# Next-Generation Firewall Management of Personal Data

Forcepoint

# Table of Contents

# General Information

## Document Purpose

This document is designed to provide transparency and explanation regarding the management of personal data by the following Forcepoint products and services: Next-Generation Firewall (NGFW), Security Management Center (SMC), Endpoint Context Agent (ECA), User ID Service 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 products and services.

## General Data Protection Regulation (GDPR)

The operation of Forcepoint products and services are designed to comply with the 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 NGFW, SMC, ECA, User ID Service and VPN Client products and services. Further information regarding GDPR is available at https://ec.europa.eu/info/law/law-topic/data-protection/reform_en.

## Personal Data

This document applies the definition of personal data found in article 4.1 of the GDPR, 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, by reference to an identifier such as, but not limited to, a name, an identification number, location data, an online identifier or other 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 Forcepoint products, including personal data. This approach to data security helps to ensure that the high-risk data 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/forcepoint-privacy-hub.

### 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 is provided *as is*, without any representation or warranty, express or implied, and is subject to change without notice.

Any references to future releases or functionality are forecasts and not intended to be commitments. Forcepoint assumes no liability for the use of this information.

## Identity & Policy

| Data Set | What Personal Data is Used? | Purpose | Data Status | Storage, Flow & Protection | Retention |
|---|---|---|---|---|---|
| **Administrator accounts** | A superuser account is created during the installation of the SMC. This account is used to create administrator accounts after the installation.<br><br>If customers elect to employ certificate authentication, a subject identifier such as an email address is used to identify the administrators. | Administrators who have different access levels can perform tasks in the SMC according to the administrator roles assigned to them. | The data is not pseudonymized | The usernames and SMC generated SHA-512 hashes of the administrator passwords are stored in the Management Server database, which customers maintain either in their on-premise/internal network installation of the product or their own cloud tenant/solution outside of Forcepoint. | The customer can delete administrator accounts manually. |
| **Internal LDAP user database** | The internal LDAP user database in the SMC contains usernames and hashes of user passwords.<br><br>If certificate authentication is used, a subject identifier such as an email address is used to identify the users. | User accounts can be used for authentication and network access control. | The data is not pseudonymized | The usernames and AES hashes of the user passwords are stored in the internal LDAP user database on the Management Server. They can be replicated to the NGFW Engines over an industry standard TLS-protected connection. The customer can access the data using an account that allows access to the operating system. | The customer can delete user accounts manually. |

## How to Manage Subject Access Request (SAR)

| | |
|---|---|
| **SAR - Right to Access** | Customer assigned SMC superuser administrator can access and manage (add/modify/delete) the administrator and user account data in the SMC user accounts database that is stored in the SMC server configuration. |
| **SAR - Correction/Rectification** | SMC superuser administrator can access and manage (add/modify/delete) the administrator and user account data in the SMC user accounts database that is stored in the SMC server configuration. |
| **SAR - Right to be Forgotten** | Superuser administrator can delete administrator & user account data in the SMC user accounts database that is stored in the SMC server configuration.<br>All SMC administrators' actions are collected and stored in audit logs that cannot be filtered or deleted based on a specific administrator account. |
| **Data Storage / Localization** | NGFW and SMC user and administrator account data is stored on the customer's managed servers. |

## Activity Logging

| Data Set | What Personal Data is Used? | 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 NGFW Engines to log access data that can include information about IP addresses, URLs, usernames, and applications. The data can 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 NGFW 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 the customer to benefit from faster log queries and transparent statistical reports through the SMC user interface. The customer can access the data using an account that allows access to the NGFW operating system. | The customer can remove or archive access monitoring activity 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 the client workstations. For details, see TABLE 2: Personal Data Attributes for Audit Logs in the SMC in Appendix A. | To audit administrator 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 NGFW Engines over a TLS-protected connection. The customer can access the data using an account that allows access to the operating system. | The customer can use the SMC to remove or archive audit log data either manually utilizing the SMC and/or automatically with SMC scheduled task functionality. |
| **Scheduled 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 reporting needs | The data is not pseudonymized | Reports are stored on the Management Server disks in a proprietary format. The customer can access the data using an account that allows access to the operating system or to the management interfaces of the SMC. | The customer can define report expiration time in report designs. The default report expiration time is 10 days. |
| **ECA debug dump logs on Windows endpoints** | The data in the ECA debug dump logs includes the users currently logged on to the endpoint and their domains, as well as some basic information such as the operating system, CPU type, free and total physical memory, free and total disk space, and installed applications. | To resolve technical issues for the customers. | The data is not pseudonymized | Customers should store debug dump logs under the ECA installation folder. | Debug dump log data is stored in 2 MB files. As the maximum amount of log data that can be retained is 10 MB, the system can retain up to 5 2 MB files. When the maximum number of log files is reached the system rotates out the oldest to make room for more current log data files |

## How to Manage Subject Access Request (SAR)

| | |
|---|---|
| **SAR - Right to Access** | NGFW administrators can access and manage SMC log and report data through the SMC Management – API. |
| **SAR - Correction/Rectification** | NGFW and SMC are designed to prevent any editing (correction/rectification) of the stored log data for security and auditing purposes. |
| **SAR - Right to be Forgotten** | NGFW and SMC superuser administrator can filter and delete selected logs based on a specific user identity (e.g., username, user account ID). All SMC administrators' actions are collected and stored in audit logs that cannot be filtered or deleted based on a specific administrator account. |
| **Data Storage / Localization** | NGFW customer chooses and manages the location of their NGFW and SMC installation and data servers. |

## Add-On Modules

| Data Set | What Personal Data is Used? | Purpose | Data Status | Storage, Flow & Protection | Retention |
|---|---|---|---|---|---|
| **Advanced Malware Detection (AMD)** | AMD receives files, which are to be analyzed for malware, from the NGFW product. Upon receiving the file, AMD conducts analysis of the file to determine whether malware is contained in the file. Files uploaded to be analyzed by AMD may potentially contain personal data. The customer administrator is able to configure which file types are submitted to AMD. | To understand if the entire submitted file presents a malware risk. | The results of the files are anonymized by generating a SHA-1 hash of the submitted file and associating the result of the analysis with the file hash. Upon completion of the analysis, the file and any of its contents are then immediately deleted. | Advanced Malware Detection stores the result of the malware analysis which is tied to the file hash generated by AMD. The submitted file is immediately deleted upon completion of the analysis. Analysis can take between 10 seconds to 5 minutes, depending on the size and type of the file being analyzed. The file is submitted to AMD via an industry standard TLS encrypted channel. The analysis capability of AMD is outsourced. Analysis takes place in two data centers, located in Los Angeles, United States and Amsterdam, Netherlands. Customers select the data center they use or can select "Automatic" which will configure the geographically closest data center to the NGFW public IP address that is making the DNS resolver request. | Advanced Malware Detection does not retain the submitted file. AMD retains the analysis results of a file indefinitely. Furthermore, if any malware code is found during analysis, the malware code (malware artefact) is kept indefinitely. |
| **User ID Service** | 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. | Logs customer VPN use through NGFW and can also be used to resolve technical issues for the customers. | 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. |

The following products that can be integrated with or used with Next-Generation Firewall 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** | AMD: NGFW customers can access their sandbox reports from the customer AMD portal account and the “Scan report” links in the file filtering logs. Forcepoint AMD product support documents should be referenced to provide additional AMD specific data protection and reporting details.<br><br>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 NGFW customer. The FUID user data can be accessed and managed (accessed/modified/deleted) via the NGFW – FUID administrator 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 its appears in Microsoft AD. Corrections to user data must be made in Microsoft AD and re-imported into FUID. |
| **SAR - Right to be Forgotten** | Uninstalling the FUID services will automatically delete all user data. |
| **Data Storage / Localization** | NGFW customer chooses and manages the location of their FUID installation and data server. |

# Appendix A

## Terminology

| Term | Explanation |
|---|---|
| **Next-Generation Firewall (NGFW)** | Next-Generation Firewall solution includes Next-Generation Firewall Engines, SMC server components, and SMC user interface components. |
| **Security Management Center (SMC)** | The SMC is the management component of the Next-Generation Firewall 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 NGFW Engines, show real-time statistics, and forward logs to third-party devices. |
| **Next-Generation Firewall Engines (NGFW Engines)** | Next-Generation Firewall Engines inspect traffic. They are used to configure access control to resources and to monitor user and administrator actions. Next-Generation Firewall 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. NGFW 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 NGFW to receive user and application information about Windows endpoint clients that connect through an NGFW 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 NGFW 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

Personal data in this data set cannot be anonymized 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 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 remove also all cached data in FUID installation.

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