# SPIRION

# Spirion SDM/SDP – Thales CipherTrust Transparent Encryption Integration Guide

# Contents

Introduction1
Requirements2
Limitations2
Important Notes2
Integration Process2
STEP 1 – Install the CipherTrust Transparent Encryption Agent2
STEP 2 – Create the GuardPoint folder on the Windows Endpoint Filesystem
STEP 3 – Set Up a GuardPoint on the Windows Endpoint Filesystem4
STEP 4 – Install the Spirion Agent and Connect to the Console6
STEP 5a – In Sensitive Data Platform: Create a Spirion SDP Playbook6
STEP 6a – In Sensitive Data Platform: Create a Spirion SDP Scan9
STEP 5b – In Sensitive Data Manager: Create a SDM Workflow15
STEP 6b – In Sensitive Data Manager: Create a Spirion SDM Scan

# 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 finegrained 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 <u>Customer Support Portal</u>.

# **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 :

<u>CTE Agent for Windows Quick Start Guide</u>



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

- <u>CipherTrust Manager: CTE Administration, Managing Policies</u>
- <u>CipherTrust Manager: Managing Policies, Modifying Policies and Rules</u>
- <u>CipherTrust UserSpace Administration: Access Policies</u>
- 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:

Live Data Transformation for network shares	CipherTrust Data Security Platform	
On this server do you plan to protect CIFS/S with Live Data Transformation (LDT) add on	IMB based GuardPoints ? If so, select yes	
⊖ Yes		
No		
InstallShield		

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

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



	File Home Share	View						
*	> × 🛧 💺 > This	PC > Local Disk (C:) >			~	Ö	🧢 Search Local Disk (C:)	
		Name	Date modified	Туре	Size			
	A Quick access	\$WinPEAcent	4/1/2022 10-20 AM	File folder				
	Desktop 🖈	Perfloar	12/7/2019 1-14 AM	File folder				
	🕹 Downloads 🛛 🖈	Program Files	4/1/2022 11:03 AM	File folder				
	😫 Documents 🛛 🖈	Program Files (x86)	4/1/2022 5-38 AM	File folder				
	Fictures 🖈	ProgramData	4/1/2022 11:03 AM	File folder				
	\\VBOXSVR\win10-r	Users	4/1/2022 4-15 AM	File folder				
	b Music	Windows	4/1/2022 3:54 AM	File folder				
	Videos	GuardPoint	4/1/2022 11:08 AM	File folder				
	OneDrive							
	This DC							
	this re							
	Network							
	S VBOXSVR							
								1000
8	items 1 item selected							

#### 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\



Ш ТН	ALES Transp					admin 🚨
Clients Clients Client G		<ul> <li>Clients</li> <li>desktop-nr8n2</li> <li>Live Data</li> <li>Transformation</li> </ul>	Create GuardPoint	×		O ItClientProfile
LDT Con K8s Clie K8s Stor		Encryption Key     Protection     File Header Supported     Secure Start	Policy: * spirion-policy Type: *	Select		
Policies       Eff     Reports       Of     Settings		GuardPoints Client Sett	Auto Directory  Path:  Path:	Droutes		Apply
		0 Total GuardPoints	C:\GuardPoint\	Browse		
		Protected Path - Q s 0 Selected 0 Results   0 Guard	O To apply the same GuardPoint settings to multiple paths, type paths specify them using the Browse button. A maximum of 200 GuardPati specified.	in the Path field or hs can be		e GuardPoint
		Status Policy Name 🛧	Secure Start: 📃 🔀	Cancel		ogress 🐵
				Create		

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

Ⅲ	THALES Trans	parent Encryption	١	API	8	admin 🚨
<b>■</b> *	Clients × Policies × Reports ×	<ul> <li>Clients</li> <li>Clients</li> <li>Client Password Creation</li> <li>Client P</li> <li>Unlock Agent Lock</li> <li>Protection</li> <li>File Header Supported</li> <li>✓ Secure Start</li> </ul>	rofile		DefaultClie	Apply
		GuardPoints       Client Settings       Membership       Challenge Response         Refresh GuardPoints       C       Image: Comparison of the set of t	0	0 Unkn	own	
		Protected Path →       Q. Search by Protected Path         □ 0 Selected 1 Result   1 GuardPoint         Status       Policy Name ↑         Protected Path       Type         SMB Connection       Efficient Storage         Client Group       Rekey Statu         ▲ Active       spirion-policy         C:\GuardPoint       directory_auto         N/A       No	is Enab Yes 1 G	+ led ⊽	Create Gua LDT Progre N/A nt 10 per	rdPoint) ss (©)  page •
	«					

#### 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%2 Owith%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.

(1)	Sensitive Data Platform	Actions • 🕞 Steps < >	Playbook:	Zoom + - ⑦ Help
	Client Admin Administrator		Start 0 Yes	= =
		€ Select Action ~	Select Action ~	⊕
			New Playbook ×	
		Please select the action type.	Quarantine to GuardPoint Playbook Please select the action type.	
			Description	
		Đ	Cancel Continue	

Click "Continue."

SPIRION

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."

(1)	Sensitive Data Platform	Actions • 🕞 Steps < >	Playbook: Quarantine to GuardPoint Playbook		Zoom + - @Help
	Client Admin Administrator	~			
	Scans			_	
		Decision Point	C	9 HELP	×
		Step Logic			
		Name is email?			
		Logic			
		Data Types Contains	✓ E-Mail Address ···· ↔		
		Decision Weight 0			
			Cancel	Save	
		⊕	$\odot$		

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).



n 🕅	Sensitive Data Platform	Ļ <mark>1</mark>	Actions • 🕞 Steps < >	Playbook: Quarantine to G	uardPoint	Zoom + - O Help
•	Client Admin Administrator	~		Start		
So	cans			0		
	BACK		Take No Action   ~	No Yes Classificat	tion ~ 🗍	) → Quarantine ~ 🗍
	All Soono		Automated Action	Action Optio	ons:	Quarantine Path is managed by the
	All Scalls			Perform	Action on File a 💙	Platform administrator in Application Settings.
\$	Scan Playbooks		Complete ×	Classificati	on Type:	Automated Action
	Scan Results			Add Clas	sification 🗸	
				Select Class	sification:	Complete ×
				Classifie	d ~	
				🗹 Auton	nated Action	
			+			
я <sup>к</sup>	Minimize		-			
٩	Settings	>				
Versi	on: 22.Q1.2.171.0					

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).



(1)	Sersitive Data Platform	Actions • 🔂 Steps < >	Playbook: Quarantine to GuardPoint	Zoom + - O Help
	Client Admin Administrator Scans		Start	
		Automated Action	Quarantine Paths × Quarantine Path is managed by the	
			Select an Environment to Assign a Path	
		Complete ×	Filesystem X V Automated Action	
			Windows Quarantine File Path   C:GuardPoint     Mac Quarantine File Path   /GuardPoint     Cancel   Confirm	

## 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".



Name and Description > Scan Type	
Client Admin Administrator Enter a name and description	
Scans	
BACK Name * Description Quarantine to GuardPoint	
😂 All Scans	
Scan Playbooks	
Scan Results	
» <sup>#</sup> Minimize	
Image: Settings	

Select "Sensitive Data Scan."

Click on "Next."





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

Click on "I	Next."
-------------	--------

Senative Data Platform	Create New Scan	pok > Target Type	Help
Administrator	Select a Playbook to appl	y to the scan	
Scans	Search	٩	
< BACK	Selected Playbook: Quarantine to GuardPoint		
🖯 All Scans	Playbook Name	Playbook Description	
୍ଭିଲ Scan Playbooks	ePHI	SE playbook designed to classify data that would be covered under HIPAA.	
🗹 Scan Results	説 HR Data - Resumes	SE playbook that shows classification of HR data and specifically resumes.	
	a PCI	SE designed playbook to demonstrate a basic PCI-DSS scan.	
	🔐 pst or msg search	Search for .pst or .msg files	
	💭 Quarantine to GuardPoint	playbook	
	🔝 simple	simple	
	♂ Items per Page: 100 ∨ Displayi	ng 1-16 of <b>16 Items</b>	« < 1 >
א <sup>د</sup> Minimize			
Settings >	C Evit Without Souing	10º Complete	
	C Exit without saving	10% Complete	← Previous → Ne

Select the "Files & Folders" tile.

Click on "Next."





Ensure your Windows Endpoint Agent is under "Selected Targets."

#### Click "Next."

(1)	Sensitive Data Platform	Create New Scan Name and Description > Scan Type > Playbook > Target Type > Local or Remote > Targets > Location Type	⑦ HELP
	Administrator	Select the target(s) to scan	
	< BACK	All Targets Selected Targets	
	🕄 All Scans	Search Q Search	Q
-	Image: A constraint of the second of the	<ul> <li>✓ ○ ④ Unassigned</li> <li>◎ △ APIAUTO2_a94a5946-1ff9-41e7-9670-33809d03f32b</li> <li>◎ ② DESKTOP-NR8N2MQ</li> <li>◎ ③ ODESKTOP-NR8N2MQ</li> <li>◎ ③ ODESKTOP-NR8N2MQ</li> <li>◎ ③ ODESKTOP-NR8N2MQ</li> <li>◎ ③ ODESKTOP-NR8N2MQ</li> <li>◎ ③ DESKTOP-NR8N2MQ</li> <li>◎ ○ DESKTOP-NR8N2MQ</li> </ul>	
	a <sup>ĸ</sup> Minimize		
	Settings >	Sexit Without Saving 39% Complete	→ Next



Under "Include," enter the path to your Windows endpoint user's Documents folder.

Click on "Next."

(1)	Sensitive Data Platform	Create New Scan	Options > Scan and Compress > Exchange/Outlook > Advanced > Sc	HELP hedule > Notifications > Summary
	Client Admin Administrator	Select which custom folders to a	add (③ Import Custom	Folders Advanced Options
	< BACK	Include	Exclude	
	🚼 All Scans	C:\Users\win10\Documents	× Add Folders to Exclude	
	🔉 Scan Playbooks			
	🗹 Scan Results			
	ج <sup>د</sup> Minimize			
	ô Settings >			
		S Exit Without Saving	46% Complete	← Previous → 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."



Sensit		Ċ,	Create New Scan	⑦ HELP
			и Remote > Targets > Location Type > Folders > Scan Options > Scan and Compress > Exchange/Outlook > Advanced > Schedule > Notific	ations > Summary
	Client Admin Idministrator	~	Summary	
Scan	IS		∧ Name and Description <sup>2</sup>	
< BA	аск		Name: Quarantine to GuardPoint	
E All	l Scans		Description: N/A	
्रज्ञ Sc	can Playbooks		∧ Scan Type 🖗	
🖸 Sc	can Results		Sensitive Data Scan	
			✓ Playbook	
			✓ Target Type	
			✓ Local or Remote	
			✓ Targets	
			✓ Location Type	
,₃ <sup>⊮</sup> Mi	inimize		Faldana 10)	
<li>Se</li>	ettings	>		
			V Exit Without Saving	E 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.



ני	Sensitive Data Platform	Ċ,	Scans						⑦ HELP
	Client Admin Administrator	~	Qua		×	a			+ Add Scan
	Scans		HALL SCAN	Q DISCOVERY SCANS	SENSITIVE DATA				
	< BACK			Name	Status	Agents	Target(s) Scanned	Next Run	Last Run
Ę	🕂 All Scans			Quarantine to GuardPoint	Not Run	1	0	N/A	N/A Run Scan Now
	බ Scan Playbooks								Manage Scan
(	🗹 Scan Results								Clone Scan
									Delete Scan
	<b>⊿<sup>⊭</sup> Minimize</b>		🤁 Items per	Page: 100 V Display	ing 1-1 of <b>1 Items</b>				« < 1 >
{	🕄 Settings	>							
Ve									

#### 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.

Spirion Console	× -	F						
< → C ☆ 🤇	) localhost/consc	ole/#/Workflo	w					
👧 Spirion Identity Ass	Spirion Console	9						
R SPIRION	Spyglass	Results	Reports	Policies	Workflow	Status	Logs	Admin

3. Select "Rule / Add."





4. Enter the Name and Description of the Workflow.

SPIRION Spyglass	Results Reports	Policies worknow	status Logs	Admin		admin 👻
e Classification Definitions Edit Endpoir UI Settings	M Set Results Filter					
Workflow Rules						
W Rules List	Workflow Rule Definit	ion Endpoints Actions	Assignments	Notifications		
50804	Specify the name and the remediation actions, as	e description (optional) for the ign results to one or more use	rule. Workflow Rurs, and/or send no	les can automatically change the cl tifications that the rule has been trig	assification of a result, apply gered.	
	Name:	Quarantine				
	Description:	Workflow will move Quaranti	ned files to	1		
		C:\GuardPoint				
	Location Weight:	0 🗘				
i						

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

TRA SPIRION	Spyglas	55	Results Re	ports Pol	icies Wor	kflow	Status Logs	Admin						admin 👻
Rule Classification	Definitions Edit I V UIS	Endpoint Settings	Set Results Filter											
Workflow Rules List	Q. 🕅 .	C	Workflow Rule	Definition	Endpoints	Actions	Assignments	Notifications						
Redact		- -	The workflow r whether the ru when a single- or across all lo operation and operator (And/ Scope: Type: N Totals: C Definition:	ule definition s le will apply to result matches cations in the then specifyin Or) above the Location: A Search: App feet conditions A single n A group o calculate totals	specifies when individual loca is all of the conc g the value. To desired group, pply actions and ply actions and i linked with an esult matches if results match across only th	the associations or to a itions for to a itions that it ding on the add additional as appropri- diassignment assignment AND when all of the co- all of the co- ser results	ted actions and at all of the locations are joined by that / scope. Finally, spe scope. Final reteria, use the late. In the second scope of the second to all of the loca : multions onditions that match all of the	signments will it ound during a s IND or whene as offy the oriteria plus symbol to n that meets thi tions from a sea	e applied and n earch. Next, sp ch condition iss hat will trigger it the right of the s rule. Send a n irch that meets i	otifications will b cify whether to i attisfied by at lea ter rule by select current condition otification that in his rule. Send a	e triggered. First, si reat AND clauses a st one result in their ing an item and an or to the right of th cludes all locations notification that incl	pecify is met location e that meet this rul ludes all locations	e. s from a search	that meets this n
			X	Data Types		Contains	•	E-Mail Addre	55	+	Cancel	Back	Next	Finish



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

SPIRION	Sp	oyglass	Results F	Reports Pol	icies Wor	kflow	Status Logs	Admin						admi	n <del>-</del>
Rule Classification	Definitions	Edit Endpoin UI Settings	t Set Results Filter												
Inflow Dulos List	Workflow I	Rules				1	1								
low Rules List	4	4 5	Workflow Rule	e Definition	Endpoints	Actions	Assignments	Notifications							
			First, specify searches, th until applied System: Scope:	y whether the rule lese options are in to one or more to Target: Use Source: Use	e should apply dentical. Then ags or endpoir endpoint on w e endpoint fror bints	to the endp , select the nts. which the re- m which the	oint on which the tag(s) and/or end sults were found search was perfo	results were four point(s) whose re rmed	d or to the endpoin sults the rule applie	nt that performe es to. The rule	ed the search. will not have a	For local hy effect			Î
		i													
															4
											Cancel	Back	Next	Fini	sh

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

-----

A SPIRION	Spygiass	Results Rep	ports Pol	icies wor	KTIOW	status Logs	Admin						admin 👻
Rule Classification Definitio	ns Edit Endpoli UI Settings w Rules	nt Set Results Filter											
Workflow Rules List	x 11. 0	Workflow Rule	Definition	Endpoints	Actions	Assignments	Notifications						
Redact		To apply a class specify whether remediation action performed direct Perform the Perform the Execute sort Sefe Perform the Quara Street Execute sort Sefe Execute sort Sefe Execute sort Sefe Redaa Redaa Execute sort Street Redaa Redaa Redaa Redaa Redaa Redaa Redaa Redaa	sification level if the results si tion, check the chy on the end uits as: following MIP we all existing we all existing provide the end of console of social site of following rem antine is ct tate script Run as Local S Run as Local S Run as Local S	to results that would be class "Perform the point." Iabel action: Iabels and ap server: <i>upload</i> ediation action Select so. ystem Accour Logged on Ut	match this fifed directly following re ply the spec	Inde, check the "Counter of the endpoint of th	assify results as a ronly in the control of the con	* box and select th sole database when he desired action. I desired action for system)	ne dealined class in the results ar Remediation ac	uffcation level. To p	hen, erform a be		
										Cancel	Back	Next	Finish

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.



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

licy	Template	Schedule	Endpoints	Results	Data Types	Locations				
pecify	the name, d	escription (opt	tional) and type	e of policy. T	he policy type c	nnot be changed after the po	licy has been crea	ated.		
lame:	C	Quarantine Wo	rkflow							
)escrip	otion: Q ar	uarantine files Id move them	that contain er to C:\GuardPo	mail address int	es					
licy T	уре: 🔿	System:	Define settings policy cannot I	s to be used be changed	during all searc	es including those launched	interactively. Setti	ings defined in this	3	
		User Def	ault: Define se changed	ettings to be by end-user	used in place o	he application default setting	s. Settings define	ed in this policy ca	n be	
		C At th	e start of each	interactive s	session, reset a	changes made by the end-u	ser to the setting	s defined in this p	olicy	
	۲	<u> S</u> Schedule	ed Task: Autor canno polici	matically exe ot be change es and the a	ecute a search a ed by end-users opplication defau	cording to the schedule defin If no settings are defined in this will be used.	ed in the policy. S his policy, the sett	Settings defined in ings from any Sys	this policy tem	
		Spec	cify settings to	be used duri	ing the tasks sp	cified in this policy				
							Capaci	Consta 1	Neut	Finish



4. Select the "Scheduled" tab and click "Add."

SPIRION	Spyglass	Results	Reports	Policie	es Workf	low St
Add Edit Remove						
Policy List		T 🗊	Policy	Template	Schedule	Endpoint
▶ <u> </u> GatherData Test						
Google Drive			Specify o	ne or more	schedules to	automatica
Linux File Search						

- 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."

Name:	Quarantir	ne Work	low									
One	Time	Start:	4/8/2022	12:00 AM	÷	C	Synchro	onize	across	s time zo	ones	
Daily       Wee	y ekly	🗆 Begi	in after a ra	andomize	ed start tin	ne betweer	0	*	and	0	*	minutes
Mon	ithly	Recu	r every:	1	days							
Run sea	arch as this	user:										
۲	Local Syst	tem Acco	ount									
	Locally Lo	ogged on	User (Inte	ractive)								
	Locally Lo	ogged on	User (Bad	kground)								
If Spirio	n is already	y running	when this	task beg	ins, this ta	ask will:						
s	top all insta	ances of	Spirion and	d run this	search							
When ta	ask missed:											
n	un as soon	as possi	ble	•								
_	Except w	hen endp	point is firs	t installed	l or regist	ered with c	onsole					
C						¥						
A	Always run											

6. Verify the schedule was added.

	,													
Policy	Template	Schedule	Endpoints	Results	Data Types	Locations								
Specify	one or more	schedules to	automatically e	execute a se	earch by clicking	the Add butto	n in the Schedule	d Tasks ribbo	n gro	oup.				
Name				Sch	edule			Bound	aries					
Quaranti	ne Workflow			eve	ry 1 day			2022-0	)4-08	T00:00:00-04:	00			^
														÷
								Cancel		Back	Next	] [	Finish	



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



- 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
  - Add Edit Remove
- b. Click "Add." Custom Folders
- c. Enter the folder location and select "Include in Search." (Default is to Exclude)

   Policy
   Template
   Schedule
   Endpoints
   Results
   Data Types

	Custom	•	To add folders to the search, click the Add button in the Custom Folders ribbon group	up.
🗹 🖹 Se	earch compressed fil	les		
🖯 🔛 E-Mail	l.			
🗹 🕙 Se	earch attachments			
🗹 🧕 Se	earch Exchange and	Outlook	profiles	
	🔄 Include remote ma	ail folders	j	
	📄 🐻 Exclude Excha	ange pub	uic folders	
	Exclude IMAP	folders		
	earch Mozilla Thunde	erbird		
🔄 🧐 Se				
🛛 🧐 Se ] 📴 Brows	sers			
I G G G G G G G G G G G G G G G G G G G	ers olders will be included	d/exclude	ed from the search:	
G Se Brows following fo Folde	sers olders will be included er Location	d/exclude	ed from the search:	Scope

d. Click "Finish."