Sentinel Security Pack
for Microsoft System Center
Operations Manager

Sentinel Security Pack

Deployment Guide

Release 1.2
September 2018

Disclaimer
The information in this document is furnished for informational use only, and is subject to change without notice. Silect Software, Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Contents

Preface

About the Sentinel Security Pack Deployment Guide

The Sentinel Security Pack Deployment Guide describes how to install and configure the Sentinel Security Pack for use with Microsoft System Center Operations Manager. It contains the following sections:

Audience

This document is intended for the following users of the Sentinel Security Pack:

- Administrators
- Operators
- Maintenance Personnel

Familiarity with general use of the Operations Manager console and some basic Operations Manager terminology is assumed.

Document Conventions

This document uses **bold** to identify the following:

- Commands that have to be clicked on
- Section names, window names and prompts as they appear on the screen
- File names

Italics are used the first time a new important term is introduced.

Wherever **Operations Manager** is mentioned in this document without referring to any particular version, it can be assumed that the subject being discussed applies equally across all versions of Operations Manager supported by the Sentinel Security Pack.

Microsoft System Center Operations Manager is abbreviated in this document as **OpsMgr**.

Microsoft SQL Server Reporting Services is abbreviated in this document as **SSRS**.

Management Pack is abbreviated in this document as **MP**.

Overview of the Sentinel Security Pack

About the Sentinel Security Pack

The Sentinel Security Pack by Silect Software, Inc. is a Management Pack (MP) intended to be used with Microsoft System Center Operations Manager (OpsMgr) 2012 or newer. Its purpose is to gather configuration information from Windows computers that are being monitored by OpsMgr and report whether those computers are compliant with a number of *safeguards* defined by the Sentinel Security Pack, and if not, provide an administrator with simple methods to run *remediation* scripts to bring those computers into compliance where feasible (Sentinel Pro version only).

The Management Pack is delivered as two files; one with the .MPB extension containing most of the definitions; and a second with the .XML extension containing groups and overrides.

A working OpsMgr 2012 or newer environment is required to use the Sentinel Security Pack. Installation and configuration of OpsMgr itself is beyond the scope of this guide; for help on this topic, refer to the documentation for your specific version of OpsMgr.

Discovery

Discovery is performed against Windows computers—workstation and server versions alike—when the Security Pack is imported; subsequent discoveries take place every 24 hours at 5:00am. To avoid an alert storm, which could be created by reporting the compliance issues with every single Windows computer in your installation, discovery is limited to computers (and groups) added to the **Silect Sentinel Computers To Monitor Group** group. No computers will be monitored for compliance until they are added to

this group (or a group containing those computers, such as **All Windows Computers**, is added to the group).

Installation and Configuration

Prerequisites

This section enumerates the versions of System Center Operations Manager supported by the Sentinel Security Pack, as well as the versions of Windows required by the computers being monitored, and the languages supported.

Supported versions of System Center Operations Manager

The Sentinel Security Pack supports all versions of OpsMgr, from 2012 through 1807, with and without their respective service packs and update rollups. OpsMgr 2007 or 2007 R2 are not supported.

The Sentinel Security Pack includes a number of custom reports specifically designed to show summarized as well as detailed views of the information it gathers. The use of these reports is optional; to make use of them, it is necessary to have a functional instance of SQL Server Reporting Services (SSRS). Without SSRS, the reports cannot be viewed, but you can still use some of the views built into the OpsMgr console to access some of the data in its raw form. One of the benefits of using the custom reports, over the views built into the OpsMgr console, is that the reports focus solely on the compliance data retrieved by the Management Pack, and you do not have to set any filter to hide data that comes from the other Management Packs you may be using. You can also print these reports and export them to PDF files and other formats.

Supported Operating Systems

The computers being monitored by OpsMgr must run one of the following operating systems for the Sentinel Security Pack to correctly gather all compliance information:

Microsoft Windows version	Supported Releases

Client releases	Windows Vista Windows 7 Windows 8 Windows 8.1 Windows 10
Server releases	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016

Note that computers running recent operating system versions may require one of the Update Rollups for OpsMgr's agent to function correctly. Refer to the documentation for your version of OpsMgr for details.

PowerShell 2.0 must be present and enabled on the computers being monitored by OpsMgr for the Sentinel Security Pack to correctly gather its information.

Supported Languages

The Sentinel Security Pack supports US English only. While the OpsMgr agent should work on computers that are running versions of Windows using different languages, all information gathered by the Management Pack and all reports it displays are in US English only.

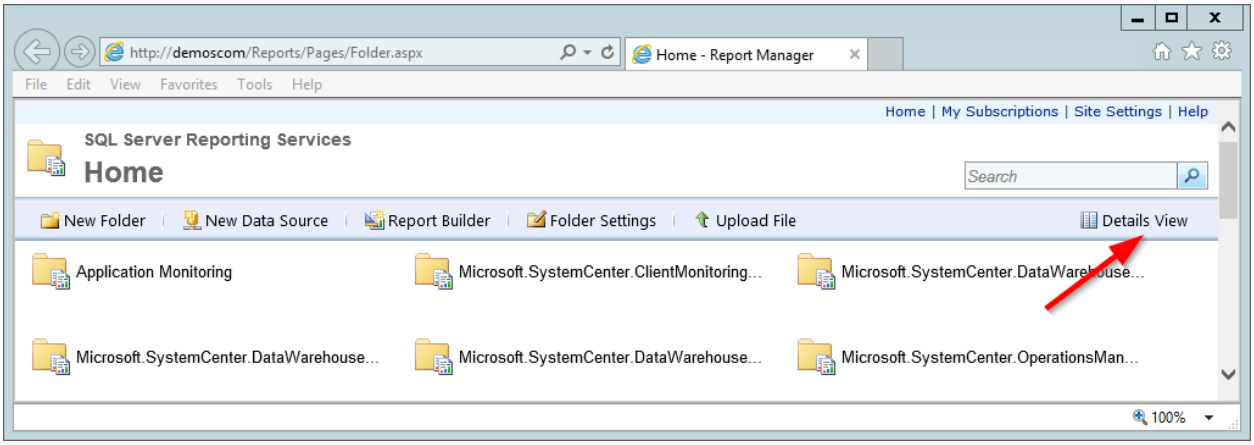
Installing the Management Pack

As described in the Prerequisites section, the Sentinel Security Pack includes a number of custom reports that can be used to view the detailed information it gathers. While the use of these reports is optional, if they are going to be used, then your instance of SQL Server Reporting Services (SSRS) must be configured *before* importing the Management Pack itself into OpsMgr.

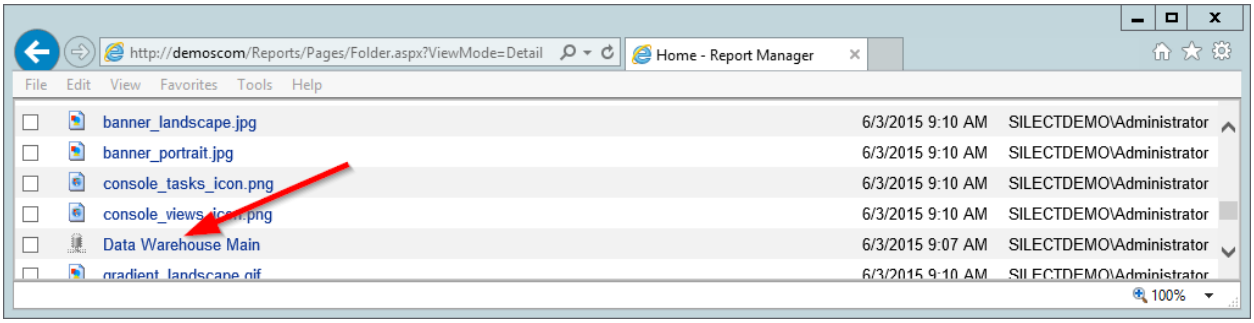
Configuring SQL Server Reporting Services

To use the Sentinel Security Pack custom reports, follow these steps. You can skip this section and go directly to the Importing the Management Pack into Operations Manager section if you do not intend to use the custom reports.

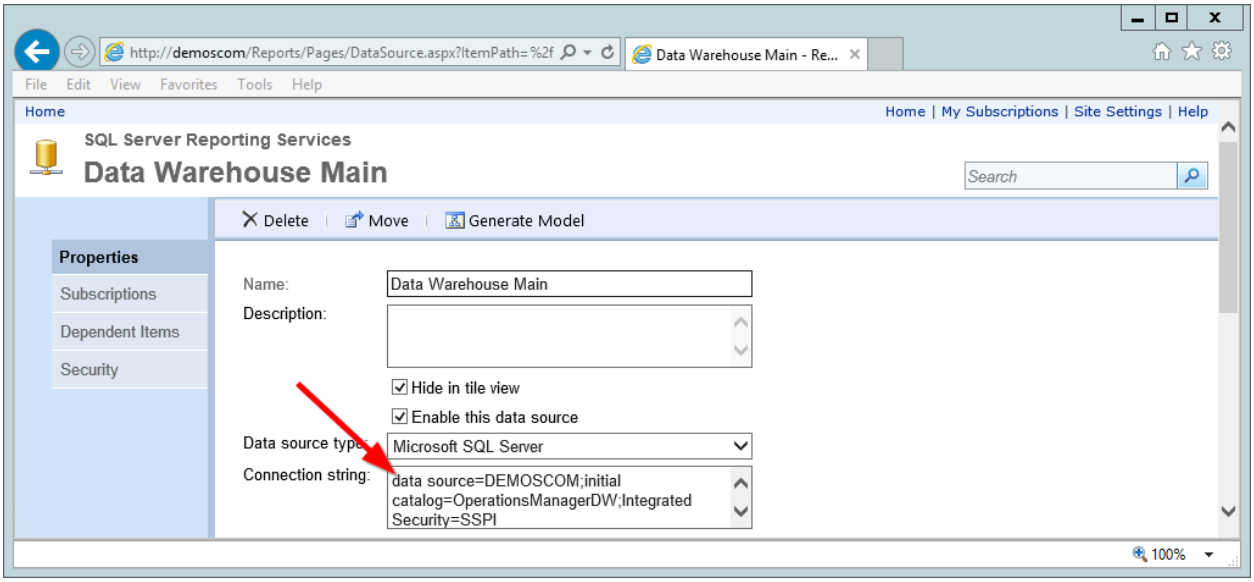
- Step 1: Using the web browser of your choice, go to http://YourServerNameHere/Reports, where "YourServerNameHere" is the name of your SSRS server. Your browser should be redirected to http://YourServerNameHere/Reports/Pages/Folder.aspx.
- Step 2: Click on **Details View**, in the top-right corner



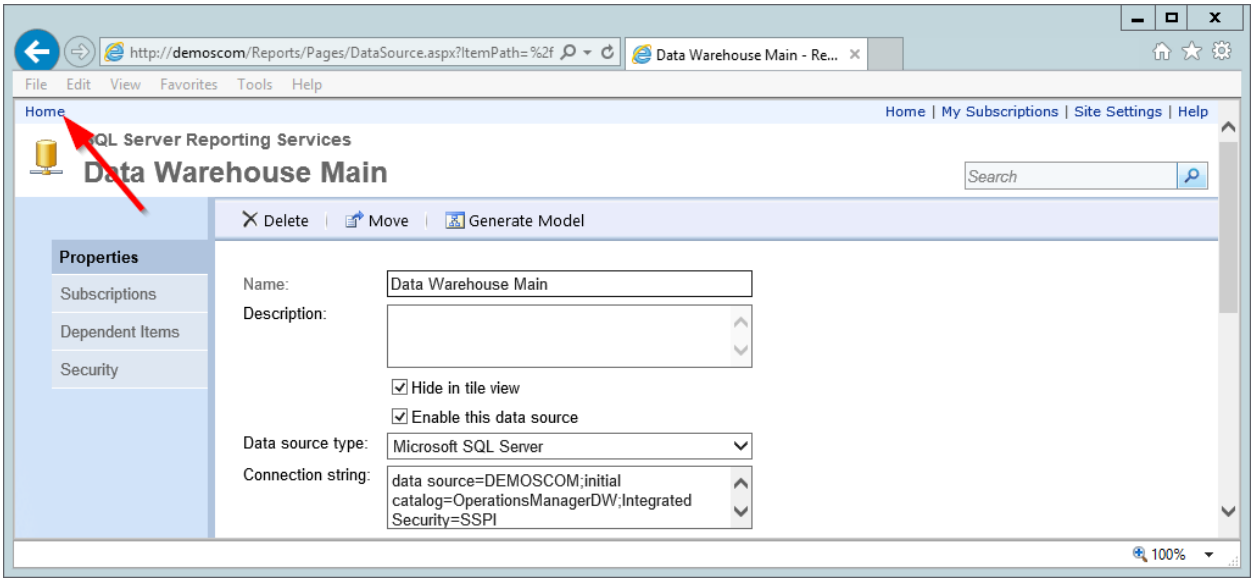
- Step 3: You need a database connection string to connect to your main OpsMgr database. If you don't know what connection string is used by your main OpsMgr database, follow steps 3a through 3c. While these steps show how to obtain the connection string to your OpsMgr *data warehouse* database, the connection string for your main OpsMgr database should be very similar, so using the connection string for your OpsMgr data warehouse database is a good starting point. Step 7 will show you exactly how to further edit the connection string to connect to the correct database.
    - Step 3a: Locate the **Data Warehouse Main** entry in the list.



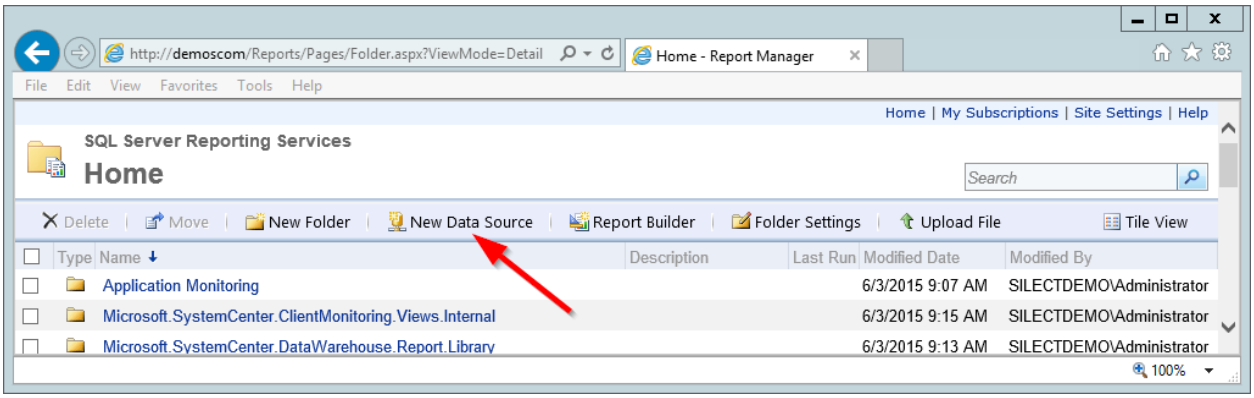
- Step 3b: Click on the **Data Warehouse Main** entry. A new page will load, showing you the details of an existing data source for your OpsMgr *data warehouse* database, including its connection string. Make a note of it – for example, copy it to the clipboard by highlighting all the text in the **Connection string** box and pressing **Ctrl-C**.



- Step 3c: Once you have the connection string, click **Home**, in the upper-left corner, to return to SSRS's main reports page



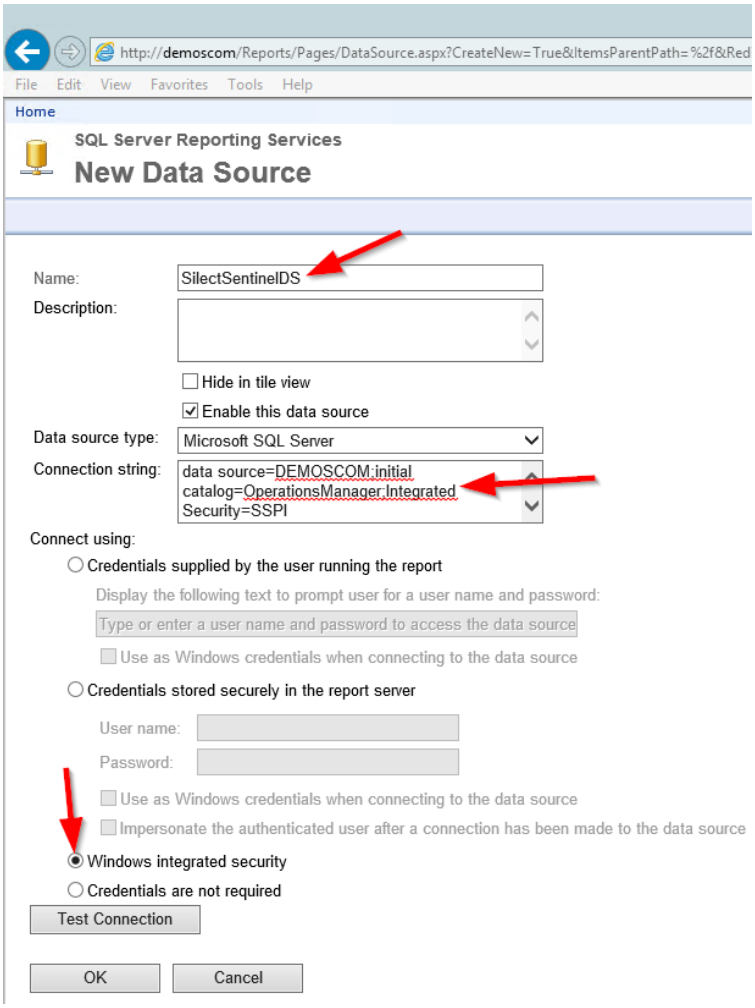
- Step 4: Once you have the connection string for your OpsMgr data warehouse database, click on **New Data Source**, near the middle of the toolbar at the top of the page. This will load a new page that looks similar to the one seen during Step 3b:



- Step 5: Type in "**SilectSentinelDS**" in the **Name** box (without the quotes).
  - **NOTE**: It's important to type this name *exactly* as it shown above.
- Step 6: Add the data warehouse connection string in the **Connection string** box, either by typing it in, or by pasting the value that was copied to the clipboard during step 3b.
- Step 7: IMPORTANT – As described during Step 3, this is the connection string for your OpsMgr *data warehouse* database, which is not the same as your *main* OpsMgr database.

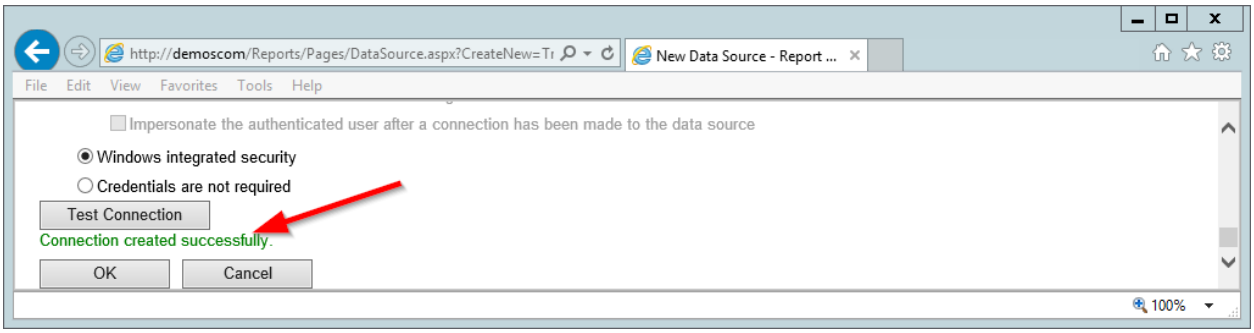
- By default, when OpsMgr is installed, the main database is called **OperationsManager**, and the data warehouse database is called **OperationsManagerDW**. Unless your OpsMgr installation was customized, the value that follows **Initial catalog** should be **OperationsManagerDW**.
    - If this is the case, simply remove the “DW” characters at the end of “OperationsManagerDW”. Generally, this should be the *only* difference between the connection strings for your OpsMgr data warehouse database, and the main database.
    - If the value is different however, consult the person who set up your Operations Manager environment and ask for the name of its database. Replace the value that follows **Initial catalog** with that name.

- Step 8: Once you have the correct database name following the **Initial catalog** section of the **Connection string** box, select **Windows integrated security**, in the **Connect using** section. After steps 5 through 8, the page should now look as follows:



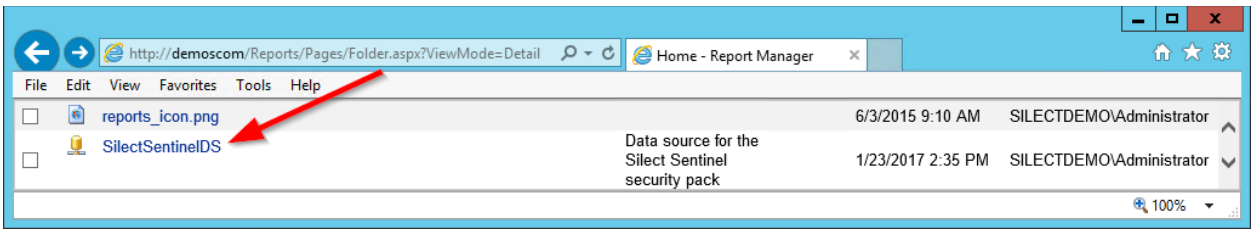
- Note that the value that follows **data source**, in the **Connection string** box, will probably not match the sample above (“DEMOSCOM”). This value is the name of the server running your OpsMgr database. Unless the main database was placed on a server that is different from the one running the data warehouse database, you should not have to change the value that immediately follows **data source**. If your OpsMgr database is running on a different server however, you will have to check with the person who set up your Operations Manager environment and ask for the name of the server. Once you have it, replace the value that follows **data source** with that name.

- Step 9: Click on the **Test Connection** button to verify that the connection has been set up correctly. If so, you should see a green **Connection created successfully** message.



  - If an error is instead reported, the setup of your Operations Manager environment may have been customized, and you will have to consult with the person who set it up. You may have to provide credentials in the **Credentials stored securely in the report server** section of the page, or use one of the other connection methods available on the **New Data Source** page. The person who set up your Operations Manager environment should know how to configure this connection correctly.
  - **If you cannot get past this step, the Management Pack's custom reports *will not work***. You can always revisit this section at a later time however to change the connection string.

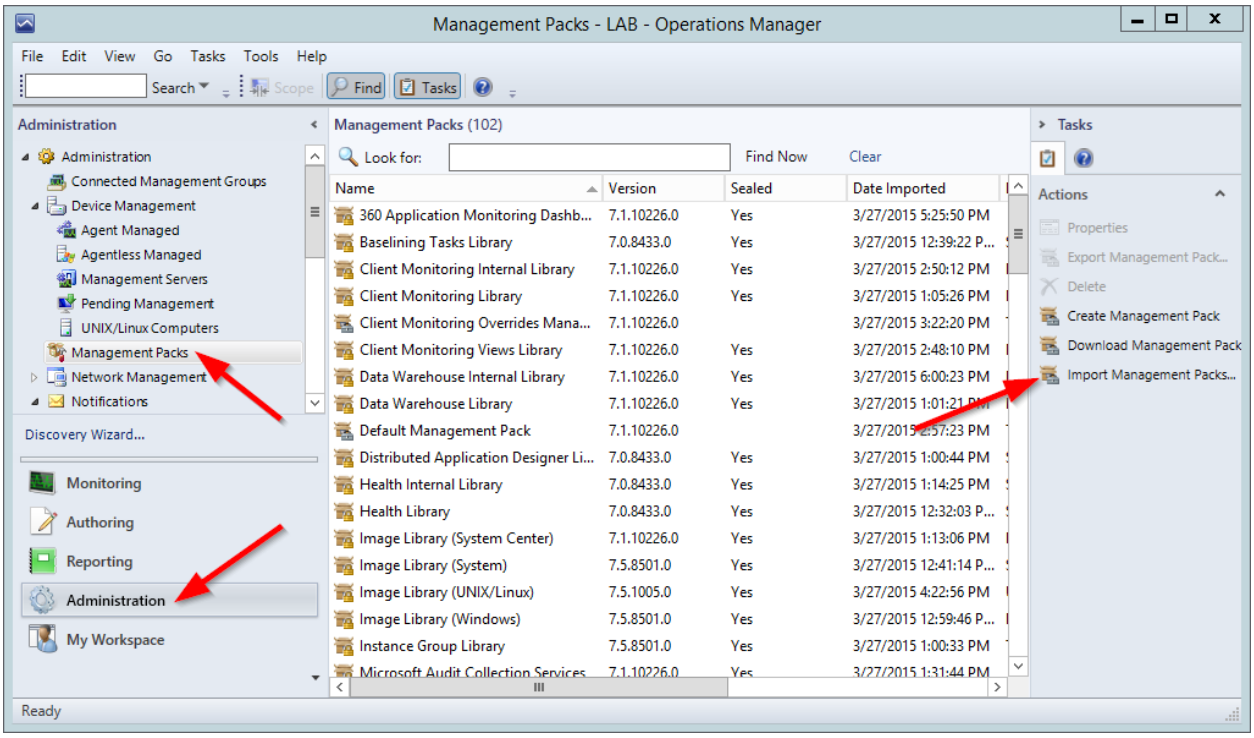
- Step 10: Once you get a green "**Connection created successfully**" message when clicking the **Test Connection** button, click **OK**; you will be returned to the main SSRS page. You should now see the newly created data source that is needed by the custom reports in the Sentinel Security Pack. You can close your web browser.



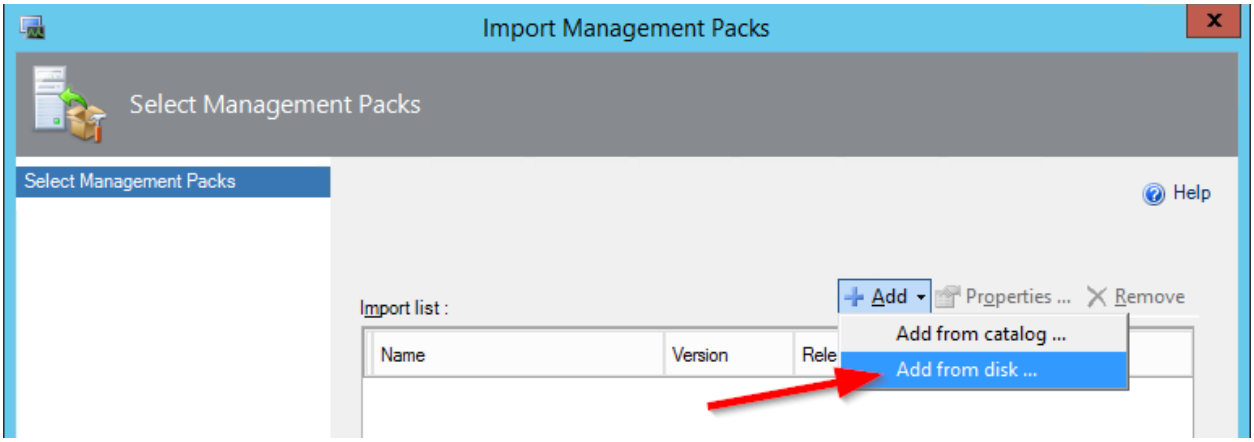
Importing the Management Pack into Operations Manager

To use the Sentinel Security Pack, import it into your OpsMgr environment like you would import any other Management Pack:

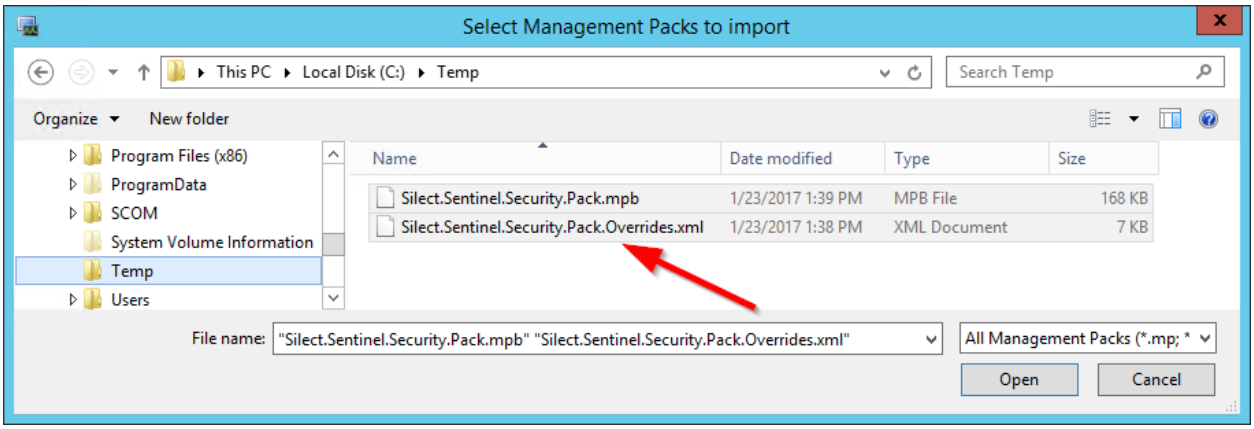
- Step 1: Launch your Operations Manager console. Go to the **Administration** Workspace, click on **Management Packs**, and click **Import Management Packs…** from the **Actions** menu on the right-hand side of the screen



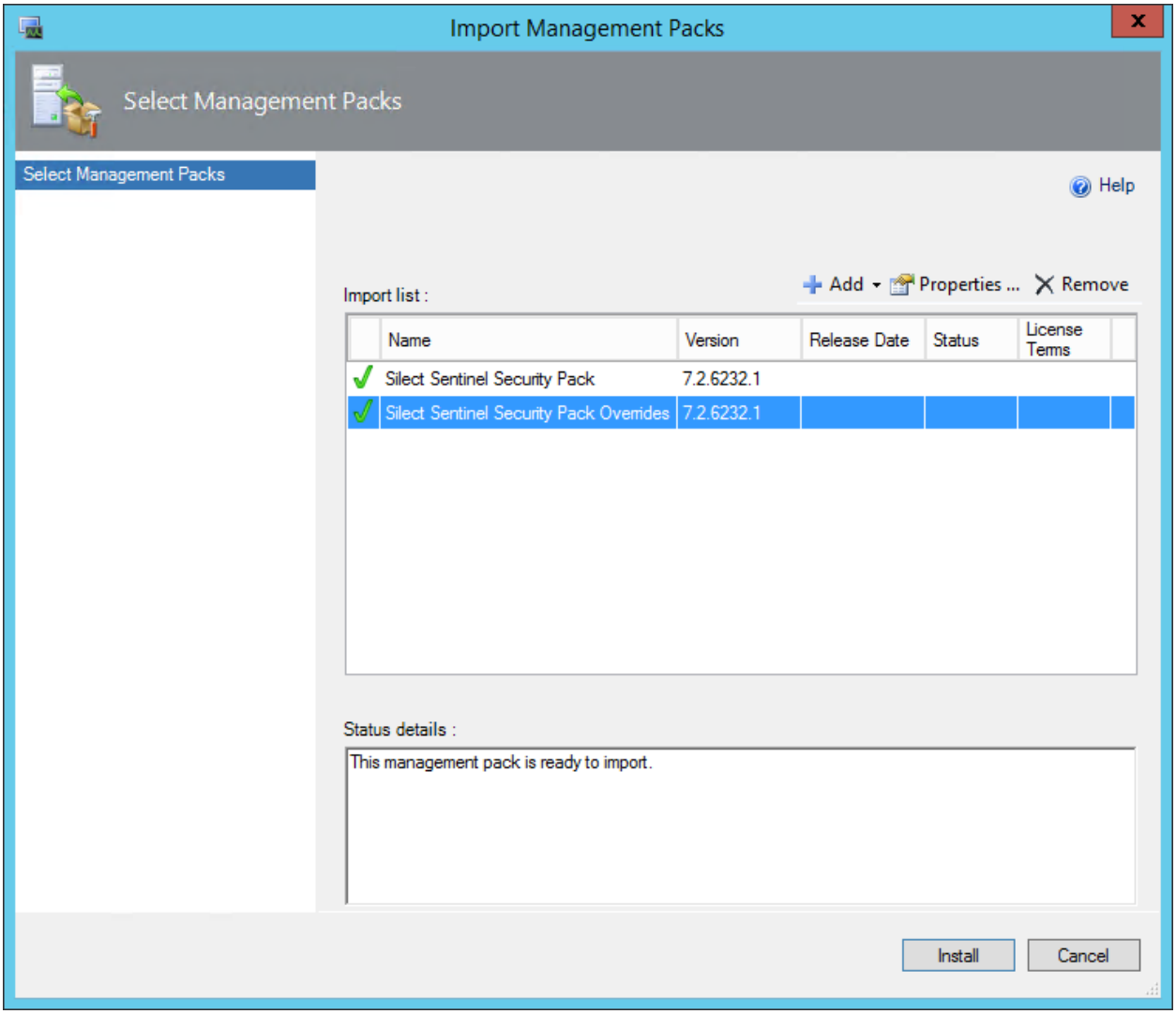
- Step 2: In the **Import Management Packs** wizard, click on **Add**, then **Add from disk…**:



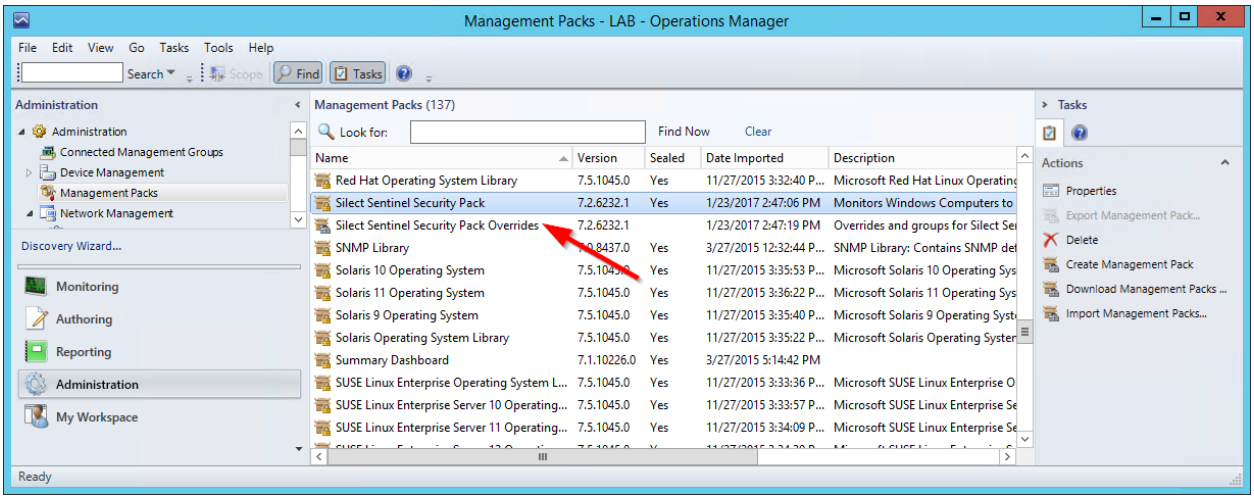
- Step 3: If you're prompted to **search the online catalog for dependencies**, select **No**.
- Step 4: In the **Select Management Packs to import** dialog box, navigate to the location where your copy of the Sentinel Security Pack Management pack is stored. The pack consists of two files. The files are named **Silect.Sentinel.Security.Pack.mpb** and **Silect.Sentinel.Security.Pack.Overrides.xml**. Select the files, and then click on **Open**.



- Step 5: Details of the Management Packs will be displayed before importing them. Click on **Install** to start the import process.



- Step 6: If everything worked correctly, you will see green checkmarks, and the Status section will indicate **Imported** for both MPs. If the import process encountered a failure, the **Import Status Details** section will contain details that should explain why the failure occurred. Make a note of this – if you need to contact technical support, you will need this information.
- Step 7: Click on **Close**. After a few seconds to a few minutes, depending on the performance of your OpsMgr environment, the Management Pack will appear in the list as **Silect Sentinel Security Pack** and **Silect Sentinel Security Pack Overrides**, if Step 6 above completed with a status of **Imported**.



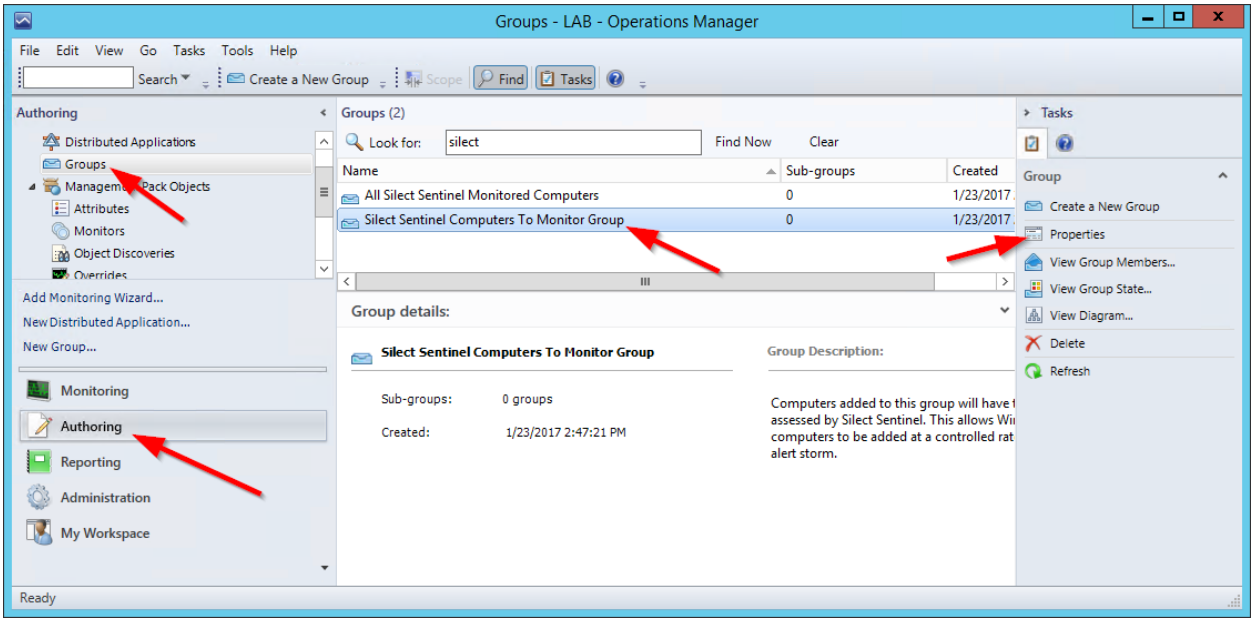
Selecting Computers to Monitor with the Management Pack

By default, the discovery for computers to monitor is disabled, and only enabled for computers that are members of the **Silect Sentinel Computers To Monitor Group** group. Before any computers will be monitored, they need to be added to the group.

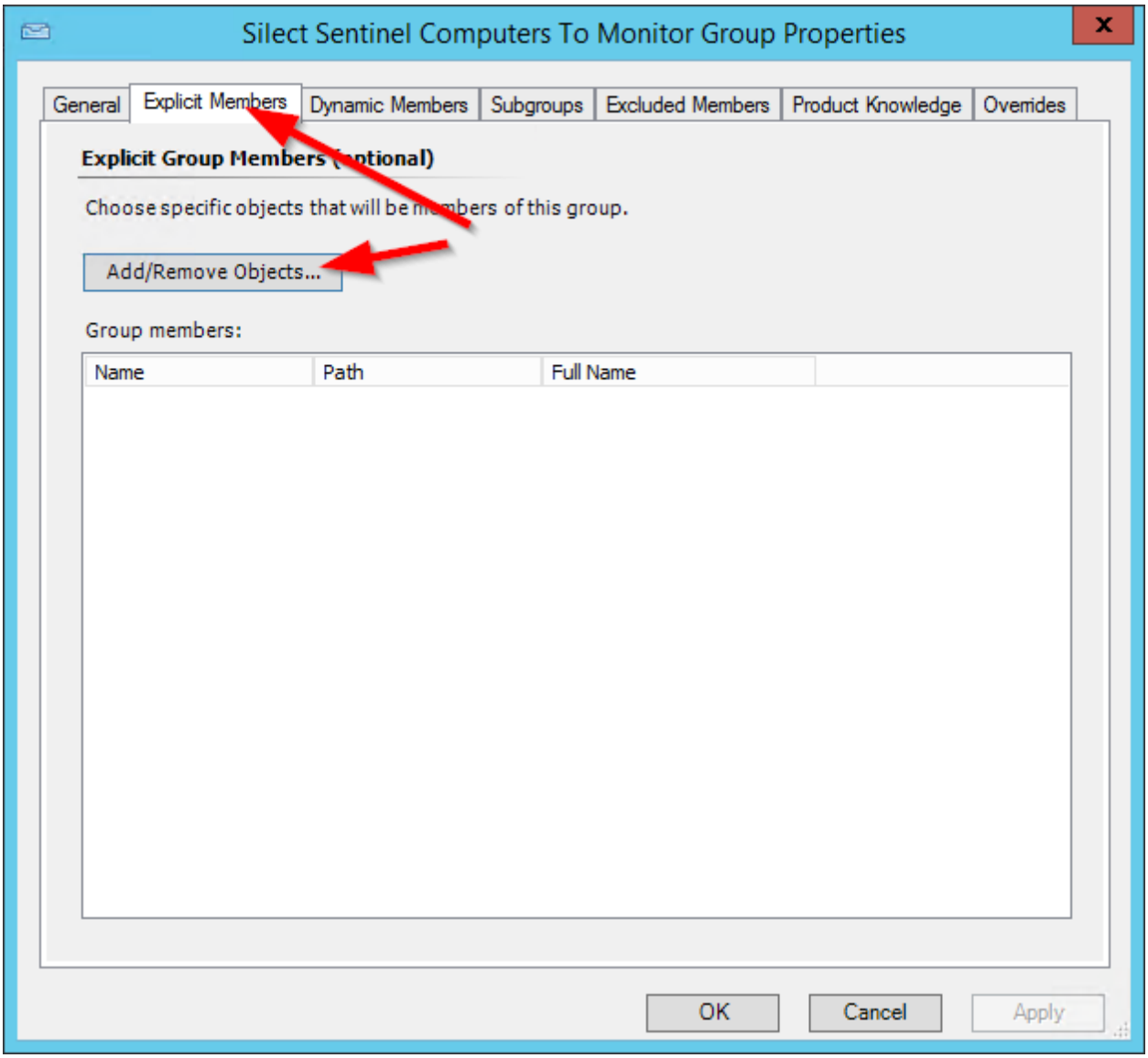
The reason for this behavior is to avoid a sudden *alert storm*, which could occur if all computers were suddenly being monitored. Manually adding computers (and/or groups) allows greater control to ensure that your OpsMgr server does not create a large volume of alerts. Silect recommends adding only one or two computers to this group initially. They may report compliance issues that could be common amongst most computers on your network. This allows you to remediate the common issues before monitoring all systems. If remediation is done with group policies, it will minimize the amount of work needed to bring most systems into compliance. Once your first few test systems are brought into compliance, you can add more computers (or groups like **All Windows Computers**), without fearing a flood of alerts.

To add computers (or groups) to the **Silect Sentinel Computers To Monitor Group**:

- Step 1: Launch your Operations Manager console. Go to the **Authoring** Workspace, click on **Groups**, select **Silect Sentinel Computers To Monitor Group** and click **Properties** from the **Actions** menu on the right-hand side of the screen

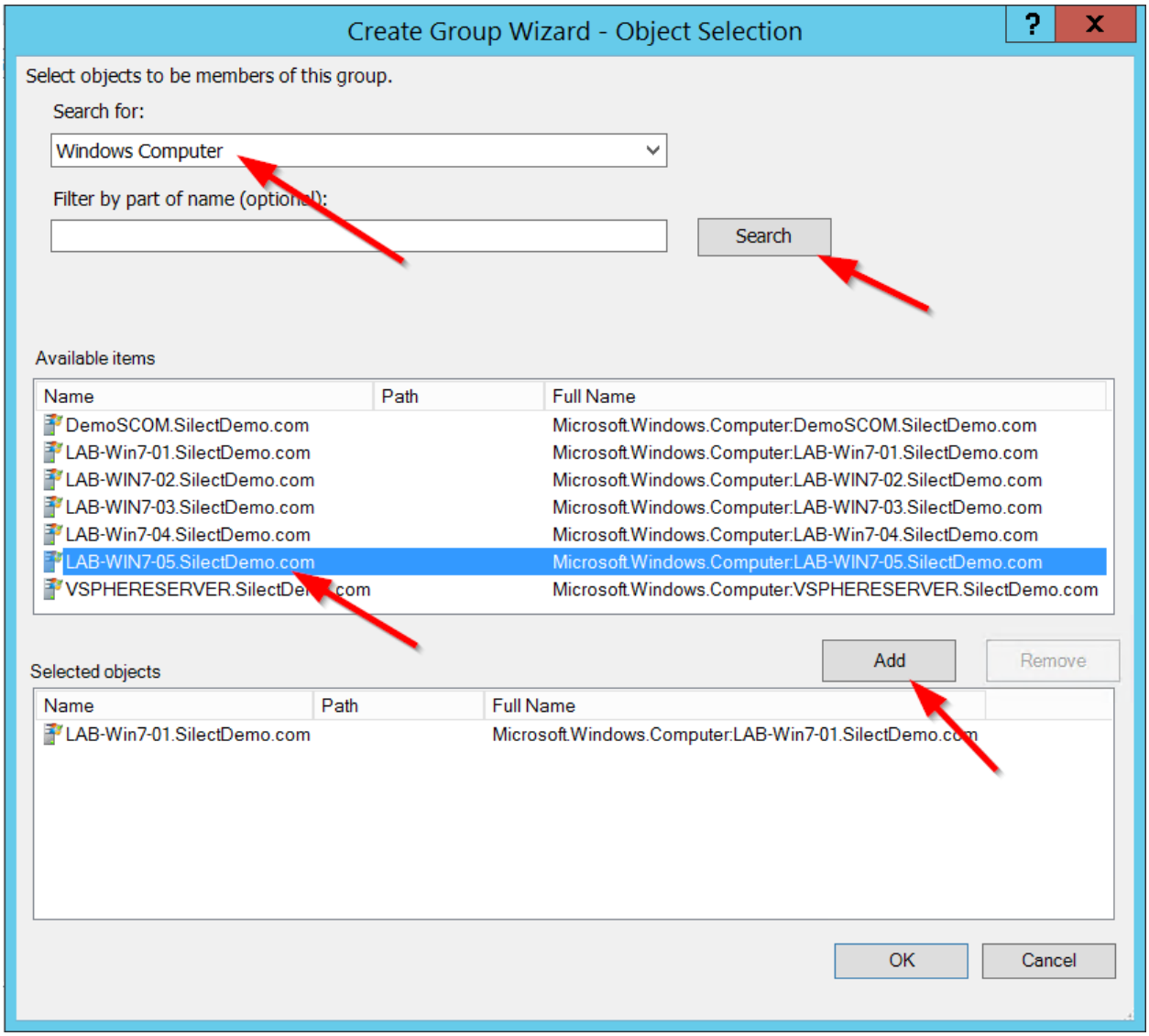


- Step 2: From the **Properties** window, select the **Explicit Members** tab, then click the **Add/Remove Objects** button.



- Step 3: From the **Object Selection** window, choose **Windows Computer** from the **Search for** drown down list, click **Search** to get a list of all Windows computers, select the computers you wish to monitor, and click **Add**. When all

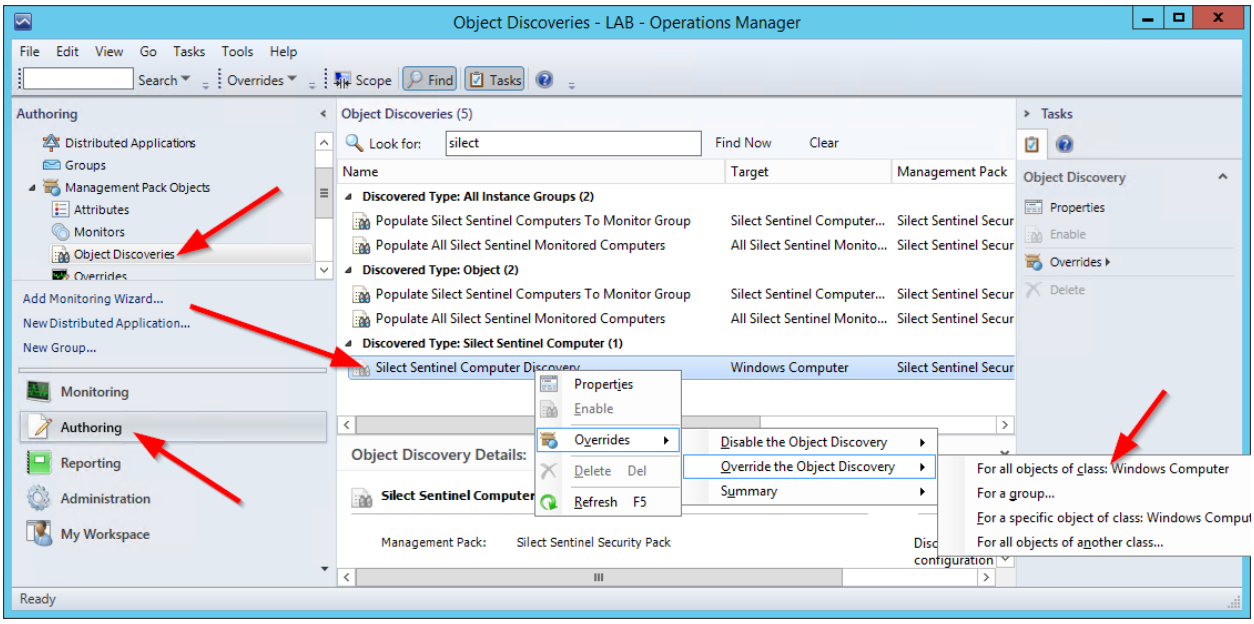
computers are selected, click **OK**.



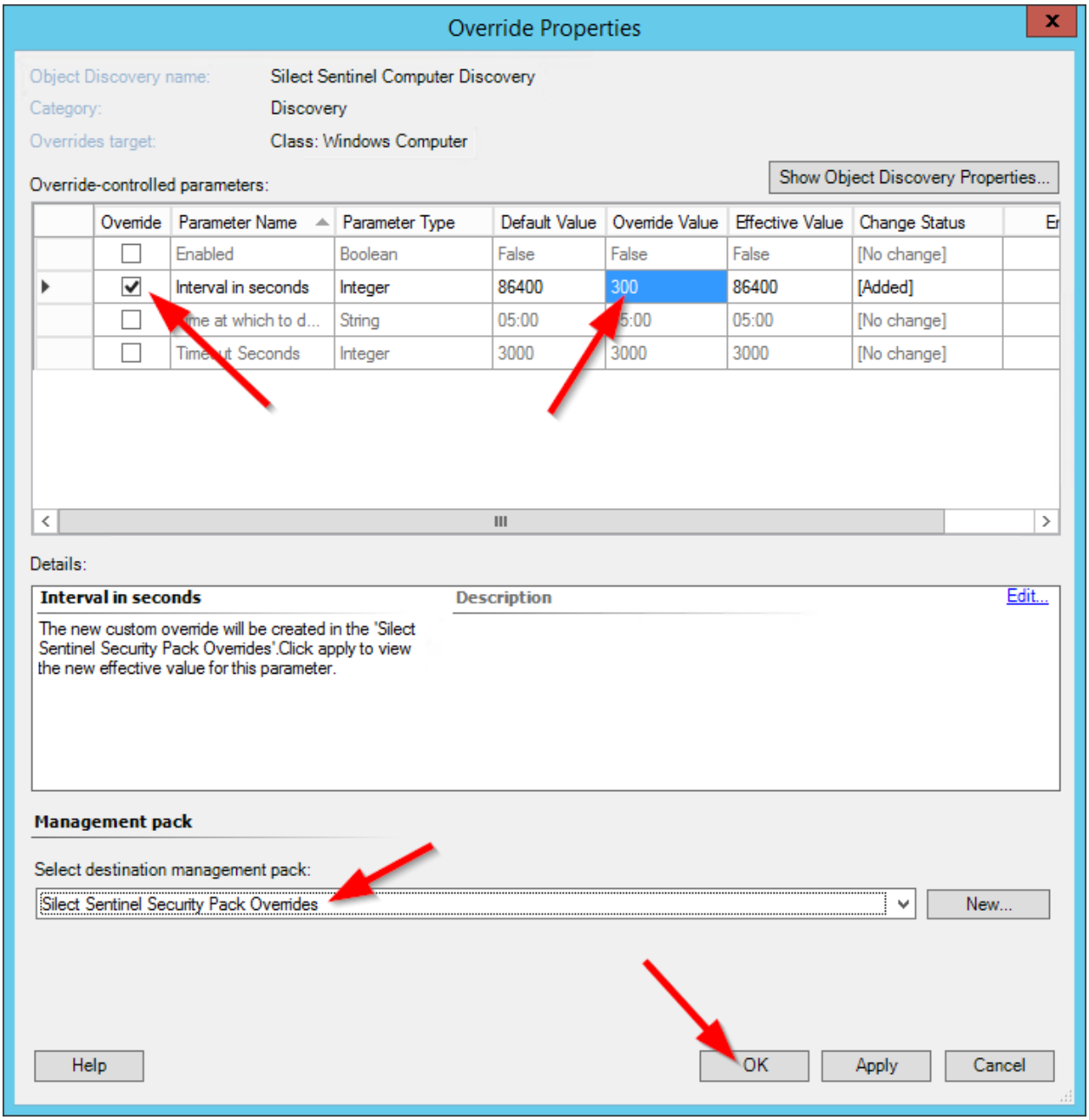
- Step 4: (Optional) You can also select the **Subgroups** tab to add other groups (like **All Windows Computers**) to this group. The **Excluded Members** tab allows you to specify computers which are not to be monitored.
- Step 5: Click **OK** to close the **Properties** window and update the group.

By default, the discovery of computers is scheduled to happen once a day, at 05:00. You may want to speed that up temporarily, for testing purposes. To do that, you need to create an override for the discovery period.

- Step 1: Launch your Operations Manager console. Go to the **Authoring** Workspace, click on **Object Discoveries**, select **Silect Sentinel Computer Discovery** (under **Discovered Type: Silect Sentinel Computer**), right-click and select **Overrides**, then **Override the Object Discovery**, and then **For all objects of class: Windows Computer** from the context menu



- Step 2: From the **Override Properties** page, put a check mark in the **Override** column for **Interval in seconds** and change the **Override Value** from **86400** seconds (1 day) to a smaller number. Try **300** seconds (5 minutes). Select **Silect Sentinel Security Pack Overrides** for the destination management pack. Click **OK** when finished.



Once this override is set, discovery will take place every 5 minutes, so your results should be visible shortly. **Remember to remove the discovery interval override when done testing to minimize the load on your SCOM server and all monitored computers.**

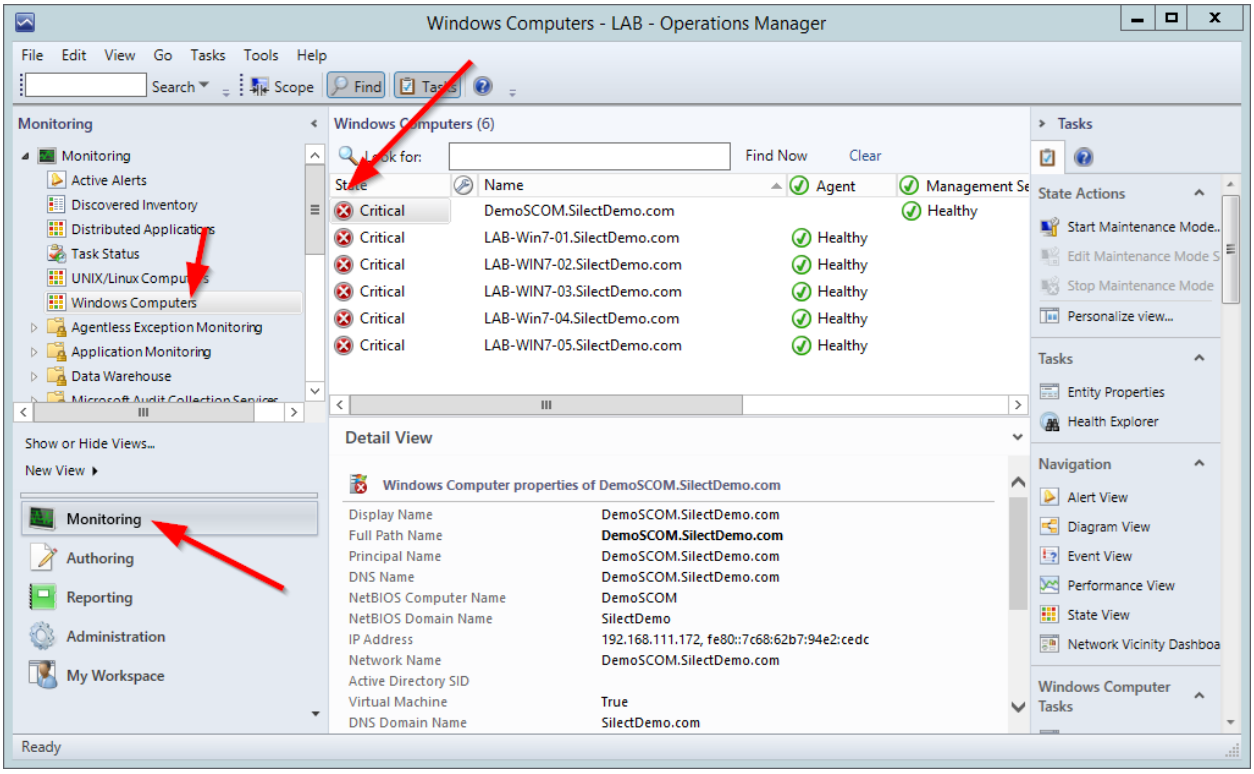
Using the Sentinel Security Pack

Overview

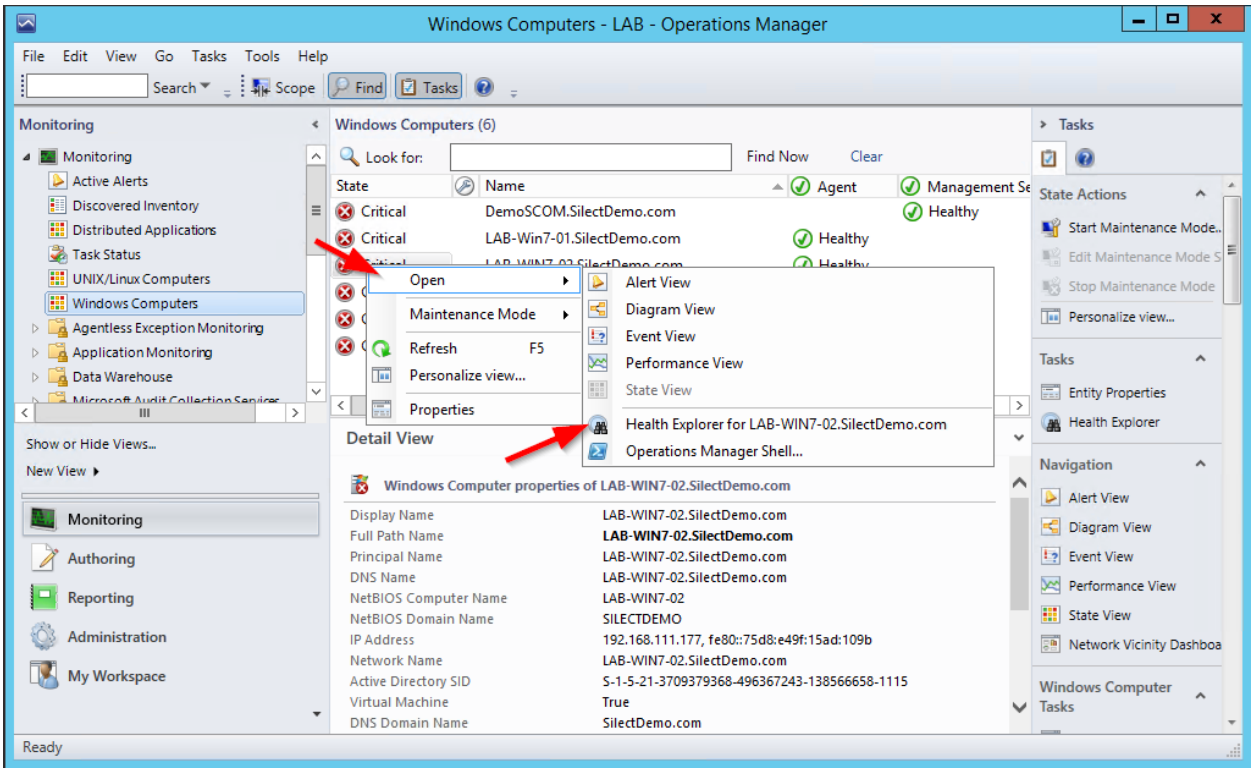
Once the Sentinel Security Pack has been imported into your OpsMgr environment, and computers have been added to a group designated for monitoring, a series of data points used to help determine whether computers are Sentinel-compliant or not are retrieved on a regular basis, through OpsMgr *monitors*, from all computers that have been selected for monitoring. How quickly immediately after importing the Sentinel Security Pack you can start seeing some of its data depends on your environment – as is the case with any other Management Packs, it could take anywhere between a few minutes to a few hours before some of that data starts trickling in.

The Built-in Views

If you have any familiarity with the OpsMgr console, you should know that you can get an overview of the health state of the Windows computers that are being monitored by going to the **Monitoring** workspace, and selecting **Windows Computers**. If any health monitor currently defined by any of the Management Packs that currently exist in your OpsMgr environment is found to be in a non-healthy state for a given computer, the **State** of that computer will be set to a red X. If all monitors for a computer have been found to be in a healthy state, the **State** will be set to a green checkmark. The following figure shows a sample of the OpsMgr console's main **Windows Computers** dashboard.

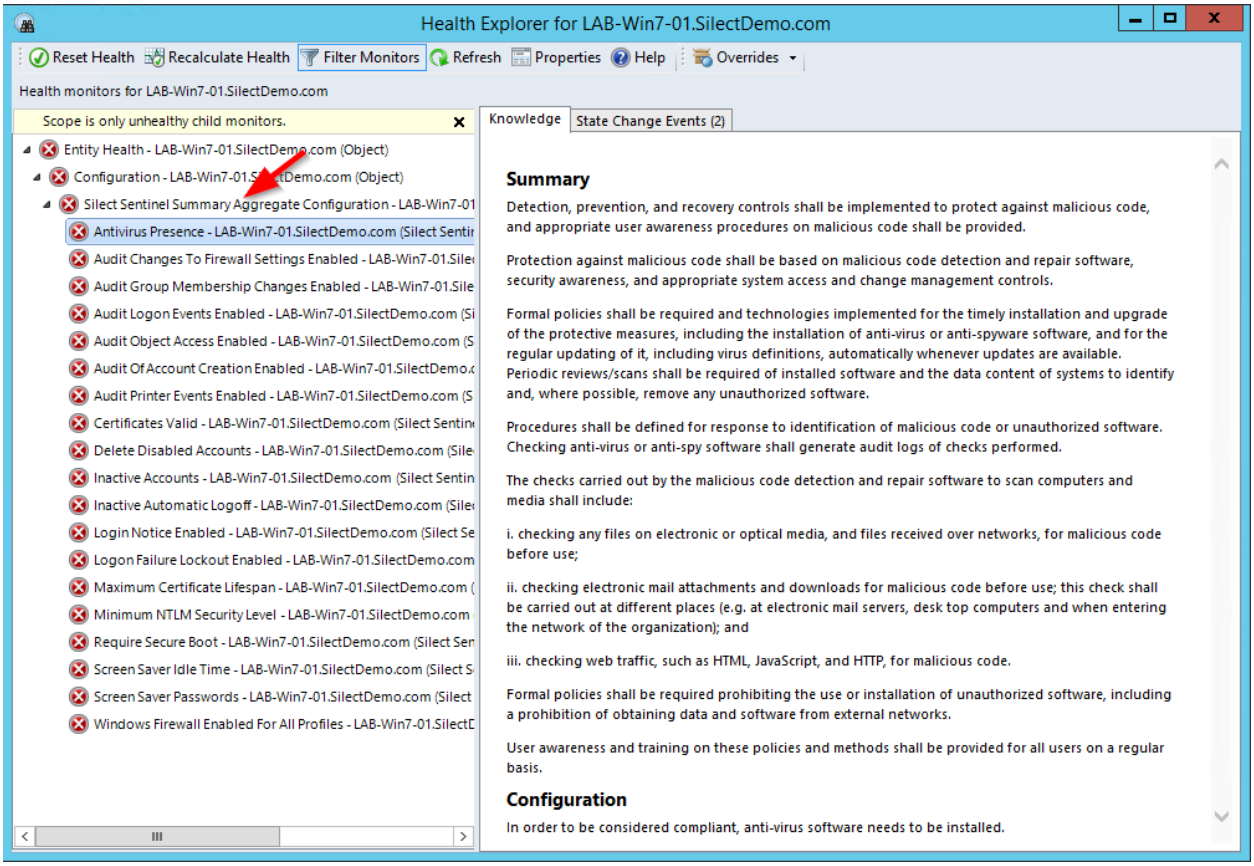


You can right-click on any computer in the list and select **Open**, **Health Explorer for <computer name>** to view a detailed list of all monitors that are currently in an unhealthy state for the selected computer.



All data points collected by the Sentinel Security Pack can be found in the **Health Explorer** window under **Entity Health**, **Configuration**, under a single summarized entry named **Silect Sentinel Summary Aggregate Configuration**.

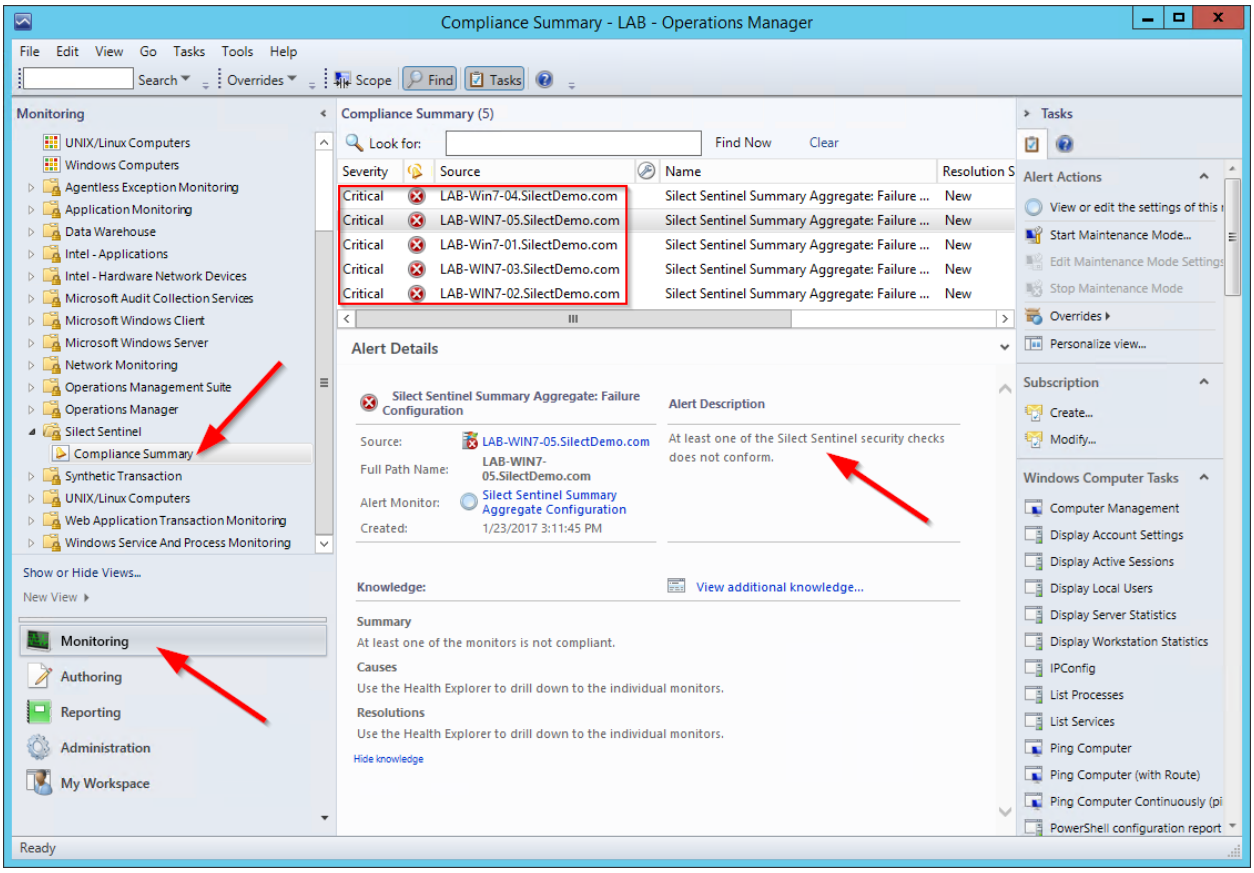
By default, the **Health Explorer** window only shows the health monitors that are currently unhealthy for a given computer.



The Silect Sentinel folder

The main **Windows Computers** dashboard described in the previous section shows a list of Windows computers and the state of all monitors across all of these computers, regardless of which Management Pack these monitors come from. To focus only on data that is related to the Sentinel Security Pack, open the **Silect Sentinel** folder in the **Monitoring** workspace. Under that folder, you will find one Alert view, named **Compliance Summary**; this view displays alerts that have been generated from the summarized state of all monitors defined by the Sentinel Security Pack. Select this view to get a list of all alerts—there will be, at most, one entry per computer. This is not a list

of all computers – this is a list of all computers that have had alerts raised for them because at least one of the Sentinel safeguards has been found to be in a non-compliant state on those computers. If a computer is fully compliant, no alert will be raised, and there won't be any entry for that computer in the list.



As with the **Windows Computers** dashboard, you can right-click on any of the computers in the alert list and select **Open**, **Health Explorer** to get a Health Explorer window showing the state of all unhealthy monitors for the selected computer.

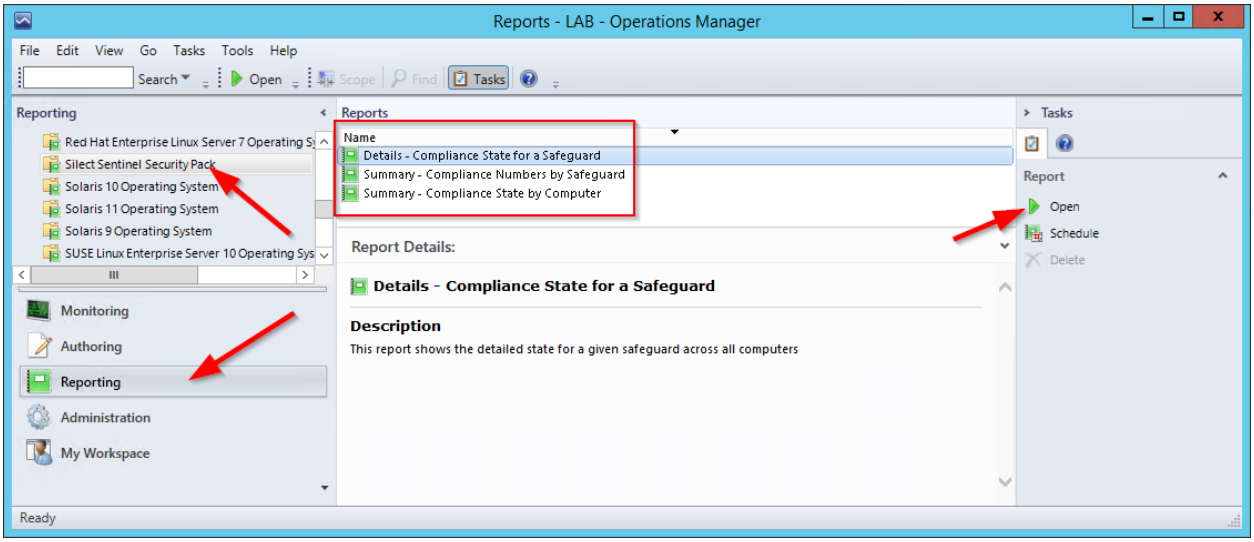
The Sentinel Security Pack reports

The **Windows Computers** dashboard built into OpsMgr provides a list of computers being monitored, and the **Silect Sentinel Security Pack** folder focuses on alerts that originate from the Sentinel Security Pack. The **Health Explorer** view provides a detailed list of all monitors that are in an unhealthy state. While these dashboards, views, and windows can, together, display all the data that is retrieved by the Sentinel Security Pack, the data can appear to be disjointed and cumbersome to use as going to all these

distinct areas of the console involves a lot of navigation. For this reason, the Sentinel Security Pack also includes a number of reports that better organizes the data in an intuitive format tailored for summarizing detailed Sentinel compliance state information, without including data from any other Management Pack's monitors.

The Sentinel Security Pack reports require an instance of SQL Server Reporting Services (SSRS), and a custom data source to be created. The Configuring SQL Server Reporting Services section covers step-by-step instructions to getting this required data source created. The section that follows assumes this has already been set up.

A folder, named **Silect Sentinel Security Pack**, gets created in the **Reporting** workspace when the Sentinel Security Pack is imported into your OpsMgr environment. In the OpsMgr console, select **Reporting**, and **Silect Sentinel Security Pack**. You should see the names of the reports and a short description when one is selected from the list.



To view one of the reports, select it, and then click on the **Open** command in the **Tasks** section on the right side of the window. This opens a new report window.

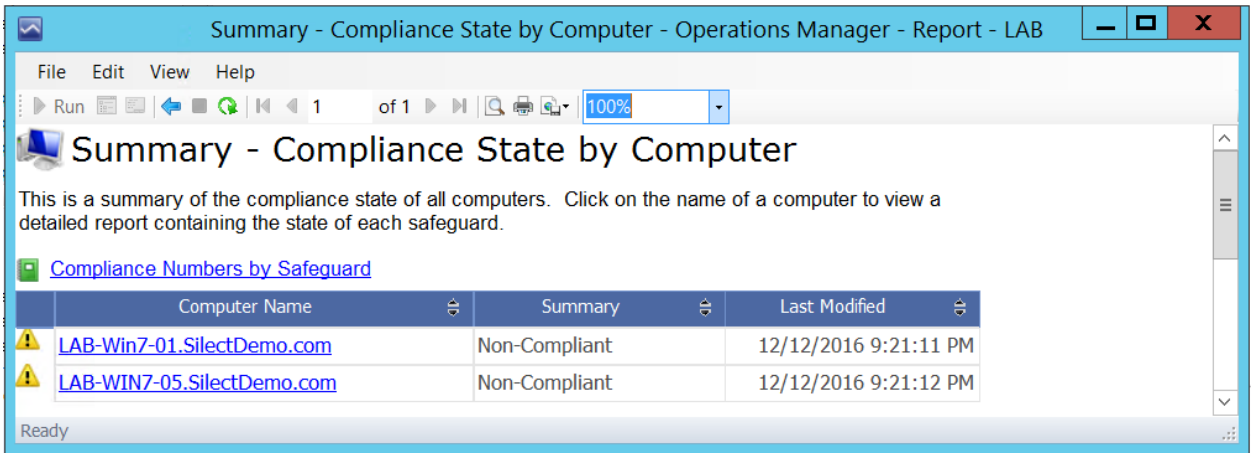
The Sentinel Security Pack includes four reports; one Detailed and two Summary reports are accessible from the **Silect Sentinel Security Pack** report folder. The

second Detailed report is loaded by following links that exist in the Summary reports, and focus on details based on selections made from those summaries.

The next section goes through all reports, one-by-one, navigating between reports by following links. To follow along, start by selecting the **Summary – Compliance State by Computer** report in the **Silect Sentinel Security Pack** report folder in the OpsMgr console and clicking **Open**.

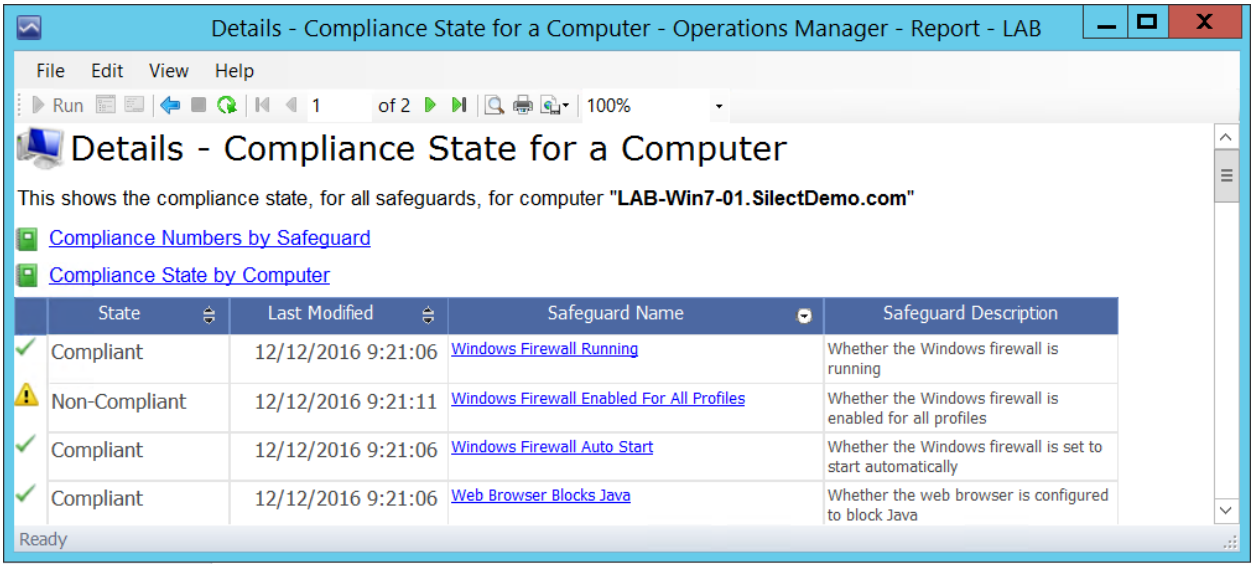
Summary – Compliance State by Computer

The **Summary - Compliance State by Computer** report is essentially a list of all computers, a summarized Sentinel compliance state for each of these computers, and a timestamp indicating when the data that establishes the compliance state was obtained. All computer names in the list are clickable links. When a link is clicked, the **Details – Compliance State for a Computer** report is loaded.



Details – Compliance State for a Computer

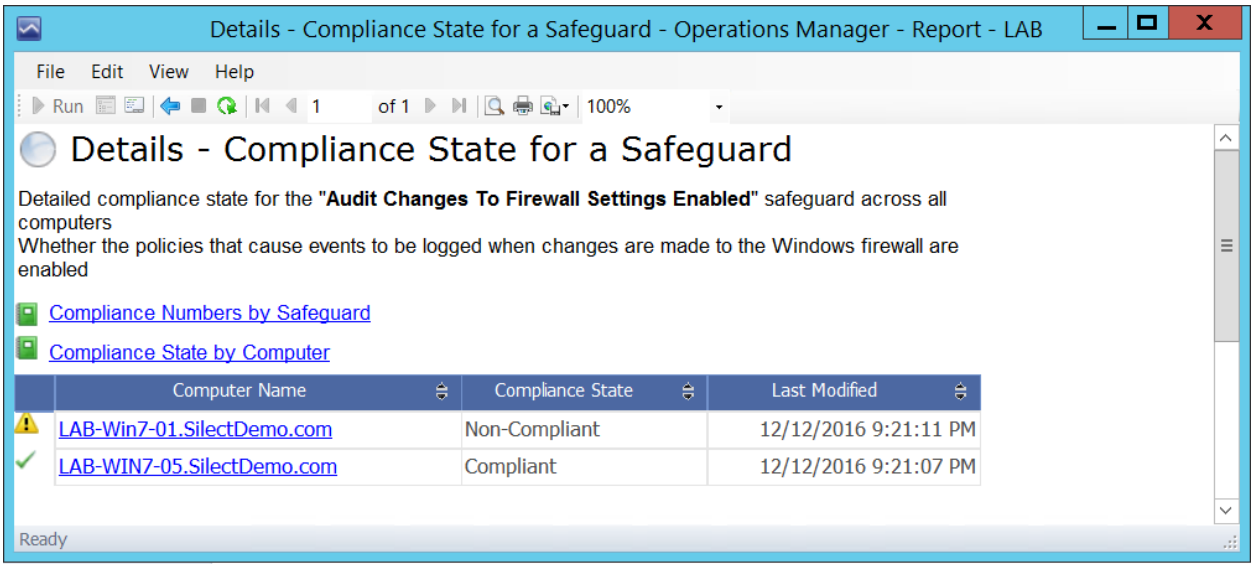
The **Details – Compliance State for a Computer** report is a list of all of the health monitors (“safeguards”, in Sentinel terminology) that were retrieved from a given computer to establish its Sentinel compliance state. The name of each monitor / safeguard is displayed, along with the timestamp at which the data point was obtained, its state (“Compliant” or “Non-Compliant”) as well as a short description of the safeguard.



Each named safeguard in the list is a clickable link – when these links are followed, the **Details – Compliance State for a Safeguard** report is loaded.

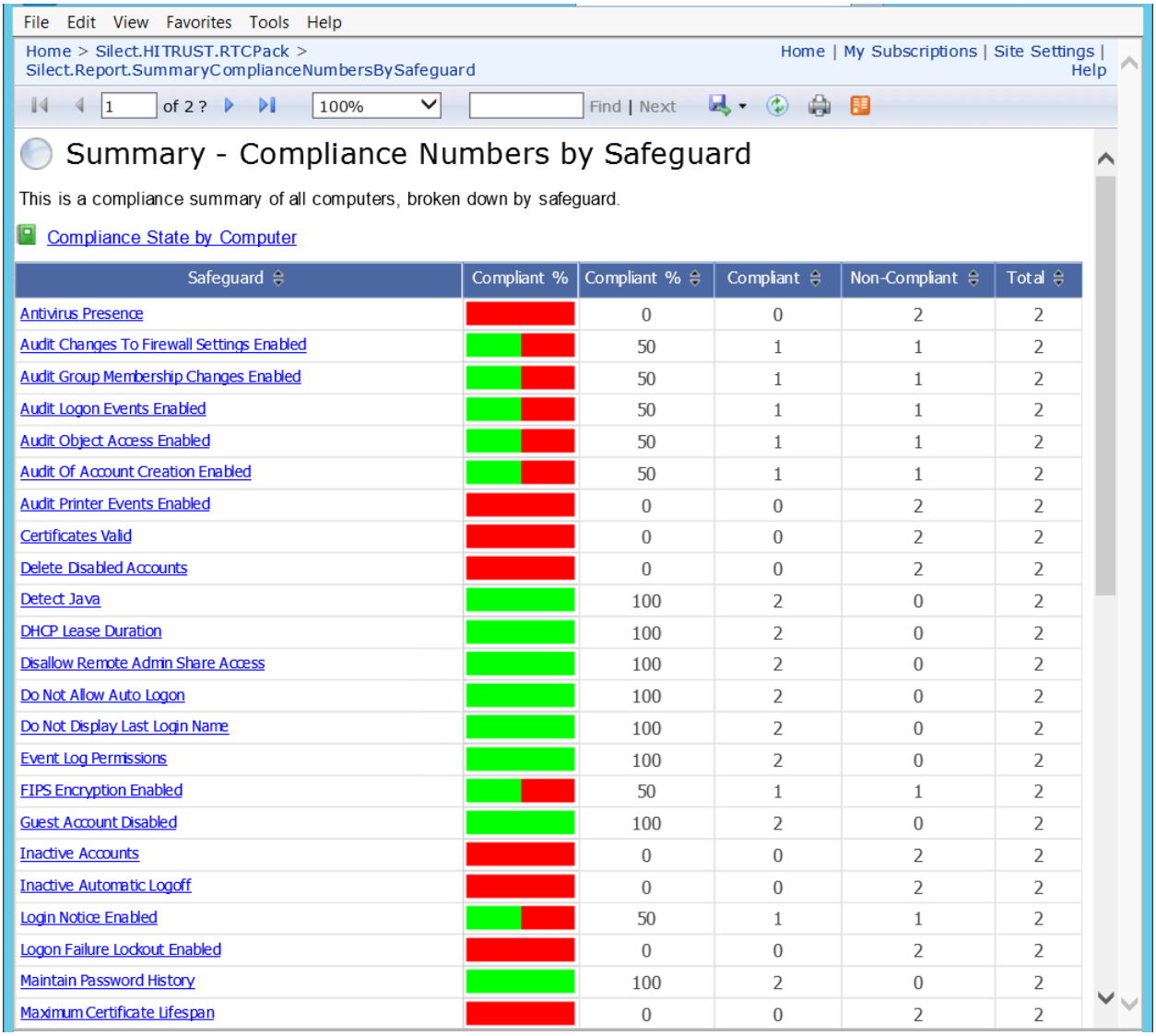
Details – Compliance State for a Safeguard

The **Details – Compliance State for a Safeguard** report is a list showing the compliance state, across all computers, for a given safeguard. Each computer in the list is a clickable link; when one of these links is followed, the **Details – Compliance State for a Computer** report is loaded. This report has already been covered.



Summary - Compliance Numbers by Safeguard

The **Summary – Compliance Numbers by Safeguard** report shows a list of all Sentinel safeguards, and presents a compliance summary for each in terms of number and percentage of computers that are compliant. Each named safeguard is a clickable link; when followed, the **Details – Compliance State for a Safeguard** report (already covered) is loaded. The grid also contains a simple compliant/non-compliant green/red bar graph showing compliance as a percentage of all computers, a column showing the actual percentage as a number, the number of computers that are compliant and non-compliant, and finally, the total number of computers for which compliance data was available.

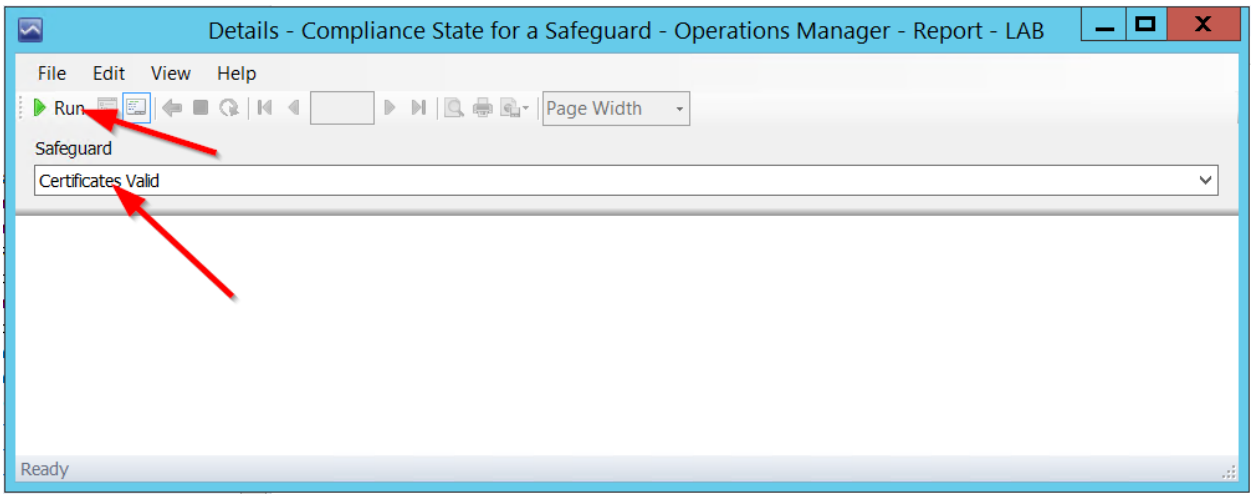


Safeguard	Compliant %	Compliant %	Compliant	Non-Compliant	Total
Antivirus Presence		0	0	2	2
Audit Changes To Firewall Settings Enabled		50	1	1	2
Audit Group Membership Changes Enabled		50	1	1	2
Audit Logon Events Enabled		50	1	1	2
Audit Object Access Enabled		50	1	1	2
Audit Of Account Creation Enabled		50	1	1	2
Audit Printer Events Enabled		0	0	2	2
Certificates Valid		0	0	2	2
Delete Disabled Accounts		0	0	2	2
Detect Java		100	2	0	2
DHCP Lease Duration		100	2	0	2
Disallow Remote Admin Share Access		100	2	0	2
Do Not Allow Auto Logon		100	2	0	2
Do Not Display Last Login Name		100	2	0	2
Event Log Permissions		100	2	0	2
FIPS Encryption Enabled		50	1	1	2
Guest Account Disabled		100	2	0	2
Inactive Accounts		0	0	2	2
Inactive Automatic Logoff		0	0	2	2
Login Notice Enabled		50	1	1	2
Logon Failure Lockout Enabled		0	0	2	2
Maintain Password History		100	2	0	2
Maximum Certificate Lifespan		0	0	2	2

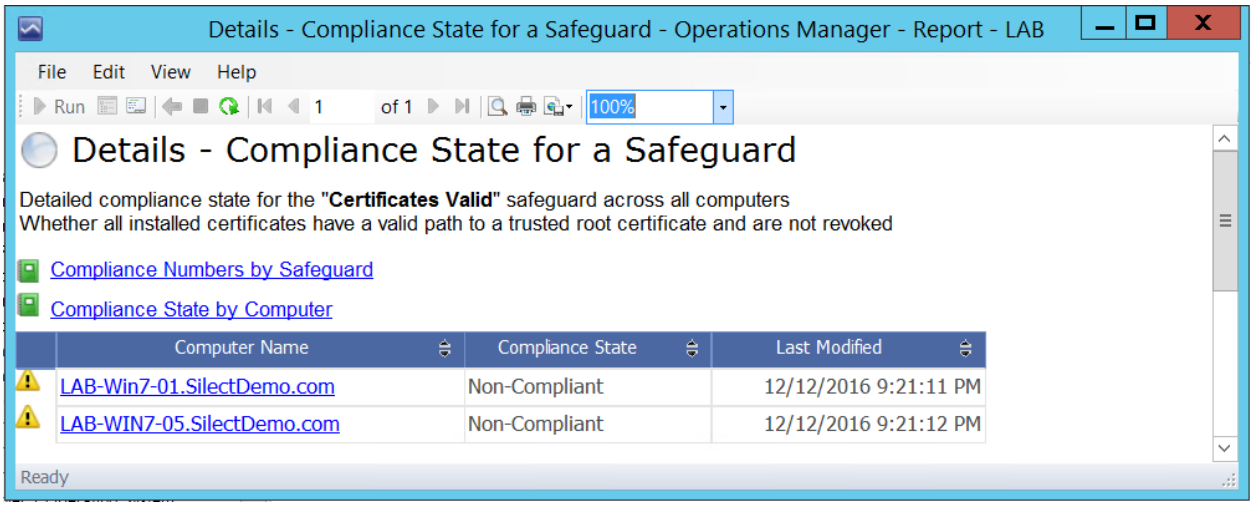
Details - Compliance State for a Safeguard

The **Details - Compliance State for a Safeguard** report shows the detailed state for a given safeguard across all computers. A single safeguard is selected and the report shows all computers and indicates which are compliant or non-compliant. Each computer is a clickable link; when followed, the **Details – Compliance State for a Computer** report (already covered) is loaded.

When the report is initially shown, the user must select a safeguard from the drop down list and then click Run to display the report for the selected safeguard.

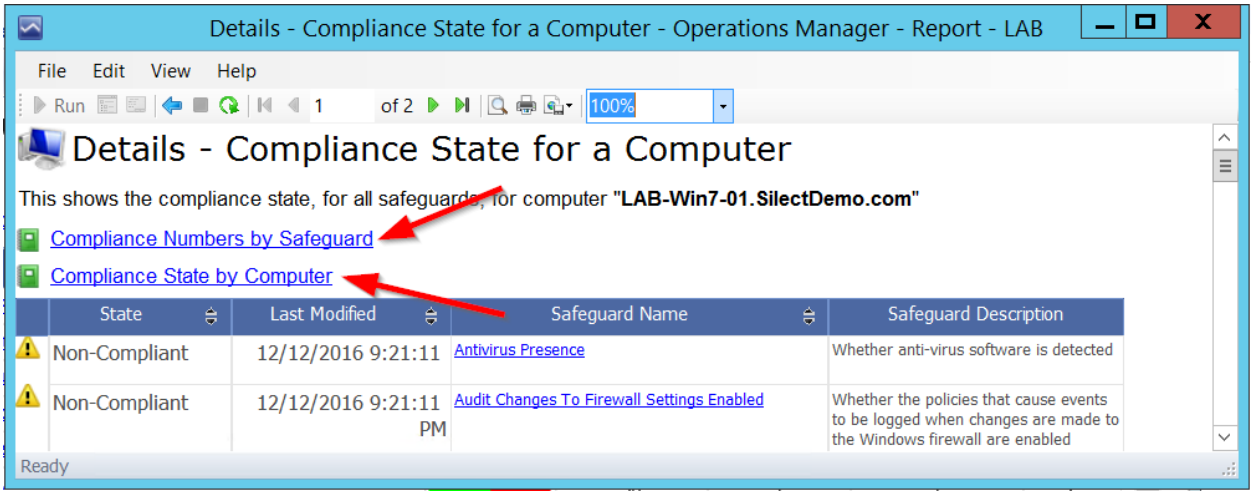


Once the safeguard has been selected and the report is run, the results will be shown.

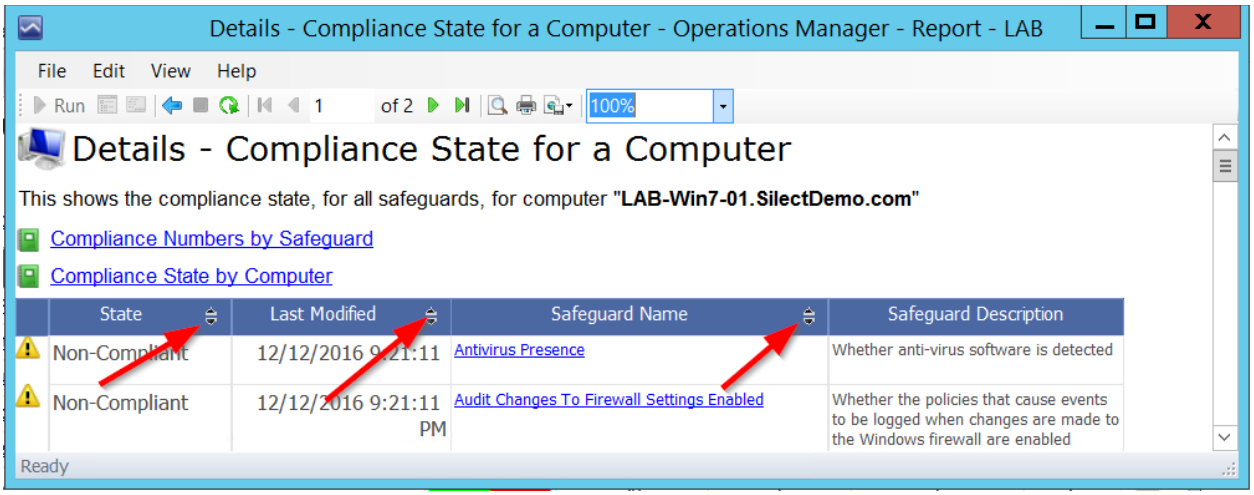


Other report details

All reports contain links near the top that provide shortcuts to the summary reports. Once a report is loaded from the OpsMgr console, you can navigate to any of the other ones by following either of these links, or the links in the grid displayed by the report, without having to go back to the OpsMgr console to load a different report.



Most columns in all grids can be sorted by clicking on the small arrows that appear on the right side of each column's header.



Remediation Tasks

Please note that Remediation Tasks are only available in the Sentinel Pro Security Pack.

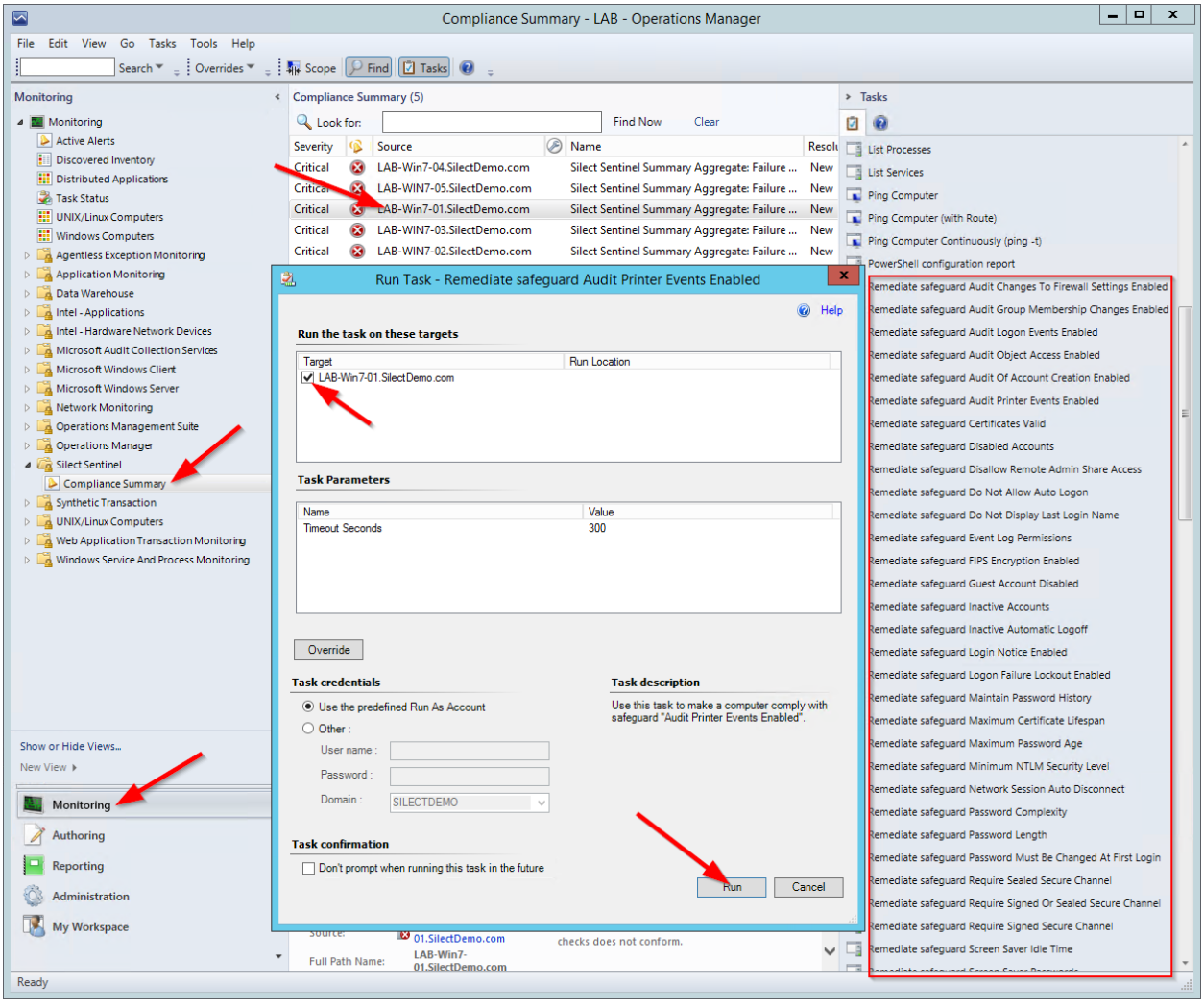
The purpose of using the Sentinel Security Pack is to help establish which computers within an organization are not compliant with some of the Sentinel safeguards, and then to bring those computers that are not compliant into compliance by applying changes to their configuration—this is the remediation process.

While a network administrator could visit each non-compliant computer one-by-one and manually apply changes to their configuration to bring them into compliance, or even apply these changes remotely, the Sentinel Security Pack defines a number of *tasks* that can be invoked from within the OpsMgr console to run scripts to do that. Another alternative for remediation is to use Group Policy to change the configuration of many computers at a time.

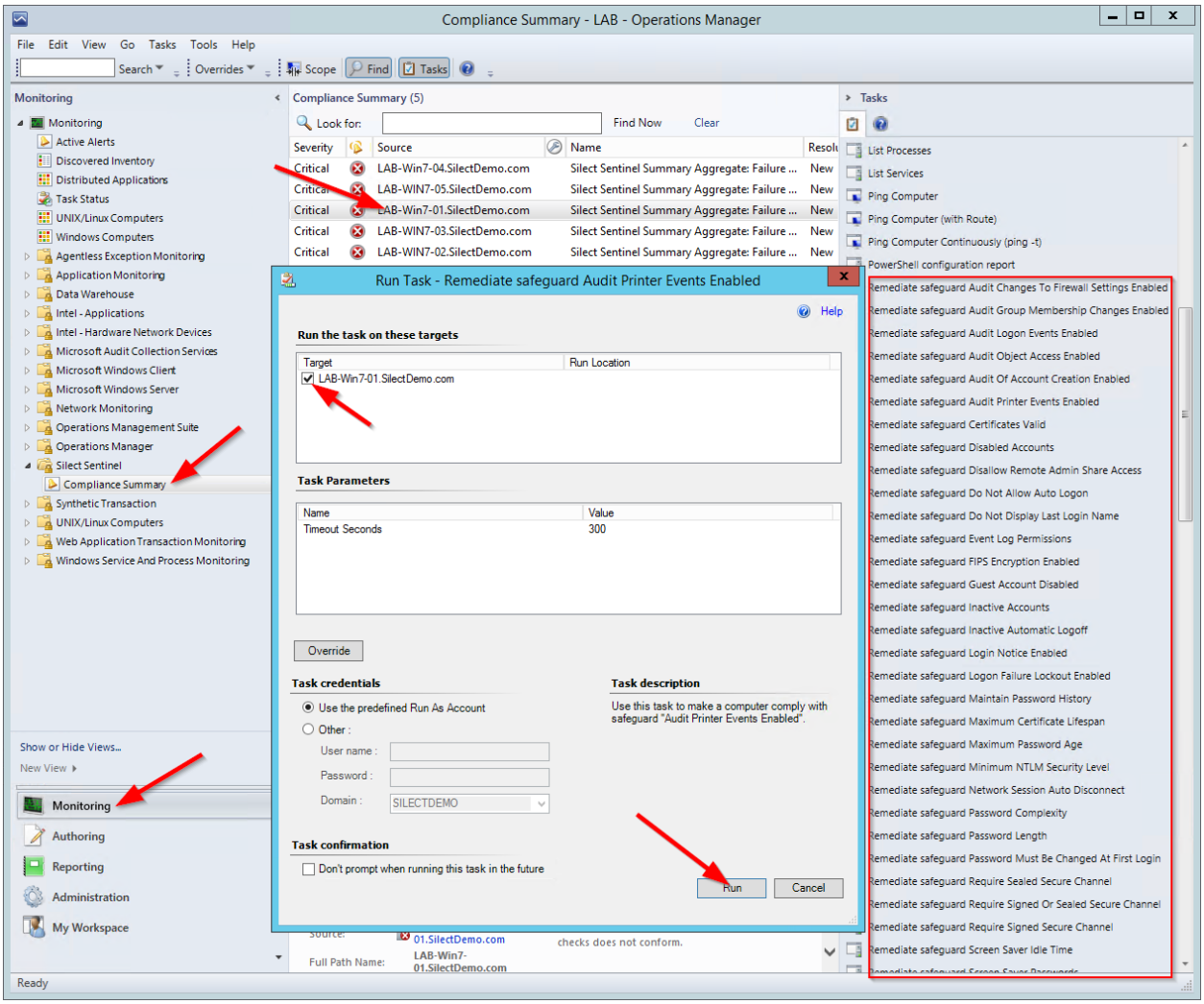
To be clear, **these remediation scripts modify the configuration of the computers they're executed on**, which is something that can have far-reaching consequences. As such, each health monitor / Sentinel safeguard defined by the Management Pack has its own script, which has to be invoked by itself—there is no bulk, "click-once" facility to allow all settings to be changed all at once – it is the responsibility of the user of the Sentinel Security Pack to decide which scripts should be run, and which computers to run them on. The next few pages describe the process of invoking these tasks, which should be familiar to experienced OpsMgr users.

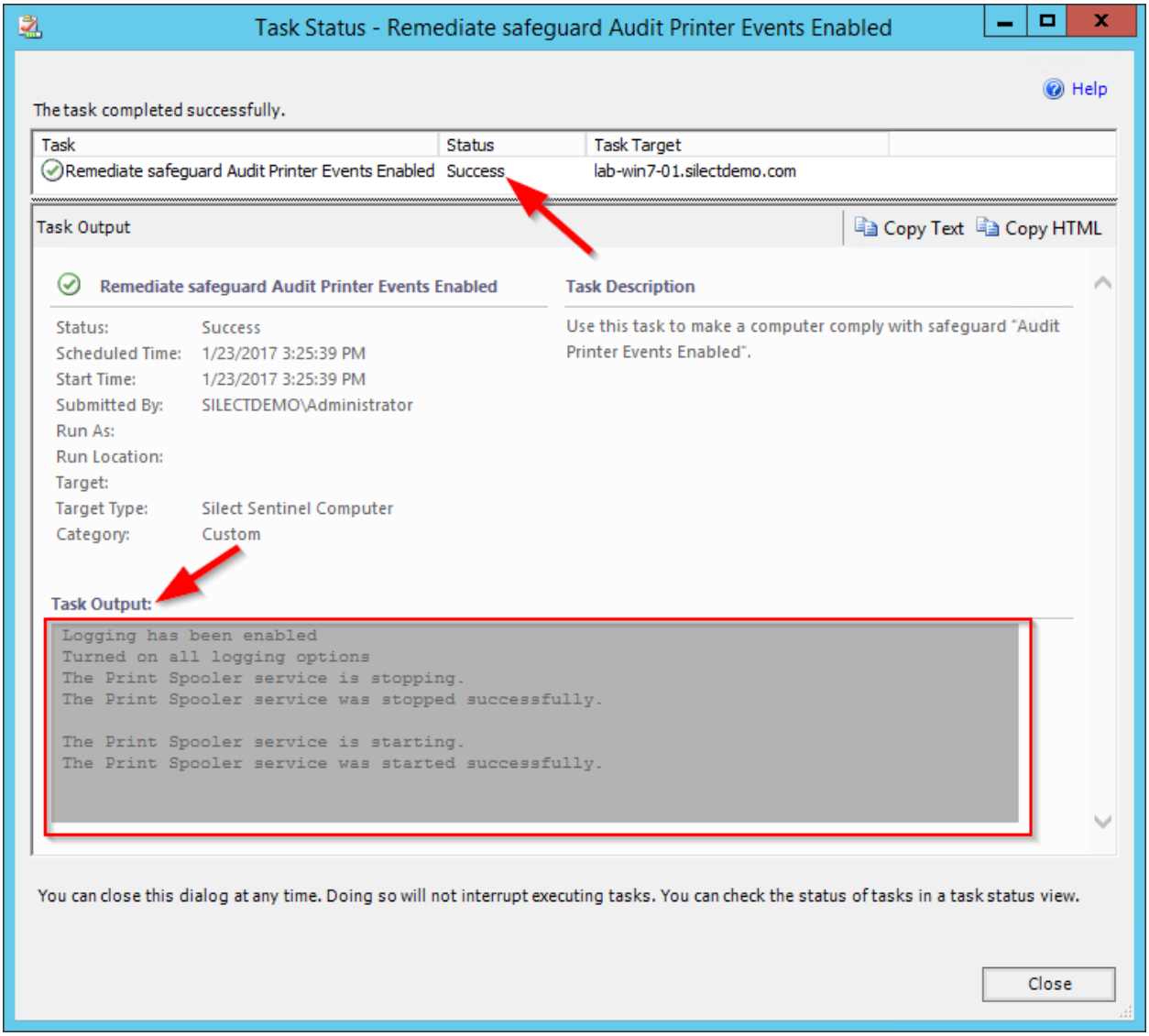
The first step for applying remediation is to establish which Sentinel safeguards are not compliant for each computer. The OpsMgr console's **Health Explorer** window can show which monitors are not in a healthy state; as does the Details – Compliance State for a Computer report. However, you will probably find that navigating between computers is quicker using links in the report rather than using the Health Explorer window—not to mention that the Health Explorer window does not focus strictly on the Sentinel-related monitors. You can open either one of these windows and leave them opened side-by-side with the main OpsMgr console window, so both are visible at the same time as you select from the console window the tasks that need to be run.

Once you have a window opened, showing which Sentinel safeguards are in a non-compliant state for a given computer, select that same computer from one of the Alert views under the **Silect Sentinel** folder in the OpsMgr console's **Monitoring** workspace. When a computer is selected, the **Windows Computer Tasks** section on the right side of the console window will show a list of tasks that can be run against the computer. There is one task for every monitor which can be remediated mechanically, and its name corresponds to the name of a Sentinel safeguard. There are also utility tasks to display certain settings of a computer. Look up the name of a non-compliant Sentinel safeguard, and click on the corresponding entry in the **Windows Computer Tasks** list. A **Run Task** dialog box will appear, showing the name of the task, a short description and the name of the computer on which the task will be executed. Click on **Run** to execute the task.



After a few seconds, a **Task Status** dialog box will appear and indicate the outcome of the script that was just invoked by running the task.



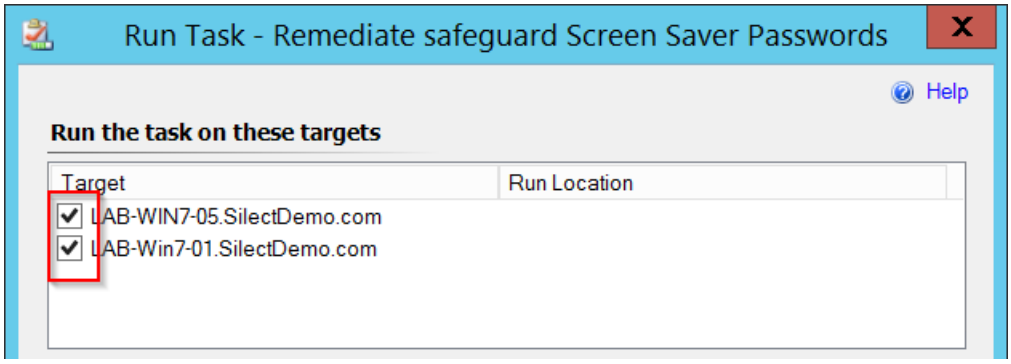


Generally, when these scripts run successfully, the **Error** section in the **Task Status** dialog box will simply indicate “None” and the **Exit Code** section will report “0”. If errors were encountered by the remediation script, this section will contain data that should provide important clues about the nature of the error that occurred. If an error is reported by any of the scripts, the configuration of the computer will not have changed, and it will remain in a non-compliant state.

Whether a script successfully managed to reconfigure a computer or not, the monitor for that Sentinel safeguard will be re-evaluated after a while—the frequency is which is determined by your OpsMgr configuration. If a script was successful in changing a

computer's configuration, the monitor will report back in a healthy state when it gets re-evaluated, unless an individual or an automated process somehow reconfigures the computer in a way that negates the effects of running the task.

Note that the list of computers that is displayed when selecting one of the Alert views under the **Silect Sentinel** folder allows multiple computers to be selected at the same time, by holding the **Ctrl** and/or **Shift** keys. When multiple computers are selected when a task is clicked, the **Run Task** window will show all of the computers that the task will run against.



While this allows you to run the same task in bulk against many computers, you should not do so before you're familiar with the process, have run tasks on a few computers, and verified that running these scripts has no ill effect in your environment. Even so, be aware that even though the OpsMgr console allows you to launch tasks on a large number of computers at once in this fashion, doing so can put a significant strain for a prolonged period of time not only on your OpsMgr server, but on your network infrastructure as well.

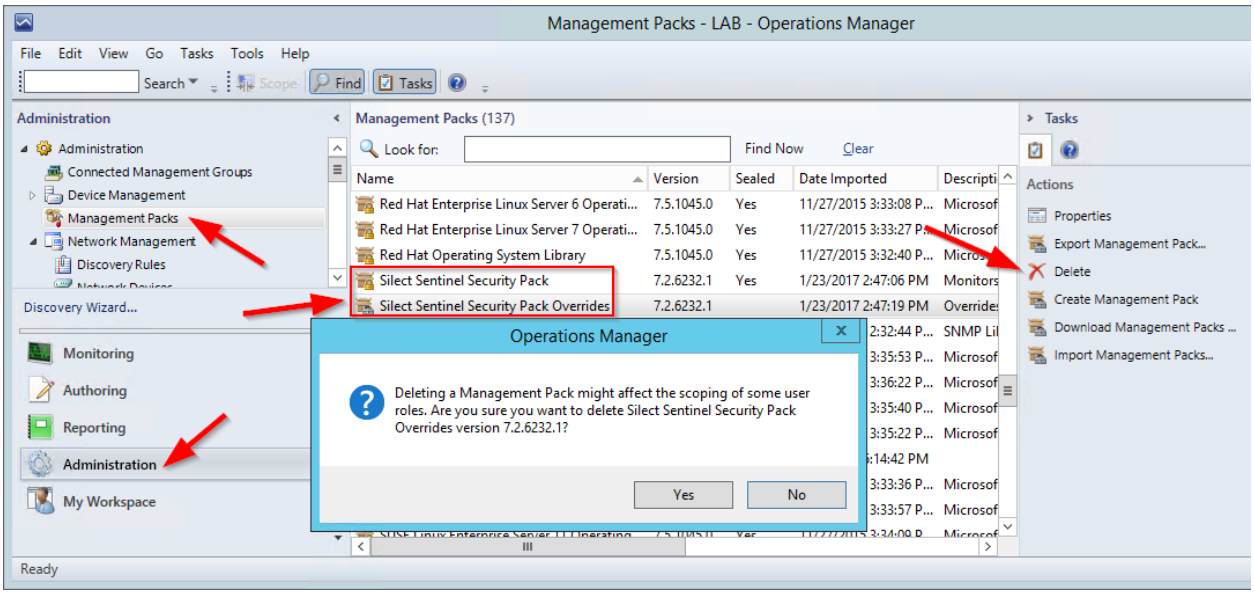
Removing the Sentinel Security Pack

This section describes the steps that need to be taken to completely remove the Sentinel Security Pack, along with the data source that may have been optionally created before importing it.

Removing the Management Pack

The Sentinel Security pack can be removed like any other Management Pack:

- Step 1: In the OpsMgr console, go to the **Administration** workspace, click on **Management Packs**, select the **Silect Sentinel Security Pack Overrides** entry from the Management Pack list, and click on **Delete** in the **Actions** section on the right side of the screen. Repeat for the **Silect Sentinel Security Pack** MP. If you have a lot of management packs, you can more quickly locate the entry in the list by typing "**Silect**" in the **Look for** section and pressing **Find Now**.



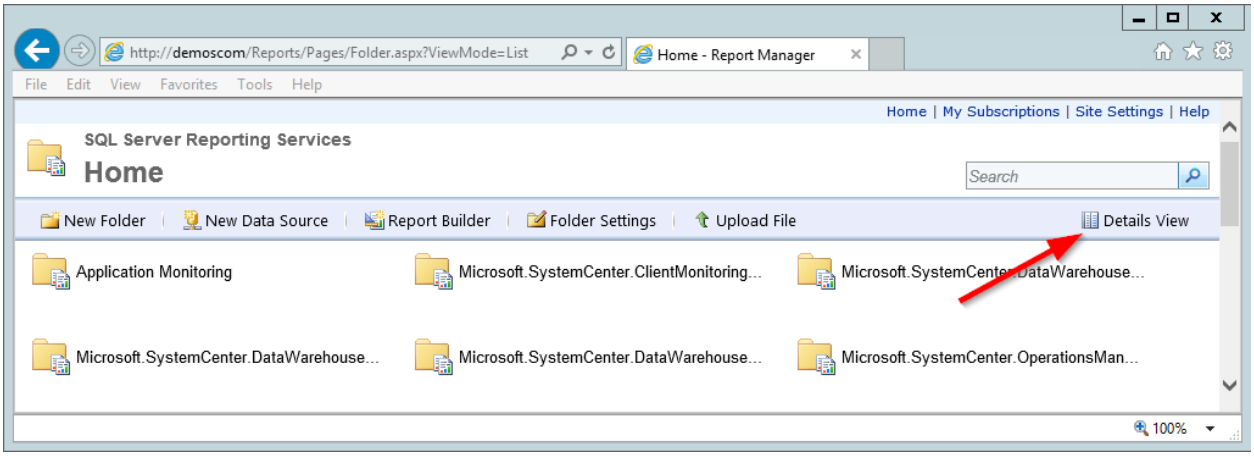
- Step 2: When prompted to confirm the removal of the Management Pack, click **Yes**. After a few seconds to a few minutes, depending on the performance of

your OpsMgr environment, the entry will be removed, as well as the **Silect Sentinel** folders from the **Monitoring** and **Reporting** workspaces.

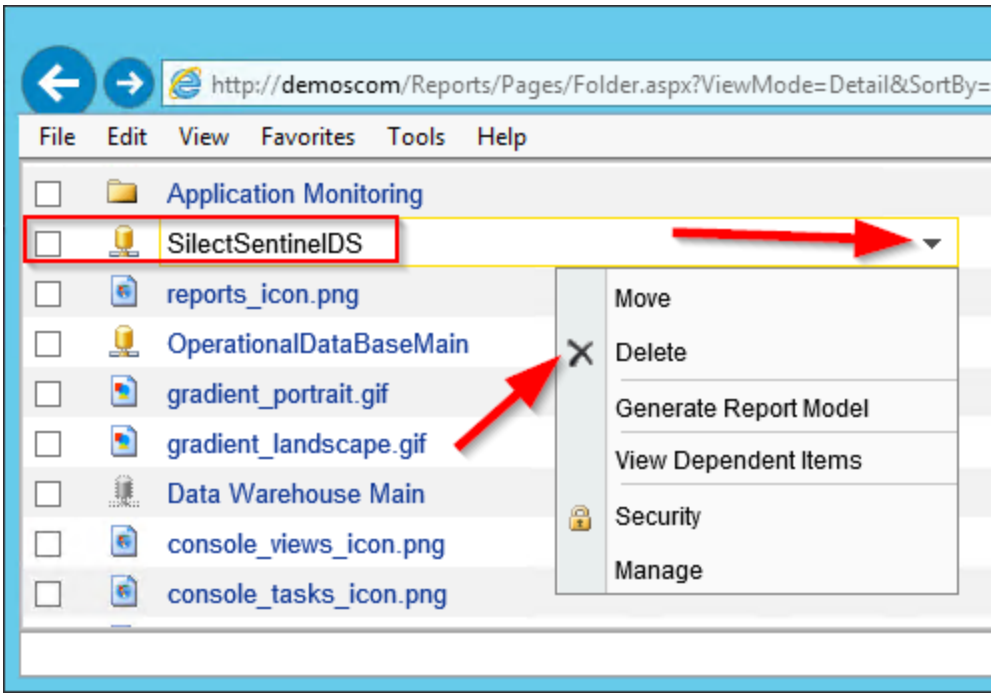
Removing the custom Data Source from SSRS

If you followed the Configuring SQL Server Reporting Services steps from the Installing the Management Pack section, a data source for the custom reports was created in SSRS. Removing the Management Pack following the steps described in the section above does not remove this data source. While its presence is entirely harmless, as a best practice, you should follow these steps to remove it:

- Step 1: Using the web browser of your choice, go to http://YourServerNameHere/Reports, where "YourServerNameHere" is the name of your SSRS server. Your browser should be redirected to http://YourServerNameHere/Reports/Pages/Folder.aspx.
- Step 2: Click on **Details View**, in the top-right corner



- Step 3: Place a checkmark next to the **SilectSentinelDS** entry, then click on the **Delete** button on the top-left side of the toolbar, or click on the down arrow to the right of "**SilectSentinelDS**" and select **Delete**.



- Step 4: Click **OK** when prompted to confirm the deletion of the data source. The page should be redisplayed with the item gone. You can close the browser.

Contacting Technical Support

Before contacting Technical Support, please ensure that you can successfully launch the System Center Operations Manager console.

Additional product support information can be found at:
https://www.silect.com/sentinel-mp/

Support requests can be made either online at:
http://www.silect.com/support
or via email at:
support@silect.com