Access and Authorization

- VINCE Accounts
  - Creating an Account
  - Vendor Association
  - Multifactor Authentication
    - Using TOTP
- Authentication reset requests
  - MFA Reset Requests
  - Password Recovery

**VINCE Accounts**

The VINCE coordination platform allows for anyone to anonymously report vulnerabilities. However, if you wish to participate in the coordination process, including discussions with vendors and researchers/reporters, then an account is required. We recommend that each individual on a team creates a VINCE account to participate on behalf of their organization. The account will provide the ability to view case information, post in the case discussion, provide vendor status and statement updates, and direct message CERT/CC. VINCE was designed and created to encourage the interaction between vendors and reporters, so creating an account and participating in the coordination efforts will increase cooperation, information sharing, and allow

**Creating an Account**

The overall process of obtaining a VINCE account is:

1. Navigate to the VINCE website
2. Click on "Create an Account", or go directly to this link
3. Complete the signup form
   a. When filling out the form, please note that your **Display Name** will be visible to other VINCE users. It can be changed later in your account settings.
4. Once your account has been approved and you can login, you will be able to select your method of 2FA

**Vendor Association**

If you are a **researcher** or the **first** employee from your vendor organization to create a VINCE account then your account is placed into a pending state for CERT/CC review and approval. Once approved, you will receive an email letting you know that you have been approved. **You will still need to be associated with your organization in VINCE by a CERT/CC analyst.** Please send us a **direct message** requesting to be associated with your organization and we will independently verify with your organization that the request is valid. If you are the first user for the vendor, we will additionally make you the administrator so that you may manage the group.

If you are a part of an existing vendor and your group administrator invited you directly to VINCE, then you should automatically be associated properly with your vendor and see any cases that they are involved in on your Dashboard. If you do not see cases and expect to, please send us a **direct message**.

If your group has an administrator in VINCE, we will transfer your request to be associated with them to the admin.

**Multifactor Authentication**

VINCE accounts require multifactor authentication for obvious security reasons. This requirement is part of the reason we recommend that each user has their own individual account, as opposed to a shared team account, as the team would have to securely share the MFA token as well. VINCE previously allowed users to perform multifactor authentication with Short Message Service (SMS) text messages. However, since November 8, 2023, the SMS option has been disabled, and all multifactor authentication must be performed using time-based one-time passwords (TOTP). TOTP requires access to a third-party application, such as Google Authenticator, Duo, or LastPass Authenticator.

**Using TOTP**

1. A QR code will be generated that can be scanned using the authentication application of your choice.
2. Enter that temporary password generated by the application.
3. (Optional) Give your device a friendly name.
4. You will have two forms of confirmation that your account has successfully enabled TOTP multifactor authentication on your account:
   a. A green banner on the web page indicating success and displaying your User Profile (see below), and
   b. An email message confirming your MFA was successfully enabled.
Authentication reset requests

MFA Reset Requests

If a user needs to reset their MFA due to lost/new device, please use the MFA reset process. The user must first login using their name and password. When the MFA prompt appears, click the “Troubleshoot MFA” link and follow the instructions on resetting the MFA. Note that if a password reset is required, this must be completed prior to any request to reset MFA.

The user will be required to provide a reason for the reset.

Upon completing the form, follow the instructions in the email sent to the user. A VINCE analyst will receive the request and will reset the MFA within 1-3 business days.

Once the VINCE analyst has reset the MFA, the user will receive an automated email that their MFA has been reset. Upon logging in to VINCE, the user will be prompted to select a new MFA method.

Password Recovery

If a user needs to recover their password, they can use the VINCE password recovery feature. This can be accessed by clicking “Forgot your password?” on the login page or clicking the previous link. CERT/CC analysts will review these requests and may reach out to you for confirmation or validation of the request.

If you need additional help, you can click the “Need help?” link that will share the following information:

If you forgot your password, you can reset your password.