Vault Vision Documentation

Release 0.1

Vault Vision

Feb 17, 2022

CONTENTS

Vault Vision is a Login-as-a-Service provider whose passwordless login technology powered by authentication software and devices enables easier authentication system integration for startup developers, IT security teams and seamless security for end users.

Note: This project is under active development.

CHAPTER

ONE

CONTENTS

1.1 Tenants

Tenants are the center hub of your authentication platform. It is the core entity that holds all your users, application links, and unique branding and authentication settings.

1.1.1 Properties

Domain - This is the domain for your auth platform, this is where your signup and login pages will live. This is what will show in the users address bar when signing up or logging in to your services. Once set, this can not be changed without contacting support. This is because your users are familiar with where they signed up, and any changes need to be communicated and coordinated with them so that they understand where and how they are authenticating for your service.

Note: Custom Domains If you choose a custom domain for your tenant, something like auth.mycompany.com, then you will need to make sure you create a DNS CNAME record for that custom domain (auth.mycompany.com in this example) to point to nextgenauth.vaultvision.com

This is how you will connect your custom domain to our services

Display Name - This is usually just your company name. It is the name that you can use to indentify yourself to end users. We will default to this name when sending system messages.

Support Email - This is the email address we will show to your end users so they can reach out for support if needed. Usually displayed in either system messages or if an error condition arises.

Support URL - This is the website URL we will show to your end users so they can reach out for support if needed. Usually displayed in either system messages or if an error condition arises. Additionally, this is where we will send end users that need more help during signup or login.

Terms of Service URL - This is the link to your terms of service for your web application. We show this link on your signup page and require that your end users agree to it during signup.

Terms of Service Version - This is the version of your terms of service that we record when a users signs up for your service. At signup, after they agree to the terms of service, we will record which version of the terms they agreed to based on what is currently set in this field for your tenant. When you update your terms of service you should update this version number as well so that we will maintain accurate records of what version users agreed to when they signed up.

Privacy Policy URL - This is the link to your privacy policy for your company. We show this link on your signup page and require that your end users agree to it during signup.

Privacy Policy Version - This is the version of your privacy policy that we record when a users signs up for your service. At signup, after they agree to the privacy policy, we will record which version of the policy they agreed to based on what is currently set in this field for your tenant. When you update your privacy policy you should update this version number as well so that we will maintain accurate records of what version users agreed to when they signed up.

Logo - This is the image that will be displayed on your sigunp and login pages. It will also be used in emails and system messages.

1.1.2 Actions

None currently, Once

1.2 Applications

Note: OAuth Client An Application in our Vault Vision parlance is synonymous with an OAuth Client. Our Vault Vision service provides the OAuth identity authentication for your OAuth Client Applications.

1.2.1 Properties

Application Name - This name that will refer to the application you are configuring to be linked to your tenant. It is only for management purposes and is never displayed to an end user.

Callback URLs - At the initiation of the user authentication process, your service will redirect a user to our login page with a special callback redirect uri that you specify in the querystring of that 302 redirect. After our auth platform authenticates that user, we check if the callback redirect uri that was specified in the querystring matches a Callback URL set here in the Application setting screen. If there is a match, then our auth platform will call the specified callback redirect uri and it will pass the OAuth token. On the service handler for this callback, that is hosted on your system, you will validate that OAuth token using our token endpoint and a signed JWT with the users idenity embedded in it will be generated and returned. This JWT can then be used to further authenticate the user in additional service calls. Usually this URL is located as something like: https://yoursite.com/auth/callback

Login URL - This this the URL that our auth platform will redirect unauthenticated users to so that a new user authentication process can be initiated by your application. The handler for this URL should generate a redirect to our authorize endpoint ('/authorize') on your tenant domain hosted on our systems. As part of that redirect, the Application client_id and callback redirect uri need to be included in the query string. Usually this URL is located as something like: https://yoursite.com/login

Logout URLs - At the initiation of the user logout process, your service will redirect a user to our logout handler with a special callback redirect uri that you specify in the querystring of that 302 redirect. After our auth platform ends all the sessions for that user, we check if the callback redirect uri that was specified in the querystring matches a Logout URL set here in the Application setting screen. If there is a match, then our auth platform will call the specified callback redirect uri so that your application can finish any remaining session closures if needed. In most cases, applications will usually remove any user sessions prior to initiating a user logout process, and in those cases, this Logout URL can simply be the home page, or whatever page you want to drop off newly logged out users. Usually this URL is located as something like: https://yoursite.com/loggedout

1.2.2 Actions

Edit - Using this action you can view or changes the URL and Name properties for your application.

Delete - This action will delete the Application and it will no longer be able to authorize or validate OAuth tokens or JWTs.

1.3 Users

1.3.1 Properties

Name - This name that will refer to the user in this tenant. It does not have to be unique and will be used for system and email messages to the User.

Email - This is the email address for the user, and must be unique inside each tenant. There can not be two users in the same tenant using the same email, it is akin to a username, and is the unique identifier for a user account.

Password - This is the password credential users provide to authenticate themselves. Setting this Password field for a user that currently has a FIDO security key credential assigned as the account credential, will cause that FIDO security key credential to be removed from the user account and it will be replaced by the password set in this field.

1.3.2 Actions

Update - The user’s name can be updated

Block/Unblock - Blocking a use will cause them to be blocked from authenticating, meaning they won’t be able to login anymore. This can be undone by Unblocking the user.

Delete - This will remove the user from the tentant, they will no longer be able to login and if they re-register, they will have a different id and user account.

1.4 Tenant Integration

1.4.1 Prerequisites