



SECURE WEB SERVICE-HYBRID

Support Policy

- Manual Version 2.01

SECURE WEB SERVICE HYBRID SUPPORT POLICY

© 2012 M86 Security
All rights reserved.
8845 Irvine Center Drive, Irvine, CA 92618,
USA

Version 2.01, published March 2012.

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from M86 Security.

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

CONTENTS

INTRODUCTION	1
Glossary of Terms	1
SUPPORT RESPONSIBILITIES	2
PARTNER / CUSTOMER RESPONSIBILITIES	3
CASE HANDLING PROCESS	4
REMOTE SESSIONS	6
SCENARIOS LIST	6
ESCALATION AND SEVERITY PARAMETERS GUIDELINES8

INTRODUCTION

M86 Secure Web Service (SWS-H) is a Web Security Gateway which is hosted on a 3rd party Cloud Infrastructure (IaaS).

M86 SWS-H provides unified web security to the entire borderless enterprise including the corporate headquarters, remote workers and branch offices, while keeping costs at a minimum.

M86 SWS-H is available in a hybrid model that combines on-premise policy server and scanners combined with cloud-based scanners.

The policies are managed by the customer on the policy server (on premises) and are propagated to the SWS-H scanners.

This document entails the responsible parties, support processes and troubleshooting scenarios for this product.

Glossary of Terms

Term	Definition
Partners	Includes M86 Security authorized Distributors and Resellers.
Customer	Refers to the company, organization, government department or other group entity that is the end user of the product - and is under a paid Support Plan.
On premises SWG appliance.	Refers to the SWG appliance which is located physically at the customer's site
Secure Web Service (SWS-H) Scanner	Refers to the SWG scanner which is located on the cloud infrastructure.
3RD Party Infrastructure as a Service (IaaS).	Refers to the infrastructure which the SWS-H scanner is running on

SUPPORT RESPONSIBILITIES

The SWS-H- infrastructure provided by a 3RD party IaaS provider will be managed solely by M86 Security.

M86 Security Support will have full access to the SWS-H scanners located on the IaaS environment. M86 Security will not access the SWS-H scanners without direct permission from the customer / partner

Configuration changes relating to the IaaS environment will be performed by M86 Security.

The following are possible examples of such changes:

- IP address assigned to the SWS-H scanners
- Firewall of the SWS-H scanners
- SWG version of Instances
- Additional scanner Instances

Partners / customers will not have direct access to the SWS-H scanners and the IaaS environment, however, they will have full access to the scanner application running on the IaaS environment.

M86 Security is contractually bound to manage any SWS-H information in a confidential and discreet manner. Should there be a need, a Non-Disclosure Agreement can be signed.



NOTE: The above is only relevant for customers using M86 Security SWS-H service in which the IaaS is managed by M86 Security. Customers who manage their environment should refer to M86 Security Support Services Policy.

PARTNER / CUSTOMER RESPONSIBILITIES

The customer / partner will have full control over the configuration of the SWG Policy Server, scanners (on premises) and SWS-H scanners (including security policies and the like). The exception to this concerns any configuration changes that relate to the IaaS environment (as specified in Chapter 2).

The customer / partner should contact M86 Security Technical Support as described in the [M86 Security Product Support Policy](#) to report any issue that pertains to any one of the following:

- Loss of connectivity to SWS-H scanners
- Synchronization between on-premise Policy Servers and SWS-H scanners
- Disk space consumption
- Memory consumption
- SWS-H scanner restarts
- Any other issue that may be related to the SWS-H environment

The SWS-H scanners and the IaaS environment will not be monitored by M86 Security. It is the responsibility of the customer / partner to report issues which pertain to remote scanners. As such, unreported issues will not be handled proactively.

Configuration changes that pertain to the IaaS environment as specified in Chapter 2 should be reported and approved by M86 Security. Once the requested changes have been approved, M86 Support will execute the changes within 3 Business days.

All inbound and outbound communication will be done between the customer / partner and M86 Security Support. Communication to the IaaS provider will be done by M86 Security.



NOTE: The above is only relevant for customers using M86 Security SWS-H service in which the IaaS is managed by M86 Security. Customers who manage their environment should refer to M86 Security Support Services Policy.

CASE HANDLING PROCESS

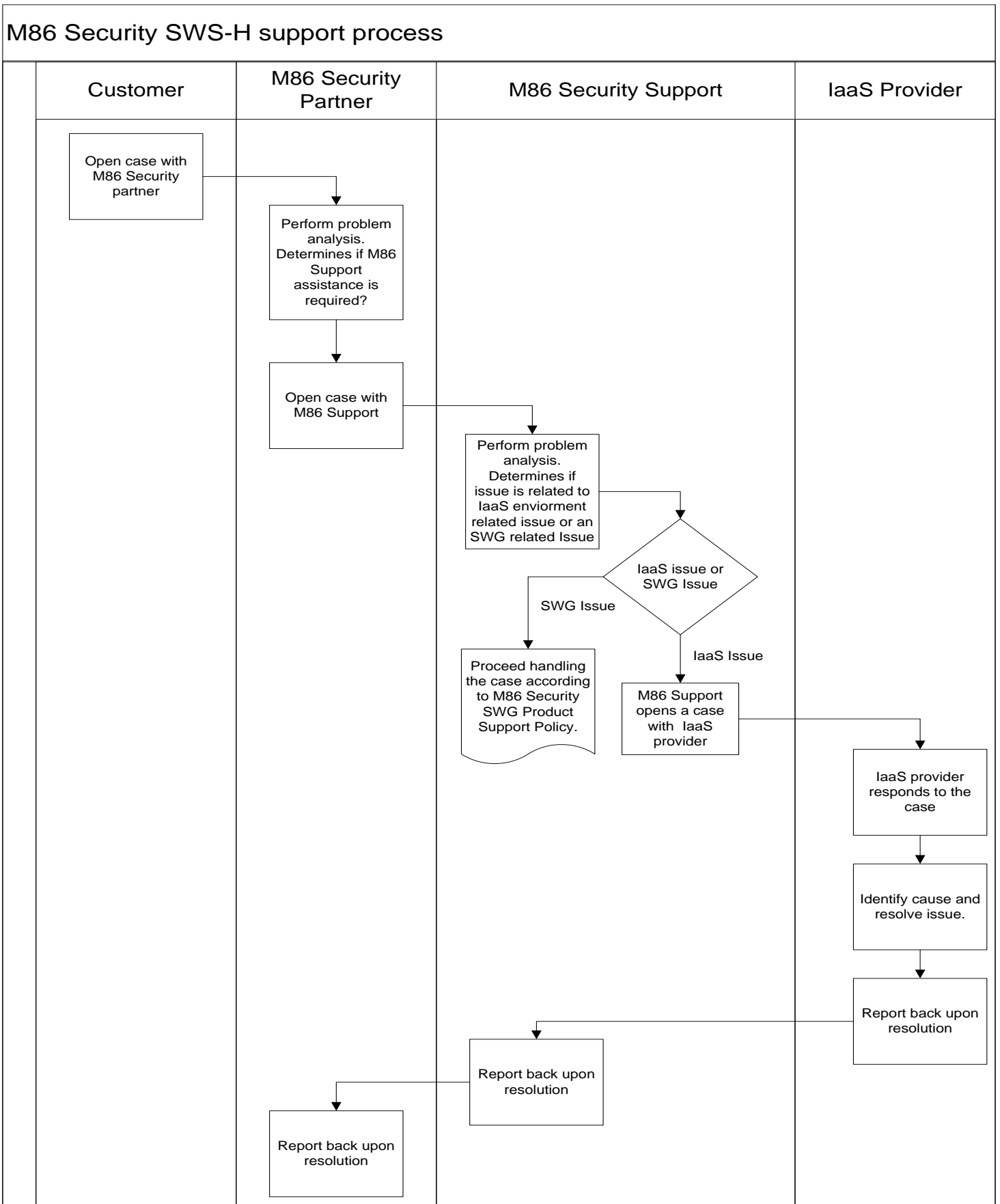
Once a customer / partner logs a case, the following steps shall be taken by M86 Security Support:

1. The case will be assigned to a Level 1 support, SWS-H trained, engineer.
2. The Level 1 Engineer assigned to the case will determine if the reported issue is caused due to a IaaS Environment issue or a SWG related issue.

Once the source of the issue has been determined, the engineer will:

- Open a case with the 3rd party Infrastructure support team and will monitor the progress of the case until the issue is resolved.
- Proceed to handle the case according to the SWG Case Handling process (as specified in M86 Security SWG Product Support Policy).

The following diagram provides a detailed description of the process:



REMOTE SESSIONS

SWG related issues might require a remote session (via remote session tools such as "Netviewer", "WebEx", etc..) to a desktop computer with access to the on-premises Policy Server and Scanners (HTTPS and SSH protocols).



In such cases the customer / partner is responsible to enable access to the on premises SWG appliances for M86 Security Support.

SCENARIOS LIST

This is a list of support related scenarios customers may encounter when using the M86 SWS-H solution. In each scenario, if/when the customer / partner experiences such symptoms (described below), M86 Security Support should be contacted.

Scenarios List:

#	Issue	Symptoms	Indications	Source
1	Power failure	Service unreachable (browsing)	M86 SWS-H scanner cannot be reached via SSH	Cloud Infrastructure Issue
2	Connectivity issues - M86 SWS-H scanner is unavailable	Service unreachable (management)	- M86 SWS-H scanner cannot be reached via SSH - Red icon in the M86 Devices section in the Management Console.	Cloud Infrastructure Issue
3	Hard disk is full	Failed updates (AV, URL Categorization / maintenance release) Performance issues (browsing is slow) Management console is unreachable. Commit changes fails	System log alerts - Dashboard indication - SNMP alerts SWS-H scanner Issue	SWS-H scanner Issue
4	Memory consumption / free memory is low	Performance issues (browsing is slow) Commit changes takes a long time	System log alerts - Dashboard indication - SNMP alerts	SWS-H scanner Issue

#	Issue	Symptoms	Indications	Source
5	Scanner restarts	Service unreachable (browsing)	- System log alerts - SNMP alerts	SWS-H scanner Issue
6	Connectivity issues - M86 SWS-H scanner cannot go out to the Internet	Service unreachable (browsing)	- Red icon () in the M86 Devices section in the Management Console. - wget request from M86 SWS- H scanner limited shell (SSH) fails - Connection Status: Not active	SWS-H scanner Issue
7	M86 SWS-H scanner is unsynchronized	Changes are not committed to the M86 SWS-H scanner by the Policy Server	- Gray icon () in the M86 Devices section in the Management Console. - Sync Status: Unsynchronized	Cloud Infrastructure / SWS-H scanner Issue

ESCALATION AND SEVERITY PARAMETERS GUIDELINES

Both the customer / partner and M86 Security Support will agree on the severity level based on the following factors:

Severity	Description	M86 Security Work Effort
Mission Critical Showstopper	Production SWS-H scanner is inoperative, severely impacting business processes, and problem is not readily circumvented.	M86 Security will assign all necessary resources to identify and resolve the problem to obtain a workaround or to reduce the severity level of the problem. M86 Security will work on the problem 24 hours per day, 7 days a week, every day of the year, including holidays (24x7x365).
High	SWS-H scanner is severely impacted in a way that substantially degrades the product performance or materially restricts business processes. For example, moderate system impact or system hanging.	M86 Security will identify, find a workaround and/or correct the problem using all available resources during normal business hours.
Medium	SWS-H scanner has limited functionality or a workaround is available to bypass the problem	M86 Security will commit full time resources to identify and correct the problem or find a workaround during normal business hours.
Low	Anomalies in the appliance processing that do not impact ongoing usage. This category includes documentation corrections, nuisance issues and messages.	M86 Security will work to identify and resolve the problem according to available resources during normal business hours.