



VIBE End-to-End Encryption (E2EE)

System Administration Guide

Version 1.2.1

Index

<i>Introduction to Verifiable Identity-Based Encryption (VIBE)</i>	<i>3</i>
<i>VIBE E2E encryption in the Nextcloud App store</i>	<i>3</i>
<i>The Process of adding VIBE - what's needed</i>	<i>3</i>
<i>Activating VIBE E2EE in Nextcloud</i>	<i>3</i>
<i>Error Messages/Codes and resolution</i>	<i>14</i>

Introduction to Verifiable Identity-Based Encryption (VIBE)

Based on the Identity Based Encryption (IBE) standard invented in 2001 and commercialized in 2004, VIBE is an industrial grade, end-to-end authentication and encryption technology that greatly improves upon IBE and the more pervasive public key cryptography - PKI- thereby rendering it highly effective in solving numerous security challenges inherent in our connected world:

VIBE E2E encryption in the Nextcloud App store

The VIBE E2E encryption functionality has been implemented into Nextcloud using the Application add-on scheme in which Nextcloud core functionality is enhanced by adding open source or commercial Apps accessible in the Nextcloud App store. VIBE's E2EE solution is available for Nextcloud version 20 or above. Currently all desktop platforms (Windows 10 , Mac OSX 14 or higher and Linux) are supported; with iOS and Android available in late Q4 2021.

The Process of adding VIBE - what's needed

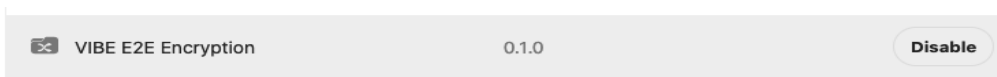
To add VIBE E2E to an Nextcloud installation one needs the following:

- ✓ A Nextcloud Administrator account for your Nextcloud instance, with full Admin Rights
- ✓ An updated instance of Nextcloud 20 or above

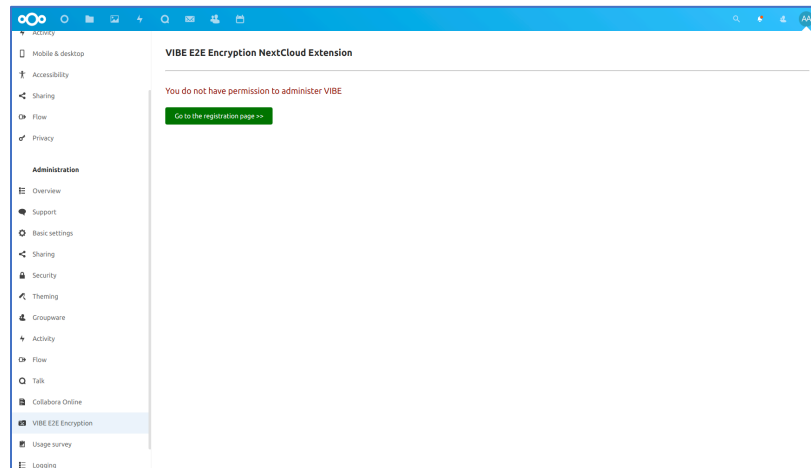
Activating VIBE E2EE in Nextcloud

The VIBE E2E deployment steps are as follows:

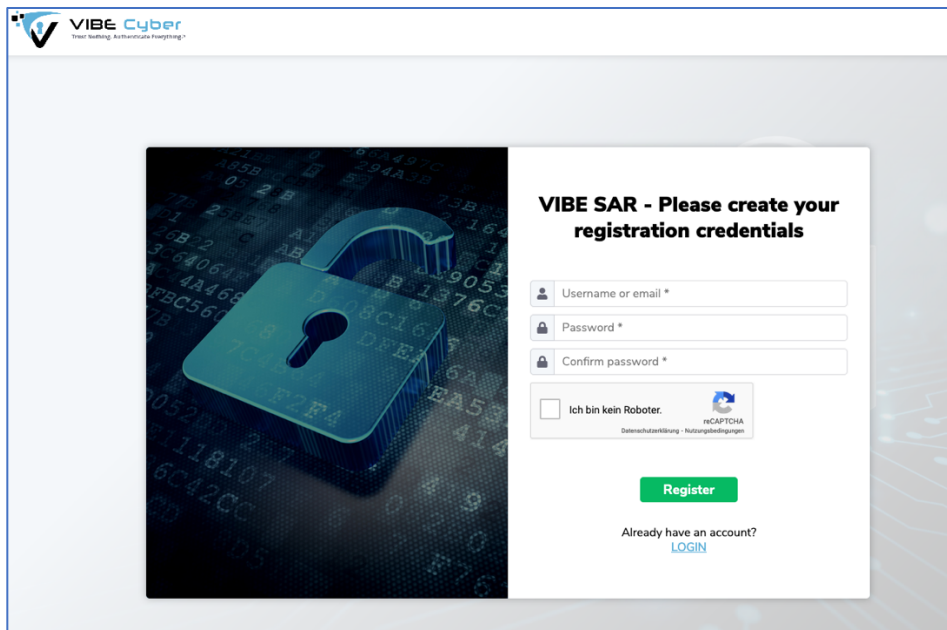
1. Log into Nextcloud with your admin account, click the profile icon on the top left, click Apps and navigate to the Security section.
2. Add the VIBE E2E encryption App to the server/backend installation by locating the VIBE E2E Encryption App and click the "Download and enable" button. The VIBE App is automatically enabled through the installation process.



3. Move to the "VIBE E2E Encryption" menu in the "Administration" section of the "Settings" menu. When selecting this VIBE E2E Encryption menu for the first time, the Administrator is informed that he doesn't have permission to administer VIBE until he has registered the Nextcloud installation (server/backend) with VIBE.

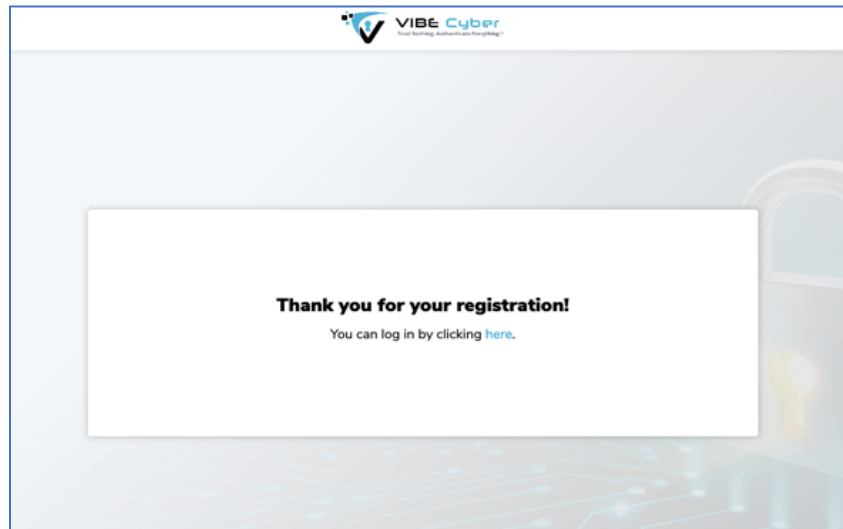


4. By clicking the green “Go to the registration page” button the Administrator is directed to the VIBE Subscriber Authentication & Registration (V-SAR) Portal to create his V-SAR Secure Remote Password (SRP) credentials, and associate a second device/channel to his preferred Multi-factor Authentication (MFA) application (such as MS Authenticator, Google Authenticator or most other Time-based One-time Password [TOTP] Authenticators).

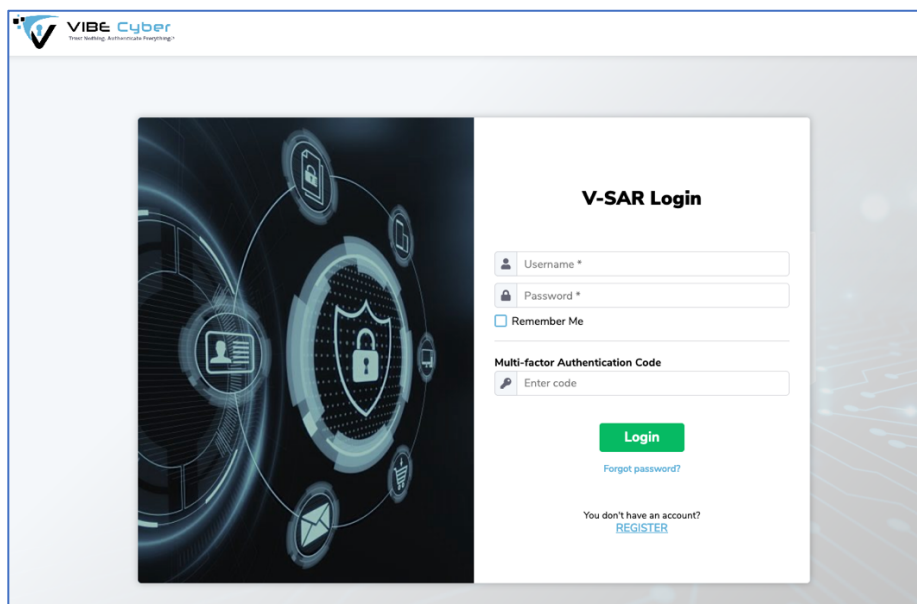


By using the Secure Remote Password (SRP) protocol, the V-SAR registration process ensures that no Administrator or user credential data is stored, eliminating the threat of sensitive data being stolen or otherwise compromised. This high-level security feature

comes with the tradeoff that the Administrator has to ensure that he remembers his created credentials until he first logs into the V-SAR Portal.

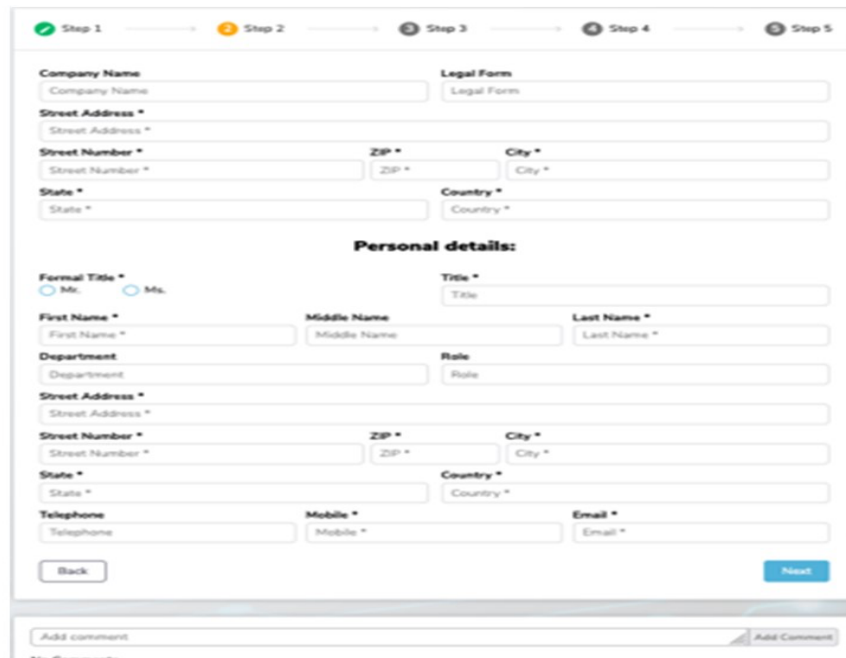


5. Following successful completion of step 4, the Administrator is directed to the V-SAR where he is asked to log in with his created credentials and associated MFA code.



6. The Nextcloud Administrator is then guided through the authentication and subscriber registration process in which the following information is entered:
 - ✓ Organization (Tenant) information

- ✓ Position/role in the organization, and related details
- ✓ Personal information verified by upload of government-issued or equivalent identity document such as a driver's license (e.g. Organization ID could be deemed acceptable, at your discretion).
- ✓ Invoicing information*
- ✓ Secure Remote Password (SRP) credentials for later access to the VIBE Management Console (V-WMC)
- ✓ Unique ID (UID) selection (e.g. email address) and entry, and upload of a proof document or entry of an UID-dependent verification code (in case of email!)



Step 1 Step 2 Step 3 Step 4 Step 5

Company Information

Company Name Legal Form

Street Address *

Street Number * ZIP * City *

State * Country *

Personal details:

Formal Title * ☐ Mr. ☐ Ms. Title *

First Name * Middle Name Last Name *

Department Role

Street Address *

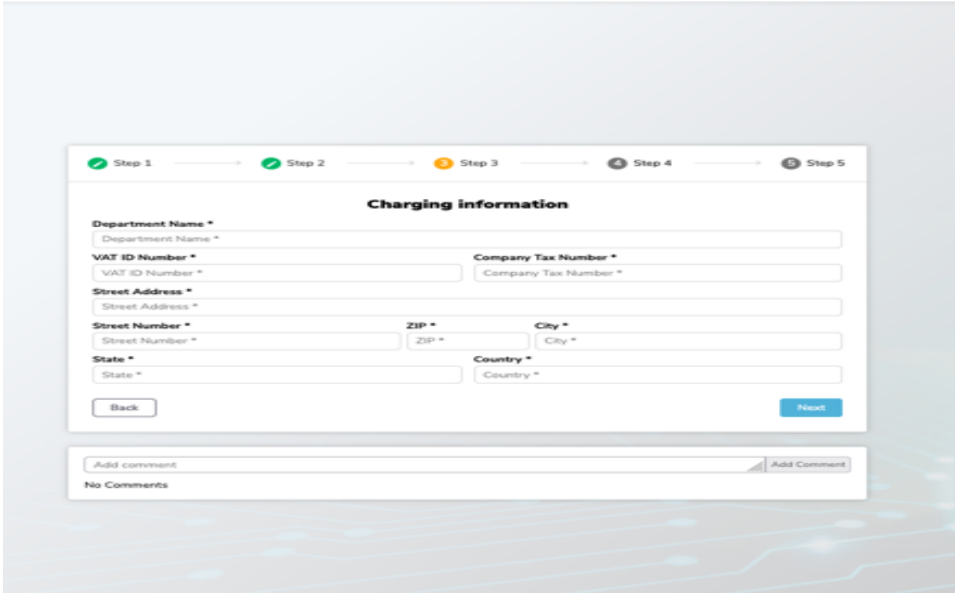
Street Number * ZIP * City *

State * Country *

Telephone Mobile * Email *

No Comments

*VIBE is provided to the subscribing System Admin and all registered subscribers as a free 60-day trial which can be cancelled at any time. Following the free trial period, subscribers are automatically granted a pre-paid, binding VIBE 12-month subscription. Subscriptions will auto-renew annually, unless cancelled 4 weeks or more, prior to the end of the subscription period. Any VIBE subscribers added to the organization during the initial and subsequent one-year terms will be invoiced on a pro rata basis, such that all subscribers in a given organization are under a co-terminus agreement. For clarity, the contracts for all users in the organization expire/renew on the same day, regardless of initial date of deployment.



Step 1 → Step 2 → **Step 3** → Step 4 → Step 5

Charging information

Department Name *

VAT ID Number *

Company Tax Number *

Street Address *

Street Number *

ZIP *

City *

State *

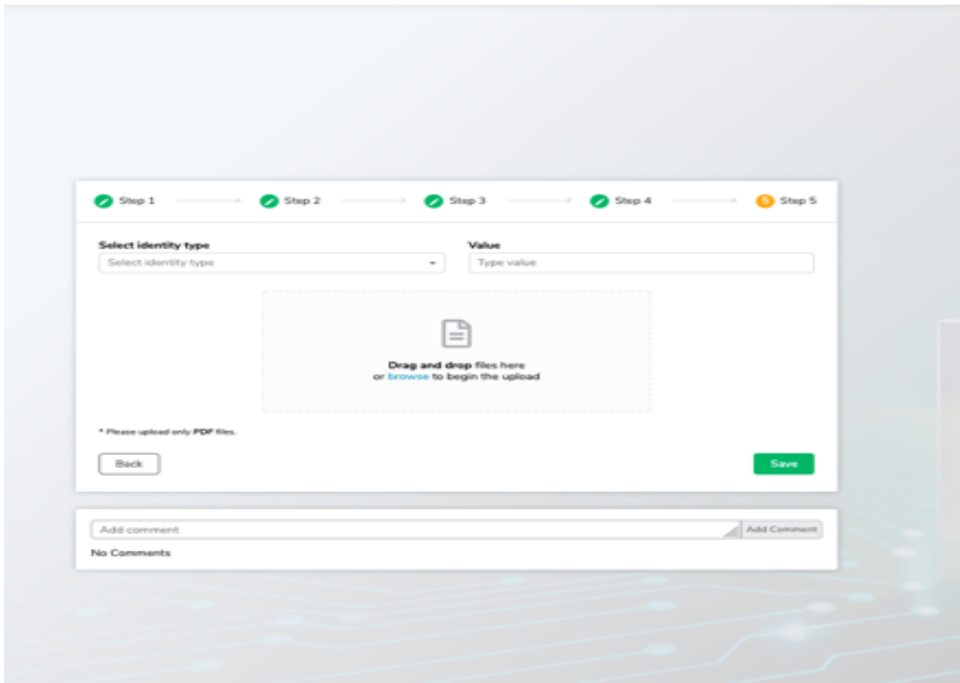
Country *

[Back](#) [Next](#)

Add comment [Add Comment](#)

No Comments

✓



Step 1 → Step 2 → Step 3 → Step 4 → **Step 5**

Select identity type

Value

Drag and drop files here
or [browse](#) to begin the upload

* Please upload only PDF files.

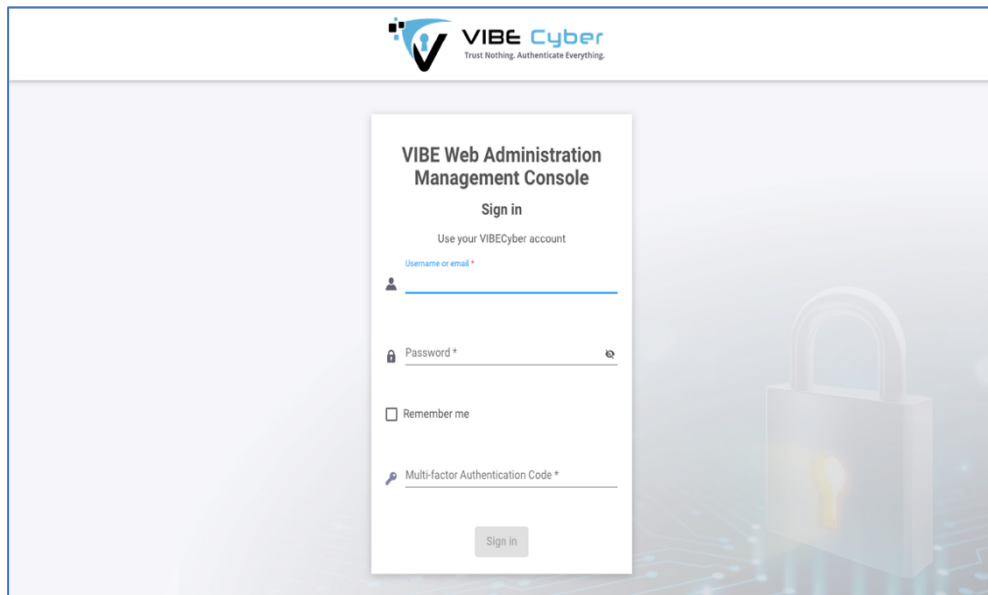
[Back](#) [Save](#)

Add comment [Add Comment](#)

No Comments

- When the registration process is completed, the System Administrator will receive an email message stating that he will be notified once the Subscription application has been approved by VIBE.

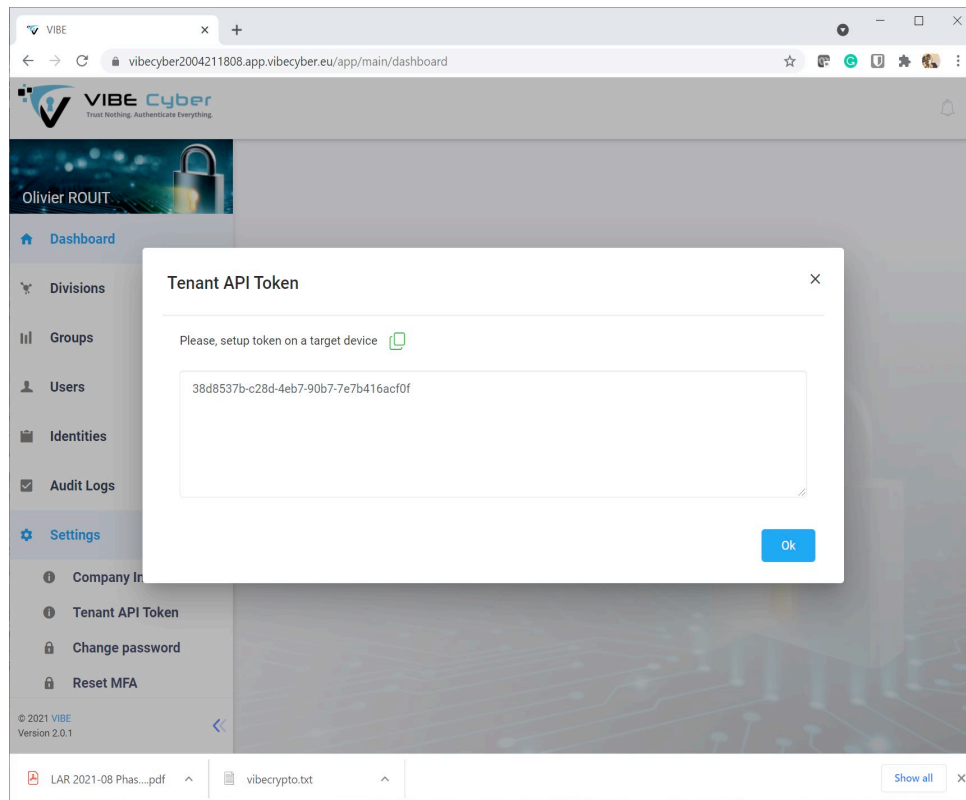
8. Once the Administrator's subscription is approved, the data required for creation of the Tenant in the Trusted Centre is automatically sent by the V-SAR to the V-WMC. The Administrator then receives an email message asking him to connect to his company's Tenant account. By clicking on the link provided in the email message, the Administrator is directed to the V-WMC and invited to login by inputting the credentials that he created in the V-SAR registration process, in combination with his MFA code.



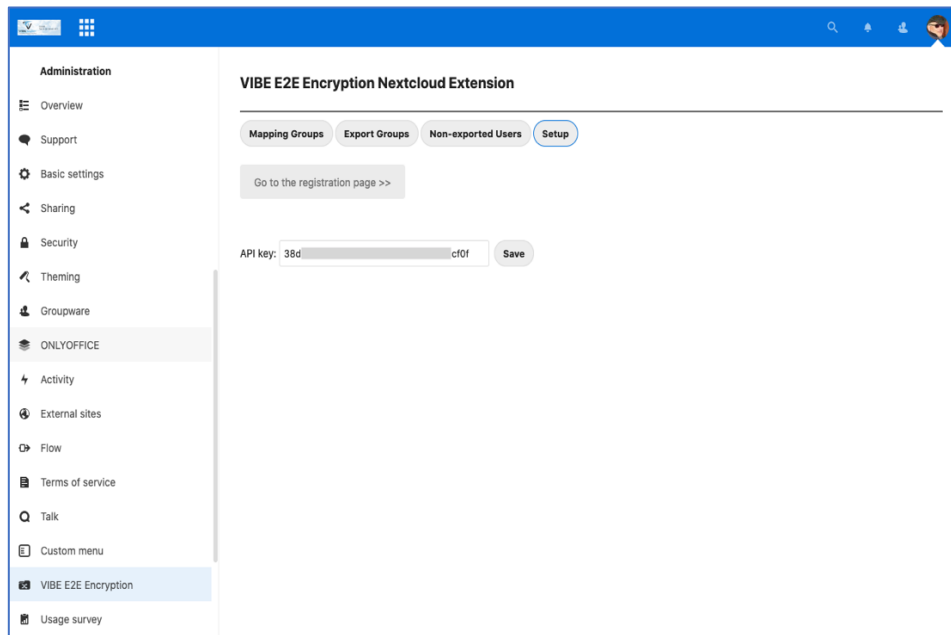
The screenshot shows the VIBE Web Administration Management Console Sign in page. The page has a light blue background with a large, faint padlock icon on the right. The sign-in form is centered and contains the following elements:

- VIBE Cyber logo and tagline at the top.
- Form title: "VIBE Web Administration Management Console"
- Section header: "Sign in"
- Instruction: "Use your VIBECyber account"
- Username field: "Username or email" with a red asterisk and a user icon.
- Password field: "Password" with a red asterisk, a lock icon, and a toggle icon.
- Remember me checkbox: "Remember me"
- MFA field: "Multi-factor Authentication Code" with a red asterisk and a user icon.
- Sign in button: "Sign in"

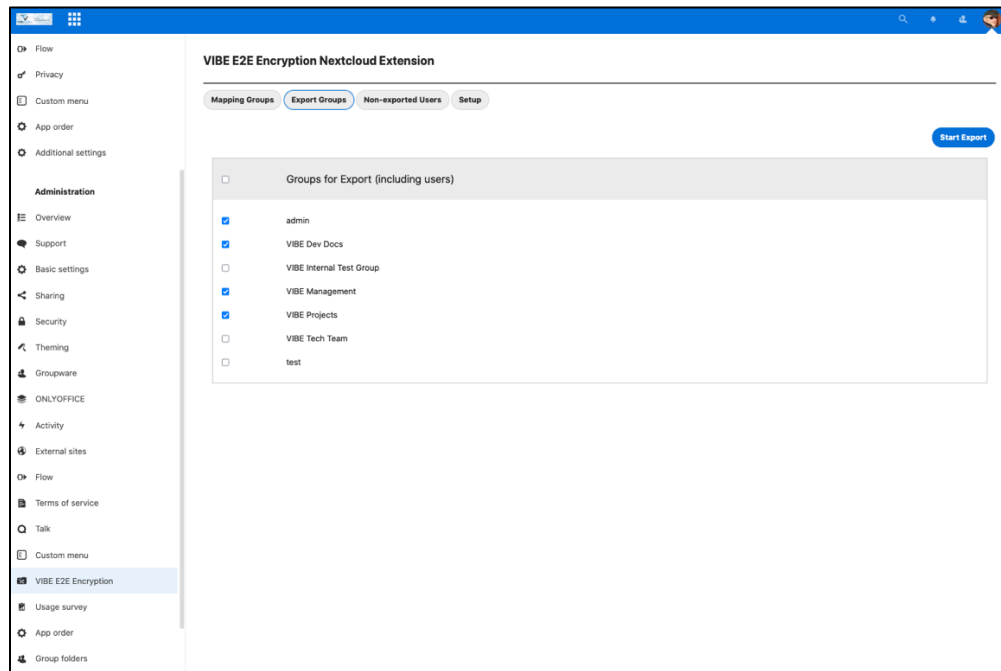
9. The customer Systems Administrator – now established as the VIBE Tenant Admin - is instructed by email to log in to the V-WMC, go to the Settings section and access the [Tenant API Token](#) sub-menu to obtain an API Token.



10. Next, the Admin copies and enters the token in the API section of the [VIBE E2E Administration](#) menu on the Nextcloud backend, thus triggering activation of the VIBE service. By clicking the [SAVE](#) button, the Nextcloud backend is validated at the VIBE Trusted Centre, and assigned the Hardware Security Modules (HSM) mapped/associated with the subscription.

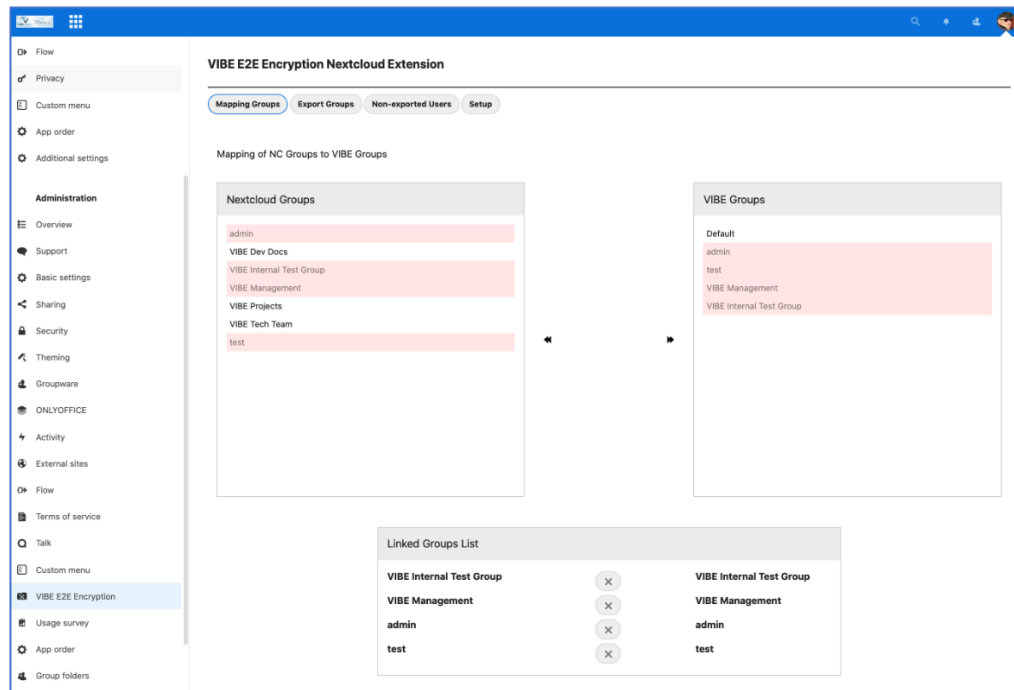


11. Once the VIBE Service has been activated, the Administrator can enable creation of the Public/Private Key pairs for all the Nextcloud users under his jurisdiction by exporting their user profiles to the V-WMC. This is easily accomplished via the VIBE User & Group export mechanism accessible under the *VIBE E2E Encryption* menu in the “Administration” section of the *Settings* menu.



The VIBE service allows Administrators to create rules-based “circles of trust” which allow different levels of sharing based on the organization’s needs. For example, a company might have a Senior Management Group in which only those who have this designation can exchange encrypted files. It might have a different trust circle related to a specific, highly-confidential project, and another that is solely for the sharing of authenticated, encrypted files with a key supplier. In essence, the VIBE structure affords the Admin the ability to reflect the hierarchical and relational secure information-sharing requirements of a typical organization.

In a new VIBE Nextcloud setup, a default VIBE Division is created to which all VIBE Groups are initially assigned. This serves as a starting-point from which an Admin can create their own information-sharing structure, which might involve mapping or exporting existing Nextcloud Groups to the V-WMC. (e.g. select the relevant NC groups to export and click the Export Groups button).

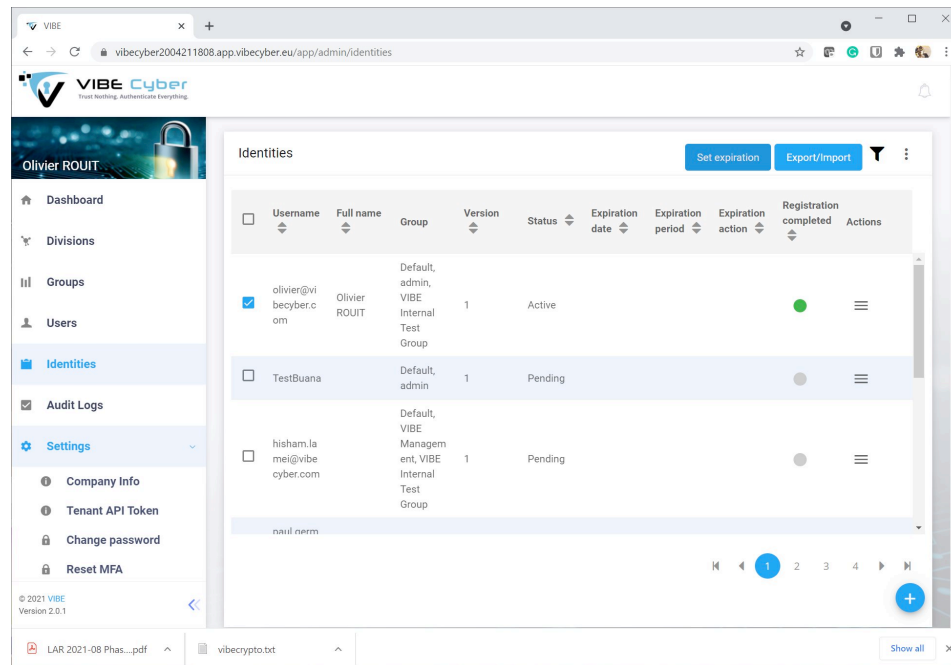


By mapping Nextcloud Groups to VIBE Groups, the users are empowered to share encrypted files, and it's guaranteed that their identity is properly authenticated when uploading or retrieving such files.

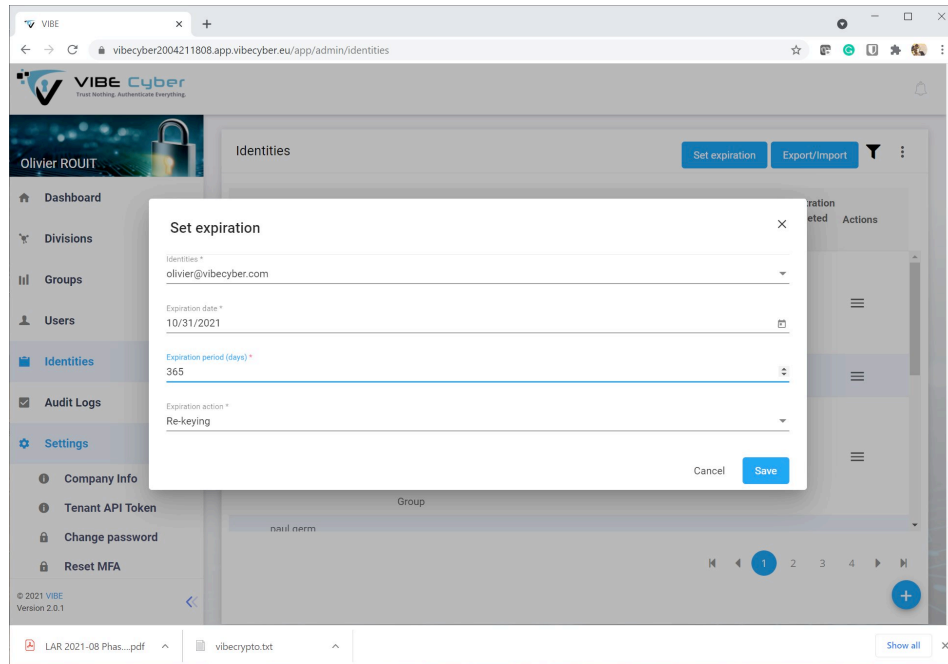
Also, Administrators can easily remove any existing linked groups by clicking on the delete button.

12. Once the Administrator has imported all User and Group information to the V-WMC, he is able to review and manually amend and/or input missing information. Further, the data required for the users to register and activate their VIBE subscription is easily replicated to the V-SAR to simplify and accelerate the identification and registration process for users. This exchange between V-WMC and V-SAR is accomplished using VIBE's own authenticating encryption technology to ensure hardened data exchange and superior security. Additionally, the Admin can determine which data fields require mandatory completion by the end user.
13. Once the user data is replicated in the V-SAR, each user is notified via email that their organization's System Administrator has subscribed them to VIBE E2E Encryption. They are instructed to log in to their Nextcloud account to register for the VIBE service. The subscriber registration process is described in detail in the VIBE E2EE User's Guide.

14. Administrators have access to additional features in the V-WMC, which allow for actions such as user deactivation, setting of rules-based identity expiration dates etc.



Expiration dates might be used when users are registered to receive encrypted files related to a specific event, such as an RFP response deadline that includes 3rd-party vendors. Once the deadline is passed and the RFP submitted, the 3rd party VIBE subscriptions could be easily dissolved.



Error Messages/Codes and resolution

Errors in Nextcloud Administration GUI (Popup)

Error Type	Error Appearance	Description	Suggestion/Remedy
WMC API error	Error: {WMC API error}, where {WMC API error} is an error received from WMC API.	displayed in a case of failed WMC API call: <ul style="list-style-type: none"> during exporting users: user already exist, or any other processing error on WMC API side; during setting up API key ("Invalid API token"). 	if error is not self-descriptive (e.g. mentioning that user's identity to export already exists on WMC side), contact WMC Administration with the error text.

Errors in Nextcloud Logs

Error Type	Error Appearance	Description	Suggestion/Remedy
WMC WEB API	Status code: {HTTP Status Code}, message: {Error message}, where {HTTP Status Code} is	Logged in a case of failed WMC API call.	If error is not self-descriptive (e.g. mentioning that user identity to export

	HTTP error code received from WMC API, and {Error message} is a message received from WMC API.		already exists on WMC side), contact WMC Administration with the error text.
Error Checking and preparation of users	{Nextcloud error message}, where {Nextcloud error message} is internal Nextcloud error/exception.	Could occur during exporting user to WMC in a case where user information could not be read via Nextcloud API (e.g. due to database connection lost, incompatible 3rd party apps etc).	Check Nextcloud guidelines on details for {Nextcloud error message} error.
GroupDeletedListener	GroupId: {Nextcloud Group identifier}, where {Nextcloud Group identifier} is Nextcloud group name.	Could occur during removing users from the group on WMC side after group deletion in Nextcloud Administration. Related error will be logged as a dedicated log message (for example, failed WMC API call details).	Check additional error message in the Nextcloud log for details.
UnlinkedGroupsListener	GroupId: {Nextcloud Group identifier}, where {Nextcloud Group identifier} is Nextcloud group name.	Could occur during removing users from the group on WMC side after unlinking Nextcloud group and VIBE group in Nextcloud Administration, VIBE settings. Related error will be also logged as a dedicated log message (for example, failed WMC API call details).	Check additional error message in the Nextcloud log for details.
UserAddedToGroupListener	UserId: {Nextcloud User identifier}, GroupId: {Nextcloud Group identifier}. {Error message} Where {Nextcloud User	Could occur after adding user to the group in Nextcloud Administration area in a case where specified user couldn't be added	Check error message for details; in most cases this could be WMC API call fail, or internal Nextcloud error due to absent

	identifier} is an identity of the Nextcloud user, and {Nextcloud Group identifier} is Nextcloud group name.	to the related group on WMC side.	database connection, internal data inconsistency, incompatible 3rd party apps etc.
UserRemovedFromGroupList ener	UserId: {Nextcloud User identifier}, GroupId: {Nextcloud Group identifier}. {Error message} Where {Nextcloud User identifier} is an identity of the Nextcloud user, and {Nextcloud Group identifier} is Nextcloud group name.	Could occur after removing user from the group in Nextcloud Administration area in a case where specified user couldn't be removed to the related group on WMC side.	Check error message for details; in most cases this could be WMC API call fail, or internal Nextcloud error due to absent database connection, internal data inconsistency, incompatible 3rd party apps etc.

VIBE Cybersecurity thanks you for using VIBE, and hope that you can rest easier knowing that you have guided your organization to an unparalleled level of security that will protect your most sensitive data from external threats.

If you require additional information or more guidance on how to deploy VIBE, please email info@vibecyber.com