

Documentation

O-previous

Delinea

Table of Contents

Overview	4
Overview	5
Overview	6
What is SCIM?	6
SCIM Extension Support	6
Setup	7
Getting Started	8
Minimum System Requirements	9
Account Permissions	10
Standard Installation	11
Download the Installer	11
Installing SCIM Connector	11
Basic Installation	11
Standard Installation Process	11
Upgrade from Version 2.5 to 3.0	17
Launch SCIM Connector after Installation/Upgrade	18
Advanced Installation	20
Download the Installer	20
SCIM Connector Best Practices for Integration With Secret Server	29
Introduction	29
Broad SCIM Implementation Considerations	29
Sailpoint Specific Concepts and Limitations	30
SCIM - Creating New Users	31
SCIM – Assigning Users to Local Secret Server groups	37
SCIM – Creating New Groups	38
SCIM – Assigning Users To Folders	40
Architecture Diagrams for SCIM 2.5	43
Definitions for SS-SCIM-REF #01 - A-1	43
Requirements for SS-SCIM-REF #01 - A-1	43
Definitions for SS-SCIM-REF #01 - A-2	44
Requirements for SS-SCIM-REF #01 - A-2	44
Definitions for SS-SCIM-REF #01 - B-1	45
Requirements for SS-SCIM-REF #01 - B-1	45
SS-SCIM-REF#01 - C-1 - Request Communication Flow	46
SCIM Connector Integrations	48
Release Notes	50

3.0 Release Notes	51
Upgrade and Installation Notes	51
Enhancements	51
Known Issues	51
Workaround	51
SQL Queries	51
Changelog	53
April 2022	53
September 2021	53

This area provides previous versions of our integrations documentation.

This area provides previous versions of our integrations documentation. For the latest versions, please navigate to the current version.

• SCIM Connector - Previous Version

Overview

The Delinea System for Cross-Domain Identity Management (SCIM) connector is a web application that can be installed on a server machine, which exposes SCIM-defined endpoints and Secret Server (SS) APIs. The SCIM connector translates user, group, and privilege access management information into SCIM-defined JavaScript Object Notation (JSON) responses. The web application enables any SCIM endpoint to interact with SS using a well-defined standard method.

SCIM is an open standard that allows you to automate user provisioning using a *Representational State Transfer* (REST) API and JSON. The SCIM specification (RFC7643) provides schemas that represent common identity information about users and groups. See the <u>SCIM</u> <u>Specification</u> for more information about SCIM.

Privileged Access Management (PAM) software typically makes use of common user and group models, as well as defining additional constructs, to provide fine-grained authorization and management for privileged access. The <u>SCIM 2.0 Extension for PAM</u> includes extensions to the core user and group objects and new resource types and schemas for standard PAM constructs. This extension is intended to provide greater interoperability between PAM software and clients, a common language for PAM concepts, and a baseline that can be further extended to support more complex PAM requirements.

The Delinea System for Cross-Domain Identity Management (SCIM) connector is a Web application that can be installed on a server machine, which exposes SCIM-defined endpoints and Secret Server APIs.

This section covers the system Requirements and two available installation approaches.

The following topics are available:

- <u>Getting Started</u>
- <u>System Requirements</u>
- <u>Account Permissions</u>
- <u>Standard Installation</u>
- <u>Advanced Installation</u>
- Best Practices and Implementation Considerations

Before installing the SCIM Connector you should have:

- 1. Secret Server Local Administrator Account.
- 2. Secret Server Application Account.
- 3. Windows 2012R2, 2016 or 2019 Server with:
 - IIS Web Server
 - .net 4.52 or higher
 - The ability to connect to Secret Server (use the browser on the web server you intend to install SCIM Connector on and log into Secret Server to ensure the Web Server can connect to the Secret Server / Web Site
 - The ability to connect to SCIM Endpoints (such as Sailpoint, Okta, etc...)
 - The account information to connect to each SCIM Endpoint
 - URL to SCIM Endpoint

To install and run the SCIM Connector as a Web application in your environment, Delinea recommends installing the SCIM Connector on a server machine that meets at least these requirements.

Storage	300 MB of free space			
Drives	7200 RPM IDE drives			
Processor	2 GHz Pentium 4 CPU			
Memory	4 GB RAM			
OS	Windows Server 2012/2016/2019			
	IIS Enabled			
Framework	.NET 4.5.1 or later			
Browsers	Chrome, Edge, FireFox, IE			
License	Valid Secret Server licenses: Professional or Platinum			

A Local Administrator Account must be used to initially setup the SCIM Connector and connect it to Secret Server.

The Application Account use in the SCIM Connector must have the following permissions:

Add Secret
View Users
Administer Folders
Administer Groups
Administer Reports
Administer Secret Templates
Administer Users
Create Root Folders
Delete Secret
Edit Secret
Own Secret
View Advanced Secret Options
View Secret

Download the Installer

Download the installer file at:

• SCIM software download

Installing SCIM Connector

The Delinea SCIM Connector uses a Windows Installer installation to install and configure the SCIM Connector website. There are three main paths that the installer leverages to setup the website.

Basic Installation

Run the SCIMConnector.msi on the server where IIS is available. The installation will perform basic readiness checks and guide you through the website setup.



After the initial welcome dialog, select the type of installation to perform.

Standard Installation Process

The standard installation process is used to install the SCIM Connector into a new website in IIS. Often this will require a custom port, however if port 443 and port 80 (standard https/http ports) are not bound to any site, SCIM Connector site will be bound to them by default. If Ports 443 or 80 are already bound to a website on the IIS server, a new port will be selected for the SCIM Connector site. Port selection for https will start from 8443 and increment by one (e.g. 8444) until an available port is found. For http, the port selection will start at 8080 and increment up by one. Use the Advanced option if you want to pick the ports that SCIM Connector will use.

1. Select the Standard option to create a new website in IIS and click Next.

SCIMConnector			×
Configure your installer			
Ease your Installer by selecting one of the	option		A second
The Installer will install SCIM Connecto Connector website in IIS. Choose Stan to create a Virtual Directory under def	r on your compu idard to create ault website	uter by creating a S a new website or A	iCIM dvance
Standard			
Create new Website, No V	'irtual directory		
○ Advanced			
Customize Port number, En	able http		
	De de	Next	Consul
	DdCK	INEXL	Cancel

2. Provide the Application Name (this will also be the website name) and click **Next**.

			×
		1	
e of the application			
for the name of the So	CIM Connector v	website and the ap	plication pool
SCIMConnector			
	ne of the application d for the name of the So SCIMConnector	ne of the application	ne of the application

3. Review the license agreement. Once satisfied, check the **I accept the terms and the License Agreement** checkbox and click **Next**.

nd-User License A	greement			
Please read the follow	wing license agreem	ent carefully		
TERMS AND CON	DITIONS FOR TH	HYCOTIC FREE S	OFTWARE P	RODUCTS
This agreement (the "Agreemen	nt") sets forth t	he terms an	d
conditions under	r which Thycotic	c Software, LLC	("Thycotic")	agrees
to license and the	e party whose r	name appears	on the signat	ture page
to license and the of this Agreemer certain software	e party whose r nt under License products that a	name appears ee (the "Licens re offered free	on the signative ee") agrees	ture page to use
to license and the of this Agreemer certain software Thycotic's websit	e party whose r nt under License products that a te ("Free Produ	name appears ee (the "Licens re offered free cts"). This Agre	on the signat ee") agrees from or thr eement form	ture page to use ough ns the
to license and the of this Agreemer certain software Thycotic's websit entire agreemen	e party whose r nt under License products that a te ("Free Produ t between Thyo	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen	on the signative ee") agrees from or thr eement form see regardin	ture page to use ough ns the ng Free
to license and the of this Agreemer certain software Thycotic's websit entire agreemen Products.	e party whose r nt under License products that a te ("Free Produ t between Thyo	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen	on the signa ee") agrees from or thr eement form see regardin	ture page to use ough ns the g Free
to license and the of this Agreemer certain software Thycotic's websit entire agreemen Products. License. Thycotic	e party whose r nt under License products that a te ("Free Produ t between Thyo chereby grants t	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen to Licensee a p	on the signative on the signative of the signature of the second of the	ture page to use ough is the ig Free on-
to license and the of this Agreemer certain software Thycotic's websit entire agreemen Products. License. Thycotic	e party whose r nt under License products that a te ("Free Produ t between Thyo c hereby grants i in the License Agree	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen to Licensee a p ement	on the signat ee") agrees e from or thr eement form see regardin perpetual, no	ture page to use ough ns the g Free on-
to license and the of this Agreemer certain software Thycotic's websit entire agreemen Products. License. Thycotic	e party whose r nt under License products that a te ("Free Produ t between Thyo c hereby grants in the License Agree	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen to Licensee a p	on the signal ee") agrees e from or thr eement form see regardin perpetual, no	ture page to use ough is the g Free on-
to license and the of this Agreemer certain software Thycotic's websit entire agreemen Products. License. Thycotic	e party whose r nt under License products that a te ("Free Produ t between Thyo c hereby grants i in the License Agree	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen to Licensee a p ement	on the signal ee") agrees e from or thr eement form see regardin eerpetual, no	ture page to use ough as the g Free on-

4. Provide the path where the application files will be installed. A subdirectory (SCIMConnector) will be created in the specified path. For example, C:\inetpub\wwwroot\SCIMConnector then click **Next**.

🛃 SCIMConnector Setup					×
Destination Folder					
Click Next to install to the default	t folder or click Chan	ge to choose	another.		
Install SCIMConnector to:					
C:\inetpub\wwwroot\					
Change					
	Back	C N	ext	Cano	:el

5. At this point the SCIM Connector installation is ready to create the website.

🛃 SCIMConnector Setup		-		×
Ready to install SCIMConnector		1		2
Click Install to begin the installation. Click Back installation settings. Click Cancel to exit the wi	to review or chang izard.	ge <mark>any of</mark> you	r	
Back	k <u>I</u> nsta		Cano	el

localhost:8443/#/?returnUrl=%2Fsettings

6. After the installation has completed the default browse is launched and SCIM Connector is now ready to be configured. See Configuration section for additional details.

Secret Server Integrations
Sign In
Base url
Username
Password
Sign In

7. The install has created a subdirectory called SCIMConnector and the application files can be seen in this folder.

Ν	lame	Date modified	Туре	Size
I	assets	10/28/2020 12:08	File folder	
	bin	10/28/2020 12:08	File folder	
	Log	10/28/2020 12:10	File folder	
1	Responses	10/28/2020 12:08	File folder	
	Server	10/28/2020 12:08	File folder	
	SqlQuery	10/28/2020 12:08	File folder	
	3rdpartylicenses	10/28/2020 11:38	Text Document	48 KB
[active.72d931449243390e006d	10/28/2020 11:38	PNG File	1 KB
	ApplicationInsights.config	10/28/2020 11:34	CONFIG File	8 KB
8	s2015-polyfills.5e60b7ad6e87c6cc59ea	10/28/2020 11:38	JavaScript File	57 KB
6	favicon	10/28/2020 11:38	lcon	2 KB
	fontawesome-webfont.674f50d287a8c48	10/28/2020 11:38	EOT File	162 KB
Ę	fontawesome-webfont.912ec66d7572ff82	10/28/2020 11:38	SVG Document	434 KB
	fontawesome-webfont.af7ae505a9eed50	10/28/2020 11:38	WOFF2 File	76 KB
1	fontawesome-webfont.b06871f281fee6b	10/28/2020 11:38	TrueType font file	162 KB
	fontawesome-webfont.fee66e712a8a08e	10/28/2020 11:38	WOFF File	96 KB
	Global.asax	10/28/2020 11:34	ASAX File	1 KB
(👂 index	10/28/2020 12:08	Chrome HTML Do	1 KB
8	main.12cfed4135e337f310d2	10/28/2020 11:38	JavaScript File	572 KB
	Materiallcons-Regular.29b882f018fa6fe75	10/28/2020 11:38	WOFF File	78 KB
	Materiallcons-Regular.96c476804d7a788c	10/28/2020 11:38	EOT File	68 KB
	Materiallcons-Regular.0509ab09c1b0d22	10/28/2020 11:38	WOFF2 File	60 KB
1	Materiallcons-Regular.d120c85b6eb0549	10/28/2020 11:38	TrueType font file	171 KB
[outline.da1dce55e6be63488a16	10/28/2020 11:38	PNG File	1 KB
8	polyfills.7b94fcaa94c69f287a8a	10/28/2020 11:38	JavaScript File	41 KB
[register.c57daf8ed08b7c9138c8	10/28/2020 11:38	PNG File	2 KB
	Roboto-Regular.6a561d68369fd1fb9768.eot	10/28/2020 11:38	EOT File	22 KB
	Roboto-Regular.081b11ebaca8ad30fd09	10/28/2020 11:38	WOFF File	88 KB
1	Roboto-Regular.99b14f0da0591e0d7167	10/28/2020 11:38	TrueType font file	167 KB
4	Roboto-Regular.766c8926f6d9061fef24	10/28/2020 11:38	SVG Document	717 KB
	Roboto-Regular.b2a6341ae7440130ec4b	10/28/2020 11:38	WOFF2 File	63 KB
8	runtime.aa5b8c69ed805056b567	10/28/2020 11:38	JavaScript File	2 KB
	Settings.enc	10/28/2020 12:11	ENC File	1 KB
1.000	styles.d11ecac23bb2dbec0803	10/28/2020 11:38	Cascading Style S	175 KB
Г	web config	10/28/2020 12:10	CONFIG File	9 KB

8. A new website has been created which can be seen in the IIS Manager.



9. An Application Pool has been created called **SCIMConnectorAppPool**. This can also be viewed in the IIS Manager.

Internet Information Services (IIS) M	lanager
← → WIN-M7SDCC02	8EI Application Pools
File View Help	
Connections	Application Pools This page lets you view and manage the
 WIN-MTSDCC028EI (CMDCO) Application Pools Sites Default Web Site SCIMConnector Sises SciMConnector Server Server 	Filter: Co ~ Name NET v4.5 Construction DefaultAppPool SCIMConnectorAppPool

Reviewing the Basic Settings of the SCIMConnector website, the site is

associated with the application pool that was created.

SCIMConnector SCIMConnector Science assets Science assets Science assets	.NET Authorizat	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	.NET Users	Application Settings	Connection Strings	Machine Key	Pages and Controls	Providers	Sessio
> Log > Responses > Server > SqlQuery	ASP	Authentic	2 Compression	Default Document	Directory Browsing	404 Error Pages	Failed Request Tra	Handler Mappings	HTTP Redirect	HTTP Respon	ISAPI Filters	Logging	MIME Type	s Mo
	Manageme	nt												
		82					Edit Sit	e					?	×
	Configurat	IIS Manager					Site r	name:		Applicatio	n pool:			
	Editor	Permissions					SCIM	1Connector		SCIMCon	nectorAppPool		Select	
							Phys	ical path:	ot\SCIMConn	ector				
							Pass-	through auth	entication					
							Cor	nnect as	Test Setting	s				
											(ОК	Cancel	

10. HTTP and HTTPS Bindings have been created for the web site.

Note: The ports may differ from the standard http / https ports. This is due to another website in IIS has already consumed the standard ports for https (80/443).

Oefault Web Site Oefault Web Site SCIMConnector Connector SCIMConnector Default Sector	.NET Authorizat	.NET Compilation	.NET Error Pages	.NET Globalization	.NET Profile	.NET Roles	.NET Trust Levels	.NET Users	Application Settings	Connection Strings	Machine Key	Pages and Controls	Providers	Session State	e SMTP E
> Din >	IIS ASP Managemen	Authentic	Compression	Default Document	Directory Browsing	Error P	Enited e Bindings Type Host I http	Vacadar Name	Port IP A 8080 *	ddress	EADLEIMAN Binding Inform	l annia		? ×	Outp Cachi
	Configurat Editor	IIS Manager Permissions					https		8443 *					Remove Browse Close	

The installation will search for a certificate with the hostname and use this for configuring https. This can be changed after the installation to any certificate that is desired and available. If no certificate is found, the installation will create a self-signed one.

Upgrade from Version 2.5 to 3.0

1. Select the installer option (Standard):



2. Click Install.

🕼 SCIMConnector Setup			×
Ready to install SCIMConnector			2
Click Install to begin the installation. Click Back to review or change an settings. Click Cancel to exit the wizard.	ny of you	r installation	
Back	all	Can	cel

Launch SCIM Connector after Installation/Upgrade

1. Open run from the **Start** menu and enter inetmgr.

🧾 Run				×
	Type the n Internet re	ame of a pro source, and	ogram, folder, do Windows will op	ocument, or en it for you.
Open:	inetmgr			~
		ОК	Cancel	Browse

- 2. Navigate to **IIS** and locate the installed SCIM Connector site.
- 3. click on the **Browse Website** option to launch SCIM connector.

Connections		sc	IMConner	tor Home	P									Actions
Start Dags		•			-									A Explore
✓ GINT Page ✓ CYB-SCIMS2019 (CTHYCOTIC\ssupeka	ar)	Filten		- 7 Go - 6	Show All G	roup by: Area								Edit Cite
- Application Pools		ASP.NET		-	-	(mark)	(10)	0	0		-		(SECON)	Bindings
Sites				404	•		0		Ċ.	¥=	ab	- P	8	Basic Settings
> 🕘 SafariWeblauncher		.NET	NET	.NET Error	NET	NET Profile .N	NET Roles	NET Trust	.NET Users	Application	Connection	Machine Key	Pages and	View Applications
> 😌 TestSite		Authorizat	Compilation	Pages	Globalization			Levels		Settings	Strings		Controis	View Virtual Directories
> 🕘 Weblauncher		10	8											Manage Website
		Providers	Session State	SMTP E-mail										Start
														Start
			Ð		(100 million)			-		BIB.	38		B	Browse Website
			Z	0	HO	404	8				e		1100	Browse *:87 (http)
		Authentic	Compression	Default	Directory Browsing	Error Pages Re	Failed quest Tra	Handler Mappings	HTTP Redirect	HTTP Respon	ISAPI Filters	Logging	MIME Types	Browse *:86 (https)
			-		0									Advanced Settings
			and the second s	•										Configure
		Modules	Output Caching	Filtering	SSL Settings									Limits
		Manageme	int											HSTS
			52											😧 Help
Internet Information Services (IIS) Manager ())))))))))))))))))	es 🕨 Default Web Sit	► SCIMCor	nnector 🕨											- 0 ×
Internet Information Services (IIS) Manager C SAGE-VDI-013 + Site File View Help Connections	es > Default Web Sit	SCIMCor	nnector 🕨											- Ů ×
Intermet Information Services (IIS) Manager Competition (IIS) Manager File View Help Connections	es > Default Web Sit	→ scimcoi	nnector >											- Ů ×
Intermet Information Services (IIS) Manager Connections Connection	es > Default Web Sit	→ scimcon	r Home	All Group by	5 Årea	• (m) •								- C × C × Actions Actions Edit Permissions
Intermet Information Services (IIS) Manager Connections Connections Connections CYBAGE-VDI-013 (CYBAGE-VDI-013\Nii CYBAGE-VDI-013 (CYBAGE-VDI-013\Nii CYBAGE-VDI-013\Ni CYBAGE-VDI-013 (CYBAGE-VDI-013\Ni CYBAGE-VDI-013	es > Default Web Sit	 SCIMCon Connector 	r Home	All Group by	y: Area	•								Actions Actions Actions Basic Settings
Internet Information Services (IIS) Manager Connections Connections	es > Default Web Sit	SCIMCon	r Home	All Group by	/- Area	• 20 •						Î	٥.	Actions Actions Actions Edit Permissions Basic Settings View Virtual Directories
Internet Information Services (IIS) Manager	es > Default Web Sit	SCIMCon	r Home	All Group by	v: Area	• SB •	.NET Users		n Connettic	m Machine Ka	v Pages and	Providers	Session State	Actions Actions Edit Permissions Basic Settings View Virtual Directories Manage Application
Internet Information Services (IIS) Manager Information Services (IIS) Manager Internet Informatinger Internet Informa	es > Default Web Sit	SCIMCon	r Home Go ~ Show	All Group by	v: Area ofile .NET Rol	• 🗊 • NET Trust Levels	.NET Users	Application Settings	n Connectic Strings	n Machine Ke	y Pages and Controls	Providers	Session State	Actions Consecutive Section S
Internet Information Services (IIS) Manager	es > Default Web Sit	SCIMCon	r Home	All Group by T .NET Prr ation	r Area ofile NETRO	• 📰 • les .NET Trust Levels	.NET Users	s Application Settings	n Connectio Strings	n Machine Ko	y Pages and Controls	Providers	Session State	Actions Actions Actions Basic Setling View Virtual Directories Manage Application Browse Application Browse *80 (htp) Browse *10 (htp)
Internet Information Services (IIS) Manager Internet Information Services (IIS) Manager Image: Service Ser	es > Default Web Sit SCIM Filte: ASP.NET ASP.NET Authorizat Con SMTP E-mail	SCIMCor Connecto	r Home Go - C Show T Error NE ages Globaliz	All Group by NET Privation	/F Area	•	JET Users	Application Settings	n Connectio Strings	n Machine Ke	y Pages and Controls	Providers	Session State	Actions Actions Actions Basic Settings View Virtual Directories Manage Application Browse Application Browse *80 (http) Advanced Settings
Internet Information Services (IIS) Manager Internet Information Services (IIS) Manager Image: Service Ser	es > Default Web Site Filter: ASP NET Authorizat Con SMTP E-mail	SCIMCon Connecto	r Home Go - C Show	All Group by T .NET Pr ation	r Ares	• 🗊 • es .NET Trust Levels	.NET Users	s Application Settings	n Connection Strings	n Machine Ke	y Pages and Controls	Providers	Session State	Actions Actions Basic Settings View Virtual Directories Manage Application Browse Application Bro
Internet Information Services (IIS) Manager Internet Information Services (IIS) Manager Image: Service Ser	es > Default Web Site /SCIM Filter: ASP NET Authorizat Con SMTP E-mail IIS	SCIMCor	r Home	All Group by T .NET Pri ation	r: Area	• . • • • • • • • • • • • • • • • • • •	NET Users	Application Settings	n Connection Strings	m Machine Kr	y Pages and Controls	Providers	Session State	Actions Actions Actions Actions Basic Settings View Virtual Directories Manage Application Browse Application Browse Application Browse Application Browse Add (http:) Advanced Settings Prior Help
Internet Information Services (IIS) Manager Connections Connections	es > Default Web Sit Filter: ASP NET Authorizat Con SMTP E-meil IIS IIS	SCIMCon Connecto	r Home Go - C Show	All Group by TNET Pri ation	r Area ofile NET Rol	•	NET Users	s Application Settings	n Connection Strings	n Machine Ko	y Pages and Controls	Providers	Session State	Actions Actions Actions Explore Exp
Internet Information Services (IIS) Manager	es > Default Web Sit Filter: ASP.NET Authorizat Com SMTP E-mail IIS IIS ASP Aut	SCIMCon Connecto Vet Station P	r Home Go - Show T Error JNE T Error JNE Globaliz	All Group by T NET Pration	r Area	•• es	NET Users	Application Settings	n Connection Strings	n Machine Ka MiME Type	y Pages and Controls	Providers Dittorio	Session State	Actions Actions Actions Actions Basic Settings View Virtual Directories Manage Application Browse Application Browse Application Construct and Orthopol Advanced Settings Prep
Internet Information Services (IIS) Manager	es > Default Web Sit Filter: ASP.NET Authorizat Con SMTP E-mail IIS IIS ASP Aut	SCIMCon Connecto	r Home Go - Show T Error JNE Terror JNE Globalia	All Group by T .NET Pri ation Directs Browsi	r Area ofile NET Rol	• III • es .NET Trust Levels Handler Mappings	.NET Users	Application Settings	n Connection Strings	n Mechine Kr MIME Type	y Pages and Controls	Providers Dutput Caching	Session State	Actions Explore Edit Permissions Basic Settings View Virtual Directories Manage Application Browse Application Browse Application Browse Application Browse Application Advanced Settings Hep
Internet Information Services (IIS) Manager	es > Default Web Sit Filter: ASP.NET Authorizat Con SMTP E-mail IIS IIS IIS ASP Aut OFI Catings (1) (1) (1) (1) (1) (1) (1) (1)	SCIMCon Connecto Ver Net Net Net Con Net Con	r Home 60 - Show F Fror Ages Globaliz	All Group by T.NET Print ation .NET Print tuit Browsi	r Area ofile .NET Rol	• III • es .NET Trust Levels ges Handler Mappings	.NET Users	Applications Settings	n Connection Strings	n Machine Kr	y Pages and Controls	Providers Providers	Session State	Actions Edit Permissions Basic Settings View Virtual Directories Manage Application Browse Application Browse Application Browse Application Browse Application Advanced Settings Hep
Internet Information Services (IIS) Manager	es > Default Web Sit Filter ASP.NET ASP.NET Asthorizat Con SMTP E-mail IIS IIS IIS SSL Settings W Auto	SCIMCon Connecto VET NEE P entic Com DDAV bDAV	r Home Go - C Show T Error JAE Globaliz pression Defa Docun	All Group by TNET Printion	of Area	• . • • • • • • • • • • • • • • • • • •	NET Users	: Application Settings	n Connection Strings	n Machine Ke MIME Type	y Pages and Controls	Providers Dutput Caching	Session State	Actions Consequence
Internet Information Services (IIS) Manager	es > Default Web Sit Filten ASP.NET ASP.NET ASP.NET ASP.NET SNTP E-mail IIS SSNTP E-mail IIS SSL Settings Way Management	SCIMCon Connecto Ver Ver Ver Ver Ver Con	r Home Go - C Show F Error Globaliz pression Defe Docun	All Group by T .NET Pr ation NET Pr	ofile .NET Rol	es MET Frust Levels	NET Users	Application Settings	n Connectic Strings	n Machine Ka MiME Type	y Pages and Controls	Providers Providers Output Caching	Session State	Actions Actions Actions Basic Settings View Virtual Directories Manage Application Browse Pylication Browse 7:80 (http) Advanced Settings Advanced Settings
 Internet Information Services (IIS) Manager 	es > Default Web Sit Filter ASP.NET ASP.NET ASP.NET ASP.NET SMTP E-mail IIS SMTP E-mail IIS SSI Settings Management IIS	SCIMCon Connecto Ver Ver Ver Ver Ver Con	r Horne Go - C Show F Error JNE Globaliz pression Defe Docun	All Group by T .NET Pr ation NET Pr	ofile .NET Rol	• E • NET Frust Levels	NET Users	Application Settings	n Connectie Strings	n Machine Ka MIME Type	y Pages and Controls	Providers Providers Output Caching	Session State	 Actions Actions Edd Permissions Basic Settings View Virtual Directories Manage Application Browse 7:60 (http) Browse 7:60 (http) Advanced Settings Help

Download the Installer

Download the installer file at:

• SCIM software download

The advanced Installation Process will use the Default Web Site.

The Advanced options allow the SCIM Connector to be installed as either a virtual directory under the default web site or the creation of a new website while defining the binding ports. Much of the installation experience is the same as the standard installation process.

1. To install the SCIM Connector as a virtual directory under the Default Web Site select the Advanced option and then click **Next**.

🖟 SCIMConnector			×
Configure your installer			
Ease your Installer by selecting one of the	option		1
The Installer will install SCIM Connecto Connector website in IIS. Choose Star to create a Virtual Directory under def	r on your compu ndard to create ault website	uter by creating a a new website or	a SCIM Advance
○ Standard			
Create new Website, No V	/irtual directory		
Advanced			
Customize Port number, En	able http		
	Back	Next	Cancel

2. Select Use Default Web Stie and click Next.

Select Your Choice Host your application Using	
Host your application Using	
Host your Application under	
Do you want to install this as a web site or a new application un	ider
Our Use Default Web Site	
○ Create new website	
Back Next	Cancel

3. Fill in the name for the application. This will be used for the virtual folder name as well as the Application Pool name. Select **Next**.

SCIMConnector				×
Application Name				
Please enter the nam	e of the application			
This value will be used that will be created.	for the name of the	SCIM Connect	or website and the	application pool
Application Name	SCIMConnector			
		22		
		Back	Next	Cancel

4. Review the license agreement. Once satisfied, check the **I accept the terms and the License Agreement** checkbox and click **Next**.

nd-User License A	greement				
Please read the follow	ving license agreem	ent carefully			
TERMS AND CONI	DITIONS FOR TH	IYCOTIC FREE	SOFTWARE P	RODUCTS	^
This agreement (t	the "Agreemen	t") sets forth t	the terms an	d) agrees	
conditions under	which mycolic	Soluvare, LLC	(mycouic	agrees	
to license and the	e party whose n	ame appears	on the signa	ture page	
to license and the of this Agreemen	e party whose n t under License	ame appears ee (the "Licens	on the signa see") agrees	ture page to use	
to license and the of this Agreemen certain software	e party whose n t under License products that ar	ame appears ee (the "Licens re offered free	on the signa see") agrees e from or thr	ture page to use ough	
to license and the of this Agreemen certain software p Thycotic's websit entire agreement	e party whose n t under License products that ar e ("Free Produc t between Thyc	ame appears ee (the "Licens re offered free cts"). This Agre potic and Licen	on the signa see") agrees e from or thr eement forn see regardir	ture page to use ough ns the	
to license and the of this Agreemen certain software p Thycotic's websit entire agreement Products.	e party whose n t under License products that ar e ("Free Produc t between Thyc	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen	on the signa see") agrees e from or thr eement forn see regardir	ture page to use rough ns the ng Free	
to license and the of this Agreemen certain software p Thycotic's websit entire agreement Products. License. Thycotic	e party whose n t under License products that ar e ("Free Produc t between Thyc hereby grants t	name appears ee (the "Licens re offered free cts"). This Agre cotic and Licen to Licensee a p	on the signa see") agrees e from or thr eement forn see regardir perpetual, no	ture page to use ough ns the ng Free on-	~
to license and the of this Agreemen certain software p Thycotic's websit entire agreement Products. License. Thycotic	e party whose n t under License products that ar e ("Free Produc t between Thyc hereby grants t n the License Agree	name appears ee (the "Licens re offered free cts"). This Agro cotic and Licen to Licensee a p	on the signa see") agrees e from or thr eement forn see regardir perpetual, no	ture page to use rough ns the ng Free on-	~
to license and the of this Agreemen certain software Thycotic's websit entire agreement Products. License. Thycotic	e party whose n t under License products that ar e ("Free Produc t between Thyc hereby grants t n the License Agree	e (the "Licens re offered free cts"). This Agro cotic and Licen to Licensee a p	on the signa see") agrees e from or thr eement forn see regardir perpetual, no	ture page to use rough ns the ng Free on-	~
to license and the of this Agreemen certain software Thycotic's websit entire agreement Products. License. Thycotic	e party whose n it under License products that ar e ("Free Product t between Thyc hereby grants t n the License Agree	e (the "Licens re offered free cts"). This Agro cotic and Licen to Licensee a p ment	on the signa see") agrees e from or thr eement form see regardir perpetual, no	ture page to use ough ns the ng Free on-	V

- 5. Provide the path where the application files will be installed. A subdirectory (SCIMConnector) will be created in the specified path. Example C:\inetpub\wwwroot\SCIMConnector then click **Next**.
- 6. For Virtual Directory installations, it is recommended that you change the path otherwise IIS Manager will show both the folder and the virtual directory.

SCIMConnector Setup		_		×
Destination Folder				30
Click Next to install to the default fi	older or dick Change	to choose another.		1
Install SCIMConnector to:				
				,
C:\inetpub\wwwroot\				
Change				
	Back	Nevt	Can	el
	buck	HEAL	Cont	

7. At this point the SCIM Connector installation is ready to create the website.



8. After the installation has completed the default browse is launched and SCIM Connector is now ready to be configured. See Configuration section for additional details.

Note: Instead of creating a new web site the installation has created a virtual directory under the default website. The bindings or ports associated with the virtual directory are the same as the **Default Web Site**.



Note: the URL to access the SCIM Connector is different. To access the SCIM Connector when it is a Virtual Directory, use the host name or IP address and append /SCIMConnector.

💐 Internet Information Services (IIS) Manager

← → C ▲ Not secure localhost/SCIMConnector/#/?returnUrl=%2Fsettings	
	Secret Server Integrations
	Sign In
	Base url
	Username
	Password
	Sign In

- 9. The advanced Installation Process will create a new website.
- 10. The **Create new website with port options** installation process is the same as the standard process with the addition of having the ability to predefine the ports that will be used.
- 11. Select Create new website and click Next.

SCIMConnector			×
Select Your Choice Host your application Using		1	
Host your Application	ion under		
Do you want to install this	as a web site or a new	application under	
🔿 Use Default Web	Site		
Create new web	site		
	Back	Next	Cancel

Note: It is likely that there is already a default web site in IIS. If there is a port conflict the following dialog will appear allow the selection of a custom https port. Enter the https port that is desired in the provided field.

SCIMConnector		×
Existing Site Port Conflict		
Set custom port and Enable http		12-4
Detected existing sit	te running on po	rt
Another website which is already ru port. Choose a port that is not in u Connecting to SCIM Connector will URL(e.g. https://localhost:portnum	unning in IIS is using the sta ise for the SCIM Connector require adding the port nun iber)	andard 443 Site. aber to the
HTTPS Port: 8443		
Enable http (https binding will	also be enabled)	
	Back	ext Cancel

12. By default, HTTPS communication is recommended however in cases where SCIM endpoints may not work with HTTPS, enable http by selecting the **Enable Http** checkbox. Supply the custom available port for http and click **Next**.

BCIMConnector		×
Existing Site Port Conflict		
Set custom port and Enable http		
Detected existing si	ite running on por	t
Another website which is already port. Choose a port that is not in Connecting to SCIM Connector w URL(e.g. https://localhost:portnu	running in IIS is using the star use for the SCIM Connector S ill require adding the port num umber)	ndard 443 ite. ber to the
HTTPS Port: 8443		
Enable http (https binding wi	ill also be enabled) 8080	
	Back Ne	xt Cancel

13. The remainder of this Advanced option is identical to the Standard installation process.

B Schriediniector				×
Application Name				
Please enter the nam	e of the application			24
This value will be used that will be created.	for the name of the S	CIM Connecto	or website and the a	pplication pool
Application Name	SCIMConnector			
		D- di	Next	C1
		Back	Next	Cancel
SCIMConnector Setun			_10	
Serviconnector Setup			1	
	•			
End-User License Ag	reement	C .!!		State of Lot
End-User License Ag Please read the following	reement ng license agreement o	carefully		
End-User License Ag Please read the followir	reement	carefully		
Please read the followin	reement ng license agreement (TIONS FOR THYCO 10 ("Agreement")	carefully OTIC FREE S	OFTWARE PRO	
End-User License Ag Please read the followin TERMS AND CONDI This agreement (th conditions under v	reement ng license agreement (ITIONS FOR THYCO IE "Agreement") vhich Thycotic Soi	OTIC FREE S sets forth t ftware, LLC	OFTWARE PRO he terms and ("Thycotic") ag	DUCTS ^ rees
TERMS AND COND This agreement (th conditions under v to license and the	reement ng license agreement (ITIONS FOR THYCO 10 "Agreement") vhich Thycotic So party whose nam	Carefully OTIC FREE S sets forth t ftware, LLC e appears (OFTWARE PRO he terms and ("Thycotic") ag on the signature	DUCTS ^ rees a page
TERMS AND COND This agreement (th conditions under v to license and the of this Agreement	reement Ing license agreement (ITIONS FOR THYC(10 "Agreement") which Thycotic So party whose nam under Licensee (1 reduct that are o	CATE FAILS OTIC FREE S Sets forth t ftware, LLC ie appears (the "Licens the fford from	OFTWARE PRO he terms and ("Thycotic") ag on the signature ee") agrees to i from or thous	DUCTS A rees 2 page Jse
TERMS AND COND This agreement (th conditions under v to license and the of this Agreement certain software pi Thycotic's website	reement ng license agreement (ITIONS FOR THYC(ne "Agreement") which Thycotic Soi party whose nam under Licensee (f roducts that are o ("Free Products")	CATE CATERNIC CATERNI	OFTWARE PRO he terms and ("Thycotic") ag on the signature ee") agrees to from or throug ement forms t	DUCTS A rees e page use th ne
TERMS AND COND This agreement (th conditions under v to license and the of this Agreement certain software p Thycotic's website entire agreement	reement ITIONS FOR THYCO ITIONS FOR THYCO ("Agreement") which Thycotic So party whose nam under Licensee (1) roducts that are o ("Free Products") between Thycotic	Carefully OTIC FREE S sets forth t ftware, LLC e appears of the "Licens offered free (). This Agre c and Licens	OFTWARE PRO he terms and ("Thycotic") ag on the signature ee") agrees to o from or throug eement forms t see regarding F	DUCTS A rees a page ise th he ree
TERMS AND COND This agreement (th conditions under v to license and the of this Agreement certain software p Thycotic's website entire agreement Products.	reement Ing license agreement (ITIONS FOR THYCO ("Agreement") which Thycotic So party whose nam under Licensee (troducts that are of ("Free Products") between Thycotic	Carefully OTIC FREE S sets forth t ftware, LLC te appears of the "Licens offered free (). This Agre c and Licens	OFTWARE PRO he terms and ("Thycotic") ag on the signature ee") agrees to from or throug eement forms ti see regarding F	DUCTS A rees page sse th ne ree
TERMS AND COND This agreement (th conditions under v to license and the of this Agreement certain software pu Thycotic's website entire agreement Products. License. Thycotic h	reement Ing license agreement (ITIONS FOR THYCO ("Agreement") which Thycotic Sor party whose nam under Licensee (the roducts that are of ("Free Products") between Thycotic ereby grants to Li	Carefully OTIC FREE S sets forth t ftware, LLC ie appears of the "Licens offered free (). This Agre c and Licens icensee a p	OFTWARE PRO he terms and ("Thycotic") ag on the signature ee") agrees to from or throug eement forms ti see regarding F erpetual, non-	DUCTS A rees page spage spage ree
TERMS AND COND This agreement (th conditions under v to license and the of this Agreement certain software p Thycotic's website entire agreement Products. License. Thycotic h	reement Ing license agreement (ITIONS FOR THYCO ("Agreement") which Thycotic So party whose nam under Licensee (no roducts that are o ("Free Products" between Thycotic ereby grants to Li the License Agreement	Carefully OTIC FREE S sets forth t ftware, LLC te appears of the "Licens offered free (). This Agre c and Licens icensee a p	OFTWARE PRO he terms and ("Thycotic") ag on the signature ee") agrees to o from or throug eement forms ti see regarding F erpetual, non-	DUCTS A rees page sse th ne ree
TERMS AND COND This agreement (th conditions under v to license and the of this Agreement certain software p Thycotic's website entire agreement Products. License. Thycotic h	reement Ing license agreement (ITIONS FOR THYC) ("Agreement") which Thycotic Soi party whose nam under Licensee (fr roducts that are o ("Free Products" between Thycotic ereby grants to Li the License Agreement	Carefully OTIC FREE S sets forth t ftware, LLC e appears o the "Licens offered free c and Licens icensee a p the Back	OFTWARE PRO he terms and ("Thycotic") ag on the signature ee") agrees to t efrom or throug eement forms ti see regarding F erpetual, non-	DUCTS A rees 2 page 1se th he ree v

* SCIMConnector Setup			
Destination Folder		-	
Click Next to install to the default fo	lder or <mark>d</mark> ick Change	to choose another	
Install SCIMConnector to:			
C:\inetpub\wwwroot\			
, Change			
	Back	Next	Cancel
R SCIMConnector Setup			
Ready to install SCIMConnecto	or		44
Click Install to begin the installation. installation settings. Click Cancel to e	Click Back to review exit the wizard.	or change any of	your
	Back	Install	Cancel

Once the installation has completed, the log in page for SCIM Connector should be viewable in the default browser. If the browser does not launch you can access the SCIM Connector by browsing to the Website or Virtual application that was created. The login page requires the URL to Secret Server and a local Secret Server Administrator account.

- 14. Enter the URL to Secret Server and the Secret Server local Administrator Username and Password.
- 15. Click Sign in.

SCIM Server for Secret Server × +		-	-		×
← → C ▲ Not secure localhos	t:8443/#/?returnUrl=%2Fsettings	۵ C	*	θ	:
	Secret Server Integrations				-
	Sign In				
	Base url				
	Username				
	Password				
	Sign In				
4					+

Note: You may not see the in the Base URL with future logins. This is expected. The SCIM Connector will always attempt to Secret Server over https. In cases where Secret Server does not support https (not recommended), SCIM Connector will communicate over http, however the **Allow Http** option must be selected.

Even if the **Allow Http** option is selected, if Secret Server allows an https connection, SCIM Connector will communicate with Secret Server over https.

Introduction

This document is intended to provide best practices in relation to configuring SCIM for use with Secret Server. While we try to generalize much of the suggestions within this document so that it can apply to others vendors that are leveraging SCIM, we have chosen to work directly with Sailpoint as a partner for the development of this document. This means that some of the documentation does include screenshots specific to Sailpoint's IdentityIQ interface and configuration. We also reiterate Sailpoint specific limitations and concepts and walk through a few typical use cases that may be specific to Sailpoint.

Broad SCIM Implementation Considerations

- Secret Server does not delete users in order to maintain audit trails. As a result, when you delete a user with a SCIM call, it disables the user. The disabled user cannot be granted access to a container, privileged data, or group unless they are enabled again.
- Secret Server throws an error if instructed to delete an already deleted user. Disabling (deleting) already disabled users (by ID) will result in the SCIM Connector reporting a 404 error in the logs.
- The process for provisioning local user accounts versus adding AD accounts to Secret Server via SCIM may look vastly different based on each vendor. If you do plan to leverage local accounts in Secret Server, it is recommended in your SCIM provider to auto-create passwords that align with the local user password policy configured within Secret Server. Otherwise you may get an error when generating a new account through SCIM that does not conform to the Secret Server Local User password requirements. This can be found in Admin > Configuration > Local User Passwords. Below is a screenshot of the local user password requirement that will clear our security hardening report.

Symbols Required for Passwords	Yes
Lowercase Letters Required for Passwords	Yes
Uppercase Letters Required for Passwords	Yes
Numbers Required for Passwords	Yes
Minimum Password Length	8

- Some SCIM providers when creating an Application define an "Owner" of that application. This owner may be leveraged for approvals of
 some requests within the SCIM Server. It is important to think about who you want the Application owners to be. This often may be
 aligned with Secret Server SMEs but may also be aligned with "approvers" that you use within Secret Server for Request Access For
 Approval workflows.
- Careful consideration should be made when determining who should have access to the "SCIM Connector Secret" that is stored within Secret Server long term. Those who are Administering the SCIM Connector should have access to this Secret, but likely no other users except for possibly a Secret Server SME/Admin. This is because this Secret Contains legitimate account information for an API user within Secret Server. It is recommended to combine this Secret with a Request For Access workflow process for any additional users that may request access to this Secret outside of your initial defined list of users. This flow is documented in our recently published SCIM 2.5 documentation.

SCIM AWS-WIN-CLIENT1 > SCIMSecret AWS-WIN-CLIENT1 ☆



- It is recommended to track where all within your environment your SCIM API user account is being leveraged so that you can ensure
 that account does not have access to secrets or folders that you do not want it to have access to. Since the account has privileged
 access within Secret Server, this is important. You may even want to align specific event subscriptions within Secret Server to track
 the activity of SCIM. There are several reports that are generated when using SCIM to help track this type of activity as well that can be
 sent to specific people on a schedule. Below is a list of the built in reports that are generated and can be used:
 - SCIM All Users
 - SCIM All Groups
 - SCIM All User Groups
 - SCIM All Folders
 - SCIM All Folder Permissions
 - SCIM All Secrets
 - SCIM All Secrets Permissions
- It is important to be mindful of this setting under Admin > Configuration > Folders.

Require View Permission on Specific Folder for Visibility		
---	--	--

If this is set to Yes, which is a best practice within Secret Server, you will need to be careful when breaking inheritance to assign permissions to a user to a subfolders from your SCIM provider. If for example they are assigned "View" access to a subfolder but not the parent folder, then they may not be able to navigate to the folder that they have been provisioned access to. If this setting is unchecked, they will be able to view the folder structure and access the specific subfolder they've been regardless of parent folder level access.

Sailpoint Specific Concepts and Limitations

https://docs.delinea.com/scim/current/vendors/sailpoint/sp-constraints.md

• In SailPoint IdentityIQ, there are "containers" and "privileged data." The containers map to Secret Server folders, and privileged data

maps to secrets.

- SailPoint allows adding permissions to containers, but they cannot be directly added to privileged data. That is, they cannot be added directly to a Secret Server Secret. So when a user gets access to a container, the user is really getting access to a Secret Server folder.
- While there is no direct way to give users access to a specific secret, they can still be given access indirectly by adding a user into a group that already has access to both the folder/container and the secret/privileged data.
- When a users are given access to a container/folder, either with direct access or by adding them to a group, they only have "view" access to the container. More granular assignment of permission levels can only be defined in SS.
- If the "view" permission setting seen in the Configuring a "SailPoint IdentityIQ Endpoint" section is not configured correctly, an incorrectly formatted POST call to the SCIM Connector application will result, which returns a HTTP 400 error message.
- Any sensitive information that is associated with a secret/privileged data, such as a password, is not shared over the SCIM Connector and must be viewed in SS.
- Personal folders in Secret Server can be viewed in SailPoint, but users cannot be given direct access to the folders. However, users can be given access by adding them to an existing group. The owner of the personal folder cannot have their access removed from the folder.
- Using custom attributes or extensions with SailPoint IdentityIQ and the SCIM Connector is not currently supported.

The following sections assumes that you have Sailpoint connected to Secret Server SCIM and that the connectivity has been validated as working. Below we cover the most common "Create" type use cases

SCIM - Creating New Users

For creating new "Local" users in Secret Server from Sailpoint, ensure that you have a Provisioning policy with a form for creating new accounts. Below is a screenshot of this area in Sailpoint.

Edit Application Thycotic PAM

Details	Configuration	Correlation	Accounts	Risk	Activity Data Sources	Unstructured Targets	Rules	Password Policy
Settings	Schema Pro	visioning Po	licies					
A list of pro	ovisioning policies a	ssociated with thi	s application. Ac	id a new	v policy with Add Provisioning Po	olicy or edit an existing policy b	y selecting	it from the list.
Object	Type: account							
Туре			Name				Des	cription
Create		(Create Account	Form			Provis	sioning form for create account.
Update								
Delete								
Enable Ac	ccount							
Disable A	ccount							
Unlock Ac	count							
Change P	assword							

The form itself has a few fields that are relevant to be completed for new users provisioned through Sailpoint

Create Ac	count Form	Provisioning form for create account.					
	Add Section	Preview Form					
÷				•	ø	×	
÷	User Name				din .	×	
+	Formatted Name				dit .	×	
4	Family Name				din .	×	
4	Given Name				dit .	×	
4	Display Name				di s	×	
+	Email				dir.	×	
+	Password				din .	×	

The password field aligns with a password policy rule. This rule should align with your Secret Server's local password policy so that you can ensure when users are provisioned through Sailpoint, that they are compliant with the rules enforced for new local users in Secret Server, and provision correctly.

Settings			^
Name			
password			
Display Name			
password			
Help Text			
Туре			
String			*
Type Settings			^
Multi-Valued Required	 Refresh on Change Review Required 	Authoritative Display Only	

Multi-Valued	Refresh on Change	Authoritative	
Required	Review Required	Display Only	
Read Only			
False			•
Hidden			
False			*
Owner			
None			*
alue Settings			-
Dynamic			
Value			
Rule			*
Thycotic PW Rule		~	
Allowed Values			
None			*
Validation			
None			~

Create a new identity in Sailpoint. This can be done under the **Manage Identity** section and by clicking **Create Identity**.

Create Identity

If you would like to request that a new identity be created, please fill in the fields below. Fields marked with an asterisk are required.

IdentityInc - Create Identity		
Basic User Information		
First Name *		Last Name *
Tester		McTester
User Type *		Location
Employee	~	
Mobile Phone #		Calculated User Name *
		Tester.McTester
This will be used for SMS Password Reset		
Calculated Email		
Tester.McTester@salipointdemo.com		
Organizational Information		
Manager *		
David Anderson		
Department *		
Human Resources		
Job Title *		
Accounts Payable Analyst		
Ca	ncel	Submit

Approve the creation of the account. Under Manage Access > Manage Accounts section, locate the user you created then click Manage

Manage Accounts		
	A	
	Tester McTester	
Username: Tester.McTester		
Manager: David Anderson		
	Manage	

Click the Request Account button

 Identity Details 	
Accounts 0	Requet/Account
	No Results

Select Delinea PAM.

Request Account	×
Summary of Request for Tester McTester Verify the changes you have requested below. Application *	
Thycotic PAM	~
Type your comment here	
	Submit Cancel

When you get to the **Submit** page it will indicate that more information is needed and you need to complete a form.

Complete the form.

Request Information

Requester The Administrator

TMcTester

Tester McTester

Target Identity			
First Name Tester	Last Name McTester	Account ID Tester McTester	
Thycotic PAM			
User Name *			
TMcTester			
Formatted Name *			
Tester McTester			
Family Name *			
McTester			
Given Name *			
Tester			
Display Name *			
Tester McTester			
Email *			
Tester.McTester@gmail.com			
Password *			
Cancel		O	
Click OK at the bottom. The account char	nge submission should happen and can be	tracked under My Work > Access F	Requests.
Manage Accounts: Tester McTester Requested by The Administrator on 11/24/20 Request ID: 33			
O Request pending			
Create: TMcTester on Thycotic PAM		0	Provisioning
You can check Secret Server to verify tha	t the account has been created under Ad	min > Users.	

If you run your Perform Identity Request Maintenance task, you should see the My Work Access Request show up as complete

Yes

Local

< None >

Never

Tester.McTester@gmail.com

Manage Accounts: Tester McTester Requested by The Administrator on 11/24/20 Request ID: 33	
O Request pending	
Create: TMcTester on Thycolic PAM	Complete

When assigning a user to an AD group, simply provision the user to the AD group within Sailpoint. The easiest way we have found to do this is under the **Manage Access > Manage User Access** tab. Filter based on the Active Directory Application you have already added to Sailpoint.

Manage User Access							Help
1 Select Users Find and select users for whom you want to manage access.			2 Manage Access Add access for the users you've selected.		3 Review and Submit Look over your selections and confirm.		
	tester				Q T Filters	×	
Identities Selected: Tester McTester				Showing 1-1 of 1			
Tester McTester							
Username: Tester McTester Manager: David Anderson							
Identities Selected: Tester McTester				Showing 1-1 of 1			
Select Users Find and select users for whom you want to manage access.			2 Manage Access Add access for the users you've selected.		3 Review and Submit Look over your selections and confirm.		0
	Add	Access			Remove Access		
	Search By Keywords 🗸	Search Access			Q T Filters V		
Identities Selected: Tester McTester				Showing 1-12 of 69			
AccountingGeneral						D) etails
Grants basic accounting access to the internal Accounting System Type: Entitlement Owner: Loti Ferguson Application: Active Dir	ectory Attribute: memberOf						
1 Select Users Find and select users for whom you want to manage access.			2 Manage Access Add access for the users you've selected.		3 Review and Submit Look over your selections and confirm.		0
Identities Selected: Tester McTester							
Add Access 1							
× AccountingGeneral							Details
Grants basic accounting access to the Internal Accounting System Type: Entitlement Owner: Lori Ferguson Application: Active Dire	ctory Attribute: memberOf						

Ensure that on the Secret Server side, that this group is set up for Synchronization for the Domain you have added. On the next Secret Server AD synchronization, this user will be added to Secret Server and will be provisioned access to any folders where that AD group is aligned for access.

SCIM - Assigning Users to Local Secret Server groups

Go to the **Manage Access > Manage User Access** tab and apply a filter to filter based on the Delinea PAM application. This should reveal any local groups in Secret Server

1 Select Users Find and select users for whom you want to manage access.		2 Manage Access Add access for the users you've selected.		3 Review and Submit Look over your selections and contrex.	0
	Ac	dd Access 🕦		Remove Access	
	Search By Keywords 🗸	Search Access		Q T Filters v	
Identities Selected: Tester McTester		Shi	wing 1-6 of 6		
Everyone					Details
Type: Entitlement Application: Thycolic PAM Attribute: groups					
Management					Details
Type: Entitlement Application: Thycolic PAM Attribute: groups					

Select Users Find and select users for whom you want to manage access.	2 Manage Access Add access for the users you've selected.	3 Review and Submit Look over your selections and confirm.	0
Identities Selected: Tester McTester			
Add Access 1			m
× Management			Details
Type: Entitlement Application: Thycolic PAM Attribute: groups			

You can verify this user was added to the group in Secret Server

View User

User Name	TMcTester
Display Name	Tester McTester
Email Address	Tester.McTester@gmail.com
Domain	Local
Two Factor	< None >
Enabled	Yes
Locked Out	No
Application Account	No

IP Address Restrictions

None

Restricted By Team No

GROUPS FOR USER

Save To File < 1 to 1 of 1 >

GROUP NAME

Management

ROLES FOR USER

Save To File < 1 to 1 of 1 >

ROLE NAME

User

SCIM - Creating New Groups

One way to create local groups within Secret Server through Sailpoint is under the **Applications > Entitlement Catalog** section. You can click on **Add New Entitlement**

Entitlement Catalog							
Filter Entitlements	Advanced Search						Import Export Add New Entitlement
Application	Attribute	Display Name	Туре	Description	Owner	Requestable	Classifications
Oracle EBS	RESPONSIBILITIES	1Sync Super User	RESPONSIBILITY	Administrative rights to 1Sync		8	



Then click on the Delinea PAM Application. For Type, choose Group, and for Display Value enter the display value of your group.

New Group

Standard Pro	perties	Object Properties	Classifications	
*Indicates a requ	uired field.			
Application *	Thycotic	PAM	*	
Type *	Group		*	
Attribute *	groups			
Value *	The value	e for this group will correspo	ond to the id attribute f	rom the group schema.
Display Value	ThisIsMy	Group		
Requestable				
Description	B 7 of 1024	I I I IIII IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII		English (United States) -
Owner	a Tester	r McTester	*	
Scope			~	

New Group

tandard Properties	Object Properties	Classifications	
Object Attributes			
Display Name*	ThisIsMyGroup		

After you click save, you will have to approve the workflow. Then the group will be created in Secret Server.

7 Items All Domains 🗸 🔾

GROUP NAME	1	ENABLED	CREATED
Everyone		Yes	2/16/2017 04:46 pm
Management		Yes	1/17/2018 08:31 pm
Secret Server Administrators		Yes	2/17/2017 02:01 pm
Secret Server Basic Users		Yes	1/10/2018 10:47 pm
Secret Server Users		Yes	2/17/2017 02:01 pm
sptAppTestGroup		Yes	11/19/2020 06:32 pm
ThisIsMyGroup		Yes	11/24/2020 06:33 pm

As previous examples have shown, you can create a provisioning policy form similarly to the Create Identity form we did earlier.

SCIM - Assigning Users To Folders

When assigning users to folders, please ensure that the SCIM API account has the correct access to the folder in which you want to add the user to. As mentioned in the best practices, assign the minimum permissions needed for anticipated access that is required to be provisioned through SCIM.

In this example I removed the Tester account from the management group in Secret Server. I then assigned the user to the Data Management folder in Secret Server through Sailpoint.

(Before)



Folder Permissions Edit

Sets who may access the folder. This is determined by folder inheritance, as well as user and group permissions.

Inherit Permissions No

Selected Groups		
User or Group	Folder Permission	Secret Permission
localAdmin	Owner	Owner
Management	Owner	Owner
scim	View	View

In Sailpoint, go to Manage Access > Privileged Account Management. Locate the Folder in question and click manage

Data Manageme	ent
Total Identities	2
Groups	1
Privileged Items	0
Manage	

Click the Add Identities button

<pre>ver @ ver @ v</pre>	< Data Management		
Interest and independent of the second of the s	Identifies 2 Groups () Privileged Items ()		
Image: No Results Image: Order Description Image: Order Description </th <th>Direct Access Effective Access 2</th> <th></th> <th>+ Add Identities</th>	Direct Access Effective Access 2		+ Add Identities
Choose Identities Add Container Permissions Search Identities Tester McTester	Buk Remove		Columns 🗸
 Choose Identities Choose Identities Add Container Permissions Search Identities Tester McTester 	No F	Results	
 Choose Identities Add Container Permissions Search Identities Tester McTester 			
Choose Identities Add Container Permissions Search Identities Tester McTester			
Choose Identities Search Identities Tester McTester	Choose Identities	X .	
Choose Identities 2 Add Container Permissions Search Identities • Tester McTester 			
Search Identities Tester McTester	Choose Identifies 2. Add Container Bermissions		
Search Identities Tester McTester	2 Add Container Permissions		
Tester McTester			
Tester McTester	Search Identities	~	
Tester McTester			
	Tester McTester		
Cancel	Cancel	Next	

Align the View permission

Add Container Permissions	×
1 Choose Identities 2 Add Container Permissions	
✓ View	
Owner	
Edit	
Cancel	Previous Submit

After the task has ran, verify that the account has been added to the folder

Folder Permissions Edit

Sets who may access the folder. This is determined by folder inheritance, as well as user and group permissions.	Inherit Permissions	No	
	Selected Groups		
	User or Group	Folder Permission	Secret Permission
	localAdmin	Owner	Owner
	Management	Owner	Owner
	scim	View	View
	TMcTester	View	View

This reference architecture is our best practice architecture/design for Delinea Secret Server leveraging SCIM 2.5. We have provided high level communication requirements, which does not include Secret Server component specific communication. These variations can be combined with either Secret Server or Secret Server Cloud.

Below is a high level summary of the design variations:

- SS-SCIM-REF#01 A-1 SS On Prem + SCIM
- SS-SCIM-REF#01 A-2 SS On Prem + SCIM (Perimeter Network)
- SS-SCIM-REF#01 B-1 SSC + SCIM
- SS-SCIM-REF#01 C-1 Request Communication Flow

Definitions for SS-SCIM-REF #01 - A-1

- Customer issuing an on-premise installation of Secret Server installed in an on premise location with a dedicated system for the SCIM Connector. While the SCIM Connector can be installed on the same system as Secret Server, this is not recommended for large production environments.
- The SCIM Server Layer is your 3rd party SCIM Server installed in an on-premise location (Examples include Sailpoint IdentityIQ, Pingldentity, etc).

Requirements for SS-SCIM-REF #01 - A-1

- Outbound communication from your SCIM Server to the SCIM Connector is required for integration.
- Outbound communication from your SCIM Connector to the SCIM Server is not required currently, but may be required in the future.
- While this diagram shows the default port for https (443), other ports may be leveraged between your SCIM. Server and SCIM Connector and between your SCIM Connector and Secret Server.
- SCIM Connector System Requirements:
 - Windows Server 2012 R2+, Windows Server 2019
 - 4 Core CPU
 - 4 GB RAM



Definitions for SS-SCIM-REF #01 - A-2

- Customer issuing an on-premise installation of Secret Server installed in an on premise location with a dedicated system for the SCIM Connector. While the SCIM Connector can be installed on the same system as Secret Server, this is not recommended for large production environments.
- The SCIM Server Layer is your 3rd party SCIM Server SaaS offering.

Requirements for SS-SCIM-REF #01 - A-2

- Outbound communication from your SCIM Server to the SCIM Connector is required for integration.
- Outbound communication from your SCIM Connector to the SCIM Server is not required currently, but may be required in the future.
- It is recommended that your SCIM SaaS Server and your On Premise data center be located in a similar region, although the application can accomodate high latency.
- While this diagram shows the default port for https (443), other ports may be leveraged between your SCIM Server and SCIM Connector and between your SCIM Connector and Secret Server.
- SCIM Connector System Requirements:
 - Windows Server 2012 R2+, Windows Server 2019
 - 4 Core CPU
 - 4 GB RAM



Definitions for SS-SCIM-REF #01 - B-1

- Customer issuing SSC hosted in Azure with a dedicated system for the SCIM Connector installed in the customers Azure private cloud. SCIM Connector does not have an option to be installed on SSC application servers.
- The SCIM Server Layer is your 3rd party SCIM Server SaaS offering.

Requirements for SS-SCIM-REF #01 - B-1

- Outbound communication from your SCIM Server to the SCIM Connector is required for integration.
- Outbound communication from your SCIM Connector to the SCIM Server is not required currently, but may be required in the future.
- It is recommended that your SCIM SaaS Server and your private cloud data center be located in a similar region, although the application can accomodate high latency. Azure is provided as an example, but any other private cloud vendor may be leveraged for installing the SCIM Connector.
- While this diagram shows the default port for https (443), other ports may be leveraged between your SCIM Server and SCIM Connector and between your SCIM Connector and Secret Server. SSC currently only uses port 443.
- SCIM 2.5 is required for integration with Secret Server Cloud
- WAF Inbound Firewall Requirements for SSCare:
 - Public IP is based on geographical location
 - IP Addresses for all regions: 45.60.38.37, 45.60.40.37, 45.60.32.37, 45.60.34.37, 45.60.36.37, 45.60.104.36

- SCIM Connector System Requirements:
 - Windows Server 2012 R2+, Windows Server 2019
 - 4 Core CPU
 - 4 GB RAM



SS-SCIM-REF#01 - C-1 - Request Communication Flow





This section provides documentation links to currently supported third-party vendors for the SCIM Connector.

SCIM is a standard for automating the exchange of user identity information between identity domains, or IT systems. Secret Server is fully SCIM compatible today, so any 3rd party product that supports SCIM can talk to Secret Server out-of-the-box. Leveraging the SCIM connector allows Secret Server to be fully SCIM compatible.

Below is a list of integrations we have already tested and documented. These include but are not limited to:

- Okta SCIM Integration
- <u>SailPoint IdentityIQ</u>
- <u>OneLogin</u>

The following table provides links to other SCIM compatible third-party product documentation pages:

Active Directory SCIM Provisioning - Automatic provisioning of users and groups between your Secret Server and Azure AD (AAD). Secret Server also has native Azure AD integration which is the preferred Azure AD integration choice.	Microsoft	<u>Reference</u>
AuthX	The Control Group	<u>Reference</u>
Federated Directory	Fed Blokes	Reference
GitHub	GitHub, Inc.	Reference
Gluu	Gluu.org	Reference
Idaptive	Cyberark, Inc.	<u>Reference</u>
Microsoft Identity Manager (MIM) - SCIMv2 Management Agent	Traxion	Reference
Omada Identity Suite	Omada	Reference
One Identity - Identity Manager	One Identity	Reference
Oracle Identity Cloud Service	Oracle	Reference
Oracle Identity Manager	Oracle	Reference
Peakon	Peakon	Reference
PingDataGovernance	Ping Identity	<u>Reference</u>

RadiantOne Federated Identity Service	Radiant Logic	<u>Reference</u>
SCIM	Elimity	Reference
SOFFIDIAM	soffid	Reference
Trello	Trello	<u>Reference</u>

This section includes the most recent SCIM Connector Release Notes.

• <u>3.0 Release Notes</u>

Previously released versions:

- 2.5 Release Notes
- 2.0 Release Notes

Release Date: September 2021

Upgrade and Installation Notes

- The newly created SCIM Installer will upgrade the previous SCIM installer from 2.5 to 3.0.
- The new installer has added Flexibility for installation. i.e. the user can customize the installer.

Enhancements

- The new release includes making resource ID's unique across all resources for Users, Groups, Containers, PriviledgeData, Container Permission, Priviledged Data Permission.
- Patch remove value operation:
 - If the value attribute passes in the patch request for remove operation, it should return error Error: "Value attribute not supported in remove operation".
 - Newly added Setting in the SCIM Config Page for Patch remove value operation.
 - The default value is false.
 - When the setting is **true**, the Patch remove value operation will remove the value from the resource.

Known Issues

With the latest release of the Delinea Secret Server two new tables were added, **tbFolderACL** for folders and **tbSecretACL** for secrets in the Reports named SCIM ALL Folder Permission and SCIM ALL Secrets Permission respectively. With that change, data might not be promoted correctly for SCIM integrations, since the SCIM Connector 3.0 references the old tables,

with that change, data might not be promoted correctly for SCIM integrations, since the SCIM Connector 3.0 references the old tables which are **tbFolderGroupPermission** and **tbGroupSecretPermission**.

Workaround

This can be fixed with the following workaround, by updating the query in the Delinea Secret Server Reports named *SCIM ALL Folder* permission and *SCIM ALL Secrets* permission.

Please follow these steps for the workaround:

- 1. Login to Delinea Secret Server.
- 2. Navigate to Reports.
- 3. Click on SCIM All Folder Permission.
- 4. On the SCIM All Folder Permission page, click Edit.
- 5. Replace the query: SS_Report_All_Folders_Permission.sql
- 6. Click Save.
- 7. Click on SCIM All Secret Permission.
- 8. On the SCIM All Secret Permission page, click **Edit**.
- 9. Replace the query : SS_Report_All_Secrets_Permission.sql
- 10. Click Save.

SQL Queries

• SS_Report_All_Folders_Permission

SELECT X.Id, X.Folderld, FolderName, GroupId, GroupName, Userld, UserName, FolderAccessRoleName,KnownAs, ISNULL(Y.Created,X.Created) Created,ISNULL(Y.LASTMODIFIED, X.Created) LastModified FROM

- (
- SELECT FACL.FolderGroupPermissionId Id ,FACL.FolderId

```
,F.FolderName
                ,CASE WHEN G.ISPERSONAL = 0 THEN FACL.GroupId ELSE NULL END GroupId
               ,CASE WHEN G.ISPERSONAL = 0 THEN G.GroupName ELSE NULL END GroupName
                .U.UserId
                ,U.UserName
               CASE (FACL FolderPermissions) WHEN 1 THEN 'View' WHEN 1 | 2 THEN 'Add Secret' WHEN 1 | 2 | 4 THEN 'Edit' WHEN 1 | 2 | 4 | 8 THEN 'Owner' END
As FolderAccessRoleName
               ,CASE WHEN G.ISPERSONAL = 0 then G.GroupName ELSE isnull(U.DisplayName, U.UserName) END KnownAs
                .U.Created
           FROM DBO.tbFolderACL FACL WITH(NOLOCK)
          INNER JOIN dbo.tbGroup G WITH(NOLOCK)
ON FACL.GroupId = G.GroupId
LEFT JOIN dbo.tbfolder F WITH(NOLOCK)
            ON FACL.folderId= F.folderid
           LEFT JOIN dbo.tbUserGroup UG WITH(NOLOCK)
            ON G.GroupId = UG.GroupId
            AND G.IsPersonal = 1
           LEFT JOIN dbo.tbUser U WITH(NOLOCK)
            ON UG.UserId =U.UserId
           WHERE
              (G.Active = 1 OR (G.IsPersonal = 1 AND U.Enabled = 1))
  ) X
  LEFT JOIN
    SELECT FOLDERID. MIN(DATERECORDED) CREATED.MAX(DATERECORDED) LASTMODIFIED
     FROM DBO.TBAUDITFOLDER WITH(NOLOCK)
    WHERE FOLDERID IS NOT NULL
     GROUP BY FOLDERID
```

) Y ON X.FolderId = Y.FolderId

• SS_Report_All_Secrets_Permission

SELECT X.Id, X.SecretID, SecretName, GroupId, GroupName, UserId, UserName, SecretAccessRoleName,KnownAs, Y.Created, Y.LastModified FROM

```
(
      SELECT SACL.GroupSecretPermissionId Id
           ,SACL.SecretID
           ,S.SecretName
           ,ST.SecretTypeName
          ,CASE WHEN G.ISPERSONAL = 0 THEN SACL. GroupId ELSE NULL END GroupId
          ,CASE WHEN G.ISPERSONAL = 0 THEN G.GroupName ELSE NULL END GroupName
           .U.UserId
           U.UserName
          CASE (SACL.Permissions) WHEN 1 THEN 'List' WHEN 1 | 2 THEN 'View' WHEN 1 | 2 | 4 THEN 'Edit' WHEN 1 | 2 | 4 | 8 THEN 'Owner' END As
SecretAccessBoleName
          ,CASE WHEN G.ISPERSONAL = 0 then G.GroupName ELSE isnull(U.DisplayName, U.UserName) END KnownAs
       ,U.Created
FROM
          DBO.tbSecretACL SACL WITH(NOLOCK)
       INNER JOIN DBO.tbGroup G WITH (NOLOCK)
         ON SACL.GroupId = G.GroupId
        LEFT JOIN dbo.tbSecret S WITH(NOLOCK)
         ON SACL.SecretId= S.SecretId
        LEFT JOIN dbo.tbSecretType ST WITH(NOLOCK)
         ON S.SecretTypeID= ST.SecretTypeID
        LEFT JOIN DBO.tbUserGroup UG WITH(NOLOCK)
         ON g.GroupId = UG.GroupId
       AND g.IsPersonal = 1
LEFT JOIN DBO.tbUser U WITH(NOLOCK)
         ON UG.UserId = U.UserId
       WHERE
          (G.Active = 1 OR (G.IsPersonal = 1 AND U.Enabled = 1))
  ) X
  LEFT JOIN
    SELECT SecretId, MIN(DATERECORDED) CREATED, MAX(DATERECORDED) LASTMODIFIED
     FROM DBO.TBAUDITSecret WITH(NOLOCK)
    WHERE SecretId IS NOT NULL
     GROUP BY SecretId
  ) Y ON X.SecretID = Y.SecretID
```

April 2022

• Added <u>known issue and workaround</u> to SCIM Connector 3.0 release notes to address table changes introduced via the last Secret Server release.

September 2021

• SCIM Connector 3.0 release, added <u>Release Notes</u>