About This Guide

Introduction

This guide provides information for those familiar with using the 1.4.x and 2.x version WS5100 switch software who require orientation to the new WS5100 3.0 switch features and functionality.

- **NOTE**  Screens and windows pictured in this guide are samples and can differ from actual screens.

Documentation Set

The documentation set for the WS5100 Series Switch is partitioned into the following guides to provide information for specific user needs.

- **WS5100 System Reference Guide** - describes advanced setup and configuration activities for all facets of the WS5100 Series Switch.
- **WS5100 Installation Guide** - describes the basic setup and configuration required to transition to more advanced configuration of the switch.
- **WS5100 CLI Reference** - describes the Command Line Interface (CLI) and Management Information Base (MIB) commands used to configure the WS5100 Series Switch.
- **WS5100 Troubleshooting Guide** - describes workarounds to known conditions the user may encounter.

Document Conventions

The following conventions are used in this document to draw your attention to important information:

- **NOTE**  Indicate tips or special requirements.

- **CAUTION**  Indicates conditions that can cause equipment damage or data loss.
Notational Conventions

The following additional notational conventions are used in this document:

- **Italics** are used to highlight the following:
  - Chapters and sections in this and related documents
  - Dialog box, window and screen names
  - Drop-down list and list box names
  - Check box and radio button names
  - Icons on a screen.

- **GUI** text is used to highlight the following:
  - Screen names
  - Menu items
  - Button names on a screen.

- bullets (•) indicate:
  - Action items
  - Lists of alternatives
  - Lists of required steps that are not necessarily sequential

- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.
# Chapter 1. Overview

# Chapter 2. Switch Web UI and Image Upgrades

- Accessing the Switch Web UI ................................................................. 2-1
  - Web UI Requirements ................................................................. 2-1
  - Connecting to the Switch Web UI ............................................... 2-2
- Switch Password Recovery ................................................................. 2-3
  - Recovering the Switch Password using the Web UI ....................... 2-3
  - Recovering the Switch Password using the CLI ............................... 2-4
- Shutting Down the Switch ............................................................... 2-5
  - Shutting Down the Switch using the 1.4.x/2.x Shutdown Command ........ 2-5
  - Shutting Down the Switch using the 3.0 Halt Command ................. 2-6
- Upgrading the Switch Image ............................................................ 2-7
  - Upgrading the Switch Image from 1.4.x or 2.x to Version 3.0 ........ 2-7
  - Downgrading the Switch Image from Version 3.0 to 1.4.x or 2.x ....... 2-8

# Chapter 3. Use Cases

- Tempest University’s Hotspot Deployment ........................................ 3-1
- Tempest University’s Current WS5100 Configuration ......................... 3-2
- Migrating the Existing Configuration to the 3.0 Baseline .................. 3-2
  - Migrating Up to the 3.0 Baseline ............................................... 3-3
  - Porting a WS5100 2.0 Configuration to a 3.0 Migrated WS5100 ........ 3-4
  - Configure New Hotspots on Campus ........................................... 3-4
- Configuring a Windows 2003 IIS Server for Hotspot Support ............. 3-14
  - IIS Server Configuration .......................................................... 3-17
  - Sample HTML Pages / CGI Script for External Hotspots ............... 3-18
- Use Case: Remote VPN ................................................................. 3-20
  - Network Overview ................................................................. 3-20
  - Configuring DHCP Server to serve public IP addresses .................. 3-21
    - Adding a New DHCP Pool ....................................................... 3-21
    - Adding a New DHCP Pool ....................................................... 3-22
  - Configuring Crypto Policy (IKE) ............................................... 3-22
    - Create IKE Policies ............................................................. 3-23
    - Configure Pre-Shared Keys .................................................... 3-24
    - Enable or Disable IKE .......................................................... 3-25
  - Set Global Lifetimes for IPSec Security Associations ...................... 3-25
Define Transform Sets ........................................ 3-25
Create Client Related Mode Configuration (Remote Access VPN) ............ 3-25
Configuring IPSec Security Associations (Crypto Map) ...................... 3-26
  Creating An Entry for Establishing Manual Security Associations .... 3-26
  Creating An Entry that Uses IKE to Establish Security Association .. 3-27
Apply Crypto Map Sets to Interfaces ................................... 3-27
Monitor and Maintain IPSec Tunnels ..................................... 3-27
Network Address Translation in IPSec ..................................... 3-27

Chapter 4. Web UI Menu Path Comparison
Web UI Menu Path Navigation ............................................. 4-2
  High-Level Device Information ....................................... 4-2
  Configuring the System Time (NTP) Settings ............................ 4-3
  Managing Software, Configuration and Log Files ...................... 4-3
    WS5100 Switch Firmware ............................................ 4-3
    WS5100 Switch Configuration Files ................................ 4-4
    WS5100 Log Files ................................................... 4-5
VLAN Configuration ....................................................... 4-6
Configuring Switch Security ................................................ 4-7
  ACL Configuration ..................................................... 4-7
  Encryption and Authentication ....................................... 4-9
  Rouge AP Detection ................................................... 4-12
  Configuring the On-Board Radius Server ................................ 4-13
Viewing Switch Statistics .................................................. 4-15
Switch Certificate Management ............................................ 4-17

Chapter 5. WS5100 LED Behavior Comparison
WS5100 1.4.x and 2.x Baseline LED Behavior ................................ 5-2
  Start Up ............................................................... 5-2
  Configured as a Primary Switch ..................................... 5-2
  Configured as a Standby Switch .................................... 5-2
  Error Codes ......................................................... 5-2
WS5100 3.0 LED Behavior .................................................. 5-3
  Start Up ............................................................... 5-3
  Primary ............................................................... 5-3
  Standby .............................................................. 5-3
  Error Codes .......................................................... 5-4
This WS5100 Series Switch Migration Guide is designed to provide users familiar with the 1.4.x and 2.x switch baselines an overview of the significant changes to the switch Web UI and switch LED activity. The Web UI used for the new 3.0 baseline shares almost no similarities with the applet used in previous releases. Therefore, Symbol recommends you familiarize yourself with the following content to make your WS5100 3.0 configuration activity more effective.

- Switch Web UI and Image Upgrades
- Use Cases
- Web UI Menu Path Comparison
- WS5100 LED Behavior Comparison
With the release of the 3.0 version of the WS5100 Series Switch the switch user interface is no longer called the switch Web UI within Symbol’s end-user documentation. The user interface going forward from the 3.0 release is now called the Web UI. It is still launched the same from a Web browser using the IP address assigned to the switch’s wired Ethernet port.

2.1 Accessing the Switch Web UI

2.1.1 Web UI Requirements

The switch Web UI is accessed using Internet Explorer version 5.5 (or later) and SUN JRE (Java Runtime Environment) 1.5 (or later). Refer to the Sun Microsystems Web site for information on downloading JRE.

To prepare Internet Explorer to run the Web UI:

1. Open IE’s Tools > Internet Options panel and select the Advanced tab.
2. Uncheck the following checkboxes:
2.1.2 Connecting to the Switch Web UI

To display the Web UI, launch a Web browser on a computer with the capability of accessing the switch.

NOTE Ensure you have HTTP connectivity to the switch, as HTTP is a required to launch the switch Web UI from a browser.

To display the switch Web UI:

1. Point the browser to the IP address assigned to the wired Ethernet port (port 2). Specify a secure connection using the https:// protocol.

   The switch login screen displays:

   Enter User ID and Password.
   User ID: admin
   Password: ********
   Login

2. Enter the User ID admin, and Password superuser. Both are case-sensitive. Click the Login button.

   NOTE If using HTTP to login into the switch, you may encounter a Warning screen if a self-signed certificate has not been created and implemented for the switch. This warning screen will continue to display on future login attempts until a self-signed certificate is implemented. Symbol recommends only using the default certificate for the first few login attempts until a self-signed certificate can be generated.
Switch Web UI and Image Upgrades

Once the Web UI is accessed the Switch main menu item displays a configuration tab with high-level switch information. Click the Show Dashboard button to display an overall indicator of switch health. Once the switch is fully configured, the dashboard is the central display for the user to view the version of firmware running on the switch, quickly assess the last 5 alarms generated by the switch, view the status of the switch’s Ethernet connections and view switch CPU and memory utilization statistics.

2.2 Switch Password Recovery

With the release of the 3.0 version switch software, your Web UI login password can be recovered, but at the expense of updates you have made to your configuration file since the default image was updated.

If the switch Web UI password is lost, you cannot get passed the Web UI login screen for any viable switch configuration activity. Consequently, a password recovery login must be used that will default your switch back to its factory default configuration. The switch password can be recovered using either the Web UI or the switch CLI.

If you know your existing password and wish to change it, go to the Switch main menu item, select the Configuration tab and click the Reset Password button. A screen displays prompting for the existing password and the new password.

2.2.1 Recovering the Switch Password using the Web UI

To access the switch using a password recovery username and password:

1. Point the browser to the IP address assigned to the wired Ethernet port (port 2).

   The switch login screen displays:

2. Enter a password recovery username of restore and password recovery password of restoreDefaultPassword. Click the Login button.
The switch will login into the Web UI with its reverted default configuration. If you had exported the switch’s previous configuration to an external location, it now can be imported back to the switch. For information on importing switch configuration files, see Transferring a Config File on page 3-18.

2.2.2 Recovering the Switch Password using the CLI

To access the command line interface and using a password recovery username and password:

---

**CAUTION** Using this recovery procedure erases the switch’s current configuration and data files from the switch /flash dir. Only the switch’s license keys are retained. You should be able to log in using the default username and password (admin/superuser) and restore the switch’s previous configuration (only if it has been exported to a secure location before the password recovery procedure was invoked).
---

1. Connect to the CLI using either Telnet, SSH or a Serial cable. You should see the following:
   
   Please press Enter to activate this console.

2. Press Enter and enter cli at the login prompt.

   WS5100 login: cli

3. Once you enter the User Access Verification. Enter the username restore and press Enter.

   User Access Verification
   Username: restore
   
   When prompted to enter a password enter restoreDefaultPassword and press Enter. For security reasons the password you enter is not displayed.

   Password:

4. When the warning prompt appears type y and press Enter. The following will display:

   WARNING:This will wipe out the configuration (except license key) and user data under "flash:"/" and reboot the device
   
   Do you want to continue? (y/n):y

   Switch will be rebooted with default configuration...
   The system is going down NOW !!

5. Once the switch has rebooted login using the default username and password.
2.3 Shutting Down the Switch

The CLI commands used to shutdown the switch have changed with the release of the 3.0 version WS5100 Series Switch. Please refer to the following to differentiate between the shutdown command (1.4.x and 2.x) from the halt command (3.0).

2.3.1 Shutting Down the Switch using the 1.4.x/2.x Shutdown Command

To gracefully shutdown the WS5100, issue the `shutdown` command from the configure context in the CLI:

```
WS5000.(Cfg)> shutdown
This command will halt the system.
A manual power cycle will be required to re-start the switch.
Do you want to proceed (yes/no) : yes

System shut down might take a few mins....
Shutting down the switch...
Shutting down dhcp daemon.. done
Shutting down apache server in the OPEN mode...done.
Shutting down cell controller........ done
Shutting down snmpd agent...done.
Shutting down Postgres....done.
INIT: Sending processes the TERM signal
Shutting down PacketSwitch interface ..... 
Shutting down dhcp daemon.. done
Shutting down apache server in the OPEN mode...done.
Cell controller not running.
i2c-core: Device or resource busy
Shutting down Postgres....done.
Stopping periodic command scheduler: cron.
Stopping internet superserver: inetd.
Saving random seed... done.
Stopping deferred execution scheduler: atd.
Stopping kernel log daemon: klogd.
Stopping system log daemon: syslogd.
flushing ide devices: hda
System halted.
```

As directed, wait 10 seconds and turn off the device by toggling the power switch.
2.3.2 Shutting Down the Switch using the 3.0 Halt Command

To shut down the WS5100 from the CLI, issue a `halt` command, as the `halt` command is now used to shut down the WS5100 Series Switch with the release of the 3.0 version WS5100 baseline:

```
WS5100#halt
Wireless switch will be halted, do you want to continue? (y/n):y
The system is going down NOW !!

% Connection is closed by administrator!
WIOS_SECURITYMGR[395]: DNSALG: Shutting down.
WIOS_SECURITYMGR[395]: FTPALG: Shutting down.
The system is halted.
```

**NOTE** The WS5100 will power off after issuing a `halt` command through a software toggle of the power supply. Be sure to flip the power switch to the Off position. If the power cord is removed and reinstalled, or power is lost and restored, the switch will power back on.
2.4 Upgrading the Switch Image

The WS510 Series Switch ships with a factory installed firmware image with the full feature functionality described in this System Reference Guide. However, Symbol periodically releases switch firmware that includes enhancements or resolutions to known issues. Verify your current switch firmware version with the latest version available from the Symbol Web site before determining if your system requires an upgrade.

Additionally, legacy users running either the 1.4.x or 2.x version switch firmware may want to upgrade to the new 3.0 baseline to take complete advantage of the new diverse feature set available to them. This chapter describes the method to upgrade from either the 1.4.x or 2.x baseline to the new 3.0 baseline.

### 2.4.1 Upgrading the Switch Image from 1.4.x or 2.x to Version 3.0

To upgrade a switch running either a 1.4.x or 2.x version to the latest 3.0 version switch firmware:

1. Execute the PreUpgradeScript utility (or use the CLI) to ensure there is enough space on your system to perform the upgrade. The PreUpgradeScript utility should be in the same directory as the upgrade files.

2. Install the Cfgupgrade1.x-setup utility on a Windows desktop system by double clicking the Cfgupgrade 1.x-setup file. Follow the prompts displayed by the installer to install Cfgupgrade 1.x-setup.

A WS5100 Configuration Upgrade icon gets created within the Program Files folder. The icon can be optionally created on your Windows desktop as well.

3. From the WS5100 running either 1.4.x or 2.x, create a configuration and save it on the switch.

   ```
   WS5100# save <file name> <.cfg>
   ```

   This is the configuration that will be upgraded to the new 3.0 baseline.

### CAUTION

Symbol recommends caution when upgrading your WS5100 switch image to the 3.0 baseline as portions of your configuration will be lost and unrecoverable. Ensure that you have exported your switch configuration to a secure location before upgrading your switch. The upgrade.log file will contain a list of the issues found in the conversion of the configuration file to the new format.

### CAUTION

If using a 1.4.x or 2.x admin user password shorter than 8 characters (such as the default symbol password), the password will be converted to the 3.0 baseline admin password of “password” upon a successful update to the 3.0 baseline. Ensure your existing 1.4.x or 2.x admin password is longer than 8 characters before updating, or leave as is and use “superuser” to login into an updated 3.0 baseline.

### CAUTION

After upgrading the switch baseline from 1.4.x or 2.x to the 3.0 baseline, applet caching can produce unpredictable results and contents. After the upgrade, ensure your browser is restarted. Otherwise, the credibility of the upgrade can come into question.

### NOTE

Symbol recommends saving a copy of the switch configuration to a secure location before the upgrade. If an error occurs with the upgrade a viable configuration will be needed to restore on the switch.
4. Copy the configuration file <.cfg> from the legacy WS5100 to the Windows system where the conversion utility resides.
   Use ftp or tftp to transfer the file.
5. Click on the **WS5100 configuration Upgrade** icon (from the Windows system).
6. Select the config file copied on to the windows system and run it.
   A folder having the same name as the config file is created. The folder contains the converted startup-config file (in the new upgraded format) along with other log files.
7. Copy the startup-config file back to the WS5100 running using either tftp or ftp.
8. Download or copy the image file <WS5100-3.0.0.0-XX.v1> or <WS5100-3.0.0.0-XX.v2> to the WS5100 running the legacy switch firmware.

9. On the WS5100, type:
   ```
   WS5100#service
   WS5100#password "password"
   exec
   ```
   Upon reboot, the switch runs the 3.0 image using startup-config as the running configuration.
10. Repeat the instructions above for additional switch upgrades, ensuring
    <WS5100-3.0.0.0-XX.v1> is used for 1.4.x version upgrades, and
    <WS5100-3.0.0.0-XX.v2> is used for 2.x version upgrades.

### 2.5 Downgrading the Switch Image from Version 3.0 to 1.4.x or 2.x

If for some reason you want to downgrade your WS5100 back down to a 1.4.x or 2.x version firmware image, use one of the two following image files:

- WS5100-1.4.3.0-012R.img
- WS5100-2.1.0.0-029R.img
3.1 Tempest University’s Hotspot Deployment

This chapter presents a use case illustrating the challenges faced by Tempest University when migrating their existing WS5100 2.x implementation to the new WS5100 3.0 baseline.

Tempest University (inaugurated in 1993) has grown rapidly in recent years and is one of the most popular universities in Ireland. The university has approximately 18,000 students, but has increased its student enrollment applications 70% in the last three years.

With this expanding student population in mind, the Tempest University IT department needed to provide its students a flexible and convenient means to access their wireless infrastructure. The University purchased 1500 wired PCs for student access in fixed areas, but faced the problem of providing students wireless access to the university’s network using mobile devices connecting to the campus WLAN.

The University required a system that could be easily administered, secure and be relocated as their campus grew. The IT department determined a wireless switch system would significantly lower the cost of deploying a scalable network infrastructure and drive down the cost of managing, maintaining and upgrading wireless systems as the student population and number of mobile users grew.
The University decided to standardize on Symbol’s WS5100 and AP300 Access Port. The first switches and access ports were deployed at the University network in December 2002 and the system provided students with wireless networking speeds of up to 54 Mbps.

Free from the constraints of cables, the new WS5100 managed WLAN allowed student network access from seminar rooms, lecture theatres, student unions and other areas across campus. In addition, the WS5100 deployment allowed the University to increase the computer-to-students ratio without having to dedicate additional (and expensive) floor space to fixed PCs.

### 3.2 Tempest University’s Current WS5100 Configuration

Tempest University currently deploys the following WS5100 configuration:

- Five primary WS5100 switches (running the 2.x baseline) backed by an additional five switches for redundancy.
- 400 AP300 Access Ports to support the 1500 PCs receiving wireless radio coverage around the campus.
- EAP support on each switch with 5 switches configured as masters and the remaining 5 configured as slaves.

### 3.3 Migrating the Existing Configuration to the 3.0 Baseline

Tempest University wants to update their switches to the new Symbol 3.0 baseline, add support for its increasing student population and create hotspots strategically on campus that optimize data, video and wireless traffic depending on the requirement for specific campus segments. Specific challenges include:

- Adding wireless support for an additional 1500 students in addition to the existing 1500 on wired PCs. Adding the 1500 students constitutes migrating the existing 2.0 configuration to the 10 existing switches, then adding 5 new WS5100 switches and moving the newly created WS5100 3.0 configuration to the 5 new switches.
- Create new hot spots on campus. Some hot spots are intended to cover a single large room, others cover complete buildings (to support separate departments on campus). The new hot spot implementation would allow students more flexibility to conduct research, access the internet, check email and obtain files from their respective departments using their own laptops or PDAs.
3.3.1 Migrating Up to the 3.0 Baseline

Tempest University is required to migrate each of its existing ten WS5100s to the new 3.0 baseline to optimize the 3.0 feature set to achieve its goals for expanding their coverage area and utilizing the 3.0 feature set.

NOTE  Migrating the 2.0 baseline up to the 3.0 baseline does not preserve the switch's previous 2.0 configuration. Consequently, the IT Department at Tempest University must save each switch's existing configuration and port it to the new 3.0 baseline as a separate activity from the switch operating system migration.

To migrate up to the 3.0 baseline, the Tempest University IT department completes the following:

CAUTION  Symbol recommends caution when upgrading the WS5100 switch image to the 3.0 baseline as portions of your configuration will be lost and unrecoverable. Ensure that you have exported your switch configuration to a secure location before upgrading your switch.

2. Install the utility on a Windows desktop system by double clicking the Cfgupgrade 1.0-setup file. Follow the prompts displayed by the installer to install Cfgupgrade 1.0-setup.
   A WS5100 Configuration Upgrade icon gets created within the Program Files folder. The icon can be optionally created on your Windows desktop as well.
3. From the WS5100 running 2.x, create a configuration and save it on the switch.
   WS5100# save <file name> <.cfg>
   This is the configuration that will be upgraded to the new 3.0 baseline.

NOTE  Symbol recommends saving a copy of the switch configuration to a secure location before the upgrade. If an error occurs with the upgrade a viable configuration will be needed to restore on the switch.

4. Copy the configuration file <.cfg> from the legacy WS5100 to the Windows system where the conversion utility resides.
   Use ftp or tftp to transfer the file.
5. Click on the WS5100 configuration Upgrade icon (from the Windows system).
6. Select the config file copied on to the windows system and run it.
   A folder having the same name as the config file is created. The folder contains the converted startup-config file (in the new upgraded format) along with other log files.
7. Copy the startup-config file back to the WS5100 running using either tftp or ftp.
8. Download or copy the image file <WS5100-3.0.0-XX.v2> to each WS5100 running the 2.x legacy switch firmware.

NOTE  If upgrading a 2.x version WS5100 to the new 3.0 baseline, be sure you are using the <WS5100-3.0.0-XX.v2> image file.

9. On WS5100 running the legacy switch firmware, type:
WS5100#service
WS5100#password "password"
exec

Upon reboot, the switch runs the 3.0 image using startup-config as the running configuration.

10. Tempest University repeats the instructions above for each switch upgrade, ensuring `<WS5100-3.0.0.0-XX.v2>` is used for 2.x version upgrades.

| NOTE | Once each Tempest University switch has been migrated up to the 3.0 baseline, each switch is ready to have its configuration ported from the 2.x baseline to the 3.0 baseline. |

### 3.3.2 Porting a WS5100 2.0 Configuration to a 3.0 Migrated WS5100

Configuration upload tool currently not available (3-31-06)

### 3.3.3 Configure New Hotspots on Campus

Tempest University wants to extend its WLAN access to students in various parts of the campus to provide Internet hotspot access using their existing wireless infrastructure (WS5100 + AP300). Security requirements in extending the guest access include separating the secured corporate WLAN from the less secure hotspot WLAN and limiting student access to Web browsing the Internet and student periodical resources only. FTP, Telnet and all other applications will be blocked.

The Tempest University IT team wishes to deploy the hotspots with each hotspot using the external hotspot option using Windows 2003 IIS servers + WS5100 Onboard Radius servers with the built-in user database. The team will use the switch Web UI to configure the hotspots.

| NOTE | The Tempest University IT team plans to develop hotspot supported WLANs for different academic areas and gathering areas on campus. Though each hotspot will share numerous attributes, there will be subtle differences between them, as certain user populations will be included (excluded) from accessing the resources within specific hotspots. The Tempest University IT team will begin by developing a hotspot for the Humanities area. Once completed with this initial example, the team will define additional hotspots to support the entire campus. |

The Tempest University IT team wants to begin by creating a VLAN interface for use with the hotspot supported Humanities WLAN.
1. The Tempest University IT team selects **Network > Switch Virtual Interface** from the main menu tree and ensures the **Configuration** tab is selected.

2. The team clicks the **Add** button to create a new switch virtual interface.

3. The team assigns a **VLAN ID** of 101. The team wants IP address assignments to be made automatically, so the **Use DHCP to obtain IP Address automatically** checkbox is selected. With these changes made, the team clicks the **OK** button.

   The Tempest University IT team is now ready to define a VLAN for use with the WLAN the team will eventually configure. for the hotspot enabled WLAN.

4. The Tempest University IT team selects **Network > Layer 2 Virtual LANs** from the main menu tree.
5. The Tempest University IT team highlights eth2 (from within the Name column) and clicks the Edit button. A Port VLAN Change Warning message displays. The team clicks OK to continue.

6. The Tempest University IT team selects Trunk from the Mode drop-down menu. The Selected VLANs option becomes available for additions.

7. The Tempest University IT team adds VLAN 101 to the Selected VLANs listed (separated by a comma). The team clicks OK to continue. The Tempest University IT team is now to create an IP Extended ACL for the hotspot. This step is recommended for hotspot developers but can be skipped.

8. The Tempest University IT team selects Security > ACLs from the main menu tree, and clicks the Add button within the Configuration tab.
9. The Tempest University IT team selects **Extended IP List** from the **ACL Type** drop-down menu. This option uses source and destination IP addresses and an optional protocol type.

10. The Tempest University IT team enters a **ACL ID** of 2000. This is the ID to be used specifically for the Humanities Department ACL. The team clicks **OK** to continue.

11. The Extended IP List 2000 displays in the list of ACLs. The Tempest University IT team highlights the Extended IP List 2000 by selecting it and then clicks **Add** from the Associated Rules field to display the **Add Rule** sub screen.

12. The Tempest University IT team defines a Precedence of 1 and permit designation for the ACL.
13. With the changes complete, the Tempest University IT team clicks OK to continue. The Tempest University IT team is now ready to apply the ACL to the VLAN interface created for the Humanities department hotspot.

14. From the ACLs screen the team selects the Attach tab and clicks the Add button.

15. The Tempest University IT team selects (the previously configured values) of **vlan 101** from the Interface drop-down menu and the ACL ID of **2000** from the IP ACL drop-down menu. OK is then selected to continue. The Tempest University IT team is now ready to create a hotspot enabled WLAN for the Humanities department hotspot.
16. The Tempest University IT team selects **Network > Wireless LANs** from the switch main menu tree.

17. The IT team selects an available ESSID (not already enabled) and clicks the **Edit** button at the bottom of the screen.

18. The Tempest University IT team changes the ESSID to **Humanities Hotspot**.

   It is the team’s plan to assign an ESSID to each hotspot representative of where the target hotspot is to be deployed on campus.

19. The Tempest University IT team changes the VLAN ID to 101.
20. The Tempest University IT team selects Hotspot from the Authentication options. The team is now ready to define the properties of the external hotspot’s configuration.
21. The Tempest University IT team clicks the **Config** button next to the hotspot authentication item.

![Network > Wireless LANs > Edit > Hotspot](image)

22. The Tempest University IT team selects **External** from the drop-down menu and enters the URL locations for the 3 HTML pages as displayed above.

```plaintext
NOTE
For information on enabling an External Web Server, see Configuring a Windows 2003 IIS Server for Hotspot Support on page 3-14. For sample HTML Page/CGI Script content, see Sample HTML Pages / CGI Script for External Hotspots on page 3-18.
```

23. The Tempest University IT team references the **Allow List** to enter an IP address for the Humanities department Web site (that may be accessed by the Hotspot user even without authentication).

When setting up hotspots for various segments on campus, the team plans to make the online periodicals relevant to the area the hotspot supports available to the student population. By just making the Humanities periodicals available to the Humanities hotspot, the user base is better served and radio traffic noise is reduced.

24. The Tempest University IT team clicks **OK** to exit the screen and return to the Wireless LAN Edit window.

With the properties of the Humanities department external hotspot defined, the Tempest University IT department can now configure how users are authenticated to access the hotspot’s resources.
25. The Tempest University IT team clicks on Radius Config button to display the Network Wireless LANs Edit Radius Configuration sub screen.

![Radius Configuration Screen]

26. The Tempest University IT team enters 157.235.10.1 as the Radius Server IP address for the Primary Radius server and 157.235.10.2 as the address for the secondary server.

27. The Tempest University IT team sets the shared secret password to humanity for both servers. The team clicks OK to save the change. The team clicks OK again within the Wireless LANs Edit screen. The Tempest University IT team is now ready to adjust the Hotspot WLAN QoS policy to customize it for data throughput within the Humanities hotspot. Once customized, the WLAN can be enabled.

28. The Tempest University IT team selects Network > Wireless LANs > WMM from the main menu tree.

29. The team locates the Humanities Hotspot within the list of hotspots and selects the Background access method (since the Humanities department needs to prioritize data transfers) from among the four access methods listed per WLAN.

![NOTE]

**NOTE** Other hotspot supported WLANs on campus would have different access methods selected and configured based on the priority of the data proliferating within that campus segment (video and voice versus data etc.).
30. The **Edit** button is selected, and the AIFS\(N\), Transmit Ops, CW Minimum and CW Maximum are adjusted to provide Background traffic priority. When completed, the team click the **OK** button.

The Tempest University IT team is now ready to enable (activate) the Humanities WLAN and begin supporting the student population within that area of campus.
31. Still within the **Network > Wireless LANs** screen, the team switches from the WMM tab to the Configuration tab.

32. The Tempest University IT team selects the **Humanities Hotspot** WLAN from those displayed within the table and clicks the **Enable** button.

The WLAN supporting the Humanities hotspot is now ready to be supported by the switch managed network.

---

**NOTE**

The Tempest University IT team is now ready to define additional hotspots for all of the other departments and areas on campus requiring user access to the switch managed network. Each hotspot will have a unique ESSID and the external hotspot page will most likely have a different allow list as Web resources are restricted based on the access needs of each hotspot. Additionally, each WLAN should have an ACL and QoS policy configured supporting the user base and data type proliferating that part of the campus. For instance, the Audio Visual Department should have a QoS policy defined that prioritizes video and voice at the expense of data transfers, whereas the Humanities hotspot described in this use case requires data prioritization at the expense of high priority traffic like video and voice.

---

### 3.3.4 Configuring a Windows 2003 IIS Server for Hotspot Support

The IIS services installed on the Windows 2003 Server are part of the Application Server. The Application Server in turn has other components which can selectively be installed during the Windows 2003 Server installation or can be later added.

The Tempest University IT team is working with a Windows Server installation that does not include IIS services. Therefore, they need to add ISS through the following steps:

1. The Tempest University IT team selects **Start > Settings > Control Panel > Add or Remove Programs**.
2. The Tempest University IT team selects **Add/Remove Windows Components** from the left-hand side of the screen.

3. The Tempest University IT team selects the **Application Server** checkbox (if not already selected). Click the **Details** button.
4. The Tempest University IT team selects the **Internet Information Services (IIS)** checkbox and clicks **OK**. They then click **Next**.

This will start the IIS installation. The Tempest University IT team may be prompted to insert their Windows 2003 Server CD to complete installation. The Tempest University IT team is now ready to configure the IIS Server, for more information, see **IIS Server Configuration on page 3-17**.
3.3.4.1 IIS Server Configuration

To configure the IIS Server to support their hotspot, the Tempest University IT team does the following:

1. The Tempest University IT team uses Start > All Programs > Administrative Tools > Internet Information Service (IIS) Manager to Start/Stop the Default Web Site.

   After the Tempest University IT team has the IIS Server up and running, their 3 hotspot Web Pages (Login.htm, Welcome.htm and Failure.htm) need to be copied to the ISS Web Server's root directory.

2. The Tempest University IT team copies text for the 3 HTML files into a text editor (MS Word) and saves them as (Login.htm, Welcome.htm and Failure.htm).

   **NOTE** For sample text of the content of the Login, Welcome and Failure pages, see Sample HTML Pages / CGI Script for External Hotspots on page 3-18.

3. The Tempest University IT team edits the 3 HTML pages to change the IP address in the HTML page to the IP address of their switch (running the Radius Server).

4. The Tempest University IT team copies these 3 htm files onto their Windows IIS Servers root directory, launch Windows file explorer and copy the files under C:\inetpub\wwwroot directory.
3.3.5 Sample HTML Pages / CGI Script for External Hotspots

**Login.htm**

```html
<br>
<br>
```

```html
<title>Login Page 111</title>
```

```html
<body>
```

```html
<form action="https://10.0.1.77:444/cgi-bin/hslogin.cgi" method="POST" >
```

```html
<tr><td><b>Username:</b></td><td><input type="text" size="20" name="f_user"></td></tr>
```

```html
<tr><td><b>Password:</b></td><td><input type="password" size="20" name="f_pass"></td></tr>
```

```html
<input type="submit" name="submit" value="LogIn"></td></tr>
```

```html
</form>
```

```html
</body>
```

**Welcome.htm**

```html
<br>
<br>
```

```html
<title>Authentication success.222</title>
```

```html
<body>
```

```html
<form method="POST" action="https://10.0.1.77:444/cgi-bin/hslogout.cgi">
```

```html
<a href="https://10.0.1.77:444/cgi-bin/hslogout.cgi">Disconnect</a>
```

```html
</form>
```

```html
</body>
```

```html
</html>

```html
</html>
```
**Failure.htm**

```html
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=us-ascii">
<html>
<head>
<title>Unable to authenticate 333</title></head>
<body link="#FFFF77" alink="#FFFF77" vlink="#FFFF77" bgcolor="#225599">
<font face="Verdana" color="#EEEEFF">
<center><img src="333"></center><center><h2>Authentication Failed. 333</h2></center><br>
<center><h4>Either the username and password are invalid, or service is unavailable at this time 333</h4></center><br>
<center><a href="http://192.168.1.1/login.htm"><h4>Try Again</h4></a></center><center><img src="333"></center><center><h5><i>Contact the network administrator if you do not have an account 333</i></h5></center>
This should be the IP address of your WS5100
This should be the IP address of your IIS Server
```
3.4 Use Case: Remote VPN

In this scenario, there is a mobile unit connected wirelessly to a WS5100 switch which needs to access a corporate network (trusted network) securely using the switch’s IPSec VPN functionality.

In the above diagram, a Symbol client is associated to WLAN 1 (attached to VLAN1 on the switch). VLAN1 is on the 157.235.188.x subnet and running a DHCP Server that supplies IP addresses for the subnet. The corporate network is on VLAN3 of the switch, which has a 192.168.0.x subnet.

The two networks use unregistered addresses and are connected over the public Internet by site-to-site VPN. In this example, NAT is required for the connections to the public Internet. However, NAT is not required for traffic between the two networks, which can be transmitted using a VPN tunnel over the public Internet. This allows a wired LAN in branch offices to be bridged directly to the central site while maintaining security.

3.4.1 Network Overview

The Symbol client in this example is associated with WLAN1 and received an IP address of 157.235.188.4 from the DHCP server on VLAN1. This client wants to access the 192.168.0.x network securely. This is accomplished using the switch’s IP Sec, IKE and XAuth VPN features.

If the client is VPN enabled, it initiates a connection with the VPN server on the switch, the client and server then exchange device authentication via Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth). Client related configuration is then pushed to the client using Mode Configuration, and an IPsec security association (SA) is created. Once the client establishes an IKE SA configured for Xauth, the client must wait for a “username/password” challenge and then responds to the challenge with their username and password.

If the switch indicates that authentication was successful, the client requests further configuration parameters from the switch. At this stage the internal IP address (virtual IP) is pushed to the client from a pool configured under Client Mode Configuration, IPsec SAs are created, and the connection is complete.

Once the client has received a virtual IP (192.168.0.11), additional packets from the client within the IPSec tunnel are routed to the corresponding interface (VLAN3) and the client gains access to the corporate network.
The following sections provide step-by-step instructions for setting up the remote VPN setup described in the example above.

### 3.4.2 Configuring DHCP Server to serve public IP addresses

The client needs to have an IP address before it can connect to the VPN Server on the switch to create an IPSec tunnel. To do this, you need the DHCP Server on the interface to provide public IP address to the IPSec clients.

#### 3.4.2.1 Adding a New DHCP Pool

The first step is to enable the DHCP server to assign an IP address to the client.

1. Select **Services > DHCP Server** from the main menu tree.

   The DHCP Server screen appears with the **Configuration** tab displayed.

2. Select the **Enable DHCP Server** checkbox to enable the switch’s internal DHCP Server on the current interface.

3. Restart the switch’s DHCP server by clicking the **Restart DHCP Server** button.
3.4.2.2 Adding a New DHCP Pool

1. Click the Add button at the bottom of the DHCP Server screen.

2. In the Pool Name field, enter the name of the IP pool from which IP addresses can be issued to client requests on this interface. In the case of our example we’ll call this pool Wireless Clients.

3. In this example, skip the Domain, NetBios Node, and Boot File fields, as they are not necessary for this setup.

4. Enter the name of the boot file used for this pool within the Boot File parameter.

5. From the Network field, define the IP Address and Subnet Mask used for DHCP discovery and requests between the DHCP Server and DHCP clients. For this example enter 157.235.188.0 for IP address and 24 for subnet.

6. The Lease Time field defines one of the two kinds of leases the DHCP Server assigns to its clients. For this example leave the Lease Time field, set at the default value of 1:00:00.

7. Skip the Server section since it is irrelevant to this example.

8. Provide the Included Ranges (starting and ending IP addresses) for this particular pool. For this example enter 157.235.188.2 in the Start IP field and 157.235.188.50 in the End IP field. This provides 49 addresses that can be assigned to clients on this network.

9. Click OK to save and add the changes to the running configuration and close the dialog.

10. Click the Apply button on the main DHCP screen to save the configuration and then click the Restart DHCP Server button to restart the DHCP server with the new settings.

3.4.3 Configuring Crypto Policy (IKE)

IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual pre-configuration.

IKE provides the following benefits:

- Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
- Allows you to specify a lifetime for the IPSec security association.
- Allows encryption keys to change during IPSec sessions.
- Permits Certification Authority (CA) support for a manageable, scalable IPSec implementation.
- Allows dynamic authentication of peers.

If you do not want IKE to be used with your IPSec implementation, you can disable it for all IPSec peers.

**NOTE**  IKE must be enabled or disabled at all IPSec peers; you cannot have a mix of IKE-enabled and IKE-disabled peers within your IPSec network you must manually specify all the IPSec security associations in the crypto maps at all peers.

To configure IKE, perform the following steps:

- Create IKE Policies
- Configure Pre-Shared Keys
- Enable IKE

### 3.4.3.1 Create IKE Policies

An IKE policy must be established identically on both the peers including the pre-shared key. An IKE policy defines a combination of security parameters to be used during the IKE negotiation. Before configuring a crypto policy five parameters must be decided upon by both ends of the VPN tunnel. If any of these parameters do not match, the VPN tunnel cannot be established.

**NOTE**  Only the main mode of IKE negotiation is supported.

The following are the five parameters required to define each IKE policy:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Accepted Values</th>
<th>Keyword</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption algorithm</td>
<td>56-bit DES-CBC, 128-bit AES</td>
<td>Des, Aes</td>
<td>56-bit DES-CBC</td>
</tr>
<tr>
<td>Hash Algorithm</td>
<td>SHA-1 (HMAC variant), MD5 (HMAC variant)</td>
<td>sha, md5</td>
<td>SHA-1 (HMAC variant)</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>Pre-Shared Keys, CA-Certificate</td>
<td>pre-share cert</td>
<td>Pre-Shared Keys</td>
</tr>
<tr>
<td>Security Association’s Lifetime</td>
<td>Can specify any number of seconds</td>
<td>-</td>
<td>86400 seconds (one day)</td>
</tr>
</tbody>
</table>
Navigate to the Security> IKE Settings> IKE Policy screen. For this example set the parameters as follows:

1. Enter a **Priority** value of 1.
2. Set the **Encryption** to **DES**.
3. Set the **Hash** Value to **MD5**.
4. Set the **Authentication** type to **Pre-Shared Key**.
5. Set the **SA Lifetime** to **10800** seconds (3 hours).
6. Click **OK** to return to the **IKE Policy** screen.
7. Click **Apply** to save the new IKE Policy.

### 3.4.3.2 Configure Pre-Shared Keys

To configure pre-shared keys, specify the shared keys at each peer.

For this example, only set up the pre-shared key for the one client that wishes to connect to the remote network. In your network you will likely set up pre-shared keys for each of the clients using VPN.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>5</td>
<td>14</td>
</tr>
<tr>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
</tr>
</tbody>
</table>

For a given pre-shared key is shared between two peers. At a given peer you can specify the same key to share with multiple remote peers; however, a more secure approach is to specify different keys to share between different pairs of peers.

Navigate to the Security> IKE Settings> Configuration screen.

1. Click the **Add** button.
2. In the Add Pre-shared Key dialog, choose **Peer IP Address** and enter in the IP address of the client. In this case 157.235.188.4
3. Enter a **Key** to be used as the pre-shared key for both client and server. For this example, enter in **test12345** as the key.
4. Click **OK** to return to the Configuration screen.
5. Click **Apply** to save the new pre-shared key.

6. You must then set up the pre-shared key of `test12345` on the client. Refer to the client’s documentation for information on adding an IKE Pre-shared key.

### 3.4.3.3 Enable or Disable IKE

IKE is enabled by default. IKE does not have to be enabled for individual interfaces, but is enabled globally for all interfaces at the switch.

For this example, leave IKE enabled.

---

**NOTE**

The following information is not needed to complete the IPSec VPN use case outlined above, but contains additional information on IPSec VPN configuration that may be useful in your implementation.

---

### 3.4.4 Set Global Lifetimes for IPSec Security Associations

You can change the global lifetime values used when negotiating new IPSec security associations. (These global lifetime values can be overridden for a particular crypto map entry).

These lifetimes only apply to security associations established via IKE. Manually established security associations do not expire.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. A security association expires after the first of these lifetimes is reached. The default lifetimes are 3600 seconds (one hour) and 4,608,000 kilobytes (10 megabytes per second for one hour).

If you change a global lifetime, the new lifetime value will not be applied to currently existing security associations, but will be used in the negotiation of subsequently established security associations. If you wish to use the new values immediately, you can clear all or part of the security association database.

### 3.4.5 Define Transform Sets

A transform set represents a certain combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting data flow.

With manually established security associations, there is no negotiation with the peer, so both sides must specify the same transform set. If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the `clear crypto sa` command.

### 3.4.6 Create Client Related Mode Configuration (Remote Access VPN)

When the client initiates a connection with the VPN server on our switch, the "conversation" that occurs between the peers consists of device authentication via Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth), push client relate configuration (using Mode Configuration), and IPsec security association (SA) creation.
Refer to the following for an overview of this process:

1. The client attempts to establish an IKE SA between its public IP address and the public IP address of the switch where the VPN server is running.
2. After the IKE SA is successfully established, and if the switch is configured for Xauth, the client waits for a "username/password" challenge and then responds to the challenge of the switch.
3. The information that is entered is checked against authentication entities (either configured on the switch or using radius server).
4. If the switch indicates that authentication was successful, the client requests further configuration parameters from the switch. The remaining system parameters (for example, IP address, DNS, and split tunnel attributes) are pushed to the client at this time using Client Mode Configuration.
5. After the client has received the configuration parameters, IKE quick mode is initiated to negotiate IPsec SA establishment.
6. Following this IPsec SAs are created and the connection is complete.

Once you have configure the client related parameters as a group using mode configuration, attach this group to the crypto map entry assigned on an interface.

### 3.4.7 Configuring IPSec Security Associations (Crypto Map)

To configure SAs, use the concept of crypto-map entries. Crypto map entries created for IPSec pull together the various parts used to set up IPSec security associations, including:

- Crypto access list defines what traffic should be protected and what traffic should not be protected – for example access list can be created to protect traffic between Subnet A and Subnet Y or between Host A and Host B. The particular crypto map entry will reference the specific access list that defines whether IPSec processing is to be applied to the traffic matching the permit in the access list.
- Where IPSec-protected traffic should be sent (who the remote IPSec peer is)
- The local address to be used for the IPSec traffic
- What IPSec security should be applied to this traffic (selecting from a list of one or more transform sets)
- Whether security associations are manually established or are established via IKE
- Other parameters that might be necessary to define an IPSec security association

The policy described in the crypto map entries is used during the negotiation of security associations. For IPSec to succeed between two IPSec peers, both peers’ crypto map entries must contain compatible configuration statements.

**NOTE**

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPSec/IKE, and IPSec/manual entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

### 3.4.7.1 Creating Crypto Map Entry for Establishing Manual Security Associations

The use of manual security associations is a result of a prior arrangement between the users of the local switch and the IPSec peer. If IKE is not used for establishing the security associations, there is no negotiation of security associations, so the configuration information in both systems must be the same in order for traffic to be processed successfully by IPSec.
3.4.7.2 Creating Crypto Map Entry that Use IKE to Establish Security Association

When IKE is used to establish security associations, the IPSec peers can negotiate the settings they will use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

3.4.8 Apply Crypto Map Sets to Interfaces

You need to apply a crypto map set to each interface through which IPSec traffic will flow. Applying the crypto map set to an interface instructs the switch to evaluate all the interface’s traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto (either CET or IPSec).

3.4.9 Monitor and Maintain IPSec Tunnels

New configuration changes will only take effect when negotiating subsequent security associations. If you want the new settings to take immediate effect, you must clear the existing security associations so that they will be re-established with the changed configuration.

For manually established security associations, you must clear and reinitialize the security associations or the changes will never take effect.

3.4.10 Network Address Translation in IPSec

NAT is most often used to convert private address into routable public addresses. With static NAT each private address maps to one public address. In a dynamic/hide NAT both IP address and Port are mapped, allowing many privately addressed hosts to share one public IP address. Check sums must be recomputed and embedded IP addresses carried in application protocols like FTP may be translated. There is a problem when NAT is applied before IPSec.

- The IPSec Authentication Header protects entire IP packets including IP headers, against modification in transit. NAT will modify the IP header so inherently NAT is incompatible with AH.
- The IPSec Encapsulating Security Payload (ESP) usually encrypts IP packets. NAT modifies TCP and UDP ports, but clearly can’t do so when the packet is encrypted. Hence NAT is incompatible with ESP.

The solution to overcome this problem is UDP encapsulation. In this approach the IPSec packet is encapsulated in an UDP/IP header which lets NAT do their thing. This works for IPSec ESP. ESP encapsulated packets are exchanged between IKE peers. The peers must support the same method of UDP ESP encapsulation. IKE peers will exchange a known value to determine whether they both support NAT traversal (UDP Encapsulation). If the IKE peers agree, they use IKE probes or discovery payloads to determine whether NAT is being applied at some point between them. Only when IKE peers agree and NAT is encountered UDP encapsulation is used.

IKE peers communicate over UDP port 500, UDP encapsulated ESP communicates on the same port. It ensures that IKE and UDP encapsulated ESP packets are subjected to the same mid-stream address translation. The sender indicates that an encapsulated packet follows by setting the first 8 bytes of UDP payload to zero. These bytes overlap the IKE initiator cookie field, for which zero is an invalid value. Thus, implementations can use these bytes to discriminate between the IKE and UDP-encapsulated ESP arriving on port 500. Because only peers that agree will ever send UDP-encapsulated ESP packets.
In hide NAT private IP address and source port are temporarily bound to a shared public IP address and a used port. A timeout dissolves this binding after seconds or minutes of inactivity, enabling hide NAT pool reuse. IPSec VPN’s protect traffic exchanged between mutually authenticated endpoints. For NAT traversal to work, endpoints cannot be dynamically remapped mid-session. To preserve dynamic NAT bindings for the life of an IPSec session, a one byte UDP “keepalive” may be used.
This chapter provides a sample of the differences a user will experience when navigating within the WS5100 3.0 Web UI. The new WS5100 3.0 Web UI is a departure from the applet used in previous WS5100 switch releases. Consequently, every previous navigation used to access a specific feature in the 1.4.x and 2.x baselines is different in the 3.0 baseline. The goal of this chapter is to provide Web UI navigation samples enabling 1.4.x and 2.x users to familiarize themselves with the differences within the new WS5100 3.0 baseline.

**CAUTION** This chapter does not contain information on how to configure switch settings. This chapter’s intention is to define the differences in Web UI navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines. This chapter does not include an overview of the CLI differences for each Web UI function described. For information on the implications of configuring your WS5100, see the WS5100 System Reference Guide available from the Symbol Web site. For an extensive description of the new CLI commands available to the new WS5100 3.0 baseline, see WS5100 CLI Reference Guide.
4.1 Web UI Menu Path Navigation

This section provides a comparison in Web UI menu navigation amongst the 1.4.x, 2.x and 3.0 baselines. This information is presented by displaying the menu paths and button actions used to navigate to the target feature.

4.1.1 High-Level Device Information

This section describes the differences in Web UI menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when accessing high-level switch information. Information is also provided for re-booting and powering off the switch using the WS51005100 Web UI.

From the 1.4.x and 2.x WS5100 baselines, accessing high-level device information (such as the quick start and chassis information) is accomplished from submenu items within the View parent menu.

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.0 Location</th>
<th>3.0 Location</th>
</tr>
</thead>
</table>
| Accessing Switch Quick Start Data | View > Quick Start | View > Quick Start | Switch > | 1) Click the Configuration Tab.  
2) Click the Show Dashboard button. |
| Accessing System, Network and Diagnostic Performance Information | View > Chassis | View > Chassis | Switch > | 1) Click the Configuration tab.  
---------------------------------  
Network > | 1) Click the Configuration tab.  
---------------------------------  
Diagnostics > | 1) Click the Environment, CPU, Memory, Disk, Processes or Other Resources tabs. |
| Reboot (Restart) or Shutdown the Switch | Run a “reset” command using the switch CLI. or Run a “shutdown” command using the switch CLI. | System Settings > Device > Reboot | Switch > | 1) Click the Configuration tab.  
2) Click the Restart or Shutdown buttons. |
4.1.2 Configuring the System Time (NTP) Settings

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when using the Web UI to define the switch system time.

Table 4.2 WS5100 Switch System (NTP) Configuration

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.0 Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting System Time</td>
<td>For switch time: System Settings &gt; Date/Time</td>
<td>For switch time: System Settings &gt; Date/Time</td>
<td>For secure NTP: Services &gt; Secure NTP</td>
</tr>
<tr>
<td>and Synchronizing WS5100 with NTP Server</td>
<td>For NTP time: System Settings &gt; Kerberos &gt; Configuration &gt; NTP</td>
<td>For NTP time: System Settings &gt; Kerberos &gt; Configuration &gt; NTP</td>
<td></td>
</tr>
</tbody>
</table>

4.1.3 Managing Software, Configuration and Log Files

4.1.3.1 WS5100 Switch Firmware

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when using the Web UI to manage switch software.

Table 4.3 WS5100 Switch Software Management

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.0 Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing the Attributes of Existing Switch Firmware Files</td>
<td>System Settings &gt; Firmware Management &gt; Available Images</td>
<td>System Settings &gt; Firmware Management &gt; Available Images</td>
<td>Switch &gt; Firmware</td>
</tr>
<tr>
<td>Setting Global Software Settings</td>
<td>Not Available</td>
<td>Not Available</td>
<td>Switch &gt; Firmware</td>
</tr>
<tr>
<td>Upload/Update Firmware</td>
<td>System Settings &gt; Firmware Management &gt; Available Images</td>
<td>System Settings &gt; Firmware Management &gt; Available Images</td>
<td>Switch &gt; Firmware</td>
</tr>
<tr>
<td>1) Select a target firmware version.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) Click the Upload Files button.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) Use the Browse button to select the target firmware version.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1) Select a target firmware version.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) Click the Upload Files button.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) Use the Browse button to select the target firmware version.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 4.1.3.2 WS5100 Switch Configuration Files

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when using the Web UI to manage switch configuration files.

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Existing Config Files</td>
<td>Use the “directory” CLI command (System Context).</td>
<td>Use the “directory” CLI command (System Context).</td>
<td>Switch &gt; Configurations</td>
</tr>
</tbody>
</table>
| Editing Existing Config Files | Use the “configure” CLI command (System Context). | Use the “configure” CLI command (System Context). | Switch > Configurations  
1) Select an existing file and click **Edit**. |
| Viewing the Contents of a Config File | Use the “show” CLI command (System Context). | Use the “show” CLI command (System Context). | Switch > Configurations  
1) Select an existing file and click **View**. |
| Transferring Config Files | Use the “copy” CLI command (System Context). | Use the “copy” CLI command (System Context). | Switch > Configurations  
1) Select an existing file and click **Transfer Files**. |
### 4.1.3.3 WS5100 Log Files

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when using the Web UI to manage the logging of system events.

**Table 4.5 WS5100 Logging System Events**

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure (Enable) Event Logging</strong></td>
<td>System Settings &gt; Event Notification &gt;</td>
<td>System Settings &gt; Event Notification &gt;</td>
<td>Diagnostics &gt; System Logging &gt;</td>
</tr>
<tr>
<td></td>
<td>1) Select the Events tab.</td>
<td>1) Select the Events tab.</td>
<td>2) Click the Enable Logging Module checkbox.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) Set logging configuration.</td>
</tr>
<tr>
<td><strong>Manipulating Individual Log Files</strong></td>
<td>System Settings &gt; Event Notification &gt;</td>
<td>System Settings &gt; Event Notification &gt;</td>
<td>Diagnostics &gt; System Logging &gt;</td>
</tr>
<tr>
<td></td>
<td>1) Select the Events tab.</td>
<td>1) Select the Events tab.</td>
<td>1) Click the Log Options tab.</td>
</tr>
<tr>
<td></td>
<td>2) Select the checkboxes of specific target events to generate a log file upon their occurrence.</td>
<td>2) Select the checkboxes of specific target events to generate a log file upon their occurrence.</td>
<td>2) Select the File Mgt tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) View, clear buffer or transfer files as needed.</td>
</tr>
<tr>
<td><strong>Viewing the Contents of Individual Files</strong></td>
<td>Use an “logdir” CLI command (System Context).</td>
<td>Use an “logdir” CLI command (System Context).</td>
<td>Diagnostics &gt; System Logging &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Select the File Mgt tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Select a single log file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) Click the View button.</td>
</tr>
<tr>
<td><strong>Transferring Log Files</strong></td>
<td>Use an “export” CLI command (System Context).</td>
<td>Use an “export” CLI command (System Context).</td>
<td>Diagnostics &gt; System Logging &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Select the File Mgt tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Select a single log file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) Click the Transfer Files button.</td>
</tr>
</tbody>
</table>
4.1.4 VLAN Configuration

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when using the Web UI to configure VLANs.

Table 4.6 WS5100 VLAN Configuration

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing the Existing Switch</td>
<td>Create &gt; Ethernet &gt; New Policy</td>
<td>Create &gt; Ethernet &gt; New Policy</td>
<td>Network &gt; Layer 2 Virtual LANs</td>
</tr>
<tr>
<td>VLAN Configuration</td>
<td>1) Enter a name and description for the policy.</td>
<td>1) Enter a name and description for the policy.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2) Click Next.</td>
<td>2) Click Next.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3) Click VLAN Discovery...</td>
<td>3) Click VLAN Discovery...</td>
<td></td>
</tr>
<tr>
<td>Adding a New VLAN ID</td>
<td>Create &gt; Ethernet &gt; New Policy</td>
<td>Create &gt; Ethernet &gt; New Policy</td>
<td>Network &gt; Wireless LANs</td>
</tr>
<tr>
<td></td>
<td>1) Enter a name and description for the policy.</td>
<td>1) Enter a name and description for the policy.</td>
<td>1) Click the Configuration tab.</td>
</tr>
<tr>
<td></td>
<td>2) Click Next.</td>
<td>2) Click Next.</td>
<td>2) Click the Add button.</td>
</tr>
<tr>
<td></td>
<td>3) Click Add.</td>
<td>3) Click Add.</td>
<td>3) Select the VLAN ID checkbox.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4) Assign a new VLAN ID.</td>
</tr>
<tr>
<td>Removing a VLAN or removing a</td>
<td>Create &gt; Ethernet &gt; New Policy</td>
<td>Create &gt; Ethernet &gt; New Policy</td>
<td>Network &gt; Layer 2 Virtual LANs</td>
</tr>
<tr>
<td>VLAN/WLAN Assignment</td>
<td>1) Enter a name and description for the policy.</td>
<td>1) Enter a name and description for the policy.</td>
<td>1) Select the VLAN Assignment tab.</td>
</tr>
<tr>
<td></td>
<td>2) Click Next.</td>
<td>2) Click Next.</td>
<td>2) Remove the VLAN assignment checkmarks as required to remove the WLAN/VLAN assignment.</td>
</tr>
</tbody>
</table>
4.1.5 Configuring Switch Security

4.1.5.1 ACL Configuration

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when accessing the switch Access Control List (ACL).

Table 4.7 Navigating the WS5100 ACL

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating an ACL</td>
<td>Create &gt; Access Port &gt; Access Control List &gt;</td>
<td>Create &gt; Access Port &gt; Access Control List</td>
<td>Security &gt; ACLs</td>
</tr>
<tr>
<td></td>
<td>Create &gt; Access Port &gt; Access Control List &gt;</td>
<td></td>
<td>1) Click the Configuration tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Click the Add button.</td>
</tr>
<tr>
<td>Adding an ACL Rule</td>
<td>Create &gt; Access Port &gt; Access Control List &gt;</td>
<td>Create &gt; Access Port &gt; Access Control List &gt;</td>
<td>Security &gt; ACLs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Enter an ACL Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Define an Allow/Deny designation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) Click the Use an existing Access Control List as a template checkbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4) Click the Next button</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5) Click the Add button</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security &gt; ACLs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Click the Configuration tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Click the Add button (from the Associated Rules field).</td>
</tr>
<tr>
<td>Edit an Existing ACL</td>
<td>Modify &gt; Access Port &gt; Access Control List &gt;</td>
<td>Modify &gt; Access Port &gt; Access Control List &gt;</td>
<td>Security &gt; ACLs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Enter an ACL Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Define an Allow/Deny action</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) Click the Use an existing Access Control List as a template checkbox</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4) Click the Next button</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5) Select an ACL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6) Click the Edit button</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security &gt; ACLs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Click the Configuration tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Click the Edit button (from the Associated Rules field).</td>
</tr>
</tbody>
</table>
### Table 4.7 Navigating the WS5100 ACL

<table>
<thead>
<tr>
<th>Deleting an Existing ACL Policy</th>
<th>Modify &gt; Access Port &gt; Access Control List &gt;</th>
<th>Modify &gt; Access Port &gt; Access Control List &gt;</th>
<th>Security &gt; ACLs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-------------------------------------------</td>
<td>-------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td></td>
<td>1) Enter an ACL Name</td>
<td>1) Enter an ACL Name</td>
<td>1) Click the Configuration tab.</td>
</tr>
<tr>
<td></td>
<td>2) Define an Allow/Deny action</td>
<td>2) Define an Allow/Deny action</td>
<td>2) Click the Delete button</td>
</tr>
<tr>
<td></td>
<td>3) Click the <strong>Use an existing Access Control List as a template</strong> checkbox</td>
<td>3) Click the <strong>Use an existing Access Control List as a template</strong> checkbox</td>
<td>(from the either the ACLs or Associated Rules fields).</td>
</tr>
<tr>
<td></td>
<td>4) Click the <strong>Next</strong> button</td>
<td>4) Click the <strong>Next</strong> button</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5) Select an ACL</td>
<td>5) Select an ACL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6) Click the <strong>Delete</strong> button</td>
<td>6) Click the <strong>Edit</strong> button</td>
<td></td>
</tr>
</tbody>
</table>
### 4.1.5.2 Encryption and Authentication

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when using the Web UI to define an encryption or authentication based security policy.

This section describes how to navigate to the target security screen described in the **Configuration Option/Feature** portion of the table. Once you navigate to the target security screen, a thorough knowledge of the security feature is required to adequately protect the data within your network.

#### Table 4.8 WS5100 Switch Security Policies

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access the Security Configuration Screen(s)</strong></td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Network&gt; Wireless LANs&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Select a WLAN.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) Click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4) Select an authentication or encryption checkbox.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5) Click the <strong>Config</strong> button.</td>
</tr>
<tr>
<td><strong>Create an “Open” Configuration</strong></td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Network&gt; Wireless LANs&gt;</td>
</tr>
<tr>
<td></td>
<td>1) Name the policy.</td>
<td>1) Name the policy.</td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
</tr>
<tr>
<td></td>
<td>2) Enter a description.</td>
<td>2) Enter a description.</td>
<td>2) Select a WLAN Index.</td>
</tr>
<tr>
<td></td>
<td>3) Select the <strong>None</strong> checkbox.</td>
<td>3) Select the <strong>None</strong> checkbox.</td>
<td>3) Click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td>4) Click <strong>Next</strong>.</td>
<td>4) Click <strong>Next</strong>.</td>
<td>4) Revise the SSID (if necessary).</td>
</tr>
<tr>
<td><strong>Configure WEP</strong></td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Network&gt; Wireless LANs&gt;</td>
</tr>
<tr>
<td></td>
<td>1) Name the policy.</td>
<td>1) Name the policy.</td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
</tr>
<tr>
<td></td>
<td>2) Enter a description.</td>
<td>2) Enter a description.</td>
<td>2) Select a WLAN Index.</td>
</tr>
<tr>
<td></td>
<td>3) Select the <strong>WEP</strong> checkbox.</td>
<td>3) Select the <strong>WEP</strong> checkbox.</td>
<td>3) Click the <strong>Edit</strong> button.</td>
</tr>
<tr>
<td></td>
<td>4) Click <strong>Next</strong>.</td>
<td>4) Click <strong>Next</strong>.</td>
<td>4) Revise the SSID (if necessary).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5) Revise the configuration description (if necessary).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4) Select either the <strong>WEP 64</strong> or <strong>WEP 128</strong> checkbox.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6) Click the <strong>Config</strong> button.</td>
</tr>
</tbody>
</table>
Table 4.8 WS5100 Switch Security Policies

| Configure KeyGuard | Create > Access Port > Security Policy | Create > Access Port > Security Policy | Network> Wireless LANs>  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Name the policy</td>
<td>1) Name the policy</td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>2) Enter a description</td>
<td>2) Enter a description</td>
<td>2) Select a WLAN Index.</td>
<td></td>
</tr>
<tr>
<td>3) Select the <strong>KeyGuard</strong> checkbox</td>
<td>3) Select the <strong>KeyGuard</strong> checkbox</td>
<td>3) Click the <strong>Edit</strong> button.</td>
<td></td>
</tr>
<tr>
<td>4) Click <strong>Next</strong></td>
<td>4) Click <strong>Next</strong></td>
<td>4) Revise the SSID (if necessary).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5) Revise the configuration description (if necessary).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4) Select the <strong>KeyGuard</strong> checkbox.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6) Click the <strong>Config</strong> button.</td>
<td></td>
</tr>
</tbody>
</table>

| Configure TKIP | Create > Access Port > Security Policy | Create > Access Port > Security Policy | Network> Wireless LANs>  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Name the policy</td>
<td>1) Name the policy</td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>2) Enter a description</td>
<td>2) Enter a description</td>
<td>2) Select a WLAN Index.</td>
<td></td>
</tr>
<tr>
<td>3) Select the <strong>TKIP</strong> checkbox</td>
<td>3) Select the <strong>TKIP</strong> checkbox</td>
<td>3) Click the <strong>Edit</strong> button.</td>
<td></td>
</tr>
<tr>
<td>4) Click <strong>Next</strong></td>
<td>4) Click <strong>Next</strong></td>
<td>4) Revise the SSID (if necessary).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5) Revise the configuration description (if necessary).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4) Select the <strong>WPA/WPA2-TKIP</strong> checkbox.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6) Click the <strong>Config</strong> button.</td>
<td></td>
</tr>
</tbody>
</table>

| Configure AES CCMP or WPA2-AES | Create > Access Port > Security Policy | Create > Access Port > Security Policy | Network> Wireless LANs>  
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Name the policy</td>
<td>1) Name the policy</td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>2) Enter a description</td>
<td>2) Enter a description</td>
<td>2) Select a WLAN Index.</td>
<td></td>
</tr>
<tr>
<td>3) Select the <strong>TKIP</strong> checkbox</td>
<td>3) Select the <strong>TKIP</strong> checkbox</td>
<td>3) Click the <strong>Edit</strong> button.</td>
<td></td>
</tr>
<tr>
<td>4) Click <strong>Next</strong></td>
<td>4) Click <strong>Next</strong></td>
<td>4) Revise the SSID (if necessary).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5) Revise the configuration description (if necessary).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4) Select the <strong>WPA2-CCMP</strong> checkbox.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>6) Click the <strong>Config</strong> button.</td>
<td></td>
</tr>
<tr>
<td>Configure a Manual Pre-Shared Key</td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Create &gt; Access Port &gt; Security Policy</td>
<td>Not Supported</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>1) Name the policy</td>
<td>1) Name the policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) Enter a description</td>
<td>2) Enter a description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) Click <strong>Next</strong></td>
<td>3) Click <strong>Next</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4) Select the Manually Pre-Shared Key checkbox</td>
<td>4) Select the Manually Pre-Shared Key checkbox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5) Click <strong>Next</strong></td>
<td>5) Click <strong>Next</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configure Kerberos</th>
<th>Create &gt; Access Port &gt; Security Policy</th>
<th>Create &gt; Access Port &gt; Security Policy</th>
<th>Network &gt; Wireless LANs &gt;</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Name the policy.</td>
<td>1) Name the policy.</td>
<td></td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
<td></td>
</tr>
<tr>
<td>2) Enter a description.</td>
<td>2) Enter a description.</td>
<td></td>
<td>2) Select a WLAN Index.</td>
<td></td>
</tr>
<tr>
<td>3) Click <strong>Next</strong>.</td>
<td>3) Click <strong>Next</strong>.</td>
<td></td>
<td>3) Click the <strong>Edit</strong> button</td>
<td></td>
</tr>
<tr>
<td>4) Select the Kerberos checkbox.</td>
<td>4) Select the Kerberos checkbox.</td>
<td></td>
<td>4) Revise the SSID (if necessary)</td>
<td></td>
</tr>
<tr>
<td>5) Click <strong>Next</strong>.</td>
<td>5) Click <strong>Next</strong>.</td>
<td></td>
<td>5) Revise the configuration description (if necessary)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4) Select the Kerberos checkbox</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6) Click the <strong>Config</strong> button</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configure EAP</th>
<th>Create &gt; Access Port &gt; Security Policy</th>
<th>Create &gt; Access Port &gt; Security Policy</th>
<th>Network &gt; Wireless LANs</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Name the policy</td>
<td>1) Name the policy</td>
<td></td>
<td>1) Click the <strong>Configuration</strong> tab</td>
<td></td>
</tr>
<tr>
<td>2) Enter a description</td>
<td>2) Enter a description</td>
<td></td>
<td>2) Select a WLAN Index</td>
<td></td>
</tr>
<tr>
<td>3) Click <strong>Next</strong></td>
<td>3) Click <strong>Next</strong></td>
<td></td>
<td>3) Click the <strong>Edit</strong> button</td>
<td></td>
</tr>
<tr>
<td>4) Select the EAP checkbox</td>
<td>4) Select the EAP checkbox</td>
<td></td>
<td>4) Revise the SSID (if necessary)</td>
<td></td>
</tr>
<tr>
<td>5) Click <strong>Next</strong></td>
<td>5) Click <strong>Next</strong></td>
<td></td>
<td>5) Revise the configuration description (if necessary)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4) Select the <strong>802.1x EAP</strong> checkbox</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6) Click the <strong>Config</strong> button</td>
<td></td>
</tr>
</tbody>
</table>
4.1.5.3 Rogue AP Detection

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when using the Web UI to manage Rogue AP Detection. Rogue AP is not available in the 1.4.x switch software.

Table 4.9 WS5100 Rogue AP Detection

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Rogue AP Detection Menu</td>
<td>Not Supported</td>
<td>System Settings &gt; Rogue AP Detection</td>
<td>Security &gt; Access Point Detection</td>
</tr>
<tr>
<td>Define Rogue AP Detection Method</td>
<td>Not Supported</td>
<td>System Settings &gt; Rogue AP Detection</td>
<td>Security &gt; Access Point Detection</td>
</tr>
<tr>
<td>Rogue AP Rule Management</td>
<td>Not Supported</td>
<td>System Settings &gt; Rogue AP Detection</td>
<td>Security &gt; Access Point Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1) Select amongst the RF Scan by MU, RF Scan by AP and RF Scan by Detector AP checkboxes button within Detection Method field.</td>
<td>1) Select Configuration tab. 2) Select Enable checkbox. 3) Select Allowed APs tab. 4) Click Add or Edit button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1) Click Add, Delete or Delete All from within the Rule Management tab.</td>
<td>1) Select Configuration tab. 2) Select Enable checkbox. 3) Select Allowed APs tab. 4) Click Add or Edit button.</td>
</tr>
</tbody>
</table>
4.1.5.4 Configuring the On-Board Radius Server

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when accessing the switch's on-board Radius server.

**Table 4.9 WS5100 Rogue AP Detection**

<table>
<thead>
<tr>
<th>Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a Detected AP to Approved AP List</td>
<td>Not Supported</td>
<td>System Settings &gt; Rogue AP Detection</td>
<td>Security &gt; Access Point Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1) Click the AP List tab 2) Select an AP and click the Add AP to Rule List button.</td>
<td>1) Select Unapproved APs tab. 2) Select an unapproved AP. 3) Click the Allow button.</td>
</tr>
<tr>
<td>View Rogue AP Details</td>
<td>Not Supported</td>
<td>System Settings &gt; Rogue AP Detection</td>
<td>Security &gt; Access Point Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1) Click the AP List tab 2) Select an AP and click the View Details button.</td>
<td>1) Select Unapproved APs tab.</td>
</tr>
</tbody>
</table>

**Table 4.10 Viewing WS5100 Statistics**

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessing the Radius Configuration</td>
<td>No On-Board Radius Support.</td>
<td>System Settings &gt; Radius &gt; Configuration</td>
<td>Security &gt; Radius Server</td>
</tr>
<tr>
<td>Editing the Existing Radius Configuration</td>
<td>No On-Board Radius Support.</td>
<td>System Settings &gt; Radius &gt; Configuration</td>
<td>Security &gt; Radius Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1) Select an existing Server. 2) Click the Edit Configuration button.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4.10 Viewing WS5100 Statistics

<table>
<thead>
<tr>
<th>Configuring Radius Accounting</th>
<th>No On-Board Radius Support.</th>
<th>System Settings &gt; Radius &gt; Configuration</th>
<th>Security &gt; Radius Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1) Select the <strong>Radius Accounting Server</strong> tab.</td>
<td>1) Click the <strong>Accounting Logs</strong> tab.</td>
</tr>
<tr>
<td>Configuring the Radius Proxy Configuration</td>
<td>No On-Board Radius Support.</td>
<td>System Settings &gt; Radius &gt; Configuration</td>
<td>Security &gt; Radius Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1) Select the <strong>Proxy</strong> tab.</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2) Select the <strong>Proxy Servers</strong> tab.</td>
<td>1) Click the <strong>Configuration</strong> tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3) Click <strong>Add</strong> or <strong>Delete</strong>.</td>
<td>2) Select the <strong>Proxy Servers</strong> tab.</td>
</tr>
<tr>
<td>Configuring Radius Users and Groups</td>
<td>No On-Board Radius Support.</td>
<td>System Settings &gt; Radius &gt; Users</td>
<td>Security &gt; Radius Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1) Click the <strong>Add</strong> or <strong>Delete</strong> button as needed to for User and Group inclusions.</td>
<td>1) Click the <strong>Users</strong> or <strong>Groups</strong> tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3) Click <strong>Add</strong>, <strong>Delete</strong> or <strong>Edit</strong> as needed.</td>
<td>3) Click <strong>Add</strong>, <strong>Delete</strong> or <strong>Edit</strong> as needed.</td>
</tr>
</tbody>
</table>
### 4.1.6 Viewing Switch Statistics

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when accessing switch statistics.

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Display High-Level Wireless Statistics</strong></td>
<td>View &gt; Chassis</td>
<td>View &gt; Chassis</td>
<td>Switch &gt;</td>
</tr>
<tr>
<td><strong>Display High-Level Switch Statistics</strong></td>
<td>Use a “show switchpolicy” CLI command.</td>
<td>Use a “show switchpolicy” CLI command.</td>
<td>Switch &gt;</td>
</tr>
<tr>
<td><strong>Display Ethernet Statistics</strong></td>
<td>Use a “show ethernet” CLI command.</td>
<td>Use a “show ethernet” CLI command.</td>
<td>Network &gt;</td>
</tr>
<tr>
<td><strong>Display Detailed Ethernet Statistics</strong></td>
<td>Use a “show etherpolicy” CLI command.</td>
<td>Use a “show etherpolicy” CLI command.</td>
<td>Network &gt; Access Port Radios</td>
</tr>
<tr>
<td><strong>Display High-Level Radio Statistics</strong></td>
<td>Use a “show WSRfstats” CLI command.</td>
<td>Use a “show WSRfstats” CLI command.</td>
<td>Network &gt; Access Port Radios</td>
</tr>
<tr>
<td><strong>Display MU Details</strong></td>
<td>Use a “show mu” or “show musummary” CLI command.</td>
<td>Use a “show mu” or “show musummary” CLI command.</td>
<td>Network &gt; Mobile Units</td>
</tr>
<tr>
<td><strong>Display Detailed Radio Statistics</strong></td>
<td>Use a “show rfstats” CLI command.</td>
<td>Use a “show rfstats” CLI command.</td>
<td>Network &gt; Access Port Radio</td>
</tr>
<tr>
<td><strong>Display WLAN Statistics</strong></td>
<td>View &gt; Quick Start 1) Refer to WLAN tabs on bottom of screen. 2) Click on the target WLAN tab.</td>
<td>View &gt; Quick Start 1) Refer to WLAN tabs on bottom of screen. 2) Click on the target WLAN tab.</td>
<td>Network &gt; Wireless LANs</td>
</tr>
</tbody>
</table>
Table 4.11 Viewing WS5100 Statistics

<table>
<thead>
<tr>
<th>Display Detailed WLAN Statistics</th>
<th>Use a “show wlan” CLI command.</th>
<th>Use a “show wlan” CLI command.</th>
<th>Network &gt; Wireless LANs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>1) Click on <strong>Statistics</strong> tab.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>2) Select a WLAN Index.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3) Click the <strong>Details</strong> button.</td>
</tr>
</tbody>
</table>
### 4.1.7 Switch Certificate Management

This section describes the differences in menu path navigation amongst the WS5100 1.4.x, 2.x and 3.0 baselines when displaying switch certificate information and generating a request for a signed certificate.

<table>
<thead>
<tr>
<th>Configuration Option/Feature</th>
<th>1.4.x Location</th>
<th>2.x Location</th>
<th>3.0 Location</th>
</tr>
</thead>
</table>

A Warning Message displays stating that reverting back to the default certificate destroys the certificate currently in use.

1) Click **OK** to revert to default certificate.

A Warning Message displays stating that creating a self-signed certificate destroys the certificate currently in use.

1) Click **OK** to continue.
<table>
<thead>
<tr>
<th><strong>Create a Certificate Request</strong></th>
<th><strong>System Settings &gt; Server Certificate &gt; Create Certificate Request</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Complete required fields within the <strong>Create Certificate Request</strong> screen.</td>
<td>1) Complete required fields within the <strong>Create Certificate Request</strong> screen.</td>
</tr>
<tr>
<td>2) Click the <strong>OK</strong> button when completed.</td>
<td>2) Click the <strong>OK</strong> button when completed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Restart Web Request</strong></th>
<th><strong>System Settings &gt; Server Certificate &gt; Restart Web Request</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A Warning Message displays stating that restarting the switch Web UI could render the switch inoperable if the data within the certificate request does not match the actual certificate.</td>
<td>A Warning Message displays stating that restarting the switch Web UI could render the switch inoperable if the data within the certificate request does not match the actual certificate.</td>
</tr>
<tr>
<td>1) Verify the contents of the certificate match the data within the certificate request.</td>
<td>1) Verify the contents of the certificate match the data within the certificate request.</td>
</tr>
<tr>
<td>2) Click <strong>OK</strong> to continue.</td>
<td>2) Click <strong>OK</strong> to continue.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Table 4.12 Switch Certificate Management</strong></th>
<th><strong>Security &gt; Server Certificates</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1) Click the <strong>Certificates Wizard</strong> button.</td>
</tr>
<tr>
<td></td>
<td>2) Select the <strong>Create a new Certificate</strong> option.</td>
</tr>
</tbody>
</table>

**Not supported.**
The 1.4.x and 2.x version WS5100 switches have LED behavior that differs from the new 3.0 baseline switch. The 3.0 version switch does not have the same “standby” switch LED functionality that was present in the 1.4.x and 2.x baselines. Additionally, the new 3.0 version switch has a cluster functionality resulting in LED behavior previously unseen in the earlier baselines. This chapter contains an overview of the differences in LED behavior between the 1.4.x and 2.x baselines and the new 3.0 WS5100 baseline.
5.1 WS5100 1.4.x and 2.x Baseline LED Behavior

All versions of the WS5100 switch have two vertically-stacked LEDs on its front panel. The LEDs display three colors (blue, amber, and red), and three lit states (solid, blinking, and off). However, there are some states that are unique to the WS5100 1.4.x and 2.x version models.

### 5.1.1 Start Up

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Power On Self Test (POST) running</td>
<td>All colors in rotation</td>
<td>All colors in rotation</td>
</tr>
<tr>
<td>POST succeeded</td>
<td>Blue solid</td>
<td>Blue solid</td>
</tr>
<tr>
<td>Software initializing</td>
<td>Blue solid</td>
<td>Off</td>
</tr>
<tr>
<td>Software initialized</td>
<td>Blue blinking</td>
<td>Off</td>
</tr>
</tbody>
</table>

### 5.1.2 Configured as a Primary Switch

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Blue blinking</td>
<td>Blue solid</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Blue blinking</td>
<td>Amber solid</td>
</tr>
<tr>
<td>Standby missing or not enabled</td>
<td>Blue blinking</td>
<td>Off</td>
</tr>
<tr>
<td>Inactive</td>
<td>Amber blinking</td>
<td>Blue blinking</td>
</tr>
</tbody>
</table>

### 5.1.3 Configured as a Standby Switch

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active (acting as primary)</td>
<td>Blue blinking</td>
<td>Blue blinking</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Blue blinking</td>
<td>Amber solid</td>
</tr>
<tr>
<td>Standby not enabled</td>
<td>Blue blinking</td>
<td>Off</td>
</tr>
<tr>
<td>Inactive</td>
<td>Amber blinking</td>
<td>Amber blinking</td>
</tr>
</tbody>
</table>

**NOTE** The Primary and Standby LED activity described above is unique to the WS5100 1.4.x and 2.x baselines. The primary and standby designations do not apply to the 3.0 version switch.
### 5.1.4 Error Codes

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST failed (critical error)</td>
<td>Red blinking</td>
<td>Red blinking</td>
</tr>
<tr>
<td>Software initialization failed</td>
<td>Amber solid</td>
<td>Off</td>
</tr>
<tr>
<td>Country code not configured. <strong>Note:</strong> During first time setup, the LEDs will remain in this state until the country code is configured.</td>
<td>Amber solid</td>
<td>Amber blinking</td>
</tr>
<tr>
<td>No access ports have been adopted</td>
<td>Blue blinking</td>
<td>Amber blinking</td>
</tr>
<tr>
<td>Primary inactive or failed</td>
<td>Amber blinking</td>
<td>Blue blinking</td>
</tr>
</tbody>
</table>

### 5.2 WS5100 3.0 LED Behavior

The WS5100 3.0 version switch uses an LED scheme that takes advantage of the switch’s failover capabilities in addition to displaying LED events central to power up and error reporting. Refer to the following for LED behavior unique to the 3.0 version WS5100 Series Switch:

#### 5.2.1 Start Up

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td>Power On Self Test (POST) running</td>
<td>All colors in rotation</td>
<td>All colors in rotation</td>
</tr>
<tr>
<td>POST succeeded</td>
<td>Blue solid</td>
<td>Blue solid</td>
</tr>
</tbody>
</table>

#### 5.2.2 Primary

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active (Continually Adopting Access Ports)</td>
<td>Blue blinking</td>
<td>Blue solid</td>
</tr>
<tr>
<td>No License to Adopt</td>
<td>Amber blinking</td>
<td>Amber blinking</td>
</tr>
</tbody>
</table>

#### 5.2.3 Standby

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active (Failed Over and Adopting Ports)</td>
<td>Blue blinking</td>
<td>Blue blinking</td>
</tr>
<tr>
<td>Active (Not Failed Over)</td>
<td>Blue blinking</td>
<td>Amber solid</td>
</tr>
</tbody>
</table>
### 5.2.4 Error Codes

<table>
<thead>
<tr>
<th>Event</th>
<th>Top LED</th>
<th>Bottom LED</th>
</tr>
</thead>
<tbody>
<tr>
<td>POST failed (critical error)</td>
<td>Red blinking</td>
<td>Red blinking</td>
</tr>
<tr>
<td>Software initialization failed</td>
<td>Amber solid</td>
<td>Off</td>
</tr>
<tr>
<td>Country code not configured. <strong>Note:</strong> During first time setup, the LEDs will remain in this state until the country code is configured.</td>
<td>Amber solid</td>
<td>Amber blinking</td>
</tr>
<tr>
<td>No access ports have been adopted</td>
<td>Blue blinking</td>
<td>Amber blinking</td>
</tr>
</tbody>
</table>
Appendix A

Customer Support

Symbol Technologies provides its customers with prompt and accurate customer support. Use the Symbol Support Center as the primary contact for any technical problem, question or support issue involving Symbol products.

If the Symbol Customer Support specialists cannot solve a problem, access to all technical disciplines within Symbol becomes available for further assistance and support. Symbol Customer Support responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements.

When contacting Symbol Customer Support, please provide the following information:

- serial number of unit
- model number or product name
- software type and version number.

**North American Contacts**

Inside North America:

Symbol Technologies, Inc.
One Symbol Plaza Holtsville, New York 11742-1300
Telephone: 1-631-738-2400/1-800-SCAN 234
Fax: 1-631-738-5990

Symbol Support Center (for warranty and service information):

- telephone: 1-800-653-5350
- fax: (631) 738-5410
- Email: support@symbol.com

**International Contacts**

Outside North America:

Symbol Technologies
Symbol Place
Winnersh Triangle, Berkshire, RG41 5TP
United Kingdom
0800-328-2424 (Inside UK)
+44 118 945 7529 (Outside UK)
Web Support Sites

MySymbolCare

http://www.symbol.com/services/msc/msc.html

Symbol Services Homepage

http://symbol.com/services

Symbol Software Manuals

http://www.symbol.com/legacy_manuals/wire/ws5100.html

Symbol Developer Program

http://devzone.symbol.com

Additional Information

Obtain additional information by contacting Symbol at:

  1-800-722-6234, inside North America
  +1-516-738-5200, in/outside North America

http://www.symbol.com/