Dell™ GPOADmin™ 5.9

User Guide

If you have any questions regarding your potential use of this material, contact:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (software.dell.com) for regional and international office information.

Trademarks

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

GPOADmin User Guide
Updated - June 2015
Software Version - 5.9

Contents

1

Introducing Dell™ GPOADmin™

- GPOADmin overview
- GPOADmin features
- Client/server architecture
- Multi-forest support
- Group Policy Management Console extension
- Version control
- Change approval process
- Role-based delegation
- Notification system
- GPO ACL editor
- Reporting options
- Templates
- Customized views
- Offline GPO testing
- Custom workflow actions
- GPOADmin Dashboard

GPOADmin overview

Security issues are becoming paramount within organizations. Within Active Directory®, Group Policy Objects (GPOs) are at the forefront of an organization's ability to roll out and maintain functional security. Core aspects such as password policies, logon hours, software distribution, and other crucial security settings are handled through GPOs. Organizations need methods to control the settings of these GPOs and to deploy GPOs in a meaningful and safe manner with confidence. Since GPOs are so important to the proper operating of the Active Directory®, organizations also need methods to restore GPOs when they are either incorrectly updated or have become corrupt.

Dell GPOADmin offers a mechanism to control this highly important component of Active Directory. First, GPOs are backed up in a secure manner, then placed under version control. When changes are made, a backup of the GPO is again made. Changes are managed from the Version Control system, and approvals for any changes are required. Stored GPOs can be retrieved if the current GPO in the directory is not valid for any reason. This means that GPOs are managed and deployed with a secure rollback capability. When an issue does arise, the time between the discovery of the issue and its resolution is kept to a minimum, because a previous version of the GPO can be restored.

GPO implementation is a key consideration when planning your organization’s Active Directory structure, because it streamlines management of all user, computer, and configuration issues, ensuring the smooth day-to-day operation of the network.

You can use GPOs to control specific configurations applied to users and computers through policy settings. When grouped together, the policy settings form a single GPO, which you can then apply to sites, domains, and OUs.

You can define settings for users and computers and then rely on the system to enforce the policies. GPOs provide the following types of policies:

- Computer configuration policies, such as security and application settings, which are applied when the operating system is initialized.
- User configuration policies, such as desktop settings, security settings, logon and logoff scripts, which are applied when users log on to the computer.
- Registry-based policies, such as administrative templates.

GPOADmin features

Group policy version control is crucial to an organization's efforts to safeguard continual operation. GPOs can have a negative impact on users' ability to access the network and resources they need to work efficiently.

Dell GPOADmin allows administrators to check the current status of a GPO, back up changes into a common data repository, and report on that repository as required. If a GPO has become corrupt or is no longer in a working state, any previous iteration of a GPO can be retrieved.

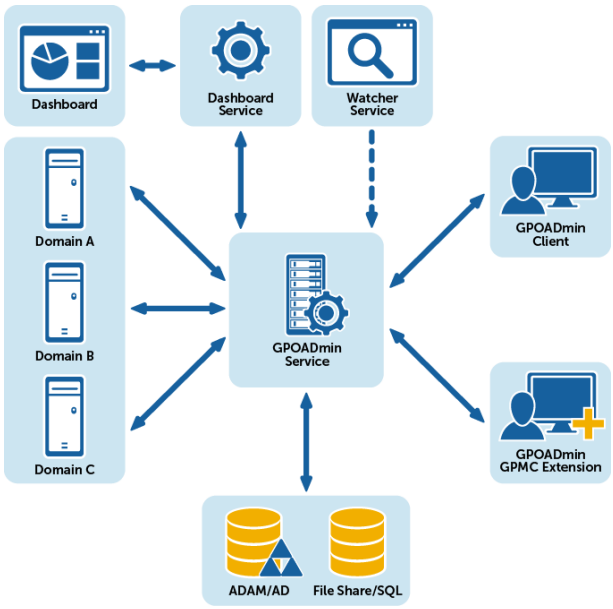


Figure 1. Group Policy Workflow

- Client/server architecture
- Multi-forest support
- Group Policy Management Console extension
- Version control
- Role-based delegation
- Change approval process
- Notification system
- GPO ACL editor
- Reporting options
- Templates
- Customized views
- Offline GPO testing
- Custom workflow actions
- GPOADmin Dashboard

Client/server architecture

The client/server architecture facilitates granular security and delegation. GPOADmin runs under the security context of a privileged service account that must have full access to GPOs in the managed forest.

This architecture allows for multiple servers to be installed within the same forest, providing the ability to manage domains independently.

Clients can connect to any deployed server within any Active Directory® forest. GPOADmin maintains a most recently used (MRU) list of servers to which the users have previously connected to facilitate quick subsequent server connections.

NOTE: For more information on Permissions required for the Service Account, see the Dell GPOADmin Quick Start Guide.

Multi-forest support

The GPOADmin management console allows you to connect to multiple GPOADmin Server Service instances within the same console. The GPOADmin Server Service could be from a trusted or non-trusted domain/forest. You now have the option to provide credentials for all non-trusted domains/forests while connecting to the non-trusted environments. By enumerating all GPOADmin Server Service instances, you can manage all Version Control systems from a single console, thus making it much easier to transition GPOs from a test environment to production.

NOTE: **Known Limitations of Managing objects in an untrusted domain**

Although not recommended, if you plan to manage GPOs in an untrusted domain from your local client console, the following limitations must be considered:

- File and directory browsing is performed locally on the client computer.
- Users and groups can only be selected from the client domain and trusted domains.
- Domain specific information of work-flow enabled Group Policy Objects cannot be set.
- Internet Protocol Security (IPSec) will not load in the Group Policy editor when editing a work-flow enabled Group Policy Object.
- Workflow disabled Group Policy Objects cannot be edited.
- Workflow disabled Group Policy Objects cannot be copied.
- Workflow disabled Group Policy Objects cannot be renamed.
- Objects cannot be exported to the Live Environment of an untrusted domain.
- Objects cannot be imported from the Live Environment of an untrusted domain.

Group Policy Management Console extension

You can work in the Group Policy Management Console (GPMC) to perform many GPO related tasks. GPOADmin comes with two interfaces — the GPOADmin Console, and the GPMC Extension. The console provides full functionality, and is intended for administrators responsible for a wide variety of tasks. The GPMC Extension is a convenient tool for users who are already comfortable with the GPMC, or for GPO administrators who do not need the advanced features of the GPOADmin Console.

The following tasks can be performed using the GPMC Extension:

- Create GPOs
- Register/Unregister GPOs
- Create labels
- Cloak and uncloak
- Lock and unlock

- View and edit properties
- View the history
- View the differences between versions
- Roll back a GPO to a previous version
- Check in and out
- Edit
- Request approval
- Approve or reject changes
- Deploy
- Generate Working Copy, Latest Version and Differences reports

For more information, see Using Dell GPOADmin on page 29 and Accessing the GPMC extension on page 31.

Version control

GPOs, WMI filters, templates, and Scopes of Management (domains, sites, and OUs) links can be stored and backed up in a secure AD, ADAM/AD LDS, network share, or SQL repository. Objects that are stored within the Version Control system are labeled with a version number. You can view all changes made to the controlled object through the object history and through numerous reports.

For detailed information, see Registering objects on page 33, Proposing the creation of controlled objects on page 40 and Controlled object reports on page 72.

Change approval process

All changes made within the Version Control system are not rolled out into the online Active Directory® environment until approved and deployed by specifically assigned users.

You can enforce a multi-approval process at the container/object level so that all changes made to the live production environment have been carefully approved by all specified approvers.

The objective of the multi-approval feature is to allow the approval process to rely on the combined agreement of multiple approvers rather than just one. This provides better security to the customer, who can rest assured that many eyes are vetting the process.

Deploying changes within the system is a critical process that affects the live environment. To minimize the impact of disruption, this process should be carried out during a time period when the impact to users is minimal as the changes to the GPO might alter the behavior of particular systems.

To avoid any issues, you can schedule the deployment of the changes for a specific date and time that best suits your needs.

For detailed information, see Approving and rejecting edits on page 57 and Scheduling deployment on page 58.

Role-based delegation

GPOADmin users can create and define roles that consist of a set of rights to perform actions on the Version Control system. These roles can delegate users specific access to resources within the system. GPOADmin includes predefined Built In roles (Moderator, System Administrator, and User), and granular rights users can define through a custom role. For a list of rights, see Configuring role-based delegation on page 19.

For more information, see Configuring the Version Control server on page 14 and Configuring role-based delegation on page 19.

Table 1. Custom rights

Right	Users with this right can...
Version Controlled Object Rights	• Block Inheritance • Cloak/Uncloak • Compliance Action • Create • Delegate Security • Delete • Delete links outside of workflow • Deploy • Edit • Enable/Disable Workflow • Export • Label • Link • Lock/Unlock • Modify Approval Workflow • Modify Keywords • Modify Managed By • Modify Native Security • Read • Register • Synchronize • Undo Check-out • Unregister • View Cloaked
Version Control Container Rights	• Create Subcontainers • Delegate Container Security • Delete Container • Rename Container
Protected Settings Rights	• Block Protected Settings Inheritance • Export Group Policy Objects as Protected Settings Policies • Modify Protected Settings • Modify Protected Settings Assignments • Modify Protected Settings Exclusions

Notification system

GPOADmin contains a rich notification system that allows users to control a wide variety of Version Control events, sending details by email as the events occur.

Users can subscribe to the notification service, which is based on a granular defined event trigger including such actions as Register, Check In, Create, and Delete for each object under the Version Control system. For approve and reject notifications, the email will also include information on who was the last to approve any changes and the date of the last approved change.

Reports are included in notification emails when more details are required. For example, check-in notifications come with a settings report (to show the settings that were just checked in) and a difference report (to show the differences between this version and the last version).

In addition, Administrators can delegate notifications to users who do not use GPOADmin, but who for business reasons, need to be notified when an object is created, modified, or deleted.

For detailed information, see Selecting events on which to be notified on page 22, Adding notifications for users on page 21, and Configuring user preferences on page 32.

GPO ACL editor

A security group, user, or computer must have both Read and Apply Group Policy permissions for a policy to be applied. By default, all users and computers have these permissions for all new GPOs. They inherit these permissions from their membership in the group Authenticated Users. In GPOADmin, aside from changing the Security Filter, you can also manage the permissions of a particular group. For example, if you do not want a GPO to be applied to a group of users you can easily configure the permission on a particular GPO ("Deny Apply Group Policy") so that it is not applied to the group of users.

For more information, see Selecting security, levels of approval, and notification options on page 38.

Reporting options

GPOADmin allows you to configure real-time (for quick regeneration of live data) and historical snapshot report templates. All reports now run asynchronously; therefore, you no longer have to wait until one report has rendered before initiating a new report.

For detailed reporting options, see Creating Reports on page 70.

Templates

As an administrator, you want to ensure that Group Policy settings for your Group Policy Objects are entered correctly and conform to the organization's standards. As your organizations standards change, you will need to re-visit your Group Policy Objects and make the necessary setting changes.

By using Templates you can simplify Group Policy management by creating GPO templates once, then distributing them for reuse. This provides a mechanism to ensure that Group Policy settings are consistent across your Group Policy Objects in your organization.

Templates are a grouping of policy settings that you can apply to existing GPOs or use to create new GPOs. They can be reused in other domains, children of a parent domain or domains in another forest. They can also be distributed across an organization, from central administrators to local administrators in branch offices. The administrators can then create similar GPOs based on the templates or create new GPOs that are the same as corporate policy.

Templates can include the following settings:

- Computer configuration settings, such as security and application settings, which are applied when the operating system is initialized.
- User configuration settings, such as desktop settings, security settings, logon and logoff scripts, which are applied when users log on to the computer.
- Registry-based settings, such as administrative templates.

Templates can be applied only to registered GPOs within the Version Control system. The changes made to a GPO based off of template settings must go through the same approval process as all other changes made to GPOs within the system.

The Dell ADM Editor is included with GPOADmin to help you create and edit ADM files through a user-friendly interface. The ADM files can then be imported into the Version Control system, and can be used by the templates.

NOTE: GPOADmin does not support the use of templates on Windows® 7, Windows Server 2008, and later. The support on earlier Windows operating systems is also limited.

For more information, see Creating templates on page 42, Editing templates on page 63, Applying templates on page 62 and Working with the ADM Editor on page 89.

Customized views

You can organize controlled objects into a user-defined container hierarchy. Each container has its own security descriptor in which trustees can be granted (delegated) roles to define access to the container, subcontainer, or simply a specific GPO within these containers.

Version Control Root Hierarchy should be used for administrator management as a means to organize many objects into a logical view based on their enterprise structure.

The Search folders allow you to quickly view controlled objects based on their state within the Version Control system. Search folders are used as an easy way for users to view the status of objects within the Version Control system.

For more information, see Creating a custom container hierarchy on page 38.

Offline GPO testing

Using the Export Wizard, you can test GPOs offline before implementing them. For more information, see Exporting and importing on page 67.

Custom workflow actions

You can extend GPOADmin's version control system to incorporate customized actions based on your organizations existing workflow. This allows you to customize and control the deployment of controlled objects (such as GPOS, SOMs, and WMI filters) to meet your individual needs. For details, see Appendix: Customizing your workflow on page 115.

GPOADmin Dashboard

The GPOADmin dashboard offers a quick overview of the sate of your GPO deployment and enables you to affect changes where required. For details, see Working with the GPOADmin Dashboard on page 94.

2

Configuring Dell GPOADmin

- Configuring the Version Control server
- Setting permissions on ADAM/AD LDS
- Port requirements
- Editing the Version Control server properties
- Configuring role-based delegation
- Adding notifications for users
- Selecting events on which to be notified
- Creating email templates
- Working with Protected Settings policies

Configuring the Version Control server

You will be required to configure the Version Control server the first time that you connect to it.

To configure the Version Control server

NOTE: Configure the server using the GPOADmin console, even if you intend to use the GPMC Extension.

1. Right-click the **GPOADmin** node and select **Connect To**.
2. Select the required Version Control server and click **Connect** to connect with the current logged on user credentials or select the down arrow in the Connect button and select Connect As to enter new credentials (domain\user and password).
3. To save the credentials, select the **Remember my password** check box and click OK.

   For information on saving connections, see Connecting to the Version Control system on page 30.
4. In the Select a Configuration Store dialog box, select Active Directory® or ADAM/AD LDS for your configuration storage location.

   If you select Active Directory, select the domain controller (DC) to be the Version Control server, and click **Next**.

TIP: The best practice is to use ADAM/AD LDS as the configuration store.

Any DC in any domain of the selected forest can be specified as the version control master. The version control master can be thought of as another FSMO role in the Microsoft® sense (such as Schema master, PDC Emulator, and RID master).

GPOADmin is a directory-enabled application and all of its application information is stored in the configuration container of Active Directory. Because of this, all information is automatically replicated to all other DCs. However, the version control master is the authoritative source for all version control actions required. If it goes offline, users will not be able to perform actions such as check-in a desired group policy object change until the problem has been rectified.

If you select ADAM/AD LDS, enter the NetBIOS name of the computer you are installing to, followed by the port number, in the format: `server_name:port`, and click **Next**.

For example, gpoadmin_svr:389.

NOTE: The username/port/server (but not password) will be cached, so the next time you open the console you will not need to enter this information.

5. In the Select Storage Options dialog box, select where you would like to store the historical backup information.

   Backups can grow to be quite large. Storing these in AD may not be the most optimal configuration in some enterprise environments.

   You have the option of choosing AD, Active Directory Application Mode (ADAM/AD LDS), SQL Server, or a network share.

TIP: The Best Practice is to use a network share as the backup store.

Table 2. Storage Options

Option	If you select this option
Active Directory	Click **Next**.
ADAM/AD LDS	Enter the server and port name, and click **Next**. For more information on an ADAM/AD LDS deployment, see Setting permissions on ADAM/AD LDS on page 15.

Table 2. Storage Options

Option	If you select this option
SQL Server	Enter the server name and the required authentication information, and click **Next**. NOTE: If the server is installed as a unique instance, it must be specified as servername\instancename rather than just the SQL Server name.
Network Share	Browse to and select the required network share or directory, and click **Next**.

6 Select which users will have the right to connect to and administer the Version Control server, and click **Next**.

7 Click **Finish**.

Now that the system has been configured, users can connect to and use the Version Control features.

NOTE: Users with the appropriate rights can modify the server settings at anytime by right-clicking the GPOADmin node and selecting Server Properties.

Setting permissions on ADAM/AD LDS

To use GPOADmin with an ADAM/AD LDS deployment, users must be assigned the Administrators role.

To set permissions on ADAM/AD LDS

1 Open ADSI-Edit (ADSI-Edit is installed as part of the ADAM/AD LDS tools.)

2 Connect to the configuration naming context and browse to the roles container.

3 To grant the user rights, right-click the **Administrators** role and select **Properties**.

4 Browse to the member attribute and click **Edit**.

5 Add the service account to the selected role.

NOTE: If required, you can use the ADAM/AD LDS support tool dsacls.exe to fine-tune the rights given by these roles or to grant specific rights to users.

Port requirements

CAUTION: **It is recommended to conduct a thorough threat analysis before opening these services to an untrusted network.**

The following ports must be open for the application to function correctly:

Name resolution can be achieved using DNS on port 53 or WINS (downlevel) on port 137.

Between the client and the GPOADmin Server:

- Inbound: Port 40200 (default)
- Outbound: TCP ports within the following range (1024-65535). For more details on default dynamic port range for TCP/IP see https://support.microsoft.com/en-us/kb/929851.)

NOTE: To run the Version Control server on a custom port, you must set the following registry value:

Key: HKLM/Software/Quest Software/Quest Group Policy Manager/Remoting
Value Name: Port
Value Type: DWord
Valid Values: 1-65536

If this value is not set, the default (port 40200) will be used.

From the GPOADmin Server:

Configuration storage

- LDAP Service - TCP/UDP - 389 -or- ADAM/AD LDS port (defaults to 389 or 50000)

GPO Archives

- If you are using a network share for GPO backup storage, you may require open ports on 135, 136, 138, 139, and/or 445.
- If you are using SQL Server for GPO backup storage, the appropriate ports will need to be open. SQL Server's default port is 1433 or 1533 if the "hide server" option is enabled.
- If you are using Named Pipes with SQL, arbitrary ports may be required. SQL Named Pipes is not a recommended configuration through firewalls.
- If you are using ADAM/AD LDS for GPO backup storage or configuration data, ADAM/AD LDS will default to port 389 if not coexisting with AD. If AD is already installed, ADAM/AD LDS will default to port 50000.

Editing the Version Control server properties

Users that are logged on with an account that is a member of the GPOADmin administrators group can edit the properties of the Version Control server when required. These properties include the directory server, where the GPO backups are stored, roles used to define security within the system, SMTP settings and the access to edit these settings, logging, preferred domain controller, mandatory comments, naming conventions, and license options.

To edit the Version Control Server configuration

NOTE: You must use the GPOADmin console to edit server configuration, not the GPMC Extension.

1. Right-click the forest, and select **Properties**.
2. Select the **Access** tab to add and remove users who can connect to and alter the server options.

   From here you can also add and remove users who can simply connect to the Version Control server.
3. Select the **Storage** tab to change the required storage options (Active Directory®, ADAM/AD LDS, SQL, or shared folder).
4. Select the **Roles** tab to create and edit roles that will be used to delegate rights over the Version Control system.

   The built in roles are displayed. You can easily see the permissions contained within each by selecting the role and clicking the **View Role** button. You cannot alter predefined roles.

   For complete information on creating and delegating roles, see Configuring role-based delegation on page 19.

5 Select the **SMTP** tab to change the global SMTP notification options.

NOTE: Users can alter the email address for their notification email through their personal settings, or through the Notification Manager. For more information see Configuring user preferences on page 32 or Selecting events on which to be notified on page 22.

6 If you would like the ability to have changes approved and rejected through email, select the **Enable workflow approval through email** option.

NOTE:

- This option requires at a minimum Microsoft® Exchange 2010 and all approvers and the service account must have a valid Exchange Inbox. Distribution lists should be used for approval groups.
- Ensure that the proper Exchange certificates are installed on the GPOADmin server if certificates are being used in your Exchange environment.
- You must restart the GPOADmin service when you enable or disable this option.

By default, GPOADmin will use the service accounts mailbox. If required, you can specify the mailbox and Exchange Server that you want to use to process the approvals/rejections through email.

To do so, uncheck the **Use the service accounts mailbox** option. Enter the mailbox that you want to connect to, the account to use to connect to it, and the password for the account.

NOTE: To connect as the service, leave the account blank and password blank.

Enter the Exchange Server Url or select **Autodiscover Exchange Server Url** to locate the Exchange server that is hosting the specified mailbox.

Once you have entered all the required information, click **OK**.

7 Click the **Logging** tab and select the log location and the type of information you want to track.

You can choose to log to the Event Log, to a specific directory where log files will be created, or not at all.

You can also select which (if any) types of events to log. The types of events are as follows: Service Actions (such as service startup and shutdown), User Actions (such as check in, approve, edit), Errors, and Debug Information (used by Dell support personnel).

8 Select the **Options** tab, and click **Add** to choose the domain controller that GPOADMin will use for all Active Directory actions.

By default, GPOADmin uses the Primary Domain Controller.

9 If you want to make comments on actions mandatory, click the **Options** tab, select the **Comments** check box, and set a minimum comment length greater than 0.

Leaving the value at 0 means comments are optional for all actions. Any value greater than zero makes comments mandatory for all actions and all users.

10 To enforce naming conventions for newly created objects, select the **Enforce Naming Standards** option. Select to apply the conventions to GPOs and/or WMI filters, and enter the pattern that you want to use.

NOTE: Example rule

^[a-z]+[0-9]+_GPO$

The caret character (^) means the start of the line.
The grouping [a-z]+ means at least one or more lower-case characters between a and z.
The grouping [0-9]+ means at least one or more numeric characters between 0 and 9.
The dollar sign character ($) means the end of the line.

This rule states that from the start of the line there must be at least one or more lower-case character immediately followed by at least one or more numeric character immediately followed by the literal string "_GPO" and nothing after that.

a1_GPO will pass
abc123_GPO will pass
_a1_GPO will fail
a1_GPO_ will fail
A1_GPO will fail
A1_gpo will fail

You can test your rule, by entering a name that conforms to your desired naming standard and selecting **Verify**. If you validate the rule here, users will see both the rule and your sample text if they try to use a non-conforming name.

If you receive a green check, then the name you entered is allowed and your rule is running as desired. If you receive a red X, then the name you entered failed the verification. You should adjust the rule to allow the name to pass or adjust the name to match the rule.

Once you are satisfied with the rule, select **Apply**. Users will now be forced to use names that adhere to your organization's standards. If they enter a name that does not comply, they will see the rule details that they must comply with.

11 To ensure that GPOs and WMI filters cannot be created with the same name as an existing GPOs or WMI filter in a domain, select the **Enforce Unique Names** option. If a non-deployed GPO indicates that a duplicate name exists, run a full compliance check to determine if any GPOs were modified outside of GPOADmin. For more info see, Checking compliance on page 59.

12 Click the **License** tab to view the current license information.

Select the **Update License** option, browse to the new license location and click **OK**.

13 If you have multiple Change Auditor™ coordinators installed, you can click the **Change Auditor™** tab to select a specific coordinator to use for reports and auditing.

If required, you can also select to turn off Change Auditor, by selecting **Not Set**.

14 When you have made all the required selections, click **OK**.

Configuring role-based delegation

NOTE:

- The predefined roles cannot be altered.
- You must perform all role-related tasks in the GPOADmin console.
- When using the Link right, you must have Link right on the GPO and the SOM.

GPOADmin Administrators can create custom roles that can be applied to specific users to allow them to perform certain functions within the Version Control system. For more information on users with permissions to create roles see Configuring the Version Control server on page 14.

Table 3. Roles and rights

Role	Rights included in the role
System Administrator	System Administrators can perform any action in the Version Control system. Version Controlled Object Rights include: • Block Inheritance • Cloak/Uncloak • Compliance Action • Create • Delegate Security • Delete • Delete links outside of workflow • Deploy • Edit • Enable/Disable Workflow • Export • Label • Link • Lock/Unlock • Modify Approval Workflow • Modify Keywords • Modify Managed By • Modify Native Security • Read • Register • Synchronize • Undo Check-out • Unregister • View Cloaked

Role	Rights included in the role
System Administrator (continued)	Version Control Container Rights include: • Create Subcontainers • Delegate Container Security • Delete Container • Rename Container Protected Settings Rights include: • Block Protected Settings Inheritance • Export Group Policy Objects as Protected Settings Policies • Modify Protected Settings • Modify Protected Settings Assignments • Modify Protected Settings Exclusions
Moderator	Moderator (Moderators can perform every action a user can, plus undoing check outs from other users and running the compliance wizard.) They can also: • Create • Delete • Edit • Export • Label • Read • Undo Check Out
User	User (Users can perform all the basic actions of the Version Control system, such as check in, check out, edit, applying templates, and so on.) They can also: • Create • Delete • Edit • Export • Label • Read

Creating Roles

You can easily create new roles with any of the customized rights.

To create a new role

NOTE: You must use the GPOADmin console to create roles, not the GPMC Extension.

1. Right-click the forest, and select **Properties**.
2. Select the **Roles** tab.
3. Click **Add New Role**.
4. Enter a name and description for the role, and click **Next**.

   You have the option to create a new role that is based on an existing role. (To see which rights are assigned to a particular role, hover the cursor over it.)
5. Select the role or roles you want to copy and click **Next**.

If you want to create the role from scratch, simply do not select an existing role before clicking **Next**.

6 Select the rights that you want included in the role, and click **Finish**.

Editing roles

To edit roles

NOTE: You must use the GPOADmin console to edit roles, not the GPMC Extension.

1 Right-click the forest node, and select **Properties**.

2 Select the **Roles** tab.

3 Select the role that you want to edit and click **Edit Role**.

4 Make the required changes and click **OK**.

5 Click **OK** again to apply the changes.

Delegating roles

Once the required roles are in place, GPOADmin Administrators can begin to delegate the security over containers and GPOs to specific users and groups.

To delegate rights on the Version Control system through roles

NOTE: You must use the GPOADmin console to delegate roles, not the GPMC Extension.

1 Right-click the Version Control Root node, required container or object, and select **Properties**.

2 Select the **Security** tab.

3 Click **Add** to select the users and groups to which you want to apply the role.

4 Select the role that you want to apply and click **OK**.

The specified users will now have the specified rights included in the assigned role over the selected container or object.

Adding notifications for users

An administrator can add notifications for multiple users. Such users may never login to GPOADmin, but for business reasons, may need to be notified when an object is created, modified, or deleted.

Administrators can also copy notification settings from one user to other users or merge new notification settings with existing ones.

To add notifications

1 Right-click the **Forest** node and select **Notification Manager**.

2 Select the container you wish to set notifications on.

3 Under the Notifications menu, select **Add Subscribers**.

4 If there are no users listed, you can add either an Administrator or a User by selecting **Add Administrator** or **Add User**.

5 Select the check box next to the user and click **OK**.

6 You can have the application attempt to discover the user's email address by clicking the **Autodiscover email address** button.

   If the application fails to discover the user's email, or you would like to redirect it, type the email address in the Email box and click **Set**.

7 Click **OK**.

8 In the Notification Manager window, select the user and then under the Notifications menu, select **Set Notifications**.

NOTE: A newly added user will not be retained until you assign notifications for that user.

9 Select the actions for which you would like to have the user notified and click **OK**.

To paste and merge notification settings

1 In the Notification Manager window, right-click the name of the user from which you want to copy notifications and select **Copy Notifications**.

2 Select the target user or group of users and do one of the following:

   To paste notifications, select **Paste Notifications**.

   Pasting will overwrite the target user's existing notifications.

   To merge the copied notifications with the target user's existing notifications, select **Merge Notifications**.

Selecting events on which to be notified

Using the notification option you can set up a mechanism where you will receive an email each time a specified action is performed within the Version Control system.

To set up notification

1 Navigate to the version controlled object for which you want to be notified.

2 Right-click the object and select **Properties**.

3 Select the **Notifications** tab.

4 Select the events that you want to be notified about, and click **OK**.

   A notification email will now be sent when the specified events take place on (and beneath, in the case of a container) the selected object.

NOTE: To setup the email address for the notification messages, see Configuring user preferences on page 32 or Adding notifications for users on page 21.

Creating email templates

You can create a customize email template for notifications or email requests (provided that this option is enabled, see Configuring the Version Control server for details) and associate it with specific roles. This allows you to standardize the information that is presented to users based on their role within your organization.

You can also choose to include attachments for specified version control actions. For example, you can easily include forms used to track change requests in an external system, risk assessment check list, or logs in the email.

NOTE: Administration accounts must be explicitly added to the GPOADmin Administrators group in order for the email template assigned to the System Administrator Role to be used when sending notification to an administrator. You can set this option through the Access tab in the Version Control properties.

GPOADmin includes a sample template (DefaultNotificationTemplate.html) in the server installation directory. This file should not be moved or modified; however, you can use it as a basis for the creation of new templates.

To select an email template for an existing role

1. Open the Server Properties.
2. Select the **Roles** tab, select the required role, and click **View Role**.
3. Select the **Email Template** tab.
4. Click **Browse** to select the template to use for the selected role.

   By default, the DefaultNotificationTemplate.html in the server install directory will be used by the notification system if the specified custom template cannot be found.

   If there are no templates displayed, click **Add** and browse to where the templates are located. The default template is located at C:\Program Files\Dell\GPOADmin.
5. Select the template and click **OK**.
6. Select the cost for this template.

   If a user is a member of two or more roles which have subscribed to the same notification, the email template associated with the role with the lowest cost will be the one used for that user.

   For example, User A has subscribed to all event on Version Control Root. He is a member of the Moderators role set on the Version Control Root container and a member of the Administrators Role set on a child container. When a version controlled object is Checked-Out in the child container a notification will be send to him. GPOADmin determines that user A is a member of two roles. The cost that you have applied to the role will tell the system which template to use when sending the notification. If the Moderators role has a lowest cost than the cost associated with the Administrators role, then the template associated with the Moderators role will be used.
7. If required, click **Add** to select an attachment to include in the email.
8. Select the action that will trigger the attachment inclusion from the list.
9. Select the attachment to include by entering its location or browsing to it.

   NOTE: You can optionally use any GPOADmin predefined tag in this field.

   If desired, you can use keywords to further control the inclusion of attachments. It would only be included if the specified keywords are present in the list of keywords on the version controlled object.

   Enter, enable, disable keywords as required. (Check an existing keyword to have it associated with this attachment and click to clear the keyword to exclude it.)

   NOTE: Any attachment with an empty keyword list would always be included for the associated action.
10. Click **OK**.
11. Click **Apply** to associate the template.

Working with Protected Settings policies

Protected Settings policies contain settings that you want to control. They are protected in the sense that they contain and identify the settings that may not be altered by users. This provides an added level of security for the policies within your organization. If a user attempts to create, edit, or remove the flagged settings they will be stopped.

Protected Settings are identified by examining the difference report between the Protected Settings policies and the Group Policy Object being checked in. The difference is produced by using the Difference Engine in GPOADmin. Once this is completed, the protected setting function searches the difference report for matches based on the specified validation mode.

Protected Settings policies have a modified workflow and follow the typical check-out, edit, and check-in process. As with any other object, when you are ready to make the newly created Protected Settings policy active or edit an existing policy, a request approval action must be initiated.

Once the approval is granted, the Protected Settings policy will be available for use.

NOTE: These policies differ from other GPOs in that they are not deployed to the environment.

Protected settings must be:

- Enabled within the domain
- Created with the selected settings
- Applied to the required container within GPOADmin

To enable Protected Settings for Group Policy Objects

1. Right-click the forest and select **Properties**.
2. Select the **Options** tab.
3. Select **Enable Protected Settings for Group Policy Objects**.
4. Click **Apply** or **OK**.

   A new Protected Settings container is created to store and manage the Protected Settings policies deployed within your environment.

Rights and role for Protected Settings for GPOs

The Protected Settings for GPOs requires the following rights to control the actions of the Protected Settings tab on containers and provide the ability to export GPOs to create protected settings:

- Block Protected Settings Inheritance
- Export Group Policy Objects as Protected Settings Policies
- Modify Protected Settings Assignments
- Modify Protected Settings Exclusions

NOTE: These rights are not available until the Protected Settings for Group Policy Objects is enabled through the server properties. See Working with Protected Settings policies on page 23.

These rights are automatically assigned to the System Administrator role when Protected Settings are enabled. No other roles, built-in or otherwise, are given the Protected Settings rights. They must be assigned.

IMPORTANT: Built-in roles cannot be modified, so if users require these rights then a new role must be created.

To create and assign the required role to the user responsible for managing containers and controlling the settings on the Protected Settings tab for containers

1. Create a new role called **Prot_All** and assign rights listed above as well as the **Read** right to this role. No other rights need to be given to this Role.
2. Right-click the **Protected Setting** container, and select the **Security** tab. Click **Add** and add the user who is going to manage the container. Give them the **Prot_All** role. Do not give them any other roles to the Protected Settings container. Select **OK** to apply the security changes.
3. Right-click the container that the user is to manage, and select **Properties**.
4. Select the **Security** tab, and click **Add** to add the user account. Give them the **User (built-in)** and the **Prot_All** roles. Click **Apply** and **OK**.

   The user account now has the necessary rights to make all the required changes to the container.

To review why the above roles were created and assigned consider the following:

- The Prot_All role gives the user the necessary rights to perform any of the Protected Settings functions and because they has the Read right, the user can see what is in the Protected Settings container but cannot change or add anything to the container. The ability to Read is needed so the user can assign a Protected Settings policy to a container or any sub containers being managed.
- The User role is also given so he user can do the normal actions such as create, check out, edit, and check in a GPO in the container. The role Prot_All has the right, Export Group Policy Objects as Protected Settings policies. The user also needs the Create right which is part of the built-in User role.

Securing protected settings

Protected Settings policies can be further controlled by delegating who has permission to modify protected settings. To secure the protected settings, you can assign a role (that contains the "Modify Protected Settings" right) to a user on the Protected Settings policy. If during the validation process, GPOADmin determines the current user possess this right, the associated Protected Settings policy will be excluded from the validation allowing the modification of those protected settings to proceed.

Create a Protected Settings policy

Once the ability to use Protected Settings has been enabled, you can create the policies using one of the following methods:

- Create a policy directly from the Protected Settings container.
- Export a GPO to the Protected Settings container.
- Drag and drop a GPO onto the Protected Settings container.

To create Protected Settings Policy from the Protected Settings container

1. Select the **Protected Settings** container in the tree view.
2. Right-click and select **New | New Protected Settings Policy**.
3. Enter a name for the policy. It is recommended to use a naming convention that will set these GPOs apart from other GPOs and make them easily identifiable as protected. For example, PROT_01.
4. Select the domain that the Protected Settings policy will be related to and click **Next**.
5. Select a template to apply, if applicable, and click **Next**.
6. In the Settings page, edit the policy and configure the setting you want to protect.

   NOTE: You can elect to configure the settings at a later date.

7. Click **Finish**.

   The policy is identified as a Protected Setting Policy type and has the same icon as the Protected Settings container.

   At this point, the Protected Settings policy is checked out and has a version of 0.0.

   Protected Settings policies have a modified workflow and therefore require workflow processing such as requesting approval during creation.

To export a GPO to the Protected Settings container

1. In the Version Control Root, right-click the GPO you want to export, and select **Protected Settings | Export as Protected Settings**.
2. Select the version of the GPO you want to make as a Protected Settings policy, and click **Next**.
3. Review and confirm the version and GPO to export, and click **Finish**.

   The selected GPO will export and then import into the Protected Settings container.

4 Refresh the **Protected Settings** container.

The newly imported GPO will have the same name as the exported GPO. Best practice is to rename it using a naming convention that identifies it as protected. For example, PROT_01.

To create a Protected Settings policy through drag and drop

1 In the **Version Control Root**, select the GPO you want to use for a Protected Settings policy.

2 Drag and drop it on the Protected Settings container.

The Export Wizard will open.

3 Select the version of the GPO you want to make as a Protected Settings policy, and click **Next**.

4 Review and confirm the version and GPO to export, and click **Finish**.

The selected GPO will export and then import into the Protected Settings container.

5 Refresh the **Protected Settings** container.

6 The newly imported GPO will have the same name as the exported GPO. Best practice is to rename it using a naming convention that identifies it as protected. For example, PROT_01.

Generating Protected Settings policies reports

The following reports are available for Protected Settings policies: Latest, Working Copy, and Differences reports.

To generate a report

1 Select the **Protected Settings Root** container in the tree view.

2 Right-click the Protected Settings Policy, and select **Reports**.

3 Select the type of report to run.

NOTE: When a Protected Settings policy is used in GPOADmin, a separate report is generated by the protection process and will be generated when the comparison is made between a Protected Settings policy and a GPO.

Using Protected Settings policies

Once Protected Settings policies have been enabled through the Version Control properties (Options tab) and created they need to be applied to a container in GPOADmin.

This is done through new option on all containers that becomes available when the Enable Protected Settings for Group Policy Object is enabled.

To apply a Protected Settings policy

1 Right-click a container and select **Properties**.

2 Select the **Protected Settings** tab.

3 Select the **Add** button.

4 Select the policy to apply and click **OK**.

The selected protected policy displays in the Assigned Protected Settings policy window with the default validation rule.

5 To change the rule, right-click on the policy and select the validation rule that will be used to detect if a user is attempting to use or alter a protected setting. A check will be made for any similarities between the Protected Settings policy and the GPO being checked in.This can be either based on the settings name or value.

a **Settings defined in the Protected Settings policy are not allowed**: If a setting with the same name as a setting in the protected policy is detected in an active GPO, notification will be generated. The value does not have to be the same for the setting, just the setting name.

b **Values other than those defined in the Protected Settings policy are not allowed**: If there is a setting used in the active GPO that has a value different than the protected value then a notification is generated.

6 To block the Protected Settings from the parent container, select the **Block Protected Settings Inheritance** setting. You may want to do this as this container needs a unique protected setting and the setting from the parent would conflict with the new settings being applied.

7 Exclusions can be set for any GPO in the container which may contain protected settings. This allows specific GPOs to be excluded from any protected setting checking. Place a tick in the check box for any of the listed GPOs that you want to exclude from the Protected Settings policy.

8 If required, select **Include Group Policy Objects in all child containers** to allow the checking of all child containers against the assigned protected settings policy.

NOTE: Because there can be GPOs with the same name in GPOADmin, the path of the GPO is also listed to ensure you select the correct GPO for exclusion.

9 Once you are satisfied with your selections, click **Apply** and then **OK**.

Checking a GPO against a Protected Settings policy

A GPO that resides in a container with Protected Settings enabled will not be checked against the protected settings policy until the GPO is checked in using Check-In.

During a check in, the GPO is checked against the Protected Settings policy and if the GPO includes secured settings, a dialog box displays with the associated Protected Settings policies, how many matches were found, and the Validation mode (either setting name or value).

To generate a report that displays the differences between the GPO and the Protected Settings policy, select View Report. You can select to print or save the report. Once you have finished viewing the report click Close.

Click OK in the Protected Settings Modifications Detected dialog box to close it.

NOTE: The GPO will remain checked out until the issue with the Protected Settings policy is rectified and the GPO passes the check.

Validating a GPO against a Protected Settings policy before a check in

A GPO can be checked against the Protected Setting policy before checking it in.

To check a GPO before a check in

1 Right-click the GPO you want to check and select **Protected Settings | Verify Protected Settings**.

This checks the GPO against the Protected Settings policy. If the GPO includes secured settings, a dialog box displays with the associated Protected Settings policies, how many matches were found, and the Validation mode (either setting name or value).

2 Select **View Report** to generate a report that displays the differences between the GPO and the Protected Settings policy. You can select to print or save the report. Once you have finished viewing the report click **Close**.

3 Click **OK** in the Protected Settings Modifications Detected dialog box to close it.

NOTE: The GPO will remain checked out until the issue with the Protected Settings policy is rectified and the GPO passes the check.

3

Using Dell GPOADmin

- Connecting to the Version Control system
- Navigating the GPOADmin console
- Search folders
- Accessing the GPMC extension
- Configuring user preferences
- Working with the live environment
- Registering objects
- Working with controlled objects (version control root)
- Proposing the creation of controlled objects
- Checking compliance
- Editing objects
- Synchronizing GPOs
- Exporting and importing

Connecting to the Version Control system

Once the application has been fully configured (see Configuring the Version Control server on page 14) by the administrator, users connect to the Version Control system.

When the GPOADmin console is closed, the GPOADmin servers you were connected to are persisted, so the next time you open the GPOADmin console the connections to those servers are initiated automatically.

If you selected the “Remember my password” check box during the initial connection, then you will not be prompted for credentials the next time you connect. Each connection to this server from here on will automatically use the specified credentials, which are stored in Windows® Credentials Manager. To logon as a different user, you must remove the entry from the Windows® Credentials Manager.

To connect to the Version Control system using the GPOADmin console

1. Right-click the **GPOADmin** node and select **Connect To**.
2. Click **New** to create a new connection and enter the server name.

   The connection dialog, is automatically populated with GPOADmin Services detected in the environment.
3. Select the required Version Control server and click **Connect** to connect with the current logged on user credentials or select the down arrow in the Connect button and select **Connect As** to enter new credentials (domain\user and password).
4. To save the credentials, select the **Remember my password** check box and click OK.

Navigating the GPOADmin console

The GPOADmin console consists of a window divided into two panes.

The left pane displays the **console tree**. The console tree is a hierarchical structure that shows items (nodes) available in a console. From here you can view the live enterprise objects and the Version Control systems that are available to you. Version Control Root Hierarchy enables administrators to organize many objects logically based on their enterprise structure.

The right pane displays the details that pertain to the selected item in the console tree. For version controlled objects this includes:

- name
- type
- version
- status
- pending action
- whether workflow is enabled
- deployment time
- managed by (who is responsible for it)
- the user who has it checked out
- the domain where it is applied
- when it was modified
- when it was last deployed
- associated keywords

Search folders

Search folders are an easy way to view the status of objects within the Version Control system.

- All Managed objects: Displays all registered objects under version control within GPOADmin.
- Available: Displays all objects with an available status within the version control system.
- Checked out: Displays all objects not available due to being checked out for modification.
- Checked out to me: Displays all objects checked out to the user who is logged in to GPOADmin.
- Pending approval: Displays all objects awaiting specified approvals before being deployed.
- Pending deployment: Displays all objects awaiting deployment to the live environment.
- Cloaked: Displays all cloaked GPOs.

NOTE: You must have the View Cloaked right to see these GPOs.

- Locked: Displays all locked GPOs.
- Unauthorized modifications: Displays all registered objects that were modified in the live environment outside of the GPOADmin version control system.
- Deleted objects: Displays all objects awaiting deletion.
- Unregistered: Displays all objects in the managed forest not registered within the version control system.
- Workflow enabled objects: Displays all objects registered within the version control system which are workflow enabled.
- Workflow disabled objects: Displays all GPOs registered within the version control system as workflow disabled.

NOTE: Any setting changes to these GPOs will be applied within version control as well as to the live environment.

- Linked scopes of management: Displays Scopes of Management that have linked GPOs.
- Unlinked scopes of management: Displays Scopes of Management that have no linked GPOs.

Accessing the GPMC extension

As part of its installation, GPOADmin appears as a tab in Microsoft® Group Policy Management Console (GPMC). In the right pane, there are now two tabs: one for native GPMC, and one for GPO Management. On the GPO Management tab, all GPOs are listed, regardless of whether they are under version control. The GPMC Extension has a toolbar for easy access to commonly used functions.

NOTE: Most tasks can be performed using either the toolbar or the context menu.

You are automatically connected to the Version Control server selected during the installation process, based on the credentials of the currently logged in user. You can connect to other Version Control servers if needed.

For a full list of tasks you can perform using the GPMC Extension, see Group Policy Management Console extension on page 8.

To access the GPMC Extension

1. In the GPMC, expand the forest, domain and domain node.
2. Click the **Group Policy Objects** node.
3. Click the **GPO Management** tab.

Configuring user preferences

To configure user preferences

NOTE: You must configure user preferences in the GPOADmin console.

1. Right-click the forest, and select **User Preferences**.
2. Select the Preferences tab, and choose a folder or disk where you would like your reports to be stored.
3. Select the **Notifications** tab and enter the email address where you want to have the notification messages sent.

   For more information on configuring the Notification system, see Selecting events on which to be notified on page 22.
4. To remove a notification, select the notification source and click the **Remove** button.
5. Click **OK**.

Adding and removing custom ADM files

You can add custom .adm files and apply their associated settings to GPOs and templates. For example, you can add Office .adm files to control and configure its particular settings.

NOTE: All ADM files used with Dell GPOADmin templates must be Unicode. ADM files are managed using the GPOADmin console.

NOTE: ADMX files are not supported.

NOTE: GPOADmin does not support the use of templates on Windows® 7, Windows Server 2008, and later. The support on earlier Windows operating systems is also limited.

To add custom ADM files

1. Expand **GPOADmin**, right-click the forest node, and select **Add/Remove ADM**.
2. Add new .adm files by clicking **Add**.
3. Select the required .adm file and click **Open**.
4. Click **OK**.

   When you create a template, the Administrative Templates folder will include the settings from the .adm file.

To remove custom ADM files

1. Expand Dell GPOADmin, right-click the forest node, and select **Add/Remove ADM**.
2. Remove .adm files by clicking **Remove**.
3. Click **OK**.

For more information on creating ADM files, see Creating and editing ADM files on page 90.

Working with the live environment

Registering objects

To start working with the Version Control system, the GPOs, WMI filters, and Scopes of Management (Sites, Domains, and Organizational Units) must be registered. You have the option to make GPOs workflow enabled at the time of registration and to maintain the version history of objects that were previously registered within GPOADmin.

Registering and unregistering are recursive for objects when they are selected from the treeview on the left of the console. All child objects are included unless you individually select lower-level objects to register.

You have the choice of registering all items in the selected container or domain, all GPOs, or all WMI Filters when you use the Register menu. When you register objects at the domain level, you do not automatically register GPOs or WMI filters in the domain unless they are already linked to the Scopes of Management that are being registered. You can select WMI Filters and GPOs separately, using their respective folders.

NOTE: Only users with the Register and Unregister rights can register and unregister objects. For more information, see Configuring role-based delegation on page 19.

When an object is added to the system for the first time, it will be automatically backed up (stored) in the Version Control system history and labeled with a version of 1.0, unless another major version number is specified during the registration process. Each time a change is made (an object is checked in) a minor number is added. For example, v1.2, v1.3, and v1.4. When a change is deployed to the enterprise by a user with the appropriate role, the version number will change to the next major number, for example, v2.0 and v3.0.

NOTE: GPOADmin works with pre-existing GPOs, WMI filters, and Scopes of Management, as well as any templates or other objects created from within the system.

NOTE: If an object is not registered in version control, the modified date displayed is returned from the live object.

NOTE: You must have the Register right and access to the Live Environment to perform the following steps.

To register objects using the GPOADmin console

1. Expand **GPOADmin**, the **Live Environment**, and domain nodes, and select the object you want to register within the Version Control system.
2. Right-click and select one of the following: **Register - This Object Only, - All**, **- Group Policy Objects**, **- Scopes of Management,** or **- WMI Filters**.
3. Select the container in which you want to place the registered object, or create a new container, and click **OK**.

   Once the objects have been registered, they are located in the selected container under the Version Control Root with the initial version number set to 1.0. They are now available to be checked out and edited. You can set the major version number to any number greater than 1.0 (for example to maintain a version number if you are migrating from another Version Control system).

   Users with the delegated rights can link registered GPOs to Scopes of Management (Sites, Domains, and Organizational Units) and add WMI Filters. For more information about linking GPOs, see Linking GPOs on page 63. For information about adding WMI Filters, see Creating Group Policy Objects (GPOs) on page 40.

To register GPOs using the GPMC Extension

NOTE: You must use the GPOADmin console to register WMI filters and Scopes of Management.

Registering GPOs using the GPMC Extension is not recursive. If you want to register all child objects at once, use the GPOADmin console.

1. Expand the forest, domains, and domain nodes. Click the **Group Policy Objects** node, and select the GPO you want to register within the Version Control system.
2. Click **Register**.
3. Select the container in which you want to place the registered object and click **OK.**
4. Click **New Container** and name the container. Click **OK**.

Registered status

You can quickly see the status of registered GPOs, WMI filters, templates, sites, domains, and OUs. The objects will either be available for check out, already checked out, or checked in and awaiting approval to be committed to the enterprise. The options available to you at each state will depend on your specific role and permission. Registered objects will be in one of the following states:

Table 4. Registered Status

Status	From this state, depending on your assigned role and enabled options, you may have the ability to:
Available	• link • search and replace • edit • check out • import and export GPO settings • request approval (for objects that have minor versions greater than zero) • deploy (for objects that have minor versions greater than zero) • label • cloak/uncloak GPOs • lock/unlock GPOs • enable/disable workflow for GPOs • managed by • check compliance • unregister objects • protected setting - export • templates - apply and create • create and save reports dealing with latest, and live objects, and the • difference between them • show history • Synchronize – Synchronize Now and Set Synchronization Targets • edit object properties • refresh the object • cut • copy • mark objects for deletion • rename

Table 5. Registered Status

Status	From this state, depending on your assigned role and enabled options, you may have the ability to:
Checked Out	• link • search and replace • edit objects • check in objects • undo any check out • import and export GPO settings • request approval (for objects that have minor versions greater than zero) • deploy (for objects that have minor versions greater than zero) • label • managed by • protected setting - export and verify • templates - apply and create • create and save reports dealing with latest, live, and working copy objects, and the difference between them • show history • Synchronize – Synchronize Now and Set Synchronization Targets • edit object properties • refresh the object • cut • copy • rename

Table 5. Registered Status

Status	From this state, depending on your assigned role and enabled options, you may have the ability to:
Pending Approval	• link • search and replace • export GPO settings • withdraw approval request • approve changes • reject • deploy the changes to the environment • label • managed by • protected setting - export • templates - create • create and save reports dealing with latest and live objects, and the difference between them • show history • Synchronize –Set Synchronization Targets • edit object properties • refresh the object • cut • copy
Pending Deployment	• link • search and replace • export GPO settings • reject • withdraw approval • deploy the changes to the environment • label • managed by • protected setting - export • templates - create • create and save reports dealing with latest, and live objects, and the difference between them • show history • Synchronize –Set Synchronization Targets • edit object properties • refresh the object • cut • copy

Removing registered objects

If you no longer want the object to be available for changes, you can remove it from the Version Control system, as long as you have been granted the Unregister right. Unregistering version-controlled objects is now recursive, unless you select the lower-level objects individually.

To remove objects from the Version Control system using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click the object and select **Unregister**.

To remove GPOs from the Version Control system using the GPMC Extension

Unregistering GPOs using the GPMC Extension is not recursive. If you want to unregister all child objects, use the GPOADmin console.

1. Select the **Group Policy Objects** node and then select the GPO.
2. Click **Unregister**.

NOTE: You can view a list of Unregistered objects in the Search Folders in the GPOADmin console. This includes GPOs, WMI filters, and SOMs.

Viewing the live environment

As the administrator, may want to allow users to see the live environment from within the GPOAdmin console. This will, for example, enable you to delegate GPO, OU, or SOM object registration (and recursive registration) to specific users in your organization.

To permit a user to see the live environment:

1. Login to GPOADmin as a GPOADmin administrator.
2. Right-click the **Live Environment** node and select **Properties**.
3. On the Security tab, add one or more user who require access to the live environment.
4. Click **OK**.

Working with controlled objects (version control root)

- Creating a custom container hierarchy
- Selecting security, levels of approval, and notification options
- Copying/pasting objects
- Proposing the creation of controlled objects
- Working with registered objects
- Working with available objects
- Working with checked out objects
- Working with objects pending approval and deployment

Creating a custom container hierarchy

You can organize registered objects into a user-defined hierarchy under the Version Control Root container.

Each container has its own “security descriptor” in which trustees can be delegated roles to define their access to the contained objects. For more information see Configuring role-based delegation on page 19.

Once you have the containers created, you can easily move and copy objects to other containers within the same domain.

To create a new container

1. Expand the treeview and select the **Version Control Root** or subcontainer.
2. Right-click and select **New | Container**.
3. Enter the container name and click **OK**.

NOTE: If you are working in the GPMC Extension, you can only create a container when you are registering an object (for more information see Registering objects on page 33). You cannot delete or label containers in the GPMC Extension.

To delete a container

NOTE: You must use the GPOADmin console to delete a container.

1. Expand the treeview and locate the container under the Version Control Root node.
2. Right-click the container and select **Delete**.

To label a container

NOTE: You must use the GPOADmin console to label a container.

1. Expand the treeview and locate the container under the Version Control Root node.
2. Right-click, and select **Label**.
3. Enter the label for the container, and click **OK**.

Selecting security, levels of approval, and notification options

You have the option of implementing safeguards by designating multi-level approvers. With this option, a change must be approved by the designated number of approvers before it will become available for deployment in the live environment.

To set the security, approval level, and notification options on an object or container

- Right-click the **Version Control Root** node, required container or object, and select **Properties**.

  From here you will be able to delegate responsibilities over the container through the Security options, configure the approval levels, and set the events to be notified on through the Notification tab. If the Protected Settings option has been enabled you will be able to assign protected setting and set exclusions.

  For more information on delegating roles see Configuring role-based delegation on page 19. For more information on configuring the notification system, see Selecting events on which to be notified on page 22.

NOTE: If you are using the GPMC Extension, you can only set these options for GPOs.

Viewing the differences between objects

You can create a report that shows the differences between two or more objects.

To view the difference between settings using the GPOADmin console

1. Expand the **Version Control Root** node, and the required container.
2. Select two or more similar objects, right-click and select **Reports | Differences**.
3. In the **Base** column, select the Base object that you want to compare the other objects to.
4. In the **Version** column, select a version for each object to compare.
5. In the **Show** list, choose an option for which data to show in the report.
6. Click **OK**.
7. View the Report.

   If you choose to compare more than one object to the base, each comparison report is displayed in its own tab.
8. Click **Print** to print the report.

   Click **Save As** to save the report in HTML.
9. Click **Close**.

To view the difference between GPO settings using the GPMC Extension

1. Select the two or more GPOs to compare.
2. Click **Reports | Differences**. Select the version that you want to compare from the lists, and click **OK**.
3. In the **Base** column, select the Base object that you want to compare the other objects to.
4. In the **Version** column, select a version for each object to compare.
5. In the **Show** list, choose an option for which data to show in the report.
6. Click **OK**.
7. View the Report.

   If you choose to compare more than one object to the base, each comparison report is displayed in its own tab.
8. Click **Print** to print the report.
9. Click **Save As** to save the report in HTML.
10. Click **Close**.

Copying/pasting objects

You can easily copy and paste objects within the hierarchy. When you copy and paste an object within the version control system, you have the option to preserve the object's history.

NOTE: Multiple objects can be cut and pasted, but you can only copy and paste one object at a time.

You can choose the version of the object to copy. When a single object is pasted, you have the option to select the live version (if available), the working copy (if the object is currently checked out to you) or any of the historical versions of the object.

You cannot copy or move (cut/paste) objects from one server/forest to another. If objects are cut and pasted to a server/ forest that was not the same as the one from which they were cut, the cut becomes a copy upon pasting them. All normal copy/paste rules then apply.

When you paste the object, it becomes a new object with a version of 0.0 in the checked out state. This version number indicates that the version is not considered "live" until it goes through the approval process. If you copy and paste the GPO with the history, it becomes a GPO that is shared with the original GPO.

NOTE: If you copy and paste an object that is checked out, changes to the working copy will not be pasted. Only the history, up to the last checked out version, can be pasted.

When you drag and drop an object between containers on the same service, it will invoke the "move" operation. If dragging and dropping between containers on different services, it will invoke the "copy" operation.

When you right-click and drag and drop, you will be presented with two options: "Copy here" and "Move here". When dragging between containers on the same service, a copy means copy and a move means move. However, when dragging and dropping between containers on different services, regardless of which option is selected, the copy operation will be invoked.

To copy and paste an object

NOTE: You cannot copy and paste objects in the GPMC Extension.

1. Expand the **Version Control Root** node and the required container.
2. Right-click an object and select **Copy**.
3. Right-click the target container, and select **Paste**.
4. From the Export wizard, select the version that you want to test and click **Next**.
5. Select the target Version Control domain for the object and click **Next**.

   If you choose to copy the history from the source, when you view the history on the pasted object, the actions are clearly marked as having been actions on the source.

   If an object with the same name already exists in the target container you will have the following options: cancel the paste, edit the name, or continue using the duplicate name.
6. Select a migration table (if required) and click **Next**.
7. Click **Finish**.

   NOTE: If the Enable Unique Names option is selected, the copied object with have "Copy of" appended to the object name.

Proposing the creation of controlled objects

- Creating Group Policy Objects (GPOs)
- Creating WMI filters
- Creating templates
- Creating templates from registered GPOs

Creating Group Policy Objects (GPOs)

Users with the appropriate permission can propose the creation of a GPO that does not currently exist in the enterprise environment and have it placed within the Version Control system.

When you create a Group Policy Object (GPO) as Workflow Disabled, you are creating it in the context of the user you are logged on as. This GPO sits immediately in the live environment.

When you create a GPO as Workflow Enabled, you create it in the context of the GPOADmin Service Account and this GPO sits awaiting deployment. Once deployed, it sits in the live environment.

Creating a new GPO manually can be time consuming. Creating a GPO based on a previously created template simplifies this process.

Creating a GPO based on a template is also valuable when the template is used to create many GPOs with common settings. Once the GPO has been created from this base, each GPO can be tailored to meet specific needs.

When you create a new GPO, you will have the opportunity to apply one or more templates to that GPO.

NOTE: Checking for Conflicting Template Settings

GPOADmin checks for conflicting template policy settings when you either create a new GPO and apply templates to it, or when you select a GPO that has already been created and select to apply a template. If two or more templates are selected, a dialog box will open and you will have the option to skip checking for conflicts.

If conflicts are found, you can choose to continue with the understanding that the last template's settings will win. You can view the details of the conflicting settings by clicking the Details button, which opens the Template Conflict Report.

To propose the creation of a GPO in the GPOADmin console

1. Expand the **Version Control Root** node, right-click the required container, and select **New | Group Policy Object**.
2. Enter a name and select the location for the GPO and click **Next**.
3. If required, select templates to apply to the GPO, and click **Next**.
4. Click **Launch Editor**.
5. Make the required edits to the new GPO and close the Group Policy Editor.
6. Modify any additional GPO settings if required and click **Next**.
7. If required, click **Add**, enter security filters, and click **Next**.
8. If required, select WMI filters to apply, and click **Finish**.

   When you make edits and check the GPO in, the version will be updated to version 0.1. This number will increase by .1 until you select to Check In and Request Approval. At this point the GPO is not live.

   Once you complete your edits, you can select Check In and Request Approval. If approved and deployed, the new GPO will become available with a version number of 1.0. For more information on the approval and deployment process, see Requesting approval on page 50 and Scheduling deployment on page 58.

   Users with the delegated rights, can link registered GPOs to Scopes of Management (Sites, Domains, and Organizational Units) and add WMI Filters. For more information about linking GPOs, see Linking GPOs on page 63. For information about adding WMI Filters, see Creating WMI filters on page 42 and Creating Group Policy Objects (GPOs) on page 40.

To propose the creation of a GPO in the GPMC Extension

1. Right-click in any blank area of the GPO Management pane and choose **New | Group Policy Object**.
2. Enter a name and select the location for the GPO and click **Next**.
3. If required, select templates to apply to the GPO, and click **Next**.
4. Click **Launch Editor**.
5. Make the required edits to the new GPO and close the Group Policy Editor.
6. Modify any additional GPO settings if required and click **Next**.
7. If required, click **Add**, enter security filters, and click **Next**.
8. If required, select WMI filters to apply, and click **Finish**.

For more information on WMI Filters, see Creating WMI filters on page 42. For more information on Templates, see Creating templates on page 42.

Creating WMI filters

Using Windows® Management Instrumentation (WMI) filters, you can control where GPOs are applied based on the attributes of a target computer.

The WMI filter associated with the GPO is processed on the target computer. The query, in the WMI filter that is linked to a GPO, is evaluated on the target computer.

For example, your filter may be “Select computers that have a processor speed higher than 2 GHz”. If the target computer meets the criteria, the GPO is applied. If not, the GPO is not applied.

NOTE: The WMI filter and the GPO to which it is linked to must be in the same domain.

To propose the creation of a WMI filter

NOTE: WMI filters must be created using the GPOADmin console.

1. Expand the Version Control container where you want to place the new WMI filter.
2. Right-click and select **New | WMI Filter**.
3. Enter a name for the new WMI filter.
4. Select a domain in which the WMI filter will be created, add a description if required, and click **Next**.
5. Select a Root Namespace (default: root\CimV2) and enter a valid WQL (Windows® Query Language) string in the Query field.

   You must have at least one query associated with a WMI Filter to continue.
6. To add an additional query to the filter, select **New Query**, and specify the Root Namespace and Query as described in Step 5.
7. To delete a query, click the “x” button next to the query in the list.
8. Click **Finish**.

   The WMI Filter must go through the approval and deployment process before it can be applied.For further information, see Requesting approval on page 50 and Scheduling deployment on page 58.

For more information about applying WMI Filters to GPOs, see Creating Group Policy Objects (GPOs) on page 40.

Creating templates

You can establish a template of policy settings to use when creating or updating GPOs.

NOTE: You must create templates using the GPOADmin console.

NOTE: GPOADmin does not support the use of templates on Windows® 7, Windows Server 2008, and later. The support on earlier Windows operating systems is also limited.

To create a template

NOTE: You must create templates using the GPOADmin console.

1. Expand the **Version Control Root** or subcontainer, right-click, and select **New | Template**.
2. Enter a name for the template and a description if required.

   You are now ready to select policies that you want to include in the template.
3. Click the **Details** tab, and click **Add**.
4. Select the required policies, and click **Add**.
5. Select the policy, and click **Modify** to configure the policy settings.
6. Enter the requested information, and click **OK**.

7 Click **OK** once you have added all the required policy settings.

The template must go through the approval and deployment process before it can be applied. For further information, see Requesting approval on page 50 and Scheduling deployment on page 58.

For information on editing templates, see Editing templates on page 63.

For information on basing templates on existing GPOs, see Creating templates from registered GPOs on page 43.

Creating templates from registered GPOs

To take advantage of the portability of templates, you can convert existing GPOs and their settings into templates.

NOTE: All ADM files used with Dell GPOADmin templates must be Unicode.

NOTE: GPOADmin does not support the use of templates on Windows® 7, Windows Server 2008, and later. The support on earlier Windows operating systems is also limited.

To create a template from a GPO

NOTE: You must create templates from registered GPOs using the GPOADmin console.

1 Expand the **Version Control Root** or subcontainer.

2 Right-click the required GPO, and select **Templates | Create Template**.

3 Click the container where you want to place the template and click **OK**.

4 Click **New Container** to create a new container, enter a name for the container, and click **OK**.

You can now apply this template to other GPOs. For further information, see Creating Group Policy Objects (GPOs) on page 40.

Working with registered objects

Regardless of the status of the registered GPO, WMI filter, template, domain, site, or OU (Available, Checked Out, Pending Approval, and Pending Deployment), you can perform the following tasks if you have the appropriate role:

- Creating labels
- Cloaking a GPO (applies to available GPOs only)
- Locking a GPO (applies to available GPOs only)
- Establishing Management for an Object
- Viewing and editing object properties
- Creating a report

NOTE: You can view a list of all registered objects in the All Managed Objects in the Search Folders in the GPOADmin console.

Creating labels

You can include user-defined history comments (labels) on objects and containers in the Version Control system. This functionality allows users to rollback to an object identified by a specific label.

To create a label using the GPOADmin console

1 Expand the **Version Control Root** node, and select an object.

2 Right-click and select **Label**.

3 Enter the label in the Comment dialog box and click **OK**.

To create a label for a GPO using the GPMC Extension

1 Select the GPO and click **Workflow | Label**.

2 Enter the label in the Comment dialog box and click **OK**.

Cloaking a GPO

Cloaking allows you to hide Group Policy Objects (GPOs) from other users. The Cloaking role is not a default role installed with the product, and must be created with the Cloak/Uncloak and View Cloaked rights. By default, Domain Administrators can see all cloaked GPOs.

When a GPO is cloaked using GPOADmin, it is also cloaked in the live environment. Only users with the Cloak/Uncloak or View Cloaked right can see the GPO in the live environment. A cloaked GPO will only be applied to users who have the Cloak/Uncloak or View Cloaked right during group policy processing. All other users will no longer have the GPO applied.

Cloaked GPOs are indicated by a lighter GPO icon.

NOTE: Only GPOs can be cloaked. (You cannot cloak WMI Filters or Scopes of Management).

To cloak a GPO using the GPOADmin console

1 Select the GPO you want to cloak from the list of GPOs within the Version Control Root node.

2 Right-click and select **Cloak**.

Cloaked GPOs are displayed in the Cloaked search folder. Enter a comment and click **OK**.

NOTE: Users can also have the View Cloaked right only. This means that they can see cloaked GPOs but do not have permission to "uncloak" them. Cloaked GPOs can be viewed in the Search Folders in the GPOADmin console.

To cloak a GPO using the GPMC Extension

1 Select the GPO you want to cloak from the list of GPOs and click **Cloak**.

2 Enter a comment and click **OK**.

Locking a GPO

Locking allows you to lock a policy so other users cannot edit it. The Locking role has to be created and consists of the Lock/Unlock right. For example, you may choose to lock the Default Domain Policy and/or Default Domain Controller Policy as any modification to these settings would affect every GPO in the organization.

When a GPO is locked using GPOADmin, it is also locked in the live environment. All users can see the GPO, but no one can edit it.

By default, Domain Administrators can see all locked GPOs and unlock any locked GPO. Locked GPOs are indicated by a lock icon.

NOTE: Only GPOs can be locked. (You cannot lock WMI Filters or Scopes of Management).

To lock a GPO using the GPOADmin console

1 Select the GPO you want to lock from the list of GPOs within the Version Control Root node.

2 Right-click and select **Lock**.

Locked GPOs are displayed in the Locked search folder.

NOTE: When a user with the right to lock GPOs connects to the GPOADmin console, they will see all locked GPOs. A Locked GPO must be unlocked before any actions can be performed (even if you are a system administrator.) Locked GPOs can be viewed in the Search Folders in the GPOADmin console.

3 Enter a comment and click **OK**.

To lock a GPO using the GPMC Extension

1 Select the GPO you want to lock from the list of GPOs and click **Lock**.

2 Enter a comment and click **OK**.

Establishing Management for an Object

If you have the Modify Managed By right, you can set the user responsible for an object's management.

To set or change the user responsible for an object's management

1 Expand the **Version Control Root** node, and select an object.

2 Right-click and select **Managed By**.

3 Enter or browse for the required account and click **OK**.

You can also assign management on a container by right-clicking on it an selecting Properties and selecting the required account.

NOTE: Any child containers or objects below this container that do not have a managed assigned to them will automatically use this one.

Viewing history

You can easily create a report that displays the historical settings for objects in the Version Control system or a comparison of versions. When you view the history in the GPMC Extension, all events are shown. The GPOADmin console has a filter option that you can use to choose which events to display.

To view the history using the GPOADmin console

1 Expand the **Version Control Root** node, and the required container.

2 Right-click an object and select **Show History**.

3 Select a version in the list.

4 Select which, if any, filtering options you would like to apply, then right-click, and select **View** to view the historical information.

5 To view the difference between various check ins, select the required versions, right-click and select **Differences**.

6 Click **Print** to print the report.

Click **Save As** to save the report in HTML.

7 Click **Close**.

NOTE: You can also restore links between a GPO and its Scopes of Management from the history view. For more information, see Restoring links to a previous version on page 53.

To view the history using the GPMC Extension

1 Select the GPO and click **Show History**.

The history displays in the bottom pane of the GPO Management tab. You will see the name, version, action, account, date and comment pertaining to the history item.

2 To view the difference between various check ins, select the required versions, right-click and select **Differences**.

3 Click **Print** to print the report.

Click **Save As** to save the report in HTML.

4 Click **Close**.

For more information on the available reports, see Creating Reports on page 70.

Deleting version history

As you progress an object through the Version Control workflow, GPOADmin keeps an audit trail, as well as a history of all minor and major versions. If you no longer need to keep this history, you can selectively delete any of the versions except your last backup. Only the object settings are deleted; the audit trail is preserved, and you still see the entry in the object history. Deletions are permanent.

NOTE: When a new version is created, an internal record of the action that generated the version is kept—including the user that performed the action, the date and a label if one was created. You may wish to view this audit trail in a History report before deciding which versions you want to delete. For more information, see Historical Settings Reports on page 87.

To delete version history in the console

1 Expand the **Version Control Root** node, and the required container.

2 Right-click an object and select **Show History**.

3 In the **History** dialog box, select a version from the list. (Press **CTRL** and click to select multiple versions.)

You can only delete major and minor versions. If you have Show All Events enabled, events that have occurred between versions cannot be deleted, as there are no settings associated with them.

4 Right-click and then select **Delete**.

5 In the confirmation dialog box, click **OK**.

After you delete a version history, it remains on the list, but is unavailable.

NOTE: Once you have deleted version history, it cannot be undone.

To delete version history of a GPO using the GPMC Extension

1 Select the GPO and click **Show History**.

2 In the bottom pane, select a version. (Press **CTRL** and click to select multiple versions.)

You can only delete major and minor versions. Events that have occurred between versions cannot be deleted, as there are no settings associated with them.

3 Click **Delete**.

4 In the confirmation dialog box, click **OK**.

Viewing and editing object properties

You can easily view and edit the details for the current version of an object in the Version Control system including the security, notification settings, keywords, and approvals, as well as the object's location within version control.

You can also view important information about changes made in the live environment on the Change Auditor™ tab, if you have a supported version of Change Auditor. See the Release Notes for a complete list of supported versions. You can view changes made to GPOs, domains, and sites on this tab.

NOTE: Users with the appropriate permission can alter the security settings. For more information, see Configuring role-based delegation on page 19.

To view the properties using the GPOADmin console

1 Expand the **Version Control Root** node, and the required container.

2 Right-click the required object and select **Properties**.

3 From the Properties dialog box, click the required tab to see the associated information.

Table 6. Options

Option	Description
General	View the domain, user, the creation and modification dates, the version, the unique ID, location in version control, and the GPO status. From here you can also see and, if required, change the user responsible for an object's management (Managed By property).
Security	Delegate responsibilities over the object.
Approvals	Approval workflows for object creation, deletion, or modification. **NOTE:** Click the **Override inherited work flow** check box if you want the approvals process for this container to be different from its top level container.
Notifications	Select the actions to be notified on.
Change Auditor™	View changes made to objects in the live environment. You can move the columns and sort by columns. **NOTE:** You must have a supported version of Change Auditor installed. See the Release Notes for a complete list of supported versions. You can also view and save a report of changes. For information, see Change Auditor™ Report on page 76.
Keywords	View all the keywords for a given object. For here you can also, add and remove keywords as required. When a new keyword is entered it is saved into a master list of keywords. This master list is displayed for each object. The checkboxes indicate which keywords are applied to each object.

To view the properties using the GPMC Extension

1 Right-click the GPO and select **Properties**.

2 From the Properties dialog box, click the required tab to see the associated information.

Table 7. Options

Option	Description
General	View the domain, user, the creation and modification dates, the version, the unique ID, location in version control, and the GPO status. From here you can also see and, if required, change the user responsible for an object's management (Managed By property).
Links (From the GPO Properties page)	Edit the link to Scopes of Management. **NOTE:** You must have the Link permission to add or edit links.
Security	Delegate responsibilities over the object.
Approvals	Number of required approvers for object creation, deletion, or modification.
Notifications	Select the actions to be notified on.

Table 7. Options

Option	Description
Keywords	View all the keywords for a given object. For here you can also, add and remove keywords as required. When a new keyword is entered it is saved into a master list of keywords. This master list is displayed for each object. The checkboxes indicate which keywords are applied to each object.
Change Auditor™	View changes made to objects in the live environment. You can move the columns and sort by columns. **NOTE:** You must have a supported version of Change Auditor installed. See the Release Notes for a complete list of supported versions. **NOTE:** You can also view and save a report of changes. For information, see Change Auditor™ Report on page 76.

For more information on the available reports, see Creating Reports on page 70.

Creating a report

You can create reports that show the details of controlled objects, as well as diagnostic and troubleshooting information. For more information see, Creating Reports on page 70.

Working with available objects

With available objects, you can perform all the tasks of registered objects (Show history, view live reports, view properties, unregister, create labels, and import/export), as well as:

- Enabling/disabling workflow
- Checking out objects
- Requesting the deletion of an object
- Requesting approval
- Checking compliance
- Synchronizing GPOs

NOTE: You can view a list of all Available objects in the Search Folders in the GPOADmin console.

Enabling/disabling workflow

If you have the Enable/Disable right, you can enable/disable the workflow for a deployed GPO. The object must be under version control and be a major version (for example, 2.0).

NOTE: You can view a list of Workflow Enabled or Workflow Disabled objects in the Search Folders in the GPOADmin console.

To enable/disable workflow in the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click a major version of an available GPO and select **Disable Workflow.**

   Right-click a GPO that is not workflow enabled and select **Enable Workflow.**

3 Enter a comment and click **OK**.

NOTE: If you disable the workflow, any changes made are immediately deployed in the live environment. To bring the GPO back under version control, enable the workflow.

NOTE: When managing GPOs across forests, they must be workflow enabled.

To enable/disable workflow in the GPMC Extension

1 Select a major version of an available GPO and click **Workflow | Disable Workflow**.

Select a GPO that is not workflow enabled and click **Workflow | Enable Workflow**.

2 Enter a comment and click **OK**.

Checking out objects

Before users can edit registered objects, they must be checked out. The workflow is as follows: Check-out the object from the system, make the required edits, and check in the changes to the system.

Checking out an object for the first time creates a copy of the original live version.

NOTE: The changes are only applied to the live enterprise when they are approved by users included in the approval workflow and deployed by users with the Deploy permission.

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

NOTE: If you have all required rights, you can approve and deploy an object from the checked out state and all workflow steps happen automatically.

NOTE: You can view a list of checked out objects in the Checked Out or Checked Out to Me Search Folders in the GPOADmin console.

To check out an object using the GPOADmin console

1 Expand the **Version Control Root** node and the required container.

2 Right-click an object in the Available state and select **Check Out**.

3 Enter a comment and click **OK**.

NOTE: When a GPO is checked out only the settings are maintained — not the GPO links. You can check out multiple GPOs at once.

To check out a GPO using the GPMC Extension

1 Select an available GPO and click **Workflow | Checkout**.

2 Enter a comment and click **OK**.

Requesting the deletion of an object

Users can propose the deletion of objects in the enterprise environment that are currently registered in the Version Control system and in the Available state. If the request is approved, the object will be removed from the system and deleted from the live environment.

NOTE: If you simply want to remove the object from the Version Control system (not the live environment), unregister it. For more information on unregistering objects, see Removing registered objects on page 37.

NOTE: You can view a list of Deleted objects in the Search Folders in the GPOADmin console.

To delete an object using the GPOADmin console

1 Expand the **Version Control Root** node and the required container.

2 Right-click the required object and select **Delete**.

3 Enter a comment and click **OK**.

The object is now in the Pending Approval state.

NOTE: Objects with a version number of 0.0 can be deleted by the user who created them.

To delete a GPO in the GPMC Extension

1 Right-click the GPO and select **Delete**.

2 Enter a comment and click **OK**.

Requesting approval

Once an object has been altered and checked in to the system, the update is ready to go through the approval process. (For more information on checking in objects, see Checking in controlled objects on page 51.)

To request approval using the GPOADmin console

1 Expand the **Version Control Root** node and the required container.

2 Right-click the altered object and select **Request Approval.**

3 Enter a comment and click **OK**.

The object will now be in the Pending Approval state.

To request approval using the GPMC Extension

1 Select the altered GPO and click **Workflow | Request Approval**.

2 Enter a comment and click **OK**.

Working with checked out objects

With checked out objects, you can perform all the tasks of registered objects (Show history, view live reports, view properties, unregister, create labels, and import/export), as well as:

- Undoing a check out
- Checking in controlled objects
- Restoring an object to a previous version
- Checking compliance
- Synchronizing GPOs

NOTE: If you have all required rights, you can approve and deploy an object from the checked out state and all workflow steps happen automatically.

Undoing a check out

The user who checked out an object has the option of undoing the check out and reverting the state back to Available.

To undo a check out

1 Expand the **Version Control Root** node and the required container.

2 Right-click the object and select **Undo Check Out**.

3 Enter a comment and click **OK**.

To undo a checkout in the GPMC Extension

1. Select the checked out GPO and click **Workflow | Undo Check Out**.
2. Enter a comment and click **OK**.

NOTE: If you undo a check out of an object with a version 0.0, the working copy will be deleted and there will be no record of the object in the Version Control System.

Checking in controlled objects

Once you have checked out an object and edited its settings (for more information, see Editing objects on page 61), you have the option to:

- Check in objects in their temporary state for further updates
- Check in objects and notify Approvers that it is ready to be approved or rejected (For more information, see Requesting approval on page 50.)
- Undo the check out (For more information, see Undoing a check out on page 50.)

A check in updates the history of the object within the Version Control system with the changes made while it was checked out. Included with any check-in is a comment and a unique minor version number (such as 1.1).

A check in does not allow the offline changes to go live into the enterprise environment as it must first be approved. Once an object is marked as Pending Approval, it cannot be checked out by any other user of the system.

Multiple check in and check outs are allowed to occur within the system without requiring approval. When a user checks in an object so it is available to another system user, the next user to check out the same object will be working with the current offline version consisting of all changes made to date. After all the users have made their required changes to the offline object it is processed by the approval system to determine if the changes are accepted to go live into the enterprise or not.

To check in an object using the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click an object and select **Check In**.
3. Enter a comment if required and click **OK**.
4. Right-click and select **Request Approval** if required. Enter a comment and click **OK**.

To check in a GPO using the GPMC Extension

1. Select the GPO and click **Workflow | Check In**.
2. Enter a comment if required and click **OK**.
3. Click **Workflow | Request Approval** if required. Enter a comment and click **OK**.

Withdrawing an approval request

Any user who proposes a change to an object can withdraw their own request for approval while the change is in the Pending Approval state.

To withdraw an approval request in the GPOADmin console

1. Right-click an object in the Pending Approval state, and select **Withdraw Approval Request**.
2. Click **OK**.

   The object is returned to the Available state.
3. Enter a comment and click **OK**.

To withdraw an approval request in the GPMC Extension

1. Select a GPO in the Pending Approval state, and click **Workflow | Withdraw Approval Request**.
2. Enter a comment and click **OK**.

Restoring an object to a previous version

You can easily create a report that displays the historical settings for objects in the Version Control system or a comparison of versions to locate the differences. For more information, see Establishing Management for an Object on page 45 and Creating Reports on page 70.

You can also import settings from any version in the history of the Version Control System, as well as links between Group Policy Objects and Scopes of Management. This effectively creates a roll back to an earlier set of parameters. You must have the object checked out to perform this action. You must also have the Link right to restore links. For more information, see Configuring role-based delegation on page 19.

Rolling back to a particular version of a workflow enabled GPO does not affect the live enterprise environment until it has gone through the complete approval process. For a workflow disabled GPO, the effect is immediate.

From this point forward, the basic workflow of GPOADmin takes over once again. You must check in and approve the changes to have them go live in the enterprise environment.

For information about restoring inks, see Restoring links to a previous version on page 53.

To restore a previous version of an object using the GPOADmin console

1. Expand the **Version Control Root** node and select the required container.
2. In the right pane, select the required object, right-click and select **Show History**.

   You will see the name, type, version, action, account, date and comment pertaining to the history item.
3. Select the filtering options you want to apply.
4. To view the settings of a previous version, right-click the specific version you want, and click **View**.

   To view the difference in settings between two versions, select the versions using Ctrl + select, then right-click and click **Differences**.
5. Right-click the specific version you want to restore and click **Get**.

> **NOTE:** When you Get a previous version of a workflow disabled GPO, the major version number will be increased by one.
>
> The Get command replaces the settings in the working copy with those from the selected version. If the current object is not checked out, then the Get command will automatically perform a checkout, provided you have the required Edit right. If you do not have the Edit right then the Get option will not be available.
>
> If you are rolling back the links of a GPO whose domain is different to that of the SOM to which it is linked, that SOM would not be available in the dialog box for management.

6. Enter a comment if required.

   You can choose to restore GPO Links. For more information, see Restoring links to a previous version on page 53.
7. Click **OK**.
8. Click **Close**.

To restore a previous version of a GPO using the GPMC Extension

1. Select the GPO and click **Show History**.

   The history displays in the bottom pane of the GPO Management tab. You will see the name, version, action, account, date and comment pertaining to the history item.

2 To view the settings of a previous version, select the version, right-click it and select **View**.

   To view the difference in settings between two versions, select the versions using Ctrl + select, then right-click and click **Differences**.

3 Right-click the version you want to restore and click **Get**.

NOTE: When you Get a previous version of a workflow disabled GPO, the major version number will be increased by one.

The Get command replaces the settings in the working copy with those from the selected version. If the current object is not checked out, then the Get command will automatically perform a checkout, provided you have the required Edit right. If you do not have the Edit right then the Get option will not be available.

4 Enter a comment if required.

   You can choose to restore GPO Links. For more information, see Restoring links to a previous version on page 53.

5 Click **OK**.

Restoring links to a previous version

You can restore the links between a GPO and its Scopes of Management, either to the last backup settings or to a specific history version that you select.

The affected Scopes of Management must be in the Available state, and the user must have rights to edit the SOMs, as well as the Link right, to restore the links. For more information, see Configuring role-based delegation on page 19.

To restore links to a previous version using the GPOADmin console

1 Expand the **Version Control Root** node and the required container.

2 Right-click an object and select **Show History**.

   You will see the date, account, version, comment, and applicable action that generated the history item.

3 Select the version you would like to restore, right-click and select one of the following:

   To restore just the links, select **Restore Links**.

   To restore the object and the links together, select **Get** and then select the **Restore GPO Links** in the Comment box.

4 In the **Restore Links** box, you can review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

   Hover over a link to get more information. If a link has an exclamation mark beside it, the Scope of Management Object is not Available.

5 Click **OK** and close the History box to complete the restore.

   At this point the modified SOMs, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

NOTE: You may need to right-click the object and select Refresh to ensure that you see its updated Status.

You can also restore Scope of Management links when rolling back a noncompliant GPO and when restoring a deleted GPO. For more information see, Checking compliance on page 59.

To restore links to a previous version using the GPMC Extension

1 Check out the Group Policy Object you want to restore.

2 Select the object and in the toolbar above, select **Show History**.

You will see the date, account, version, comment, and applicable action that generated the history item in a list below the Group Policy Objects list on the right.

3 Select the version you would like to restore, right-click and select one of the following:

To restore just the links, select **Restore Links**.

To restore the object and the links together, select **Get** and then select the **Restore GPO Links** in the Comment box.

4 In the **Restore Links** dialog box, you can review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

5 Click **OK** and close the History box to complete the restore.

At this point the modified SOMs, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

Managing your links with search and replace

You can select a GPO that is currently linked to an OU and search for all occurrences of that link, then choose to replace, remove, or append anywhere that GPO is linked. This can also be done manually, but the Search and Replace is faster and it ensures all links are included.

NOTE: You must have the link right on each GPO and SOM you wish to manage.

To append links

1 Expand the node containing the GPO that you wish to manage and select it, then right-click the GPO and select **Search and Replace**.

2 To append the new links, leaving the original links intact, select **Append**.

You will be asked to select the second GPO in the next step.

3 Click **Next**.

4 Expand the tree to select the GPO to append, then click **Next**.

The **Review Links** panel now shows you the links with color coding. Red links are marked for deletion, green links are marked for addition and yellow links indicate that an attribute of the link has changed. If you notice at this point that you have made an error, click **Back** or **Cancel** to undo the proposed changes.

5 Right-click a link to change its link order, to remove it, or to set other properties.

6 Click **Finish**.

To replace links

1 Expand the node containing the GPO that you wish to manage and select it, then right-click the GPO and select **Search and Replace**.

2 To replace the links to the SOMs, select **Replace**.

You will be asked to select the second GPO in the next step.

3 Click **Next**.

4 Expand the tree to select the replacement GPO, then click **Next**.

The **Review Links** panel now shows you the links with color coding. Red links are marked for deletion, green links are marked for addition and yellow links indicate that an attribute of the link has changed.If you notice at this point that you have made an error, click **Back** or **Cancel** to undo the proposed changes.

5 **Right-click** a link to change its link order, to remove it, or to set other properties.

6 Click **Finish**.

To remove links

1. Expand the node containing the GPO that you wish to manage and select it, then right-click the GPO and select **Search and Replace**.
2. To remove the links, select **Remove**.
3. Click **Next**.

   The **Review Links** panel now shows you the links with color coding. Red links are marked for deletion, green links are marked for addition and yellow links indicate that an attribute of the link has changed. If you notice at this point that you have made an error, click **Back** or **Cancel** to undo the proposed changes.
4. **Right-click** a link to change its link order, to remove it, or to set other properties.
5. Click **Finish**.

Working with objects pending approval and deployment

Only users with the Deploy permission can make the changes go live in the enterprise. The approval system safeguards the enterprise environment from any unauthorized live changes that could cause unwanted results. For more information on delegating permissions, see Configuring role-based delegation on page 19.

The types of requests from users that require approval are

- Changes to offline objects that are required to go live
- Creation of new objects
- Deletion of existing objects

NOTE: Using the Export Wizard, you can test GPOs offline before they are implemented in the live enterprise. For more information, see Exporting and importing on page 67.

NOTE: You can view a list of all objects Pending Deployment or Approval in the Search Folders in the GPOADmin console.

For more information, see Selecting security, levels of approval, and notification options on page 38, Approving and rejecting edits on page 57, and Scheduling deployment on page 58.

Enhanced workflow approval

You have the option of implementing a further safeguard by designating and modifying multi-level approvers. With this option, the required approvals at all levels must be granted before an object becomes available for deployment in the live environment.

Not everyone in a named group has to approve, just the required number. For example there may be 10 members in Group B but we may require only 3 approvals from that group to satisfy our requirements.

When you create a role within GPOADmin, you now have the option of empowering that role with the **Modify Approval Workflow** permission.

To grant Modify Approval Workflow permission

1. Select the forest node, right-click and select **Properties.**
2. Open the **Roles** tab and select **Add New Role**.
3. Type the name of the new role and click **Next.**
4. Scroll down the list of permissions and select the **Modify Approval Workflow** check box.
5. Once you have granted all relevant permissions, click **Finish**, click **Apply** and then **OK**.

NOTE: You can view an existing role's rights by selecting the role, selecting **View Role**, opening the **Rights** tab, and noting the permissions that have been grated.

Use caution granting this permission. A user with this permission can add, modify or delete the approval workflow a requested change must follow before it modifies the live environment.

Changing the approval workflow

To change an approval workflow

1. Select a version control container or object, right-click and select **Properties.**
2. Open the **Approvals** tab and select the workflow type you want to manage.

   Approval workflows can be set for object creations, deletions, and modifications.

To add a level of approval

1. Click **Add** to select a user or group.
2. Use the arrow keys to the left of the dialog box to alter the order in which the approvals must take place.

   If a group is selected, you must specify how many members of that group must approve the item before it can proceed to the next stage.
3. Once you have all steps added to the new workflow, click **Apply**, then **OK**.

To delete a level of approval

1. Click the "**-**" button to the right of the level of approval you do not want.

NOTE: Be certain you want to remove the level as there is no step to ensure you have chosen the correct level - it is removed as soon as you click on the "-" button.

2. Use the arrow keys to the left of the dialog box to alter the order in which the approvals must take place.
3. Once you have all steps added to the new workflow, click **Apply**, then **OK**.

To modify a level of approval

1. Follow the steps above to add or delete steps in the workflow.
2. Where you have selected a group as part of the approval workflow, you can change the value in the Approval Count Window to modify the number of members of that group who must agree to the change before it proceeds to the next level of approval.
3. Use the arrow keys to the left of the dialog box to alter the order in which the approvals must take place.

   The approvals will be handled from top to bottom of the displayed table.
4. Once you have modified the workflow, click **Apply**, then **OK**.

Withdrawing approval

Before the final approval has been made and the changes have been deployed, any approver has the right to withdraw their approval. When any approval is withdrawn, the process begins again from the start.

Approving and rejecting edits

Once an object has been checked in and the Approver has been notified that the offline changes are ready for approval, the changes are either approved or rejected.

NOTE: Before the approval of a change takes effect, the Version Control system detects if an object was changed unknowingly or outside the scope of the system (such as through native tools) and prompts the approver with the appropriate action to take. They can choose to overwrite the object or leave it as is.

Table 8. Approving Changes

If the changes are approved and deployed	If the changes are rejected
• The settings are applied to the live object and its major version number is incremented. (For example, v2.0) • The settings from the offline object are applied to the live object. • The next time a check out occurs, the process repeats of creating a new offline copy of the live group policy object.	• Nothing happens and the status is set back to an available state so it can be checked out again. **NOTE:** If the changes are only approved but not deployed, their status is changed to Pending Deployment and those GPOs can be seen in the Pending Deployment search folder.

To approve edits in the GPOADmin console

1. Expand the **Version Control Root** node, and the required container.
2. Right-click a controlled object in the Pending Approval state, and select **Approve**.
3. Enter a comment and click **OK**.

   If you have the required permission, you can deploy the updates to the enterprise at this time. If not, the object will be set to the Pending Deployment state. For information on deploying objects, see Scheduling deployment on page 58.

To approve edits in the GPMC Extension

1. Click the GPO in the Pending Approval state, and click **Workflow | Approve**.
2. Enter a comment and click **OK**.

To approve or reject edits through email

1. If this option has been configured by the administrator (see Configuring the Version Control server on page 14), approvers will receive an email with the subject line “Approval Request Notification”.

   The email contains a Settings report that you can review before making your decision.
2. Click to **Approve** or **Reject** and enter a comment as the body of the new email message to perform the selected action for the requested changes.

To reject edits in the GPOADmin console

1. Expand the **Version Control Root** node, and the required container.
2. Right-click a controlled object in the Pending Approval state, and select **Reject**.
3. Enter a comment, and click **OK**.

To reject edits in the GPMC Extension

1. Right-click the GPO in the Pending Approval state, and click **Workflow | Reject**.
2. Enter a comment, and click **OK**.

Scheduling deployment

Deploying changes within the system is a critical process that affects the live environment. To minimize the impact of disruption, this process should be done during a time period when the impact to users is minimal as the changes may alter the behavior of particular systems.

To reduce any issues, you can schedule the deployment of the changes for a specific date and time that best suits your needs. You can also schedule a deployment based on a different time zone, for example if the client is not in the same time zone as the server and you want to deploy based on the client's time zone.

If you have multiple approvers:

- Scheduling will only be available during the final approval and deployment.
- If the scheduled approval fails due to non-compliance or for any other reason, the Deployer will be notified.
- Only the Deployer can cancel the scheduled deployment.

NOTE: Before you deploy a GPO, ensure that it is not cloaked. If you deploy a cloaked GPO, and then later deploy it uncloaked, it will be flagged as noncompliant.

To deploy an approved object using the GPOADmin console

1. Expand the **Version Control Root** node, and the required container.
2. Right-click an object in the Approved state, and select **Deploy**.
3. Enter a comment.
4. Select the deployment time frame and click **OK**.

   You have the option to deploy the changes immediately or at a specified time.

   If you select Schedule deployment for a later date, set the date and time, select an appropriate time zone if required, enter a comment, and click **OK**.

   After you have scheduled a time, a clock icon appears beside the object and the Deployment Time column reflects the scheduled deployment.

NOTE: If a scheduled deployment fails for any reason, the deployment is cancelled and the object remains in the Pending Deployment state.

To deploy an approved GPO using the GPMC Extension

You can only deploy GPOs using the GPMC Extension. To deploy SOMs or WMI filters, use the GPOADmin console.

1. Select the approved GPO and click **Workflow | Deploy**.
2. Enter a comment.
3. Select the deployment time frame, including a time zone if required, and click **OK**.

To reschedule a deployment using the GPOADmin console

1. Right-click the required controlled object and select **Deploy**.
2. Select the date and time, select an appropriate time zone if required, enter a comment, and click **OK**.

To reschedule a deployment using the GPMC Extension:

1. Select the GPO and click **Workflow | Deploy**.
2. Select the date and time, select an appropriate time zone if required, enter a comment, and click **OK**.

To cancel a deployment using the GPOADmin console

- Right-click an object in the Pending Deployment state and choose **Cancel Deployment.**

  Right-click an object in the Pending Deployment state and choose **Deploy**. Select **Cancel pending deployment**.

To cancel a deployment using the GPMC Extension

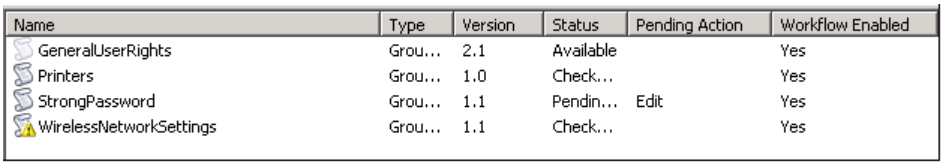
- Select the GPO in the Pending Deployment state and click **Workflow | Cancel Deployment.**

  Select the GPO in the Pending Deployment state and click **Workflow | Deploy,** then select **Cancel pending deployment**.

Checking compliance

GPOADmin provides two options to determine if an object has been changed outside the scope of the system in the live enterprise environment. You can manually check any object for compliance (GPOs, Scopes of Management, and WMI filters), and you can let the GPOADmin Watcher Service detect unauthorized modifications to GPOs and Scopes of Management. For more information on configuring the Watcher service, see the GPOADmin Quick Start Guide.

If you are running the Watcher Service, noncompliant GPOs and Scopes of Management are automatically flagged with a yellow exclamation point, regardless of their status:



Name	Type	Version	Status	Pending Action	Workflow Enabled
GeneralUserRights	Grou...	2.1	Available		Yes
Printers	Grou...	1.0	Check...		Yes
StrongPassword	Grou...	1.1	Pendin...	Edit	Yes
WirelessNetworkSettings	Grou...	1.1	Check...		Yes

NOTE: To ensure that you are notified immediately of noncompliant GPOs and Scopes of Management, make sure the Watcher Service is running.

NOTE: You can view a list of all objects that have been flagged as noncompliant in the Unauthorized Modifications Search Folder in the GPOADmin console.

NOTE: When the Watcher Service detects a noncompliant GPO and Scopes of Management under version control, it creates a backup of the change and increases the minor version number by one. If the noncompliant GPO is Workflow Disabled, it creates a backup of the change and increases the major version number by one. For details on enabling or disabling workflow, see Enabling/disabling workflow on page 48.

If a delta is determined between the last historical backup and the live object, a user with the appropriate permissions will be able to either:

- Roll back: Restore the object in the live environment from the most current backup found in the system to overwrite the unauthorized live change.
- Roll back with Links: Restore a Group Policy Object in the live environment from the most current backup, including its links to Scopes of Management, and overwrite the unauthorized live change.

  You can also roll back links from a different history version. For information, see Restoring links to a previous version on page 53.
- Incorporate Live: Accept the live changes as being authorized and more up-to-date than what is currently already in the system. This will automatically back up those changes into the system and increment the version number of the backup to the next major number.
- Leave the live object alone in its noncompliant state.

NOTE: If the change to the live environment occurs while the GPO is checked out, when you check it in you can choose which version of the GPO to accept.

If an object has been deleted in the live environment, a user with the appropriate permissions will be able to:

- Restore the object in the live environment
- Restore a Group Policy Object in the live environment and restore its links to Scopes of Management.
- Unregister the object from the Version Control system

NOTE: If a SOM has been deleted, you will only have the option to Unregister.

To check if any registered objects have been changed since their last backup

1. Right-click the required object in the Available state and select **Check Compliance**.
2. Right-click the **Version Control Root** node or subcontainer, and select **Check Compliance**.

NOTE: If you are using the GPMC Extension you can select the GPO and click Workflow | Check Compliance.

3. Click **Next** to run the compliance check.

   The objects that are not compliant are displayed.
4. Select the required course of action by clicking in the Action field to open the list of options, and click **Next**.
5. If you are restoring GPO links, select the **More** (**...**) button to see the details of the links you will be restoring.

   In the Restore Links box, you can review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.
6. Click **OK** save the Restore Links settings.
7. Click **Finish**.

   At this point the modified SOMs affected by the restored links, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

NOTE: If you attempt to deploy a noncompliant compliant GPO, you have the option of running the Compliance Wizard or proceeding with the deployment.

To make a flagged GPO compliant

1. Right-click the noncompliant GPO and choose one of the following
   - Incorporate Live
   - Rollback

   If you choose Incorporate Live, you cannot restore links.
2. Enter a comment and click **OK**.
3. Select the **Restore GPO Links** option in the Comment box.
4. In the **Restore Links** box, review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

   Hover over a link to get more information. If a link has an exclamation mark beside it, the Scope of Management Object is not Available.
5. Click **OK** save the Restore Links settings.

   At this point the modified SOMs affected by the restored links, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

To restore a deleted GPO with links

When a Group Policy Object is deleted in the live environment, its status shows as Noncompliant - Deleted in GPOADmin.

1. Right-click the noncompliant GPO and select **Restore**.
2. Select the **Restore GPO Links** option in the Comment box.
3. In the Restore Links box, review the settings that will be restored (right side) and use the toolbar buttons at the top to change the link order, remove links, or set other group policy properties.

   Hover over a link to get more information. If a link has an exclamation mark beside it, the Scope of Management Object is not Available.

4 Click **OK** save the Restore Links settings. At this point the modified SOMs affected by the restored links, if registered, are put into a Pending Approval State. If not registered, the changes are made in the live environment.

Editing objects

- Editing GPOs
- Applying templates
- Editing WMI filters
- Linking GPOs
- Importing INF file settings

Editing GPOs

Once you have a GPO checked out, you can edit its settings within the Group Policy Editor, create security and WMI filters, and enable/disable computer and user settings.

Because you can only link GPOs to sites, domains, and OUs, setting up security filters helps you to refine the application of GPO settings to a group, user, or computer.

NOTE: The users and computers that you select while setting up security filtering must have both Read and Apply Group Policy (AGP) permissions on the GPO.

When you check out a GPO, the changes you make are to a copy of the live GPO. The changes that you make do not affect the GPO settings in the enterprise until it is approved and deployed.

NOTE: You can also edit GPOs by applying templates. GPOs must be checked out before you can apply a template to them. When you apply a template to a GPO, you will be applying the major version stored within the Version Control system. For more information, see Applying templates on page 62.

To edit GPO settings

1 Right-click a checked out GPO, and select **Edit**.

2 Click **Launch Editor**, make the required changes, and close the Group Policy Editor.

When you register GPOs, the GPO status (Enabled/Disabled Computer and User settings) will be maintained. However, if required, you can also easily change these settings from within the Version Control system.

3 Select or clear the user and computer setting options as required.

4 If required, select the Security tab and click **Add**, enter or search for the required user, computer, or group, and click OK.

To change the current security filters, select the required entry, and click **Remove**.

5 Click the **Advanced** button to select advanced permissions.

6 To link the GPO to a pre-existing WMI filter in the domain, select the WMI Filter tab and choose the filter from the list.

Upon approval the link will be added to the GPO.

To remove any existing WMI filtering select **None.**

If the GPO was previously linked to a WMI filter, the GPO will be unlinked from the filter upon approval.

7 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. See Checking in controlled objects on page 51 and Requesting approval on page 50 for more information.

Removing persistent registry settings

Some GPO settings create registry entries when they are processed. When these settings are removed and the policy is processed, their corresponding registry entries may not be removed from client computers.

GPOADmin notifies you when potentially persistent registry values exist and allows you to remove them.

NOTE: Because this option removes registry data when the policy is processed, you must take care to ensure that you do not remove settings set by other policies.

To remove these settings

1. Right-click a checked out GPO, and select **Edit**.
2. Click the **Registry Cleanup** button.

   The registry settings that persist as a result of removing GPO settings will display. Settings that are unavailable will never persist as the Group Policy processing engine resets these settings before processing the GPO.
3. Select the registry settings that you want to remove when the policy is re-processed, and click **OK**.

Applying templates

Templates can be applied only to registered GPOs within the Version Control system. When you apply a template, changes are made to the GPO settings; therefore, they must go through the same approval process as all other changes made to GPOs within the system. The workflow is as follows:

- Check out the GPO
- Apply a template
- Check in the changes to the system

NOTE: Checking for Conflicting Template Settings

GPOADmin checks for conflicting template policy settings when you either create a new GPO and apply templates to it, or when you select a GPO that has already been created and select to apply a template. If two or more templates are selected, a dialog box will open and you will have the option to skip checking for conflicts.

If conflicts are found, you can choose to continue with the understanding that the last template's settings will win. You can view the details of the conflicting settings by clicking the Details button, which opens the Template Conflict Report.

NOTE: You must apply a template to an existing GPO or edit a template using the GPOADmin console.

NOTE: GPOADmin does not support the use of templates on Windows® 7, Windows Server 2008, and later. The support on earlier Windows operating systems is also limited.

For information on creating templates, see Creating templates on page 42.

To apply a template

NOTE: You must apply a template to an existing GPO using the GPOADmin console.

1. Expand the required container, right-click the checked out GPO, and select **Templates | Apply Templates**.

2 Click **Add** to select one or more templates.

   If you have more than one template selected, you can use the Up and Down buttons to select the order in which the templates will be applied. The order of application is from top to bottom.

3 Click **OK**.

NOTE: Once a template is applied the settings cannot be removed without undoing the checkout.

Editing templates

Changes made to the template settings must be applied to the GPO to take affect. For more information on applying templates, see Applying templates on page 62.

NOTE: You must edit templates using the GPOADmin console.

NOTE: GPOADmin does not support the use of templates on Windows® 7, Windows Server 2008, and later. The support on earlier Windows operating systems is also limited.

To edit a template

1 Expand the **Version Control Root** and the required container.

2 Right-click the required template and select **Edit**.

3 Click the **Details** tab and click **Add**.

4 Select the required policies and click **Add or Remove**.

   Select the policy, click **Modify** to configure the policy settings, enter the requested information, and click **OK**.

5 Click **OK** once you have added all the required policy settings.

Editing WMI filters

NOTE: You must edit WMI filters using the GPOADmin console.

To edit a WMI filter

1 Expand the **Version Control Root** and the required container. Select the WMI filter you want to edit within the version control container node in which it exists.

2 Right-click the WMI filter and select **Edit**.

3 Edit the settings of the WMI filter.

4 Click **OK**.

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

For information on creating WMI filters, see Creating WMI filters on page 42.

Linking GPOs

Once GPOs have been created and configured, they must be linked to the appropriate sites, domain, or OU. Before you can link a GPO, you must register and check out the site, domain, or OU. For information on registering Scopes of Management, see Registering objects on page 33.

Users with the Link right can link a single GPO with numerous sites, domains, or OUs and link multiple GPOs to a site, domain, or OU. (For more information on setting permissions, see Configuring role-based delegation on page 19.)

If you link more than one GPO, you must pay attention to their order. The first GPO has the highest precedence because it is processed last. The Link Report and Group Policy Results Report can help you understand the inheritance structure of your group policies.

NOTE: The policies are applied according to the hierarchical structure of Active Directory®. You can change the order in which the GPO is applied through the provided arrows.

NOTE: You must have the Link right on each GPO and SOM to which you wish to link.

By default, GPOs affect all users and computers contained within a linked site, domain, or OU. To refine the application of a GPO, see Editing GPOs on page 61.

To link GPOs to a single site, domain, or OU

1. Right-click a checked out site, domain, or OU and select **Edit**.
2. Click **New Link** to add another GPO.
3. Select the appropriate option to either Enable or Enforce the GPO link.
4. Enable **Block Inheritance** if required.

   You must have the Block Inheritance right to enable this option.
5. Click **OK**.

To link multiple GPOs to multiple sites, domains, or OUs

1. Right-click one or more GPOs and select **Link**.

   Any SOMs that you want to link the GPOs to must be in the available state.
2. In the left pane of the Link dialog box, expand the domains and select the SOMs you want to link to.
3. In the right pane, ensure that the **Add** check box is selected for the GPOs you want to link.
4. Select the appropriate option to either Enable or Enforce the GPO link. You can use the arrows provided to modify the link order.
5. Click **OK**.

You can also rollback pre-existing links between GPOs and sites, domains, and OUs when restoring GPOs. For information, see Restoring links to a previous version on page 53 and Checking compliance on page 59.

Importing INF file settings

You can easily import security policy settings from an INF file into a template, then edit the template, and apply it to GPOs.

NOTE: You must import INF File Settings using the GPOADmin console.

To import INF files

1. Right-click the **Version Control Root** node or required container, and select **Import INF file**.
2. Select the required file and click **Open**.

Synchronizing GPOs

Synchronizing GPOs allows you to automatically push out pre-defined “master GPO” settings to specified targets both within a forest and between two forests. This allows you to ensure specific GPOs, which are required in every domain, contain the same settings without having to link to a GPO outside of the domain.

You will be able to select one or more GPOs from various domains as synchronization targets for the source GPO. When the source GPO has been successfully deployed, the settings from the last major backup will be imported into each synchronization target GPO.

NOTE: If permissions between forests are not identical, a mapping table is also available to ensure that forest specific settings are covered.

The ability to synchronize GPOs require that:

- It is enabled within the source domain.
- The source GPO must be workflow-enabled to ensure that any changes can be propagated to the targets. (The targets, however, can be workflow-disabled.)
- Targets are registered.
- The source GPO has been deployed at least once.
- Target synchronization settings are configured.
- Each domain has a GPOADmin server. Child domains of a parent domain will appear in the client by default. Trusted siblings however will not.
- The user performing a manual synchronization or setting the synchronization targets has the Synchronize right.

To enable GPO synchronization

1. Right-click the forest and select **Properties**.
2. Select the **Options** tab.
3. Select **Enable Group Policy Object Synchronization.**
4. Click **Apply** or **OK**.

   Once this has been enabled, you can access the synchronization options by right-clicking a GPO in the Version Control Root and selecting **Synchronize**.

Working with GPO synchronizations

Keep the following in mind when working with synchronizations:

- The target settings will be overwritten with the settings from the source.
- If a synchronization is attempted while a target GPO is checked out, the synchronization will fail.
- If a target is off line, the synchronization will fail.
- If the source GPO is out of compliance and either a ‘Rollback’ or ‘Incorporate Live’ compliance action will trigger a synchronization.
- Communicate synchronizations plans to those responsible for GPO administration in other domains.
- If GPO synchronization is enabled on a targeted GPOADmin server, ensure that the target GPO does not have the source GPO set as a synchronization target. Doing so will place the two GPOs in an endless synchronization loop.
- When changing the service account, any existing GPO synchronization configuration should be reconfigured to ensure the proper password is used to connect to the target GPOADmin server.

To set up synchronization

1 In the **Version Control Root**, right-click the source GPO, and select **Set Synchronization Targets**.

This will open a dialog where you can add GPO targets and configure their synchronization settings. By default, the server that you are currently connected to will be displayed. It cannot be removed.

2 If required, select **Add Servers** to include other servers that contain the GPOs that you want to target. Select the server and click **Connect**. Enter the required credentials and click **OK**.

NOTE: The credential entered will be stored and used to connect to the associated server during the synchronization process.This allows for the synchronization of GPOs between untrusted domains. If Auto Deploy is to be used, it is recommended that this account is a member of the GPOADmin Administrators as they are the only ones who can Approve multiple times.

You can also select to remove any servers that have been added. If you do however, any target GPOs setup from this server for synchronization will also be removed.

3 Right-click in the dialog and select **Add Synchronization Target** to select the required target GPOs. The list of all available GPOs will display.

4 Select the required targets and click **OK**.

5 If required, we provide the option to setup a migration table by right-clicking the target and choosing **Select Migration Table**. From here, you can add (or remove), create, modify the migration tables that are going to be used during the synchronization using the Microsoft Migration Table Editor.

The migration tables, which are xml files, contain the mapping between the source and the target accounts to ensure they have the same access. If permissions are not an issue, the migration table would not be required. It is stored in Program files | Dell | GPOADmin | MigrationTables.

You are now ready to set the synchronization options.

6 Right-click the target to set the synchronization options. You can choose between the following:

- Auto Deploy: If enabled, the target will be automatically checked out, the settings will be imported, the approval process will run and the GPO will be deployed. If not enabled, the GPO will remain checked out.
- Use Migration Table Exclusively: If enabled, the migration (import operation) will not proceed if any settings security principals or UNC paths configured within the source GPO do not exist in the migration table.
- Migrate Security Filters: Migrates any security principals from the security filter that are found in the migration table.
- Clear Migration table: Clear the tables when no longer required.

7 Once you have your targets set, it is recommended to validate the synchronization targets by selecting the target GPO and clicking **Validate Synchronization Targets**.

The synchronization targets are stored using their version control id and their display name. Over the course of time, the name may change or the object may be deleted. During the validation a connection to the target server is made and a check is performed to see if the synchronization target still exists or if the name has changed.

If there is an issue, the target will be displayed with warning icon and a tool-tip to inform you of the issue.

1 If you select to **Cancel the editor, t**he warning will not persist.

2 If you select **OK**, the warning will remain to alert you that the issues must be addressed. When ready to address the issue, simply select the **Correct** button at the top of the dialog or right-click and select **Correct.**

To perform a manual synchronization

- In the **Version Control Root**, right-click the source GPO and select **Synchronization Now**.

This allows you to perform a synchronization without redeploying the source GPO.

Generating Synchronized GPO report

You can create a report that contains information on the GPO synchronizations that have been performed in your environment.

For details see the section To create troubleshooting reports on page 80.

Exporting and importing

Export objects

Using the Export Wizard, you can test objects offline before they are implemented in the live enterprise. A typical scenario would be to:

- Check-out an object and make the desired changes.

  Before you check in the change and request approval, you can test the edits.
- Export the object to another domain and test the updates.

  If you see an issue you can change it in the test domain.
- Import the object.
- Check in the new and improved changes for approval.

  NOTE: In the Pending Approval state, exporting the object provides an additional level of quality control before changes are made live in the enterprise.

The following built in roles can perform an export:

- Moderator
- System Administrator
- User

Alternatively, you can create a custom role that includes Read and Export rights.

Migration table considerations

- When migrating to an untrusted domain, the source entries must be SIDs and the Source Type must be set to Free Test or SID.
- When migrating to a trusted domain, the source entries must be in domain\account format.
- When migrating to the same domain, the entries can be in a UNC format (email style).
- If an account cannot be mapped, it is logged in the format that GPMC is looking for.
- If an entry is logged, change the source format to the format that is logged and try again.

To export objects to a test environment

1. Select the number of objects you want to export, either by using **Ctrl** + click to select multiple items, or **Shift** + click at the top and bottom of a contiguous series of items to select them all.
2. To export a single object, right-click the object.

3 Select **Export**.

> **NOTE:** If you are using the GPMC Extension, you can also select the GPO and click **Workflow | Export**.

4 Select the version that you want to export and click **Next**.

5 Select the target.

You can select a local directory or network share, another version control system, or a test domain in the live network.

To select a local directory or network share:

- Select **A backup on disk** and click **Next**.
  - Select the backup directory and click **Next**.
  - Click **Finish**.

To select another Version Control system

- Select a Version Control Server and click **Next**.
  - Select a Target Folder and click **Next**.
  - Select a Version-Controlled Domain and click **Next**.
  - Select a migration table, if required, and click **Next**.

    > **NOTE:** You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

To select a test domain in the live environment

- Select **The live environment** and click **Next**.
  - Select the target domain and click **Next**.
  - Select a migration table, if required, and click **Next**.

    > **NOTE:** You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

Once you have reviewed the settings and the effects on the target domain, check in the object and request Approval. For more information, see Requesting approval on page 50.

Import objects

Using the Import Wizard, you can import objects from a local directory or network share, another version control system, or a version in the live network.

Migration table considerations

- When migrating to an untrusted domain, the source entries must be SIDs and the Source Type must be set to Free Test or SID.
- When migrating to a trusted domain, the source entries must be in domain\account format.
- When migrating to the same domain, the entries can be in a UNC format (email style).
- If an account cannot be mapped, it is logged in the format that GPMC is looking for.
- If an entry is logged, change the source format to the format that is logged and try again.

To update an object in the Version Control system

1 Right-click an object and select **Import**.

> **NOTE:** If you are using the GPMC Extension you can also select the GPO and click Workflow | Import.

2 Select the import source.

If you select a local directory or network share:

- Select **A backup on disk** and click **Next**.
  - Select the backup directory and the backup that you want to import, and click **Next**.
  - Select to use the migration table if required, and click **Next**.

> **NOTE:** You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

If you select another version control system:

- Select **A version control system** and click **Next**.
  - Select the Version Control server and click **Next**.
  - Select the object that has the settings that you want to import and click **Next**.
  - Select the version of the controlled object that you want to import and click **Next**.
  - Select to use the migration table if required, and click **Next**.

> **NOTE:** You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

If you select a version in the live environment:

- Select **The live environment** and click **Next**.
  - Select the domain and the object with the settings you want to import and click **Next**.
  - Select to use the migration table if required, and click **Next**.

> **NOTE:** You also have the option to use the migration table exclusively and to migrate the security filter.

  - Click **Finish**.

4

Creating Reports

- Available reports
- Controlled object reports
- Diagnostic and troubleshooting reports
- Live, working copy, latest version, and differences reports
- Historical Settings Reports
- Working with report folders

Available reports

You can generate report templates for quick real-time reporting purposes, as well as simple point-in-time reports for historical reasons.

Report templates are saved as XML files and historical reports are saved as HTML files.

NOTE: If you change regional options on your local machine, restart the GPOADmin client to ensure your changes are reflected in your reports.

To create a report template

NOTE: You must use the GPOADmin console to create report templates.

- Run the report wizard and select to save the report settings to a file.

  You can double-click the report template to generate a report or right-click the report from within the Reports folder, and select **Run**.

To create a Historical report

- Run the report wizard and enter a unique filename in the "Save report settings to file" file.

  You can double-click the report to view the saved version or right click the report and select **Run**.

The available reports include:

- Controlled object reports
- Diagnostic and troubleshooting reports
- Live, working copy, latest version, and differences reports
- Historical Settings Reports

NOTE: If you are using the GPMC Extension, you only have access to the History, Latest Version, Working Copy, Live, and Differences Reports.

Controlled object reports

Settings Report

This report generates a settings report for a controlled object. The settings retrieved for the selected object or objects will be displayed in the report.

Difference Report

This report shows the difference between versions of one or more objects of the same type in the Version Control system. It allows you to compare a base object and version with one or multiple other objects. Each separate comparison will appear in a different tab when the report is displayed.

History Report

This report shows all historical actions performed on an object in the Version Control system.

Group Policy Object Settings Search Report

This report executes a text search against Group Policy Object settings for names and values. The most recent version of the GPO is searched for any details containing the text string you have submitted.

User Activity Report

This report shows all actions performed by specified users in the Version Control system.

Compliance Report

This report shows which items in the live environment are not compliant with the latest major version stored in the Version Control system. The categories of changes from the stored version are highlighted, to provide a quick compliance overview.

Template Conflict Report

This report details any settings that will be overwritten when applying a list of templates to a GPO. You can select more than one template and quickly view the different settings, allowing a cleaner and more reliable application of changes.

Change Auditor™ Report

This report shows Change Auditor events for a set of objects. Change Auditor is a comprehensive, low level auditing tool that bypasses native auditing mechanisms and provides a more robust audit trail. To run Change Auditor reports, you must have Change Auditor installed (version 5.5), and the GPOADmin service account must be added to the Change Auditor Administrators group.

When a user logs into GPOADmin and deploys a change to the live environment, those changes are actually made on their behalf by the GPOADmin service account. With Change Auditor version 5.7, you can see more information about that user in the Initiator Username, Initiator SID (if the name cannot be resolved), and Comment columns of this report. This information is also available in the Change Auditor client.

NOTE: If the Change Auditor coordinator is installed after GPOADmin, you need to restart the GPOADmin service. The Change Auditor agent may take a few minutes to refresh its configuration or you can manually restart it.

NOTE: The Change Auditor report shows changes made in the live environment only.

Change Auditor™ Working Copies Report

This report shows Change Auditor events for any edits made to a checked-out working copy of a GPO. To run this report, you must have Change Auditor 5.7 installed, and the GPOADmin service account must be added to the Change Auditor Administrators group.

Deployment Report

This report displays the deployment details for all object types and gives you the option to view deployments within a specified date range.

To create Controlled Object Reports

NOTE: You must use the GPOADmin console to create Controlled Object Reports.

1. Expand the **GPOADmin** node.
2. Right-click **Reports** and select **New | Report**.
3. Select the type of report to run.

NOTE: Checking for Conflicting Template Settings

GPOADmin checks for conflicting template policy settings when you either create a new GPO and apply templates to it, or when you select a GPO that has already been created and select to apply a template. If two or more templates are selected, a dialog box will open and you will have the option to skip checking for conflicts.

If conflicts are found, you can choose to continue with the understanding that the last template's settings will win. You can view the details of the conflicting settings by clicking the Details button, which opens the Template Conflict Report.

If you select...	procedure
Settings Report	1 Click **Next**. 2 Select the service that you want to report on and click **Next**. 3 Select the object you want to report on and click **Next**. 4 Select the version you want to report on and click **Next**. 5 Select to run the report or to save the report settings, and click **Finish**.
Difference Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the object, or objects you want to report on and click **Next**. 4 If you are comparing different versions of one object, select a Base version and then the Comparison versions. – OR – If you are comparing multiple objects, in the **Base** column, select the Base object that you want to compare the other objects to. In the **Version** column, select a version for each object to compare. 5 In the **Show** drop-down list, choose an option for which data to show in the report and click **Next**. 6 Select to run the report or to save the report settings, and click **Finish**. *If you have chosen to compare more than two objects, click the tab corresponding to the object you are comparing to the base object to see those differences.*

If you select...	procedure
History Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the object you want to report on and click **Next**. 4 Select to run the report or to save the report settings and click **Finish**.
Group Policy Object Settings Search Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the object you want to report on and click **Next**. If you want to report on all the Group Policy Objects contained in this container and all subcontainers, select the **Include subcontainers** check box. 4 Enter the setting name or value you want to report on and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
User Activity Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the user you want to report on and click **Next**. 4 Select to run the report or to save the report settings, and click **Finish**.
Compliance Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to run the report or to save the report settings and click **Finish**.

If you select...	procedure
Template Conflict Report	1 Click **Next**. 2 Select the service you want to report and click **Next**. 3 Click **Add** to view the list of templates available to include in the report. **Select** check boxes next to the templates you wish to compare and click **OK**. The templates will be added to the list view on the wizard page. You can alter the order in which the template application can be compared using the arrows on the right side of the window. **NOTE:** For more information, see Creating templates on page 42. 4 Once the list of templates is correct, click **Next**. 5 Select to run the report or to save the report settings, and click **Finish**.
Change Auditor™ Report	1 Select the service you want to report on and click **Next**. 2 Select the object you want to report on and click **Next**. 3 Select a time interval to report on, and click **Next**. 4 Choose the object you want to Group by, Sort by, and the Sort order, and click **Next**. 5 Select to run the report and/or to save the report settings and click **Finish**. 6 When you are finished with the report, click **Close**. You can also see Change Auditor information about objects on their Property pages, on the **Change Auditor™** tab (Viewing and editing object properties on page 46).

If you select...	procedure
Change Auditor™ Working Copies Report	1 Select the service you want to report on and click **Next**. 2 Select the objects you want to report on and click **Next**. 3 Select a time interval to report on, and click **Next**. 4 Select to run the report and/or to save the report settings and click **Finish**. You can see the changes made to the working copies under the Check Out section of the report. 5 When you are finished with the report, click **Close**.
Deployment Report	1 Select the domain you want to report on and click **Next**. 2 Select the object types to display as well as an optional date range and click **Next**. 3 Select to run the report and/or to save the report settings and click **Finish**. 4 When you are finished with the report, click **Close**.

Diagnostic and troubleshooting reports

FRS Troubleshooter Report

This report troubleshoots File Replication Service (FRS) replication problems on a domain controller.

FRS Event Log Report

This report retrieves events from the File Replication Service Event Log for the specified domain controller.

FRS Log Report

This report retrieves the File Replication Service log from the server, allowing troubleshooting of NTFRS replication problems.

FRS Parameters Report

This report retrieves FRS parameters from the registry for the specified domain controller.

Set NTFRS Parameters Reports

This report creates log files for troubleshooting NT File Replication Service (NTFRS) replication problems, allowing you to enable or disable logging and set logging options, such as location and limits.

SYSVOL Connectivity Report

This report checks for errors in connecting to and accessing the SYSVOL directory share.

Cross-Domain Linked Group Policy Objects Report

This report lists GPOs that are linked to a different domain. These links can slow down response time, so this report is useful in improving system performance.

Conflicting Objects Report

This report checks for replication conflicts in Active Directory® such as when an object is created on one domain controller and an object with the same name is created in the same container on another domain controller before replication occurs.

Group Policy Object Consistency Report

This report tests all the domain controllers in a given domain to ensure the Active Directory® and SYSVOL portions of all GPO's have replicated correctly and consistently.

Software Installation Package Report

This report shows a list of all GPOs that include software installation packages.

Linked/Unlinked Report

This report details GPOs that are linked to certain Scopes of Management and the GPOs that are not linked to anything.

Inactive Policy Settings Report

This report shows the registered GPOs that have settings defined within disabled user or computer sections.

Group Policy Object Security Report

This report details the security of GPOs, specifically where certain trustees are either present or not present.

GPO Synchronization Report

This report details the GPO synchronizations that have been performed in your environment.

Group Policy Results

This report shows the resultant set of policies (RSoP) for a given user or computer, or both.

Group Policy Results Difference Report

This report displays the resultant set of policies (RSoP) differences between the selected users or computers. The Group Policy Results Difference Report does not include the Remote Installation extension in the report settings.

Group Policy Modeling Report

This report displays the resultant set of policies based on the selected simulation options within the modeling session. You can use this report to simulate changes and validate that the results match the desired outcome before actually implementing any changes within your environment. Using this report, you can evaluate checked out GPO working copies so that you can mitigate any unexpected effects once the changes are made to the live version.

NOTE: This report will not function when delegating permissions for the service account.

IMPORTANT: An application partition is created during the simulation to house the report. It contains a temporary staging container that will be deleted once the report has been generated. The service account must have permissions to create an Application Partition in Active Directory.

If required, you can create or delete the staging application directory partition:

1. Open Command Prompt.
2. Type:

   ntdsutil
3. At the ntdsutil command prompt, type:

   domain management or partition management
4. At the domain management command prompt, type:

   connection
5. At the server connections command prompt, type:

   connect to server ServerName
6. At the server connections command prompt, type:

   quit
7. At the domain management command prompt, do one of the following:
   - To create an application directory partition, type:

     create nc dc=staging,dc=gpoadmin DomainController

     For every domain controller which might be used to run the Group policy modeling report on, type the following:

     add nc replica "dc=staging,dc=gpoadmin" DomainControllerName
   - To delete an application directory partition, type:

     delete nc dc=staging,dc=gpoadmin

To create troubleshooting reports

NOTE: You must use the GPOADmin console to create Troubleshooting Reports.

1. Expand the **GPOADmin** node.
2. Right-click **Reports** and select **New| Report**.
3. Select the type of report to run under Diagnostic and Troubleshooting Reports:

if you select...	procedure
FRS Troubleshooter Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select the domain controller(s) you want to report on and click **Next**. **NOTE:** The Configuration options link allows configuration of the DC if required. 5 Select to run the report or to save the report settings and click **Finish**.
FRS Event Log Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select the domain controller(s) you want to report on and click **Next**. 5 Select the events to display and, if required, specify a date range and click **Next**. **NOTE:** If no date is entered, all event data will be returned. 6 Select to run the report or to save the report settings and click **Finish**.
FRS Log Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select the domain controller(s) you want to report on and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
FRS Parameters Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select the domain controller(s) you want to report on and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.

if you select...	procedure
Set NTFRS Parameters Reports	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select the domain controller(s) you want to report on. **NOTE:** The Configuration options link allows configuration of the NTFRS parameters for the selected DC. You are required to set at least one option before proceeding with this report. 5 Click **Next**. 6 Select to run the report or to save the report settings and click **Finish**.
SYSVOL Connectivity Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select the domain controller(s) you want to report on and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
Cross-Domain Linked Group Policy Objects Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to run the report or to save the report settings and click **Finish**.
Conflicting Objects Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to run the report or to save the report settings and click **Finish**.
Group Policy Object Consistency Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to include the GPO ACL, SYSVOL, or SYSVOL Scripts folder in the report and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.

if you select...	procedure
Software Installation Package Report Linked/Unlinked Report Inactive Policy Settings Report	1 Click **Next**. 2 Select the service you want to report on, and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Select to run the report or to save the report settings, and click **Finish**.
Group Policy Object Security Report	1 Click **Next**. 2 Select the service you want to report on and click **Next**. 3 Select the domain you want to report on and click **Next**. 4 Specify accounts to include or exclude in the report and click **Next**. 5 Select to run the report or to save the report settings and click **Finish**.
GPO Synchronization Report	1 Select the service on which to run the report and click **Next**. 2 Select the GPO on which to run the report and click **Next**. 3 Select to run the report or to save the report settings and click **Finish.**
Group Policy Results	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next.** 3 Select the domain you want to report on and click **Next**. 4 Select the computer from where you want to display the policy settings and click **Next**. 5 Select the user whose policy settings you would like to view and click **Next**. 6 Select to run the report, save the report so that you can compare it to another report, or save the report settings, and click **Finish**.

if you select...	procedure
Group Policy Results Difference Report	1 Click **Next**. 2 If you are connected to more than one service, you will be asked "Which service do you want to run the report on?". Select a service and click **Next.** 3 Select the domain you want to report on and click **Next**. 4 Choose initial report to use in the comparison and click **Next**. You can choose between a new report, a dynamic report, or a previously saved report. If you choose to create a new report, you will need to click through the wizard to select the required user and computer. 5 Choose the second report to use in the comparison and click **Next**. You can choose between a new report, a dynamic report, or a previously saved report. If you choose to create a new report, you will need to click through the wizard to select the required user and computer. 6 Select the required display options and click **Next**. *You can choose to see all settings, differences only, or similarities only.* 7 Select to run the report or to save the report settings and click **Finish**.

if you select...	procedure
Group Policy Modeling Report	1 Click **Next**. 2 Select the domain and the domain controller where the RSoP report will be run, and click **Next**. You can select any domain controller or a specific domain controller within the domain with the supported operating system. 3 Browse to and select the required user or computer (or container that contains the user or computer), and click **Next**. 4 If required, you can select to: • Simulate a slow network connection. • Enable loopback processing. This option is only available if a computer has been selected. You can use this to narrow down the settings to be considered in the simulation and focus on only those of interest to you. If **Replace** is selected, ONLY computer GPOs and WMI filters will be considered for the simulation. If **Merge** is selected, all GPOs and WMI filters (user and computer) will be included. When being evaluated for the simulation, the computer GPOs will be placed with a higher precedence than the user GPOs. • Select to use a site other than the default site. Click **Next** when satisfied with your selections. 5 If required, browse to and select an alternate network location for the user or computer.This option is only available for users or computers - you cannot select this for containers. **Note**: You can select the **Restore to Default** option to return to the initial state. Click **Next** when satisfied with your selections. 6 The top level groups where the user or computer is a member will display. Select to see the effect of adding or removing users from groups as required. **Note**: You can only select to add immediate groups. Any group can be removed with the exception of the Authenticated Users and Everyone groups. Click **Next** when satisfied with your selections. 7 If required, select to see the effects of removing WMI filters. You can select to see all linked filters or choose specific filters. • **All linked filters**: This option assumes the user meets the criteria and all filters will be applied. • **Only these filters**: This option enables you to list all available filters and remove as required.

if you select...	procedure
Group Policy Modeling Report	**Note**: If you plan to alter GPO link properties, you should select the default **All linked filters**. If you select to include only select filters some changes may not be reflected in the simulation. Click **Next** when satisfied with your selections. 8 If required, select to simulate link modifications to a Scope of Management. • Right-click a GPO and select whether to have the GPO link enforced or link enabled), alter their link order, and simply remove them. • Right-click a parent OU to block inheritance or add GPOS are required. **Note**: You will only be able to choose checked out working copy or deployed GPOs. **Note**: GPOs are added as unenforced, link enabled or disabled depending on the Default link state sever option, and at the bottom of the list. Select **Restore** to undo any changes. This will only affect the immediate OU. Child OUs will not be undone. Select **Restore All Defaults**, to undo all changes. Click **Next** when satisfied with your selections. 9 Review the summary page and click **Next** to proceed. 10 Select to run the report, save the report so that you can compare it to another report, or save the report settings, and click **Finish**.

Live, working copy, latest version, and differences reports

You can create a report that shows information about the live, working copy, or latest versions of an object, or that compares two or more versions of the same object.

To create a report in the GPOADmin console

1. Expand the **Version Control Root** node and the required container.
2. Right-click the required controlled object and select **Reports**.
   - To create a report of the live controlled object's settings, select **Live**.
   - To create a report on the checked out and working copy settings, click **Working Copy**.
   - To create a report on the latest version of the controlled object in Version Control, click **Latest**.
   - To create a report to show the differences between two or more object's settings, click **Differences**.
3. View the report.

   Click **Print** to print the report.

   Click **Save As** to save the report as an HTML file.

   To view the report in the Reports node, save it in the My GPOADmin Reports folder in the Documents folder.

> **NOTE:** By default, GPOADmin looks to the My GPOADmin Reports folder (C:\Users\gpoadmin\Documents\My GPOADmin Reports) for saved reports. To point to a different folder, change your User Preferences. For more detail see Configuring user preferences on page 32.

4. Click **Close**.

   To view the report at a later time, double-click the required report and click to expand the section you want to view.

To create a report in the GPMC Extension

1. Select the GPO and click **Reports**.
   - To create a report of the live GPO's settings, select **Live**.
   - To create a report on the checked out and working copy settings, click **Working Copy**.
   - To create a report on the latest version of the GPO in Version Control, click **Latest**.
   - To create a report to show the differences between two or more GPO's settings, click **Differences**.
2. View the report.

   Click **Print** to print the report.

   Click **Save As** to save the report as an HTML file.
3. Click **Close**.

Historical Settings Reports

To create a Historical Settings Report

1. Expand the **Version Control Root** node and the required container.
2. Right-click the required controlled object and select **Show History**.

3 To view the settings of a previous version, right-click the version and select **View**.

4 View the report. Click **show** or **hide** to expand or collapse each section.

Click **Print** to print the report.

Click **Save As** to save the report as an HTML file.

5 Click **Close**.

To view the report at a later time, double-click the required report and click to expand the section you want to view.

To create a Historical Settings Report in the GPMC Extension

1 Click **Show History**.

2 In the bottom pane, right-click the version of the GPO and select **View**.

3 View the report. Click **show** or **hide** to expand or collapse each section.

Click **Print** to print the report.

Click **Save As** to save the report as an HTML file.

Files saved in the GPMC Extension are visible in the Reports node of the GPOADmin console.

4 Click **Close**.

Working with report folders

Reports in Dell GPOADmin mirrors the contents of My GPOADmin Reports folder in the Documents folder.

NOTE: Report Folders are only available in the GPOADmin console.

To create a new folder

- Right-click **Reports** or any subfolder, and select **New | Folder**.

To rename a folder

- Right-click any subfolder under Reports, select **Rename** and enter the new name.

NOTE: The name must be a valid Windows® folder and must not conflict with any other folder names of the same parent.

To delete a folder

- Right-click any subfolder under Reports and select **Delete**.

To manage reports using Windows *Explorer*

1 Right-click **Reports** and select **Open Folder in Explorer**.

From here, you can manage your files in the typical manner.

2 Once you return to Dell GPOADmin, right-click **Reports**, and select **Refresh** to ensure your view is updated.

5

Working with the ADM Editor

- Working with ADM files
- Creating and editing ADM files
- Customizing the ADM editor display

Working with ADM files

Working with registry-based Group Policy becomes a little less difficult when you use Administrative templates (.adm) files. The .adm files define what GPO settings are displayed under the Administrative Template folder for user and computer configuration.

NOTE: GPOADmin does not support the use of templates if the client and/or server are installed on Windows® 8 and Windows Server 2012. The support on earlier Windows operating systems is also limited.

NOTE: The ADM Editor is not supported if you have the GPOADmin client installed on Windows 8 or Windows 2012.

In effect, the .adm file is a template that defines the administrative interface that will be available during a GPO edit. The data required for creating and editing .adm files is easily accessed with the ADM Editor. The content of an .adm file includes

- Registry locations
- Options for each setting
- Input methods for parameters
- Default value to display
- Descriptions of the settings in the Explanation tab
- Supported settings within each Windows® version

NOTE: All ADM files used with GPOADmin templates must be Unicode.

For more information on ADM files see Adding and removing custom ADM files on page 32.

Creating and editing ADM files

The ADM Editor is included with GPOADmin. Using this tool, you can create and edit .adm files through a user-friendly interface.

To create an ADM file

1. Right-click **GPOADmin** and select **ADM Editor**.
2. Select **File | New**.
3. Click **Next** in the New ADM File Wizard.
4. Choose the type of file you want to create, and click **Next**.

   In this procedure, an empty .adm file is created. If you select User, Computer, or User and Computer the associated Administrative Template folder will be added to the file automatically.
5. Click **Finish**.

   A new ADM file is created.
6. Right-click the .adm file, and select **Add user configuration** or **Add computer configuration**, or both.

   The Administrative Templates container is displayed.
7. Right-click **Administrative Templates**, and select **Add category**.
8. Enter a name for the category.
9. Right-click the category, and select **Add policy**.
10. Enter a name for the policy.

You can now configure the policy to contain the required settings by adding controls and editing the properties.

11 Add a control by double-clicking the desired option in the Toolbox and editing its properties.

Right-click the policy and step through the New Part Wizard to include predefined parts for editing.

12 Enter a name for the .adm file, and select **Save**.

You can now add the .adm file to Group Policy Templates.

For information on using ADM files see Adding and removing custom ADM files on page 32.

To edit an ADM file

1 Right-click **GPOADmin** and Select **ADM Editor**.

2 Select **File | Open**, and choose a previously saved .adm file.

3 Edit the file as required.

You can add a category, add a policy, or remove existing policies and categories.

4 Select **File | Save**.

NOTE: You can check a new or existing file to ensure that it is well formed by clicking either **Check file** or pressing **F7**.

Example .adm file created with the ADM editor

This example displays how to create the following ADM file through the ADM Editor for defining the configuration of miscellaneous Internet Explorer settings:

```
CLASS USER

CATEGORY "Advanced settings"

    POLICY "Searching"

        KEYNAME "Software\Microsoft\Internet Explorer\Main"

        PART "Search Provider Keyword (type INTRANET if you have an internal
AutoSearch server):" EDITTEXT

            VALUENAME "Provider"

            KEYNAME "Software\Microsoft\Internet Explorer\SearchURL"

        END PART

        PART "When searching from the address bar:" DROPDOWNLIST

            VALUENAME "AutoSearch"

            ITEMLIST

               NAME "Display results, and go to the most likely site" VALUE NUMERIC
3 DEFAULT

                NAME "Just go to the most likely site" VALUE NUMERIC 2

                NAME "Just display the results in the main window" VALUE NUMERIC 1

                NAME "Do not search from the address bar" VALUE NUMERIC 0

            END ITEMLIST

        END PART

    END POLICY

END CATEGORY ;Advanced settings
```

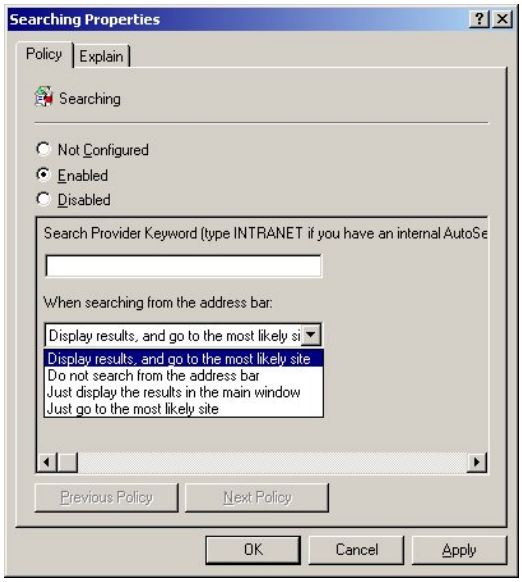
To create this ADM file

1. Right-click **GPOADmin** and select **ADM Editor**.
2. Select **File | New**.
3. Click **Next** in the New ADM File Wizard to begin.
4. Select **User** and click **Next**.
5. Click **Finish**.
6. Right-click **Administrative Templates** and select **Add category**.
7. Type **Advanced Settings** as the name for the category.
8. Right-click the category and select **Add policy**.
9. Type **Security** as the name for the policy.
10. Add a dropdown list.
11. Select the list, choose the list items property (in Properties view), click the **Browse** button, and add items in the List Item Editor.
12. Add additional value to the item (action list) by clicking **Add Registry Value**.
13. Once you have made all the required changes click **OK**.
14. Enter a name for the .adm file, and select **Save**.

The drop down list now has the following format:

```
PART "When searching from the address bar:" DROPDOWNLIST
        VALUENAME "AutoSearch"
        ITEMLIST
                NAME "Display results, and go to the most likely site" VALUE NUMERIC 3 DEFAULT
                        ACTIONLIST
                                KEYNAME "Software\Microsoft\Internet Explorer\Main"
                                VALUENAME "Additional value" VALUE NUMERIC 0
                                VALUENAME "Additional string value" VALUE "something"
                        END ACTIONLIST
                NAME "Just go to the most likely site" VALUE NUMERIC 2
                NAME "Just display the results in the main window" VALUE NUMERIC 1
                NAME "Do not search from the address bar" VALUE NUMERIC 0
        END ITEMLIST
END PART
```

The completed file displays as follows:



Customizing the ADM editor display

You can customize the ADM Editor to display any or all of the following: Policies and Categories, Properties View, Toolbox, Status Bar, Toolbar, and Registry values.

To alter the display

1. Right-click **GPOADmin** and select **ADM Editor**.
2. Select **File | Open** and choose a previously saved .adm file.
3. Click **View**.
4. Enable and disable the options as required.
5. If you select **Registry values**, once your file is complete, a treeview of the policy as it would be applied in the registry will display.

   From here you can also check for duplicates in the file, by selecting **Duplicates Only** from the list.

6

Working with the GPOADmin Dashboard

- Overview and installation notes
- Working within the Dashboard

Overview and installation notes

GPO implementation is a key consideration when planning your organization's Active Directory® structure, because it streamlines management of all user, computer, and configuration issues, ensuring the smooth day-to-day operation of the network.

The GPOADmin Dashboard offers a quick overview of the state of your GPO deployment and enables you to affect changes where required.

NOTE: For the best performance when using the dashboard, we recommend that you install the GPOADmin service on a computer with at least two CPUs.

When you install GPOADmin, by default the GPOADmin service and the Dashboard service are installed on the same computer with the Dashboard service configured to communicate with GPOADmin service "localhost". However, to improve performance you can install the Dashboard service as a standalone option or change the default GPOADmin service the Dashboard service communicates with.

NOTE: The dashboard is not supported on Windows 2003 and Windows 2003 R2.

To configure the Dashboard service to communicate with a specific GPOADmin service

1. Open Regedit.exe on the computer hosting the Dashboard service.
2. Navigate to "HKEY_LOCAL_MACHINE\SOFTWARE\Quest Software\Quest Group Policy Manager\DashboardConfig".
3. Specify the fully qualified domain name of the GPOADmin service you want the Dashboard service to communicate with in the "ServerName" value.
4. If you are using a custom port, include this in the "ServerName" by adding a colon (:) then the port number.
5. Restart the Dashboard service.

Working within the Dashboard

The Dashboard allows you to view GPO deployment summary and detailed information, configure the interval at which the dashboard data is updated, and perform actions that are available from within the GPOADmin client. For complete details on the available actions, see Using Dell GPOADmin on page 29.

To access the dashboard

- Select **Start | GPOADmin Dashboard**.

  The Dashboard opens with the overview view. From here you can get a quick summary of any actions that require your attention.

To configure the view

1. To have a full view of an individual tile, select it from the menu option on the left side or select **Show All**.
2. To move the position of a particular tile, select it and drag and drop it to the desired position. Keep in mind, you can only place it in a tile of similar size.
3. To sort information, select the desired column header and click it to sort in ascending and descending order.
4. To re-order the columns, select it and drag and drop it to the desired location.

NOTE: If you make changes to the column order or sorting, it is not maintained once you close the Dashboard or move between the tile view and the full page view.

To configure how often you want to refresh the Dashboard

NOTE: The polling interval for the communication between the Dashboard service and the GPOADmin server is not reflected in this setting. To configure the communication between the services, you must update the Dashboard service's configuration file.

The dashboard service configuration file is located in the install directory. The file name in "Quest.Avalanche.Dashboard.Service.dll.config". Intervals are adjusted under the "applicationSettings" section. Do not adjust the settings in any other sections.

1. Select the gear icon on the bottom left of the tile to view the configuration options.
2. Select the required polling interval (how often the dashboard display will communicate with the Dashboard service to refresh the information that is displayed).

   The default is every 60 seconds but this can be adjusted to suit your environment. You can choose the required seconds/minutes/hours.

Connections

The Connections view displays the installed dashboard servers along with its port information. If you have more than one server, you can easily move between them to view information about the version controlled items managed by the GPOADmin service associated with a particular Dashboard service.

To select a different server

- From the Dashboard homepage, select the required server from those available in the **Connections** list at the top of the page.

Unauthorized Modifications

This view displays all registered objects that were modified in or deleted from the live environment outside of the GPOADmin version control system. The details include the object name, type, version, status, and domain. A user with the appropriate permissions will be able to perform the following actions:

- Rollback: Restore the object in the live environment from the most current backup found in the system to overwrite the unauthorized live change.
- Rollback with Links: Restore a Group Policy Object in the live environment from the most current backup, including its links to Scopes of Management, and overwrite the unauthorized live change.
- Incorporate Live: Accept the live changes as being authorized and more up-to-date than what is currently already in the system. This will automatically back up those changes into the system and increment the version number of the backup to the next major number.
- Restore: Restore the object in the live environment.
- Unregister: Unregister the object from the Version Control system.

Checked Out

This view displays all objects that are checked out for modification. The details include the object name, type, version, status, user who has it checked out, and domain.

A user with the appropriate permissions will be able to perform the following actions:

- Check In: A check in updates the history of the object within the Version Control system with the changes made while it was checked out. Included with any check-in is a comment and a unique minor version number (such as 1.1). A check in does not allow the offline changes to go live into the enterprise environment as it must first be approved. Once an object is marked as Pending Approval, it cannot be checked out by any other user of the system.

- Undo Checkout: The user who checked out an object or who has the Undo Checkout right has the option of undoing the check out and reverting the state back to Available.
- Request Approval: Once an object has been altered and checked in to the system, the update is ready to go through the approval process.

Pending Approvals

This view displays all objects awaiting your approval. The details include the object name, type, version, status, pending action, and domain.

The approval system safeguards the enterprise environment from any unauthorized live changes that could cause unwanted results. The types of requests from users that require approval are:

- Changes to offline objects that are required to go live
- Creation of new objects
- Deletion of existing objects

Once an object has been checked in and the Approver has been notified that the offline changes are ready for approval by a user with the Deploy privilege.

To view and work with pending approvals

1 Select **Pending Approvals** from the menu.

2 Right-click the object change that is pending approval, and select **Approve** or **Reject**.

Deployments

This view displays all deployments (pending and scheduled) for the selected server including the name, type, version, status, pending action, and domain.

To view and work with deployments

1 Select **Deployments** in from the menu to view all deployments.

To view pending or scheduled deployments, select the associated option from the menu.

2 From here, you can select the **Deploy** or **Reject** any or all deployments.

A

Appendix: Windows® PowerShell Scripts

- Windows® PowerShell commands
- Dell GPOADmin scripts

Windows® PowerShell commands

The GPOADmin commands are installed during a complete or custom installation. (This is assuming that you have PowerShell currently installed.)

The GPOADmin provider and commands allow you to perform virtually all available functionality through a command line.

To load the GPOADmin PowerShell provider

1 Open PowerShell and run the following command: `Import-Module -Name <GPOADmin Install Directory>\GPOADmin.psd1`.

Once the GPOADmin provider is loaded, it will create two default drives called "VCRoot" and "PSRoot".

NOTE: PSRoot is the virtual directory created when Protected Settings policies are enabled for the specified server. All Protected Settings policy management and workflow actions are performed from here.

To access the drive, enter the following command: `CD VCRoot: or CD PSRoot:`

NOTE: You must include the colon.

If you are running only the GPOADmin client, you must create a PSDrive mapped to the version control root to use the available PowerShell capabilities.

NOTE: The account used in the credentials parameter must have permission to connect to the specified GPOADmin server. This is done by adding the user as either a GPOADmin user or administrator on the Access tab of the targeted GPOADmin Server Properties dialog.

Table 1. Connection options

Connection requirement	Command
Connect to the Version Control Root of GPOADmin on this computer as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root"`
Connect to the Protected Settings Root of GPOADmin on this computer as the current user	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT`
Connect to the Version Control Root of GPOADmin on this computer as a different user (a dialog will appear prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Credential "domain\user"`
Connect to the Protected Settings Root of GPOADmin on this computer as a different user (a dialog will appear prompting for the user password)	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT -Credential "domain\user"`
Connect to the Version Control Root of GPOADmin on a different computer using the default port number as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server"server.domain.com"`
Connect to the Protected Settings Root of GPOADmin on a different computer using the default port number as the current user	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT -Server"server.domain.com"`

Connection requirement	Command
Connect to the Version Control Root of GPOADmin on a different computer using the default port number as a different user (a dialog will appear prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server "server.domain.com" -Credential "domain\user"`
Connect to the Protected Settings Root of GPOADmin on a different computer using the default port number as a different user (a dialog will appear prompting for the user password)	`New-PSDrive -Name "PSRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -DriveType PSROOT -Server"server.domain.com" -Credential "domain\user"`
Connect to the Version Control Root of a GPOADmin server on a different computer using a custom port number of 40201 as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server "server.domain.com" -Port 40201`
Connect to the Protected Settings l Root of a GPOADmin server on a different computer using a custom port number of 40201 as the current user	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -Server "server.domain.com" -Port 40201`
Connect to the Version Control Root of a GPOADmin server on a different computer using a custom port number of 40201 as a different user (a dialog will appear prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Version Control Root" -Server "server.domain.com" -Port 40201 -Credential "domain\user"`
Connect to the Protected Settings Root of a GPOADmin server on a different computer using a custom port number of 40201 as a different user (a dialog will appear prompting for the user password)	`New-PSDrive -Name "VCRoot" -PSProvider PSGPOADmin -Root "Protected Settings Root" -Server "server.domain.com" -Port 40201 -Credential "domain\user"`

To see a list of all available commands

- Open PowerShell, load the GPOADmin provider, and run the following command: `get-command -module GPOADmin`.

  To see cmdlet details including the required parameters, run the PowerShell `get-help` command.

Table 2. Commands

Type	Available commands
Add	• Add-Administrator • Add-EmailTemplates • Add-Keywords • Add-ProtectedSettingsExclusions • Add-ProtectedSettingsPolicies • Add-Role • Add-User
Clear	• Clear-AssignedProtectedSettingsPolicies • Clear-EmailTemplate • Clear-KeywordsList • Clear-ProcessLock • Clear-ProtectedSettingsExclusions

Table 2. Commands

Type	Available commands
Get	• Get-Administrators • Get-AllManagedObjects • Get-ApprovalWorkflow • Get-AssignedProtectedSettingsPolicies • Get-Available • Get-BlockProtectedSettingsInheritance • Get-ChangeAuditorDateRange • Get-ChangeAuditorService • Get-CheckedOut • Get-ChecktedOutToMe • Get-CloakedGPOs • Get-CommentMaximumLength • Get-CommentMinimumLength • Get-Compliance • Get-CurrentUser • Get-DefaultLinkStateIsEnabled • Get-DeletedObjects • Get-Diagnostics • Get-DifferenceReport • Get-DisableAllGPOWorkflow • Get-DynamicReport • Get-EmailTemplates • Get-EnableCustomWorkflowActions • Get-EnableGPOSynchronization • Get-EnableProtectedSettings • Get-EnforceNamingStandards • Get-EnforceUniqueNames • Get-GPMCVersionCheck • Get-GPOLinks • Get-GPOs • Get-ItemByID • Get-KeywordsList • Get-LicenseInfo • Get-LinkedSOMs • Get-LockedGPOs • Get-LoggingOptions • Get-NotificationEmailAddress • Get-NotificationList • Get-Notifications • Get-PendingApproval • Get-PendingDeployment • Get-Permissions • Get-PreferredDomainController • Get-Properties

Table 2. Commands

Type	Available commands
Get	• Get-ProtectedSettingsExclusions • Get-ProtectedSettingsExclusionsRecursion • Get-ProtectedSettingsPolicies • Get-Rights • Get-Roles • Get-Security • Get-ServerDomain • Get-ServerVersion • Get-ServiceAccount • Get-SettingsReport • Get-SMTPOptions • Get-StorageOptions • Get-SynchronizationTargets • Get-UnauthorizedModifications • Get-UnlinkedSOMs • Get-Unregistered • Get-Users • Get-VCItemHistory • Get-WorkflowDisabledGPOs • Get-WorkflowEnabledGPOs
New	• New-Container • New-EmailTemplate • New-EmailTemplateAttachment • New-GPOLink • New-ProtectedSettingsPolicyAssignment • New-SyncTargetData • New-VCAce
Push	• Push-Notification
Remove	• Remove-Administrator • Remove-Backups • Remove-EmailTemplates • Remove-GPOLink • Remove-Keywords • Remove-Role • Remove-User

Table 2. Commands

Type	Available commands
Select	• Select-Approve • Select-CancelDeployment • Select-CheckIn • Select-Checkout • Select-Cloak • Select-Deploy • Select-Export • Select-ExportAsProtectedSettingsPolicy • Select-Import • Select-Label • Select-Lock • Select-RecursiveRegistration • Select-RecursiveUnregistration • Select-Register • Select-Reject • Select-RequestApproval • Select-Restore • Select-ScheduledDeploy • Select-SearchAndReplaceGPO • Select-SynchronizeNow • Select-Uncloak • Select-UndoCheckout • Select-Unlock • Select-Unregister • Select-VerifyProtectedSettings • Select-WithdrawApproval • Select-WithdrawApprovalRequest • Select-WorkflowDisable • Select-WorkflowEnabled

Table 2. Commands

Type	Available commands
Set	• Set-ApprovalWorkflow • Set-BlockProtectedSettingsInheritance • Set-ChangeAuditorDateRange • Set-ChangeAuditorService • Set-CommentMaximumLength • Set-CommentMinimumLength • Set-Compliance • Set-Configuration • Set-DefaultLinkStateIsEnabled • Set-DisableAllGPOWorkflow • Set-EmailTemplate • Set-EnableCustomWorkflowActions • Set-EnableGPOSynchronization • Set-EnableProtectedSettings • Set-EnforceUniqueNames • Set-GPMCVersionCheck • Set-Keywords • Set-License • Set-LoggingOptions • Set-ManagedBy • Set-NotificationEmailAddress • Set-Notifications • Set-PreferredDomainController • Set-ProtectedSettingsExclusionsRecursion • Set-Role • Set-Security • Set-SMTPOptions • Set-SynchronizationTargets
Watch	• Watch-PolicyTemplate

The GPOADmin PowerShell provider has extended the Get-ChildItem and the New-PSDrive command to include the following parameters:

Table 3. Commands

command	parameters
Get-ChildItem extensions	NOTE: If no parameters are specified then all objects are enumerated and returned. • Container: Returns Version Control containers. • Domain: Returns domain scopes of management. • GPO: Returns Group Policy Objects. • OrganizationalUnit: Returns Organizational Units. • Site: Returns site scopes of management. • SOM: Returns all scopes of management (domain, Organizational Units, and sites). • Template: Returns templates. • WMIFilter: Returns WMIFilters. • Count: Instructs the provider to return only the number of specified objects.
New-PSDrive extensions	• Server: Specifies the GPOADmin server service to connect to. • Port: Specifies the port to use when connecting to the specified server.
New-Item	• Path: The fully qualified path to the new item. • ItemTypeName: The type of item to create. Valid values are: CONTAINER, GPO, and WMIFILTER. • Domain: The domain in which the new item belongs. • Comment: A comment to associate with the creation of this item. • WorkflowDisabled: Creates the item as Workflow Disabled. Valid only with an ItemTypeName of GPO. • WMIFilter: The VersionControlledData representing the WMIFilter to be linked to this item. Valid only with an ItemTypeName of GPO. • Queries: The queries to be associated with this item. Valid only with an ItemTypeName of WMIFILTER • Description: The description for this item. Valid only with an ItemTypeName of WMIFILTER.
Remove-Item	• Comment: A comment to associate with this item.

Dell GPOADmin scripts

Dell GPOADmin installs the following PowerShell scripts to `c:\Program Files\Dell\GPOADmin\Scripts`:

- GPOADmin.AddServiceAccountToAllGPOs.ps1
- GPOADmin.RunDynamicReport.ps1

GPOADmin.AddServiceAccountToAllGPOs.ps1

Grants the specified service account Edit settings, Delete, and Modify Security privileges and assigns ownership to all the GPOs in the specified domain.

Parameters

- Domain: Specifies the DNS name of the domain in which to modify the GPOs.
- ServiceAccount: Specifies the account, in domain\user format, that will be granted access to and made the owner of all the GPOs.

Syntax

```
GPOADmin.AddServiceAccountToAllGPOs -Domain <string> -ServiceAccount <string>
```

Example

```
GPOADmin.AddServiceAccountToAllGPOs -Domain "MyDomain.com" -ServiceAccount
"mydomain\Service Account"
```

GPOADmin.RunDynamicReport.ps1

Runs a specified GPOADmin dynamic report and emails the results to a list of recipients.

Parameters

- gpmServer: Specifies the GPOADmin server to connect to. (Optional)
- gpmPort: Specifiec the port number of the GPOADmin server. Default is 40200. (Optional)
- DynamicReportFile: Specifies the path to the dynamic report file to execute.
- Recipients: Specifies the list of e-mail recipients.

Syntax

```
GPOADmin.RunDynamicReport.ps1 -Server <string> -Port <int> -DynamicReportFile
<string> -Recipients <stringArray>
```

Example

```
GPOADmin.RunDynamicReport.ps1 -Server "localhost" -Port 40200 -DynamicReportFile
"DynamicReport.xml" -Recipients ("recepient@company.com")
```

B

Appendix: GPOADmin Event Log

- What is the GPOADmin event log?
- Interpreting the GPOADmin event log
- Example GPOADmin events

What is the GPOADmin event log?

You can configure GPOADmin's event notification system to notify you of actions such as register, check in and check out. You can find details on configuring the event notification system in the section titled Selecting events on which to be notified on page 22.

The GPOADmin event log can be searched and filtered.

Interpreting the GPOADmin event log

GPOADmin logs events in the following format:

Table 4. Log Format

Information Item	Purpose
Level	The event severity levels are: • Information • Warning • Error
Source	Indicates the GPOADmin application or associated GPOADmin service generating the event: • GPOADmin • Dell GPOADmin Watcher Service • Dell GPOADmin Service
Event ID	A code you can use to look up the type of event. See Event ID types on page 109 for a list of event IDs.
Task Category	Provides additional information about the event ID. • 0 - None • 1 - User action - check in, check out, and so on. • 2 - Service Action - startup, shutdown, and so on. • 4 - Error - an error has occurred. • 8 - Troubleshooting
Description	Provides detailed information about the event. It may include an object's name, the action performed on the object (such as check in or deployed) and by whom, as well as any other information relating to the event.

Event ID types

The Event IDs generated by GPOADmin are broken into the following types:

Event ID	Description
0	Associated with the GPOADmin Server Service
1000	Request
1001	Deploy
1002	Approve
1003	Reject
1004	Create
1005	Check Out

Event ID	Description
1006	Check In
1007	Move
1008	Undo check out
1009	Register
1010	Unregister
1011	Modify Security
1012	Withdraw Approval
1013	Withdraw Approval Request
1014	Compliance Action
1015	Create Container
1016	Delete Container
1017	Edit Container
1018	Modify Container Security
1019	Disable Workflow
1020	Enable Workflow
1050	The Watcher Service
1100	Email Message: "SMTP Host is undefined"
1150	Email Message: Exceptions
2001	Error importing settings to object
2002	Various generic exception messages
2004	Various generic exception messages
2005	Various generic exception messages
2006	Various generic exception messages
2007	Various generic exception messages
2010	Problem with Access Control List (ACL) attribute.
2013	GPOADmin server process – Information
2014	GPOADmin server process – Errors
2015	Custom Workflow Action process – Standard Output stream
2016	Custom Workflow Actions process – Error stream
2245	Problem with Read Only domains or a problem with the version control containers.
5000	Problem with the license – error code and error message
5000-2086928381	Invalid license – wrong product
5000-2086928382	Invalid license – demo expired
5000-2086928383	Invalid license – license expired
5000-2147467259	Invalid license
6000	Error starting Dashboard service
6001	Dashboard service starting
6002	Dashboard service has started
6003	Dashboard service stopping
6004	Dashboard service has stopped
6010	Collector initialization
6015	Polling interval set

Event ID	Description
6040	Failed to load configuration file
6045	Problem loading configuration file
6046	Configuration file corrupt
6047	Configuration file missing
6050	Error adding items to collection
6060	Configuration file deleted
6065	Configuration file renamed
6066	Configuration file name restored
6070	Configuration file restored
6100	Error during search
6101	Error during collection of object for GPO Statistics
6102	Error during parsing of objects for GPO Statistics

Example GPOADmin events

The following table illustrates how events display in your log.

Table 5. Log Events

LEVEL	SOURCE	EVENT ID	TASK CATEGORY	DESCRIPTION
Information	GPOADmin	1050	2	The change is an authorized change made by GPOADmin on a working copy.
Warning	GPOADmin	1050	2	Unable to locate any domain controllers to monitor.

C

Appendix: GPOADmin Backup and Recovery Procedures

- GPOADmin Backup Requirements
- Restoring GPOADmin

GPOADmin Backup Requirements

As part of your normal disaster procedures or requirements, GPOADmin should be considered for inclusion. In the event of a computer or network failure, the GPOADmin deployment and its data can be restored if you have performed regular and distributed backups of the following:

- The GPOADmin configuration store.
- The GPO backups store.

During the initial installation of GPOADmin, you must specify where to place these two items within your environment. The configuration store can reside in either Active Directory® or ADAM/AD LDS. The GPO backup store can be in Active Directory®, ADAM/AD LDS, a network share, or on a SQL server. The recommended location is on a network share.

Each of these options has its own backup strategies and requirements and should be included in your regular backup schedule.

NOTE: While GPOADmin is inaccessible, you can manage GPOs through the Group Policy Management Console (GPMC).

Restoring GPOADmin

Once you have performed the required recovery procedures listed below, simply reinstall GPOADmin, configure the services to use the recovered stores and resume the management of GPOs. For configuration details, see Configuring the Version Control server on page 14.

Any policies that were checked out, checked in, or pending approval up to the time of the last backup will be not be affected by the failure.

To restore the ADAM instance

- For information on how to backup Microsoft® ADAM/AD LDS see: http://technet.microsoft.com/en-us/library/cc780870(WS.10).aspx or Microsoft® TechNet.

To restore the file share

- Follow your internal procedure for recovering files and folders.

  If you plan to use a new host computer for the GPOADmin backup store, or the host computer has been renamed, please contact Dell Customer Support for assistance.

D

Appendix: Customizing your workflow

- What is a custom workflow action?
- Working with custom workflow actions in the Version Control system
- Working with the custom workflow actions xml file
- Troubleshooting custom workflow actions

What is a custom workflow action?

You can extend GPOADmin's version control system to incorporate customized actions based on your organizations existing workflow. This allows you to customize and control the deployment of controlled objects (such as GPOS, SOMs, and WMI filters) to meet your individual needs. For example, you can configure a pre-action to send the help desk distribution list an email each time a GPO change is requested.

Also, if you have a workflow tool in place that encompasses many different organizational tools you no longer need to use the workflow in both applications. With pre and post actions, a GPO check out, modification, and request for approval can be configured to create a ticket in an existing workflow system. Subsequent approval in the external workflow system can be configured to approve and deploy that same policy in GPOADmin. A post action can be configured to add additional ticket information about the deployment of the GPO into the customers external workflow application.

Custom actions are available on the following Version Control actions:

Action	Executes when...
ApplyPolicyTemplate	A policy template has been applied to a version controlled policy.
Approve	A change to a version controlled object is approved.
CancelScheduledApproval	A version controlled object's scheduled deployment has been canceled.
CheckIn	A version controlled object is checked in.
CheckOut	A version controlled object is checked out.
Cloak	A version controlled object has been cloaked.
ComplianceAction	Either a "Rollback" or "IncoporateLive" compliance action is performed.
Create	A version controlled object has been created.
Delete	A version controlled object has been deleted.
Deploy	A version controlled object has been deployed into the live environment.
DisableWorkflow	A version controlled object has been workflow disabled.
Edit	A version controlled object has been modified.
EnableWorkflow	A version controlled object has been workflow enabled.
Label	A label has been applied to one or more version controlled objects.
Lock	A version controlled object has been locked.
ModifySecurity	The security has been modified on a version controlled object.
Move	A version controlled object is moved.
Register	An object is registered with the version control system.
Reject	A change to a version controlled object is rejected.
Rename	A version controlled object is renamed.
RequestApproval	An approval for a version controlled object is requested.
Restore	A version controlled object has been restored.
SubmitScheduledApproval	A version controlled object has been scheduled for deployment.
Synchronization	A version controlled Group Policy Object has been synchronized with another Group Policy Object.
Uncloak	A version controlled object has been uncloaked.
UndoCheckOut	A version controlled object's checkout is undone.
Unlock	A version controlled object has been unlocked.
Unregister	A version controlled object is unregistered.
WithdrawApproval	An approval on a version controlled object is withdrawn.
WithdrawApprovalRequest	A request for approval has been withdrawn.

Working with custom workflow actions in the Version Control system

GPOADmin provides an easy to use editor to help you set up and configure your custom actions.

Each custom workflow action has two phases; pre-actions (processed prior to the version control action being executed), and post-actions (processed after the version control action has been executed).

Whether or not an action is processed can be controlled by the use of conditions. This must be set through the editing the xml file directly. For details see, Conditions on page 121.

GPOADmin includes a sample custom workflow to get you started that shows how to incorporate the creation of Help desk ticket with each approval request generated from the Version Control system.

To access the sample custom workflow template

1. Right-click the forest, and select **Properties**.
2. Select the **Options tab**, scroll to locate the custom workflow actions option, and select **Launch Editor.**
3. In the editor, select File \ Open and select the CustomWorkflowActions.xml file located in the installation directory. (C:\Program Files\Dell\GPOADmin\Examples)
4. Select the **Request approval | Pre-Action** to view the sample.

To create a new custom workflow action

1. Right-click the forest, and select **Properties**.
2. Select the **Options tab**, scroll to locate the custom workflow actions option, and select **Launch Editor.**
3. Select the required action and click the **Pre-Actions** option.
4. Enter a name and comment for the action.
5. If desired, select the **Stop on error** option. This will instruct the service to stop all processing for the current object when an error occurs.
6. Enter the location or browse to the required application to run.
7. Enter the required parameters in the Parameters window. To insert a tag, right-click in the Parameters window, select **Insert Tag**, and choose the required tag. For details on the available options, see Predefined Tags on page 120.
8. If required, select the **Post-Actions** tab and configure its options.
9. Click **Add**.
10. Once you have entered all the required pre and post actions, save your workflow.

> **NOTE:** Because custom workflow actions are performed in the background by the GPOADmin service, they will not be visible from the interface and depending on the number and complexity of scripts defined for a given action, there may be a delay as the custom actions are being processed by the server.
>
> When required, you can suspended custom workflow actions through the Server properties dialog. To pause or stop the custom workflow action on page 118.

11. When you are ready to deploy the workflow, select **Enable the processing of custom workflow actions**.

To edit a custom workflow action

1. Right-click the forest, and select **Properties**.
2. Select the **Options tab**, scroll to locate the custom workflow actions option, and select **Launch Editor.**
3. Select the required action and pre or post action.

4 Edit the action as required. You can:

   a Change the name, comment, executable, and parameters.

   b Right-click and add or remove actions.

   c Right-click and adjust the order in which they are performed.

   d Copy and past actions.

5 When you have made all your changes, click **Update**.

To pause or stop the custom workflow action

1 Right-click the forest, and select **Properties**.

2 Select the **Options tab**, scroll to locate the custom, workflow actions option, and select **Launch Editor.**

3 Click to disable the custom workflow actions option.

Working with the custom workflow actions xml file

Custom workflow actions are defined in an XML file (CustomWorkflowActions.xml) which must be located in the same directory as the GPOADmin Service executable.

Actions

For a list of available actions, see What is a custom workflow action? on page 116. Custom workflow actions are defined in the CustomWorkflowActions.xml file as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
  </CheckIn>
</CustomWorkflowActions>
```

NOTE: Actions names are case sensitive.

PreActions and PostActions

The PreActions and PostActions are defined as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions/>
    <PostActions/>
  </CheckIn>
</CustomWorkflowActions>
```

Each phase may contain one or more actions with the following properties:

Table 6. Properties

Property	Description
Name	Identifies the action.
Comment	Describes the action.
StopOnErrors	Instructs the service to stop all processing for the current object when an error occurs.

The properties are defined as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions>
      <Action Name="CheckIn pre-action" Comment="A custom action."
StopOnError="false">
      </Action>
    </PreActions>
    <PostActions>
    </PostActions>
  </CheckIn>
</CustomWorkflowActions>
```

Each action also contains the following nodes:

Table 7. Nodes

Action	Description
Executable	The full path to the executable.
Parameters	The list of parameters to pass to the executable.
Conditions	A list of conditions which determine whether or not to process the action.

The nodes are defined as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions>
      <Action Name="CheckIn pre-action" Comment="A custom action."
StopOnError="false">
        <Executable>c:\windows\system32\cmd.exe</Executable>
        <Parameters>/C mkdir "c:\GPOSettingsReports\CheckIn"</Parameters>
        <Conditions>
        </Conditions>
      </Action>
    </PreActions>
    <PostActions>
    </PostActions>
  </CheckIn>
</CustomWorkflowActions>
```

Predefined Tags

Tags are typically replaced with their corresponding values by the service. However, there are cases where the tags will not be converted. For example, if a comment is not specified during the version control action then the [COMMENT] tag will be empty; or if the object is not checked out then the [TRUSTEENAME] and [TRUSTEESID] will be empty.

Keep in mind that in some cases the tags will always be empty as is the case of a pre-action for the Register version control action. At the time the pre-action is processed, the corresponding version control information would not exist.

NOTE: Tags must be uppercase and enclosed in square brackets.

Parameters and conditions support the following predefined tags:

Table 8. Available tags

Tag	Description
[ACTION]	The currently executing version control action.
[VCID]	The version control identifier of the current object.
[DOMAINNAME]	The name of the domain for the current object.
[FULLPATH]	The full path of the current object in the version control system.
[ID]	The native identifier for the current object.
[LASTBACKUPID]	The identifier of the last backup for the current object.
[NAME]	The name of the current object.
[STATUS]	The version control status for the current object.
[SUBSTATUS]	The version control sub status for the current object.
[TRUSTEENAME]	The name of the user the current object is checked out to.

Table 8. Available tags

Tag	Description
[TRUSTEESID]	The SID of the user the current object is checked out to.
[TYPE]	The version control type of the current object.
[VERSION]	The version of the current object.
[COMMENT]	The comment associated with the version control action.

Conditions

Whether or not an action is processed can be controlled by the use of conditions. A condition must evaluate to true in order for the action to be processed. If the condition evaluates to false then a log entry stating such is created and the current custom workflow action is not processed.

Each condition node has the following properties:

Table 9. Condition properties

Property	Description
DataType	The data type of the property being compared.
Value1	The left side of the comparison.
Value2	The right side of the comparison.
Operator	The operation to perform. Options depend on the DataType.
IgnoreCase	This is only valid for the string DataType. This property instructs the service to perform any string operations case insensitively.

The type of operations available depends on the DataType property.

The following DataTypes are available:

Table 10. DataTypes

DataType	Description
String	This condition is performed on a string.
Guid	This condition is performed on a Guid.
Version	The condition is performed on a version.

The following operations are available for a String DataType:

Table 11.

String operator	Description
equal	Determines whether or not Value1 and Value2 have the same value.
not equal	Determines whether or not Value1 and Value2 are different.
contains	Determines whether or not Value2 is present in Value1
not contains	Determines whether or not Value2 is missing from Value1.
starts with	Determines whether or not Value1 starts with Value2.
not starts with	Determines whether or not Value1 does not start with Value2.
ends with	Determines whether or not Value1 ends with Value2.
not ends with	Determines whether or not Value1 does not end with Value2.

The following operations are available for a Guid DataType:

Table 12. Guid operators

Guid operator	Description
equal	Determines whether or not Value1 and Value2 have the same value.
not equal	Determines whether or not Value1 and Value2 are different.

The following operations are available for a Version DataType:

Table 13. Version operators

Version operator	Description
equal	Determines whether or not Value1 and Value2 have the same value.
not equal	Determines whether or not Value1 and Value2 are different.
greater than	Determines whether or not Value1 is greater than Value2.
greater than or equals	Determines whether or not Value1 is greater than or equal to Value2.
less than	Determines whether or not Value1 is lesser than Value2.
less than or equals	Determines whether or not Value1 is lesser than or equal to Value2.

The available logical operators include:

Table 14. Operators

Operator	Description
And	Logically ANDs to conditions.
Or	Logically ORs to conditions.

The logical operators ‘And’ and ‘Or’ function sequentially and grouping is not supported. For example:

```
Condition1 And Condition2 Or Condition3
```

would be processed as:

```
(Condition1 And Condition2) Or Condition3
```

not as:

```
Condition1 And (Condition2 Or Condition3)
```

To use a logical “And” or “Or” operator, specify a new Condition with only the Operator property.

For example:

```
<Condition Operator="And"/>
<Condition Operator="Or"/>
```

Example of a complete pre-action

The following example demonstrates a pre-action that creates a CheckIn directory below the GPOSettingsReports directory provided that the name of the version controlled object contains an underscore and the version is less than 4.5 or the comment ends with "_AMER".

```
<?xml version="1.0" encoding="utf-8"?>
<CustomWorkflowActions>
  <CheckIn>
    <PreActions>
      <Action Name="CheckIn pre-action" Comment="A custom action."
StopOnError="false">
        <Executable>c:\windows\system32\cmd.exe</Executable>
        <Parameters>/C mkdir "c:\GPOSettingsReports\CheckIn"</Parameters>
        <Conditions>
       <Condition DataType="String" Value1="[NAME]" Operator="contains" Value2="_"
IgnoreCase='true'/>
        <Condition Operator="And"/>
        <Condition DataType="Version" Value1="[VERSION]" Operator="less than"
Value2="4.5"/>
        <Condition Operator="Or"/>
        <Condition DataType="String" Value1="[COMMENT]" Operator="ends with"
Value2="_AMER"/>
        </Conditions>
      </Action>
    </PreActions>
    <PostActions>
    </PostActions>
  </CheckIn>
</CustomWorkflowActions>
```

Troubleshooting custom workflow actions

Because custom workflow actions are performed in the background by the GPOADmin service, they will not be visible from the interface. However, you can use the logs to assess any issues. When a custom workflow action is processed, the Standard Output and Error streams are redirected and logged as part of the server actions provided the Debug logging option is enabled.

NOTE: Depending on the custom workflow action, there can be a large amount of data written to the logs. It is strongly recommended that all custom workflow actions be thoroughly tested by a user who has access to the GPOADmin server logs.

Table 15. Event IDs and corresponding source

Event ID	Source
2013	GPOADmin server process - Information
2014	GPOADmin server process - Errors
2015	Custom Workflow Action process - Standard Output stream
2016	Custom Workflow Actions process - Error stream

E

Appendix: GPOADmin Silent Installation Commands

- Installing GPOADmin with msiexec.exe

Installing GPOADmin with msiexec.exe

If required, GPOADmin and its various components can be installed silently from the command line using the msiexec.exe utility. This section details the commands and provides examples for the following types of installation options:

- All components (Complete GPOADmin installation)
- Client and components
- Watcher Service
- GPMC Extension
- GPOADmin Dashboard

All components (Complete GPOADmin installation)

This command installs all GPOADmin components.

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64"
SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password" LICENSEACCEPTED=1
INSTALLLEVEL="1000"
```

NOTE: The parameters "domain\account" and "password" are the service account and its associated password used for GPOADmin.

NOTE: In this example, the 64 bit version of GPOADmin is being installed. To install the 32 bit version of GPOADmin, replace "dell gpoadmin x64" with "dell gpoadmin x86".

Client and components

You can alternatively select to install the GPOADmin client and specific components on select computers. You can choose from the following:

- Server and client
- Client only
- Client and scripts (Client Only button on Installation dialog)
- Scripts only

Server and client

This command installs both the server (QGPMService) and client.

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=ClientComponentFeature,ServerComponentFeature,ServerFeature
SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password"
```

NOTE: The parameters "domain\account" and "password" are the service account and its associated password used for GPOADmin.

Client only

This comand installs the client only.

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=ClientFeature
```

Client and scripts (Client Only button on Installation dialog)

These commands install the client only and scripts.

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1
INSTALLLEVEL="3"
```

OR

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=ClientFeature,ScriptingFeature
```

Scripts only

This command installs the scripts only.

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=ScriptingFeature
```

Watcher Service

You can easily install the Watcher Service (QGPOADminWatcherService) on select computers. The following installation options are available:

- Watcher Service on localhost
- Watcher Service on another computer
- Watcher Service and GPMC Extension on another computer
- Watcher Service and Client only on another computer
- Watcher Service, Client, and GPMC Extension on another computer

NOTE: For each of these commands:

- The parameter "server_name" is the name of the computer where the GPOADmin service is installed.
- The parameters "domain\account" and "password" are the service account and its associated password used for GPOADmin.

Watcher Service on localhost

This command installs the Watcher Service on a computer where the GPOADmin components are installed (localhost).

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password"
```

Watcher Service on another computer

This command installs the Watcher Service on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature SERVICEACCOUNT=domain\account SERVICEPASSWORD="password"
SERVERNAME="server_name"
```

Watcher Service and GPMC Extension on another computer

This command installs the Watcher Service and the GPMC Extension on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature,GPMCExtensionFeature SERVICEACCOUNT=domain\account
SERVICEPASSWORD="password" SERVERNAME="server_name"
```

Watcher Service and Client only on another computer

This command installs the Watcher Service and Client only on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature,ClientFeature SERVICEACCOUNT="domain\account"
SERVICEPASSWORD="password" SERVERNAME="server_name"
```

Watcher Service, Client, and GPMC Extension on another computer

This command installs the Watcher Service, Client, and GPMC Extension on a computer that does not have other GPOADmin components installed.

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=WatcherFeature,ClientFeature,GPMCExtensionFeature
SERVICEACCOUNT=domain\account SERVICEPASSWORD="password" SERVERNAME="server_name"
```

GPMC Extension

You can select to install the GPMC Extension computers where GPMC is installed. The following options are available:

- GPMC Extension on a localhost
- GPMC Extension on another computer

GPMC Extension on a localhost

This command installs the GPMC Extension on a computer where the GPOADmin components are installed (localhost).

```
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=GPMCExtensionFeature
```

GPMC Extension on another computer

This command installs the GPMC Extension on a computer that does not have GPOADmin components installed.

```
Silent install of GPMC Extension (specified server):
msiexec /quiet /l* Install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=GPMCExtensionFeature SERVERNAME="server_name"
```

NOTE: The parameter "server_name" is the name of the computer where the GPOADmin service is installed.

GPOADmin Dashboard

You can select to install the GPOADmin Dashboard on a computer where GPOADmin is installed. The following options are available:

- Dashboard Service and Client
- Dashboard Client only
- Dashboard Service only
- Client, Dashboard (no service), and GPMC Extension

NOTE: For these commands:

- The parameters "domain\account" and "password" are the service account and its associated password used for GPOADmin.

Dashboard Service and Client

This command installs the Dashboard Service and Dashboard Client on a computer that has the GPOADmin components installed (localhost).

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=DashboardServiceComponentFeature,DashboardFeature,DashboardComponentFeatur
e SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password"
```

Dashboard Client only

This command installs the Dashboard Client on a computer that has the GPOADmin components installed.

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=DashboardFeature,DashboardComponentFeature SERVICEACCOUNT="domain\account"
SERVICEPASSWORD="password"
```

Dashboard Service only

This command installs the Dashboard Service only on a computer that has the GPOADmin components installed (localhost).

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=DashboardServiceComponentFeature,DashboardFeature
SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password"
```

Client, Dashboard (no service), and GPMC Extension

This command installs the Client, Dashboard (no service) and GPMC Extension on a computer that has the GPOADmin components installed (localhost).

```
msiexec /quiet /l* install.log /i "dell gpoadmin x64" LICENSEACCEPTED=1 /q
ADDLOCAL=ClientFeature,DashboardFeature,DashboardComponentFeature,GPMCExtensionFeat
ure SERVICEACCOUNT="domain\account" SERVICEPASSWORD="password"
```

About Dell

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit http://software.dell.com/.

Contacting Dell

Technical support:
Online support

Product questions and sales:
(800) 306-9329

Email:
info@software.dell.com

Technical support resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to https://support.software.dell.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to Trial Downloads.
- View how-to videos
- Engage in community discussions
- Chat with a support engineer