Group Policy Auditing and Attestation

SDM Software Group Policy Auditing & Attestation

Version 3.0

User Guide

Revision April 2020

Contents

Introduction

This document presents a user guide for information on the use of GPAA. Basic information on getting the program working is presented first, followed by an Advanced section for more in-depth tweaks and features.

Welcome to SDM Software Group Policy Auditing & Attestation

Overview

SDM Software Group Policy Auditing & Attestation (GPAA) provides an easy, reliable way to handle recurring GPO attestations, keep track of responses, and monitor your GPO environment to meet auditing requirements. With GPAA, you can:

- Automatically send periodic emails to GPO owners, requesting attestation responses of Accepted or Rejected
- Monitor GPO changes and receive email alerts regarding GPO change activity
- Configure how often to request attestation, to whom to send the attestation, when to send follow-up emails if there is no response, to whom to send auditing alerts, and more
- Keep track of attestations and auditing with several pre-defined reports to analyze data such as the attestation history of GPOs, unattested GPOs, and changes by GPO
- Perform automatic backups when GPOs change
- Easily roll back GPO changes using application-maintained backups
- Be notified with Offline Alerting if the GPO auditing service loses contact with the GPAA database

Getting Started—Configuring GPAA for First Use

The first user or group member with rights to log in to GPAA Manager will be designated during the GPAA setup (see the GPAA Installation Guide for more details) routine. By default, this first user can perform all features of the program. Other users who will manage the product must then be added using the User Management menu (see the Adding Users section under User Management), and their roles assigned as desired.

The IIS-based web front-end, GPAA Manager, uses Microsoft's Integrated Windows Authentication (IWA) for quick logons. This means that whatever domain logon ID was used to log onto the computer where you browse to GPAA Manager, that will be the user logged in automatically to GPAA Manager.

The product does have the ability to log on as a different user (see the button on the upper right of the GPAA web console), for those instances when you're logged onto the workstation as someone other than your GPAA administrative ID.

The following steps are the high-level tasks required to start using GPAA:

Step 1: Configure the domain(s) of your GPO environment, and the mail server to use for outgoing emails from the Configuration Menu.

Step 2: Add users or groups in User Management, if necessary. Note that a user does not need to be added here in order to be assigned as a primary or secondary owner/support person for a GPO, which allows them to receive attestation or auditing emails. **User Management is only required for users who will be configuring, managing and reporting with GPAA.**

Step 3: Assign GPO Owner and Support emails. GPO Owner email addresses receive attestation emails; GPO Support email addresses receive auditing change alert emails. When you set a GPO's status to Active on the Manage GPOs page, this will begin the attestation process for that GPO (for more about configuring the attestation process, see Managing the Attestation Process for more details on how GPO attestation works. The Auditing service will automatically begin sending emails to Support email addresses after the Auditing service detects them. This is usually after a 15 minute polling interval configured at the auditing service on each domain controller. This 15 minute interval is the frequency with which the Auditing Service contacts the GPAA database to find out about new or deleted GPOs, new or added GPO owner or support emails, as well as other global settings such as SMTP information.

Step 4: Review Attestation and Auditing settings in the Manage Attestation and Manage Auditing sections, and update if necessary. By default, attestation is set to send attestations one year after a GPO is manually made active, then a year after they are attested, and so on, in a repeating cycle until the GPO's status in GPAA is set to Inactive.

The Configuration Menu

In order to see this section of GPAA Manager, users must be added within User Management and given the Configuration Manager role. By default, the user or group designated in the setup utility has all roles.

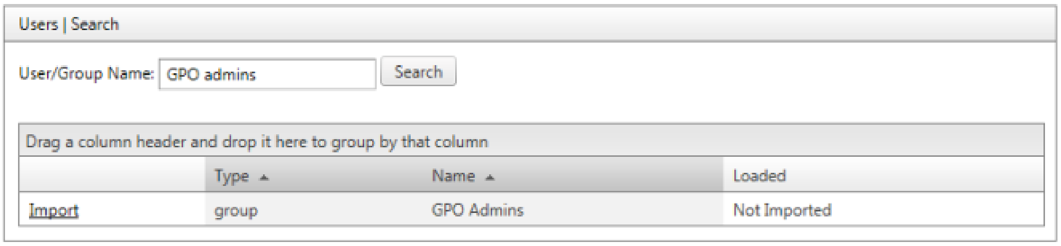
The first step in using the product is adding the domain(s) to be used for auditing and attestation. The next step is to configure the mail server in order for auditing and attestation emails to be sent. Each of these is described next.

Domains

Mail Server

The User Management Menu

The User Management section of GPAA Manager is where you add, modify or remove users or groups defined within Active Directory. User authorization for the GPAA product is controlled here:



Users | Search

User/Group Name: GPO admins

Drag a column header and drop it here to group by that column

	Type ▲	Name ▲	Loaded
Import	group	GPO Admins	Not Imported

In order to see the User Management section, logged in users must have the User Manager role.

Adding Users

Edit Users

Roles

The Manage Product Menu

Once the auditing and attestation services have been installed, and your domain(s) and mail server have been added in the Configuration section, define the settings for auditing and attestation of your environment here. To receive emails requesting attestation, GPOs must be assigned email addresses for Primary Owners, and have their statuses changed from Inactive to Active on the Manage GPOs page. Assign email addresses for GPO Primary and, optionally, Secondary Support users to receive auditing emails for those GPOs.

> *The process of marking a GPO 'active' for attestation in GPAA has no bearing on whether that GPO is processed or active in Active Directory. They are separate distinctions. By default, all GPOs are marked inactive when imported into GPAA.*

Note that any changes made within GPAA Manager, such as email addresses or number of backups to keep for rollback, can take up to 15 minutes to be detected by the auditing service running on each domain controller.

The Manage GPOs Menu

You can assign emails on a per-GPO basis to be used for attestation and auditing and set their statuses to Active to start the attestation process. Auditing will occur on all GPOs regardless of whether they have an Active or Inactive status.

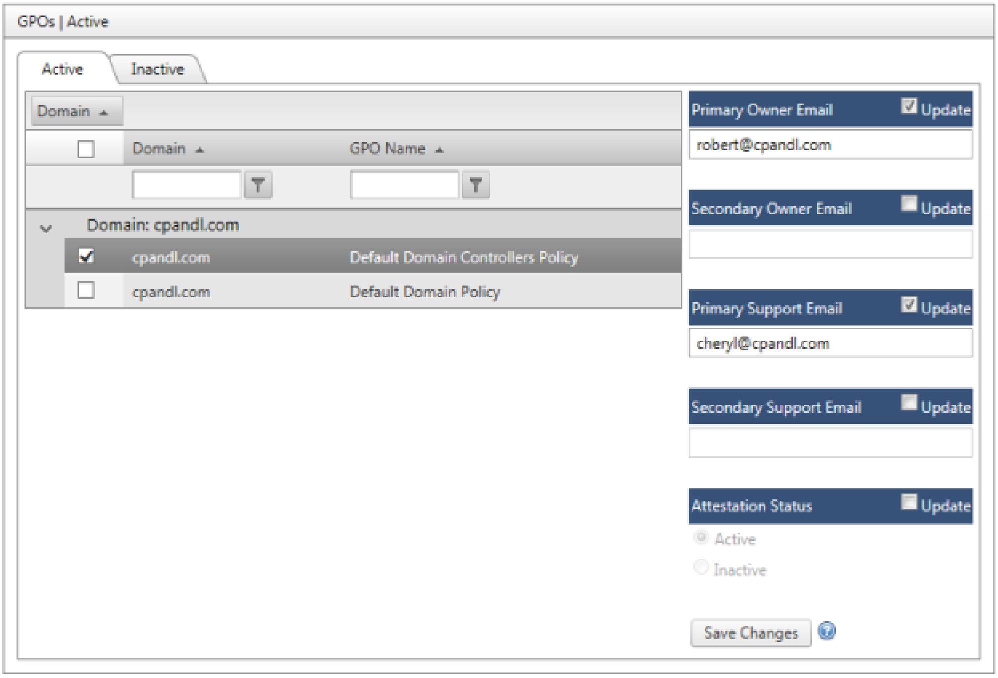
Attestation emails are sent to the Primary and Secondary Owner emails. The Secondary Owner email field is optional; if used, they will receive an email if the Primary Owner does not respond to the initial or follow-up email. The amount of time between each of the initial, follow-up, and secondary emails can be changed on the Manage Attestation - GPO Attestation page, described in the Manage Attestation section below.

Auditing emails are sent to the Primary and Secondary **Support** emails, and, optionally, to the General Alerts Email found on the Configuration - Mail Server page for some types of notifications. The Secondary Support email field is optional. Support emails also receive emails if a GPO attestation was rejected by an owner. If no support email addresses are defined for a GPO that was rejected, an alert will go to the General Alerts Email, defined on the Configuration - Mail Server page.

The list of GPOs is separated into tabs by attestation status - Active or Inactive. To update a field, click the checkbox to the left of the GPO name, then click the Update checkbox to the right of the field you would like to update. Enter the data, then click Save Changes. The same information can be entered for more than one GPO by checking multiple checkboxes to the left of the GPOs.

GPOs are listed on this page once their host domain is added in the Configuration | Domains menu section, as soon as the number of Active Directory Query Frequency seconds has passed, as defined in the Manage Attestation Service section (15 minutes by default).

Search for a GPO or domain by typing its name into the GPO Name or Domain text box at the top of the list. Click the Filter button to refine the search with different filter types as shown below:



GPOs | Active

□	Domain ▲	GPO Name ▲
Domain: cpandl.com		
☑	cpandl.com	Default Domain Controllers Policy
□	cpandl.com	Default Domain Policy

Primary Owner Email ☑ Update
robert@cpandl.com

Secondary Owner Email □ Update

Primary Support Email ☑ Update
cheryl@cpandl.com

Secondary Support Email □ Update

Attestation Status □ Update
● Active
○ Inactive

The Manage Auditing Menu

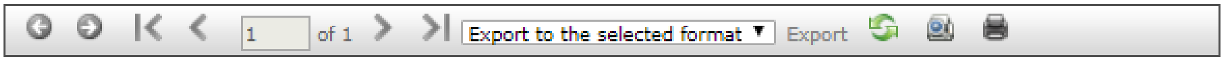
The Manage Attestation Menu

Reports

GPAA provides two reporting sections with the product—one for attestations and the other related to GPO changes and rollbacks. This section describes each report. All reports can be printed or exported to the following formats:

- PDF
- CSV
- Excel
- RTF
- TIFF
- Web Archive file

These export and print options can be found on the toolbar at the top of each report, as shown here:

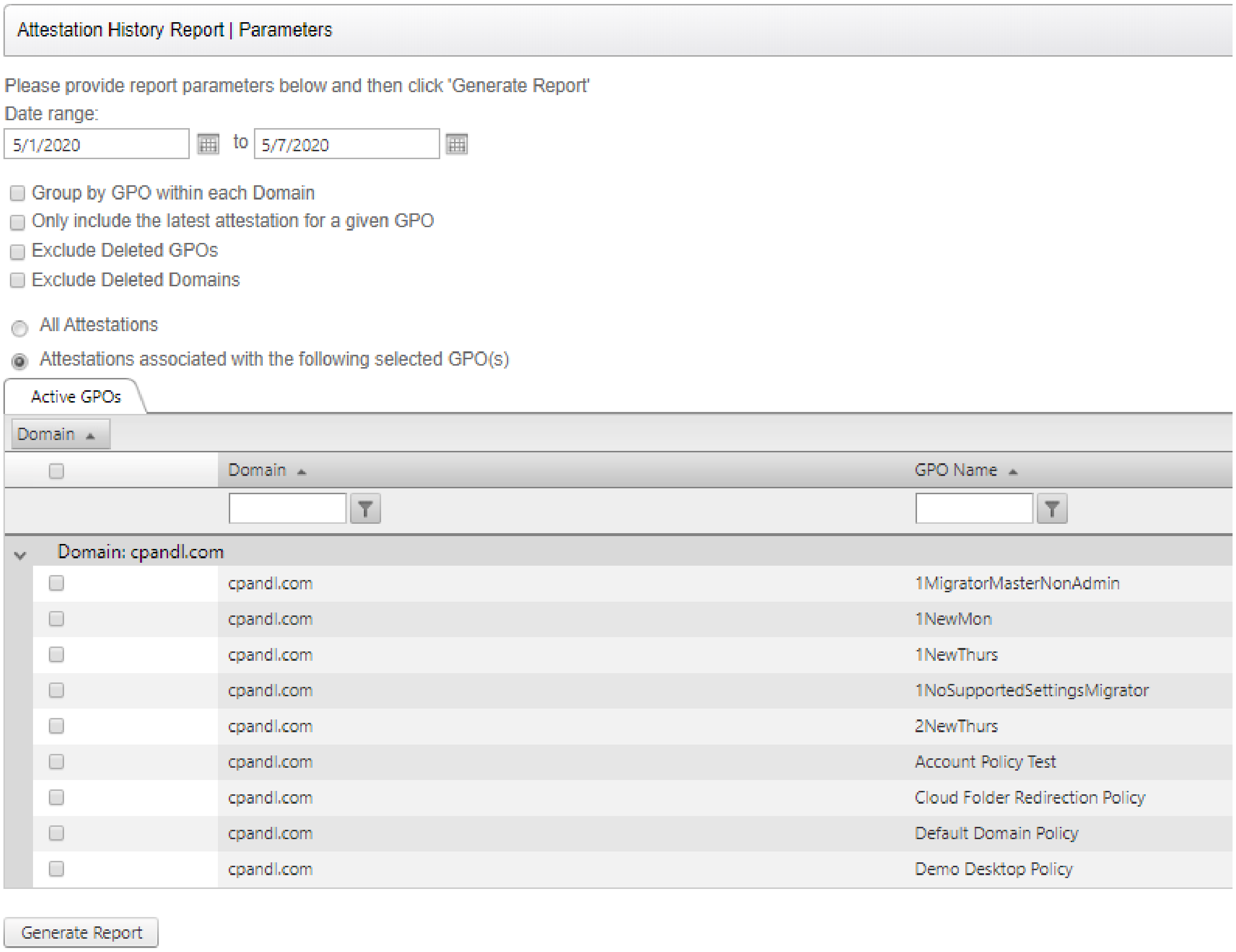


Which allows you to page through a given report, refresh the report or output it.

GPO Attestation Reports

GPOs by Owner: The GPOs by Owner report lists all GPOs active for attestation, grouped by their primary owner email addresses.

Attestation History: The Attestation History report is designed to report on completed (accepted or rejected) or incomplete attestations (i.e. attestations that are not still open). This report gives you a variety of query options, as shown here:



Attestation History Report | Parameters

Please provide report parameters below and then click 'Generate Report'

Date range:

5/1/2020 to 5/7/2020

□ Group by GPO within each Domain
□ Only include the latest attestation for a given GPO
□ Exclude Deleted GPOs
□ Exclude Deleted Domains

○ All Attestations
● Attestations associated with the following selected GPO(s)

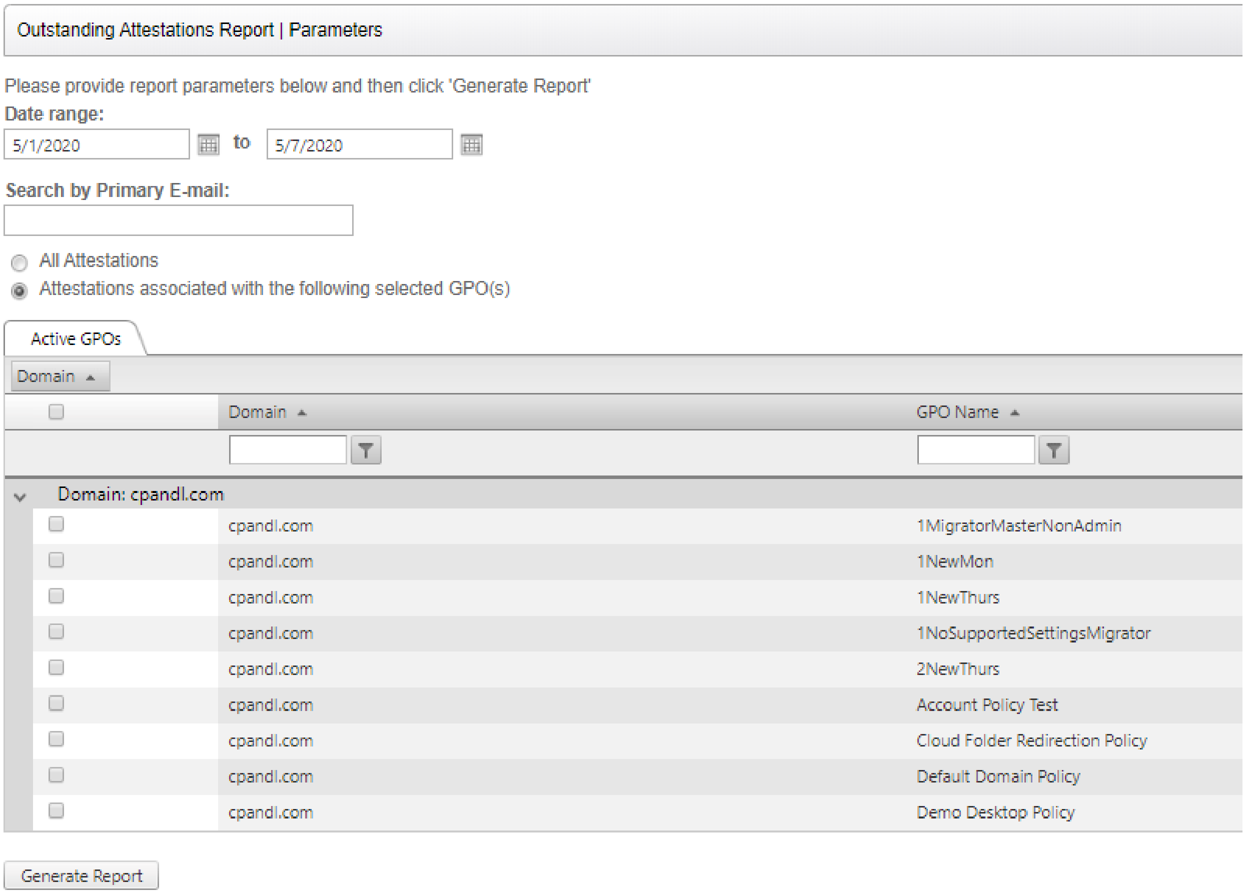
□	Domain ▲	GPO Name ▲
Domain: cpandl.com		
□	cpandl.com	1MigratorMasterNonAdmin
□	cpandl.com	1NewMon
□	cpandl.com	1NewThurs
□	cpandl.com	1NoSupportedSettingsMigrator
□	cpandl.com	2NewThurs
□	cpandl.com	Account Policy Test
□	cpandl.com	Cloud Folder Redirection Policy
□	cpandl.com	Default Domain Policy
□	cpandl.com	Demo Desktop Policy

You can choose attestations for specific GPOs, or all attestations, and you can set a date range that represents the date that the attestation was completed. You can also perform grouping and filtering based on a variety of criteria, as shown above.

Unowned GPOs: The Unowned GPOs report lists all GPOs with no primary owner associated with them, regardless of active or inactive state.

Inactive GPOs: The Inactive GPOs report lists all GPOs that are inactive, and if those GPOs have a primary owner defined.

Outstanding Attestations: The Outstanding Attestations report lists GPOs that have active attestations currently pending. You have a variety of parameters you can search on, as shown here:



Outstanding Attestations Report | Parameters

Please provide report parameters below and then click 'Generate Report'

Date range:

5/1/2020 to 5/7/2020

Search by Primary E-mail:

○ All Attestations

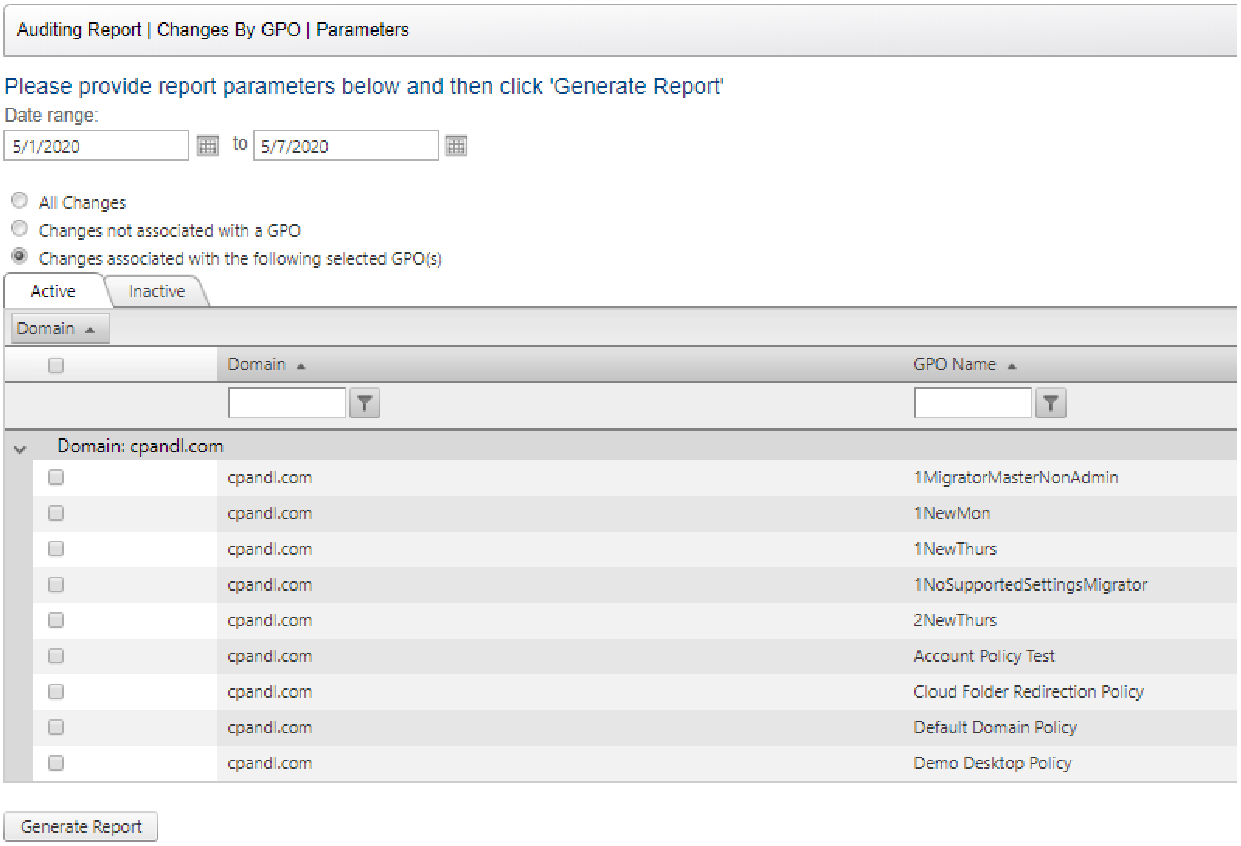
● Attestations associated with the following selected GPO(s)

□	Domain ▲	GPO Name ▲
Domain: cpandl.com		
□	cpandl.com	1MigratorMasterNonAdmin
□	cpandl.com	1NewMon
□	cpandl.com	1NewThurs
□	cpandl.com	1NoSupportedSettingsMigrator
□	cpandl.com	2NewThurs
□	cpandl.com	Account Policy Test
□	cpandl.com	Cloud Folder Redirection Policy
□	cpandl.com	Default Domain Policy
□	cpandl.com	Demo Desktop Policy

Options include the ability to search for all GPOs, or only those you specify, search by primary owner email, or search by the date range that incorporates when the first attestation email was sent.

Auditing Reports

Changes by GPO: The Changes by GPO report allows you to search for changes for all GPOs, by a given GPO, or those not associated with a GPO (e.g. changes to WMI filters or SOMs - Scopes of Management), as shown here:


Auditing Report | Changes By GPO | Parameters

Please provide report parameters below and then click 'Generate Report'

Date range:

5/1/2020 to 5/7/2020

○ All Changes
○ Changes not associated with a GPO
● Changes associated with the following selected GPO(s)

□	Domain ▲	GPO Name ▲
Domain: cpandl.com		
□	cpandl.com	1MigratorMasterNonAdmin
□	cpandl.com	1NewMon
□	cpandl.com	1NewThurs
□	cpandl.com	1NoSupportedSettingsMigrator
□	cpandl.com	2NewThurs
□	cpandl.com	Account Policy Test
□	cpandl.com	Cloud Folder Redirection Policy
□	cpandl.com	Default Domain Policy
□	cpandl.com	Demo Desktop Policy

The Date range selected here corresponds to the date that the change occurred.

GPO Changes by Date: The GPO Changes by Date report allows you to choose a start and end date to search for GPO changes. Note that this report will show all change types, including those not associated directly with a GPO.

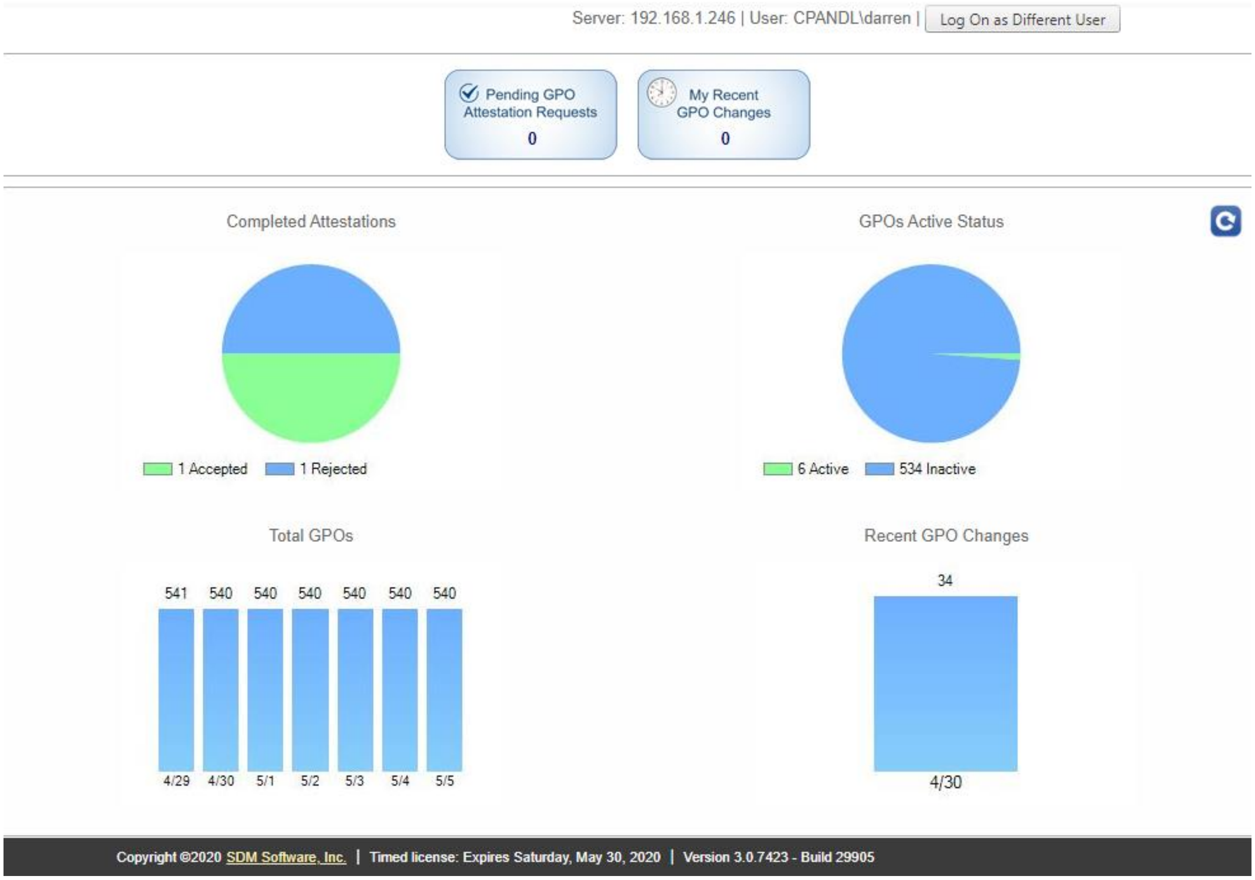
GPO Changes for User: The GPO Changes for User report allows you to report on all changes performed by a given user, and for a given date range. The user to search for needs to be provided in the **domain\user** format (e.g. mycompany\joeadmin).

GPO Change Alerts Sent: The GPO Change Alerts Sent report allows you to see who has received an email alert for a given GPO change, and when. The details of the email are not listed, but the type of change and the GPO name is listed, along with the email address of the recipient.

Rollback Events: The Rollback Events report allows you to report on any rollback operations that have occurred within a given timeframe, including when the rollback was performed, who performed it and what GPO and GPO backup timestamp was restored.

The GPAA Dashboard

The Dashboard displays on the home screen of GPAA, and when you press the **Dashboard** menu item at the top of the navigation menu. The Dashboard has a number of elements, including a set of charts and two “buttons” or widgets at the top of the screen. For users who are not defined within GPAA’s User Management (e.g. users who are only attesting to GPOs) the charts section of the Dashboard will not be displayed. Below is an example of the Dashboard:

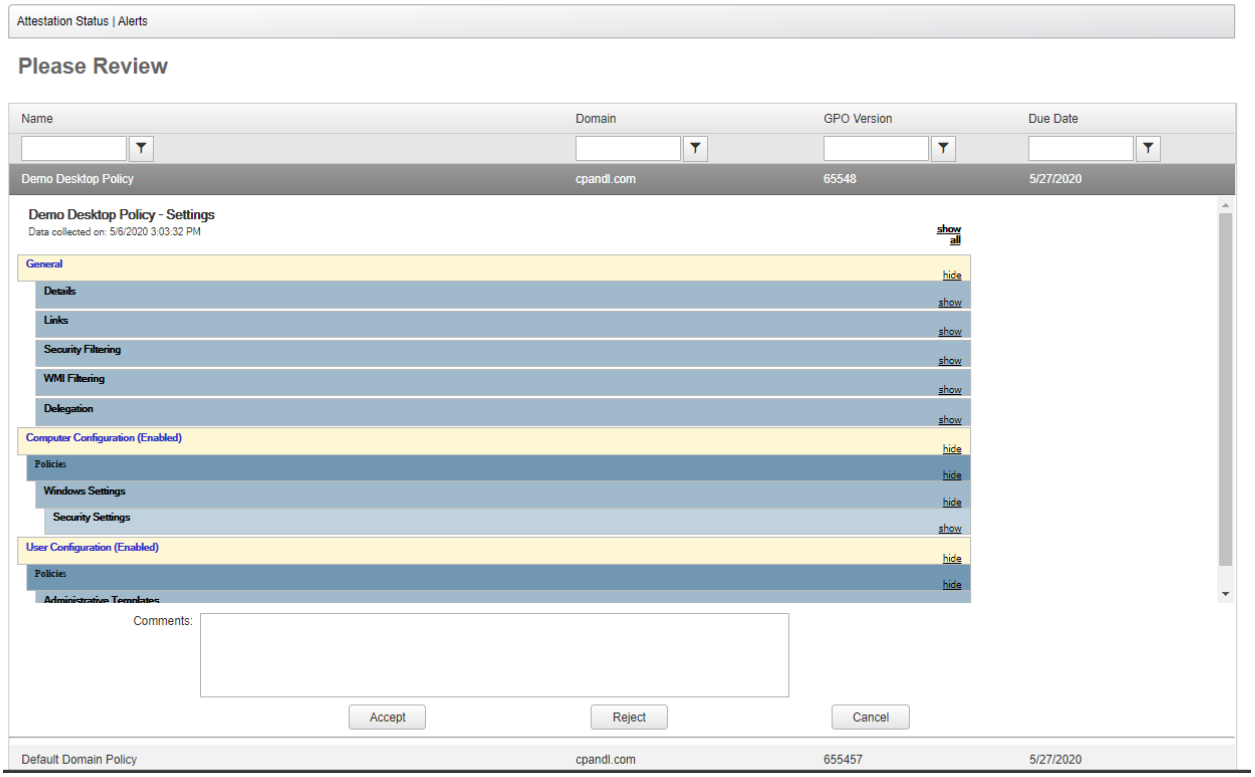


Server: 192.168.1.246 | User: CPANDL\darren |

Copyright ©2020 SDM Software, Inc. | Timed license: Expires Saturday, May 30, 2020 | Version 3.0.7423 - Build 29905

The two widgets at the top present 1) any current or upcoming attestations due for the logged in user, and 2) GPO changes that were made in the past week to GPOs for which the logged-in user is Primary Owner (matched by the email attribute on the logged-in user’s Active Directory account).

Click the top left button to get a list of the GPOs due for attestation, then click a GPO name to get its details and access to buttons to Accept or Reject, as shown here:



Attestation Status | Alerts

Please Review

Name	Domain	GPO Version	Due Date
Demo Desktop Policy	cpandl.com	65548	5/27/2020
Default Domain Policy	cpandl.com	655457	5/27/2020

Demo Desktop Policy - Settings
Data collected on: 5/6/2020 3:03:32 PM

If a selected GPO has not seen any changes since the last time that GPO was attested, you will see red text below the comments box indicating this. This is a way for the owner attesting the GPO to know that nothing has changed in the GPO since its last attestation cycle.

Pending GPO Attestation Requests display on the Dashboard **seven** days before the first attestation email is sent to the Primary Owner. This number of days can be changed on the Manage Attestations page, in the GPO Attestation tab, with the setting called "Number of Days before Attestations become pending to warn me on Dashboard."

The **version number** listed next to each Pending GPO Attestation is the GPO version as held on the AD portion of the GPO. This is a calculated version based on the number of computer and user changes on that GPO.

The **due date** listed next to each Pending GPO Attestation is the date calculated as such: the date the first attestation email was sent plus the followup notification interval’s time period plus the secondary notification interval’s time period, since this is the last day a notification will be sent about that GPO’s attestation request.

Dashboard Charts

In addition to the two buttons at the top that show currently active GPO attestations and recent GPO changes, administrators of GPAA will see a set of three to four Dashboard charts (users that have not installed the GPAA auditing service will only see three charts). These charts are explained here:

Completed Attestations – A pie chart that shows the number of attestations that were accepted vs. rejected in the past week.

GPOs Active Status – A pie chart that shows the current number of GPOs, broken into those that are active for attestation and those that are not.

Total GPOs – the count of GPOs from all domains managed by GPAA, from the past week.

GPO Changes – A bar graph that shows the number of all GPOs changes by day for the last week.

The Perform Rollback Menu

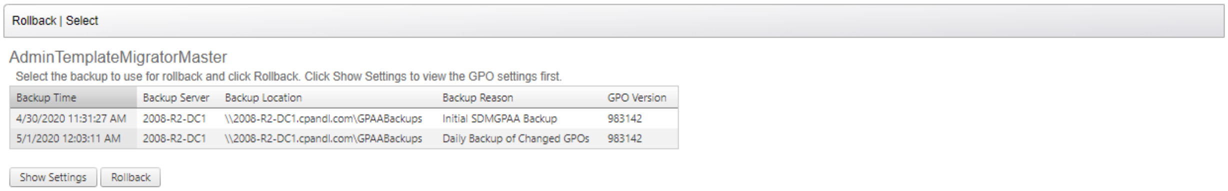
The Rollback section of GPAA Manager provides an easy way to revert GPOs to prior versions after a change occurs. Note that the rollback feature currently supports rolling back only GPO changes. It does not support rolling back changes to GPO links, SOM (Scope of Management) changes or WMI filters.

In order to see this section of GPAA Manager, users must be added within User Management and given the Rollback Operator role.

To see a list of GPOs with backups, click the **Perform Rollback** link in the **Rollback** menu section. The list of GPOs with backups is separated into tabs by attestation status - Active or Inactive - and whether the GPO has been deleted from GPMC. A GPO will display in this list only if there is at least one backup for it, performed by the GPAA auditing service. The auditing service will create an initial backup for all GPOs in domains that have been added to the Domains page once the auditing service is installed on each domain. Additional backups are created at midnight if a change is made to a GPO. The backup time is the local time of the server where auditing is installed. To change the backup time, use the configuration utility that gets installed with the auditing service on the primary domain controller.

The default number of backups to keep for rollback purposes is 5, but this number can be changed by clicking the **Manage Auditing** link in the **Manage Product** menu section and changing the value next to "Number of GPO Backups to Keep for Rollback." Backups are kept for deleted GPOs, which are sorted at the top of the list. Note that backups are stored on the AD PDC Emulator DC within the file system, so care should be taken before expanding the backup depth too large, to ensure the DC has enough disk space.

You can display a list of backups for a specific GPO by clicking the GPO name from under the Deleted, Active or Inactive tabs. You have the option to view the settings in a particular backup prior to reverting it. Just select the backup you wish to view from the list (see below) and then press the **Show Settings** button. An HTML settings report showing the contents of the GPO will appear below. Then, select the backup you wish to revert the GPO to and click the **Rollback** button. The current live GPO is overwritten with the backup (note: existing settings are completely overwritten—no merging of settings occurs).



AdminTemplateMigratorMaster

Select the backup to use for rollback and click Rollback. Click Show Settings to view the GPO settings first.

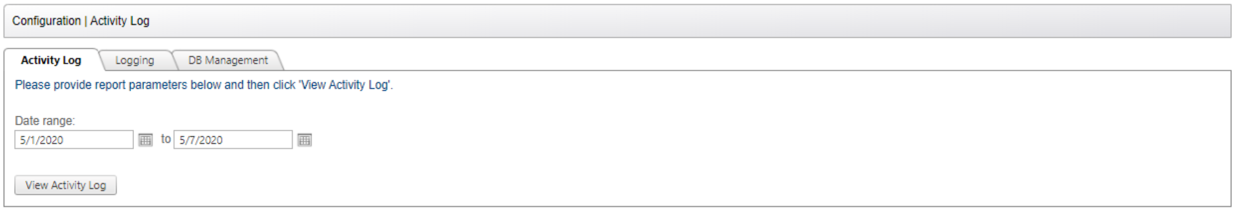
Backup Time	Backup Server	Backup Location	Backup Reason	GPO Version
4/30/2020 11:31:27 AM	2008-R2-DC1	\\2008-R2-DC1.cpandl.com\GPAABackups	Initial SDMGPAA Backup	983142
5/1/2020 12:03:11 AM	2008-R2-DC1	\\2008-R2-DC1.cpandl.com\GPAABackups	Daily Backup of Changed GPOs	983142

Advanced GPAA Management Tasks

Powershell

Activity Log

GPAA provides an audit log of its and users' activities, called the Activity Log. The Activity log is accessible from the main menu, under the Configuration Section, as shown here:



Please provide report parameters below and then click 'View Activity Log'.

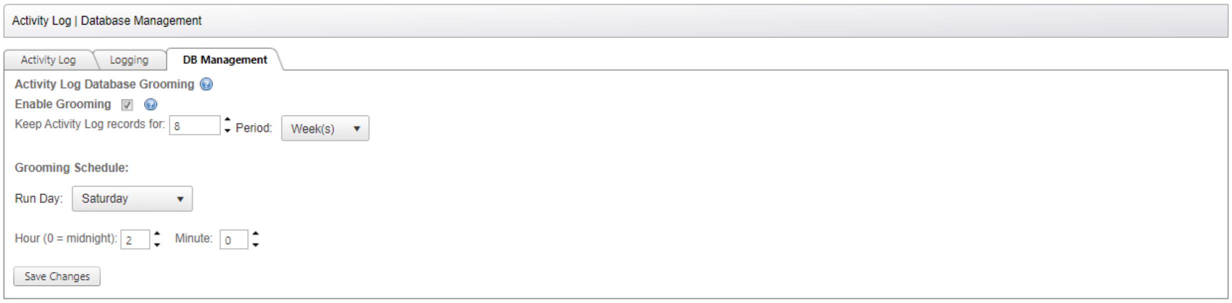
Date range: 5/1/2020 to 5/7/2020

You can enter a date range to view activities within that range. The Activity Log report shows the date/timestamp of the activity, the user who performed the activity, and the details of the activity. Some activities are performed by end users. Other activities are performed by GPAA itself, and those records will show the username as "GPAA Attestation Service" or just "GPAA."

You have the option to have all activity log records sent to a special Event Log on the server where the GPAA attestation service is running. This log can be found in the Event Viewer under **Applications and Services Logs\SDM Software**. Logging activities to the event log is not enabled by default. If you select the **Logging** tab from the screen above, you can enable event log logging for all activities. Make sure to press the **Save Changes** button after enabling or disabling event logging.

DB Management—Grooming the Activity Log

The DB Management tab on the Activity Log menu allows you to configure grooming of the Logs table within the GPAA database. Grooming is a process by which old data is deleted from the GPAA database, based on your criteria. From this menu, you have the ability to enable grooming for the Logs table, as shown here:



Activity Log Database Grooming

Enable Grooming ☑

Keep Activity Log records for: 8 Period: Week(s)

Grooming Schedule:

Run Day: Saturday

Hour (0 = midnight): 2 Minute: 0

Once grooming is enabled by selecting the **Enable Grooming** checkbox, you can configure the following options:

Keep Activity Log records for __ Period: This allows you to configure how long to keep Activity Log data before it is deleted from the GPAA database. This can be set from 1 week or longer, depending upon how much data you want to keep and how large the GPAA SQL Server database will get.

Grooming Schedule—Run Day and Hour: The grooming process, once enabled, runs once per week. You can control what day and time the process runs by setting the **Run Day** and **Hour** options on this screen.

Once all settings have been defined, make sure you press the **Save Changes** button to commit the grooming schedule and status.

Appendix A: Event Log IDs Generated by GPAA

GPAA logs two main types of events to the Windows Event Log. GPAA attestation service debug logs are sent to the Windows Application event log. And, if enabled from the Activity Log menu, GPAA Activity Log events are sent to an **SDM Software** log under **Applications and Services Logs** in the Windows Event Viewer. Each different type of event has a different event log ID and source, depending upon its usage. These are defined in the following table

Event Type	Event ID	Event Log Name	Description
Debug logging for GPAA attestation service	None	Application Event Log	Logged with Event Source: "SDM GPAA Attestation Service"
Activity Log	100	SDM Software Log	Changes to Attestation configuration
Activity Log	101	SDM Software Log	Email Notifications sent
Activity Log	102	SDM Software Log	Audit Agent status changes
Activity Log	103	SDM Software Log	GPO Rollback performed
Activity Log	104	SDM Software Log	Domains added/removed
Activity Log	105	SDM Software Log	GPO Status changes (e.g. activated, inactivated)
Activity Log	106	SDM Software Log	GPO Email changes (e.g. changes to owner and support emails)
Activity Log	108	SDM Software Log	Changes to User Management
Activity Log	109	SDM Software Log	Attestation Grooming Performed
Activity Log	110	SDM Software Log	Audit Grooming Performed
Activity Log	111	SDM Software Log	Activity Log Grooming Performed
Activity Log	112	SDM Software Log	Grooming Check Performed

Activity Log	113	SDM Software Log	Dashboard updates performed
Activity Log	115	SDM Software Log	Attestation email sent
Activity Log	116	SDM Software Log	New GPO Discovered by GPAA
Activity Log	117	SDM Software Log	Existing GPO marked deleted in database
Activity Log	118	SDM Software Log	Existing GPO renamed in database
Activity Log	119	SDM Software Log	GPO status changed from deleted to inactive
Activity Log	120	SDM Software Log	A GPO attestation was marked incomplete because it passed the due date and grace period.

Appendix B: GPAA Auditing & GPAA Attestation Service Configuration Settings

There are some service-specific configuration options available within both the GPAA Auditing Service and GPAA Attestation Service. Generally these should not be adjusted unless SDM Software Support has recommended it, but the options are documented here.

GPAA Auditing Service

The GPAA Auditing Service configuration file is stored within the Program Files folder where the Auditing Service is installed (usually on every writeable domain controller). The configuration file is called **GPAuditService.exe.config** (or GPAuditService7.exe.config on Windows 2008-R2 DCs). This config file is an XML file that can be edited directly, when recommended by SDM Software Support. NOTE: If you see a value in the configuration file that is not shown here, that is because that setting is not recommended to be adjusted. The following are parameters that can be adjusted within this file.

Parameter Name	Description	Default Value
ReadQueueInterval	Interval, in milliseconds, that the Auditing Service will look for new events on the queue and process them.	5000
EventLookupInterval	Interval, in milliseconds, that the Security Event Log on DCs are polled	5000
SettingsRefreshInterval	The frequency in milliseconds, that the Auditing Service updates its local cache of GPOs, GPO owner and support emails, SMTP settings and global settings	300000
dbConnection	The database connection string used by the auditing service to talk to the GPAA database	
GPOBackupTime	The time that GPO backups will be performed on GPOs that have changed (on the PDC emulator only)	12:00:00 AM

MaxEmailThreshold	The number of changes seen by the auditing service for a given GPO, before those changes are bundled into a single notification email (as a CSV attachment)	10

GPAA Attestation Service

The GPAA Attestation Service configuration file is stored within the Program Files folder where the Attestation Service is installed. The configuration file is called **SDM GPAA Attestation Service.exe.config**. This config file is an XML file that can be edited directly, when recommended by SDM Software Support. NOTE: If you see a value in the configuration file that is not shown here, that is because that setting is not recommended to be adjusted. The following are parameters that can be adjusted within this file.

Parameter Name	Description	Default Value
OverdueGraceInDays	This parameter controls how long after the due date for an open attestation, that attestation will be marked incomplete by GPAA. The value is in days.	14