Addendum to Micro Focus Business Support Agreement

Voltage SecureMail SaaS

This addendum ("Addendum") applies to the Voltage SecureMail products. This Addendum amends and is made part of the Micro Focus® Business Support Agreement ("BSA").

The provisions of the Addendum add to or modify the provisions of the BSA for the Voltage SecureMail products, as further outlined herein. To the extent that there is any conflict between the provisions of this Addendum and the provisions of the BSA, the provisions of this Addendum shall control.

High-Level Summary
SecureMail SaaS is a remotely delivered, hosted email encryption service offered and managed solely by Data Security Voltage for businesses and enterprises. SecureMail SaaS is safely operated in multiple data centers diversely located on the east and west coasts of the United States, providing encryption and authentication services for its customers.

Solution Components
Users of SecureMail SaaS using Microsoft Outlook can download the SecureMail Encryption Client plug-in to send and read encrypted emails. Users without Outlook can send and read encrypted emails using the Zero Download Messenger (ZDM) through a supported web browser. Additionally, the SecureFile plug-in for Microsoft Office enables users to encrypt files and documents.

User of the SecureMail Encryption Client plug-in and the SecureFile plug-in authenticate themselves via an email answerback message and then set a password for future authentication. Password reset is accomplished by another email answerback message.

SecureMail SaaS is available in two editions:
1. Standard Edition
2. Enterprise Edition

Service Features
This section defines what is included in the service of the SecureMail Software as a Service (SaaS) offering provided by Data Security Voltage during the SecureMail SaaS Order term.

SecureMail SaaS provides the following Data Security Voltage products and components:
- SecureMail Encryption Client plug-in
- SecureFile plug-in
- SecureMail Mobile Edition

Summary—Standard Edition
SecureMail SaaS Standard Edition includes the following features, functionality, and components:
- SecureMail Client plug-in for Microsoft Outlook
- SecureFile plug-in for encrypting files and documents (included in the installation with
- SecureMail Encryption Client plug-in)—ZDM for users who do not have Microsoft Outlook
- SecureMail Mobile Edition application for iOS or Android (available from the iOS AppStore and the Google Play Store)

Encrypted email is sent through the SecureMail SaaS Standard domain, vla@vsn.voltage.com.
Summary—Enterprise Edition
SecureMail SaaS Enterprise Edition includes the following features, functionality, and components:
- SecureMail Encryption Client plug-in for Microsoft Outlook
- SecureFile plug-in for encrypting files and documents (included in the installation with SecureMail Encryption Client plug-in)
- ZDM for users who do not have Microsoft Outlook
- Custom domain
- Custom branding for each domain, which consists of logo and color changes
- Multilanguage support
- Integration with archiving and eDiscovery systems
- Client policy settings (if applicable) for the customer
- Auto-encrypt configuration ability rules based on customer requirements

Encrypted email sent through SecureMail SaaS Enterprise Edition use a subdomain of the customer email domain.

Note: SecureMail SaaS Enterprise Edition does not include SecureMail Mobile Edition, which can be purchased separately

Architecture Components

Architecture Components—Standard Edition
Customers are on-boarded as individual users on a hosted, single tenant within a multitenant farm. The key management, authentication, and web services are managed by Data Security Voltage through hosted key servers.

Architecture Components—Enterprise Edition
SecureMail SaaS Enterprise Edition is a multitenant, hybrid SaaS offering, meaning each customer of SecureMail SaaS receives its own segregated tenant on a hosted, multitenant farm. All of the configuration, key management, authentication, and web services for internal and external users are hosted by Data Security Voltage. Changes to the application configuration are made by submitting a request to the Data Security Voltage support.

SecureMail SaaS Enterprise Edition customers can create their own installer for the SecureMail Encryption Client plug-in and SecureFile plug-in if needed.

Additional Solution-Specific Components and Restrictions
SecureMail SaaS and Data Security Voltage do not operate or support third-party, on-site components on behalf of the customer.

Application Administration—Standard Edition
Using the SecureMail SaaS Standard Administrator Console, SecureMail SaaS Standard Edition customers can govern who can administer the account. Administrators can manage which email addresses are permitted to send encrypted messages.

Application Administration—Enterprise Edition
SecureMail SaaS Enterprise Edition customers do not have access to a management interface. However, they can request specific policies, which the Data Security Voltage and SecureMail SaaS technical support team implements on behalf of the customer.

Service Components
SecureMail SaaS includes the following support and operational services.

Service Support
Data Security Voltage provides Level 3 technical support for SecureMail SaaS as defined in the following.

Level 1 support and Level 2 support are initial self-help actions taken by the customer.

- **Level 1**—Answers to basic end user questions that can usually be found by referring to the product documentation or technical support provided by the customer’s internal help-desk-like service. Level 1 is an initial self-help action taken by the Customer.
- **Level 2**—Technical support performed by the customer when no solution could be found through Level 1 technical support. Level 2 technical support includes more advanced troubleshooting methods such as collecting logs and qualifying the Support Request particulars. Level 2 is an advanced self-help action taken by the customer.
- **Level 3**—Request is elevated to Level 3 only after Level 1 and Level 2 technical support efforts are unable to successfully resolve the Support Request. Data Security Voltage technical support will act as the single point of contact to work with the customer to provide timely communications through the resolution process. When Level 3 Support Requests are elevated to Data Security Voltage technical support, four levels of impact are considered for managing the request:
  - **Impact Level 1**—Critical: Enterprise wide impact with no production service and/or software outage with no functionality available to users.
- **Impact Level 2**—Operations are severely restricted and no workaround exits.

- **Impact Level 3**—The product does not operate as designed; there is a minor impact on usage and an acceptable workaround deployed.

- **Impact Level 4**—This can be classified as a request for documentation, general information, or for enhancement requests.

Data Security Voltage provides access to certain software-related electronic and web-based tools and services, as applicable. When experiencing a problem, the customer must use established communication channel(s) to initiate a Support Request with Data Security Voltage. The service coverage window specifies the time during which the customer may call and receive Data Security Voltage support and is specific to the SecureMail SaaS edition purchased.

Data Security Voltage technical support may ask the customer to provide relevant information, start diagnostic tools, and perform other supporting activities, then work with the customer remotely to isolate the problem. Technical support documents and knowledge databases are available for customer personnel who have registered with Data Security Voltage technical support team via the registration form in their Welcome Packet.

**Capacity and Performance Management**
Data Security Voltage proactively monitors the SecureMail SaaS infrastructure for capacity and performance. The architecture allows for addition of capacity to applications, databases, and storage.

**Solution Data Backup and Retention**
Data Security Voltage performs data backups and retention as described in this section, as part of their overall business continuity management practices, designed to attempt to restore availability for customers of SecureMail SaaS and access the customer data, following an outage or similar loss of service.

The following types of customer-specific data are included in the user enrollment and the account databases that reside in the SecureMail SaaS environment.

The user enrollment database consists of email addresses that users input for enrollment. The account database consists of account-related information including user names and hashed passwords. The SecureMail SaaS system does not generate any metadata about the customer data. Customers may send encrypted emails to the ZDM server that resides in the SecureMail SaaS system for temporary decryption and customer access. These encrypted emails are destroyed following use.

The Data Backup Frequency is one (1) day and Data Security Voltage performs that daily backup of the user enrollment and account databases (including configuration data). The Backup Retention Time is seven (7) days, meaning Data Security Voltage retains each daily backup for the most recent seven (7) days (Data Retention Time).

The standard storage and backup measures of Data Security Voltage are its only responsibility regarding the retention of this data, irrespective of any assistance or efforts provided by it to recover or restore customer’s data. Customers may request via a service request for Data Security Voltage to attempt to restore such data from its most current backup. Data Security Voltage will be unable to restore any data not included in the database (not properly entered by the user, or lost or corrupted, and so on) at the time of backup or if customer’s request comes after the Data Retention Time of such backup.

**Disaster Recovery**
Data Security Voltage has a disaster recovery solution in place to recover from potential disaster scenarios. Data Security Voltage replicates most of the customer data for storage at an alternate data center. Data Security Voltage utilized data centers are tested for the wide range of disaster scenarios including fire, loss of Internet connectivity, physical security breaches, and power outages.

**Scheduled Maintenance**
For scheduled maintenance, Data Security Voltage will notify customers at least one (1) week in advance (where feasible) for maintenance releases where customer action is required. Additionally, Data Security Voltage may occasionally perform hotfixes or patches to the SecureMail SaaS system. In the event of a hotfix or patch, customers will be notified promptly. However, for issues of critical impact, customers may receive same day notification.

**Scheduled Version Updates**
SecureMail SaaS Upgrades are defined as both major version updates, minor version updates, and binary patches applied by Data Security Voltage to the SecureMail SaaS production environment. These may or may not include new features or enhancements. Data Security Voltage determines whether and when to develop, release, and apply any SecureMail SaaS Upgrades.

Customer is entitled to SecureMail SaaS Upgrades as part of SecureMail SaaS unless the SaaS Upgrades introduces new functionality that Data Security Voltage offers on an add-on for an additional fee.

Data Security Voltage will use the scheduled maintenance windows defined previously to apply the most recent service packs and hotfixes and to perform upgrade to minor versions of SecureMail SaaS.
**Service-Level Objectives**

Solution Provisioning Time SLO: Solution Provisioning is defined as the SecureMail SaaS solution being available for access over the Internet. Data Security Voltage targets to make SecureMail SaaS Enterprise Edition available within three to five business days of the customer's purchase order (PO) being booked within the Data Security Voltage order management system and SecureMail SaaS Standard Edition immediately available under ordinary circumstances.

Customer is responsible for installing and configuring any additional on-site components for his applications. Any on-site components of the solution are not in scope of the Solution Provisioning Time service-level objective (SLO).

Additionally, the import of customer data into the application is not in scope of the Solution Provisioning Time SLO.

**Online Support Availability SLO**

Online Support Availability SLO is defined as the Data Security Voltage SaaS support portal support.voltage.com being available for access and use by SecureMail SaaS Enterprise Edition customers and its authorized users over the Internet. Data Security Voltage targets to provide customer access to the SaaS support portal on a 24x7 basis at a rate of 99.9% (Online Support Uptime).

**Boundaries and Exclusions**

Online Support Uptime shall not apply to any of the following exceptions:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (for example, DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of agreement
- Actions or inactions of customer (unless undertaken at the express direction of Data Security Voltage)
- Unavailability due to customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Data Security Voltage
- Scheduled maintenance (as described in Scheduled maintenance section)

**Support Request SLO**

**Support Request SLO for Standard Edition**

Data Security Voltage provides support for SecureMail SaaS Standard Edition by the following method:

- Email (datasecurity.voltage.support@microfocus.com)
  Support is available for SecureMail SaaS Standard Edition according to the following availability:
  - Monday to Friday
  - 6 a.m. to 6 p.m. PST

**Support Request SLO for Enterprise Edition**

Data Security Voltage provides support for customers of SecureMail SaaS Enterprise Edition using their access ID by the following methods:

- Web (support.voltage.com)
- Email (datasecurity.voltage.support@microfocus.com)
- Phone (866.440.8917)

Support is available for SecureMail SaaS Enterprise Edition according to the following availability:

- Monday to Sunday
- 24x7, 365 days per year

**Support Response Time Objectives**

The Response and Resolution Targets are provided as guidelines and represent typical request processing by Voltage support teams. They in no way create a legal requirement or obligation for Data Security Voltage to generally respond in the stated time.

**Support Response Time Objectives for Standard Edition**

Response Time Objectives for SecureMail SaaS Standard Edition, for all levels of impact (described in Service support section), are one (1) business day.

**Support Response Time Objectives for Enterprise Edition**

Response Time Objectives for SecureMail SaaS Enterprise Edition, for each level of impact (described in Service support section), are as follows:

- Impact Level 1—30 minutes with prioritized support response
- Impact Level 2—4 hours
- Impact Level 3—6 hours
- Impact Level 4—1 business day

**Service Level Commitments**

further measuring the quality of service that Data Security Voltage is delivering to the customer.

**Solution Availability SLA**

Solution Availability is defined as the SecureMail SaaS production application being available for access and use by customer and its authorized users over the Internet.
Data Security Voltage should provide an improved uptime for the SecureMail SaaS infrastructure. The service uptime metric shall not apply to performance issues resulting from the following situations:

- Caused by overall Internet congestion, slowdown, or unavailability
- Caused by unavailability of Internet services due to third-party service providers outside of the control of Data Security Voltage, such as DNS Servers, network operators, and carrier outages, or third-party system compromises
- That resulted from actions or inactions of the customer (unless undertaken at the express direction of Data Security Voltage or third parties beyond the control of Data Security Voltage)
- That resulted from the customer's equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Data Security Voltage
- That resulted from scheduled infrastructure maintenance and scheduled version updates

**Editions and Entitlements**

SecureMail SaaS is available in different editions with different features and different service levels.

Table 1 summarizes the service entitlements for the various editions of the offering.

<table>
<thead>
<tr>
<th>SecureMail SaaS Edition</th>
<th>Entitlements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecureMail Standard Edition</td>
<td>Email encryption, File encryption, Document encryption, Desktop client, Browser support, Mobile</td>
</tr>
<tr>
<td>SecureMail Enterprise Edition</td>
<td>Email encryption, File encryption, Document encryption, Desktop client, Browser support, Fully customizable policy, Branding options, Policy-based encryption</td>
</tr>
</tbody>
</table>

**Service Requirements**

Assumptions and Dependencies

This service description is based on the following assumptions and dependencies between the customer and Data Security Voltage:

- Customer must have Internet connectivity to access SecureMail SaaS.
- SecureMail SaaS can be performed remotely.
- A SecureMail SaaS Order term is valid for a single application deployment, which cannot be changed during the SecureMail SaaS Order term.
- The service commencement date is the date on which the service is provisioned (as defined in Solution Provisioning Time SLO section).

Furthermore, this SecureMail SaaS Service is provided based on the assumption that customer will implement and maintain the following controls in its use of SecureMail SaaS Service:

- Configuring customer's browser to interact with SecureMail SaaS (if needed)
- Configuring customer's network devices to access SecureMail SaaS (if needed)
- Appointing authorized users
- Configuring its SecureMail SaaS account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications, and terminations

**Good Faith Cooperation**

Customer acknowledges that Data Security Voltage ability to perform the services depends upon customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Data Security Voltage. Where this service description requires agreement, approval, acceptance, consent, or similar action by either party, such action will not be unreasonably delayed or withheld. Customer agrees that to the extent its failure to meet its responsibilities results in a failure, or delay by Data Security Voltage in performing its obligations under this service description, Data Security Voltage will not be liable for such failure or delay.

Learn more at [www.microfocus.com/securedata](http://www.microfocus.com/securedata)

---

www.microfocus.com