SDM Software Group Policy Auditing & Attestation

Version 3.0

Installation Guide

Revision April 2020

Contents

Overview 3

The Components of GPAA 3

- Separating GPAA Components 4
- Network and Port Usage for GPAA 4
  - GPAA ASP.Net Web Application 5
  - GPAA ASP.Net Web Service Proxy 5
  - GPAA Attestation Service 5
  - GPAA Auditing Service 6
  - GPAA Untrusted Proxy Service 6
- GPAA Server Requirements and Software Prerequisites 6
  - Supported Windows OS Version 7
  - Component Requirements 7

GPAA Security & User Accounts 8

Requirements for Active Directory Auditing 9

Step-by-Step Installation & Upgrade 14

1. Set up the GPAA Database 15
2. Set up the GPAA Web/Proxy Applications 18
4. Set up the GPAA Attestation Service 22
5. Set up the GPAA Auditing Service 24
6. Set up the GPAA Untrusted Proxy Service 27

Support 28

Appendix A: Installing the GPAA Auditing Agent as LocalSystem 29

Overview

This guide provides detailed information on the installation of GPAA. GPAA provides Group Policy change auditing, Group Policy attestation/re-certification and Group Policy Object (GPO) change rollback. The product has several components and a set of environmental requirements that must be adhered to in order to create a successful installation. This document details those requirements and how you can deploy GPAA to either a new or existing GPAA environment.

The Components of GPAA

GPAA is composed of the following components:

1. **GPAA Web Application ("GPAA Manager")** – An ASP.Net 4.0 (or greater) web application
2. **GPAA Database** – Installed on SQL Server 2014 (normal or Express version) and above (currently tested through SQL Server 2019)
3. **GPAA Attestation Service** – a Windows Service that works with the GPAA Web Application and performs several functions, including managing attestation workflow, addition/deletion of new/removed GPOs and more. Can be deployed on the same or a different server as the GPAA web application
4. **GPAA Auditing Service** – A Windows Service to be installed on all domain controllers within your environment, if you wish to perform Group Policy change auditing, rollback and alerting. (N*ote that the GPAA auditing service is only required if you are performing real-time change auditing and alerting or GPO rollback. It has no role in GPO Attestation.*)
5. **GPAA Web Service Proxy Application** – Optional, an ASP.Net 4.5+ web service, which can run on the same web server as the main GPAA Web Application. The Web Service is the "listener" for the next component—the GPAA Untrusted Proxy Service.
6. **GPAA Untrusted Proxy Service**— Optional, a .Net 4.52 Windows Service, installed on a server within the untrusted domain, that communicates with the GPAA Web Proxy Service Application to perform untrusted attestations.

In the simplest configuration, #1-3 and #5 can run on a single server, as shown in Figure 1 below:

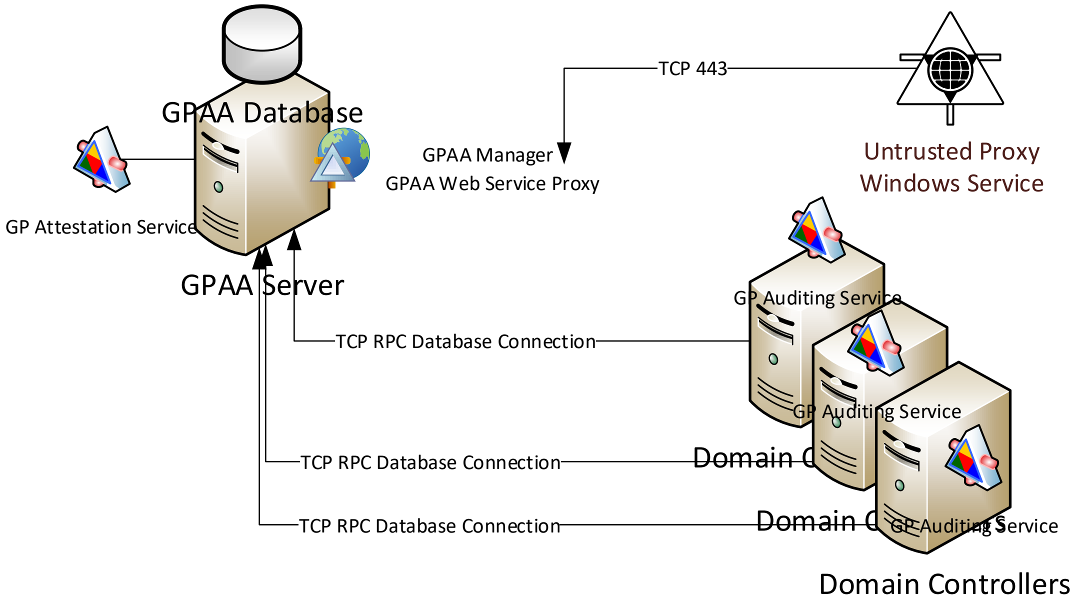


Figure 1: Viewing a typical GPAA Deployment

The first 3 components on the GPAA server — GPAA Manager, the GPAA database, and the GP Attestation Service – work together to create the GPAA application. The GPAA Auditing Service and the GPAA Untrusted Proxy Service are the only components that must run on a separate box. The Auditing Service is intended to be installed and run on each writeable domain controller within a domain that GPAA is managing. The Proxy Service can be installed on a single server within the untrusted domain.

NOTE: Installation of the GPAA Auditing Service and the GPAA Web Service Proxy Application / GPAA Untrusted Proxy Service are only required if you plan to use the Group Policy Change Auditing and Rollback features or Untrusted Domain GPO Attestation feature.

Separating GPAA Components

In enterprise environments where existing shared SQL Server farms are in place, it is completely supported to run the GPAA database on a different server than the Server where the GPAA Manager, Proxy and Attestation Service run. In addition, if needed, the **GPAA Manager Web application, Web Service Proxy and GPAA Attestation Service** can also each be installed on separate servers. To facilitate using a database on a separate server, you'll need to ensure that when you run the GPAA web application setup and the GPAA Attestation Service Setup, that you select the correct database server name, port and instance (where appropriate). The next section on "Network and Port Usage for GPAA" describes how each component communicates over the network to other components and to Active Directory.

Network and Port Usage for GPAA

This guide lists the network ports and protocols used between the various components within the SDM Software Group Policy Auditing & Attestation (GPAA) product.

Each section below covers the ports and protocols used by each of these components.

GPAA ASP.Net Web Application

The GPAA ASP.Net web application ("GPAA Manager") performs the following functions and uses the following ports and protocols:

- IIS authenticates the user to Active Directory
    - **TCP 389 (or 636 if LDAPS is enforced) from web server to closest AD domain controller**
    - **TCP or UDP (usually TCP) 88 (Kerberos) from web server to closest AD domain controller**
- IIS/ASP.Net makes GPMC API Calls
    - **TCP 445 to closest AD domain controller**
    - **TCP 135 (RPC Portmapper) to closest AD domain controller**
    - **TCP 49152-65535. (RPC dynamic ports) to closest AD domain controller**
- IIS/ASP.Net application communicates to GPAA SQL Server
    - **TCP 1433 or dynamic high-numbered port (See your SQL Server Services Configuration to verify which port SQL Server is listening on)**
- IIS/ASP.Net sends attestation rejection or general alert emails
    - **TCP SMTP (port depends upon your mail configuration within the product) to configured mail server**
- IIS/ASP.Net perform GPO rollback (requires auditing agent)
    - **TCP 445 to closest AD domain controller**
    - **TCP 135 (RPC Portmapper) to closest AD domain controller**
    - **TCP 49152-65535. (RPC dynamic ports) to closest AD domain controller**
    - **TCP 389 (or 636 if LDAPS is enforced) from web server to closest AD domain controller**

GPAA ASP.Net Web Service Proxy

- IIS authenticates the user to Active Directory
    - **TCP 389 (or 636 if LDAPS is enforced) from web server to closest AD domain controller**
    - **TCP or UDP (usually TCP) 88 (Kerberos) from web server to closest AD domain controller**
- IIS/ASP.Net makes GPMC API Calls
    - **TCP 445 to closest AD domain controller**
    - **TCP 135 (RPC Portmapper) to closest AD domain controller**
    - **TCP 49152-65535. (RPC dynamic ports) to closest AD domain controller**
- IIS/ASP.Net application communicates to GPAA SQL Server
    - **TCP 1433 or dynamic high-numbered port (See your SQL Server Services Configuration to verify which port SQL Server is listening on)**

GPAA Attestation Service

The GPAA attestation service performs a number of tasks, including sending attestation emails, reconciling AD GPOs and Groups within the GPAA database and performing periodic reconciliation tasks against the GPAA database. The following ports and protocols are used during these communications:

- GPAA Attestation Service communicates with AD to get current list of GPOs and/or Groups
  - **TCP 445 to closest AD domain controller**
  - **TCP 135 (RPC Portmapper) to closest AD domain controller**
  - **TCP 49152-65535. (RPC dynamic ports) to closest AD domain controller**
  - **TCP 389 (or 636 if LDAPS is enforced) from web server to closest AD domain controller**
- GPAA Attestation Service communicates with GPAA SQL Server database to add/remove GPOs and groups and update attestation information
  - **TCP 1433 or dynamic high-numbered port (See your SQL Server Services Configuration to verify which port SQL Server is listening on)**
- GPAA Attestation Service sends attestation emails
  - **TCP SMTP (port depends upon your mail configuration within the product) to configured mail server**

GPAA Auditing Service

The GPAA auditing service provides real-time change auditing and alerting of Group Policy changes. Because the auditing service resides on each domain controller, most of its communications are local to that box. That said, the main two “off-box” communications in which the GPAA Auditing Service participates are: communicating with the GPAA SQL Server database, and communicating with the configured SMTP service to send auditing email alerts, as follows:

- GPAA Auditing Service communicates with GPAA SQL Server Database
  - **TCP 1433 or dynamic high-numbered port (See your SQL Server Services Configuration to verify which port SQL Server is listening on)**
- GPAA Auditing Service communicates with configured Mail server to send auditing alert emails
  - **TCP SMTP (port depends upon your mail configuration within the product) to configured mail server**

GPAA Untrusted Proxy Service

- GPAA Untrusted Proxy Service communicates with GPAA Web Service Proxy Application
  - **TCP 443 or SSL/TLS listening port**
- GPAA Untrusted Proxy Service communicates with AD in the Untrusted Domain to get a current list of GPOs and/or Groups
  - **TCP 445 to closest AD domain controller**
  - **TCP 135 (RPC Portmapper) to closest AD domain controller**
  - **TCP 49152-65535. (RPC dynamic ports) to closest AD domain controller**
  - **TCP 389 (or 636 if LDAPS is enforced) from web server to closest AD domain controller**

GPAA Server Requirements and Software Prerequisites

This section provides details on the software and components required on servers that run GPAA.

Supported Windows OS Version

GPAA components have been tested and certified on all versions of Windows Server from **2012-R2 to 2019 (note that the GPAA Auditing Service still supports running on Windows Server 2008-R2 DCs, but no other GPAA components do)**. If GPAA components are installed on separate servers, they can be of different OS versions as long as the prerequisites are installed for each component.

Component Requirements

The following lists the software components required for each GPAA component:

- **GPAA Database**
    - Microsoft SQL Server 2014 or newer (note that we only recommend running SQL Server Express for **test** environments)
- **GPAA Manager Web Application (see the following screenshots for examples of the features to install on a Windows Server 2012-R2 system)**
    - .Net Framework 4.52 or greater (full) and ASP.Net 4.0+
    - IIS and ASP.Net Features installed with Windows Authentication enabled for the GPAA Web Application and Anonymous Authentication disabled
    - Group Policy Management Console (GPMC)
    - Licensing--The GPAA Web Application is where GPAA licensing is validated
- **GPAA ASP.Net Web Service Proxy Application**
    - Net Framework 4.5.2 or greater and ASP.Net 4.0+
    - IIS and ASP.Net Features with only Anonymous Authentication enabled for the GPAA Web Service Proxy Application
    - SSL/TLS certificate required for Web Service Proxy Application
    - Group Policy Management Console (GPMC)
- **GPAA Attestation Service**
    - .Net Framework 4.52 or greater (full)
    - Group Policy Management Console (GPMC)
- **GPAA Auditing Service**
    - .Net Framework 4.52 or greater (full)
    - Group Policy Management Console (GPMC)
- **GPAA Untrusted Proxy Service**
    - .Net Framework 4.52 or greater
    - Group Policy Management Console (GPMC)

Windows Feature Installation Scripts

The GPAA installation zip file contains two signed PowerShell scripts that will automate the installation of the required Windows Features for the GPAA Web Application server. These scripts are called:

2012-R2AddGPAAWebFeatures.ps1

2016-9AddGPAAWebFeatures.ps1

Which can be run on Windows Server 2012-R2 or Server 2016/9, respectively. The scripts call *Add-WindowsFeature* on each required feature to ensure that they are installed on the GPAA Web Application server. Note that these scripts **only** apply to the GPAA Web Application server role.

GPAA Security & User Accounts

GPAA requires Active Directory domain-based service accounts for several of its functions. In the simplest configuration, you can use the same service account for all functions. GPAA is designed to work in least privilege environments within the limits of the host Operating System. Most service accounts won't need blanket administrative access to perform their functions. Review Appendix A to see instructions on how to run the GPAA Auditing Service as LocalSystem. The following permissions are needed within each component of GPAA:

- Both the **GPAA Web Application and the Web Service Proxy** should be installed as applications into an IIS Application Pool. If both applications reside on the same web server, then the GPAA Installer will install them into a single App Pool, by default. The App Pool should run using the identity of an AD user with the following requirements:
    - ✓ The App Pool identity will need to have **local Administrators group** membership on the web server(s) **only during the evaluation period**. This has to do with the need for the App Pool identity to be able to right to the HKEY_CURRENT_USER registry hive to record evaluation license information. This is not required for a customer license.
    - ✓ Permissions to read GPOs in all domains being managed.
    - ✓ If GPO rollback feature is used, the App Pool identity needs to be able to write to any GPOs that are rolled back.
    - ✓ Permission to read and write to the **GPAA database** (db_datareader and db_datawriter permissions are sufficient). This permission is set up for the specified service account when the GPAA database is installed.
- The **GPAA Attestation Service Account** is an AD service account that is used to run this service. The account requires the following privileges:
    - ✓ Permission to log on as a service on the server where its running (automatically granted by GPAA Attestation Service installer).
    - ✓ Administrators group permission on the server where it runs only the **first time** it is started. This permission allows the service to create a customer Windows event log category. Once created, the Attestation Service no longer needs to be administrator on the server where it's installed.
    - ✓ Permission to read and write (db_reader and db_writer) to the GPAA database.
    - ✓ Permission to read GPOs and in domains under management (it's the GP Attestation Service's job to keep GPOs stored in the GPAA database in sync with live GPOs in the domains under management.
- **GPAA Auditing Service Account**
    - ✓ Permission to logon as a service on domain controllers. Usually granted via the "Default Domain Controllers Policy" GPO.

  - ✓ For Server 2012 and above, the GPAA Auditing Service needs to at least be a member of the **domain local Administrators group** (see Appendix A if you would rather run the Auditing Service as LocalSystem on the DC) to function. This is a requirement due to the way these newer OS versions handle certain processes used by the service and its use of GPMC APIs. On Server 2008-R2, the service account needs to have read access to the AD security event log on each DC. Details on how to grant this permission more granularly to a given account can be found here: https://blogs.technet.microsoft.com/janelewis/2010/04/30/giving-non-administrators-permission-to-read-event-logs-windows-2003-and-windows-2008/ .
  - ✓ Permission to read and write to the GPAA database (db_datareader and db_datawriter permissions are sufficient).
  - ✓ Permissions to write to the %ProgramData% folder on each Domain Controller.
  - ✓ Permission to read GPOs within the domain where it's installed.
- **GPAA Untrusted Proxy Service**
  - ✓ This service runs as localSystem and therefore no service account is required.
  - ✓ The Untrusted Proxy Service communicates with the Web Service Proxy Application using SSL/TLS. In addition, both the Untrusted Proxy Service and Web Service Proxy Application must be configured with a matching pre-shared key, which encrypts the payload that passes between client and web service.

Depending upon the environment and the level of security lockdown in place between servers, Group Policy and Active Directory, you may need to adjust the rights of the service account. The key here is that the service account does not REQUIRE Domain Admin rights to accomplish its job. If you run into issues implementing this, contact support@sdmsoftware.com for help troubleshooting permission challenges.

Requirements for Active Directory Auditing

In order to leverage the capabilities of the Group Policy change auditing, the GPAA Auditing Service, running on your Active Directory Domain Controllers, uses Windows native security events to detect when changes happen for Group Policy related activities. GPAA can detect the following types of Group Policy changes:

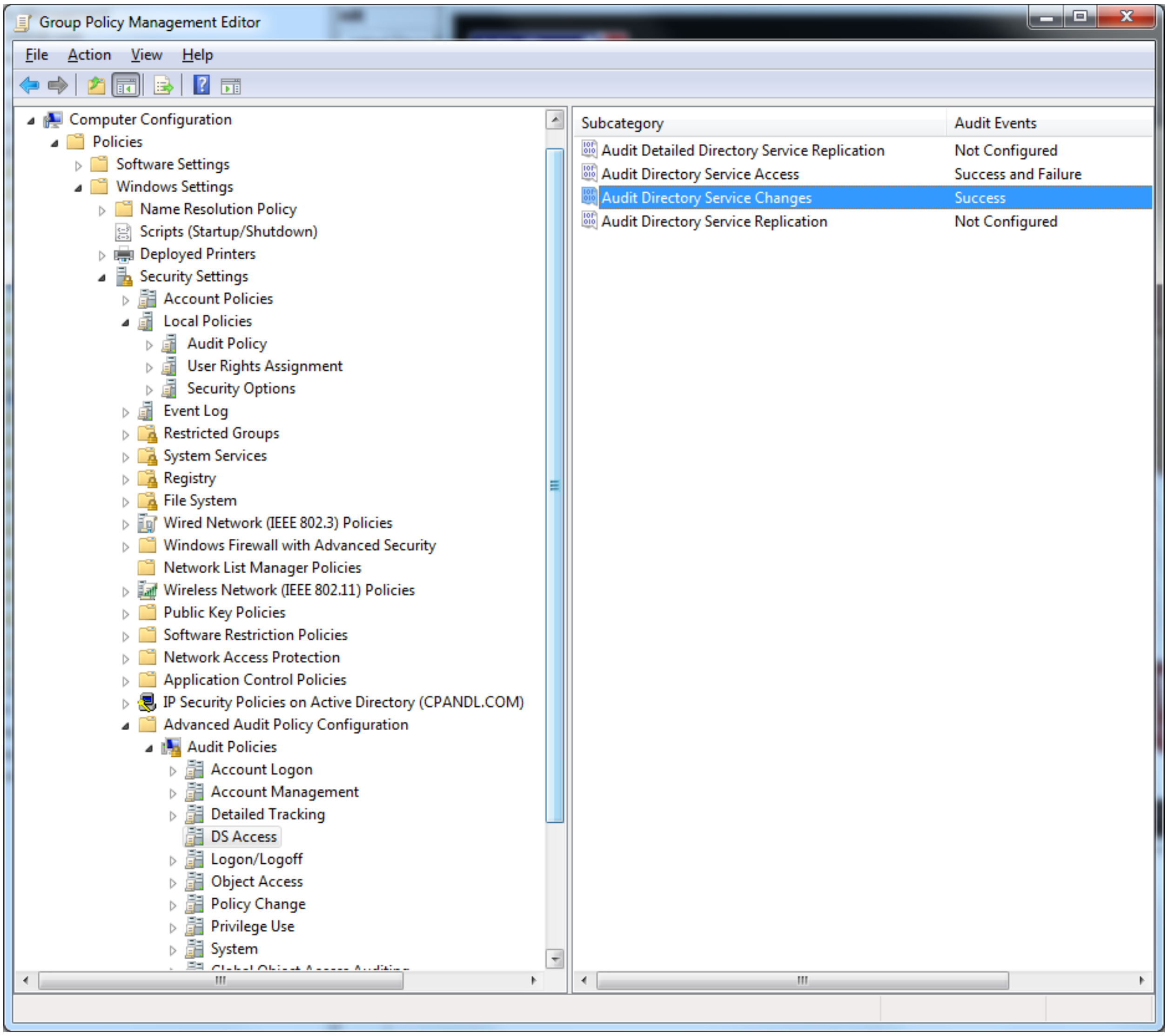
- Creation, Deletion and Modification of GPOs, including GPO settings
- Creation, Deletion and Modification of WMI Filters
- Linking and unlinking GPOs to Scopes of Management (SOMs), such as sites, domains or OUs
- Linking and unlinking WMI filters to GPOs
- Enforcing, un-enforcing or disabling a GPO link
- Changing GPO permissions
- Changing GPO status (e.g. user disabled, computer disabled, etc.)

In order to facilitate capturing all of these changes, we require a few steps be taken to enable a specific auditing of Active Directory changes. Namely, we use the **Directory Services Changes** sub-category of Advanced Audit Policy Configuration to capture changes. This sub-category generates events with IDs of :

- 5136
- 5137
- 5141

These are the 3 ids that GPAA is interested in. If you aren't already capturing these events, you must enable this auditing.   On Server 2008-R2 and above, domain controllers, you can take the following steps to enable this auditing:

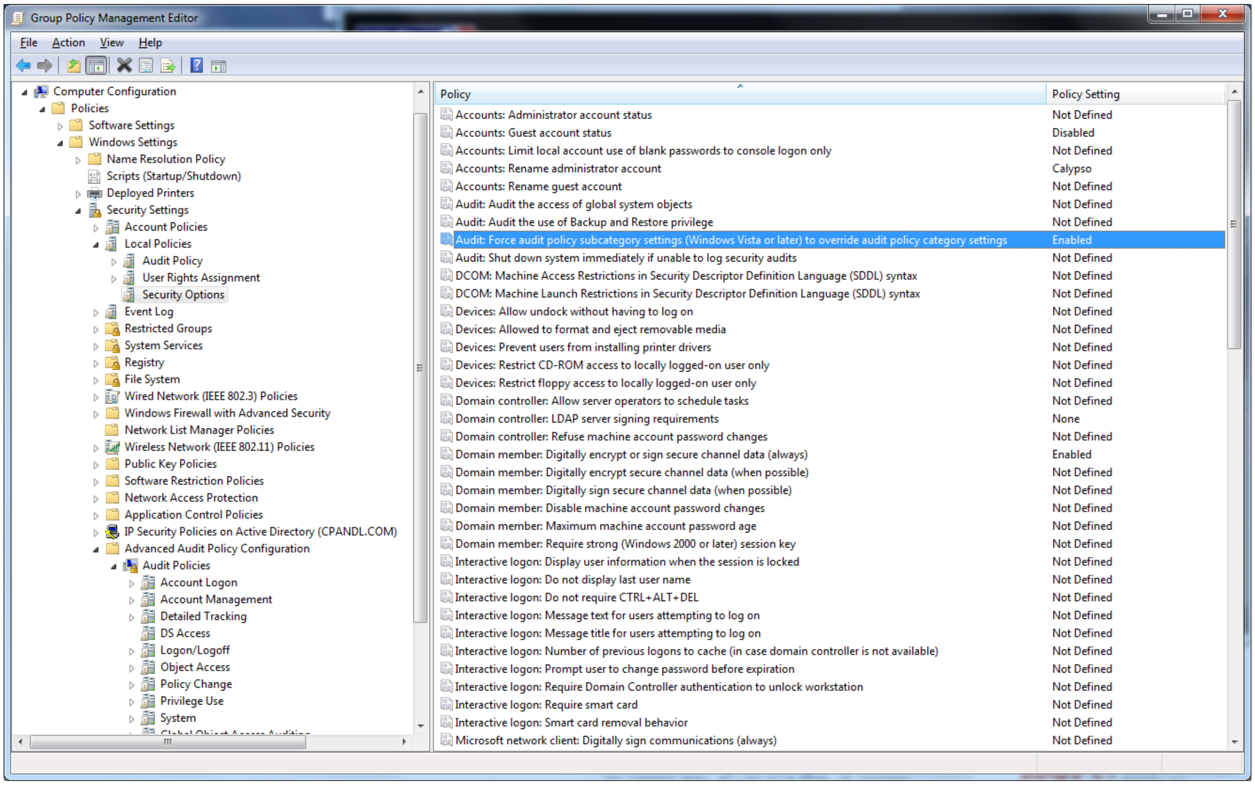
1. First, if you are not already auditing for **Directory Services Changes** events, you'll need to enable the auditing using Group Policy. Typically this is done within the **Default Domain Controllers Policy** GPO, or any GPO that you have linked to the Domain Controllers OU. From within that GPO, You'll set the following policy under **Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Services Changes**:



Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Success and Failure
Audit Directory Service Changes	Success
Audit Directory Service Replication	Not Configured

Figure 2: Enabling Directory Services Changes Auditing in GP

2. Next, assuming you are still using the old audit categories for AD auditing and no longer want to log those events, you'll want to tell domain controllers to disable legacy audit categories auditing, enabling the policy at **Computer Configuration\Policies\Windows Settings\Security Settings\Security Options\ Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings.**



Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Not Defined
Accounts: Rename administrator account	Calypso
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Audit: Shut down system immediately if unable to log security audits	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user only	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	None
Domain controller: Refuse machine account password changes	Not Defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Not Defined
Domain member: Digitally sign secure channel data (when possible)	Not Defined
Domain member: Disable machine account password changes	Not Defined
Domain member: Maximum machine account password age	Not Defined
Domain member: Require strong (Windows 2000 or later) session key	Not Defined
Interactive logon: Display user information when the session is locked	Not Defined
Interactive logon: Do not display last user name	Not Defined
Interactive logon: Do not require CTRL+ALT+DEL	Not Defined
Interactive logon: Message text for users attempting to log on	Not Defined
Interactive logon: Message title for users attempting to log on	Not Defined
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	Not Defined
Interactive logon: Prompt user to change password before expiration	Not Defined
Interactive logon: Require Domain Controller authentication to unlock workstation	Not Defined
Interactive logon: Require smart card	Not Defined
Interactive logon: Smart card removal behavior	Not Defined
Microsoft network client: Digitally sign communications (always)	Not Defined

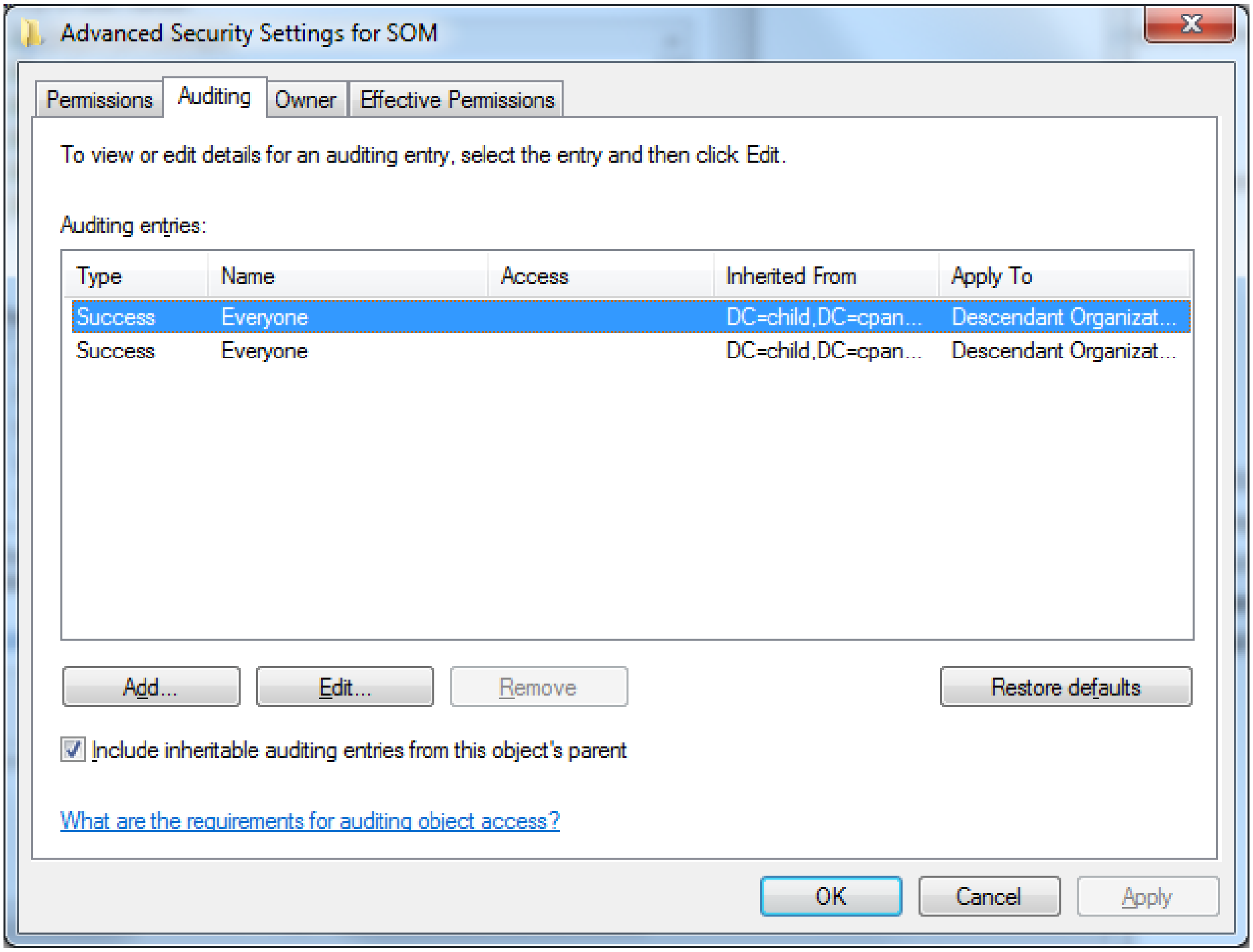
Figure 3: Configuring Security Option to disable legacy auditing

3. Now that auditing is configured, the final step is enabling the correct SACLs on AD to ensure that GP-related events log security event logs when changes occur. GPAA requires the following auditing events to capture all Group Policy management-related changes:

Table 1: Auditing required by GPAA to capture all GP events

Change Tracked	SACL Required	Present by Default in AD?
Create a GPO	**Create GroupPolicyContainer Objects** for group Everyone on CN=Policies, CN=System	Yes
Delete a GPO	**Delete** for group Everyone on CN=Policies, CN=System and all descendent objects	No
Modify GPO Settings, GPO Status and WMI filter linked/un-linked to GPO	**Write All Properties** for group Everyone on CN=Policies, CN=System and all descendent objects	Yes
Modify GPO Permissions	**Modify Permissions** for group Everyone on CN=Policies, CN=System and all descendent objects	Yes
Link and Unlink GPOs and GPO Link Options (e.g. Enforced, Disabled)	**Write GPLink** for group Everyone on domain NC Head, all descendent Organizational Unit objects and all Site objects	Yes
Set or Unset Block Inheritance	**Write GPOptions** for group Everyone on all descendent Organizational Unit objects and all Site objects	Yes
Create WMI Filter	**Create ms_WMISOM objects** for group Everyone on CN=SOM, CN=WMIPolicy, CN=System	No
Delete WMI Filter	**Delete ms_WMISOM objects** for group Everyone on CN=SOM, CN=WMIPolicy, CN=System	No
Change WMI Filter	**Write All Properties** for group Everyone on CN=SOM, CN=WMIPolicy, CN=System	No

Note that only 4 SACL changes (highlighted in blue) are required in default AD installations to implement all change auditing within GPAA. Auditing is typically configured within the AD Users and Computers (ADUC) (or AD Sites and Services) by right-clicking on the object in question, choosing Properties, the Security tab and the **Advanced** button. From there, select the Auditing to set SACLs on the object, as shown below:



To view or edit details for an auditing entry, select the entry and then click Edit.

Auditing entries:

Type	Name	Access	Inherited From	Apply To
Success	Everyone		DC=child,DC=cpan...	Descendant Organizat...
Success	Everyone		DC=child,DC=cpan...	Descendant Organizat...

☑ Include inheritable auditing entries from this object's parent

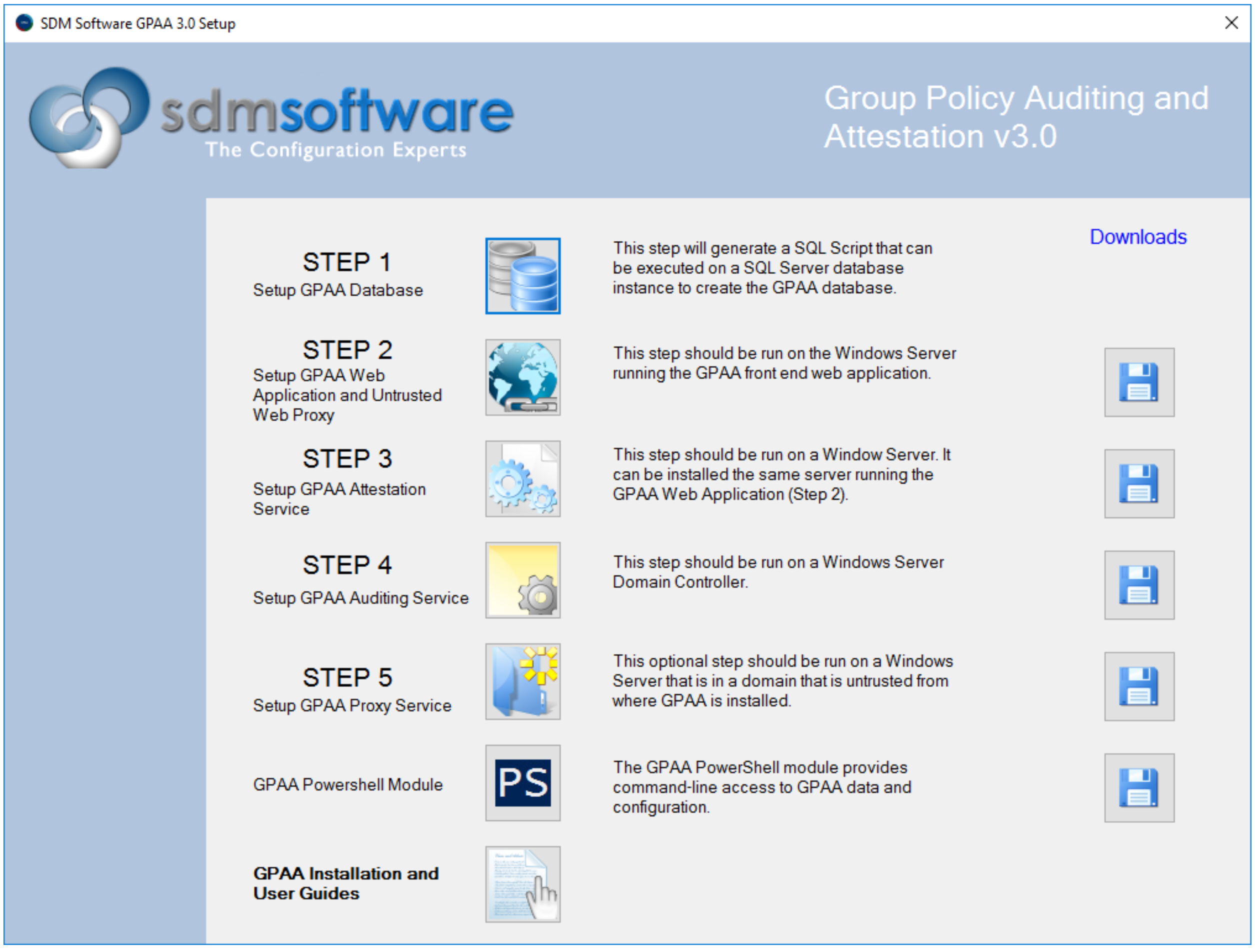
What are the requirements for auditing object access?

Figure 4 Setting native auditing from ADUC

Once auditing is configured within AD, the GPAA auditing service will detect all changes related to Group Policy management.

Step-by-Step Installation & Upgrade

The setup comes in the form of a self-extracting setup called **GPAA3.0Setup.exe**, found in the downloaded GPAA 3.0 installation Zip file. All files related to GPAA are extracted to the machine where the setup is running. The following menu appears:



Group Policy Auditing and Attestation v3.0

STEP 1
Setup GPAA Database

This step will generate a SQL Script that can be executed on a SQL Server database instance to create the GPAA database.

STEP 2
Setup GPAA Web Application and Untrusted Web Proxy

This step should be run on the Windows Server running the GPAA front end web application.

STEP 3
Setup GPAA Attestation Service

This step should be run on a Window Server. It can be installed the same server running the GPAA Web Application (Step 2).

STEP 4
Setup GPAA Auditing Service

This step should be run on a Windows Server Domain Controller.

STEP 5
Setup GPAA Proxy Service

This optional step should be run on a Windows Server that is in a domain that is untrusted from where GPAA is installed.

GPAA Powershell Module

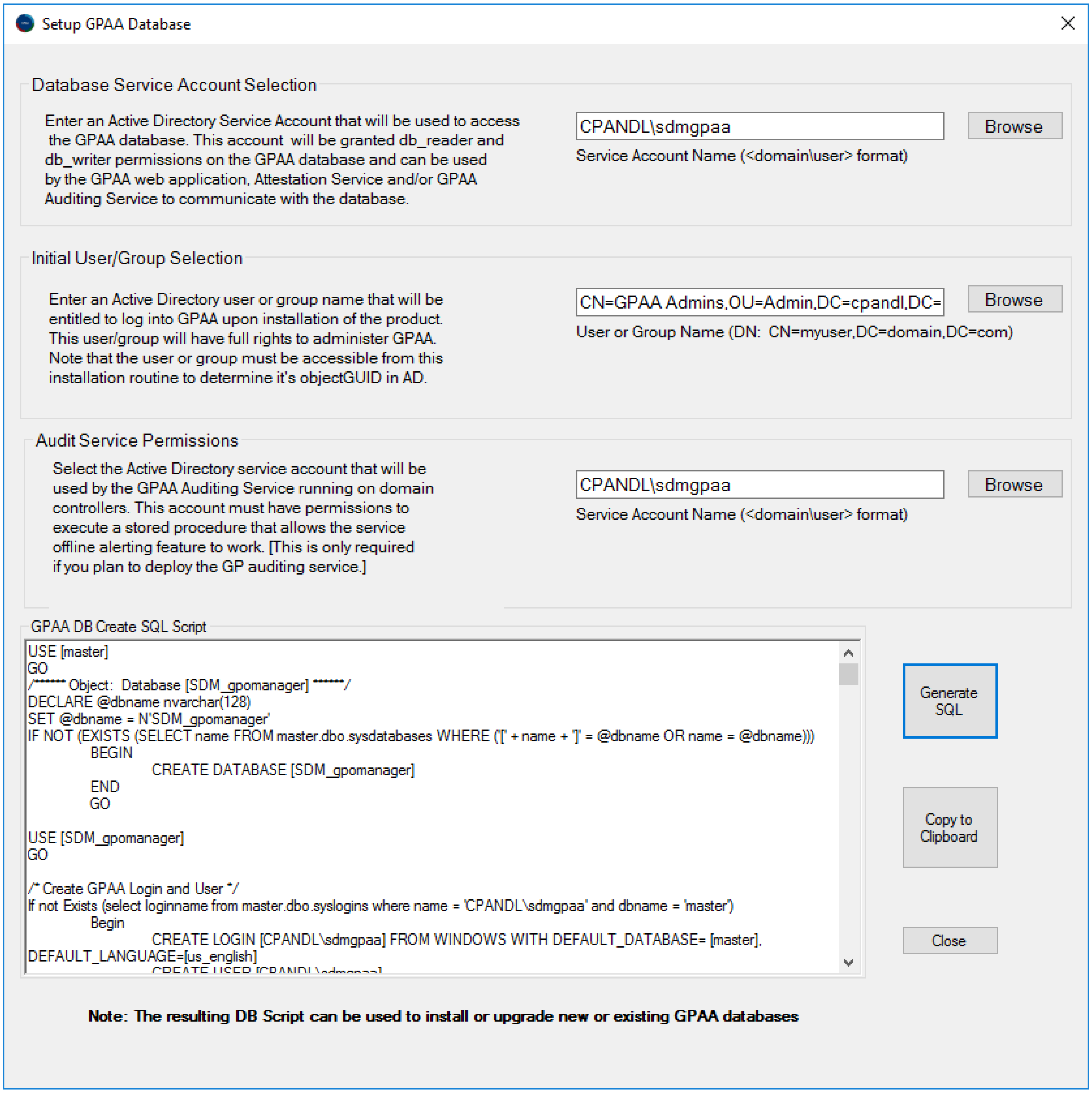
The GPAA PowerShell module provides command-line access to GPAA data and configuration.

GPAA Installation and User Guides

This setup should be run from the server or servers where GPAA roles are being installed/upgraded and/or the individual DCs where you are installing the GP Auditing Service. Note that the Self-Extractor will create a temporary folder under **%temp%** and will place the GPAA setup source files, including MSI files, into that folder. You can separately download each installer using the disk (💾) icon to save each MSI or web content file to your local file system.

To begin with, run the setup from the server you plan to use as the GPAA web application server.

1. Set up the GPAA Database: On the GPAA Server, run the "**Setup GPAA Database**" option first. The output of this option is a SQL Script that lets you or your Database Administrator create or update the GPAA database interactively on your database server. This option presents the following dialog:


Setup GPAA Database
Database Service Account Selection
Browse
Initial User/Group Selection
Browse
Audit Service Permissions
Browse
GPAA DB Create SQL Script
Generate SQL
Copy to Clipboard
Close

Enter an Active Directory Service Account that will be used to access the GPAA database. This account will be granted db_reader and db_writer permissions on the GPAA database and can be used by the GPAA web application, Attestation Service and/or GPAA Auditing Service to communicate with the database.

CPANDL\sdmgpaa

Service Account Name (<domain\user> format)

Enter an Active Directory user or group name that will be entitled to log into GPAA upon installation of the product. This user/group will have full rights to administer GPAA. Note that the user or group must be accessible from this installation routine to determine it's objectGUID in AD.

CN=GPAA Admins,OU=Admin,DC=cpandl,DC=

User or Group Name (DN: CN=myuser,DC=domain,DC=com)

Select the Active Directory service account that will be used by the GPAA Auditing Service running on domain controllers. This account must have permissions to execute a stored procedure that allows the service offline alerting feature to work. [This is only required if you plan to deploy the GP auditing service.]

CPANDL\sdmgpaa

Service Account Name (<domain\user> format)

```
USE [master]
GO
/****** Object:  Database [SDM_gpomanager] ******/
DECLARE @dbname nvarchar(128)
SET @dbname = N'SDM_gpomanager'
IF NOT (EXISTS (SELECT name FROM master.dbo.sysdatabases WHERE ('[' + name + ']' = @dbname OR name = @dbname)))
		BEGIN
				CREATE DATABASE [SDM_gpomanager]
		END
		GO

USE [SDM_gpomanager]
GO

/* Create GPAA Login and User */
If not Exists (select loginname from master.dbo.syslogins where name = 'CPANDL\sdmgpaa' and dbname = 'master')
		Begin
				CREATE LOGIN [CPANDL\sdmgpaa] FROM WINDOWS WITH DEFAULT_DATABASE= [master],
DEFAULT_LANGUAGE=[us_english]
				CREATE USER [CPANDL\sdmgpaa]
```

Note: The resulting DB Script can be used to install or upgrade new or existing GPAA databases

This dialog prompts for three pieces of information, in order to create the SQL Script that you will use to create your GPAA database:

a. **Database Service Account Selection:** This will be the service account that can read and write from/to the GPAA database from the GPAA auditing, attestation and web application services. Note that you can have multiple service accounts being used for GPAA database access but this script only creates one of those and grants it db_reader and db_writer. You will have to add the others manually, via the script or after the GPAA database is created.

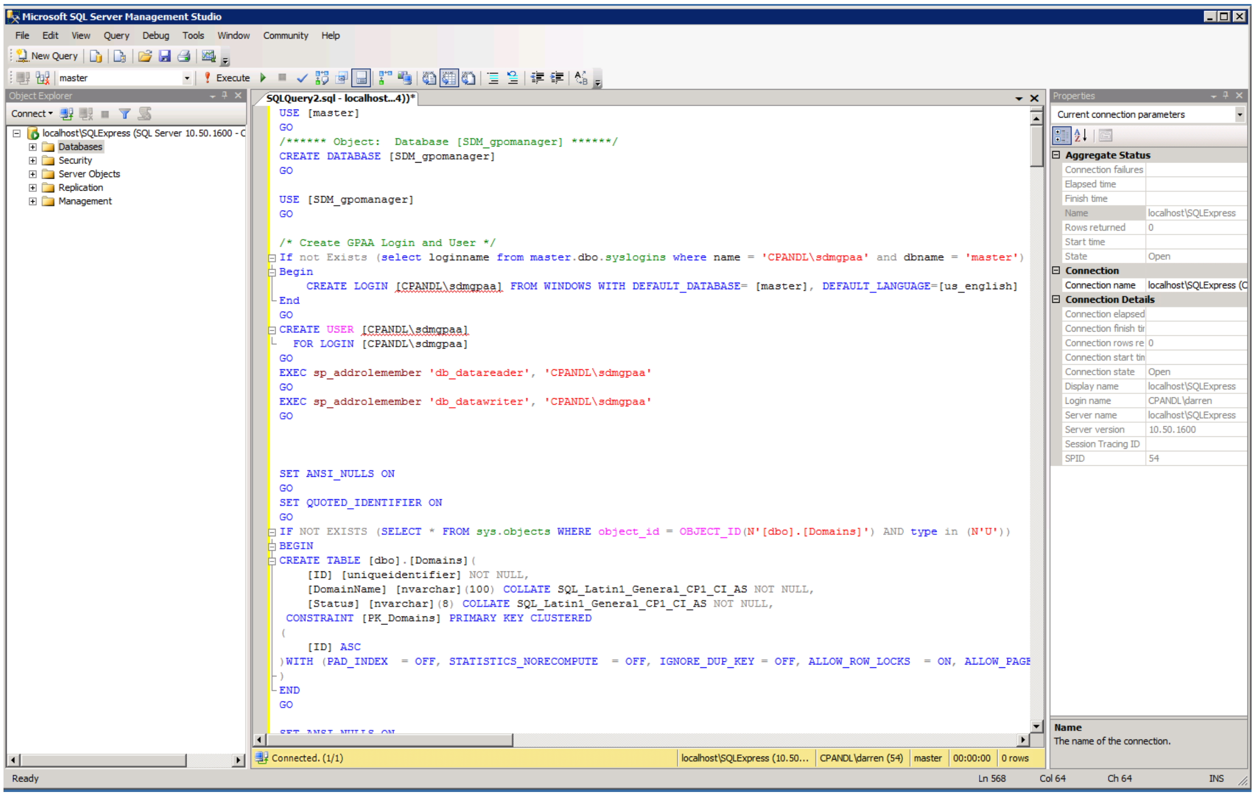
b. **Initial User/Group Selection**: This option tells GPAA what user or group will have full access to GPAA once the installation is done. By default, any member of the Domain

Admins group will have this access but you can optionally specify a user or group here that will be granted that access instead.

c. **Audit Service Permissions**: This option is required to specify what service account will be used by your GPAA auditing service agents. This is required to grant that service account the rights to execute a stored procedure on the database required when using the GPAA auditing service offline notification feature.

Once the script is generated, use the “Copy to Clipboard” button to save the script. The easiest way to create the database from the script is to open SQL Server Management Studio, select the database instance on which you wish to create the GPAA Database, and select the “New Query” button. Then paste the GPAA SQL script into the new query, as shown below, and run Execute.

You should not see any errors when the script runs. If you do, contact SDM Software support with the error information.


Microsoft SQL Server Management Studio
File Edit View Query Debug Tools Window Community Help
New Query
master
Execute
Object Explorer
Connect
localhost\SQLExpress (SQL Server 10.50.1600 - C
Databases
Security
Server Objects
Replication
Management
SQLQuery2.sql - localhost...4))*
Properties
Current connection parameters
Aggregate Status
Connection
Connection Details
Name
The name of the connection.
Ready
Ln 568
Col 64
Ch 64
INS

```
USE [master]
GO
/****** Object:  Database [SDM_gpomanager] ******/
CREATE DATABASE [SDM_gpomanager]
GO

USE [SDM_gpomanager]
GO

/* Create GPAA Login and User */
If not Exists (select loginname from master.dbo.syslogins where name = 'CPANDL\sdmgpaa' and dbname = 'master')
Begin
    CREATE LOGIN [CPANDL\sdmgpaa] FROM WINDOWS WITH DEFAULT_DATABASE= [master], DEFAULT_LANGUAGE=[us_english]
End
GO
CREATE USER [CPANDL\sdmgpaa]
  FOR LOGIN [CPANDL\sdmgpaa]
GO
EXEC sp_addrolemember 'db_datareader', 'CPANDL\sdmgpaa'
GO
EXEC sp_addrolemember 'db_datawriter', 'CPANDL\sdmgpaa'
GO



SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
IF NOT EXISTS (SELECT * FROM sys.objects WHERE object_id = OBJECT_ID(N'[dbo].[Domains]') AND type in (N'U'))
BEGIN
CREATE TABLE [dbo].[Domains](
    [ID] [uniqueidentifier] NOT NULL,
    [DomainName] [nvarchar](100) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL,
    [Status] [nvarchar](8) COLLATE SQL_Latin1_General_CP1_CI_AS NOT NULL,
 CONSTRAINT [PK_Domains] PRIMARY KEY CLUSTERED
(
    [ID] ASC
)WITH (PAD_INDEX  = OFF, STATISTICS_NORECOMPUTE  = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS  = ON, ALLOW_PAGE
)
END
GO
```

Connected. (1/1) | localhost\SQLExpress (10.50... | CPANDL\darren (54) | master | 00:00:00 | 0 rows

Connection failures	
Elapsed time	
Finish time	
Name	localhost\SQLExpress
Rows returned	0
Start time	
State	Open
Connection name	localhost\SQLExpress (C
Connection elapsed	
Connection finish ti	
Connection rows re	0
Connection start tin	
Connection state	Open
Display name	localhost\SQLExpress
Login name	CPANDL\darren
Server name	localhost\SQLExpress
Server version	10.50.1600
Session Tracing ID	
SPID	54

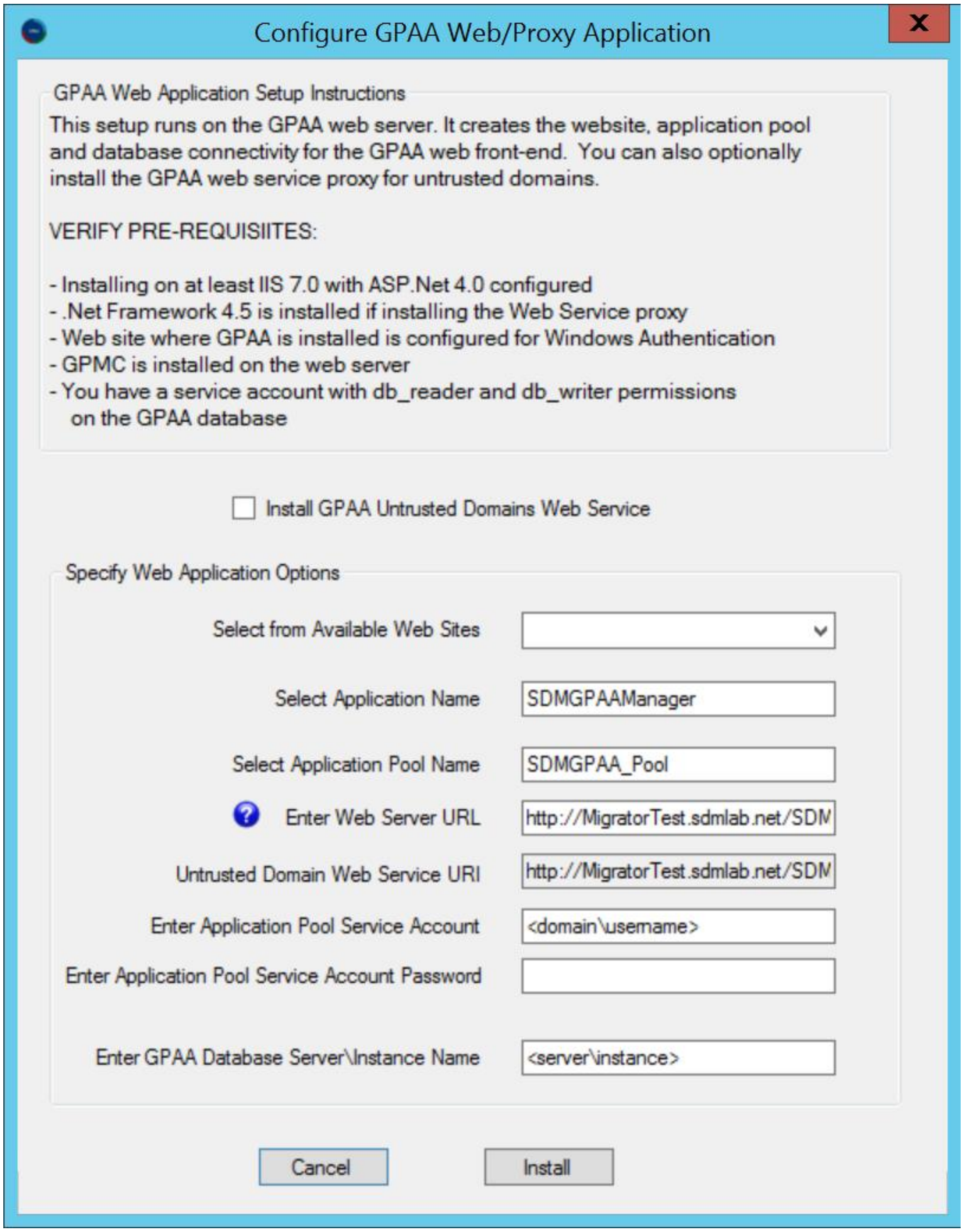
[UPGRADE NOTE]

If you are upgrading your existing GPAA 2.5 instance, then you will need to run the SQL script provided in the steps above against your existing SDM_GPOManager database to upgrade it to the 3.0 schema. Contact SDM Software Support (support@sdmsoftware.com) if you have any questions on errors that you see during this phase.

Once the database is created or updated, you are ready to move on to creation/update of the GPAA web application.

2. Set up the GPAA Web/Proxy Applications: This step performs the setup of the GPAA Web Application and optionally when you check the box to **"Install GPAA Untrusted Domains Web Service,"** the GPAA Web Service Proxy Application. The GPAA Web Proxy Application is used when you plan to perform GPO attestations (but not auditing) against untrusted domains. The setup for these ASP.Net applications performs the following actions:
    a. Creates the application(s) under the website you choose (usually called SDMGPAAManager & SDMGPAAProxy).
    b. Creates the Application Pool (running ASP.Net 4.0) and changes the identity of the Application pool to the AD service account you've created for GPAA in the previous step.
    c. Sets **Windows authentication to enabled** and anonymous authentication to disabled for the GPAA Web Application and sets **authentication to Anonymous** for the GPAA Web Service Proxy Application. *(**Note** that you may need to manually set this if the parent web site enforces other authentication defaults.)*
    d. Configures the database connection string for the web application (and web proxy).
    e. Copies the web application files under the application directories (usually under %systemdrive%\inetpub\wwwroot). If the files exist from a previous version, those files will be deleted prior to copying the new version of the web applications.
    f. Installs the evaluation license for the product to the registry on the web server (the GPAA license material is stored in HKLM\Software\GP\GPAA on the GPAA web server).
    g. Prompts you for the web server's URL. In situations where the web server application is load balanced, the application has to know the "virtual" URL that will always be used in attestation emails. When you enter the full URL in this step (e.g. http(s)://mywebserver.mydomain.com\sdmgpaamaanger) after the web application is created, a **window will pop-up with a small bit of SQL Script that must be run against the GPAA database**. This script sets the "Website" row value in the Settings table. You can copy and paste this and run it against the GPAA database to set this value.
    h. Enable SSL for the SDMGPAAManager and optionally, the SDMGPAAProxy applications after installation. These applications are not bound to SSL by default. You'll need to provide and select your own SSL keys and set the binding for these two applications within the IIS Administrator application. You can view this Microsoft video for instructions on how to configure IIS applications for SSL.

The dialog for this web application installation step is shown here:



Configure GPAA Web/Proxy Application

GPAA Web Application Setup Instructions

This setup runs on the GPAA web server. It creates the website, application pool and database connectivity for the GPAA web front-end. You can also optionally install the GPAA web service proxy for untrusted domains.

VERIFY PRE-REQUISIITES:

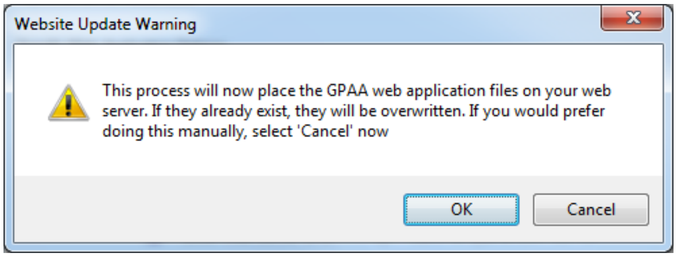
- Installing on at least IIS 7.0 with ASP.Net 4.0 configured
- .Net Framework 4.5 is installed if installing the Web Service proxy
- Web site where GPAA is installed is configured for Windows Authentication
- GPMC is installed on the web server
- You have a service account with db_reader and db_writer permissions on the GPAA database

☐ Install GPAA Untrusted Domains Web Service

Specify Web Application Options

Select from Available Web Sites	
Select Application Name	SDMGPAAManager
Select Application Pool Name	SDMGPAA_Pool
Enter Web Server URL	http://MigratorTest.sdmlab.net/SDM
Untrusted Domain Web Service URI	http://MigratorTest.sdmlab.net/SDM
Enter Application Pool Service Account	<domain\username>
Enter Application Pool Service Account Password	
Enter GPAA Database Server\Instance Name	<server\instance>

When you press the install button, you are given the following prompt:



Website Update Warning

This process will now place the GPAA web application files on your web server. If they already exist, they will be overwritten. If you would prefer doing this manually, select 'Cancel' now

If you select OK here, the assumption is that you are running this setup on the web server itself and the web application will be created with the options specified. If not, you can select Cancel here. The setup stops and you're prompted to provide a folder location to save the web application and web service proxy application files (webcontent.zip). If you should this option case, you would manually create the web application(s) under the website, place it in the Application Pool you created and then extract the zip file's contents (folders and files) to the web application's directory (e.g. c:\inetpub\wwwroot\sdmgpaamanager and c:\inetpub\wwwroot\sdmgpaaproxy, respectively). The web.config file under each directory contains the database connection string, amongst other options that can be modified manually, if needed. Within the GPAA Web Application folder the web.config contains the following connection string that can be modified:

```
<connectionStrings>
    <add name="SDMGPAAEntities"
connectionString="metadata=res://*/GPAADB.csdl|res://*/GPAADB.ssdl|res://*/GPAADB.
msl;provider=System.Data.SqlClient;provider connection string=&quot;data
source=SERVER\INSTANCE;initial catalog=SDM_GPOManager;integrated
security=True;persist security info=True;multipleactiveresultsets=True;application
name=EntityFramework&quot;"
      providerName="System.Data.EntityClient" />
  </connectionStrings>
```

The highlighted SERVER\INSTANCE text needs to be replaced with database server name, optional port, and instance name where your GPAA database is installed.

For the GPAA Web Service Proxy Application, it has its own web.config that requires modification. The connection string for that application is as follows:

```
<connectionStrings>
    <add name="SDMGPAAManagerDB"
connectionString="metadata=res://*/SDMGPAAManagerV613.csdl|res://*/SDMGPAAManagerV
613.ssdl|res://*/SDMGPAAManagerV613.msl;provider=System.Data.SqlClient;provider
connection string=&quot;data source=SERVER\INSTANCE;initial
catalog=SDM_gpomanager;integrated security=True;persist security
info=True;multipleactiveresultsets=True;application name=EntityFramework&quot;"
      providerName="System.Data.EntityClient" />
</connectionStrings>
```

In addition, the GPAA Web Service Proxy Application also requires that a "pre-shared key" be configured, which will need to match the Untrusted Proxy Service Client described in Step 6 below. The pre-shared key is also found in the web.config file and looks as follows:

```
  <add key="Key" value="$zaq1xsw2cde3vfr4bgt5nhy6mju7,ki8.lo9/;p0" />
```

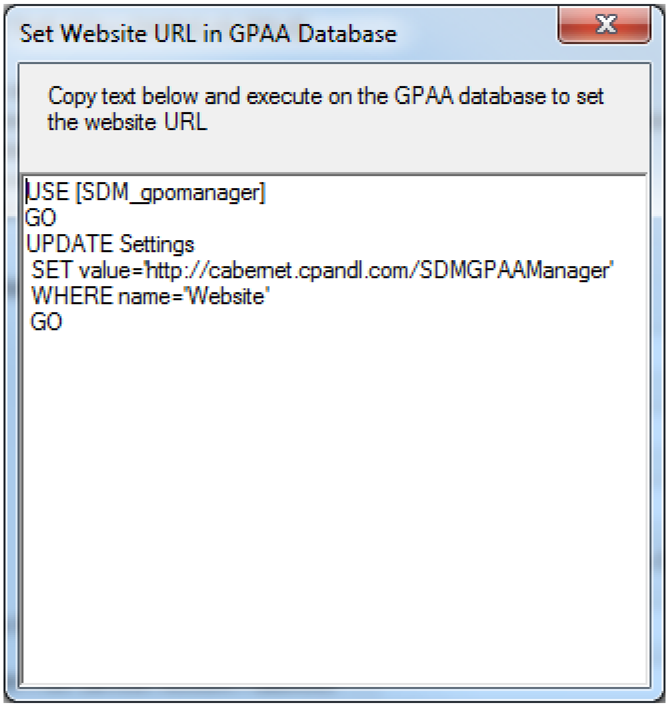
The value can be modified to be unique, though it should match the same number of characters as shown in its default value above. You'll need to use the same value in the Untrusted Proxy

Service client configuration in Step 6 below. **NOTE: You must use HTTPS for the Web Service Proxy Application. It will not function correctly over HTTP.**

[UPGRADE NOTE]

In some cases, the automated upgrade of the web site from GPAA 2.5 will not work, because some folders within the existing file structure may not be deleted correctly. In that case, re-run this step and choose "Cancel" to copy the webcontent.zip to an alternate location—then manually copy the contents of the zip file into the c:\inetpub\wwwroot\sdmgpaamanager (or c:\inetpub\wwwroot\sdmgpaaproxy) folders, ensuring that you replace any existing files or folders that were left from the 2.5 install.

As a final step, after either creating the web application or saving off the web application files, a popup window appears as below:



Copy text below and execute on the GPAA database to set the website URL

```
USE [SDM_gpomanager]
GO
UPDATE Settings
 SET value='http://cabernet.cpandl.com/SDMGPAAManager'
 WHERE name='Website'
 GO
```

This is a piece of SQL script that needs to be run against your GPAA database. It sets the website URL that GPAA uses when it embeds links in attestation emails for GPOs or groups. You would select the text in this dialog, then press Ctrl-C to copy it, and then paste it into a New Query window in SQL Server Management Studio to execute it.

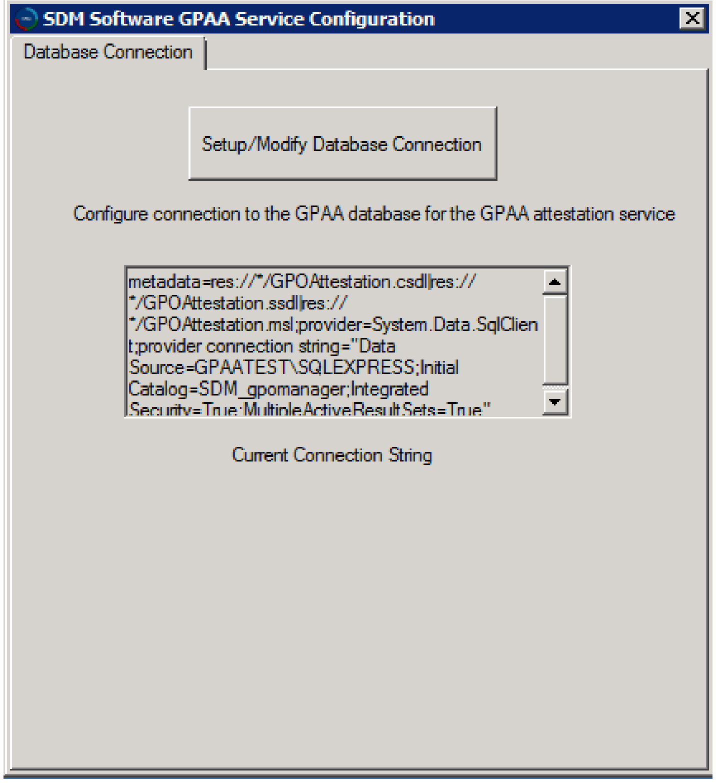
3. The next step that should be performed prior to installing the Attestation and Auditing services, is to configure the GPAA web application for your environment. To open GPAA Manager for configuration, go to the URL you defined for the application in the previous step (e.g. http://<webservername>/sdmgpaamanager, where <webservername> is the server name on which you installed the GPAA Manager application, and "sdmgpaamanager" is the default application name). Log on to the application as the user or member of the group that you

defined as the first time user or group during the database setup routine. See the GPAA User Guide for information on configuring the product, such as adding additional users, a domain and mail server, and activating GPOs. This configuration is needed before starting the attestation service, installed below. In particular, the domain that you want to perform GPO auditing and/or GPO and Group Attestation against, should be added at a minimum.

[UPGRADE NOTE]

This step is not required when upgrading from GPAA 2.5.

4. Set up the GPAA Attestation Service: The next step is to install the **GPAA Attestation** service, typically installed on the same server as the GPAA web application, but not required to be. Ensure that you have created the service account that you plan to use for this service. Run the "**Setup the GPAA Attestation Service"** setup from the GPAA Setup program. You will be prompted to enter the service account name and password and that service account **will be granted "Logon as a Service" user right** on the system where it's installed. Once this completes, the service will be configured to run automatically, but you'll need to manually start the service once after installing it. **Don't start the GPAA Attestation Service before configuring the GPAA Manager application as described in the previous step.** You will also need to run the GPAA Attestation Service Configuration Utility prior to starting the service. This configures the correct database connection needed for the attestation service. The utility is shown here:

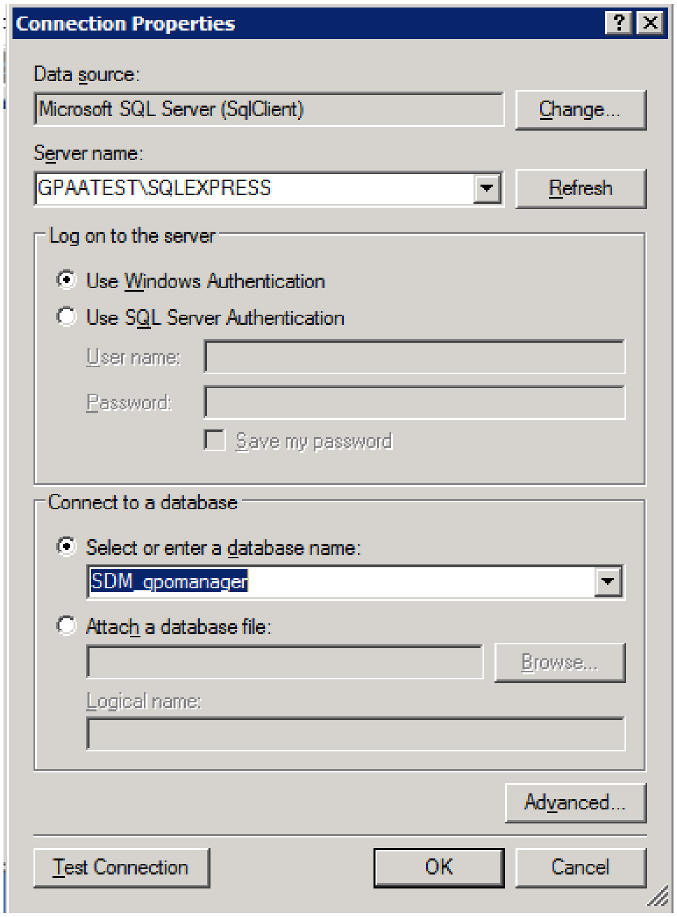

SDM Software GPAA Service Configuration
Database Connection
Setup/Modify Database Connection

Configure connection to the GPAA database for the GPAA attestation service

```
metadata=res://*/GPOAttestation.csdl|res://
*/GPOAttestation.ssdl|res://
*/GPOAttestation.msl;provider=System.Data.SqlClien
t;provider connection string="Data
Source=GPAATEST\SQLEXPRESS;Initial
Catalog=SDM_gpomanager;Integrated
Security=True;MultipleActiveResultSets=True"
```

Current Connection String

Press the "Setup/Modify Database Connection" button, then select "Microsoft SQL Server" as the data source. On the next screen, type in or browse for the server name and database instance name where your GPAA database is installed. Once selected, click the dropdown on the “Select or enter a database name” to browse to the GPAA database (usually SDM_gpomanager), as shown here:



Connection Properties

Data source: Microsoft SQL Server (SqlClient)

Server name: GPAATEST\SQLEXPRESS

Log on to the server

● Use Windows Authentication

○ Use SQL Server Authentication

User name:

Password:

☐ Save my password

Connect to a database

● Select or enter a database name: SDM_gpomanager

○ Attach a database file:

Logical name:

Once selected, press the OK button and the connection will be saved to the attestation service configuration (note that you don’t receive a confirmation when that occurs). You can then successfully start the attestation service, assuming the base GPAA configuration has been completed.

Note: The user account that you run the GPAA Attestation Service Configuration Utility under, must have rights to read the GPAA database in order to be able to browse to it. If you are unable to configure the connection through the UI, you can configure it manually. The connection string for the Attestation Service is in the service install folder—usually “C:\Program Files\SDM Software\SDM GPAA Attestation. The file you need to edit is called *“SDM GPAA Attestation Service.exe.config.”* You will need to open that file for editing using your favorite text editor, but it will need to be opened as an **elevated user (e.g. runas Administrator)**. Once open, look for the connection string, as shown here:

```
<connectionStrings>
    <add name="SDM_gpomanagerEntities"
connectionString="metadata=res://*/GPOAttestationEnitiies.csdl|res://*/GPOAttestat
ionEnitiies.ssdl|res://*/GPOAttestationEnitiies.msl;provider=System.Data.SqlClient
;provider connection string=&quot;data source=SERVER\INSTANCE;initial
catalog=SDM_gpomanager;integrated
security=True;multipleactiveresultsets=True;App=EntityFramework&quot;"
providerName="System.Data.EntityClient" />
  </connectionStrings>
```

Replace the “SERVER\INSTANCE” text under the data source, with the server name and optionally, the instance name where your GPAA database is held. For the default instance, simply enter the server name. For a non-standard port, use this format:

DBServer,49532\SQLEXPRESS

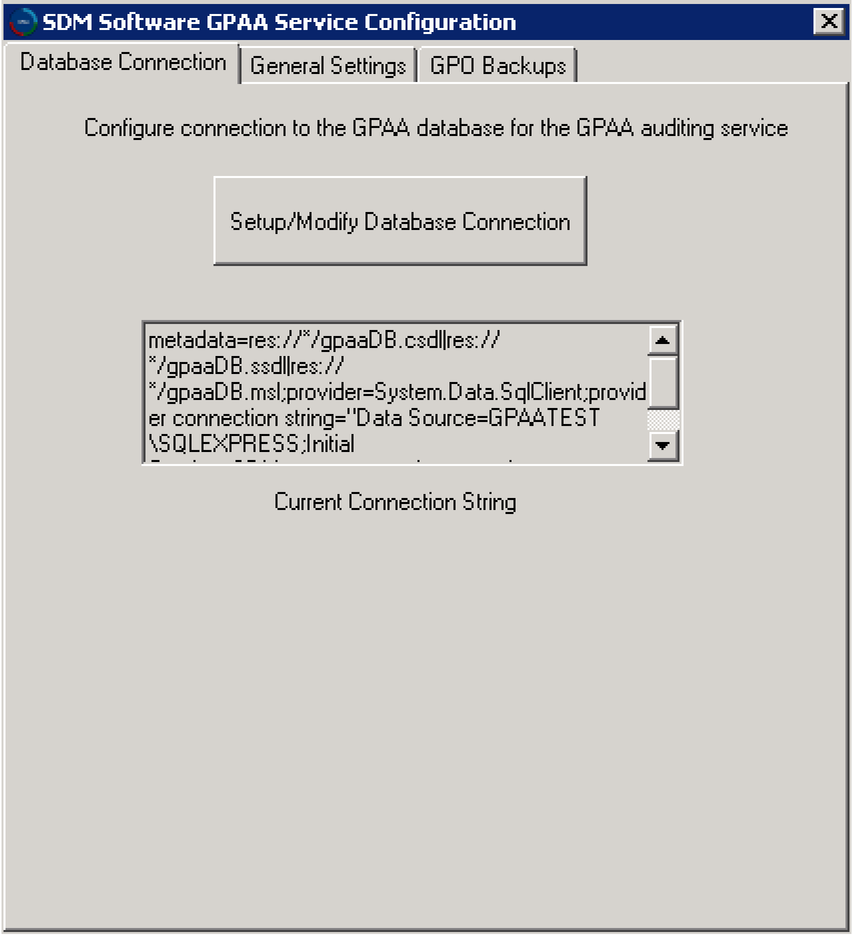
Where 49532 is the listening port for the SQLExpress instance.

Save the config file and then you can start the GPAA Attestation Service.

[UPGRADE NOTE]

When upgrading from GPAA 2.5, first de-install the existing GPAA Attestation service from Control Panel, Add/Remove Programs. Then you can install the 3.0 version of the service as shown above.

5. Set up the GPAA Auditing Service: The next step is to run the **Setup GPAA Auditing Service** option on all domain controllers within domains where you plan to perform GP change auditing. The included MSI setup file works for all versions of Windows Server from 2008-R2 to 2019. Note that during the GP Auditing Service installation process, you will be prompted to choose the service account required for the service to function. Make sure this service account has the required permissions, as described above, and has the “Logon as a service” right on your domain controllers. As with the GPAA Attestation Service, after installing the auditing service, you need to run the GPAA Auditing Service Configuration Utility that is installed with the product, to configure the database connection as shown here:


SDM Software GPAA Service Configuration
Database Connection
General Settings
GPO Backups
Setup/Modify Database Connection
Current Connection String

Configure connection to the GPAA database for the GPAA auditing service

```
metadata=res://*/gpaaDB.csdl|res://
*/gpaaDB.ssdl|res://
*/gpaaDB.msl;provider=System.Data.SqlClient;provid
er connection string="Data Source=GPAATEST
\SQLEXPRESS;Initial
```

This utility provides the same options to configure the database connection as the attestation service configuration utility and follows the same directions. Since the auditing service needs to be on all DCs in a domain, it's important to note that this configuration utility is simply modifying the GPAuditService.exe.config file within the GPAA Auditing Service installation directly (usually c:\program files\sdm software\SDM GPAA Audit Service), and therefore once this file is configured on one DC, it can be copied to all DCs without having to run the configuration utility manually on each DC. The other options on this page allow you to enable trace logging and change the time for nightly GPO backups (under the General Settings tab) as well as clean up GPO backups that were held on this DC when it's no longer using the GPAA auditing feature (under the GPO backups tab) or as instructed by SDM Software Support. If you choose to manually adjust the database connection string within GPAuditService.exe.config, the relevant connection string is:

```
<setting name="dbConnection" serializeAs="String">

<value>metadata=res://*/gpaaDB.csdl|res://*/gpaaDB.ssdl|res://*/gpaaDB.msl;provide
r=System.Data.SqlClient;provider connection string="Data
Source=SERVER\INSTANCE;Initial Catalog=SDM_gpomanager;Integrated
Security=True;MultipleActiveResultSets=True"</value>
</setting>
```

Replace the “SERVER\INSTANCE” text under the data source, with the server name and optionally, the instance name where your GPAA database is held.

In addition to the database connection setup, there is at least one other parameter you will want to consider modifying in the GPAA Auditing Service configuration file. GPAA has the ability to bundle up change notification emails when multiple changes occur in a short time interval. The default is that any time more than **10 change events** occur in a single interval, they will be bundled together and delivered as a csv attachment on the notification email that is sent. This option is controlled using the following section with the GPAuditService.exe.config file:

```
<setting name="MaxEmailThreshold" serializeAs="String">

      <value>10</value>

    </setting>
```

As previously stated, you will need to edit this file from an elevated command prompt in order to be able to save changes to it. If you wish to disable this email bundling feature, you can set the MaxEmailThreshold to -1. Changing this parameter requires restarting the GPAA Auditing Service to take effect.

Automating Deployment and Upgrade of the Audit Service

GPAA’s setup zip includes two methods for deploying and upgrading the GPAA Audit Service on your domain controllers. For upgrading an existing GPAA 2.5 Audit Service, we provide the **GPAAAuditUpdater.exe** command line utility. This utility runs on the domain controller and contains the updated files required to upgrade the audit service. It will stop the GPAA Audit Service, update its files and then restart it.

The second method provides a PowerShell installation script, that will install all relevant files silently on the domain controller where it is run. The script and accompanying zip file are meant to be deployed using an automated software installation solution such as Microsoft System Center Configuration Manager (SCCM). This installation script is called:

GPAA-AuditInstall_Silent.ps1

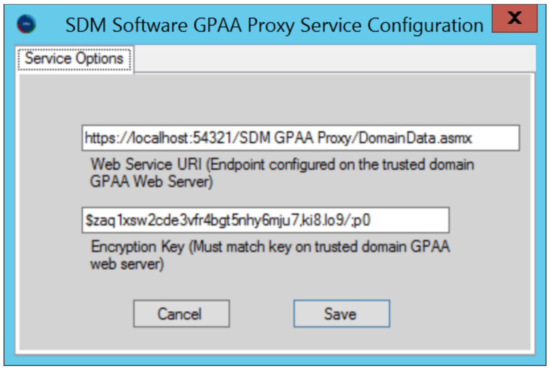
And comes with an accompanying zip file that must be distributed with the script whose name depends upon what version of Windows your DCs are running. The correct file name to distribute is documented in the comments of the script.

The zip file contains all the relevant GPAA Audit Service 3.0 Installation files required to perform the installation. You will need to replace the existing GPAuditService.exe.config (or GPAuditService7.exe.config for 2008-R2 domain controllers) file in the zip file with a version that contains your edited database connection string and any other parameters you’ve modified, in order to ensure that this version gets distributed to all DCs on deployment.

6. Set up the GPAA Untrusted Proxy Service: The final (optional) step is to install the **GPAA Untrusted Proxy Service**. If you plan to use the untrusted domain GPO Attestation feature, then you will need to run the installer for the GPAA Untrusted Proxy Service client on a server in the untrusted domain. You can install the service on either a member server or domain controller within the untrusted domain. Because the service runs as LocalSystem (i.e. the machine account where it's installed) then its ability to discover GPOs in the untrusted domain is limited by the Read permissions you have on those GPOs. By default, Authenticated Users has read permission on every GPO created, but this can be modified via Group Policy delegation. Therefore, you will need to ensure that the machine account where the Untrusted Proxy Service is installed has read permissions on any GPOs you wish to discover.

   The Untrusted Proxy Service client requires two pieces of configuration information to properly communicate with the GPAA Web Service Proxy installed in Step 2 above—a pre-shared key that matches the one configured in Step 2 on the web server, and a URI that points to the Web Service Proxy Application endpoint. The configuration file that stores this information is found in the installation folder for the Untrusted Proxy Service (usually in C:\Program Files\SDM Software\SDM GPAA Proxy Service 3.0) and is called **SDM GPAA Attestation Proxy Service.exe.config**.

   These two settings can be configured as part of the service installer, which presents itself as show here:

   https://localhost:54321/SDM GPAA Proxy/DomainData.asmx

   Web Service URI (Endpoint configured on the trusted domain GPAA Web Server)

   $zaq1xsw2cde3vfr4bgt5nhy6mju7,ki8.lo9/;p0

   Encryption Key (Must match key on trusted domain GPAA web server)

   Or, you can manually configure the settings within the config file. These two settings are listed in the config file here:

   The pre-shared key is defined in the **appSettings** section here:

   ```
   <add key="Key" value="$zaq1xsw2cde3vfr4bgt5nhy6mju7,ki8.lo9/;p0" />
   ```

   The web service URI is found within the **client** section as shown here:

```
<endpoint address="https://WebServer1/SDM GPAA Proxy/DomainData.asmx"
    binding="basicHttpBinding" bindingConfiguration="DomainDataSoap"
    contract="RemoteDomainData.DomainDataSoap" name="DomainDataSoap" />
```

If you use load balanced endpoints for your GPAA web servers, then the URI for the Untrusted proxy service client should use that endpoint as well.

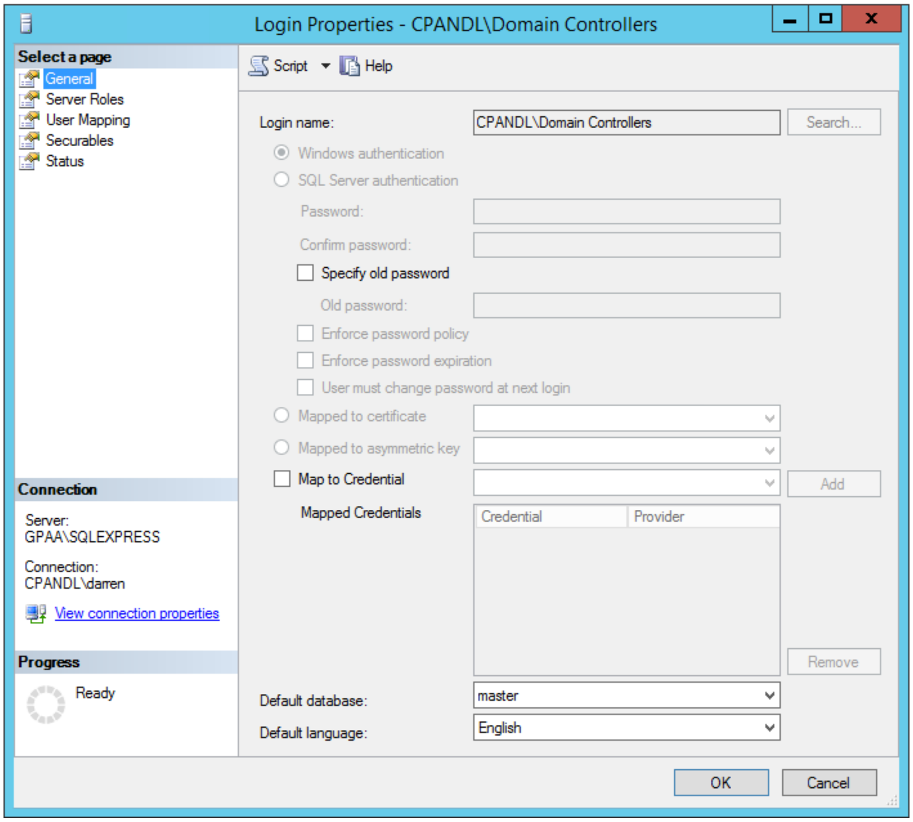
Support

If you have any questions or issues installing GPAA, please contact the SDM Software Support Team at support@sdmsoftware.com. We will be happy to walk you through the setup and ensure your components are configured correctly for proper operation of the product.

Appendix A: Installing the GPAA Auditing Agent as LocalSystem

Overview: In an effort to support least-privilege installations, GPAA 3.0 has been tested to run the GPAA Audit Service agent as localSystem on domain controllers, instead of the recommend domain service account that is a member of the Domain local Administrators security group. Two main changes need to be made in order to accommodate running the Audit Service as localSystem:

1. The domain controller machine account needs to be able to read the **Security Event Log**. By default, the localSystem account on a DC (i.e. the machine account) **already has the ability to read the security event log.** In most cases, you don't need to do anything for this step. However, if you have explicitly configured your environment otherwise, you will need to grant this right. The easiest way to do this is to grant the **Domain Controllers** built-in group, membership in the "Event Log Readers" group. This should be sufficient to grant read access to the security event log, to all DCs.
2. The group of DCs in your domain need read and write access to the GPAA database. The easiest way to do this is to use SQL Server Management Studio on your GPAA database server to perform the following steps (NOTE—these steps should be done AFTER you've created the GPAA database as part of the setup routine):
    a. From the database-wide "Security" node in SQL Server Management Studio, right-click "Logins" and create a "New Login".
    b. Under login name, make sure Windows Authentication is selected and Search for a group in your domain containing all of your DCs. You can use the built-in "Domain Controllers" group for this, as shown here:



Login Properties - CPANDL\Domain Controllers

Login name: CPANDL\Domain Controllers

● Windows authentication

○ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☐ Enforce password policy

☐ Enforce password expiration

☐ User must change password at next login

○ Mapped to certificate

○ Mapped to asymmetric key

☐ Map to Credential

Default database: master

Default language: English

Server:
GPAA\SQLEXPRESS

Connection:
CPANDL\darren

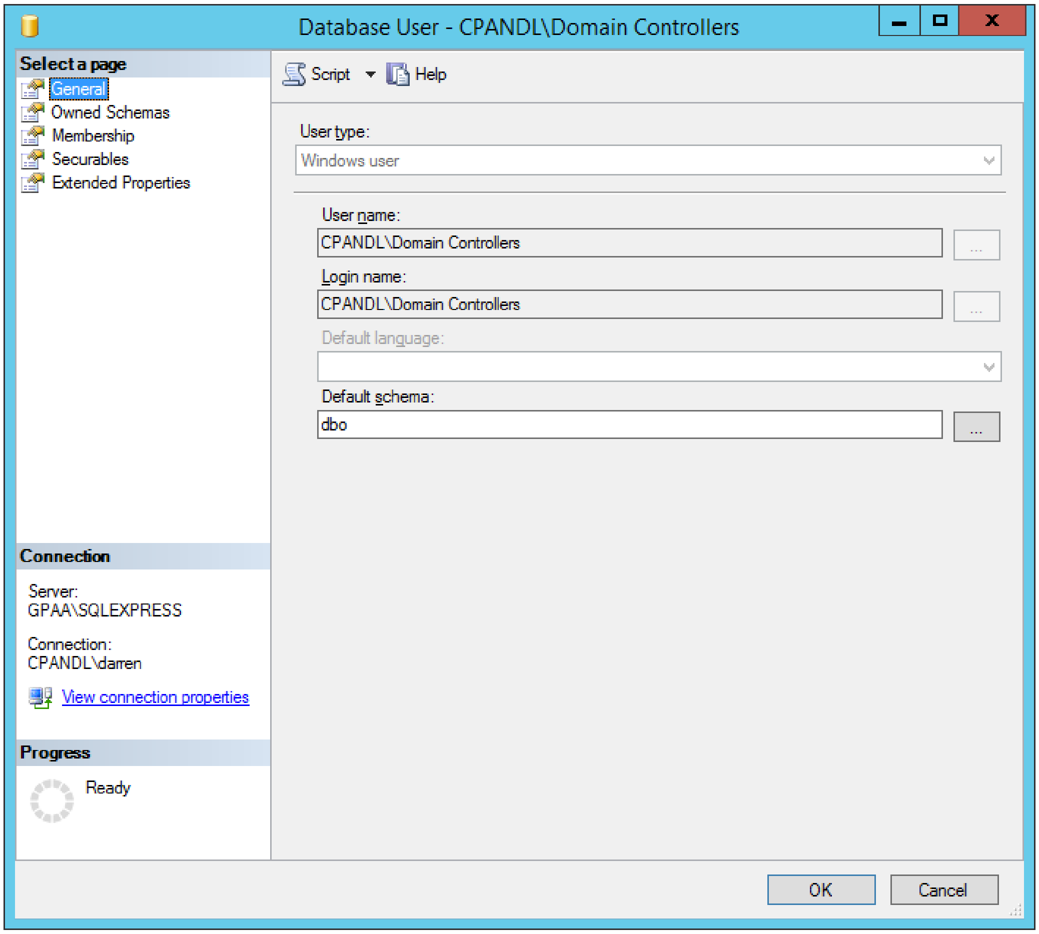
c. You can accept the defaults on the login—just make sure the login is set to Enabled from the Status page.

d. Next, expand the node under Databases that is your GPAA database (usually called SDM_GPOManager), right-click the Security node and select “New User”.

e. From the New User Dialog, select Windows user from the User type dropdown and then press the ellipsis (…) button on the username dialog.

f. Search your AD domain for the group specified in b) above (e.g. Domain Controllers) and press OK.

g. In the Default schema dialog, press the ellipsis button and search for and accept “dbo”. The screen will look as follows:



User type: Windows user

User name: CPANDL\Domain Controllers

Login name: CPANDL\Domain Controllers

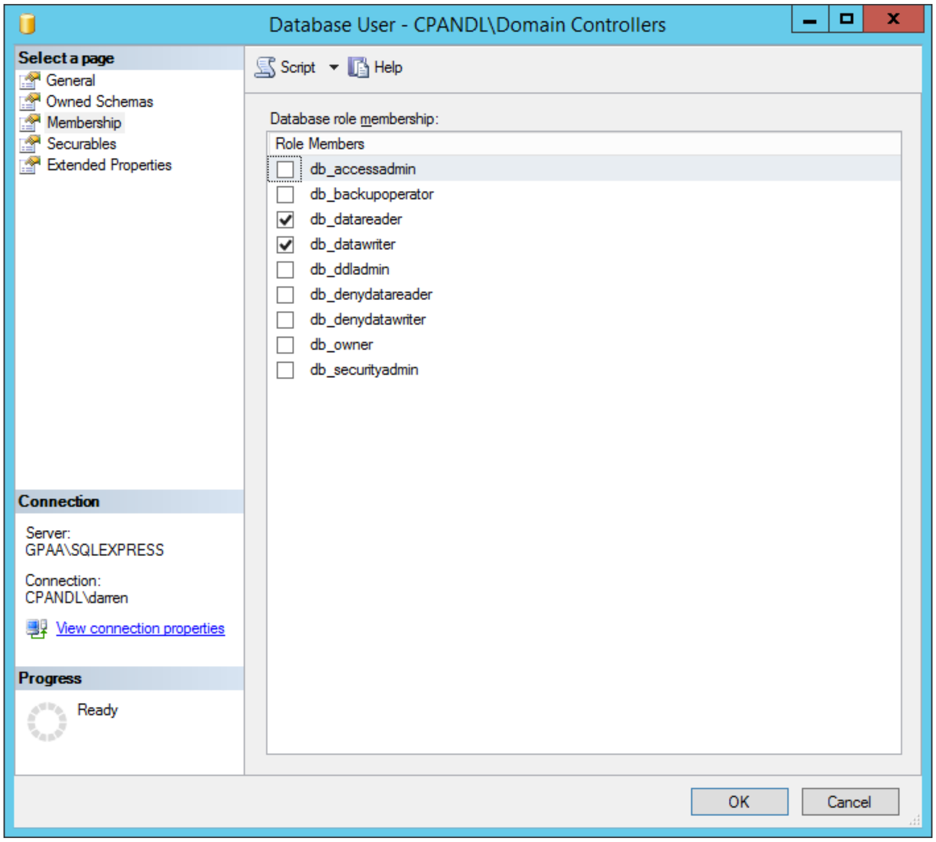
Default language:

Default schema: dbo

Server: GPAA\SQLEXPRESS

Connection: CPANDL\darren

h. Select the “Membership” menu on the left-hand side of the screen and select db_datareader and db_datawriter permissions, as shown here:



Server:
GPAA\SQLEXPRESS

Connection:
CPANDL\darren

Ready

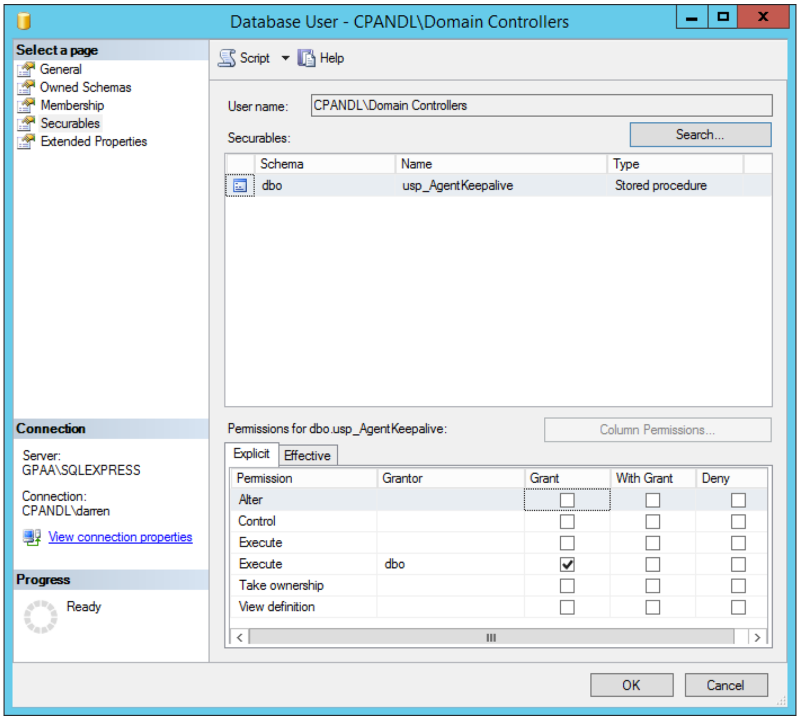
Database role membership:

Role Members
- ☐ db_accessadmin
- ☐ db_backupoperator
- ☑ db_datareader
- ☑ db_datawriter
- ☐ db_ddladmin
- ☐ db_denydatareader
- ☐ db_denydatawriter
- ☐ db_owner
- ☐ db_securityadmin

i. Select the “Securables” menu on the left-hand side of the screen and press the Search button. From the Add Objects dialog, select “Specific objects” and when the Object Types dialog comes up, press the Object types button and select Stored Procedures, then select the Browse button.

j. From the list of stored procedures, select the [dbo].[usp_AgentKeepalive] stored procedure and press OK.

k. Under the permissions for the Stored Procedure, select the “Execute” permission on the Grantor dbo by checking the Grant column, as shown here:



User name: CPANDL\Domain Controllers

Securables:

Schema	Name	Type
dbo	usp_AgentKeepalive	Stored procedure

Server: GPAA\SQLEXPRESS

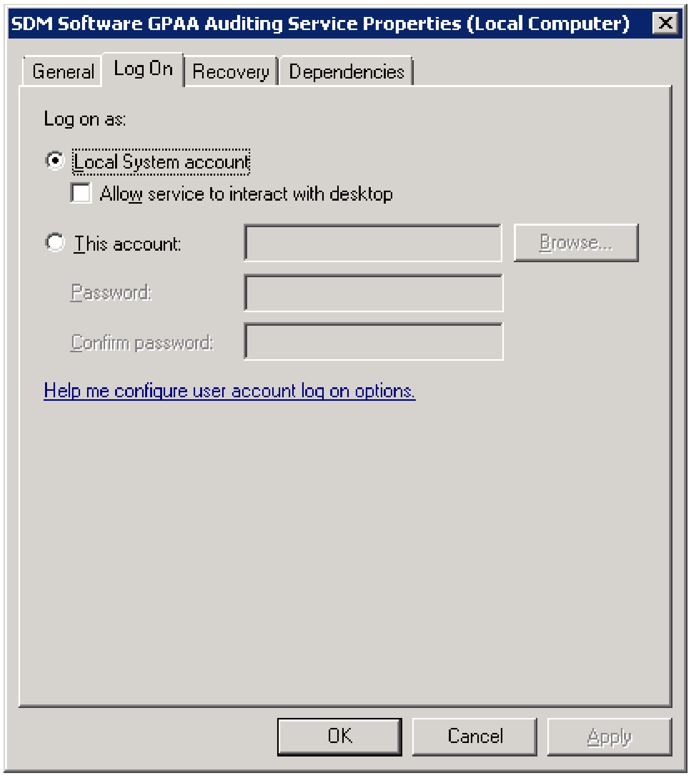
Connection: CPANDL\darren

Ready

Permissions for dbo.usp_AgentKeepalive:

Permission	Grantor	Grant	With Grant	Deny
Alter		☐	☐	☐
Control		☐	☐	☐
Execute		☐	☐	☐
Execute	dbo	☑	☐	☐
Take ownership		☐	☐	☐
View definition		☐	☐	☐

l. Press OK and you will now be able to run the GPAA Audit Service successfully as localSystem. You can do this by simply double-clicking the service on the DC from the Service Control Manager, selecting the Logon tab, and selecting Local System account, as shown here:


SDM Software GPAA Auditing Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Browse...
Help me configure user account log on options.
OK
Cancel
Apply

Log on as:

● Local System account

☐ Allow service to interact with desktop

○ This account:

Password:

Confirm password: