Spirion SDM/SDP – Thales CipherTrust Transparent Encryption Integration Guide

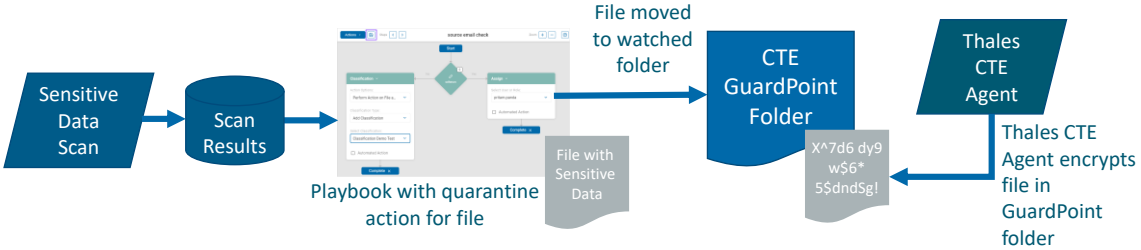
Contents

Introduction 1
Requirements 2
Limitations 2
Important Notes 2
Integration Process 2
STEP 1 – Install the CipherTrust Transparent Encryption Agent 2
STEP 2 – Create the GuardPoint folder on the Windows Endpoint Filesystem 3
STEP 3 – Set Up a GuardPoint on the Windows Endpoint Filesystem 4
STEP 4 – Install the Spirion Agent and Connect to the Console 6
STEP 5a – In Sensitive Data Platform: Create a Spirion SDP Playbook 6
STEP 6a – In Sensitive Data Platform: Create a Spirion SDP Scan 9
STEP 5b – In Sensitive Data Manager: Create a SDM Workflow 15
STEP 6b – In Sensitive Data Manager: Create a Spirion SDM Scan 18

Introduction

Thales and Spirion are helping organizations stay ahead of shifts in the modern data risk landscape by delivering solutions that focus directly on the data without reliance on an increasingly porous security perimeter. Thales CipherTrust Transparent Encryption (CTE) allows IT organizations to easily control access to sensitive or restricted documents, enabling fine-grained and reversable data access governance.

Thales CTE integrates with Spirion's on-premises Sensitive Data Manager (SDM) and SaaS Sensitive Data Platform (SDP) using a quarantine action to move a file discovered by SDM or SDP to contain sensitive or restricted data to a CipherTrust Transparent Encryption GuardPoint folder where it is encrypted.



Requirements

- Thales CipherTrust Transparent Encryption version 7.2.0 or later.
- Spirion products – one of:
    - On-Premises: Spirion Sensitive Data Manager version 12.4 or later.
    - SaaS/Cloud: Spirion Sensitive Data Platform version 22.Q1.3 or later.

This Integration Guide was released in May 2022. Check the Spirion Customer Support Portal for updates.

Limitations

This initial integration has the following limitations:

1. It only supports unstructured data (files) located in a file system accessible to both the Spirion and Thales agent software.
2. It requires remediation via SDM Workflows or SDP Playbooks – i.e., it will not encrypt a file when classified via the Spirion Office or File Explorer plug-ins as those tools do not yet have the ability to quarantine a file upon classification.
3. It currently only works for Windows endpoints, including synced copies of cloud repository files stored on the endpoint, along with Windows-accessible file servers.
4. There is no support yet for macOS endpoints or for encrypting directly in cloud repositories.

Important Notes

1. This guide was published in April 2022; updated guides will be made available in the Spirion Customer Support Portal Knowledgebase.
2. These instructions are meant to be used by a trained SDM or SDP administrators. They are intended to illustrate how to integrate Spirion and Thales products as proof of concept, not as a product-level guide to a scaled-up implementation.
3. Please ensure you test in a small test environment before implementing in production.
4. If you need help, reach out to Spirion's Support team, or contact your Customer Success Manager via Spirion's Customer Support Portal.

Integration Process

STEP 1 – Install the CipherTrust Transparent Encryption Agent

Follow the "CTE Agent for Windows Quick Start Guide," Chapter 3 – "Installation Prerequisites" and "Installing and Registering CTE" to install the CTE Agent on a Windows endpoint in the Thales :

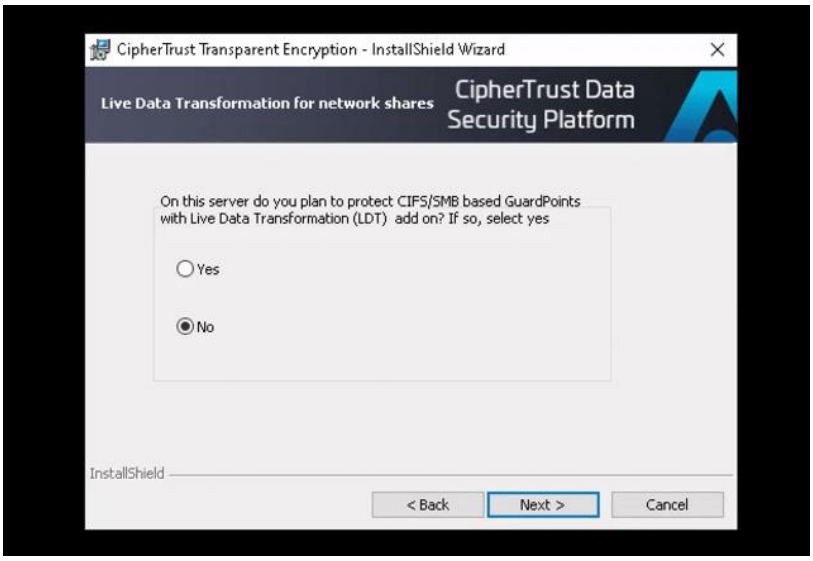
- CTE Agent for Windows Quick Start Guide

Additional information on creating and managing access policies to support the Spirion integration can be found at these Thales documentation links:

- CipherTrust Manager: CTE Administration, Managing Policies
- CipherTrust Manager: Managing Policies, Modifying Policies and Rules
- CipherTrust UserSpace Administration: Access Policies
- CipherTrust Transparent Encryption (CTE) Documentation Set

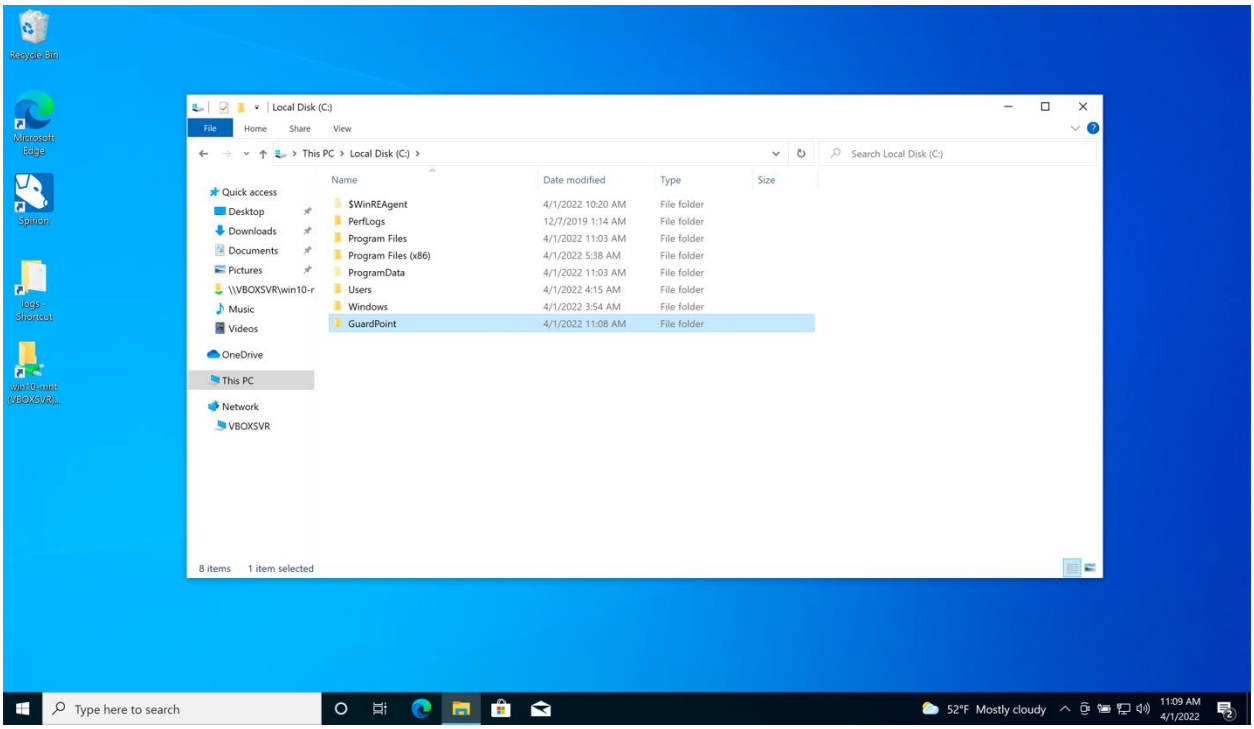
Important Note:

During the InstallShield Wizard process, ensure to select “No” when prompted to “protect CIFS/SMB based GuardPoints with Live Data Transformation (LDT) add on” as shown below:



STEP 2 – Create the GuardPoint folder on the Windows Endpoint Filesystem

On the Windows endpoint filesystem, create a folder at C:\GuardPoint.

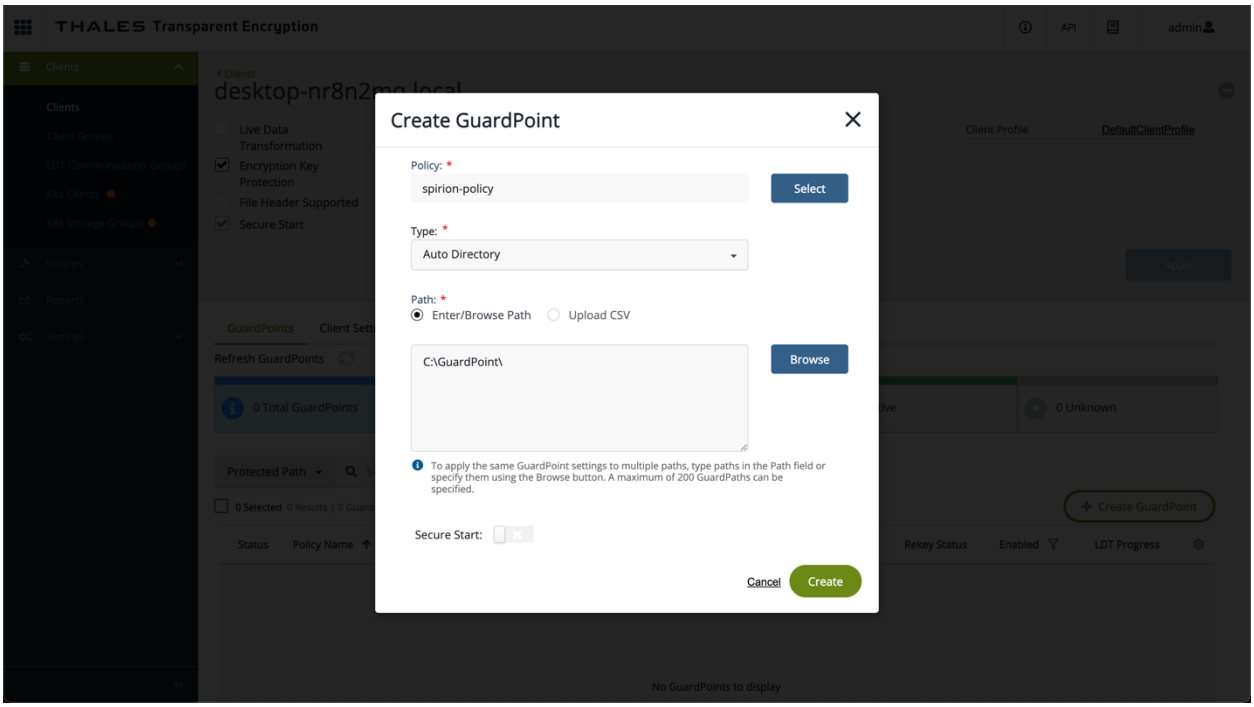


STEP 3 – Set Up a GuardPoint on the Windows Endpoint Filesystem

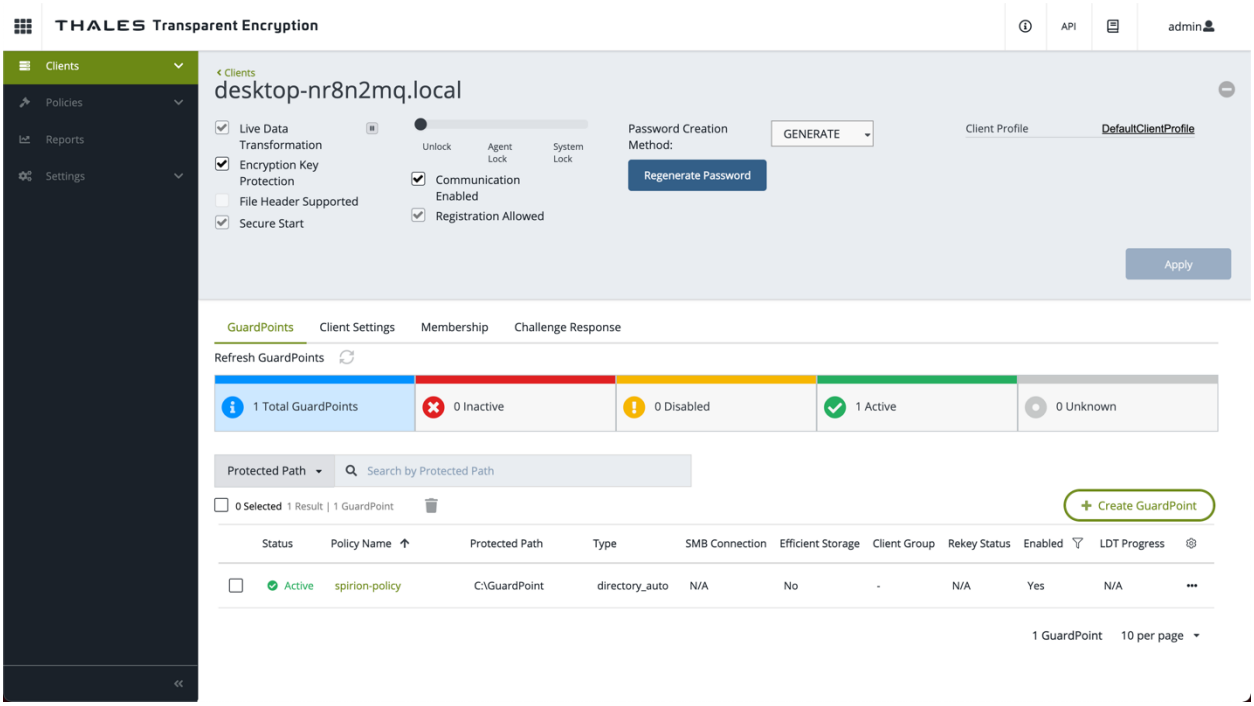
Follow the “CTE Agent for Windows Quick Start Guide”, Chapter 3 – “Guarding a Device with CipherTrust Manager” to set up a GuardPoint on a Windows endpoint.

Important Note:

For the purposes of this guide, when you reach the GuardPoint creation wizard, set the GuardPoint “Path” to C:\GuardPoint\



You should now have an active GuardPoint at C:\GuardPoint on your Windows endpoint filesystem.



STEP 4 – Install the Spirion Agent and Connect to the Console

This guide assumes you have a working installation of Spirion's SDM or SDP products. Make sure to follow this guide to configure and register the Spirion Agent on your Windows endpoints:
https://docs.spirion.com/Content/Sensitive%20Data%20Platform/Platform/Agents/Working%20with%20Registration.htm

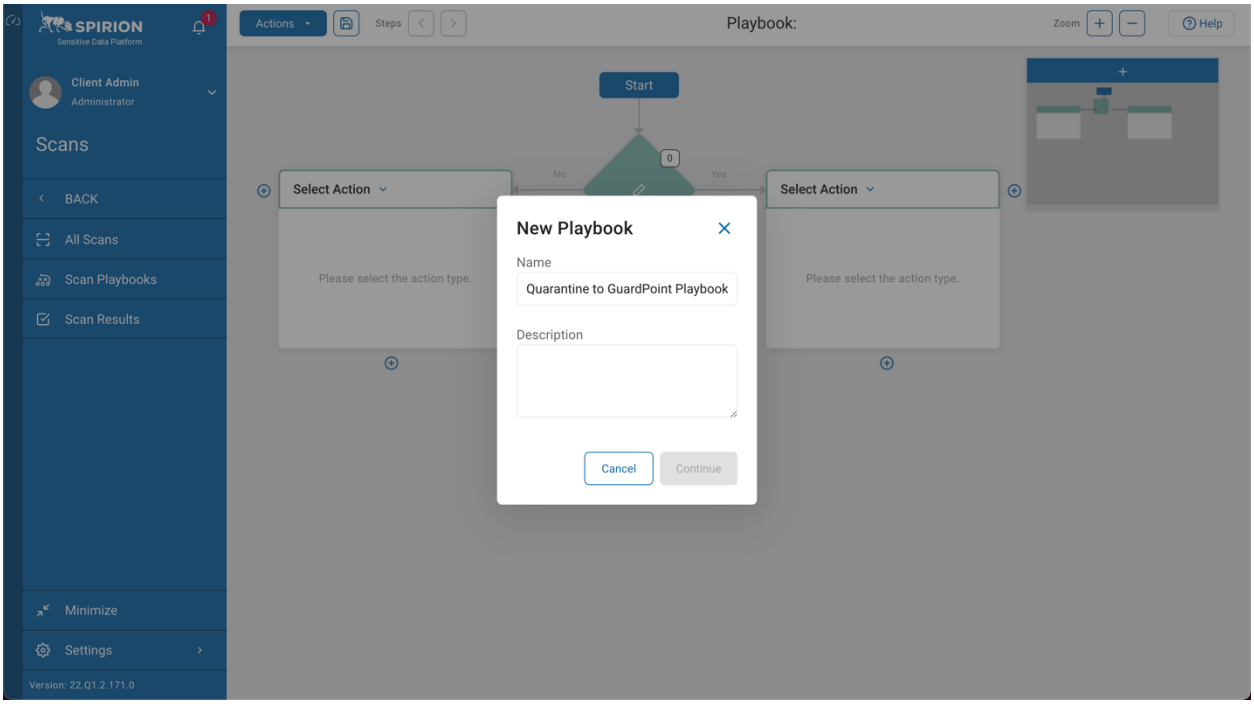
STEP 5a – In Sensitive Data Platform: Create a Spirion SDP Playbook

If using Sensitive Data Platform, click on "Scans" and then click on "Scan Playbooks" on the left side menu.

Towards the top right corner, click on "+ Add Playbook"

Enter a name and a description for the playbook.

Click "Continue."



Click on the edit icon in the center of the first decision point.

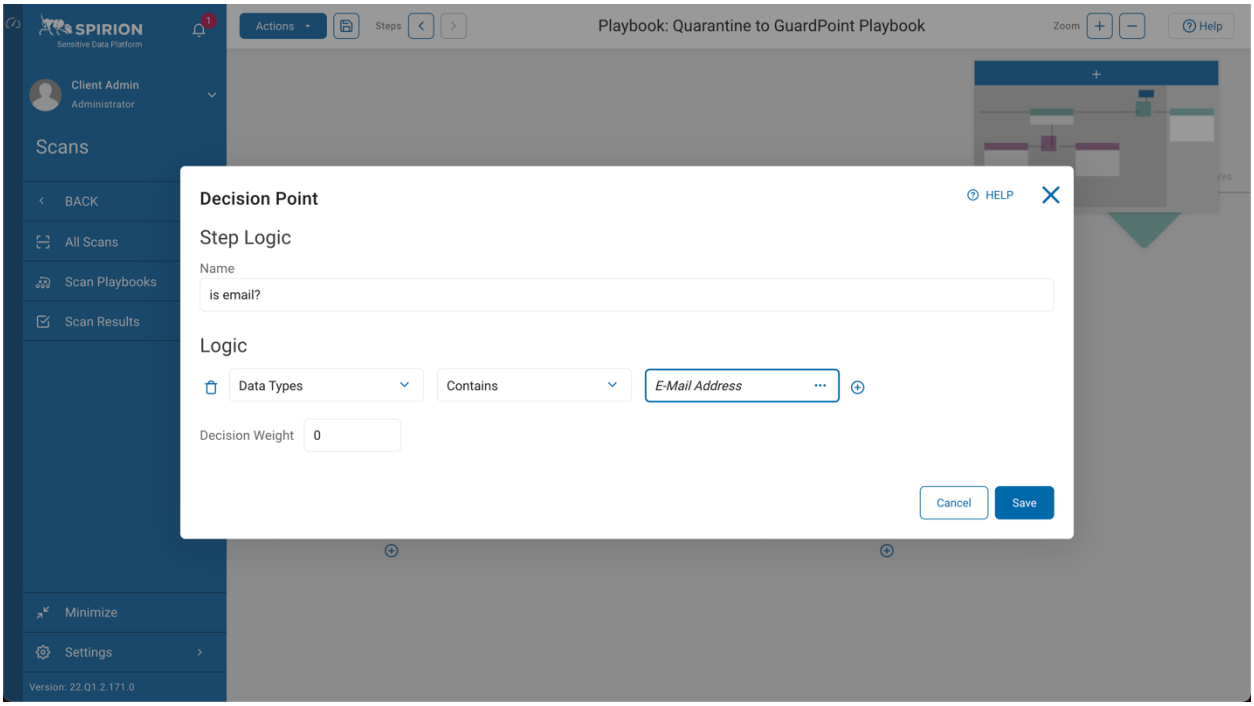
Enter a name for the decision point.

Under Logic, for the left-most drop-down menu, select "Data Types."

Under Logic, for the second drop-down from the left, select "Contains."

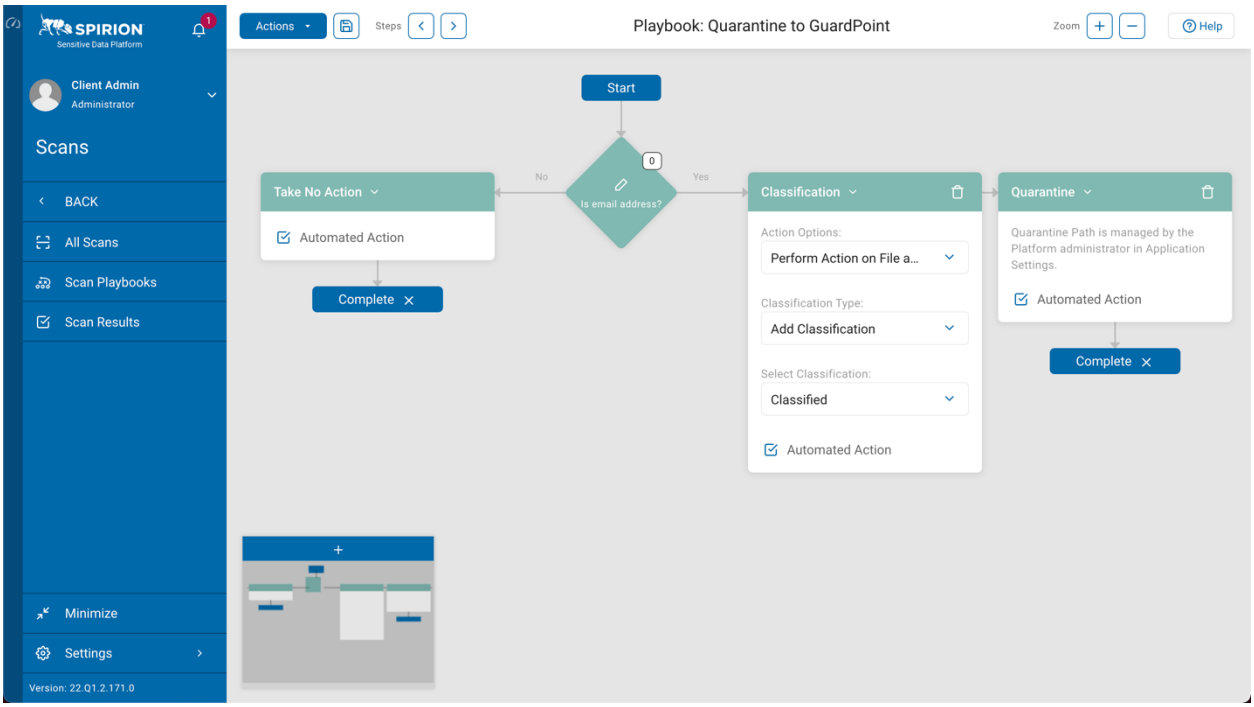
Under Logic, for the right-most box, click on the three dots and select “E-Mail Address.”

Click on “Save”.”



To configure the playbook as shown in the below image.

Click on the “Save” icon (hint: to the left of the “Actions” button).



Click on the “Actions” drop-down button.

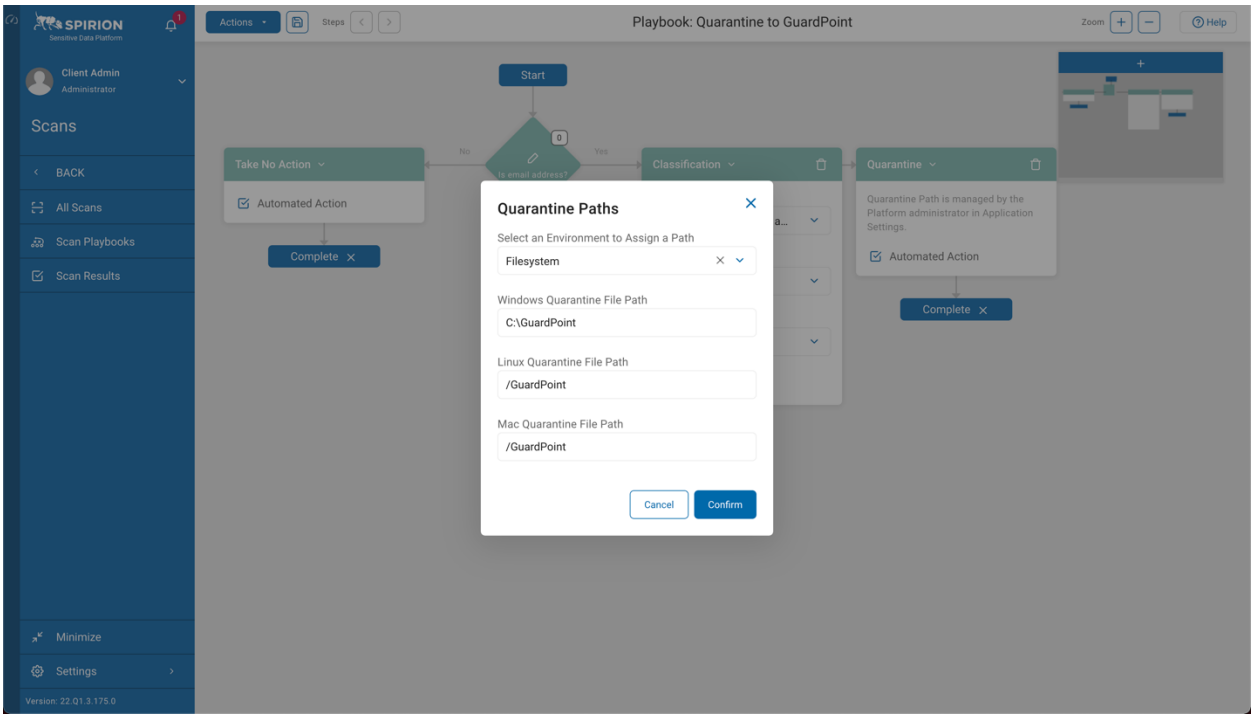
From the “Actions” drop-down, click on “Manage Quarantine Path.”

Under “Select an Environment to Assign a Path,” select “Filesystem”

Under “Windows Quarantine File Path,” enter the path C:\GuardPoint.

Click “Confirm.”

Once again, click on the “Save” icon (hint: to the left of the “Actions” button).



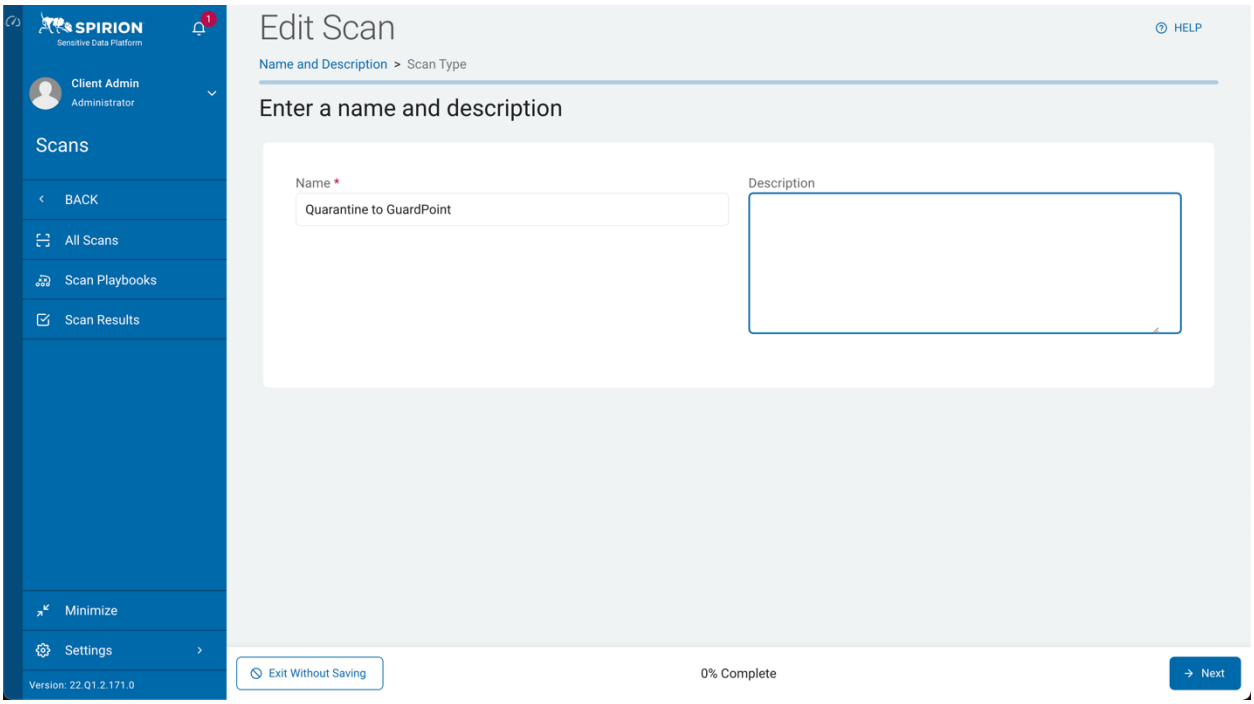
STEP 6a – In Sensitive Data Platform: Create a Spirion SDP Scan

If using Sensitive Data Platform, click on “Scans” on the left side menu.

Towards the right top corner, click on “+ Add Scan.”

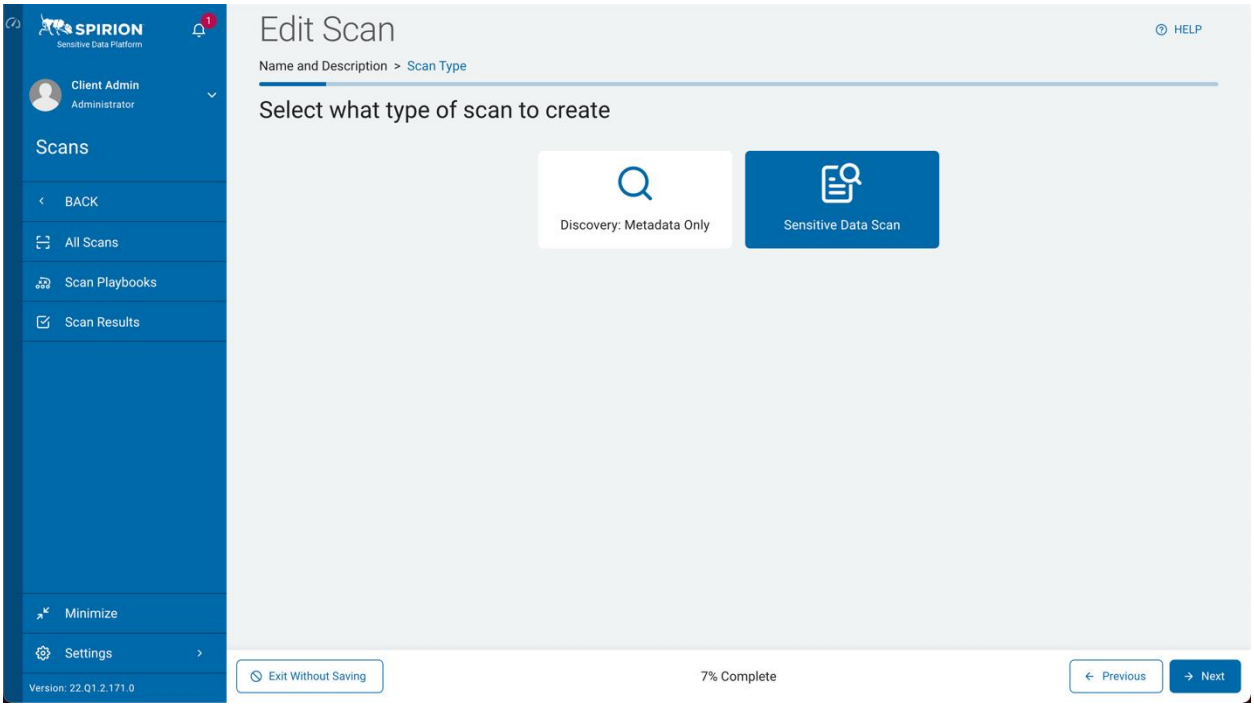
Enter a name and an optional description for the new scan.

Click on “Next”.



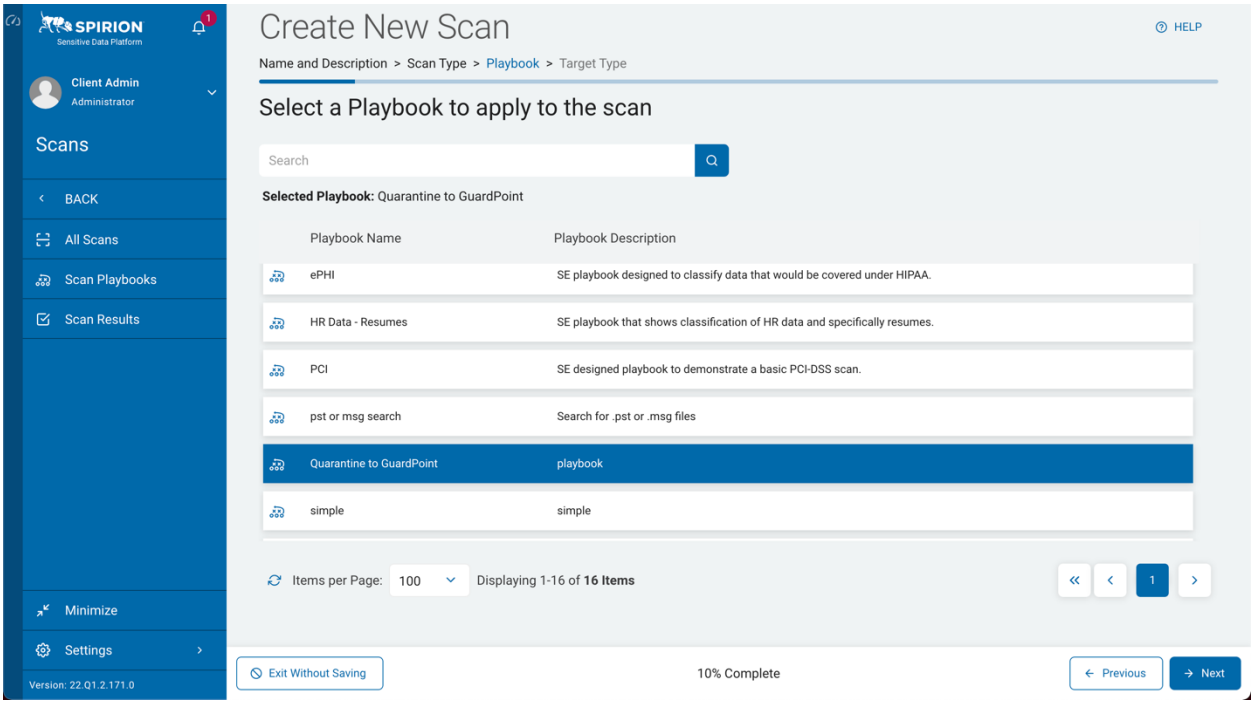
Select “Sensitive Data Scan.”

Click on “Next.”



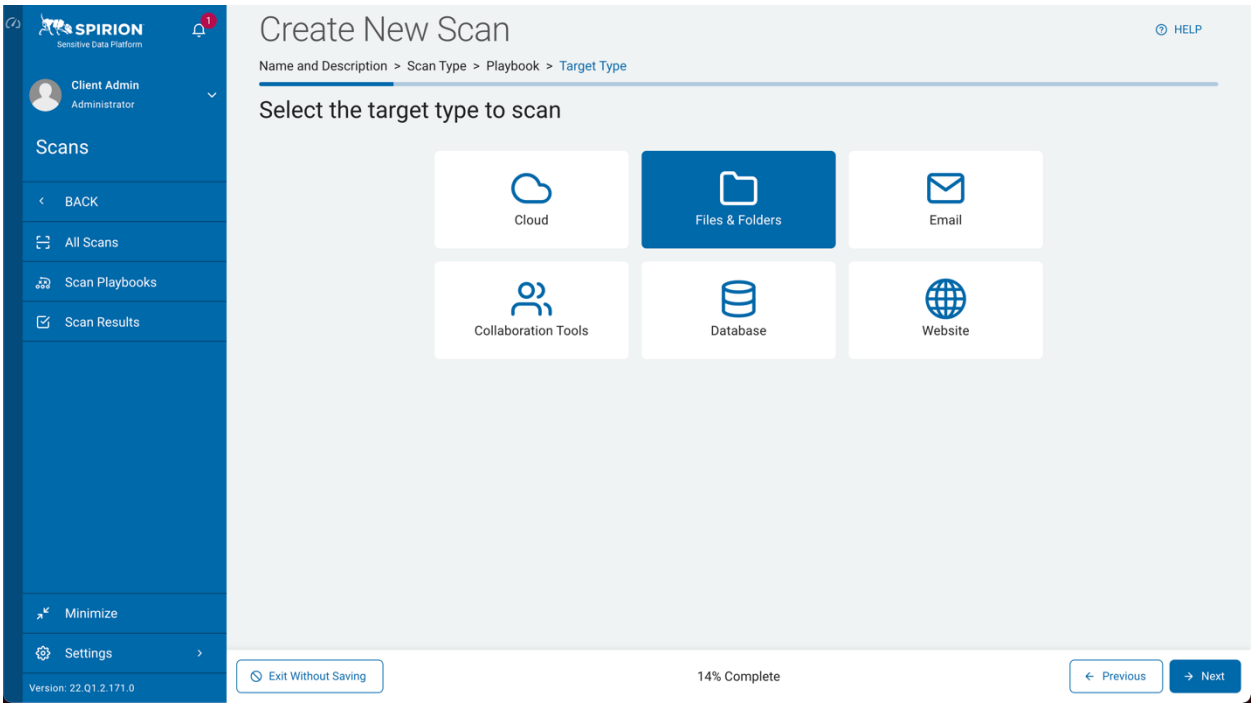
Select the playbook you just created as described by this guide.

Click on “Next.”



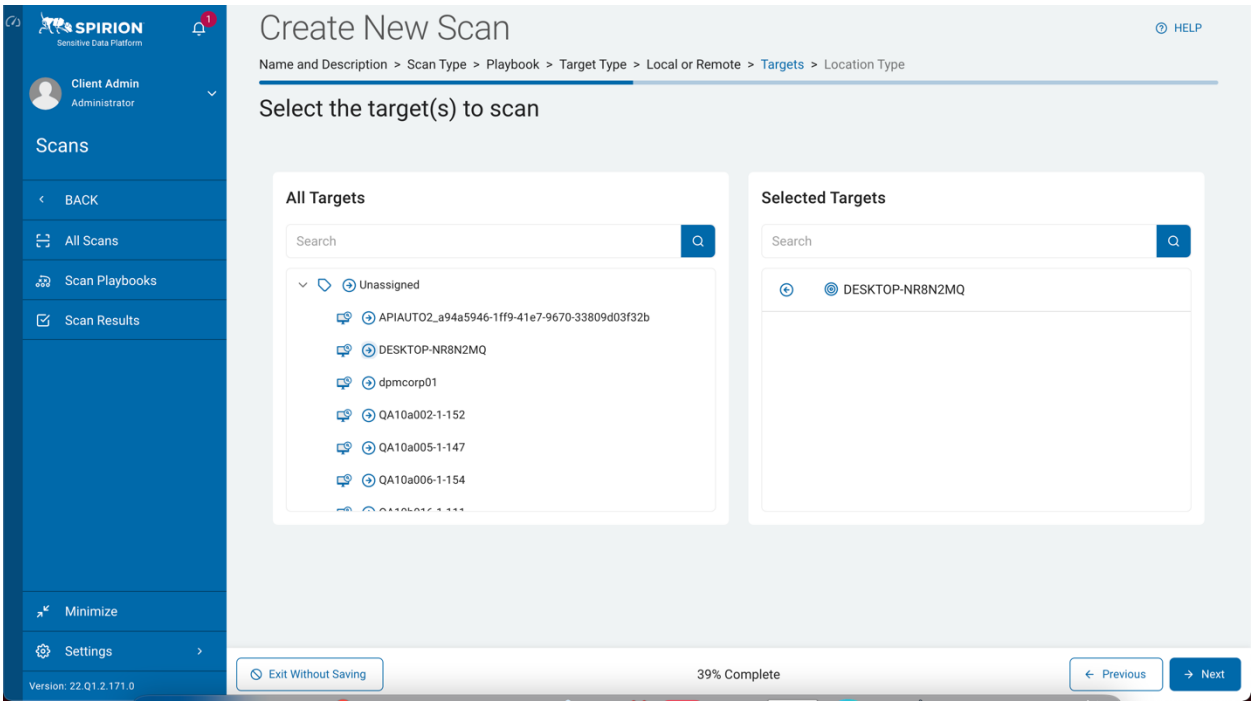
Select the “Files & Folders” tile.

Click on “Next.”



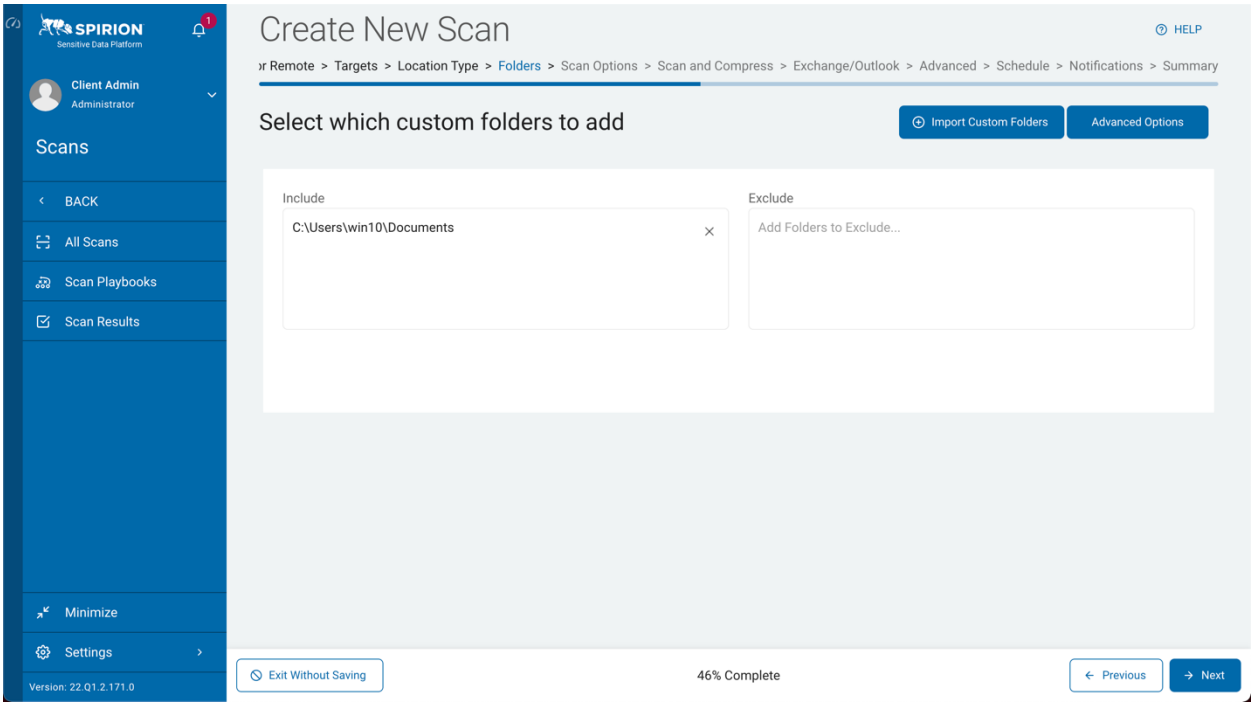
Ensure your Windows Endpoint Agent is under “Selected Targets.”

Click “Next.”



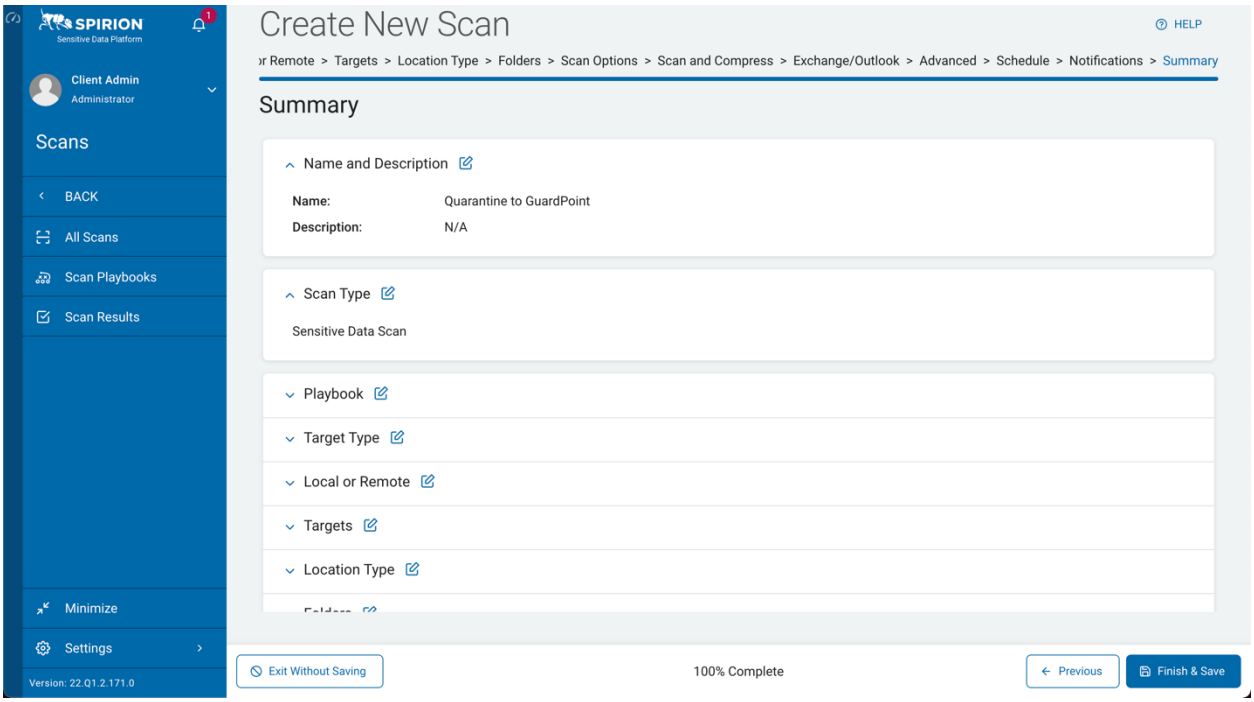
Under “Include,” enter the path to your Windows endpoint user’s Documents folder.

Click on “Next.”



For the Remainder of the sections in the Scan wizard, leave all settings at their default values.

At the “Summary” page, click on “Finish & Save.”

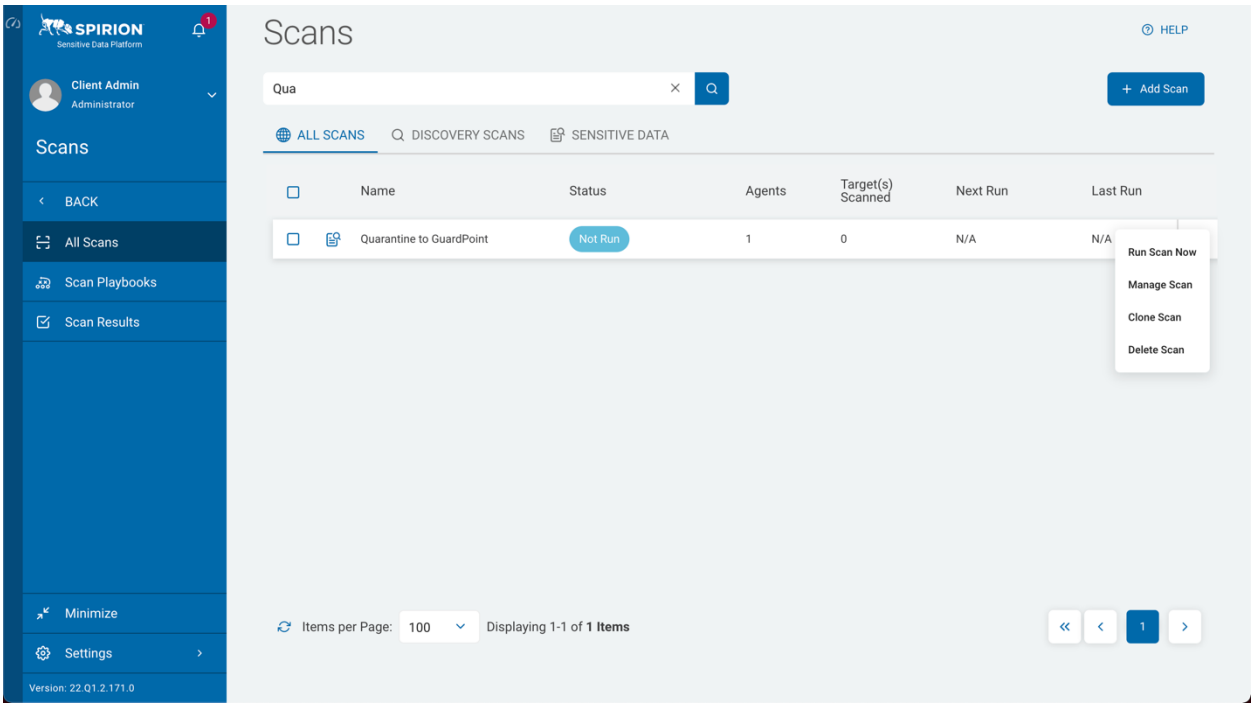


Optional:

Create a file called “email.txt” in the endpoint user’s Documents folder. Edit the file and add an email address “poochy@spirion.com.” Save and close the file.

On the “Scans” page, click on the three dots on the left side of the new scan and click on “Run Scan Now.”

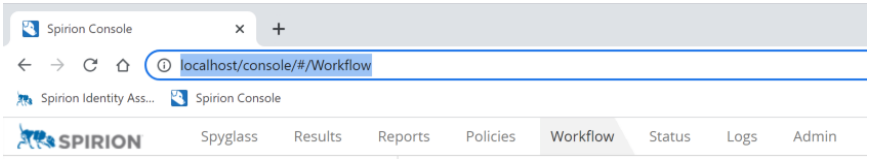
If files exist in the user’s “Documents” directory that contain an email address, those files will be moved to the configured GuardPoint at C:\GuardPoint and the CTE Agent will transparently encrypt them.



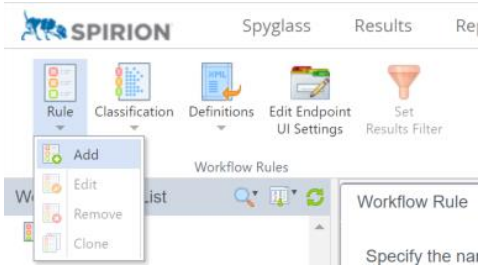
STEP 5b – In Sensitive Data Manager: Create a SDM Workflow

If using Sensitive Data Manager, first create a Workflow to process scan results:

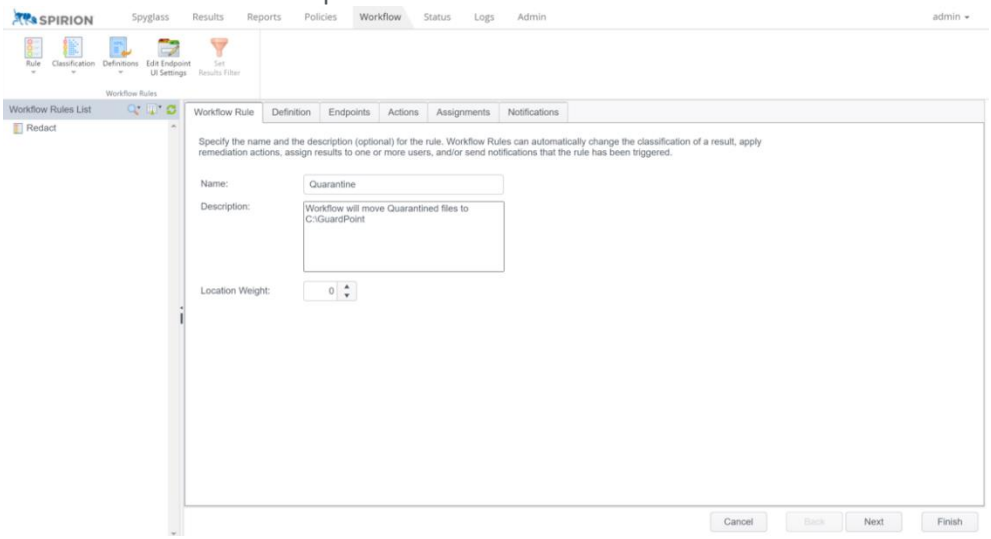
1. Login to SDM Console.
2. Click the “Workflow” tab.



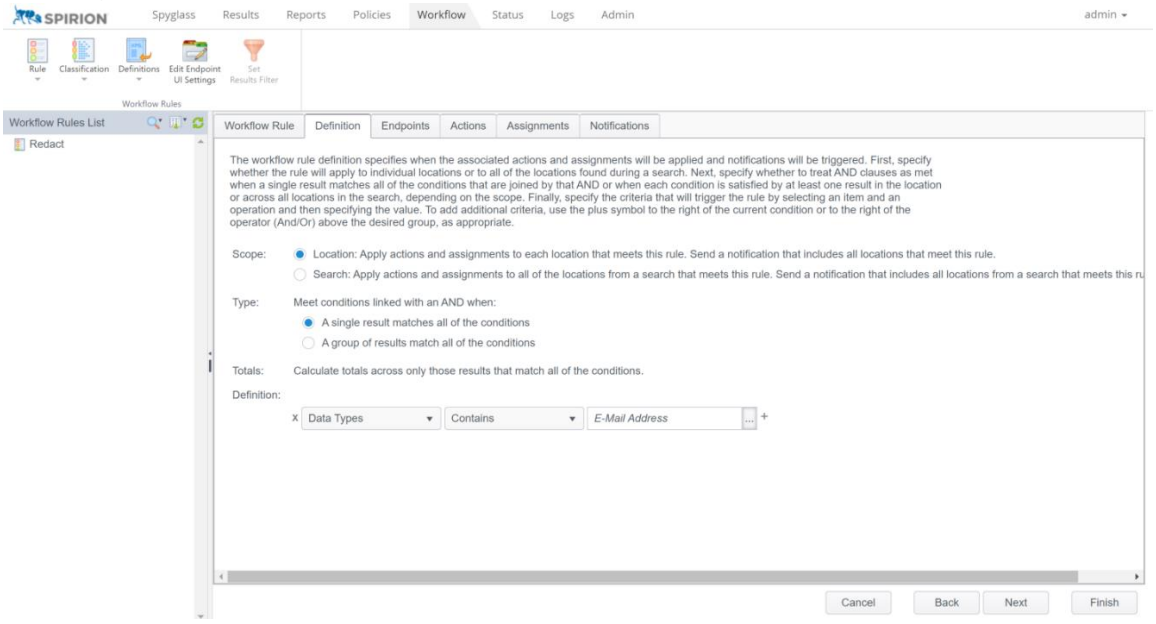
3. Select “Rule / Add.”



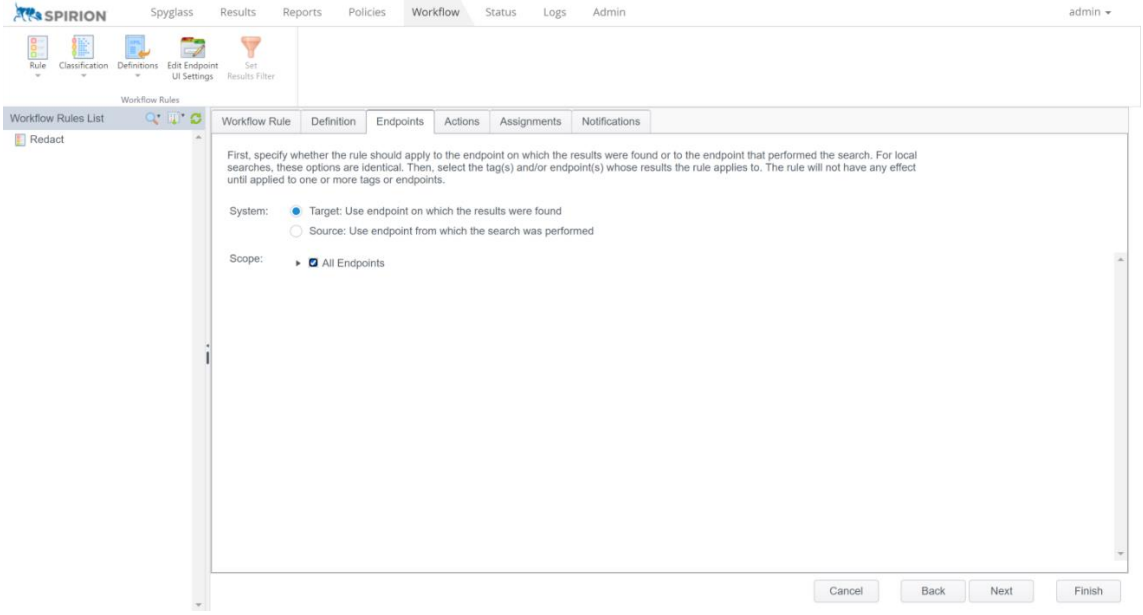
4. Enter the Name and Description of the Workflow.



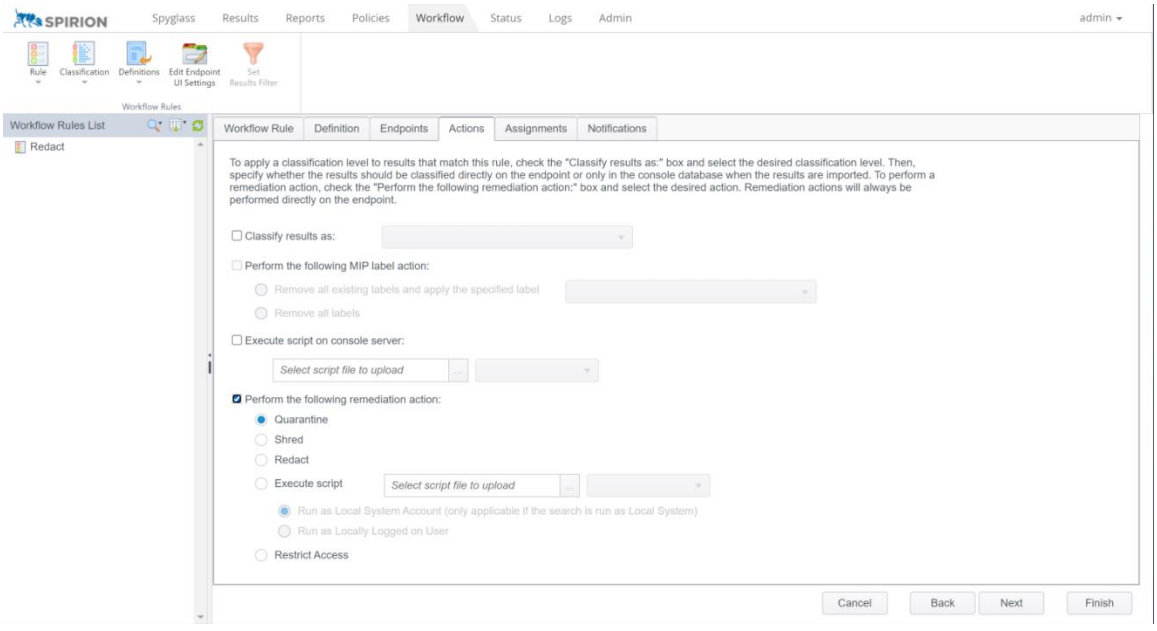
5. Click “Next” and create the Workflow Definition (Data Types | Contains | E-Mail Address).



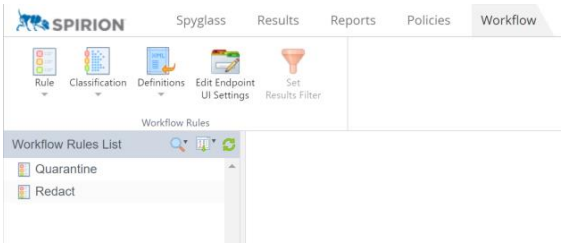
6. Click “Next” and proceed to the Endpoints tab (Select All Endpoints).



7. Click “Next” and proceed to the “Actions” tab and select “Perform the following remediation” and click the radio button for “Quarantine.”



8. Click Finish and see that the Quarantine workflow was added to the list



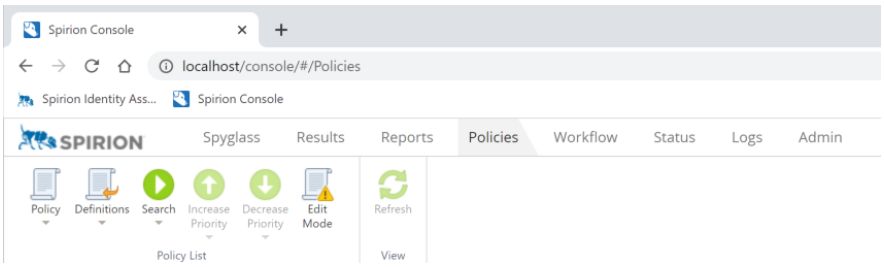
STEP 6b – In Sensitive Data Manager: Create a Spirion SDM Scan

If using Sensitive Data Manager, next create a Scan that uses the previously created:

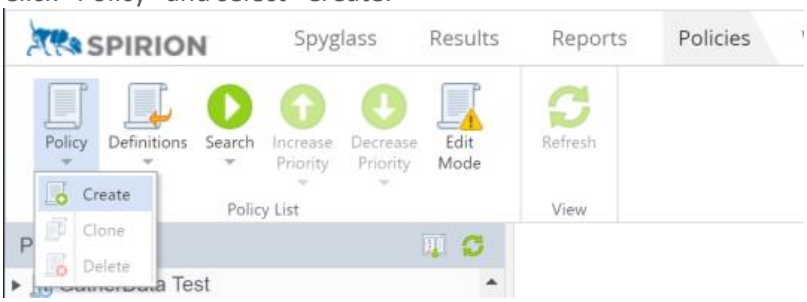
Important Note:

The following assumes that the policy being created is using the settings defined in the Default policy.

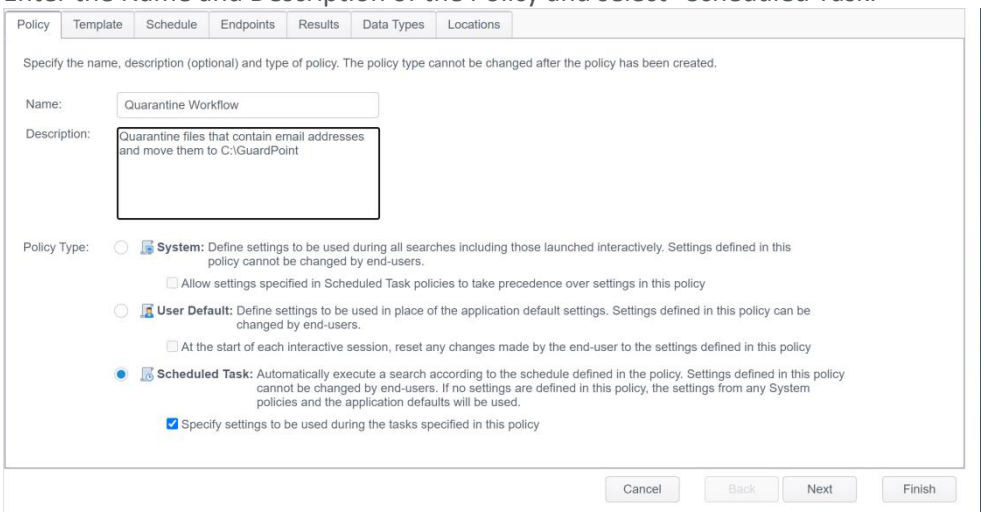
1. Select the "Policies" tab.



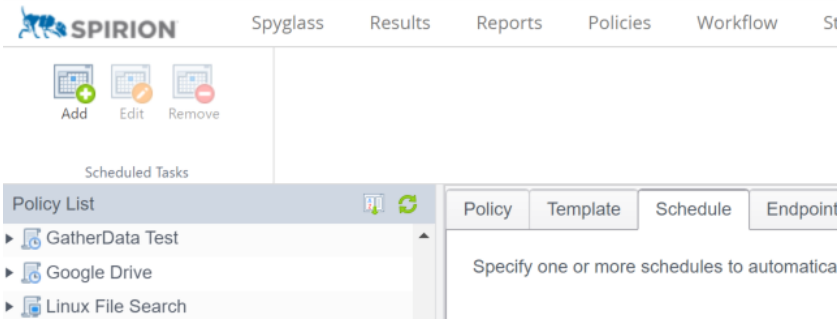
2. Click "Policy" and select "Create."



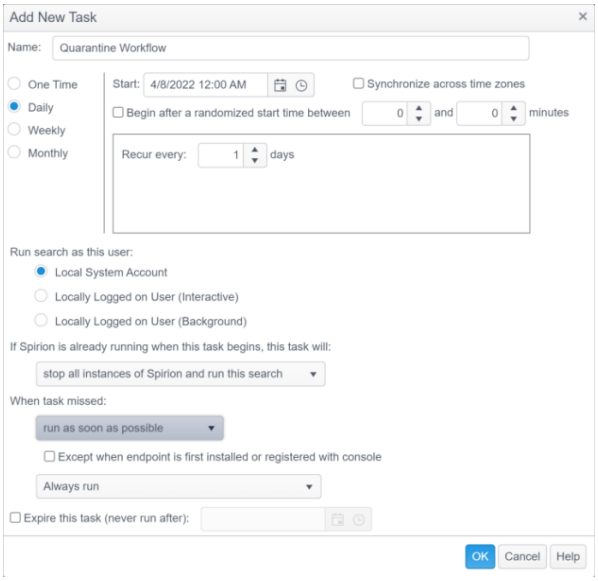
3. Enter the Name and Description of the Policy and select "Scheduled Task."



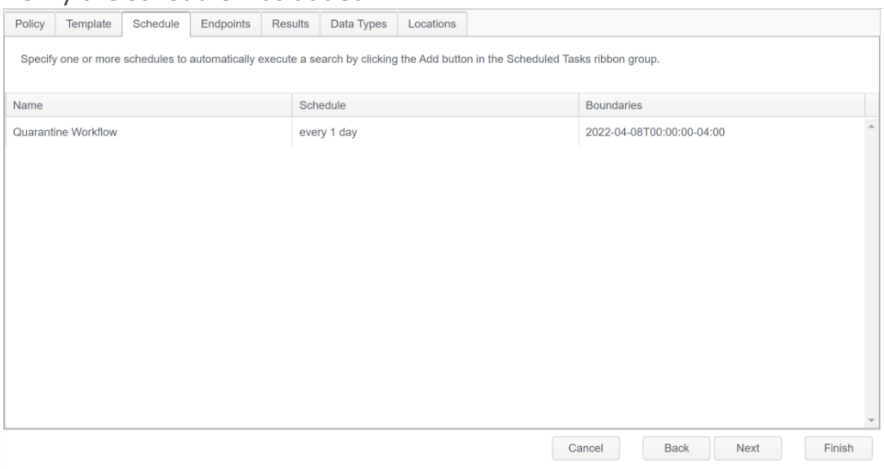
4. Select the “Scheduled” tab and click “Add.”



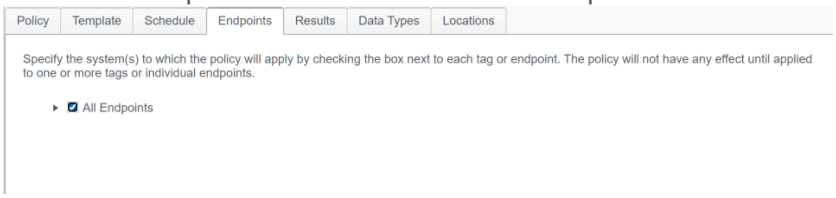
5. In the “Add New Task” window enter the following information
    a. How often should the scan run and when should it start?
    b. Run search as this user
    c. If Spirion is already running what should this task do?
    d. What should happen if the task is missed?
    e. Click “OK.”



6. Verify the schedule was added.



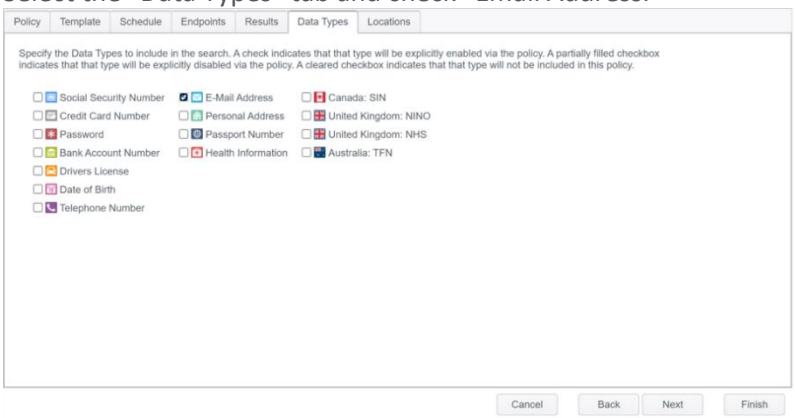
7. Select the “Endpoints” tab and select which “Endpoints” the scheduled task will run on



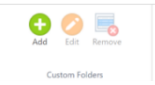
8. “Results” tab can be left at defaults.

g

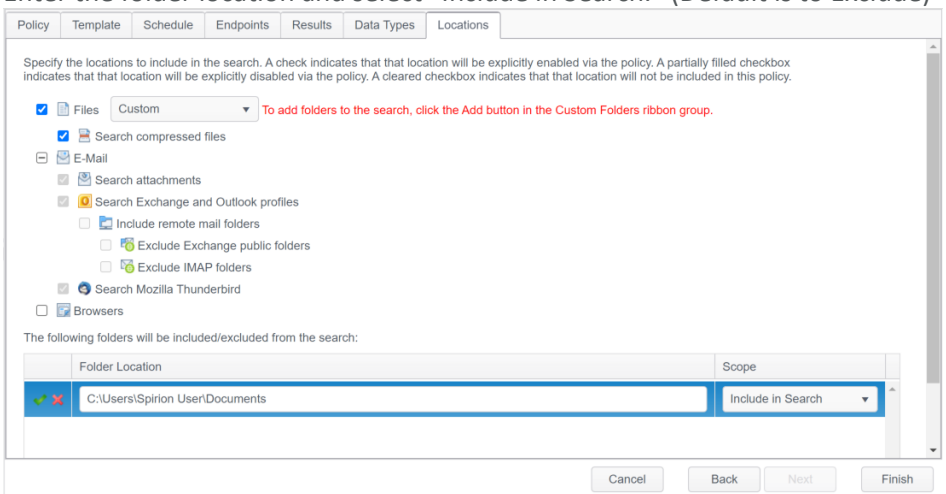
9. Select the “Data Types” tab and check “Email Address.”



10. Select the Locations tab and enter the location where the scan should search
    a. Select “Files” and “Custom” from the dropdown list



    b. Click “Add.”
    c. Enter the folder location and select “Include in Search.” (Default is to Exclude)



    d. Click “Finish.”