



Delinea

Delinea Integrations

Documentation © 0-previous



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
<i>Download the Installer</i>	11
<i>Installing SCIM Connector</i>	11
<i>Basic Installation</i>	11
<i>Standard Installation Process</i>	11
<i>Upgrade from Version 2.5 to 3.0</i>	17
Launch SCIM Connector after Installation/Upgrade	18
Advanced Installation	20
<i>Download the Installer</i>	20
SCIM Connector Best Practices for Integration With Secret Server	29
<i>Introduction</i>	29
<i>Broad SCIM Implementation Considerations</i>	29
<i>Sailpoint Specific Concepts and Limitations</i>	30
<i>SCIM - Creating New Users</i>	31
<i>SCIM – Assigning Users to Local Secret Server groups</i>	37
<i>SCIM – Creating New Groups</i>	38
<i>SCIM – Assigning Users To Folders</i>	40
Architecture Diagrams for SCIM 2.5	43
<i>Definitions for SS-SCIM-REF #01 - A-1</i>	43
Requirements for SS-SCIM-REF #01 - A-1	43
<i>Definitions for SS-SCIM-REF #01 - A-2</i>	44
Requirements for SS-SCIM-REF #01 - A-2	44
<i>Definitions for SS-SCIM-REF #01 - B-1</i>	45
Requirements for SS-SCIM-REF #01 - B-1	45
<i>SS-SCIM-REF#01 - C-1 - Request Communication Flow</i>	46
SCIM Connector Integrations	48
Release Notes	50

3.0 Release Notes	51
<i>Upgrade and Installation Notes</i>	51
<i>Enhancements</i>	51
<i>Known Issues</i>	51
Workaround	51
SQL Queries	51
Changelog	53
<i>April 2022</i>	53
<i>September 2021</i>	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 [SCIM Specification](#) 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 [SCIM 2.0 Extension for PAM](#) 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:

- [Getting Started](#)
- [System Requirements](#)
- [Account Permissions](#)
- [Standard Installation](#)
- [Advanced Installation](#)
- [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:
 - o IIS Web Server
 - o .net 4.52 or higher
 - o 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 Server / Web Site
 - o The ability to connect to SCIM Endpoints (such as Sailpoint, Okta, etc...)
 - o The account information to connect to each SCIM Endpoint
 - o 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:

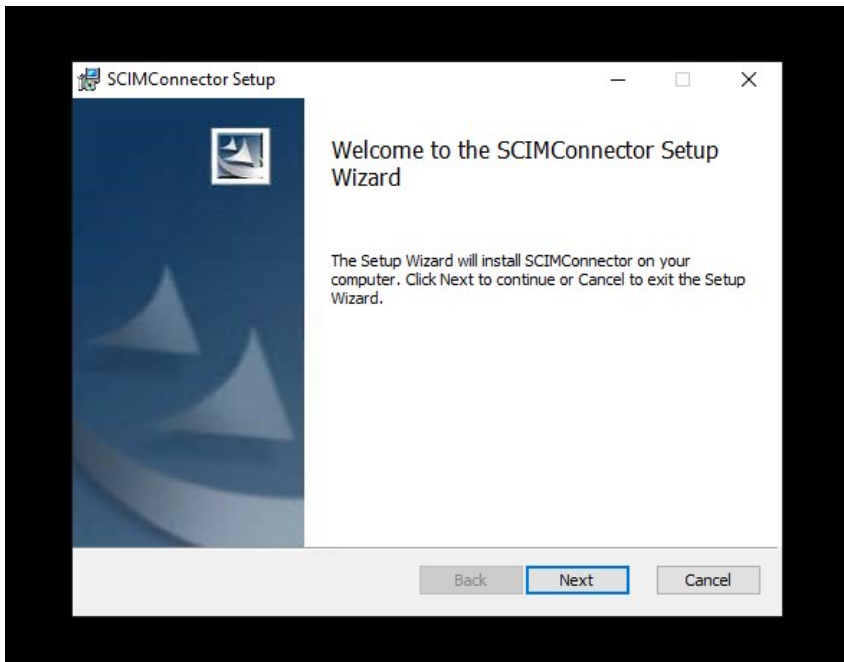
- [SCIM software download](#)

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.

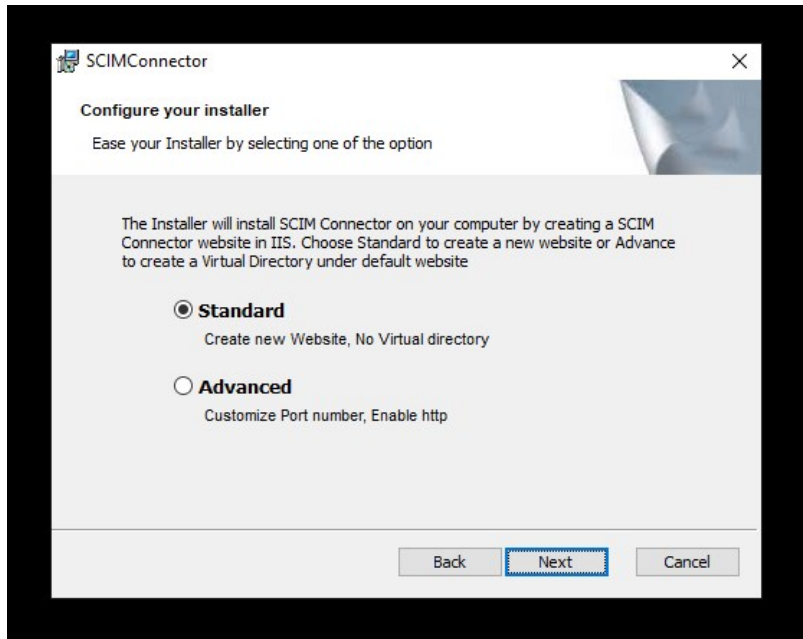


After the initial welcome dialog, select the type of installation to perform.

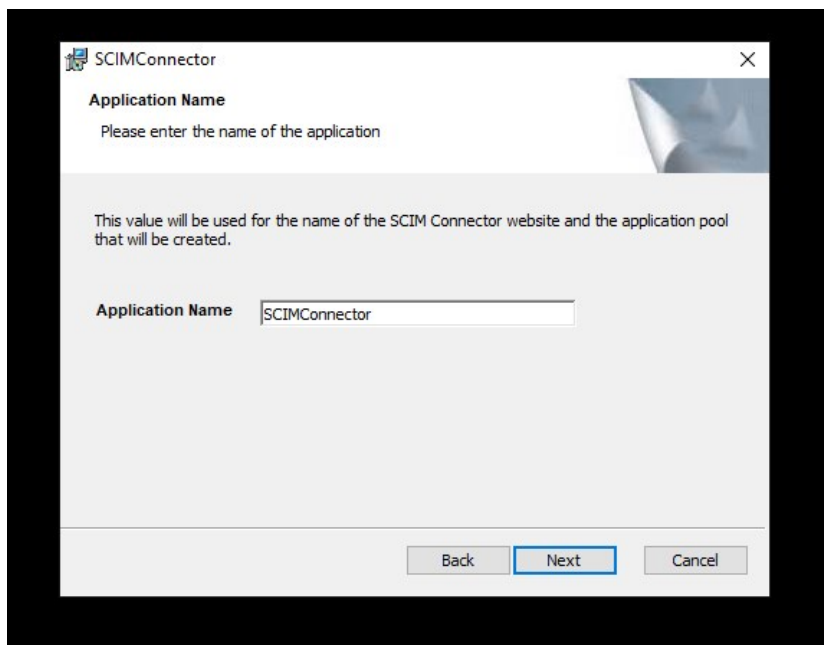
Standard Installation Process

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.

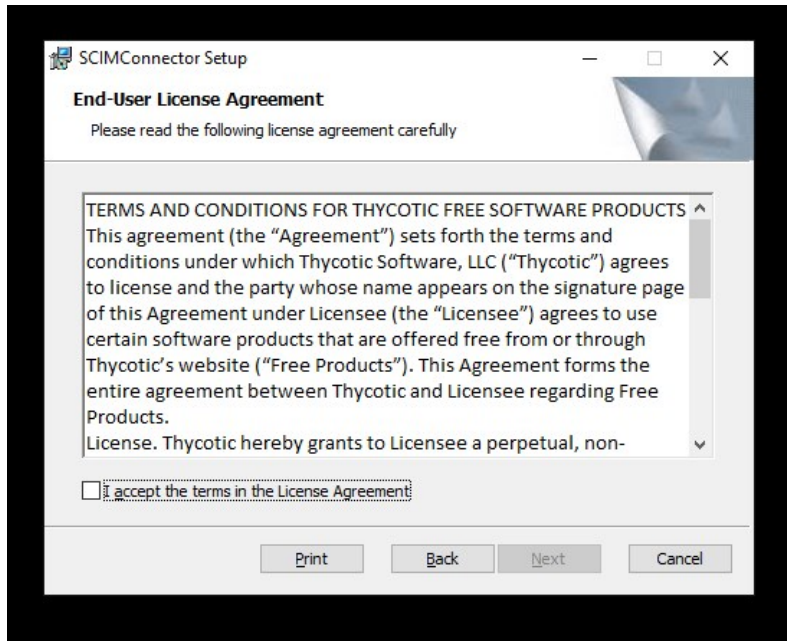
1. Select the Standard option to create a new website in IIS and click **Next**.



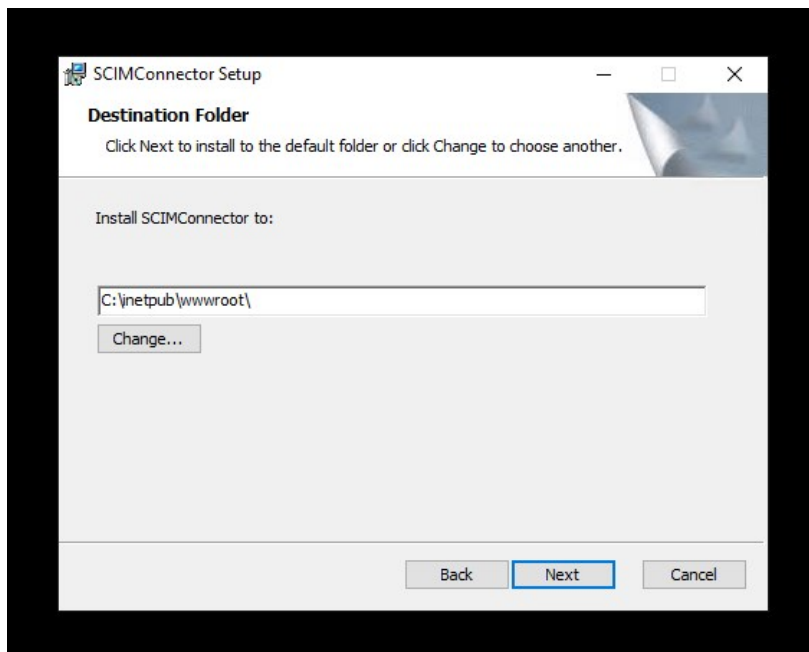
2. Provide the Application Name (this will also be the website name) and click **Next**.



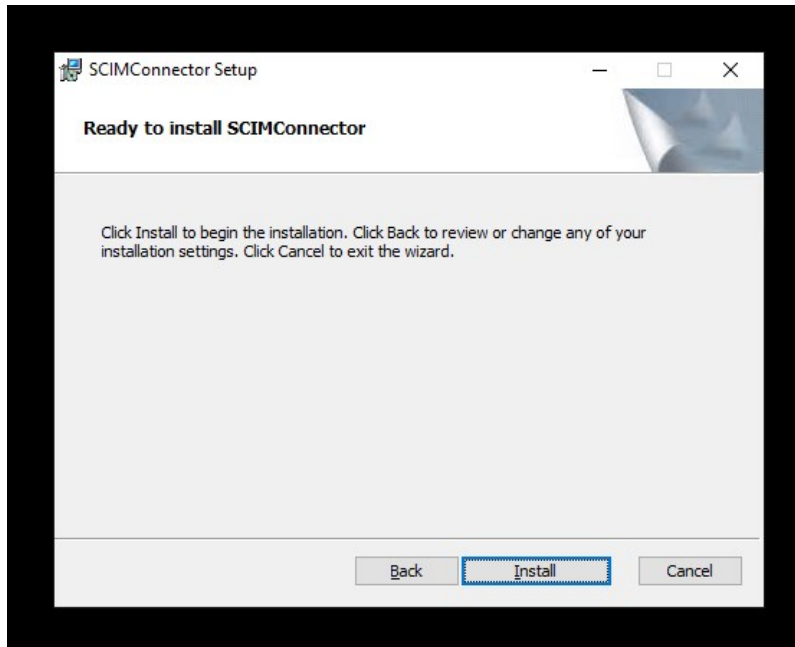
3. Review the license agreement. Once satisfied, check the **I accept the terms and the License Agreement** checkbox and click **Next**.



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**.



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



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

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

Secret Server Integrations

Sign In

Base url

Username

Password

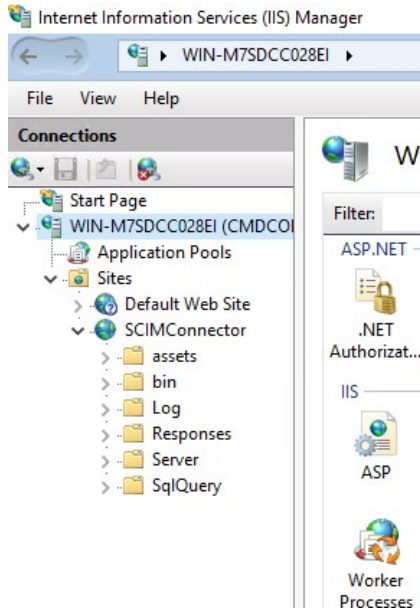
Sign In

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

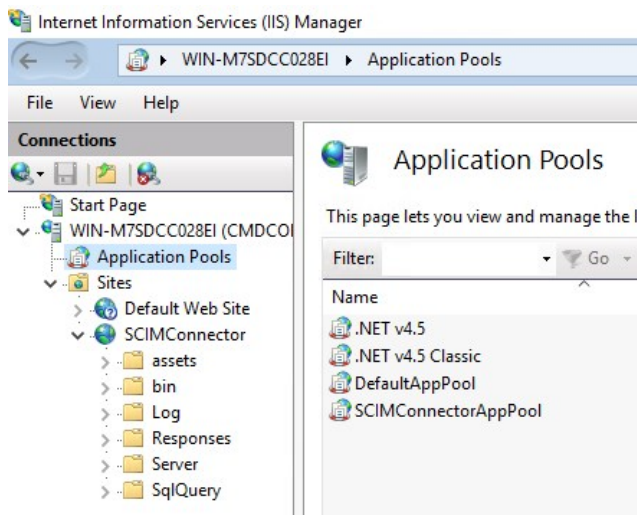
\\inetpub\wwwroot\SCIMConnector

Name	Date modified	Type	Size
assets	10/28/2020 12:08 ...	File folder	
bin	10/28/2020 12:08 ...	File folder	
Log	10/28/2020 12:10 ...	File folder	
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
es2015-polyfills.5e60b7ad6e87c6cc59ea	10/28/2020 11:38 ...	JavaScript File	57 KB
favicon	10/28/2020 11:38 ...	Icon	2 KB
fontawesome-webfont.674f50d287a8c48...	10/28/2020 11:38 ...	EOT File	162 KB
fontawesome-webfont.912ec66d7572ff82...	10/28/2020 11:38 ...	SVG Document	434 KB
fontawesome-webfont.af7ae505a9eed50...	10/28/2020 11:38 ...	WOFF2 File	76 KB
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
main.12cfed4135e337f310d2	10/28/2020 11:38 ...	JavaScript File	572 KB
MaterialIcons-Regular.29b882f018fa6fe75...	10/28/2020 11:38 ...	WOFF File	78 KB
MaterialIcons-Regular.96c476804d7a788c...	10/28/2020 11:38 ...	EOT File	68 KB
MaterialIcons-Regular.0509ab09c1b0d22...	10/28/2020 11:38 ...	WOFF2 File	60 KB
MaterialIcons-Regular.d120c85b6eb0549...	10/28/2020 11:38 ...	TrueType font file	171 KB
outline.da1dce55e6be63488a16	10/28/2020 11:38 ...	PNG File	1 KB
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
Roboto-Regular.99b14f0da0591e0d7167	10/28/2020 11:38 ...	TrueType font file	167 KB
Roboto-Regular.766c8926f6d9061fef24	10/28/2020 11:38 ...	SVG Document	717 KB
Roboto-Regular.b2a6341ae7440130ec4b....	10/28/2020 11:38 ...	WOFF2 File	63 KB
runtime.aa5b8c69ed805056b567	10/28/2020 11:38 ...	JavaScript File	2 KB
Settings.enc	10/28/2020 12:11 ...	ENC File	1 KB
styles.d11ecac23bb2dbec0803	10/28/2020 11:38 ...	Cascading Style S...	175 KB
web.config	10/28/2020 12:10 ...	CONFIG File	9 KB

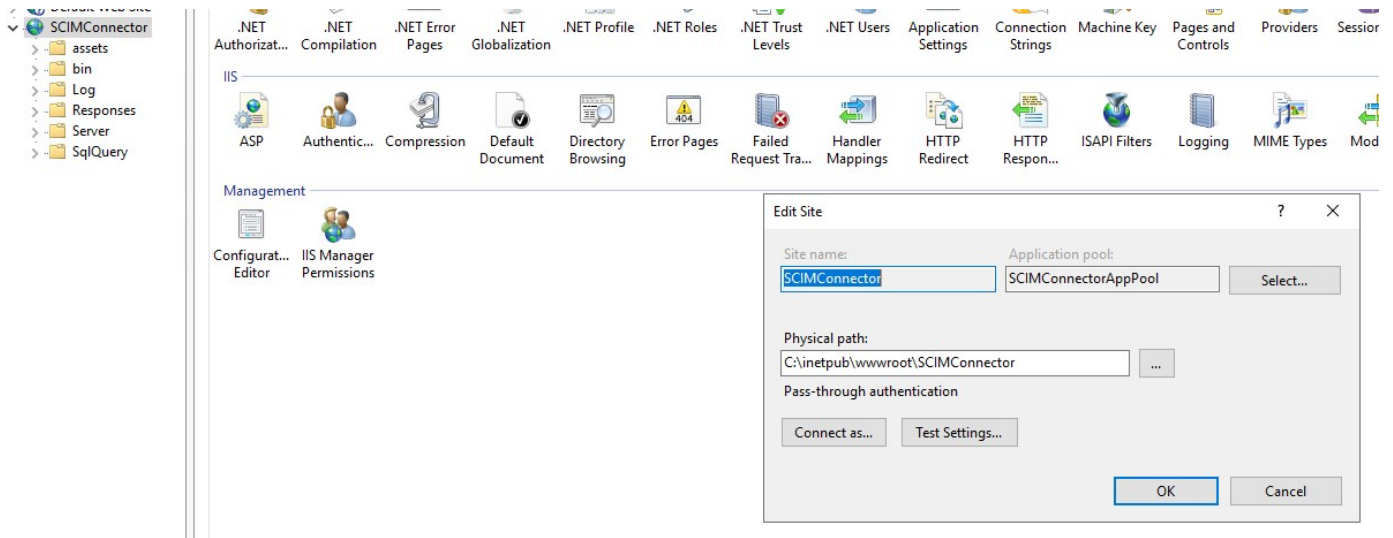
8. A new website has been created which can be seen in the IIS Manager.



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

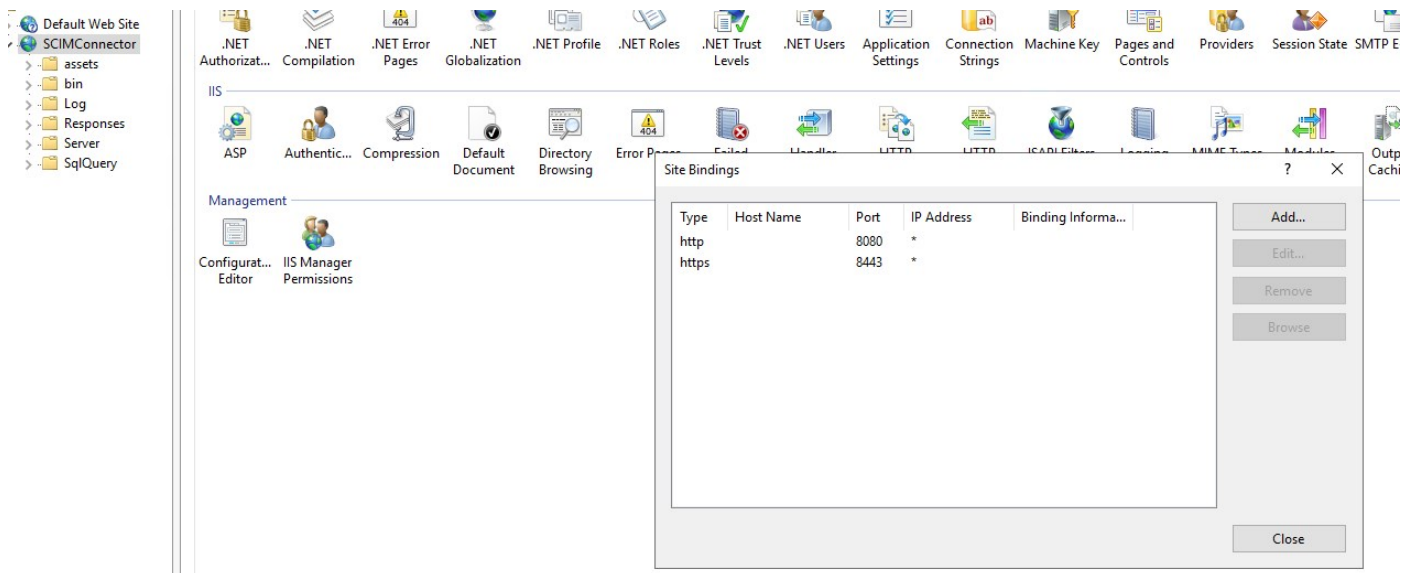


Reviewing the Basic Settings of the SCIMConnector website, the site is associated with the application pool that was created.



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

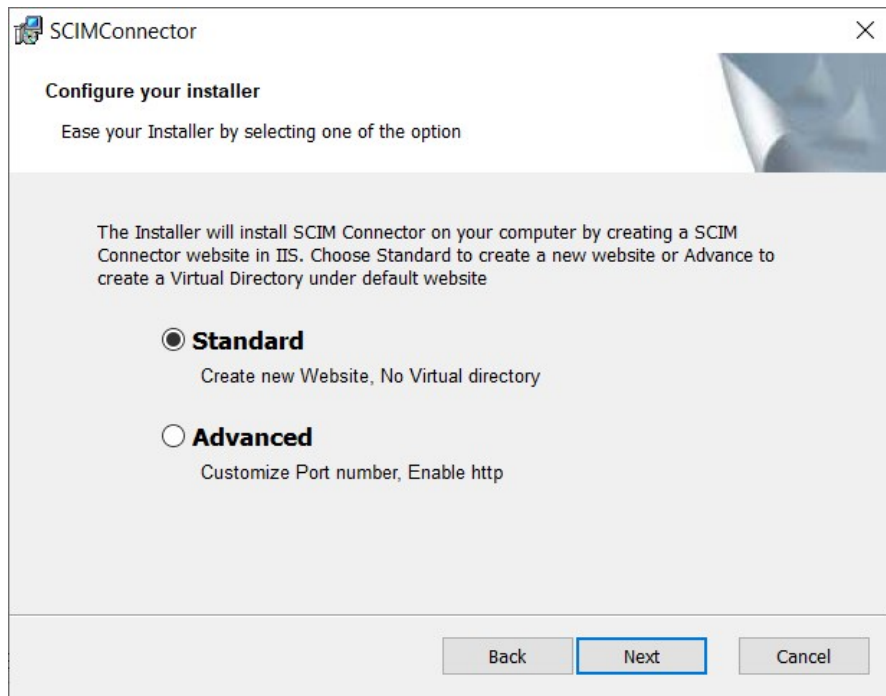
Note: The ports may differ from the standard http / https ports. This is due to another website in IIS has already consumed the standard ports for http and https (80/443).



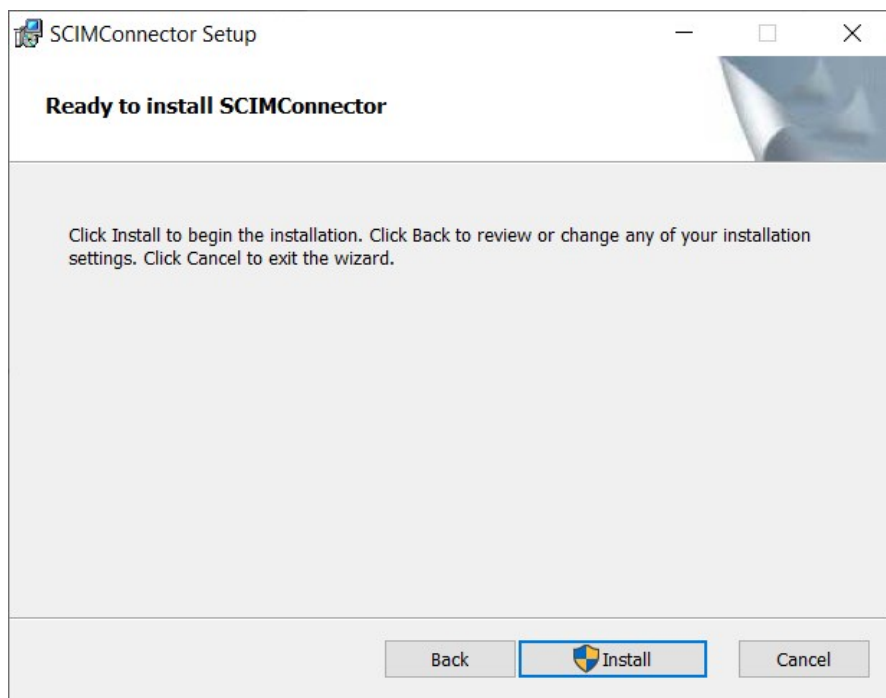
The installation will search for a certificate with the hostname and use this for configuring https. This can be changed after the installation to any certificate that is desired and available. If no certificate is found, the installation will create a self-signed one.

Upgrade from Version 2.5 to 3.0

1. Select the installer option (Standard):

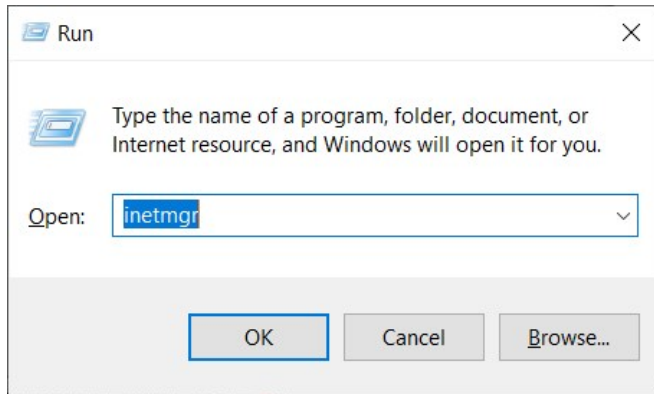


2. Click **Install**.

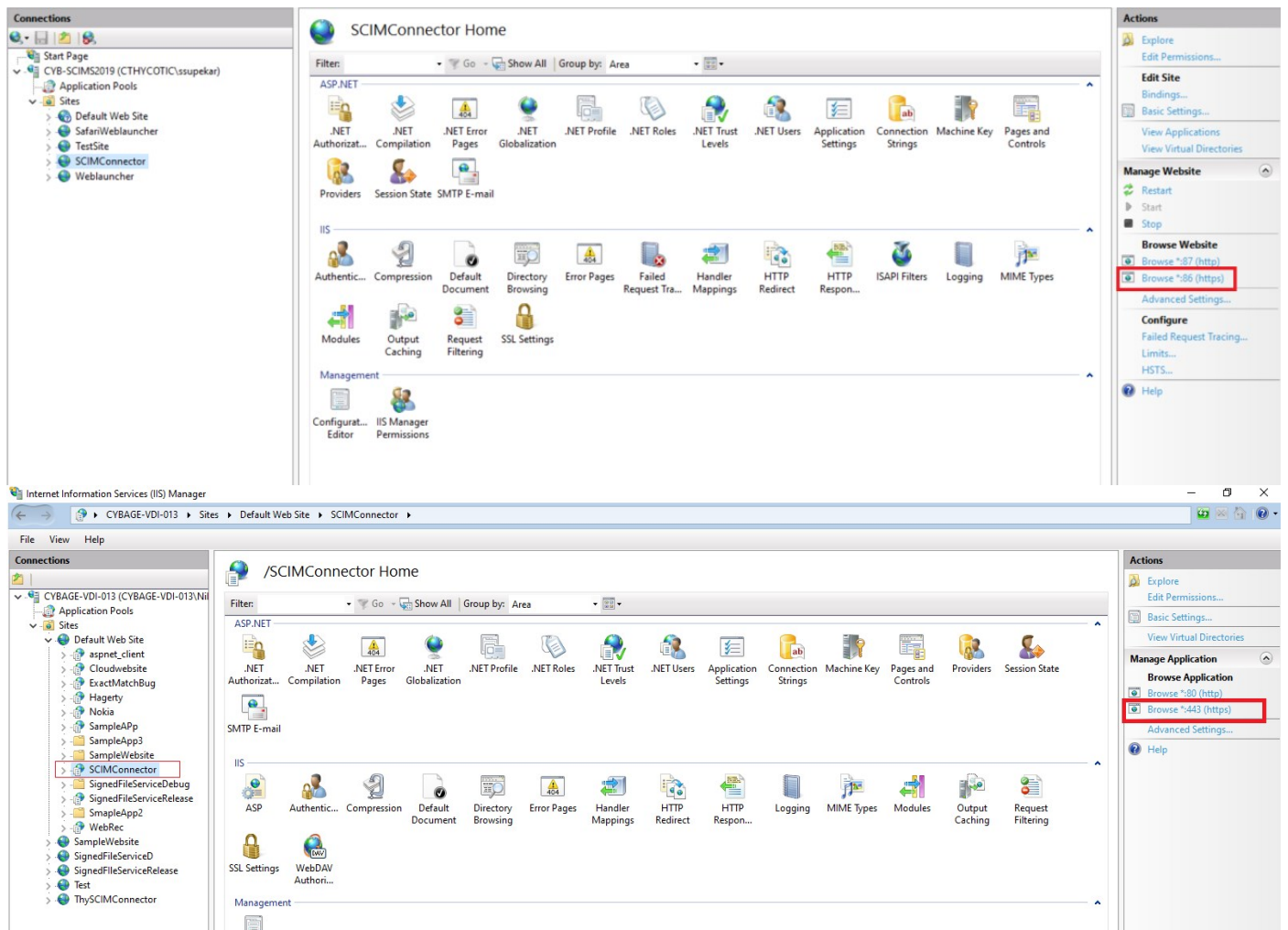


Launch SCIM Connector after Installation/Upgrade

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



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



Download the Installer

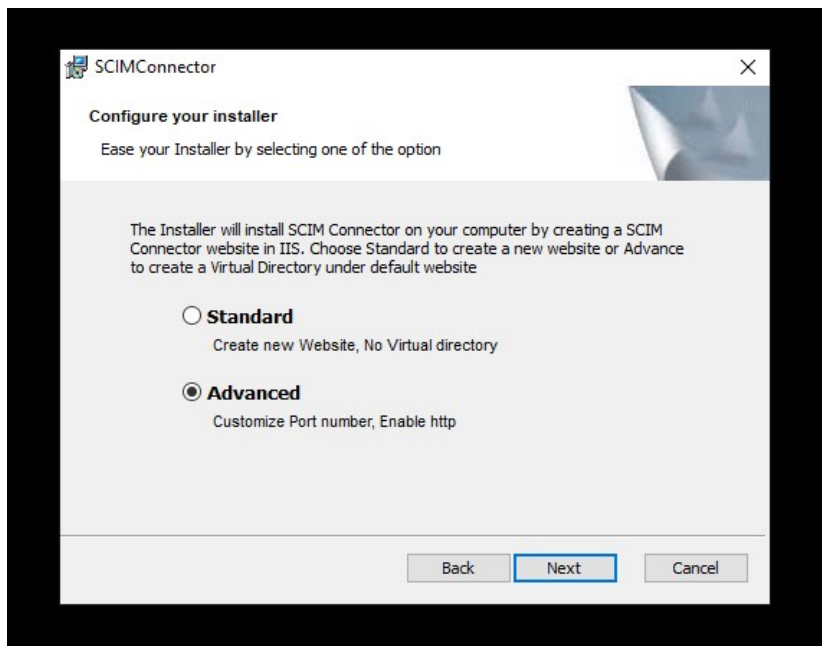
Download the installer file at:

- [SCIM software download](#)

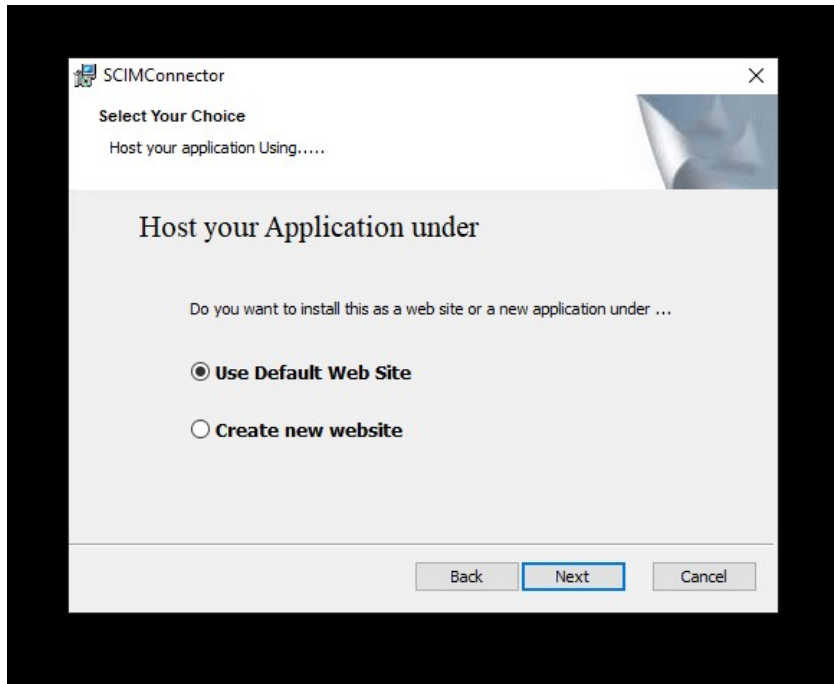
The advanced Installation Process will use the Default Web Site.

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.

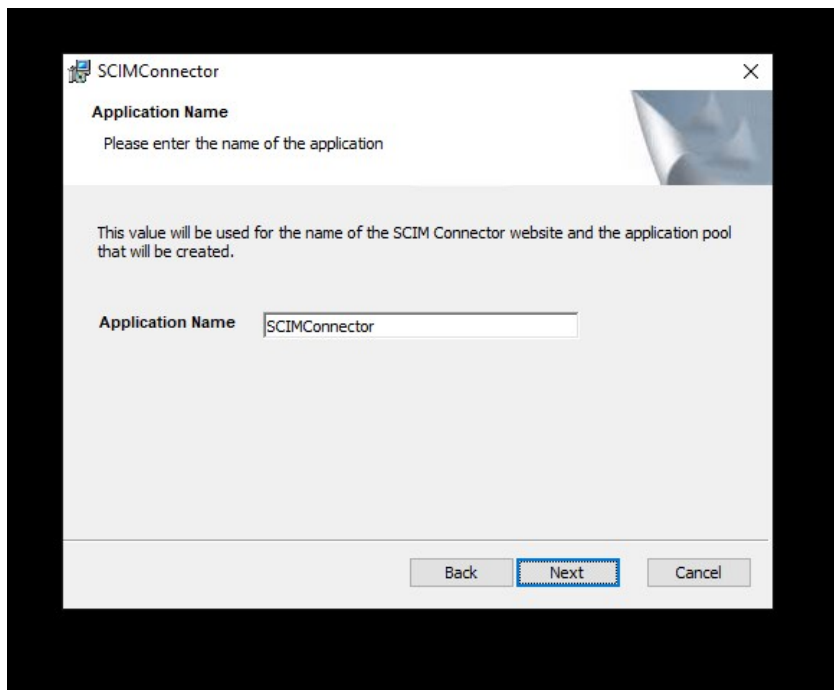
1. To install the SCIM Connector as a virtual directory under the Default Web Site select the Advanced option and then click **Next**.



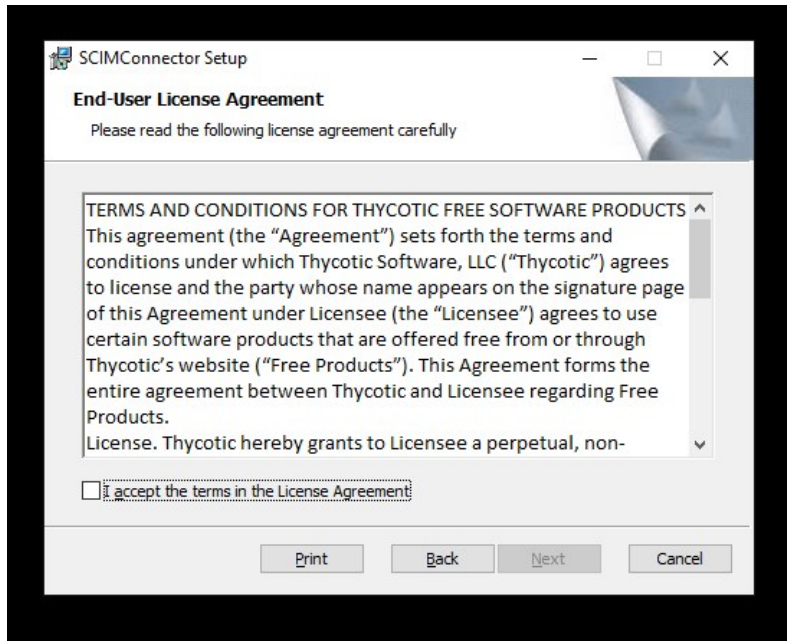
2. Select **Use Default Web Stie** and click **Next**.



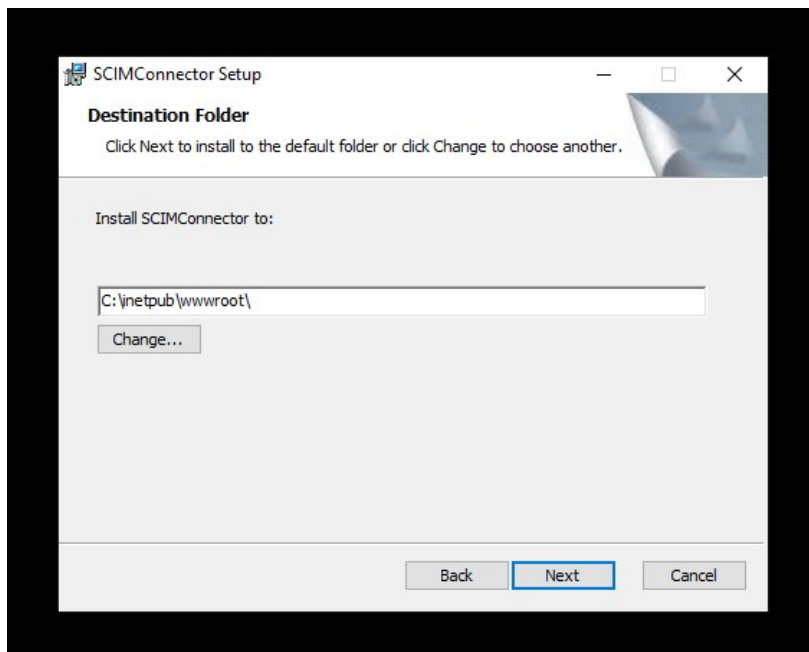
3. Fill in the name for the application. This will be used for the virtual folder name as well as the Application Pool name. Select **Next**.



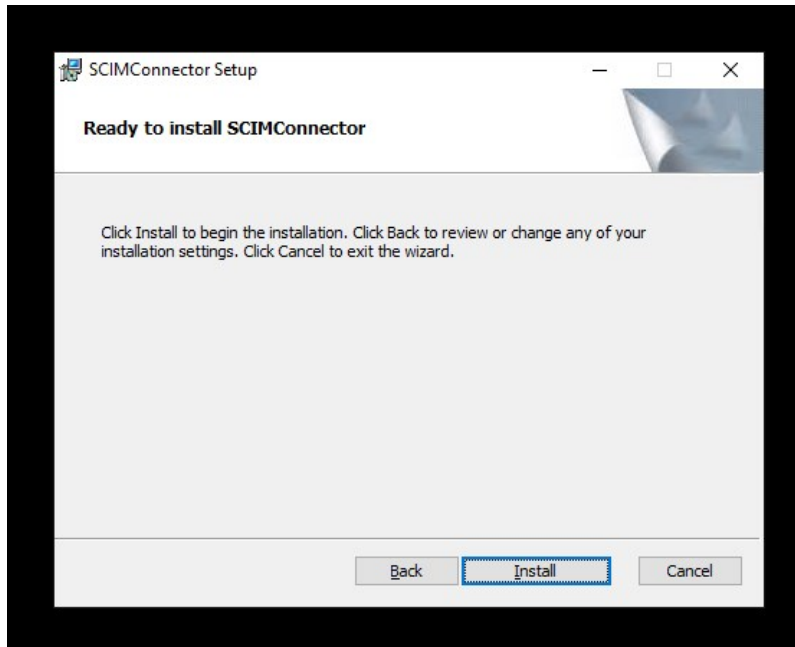
4. Review the license agreement. Once satisfied, check the **I accept the terms and the License Agreement** checkbox and click **Next**.



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.

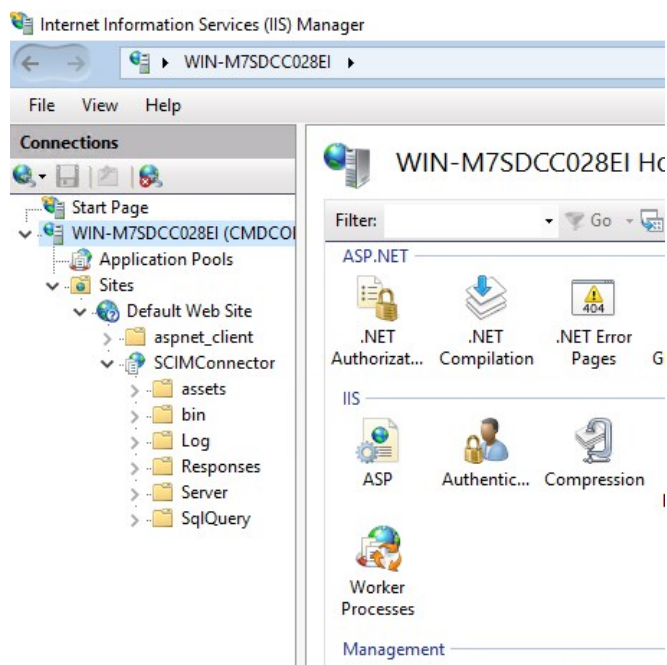


7. At this point the SCIM Connector installation is ready to create the website.



8. After the installation has completed the default browser 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.

SCIM Server for Secret Server

Not secure | localhost/SCIMConnector/#/?returnUrl=%2Fsettings

Secret Server Integrations

Sign In

Base url

Username

admin

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.....

Host your Application under

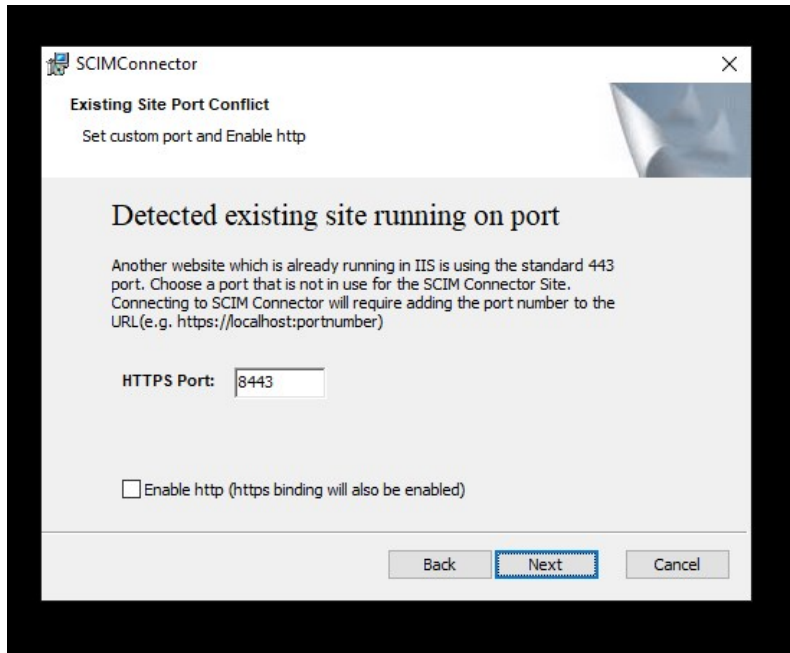
Do you want to install this as a web site or a new application under ...

Use Default Web Site

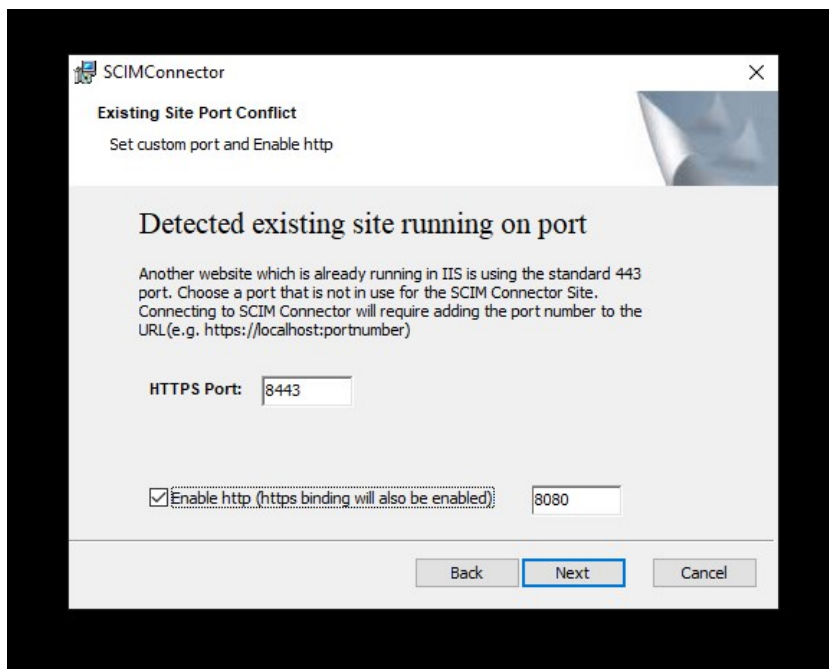
Create new website

Back Next Cancel

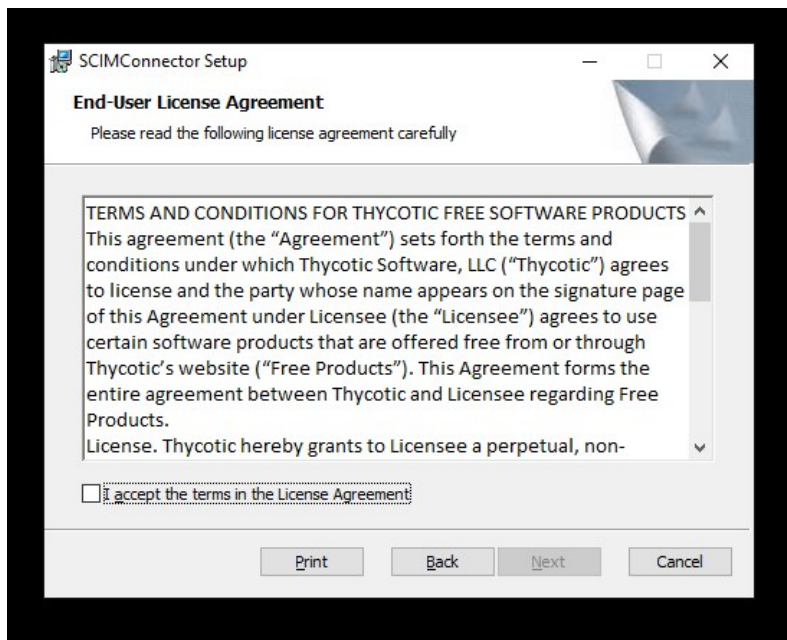
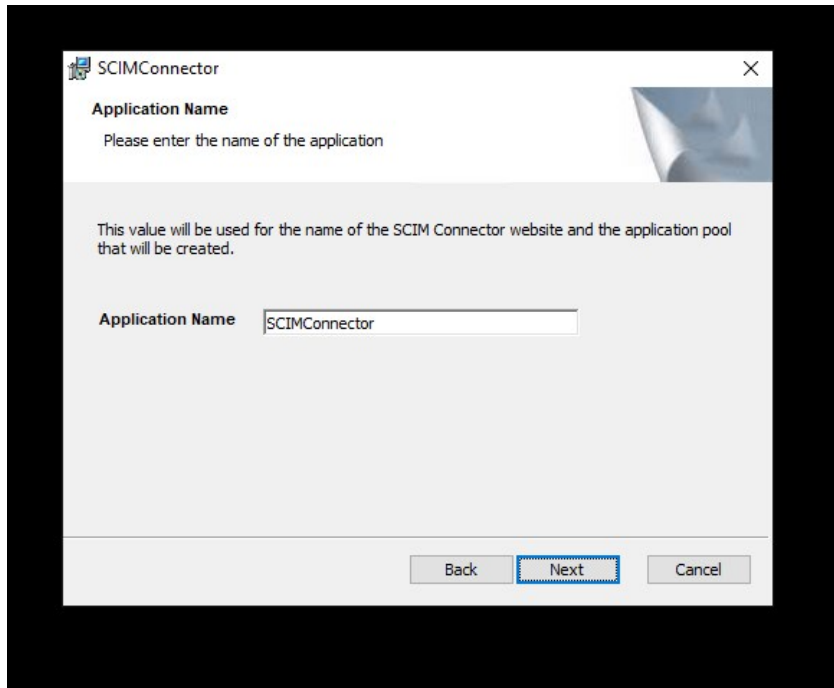
Note: It is likely that there is already a default web site in IIS. If there is a port conflict the following dialog will appear allow the selection of a custom https port. Enter the https port that is desired in the provided field.

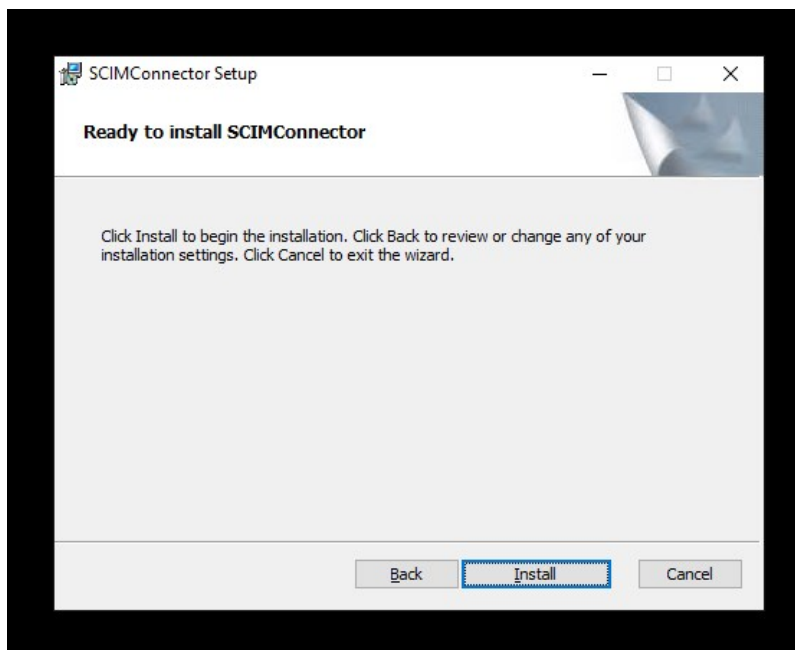
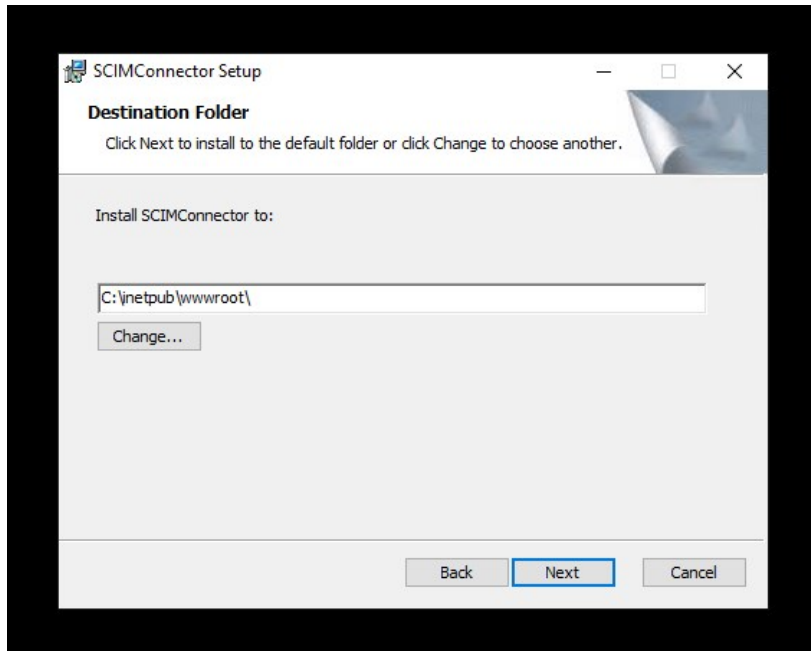


12. By default, HTTPS communication is recommended however in cases where SCIM endpoints may not work with HTTPS, enable http by selecting the **Enable Http** checkbox. Supply the custom available port for http and click **Next**.



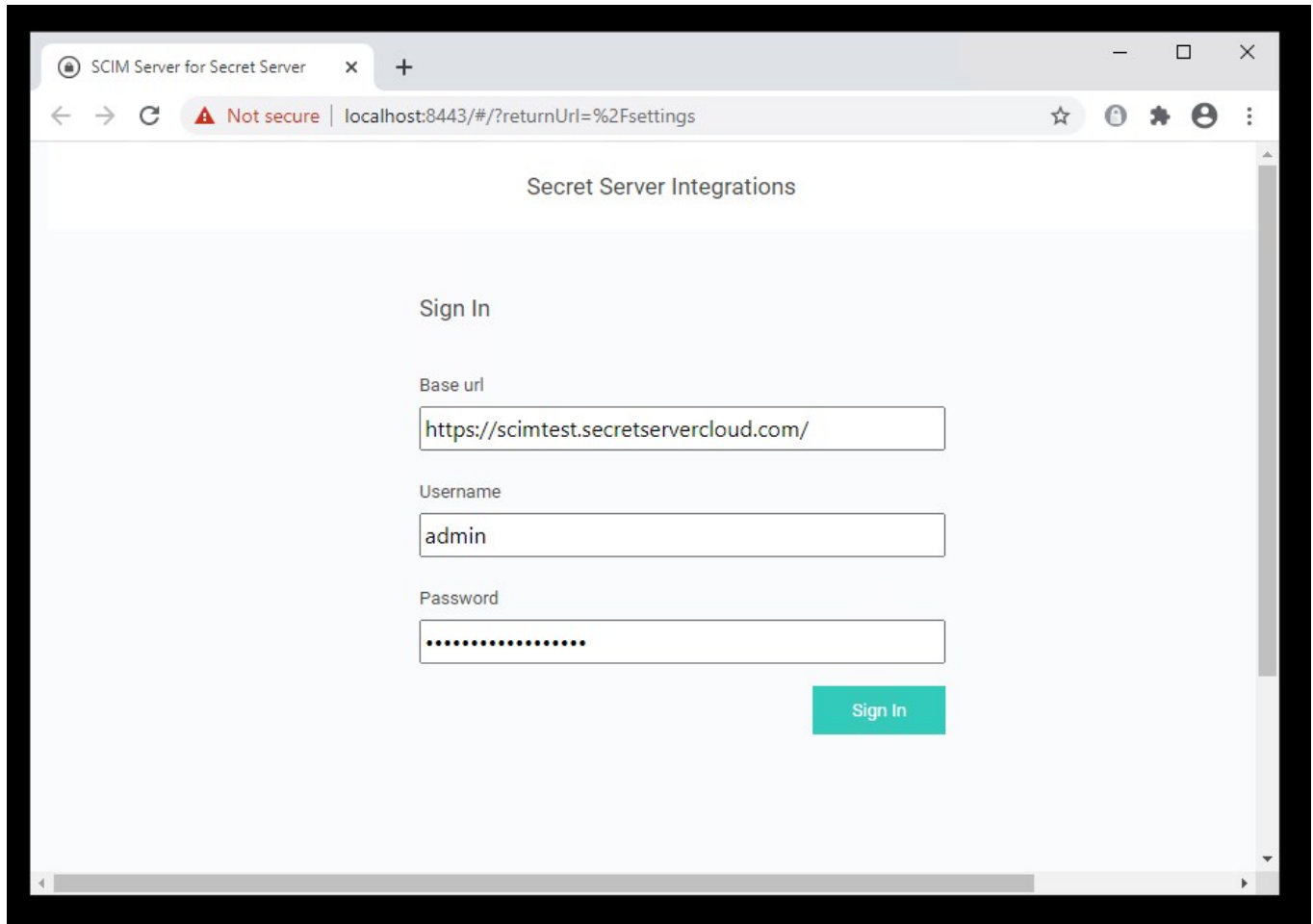
13. The remainder of this Advanced option is identical to the Standard installation process.





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**.



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 ☆

General Security Audit RPC Dependencies Sharing Settings

SHARE SECRET

Edit

Inherit Permissions from folder No

SHARED WITH	
Everyone	View
scim	Owner

Remove This, Add Explicit Users For Access

- 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

The screenshot shows the configuration interface for the Thycotic PAM application. The top navigation bar includes tabs for Details, Configuration (selected), Correlation, Accounts, Risk, Activity Data Sources, Unstructured Targets, Rules, and Password Policy. Below this, there are sub-tabs for Settings, Schema, and Provisioning Policies (selected). A text box explains that this is a list of provisioning policies for the application, with instructions on how to add or edit policies. Below the text is a table with the following data:

Object Type: account		
Type	Name	Description
Create	Create Account Form	Provisioning form for create account.
Update		
Delete		
Enable Account		
Disable Account		
Unlock Account		
Change Password		

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

Create Account Form		Provisioning form for create account.		
Add Section		Preview Form		
+		+		
+	User Name			
+	Formatted Name			
+	Family Name			
+	Given Name			
+	Display Name			
+	Email			
+	Password			

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

Type
String

Type Settings

Multi-Valued Refresh on Change Authoritative
 Required Review Required Display Only

Type Settings ^

<input type="checkbox"/> Multi-Valued	<input type="checkbox"/> Refresh on Change	<input type="checkbox"/> Authoritative
<input checked="" type="checkbox"/> Required	<input checked="" type="checkbox"/> Review Required	<input type="checkbox"/> Display Only

Read Only

False ▼

Hidden

False ▼

Owner

None ▼

Value Settings ^

Dynamic

Value

Rule ▼

Thycotic PW Rule ▼ ...

Allowed Values

None ▼

Validation

None ▼

[Apply](#)

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 *	Tester	Last Name *	McTester
User Type *	Employee	Location	
Mobile Phone #		Calculated User Name *	Tester McTester

This will be used for SMS Password Reset

Calculated Email
Tester.McTester@salpointdemo.com

Organizational Information

Manager *
David Anderson


Department *
Human Resources

Job Title *
Accounts Payable Analyst

Cancel Submit

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

Manage Accounts


Tester McTester

Username: Tester.McTester

Manager: David Anderson

[Manage](#)

Click the **Request Account** button

< Identity Details

Accounts 0 [Request 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

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

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 *

[REDACTED]

Cancel

Ok

Click OK at the bottom. The account change submission should happen and can be tracked under **My Work > Access Requests**.

Manage Accounts: Tester McTester
Requested by The Administrator on 11/24/20 | Request ID: 33

Request pending

Create: TMcTester on Thycotic PAM Provisioning

You can check Secret Server to verify that the account has been created under **Admin > Users**.

<input type="checkbox"/> TMcTester	Tester McTester	Tester.McTester@gmail.com	Yes	Local	< None >	Never
------------------------------------	-----------------	---------------------------	-----	-------	----------	-------

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

Manage Accounts: Tester McTester
 Requested by The Administrator on 11/24/20 | Request ID: 33

Request pending

Create: TMcTester on Thycotic 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.

Search: tester Filters

Identities Selected: Tester McTester Showing 1-1 of 1 Add

Tester McTester

Username: Tester McTester
 Manager: David Anderson

Identities Selected: Tester McTester Showing 1-1 of 1

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.

Add Access Remove Access

Search By Keywords Search Access Filters

Identities Selected: Tester McTester Showing 1-12 of 69

AccountingGeneral Details

Grants basic accounting access to the internal Accounting System
 Type: Entitlement Owner: Lori Ferguson Application: Active Directory 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.

Add Access Remove Access

Search By Keywords Search Access Filters

Identities Selected: Tester McTester

AccountingGeneral Details

Grants basic accounting access to the internal Accounting System
 Type: Entitlement Owner: Lori Ferguson Application: Active Directory 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 confirm.

Add Access Remove Access

Search By Keywords Search Access Filters

Identities Selected: Tester McTester Showing 1-6 of 6

Everyone Details

Type: Entitlement Application: Thycotic PAM Attribute: groups

Management Details

Type: Entitlement Application: Thycotic PAM Attribute: groups

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.

Identities Selected: Tester McTester

Add Access

Management

Type: Entitlement Application: Thyotic 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

Application	Attribute	Display Name	Type	Description	Owner	Requestable	Classifications
Oracle EBS	RESPONSIBILITIES	19ync Super User	RESPONSIBILITY	Administrative rights to 19ync			

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 Properties | Object Properties | Classifications

*Indicates a required field.

Application * ▼

Type * ▼

Attribute * groups

Value * The value for this group will correspond to the id attribute from the group schema.

Display Value

Requestable

Description

B *I* U |

English (United States) ▼

7 of 1024 characters (including markup)

Owner ▼

Scope ▼

New Group

Standard Properties | **Object Properties** | Classifications

Object Attributes

Display Name*

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	↑ 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

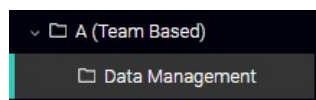
As previous examples have shown, you can create a provisioning policy form similarly to the Create Identity form we did earlier.

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 Management

Total Identities	2
Groups	1
Privileged Items	0

Manage

Click the **Add Identities** button

< Data Management

Identities 2 Groups 1 Privileged Items 0

Direct Access 0 Effective Access 2 + Add Identities

Bulk Remove Columns

No Results

Choose Identities

1 Choose Identities 2 Add Container Permissions

Search Identities

Tester McTester

Cancel Next

Align the View permission

1 Add Container Permissions ✕

1 Choose Identities 2 Add Container Permissions

<input checked="" type="checkbox"/> View
<input type="checkbox"/> Owner
<input type="checkbox"/> 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:

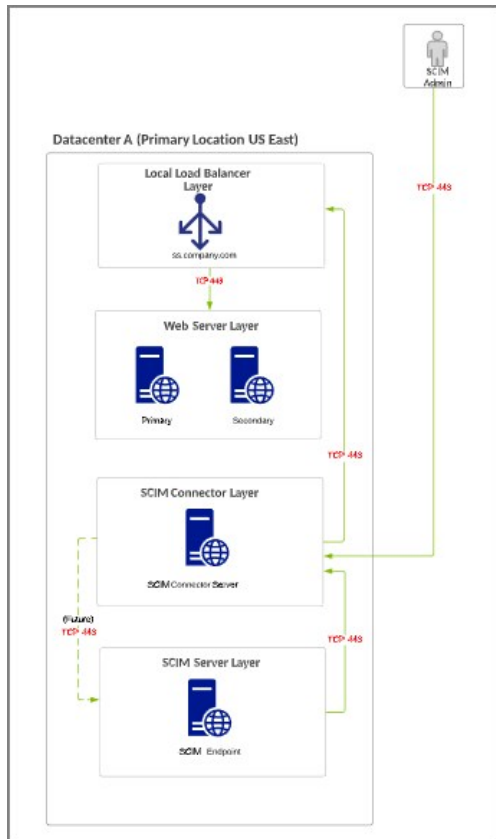
- SS-SCIM-REF#01 - A-1 - SS On Prem + SCIM
- SS-SCIM-REF#01 - A-2 - SS On Prem + SCIM (Perimeter Network)
- SS-SCIM-REF#01 - B-1 - SSC + SCIM
- SS-SCIM-REF#01 - C-1 - Request Communication Flow

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

- Customer is using 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, PingIdentity, 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

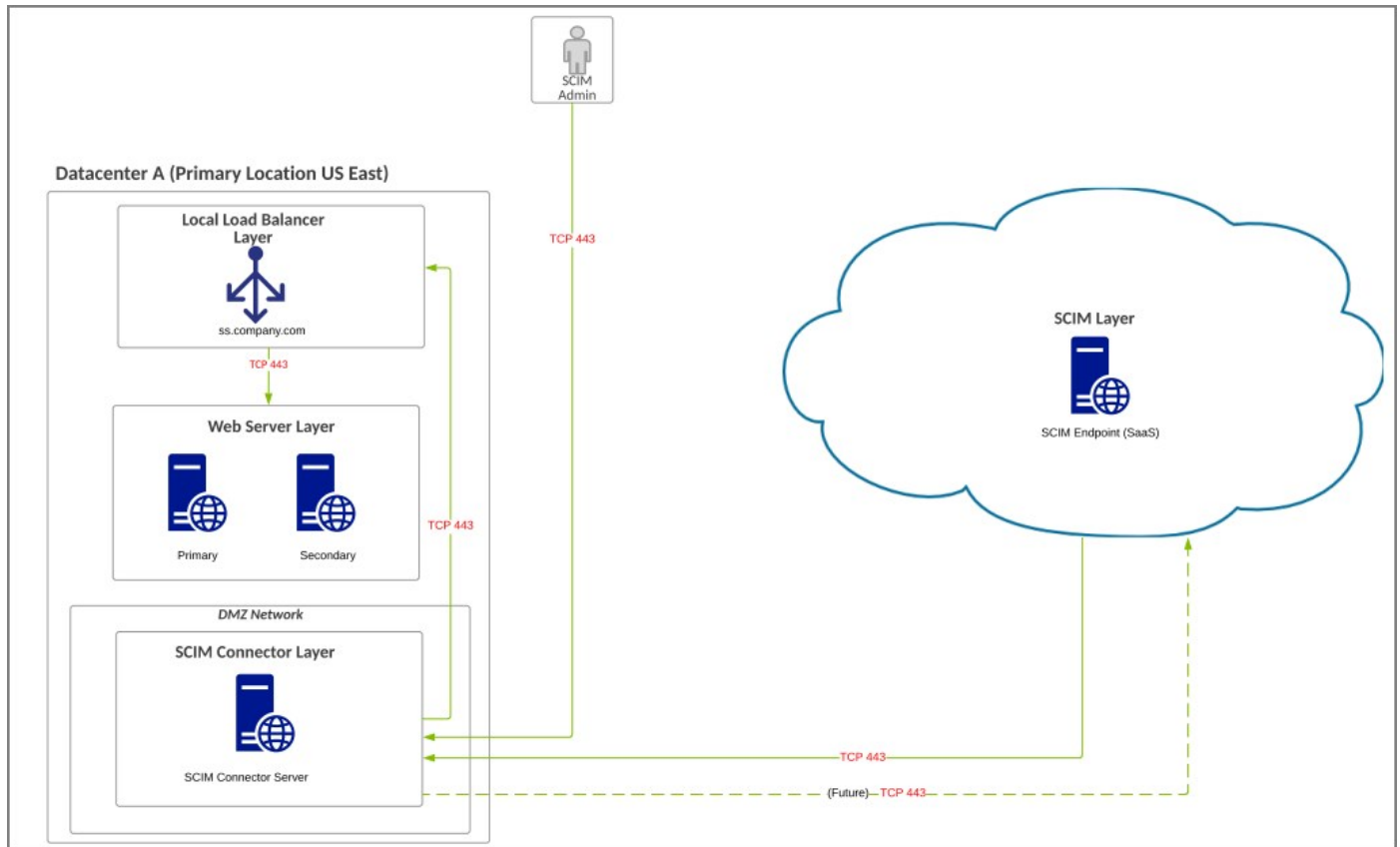


Definitions for SS-SCIM-REF #01 - A-2

- Customer is using 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 accommodate 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



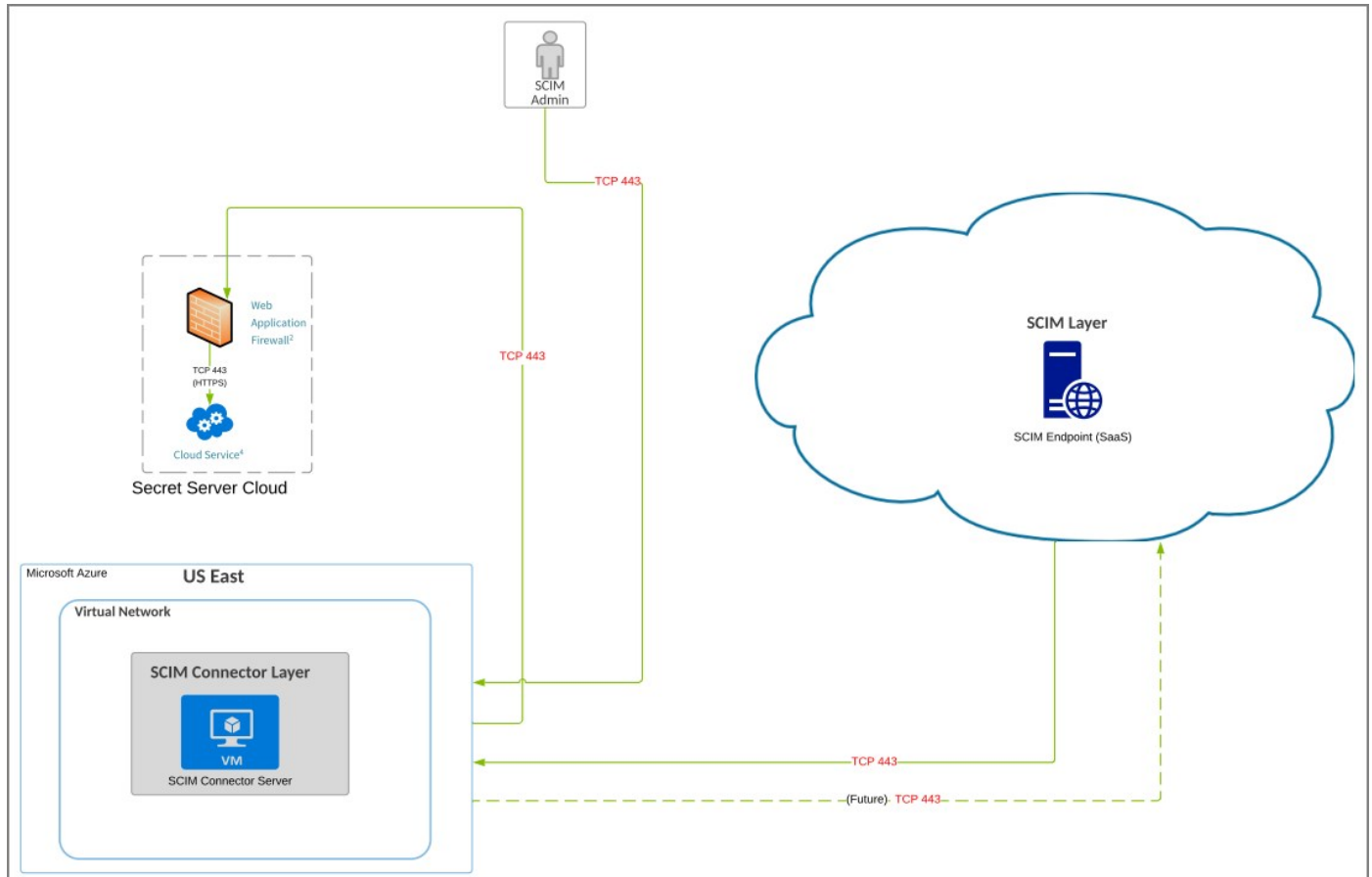
Definitions for SS-SCIM-REF #01 - B-1

- Customer is using SSC hosted in Azure with a dedicated system for the SCIM Connector installed in the customer's 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.

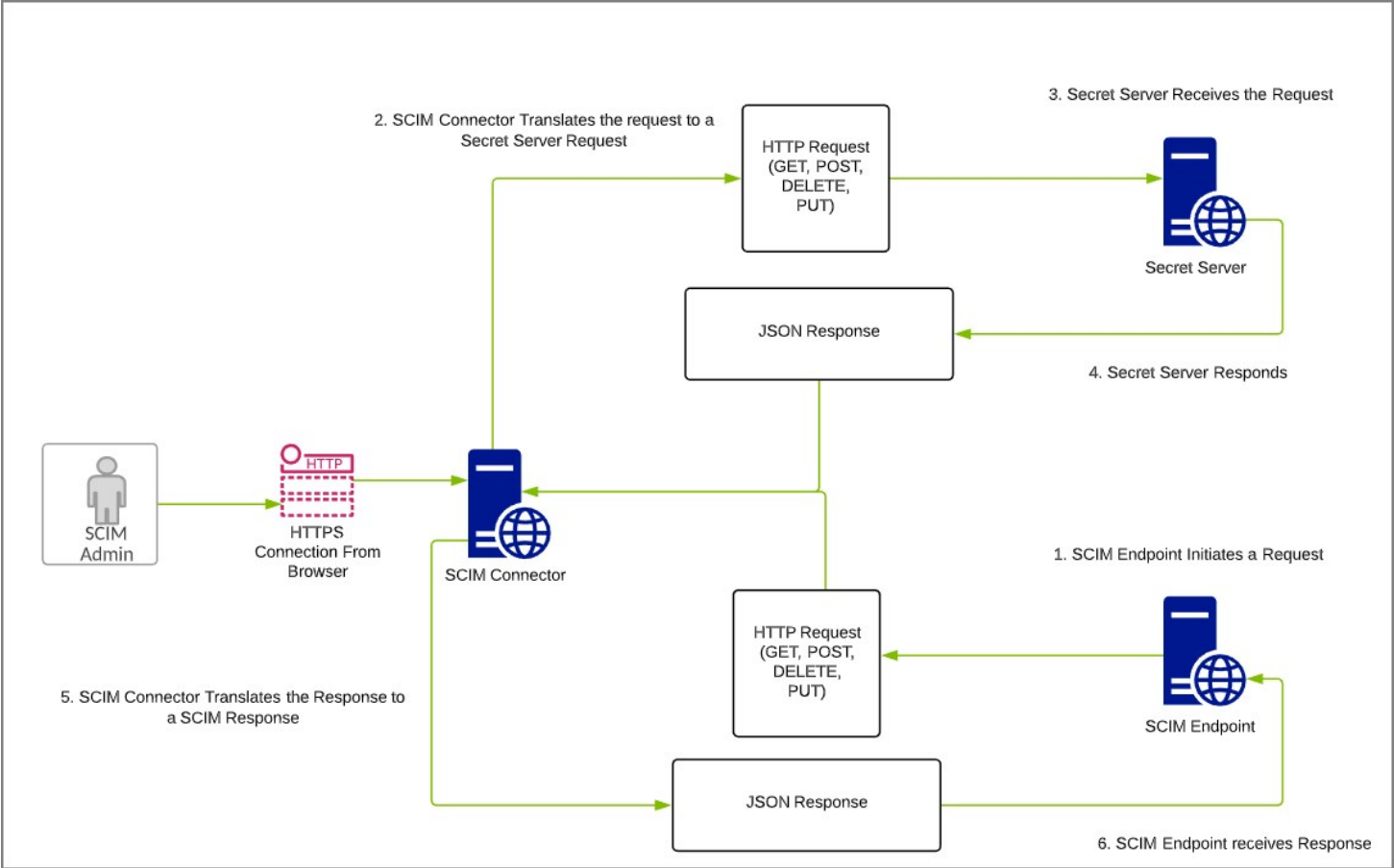
Requirements for SS-SCIM-REF #01 - B-1

- 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 accommodate 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](#)
- [SailPoint IdentityIQ](#)
- [OneLogin](#)

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	Reference
AuthX	The Control Group	Reference
Federated Directory	Fed Blokes	Reference
GitHub	GitHub, Inc.	Reference
Gluu	Gluu.org	Reference
Idaptive	Cyberark, Inc.	Reference
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	Reference

RadiantOne Federated Identity Service	Radiant Logic	Reference
SCIM	Elimity	Reference
SOFFID IAM	soffid	Reference
Trello	Trello	Reference

This section includes the most recent SCIM Connector Release Notes.

- [3.0 Release Notes](#)

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, PrivilegedData, Container Permission, Privileged 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, 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.FolderId, FolderName, GroupId, GroupName, UserId, 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
SecretAccessRoleName
        ,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 [known issue and workaround](#) 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 [Release Notes](#)