Group Policy Auditing and Attestation

SDM Software Group Policy Auditing & Attestation

Version 2.5

User Guide

Revision May 2017

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 and Group attestations, keep track of responses, and monitor your GPO environment to meet auditing requirements. With GPAA, you can:

- Automatically send periodic emails to GPO and AD Group 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 and Groups, unattested GPOs and Groups, 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

The first user to log in to GPAA Manager, where the services are configured, will be designated during the setup 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 User Management, and their roles assigned as desired.

The IIS-based web front-end, GPAA Manager, uses Microsoft's Integrated Windows Authentication 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, for those instances when you're logged onto the workstation as someone other than your domain administrative ID, but this feature results in limited functionality and should be used only temporarily.

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

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

Step 2: Add users in User Management, if necessary. Note that a user does not need to be added in order to be assigned as a primary or secondary owner/support person for a GPO or Group, 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 and Group Owners and Support emails. GPO and Group Owner email addresses receive attestation emails; GPO Support email addresses receive auditing change alert emails. Set GPO and Group statuses to Active on the Manage GPOs and Manage Groups pages. A status of Active will begin the attestation process. The Auditing service will automatically begin sending emails to Support email addresses after the Auditing service detects changes to ownership. This is usually after a 15 minute polling interval configured at the auditing service on each domain controller.

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 they are manually made active, then a year after they are attested, in a repeating cycle until the GPO or Group is set to Inactive status.

See Rollbacks for more information on rolling GPOs back to backups performed by the auditing service.

Configuration

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 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.

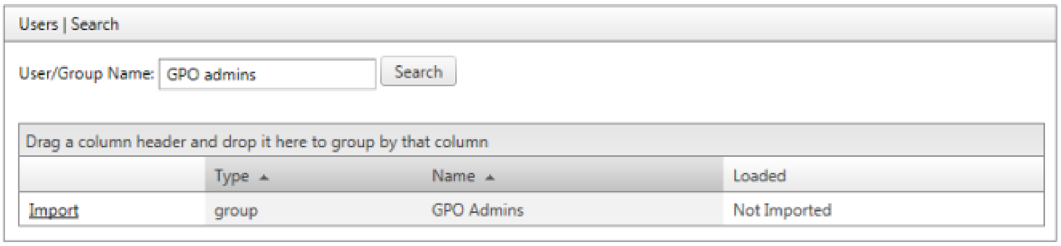
The next step is to configure the mail server in order for auditing and attestation emails to be sent.

Domains

Mail Server

User Management

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



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. By default, the user or group designated in the setup utility has all roles.

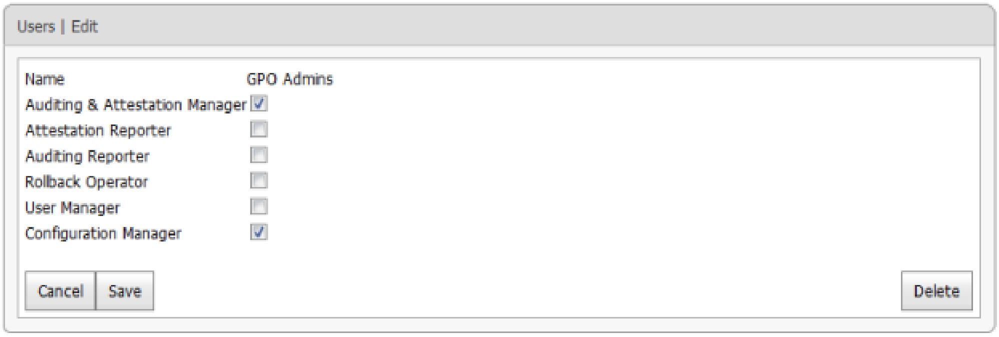
Add Users

To add a user or group, click the Manage Users link. Then click the "Add a user or group" button. Users must exist in the domain where GPAA Manager and its database are installed. Enter the user or group name in the text box and click Search. If the user or group name exists, it will be displayed in a list. The Loaded field indicates a "True" or "False" based on whether they are already added to GPAA Manager. If they have not already been added, click the Import link. Then assign them permissions by checking next to the roles they should receive, which will allow them to view those sections when logged in to GPAA Manager.

Note that a user does not have to be added to the User Management section in order to receive attestation emails, or attest a GPO or Group. In order to be the primary or secondary owner (in order to attest), the owner's email address just needs to be assigned to that GPO or Group in the Manage GPOs or Manage Groups section, as a Primary Owner or Secondary Owner.

Edit Users

To change roles for a user or group, click the Manage Users link in the User Management section. Then click the user or group name. Check or uncheck the checkbox next to the role names for that user, based on which permissions they should have.



Name	GPO Admins
Auditing & Attestation Manager	☑
Attestation Reporter	☐
Auditing Reporter	☐
Rollback Operator	☐
User Manager	☐
Configuration Manager	☑

Roles

Roles granted to an Active Directory group will allow any member of that group to log into GPAA Manager and have those roles.

Auditing & Attestation Manager - Can view and edit the Manage Product section, including Manage Auditing, Manage Attestation, Manage GPOs and Manage Groups pages.

GPO Attestation Reporter - Can view GPO attestation reports.

Group Attestation Reporter - Can view Group attestation reports.

Auditing Reporter - Can view auditing reports.

Rollback Operator - Can view the Rollback section and perform rollbacks.

User Manager - Can view and edit the User Management section, which includes the ability to add users or Active Directory groups, and assign roles.

Configuration Manager - Can view and edit the Configuration section, including Domains and Mail Server pages.

Manage Product

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, the GPOs and Groups 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 Support users to receive auditing emails.

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.

To see this section of GPAA Manager, users must be added within User Management and given the Auditing/Attestation Manager role. By default, the user designated in the setup utility has all roles.

Manage GPOs

Assign emails on a per-GPO basis to use 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.

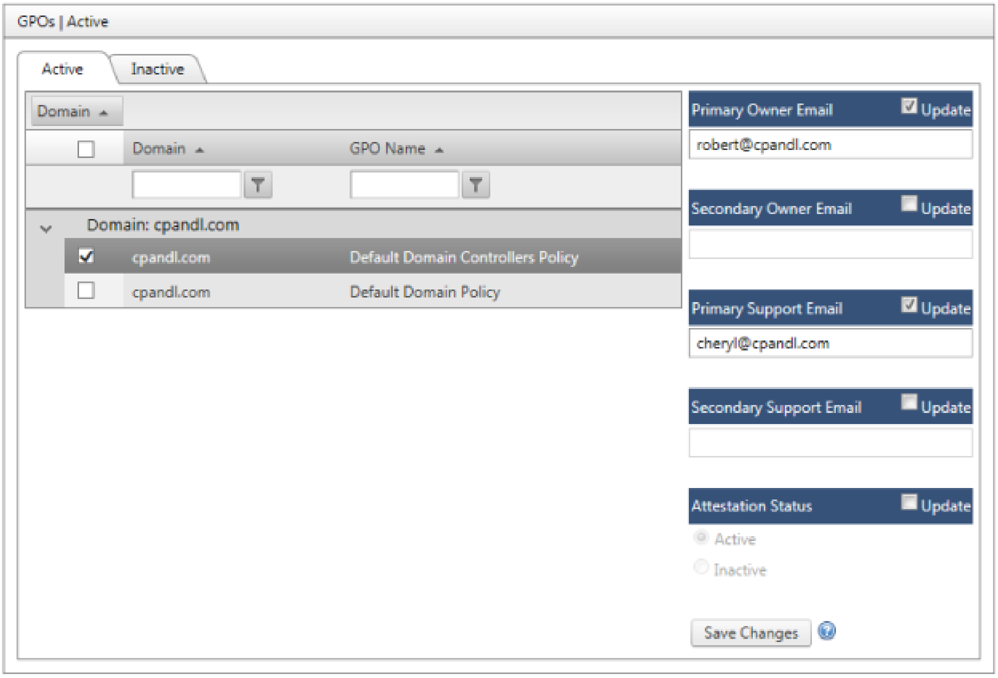
Attestation emails are sent to the Primary and Secondary Owner emails. The Secondary Owner email field is optional; if used, they will receive an email if the Primary Owner does not respond to the initial or follow-up email. The amount of time between each of the initial, follow-up, and secondary emails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

Auditing emails are sent to the Primary and Secondary Support emails, and the General Alerts Email found on the Configuration - Mail Server page. 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'd 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.

Search for a GPO by typing its name into the GPO Name 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

Manage Groups

Assign emails on a per-Group basis to use for attestation, and set their statuses to Active in order to start the attestation process.

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 - Group Attestation page.

The list of Groups is separated into tabs by attestation status - Active or Inactive. A third tab is for the Delete Queue (see below). To update a field, click the checkbox to the left of the Group name, then click the Update checkbox to the right of the field you'd like to update. Enter the data, then click Save Changes. The same information can be entered for more than one Group by checking multiple checkboxes to the left of the Groups.

Groups 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.

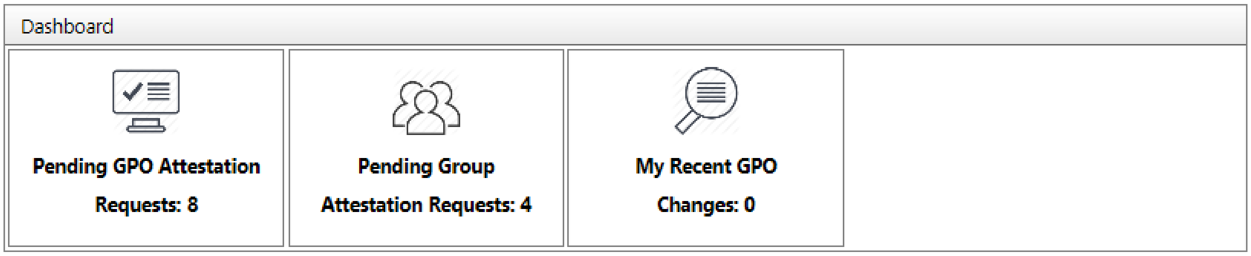
Search for a Group by typing its name into the Group Name text box at the top of the list. Click the Filter button to refine the search with different filter types.

Delete Queue

A Group owner can click a button on the Dashboard to request to have the Group not only rejected but deleted from Active Directory. If "Reject/Delete" is clicked by the Group owner, an email will go to the General Alerts Email (defined on the Configuration - Mail Server page) with a request for deletion, and the Group will display in the Delete Queue tab. If deleted from the Delete Queue tab, the Group is deleted from Active Directory. "Remove from List" can be clicked in the tab for a Group, if a user does not want to delete it from Active Directory. The Group will then remain in the Active or Inactive tab, depending on which of those tabs it was in last.

Dashboard

The Dashboard displays at the top of the default page, and can be found again by clicking the top left GPAA icon. A GPO or Group owner is also taken here when the link in an attestation email is clicked, to accept or reject an attestation. It is a quick glance into upcoming attestations due for the logged in user, and GPO changes that were made in the past week, to GPOs of which the logged-in user is Primary Owner (matched by email address).


Dashboard
Pending GPO Attestation Requests: 8
Pending Group Attestation Requests: 4
My Recent GPO Changes: 0

Click each square to get a list of the GPOs or Groups due for attestation, then click a GPO or Group name to get its details and access to buttons to Accept, Reject, or Reject/Delete.

Pending GPO and Group 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 GPOs and Groups tabs, with the setting called "Number of Days before Attestations become pending to warn me on Dashboard."

The Due Date listed next to each Pending GPO and Group Attestation is the date that the Secondary Owner receives an attestation email, since this is the last notification that will be sent about that GPO/Group's attestation request.

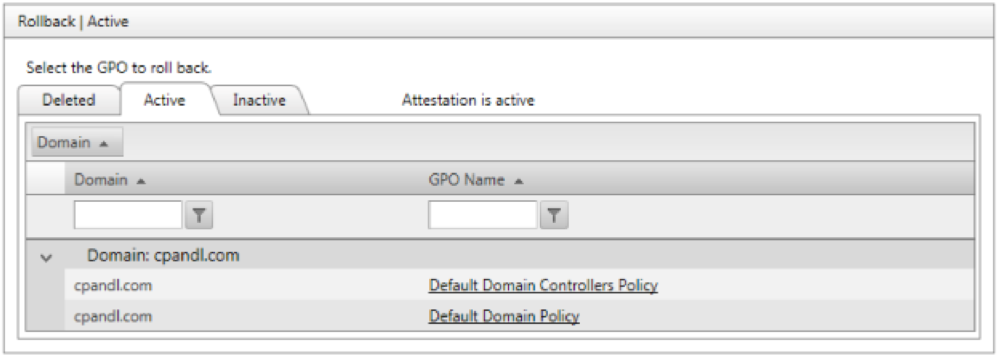
GPO Rollback

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. By default, the user designated in the setup utility has all roles.

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 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 sufficient disk space.

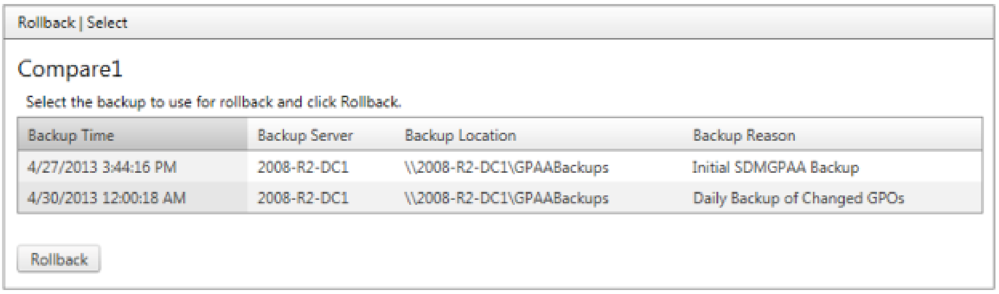


Select the GPO to roll back.

Attestation is active

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

Display a list of backups for a specific GPO by clicking the GPO name. Select the backup you wish to revert the GPO to and click Rollback (see below). The current live GPO is overwritten with the backup.



Compare1

Select the backup to use for rollback and click Rollback.

Backup Time	Backup Server	Backup Location	Backup Reason
4/27/2013 3:44:16 PM	2008-R2-DC1	\\2008-R2-DC1\GPAABackups	Initial SDMGPAA Backup
4/30/2013 12:00:18 AM	2008-R2-DC1	\\2008-R2-DC1\GPAABackups	Daily Backup of Changed GPOs

Advanced

Manage Auditing

Settings

Number of GPO Backups to Keep for Rollback - The auditing service will save 5 backup versions of GPOs by default. New backups are created once a day (midnight by default), if a change is made to a GPO. Once the maximum number of backups is reached, the service will delete the oldest backup when new ones are made. Change the number here, if desired, and click Save Changes. This number affects all GPOs in all domains listed on the Configuration | Domains page. Keep in mind that backups are only stored on the Active Directory Domain Controller (PDC) emulator.

DC Status

Offline Alerting will notify the General Alerts Email address, defined on the Configuration - Mail Server page, if a domain controller's agent is no longer communicating with the GPAA server, meaning that the GPO auditing service is down. Control when and how often alerts will be sent with the fields on this page.

DC to Agent Heartbeat Interval (minutes) - How often each domain controller checks in with the database, which in turn tells the Agent Heartbeat Service that it's running.

Agent Heartbeat to DC interval (minutes) - How often the attestation service checks to see if a domain controller has checked in recently.

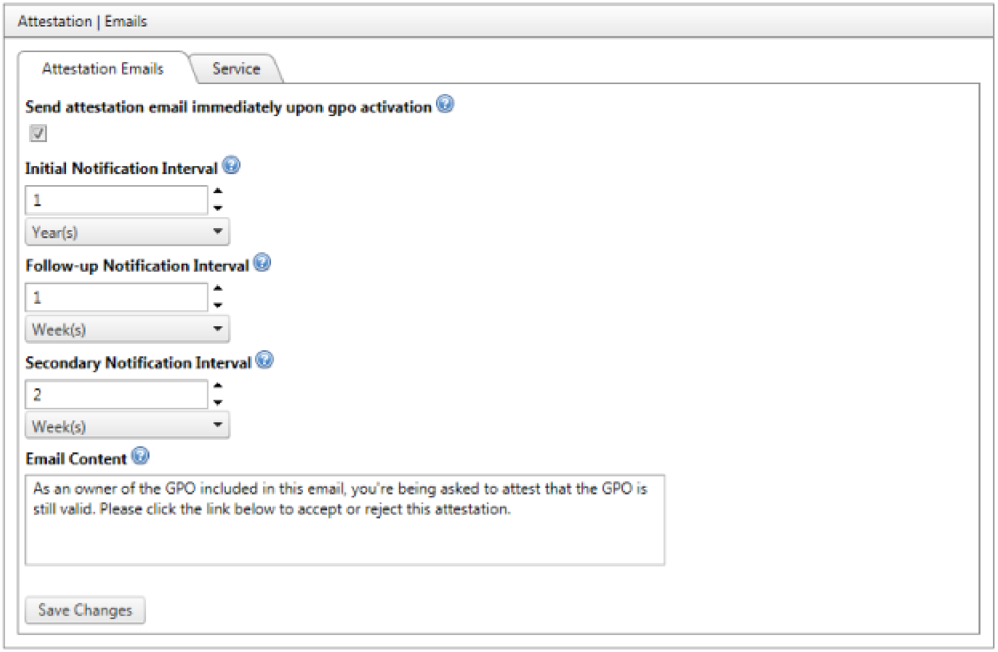
Minutes DC must be offline before alert is sent - How long the attestation service waits before declaring a domain controller's auditing service offline and sending an alert.

Maximum number of alerts to send per offline event - The number of times the attestation service sends an alert about an offline domain controller to the General Alerts Email defined on the Configuration - Mail Server page.

Manage Attestation Emails

GPO Attestation

Settings in the Manage Attestation tab for GPO Attestation affect all GPOs that have a status of Active on the Manage GPOs page. Attestation emails are sent out automatically for Active GPOs, in cycles based on the settings below:



Send attestation email immediately upon gpo activation
☑

Initial Notification Interval
1
Year(s)

Follow-up Notification Interval
1
Week(s)

Secondary Notification Interval
2
Week(s)

Email Content
As an owner of the GPO included in this email, you're being asked to attest that the GPO is still valid. Please click the link below to accept or reject this attestation.

Settings are broken into two types:

Existing GPOs - These are GPOs that are currently in Active Directory, and display in your Active or Inactive tabs of the Manage GPOs page.

New GPOs - This refers to future GPOs that are created in Active Directory, which will be detected by GPAA Manager and displayed in the Active or Inactive tab, depending on the setting you choose in this section.

For Existing GPOS, selecting "Attest immediately upon manual activation" will ensure that attestation emails will be sent immediately after a GPO is marked Active on the Manage GPOs page, regardless of the Initial Notification Interval setting. If the other option is selected, the initial attestation email will be sent once the Initial Notification Interval passes. In either case, once an attestation email is sent, the cycle begins again once the GPO is accepted or rejected.

For New GPOs, selecting "Automatically activate; attest immediately using __" will set any newly detected GPOs immediately to the Active status, display them in the Active tab, and insert the email address you type here into the Primary Owner field. It will then immediately send an attestation email to that email address. If the other option is selected, "Manually activate, then treat as Existing GPO," newly detected GPOs will be given an Inactive status. Users will have to manually change the new GPO to Active, and add a Primary Owner email address. The GPO will then use whatever setting is selected in the Existing GPOs section, to determine whether to immediately send the attestation email once manually activated, or to wait until the initial notification interval passes in order to send the attestation email.

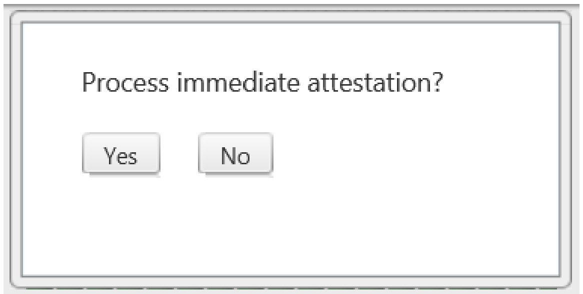
For all settings that are selected, if the GPO is not attested from the first email (responded as accepted or rejected) within the amount of time set for the Follow-up Notification Interval, a followup email will be sent to the Primary Owner. If they do not attest the GPO within the amount of time set for the Secondary Notification Interval, which counts the time starting from when the followup email was sent, an email will be sent to the Secondary Owner. Any GPOs that have not been attested will be listed in the Outstanding Attestations report, and will **not** receive a new cycle of attestation emails.

If a GPO is changed to Inactive on the Manage GPOs page, no more attestation emails will be sent. If an attestation email had already been sent for that GPO while it had a status of Active, the GPO Attestation History report will show a Response of "Incomplete - Due to gpo inactivation."

Number of Days before Attestations become pending to warn me on Dashboard - This setting affects when to display a GPO or group needing attestation on the Dashboard, the 3 square tiles on the home page. This is the number of days before the first email will go to the Primary Owner of the GPO or group, requesting attestation. If many attestations are due around the same time, users may wish to avoid receiving emails for the attestations, and instead go to the Dashboard to attest or reject all pending attestations in one place.

Changing GPO Owners

If you change the owner of a GPO, you have the ability to trigger an automatic attestation. When you change the primary owner of a GPO, the following dialog appears:



Process immediate attestation?

If you answer “Yes” to the dialog, then a new attestation for the new owner will be triggered immediately.

Group Attestation

As with GPO Attestation, settings in the Manage Attestation tab for Group Attestation affect all Groups that have a status of Active on the Manage Groups page. Attestation emails are sent out automatically for Active Groups, in cycles based on the settings on this tab.

Settings are broken into two types:

Existing Groups - These are Groups that are currently in Active Directory, and display in your Active or Inactive tabs of the Manage Groups page.

New Groups - This refers to future Groups that are created in Active Directory, which will be detected by GPAA Manager and displayed in the Active or Inactive tab, depending on the setting you choose in this section.

For Existing Groups, selecting "Attest immediately upon manual activation" will ensure that attestation emails will be sent immediately after a Group is marked Active on the Manage Groups page, regardless of the Initial Notification Interval setting. If the other option is selected, the initial attestation email will be sent once the Initial Notification Interval passes. In either case, once an attestation email is sent, the cycle begins again once the Group is accepted or rejected.

For New Groups, selecting "Automatically activate; attest immediately using __" will set any newly detected Groups immediately to the Active status, display them in the Active tab, and insert the email address you type here into the Primary Owner field. It will then immediately send an attestation email to that email address. If the other option is selected, "Manually activate, then treat as Existing Group," newly detected Groups will be given an Inactive status. Users will have to manually change the new Group to Active, and add a Primary Owner email address. The Group will then use whatever setting is selected in the Existing Groups section, to determine whether to immediately send the attestation email once manually activated, or to wait until the initial notification interval passes in order to send the attestation email.

For all settings that are selected, if the Group is not attested from the first email (responded as accepted or rejected) within the amount of time set for the Follow-up Notification Interval, a follow-up email will be sent to the Primary Owner. If they do not attest the Group within the amount of time set for the Secondary Notification Interval, which counts the time starting from when the follow-up email was sent, an email will be sent to the Secondary Owner. Any Groups that have not been attested will be listed in the Outstanding Attestations report, and will **not** receive a new cycle of attestation emails.

If a Group is changed to Inactive on the Manage Groups page, no more attestation emails will be sent. If an attestation email had already been sent for that Group while it had a status of Active, the Group Attestation History report will show a Response of "Incomplete - Due to group inactivation."

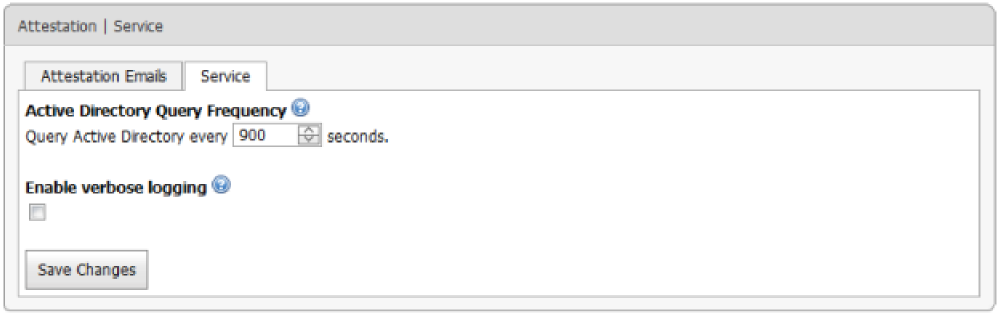
Changing Group Owners

Just as with GPO attestation, if you change the primary owner of a group, you have the option to trigger an immediate attestation.

Manage Attestation Service

Set the Active Directory Query Frequency to the number of seconds you'd like the attestation service to wait to check for added, deleted, or changed GPOs, Groups, or domains, in order to refresh information displayed in the GPAA Manager. Click Save Changes.

Check the "Enable verbose logging" checkbox to log attestation service activities in the Windows application event log for debugging purposes (see below). Click Save Changes to commit the change.



Active Directory Query Frequency

Query Active Directory every 900 seconds.

Enable verbose logging

□