

---

# Additional License Authorizations

For Data Security (Voltage) software products

## Additional License Authorizations

For Data Security (Voltage) software products

## Products and Suites covered

Products	E-LTU or E-Media available*	Perpetual License Non-production software class**	Subscription License Non-production software class
SecureData Enterprise	Yes	Class 2 & 3 ***	Class 3
SecureData Enterprise Integrations to Cloud Services	Yes	Class 3	Class 3
SecureData Enterprise Data Warehouse	Yes	Class 3	Class 3
SecureData for Snowflake	Yes	Class 3	Class 3
SecureData Format-Preserving Encryption (FPE) for ArcSight Data Platform	Yes	Class 3	Class 3
SecureData Mobile	Yes	Class 2 & 3 ***	Class 3
SecureData Payments	Yes	Class 2 & 3 ***	Class 3
SecureData Sentry	Yes	Class 3	Class 3
SecureData Transparent Data Protection for HPE NonStop	Yes	Class 3	Class 3
SecureData Web	Yes	Class 2 & 3 ***	Class 3
SecureFile	Yes	Class 3	Class 3
SecureMail	Yes	Class 3	Class 3
SmartCipher	Yes	Class 3	Class 3
Basic Package	Yes	N/A	Class 3
Standard Package	Yes	N/A	Class 3
Premium Package	Yes	N/A	Class 3

Suites	E-LTU or E-Media available*	Perpetual License Non-production software class**	Subscription License Non-production software class
SecureData Enterprise Data Warehouse Starter Edition	Yes	Class 3	Class 3
SecureData Enterprise Data Warehouse Enterprise Edition	Yes	Class 3	Class 3
SecureData Enterprise Infrastructure Suite 1 – Production and Test and Development	Yes	Class 2	Class 3
SecureData Enterprise Infrastructure Suite 1 – Disaster Recovery	Yes	Class 2	Class 3
SecureData Enterprise Infrastructure Suite 2 – Production and Test and Development	Yes	Class 2	Class 3
SecureData Enterprise Infrastructure Suite 2 – Disaster Recovery	Yes	Class 2	Class 3
SecureData Suite for Hadoop Starter Edition	Yes	Class 3	Class 3
SecureData Suite for Hadoop Enterprise Edition	Yes	Class 3	Class 3
SecureData Suite for Open Systems Suite Standard Edition – Test and Development	Yes	Class 2	Class 3
SecureData Suite for Open Systems Suite Enterprise Edition – Test and Development	Yes	Class 2	Class 3

\* Any product sold as E-LTU or E-Media shall be delivered electronically regardless of any contrary designation in a purchase order.

\*\* Non-production use rights, if any, can be found at [software.microfocus.com/legal/software-licensing](https://software.microfocus.com/legal/software-licensing).

\*\*\* Specific parts of this product offering have Non-Production licenses for Development and Test and for Disaster Recovery purposes, those are Class 2; all other parts of this product offering are Class 3.

**Note: SecureData for Vertica is licensed as a Vertica product. Refer to the Vertica Additional License Authorizations document or equivalent for further information.**

## Additional License Authorizations

For Data Security (Voltage) software products

# Definitions

Capitalized terms not otherwise defined in this ALA document are defined in the governing agreement.

Term	Definition
Acquirer	Means when referring to a payment processor entity, an organization that facilitates electronic payment authorization and/or settlement for payment transactions and related services.
Application	Means a single module or service, or a collection of integrated software modules or services, or a distinct process designed to perform a specific single Organization Function. For SecureData, in particular, the Organization Function must include the transacting, processing, or storing of protected data. Any Application that uses SecureData or SecureMail indirectly, such as via a service, microservice or proxy, must be licensed as a separate Application.
Application, External	Means, for SecureData Sentry, an Application that a customer does not own but uses through a subscription or term license (e.g., a SaaS application, such as Salesforce).
Application, Internal	Means, for SecureData Sentry, an Application that a customer owns, such as through self-development or from a perpetual use license. This may include COTS applications.
Basic Package	Means SecureData Enterprise products and suites. Doesn't include SecureData Payments and SecureData Sentry products and suites.
Ciphertext	Means the result of protecting Plaintext through encryption, hashing, or tokenization.
Cold Standby System	Means a secondary standby non-production system that is not handling any transactions or being otherwise used, and is also NOT up and running. If the primary production system breaks down, or needs to be taken out of service, the Cold Standby System will be started to take over for the primary production system.
Connector	Means a connection that provides point- to- point transmission of Transaction data from point of capture to its point of destination, counted by number of unique capture points. For example, a connection from a card reading terminal at a POS transmitting encrypted payment card data to a server host system, or transmitting tokenized data in the reverse direction to a unique destination.
Core	Means a discrete package of an arithmetic-logic unit, instruction unit, and registers that are autonomously able to address random access memory and execute a software program.
COTS	Means Commercial-Off-The-Shelf software.
CPU	Means a system in a single integrated circuit (IC) package with at least one Core, but usually more. For example, the Intel Core i7 5960X CPU is an IC package of eight cores.
Database	Means a container that stores application data including table structure, stored procedures, and other functionality that runs on a Database Instance.
Database Instance	Means a software application that has the sole purpose of acting as a container that hosts and executes one of more Databases.
Data Center	Means a single, physical collection of networked computer systems with a defined geographic location. For public cloud services providers, a Data Center is an Availability Zone. Availability Zones (AZ) are unique physical locations within Cloud Service Provider Region. Each AZ is made up of one or more datacenters equipped with independent power, cooling, and networking.
Data Masking	Means obfuscating data using FPE or SST to protect sensitive data such as payment card numbers, national identification numbers, and so on. Masked data can be used within test, development, analytics, or production environments.
Developed Code	Means the software and scripts developed and/or deployed by licensee using Voltage products.
Development System	Means a non-production development system that has a software product installed and is to be used for developing software product add-on applications.
Device	Means an addressable entity, physical or virtual, including but not limited to router, switch, bridge, hub, server, PC, laptop, handheld device, or printer that resides within the range defined for interrogation and asset tracking.
Digest	See Hash.

## Additional License Authorizations

For Data Security (Voltage) software products

Term	Definition
Disaster Recovery (DR) System	Means a Cold- Standby System or Hot- Standby System.
Driver Interception	Means, for SecureData Sentry, the interception of an Application's database API calls (e.g., over JDBC or ODBC) by a Sentry driver wrapper.
E-Commerce	Means the encryption of digital transactions from payment capture points (e.g., desktop browser, mobile browser, mobile app on consumer-owned COTS) to processing hosts at a Merchant, Processor, Acquirer, Gateway or ISO.
Encryption	Means a key-based, cryptographic transformation of sensitive data into a non-sensitive de-identified form (ciphertext).
Endpoint	Means a device or system that a user interacts with.
External Application	See Application, External.
External User	Means a person who is not a contractor or employee of the licensee.
Event	Means a single protection; access; field discovery and classification; test data record creation; data record archival; or record deletion operation.
Format-Preserving Encryption	Means an encryption algorithm that produces output of the same size and format as the input. For example, if the input comprises all digits, the output will also consist of digits. Voltage SecureData offers various forms of Format-Preserving Encryption.
Format-Preserving Hash	Means a hash algorithm that produces output of the same size and format as the input. For example, if the input comprises all digits, the output will also consist of digits. The Voltage SecureData Format-Preserving Hash uses a key, increasing security.
Gateway	Means an intermediary organization or service that facilitates data exchange between merchants and processors and may provide additional value-added service offerings to facilitate merchant needs. Gateways can be independent organizations or associated directly with a processor.
Gigabytes (GB)	Means 10 <sup>9</sup> bytes, designating an amount of physical data capacity.
Hash	Means a Hash or Digest: a value of a fixed size created from a value of arbitrary size. Unlike encryption and tokenization, hashes are not reversible: they cannot be converted back to the original value. Hashes also imply collisions: it is possible (although, with modern hashing algorithms, non-trivial) to select two input values that produce the same hash.
Hashing	Means one-way generation of de-identified values using a mathematical function.
Hot Standby System	Means a secondary non-production system that is not handling any transactions but is up and running, ready to take over from the production system if the primary production system breaks down or needs to be taken out of service.
IFL	Means Integrated Facility for Linux, a Processor dedicated to Linux workloads on IBM Z systems.
Implementation	Means an installation of the software on a single Server, or installed on a cluster of Servers which work together as a single installation of the software.
Installation Kit	Means a collection of software products in ready-to-install form.
Instance	Means each implementation of the software installed on a either a Physical or a Virtual Server.
Internal Application	See Application, Internal.
Internal User	Means a person who is a contractor or employee of the licensee who has Use rights.
ISO	Means Independent Sales Organization in relation to payment facilitation companies that sell acquiring services on behalf of gateways and processors.
Key Server	Means an appliance configured to provide key management and key derivation services per configurable policies.
Lane	Means in retail environment a single payment terminal, either an electronic card reader or virtual terminal but not both, is connected to a single point of sale (cash register) to collect cardholder data for electronic payments (typically credit/debit card payment data).
Merchant	Means a payment-accepting business. Merchants may engage in either or /both of card-present physical or/and card-not-present transactions (eCommerce stores).

## Additional License Authorizations

For Data Security (Voltage) software products

Term	Definition
Messages	Means in relation to electronic statements, a unique message from a sending organization, application, or automated system to an Internal or External User.
Mobile	Means personal computing devices running some COTS operating system.
MSU (Millions of Service Units)	Means the IBM standard rating of computing work capacity.
Named Application	See Application.
Node	Means any computing Server where a datastore application software is running and where SecureData APIs are deployed, and/or where data protected by SecureData is stored, processed or used.
Organization Function	Means an activity carried out by an organization that yields income for the organization (a core organization function) or supports an activity that yields income for the organization (a support organization function).
PAN	Means, as defined by PCI Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS,) version 3.2: "Acronym for 'primary account number', also referred to as 'account number.' Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account."
PCI	Means Payment Card Industry, a global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide.
Per Protect Event	Means the Encryption, Hashing, or Tokenization of a single Plaintext value into a single element of Ciphertext. Where a bulk or batch operation is performed, each Plaintext value within such bulk or batch operation would count as a Per Protect Event.
Petabytes (PB)	Means 10 <sup>15</sup> bytes, designating an amount of physical data capacity.
Plaintext	Means unencrypted information.
Physical Server	Means a Server that runs with an operating system directly controlling hardware, sometimes called "bare metal." This definition excludes a Server that runs with a hypervisor directly controlling hardware instead.
Plaintext	Means data/information that has not been protected using Encryption, Hashing, or Tokenization.
Point of Encryption	Means a device deployed for the purpose of allowing a business entity to capture and apply encryption and or tokenization to sensitive data. Devices include but are not limited to purpose-built terminals; devices with integrated terminals; and Commercial Off the Shelf (COTS) devices. Such Devices support PAN, SAD, or other sensitive data capture through various means of data conveyance, including but not limited to manual entry, electromagnetic, radio (NFC,) visual, and audio.
POS	Means Point Of Sale. Includes purpose-built hardware and software combinations as well as COTS devices with POS application(s) installed, web-based POS solutions, and unattended devices such as kiosks, vending machines, and access control devices capable of conveying fees and taking payments. products/components/suites.
Premium Package	Means SecureData Enterprise, SecureData Payments, SecureData Sentry, and Structured Data Manager.
Processor	Means, when referring to a payment processor entity, an organization that facilitates electronic payment authorization and/or settlement for payment transactions and related services.
Protect Event	Means an Encryption, Hashing, or Tokenization operation of a single Plaintext value. Where a bulk or batch operation is performed, Encryption, Hashing, or Tokenization of each Plaintext value within the bulk or batch operation would count as a Protect Event.
Proxy Interception	Means, for SecureData Sentry, the interception of Application data (e.g., over HTTP/S) by a Sentry ICAP server.
Record	Means a set of related data stored in a data set (file) or table. A record can contain one or more values. Groups of records are saved in a data set or database table, in a defined format.
SAD	Means sensitive authentication data as defined by PCI Point-to-Point Encryption, version 3.0: "Security-related information (including, but not limited to, card validation codes/values, full-track data from the magnetic stripe, magnetic-stripe image on the chip or elsewhere, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions."
Sensor	Means a SmartCipher endpoint client software that is installed on a supported end user device.
Server	Means any designated computer system in which an Instance or Instances of the software is installed.

## Additional License Authorizations

For Data Security (Voltage) software products

Term	Definition
Standard Package	Means SecureData Enterprise and SecureData Payments products and suites. Doesn't include SecureData Sentry products and suites. Software-specific license terms below. Software products included in a Suite are governed by the individual authorizations and use restrictions associated with each software product, except where otherwise specified in the specific Suite software-specific license terms below.
Suite	Means two or more software products combined into a single license offering or a single software product that includes two or more licenses. The specific software products included in a Suite are specified in the Software Specific License Terms below. Software products included in a Suite are governed by the individual authorizations and use restrictions associated with each software product except where specified in the specific Suite software specific license terms below.
Terabytes (TB)	Means 10 <sup>12</sup> bytes, designating an amount of physical data capacity.
Term License to Use or Term LTU	Means a software license to use (LTU) that indicates in its license description that the license is valid for a specific period of time such as One Month (1M), One Year (1Y) etc. Term LTUs are not perpetual licenses.
Term Support	Means a fixed-period support offering that is only valid during the time period of the associated Term LTU.
Terminal	Means a purpose-built device with hardware and software capabilities to capture PAN and or SAD data.
Test System	Means a non-production test system that has a software product installed and is to be used for a) software product migration testing, and/or b) software product pre-production staging.
Tier	Means the level of Processors or Merchants as determined by annual card payment transaction volume. For Processors, the Tier level is based on the industry standards of tiering which are determined by the annual volume of payment transactions. For Merchants, the Tier level is based on the PCI Data Security Standard (DSS) tiering definitions, which are determined by the Merchant's annual payment card transaction volumes.
Token	Means a surrogate value created by a Tokenization process. A token shares some of the characteristics of the original data element, such as format, length, etc., and is deterministically created, i.e., repeatedly asking for a token for a given data item will yield the same token.
Tokenization	Means a process by which sensitive data elements, such as PANs, Personal Identifiable Information, etc. are replaced by surrogate values. The surrogates can replace the Plaintext value in databases, applications, and data stores. The process can be reversible or irreversible, and may be cryptographic or non-cryptographic. The term Tokenization is frequently used to mean any format-preserving data protection. Voltage SecureData offers various tokenization techniques such as FPE, eFPE, FPH, and SST.
Transaction	Means the transfer of data from a point of capture to a destination host. Transactions may involve payment card data, or capture and transfer of other values including credentials, tax IDs, and other regulated sensitive data. For payments data, the volume of transactions includes payment card authorization requests (including zero-dollar requests) to the host, in addition to authorization and settlement requests. The total transaction volume therefore includes standalone authorization requests, authorization and settlement requests, and card validation requests.
Unlimited events	Means that the number of events that can be consumed by a customer has no limit within the length of the subscription. Refer to Licensing Unlimited Events SKUs section under Software specific license terms for further details.
Use	Means to install, store, load, execute, and/or view one copy of the software and/or its function(s).
User	Means a user whose Use is restricted to the type of software that is being licensed.
User Pack	Means a predetermined number of Users.
Virtual Machine	Means a computer that does not physically exist but is simulated on another computer.
Virtual Server	Means a Virtual Machine running an operating system controlling hardware not directly but via a hypervisor. A computer running a hypervisor may run more than one Virtual Machine at the same time.
Virtual Terminal	Means a web-based solution capable of capturing keyed PAN and or SAD data on a merchant-controlled computing device.
Volume	Means a storage medium mounted on a Node or a Server. For payments, volume means total number of Transactions.

## Additional License Authorizations

For Data Security (Voltage) software products

# Software Specific License Terms

Software products with software-specific license terms are described below. Software products covered by this ALA document (as listed above) and not covered in this section do not have software-specific license terms.

## SecureData Enterprise

**SecureData Enterprise** software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Enterprise Integrations to Cloud Services	Data Volume			Yes
SecureData Enterprise –Open Systems	Named Application or Gigabyte	Yes	Yes	Yes
SecureData Enterprise Data Warehouse (Non-Hadoop/Non-Cloud Service)	Node <sup>2</sup>			
SecureData Enterprise for Hadoop	Node <sup>3</sup>			Yes
SecureData for Snowflake	Data Volume <sup>1</sup>	No	No	Yes
SecureData for Stratus VOS	Named Application	Yes	Yes	No
SecureData Format- Preserving Encryption (FPE) for ArcSight Data Platform	Gigabyte <sup>6</sup>	Yes	No	No
SecureData z/Protect (IBM z/OS)	MSU	Yes	Yes	Yes
SecureData Protected Data Downstream Usage	Terabyte <sup>7</sup>			Yes

<sup>1</sup> Data Volume means the terabytes of data moved/ingested for storage/processing/use, and is either wholly or partially protected by Voltage SecureData.

<sup>2</sup> Node means, for Data Warehouse (Non-Hadoop/Non-Cloud Service), any computing Server where the Data Warehouse software is running and where SecureData APIs are deployed, and/or where data protected by SecureData is stored, processed or used.

<sup>3</sup> Node means, for Hadoop, any computing Server where the Hadoop software is running, and where SecureData APIs are deployed, and/or where data protected by SecureData is stored, processed or used.

<sup>6</sup> Gigabyte means the gigabytes (10<sup>9</sup> bytes) of data ingested by ArcSight per day.

<sup>7</sup> Terabyte means the volume of data measured in terabytes (10<sup>12</sup> bytes) provided downstream, either wholly or partially protected by Voltage SecureData.

The Events and Protect Events SKUs Basic Package Event SKUs allow customers to use all SecureData Enterprise products suites/components EXCEPT SecureData Sentry for internal privacy use cases.

Entitlements under any of these event-based SKUs cover both cloud and on-premises usage, and include:

- **Any number of** Infrastructure Suites; Appliances and Clusters/Nodes/Pods; Datacenters; HSM Engines/Connectors; Named Applications; EDW or Hadoop Nodes; TB/PBs of Data; LBs/Gateways; Clients, Bundles, SDKs, Utilities, and Command Line tools; Cloud Integration Templates and Software; and Developer Templates.
- **All type of** Platforms (open systems, IBM Z, Hadoop, HPE NonStop, Stratus); Clients, Bundles, SDKs, Utilities, and Command Line tools; Environments (Production, Test, Dev, DR); Cloud Integration Templates and Software; and Developer Templates; Operations (Encryption, Tokenization/SST, Hashing, Masking).

## Additional License Authorizations

For Data Security (Voltage) software products

---

Standard Package Event SKUs allow customers to use all SecureData Enterprise and SecureData Payments products suites/components EXCEPT SecureData Sentry for both privacy and payments internal use cases.

Entitlements under any of these event-based SKUs cover both cloud and on-premises usage, and include:

- **Any number of** Infrastructure Suites; Appliances and Clusters/Nodes/Pods; Datacenters; HSM Engines/Connectors; Named Applications; EDW or Hadoop Nodes; TB/PBs of Data; Payments POIs/Lanes; Payments Terminal/Mobile/Host SDKs; LBs/Gateways; Clients, Bundles, SDKs, Utilities, and Command Line tools; Cloud Integration Templates and Software; and Developer Templates.
- **All type of** Platforms (open systems, IBM Z, Hadoop, HPE NonStop, Stratus); Clients, Bundles, SDKs, Utilities, and Command Line tools; Environments (Production, Test, Dev, DR); Cloud Integration Templates and Software; and Developer Templates; Operations (Encryption, Tokenization/SST, Hashing, Masking).

Premium Package Event SKUs allow customers to use all SecureData Enterprise use, SecureData Payments, SecureData Sentry, and Structured Data Manager products/suites/components for both privacy and payments internal use cases.

Entitlements under any of these event-based SKUs cover both cloud and on-premises usage, and include:

- **Any number of** Infrastructure Suites; Appliances and Clusters/Nodes/Pods; Datacenters; HSM Engines/Connectors; Named Applications – Custom and SaaS; EDW or Hadoop Nodes; TB/PBs of Data; Payments POIs/Lanes; Payments Terminal/Mobile/Host SDKs; LBs/Gateways; Clients, Bundles, SDKs, Utilities, and Command Line tools; Cloud Integration Templates and Software; xDBC Drivers and HTTP/Proxy Interceptors, Database Instances, and Developer Templates.
- **All type of** Platforms (open systems, IBM Z, Hadoop, HPE NonStop, Stratus); Clients, Bundles, SDKs, Utilities, and Command Line tools; Environments (Production, Test, Dev, DR); Cloud Integration Templates and Software; and Developer Templates; Operations (Encryption, Tokenization/SST, Hashing, Masking).

Licensing Unlimited Events SKUs: Based on the estimation of the number of events, the Unlimited Events SKUs are licensed for the entire duration of the subscription. The price for the Unlimited Events SKUs are valid only for the duration of the subscription. There is no surcharge for consumption of events over the estimate within the duration of the subscription. Upon renewal, the events are re-estimated and priced appropriately for the next subscription length.

**SecureData Enterprise** use for Integrity NonStop Guardian or OSS is licensed per CPU.

**SecureData Distributed Encryption Engine (Entrust nShield Connect or Atalla HSM Support)** is licensed per Key Server.

**SecureData Encryption or Tokenization for Network Gateways** is licensed per Application for up to 1 million Transactions per year per annum as authorized in your order for the software (Authorized Transactions). If during the one-year period you exceed the Authorized Transactions, you are required to purchase additional Application licenses for the required total volume of Transactions. This license is not authorized to be used with SaaS Gateways.

**SecureData Key Servers** are licensed per Server.

**SecureData Mobile Encryption** is licensed based on the estimated annual volume of Transactions. Additional license(s) are required if the usage exceeds the annual estimated volume. Also requires infrastructure licenses along with the appropriate SecureData client software for the required platforms.

**SecureData Protected Data Downstream Usage** is licensed per Terabyte of total data, either partially or wholly protected by SecureData, and moved to downstream systems not otherwise licensed This license doesn't permit unprotecting protected data at those downstream systems.



## Additional License Authorizations

For Data Security (Voltage) software products

**SecureData Web Encryption** is licensed based on the estimated annual volume of Transactions. Additional license(s) are required if the usage exceeds the annual estimated volume. Also requires infrastructure licenses along with the appropriate SecureData client software for the required platforms.

**SecureData Web FES (Front End Server)** is licensed per Server.

**SecureData Web Services Servers** are licensed per Server.

## SecureData Enterprise suites

Suite	Offering includes
SecureData Enterprise Data Warehouse Starter Edition	<ul style="list-style-type: none"><li>1 SecureData Key Server</li><li>1 SecureData Enterprise Web Services Server</li><li>1 SecureData Enterprise for EDW Installation Kit</li><li>1 SecureData Usage License for one Enterprise Data Warehouse Node *</li></ul>
SecureData Enterprise Data Warehouse Enterprise Edition	<ul style="list-style-type: none"><li>2 SecureData Key Servers</li><li>2 SecureData Enterprise Web Services Server</li><li>1 SecureData Enterprise for EDW Installation Kit</li><li>1 SecureData Usage License for up to 5 Enterprise Data Warehouse Nodes *</li></ul>
SecureData Enterprise Infrastructure Suite 1 – Production and Test and Development	<ul style="list-style-type: none"><li>2 SecureData Key Servers</li><li>2 SecureData Enterprise Web Services Servers</li><li>2 SecureData Key Servers for Test and Development Systems</li><li>2 SecureData Enterprise Web Services Servers for Test and Development Systems</li></ul>
SecureData Enterprise Infrastructure Suite 1 – Disaster Recovery	<ul style="list-style-type: none"><li>2 SecureData Key Servers for Disaster Recovery</li><li>2 SecureData Enterprise Web Services Servers for Disaster Recovery</li></ul>
SecureData Enterprise Infrastructure Suite 2 – Production and Test and Development Systems	<ul style="list-style-type: none"><li>2 SecureData Key Servers for Development Systems</li><li>2 SecureData Enterprise Web Services Servers for Development Systems</li><li>2 SecureData Key Servers for Test and Development Systems</li><li>2 SecureData Enterprise Web Services Servers for Test and Development Systems</li><li>2 SecureData Distributed Encryption Engine for Entrust nShield Connect <b>or Atalla HSM</b></li><li>2 SecureData Distributed Encryption Engine for Entrust nShield Connect <b>or Atalla HSM</b> for Test and Development Systems</li></ul>
SecureData Enterprise Infrastructure Suite 2 – Disaster Recovery	<ul style="list-style-type: none"><li>2 SecureData Key Servers for Disaster Recovery</li><li>2 SecureData Enterprise Web Services Servers for Disaster Recovery</li><li>2 SecureData Distributed Encryption Engine for Entrust nShield Connect <b>or Atalla HSM</b> for Disaster Recovery</li></ul>
SecureData Suite for Hadoop Starter Edition	<ul style="list-style-type: none"><li>1 SecureData Key Server</li><li>1 SecureData Web Services Server</li><li>1 SecureData Enterprise Client Simple API and Client Installation Kit for Red Hat Linux Data Center</li><li>5 SecureData Hadoop Protection Encryption and Tokenization Nodes *</li><li>1 SecureData Hadoop Installation Kit</li></ul>
SecureData Suite for Hadoop Enterprise Edition	<ul style="list-style-type: none"><li>2 SecureData Key Servers</li><li>2 SecureData Enterprise Web Services Servers</li><li>2 SecureData Enterprise Client Simple API and Client Installation Kit for Red Hat Linux Data Center</li><li>20 SecureData Hadoop Protection Encryption and Tokenization Nodes *</li><li>1 SecureData Hadoop Installation Kit</li></ul>

## Additional License Authorizations

For Data Security (Voltage) software products

Suite	Offering includes
SecureData Suite Open System Standard Edition – Test and Development	<ul style="list-style-type: none"><li>▪ 1 SecureData Key Server</li><li>▪ 1 SecureData Enterprise Web Services Server</li><li>▪ 1 SecureData Enterprise Client - Open Systems Bundle (Windows/Linux/Solaris/AIX/HP/UX/Mac OS X) Data Center</li><li>▪ covers up to 500 GB of source data</li><li>▪ limited to Test Data Management Use Cases only</li></ul>
SecureData Suite Open System Enterprise Edition – Test and Development	<ul style="list-style-type: none"><li>▪ 1 SecureData Key Server</li><li>▪ 1 SecureData Key Servers for Test and Development Systems</li><li>▪ 1 SecureData Enterprise Web Services Server</li><li>▪ 1 SecureData Enterprise Web Services Server for Test and Development Systems</li><li>▪ 1 SecureData Enterprise Client - Open Systems Bundle (Windows/Linux/Solaris/AIX/HP/UX/Mac OS X) Data Center</li><li>▪ covers up to 1 TB of source data</li><li>▪ limited to Test Data Management Use Cases only</li></ul>

\* See software-specific license terms of SecureData Enterprise for definition of Node for Data Warehouse, and of Node for Hadoop.

## SecureData Enterprise client software

**SecureData Enterprise Client Open Systems Bundle** is licensed by Data Center.

**SecureData Enterprise Client Simple API and CL Installation Kit** is licensed by Data Center.

**SecureData Enterprise Client Simple API for Linux on IBM Z** is licensed by Data Center.

**SecureData Host SDK Open Systems Installation Kit** is licensed by Data Center.

**SecureData Enterprise Client Hadoop** is licensed by Data Center.

**SecureData Installation Kit for Hadoop** is licensed by Data Center.

**SecureData Mobile Installation Kit for Enterprise/Merchant** is licensed by Data Center.

**SecureData File Processor** is licensed by Data Center.

You are authorized to use and copy the SecureData client software and Installation Kits client software in object code form only solely to create Developed Code and to use and copy Developed Code solely for your internal use with the SecureData software. No rights to distribute the Developed Code are granted herein. You may make and use the number of copies of client software that you deem appropriate unless the number of copies of client software is restricted as set forth in the applicable order.

## SecureData Format-Preserving Encryption (FPE) for ArcSight Data Platform

**SecureData Format-Preserving Encryption (FPE) for ArcSight Data Platform** is licensed per Gigabyte of data ingested by ArcSight per day.

## Additional License Authorizations

For Data Security (Voltage) software products

### SecureData Mobile

**SecureData Mobile** software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Mobile SDK	Transactions per Annum	Yes		

**SecureData Mobile Infrastructure** is licensed per number of Transactions per annum and by Data Center and limited to use for Encryption.

**SecureData Mobile Add-on Infrastructure Suite for Acquirer/ISO/OEM (Service Provider)** is licensed by Data Center and limited to use for Mobile. Base Infrastructure license needs to be included with this license.

### SecureData Payments

**SecureData Payments** software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Payments Base Infrastructure Suite for Acquirer/ISO/OEM (Service Provider) Tier1/Tier2/Tier3/Tier 4	Transactions per annum	Yes	Yes	Yes
SecureData Payments Encryption Add-on Infrastructure Suite for Acquirer/OEM/ISO (Service Provider) Tier1/Tier2/Tier3/Tier 4	Transactions per annum	Yes		Yes
SecureData Payments Tokenization Add-on Infrastructure Suite for Acquirer/OEM/ISO (Service Provider) Tier1/Tier2/Tier3/Tier 4	Transactions per annum		Yes	Yes
SecureData Payments Encryption for Point of Sale (POS) for Acquirer/OEM/ISO (Service Provider)	Lane	Yes		
SecureData Payments Tokenization for Point of Sale (POS) for Acquirer/OEM/ISO (Service Provider)	Lane		Yes	
SecureData Payments Encryption and Tokenization for Point of Sale (POS) for Acquirer/OEM/ISO (Service Provider)	Lane			Yes
SecureData Payments Encryption for Point of Sale (POS) for Enterprise/Merchant	Lane	Yes		
SecureData Payments Tokenization for Point of Sale (POS) for Enterprise/Merchant	Lane		Yes	
SecureData Payments Encryption and Tokenization for Point of Sale (POS) for Enterprise/Merchant	Lane			Yes

## Additional License Authorizations

For Data Security (Voltage) software products

**SecureData Payments Infrastructure for Encryption** is licensed per number of Transactions per annum and per Data Center and limited to use for Encryption.

**SecureData Payments Infrastructure for Tokenization** is licensed per number of Transactions per annum and per Data Center and limited to use for Tokenization.

**SecureData Payments Infrastructure for E-Commerce** is licensed by Data Center and limited to use for E-Commerce.

**SecureData Payments POS Connectors** is licensed by Lane. Lane means in retail environment a single payment terminal. This is the license that needs to be licensed in addition to the Infrastructure license.

## SecureData Sentry

**SecureData Sentry** software as indicated in the table below is licensed in accordance with the following License Metrics. For driver interception, encryption and tokenization licensing is via SecureData open systems licensing. For proxy interception, no separate encryption or tokenization licensing is required.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Sentry for driver interception	Application			Yes
SecureData Sentry for proxy interception	User			Yes

## SecureData Web

**SecureData Web** software as indicated in the table below is licensed in accordance with the following License Metric. Encryption or Tokenization can be licensed independently or together.

Name	License metric	Available encryption only	Available tokenization only	Available encryption and tokenization
SecureData Web Add-on Infrastructure Suite for Acquirer/OEM/ISO (Service Provider) Tier 1/Tier 2/Tier 3/Tier 4	Transactions per annum	Yes	Yes	Yes
SecureData Encryption Use License for SecureData Web for Acquirer/OEM/ISO (Service Provider)	Transactions per annum	Yes		
SecureData Tokenization Use License for SecureData Web for Acquirer/OEM/ISO (Service Provider)	Transactions per annum		Yes	

**Note:** Encryption and Tokenization licenses for SecureData Web are listed under SecureData Enterprise.

**SecureData Web** is licensed based on the annual estimated Volume of Transactions. Add-on infrastructure for SecureData Payment Web is also required.

**SecureData Web Add-on Infrastructure Suite for Acquirer/ISO/OEM (Service Provider)** is licensed per Data Center. Payments Base Infrastructure license is also required.

**SecureData Web Infrastructure** is licensed by number of Transactions per annum and per Data Center and limited to use for Encryption.

## Additional License Authorizations

For Data Security (Voltage) software products

---

### SecureFile

**SecureFile** is an Add-on to SecureMail and is licensed by User and by Application; when licensed by Application a minimum of 50 Users must also be licensed.

### SecureMail

**SecureMail Application Edition** is licensed by number of Applications.

**SecureMail Essentials Edition** is licensed by User.

**SecureMail Standard Edition** is licensed by User.

**SecureMail Enterprise Edition** is licensed by User.

**SecureMail Edition Upgrade** is licensed by User.

**SecureMail Mobile Edition** is licensed by User.

**SecureMail Statements Edition** is licensed per the number of Messages per annum as authorized in your order for the software (“Authorized Messages”). If during the one-year period you exceed the Authorized Messages, you are required to purchase additional licenses for the required total volume of Messages.

**SecureMail for BlackBerry Dynamics** is licensed by User.

**SecureMail for BlackBerry Enterprise Server Add-on** is licensed by User.

**SecureMail for Symantec Enterprise Vault Add-on** is licensed by User.

**SecureMail eDiscovery Accelerator Add-on** is licensed by User.

**SecureMail Large Attachment Delivery Add-on** is licensed by User.

**SecureMail for Remote Desktop Services Add-on** is licensed by User.

**SecureMail Connector for Entrust nShield Connect Add-on** is licensed by User.

### SmartCipher

**SmartCipher** software as indicated in the table below is licensed in accordance with the following License Metric.

Name	License metric
SmartCipher Data Protection Suite for Endpoint Sensor	Per Device

---

### Structured Data Manager

Refer Secure Content Management ALA for Structured Data Manager definitions, software specific license terms, and additional license terms.

## Additional License Authorizations

For Data Security (Voltage) software products

---

# Additional License Terms

### Term

---

- A. Any licensing terms designated as being of Voltage Security Inc. that may be embedded in the software are inapplicable in their entirety.
  - B. Software contains software and associated specifications licensed from third parties that are confidential to, and trade secrets of, such parties. You will not take any action other than to Use it as authorized under the agreement as part of the software products and will not disclose it to third parties.
- 

[software.microfocus.com/legal/software-licensing](https://software.microfocus.com/legal/software-licensing)

Latest version of software licensing documents

---