AU 2025
THE DESIGN & MAKE CONFERENCE

1343

Unlocking the Potential of the Autodesk Vault Data API

Christian Gessner
COOLORANGE S.r.l.

Learning Objectives

- Learn about the fundamentals of the Vault Data API
- Learn about the differences between the traditional Vault SDK and the Vault Data API
- See a real-world example of how to surface Vault data directly within Microsoft Teams using custom integrations
- Discover how a ChatBot can leverage the Vault Data API to enable interactive, conversational queries and information retrieval

Description

Autodesk's Vault Data API offers a modern, RESTful approach to interacting with Vault data, streamlining integration and automation processes. In this session, we'll explore the core functionalities of the Vault Data API, highlighting its advantages over the traditional Vault SDK. Attendees will see a real-world example of what is possible with the Vault Data API, including how Vault data can be surfaced directly in Microsoft Teams through custom integrations. The session will also demonstrate a ChatBot that allows users to interactively query Vault information, showcasing new and innovative ways to make Vault data more accessible and collaborative. This class aims to equip software developers with the knowledge to enhance their applications by integrating Vault data seamlessly.

Speaker(s)

Christian Gessner is a co-founder and Head of Research & Innovation at COOLORANGE. In this role, he drives research into cutting-edge technologies that enable customers to effectively automate, implement, and customize Autodesk CAD, PDM, and PLM solutions, ensuring seamless integration with enterprise systems. With over 25 years of experience in full-stack software development, Christian specializes in Autodesk product data and lifecycle management and Microsoft development technologies. Before founding COOLORANGE, he was a member of the data management software engineering team at Autodesk.

Table of Contents

Introduction

Introduction

This handout complements the AU2025 presentation on the Autodesk Vault Data API. It provides additional resources, practical guidance, and tips to help you get started with the API. It will go deeper into topics covered in the sides. It will also cover additional topics that were not able to be presented due to time constraints.

History of the Vault Data API

The **Vault Data API** was first introduced alongside the release of the redesigned Vault Thin Client in Vault 2022. The modernized Thin Client required a new mechanism to retrieve data from the Vault Server, leading to the creation of the Data API. Initially, this API was exclusively used by the Thin Client. However, in 2024 Autodesk extended its availability to developers, marking a significant milestone in Vault's evolution:

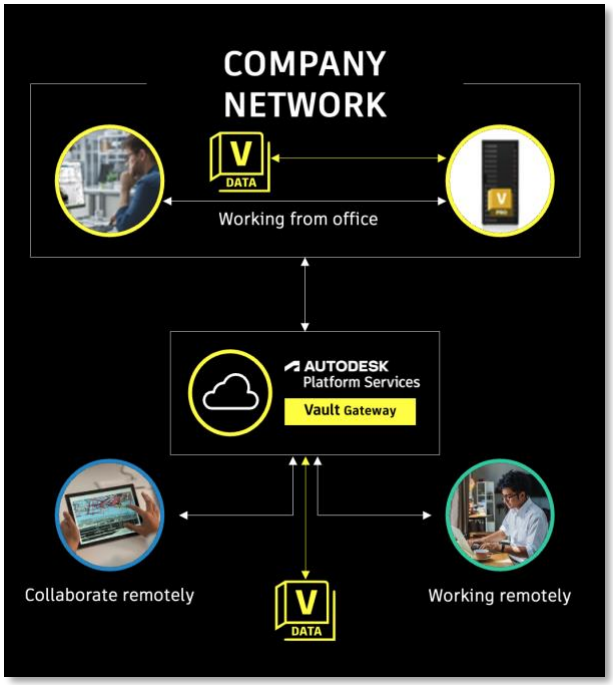
Key Milestones:

- **July 2024**
  Autodesk announced the launch of the Vault Data API Beta Program.
- **October 2024**
  The Vault 2025.2 Beta was released, featuring the API for the first time.
- **November 2024**
  The Vault 2025.2 public release officially included the Vault Data API.
- **March 2025**
  The Vault 2026 public release continued to provide the Vault Data API as a core capability.

Connectivity

Vault Gateway

The **Vault Gateway** is a secure cloud-mediated technology that allows users to access an on-premises Autodesk Vault Server from anywhere without the need for VPN connections or open firewall ports.



VAULT GATEWAY DIAGRAM

Instead of connecting directly to the server, clients use a dedicated gateway URL provided by Autodesk, which safely relays requests between the remote user and the internal Vault environment. This approach significantly reduces infrastructure exposure while making administration easier, as configuration is handled directly in the Vault Server's ADMS console.

Authentication is supported through Autodesk IDs or Vault accounts, ensuring secure access, although Windows authentication is not available when connecting through the Gateway. First introduced with Vault 2022, the Gateway is supported in current and recent releases, and has become an important enabler for distributed teams, contractors, and remote workers who need reliable, secure, and straightforward access to Vault data.

The configuration of Vault Gateway gets explained in the official documentation: https://help.autodesk.com/view/VAULT/2026/ENU/?guid=GUID-725723AF-CCFD-48A2-8A20-C332B9A75608

RESTful Web Services

A RESTful web service is an API that follows the principles of REST (Representational State Transfer). It uses HTTP methods (like GET, POST, PUT, DELETE) to interact with resources, which are represented by URLs.

Wikipedia page on REST:
https://en.wikipedia.org/wiki/REST

Blog post from the Postman Team on REST:
https://blog.postman.com/rest-api-examples/

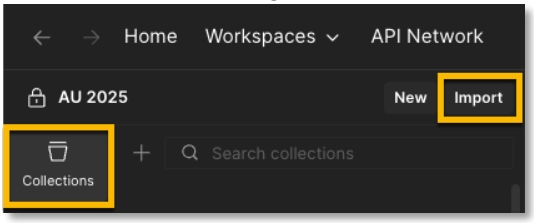
Best practice:
Always test endpoints in Postman before implementing in production code.

Postman

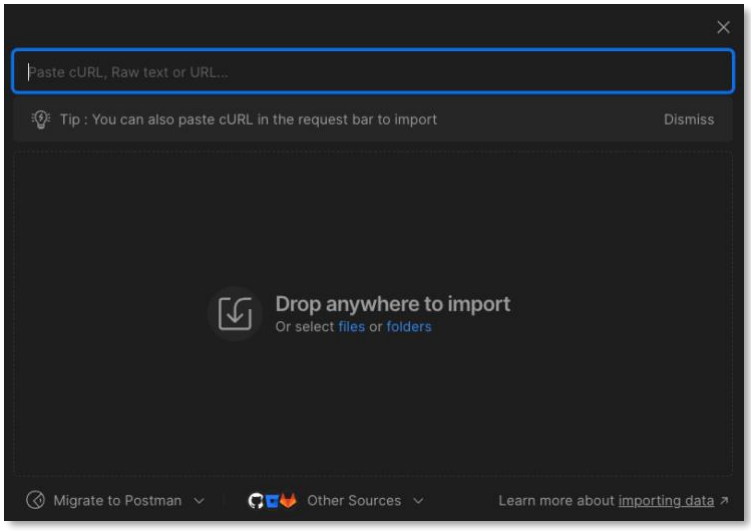
Step-by-step instructions to import the Vault Data API in Postman

The Vault Data API provides an OpenAPI (Swagger) specification endpoint can be imported directly into Postman. The following steps explain the import procedure:

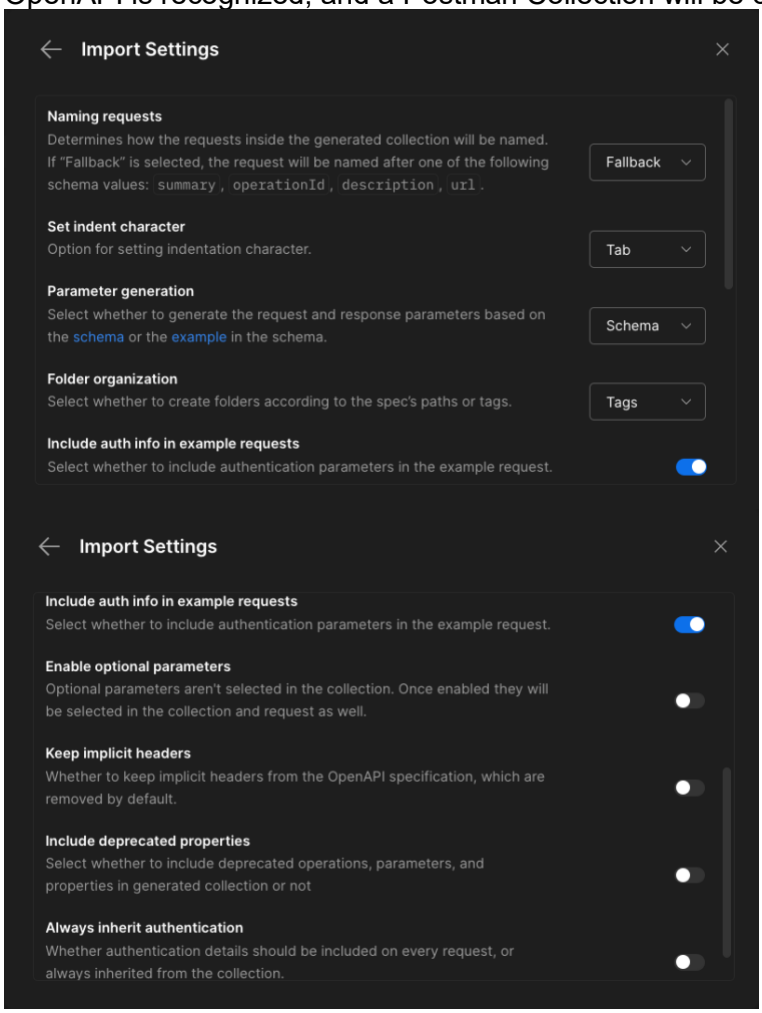
1. Open **Postman** and go to **Collections** → **Import**:



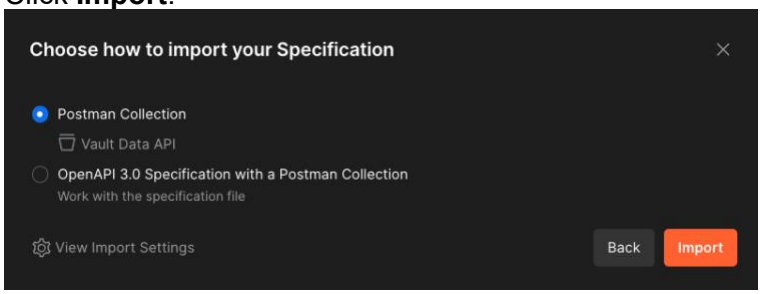
2. In the **Import** dialog, paste the OpenAPI URL:
   `https://{vault-server}/AutodeskDM/Services/api/vault/v2/openapi-spec.yml`



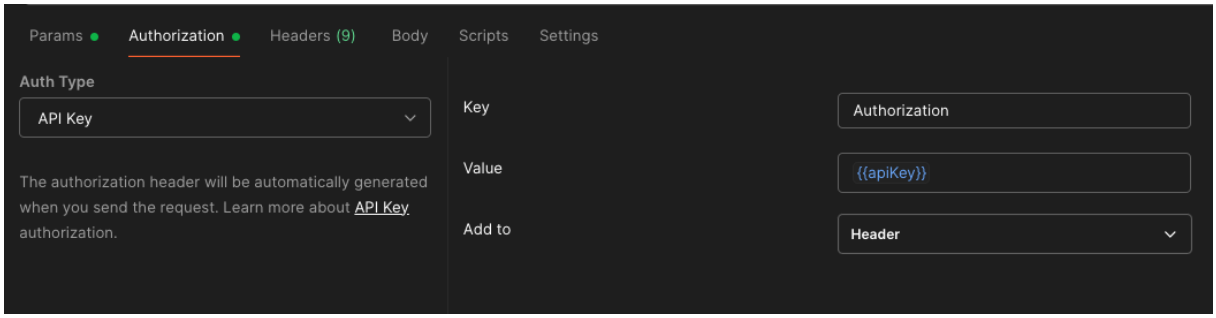
3. Select **Import Settings** and adjust all settings to match the screenshots below (ensure OpenAPI is recognized, and a Postman Collection will be created).



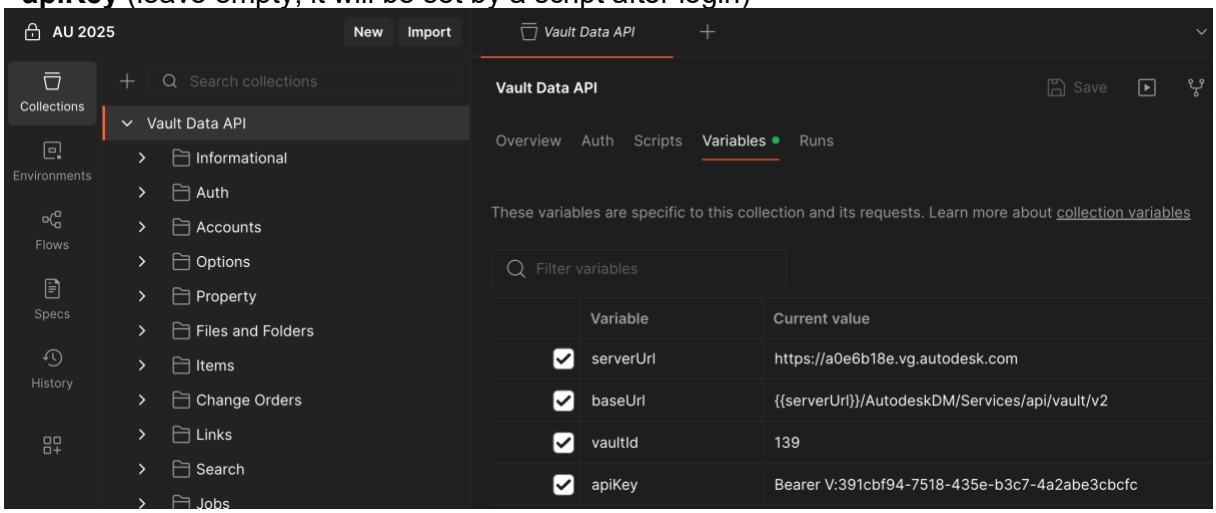
4. Click **Import**:



Postman generates a collection with endpoints grouped by category (e.g., Informational, Auth, Files and Folders, Items, Options, Jobs) and preconfigures all secured endpoints to use the Auth Type **API Key** for Authorization:



5. In the newly created collection (root node “Vault Data API”), open **Variables** and add:
   - **serverUrl** (empty for now)
   - **apiKey** (leave empty; it will be set by a script after login)



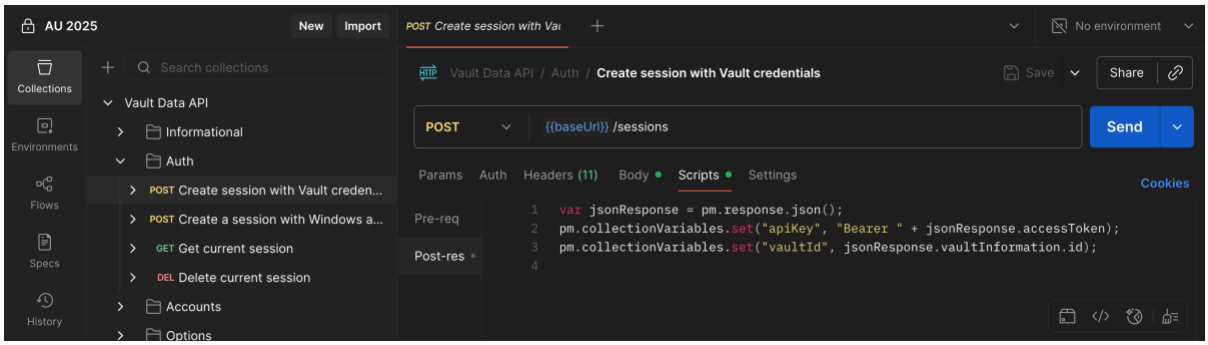
The **apiKey** is required for Authorization, the **serverUrl** used in the next step

6. Still under **Variables**, update **baseUrl** so it references your server variable:
   `{{serverUrl}}/AutodeskDM/Services/api/vault/v2/`

7. In the **Current Value** of **serverUrl**, enter your Vault Server or Vault Gateway base address (including protocol and port if required), e.g.:
   `https://a0e6b18e.vg.autodesk.com`

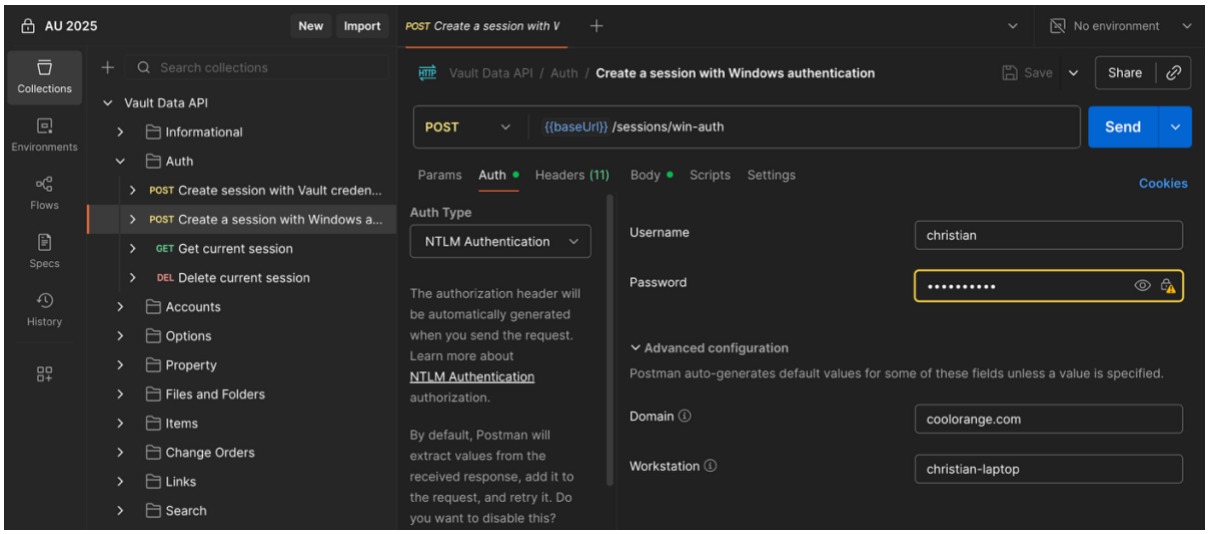
8. In the collection, navigate to **Auth → Create session with Vault credentials**. Open the **Script** tab and add this **Post-response** script:

```
var jsonResponse = pm.response.json();
pm.collectionVariables.set("apiKey", "Bearer " + jsonResponse.accessToken);
pm.collectionVariables.set("vaultId", jsonResponse.vaultInformation.id);
```



This automatically refreshes **apiKey** (as Authorization: Bearer …) and **vaultId** each time the session endpoint is used.

9. Optional: Navigate to **Auth → Create session with Windows authentication** and add the code from step 8 to the **Post-response** script. Then open the **Auth** tab, change the **Auth Type** to `NTLM Authentication` and enter your Windows Username, Password, Domain and Workstation:



After completing these steps, Postman can be used to test all Vault Data API endpoints. Use one of the two `sessions` endpoints first to obtain an access token.
The authentication calls persist the access token (apiKey) and the ID of the Vault (vaultId) in Postman collection variables which are used by the secured endpoints.

Tip:
To skip steps 3–9, import the predefined collection from the class GitHub repository and only update your server address:

https://raw.githubusercontent.com/christiangessner/AU2025_1343/refs/heads/main/Vault%20Data%20API.postman_collection.json

---

Authentication

The Vault Data API authorization relies on access tokens, which are passed in the HTTP **Authorization** header. Tokens can be obtained in different ways, depending on how the application or service connects to Vault.

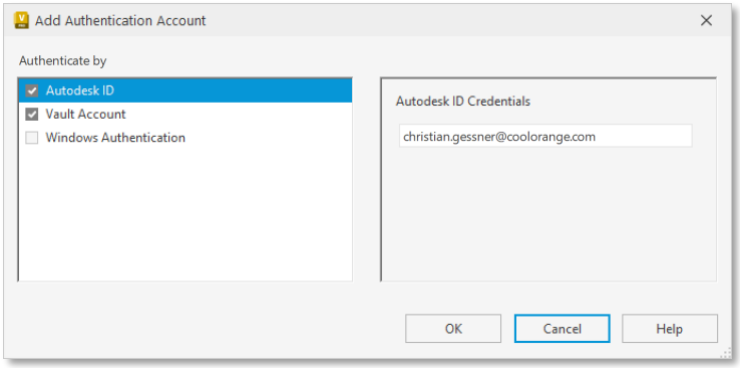
Samples obtaining an access token using the Vault Data API can be found in the Vault Data API online documentation:
https://aps.autodesk.com/en/docs/vaultdataapi/v2/developers_guide/basics/authentication/

Authentication: Autodesk ID

https://aps.autodesk.com/developer/overview/authentication-api

For integrations that rely on **Autodesk ID**, the APS **OAuth** flow is used. After signing in, a three-legged token is issued and must be sent with each request. This is often preferred when Vault is accessed outside the company network or when single sign-on is desired.

In the Vault **User Profile** settings, an Autodesk ID must be assigned to a Vault user:



VAULT USER PROFILE SETTINGS: ACCOUNT

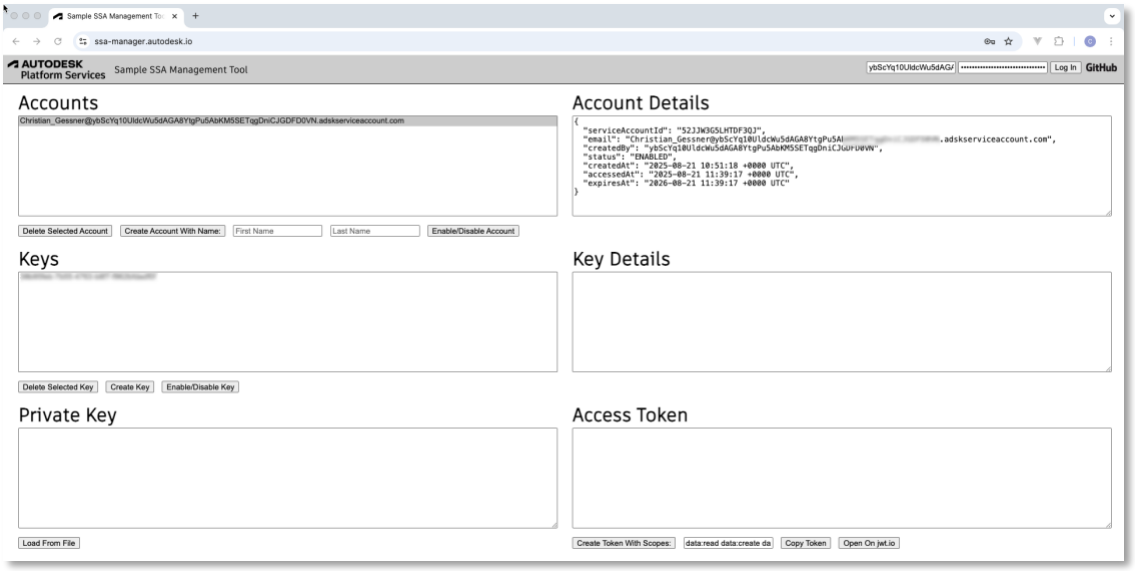
Add an Authentication Account to a User Profile:
https://help.autodesk.com/view/VAULT/2026/ENU/?guid=GUID-3EFC6249-BF3F-4787-9842-3D12DB502E14

Authentication: Secure Service Accounts (SSA)

https://aps.autodesk.com/en/docs/ssa/v1/developers_guide/overview/

For automated tasks, **Secure Service Accounts (SSA)** provide a headless option. These “robot accounts” can request tokens programmatically without user interaction.

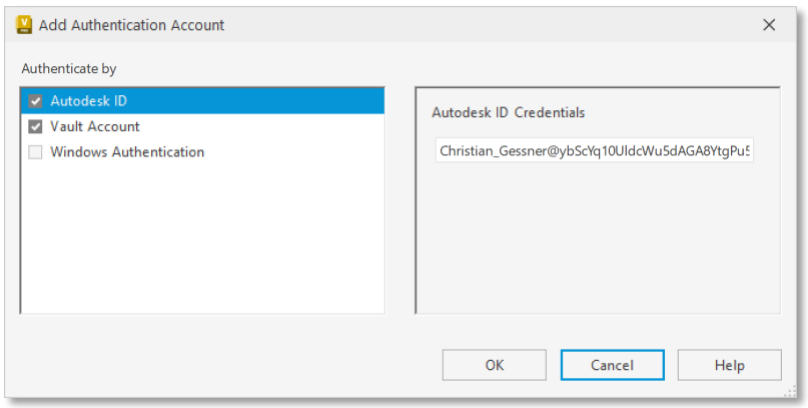
The **Autodesk Sample SSA Management Tool** (https://ssa-manager.autodesk.io/) can be used to create and manage Secure Service Accounts:



SSA MANAGEMENT TOOL

This tool can also be used to generate Access Tokens for testing purposes. The source code of the tool is publicly available on GitHub (https://github.com/autodesk-platform-services/ssa-manager-sample) and helps developers to understand how to integrate SSA into their own applications or integrations.

Because SSA creates unique email addresses for each account, these email addresses must be configured in the **Vault User Profile** settings:

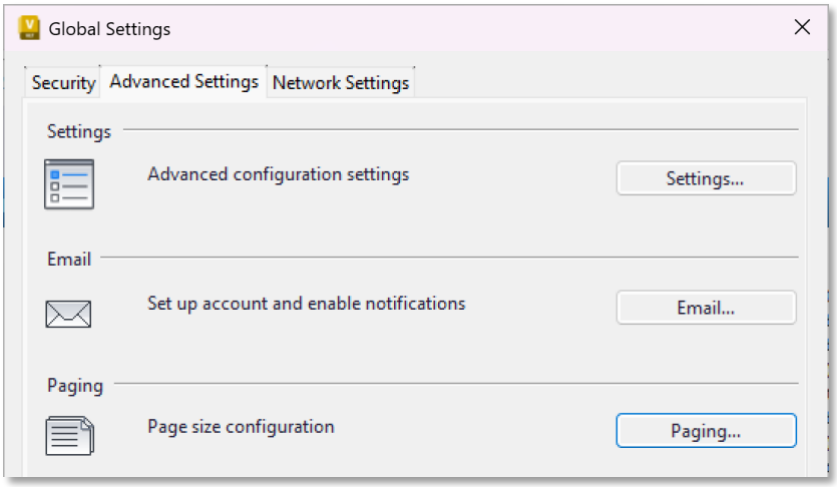


VAULT USER PROFILE SETTINGS: ACCOUNT

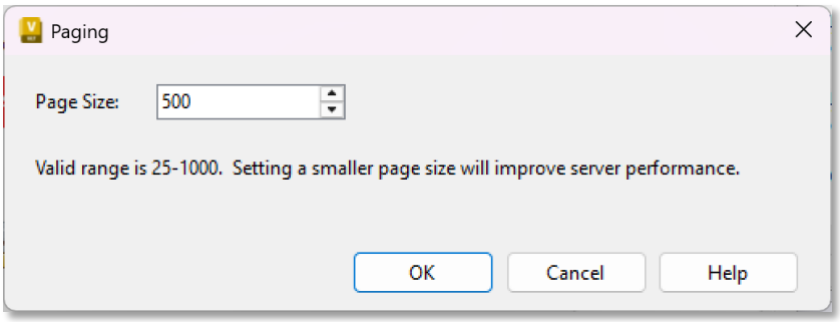
Tip:
In Vault, the Job Processor Account is usually a good fit for SSA Authentication.

Pagination

In the Vault Data API, **Collection Resources** always return paginated results. The API responds in "pages" instead of returning all the requested data at once. In the **Query String Parameter** of an HTTP request, a `limit` can be set, which specifies the page size. This page size must not be bigger, than the **Page Size** configured in Vault's **Global Settings**:



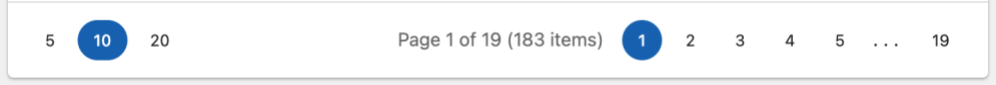
GLOBAL SETTINGS



PAGING

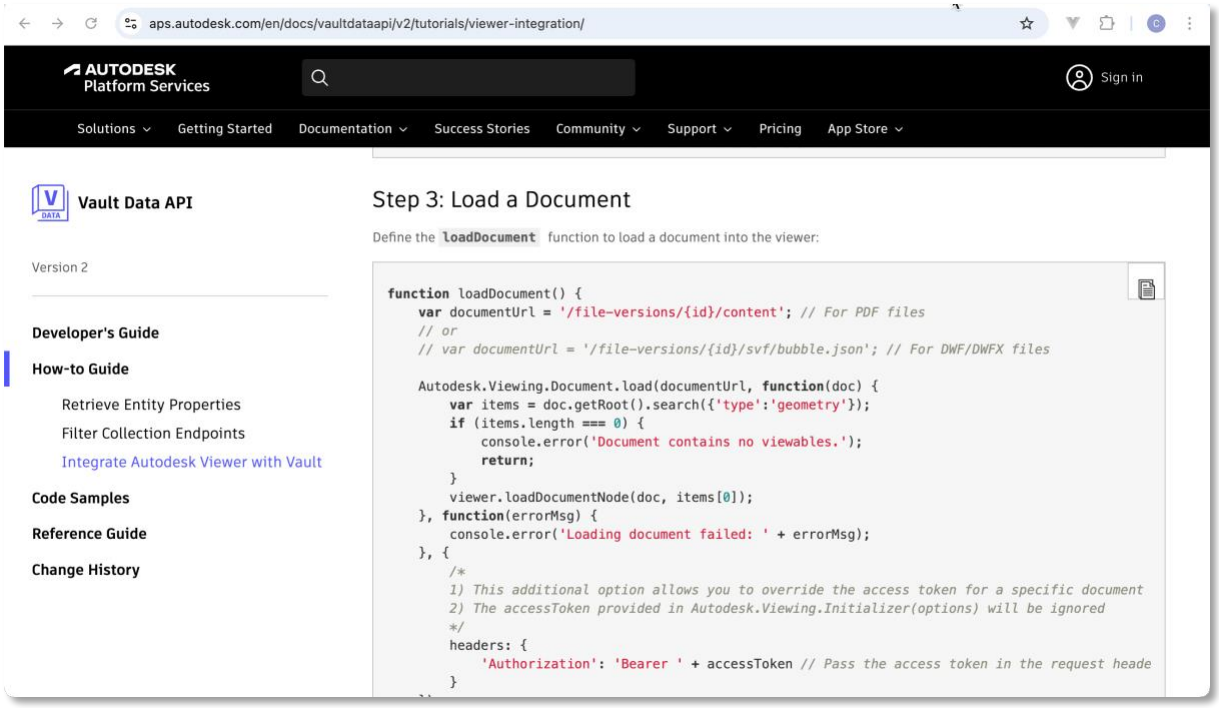
Configure Paging:
https://help.autodesk.com/view/VAULT/2026/ENU/?guid=GUID-35DC5E52-EF08-4864-8263-5E250F10714F

Tip:
Vault's pagination mechanism is ideal for "Infinite Scrolling" but cannot be used to develop a paging that allows users to jump between pages, e.g.



APS Viewer

According to the Autodesk Viewer Integration Tutorial, PDF-, DWF-, and DWFx-files are supported for Autodesk Viewer embedding. For DWF- and DWFx-files, viewables (SVF) are generated by the Vault Server and can be passed to the Autodesk Viewer using the endpoint `file-versions/{id}/svf/bubble.js`



TUTORIAL: INTEGRATE AUTODESK VIEWER WITH VAULT

The sample code in this tutorial indicates that PDF files can be passed directly using the endpoint `/file-versions/{id}/content`

This sample doesn't work but Tyler Warner described on LinkedIn how PDFs can be fetched from Vault and passed to the APS Viewer:
https://www.linkedin.com/feed/update/urn:li:activity:7372002940259201026

Cross-Origin Resource Sharing (CORS)

Vault Gateway enforces strict CORS, so use a proxy for browser apps. On-premises Vault Server allows enabling CORS in IIS if needed!

The Autodesk Vault development team recommends using a proxy API:
"The Proxy Server Approach is the most common and recommended solution for handling CORS issues when your server doesn't support cross-origin requests."
(Source: Irvin Hayes, Jr.; August 5, 2025)