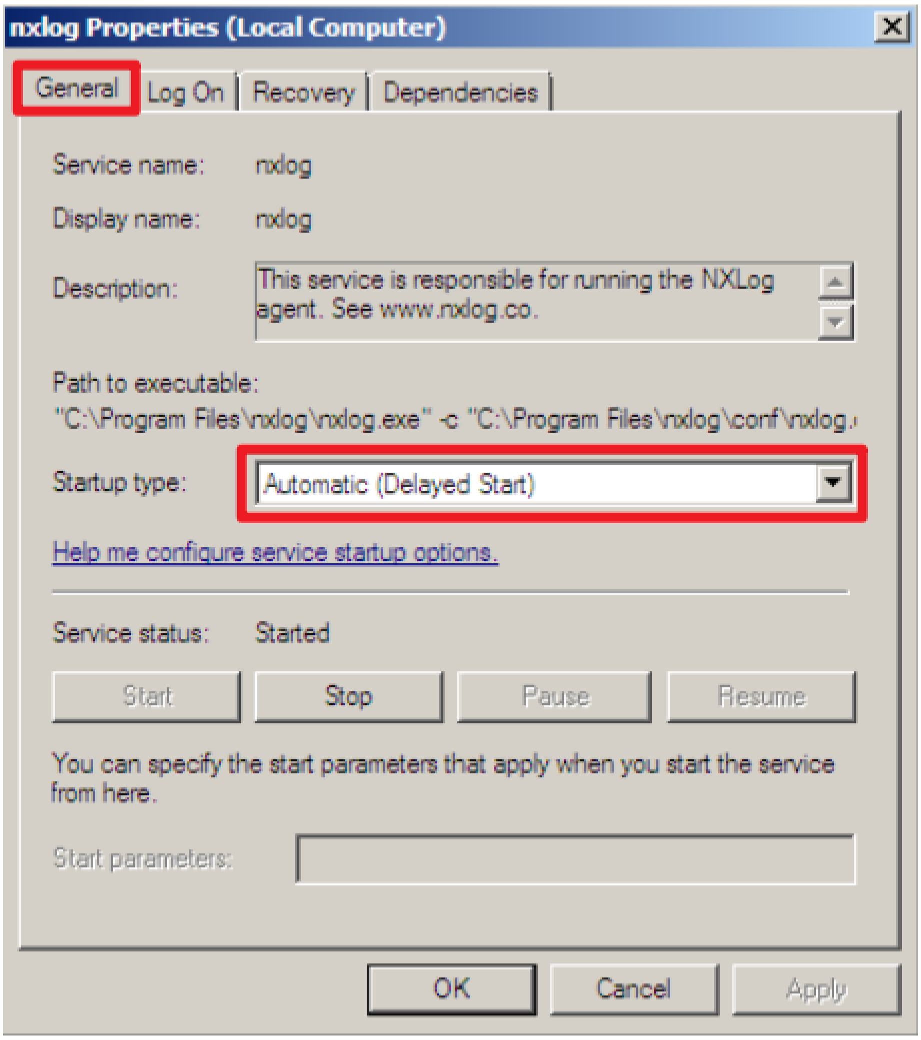
nxlog

Stop the service
Restart the service

Description:
This service is responsible for running the NXLog agent. See www.nxlog.co.

Name	Description	Status	Startup Type	Log On As
Network Connections	Manages o…	Started	Manual	Local System
Network List Service	Identifies t…	Started	Manual	Local Service
Network Location A…	Collects an…	Started	Automatic	Network S…
Network Store Inte…	This servic…	Started	Automatic	Local Service
nxlog	This servic…	Started	Automatic (D…	Local System
Offline Files	The Offline…		Disabled	Local System
Performance Count…	Enables re…		Manual	Local Service
Performance Logs …	Performan…		Manual	Local Service
Plug and Play	Enables a c…	Started	Automatic	Local System
PnP-X IP Bus Enum…	The PnP-X …		Disabled	Local System

(5) On the General tab, verify that Startup type is set to Automatic (Delayed Start).



nxlog Properties (Local Computer)
General
Log On
Recovery
Dependencies
Help me configure service startup options.
Start
Stop
Pause
Resume
OK
Cancel
Apply

Service name: nxlog

Display name: nxlog

Description: This service is responsible for running the NXLog agent. See www.nxlog.co.

Path to executable:
"C:\Program Files\nxlog\nxlog.exe" -c "C:\Program Files\nxlog\conf\nxlog.

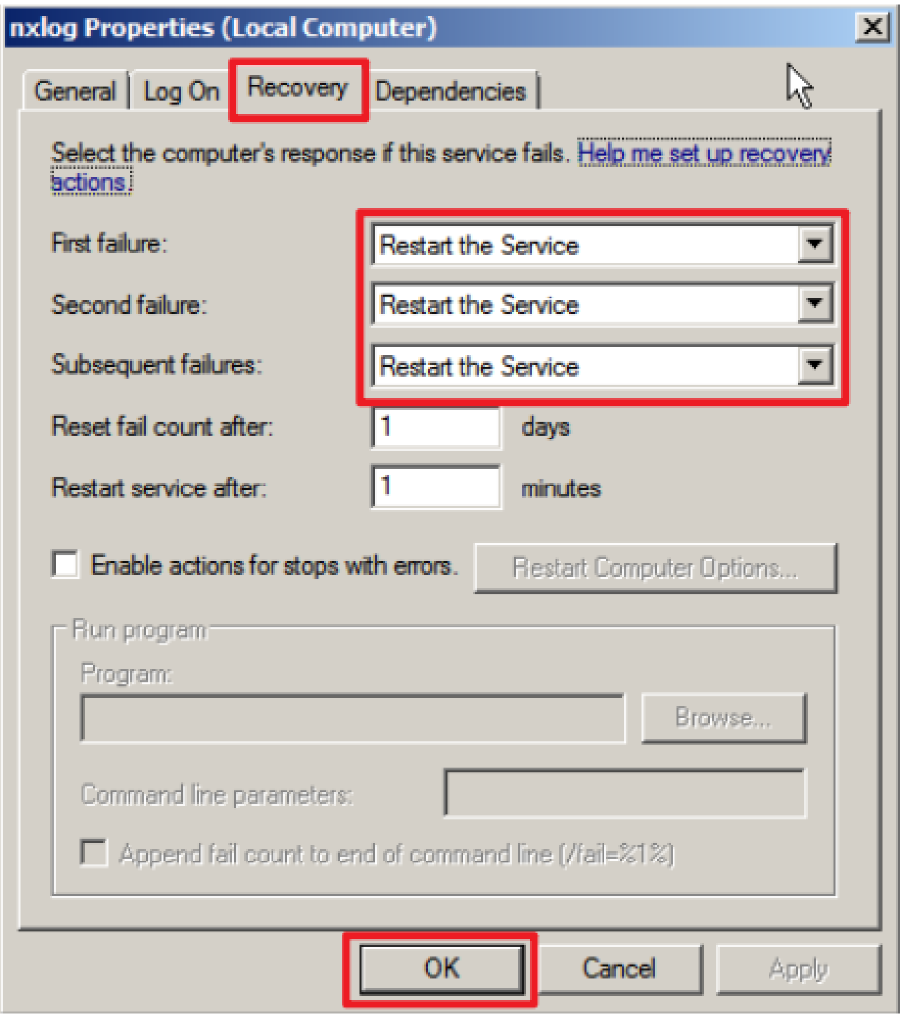
Startup type: Automatic (Delayed Start)

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

(6) On the Recovery tab, verify that First failure, Second failure, and Subsequent failures are all set to "Restart the Service", then click "OK."



nxlog Properties (Local Computer)

Select the computer's response if this service fails. Help me set up recovery actions

First failure: Restart the Service

Second failure: Restart the Service

Subsequent failures: Restart the Service

Reset fail count after: 1 days

Restart service after: 1 minutes

□ Enable actions for stops with errors.

Run program

Program:

Command line parameters:

□ Append fail count to end of command line (/fail=%1%)

2. Exchange 2007

The Example here: Exchange 2007 installed on a Windows 2003 server.

You can configure message tracking logs using either the Exchange Management Console or the Exchange Management Shell.

2.1 Exchange MessageTracking Log

To modify nxlog.conf:

Note: Please refer to 1.3 NXLog Configuration File.

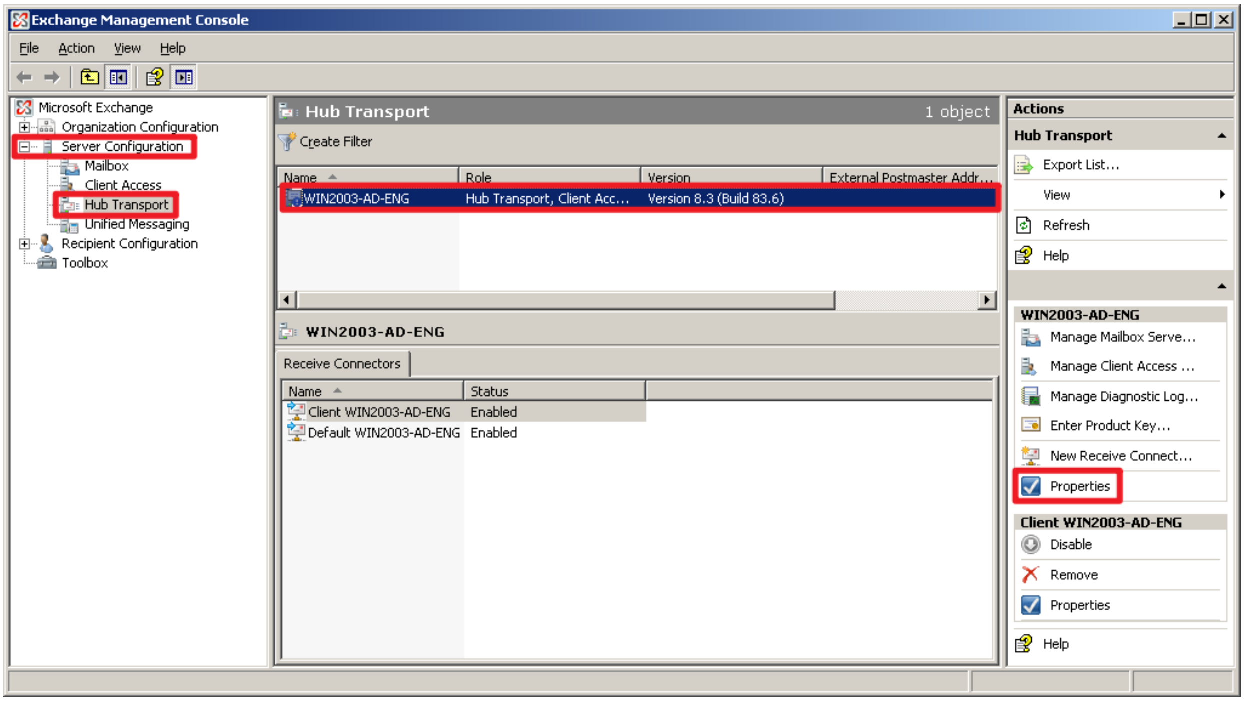
Edit the blue text section to specify the message tracking log folder:

```
define MailLog C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking
```

2.1.1 Exchange Management Console

(1) Open "Exchange Management Console."

(2) Expand "Server Configuration" → select "Hub Transport" → select "Exchange Server (WIN2003)" → select "Properties."

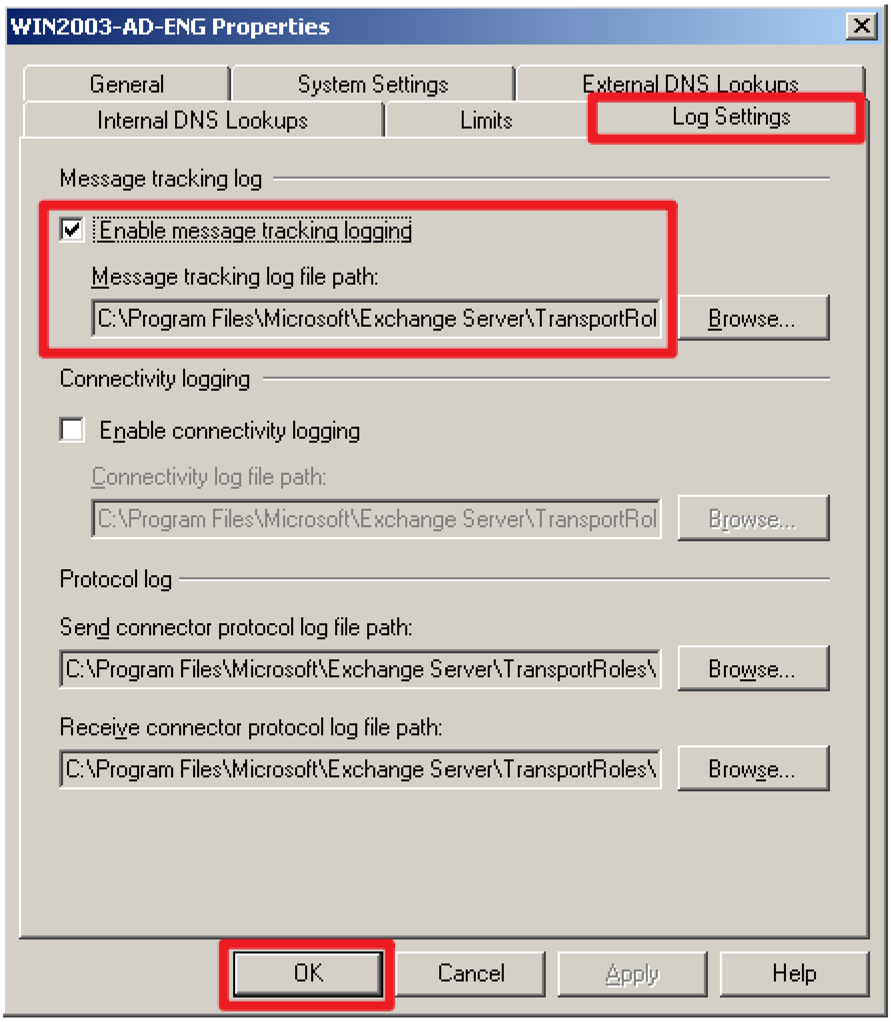


Name	Role	Version	External Postmaster Addr...
WIN2003-AD-ENG	Hub Transport, Client Acc...	Version 8.3 (Build 83.6)	

Name	Status
Client WIN2003-AD-ENG	Enabled
Default WIN2003-AD-ENG	Enabled

(3) Go to the Log Settings tab → verify that Enable message tracking log is checked and the message tracking log path is set to:

C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking



WIN2003-AD-ENG Properties

Message tracking log

☑ Enable message tracking logging

Message tracking log file path: C:\Program Files\Microsoft\Exchange Server\TransportRol

Connectivity logging

□ Enable connectivity logging

Connectivity log file path: C:\Program Files\Microsoft\Exchange Server\TransportRol

Protocol log

Send connector protocol log file path: C:\Program Files\Microsoft\Exchange Server\TransportRoles\

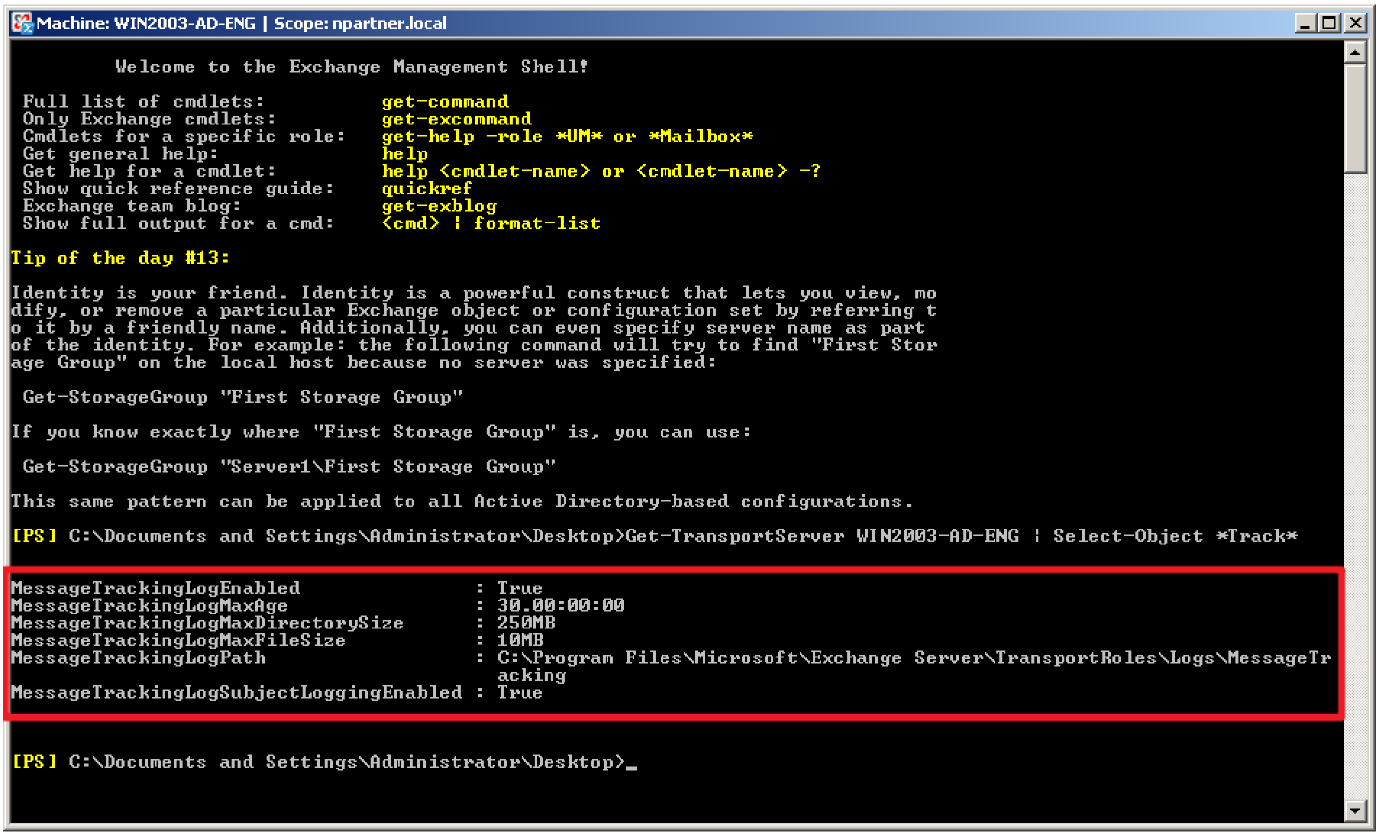
Receive connector protocol log file path: C:\Program Files\Microsoft\Exchange Server\TransportRoles\

2.1.2 Exchange Management Shell

(1) Open” Exchange Management Shell.”

(2) Verify that **Message tracking log** is enabled and check the message tracking log path:
[C:\Program Files\Microsoft\Exchange Server\TransportRoles\Logs\MessageTracking]

```
[PS] C:\> Get-TransportServer Win2003 | Select-Object *Track*
```



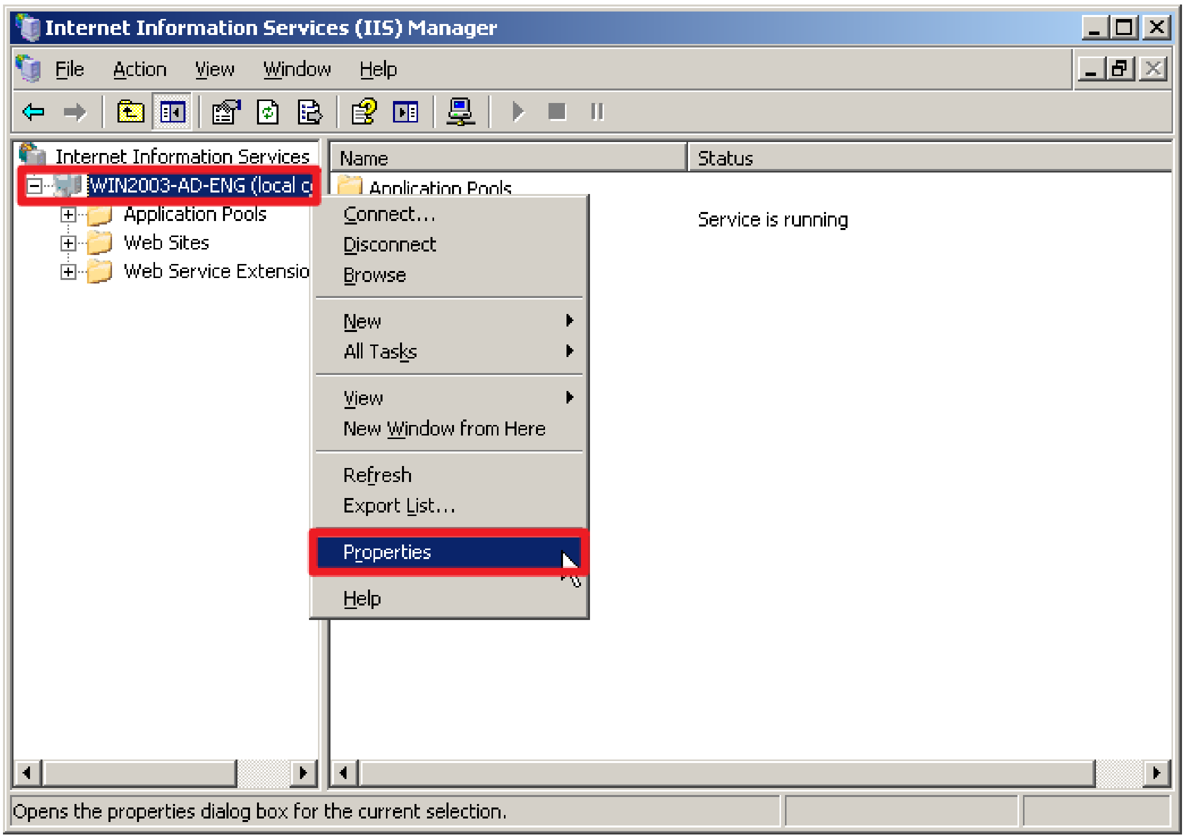
```
         Welcome to the Exchange Management Shell!

 Full list of cmdlets:          get-command
 Only Exchange cmdlets:         get-excommand
 Cmdlets for a specific role:   get-help -role *UM* or *Mailbox*
 Get general help:              help
 Get help for a cmdlet:         help <cmdlet-name> or <cmdlet-name> -?
 Show quick reference guide:    quickref
 Exchange team blog:            get-exblog
 Show full output for a cmd:    <cmd> | format-list

Tip of the day #13:

Identity is your friend. Identity is a powerful construct that lets you view, mo
dify, or remove a particular Exchange object or configuration set by referring t
o it by a friendly name. Additionally, you can even specify server name as part
of the identity. For example: the following command will try to find "First Stor
age Group" on the local host because no server was specified:

 Get-StorageGroup "First Storage Group"

If you know exactly where "First Storage Group" is, you can use:

 Get-StorageGroup "Server1\First Storage Group"

This same pattern can be applied to all Active Directory-based configurations.

[PS] C:\Documents and Settings\Administrator\Desktop>Get-TransportServer WIN2003-AD-ENG | Select-Object *Track*

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


[PS] C:\Documents and Settings\Administrator\Desktop>_
```

Replace the red text section with the name of your Exchange server

2.2 IIS Log

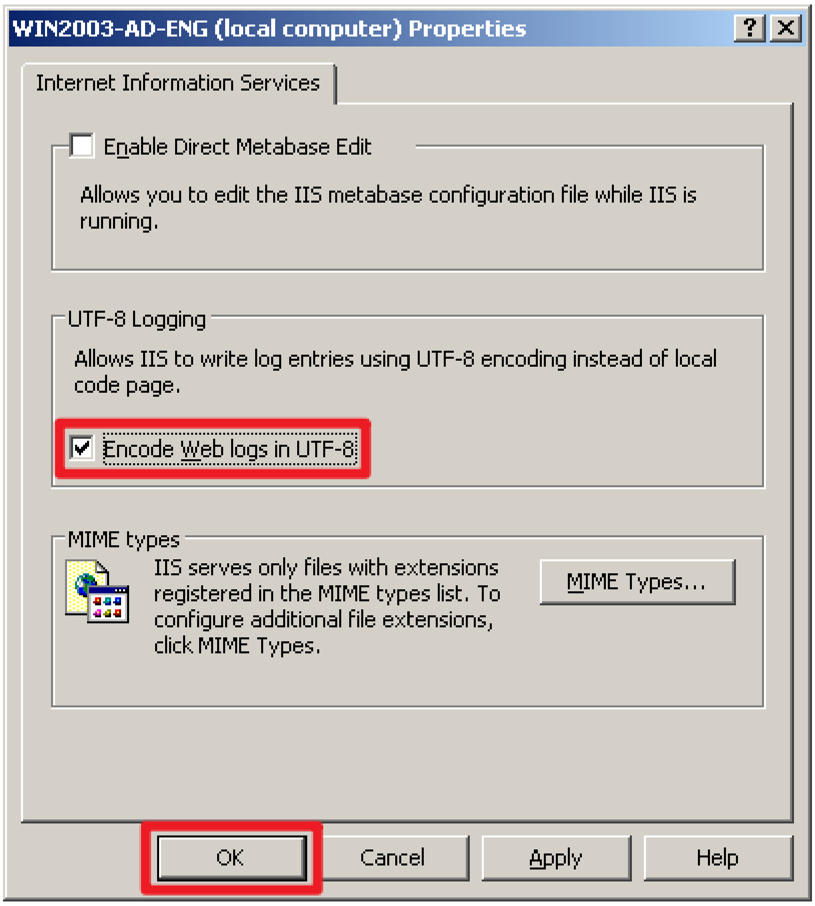
(1) Open Internet Information Services (IIS) Manager.

(2) Right-click on the “IIS server”(the example here is WIN2003-AD-ENG) → select “Properties.”



Opens the properties dialog box for the current selection.

(3) Check Encode Web site logs in “UTF-8” → click “OK.”



WIN2003-AD-ENG (local computer) Properties

Internet Information Services

☐ Enable Direct Metabase Edit

Allows you to edit the IIS metabase configuration file while IIS is running.

UTF-8 Logging

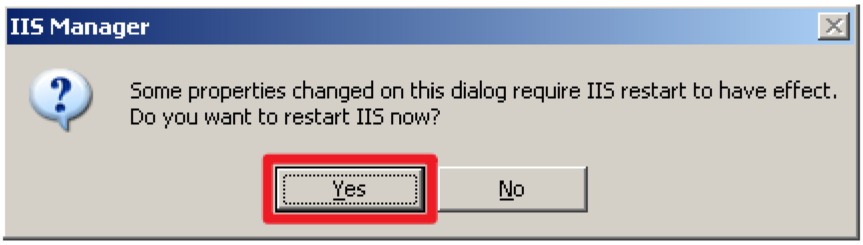
Allows IIS to write log entries using UTF-8 encoding instead of local code page.

☑ Encode Web logs in UTF-8

MIME types

IIS serves only files with extensions registered in the MIME types list. To configure additional file extensions, click MIME Types.

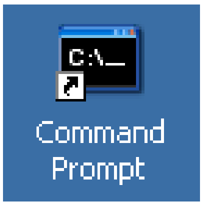
(4) Click “OK” again to restart the IIS service.



IIS Manager

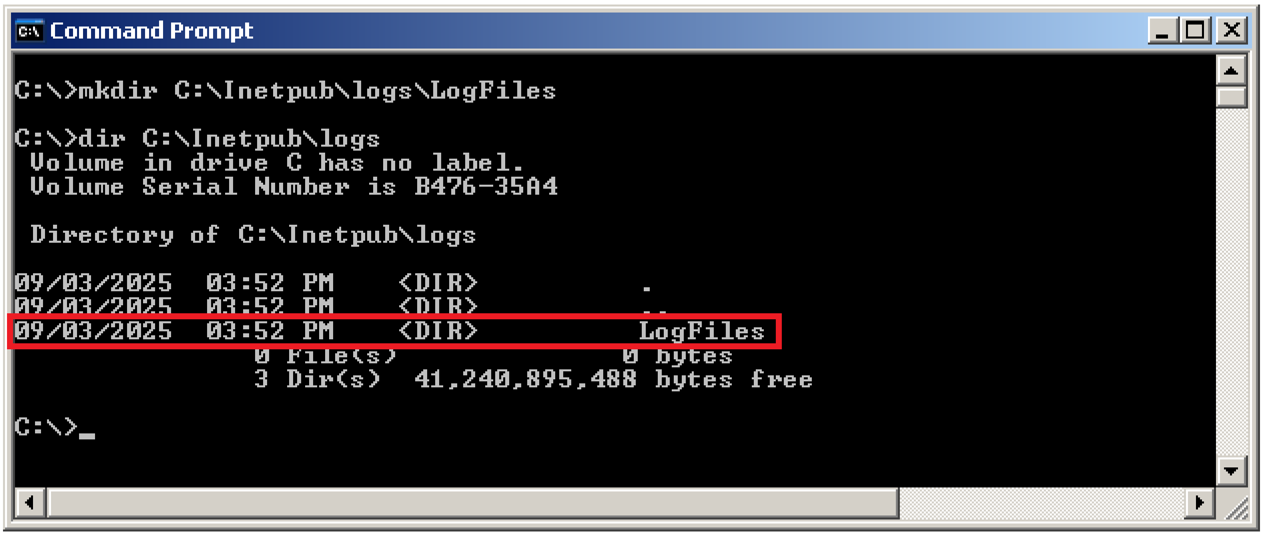
Some properties changed on this dialog require IIS restart to have effect. Do you want to restart IIS now?

(5) Open “Command Prompt.”



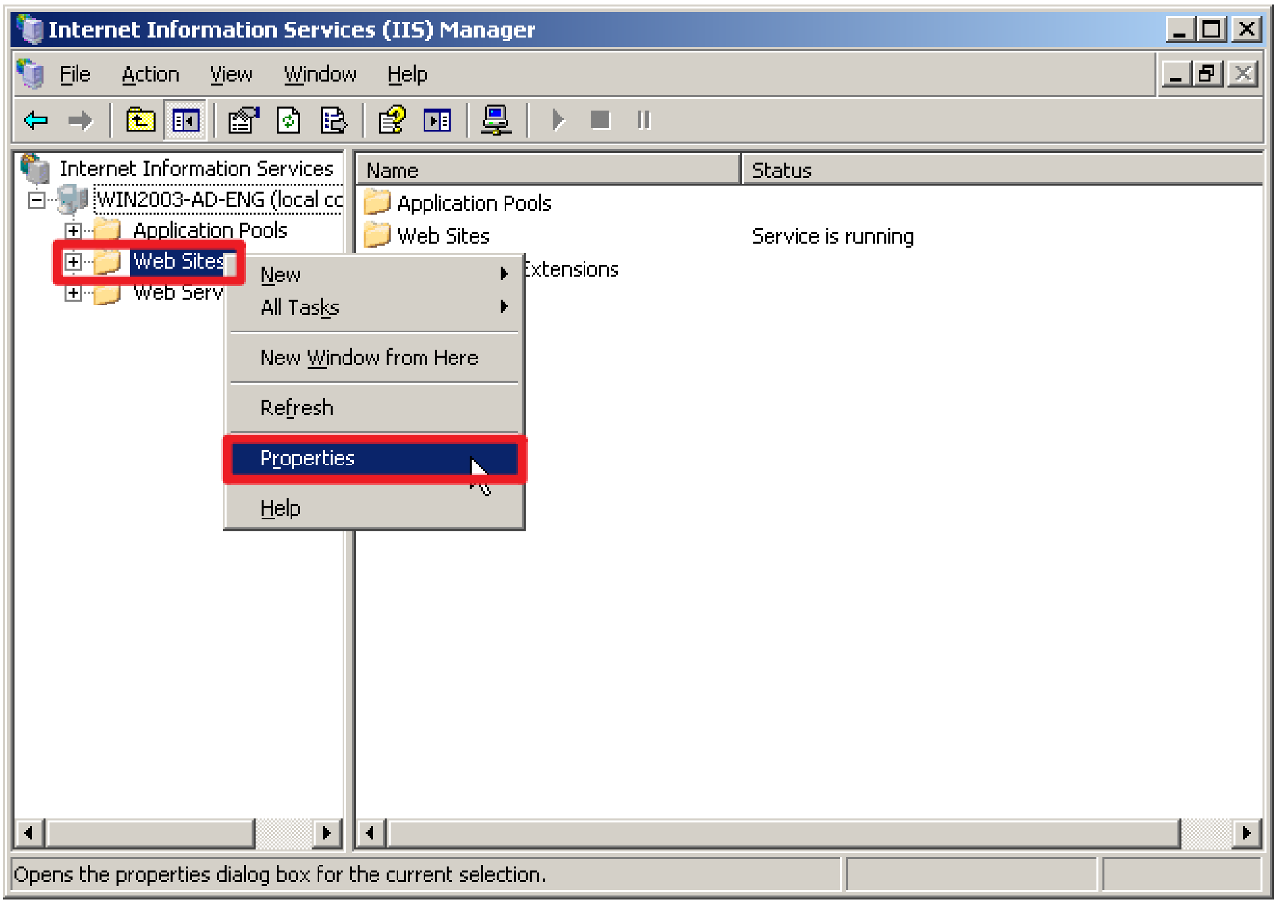
(6) Create and verify the IIS LogFiles directory:

```
C:\> mkdir C:\Inetpub\logs\LogFiles
C:\> dir C:\Inetpub\logs
```



```
C:\>mkdir C:\Inetpub\logs\LogFiles

C:\>dir C:\Inetpub\logs
 Volume in drive C has no label.
 Volume Serial Number is B476-35A4

 Directory of C:\Inetpub\logs

09/03/2025  03:52 PM    <DIR>          .
09/03/2025  03:52 PM    <DIR>          ..
09/03/2025  03:52 PM    <DIR>          LogFiles
               0 File(s)              0 bytes
               3 Dir(s)  41,240,895,488 bytes free

C:\>_
```

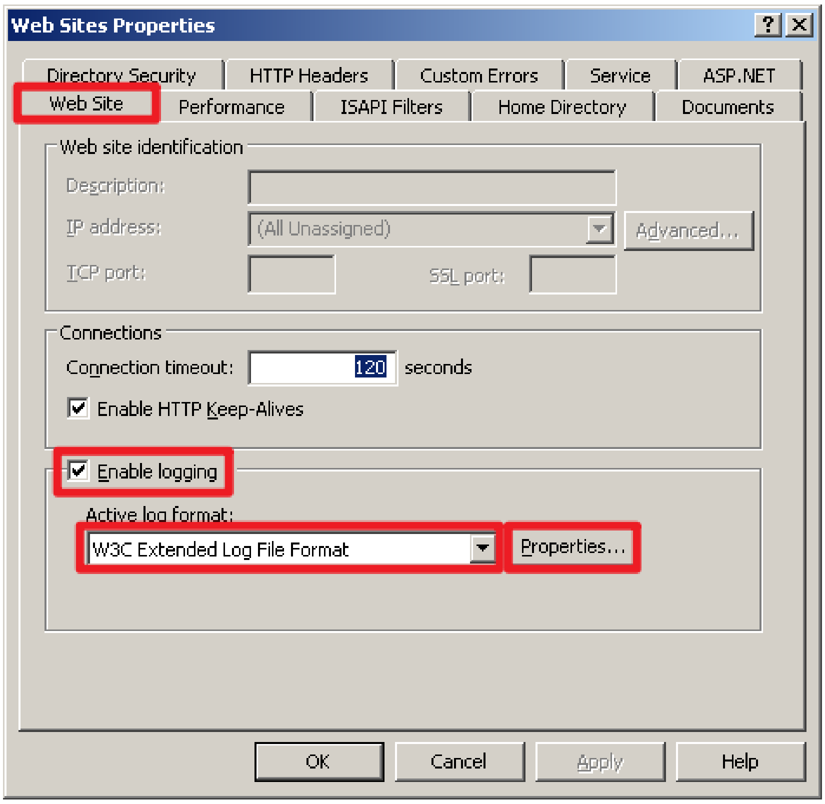
(7) Right-click on “Web Sites” → select “Properties.”



Name	Status
Application Pools	
Web Sites	Service is running
...Extensions	

Opens the properties dialog box for the current selection.

(8) In the Web Site tab: check “Enable logging” → select “W3C Extended Log File Format” as the active log format → click “Properties.”



Web site identification

Description:

IP address: (All Unassigned)

TCP port: SSL port:

Connections

Connection timeout: 120 seconds

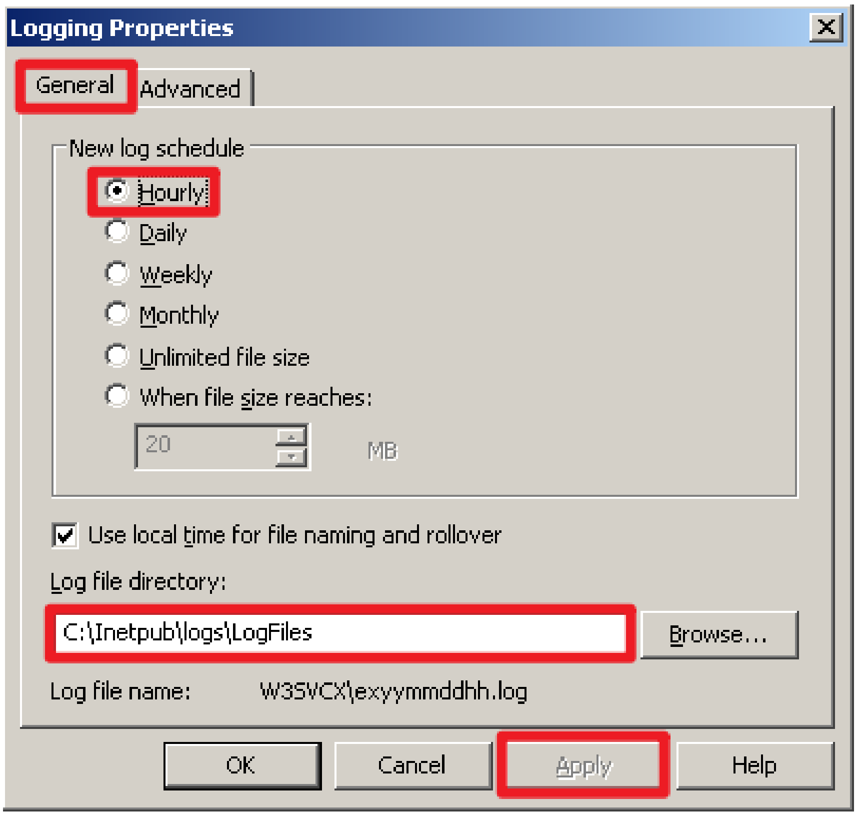
☑ Enable HTTP Keep-Alives

☑ Enable logging

Active log format: W3C Extended Log File Format

(9) In the General tab:

Set log schedule to “Hourly” → check “Use local time” for file naming and rollover→ enter the log file directory: C:\Inetpub\logs\LogFiles→ click “Apply.”



New log schedule

● Hourly

○ Daily

○ Weekly

○ Monthly

○ Unlimited file size

○ When file size reaches:

20 MB

☑ Use local time for file naming and rollover

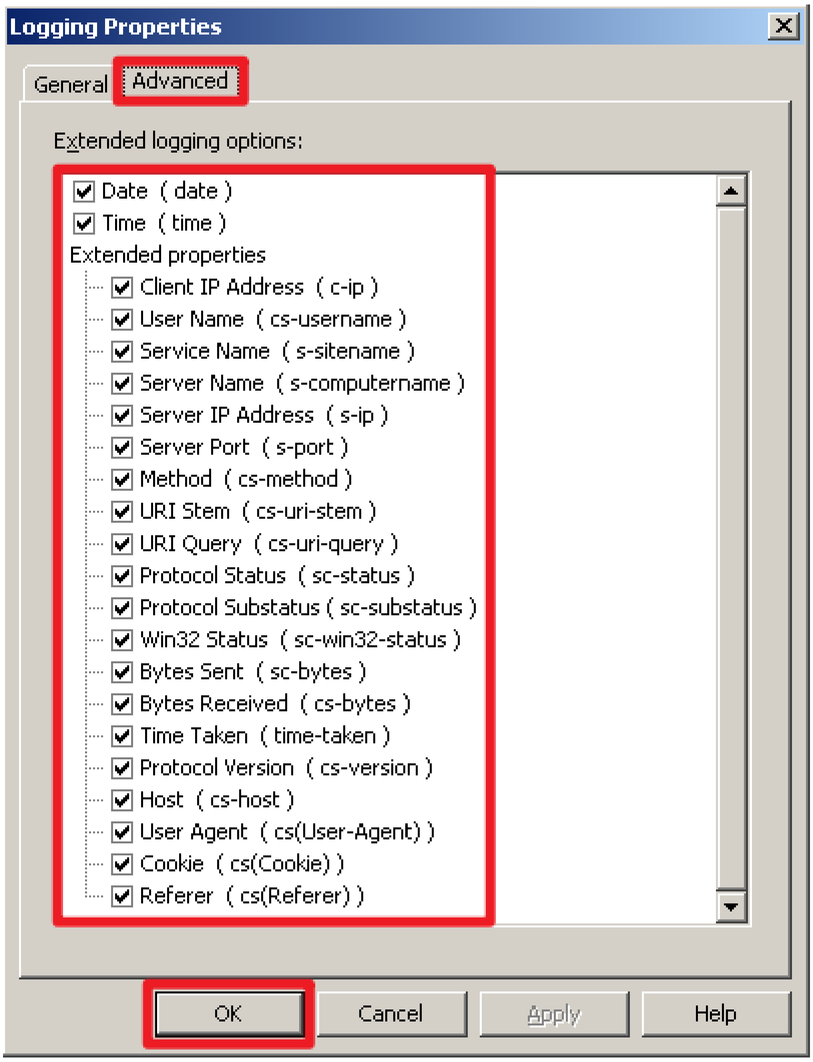
Log file directory: C:\Inetpub\logs\LogFiles

Log file name: W3SVCX\exyymmddhh.log

(10) In the **Extended Properties** tab:

Select Date (date), Time (time), Client IP Address (c-ip), User Name (cs-username), Service Name (s-sitename), Server Name (s-computername), Server IP Address (s-ip), Server Port (s-port), Method (cs-method), URI Stem (cs-uri-stem), URI Query (cs-uri-query), Protocol Status (sc-status), Protocol Substatus (sc-substatus), Win32 Status (sc-win32-status), Bytes Sent (sc-bytes), Bytes Received (cs-bytes), Time Taken (time-taken), Protocol Version (cs-version), Host (cs-host), User Agent (cs(User-Agent)), Cookie (cs(Cookie)), Referrer (cs(Referer))

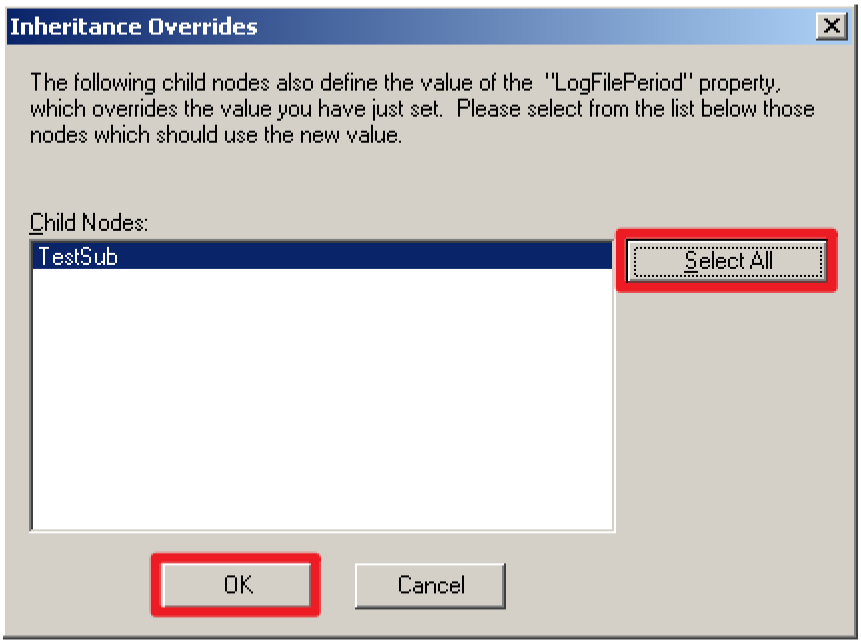
→ Click "OK."



Extended logging options:

- ☑ Date (date)
- ☑ Time (time)
- Extended properties
  - ☑ Client IP Address (c-ip)
  - ☑ User Name (cs-username)
  - ☑ Service Name (s-sitename)
  - ☑ Server Name (s-computername)
  - ☑ Server IP Address (s-ip)
  - ☑ Server Port (s-port)
  - ☑ Method (cs-method)
  - ☑ URI Stem (cs-uri-stem)
  - ☑ URI Query (cs-uri-query)
  - ☑ Protocol Status (sc-status)
  - ☑ Protocol Substatus (sc-substatus)
  - ☑ Win32 Status (sc-win32-status)
  - ☑ Bytes Sent (sc-bytes)
  - ☑ Bytes Received (cs-bytes)
  - ☑ Time Taken (time-taken)
  - ☑ Protocol Version (cs-version)
  - ☑ Host (cs-host)
  - ☑ User Agent (cs(User-Agent))
  - ☑ Cookie (cs(Cookie))
  - ☑ Referer (cs(Referer))

(11) Click “Select All” to apply to all Web sites → click “OK.”



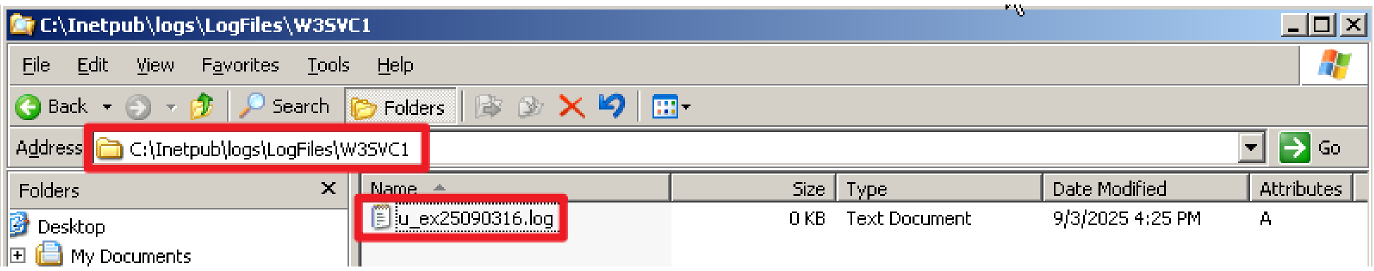
Inheritance Overrides

The following child nodes also define the value of the "LogFilePeriod" property, which overrides the value you have just set. Please select from the list below those nodes which should use the new value.

Child Nodes:

TestSub

(12) Verify IIS log files are created in the directory: C:\Inetpub\logs\LogFiles\W3SVC1



C:\Inetpub\logs\LogFiles\W3SVC1

Address: C:\Inetpub\logs\LogFiles\W3SVC1

Name	Size	Type	Date Modified	Attributes
u_ex25090316.log	0 KB	Text Document	9/3/2025 4:25 PM	A

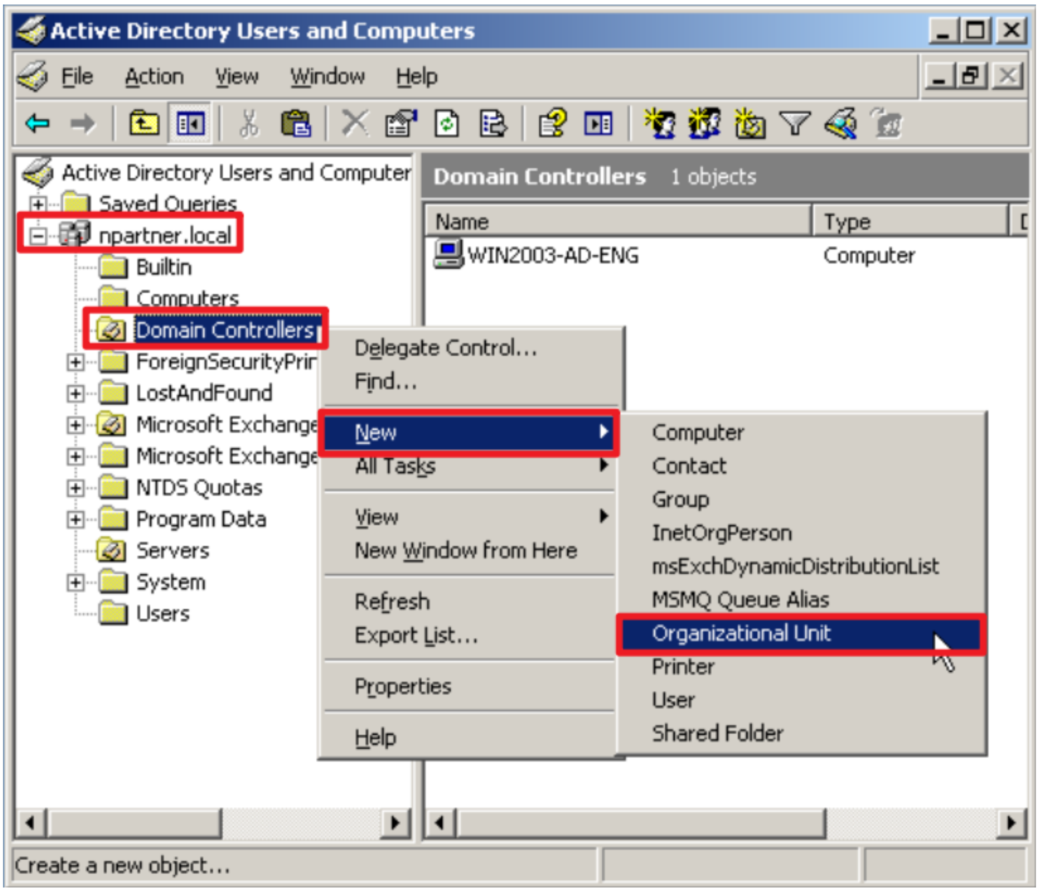
2.3 Event Log

2.3.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”

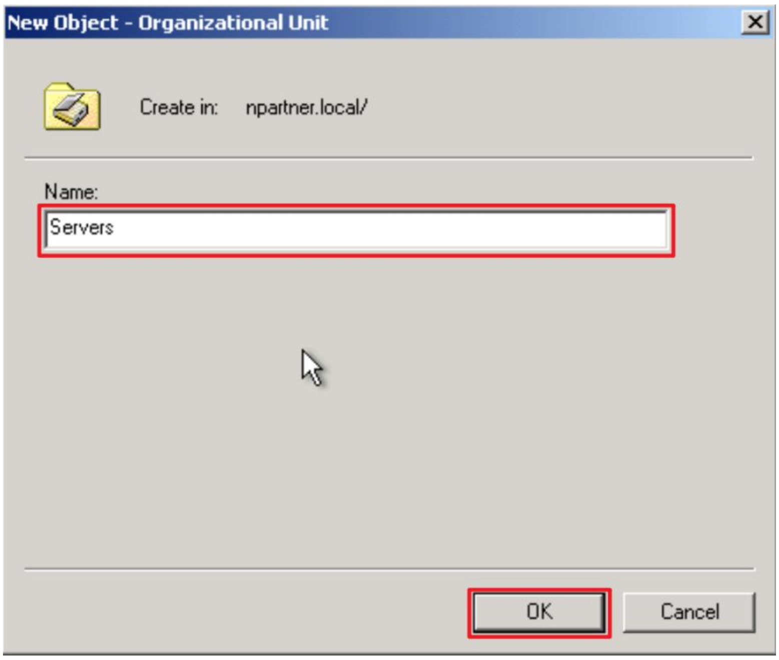
(2) Add an Organizational Unit

Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

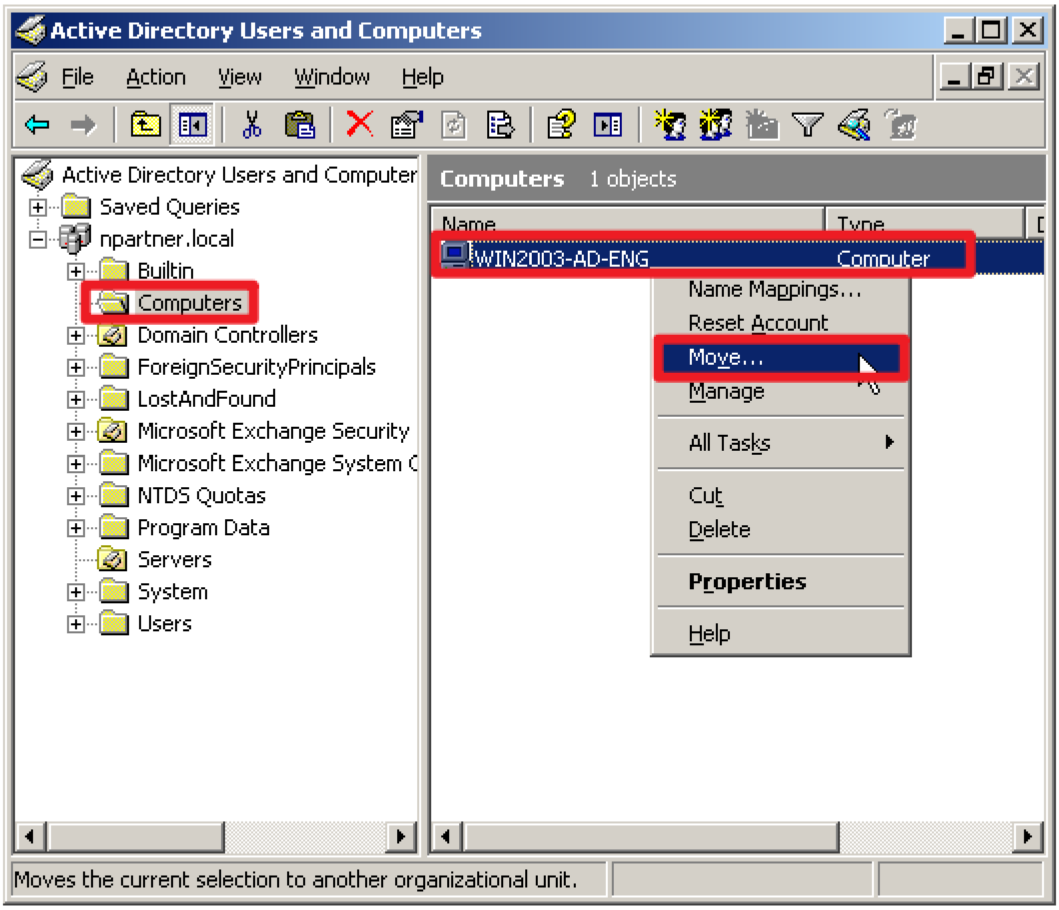
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



(4) Move the Server to your New Organizational Unit:

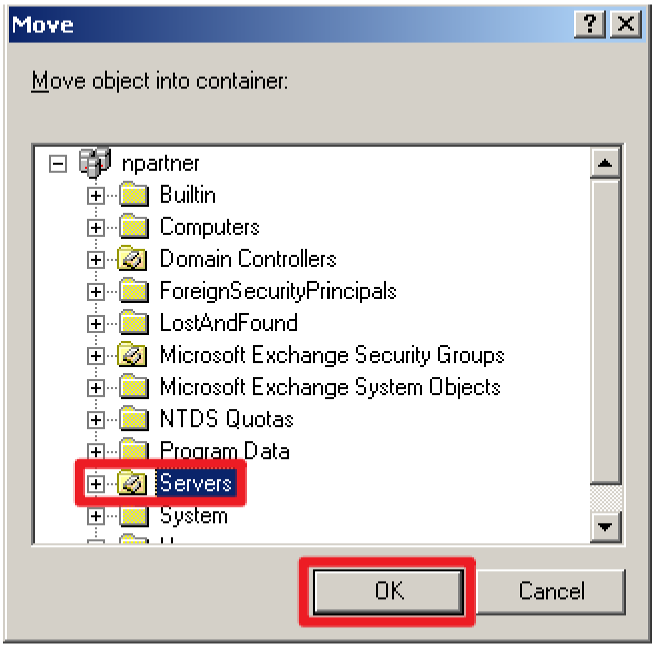
Select “Computers” → right-click on the “WIN2003-AD-ENG” server.

Note: Please select the Windows AD server according to the actual environment. → click “Move.”



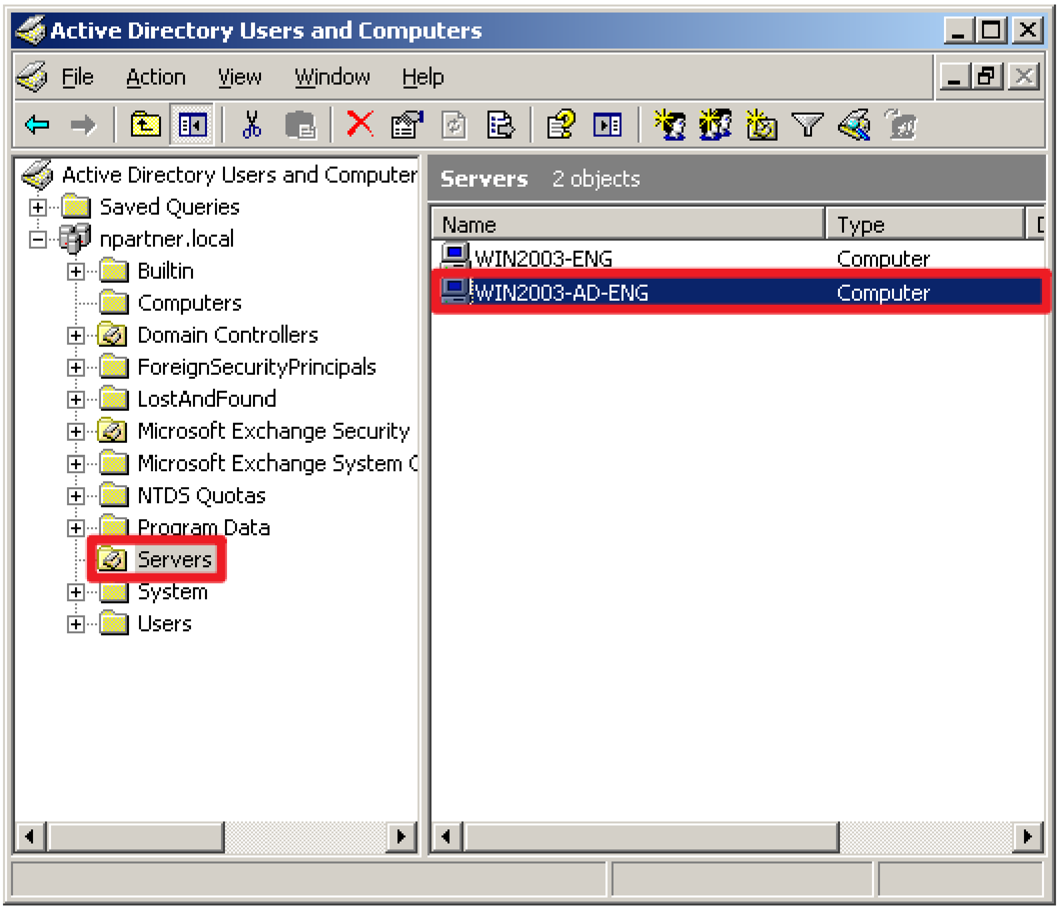
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”


Move
Move object into container:
npartner
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
Microsoft Exchange Security Groups
Microsoft Exchange System Objects
NTDS Quotas
Program Data
Servers
System
OK
Cancel

(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand “Domain Controllers” and select your OU folder (in this example, it is “Servers”) and confirm that the “WIN2003-AD-ENG” server has been moved.

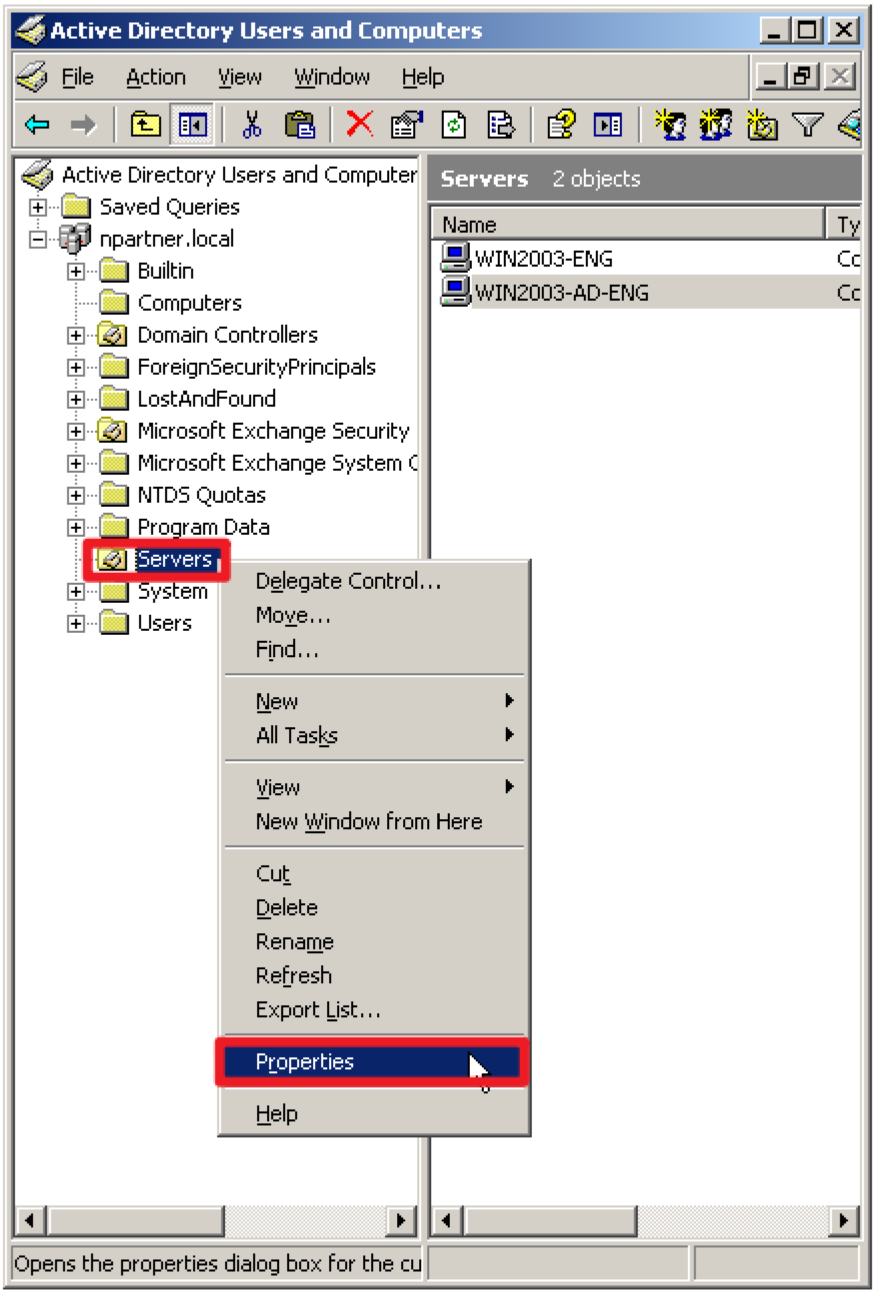

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
npartner.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
LostAndFound
Microsoft Exchange Security
Microsoft Exchange System C
NTDS Quotas
Program Data
Servers
System
Users
Servers 2 objects

Name	Type
WIN2003-ENG	Computer
WIN2003-AD-ENG	Computer

2.3.2 Group Policy Settings

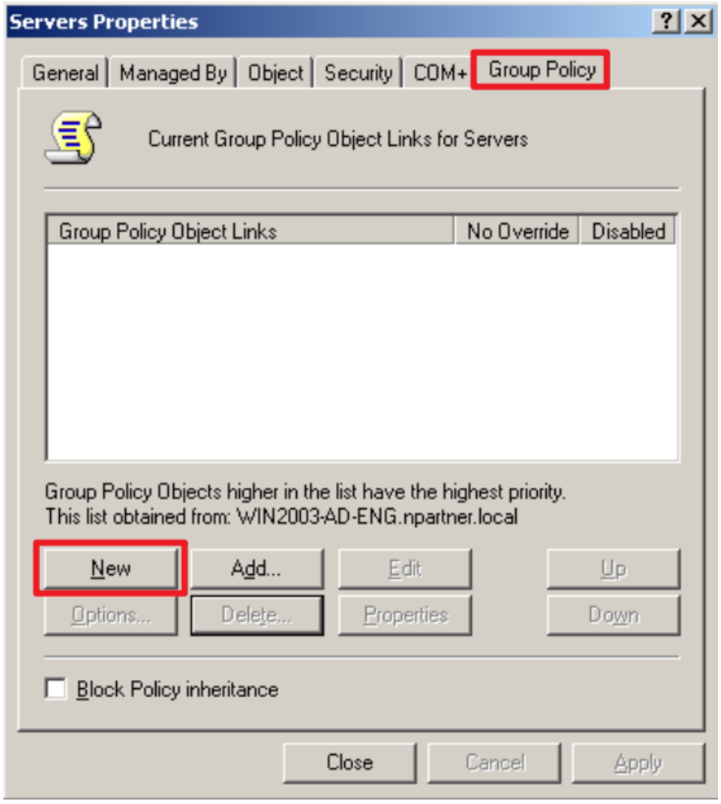
(1) Click “Active Directory Users and Computers.”

(2) In the “Servers” organizational unit (OU), right-click and select “Properties.”



(3) Enter the Group Policy Object (GPO) name

On the “Group Policy” page → click “New.”



Servers Properties

General | Managed By | Object | Security | COM+ | Group Policy

Current Group Policy Object Links for Servers

Group Policy Object Links	No Override	Disabled

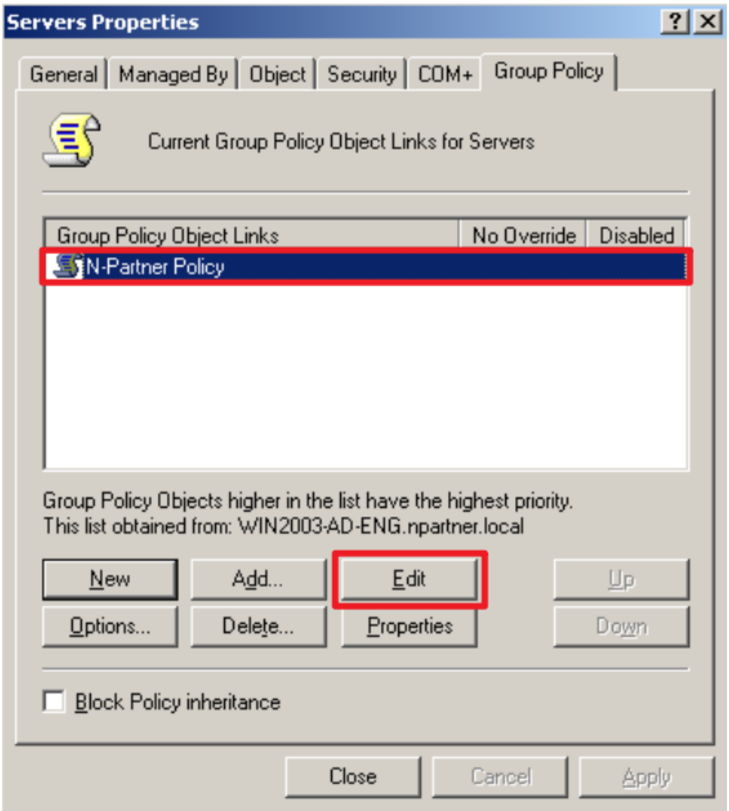
Group Policy Objects higher in the list have the highest priority.
This list obtained from: WIN2003-AD-ENG.npartner.local

(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”)

Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



Servers Properties

General | Managed By | Object | Security | COM+ | Group Policy

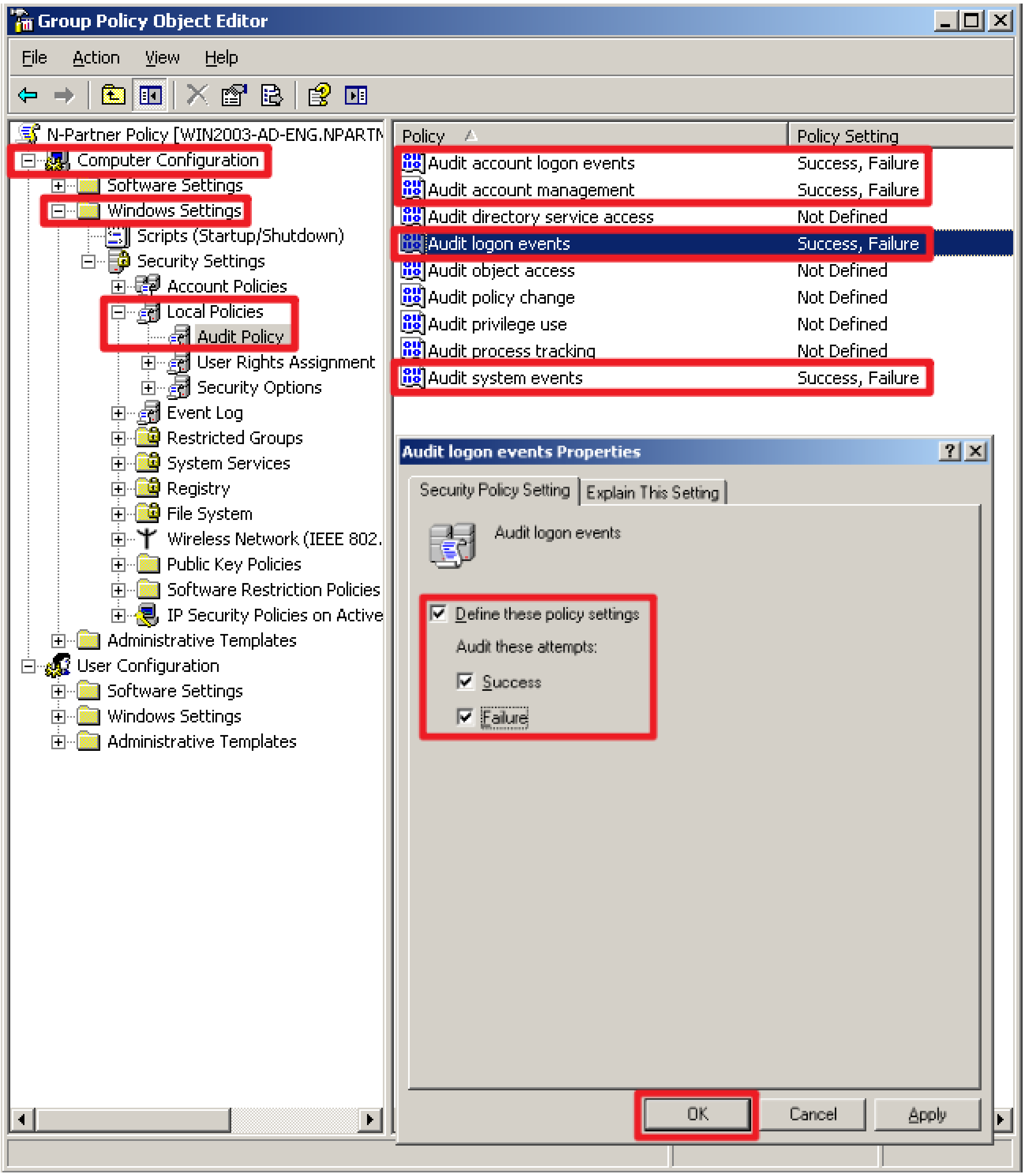
Current Group Policy Object Links for Servers

Group Policy Object Links	No Override	Disabled
N-Partner Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: WIN2003-AD-ENG.npartner.local

(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” and “Audit system events” → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Success, Failure

Audit logon events Properties

Audit logon events

☑ Define these policy settings

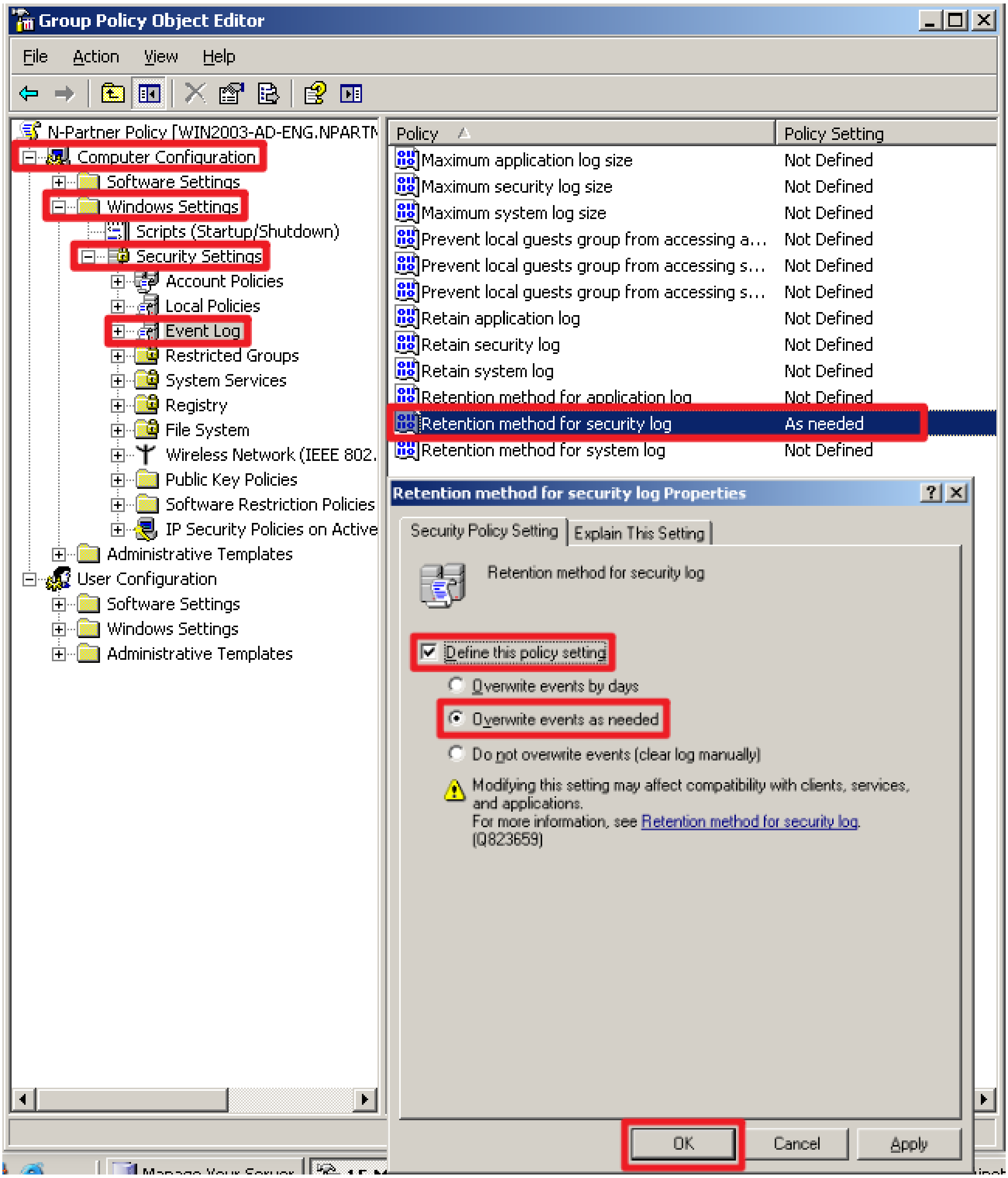
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Security Log Retention Method

Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



N-Partner Policy [WIN2003-AD-ENG.NPARTN
- Computer Configuration
  - Software Settings
  - Windows Settings
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
      - Local Policies
      - Event Log
      - Restricted Groups
      - System Services
      - Registry
      - File System
      - Wireless Network (IEEE 802.
      - Public Key Policies
      - Software Restriction Policies
      - IP Security Policies on Active
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	Not Defined
Maximum system log size	Not Defined
Prevent local guests group from accessing a...	Not Defined
Prevent local guests group from accessing s...	Not Defined
Prevent local guests group from accessing s...	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Retention method for security log Properties

Retention method for security log

☑ Define this policy setting

○ Overwrite events by days

● Overwrite events as needed

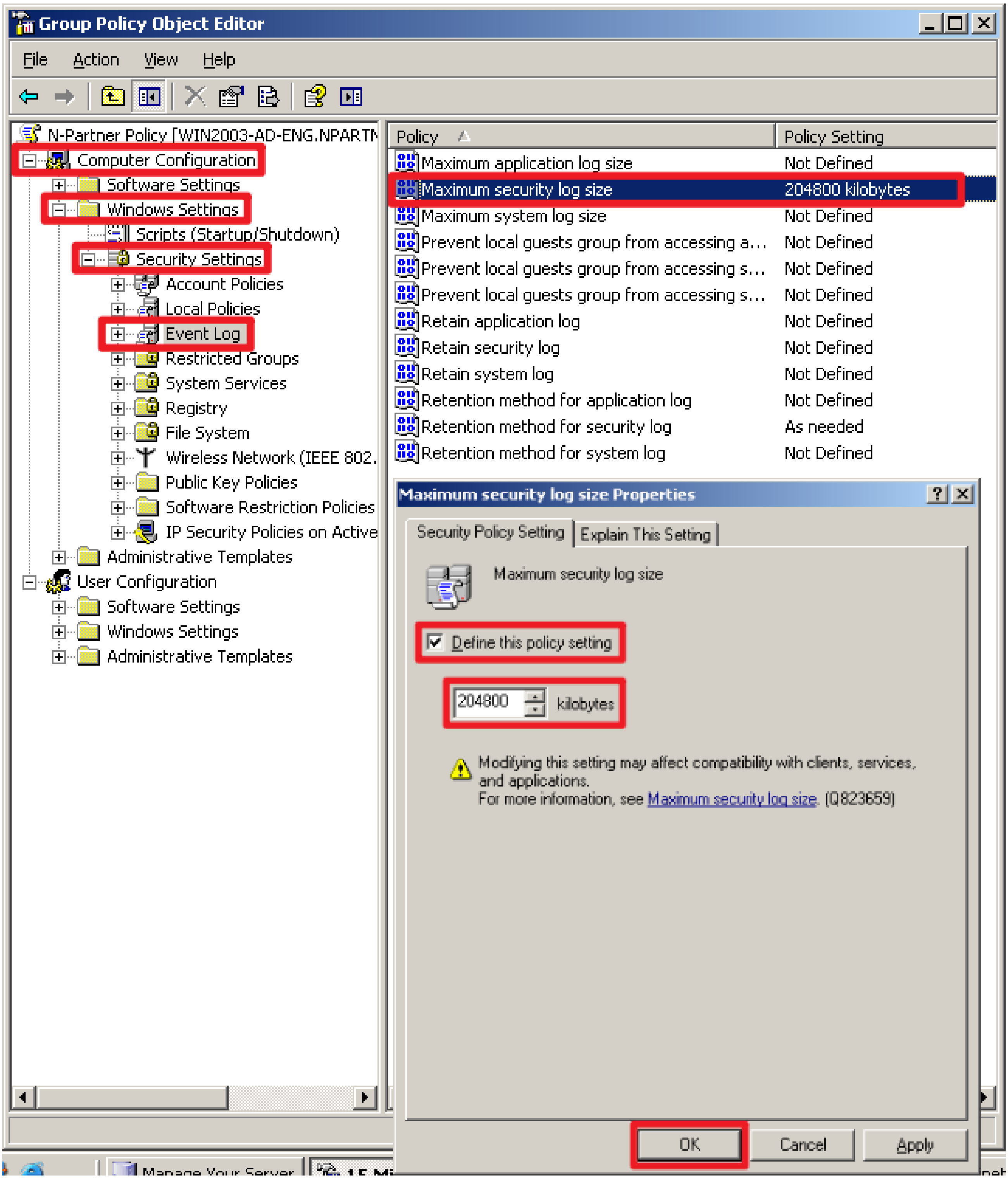
○ Do not overwrite events (clear log manually)

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Retention method for security log. (Q823659)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → and click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”



N-Partner Policy [WIN2003-AD-ENG.NPARTN

- Computer Configuration
  - Software Settings
  - Windows Settings
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
      - Local Policies
      - Event Log
      - Restricted Groups
      - System Services
      - Registry
      - File System
      - Wireless Network (IEEE 802.
      - Public Key Policies
      - Software Restriction Policies
      - IP Security Policies on Active
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing a...	Not Defined
Prevent local guests group from accessing s...	Not Defined
Prevent local guests group from accessing s...	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Maximum security log size Properties

Maximum security log size

☑ Define this policy setting

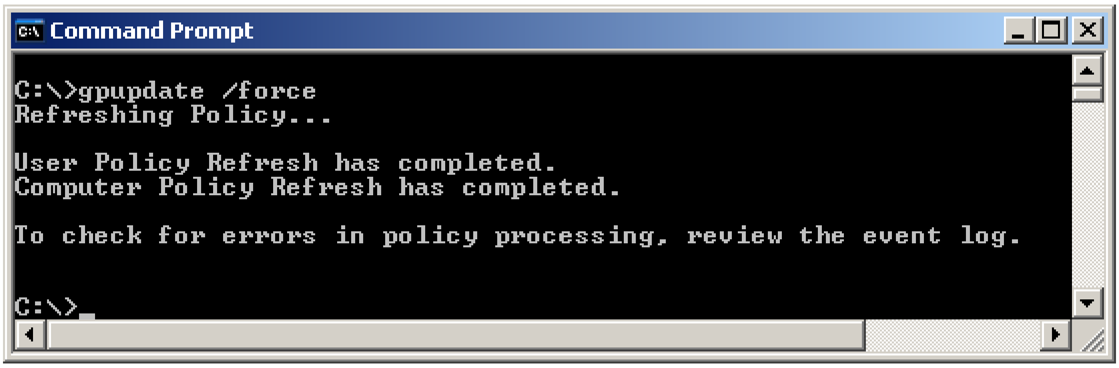
204800 kilobytes

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Maximum security log size. (Q823659)

(8) On the Exchange server, open “Command Prompt.”

(9) Enter the command below to refresh group policy.

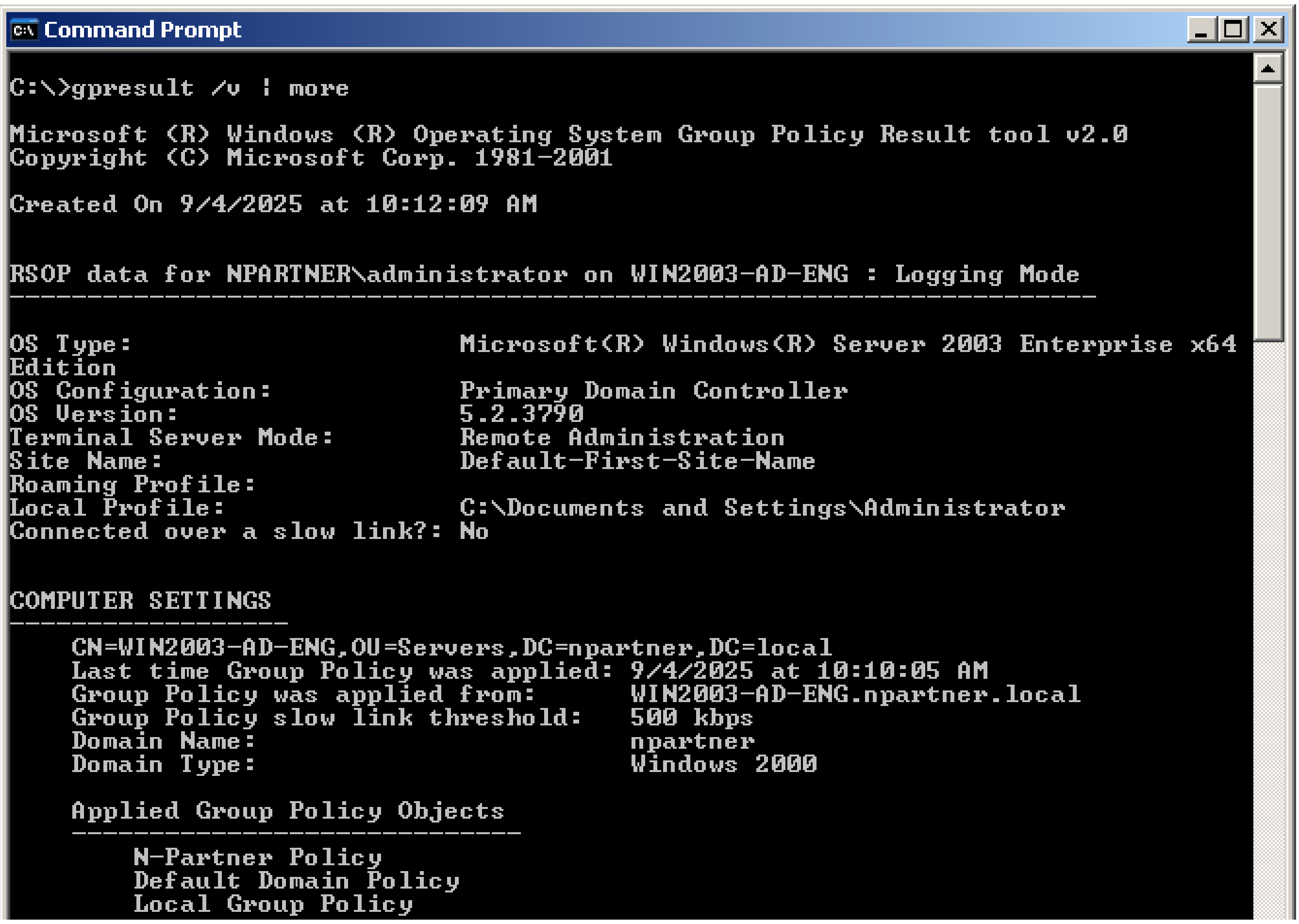
```
C:\> gpupdate /force
```



```
C:\>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.


C:\>_
```

(10) Enter the command below to verify the applied group policy settings.

```
C:\> gpresult /v
```



```
C:\>gpresult /v | more

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 9/4/2025 at 10:12:09 AM


RSOP data for NPARTNER\administrator on WIN2003-AD-ENG : Logging Mode
----------------------------------------------------------------------

OS Type:                     Microsoft(R) Windows(R) Server 2003 Enterprise x64
Edition
OS Configuration:            Primary Domain Controller
OS Version:                  5.2.3790
Terminal Server Mode:        Remote Administration
Site Name:                   Default-First-Site-Name
Roaming Profile:
Local Profile:               C:\Documents and Settings\Administrator
Connected over a slow link?: No


COMPUTER SETTINGS
------------------
    CN=WIN2003-AD-ENG,OU=Servers,DC=npartner,DC=local
    Last time Group Policy was applied: 9/4/2025 at 10:10:05 AM
    Group Policy was applied from:      WIN2003-AD-ENG.npartner.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        npartner
    Domain Type:                        Windows 2000

    Applied Group Policy Objects
    -----------------------------
        N-Partner Policy
        Default Domain Policy
        Local Group Policy
```

3. Exchange 2010

Example: Exchange 2010 installed on a Windows 2008 server.

Message tracking logs can be configured through the “Exchange Management Console” or the “Exchange Management Shell.”

3.1 Exchange MessageTracking Log

Modify nxlog.conf

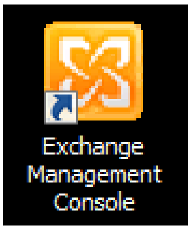
Note: Please refer to 1.3 NXLog Configuration File.

Edit the blue text section to specify the message tracking log folder:

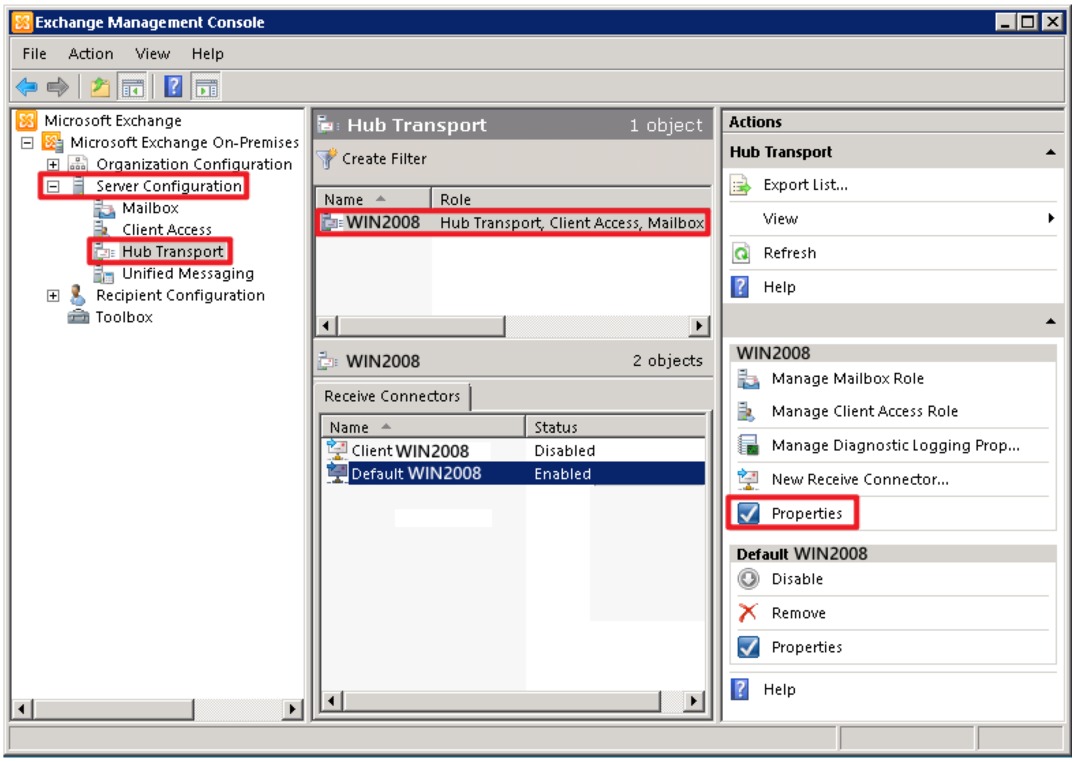
```
define MailLog\> C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking
```

3.1.1 Exchange Management Console

(1) Open “Exchange Management Console.”



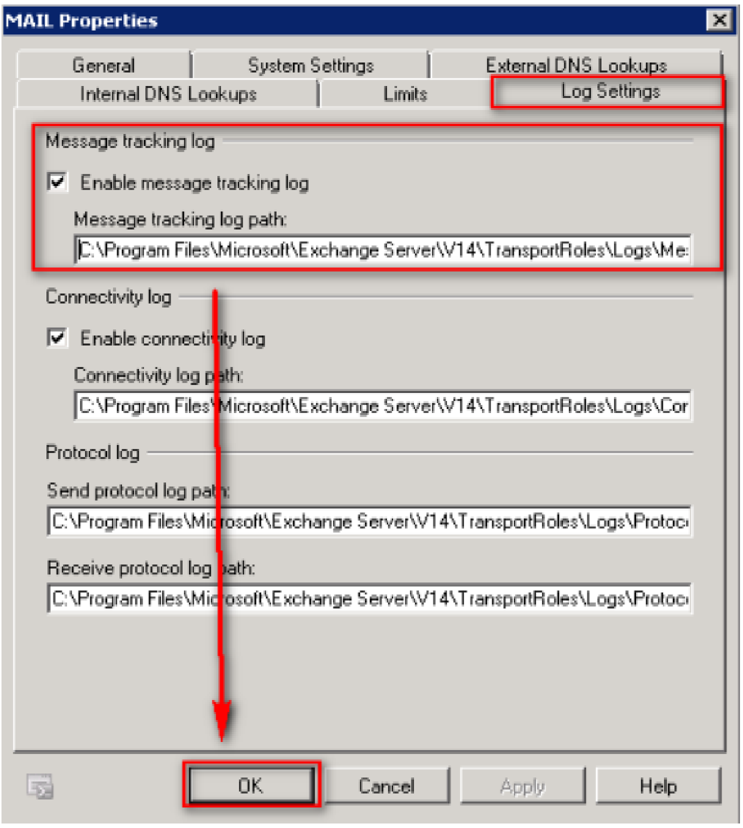
(2) Expand “Server Configuration” → select “Hub Transport” → select “Exchange Server (WIN2008)” → “Properties.”



Name	Role
WIN2008	Hub Transport, Client Access, Mailbox

Name	Status
Client WIN2008	Disabled
Default WIN2008	Enabled

(3) Go to the “Log Settings” tab → verify “Enable message tracking log” is checked and the log path is set to: C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\MessageTracking


MAIL Properties

Message tracking log

☑ Enable message tracking log

Message tracking log path:
C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Me:

Connectivity log

☑ Enable connectivity log

Connectivity log path:
C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Cor

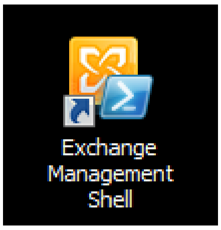
Protocol log

Send protocol log path:
C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Protoc

Receive protocol log path:
C:\Program Files\Microsoft\Exchange Server\V14\TransportRoles\Logs\Protoc

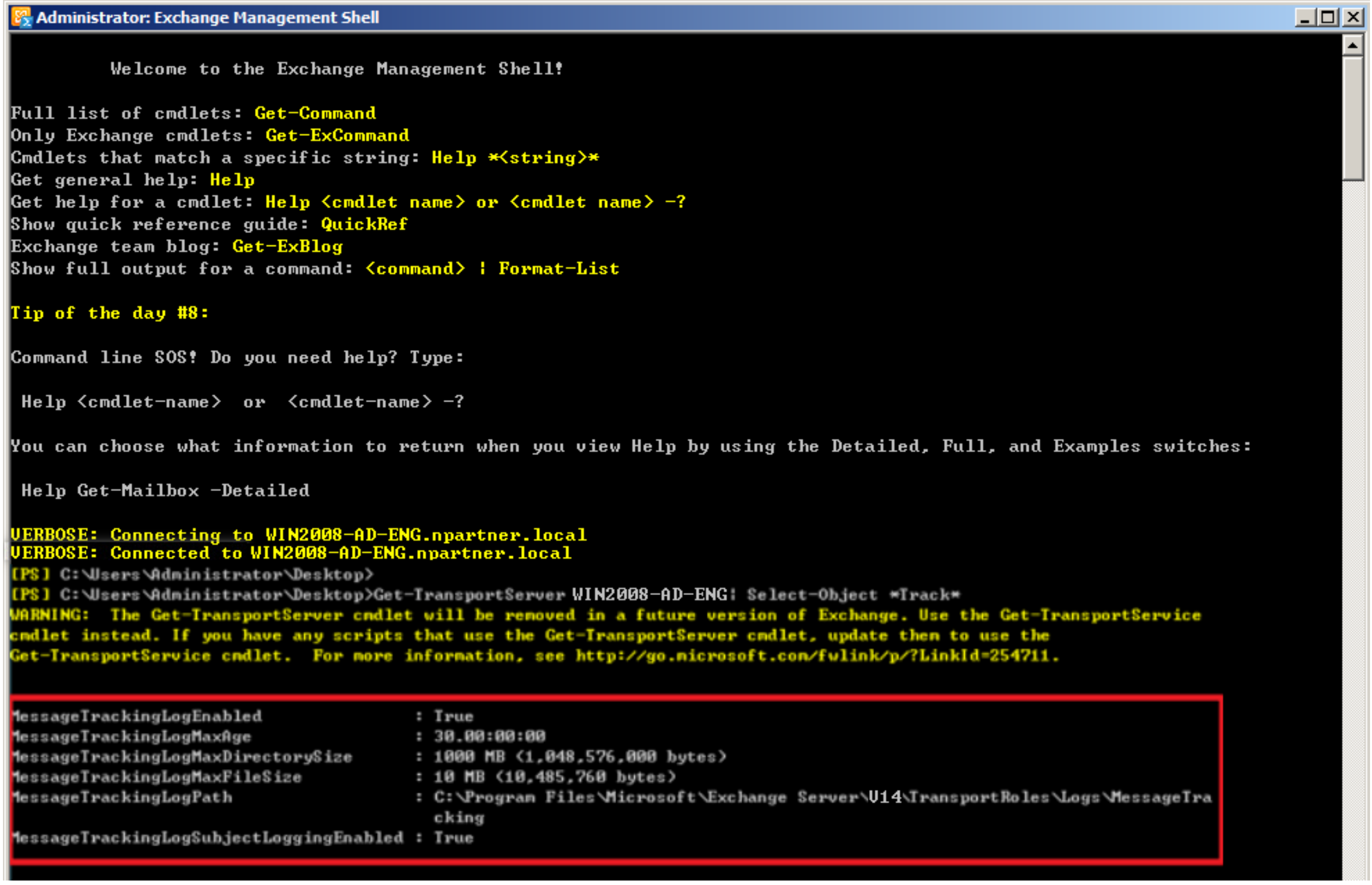
3.1.2 Exchange Management Shell

(1) Open “Exchange Management Shell.”



(2) Verify that “Message tracking log” is enabled and check the log path:

```
[PS] C:\> Get-TransportServer Win2008 | Select-Object *Track*
```



```
         Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Show quick reference guide: QuickRef
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Tip of the day #8:

Command line SOS! Do you need help? Type:

 Help <cmdlet-name>  or  <cmdlet-name> -?

You can choose what information to return when you view Help by using the Detailed, Full, and Examples switches:

 Help Get-Mailbox -Detailed

VERBOSE: Connecting to WIN2008-AD-ENG.npartner.local
VERBOSE: Connected to WIN2008-AD-ENG.npartner.local
[PS] C:\Users\Administrator\Desktop>
[PS] C:\Users\Administrator\Desktop>Get-TransportServer WIN2008-AD-ENG| Select-Object *Track*
WARNING:  The Get-TransportServer cmdlet will be removed in a future version of Exchange. Use the Get-TransportService
cmdlet instead. If you have any scripts that use the Get-TransportServer cmdlet, update then to use the
Get-TransportService cmdlet.  For more information, see http://go.microsoft.com/fwlink/p/?LinkId=254711.

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\V14\TransportRoles\Logs\MessageTra
                                           cking
MessageTrackingLogSubjectLoggingEnabled : True
```

Note: Replace the red text section with the name of your Exchange server.

3.2 IIS Log

Modify nxlog.conf

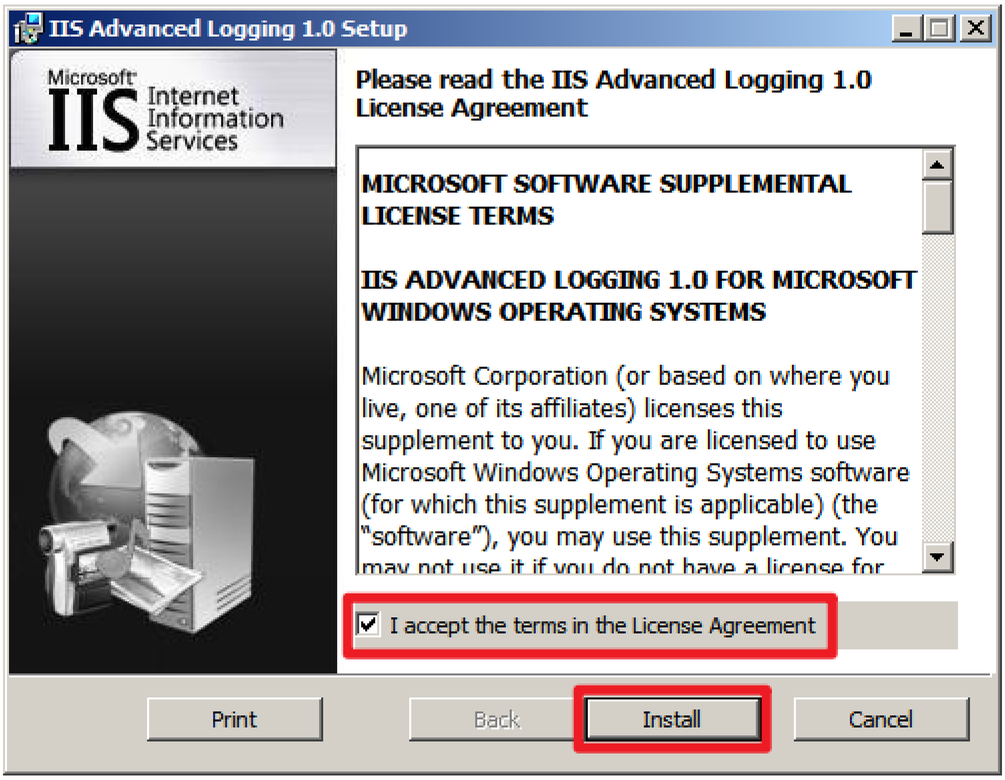
Note: Refer to "1.3 NXLog Configuration File".

Edit the blue text section to specify the IIS log folder path:

```
define IISLog C:\inetpub\logs\AdvancedLogs
```

(1) Install "IIS Advanced Logging" for Windows Server 2008.

Click “AdvancedLogging64.msi” → check “I accept the terms in the license agreement” → click “Install” → “Finish.”



IIS Advanced Logging 1.0 Setup
Microsoft
IIS Internet Information Services

Please read the IIS Advanced Logging 1.0 License Agreement

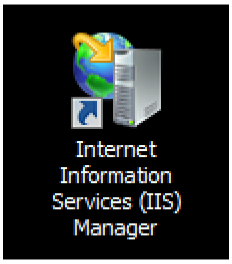
MICROSOFT SOFTWARE SUPPLEMENTAL LICENSE TERMS

IIS ADVANCED LOGGING 1.0 FOR MICROSOFT WINDOWS OPERATING SYSTEMS

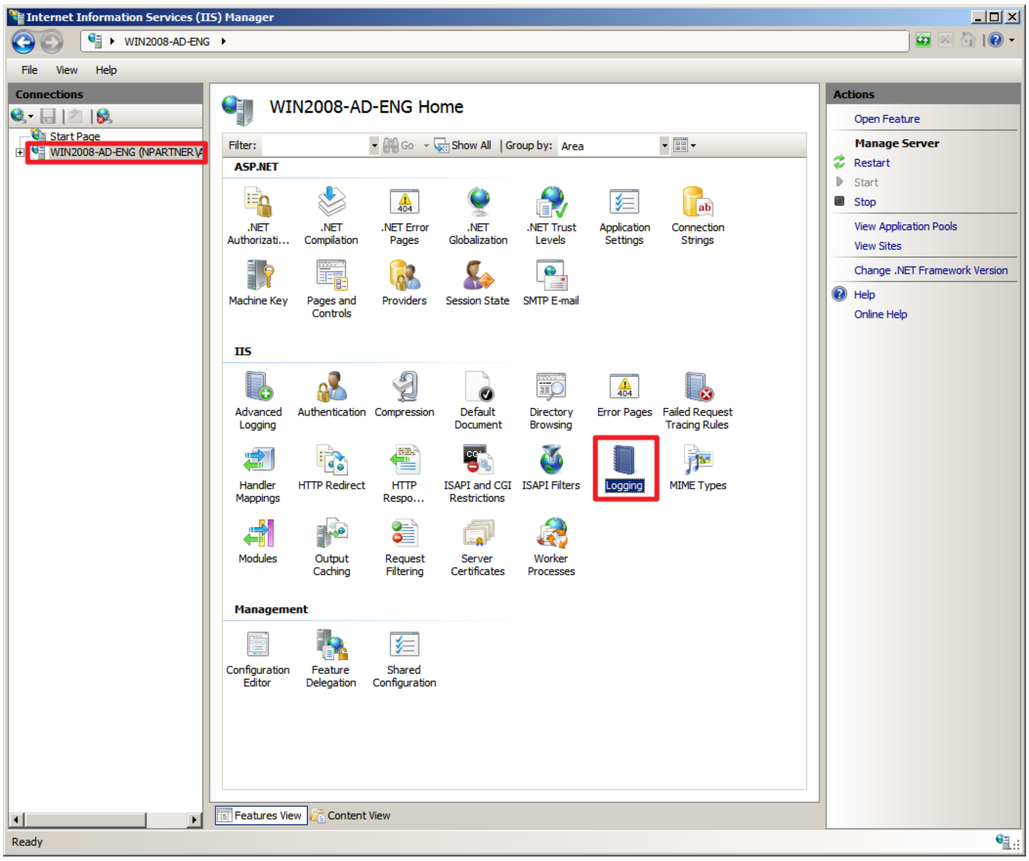
Microsoft Corporation (or based on where you live, one of its affiliates) licenses this supplement to you. If you are licensed to use Microsoft Windows Operating Systems software (for which this supplement is applicable) (the "software"), you may use this supplement. You may not use it if you do not have a license for

☑ I accept the terms in the License Agreement

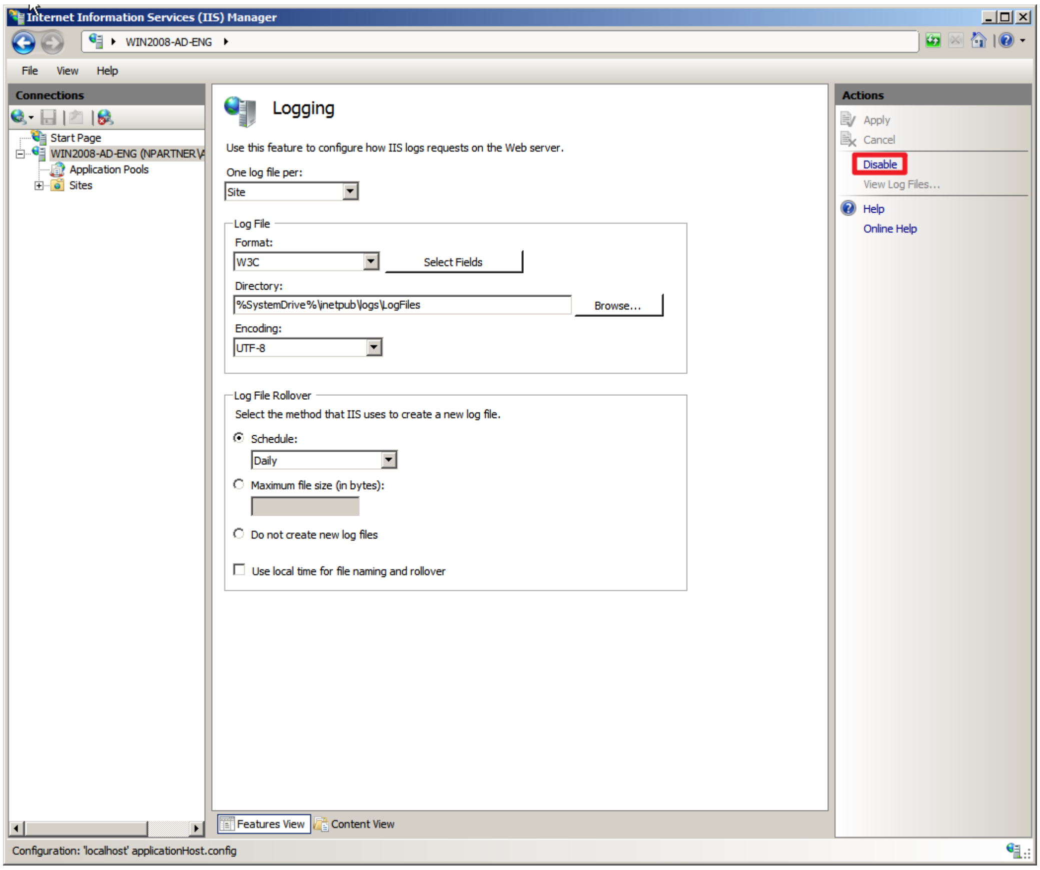
(2) Open “Internet Information Services (IIS) Manager.”



(3) Select “IIS Server” → “Logging.”



(4) Click “Disable.”



Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log File Rollover

Select the method that IIS uses to create a new log file.

● Schedule: Daily

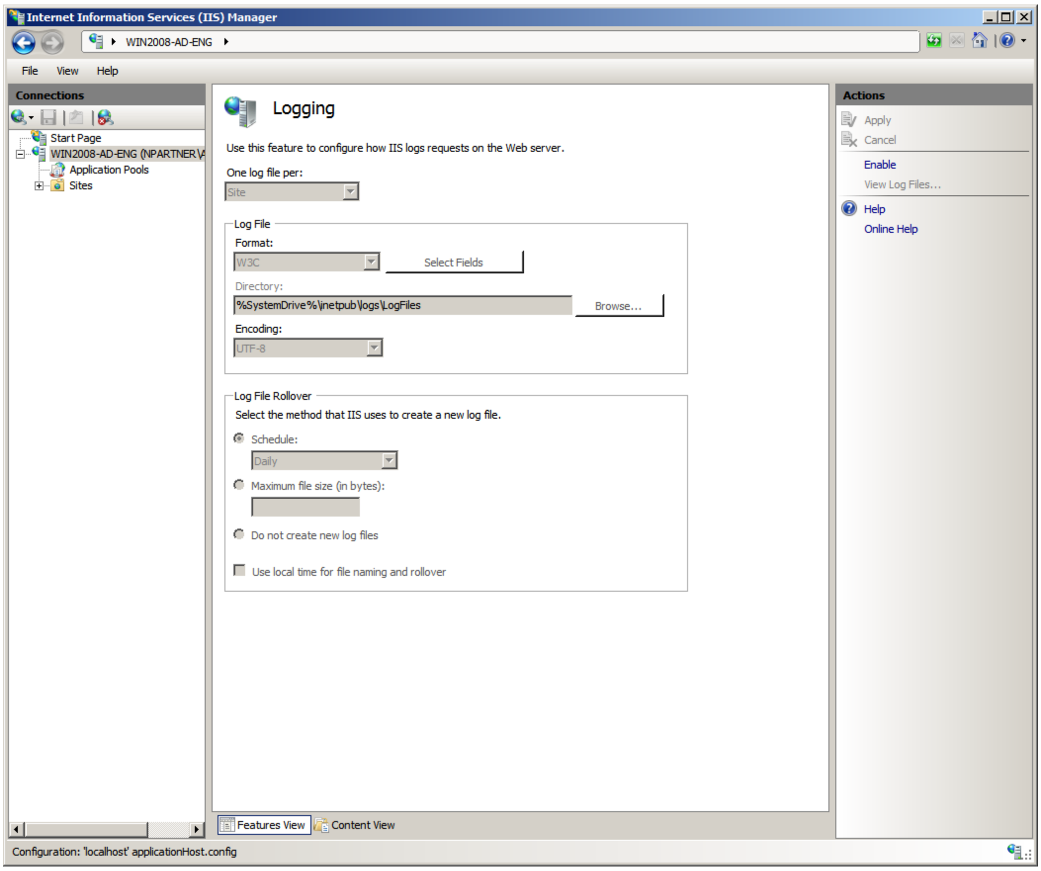
○ Maximum file size (in bytes):

○ Do not create new log files

□ Use local time for file naming and rollover

Configuration: 'localhost' applicationHost.config

(5) Verify that logging is disabled.



Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C Select Fields

Directory: %SystemDrive%\inetpub\logs\LogFiles Browse...

Encoding: UTF-8

Log File Rollover

Select the method that IIS uses to create a new log file.

● Schedule: Daily

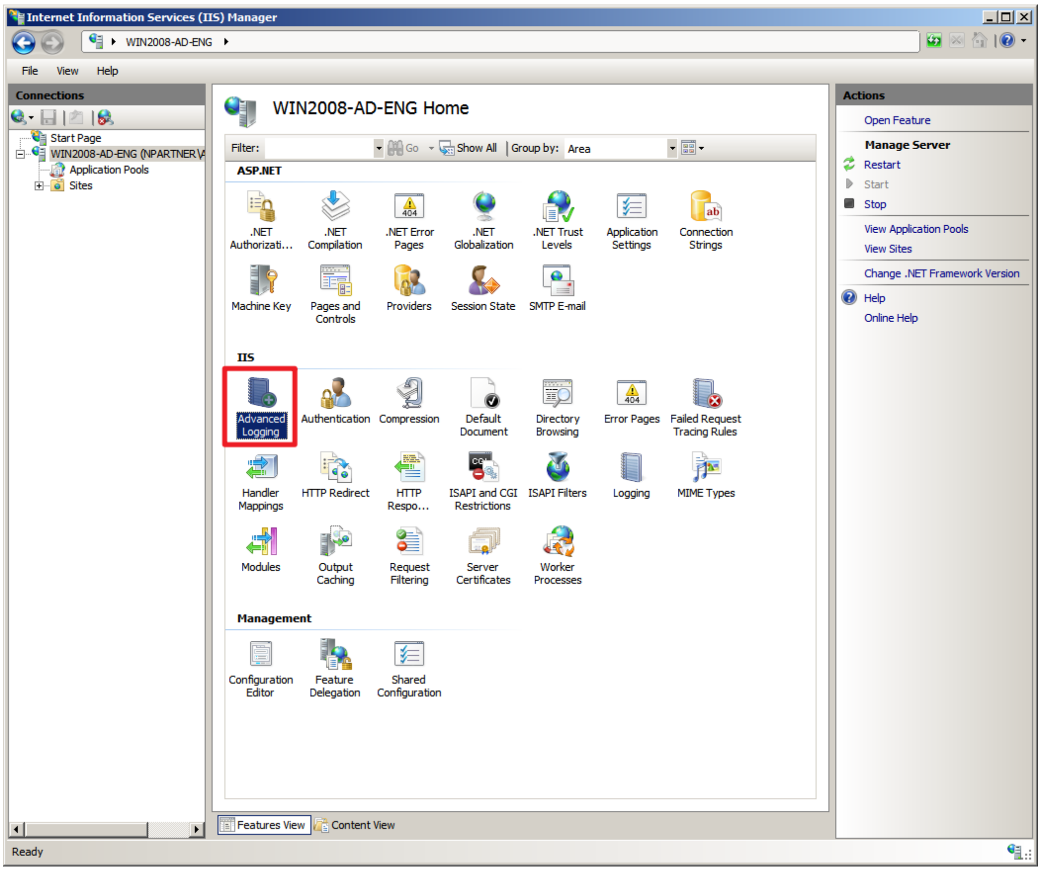
○ Maximum file size (in bytes):

○ Do not create new log files

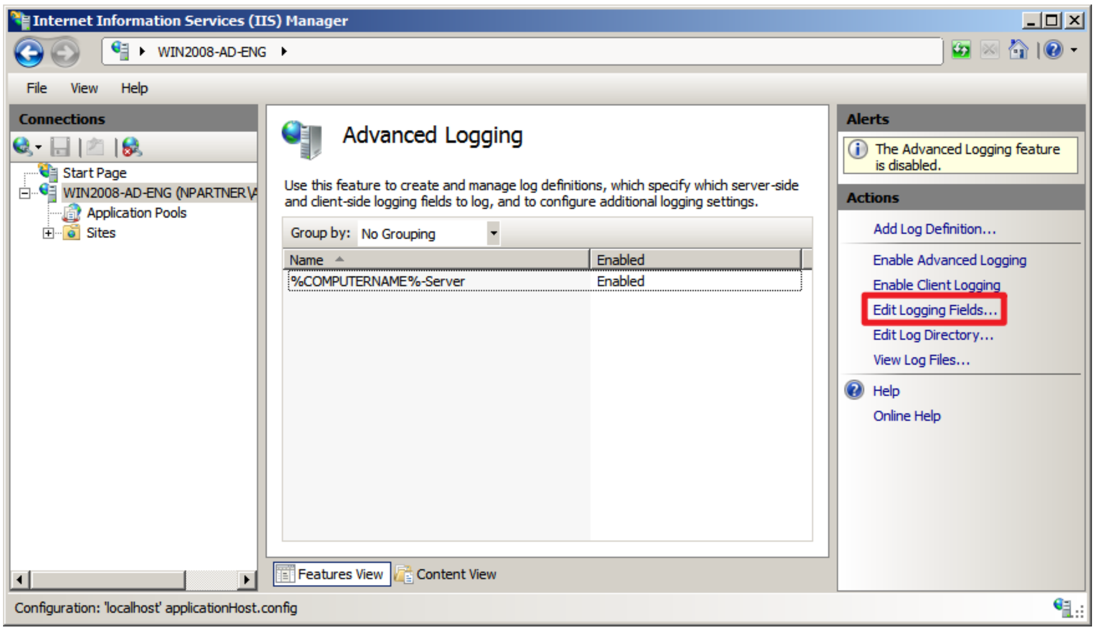
□ Use local time for file naming and rollover

Configuration: 'localhost' applicationHost.config

(6) Click “Advanced Logging.”



(7) Click “Edit Logging Fields.”



Advanced Logging

Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

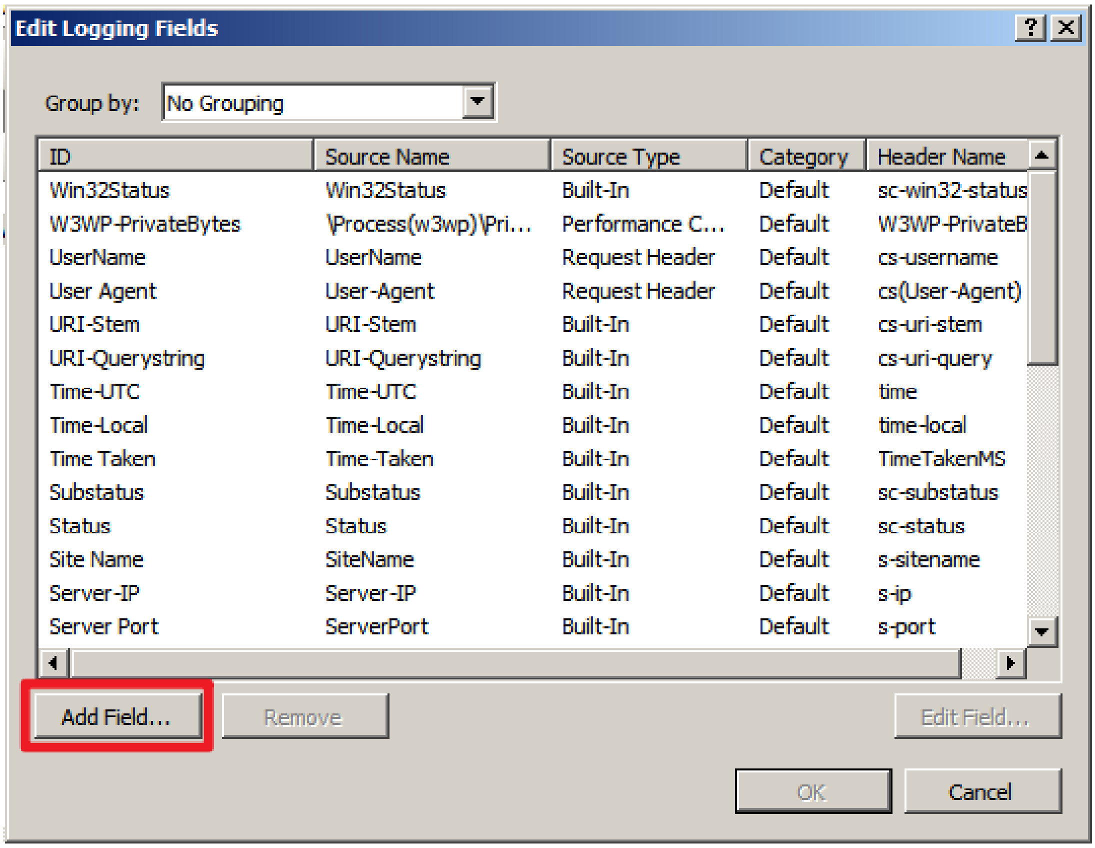
Group by: No Grouping

Name	Enabled
%COMPUTERNAME%-Server	Enabled

The Advanced Logging feature is disabled.

Configuration: 'localhost' applicationHost.config

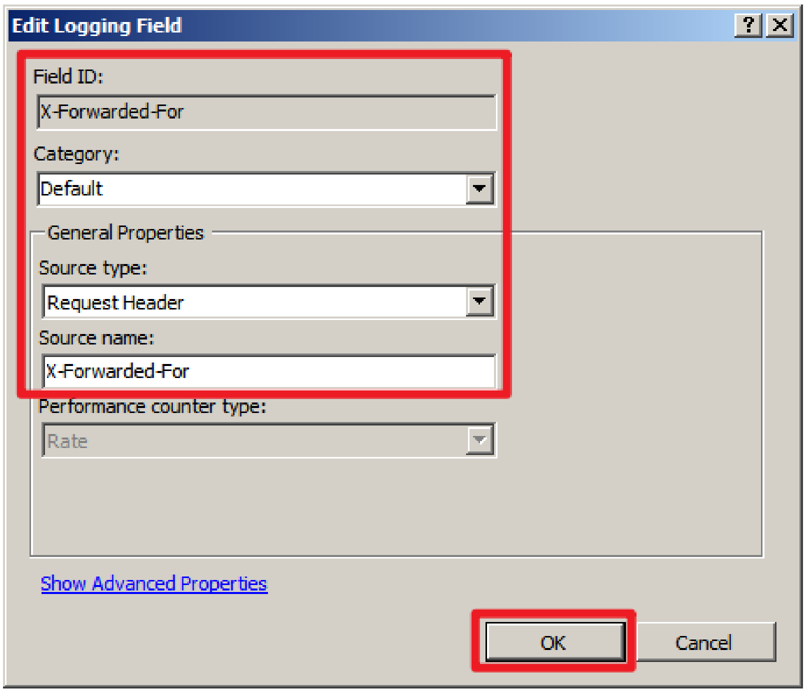
(8) Click “Add Field.”



Group by: No Grouping

ID	Source Name	Source Type	Category	Header Name
Win32Status	Win32Status	Built-In	Default	sc-win32-status
W3WP-PrivateBytes	\Process(w3wp)\Pri...	Performance C...	Default	W3WP-PrivateB
UserName	UserName	Request Header	Default	cs-username
User Agent	User-Agent	Request Header	Default	cs(User-Agent)
URI-Stem	URI-Stem	Built-In	Default	cs-uri-stem
URI-Querystring	URI-Querystring	Built-In	Default	cs-uri-query
Time-UTC	Time-UTC	Built-In	Default	time
Time-Local	Time-Local	Built-In	Default	time-local
Time Taken	Time-Taken	Built-In	Default	TimeTakenMS
Substatus	Substatus	Built-In	Default	sc-substatus
Status	Status	Built-In	Default	sc-status
Site Name	SiteName	Built-In	Default	s-sitename
Server-IP	Server-IP	Built-In	Default	s-ip
Server Port	ServerPort	Built-In	Default	s-port

(9) Enter field ID: X-Forwarded-For → select category: “Default” → source type: “Request Header” → enter source name: X-Forwarded-For → click “OK.”



Field ID: X-Forwarded-For

Category: Default

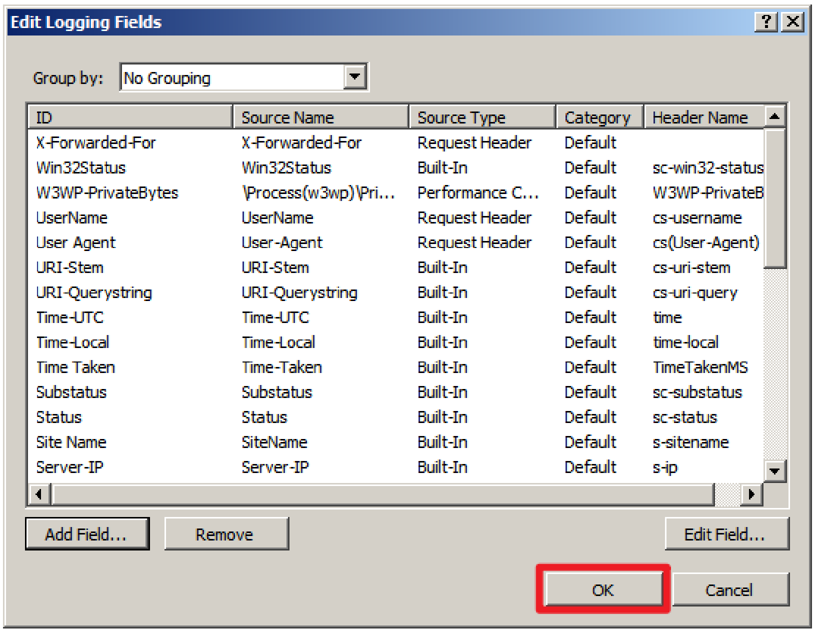
General Properties

Source type: Request Header

Source name: X-Forwarded-For

Performance counter type: Rate

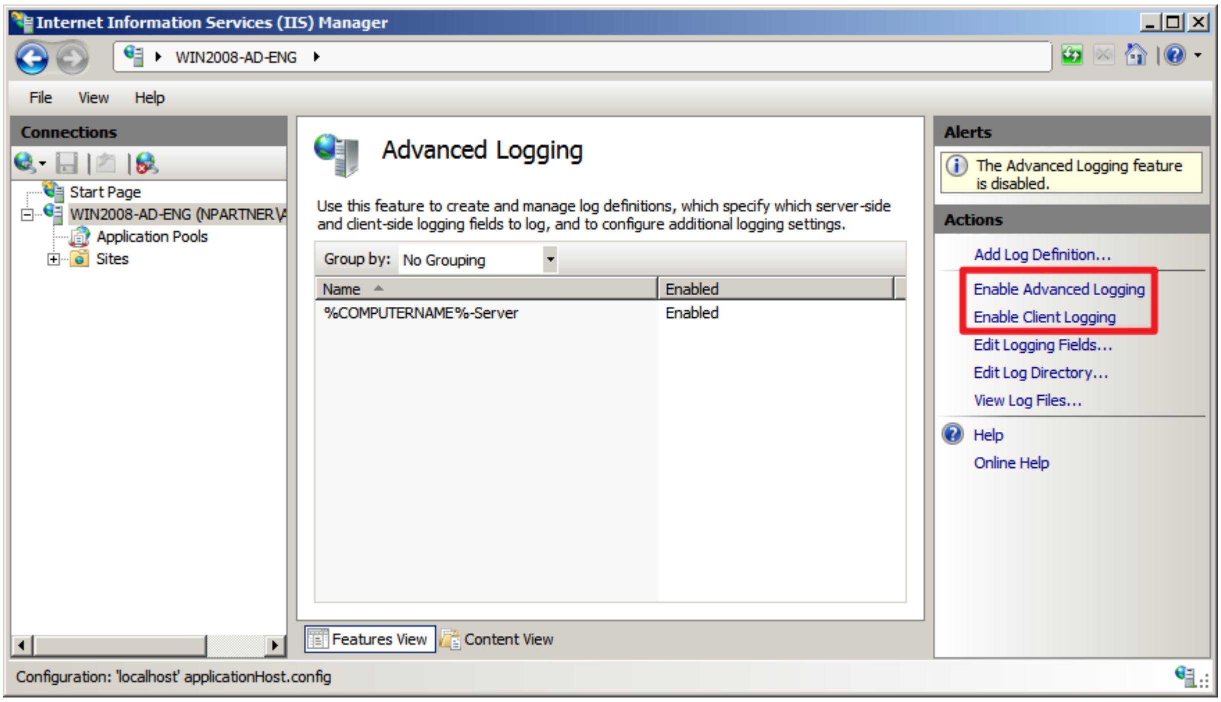
(10) Click “OK.”



Group by: No Grouping

ID	Source Name	Source Type	Category	Header Name
X-Forwarded-For	X-Forwarded-For	Request Header	Default	
Win32Status	Win32Status	Built-In	Default	sc-win32-status
W3WP-PrivateBytes	\Process(w3wp)\Pri...	Performance C...	Default	W3WP-PrivateB
UserName	UserName	Request Header	Default	cs-username
User Agent	User-Agent	Request Header	Default	cs(User-Agent)
URI-Stem	URI-Stem	Built-In	Default	cs-uri-stem
URI-Querystring	URI-Querystring	Built-In	Default	cs-uri-query
Time-UTC	Time-UTC	Built-In	Default	time
Time-Local	Time-Local	Built-In	Default	time-local
Time Taken	Time-Taken	Built-In	Default	TimeTakenMS
Substatus	Substatus	Built-In	Default	sc-substatus
Status	Status	Built-In	Default	sc-status
Site Name	SiteName	Built-In	Default	s-sitename
Server-IP	Server-IP	Built-In	Default	s-ip

(11) Click “Enable Advanced Logging” and “Enable Client Logging.”



Internet Information Services (IIS) Manager

Advanced Logging

Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

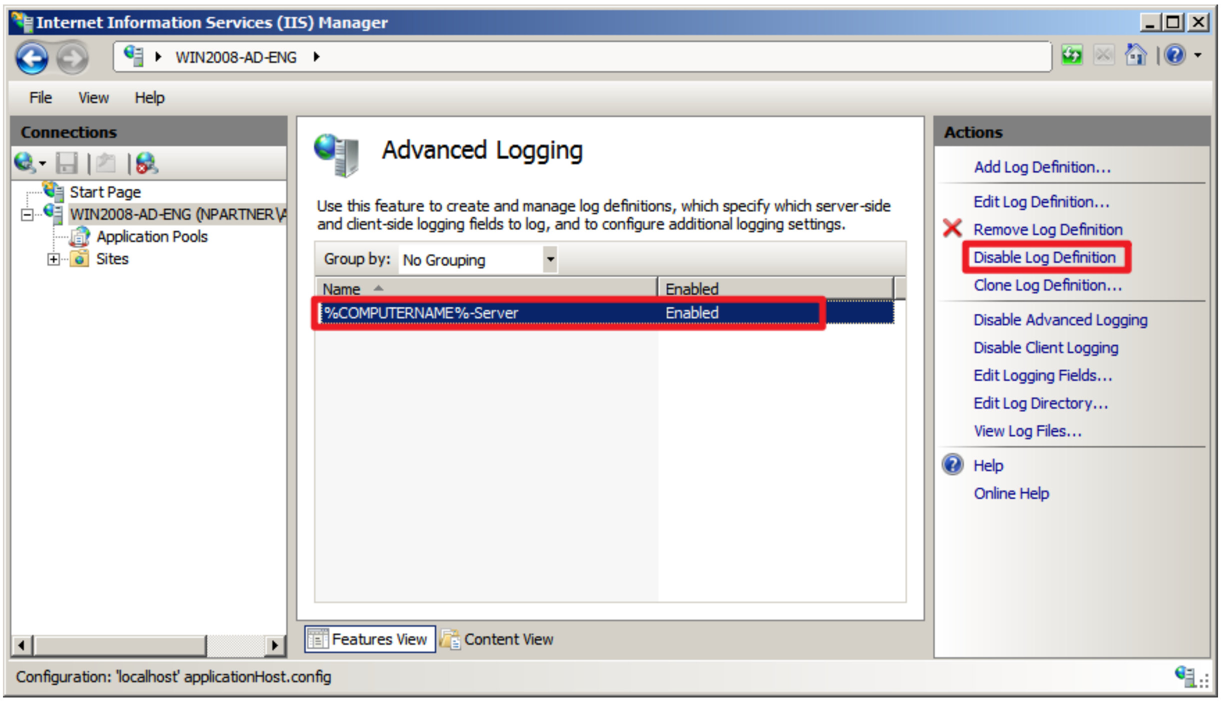
Group by: No Grouping

Name	Enabled
%COMPUTERNAME%-Server	Enabled

Alerts: The Advanced Logging feature is disabled.

Configuration: 'localhost' applicationHost.config

(12) Select “%COMPUTERNAME%-Server” → click “Disable Log Definition.”



Internet Information Services (IIS) Manager

Advanced Logging

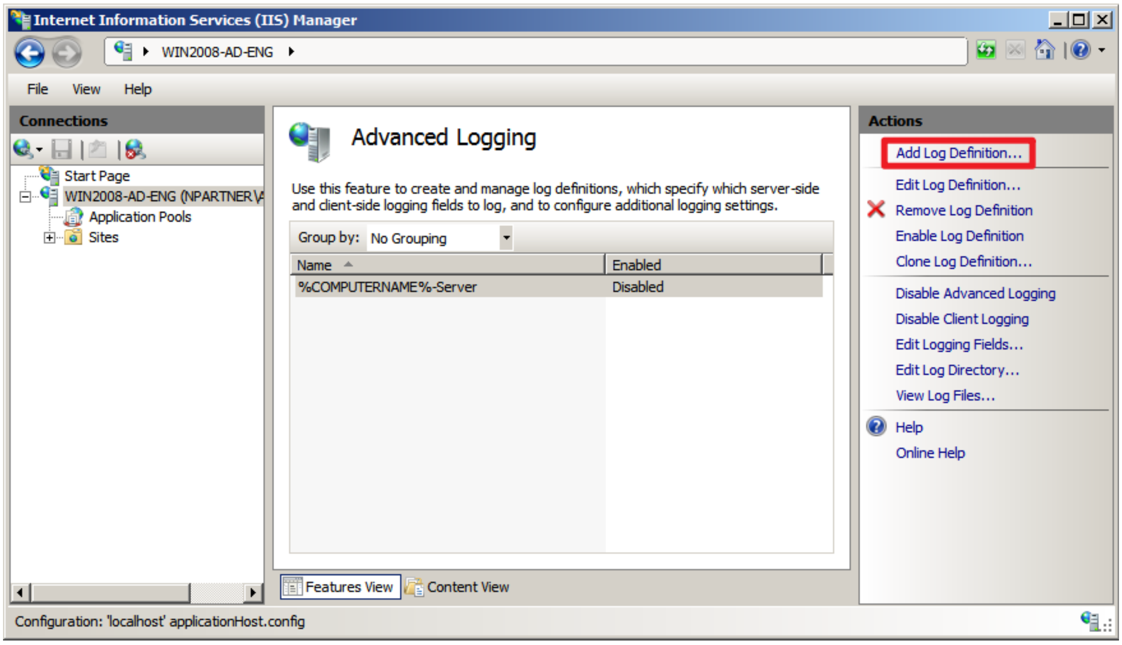
Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

Group by: No Grouping

Name	Enabled
%COMPUTERNAME%-Server	Enabled

Configuration: 'localhost' applicationHost.config

(13) Click “Add Log Definition.”



Internet Information Services (IIS) Manager

WIN2008-AD-ENG ▸

File View Help

Connections

- Start Page
- WIN2008-AD-ENG (NPARTNER\A
  - Application Pools
  - Sites

Advanced Logging

Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

Group by: No Grouping

Name	Enabled
%COMPUTERNAME%-Server	Disabled

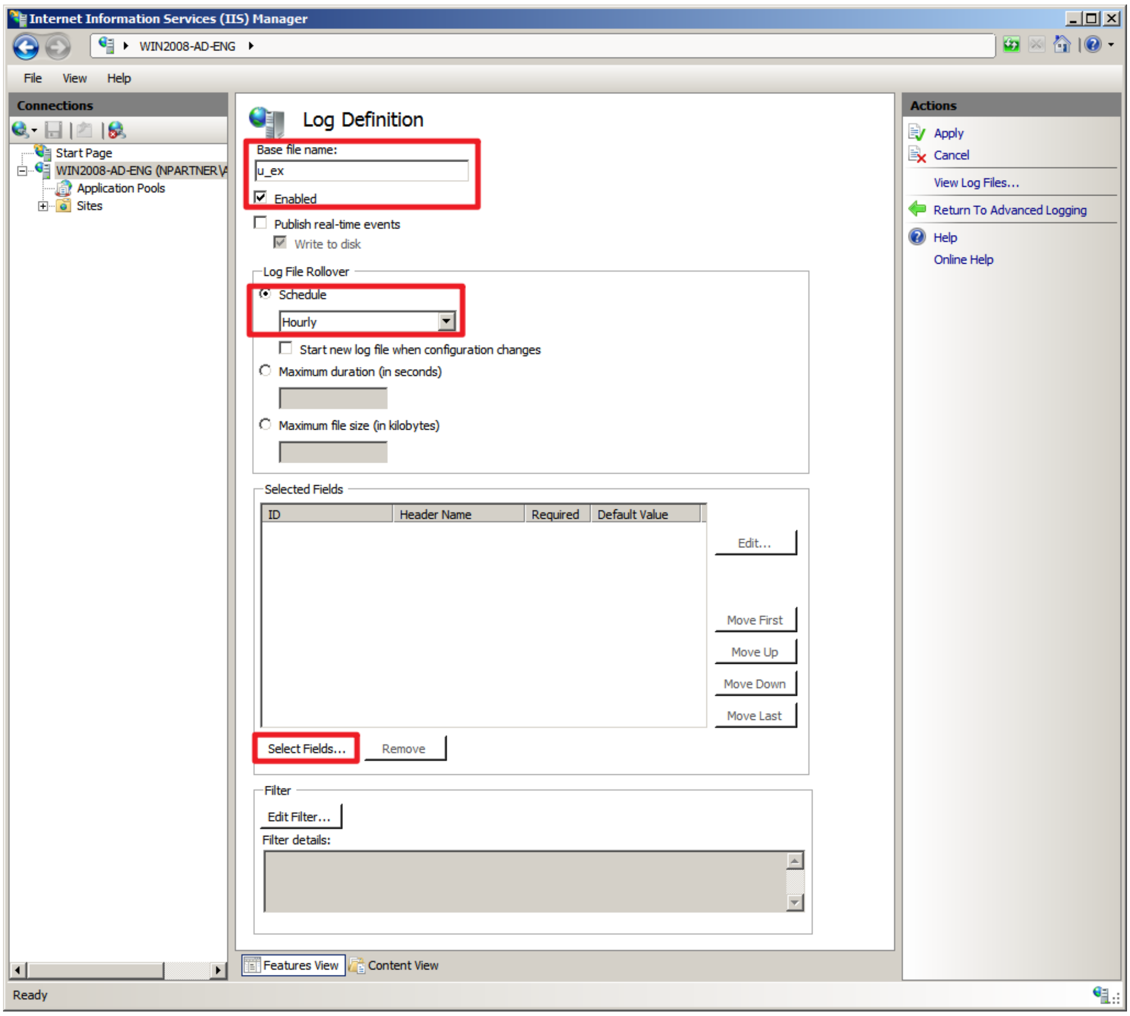
Features View | Content View

Actions

- Add Log Definition...
- Edit Log Definition...
- Remove Log Definition
- Enable Log Definition
- Clone Log Definition...
- Disable Advanced Logging
- Disable Client Logging
- Edit Logging Fields...
- Edit Log Directory...
- View Log Files...
- Help
- Online Help

Configuration: 'localhost' applicationHost.config

(14) Enter base file name: u_ex → check “Enabled” → select schedule: “Hourly” → click “Select Fields.”



Internet Information Services (IIS) Manager

WIN2008-AD-ENG ▸

File View Help

Connections

- Start Page
- WIN2008-AD-ENG (NPARTNER\A
  - Application Pools
  - Sites

Log Definition

Base file name:
u_ex

☑ Enabled

□ Publish real-time events

☑ Write to disk

Log File Rollover

● Schedule

Hourly

□ Start new log file when configuration changes

○ Maximum duration (in seconds)

○ Maximum file size (in kilobytes)

Selected Fields

ID	Header Name	Required	Default Value

Edit... Move First Move Up Move Down Move Last

Select Fields... Remove

Filter

Edit Filter...

Filter details:

Features View | Content View

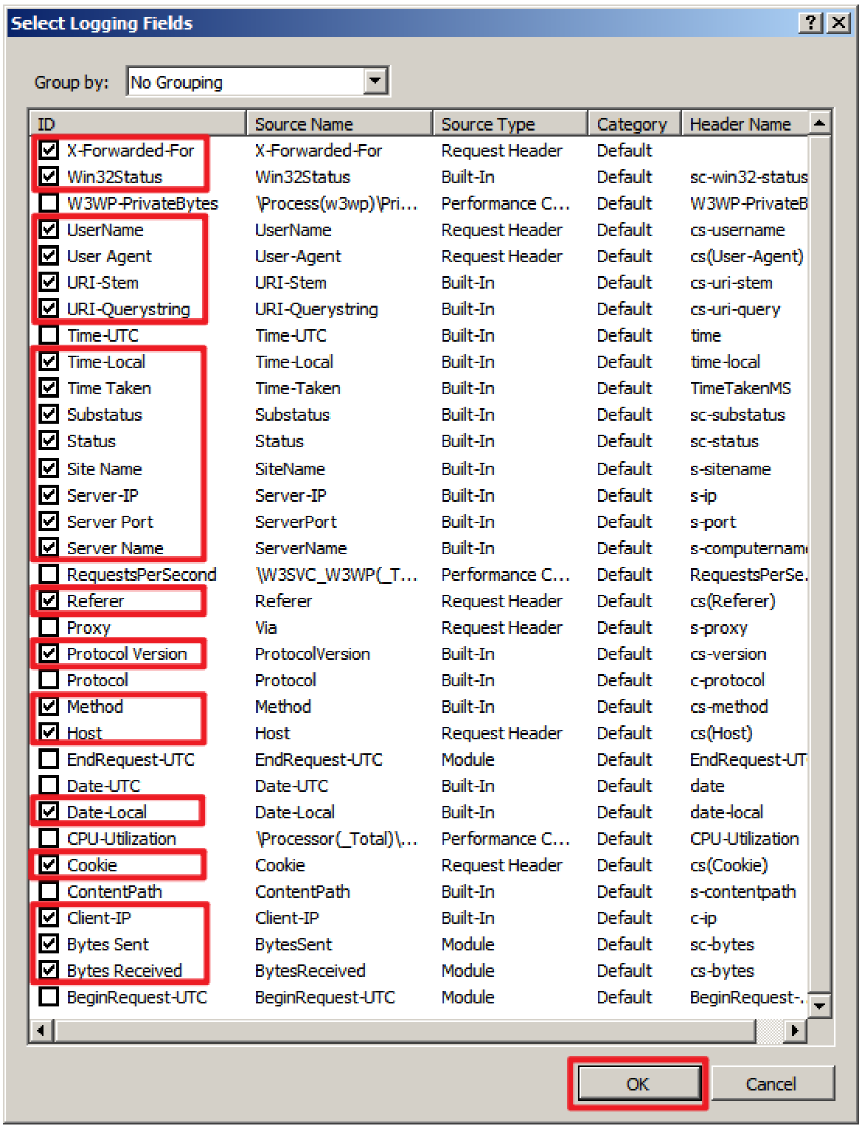
Actions

- Apply
- Cancel
- View Log Files...
- Return To Advanced Logging
- Help
- Online Help

Ready

(15) Select the following fields → click "OK":

X-Forwarded-For, Win32Status (sc-win32-status), UserName (cs-username), User Agent (cs(User-Agent)), URI-Stem (cs-uri-stem), URI-Querystring (cs-uri-query), Time-Local (time-local), Time Taken (TimeTakenMS), Substatus (sc-substatus), Status (sc-status), Site Name (s-sitename), Server-IP (s-ip), Server Port (s-port), Server Name (s-computername), Referrer (cs(Referer)), Protocol Version (cs-version), Method (cs-method), Host (cs-host), Date-Local (date-local), Cookie (cs(Cookie)), Client-IP (c-ip), Bytes Sent (sc-bytes), Bytes Received (cs-bytes).

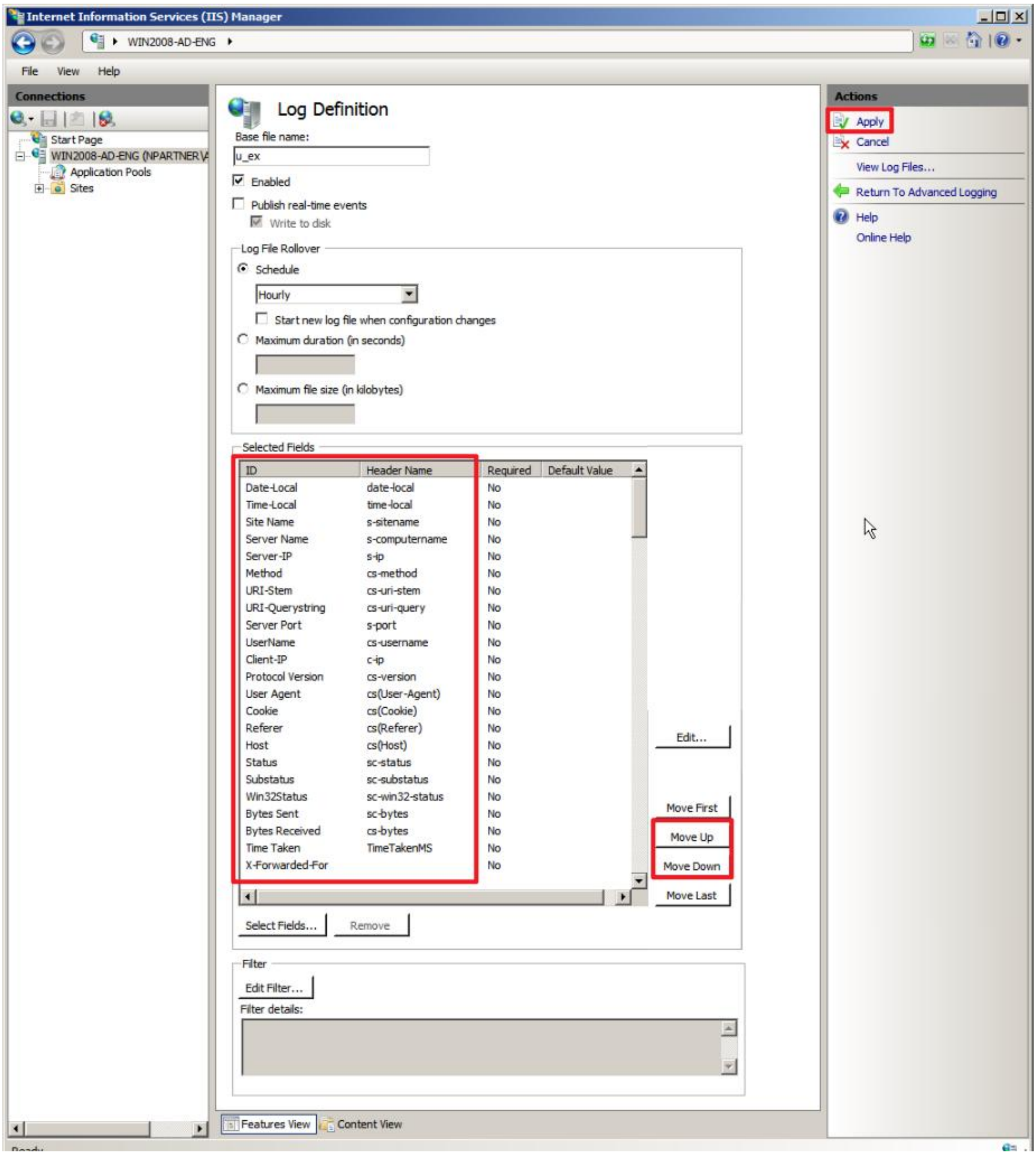


Select Logging Fields

Group by: No Grouping

ID	Source Name	Source Type	Category	Header Name
☑ X-Forwarded-For	X-Forwarded-For	Request Header	Default	
☑ Win32Status	Win32Status	Built-In	Default	sc-win32-status
□ W3WP-PrivateBytes	\Process(w3wp)\Pri...	Performance C...	Default	W3WP-PrivateB
☑ UserName	UserName	Request Header	Default	cs-username
☑ User Agent	User-Agent	Request Header	Default	cs(User-Agent)
☑ URI-Stem	URI-Stem	Built-In	Default	cs-uri-stem
☑ URI-Querystring	URI-Querystring	Built-In	Default	cs-uri-query
□ Time-UTC	Time-UTC	Built-In	Default	time
☑ Time-Local	Time-Local	Built-In	Default	time-local
☑ Time Taken	Time-Taken	Built-In	Default	TimeTakenMS
☑ Substatus	Substatus	Built-In	Default	sc-substatus
☑ Status	Status	Built-In	Default	sc-status
☑ Site Name	SiteName	Built-In	Default	s-sitename
☑ Server-IP	Server-IP	Built-In	Default	s-ip
☑ Server Port	ServerPort	Built-In	Default	s-port
☑ Server Name	ServerName	Built-In	Default	s-computernam
□ RequestsPerSecond	\W3SVC_W3WP(_T...	Performance C...	Default	RequestsPerSe.
☑ Referer	Referer	Request Header	Default	cs(Referer)
□ Proxy	Via	Request Header	Default	s-proxy
☑ Protocol Version	ProtocolVersion	Built-In	Default	cs-version
□ Protocol	Protocol	Built-In	Default	c-protocol
☑ Method	Method	Built-In	Default	cs-method
☑ Host	Host	Request Header	Default	cs(Host)
□ EndRequest-UTC	EndRequest-UTC	Module	Default	EndRequest-UT
□ Date-UTC	Date-UTC	Built-In	Default	date
☑ Date-Local	Date-Local	Built-In	Default	date-local
□ CPU-Utilization	\Processor(_Total)\...	Performance C...	Default	CPU-Utilization
☑ Cookie	Cookie	Request Header	Default	cs(Cookie)
□ ContentPath	ContentPath	Built-In	Default	s-contentpath
☑ Client-IP	Client-IP	Built-In	Default	c-ip
☑ Bytes Sent	BytesSent	Module	Default	sc-bytes
☑ Bytes Received	BytesReceived	Module	Default	cs-bytes
□ BeginRequest-UTC	BeginRequest-UTC	Module	Default	BeginRequest-.

(16) Adjust the selected fields: Date-Local (date-local), Time-Local (time-local), Site Name (s-sitename), Server Name (s-computername), Server-IP (s-ip), Method (cs-method), URI-Stem (cs-uri-stem), URI-Querystring (cs-uri-query), Server Port (s-port), UserName (cs-username), Client-IP (c-ip), Protocol Version (cs-version), User Agent (cs(User-Agent)), Cookie (cs(Cookie)), Referrer (cs(Referer)), Host (cs-host), Status (sc-status), Substatus (sc-substatus), Win32Status (sc-win32-status), Bytes Sent (sc-bytes), Bytes Received (cs-bytes), Time Taken (TimeTakenMS), X-Forwarded-For → click "Move Up" or "Move Down" → click "Apply."



Log Definition

Base file name:
u_ex

☑ Enabled

□ Publish real-time events

☑ Write to disk

Log File Rollover

● Schedule

Hourly

□ Start new log file when configuration changes

○ Maximum duration (in seconds)

○ Maximum file size (in kilobytes)

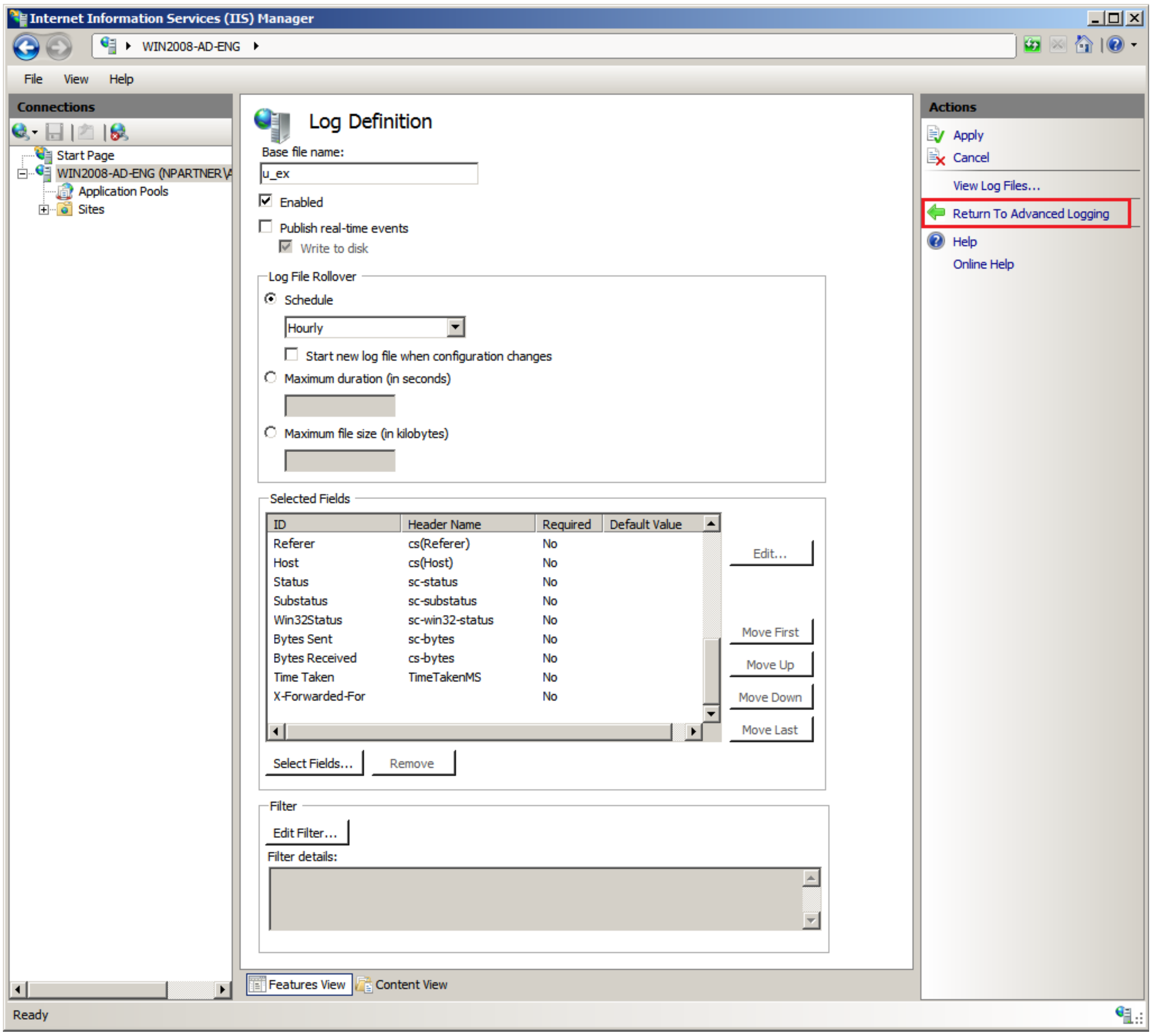
Selected Fields

ID	Header Name	Required	Default Value
Date-Local	date-local	No	
Time-Local	time-local	No	
Site Name	s-sitename	No	
Server Name	s-computername	No	
Server-IP	s-ip	No	
Method	cs-method	No	
URI-Stem	cs-uri-stem	No	
URI-Querystring	cs-uri-query	No	
Server Port	s-port	No	
UserName	cs-username	No	
Client-IP	c-ip	No	
Protocol Version	cs-version	No	
User Agent	cs(User-Agent)	No	
Cookie	cs(Cookie)	No	
Referer	cs(Referer)	No	
Host	cs(Host)	No	
Status	sc-status	No	
Substatus	sc-substatus	No	
Win32Status	sc-win32-status	No	
Bytes Sent	sc-bytes	No	
Bytes Received	cs-bytes	No	
Time Taken	TimeTakenMS	No	
X-Forwarded-For		No	

Filter

Filter details:

(17) Click “Return to Advanced Logging.”



Log Definition

Base file name: u_ex

☑ Enabled

☐ Publish real-time events

☑ Write to disk

Log File Rollover

● Schedule: Hourly

☐ Start new log file when configuration changes

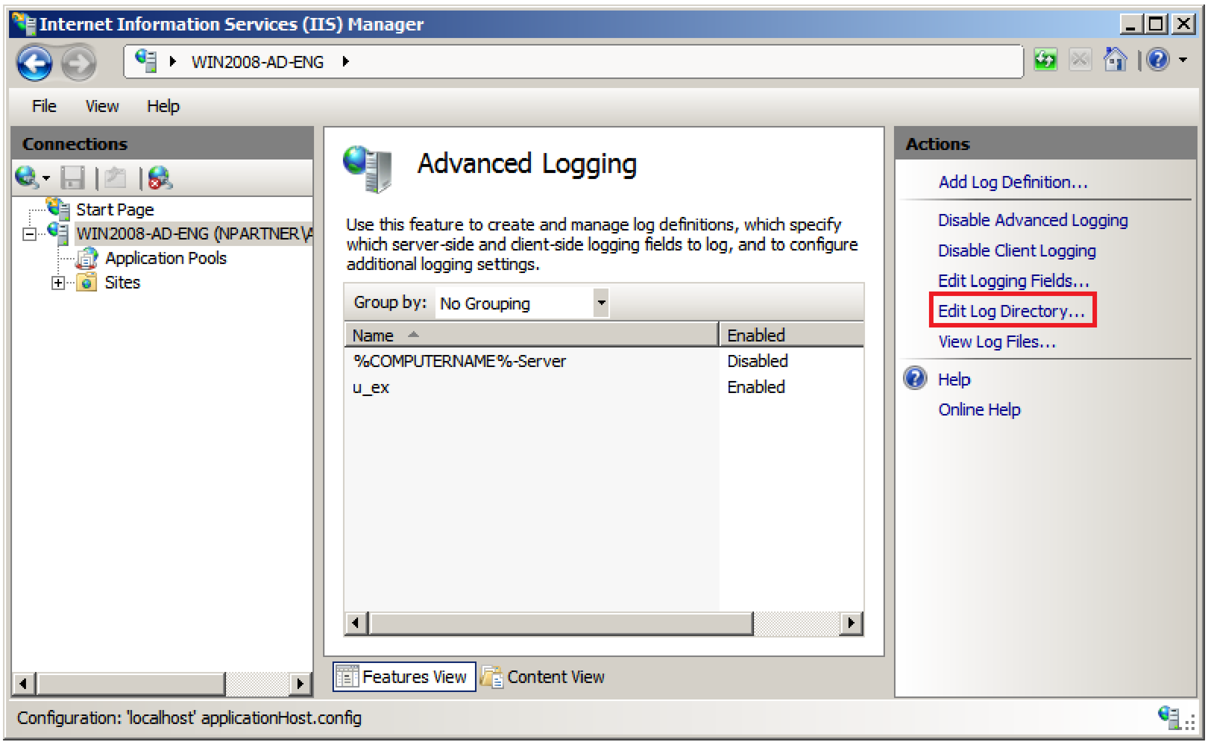
○ Maximum duration (in seconds)

○ Maximum file size (in kilobytes)

Selected Fields

ID	Header Name	Required	Default Value
Referer	cs(Referer)	No	
Host	cs(Host)	No	
Status	sc-status	No	
Substatus	sc-substatus	No	
Win32Status	sc-win32-status	No	
Bytes Sent	sc-bytes	No	
Bytes Received	cs-bytes	No	
Time Taken	TimeTakenMS	No	
X-Forwarded-For		No	

(18) Click “Edit Logging Directory.”



Advanced Logging

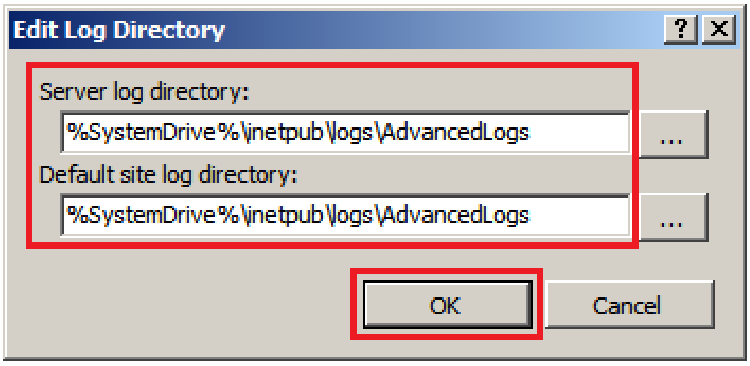
Use this feature to create and manage log definitions, which specify which server-side and client-side logging fields to log, and to configure additional logging settings.

Group by: No Grouping

Name	Enabled
%COMPUTERNAME%-Server	Disabled
u_ex	Enabled

Configuration: 'localhost' applicationHost.config

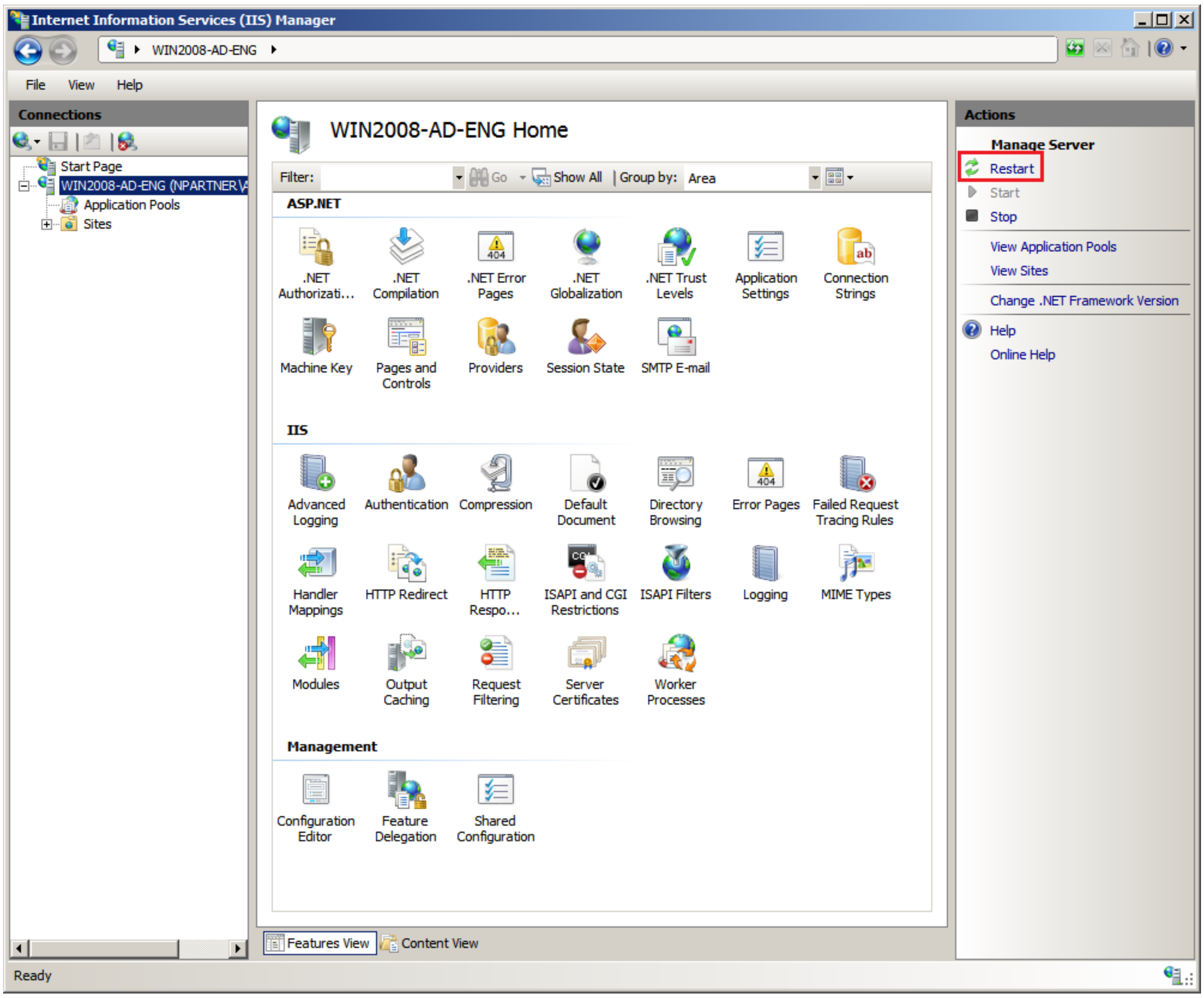
(19) Verify "Server Logging Directory" and "Default Web Site Logging Directory" paths → click "OK."



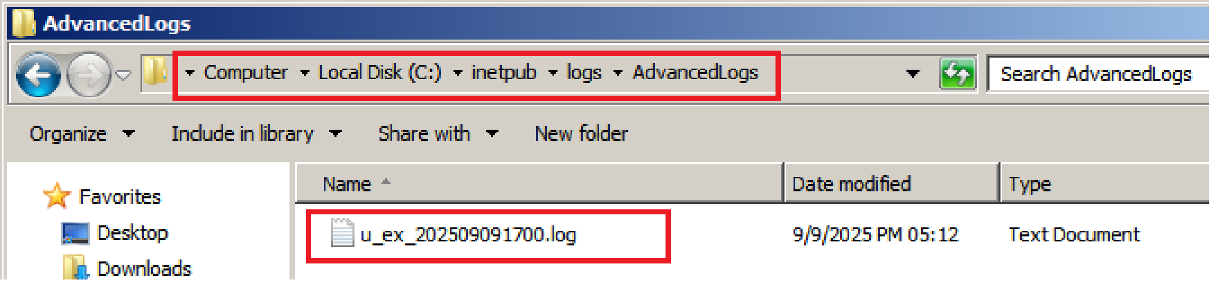
Server log directory:
%SystemDrive%\inetpub\logs\AdvancedLogs

Default site log directory:
%SystemDrive%\inetpub\logs\AdvancedLogs

(20) Click "Restart" IIS service.



(21) Verify IIS log files are created in the folder: C:\inetpub\logs\AdvancedLogs

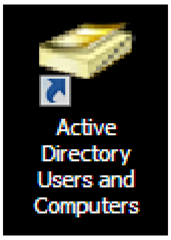


Name	Date modified	Type
u_ex_202509091700.log	9/9/2025 PM 05:12	Text Document

3.3 Event Log

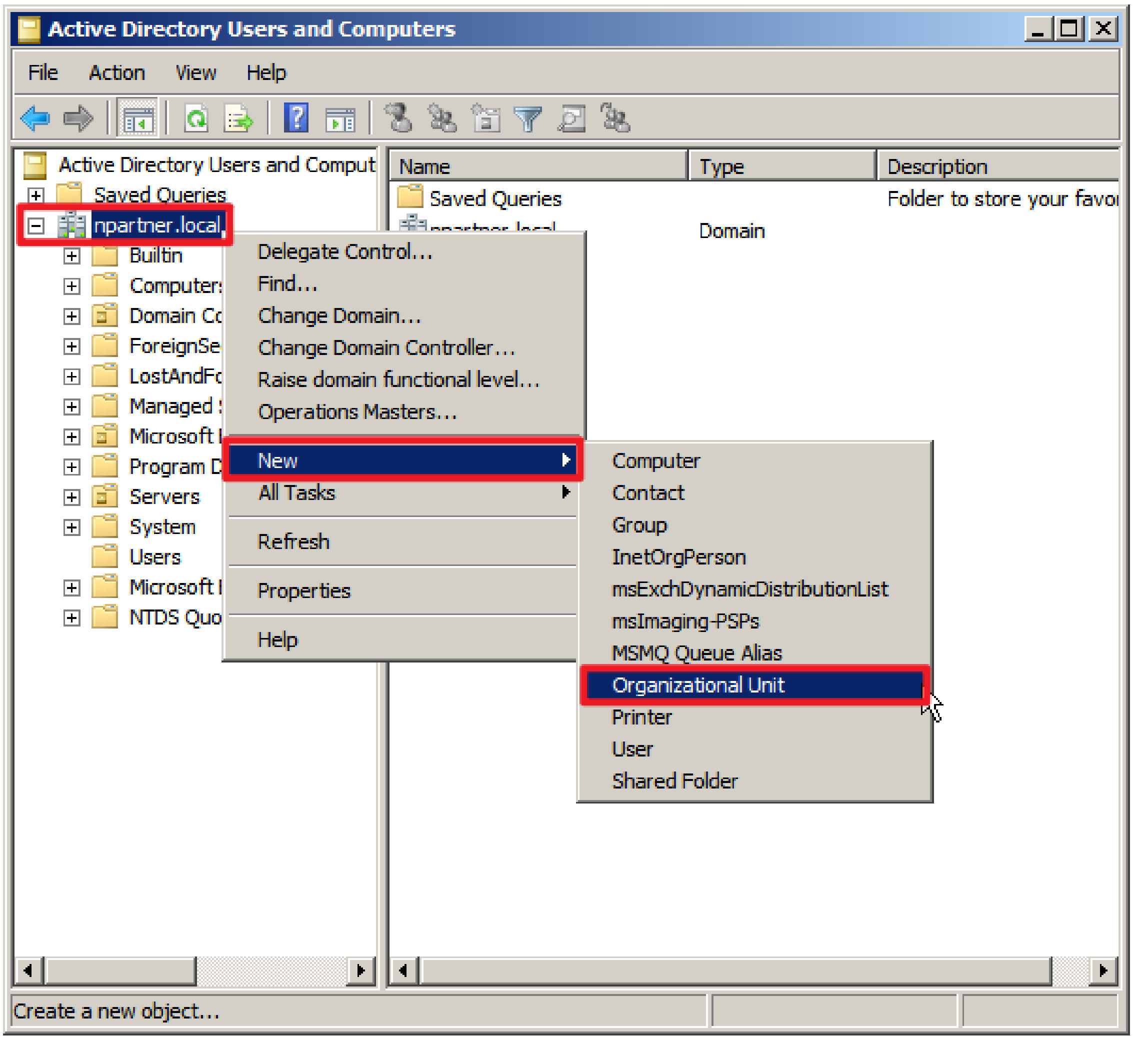
3.3.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”



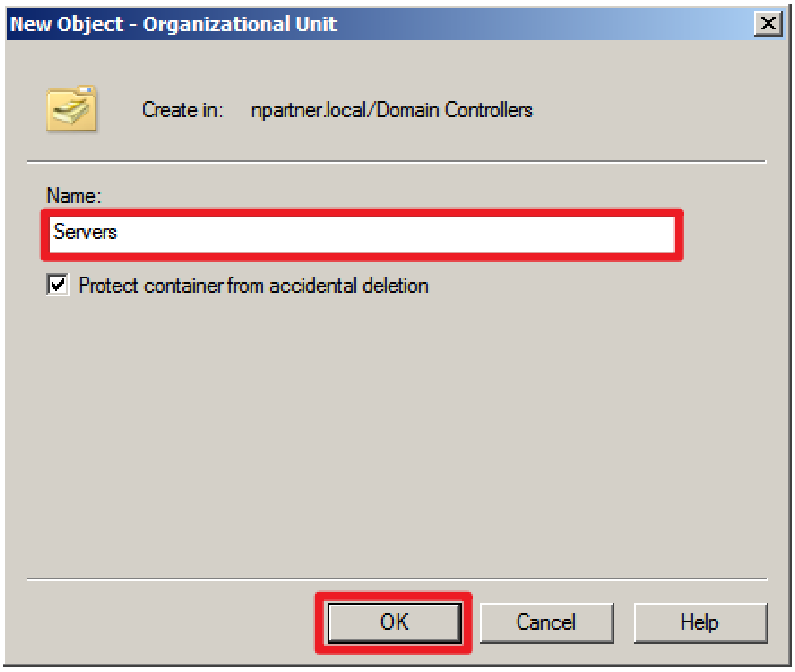
(2) Add an Organizational Unit

Right-click the “Domain Name” (the example here is npartner.local) → select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is "Servers")

Note: Please create the organizational unit name according to the actual environment. → click "OK."



New Object - Organizational Unit

Create in: npartner.local/Domain Controllers

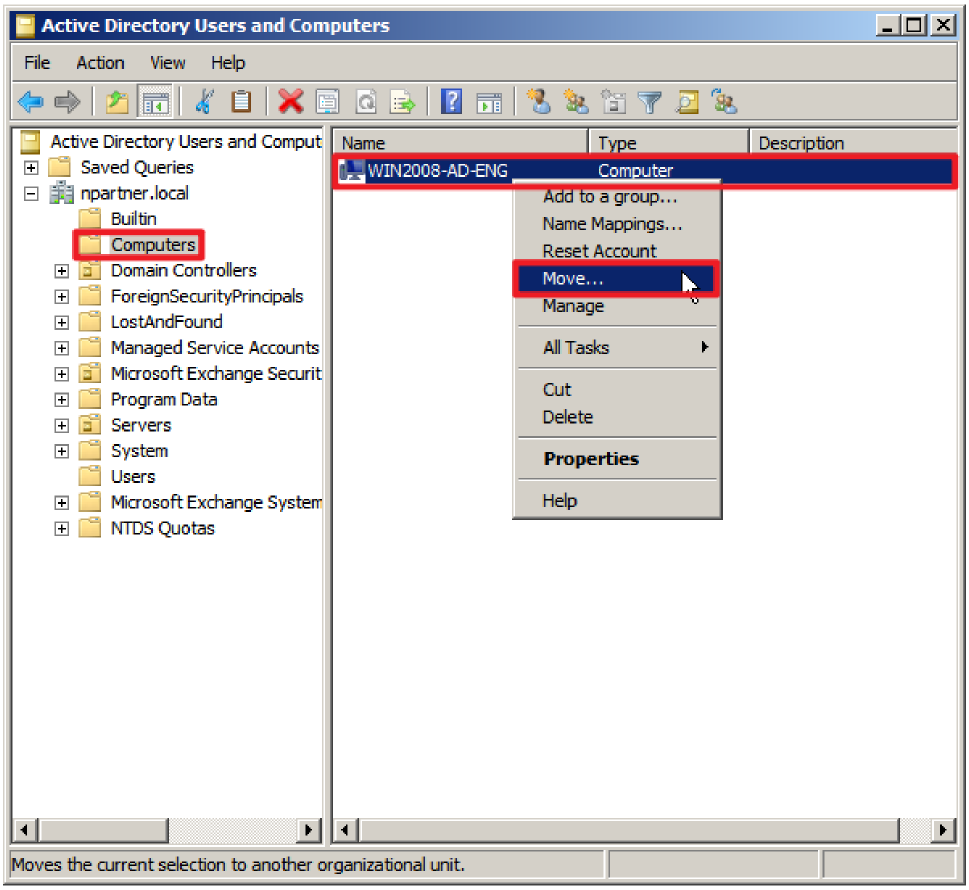
Name: Servers

☑ Protect container from accidental deletion

(4) Move the Server to your New Organizational Unit:

Select the "Computers" organizational unit (OU) → right-click on the "WIN2008-AD-ENG" server.

Note: Please select the Windows AD server according to the actual environment. → click "Move."

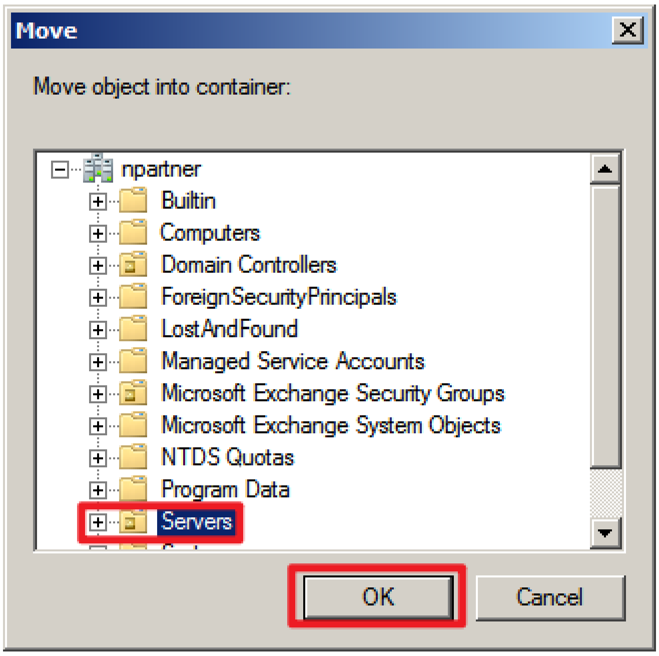


Name	Type	Description
WIN2008-AD-ENG	Computer	

Moves the current selection to another organizational unit.

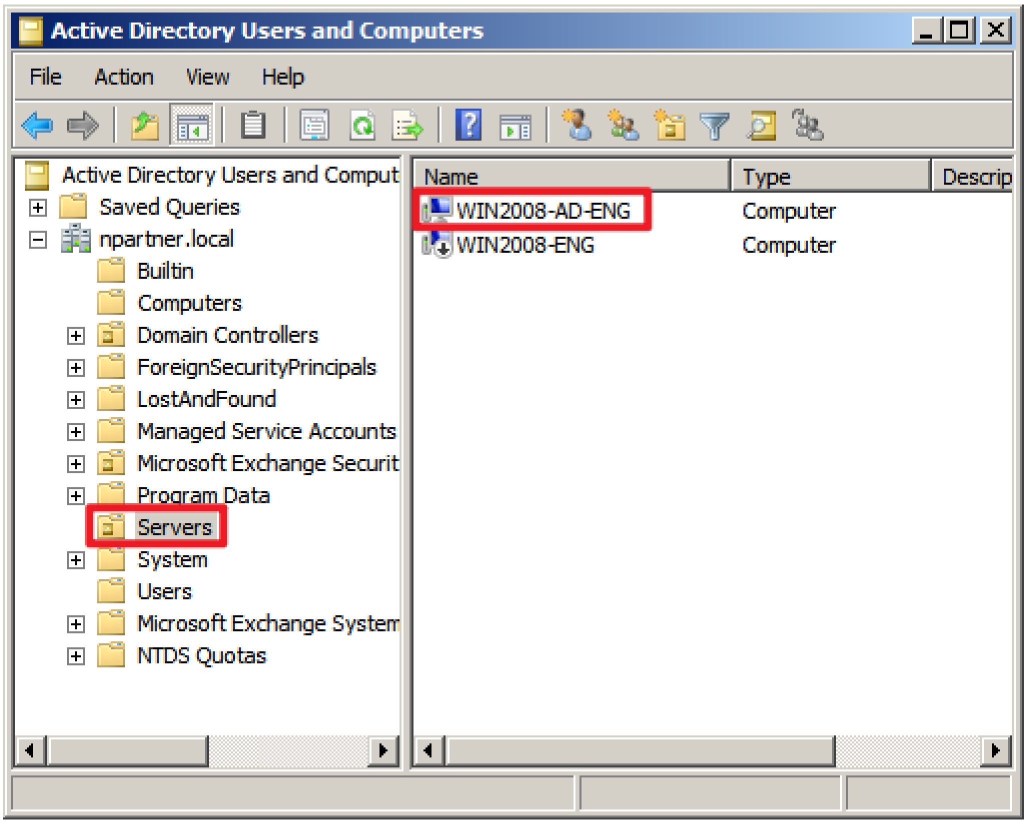
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) from the “Domain Controllers” → click “OK.”



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2008-AD-ENG” server has been moved.

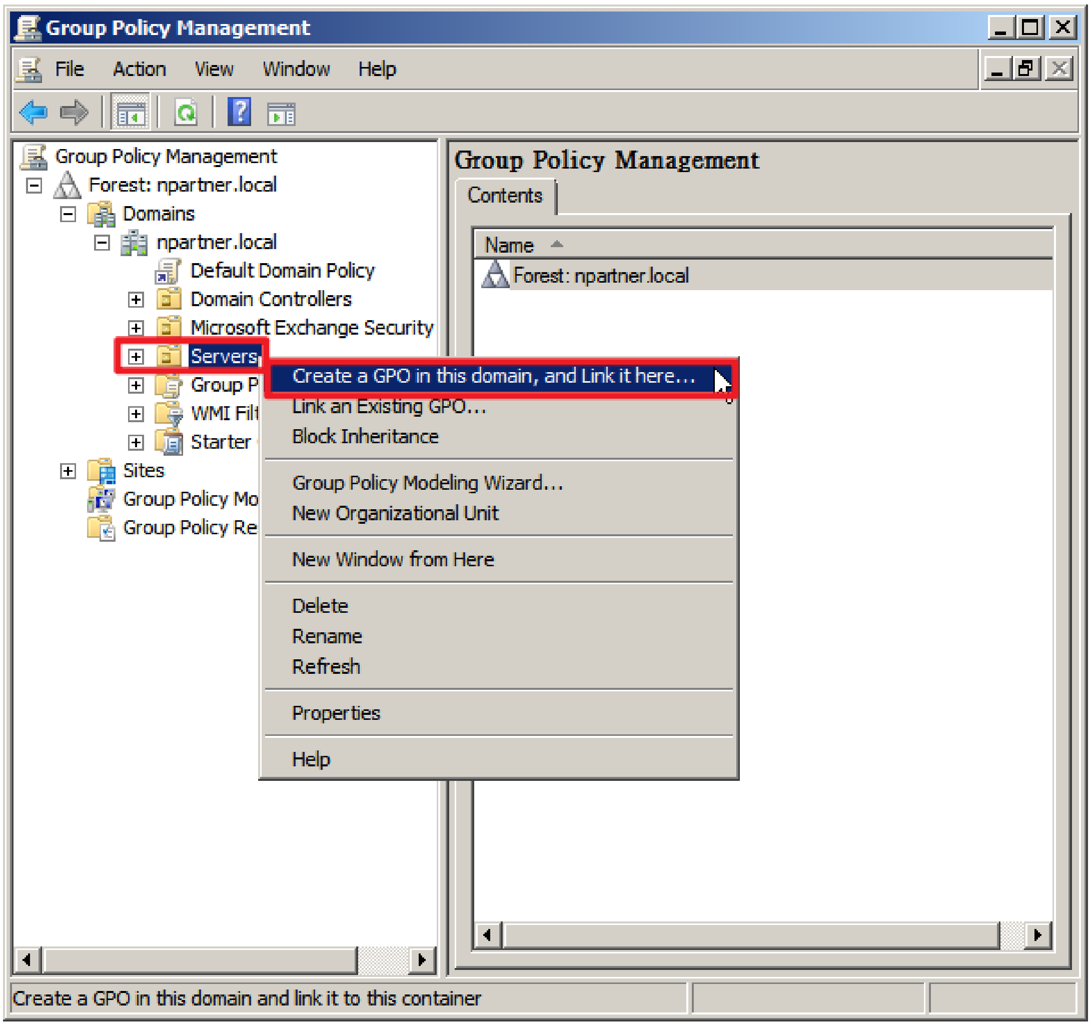


Name	Type	Descrip
WIN2008-AD-ENG	Computer	
WIN2008-ENG	Computer	

3.3.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) Right-click the “Servers” organizational unit (OU) and select “Create a GPO in this domain, and Link it here...”



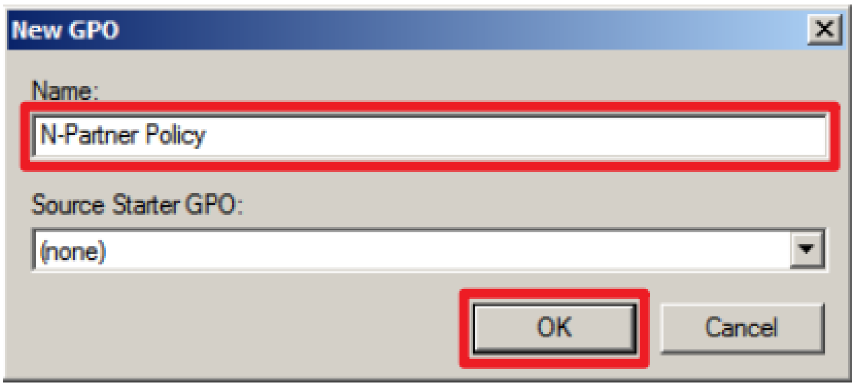
Create a GPO in this domain and link it to this container

(3) Enter the Group Policy Object (GPO) name

In your group policy object, (in this example, it is “N-Partner Policy”)

Note: Please create the GPO name according to the actual environment.

→ select “OK.”



New GPO

Name:

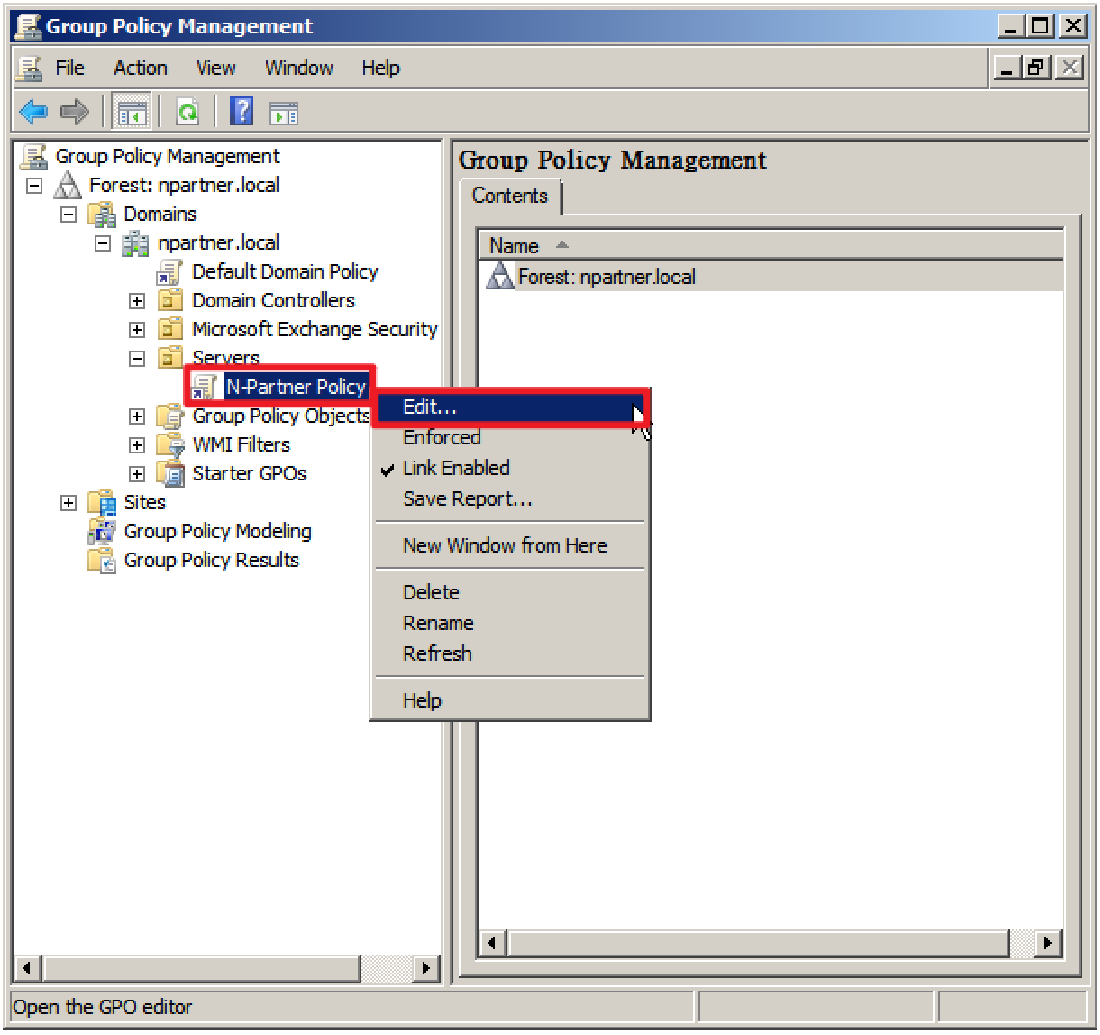
N-Partner Policy

Source Starter GPO:

(none)

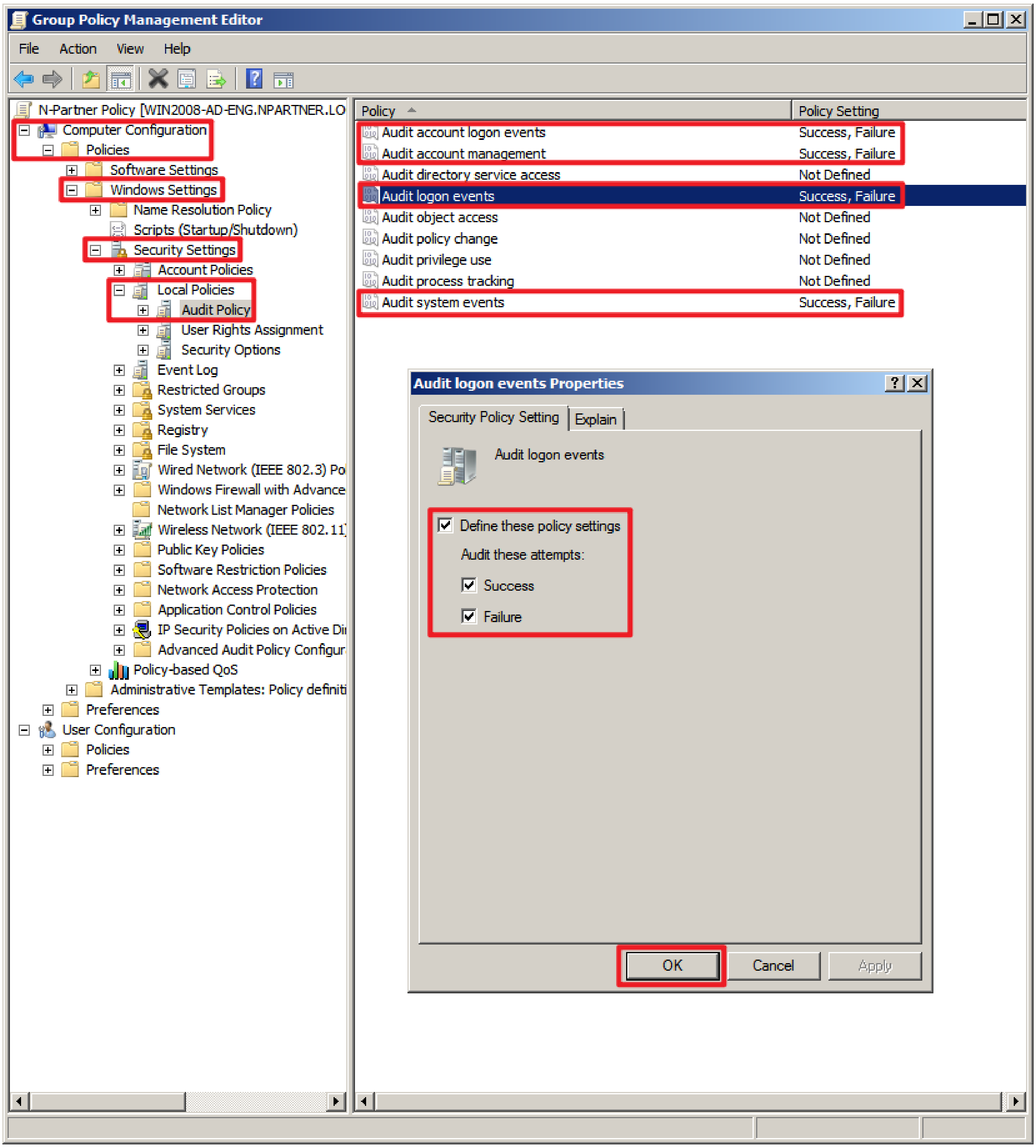
(4) Edit your Group Policy Object

Right-click the Group Policy Object (GPO) (in this example, it is “N-Partner Policy”) → select “Edit.”



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” and “Audit system events” → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Success, Failure

Audit logon events Properties

Audit logon events

☑ Define these policy settings

Audit these attempts:

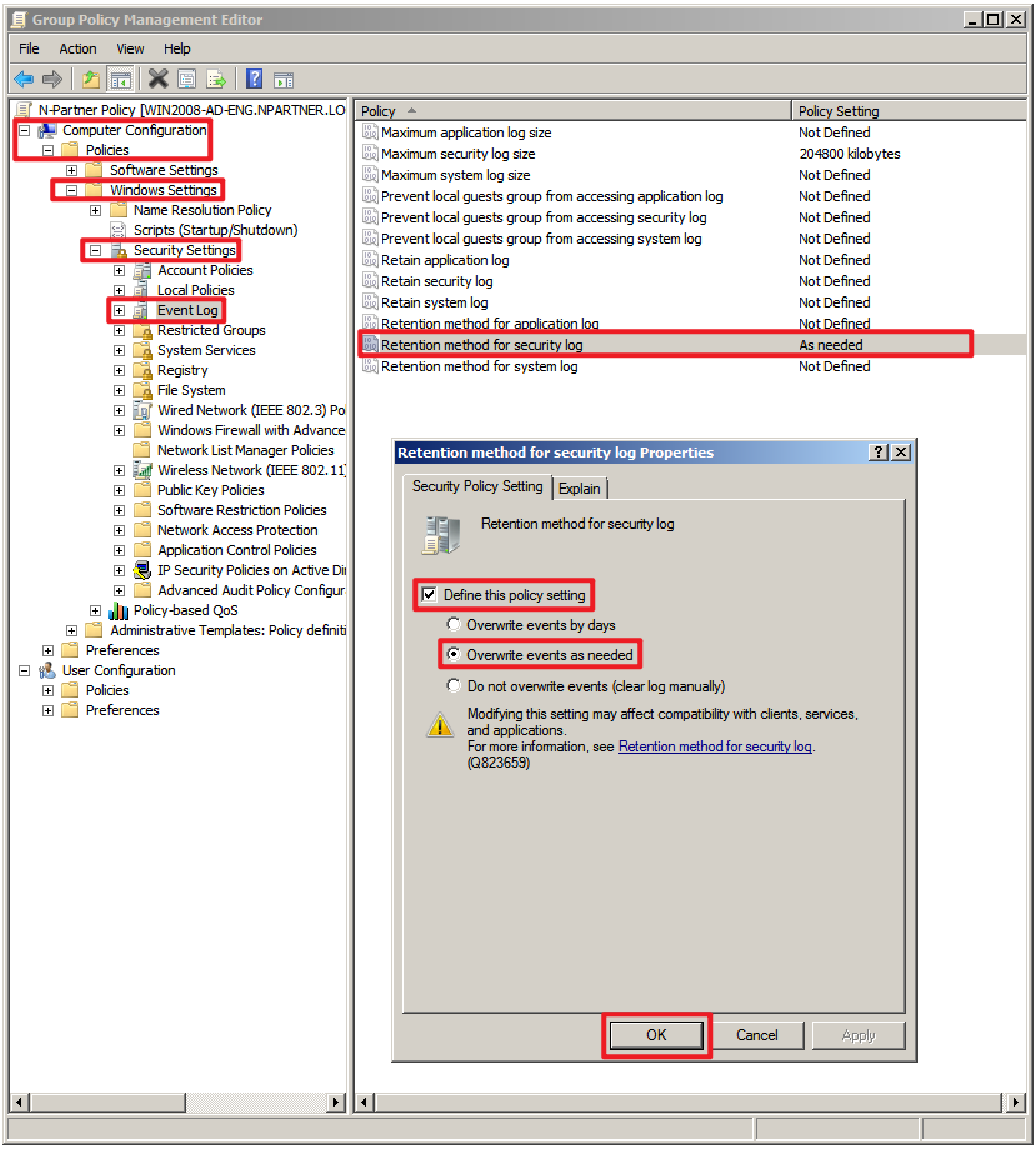
☑ Success

☑ Failure

Group Policy Management Editor
File Action View Help
N-Partner Policy [WIN2008-AD-ENG.NPARTNER.LO
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Di
Advanced Audit Policy Configur
Policy-based QoS
Administrative Templates: Policy definiti
Preferences
User Configuration
Policies
Preferences
Security Policy Setting
Explain
OK
Cancel
Apply

(6) Event Log: Security Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”


Group Policy Management Editor
File Action View Help
N-Partner Policy [WIN2008-AD-ENG.NPARTNER.LO
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Di
Advanced Audit Policy Configur
Policy-based QoS
Administrative Templates: Policy definiti
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Retention method for security log Properties

Security Policy Setting | Explain

Retention method for security log

☑ Define this policy setting

○ Overwrite events by days

● Overwrite events as needed

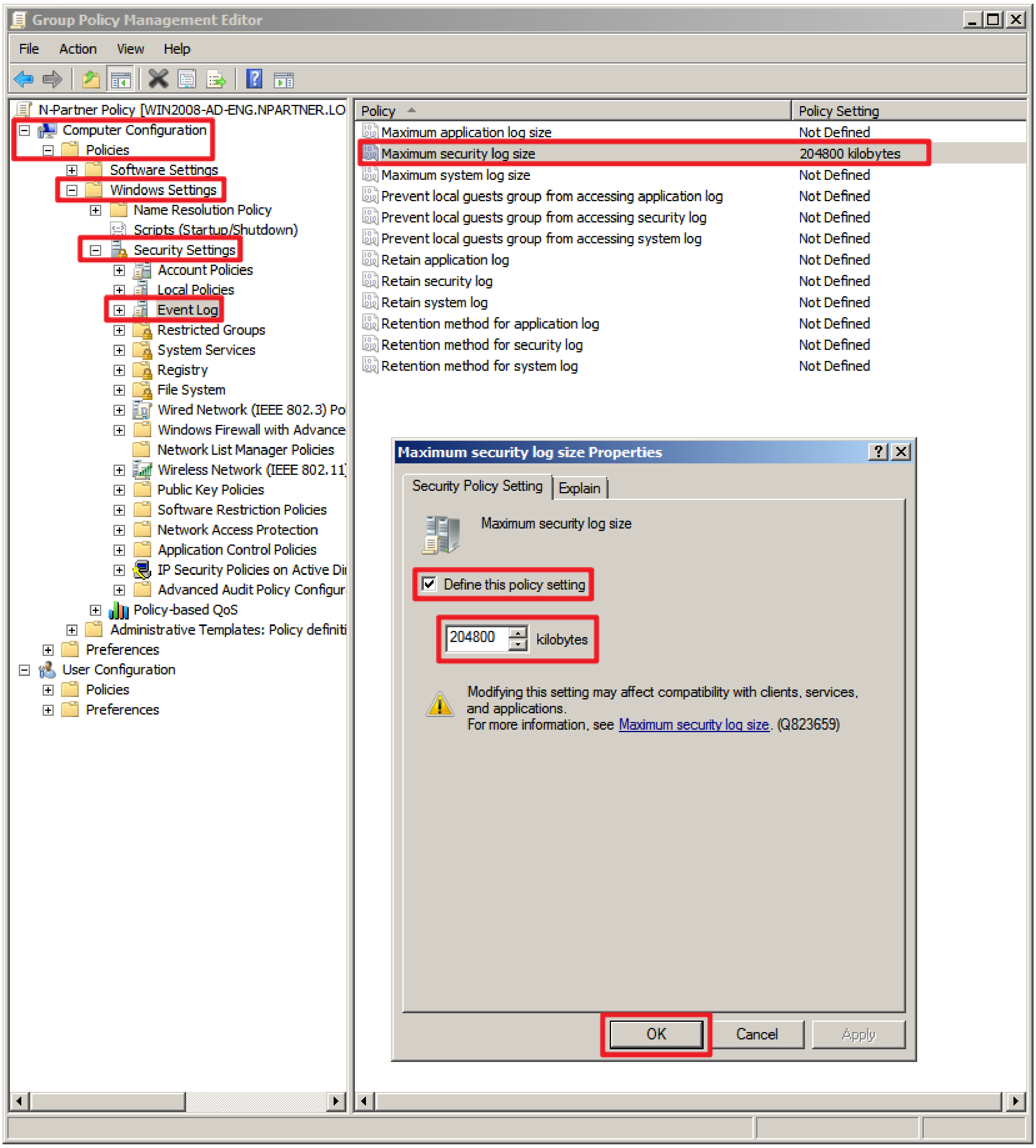
○ Do not overwrite events (clear log manually)

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Retention method for security log. (Q823659)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → and click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”


Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2008-AD-ENG.NPARTNER.LO
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Po
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Di
Advanced Audit Policy Configur
Policy-based QoS
Administrative Templates: Policy definiti
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum security log size Properties

Security Policy Setting | Explain

Maximum security log size

☑ Define this policy setting

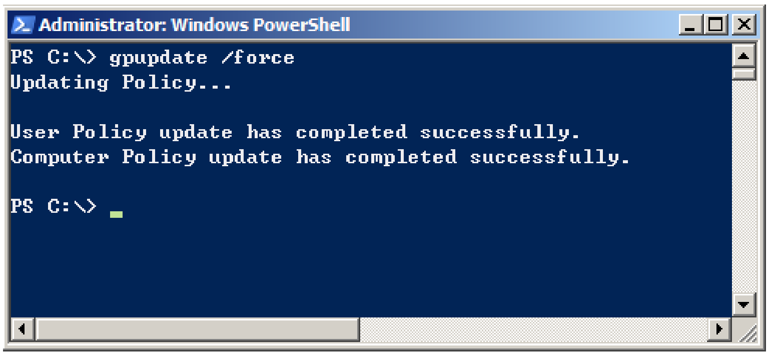
204800 kilobytes

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Maximum security log size. (Q823659)

(8) On the Exchange server, open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

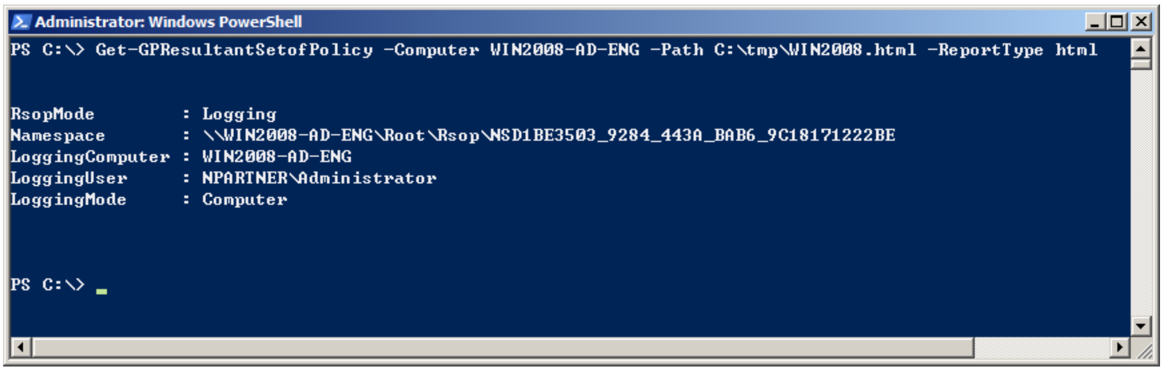
```
PS C:\> gpupdate /force
```



```
PS C:\> gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

PS C:\> _
```

(10) On the server, open “Windows PowerShell” → enter the command below to generate the group policy report for the Windows File server.

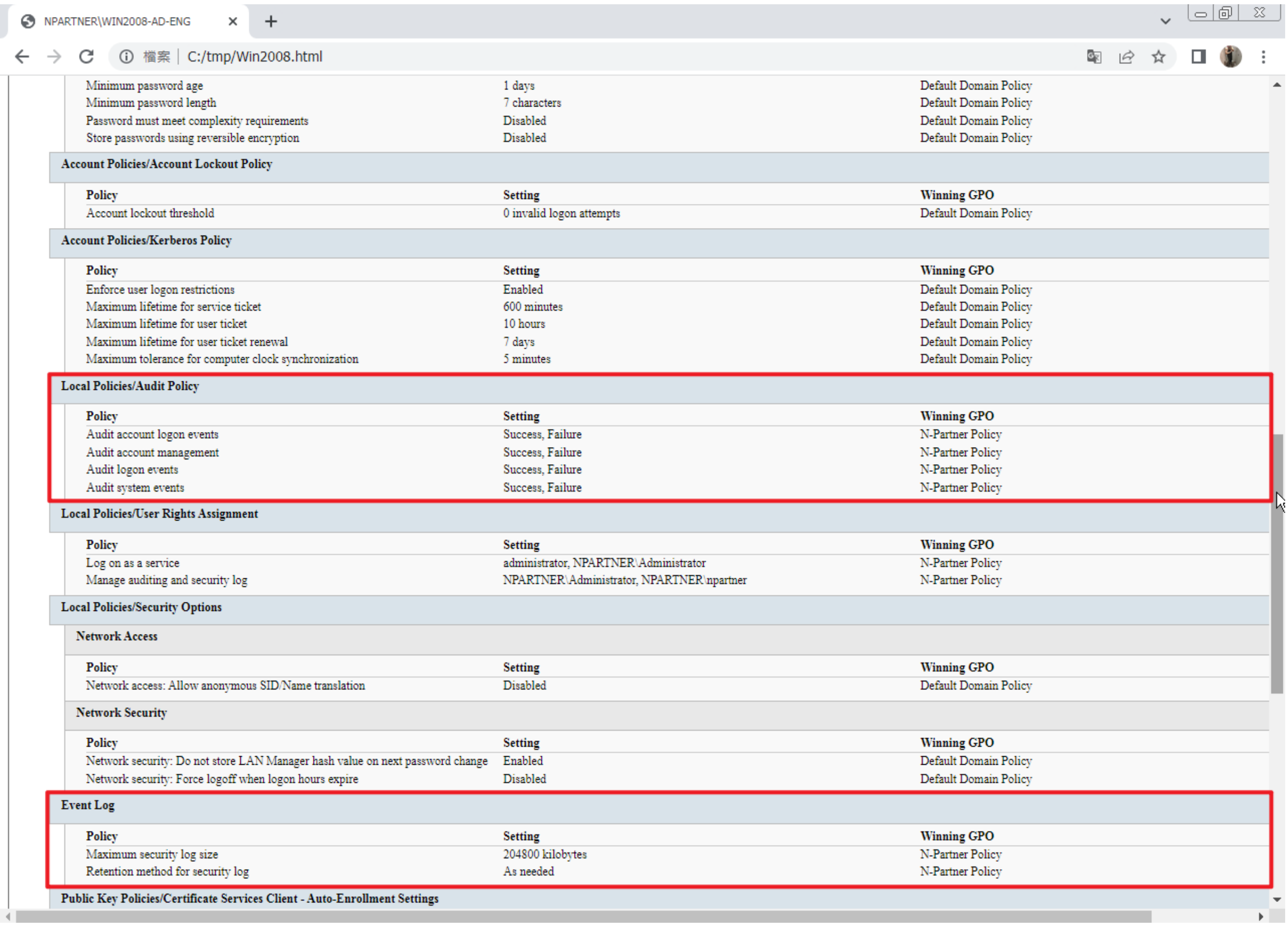
```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2008 -Path C:\tmp\Win2008.html -ReportType html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2008-AD-ENG -Path C:\tmp\WIN2008.html -ReportType html


RsopMode         : Logging
Namespace        : \\WIN2008-AD-ENG\Root\Rsop\NSD1BE3503_9284_443A_BAB6_9C18171222BE
LoggingComputer  : WIN2008-AD-ENG
LoggingUser      : NPARTNER\Administrator
LoggingMode      : Computer


PS C:\> _
```

Replace the text shown in red with the Windows server name and the folder path/filename.

(11) Open the report and verify that the Windows2008-AD-ENG server has applied the “N-Partner Policy” Group Policy Object (GPO).



Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Disabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policy

Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy

Account Policies/Kerberos Policy

Policy	Setting	Winning GPO
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy

Local Policies/Audit Policy

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy

Local Policies/User Rights Assignment

Policy	Setting	Winning GPO
Log on as a service	administrator, NPARTNER\Administrator	N-Partner Policy
Manage auditing and security log	NPARTNER\Administrator, NPARTNER\npartner	N-Partner Policy

Local Policies/Security Options

Network Access

Policy	Setting	Winning GPO
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy

Network Security

Policy	Setting	Winning GPO
Network security: Do not store LAN Manager hash value on next password change	Enabled	Default Domain Policy
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy

Event Log

Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

4. Exchange 2013

Example: Exchange 2013 installed on a Windows 2012 server.

Message tracking logs can be configured through the “Exchange Administrative Center” or the “Exchange Management Shell.”

4.1 Exchange MessageTracking Log

Modify nxlog.conf

Note: Please refer to 1.3 NXLog Configuration File.

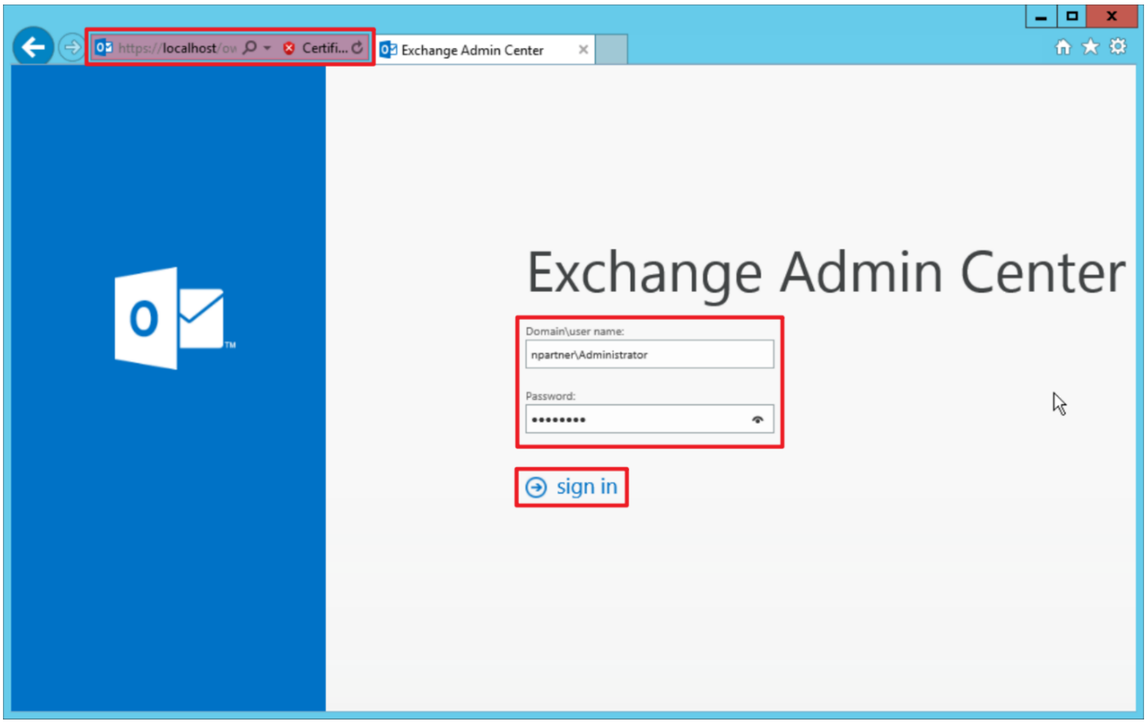
Edit the blue text section to specify the message tracking log folder:

```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

4.1.1 Exchange Administrative Center

(1) Open “Exchange Administrative Center.”

(2) Enter the URL: https://<ExchangeIP>/ecp → enter “Domain\username” and password → click “Sign in.”



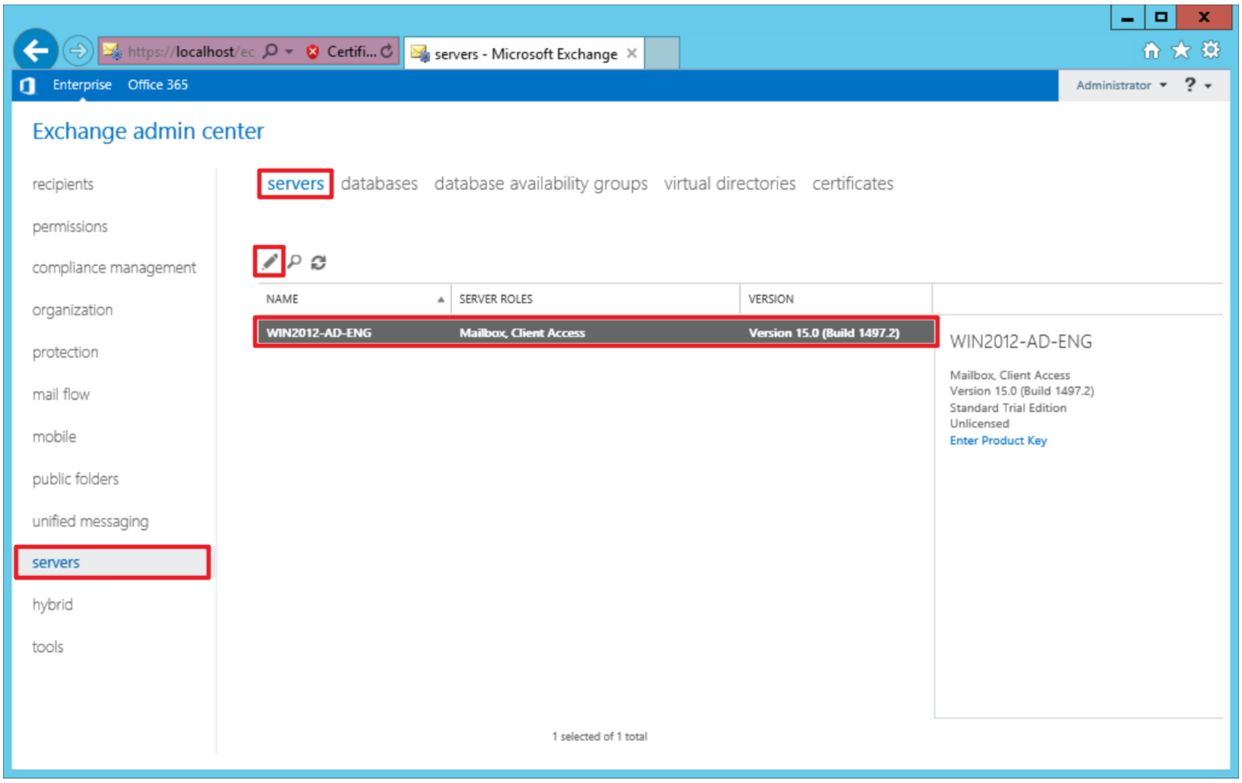
Exchange Admin Center

Domain\user name: npartner\Administrator

Password: ••••••••

sign in

(3) Select the “Servers” page → select “Servers” → select “Mailbox Server (WIN2012-AD-ENG)” → click “Edit.”



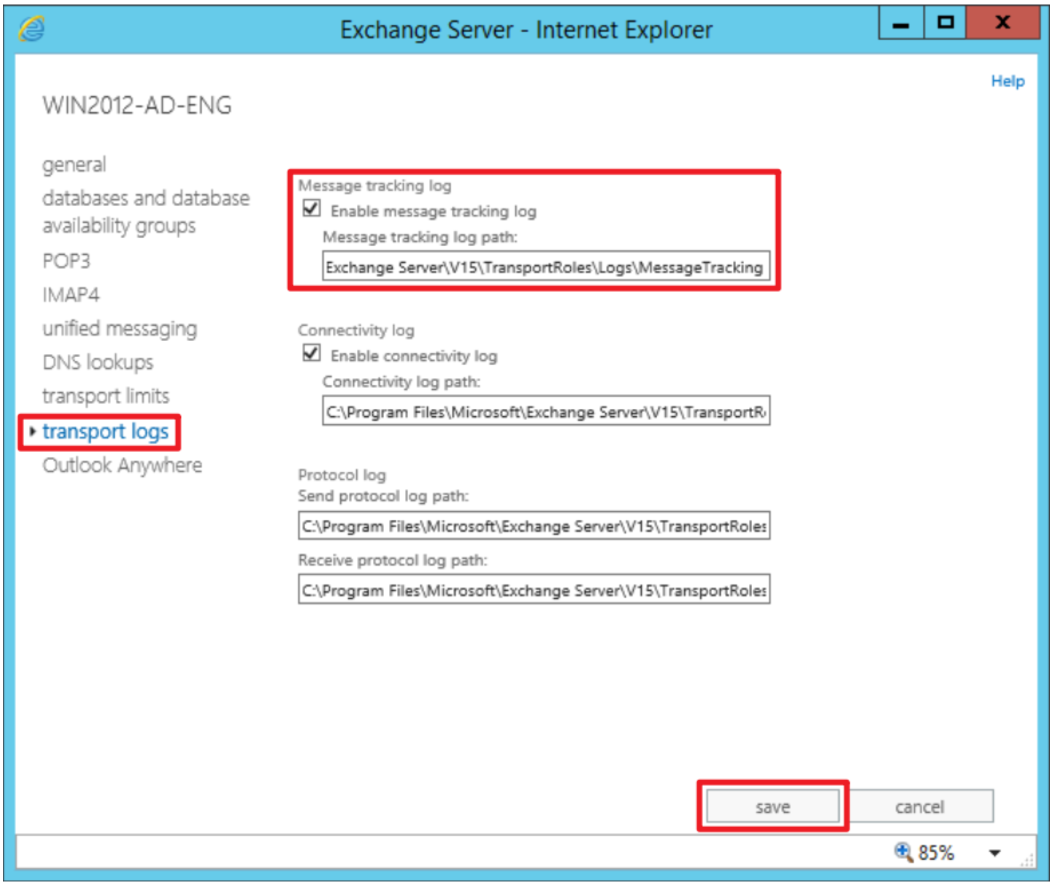
NAME	SERVER ROLES	VERSION
WIN2012-AD-ENG	Mailbox, Client Access	Version 15.0 (Build 1497.2)

WIN2012-AD-ENG

Mailbox, Client Access
Version 15.0 (Build 1497.2)
Standard Trial Edition
Unlicensed
Enter Product Key

1 selected of 1 total

(4) Select “Transport Logs” → verify “Enable message tracking log” is checked and the log path is set to: C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking → click “Save.”



WIN2012-AD-ENG

Message tracking log

☑ Enable message tracking log

Message tracking log path:

Exchange Server\V15\TransportRoles\Logs\MessageTracking

Connectivity log

☑ Enable connectivity log

Connectivity log path:

C:\Program Files\Microsoft\Exchange Server\V15\TransportR

Protocol log

Send protocol log path:

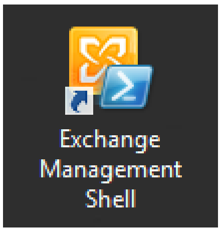
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles

Receive protocol log path:

C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles

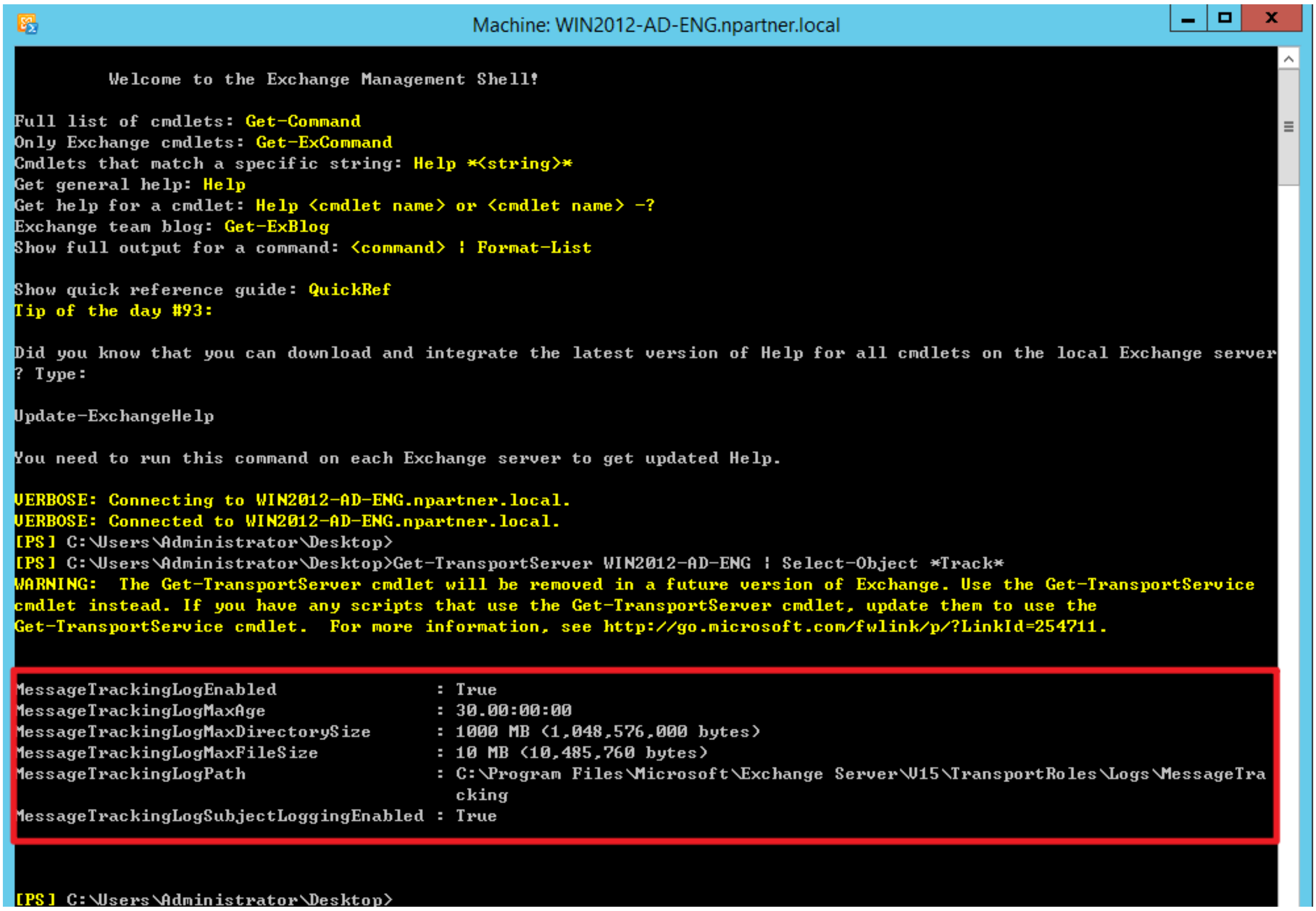
4.1.2 Exchange Management Shell

(1) Open “Exchange Management Shell.”



(2) Verify “Enable message tracking log” is checked and the log path is set to: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking] and run the following command in “Exchange Management Shell”:

```
[PS] C:\> Get-TransportServer Win2012 | Select-Object *Track*
```

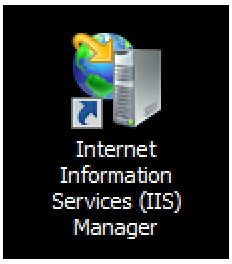


```
         Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Show quick reference guide: QuickRef
Tip of the day #93:

Did you know that you can download and integrate the latest version of Help for all cmdlets on the local Exchange server
? Type:

Update-ExchangeHelp

You need to run this command on each Exchange server to get updated Help.

VERBOSE: Connecting to WIN2012-AD-ENG.npartner.local.
VERBOSE: Connected to WIN2012-AD-ENG.npartner.local.
[PS] C:\Users\Administrator\Desktop>
[PS] C:\Users\Administrator\Desktop>Get-TransportServer WIN2012-AD-ENG | Select-Object *Track*
WARNING:  The Get-TransportServer cmdlet will be removed in a future version of Exchange. Use the Get-TransportService
cmdlet instead. If you have any scripts that use the Get-TransportServer cmdlet, update them to use the
Get-TransportService cmdlet.  For more information, see http://go.microsoft.com/fwlink/p/?LinkId=254711.


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\V15\TransportRoles\Logs\MessageTra
                                            cking
MessageTrackingLogSubjectLoggingEnabled : True


[PS] C:\Users\Administrator\Desktop>
```

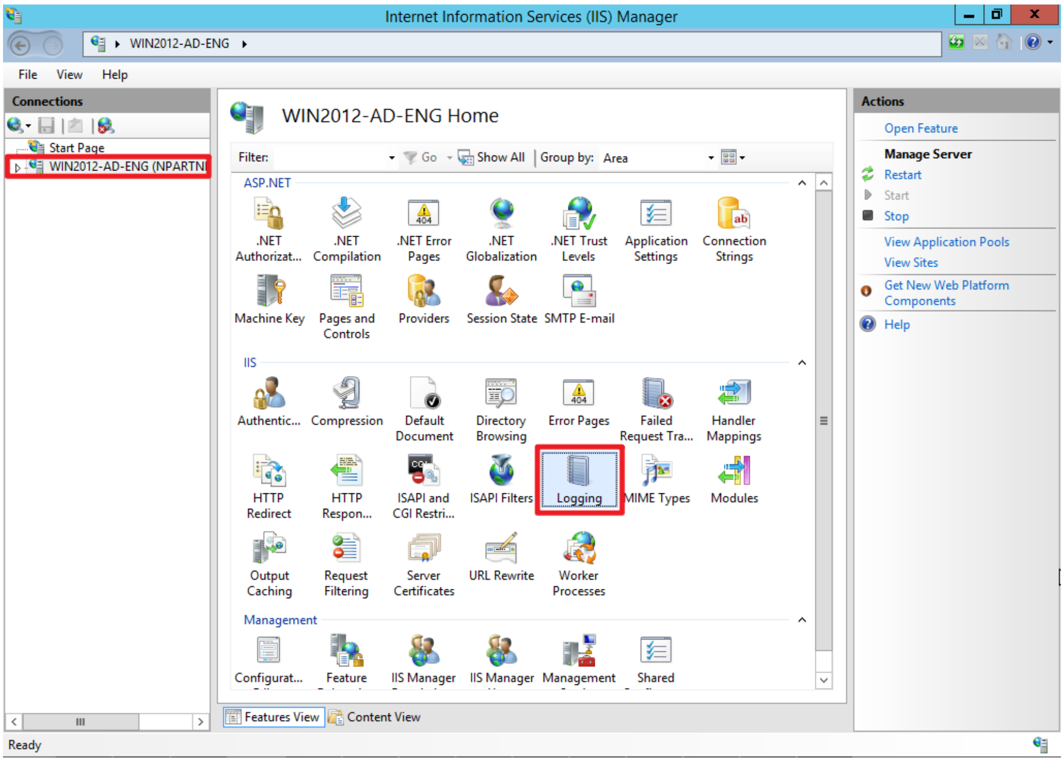
Replace the server name in red text with your Exchange server name.

4.2 IIS Log

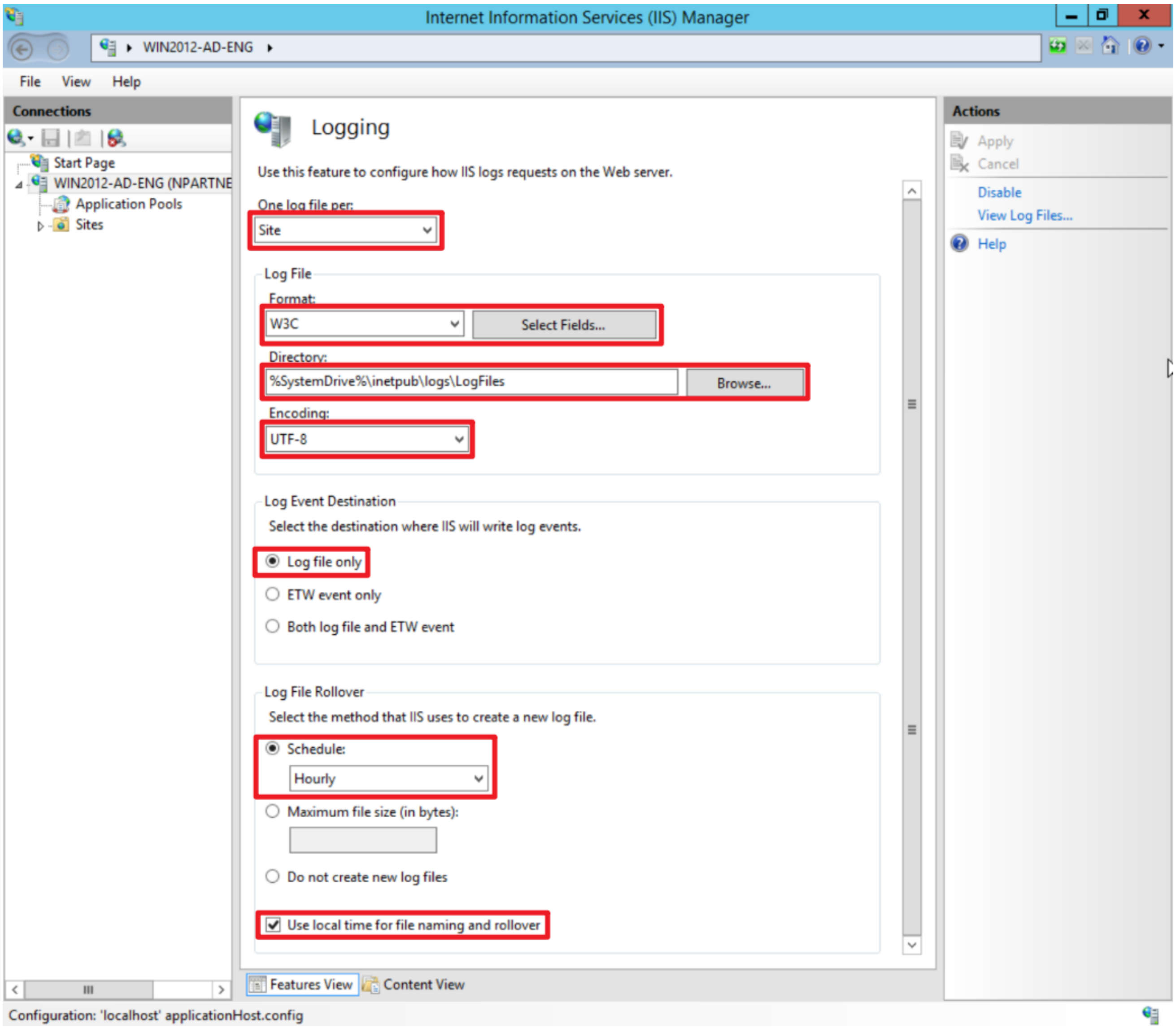
(1) Open “Internet Information Services (IIS) Manager.”



(2) Select your “IIS Server” (the example here is WIN2012-AD-ENG) → “Logging.”



(3) Select “Create a log file for each site” → set “Log file format” to “W3C” → set “Directory” to %SystemDrive%\inetpub\logs\LogFiles → set “Encoding” to “UTF-8” → set “Log event destination” to “Log file only” → set “Schedule” to “Hourly” → check “Use local time for file naming and rollover” → click “Select Fields.”



Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per:
Site

Log File

Format:
W3C
Select Fields...

Directory:
%SystemDrive%\inetpub\logs\LogFiles
Browse...

Encoding:
UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only
○ ETW event only
○ Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

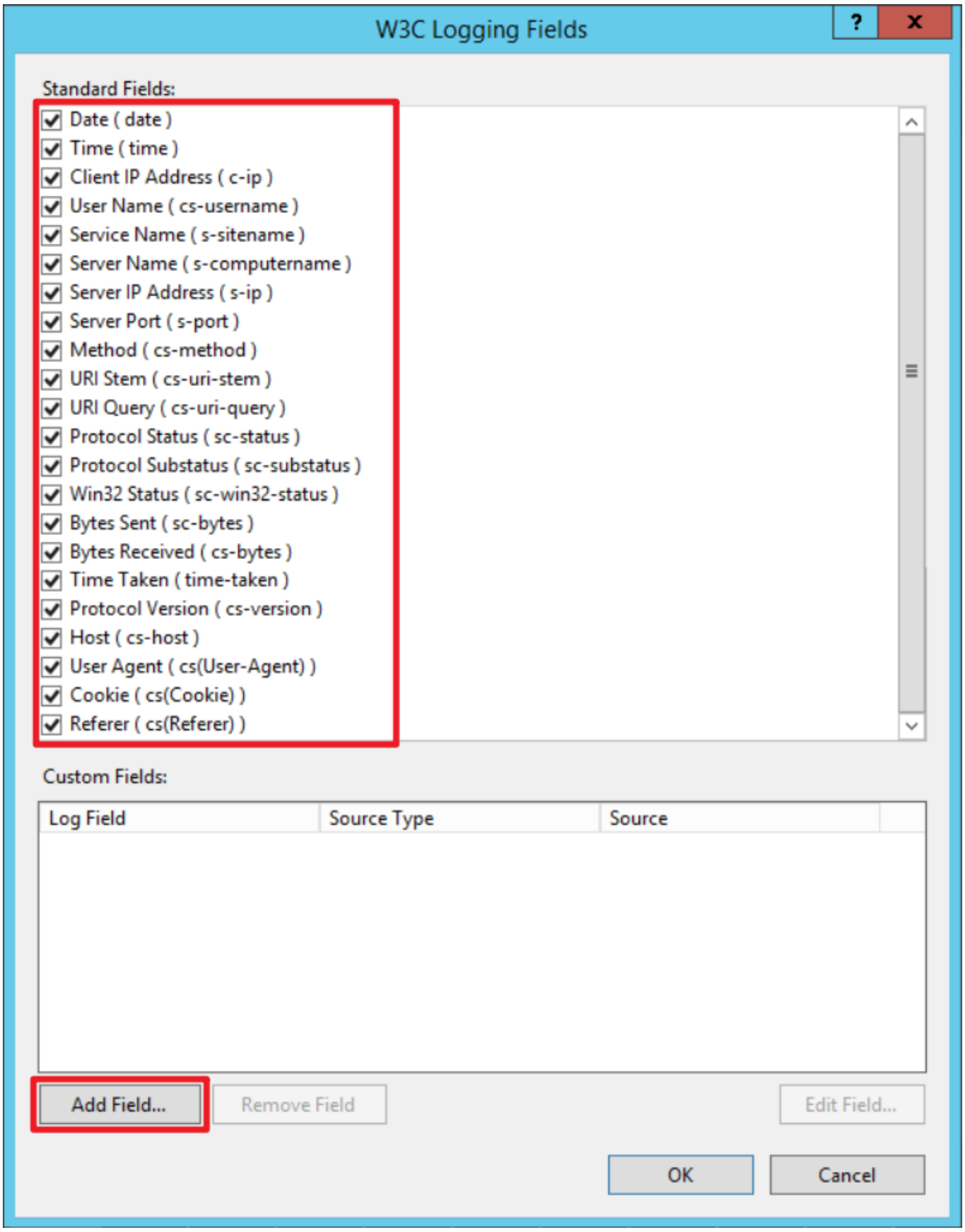
● Schedule:
Hourly
○ Maximum file size (in bytes):
○ Do not create new log files

☑ Use local time for file naming and rollover

Configuration: 'localhost' applicationHost.config

(4) Select the following fields → click “Add Field”:

“Date (date), Time (time), Client IP Address (c-ip), User Name (cs-username), Service Name (s-sitename), Server Name (s-computername), Server IP Address (s-ip), Server Port (s-port), Method (cs-method), URI Stem (cs-uri-stem), URI Query (cs-uri-query), Protocol Status (sc-status), Protocol Substatus (sc-substatus), Win32 Status (sc-win32-status), Bytes Sent (sc-bytes), Bytes Received (cs-bytes), Time Taken (time-taken), Protocol Version (cs-version), Host (cs-host), User Agent (cs(User-Agent)), Cookie (cs(Cookie)), Referrer (cs(Referer)).”



W3C Logging Fields

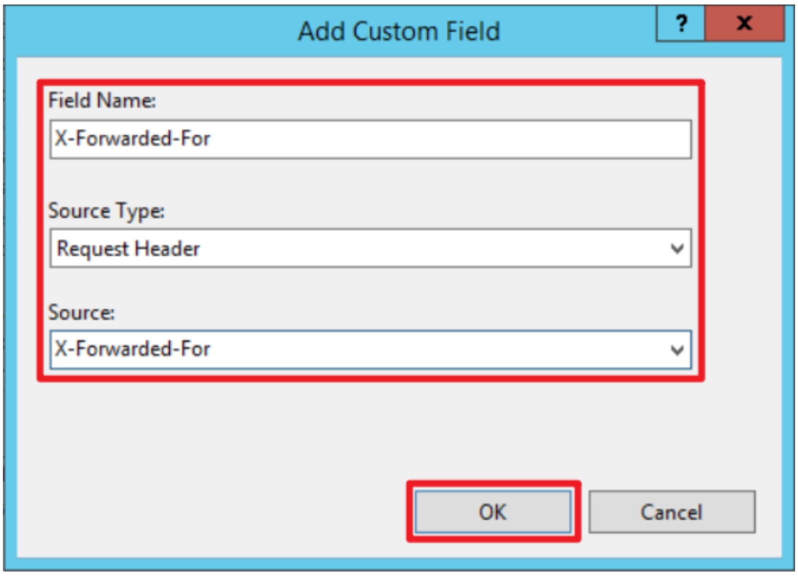
Standard Fields:

- ☑ Date (date)
- ☑ Time (time)
- ☑ Client IP Address (c-ip)
- ☑ User Name (cs-username)
- ☑ Service Name (s-sitename)
- ☑ Server Name (s-computername)
- ☑ Server IP Address (s-ip)
- ☑ Server Port (s-port)
- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ URI Query (cs-uri-query)
- ☑ Protocol Status (sc-status)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Win32 Status (sc-win32-status)
- ☑ Bytes Sent (sc-bytes)
- ☑ Bytes Received (cs-bytes)
- ☑ Time Taken (time-taken)
- ☑ Protocol Version (cs-version)
- ☑ Host (cs-host)
- ☑ User Agent (cs(User-Agent))
- ☑ Cookie (cs(Cookie))
- ☑ Referer (cs(Referer))

Custom Fields:

Log Field	Source Type	Source

(5) Enter field name: X-Forwarded-For → select "Source type": "Request Header" → enter source name: X-Forwarded-For → click "OK."



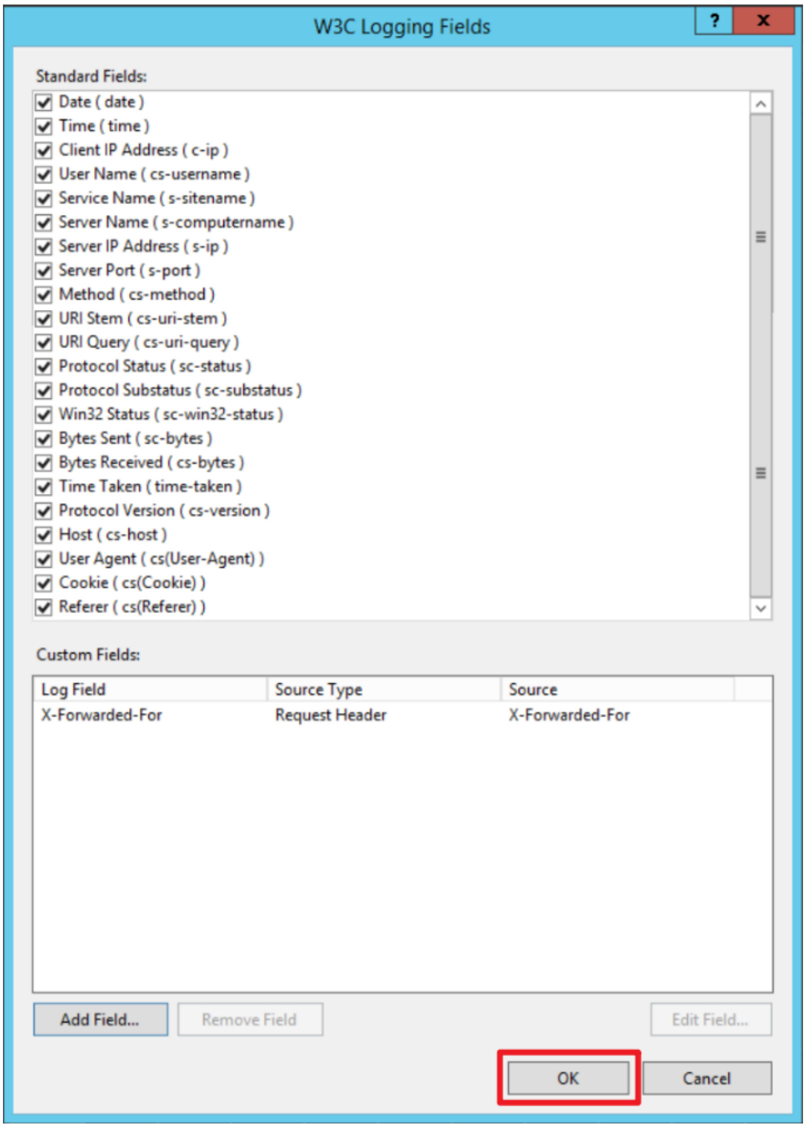
Add Custom Field

Field Name: X-Forwarded-For

Source Type: Request Header

Source: X-Forwarded-For

(6) Click "OK."



W3C Logging Fields

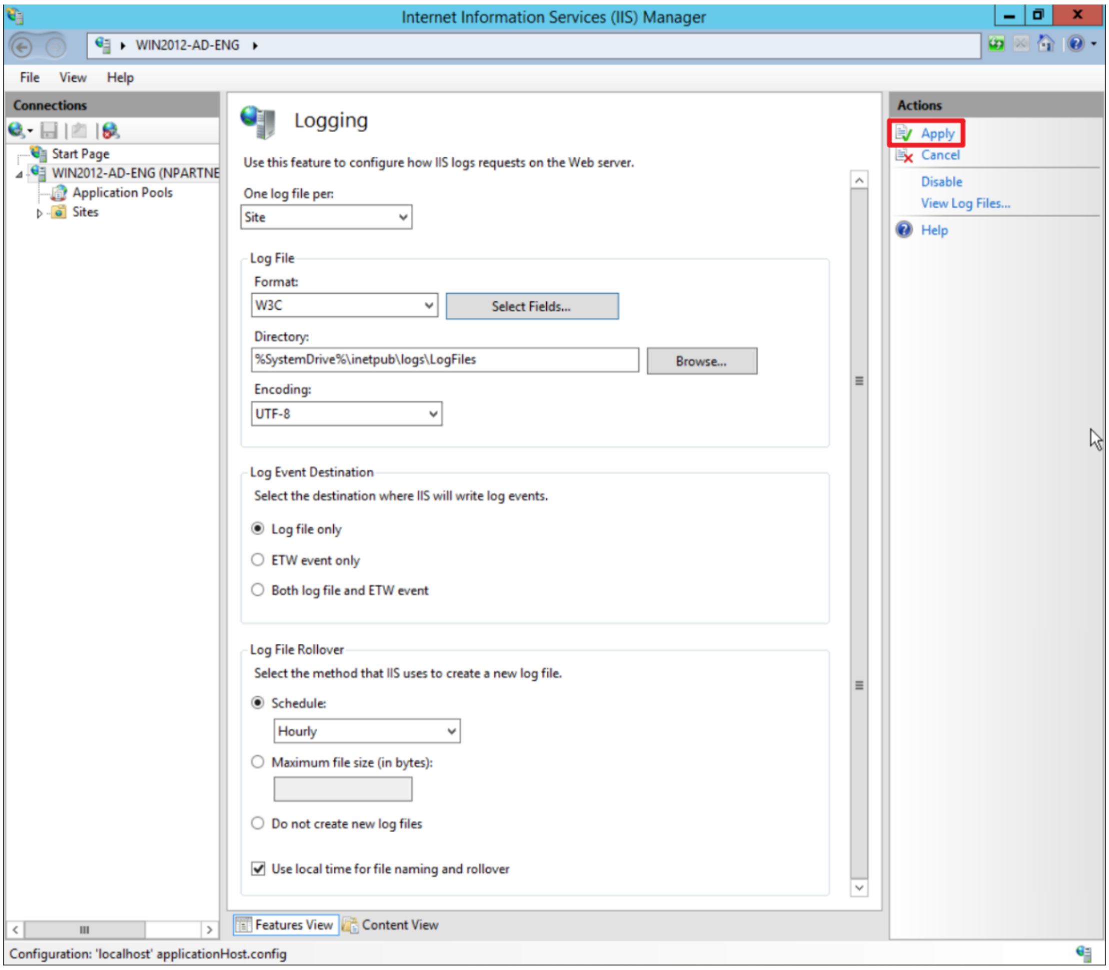
Standard Fields:

- ☑ Date (date)
- ☑ Time (time)
- ☑ Client IP Address (c-ip)
- ☑ User Name (cs-username)
- ☑ Service Name (s-sitename)
- ☑ Server Name (s-computername)
- ☑ Server IP Address (s-ip)
- ☑ Server Port (s-port)
- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ URI Query (cs-uri-query)
- ☑ Protocol Status (sc-status)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Win32 Status (sc-win32-status)
- ☑ Bytes Sent (sc-bytes)
- ☑ Bytes Received (cs-bytes)
- ☑ Time Taken (time-taken)
- ☑ Protocol Version (cs-version)
- ☑ Host (cs-host)
- ☑ User Agent (cs(User-Agent))
- ☑ Cookie (cs(Cookie))
- ☑ Referer (cs(Referer))

Custom Fields:

Log Field	Source Type	Source
X-Forwarded-For	Request Header	X-Forwarded-For

(7) Click “Apply.”



Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C [Select Fields...]

Directory: %SystemDrive%\inetpub\logs\LogFiles [Browse...]

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only

○ ETW event only

○ Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

● Schedule: Hourly

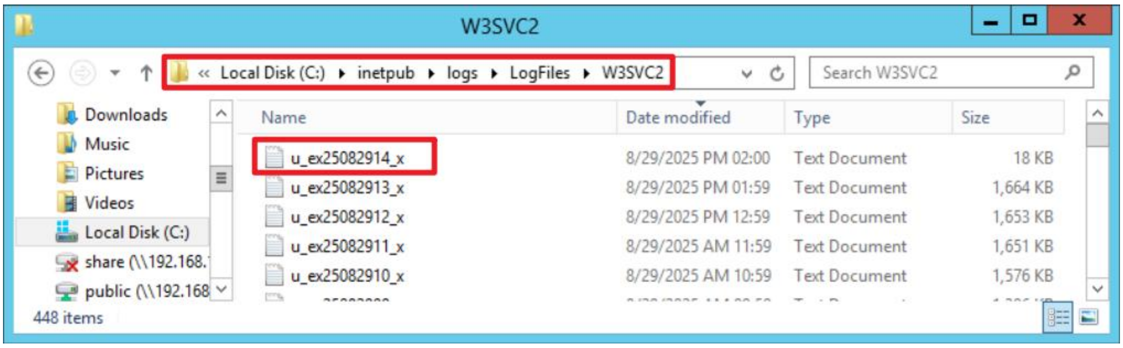
○ Maximum file size (in bytes):

○ Do not create new log files

☑ Use local time for file naming and rollover

Configuration: 'localhost' applicationHost.config

(8) Verify IIS log files are created in the folder: C:\inetpub\logs\LogFiles\W3SVC2

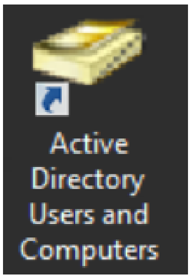


Name	Date modified	Type	Size
u_ex25082914_x	8/29/2025 PM 02:00	Text Document	18 KB
u_ex25082913_x	8/29/2025 PM 01:59	Text Document	1,664 KB
u_ex25082912_x	8/29/2025 PM 12:59	Text Document	1,653 KB
u_ex25082911_x	8/29/2025 AM 11:59	Text Document	1,651 KB
u_ex25082910_x	8/29/2025 AM 10:59	Text Document	1,576 KB

4.3 Event Log

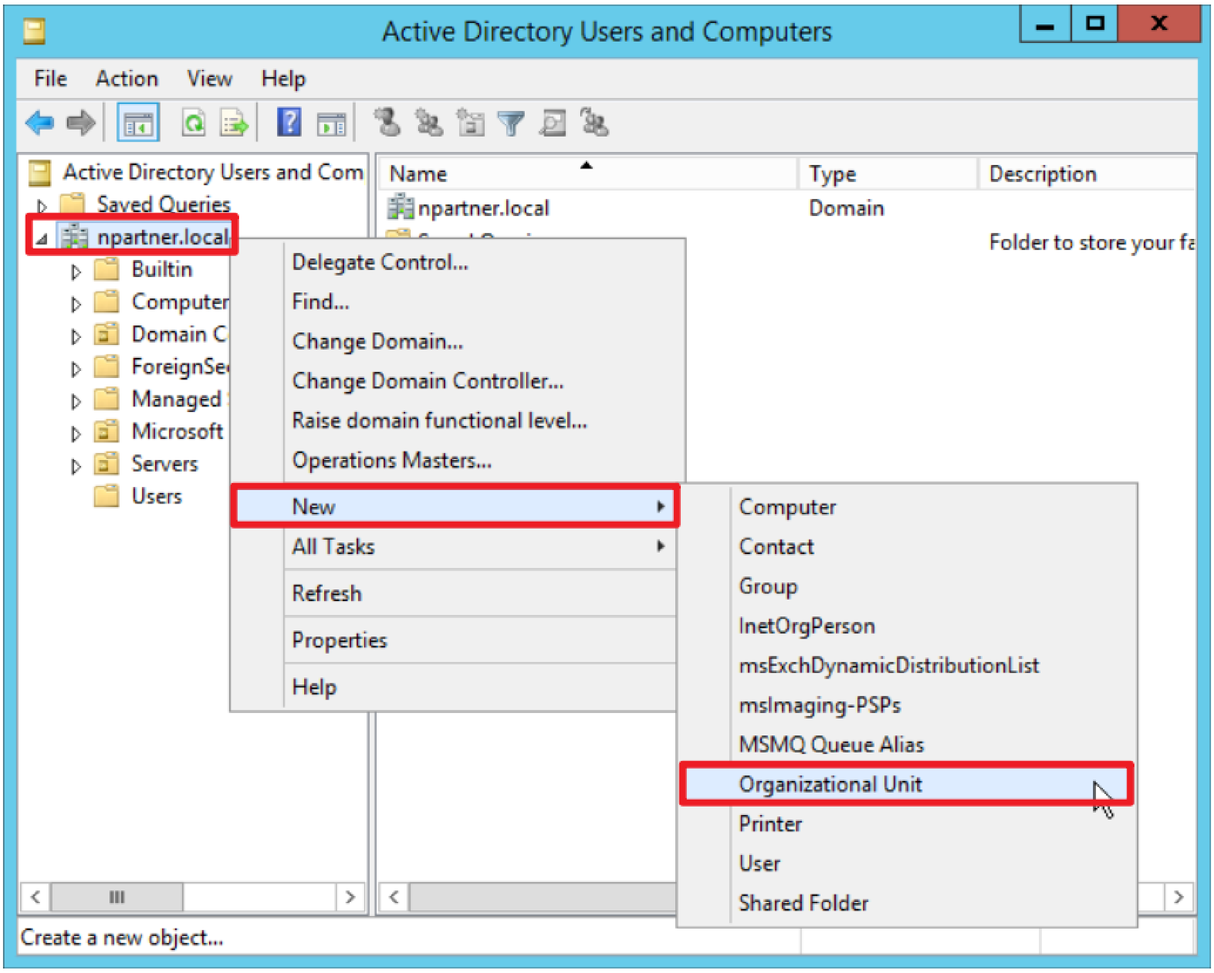
4.3.1 Organizational Unit (OU) Configuration

(1) Open “Active Directory Users and Computers.”



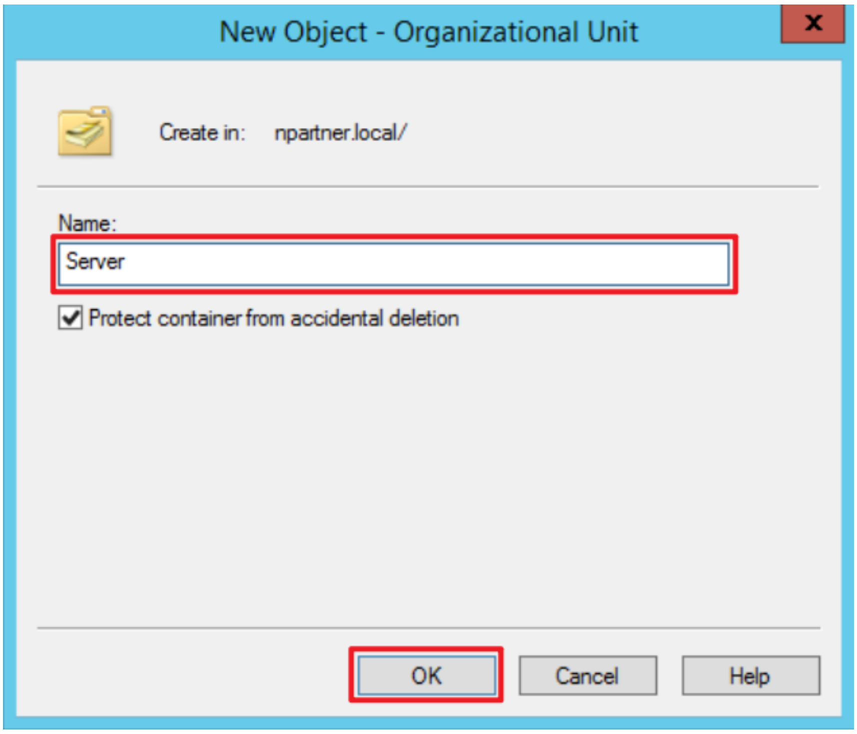
(2) Add an Organizational Unit

Right-click on the domain name (the example here is npartner.local) → select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

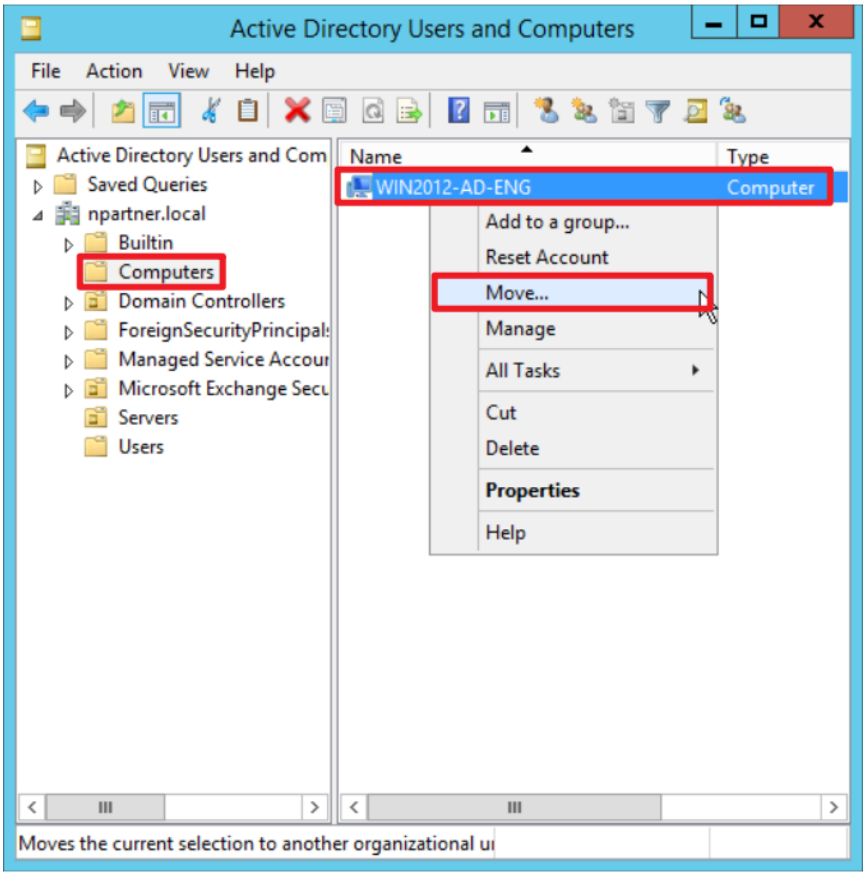
Note: Please create the organizational unit name according to the actual environment. → click “OK.”


New Object - Organizational Unit
Create in: npartner.local/
Name:
Server
☑ Protect container from accidental deletion
OK
Cancel
Help

(4) Move the Server to your New Organizational Unit:

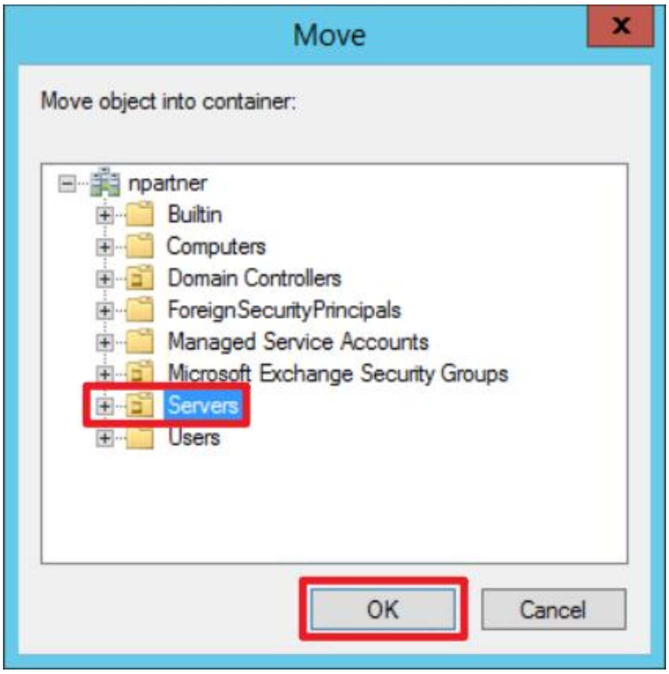
Select “Computers” → right-click on the “WIN2012-AD-ENG” server.

Note: Please select the Exchange server according to the actual environment. → click “Move.”



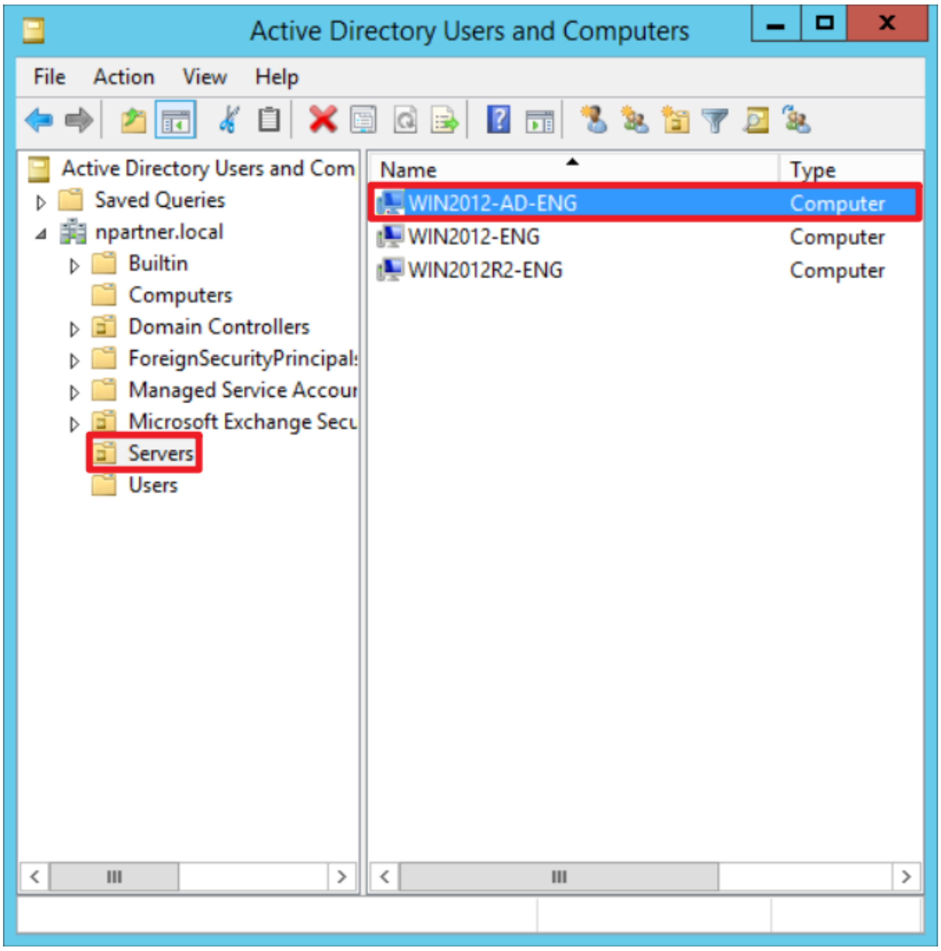
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is "Servers") → Click "OK."



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is "Servers") and confirm that the "WIN2012-AD-ENG" server has been moved.



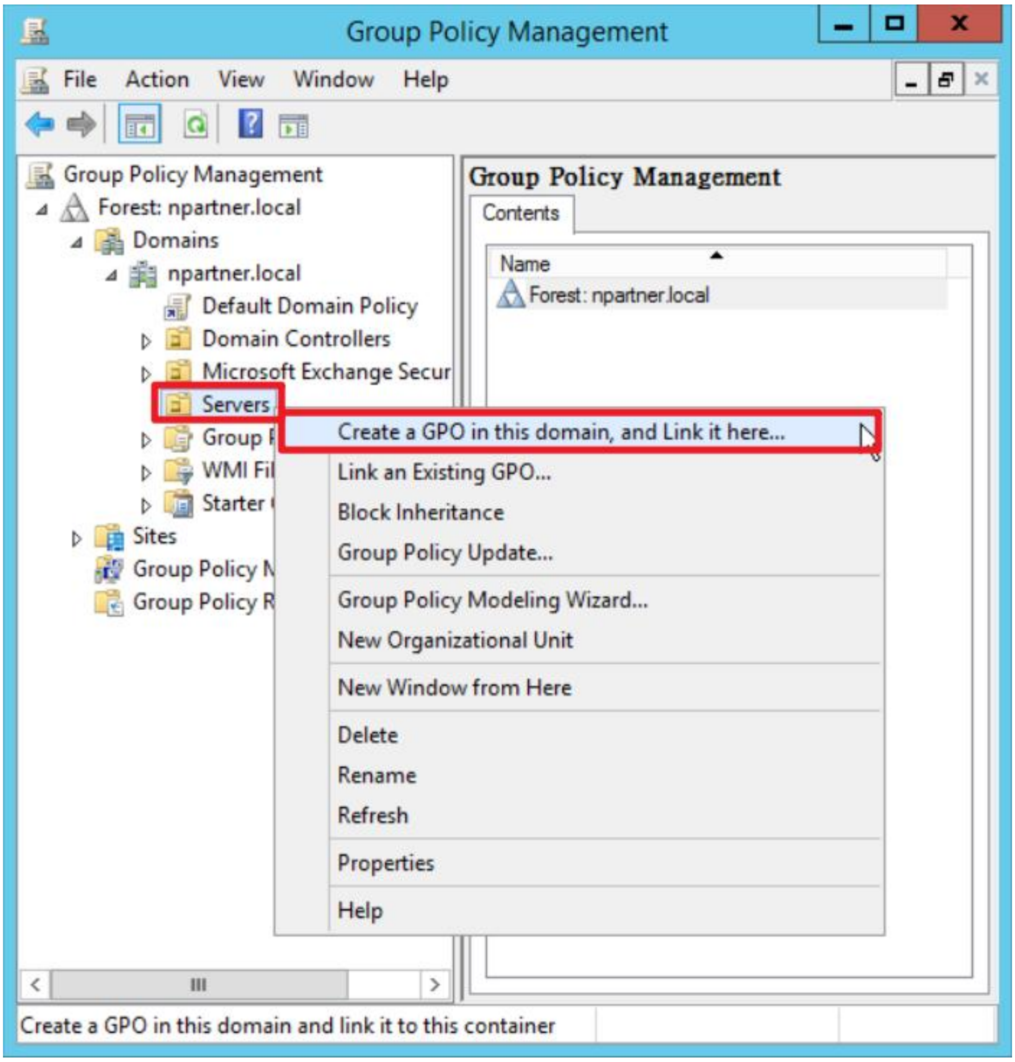
Name	Type
WIN2012-AD-ENG	Computer
WIN2012-ENG	Computer
WIN2012R2-ENG	Computer

4.3.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

Right-click the “Servers” organizational unit → select “Create a GPO in this domain, and Link it here...”

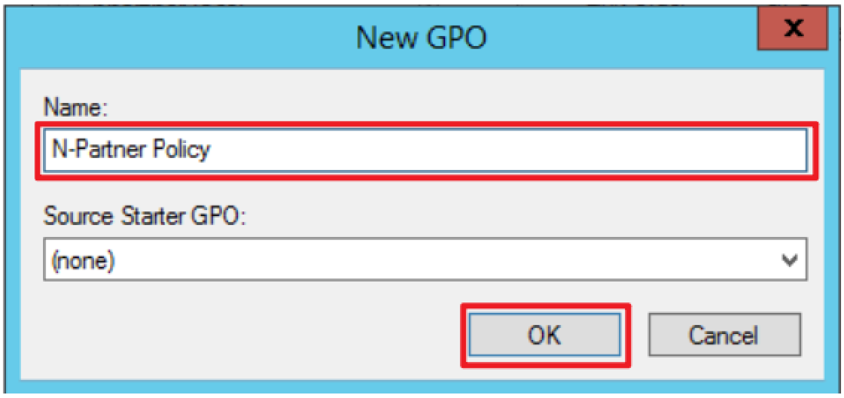


Create a GPO in this domain and link it to this container

(3) Edit your Group Policy Object

Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. → then click “Edit.”



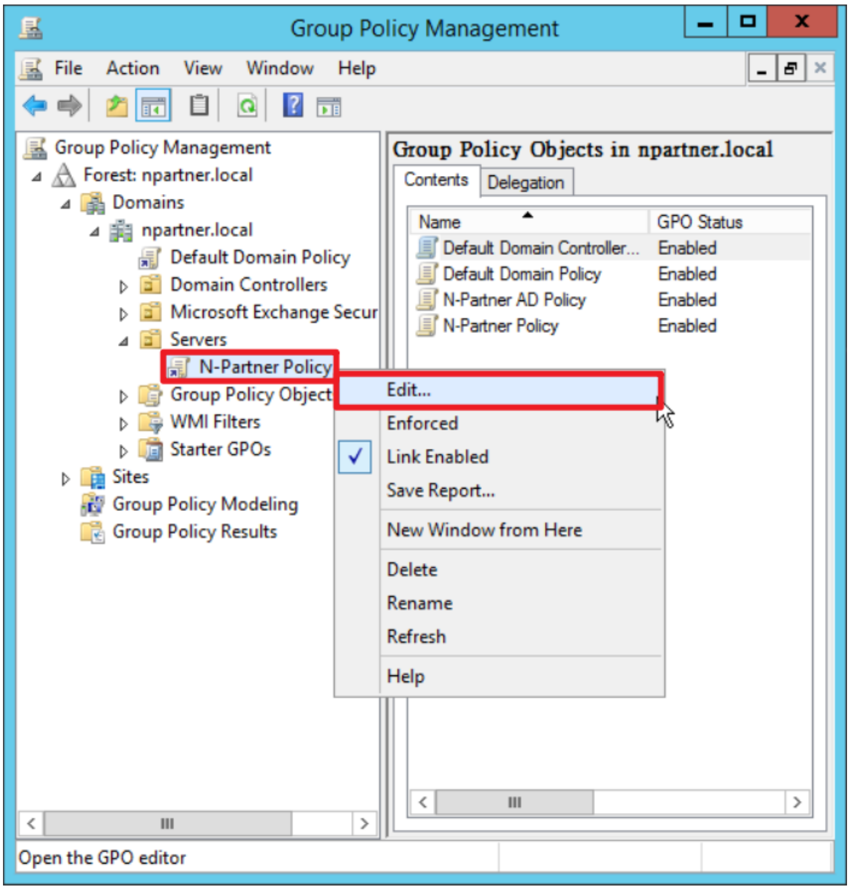
New GPO

Name: N-Partner Policy

Source Starter GPO: (none)

(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



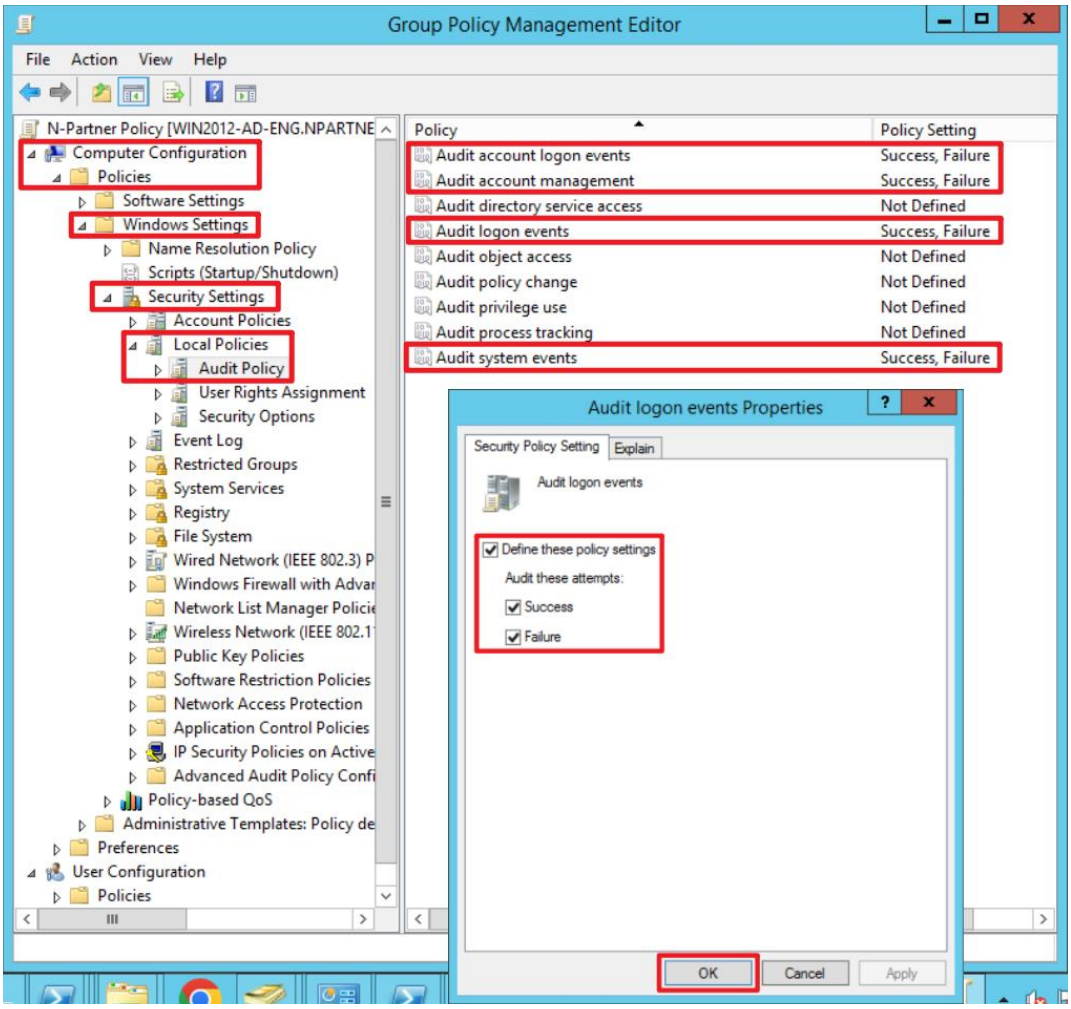
Group Policy Management

Name	GPO Status
Default Domain Controller...	Enabled
Default Domain Policy	Enabled
N-Partner AD Policy	Enabled
N-Partner Policy	Enabled

Open the GPO editor

(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” and “Audit system events” → check “Define these policy settings”: Success, Failure. → click “OK.”



N-Partner Policy [WIN2012-AD-ENG.NPARTNE
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) P
        - Windows Firewall with Advar
        - Network List Manager Policie
        - Wireless Network (IEEE 802.1
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection
        - Application Control Policies
        - IP Security Policies on Active
        - Advanced Audit Policy Confi
      - Policy-based QoS
    - Administrative Templates: Policy de
  - Preferences
- User Configuration
  - Policies

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Success, Failure

Audit logon events Properties

Security Policy Setting | Explain

Audit logon events

☑ Define these policy settings

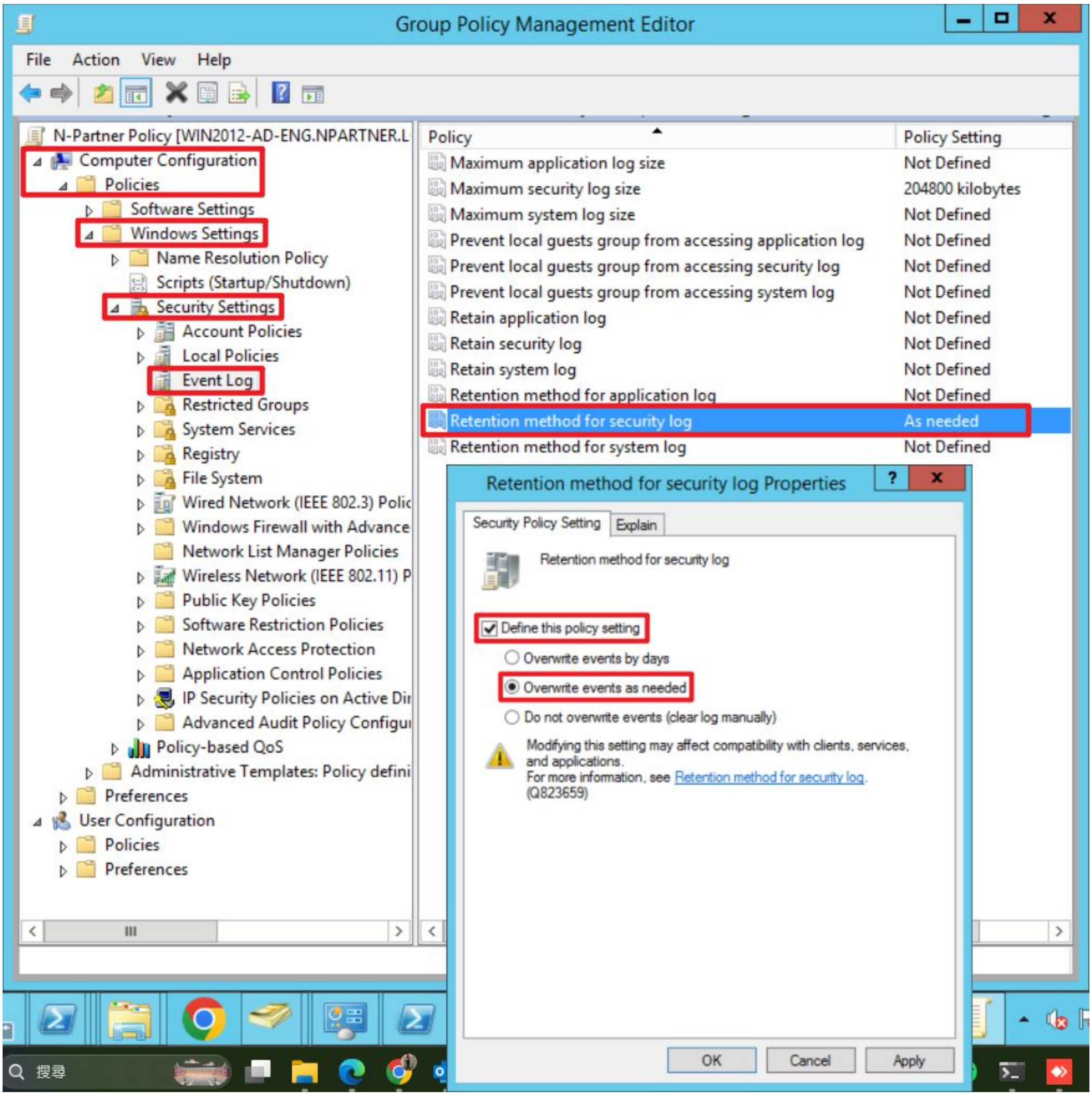
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Security Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2012-AD-ENG.NPARTNER.L
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polic
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Dir
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates: Policy defini
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Retention method for security log Properties

Security Policy Setting | Explain

Retention method for security log

☑ Define this policy setting

○ Overwrite events by days

● Overwrite events as needed

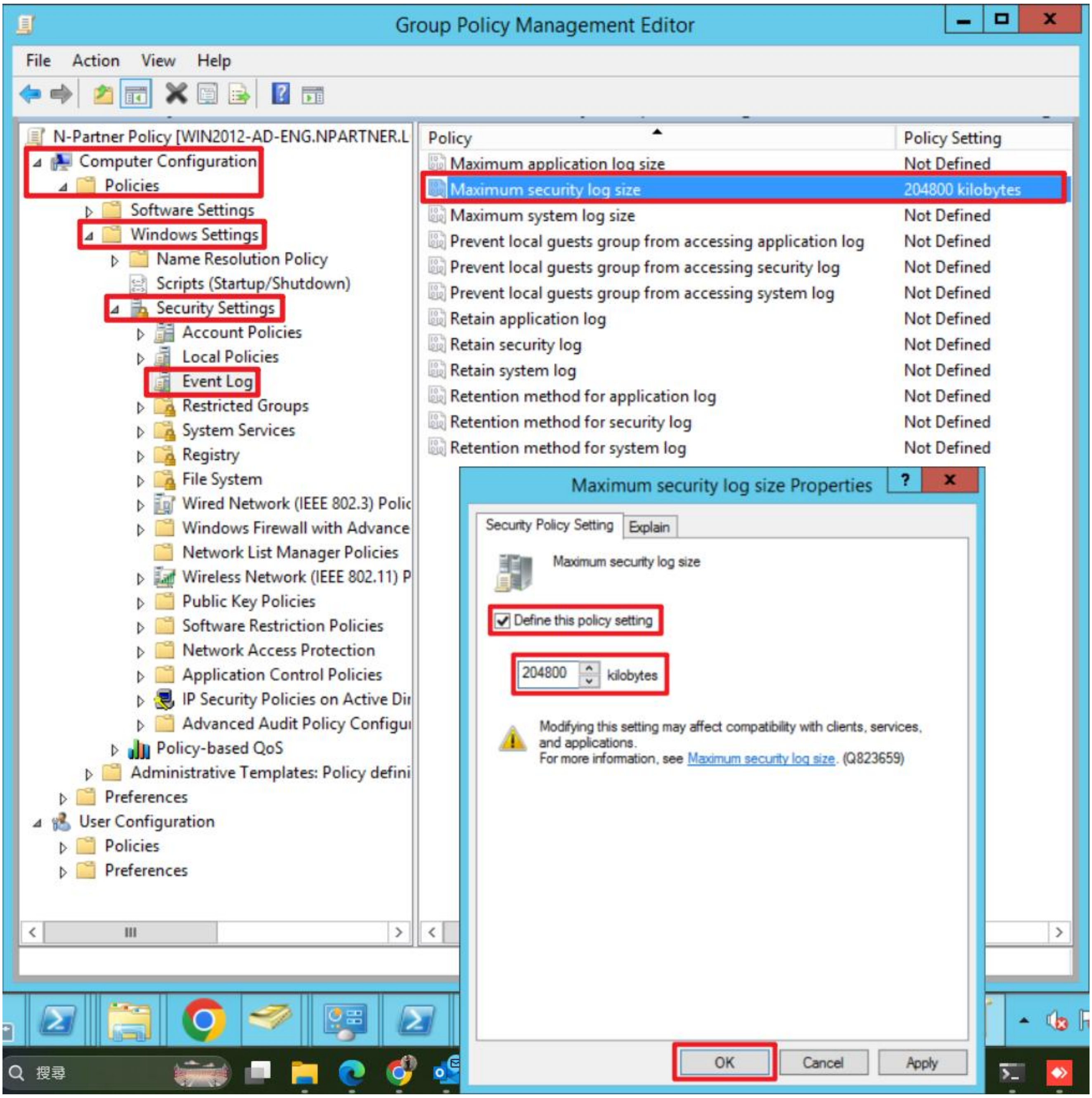
○ Do not overwrite events (clear log manually)

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Retention method for security log. (Q823659)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”


Group Policy Management Editor
File Action View Help
N-Partner Policy [WIN2012-AD-ENG.NPARTNER.L
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Polic
Windows Firewall with Advance
Network List Manager Policies
Wireless Network (IEEE 802.11) P
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Dir
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates: Policy defini
Preferences
User Configuration
Policies
Preferences
搜尋

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum security log size Properties

Security Policy Setting | Explain

Maximum security log size

☑ Define this policy setting

204800 kilobytes

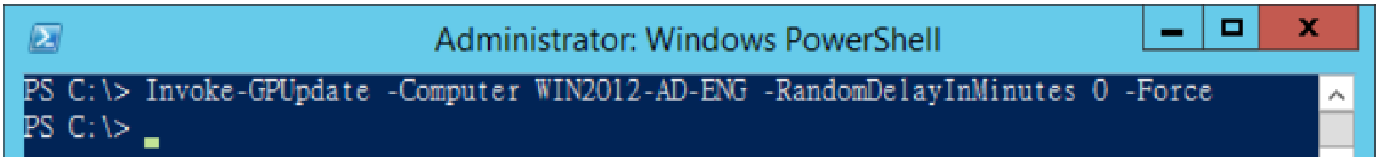
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Maximum security log size. (Q823659)

OK Cancel Apply

(8) On the server, open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer Win2012 -RandomDelayInMinutes 0 -Force
```

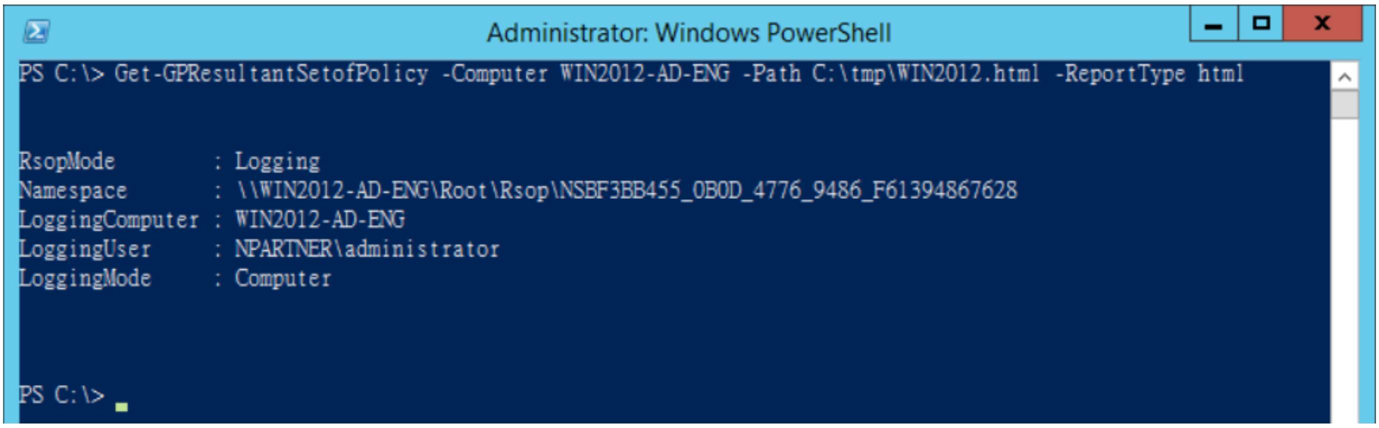


```
PS C:\> Invoke-GPUpdate -Computer WIN2012-AD-ENG -RandomDelayInMinutes 0 -Force
PS C:\> _
```

Replace the red text section with the name of your Exchange server.

(10) Enter the command below to generate server group policy report.

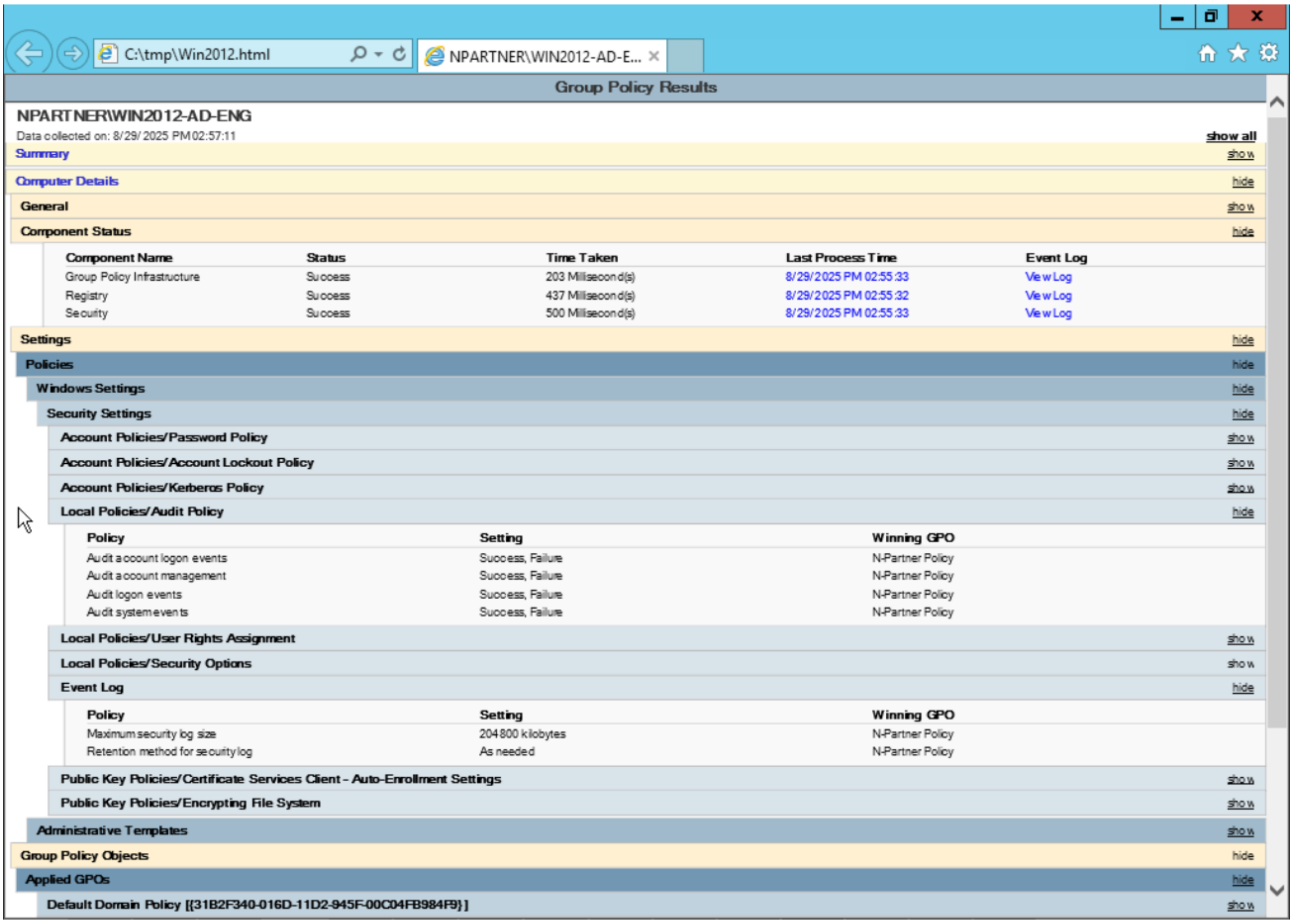
```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2012 -Path C:\tmp\Win2012.html -ReportType html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2012-AD-ENG -Path C:\tmp\WIN2012.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2012-AD-ENG\Root\Rsop\NSBF3BB455_0B0D_4776_9486_F61394867628
LoggingComputer : WIN2012-AD-ENG
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer



PS C:\> _
```

For the red text , please enter the Exchange server name and the folder path/file name.

(11) Open the report and verify that your Windows AD server is applying the N-Partner Policy Group Policy.



Group Policy Results

NPARTNER\WIN2012-AD-ENG

Data collected on: 8/29/2025 PM 02:57:11 show all

Summary show

Computer Details hide

General show

Component Status hide

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	203 Millisecond(s)	8/29/2025 PM 02:55:33	View Log
Registry	Success	437 Millisecond(s)	8/29/2025 PM 02:55:32	View Log
Security	Success	500 Millisecond(s)	8/29/2025 PM 02:55:33	View Log

Settings hide

Policies hide

Windows Settings hide

Security Settings hide

Account Policies/Password Policy show

Account Policies/Account Lockout Policy show

Account Policies/Kerberos Policy show

Local Policies/Audit Policy hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy

Local Policies/User Rights Assignment show

Local Policies/Security Options show

Event Log hide

Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings show

Public Key Policies/Encrypting File System show

Administrative Templates show

Group Policy Objects hide

Applied GPOs hide

Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}] show

5. Exchange 2016

Example: Exchange 2016 installed on a Windows 2016 server.

Message tracking logs can be configured through the “Exchange Administrative Center” or the “Exchange Management Shell.”

5.1 Exchange MessageTracking Log

Modify nxlog.conf

Note: Please refer to 1.3 NXLog Configuration File.

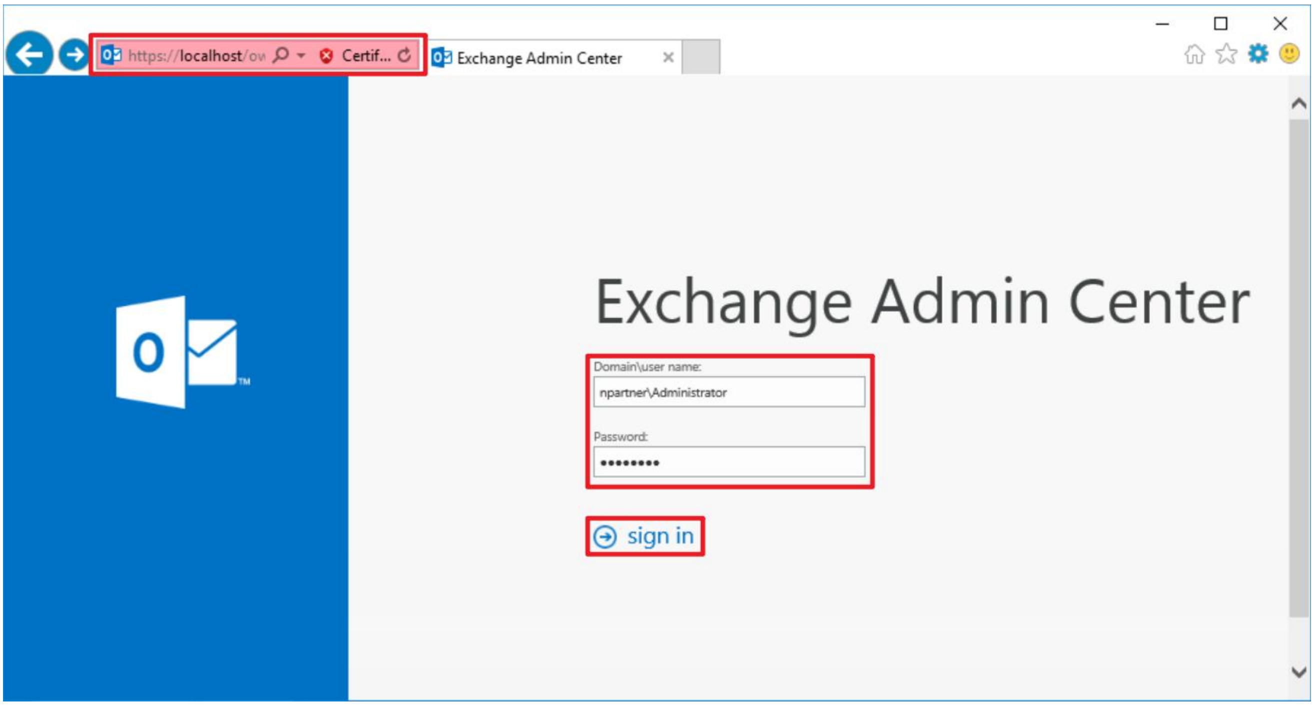
Edit the blue text section to specify the message tracking log folder:

```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

5.1.1 Exchange Administrative Center

(1) Open “Exchange Administrative Center.”

(2) Enter the URL: https://<ExchangeIP>/ecp → enter “Domain\username” and password → click “Sign in.”

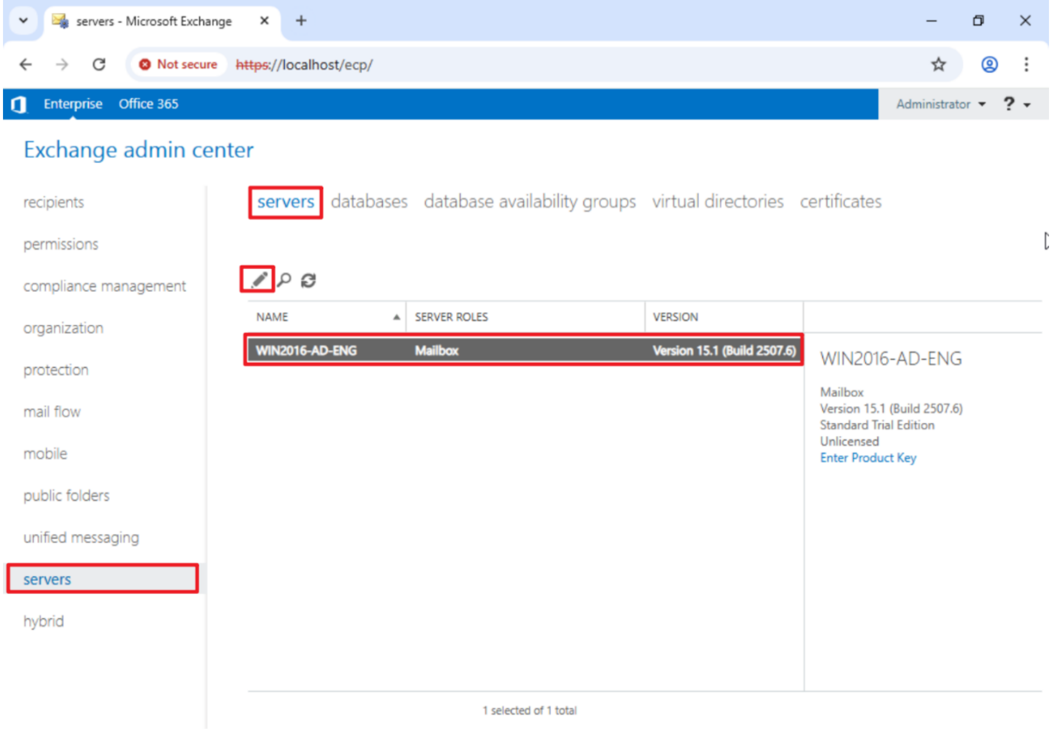


Exchange Admin Center

Domain\user name: npartner\Administrator

Password: ••••••••

(3) Select the "Servers" page → select "Servers" → select "Mailbox Server (WIN2016-AD-ENG)" → click "Edit."



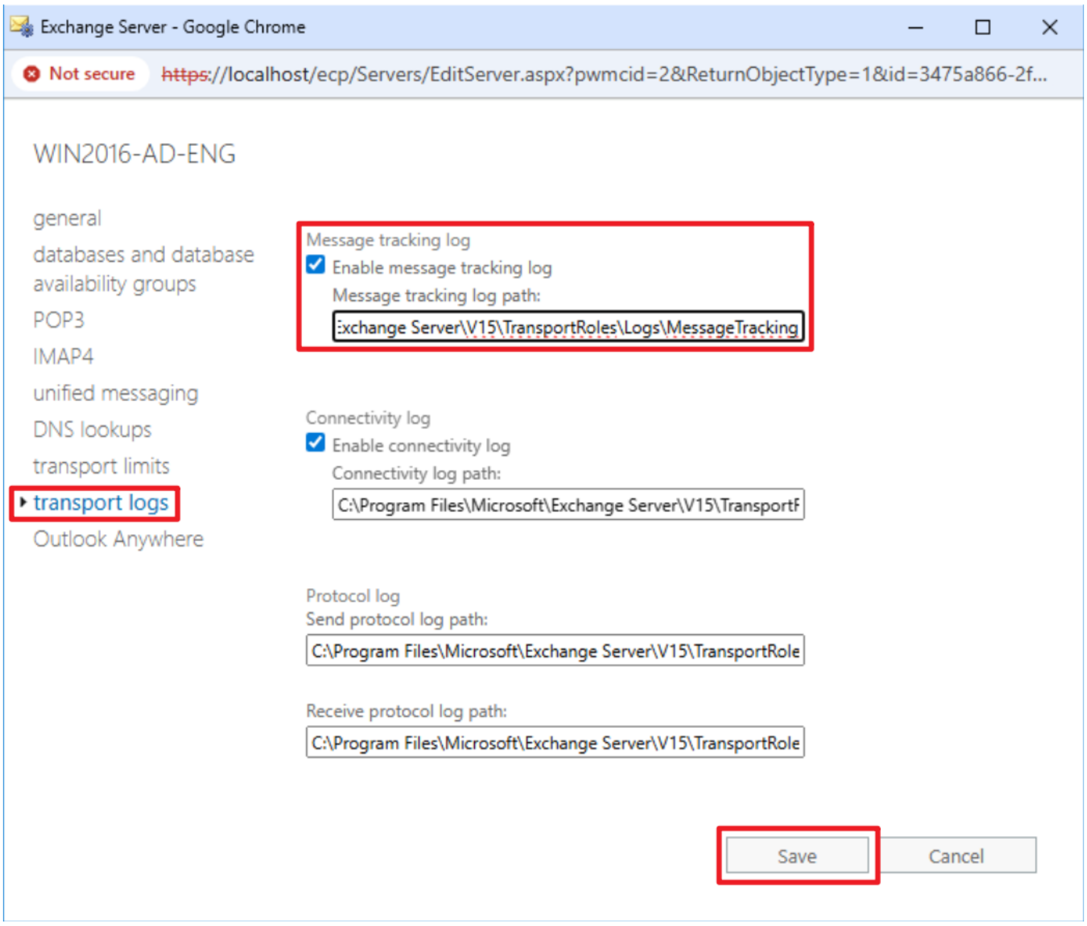
NAME	SERVER ROLES	VERSION
WIN2016-AD-ENG	Mailbox	Version 15.1 (Build 2507.6)

WIN2016-AD-ENG

Mailbox
Version 15.1 (Build 2507.6)
Standard Trial Edition
Unlicensed
Enter Product Key

1 selected of 1 total

(4) Select "Transport Logs" → verify "Enable message tracking log" is checked and the log path is set to: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking → click "Save."


Exchange Server - Google Chrome
Not secure https://localhost/ecp/Servers/EditServer.aspx?pwmcid=2&ReturnObjectType=1&id=3475a866-2f...
WIN2016-AD-ENG
general
databases and database availability groups
POP3
IMAP4
unified messaging
DNS lookups
transport limits
transport logs
Outlook Anywhere
Save
Cancel

Message tracking log
☑ Enable message tracking log
Message tracking log path:
:xchange Server\V15\TransportRoles\Logs\MessageTracking

Connectivity log
☑ Enable connectivity log
Connectivity log path:
C:\Program Files\Microsoft\Exchange Server\V15\TransportF

Protocol log
Send protocol log path:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRole

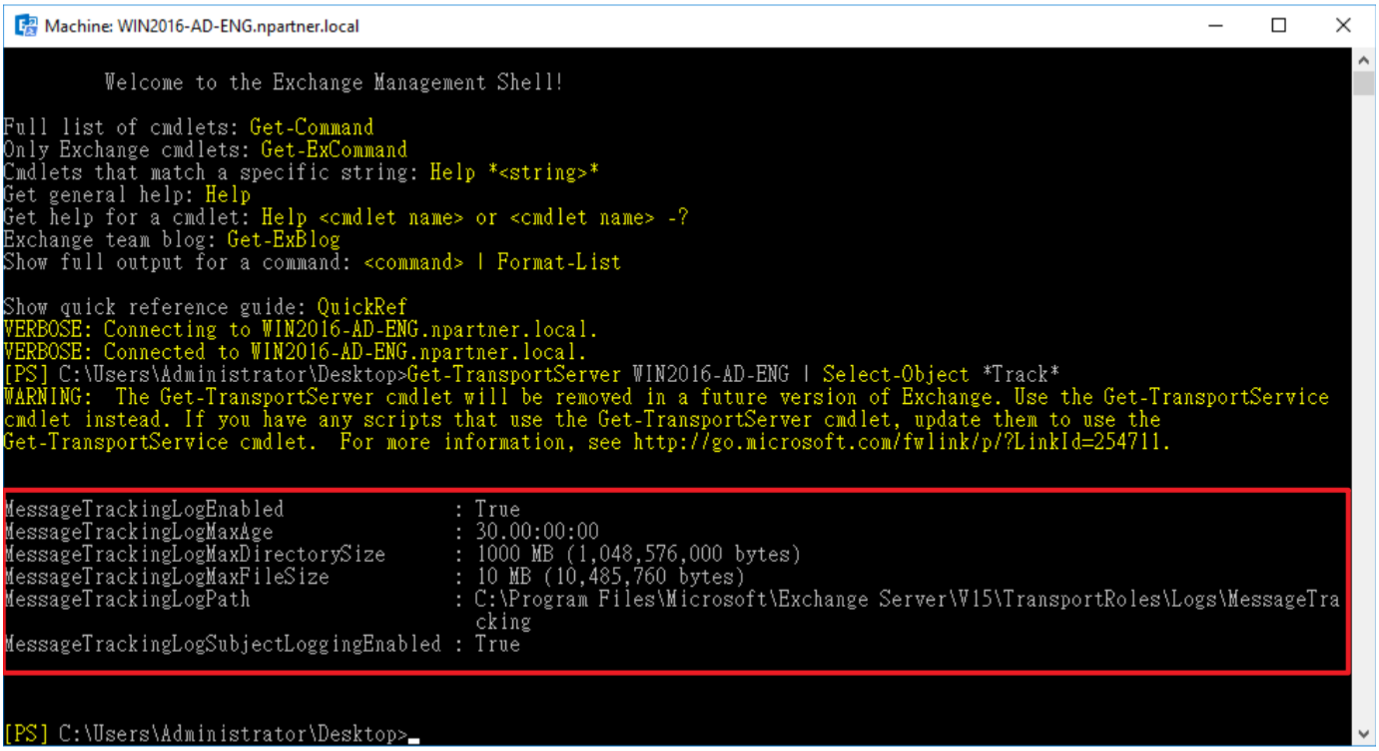
Receive protocol log path:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRole

5.1.2 Exchange Management Shell

(1) Open “Exchange Management Shell.”

(2) Verify “Enable message tracking log” is checked and the log path is set to: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking]
and run the following command in “Exchange Management Shell”:

```
[PS] C:\> Get-TransportServer Win2016 | Select-Object *Track*
```

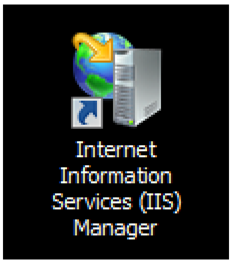


```
        Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Show quick reference guide: QuickRef
VERBOSE: Connecting to WIN2016-AD-ENG.npartner.local.
VERBOSE: Connected to WIN2016-AD-ENG.npartner.local.
[PS] C:\Users\Administrator\Desktop>Get-TransportServer WIN2016-AD-ENG | Select-Object *Track*
WARNING:  The Get-TransportServer cmdlet will be removed in a future version of Exchange. Use the Get-TransportService
cmdlet instead. If you have any scripts that use the Get-TransportServer cmdlet, update them to use the
Get-TransportService cmdlet.  For more information, see http://go.microsoft.com/fwlink/p/?LinkId=254711.


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\V15\TransportRoles\Logs\MessageTra
                                          cking
MessageTrackingLogSubjectLoggingEnabled : True



[PS] C:\Users\Administrator\Desktop>_
```

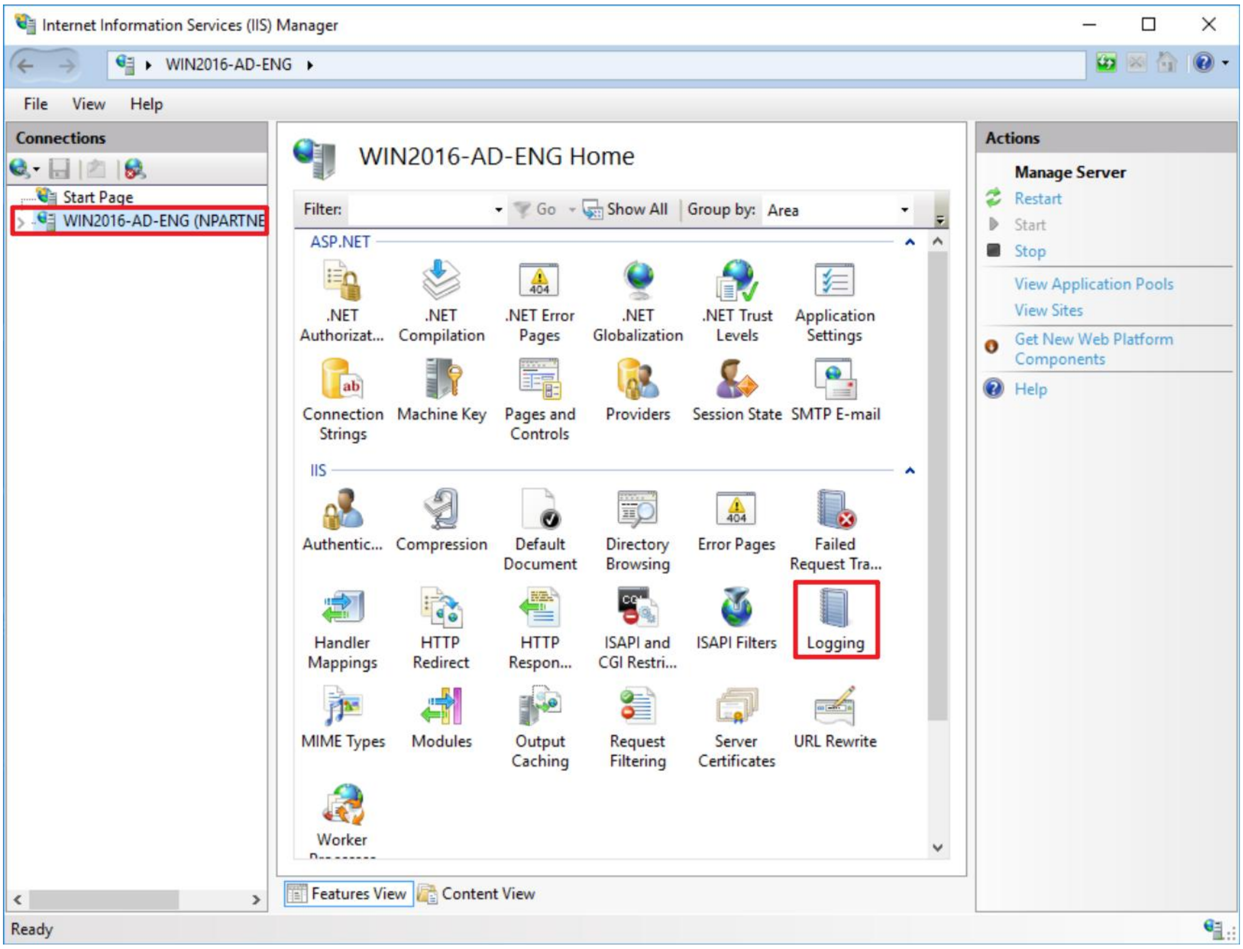
Replace the server name in red text with your Exchange server name.

5.2 IIS Log

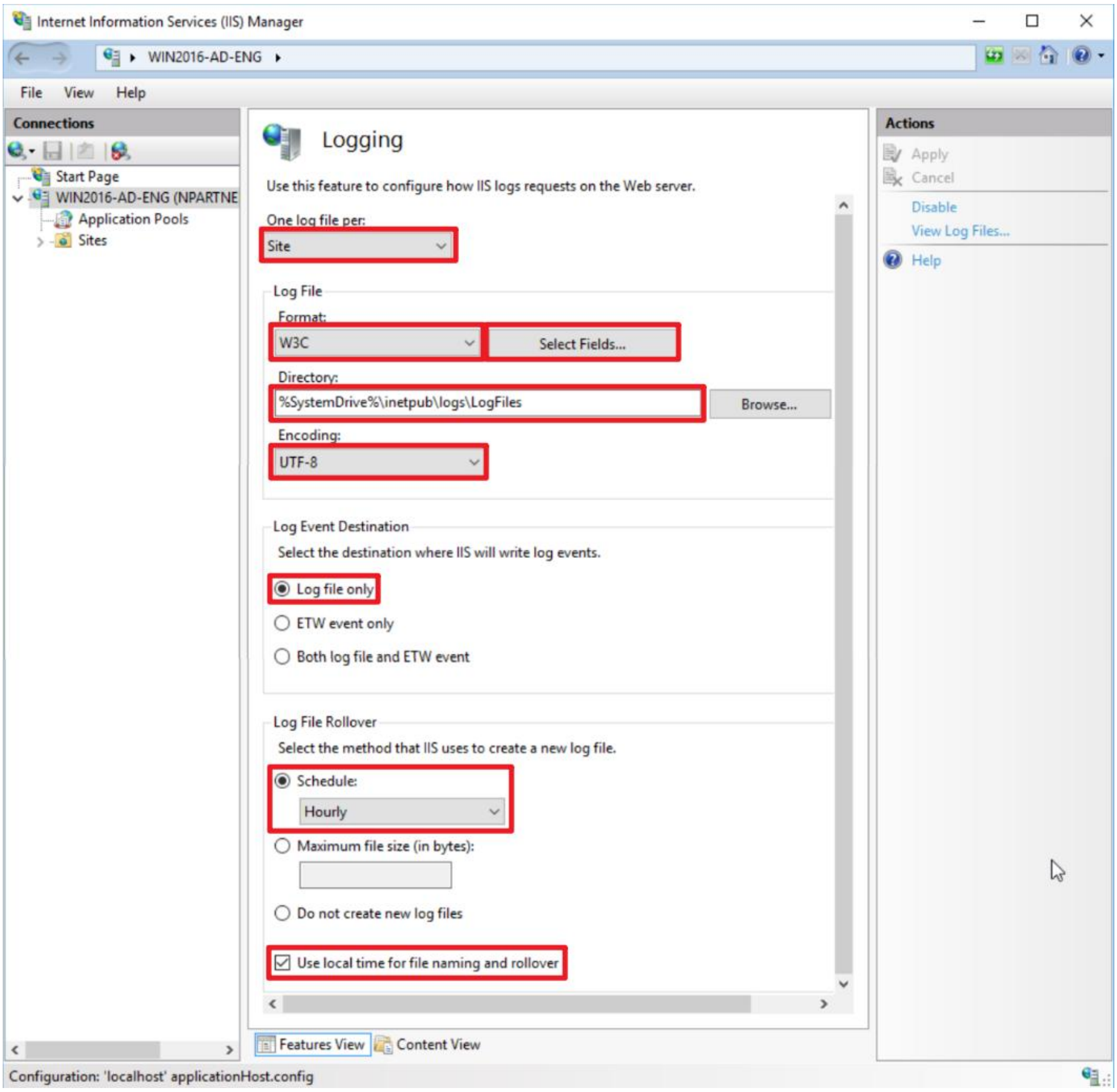
(1) Open “Internet Information Services (IIS) Manager.”



(2) Select your “IIS Server” (the example here is WIN2016-AD-ENG) → “Logging.”



(3) Select “One log file per site” → set “Log file format” to “W3C” → set “Directory” to %SystemDrive%\inetpub\logs\LogFiles → set “Encoding” to “UTF-8” → set “Log event destination” to “Log file only” → set “Schedule” to “Hourly” → check “Use local time for file naming and rollover” → click “Select Fields.”



Internet Information Services (IIS) Manager

WIN2016-AD-ENG

Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only

○ ETW event only

○ Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

● Schedule: Hourly

○ Maximum file size (in bytes):

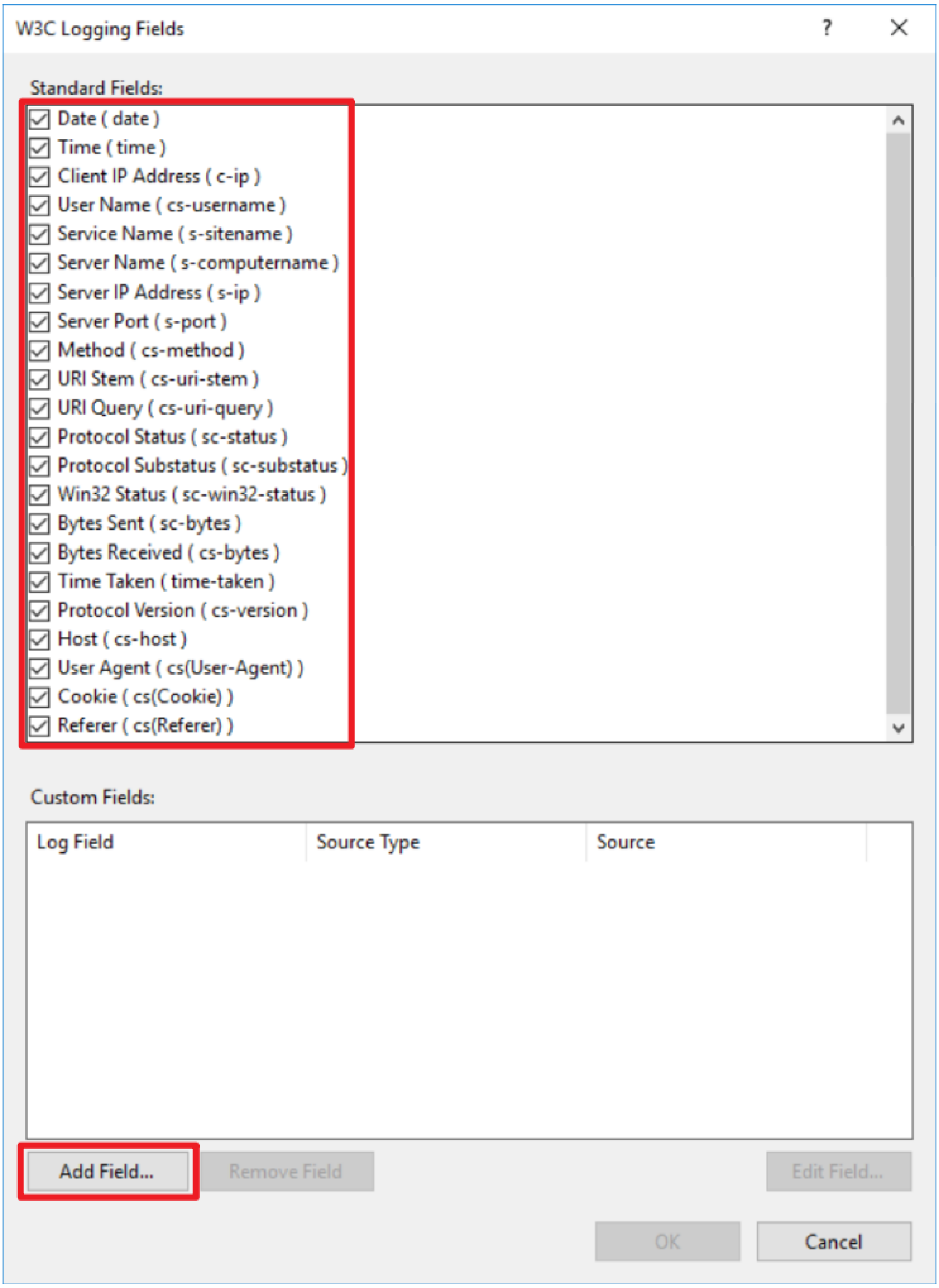
○ Do not create new log files

☑ Use local time for file naming and rollover

Configuration: 'localhost' applicationHost.config

(4) Select the following fields → click "Add Field":

"Date (date), Time (time), Client IP Address (c-ip), User Name (cs-username), Service Name (s-sitename), Server Name (s-computername), Server IP Address (s-ip), Server Port (s-port), Method (cs-method), URI Stem (cs-uri-stem), URI Query (cs-uri-query), Protocol Status (sc-status), Protocol Substatus (sc-substatus), Win32 Status (sc-win32-status), Bytes Sent (sc-bytes), Bytes Received (cs-bytes), Time Taken (time-taken), Protocol Version (cs-version), Host (cs-host), User Agent (cs(User-Agent)), Cookie (cs(Cookie)), Referrer (cs(Referer))."



W3C Logging Fields

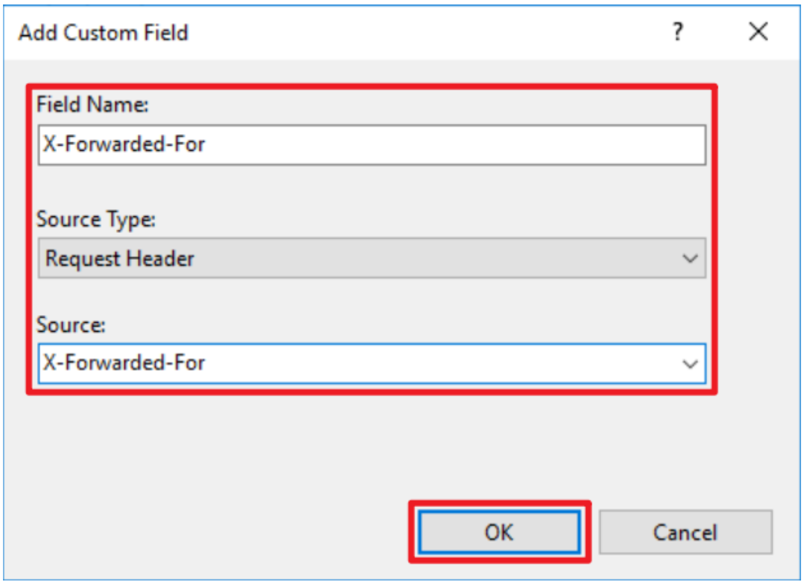
Standard Fields:

- ☑ Date (date)
- ☑ Time (time)
- ☑ Client IP Address (c-ip)
- ☑ User Name (cs-username)
- ☑ Service Name (s-sitename)
- ☑ Server Name (s-computername)
- ☑ Server IP Address (s-ip)
- ☑ Server Port (s-port)
- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ URI Query (cs-uri-query)
- ☑ Protocol Status (sc-status)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Win32 Status (sc-win32-status)
- ☑ Bytes Sent (sc-bytes)
- ☑ Bytes Received (cs-bytes)
- ☑ Time Taken (time-taken)
- ☑ Protocol Version (cs-version)
- ☑ Host (cs-host)
- ☑ User Agent (cs(User-Agent))
- ☑ Cookie (cs(Cookie))
- ☑ Referer (cs(Referer))

Custom Fields:

Log Field	Source Type	Source

(5) Enter field name: X-Forwarded-For → select "Source type": "Request Header" → enter source name: X-Forwarded-For → click "OK."



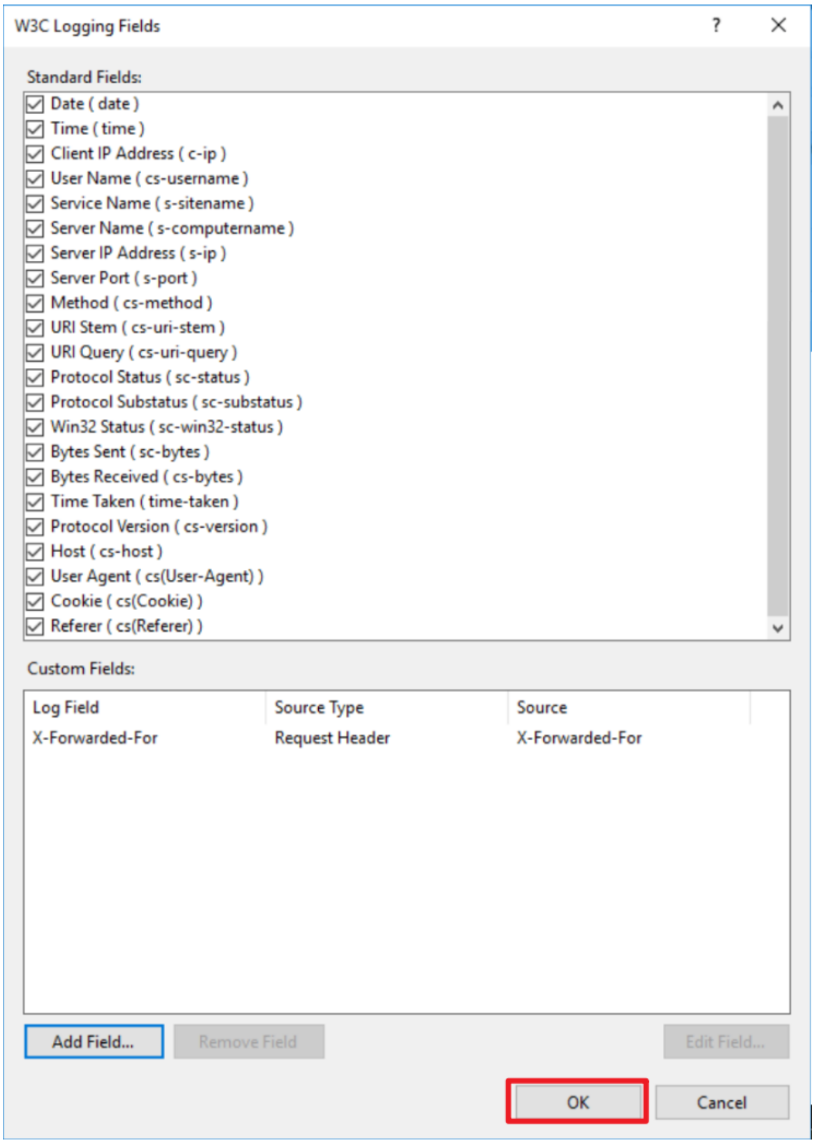
Add Custom Field

Field Name: X-Forwarded-For

Source Type: Request Header

Source: X-Forwarded-For

(6) Click "OK."



W3C Logging Fields

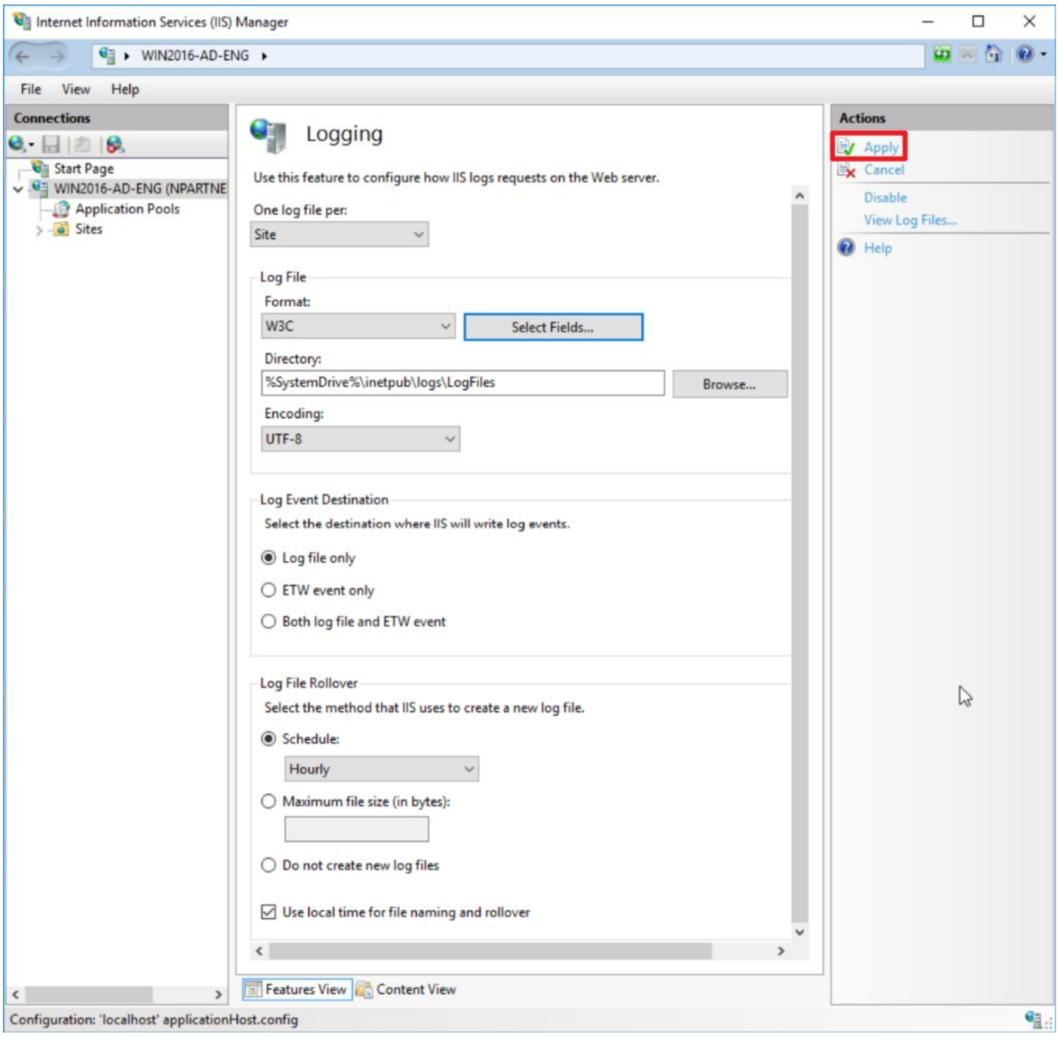
Standard Fields:

- ☑ Date (date)
- ☑ Time (time)
- ☑ Client IP Address (c-ip)
- ☑ User Name (cs-username)
- ☑ Service Name (s-sitename)
- ☑ Server Name (s-computername)
- ☑ Server IP Address (s-ip)
- ☑ Server Port (s-port)
- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ URI Query (cs-uri-query)
- ☑ Protocol Status (sc-status)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Win32 Status (sc-win32-status)
- ☑ Bytes Sent (sc-bytes)
- ☑ Bytes Received (cs-bytes)
- ☑ Time Taken (time-taken)
- ☑ Protocol Version (cs-version)
- ☑ Host (cs-host)
- ☑ User Agent (cs(User-Agent))
- ☑ Cookie (cs(Cookie))
- ☑ Referer (cs(Referer))

Custom Fields:

Log Field	Source Type	Source
X-Forwarded-For	Request Header	X-Forwarded-For

(7) Click "Apply."



Internet Information Services (IIS) Manager

WIN2016-AD-ENG ▸

File View Help

Connections

- Start Page
- WIN2016-AD-ENG (NPARTNE
  - Application Pools
  - Sites

Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C [Select Fields...]

Directory: %SystemDrive%\inetpub\logs\LogFiles [Browse...]

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only

○ ETW event only

○ Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

● Schedule: Hourly

○ Maximum file size (in bytes):

○ Do not create new log files

☑ Use local time for file naming and rollover

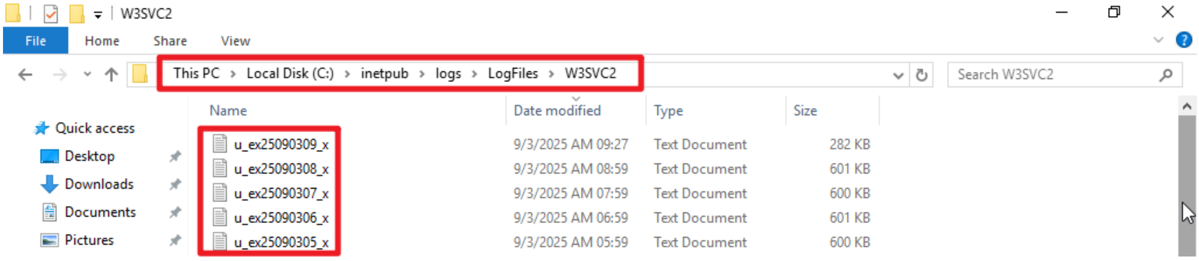
Features View | Content View

Actions

- Apply
- Cancel
- Disable
- View Log Files...
- Help

Configuration: 'localhost' applicationHost.config

(8) Verify IIS log files are created in the folder: C:\inetpub\logs\LogFiles\W3SVC2



W3SVC2

File Home Share View

This PC › Local Disk (C:) › inetpub › logs › LogFiles › W3SVC2

Search W3SVC2

Quick access: Desktop, Downloads, Documents, Pictures

Name	Date modified	Type	Size
u_ex25090309_x	9/3/2025 AM 09:27	Text Document	282 KB
u_ex25090308_x	9/3/2025 AM 08:59	Text Document	601 KB
u_ex25090307_x	9/3/2025 AM 07:59	Text Document	600 KB
u_ex25090306_x	9/3/2025 AM 06:59	Text Document	601 KB
u_ex25090305_x	9/3/2025 AM 05:59	Text Document	600 KB

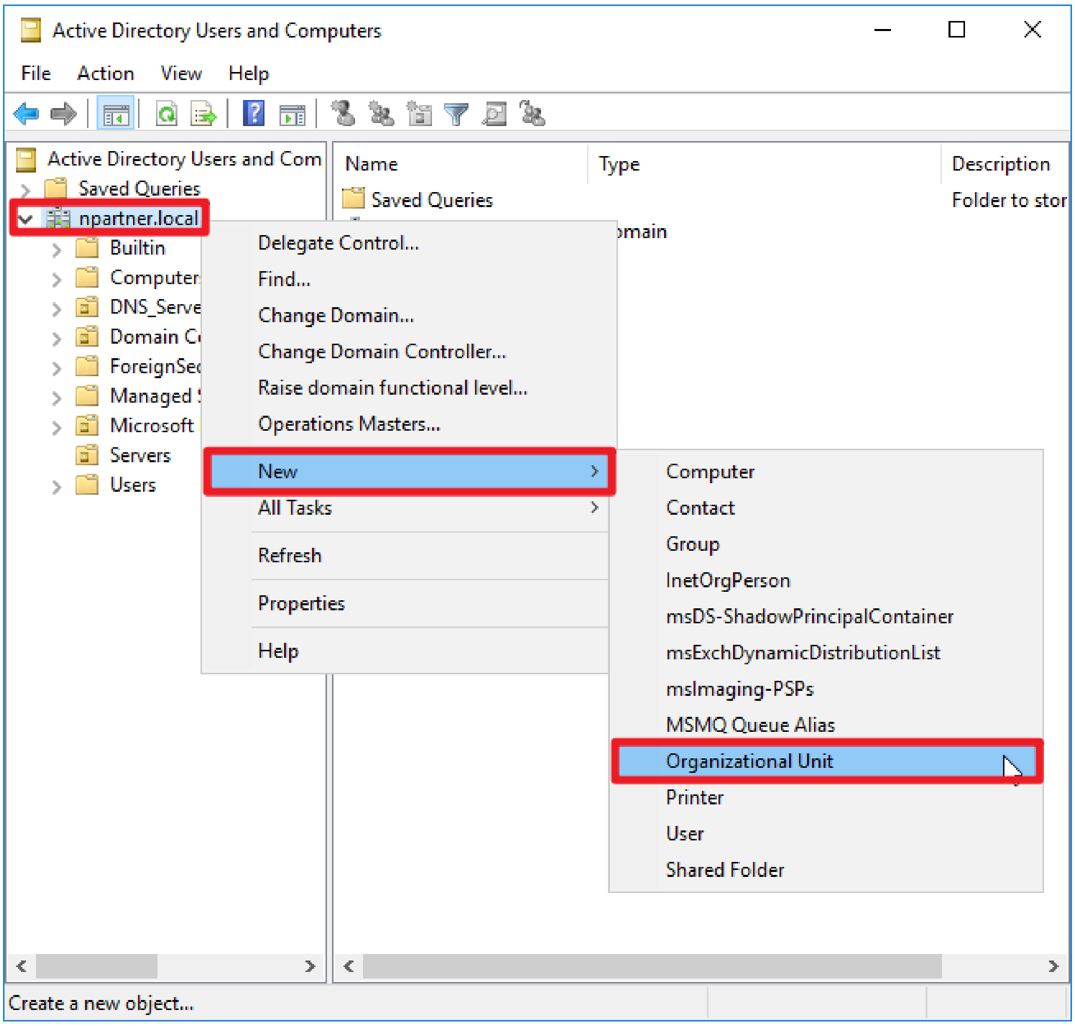
5.3 Event Log

5.3.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”

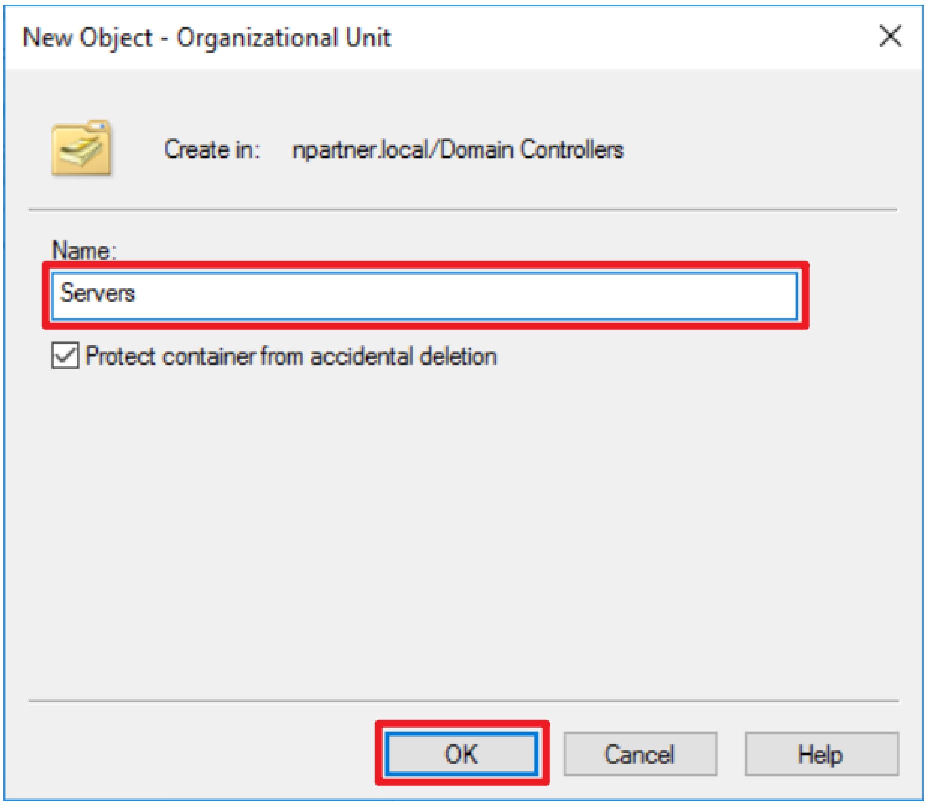
(2) Add an Organizational Unit

Right-click on the domain name (the example here is npartner.local) → select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit name according to the actual environment. → click “OK.”



New Object - Organizational Unit

Create in: npartner.local/Domain Controllers

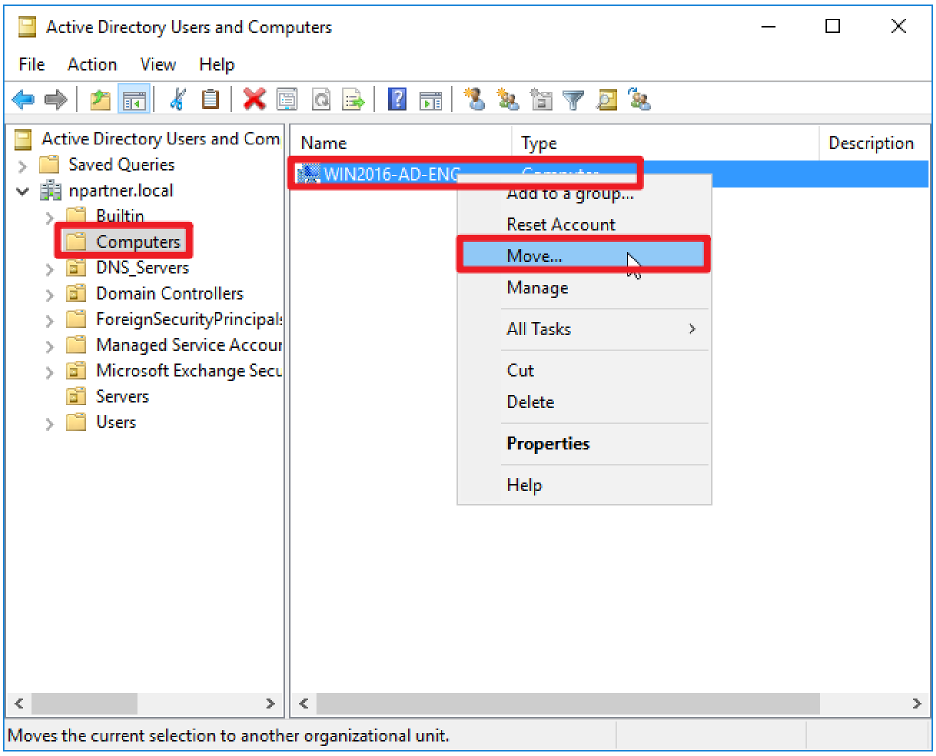
Name: Servers

☑ Protect container from accidental deletion

(4) Move the Server to your New Organizational Unit:

Select “Domain Controllers” → right-click on the “WIN2016-AD-ENG” server.

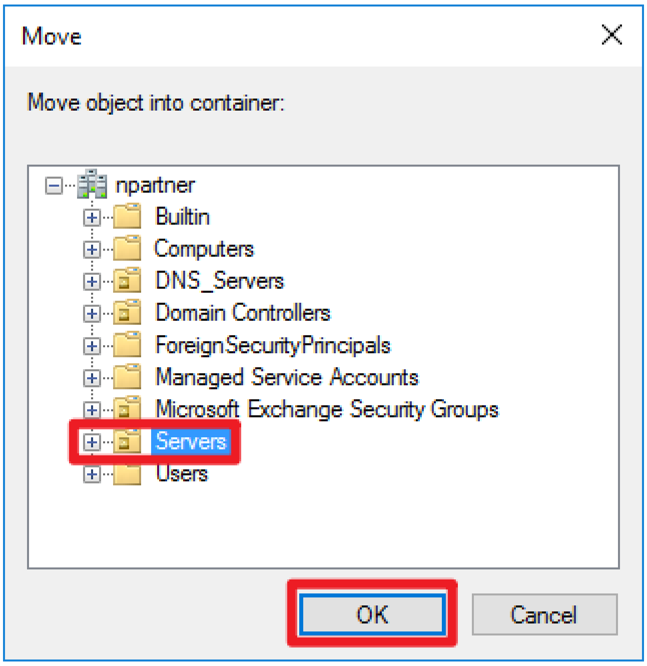
Note: Please select the Windows file server according to the actual environment. → click “Move.”



Moves the current selection to another organizational unit.

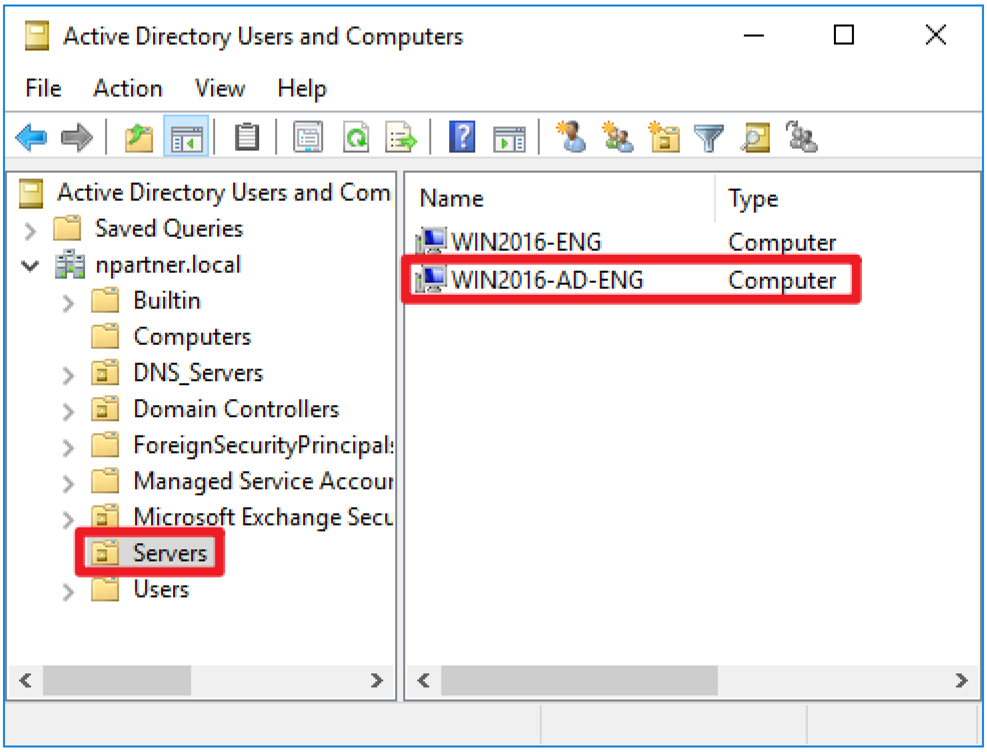
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is "Servers") → click "OK."



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is "Servers") and confirm that the "WIN2016-AD-ENG" server has been moved.



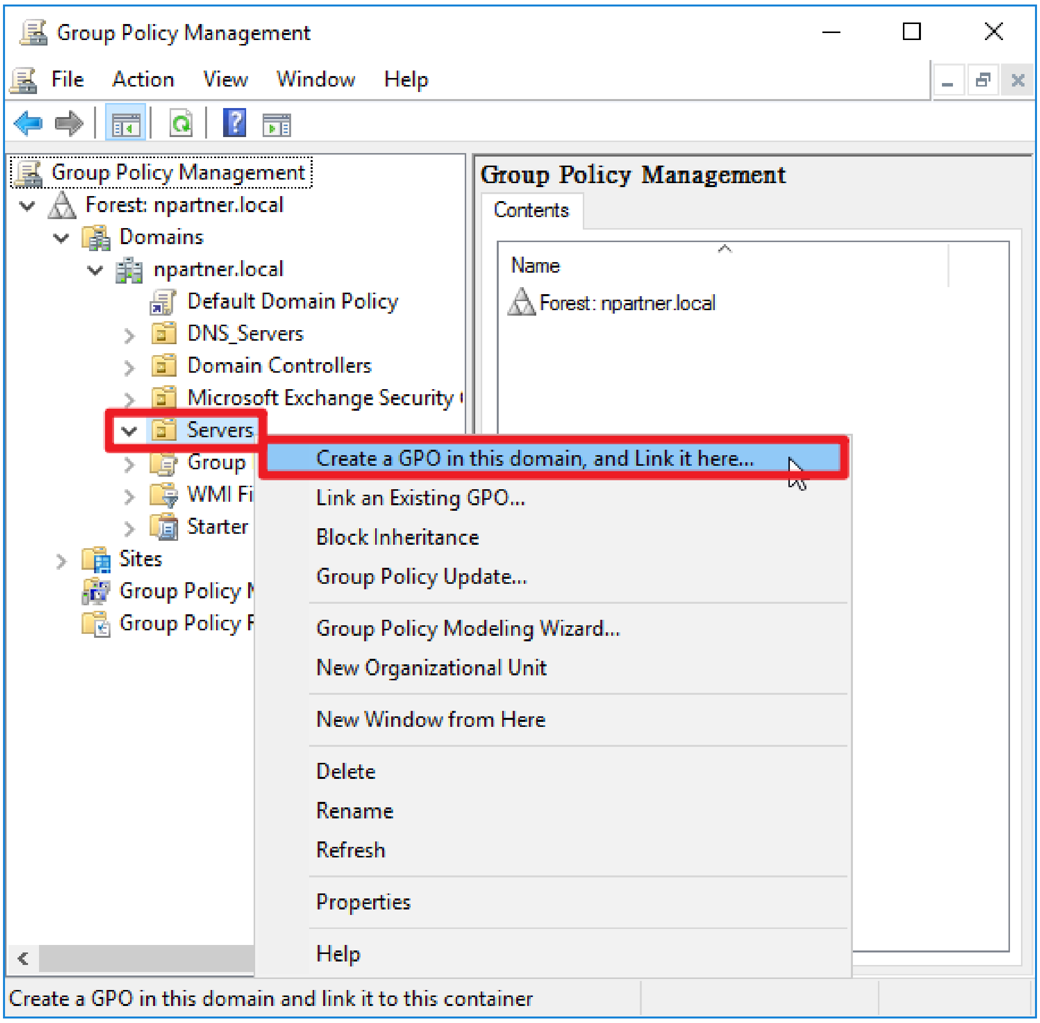
Name	Type
WIN2016-ENG	Computer
WIN2016-AD-ENG	Computer

5.3.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

Right-click the “Servers” organizational unit→ select “Create a GPO in this domain, and Link it here...”

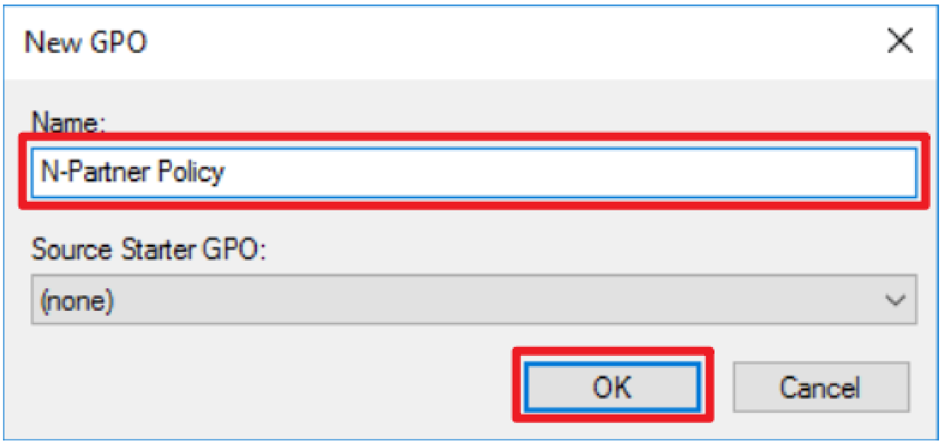


Create a GPO in this domain and link it to this container

(3) Edit your Group Policy Object

Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. Then click “Edit.”


New GPO

Name:

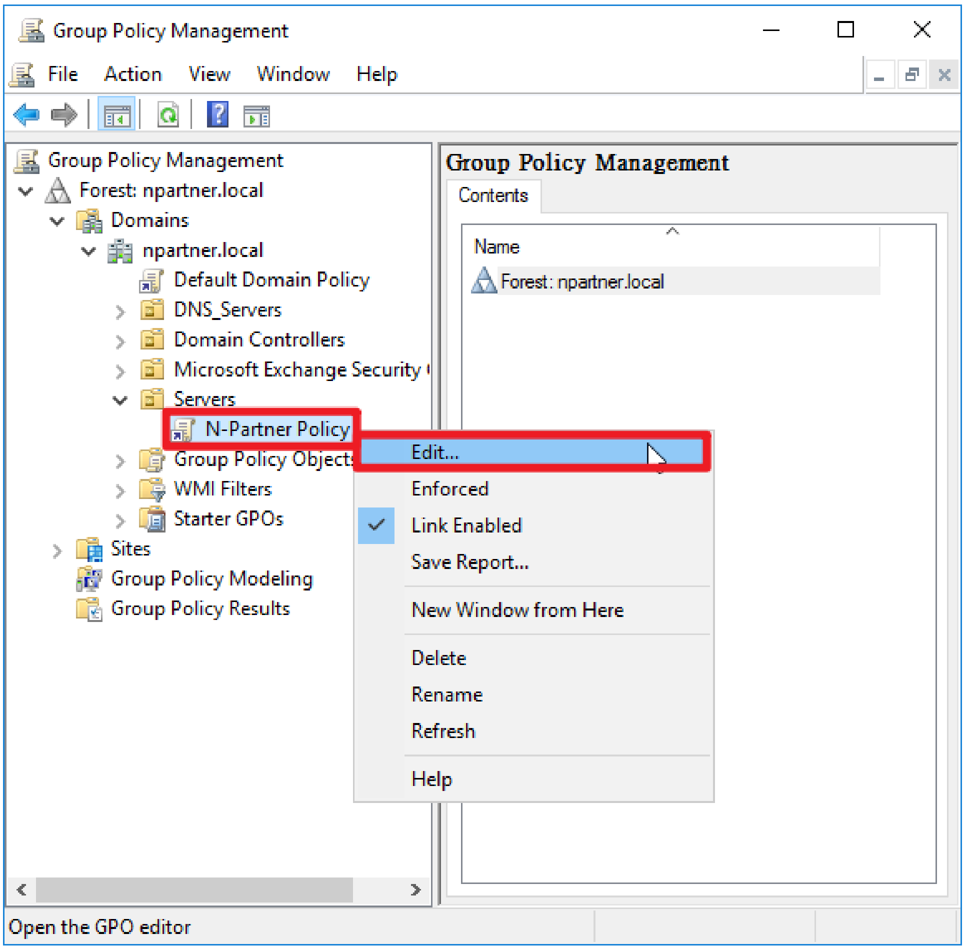
N-Partner Policy

Source Starter GPO:

(none)

(4) Edit your Group Policy Object

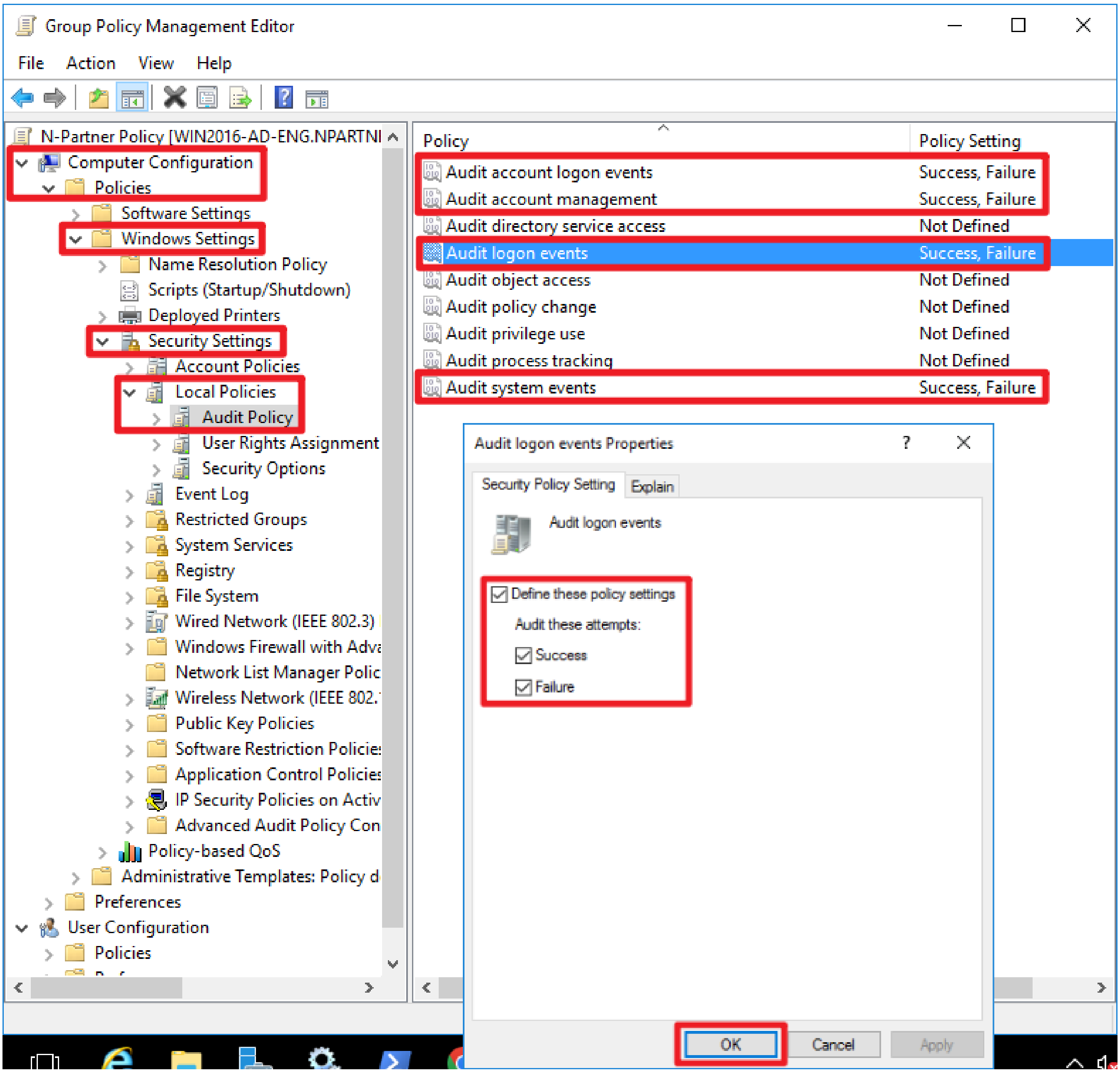
In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



Open the GPO editor

(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” and “Audit system events” → check “Define these policy settings”: Success, Failure. → click “OK.”



Group Policy Management Editor

File Action View Help

- N-Partner Policy [WIN2016-AD-ENG.NPARTNI
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Deployed Printers
        - Security Settings
          - Account Policies
          - Local Policies
            - Audit Policy
            - User Rights Assignment
            - Security Options
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3)
          - Windows Firewall with Adva
          - Network List Manager Polic
          - Wireless Network (IEEE 802.
          - Public Key Policies
          - Software Restriction Policie
          - Application Control Policies
          - IP Security Policies on Activ
          - Advanced Audit Policy Con
        - Policy-based QoS
      - Administrative Templates: Policy d
    - Preferences
  - User Configuration
    - Policies

Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Success, Failure

Audit logon events Properties

Security Policy Setting | Explain

Audit logon events

☑ Define these policy settings

Audit these attempts:

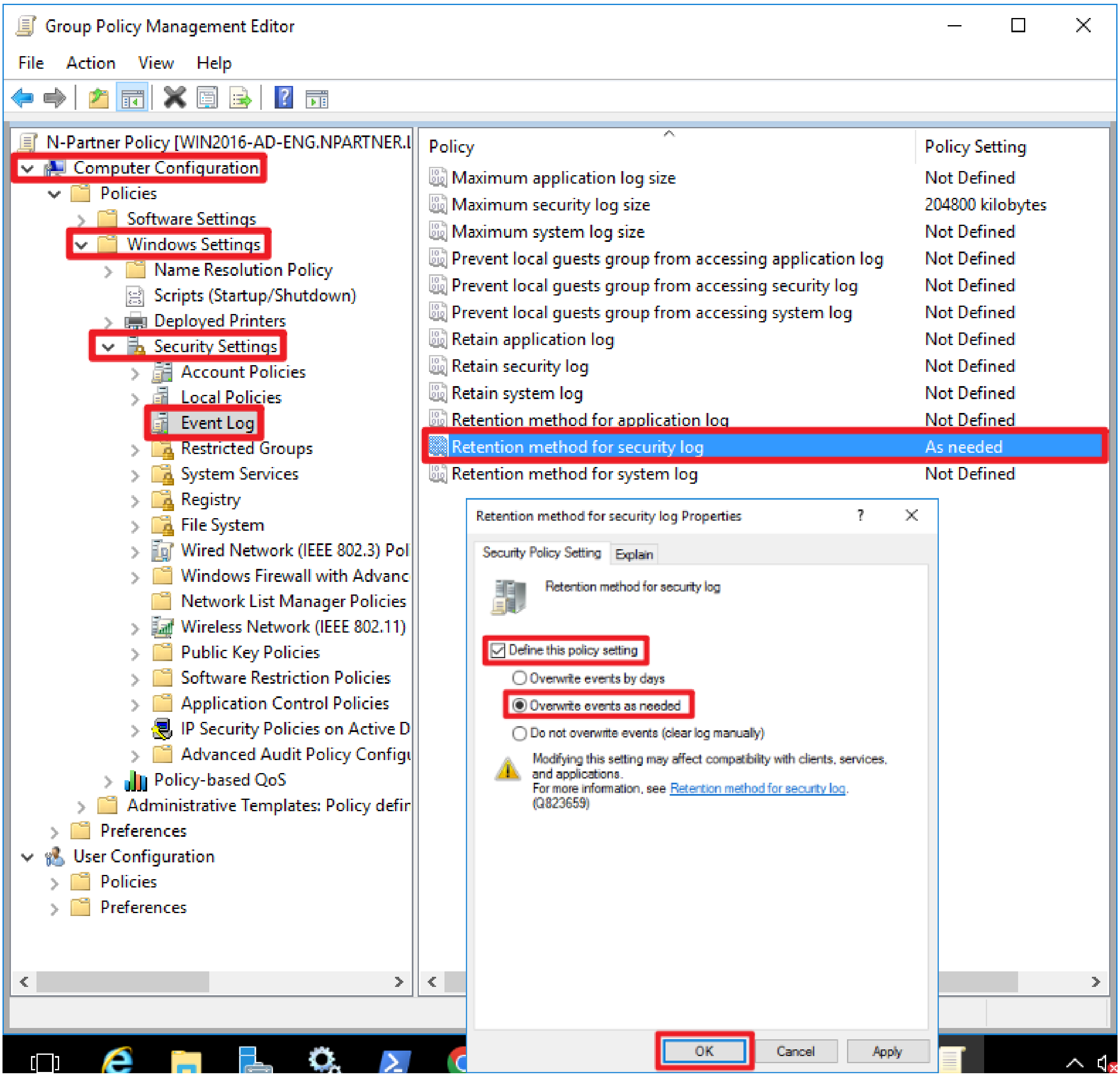
☑ Success

☑ Failure

OK | Cancel | Apply

(6) Event Log: Security Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



Group Policy Management Editor
File Action View Help
N-Partner Policy [WIN2016-AD-ENG.NPARTNER.I
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Firewall with Advanc
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates: Policy defir
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Retention method for security log

☑ Define this policy setting

○ Overwrite events by days

● Overwrite events as needed

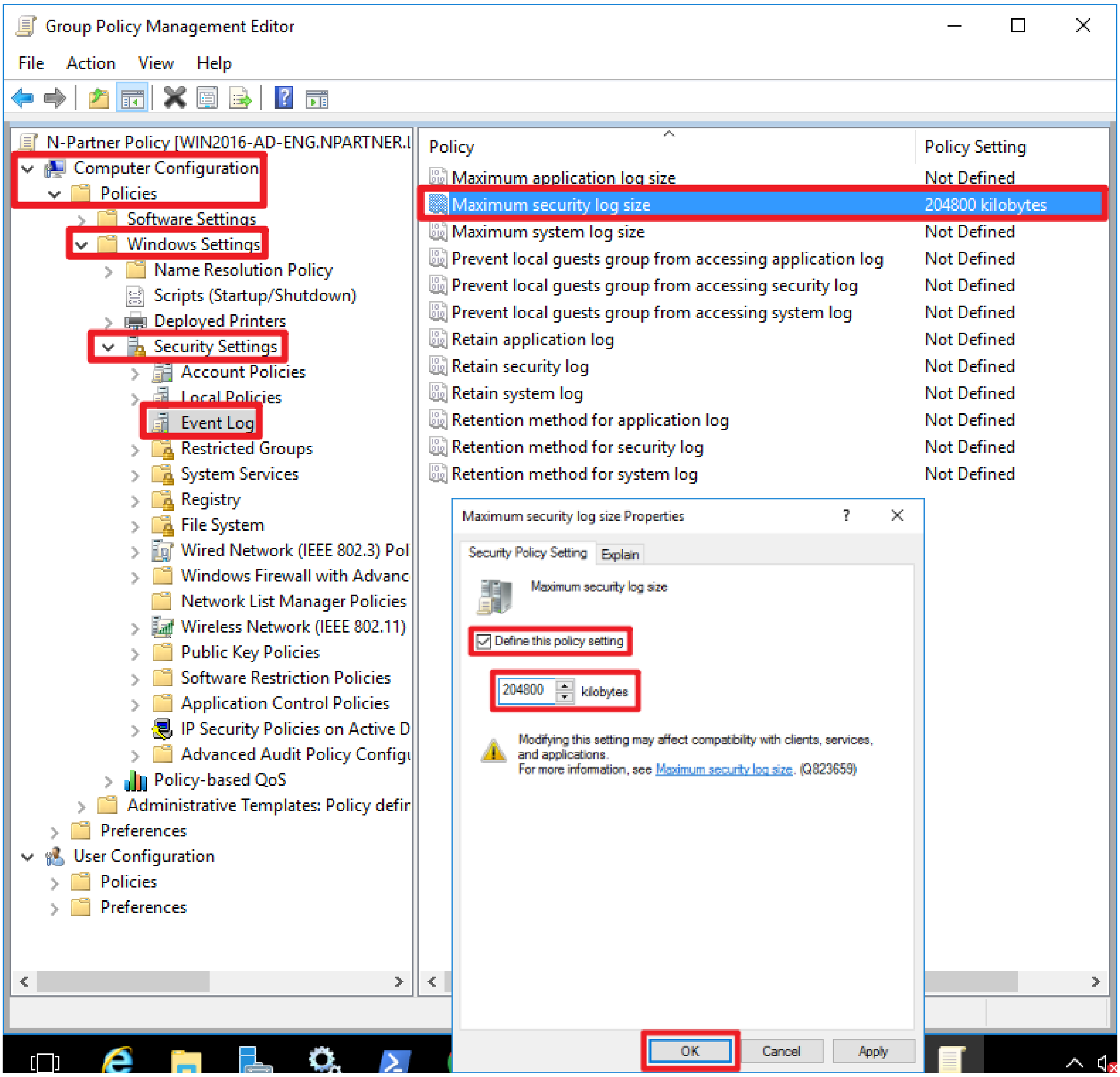
○ Do not overwrite events (clear log manually)

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Retention method for security log. (Q823659)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”


Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2016-AD-ENG.NPARTNER.l
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Firewall with Advanc
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Configu
Policy-based QoS
Administrative Templates: Policy defir
Preferences
User Configuration
Policies
Preferences
Maximum security log size Properties
Security Policy Setting
Explain
OK
Cancel
Apply

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum security log size

☑ Define this policy setting

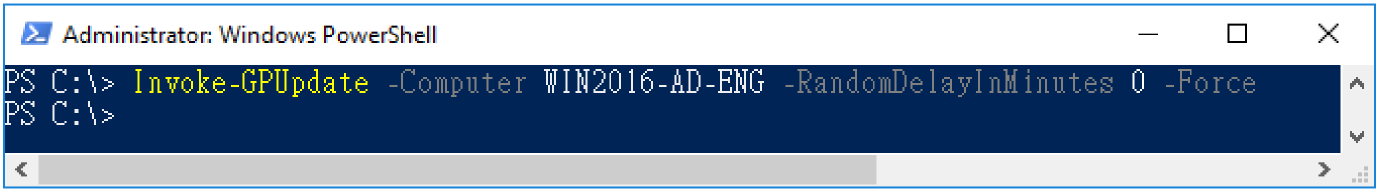
204800 kilobytes

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Maximum security log size. (Q823659)

(8) Open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer Win-AD-2016 -RandomDelayInMinutes 0 -Force
```

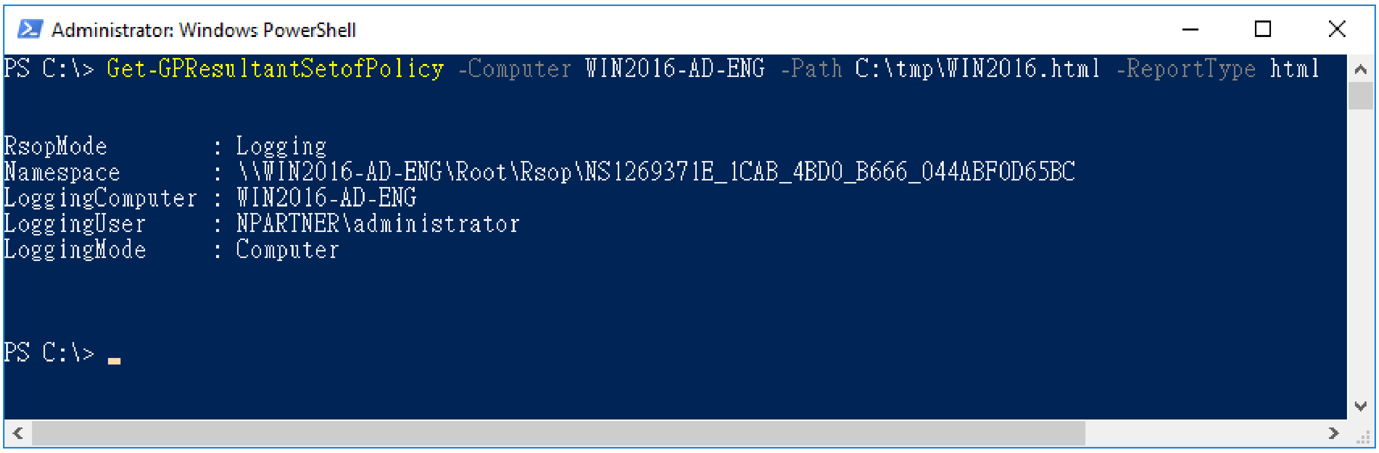


```
PS C:\> Invoke-GPUpdate -Computer WIN2016-AD-ENG -RandomDelayInMinutes 0 -Force
PS C:\>
```

Replace the red text section with the name of your Exchange server.

(10) Enter the command below to generate server group policy report.

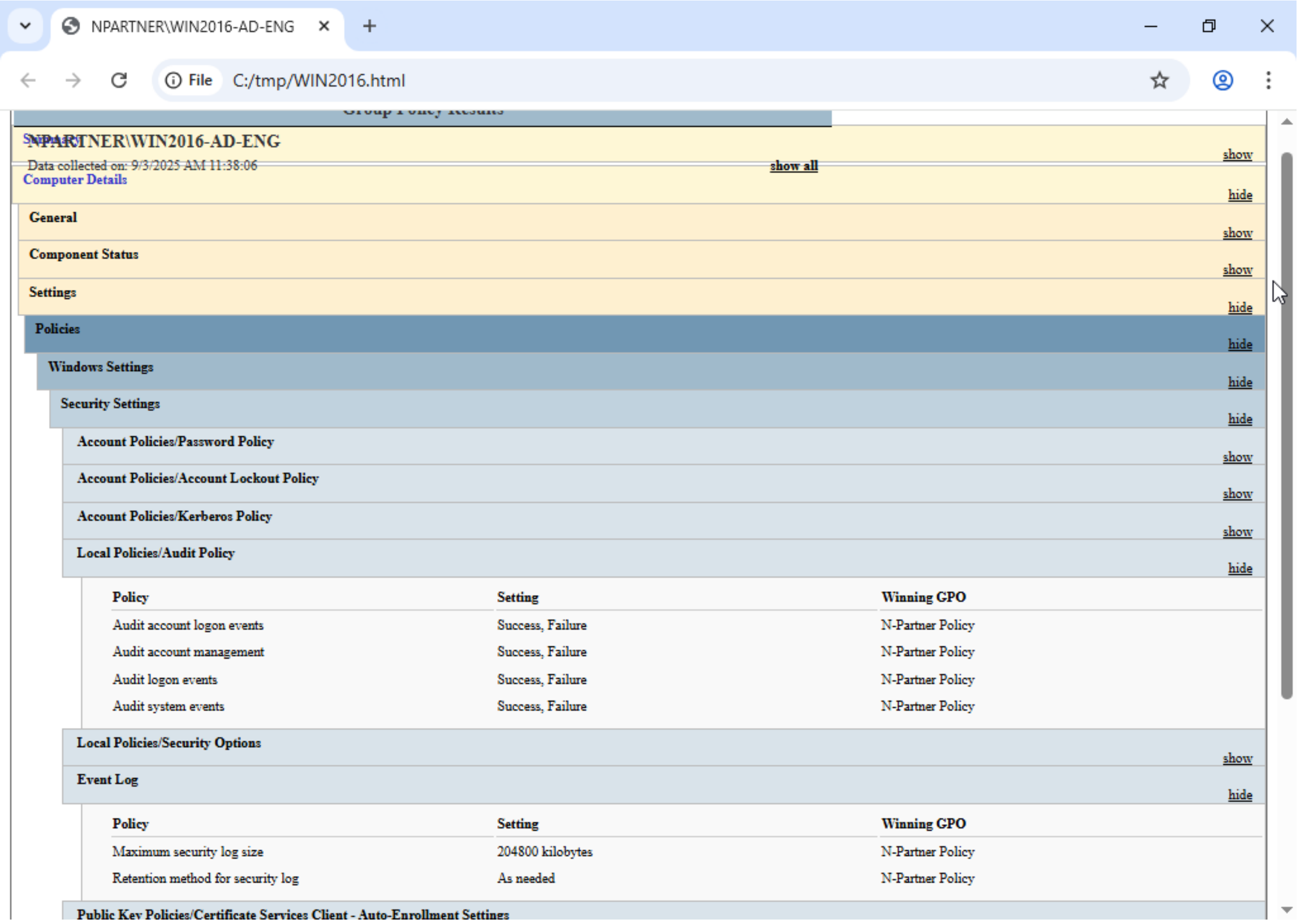
```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2016-AD-ENG -Path C:\tmp\Win2016.html -
ReportType html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2016-AD-ENG -Path C:\tmp\WIN2016.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2016-AD-ENG\Root\Rsop\NS1269371E_1CAB_4BD0_B666_044ABF0D65BC
LoggingComputer : WIN2016-AD-ENG
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer



PS C:\> _
```

For the red text , please enter the Windows file server name and the folder path/file name.

(11) Open the report and verify that your Windows AD server is applying the N-Partner Policy Group Policy.



Group Policy Results

Summary

NPARTNER\WIN2016-AD-ENG

Data collected on: 9/3/2025 AM 11:38:06 — show all — show

Computer Details — hide

General — show

Component Status — show

Settings — hide

Policies — hide

Windows Settings — hide

Security Settings — hide

Account Policies/Password Policy — show

Account Policies/Account Lockout Policy — show

Account Policies/Kerberos Policy — show

Local Policies/Audit Policy — hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy

Local Policies/Security Options — show

Event Log — hide

Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

6. Exchange 2019

Example: Exchange 2019 installed on a Windows 2022 server.

Message tracking logs can be configured through the “Exchange Administrative Center” or the “Exchange Management Shell.”

6.1 Exchange MessageTracking Log

Modify nxlog.conf

Note: Please refer to 1.3 NXLog Configuration File.

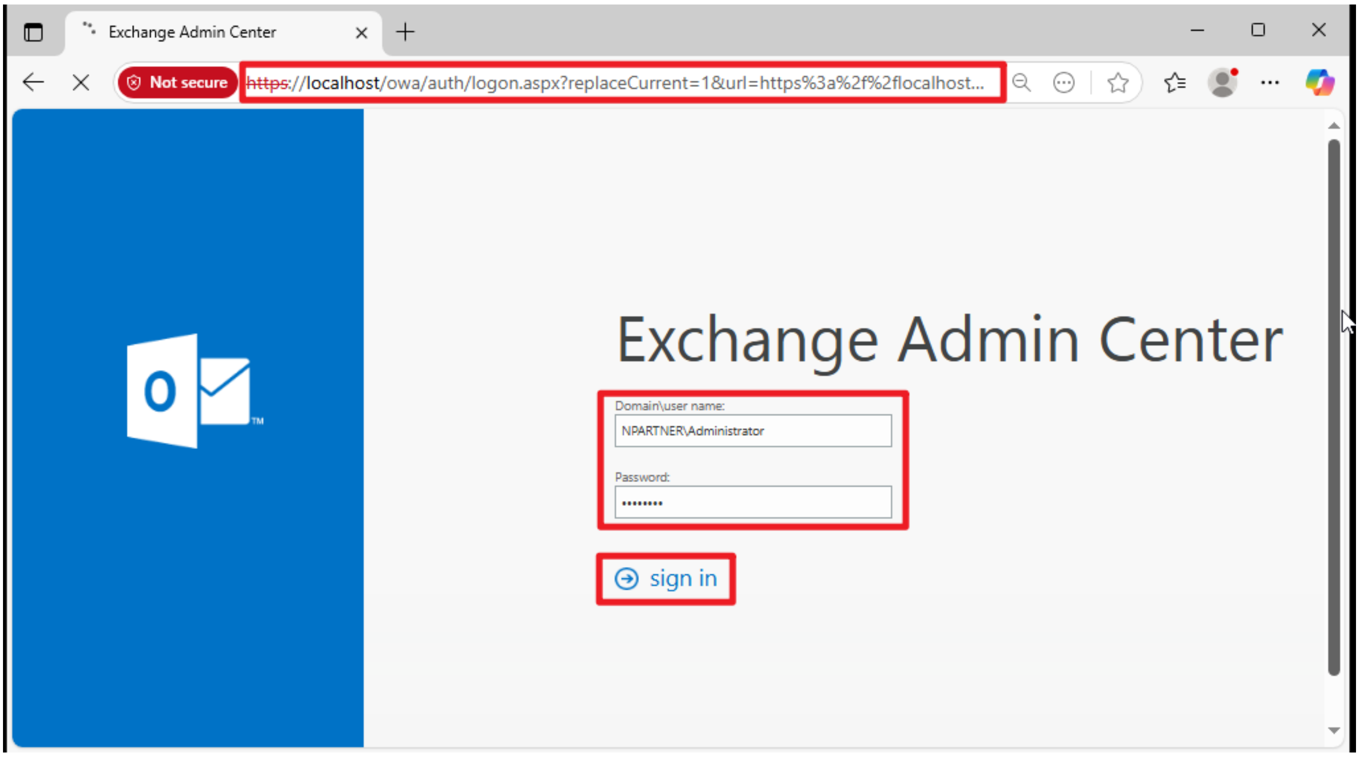
Edit the blue text section to specify the message tracking log folder:

```
define MailLog C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking
```

6.1.1 Exchange Administrative Center

(1) Open “Exchange Administrative Center.”

(2) Enter the URL: https://<ExchangeIP>/ecp → enter “Domain\username” and password → click “Sign in.”

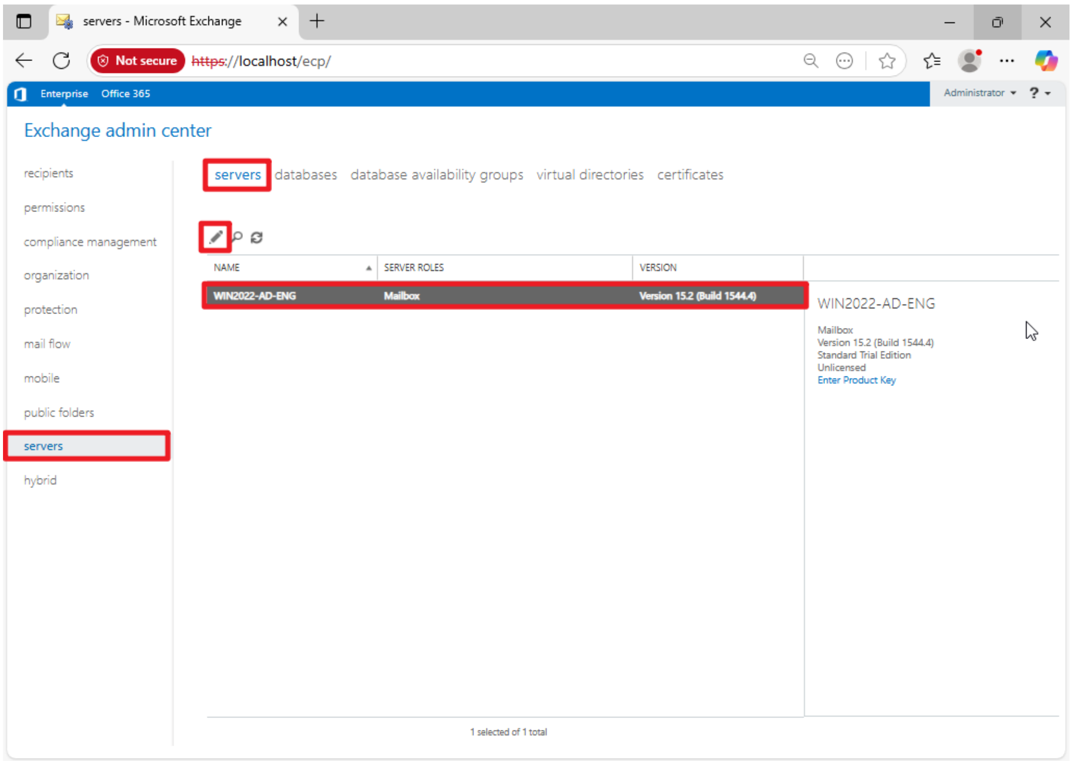

Exchange Admin Center
Not secure
~~https~~://localhost/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2flocalhost...
Exchange Admin Center

Domain\user name:
NPARTNER\Administrator

Password:
••••••••

sign in

(3) Select the “Servers” page → select “Servers” → select “Mailbox Server (WIN2022-AD-ENG)” → click “Edit.”



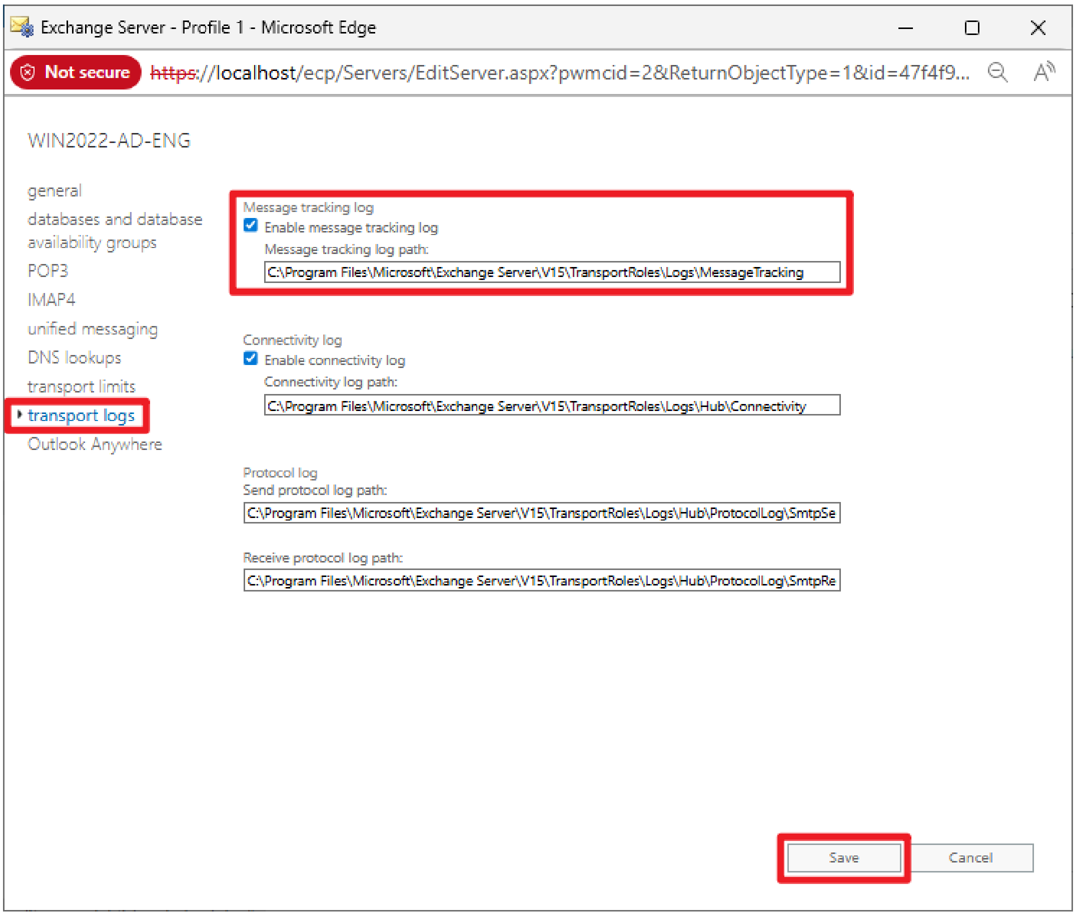
NAME	SERVER ROLES	VERSION
WIN2022-AD-ENG	Mailbox	Version 15.2 (Build 1544.4)

WIN2022-AD-ENG

Mailbox
Version 15.2 (Build 1544.4)
Standard Trial Edition
Unlicensed
Enter Product Key

1 selected of 1 total

(4) Select “Transport Logs” → verify “Enable message tracking log” is checked and the log path is set to: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking → click “Save.”


Exchange Server - Profile 1 - Microsoft Edge
Not secure
https://localhost/ecp/Servers/EditServer.aspx?pwmcid=2&ReturnObjectType=1&id=47f4f9...
WIN2022-AD-ENG
general
databases and database availability groups
POP3
IMAP4
unified messaging
DNS lookups
transport limits
transport logs
Outlook Anywhere
Save
Cancel

Message tracking log
☑ Enable message tracking log
Message tracking log path:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking

Connectivity log
☑ Enable connectivity log
Connectivity log path:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\Connectivity

Protocol log
Send protocol log path:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\ProtocolLog\SmtpSe

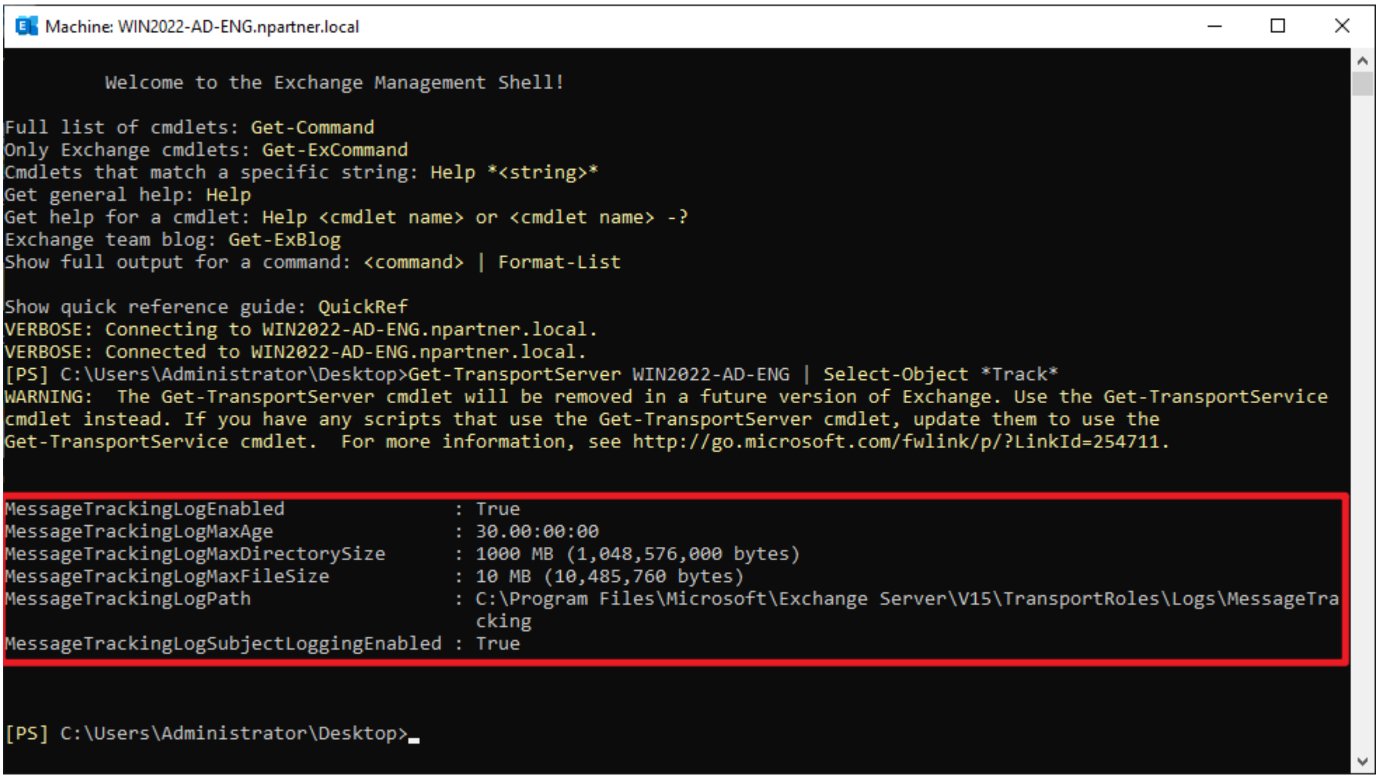
Receive protocol log path:
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\Hub\ProtocolLog\SmtpRe

6.1.2 Exchange Management Shell

(1) Open “Exchange Management Shell.”

(2) Verify “Enable message tracking log” is checked and the log path is set to: [C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Logs\MessageTracking]
and run the following command in “Exchange Management Shell”:

```
[PS] C:\> Get-TransportServer Win2022-AD-ENG | Select-Object *Track*
```

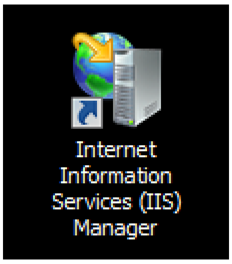


```
        Welcome to the Exchange Management Shell!

Full list of cmdlets: Get-Command
Only Exchange cmdlets: Get-ExCommand
Cmdlets that match a specific string: Help *<string>*
Get general help: Help
Get help for a cmdlet: Help <cmdlet name> or <cmdlet name> -?
Exchange team blog: Get-ExBlog
Show full output for a command: <command> | Format-List

Show quick reference guide: QuickRef
VERBOSE: Connecting to WIN2022-AD-ENG.npartner.local.
VERBOSE: Connected to WIN2022-AD-ENG.npartner.local.
[PS] C:\Users\Administrator\Desktop>Get-TransportServer WIN2022-AD-ENG | Select-Object *Track*
WARNING:  The Get-TransportServer cmdlet will be removed in a future version of Exchange. Use the Get-TransportService
cmdlet instead. If you have any scripts that use the Get-TransportServer cmdlet, update them to use the
Get-TransportService cmdlet.  For more information, see http://go.microsoft.com/fwlink/p/?LinkId=254711.


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\V15\TransportRoles\Logs\MessageTra
                                           cking
MessageTrackingLogSubjectLoggingEnabled : True



[PS] C:\Users\Administrator\Desktop>_
```

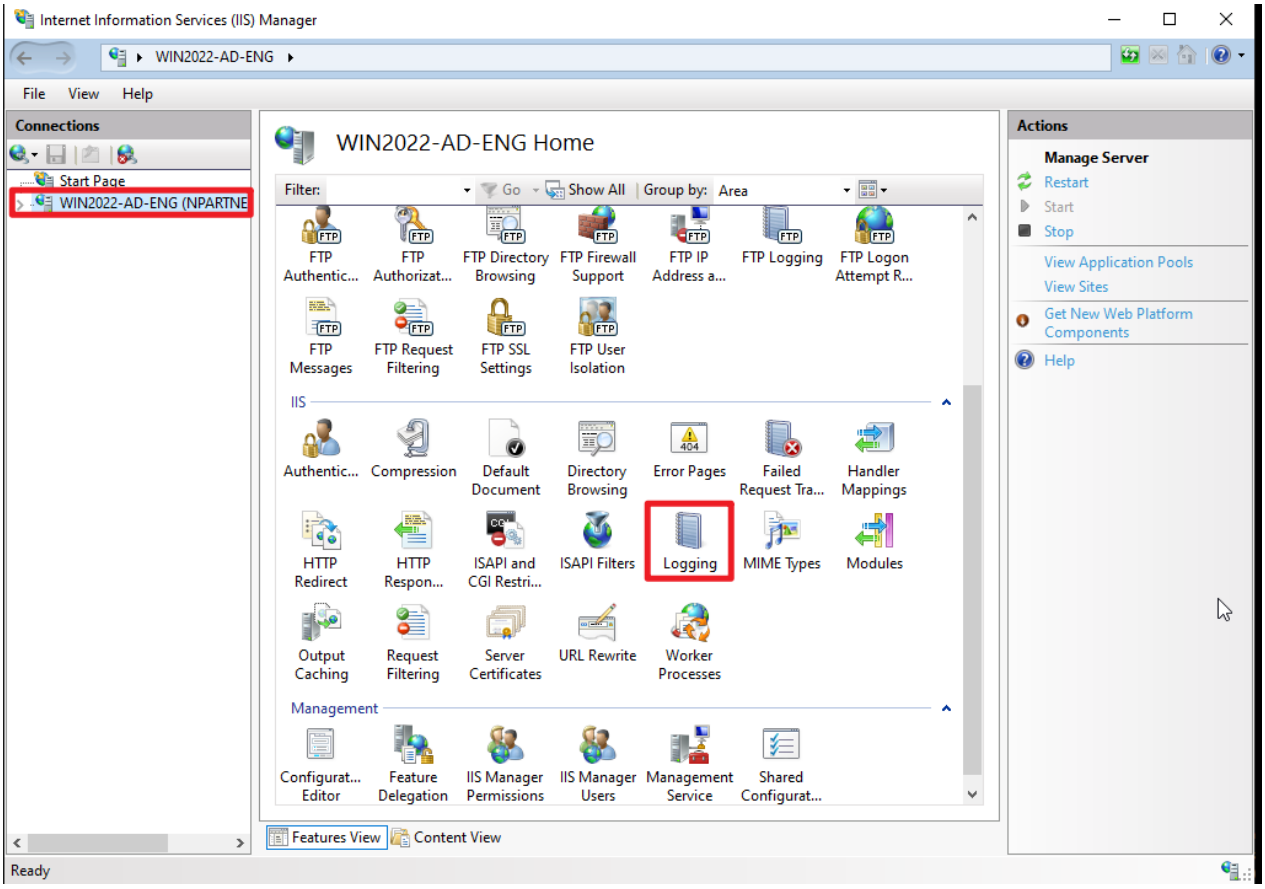
Replace the server name in red text with your Exchange server name.

6.2 IIS Log

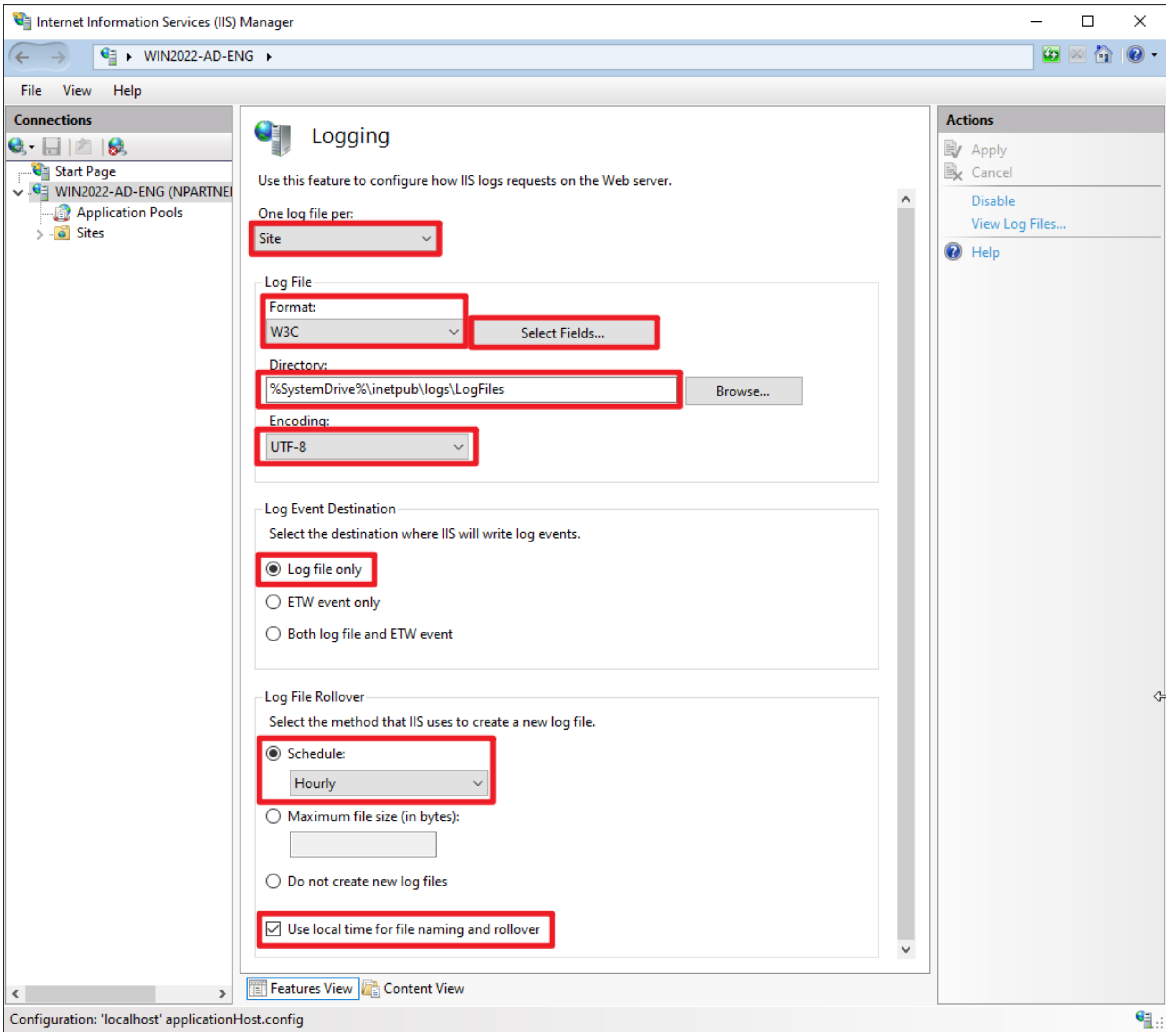
(1) Open "Internet Information Services (IIS) Manager."



(2) Select your "IIS Server" (the example here is WIN2016-AD-ENG) → "Logging."



(3) Select “One log file per site” → set “Log file format” to “W3C” → set “Directory” to %SystemDrive%\inetpub\logs\LogFiles → set “Encoding” to “UTF-8” → set “Log event destination” to “Log file only” → set “Schedule” to “Hourly” → check “Use local time for file naming and rollover” → click “Select Fields.”



Internet Information Services (IIS) Manager

WIN2022-AD-ENG

Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only

○ ETW event only

○ Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

● Schedule: Hourly

○ Maximum file size (in bytes):

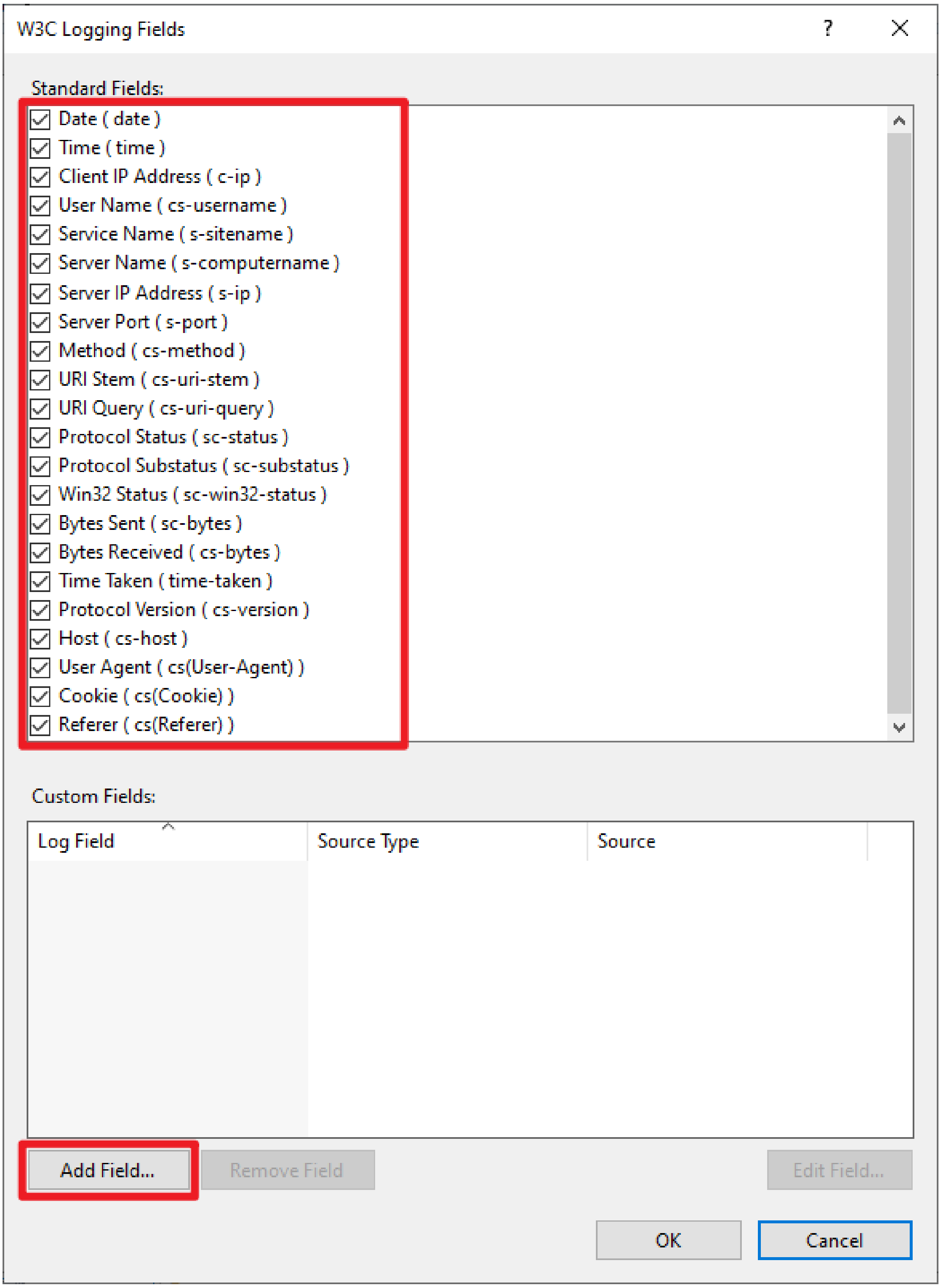
○ Do not create new log files

☑ Use local time for file naming and rollover

Configuration: 'localhost' applicationHost.config

(4) Select the following fields → click “Add Field”:

“Date (date), Time (time), Client IP Address (c-ip), User Name (cs-username), Service Name (s-sitename), Server Name (s-computername), Server IP Address (s-ip), Server Port (s-port), Method (cs-method), URI Stem (cs-uri-stem), URI Query (cs-uri-query), Protocol Status (sc-status), Protocol Substatus (sc-substatus), Win32 Status (sc-win32-status), Bytes Sent (sc-bytes), Bytes Received (cs-bytes), Time Taken (time-taken), Protocol Version (cs-version), Host (cs-host), User Agent (cs(User-Agent)), Cookie (cs(Cookie)), Referrer (cs(Referer)).”



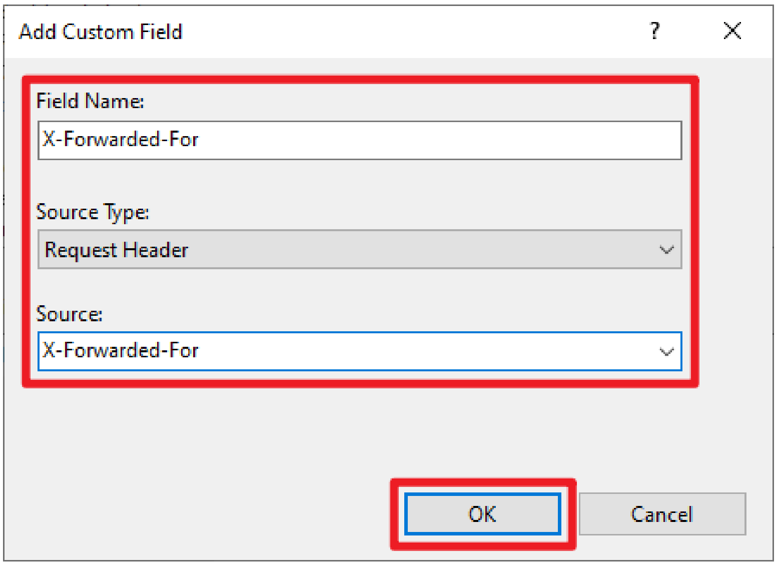
Standard Fields:

- ☑ Date (date)
- ☑ Time (time)
- ☑ Client IP Address (c-ip)
- ☑ User Name (cs-username)
- ☑ Service Name (s-sitename)
- ☑ Server Name (s-computername)
- ☑ Server IP Address (s-ip)
- ☑ Server Port (s-port)
- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ URI Query (cs-uri-query)
- ☑ Protocol Status (sc-status)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Win32 Status (sc-win32-status)
- ☑ Bytes Sent (sc-bytes)
- ☑ Bytes Received (cs-bytes)
- ☑ Time Taken (time-taken)
- ☑ Protocol Version (cs-version)
- ☑ Host (cs-host)
- ☑ User Agent (cs(User-Agent))
- ☑ Cookie (cs(Cookie))
- ☑ Referer (cs(Referer))

Custom Fields:

Log Field	Source Type	Source

(5) Enter field name: X-Forwarded-For → select “Source type”: “Request Header” → enter source name: X-Forwarded-For → click “OK.”



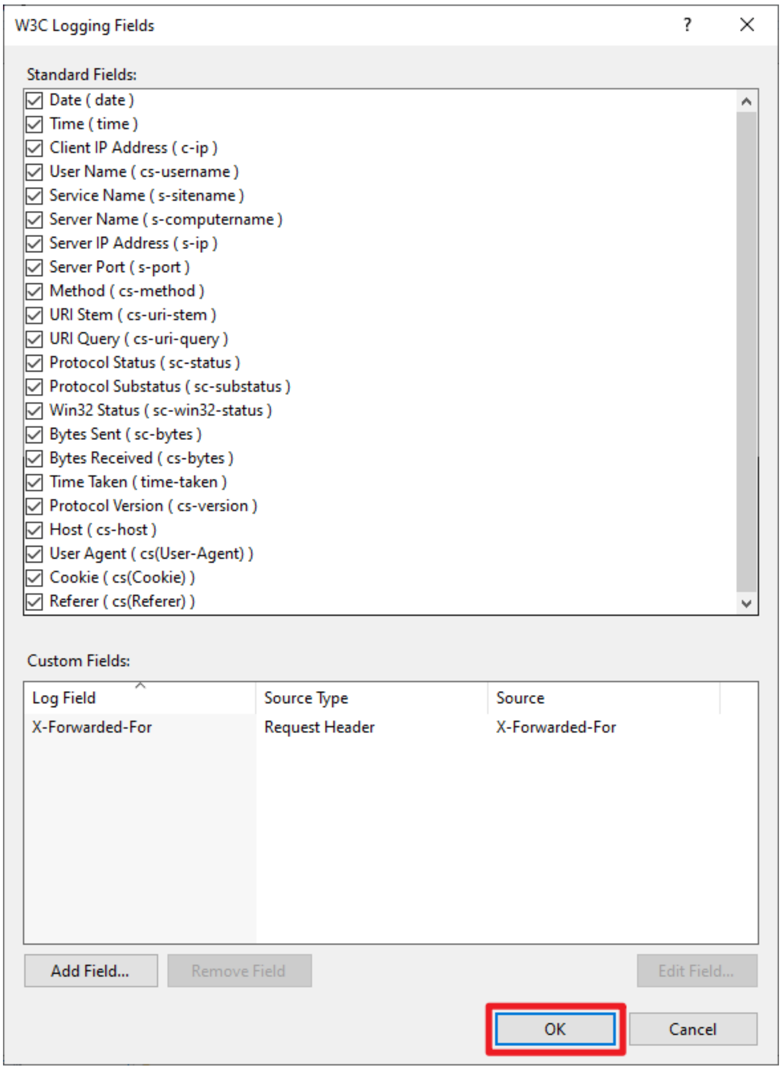
Add Custom Field

Field Name: X-Forwarded-For

Source Type: Request Header

Source: X-Forwarded-For

(6) Click “OK.”



W3C Logging Fields

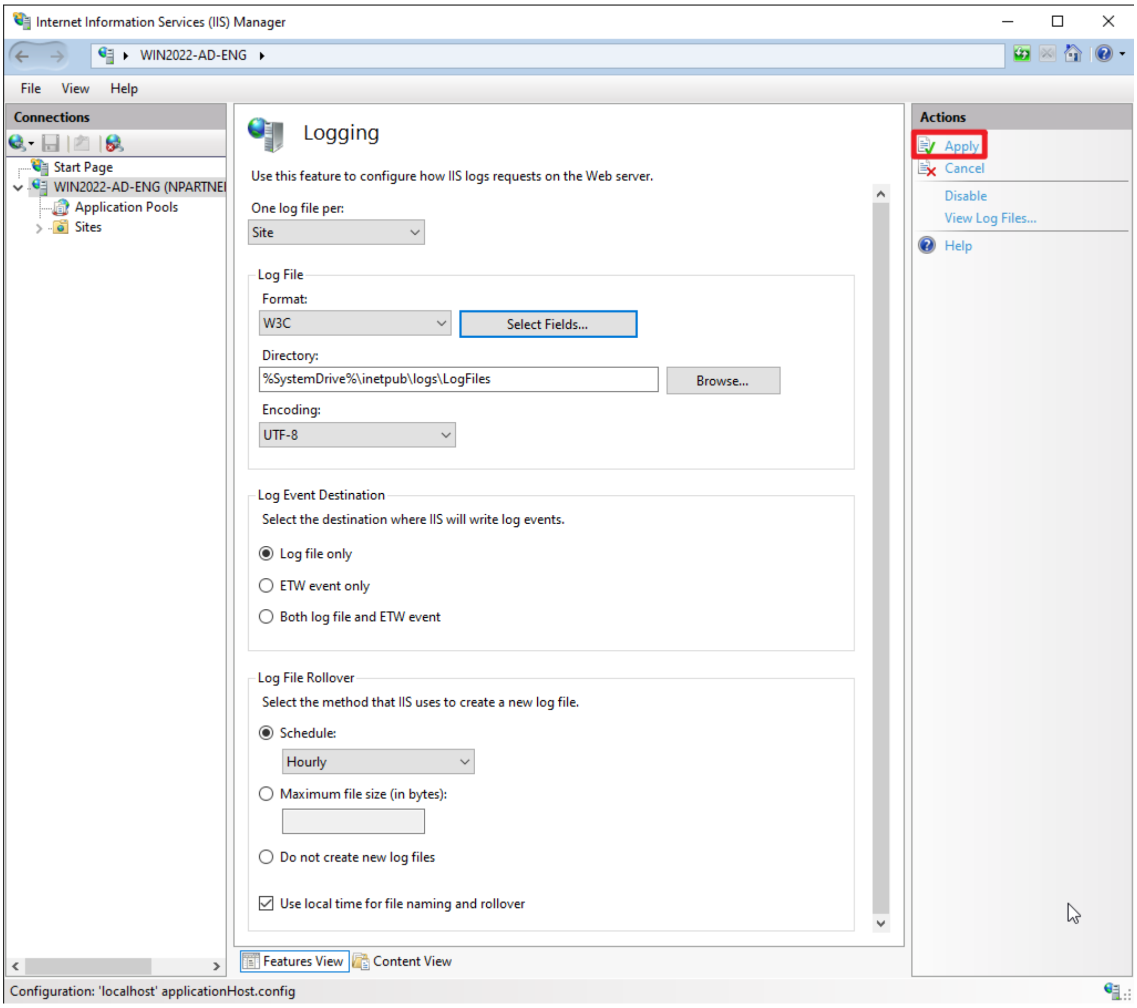
Standard Fields:

- ☑ Date (date)
- ☑ Time (time)
- ☑ Client IP Address (c-ip)
- ☑ User Name (cs-username)
- ☑ Service Name (s-sitename)
- ☑ Server Name (s-computername)
- ☑ Server IP Address (s-ip)
- ☑ Server Port (s-port)
- ☑ Method (cs-method)
- ☑ URI Stem (cs-uri-stem)
- ☑ URI Query (cs-uri-query)
- ☑ Protocol Status (sc-status)
- ☑ Protocol Substatus (sc-substatus)
- ☑ Win32 Status (sc-win32-status)
- ☑ Bytes Sent (sc-bytes)
- ☑ Bytes Received (cs-bytes)
- ☑ Time Taken (time-taken)
- ☑ Protocol Version (cs-version)
- ☑ Host (cs-host)
- ☑ User Agent (cs(User-Agent))
- ☑ Cookie (cs(Cookie))
- ☑ Referer (cs(Referer))

Custom Fields:

Log Field	Source Type	Source
X-Forwarded-For	Request Header	X-Forwarded-For

(7) Click “Apply.”



Logging

Use this feature to configure how IIS logs requests on the Web server.

One log file per: Site

Log File

Format: W3C

Directory: %SystemDrive%\inetpub\logs\LogFiles

Encoding: UTF-8

Log Event Destination

Select the destination where IIS will write log events.

● Log file only

○ ETW event only

○ Both log file and ETW event

Log File Rollover

Select the method that IIS uses to create a new log file.

● Schedule: Hourly

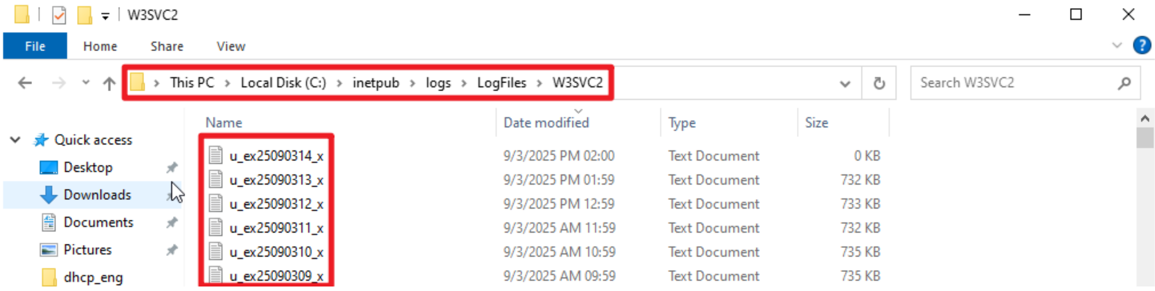
○ Maximum file size (in bytes):

○ Do not create new log files

☑ Use local time for file naming and rollover

Configuration: 'localhost' applicationHost.config

(8) Verify IIS log files are created in the folder: C:\inetpub\logs\LogFiles\W3SVC2



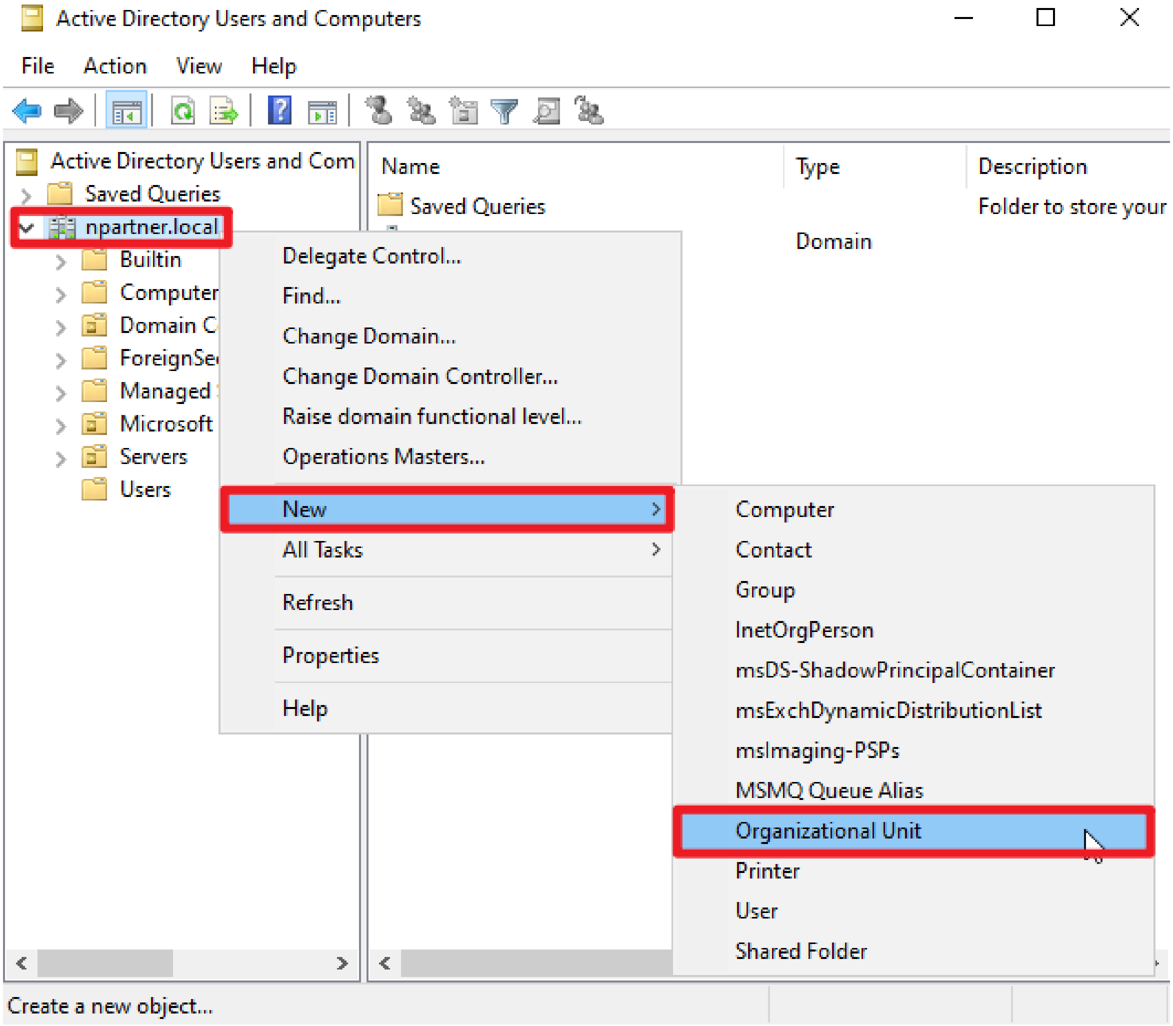
Name	Date modified	Type	Size
u_ex25090314_x	9/3/2025 PM 02:00	Text Document	0 KB
u_ex25090313_x	9/3/2025 PM 01:59	Text Document	732 KB
u_ex25090312_x	9/3/2025 PM 12:59	Text Document	733 KB
u_ex25090311_x	9/3/2025 AM 11:59	Text Document	732 KB
u_ex25090310_x	9/3/2025 AM 10:59	Text Document	735 KB
u_ex25090309_x	9/3/2025 AM 09:59	Text Document	735 KB

6.3.1 Organizational Unit (OU) Configuration

(1) Click “Active Directory Users and Computers.”

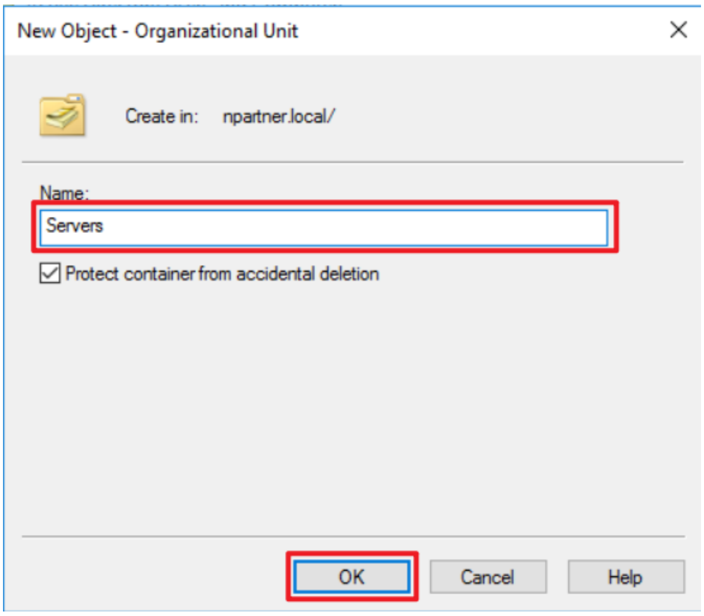
(2) Add an Organizational Unit

Right-click on “Domain Name,” (the example here is npartner.local) →select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit name according to the actual environment. → click “OK.”

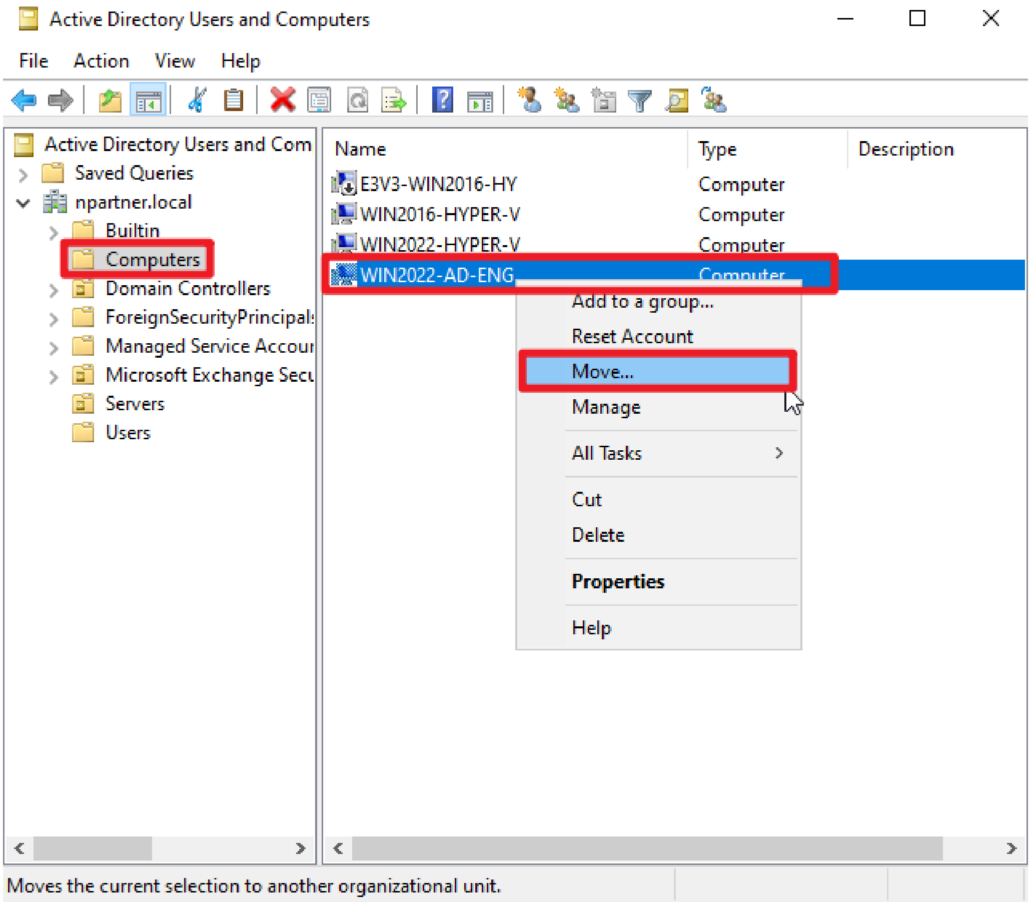


New Object - Organizational Unit
Create in: npartner.local/
Name:
Servers
☑ Protect container from accidental deletion
OK
Cancel
Help

(4) Move the Server to your New Organizational Unit:

Select your organizational unit in “Domain Controllers” → right-click on the “WIN2022-AD-ENG” server.

Note: Please select the Windows AD server according to the actual environment. → click “Move.”

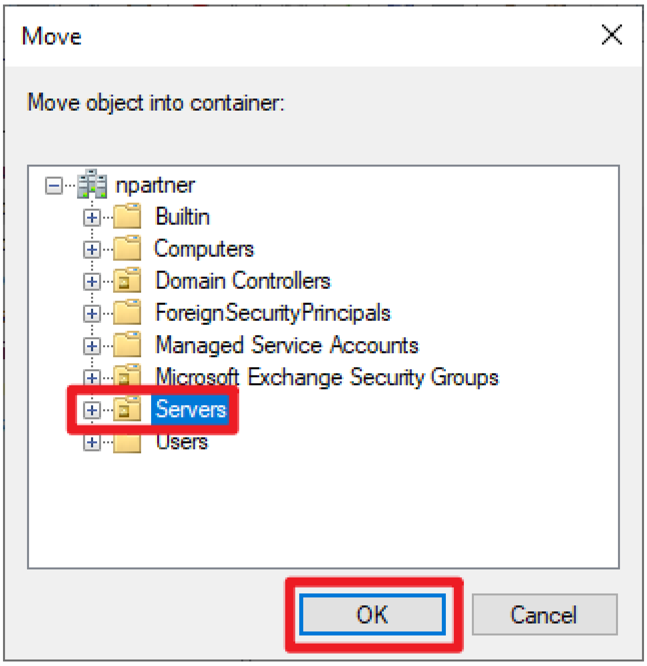


Name	Type	Description
E3V3-WIN2016-HY	Computer	
WIN2016-HYPER-V	Computer	
WIN2022-HYPER-V	Computer	
WIN2022-AD-ENG	Computer	

Moves the current selection to another organizational unit.

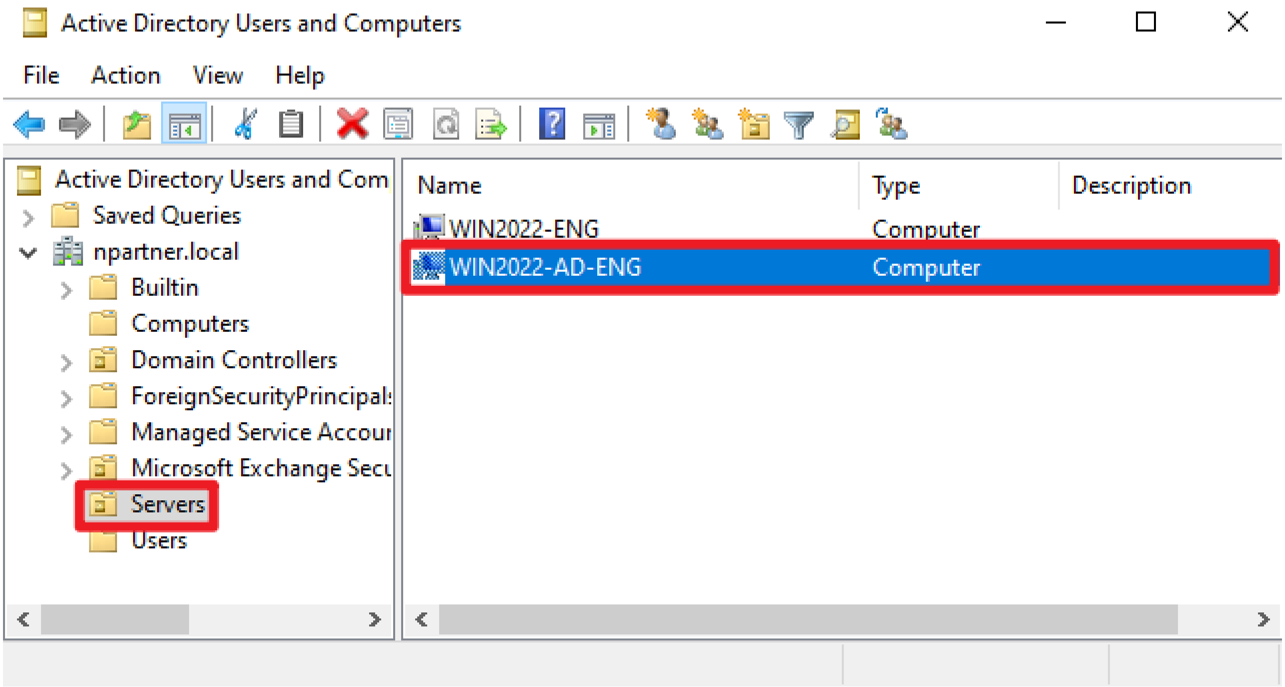
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2022-AD-ENG” server has been moved.



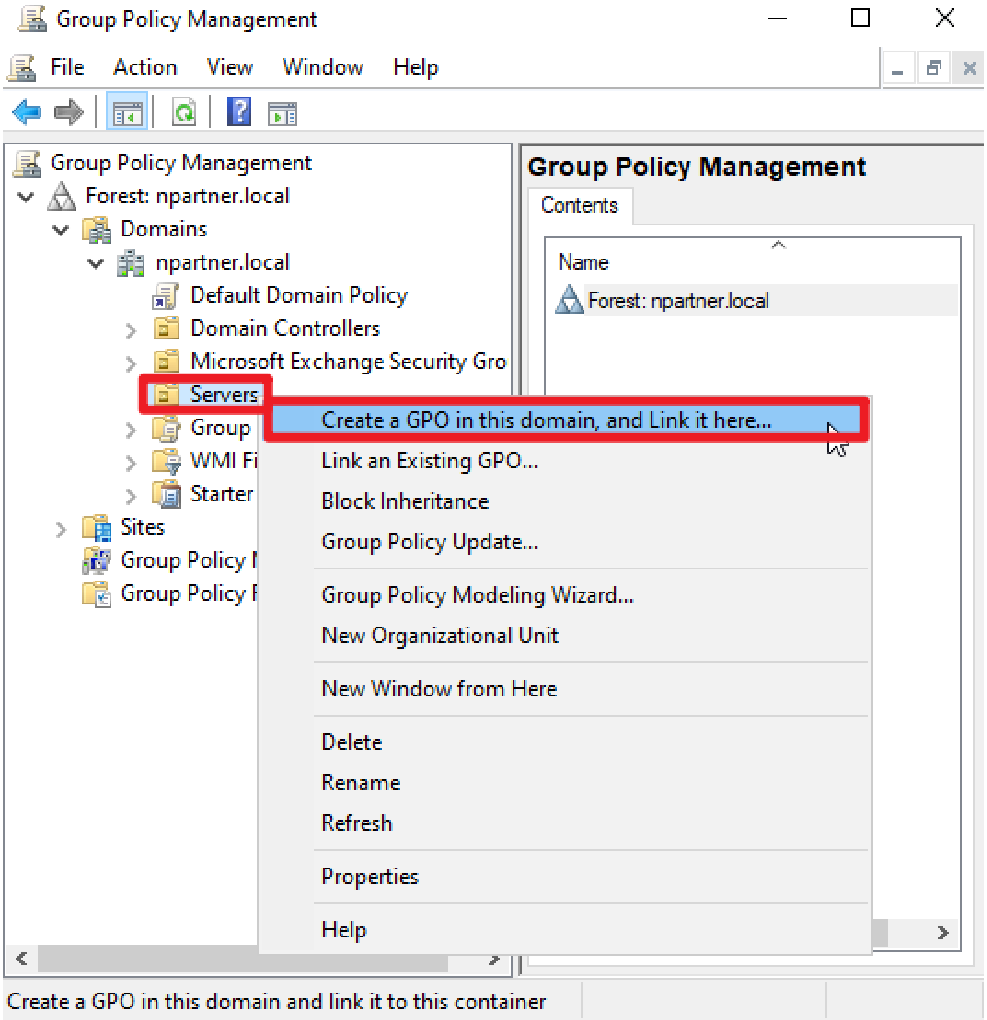
Name	Type	Description
WIN2022-ENG	Computer	
WIN2022-AD-ENG	Computer	

6.3.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

Right-click the “Servers” organizational unit → select “Create a GPO in this domain, and Link it here...”

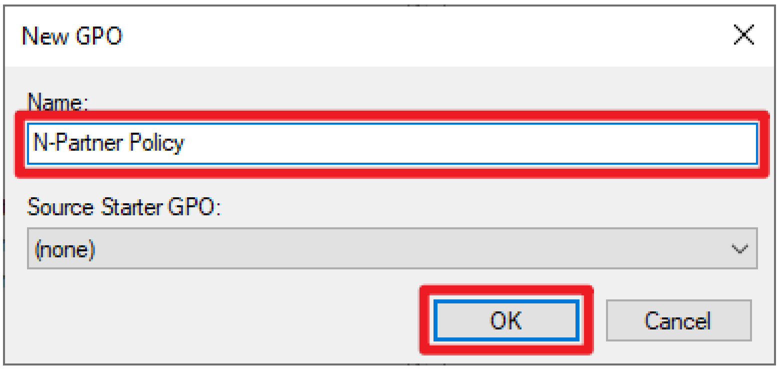


Create a GPO in this domain and link it to this container

(3) Edit your Group Policy Object

Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. Then click “Edit.”



New GPO

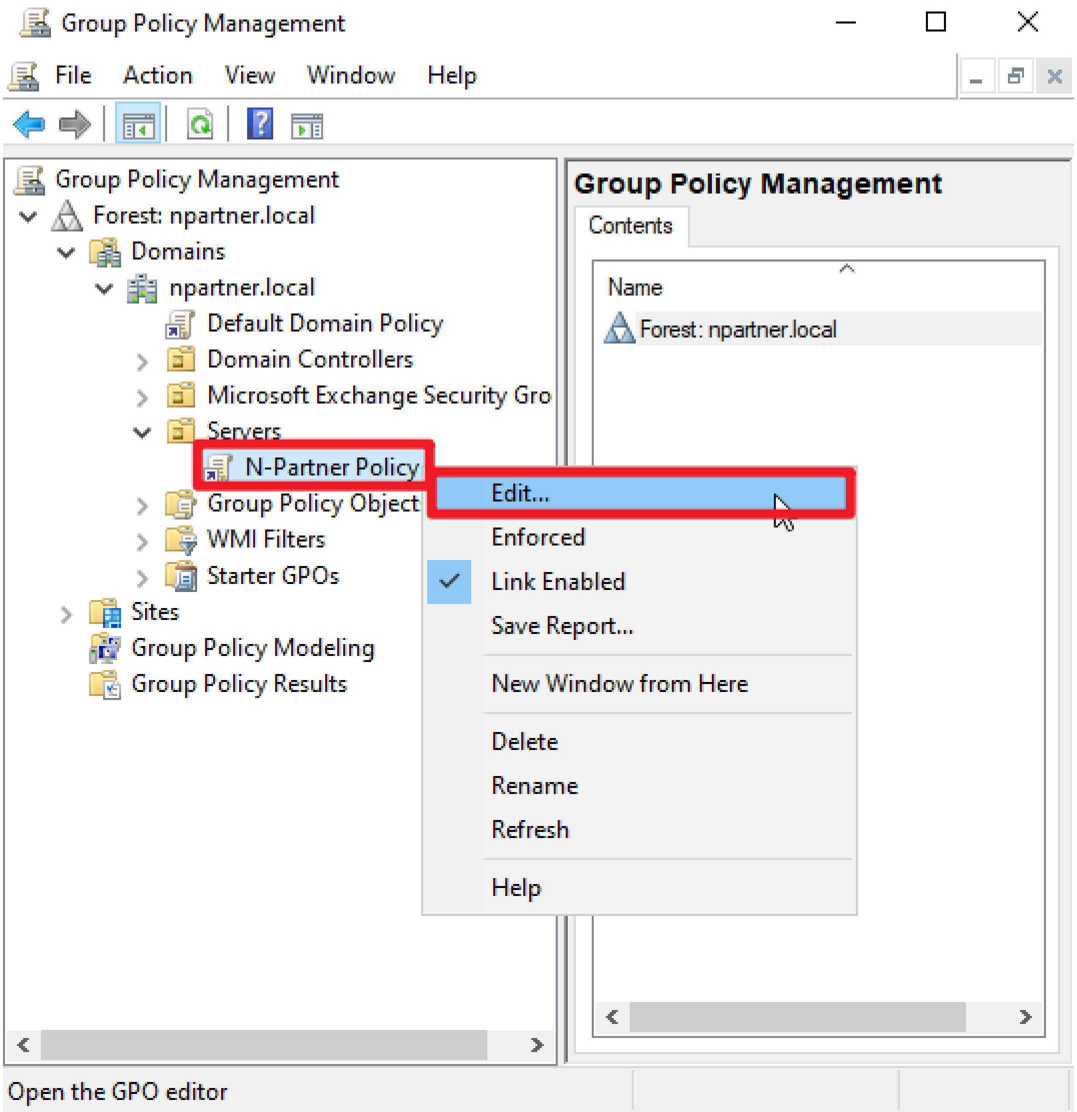
Name: N-Partner Policy

Source Starter GPO: (none)

(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”)

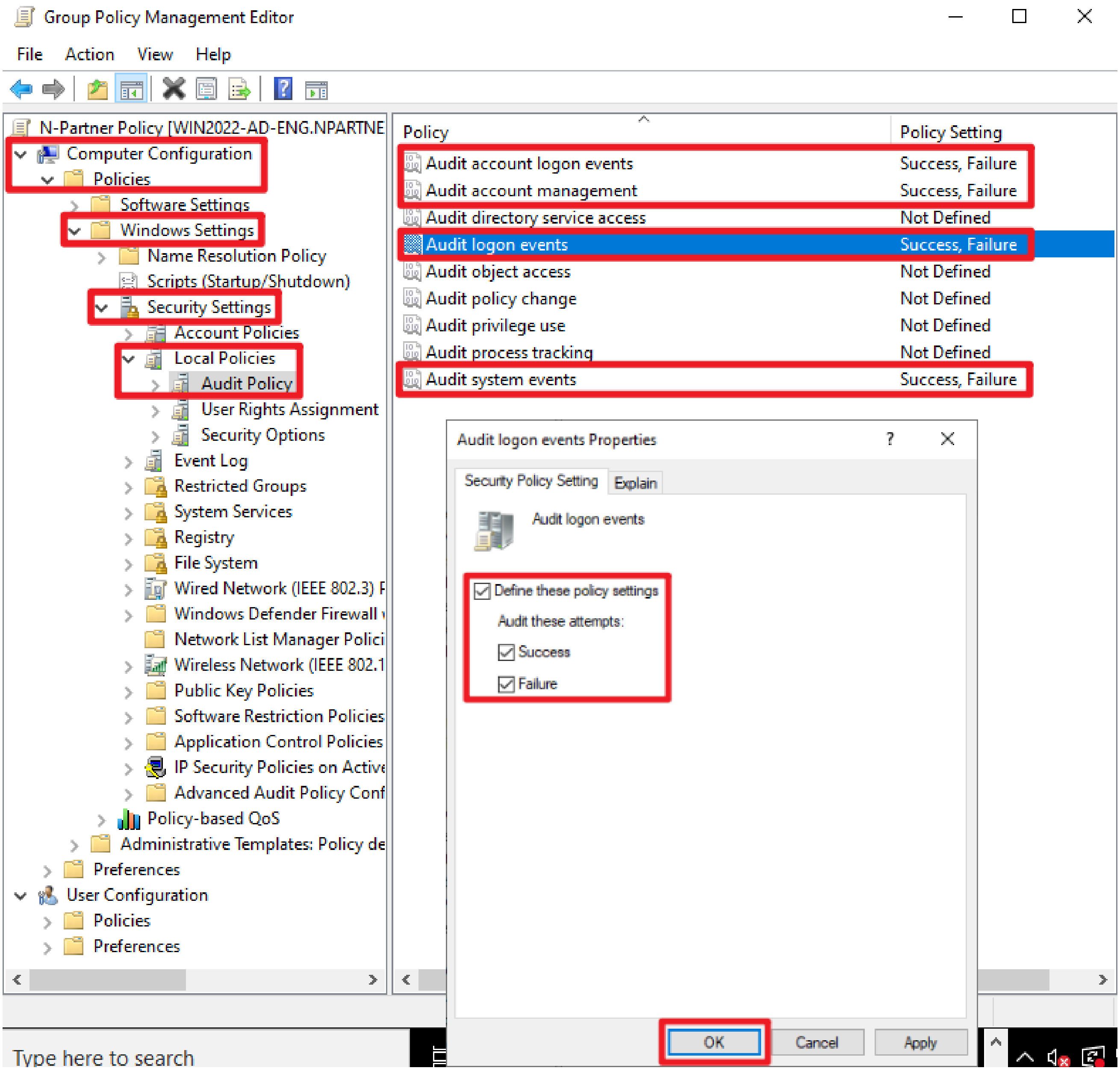
right-click and select “Edit.”



Open the GPO editor

(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events” → check “Define these policy settings”: Success, Failure. → click “OK.”



Policy	Policy Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Not Defined
Audit logon events	Success, Failure
Audit object access	Not Defined
Audit policy change	Not Defined
Audit privilege use	Not Defined
Audit process tracking	Not Defined
Audit system events	Success, Failure

Audit logon events Properties

Security Policy Setting | Explain

Audit logon events

☑ Define these policy settings

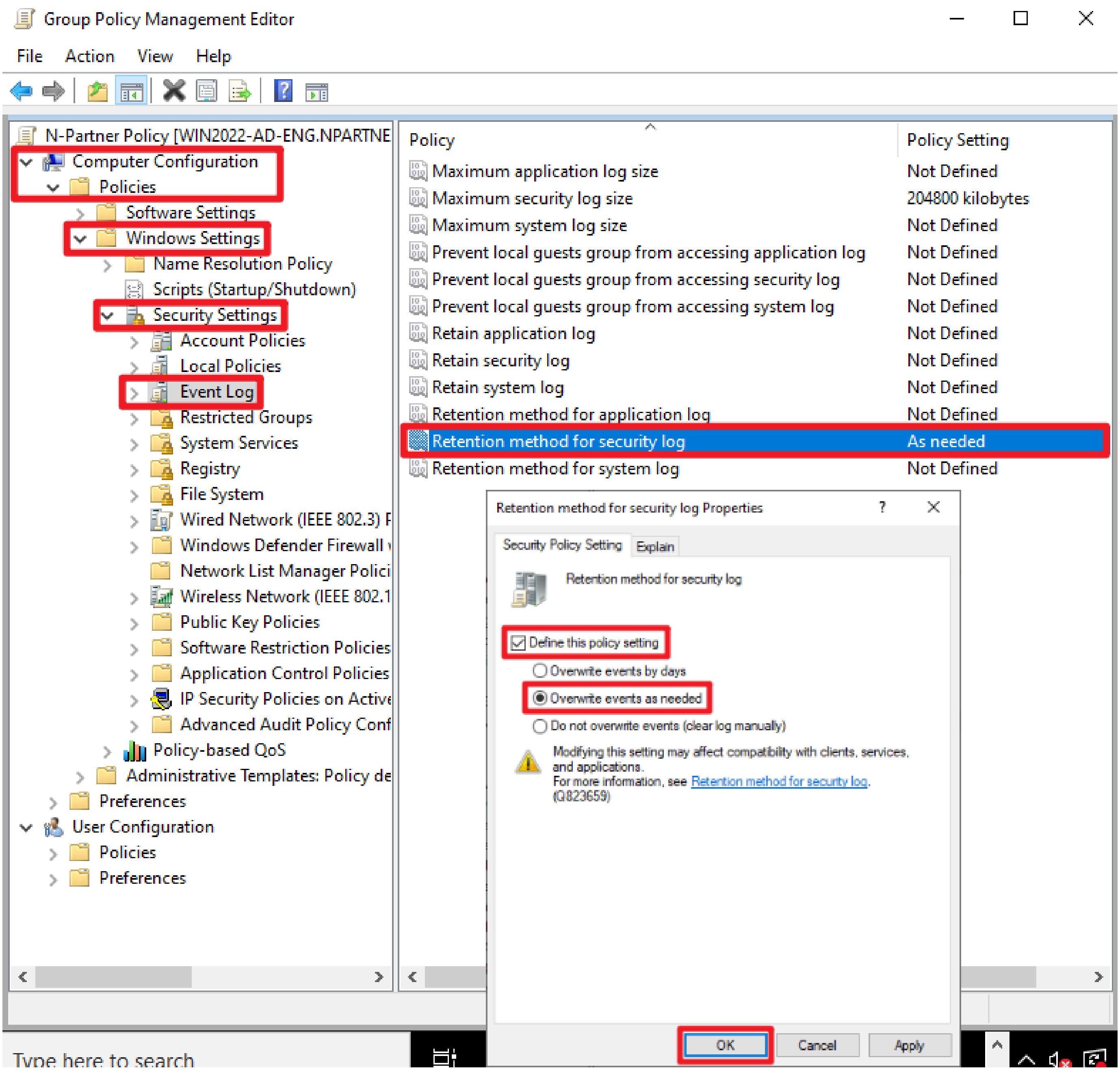
Audit these attempts:

☑ Success

☑ Failure

(6) Event Log: Security Log Retention Method

Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



Group Policy Management Editor

N-Partner Policy [WIN2022-AD-ENG.NPARTNE
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) F
        - Windows Defender Firewall v
        - Network List Manager Polici
        - Wireless Network (IEEE 802.1
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Active
        - Advanced Audit Policy Conf
      - Policy-based QoS
    - Administrative Templates: Policy de
  - Preferences
- User Configuration
  - Policies
  - Preferences

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Retention method for security log Properties

Retention method for security log

☑ Define this policy setting

○ Overwrite events by days

● Overwrite events as needed

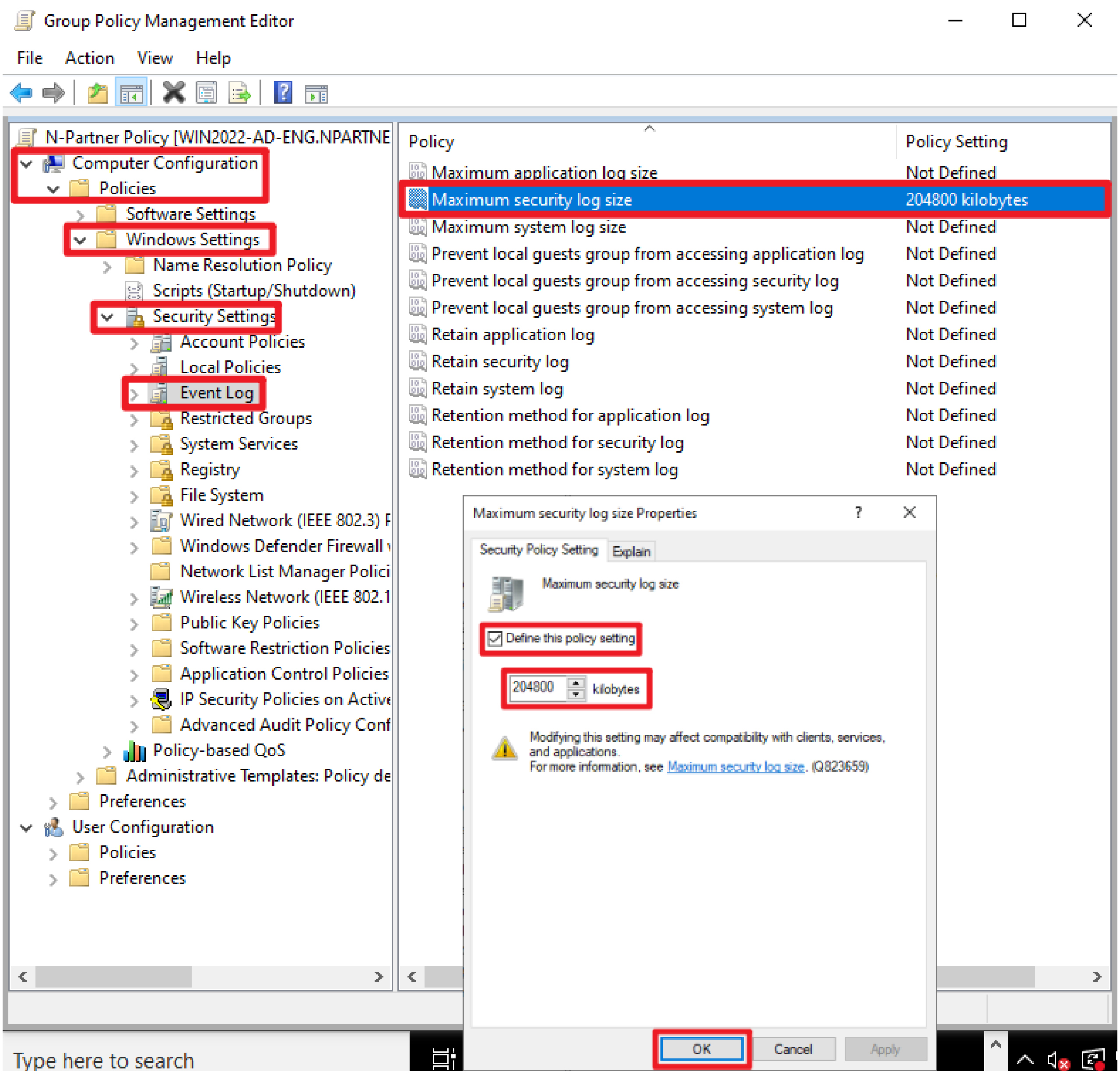
○ Do not overwrite events (clear log manually)

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Retention method for security log. (Q823659)

(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” →And click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB

Note: Please adjust the number based on the actual environment. → click “OK.”


Group Policy Management Editor
File
Action
View
Help
N-Partner Policy [WIN2022-AD-ENG.NPARTNE
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) F
Windows Defender Firewall v
Network List Manager Polici
Wireless Network (IEEE 802.1
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active
Advanced Audit Policy Conf
Policy-based QoS
Administrative Templates: Policy de
Preferences
User Configuration
Policies
Preferences
Type here to search

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

Maximum security log size Properties

Security Policy Setting | Explain

Maximum security log size

☑ Define this policy setting

204800 kilobytes

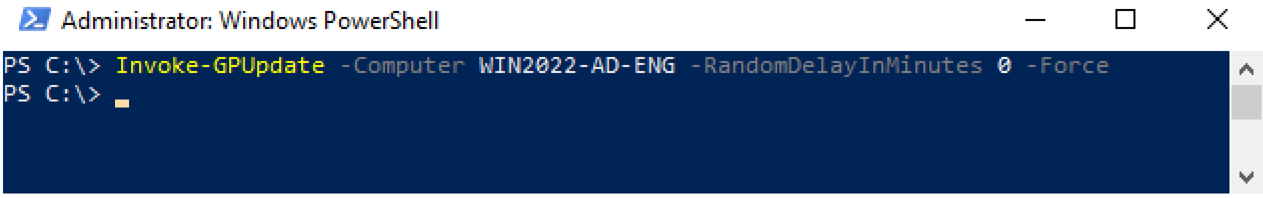
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Maximum security log size. (Q823659)

OK | Cancel | Apply

(8) Open “Windows PowerShell.”

(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer Win2022-AD-ENG -RandomDelayInMinutes 0 -Force
```

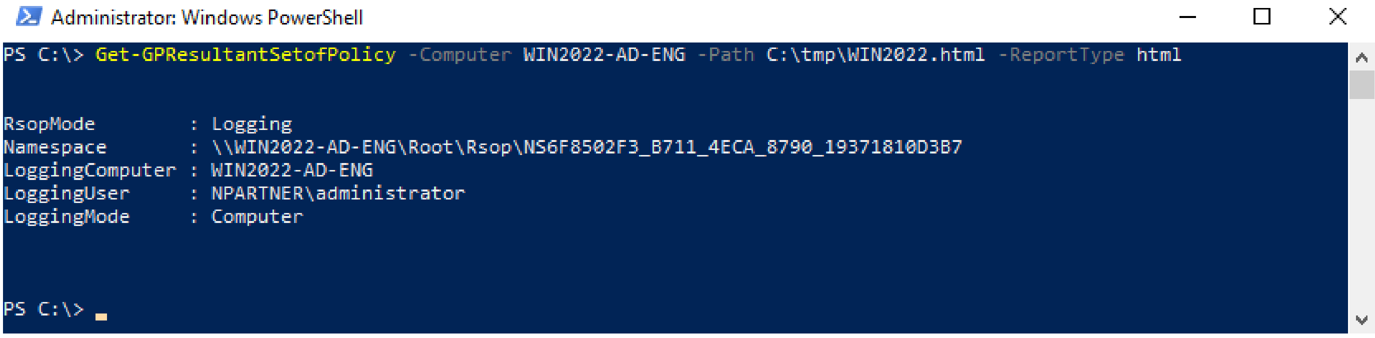


```
PS C:\> Invoke-GPUpdate -Computer WIN2022-AD-ENG -RandomDelayInMinutes 0 -Force
PS C:\> _
```

Enter the Exchange server name in the red text section.

(10) Enter the command below to generate server group policy report.

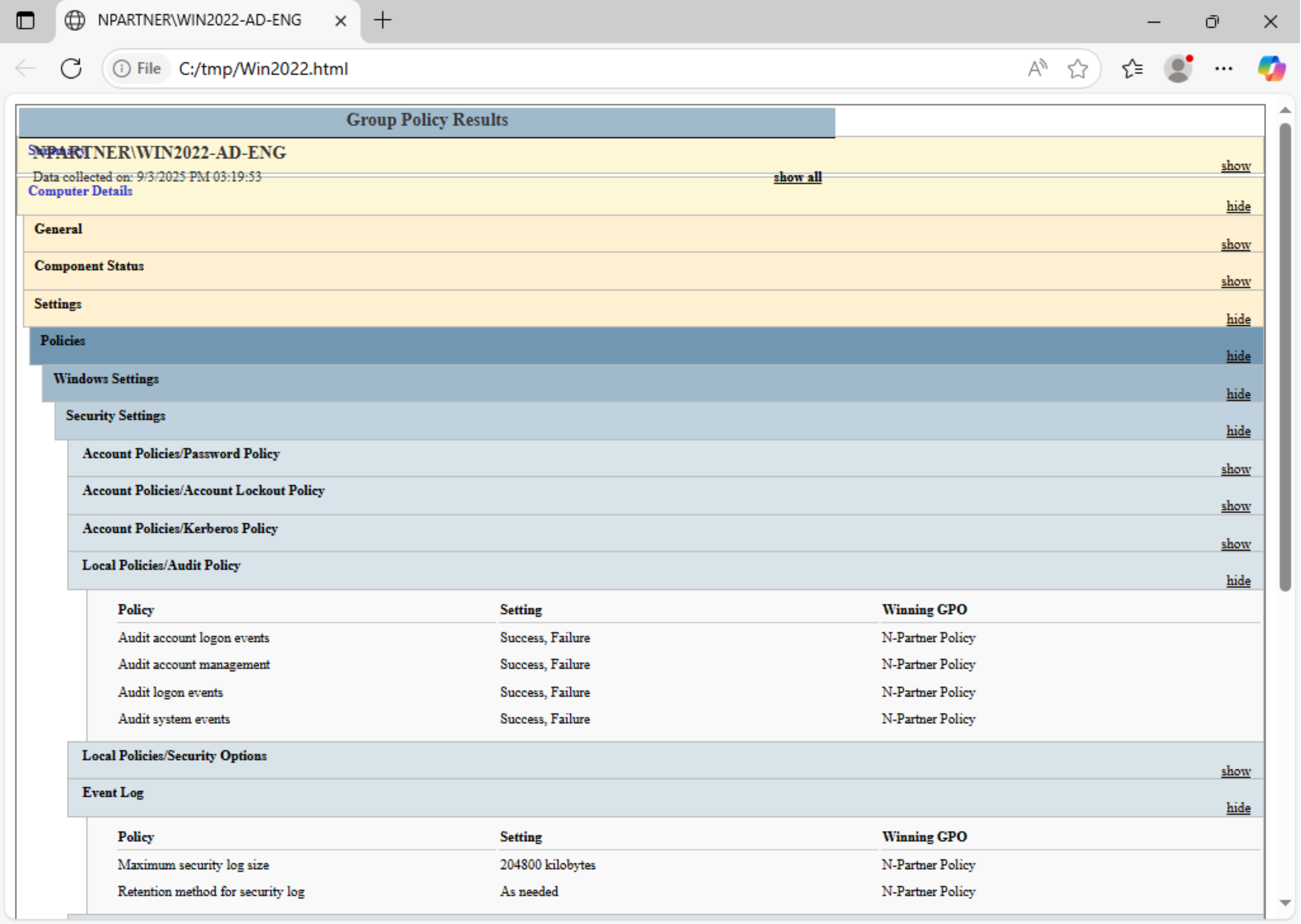
```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2022-AD-ENG -Path C:\tmp\Win2022.html -
ReportType html
```



```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2022-AD-ENG -Path C:\tmp\WIN2022.html -ReportType html


RsopMode        : Logging
Namespace       : \\WIN2022-AD-ENG\Root\Rsop\NS6F8502F3_B711_4ECA_8790_19371810D3B7
LoggingComputer : WIN2022-AD-ENG
LoggingUser     : NPARTNER\administrator
LoggingMode     : Computer



PS C:\> _
```

For the red text , please enter the Windows AD server name and the folder path/file name.

(11) Open the report and verify that your Windows AD server is applying the N-Partner Policy Group Policy.



Group Policy Results

Summary

NPARTNER\WIN2022-AD-ENG

Data collected on: 9/3/2025 PM 03:19:53

show all

show

Computer Details

hide

General

show

Component Status

show

Settings

hide

Policies

hide

Windows Settings

hide

Security Settings

hide

Account Policies/Password Policy

show

Account Policies/Account Lockout Policy

show

Account Policies/Kerberos Policy

show

Local Policies/Audit Policy

hide

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy

Local Policies/Security Options

show

Event Log

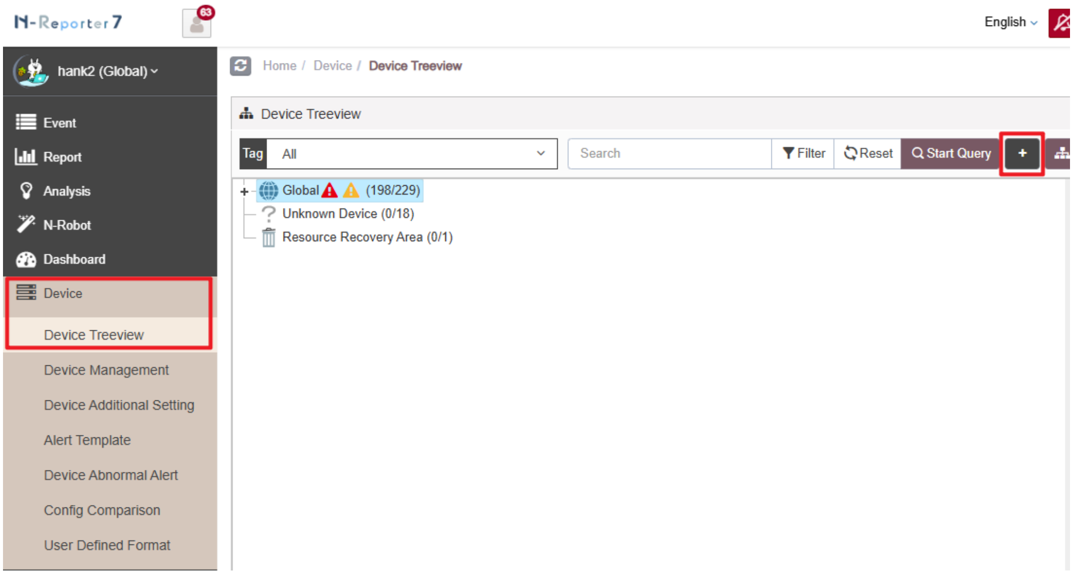
hide

Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

7. N-Reporter

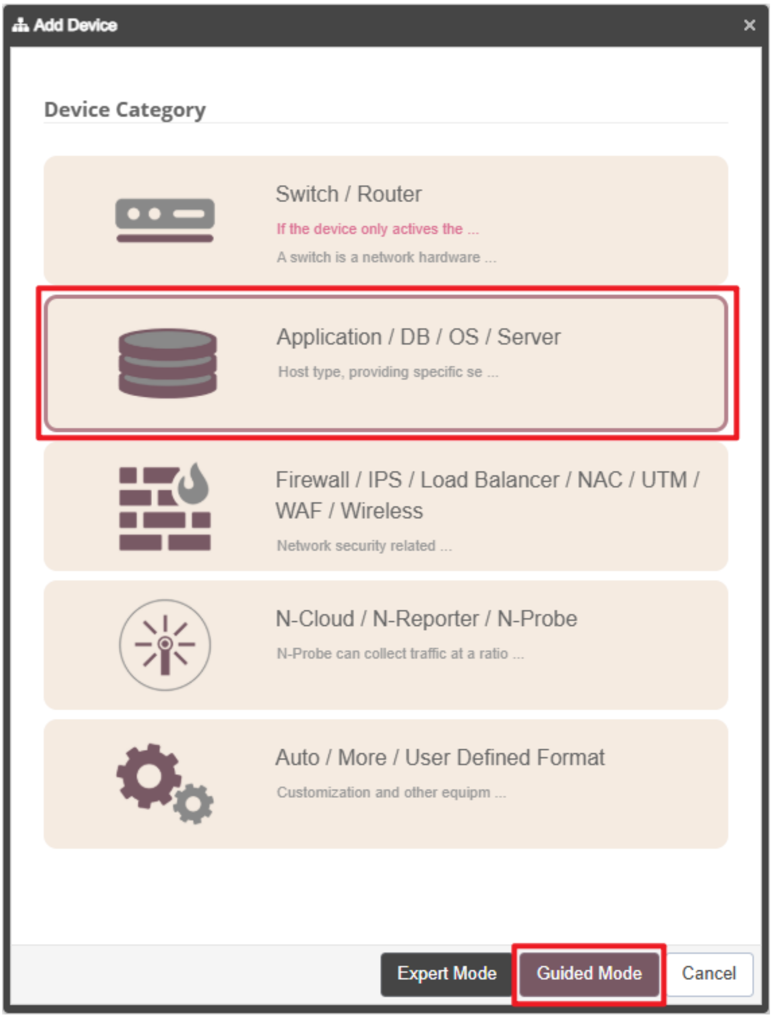
(1) Add an MS Exchange device:

Go to “Device Management” → “Device Treeview” → click “Add.”



(2) Select the device type:

Choose “Application/DB/OS/Server” → click “Guided Mode.”

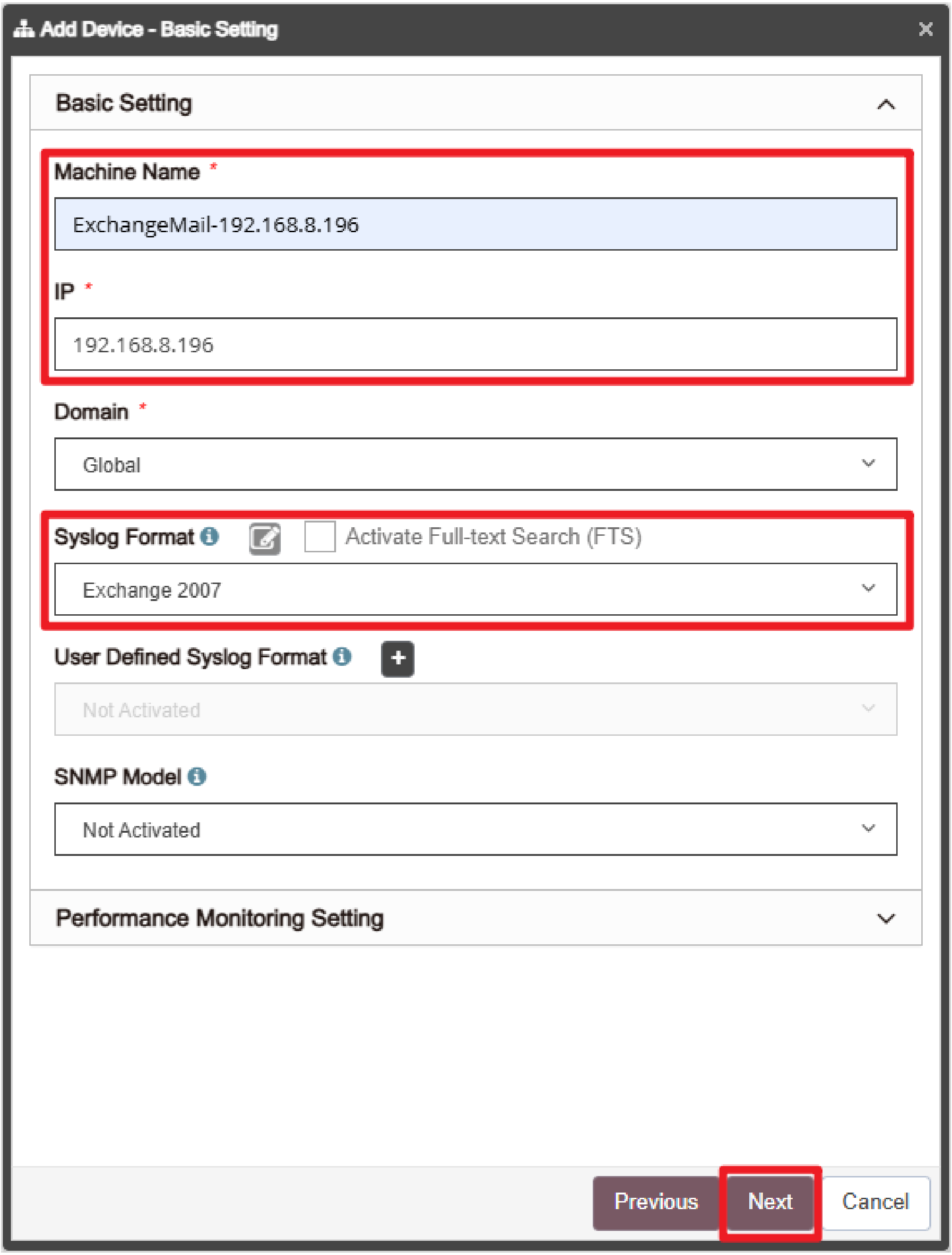

Add Device
Device Category
Switch / Router
If the device only actives the ...
A switch is a network hardware ...
Application / DB / OS / Server
Host type, providing specific se ...
Firewall / IPS / Load Balancer / NAC / UTM / WAF / Wireless
Network security related ...
N-Cloud / N-Reporter / N-Probe
N-Probe can collect traffic at a ratio ...
Auto / More / User Defined Format
Customization and other equipm ...
Expert Mode
Guided Mode
Cancel

7.1 Exchange Message Tracking Log

7.1.1 Exchange 2007

(1) Basic Device Settings:

Enter the device name and IP address → For Syslog Data Format, select “Exchange 2007” → click “Next.”



Machine Name *

ExchangeMail-192.168.8.196

IP *

192.168.8.196

Domain *

Global

Syslog Format □ Activate Full-text Search (FTS)

Exchange 2007

User Defined Syslog Format

Not Activated

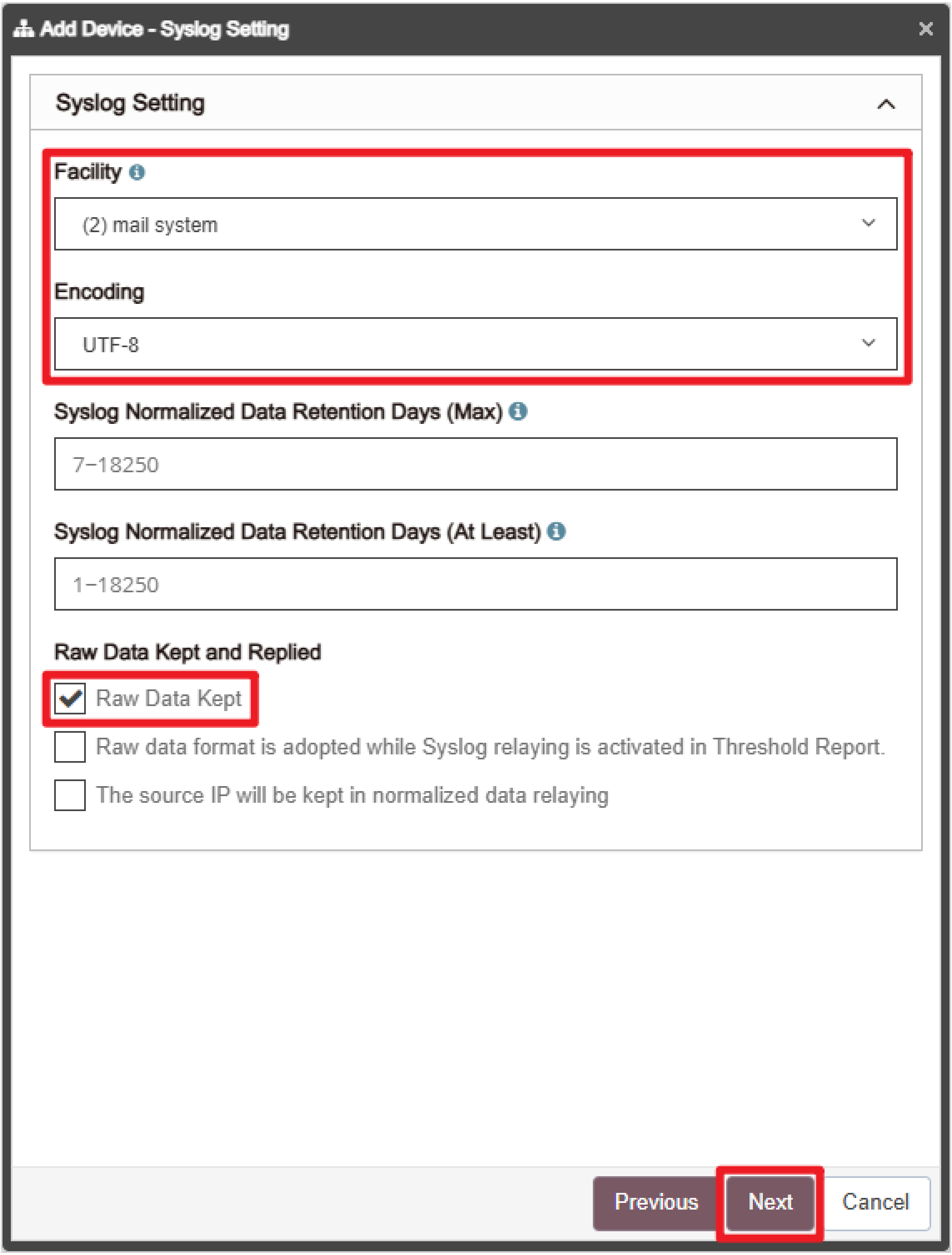
SNMP Model

Not Activated

(2) Syslog Settings

Set "Facility" to "(2) mail system" and "Encoding" to "UTF-8" → click "Next."

If "Raw Data Kept" function is enabled, the "Event Query" page will display raw data information.



Add Device - Syslog Setting

Syslog Setting

Facility

(2) mail system

Encoding

UTF-8

Syslog Normalized Data Retention Days (Max)

7~18250

Syslog Normalized Data Retention Days (At Least)

1~18250

Raw Data Kept and Replied

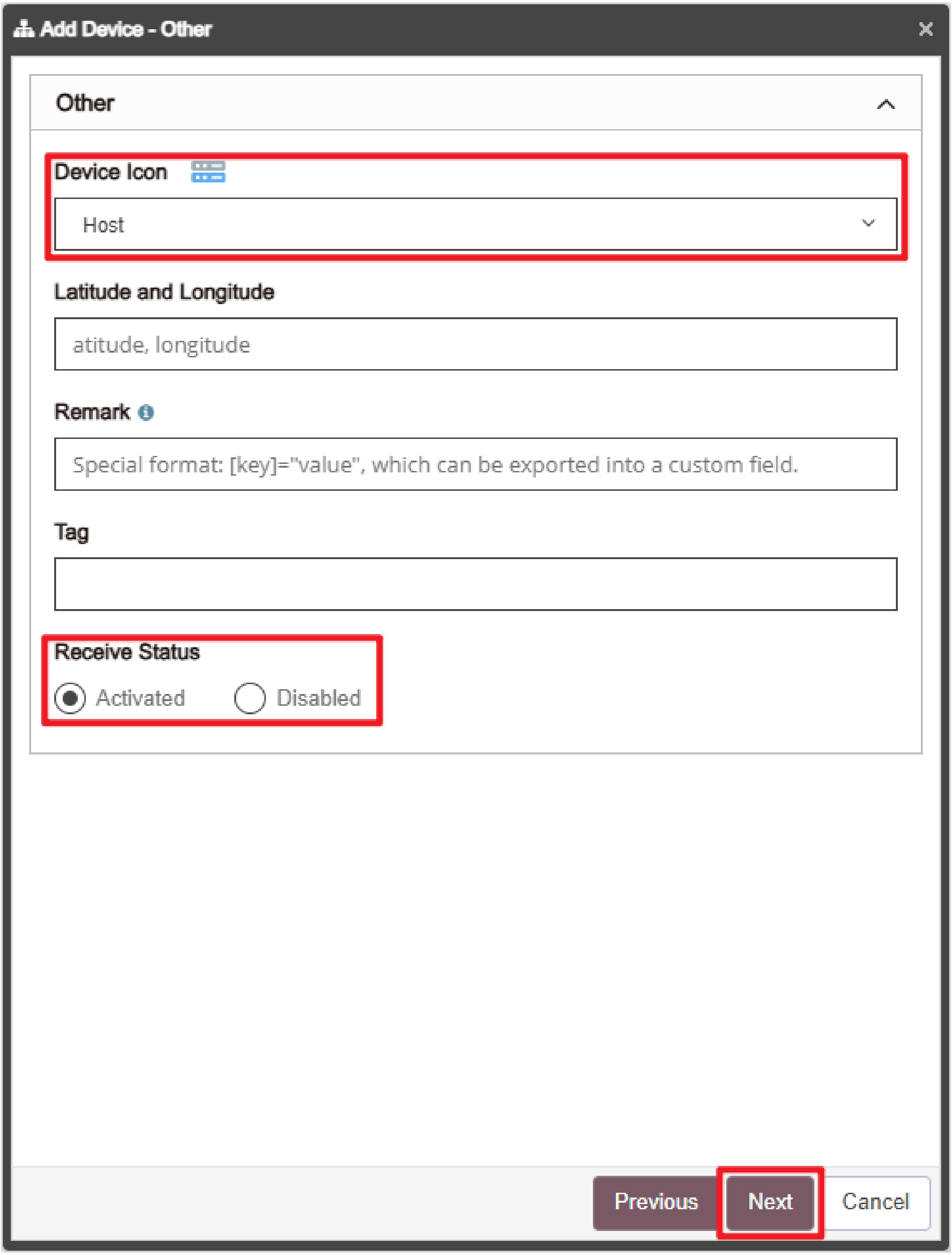
☑ Raw Data Kept

□ Raw data format is adopted while Syslog relaying is activated in Threshold Report.

□ The source IP will be kept in normalized data relaying

(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next” → Confirm.



Add Device - Other

Other

Device Icon: Host

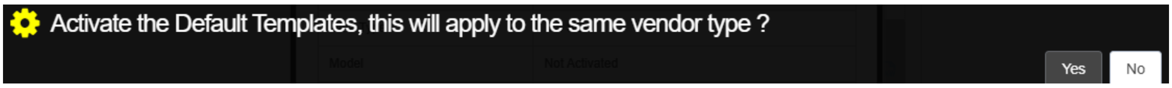
Latitude and Longitude: atitude, longitude

Remark: Special format: [key]="value", which can be exported into a custom field.

Tag:

Receive Status: ● Activated ○ Disabled

Enable default reports to be applied to devices of the same make and model → click “No.”

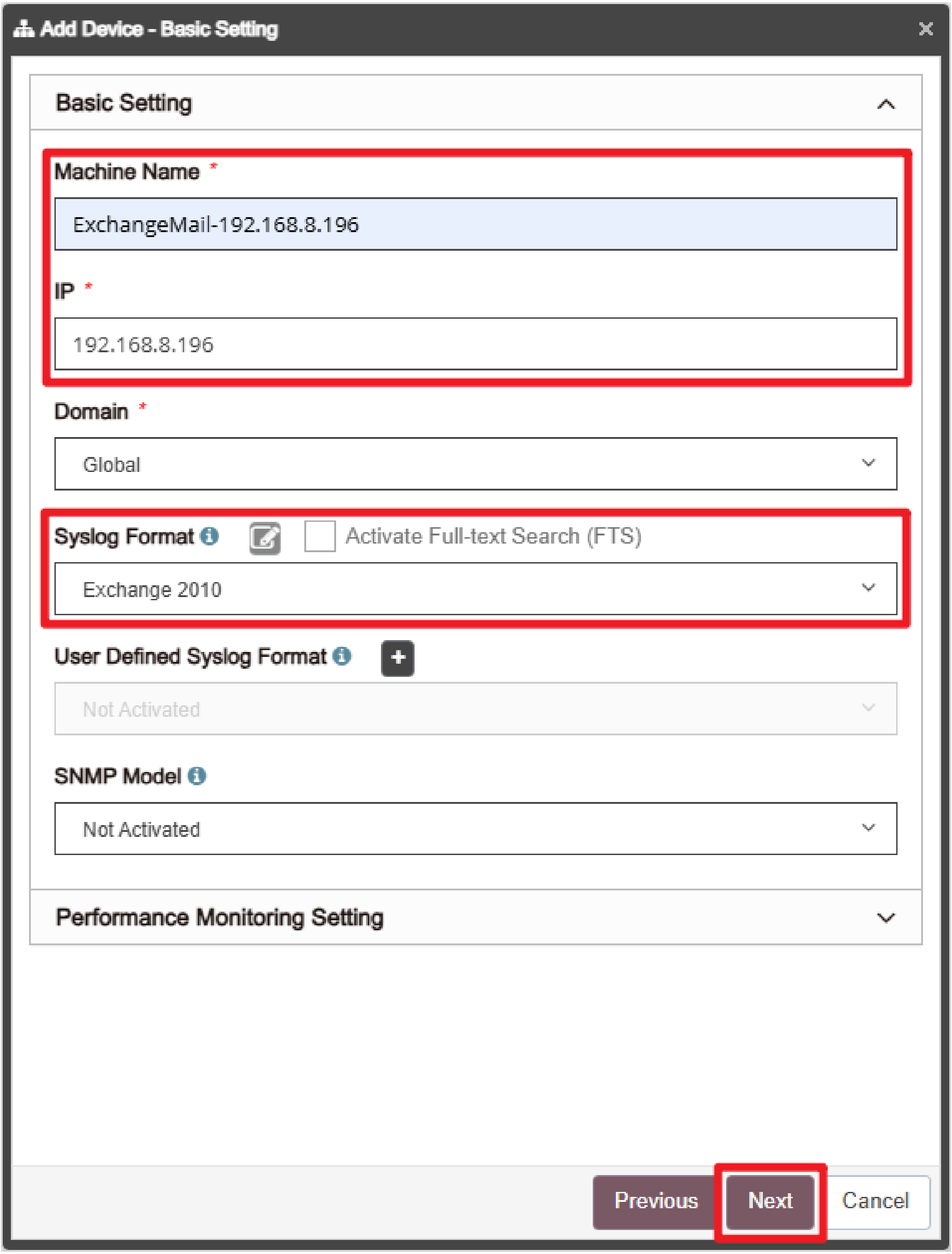


Activate the Default Templates, this will apply to the same vendor type ?

7.1.2 Exchange 2010

(1) Device Basic Settings

Enter the device name and IP → Select “Exchange 2010” for the Syslog data format → click “Next.”



Add Device - Basic Setting

Basic Setting

Machine Name *

ExchangeMail-192.168.8.196

IP *

192.168.8.196

Domain *

Global

Syslog Format □ Activate Full-text Search (FTS)

Exchange 2010

User Defined Syslog Format

Not Activated

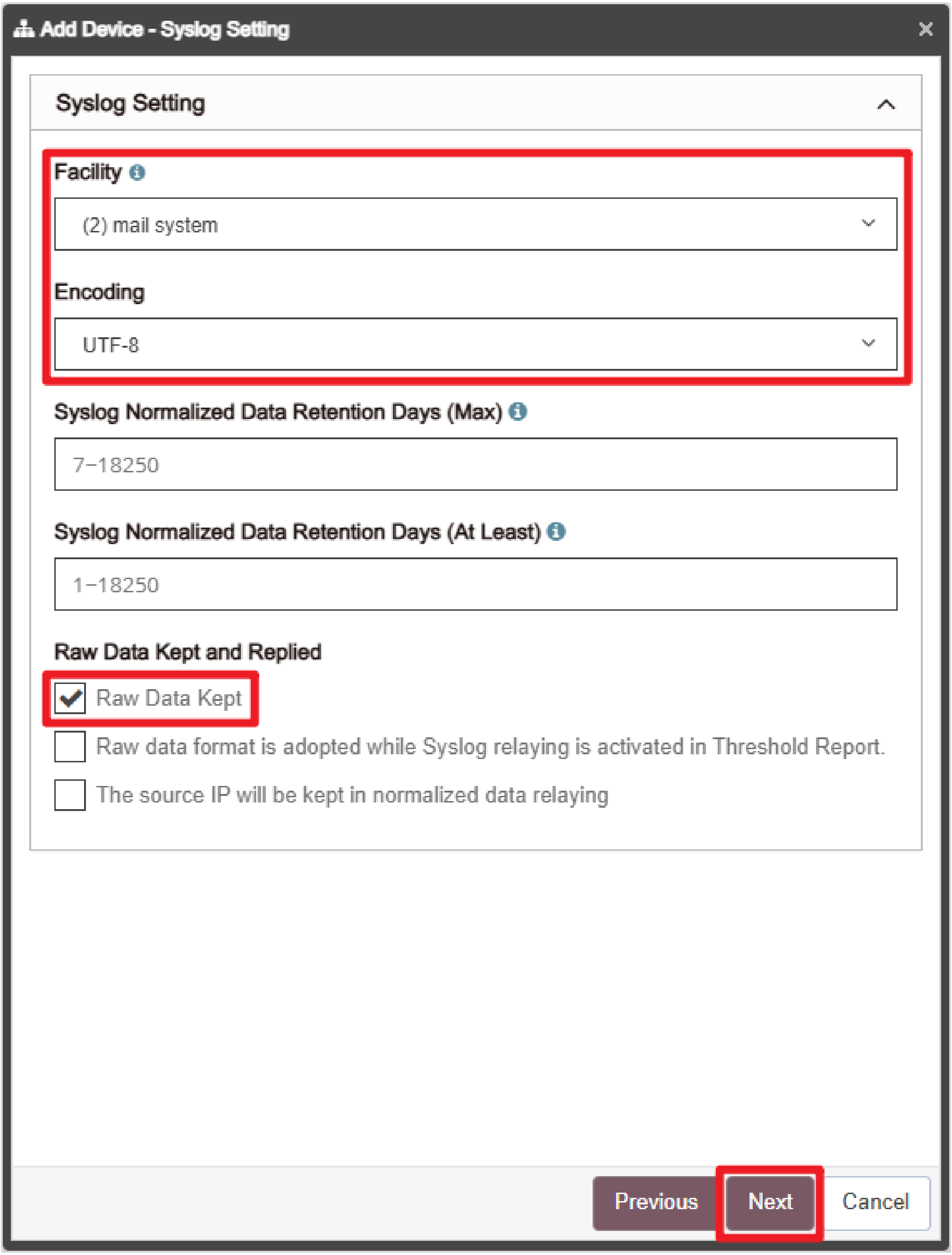
SNMP Model

Not Activated

(2) Syslog Settings

Set “Facility” to “(2) mail system” and “Encoding” to “UTF-8” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.



Add Device - Syslog Setting

Syslog Setting

Facility: (2) mail system

Encoding: UTF-8

Syslog Normalized Data Retention Days (Max): 7~18250

Syslog Normalized Data Retention Days (At Least): 1~18250

Raw Data Kept and Replied

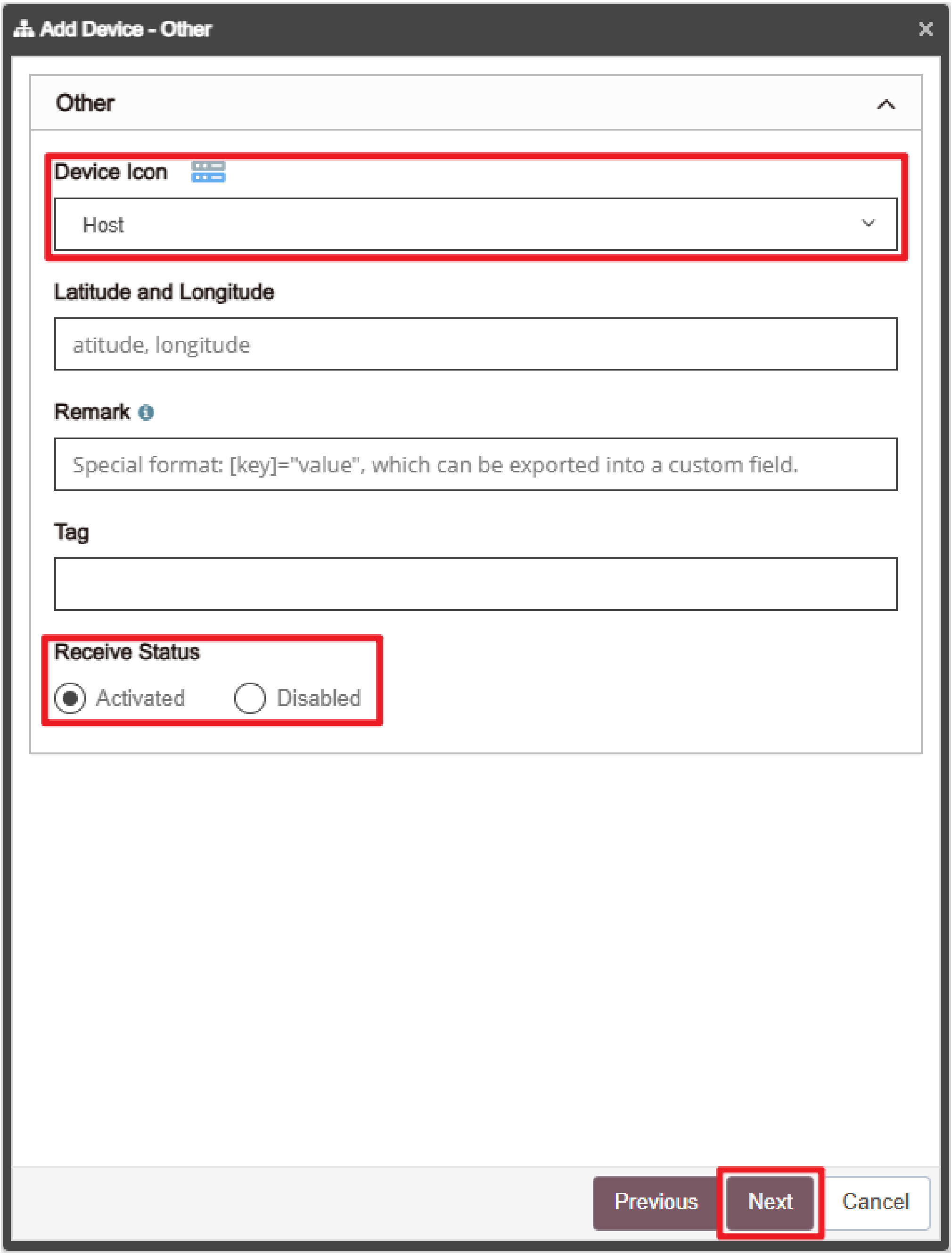
☑ Raw Data Kept

□ Raw data format is adopted while Syslog relaying is activated in Threshold Report.

□ The source IP will be kept in normalized data relaying

(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next” → Confirm.



Add Device - Other

Other

Device Icon

Host

Latitude and Longitude

atitude, longitude

Remark

Special format: [key]="value", which can be exported into a custom field.

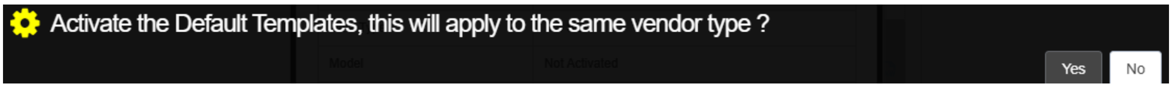
Tag

Receive Status

● Activated ○ Disabled

Previous | Next | Cancel

Enable default reports to be applied to devices of the same make and model → click “No.”



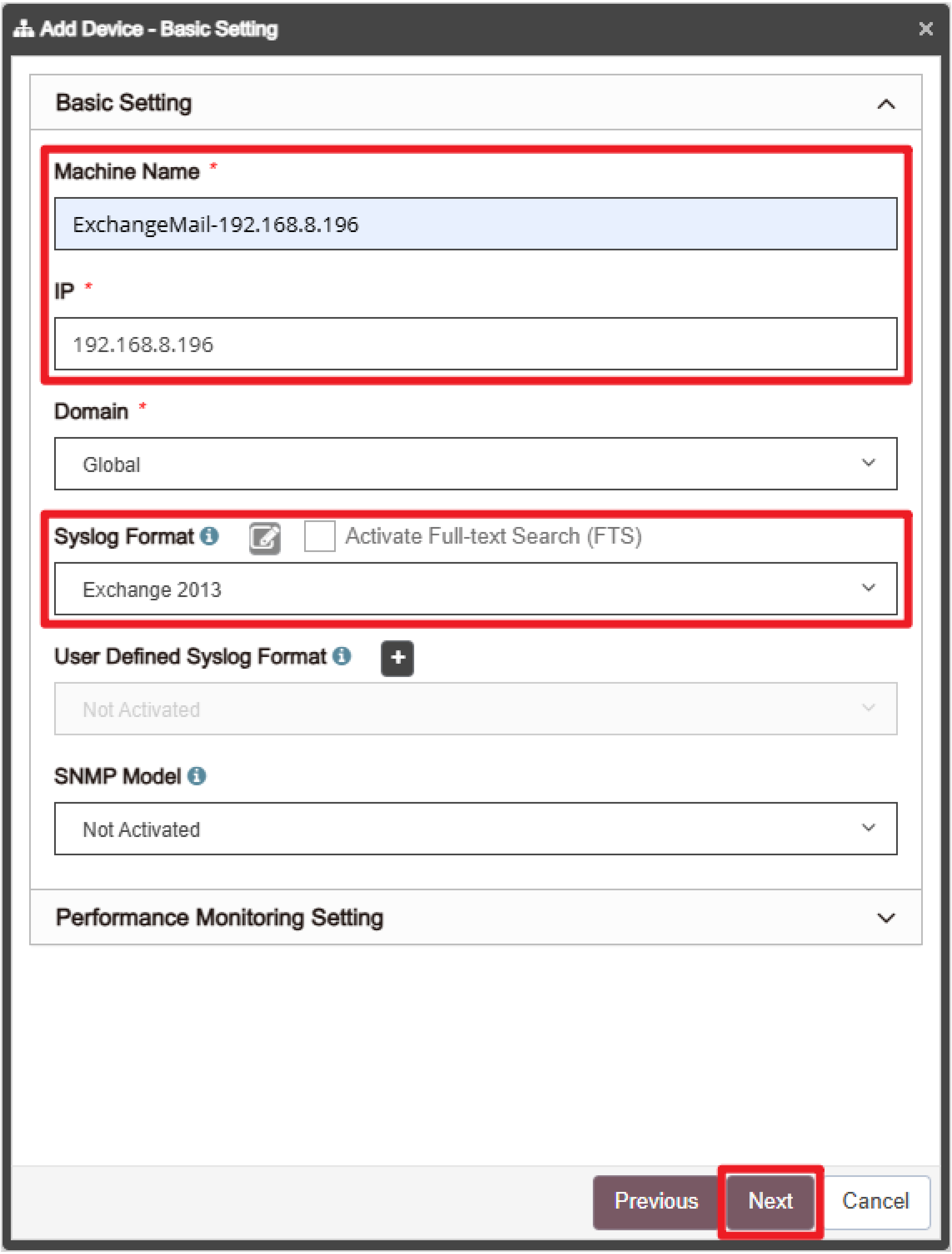
Activate the Default Templates, this will apply to the same vendor type ?

Yes | No

7.1.3 For Exchange 2013 or Later

(1) Device Basic Settings

Enter the device name and IP → Select “Exchange 2013” for the Syslog data format → click “Next.”



Machine Name *
ExchangeMail-192.168.8.196

IP *
192.168.8.196

Domain *
Global

Syslog Format □ Activate Full-text Search (FTS)
Exchange 2013

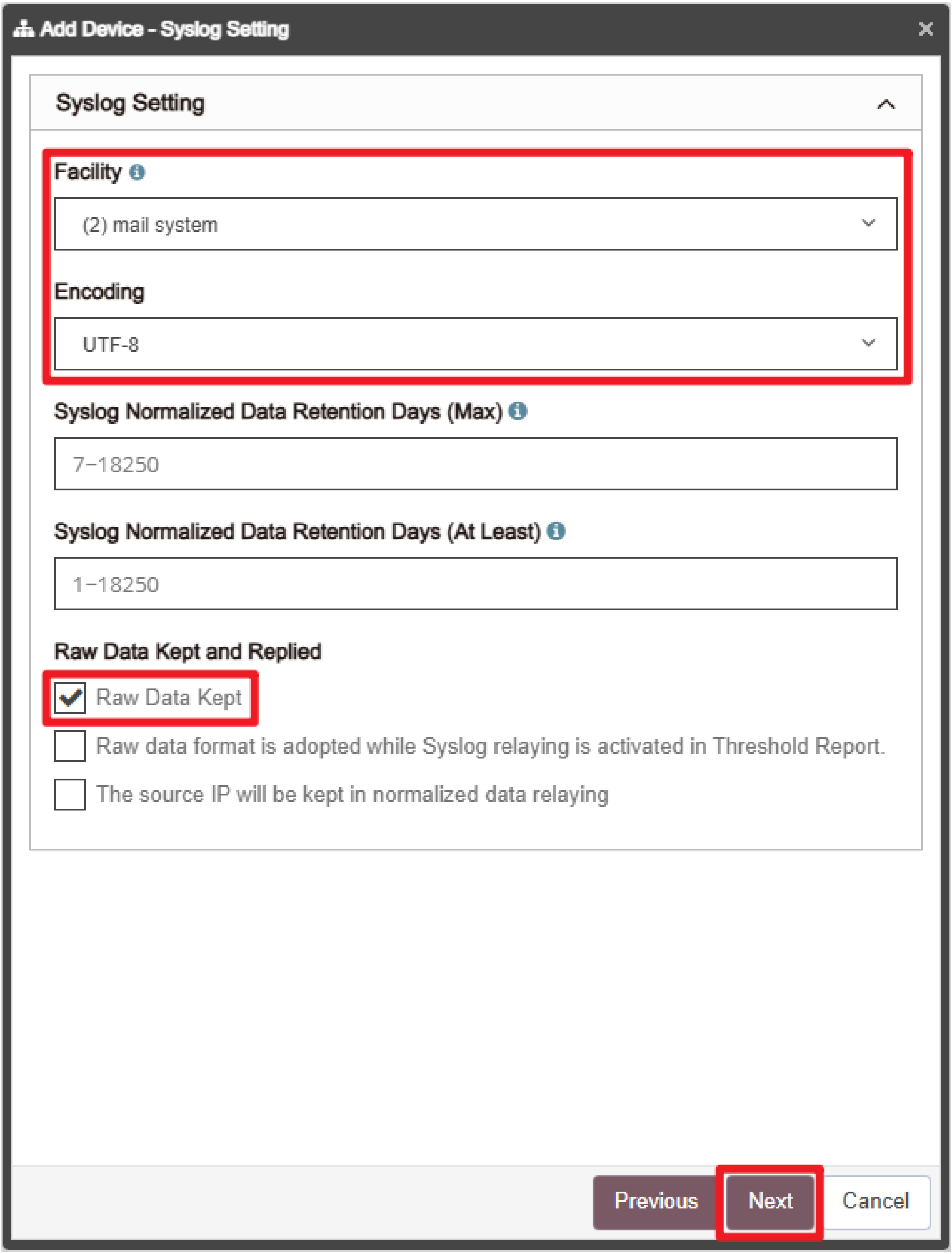
User Defined Syslog Format
Not Activated

SNMP Model
Not Activated

(2) Syslog Settings

Set “Facility” to “(2) mail system” and “Encoding” to “UTF-8” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.



Add Device - Syslog Setting

Syslog Setting

Facility: (2) mail system

Encoding: UTF-8

Syslog Normalized Data Retention Days (Max): 7~18250

Syslog Normalized Data Retention Days (At Least): 1~18250

Raw Data Kept and Replied

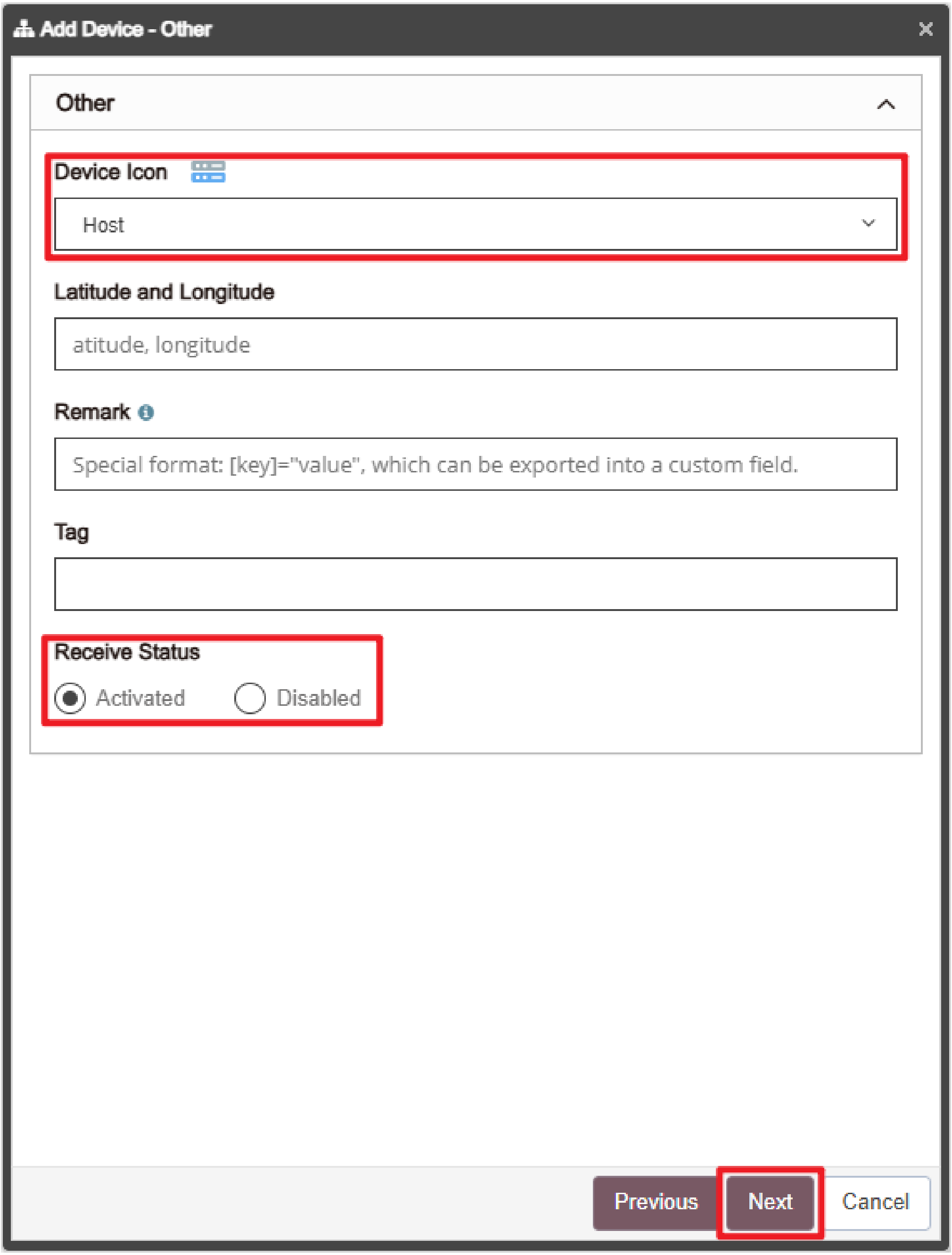
☑ Raw Data Kept

□ Raw data format is adopted while Syslog relaying is activated in Threshold Report.

□ The source IP will be kept in normalized data relaying

(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next.”



Add Device - Other ×

Other

Device Icon

Host

Latitude and Longitude

atitude, longitude

Remark

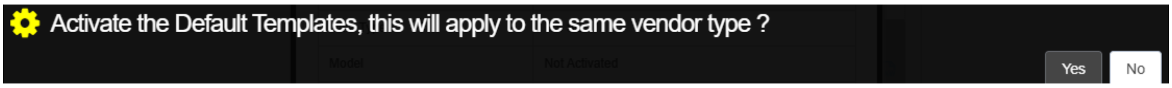
Special format: [key]="value", which can be exported into a custom field.

Tag

Receive Status

● Activated ○ Disabled

Enable default reports to be applied to devices of the same make and model → click “No.”

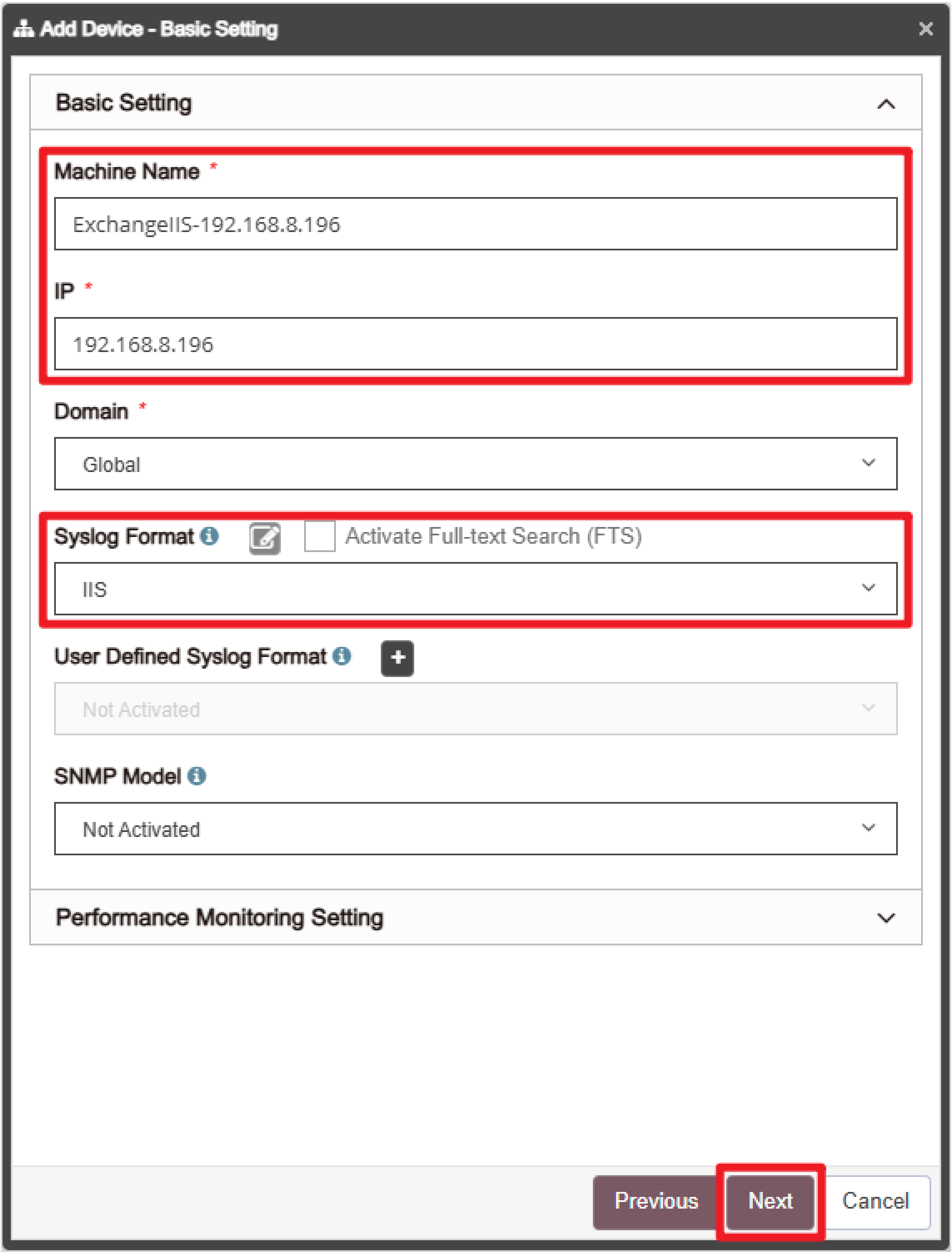


Activate the Default Templates, this will apply to the same vendor type ?

7.2 IIS Log

(1) Device Basic Settings

Enter the device name and IP → Select “IIS” for the Syslog data format → click “Next.”



Add Device - Basic Setting

Basic Setting

Machine Name *

ExchangeIIS-192.168.8.196

IP *

192.168.8.196

Domain *

Global

Syslog Format □ Activate Full-text Search (FTS)

IIS

User Defined Syslog Format

Not Activated

SNMP Model

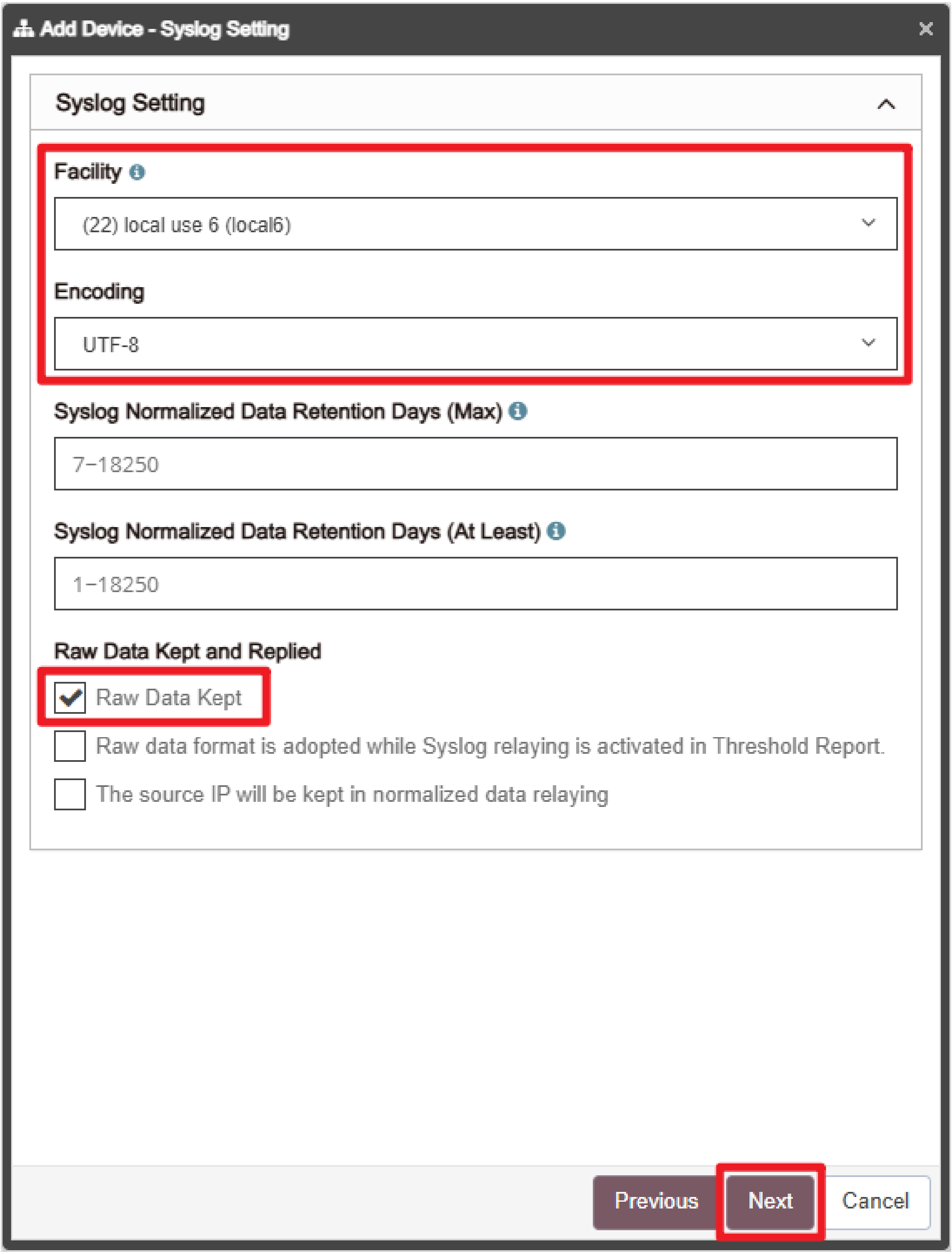
Not Activated

Performance Monitoring Setting

(2) Syslog Settings

Set “Facility” to “(22) local use 6 (local6)” and “Encoding” to “UTF-8” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.



Add Device - Syslog Setting

Syslog Setting

Facility: (22) local use 6 (local6)

Encoding: UTF-8

Syslog Normalized Data Retention Days (Max): 7~18250

Syslog Normalized Data Retention Days (At Least): 1~18250

Raw Data Kept and Replied

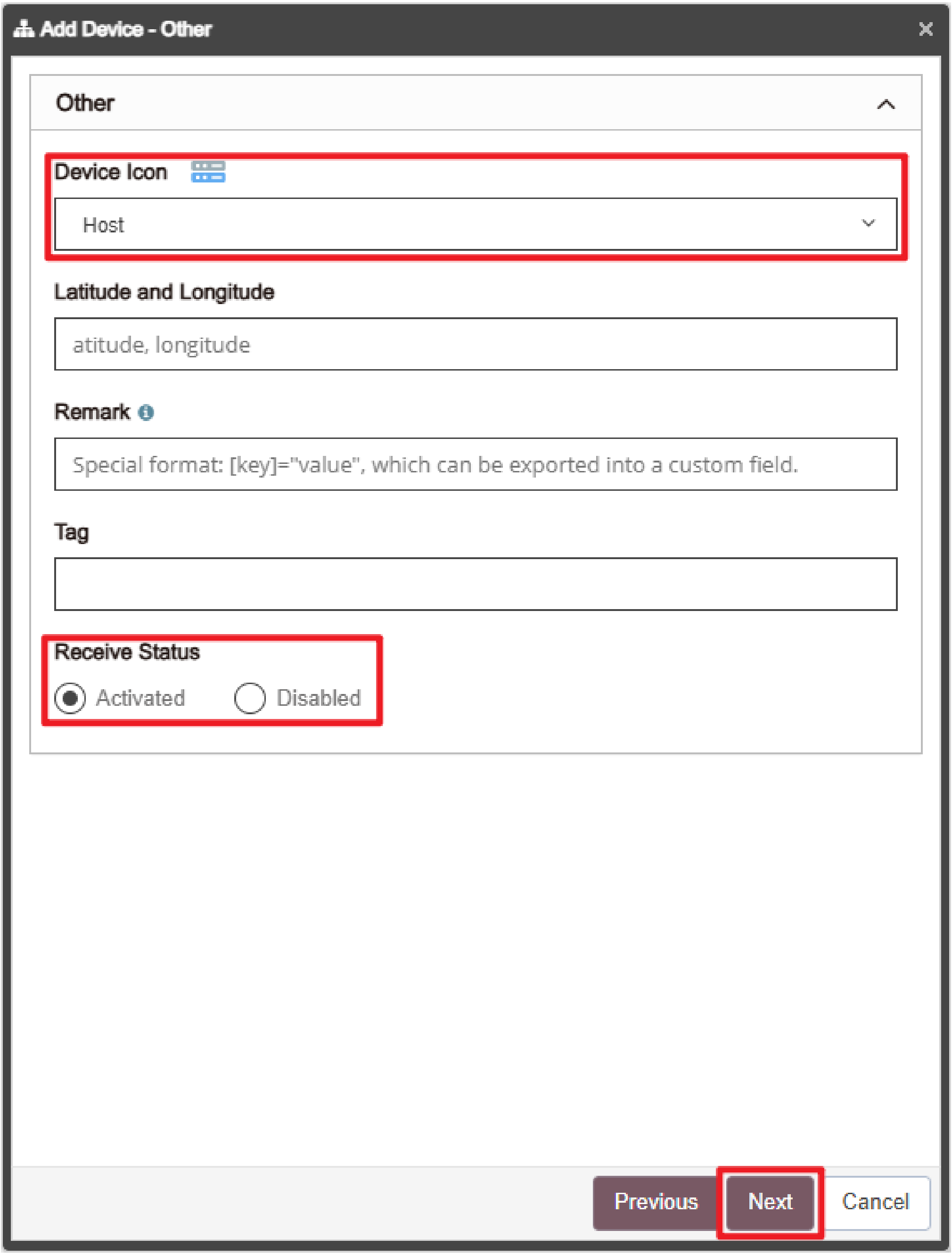
☑ Raw Data Kept

□ Raw data format is adopted while Syslog relaying is activated in Threshold Report.

□ The source IP will be kept in normalized data relaying

(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next.”



Add Device - Other

Other

Device Icon: Host

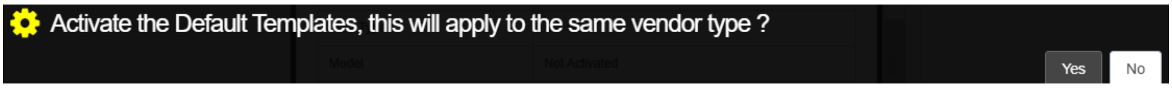
Latitude and Longitude: atitude, longitude

Remark: Special format: [key]="value", which can be exported into a custom field.

Tag:

Receive Status: ● Activated ○ Disabled

Enable default reports to be applied to devices of the same make and model → click “No.”

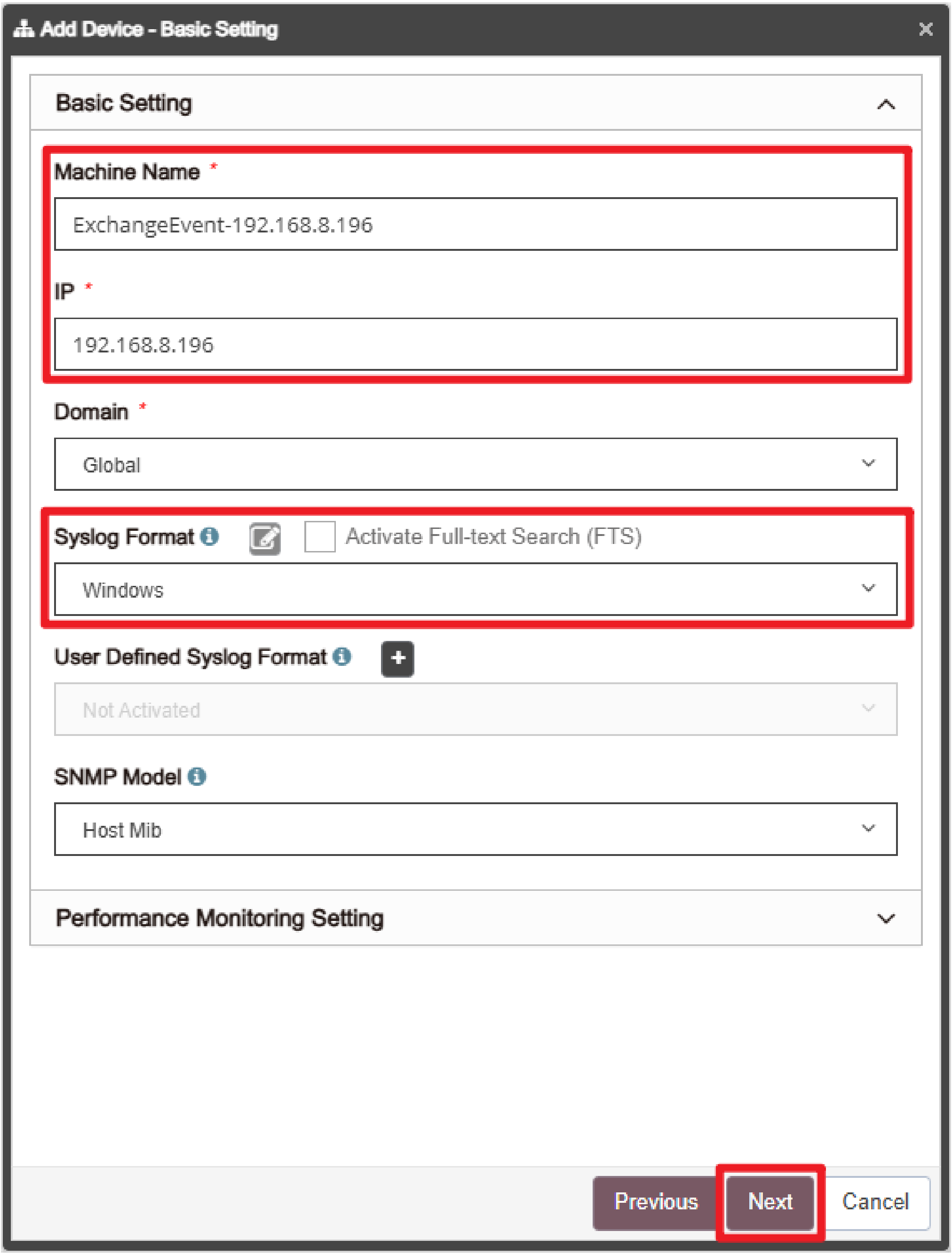


Activate the Default Templates, this will apply to the same vendor type ?

7.3 Event Log

(1) Device Basic Settings

Enter the device name and IP → Select “Windows” for the Syslog data format → click “Next.”



Add Device - Basic Setting

Basic Setting

Machine Name *: ExchangeEvent-192.168.8.196

IP *: 192.168.8.196

Domain *: Global

Syslog Format: Windows

□ Activate Full-text Search (FTS)

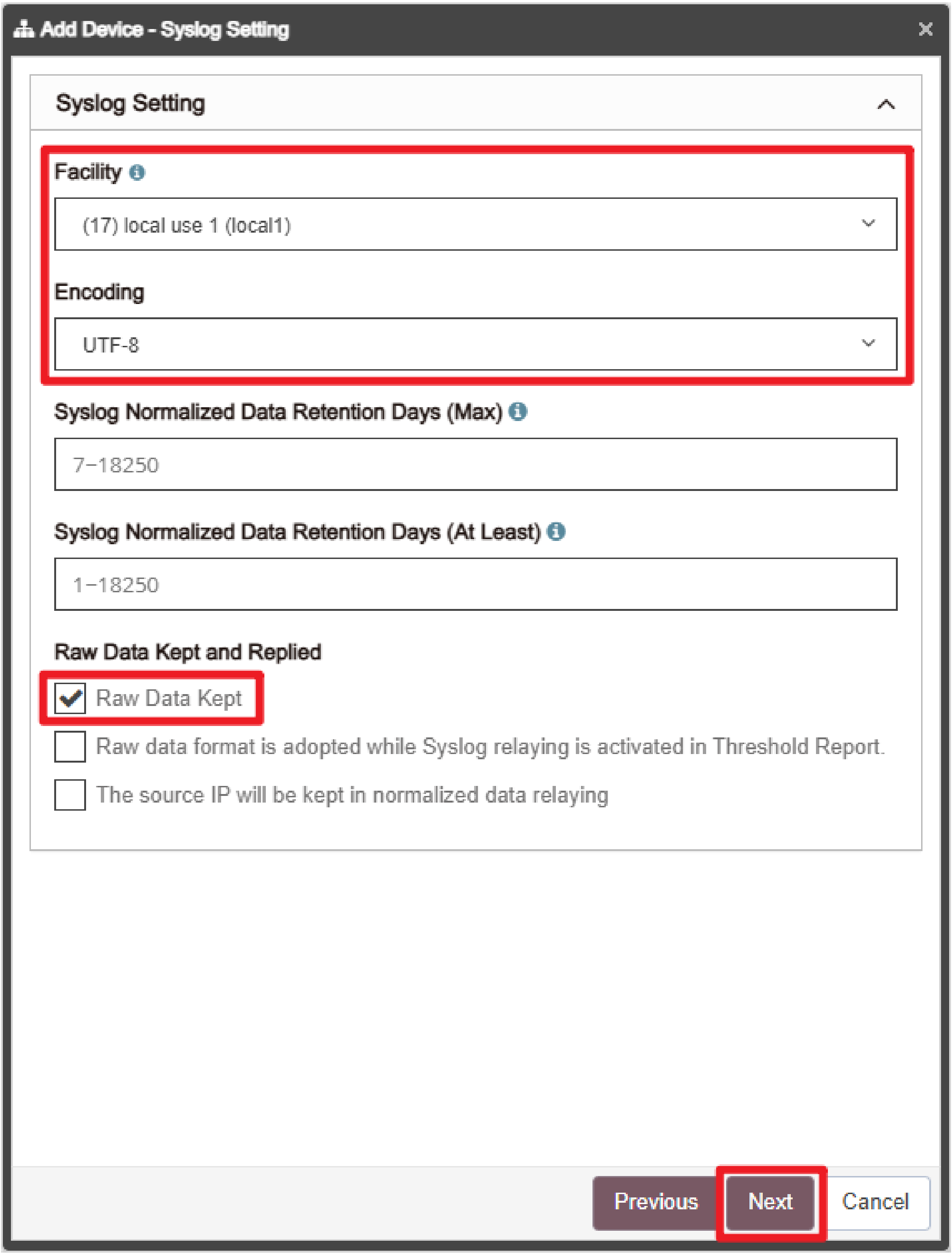
User Defined Syslog Format: Not Activated

SNMP Model: Host Mib

(2) Syslog Settings

Set “Facility” to “(17) local use 1 (local1)” and “Encoding” to “UTF-8” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.



Add Device - Syslog Setting

Syslog Setting

Facility: (17) local use 1 (local1)

Encoding: UTF-8

Syslog Normalized Data Retention Days (Max): 7~18250

Syslog Normalized Data Retention Days (At Least): 1~18250

Raw Data Kept and Replied

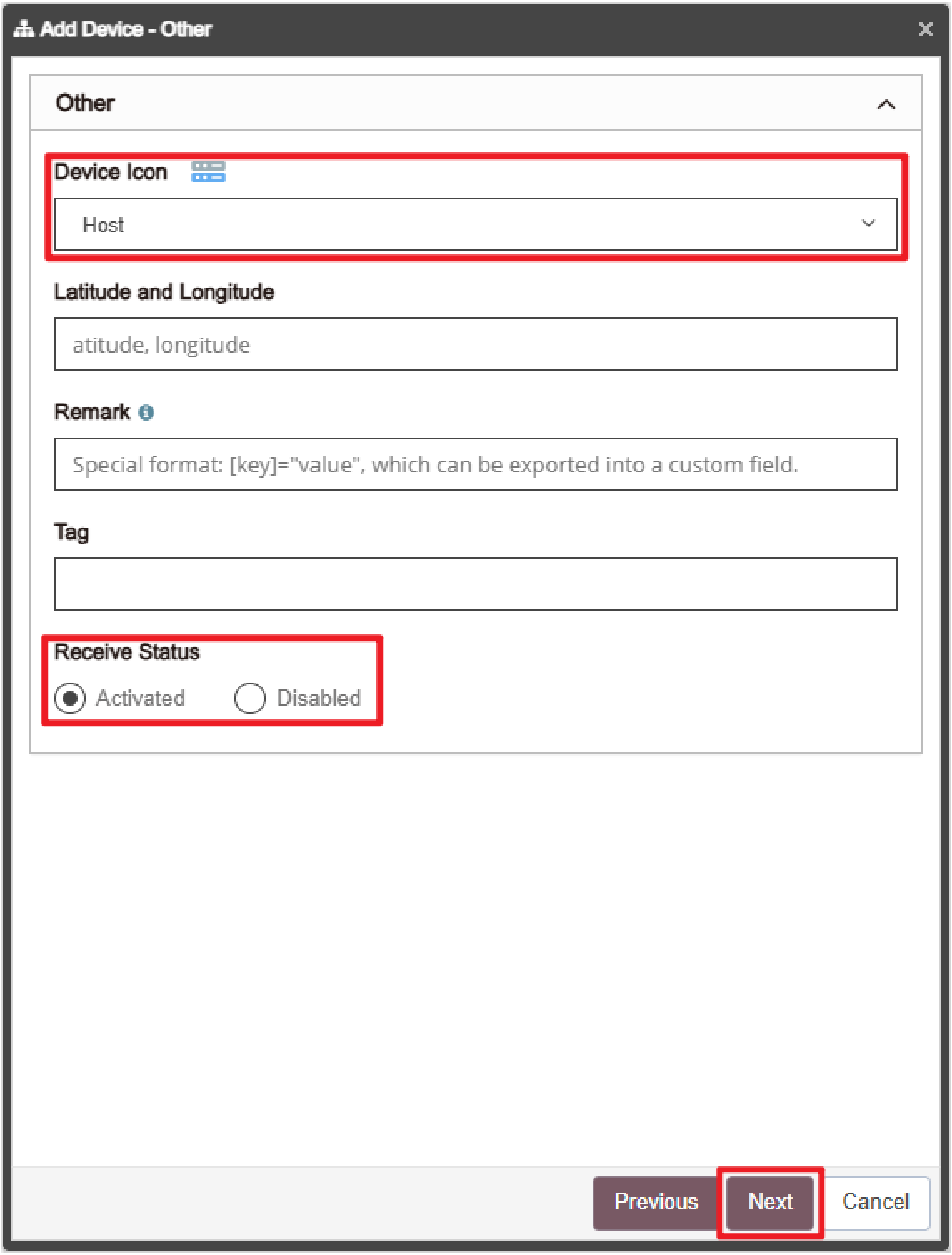
☑ Raw Data Kept

□ Raw data format is adopted while Syslog relaying is activated in Threshold Report.

□ The source IP will be kept in normalized data relaying

(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next.”



Add Device - Other

Other

Device Icon

Host

Latitude and Longitude

atitude, longitude

Remark

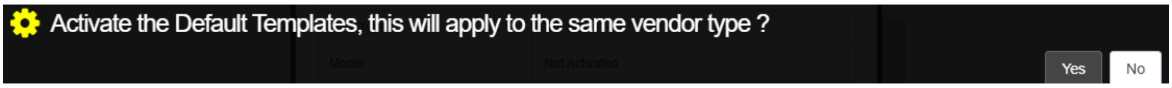
Special format: [key]="value", which can be exported into a custom field.

Tag

Receive Status

● Activated ○ Disabled

Enable default reports to be applied to devices of the same make and model → click “No.”

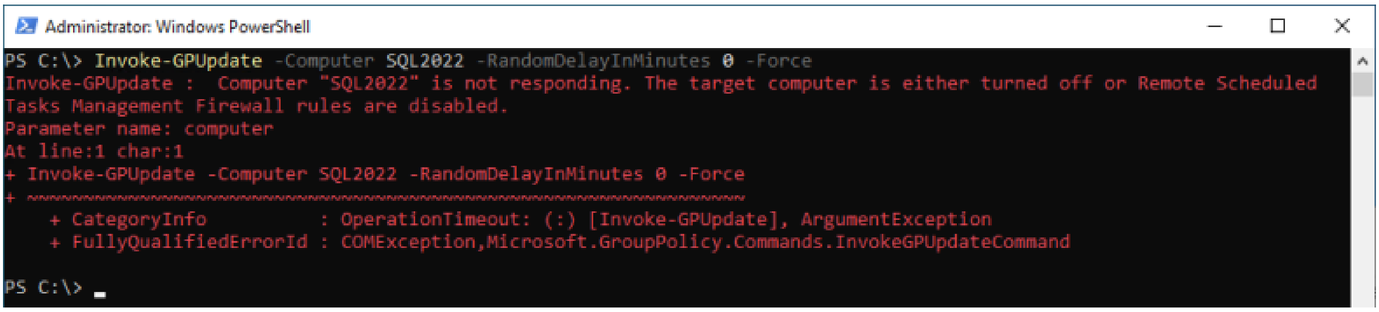


Activate the Default Templates, this will apply to the same vendor type ?

8. Troubleshooting

8.1 Invoke-GPUpdate Error

(1) On the server, run Invoke-GPUpdate to update the Windows Server Group Policy. An error message may appear.



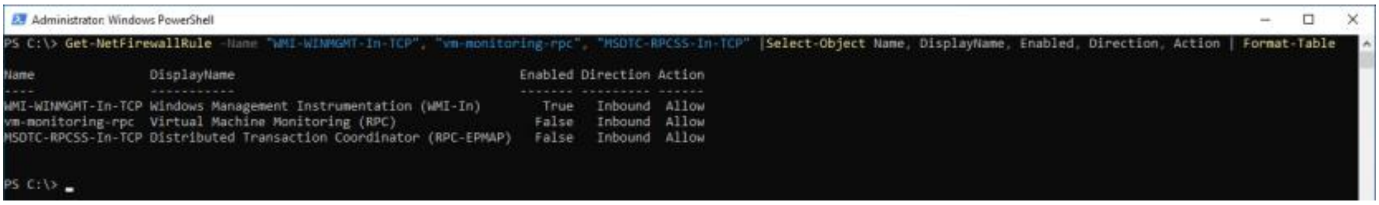
Administrator: Windows PowerShell

```
PS C:\> Invoke-GPUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
Invoke-GPUpdate :  Computer "SQL2022" is not responding. The target computer is either turned off or Remote Scheduled
Tasks Management Firewall rules are disabled.
Parameter name: computer
At line:1 char:1
+ Invoke-GPUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : OperationTimeout: (:) [Invoke-GPUpdate], ArgumentException
    + FullyQualifiedErrorId : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUpdateCommand

PS C:\> _
```

(2) On the Windows Server, open “Windows PowerShell.”

(3) Enter the following command to check the Windows Firewall rules for **WMI-WINMGMT-In-TCP, vm-monitoring-rpc, MSDTC-RPCSS-In-TCP:**

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```

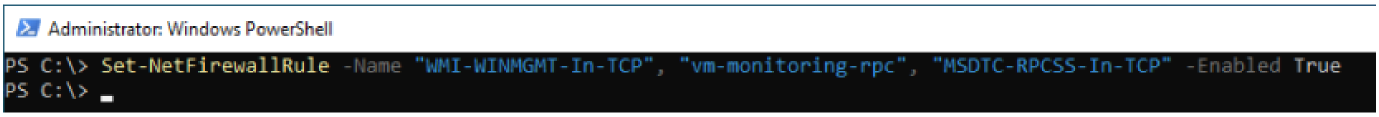


Administrator: Windows PowerShell

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table

Name               DisplayName                                  Enabled Direction Action
----               -----------                                  ------- --------- ------
WMI-WINMGMT-In-TCP Windows Management Instrumentation (WMI-In)     True   Inbound  Allow
vm-monitoring-rpc  Virtual Machine Monitoring (RPC)                False   Inbound  Allow
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP) False   Inbound  Allow


PS C:\> _
```

(4) Enter the following command to enable the Windows Firewall rules **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**:

```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
```

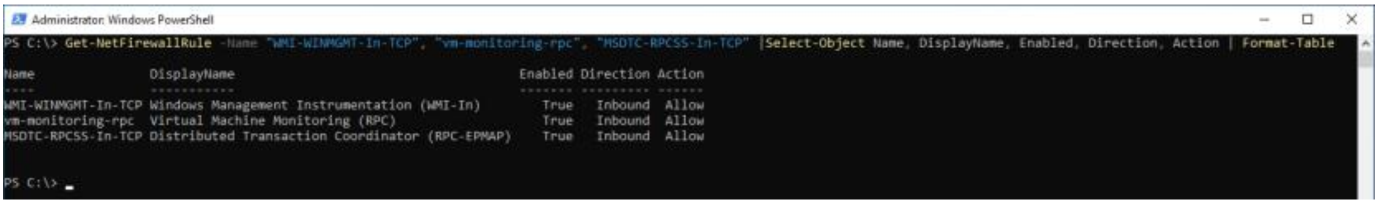


Administrator: Windows PowerShell

```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
PS C:\> _
```

(5) Enter the following command to verify the Windows Firewall rules **WMI-WINMGMT-In-TCP, vm-monitoring-rpc, MSDTC-RPCSS-In-TCP** again:

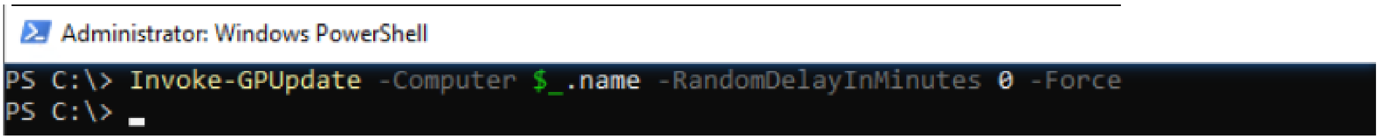
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table

Name               DisplayName                                    Enabled Direction Action
----               -----------                                    ------- --------- ------
WMI-WINMGMT-In-TCP Windows Management Instrumentation (WMI-In)       True   Inbound  Allow
vm-monitoring-rpc  Virtual Machine Monitoring (RPC)                  True   Inbound  Allow
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP)   True   Inbound  Allow


PS C:\> _
```

(6) On the server, enter the following command to update the AD Server Group Policy:

```
PS C:\> Invoke-GPUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```



```
PS C:\> Invoke-GPUpdate -Computer $_.name -RandomDelayInMinutes 0 -Force
PS C:\> _
```

Note: Replace the text shown in red with the AD Server name.

Tel：+886-4-23752865　Fax：+886-4-23757458

Sales Information：sales@npartner.com

Technical Support：support@npartner.com