Hewlett Packard Enterprise

Secure Analytics in the Cloud for HPE 3PAR StoreServ and HPE StoreOnce devices

HPE StoreFront Remote

Contents

Technical white paper

Executive summary

StoreFront Remote (SFRM) is a Web portal that offers system health and other analytics in the cloud for your HPE 3PAR StoreServ and HPE StoreOnce devices, in a secure and seamless manner. SFRM also enables proactive services to be delivered by Hewlett Packard Enterprise to its customers. Customers can control the visibility of their devices in SFRM with an opt-in registration mechanism, and through administration privileges. The SFRM service is built on HPE's Secure Service Architecture (SSA) which provides a secure communication path to send diagnostic and performance telemetry data from customers' storage devices to HPE 3PAR Central Platform, which sits in a secure data center behind an HPE firewall.

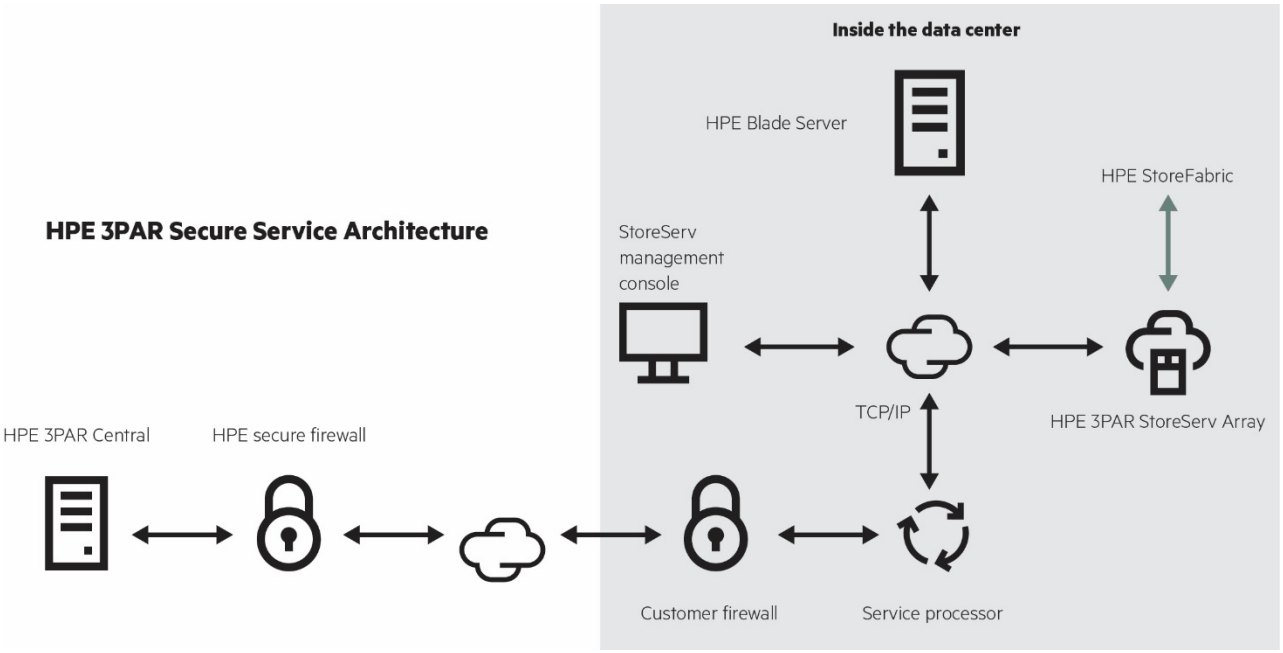


Figure 1. HPE 3PAR Secure Service Architecture

SFRM requires two things—an active connection from a storage device to HPE 3PAR Central and customers' approval to make the data available in the cloud through an explicit registration step. The data that is thus sent to Hewlett Packard Enterprise, hereby referred to as the "call home" telemetry data set, is always securely transmitted using the HTTPS protocol and this data forms the basis of the analytics and recommendations in SFRM. It's important to note that by "telemetry data", we refer only to the "system-support data" from the storage devices and not the actual "customer data" from the customers' storage devices. The telemetry data sent to Hewlett Packard Enterprise is mandatory to facilitate remote technical support and other Proactive Services but it's not mandatory for customers to sign up for SFRM, which is an opt-in based service. End-user data from a customers' storage devices is never collected or transmitted outside their data center, and additional care is taken in SFRM to protect all personally identifiable information (PII) as well.

StoreFront Remote Architecture

SFRM is a secure Web service hosted by Hewlett Packard Enterprise, illustrated below, which can be broken down into several components:

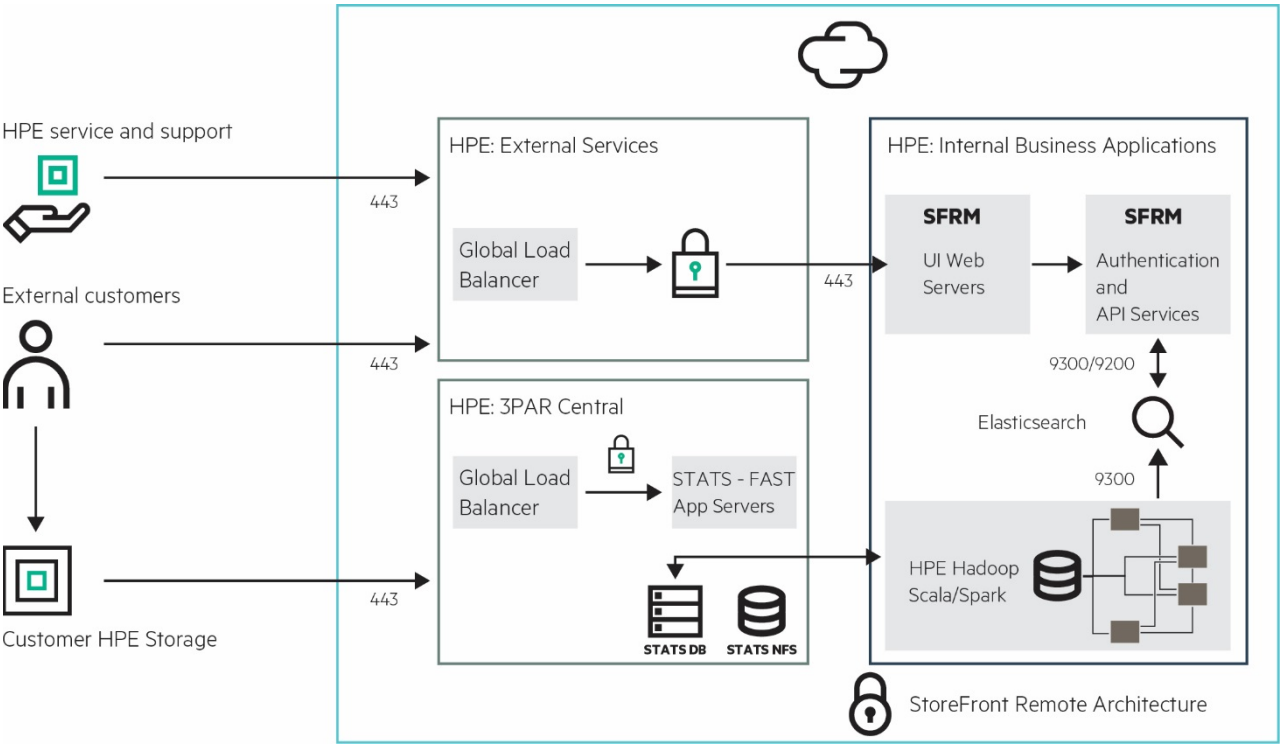


Figure 2. StoreFront Remote Architecture

- **Secure Transport Layer**—connects both internal and external users to HPE-owned and managed services
- **HPE External Services**—allows load balancing SFRM sessions for both performance and high availability; additionally, these services also provide a secure passage through the HPE firewall
- **SFRM Authentication Service**—uses both HPE Passport for User Authentication and HPE's corporate LDAP Services
- **SFRM Web UI Service**—a set of load-balanced HPE servers over multiple data centers that serve up the SFRM Web Portal
- **SFRM API Service**—the gateway to all storage data; requires authenticated users and enforces both role based access and authorization to specific devices
- **Data layer**—consists of a traditional "Big Data" lake hosted on Hadoop, fronted by Elasticsearch, which is designed for high-speed access from the API layer

The Secure Transport Layer

All communications to SFRM are facilitated using Hypertext Transfer Protocol Secure (HTTPS) over TLS 1.2—used by the world's leading financial institutions and Web commerce applications. This ensures all communications to Hewlett Packard Enterprise are protected from malicious hackers. The TLS 1.2 protocol uses public key cryptography and mutual client and server authentication to provide confidentiality, message integrity, and authentication for traffic passed over the Web.

As part of the secure protocol, TLS certificates for SFRM are signed by a trusted third-party Certificate Authority (CA), GeoTrust. The CA is a trusted entity, which validates the authenticity of SFRM utilizing a digital certificate. The certificate includes HPE's public key used for encrypted communications to SFRM as well as other information about Hewlett Packard Enterprise. Standard technology in your browser maintains a list of CA root certificates to verify that a known and trusted CA has signed and validated the digital certificate.

HPE External Services

"External services" is the only layer that sits outside the HPE firewall. All connections to and from the External Compartment are encrypted over HTTPS. An initial request to SFRM is always re-directed to SFRM Authentication Service. Once authenticated, a browser connection will embed cookies to encode both a login session ID as well as ensure that all sessions are directed to the same internal Web server if possible.

SFRM Authentication Services

SFRM utilizes different methods to authenticate a user depending on whether they are an internal HPE user, a customer or a partner. Customers and partners require an HPE Passport account to access SFRM which uses HPE Passport Authentication Service. SFRM also supports internal users and authenticates them using the Corporate LDAP Services.

For customers and partners, HPE Passport authentication gives the user only the rights to login to the SFRM portal but doesn't give authorization to view any devices, which requires a separate registration step. As part of the authentication step, SFRM will associate either a customer or partner role. The user role will determine the type of data accessible within SFRM, personably identifiable Information (PII) is visible only to the customer role. Ultimately, the customer who creates system groups and registers devices with that group is considered the group "owner." System group owners can extend access to other HPE Passport owners from within SFRM.

SFRM is also accessible to HPE personnel who are authenticated using Corporate LDAP services. Access is limited to a subset of employees who are part of Technical Services (TS) Support, Engineering Quality/Dev Team, and the Storage Sales/Pre-Sales team. Internal access is granted only upon written request, and must accompanied by a written approval from the applicant's manager. Internal users do not need to require invitations from a customer to view storage devices in SFRM.

SFRM Web Service

The SFRM Web service is provided by a scalable number of Web servers across multiple data centers interconnected via a secure fabric and this supports the user interface of SFRM. This service was designed from the ground up as a secure interface to handle customers' metadata. All communications from the UI are targeted directly to the API service via a Structured Query Language (SQL). This is a non-text based query language, which is designed to eliminate security threats such as SQL injection.

SFRM API Service

The SFRM API provides an abstraction to the data layer. The API Service authenticates every query from a valid user session ID. From the session ID, the API service is able to encapsulate all user queries, to relate them with both role and system group information to provide secure access to the data layer. If no session ID exists, the request is redirected to the authentication service for validation and a session ID will then be established.

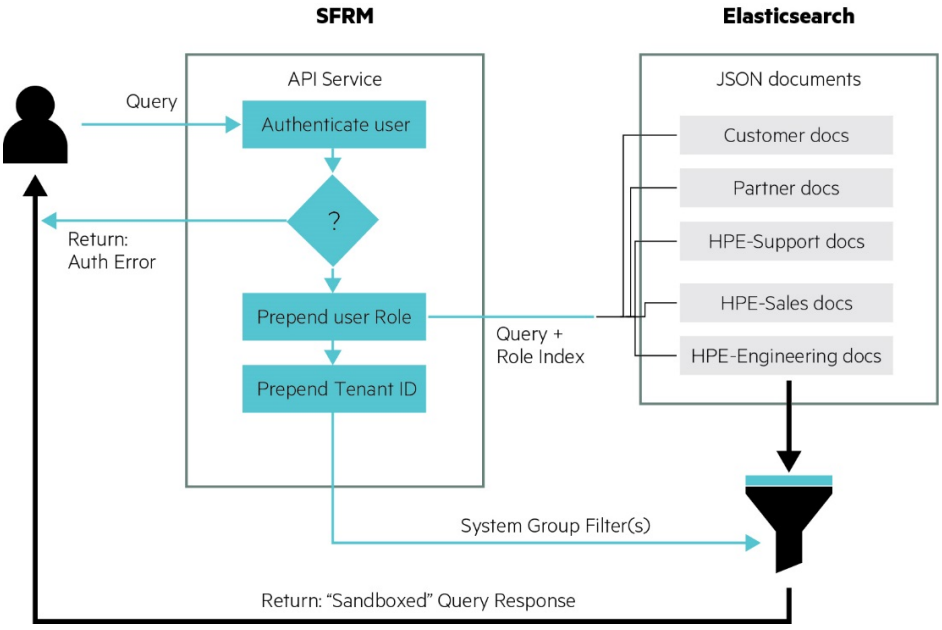


Figure 3. StoreFront Remote API Layered Architecture

Once a valid session ID is authenticated, the API Service will use the role index to direct its query to the appropriate role-based document set. Roles limit the type of information a user can see about the storage devices they are authorized to see, and eliminate things like Customer PII data from non-customer roles.

In addition to having a role, users can also belong to system groups. A new user is associated with a system group when they register devices, or if they are invited as a member to an existing system group. A system group is one or more storage devices associated with a unique SFRM token. When a user creates a system group, that user is considered the owner and can register devices, and invite other HPE Passport as members to view their system groups. With this mechanism, only a system group owner can register devices, and other users are authorized to see only the devices in the system groups they were invited to see.

SFRM data layer

The data layer is broken down into two components, Hadoop and Elasticsearch. Hadoop provides the infrastructure for both the processing needs and storage repository. The SFRM user connects to the data layer via the API and does not have direct access to this data. All API queries are serviced by a high-speed Elasticsearch (ES) database. Both the components sit securely within the HPE firewall.

Elasticsearch is a near-real–time search platform that provides low latency for indexing new objects and accessing these objects using powerful search and query semantics. In addition to maintaining a structured object for each storage device that calls home, ES is also used to store management objects for user preferences, and system groups. ES is exposed only through the SFRM API which enforces authentication, and limits user accessibility to data in the proper set of role-based documents and functions. The last step of any query response is the filtering of storage objects based on the system groups a user is authorized to see.

Secure device registration

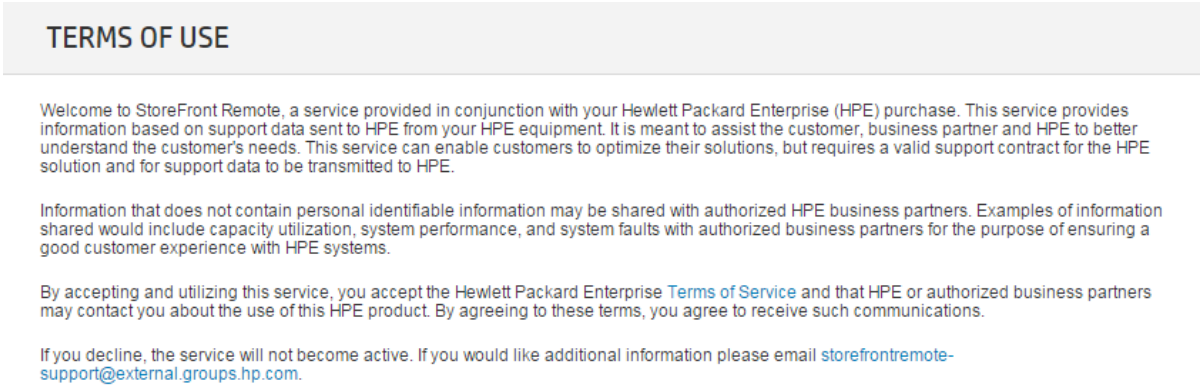
Storage devices are registered with SFRM by installing an SFRM token on the storage device itself and relying on that token to be reflected back in "call home" data set. A token is associated with a named system group and generated within the SFRM Web portal. Specific instructions are provided within SFRM on how to embed these tokens on all supported devices. Parsing the token in the call home data set allows a precise mapping for devices to system groups. SFRM maintains the list of users with privileges to access a storage group. With this mechanism, a customer has complete control over the visibility of their devices in SFRM.

Here are the summary of the requirements for device registration:

1. Install SFRM token on the storage device.
2. Connect the storage device to HPE 3PAR Central for Remote Support.
3. The storage device in question must be covered by a valid Extended Care contract. Customers under Hardware Warranty still have access to the benefits of HPE's remote support capabilities for break-fix events; however, they will not enjoy the benefits of SFRM.
4. The email address associated with the owner of the system must be validated as a pre-requisite for gaining access to SFRM for the first time. Validating email address will allow customers to subscribe to email notifications for interesting events within the SFRM portal and be ensured accurate delivery of this information.
5. The system group owner must have accepted the Terms-of-Use for General SFRM Access.
6. When creating an SFRM token, the User must accept the Terms-of-Use for SFRM Tokens

Terms of use for general SFRM access

A user is presented with a terms-of-use at first login or if the terms and conditions are modified. A record is kept of all users, and the version of the terms of use they have accepted. Below is the current terms-of-use that is presented in the SFRM portal.



TERMS OF USE

Welcome to StoreFront Remote, a service provided in conjunction with your Hewlett Packard Enterprise (HPE) purchase. This service provides information based on support data sent to HPE from your HPE equipment. It is meant to assist the customer, business partner and HPE to better understand the customer's needs. This service can enable customers to optimize their solutions, but requires a valid support contract for the HPE solution and for support data to be transmitted to HPE.

Information that does not contain personal identifiable information may be shared with authorized HPE business partners. Examples of information shared would include capacity utilization, system performance, and system faults with authorized business partners for the purpose of ensuring a good customer experience with HPE systems.

By accepting and utilizing this service, you accept the Hewlett Packard Enterprise Terms of Service and that HPE or authorized business partners may contact you about the use of this HPE product. By agreeing to these terms, you agree to receive such communications.

If you decline, the service will not become active. If you would like additional information please email storefrontremote-support@external.groups.hp.com.

Figure 4. StoreFront Remote General Terms of Use

By accepting the terms of use, the user is granted access to SFRM and all of its capabilities. In exchange for access to SFRM, the user grants Hewlett Packard Enterprise the right to provide information to a fully qualified HPE Partner without an explicit invitation from a customer to join a specific system group. A qualified HPE Partner is considered an extension of the HPE Sales and Support team. Before granting access to any storage device, HPE first ensures that a proper business relationship exists between the partner and the customer owning the device. Here are the requirements used to establish a partner/customer business relationship.

- The device is in fact registered in SFRM.
- The partner can provide the HPE Serial Number of each device they wish to access in SFRM.
- The partner can provide HPE Sales Order Number for each device they wish to access in SFRM.

Failure to accept the terms of use will result in the user being denied access to SFRM. As a customer, if you are concerned about the terms of use, please send a note to storefrontremote-support@external.groups.hp.com, or contact your HPE Sales Representative to engage in a more in-depth conversation. There may be special considerations to allow a customer to gain access to SFRM and still retain explicit control over who may view their systems.

Terms of use for SFRM tokens

Each customer system group is associated with a unique SFRM registration token that is installed on every storage device intended to be managed by that system group. An SFRM token is always of the format:

```
StoreFrontRemoteAccess[<tenant uuid>,<email>]
```

The tenant UUID is a unique identifier that is Base64 encoded and identifies a unique system group. The email address is provided for informational purposes. The tokens themselves are not encrypted; giving your token away would allow someone to attach their device to your system group, but will not allow them to see their device or other devices in that system group unless they receive a group invitation.

Each time a token is generated or presented in the portal there is an explicit terms of use associated with that token warning against improper use. Note: Installing a token on one of more of your storage devices that was created by someone other than your system administrator can result in that device being made visible by an unintended SFRM user.

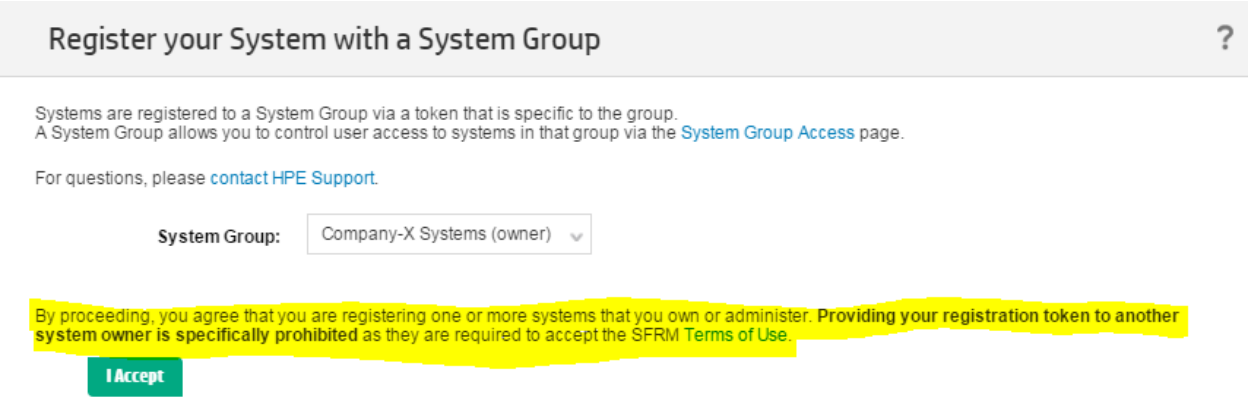


Figure 5. StoreFront Remote Token Terms of Use

If a customer has a trusted partner and wishes to share their devices with that partner then they should explicitly invite that partner to one or more of their system groups. They should not allow the partner to provide the SFRM token on their behalf. Doing so compromises their ability to properly administer access via a system group and relinquishes this right to the partner. If any customer detects an unexpected storage device in one of their system groups, they should contact storefrontremote-support@external.groups.hp.com and consider moving all storage devices to the new group.

Security—dynamic penetration testing

In addition to an architecture designed from the ground-up for secure access, the SFRM portal has undergone rigorous penetration testing prior to its first release using HPE's own WebInspect penetration tool. Each subsequent release is subjected to the same rigorous testing. WebInspect is an innovative dynamic application security test tool that mimics real-world hacking techniques and attacks and ensures that the Web portal is hardened against these attacks.

Terminology

CA: Certificate Authority

HPE: Hewlett Packard Enterprise

HTTPS: Hypertext Transfer Protocol Secure

SFRM: Storefront Remote

SSA: Secure Service Architecture

SSL: Secure Sockets Layer

STaTS: Service Tools and Technical Service

TLS: Transport Layer Security

Learn more at
storefrontremote.com

Sign up for updates

★ Rate this document

4AA6-3833ENW, April 2016