

Active Directory Management:  
Group Policy monitoring, reporting, and alerting  
....and recovery!

Derek Melber

derek@manageengine.com

---

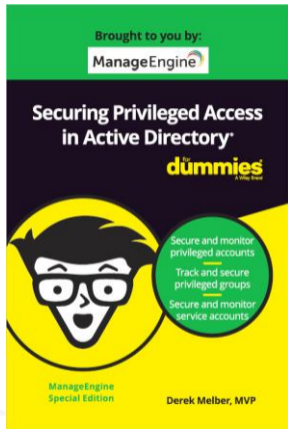
## About Your Speaker



# About Derek Melber

---

- Derek Melber, MVP (AD and Group Policy)
  - [derek@manageengine.com](mailto:derek@manageengine.com)
- Online Resources
  - ManageEngine Active Directory Blog
  - Security Hardening Site
  - Download free Dummies book



# Agenda

---

- Tracking changes made to Group Policy Objects (GPOs)
- Backing up and restoring GPOs and settings

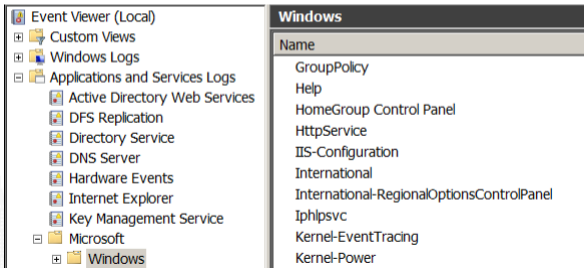
---

## Tracking changes made to Group Policy Objects (GPOs)



# Tracking changes made to (GPOs)

- Need to configure 'auditing' in Group Policy
- Need to configure SACL for Sysvol and AD (GPT and GPC)
- Results show in two locations in Event Viewer
  - Security Log
  - GroupPolicy operational log



The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs, with 'Windows' selected under the 'Microsoft' folder. The right pane, titled 'Windows', shows a list of application names.

Name
GroupPolicy
Help
HomeGroup Control Panel
HttpService
IIS-Configuration
International
International-RegionalOptionsControlPanel
Iphlpsvc
Kernel-EventTracing
Kernel-Power

# Tracking changes made to GPOs

---

- Things to consider
  - Report on changes per GPO
  - Report on changes per “CSE”
  - Report on “other changes” with GPOs (linking, ACL, etc.)
  - Historical reports showing all changes to a GPO
  - Old and New values of change
  - Real-time alerting of changes (SMS and Email)

---

## Backing up and restoring GPOs and settings





# Backing up GPOs - Microsoft

---

- GPMC
  - Backup all GPOs
  - Backup indiv GPOs
  - Stored in folder of your choice
- Automation of GPO backups
  - GPMC scripts
  - PowerShell

# Restoring GPOs and settings - Microsoft

---

- GPMC and PowerShell
  - Restore entire GPO
    - Any new settings are not available
    - Any old settings will be restored

# GPO recovery - Microsoft

---

- Microsoft can only deal with entire GPO and all settings
- There is no change monitoring
  - No indication regarding what changed in GPO
  - No alerting that GPO changed
- Need
  - Notification when GPO changes
  - Details on what changed in GPO
  - Ability to restore individual settings in GPO
  - Ability to restore GPO to point in time
    - Indiv settings
    - Entire GPO

# GPO Recovery – RecoveryManager Plus

---

- No need to automate GPO backups
- GPO changes are obtained from transaction log
- Ability to see all changes to all GPOs
  - Changes
  - Deletions
  
- Ability to restore GPO
  - See history of changes
  - Select setting that needs to be restored

# Summary

---

- Tracking changes made to Group Policy Objects (GPOs)
- Backing up and restoring GPOs and settings

ManageEngine

Thank you!

---

Derek Melber

[derek@manageengine.com](mailto:derek@manageengine.com)

