SDM Software Group Policy Compliance Manager®

Version 1.7

User Guide

Revisions:

Document Version 1.1....September 29, 2025

Document Version 1.0…… August 13, 2025

Contents

Overview

With Group Policy Compliance Manager, you can be assured your Windows desktops and servers are compliant with the Group Policy settings you have deployed to them. Using GPCM, you can prove to yourself and your management that a given GPO has been processed by any given computer or user. In addition, GPCM contains these helpful features:

- Agentless and agent-based collection (for larger environments) of GP processing health and settings data across your Windows environment
- Easy to install GUI gets you up and collecting data in minutes
- Collect and report against a single machine, an OU or across a domain
- Search for specific machines, users, GPOs or even settings across your environment
- Generate a variety of compliance and setting reports that roll up GP processing data at the OU or domain level; export to a variety of formats
- Retrieves Resultant Set of Policy settings data from remote Windows servers and workstations
- PowerShell module that allows collecting, querying, searching and manipulation of collected GP processing data
- Provides both GP processing health and timing data from all systems
- Allows saving frequently used searches and collections
- Exports processing summaries to Excel, Word, or PDF
- Supports all OS versions from Windows 10 & 11 to Windows Server 2016-2025

The product leverages SDM Software's unique expertise in Group Policy to provide the ability to analyze your Group Policy environment. Perform a collection on one computer or several computers at once, or on an entire domain; view errors for any failures; see a summary of your environment using pre-designed reports that show how many computers and users have received error-free Group Policy processing and find out where a particular setting has been deployed across your environment.

Group Policy Compliance Manager provides an invaluable resource for getting a handle on Group Policy as it's deployed to your Windows systems. You can finally answer the question, "how do I know if all of my computers or users have gotten a particular Group Policy setting?"

Using the Product

Once the product is installed and configured (see the GPCM Installation, Deployment & Troubleshooting Guide for a detailed walkthrough of the installation process), you can begin using it to report on Group Policy settings health and compliance. The main interface into the GPCM product is the GUI-based GPCM console (See Figure 1) below, or the PowerShell module called **SDM-GPCM**.

Performing a Collection

The key to using the GPCM product is the collection. A collection is a request sent to an endpoint (Windows Server or Desktop) to return information related to Group Policy health and settings that have been received by that endpoint. GPCM collections rely on a combination of a SDM Software proprietary mechanism to determine GP processing health, as well as using the existing Microsoft Resultant Set of Policy (RSoP) capability to return information about what settings have been process by a given computer or user, and what GPO delivered those settings. There are three ways to perform a collection in GPCM:

1. Through the GPCM UI, you can remotely collect data from one or more computers.
2. Through the GPCM PowerShell module, you can use the **Invoke-SDMGPCMCollection** cmdlet to perform remote collections, similar to #1 above, but using PowerShell.
3. Through the GPCM agent, deployed to desktops and servers. This option allows you to configure the frequency with which data is collected and allows for unattended collection, but does require additional be deployed to collect and process the data generated at the endpoint.

In general, the rights required to perform each type of collection are the same. The first two methods, being interactive, require a user who has **administrative permissions** on the endpoints being collected against. This translates to needing to be in the local administrators group on the endpoints in question. For #3, the GPCM agent runs as **localSystem** and thus has all the permissions it needs to be able to be able to collect the required data.

Collection from the UI

From the GPCM UI, to perform a collection, you simply need to right-click on one or more computers, or alternatively, you can right-click a container (e.g. OU) from the AD treeview and select "Collect Now' from the context menu.

Collecting against nested containers

When you right-click an OU and select "Collect Now", only the computers that are direct members of that OU will be included in the collection list. If you want to collect against computers from a nested OU hierarchy, you need to use the "Mark for collection" option. Mark each OU that contains the computers you want to collect against. Those will be highlighted in green. Once you have all the containers you wish to collect against marked for collection, right-click one of those selected containers and select "Collect Now".

When you do that, you're presented with a dialog to confirm the options you wish to collect, as shown below.

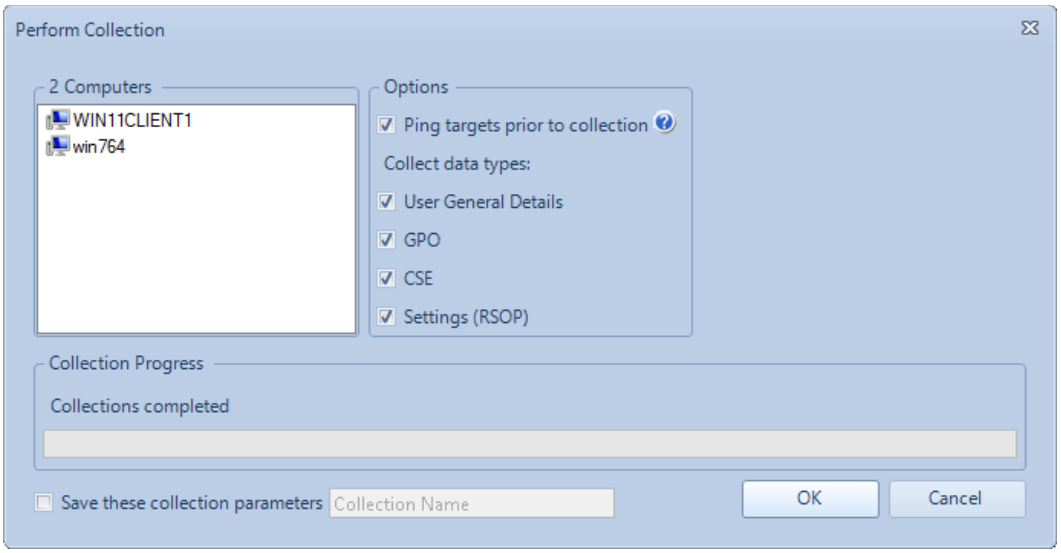


Figure 2: Collecting against multiple computers

The UI provides options for what to collect. Each option is described here:

- **Ping targets prior to collection**: In an effort to prevent long delays during collection, when this option is checked, GPCM will first attempt to ICMP ping the target computer prior to attempting further collection. If the ping fails the process will move on to the next machine
- **User General Details**: This option allows you to decide if you want to collect general GP Processing data about any user currently logged onto the computer being collected against. You can uncheck this to exclude user data from the collection, resulting only in per-computer GP processing information being retrieved
- **GPO**: Indicates whether to collect per-computer or per-user GPO metadata. This corresponds to the "Group Policy Object Details" section of the GP Processing Summary Report described in Viewing Collection Data section below.
- **CSE**: Indicates whether to collect per-computer or per-user CSE metadata. This corresponds to the "Client Side Extension Details" section of the GP Processing Summary Report described in Viewing Collection Data section below.
- **Settings (RSOP)**: This indicates whether to collect the actual settings received by the computer or user.

GPCM will collect per-computer GP processing data for a given computer. Per-user data will only be collected if a user is logged onto the system during the collection. This is true for all forms of collection including GUI-based, PowerShell and agent-based collections.

Another option you'll see on this collection screen is the ability to save a collection for future use. The "Save these collection parameters" check box, if checked, will save the list of computers that have been selected, so that they can be collected against again. When you check the box, you'll be prompted to

provide a name for the collection. Once the collection completes, the new saved collection will be saved under the “Saved Collections” node in the left-hand tree view, as shown below.

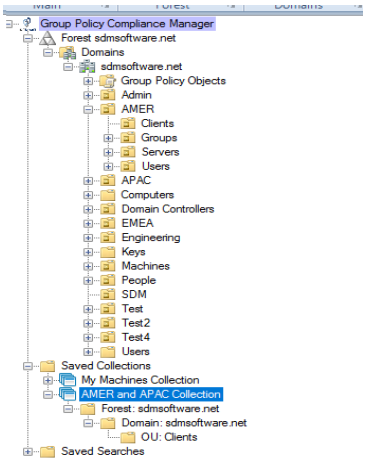


Figure 3 Viewing Saved Collections

Once a collection is saved, you can right-click the collection name to “Collect Now”, “Rename” the collection or “Delete” the saved collection.

Collection from PowerShell

The PowerShell module provides the **Invoke-SDMGPCMCollection** which can be used to perform collections against one or more computers. The form of this cmdlet is as follows:

Invoke-SDMGPCMCollection [-ComputerName] <String> [-Recurse <SwitchParameter>] [-Domain <String>] [-UseSQL <String>] [-DBCredential <PSCredential>] [-CollectCredential <PSCredential>] [<CommonParameters>]

Invoke-SDMGPCMCollection [-Scope] <String> [-Recurse <SwitchParameter>] [-Domain <String>] [-UseSQL <String>] [-DBCredential <PSCredential>] [-CollectCredential <PSCredential>] [<CommonParameters>]

The cmdlet can target collection against a single computer (by using the -ComputerName parameter) or a container of computers (e.g. an OU) by using the -Scope parameter. Both ComputerName and Scope parameters expect a Distinguished Name (DN) format. If you specify a container using -Scope, you can also use the -Recurse parameter to collect from child containers/OUs under the parent container you specify.

The -Domain parameter takes the DNS name of the AD domain you’re collecting against. The -UseSQL parameter specifies the SQL Server name and any instance name (e.g. Server1\MyInstance). The default

SQL port of 1433 is assumed but if you specify to use another port, you specify it this way: Server1,40059\MyInstance, where 40059 is the alternate port to use.

The -DBCredential and -CollectionCredential parameters are used to supply credentials for accessing the SQL Server GPCM instance and the endpoint(s) you're collecting against, respectively. If you don't provide these credentials, the current user running the cmdlet is used for both database and endpoint connections. Note that these two credential parameters require a PowerShell PSCredential object, which you can create using the **get-credential** cmdlet.

Navigating the UI

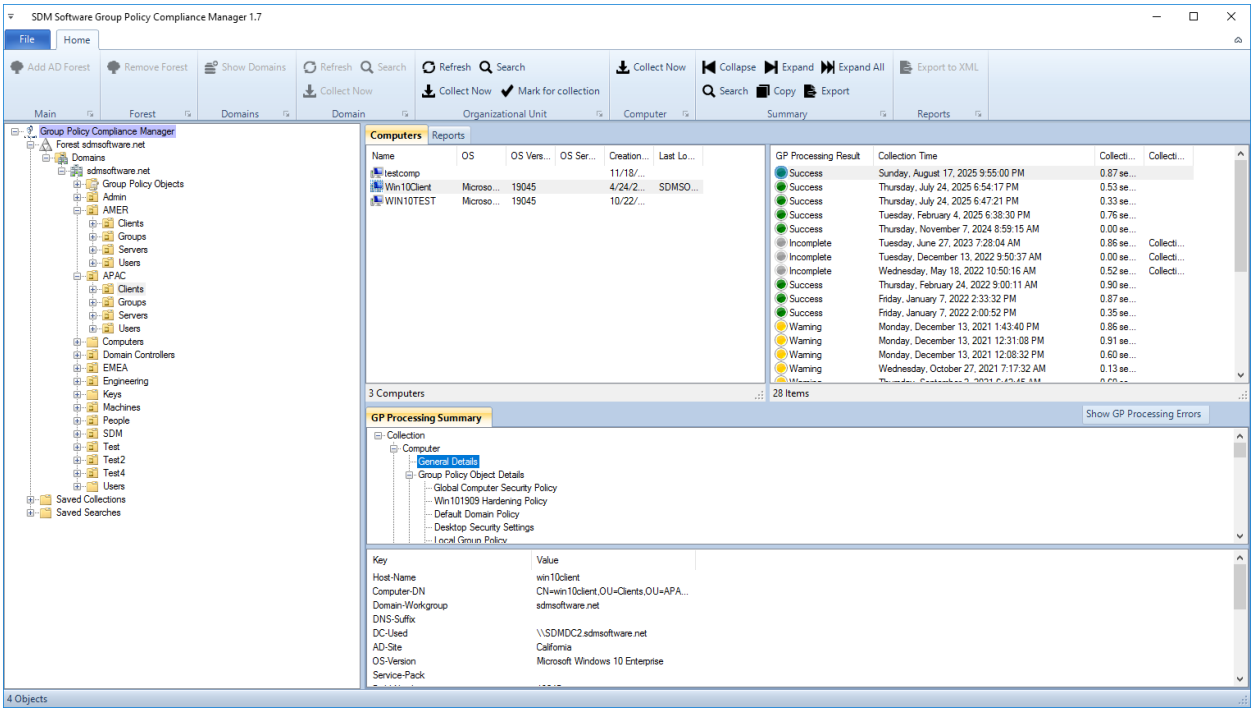


Figure 3 The GPCM GUI Console

If you followed the installation process, you will have configured a database connection to a SQL Server instance (or SQL Express for testing/evaluation purposes) where the GPCM database was created. By default, when you start the GPCM console, it will load the current, default AD forest to which your current user is a member of. Additional forests and domains can be added if desired.

- To add a forest: Right click the tree node called "Group Policy Compliance Manager" of the navigation tree in the left pane, select "Add AD Forest." Or click the "Add AD Forest" button in the Ribbon Bar that displays horizontally across the top of the program. No domains for the new forest will display at first. Add domains by doing the following:
- To add a domain: Right click the tree node called "Domains" of the navigation tree in the left pane, beneath the forest node in which your desired domain resides, then select "Show

Domains." Check the box next to the domain(s) that you want to display in the navigation tree, then click Ok.

One handy feature in the AD tree view is the ability to copy the Distinguished Name of an AD container to the clipboard. If you right-click an OU, for example, and select “Copy DN”, the DN of that OU will be copied to the clipboard.

In addition to the AD domain tree that displays in the left-hand pane, you will see a “Group Policy Objects” node that will appear right under the domain name. That node contains similar functionality to what you have in the Microsoft Group Policy Management Console (GPMC) where you’re able to view links, status and settings on each GPO in the domain. This is a “read-only” view of GPOs in the domain for your convenience. There is no GPO management capabilities available from this view, as shown below:

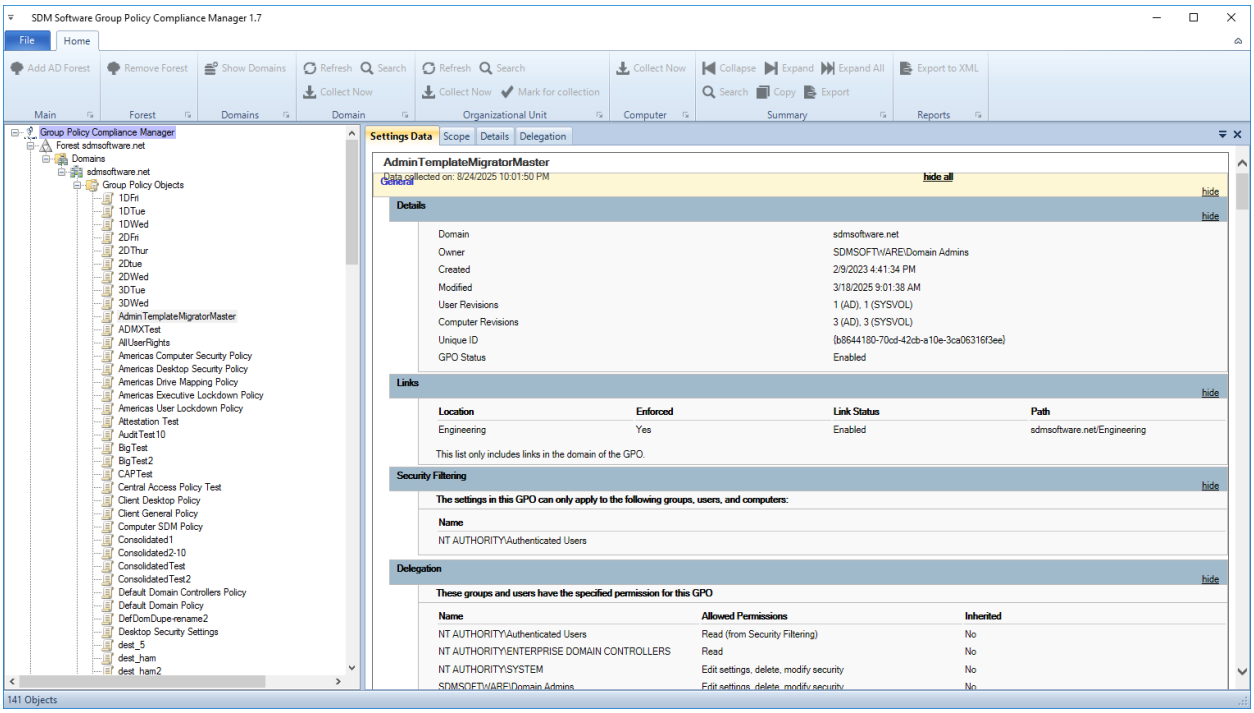


Figure 4: The Group Policy Objects node

Within the AD tree view, as you navigate through your AD domains, when you select an OU containing computers, you will the computers appear in the Computers list, highlighted below in green.

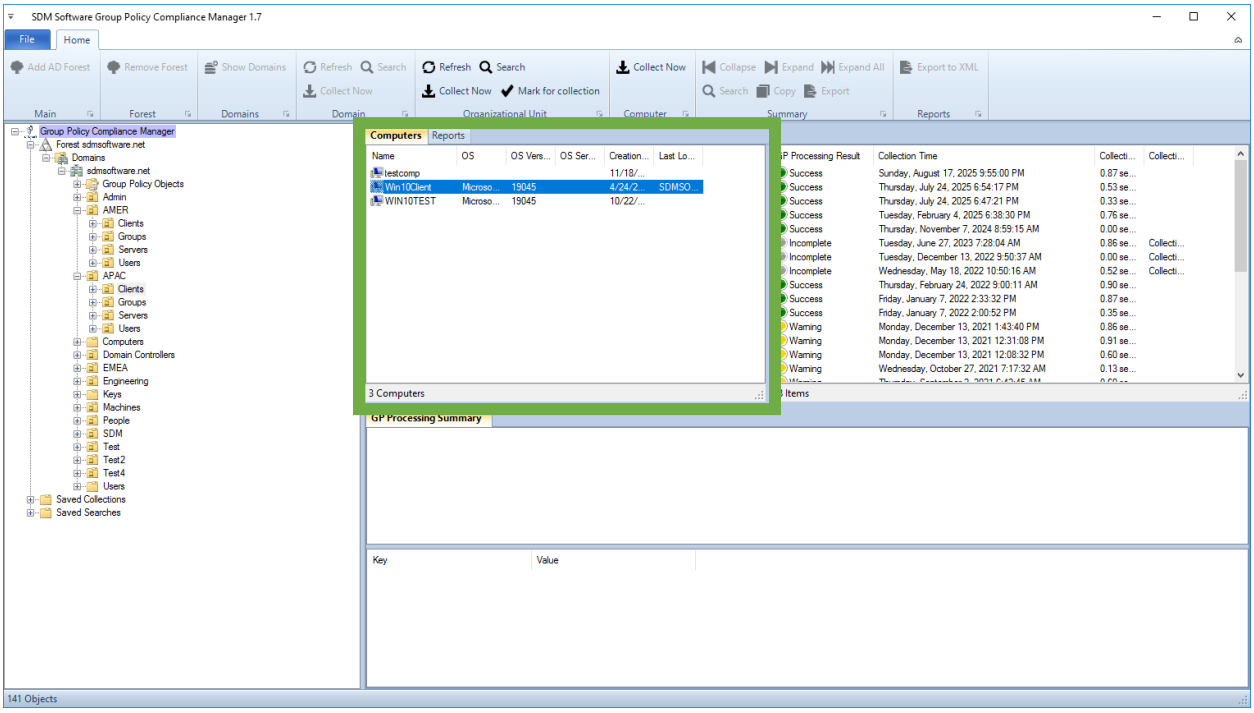


Figure 5: Viewing computers within a domain

Note: The GP Compliance Manager console does not display any objects other than computer objects.

When you select a computer object, if collections have been performed against it, those collections will appear in the list to the right of the computers, as highlighted below in green.

You can also right-click a computer object to copy either the computer name or computer Distinguished Name (DN) to the clipboard for easy documentation.

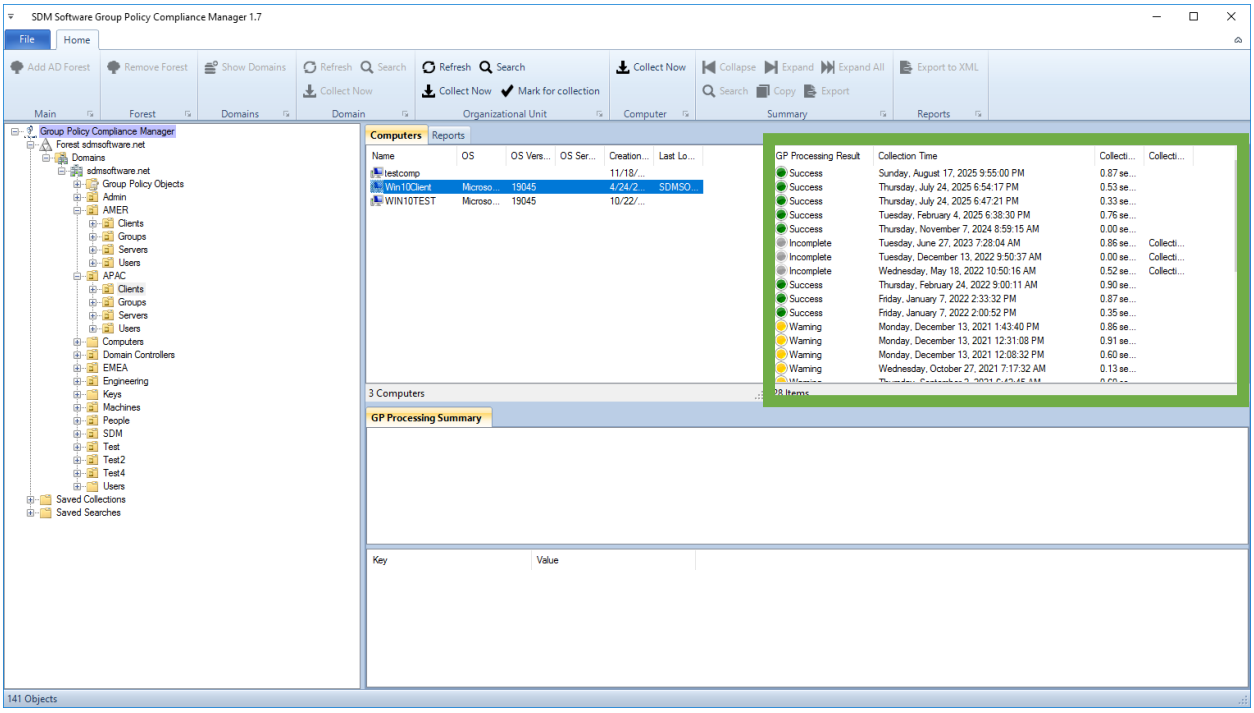


Figure 6: Viewing computer collections

A collection can have a variety of statuses, depending upon the result. It's important to note that the "GP Processing Result" column is reporting about the success or failure of Group Policy processing on the endpoint when the collection was made. For example, if you collect data from the endpoint at 12pm on Monday, the result reported in this column will be the result of the last GP processing cycle that occurred on the endpoint prior to 12pm on Monday. If the collection itself fails outright (i.e. the product is not able to successfully collect GP status) then the status in this column will show "Incomplete" and the "Collection Errors" column will show the reason why the collection failed. The possible statuses, and their explanation, is listed here:

GP Processing Result	What It Means
Success	Collection completed and the last GP processing cycle was successful
Warning	Collection completed and the last GP Processing cycle completed, but some errors were detected in one or more Client Side Extension (CSE) areas
Fail	Collection completed but the last GP processing cycle failed. This means that GP processing was not at all successful the last time it ran.
Incomplete	The collection of data failed for some reason.

Viewing Collection Data

When you select a collection, the bottom "GP Processing Summary" pane will be populated, as shown below.

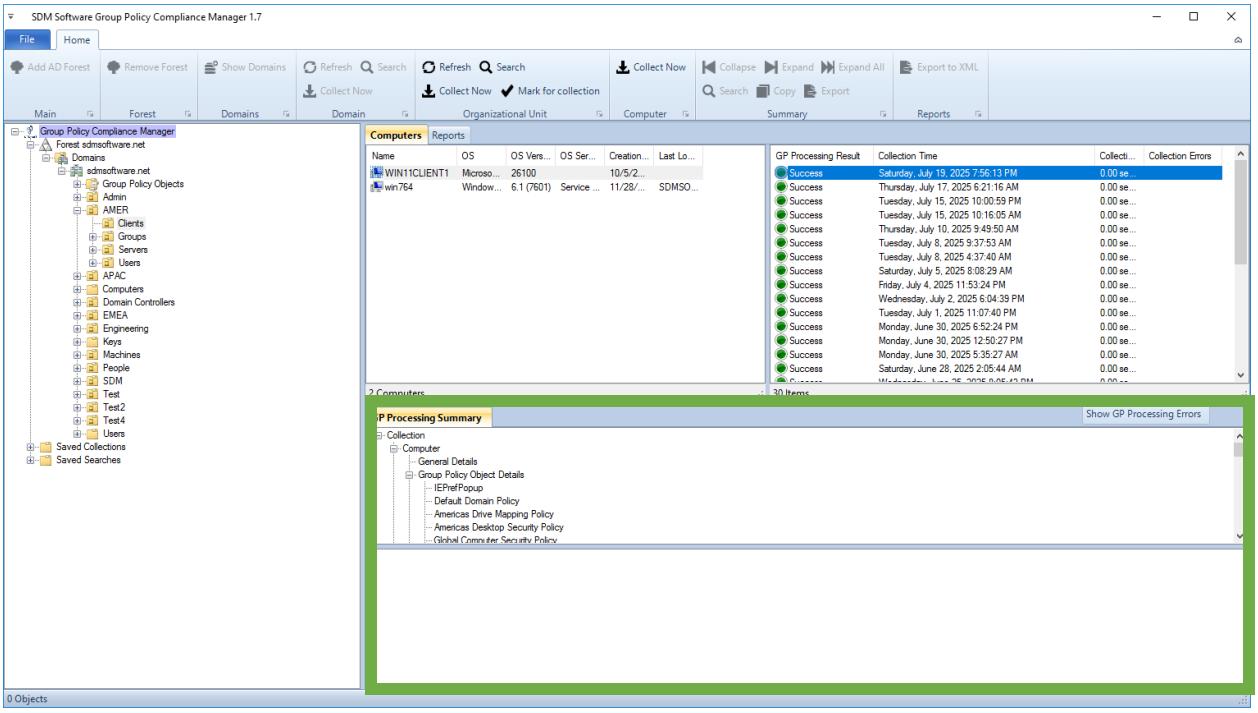
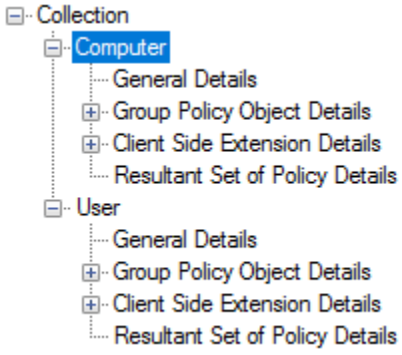


Figure 7: Viewing GP Processing Summary data

The data shown in this pane is presented in a treeview format and shows both per-computer and per-user data. The tree has the following nodes:



Each section is described here:

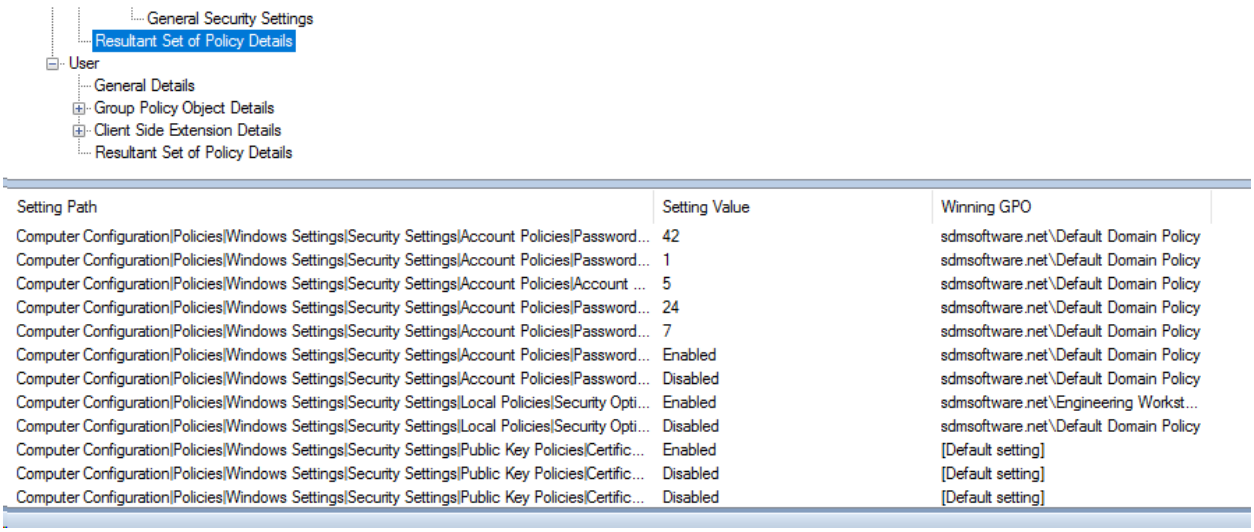
General Details: This provides metadata around the last GP processing cycle that was collected during this collection. This includes which domain controller was used for GP processing by the computer or user, what Active Directory (AD) site that computer was detected in, whether flags such as “slow link” or loopback processing were detected and the start and end times of the GP processing cycle that was captured. This section will also return the overall status of the “core” part of GP processing, which is the part that detects which GPOs the user or computer needs to process.

Group Policy Object Details: This provides a list of GPOs that were processed by the computer or user during this processing cycle and also the metadata associated with each GPO, including the version of

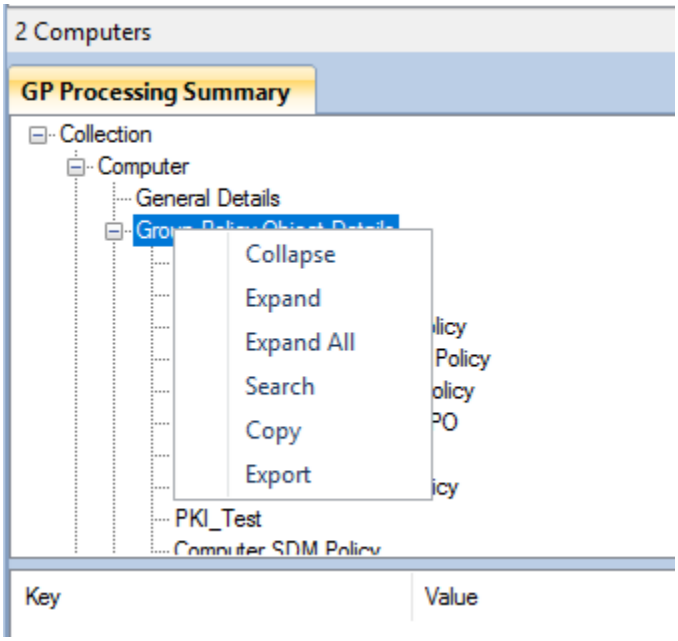
the GPO as it was read from the DC where GP processing occurred and whether the GPO was denied because of security group filtering, disabled links or WMI filters.

Client Side Extension Details: This provides a list of the Client Side Extensions that ran during GP processing. CSEs map to GPO policy areas that are implemented within each GPO. You can see, for each CSE, which GPOs contained settings from that CSE and what flags were detected for each CSE.

Resultant Set of Polices: This is the section that lists the actual settings that were received by the computer or user, and the "winning" GPO that delivered those settings. You can see an example of that here:

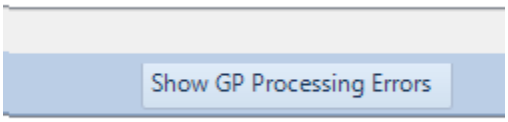


For any node within the GP Processing Summary tree, you can right-click the node to perform the following actions:



The “Export” function will allow you to export the details of everything underneath the selected node, to a CSV file.

The final thing to note about GP Processing Summary, is the “Show GP Processing Errors” button listed to the right of the GP Processing Summary window, as shown here:



When a collection has a status other than “Success”, you can press that button and it will pop up a window that displays the actual error, either per-computer or per-user, that generated the overall status.

Searching for Data

The GPCM UI provides a facility to search for data that has been collected using one of the methods previously mentioned. A variety of search criteria can be used to find computers so that you can either perform collections on them, or view collections that have already been done. Right click your targeted node in the left navigation tree and select “Search”. The following dialog will display.

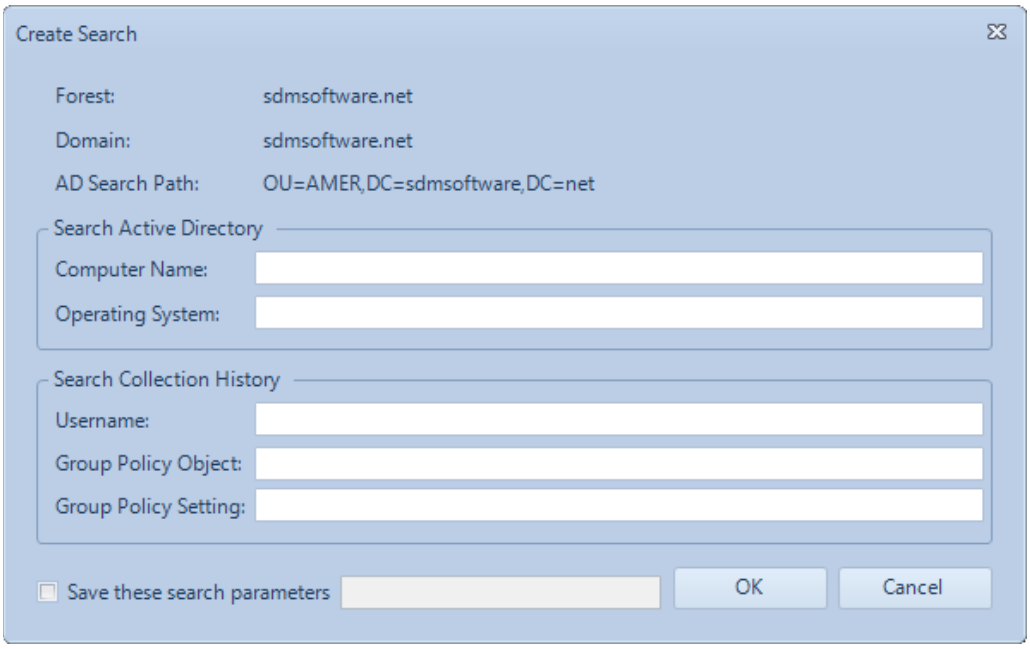


Figure 8: Viewing the Search Dialog

From the search dialog, you can search for a number of criteria within the AD container (and it’s children) that you’ve selected to search on. Note that search is recursive if you’ve selected a top-level

OU and wish to search all child OUs nested within that OU. You can search either Active Directory or the GPCM database. The first two search criteria—Computer Name and Operating System, will search AD for computers or OS versions that meet your search criteria. The search criteria you enter can be a full or partial search term. The search is conducted without regard to case and will look for the search string within AD. For example, if you search for a Computer Name of **win10**, the results will return all machines that contain **win10** in their name.

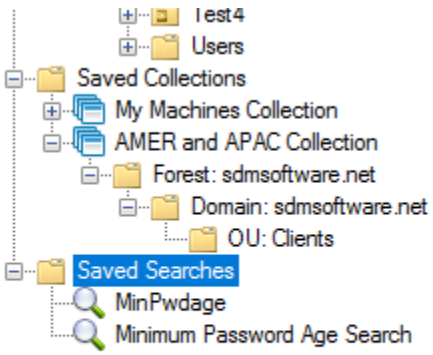
The second 3 search criteria will search the database for a particular user name that has logged into a computer, a Group Policy Object name that was processed by a computer or user, or a part of full of a GPO setting path name that was processed by a computer or user. Here are examples of valid searches for each:

Username: Search Term: smith (will return any computers where a username that contains "smith" was logged on during a GPCM collection)

Group Policy Object: Search Term: Default Domain Policy (will return any computers that processed the "Default Domain Policy" as a "Winning GPO", as stored by a GPCM collection.

Group Policy Setting: Search Term: Minimum Password Age (will return any computers that have RSOP details showing a setting that contains the text "Minimum Password Age" anywhere in the setting path. Note that if you provide a more complete setting path, it must be delimited using a | symbol. Such as "Computer Configuration|Policies|Windows Settings|Security Settings|Account Policies|Password Policies|Minimum password age"

Once you've specified search parameters, you can press the "OK" button to execute the search or you can first check the "Save these search parameters" check box and give a name to your saved search. Then, once you execute the search, it will be saved and can be re-used within the Save Searches section of the left-hand treeview, as shown here:



When you execute the search, the computers that meet your search criteria will appear in the "Search Results pane, as shown below.

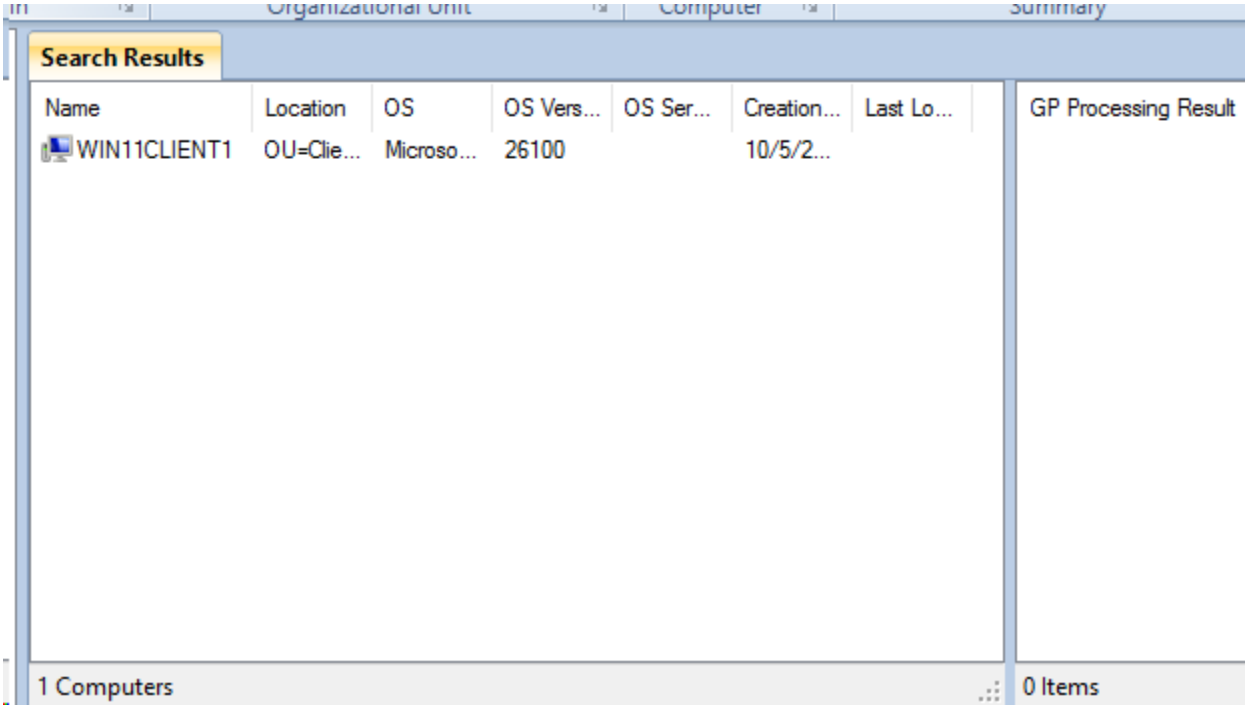


Figure 9: Viewing Search Results

When you a select a computer in search results, you'll have the ability to select the collections related to that result. If you searched for a GPO or a setting name, for example, when you select a collection from the computer search result, you'll notice that the "Resultant Set of Policy Details" node in the GP Processing Summary pane below will have been selected and the specific setting that meets your search criteria will be highlighted, as shown in the figure below.

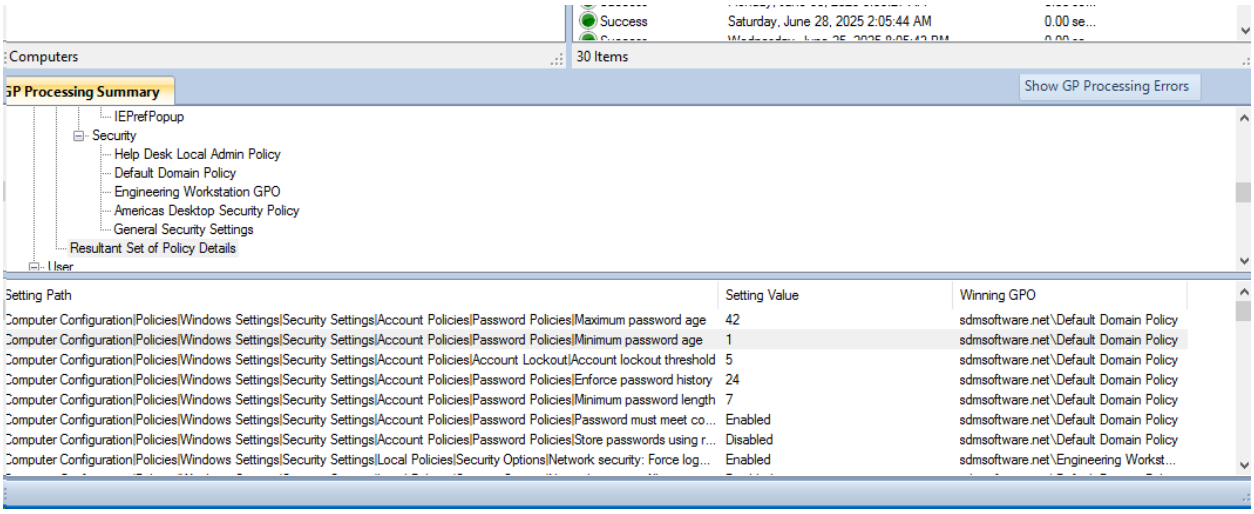


Figure 10 Viewing Setting Search Results

Settings

From the File menu in the GPCM UI, you can select the Settings option to configure certain aspects of the UI tool. The Settings dialog appears as follows:

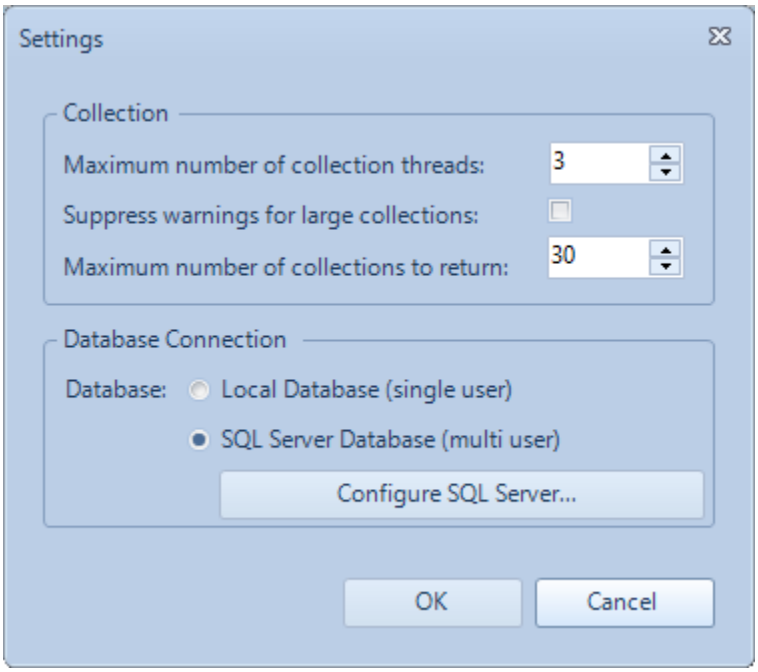


Figure 1 Viewing the Settings Dialog

This dialog is also where you will configure your connection to the GPCM database and, optionally, generate the SQL script to create the database the first time you install the product.

Please note that as of GPCM 1.7, the "local database" option shown in this dialog is no longer supported. You will use either SQL Server Express for small deployments or full SQL Server, and will define both using the SQL Server option.

The options in this dialog are defined here:

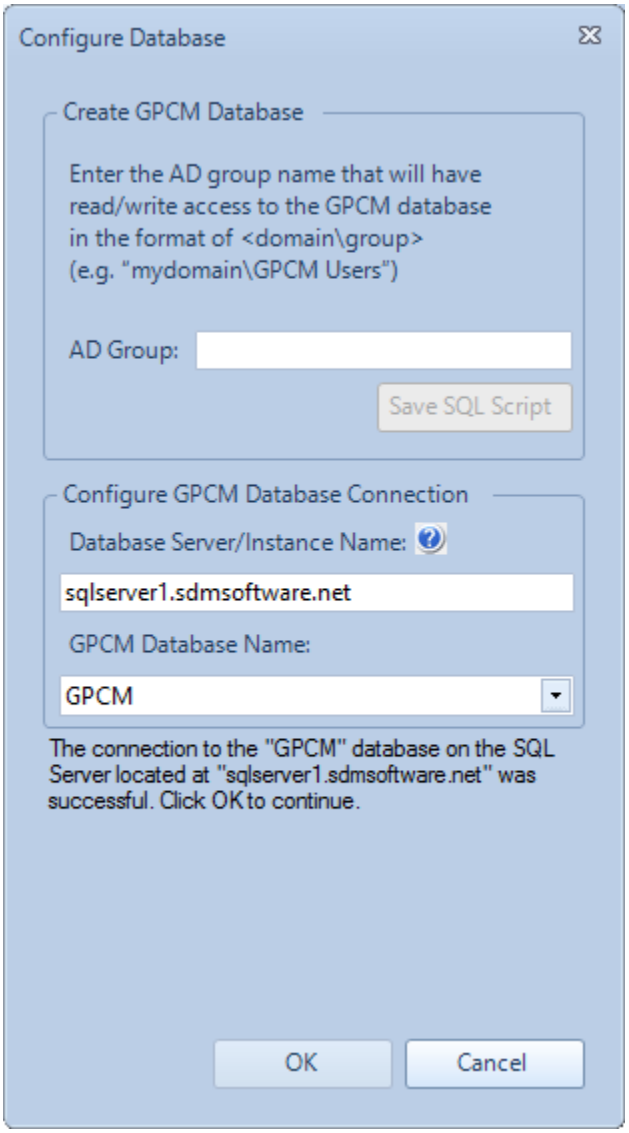
Maximum number of collection threads: When a collection is performed on more than one computer, a multi-threaded process will collect data from multiple computers simultaneously. You can control the number of threads used with this setting. The default setting is 3. The number of threads you select is a function of the number of logical and physical CPU cores you have available on the system running GPCM. For example, a system with 4 cores that support hyper-threading means you effectively have 8 cores, so you can set the GPCM threading count to a maximum of 8. Note however that if the threading count is set to a value greater than the number of machines you are collecting against, the effect can reduce collection performance.

Suppress warnings for large collections: By default, a warning displays if a Collect Now is selected for 100 or more computers, to confirm that the collection may take several minutes. This setting controls whether or not the warning will display.

Maximum number of collections to return: When selecting a particular computer to view its collections, we limit the number of collections returned to the last 30 by default. This can be adjusted up or down, but enumerating large numbers of collections can take time, so we recommend leaving this in place unless you really need to see older collections. As an alternative, you can use the PowerShell module as well to return all collection information for a given computer.

Database Connection Dialog

The database connection dialog allows you to perform two main tasks. The first task is that you can tell the GPCM Admin UI that you wish to either use the local SQL Compact repository to collect and store GP Settings data, or you can select a SQL Server instance to use for collection and reporting. The second task that can be performed, is that you can setup the GPCM SQL Server database if it hasn't been done yet. This must be done once when you are ready to deploy GPCM to SQL Server. When you select the "Configure SQL Server" button on the above dialog, you will see the following options:



The first step you'll need to complete, is to define an AD security group that will have read/write access to the GPCM database. You will specify that domain\group name in the "Connect to GPCM Database" option at the top of the dialog above. Once you populate the "AD Group" field, the "Save SQL Script" button will be enabled. Pressing the button opens a file dialog where you can save the resulting SQL Script that is generated. That script can be run in **SQL Management Studio** against the SQL Server database where you intend to house GPCM data. When you execute the query using the SQL Script, the GPCM database and all tables are created. The default GPCM database name is "GPCM."

If you need to use another name for the GPCM database other than "GPCM" please contact support@sdmsoftware.com for further details.

From the dialog above, you can then specify the database server\instance name (or just server name for the default instance; e.g. **SQLServer1\MyInstance** or just **SQLServer1**) and the database name to make the connection for the GPCM admin UI. If you are using a port other than 1433 to connect to SQL Server, you would specify that port as follows: **SQLServer1,<port>\MyInstance**. From then on, all data displayed or collected via the GPCM UI will be accessing your SQL Server GPCM database. The "Configure GPCM Database Connection" dialog will validate that you have connectivity to the SQL Server you specify after you type its name.

Reporting

GPCM version 1.7 introduced a number of reports that you can run to analyze Group Policy compliance within your environment. In general, reports are available from the “Reports” tab when you’ve selected any container within the AD tree view as shown below.

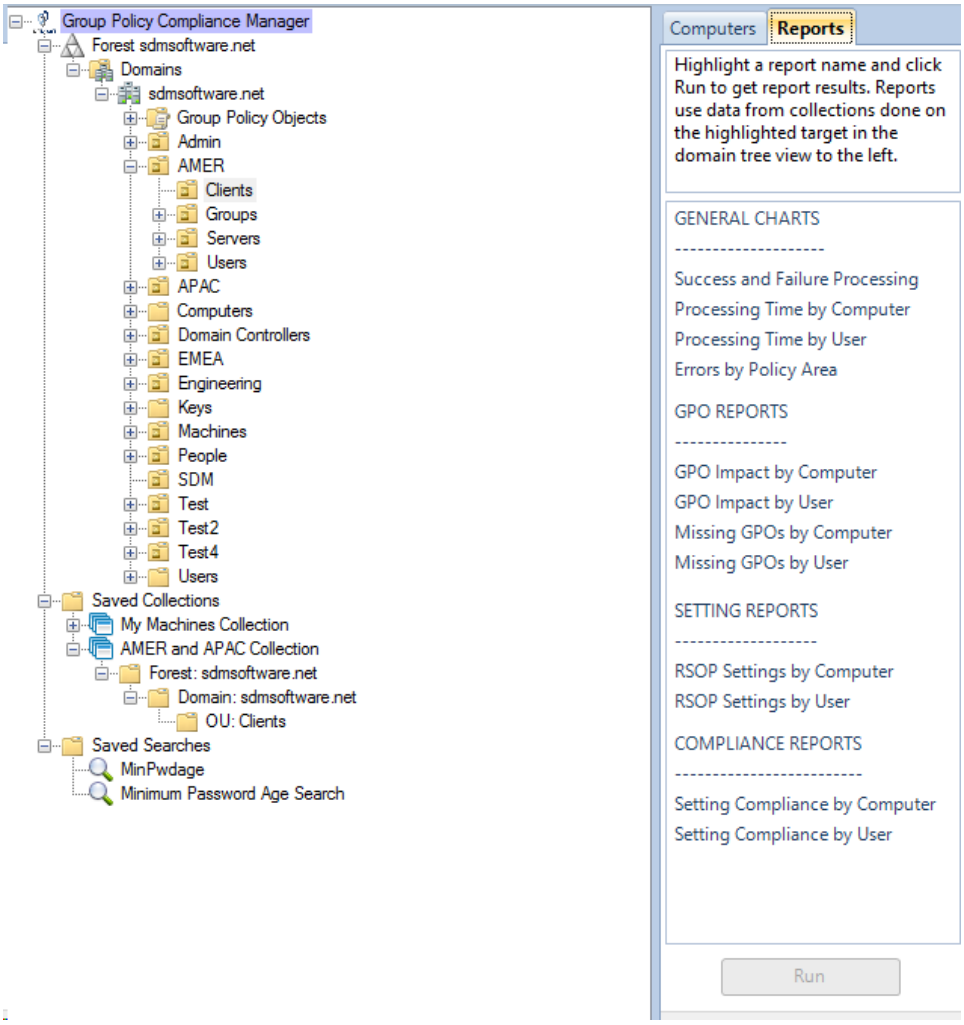


Figure 11 Viewing available reports

In general, you will choose a report name and press the “Run” button to initiate the report generation. Each report is defined here:

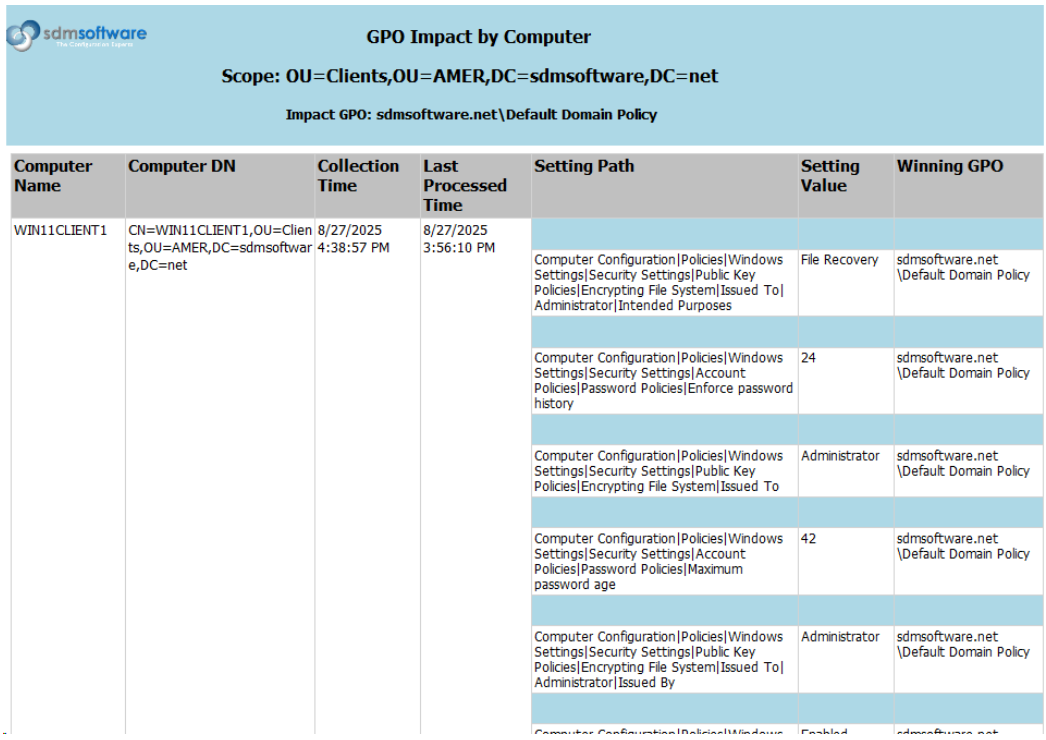
Processing Success and Failure: Presents a graph that reflects the number of computers or users that registered an overall GP processing status of success or failure, for the entire domain, OU, or container that is highlighted. When a "Collect Now" is done on a target, it returns a Success or Fail status for the most recent GP processing cycle it collects on. This graph reports on the ratio of Successes to Failures, for the last collection done for each computer in the target.

Processing Time for User: Displays the top 10 users with slow GP processing. Processing times from the last 10 GP processing cycles (or the highest number of collections up to 10 that have been completed) are averaged, for every user within the domain, OU, or container that is highlighted in the left-hand navigation tree. Then the 10 slowest user results are displayed in the report, along with the average processing times. If there is a user with much slower processing times than other users, it could be that their login times are slow.

Processing Time for Computers: Displays the top 10 computers with slow GP processing, similar to the Processing Times for User report.

Errors by Policy Area: Displays a count of errors that have been reported by Client Side Extensions (CSEs) as collected by GPCM. The count is of errors generated during the last processing cycle for all computers and users within the selected target.

GPO Impact by Computer: This report is designed to show what computers will be impacted if you make a change to a selected GPO. This report uses the latest collection for each GPO in the report results. The first step will be to select a GPO and once selected the report will return all computers that processed a setting from that GPO, along with the setting paths and values, as shown here:



sdmsoftware

GPO Impact by Computer

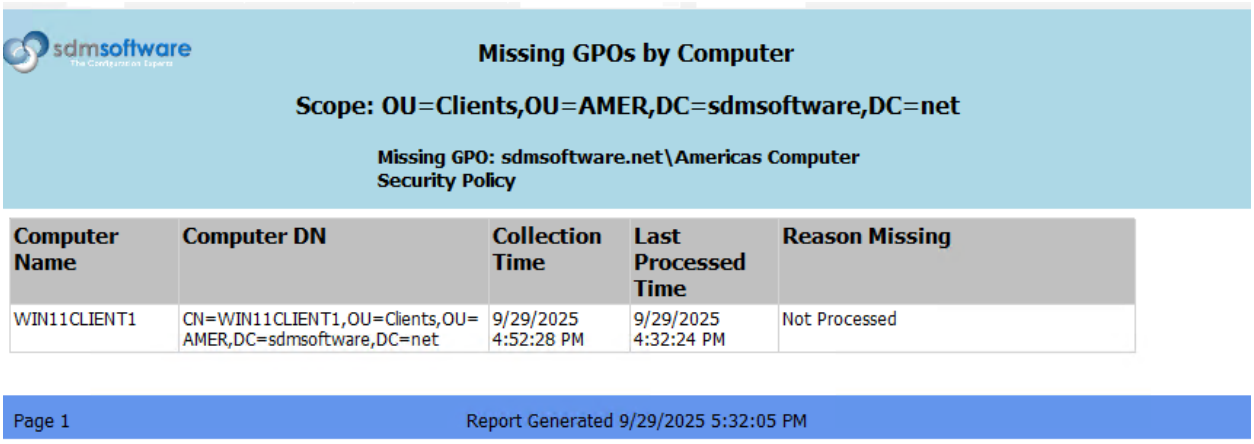
Scope: OU=Clients,OU=AMER,DC=sdmsoftware,DC=net

Impact GPO: sdmsoftware.net\Default Domain Policy

Computer Name	Computer DN	Collection Time	Last Processed Time	Setting Path	Setting Value	Winning GPO
WIN11CLIENT1	CN=WIN11CLIENT1,OU=Clients,OU=AMER,DC=sdmsoftware,DC=net	8/27/2025 4:38:57 PM	8/27/2025 3:56:10 PM			
				Computer Configuration|Policies|Windows Settings|Security Settings|Public Key Policies|Encrypting File System|Issued To|Administrator|Intended Purposes	File Recovery	sdmsoftware.net\Default Domain Policy
				Computer Configuration|Policies|Windows Settings|Security Settings|Account Policies|Password Policies|Enforce password history	24	sdmsoftware.net\Default Domain Policy
				Computer Configuration|Policies|Windows Settings|Security Settings|Public Key Policies|Encrypting File System|Issued To	Administrator	sdmsoftware.net\Default Domain Policy
				Computer Configuration|Policies|Windows Settings|Security Settings|Account Policies|Password Policies|Maximum password age	42	sdmsoftware.net\Default Domain Policy
				Computer Configuration|Policies|Windows Settings|Security Settings|Public Key Policies|Encrypting File System|Issued To|Administrator|Issued By	Administrator	sdmsoftware.net\Default Domain Policy
				Computer Configuration|Policies|Windows	Enabled	sdmsoftware.net

GPO Impact by User: This report does the same thing as the Impact by Computer report, except for users who were logged into computers within the select AD container structure when the last collection occurred.

Missing GPOs by Computer: This report is designed to show computers that have not processed a selected GPO, and the reason they haven't (e.g. out-of-scope, security filtering, WMI filtering, etc.), as shown in the report below. You can think of this report as the opposite of the GPO Impact reports above. You'll be prompted to a select a GPO and then the report will run. As with all reports, this report uses the last collection for each machine reported on:



sdmsoftware

Missing GPOs by Computer

Scope: OU=Clients,OU=AMER,DC=sdmsoftware,DC=net

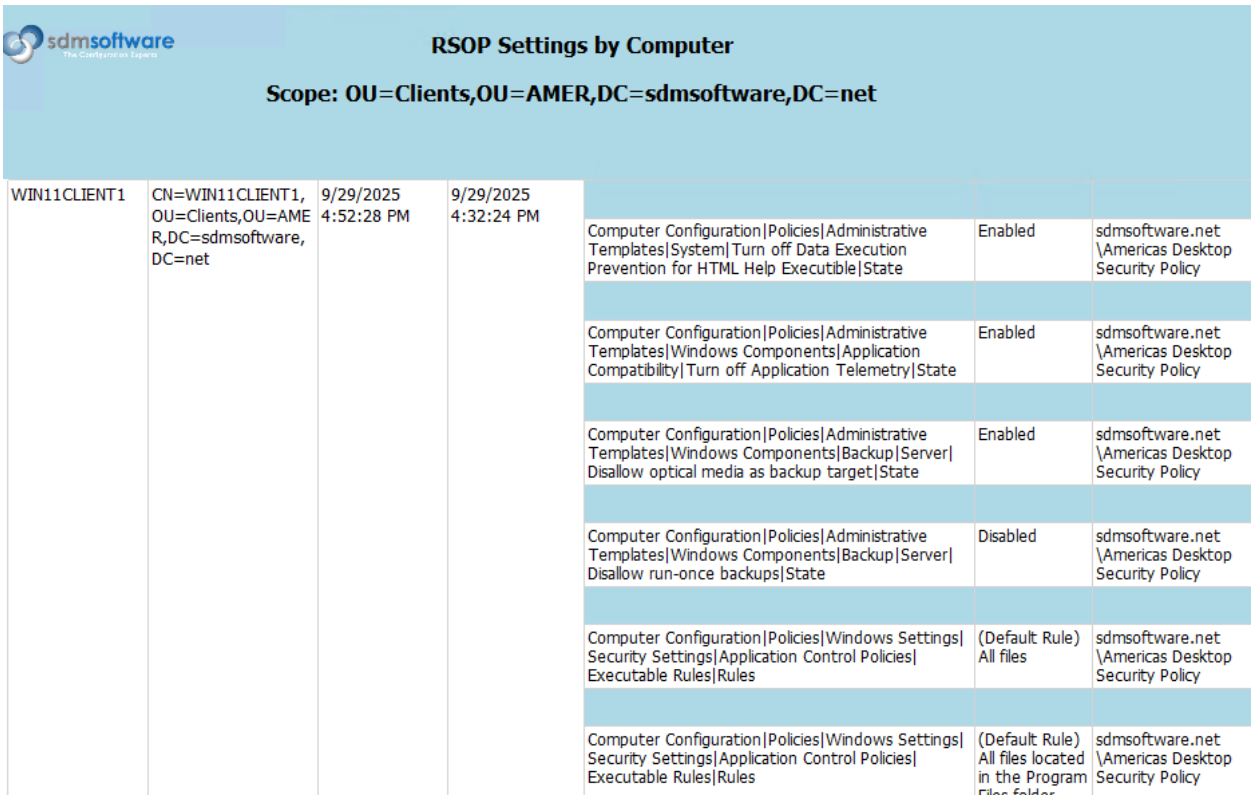
Missing GPO: sdmsoftware.net\Americas Computer Security Policy

Computer Name	Computer DN	Collection Time	Last Processed Time	Reason Missing
WIN11CLIENT1	CN=WIN11CLIENT1,OU=Clients,OU=AMER,DC=sdmsoftware,DC=net	9/29/2025 4:52:28 PM	9/29/2025 4:32:24 PM	Not Processed

Page 1 Report Generated 9/29/2025 5:32:05 PM

Missing GPOs by User: This report does the same thing as the Missing GPOs by Computer report, except for users who were logged into the computers within the select AD container structure when the last collection occurred.

RSOP Settings by Computer: This report lists the actual GPO settings that have been processed by the computer, as defined within the latest collection performed on the computer. You can think of this as a "settings inventory" report for the selected machines you're focused on, as shown here:



RSOP Settings by Computer

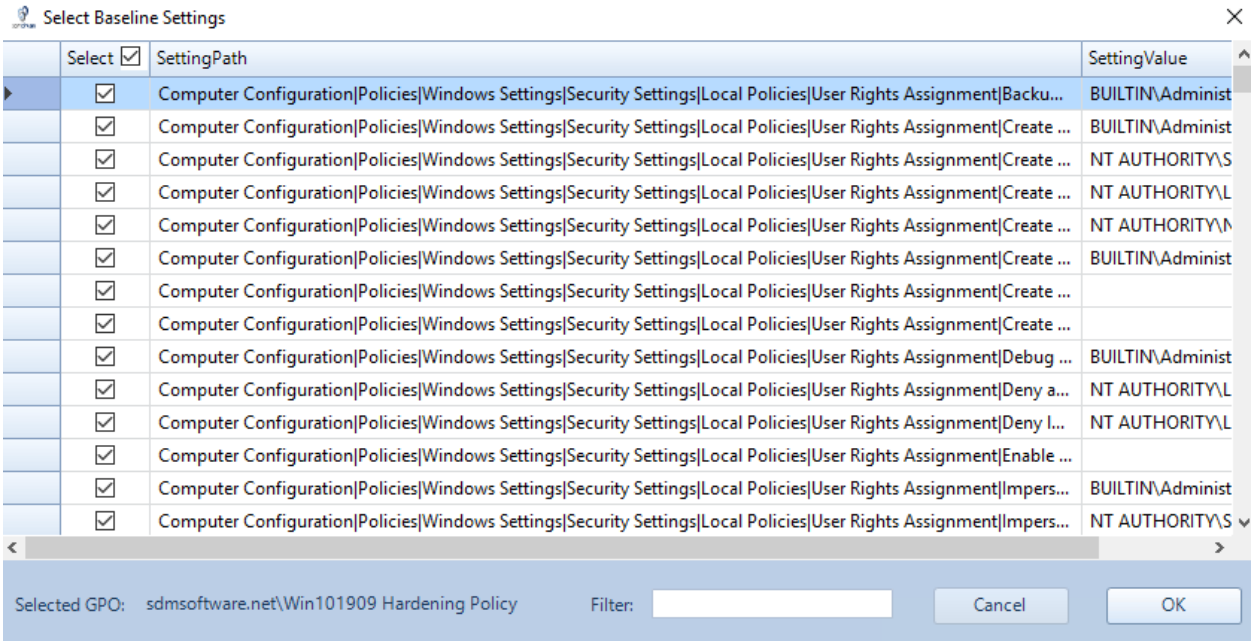
Scope: OU=Clients,OU=AMER,DC=sdmsoftware,DC=net

WIN11CLIENT1	CN=WIN11CLIENT1, OU=Clients,OU=AMER,DC=sdmsoftware, DC=net	9/29/2025 4:52:28 PM	9/29/2025 4:32:24 PM			
				Computer Configuration|Policies|Administrative Templates|System|Turn off Data Execution Prevention for HTML Help Executible|State	Enabled	sdmsoftware.net \Americas Desktop Security Policy
				Computer Configuration|Policies|Administrative Templates|Windows Components|Application Compatibility|Turn off Application Telemetry|State	Enabled	sdmsoftware.net \Americas Desktop Security Policy
				Computer Configuration|Policies|Administrative Templates|Windows Components|Backup|Server|Disallow optical media as backup target|State	Enabled	sdmsoftware.net \Americas Desktop Security Policy
				Computer Configuration|Policies|Administrative Templates|Windows Components|Backup|Server|Disallow run-once backups|State	Disabled	sdmsoftware.net \Americas Desktop Security Policy
				Computer Configuration|Policies|Windows Settings|Security Settings|Application Control Policies|Executable Rules|Rules	(Default Rule) All files	sdmsoftware.net \Americas Desktop Security Policy
				Computer Configuration|Policies|Windows Settings|Security Settings|Application Control Policies|Executable Rules|Rules	(Default Rule) All files located in the Program	sdmsoftware.net \Americas Desktop Security Policy

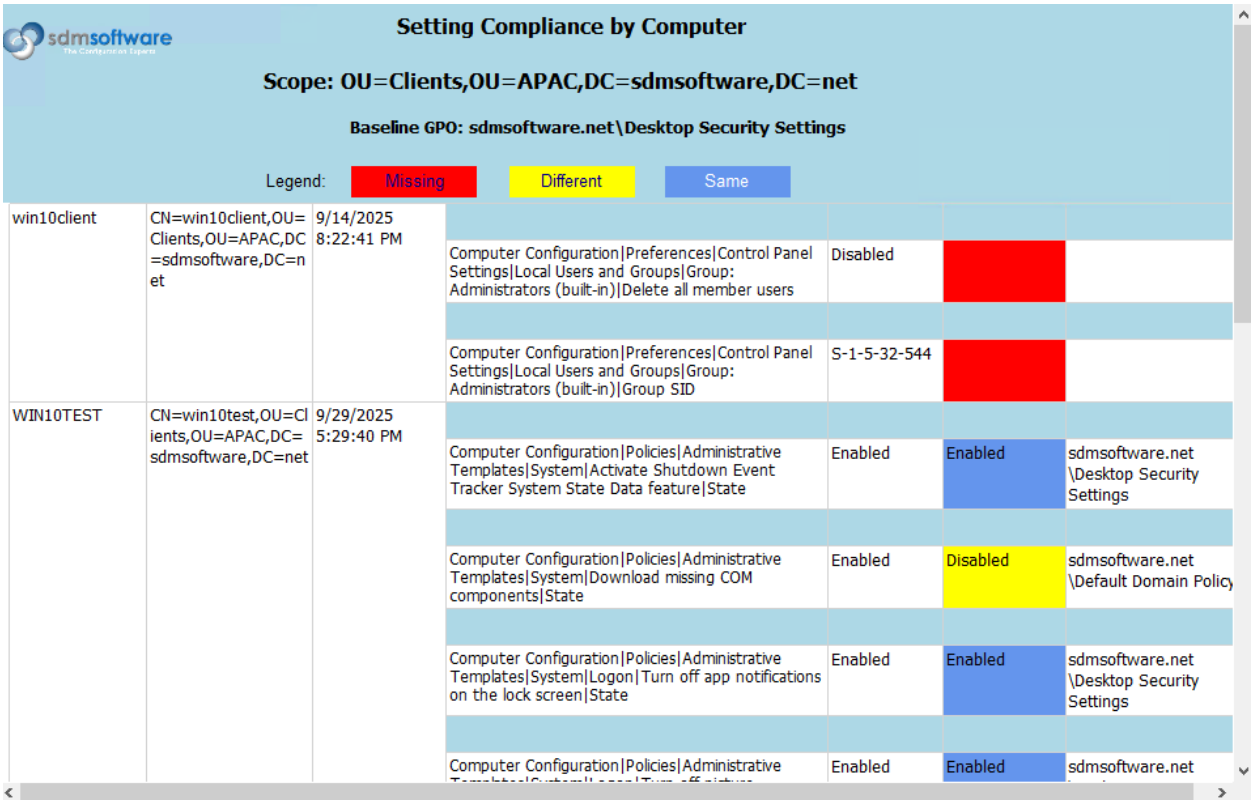
This report tends to be long since it's listing every setting for every computer within the selected scope.

RSOP Settings by User: As before, this reports on the settings received by the user who was logged into the computers within the select AD container structure when the last collection occurred. Note that it will only report on the last user who logged in.

Settings Compliance by Computer: This report is designed to allow you to see if there are specific settings that have not been received by selected computers. You will first select a GPO containing the settings you want to test for. Then you will receive a dialog that allows you to select one or more settings from the selected GPO, as shown here:



You can select individual settings, filter the list based on keywords, or press the “select” checkbox in the upper left to select all settings within the GPO. Once you press OK, the selected settings are compared against the latest collection for the computer in the selected container, and a report is generated, as shown here:



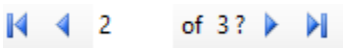
Note that the report is collect coded to show the differences between setting values in the selected GPO, and what was actually processed by the computer.

Setting Compliance by User: As before, this reports on the differences between the selected baseline GPO settings and the settings processed by the user who was logged into the computers within the select AD container structure when the last collection occurred. Note that it will only report on the last user who logged in.

Reporting Options

You will note that all reports contain the same tool bar at the top of the report, as shown here:

This toolbar provides several options for viewing and exporting your report, described from left to right here:



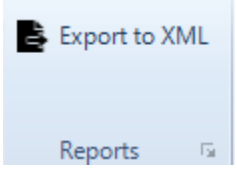
Page Navigation: The page navigation controls let you navigate forward or backward in the report, page by page, to the beginning or end, or by specifically entering a page number.

Output Options: The first control lets you refresh the report, though in this context it will not regenerate. The second control let's you print the report. The third control lets you change the print layout from portrait to landscape. The fourth control lets you control the page setup for how the report will be printed. Finally, the disc save icon lets you output the report to Excel, PDF or Word.

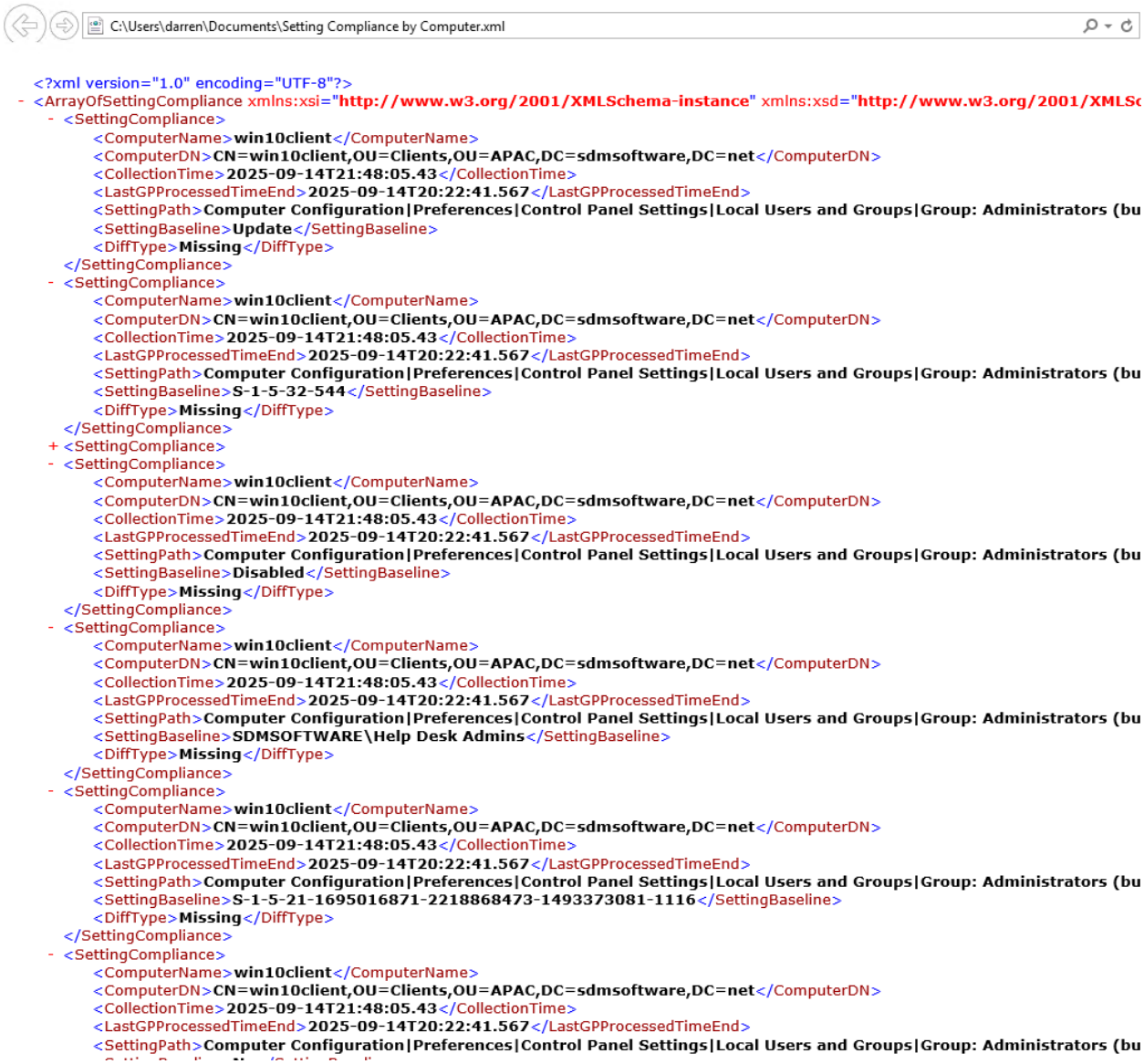
Zoom and Search: The first of these two controls lets you zoom the view of the report as it's displayed in the UI—defaulting to 100%. The second control lets you perform a text search within the contents of the report. Type full or partial text that you wish to search for and press the Find button. To find the next instance of the text, press Next.

Output to XML

You have another option for outputting each of the textual reports. Namely, you can output any of those to XML by choosing the **Export to XML** option from the toolbar's Reports menu at the top of the UI, as shown here:



When you export to XML the contents of the report are written in an XML format as shown here:



Each type of report is represented using a different schema, depending on the nature of the report data. This report above is from a Settings Compliance report, for example.

Appendix A: GPCM PowerShell Module

GPCM comes with a PowerShell module that provides command-line options for performing various tasks within the product. The module is installed using a separate MSI installer and can be installed on any machine that has access to the GPCM database. In general, the module cmdlets connect directly to the GPCM database and therefore require both network and security access to the database. The user who is running the cmdlets will need to have permissions to read (and write, depending upon the cmdlet) to the GPCM database. The available cmdlets are listed here:

Compare-SDMSettingBaseline: Allows you to compare and find differences betweeen Group Policy setting baselines and settings that have been processed by computers and users. Supports using individual settings and values, live GPOs or SDM Software GPO Reporting Pak snapshot files as baselines.

Get-SDMComputer: Returns information about computers that have been collected against in SDM Software Group Policy Compliance Manager, including machine details and collections performed against a computer.

Get-SDMGPTiming: This cmdlet takes either a computer name or username and returns the GP processing times of GPCM collections that have been performed.

Get-SDMUser: Returns information about users that have been collected against in SDM Software Group Policy Compliance Manager, including machine details and collections performed against a computer.

Invoke-SDMGPCMCollection: Allows you to perform remote collections against computers using PowerShell.

Search-SDMSetting: This cmdlet allows you to search for particular GPO settings, or their values, within the GPCM database. The search can be scope to the entire domain or, using the -Scope parameter, for a particular OU. It can also preferentially return only per-user or per-computer results, in the event that a particular search parameter is contained within both sides.

Show-SDMGPOImpact: This cmdlet provides a way to determine where a given GPO has been applied to users or computers, to determine potential impact if the GPO is changed.

Test-SDMGPO: This cmdlet tests whether a particular GPO was processed by a given computer or user and if it wasn't, why it wasn't. It's a variation of Show-SDMGPOImpact, but does not return the settings processed by the computer or user, as the Show-SDMGPOImpact cmdlet does.

Some things to keep in mind about the cmdlets:

- The **UseSQL** parameter should be used in all cases to specify the SQL Server name/Instance where the GPCM database resides. The cmdlets assume the database name is **GPCM** (the default).
- The user that runs the cmdlets need to have read access to the GPCM database. If you are using the Invoke-SDMGPCMCollection cmdlet, then that user will also need write access to the database.

- When specifying a GPO name, the format should always be: <DNS Domain Name\GPO Name>, as in "*mycompany.com**Default Domain Policy".*