3D Secure Authentications

Overview

3D Secure is a protocol designed to be an additional security layer for online payment transactions, including debit, credit, wallets and APMs. This protocol requires customers to complete an additional verification step with the card issuer when paying online.

Common 3D Secure Authentication methods include push notifications, face recognition, fingerprint, and dynamically generated one-time passwords (OTPs).

The 3D Secure Authentications report provides an overview of 3D Secure payment authentication attempts and allows you to see any 3DS details processed in transactions. You will be able to see in the 3D Secure Authentications Details panel information such as 3D Secure Authentication ID, 3DS Provider Contract ID, 3DS Version, Error number and description, Signature verification, Card brand information, Reason code and description, as well as more details.

For more information, including the frictionless and step-up flows, see the 3D Secure documentation.

Availability

Merchants with the following roles in Verifone Central can access the 3D Secure Authentications report:

- Merchant Admin
- Merchant Reviewer
- Merchant Supervisor
- Merchant User
- Merchant Cashier

> **Merchant Users** can only access the 3D Secure Authentications of their organization and cannot access the 3D Secure Authentications of their sub-organizations.

For more information on user roles and permissions, check the Users and merchant roles article.

Benefits

- One place to run reports for successful and non-successful 3DS transactions.
- Helpful for billing of 3DS authentications.
- Detailed view related to 3DS authentications (**example**: 3DS contract ID, organization ID, 3DS version etc).

3D Secure Authentications in Verifone Central

1. Log in to your Verifone Central account.

2. Navigate to **Commerce** -> *Reporting* and then click on **3D Secure Authentications**.

---
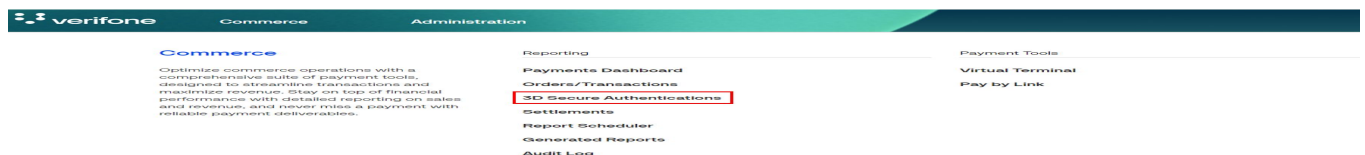
3. You can generate reports using different types of filters to query 3D Secure authentication data.

- Filter by 3DS authentication identifiers:
  - **3DS Authentication ID**: it is a unique 3D Secure ID attached to 3DS authentication.
  - **3DS Provider Contract ID**: use the 3D Secure Contract ID, that can be found under *Administration >* 3DS Contracts.
  - **Scheme Transaction ID**: is assigned by the schemes for 3DS authentication. This ID will help link 3DS Authentication, the order, and the transaction ID. It allows us to backtrack from the order and transaction page to identify the associated 3DS authentication using the Scheme Transaction ID.
- Filter by **date**: Select the start and end date for when the authentication occurred.
- Filter by **Organization**: you can filter the results according to the organization(s) you are part of, by selecting the needed organization(s) from the main dropdown menu, or by selecting one of the below three options:
  - **Name** - use the name of the desired organization or part of the name.
  - **Organization ID** - use the organization ID, that can be found under *Administration > Organization Company and Sites*.
  - **Business Identifier Value** - use the business identifier value, that can be found under *Administration > Organization Company and Sites*.
- Filter by **3DS Statuses**:

- **Successful**: 3DS authentication successfully completed
- **Failed**: 3DS authentication didn't go through
- **Unable to complete**: 3DS authentication is abandoned or dismissed
- **Successful attempts**: 3DS authentication is a successful challenged authentication
- **Challenge required**: 3DS authentication where the card issuer has determined that the transaction requires additional authentication to meet security requirement (applies to consumer authentication 2.0 - decoupled authentication)
- **Rejected**: 3DS authentication rejected by the card issuer