CionSystems

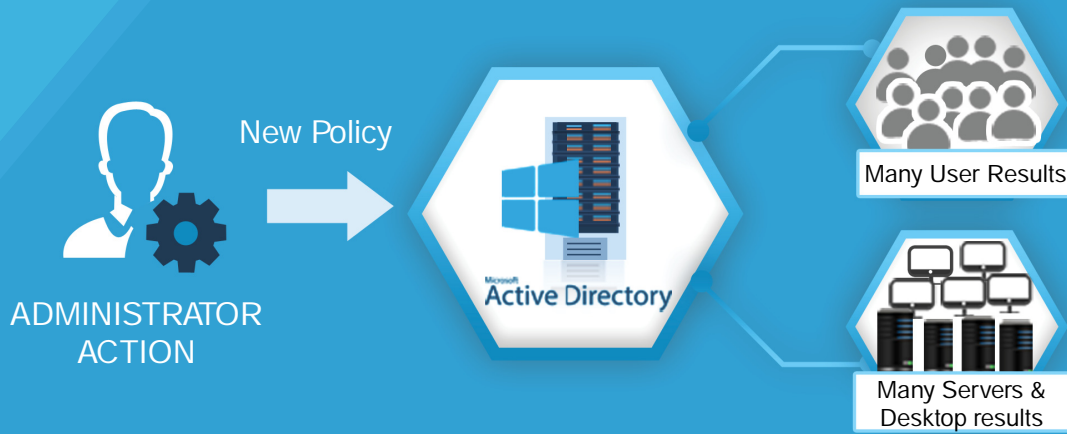## The Easiest, Most Efficient way to Manage your

Organization's Active Directory Group Policies

> Version Comparisons

> Approval-based workflow

> Check in/Checkout

> Backup/restore

> Reports

> Rollback

> Delegation

CionSystems GPO Manager provides a robust Microsoft Management Console (MMC) snap-in that dramatically improves the ability of administrators to manage GPOs.

Zubair@cionsystems.com

(425) 605-5325 Ext. 52

Mobile: (206) 437-1655

International: (425) 605-5325

Fax: (425) 605-5325

https://www.cionmfa.com/

ADMINISTRATOR ACTION

New Policy

Microsoft Active Directory

Many User Results

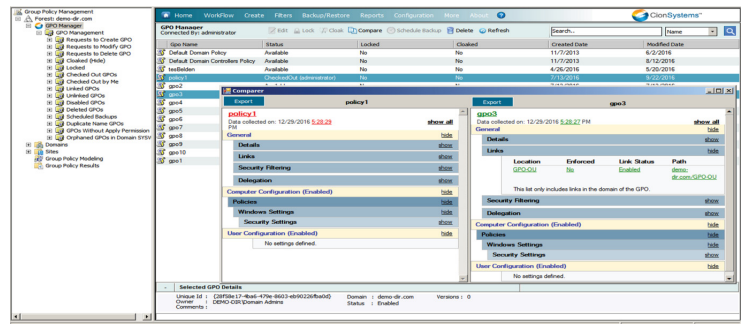Many Servers & Desktop results

Group Policy allows users administrators to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory service containers: sites, domains, or organizational units (OUs).

GPO Manager

Group Policy Objects (GPOs) are constructs that are stored within Active Directory that allow IT administrators to control a wide variety of security settings and access permissions. Examples of how GPOs are typically used include:

- Password policies
- Allowed logon hours
- What software is allowed on laptops or workstations
- Ability to read-write-update directory data
- File and printer permissions
- Centralized view of tiered and delegated GPOs
- Workflow management for policy approval
- Policy check in and check out to help manage version control and inadvertent changes
- Change control and rollback
- Backup and restore
- Built-in reports
- Helps prove compliance to ITIL, MOF, SOX, Base I II, HIPAA and C-198

Group Policy allows users administrators to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory service containers: sites, domains, or organizational units (OUs).

Why you need it

CionSystems GPO Manager offers a mechanism to control this highly important component of Active Directory. GPOs, Scope of Management links, and WMI filters are backed up in a secure, distributed manner and then placed under version control.

- Security issues are critical in any Enterprise, easily harden security with GPO Manager
- Protect enterprise by protecting and enforcing secure GPO authoring process
- Easily control manage and un-manage group policy changes
- Preconfigured template policies for many different applications hardening and pre-configure the application settings.
- Leverages, complements and extends native Microsoft technology, including Group Policy Management Console (GPMC), to strengthen infrastructure investments
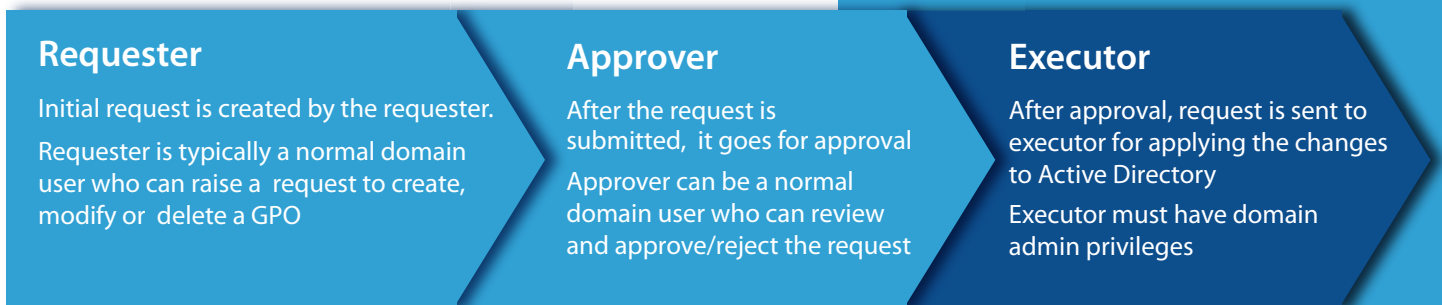
What problem does it solve

- Simplifies and automates critical tasks, reduces outages by eliminating manual process and scripts
- Helps prove compliance to ITIL, MOF, SOX, Basel II, HIPAA and C-198.
- Improves availability and disaster recovery via backup and rollback capabilities.
- Simplifies the enforcement of enterprise-wide business policies by enabling streamlined GPO control via workflow.
- Simplifies and improves network security by restricting access to production GPOs.
- Gives Active Directory administrators and security personnel's control of GPO changes, to eliminate system outages and security exposures
- Allows administrators to edit and test GPOs and have them approved before they are deployed
- Archives all GPO settings

DATA PROTECTION at backup & restore

What feature does it offer

- **Version Comparisons**: Quickly verify setting consistency and improve GPO auditing with advanced, side-by-side GPO version comparisons at different intervals.
- **Enhanced Group Policy Comparison:** And side-by-side two distinct GPO'S, two Versions and with Existing GPO with a Checkout copy GPO comparisons to verify setting consistency.
- **GPO History and Compare:** To record all changes to GPO's
- **Delete version history:** To manage and reduce size of backup store
- **Undo GPO changes:** Rolled back to previous versions.
- **Approval-based workflow:** Process to ensure that changes adhere to change management best practices before their deployment.
- **Scheduling:** Enable approved changes to be implemented immediately or on a schedule.
- **Replication:** To replicate the data among the Available domain controllers.
- **Delegation:** To grant Permission for Users to create GPO. To Apply WMI Filter.
- **Grant Permission on All GPO's:** To grant permission for users on all GPO's to read, Edit, delete.

Configure workflow

GPO Manager Workflow

Requester
Initial request is created by the requester.

Requester is typically a normal domain user who can raise a request to create, modify or delete a GPO

Approver
After the request is submitted, it goes for approval

Approver can be a normal domain user who can review and approve/reject the request

Executor
After approval, request is sent to executor for applying the changes to Active Directory

Executor must have domain admin privileges