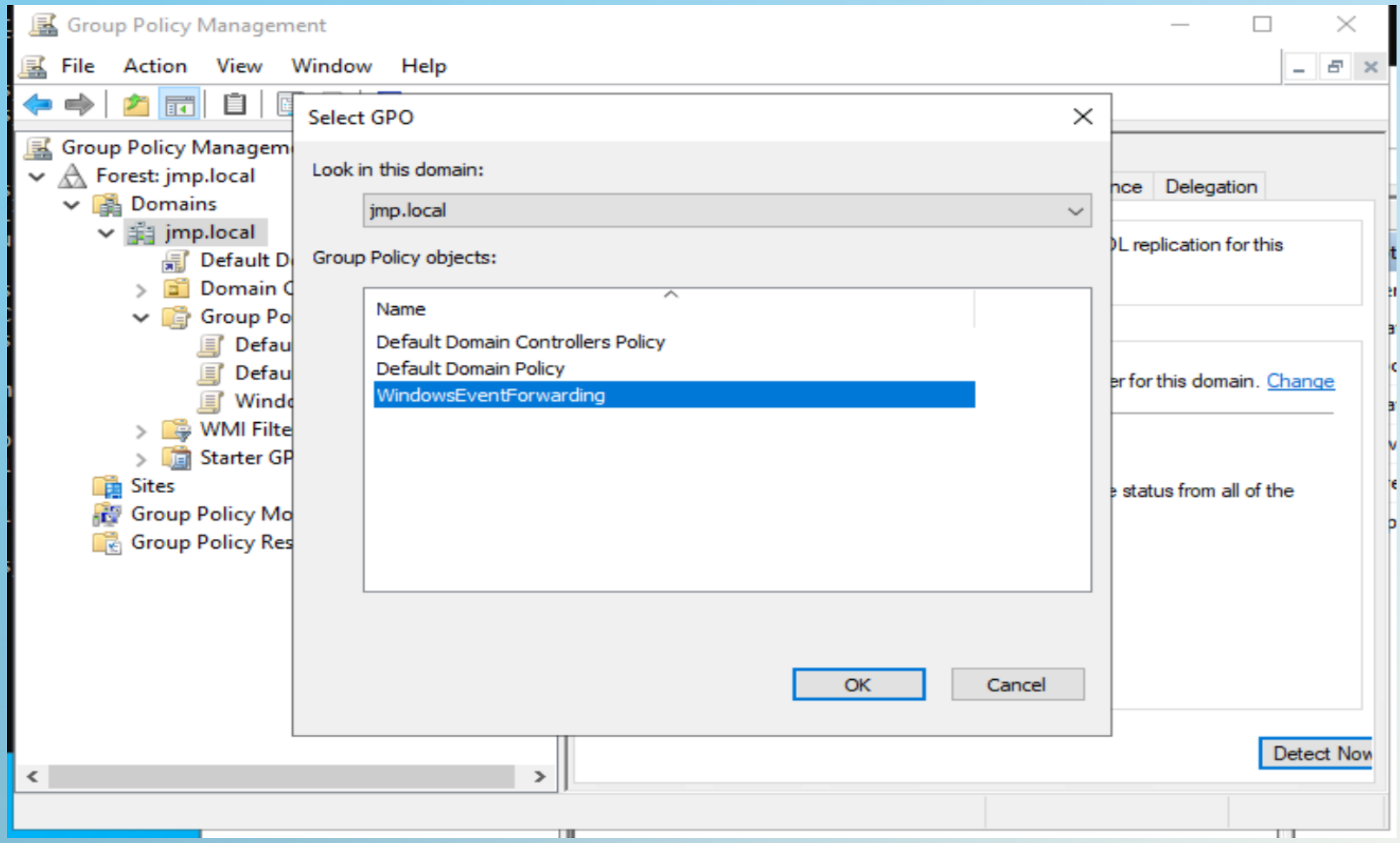
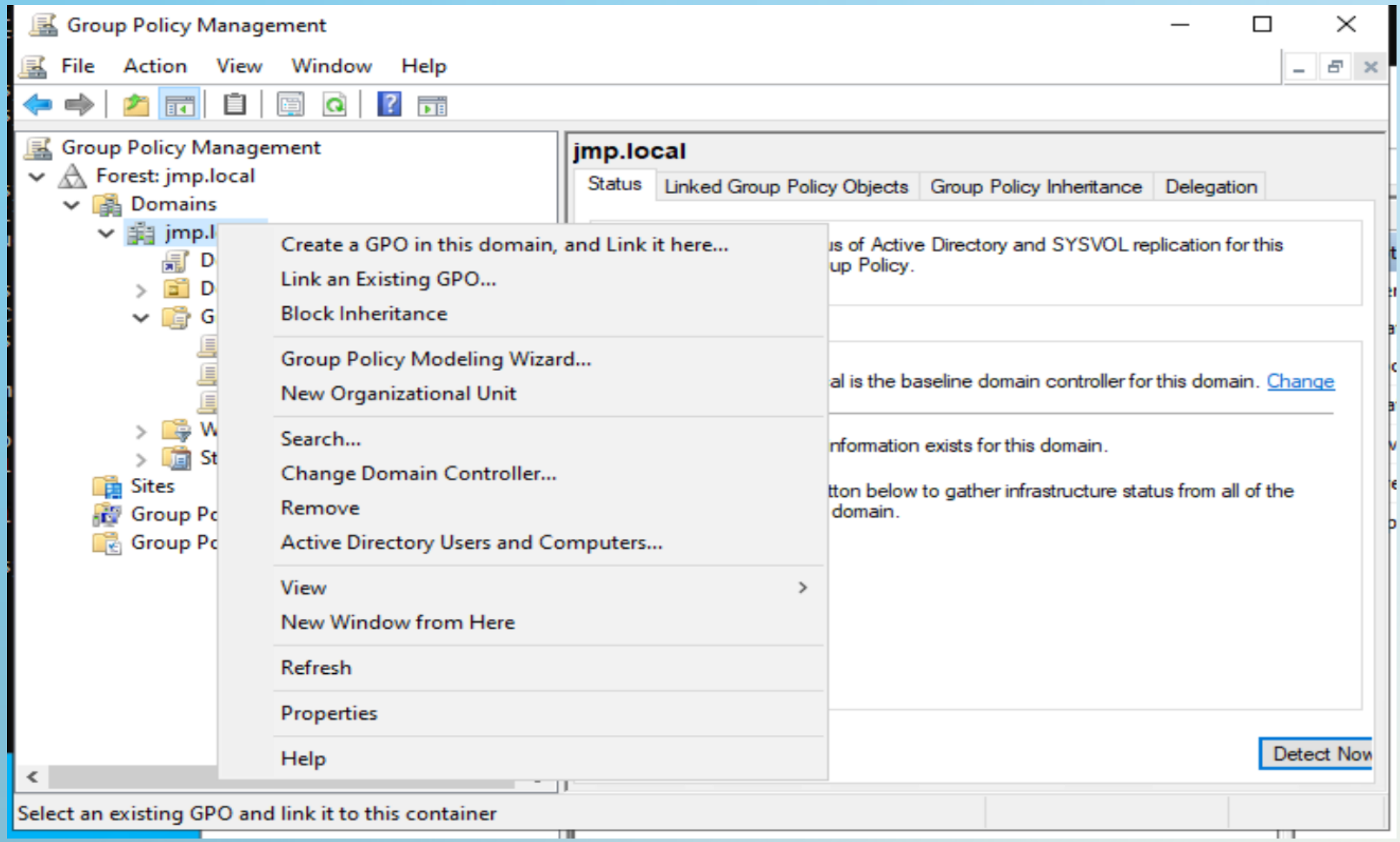
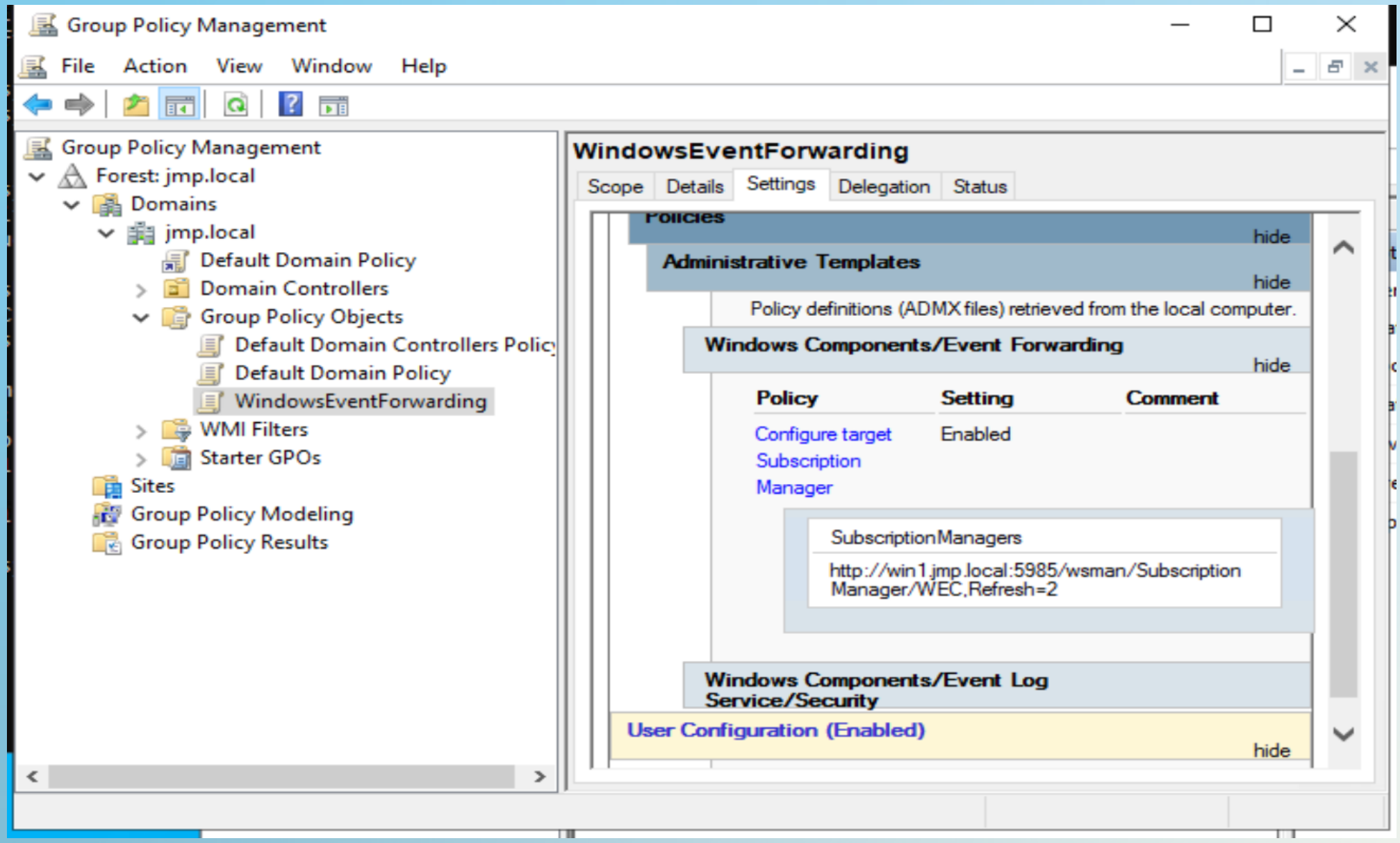
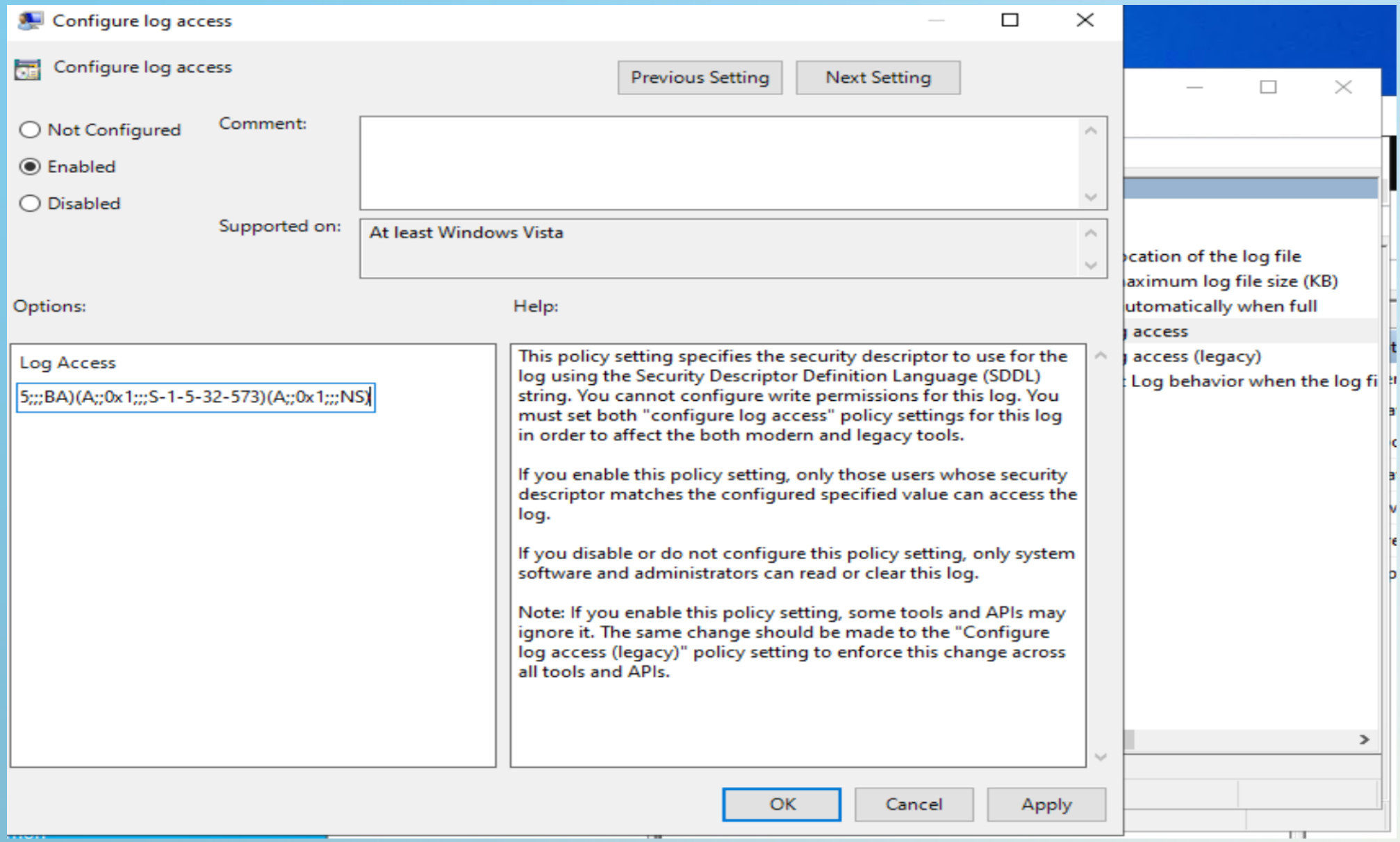
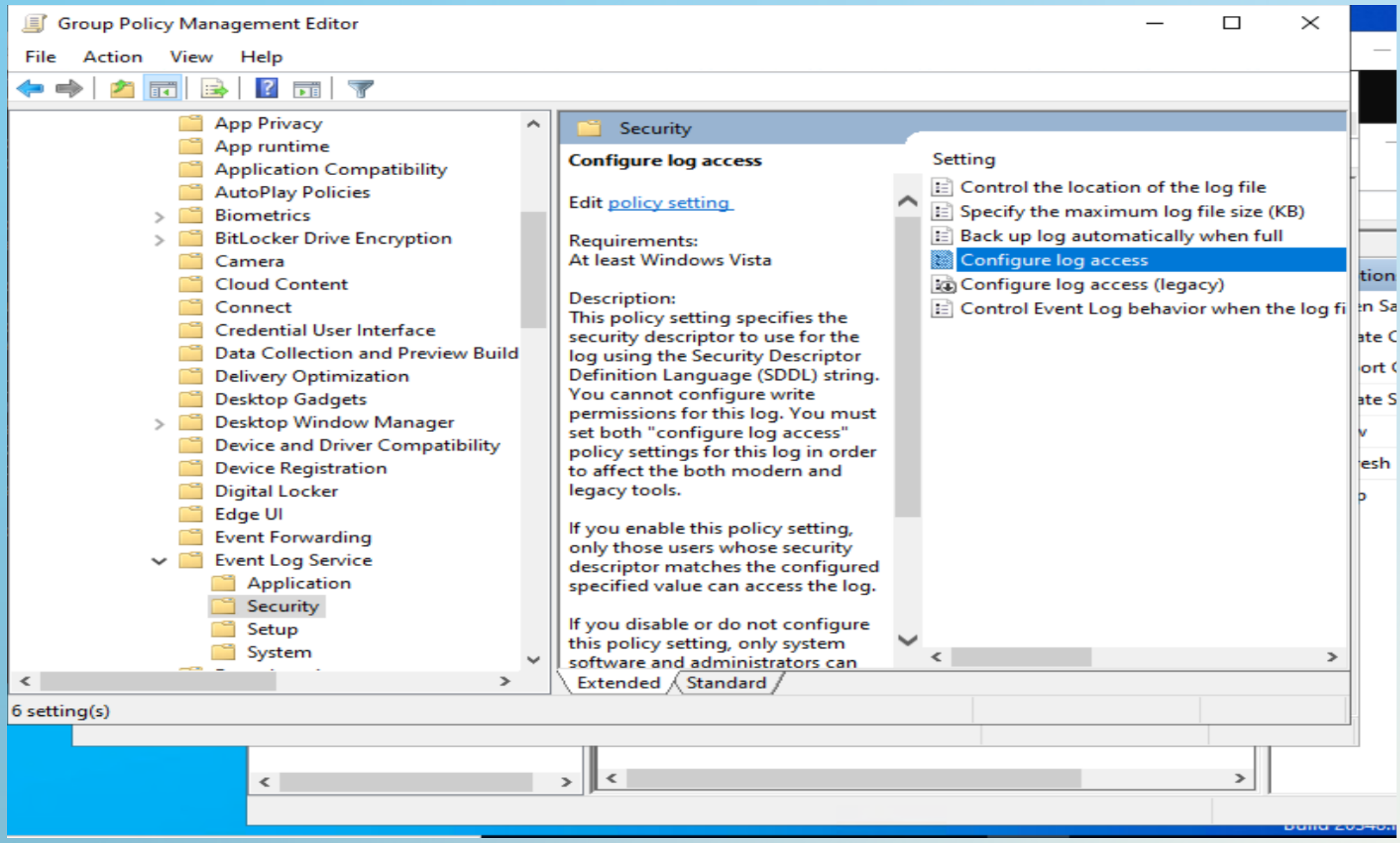
"installation d'une "WEF" en images".

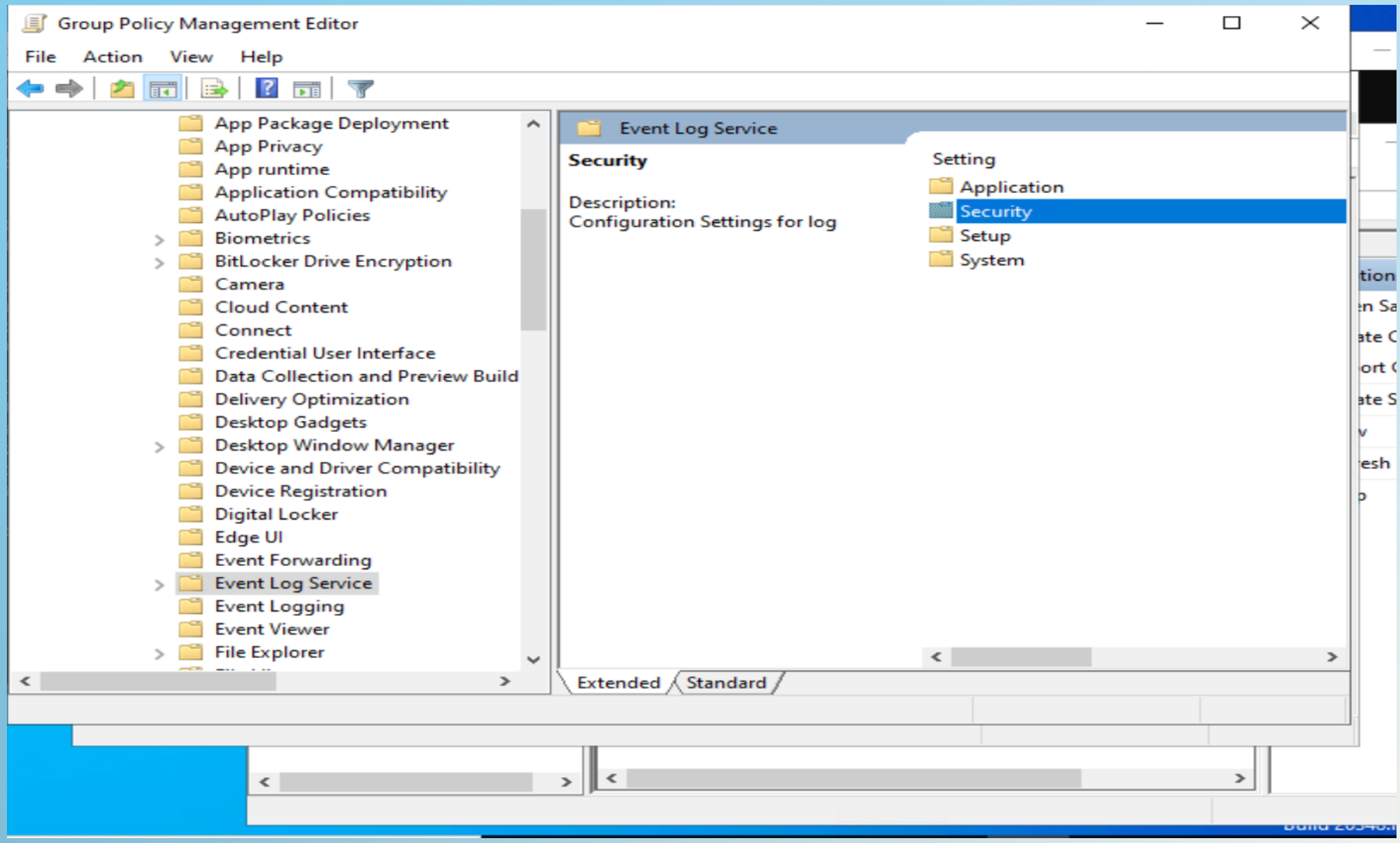

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Sites
Group Policy Mo
Group Policy Res
Select GPO
Look in this domain:
jmp.local
Group Policy objects:
Name
Default Domain Controllers Policy
Default Domain Policy
WindowsEventForwarding
OK
Cancel
Delegation
L replication for this
er for this domain. Change
status from all of the
Detect Now

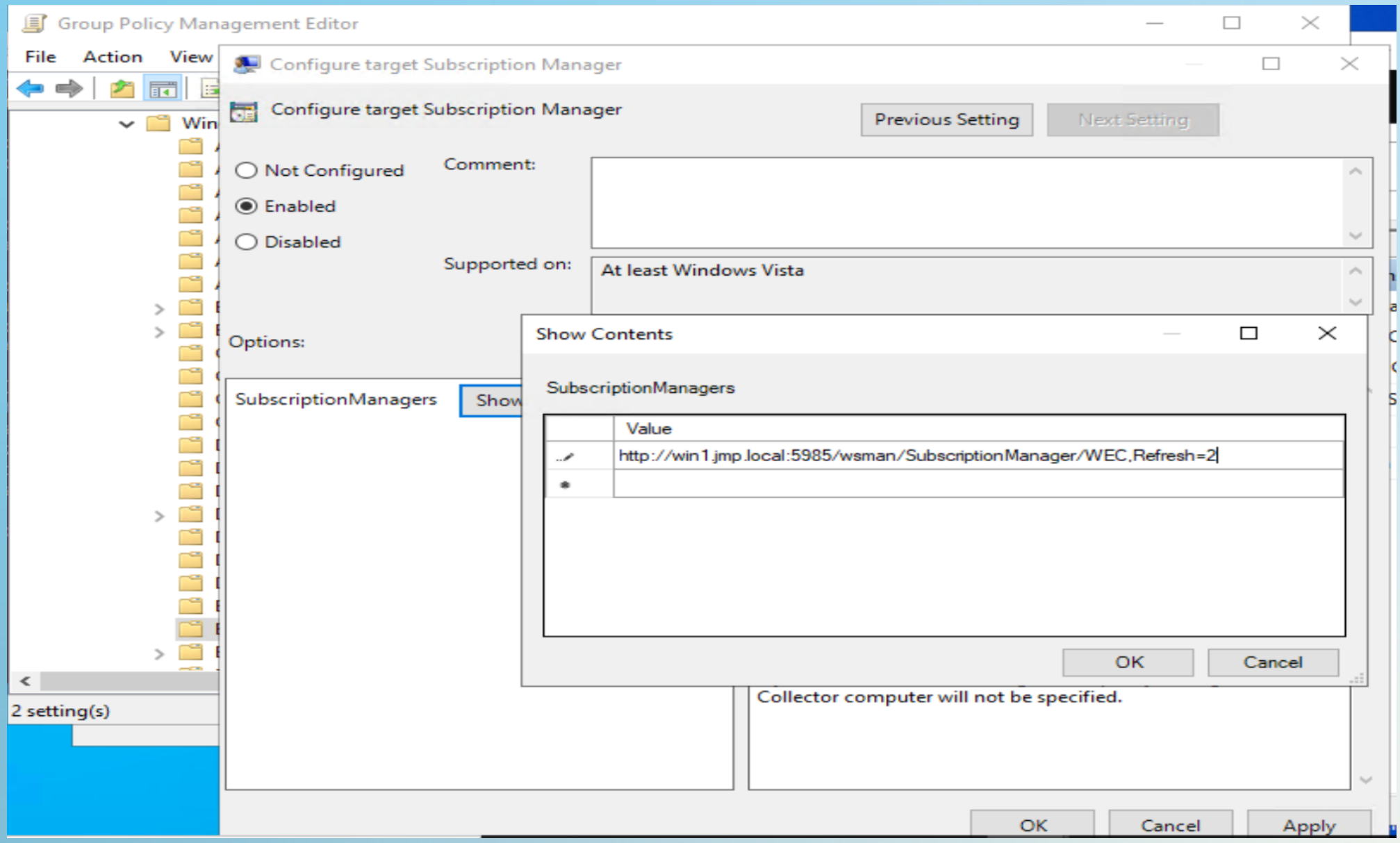

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
Sites
jmp.local
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
View
New Window from Here
Refresh
Properties
Help
Change
Detect Now
Select an existing GPO and link it to this container

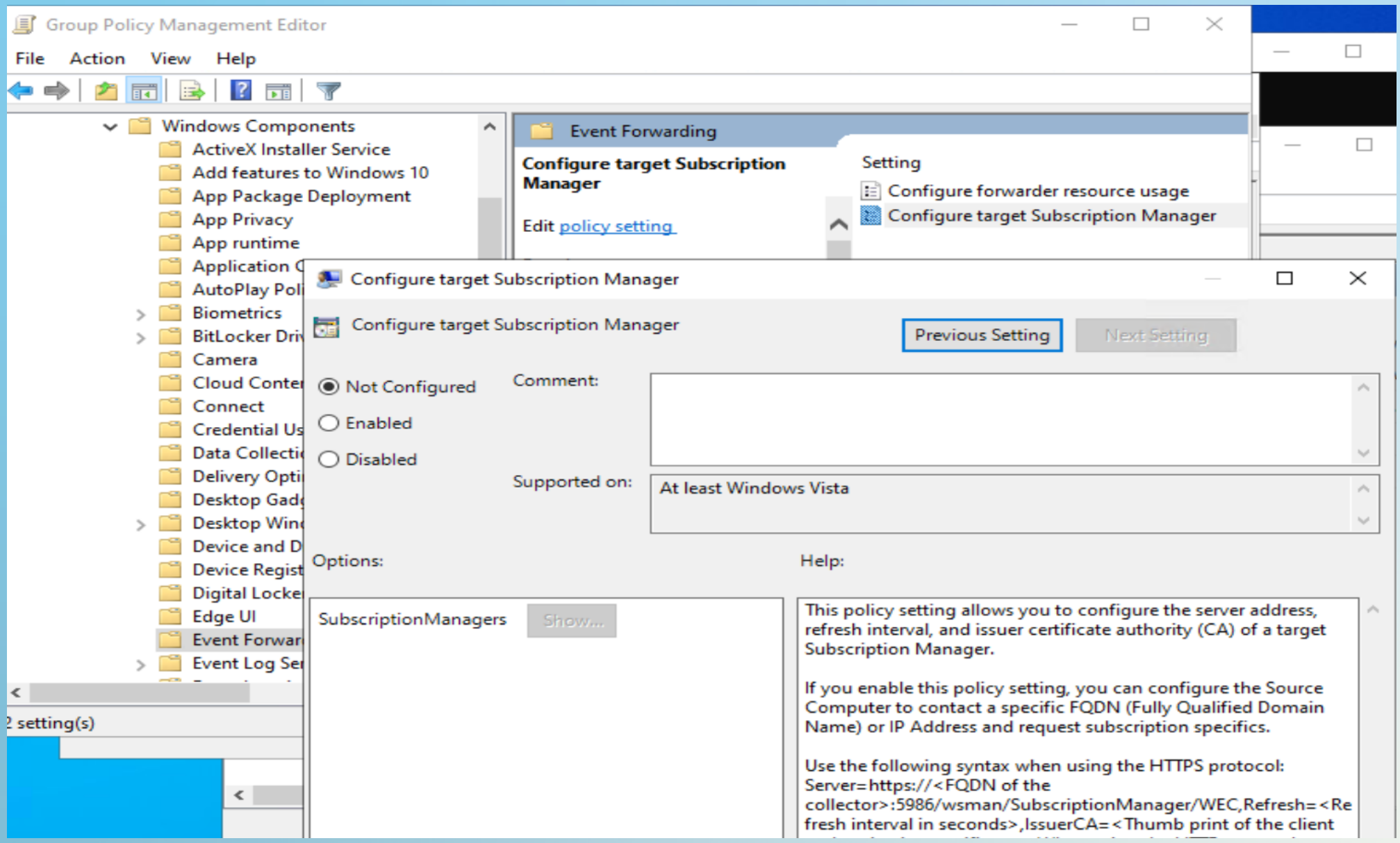

Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WindowsEventForwarding
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
WindowsEventForwarding
Scope Details Settings Delegation Status
Policies
hide
Administrative Templates
hide
Policy definitions (ADMX files) retrieved from the local computer.
Windows Components/Event Forwarding
hide
Policy
Setting
Comment
Configure target Subscription Manager
Enabled
SubscriptionManagers
http://win1.jmp.local:5985/wsman/SubscriptionManager/WEC,Refresh=2
Windows Components/Event Log Service/Security
User Configuration (Enabled)
hide

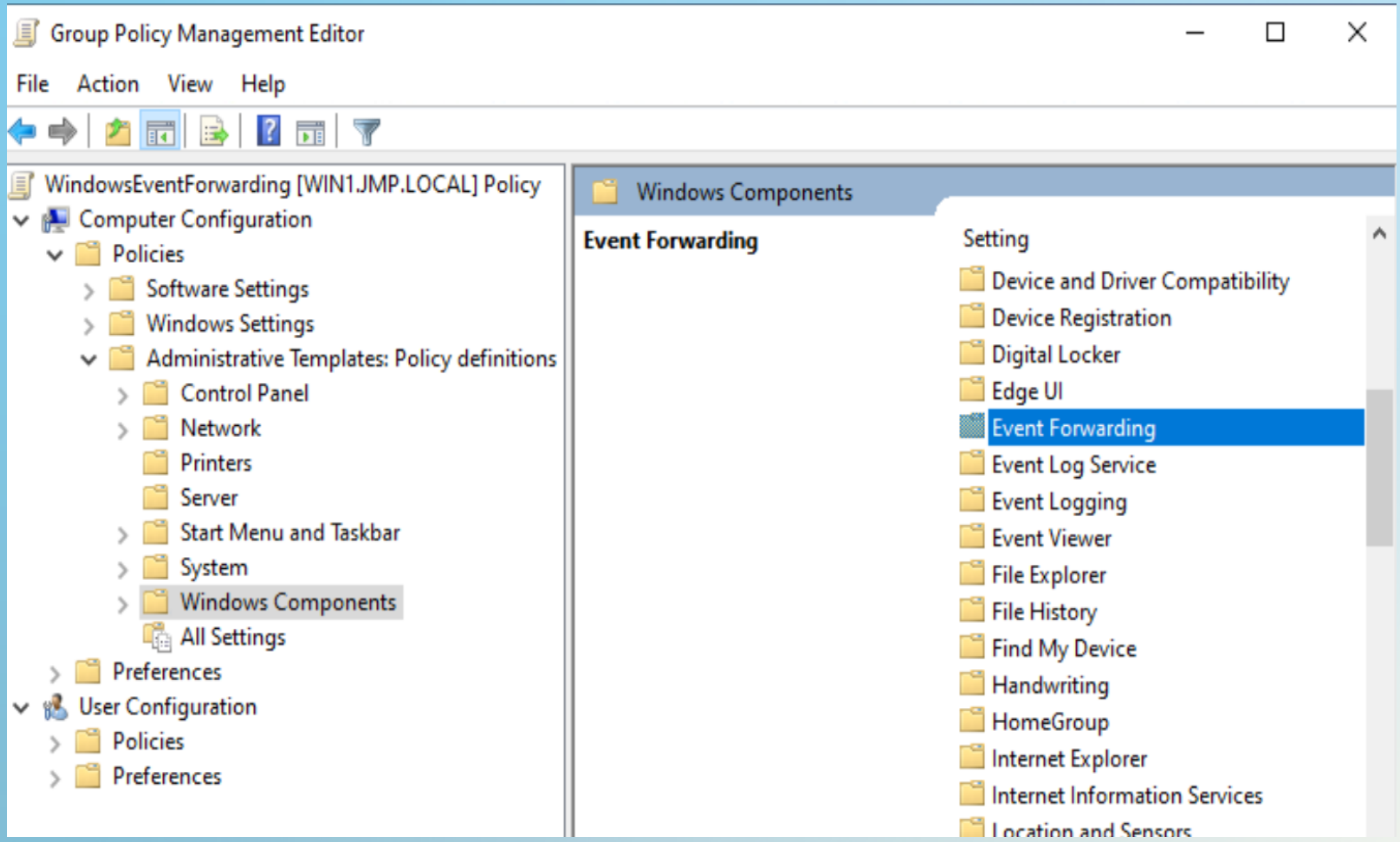

Configure log access
Configure log access
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
Log Access
5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
This policy setting specifies the security descriptor to use for the log using the Security Descriptor Definition Language (SDDL) string. You cannot configure write permissions for this log. You must set both "configure log access" policy settings for this log in order to affect the both modern and legacy tools.
If you enable this policy setting, only those users whose security descriptor matches the configured specified value can access the log.
If you disable or do not configure this policy setting, only system software and administrators can read or clear this log.
Note: If you enable this policy setting, some tools and APIs may ignore it. The same change should be made to the "Configure log access (legacy)" policy setting to enforce this change across all tools and APIs.
OK
Cancel
Apply
cation of the log file
aximum log file size (KB)
utomatically when full
access
access (legacy)
Log behavior when the log fi

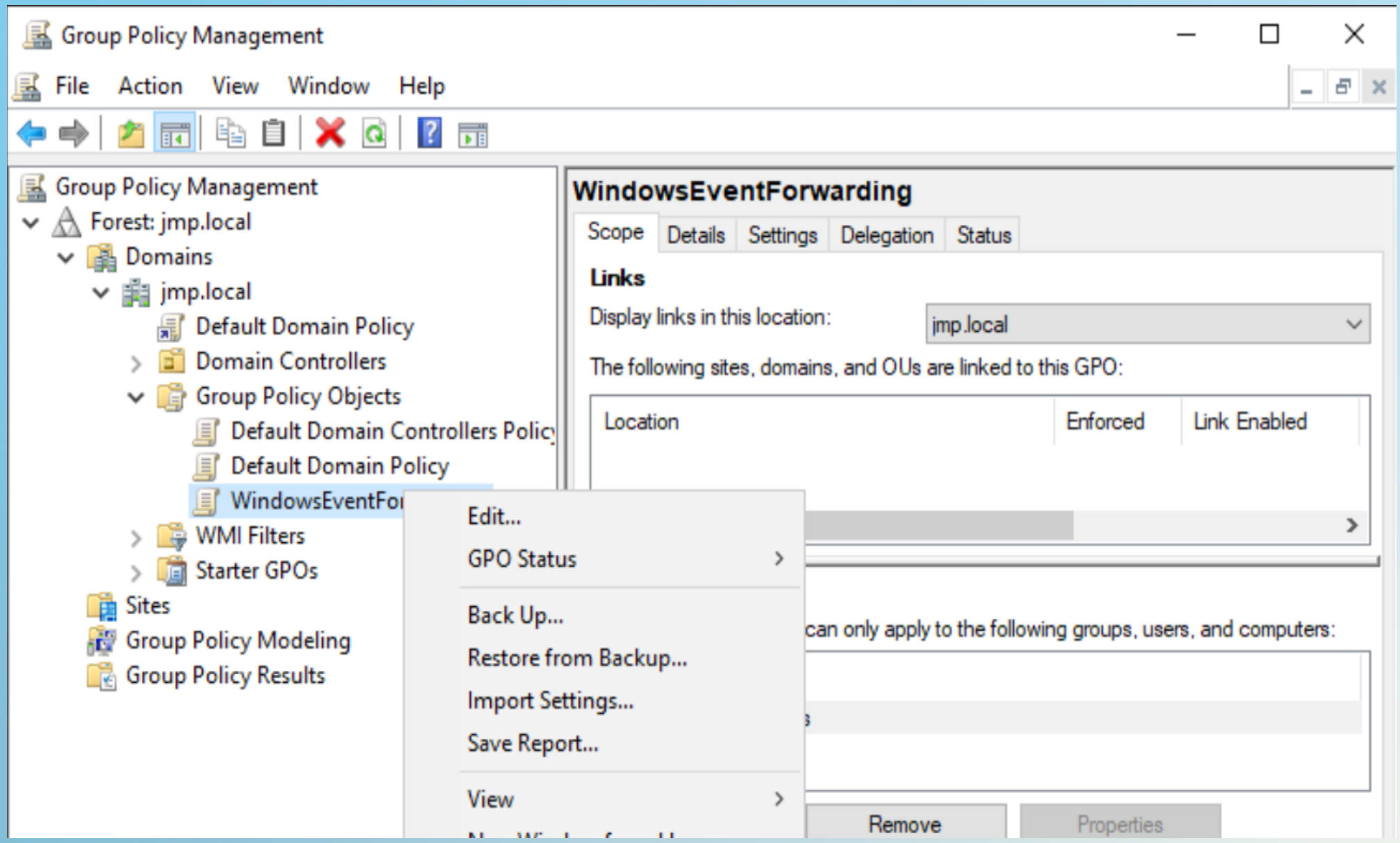

Group Policy Management Editor
File Action View Help
App Privacy
App runtime
Application Compatibility
AutoPlay Policies
Biometrics
BitLocker Drive Encryption
Camera
Cloud Content
Connect
Credential User Interface
Data Collection and Preview Build
Delivery Optimization
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility
Device Registration
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Application
Security
Setup
System
Security
Configure log access
Edit policy setting
Requirements:
At least Windows Vista
Description:
This policy setting specifies the security descriptor to use for the log using the Security Descriptor Definition Language (SDDL) string. You cannot configure write permissions for this log. You must set both "configure log access" policy settings for this log in order to affect the both modern and legacy tools.
If you enable this policy setting, only those users whose security descriptor matches the configured specified value can access the log.
If you disable or do not configure this policy setting, only system software and administrators can
Setting
Control the location of the log file
Specify the maximum log file size (KB)
Back up log automatically when full
Configure log access
Configure log access (legacy)
Control Event Log behavior when the log fi
Extended
Standard
6 setting(s)

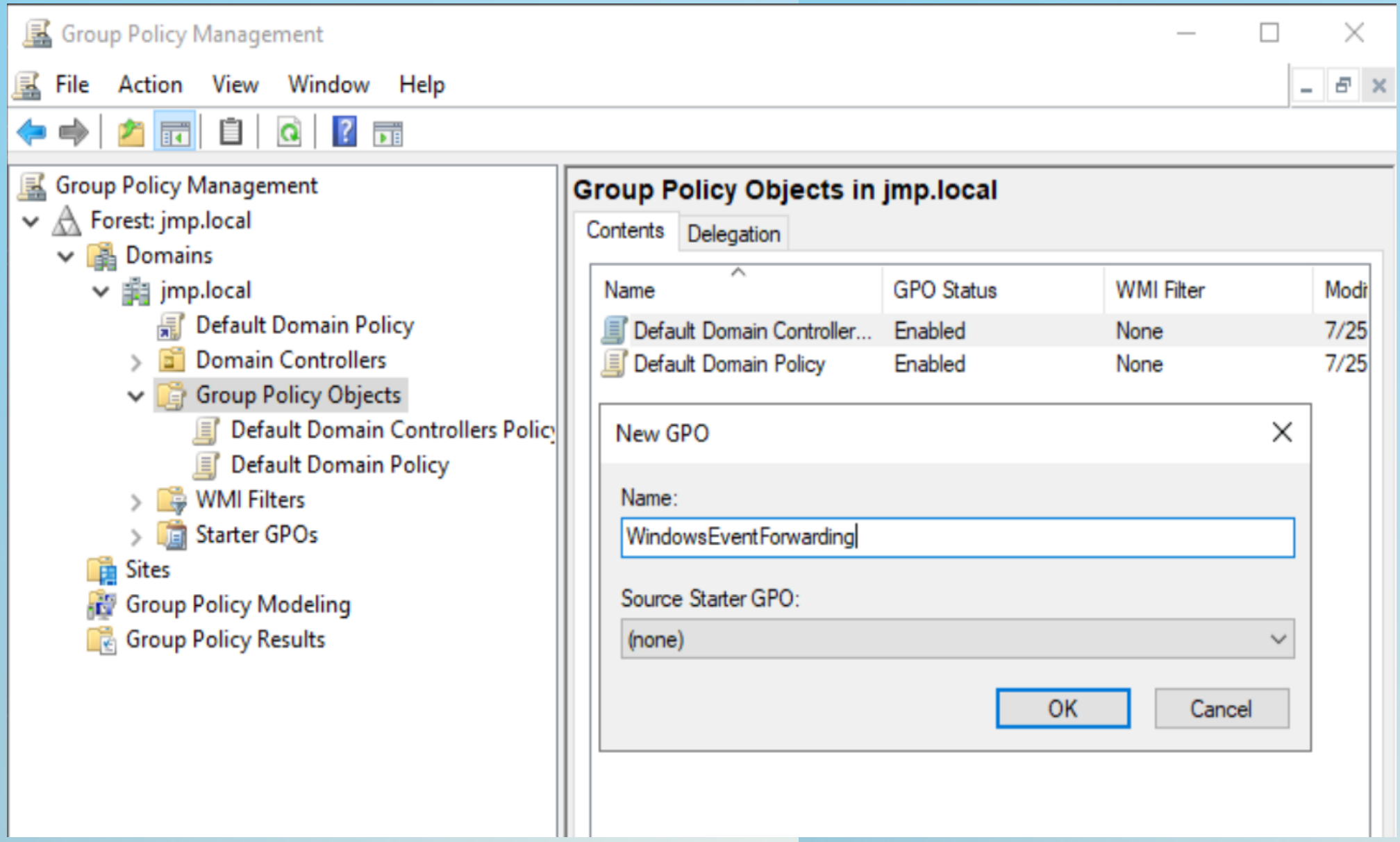

Group Policy Management Editor
File
Action
View
Help
App Package Deployment
App Privacy
App runtime
Application Compatibility
AutoPlay Policies
Biometrics
BitLocker Drive Encryption
Camera
Cloud Content
Connect
Credential User Interface
Data Collection and Preview Build
Delivery Optimization
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility
Device Registration
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Event Logging
Event Viewer
File Explorer
Event Log Service
Security
Description:
Configuration Settings for log
Setting
Application
Security
Setup
System
Extended
Standard


Group Policy Management Editor
File Action View
Configure target Subscription Manager
Configure target Subscription Manager
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
SubscriptionManagers
Show
Show Contents
SubscriptionManagers
Value
http://win1.jmp.local:5985/wsman/SubscriptionManager/WEC,Refresh=2
OK
Cancel
Collector computer will not be specified.
2 setting(s)
OK
Cancel
Apply


Group Policy Management Editor
File Action View Help
Windows Components
ActiveX Installer Service
Add features to Windows 10
App Package Deployment
App Privacy
App runtime
Biometrics
Camera
Connect
Edge UI
Event Log Se
2 setting(s)
Event Forwarding
Configure target Subscription Manager
Edit policy setting
Setting
Configure forwarder resource usage
Configure target Subscription Manager
Configure target Subscription Manager
Configure target Subscription Manager
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
SubscriptionManagers
Show...
This policy setting allows you to configure the server address, refresh interval, and issuer certificate authority (CA) of a target Subscription Manager.
If you enable this policy setting, you can configure the Source Computer to contact a specific FQDN (Fully Qualified Domain Name) or IP Address and request subscription specifics.
Use the following syntax when using the HTTPS protocol:
Server=https://<FQDN of the collector>:5986/wsman/SubscriptionManager/WEC,Refresh=<Refresh interval in seconds>,IssuerCA=<Thumb print of the client


Group Policy Management Editor
File Action View Help
WindowsEventForwarding [WIN1.JMP.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions
Control Panel
Network
Printers
Server
Start Menu and Taskbar
System
Windows Components
All Settings
Preferences
User Configuration
Policies
Preferences
Windows Components
Event Forwarding
Setting
Device and Driver Compatibility
Device Registration
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Event Logging
Event Viewer
File Explorer
File History
Find My Device
Handwriting
HomeGroup
Internet Explorer
Internet Information Services
Location and Sensors


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WindowsEventFo
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Edit...
GPO Status
Back Up...
Restore from Backup...
Import Settings...
Save Report...
View
WindowsEventForwarding
Scope Details Settings Delegation Status
Links
Display links in this location:
jmp.local
The following sites, domains, and OUs are linked to this GPO:
Location
Enforced
Link Enabled
can only apply to the following groups, users, and computers:
Remove
Properties


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jmp.local
Domains
jmp.local
Default Domain Policy
Domain Controllers
Group Policy Objects
Default Domain Controllers Policy
Default Domain Policy
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in jmp.local
Contents
Delegation
Name
GPO Status
WMI Filter
Modi
Default Domain Controller...
Enabled
None
7/25
Default Domain Policy
Enabled
None
7/25
New GPO
Name:
WindowsEventForwarding
Source Starter GPO:
(none)
OK
Cancel

```
jmp\vagrant@WIN1 C:\Users\vagrant>wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\Security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:
  fileMax: 1

jmp\vagrant@WIN1 C:\Users\vagrant>O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
```