

# **NON-PROPRIETARY CRYPTOGRAPHIC MODULE SECURITY POLICY FOR THE**

## **HP 5406 ZL [1], HP 5412 ZL [2], HP 8206 ZL [3] AND HP 8212 ZL [4] SWITCHES WITH THE HP MSM765ZL MOBILITY CONTROLLER**

**(HARDWARE VERSIONS: SWITCHES: (J8697A [1], J8698A [2], J9447A [3], AND J9091A [4] [B]); MANAGEMENT MODULES: (J8726A [1,2] AND J9092A [3,4] [B]); POWER SUPPLY: (J9306A: ONE [1,3] OR TWO [2,4]); SUPPORT MODULE: (J9095A [3,4] [B]); FABRIC MODULE: (J9093A: TWO [3,4] [B]); BLANK PLATE: (5069-8563: FOUR [1], TEN [2], FIVE [3], OR ELEVEN [4]); OPACITY SHIELD KITS: (J9710A [1], J9711A [2], J9712A [3], AND J9713A [4]); HIGH PERFORMANCE FAN TRAYS: (J9721A [1], J9722A [2], J9723A [3], AND J9724A [4]); WITH (HP GIG-T/SFP+ V2 ZL MOD: J9536A; HP MOBILITY CONTROLLER: J9370A [A] AND TAMPER EVIDENT SEAL KIT: J9709A) [1,2,3,4]; FIRMWARE VERSIONS: 5.6.0 [A] AND K.15.07.0003 [B])**

25 July 2012

**Hewlett-Packard Development Company, L.P.**  
2344 Boul. Alfred-Nobel  
St-Laurent, QC H4S 0A4



COPYRIGHT HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P.



## TABLE OF CONTENTS

|            |  |           |
|------------|--|-----------|
| <b>1</b>   | <b>Introduction .....</b>  | <b>1</b>  |
| <b>1.1</b> | <b>PURPOSE.....</b>  | <b>1</b>  |
| <b>1.2</b> | <b>SCOPE.....</b>  | <b>1</b>  |
| <b>1.3</b> | <b>INTENDED USE .....</b>  | <b>1</b>  |
| <b>1.4</b> | <b>ACRONYMS.....</b>   | <b>2</b>  |
| <b>2</b>   | <b>Cryptographic Module Overview .....</b>   | <b>4</b>  |
| <b>2.1</b> | <b>FIPS PUB 140-2 TARGETED SECURITY LEVELS .....</b>   | <b>7</b>  |
| <b>2.2</b> | <b>PORTS AND INTERFACES .....</b>  | <b>8</b>  |
| <b>2.3</b> | <b>OPACITY SHIELDS, HIGH PERFORMANCE FAN TRAYS, AND TAMPER EVIDENT SEALS.....</b>                          | <b>17</b> |
| 2.3.1      | General Instructions for Tamper Evident Seals.....   | 18        |
| 2.3.2      | Tamper Evident Seal Placement on the Switch Chassis.....   | 18        |
| 2.3.2.1    | Chassis Back .....   | 19        |
| 2.3.2.2    | Chassis Sides.....   | 20        |
| 2.3.2.3    | Chassis Top .....  | 25        |
| 2.3.2.4    | Chassis Bottom.....  | 29        |
| <b>2.4</b> | <b>TAMPER EVIDENT SEAL PLACEMENT ON CHASSIS FRONT AND INSTALLED MODULES .....</b>                          | <b>33</b> |
| <b>2.5</b> | <b>CRYPTOGRAPHIC MODULE BOUNDARY .....</b>   | <b>37</b> |
| <b>3</b>   | <b>Product Operation.....</b>  | <b>38</b> |
| <b>3.1</b> | <b>OVERVIEW.....</b>   | <b>38</b> |
| <b>3.2</b> | <b>FIPS APPROVED MODE OF OPERATION .....</b>   | <b>38</b> |
| 3.2.1      | Description.....   | 38        |
| 3.2.2      | Instructions for Putting the HP MSM765zl Mobility Controller into the FIPS Approved Mode of Operation..... | 40        |
| 3.2.2.1    | Initial Assumptions .....  | 40        |
|            | STEP 1: LOAD THE FIPS VALIDATED FIRMWARE ON THE CONTROLLER.....  | 40        |
|            | STEP 2: RESET THE CONTROLLER TO THE FACTORY DEFAULT.....   | 44        |
|            | STEP 3: CONFIGURE THE MANAGEMENT TOOL.....   | 45        |
|            | STEP 4: SELECTING SELF-TESTING AND DISABLING SERVICE OS .....  | 47        |
|            | STEP 5: AUTHENTICATION SETUP.....  | 48        |
|            | STEP 6: SET RESTRICTIONS.....  | 52        |
|            | STEP 7: SERVICES THAT ARE NOT ALLOWED IN THE FIPS APPROVED MODE OF OPERATION .....                         | 61        |



**4 Security Rules Derived from the Requirements of FIPS PUB 140-2.....71**

**4.1 FINITE STATE MODEL ..... 71**

**4.2 ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC) ..... 71**

**4.3 SELF-TESTS ..... 72**

4.3.1 Power-Up Self-Tests..... 72

4.3.2 Conditional Self-Tests ..... 73

**4.4 DESIGN ASSURANCE ..... 74**

4.4.1 Delivery and Operation..... 74

4.4.2 Functional Specification ..... 74

4.4.3 Guidance Documents..... 74

**5 Additional Security Rules .....75**

**5.1 ENFORCED SECURITY RULES..... 75**

**5.2 SECURITY RULES NOT ENFORCED BY THE CRYPTOGRAPHIC MODULE 75**

**6 Identification and Authentication Policy.....76**

**7 Access Control Policy .....78**

**7.1 OVERVIEW..... 78**

**7.2 CRYPTOGRAPHIC MODULE SERVICES ..... 78**

7.2.1 Show Status ..... 78

7.2.2 Perform Power-Up Self-Tests..... 78

7.2.3 Perform IPSec IKE ..... 79

7.2.4 Perform IPSec ESP Transfers ..... 79

7.2.5 Perform Plaintext Data Transfer ..... 79

7.2.6 Access Point Management..... 79

7.2.7 Controller Teaming..... 80

7.2.8 Management of HP MSM765zl Mobility Controller through TLS..... 80

7.2.9 Management of HP MSM765zl Mobility Controller through SSH..... 80

7.2.10 Management of HP MSM765zl Mobility Controller through SOAP..... 80

7.2.11 Firmware Load..... 81

7.2.12 Configuration File Export..... 81

7.2.13 Plaintext Key and CSP Zeroization ..... 81

**7.3 ROLES, SERVICES, AND ACCESSES ..... 82**

7.3.1 Anonymous Services ..... 82

7.3.2 Role-Based Services ..... 82

**7.4 NON-FIPS APPROVED SERVICES ..... 83**



|            |  |            |
|------------|--|------------|
| <b>7.5</b> | <b>SECURITY DATA</b> .....   | <b>84</b>  |
| 7.5.1      | General.....   | 84         |
| 7.5.2      | Cryptographic Keys .....   | 84         |
| 7.5.3      | Critical Security Parameters .....   | 84         |
| 7.5.4      | Cryptographic Key Management.....  | 85         |
| 7.6        | IMPLEMENTED CRYPTOGRAPHIC ALGORITHMS .....                                 | 98         |
| <b>8</b>   | <b>Physical Security Policy</b> .....                                      | <b>99</b>  |
| <b>8.1</b> | <b>OVERVIEW</b> .....  | <b>99</b>  |
| <b>8.2</b> | <b>PHYSICAL SECURITY MECHANISMS</b> .....                                  | <b>99</b>  |
| 8.2.1      | Tamper Evident Seals, Opacity Shields, and High Performance Fan Tray ..... | 99         |
| <b>8.3</b> | <b>INSPECTION AND TESTING</b> .....  | <b>99</b>  |
| <b>9</b>   | <b>Security Policy for Mitigation of Other Attacks</b> .....               | <b>101</b> |
| <b>9.1</b> | <b>OVERVIEW</b> .....  | <b>101</b> |
| <b>9.2</b> | <b>MECHANISMS IMPLEMENTED</b> .....  | <b>101</b> |
| <b>9.3</b> | <b>MITIGATION SUMMARY</b> .....  | <b>101</b> |



## TABLE OF TABLES

|  |     |
|--|-----|
| Table 1 – FIPS 140-2 Section Targeted Security Levels .....  | 7   |
| Table 2 – Logical Interfaces Specific to the HP MSM765zl Mobility Controller.....  | 14  |
| Table 3 – Ports for the Rest of the HP 5406 zl Switch with the HP MSM765zl Mobility<br>Controller and the HP 5412 zl Switch with the HP MSM765zl Mobility Controller<br>Cryptographic Modules..... | 16  |
| Table 4 – Ports for the Rest of the HP 8206 zl Switch with the HP MSM765zl Mobility<br>Controller and the HP 8212 zl Switch with the HP MSM765zl Mobility Controller<br>Cryptographic Modules..... | 17  |
| Table 5 – Roles and Required Identification and Authentication.....  | 76  |
| Table 6 – Strengths of Authentication Mechanisms .....   | 77  |
| Table 7 – Anonymous Services .....   | 82  |
| Table 8 – Services Authorized for Roles .....  | 82  |
| Table 9 – Cryptographic Keys and Other Critical Security Parameters Table .....  | 90  |
| Table 10 – Pseudo-Random Number Generators .....   | 91  |
| Table 11 – Cryptographic Module Cryptographic Key and Other CSP Output.....  | 93  |
| Table 12 – Access Rights within Services.....  | 97  |
| Table 13 – Implemented FIPS Approved Cryptographic Algorithms .....  | 98  |
| Table 14 – Inspection/Testing of Physical Security Mechanisms .....  | 99  |
| Table 15 – Mitigation of Other Attacks .....   | 101 |



## TABLE OF FIGURES

|  |    |
|--|----|
| Figure 1 – HP 5406 zl Switch with the HP MSM765zl Mobility Controller .....  | 8  |
| Figure 2 – HP 5412 zl Switch with the HP MSM765zl Mobility Controller .....  | 9  |
| Figure 3 – HP 8206 zl Switch with the HP MSM765zl Mobility Controller .....  | 11 |
| Figure 4 – HP 8212 zl Switch with the HP MSM765zl Mobility Controller .....  | 13 |
| Figure 5 – Tamper Evident Seal Placement on Back of 5406 zl Chassis or 8206 zl Chassis.....  | 19 |
| Figure 6 – Tamper Evident Seal Placement on Back of 5412 zl Chassis or 8212 zl Chassis.....  | 20 |
| Figure 7 – Tamper Evident Seal Placement on Side of HP 5406 zl Switch Chassis (11 Seals on this Side).....                             | 21 |
| Figure 8 – Tamper Evident Seal Placement on Side of HP 5412 zl Switch Chassis (13 Seals on this Side).....                             | 22 |
| Figure 9 – Tamper Evident Seal Placement on Side of HP 8206 zl Switch Chassis (12 Seals on this Side).....                             | 23 |
| Figure 10 – Tamper Evident Seal Placement on Side of HP 8212 zl Switch Chassis (14 Seals on this Side).....                            | 24 |
| Figure 11 – Tamper Evident Seal Placement on Top of HP 5406 zl Switch Chassis (18 Seals per Three-Quarter Rectangle).....              | 25 |
| Figure 12 – Tamper Evident Seal Placement on Top of HP 5412 zl Switch Chassis (18 Seals per Three-Quarter Rectangle).....              | 26 |
| Figure 13 – Tamper Evident Seal Placement on Top of HP 8206 zl Switch Chassis (18 Seals per Three-Quarter Rectangle).....              | 27 |
| Figure 14 – Tamper Evident Seal Placement on Top of HP 8212 zl Switch Chassis (18 Seals per Three-Quarter Rectangle).....              | 28 |
| Figure 15 – Tamper Evident Seal Placement on Bottom of HP 5406 zl Switch Chassis (12 Seals in Single Line).....                        | 29 |
| Figure 16 – Tamper Evident Seal Placement on Bottom of HP 5412 zl Switch Chassis (12 Seals in Single Line).....                        | 30 |
| Figure 17 – Tamper Evident Seal Placement on Bottom of HP 8206 zl Switch Chassis (12 Seals in Single Line).....                        | 31 |
| Figure 18 – Tamper Evident Seal Placement on Bottom of HP 8212 zl Switch Chassis (12 Seals in Single Line).....                        | 32 |
| Figure 19 – Placement of Tamper Evident Seals on Front of the HP 5406 zl Switch with the MSM765zl Mobility Controller (11 Seals) ..... | 33 |
| Figure 20 – Placement of Tamper Evident Seals on Front of the HP 5412 zl Switch with the MSM765zl Mobility Controller (20 Seals) ..... | 34 |
| Figure 21 – Placement of Tamper Evident Seals on Front of the HP 8206 zl Switch with the MSM765zl Mobility Controller (16 Seals) ..... | 35 |
| Figure 22 – Placement of Tamper Evident Seals on Front of the HP 8212 zl Switch with the MSM765zl Mobility Controller (25 Seals) ..... | 36 |



## **1 INTRODUCTION**

### **1.1 PURPOSE**

This document defines the security policy for the four cryptographic modules:

- HP 5406 zl Switch with the HP MSM765zl Mobility Controller;
- HP 5412 zl Switch with the HP MSM765zl Mobility Controller;
- HP 8206 zl Switch with the HP MSM765zl Mobility Controller; and
- HP 8212 zl Switch with the HP MSM765zl Mobility Controller.

The primary focus of this security policy is the HP MSM765zl Mobility Controller since the switch part of the cryptographic module will not be providing cryptographic services when the cryptographic module is configured to execute in the FIPS approved mode of operation.

Section 2 provides information on the version numbers of the components of each of the four cryptographic modules.

### **1.2 SCOPE**

This document is written in accordance with the requirements of Appendix C of FIPS PUB 140-2, and includes the rules derived from the requirements of FIPS PUB 140-2 and the rules derived from any additional requirements imposed by the vendor.

### **1.3 INTENDED USE**

This document is intended to be used:

- a. To provide a specification of the cryptographic security that will allow individuals and organizations to determine whether the cryptographic module, as implemented, satisfies a stated security policy; and
- b. To describe to individuals and organizations the capabilities, protection, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.



## 1.4 ACRONYMS

|                |  |
|----------------|--|
| AC             | Alternating Current  |
| AES            | Advanced Encryption Standard                               |
| ANSI           | American National Standards Institute                      |
| AP             | Access Point   |
| CA             | Certificate Authority                                      |
| CAVP           | Cryptographic Algorithm Validation Program                 |
| CBC            | Cipher Block Chaining                                      |
| CFR            | Code of Federal Regulations                                |
| CLI            | Command Line Interface                                     |
| CMVP           | Cryptographic Module Validation Program                    |
| CPU            | Central Processing Unit                                    |
| CSEC           | Communications Security Establishment Canada               |
| CSP            | Critical Security Parameter                                |
| DES            | Data Encryption Standard                                   |
| EAP            | Extensible Authentication Protocol                         |
| EAP-PEAPv0     | EAP Protected Extensible Authentication Protocol Version 0 |
| EAP-TLS        | EAP Transport Layer Security                               |
| EAP-TTLS       | EAP Tunneled Transport Layer Security                      |
| ECB            | Electronic Codebook  |
| ED             | Electronic Distribution                                    |
| EE             | Electronic Entry   |
| EMC            | Electromagnetic Compatibility                              |
| EMI            | Electromagnetic Interference                               |
| ESP            | Encapsulating Security Payload                             |
| FCC            | Federal Communications Commission (US)                     |
| FIPS           | Federal Information Processing Standard                    |
| FIPS PUB 140-2 | FIPS Publication 140 Second Revision (2)                   |
| Gb             | Gigabit  |
| GbE            | Gigabit Ethernet   |
| GHz            | Gigahertz  |
| GUI            | Graphical User Interface                                   |
| HDD            | Hard Disk Drive  |
| HMAC           | Keyed-Hashing for Message Authentication Code              |
| HP             | Hewlett-Packard  |
| HTML           | Hypertext Markup Language                                  |
| HTTP           | Hypertext Transfer Protocol                                |
| HTTPS          | Secure Hypertext Transfer Protocol                         |
| IKE            | Internet Key Exchange                                      |
| IP             | Internet Protocol  |





|               |  |
|---------------|--|
| IPSec         | Internet Protocol Security                               |
| IT            | Information Technology                                   |
| LAN           | Local Area Network                                       |
| LED           | Light Emitting Diode                                     |
| L2TP          | Layer Two (2) Tunneling Protocol                         |
| MD            | Manual Distribution or Message Digest                    |
| MIB           | Management Information Base                              |
| MSM           | Multiservice Mobility                                    |
| N             | Number of Controllers                                    |
| NIST          | National Institute of Standards and Technology           |
| NOC           | Network Operations Center                                |
| N/A           | Not Applicable   |
| OS            | Operating System   |
| PoE           | Power over Ethernet                                      |
| PPTP          | Point-to-Point Tunneling Protocol                        |
| PRNG          | Pseudo-Random Number Generator                           |
| RADIUS        | Remote Authentication Dial-In User Service               |
| RC4           | Rivest Cipher 4  |
| RJ            | Registered Jack  |
| RS            | Recommended Standard                                     |
| RSA           | Rivest Shamir Adleman asymmetric cryptographic algorithm |
| SDRAM         | Synchronous Dynamic Random Access Memory                 |
| SFP           | Small Form Factor Pluggable                              |
| SHA           | Secure Hash Algorithm                                    |
| SHA1 or SHA-1 | Secure Hash Algorithm First Revision (1)                 |
| SNMP          | Simple Network Management Protocol                       |
| SOAP          | Simple Object Access Protocol                            |
| SP            | Special Publication                                      |
| ssh           | Secure Shell   |
| SSH           | Secure Shell   |
| SSL           | Secure Sockets Layer                                     |
| TLS           | Transport Layer Security                                 |
| VLAN          | Virtual Local Area Network                               |
| VPN           | Virtual Private Network                                  |
| VSC           | Virtual Service Community                                |
| WPA           | WiFi Protected Access                                    |
| X9            | Accredited Standards Committee on Financial Services     |
| X.            | ANSI Group   |



## 2 CRYPTOGRAPHIC MODULE OVERVIEW

The HP 5406 zl Switch and HP 5412 zl Switch are advanced intelligent switches in the HP modular chassis product line. The HP 5406 zl Switch has a 6-slot chassis and includes associated zl modules and bundles. The HP 5412 zl Switch is similar but with a 12-slot chassis. The switches offer excellent investment protection, flexibility, and scalability, as well as ease of deployment, operation, and maintenance. Some of their key properties are:

- Advanced access layer, distribution, and core;
- Integrated Layer 2 to Layer 4 intelligent edge feature set;
- Enterprise-class performance and security;
- HP AllianceONE integrated; and
- Scalable 10/100/1000 and 10-GbE connectivity.

The HP 8206 zl Switch and HP 8212 zl Switch offer the same features as the HP 5400 zl Switches but also provide high availability with high performance. The HP 8206 zl Switch has a 6-slot chassis and the HP 8212 zl Switch has a 12-slot chassis. The switches with their high-availability each provide a mission-critical access layer.

The installed HP MSM765zl Mobility Controller enables strong security for wireless enterprise networking, using embedded IPSec VPN and firewall functionalities. The controller is intended for enterprise office environments of differing scales, from the corporate headquarters to remote branch sites, and therefore has been designed with ease of use in mind, making deployment and remote administration as easy as possible.

A HP MSM765zl Mobility Controller can support up to 200 Access Points. The HP MSM765zl Mobility Controller enables secure mobile access to IT resources within enterprise environments, remote access and site-to-site VPN services using the IPSec, L2TP and PPTP protocols. They securely deliver enterprise networking without bounds, significantly increasing employee productivity in corporate offices, in decentralized/remote workgroups, and in branch locations with broadband access.

One particular configuration of the HP MSM765zl Mobility Controller in each of the four Ethernet switches is validated to FIPS PUB 140-2. These are specified in this section. The four Ethernet switches can support other combinations of line cards with the HP MSM765zl Mobility Controller(s).



The four cryptographic modules covered by this Security Policy are comprised of the following components:

1. HP 5406 zl Switch with the HP MSM765zl Mobility Controller

- 1 HP 5406 zl Switch, Hardware Version: J8697A and Firmware Version: K.15.07.0003;
- 1 HP Switch 5400 zl Management Module, Hardware Version: J8726A and Firmware Version: K.15.07.0003;
- 1 HP MSM765zl Mobility Controller, Hardware Version: J9370A and Firmware Version: 5.6.0;
- 1 HP Gig-T/SFP+ v2 zl Mod, Hardware Version: J9536A;
- 4 Blank Plates, all with Hardware Version: 5069-8563;
- 1 HP 1500 W PoE+ zl Power Supply, Hardware Version: J9306A;
- 1 HP 5406 zl Opacity Shield Kit, Hardware Version: J9710A;
- 1 HP 5406 zl High Performance Fan Tray, Hardware Version: J9721A; and
- 1 Tamper Evident Seal Kit, Hardware Version: J9709A.

2. HP 5412 zl Switch with the HP MSM765zl Mobility Controller

- 1 HP 5412 zl Switch, Hardware Version: J8698A and Firmware Version: K.15.07.0003;
- 1 HP Switch 5400 zl Management Module, Hardware Version: J8726A and Firmware Version: K.15.07.0003;
- 1 HP MSM765zl Mobility Controller, Hardware Version: J9370A and Firmware Version: 5.6.0;
- 1 HP Gig-T/SFP+ v2 zl Mod, Hardware Version: J9536A;
- 10 Blank Plates, all with Hardware Version: 5069-8563;
- 2 HP 1500 W PoE+ zl Power Supplies, both with Hardware Version: J9306A;
- 1 HP 5412 zl Opacity Shield Kit, Hardware Version: J9711A;
- 1 HP 5412 zl High Performance Fan Tray, Hardware Version: J9722A; and
- 1 Tamper Evident Seal Kit, Hardware Version: J9709A.



3. HP 8206 zl Switch with the HP MSM765zl Mobility Controller

- 1 HP 8206 zl Switch, Hardware Version: J9477A and Firmware Version: K.15.07.0003;
- 1 HP Switch 8200 zl Management Module, Hardware Version: J9092A and Firmware Version: K.15.07.0003;
- 1 HP Switch 8200zl System Support Module, Hardware Version: J9095A and Firmware Version: K.15.07.0003;
- 2 HP Switch 8200 zl Fabric Modules, both with Hardware Version: J9093A and Firmware Version: K.15.07.0003;
- 1 HP MSM765zl with Mobility Controller, Hardware Version: J9370A and Firmware Version: 5.6.0;
- 1 HP Gig-T/SFP+ v2 zl Mod, Hardware Version: J9536A;
- 5 Blank Plates, all with Hardware Version: 5069-8563;
- 1 HP 1500 W PoE+ zl Power Supply, Hardware Version: J9306A;
- 1 HP 8206 zl Opacity Shield Kit, Hardware Version: J9712A;
- 1 HP 8206 zl High Performance Fan Tray, Hardware Version: J9723A; and
- 1 Tamper Evident Seal Kit, Hardware Version: J9709A.

4. HP 8212 zl Switch with the HP MSM765zl Mobility Controller

- 1 HP 8212 zl Switch, Hardware Version: J9091A and Firmware Version: K.15.07.0003;
- 1 HP Switch 8200zl Management Module, Hardware Version: J9092A and Firmware Version: K.15.07.0003;
- 1 HP Switch 8200zl System Support Module, Hardware Version: J9095A and Firmware Version: K.15.07.0003;
- 2 HP Switch 8200zl Fabric Modules, both with Hardware Version: J9093A and Firmware Version: K.15.07.0003;
- 1 HP MSM765zl Mobility Controller, Hardware Version: J9370A and Firmware Version: 5.6.0;
- 1 HP Gig-T/SFP+ v2 zl Mod, Hardware Version: J9536A;
- 11 Blank Plates, all with Hardware Version: 5069-8563;
- 2 HP 1500 W PoE+ zl Power Supplies, both with Hardware Version: J9306A;
- 1 HP 8212 zl Opacity Shield Kit, Hardware Version: J9713A;
- 1 HP 8212 zl High Performance Fan Tray, Hardware Version: J9724A; and
- 1 Tamper Evident Seal Kit, Hardware Version: J9709A.



## 2.1 FIPS PUB 140-2 TARGETED SECURITY LEVELS

Each of the four cryptographic modules covered in this Security Policy is designed to meet Security Level 2 overall.

**Table 1** specifies the security level targeted for each of the sections of FIPS 140-2.

| FIPS 140-2 Section   | Target Security Level |
|--|-----------------------|
| 4.1 Cryptographic Module Specification                                   | 2                     |
| 4.2 Cryptographic Module Ports and Interfaces                            | 2                     |
| 4.3 Roles, Services, and Authentication                                  | 2                     |
| 4.4 Finite State Model   | 2                     |
| 4.5 Physical Security  | 2                     |
| 4.6 Operational Environment  | Not Applicable        |
| 4.7 Cryptographic Key Management   | 2                     |
| 4.8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) | 2                     |
| 4.9 Self-Tests   | 2                     |
| 4.10 Design Assurance  | 2                     |
| 4.11 Mitigation of Other Attacks   | Not Applicable        |

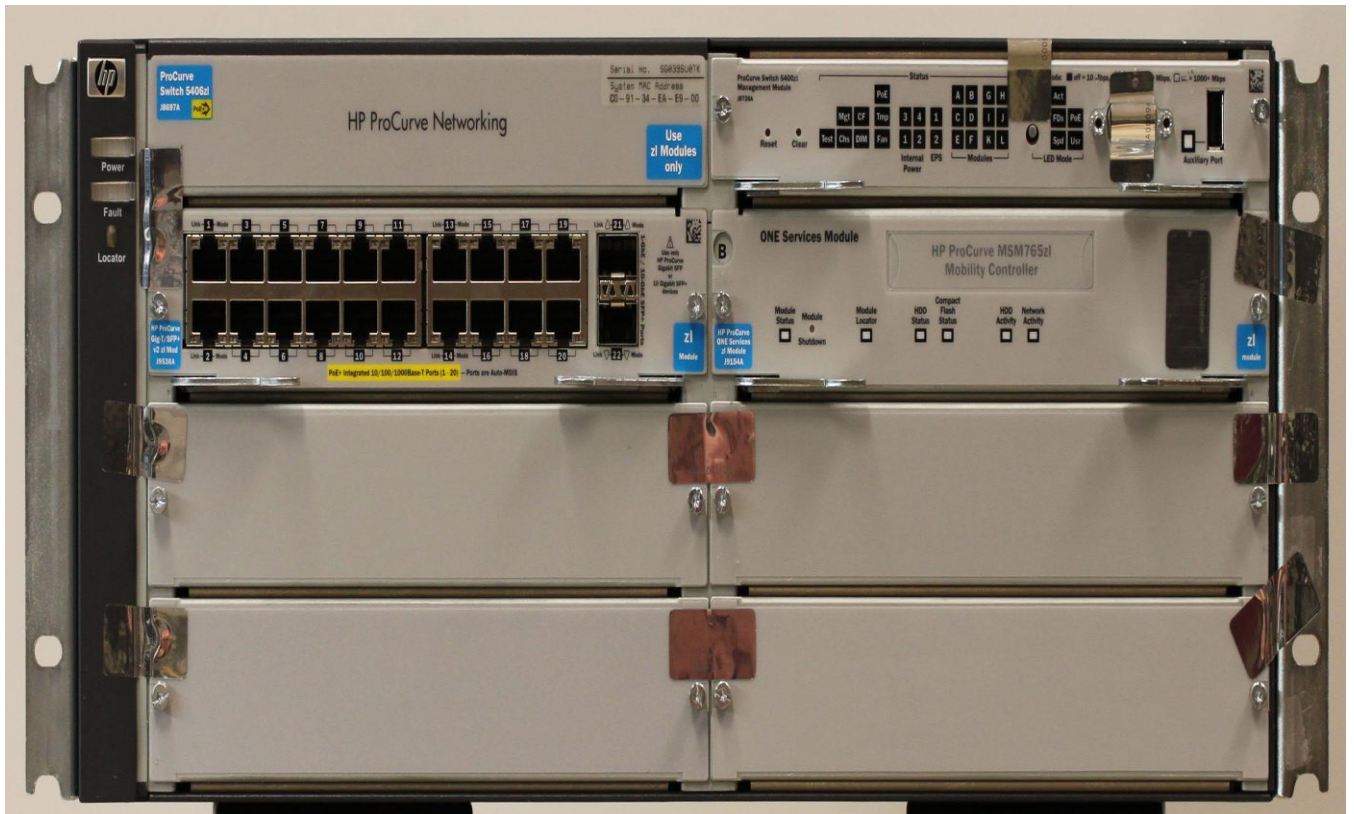
**Table 1 – FIPS 140-2 Section Targeted Security Levels**



## 2.2 PORTS AND INTERFACES

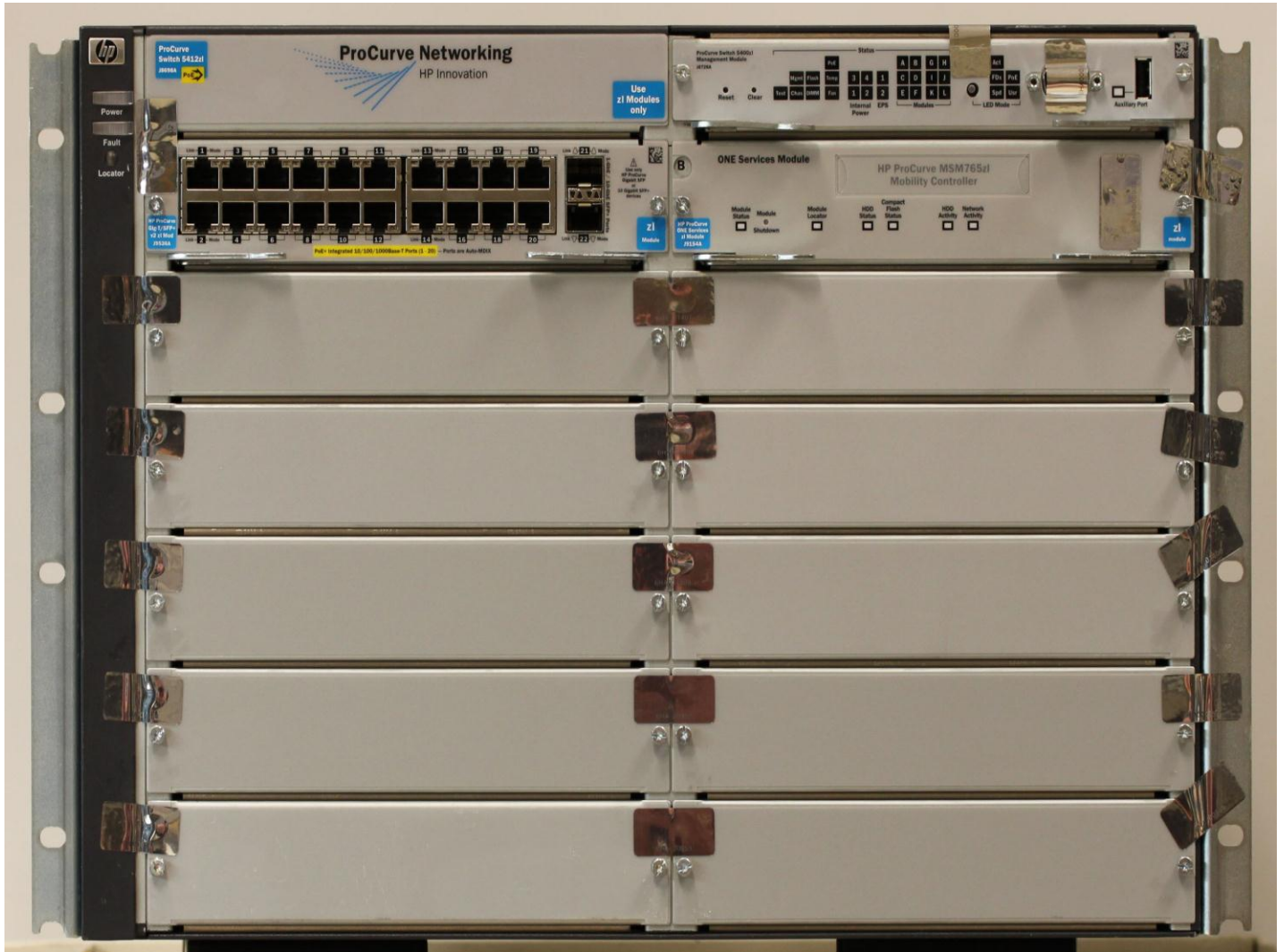
Figures 1 to 4 have photographs showing the fronts of each of each of the four cryptographic modules. The interfaces to the cryptographic modules can be seen in the photographs.

**Figure 1** shows the front of the HP 5406 zl Switch with the HP MSM765zl Mobility Controller.



**Figure 1 – HP 5406 zl Switch with the HP MSM765zl Mobility Controller**

**Figure 2** shows the front of the HP 5412 zl Switch with the HP MSM765zl Mobility Controller.



**Figure 2 – HP 5412 zl Switch with the HP MSM765zl Mobility Controller**

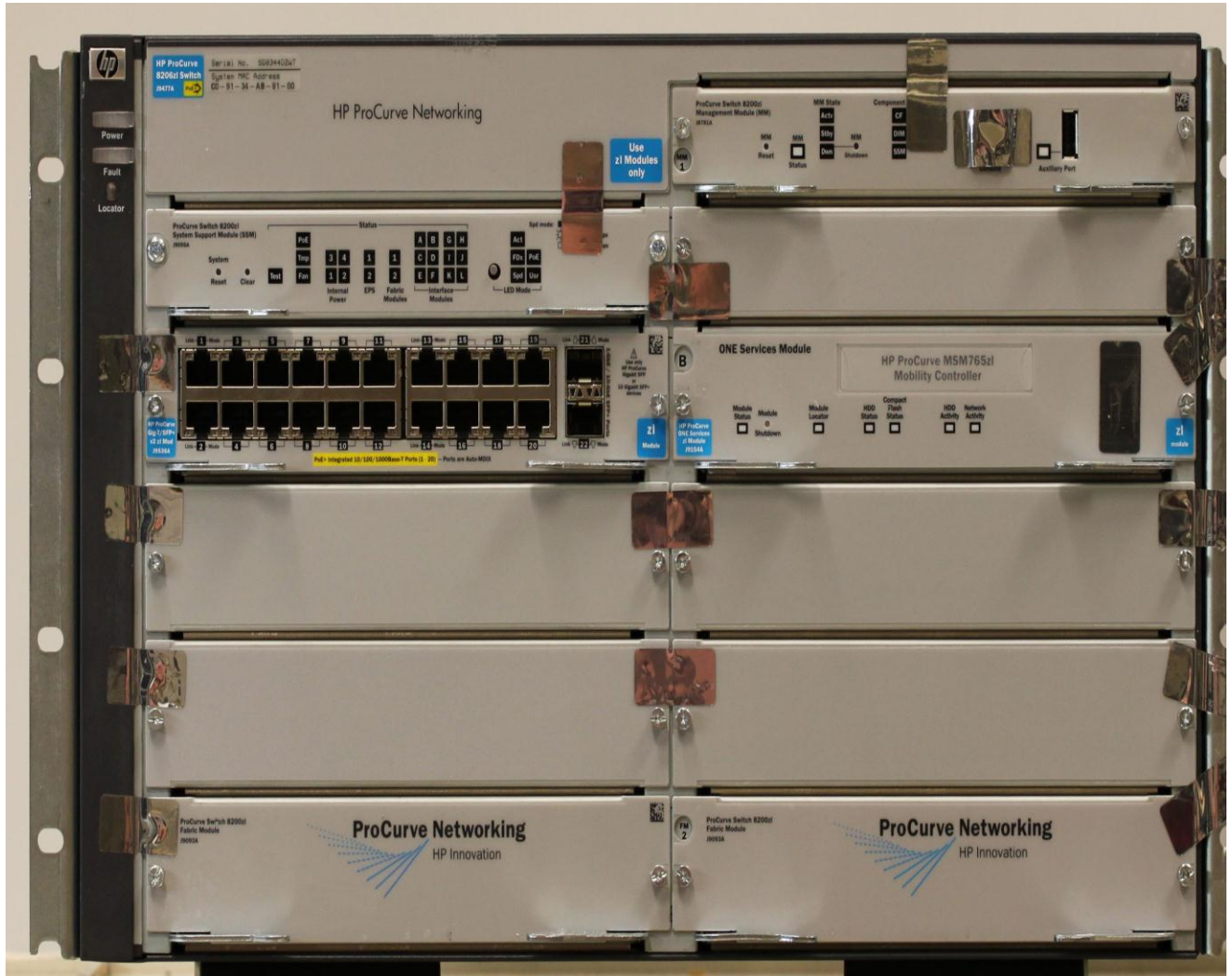


Figure 3 shows the front of the HP 8206 zl Switch with the HP MSM765zl Mobility Controller.



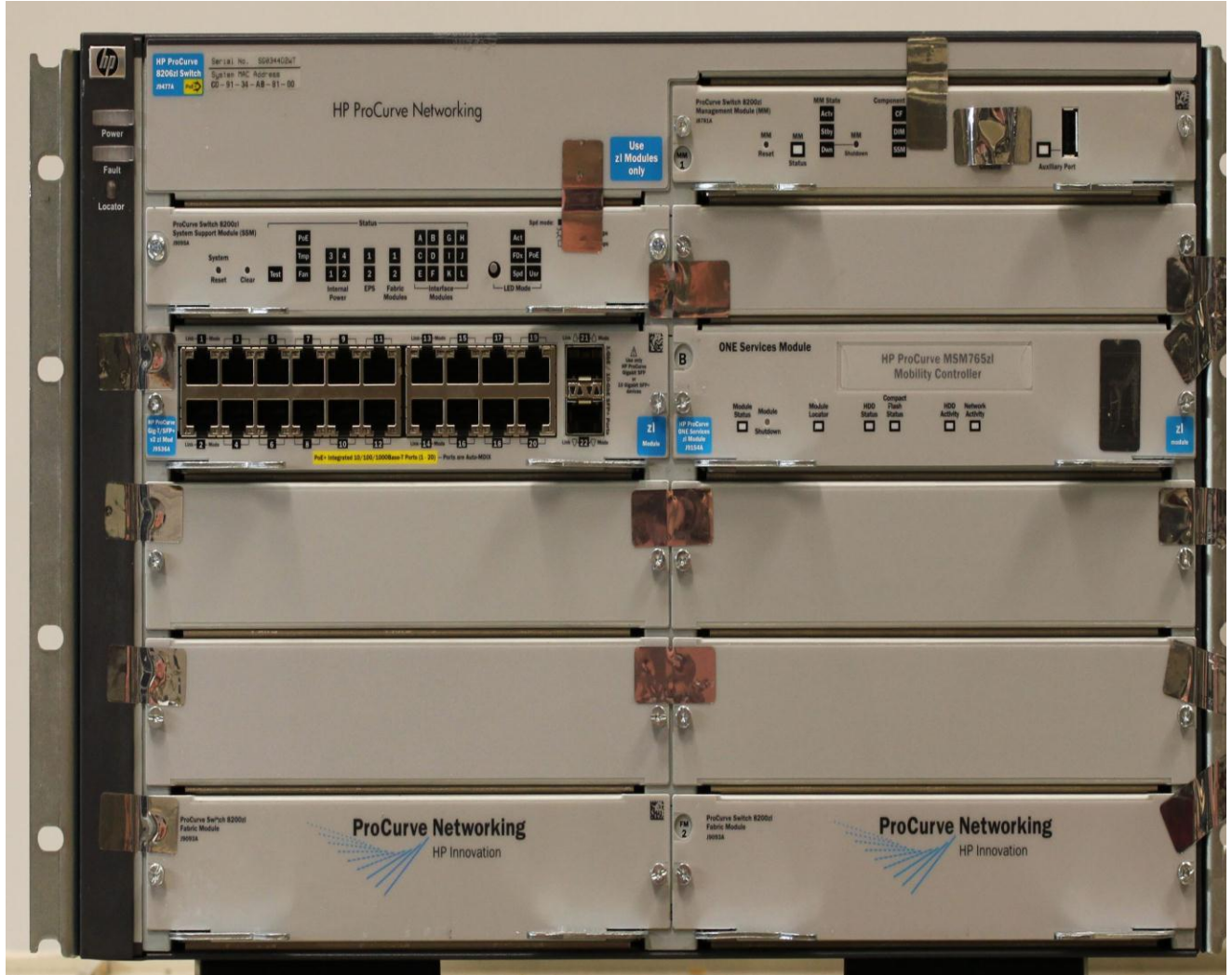


Figure 3 – HP 8206 zl Switch with the HP MSM765zl Mobility Controller



Figure 4 shows the front of the HP 8212 zl Switch with the HP MSM765zl Mobility Controller.



**Figure 4 – HP 8212 zl Switch with the HP MSM765zl Mobility Controller**

**Table 2** lists the interfaces and maps the interfaces specific to the HP MSM765zl Mobility Controller. **Table 3** specifies the interfaces for the rest of the HP 5406 zl and HP 5412 zl Switch with the HP MSM765zl Mobility Controller cryptographic modules and **Table 4** specifies the interfaces specific to the rest of the HP 8206 zl and HP 8212 zl Switch with the HP MSM765zl Mobility Controller cryptographic modules.



| Interface             | Type          | Direction                            | Description   | Related Hardware Port   |
|-----------------------|---------------|--------------------------------------|---|---|
| Cryptographic Control | Control Input | To HP MSM765zl Mobility Controller   | A web browser interface and CLI allows the Administrator to control the operation of the cryptographic module. The cryptographic module can also be controlled through a console connected to the switch. | Backplane mapped to Ethernet LAN Ports (SFP+ Ports); Backplane mapped to Serial Port                  |
| Cryptographic Status  | Status Output | From HP MSM765zl Mobility Controller | A web browser interface and/or CLI present the current status of the cryptographic module to the Administrator.   | Backplane mapped to Ethernet LAN Ports (SFP+ Ports); Backplane mapped to Serial Port                  |
| Operational Control   | Control Input | To HP MSM765zl Mobility Controller   | The shutdown switch causes the HP MSM765zl Mobility Controller to gracefully shut down. The device can also be controller through a web browser or a console.   | Shutdown Switch; Backplane mapped to Ethernet LAN Ports (SFP+ Ports); Backplane mapped to Serial Port |
| Operational Status    | Status Output | From HP MSM765zl Mobility Controller | Operational status is presented on the front panel status LEDs. A web browser interface and/or CLI present the current status of the HP MSM765zl Mobility Controller to the Administrator.                | 7 Status LEDs, Backplane mapped to Ethernet LAN Ports (SFP+ Ports); Backplane mapped to Serial Port   |
| Input Data            | Data Input    | To HP MSM765zl Mobility Controller   | Access Points are allowed to send data to the HP MSM765zl Mobility Controller over the Input Data interface.  | Backplane mapped to Ethernet LAN Ports (SFP+ Ports)   |
| Output Data           | Data Output   | From HP MSM765zl Mobility Controller | The HP MSM765zl Mobility Controller outputs data from Access Points over the Output Data interface.   | Backplane mapped to Ethernet LAN Ports (SFP+ Ports)   |

**Table 2 – Logical Interfaces Specific to the HP MSM765zl Mobility Controller**



| Interface           | Type  | Direction                 | Ports  |
|---------------------|---|---------------------------|--|
| Operational Control | Control Input   | To Cryptographic Module   | 1 RS-232 DB9 Serial Port (to be covered with tamper evident seal)<br>1 Push Button<br><br>20 RJ45 Gig-T PoE+ Ports   |
| Operational Status  | Status Output   | From Cryptographic Module | 1 RS-232 DB9 Serial Port (to be covered with tamper evident seal)<br>32 LEDs on Management Module<br><br>20 RJ45 Gig-T PoE+ Ports<br>2 SFP+ Ports<br>44 LEDs (around ports) on Line Card<br><br>2 LEDs on Internal Power Supply (back of HP 5406 zl Switch only – single power supply)<br>4 LEDs on Internal Power Supplies (back of HP 5412 zl Switch only – two power supplies)<br><br>3 LEDs on Status Panel on Chassis<br><br>3 LEDs on High Performance Fan Tray<br><br>(84 LEDs in total for HP 5406 zl Switch cryptographic module and 86 LEDs in total for HP 5412 zl Switch cryptographic module) |
| Input Data          | Data Input  | To Cryptographic Module   | 1 RS-232 DB9 Serial Port (to be covered with tamper evident seal)<br><br>20 RJ45 Gig-T PoE+ Ports<br>2 SFP+ Ports  |
| Output Data         | Data Output (disabled in the FIPS approved mode of operation) | From Cryptographic Module | 1 RS-232 DB9 Serial Port (to be covered with tamper evident seal)<br><br>20 RJ45 Gig-T PoE+ Ports<br>2 SFP+ Ports  |
| Power Interface     | Power Input   | To Cryptographic Module   | 1 AC Power Socket (HP 5406 zl Switch)<br>2 AC Power Sockets (HP 5412 zl Switch)<br><br>2 PoE Power Connectors  |



| Interface       | Type         | Direction                 | Ports                    |
|-----------------|--------------|---------------------------|--------------------------|
| Power Interface | Power Output | From Cryptographic Module | 20 RJ45 Gig-T PoE+ Ports |

**Table 3 – Ports for the Rest of the HP 5406 zl Switch with the HP MSM765zl Mobility Controller and the HP 5412 zl Switch with the HP MSM765zl Mobility Controller Cryptographic Modules**

| Interface           | Type          | Direction                 | Ports   |
|---------------------|---------------|---------------------------|---|
| Operational Control | Control Input | To Cryptographic Module   | 1 RS-232 RJ45 Serial Port (to be covered with tamper evident seal)<br>1 Push Button<br><br>20 RJ45 Gig-T PoE+ Ports   |
| Operational Status  | Status Output | From Cryptographic Module | 1 RS-232 RJ45 Serial Port (to be covered with tamper evident seal)<br>16 LEDs on Management Module<br><br>29 LEDs on System Support Module<br><br>20 RJ45 Gig-T PoE+ Ports<br>2 SFP+ Ports<br>44 LEDs (around ports) on Line Card<br><br>2 LEDs on Internal Power Supply (back of HP 8206 zl Switch only – single power supply)<br>4 LEDs on Internal Power Supplies (back of HP 8212 zl Switch only – two power supplies)<br><br>3 LEDs on Status Panel on Chassis<br><br>3 LEDs on High Performance Fan Tray<br><br>(97 LEDs in total for HP 8206 zl Switch cryptographic module and 99 LEDs in total for HP 8212 zl Switch cryptographic module) |



| Interface       | Type  | Direction                       | Ports   |
|-----------------|---|---------------------------------|---|
| Input Data      | Data Input  | To<br>Cryptographic<br>Module   | 1 RS-232 RJ45 Serial Port (to be covered with<br>tamper evident seal)<br><br>20 RJ45 Gig-T PoE+ Ports<br>2 SFP+ Ports |
| Output Data     | Data Output<br>(disabled in the<br>FIPS approved<br>mode of<br>operation) | From<br>Cryptographic<br>Module | 1 RS-232 RJ45 Serial Port (to be covered with<br>tamper evident seal)<br><br>20 RJ45 Gig-T PoE+ Ports<br>2 SFP+ Ports |
| Power Interface | Power Input   | To<br>Cryptographic<br>Module   | 1 AC Power Socket (HP 8206 zl Switch)<br>2 AC Power Sockets (HP 8212 zl Switch)<br><br>2 PoE Power Connectors         |
| Power Interface | Power Output  | From<br>Cryptographic<br>Module | 20 RJ45 Gig-T PoE+ Ports  |

**Table 4 – Ports for the Rest of the HP 8206 zl Switch with the HP MSM765zl Mobility Controller and the HP 8212 zl Switch with the HP MSM765zl Mobility Controller Cryptographic Modules**

**2.3 OPACITY SHIELDS, HIGH PERFORMANCE FAN TRAYS, AND TAMPER EVIDENT SEALS**

This section describes where the opacity shields and high performance fan trays shall be installed and where the tamper evident seals shall be affixed for each of the cryptographic modules to meet Physical Security Level 2.

Placement of the shields, fan trays, and seals is specific to the switch. The HP part numbers for the opacity shields are as follows:

- J9710A      HP 5406 zl Opacity Shield Kit;
- J9711A      HP 5412 zl Opacity Shield Kit;
- J9712A      HP 8206 zl Opacity Shield Kit; and
- J9713A      HP 8212 zl Opacity Shield Kit.



A high performance fan tray is also required for each switch. The HP part numbers for the fan trays are as follows:

|        |   |
|--------|---|
| J9721A | HP 5406 zl High Performance Fan Tray;     |
| J9722A | HP 5412 zl High Performance Fan Tray;     |
| J9723A | HP 8206 zl High Performance Fan Tray; and |
| J9724A | HP 8212 zl High Performance Fan Tray.     |

Refer to the installation instructions accompanying each part for details on how to attach the opacity shields and high performance fan tray to the switch chassis.

**Please note that the configuration steps in section 3.2 FIPS Approved Mode of Operation, to functionally put the cryptographic module in the FIPS approved mode of operation, must be completed before installing the opacity shields and high performance fan trays and affixing the tamper evident seals.**

### 2.3.1 General Instructions for Tamper Evident Seals

The surface to which any seal is applied must be clean and dry. The backing material from the seal must be peeled away without touching the adhesive. (Fingers should not be used to directly peel the seals.)

Place each seal on the required location, applying very firm pressure across the entire surface of the seal. Thirty minutes are needed for the adhesive to cure. Tamper evidence may not be apparent before this time and the controller must not be placed into operation until the curing time has expired.

If additional seals are required, the HP part number is J9709A. This kit has 120 seals. Extra seals must be stored in a secure location, with access available only to authorized Administrators.

The tamper evident seals, opacity shields, and high performance fan tray shall be installed for the module to operate in a FIPS approved mode of operation.

### 2.3.2 Tamper Evident Seal Placement on the Switch Chassis

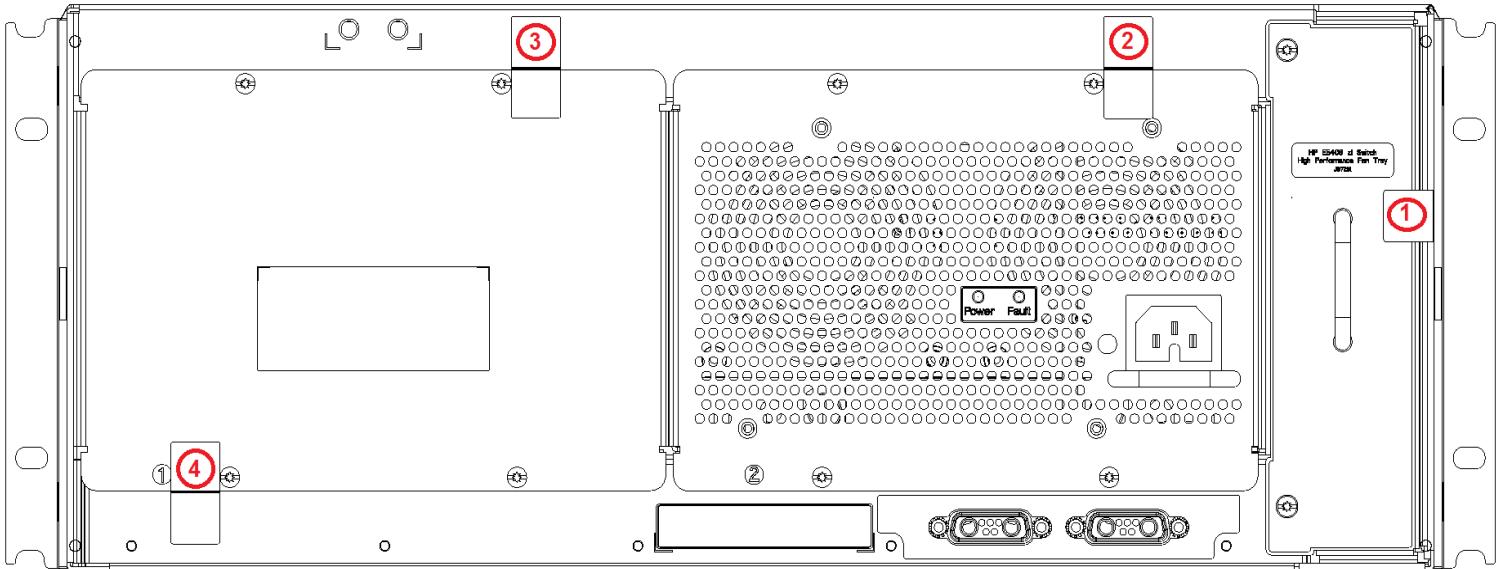
This section describes where to affix the tamper evident seals on the top, bottom, back, and sides of each Ethernet switch chassis. Instructions for the placement of seals on the front of the chassis are provided in the following section.



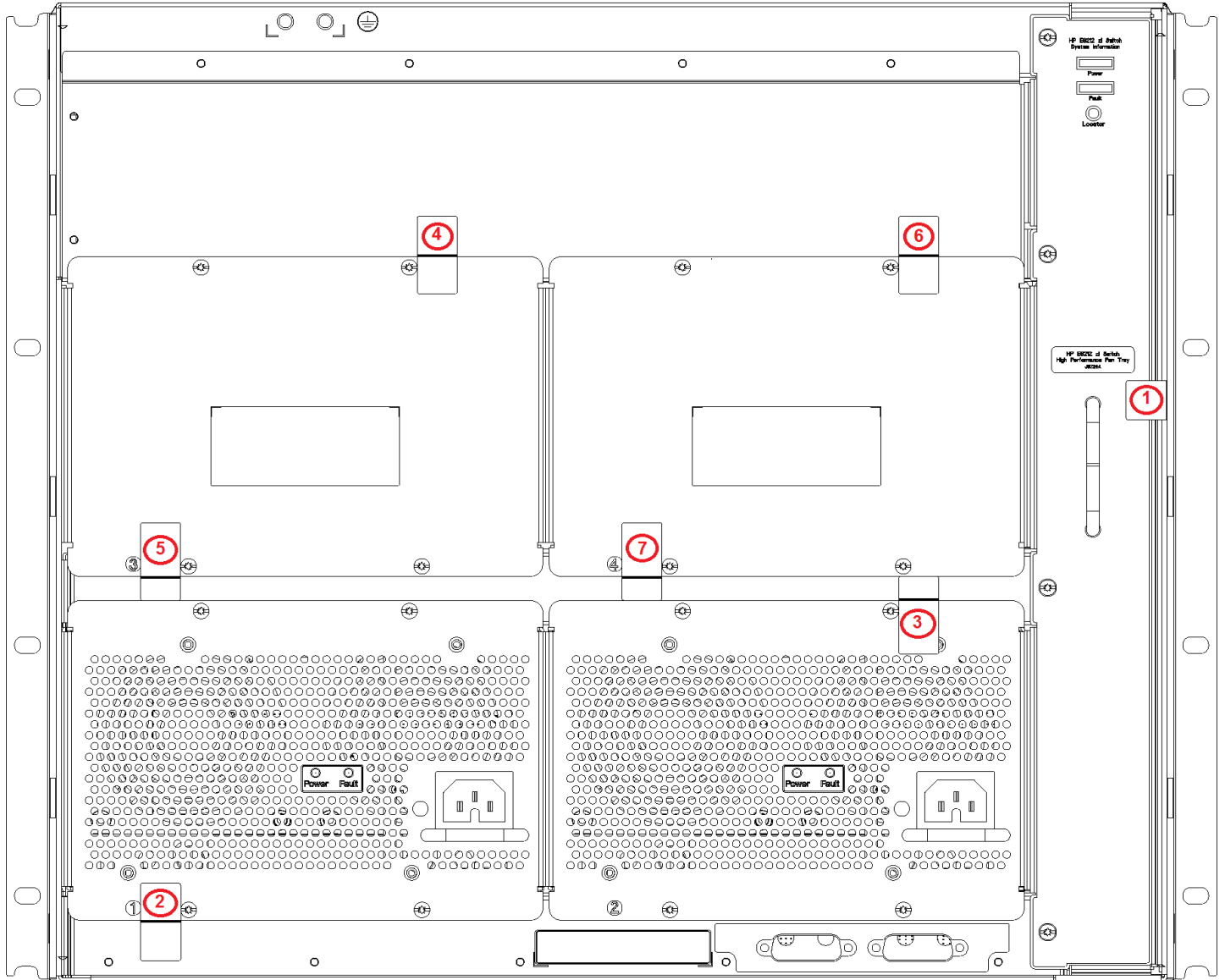


### 2.3.2.1 Chassis Back

- Secure High Performance Fan Tray to Chassis with one seal.
- Secure each Power Supply to Chassis with one seal.
- Secure each Power Supply Blank Cover to Chassis.
- Seals required:
  - HP 5406 z1 Switch: 4 tamper evident seals;
  - HP 5412 z1 Switch: 7 tamper evident seals;
  - HP 8206 z1 Switch: 4 tamper evident seals; and
  - HP 8212 z1 Switch: 7 tamper evident seals.



**Figure 5 – Tamper Evident Seal Placement on Back of 5406 z1 Chassis or 8206 z1 Chassis**



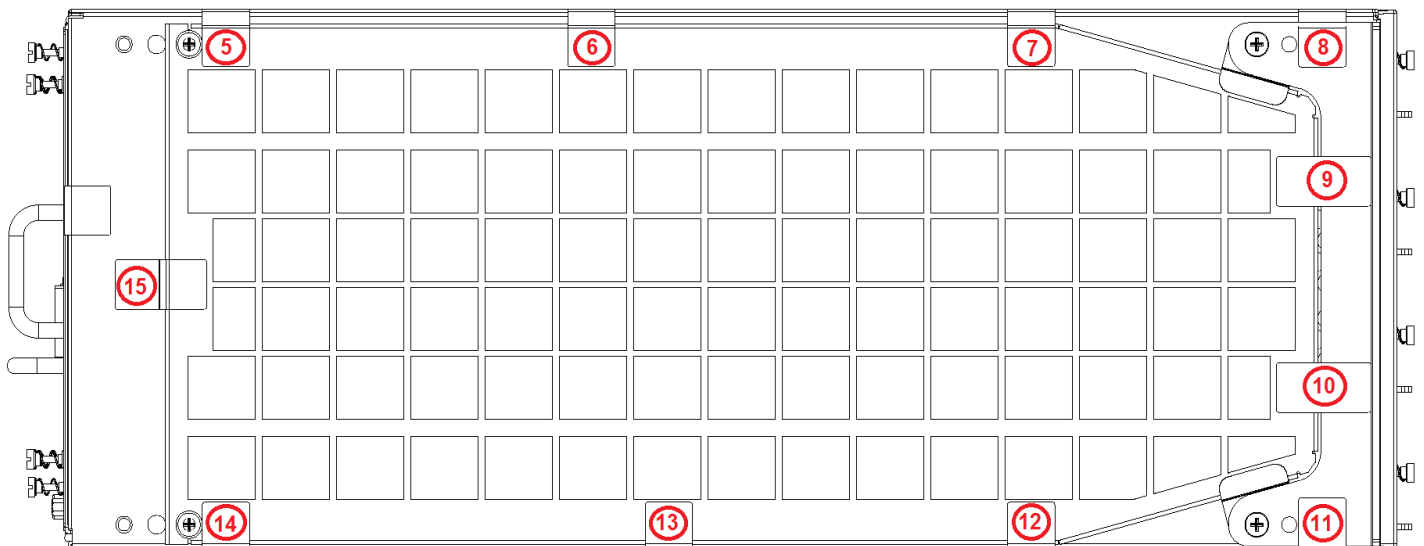
**Figure 6 – Tamper Evident Seal Placement on Back of 5412 zl Chassis or 8212 zl Chassis**

2.3.2.2 Chassis Sides

- Peel adhesive release liner off of Shield Clips and adhere to Rack Mounting Brackets.
- Assemble Rack Mounting Brackets on Chassis with four screws on each side.
- Secure Rack Mounting Brackets to Chassis with two tamper evident seals on each side.
- Assemble Opacity Shield into Shield Clips and secure with two screws on each side.

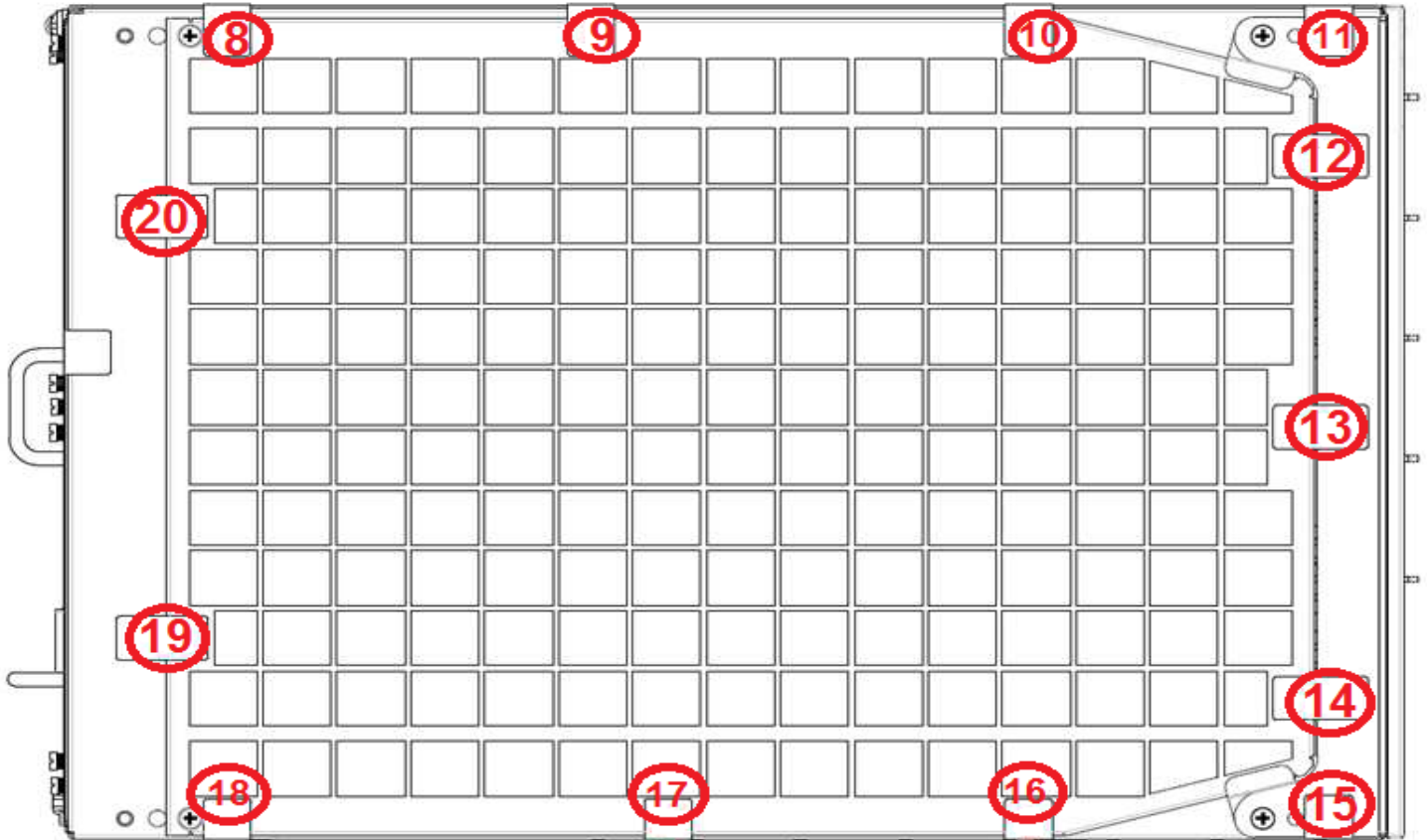


- Secure Opacity Shield to Chassis along top and bottom edges with six tamper evident seals on each side.
- Secure Opacity Shield to Chassis along front and rear edges with tamper evident seals at the shown locations on each side.
- Seals required to secure both left and right sides:
  - HP 5406 zl Switch: 22 tamper evident seals (seal numbers 5 to 26);
  - HP 5412 zl Switch: 26 tamper evident seals (seal numbers 8 to 33);
  - HP 8206 zl Switch: 24 tamper evident seals (seal numbers 5 to 28); and
  - HP 8212 zl Switch: 28 tamper evident seals (seal numbers 8 to 35).



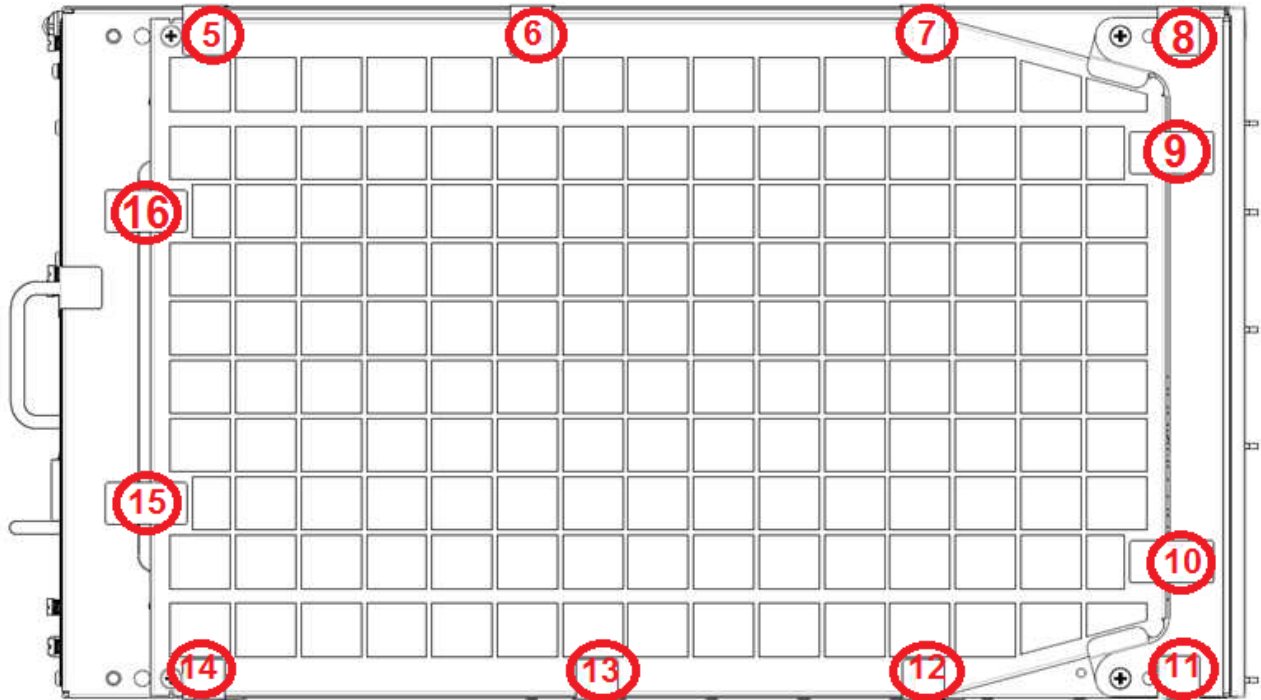
**Figure 7 – Tamper Evident Seal Placement on Side of HP 5406 zl Switch Chassis  
(11 Seals on this Side)**

The seal placement on the right side of the HP 5406 zl Switch Chassis is exactly the same as on the left side of the chassis which is shown in **Figure 7**. The seal numbers for the tamper evident seals on the right side of the HP 5406 zl Switch chassis are numbers 16 to 26 (11 tamper evident seals).



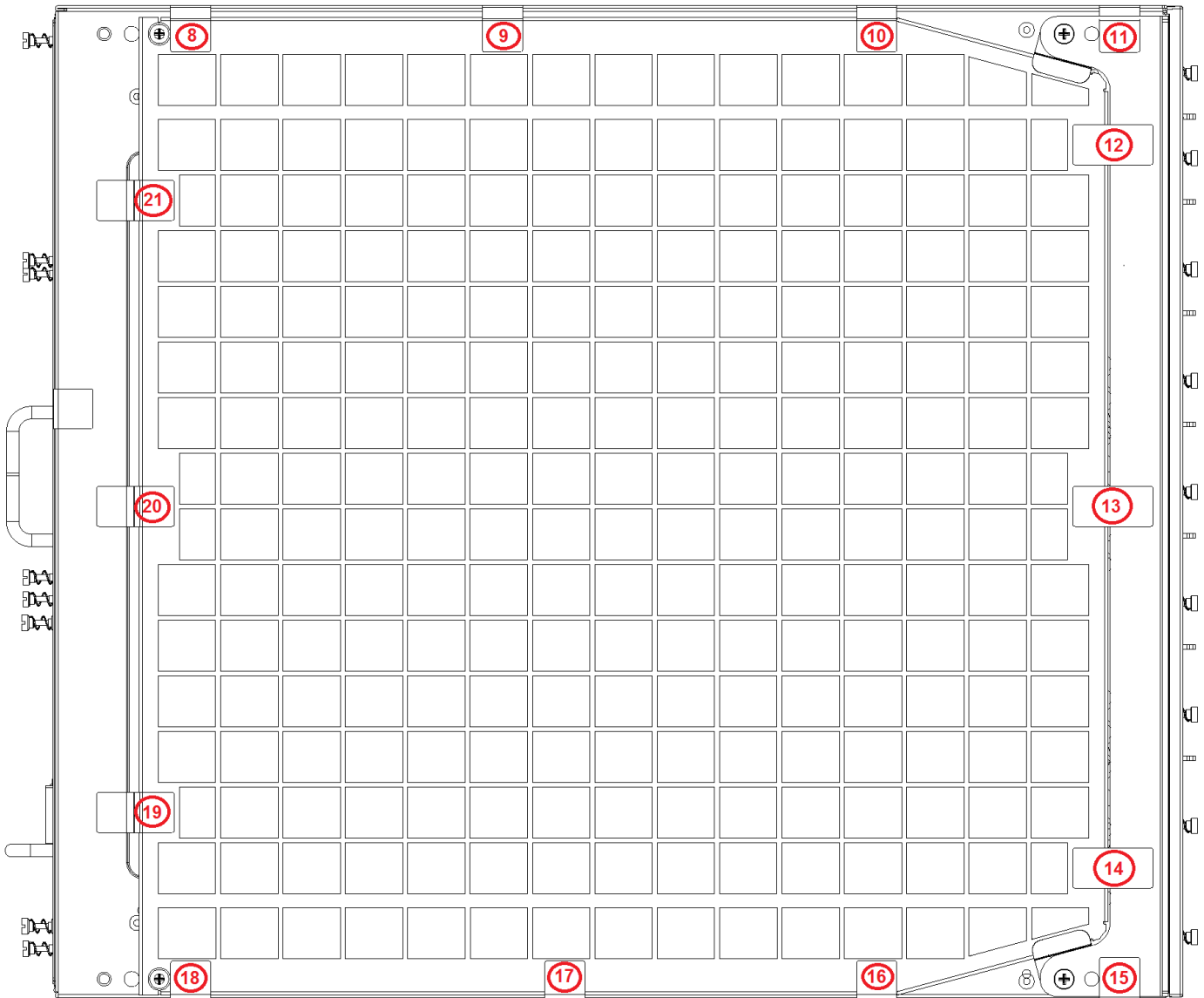
**Figure 8 – Tamper Evident Seal Placement on Side of HP 5412 zl Switch Chassis  
(13 Seals on this Side)**

The seal placement on the right side of the HP 5412 zl Switch Chassis is exactly the same as on the left side of the chassis which is shown in **Figure 8**. The seal numbers for the tamper evident seals on the right side of the HP 5412 zl Switch Chassis would be numbers 21 to 33 (13 tamper evident seals).



**Figure 9 – Tamper Evident Seal Placement on Side of HP 8206 zl Switch Chassis  
(12 Seals on this Side)**

The seal placement on the right side of the HP 8206 zl Switch Chassis is exactly the same as on the left side of the chassis which is shown in **Figure 9**. The seal numbers for the tamper evident seals on the right side of the HP 8206 zl Switch chassis would be numbers 17 to 28 (12 tamper evident seals).



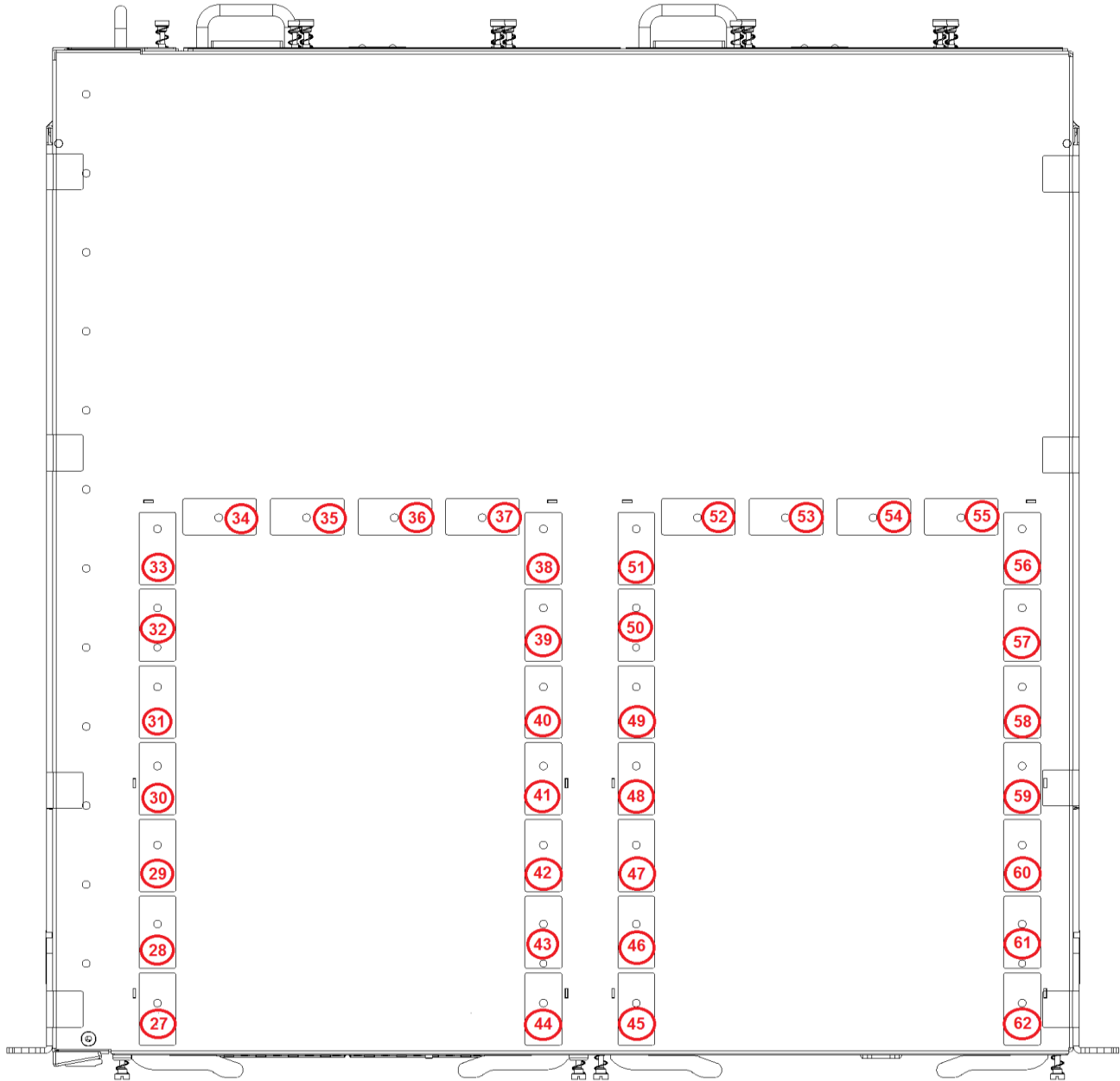
**Figure 10 – Tamper Evident Seal Placement on Side of HP 8212 zl Switch Chassis  
(14 Seals on this Side)**

The seal placement on the right side of the HP 8212 zl Switch Chassis is exactly the same as on the left side of the chassis which is shown in **Figure 10**. The seal numbers for the tamper evident seals on the right side of the HP 8212 zl Switch chassis would be numbers 22 to 35 (14 tamper evident seals).

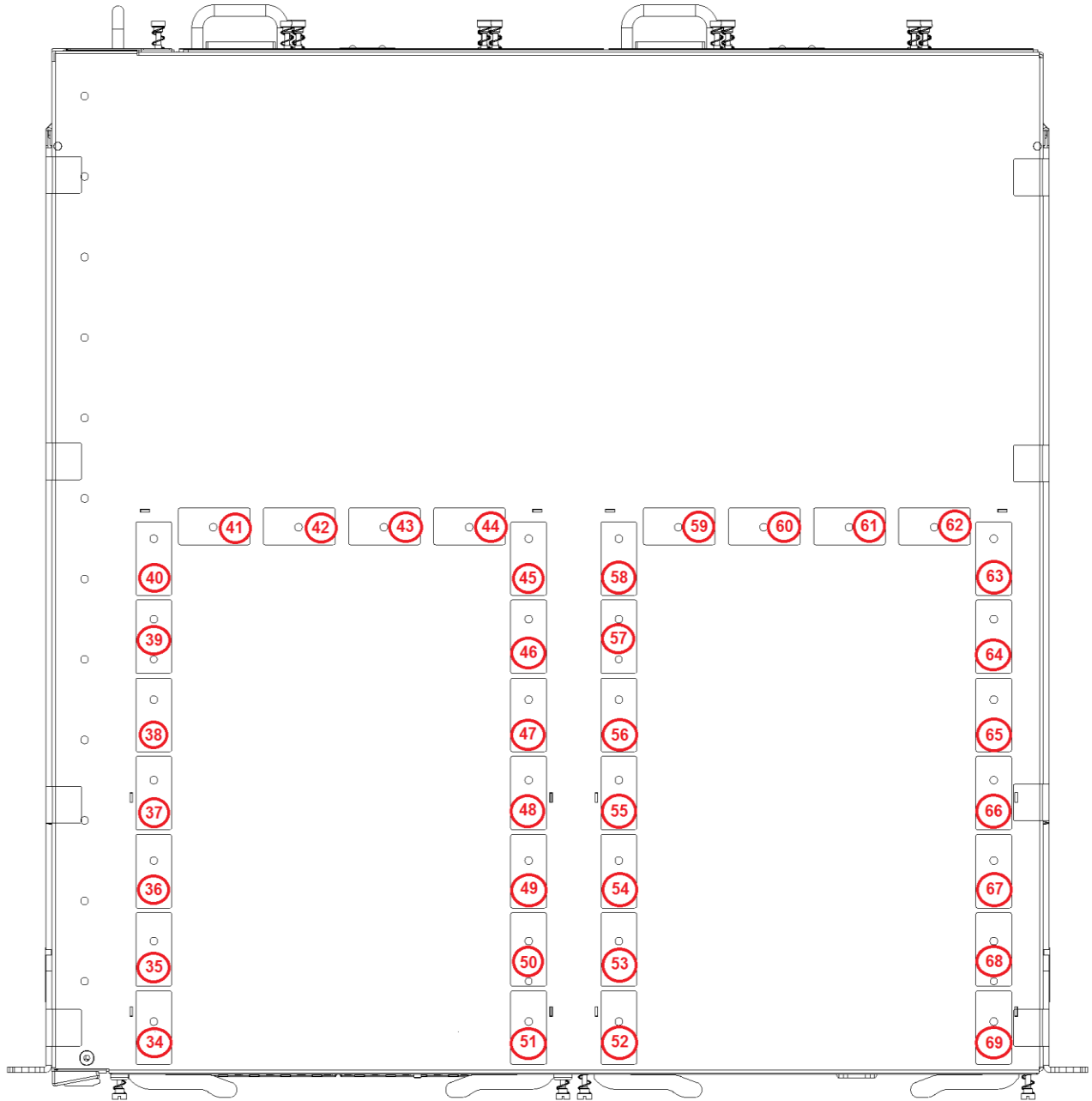


### 2.3.2.3 Chassis Top

- Tamper evident seals cover viewing holes.
- Tamper evident seals required: 36 tamper evident seals (same for each chassis).

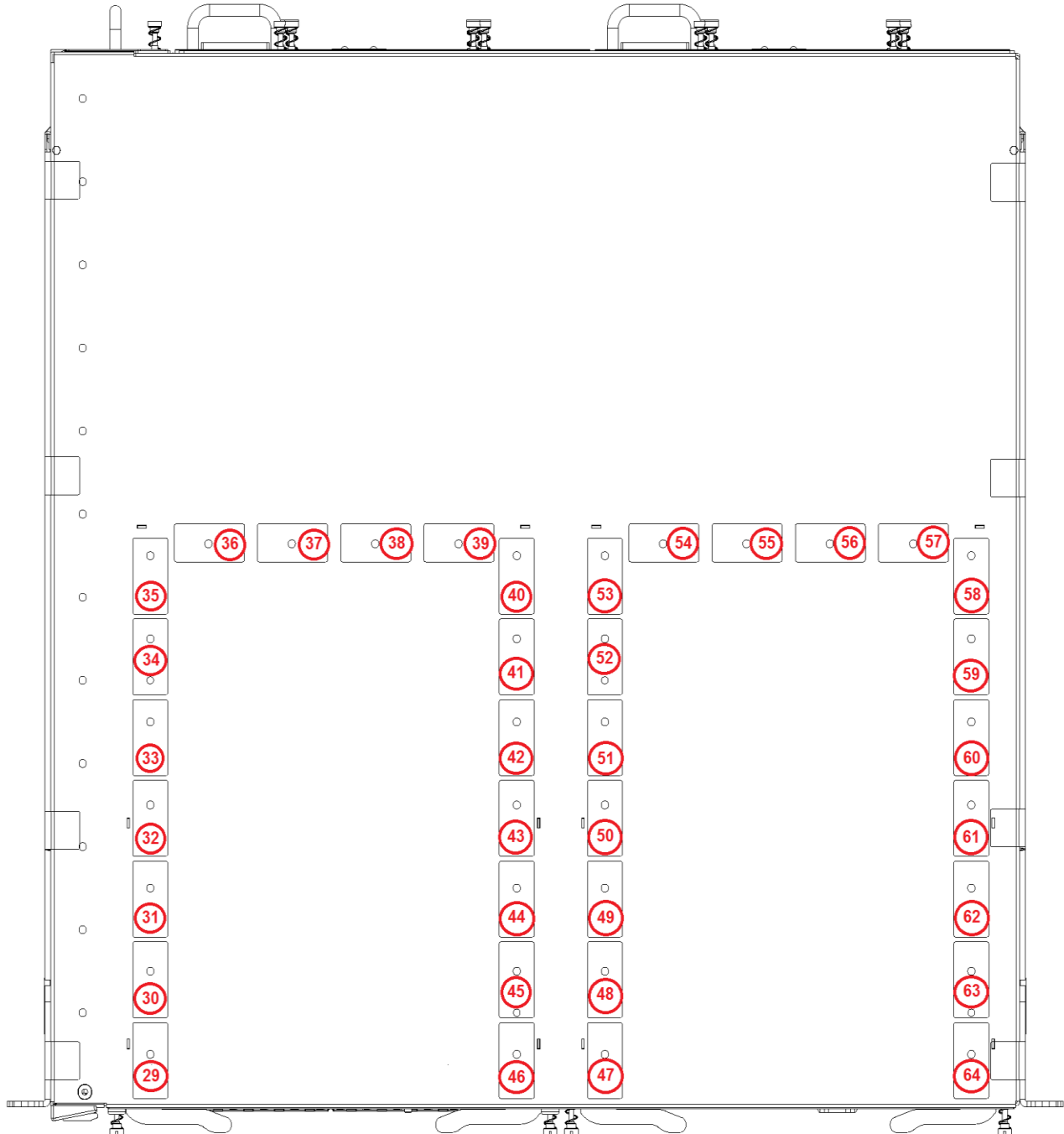


**Figure 11 – Tamper Evident Seal Placement on Top of HP 5406 zl Switch Chassis (18 Seals per Three-Quarter Rectangle)**

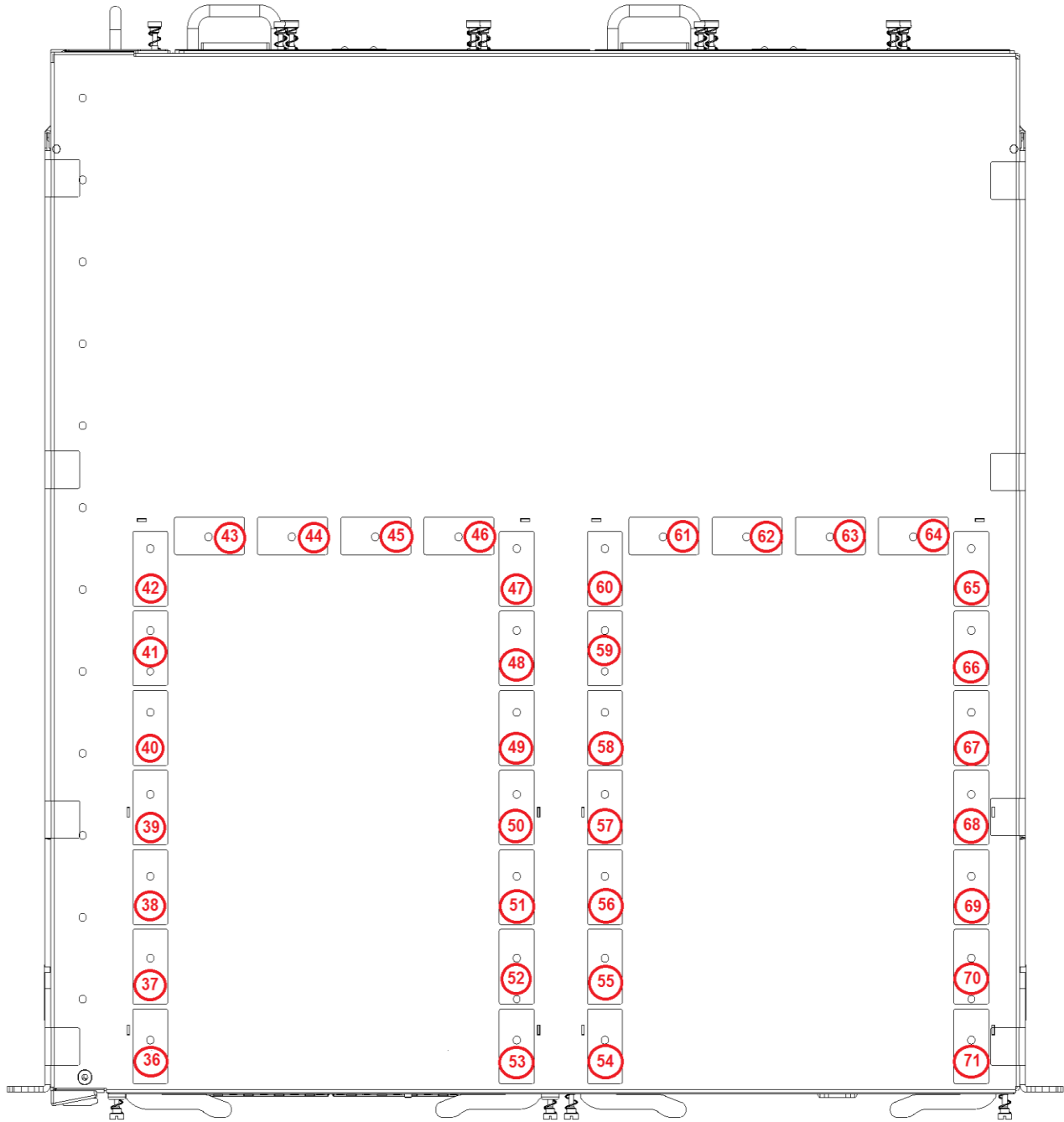


**Figure 12 – Tamper Evident Seal Placement on Top of HP 5412 zl Switch Chassis  
(18 Seals per Three-Quarter Rectangle)**





**Figure 13 – Tamper Evident Seal Placement on Top of HP 8206 zl Switch Chassis (18 Seals per Three-Quarter Rectangle)**

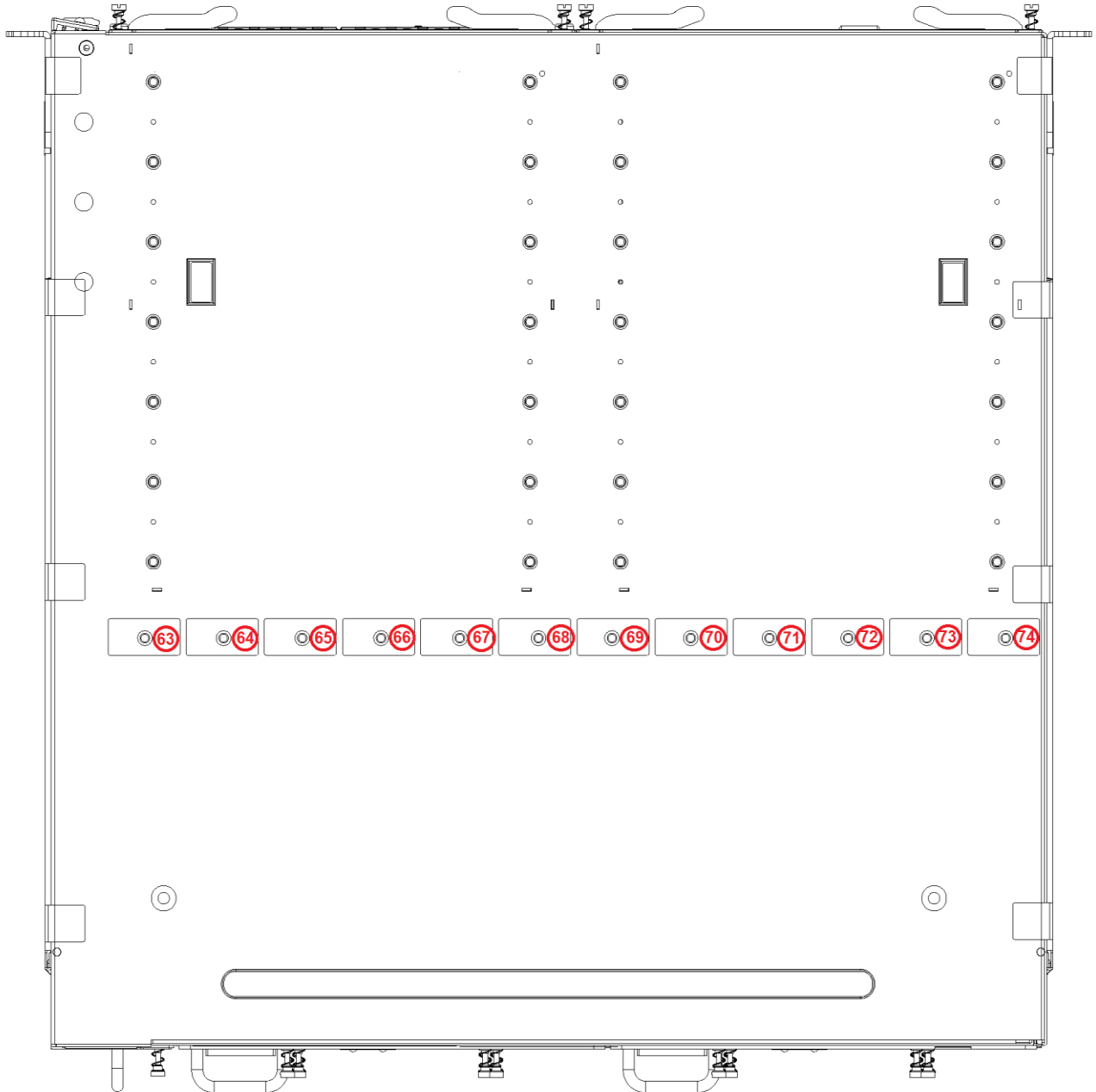


**Figure 14 – Tamper Evident Seal Placement on Top of HP 8212 zl Switch Chassis  
(18 Seals per Three-Quarter Rectangle)**

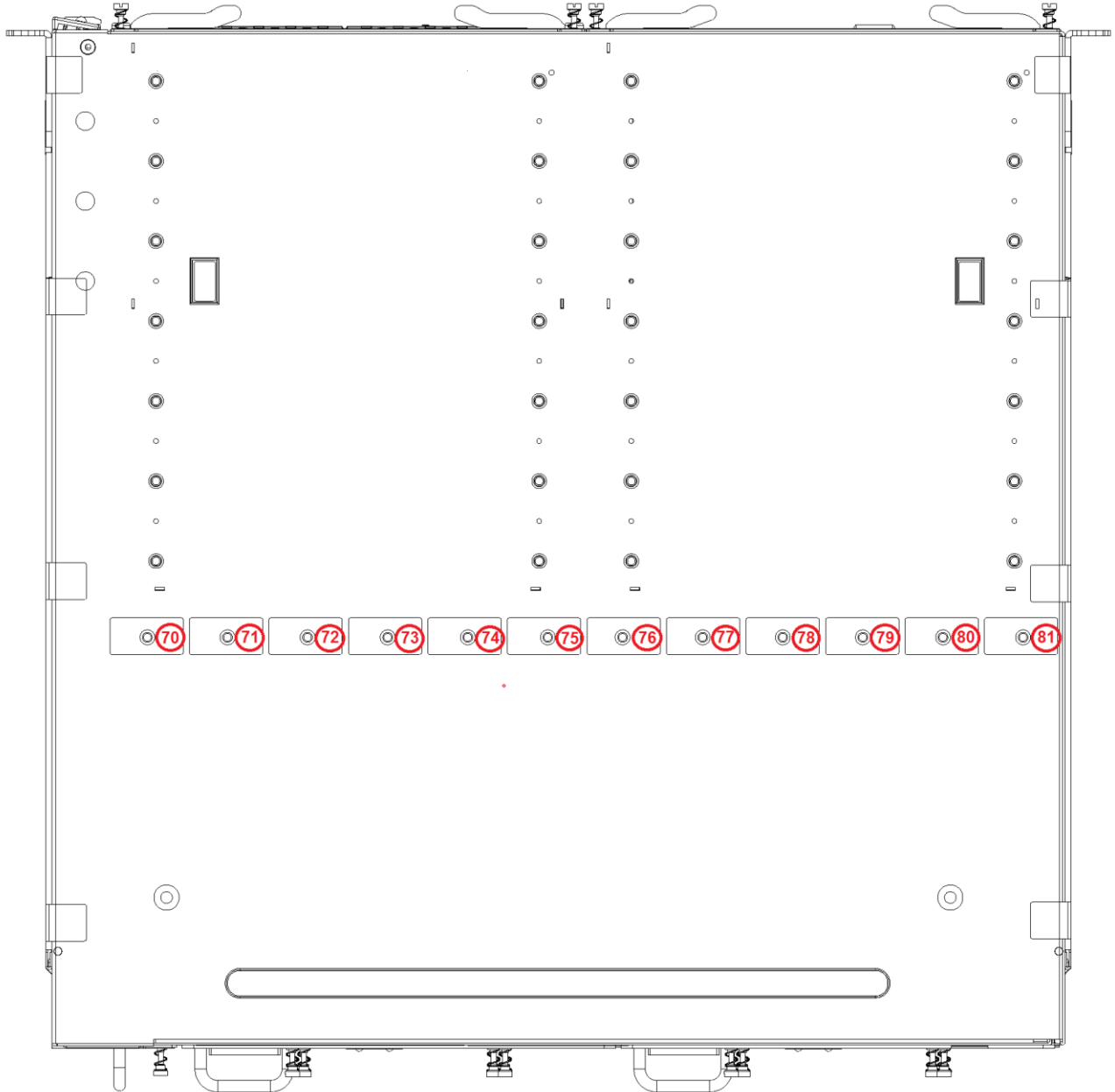


### 2.3.2.4 Chassis Bottom

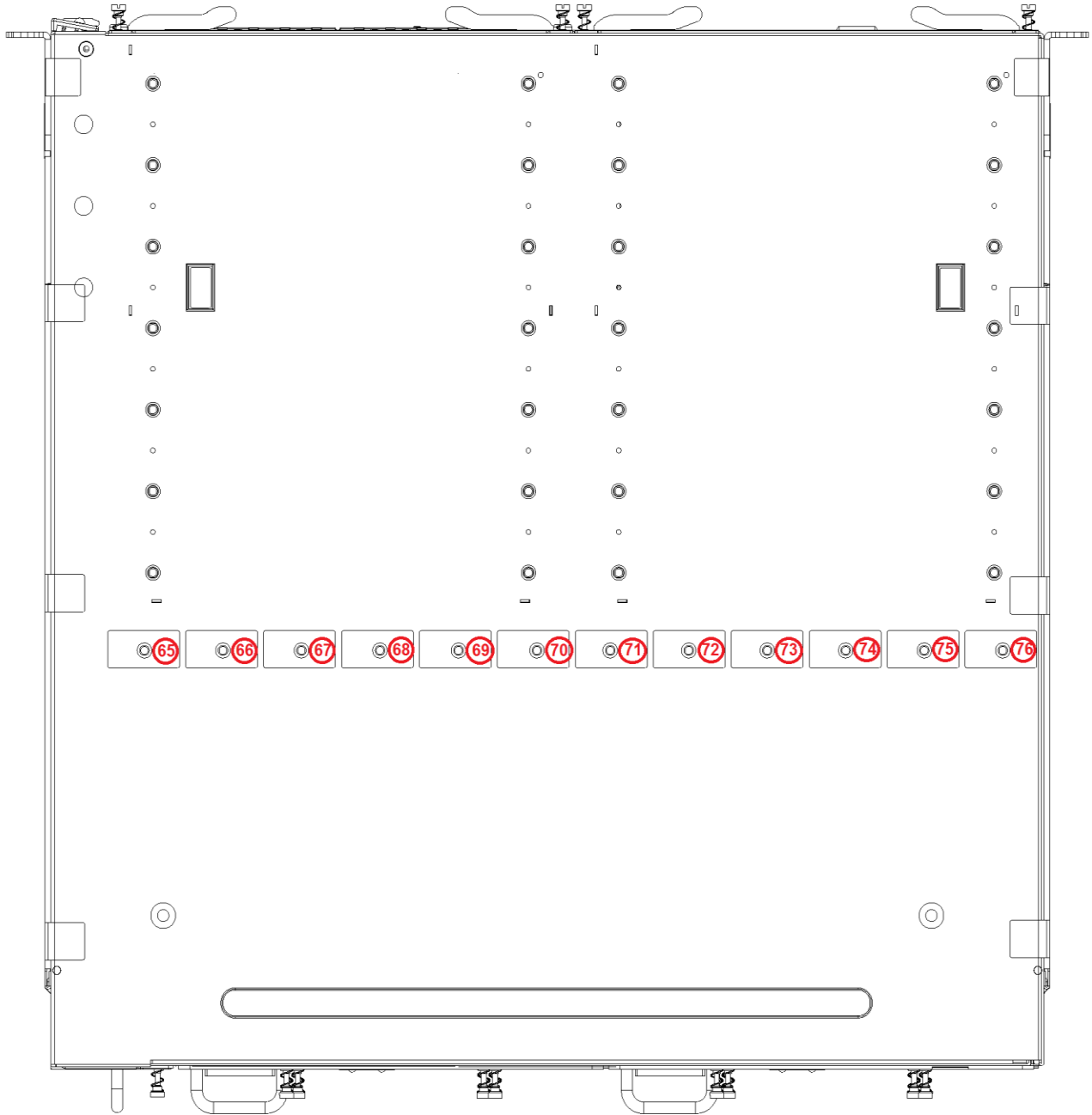
- Tamper evident seals cover viewing holes.
- Tamper evident seals required: 12 (same for each chassis).



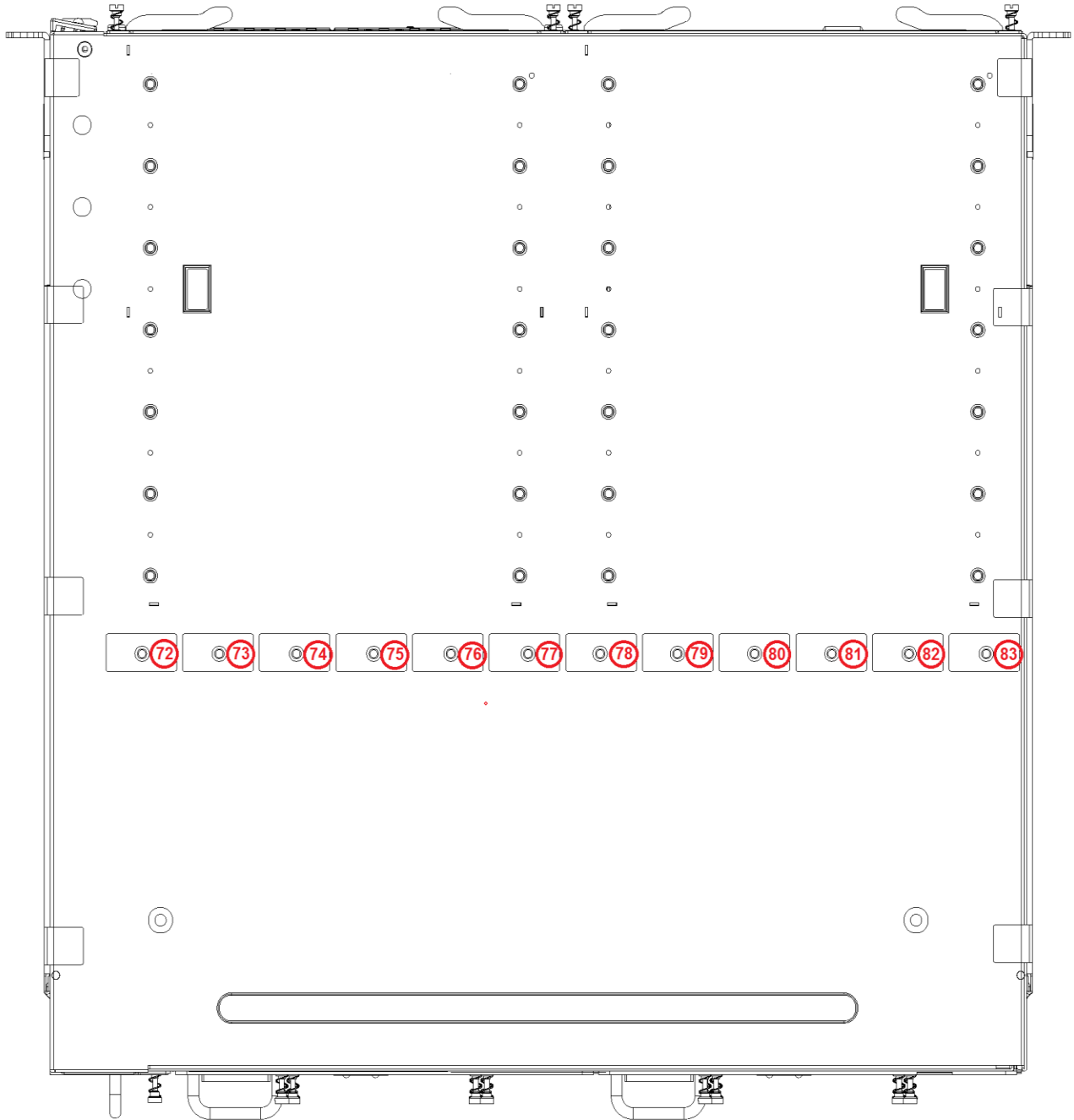
**Figure 15 – Tamper Evident Seal Placement on Bottom of HP 5406 zl Switch Chassis  
(12 Seals in Single Line)**



**Figure 16 – Tamper Evident Seal Placement on Bottom of HP 5412 zl Switch Chassis  
(12 Seals in Single Line)**



**Figure 17 – Tamper Evident Seal Placement on Bottom of HP 8206 zl Switch Chassis  
(12 Seals in Single Line)**

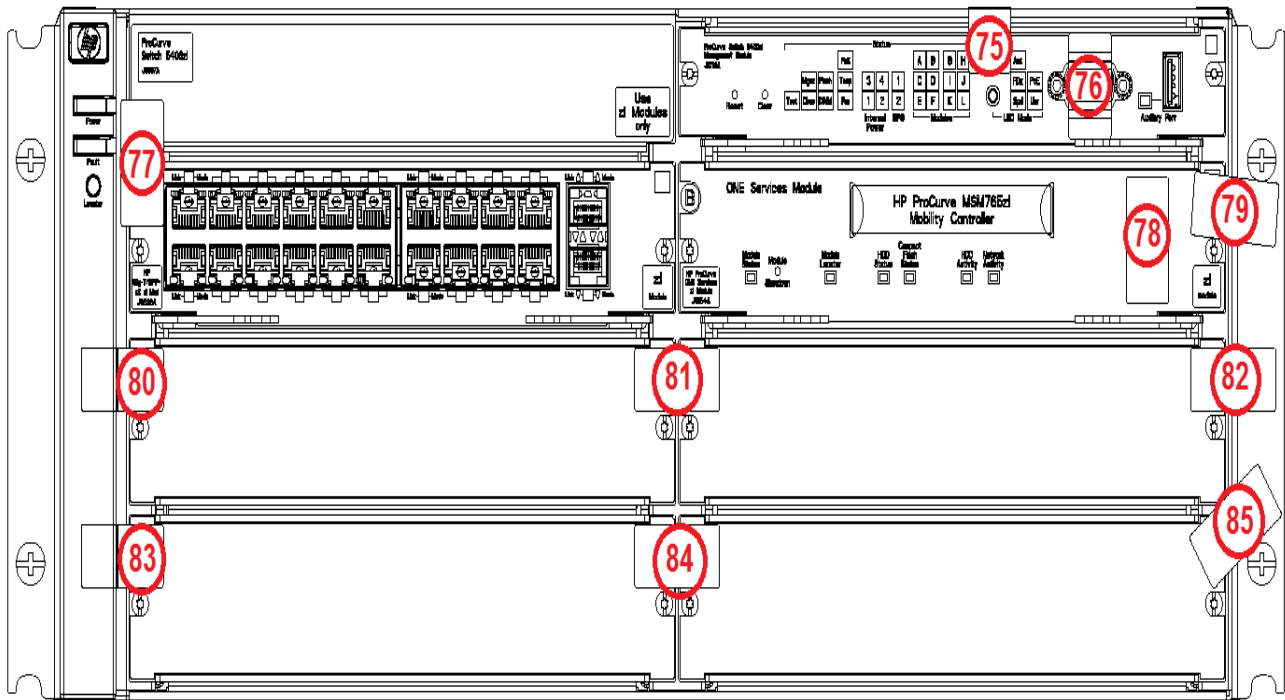


**Figure 18 – Tamper Evident Seal Placement on Bottom of HP 8212 zl Switch Chassis  
(12 Seals in Single Line)**



## 2.4 TAMPER EVIDENT SEAL PLACEMENT ON CHASSIS FRONT AND INSTALLED MODULES

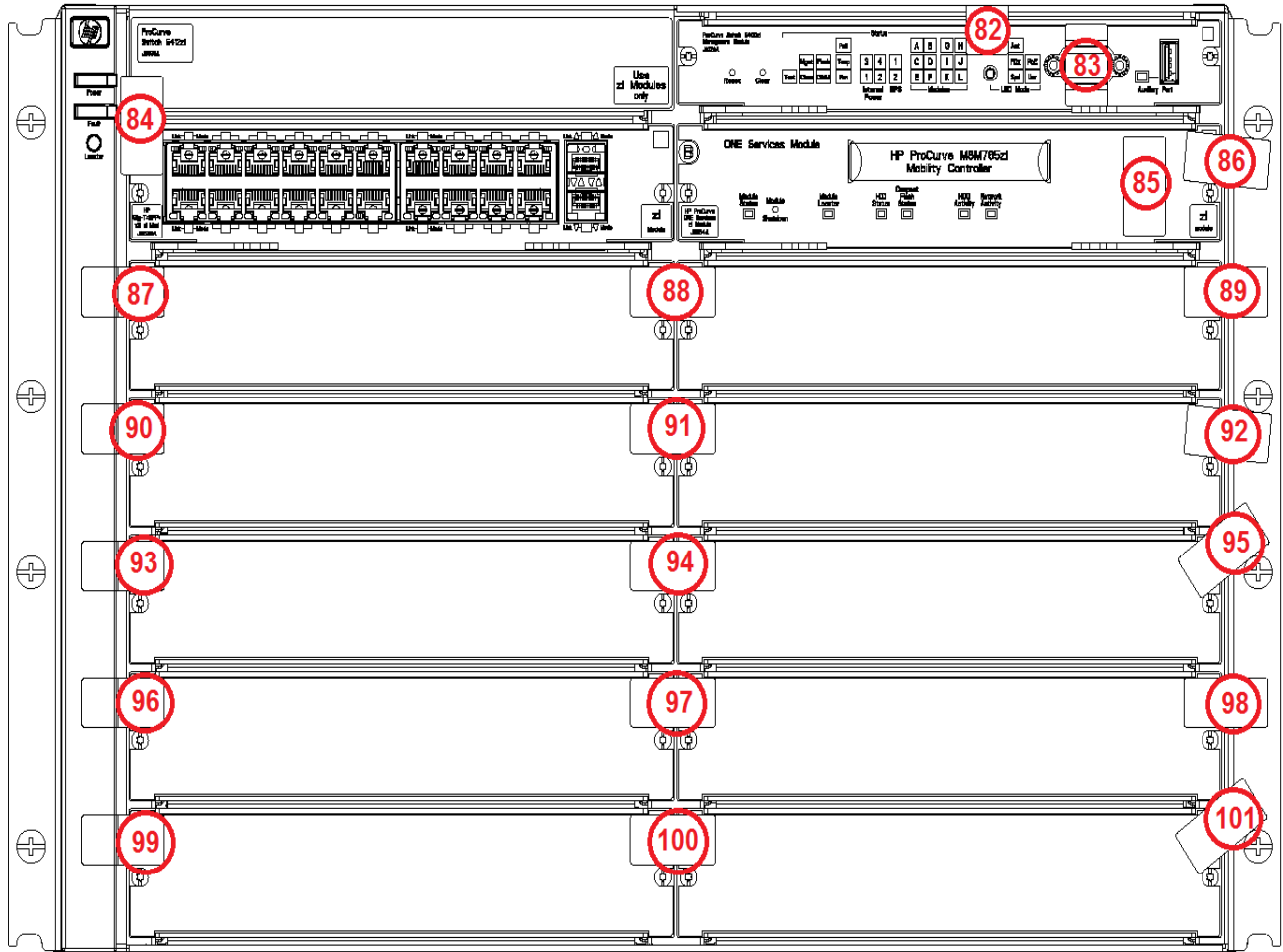
This section provides instructions on the placement of tamper evident seals on the front of the chassis including installed modules and blank slot covers. Please note that tamper evident seals on the right side are to be applied at an angle to avoid rack mounting screws.



**Figure 19 – Placement of Tamper Evident Seals on Front of the HP 5406 zl Switch with the MSM765zl Mobility Controller (11 Seals)**

Please note that the Management Module is to be secured to the top of the chassis and the serial port on the Management Module is to be covered. Blank plates require tamper evident seals on both sides of the plate. The USB port on the MSM765zl Mobility Controller is to be covered with a tamper evident seal.

The HP 5406 zl Switch with the MSM765zl Mobility Controller requires a total of 85 tamper evident seals to meet the Physical Security Level 2 opacity requirements.

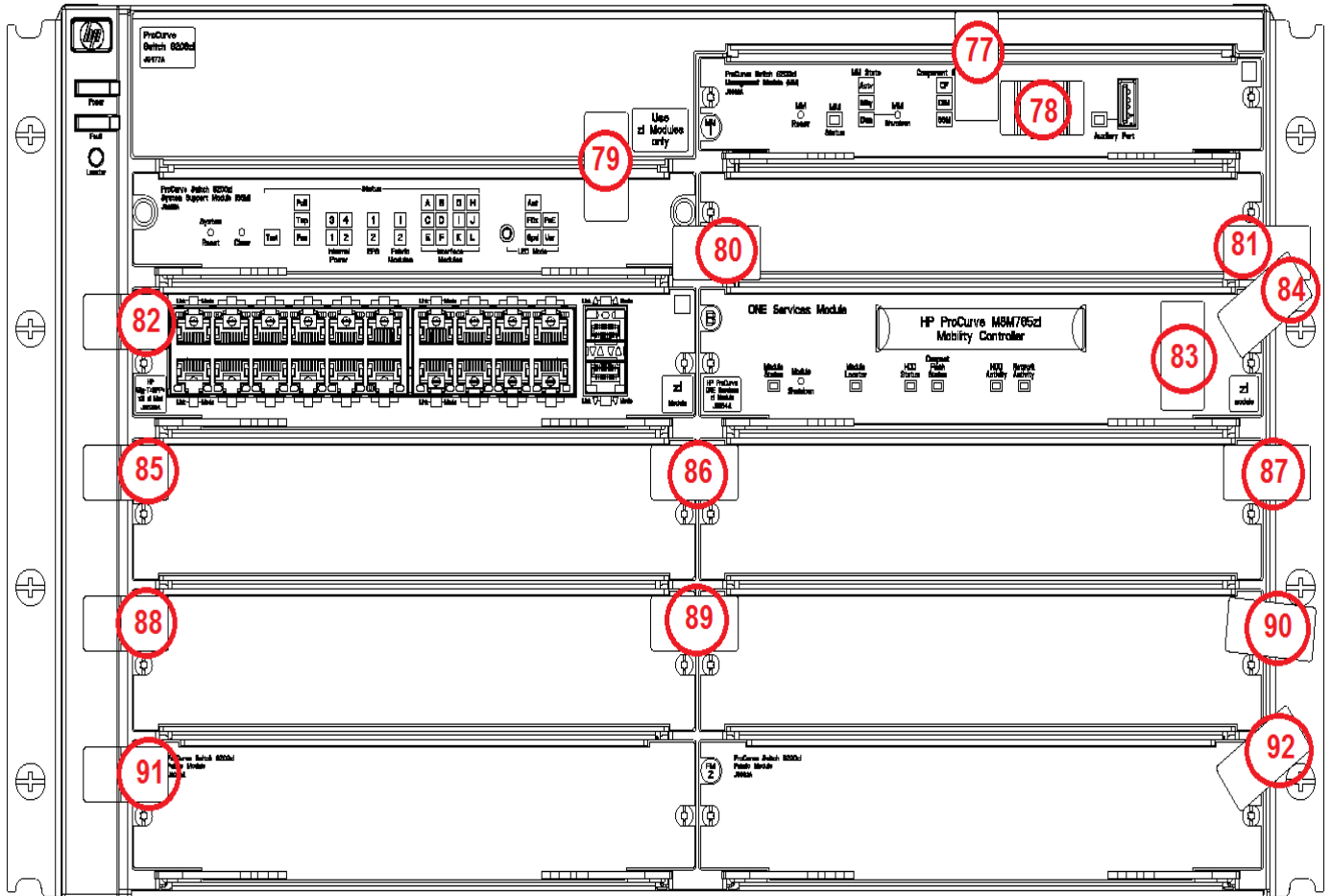


**Figure 20 – Placement of Tamper Evident Seals on Front of the HP 5412 zL Switch with the MSM765zL Mobility Controller (20 Seals)**

Please note that the Management Module is to be secured to the top of the chassis and the serial port on the Management Module is to be covered. Blank plates require tamper evident seals on both sides of the plate. The USB port on the MSM765zL Mobility Controller is to be covered with a tamper evident seal.

The HP 5412 zL Switch with the MSM765zL Mobility Controller requires a total of 101 tamper evident seals to meet the Physical Security Level 2 opacity requirements.

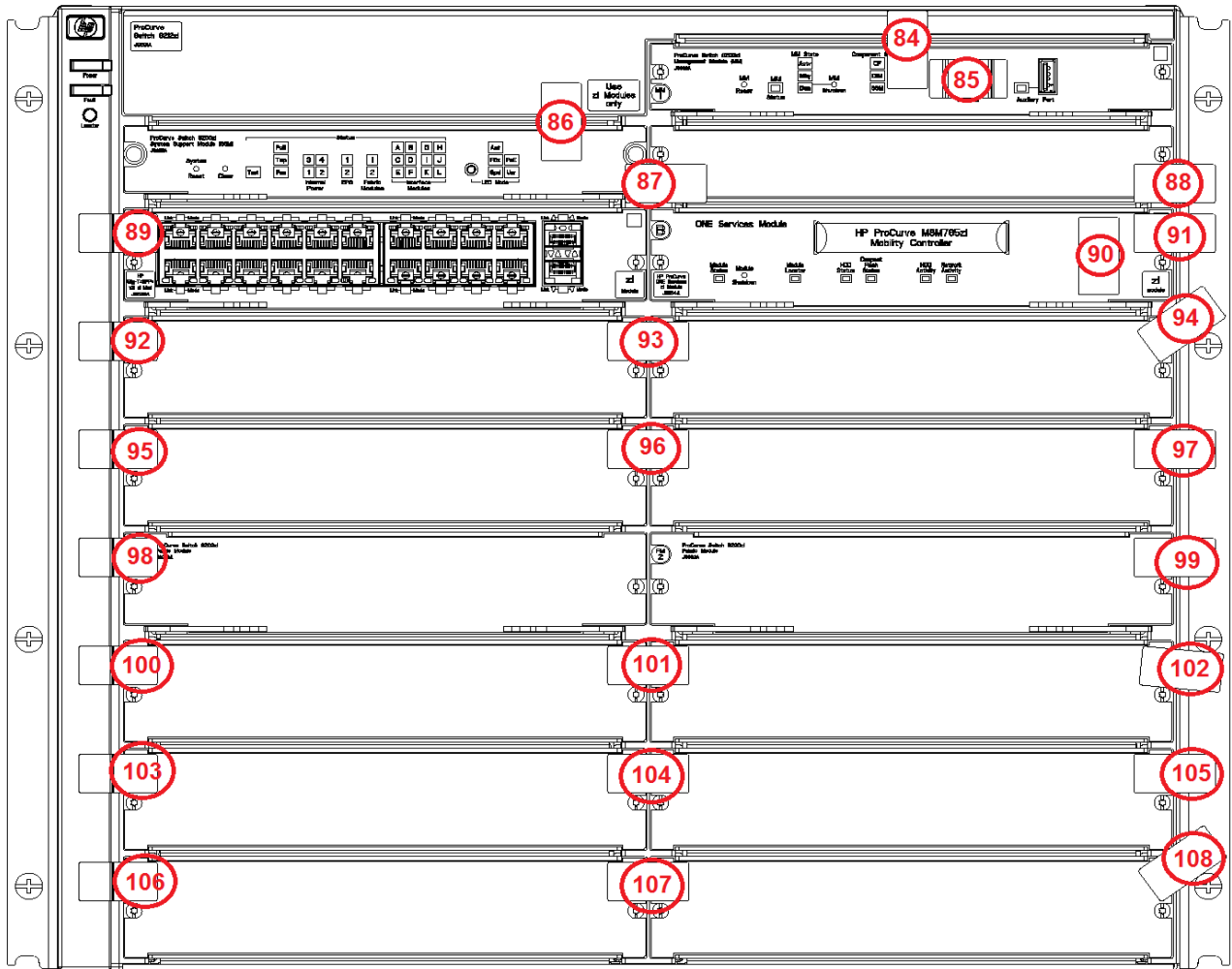




**Figure 21 – Placement of Tamper Evident Seals on Front of the HP 8206 zl Switch with the MSM765zl Mobility Controller (16 Seals)**

Please note that the Management Module is to be secured to the top of the chassis and the serial port on the Management Module is to be covered. The System Support Module requires a seal on its right side as well as a seal to secure it to the switch. Blank plates require tamper evident seals on both sides of the plate. The USB port on the MSM765zl Mobility Controller is to be covered with a tamper evident seal.

The HP 8206 zl Switch with the MSM765zl Mobility Controller requires a total of 92 tamper evident seals to meet the Physical Security Level 2 opacity requirements.



**Figure 22 – Placement of Tamper Evident Seals on Front of the HP 8212 zl Switch with the MSM765zl Mobility Controller (25 Seals)**

Please note that the Management Module is to be secured to the top of the chassis and the serial port on the Management Module is to be covered. The System Support Module requires a seal on its right side as well as a seal to secure it to the switch. Blank plates require tamper evident seals on both sides of the plate. The USB port on the MSM765zl Mobility Controller is to be covered with a tamper evident seal.

The HP 8212 zl Switch with the MSM765zl Mobility Controller requires a total of 108 tamper evident seals to meet the Physical Security Level 2 opacity requirements.



## **2.5 CRYPTOGRAPHIC MODULE BOUNDARY**

The cryptographic module boundary of the four cryptographic modules – the HP 5406 zl Switch with the HP MSM765zl Mobility Controller, the HP 5412 zl Switch with the HP MSM765zl Mobility Controller, the HP 8206 zl Switch with the HP MSM765zl Mobility Controller, and the HP 8212 zl Switch with the HP MSM765zl Mobility Controller – is the chassis of their respective switches, that is the following:

- the HP 5406 zl Switch Chassis for the HP 5406 zl Switch with the HP MSM765zl Mobility Controller;
- the HP 5412 zl Switch Chassis for the HP 5412 zl Switch with the HP MSM765zl Mobility Controller;
- the HP 8206 zl Switch Chassis for the HP 8206 zl Switch with the HP MSM765zl Mobility Controller; and
- the HP 8212 zl Switch Chassis for the HP 8212 zl Switch with the HP MSM765zl Mobility Controller.

The cryptographic modules are all multiple-chip standalone cryptographic modules.



### 3 PRODUCT OPERATION

#### 3.1 OVERVIEW

The HP MSM765zl Mobility Controller is the component in the cryptographic modules that will be providing cryptographic services while the cryptographic module is in the FIPS approved mode of operation. The HP MSM765zl Mobility Controller is a general-purpose device whose operational mode is configurable through an administrative interface.

The following section describes how to operate the cryptographic module in the FIPS approved mode of operation. The *HP MSM765zl Mobility Controller Installation and Getting Started Guide* or the *HP MSM7xx Controllers Management and Configuration Guide* can be consulted for a complete discussion of the operation of the HP MSM765zl Mobility Controller. The *HP ProCurve 5400zl Switches Installation and Getting Started Guide* provides information on the installation of the HP 5406 zl and HP 5412 zl Switches and the *HP 8200 zl Switches Installation and Getting Started Guide* provides information on the installation of the HP 8206 zl and HP 8212 zl Switches.

#### 3.2 FIPS APPROVED MODE OF OPERATION

##### 3.2.1 Description

The FIPS approved mode of operation is a special configuration of the cryptographic module, in which:

- a. The cryptographic module is configured to operate in the FIPS 140-2 approved mode;
- b. The tamper evident seals, opacity shields, and high performance fan trays are installed as prescribed;
- c. The (optional) RADIUS authentication operates over an IPsec protected link; and
- d. The (optional) SNMP management of the unit operates over an IPsec protected link.

The instructions for configuring the HP MSM765zl Mobility Controller in the switch in the FIPS 140-2 approved mode of operation are provided in section **3.2.2**. The following preliminary steps must be completed prior to configuring the HP MSM765zl Mobility Controller to operate in the FIPS approved mode of operation:

1. Configure the HP 5406 zl Switch, HP 5412 zl Switch, HP 8206 zl Switch, or HP 8212 zl Switch, as appropriate for your network.
2. If necessary, update the switch firmware to the switch firmware covered as part of this validation.
3. Install only one HP MSM765zl Mobility Controller in the switch chassis, and configure basic IP addressing and VLAN information, as appropriate for your network.



4. To prevent unintentional factory reset of the switch, the “Reset” button located on the Management Card of the HP 5406 zl Switch or the HP 5412 zl Switch, or located on the System Support Module of the HP 8206 zl Switch or the HP 8212 zl Switch, must be disabled. The Crypto-Officer must confirm the prompt with a ‘y’ to complete the command. For example:

```
HP-E8212zl(config)# no front-panel-security factory-reset
**** CAUTION ****
```

Disabling the factory reset option prevents switch configuration and passwords from being easily reset or recovered. Ensure that you are familiar with the front panel security options before proceeding.

Continue with disabling the factory reset option[y/n]? y

5. To prevent unintentional password reset of the switch, the “Clear” button located on the Management Card of the HP 5406 zl Switch or the HP 5412 zl Switch, or located on the System Support Module of the HP 8206 zl Switch or the HP 8212 zl Switch, must be disabled. The Crypto-Officer must confirm the prompt with a ‘y’ to complete the command. For example:

```
HP-E8212zl(config)# no front-panel-security password-clear
**** CAUTION ****
```

Disabling the clear button prevents switch passwords from being easily reset or recovered. Ensure that you are familiar with the front panel security options before proceeding.

Continue with disabling the clear button [y/n]? y

6. The auxiliary port located on the Management Card must be disabled avoid any unauthorized modifications to the cryptographic module. Please note: The autorun feature will not function when the USB port is disabled. For example:

```
HP-E8212zl(config)# no usb-port
```



7. Remove IP address from HP 5406 zl Switch, HP 5412 zl Switch, HP 8206 zl Switch, or HP 8212 zl Switch, as appropriate for your network (e.g. IP addressing). This will require two commands:
  - For each vlan – “no ip address”; and
  - For each vlan – “no Ipv6 address”.

The following HP documents may be of assistance in completing the above:

- *HP ProCurve 5400zl Switches Installation and Getting Started Guide*;
- *HP 8200 zl Switches Installation and Getting Started Guide*;
- *HP MSM765zl Mobility Controller Installation and Getting Started Guide*;
- *HP MSM7xx Controllers Management and Configuration Guide*; and
- Release notes that accompany any firmware update(s) installed.

Please note that to run the cryptographic module in the non-FIPS approved mode of operation after it is configured in the FIPS approved mode of operation, the operator shall first reset the HP MSM765zl Mobility Controller to the factory default configuration.

### **3.2.2 Instructions for Putting the HP MSM765zl Mobility Controller into the FIPS Approved Mode of Operation**

#### **3.2.2.1 Initial Assumptions**

- The HP MSM765zl Mobility Controller does not have the FIPS validated firmware installed.
- There are no access points currently being discovered or managed by the HP MSM765zl Mobility Controller.
- The administrator knows how to use the CLI from the chassis to configure an IP address on the controller in the case where the unit is brand new or it has been factory reset.

#### **STEP 1: LOAD THE FIPS VALIDATED FIRMWARE ON THE CONTROLLER**

- Login to the HP MSM765zl Mobility Controller through the web using the default username “admin” and password “admin” credentials.



hp **MSM765** System name: SG916GG00R

Welcome to HP  
MSM765 Integrated Controller

Internet port address: **10.212.10.210**  
Internet port MAC address: **00:24:A8:1D:A5:44**

Default country: **UNITED STATES (not configured)**  
Authentication system: **Running**  
Authenticated users: 0

Uptime: **17 minutes**

SNMP system name: **SG916GG00R**  
Software version: **5.5.2.14-01-10104**

Username: Password:

admin ●●●●●●

- Select and install the FIPS validated firmware.



The screenshot shows the HP MSM765 web interface. The top navigation bar includes 'Home' and 'Logout'. The main navigation menu includes 'Network', 'Security', 'VPN', 'Controlled APs', 'Authentication', 'Public access', 'Users', 'Management', 'Status', 'Tools', and 'Maintenance'. The 'Maintenance' menu item is highlighted in red. Below the navigation menu, there are sub-menus for 'Config file management', 'Firmware updates', 'Registration', 'Licenses', 'System', and 'EULA'. The 'Firmware updates' sub-menu is highlighted in red. The main content area is titled 'Firmware updates' and contains a section for 'Install firmware'. The text reads: 'Install firmware directly to the MSM765 from your local hard drive or schedule regular uploads from a remote server.' Below this, it states 'Current firmware version: 5.5.2.14-01-10104'. There are two sections: 'Manual install' and 'Scheduled install'. In the 'Manual install' section, the file path 'C:\MSM765-FIPS.cim' is entered in a text box, and the 'Browse...' button is highlighted in blue. The 'Install' button is highlighted in red. In the 'Scheduled install' section, the checkbox is unchecked, and the 'Day of week' is set to 'Everyday'.

After the firmware is installed, the HP MSM765zl Mobility Controller will reboot. It may be necessary to type the address of the controller directly to get the home page because the FIPS-validated firmware will have installed a new default web certificate, which interferes with the JavaScript automatic reloading of the home page. Once the home page displays, it can be verified that the version installed is the correct one by checking the specified “Software version”. Note that the CMVP considers the executables to be firmware, whereas, in generic IT terminology, they are considered to be software.





Welcome to HP  
MSM765 Integrated Controller

Internet port address: 10.212.10.210  
Internet port MAC address: 00:24:A8:1D:A5:44

Default country: CANADA  
Authentication system: Running  
Authenticated users: 0

Uptime: 78 days 6 hours 29 minutes

SNMP system name: SG916GG00R

Software version: 5.6.0.0-01-10618

Username:

Password:

Login



## STEP 2: RESET THE CONTROLLER TO THE FACTORY DEFAULT

- Reset the controller to the factory default by going to web page “Config file management” of “Maintenance” and selecting the “Reset” button. Use the chassis CLI interface to give an address to the controller. This is done to ensure the HP MSM765z1 Mobility Controller uses the default certificates which have 2048-bit RSA public keys. Operators can install their own certificates.

The screenshot displays the HP MSM765 web interface. At the top, the system name is SG915GG017. The navigation menu includes Network, Security, VPN, Controlled APs, Authentication, Public access, Users, Management, Status, Tools, and Maintenance. The 'Maintenance' menu is expanded, showing 'Config file management' as the selected option. The 'Config file management' page contains four main sections: 'Backup configuration', 'Restore configuration', 'Reset configuration', and 'Scheduled operations'. The 'Reset configuration' section includes a text input field and a 'Reset' button, both highlighted with red boxes. The 'Scheduled operations' section includes a dropdown for 'Operation' (set to Backup), a dropdown for 'Day of week' (set to Everyday), a time selector for 'Time of day' (set to 00:00), and a 'URL' input field.



### STEP 3: CONFIGURE THE MANAGEMENT TOOL

- Login using the default username and password.
- Select the “Management” tab and then select the “Management tool” tab.
- Select “TLSv1” from the drop-down list.
- Select “FIPS compliant operation”.
- Click on “Save” at the bottom of the web page.
- The Administrator will need to login again to the controller since the changes to the Management tool will force a reboot of the controller.



hp **MSM765** System name: SG916GG00R

Home [Logout](#)

Network Security VPN Controlled APs Authentication Public access Users **Management** Status Tools Maintenance

Management tool Teaming Device discovery SNMP SOAP CLI Management console System time Country

### Management tool configuration

#### Administrative user authentication

Local

RADIUS: <No RADIUS defined>

#### Security policies

Follow FIPS 140-2 guidelines

Follow PCI DSS 1.2 guidelines

#### Manager account

Username:

Current password:

New password:

Confirm new password:

If a manager is logged in, then a new manager login:

Terminates the current manager session

Is blocked until the current manager logs out

#### Operator account

Username:

New password:

Confirm new password:

If an operator is logged in, then a new operator login:

Terminates the current operator session

Is blocked until the current operator logs out

#### Login control

Lock access after  login failures

Lock access for  minutes

#### Security

Access to the management tool is enabled for the addresses and interfaces that are specified below.

**Allowed addresses:**

IP address:  Mask:

**Active interfaces:**

LAN port  VPN

Internet port

VLAN/GRE (Select from the list):

#### Web server

Secure web server port:

Web server port:

SSL/TLS version:

FIPS compliant operation

#### Auto-Refresh

Auto-Refresh



#### STEP 4: SELECTING SELF-TESTING AND DISABLING SERVICE OS

- Go to the “System” page of “Maintenance”. Note that the web page will not look the same as the shown screen shot for a teamed controller.
- Select the checkbox “Test cryptographic system (FIPS compliant operation)”.
- Select the checkbox “Disable Service OS access (FIPS compliant operation)”.
- Click on the “Save” button and then on the “Restart” button. The controller will reboot and run the power-up self-tests.

The screenshot shows the HP MSM765 web interface. The system name is SG916GG00R. The navigation menu includes Network, Security, VPN, Controlled APs, Authentication, Public access, Users, Management, Status, Tools, and Maintenance. The System page contains sections for 'Save system information', 'Restart', 'Startup self-tests', and 'Startup options'. The 'Startup self-tests' section has a checked checkbox for 'Test cryptographic system (FIPS compliant operation)'. The 'Startup options' section has a checked checkbox for 'Disable Service OS access (FIPS compliant operation)'. The 'Restart' button is highlighted with a red box. The 'Save' button is also highlighted with a red box.

- The web and CLI (through SSH) access will use only FIPS approved algorithms.



## STEP 5: AUTHENTICATION SETUP

- Login with the default username (admin) and password (admin) and select the “Management tool” tab on the “Management” web page.
- Set the **Manager account** username and password.
- If desired, set a username and password for the **Operator account**.
- Make sure that the Security policy is set to “Follow FIPS 140-2 guidelines”.
- In the login control, do not increase the number of failures to more than “5” or set the lock access (“Lock access for”) to “0” minutes.



hp **MSM765** System name: SG916GG00R

Home Logout

Network Security VPN Controlled APs Authentication Public access Users **Management** Status Tools Maintenance

**Management tool** Teaming Device discovery SNMP SOAP CLI Management console System time Country

### Management tool configuration

#### Administrative user authentication

Local  
 RADIUS: <No RADIUS defined>

#### Manager account

Username:   
Current password:   
New password:   
Confirm new password:

If a manager is logged in, then a new manager login:

Terminates the current manager session  
 Is blocked until the current manager logs out

#### Operator account

Username:   
New password:   
Confirm new password:

If an operator is logged in, then a new operator login:

Terminates the current operator session  
 Is blocked until the current operator logs out

#### Login control

Lock access after  login failures  
Lock access for  minutes

#### Security policies

Follow FIPS 140-2 guidelines  
 Follow PCI DSS 1.2 guidelines

#### Security

Access to the management tool is enabled for the addresses and interfaces that are specified below.

**Allowed addresses:**

IP address:  Mask:

#### Active interfaces:

LAN port  VPN  
 Internet port

VLAN/GRE (Select from the list):

#### Web server

Secure web server port:   
Web server port:   
SSL/TLS version:   
 FIPS compliant operation

#### Auto-Refresh



- CLI: If the CLI is to be used, do the following:
  - Select the “CLI” tab of the “Management” web page.
  - Select the “Enable CLI access using SSH” checkbox.
  - Either Authentication option may be used.

The screenshot displays the HP MSM765 web management interface. The top navigation bar includes the HP logo, the device name 'MSM765', and the system name 'SG916GG00R'. Below this, there are links for 'Home' and 'Logout'. A secondary navigation bar contains various configuration categories: Network, Security, VPN, Controlled APs, Authentication, Public access, Users, Management (highlighted with a red box), Status, and Tools. A third navigation bar shows specific configuration options: Management tool, Teaming, Device discovery, SNMP, SOAP, CLI (highlighted with a red box), Management console, System time, and Counters.

The main content area is titled 'Command Line Interface (CLI) configuration'. It features two primary configuration sections:

- Secure Shell access**: This section contains a checkbox labeled 'Enable CLI access using SSH', which is checked and highlighted with a red box.
- Authentication**: This section is titled 'Authenticate CLI logins using:' and contains two radio button options: 'Local manager account' and 'Administrative user authentication settings'. The 'Administrative user authentication settings' option is selected and highlighted with a red box.

A 'Save' button is located at the bottom right of the configuration area. On the left side of the interface, there is a 'Summary' section showing 'Controlled APs Configured 1' and a 'Network Tree' section showing a hierarchy: Controller (selected), VSCs, HP, Controlled APs, Default Group, and AP-1.





- Access Point Authentication: Select the “Device discovery” tab of the “Management” web page.
- Select the “Authenticate APs” checkbox to ensure that the Access Points authenticate to the controller.
- Enter the Shared Secret for the Access Point in the “Shared secret” and “Confirm shared secret” boxes (must be the same as on the Access Points).
- Click the “Save” button to save the setting and shared secret.

The screenshot shows the HP MSM765 web interface. The system name is SG916GG00R. The 'Management' tab is selected in the top navigation bar. The 'Device discovery' sub-tab is active. The 'Controlled AP discovery' section is expanded, showing the 'Authenticate APs' checkbox checked. The 'Shared secret' and 'Confirm shared secret' fields are filled with dots. The 'Save' button is highlighted in the bottom right corner.



### STEP 6: SET RESTRICTIONS

- Terminate WPA at the controller must NOT be used to be in the FIPS approved mode of operation. The “Terminate WPA at the controller” checkbox must not be selected.

The screenshot displays the configuration page for an HP MSM765 system. The top navigation bar includes the HP logo, the system name 'MSM765', and the system name 'SG916GG00R'. Below the navigation bar, there are tabs for 'Overview' and 'Configuration', with 'Configuration' being the active tab. Under 'Configuration', there is a sub-tab for 'VSC profile'. A yellow warning banner at the top of the configuration area states: 'Changing the configuration of this VSC will disconnect all authenticated users connected to this VSC.' Below the warning, the configuration is for 'VSC: HP | VSC profile'. The 'Global' section shows the profile name as 'HP' and 'Use Controller for:' with checkboxes for 'Authentication' and 'Access control', both of which are checked. The 'Wireless protection' section is expanded, showing 'WPA' as the selected mode. The 'Mode' dropdown is set to 'WPA2 (AES/CCMP)', which is highlighted with a red box. The 'Key source' is set to 'Preshared Key'. The 'Terminate WPA at the controller' checkbox is unchecked. There are two password fields for 'Key' and 'Confirm key', both containing masked characters. A footnote at the bottom of the wireless protection section states: '\*On radios in pure 802.11n mode WPA2 is always used instead of WPA'.



- RADIUS EAP: Select the “RADIUS server” tab of the “Authentication” web page.
- Do not select the “EAP-TTLS” checkbox but can select the “EAP-PEAPv0” and “EAP-TLS” checkboxes.
- Select the checkbox “FIPS compliant operation” to restrict the EAP ciphersuites to the FIPS approved ones.

The screenshot shows the HP MSM765 web interface. The top navigation bar includes 'Home' and 'Logout'. The main navigation menu has tabs for 'Network', 'Security', 'VPN', 'Controlled APs', 'Authentication', 'Public access', 'Users', and 'Management'. Under the 'Authentication' tab, there are sub-tabs for 'RADIUS profiles', 'RADIUS server', 'Active directory', '802.1X', and 'MAC lists'. The 'RADIUS server' sub-tab is selected. The page title is 'RADIUS server/proxy'. The main content area is divided into several sections:
 

- RADIUS server:** Includes a checkbox for 'Detect SSID from NAS-Id', a text input for 'Number of accounting sessions' (set to 2000), and 'Maximum accounting sessions' (set to 1000). It also shows 'Authentication UDP port: 1812' and 'Accounting UDP port: 1813'.
- Server authentication support:** A section with a red border containing:
  - PAP (Required to support MAC-based authentication in VSCs)
  - To support WPA/802.1X clients you must select at least one of the following:*
  - EAP-TTLS
  - EAP-PEAPv0
  - EAP-TLS
  - FIPS compliant operation
- RADIUS authorization:** A section with a red border containing a list of IP addresses, 'IP address:', 'Mask:', 'Shared secret:', and 'Add'/'Remove' buttons.
- Default shared secret:** A section with a red border containing 'Shared secret:' and 'Confirm shared secret:' text inputs.

 A 'Save' button is located at the bottom right of the page, also highlighted with a red box.

The HP MSM765zl Mobility Controller is not to be used as a generic RADIUS server.



- Provisioning from the controller
- If provisioning from the controller is enabled, then the controller must NOT remove the provisioning settings that make the Access Points operate in the FIPS approved mode of operation:
  - Ignore controller firmware update requests;
  - Test cryptographic system;
  - Authentication of the controller; and
  - AES/CCMP used when provisioning a local mesh link.
- The page to enable provisioning from the controller is “Provisioning” available from the “Controlled APs” tab.

The screenshot displays the HP MSM765 web interface. The top navigation bar includes the HP logo, the system name 'MSM765', and the system name 'SG916GG00R'. Below the navigation bar, the 'Controlled APs' tab is selected, and the 'Provisioning' sub-tab is active. The main content area shows the 'Provisioning options' section, which contains a checkbox labeled 'Replace any existing AP provisioning with controller-based provisioning settings'. A 'Save' button is located at the bottom right of this section. The left sidebar shows a 'Network Tree' with a 'Controller' section containing 'VSCs' and 'HP', and a 'Controlled APs' section containing 'Default Group' and 'AP-1'.



hp MSM765 System name: SG916GG00R

Home Logout

Overview Configuration Group management Tools **Provisioning**

Connectivity Discovery **System**

Summary  ?

Controlled APs  
Configured 1

Network Tree  ?

- Controller
  - VSCs
    - HP
  - Controlled APs**
    - Default Group
      - AP-1

Base Group: All | System ?

**Firmware update**

- Ignore controller firmware update requests

**Startup self-tests**

- Test cryptographic system (FIPS compliant operation)

Save



hp **MSM765** System name: SG916GG00R

Home Logout

Overview | Configuration | Group management | Tools | **Provisioning**

Connectivity | **Discovery** | System

Base Group: All | Discovery

**Summary** ?

Controlled APs  
Configured 1

**Network Tree** ?

- Controller
- VSCs
- HP
- Controlled APs**
- Default Group
- AP-1

**Discover using DNS** ?

**Names to search for:**

Name:

Domain name:

Primary DNS server:

Secondary DNS server:

**Discover using IP address** ?

**Addresses to search for:**

IP address:

**Controller authentication** ?

Controller shared secret:

Confirm controller shared secret:



- SOAP configuration
- If the “SOAP server configuration” checkbox is selected, the following must also be done:
  - The “Secure HTTP (SSL/TLS)” checkbox must be selected.
  - The “Require client certificate” checkbox must be selected.
  - The “FIPS compliant operation” checkbox must be selected.
  - “TLSv1” dropdown must be selected for “SSL/TLS version”.
  - A trusted CA X.509 cert must be installed that is to be used to validate the SOAP client certificate.
  - The “Save” button must be clicked to save the settings.

The screenshot displays the HP MSM765 web interface. At the top, the HP logo and 'MSM765' are visible, along with the system name 'SG916GG00R'. The navigation bar includes 'Home' and 'Logout'. The main menu has 'Management' highlighted. Below the menu, the 'SOAP server configuration' page is active, indicated by a red box around the page title. The 'Server settings' section contains several checkboxes: 'Secure HTTP (SSL/TLS)', 'Require client certificate', and 'FIPS compliant operation', all of which are checked. The 'SSL/TLS version' dropdown is set to 'TLSv1'. There are also fields for 'Username', 'Password', and 'Confirm password'. The 'TCP port' is set to '448'. A 'Security' section is also visible, with a 'Remove Selected Entry' button. A 'Save' button is located at the bottom right of the page.



- Teaming
- If the “Controller teaming” checkbox is selected, the following must also be done:
  - The “Ignore controller firmware update requests” checkbox must be selected.
  - The “Team authentication” checkbox must be selected.
  - A team shared secret must be entered in the “Team shared secret” and “Confirm team shared secret” boxes.
  - The “Save” button must be selected to save the settings.

The screenshot displays the HP MSM765 web interface. At the top, the system name is 'MSM765' and 'System name: SG916GG00R'. The navigation bar includes 'Home' and 'Logout'. The main menu has 'Management' selected, with 'Teaming' highlighted in the sub-menu. The 'Controller teaming' configuration page is shown, with the following settings:

- Connectivity:** Communicate using: Internet Port (dropdown). Radio buttons for 'No VLAN' (selected) and 'VLAN ID: 0' (input field). IP address and Mask input fields.
- Team manager:** Team name, Team IP address, Mask, and Interface (Internet Port dropdown) input fields.
- Team authentication:** Team shared secret and Confirm team shared secret (both masked with dots).
- Firmware update:**  Ignore controller firmware update requests.

A 'Save' button is located at the bottom right of the configuration area.





- Certificate Wizard
- When using the IPSec certificate request wizard, 2048-bits keys must be selected.
- The IPSec certificate request wizard is available on the “IPSec” page for the “VPN” tab.
- Click the “Certificate Request Wizard” button.
- Select the “2048 bits” dropdown for the “Length:” for “Key”.

The screenshot shows the HP MSM765 web interface. At the top, the system name is SG916GG00R. The navigation menu includes Network, Security, VPN, Controlled APs, Authentication, Public access, Users, Management, and Status. The VPN tab is selected, and the IPSec sub-tab is active. The main content area is titled 'IPSec port configuration' and contains several sections:

- IPSec VLAN mapping:** Internet port: Untagged Internet port, LAN port: Untagged LAN port.
- Local group list:** Current groups: (empty), Add new group: Group name, Password, Confirm password.
- IPSec security policy database:** A table with columns: Name, Port, Peer address, Mode, Status, Authentication. An 'Add New Policy...' button is below.
- IPSec certificates:**
  - IPSec — Trusted CA certificates:** Certificate file: (Browse...), Install.
  - IPSec — Manage CA certificates:** Certificates: (dropdown), Remove, View...
  - IPSec — Local certificate store:** Certificate Request Wizard (highlighted with a red box), Certificate file: (Browse...).
  - IPSec — Manage local certificate:** Certificate: (input), Remove, View...

A 'Save' button is located at the bottom right of the configuration section.



**MSM765** System name: SG916GG00R

[Home](#) [Logout](#)

---

Certificate Request Wizard

**Step 1 - Enter the information necessary to generate the request**

**Summary** ⌵ ?

Controlled APs  
Configured 1

**Network Tree** ⌵ ?

- ☐ **Controller**
- ☐ VSCs
- HP
- ☐ Controlled APs
- ☐ Default Group
- AP-1

**Subject name**

Common name:  *required*

Department:

Company:

Locality:

State:  Country:

**Key**

Length: 2048 bits ▾

The information you specify on this page enables the MSM765 management tool to generate a certificate request.



**STEP 7: SERVICES THAT ARE NOT ALLOWED IN THE FIPS APPROVED MODE OF OPERATION**

The following shows the services that must not be configured for the HP MSM765zl Mobility Controller to operate in the FIPS approved mode of operation.

- NOC Based Authentication
- Do not check “NOC-based authentication” on the “Web server” page of the “Public Access” web page.

The screenshot displays the HP MSM765 web management interface. At the top, the system name is 'SG916GG00R'. The navigation menu includes 'Home' and 'Logout'. The main menu has 'Public access' highlighted with a red box. Below it, the 'Web server' sub-menu is also highlighted with a red box. The 'Web server configuration' page is shown, with the 'Options' section containing a red box around the 'NOC-based authentication' checkbox, which is currently unchecked. Other sections include 'Ports' (HTTP: 8080, HTTPS: 8090), 'MIME types', and 'Security' (Allowed addresses, Active interfaces). A 'Save' button is located at the bottom right.



- HTML Authentication
- Do not check “HTML-based user logins” on the “VSC profile” page of the “Configuration” web page.

The screenshot displays the HP ProCurve VSC configuration interface. The top navigation bar includes 'Home' and 'Logout'. Below the navigation bar, there are tabs for 'Overview' and 'Configuration', with 'Configuration' being the active tab. A sub-tab 'VSC profile' is also visible. A yellow warning banner at the top of the main content area states: 'Changing the configuration of this VSC will disconnect all authenticated users connected to this VSC.' The main content area is titled 'VSC: HP ProCurve | VSC profile'. The left sidebar shows a 'Network Tree' with 'Controller' expanded to 'VSCs', where 'HP ProCurve' is selected. The main configuration area is divided into several sections: 'Global' (Profile name: HP ProCurve, Use Controller for: Authentication and Access control), 'Access control' (Present session and welcome page to 802.1x users, Identify stations based on IP address only, Local NAS Id), 'VSC ingress mapping' (SSID, VLAN: <No VLAN defined>), 'Virtual AP' (WLAN Name (SSID): HP ProCurve, DTIM count: 1, Broadcast name (SSID), Advertise TX power, Broadcast filtering, Band steering), 'Wireless protection' (Mode: WPA (TKIP), Key source: Preshared Key, Terminate WPA at the controller, Key, Confirm key), '802.1X authentication' (Local, Remote), 'RADIUS authentication realms' (RADIUS accounting: <No RADIUS defined>), and 'HTML-based user logins' (HTML-based user logins, Local). The 'HTML-based user logins' checkbox is highlighted with a red box.



- Payment Services
- Do not check “Credit card” or enter information on the “Payment services” page of the “Public Access” web page.

The screenshot shows the HP MSM765 web interface. The top navigation bar includes the HP logo, the system name 'MSM765', and the system name 'SG916GG00R'. Below the navigation bar, there are tabs for 'Network', 'Security', 'VPN', 'Controlled APs', 'Authentication', 'Public access', 'Users', 'Management', and 'Status'. The 'Public access' tab is highlighted with a red box. Below this, there are sub-tabs for 'Access control', 'Web server', 'Web content', 'Payment services', 'Billing records', and 'Attributes'. The 'Payment services' sub-tab is also highlighted with a red box. The main content area shows the 'Payment services' configuration page. On the left, there is a 'Summary' section with a 'Controlled APs' link showing 'Configured 1'. Below that is a 'Network Tree' section with a 'Controller' link and a list of VSCs (HP) and Controlled APs (Default Group, AP-1). The main configuration area is divided into two sections: 'Service settings' and 'Authorize.Net service'. In the 'Service settings' section, the 'Payment method' is set to 'Credit card', which is highlighted with a red box. The 'Currency code' is 'USD' (3 letters) and the 'Tax rate' is '0 %'. In the 'Authorize.Net service' section, the 'Payment URL' is 'https://test.authorize.net/'. There are also fields for 'Login ID' and 'Transaction key'. A 'Save' button is located at the bottom right of the configuration area.



- Billing Records Logging
- Do not select any checkboxes or enter information on the “Billing records” page of the “Public Access” web page.

The screenshot displays the HP MSM765 web interface for the 'Billing records logging system'. The top navigation bar includes 'Home' and 'Logout'. The main navigation menu has 'Public access' and 'Billing records' highlighted. The left sidebar shows a 'Network Tree' with a 'Controller' section containing 'VSCs', 'HP', 'Controlled APs', 'Default Group', and 'AP-1'. The main content area is titled 'Billing records logging system' and contains two panels: 'Settings' and 'Persistence'. The 'Settings' panel has a checkbox for 'Suspend payment system when log is full of queued records' and a 'Configure Record Formats...' button. The 'Persistence' panel has a 'Save queued records every 120 minutes' field and a 'Save Queued Records Now' button. A 'Save' button is located at the bottom right of the settings section. Below this is a section for 'External billing records server profiles' with a table and an 'Add New Profile...' button.



hp **MSM765** System name: SG916GG00R

Home Logout

Network Security VPN Controlled APs Authentication **Public access** Users Management Stat

Access control Web server Web content Payment services **Billing records** Attributes

Summary ?

Controlled APs  
Configured 1

Network Tree ?

- Controller
  - VSCs
    - HP
  - Controlled APs
    - Default Group
      - AP-1

### Add/Edit external billing records server profile

#### Settings

Type: Primary

Profile name:

Hostname/IP address:

Port:

URL:

Transmission timeout:  seconds

#### Security

Secret key:

Use HTTPS

Validate server certificate

Use HTTP authentication

Username:

Password:

#### Failover

Available backup servers:

Use these backup servers:

Retries per server:

Delay between retries:  seconds

#### Fault tolerance

Retransmit until successful

Stop after  failed retransmissions



- L2TP Server
- Do not check the checkbox for “L2TP over IPSec configuration - LAN port”.

The screenshot displays the configuration interface for an HP MSM765 device. The top navigation bar includes the HP logo, the device name 'MSM765', and the system name 'SG916GG00R'. Below this, there are tabs for 'Home' and 'Logout'. The main navigation menu includes 'Network', 'Security', 'VPN', 'Controlled APs', 'Authentication', 'Public access', 'Users', 'Management', and 'Status'. The 'VPN' tab is selected, and within it, the 'L2TP server' sub-tab is active. The main content area shows the configuration for 'L2TP over IPSec configuration - LAN port'. The 'Settings' section has two radio buttons: 'X.509 certificates' (selected) and 'Preshared key:'. The 'Address allocation' section has a dropdown menu for 'Address source' set to 'VPN address pool'. A 'Save' button is located at the bottom right of the configuration area.





- PPTP Server
- Do not select the “PPTP server configuration – LAN port” checkbox on the “PPTP server” page of the “VPN” web page.

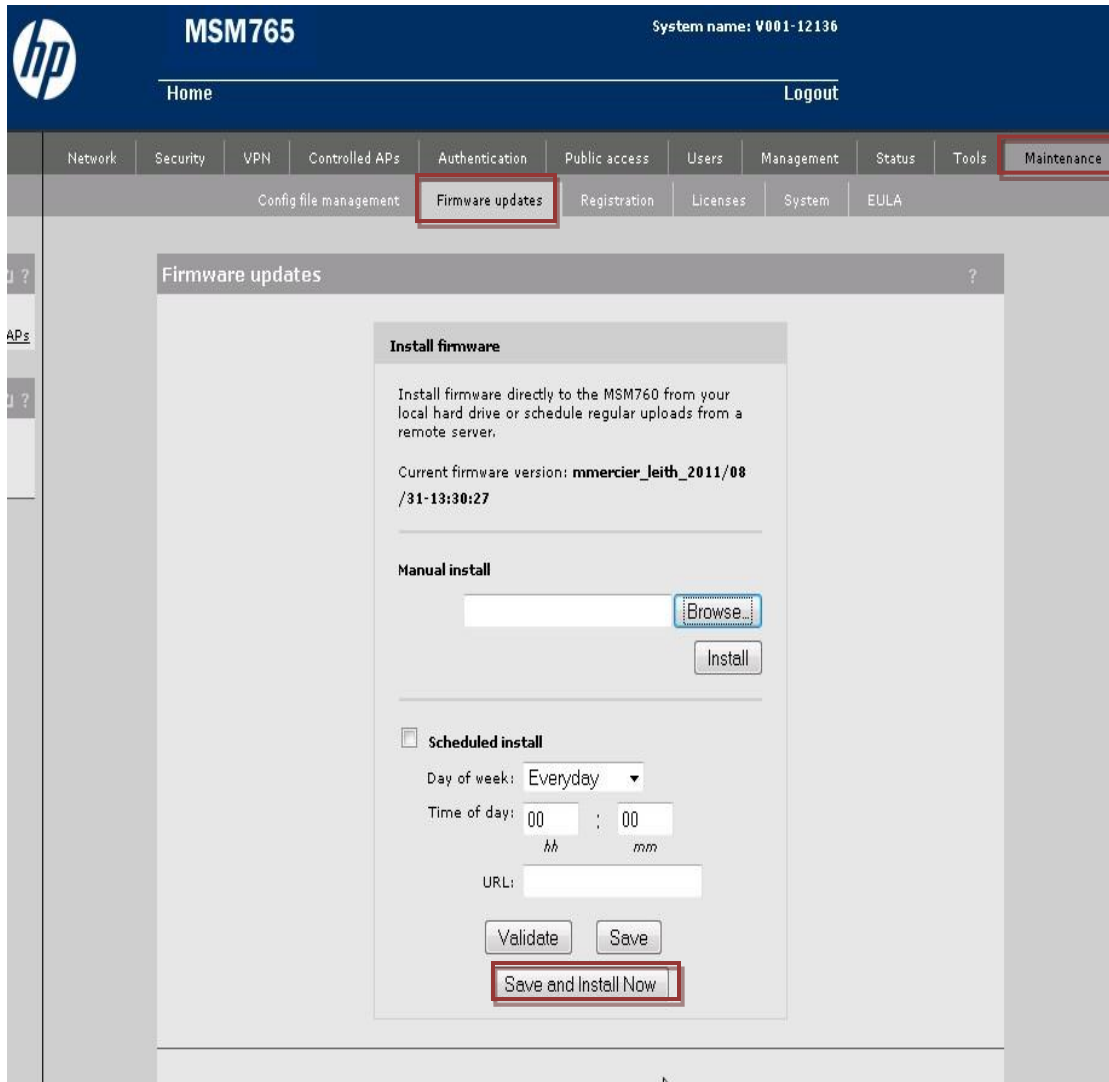
The screenshot displays the HP MSM765 web interface. The top navigation bar includes the HP logo, the system name 'MSM765', and the system name 'SG916GG00R'. Below the navigation bar, there are tabs for 'Network', 'Security', 'VPN', 'Controlled APs', 'Authentication', 'Public access', 'Users', 'Management', and 'Status'. The 'VPN' tab is highlighted with a red box. Under the 'VPN' tab, there are sub-tabs for 'IPSec', 'L2TP server', 'PPTP server', and 'PPTP client'. The 'PPTP server' sub-tab is also highlighted with a red box. The main content area shows the 'PPTP server configuration - LAN port' page. In this page, there is a section titled 'Address allocation' with a dropdown menu set to 'VPN address pool'. A 'Save' button is located at the bottom right of the configuration area. On the left side, there is a sidebar with a 'Controller' section containing 'VSCs' (HP) and 'Controlled APs' (Default Group, AP-1).



- Mobility Manager
- Uncheck the “**Mobility Manager**” checkbox on the “Management console” page of the “Management” web page.
- Click the “Save” button to save the configuration.

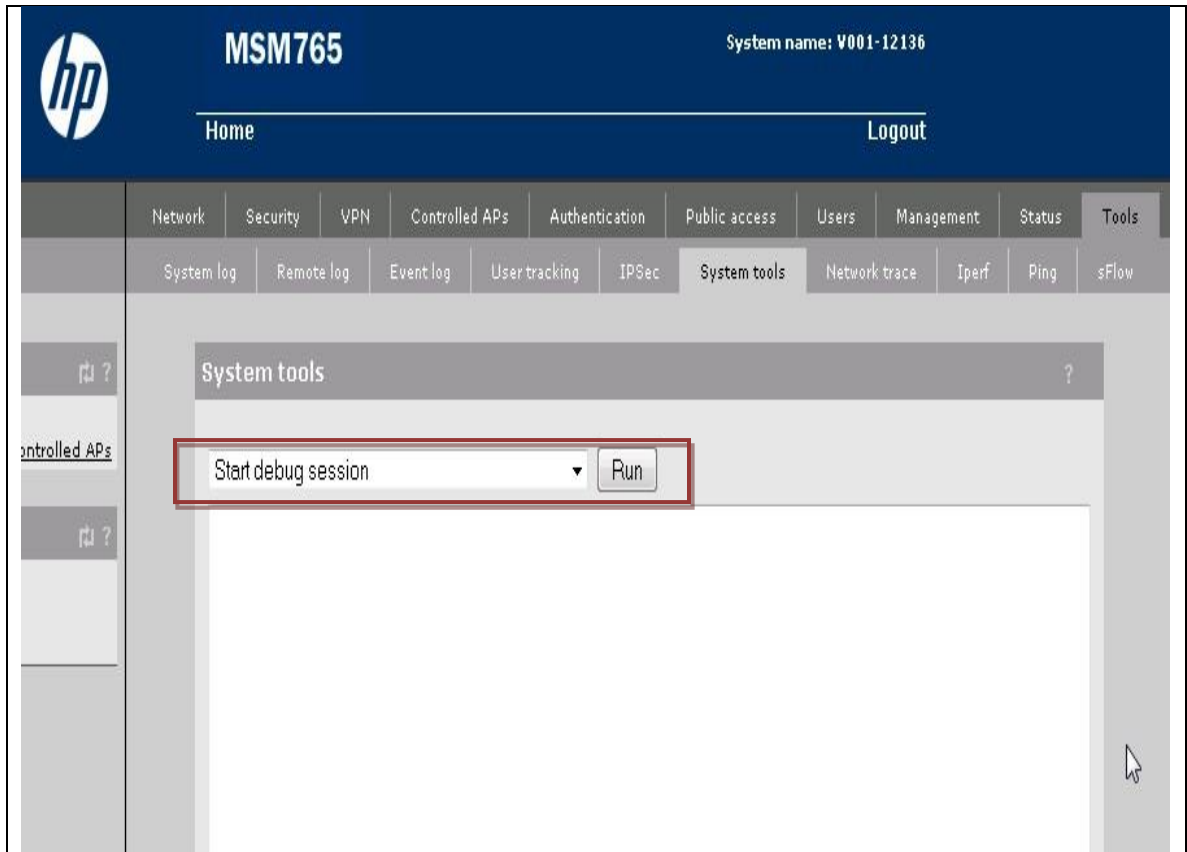


- Automatic Firmware Installations
- Do not check the “**Scheduled install**” checkbox on the “Firmware updates” page of the “Maintenance” web page and click the “Save” or the “Save and Install Now” buttons.





- System tool debug session
- Do not run the “Start debug session” system tool available on the “System tools” page of the “Tools” web page. It starts an SSH server that is not under control of the Crypto-Officer.





## **4 SECURITY RULES DERIVED FROM THE REQUIREMENTS OF FIPS PUB 140-2**

### **4.1 FINITE STATE MODEL**

The cryptographic functionality of the cryptographic modules is provided by the HP MSM765zl Mobility Controller. The finite state model for the HP MSM765zl Mobility Controller is shown and described in the *HP MSM765zl Mobility Controller Finite State Model*.

### **4.2 ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC)**

The HP MSM765zl Mobility Controller and the HP 8206 zl Switch (including Management Module, System Support Module, Fabric Modules, and line cards) were tested as meeting FCC 47 CFR Part 15, Subpart B: 1999 Class A by the Roseville Hardware Test Center which is accredited for EMI/EMC testing by the American Association for Laboratory Accreditation with laboratory number 0923-01. The HP 5406 zl Switch, the HP 5412 zl Switch, and HP 8212 zl Switch are formally declared to have similar EMI/EMC characteristics.



## 4.3 SELF-TESTS

### 4.3.1 Power-Up Self-Tests

The cryptographic modules implement the following power-up self-tests that are initiated on the application of power:

- Firmware integrity test verifying the SHA-1 hash on all executables, shared libraries, and kernel loadable modules;
- Known answer test for the AES-using, FIPS-approved deterministic random number generator specified in *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms* in firmware;
- Encryption and decryption known answer tests on the user space firmware implementation of Triple DES, with 2 and 3 keys;
- Encryption and decryption known answer tests on the kernel space firmware implementation of Triple DES, with 3 keys;
- Encryption and decryption known answer tests, with 128 bit keys, on the user and kernel space firmware implementations of AES;
- PKCS#1 v1.5, PSS, and ANSI X9.31 RSA in firmware tested with signature generation and verification known answer tests using 1024 bit keys and the hash algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 (implementation used for TLS and SSH);
- Second implementation of PKCS#1 v1.5 RSA in firmware tested with signature generation and verification known answer tests with 1024 bit keys and using the SHA-1 hash algorithm (implementation used for IPSec);
- Known answer test on user space implementation of SHA-1 in firmware;
- Known answer test on kernel space implementation of SHA-1 in firmware;
- Known answer test on kernel space implementation of HMAC-SHA-1 in firmware; and
- Known answer test on user space implementations of HMAC-SHA-1 in firmware.

These tests can be executed on demand by rebooting the controller.



### 4.3.2 Conditional Self-Tests

The cryptographic modules implement the following conditional self-tests:

- Firmware load test, verification of a HMAC-SHA-1 message digest, on the entire firmware loaded on to the HP MSM765zl Mobility Controller;
- Pair-wise consistency tests on generated RSA key pairs;
- Cryptographic bypass test on peer-to-peer policies defined in the IPSec policy database (verification of the HMAC-SHA-1 hash over the table when a policy is to be added, modified, or deleted); and
- Continuous random number generator tests on the FIPS-approved ANSI X9.31 with AES deterministic random number generator and on /dev/urandom, which provides random data for the seed key and seed for the FIPS-approved PRNG.

The cryptographic modules do not support manual key entry. The two independent actions for bypass are the configuration of the IPSec security policy to include certain IP addresses and the searching of the security associations table for the IP address.

If a conditional self-test passes, the associated service will be provided. If the firmware load test fails, the firmware will not be updated. If the cryptographic bypass test fails, the error is reported and all IPSec connections are terminated. If the pair-wise consistency test fails or the continuous random number generator test fails, an error is reported.



## **4.4 DESIGN ASSURANCE**

### **4.4.1 Delivery and Operation**

HP tracks each shipment and is able to provide confirmation to the customer that the FIPS-validated cryptographic module has been received. The *HP MSM765zl Mobility Controller Installation and Getting Started Guide* and the *HP MSM7xx Controllers Management and Configuration Guide* describe how the user can validate the receipt of an HP MSM765zl Mobility Controller that is part of the FIPS 140-2 validated cryptographic module.

HP MSM765zl Mobility Controllers are shipped in static bags with a seal closing each bag.

### **4.4.2 Functional Specification**

The functional specification for the HP MSM765zl Mobility Controller is contained in the *Functional Specification for the HP MSM765zl Mobility Controller* document. Functional specifications for the switches with their component modules also exist and were provided in support of the validation of the 5400/8200 zl Switch Series cryptographic modules.

### **4.4.3 Guidance Documents**

Crypto-Officer guidance for the cryptographic module is provided in this document and in the *HP MSM765zl Mobility Controller Installation and Getting Started Guide*, the *HP MSM7xx Controllers Management and Configuration Guide*, the *HP Switch Software Management and Configuration Guide* 3500 switches, 3500yl switches, 5400zl switches, 6200yl switches, 6600 switches, 8200zl switches.

User guidance for the HP MSM765zl Mobility Controller is provided in the Security Policy for the HP MSM430, HP MSM460, and HP MSM466 dual radio access points.





## 5 ADDITIONAL SECURITY RULES

### 5.1 ENFORCED SECURITY RULES

1. IPSec Security Associations are restricted to transforms Triple DES-SHA1 or AES-SHA1<sup>1</sup>.
2. Only 128-bit AES, 256-bit AES, or 3 key Triple DES will be negotiated as an encryption algorithm for an SSH session.

### 5.2 SECURITY RULES NOT ENFORCED BY THE CRYPTOGRAPHIC MODULE

1. When using a RADIUS server for authentication, the link between the HP MSM765zl Mobility Controller and the RADIUS server must be protected by IPSec. An IPSec transport mode connection for the RADIUS server can be configured on the **Authentication** page within the GUI management tool. Information on how to do this is provided in the *HP MSM765zl Mobility Controller Installation and Getting Started Guide* or the *HP MSM7xx Controllers Management and Configuration Guide*.
2. Any SNMP management must be done through IPSec sessions.
3. Automatic configuration backups must be secured through IPSec.
4. Active Directory, if used, must be used over IPSec.

---

<sup>1</sup> Please see NIST Special Publication 800-131A for requirements about SHA1 (SHA-1) usage.



## 6 IDENTIFICATION AND AUTHENTICATION POLICY

The identification and authentication policy includes specification of all roles, the associated type of authentication, the authentication data required of each role or operator, and the corresponding strength of the authentication mechanism.

| Role                                  | Type of Authentication | Authentication Data  |
|---------------------------------------|------------------------|--|
| Basic IPSec VPN User                  | Role-Based             | IPSec Preshared Secret   |
| X.509 IPSec VPN User                  | Identity-Based         | IPSec Local X.509 Certificate  |
| IPSec VPN User<br>(Aggressive Mode)   | Identity-Based         | IPSec Preshared Secret and IPSec Group Name and IPSec Group Password |
| SOAP Administrator                    | Identity-Based         | SOAP X.509 Certificate   |
| Access Point<br>(User)                | Role-Based             | Shared Secret for the Access Point                                   |
| Teamed Controller<br>(Crypto-Officer) | Role-Based             | Team Shared Secret   |
| Administrator<br>(Crypto-Officer)     | Role-Based             | Administrator Password   |

**Table 5 – Roles and Required Identification and Authentication**

There are no authorized physical maintenance activities for the cryptographic modules, and thus they do not support a Maintenance role.

| Authentication Mechanism | Strength of Mechanism  |
|--------------------------|--|
| IPSec Preshared Secret   | Minimum of 8 printable ASCII characters (82 different characters); probability of guessing preshared secret: 1 in $2.04 \times 10^{15}$<br>Maximum of 20 characters per preshared secret |
| IPSec Group Password     | Minimum of 8 printable ASCII characters (82 different characters); probability of guessing password: 1 in $2.04 \times 10^{15}$<br>Maximum of 20 characters per password                 |
| X.509 Certificates       | 2048-bit RSA keys, resulting in strength of 1 in $2^{112}$   |



|   |  |
|---|--|
| Shared Secret for the Access Point (used as key in HMAC-SHA-1 message authentication code provided to access point) | Minimum of 8 printable ASCII characters (82 different characters); probability of guessing shared secret: 1 in $2.04 \times 10^{15}$<br>Maximum of 20 characters per shared secret |
| Team Shared Secret (used as key in HMAC-SHA-1 message authentication code provided to access point)                 | Minimum of 8 printable ASCII characters (82 different characters); probability of guessing shared secret: 1 in $2.04 \times 10^{15}$<br>Maximum of 20 characters per shared secret |
| Administrator Password  | Minimum of 8 printable ASCII characters (82 different characters); probability of guessing password: 1 in $2.04 \times 10^{15}$<br>Maximum of 20 characters per password           |

**Table 6 – Strengths of Authentication Mechanisms**

The Administrator role, a Crypto-Officer type role, is assumed by executing the web configurator or starting an ssh session and logging in with the Administrator username and password. The Crypto-Officer role can also be assumed through a SOAP session. The cryptographic modules lock out access to it for five minutes after five invalid passwords. Therefore, for a one-time strength of 1 in  $2.04 \times 10^{15}$ , the corresponding strength for a one minute period is 1 in  $4.1 \times 10^{14}$ .

Authentication based upon RSA-signed certificates gives a much greater strength than 1 in 100,000. With the 10 Gb transceiver interface of the cryptographic modules, the authentication strength in a one minute period is greater than  $2^{102}$ . This also applies to IPsec User Roles. The authentication strength in a one minute period is greater than 1 in  $2.04 \times 10^5$ .

The access point authentication occurs over the Ethernet and could be automated. The processor speed for the HP MSM765zl Mobility Controller is 2.13 GHz. Also note that the Shared Secret for the Access Point or the Team Shared Secret is used in an HMAC computation and thus the controller would have to compute an HMAC from its copy of the Shared Secret for the Access Point or the Team Shared Secret. The maximum number of instructions that the processor can execute in a minute is  $1.28 \times 10^{11}$  so, to have an authentication strength of less than 1 in 100,000 or  $1 \times 10^5$ , the receipt and processing of the shared secret would need to take less than seven instructions. It of course takes more than seven seconds that so the required strength of authentication in a one minute period is met. The receipt of the HMAC computed using the Shared Secret for the Access Point, the computation of the HMAC from the copy of the shared secret that the controller has, and the comparison of the computed HMAC with the received HMAC, along with the other processing needed for the authentication, takes more than seven instructions.



## **7 ACCESS CONTROL POLICY**

### **7.1 OVERVIEW**

Section 7 Access Control Policy discusses the access that operator X, performing service Y while in role Z, has to security-relevant data item W for every role, service, and security-relevant data item contained in the cryptographic module.

The specification is of sufficient detail to identify the cryptographic keys and other CSPs that the operator has access to while performing a service, and the type(s) of access the operator has to the parameters.

### **7.2 CRYPTOGRAPHIC MODULE SERVICES**

#### **7.2.1 Show Status**

Purpose: Provide operating status information for the HP MSM765zl Mobility Controller  
 Approved Functions: AES, Triple DES, SHA-1, RSA, HMAC-SHA-1, PRNG  
 Service Inputs: Power-On  
 Service Outputs: LED Array

Status lights indicate the operational status of the HP MSM765zl Mobility Controller.

The home page of the web browser-based management tool provides a quick overview of the operational status of the HP MSM765zl Mobility Controller and provides a means of selecting more detailed status of the ports and connections.

#### **7.2.2 Perform Power-Up Self-Tests**

Purpose: Verify that the cryptographic module is operating correctly  
 Approved Functions: AES, Triple DES, SHA-1, RSA, HMAC-SHA-1, PRNG  
 Service Inputs: Self-Test Command  
 Service Outputs: Self-Test Result (via LED)

The success of the power-up self-tests is indicated by the Module Status LED, the first LED, being a solid green. The controller is operational.



### 7.2.3 Perform IPsec IKE

Purpose: Complete the IPsec IKE Exchange in preparation for ESP data transfer  
 Approved Functions: RSA Signature Verification, FIPS-Approved Pseudo-Random Number Generation  
 Allowed Function: Diffie-Hellman Key Establishment  
 Service Inputs: IKE Inputs  
 Service Outputs: IKE Outputs

### 7.2.4 Perform IPsec ESP Transfers

Purpose: Transfer authentication data and SNMP MIBs securely using the IPsec Encapsulating Security Payload packets  
 Approved Functions: AES, Triple DES, SHA-1, HMAC-SHA-1  
 Service Inputs: Packet to be Processed  
 Service Outputs: Processed Packet

The packet to be processed may be an outgoing plaintext packet that is to be converted into an IPsec packet before transmission or an incoming IPsec packet that is to be converted into a plaintext packet.

### 7.2.5 Perform Plaintext Data Transfer

Purpose: Transfer authentication data and SNMP MIBs in plaintext; bypass service  
 Approved Functions: HMAC-SHA-1  
 Service Inputs: Packet  
 Service Outputs: Unprocessed Packet

### 7.2.6 Access Point Management

Purpose: Configuration of HP MSM4xx Access Points  
 Approved Functions: RSA Key Generation and Signature Verification, Diffie-Hellman Key Agreement, AES in CBC mode, HMAC-SHA-1  
 Service Inputs: Configuration Information  
 Service Outputs: Indicator of Success or Failure of Operation



### **7.2.7 Controller Teaming**

Purpose: Teaming of the Controllers to Manage Access Points  
 Approved Functions: RSA Key Generation and Signature Verification, Diffie-Hellman Key Agreement, AES in CBC mode, HMAC-SHA-1  
 Service Inputs: Configuration Information  
 Service Outputs: Indicator of Success or Failure of Operation

### **7.2.8 Management of HP MSM765zl Mobility Controller through TLS**

Purpose: Management of HP MSM765zl Mobility Controller through Web  
 Approved Functions: RSA Key Generation and Signature Verification, Diffie-Hellman Key Agreement, AES in CBC mode, Triple DES in CBC mode, HMAC-SHA-1  
 Service Inputs: Configuration Information  
 Service Outputs: Indicator of Success or Failure of Operation

### **7.2.9 Management of HP MSM765zl Mobility Controller through SSH**

Purpose: Management of HP MSM765zl Mobility Controller through Console  
 Approved Functions: RSA Signature Verification, Diffie-Hellman Key Agreement, AES in CBC mode, Triple DES in CBC mode  
 Service Inputs: Configuration Information  
 Service Outputs: Indicator of Success or Failure of Operation

### **7.2.10 Management of HP MSM765zl Mobility Controller through SOAP**

Purpose: Management of HP MSM765zl Mobility Controller through Web  
 Approved Functions: RSA Key Generation and Signature Verification, Diffie-Hellman Key Agreement, AES in CBC mode, Triple DES in CBC mode, HMAC-SHA-1  
 Service Inputs: Configuration Information  
 Service Outputs: Indicator of Success or Failure of Operation



### **7.2.11 Firmware Load**

Purpose: Upgrade Firmware  
Approved Functions: HMAC-SHA-1, AES  
Service Inputs: New Firmware to be loaded on the HP MSM765zl Mobility Controller  
Service Outputs: New Firmware loaded on the HP MSM765zl Mobility Controller

### **7.2.12 Configuration File Export**

Purpose: Export Configuration File for Backup through TLS Session or SSH  
Approved Function: RSA Key Generation and Signature Verification, Diffie-Hellman Key Agreement, AES in CBC mode, Triple DES in CBC mode, HMAC-SHA-1  
Service Inputs: Backup Selected  
Service Outputs: Encrypted Configuration File with Encrypted Preshared Secrets, Passwords, Certificates, and Local RSA Private Key

### **7.2.13 Plaintext Key and CSP Zeroization**

Purpose: Zeroize Plaintext Cryptographic Keys and CSPs  
Approved Function: Zeroization  
Service Inputs: Request to Reset to Factory Default through web configurator  
Service Outputs: Factory Default Reset, Flash Memory Zeroized



### 7.3 ROLES, SERVICES, AND ACCESSES

#### 7.3.1 Anonymous Services

The following services are provided to users without requiring them to assume an authorized role.

| Service                     | Description  | Security Considerations   |
|-----------------------------|--|---|
| Perform Power-Up Self-Tests | The initial power-up self-tests of the cryptographic module do not require the operator to assume a role. It only requires the application of power. | The initial power-up self-tests do not use operational keys or CSPs and therefore do not affect the security of the cryptographic module. |

**Table 7 – Anonymous Services**

#### 7.3.2 Role-Based Services

This section discusses, for each role, the services an operator is authorized to perform within that role, and for each service within each role, the type(s) of access to the cryptographic keys and CSPs.

| Role   | Authorized Services   |
|--|---|
| IPSec VPN User (independent of authorization type) | Perform IPSec IKE<br>Perform IPSec ESP Transfers<br>Perform Plaintext Data Transfer   |
| Access Point (User)                                | Access Point Management   |
| Teamed Controller (Crypto-Officer)                 | Controller Teaming  |
| SOAP Administrator (Crypto-Officer)                | Management of HP MSM765zl Mobility Controller through SOAP  |
| Administrator (Crypto-Officer)                     | Perform Power-Up Self-Tests (Command)<br>Show Status<br>Management of HP MSM765zl Mobility Controller through TLS<br>Management of HP MSM765zl Mobility Controller through SSH<br>Firmware Load<br>Configuration File Export<br>Plaintext Key and CSP Zeroization |

**Table 8 – Services Authorized for Roles**





## 7.4 NON-FIPS APPROVED SERVICES

The cryptographic modules also provide the following services that are not allowed in the FIPS approved mode of operation:

- NOC-based authentication  
An HTTP interface where an external server can tell us if a given user is authorized for access;
- Payment services  
The acquiring of credit card or PayPal information;
- Billing records logging;
- L2TP services;
- PPTP services;
- Mobility manager services  
Provided through a management console that uses a TLS tunnel to transfer status and configuration information to the controller;
- Automatic firmware installation  
Provision for the automatic update of the firmware of the controller; not allowed in FIPS mode because it cannot be verified that the automatically loaded firmware has been FIPS-validated; and
- System debug tool.



## **7.5 SECURITY DATA**

### **7.5.1 General**

Security data comprises all cryptographic keys and CSPs employed by the cryptographic module, including secret, private, and public cryptographic keys (both plaintext and encrypted), authentication data such as passwords or PINs, and other security-relevant information (e.g., audited events and audit data).

### **7.5.2 Cryptographic Keys**

- AES Secret Keys
- Triple DES Secret Keys
- HMAC Secret Keys
- RSA Public and Private Keys
- PRNG Seed Key
- Diffie-Hellman Public and Private Keys

RSA public keys in X.509 certificates are stored by the cryptographic module.

RSA public keys and Diffie-Hellman public keys are not considered to be critical security parameters.

### **7.5.3 Critical Security Parameters**

- IPSec Preshared Secret
- Shared Secret for the Access Point
- Team Shared Secret
- Administrator Password
- IPSec Group Password
- PRNG Seed



### 7.5.4 Cryptographic Key Management

| Cryptographic Key or CSP   | Key Length | Key Strength | FIPS Approved Establishment Mechanism   | State within Module |
|--|------------|--------------|---|---------------------|
| IPSec Local X.509 Certificates RSA Public Keys (not CSPs)                        | 2048 bits  | 112 bits     | Internally-generated with ANSI X9.31 RSA Key Generation<br>or<br>Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with IPSec RSA Private Key)         | Plaintext in HDD    |
| IPSec RSA Private Keys (mates of IPSec Local X.509 Certificates RSA Public Keys) | 2048 bits  | 112 bits     | Internally-generated with ANSI X9.31 RSA Key Generation<br>or<br>Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with IPSec Local X.509 Certificate) | Plaintext in HDD    |
| IPSec CA X.509 Certificate RSA Public Key (not a CSP)                            | 2048 bits  | 112 bits     | Internally-generated with ANSI X9.31 RSA Key Generation<br>or<br>Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with IPSec CA RSA Private Key)      | Plaintext in HDD    |



|   |                                     |                                  |   |                         |
|---|-------------------------------------|----------------------------------|---|-------------------------|
| <p>IPSec CA RSA Private Key (mate of IPSec CA X.509 Certificate RSA Public Key)</p> | <p>2048 bits</p>                    | <p>112 bits</p>                  | <p>Internally-generated with ANSI X9.31 RSA Key Generation<br/>or<br/>Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with IPSec CA X.509 Certificate)</p> | <p>Plaintext in HDD</p> |
| <p>SOAP X.509 Certificates RSA Public Keys (not CSPs)</p>                           | <p>1024 bits<br/><br/>2048 bits</p> | <p>80 bits<br/><br/>112 bits</p> | <p>Externally-generated; included with firmware<br/>or<br/>Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with SOAP RSA Private Key)</p>                  | <p>Plaintext in HDD</p> |
| <p>SOAP RSA Private Keys (mates of SOAP X.509 Certificates RSA Public Keys)</p>     | <p>1024 bits<br/><br/>2048 bits</p> | <p>80 bits<br/><br/>112 bits</p> | <p>Externally-generated; included with firmware<br/>or<br/>Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with SOAP X.509 Certificate)</p>                | <p>Plaintext in HDD</p> |



|  |                        |                     |   |                  |
|--|------------------------|---------------------|---|------------------|
| Web Server X.509 Certificates RSA Public Keys (not CSPs)                             | 2048 bits              | 112 bits            | Externally generated; part of new firmware or Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with Web Server RSA Private Key)     | Plaintext in HDD |
| Web Server RSA Private Keys (mates of Web Server X.509 Certificates RSA Public Keys) | 2048 bits              | 112 bits            | Externally generated; part of new firmware or Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with Web Server X.509 Certificate)   | Plaintext in HDD |
| RADIUS EAP X.509 Certificates RSA Public Keys (not CSPs)                             | 1024 bits<br>2048 bits | 80 bits<br>112 bits | Externally-generated; included with firmware or Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with RADIUS EAP RSA Private Key)   | Plaintext in HDD |
| RADIUS EAP RSA Private Keys (mates of RADIUS EAP X.509 Certificates RSA Public Keys) | 1024 bits<br>2048 bits | 80 bits<br>112 bits | Externally-generated; included with firmware or Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key (in PKCS #12 file with RADIUS EAP X.509 Certificate) | Plaintext in HDD |



|  |  |  |  |                    |
|--|--|--|--|--------------------|
| CA X.509 Certificates RSA Public Keys (not CSPs)                                 | 2048 bits  | 112 bits   | Externally-generated; included with firmware or Externally-generated and EE/ED encrypted with TLS Session Key or SSH Session Key | Plaintext in HDD   |
| Controller X.509 Certificate RSA Public Key (not a CSP)                          | 2048 bits  | 112 bits   | Internally-generated with ANSI X9.31 RSA Key Generation; ED  | Plaintext in HDD   |
| Controller RSA Private Key (mate of Controller X.509 Certificate RSA Public Key) | 2048 bits  | 112 bits   | Internally-generated with ANSI X9.31 RSA Key Generation  | Plaintext in HDD   |
| Access Points X.509 Certificates RSA Public Keys (not CSPs)                      | 2048 bits  | 112 bits   | EE/ED  | Plaintext in HDD   |
| Slave Controllers X.509 Certificates RSA Public Keys (not CSPs)                  | 2048 bits  | 112 bits   | EE/ED  | Plaintext in HDD   |
| Diffie-Hellman Private Keys  | 1024 or 1536 bits                                | 80 or 96 bits  | Internally-generated with ANSI X9.31 PRNG  | Ephemeral in SDRAM |
| Diffie-Hellman Public Keys (not CSPs)  | 1024 or 1536 bits                                | 80 or 96 bits  | Internally-generated with ANSI X9.31 PRNG; EE/ED to and from controller  | Ephemeral in SDRAM |
| TLS Session Keys   | 168-bit Triple DES key or 128 or 256 bit AES key | 112 bits for 168-bit Triple DES key; 128 or 256 bits for AES key | EE/ED; encrypted with RSA public key or agreed upon using Diffie-Hellman key agreement   | Ephemeral in SDRAM |



|   |  |  |   |   |
|---|--|--|---|---|
| TLS Integrity Keys                      | HMAC keys  | All HMAC key sizes   | EE/ED; encrypted with RSA public key  | Ephemeral in SDRAM                                |
| SSH Session Keys                        | 168-bit Triple DES key or 128 or 256 bit AES key | 112 bits for 168-bit Triple DES key; 128 or 256 bits for AES key | EE/ED; agreed upon using Diffie-Hellman key agreement   | Ephemeral in SDRAM                                |
| AES Session Keys                        | 128 or 256 bits                                  | 128 or 256 bits  | IPSec IKE   | Ephemeral in SDRAM                                |
| HMAC IPSec Keys                         | 20-byte HMAC key                                 | 160 bits   | IPSec IKE   | Ephemeral in SDRAM                                |
| IPSec Initialization Vectors (not CSPs) | 128 bits   | N/A  | IPSec IKE; ED   | Ephemeral in SDRAM                                |
| HMAC Bypass Key                         | 160 bits   | 160 bits   | EE/ED; Encrypted with AES Firmware Encryption Key   | Plaintext in HDD and SDRAM; hardcoded in firmware |
| AES Firmware Encryption Key             | 128 bits   | 128 bits   | N/A   | Plaintext in HDD and SDRAM; hardcoded in firmware |
| HMAC Firmware Verification Key          | 160 bits   | 160 bits   | EE/ED; Encrypted with AES Firmware Encryption Key   | Plaintext in HDD and SDRAM; hardcoded in firmware |
| Administrator Password                  | Minimum of 8 characters                          | 1 in 2.04 X 10 <sup>15</sup>                                     | EE; ED – Web Configurator; MD – console; RSA key transport – minimum 80 bits equivalent encryption strength | Plaintext in HDD                                  |



|                                    |                         |                            |  |                    |
|------------------------------------|-------------------------|----------------------------|--|--------------------|
| IPSec Preshared Secrets            | Minimum of 8 characters | 1 in $2.04 \times 10^{15}$ | EE;<br>ED – Web Configurator;<br>MD – console;<br>RSA key transport – minimum 80 bits equivalent encryption strength | Plaintext in HDD   |
| Group Passwords                    | Minimum of 8 characters | 1 in $2.04 \times 10^{15}$ | EE;<br>ED – Web Configurator;<br>MD – console;<br>RSA key transport – minimum 80 bits equivalent encryption strength | Plaintext in HDD   |
| Shared Secret for the Access Point | Minimum of 8 characters | 1 in $2.04 \times 10^{15}$ | N/A;<br>Used as HMAC key for HMAC computation  | Plaintext in HDD   |
| Team Shared Secret                 | Minimum of 8 characters | 1 in $2.04 \times 10^{15}$ | N/A;<br>Used as HMAC key for HMAC computation  | Plaintext in HDD   |
| PRNG Seed Key (AES Key)            | 256 bits                | 256 bits                   | Internally generated with /dev/urandom PRNG  | Ephemeral in SDRAM |
| PRNG Seed                          | 128 bits                | 128 bits                   | Internally generated with /dev/urandom PRNG  | Ephemeral in SDRAM |

**Table 9 – Cryptographic Keys and Other Critical Security Parameters Table**





**Table 10** specifies the pseudo-random number generators utilized by the cryptographic modules.

| Identification   | Type         | Usage  |
|--|--------------|--|
| <i>ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES PRNG using AES with 256-bit keys</i> | Approved     | Used when random data is needed when generating an RSA key pair or a Diffie-Hellman key pair |
| /dev/urandom PRNG  | Not Approved | Generation of seed keys and seed values for approved PRNG                                    |

**Table 10 – Pseudo-Random Number Generators**

**Table 11** specifies for all cryptographic keys and other CSPs, whether or not they are output, and, if so, the format in which they are output and their destination.

| Identification  | Output | Destination        | Format                         |
|---|--------|--------------------|--------------------------------|
| IPSec Local X.509 Certificates RSA Public Keys (not CSPs) | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| IPSec RSA Private Keys                                    | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| IPSec CA X.509 Certificate Public Key (not a CSP)         | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| IPSec CA RSA Private Key                                  | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| SOAP X.509 Certificates RSA Public Keys (not CSPs)        | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| SOAP RSA Private Keys                                     | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| Web Server X.509 Certificates RSA Public Keys (not CSPs)  | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| Web Server RSA Private Keys                               | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| RADIUS EAP X.509 Certificates RSA Public Keys (not CSPs)  | Yes    | To Backup Computer | Encrypted with TLS Session Key |
| RADIUS EAP RSA Private Keys                               | Yes    | To Backup Computer | Encrypted with TLS Session Key |



|   |     |   |                                |
|---|-----|---|--------------------------------|
| CA X.509 Certificates RSA Public Keys (not CSPs)                | Yes | To Backup Computer  | Encrypted with TLS Session Key |
| Controller X.509 Certificate RSA Public Key (not a CSP)         | Yes | To HP MSM4xx Access Points  | Plaintext                      |
| Controller RSA Private Key                                      | No  | Not Applicable  | Not Applicable                 |
| Access Points X.509 Certificates RSA Public Keys (not CSPs)     | Yes | To HP MSM4xx Access Points  | Plaintext                      |
| Slave Controllers X.509 Certificates RSA Public Keys (not CSPs) | Yes | To Slave Controllers  | Plaintext                      |
| Diffie-Hellman Private Key                                      | No  | Not Applicable  | Not Applicable                 |
| Diffie-Hellman Public Keys (not CSPs)                           | No  | To HP MSM4xx Access Points, RADIUS Server, or Management Computer | Plaintext                      |
| TLS Session Keys  | Yes | To HP MSM4xx Access Points or Management Computer                 | Encrypted with RSA Public Key  |
| TLS Integrity Keys  | Yes | To HP MSM4xx Access Points or Management Computer                 | Encrypted with RSA Public Key  |
| SSH Session Keys  | No  | Not Applicable  | Not Applicable                 |
| AES Session Keys  | No  | Not Applicable  | Not Applicable                 |
| HMAC IPsec Keys   | No  | Not Applicable  | Not Applicable                 |
| IPsec Initialization Vectors                                    | Yes | To RADIUS Server or Management Computer                           | Plaintext                      |
| HMAC Bypass Key   | No  | Not Applicable  | Not Applicable                 |
| AES Firmware Encryption Key                                     | No  | Not Applicable  | Not Applicable                 |
| HMAC Firmware Verification Key                                  | No  | Not Applicable  | Not Applicable                 |
| Administrator Password  | Yes | To Backup Computer  | Encrypted with TLS Session Key |
| IPsec Preshared Secrets   | Yes | To Backup Computer  | Encrypted with TLS Session Key |



|                                    |     |                    |                                |
|------------------------------------|-----|--------------------|--------------------------------|
| Group Passwords                    | Yes | To Backup Computer | Encrypted with TLS Session Key |
| Shared Secret for the Access Point | No  | Not Applicable     | Not Applicable                 |
| Team Shared Secret                 | No  | Not Applicable     | Not Applicable                 |
| PRNG Seed Key (AES Key)            | No  | Not Applicable     | Not Applicable                 |
| PRNG Seed                          | No  | Not Applicable     | Not Applicable                 |

**Table 11 – Cryptographic Module Cryptographic Key and Other CSP Output**

**Table 12** specifies the access to cryptographic keys and other CSPs that an operator has to each of the cryptographic keys and other CSPs for all services.

| Service                     | Cryptographic Keys and CSPs   | Type(s) of Access (e.g., Read, Write, Execute) |
|-----------------------------|---|--|
| Show Status                 | Administrator Password  | E  |
|                             | TLS Session Keys  | E  |
|                             | TLS Integrity Keys  | E  |
| Perform Power-Up Self-Tests | AES Keys, Triple DES Keys, RSA Public and Private Keys, HMAC Keys, PRNG Seed, PRNG Seed Key (Power-Up Self-Test Only Keys – not CSPs) | E  |
|                             | Administrator Password (for command)  | E  |
|                             | TLS Session Key (for command)   | E  |
|                             | TLS Integrity Key (for command)   | E  |



|                                 |   |      |
|---------------------------------|---|------|
| Perform IPSec IKE               | Administrator Password                                      | E    |
|                                 | IPSec Preshared Secrets                                     | E    |
|                                 | IPSec Group Passwords                                       | E    |
|                                 | IPSec Local X.509 Certificates RSA Public Keys (not CSPs)   | W, E |
|                                 | IPSec RSA Private Keys                                      | W, E |
|                                 | IPSec CA X.509 Certificate RSA Public Key (not a CSP)       | E    |
|                                 | IPSec CA RSA Private Key                                    | E    |
|                                 | PRNG Seed   | W, E |
|                                 | PRNG Seed Key   | W, E |
|                                 | AES Session Keys  | W    |
|                                 | HMAC IPSec Keys   | W    |
|                                 | HMAC Bypass Key   | E    |
|                                 | Diffie-Hellman Private Keys                                 | W, E |
|                                 | Diffie-Hellman Public (not CSPs)                            | W, E |
| Perform IPSec ESP Transfers     | AES Session Keys  | E    |
|                                 | HMAC IPSec Keys   | E    |
|                                 | IPSec Initialization Vectors (not CSPs)                     | W, E |
| Perform Plaintext Data Transfer | Administrator Password                                      | E    |
|                                 | HMAC Bypass Key   | E    |
| Access Point Management         | Administrator Password                                      | E    |
|                                 | Shared Secret for the Access Point                          | E    |
|                                 | CA X.509 Certificate RSA Public Key (not a CSP)             | E    |
|                                 | Controller X.509 Certificate RSA Public Key (not a CSP)     | W, E |
|                                 | Controller RSA Private Key                                  | W    |
|                                 | Access Points X.509 Certificates RSA Public Keys (not CSPs) | W, E |
|                                 | RADIUS EAP X.509 Certificates RSA Public Keys (not CSPs)    | W, E |
|                                 | RADIUS EAP RSA Private Keys                                 | W    |
|                                 | Diffie-Hellman Private Keys                                 | W, E |
|                                 | Diffie-Hellman Public Keys (not CSPs)                       | W, E |
|                                 | TLS Session Keys  | W, E |
|                                 | TLS Integrity Keys  | W, E |
|                                 | PRNG Seed   | W, E |
|                                 | PRNG Seed Key   | W, E |



|   |  |                        |
|---|--|------------------------|
| Controller Teaming  | Administrator Password   | E                      |
|   | Team Shared Secret   | E                      |
|   | CA X.509 Certificate RSA Public Key (not a CSP)                | E                      |
|   | Controller X.509 Certificate RSA Public Key (not a CSP)        | W, E                   |
|   | Controller RSA Private Key                                     | W, E                   |
|   | Slave Controllers X.509 Certificate RSA Public Keys (not CSPs) | W, E                   |
|   | Diffie-Hellman Private Keys                                    | W, E                   |
|   | Diffie-Hellman Public Keys (not CSPs)                          | W, E                   |
|   | TLS Session Keys   | W, E                   |
|   | TLS Integrity Keys   | W, E                   |
|   | PRNG Seed  | W, E                   |
|   | PRNG Seed Key  | W, E                   |
|   | Management of HP MSM765zl Mobility Controller through TLS      | Administrator Password |
| Web Server X.509 Certificates RSA Public Keys (not CSPs)  |  | R, W                   |
| Web Server RSA Private Keys                               |  | W                      |
| CA X.509 Certificates RSA Public Key (not a CSP)          |  | E                      |
| Diffie-Hellman Private Keys                               |  | W, E                   |
| Diffie-Hellman Public Keys (not CSPs)                     |  | W, E                   |
| TLS Session Keys  |  | W, E                   |
| TLS Integrity Keys  |  | W, E                   |
| PRNG Seed   |  | W, E                   |
| PRNG Seed Key   |  | W, E                   |
| Management of HP MSM765zl Mobility Controller through SSH | Administrator Password   | E                      |
|   | Diffie-Hellman Private Keys                                    | W, E                   |
|   | Diffie-Hellman Public Keys (not CSPs)                          | W, E                   |
|   | SSH Session Keys   | W, E                   |
|   | PRNG Seed  | W, E                   |
|   | PRNG Seed Key  | W, E                   |



|  |   |      |
|--|---|------|
| Management of HP MSM765zl Mobility Controller through SOAP | SOAP X.509 Certificates RSA Public Keys (not CSPs)        | R, W |
|  | SOAP RSA Private Keys                                     | W    |
|  | Diffie-Hellman Private Keys                               | W, E |
|  | Diffie-Hellman Public Keys (not CSPs)                     | W, E |
|  | TLS Session Keys  | W, E |
|  | TLS Integrity Keys  | W, E |
|  | PRNG Seed   | W, E |
|  | PRNG Seed Key   | W, E |
| Firmware Load  | Administrator Password                                    | E    |
|  | TLS Session Key   | E    |
|  | TLS Integrity Key   | E    |
|  | AES Firmware Encryption Key                               | E    |
|  | HMAC Firmware Verification Key                            | E    |
| Configuration File Export                                  | Administrator Password                                    | E    |
|  | AES Session Key   | E    |
|  | TLS Session Key   | E    |
|  | TLS Integrity Key   | E    |
|  | IPSec Local X.509 Certificates RSA Public Keys (not CSPs) | W    |
|  | IPSec RSA Private Keys                                    | W    |
|  | IPSec CA X.509 Certificate Public Key (not a CSP)         | W    |
|  | IPSec CA RSA Private Key                                  | W    |
|  | SOAP X.509 Certificates RSA Public Keys (not CSPs)        | W    |
|  | SOAP RSA Private Keys                                     | W    |
|  | Web Server X.509 Certificates RSA Public Keys (not CSPs)  | W    |
|  | Web Server RSA Private Keys                               | W    |
|  | RADIUS EAP X.509 Certificates RSA Public Keys (not CSPs)  | W    |
|  | RADIUS EAP RSA Private Keys                               | W    |
|  | CA X.509 Certificates RSA Public Keys (not CSPs)          | W    |
|  | IPSec Preshared Secrets                                   | W    |
|  | IPSec Group Passwords                                     | W    |
|  | Shared Secret for the Access Point                        | W    |
| Team Shared Secret   | W   |      |



|                                      |   |      |
|--------------------------------------|---|------|
| Plaintext Key and CSP<br>Zeroization | Administrator Password  | E, W |
|                                      | TLS Session Key   | E    |
|                                      | TLS Integrity Key   | E    |
|                                      | IPSec Local X.509 Certificates RSA Public Keys (not CSPs)       | W    |
|                                      | IPSec RSA Private Keys  | W    |
|                                      | IPSec CA X.509 Certificate Public Key (not a CSP)               | W    |
|                                      | IPSec CA RSA Private Key  | W    |
|                                      | SOAP X.509 Certificates RSA Public Keys (not CSPs)              | W    |
|                                      | SOAP RSA Private Keys   | W    |
|                                      | Web Server X.509 Certificates RSA Public Keys (not CSPs)        | W    |
|                                      | Web Server RSA Private Keys                                     | W    |
|                                      | RADIUS EAP X.509 Certificates RSA Public Keys (not CSPs)        | W    |
|                                      | RADIUS EAP RSA Private Keys                                     | W    |
|                                      | CA X.509 Certificates RSA Public Keys (not CSPs)                | W    |
|                                      | Controller X.509 Certificate RSA Public Key (not a CSP)         | W    |
|                                      | Controller RSA Private Key                                      | W    |
|                                      | Access Points X.509 Certificates RSA Public Keys (not CSPs)     | W    |
|                                      | Slave Controllers X.509 Certificates RSA Public Keys (not CSPs) | W    |
|                                      | IPSec Preshared Secrets   | W    |
|                                      | IPSec Group Passwords   | W    |
| Shared Secret for the Access Point   | W   |      |
| Team Shared Secret                   | W   |      |

**Table 12 – Access Rights within Services**



## 7.6 IMPLEMENTED CRYPTOGRAPHIC ALGORITHMS

The following table outlines the FIPS approved cryptographic algorithms that are implemented in the cryptographic modules, along with the Cryptographic Algorithm Validation Program (CAVP) validation number for each algorithm.

| FIPS Approved Cryptographic Algorithm  | Algorithm Validation Number(s) |
|--|--------------------------------|
| AES (128 or 256 bit keys) CBC encryption in firmware (2 implementations)   | 1824 and 1825                  |
| *Triple DES (168-bit keys) encryption and decryption in CBC mode in firmware (2 implementations)   | 1177 and 1178                  |
| *SHA-1 hashing (firmware – 2 implementations)  | 1603 and 1604                  |
| HMAC-SHA-1 message authentication (firmware – 2 implementations)   | 1107 and 1079                  |
| RSA (2048 bit key PKCS#1 v1.5 signature verification and ANSI X9.31 key generation in firmware and 1024 and 2048 bit PKCS#1 v1.5 RSA signature verification in firmware) | 917 and 921                    |
| *ANSI X9.31 PRNG using 256-bit AES   | 961                            |

\* For deprecation information, see NIST SP800-131A.

**Table 13 – Implemented FIPS Approved Cryptographic Algorithms**

The cryptographic modules implement the following non-FIPS approved cryptographic algorithms: RC4, MD5, HMAC-MD5, Diffie-Hellman key agreement with 1024 bit (Group 2) or 1536 bit (Group 5) keys (key establishment methodology provides 80 or 96 bits of equivalent encryption strength), and RSA key transport with 1024 or 2048 bit keys (key transport method provides 80 or 112 bits of equivalent key strength).

The cryptographic modules also implement SHA-224, SHA-256, SHA-384, SHA-512, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512, which are not FIPS compliant because all cryptographic module requirements for these cryptographic algorithms have not been met.





## 8 PHYSICAL SECURITY POLICY

### 8.1 OVERVIEW

Section 8 Physical Security Policy discusses the physical security mechanisms that are implemented to protect the cryptographic modules and the actions that are required to ensure that the physical security of the cryptographic module is maintained.

### 8.2 PHYSICAL SECURITY MECHANISMS

#### 8.2.1 Tamper Evident Seals, Opacity Shields, and High Performance Fan Tray

The cryptographic modules are completely enclosed within metal Ethernet switch chassis.

The cryptographic modules are protected by tamper evident seals on all sides of the switch chassis. Opacity shields are to be installed on either side of the switch chassis and a high performance fan tray is to be used at the back of the chassis to cover the fan. See sections 2.3 and 2.4 for details on where and how to install the opacity shields and high performance fan tray and on how and where to affix the tamper evident seals.

The tamper evident seals provided by HP should be kept in a locked cabinet, accessible only by the Administrator (Crypto-Officer) for the particular cryptographic module. The cryptographic module should be kept in a locked cabinet or room until the opacity shields and high performance fan tray are installed on the chassis and until the tamper evident seals can be affixed where required.

### 8.3 INSPECTION AND TESTING

| Physical Security Mechanism                   | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details   |
|---|--|--|
| High Performance Fan Tray and Opacity Shields | Monthly                                  | Examine visually to ensure the fan tray or opacity shields have not been bent, have not had holes drilled in them, or have not been removed. |
| Tamper Evident Seals                          | Weekly preferred but at least monthly    | Examine visually for evidence that any seal has been damaged, broken, or missing   |

**Table 14 – Inspection/Testing of Physical Security Mechanisms**



The inspection of the tamper evident seals, high performance fan tray, and opacity shields is to be done by the Administrator (Crypto-Officer).



**9 SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS**

**9.1 OVERVIEW**

The cryptographic modules do not mitigate against specific attacks for which testable requirements are not defined in FIPS 140-2.

**9.2 MECHANISMS IMPLEMENTED**

Not applicable

**9.3 MITIGATION SUMMARY**

| Other Attacks | Mitigation Mechanisms | Specific Limitations |
|---------------|-----------------------|----------------------|
| None          | N/A                   | N/A                  |

**Table 15 – Mitigation of Other Attacks**