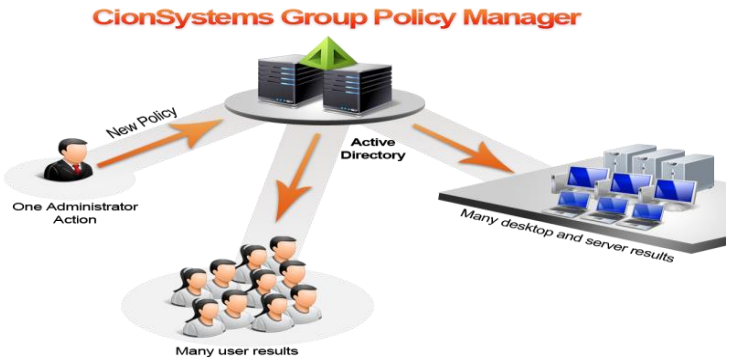
Group Policy Manager

Quick start Guide



Software version 3.0.0.1

CionSystems

General Information: info@cionsystems.com

Online Support: support@cionsystems.com

CionSystems Inc.
6640 185th Ave NE
Redmond, WA-98052, USA
http://www.CionSystems.com
Phone: +1.425.605.5325

Trademarks

Contents

Overview

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 directory service containers: sites, domains, or organizational units (OUs). The settings within GPOs are then evaluated by the affected targets, using the hierarchical nature of Active Directory. By using Group Policy, users can define the state of someone's work environment once, and then rely on Windows Server 2000/2003/2008/2012 to continually force the Group Policy settings applied across an entire organization or to specific groups of people and computers.

As security issues are becoming paramount within any organizations. Within Active Directory (AD), the Group Policy Objects (GPOs) are at the forefront of an organization's ability to roll out and control functional security. Core aspects of user life cycle such as password policies, logon hours, software distribution, and other critical security settings are handled through GPOs. It is paramount for Organizations to have proper methods to control the settings of these GPOs and to deploy GPOs in a meaningful and safe manner with confidence, easily backup and restore GPOs when they are either incorrectly updated or corrupt.

Windows Group Policy is powerful and allows user centralized management. However, uncontrolled and unintentional changes can have disastrous consequences. For example, unintended effects of a GPO change could stop hundreds of users from logging on, exclude access to critical software applications, or expose system settings. The Group Policy Management Console (GPMC) from Microsoft is a useful tool for the individual administrator, but additional functionality—such as GPO workflow management, check in/check out, change control, backup/restore, reports and rollback—is needed to effectively manage GPOs across the enterprise.

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. GPO Manager offers following benefits and more:

- Gives Active Directory administrators and security personnel 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
- Provides a way to quickly roll back changes
- Archives all GPO settings
- Leverages, complements and extends native Microsoft technology, including Group Policy Management Console (GPMC), to strengthen infrastructure investments

Highlights of the product

- **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.
- **Configure workflow**: to enable organizational requirements and set for specified users or groups on edit settings, cloak and uncloak and lock and unlock.
- **Workflow Commenting:** Track the request, review and approval process with comments and e-mail notifications at any stage.
- **Scheduling:** Enable approved changes to be implemented immediately or on a schedule.
- **Microsoft Group Policy Management Console** (GPMC) for familiar look and feel.
- **Cloaking:** Hidden pre-production GPS from all but selected administrators.
- **GPO check-in** and check-out to prevent simultaneous editing conflicts.
- **GPO locking:** to prevent unwanted changes to product GPOs.
- **Backup and Restore:** Schedules the ALL GPO's Backup or selected GPO's to be taken at a specified date and time
- **Delegation and permissions management:** Delegates or provide Read, Edit, Apply Permissions on GPO to Users
- **Day to Day task :** Perform common GPO Actions/Tasks like Create , Edit, Delete, Link, Rename ,Backup, Import, Restore GPO, add comments to GPO, View, Enable, Disable
- **Manage security:** Apply Filters to GPO
- **Copy /Paste :** Create a duplicate GPO with same settings
- **Reports:** Creates Report of all GPO'S at a specified Location.
- **Advance Categorizing:** Easily find GPOS that are Linked, Unlinked, Orphaned, Disabled, Deleted etc.
- **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.

System Requirements


CionSystems GPO Manager needs:

- 2 GHz processor
- 4 GB RAM or greater
- 100 MB hard disk space
- Windows Server 2003 Service Pack 2, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows 8 or Windows 7 operating systems
- MMC 3.0

- .NET Framework 3.5 and 4.0
- Microsoft Group Policy Management Console with Service Pack 1 or Remote Server Administration Tools
- System must be domain joined

Backup Repository (Storage Method)

You have the option of choose the following for the location of the physical backup copy of the object versions and other configuration:

 A network share For the majority of deployments, network share is the best approach as it provides a high performance backup store with a minimum of configuration and maintenance overhead.

Installation on Windows Server 2008

- Install .Net framework4.0 (specify from where)?
- Download CionSystems GPO Manager
- Walk through the installation wizard
- After the install the following GPO Manager icon will be added to the desktop

Installation on Windows Server 2012

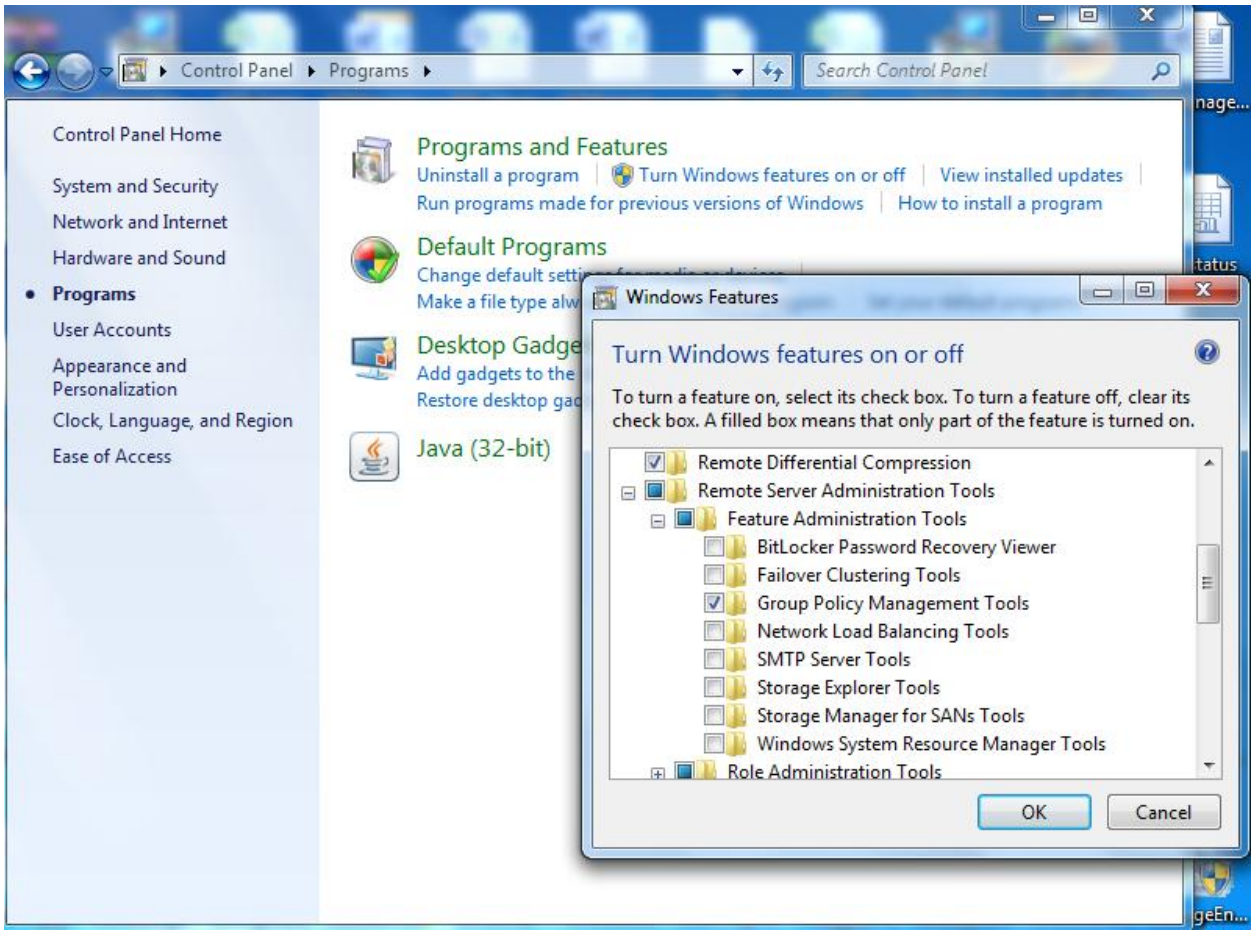
- Install .Net framework4.0 (specify from where)?
- Download CionSystems GPO Manager
- Walk through the installation wizard
- After the install, GPO Manager icon will be added to the desktop

Installation on Windows 8

- Install .Net Framework 4.0
- Download and Install RSAT Tools from site: http://www.microsoft.com/en-us/download/details.aspx?id=7887
- Go to control panel. Click on Programs, click on Turn Windows Features on or off

Installation on Windows 7

- Install .Net Framework 4.0
- Download and Install RSAT Tools from site: http://www.microsoft.com/en-us/download/details.aspx?id=7887
- Go to control panel. Click on Programs, click on Turn Windows Features on or off



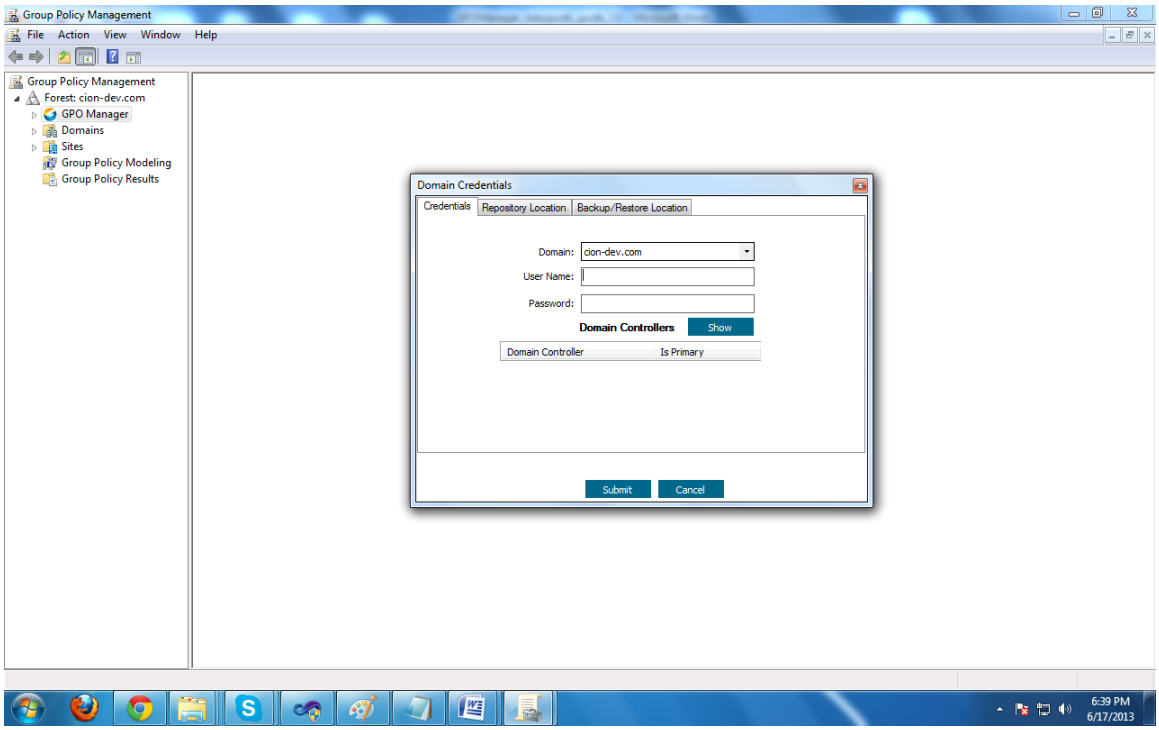
- Select Remote Server Administration Tools; Turn on Group Policy Management Tools. Click on ok
- Download CionSystems GPO Manager
- Walk through the installation wizard
- After the install, GPO Manager icon will be added to the desktop

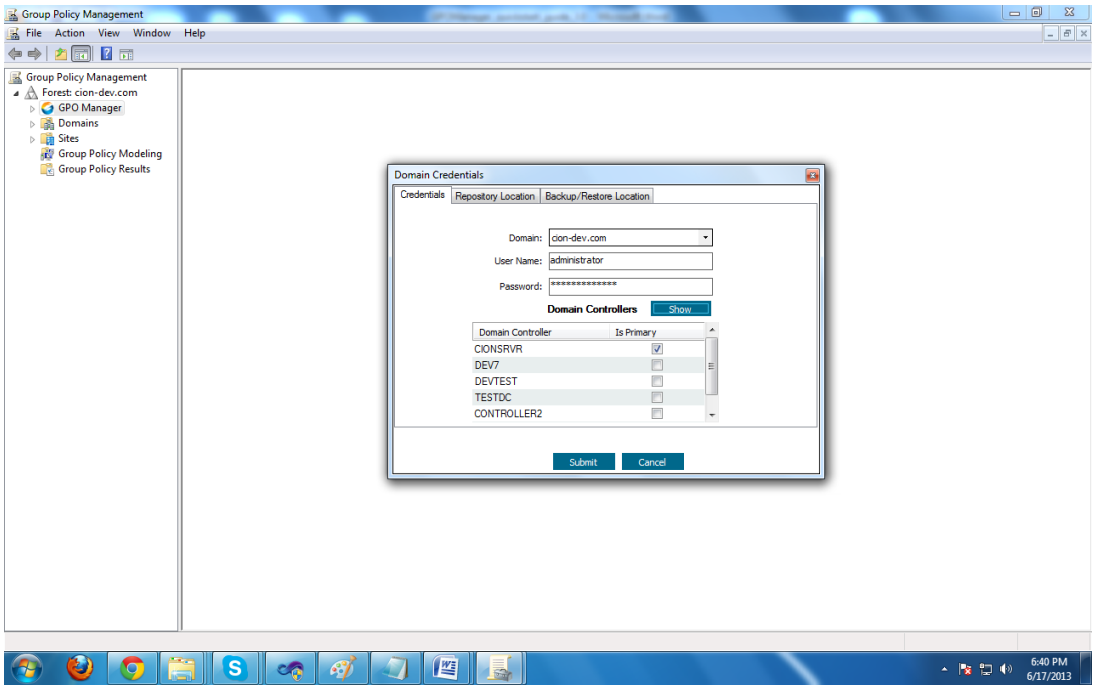
Installation on Windows Server 2003 R2

- Install .Net framework4.0
- Make sure you have Windows Server Service pack 2 installed
- Download and Install GPMC Service pack 1 from site: http://www.microsoft.com/en-us/download/details.aspx?id=21895
- Download and Install MMC3.0 from below site: **http://support.microsoft.com/kb/907265**
- Download CionSystems GPO Manager
- Walk through the installation wizard
- After the install, GPO Manager icon will be added to the desktop

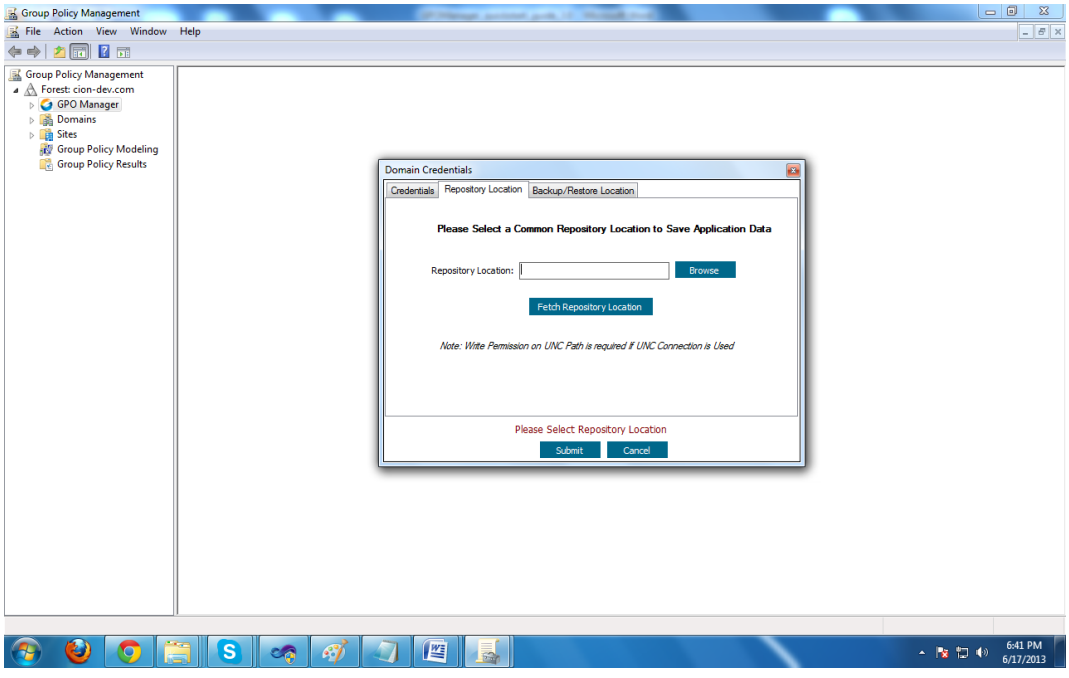
Configuring the Application

Install the CionSystems GPO Manager. Open the application by double clicking on the GPO Manager icon from the desktop. Enter the Credentials and click on Show. From the list of domain controllers, Select One Domain controller as Primary





Next, Select the Repository common location. Select Network location so that it can be accessible from any system joined in the same domain as managed GPO's. Ensure this is a file share and all users of the application have read and write privilege to the shared folder.



Click on Submit.

Note: 1. If you installed the application on other Systems that was joined in Domain (If application is installed on a Domain controller and Repository location is already defined) click on "check" button in Repository location. The Application will show the repository location from the previous installs.

2.If you installed the application on other Systems that was joined in Domain, The user which is use to login to CionSystems GPO Manager must be in Domain Admins Group and must be added into Local Administrators group to the local machine.

Step-By-Step Walkthrough

This step-by-step walkthrough takes you through CionSystems GPO Manager Scenario that includes the following:

- Connect to the Version Repository
- Registering an object/GPO, by attempting to edit
- Check out and edit an object
- Check in the object and request approval. CionSystems GPO Manager provides roles that enable users to perform actions within the GPO Manager work space. The following scenario is created on the assumption that the administrator has already delegated the User and Moderator roles to the required users.

To view the roles applied to a specific container, right-click it, select Properties, and click the Security tab. For complete information on how to create and delegate roles, see "Configuring Role-based Delegation" in the *CionSystems GPO Manager User Guide*.

Add GPO to versioning

Initially all GPOs are unregistered. To add GPOs to the Version Control system, they must be first open for edit and saved. This process forces the system to register the GPO in version control and maintain their GPO status (User and Computer settings enabled or disabled), links, security, and WMI filters.

To add a GPO for version

- Expand **CionSystems GPO Manager**, ensure under **configuration**, the **connect**, **The Repository location and the Backup and Restore location** are defined. Now select the GPO, right click and **Edit** and close the editor.
- *Once objects have been added, they are located in the selected container under the versioning with their initial version number set to 1.0. They are now available to be checked out and edited.*

Check Out and Edit GPOs

Before users can edit registered GPOs, the GPOs must be checked out.

The workflow is as follows:

- Check out the GPO from the system,
- make the required edits, and
- check in the changes to the system.

Version information is updated in the system's history when the GPO is checked back in. Only one person within the system can check out and work on any GPO at a given time.

Checking out a GPO for the first time creates a copy of the original GPO. The copy is an exact duplicate of the original GPO until it passes through the approval process.

To check out a GPO

- Expand the **GPO Manager work space** and select the available GPO.
- Right-click a GPO and select **Check Out**.
- Enter a comment and click **OK**.

Once you have a GPO checked out, you can edit the settings from the Group Policy Management Editor as well as edit the Security and WMI Filter settings. When you check out a GPO, the changes are made to a copy of the live GPO. Those changes do not affect the GPO settings on the network until the changes are checked in and deployed.

To edit a GPO

- Right-click a checked out GPO and select **Edit**.
- Click **Launch Editor** and make the required changes.
- If required, select the **Security** tab and click **Add** or **Remove** to modify the current security filter. Enter or search for the required user, computer, or group, and click **OK**.
- Click the **Advanced** button to select advanced permissions.
- To add or remove a WMI filter, select the **WMI Filter** tab and choose a filter from the list of available WMI filters. Click **OK**.

You now have the option to check in the GPO to be stored for later use or check in and request approval of the changes.

To check in and request approval

- Expand the Version Control Root node and select the checked out GPO.
- Right-click and select Check In.
- Enter a comment and click OK.
- Right-click the GPO and select Request Approval.
- Enter a comment and click OK.

The GPO status will be Pending Approval until the changes are approved or rejected by a user with the appropriate permissions. When the GPO has been approved it is ready to be deployed into the live environment.

Contact Notes:

For technical support or feature requests, please contact us at Support@CionSystems.com or 425.605.5325

For sales or other business inquiries, we can be reached at Sales@CionSystems.com or 425.605.5325

If you'd like to view a complete list of our Active Directory Management solutions, please visit us online at www.CionSystems.com

Disclaimer

The information in this document is provided in connection with CionSystems products. No license, express or implied, to any intellectual property right is granted by this document or in connection with the sale of CionSystems products. EXCEPT AS SET FORTH IN CIONSYSTEMS' LICENSE AGREEMENT FOR THIS PRODUCT, CIONSYSTEMS INC. ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL CIONSYSTEMS INC. BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF CIONSYSTEMS INC. HAS BEEN ADVISED IN WRITING OF THE POSSIBILITY OF SUCH DAMAGES. CionSystems may update this document or the software application without notice.

CionSystems Inc

6640 185th Ave NE,

Redmond, WA-98052, USA

www.CionSystems.com

Ph: +1.425.605.5325

This guide is provided for informational purposes only, and the contents may not be reproduced or transmitted in any form or by any means without our written permission.

