Product Transparency Notice

For any queries, please contact privacyteam@symantec.com

VIP Enterprise Gateway, VIP Access Manager, VIP Access Mobile and Desktop, VIP Trusted Device, VIP Mobile Software Development Kit

This Privacy Transparency Notice describes how VIP Enterprise Gateway, VIP Access Manager, VIP Access Mobile and Desktop, VIP SDK ("Product") collects and processes Personal Data. Its purpose is to provide You (our current or prospective "Customer") the information You need to assess the Personal Data processing that is involved in using the Product.

1. Product Description

VIP Enterprise Gateway (VIP EG) is a 'self-hosted' on-premise software component deployed by the customer to integrate enterprise applications and directories with the VIP Authentication Service. VIP Enterprise Gateway enables multi-factor authentication by utilizing a first- and layering multiple second-factors of authentication. The first factor is a username/password associated with each end user, which is stored in the customer's enterprise directory. The second-factor can be any of the many Authenticators as supported by the VIP Service. The second factor validation is performed by the Service. For each validation request sent to the VIP Enterprise Gateway, the first-factor validation is performed locally at the enterprise directory. VIP Enterprise Gateway then completes the second factor authentication against the Service. VIP Enterprise Gateway also records audit logs that record authentication events processed through it. Enterprise Gateway includes an LDAP synchronization component that adds or removes information related to the user from the VIP Service.

VIP Access Manager (VIP AM) is a 'self-hosted' virtual appliance deployed by the customer that provides single sign-on with strong authentication, access control, and user management. Additionally, this solution allows the customer to extend internal security policies to public and private cloud services in support of compliance and auditing requirements. It includes a Single Sign-On ("SSO") portal and an administrator portal responsible for enforcing access policies. The administrator portal permits certain designated and authorized users to add Connectors, polices, and user stores (or authentication sources). VIP AM enables end users to authenticate against single or multiple user stores, including, but not limited to Microsoft Active Directory, LDAP, IWA, ADFS, and third-party identity providers which support identity federation based on SAML. Administrators can control which cloud applications an end user may access by defining policies, based on the end user's identity and session context and enforce strong authentication. Administrators can also create Connectors to various service providers from the application catalog. VIP Access Manager records important security events to create audit trails that can be transmitted to a log management and SIEM solution. The customer can archive the logs according to its requirements and internal policies.

VIP Access is a software Authenticator that is made available to a customer's end users. This software is an application that is compatible with various mobile and personal computer operating systems. VIP Access offers the customer's end user the capability to authenticate to the Service using an OTP or a VIP Push, where available.

VIP Trusted Device is an Authenticator in the shape of a single-factor cryptographic software. This Authenticator consists of a cryptographic key stored on disk and associated with a unique VIP Credential ID. It utilizes a browser plug-in to manage cryptographic keys generated and stored in a proprietary key-store on the End User's device. Authentication is accomplished by proving possession of the device. The Authenticator's output is provided by direct connection to the user endpoint, facilitated by the browser plug-in, and consists of a signed message. This is used as a second authentication factor when it is associated with a local End User identity at the customer.

VIP Mobile Software Development Kit (VIP SDK), sometimes referred to as the Credential Development Kit (CDK), is a software development kit for iOS and Android mobile operating systems. The SDK is typically useful for mobile application developers who prefer to add VIP second factor authentication, transaction signing, and risk based authentication capabilities to their custom mobile application.

Further information about the Product is available at:

https://vip.symantec.com/

2. Personal Data Collection And Processing

Sources of Data

VIP Enterprise Gateway utilizes customer active directory information. If the customer has configured LDAP synch, then VIP EG can upload end user usernames to the VIP Service. Optionally, with LDAP synchronization configured, additional user attributes can be specified by the customer to be synchronized: first name, last name, email address to facilitate helpdesk functions.

VIP Access Manager collects end user and admin login information from user input. If third-party identity providers are used, then other forms of data might be collected, per the customer's implementation and choice. If the local directory feature is enabled, then data is stored locally. Else, only the first/super admin's information is collected and stored locally.

VIP Access is installed at the customer's end user endpoint. For mobile devices, nothing is collected by the application by default. The customer can configure the service to collect data on device hygiene for authentication purposes (e.g. deny access to a user with a phone where malware is detected. For desktop, no data is collected.

VIP Trusted Device collects local device information and shares it with VIP Services.

VIP SDK: If the customer utilizes the VIP SDK to enhance their mobile application with Intelligent Authentication capabilities, then the following data is collected: OS name and version; Wifi and Bluetooth MAC address; GPS coordinates; application ID; device name, model, OS details, SIM serial number and operator info, and subscriber ID.

Respective Roles of Symantec and Customer

The product is an on premise offering. The customer is the data controller of Personal Data collected in the course of the use of the product. The use of the product does involve Symantec as a data processor. However with respect to any Personal Data transmitted voluntarily from the Customer to Symantec for the purposes of the Product, the Customer remains the Controller, and Your Symantec contracting entity as specified in Your applicable Agreement ("Symantec") acts as a Processor. For such cases, the rights and obligations of both parties with respect to Personal Data processing are defined in the applicable Data Processing Addendum available on the Symantec Privacy - GDPR Portal.

Personal Data Elements Collected and Processed, Data Subjects, Purpose of Processing

Personal Data Category	Data Subject Category	Purpose Of Processing
Individual identifiers (names), contact information (email address, other contact information the customer may configure to include)	Customer employees and contractors, clients and vendors	Delivery of the authentication services **VIP AM**: stores the first admin/superadmin information locally. If local directory is used, then data is stored locally User first/last name can be used as admin ID. **VIP EG**: (optional) helpdesk/admin user management. The data subjects are anyone in a customer's AD, which CAN include the categories shown, email address can be used as user ID for validations
Location data (e.g. GPS, device/network locale)	Customer employees and contractors, clients and vendors	To develop risk analysis in the Intelligent Authentication feature (**VIP SDK** only)
Online identifiers and trackers (IP address, OS and browser information)	Customer employees and contractors	Device identification and access rule enforcement (**VIP AM**)
Network activity data (browsing activity and history, telemetry such as proxy, usage and session logs, traffic data, electronic communications metadata)	Customer employees and contractors, clients and vendors	Optional (per customer configuration): **VIP Access** for Mobile and **VIP SDK** can gather this if configured to do so, to be used for any purpose defined by the customer
Others	Customer employees and contractors	**VIP AM** can pull any type of end user attribute that is passed into it by a third-party identity provider and relay the information to any downstream service provider

The Product does not need and is not meant to collect or process any Special Categories of Personal Data.

Personal Data Retention Schedule

As the controller, the customer is solely responsible for defining and implementing the retention policies and periods applicable to Personal Data collected through the use of the product. The use of the product does not involve Symantec as a data processor.

For the duration of the contractual relationship with the Customer, Personal Data voluntarily transmitted by the customer to Symantec is retained as described in the applicable product description. After the expiry or termination of the contractual relationship, Personal Data is decommissioned except where its retention is required by applicable law, in which case Personal Data covered by such requirement will be further retained for the legally prescribed period.

3. Disclosure and International Transfer of Personal Data

Recipients of Personal Data

If necessary to execute customer instructions, Symantec will send Personal Data voluntarily transmitted by the customer to internal recipients (affiliated Symantec entities) and external recipients (third party sub-processors) if necessary for the facilitation or provision of the Product. The list of Symantec affiliated entities and their geographical locations are available on the Symantec Privacy - GDPR Portal.

Third-Party Sub-Processors

No third-party sub-processor is involved in delivering the Product.

International Transfers of Personal Data

As the controller, the customer is solely responsible for complying with any rules applicable to the international transfers of Personal Data that the customer collects by using the product. The use of the product does not involve Symantec as a data processor.

You are however advised that if necessary to execute customer instructions, Symantec and its affiliated entities will transfer Personal Data voluntarily transmitted by the Customer to locations outside of the European Economic Area, including to external recipients, on the basis of European Commission Decision C(2010)593 on Standard Contractual Clauses (processors), or of any alternate, legally permitted means.

4. Exercise Of Data Subject Rights

As the controller, the customer is solely responsible for complying with any rules applicable to the exercise of Data Subject Rights related to Personal Data that the customer collects by using the product. The use of the product does not involve Symantec as a data processor.

Moreover, pursuant to the applicable Data Processing Addendum if any, and to the extent possible taking into account the nature of the processing, Symantec will assist the Customer, insofar as this is feasible, with the fulfillment of the Customer’s obligation to respond to requests for exercising Data Subjects’ rights such as the rights of access, rectification, deletion and objection laid down in Chapter III of the EU General Data Protection Regulation (GDPR).

5. Information Security

Technical and Organizational Measures

For VIP EG, no Personal data is stored. It is merely forwarded to the service in the cloud over an SSL-protected channel. For VIPAM, local databases with ACLs and passwords are hashed. For VIP Access Mobile and SDK, device hygiene data is stored locally in device application sandbox and encrypted. It is Symantec’s and all of its affiliated entities’ commitment to implement, and contractually require all sub-processors to implement, appropriate technical and organizational measures to ensure an appropriate level of security, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk for the rights and freedoms of Data Subjects. Additional security documentation is available on the Symantec Customer Trust Portal.

This notice is the sole authoritative statement relating to the Personal Data processing activities associated with the use of this Product. It supersedes any prior Symantec communication or documentation relating thereto.