Sentinel Security Pack
for Microsoft System Center
Configuration 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.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

The information contained herein is the property of Silect Software, Inc. and is strictly confidential. Except as expressly authorized in writing by Silect Software, Inc., the holder of this document shall keep all information contained herein confidential. Except as expressly authorized in writing by Silect Software Inc., the holder is granted no rights to use, reproduce, or otherwise disclose or disseminate the information contained herein.

Copyright © 2015-2018
Silect Software, Inc.
6333 Rideau Valley Dr. N
Manotick, Ontario
K4M 1B3 Canada

http://www.silect.com

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

Contents

Preface **4**
About the Sentinel Security Pack Deployment Guide 4
Audience 4
Document Conventions 4
Overview of the Sentinel Security Pack **6**
About the Sentinel Security Pack 6
Installation and Deployment **7**
Prerequisites 7
Supported versions of System Center Configuration Manager 7
Supported Operating Systems 10
Supported Languages 11
Installing the Configuration Pack 11
Importing the Configuration Pack into Configuration Manager 11
Deploying the Configuration Pack 16
Using the Sentinel Security Pack **20**
Overview 20
The Deployment Summary View 20
Additional Reports 22
Removing the Sentinel Security Pack **24**
Removing the Configuration Pack 24
Contacting Technical Support **25**

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

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 Configuration Manager. It contains the following sections:

- Overview of the Sentinel Security Pack
- Installation and Configuration
- Using the Sentinel Security Pack
- Removing the Sentinel Security Pack
- Contacting Technical Support

Audience

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

- Administrators
- Operators
- Maintenance Personnel

Familiarity with general use of the Configuration Manager console and some basic Configuration 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 “Configuration 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 Configuration Manager supported by the Sentinel Security Pack.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

“Microsoft System Center Configuration Manager” is abbreviated in this document as “ConfigMgr”.

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

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

Overview of the Sentinel Security Pack

About the Sentinel Security Pack

The Sentinel Security Pack by Silect Software, Inc. is a Configuration Pack (CP) intended to be used with Microsoft System Center Configuration Manager (ConfigMgr) versions 2012 and newer. Its purpose is to gather configuration information from computers that are being managed by ConfigMgr and report whether those computers are compliant with a number of *safeguards* defined by the Sentinel Security Pack.

The Configuration Pack is delivered as a single file with the .CAB extension.

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

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

Installation and Deployment

Prerequisites

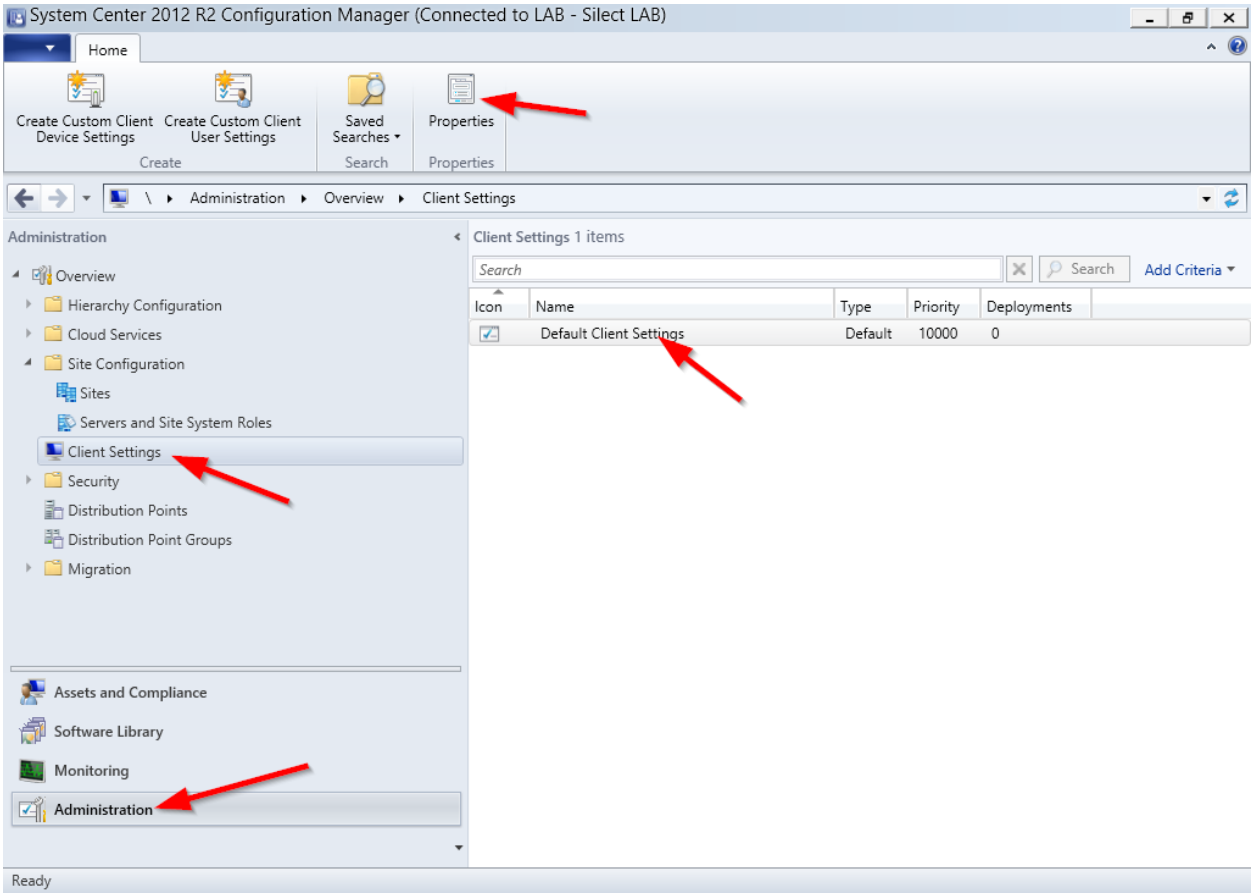
This section enumerates the versions of System Center Configuration Manager supported by the Sentinel Security Pack, as well as the versions of Windows required by the computers being monitored, and the languages supported.

Supported versions of System Center Configuration Manager

The Sentinel Security Pack supports all versions of Microsoft System Center Configuration Manager, from 2012 through 2016, with and without their respective service packs and update rollups. ConfigMgr 2007 or 2007 R2 are not supported.

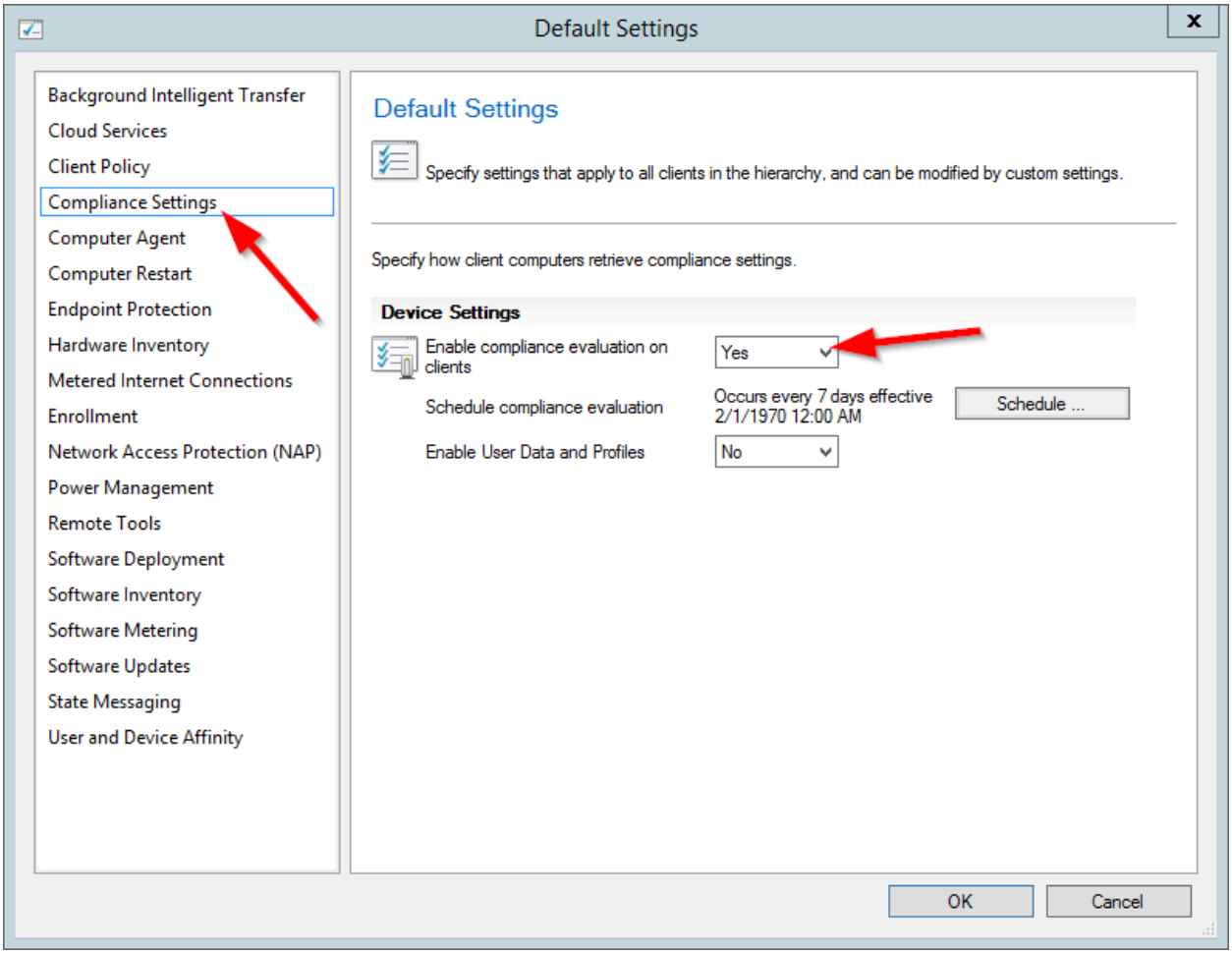
The ConfigMgr agent must be configured to enable compliance evaluation on clients. Verify this is the case by going to the **Administration** workspace in the ConfigMgr console, navigating to **Overview**, **Site Configuration**, **Client Settings**, selecting the **Default Client Settings** entry from the **Client Settings** list, and selecting **Properties** from the toolbar.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited



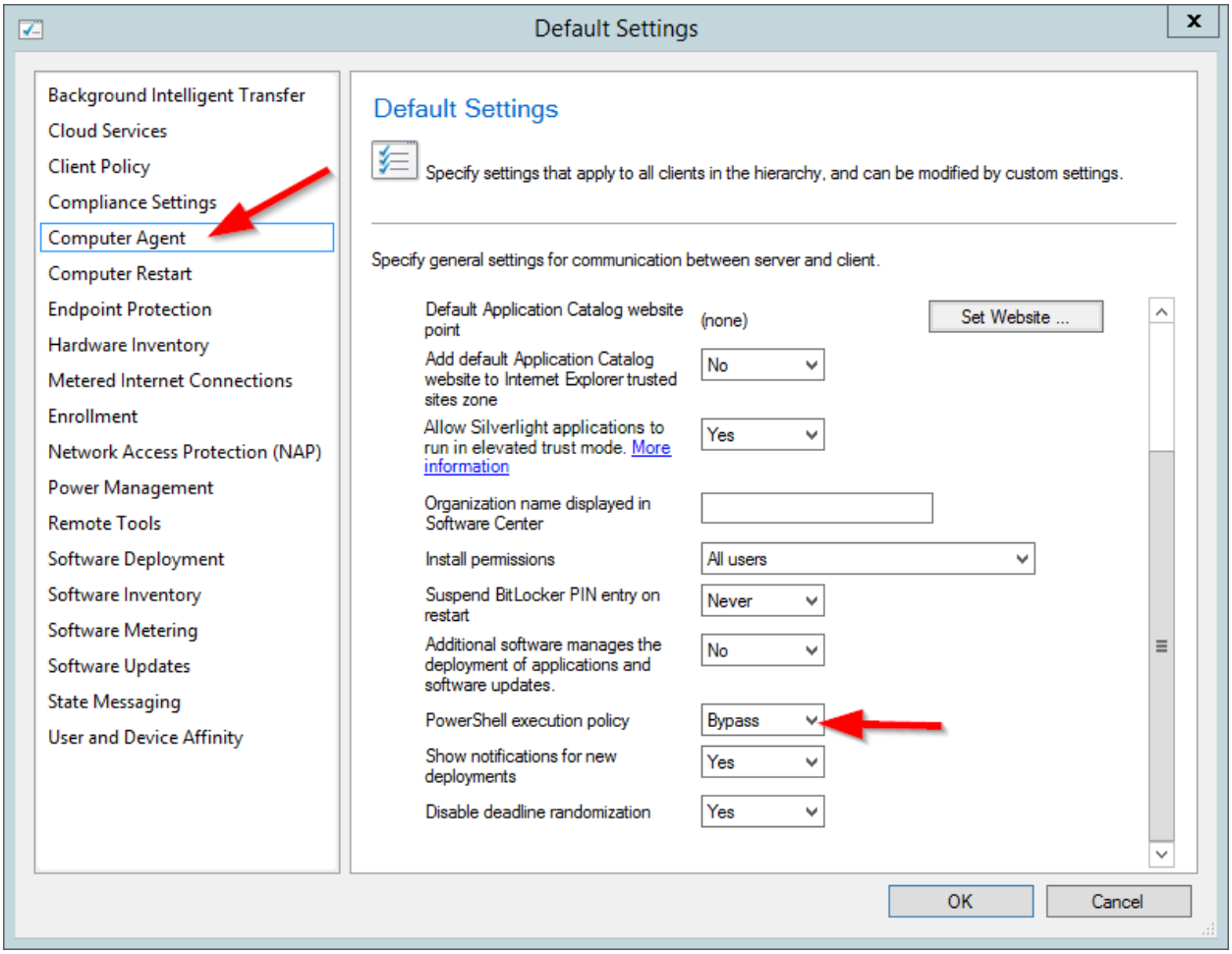
This will bring up a dialog box showing the default settings for the ConfigMgr client. Go to **Compliance Settings** (on the left side of the dialog box), and verify that **Enable compliance evaluation on clients** is set to **Yes**.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited



Additionally, the ConfigMgr client must be allowed to execute PowerShell scripts. In the same dialog box, select **Computer Agent** from the left side of the dialog box, and make sure that **PowerShell execution policy** is set to either **All Signed** or **Bypass**.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited



Supported Operating Systems

The computers being managed by ConfigMgr 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

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

	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 ConfigMgr's agent to function correctly. Refer to the documentation for your version of ConfigMgr for details.

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

Supported Languages

The Sentinel Security Pack supports US English only. While the ConfigMgr agent may work on computers that are running versions of Windows using different languages, all information gathered by the Configuration Pack is in US English only.

Installing the Configuration Pack

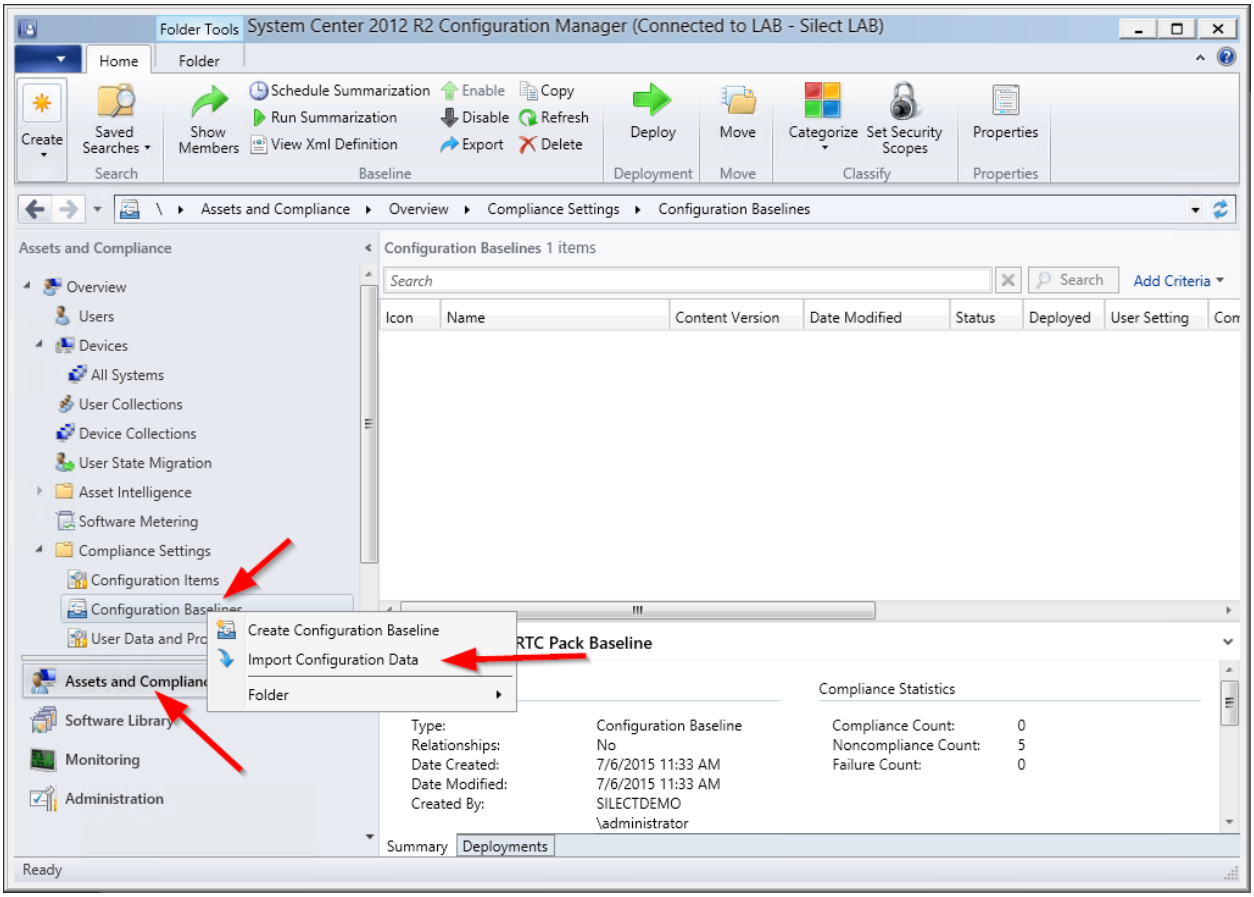
Before using the Configuration Pack, it first needs to be imported into your ConfigMgr environment. After it's been imported, it needs to be deployed against ConfigMgr collections.

Importing the Configuration Pack into Configuration Manager

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

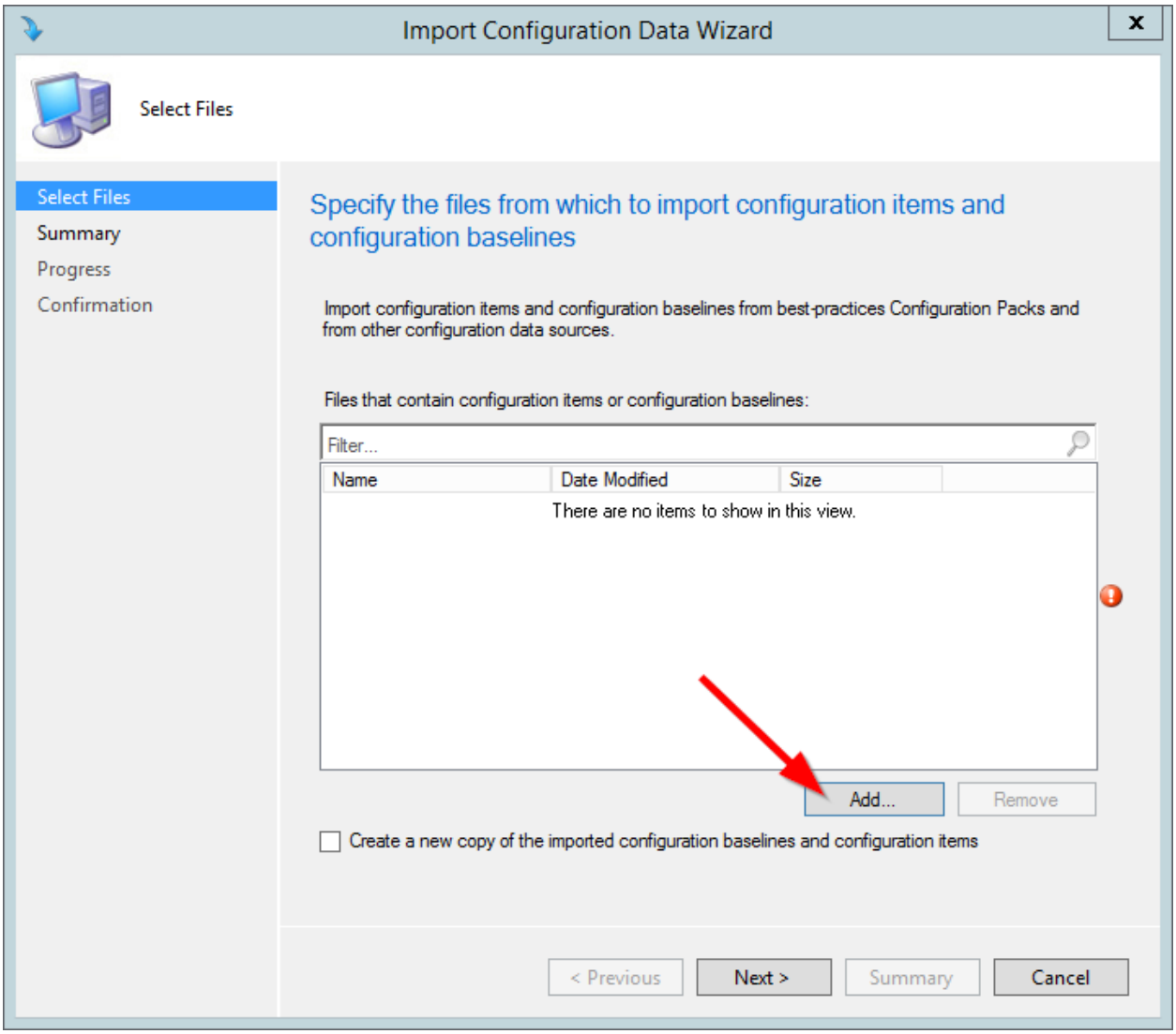
- Step 1: Launch your Configuration Manager console. Go to the **Assets and Compliance** Workspace, navigate to **Overview**, **Compliance Settings**, right-click on **Configuration Baselines**, and select **Import Configuration Data**.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited



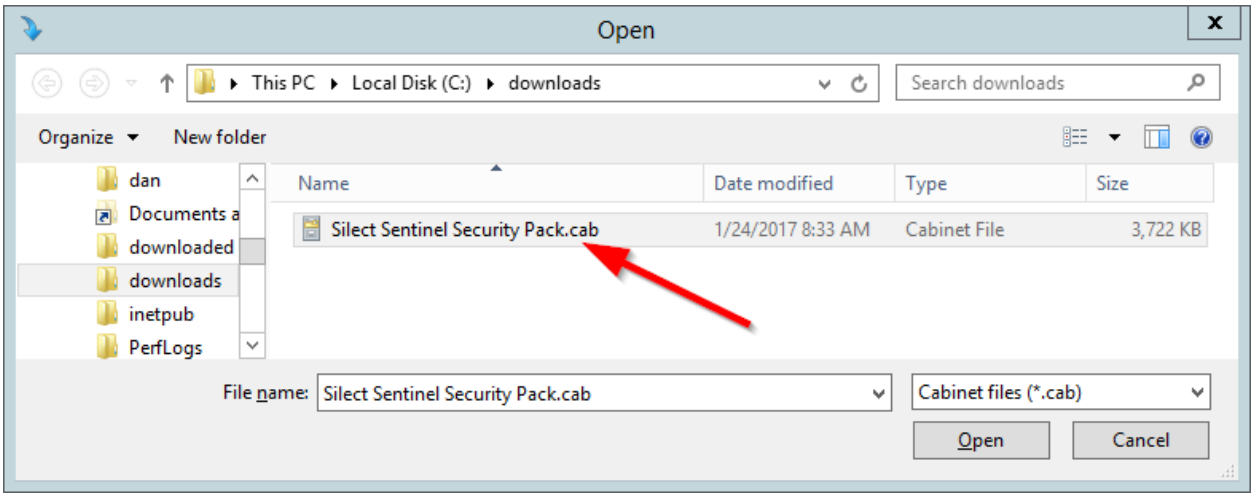
- Step 2: In the **Import Configuration Data** wizard, click on **Add**:

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

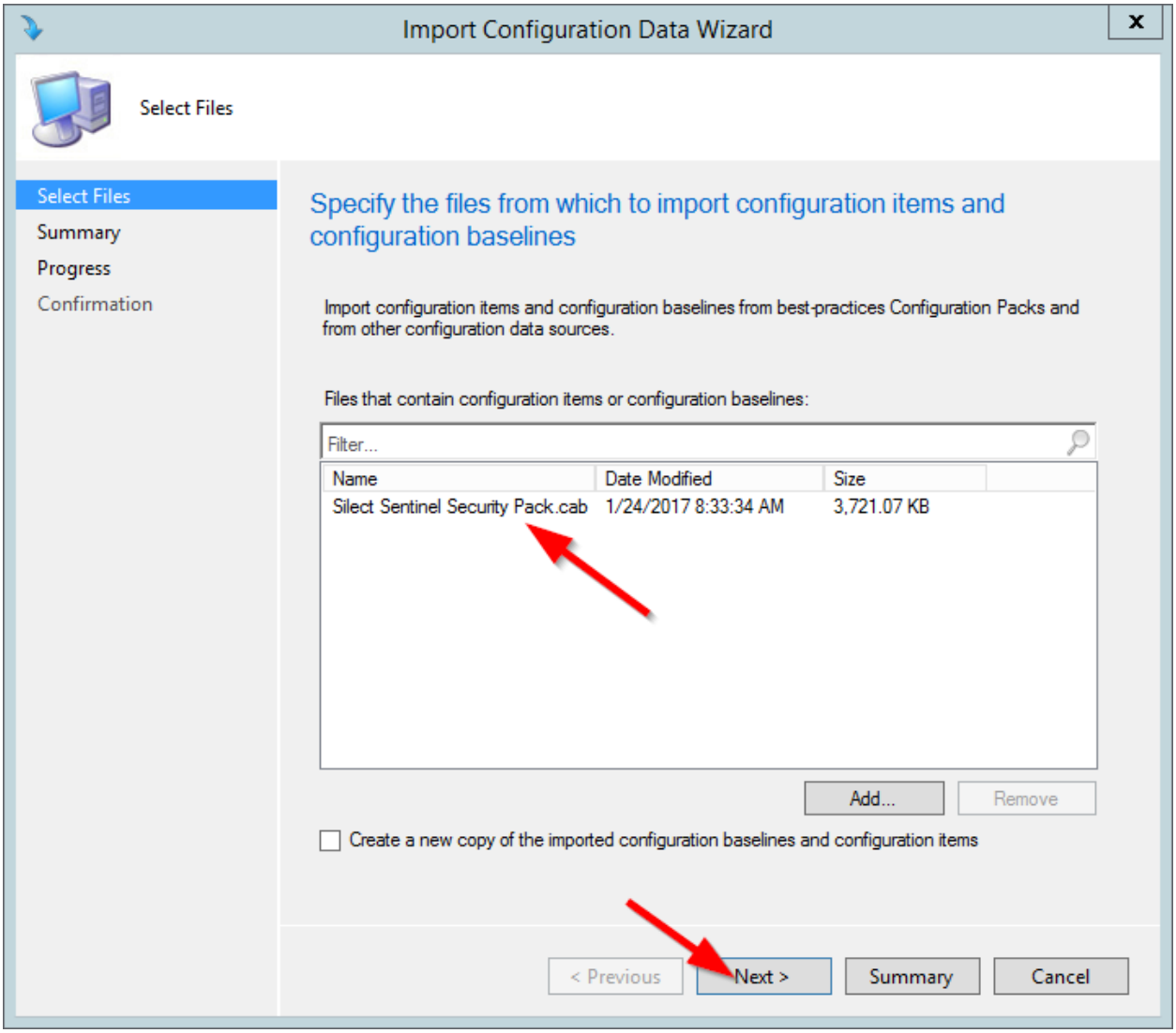


- Step 3: In the **Open** dialog box, navigate to the location where your copy of the Sentinel Security Pack Configuration Pack is stored. The file is named **Silect Sentinel Security Pack.cab**. Select the file, and then click on **Open**. Select **Yes** to confirm that you want to import the file despite not being able to verify its publisher.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

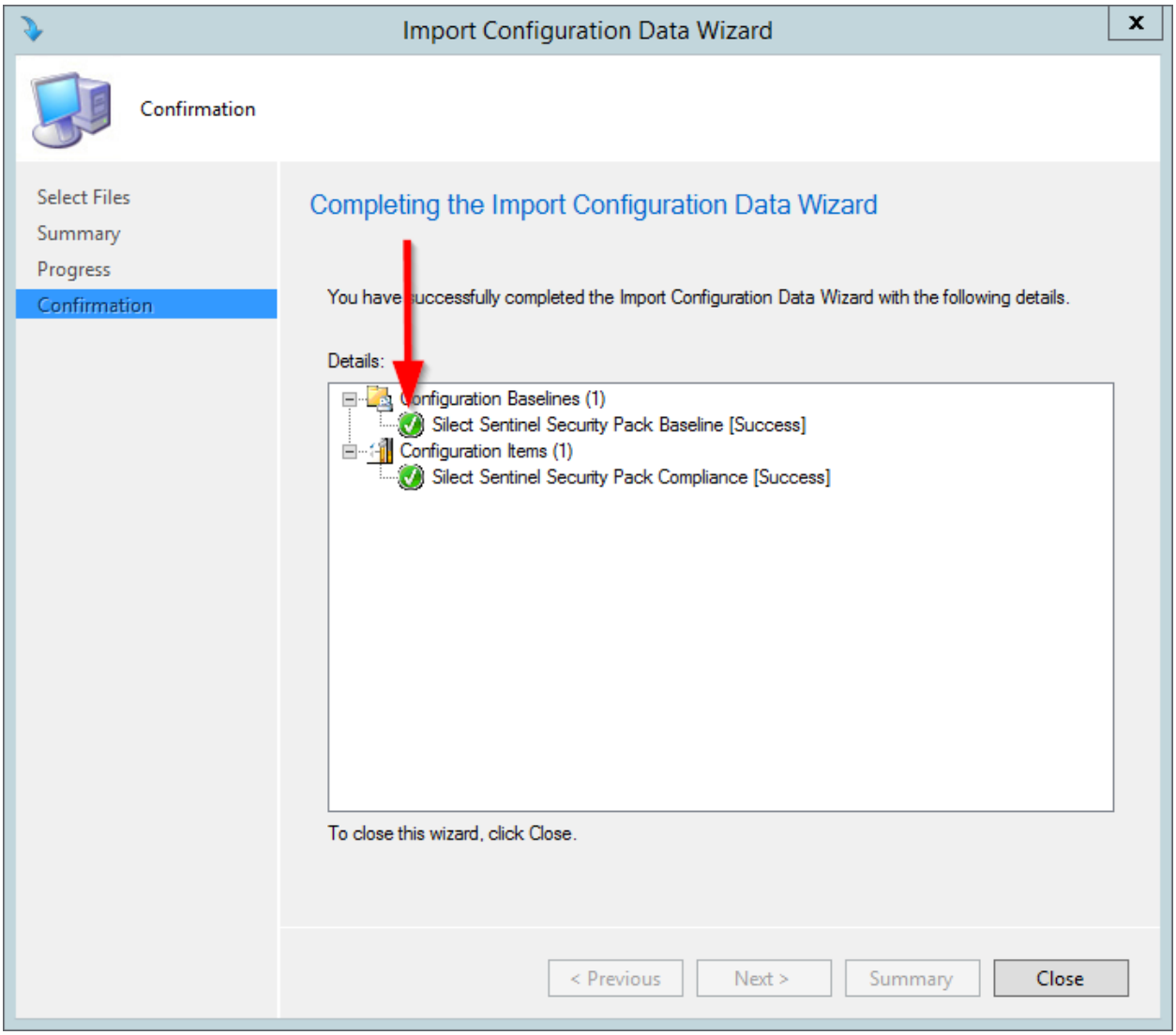


- Step 4: Details of the Configuration Pack will be displayed before importing it. Click on **Next**, and **Next** once more.



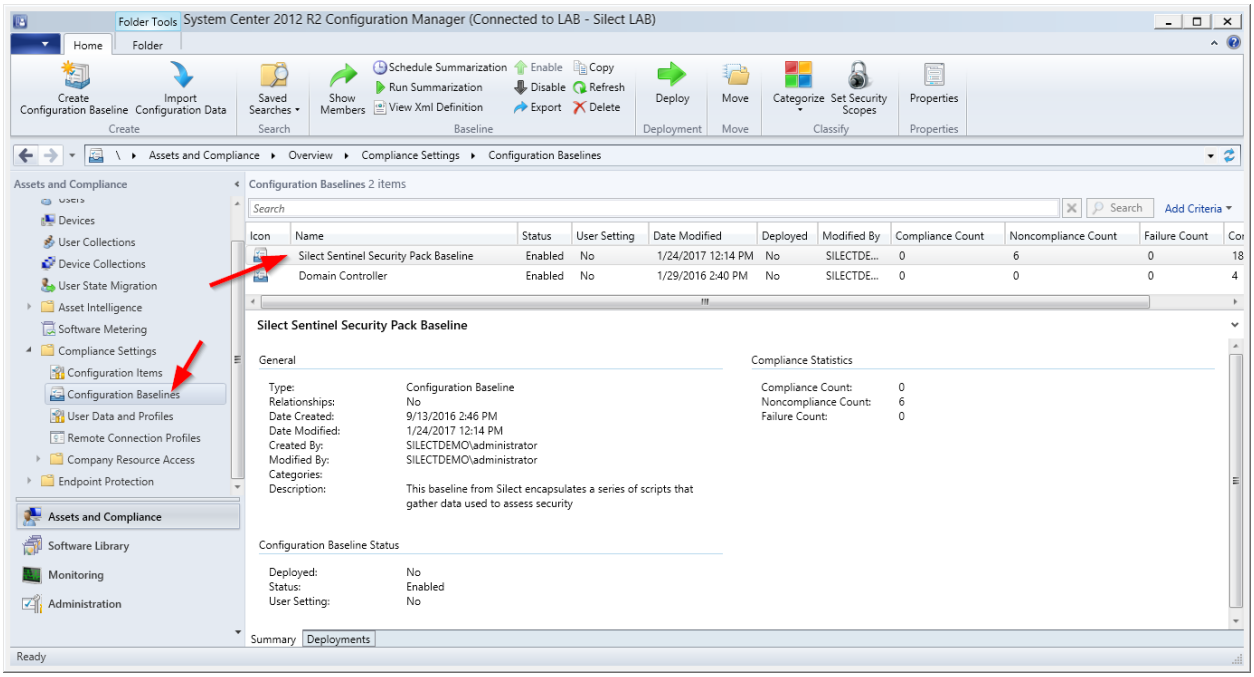
Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

- Step 5: If everything worked correctly, you will see green checkmarks next to the name of the baseline and configuration items contained in the Configuration Pack just imported. If the import process encountered a failure, the dialog box 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 6: Click on **Close**. After a few seconds to a few minutes, depending on the performance of your ConfigMgr environment, the Configuration Baseline will appear in the list as **Silect Sentinel Security Pack Baseline**, if Step 5 above completed successfully.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

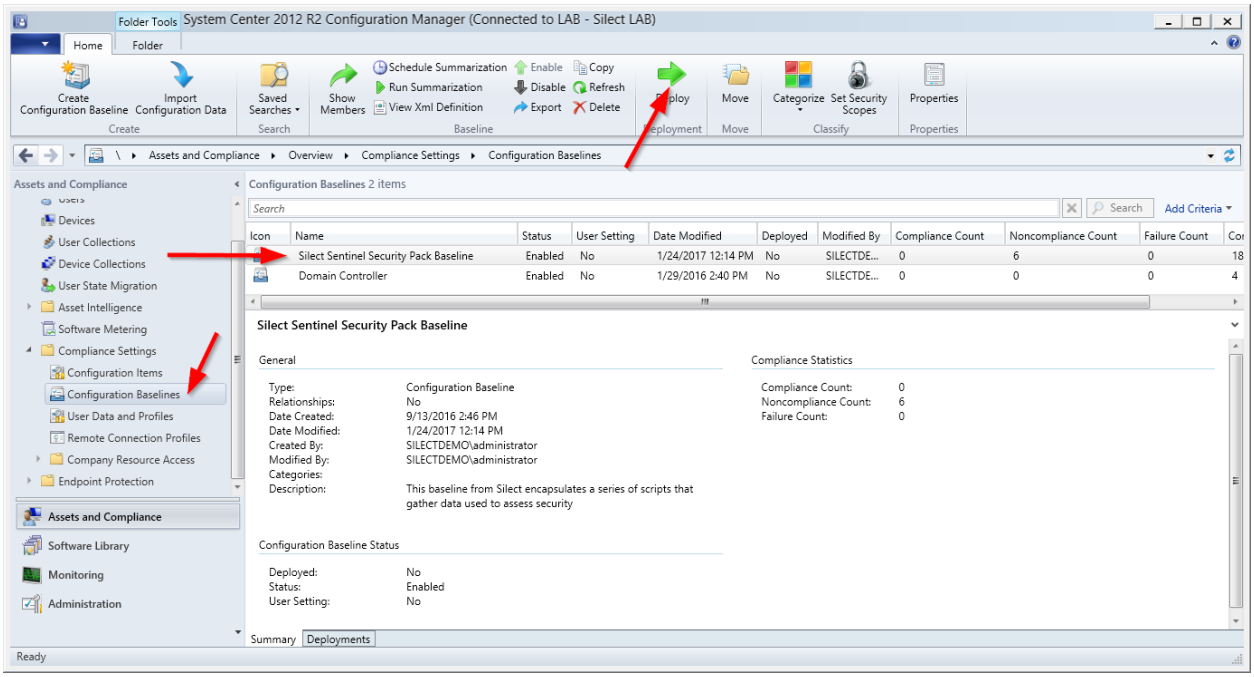


Deploying the Configuration Pack

The Sentinel Security Pack is deployed in the same way you would deploy any other Configuration Pack.

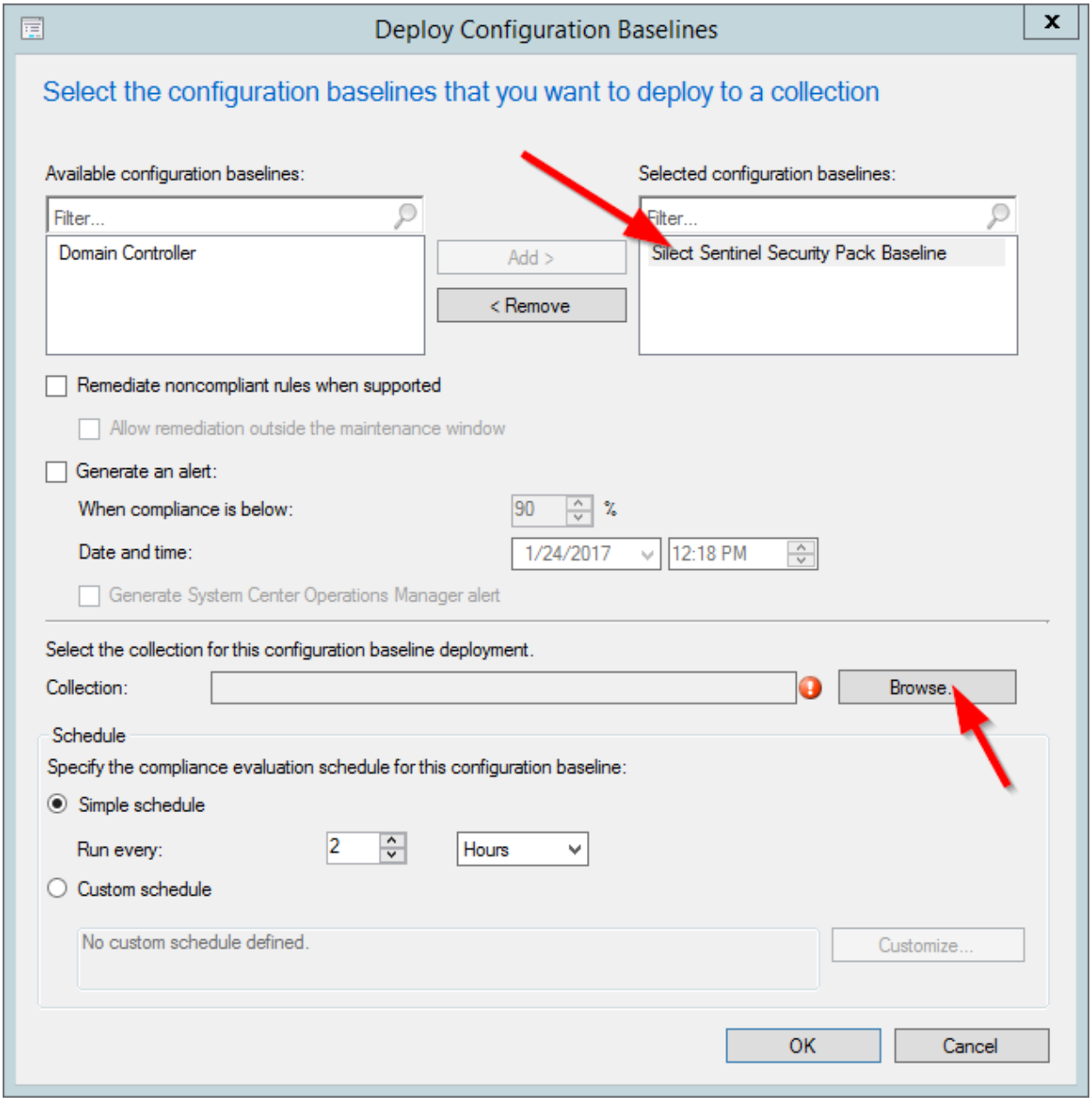
- Step 1: In the ConfigMgr console, go to the **Assets and Compliance** workspace, navigate to **Overview**, **Compliance Settings**, **Configuration Baselines**, and then click on the **Deploy** button on the toolbar.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited



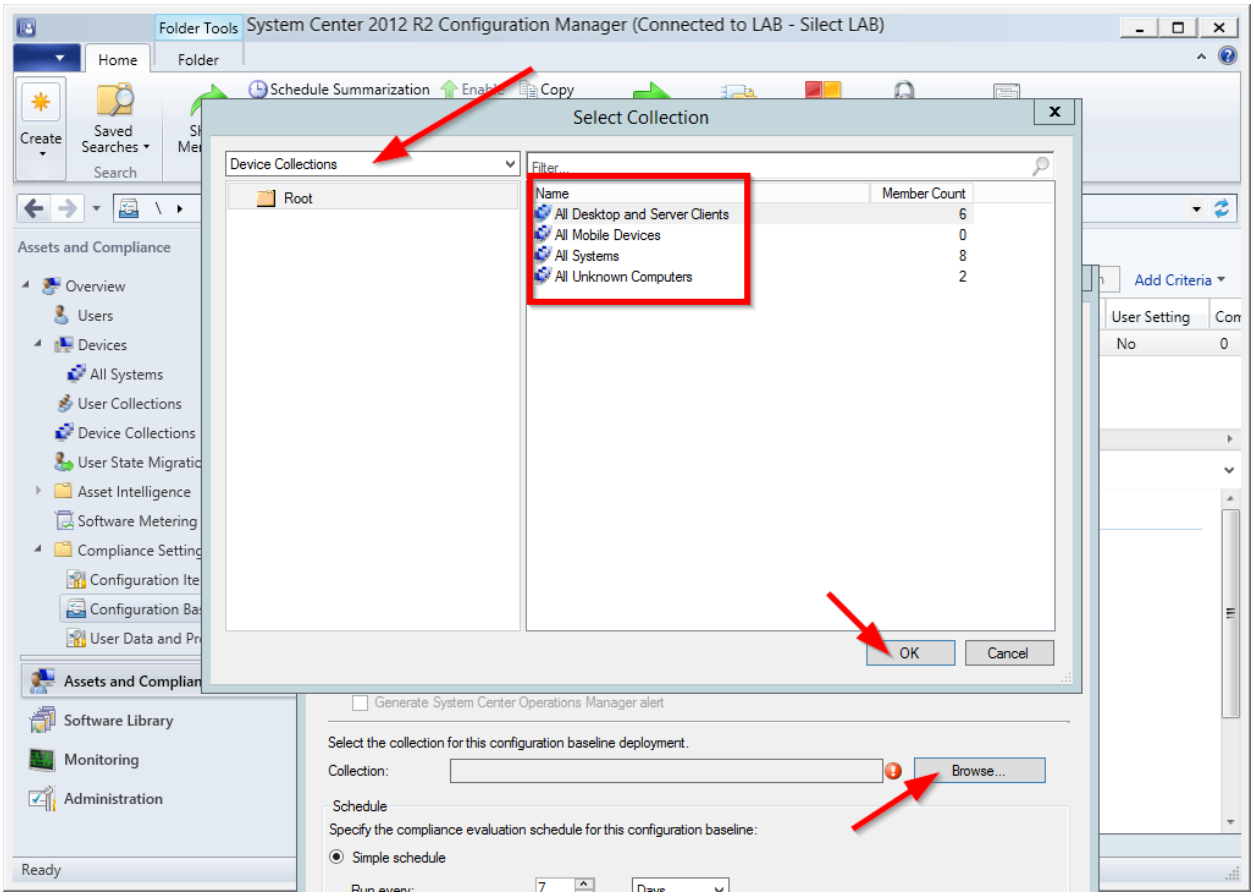
- Step 2: In the **Deploy Configuration Baselines** dialog box, select the **Silect Sentinel Security Pack Baseline** from the **Available Configuration baselines** list on the left and click the **Add** button so it appears in the **Selected configuration baselines** list on the right. After clicking the Add button, the dialog box should appear as follows:

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

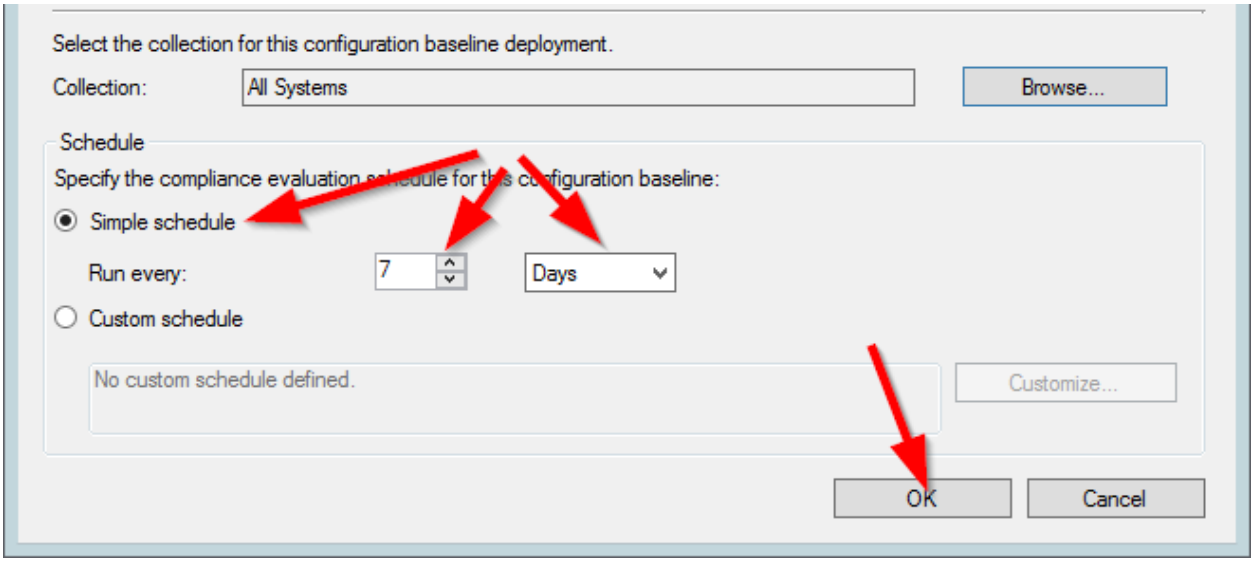


- Step 3: Click on the **Browse** button on the right of the **Collection** text box to bring up the **Selection Collection** dialog box to select which collection the Configuration Pack should be deployed to. Locate the collection, select it from the list on the right, and then click **OK**.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited



- Step 4: Customize the compliance evaluation schedule if you'd like – the default schedule set up by ConfigMgr will evaluate the state of all computers in the collection once every 7 days. Click **OK** to deploy the Configuration Pack to the selected collection.



Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

Using the Sentinel Security Pack

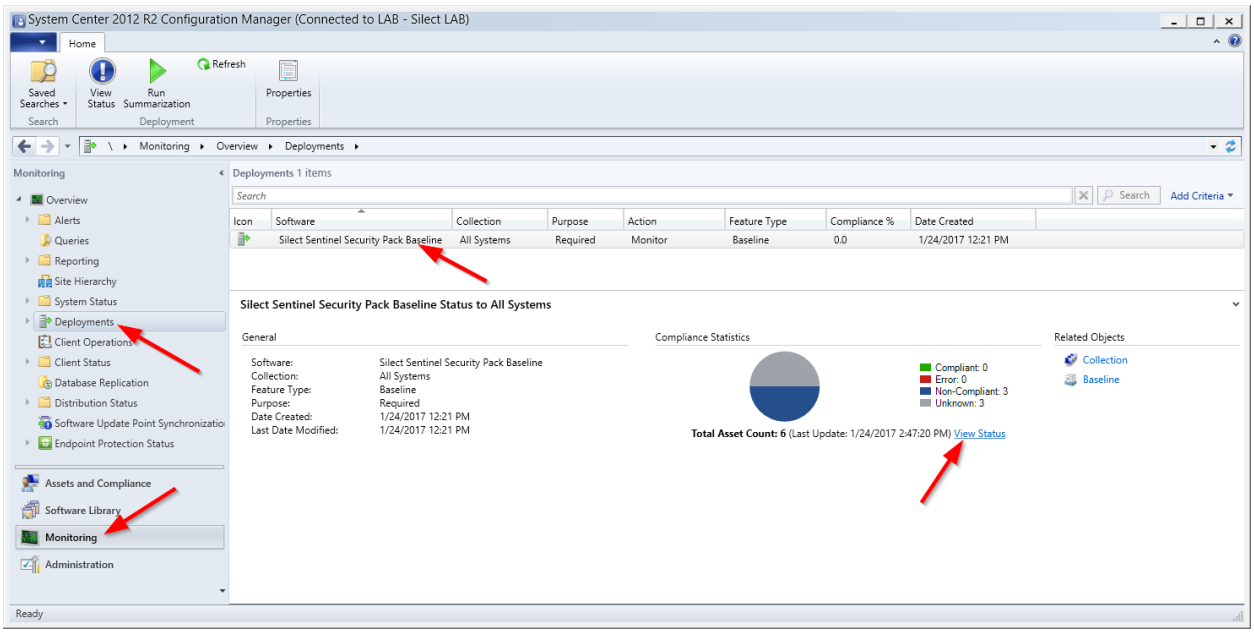
Overview

Once the Sentinel Security Pack has been imported into your ConfigMgr environment, a series of data points used to help determine whether computers are Sentinel-compliant or not are retrieved on a regular basis, through ConfigMgr's *agent*, from all Windows computers that are part of the collection(s) the Configuration Pack has been deployed against. How quickly immediately after importing the Sentinel Security Pack and deploying it you can start seeing some of its data depends on the schedule you have selected and your environment – as is the case with any other Configuration Pack, it could take anywhere between a few minutes to a few hours, or even days, depending on the selected schedule, before some of that data starts trickling in.

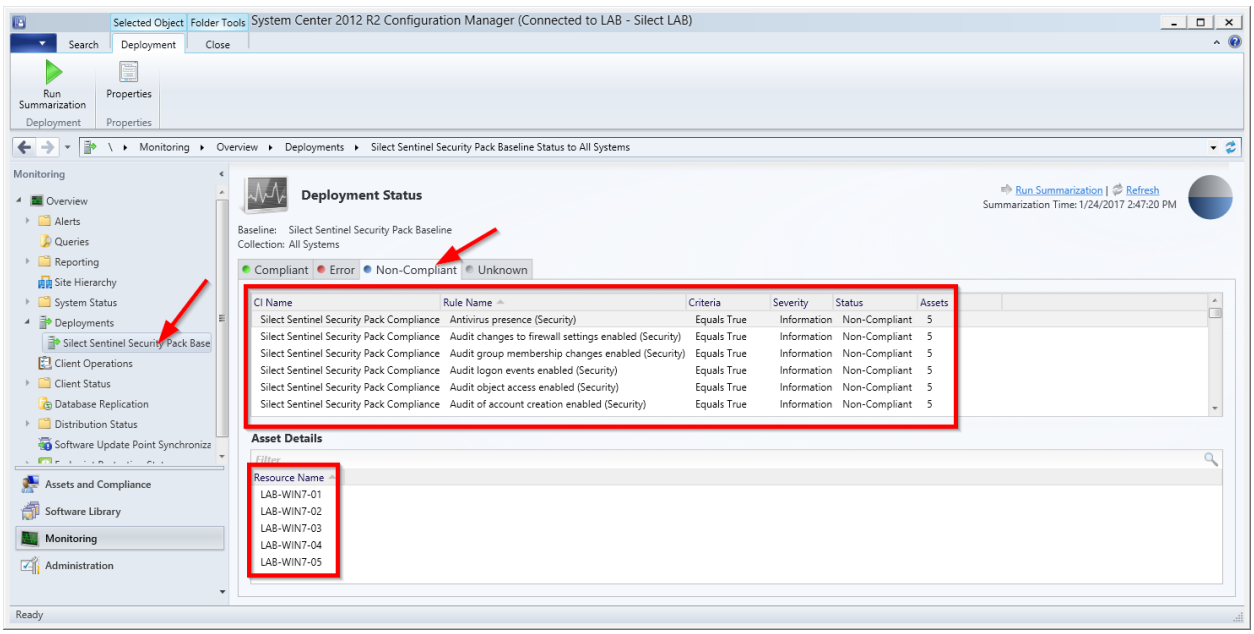
The Deployment Summary View

If you have any familiarity with the ConfigMgr console, you should know that you can get an overview of the compliance state of the Windows computers that are being monitored by going to the **Monitoring** workspace, navigating to **Overview**, **Deployments** and selecting the **Silect Sentinel Security Pack Baseline** entry from the list. While this provides a very high-level summary of the compliance data, you will probably want to view further details by clicking on the **View Status** link.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited



Fully compliant computers will be shown under the **Compliant** tab. Errors encountered by the ConfigMgr agent while attempting to collect compliance data will be detailed under the **Error** tab. Computers in an unknown state—for example, those for which compliance data for the Configuration Pack has not yet been retrieved—will appear under the **Unknown** tab. The most interesting data however will appear under the **Non-Compliant** tab.

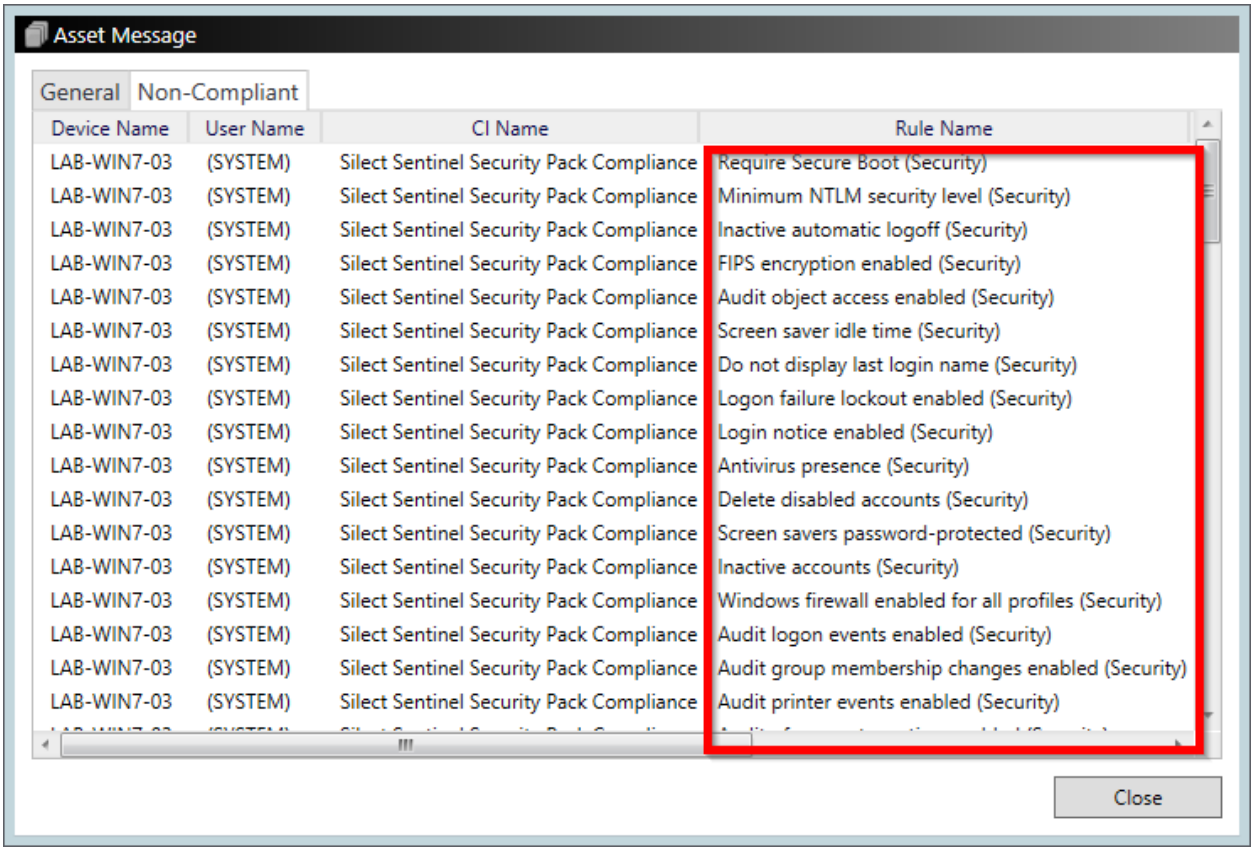


The list that appears immediately under the **Non-Compliant** tab details which *Sentinel Safeguards* have been found to be in a non-compliant state; for each safeguard, the list

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

shows the number of computers, in the **Assets** column, that are not compliant. When a row from this list is selected, the names of the computers that are not compliant for the selected safeguard are shown in the **Asset Details** list.

Note that if you right-click on the name of one of the computers in the **Asset Details** list, a **More Details** menu brings up a window that contains a **Non-Compliant** tab; the list shows all safeguards that have been found to be in a non-compliant state for the selected computer:



Device Name	User Name	CI Name	Rule Name
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Require Secure Boot (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Minimum NTLM security level (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Inactive automatic logoff (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	FIPS encryption enabled (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Audit object access enabled (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Screen saver idle time (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Do not display last login name (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Logon failure lockout enabled (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Login notice enabled (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Antivirus presence (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Delete disabled accounts (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Screen savers password-protected (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Inactive accounts (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Windows firewall enabled for all profiles (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Audit logon events enabled (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Audit group membership changes enabled (Security)
LAB-WIN7-03	(SYSTEM)	Silect Sentinel Security Pack Compliance	Audit printer events enabled (Security)

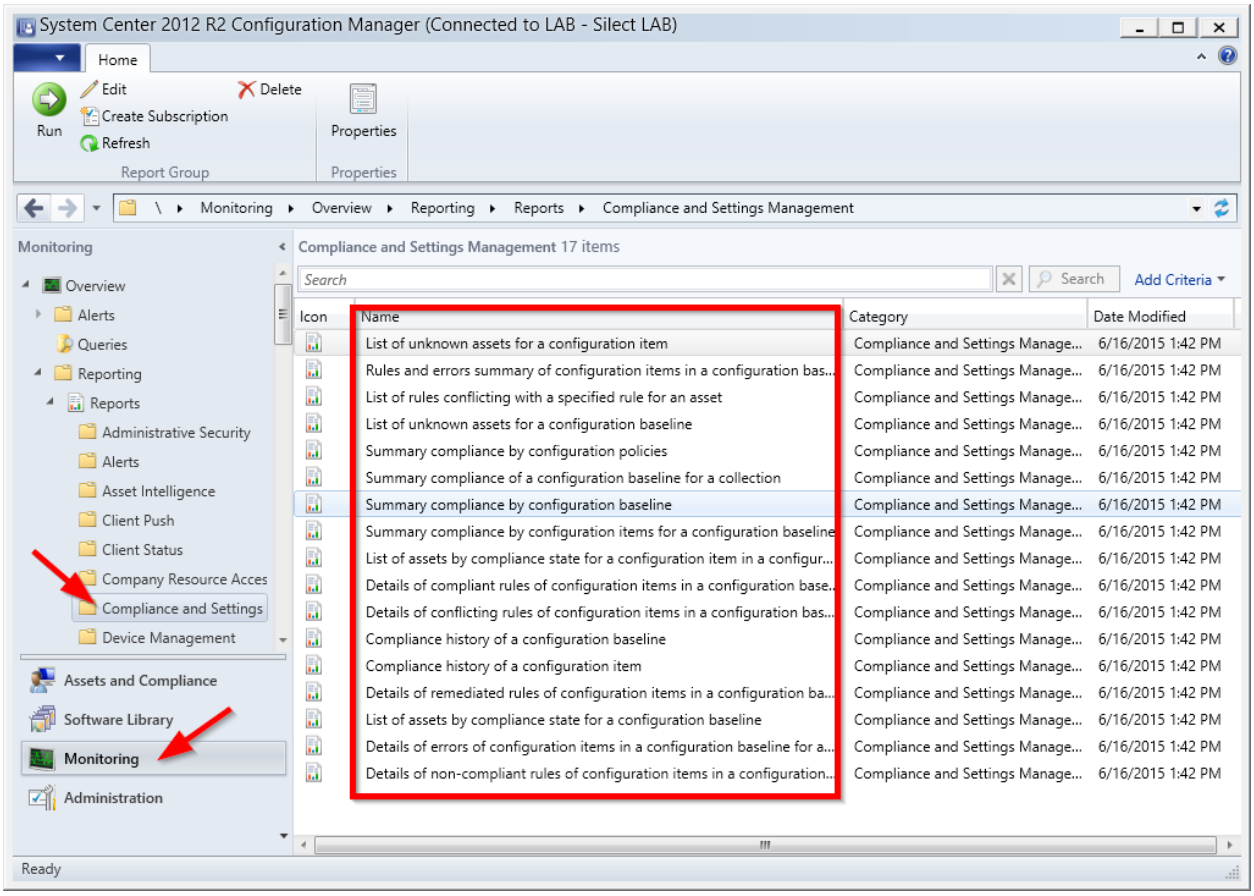
Additional Reports

If your ConfigMgr environment has been configured to include the **Reporting services point** role, ConfigMgr also includes a number of built-in reports that can be used to view details about the data retrieved by the Sentinel Security Pack (and others) in a wide variety of ways. Installation and configuration of this ConfigMgr role, as well as the

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

details of these reports, are beyond the scope of this document—for help on these topics, consult the documentation for your version of ConfigMgr.

To view the reports, go to the **Monitoring** workspace, and then navigate to **Overview**, **Reporting**, and **Reports**. The reports that focus on Configuration Item compliance are located in the **Compliance and Settings** folder.



Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

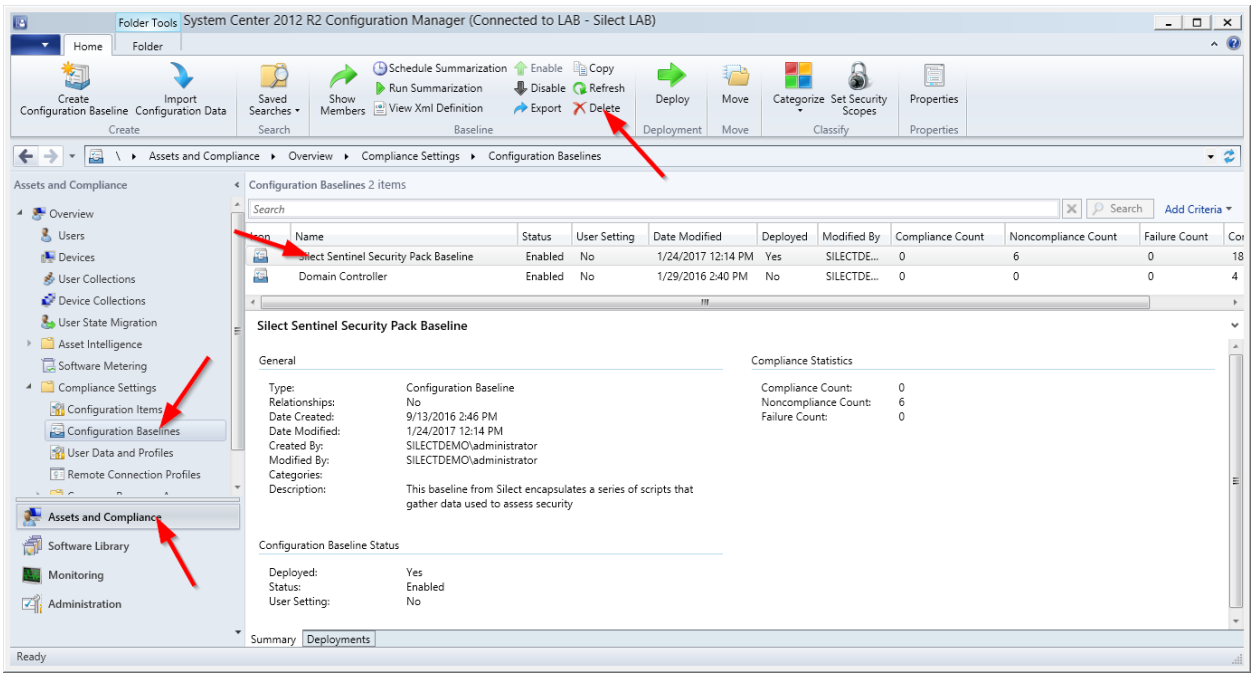
Removing the Sentinel Security Pack

This section describes the steps that need to be taken to completely remove the Sentinel Security Pack.

Removing the Configuration Pack

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

- Step 1: In the ConfigMgr console, go to the **Assets and Compliance** workspace, navigate to **Overview**, **Compliance Settings**, **Configuration Baselines**, and select the **Silect Sentinel Security Pack Baseline** entry from the Configuration Baselines list, and click on the **Delete** button on the toolbar.



- Step 2: When prompted to confirm the removal of the baseline, click **Yes**. After a few seconds to a few minutes, depending on the performance of your ConfigMgr environment, the entry will be removed.

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited

Contacting Technical Support

Before contacting Technical Support, please ensure that you can successfully launch the System Center Configuration 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

Copyright © 2015-2018 Silect Software, Inc. All rights reserved.
Unauthorized reproduction or distribution prohibited