Forcepoint Secure SD-WAN Management of Personal Data

Guide

Forcepoint

Table of Content

Disclaimer

This document contains information regarding Forcepoint products and/or services. The information is Forcepoint's property. While every effort was made to ensure the content is up-to-date and accurate, the information provides AS IS, without any representation or warranty, express or implied, and is subject to change without notice. Any reference to future releases or functionality are forecasts and not intended to be commitments. Forcepoint assumes no liability for the use of this information.

General

Document Purpose
This document is designed to provide transparency and explanation regarding the management of personal data by the following Forcepoint products and services: Secure SD-WAN Engine, Secure SD-WAN Manager Console (SMC), Endpoint Context Agent (ECA), Forcepoint User ID Service (FUID) and VPN Client. This document aims to provide the necessary information for procurement and privacy assessment teams to make informed decisions regarding the previously mentioned Forcepoint product and services.

General Data Protection Regulation (GDPR)
The operation of Forcepoint products and services are designed to comply with privacy principles set forth in the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Consistent with GDPR's principles, Forcepoint customers are considered the sole data controller. Forcepoint is neither the data controller, not the data processor, with respect to customer data stored in Forcepoint Secure SD-WAN Engine, SMC, ECA, FUID and VPN Client products and services. Further information regarding GDPR is available at https://commission.europa.eu/law/law-topic/data-protection/reform_en.

Forcepoint Insider Threat is designed to comply with applicable data privacy principles, including those contained in GDPR. Consistent with these principles, Forcepoint's customers are considered to be the sole data controller.

Personal Data
This document adheres to the definition of personal data as defined in article 4.1 of the General Data Protection Regulation, which defines 'personal data' as any information relating to an identified or identifiable natural person ('Data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Safeguarding Personal Data
Forcepoint uses industry-standard techniques to protect data held within the Forcepoint product, including personal data. This approach to data security helps ensure that high-risk is unintelligible to any person who is not authorized to access it. Full details on Forcepoint's privacy policy and processes can be found at https://www.forcepoint.com/legal/forcepoint-trust-hub.

Identity and Policy

Data Set	What Person Data is Use?	Purpose	Data Status	Storage, Flow & Protection	Retention
Administrator Accounts	During the installation of the SMC, a super account is created. This account is utilized to create administrator accounts once the installation is finalized. If customers choose to implement certificate authentication, a subject identifier, such as an email address is used to uniquely identify the administrator.	Administrators with varying access level can carry out tasks within the SMC based on the specific roles assigned to them.	The data is pseudonymized.	The SMC generates SHA-512 hashes of the administrator usernames and passwords which are stored in the Management Server database. Customers manage these passwords themselves within their internal network or public cloud environment outside of Forcepoint. If RADIUS/TACACS+ or LDAP is used as an authentication method, the administrator's username and encrypted password are sent to the Authentication Server. In case of SAML/OpenID Connect method, only the administrator's username is sent to the Identity Provider Service.	Customers can manually delete administrator accounts.
Internal LDAP Under Database	The internal LDAP user database within the SMC contains usernames and hashes of user passwords. If customers choose to implement a certificate authentication, a subject identifier, such as an email address is used to uniquely identify the administrator.	User accounts can be used for authentication and network access control.	The data is not pseudonymized.	The usernames and SHA hashes of user passwords are stored in the internal LDAP user database within the Management Server. They can be replicated to the Secure SD-WAN Engines over an industry standard TLS-protected connection. The customer can access the data using an account that allows access to the operating system. If RADIUS/TACACS+ or LDAP is used as an authentication method, then admin username and encrypted password is sent to the Authentication Server.	The user accounts can be deleted by the customer admins. By deleting the user in the customer's LDAP system, then resyncing the updated customer LDAP database with the SMC LDAP user database.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	The customer-assigned SMC superuser administrator can access and manage (add/modify/delete) both the administrator and user account data. The database is stored within the SMC server configuration.
SAR – Correction/Rectification	The SMC superuser administrator can access and manage (add/modify/delete) the data for both administrator and user accounts in the SMC user accounts database, which is stored within the configuration of the SMC server.
SAR – Right to be Forgotten	The superuser administrator has the ability to delete both administrator and user accounts from the SMC user accounts database, which is stored in the configuration of the SMC server. All actions performed by the administrators are logged and stored in the audit logs. The audit logs can be deleted by removing the log files from the OS file system. However, selective deletion or modification of the audit logs is not supported.
Data Storage/Localization	In the Secure SD-WAN Engine and SMC, the user and administrator account data are stored on servers that are managed by the customer themselves.

Active Logging

Data Set	What Person Data is Use?	Purpose	Data Status	Storage, Flow & Protection	Retention
Log Server Storage (Includes access, inspection and alert logs and counter data)	By default, no personal data is logged in access logs. However, customers can configure Secure SD-WAN Engines to log access data that - may include information about IP addresses, URLs, usernames, and applications. The data - may be used for various purposes such as collecting statistics. For details, see TABLE 1: Personal Data Attributes for Access Logs in the SMC in Appendix A.	To monitor network traffic and create reports.	The data is not pseudonymized	Access logs are stored on the Log Server disks in a proprietary format. The data is received from Secure SD-WAN Engines over an industry standard TLS-protected connection. When integration with Elasticsearch is configured, the SMC can delegate indexing of SMC logs to a customer managed local ElasticSearch database instance. This allows customers to benefit from faster log queries and transparent statistical reports through the SMC user interface. Customers can access the data using an account that allows access to the Secure SD-WAN Engine operating system.	Customer can remove or archive access log data either manually, or automatically, by utilizing the SMC and/or SMC scheduled task functionality

Audit Logs	Audit logs include administrator account names and the IP addresses of client's workstations. For details, see TABLE 2: Personal Data Attributes for Audit Logs in the SMC in Appendix A.	To audit administrators actions	The data is not pseudonymized.	Audit logs are stored on the Management Server and Log Server disks in a proprietary format. The data is received from Secure SD-WAN Engines over a TLS-protected connection. Customers can access the data using an account that allows access to the operating system.	Customers can use the SMC to remove or archive audit log data either manually utilizing the SMC and/or automatically with SMC scheduled task functionality
Schedule Reports	Reports are used to present statistics from log data, which may include personal data depending upon the customer's log configuration.	To create reports about network traffic, events, and/or to meet customer's reporting needs.	The data is not pseudonymized.	Reports are stored on the Management Server disks in a proprietary format. Customers can access the data using an account that allows access to the operating system or to the management interfaces of the SMC.	Customers can define report expiration time in report designs. The default report expiration time is 10 days.

How to Manage Subject Access Request (SAR)

SAR - Right to Access	Secure SD-WAN administrators can access and manage SMC log and report data through the SMC Management user interface or API.
SAR – Correction/Rectification	Secure SD-WAN Engine and SMC does not allow editing (correction/rectification) of the stored log data for security and auditing purposes.
SAR – Right to be Forgotten	Secure SD-WAN Engine and SMC superuser administrator can filter and delete selected logs based on a specific user identity (e.g., username, user account ID). All actions performed by the administrators are logged and stored in the audit logs. The audit logs can be deleted by removing the log files from the OS file system. However, selective deletion or modification of the audit logs is not supported.
Data Storage/Localization	Customers can choose and manage the location of their Secure SD-WAN Engine and SMC installation and data servers.

Add-on Modules

Data Set	What Person Data is Use?	Purpose	Data Status	Storage, Flow & Protection	Retention
Data Security (DLP)	Username and domain Source IP address Destination IP address File Hash Full File	Customers can allow scanning files transferred over Secure SD-WAN Engine against their internal/local DLP solution that supports ICAP integration to protect against data leaks.	The data is not pseudonymized.	Data Security events are recorded in the regular Secure SD-WAN logs under file filtering facility and the content depends on which DLP solution is used. The Secure SD-WAN supports ICAPS for encrypting ICAP connections with TLS.	Customers can remove or archive access log data either manually, or automatically, by utilizing the SMC and/or SMC scheduled task functionality.
Endpoint Integration (ECA)	The data in the ECA debug dump logged on to the endpoints includes username and user domain, as well as basic information about OS, CPU type, RAM, disk space, and installed applications.	To resolve technical issues for the customers.	The data is not pseudonymized.	ECA keeps latest debug dump logs under the ECA installation folder locally. Technical support may ask for these files for troubleshooting if there is an open issue.	The Maximum amount of log data to retain is fixed to 10 MB, ECA retains up to five 2 MB files in rotation. When the limit is reached, the oldest debug dump log file is discarded.
Sandbox (AMD/AMDP)	Secure SD-WAN Engine can send files for external local or cloud-based sandbox services. The customer's administrator can configure which file types are submitted to sandbox service.	Sandbox services can analyze the behavior of files by detonating the file's content in an isolated virtual environment to detect advanced threats.	The data is not pseudonymized.	Sandbox service stores the result of the malware analysis with SHA-256 hash of the file. If there were no threats detected, the submitted files are discarded upon completion of the analysis, which can take up to 5 minutes, depending on the size and type of the file being analyzed. Forcepoint sandbox services are located in Europe and North America. Customers can select which data center to use for sandbox service, In the case of a local sandbox, customers manage the location of the service by themselves. Sandbox connections are TLS encrypted.	Sandbox retains the analysis results of the file HASH. The original file is deleted after 40 days. Furthermore, if any malware code is found during analysis, the malware code (malware artefact) is kept indefinitely.

Data Set	What Person Data is Use?	Purpose	Data Status	Storage, Flow & Protection	Retention
User Identification Service (FUID)	User and IP address pairs. For details, see TABLE 3: Personal Data Attributes for the Forcepoint User ID Service in Appendix A.	To resolve associations between user IP addresses and user groups.	The data is not pseudonymized.	The data is stored in clear text in an internal database. Customers have the option to encrypt the database with an encryption of their choosing. The database contains a subset of user-specific Active Directory attributes such as username, email address, group memberships, and the current IP address. Access to the data requires an account that allows access to the operating system. The UID Service API allows unauthenticated queries for this data from the network. The operating system firewall can be used to control network access to the API.	User and IP address pair data is stored for 6 hours. To remove data, the customer may uninstall the Forcepoint User ID Service.
VPN Client for Windows	VPN Client log data contains the users' email addresses if a certificate that contains the email addresses is used as an authentication method in VPNs.	The logs collected locally by the VPN endpoint software have records of VPN connections between the VPN client workstation and Secure SD-WAN engine. These logs may be used for diagnostics as part of technical support process.	The data is not pseudonymized.	VPN Client log data is stored as plain text files under the VPN Client data folder (by default, C:\ProgramData\Forcepoint\Stonesoft VPN Client\log or C:\ProgramData\Forcepoint\VPN Client\log).	The data in the VPN Client log data files is automatically overwritten when new log data is created. To remove the data, uninstall the VPN Client for Windows, then manually remove the files from the VPN Client data folder.
TreatSeeker	FQDN and path parts from the original URL that is accessed through the Secure SD-WAN Engine.	Secure SD-WAN Engines rely on Forcepoint ThreatSeeker- an external cloud API service - for resolving URL categories from the web request URL.	The data is not pseudonymized.	URL and URL categories can be included in the regular Secure SD-WAN access logs.	The customer can remove or archive access log data either manually, or automatically, by utilizing the SMC and/or SMC scheduled task functionality.

The following products can be integrated with or used with Secure SD-WAN do not store personal data locally:

- Forcepoint VPN Client for Android
- Forcepoint VPN Client for Mac

How to Manage Subject Access Request (SAR)

SAR - Right to Access	**Sandbox:** Secure SD-WAN customers can access their sandbox reports via the “Scan report” links in the file filtering logs. Forcepoint Sandbox Management of Personal Data should be referenced to provide additional service specific data protection and reporting details. **User ID service:** The user data in the Forcepoint User ID (FUID) service is imported directly from the Microsoft Active Directory (AD) that was configured by the Secure SD-WAN customer. The FUID user data can be accessed and managed (accessed/modified/deleted) via the FUID server root account and the customer’s Microsoft AD management tools.
SAR – Correction/Rectification	FUID holds the user data that was imported directly from the customer Microsoft Active Directory (AD) system as it appears in Microsoft AD. Corrections to user data must be made in Microsoft AD and synchronized with FUID by waiting for the periodic sync with Microsoft AD or restarting the services manually for immediate updating of the user data. Forcepoint Sandbox Management of Personal Data should be referenced to provide additional service specific data protection and reporting details.
SAR – Right to be Forgotten	Uninstalling the FUID services will automatically delete all user data. Forcepoint Sandbox Management of Personal Data should be referenced to provide additional service specific data protection and reporting details.
Data Storage/Localization	Secure SD-WAN customer chooses and manages the location of their FUID installation and data server. Forcepoint Sandbox Management of Personal Data should be referenced to provide additional service specific data protection and reporting details.

Appendix A: Terminology

Term	Explanation
Secure SD-WAN	Secure SD-WAN includes Secure SD-WAN Engines, Secure SD-WAN Manager server components for management, logs, and user interface functionality.
Secure SD-WAN Manager Console (SMC)	The SMC is the management component of the Secure SD-WAN solution. The SMC manages and controls the other components in the system.
Management Server	The Management Server is the central component for system administration.
Log Server	Log Servers store traffic logs that can be managed and compiled into reports. Log Servers also correlate events, monitor the status of Secure SD-WAN Engines, show real-time statistics, and forward logs to third-party devices.
Secure SD-WAN Engines (Secure SD-WAN Engines)	Secure SD-WAN Engines inspect traffic. They are used to configure access control to resources and to monitor user and administrator actions. Secure SD-WAN Engines in the Firewall/VPN role can also be used as VPN gateways.
Advanced Malware Detection (AMD)	Forcepoint AMD detects advanced threats by analyzing the behavior of files. Secure SD-WAN Engines can be configured to send files to AMD for analysis.
Endpoint Context Agent (ECA)	ECA collects per-connection user and application information about Windows endpoint clients. You can integrate ECA with Forcepoint Secure SD-WAN to receive user and application information about Windows endpoint clients that connect through a Secure SD-WAN Engine managed by the SMC. You can use the information as criteria for access control and monitoring and to create reports.
Forcepoint User ID Service (FUID)	The Forcepoint User ID Service collects information about users, groups, and IP addresses from Windows Active Directory (AD) servers and Microsoft Exchange Servers. You can integrate the Forcepoint User ID Service with the Forcepoint Secure SD-WAN and use the information that the Forcepoint User ID Service provides in monitoring users and configuring access control.

Personal Data Attributes

Table 1: Personal Data Attributes for Access Logs in the SMC

Person data in this data set cannot be anonymised as this would contravene security best practices by muting the network access and inspection incident audit trails, however collecting these logs are optional.

Attribute	Requirement
IP address	Optional
User logon name and domain	Optional

Table 2: Personal Data Attributes for Audit Logs in the SMC

Personal data in this data set cannot be anonymized as this would prevent correct operation of the security policy. Audit logs cannot be disabled; however they can be deleted via SMC scheduled log management tasks or by removing the audit log data from the disk.

Attribute	Requirement
Admin logon name	Mandatory
Admin client IP address	Mandatory

Table 3: Personal Data Attributes for the User ID Service

Personal data in this data set is mirrored from configured Microsoft Active Directory environment and automatically removed when removed from the AD. Personal data in this data set cannot be anonymized as this would contravene security best practices by preventing the matching of users in the network access policy. Uninstalling FUID server will also remove all cached data in FUID installation.

Attribute
User logon name and domain
User AD group membership
User IP address (as seen by AD Domain Controller)
User email address

Forcepoint

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[FP-SD-WAN Management of Personal Data Guide] 09 Oct. 23