NON-PROPRIETARY CRYPTOGRAPHIC MODULE SECURITY POLICY FOR THE

HP MSM430 DUAL RADIO 802.11N TAA AP,
HARDWARE VERSION: J9654A;

HP MSM430 DUAL RADIO 802.11N AP (WW),
HARDWARE VERSION: J9651A;

HP MSM430 DUAL RADIO 802.11N AP (JP),
HARDWARE VERSION: J9652A;

HP MSM460 DUAL RADIO 802.11N TAA AP,
HARDWARE VERSION: J9655A;

HP MSM460 DUAL RADIO 802.11N AP (WW),
HARDWARE VERSION: J9591A;

HP MSM460 DUAL RADIO 802.11N AP (JP),
HARDWARE VERSION: J9589A;

HP MSM466 DUAL RADIO 802.11N TAA AP,
HARDWARE VERSION: J9656A;

HP MSM466 DUAL RADIO 802.11N AP (WW),
HARDWARE VERSION: J9622A; AND

HP MSM466 DUAL RADIO 802.11N AP (JP),
HARDWARE VERSION: J9620A

WITH

FIRMWARE VERSION: 5.6.0

DOCUMENT VERSION: 1.10
23 APRIL 2012

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

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 PURPOSE 1
1.2 SCOPE 2
1.3 INTENDED USE 3
1.4 ACRONYMS 3

2 HP MSM4xx ACCESS POINTS OVERVIEW 6

2.1 ENCLOSURE AND CONNECTORS 6
2.2 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES 8
2.3 TAMPER EVIDENT SEALS 10
2.4 FEATURES 12
2.5 HP MSM4XX AP CRYPTOGRAPHIC MODULE BOUNDARY 12
2.6 FIPS PUB 140-2 TARGETED SECURITY LEVELS 13

3 PRODUCT OPERATION 13

3.1 OVERVIEW 13
3.2 FIPS APPROVED MODE OF OPERATION: CONTROLLED MODE 14
STEP 1: LOAD THE FIPS VALIDATED FIRMWARE ON THE ACCESS POINT 14
STEP 2: PROVISIONING FROM THE AUTONOMOUS MODE 18
STEP 3: PROVISIONING FROM THE CONTROLLED MODE 21
3.3 FIPS APPROVED MODE OF OPERATION: CONFIGURATION TO BE DONE WITH THE HP MSM765ZL MOBILITY CONTROLLER 24
STEP 1: SETTING TLSV1 FOR THE MANAGEMENT LINK FROM THE MOBILITY CONTROLLER 25
STEP 2: ENTER THE SHARED SECRET FOR THE ACCESS POINTS TO BE CONTROLLED 26
STEP 3: SPECIFY THE WIRELESS SECURITY FOR THE ACCESS POINT 27
STEP 4: SET THE REQUIRED RESTRICTIONS 31

4 SECURITY RULES DERIVED FROM THE REQUIREMENTS OF FIPS PUB 140-2 43

4.1 FINITE STATE MODEL 43
4.2 ELECTROMAGNETIC INTERFERENCE / ELECTROMAGNETIC COMPATIBILITY (EMI/EMC) 43

4.3 SELF-TESTS 44
4.3.1 Power-Up Self-Tests 44
4.3.2 Conditional Self-Tests 45
4.4 DESIGN ASSURANCE 46
4.4.1 Delivery and Operation 46
4.4.2 Functional Specification 46
4.4.3 Guidance Documents 46

5 ADDITIONAL SECURITY RULES 47

6 IDENTIFICATION AND AUTHENTICATION POLICY 48

7 ACCESS CONTROL POLICY 49

7.1 OVERVIEW 49
7.2 CRYPTOGRAPHIC MODULE SERVICES 49
7.2.1 Show Status 50
7.2.2 Perform Power-Up Self-Tests 50
7.2.3 Perform EAPOL Communication 50
7.2.4 Perform WPA2 Secure Wireless Communication 50
7.2.5 Perform Plaintext Wireless Communication 51
7.2.6 Management through TLS Session 51
7.2.7 Plaintext Key and CSP Zeroization 51
7.3 ROLES, SERVICES AND ACCESSES 52
7.3.1 Anonymous Services 52
7.3.2 Role-Based Services 52
7.4 SECURITY DATA 53
7.4.1 General 53
7.4.2 Cryptographic Keys 53
7.4.3 Critical Security Parameters 53
7.4.4 Cryptographic Key Management 54
7.5 IMPLEMENTED CRYPTOGRAPHIC ALGORITHMS 60

8 PHYSICAL SECURITY POLICY 61

8.1 OVERVIEW 61
8.2 PHYSICAL SECURITY MECHANISMS 61
8.2.1 Tamper Evident Seals 61
8.3 INSPECTION AND TESTING 61

9 SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS 62

9.1 OVERVIEW 62
9.2 MECHANISMS IMPLEMENTED 62
9.3 MITIGATION SUMMARY 62

TABLE OF TABLES

Table 1 – Cryptographic Module Ports and Interfaces 9
Table 2 – FIPS 140-2 Targeted Security Levels for Requirement Sections 13
Table 3 – Roles and Required Identification and Authentication 48
Table 4 – Strengths of Authentication Mechanisms 48
Table 5 – Anonymous Services 52
Table 6 – Services Authorized for Roles 52
Table 7 – Cryptographic Keys and Other Critical Security Parameters Table 56
Table 8 – HP MSM4xx AP Pseudo-Random Number Generators 56
Table 9 – HP MSM4xx AP Key Output 57
Table 10 – Access Rights within Services 59
Table 11 – Implemented FIPS Approved Cryptographic Algorithms 60
Table 12 – Inspection/Testing of Physical Security Mechanisms 61
Table 13 – Mitigation of Other Attacks 62

TABLE OF FIGURES

Figure 1 – HP MSM4xx APs 7
Figure 2 – Back View of the HP MSM430/460 8
Figure 3 – Placement of Tamper Evident Seals on the HP MSM430, HP MSM460, and HP MSM466 Access Points 11
Figure 4 – Back of an HP MSM430/460 with the Tamper Evident Seal (Second Seal) Affixed. 12

1 INTRODUCTION

1.1 PURPOSE

This document defines the security policy for the following wireless access points:

MSM430
- HP MSM430 Dual Radio 802.11n TAA AP (hardware version: J9654A);
- HP MSM430 Dual Radio 802.11n AP (WW) ((hardware version: J9651A); and
- HP MSM430 Dual Radio 802.11n AP (JP) ((hardware version: J9652A);

MSM460
- HP MSM460 Dual Radio 802.11n TAA AP ((hardware version: J9655A);
- HP MSM460 Dual Radio 802.11n AP (WW) ((hardware version: J9591A); and
- HP MSM460 Dual Radio 802.11n AP (JP) ((hardware version: J9589A); and

MSM466
- HP MSM466 Dual Radio 802.11n TAA AP ((hardware version: J9656A);
- HP MSM466 Dual Radio 802.11n AP (WW) ((hardware version: J9622A); and
- HP MSM466 Dual Radio 802.11n AP (JP) ((hardware version: J9620A).

TAA stands for Trade Agreements Act; WW stands for worldwide; and JP stands for Japan.

These access points all have firmware version 5.6.0.

The designation HP MSM4xx AP will be used to refer to an access point when the statement made applies to any of the access points covered by this document.

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 HP MSM4xx AP, as implemented, satisfies a stated security policy; and

b. To describe to individuals and organizations the capabilities, protection, and access rights provided by the HP MSM4xx AP, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

1.4 ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Access Point
ASCII	American Standard Code for Information Interchange
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining Mode
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CFR	Code of Federal Regulations
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
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)
HMAC	Keyed-Hashing for Message Authentication Code
HP	Hewlett-Packard
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
JP	Japan
KCK	Key Confirmation Key
KEK	Key Encryption Key
LAN	Local Area Network
LED	Light Emitting Diode
L2TP	Layer Two (2) Tunneling Protocol
MAC	Media Access Control or Message Authentication Code
MD	Manual Distribution or Message Digest
MHz	Megahertz
MPDU	MAC Protocol Data Unit
MSM	Multiservice Mobility
NAND	Not AND (a type of flash memory)
NIST	National Institute of Standards and Technology
N/A	Not Applicable
PEAP	Protected Extensible Authentication Protocol
PKCS#1	Public Key Cryptographic Standard #1
PMK	Pairwise Master Key
PPTP	Point-to-Point Tunneling Protocol
PRF	Pseudo-Random Function
PRNG	Pseudo-Random Number Generator
PSK	Preshared Key
PTK	Pairwise Transient Key
RSA	Rivest Shamir Adleman asymmetric cryptographic algorithm
RSN	Robust Security Network
SDRAM	Synchronous Dynamic Random Access Memory
SHA-1	Secure Hash Algorithm First Revision (1)
SOAP	Simple Object Access Protocol
SP	Special Publication
SSL	Secure Sockets Layer

TAA	Trade Agreements Act
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
Triple DES	Triple Data Encryption Standard
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSC	Virtual Service Community
WPA2	WiFi Protected Access version 2
WW	Worldwide

2 HP MSM4XX ACCESS POINTS OVERVIEW

The HP MSM4xx APs enable strong security for wireless enterprise networking using IEEE 802.11i RSN encrypted wireless communication. They are intended for enterprise office environments of differing scales, from the corporate headquarters to remote branch sites, and therefore have been designed with ease of use in mind, making deployment and remote administration as easy as possible.

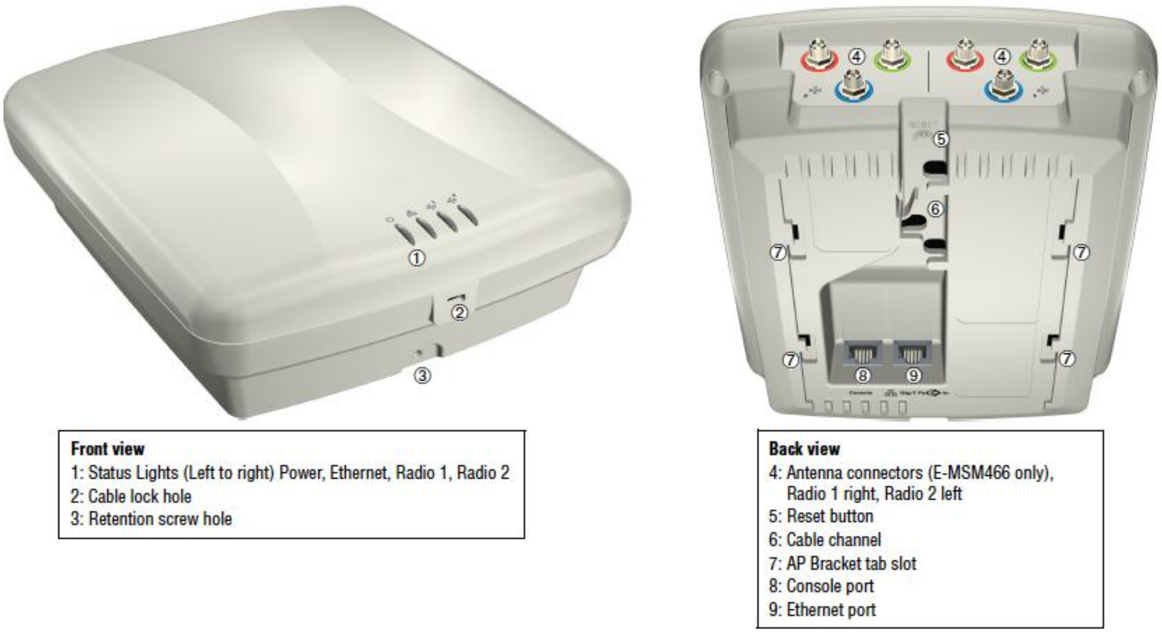
Supporting up to 255 concurrent sessions on each of its dual radios (100 stations in FIPS approved mode), the HP MSM4xx APs enable secure mobile access to IT resources within enterprise environments. They securely deliver enterprise networking without bounds, significantly increasing employee productivity in corporate offices, in decentralized/remote workgroups, and in branch locations with broadband access.

An access point may be referred to as the HP MSM4xx AP, the access point, the unit, or the cryptographic module throughout the document. When any of these designations are used, the statements made apply to any of the access points covered by this Security Policy.

2.1 ENCLOSURE AND CONNECTORS

Figure 1 shows the front of the HP MSM4xx APs with the four LEDs and the holes**. Figure 1** also shows the underside of the HP MSM466 with its antenna connectors, the reset button, and the console and Ethernet ports. The underside of the HP MSM430 and the HP MSM460 is the same as the underside of the HP MSM466 except they do not have any antenna connectors.

Figure 2 shows the underside of the HP MSM430/460 from the perspective of looking at the console port and Ethernet port. There are no antenna connectors as can be seen from the bottom of the photograph.



Front view
1: Status Lights (Left to right) Power, Ethernet, Radio 1, Radio 2
2: Cable lock hole
3: Retention screw hole

Back view
4: Antenna connectors (E-MSM466 only), Radio 1 right, Radio 2 left
5: Reset button
6: Cable channel
7: AP Bracket tab slot
8: Console port
9: Ethernet port

Figure 1 – HP MSM4xx APs

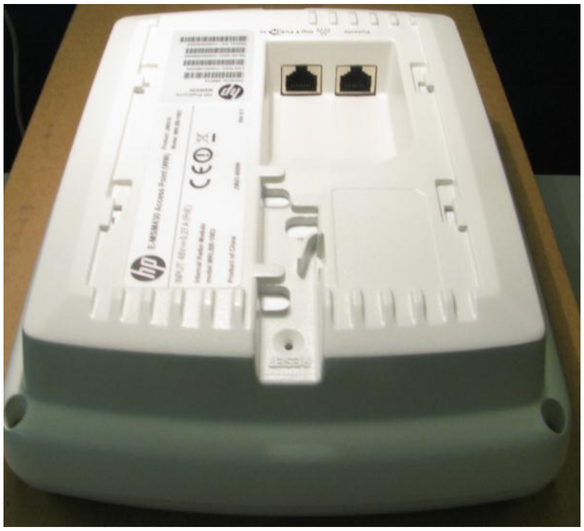


Figure 2 – Back View of the HP MSM430/460

2.2 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

Table 1 lists the interface types for the HP MSM4xx APs and maps each interface to the associated ports.

Interface	Type	Direction	Description	Related Hardware Port
Cryptographic Control	Control Input	To HP MSM4xx AP	A HP MSM765zl Mobility Controller allows the Administrator to control the operation of the cryptographic module.	Ethernet Port, Console Port

Cryptographic Status	Status Output	From HP MSM4xx AP	Success of the power-up self-tests is indicated by the first three LEDs blinking sequentially, the LED pattern that indicates the AP has received an IP address and is looking for a controller. A web browser interface for the managing HP MSM765zl Mobility Controller presents the current status of the cryptographic module to the Administrator.	LED Array, Ethernet Port, Console Port
Operational Control	Control Input	To HP MSM4xx AP	A web browser interface for the managing HP MSM765zl Mobility Controller allows the Administrator to control the operation of the access point or cryptographic module	Ethernet Port, Console Port
Operational Status	Status Output	From HP MSM4xx AP	Operational status is presented on the LED array. A web browser interface for the managing HP MSM765zl Mobility Controller provides the current status of the HP MSM4xx AP to the Administrator.	LED Array, Ethernet Port, Console Port
Input Data	Data Input	To HP MSM4xx AP	Users of the HP MSM4xx AP are allowed to send data to it over the Input Data interface.	Antennas, Ethernet Port
Output Data	Data Output	From HP MSM4xx AP	Users of the HP MSM4xx AP receive data from it over the Output Data Interface.	Antennas, Ethernet Port
Power	Power	To HP MSM4xx AP	Power over Ethernet	Ethernet Port

Table 1 – Cryptographic Module Ports and Interfaces

The console port does not need to be used when an HP MSM765zl Mobility Controller is being used to setup and manage the access point. By default, the console port is not activated.

2.3 TAMPER EVIDENT SEALS

This section describes where the tamper evident seals must be affixed to the HP MSM4xx APs for them to meet FIPS 140-2 Physical Security Level 2. The tamper evident seals are not affixed to an HP MSM4xx AP when it is delivered; they must be affixed by the Crypto-Officer before operating in the FIPS approved mode of operation.

Please note that a tamper evident seal is to be affixed over the reset button. The tamper evident seal shall not be affixed over the reset button until all functional steps to put the access point in the FIPS approved mode of operation are completed.

Three tamper evident seals are required for each HP MSM430, HP MSM460, or HP MSM466 access point.

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.) The seal must be affixed to one of the locations on the access point indicated in **Figure 3** 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 access point must not be placed into operation until the curing time has expired.

If additional seals are required, the HP part number is J9740A. The kit has 20 tamper evident seals. Extra seals must be stored in a secure location, with access available only to authorized Administrators.

Figure 3 illustrates where the tamper evident seals must be affixed on the HP MSM430, HP MSM460, and HP MSM466 Access Points. One seal should be affixed to each location indicated. These seals prevent the interior of the enclosure from being accessed without their being evidence of tampering.

Figure 4 shows the second seal affixed on an HP MSM430/460.

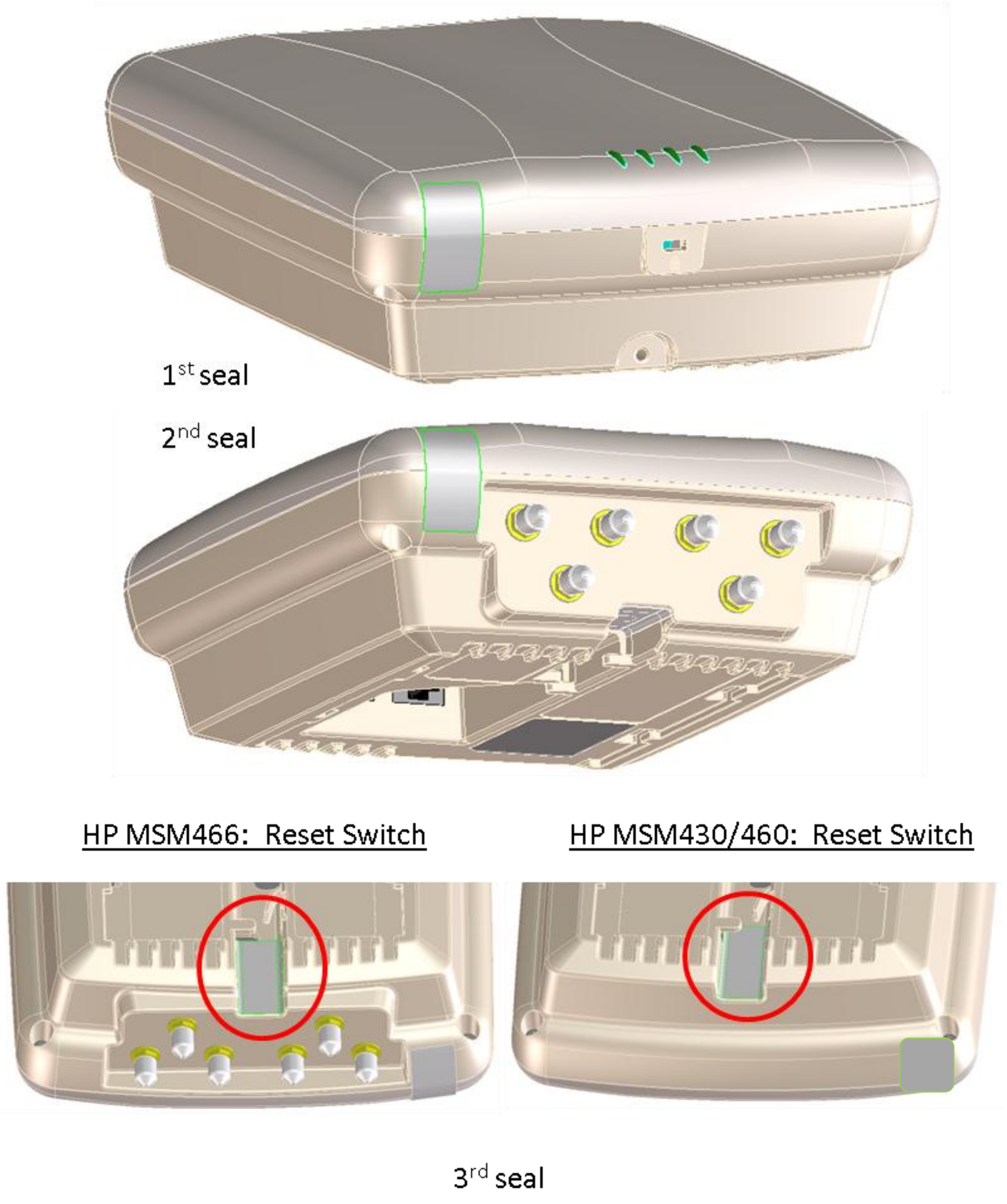


Figure 3 – Placement of Tamper Evident Seals on the HP MSM430, HP MSM460, and HP MSM466 Access Points

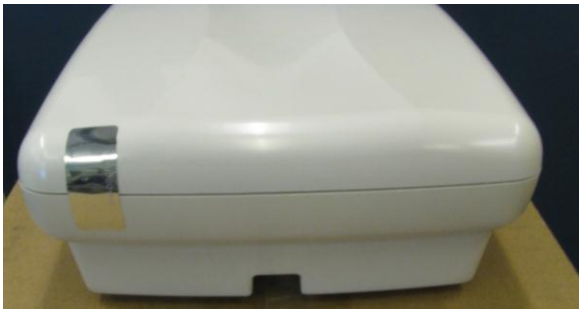


Figure 4 – Back of an HP MSM430/460 with the Tamper Evident Seal (Second Seal) Affixed

The tamper evident seals shall be installed for the module to operate in a FIPS approved mode of operation.

2.4 FEATURES

The HP MSM4xx AP provides:

a. WPA2-based encryption and authentication on the wireless networks;
b. Secure management from the HP MSM765zl Mobility Controller using TLS sessions; and
c. Efficient cryptography via the radio module processor and general-purpose dual-core processor.

2.5 HP MSM4XX AP CRYPTOGRAPHIC MODULE BOUNDARY

The HP MSM4xx AP cryptographic module boundary is the hard plastic enclosure surrounding the entire access point. The HP MSM4xx AP is a multiple-chip standalone cryptographic module.

The primary components of the HP MSM4xx AP providing cryptographic functionality are the main CPU, the radio module processor, the memory, and the LED array.

2.6 FIPS PUB 140-2 TARGETED SECURITY LEVELS

Table 2 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 2 – FIPS 140-2 Targeted Security Levels for Requirement Sections

3 PRODUCT OPERATION

3.1 OVERVIEW

HP MSM4xx Access Points are general-purpose wireless network devices whose operational mode is configurable through an administrative interface. Each access point can operate in one of two modes:

1. **Controlled mode**: The access point is centrally managed and configured via a HP MSM765zl Mobility Controller. Management and configuration of the access point is done entirely with the controller and not performed through a console directly connected to the access point. This is the factory-default mode.

2. **Autonomous mode**: The access point is a standalone device that is individually configured and managed.

Only the Controlled mode of operation is to be covered by the FIPS 140-2 validation. The Autonomous mode of operation is not covered.

To configure the access point in the FIPS approved mode of operation, refer to section **3.2**.

The *MSM430, MSM460, and MSM466 802.11n Access Points Quickstart* and the *HP MSM3xx / MSM4xx Access Points Management and Configuration Guide* can be consulted for a complete discussion of each model's operation.

3.2 FIPS APPROVED MODE OF OPERATION: CONTROLLED MODE

The FIPS approved mode of operation is a special configuration of the HP MSM4xx AP in which the FIPS validated version of the firmware is loaded on the unit, the unit is configured to operate in the FIPS 140-2 mode; and the wireless LAN is configured to use WPA2 or no encryption.

The following steps to configure the access point in the FIPS approved mode of operation assume the following:

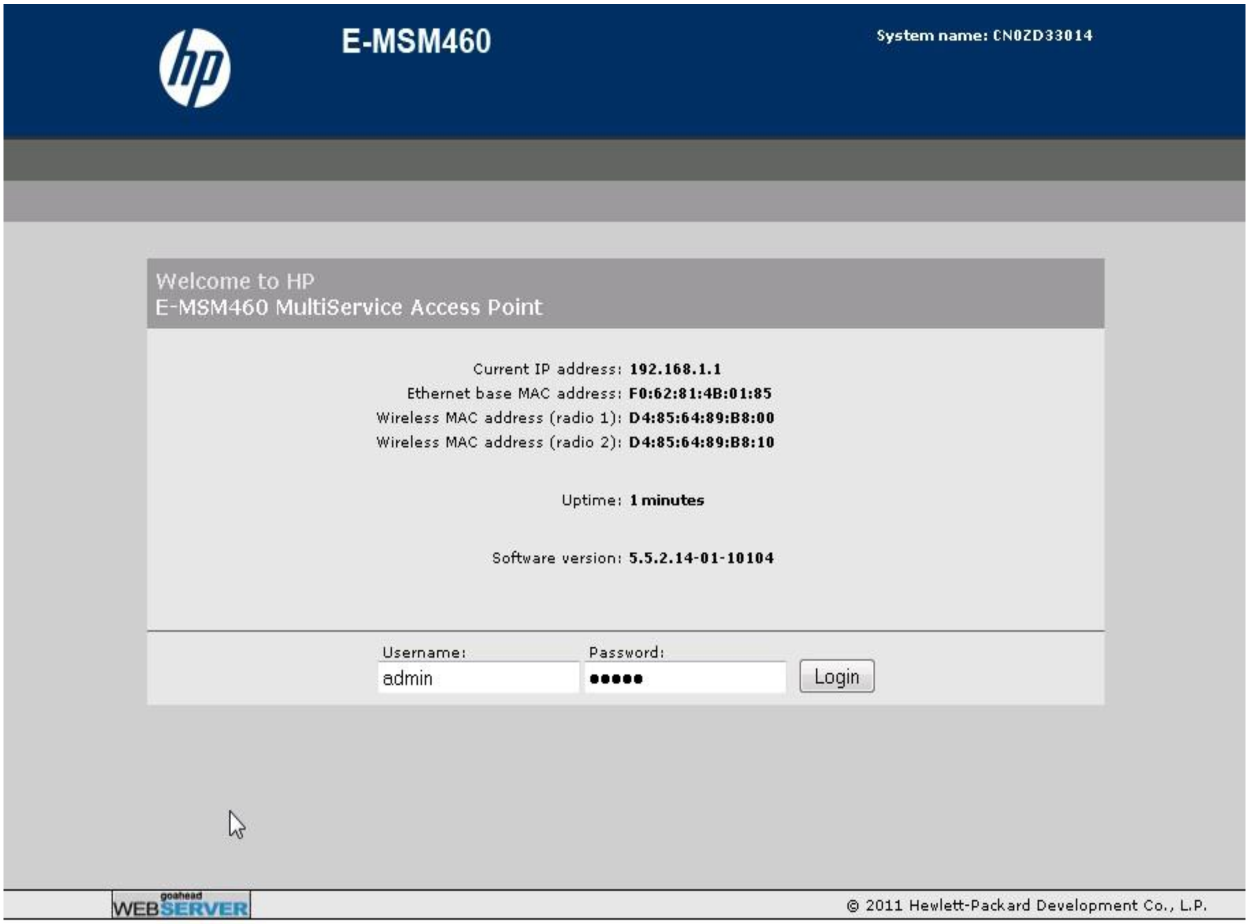
- The administrator has received an access point with an installed firmware version that is not FIPS 140-2 validated. This is likely because the FIPS 140-2 validated version of the firmware will be available on the Hewlett-Packard website.
- The access point is in controlled mode.
- The unit has never been synchronized to a controller. If it was once connected to a controller, the web interface will be completely shut down. The only way to bring back up the provisioning interface would be to use the reset button.
- The access point is on a network where no controller can be discovered through the UDP broadcast or DHCP option mechanism, nor by resolving the cnsrv1/cnsrv2/cnsrv3 predefined DNS host names.

STEP 1: LOAD THE FIPS VALIDATED FIRMWARE ON THE ACCESS POINT

A. Using a tool such as a paper clip, press and hold the reset button on the access point for a few seconds until the front status LEDs blink three times to zeroize any CSPs in the access point.

B. Using a web browser go to the default address of the access point or, if DHCP server is present on the network, find out what IP address it has assigned to the access point. The rest of this document assumes that the AP can be reached at its default address of 192.168.1.1

C. Login using the default username/password = admin/"admin".



E-MSM460

System name: CN0ZD33014

Welcome to HP
E-MSM460 MultiService Access Point

Current IP address: 192.168.1.1
Ethernet base MAC address: F0:62:81:4B:01:85
Wireless MAC address (radio 1): D4:85:64:89:B8:00
Wireless MAC address (radio 2): D4:85:64:89:B8:10

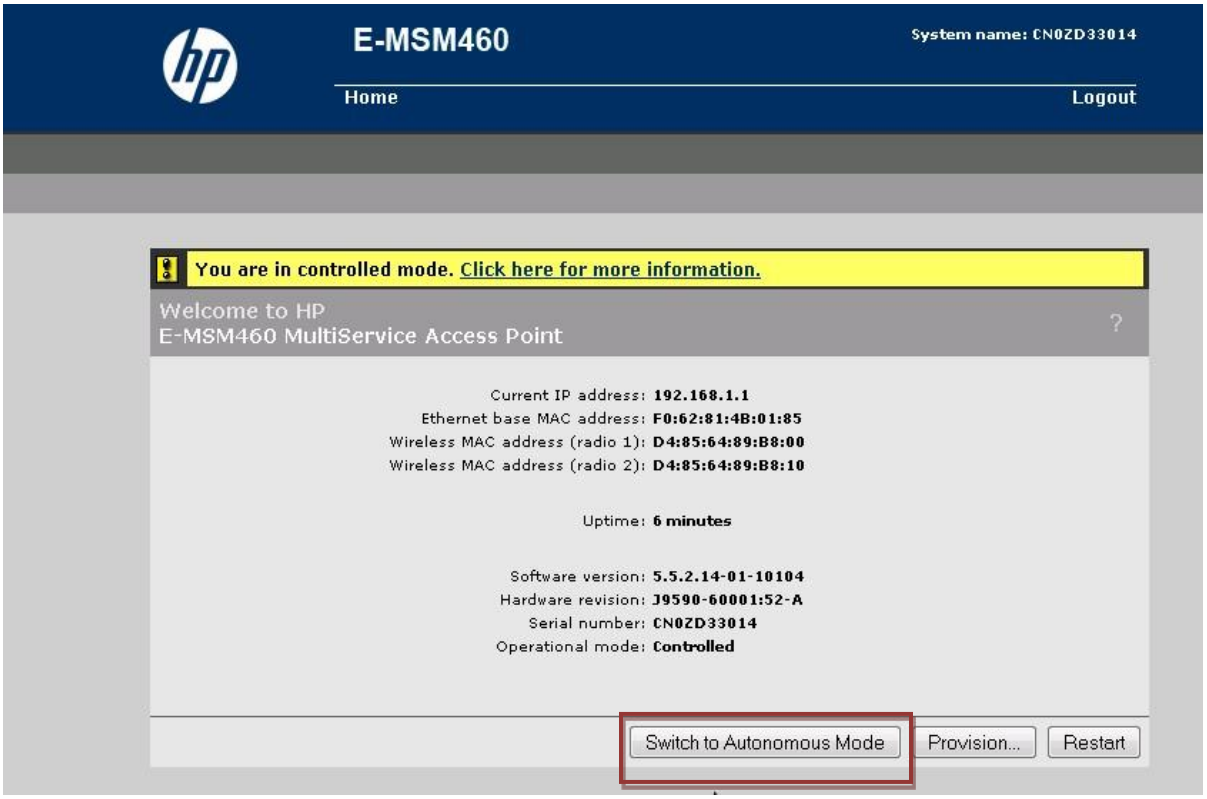
Uptime: 1 minutes

Software version: 5.5.2.14-01-10104

Username: admin
Password: ●●●●●

© 2011 Hewlett-Packard Development Co., L.P.

D. Click on the “Switch to Autonomous Mode” button in order to load the FIPS validated firmware.



You are in controlled mode. Click here for more information.

Welcome to HP
E-MSM460 MultiService Access Point

Current IP address: **192.168.1.1**
Ethernet base MAC address: **F0:62:81:4B:01:85**
Wireless MAC address (radio 1): **D4:85:64:89:B8:00**
Wireless MAC address (radio 2): **D4:85:64:89:B8:10**

Uptime: **6 minutes**

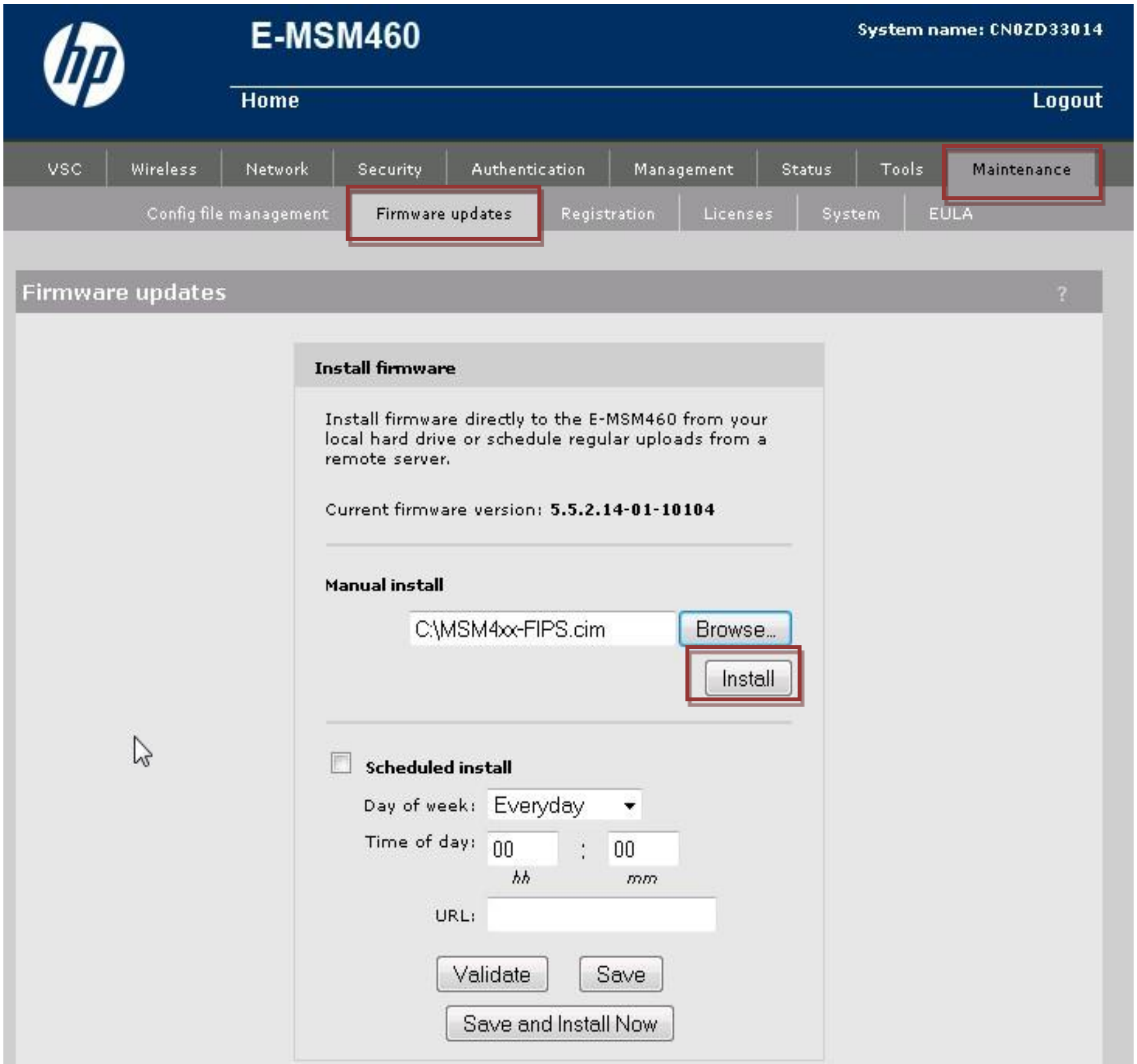
Software version: **5.5.2.14-01-10104**
Hardware revision: **J9590-60001:52-A**
Serial number: **CN0ZD33014**
Operational mode: **Controlled**

E. Click the “OK” button when prompted.

F. Login again with admin/admin when the home page comes back. Also, accept the license and save the appropriate country when prompted.

Saving the country is the last required step. The next steps of the startup wizard are optional; they can be skipped by clicking on the home link.

G. Select the “Maintenance” tab and then the “Firmware updates” tab. Select the FIPS validated firmware from the filesystem and click on the “Install” button.



System name: CN0ZD33014

Install firmware directly to the E-MSM460 from your local hard drive or schedule regular uploads from a remote server.

Current firmware version: 5.5.2.14-01-10104

C:\MSM4xx-FIPS.cim

□ Scheduled install

Day of week: Everyday

Time of day: 00 : 00

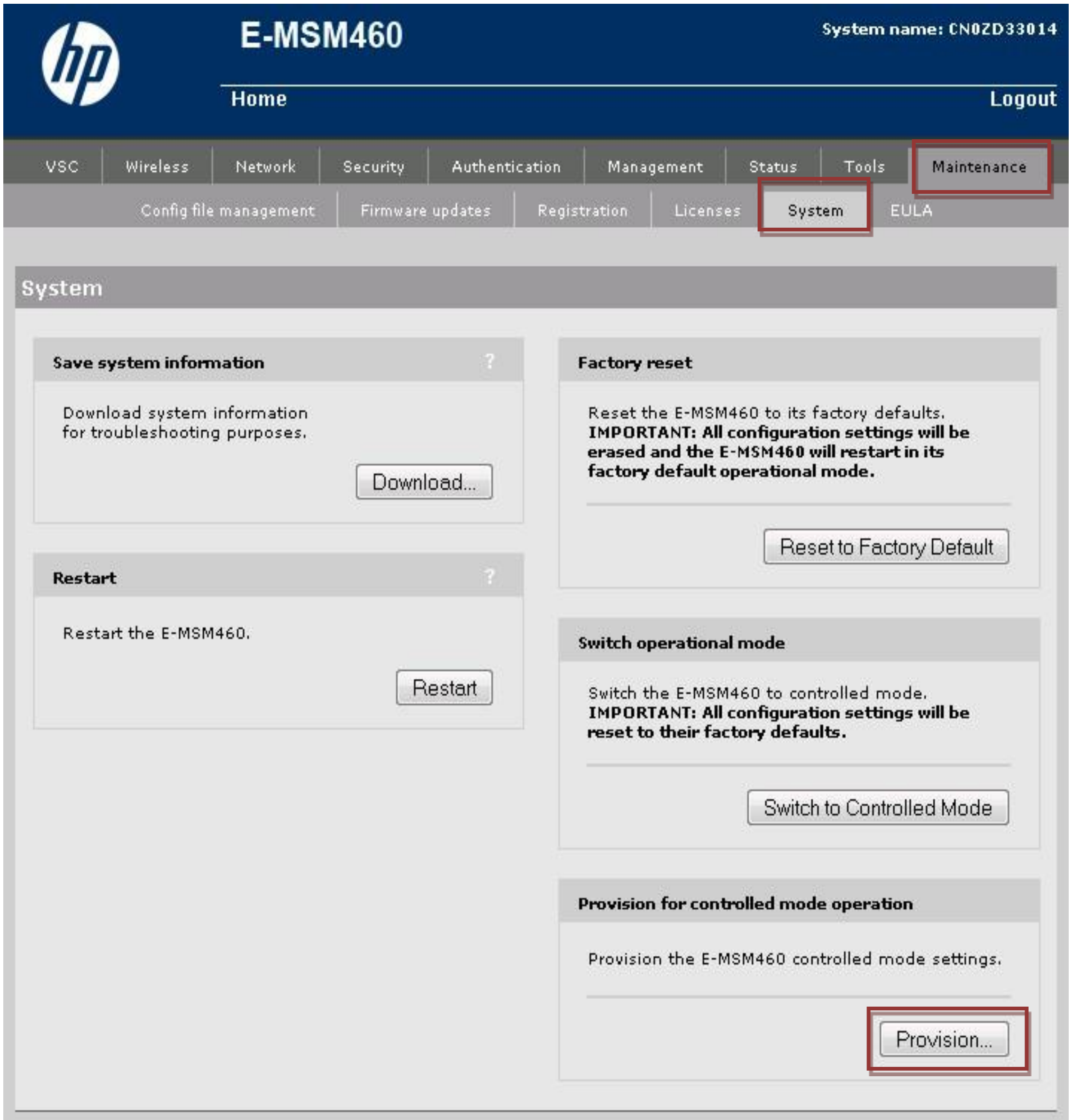
At this point, the correct firmware is loaded on the access point. In the further steps, the access point is switched to controlled mode and the firmware updates from the controller are disabled.

STEP 2: PROVISIONING FROM THE AUTONOMOUS MODE

A. The unit will reboot and go back to the home page. You can verify that you have the FIPS validated version of the firmware as it is displayed as the “Software version” on this web page. Please note that the version identification shown in the screenshot is not the FIPS validated version of the firmware. Login again with the admin/admin credentials.

   Note that you may need to click the refresh button of the browser since the FIPS validated version of the new firmware has a new web server certificate. Because of the new web server certificate, the automatic reload of the home page to fail following the firmware upgrade.

B. Click on the “Maintenance” tab, then the “System” tab, and then click on the “Provision” button.



System

Save system information

Download system information for troubleshooting purposes.

Factory reset

Reset the E-MSM460 to its factory defaults. **IMPORTANT: All configuration settings will be erased and the E-MSM460 will restart in its factory default operational mode.**

Restart

Restart the E-MSM460.

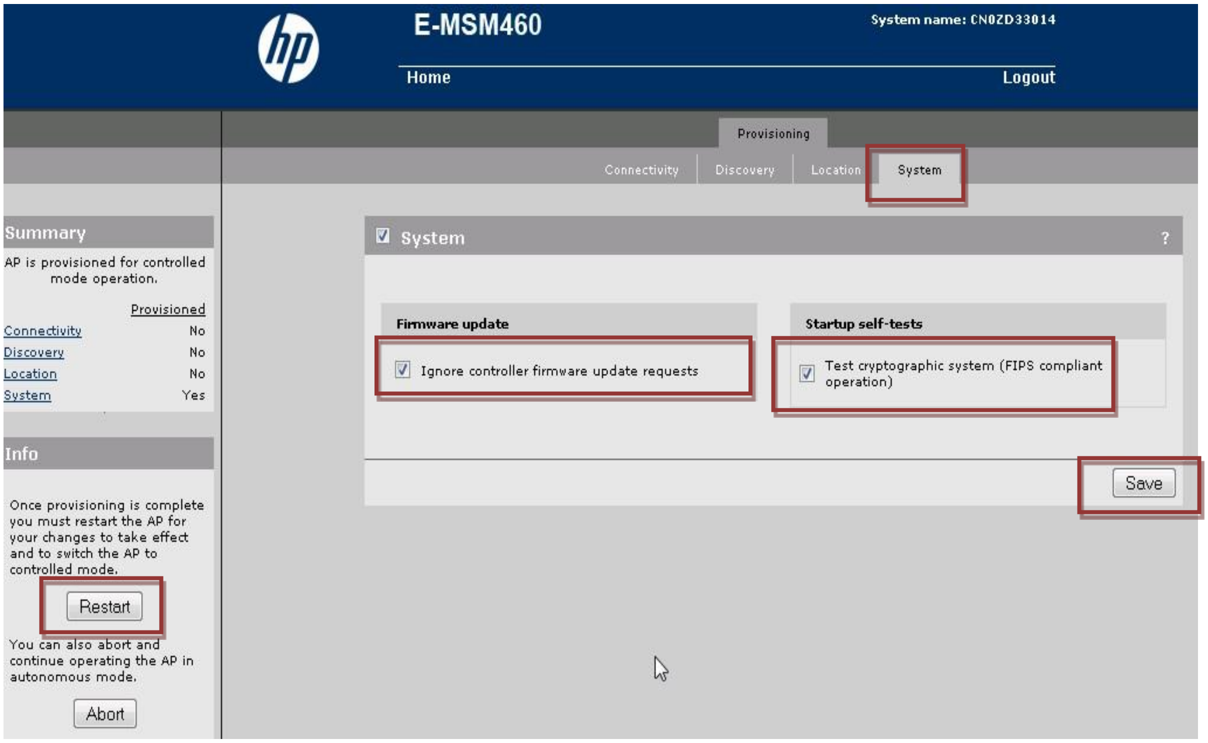
Switch operational mode

Switch the E-MSM460 to controlled mode. **IMPORTANT: All configuration settings will be reset to their factory defaults.**

Provision for controlled mode operation

Provision the E-MSM460 controlled mode settings.

C. Click on the “System” tab again. Select the “Ignore controller firmware update requests” and the “Test cryptographic system (FIPS compliant operation)” check boxes, and then click the “Save” button. Finally click on the “Restart” button on the left, which will reboot the device.



Summary

AP is provisioned for controlled mode operation.

	Provisioned
Connectivity	No
Discovery	No
Location	No
System	Yes

Info

Once provisioning is complete you must restart the AP for your changes to take effect and to switch the AP to controlled mode.

You can also abort and continue operating the AP in autonomous mode.

☑ System

Firmware update

☑ Ignore controller firmware update requests

Startup self-tests

☑ Test cryptographic system (FIPS compliant operation)

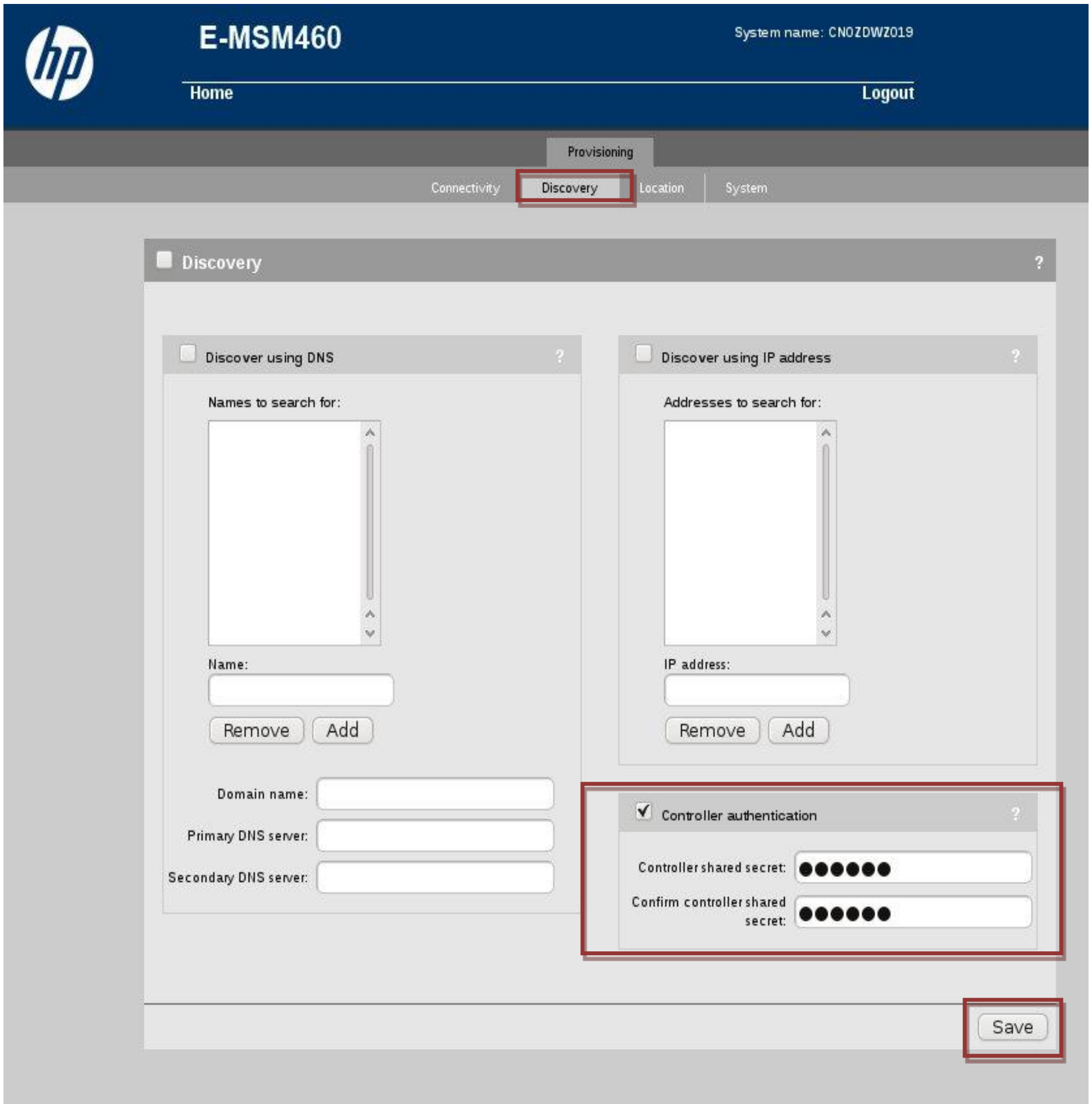
After the reboot:

- The access point will switch from autonomous mode to controlled mode.
- The power-up self-tests will run.
- Firmware updates from the controller will be rejected.
- Only FIPS approved ciphersuites will be negotiated for the web server TLS.

STEP 3: PROVISIONING FROM THE CONTROLLED MODE

A. When the home page comes back, login with username admin and password "admin", and click on the "Provision" button.

B. Click on the "Discovery" tab. Select the "Controller authentication" box and enter the shared secret that will be used to authenticate the controller, and then save. You may also at this point provision any other settings that are necessary in your particular network (see admin and deployment guides for the access points).

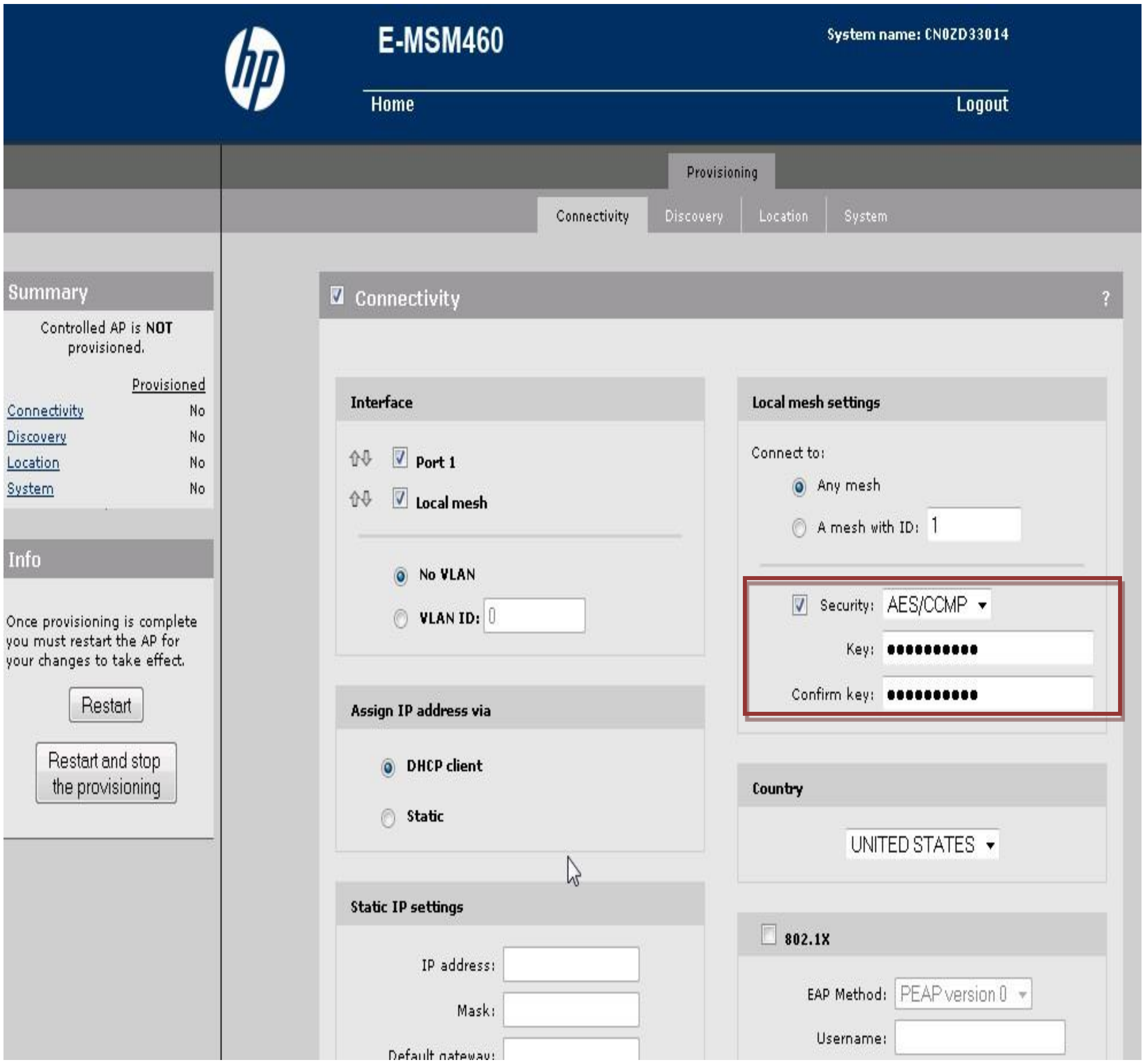


☑ Controller authentication

Controller shared secret: ●●●●●●

Confirm controller shared secret: ●●●●●●

C. If you provision an optional Local Mesh link, you must select "Security" and select "AES/CCMP" encryption and then input a FIPS-compliant AES/CCMP secret key.



System name: CN0ZD33014

Controlled AP is **NOT** provisioned.

	Provisioned
Connectivity	No
Discovery	No
Location	No
System	No

Once provisioning is complete you must restart the AP for your changes to take effect.

☑ Connectivity

Interface

- ☑ Port 1
- ☑ Local mesh
- ● No VLAN
- ○ VLAN ID: 0

Assign IP address via

- ● DHCP client
- ○ Static

Static IP settings

IP address:

Mask:

Default gateway:

Local mesh settings

Connect to:

- ● Any mesh
- ○ A mesh with ID: 1

☑ Security: AES/CCMP

Key: ●●●●●●●●●●●

Confirm key: ●●●●●●●●●●●

Country: UNITED STATES

☐ 802.1X

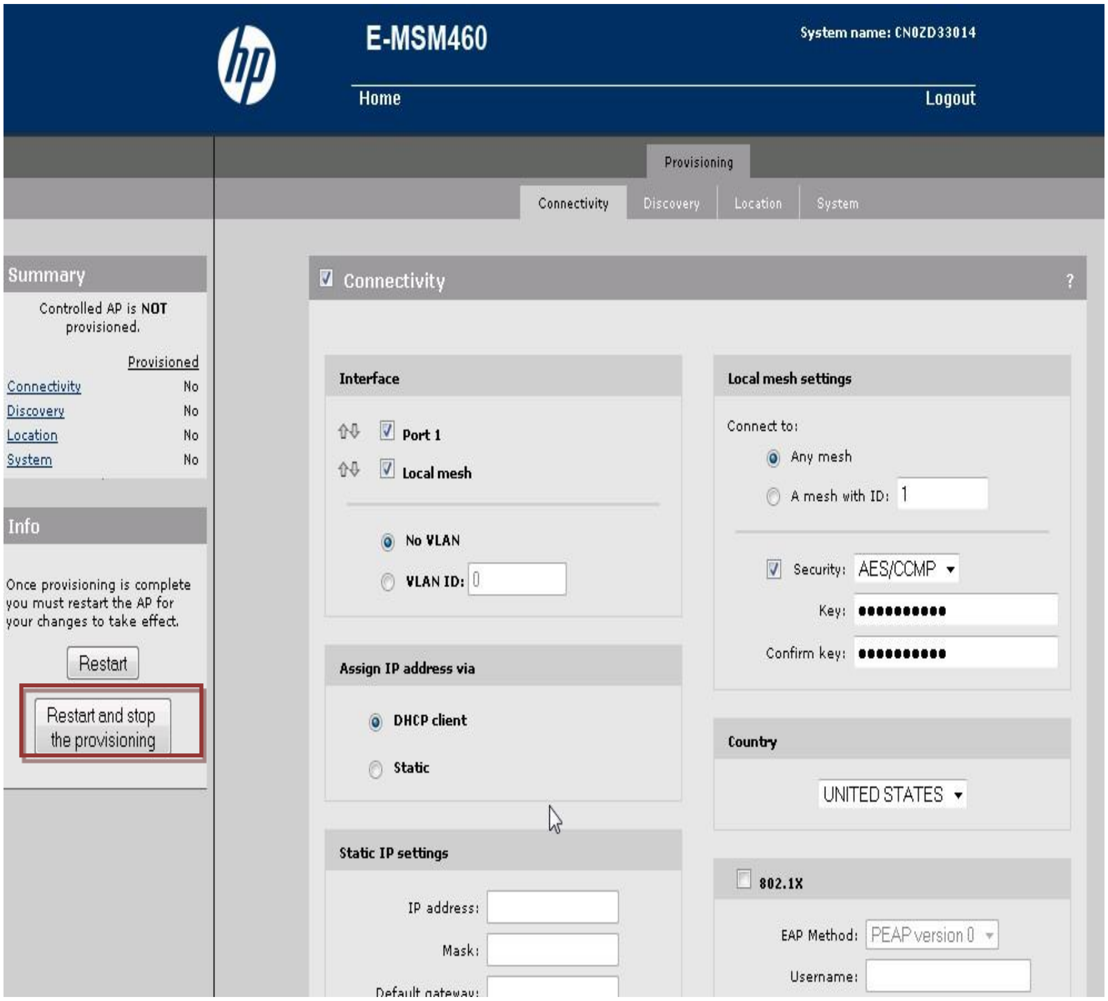
EAP Method: PEAP version 0

Username:

D. Click on the “Restart and stop the provisioning” button. This will reboot the access point and close down the provisioning interface. The access point can then be plugged in its final place of operation, where it will discover a controller and start offering services according to the configuration that the controller will send. Configuration of the access point that must be done is specified in section **3.3**.

The tamper evident seals must be affixed at the specified three locations before putting the access point into operation before running in the FIPS approved mode of operation.

Note that after this step, the only way to manage the device is through a controller. A tamper evident seal covers the hardware reset button when prepared for FIPS approved operation.



System name: CN0ZD33014

Controlled AP is **NOT** provisioned.

	Provisioned
Connectivity	No
Discovery	No
Location	No
System	No

Once provisioning is complete you must restart the AP for your changes to take effect.

☑ Connectivity

☑ Port 1
☑ Local mesh

● No VLAN
○ VLAN ID: 0

● DHCP client
○ Static

IP address:
Mask:
Default gateway:

Connect to:
● Any mesh
○ A mesh with ID: 1

☑ Security: AES/CCMP
Key: ●●●●●●●●●●
Confirm key: ●●●●●●●●●●

UNITED STATES

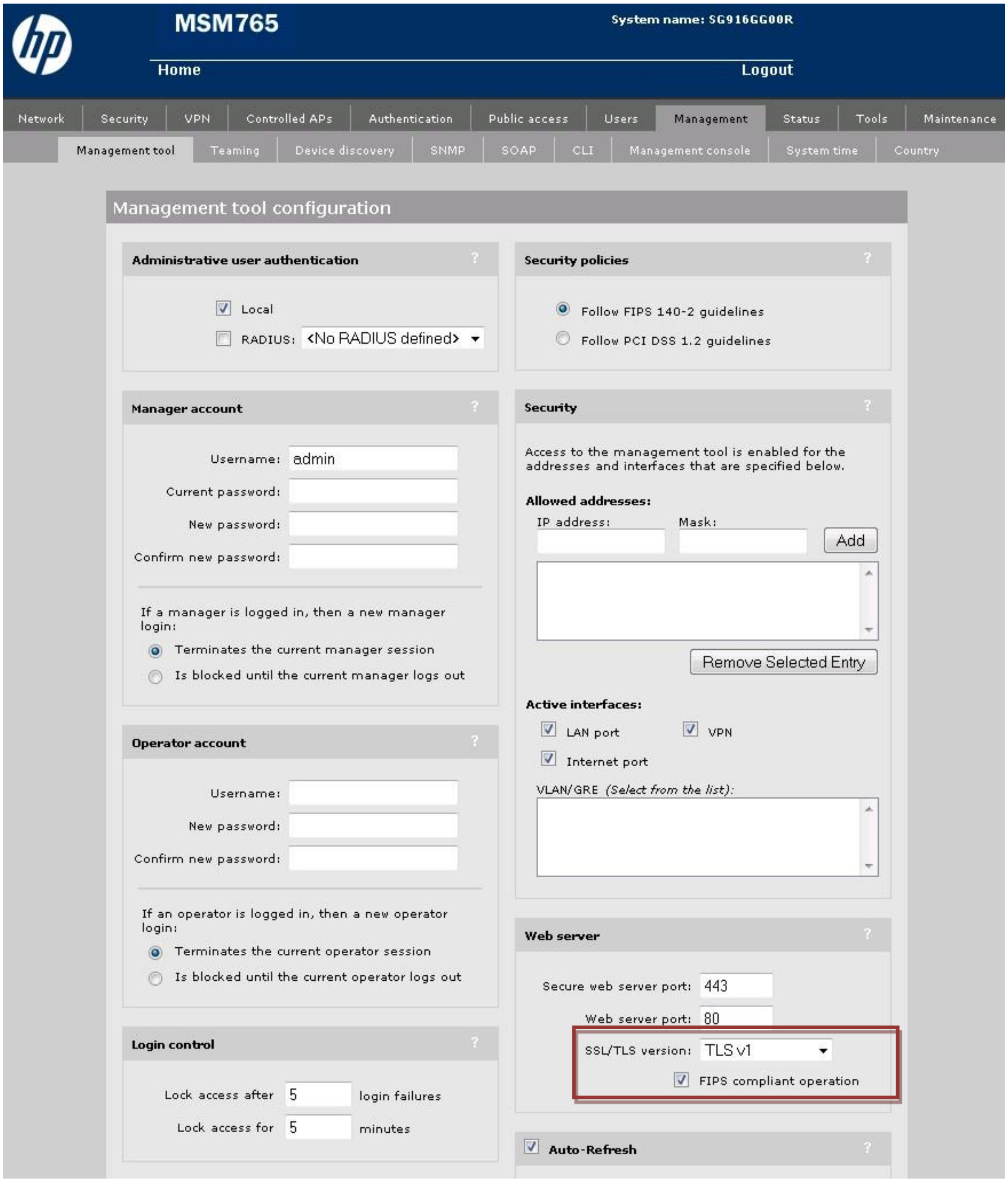
☐ 802.1X
EAP Method: PEAP version 0
Username:

3.3 FIPS APPROVED MODE OF OPERATION: CONFIGURATION TO BE DONE WITH THE HP MSM765ZL MOBILITY CONTROLLER

The following steps must be done through the HP MSM765zl Mobility Controller managing the access point to run the access point in the FIPS approved mode of operation.

STEP 1: SETTING TLSV1 FOR THE MANAGEMENT LINK FROM THE MOBILITY CONTROLLER

A. Select the "Management" tab and then select the "Management tool" tab. Select "TLSv1" from the drop-down list and select "FIPS compliant operation". Click on the "Save" button at the bottom of the page.



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: admin

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

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)*:

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

Web server

Secure web server port: 443

Web server port: 80

SSL/TLS version: TLS v1

☑ FIPS compliant operation

Login control

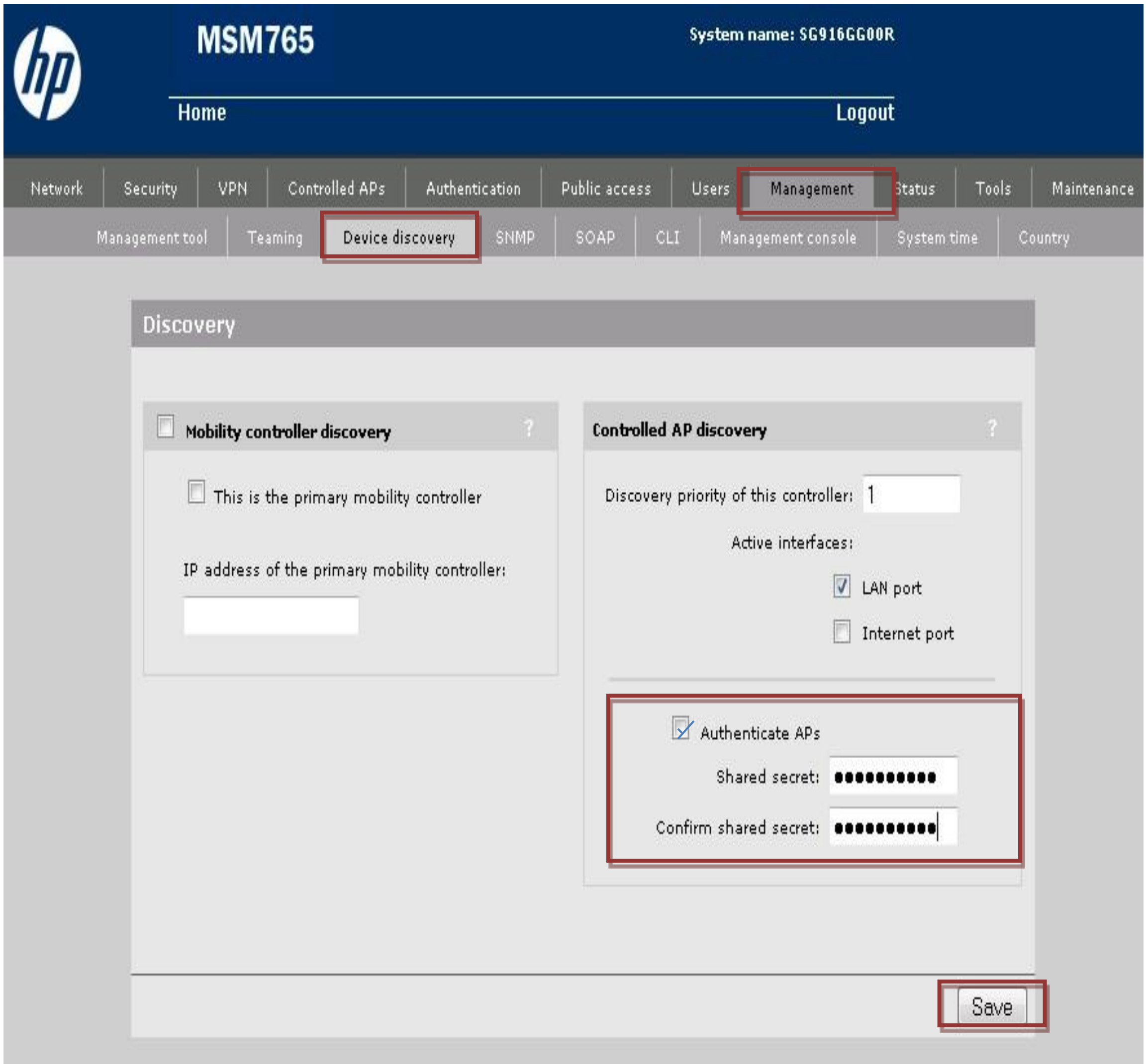
Lock access after 5 login failures

Lock access for 5 minutes

☑ **Auto-Refresh**

STEP 2: ENTER THE SHARED SECRET FOR THE ACCESS POINTS TO BE CONTROLLED

A. Select the “Management” tab and then the “Device discovery” tab. Enter the same shared secret that was entered in B for STEP 3: PROVISIONING FROM THE CONTROLLED MODE. Click the “Save” button.



□ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of this controller: 1

Active interfaces:

☑ LAN port

□ Internet port

☑ Authenticate APs

Shared secret: ●●●●●●●●●●

Confirm shared secret: ●●●●●●●●●●●

Note that “Authenticate APs” must be selected for the HP MSM765zl Mobility Controller to operate in the FIPS approved mode of operation.

STEP 3: SPECIFY THE WIRELESS SECURITY FOR THE ACCESS POINT

What encryption and authentication is offered on each wireless network is determined by the HP MSM765zl Mobility Controller.

The FIPS compliant configurations for a Virtual Service Community (VSC) that can be applied to an access point to operate in the FIPS approved mode of operation are the following:

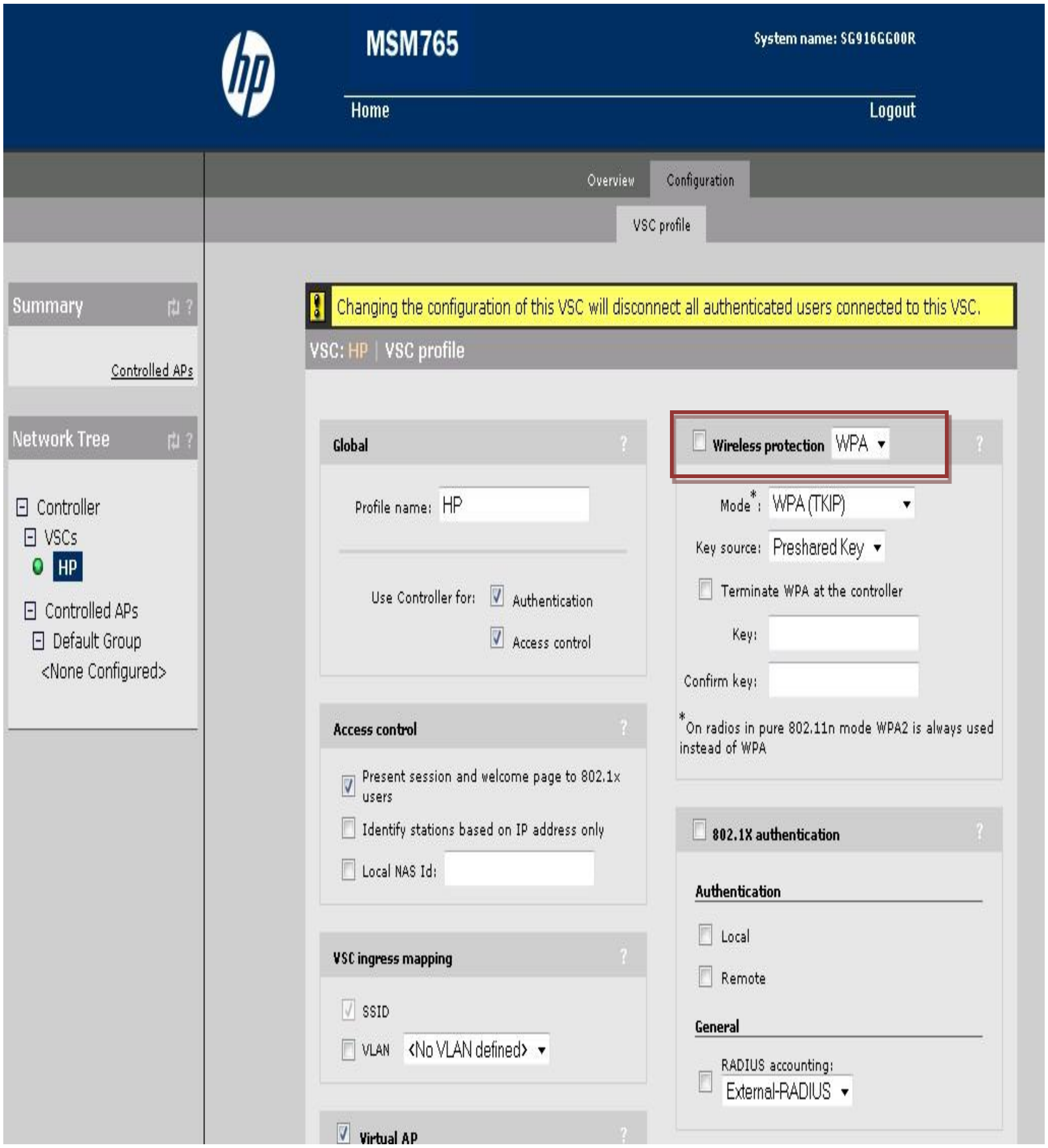
- No security or authentication (open wireless network or bypass);
- WPA2 + preshared key;
- WPA2 + dynamic key, with EAP terminated at the controller; or
- WPA2 + dynamic key, with EAP terminated at an external Active Directory or RADIUS server[1].

The following pages illustrate how to configure each type of wireless network.

[1] The link between the controller and the external Active Directory or RADIUS server must be secured by IPSec.

- Open wireless network

Uncheck the “Wireless protection” checkbox and click on the “Save” button at the bottom of the page.



Changing the configuration of this VSC will disconnect all authenticated users connected to this VSC.

VSC: HP | VSC profile

Global

Profile name: HP

Use Controller for: ☑ Authentication

☑ 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**

□ **Wireless protection** WPA

Mode*: WPA (TKIP)

Key source: Preshared Key

□ Terminate WPA at the controller

Key:

Confirm key:

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

□ **802.1X authentication**

Authentication

□ Local

□ Remote

General

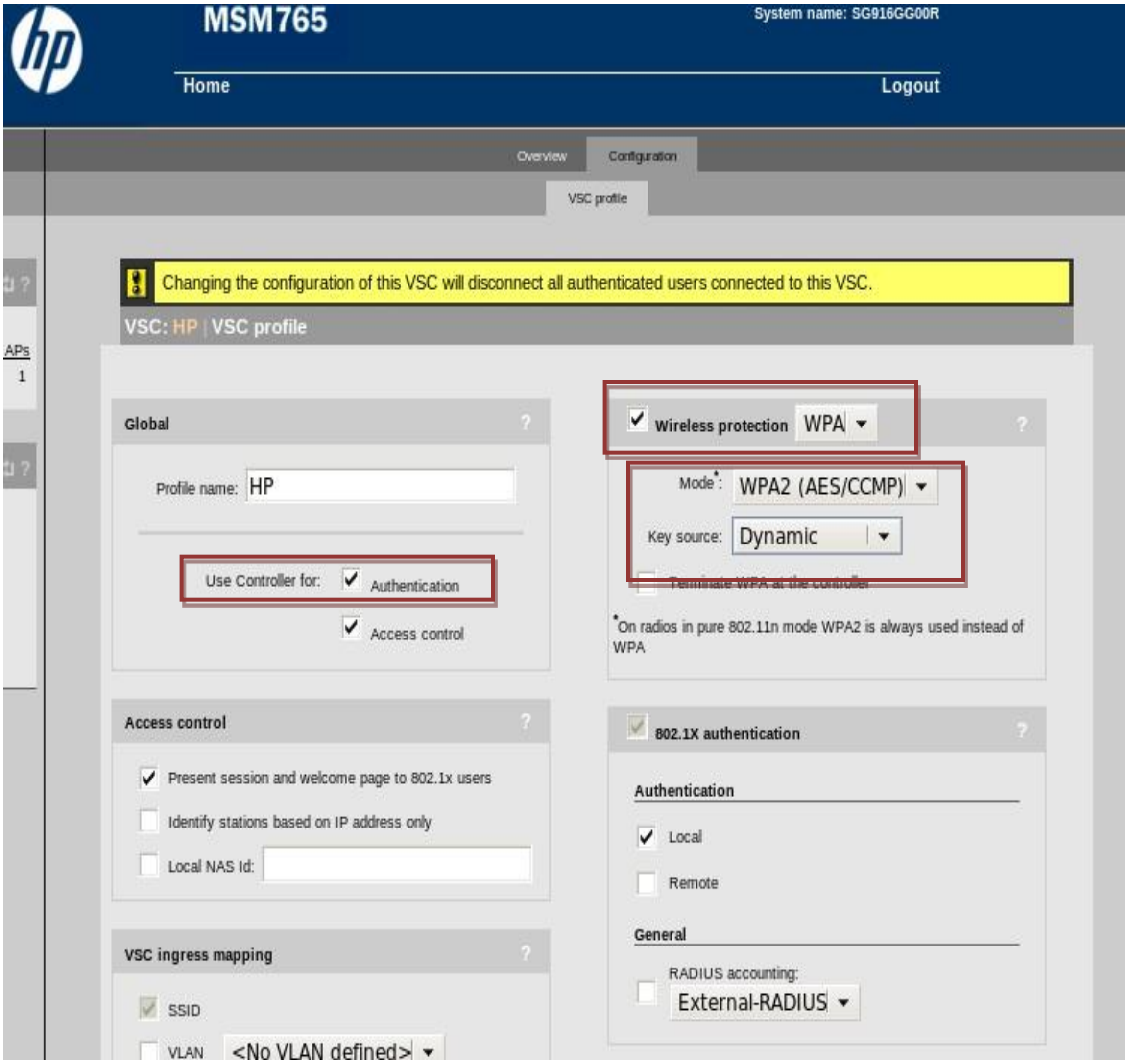
□ RADIUS accounting: External-RADIUS

- WPA2 PSK

  Select the “Wireless protection” checkbox. Select “WPA2 (AES/CCMP)” as the “Mode:” and “Preshared Key” as the “Key source:”. Enter the Preshared Key. Click on the “Save” button at the bottom of the page.

- WPA2 with dynamic keys

  Select the “Authentication” checkbox for “Use Controller for:”. Select the “Wireless protection” checkbox. Select “WPA2 (AES/CCMP)” as the “Mode:” and “Dynamic” as the “Key source:”. Click on the “Save” button at the bottom of the page.



Changing the configuration of this VSC will disconnect all authenticated users connected to this VSC.

VSC: HP | VSC profile

Global

Profile name: HP

Use Controller for: ☑ Authentication

☑ Access control

☑ Wireless protection WPA

Mode*: WPA2 (AES/CCMP)

Key source: Dynamic

□ Terminate WPA at the controller

*On radios in pure 802.11n mode WPA2 is always used instead of WPA

Access control

☑ Present session and welcome page to 802.1x users

□ Identify stations based on IP address only

□ Local NAS Id:

☑ 802.1X authentication

Authentication

☑ Local

□ Remote

General

□ RADIUS accounting: External-RADIUS

VSC ingress mapping

☑ SSID

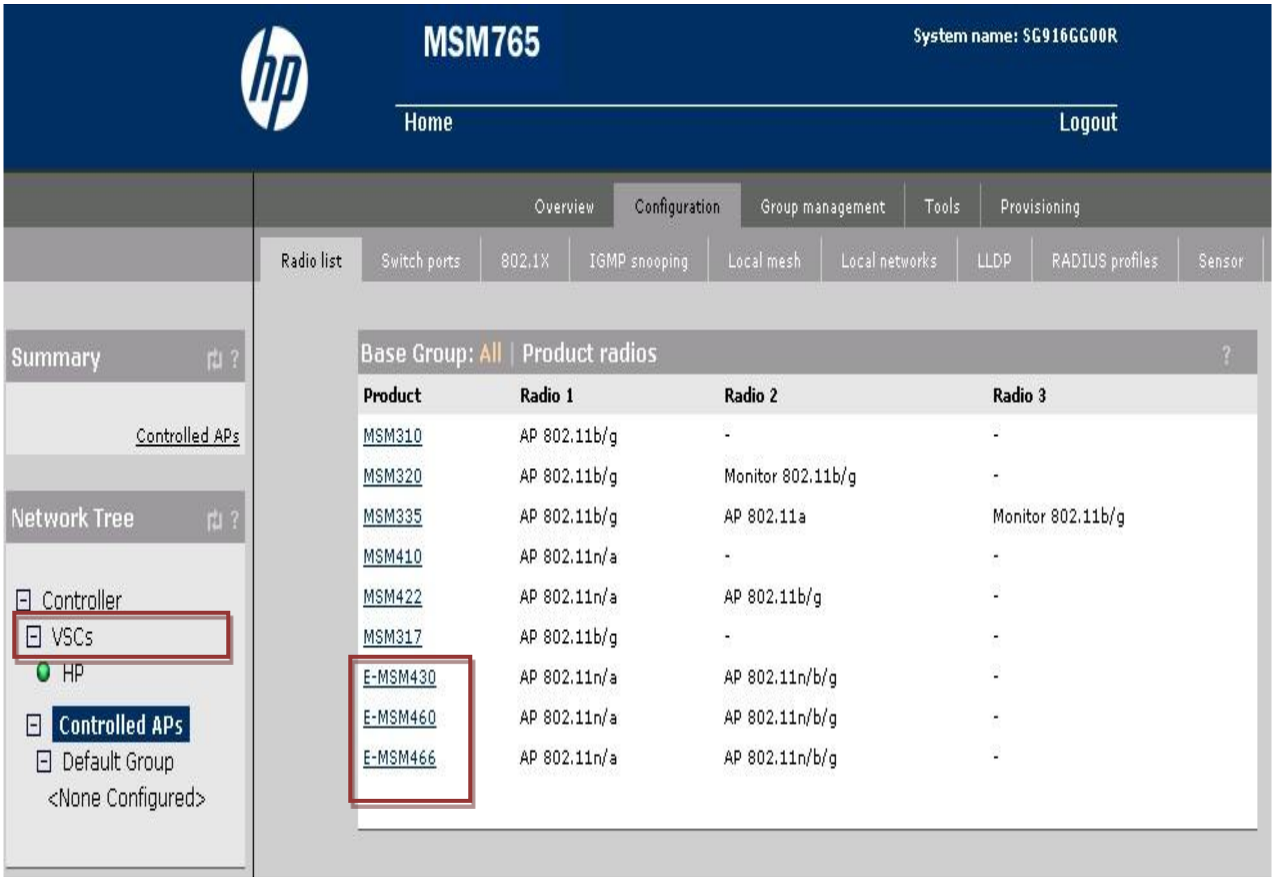
□ VLAN <No VLAN defined>

The controller must be used for Authentication. Otherwise, the access point will communicate directly with the external RADIUS server to perform the EAP rather than using the controller as a termination or proxy of the EAP.

STEP 4: SET THE REQUIRED RESTRICTIONS

- Restrict the number of simultaneous wireless clients to 100 per access point.

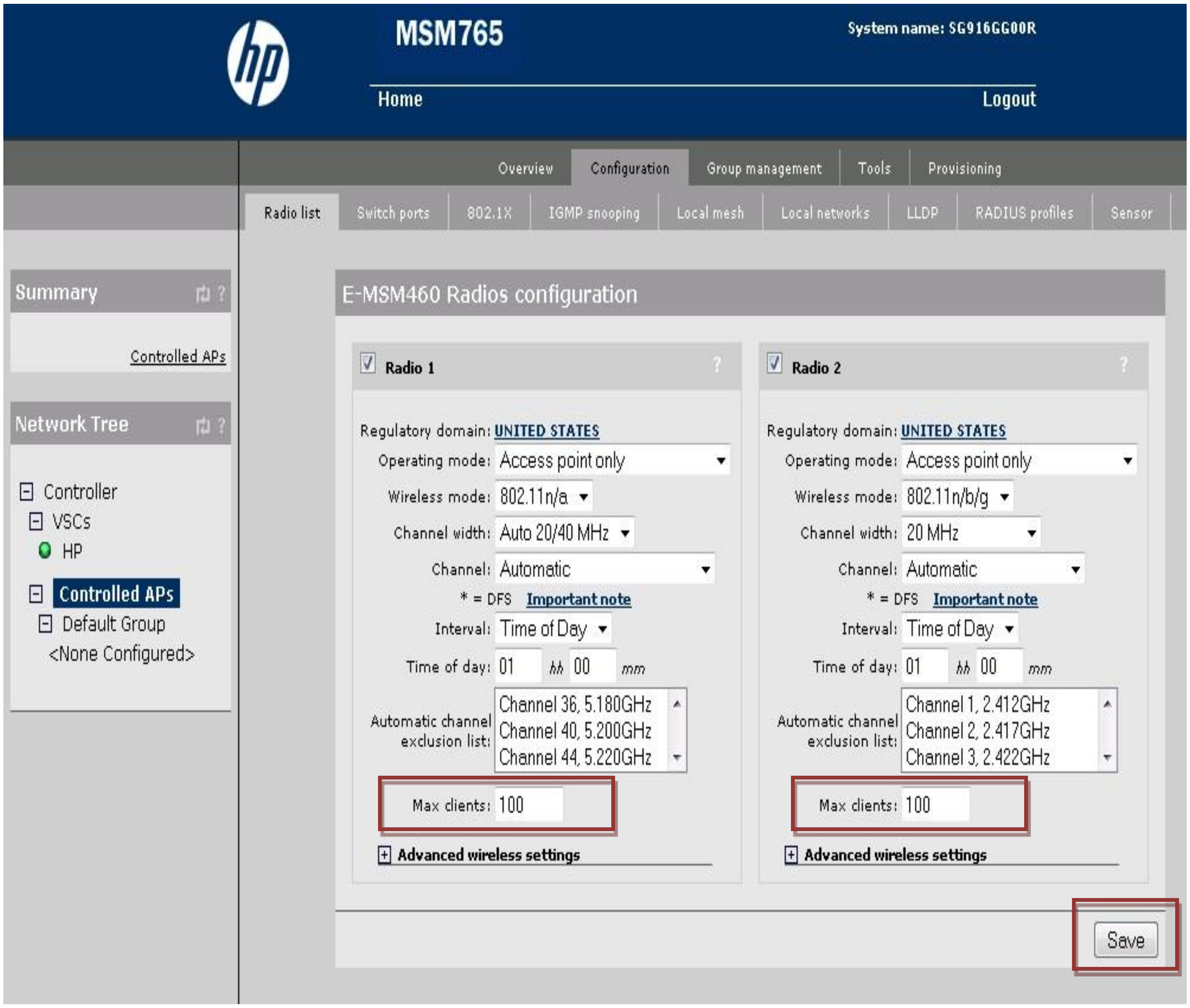
Select the "Controlled APs" link in the left column and then select the link for the particular access point.



Base Group: All | Product radios

Product	Radio 1	Radio 2	Radio 3
MSM310	AP 802.11b/g	-	-
MSM320	AP 802.11b/g	Monitor 802.11b/g	-
MSM335	AP 802.11b/g	AP 802.11a	Monitor 802.11b/g
MSM410	AP 802.11n/a	-	-
MSM422	AP 802.11n/a	AP 802.11b/g	-
MSM317	AP 802.11b/g	-	-
E-MSM430	AP 802.11n/a	AP 802.11n/b/g	-
E-MSM460	AP 802.11n/a	AP 802.11n/b/g	-
E-MSM466	AP 802.11n/a	AP 802.11n/b/g	-

In the “Radios configuration” page, set the “Max clients:” to 100 for both radios. Click the “Save” button.



E-MSM460 Radios configuration

☑ Radio 1

Regulatory domain: UNITED STATES
Operating mode: Access point only
Wireless mode: 802.11n/a
Channel width: Auto 20/40 MHz
Channel: Automatic
* = DFS
Interval: Time of Day
Time of day: 01 hh 00 mm
Automatic channel exclusion list: Channel 36, 5.180GHz
Channel 40, 5.200GHz
Channel 44, 5.220GHz
Max clients: 100

☑ Radio 2

Regulatory domain: UNITED STATES
Operating mode: Access point only
Wireless mode: 802.11n/b/g
Channel width: 20 MHz
Channel: Automatic
* = DFS
Interval: Time of Day
Time of day: 01 hh 00 mm
Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz
Max clients: 100

The maximum clients must be set to 100 or less so that the radio chip will be used for AES CCMP.

Note that the Administrator must ensure that the setting of the maximum clients is not changed in the group or access point lower level web pages.

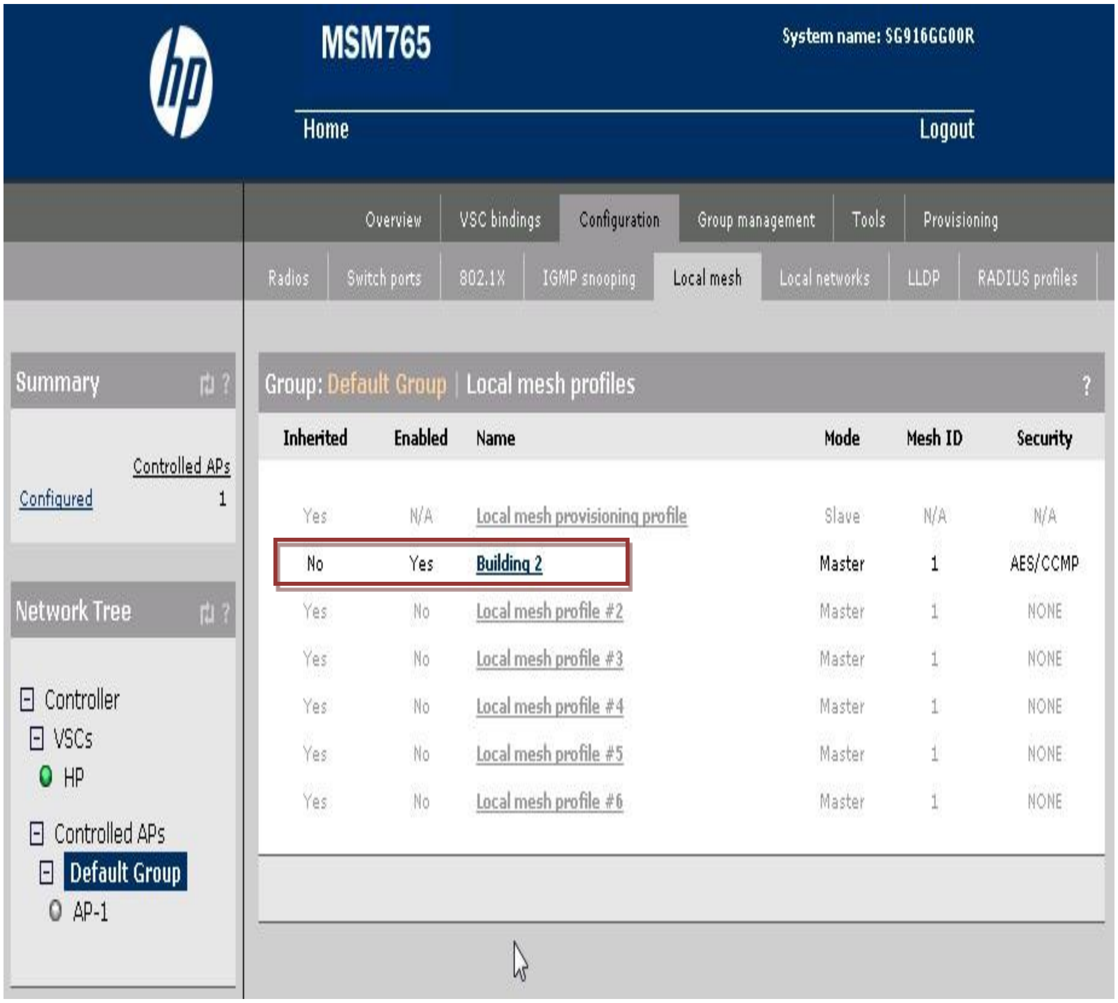
- Use only one local mesh profile for the access point.

  The reason for enforcing this is that the local mesh profiles use hardware encryption resources. This is why they are limited to only one per access point.

  If an access point has been provisioned with a local mesh link, then no additional local mesh networks must be added to the access point. If the access point has not been provisioned with a local mesh link, then only one local mesh link can be added on the access point.

  Local meshes can be defined at all three levels in the hierarchy “Controlled APs/AP group/Specific AP”. **Note that no more than one local mesh link must be provisioned for an access point so operators must be careful not to provision another local mesh link for an access point at another level of the hierarchy of the web management tool if a local mesh link has already been provisioned for the access point.**

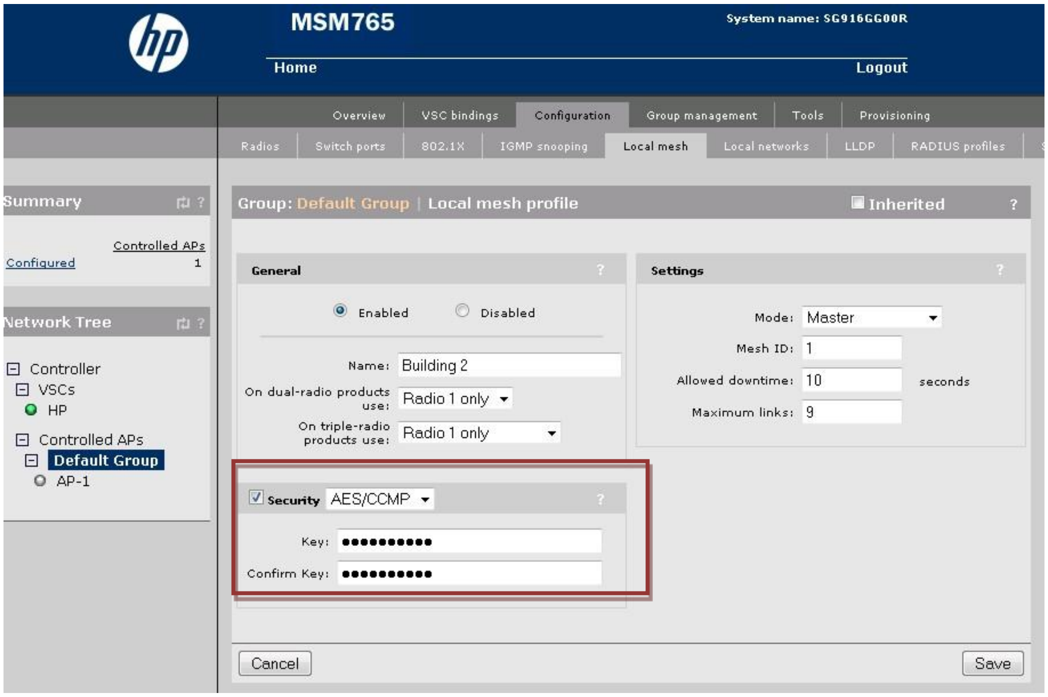
  In this example one local mesh has been enabled for all the access points that belong to the group “Default Group”.



Group: Default Group | Local mesh profiles

Inherited	Enabled	Name	Mode	Mesh ID	Security
Yes	N/A	Local mesh provisioning profile	Slave	N/A	N/A
No	Yes	Building 2	Master	1	AES/CCMP
Yes	No	Local mesh profile #2	Master	1	NONE
Yes	No	Local mesh profile #3	Master	1	NONE
Yes	No	Local mesh profile #4	Master	1	NONE
Yes	No	Local mesh profile #5	Master	1	NONE
Yes	No	Local mesh profile #6	Master	1	NONE

The local mesh security must be set to AES/CCMP and the specified keys must be a minimum of 32 ASCII characters.



Group: Default Group | Local mesh profile

General

● Enabled ○ Disabled

Name: Building 2

On dual-radio products use: Radio 1 only

On triple-radio products use: Radio 1 only

☑ Security AES/CCMP

Key: ●●●●●●●●●●●

Confirm Key: ●●●●●●●●●●●

Settings

Mode: Master

Mesh ID: 1

Allowed downtime: 10 seconds

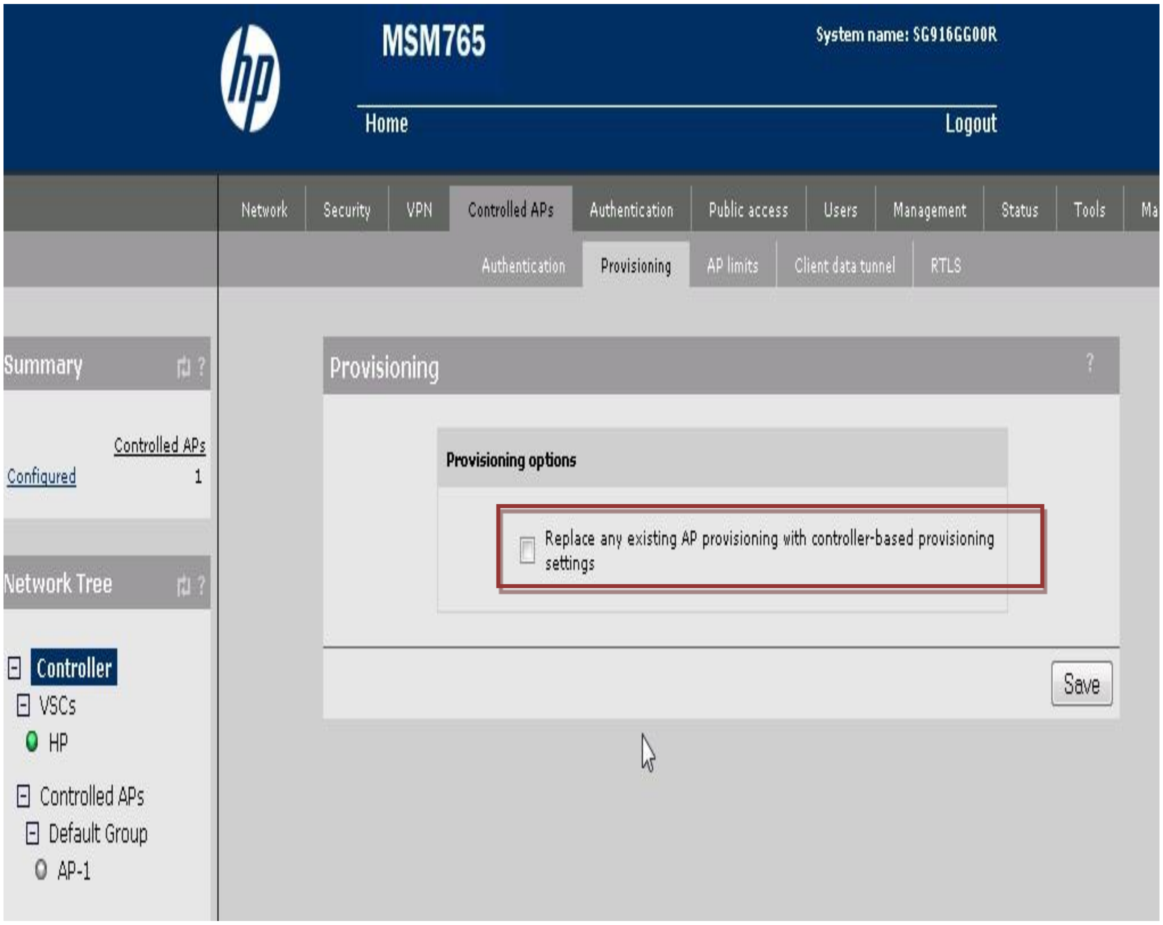
Maximum links: 9

- Provisioning from the mobility controller

If provisioning from the mobility controller is enabled, then the controller must not remove the provisioning settings that ensures an access point operates in the FIPS approved mode of operation. These settings are:

- “Ignore controller firmware update requests”;
- “Test cryptographic system (FIPS compliant operation)”;
- “Controller authentication”; and
- Use of AES/CCMP for the local mesh link.

The page to enable provisioning from the HP MSM765zl Mobility Controller is “Provisioning” accessible from the “Controlled APs” tab.

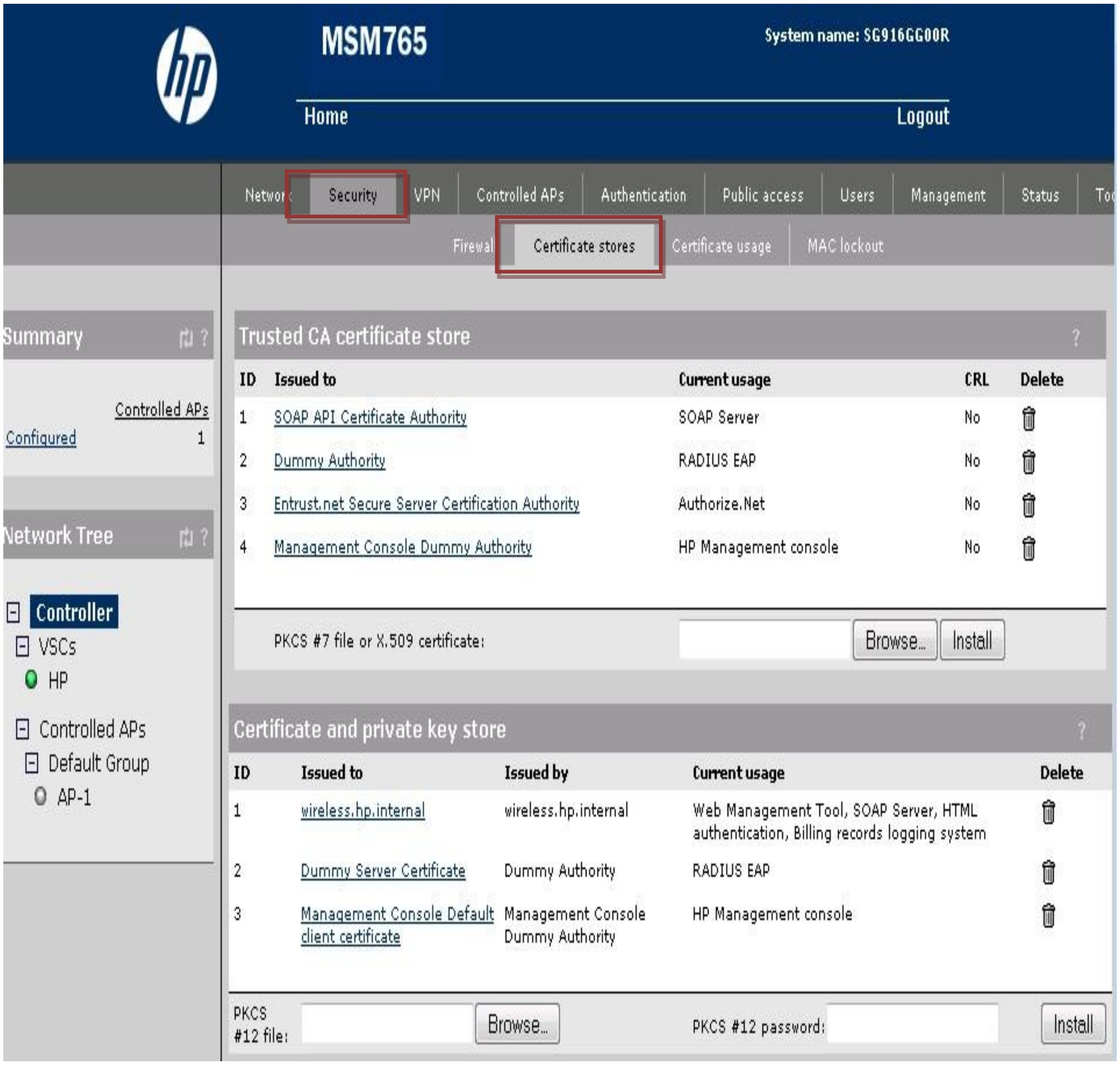


Provisioning options

☐ Replace any existing AP provisioning with controller-based provisioning settings

- Certificates

Only certificates with 2048-bit RSA public keys must be used.



Trusted CA certificate store

ID	Issued to	Current usage	CRL	Delete
1	SOAP API Certificate Authority	SOAP Server	No	🗑
2	Dummy Authority	RADIUS EAP	No	🗑
3	Entrust.net Secure Server Certification Authority	Authorize.Net	No	🗑
4	Management Console Dummy Authority	HP Management console	No	🗑

PKCS #7 file or X.509 certificate:

Certificate and private key store

ID	Issued to	Issued by	Current usage	Delete
1	wireless.hp.internal	wireless.hp.internal	Web Management Tool, SOAP Server, HTML authentication, Billing records logging system	🗑
2	Dummy Server Certificate	Dummy Authority	RADIUS EAP	🗑
3	Management Console Default client certificate	Management Console Dummy Authority	HP Management console	🗑

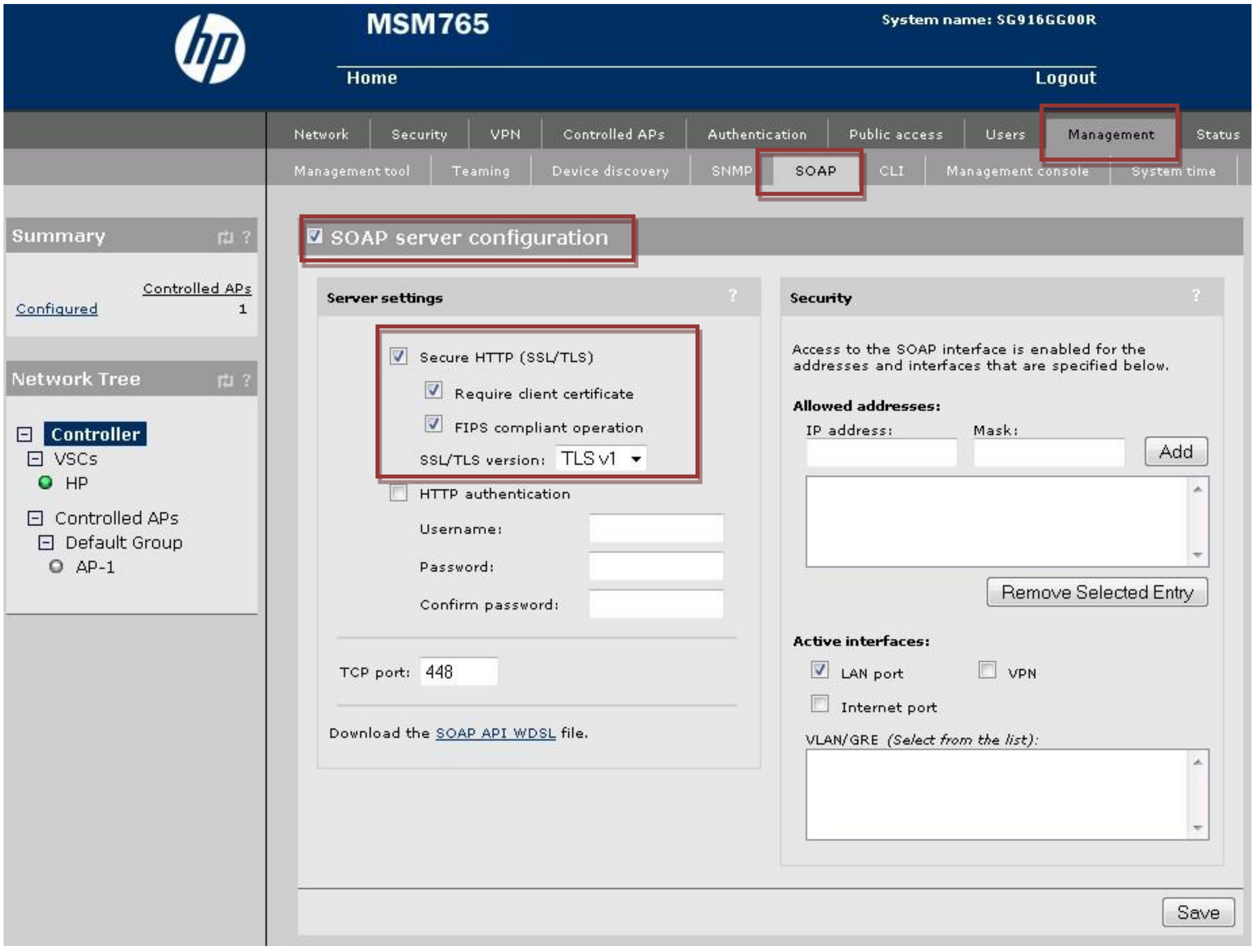
PKCS #12 file:

PKCS #12 password:

- SOAP Configuration

  If SOAP is to be used, the following must be done for the HP MSM765zl Mobility Controller:

  - 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” must be selected from the “SSL/TLS version:” dropdown.
  - A trusted CA X.509 certificate, that will be used to validate the SOAP client certificate, must be installed; and
  - The new page settings must be saved by clicking the “Save” button.



☑ SOAP server configuration

Server settings

☑ Secure HTTP (SSL/TLS)

☑ Require client certificate

☑ FIPS compliant operation

SSL/TLS version: TLS v1

□ HTTP authentication

Username:

Password:

Confirm password:

TCP port: 448

Download the SOAP API WDSL file.

Security

Access to the SOAP interface is enabled for the addresses and interfaces that are specified below.

Allowed addresses:

IP address: Mask:

Active interfaces:

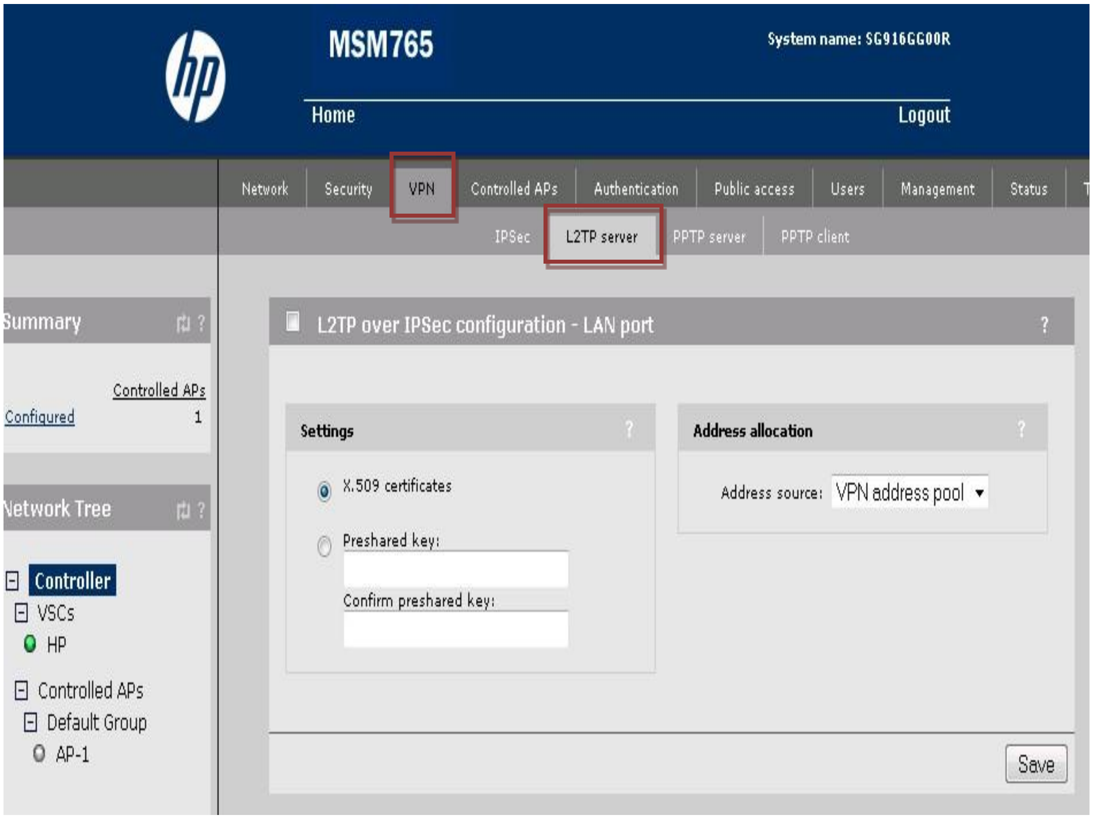
☑ LAN port □ VPN

□ Internet port

VLAN/GRE (*Select from the list*):

- L2TP Server

The L2TP server is not supported in the FIPS approved mode of operation and must not be configured.



Settings

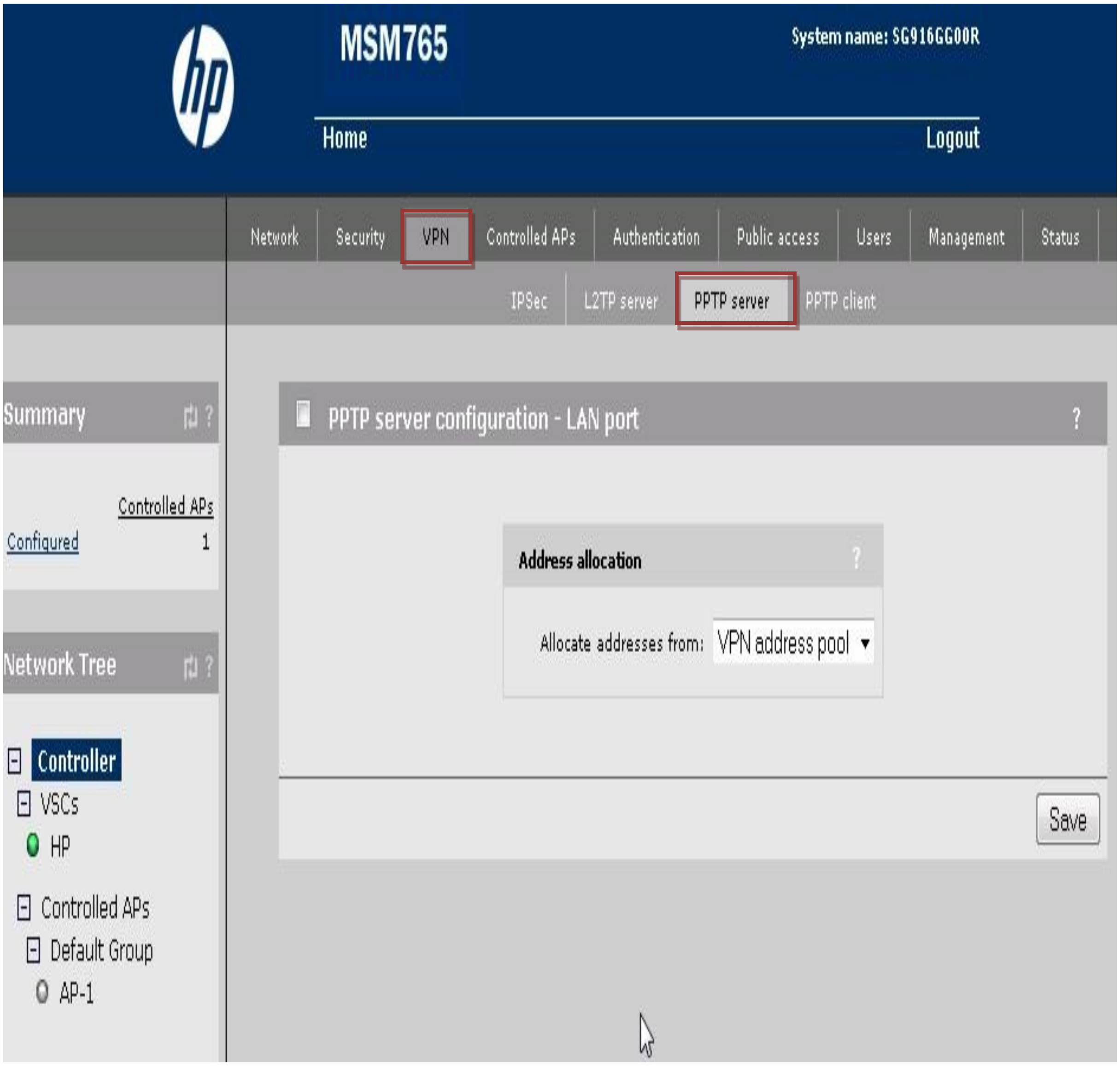
● X.509 certificates

○ Preshared key:

Address source: VPN address pool ▾

- PPTP Server

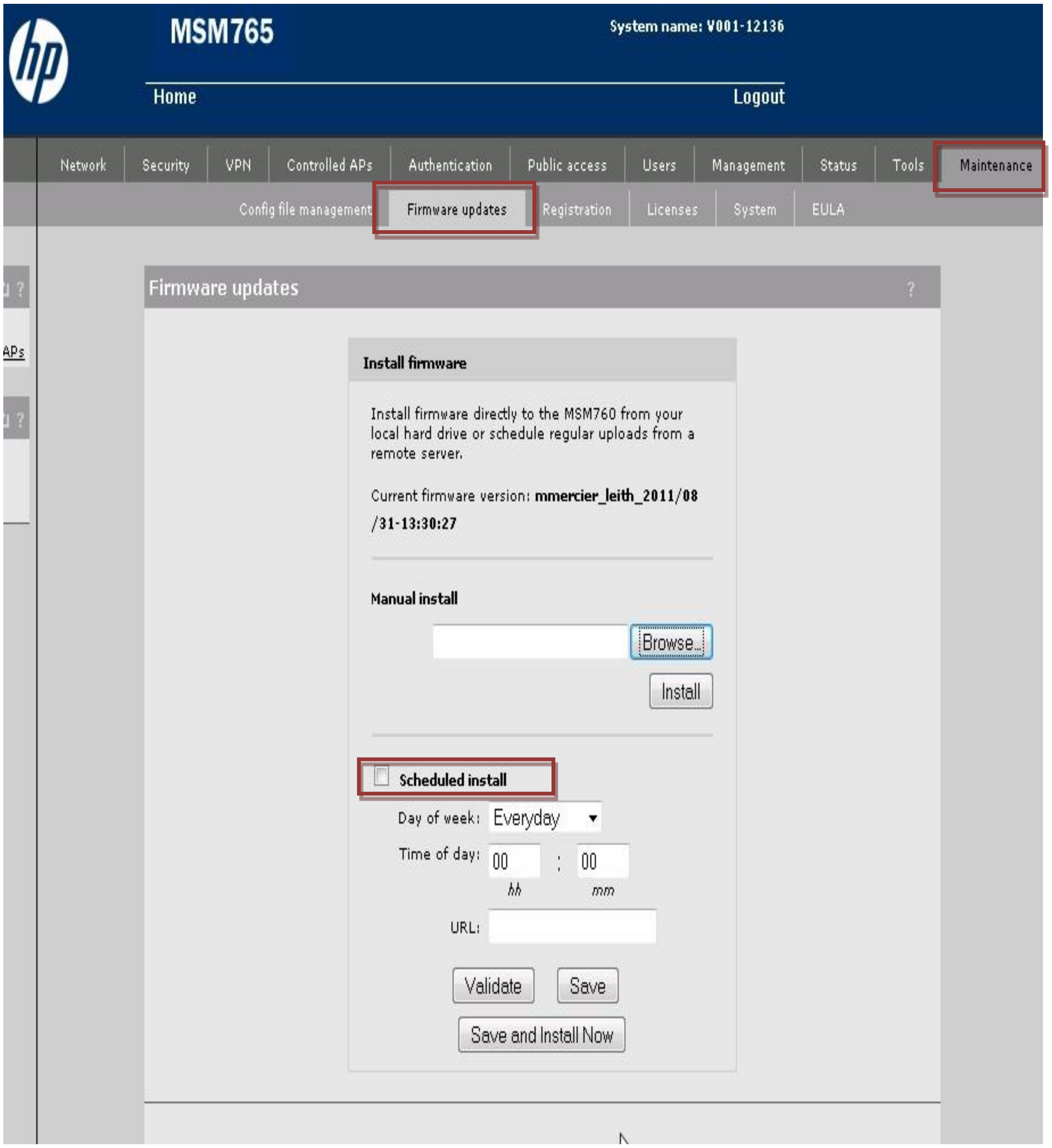
The PPTP server must not be used in the FIPS approved mode of operation.



Allocate addresses from: VPN address pool

- Automatic Firmware Install

  Automatic firmware install must not be configured in the FIPS approved mode of operation.



System name: V001-12136

Firmware updates

Install firmware

Install firmware directly to the MSM760 from your local hard drive or schedule regular uploads from a remote server.

Current firmware version: **mmercier_leith_2011/08/31-13:30:27**

Manual install

□ Scheduled install

Day of week: Everyday

Time of day: 00 : 00 (hh mm)

URL:

The following HP documents may be of assistance in utilizing the HP MSM765zl Mobility Controller:

- *HP 5400zl Switches Installation and Getting Started Guide*;
- *HP 8200zl Switches Installation and Getting Started Guide*;
- *HP Switch Software Management and Configuration 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.

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

4.1 FINITE STATE MODEL

The finite state model for the HP MSM4xx AP is shown and described in the *HP MSM4xx Access Points Finite State Model* document.

4.2 ELECTROMAGNETIC INTERFERENCE / ELECTROMAGNETIC COMPATIBILITY (EMI/EMC)

The HP MSM4xx AP is a wireless LAN device providing 802.11 wireless signals. It is thus an intentional emitter.

The HP MSM4xx APs were tested as meeting FCC 47 CFR Part 15, Subpart B, Class B by the NVLAP-accredited Bureau Veritas Consumer Products Services (H.K.) Ltd., Taoyuan Branch. The EMI/EMC testing is discussed in reports FD990716C01 and FD990622C09.

4.3 SELF-TESTS

4.3.1 Power-Up Self-Tests

The HP MSM4xx AP implements the following power-up self-tests that are initiated on the application of power to the access point:

- Firmware integrity test verifying an 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 firmware implementation of Triple DES;

- Encryption and decryption known answer tests, with 128 bit keys, on the firmware implementation of AES;

- PKCS#1 v1.5 RSA tested with 1024 with signature generation and verification known answer tests in firmware;

- Known answer test on user mode implementation of SHA-1 in firmware;

- Known answer test on user mode implementation of HMAC-SHA-1 in firmware; and

- Generation-encryption and decryption-verification known answer tests on the hardware implementation of AES CCM.

These tests can be executed on demand by rebooting the access point.

4.3.2 Conditional Self-Tests

The HP MSM4xx AP implements the following conditional self-tests:

- Pair-wise consistency tests on generated RSA key pairs;
- Cryptographic bypass test on 802.11i policies (verification of the HMAC-SHA-1 message authentication code 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 HP MSM4xx AP does not support manual key entry. The two independent actions for bypass are the configuration of an open wireless network security policy for the wireless network and the verification of the configuration table when a change is made.

If a conditional self-test passes, the associated service will be provided. If a conditional self-test fails, the access point will reboot.

4.4 DESIGN ASSURANCE

4.4.1 Delivery and Operation

HP tracks each shipment and is able to provide confirmation to the customer that a FIPS-validated HP MSM4xx AP has been received. The *HP MSM4xx Access Point Quickstart* and the *HP MSM 3xx/4xx Access Point Management and Configuration Guide* describe how the user can validate the receipt of a FIPS 140-2 validated HP MSM4xx AP.

The FIPS-compliant firmware is available for download from the HP website. There is controlled access to this firmware and the firmware is encrypted with AES.

4.4.2 Functional Specification

The functional specification for the HP MSM4xx AP is contained in the *Functional Specification for the HP MSM4xx Access Points* document.

4.4.3 Guidance Documents

Crypto-Officer and User guidance for the HP MSM4xx AP is provided in this document and in the *HP MSM4xx Access Point Quickstart*, the *HP MSM 3xx/4xx Access Point Management and Configuration Guide*, and in the *HP MSM7xx Controllers Management and Configuration Guide*.

5 ADDITIONAL SECURITY RULES

1. Public key certificates must only be imported if the key length of the RSA public key is equal to or greater than 2048 bits. The requirement is not enforced by the HP MSM4xx AP.

2. The EAP-TTLS protocol is currently not to be used in the FIPS approved mode of operation since it has not been assessed by the validation authorities. EAP-TLS and PEAP-TLS are allowed in the FIPS approved mode of operation.

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.

When the HP MSM4xx AP is in the FIPS approved mode of operation, it is managed by an Administrator through the HP MSM765zl Mobility Controller. The controller is authenticated to both the Crypto-Officer role and the User role when it is authenticated to the HP MSM4xx AP.

Role	Type of Authentication	Authentication Data
Crypto-Officer	Role-Based	Shared Secret for the Controller
User	Role-Based	Shared Secret for the Controller

Table 3 – Roles and Required Identification and Authentication

There are no authorized physical maintenance activities for the HP MSM4xx AP, and thus the access point does not support a Maintenance role.

Authentication Mechanism	Strength of Mechanism
Shared Secret for the Controller (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 X 10^{15} Maximum of 20 characters per shared secret

Table 4 – Strengths of Authentication Mechanisms

The controller authentication occurs over the Ethernet and could be automated. The processor speed for the HP MSM4xx AP is 800 MHz. Also note that the Shared Secret for the Controller is used in an HMAC computation and thus the access point would have to compute an HMAC from its copy of the Shared Secret for the Controller. The maximum number of instructions that the processor can execute in a minute is 4.8 X 10^{10}, so to have an authentication strength of less than 1 in 100,000 or 1 X 10^{5}, the receipt and processing of the shared secret would need to take less than one instruction. It is of course takes more than 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 Controller, the computation of the HMAC from the copy of the shared secret that the access point has, and the comparison of the computed HMAC with the received HMAC, along with the other processing needed for the authentication, takes more than this number of single 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

The non-FIPS approved services provided by the HP MSM4xx AP – only in the non-FIPS approved mode of operation – are the following:

- Management through an SSL session, or SOAP with SSL, which could make use of a cryptographic algorithm such as Blowfish, MD5, SHA-224, SHA-256, SHA-384, SHA-512, HMAC-MD5, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, or HMAC-SHA-512. The SHA cryptographic algorithms and HMAC cryptographic algorithms are not used, and cannot be used, in the FIPS approved mode of operation, even though they are FIPS-approved algorithms, because not all the requirements of FIPS 140-2 are met for these cryptographic algorithms;

- Authentication of user traffic through a UDP tunnel using HMAC-MD5; and

- Firmware updates[2].

The following sections discuss the FIPS approved services provided by the HP MSM4xx AP in the FIPS-approved mode of operation.

[2] This service is only available during pre-operational initialization and in the non-FIPS-approved mode of operation. Firmware updates are inhibited in the FIPS-approved mode of operation. If a firmware load is done at any time after the access point is configured for the FIPS approved operation, the access point can no longer be FIPS 140-2 compliant unless returned for repair.

7.2.1 Show Status

Purpose:	Provide an indication that the cryptographic module is operating correctly
Approved Functions:	AES, Triple DES, SHA-1, RSA, HMAC-SHA-1, CCM, PRNG
Service Inputs:	Power-On
Service Outputs:	LED Array or Status Indicators to HP MSM765zl Mobility Controller

Status lights indicate the operational status of the HP MSM4xx AP.

The web browser-based management tool on the HP MSM765zl Mobility Controller provides information on the operational status of the HP MSM4xx AP.

7.2.2 Perform Power-Up Self-Tests

Purpose:	Verify that the HP MSM4xx AP is operating correctly
Approved Functions:	AES, Triple DES, SHA-1, RSA, HMAC-SHA-1, CCM, PRNG
Service Inputs:	Power-On
Service Outputs:	LED Array

The success of the power-up self-tests is indicated by the first three LEDs blinking sequentially, the LED pattern that indicates the AP has received an IP address and is looking for a controller.

7.2.3 Perform EAPOL Communication

Purpose:	EAP Authentication of Stations
Approved Functions:	
Service Inputs:	Authentication Request from Station
Service Outputs:	EAP Authentication Packet

7.2.4 Perform WPA2 Secure Wireless Communication

Purpose:	Transfer data securely on wireless network using AES CCMP
Approved Functions:	AES CCM, HMAC-SHA-1, AES key wrap
Service Inputs:	MPDU to be Encrypted or Decrypted
Service Outputs:	Processed MPDU

7.2.5 Perform Plaintext Wireless Communication

Purpose: Transfer plaintext data on wireless network; bypass service
Approved Functions: HMAC-SHA-1
Service Inputs: MPDU
Service Outputs: Unprocessed MPDU

7.2.6 Management through TLS Session

Purpose: Configuration of HP MSM4xx AP through HP MSM765zl Mobility Controller
Approved Functions: RSA Key Generation and Signature Verification, Diffie-Hellman Key Agreement, AES in CBC mode, Triple DES in CBC mode
Non-Approved
Function: MD5 (used in the derivation of the master key)
Service Inputs: Configuration Information from Controller, PMK
Service Outputs: Indicator of Success or Failure of Operation

7.2.7 Plaintext Key and CSP Zeroization

Purpose: Zeroize Plaintext Cryptographic Keys and Other CSPs
Approved Function: Zeroization
Service Inputs: Request to Reset to Factory Defaults through Controller Command or Press of Reset Button (non-FIPS approved mode of operation)
Service Outputs: Factory Defaults Reset

7.3 ROLES, SERVICES AND ACCESSES

7.3.1 Anonymous Services

The following services are provided to operators 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 HP MSM4xx AP do not require the operator to assume a role. It only requires the provision of power.	The initial power-up self-tests do not use operational keys or other CSPs and therefore do not affect the security of the cryptographic module.

Table 5 – 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.

Role	Authorized Services
User (Configuration of Wireless Communication through HP MSM765zl Mobility Controller)	Perform EAPOL Communication Perform WPA2 Secure Wireless Communication Perform Plaintext Wireless Communication Show Status
Crypto-Officer (Management of HP MSM4xx AP through HP MSM765zl Mobility Controller)	Management through TLS Session Show Status Plaintext Key and CSP Zeroization (Command) Perform Power-Up Self-Tests (Command)

Table 6 – Services Authorized for Roles

7.4 SECURITY DATA

7.4.1 General

Security data comprises all cryptographic keys and other 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).

7.4.2 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 HP MSM4xx AP.

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

7.4.3 Critical Security Parameters

Shared Secret for the Controller
PRNG Seed

7.4.4 Cryptographic Key Management

Cryptographic Keys and CSPs	Key Length	Key Strength	FIPS Approved Establishment Mechanism	State within Module
Local X.509 Certificate RSA Public Key	2048 bits	112 bits	Internally-generated with ANSI X9.31 RSA Key Generation; EE/ED to controller	Plaintext in NAND Flash
Local RSA Private Key (mate of Local X.509 Certificate RSA Public Key)	2048 bits	112 bits	Internally-generated with ANSI X9.31 RSA Key Generation	Plaintext in NAND Flash
Web Server X.509 Certificate RSA Public Key	2048 bits	112 bits	Externally generated; part of new firmware	Plaintext in NAND Flash
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	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 bit for AES key	EE/ED; RSA public key encrypted from controller or agreed upon using Diffie-Hellman key agreement	Ephemeral in SDRAM

Shared Secret for the Controller	Minimum 8 printable ASCII characters	1 in 2.04 X 10^{15}	EE/ED;
			Encrypted with TLS Session Key, initial entry;
			Used as HMAC key for HMAC computation when used for authentication
				Plaintext in NAND Flash

PSK	256 bits	256 bits	EE/ED; Encrypted with TLS Session Key; from controller	Plaintext in NAND Flash
PMK	256 bits	256 bits	EE/ED; Encrypted with TLS Session Key; from controller	Plaintext in NAND Flash
HMAC Keys	160 bits	160 bits	Used in PRF; Generated with FIPS-approved PRNG	Plaintext in NAND Flash
KCK	128 bits	128 bits	Derived from PSK or PMK using PRF	Plaintext in NAND Flash
KEK (AES Key)	128 bits	128 bits	Derived from PSK or PMK using PRF	Plaintext in NAND Flash

AES CCMP Temporal Keys	128 bits	128 bits	Derived from PSK or PMK using PRF;
			EE/ED;
			Output encrypted with KEK to stations
				Plaintext in NAND Flash

Link Mesh Master Key	128 bits	128 bits	EE/ED;
			Encrypted with TLS Session Key;
			from controller
				Plaintext in NAND Flash

Link Mesh Temporal Key	128 bits	128 bits	Derived from Link Mesh Master Key using PRF;
			EE/ED;
			Output encrypted with KEK to stations
				Plaintext in NAND Flash

Group Master Key	128 bits	128 bits	EE/ED;
			Encrypted with TLS Session Key;
			from controller
				Plaintext in NAND Flash

Group Temporal Key	128 bits	128 bits	Derived from Group Master Key using PRF;
			EE/ED;
			Output encrypted with KEK to stations
				Plaintext in NAND Flash

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 7 – Cryptographic Keys and Other Critical Security Parameters Table

Table 8 specifies the random number generators employed by the HP MSM4xx AP.

Identification	Type	Usage
ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES PRNG using AES with 256-bit keys	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 8 – HP MSM4xx AP Pseudo-Random Number Generators

Table 9 specifies, for those keys that are generated automatically, whether or not they are output, and, if so, the format in which they are output and their destination.

Identification	Output	Destination	Format
Local X.509 Certificate RSA Public Key	Yes	To HP MSM765zl Mobility Controller	Plaintext
Local RSA Private Key (mate of Local X.509 Certificate RSA Public Key)	No	Not Applicable	Not Applicable
Web Server X.509 Certificate RSA Public Key	No	Not Applicable	Not Applicable
Diffie-Hellman Private Key	No	Not Applicable	Not Applicable
Diffie-Hellman Public Keys	Yes	To HP MSM765zl Mobility Controller	Plaintext
TLS Session Keys	No	Not Applicable	Not Applicable
PSK	No	Not Applicable	Not Applicable
PMK	No	Not Applicable	Not Applicable
HMAC Keys	No	Not Applicable	Not Applicable
KCK	No	Not Applicable	Not Applicable

KEK (AES Key)	No	Not Applicable	Not Applicable
AES CCMP Temporal Keys	Yes	To Wireless Stations	Encrypted with KEK
Link Mesh Master Key	No	Not Applicable	Not Applicable
Link Mesh Temporal Key	Yes	To Wireless Stations	Encrypted with KEK
Group Master Key	No	Not Applicable	Not Applicable
Group Temporal Key	Yes	To Wireless Stations	Encrypted with KEK
PRNG Seed Key (AES Key)	No	Not Applicable	Not Applicable
PRNG Seed	No	Not Applicable	Not Applicable

Table 9 – HP MSM4xx AP Key Output

Table 10 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 Other CSPs**	**Type(s) of Access (Read (R), Write (W), Execute (E))**
Show Status	Shared Secret for the Controller	E
	TLS Session Keys	E
Perform Power-Up Self-Tests	AES, Triple DES, RSA, HMAC, PRNG Seed, PRNG Seed Key (Power-Up Self-Test Only Keys – not CSPs)	E
	Shared Secret for the Controller (for command)	E
	TLS Session Key (for command)	E
Perform EAPOL Communication	None	

Perform WPA2 Secure Wireless Communication	Shared Secret for the Controller	E
	TLS Session Key	E
	PSK	W, E
	PMK	W, E
	HMAC Keys	W, E
	KCK	W, E
	KEK	W, E
	AES CCMP Temporal Keys	W, E
	Link Mesh Master Key	W, E
	Link Mesh Temporal Key	W, E
	Group Master Key	W, E
	Group Temporal Key	W, E
	PRNG Seed	W, E
	PRNG Seed Key	W, E
Perform Plaintext Wireless Communication	Shared Secret for the Controller	E
	TLS Session Key	E
	HMAC Key	E
Management through TLS Session	Shared Secret for the Controller	E
	Local RSA Private Key	W, E
	Local X.509 Certificate RSA Public Key (not a CSP)	W
	Web Server X.509 Certificate RSA Public Key (not a CSP)	R, W
	Diffie-Hellman Private Keys	W, E
	Diffie-Hellman Public Keys (not CSPs)	W, E
	TLS Session Keys	W, E
	PRNG Seed	W, E
	PRNG Seed Key	W, E

Plaintext Key and CSP Zeroization	Shared Secret for the Controller	E, W
	Local X.509 Certificate RSA Public Key (not a CSP)	E, W
	RSA Private Key	E, W
	TLS Session Keys	E, W
	Diffie-Hellman Public Keys (not CSPs)	W
	Diffie-Hellman Private Keys	W
	PSK	W
	PMK	W
	HMAC Keys	W
	KCK	W
	KEK	W
	AES CCMP Temporal Keys	W
	Link Mesh Master Key	W
	Link Mesh Temporal Key	W
	Group Master Key	W
	Group Temporal Key	W
	PRNG Seed	E, W
	PRNG Seed Key	E, W

Table 10 – Access Rights within Services

7.5 IMPLEMENTED CRYPTOGRAPHIC ALGORITHMS

The following table outlines the FIPS approved cryptographic algorithms that are implemented in the HP MSM4xx AP, 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	1823
AES CCM (128 bit keys) generation-encryption and decryption-verification in hardware	1840
*Triple DES (168-bit keys) encryption and decryption in CBC mode in firmware	1176
*SHA-1 hashing (firmware)	1602
HMAC-SHA-1 message authentication (firmware)	1078
*RSA (2048 bit keys) PKCS#1 v1.5 signature verification and ANSI X9.31 key generation in firmware	916
*ANSI X9.31 PRNG using 256-bit AES key	960

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

Table 11 – Implemented FIPS Approved Cryptographic Algorithms

The HP MSM4xx AP implements the following non-FIPS approved cryptographic algorithms: Blowfish, MD5, HMAC-MD5, Diffie-Hellman key agreement for TLS with 1024 bit (Group 2) or 1536 bit (Group 5) keys (key establishment methodology provides 80 or 96 bits of equivalent encryption strength), RSA key wrapping for TLS with 1024 and 2048 bit keys (key transport method provides 80 or 112 bits of equivalent key strength), and AES key wrapping for 802.11i handshake with 128-bit AES keys (key establishment methodology provides 128 bits of encryption strength).

The HP MSM4xx APs also implements 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 HP MSM4xx AP from unauthorized physical access and the actions that are required to ensure that the physical security of the module is maintained.

8.2 PHYSICAL SECURITY MECHANISMS

8.2.1 Tamper Evident Seals

The HP MSM4xx AP is completely enclosed within a hard plastic with a metal bottom, production-grade enclosure.

The HP MSM4xx AP is protected from opening by tamper evident seals on the front and back of the enclosure. A third tamper evident seal is affixed over the reset button to prevent the access point to be put in an open, non-FIPS approved state. **Figure 3** shows the locations of the three affixed seals.

Before being used, tamper evident seals provided by HP should be kept in a locked cabinet, accessible only by the HP MSM4xx AP Administrator (Crypto-Officer). The HP MSM4xx AP should be kept in a locked cabinet until the tamper evident seals are affixed.

8.3 INSPECTION AND TESTING

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	Weekly preferred but at least monthly	Examine visually for evidence that any seal has been damaged, broken, or missing

Table 12 – Inspection/Testing of Physical Security Mechanisms

The inspection of the tamper evident seals is to be done by the Administrator (Crypto-Officer).

9 SECURITY POLICY FOR MITIGATION OF OTHER ATTACKS

9.1 OVERVIEW

The HP MSM4xx AP does 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 13 – Mitigation of Other Attacks