Single Sign-On (SSO) Authentication

Overview

The federated Single Sign-On (SSO) system enables users to authenticate to one domain or platform and access connected domains without logging in again each time. The Federated Identity Management (FIM) system facilitates organizations to share user identities and user credentials across various domains. Open standard protocols such as SAML, OAuth, OpenID Connect or SCIM ensure that the authentication and sharing of user identities across domains is secure.

Once two or more domains are federated, you can log into one and thus be authenticated and logged in to the others automatically.

Availability

The feature is especially suited for acquirers and financial/banking institutions that act as acquirers that want to integrate Verifone Central into their solution or offering.

To start the integration process, please contact your Verifone Sales representative.

To make SSO available, a collaboration between the client's system admins and Verifone IT department is necessary.

> **Note:** The Single Sign-On (SSO) Authentication is available only for the US region.

Benefits

The federated SSO feature provides the following benefits:

- Improves the user experience by enabling easy access to all connected applications
- Saves time
- Provides secure access to all the applications and domains users need, avoiding a cumbersome password management system

Requirements

To use the federated SSO feature, your corporate identity management system should support one the following technology standards

- SAML
- OIDC

Two platforms that use the standards listed above that most other clients use are:

- Okta
- Azure Active Directory

Set-up and configuration in Verifone Central

After all the necessary system administration tasks have been done, the required changes in Verifone Central can be made as well.

To configure and activate the federated SSO feature, the Verifone admin will mark the customer organization as a **federated entity**.

Every user onboarded to the organization will be automatically considered a **federate user**. As a result, the users will be able to login to Verifone Central only via the SSO function.

After the organization is marked as federated the following settings will be applied:

1. All password management capabilities will be disabled for a federated user. As a result:
    - The **Change password** and **Reset password** functions will be disabled in Verifone Central.
    - Password related emails (welcome email, reset password email, password expiry email) will not be sent out to federated users.
2. The login function will be disabled, and authentication will be blocked for federated users:
    - A message suggesting to login from your own internal systems will be sent to federated users when they attempt to login.
3. Federated users will be redirected to a special page after they log out and not to the login page.
4. No API Keys related changes will be needed. A federated user will be able to generate and use API keys like a standard user.