# Wireless Switch 5000

## Quick Setup Guide

WS 5000 Wireless Switch Version 1.1.4.30

*symbol*®

www.symbol.com

# Copyright

# Patents

(3/02)

# Configuring the WS 5000 and Applying a WEP-128 Policy

Before using this quick setup guide, be sure to complete the tasks in the *WS 5000 Wireless Switch Quick Install Guide* (QIG).

This document is written for the network installer or administrator who is familiar with their Ethernet IP network but who is not necessarily trained on Symbol Technologies equipment. The goal of this document is to show this user how to: (1) Connect the WS 5000 in a basic, flat switch network topology and verify that it is properly connected, (2) Configure the WS 5000 to support the network topology and (3) Apply a basic WEP 128 policy.

### Step 1: Connect Hardware & Ping

- WS-5000 to AC Power
- Port 1 to L2 switch
- Port 2 to L2 switch
- In-Line Power to AP
- AP to L2 switch
- Test Default Config with Ping
  - ESSID = 101
  - No Encryption
- Goto Step #2

### Step 2: Set IP Address of WS-5000

- Serial Console to CLI
  - 19.2,N,8,1
  - Null Modem Cable
- CFG ethernet 2
- Set DHCP Disable
- IP Address x.x.x.x  y.y.y.y
- Set Gateway z.z.z.z
- Show Ethernet 2
- Goto Step #3

### Step 3: Config Secure WLAN

- Connect HTTPS to WS-5000
- Login: admin  pw: symbol
- Create Wireless Switch Policy
- Create Access Port Policy
- Create WLAN Policy
- Create Security Policy
- Test new secure WLAN with Ping
- Done

Figure 1: The WS 5000 Setup Steps

When the user has completed this setup guide, the WS 5000 switch will be able to support their WLAN with the basic, minimum configuration recommended by Symbol Technologies, Inc. The time required to complete these three steps is normally less than an hour.

## Step 1: Connecting the WS 5000 to the Network

This step should take less than 15 minutes to complete.

Refer to Figure 2 for cabling details and specific device configurations (required for the ping test). All the wireless LAN (WLAN) devices are connected to Layer-2 switch A and all the wired LAN devices are connected to Layer-2 switch B. Connect Layer-2 switch A to Ethernet port 1 on the WS 5000 (labeled WLAN 0) to connect the wireless traffic, and connect Layer-2 switch B to Ethernet port 2 on the WS 5000 (labeled LAN 1) to connect the wired LAN traffic.

Figure 2: The Network Topology

## Verifying the Connections

If the WS 5000 is connected correctly, devices on the wireless LAN should be able to connect to devices on the LAN. To test the connection between the wireless client device and the computer shown in Figure 2, from the wireless client, enter:

```
C:> ping xxx.xxx.xxx.yyy
PING xxx.xxx.xxx.yyy (xxx.xxx.xxx.yyy): 56 data bytes
64 bytes from xxx.xxx.xxx.yyy: icmp_seq=0 ttl=127 time=0.39 ms
64 bytes from xxx.xxx.xxx.yyy: icmp_seq=1 ttl=127 time=0.327 ms
64 bytes from xxx.xxx.xxx.yyy: icmp_seq=2 ttl=127 time=0.33 ms
64 bytes from xxx.xxx.xxx.yyy: icmp_seq=3 ttl=127 time=0.309 ms

--- xxx.xxx.xxx.yyy ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.309/0.338/0.39 ms

C:>
```

Because the wireless client was able to connect to a computer on the network through the switch, the network connections are functioning properly. If the ping test fails, make sure the target computer is turned on, connected to the network, and is configured with the IP address used in the ping.

# Step 2: Initial Configuration Using the CLI

This step should take less than 10 minutes to complete.

Note: In this guide, MAC and IP addresses have been changed to protect actual devices from unauthorized access.

To configure the WS 5000 with site-specific IP addressing and network policies, connect the administrative PC to the WS 5000 with the serial cable  (as discussed in the QIG). Once the basic WS 5000 network configuration is complete, administrators can create a policy as discussed in "Basic WS 5000 Configuration."

The terminal emulation window will display the Wireless Switch login screen (if the login prompt does not display, press <Enter> until the Command Line Interface (CLI) appears:

```
Wireless Switch…
userid:
```

Enter `admin` at the userid prompt:

```
userid:admin<enter>
```

Enter `symbol` at the password prompt:

```
password:symbol<enter>
```

The system displays the following:

```
Retrieving user and system information...

Setting user permissions flags..
Checking KDC access permissions...

Welcome...

System information...

System Name                 : WS5000
Descriptions                : WS 5000 Wireless Network
Software Ver.               : 1.1.4.30
Licensed to                 : Symbol Technologies
Copyright                   : Copyright (c) 2000-2003.  All rights reserved.
Serial Number               : 00A0xxxxxxxx
Number of Licenses          : 30
Max Access Port             : 30
Max Mobile Clients          : 4096
Active Switch Policy        : Default Wireless Switch Policy
Emergency Switch Policy     : Not defined
Switch Uptime               : 00d:00h:00m
# of Unassigned Access Ports : 0

WS5000>
```

Verify that the software version shown in the `Software Ver.` field is the current version by comparing this value with that on the Symbol website at:

http://www.symbol.com/services/downloads/download_switchwireless.html

If the WS 5000 software version is older than what is on the Symbol Technologies, Inc. website, then refer to the Release Notes for this WS 5000 for instructions on upgrading the software.

The following steps create a typical network configuration. Modify this configuration as necessary.

## Configuring Ethernet Ports

```
WS5000>config<enter>
```

The system enters into the configuration mode and displays the following prompt:

```
WS5000.(Cfg)>
```

### To change Ethernet port 2 configuration:

```
WS5000.(Cfg)>Ethernet<enter>
```

The system enters into Ethernet configuration mode. To configure the Ethernet port parameters, enter the following:

```
WS5000.(Cfg).Ethernet> 2<enter>
```

Where: 2 is the port being configured. Only port 2 needs to be configured for this procedure.

### To disable DHCP:

```
WS5000.(Cfg).Ethernet.[2]>set dhcp disable<enter>
```

Symbol recommends assigning static IP addresses for Ethernet ports.

### To change the Ethernet port 2 IP address:

This step is required to manage the WS 5000.

```
WS5000.(Cfg).Ethernet.[2]>ipaddress <address><net_mask><enter>
```

Where: **<addres**s> is the IP address assigned to this port.

Where: **<net_mas**k> is the subnet mask for this port.

For example:

```
WS5000.(Cfg).Ethernet.[2]>ipaddress 192.168.123.102 255.255.255.0
```

### To configure a gateway:

```
WS5000.(Cfg).Ethernet.[2]>set gateway <address><enter>
```

Where: **<addres**s> is the IP address for the gateway device.

### To specify a DNS server:

```
WS5000.(Cfg).Ethernet.[2]>set dns <address><enter>
```

Where: **<addres**s> is the IP address of the DNS server.

## To verify information about an Ethernet port:

```
WS5000.(Cfg)>show ethernet 2<enter>
```

The system displays information about Ethernet port 2 (as opposed to port 1):

```
WS5000.(Cfg)> show ethernet 2
Name                        : Ethernet 2
Network Interface Card #    : 2
Description                 : Ethernet Adapter
MAC Address                 : 00:A0:xx:xx:xx:xx
Status                      : Enable
Online                      : Yes
Speed                       : 100
DHCP status                 : Disable
IP Address                  : 192.168.91.153
Network Mask                : 255.255.255.0
Port type (trunk/non-trunk) : Non-Trunk
VLAN Tags seen              : None
Up-Time                     : 00d:00h:16m
Transmit packets            : 852
Received packets            : 12783
Gateway details             :
        1. 192.168.91.2.
DNS details                 :
        1. 192.168.95.1.
        2. 192.168.95.229.

WS5000.(Cfg)>
```

After the Ethernet port has been configured and verified, type **exit** to return to the Console command prompt.

The switch installation is complete. The serial cable can be disconnected from the administrative PC. The next section describes a basic switch security policy configuration using the browser interface of a PC connected to the same subnet as Ethernet port 2 on the WS 5000.
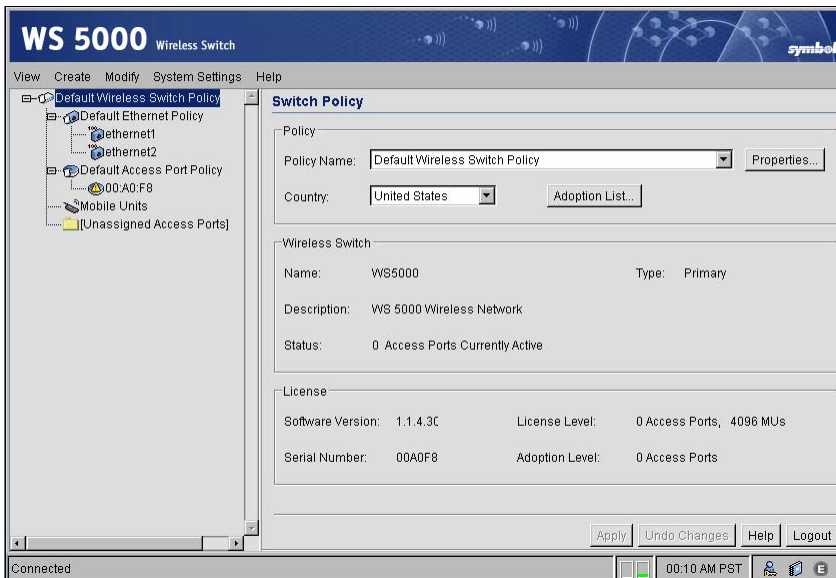
# Step 3: Creating a Policy Using the GUI

This step should take less than 15 minutes to complete. When you finish this step, the WS 5000 will be operating with a WEP 128 security policy.



The WS 5000 GUI simplifies creating policies. To use the GUI, start a web browser on a computer connected like the computer on the wired LAN in Figure 2. Direct the browser to the secure connection at 'https://nnn.nnn.nnn.nnn', (not http://) where nnn.nnn.nnn.nnn is the IP address of the Ethernet port 2 on the WS 5000. (In the example in "To change the Ethernet port 2 IP address:" this IP address is 192.168.123.102.) The browser should be able to connect immediately, and display the login screen as shown here.

Enter the User ID `admin`, and Password `symbol`. (Both are case-sensitive.) Then click the **Login** button. The WS 5000 main window appears.



On the left panel of this main window, notice that the *Default Wireless Switch Policy* (highlighted) includes a *Default Ethernet Policy*, which applies to both Ethernet ports, and a *Default Access Port Policy* which applies to any connected Access Ports.

This section will explain how to replace the Default Wireless Switch Policy and the Default Access Port Policy with a new switch-level WEP 128 policy. (The Default Ethernet Policy does not need to be changed.) To do this, users will need to create a Security Policy and define a WLAN that will use this new Security Policy. The policy wizard will guide the user through the procedures.

## Basic WS 5000 Configuration

The following steps to enable WEP 128 security for a new ESSID are simple yet powerful. The WS 5000 GUI can also be used to create a wide variety of complex network policies. Using the GUI to create these advanced policies requires a thorough understanding of concepts that are beyond the scope of this document. For a complete explanation of WS 5000 policies, see the *System Reference Guide* included on the WS 5000 CD.

These instructions apply to WS 5000s with the **Type** value set to **Primary**. If this WS 5000 is configured as **Standby**, no Access Ports will be adopted and no policies will be applied.
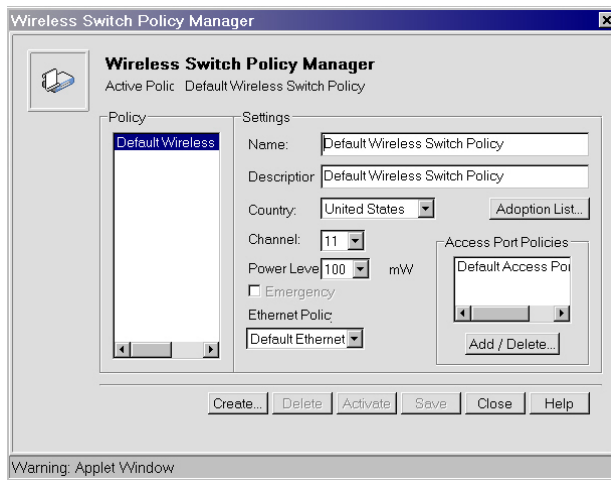
## To change the Type setting:

1. From the toolbar, select **System Settings** → **Standby Management…**

2. Click **Primary** for the Wireless Switch Mode selection.

3. Click **Apply**, then click **Close**.
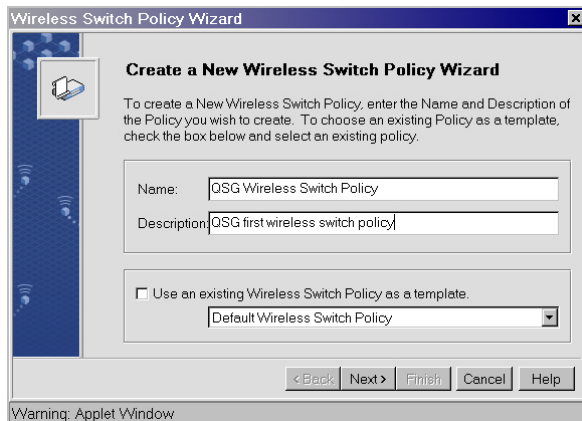
The main screen should now show the Type as **Primary**.

## To create a new WLAN and a security policy:

1. On the main WS 5000 window, select the *Default Wireless Switch Policy* from the tree view on the left panel of the main screen.

2. Click **Properties** on the upper right corner of the main screen. The *Wireless Switch Policy Manager* screen appears.



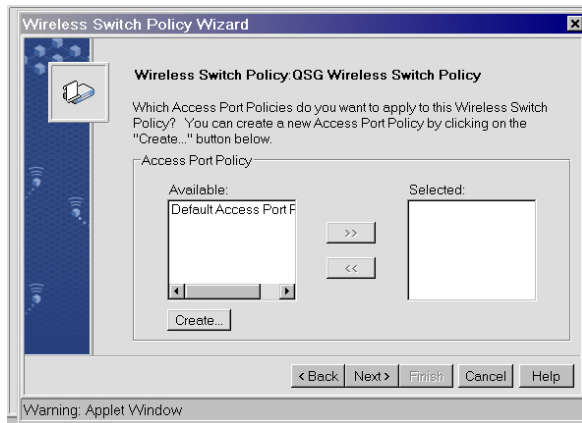3. From the *Wireless Switch Policy Manager* screen, click **Create.**

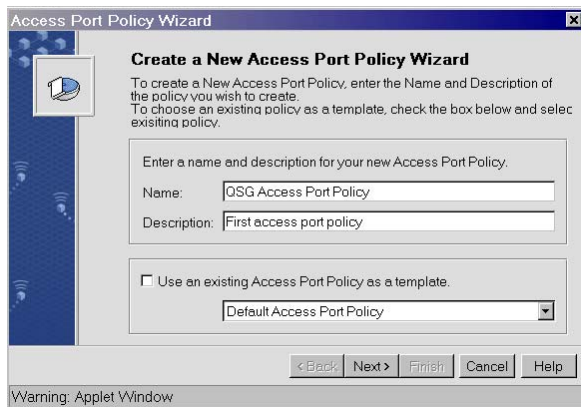   The *Create a New Wireless Switch Policy Wizard* screen appears.



4. On the *Create a New Wireless Switch Policy Wizard* screen, enter a **Name** and (optional) **Description** for the Wireless Switch policy. In this example, the Name is *QSG Wireless Switch Policy* and the Description is the *First wireless switch policy.* Click **Next** to display the *Wireless Switch Policy* screen.

7

5.  On the *Wireless Switch Policy* screen, select the appropriate **Country**. The Channel and Power Level settings adjust to the country selected.  Click **Next** to display available Access Port policies.
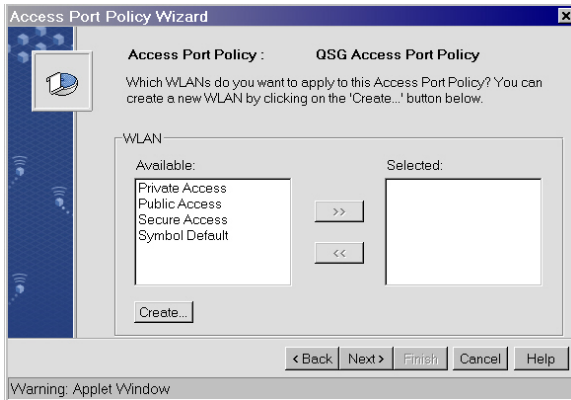


6.  On this Wireless Switch Policy screen, click **Create** to define a new Access Port policy. The *Create a New Access Port Policy Wizard* screen appears.
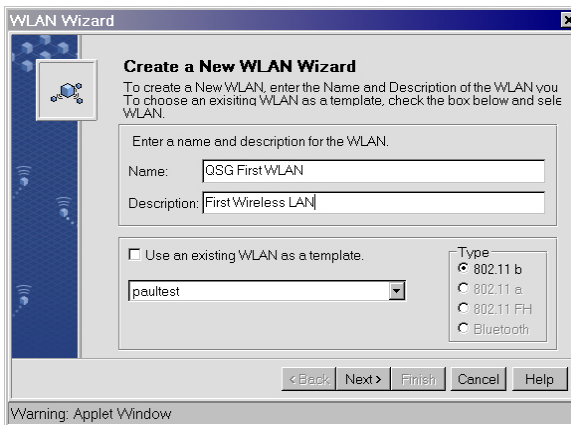


7.  On the *Create a New Access Port Policy Wizard* screen, enter a **Name** and (optional) **Description** for this Access Port policy. In this example, the Name is *QSG Access Port Policy* and the Description is *First access port policy*.

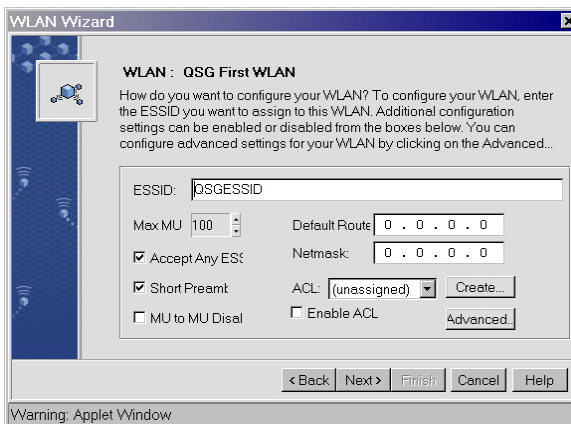    Click **Next** to start the process of creating a WLAN for this Access Port policy.

8

8. On this *Access Port Policy* screen, click **Create**. The *Create a New WLAN Wizard* screen appears.



9. On the *Create a New WLAN Wizard* screen, enter a **Name** and (optional) **Description** for this WLAN. For this example, the Name is *QSG First WLAN* and the Description is *First Wireless LAN*.

    Click **Next** to display the WLAN details screen.



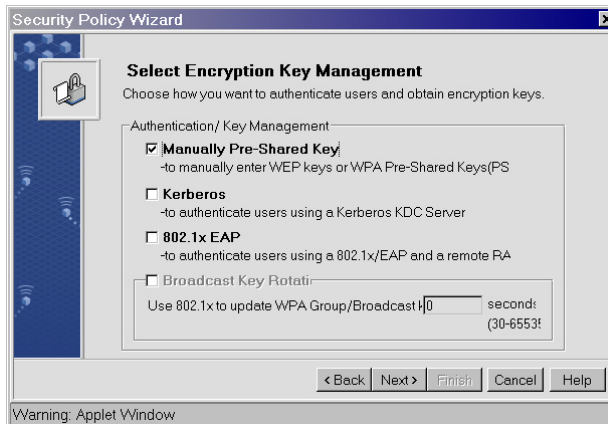10. Enter an **ESSID**. In this example, the ESSID is *QSGESSID*.

    Click **Next** to define the security policy for this WLAN.

11. On this WLAN screen click **Create** to define a new security policy. The *Create a New Security Policy Wizard* screen appears.



12. On the *Create a New Security Policy Wizard* screen, enter a **Name** and (optional) **Description** for this new security policy. In this example, the Name is *QSG First Security Policy* and the Description is *First security policy.*

13. Click the **WEP** checkbox to enable encryption of wireless traffic and click **Next**. The *Select Encryption Key Management* screen appears.



14. On this *Select Encryption Key Management* screen, click **Manually Pre-Shared Key** and click **Next** to display the *WEP Encryption Key Settings* screen.

15. For wireless clients using Symbol Technologies adapters, enter a **Pass Key** value and click **Generate**. Remember this Pass Key as it will be needed to configure wireless clients. Click **Next** and skip to step 17.
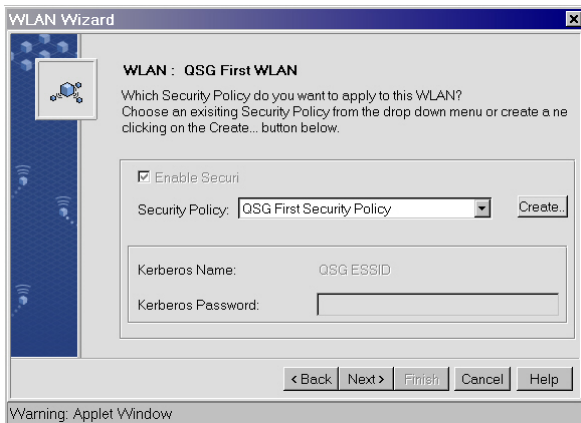


16. For wireless clients using non-Symbol Technologies adapters, enter a 26-character hexadecimal value for Key#1. Remember this 26-character value as it will be needed to configure wireless clients. Click **Next** to display the Security Policy confirmation screen.



17. From this Security Policy confirmation screen, click **Finish** to save the policy and exit the Security Policy Wizard and display the *WLAN Wizard* screen. The newly created security policy will now be attached to the WLAN.

18. From the *WLAN Wizard* screen,
    select the security policy just created.
    In this example, this is *QSG First
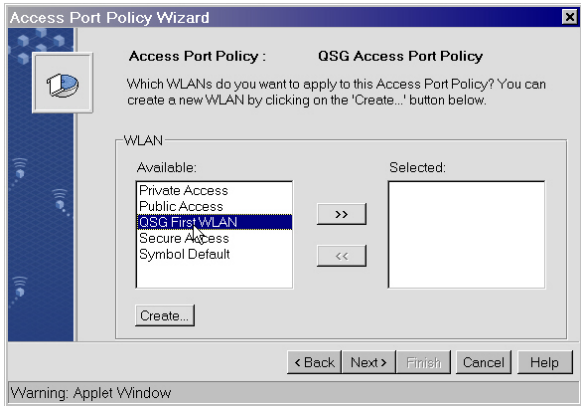    Security Policy*.  Click **Next** to display
    the next WLAN Wizard screen.



19. From this WLAN Wizard screen, click
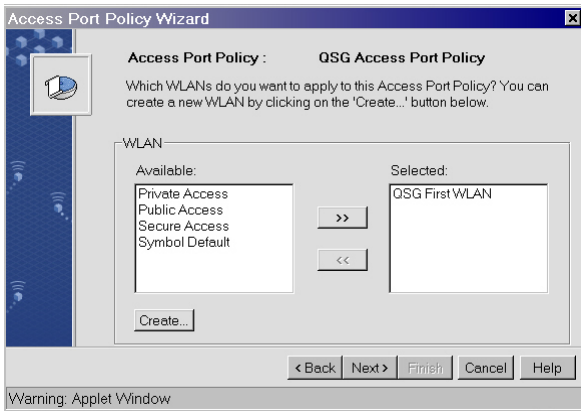    **Next** to display the WLAN creation
    confirmation screen.



20. From this WLAN Wizard confirmation
    screen, click **Finish** to save the
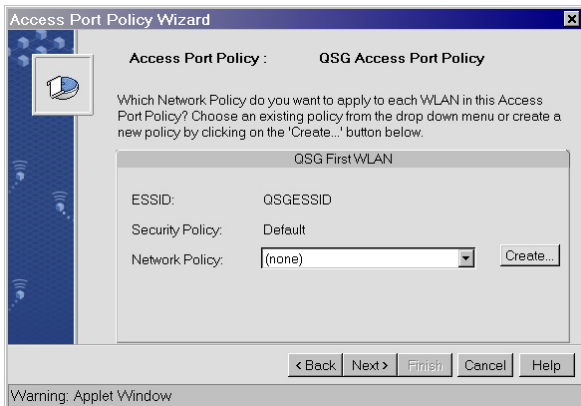    WLAN policy and exit the WLAN
    Wizard.

    The *Access Port Policy Wizard*
    screen appears which allows the
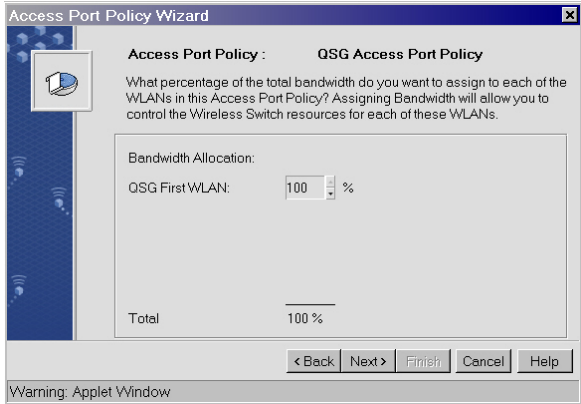    newly created WLAN to be attached
    to the Access Port policy.

12

21. On the *Access Port Policy Wizard* screen, select the WLAN policy just created and click the **>>** button to move the policy from the Available box to the Selected box. The *Access Port Policy Wizard* screen redisplays showing the WLAN policy in the Selected box.
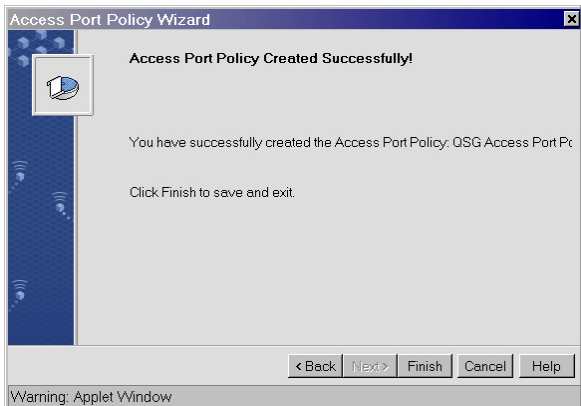


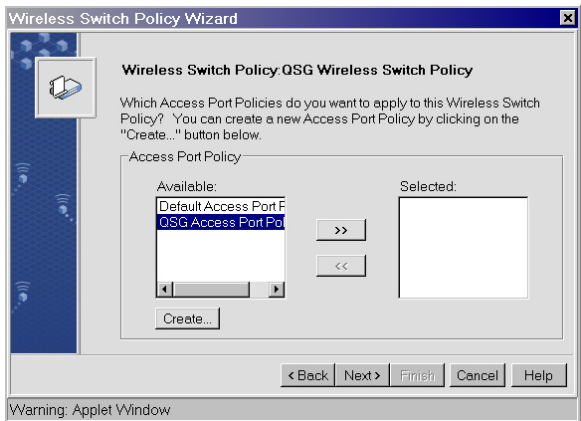22. From this *Access Port Policy Wizard* screen, click **Next** to apply the Network Policy to this WLAN.



23. Click **Next** without making any changes to the settings on this *Access Port Policy Wizard* screen. The Bandwidth Allocation screen appears.
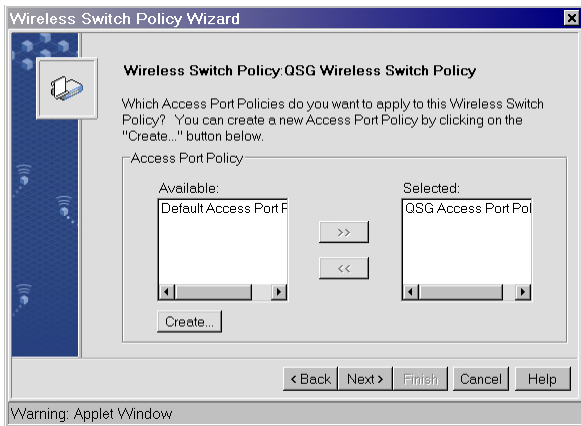
13

24. Click **Next** without making any changes to the bandwidth settings on this *Access Port Policy Wizard* screen. The Access Port Policy confirmation screen appears.



25. On the Access Port Policy confirmation screen, click **Finish** to save this Access Port policy and exit the Access Port Policy Wizard. The *Wireless Switch Policy Wizard* screen appears to allow the newly created Access Port Policy to be attached to the switch policy.



26. From the *Wireless Switch Policy Wizard* screen, select the Access Port Policy just created (in this example, *QSG Access Port Policy*) and click the **>>** button to move the policy from the Available box to the Selected box. The *Wireless Switch Policy Wizard* screen redisplays showing the Access Port Policy in the Selected box.
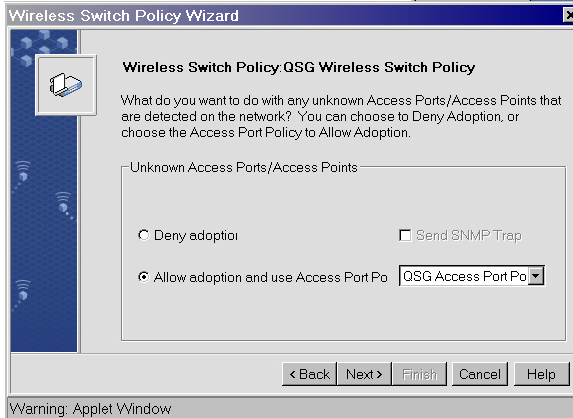
14

27. From this Wireless Switch Policy Wizard screen, click **Next** to display the *Adoption List Allow* screen.



28. Click **Next** without making any changes to this *Wireless Switch Policy Wizard* screen. The *Adoption List Disallow* screen appears.
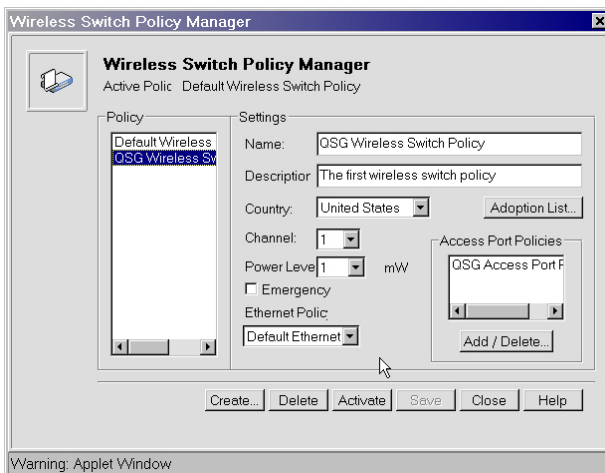


29. Click **Next** without making any changes to this *Wireless Switch Policy Wizard* screen. The *Unknown Access Ports/Access Points* screen appears.

15

30. Click the **Allow adoption and use Access Port Policy** button and click **Next** to display the Wireless Switch Policy confirmation screen.
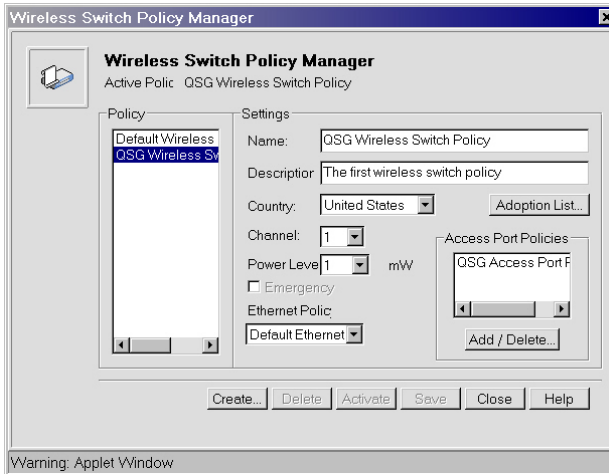


31. From this Wireless Switch Policy confirmation screen click **Finish** to save this Wireless Switch policy and exit the Wireless Switch Policy Wizard. The *Wireless Switch Policy Manager* screen appears.
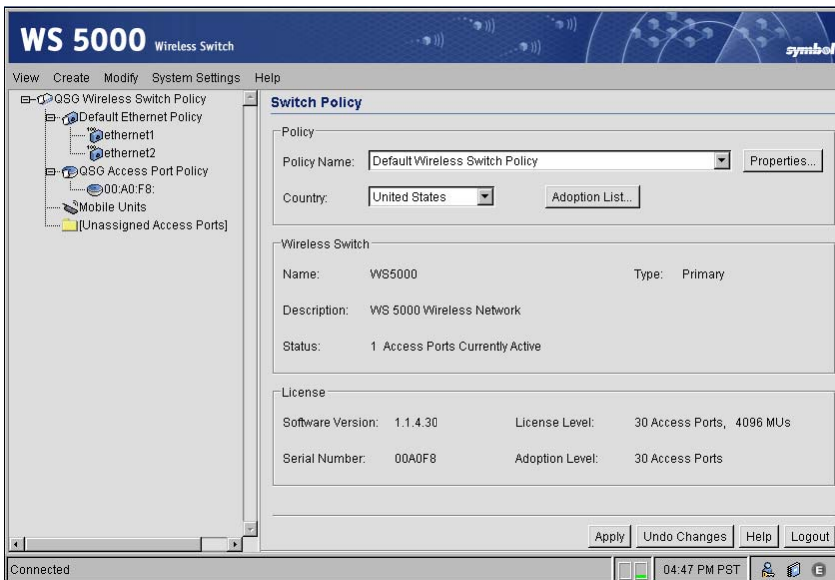


32. From the *Wireless Switch Policy Manager* screen, select the Wireless Switch Policy just created (in this example, *QSG Wireless Switch Policy*) and click **Activate**. A warning box appears.

33. From the Warning box, click **OK**. The *Wireless Switch Policy Manager* screen reappears.
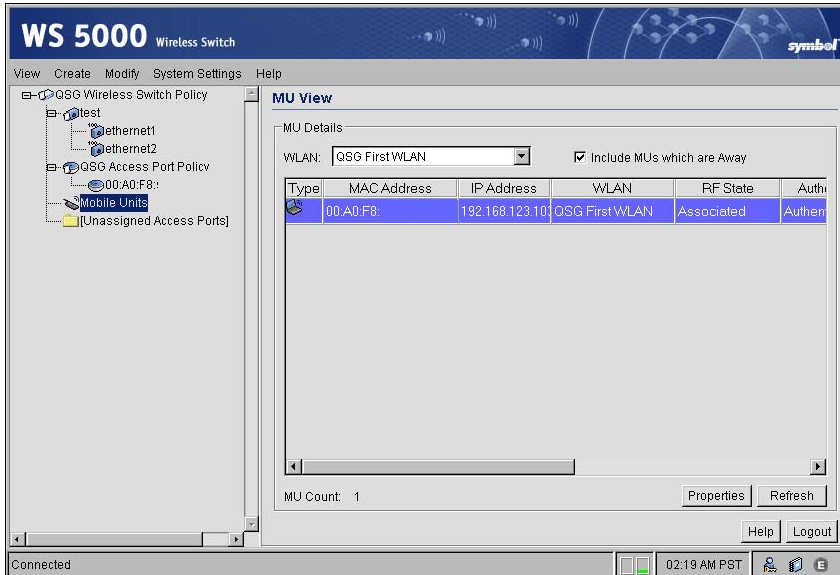


34. From the *Wireless Switch Policy Manager* screen, click **Close**. The WS 5000 main screen reappears.
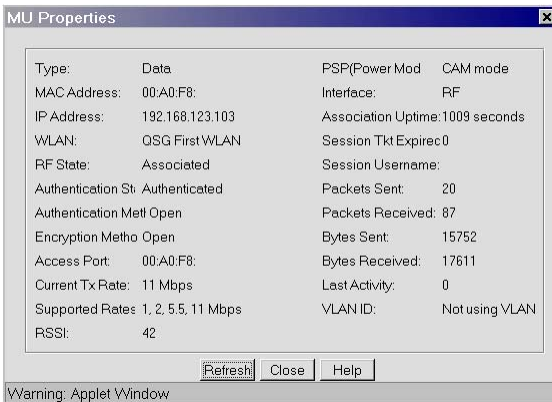


35. Notice that the policy tree on the left panel of the WS 5000 main screen shows the new policy (*QSG Wireless Switch Policy*), which makes WEP 128 active for this WS 5000 (and all attached Access Ports and Mobile Units). Notice that the new switch-level policy also includes the newly created QSG Access Port Policy, which in turn controls the *QSG First WLAN* policy with the new ESSID.

## To verify that the new policy is working:

1. Reconfigure wireless clients to match these new settings (ESSID, etc.) as shown in Figure 2.

2. Reissue the ping test done in "Verifying the Connections" to confirm that a wireless client can still reach the wired LAN. Or, use the GUI to confirm connectivity with mobile units. To verify the connectivity of mobile units using the GUI, click **Mobile Units** (highlighted) on the left panel of the WS 5000 main screen (shown below). The *MU View* screen appears.



3. Select a mobile unit and click **Properties**. The *MU Properties* screen appears.



From the *MU Properties* screen, the identity and connection status of the selected mobile unit can be verified. Notice the wide variety of identification, status, and traffic information available for this mobile device.

# Conclusion

The WS 5000 is now fully operational and secured with WEP 128. No additional configuration is required unless desired. To create additional policies, refer to the *System Reference Guide* on the CD included with this WS 5000.