



HP ProCurve M111 Client Bridge

Management and Configuration Guide

HP ProCurve M111 Client Bridge

Management and Configuration Guide

© Copyright 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number

5998-0329

April 2010

Applicable Products

M111 Client Bridge (WW J9389A)

M111 Client Bridge (Japan J9523A)

Trademark Credits

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Open Source Software Acknowledgement Statement

This software incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, HP ProCurve Networking will make available a complete, machine-readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:

Hewlett-Packard Company, L.P.

GNU GPL Source Code

Attn: ProCurve Networking Support

Roseville, CA 95747 USA

Safety

Before installing and operating this product, please read *Safety information on page 1-5*.

Contents

1 Introduction

About this guide	1-2
Products covered.....	1-2
Important terms.....	1-2
Conventions	1-2
Warnings and cautions	1-2
Commands and program listings	1-3
Introducing the M111 Client Bridge.....	1-4
Key features.....	1-4
Safety information.....	1-5
Professional Installation Required	1-5
Servicing.....	1-5
HP ProCurve Networking support.....	1-6
Before contacting support.....	1-6
Online documentation	1-6

2 Getting started

Deploying the M111	2-2
Scenario 1: Connecting wired devices to a wireless network.....	2-2
Overview.....	2-2
Configuration procedure	2-3
A. Configure your computer.....	2-3
B. Connect to the M111	2-4
C. Start the M111.....	2-4
D. Connect to the management tool and login.....	2-4
E. Set the M111 IP address	2-5
F. Configure a station profile.....	2-6
G. Connect the wired computers to the M111.....	2-7

Scenario 2: Connecting a wired device using MAC address cloning.....	2-8
Overview	2-8
Configuration procedure	2-9
A. Configure your computer.....	2-9
B. Connect to the M111	2-9
C. Start the M111.....	2-9
D. Connect to the management tool and login.....	2-9
E. Set the M111 IP address	2-9
F. Configure a station profile.....	2-9
G. Configure MAC cloning options.....	2-9
H. Connect the wired device to the M111	2-10
Scenario 3: Connecting a serial device to a wireless network	2-11
Overview	2-11
Configuration procedure	2-12
A. Configure your computer.....	2-12
B. Connect to the M111	2-12
C. Start the M111.....	2-12
D. Connect to the management tool and login.....	2-12
E. Set the M111 IP address	2-12
F. Configure a station profile.....	2-12
G. Configure the serial connection.....	2-12

3 Working with the M111

Management tool.....	3-3
Starting the management tool.....	3-3
Customizing management tool settings.....	3-4
Manager and Operator accounts.....	3-4
Security policies.....	3-6
Security	3-6
Web server	3-7
Auto-refresh.....	3-7
IP address configuration	3-7
To configure IP addressing.....	3-8
Radio configuration	3-9
Wireless range	3-9

To configure the radio.....	3-10
Wireless mode	3-10
Restrict channels to	3-10
Antenna selection	3-11
Fast roaming threshold	
Fast roaming delta threshold	3-11
Fast roaming threshold count	3-12
Minimum SNR threshold.....	3-12
Scan channel delay	3-12
Fast scan channel delay	3-12
Roaming persistence	3-12
Advanced wireless settings	3-13
RTS threshold.....	3-13
Transmit power control	3-13
Using station profiles to establish a wireless link.....	3-13
To add or edit a station profile.....	3-15
General	3-15
Wireless security	3-16
Quality of service	3-18
Viewing APs in the neighborhood.....	3-18
Field descriptions	3-19
Configuring Quality of Service (QoS).....	3-19
QoS settings in a station profile.....	3-20
Priority mechanisms.....	3-20
Upstream DiffServ tagging.....	3-22
Creating IP QoS profiles	3-22
To define an IP QoS profile	3-22
Settings.....	3-23
Connecting serial devices	3-23
Serial port connector	3-24
To connect a serial device	3-24
DNS configuration.....	3-27
Handling unsupported traffic	3-29
To forward unsupported traffic	3-29
IP forwarding	3-30

Cloning the address of a wired device.....	3-30
Limitations	3-30
Enabling Ethernet MAC cloning.....	3-31
Wireless access to the M111 when MAC cloning is active	3-31
Setting up management traffic interception.....	3-32
Using filters to restrict wireless traffic.....	3-33
Assigning a management address	3-34
To assign a management address	3-34
SNMP	3-35
Attributes	3-36
v1/v2c communities	3-36
v3 users	3-36
Notification receivers.....	3-37
Security	3-37
Managing certificates.....	3-37
802.1X certificates	3-38
802.1X — Install TLS client certificate.....	3-38
802.1X — Manage TLS client certificates	3-39
802.1X — Trusted CA certificates.....	3-39
802.1X — Manage CA certificates.....	3-39
Certificate stores	3-39
Trusted CA certificate store	3-40
Certificate and private key store.....	3-41
Certificate usage	3-42
Changing the certificate assigned to a service	3-43
About certificate warnings	3-43
Configuration file management.....	3-44
Manual configuration file management.....	3-44
Backup configuration.....	3-44
Reset configuration	3-45
Restore configuration.....	3-45
Scheduled operations.....	3-45
Software updates.....	3-46
Performing an immediate software update.....	3-47
Performing a scheduled update	3-47

A Regulatory information

Notice for U.S.A.	4-2
Notice for Canada.....	4-3
Notice for the European Community.....	4-3
Disposal of Waste Equipment by Users in Private Household in the European Union	4-5
Supported External Antennas.....	4-5
Notice for Brazil.....	4-5
Notice for Japan.....	4-6
Notice for Taiwan	4-6
Notice for Korea	4-6

B Resetting to factory defaults

How it works.....	5-2
Using the Reset button.....	5-2
Using the management tool.....	5-2

Introduction

Contents

About this guide	1-2
Products covered.....	1-2
Important terms.....	1-2
Conventions	1-2
Introducing the M111 Client Bridge.....	1-4
Key features.....	1-4
Safety information.....	1-5
HP ProCurve Networking support.....	1-6
Online documentation	1-6

About this guide

This guide explains how to install, configure, and operate the M111 Client Bridge.

Products covered

The manual applies to the M111 Client Bridge (J9389A WW, J9523A Japan).

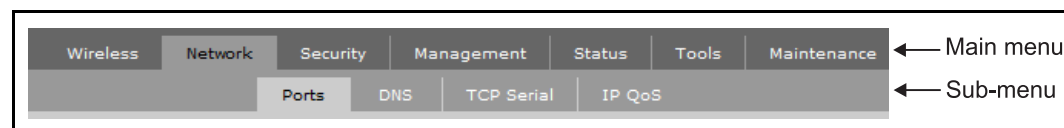
Important terms

The following terms are used in this guide.

Term	Description
MSM AP	Refers to any HP ProCurve Networking MSM3xx or MSM4xx Access Point.
Controller	Refers to any HP ProCurve Networking MSM7xx Controller, including both Access Controller and Mobility Controller variants.

Conventions

This guide uses specific syntax when directing you to interact with the management tool user interface. Refer to the following image for identification of key user-interface elements and then the table below for example directions:



Example directions in this guide	What to do in the user interface
Select Network > Ports	On the main menu select Network and then select Ports on the sub-menu.
For Password specify secret22 .	In the Password field enter the text secret22 exactly as shown.

Warnings and cautions

Do not proceed beyond a WARNING or CAUTION notice until you fully understand the hazardous conditions and have taken appropriate steps.

Warning

Identifies a hazard that can cause physical injury or death.

Caution

Identifies a hazard that can cause the loss of data or configuration information, create a non-compliant condition, or hardware damage.

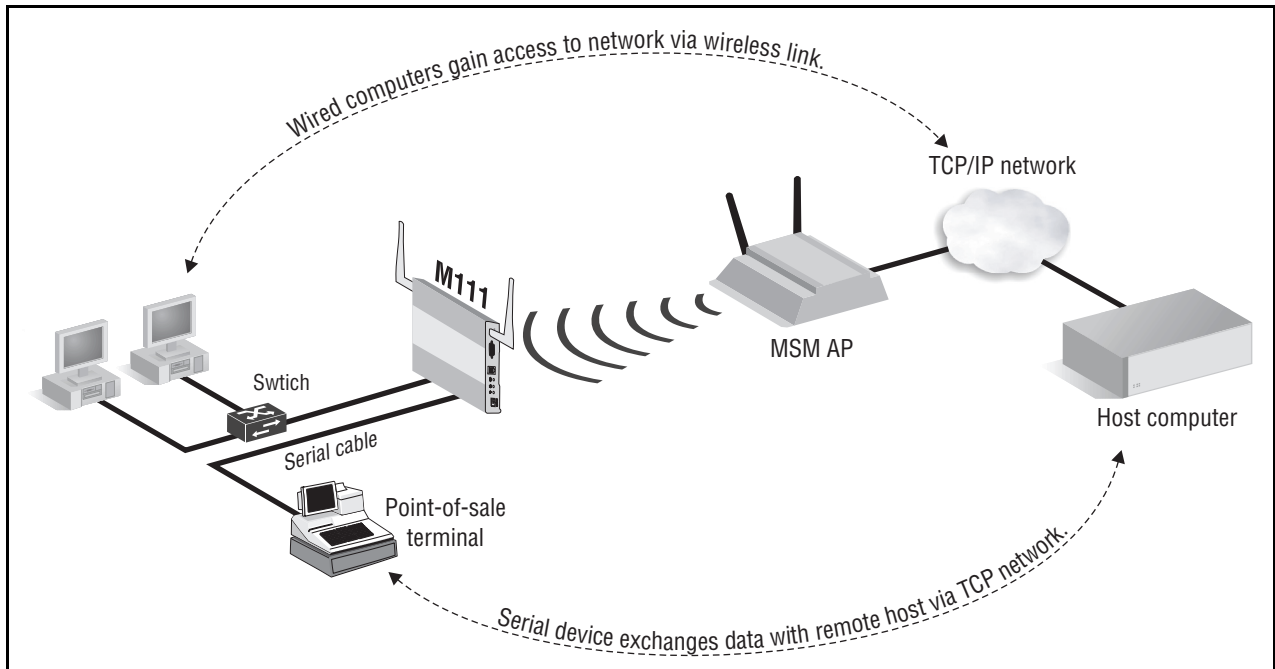
Commands and program listings

Monospaced text identifies commands and program listings as follows:

Example	Description
<code>use-access-list</code>	Command name. Specify it as shown.
<code>ip_address</code>	Items in italics are parameters for which you must supply a value.
<code>ssl-certificate=<i>URL</i> [%s]</code>	Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can either include the “%s” or omit it.
<code>[ONE TWO]</code>	Items separated by a vertical line indicate a choice. Specify only one of the items. Do not include the vertical line.

Introducing the M111 Client Bridge

The M111 connects legacy Ethernet or serial communications devices to a wireless local area network (WLAN) with simplicity and security. It enables the deployment of legacy client devices (such as electronic cash registers, servers, printers), in any location where a WLAN signal is available, eliminating the installation of a cabling infrastructure.



In this sample deployment, the M111 provides a wireless link to a TCP/IP network for a pair of desktop computers and a serial point-of-sale terminal. An MSM AP is used to create the wireless network.

Key features

- Bridges an Ethernet LAN segment to a wireless network, providing connectivity for up to 20 client devices that run IPV4 and a single client device running a legacy networking protocol, such as DECnet, IPX, or Appletalk.
- Provides an integrated serial-to-TCP/IP converter which enables a TIA-232 asynchronous terminal device to communicate with a compatible station over a wireless network.
- 802.11b a/b/g radio supporting antenna diversity.
- Provides enhanced security using configurable Ethernet MAC and bidirectional Layer 2 and Layer 3 protocol filters.
- Ensures wireless network privacy using WPA2, WPA, and WEP security and high performance hardware-assisted AES, TKIP, WEP encryption.
- Provides 802.1X, PEAP, EAP-TLS, EAP-FAST, and EAP-TTLS authentication.
- Features a rugged, plenum-rated metal enclosure.

Safety information

Warning

Professional Installation Required

Prior to installing or using an M111, consult with a professional installer trained in RF installation and knowledgeable in local regulations including building and wiring codes, safety, channel, power, indoor/outdoor restrictions, and license requirements for the intended country. It is the responsibility of the end user to ensure that installation and use comply with local safety and radio regulations.

Surge protection and grounding: If you plan on connecting an outdoor antenna to an M111, make sure that proper lightning surge protection and grounding precautions are taken according to local electrical code. Failure to do so may result in personal injury, fire, equipment damage, or a voided warranty. The HP ProCurve hardware warranty provides no protection against damage caused by static discharge or a lightning strike.

Cabling: You must use the appropriate cables, and where applicable, surge protection, for your given region. For compliance with EN55022 Class-B emissions requirements use shielded Ethernet cables.

Country of use: In some regions, you are prompted to select the country of use during setup. Once the country has been set, the M111 will automatically limit the available wireless channels, ensuring compliant operation in the selected country. Entering the incorrect country may result in illegal operation and may cause harmful interference to other systems.

Safety: Take note of the following safety information during installation:

- If your network covers an area served by more than one power distribution system, be sure all safety grounds are securely interconnected.
- Network cables may occasionally be subject to hazardous transient voltages (caused by lightning or disturbances in the electrical power grid).
- Handle exposed metal components of the network with caution.
- An M111 and all interconnected equipment must be installed indoors within the same building (except for outdoor models / antennas), including all PoE-powered network connections as described by Environment A of the IEEE 802.3af standard.

Servicing

There are no user-serviceable parts inside HP ProCurve Networking products. Any servicing, adjustment, maintenance, or repair must be performed only by trained service personnel.

HP ProCurve Networking support

HP ProCurve Networking offers support 24 hours a day, seven days a week through a number of automated electronic services. See the Customer Support/Warranty booklet included with your product.

The HP ProCurve Networking Web site, www.hp.com/go/procurve/support provides up-to-date support information.

Additionally, your HP-authorized network reseller can provide you with assistance, both with services that they offer and with services offered by HP.

Before contacting support

To make the support process most efficient, before calling your networking dealer or HP Support, you first should collect the following information:

Collect this information	Where to find it
Product identification.	On the rear of the product.
Software version.	The M111 management tool Login page.
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

Online documentation

For the latest documentation, visit the HP ProCurve Networking manuals Web page at: www.hp.com/go/procurve/manuals.

Getting started

Contents

Deploying the M111	2-2
Scenario 1: Connecting wired devices to a wireless network	2-2
Overview	2-2
Configuration procedure	2-3
Scenario 2: Connecting a wired device using MAC address cloning	2-8
Overview	2-8
Configuration procedure	2-9
Scenario 3: Connecting a serial device to a wireless network	2-11
Overview	2-11
Configuration procedure	2-12

Deploying the M111

This chapter provides step-by-step instructions that explain how to configure the M111 for the following frequently used deployments.

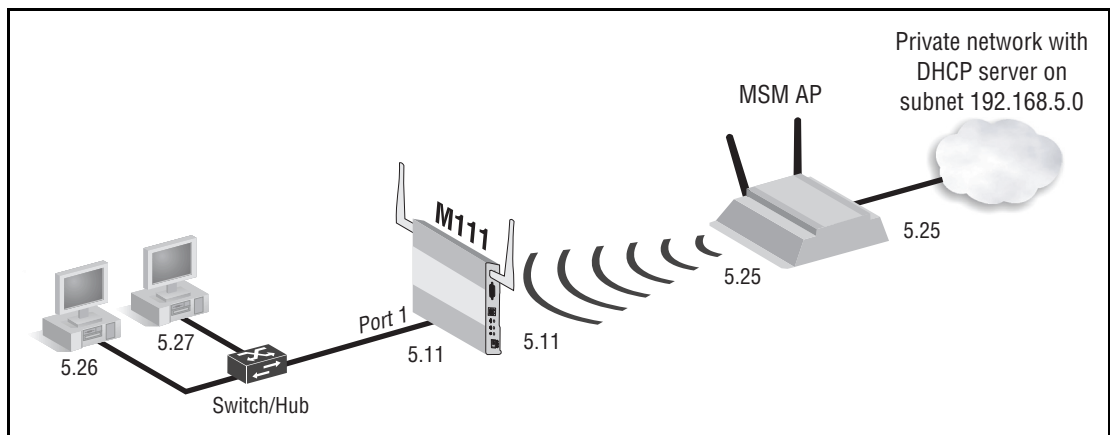
- *Scenario 1: Connecting wired devices to a wireless network on page 2-2*
- *Scenario 2: Connecting a wired device using MAC address cloning on page 2-8*
- *Scenario 3: Connecting a serial device to a wireless network on page 2-11*

Scenario 1: Connecting wired devices to a wireless network

This scenario explains how to use the M111 to connect several wired devices to a network via a wireless link.

Overview

In this scenario, the M111 connects two wired computers to a private network via a wireless connection. The two computers are linked to a hub or switch which is plugged into Port 1 on the M111. Once connected to the private network via the wireless link, the computers obtain an IP address from the DHCP server and can then communicate with resources on the private network.



(Although this scenario shows two connected devices, up to 20 Ethernet devices can share the wireless link, with each device getting its own unique IP address from the DHCP server.)

This scenario assumes that:

- The M111 is in its factory-default state.
- A DHCP server is operating on the private network, assigning addresses on the subnet 192.168.5.0.

- The MSM AP is operating in autonomous mode in its factory-default configuration. (As such, it obtains an IP address of 5.25 from the DHCP server and creates a wireless network call *HP ProCurve*.) Install the MSM AP as described in its Quickstart.
- The wired computers are configured to obtain their IP addresses automatically (DHCP clients).

Configuration procedure

Configuration of the M111 occurs via its Web-based management tool. To access this tool you need a computer running at least Microsoft Internet Explorer 7/8 or Firefox 3.x.

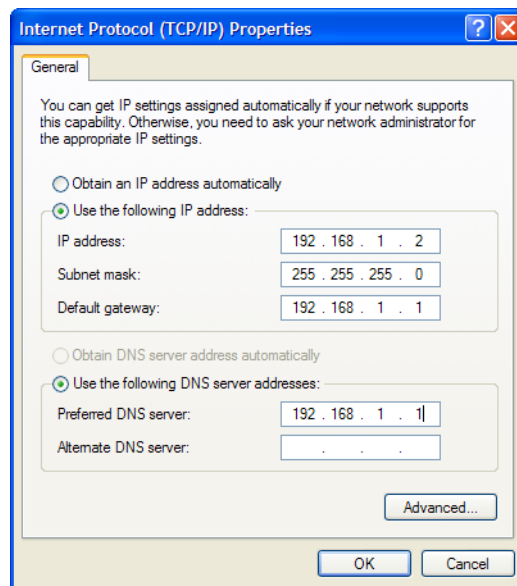
Note

Do not power on the M111 until directed.

A. Configure your computer

1. Configure the LAN port on a computer to use the static IP address **192.168.1.2** with a subnet mask of **255.255.255.0**. Set the default gateway to **192.168.1.1**, and DNS server to **192.168.1.1**.

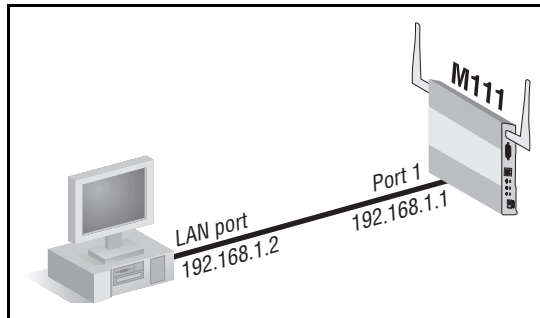
For example, in Windows XP, select **Control Panel > Network Connections > Local Area Connection > Properties > Internet Protocol (TCP/IP) > Properties**.



2. Disable any wireless connection.

B. Connect to the M111

Connect the LAN port on the computer to the Ethernet port on the M111 using a standard Ethernet cable. (If your computer has an older 10BaseT-only Ethernet interface, then use a crossover cable instead.)



C. Start the M111

Power on the M111 using one of the following methods.

- • A PoE-enabled switch. Various PoE-enabled switches are available from HP ProCurve.
- • An HP ProCurve PoE 1-Port Power Injector (J9407A)
- • An HP ProCurve MSM31x Power Supply (J9405A). This scenario uses this method.

Proceed to the next step once the Power light stops blinking and remains on.

D. Connect to the management tool and login

1. Open a web browser on the computer and specify the address: **https://192.168.1.1**.
2. A security certificate warning is displayed the first time that you connect to the management tool. This is normal. Select whatever option is needed in your Web browser to continue to the management tool. The security warning will not appear again unless you change the IP address of the M111.

To eliminate the security warning, you need to replace the default certificate that is installed on the M111. See [About certificate warnings on page 3-43](#).

3. On the Login page, specify **admin** for both **Username** and **Password** and then select **Login**.
4. On the License Agreement page, read and then select **Accept License Agreement**.
5. The Registration page appears. It is recommended that you register later by selecting **Maintenance > Registration**.
6. If a **Country** prompt appears, select the country in which the M111 will operate.

Caution

Once the country has been set, the M111 will automatically limit the available wireless channels, ensuring compliant operation in the selected country. Entering the incorrect country may result in illegal operation and may cause harmful interference to other systems.

7. At the password prompt it is recommended that you change the default password. Enter the new password and select **Save**.

About passwords

The default username and password is admin. New passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (") cannot be used. Passwords must also conform to the selected security policy as described in [Security policies on page 3-6](#).

E. Set the M111 IP address

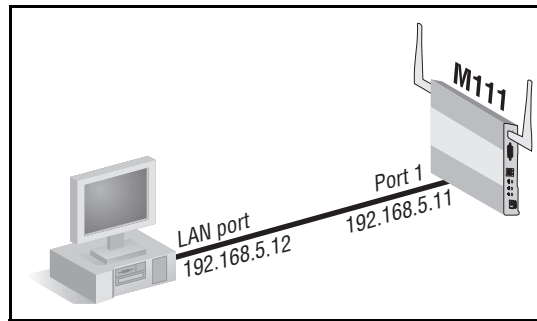
By default the M111 operates as a DHCP client on both the Ethernet port and the Wireless port. Once it establishes a connection with a DHCP server via either port, it will receive a new IP address from the DHCP server address pool, and the management tool will no longer be accessible at the default address of 192.168.1.1. To maintain access to the management tool at a known IP address, you can use one of the following strategies:

- Pre-configure the DHCP server on the network to assign a specific IP address to the M111. To do this you need to specify the M111 MAC address and a reserved IP address on the DHCP server. The M111 MAC address is printed on the M111 label identified as **Wireless Base MAC**, or listed on the management tool **Home** or **Login** page as **Wireless MAC address**.
- Define a management address. This is a secondary IP address on which the management tool can be reached. See [To assign a management address on page 3-34](#).
- Assign a static IP address to the M111 as follows:
 1. Select **Network > DNS**.
 2. Under **DNS servers**, set **Server** to the IP address of the DNS server on the private network.
 3. Select **Network > Ports > Bridge port**.
 4. Under **Assign IP address via**, select **Static** and then **Configure**.
 5. Under **Port settings**, configure the following settings:
 - **IP address:** Set the IP address on the same subnet as the MSM AP to which the M111 will connect once installed. Respect any DHCP server-mandated static address ranges. For this scenario, use **192.168.5.11**.
 - **Mask:** Set the corresponding mask for the IP address. This scenario uses the mask **255.255.255.0**.
 - **Default gateway:** Set the IP address of the gateway on the network.

Getting started

Scenario 1: Connecting wired devices to a wireless network

6. Select **Save**. The IP address of the M111 will immediately change, causing you to lose your connection to the management tool. This is normal. To re-establish the connection, configure the computer with a static IP address on the same subnet as the M111. For this scenario, use **192.168.5.12**.



7. Re-launch the management tool by browsing to the new IP address assigned to the M111: **https://192.168.5.11**.

F. Configure a station profile

A station profile contains the settings that the M111 uses to establish a connection with a wireless network. This section explains how to customize the default station profile that is pre-configured on the M111.

1. Select **Wireless > Station profiles** and select the **HP ProCurve** profile in the table. The **Add/Edit Stations profile** page opens.

The screenshot shows the 'Station profiles - Add/Edit Station profile' configuration window. It is divided into three main sections: General, Wireless security, and Quality of service.

- General:** Includes radio buttons for 'Enabled' (selected) and 'Disabled'. Fields for 'Profile name' (HP ProCurve), 'WLAN name (SSID)' (HP ProCurve), and 'AP's MAC address' (00:00:00:00:00:00, optional). There is an 'Active scanning' checkbox.
- Wireless security:** Includes dropdown menus for 'Wireless protection' (None), 'Key source' (None), and 'Encryption type' (None).
- Quality of service:** Includes a 'Priority mechanism' dropdown (Diffsv), an 'IP QoS profiles' list box, and a checked 'Upstream diff serv tagging' checkbox.

At the bottom, there are 'Cancel' and 'Save' buttons.

2. Under **General**, configure settings as follows:

- Select **Enabled**.
- **Profile name:** The Profile name is just a friendly name used for display purposes. You can use the default value.
- **WLAN name (SSID):** This is the name of the wireless network that to which the M111 will attempt to connect. By default, the M111 uses the WLAN name **HP ProCurve**, which is the default name used by MSM APs. If you are using your own name, define the same name on both the M111 and the MSM AP.
- **AP's MAC address:** Leave this set to its default value.
- **Active scanning:** If the MSM AP to which the M111 will connect does not broadcast its WLAN name (SSID), you will have to enable this option for the M111 to successfully connect. By default, MSM APs broadcast their SSID, and this option does not need to be enabled.

3. Under **Wireless security**, select the **Authentication type** and **Encryption type** that are configured on the MSM AP to which the M111 will connect. You must define the same security settings on both the M111 and on the MSM AP. By default, MSM APs do not have security enabled.

Caution

It is strongly recommended that wireless security settings be enabled on the MSM AP and the M111 to safeguard traffic on the wireless network.

4. Select **Save**. The M111 automatically attempts to establish a wireless connection with the MSM AP. To check the status of the connection, select **Wireless > Overview**. The **Station State** should indicate **Associated**.

Once the wireless connection is established, the M111 is ready for operation, and can transport traffic from connected devices across the wireless link. In addition, access to the M111 management tool is now possible across the wireless link.

G. Connect the wired computers to the M111

Connect the wired computers to a switch/hub and plug the switch/hub into Port 1 on the M111. The computers should be configured to obtain their IP addresses automatically (DHCP client).

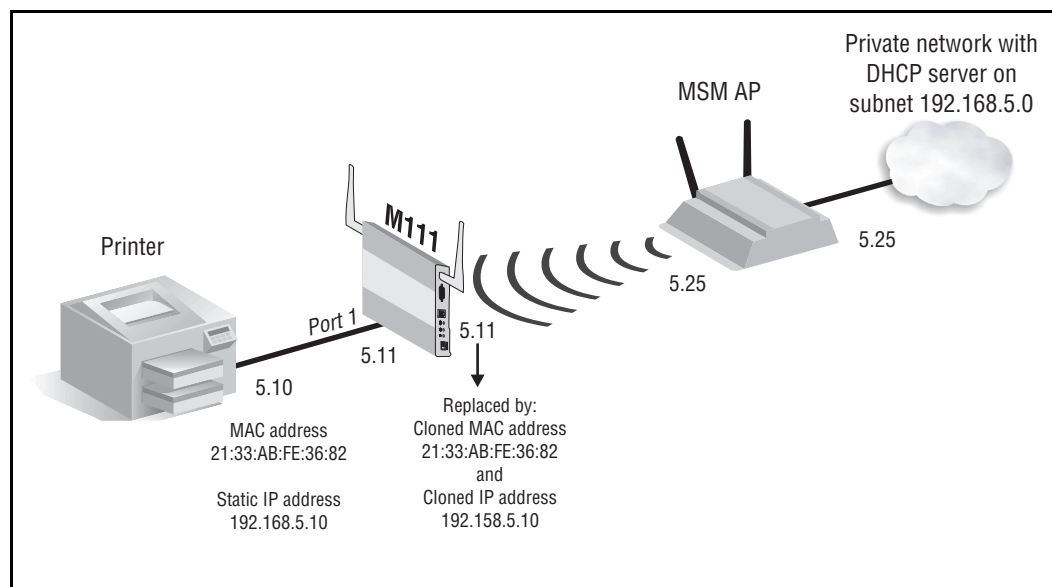
Start up a wired computer. It will receive an IP address from the DHCP server on the private network (for example, 192.168.5.26). The computer can now exchange data with the private network.

Scenario 2: Connecting a wired device using MAC address cloning

This scenario explains how to connect a single wired device to a wireless network using the M111's Ethernet MAC cloning feature.

Overview

In this scenario, a wired printer is converted to wireless access. Since the printer is already known by users on the network, the MAC cloning feature is used to preserve the printer's network identity. This enables users to maintain access to the printer without changing their settings.



This scenario assumes that:

- The M111 is in its factory-default state.
- A DHCP server is operating on the private network, assigning addresses on the subnet 192.168.5.0
- The MSM AP is operating in autonomous mode in its factory default configuration. (As such, it obtains an IP address of 5.25 from the DHCP server and creates a wireless network call *HP ProCurve*.) Install the MSM AP as described in its Quickstart.
- The printer is configured with a static IP address of 192.168.5.10.

Configuration procedure

The initial configuration steps for this scenario are the same as for Scenario 1. For each step see the instructions on the indicated page.

A. Configure your computer

See [Configure your computer on page 2-3](#).

B. Connect to the M111

See [Connect to the M111 on page 2-4](#).

C. Start the M111

See [Start the M111 on page 2-4](#).

D. Connect to the management tool and login

See [Connect to the management tool and login on page 2-4](#).

E. Set the M111 IP address

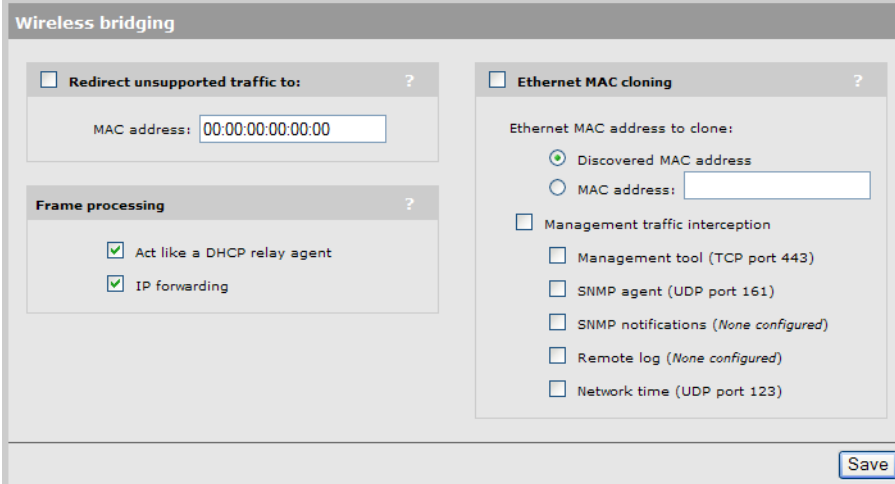
See [Set the M111 IP address on page 2-5](#).

F. Configure a station profile

See [Configure a station profile on page 2-6](#).

G. Configure MAC cloning options

1. Select **Wireless > Bridging**. The Wireless bridging page opens.



The image shows a 'Wireless bridging' configuration window. It has a title bar 'Wireless bridging' and a question mark icon. The window is divided into two main sections. The left section contains a checkbox 'Redirect unsupported traffic to:' with a question mark, a text field 'MAC address:' with the value '00:00:00:00:00:00', and a 'Frame processing' section with two checked checkboxes: 'Act like a DHCP relay agent' and 'IP forwarding'. The right section contains a checkbox 'Ethernet MAC cloning' with a question mark, a text field 'Ethernet MAC address to clone:' with two radio buttons: 'Discovered MAC address' (selected) and 'MAC address:' (empty), and a 'Management traffic interception' section with five unchecked checkboxes: 'Management tool (TCP port 443)', 'SNMP agent (UDP port 161)', 'SNMP notifications (None configured)', 'Remote log (None configured)', and 'Network time (UDP port 123)'. A 'Save' button is located at the bottom right of the window.

2. Select **Ethernet MAC cloning**, then configure the following options:

- Select the **Discovered MAC address** option. This option causes the M111 to take the MAC address of the wired device that is connected to Port 1 (the printer) and assign it to the Wireless port. Once this is done, the M111 re-associates with the MSM AP using the current station profile.
- A limitation of MAC cloning is that once the cloned MAC address is used to establish the wireless connection, the M111 itself is no longer accessible through the wireless port. To enable support for wireless access to the management tool, select **Management tool (TCP port 443)**. Note that to reach the management tool you must use the IP address assigned to the cloned device (5.10) and not the IP address assigned to the M111 (5.11). For information on the other interception options, see [*Setting up management traffic interception on page 3-32*](#).

3. Select **Save**.

H. Connect the wired device to the M111

Connect the printer to Port 1 on the M111 using a standard Ethernet cable.

The M111 will automatically re-connect to the wireless network using the IP address 192.168.5.10. Computers on the private network should now be able to send print jobs to the printer.

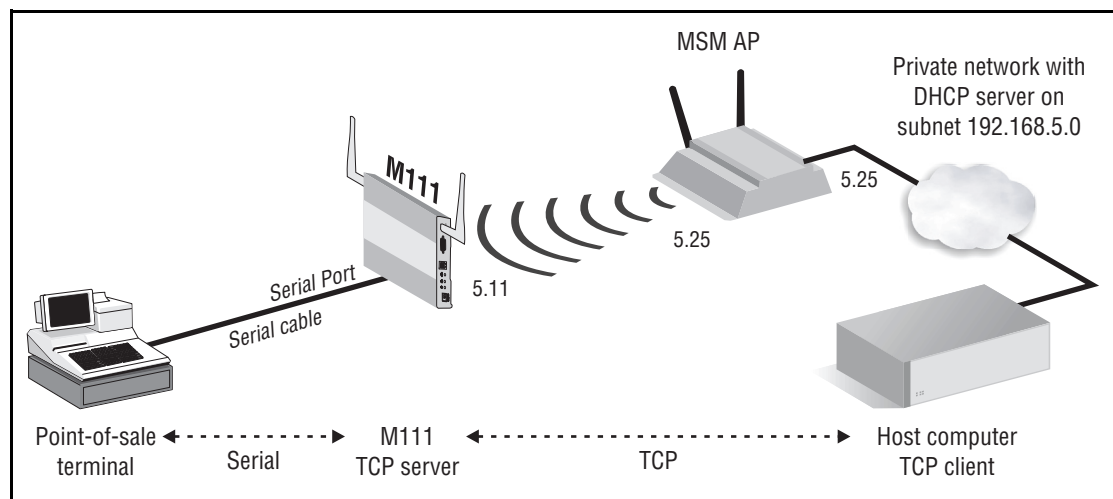
To reach the M111 management tool from the private network, use the address 192.168.5.10.

Scenario 3: Connecting a serial device to a wireless network

This scenario explains how to connect a serial device to a wireless network, enabling serial traffic to be sent to a remote host via TCP/IP.

Overview

In this scenario, the M111 enables a point-of-sale terminal to exchange traffic with a remote host. In addition to providing the connection to a wireless network, the M111 also converts traffic between serial and TCP/IP.



This scenario assumes that:

- The M111 is in its factory-default state.
- A DHCP server is operating on the private network, assigning addresses on the subnet 192.168.5.0
- The MSM AP is operating in autonomous mode in its factory default configuration. (As such, it obtains an IP address of 5.25 from the DHCP server and creates a wireless network call *HP ProCurve*.) Install the MSM AP as described in its Quickstart.
- The remote host is operating as a TCP client.

Configuration procedure

The initial configuration steps for this scenario are the same as for Scenario 1. For each step see the instructions on the indicated page.

A. Configure your computer

See [Configure your computer on page 2-3](#).

B. Connect to the M111

See [Connect to the M111 on page 2-4](#).

C. Start the M111

See [Start the M111 on page 2-4](#).

D. Connect to the management tool and login

See [Connect to the management tool and login on page 2-4](#).

E. Set the M111 IP address

See [Set the M111 IP address on page 2-5](#).

F. Configure a station profile

See [Configure a station profile on page 2-6](#).

G. Configure the serial connection

1. Connect the serial device to the serial port on the M111 using a straight-through serial cable. (For serial port specifications, see [Serial port connector on page 3-24](#).)
2. Select **Network > TCP Serial**. The **TCP to serial configuration** page opens.

☐ TCP to serial configuration

TCP connection ?

Mode: Server

TCP port: 8000

☐ Transmit timeout: 100

☐ Idle timeout: 30

Serial port ?

Data bits: 8

Parity bit: None

Stop bits: 1

Baud rate: 38400

Software flow control: None

Hardware flow control: None

Max receive buffer: 1024

TCP connection status ?

State	Not connected
Remote IP address:	
Connection time:	
Tx (kbytes):	
Rx (kbytes):	

Port control ?

☐ Drop wireless link when port 1 is connected

Save

3. Under **TCP connection**, set **Mode** to **Server**. In this scenario, the M111 acts as a TCP server and will listen for an incoming connection from the Host computer (TCP client). Leave the other parameters at their default settings. (For more information on these settings, see [TCP connection on page 3-25](#).)
4. Under **Serial port**, configure the serial parameters to match those of the serial device. This scenario assumes that the default settings are correct. For parameter descriptions see [Serial port on page 3-25](#).
5. Select **Save**. The M111 will listen for a connection request from the host.
6. Check the value of **State** under **TCP connection status**. When it changes to **Active**, it means that the TCP connection has been established with the host, and that the point-of-sale terminal can now exchange traffic with the host.

Getting started

Scenario 3: Connecting a serial device to a wireless network

Working with the M111

Contents

Management tool.....	3-3
Starting the management tool.....	3-3
Customizing management tool settings.....	3-4
IP address configuration	3-7
To configure IP addressing.....	3-8
Radio configuration	3-9
Wireless range	3-9
To configure the radio.....	3-10
Advanced wireless settings	3-13
Transmit power control	3-13
Using station profiles to establish a wireless link.....	3-13
To add or edit a station profile.....	3-15
Viewing APs in the neighborhood	3-18
Configuring Quality of Service (QoS).....	3-19
QoS settings in a station profile.....	3-20
Creating IP QoS profiles	3-22
To define an IP QoS profile	3-22
Connecting serial devices	3-23
Serial port connector	3-24
To connect a serial device	3-24
DNS configuration.....	3-27
Handling unsupported traffic	3-29
To forward unsupported traffic	3-29
IP forwarding	3-30

Cloning the address of a wired device.....	3-30
Enabling Ethernet MAC cloning.....	3-31
Wireless access to the M111 when MAC cloning is active	3-31
Using filters to restrict wireless traffic.....	3-33
Assigning a management address	3-34
To assign a management address	3-34
SNMP	3-35
Managing certificates.....	3-37
802.1X certificates	3-38
Certificate stores	3-39
Certificate usage	3-42
Configuration file management.....	3-44
Manual configuration file management	3-44
Scheduled operations.....	3-45
Software updates.....	3-46
Performing an immediate software update.....	3-47
Performing a scheduled update	3-47

Management tool

The management tool is a web-based interface to the M111 that provides easy access to all configuration and monitoring functions.

The computer used to connect to the management tool must:

- Have at least Microsoft Internet Explorer 7/8 or Firefox 3.x.
- Be able to establish an IP connection with the AP.

Starting the management tool

To launch the management tool, specify the following in the address bar of your browser:

`https://M111_IP_address`

The factory default IP address is 192.168.1.1.

About passwords

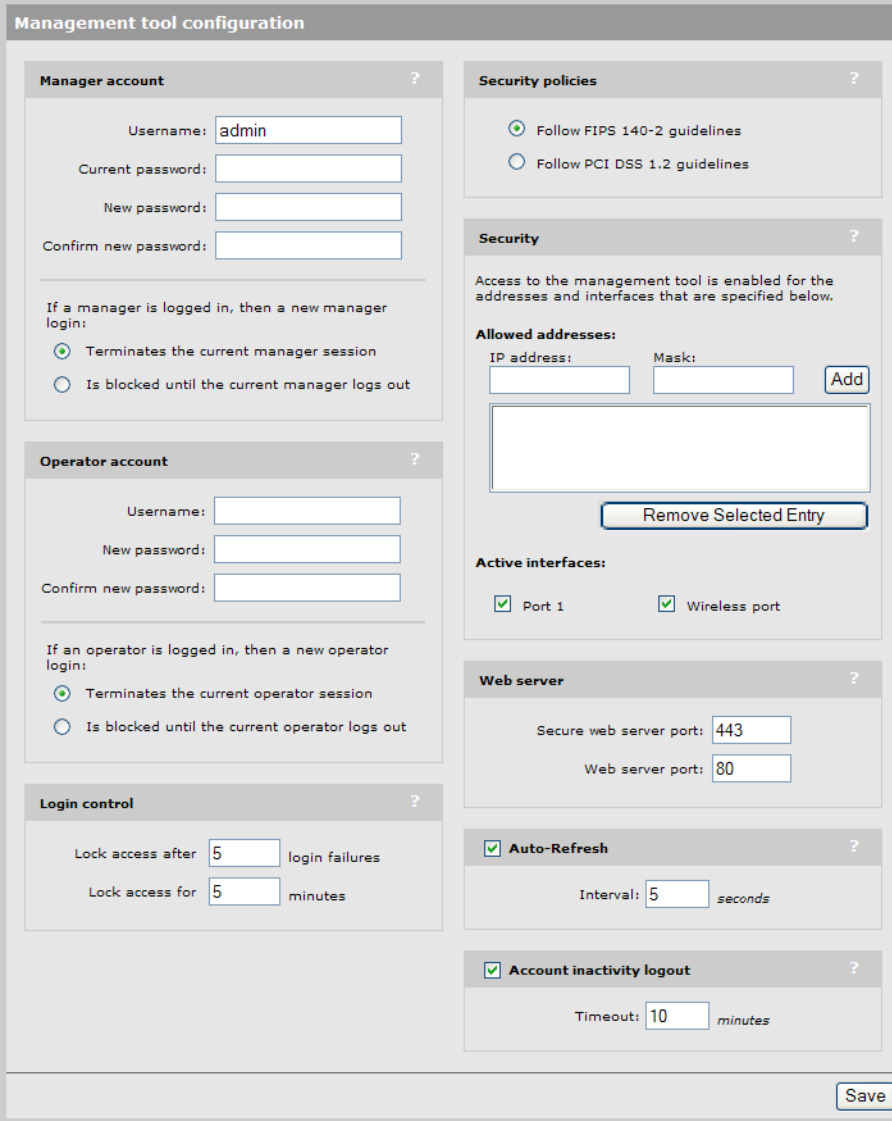
The default username and password is admin. New passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (") cannot be used. Passwords must also conform to the selected security policy as described in [Security policies on page 3-6](#).

For information on starting the management tool for the first time, see the *M111 Quickstart Guide* available at www.hp.com/go/procurve/manuals.

A security certificate warning is displayed the first time that you connect to the management tool. This is normal. Select whatever option is needed in your Web browser to continue to the management tool. The default certificate provided with the M111 will trigger a warning message on most browsers because it is self-signed. To remove this warning message, you must replace the default certificate. See [About certificate warnings on page 3-43](#).

Customizing management tool settings

To customize management tool settings, select **Management > Management tool**.



The image shows a web-based configuration interface for the Management tool. The title bar at the top reads "Management tool configuration". The interface is divided into several sections, each with a question mark icon in the top right corner:

- Manager account:** Contains fields for Username (pre-filled with "admin"), Current password, New password, and Confirm new password. Below these is a section titled "If a manager is logged in, then a new manager login:" with two radio button options: "Terminates the current manager session" (selected) and "Is blocked until the current manager logs out".
- Operator account:** Contains fields for Username, New password, and Confirm new password. Below these is a section titled "If an operator is logged in, then a new operator login:" with two radio button options: "Terminates the current operator session" (selected) and "Is blocked until the current operator logs out".
- Login control:** Contains two input fields for "Lock access after" and "Lock access for", both pre-filled with the number "5". The first is followed by "login failures" and the second by "minutes".
- Security policies:** Contains two radio button options: "Follow FIPS 140-2 guidelines" (selected) and "Follow PCI DSS 1.2 guidelines".
- Security:** Contains a text block stating "Access to the management tool is enabled for the addresses and interfaces that are specified below." Below this is a section titled "Allowed addresses:" with input fields for "IP address:" and "Mask:", followed by an "Add" button. There is a large empty text area below this, and a "Remove Selected Entry" button. Below the text area is a section titled "Active interfaces:" with two checked checkboxes: "Port 1" and "Wireless port".
- Web server:** Contains two input fields: "Secure web server port:" (pre-filled with "443") and "Web server port:" (pre-filled with "80").
- Auto-Refresh:** Contains a checked checkbox and an "Interval:" input field (pre-filled with "5") followed by the word "seconds".
- Account inactivity logout:** Contains a checked checkbox and a "Timeout:" input field (pre-filled with "10") followed by the word "minutes".

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

Manager and Operator accounts

Two types of administrative accounts are defined: manager and operator.

- The manager account provides full management tool rights.
- The operator account provides read-only rights plus the ability to perform troubleshooting.

Only one administrative account can be logged in at any given time. Options are provided to control what happens when an administrator attempts to log in while another administrator (or the same administrator in a different session) is already logged in. In every case, the manager's rights supersede those of an operator.

The following options can be used to prevent the management tool from being locked by an idle manager or operator:

- **Terminates the current manager session:** When enabled, an active manager or operator session will be terminated by the login of another manager. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.
- **Is blocked until the current manager logs out:** When enabled, access to the management tool is blocked until an existing manager logs out or is automatically logged out due to an idle session.

An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.

- **Terminates the current operator session:** When enabled, an active operator session will be terminated by the login of another operator. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.

Operator access to the management tool is blocked if a manager is logged in. An active manager session cannot be terminated by the login of an operator.

An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.

- **Login control:** If login to the management tool fails five times in a row (bad username and/or password), login privileges are blocked for five minutes. Once five minutes expires, login privileges are once again enabled. However, if the next login attempt fails, privileges are again suspended for five minutes. This cycle continues until a valid login occurs. You can configure the number of failures and the timeout.
- **Account inactivity logout:** By default, if a connection to the management tool remains idle for more than ten minutes, the connection is terminated. You can configure the timeout.

Caution

If you forget the manager password, the only way to access the **management tool** is to reset the M111 to factory default settings. For information see [Appendix B: Resetting to factory defaults](#).

Passwords

Passwords must be 6 to 16 printable ASCII characters in length with at least 4 different characters. Passwords are case sensitive. Space characters and double quotes (") cannot be used. Passwords must also conform to the selected security policy as described below.

Security policies

Security policies affect both manager and operator accounts. Select from one of the following options:

- **Follow FIPS 140-2 guidelines:** When selected, implements the following requirements from the FIPS 140-2 guidelines:
 - Passwords must be at least six characters long.
 - Passwords must contain at least four different characters.

For more information on these guidelines, refer to the *Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules*.

- **Follow PCI DSS 1.2 guidelines:** When selected, implements the following requirements from the PCI DSS 1.2 guidelines:
 - Passwords must be at least seven characters long.
 - Passwords must contain both numeric and alphabetic characters.
 - The settings under **Login control** must be configured as follows:
 - **Lock access after *nn* login failures** must be set to 6 or less.
 - **Lock access for *nn* minutes** must be set to 30 minutes or more.
 - The settings under **Account inactivity logout** must be configured as follows:
 - **Timeout** must be set to 15 minutes or less.
- For more information on these guidelines, refer to the *Payment Card Industry Data Security Standard v1.2* document.

Security

The management tool is protected by the following security features:

- **Allowed addresses:** You can configure a list of subnets from which access to the management tool is permitted.
- **Active interfaces:** You can enable or disable access to the management tool for each of the following:
 - Port 1
 - Wireless port

Web server

You can also configure the web server ports from which access to the management tool is permitted.

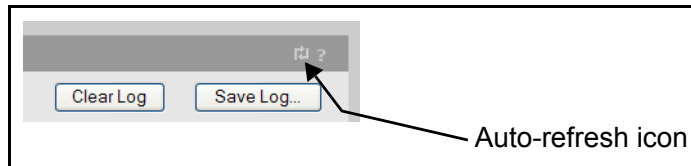
- **Secure web server port:** Specify a port number for the M111 to use to provide secure HTTPS access to the management tool. Default is 443.

Before logging on to the management tool, you must accept a security certificate. The default certificate provided with the M111 will trigger a warning message on most browsers because it is self-signed. To remove this warning message, you must replace the default certificate. See [About certificate warnings on page 3-43](#).

- **Web server port:** Specify a port number for the M111 to use to provide standard HTTP access to the management tool. These connections are met with a warning, and the browser is redirected to the secure web server port. Default is 80.

Auto-refresh

This option controls how often the M111 updates the information in group boxes that show the auto-refresh icon in their title bar. Under **Interval**, specify the number of seconds between refreshes.



IP address configuration

IP address settings are configured using the Bridge port. This is a logical port that handles the addressing settings for both Port 1 and the Wireless port.

By default, the M111 is configured to operate as a DHCP client on both ports. If no DHCP server is found on either port, the M111 assigns the address 192.168.1.1 to Port 1 and the Wireless port.

Note

Make sure that only one DHCP server is accessible via either Port 1 or the Wireless port. If a DHCP server is accessible via both ports, the M111 will randomly choose one of the servers.

When operating as a DHCP client, it is possible that the address assigned to the M111 will change whenever the DHCP address lease is renewed. This will disrupt access to the management tool, as you must determine the new address (likely by querying the DHCP server).

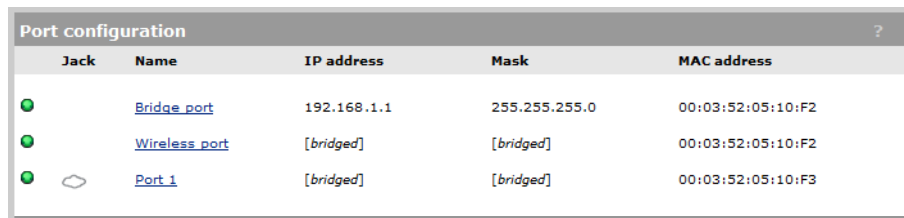
There are several solutions to this problem:


- Pre-configure the DHCP server on the network to assign a specific IP address to the M111. To do this you need to specify the M111 MAC address and a reserved IP address on the DHCP server. The M111 MAC address is printed on the M111 label identified as **Wireless Base MAC**, or listed on the management tool **Home** or **Login** page as **Wireless MAC address**.
- Assign a static IP address to the M111 as explained in the next section [To configure IP addressing](#). The address must be on the same subnet as the MSM AP to which the M111 will connect.
- Define a management IP address. See [To assign a management address on page 3-34](#).

The M111 provides MAC address translation for all devices connected to Port 1 as their traffic is forwarded across the wireless link. This enables up to 20 Ethernet devices to share the wireless link, yet at the same time have their own unique IP addresses.

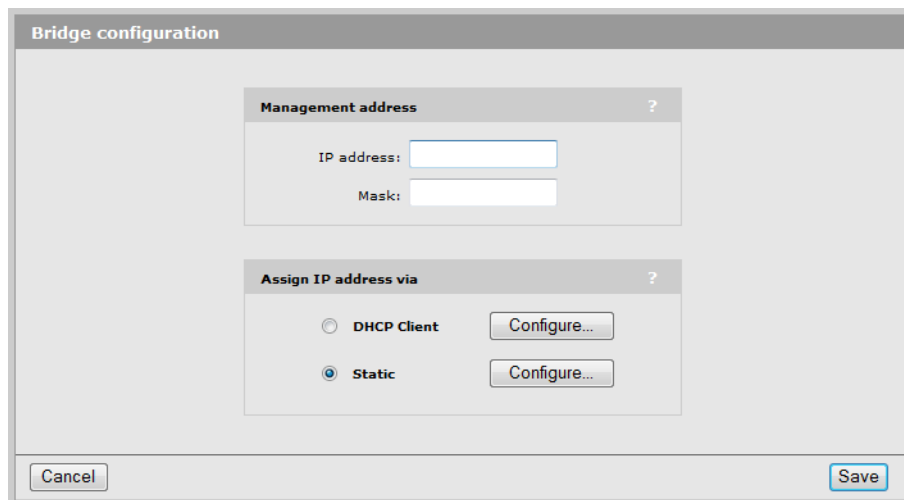
To configure IP addressing

1. Select **Network > Ports**.



Port configuration ?				
Jack	Name	IP address	Mask	MAC address
●	Bridge port	192.168.1.1	255.255.255.0	00:03:52:05:10:F2
●	Wireless port	[bridged]	[bridged]	00:03:52:05:10:F2
●	 Port 1	[bridged]	[bridged]	00:03:52:05:10:F3

2. Select **Bridge port** in the table.



Bridge configuration

Management address ?

IP address:

Mask:

Assign IP address via ?

☐ DHCP Client

☒ Static

3. Under **Assign IP address via**, select the option you want to use, and select **Configure**.
4. Specify your settings and select **Save**, and then from the **Bridge configuration** page select **Save** again.

5. When you save the IP address change, the connection to the management tool will be lost. To-reconnect, you need to re-launch the M111 management tool by browsing to:
https://new IP address assigned to the M111. (For this to work, your computer must be on the same subnet as the M111.)

Radio configuration

The M111 radio is an RF direct sequence spread spectrum (DSSS) device that operates in the Industrial, Scientific, Medical (ISM) frequency spectrum. It provides the link between the M111 and a wireless access point.

Wireless range

At high power the M111 can communicate with access points within a wireless cell that has a diameter of up to 300 feet (100 meters).

The following factors can affect wireless performance:

- **Radio power:** More radio power means better signal quality and the ability to create bigger wireless cells. However, cell size should generally not exceed the range of transmission supported by client stations. If it does, wireless clients (like the M111) will be able to receive signals from the access point, but may not be able to reply, rendering the connection useless.

Governmental regulations in different parts of the world determine the maximum power output of the M111 radio.

- **Antenna configuration:** Antennas play a large role in determining the shape of the wireless cell and transmission distance. Consult the specifications for the antennas you are using to determine how they affect wireless coverage.
- **Interference:** Interference is caused by other access points or devices (cordless phones, microwaves) that operate in the same 2.4 GHz frequency band as the M111 when it is set to b or g modes. Such interference can substantially affect throughput.
- **Physical characteristics of the location:** Radio waves have a limited ability to penetrate metal. The steel reinforcing found in concrete walls and floors may block transmissions or reduce signal quality. However, the M111 is able to transmit through wood or plaster walls and closed windows. To maximize the range of the wireless cell, the M111 is best installed in an open area with as few obstructions as possible.

To configure the radio

Select **Wireless > Radio**. This opens the Radio configuration page:

The screenshot shows the 'Radio configuration' window. It has a title bar 'Radio configuration' and a sub-header 'Radio'. The 'Wireless mode' is set to 'Auto'. Below it, 'Currently: Channel 6, 2.437GHz' is displayed. There is a checkbox for 'Restrict channels' which is currently unchecked. To its right, a list of channels is shown: 'Channel 1, 2.412GHz', 'Channel 2, 2.417GHz', and 'Channel 3, 2.422GHz'. Below this, 'Antenna selection' is set to 'Diversity (both antennas)'. There are several checked options: 'Fast roaming' with a threshold of 12 dB, 'Fast roaming delta' with a threshold of 14 dB, 'Minimum SNR' with a threshold of 5 dB, 'Scan channel delay' of 200 msec, 'Fast scan channel delay' of 30 msec, and 'Roaming persistence' of 400 msec. There is an expandable section 'Advanced wireless settings' which is currently collapsed. Below it, 'RTS threshold' is set to an empty field. The 'Transmit power control' section is expanded, showing 'Maximum available output power' checked, with a value of 18 dBm = 100 % of max output power. A 'Save' button is at the bottom right.

Configure parameter settings as follows:

Wireless mode

Select the transmission speed and frequency band. The permitted frequencies and channels are determined by the country of operation, and may include:

- Auto: The M111 automatically selects the correct frequency band (a, b, g) depending on the AP it is connecting to.
- 802.11b: Up to 11 Mbps in the 2.4 GHz frequency band.
- 802.11b + 802.11g: Up to 11 and 54 Mbps in the 2.4 GHz frequency band.
- 802.11g: Up to 54 Mbps in the 2.4 GHz frequency band.
- 802.11a: Up to 54 Mbps in the 5 GHz frequency band.

Restrict channels to

Select the channels that the M111 will scan. By limiting the channels that are scanned, the speed at which the M111 switches to a new AP can be increased.

To select more than one channel, hold down the CTRL key as you select the channel names.

Antenna selection

Select the antenna on which the radio will transmit and receive.

If a single antenna is used, it can be connected to either Main or Aux.

- **Diversity:** In this mode both antennas are used to transmit and receive. The M111 supports both transmit and receive diversity.
 - **Transmit diversity:** For a given connection, the M111 always transmits on the antenna it receives. If transmission fails, the M111 automatically switches antennas and retries.
 - **Receive diversity:** In 802.11b, the M111 does selection diversity, which means selecting the antenna used to receive based on the SNR calculated while receiving the preamble, on a per frame basis.

For 802.11a and 802.11g, including mixed 802.11b and 802.11g, the receiver switches antennas when the signal quality goes below a certain threshold.

- **Main antenna:** Select this option to use the Main antenna to transmit only.
- **Auxiliary antenna:** Select this option to use the Auxiliary antenna to transmit only.

Fast roaming threshold

Fast roaming delta threshold

These two options function in a similar manner. The only difference is how they determine when roaming will occur. Both options are used when the M111 is mobile and must switch between APs without causing a degradation in wireless service.

Fast roaming enables the M111 to quickly switch between two APs with the same SSID operating on the same channel (frequency). Without fast roaming, the M111 may take as much as 5 seconds to determine that the AP it is connected to is no longer available or out of range. Once this occurs, the M111 scans for a new connection according to the settings on the **Wireless > Station profiles** page.

When fast roaming is enabled, the M111 continuously monitors the SNR (signal-to-noise ratio) of all wireless beacons with the same SSID and frequency as that of the current connection to determine if it should roam to a new AP. This decision is made as follows:

- **Fast roaming threshold:** The M111 will only switch to a new AP if the SNR of the new AP is greater than the setting for **Fast roaming threshold** (for the number of beacons specified for **Fast roaming threshold count**) and the SNR of the current AP is less than the **Fast roaming threshold**. For example, if set to 10, then the M111 will only switch to a new AP if its SNR is greater than 10 dB and the AP it is currently connected to has an SNR less than 10 dB. Once switched, Roaming persistence (if enabled) takes effect.
- **Fast roaming delta threshold:** If the difference in SNR between the current and new AP is greater than the **Fast roaming delta threshold** (for the number of beacons specified for **Fast roaming threshold count**), then the M111 automatically switches over to the new AP. Once switched, Roaming persistence (if enabled) takes effect.

If both options are enabled at the same time, whichever option is triggered first takes precedence.

SNR is expressed in decibels (dB). The higher the number the stronger the signal.

Note

If 802.1X/ WPA/WPA2 is enabled, this can add an unpredictable delay based on network topology. For example, if a RADIUS server is being used for authentication as opposed to preshared keys.

Fast roaming threshold count

Sets the number of contiguous beacons that must be received satisfying the **Fast roaming threshold** for the M111 to switch over to a new AP.

Minimum SNR threshold

Use this parameter to speed up roaming between two APs with the same SSID and operating on **different** channels (frequencies)

When the value of SNR falls below the set threshold, the M111:

- Disassociates from the current AP (it does not wait until the connection is lost).
- Performs a wireless scan.
- Selects a new AP with which to AP to connect.

SNR is expressed in decibels (dB). The higher the number the stronger the signal.

Signal to noise ration (SNR) Indicates the relative strength of radio signals versus radio interference (noise) in the radio signal path. In most environments, SNR is a good indicator for the quality of the radio link. A higher SNR value means a better quality radio link.

Scan channel delay

(Only applies when connecting using a station profile for which active scanning is disabled.)

Sets the length of time in milliseconds that the M111 will scan a channel. By default, this is set to 200 milliseconds which allows enough time for a probe/request/response exchange.

Fast scan channel delay

(Only applies when connecting using an active station profile)

Sets the length of time (in milliseconds) that the M111 will scan a channel. By default, this is set to 30 milliseconds which is much less than the standard beacon interval of 100 milliseconds used by most APs.

Roaming persistence

Sets the amount of time (in milliseconds) that the M111 waits before it uses any of the following roaming features: fast roaming threshold, fast roaming delta threshold, or minimum SNR threshold.

Advanced wireless settings

RTS threshold

Use this parameter to control collisions on the wireless link that can reduce throughput. If the **Status > Wireless** page shows increasing values for **Tx multiple retry frames** or **Tx single retry frames**, adjusting this value may help to reduce the errors. Start with a value of 1024 and then decrease to 512 until errors are reduced or eliminated. Note that using a small value for RTS threshold can affect throughput. Range: 128 to 1540.

If a packet is larger than the threshold, the M111 will hold it and issue a request to send (RTS) message to the AP. Only when the AP replies with a clear to send (CTS) message will the M111 send the packet. Packets smaller than the threshold are transmitted without this handshake.

Transmit power control

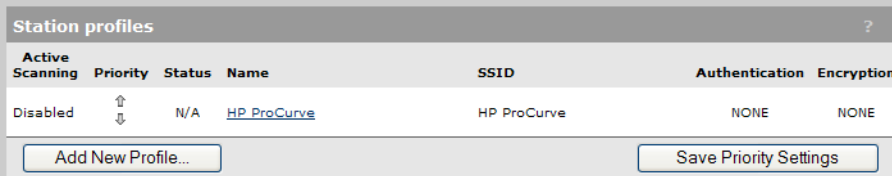
Sets the transmission power of the wireless radio. Adjustments to the transmit power control may be required to avoid interference between devices. You can specify transmission power by selecting a percentage of the maximum available power or by specifying **Maximum available output power** in dBm.

The actual transmit power used may be less than the value specified. The M111 determines the power to be used based on the country of operation and the wireless mode.

Using station profiles to establish a wireless link

A station profile contains the configuration settings that the M111 uses to establish a wireless connection with an AP. The M111 supports multiple station profiles, enabling it to automatically connect with different wireless networks.

Station profiles are defined on the **Wireless > Station profiles** page. Initially, this page contains the default profile which is named **HP ProCurve**.



Station profiles							
Active Scanning	Priority	Status	Name	SSID	Authentication	Encryption	
Disabled	↑ ↓	N/A	HP ProCurve	HP ProCurve	NONE	NONE	
Add New Profile...				Save Priority Settings			

The profile list is split into two sections according to the setting of the **Active Scanning** option for each profile. Station profiles that have the Active Scanning option enabled have priority over profiles that do not have this option enabled.

Working with the M111

Using station profiles to establish a wireless link

Each profile contains the definitions for a wireless connection. The M111 uses the profile definitions in the following order when it attempts to find an AP with which to establish a wireless link:

1. First, all profiles with **Active scanning enabled** are sequentially checked in the order that they are listed, from top to bottom. The M111 actively sends probe requests to the SSID defined in each profile. (Profiles with a status of “N/A” are skipped.) See [Active scanning on page 3-15](#).
2. Next, all profiles in the table are sequentially checked in the order that they are listed, from top to bottom. The M111 uses information collected by passively scanning the wireless neighborhood to find a match for the SSID defined in each profile.

In the following example, profiles are checked in the following order: Office-1, Office-2, Office-3, then Office-1, Office-2, Office-3, Office-21, Office-22, Office-23.

Station profiles							?
Active Scanning	Priority	Status	Name	SSID	Authentication	Encryption	
Enabled	↑ ↓	●	Office-1	Office 1	NONE	NONE	
Enabled	↑ ↓	●	Office-2	Office 2	PSK	TKIP	
Enabled	↑ ↓	●	Office-3	Office 3	NONE	NONE	
Disabled	↑ ↓	●	Office-21	Office 21	NONE	WEP	
Disabled	↑ ↓	●	Office-22	Office 22	NONE	WEP	
Disabled	↑ ↓	●	Office-33	Office 23	NONE	NONE	
Add New Profile...			Save Priority Settings				

Change profile priority by clicking the up/down arrows in the **Priority** column.

To add or edit a station profile

Select **Wireless > Station profiles** and do the following:

- To add a new profile, select **Add New Profile**.
- To edit a profile, select its name in the list.

In either case, the Station profiles - Add/Edit Station profile page opens.

The screenshot shows the 'Station profiles - Add/Edit Station profile' configuration window. It is divided into three main sections: General, Wireless security, and Quality of service. The General section has radio buttons for 'Enabled' (selected) and 'Disabled'. It includes text boxes for 'Profile name' (HP ProCurve), 'WLAN name (SSID)' (HP ProCurve), and 'AP's MAC address' (00:00:00:00:00:00, optional). There is a checkbox for 'Active scanning'. The Wireless security section has dropdown menus for 'Wireless protection' (None), 'Key source' (None), and 'Encryption type' (None). The Quality of service section has a dropdown for 'Priority mechanism' (Diffserv) and a list box for 'IP QoS profiles'. There is a checkbox for 'Upstream diff serv tagging' which is checked. At the bottom are 'Cancel' and 'Save' buttons.

Configure parameter settings as follows:

General

Profile name

Specify a name to uniquely identify the profile.

WLAN name (SSID)

Specify the SSID of the wireless network to which this profile will connect.

AP's MAC address

Specify the MAC address of the AP (BSSID) to which this profile will connect.

Active scanning

In active scanning mode, the M111 sends out *probe request* frames in an attempt to solicit responses from APs that are within range. This enables the M111 to establish a connection with an AP that does not broadcast an SSID.

Some countries prohibit active scanning on some channels. In these countries, probe requests are not sent on prohibited channels.

When this option is enabled, this profile takes priority over profiles without active scanning. The M111 attempts to connect with active profiles first before trying other profiles in the list.

Wireless security

Wireless protection

The M111 supports several authentication and encryption options for protection of wireless transmissions. To make use of these options, the remote AP to which the M111 connects must be configured appropriately. The options displayed are dependent on the **Wireless protection** option selected.

Note

Options that need support from a RADIUS server require that the connection to the RADIUS server is configured on the remote AP and not on the M111.

The following wireless protection options are available:

- **None:** No authentication.
- **802.1X:** This option enables support for 802.1X with or without WEP. Must be used with a RADIUS server.
- **WPA:** This option enables support for WPA with TKIP, supporting either a RADIUS server or a pre-shared key (PSK).
- **WPA2:** This option enables support for WPA2 with AES/CCMP, supporting either a RADIUS server or a pre-shared key (PSK).

Key source

- **PSK:** Only available if **Wireless protection** is set to WPA or WPA2.
 - **Key:** The M111 uses the key you specify in the this field to generate the TKIP or AES/CCMP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as the RADIUS option. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (") should not be used.
- **RADIUS:** The M111 obtains the Microsoft Point-to-Point Encryption (MPPE) keys from a RADIUS server (via the remote AP). This is a dynamic key that changes each time the M111 logs in and is authenticated by the AP. The MPPE key is used to generate the WEP, TKIP or AES/CCMP keys that encrypt the wireless data stream.

EAP method

Select the Extensible Authentication Protocol (EAP) authentication method the M111 will use when connecting to the AP.

- **PEAP version 0 / PEAP version 1:** These two options have the same configuration settings. PEAP version 0 only supports MS-CHAP V2 as the inner EAP protocol. PEAP version 1 only supports EAP-GTC (generic token card) as an inner EAP protocol. Both require the use of a RADIUS server by the remote AP.

- **Username:** Specify the username assigned to the M111 on the remote AP's RADIUS server.
- **Password:** Specify the password assigned to the M111 on the remote AP's RADIUS server.
- **Anonymous (Optional):** Specify the outer authentication username for the TLS tunnel.
- **TLS:** Requires that a TLS certificate is installed on the M111 and that the remote AP provides support for authentication via a RADIUS server.
 - **TLS identity:** Specify the name that was used when creating the TLS certificate.
 - **TLS certificate:** Select the Transport Layer Security certificate to send to the AP for authentication. (The certificate must first be installed on the **Security > 802.1X certificates** page before you can select it.)
- **TTLS:** This option requires that the remote AP provides support for authentication via a RADIUS server. Only supports MS-CHAP V2 as the inner EAP protocol.
 - **Username:** Specify the username assigned to the M111 on the remote AP's RADIUS server.
 - **Password:** Specify the password assigned to the M111 on the remote AP's RADIUS server.
 - **Anonymous:** Specify the outer authentication username for the TLS tunnel.
- **FAST:** EAP-FAST uses an encrypted tunnel to distribute preshared keys.
 - **Username:** Specify the username assigned to the M111 on the remote AP's RADIUS server.
 - **Password:** Specify the password assigned to the M111 on the remote AP's RADIUS server.
 - **Anonymous:** Specify the outer authentication username for the TLS tunnel.

Validate server certificate: Select this box to validate the RADIUS server's certificate before establishing the connection. Used for TLS, TTLS, and PEAP. Requires that an **802.1X Trusted CA certificate** is installed on the **Security > 802.1X certificates** page.

Common name: Use this field to test the contents of the Distinguished Name contained in the RADIUS server's X.509 certificate. If the common name you specify does not match the Distinguished name in the certificate, then the wireless connection is not established.

To facilitate matching, standard regular expressions can be used in the common name. For example:

Expression	Matches
certificate[1-3]	certificate1 certificate2 certificate3
.*certificate	Matches certificate with any number of characters in front of it. For example: ap1certificate or ap2certificate .

Use the backslash (\) as an escape character if you need to match a period (.) or other characters that have meaning in a regular expression. For example, to match any number of periods, specify the following:

.*\

Encryption type

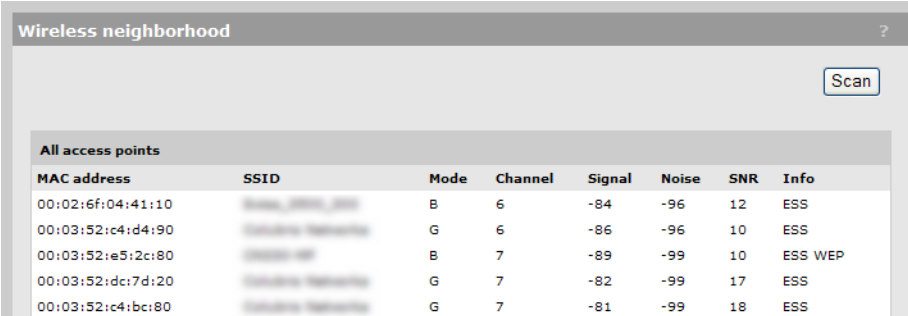
- **WEP:** Uses Wired Equivalent Privacy to secure traffic on the wireless link.
- **TKIP:** Uses Temporal Key Integrity Protocol encryption to secure traffic on the wireless link.
- **AES:** Advanced Encryption Standard is used by the U.S. Government and defined by the National Institute of Standards and Technology (NIST). This is the most secure method to secure traffic on the wireless link. It uses AES with CCMP encryption.

Quality of service

See [Configuring Quality of Service \(QoS\) on page 3-19](#)

Viewing APs in the neighborhood

The **Wireless > Neighborhood** page provides a list of all APs that are operating nearby. Select **Scan** when the M111 is not associated to an AP to refresh the list.



The screenshot shows a web interface titled "Wireless neighborhood" with a "Scan" button. Below it is a table titled "All access points" with columns: MAC address, SSID, Mode, Channel, Signal, Noise, SNR, and Info. The table lists five access points with their respective details.

All access points							
MAC address	SSID	Mode	Channel	Signal	Noise	SNR	Info
00:02:6f:04:41:10	Wireless_M111	B	6	-84	-96	12	ESS
00:03:52:c4:d4:90	Wireless_M111	G	6	-86	-96	10	ESS
00:03:52:e5:2c:80	Wireless_M111	B	7	-89	-99	10	ESS WEP
00:03:52:dc:7d:20	Wireless_M111	G	7	-82	-99	17	ESS
00:03:52:c4:bc:80	Wireless_M111	G	7	-81	-99	18	ESS

Field descriptions

- **MAC address:** MAC address of the AP (Also called the BSSID).
- **SSID:** SSID assigned to the AP.
- **Mode:** Indicates the operating mode of the AP: A, B, or G.
- **Channel:** Channel the AP is operating on.
- **Signal:** Signal strength.
- **Noise:** Amount of noise.
- **SNR:** Signal to noise ratio. Signal to noise ratio (SNR) Indicates the relative strength of radio signals versus radio interference (noise) in the radio signal path. In most environments, SNR is a good indicator for the quality of the radio link. A higher SNR value means a better quality radio link.
- **Info:** Additional information about the AP, such as:
 - **WEP:** Some type of security (like WEP) is enabled on the AP.
 - **ESS:** Operating in AP mode. Also lists security being used if enabled (WEP, WPA).
 - **IBSS:** Operating in Ad-Hoc mode.
 - **WPA:** WPA is enabled on the AP.
 - **WPA2:** WPA2 is enabled on the AP.
 - **WPA*:** WPA and WPA2 are both enabled on the AP.

Configuring Quality of Service (QoS)

The quality of service (QoS) feature provides a number of different mechanisms to prioritize traffic sent on the wireless link. This is useful when the M111 handles traffic from multiple devices (or multiple applications on a single device), that have different data flow requirements.

The QoS feature defines four traffic queues based on the Wi-Fi Multimedia (WMM) access categories. In order of priority, these queues are:

Queue	WMM access category	Typically used for
1	AC_VO	Voice traffic
2	AC_VI	Video traffic
3	AC_BE	Best effort data traffic
4	AC_BK	Background data traffic

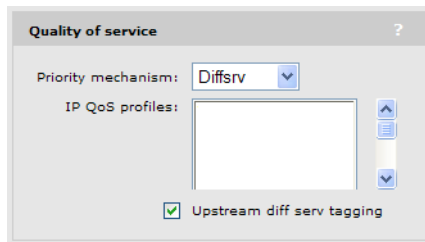
Outgoing wireless traffic on the wireless link is assigned to a queue based on the selected priority mechanism. Traffic delivery is based on strict priority (per the WMM standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

Regardless of the priority mechanism that is selected:

- Traffic that cannot be classified by a priority mechanism is assigned to queue 3.
- SVP (SpectralLink Voice Protocol) traffic is always assigned to queue 1, except if you select the Very-high, high, normal, or low priority mechanisms, in which case SVP traffic is assigned to the configured queue.

QoS settings in a station profile

QoS settings are defined in a station profile as follows:



Priority mechanisms

Priority mechanisms are used to classify traffic on a station profile and assign it to the appropriate queue.

The following mechanisms are available:

802.1p

This mechanism classifies traffic based on the value of the VLAN priority field present within the VLAN header.

Queue	802.1p VLAN priority field value
1	6,7
2	4,5
3	0,2
4	1,3

Very-high, high, normal, low priority

This mechanism is unique to the M111. It enables you to assign a single priority level to all traffic on a station profile. If you enable one of these priority mechanisms, it takes precedence regardless of the existing priority assigned to the traffic when it is received.

Queue	Priority value
1	Very-high
2	High
3	Normal
4	Low

Differentiated Services (DiffServ)

This mechanism classifies traffic based on the value of the Differentiated Services (DS) codepoint field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

Queue	DiffServ DS codepoint value
1	111000 (Network control) 110000 (Internetwork control)
2	101000 (Critical) 100000 (Flash override)
3	011000 (Flash) 000100 (Routine)
4	010000 (Immediate) 001000 (Priority)

TOS

This mechanism classifies traffic based on value of the TOS (Type of Service) field in an IP packet header.

Queue	TOS Type of Service field value
1	0x30, 0xE0, 0x88, 0xB8
2	0x28, 0xA0
3	0x08, 0x20
4	All other TOS traffic

IP QoS

This option lets you assign traffic to the queues based on the criteria in one or more IP QoS profiles. Each profile lets you target traffic on specific ports or using specific protocols. For more information, see [Creating IP QoS profiles on page 3-22](#).

Disabled

When QoS traffic prioritization is disabled, all traffic is sent to queue 3.

Upstream DiffServ tagging

Enable this option to have the M111 apply differentiated services marking to upstream traffic.

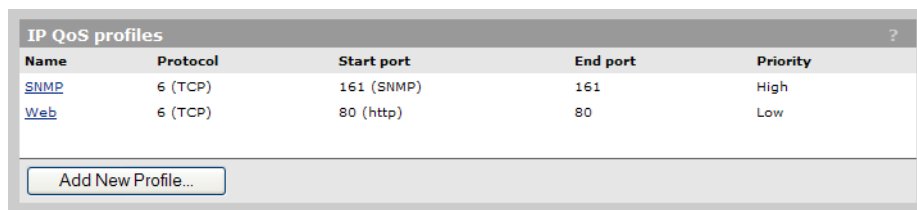
Layer 3 upstream marking ensures end-to-end quality of service in your network. Data originating on the wireless network can now be carried throughout the network (wireless *and* wired) with a consistent quality of service and priority. This feature is enabled by default.

Creating IP QoS profiles

IP QoS profiles enable you to define custom rules for classifying traffic based on port and protocol values. IP QoS profiles can be assigned to a station profile when the **Priority mechanism** is set to **IP QoS**.

To define an IP QoS profile

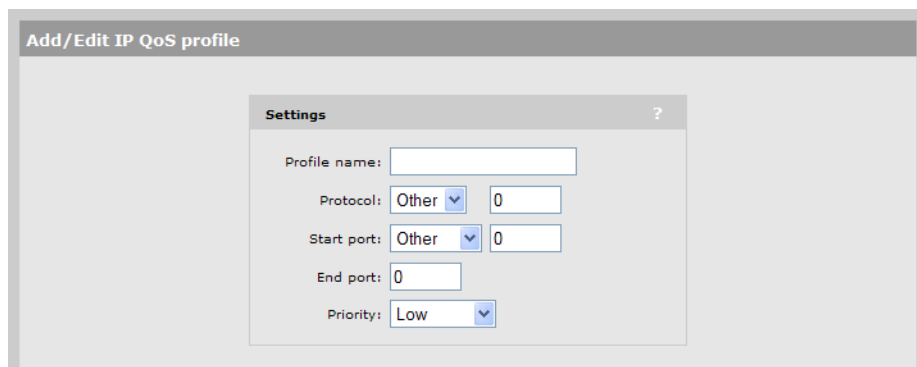
1. Select **Network > IP QoS**. Initially, no profiles are defined.



Name	Protocol	Start port	End port	Priority
SNMP	6 (TCP)	161 (SNMP)	161	High
Web	6 (TCP)	80 (http)	80	Low

[Add New Profile...](#)

2. Select **Add New Profile**.



Add/Edit IP QoS profile

Settings

Profile name:

Protocol: Other 0

Start port: Other 0

End port: 0

Priority: Low

3. Configure parameter settings as follows:

Settings

Profile name

Specify a unique name to identify the profile.

Protocol

Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually. You can find IANA-assigned protocol numbers at <http://www.iana.org>.

Start port/ End port

Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both **Start port** and **End port**. Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually.

Note

To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0**.

Priority

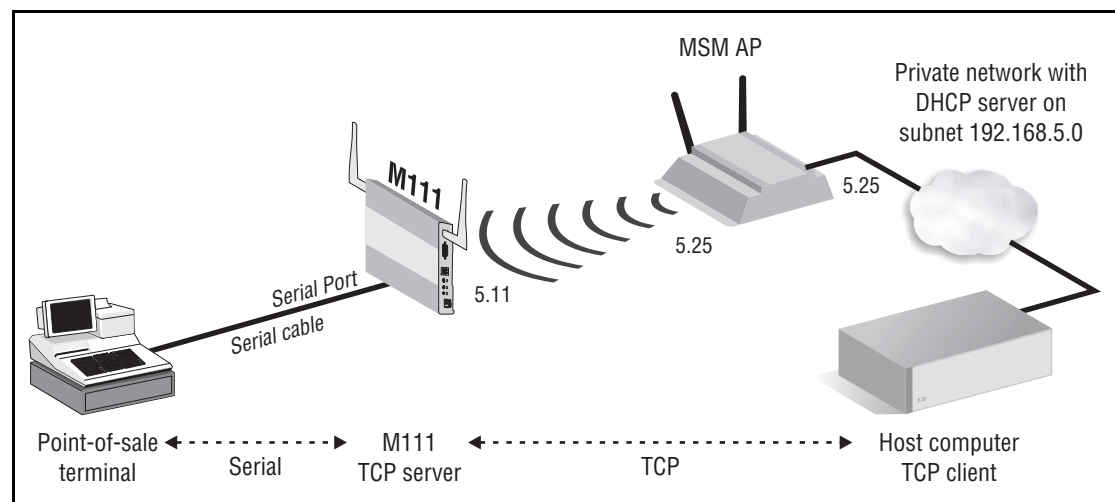
Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

Note

It is strongly recommended that you reserve **Very high** priority for voice applications.

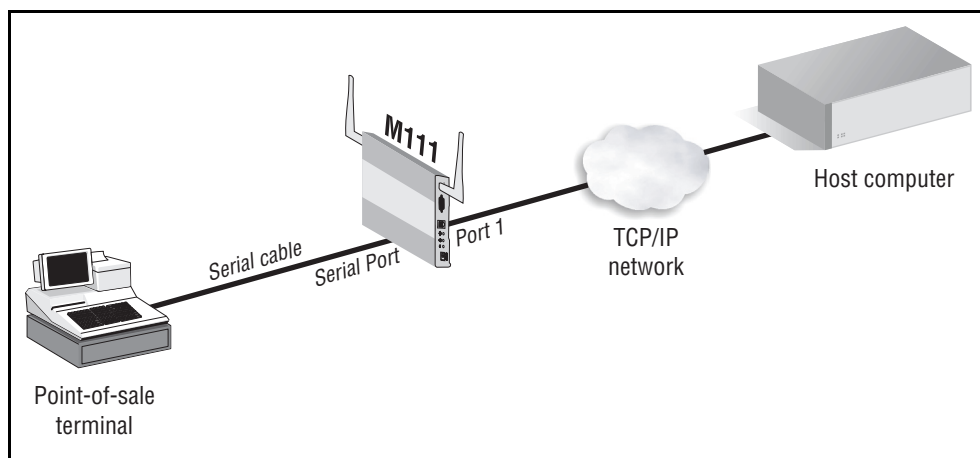
Connecting serial devices

The Serial to TCP feature enables traffic from a local serial device to be sent over a TCP/IP network. For example, the following scenario shows serial traffic from a point-of-sale terminal being forwarded to a host computer via a wireless link to a TCP/IP network.



For complete instructions on how to configure this scenario, see [Scenario 3: Connecting a serial device to a wireless network on page 2-11](#).

The M111 can also connect to a TCP host via Port 1. For example, in this scenario the host computer is on the network connected to Port 1.



If you enable the **Drop wireless link when port 1 is connected** feature, the M111 can automatically switch between port 1 and the wireless link. See [Port control on page 3-26](#).

Note

The M111 only supports **one** serial over TCP connection.

Serial port connector

The M111 features a standard serial port with DB-9 (female) connector. Pin assignments are as follows:

Pin	Signal	Direction	Connector
1	DCD	→ to PC	<p>DB-9 (female)</p>
2	RXD	→ to PC	
3	TXD	← from PC	
4	DTR	← from PC	
5	GND		
6	DSR	→ to PC	
7	RTS	← from PC	
8	CTS	→ to PC	
9	Unused		

To connect a serial device

This procedure describes how to configure all available options that are available when connecting a serial device to the M111.

1. Connect the serial device to the serial port on the M111 using a standard straight-through serial cable.

2. Select **Network > TCP serial**. The **TCP to serial configuration** page opens.

TCP to serial configuration

TCP connection

Mode: **Server**

TCP port: **8000**

☐ Transmit timeout: **100**

☐ Idle timeout: **30**

Serial port

Data bits: **8**

Parity bit: **None**

Stop bits: **1**

Baud rate: **38400**

Software flow control: **None**

Hardware flow control: **None**

Max receive buffer: **1024**

TCP connection status

State	Remote IP address	Connection time	Tx (kbytes)	Rx (kbytes)
Not connected				

Port control

☐ Drop wireless link when port 1 is connected

Save

3. Enable the **TCP to serial configuration** option and configure parameters as follows:

TCP connection

Mode

- **Client:** The M111 acts as a TCP client and initiates a connection to the specified **Remote IP address** using the specified **TCP port**.
- **Server:** The M111 acts as a TCP server and will listen for an incoming connection from a TCP client on the specified TCP port.

Remote IP address

IP address of the remote device to which the M111 will attempt to connect when operating in client mode.

TCP port

Sets the TCP port number that the M111 will use for the connection.

Transmit timeout

Specifies the length of time, in milliseconds, that traffic on the serial port will be buffered.

Idle timeout

Sets the amount of time, in seconds, that the TCP connection can remain idle before it is disconnected by the M111.

Serial port

Use these parameters to configure the serial port on the M111 to match the settings on the connected serial device.

Data bits

Number of data bits.

Parity bit

Sets the parity.

Stop bits

Number of stop bits.

Baud rate

Baud rate in bps.

Software flow control

- **None:** The M111 does not provide flow control. Instead, flow control is performed end-to-end by the remote TCP device and the locally connected serial device.
- **XON/XOFF:** Flow control is performed locally using XON/XOFF. In this case, the attached serial device must also support software flow control.

Hardware flow control

- **None:** The M111 does not provide flow control. Instead, flow performed end-to-end by the remote TCP device and the locally connected serial device.
- **RTS/CTS:** Flow control is performed locally using RTS (Request To Send)/CTS (Clear To Send). In this case, the attached serial device must also support hardware flow control.

Max receive buffer

Receive buffer size in bytes. If the buffer becomes full, data is discarded until space can be freed up.

Port control

Drop wireless link when port 1 is connected

This feature can be used in cases where the remote TCP device is accessible via both Port 1 and the wireless link. When enabled, it automatically switches the TCP connection based on the status of the Port 1 connection:

- When Port 1 is connected to an Ethernet network, the M111 drops the wireless connection and sends all traffic via Port 1.
- When Port 1 is disconnected from the Ethernet network, the M111 attempts to establish a wireless connection via the appropriate station profile. Traffic is then sent on the wireless link.

Note

To use this feature, Port 1 and the Wireless port must connect the M111 to the same subnet.

TCP connection status

This table lists status information for the TCP connection.

State

Indicates the state of the TCP connection. Possible values are:

- **Listening:** When **Mode** is set to **Server**, indicates that the M111 is waiting for the remote TCP client to establish the connection.
- **Connecting:** When **Mode** is set to **Client**, indicates that the M111 is attempting to establish a connection with the remote TCP server. If this state persists it means that the remote TCP server is not reachable. The M111 will periodically attempt to establish the connection.
- **Active:** The connection has been established, and data is being transferred.
- **Idle:** The connection has been established, but no data is currently being transferred.

Remote IP address

Address of the remote TCP client.

Connection time

Amount of time since the connection was first established.

Tx (kbytes)

Amount of traffic sent to the remote TCP client.

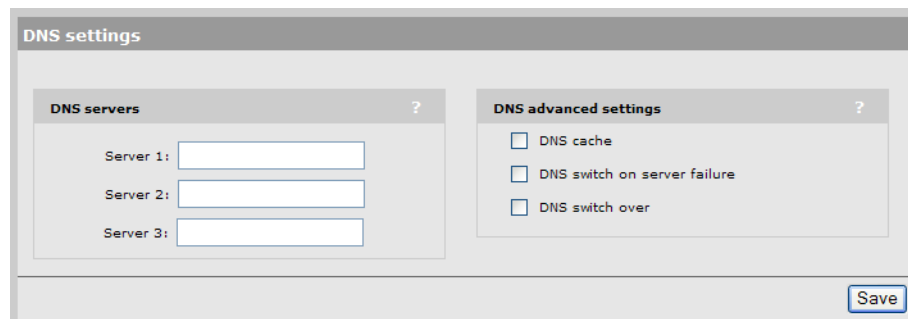
Rx (kbytes)

Amount of traffic received from the remote TCP client.

DNS configuration

Select **Network > DNS** to define DNS settings. The available parameters on this page vary depending on the IP addressing method that is being used by the M111.

- If the M111 is using static addressing, the following options are displayed:



The screenshot shows a 'DNS settings' window with two main sections: 'DNS servers' and 'DNS advanced settings'. The 'DNS servers' section contains three input fields labeled 'Server 1:', 'Server 2:', and 'Server 3:'. The 'DNS advanced settings' section contains three checkboxes: 'DNS cache', 'DNS switch on server failure', and 'DNS switch over'. A 'Save' button is located at the bottom right of the window.

- If the M111 is configured as a DHCP client, the following options are displayed:

The screenshot shows a 'DNS' configuration window. It is divided into two panels. The left panel, titled 'DNS servers', contains a section for 'Dynamically assigned DNS servers' with labels for 'Server 1:', 'Server 2:', and 'Server 3:'. Below this is a checkbox 'Override dynamically assigned DNS servers'. If checked, there are three input fields for 'Server 1:', 'Server 2:', and 'Server 3:'. The right panel, titled 'DNS advanced settings', contains three checkboxes: 'DNS cache', 'DNS switch on server failure', and 'DNS switch over'. A 'Save' button is at the bottom right.

DNS servers

Dynamically assigned DNS servers

Lists the servers that were assigned by the DHCP server.

Override dynamically assigned DNS servers

Enable this option to replace the dynamically assigned servers with manually specified ones.

Server 1

Specify the IP address of the first DNS server that the M111 will use.

Server 2

Specify the IP address of the second DNS server that the M111 will use.

Server 3

Specify the IP address of the third DNS server that the M111 will use.

DNS advanced settings

DNS cache

Enables the DNS cache. Once a host name has been successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, as the remote DNS server now does not have to be queried for subsequent requests for this host.

The entry stays in the cache until:

- An error occurs when connecting to the remote host
- The time to live (TTL) of the DNS request expires
- The M111 is restarted.

DNS switch on server failure

This setting controls how the M111 switches between the primary and secondary DNS servers.

- When enabled, the M111 switches servers if the current server replies with a DNS server failure message.
- When disabled, the M111 switches servers if the current does not reply to a DNS request.

DNS switch over

This setting controls how the M111 switches back to the primary DNS server after it has switched to the secondary DNS server because the primary was unavailable.

- When enabled, the M111 switches back to the primary server after it becomes available again.
- When disabled, the M111 switches back to the primary server only if the secondary server becomes unavailable.

Handling unsupported traffic

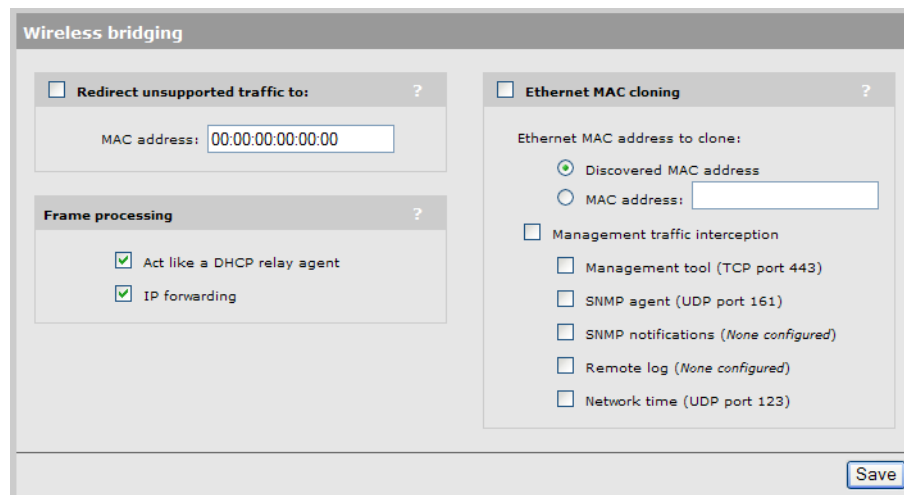
When Ethernet MAC cloning is disabled, the M111 only sends and receives IPv4 traffic on the wireless link. By default, all other traffic is *unsupported* and is dropped. In some cases, you may want to forward the *unsupported* traffic to a wired device connected to Port 1.

Note

When the Ethernet MAC cloning feature is enabled, the M111 forwards all incoming traffic on the wireless link to the attached wired device. There is no unsupported traffic.

To forward unsupported traffic

1. Select **Wireless > Bridging**. The Wireless bridging page opens.



2. Enable the **Redirect unsupported traffic to** option.
3. Specify the **MAC address** of the wired device to which you want to forward traffic. The device must be accessible via Port 1.
4. Select **Save**.

IP forwarding

Ethernet devices that do not send any IP packets at startup will have no entry in the M111 wireless-to-MAC translation table. As a result, the M111 will not be able to route incoming IPV4 wireless traffic to these devices.

When this option is enabled, the M111 sends an ARP request on Port 1 whenever a packet with an unknown destination IP address is received. After receiving an ARP response, the M111 is able to send the packet to the intended target device.

Cloning the address of a wired device

The Ethernet MAC cloning feature enables the M111 to preserve the MAC address of a connected device, thereby minimizing the impact on network configuration when the device is converted to wireless. MAC cloning is also useful when the M111 is employed with third-party access points that do not accept requests from more than one IP address per wireless MAC address.

MAC cloning renders the M111 transparent on the wireless network, as all traffic is passed-through to the cloned device. It enables devices on the network to access the cloned device by its MAC address, which is useful for tracking, security, or management tasks.

Limitations

The following limitations apply when Ethernet MAC cloning is enabled:

- Only one wired device can be connected to the M111 via Port 1.
- The TCP serial feature cannot be used to connect a serial device.
- The M111 no longer has access to the Wireless port. This means that wireless access to the management tool and the services it provides (SNMP agent, time server client, etc.) are not available. However, additional configuration settings are available that enable support for some services. See [*Wireless access to the M111 when MAC cloning is active on page 3-31*](#).

Enabling Ethernet MAC cloning

Configure Ethernet MAC cloning as follows:

1. Select **Wireless > Bridging**. The Wireless bridging page opens.

The screenshot shows the 'Wireless bridging' configuration window. It is divided into three main panels. The first panel, 'Redirect unsupported traffic to:', has a checkbox that is unchecked and a text field for 'MAC address' containing '00:00:00:00:00:00'. The second panel, 'Frame processing', has two checked checkboxes: 'Act like a DHCP relay agent' and 'IP forwarding'. The third panel, 'Ethernet MAC cloning', has a checkbox that is unchecked. Below it, there are two radio buttons: 'Discovered MAC address' (which is selected) and 'MAC address:' (which is followed by an empty text field). Below these are several unchecked checkboxes under the heading 'Management traffic interception': 'Management tool (TCP port 443)', 'SNMP agent (UDP port 161)', 'SNMP notifications (None configured)', 'Remote log (None configured)', and 'Network time (UDP port 123)'. A 'Save' button is located at the bottom right of the window.

2. Under **Ethernet MAC cloning**, enable one of the following options:
 - **Discovered MAC address:** When this option is selected, as soon as the M111 detects a wired device on Port 1, it assigns the wired device MAC address to the Wireless port and re-associates using the current station profile.
 - **MAC address:** When this option is selected, the M111 re-associates with the current station profile using the specific MAC address which you define.
3. Select **Save**.

Wireless access to the M111 when MAC cloning is active

A limitation of MAC cloning is that once the cloned MAC address is used to establish the wireless connection, the M111 itself is no longer accessible through the wireless connection. Not only does this disable wireless access to the management tool by administrators, but also blocks services operating on the management tool such as:

- Scheduled firmware updates or scheduled configuration file backup/restore operations
- SNMP agent response and notifications
- System time updates via a time server (Time server client)
- DHCP client which updates the M111 IP address when its DHCP lease expires

To resolve some of these limitations, you can use the management traffic interception feature.

Setting up management traffic interception

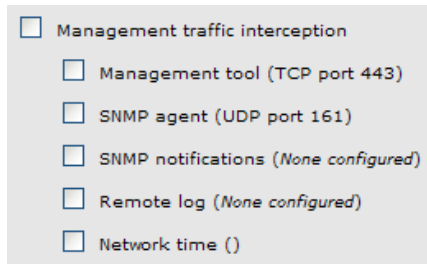
The management traffic interception feature (on the **Wireless > Bridging** page) lets you establish administrator logins to the M111 management tool when MAC cloning is active and lets you intercept incoming wireless traffic on specific ports and redirect it to the M111 internal processes (M111 management tool, M111 SNMP agent, or the M111 Network Time client) instead of forwarding it to the cloned device.

Each option displays the port that will be redirected in parenthesis. (Default values are shown in the image below.) In most cases, the port number can be changed. Consult the following descriptions for full details.

Note

SNMP notifications and Remote log are not redirected to the management tool, as they are both outbound.

The following options are available.



The image shows a configuration window titled "Management traffic interception". It contains a list of options, each with a checkbox and a label in parentheses indicating the default port or status:

- ☐ Management traffic interception
 - ☐ Management tool (TCP port 443)
 - ☐ SNMP agent (UDP port 161)
 - ☐ SNMP notifications (*None configured*)
 - ☐ Remote log (*None configured*)
 - ☐ Network time ()

Note

When using these options to reach services on the M111, you must use the IP address assigned to the cloned device and not the original IP address assigned to the M111.

Management tool (TCP port 443)

This option enables support for administrator logins to the M111 management tool by redirecting HTTPS traffic. If the cloned device needs to support HTTPS as well, you can relocate the management tool port as follows:

1. Select **Management > Management tool**.
2. Under **Web server**, set **Secure Web server port** to **8443** (which is the common alternative HTTPS port).
3. Under **Security > Active interfaces** make sure that the **Wireless port** is selected.
4. Select **Save**.

If the cloned device was at IP address 192.168.5.23, to reach the management tool you would now specify the following in your browser: 192.168.5.23:8443.

SNMP agent (UDP port 161)

This option enables support for the SNMP agent by redirecting traffic on UDP port 161. If the cloned device needs support to support SNMP as well, you can relocate the SNMP port as follows:

1. Select **Management > SNMP**.
2. Under **Attributes**, set **Port** to a new value.

3. Select **Save**.

SNMP notifications (UDP port 162)

This enables support for the SNMP notifications, allowing the M111 SNMP agent to send notifications using UDP port 162.

Remote log (UDP port 514)

This enables support for the Remote logging feature on the Tools menu, allowing the M111 to send message to remote syslog servers using UDP port 514.

Network time (UDP port 123)

This enables support for communication with a time server. If the cloned device needs to communicate with a time server as well, you should set the cloned device to use the **Time Protocol** and leave the M111 to use SNTP on UDP port 123.

Using filters to restrict wireless traffic

The M111 features filters that can be used to restrict the flow of wireless traffic. You can use filters to limit both incoming and outgoing traffic on the wireless link.

Configure traffic filters as follows:

1. Select **Security > Filters**. The Filters page opens.



2. Enable the **Wireless traffic filters** option.
3. Specify a filter for **In** and/or **Out**. Define the filters using standard pcap syntax (for details see http://www.tcpdump.org/tcpdump_man.html) with the addition of the following custom placeholders:
 - %b - MAC address of the M111 Bridge port.
 - %g - MAC address of the default gateway assigned to the M111.
 - %w - MAC address of Wireless port.

These placeholders are expanded by the M111 when the filter is activated. Once expanded, the filter must respect standard pcap syntax.

4. Select **Save**.

Assigning a management address

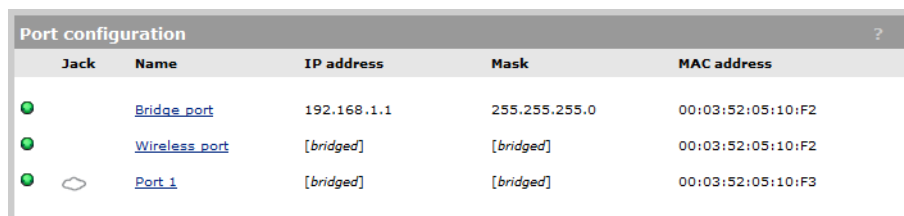
A **Management address** is a secondary, static IP address that provides a fixed address where the M111 management tool can be reached via either Port 1 or the Wireless port.


Note

The management address must be on a *different subnet* than the IP address currently assigned to the bridge port.

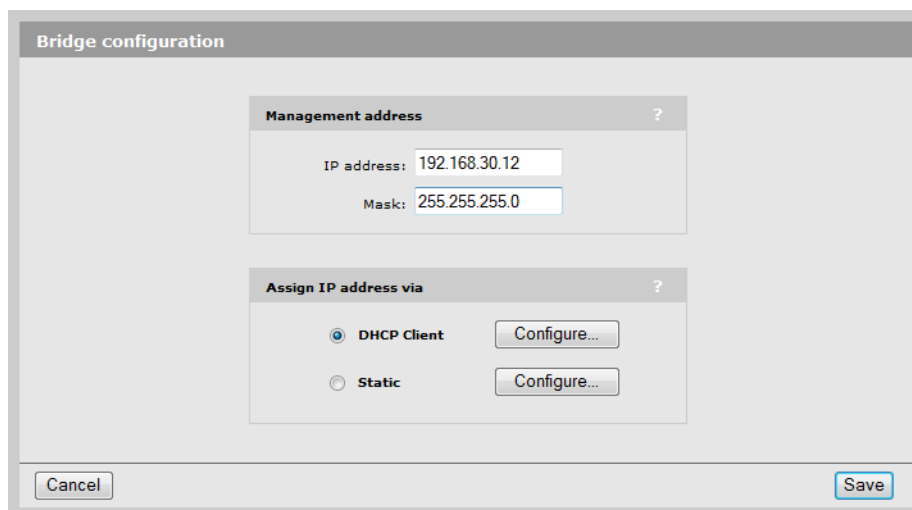
To assign a management address

1. Select **Network > Ports**.



Jack	Name	IP address	Mask	MAC address
●	Bridge port	192.168.1.1	255.255.255.0	00:03:52:05:10:F2
●	Wireless port	[bridged]	[bridged]	00:03:52:05:10:F2
●	 Port 1	[bridged]	[bridged]	00:03:52:05:10:F3

2. Select **Bridge port** in the table.
3. In the **Bridge configuration** page, **Management address** section, enter a new **IP address** and **Mask** value.



Bridge configuration

Management address

IP address: 192.168.30.12

Mask: 255.255.255.0

Assign IP address via

☒ DHCP Client

☐ Static

4. Select **Save**.

SNMP

The M111 provides a robust SNMP implementation supporting both industry-standard and custom MIBs. For information on supported MIBs, see the *M111 SNMP MIB Reference Guide*.

Select **Management > SNMP** to open the **SNMP agent configuration** page. By default, the SNMP agent is enabled (**SNMP agent configuration** in the title bar is selected). If you disable the agent, the M111 will not respond to SNMP requests.

☒ **SNMP agent configuration** ?

Attributes ?

System name:
Location:
Contact:

Engine ID: 80:00:22:28:03:00:03:52:09:66:5E
Port: UDP
SNMP protocol: ☒ version 1 ☒ version 2c ☐ version 3
Notifications: ☐

v1/v2c communities ?

Community name: Read-only name:
Confirm community name: Confirm read-only name:

v3 users ?

Username	Security	Access level
readonly	MD5/DES	read-only
readwrite	MD5/DES	read-write

Notification receivers ?

Host	UDP port	Version	Community/Username
No notifications receivers are defined.			

Security ?

Access to the SNMP agent is enabled for the addresses and interfaces that are specified below.
Allowed addresses:

IP address: Mask:

Active interfaces:

☒ Port 1 ☐ Wireless ports

Attributes

- **System name:** Specify a name to identify the M111. Default is the M111 serial number.
- **Location:** Specify a descriptive name for the location where the M111 is installed.
- **Contact:** Specify an email address for a contact person for the M111.
- **Port:** Specify the UDP port and protocol the M111 uses to respond to SNMP requests. Default port is 161.
- **SNMP Protocol:** Select the SNMP versions that the M111 will support. Default is **Version 1** and **Version 2c**.
- **Notifications:** When this feature is enabled, the M111 sends notifications to the hosts that appear in the **Notifications receivers** list.

The M111 supports the following MIB II notifications:

- coldStart
- linkUp
- linkDown
- authenticationFailure

In addition, the M111 supports a number of custom notifications. Select **Configure Notifications**. For a descriptions of these notifications, see the online help.

v1/v2c communities

- **Community name:** Specify the password, also known as the read/write name, that controls read/write access to the SNMP agent. A network management program must supply this password when attempting to **set** or **get** SNMP information from the M111. By default, this is set to **private**.
- **Confirm community name:** Re-enter the **Community name**.
- **Read-only name:** Specify the password that controls read-only access to the SNMP agent. A network management program must supply this password when attempting to **get** SNMP information from the M111. By default, this is set to **public**.
- **Confirm read-only name:** Re-enter the **Read-only name**.

v3 users

This table lists all defined SNMP v3 users. To add a new user, select **Add New User**. Up to five users are supported. To edit a user, select their link in the **Username** column.

Username

The SNMP v3 username.

Security

Security protocol defined for the user. Authentication type and encryption type are separated a slash. For example, **MD5/DES** indicates **MD5** authentication and **DES** encryption.

Access level

Type of access assigned to the user:

- **Read-only:** The user has read and notify access to all MIB objects.
- **Read-write:** The user has read, write, and notify access to all MIB objects.

Notification receivers

This table lists all defined SNMP notification receivers. SNMP notifications are sent to all receivers in this list. To add a new receiver, select **Add New Receiver**. Up to five receivers are supported. To edit a receiver, select its link in the **Host** column.

Host

The domain name or IP address of the SNMP notifications receiver to which the M111 will send notifications.

UDP port

The port on which the M111 will send notifications.

Version

The SNMP version (v1,v2c, v3) for which this receiver is configured.

Community/Username

- For SNMP v1 and v2c, the SNMP Community name of the receiver.
- For SNMP v3, the SNMP v3 Username of the receiver.

Security

Use these settings to control access to the SNMP agent.

- **Allowed addresses:** List of IP address from which access to the SNMP agent is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add**.

When the list is empty, access is permitted from any IP address.

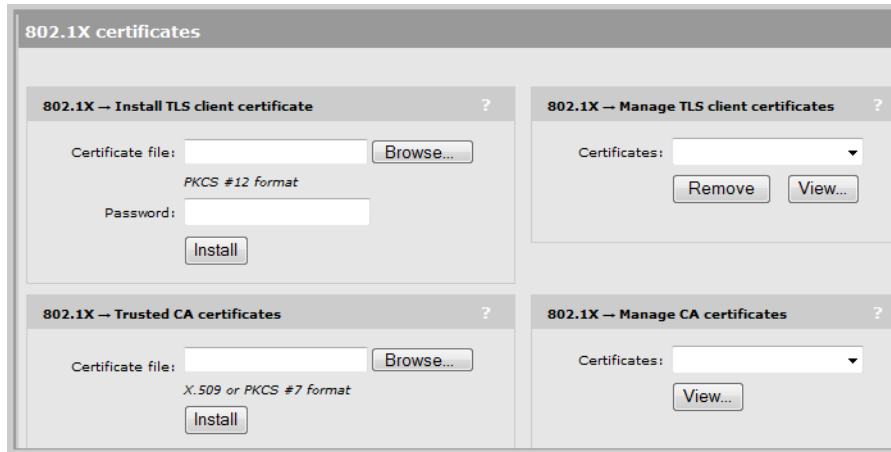
- **Active interfaces:** Select the checkboxes that correspond to the interfaces from which to allow access to the SNMP agent.

Managing certificates

Digital certificates are electronic documents that are used to validate the end parties or peers involved in data transfer. Various features on the M111 make use of certificates for authentication and/or encryption of data exchanged with peers.

802.1X certificates

802.1X certificates are managed on the **Security > 802.1X certificates** page.



The M111 supports two 802.1X certificates:

- **TLS client certificate:** Installation of this certificate is mandatory if 802.1X with an **EAP method** of **TLS** is configured under **Wireless security** in a station profile. The M111 will supply this certificate to peers during the authentication process.
- **Trusted CA certificate:** Installation of this certificate is mandatory if 802.1X with an **EAP method** of **TLS**, **TTLS**, or **PEAP** is configured under **Wireless security** in a station profile, and the **Validate server certificate** is also enabled. The M111 will use this certificate to validate certificates supplied by peers during the authentication process.

802.1X — Install TLS client certificate

Use this option to install a certificate for TLS authentication. The M111 will supply this certificate to peers during the authentication process.

The certificate must:

- be in PKCS #12 format.
- contain a private key. (The password is used to access the private key.)
- not have a name that is an IP address. The name should be a domain name containing at least one dot.

Certificate file

Specify the name of the certificate file or select **Browse** to select it.

Password

Specify the certificate password.

Install

Select this button to install the certificate.

802.1X — Manage TLS client certificates

The **Certificate** field shows the contents of the CN field in the certificate. This is the domain name of the certificate.

Select **View** to see the contents of the certificate.

802.1X — Trusted CA certificates

The M111 uses the CA certificates to validate the certificates supplied by peers during the authentication process. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

Certificate file

Enter the name of the certificate file or select **Browse** and select it. CA certificates must be in X.509 or PKCS #7 format.

Install

Select this button to install the certificate.

802.1X — Manage CA certificates

Use this box to manage the root CA certificate.

Certificate

This box shows the list of installed certificates.

Remove

Select a certificate in the list and select this button to remove it.

View

Select a certificate in the list and select this button to view it.

Certificate stores

The certificate stores provide a repository for managing all non-802.1X certificates. To view the certificate store, select **Security > Certificate stores**.

Trusted CA certificate store				
ID	Issued to	Current usage	CRL	Delete
PKCS #7 file or X.509 certificate: <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Install"/>				

Certificate and private key store				
ID	Issued to	Issued by	Current usage	Delete
1	wireless.colubris.com	wireless.colubris.com	Web Management Tool	<input type="button" value="Delete"/>

PKCS #12 file:	<input type="text"/>	<input type="button" value="Browse..."/>	PKCS #12 password:	<input type="text"/>	<input type="button" value="Install"/>
----------------	----------------------	--	--------------------	----------------------	--

Trusted CA certificate store

This list displays all CA certificates installed on the M111. The M111 uses the CA certificates to validate the certificates supplied by administrators accessing the M111 management tool. Multiple CA certificates can be installed to support validation of certificates issued by different CAs.

The following information is displayed for each certificate in the list:

- **ID:** A sequentially assigned number to help identify certificates with the same common name.
- **Issued to:** Name of the certificate holder. Select the name to view the contents of the certificate.
- **Current usage:** Lists the services that are currently using this certificate.
- **CRL:** Indicates if a certificate revocation list is bound to the certificate. An X.509 certificate revocation list is a document produced by a certificate authority (CA) that provides a list of serial numbers of certificates that have been signed by the CA but that should be rejected.
- **Delete:** Select to remove the certificate from the certificate store.

Installing a new CA certificate

1. Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
2. Select **Install** to install a new CA certificate.

CA certificate import formats

The import mechanism supports importing the ASN.1 DER encoded X.509 certificate directly or as part of two other formats:

- PKCS #7 (widely used by Microsoft products)
- PEM, defined by OpenSSL (popular in the Unix world)
- The CRL can be imported as an ASN.1 DER encoded X.509 certificate revocation list directly or as part of a PEM file.

Content and file format	Items carried in the file	Description
ASN.1 DER encoded X.509 certificate	One X.509 certificate	This is the most basic format supported, the certificate without any envelope.
X.509 certificate in PKCS #7 file	One X.509 certificate	Popular format with Microsoft products.

Content and file format	Items carried in the file	Description
X.509 certificate in PEM file	One or more X.509 certificate	Popular format in the Unix world. X.509 DER certificate is base64 encoded and placed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines. Multiple certificates can be repeated in the same file.
ASN.1 DER encoded X.509 CRL	One X.509 CRL	Most basic format supported for CRL.
X.509 CRL in PEM file	One X.509 CRL	Same format as X.509 certificate in PEM format, except that the lines contain BEGIN CRL and END CRL.

Certificate and private key store

This list displays all certificates installed on the M111. The M111 uses these certificates and private keys to authenticate itself to peers.

The following information is displayed for each certificate in the list:

- **ID:** A sequentially assigned number to help identify certificates with the same common name.
- **Issued to:** Name of the certificate holder. Select the name to view the contents of the certificate.
- **Issued by:** Name of the CA that issued the certificate.
- **Current usage:** Lists the services that are currently using this certificate.
- **Delete:** Select to remove the certificate from the certificate store.

Installing a new private key/public key certificate chain pair

The certificate you install must:

- Be in PKCS #12 format.
- Contain a private key (a password controls access to the private key).
- Not have a name that is an IP address. The name should be a domain name containing at least one dot. If you try to add a certificate with an invalid name, the default certificate is restored.

The name in the certificate is automatically assigned as the domain name of the M111.

1. Specify the name of the certificate file or select **Browse** to choose one from a list. Certificates must be in PKCS #7 format.
2. Specify the **PKCS #12 password**.
3. Select **Install** to install the certificate.

Default installed private key/public key certificate chains

The following private key/public key certificate chains are installed by default:

- **wireless.colubris.com:** Default certificate used by the management tool.

Note

When a web browser connects to the M111 using SSL, the M111 sends only its own SSL certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the web browser only knows about the root certificate authority that signed the public key certificate of the intermediate certificate authority, the web browser does not get the whole certificate chain it needs to validate the identity of the M111. Consequently, the web browser issues security warnings.

To avoid this problem, install an SSL certificate on the M111 only if it is directly signed by the root certificate authority or if you have appended all certificates that make up the chain.

Consequently, the web browser issues security warnings.

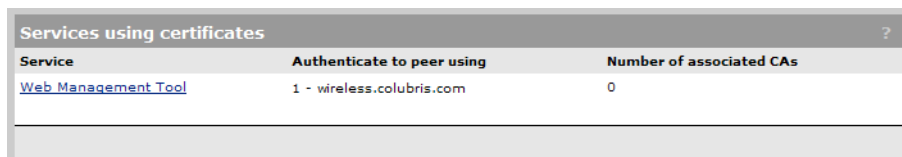
To avoid this problem, make sure that you install the entire certificate chain when you install a new certificate on the M111.

Note

An SNMP notification is generated when the M111's SSL certificate is about to expire.

Certificate usage

To see the services that are associated with each certificate, select **Security > Certificate usage**. With the factory default certificates installed, the page will look like this:

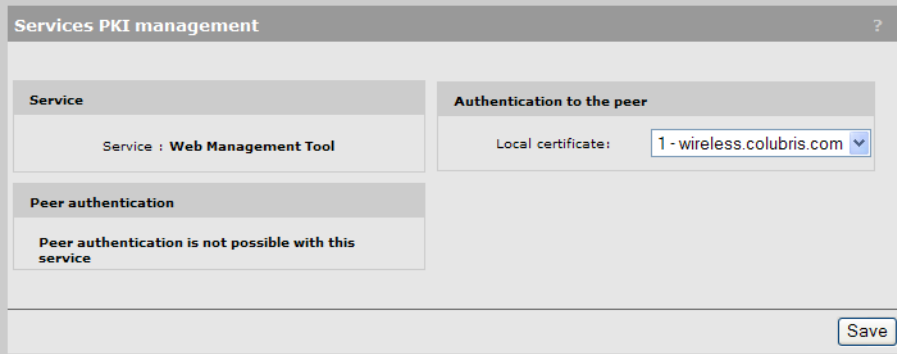


Services using certificates ?		
Service	Authenticate to peer using	Number of associated CAs
Web Management Tool	1 - wireless.colubris.com	0

- **Service:** Name of the service that is using the certificate. To view detailed information on the certificate select the service name.
- **Authenticate to peer using:** Name of the certificate and private key. The M111 is able to prove that it has the private key corresponding to the public key in the certificate. This is what establishes the M111 as a legitimate user of the certificate.
- **Number of associated CAs:** Number of CA certificates used by the service.

Changing the certificate assigned to a service

Select the service name to open the Certificate details page. For example, if you select **Web management tool**, you will see:



The screenshot shows a window titled "Services PKI management" with a question mark icon in the top right corner. The window is divided into several sections. On the left, under the "Service" header, it says "Service : Web Management Tool". Below this, under the "Peer authentication" header, it says "Peer authentication is not possible with this service". On the right, under the "Authentication to the peer" header, there is a "Local certificate:" label followed by a dropdown menu showing "1 - wireless.colubris.com". At the bottom right of the window is a "Save" button.

Under **Authentication to the peer**, select a new **Local certificate** and then select **Save**.

About certificate warnings

When you connect the management tool, certificate warnings occur because the default certificate installed on the M111 is not registered with a certificate authority. It is a self-signed certificate that is attached to the default IP address (192.168.1.1) for the M111.

To continue to work with the management tool without installing a certificate, select the option that allows you to continue to the Website.

To eliminate these warnings you can do one of the following:

- Obtain a registered X.509 (SSL) certificate from a recognized certificate authority and install it on the M111. This is the best solution, since it ensures that your certificate can be validated by any web browser. A number of companies offer this service for a nominal charge. These include: Thawte, Verisign, and Entrust.
- Become a private certificate authority (CA) and issue your own certificate: You can become your own CA. and create as many certificates as you require. However, since your CA will not be included in the internal list of trusted CAs maintained by most browsers, users will get a security alert until they add your CA to their browser.

Configuration file management

The configuration file contains all the settings that customize the operation of the M111. You can save and restore the configuration file manually or automatically by selecting **Maintenance > Config file management**.

The screenshot shows the 'Config file management' window. It contains four panels: 'Backup configuration' with password fields and a 'Backup...' button; 'Restore configuration' with a 'Manual restore' section containing a file browser and password field, and a 'Restore' button; 'Reset configuration' with a 'Reset' button; and 'Scheduled operations' which is checked and includes dropdowns for 'Operation' and 'Day of week', time fields, a 'URL' field, and 'Validate' and 'Save' buttons.

Manual configuration file management

The following options are available for manual configuration file management.

Backup configuration

The **Backup configuration** option enables you to back up your configuration settings so that they can be easily restored in case of failure. You can also use this option if you want to directly edit the configuration file.

Before you install new software, you should always back up your current configuration. Select **Backup** to start the process. You are prompted for the location in which to save the configuration file.

Configuration information is saved in the backup file as follows:

- **Certificates and private keys:** If you specify a password when saving the configuration file, certificates and private keys are encrypted with a key based on the password. If you do not specify a password, certificates and private keys are still encrypted, but with a default key that is identical on all APs.

- **Manager and operator username/password:** This information is not saved in the backup configuration file. This means that if you restore a configuration file, the current username and password on the AP are not overwritten.
- **All other configuration information:** All other configuration information is saved as plain text, allowing the settings to be viewed with a standard text editor.

Reset configuration

See [Appendix B: Resetting to factory defaults](#).

Restore configuration

The **Restore configuration** option enables you to load a previously saved configuration file.

This feature enables you to maintain several configuration files with different settings, which can be useful if you must frequently alter the configuration of the M111 or if you are managing several M111s from a central site.

Use the following steps to restore a saved configuration file.

1. Select **Maintenance > Config file management**. The **Config file management** page opens.
2. In the **Restore configuration** group box under **Manual restore**, select **Browse** to navigate to and select the configuration file that you want to restore.
3. If the configuration file is protected with a password you must supply the correct password to restore the complete configuration. If you supply an invalid password, all settings are restored except for certificates and private keys.
4. Select **Restore** to load the selected file.

The M111 automatically restarts when once the configuration file has been loaded.

Scheduled operations

The **Scheduled operations** feature enables you to schedule unattended backups or restorations of the configuration file.

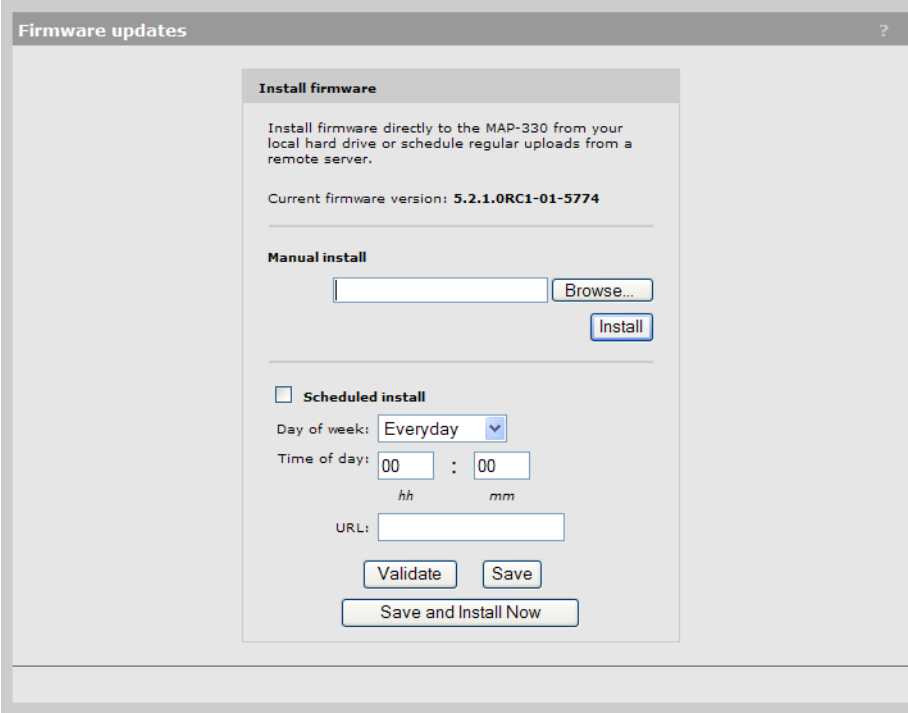
Use the following steps to schedule a backup or restoration of the configuration file.

1. Select **Maintenance > Config file management**. The **Config file management** page opens.
2. Select the **Scheduled operations** checkbox.
3. For **Operation**, select **Backup** or **Restore**.
4. For **Day of week**, select **Everyday**, or select a specific day of the week on which to perform the backup or restoration.

5. For **Time of day**, specify the hour and minute on which to perform the backup or restoration. Use the format *hh mm*, where:
 - *hh* ranges from 00 to 23
 - *mm* ranges from 00 to 59
6. For **URL**, specify the path that leads to the local or remote directory in which to save the configuration file or from which to load the configuration file. For example:
 - **ftp://username:password@192.168.132.11/new.cfg**
 - **http://192.168.132.11/new.cfg**
7. Select **Validate** to test that the specified **URL** is correct.
8. Select **Save**.

Software updates

To update M111 firmware, select **Maintenance > Firmware updates**.



The screenshot shows a web browser window titled "Firmware updates". Inside, there is a form titled "Install firmware". The form contains the following elements:

- A paragraph: "Install firmware directly to the MAP-330 from your local hard drive or schedule regular uploads from a remote server."
- Text: "Current firmware version: 5.2.1.0RC1-01-5774"
- A section titled "Manual install" with a text input field and a "Browse..." button. Below this is an "Install" button.
- A section titled "Scheduled install" with a checkbox that is currently unchecked.
- Below the checkbox, "Day of week:" is set to "Everyday" with a dropdown arrow.
- "Time of day:" is set to "00 : 00", with "hh" and "mm" labels below the respective input boxes.
- A "URL:" text input field.
- At the bottom, there are three buttons: "Validate", "Save", and "Save and Install Now".

Caution

- Before updating be sure to check for update issues in the Release Notes.
 - Even though configuration settings are preserved during software updates, it is recommended that you backup your configuration settings before updating. See [Manual configuration file management on page 3-44](#).
 - At the end of the update process, the M111 automatically restarts, causing all users to be disconnected. Once the M111 resumes operation, all users must reconnect. To minimize network disruption, use the scheduled install option to have updates performed outside of peak usage hours.
-

Performing an immediate software update

To update the M111 firmware now, **Browse** to the firmware file (extension .cim) and then select **Install**.

Performing a scheduled update

The M111 can automatically retrieve and install firmware from a local or remote web site identified by its URL.

To schedule firmware installation, follow this procedure:

1. Enable **Scheduled install**.
2. For **Day of week** select a specific day or **Everyday** and set **Time of day**.
3. For **URL**, specify an ftp or http address like this:
 - **ftp://username:password@192.168.132.11/newfirmware.cim**
 - **http://192.168.132.11/newfirmware.cim**
4. **Validate** the URL.
5. To commit the schedule, select **Save**.
6. Or, to commit the schedule and also update the firmware immediately, select **Save and Install Now**.

Note

Before a scheduled firmware update is performed, only the first few bytes of the firmware file are downloaded to determine if the firmware is newer than the current version. If it is not, the download stops and the firmware is not updated.

Regulatory information

Contents

Notice for U.S.A.	4-2
Notice for Canada.....	4-3
Notice for the European Community.....	4-3
Supported External Antennas.....	4-5
Notice for Brazil.....	4-5
Notice for Japan.....	4-6
Notice for Taiwan	4-6
Notice for Korea	4-6

Notice for U.S.A.

Manufacturer's FCC Declaration of Conformity Statement

Manufacturer: Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185 USA

Phone: 650-857-1501

For questions regarding this declaration, contact the Product Regulations Manager at the above address or phone number.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

The FCC requires the user to be notified that any changes or modifications made to the device that are not expressly approved by the Hewlett-Packard Company may void the user's authority to operate the equipment.

This device is restricted to indoor use when using the 5.15-5.25 GHz band (Channels 36, 40, 44 and 48).

Warning

Exposure to Radio Frequency Radiation

The radiated output power of this device is below the FCC radio exposure limits. Nevertheless, the device should be used in such a manner that the potential for human contact during normal operation is minimized. To avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antennas should not be less than 20 cm (8 inches) during normal operation.

Notice for Canada

This device complies with the limits for a Class B digital device and conforms to Industry Canada standard ICES-003. Products that contain a radio transmitter comply with Industry Canada standard RSS210 and are labeled with an IC approval number.

Cet appareil numérique de la classe B est conforme à la norme ICES-003 de Industry Canada. La radio sans fil de ce dispositif est conforme à la certification RSS 210 de Industry Canada et est étiquetée avec un numéro d'approbation IC.

This device complies with the Class B limits of Industry Canada. Operation is subject to the following two conditions: 1) this device may not cause harmful interference, and 2) this device must accept interference received, including interference that may cause undesired operation.

This device has been designed to operate with the antennas listed in this section, having a maximum gain of 5.6 dBi. Antennas not included in this list or having a gain greater than 5.6 dBi are strictly prohibited for use with this device. The required impedance is 50 ohms.

To reduce potential radio interference with other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

This device is restricted to indoor use when using the 5.15-5.25 GHz band (Channels 36, 40, 44 and 48).

Notice for the European Community



This device complies with the EMC Directive 2004/108/EC, Low Voltage Directive 2006/95/EC and R&TTE Directive 1999/5/EC. Compliance with these directives implies conformity to harmonized European standards (European Norms) that are listed on the EU Declaration of Conformity that has been issued by HP for this device.

Countries of Operation & Conditions of Use

This device may be used in the following EU and EFTA countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland and the United Kingdom. Requirements for indoor vs. outdoor operation, licensing and allowed channels of operation apply in some countries as described below.

Note

The user must use the configuration utility provided with this device to ensure the channels of operation are in conformance with the spectrum usage rules for EU and EFTA countries as described below.

2.4 GHz Operation

- This device may be operated indoors or outdoors in all EU and EFTA countries using the 2.4 GHz band (Channels 1 - 13), except where noted below.
- In **France**, this device may use the entire 2400 - 2483.5 MHz band (Channels 1 through 13) for indoor applications. For outdoor use, only the 2400 - 2454 MHz frequency band (Channels 1 through 9) may be used. For the latest requirements, see <http://www.art-telecom.fr>.

L'utilisation de cet équipement (2.4 GHz wireless LAN) est soumise à certaines restrictions: cet équipement peut être utilisé à l'intérieur d'un bâtiment en utilisant toutes les fréquences de 2400 à 2483.5 MHz (Chaîne 1-13). Pour une utilisation en environnement extérieur, vous devez utiliser les fréquences comprises entre 2400 à 2454 MHz (Chaîne 1-9). Pour les dernières restrictions, voir <http://www.art-telecom.fr>.

5 GHz Operation

- This device requires the user or installer to properly enter the **current country of operation** in the 5 GHz Radio Configuration Window,
- This device will automatically limit the allowable channels determined by the current country of operation. Incorrectly entering the country of operation may result in illegal operation and may cause harmful interference to other systems. The user is obligated to ensure the device is operating according to the channel limitations, indoor/outdoor restrictions and license requirements for each European Community country as described in this guide.
- This device employs a **radar detection feature** required for European Community and EFTA country operation in the 5 GHz band. This feature is automatically enabled when the country of operation is correctly configured for any European Community or EFTA country. The presence of nearby radar operation may result in temporary interruption of operation of this device. The radar detection feature will automatically restart operation on a channel free of radar.
- This device is restricted to **indoor** use when operated in EU and EFTA countries using the 5.15-5.35 GHz band (Channels 36, 40, 44, 48, 52, 56, 60 and 64). See the table below for the allowed 5 GHz channels in each band.

Operation Using 5 GHz Channels in the European Community

The user/installer must use the provided configuration utility to check the current channel of operation and make necessary configuration changes to ensure operation occurs in conformance with European National spectrum usage laws as described below and elsewhere in this guide.

Frequency Band (MHz)	Allowed Channels	Usage	Maximum EIRP (mW)
5150 - 5250	36, 40, 44, 48	Indoor use only	200
5250 - 5350	52, 56, 60, 64	Indoor use only	200

Frequency Band (MHz)	Allowed Channels	Usage	Maximum EIRP (mW)
5470 - 5725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor or outdoor use	1000

Disposal of Waste Equipment by Users in Private Household in the European Union



This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Supported External Antennas

The following table lists the available antennas for the M111.

Product Number	Antenna Type	Antenna Band (GHz)			
		2.4	5.15 - 5.35	5.47 - 5.725	5.725 - 5.850
J9401A	Omni	2.5 dBi	3.0 dBi	3.4 dBi	3.4 dBi

Caution

When using antennas outdoors, a lightning arrestor is required for lightning protection. Consider placing the lightning arrestor immediately before the antenna cable enters the building. HP offers a lightning arrestor as an accessory; it is orderable under HP product number J8996A.

All HP ProCurve devices are designed to be compliant with the rules and regulations in locations they are sold and will be labeled as required. Any changes or modifications to HP ProCurve Equipment, not expressly approved by HP, could void the user's authority to operate this device. Use only antennas approved for use with this device. Unauthorized antennas, modifications, or attachments could cause damage and may violate local radio regulations in your region.

Notice for Brazil

Aviso aos usuários no Brasil Este equipamento opera em caráter secundário, isto é, não tem direito à proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário..

Notice for Japan

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

- 1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
- 2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等（例えば、パーティションの設置など）についてご相談して下さい。
- 3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：日本ヒューレット・パッカード株式会社 TEL：0120-014121

Notice for Taiwan

DGT LPD (Low Power Device) Statement

低功率電波輻射性電機管理辦法

第十四條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Notice for Korea

(warning for wireless equipment)

당해 무선설비는 운용 중 전파혼선 가능성이 있음

Resetting to factory defaults

Contents

How it works.....5-2

 Using the Reset button.....5-2

 Using the management tool.....5-2

How it works

Caution

Resetting the M111 to factory defaults deletes all configuration settings, resets the manager username and password to “admin”, and enables the DHCP client. If no DHCP server assigns an address to the M111, its address defaults to 192.168.1.1.

Using the Reset button

Using a tool such as a paper clip, press and hold the reset button for a few seconds until the front status lights blink three times.

Using the management tool

1. Launch the management tool (default <https://<IP address of the M111>>).
2. Select **Maintenance > Config file management**.
3. Under **Reset configuration**, select **Reset**.

The screenshot displays the 'Config file management' web interface. It features four main sections: 'Backup configuration', 'Restore configuration', 'Reset configuration', and 'Scheduled operations'. The 'Reset configuration' section, which includes the instruction 'Reset the configuration to factory default.' and a 'Reset' button, is highlighted with a red dashed rectangular box. The 'Backup configuration' section has fields for 'Password' and 'Confirm password' with a 'Backup...' button. The 'Restore configuration' section has a 'Manual restore' subsection with a 'Config file' field, a 'Browse...' button, a 'Password' field, and a 'Restore' button. The 'Scheduled operations' section is currently unchecked and includes dropdowns for 'Operation' (set to 'Backup') and 'Day of week' (set to 'Everyday'), along with 'Time of day' fields (set to '00 : 00') and a 'URL' field, with 'Validate' and 'Save' buttons at the bottom.

Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

© Copyright 2010 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.



April 2010

Manual Part Number
5998-0329