

BlueView™ Management System User Guide

Software Release Version: 6.4



Bluesocket, Inc.
10 North Avenue
Burlington, MA 01803 USA
+1 781-328-0888
www.bluesocket.com

Copyright Notice

Copyright © 2001 - 2007 Bluesocket, Inc. All rights reserved.

No part of this document may be reproduced in any form or by any means, electronic or manual, including photocopying without the written permission of Bluesocket, Inc.

The products described in this document may be protected by one or more U.S. patents, foreign patents, or pending patents.

This document is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This publication could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein; these changes will be incorporated in new editions of the document. Bluesocket inc. may make improvements or changes in the products or the programs described in this document at any time.

Trademarks

Bluesocket, The Bluesocket Logo, Secure Mobility, BlueView, DynamicRF, and BlueSecure are trademarks or registered trademarks of Bluesocket, Inc.

All other trademarks, trade names and company names referenced herein are used for identification purposes only and are the property of their respective companies.



Caution: This product contains a lithium battery. There is a danger of explosion if the battery is incorrectly replaced. The battery should only be replaced by the BlueView Management System manufacturer and only with same or equivalent type recommended by the battery's manufacturer. Dispose of unused batteries according to the battery manufacturer's instructions.

Publication Date: September 17, 2008



Contents

Figures

About This Guide

Audience	xi
Document Organization	xi
Notational Conventions	xii
Related Documents	xiii
Terminology	xiii

Chapter 1

An Overview of the BlueView Management System

Manageable Bluesocket Devices	1-3
Features and Functions.....	1-3
Technical Specifications	1-6

Chapter 2

Installing the BlueView Management System

General Safety Considerations.....	2-2
Precautions for Rack-mounted Equipment	2-3
The BlueView Displays, Controls, and Connectors	2-3
Preparing Your Network	2-5
Installation Location Requirements.....	2-5
Mounting the BlueView Chassis on a Desktop	2-6
Rack-mounting the BlueView Chassis.....	2-7
Connecting the BlueView Management System to Your Network.....	2-8
Connecting BlueView to its Power Source.....	2-8
Powering Down the BlueView Management System	2-9

Chapter 3

Getting Started

Accessing the Administrator Console	3-4
Logging Into the Administrator Console for the First Time	3-4
Installing the Bluesocket SSL Certificate.....	3-5
Subsequent Administrator Console Logins	3-7
Obtaining Online Help.....	3-7
Logging Out of the Administrator Console.....	3-7
Discovering WLAN Devices on Your Network.....	3-8
Creating and Running BSC Discovery Jobs.....	3-8
Manually Adding BSCs for Management by BlueView	3-13
Organizing Your Bluesocket Devices into Groups	3-15
Creating Static Groups	3-15
Visually Organizing Bluesocket Devices within Static Groups	3-18
Creating Dynamic Groups	3-18

Chapter 4	
Configuring BlueView	
Adding a New Administrator Account	4-2
Changing an Administrator Password.....	4-3
Deleting Administrator Accounts	4-4
Defining Administrator Authentication Servers	4-4
Configuring the BlueView Network Interfaces	4-8
Adding Static Routes.....	4-10
Configuring BlueView’s Time and Date Settings	4-11
Configuring the Log and Alarm Database.....	4-12
Configuring the BlueView SNMP Agent and Remote Diagnostics.....	4-13
Specifying the BlueView Email Server	4-14
Configuring Administrator Notifications	4-15
Specifying Refresh Rates	4-16
Chapter 5	
Configuring Stand Alone Access Points with BlueView	
Listing Stand Alone Access Points	5-3
Editing Stand Alone Access Point Configurations.....	5-4
General Settings	5-4
802.11b/g Radio Settings.....	5-5
802.11a Radio Settings	5-9
Access Credentials.....	5-10
Creating a Stand Alone AP Configuration Template.....	5-11
Adding a Stand Alone AP for Management by BlueView	5-12
Configuring Stand Alone AP SSIDs	5-14
Configuring Stand Alone AP RADIUS Authentication Servers.....	5-16
Chapter 6	
Monitoring WLAN Devices	
Displaying BlueView Summary Information	6-2
Displaying Bluesocket BSC Summary Information	6-3
Displaying AP Summary Information.....	6-7
Monitoring Your Protected Airspace	6-13
Displaying an RF Summary View	6-13
Displaying a Detailed RF View	6-15
Monitoring Active User Connections	6-17
Displaying BSC Active Connection Status	6-18
Displaying AP Associations	6-20
Displaying BSC Logs.....	6-20
Generating Status Reports	6-24
Displaying and Saving Status Reports	6-27
Generating and Displaying RF Heat Maps	6-27
Sample Heat Map	6-28
Importing Floor Plans.....	6-28
Generating RF Heat Maps	6-31
Monitoring Devices in RF Autocontainment	6-34
Chapter 7	
Maintaining and Provisioning WLAN Devices	
Creating Job Elements.....	7-2
Uploading BSC Configuration Files to BlueView	7-2
Uploading BSC Image Files to BlueView	7-3
Uploading BSAP Image Files to BlueView	7-4
Uploading Stand Alone AP Image Files to BlueView.....	7-5

Uploading BSC Patch Files to BlueView	7-6
Generating a BSC Configuration Template	7-6
Editing a BSC Configuration Template	7-8
Running Jobs on BlueView	7-10
Restarting BSC Services	7-10
Rebooting BSCs.....	7-12
Shutting Down BSCs.....	7-13
Backing Up BSC Configurations	7-14
Restoring a BSC Configuration	7-14
Pushing Out a Configuration Template to a BSC	7-15
Upgrading BSCs with New System Software	7-16
Switching the BSC Runtime Image.....	7-17
Installing a System Software Patch on a BSC	7-18
Removing a System Software Patch on a BSC.....	7-19
Upgrading BSAPs with New Firmware	7-20
Upgrading Stand Alone APs with New System Software.....	7-21
Applying Stand Alone AP Configuration Changes	7-22
Sending a BlueView Report via Email	7-23
Backing Up a BVMS Configuration	7-24
Reviewing Pending Jobs	7-25
Reviewing Job History	7-25
Managing BSAP Configurations	7-26
Listing BSAP Configurations	7-27
Editing BSAP Configurations	7-28
Deleting BSAP Configurations.....	7-36
Adding/Removing BSAP Configurations to/from a BSC	7-36
Creating a BSAP Configuration Template.....	7-36
Managing BSAP SSIDs.....	7-37
Listing BSAP SSIDs	7-38
Editing BSAP SSIDs	7-38
Adding BSAP SSIDs	7-43
Deleting BSAP SSIDs	7-43
Adding/Removing SSID Configurations to/from a BSC	7-43

Chapter 8

Configuring RF Intrusion Detection and Containment

Identifying Authorized RF Stations on Your Network	8-2
Configuring Sensor Alarms and RF Autocontainment.....	8-3
Defining Approved SSIDs	8-7
Defining Manufacturer MAC Addresses	8-7
Creating New Hotspot SSID Configuration	8-7
Importing Bulk RF Configuration Data Files	8-8
Exporting Bulk RF Configuration Data Files	8-8

Chapter 9

Administering Your BlueView System

Backing Up the BlueView Database	9-3
Restoring the Database.....	9-4
Creating a Debug File	9-4
Resetting BlueView to its Default Settings.....	9-4
Upgrading to a New Version of Runtime Software.....	9-5
Installing and Uninstalling Software Patches.....	9-6
Installing a Patch	9-6
Uninstalling a Patch	9-7

Switching Between BlueView Runtime Software Versions	9-7
Running Diagnostics	9-8
Capturing Network Traffic Data	9-9
Accessing BlueView Functions via the BlueView Serial Port	9-10

Chapter 10

BVMS Central Guest Access

Benefits	10-1
Operation	10-1
Configuration	10-2
Group Configuration	10-2
Controller Configuration	10-4
User Configuration	10-7
Location Configuration	10-9
Limiting Access	10-9
Reporting	10-11

Appendix A

Contacting Bluesocket, Inc.

Obtaining Technical Support	A-1
Contacting Bluesocket Customer Support	A-1

Index

Figures

Figure 1-1:	The BlueView Management System	1-2
Figure 2-1:	BlueView Displays, Controls, and Connectors.....	2-4
Figure 2-2:	Attaching a Rubber Pad to a Desktop Bumper	2-6
Figure 2-3:	Attaching the BlueView Chassis Desktop Bumper	2-6
Figure 2-4:	Attaching the BlueView Chassis Cap.....	2-7
Figure 2-5:	Attaching the Mounting Brackets to the BlueView Chassis	2-8
Figure 3-1:	SNMP Settings Page	3-2
Figure 3-2:	New Admin User Page.....	3-3
Figure 3-3:	BlueView Administrator Login Page.....	3-4
Figure 3-4:	BlueView Getting Started Page.....	3-5
Figure 3-5:	Security Certificate Alert	3-6
Figure 3-6:	Bluesocket SSL Certificate Dialog	3-6
Figure 3-7:	Displaying the BlueView Function Map.....	3-8
Figure 3-8:	Create New Discovery Configuration Page.....	3-10
Figure 3-9:	Defined Discovery Job	3-11
Figure 3-10:	BlueSecure Controllers List.....	3-11
Figure 3-11:	Listing BSAPs.....	3-12
Figure 3-12:	Listing BSAP SSIDs	3-12
Figure 3-13:	Listing Stand Alone APs	3-13
Figure 3-14:	Create New Controller Page	3-14
Figure 3-15:	Create New Device Group Page - Static Groups	3-16
Figure 3-16:	Visually Organizing Devices within Static Groups.....	3-18
Figure 3-17:	Create New Device Groups Page - Dynamic	3-19
Figure 4-1:	Create New Administrative User Page.....	4-3
Figure 4-2:	Defining an External LDAP Authentication Server	4-5
Figure 4-3:	Defining an External RADIUS Authentication Server.....	4-7
Figure 4-4:	Network Interface Page	4-9
Figure 4-5:	Sample BlueView Routing Table.....	4-10
Figure 4-6:	Create New Route Page	4-11
Figure 4-7:	BlueView Time Settings Page.....	4-11
Figure 4-8:	Logging and Storage Settings Page.....	4-13
Figure 4-9:	SNMP Settings and Remote Diagnostics Page	4-14
Figure 4-10:	Email Settings Page.....	4-15
Figure 4-11:	GUI Settings Page.....	4-16
Figure 5-1:	Listing Stand Alone APs	5-3
Figure 5-2:	Defining Stand Alone AP Setup Information.....	5-4
Figure 5-3:	Defining Stand Alone AP 802.11b/g Radio Settings.....	5-7
Figure 5-4:	Defining Stand Alone AP 802.11a Radio Settings	5-9
Figure 5-5:	Configuring a Stand Alone AP's Access Credentials.....	5-10
Figure 5-6:	Creating a Stand Alone AP Template	5-11
Figure 5-7:	Adding a Stand Alone AP.....	5-13
Figure 5-8:	Defining Stand Alone AP SSIDs	5-15
Figure 5-9:	Defining Stand Alone AP RADIUS Authentication Servers	5-17
Figure 6-1:	BlueView Summary Information	6-2
Figure 6-2:	BlueView BSC Summary Information (Group)	6-4
Figure 6-3:	BlueView BSC Summary Information (Single BSC).....	6-6
Figure 6-4:	BlueView AP Summary Information (All).....	6-8
Figure 6-5:	BlueView AP Summary Information (Single BSAP)	6-10
Figure 6-6:	BlueView AP Summary Information (Single Stand Alone AP).....	6-11
Figure 6-7:	RF Summary Information	6-14
Figure 6-8:	RF View.....	6-15
Figure 6-9:	Detailed RF View	6-16

Figure 6-10:	Sample Location Map	6-17
Figure 6-11:	Active Connections Page	6-18
Figure 6-12:	Active Connection Details	6-20
Figure 6-13:	BSC Log Summary	6-21
Figure 6-14:	BSC Alarm Summary	6-22
Figure 6-15:	Received RF Sensor Alarms	6-23
Figure 6-16:	Report Page	6-24
Figure 6-17:	Generated Reports Page	6-27
Figure 6-18:	Sample RF Heat Map	6-28
Figure 6-19:	Map Configuration Page	6-29
Figure 6-20:	RF Heat Maps List	6-30
Figure 6-21:	RF Heat Map: Initial Display	6-31
Figure 6-22:	Generated RF Heat Map Display	6-32
Figure 6-23:	Entering a Dimensions Calibration Value	6-33
Figure 6-24:	Contained Devices Page	6-34
Figure 7-1:	BlueView Configurations Page	7-3
Figure 7-2:	BlueSecure Controller Firmware Page	7-4
Figure 7-3:	BlueSecure Access Point Firmware Page	7-4
Figure 7-4:	Stand Alone Access Point Firmware Page	7-5
Figure 7-5:	BlueView Patches Page	7-6
Figure 7-6:	BSC Configuration Templates Page	7-7
Figure 7-7:	BSC Configuration Template Page	7-7
Figure 7-8:	Configuration Template Editor Window	7-9
Figure 7-9:	Job Action Page	7-11
Figure 7-10:	Pending Jobs Page	7-25
Figure 7-11:	Jobs History Page	7-26
Figure 7-12:	Displaying BSAPs	7-27
Figure 7-13:	Edit AP Page (ID Settings)	7-28
Figure 7-14:	Edit AP Page - (802.11b/g Radio Settings)	7-30
Figure 7-15:	Edit AP Page (802.11a Radio Settings)	7-35
Figure 7-16:	BlueSecure Controllers List	7-36
Figure 7-17:	Editing a BSAP Configuration Template	7-37
Figure 7-18:	Displaying BSAP SSIDs	7-38
Figure 7-19:	Edit SSID Page	7-41
Figure 7-20:	BlueSecure Controllers List	7-44
Figure 7-21:	Edit Controller Page	7-44
Figure 8-1:	Create New Station Configuration Page	8-2
Figure 8-2:	Configured RF Sensor Alarms	8-5
Figure 8-3:	Edit Alarm Configuration Page	8-6
Figure 8-4:	Create New SSID Configuration Page	8-7
Figure 8-5:	Create New Manufacturer MAC Configuration Page	8-7
Figure 8-6:	Create New Hotspot SSID Configuration Page	8-8
Figure 8-7:	Bulk RF Configuration Data Import Page	8-8
Figure 8-8:	Bulk Configuration Data Export Page	8-9
Figure 9-1:	BlueView Management System Restart Page	9-2
Figure 9-2:	Configuration Backup and Restore Page	9-3
Figure 9-3:	BlueView Update Page	9-5
Figure 9-4:	Manage Patches Page	9-6
Figure 9-5:	BlueView Switch Page	9-7
Figure 9-6:	Task Execution Menu Page	9-8
Figure 9-7:	Traffic Capture Page	9-9
Figure 9-8:	Defined Traffic Capture Job	9-10
Figure 9-9:	Recommended Null-modem Serial Cable Pinout	9-11
Figure 10-1:	Guest Access View	10-2

Figure 10-2: Guest Groups View	10-2
Figure 10-3: Guest Access Group Settings.....	10-2
Figure 10-4: Password Setting	10-3
Figure 10-5: Account Settings	10-3
Figure 10-6: Guest Access Controllers	10-3
Figure 10-7: Role Attributes	10-4
Figure 10-8: Create New Guest Access Devices	10-4
Figure 10-9: Authentication and Accounting Port Numbers.....	10-4
Figure 10-10: Shared Secret.....	10-5
Figure 10-11: Authentication and Accounting Port Numbers.....	10-5
Figure 10-12: Authentication Server List	10-5
Figure 10-13: Authentication Server Fields Prepopulated.....	10-6
Figure 10-14: Authentication and Accounting Port Numbers.....	10-6
Figure 10-15: Authentication Server Created	10-6
Figure 10-16: Default Group Controller	10-7
Figure 10-17: Create Guest User	10-7
Figure 10-18: Guest Information	10-7
Figure 10-19: Guest Login.....	10-8
Figure 10-20: Guest Group	10-8
Figure 10-21: External Authentication Test.....	10-8
Figure 10-22: Authentication and Accounting Port Numbers.....	10-9
Figure 10-23: Create New Administrative User.....	10-10
Figure 10-24: Guest Access Tabs	10-10
Figure 10-25: Admin only can modify groups or controllers.....	10-11
Figure 10-26: Create New Report - Select Report Type	10-12
Figure 10-27: Create New Report - Completed Fields	10-13
Figure 10-28: Reports - User Creation over Time	10-13



About This Guide

The *BlueView™ Management System User Guide* provides complete instructions for installing the BlueView Management System and using it to manage and configure Bluesocket devices, i.e., BlueSecure™ Controllers (BSCs), Access Points (BSAPs), and Centralized Sensors, as well as Cisco, Proxim/Avaya/Orinoco, 3COM, Netgear, Symbol, and Enterasys access points installed on your network. This section introduces the document and describes:

- Audience
- Document Organization
- Notational Conventions
- Related Documents
- Terminology

Audience

The *BlueView™ Management System User Guide* is written for network administrators who will physically install and power up the BlueView Management System, and then use its HTML-based administrator console to discover, monitor, manage, and configure Bluesocket devices installed on their network. Administrators can also use BlueView for configuring and managing stand alone access points that may be installed on their network.

We assume our audience is knowledgeable of and has experience administering switches, routers, or similar computer hardware, and is familiar with the BlueSecure Controller and how it is configured. Complete BlueSecure Controller configuration information and procedures are included in the *BlueSecure Controller Setup and Administration Guide* shipped with each BSC.

Document Organization

The information in this guide is organized as follows:

- Chapter 1, "*An Overview of the BlueView Management System*," describes how you can use BlueView to manage and configure Bluesocket devices on your network.
- Chapter 2, "*Installing the BlueView Management System*," provides complete procedures for mounting the *BlueView Management System*, connecting it to your network, and powering it up.
- Chapter 3, "*Getting Started*," provides procedures for getting up and running with BlueView including connecting to the BlueView Management System remotely via its administrator console, discovering the Bluesocket


devices and stand alone access points on your network, and organizing these devices into groups.

- Chapter 4, "*Configuring BlueView*," provides procedures for configuring the BlueView Management System for use on your network including adding administrative users, specifying BlueView's network interface settings, adding static routes, setting BlueView's time, specifying how BlueView is to store logs and alarms in its internal database, configuring an SNMP agent on BlueView, and defining the mail server BlueView is to use to send email notifications.
- Chapter 5, "*Configuring Stand Alone Access Points with BlueView*," gives the procedures you should follow to configure stand alone APs for management by BlueView including listing stand alone access points, editing stand alone access point configurations, creating stand alone AP configuration templates, adding a stand alone AP for management by BlueView, configuring stand alone AP SSIDs, and configuring stand alone AP RADIUS authentication servers.
- Chapter 6, "*Monitoring WLAN Devices*," describes how to monitor Bluesocket devices on your network for status including summary information, log data, and alarm data. Additionally, procedures are provided for generating status reports.
- Chapter 7, "*Maintaining and Provisioning WLAN Devices*," lists procedures for running BlueView jobs to complete Bluesocket device maintenance and provisioning tasks such as: restarting services, rebooting devices, shutting down devices, backing up and restoring device configurations, generating a configuration template, pushing out a configuration template to devices, upgrading system software to a new version, and installing or removing system software patches. Additionally, procedures for pushing out a firmware image file to stand alone access points, and managing BSAPs and BSAP SSIDs are provided.
- Chapter 8, "*Configuring RF Intrusion Detection and Containment*," provides procedures for configuring BlueView to provide RF intrusion detection and containment services including: identifying authorized RF stations on your network, configuring sensor alarms and RF Autocontainment, configuring sensor notifications, identifying approved SSIDs, and importing bulk RF configuration files including authorized RF stations, approved SSIDs, and manufacturer MACs.
- Chapter 9, "*Administering Your BlueView System*," gives procedures for restarting, rebooting, and shutting down BlueView; backing up and restoring the BlueView database; upgrading the BlueView system software; installing patches for the BlueView system software; switching BlueView software images, running diagnostics; and accessing the BlueView serial interface.
- Appendix A, "*Contacting Bluesocket, Inc.*," describes how to contact Bluesocket for additional product information or support.

Notational Conventions

This guide uses the following notational conventions to convey information:

 **Note:** Notes call attention to important information.

 **Caution:** Cautionary statements call attention to a condition that could result in the loss of data, damage to equipment, or physical injury.

Italic text indicates emphasis or highlights the titles of books used in cross-references.

`Monospace` text represents information displayed on the local BlueView command console or on other computer displays.


monospace text represents information that you enter at the BlueView command console or at other computer terminals.

Related Documents

Please refer to these other documents for information about your Bluesocket products:

- *BlueSecure Controller Quick Start Guide* - Refer to this document included with your BSC distribution for a concise overview of how to get up and running quickly with the Bluesocket BlueSecure Controller.
- *BlueSecure Controller Setup and Administration Guide* - Refer to this document included with your BSC distribution for complete instructions for installing, powering up and configuring the Bluesocket BlueSecure Controller.
- *BlueSecure Access Point 1500/1540 Installation Guide* - Refer to this document included with your BSAP distribution for a concise overview of how to get up and running quickly with the Bluesocket BlueSecure Access Point.

Terminology

 **Note:** For brevity, we use the following terms and abbreviations:

- *BlueView* and *BVMS* refer to the BlueView Management System.
- *BSC* refers to the Bluesocket BlueSecure Controller product family as a whole, unless reference to a specific BlueSecure Controller model is required.
- *BSAP* refers to the Bluesocket BlueSecure Access Point product family as a whole, unless reference to a specific BlueSecure Access Point model is required.

1

An Overview of the BlueView Management System

This chapter introduces you to the BlueView™ Management System and includes:

- An Introduction to the BlueView Management System
- Manageable Bluesocket Devices
- Features and Functions
- Technical Specifications

An Introduction to the BlueView Management System

The BlueView™ Management System (BlueView) provides centralized configuration, policy-management, monitoring, and RF intrusion detection and containment capabilities to facilitate rapid configuration and remote management of multi-site Wireless LAN (WLAN) deployments.

Network Administrators can use BlueView to auto-discover the Bluesocket BlueSecure Controllers (BSCs) and BlueSecure Access Points (BSAPs) installed on their network and automate maintenance tasks such as configuration backups, patch applications and removals, and software upgrades.

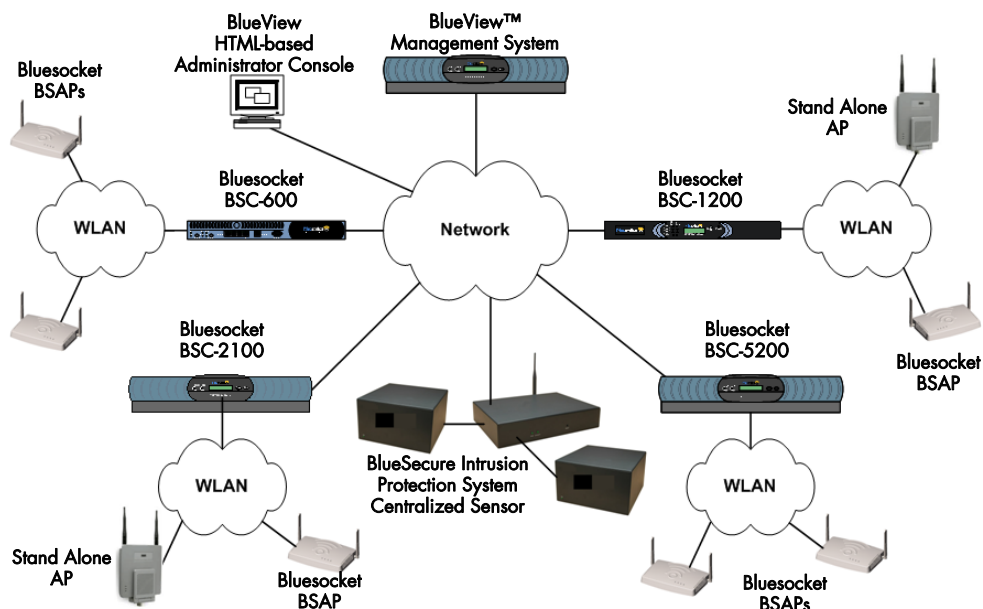


Figure 1-1: The BlueView Management System

BlueView communicates with and manages the BSCs on your network using Simple Network Management Protocol (SNMP) v2c and v3, and the Bluesocket Application Programming Interface (API). BlueView automatically polls BSCs on the network for connectivity, status, and configuration, and continually refreshes its display with the updated data.

BlueSecure Controllers on your network communicate with and manage the BSAPs connected to their managed interface. When polled, BlueSecure Controllers send status information about the BSAPs under their control to BlueView. BlueSecure Access Points can be configured to function as access points and/or RF sensors. BlueView manages BSAPs operating in AP-only mode, AP/sensor mode, or sensor-only mode. BlueView will use BSAPs operating in sensor mode to detect and contain any rogue APs discovered on the network.

Additionally, you can use BlueView to manage, monitor, and update the firmware on stand alone access points manufactured by Cisco, Proxim/Avaya/Orinoco, 3COM, Netgear, Symbol, and Enterasys that are installed on your network.

Housed in a 2U rack-mountable chassis, the BlueView hardware features dual highspeed Gigabit Ethernet interfaces to connect the system to your network, front-panel LCD and

LED status indicators, and a large capacity hard-drive to maintain an embedded database of traps and logs received from BSCs on your network.

You can establish secure remote connections to BlueView over the Internet and use its intuitive HTML-based administrator console to monitor, manage, and configure the Bluesocket devices on your network.


Manageable Bluesocket Devices

You can use BlueView to discover and manage any Bluesocket device on your network that meets the following specifications:

- **BlueSecure Controller** – Models BSC-600, BSC-1200, BSC-2100, or BSC-5200 running system software release v4.1 or later. BSCs must be running system software release v5.0 or later to communicate with and manage BlueSecure Access Points. BSCs must be running system software release v5.1 or later to configure, manage, perform RF containment using BSAP 1500/1540s operating in sensor mode.
- **BlueSecure Access Point** – Models BSAP-1500, BSAP-1540, BSAP-1700, and BSAP-1800.

BSCs meeting the above specifications are displayed in the BlueView administrator console and are manageable for software image, patch updates, and configuration backups.

BSAPs meeting the above specifications are displayed in the BlueView administrator console and are manageable for software image and configuration updates.

 **Note:** We recommend that you do not use the BSC replication feature on BSCs being managed by the BlueView Management System. Follow the procedure given in “Configuring the BSCs on Your Network to Support BlueView” on page 3-2 to prepare the BSCs on your network to be fully manageable by BlueView.

Features and Functions

The BlueView Management System provides these important features and functions to enable you to monitor, manage, and configure your multi-site deployments of Bluesocket devices:

- **auto-discovery** - You can enter a range of IP addresses across which BlueView will automatically discover manageable BlueSecure Controllers. Additionally, you can configure BlueView to discover and manage specific devices by entering individual Controller IP addresses, and you can also configure a BlueSecure Controller to “announce” itself to BlueView by logging into the BSC’s administrator console. BlueView will continually poll discovered devices for connectivity and status.
- **fault monitoring** - BlueView serves as an SNMP trap receiver for all managed BSCs on the network. BlueView intelligently interprets received traps and generates a sortable and filterable alarm table for administrator review. Alarm table entries include:
 - date and time
 - severity - critical, error, warning, and informational
 - type - cold start, warm start, link up/down, enterprise message
 - address - sending BSC’s fully qualified domain name or IP address
 - message - informative description of the fault

You can associate an action (e.g., sending an email notice) with received alarms and delete reviewed alarms. BlueView automatically manages its alarm table based on maximum table size (MB) and entry count parameters you define.

- **log management** - BlueView maintains a log database in non-volatile memory that serves as a central repository for log records received from managed Bluesocket Controllers. BlueView provides a log browser that enables you to filter and sort received log records that include the following information:
 - record number - incrementing counter of received log records
 - address - sending BSC's Fully Qualified Domain Name (FQDN) or IP address
 - date and time - indicates when log record was received
 - severity level - emergency, alert, critical, error, warning, notice, information, or debug
 - application - source BSC process, e.g., DHCP server
 - message - informative description of log entry

You can manage received log records by creating a backup file of specified records and deleting reviewed records. BlueView automatically manages its log database based on maximum size (MB) and entry count parameters you define.
- **network diagnostics** - BlueView provides you the ability to run diagnostics including ping, traceroute, and netstat on your network of BlueSecure Controllers.
- **policy management** - Bluesocket BSCs use role-based authorization to define which network resources and destinations in the enterprise a user may access, the bandwidth he or she may use, and whether a secure tunneling protocol such as IPsec or PPTP is required for the connection. You can create BSC configuration templates on BlueView to define roles that enforce network usage policies and then push these configurations out to BSCs on your network.
- **job scheduling** - BlueView provides a powerful scheduling tool that enables you to automate Bluesocket device maintenance and provisioning tasks such as: restarting BSC services, rebooting BSCs, shutting down BSCs, backing up and restoring BSC configurations, generating a BSC configuration template, pushing out a configuration template to BSCs, upgrading BSC and BSAP system software to a new version, and installing system software patches.
- **status reports** - Generate informative inventory and user activity reports in HTML, Adobe Acrobat, and Microsoft Excel formats. Reports can be generated for device groups or individual devices.
- **connection monitoring** - Display and monitor active user connection status along with other user information, such as IP address, assigned role, and throughput statistics, and Intrusion Detection System status.
- **RF heat maps** - BlueView enables you to create RF heat maps, i.e., RF coverage maps, from imported floor plans of buildings in which you have installed or plan to install WLANs secured and managed with Bluesocket devices.
- **Static and Dynamic Groups** - You can organize the devices on your network into static logical groups that have meaning for your network, e.g., geographical location, network location, software version, function, etc. You can also define dynamic groups that contain device properties in which you are interested, e.g., model number, firmware version, CPU usage, etc. Both static and dynamic groups can be referenced when defining provisioning and maintenance jobs, or status reports.
- **Stand Alone AP management** - In addition to managing and monitoring Bluesocket devices on your network, you can use BlueView to manage, monitor, and update the firmware on access points manufactured by Cisco, Proxim/Avaya/Orinoco, 3COM, Netgear, Symbol, and Enterasys.
 - Cisco Aironet access points:

- Model 350 IOS and VxWorks.
- Model 1100/1131
- Model 1200/1210/1220/1230/1231/1240 IOS and 1200/1220 VxWorks
- Model 1300
- Model 1400
- Proxim/Avaya/Orinoco access points:
 - Model AP-2000
 - Model AP-4000
- 3COM access points:
 - Model 8750 (Only credentials, SNMP location and contact, and radio settings may be edited)
- Netgear access points:
 - Model WG102
 - Model WG302
 - Model WAG302
- Symbol access points:
 - Model 4131
- Enterasys access points:
 - Roamabout RBT-4102

Additionally, the following APs are displayed within BVMS, but their configurations cannot be edited.

- Cisco:
 - Model 340
- Proxim/Avaya/Orinoco:
 - Model AP-600
 - Model AP-700
 - Model AP-1000
 - Model AP-2500
- Bluesocket:
 - AP-1600
- **RF Intrusion Detection/Protection** - Using BSAP 1500s operating in sensor mode or BlueSecure Intrusion Protection System Centralized Sensors managed by BlueView, you can perform a full-range of RF intrusion detection and protection services:
 - **Detect all rogue wireless devices and activity** - Detect unauthorized wireless devices that could be a potential gateway into the wired network, including:
 - wireless access points
 - Wi-Fi enabled clients (i.e., laptops, desktops)
 - soft access points
 - ad hoc networks
 - peer-to-peer networking between user stations
 - accidental associations
 - **Location Awareness** - Provide detailed location data about wireless devices.
 - **RF Containment** - Should a rogue AP or client be discovered, BlueView configures the BSAP nearest the rogue device to initiate containment using

802.11 de-authentication and/or disassociation messages. Up to five BSAPs can participate in the containment if range permits. The sensors participating in the RF containment remain online for wireless access during the containment period.

- **Intrusion Detection** - Detect the following wireless intrusions:
 - identity thefts from MAC spoofing
 - man-in-the-middle attacks
 - denial-of-service attacks
 - denial-of-service attacks with excessive MAC addresses
 - dictionary attacks
 - suspicious activity and impending threats
 - watch list stations/laptops entering the air space
 - repeated attempts by a station to connect with multiple applications
 - suspicious traffic from clients
 - Netstumbler and Wellenreiter probing
- **Performance Analysis** - Monitor all authorized wireless networks and clients to:
 - identity performance problems
 - monitor bandwidth and data transfer
 - monitor client connections
 - monitor channel usage

Technical Specifications

Technical Specifications for the BlueView Management System are listed below.

Physical Dimensions	Width:17.5 inches (445 mm) Depth:17.5 inches (445 mm) Height:3.6 inches (88 mm) — 2U
Network Interfaces	Two high-bandwidth 10/100/1000 Ethernet RJ-45 interfaces
Storage	High-speed disk drive accommodating up to 120 GB database
Communication Protocols	SNMP v2c, v3; XML-RPC, HTTP/HTTPS
Power	Power Supply:350 Watt, auto-sensing, 110/240 VAC @ 47/63 Hz
Environmental	Operating Temperature:50 to 95° F (10 to 35° C) Humidity:40 to 80% non-condensing
Approvals	FCC, VCCI, CE and UL

2)))

Installing the BlueView Management System

This chapter provides complete installation procedures for the BlueView Management System and includes:

- Overview of the Installation Procedure
- General Safety Considerations
- The BlueView Displays, Controls, and Connectors
- Preparing Your Network
- Installation Location Requirements
- Mounting the BlueView Chassis on a Desktop
- Rack-mounting the BlueView Chassis
- Connecting the BlueView Management System to Your Network
- Connecting BlueView to its Power Source
- Powering Down the BlueView Management System

Overview of the Installation Procedure

You must complete the following steps to install the BlueView Management System:

1. Prior to beginning the installation procedure, familiarize yourself with the safety considerations listed starting in “General Safety Considerations” on page 2-2.
2. Familiarize yourself with the BlueView front- and rear-panel displays, controls, and connectors as described starting in “The BlueView Displays, Controls, and Connectors” on page 2-3.
3. Ensure that you have completed the prerequisite steps listed in “The BlueView Displays, Controls, and Connectors” on page 2-3 to prepare your network before attempting to install and connect the BlueView Management System.
4. Evaluate your site and select a suitable location in which to install the BlueView Management System. The selected installation location must meet the environmental, rack, and power requirements listed in “Installation Location Requirements” on page 2-5.
5. Mount the BlueView chassis in the selected installation location. You may either:
 - rest the BlueView chassis on a flat, stable surface for desktop operation as described in “Mounting the BlueView Chassis on a Desktop” on page 2-6, or
 - mount the BlueView chassis in a standard 19-inch, two-post equipment rack by following the steps listed in “Rack-mounting the BlueView Chassis” on page 2-7.
6. Connect the BlueView Management System to your network(s) of Bluesocket devices as described in “Connecting the BlueView Management System to Your Network” on page 2-8.
7. Connect the BlueView Management System to an appropriate AC power source and power it up as described in “Connecting BlueView to its Power Source” on page 2-8.

General Safety Considerations

The BlueView Management System has been listed by Underwriters Laboratories (UL) and is shipped from the factory in a safe condition.

This section provides information and procedures that must be followed to ensure safe installation and operation of the BlueView Management System.



Caution: Observe the following precautions when installing or servicing the BlueView Management System:

- The power supply in the BlueView chassis may produce safety extra low voltage (SELV) or low voltage energy hazards that can cause physical injury. Never remove the BlueView chassis cover to access any of the components inside the chassis.
- Observe and follow service markings and labels on the BlueView equipment. Access and service BlueView equipment only as instructed in your Bluesocket user documentation.
- If any of the following conditions occur, disconnect the BlueView equipment from all power sources, and contact Bluesocket, Inc.:
 - the equipment power cable or connector is damaged
 - an object has fallen into the equipment
 - the equipment has been exposed to water
- Keep the BlueView Management System away from radiators and heat sources. Do not block the ventilation holes in the BlueView chassis.

- Do not allow liquid to enter the BlueView chassis, and do not operate the system in a wet environment. If the BlueView Management System gets wet, contact Bluesocket to arrange for service.
- Do not push any objects into the BlueView chassis vents or openings. Doing so can result in fire or electrical shock.
- Connect the BlueView Management System to the correct external power source as indicated on the electrical ratings label. Consult Bluesocket, Inc. if you are not sure of the power required to operate the equipment in your locale.
- Use only approved power cable(s). If you have not been provided with power cables for your BlueView Management System, purchase power cables that are approved for use in your country.
- To help protect the BlueView components from sudden transient increases or decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position BlueView cables and power cords carefully; route cables and power cords so they cannot be stepped on or tripped over. Be sure that nothing rests on the BlueView cables or power cords.

Precautions for Rack-mounted Equipment



Caution: Observe the following precautions when installing the BlueView Management System in an equipment rack:

- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Ensure the equipment rack is fixed in place.
- Extend only one component at a time from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or rest weight on a BlueView Management System installed in the rack.

The BlueView Displays, Controls, and Connectors

Prior to connecting the BlueView Management System to your network and powering it up, you should familiarize yourself with its front- and rear-panel displays, controls, and connectors.

The following figure shows the BlueView Management System front and rear panel displays, controls, and connectors.

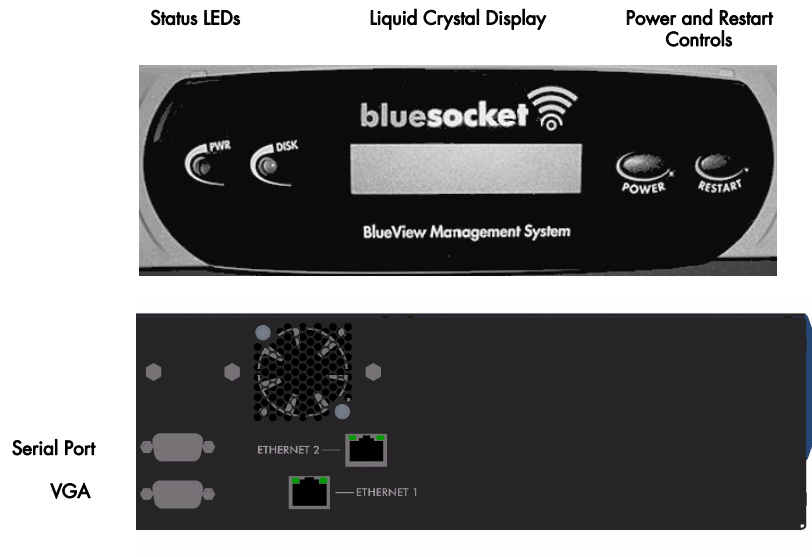


Figure 2-1: BlueView Displays, Controls, and Connectors

Status LEDs

The BlueView Management System provides the following front-panel status LEDs:

- **PWR** - Lights when BlueView is connected to an AC power source and its rear-panel power switch is in the closed position (I).
- **DISK** - Flickers when BlueView is writing data to or reading data from non-volatile memory.

On the BlueView rear-panel, **ACT/LINK** LEDs are provided for the network interface ports, Ethernet 1 and Ethernet 2. The ACT/LINK LED is off when there is no link, lights green when a 100 Mbps link is established, and lights orange when a 1000 Mbps link is established. The ACT/LINK LED blinks to indicate activity on the link.

LCD

The BlueView Management System provides a 2x16-character, liquid crystal display (LCD) to display the IP address configured for its primary network interface, Ethernet 1.

Power Control

With the BlueView Management System connected to its AC power source and its rear-panel power switch in the closed position (I), press the Power button to power up BlueView.

If the BlueView Management System is running and you press the front-panel Power button, BlueView will stop all active services after a slight delay. After all services are shutdown, BlueView executes its normal power-down sequence and shuts off completely.

Restart Control

If the BlueView Management System is running and you press the front-panel Restart button, BlueView will stop and then restart all active services automatically. In

approximately 30 to 60 seconds after you have pressed the Restart button, the LCD display will indicate that BlueView services have re-started.

Serial Port

The BlueView Management System provides a serial port equipped with a DB-9, male connector to support local console configuration. Normally, you will never use the BlueView serial port. You should configure the BlueView Management System via its serial interface only in the rare event that you lose access to the BlueView web-based administrator console due to an Internet service outage. The BlueView Management System serial interface supports only a subset of BlueView's configurable parameters. See "Accessing BlueView Functions via the BlueView Serial Port" on page 9-10 for details about accessing the BlueView serial interface.

Network Ports

Use the Network Ports to connect the BlueView Management System to your network(s) of Bluesocket devices. Each Network Port is equipped with a copper, RJ-45 10/100/1000 Mbps Ethernet connector. If you are connecting the BlueView Management System to a single network of Bluesocket devices, use the primary BlueView network port, **Ethernet1**, to complete the connection.

Preparing Your Network

Verify the following before attempting to install and connect your BlueView Management System:

- You have installed and configured your BlueSecure Controllers as described in the *Bluesocket BlueSecure Controller Setup and Administration Guide*.
- You have installed and configured your BlueSecure Access Points as described in the *Bluesocket BlueSecure Access Point Installation Guide*.
- Ensure that you have Ethernet connections to the protected network(s) on which your BlueSecure Controllers are installed.

Installation Location Requirements

Follow these guidelines when selecting an installation location for the BlueView Management System.

Environmental Ensure that the BlueView installation site meets the following environmental specifications:

- Operating Temperature: 50 to 95° F (10 to 35° C)
- Operating Humidity: 40 to 80% non-condensing

Also, ensure the installation site is free of dust and moisture.

Rack Ensure that the two-post, 19-inch equipment rack in which you install the BlueView Management System meets the following specifications:

- the rack conforms to the ANSI/EIA-310-D-92 specifications
- the rack is fixed in place
- the rack has an open back and open front to allow the BlueView Management System to cool adequately
- the rack has front and side stabilizers installed

Space Ensure that you have adequate rack space to install the BlueView Management System:

- The BlueView Management System occupies 3.50 inches/89 mm (2U) of vertical rack space.

- Ensure there is at least 15 inches/381 mm of clearance in front of and behind the rack. This space is required to connect and disconnect network cables.

AC Power Ensure that the BlueView Management System AC power source meets the following specifications:

- AC input voltage: dedicated, grounded, single-phase circuit 100 to 240 VAC
- AC frequency: 50 to 60 Hz.

Mounting the BlueView Chassis on a Desktop

Rack-mounting the BlueView Management System is optional. You may operate BlueView while it is resting on a desktop.

The BlueView Management System is cooled from ventilation holes located on the sides of its chassis and on its front and back panels. Ensure that these vents remain free of obstruction while BlueView is operating on the desktop.

To mount the BlueView Management System on a desktop:

1. Choose a level, stable desktop that will support the weight of the BlueView chassis.
2. Install a rubber pad on each of the four desktop bumpers (see Figure 2-2).

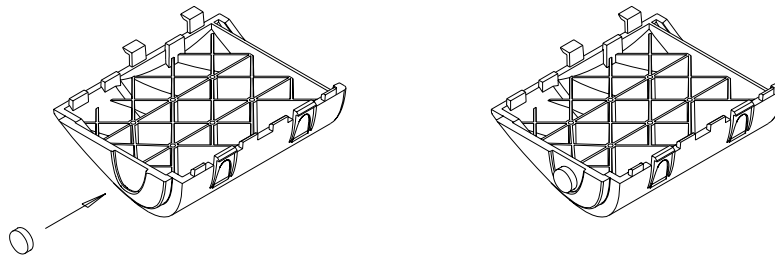


Figure 2-2: Attaching a Rubber Pad to a Desktop Bumper

3. Install each of the four BlueView desktop bumpers (see Figure 2-3).

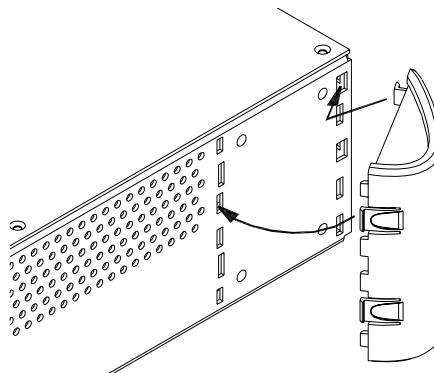


Figure 2-3: Attaching the BlueView Chassis Desktop Bumper

Snap the bumpers into the BlueView chassis to prevent the chassis from slipping on the desktop and to enhance its appearance.

4. Install the BlueView chassis cap (see Figure 2-4).

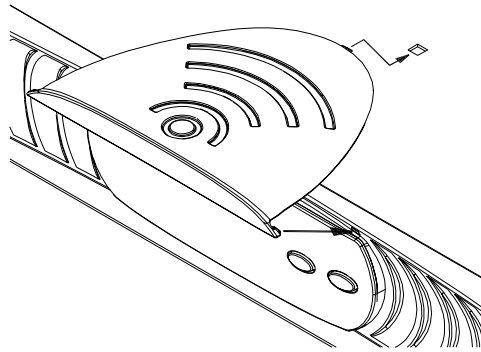


Figure 2-4: Attaching the BlueView Chassis Cap

The cap enhances the appearance of the BlueView chassis while the chassis is resting on the desktop.

After mounting the BlueView chassis on the desktop, connect the BlueView Management System to your network as described in “Connecting the BlueView Management System to Your Network” on page 2-8, and then power it up by following the procedure given in “Connecting the BlueView Management System to Your Network” on page 2-8.

Rack-mounting the BlueView Chassis

You may install the BlueView Management System in any two-post equipment rack or cabinet that conforms to ANSI/EIA-310-D-92 specifications.

- ☞ **Note:** The BlueView Management System should not have desktop feet, bumpers, or a chassis cap installed when mounted in an equipment rack. If these are installed, remove them prior to rack-mounting the BlueView chassis.

Follow these steps to mount the BlueView Management System in a two-post equipment rack:

1. Using a #2 Phillips-head screwdriver and the eight supplied #8-32 Phillips-head screws, attach the mounting brackets to the sides of the BlueView chassis as shown in Figure 2-5.
- ☞ **Note:** You can attach the mounting brackets to either the front or rear of the BlueView chassis depending on the cable access you prefer.
2. Position the BlueView chassis in your equipment rack.

3. Secure the BlueView Management System's mounting brackets to the rack rails using the appropriate hardware for your rack.

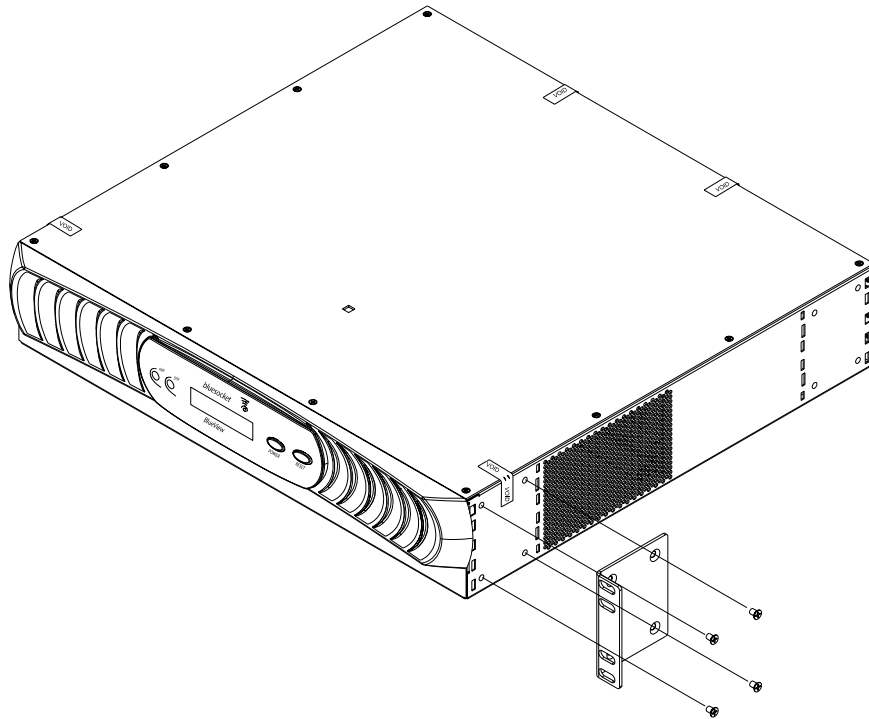


Figure 2-5: Attaching the Mounting Brackets to the BlueView Chassis

After rack-mounting the BlueView chassis, connect the BlueView Management System to your network as described in "Connecting the BlueView Management System to Your Network" on page 2-8, and then power up the BlueView Management System by following the procedure given in "Connecting the BlueView Management System to Your Network" on page 2-8.

Connecting the BlueView Management System to Your Network

After you have mounted the BlueView chassis in place, you must connect it to your network(s) of Bluesocket devices.

Follow these guidelines when connecting the BlueView Management System to your network:

- Use a straight-through Ethernet cable terminated with an RJ-45 connector to connect BlueView to your network(s) of Bluesocket devices.
- If you are connecting the BlueView Management System to a single network of Bluesocket devices, use the primary BlueView network port, **Ethernet 1**, to complete the connection.

Connecting BlueView to its Power Source

A power cord is supplied with the BlueView Management System to connect it to an AC power source. Ensure that the supplied power cord is rated for the AC power available at your location.

Follow these steps when connecting the BlueView Management System to an AC power source:

1. Ensure the AC power switch located on the BlueView rear panel is in the OFF (O) position.
2. Connect the female end of the supplied power cord to the power receptacle located on the rear panel of the BlueView chassis.
3. Connect the male end of the BlueView power cord to an AC power source meeting the following specifications:
 - AC input voltage: dedicated, grounded, single-phase circuit 100 to 240 VAC
 - AC frequency: 50 to 60 Hz.
4. Switch the AC power switch located on the BlueView rear panel to the ON position (I).
5. Press the **Power** button located on the front panel.

As the BlueView Management System powers up, its cooling fans run and its status LEDs light. The LCD on its front panel shows boot-up sequence messages, DHCP status, and IP address status. After the bootup is complete, the BlueView LCD shows the IP address for its primary network interface, Ethernet 1.

Note the IP address displayed on the BlueView front-panel LCD. You will need to know this IP address to access the BlueView administrator console as described in Chapter 3, "Getting Started".

Powering Down the BlueView Management System

You should always power down BlueView using its software shutdown feature as described in Chapter 7.



Caution: Never use the rear-panel power switch to power down the BlueView Management System. Failing to power down BlueView using its software shutdown function or the shutdown procedure listed below may render the BlueView Management System un-bootable.

Follow these steps to power down a running BlueView Management System:

1. Press the front-panel **Power** button.
2. The BlueView Management System will stop all active services after a slight delay. After all services are shut down, BlueView executes its normal power-down sequence and shuts off.

3)))

Getting Started

The BlueView Management System provides an intuitive, easy-to-use administrator console that you can access using any web browser.

To get started with the BlueView Management System, you'll need to configure the BlueSecure Controllers on your network for management by BlueView, access the BlueView administrator console, discover the Bluesocket controllers and access points installed on your network, and then organize these devices into logical groups.

This chapter provides the procedures you should follow to get up and running with the BlueView Management System and includes:

- Configuring the BSCs on Your Network to Support BlueView
- Accessing the Administrator Console
- Discovering WLAN Devices on Your Network
- Organizing Your Bluesocket Devices into Groups

Configuring the BSCs on Your Network to Support BlueView

Prior to using BlueView to discover the BSCs on your network, you must configure each BSC on your network to support management and monitoring by BlueView. To fully support management by BlueView, each BSC on your network must:

- be running an SNMP v3 agent
- have an administrator account set up with SNMP and API access rights

Follow these steps to configure a BSC to support management by BlueView:

1. Access the BSC's administrator console by entering this URL in your web browser:
https://BSC_IP_Address/admin.pl
 where **BSC_IP_Address** is the BSC's configured Protected Port IP address (i.e., the IP address displayed on the LCD of the BSC you are trying to access).
2. Configure the BSC to run an SNMP v3 agent:
 - a) Click the BSC's **General** tab, and then click the **SNMP Agent** tab.
 The SNMP Settings page appears as shown in Figure 3-1.

Figure 3-1: SNMP Settings Page

- b) Select **V3** from the **SNMP Agent** to run a v3 SNMP agent on the BSC.
 You needn't change any other settings on the page.
 - c) Click **Save** to save the SNMP agent settings to the BSC database.
3. Create an administrator account that has SNMP and API access rights to the BSC:
 - a) Click the **User Authentication** tab in the BSC administrator interface, and then click the **Administrative User** tab.
 - b) Select **Administrative User** from the **Create** drop-down list on the Auth page.
 The New admin page appears as shown in Figure 3-2.
 - c) Enter the administrator's login name in the **Name** field.
 - d) Enter the **New password**, and then re-enter it in the **Confirm new password** field.
 - e) Enter the administrator's e-mail address in the **Email address** field.
 - f) Mark **Full** to grant the administrator write access to all BSC functions.

Figure 3-2: New Admin User Page

- g) Mark the **Allow admin to access using SNMP** checkbox to grant the administrator access to the BSC using SNMP v3. Note that SNMP v3 requires a user ID and password, rather than a community string, to make SNMP requests.
- h) Mark the **Allow admin to access using the API** to grant the administrator access to the BSC using the Bluesocket API.
- i) Mark the **Enable user** checkbox to make the account available.
- j) Click **Save** to save the administrator information to the BSC database.

4. Restart the BSC to effect the configuration changes you have made:
 - a) Click the **Maintenance** tab in the BSC administrator interface, and then click **Restart Services**. The BSC restart page appears.
 - b) Mark the **Restart All Services** and **Now** radio buttons.
 - c) Click **Submit** to Restart the BSC immediately.

Accessing the Administrator Console

You may access the BlueView administrator console using any web browser. You may run multiple instances of the administrator console on your network.

- “Logging Into the Administrator Console for the First Time” on page 3-4.
- “Installing the Bluesocket SSL Certificate” on page 3-5.
- “Subsequent Administrator Console Logins” on page 3-7.
- “Obtaining Online Help” on page 3-7.
- “Logging Out of the Administrator Console” on page 3-7.

Logging Into the Administrator Console for the First Time

To access the BlueView administrator console for the first time:

1. Power up the BlueView Management System as described in “Connecting BlueView to its Power Source” on page 2-8.
2. Enter the following URL in your web browser:

`https://BVMS_IP_Address`

where **BVMS_IP_Address** is the IP address displayed on the LCD of the BlueView Management System you are trying to access. BlueView displays its primary network interface (Ethernet 1) IP address on its LCD upon startup. Your browser may display a security alert stating that data received from the web server on the BlueView Management System is not from a trusted source.

Click **Yes** to ignore the alert, and the BlueView administrator console login page appears as shown in Figure 3-3.

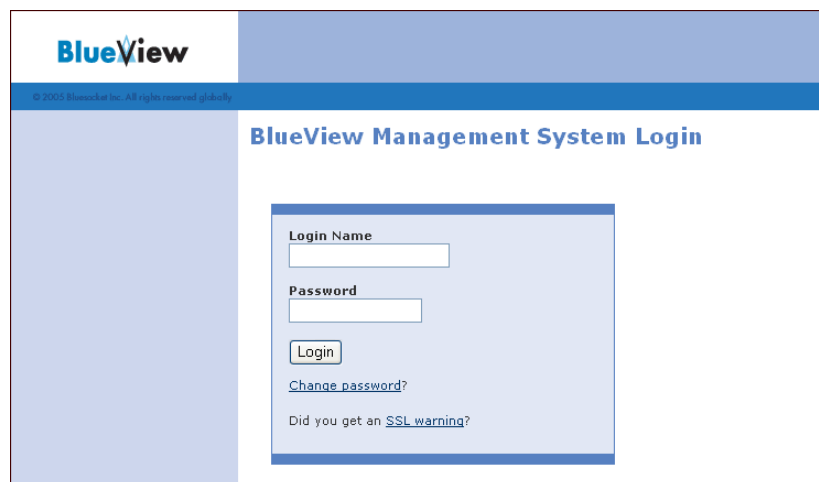



Figure 3-3: BlueView Administrator Login Page

 **Note:** If you wish to eliminate the display of future security alerts when you access the BlueView administrator console, then you must download and install the Bluesocket SSL certificate as described in “Installing the Bluesocket SSL Certificate” on page 3-5.


3. For security reasons, we recommend that you change the password associated with your default administrator account on your first login.

Click the **Change password?** link on the administrator login page to change your default administrator account password.

Note that the administrator **Login name** and **Password** fields are case-sensitive.

Enter the default administrator account of **admin** in the **Login name** field.

Enter the default password of **blue** in the **Password** field, your new password in the **New Password** and **Re-Enter New Password** fields, and then click **Login**.

 **Note:** Be sure to store your new BlueView **admin** account password in a safe location. You will not be able to log into the BlueView administrator console without it. If you forget or lose your password, access the BlueView serial port as described in “Accessing BlueView Functions via the BlueView Serial Port” on page 9-10 and then issue the dbinit command to re-initialize the BlueView database. This restores all database defaults including the default administrator account and password.

A dialog appears displaying the Bluesocket End User License Agreement. Read and acknowledge the license agreement, and then close the dialog.

The Bluesocket BlueView administrator console Getting Started page appears as shown in Figure 3-4.

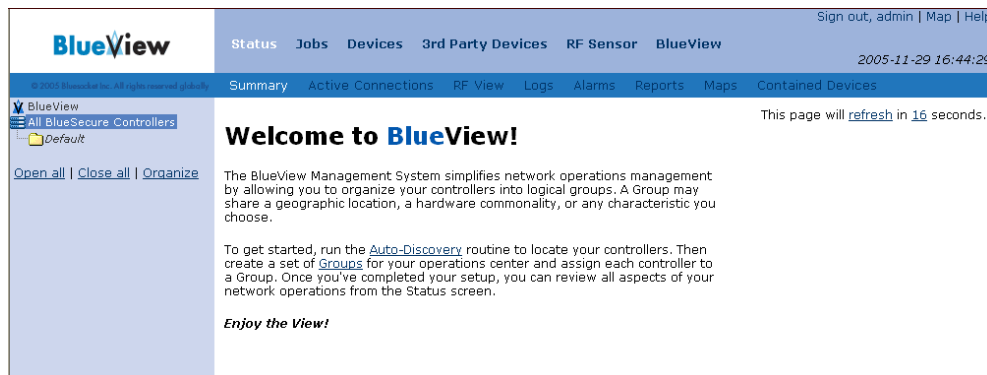


Figure 3-4: BlueView Getting Started Page

You are now ready to discover the Bluesocket devices installed on your network as described in “Discovering WLAN Devices on Your Network” on page 3-8, and then organize these devices into groups as described in “Organizing Your Bluesocket Devices into Groups” on page 3-15.

Installing the Bluesocket SSL Certificate

When accessing the administrator login page, you may receive an alert that data received from the web server on the BlueView is not from a trusted source (see Figure 3-5).

If you receive this warning, it is because BlueView ships with a private SSL digital certificate and the web browser on your computer does not have a trust relationship with the private digital certificate authority. You must install the private certificate authority's

root certificate in your browser's certificate store before your browser will trust the BlueView administrator console login page.

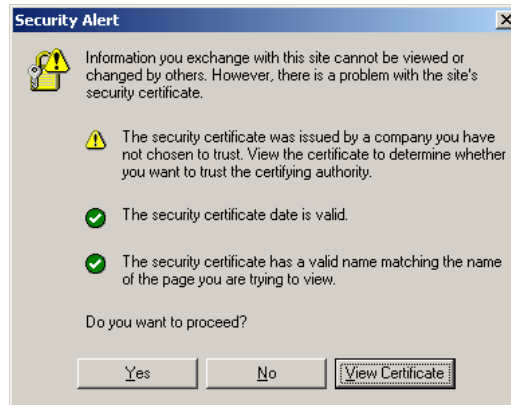


Figure 3-5: Security Certificate Alert

You can prevent the display of this security alert when you log into the BlueView administrator console by downloading the Bluesocket secure sockets layer (SSL) login certificate to the computer on which you are running your web browser.

To download the Bluesocket SSL login certificate to your web browser host computer:

1. Enter the `https://BVMS_IP_Address` URL in your web browser, where `BVMS_IP_Address` is the IP address displayed on the LCD of the BlueView Management System you are trying to access.
2. Click the **Did you get an SSL warning?** link on the administrator login page, and then click **Open** from the file download dialog.

The Certificate dialog appears.

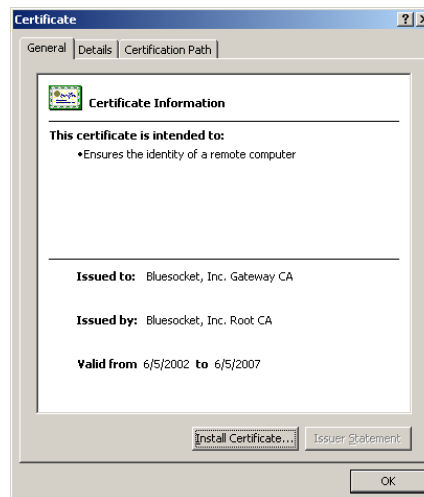


Figure 3-6: Bluesocket SSL Certificate Dialog

3. Click **Install Certificate** and then follow the instructions that appear in your web browser to download and install the Bluesocket SSL certificate on your web browser host.

As an alternative to installing the Bluesocket SSL certificate, you can acquire an SSL login certificate from another CA provider, and then upload the certificate to the BlueView.

Subsequent Administrator Console Logins

After you have logged into the BlueView administrator console for the first time, and have changed the password associated with the default admin account and installed the Bluesocket SSL Certificate on your web browser host, subsequent logins to the BlueView administrator console are quick and straight forward.

Simply log in using one of the following pre-defined administrator accounts:

- **admin** - enables you to view and change BVMS configuration settings.
- **monitor** - enables you to view but not change current BVMS configuration settings. The default password for the monitor read-only account is **blue**.

Alternatively, you can create a new administrator account and then log into the console using the new account. Refer to "Adding a New Administrator Account" on page 4-2 for details about creating a new BlueView administrator account.

Obtaining Online Help

If you need assistance using the BlueView Management System, refer to the *BlueView™ Management System User Guide* included with your BlueView shipment. You can access an HTML version of this document from any administrator console page simply by clicking on the **Help** link that appears at the top of every page.

Additionally, you can click the **Site Map** link from any administrator console page to display a map of executable BlueView functions as shown in Figure 3-7.

Logging Out of the Administrator Console

After you have finished configuring the BlueView, you should log out of the administrator console.

You can log out from any administrator console page simply by clicking the **Sign Out** link that appears at the top of the page.

- [Status](#)
 - [Summary](#)
 - [Active Connections](#)
 - [RF View](#)
 - [Logs](#)
 - [Alarms](#)
 - [RF Alarms](#)
 - [Reports - Add](#)
 - [Maps - Add](#)
 - [Contained Devices](#)
- [Jobs](#)
 - [Pending - Add](#)
 - [History](#)
 - [Job Elements](#)
 - [Controller Upgrades](#)
 - [BSAP Upgrades](#)
 - [Stand Alone AP Upgrades](#)
 - [Controller Patches](#)
 - [Controller Configurations](#)
 - [Controller Templates](#)
- [Devices](#)
 - [Groups - Add - Organize](#)
 - [Controllers - Add](#)
 - [Access Points](#)
 - [AP SSIDs - Add](#)
 - [Discovery - Add](#)
- [Stand Alone APs](#)
 - [AP Templates - Add](#)
 - [Access Points - Add](#)
 - [SSIDs - Add](#)
 - [Radius Servers - Add](#)
- [RF Sensor](#)
 - [Stations - Add](#)
 - [Approved SSIDs - Add](#)
 - [Manufacturer-MAC - Add](#)
 - [Hotspot-SSID - Add](#)
 - [Alarms](#)
 - [RF Containment](#)
 - [Bulk Import](#)
 - [Bulk Export](#)
 - [RF Power Management](#)
- [BlueView](#)
 - [Setup](#)
 - [Administrative Users - Add](#)
 - [Network](#)
 - [Routes](#)
 - [Time](#)
 - [Logging and Storage](#)
 - [SNMP Agent & Remote Diagnostics](#)
 - [Email](#)
 - [Notifications](#)
 - [GUI](#)
 - [Restart Services](#)
 - [Configuration Backup/Restore](#)
 - [Upgrade](#)
 - [Patch](#)
 - [Switch](#)
 - [Diagnostics](#)
 - [Traffic Capture](#)

Figure 3-7: Displaying the BlueView Function Map

Discovering WLAN Devices on Your Network

There are two ways to make the Bluesocket devices and stand alone access points on your network available for management by BlueView:

- Creating and Running BSC Discovery Jobs
- Manually Adding BSCs for Management by BlueView

Creating and Running BSC Discovery Jobs

Create and then run a BlueView discovery job to discover the BlueSecure Controllers on your network and make them available for management by BlueView.

BlueView does not discover BlueSecure Access Points directly. Instead, these devices are discovered and become manageable by BlueView when managed BlueSecure Controllers are polled.

Creating a Discovery Job

Follow these steps to create a BlueView discovery job:

1. On your initial login, click **Auto-Discovery** from the Getting Started page (as shown in Figure 3-4).

On subsequent logins, click **Devices/Discovery** from any Administrator Console page, and then click at the top of the page.

The Create New Discovery Configuration page appears (see Figure 3-8).

2. Enter a meaningful name for the discovery job in the **Name** field.
3. Select the default group into which to place the discovered BlueSecure Controllers from the **Default Group** drop-down menu.

The first time you run the discovery job the only group available for selection will be the Default group.

4. Specify the range of IP addresses on which BlueView is to search for BSCs.

Mark the **Range** radio button and enter the starting and ending addresses across which BlueView is to search.



Note: The starting IP address must be less than the ending IP address. The Starting and Ending Addresses must have the same first octet.

Alternatively, mark the **Network** radio button, and enter a valid network IP address along with a netmask to delimit the address search on that network.

5. Specify the Simple Network Management Protocol version BlueView is to use when querying discovered BlueSecure Controllers.



Note: Although BlueView supports both SNMP v2c and V3, we recommend that you configure BlueView to communicate with BSCs using SNMP V3 and the Bluesocket API, as a greater number of BSC maintenance and provisioning jobs are supported with SNMP v3.

Mark the **V2c** radio button and enter a community string to communicate with the BlueSecure Controllers using SNMP version 2c.

Alternatively, mark the **V3** radio button and enter a **Username** and **Password** to communicate with the BlueSecure Controllers using SNMP version 3 and the Bluesocket API.

6. Mark the **Set the controller's syslog server to the BVMS?** checkbox to configure the BSC to send its event data to BlueView to be logged.
7. Mark the **Add the BVMS as an SNMP Trap Management Station?** checkbox to configure the BSC to send its SNMP trap data to BlueView.
8. Specify the BVMS network interface on which the BSC is to communicate with BlueView by selecting Ethernet 1 or Ethernet 2 from the **Addressable Interface** drop-down menu.
9. Optional. Mark the **Do AP discovery?** checkbox to discover stand alone APs on your network as part of this discovery job.

If you enable stand alone AP discovery, then you must complete the following steps.

- a) Select the SNMP version that BlueView will use to communicate with the stand alone APs from the **SNMP Version** drop-down menu.
- b) Define the SNMP v2 passwords that will enable BlueView to access and manage discovered APs via SNMP.

Create new Discovery Configuration

Back
Reset
Save
Save and create another
Discover/Save

Name
Name

Group
Default Group
Default group to place discovered devices.

Address Range
 Range Network
 Starting Address Ending Address
Starting and ending IP range.
Starting and ending Addresses must have the same first octet.
Example: 192.168.1.1 - 192.169.1.1 is acceptable
Example: 192.168.1.1 - 193.169.1.1 is not acceptable.

Access Settings
 SNMP Version
 V2c
SNMPv3/API are needed to run jobs.
 Community String
 V3
 SNMPv3/API Username Password Confirm password
 Set the controllers syslog server to the BVMS?
 Add the BVMS as a SNMP Trap Management Station?
 Addressable Interface

Discover Stand Alone Access Points
 Do AP discovery?
 SNMP Version
 Read-only Community String (required)
 Read-write Community String
Needed to update AP settings
 Telnet User
Needed to update Cisco APs running IOS
 Telnet Password
 Telnet Enable Password

Notes

Back
Reset
Save
Save and create another
Discover/Save

Figure 3-8: Create New Discovery Configuration Page

Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-only Community String** field, and then re-enter the password in the **Confirm** field.





- Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-Write Community String** field, and then re-enter the password in the **Confirm** field.
- c) Define the authentication information required for telnet access to the AP. Telnet access to the AP is required to update the firmware on Cisco IOS model APs. Enter the telnet session username in the **Telnet User** field.
Enter the telnet session password in the **Telnet Password** field.
Enter the telnet session enable mode password in the **Telnet Enable Password** field.
10. Optional. Enter meaningful information about the device discovery job in the **Notes** field.
 11. Click **Save** to store the configured discovery job in the BlueView database.
Clicking **Save and create another** stores the discovery job configuration and enables you to create another.
Clicking **Discover/Save** stores the configured discovery job and runs it immediately.



Running a Discovery Job

To run a discovery job, click **Devices/Discovery** from any Administrator Console page. A table listing all defined device discovery jobs appears

Actions	Name	Group	Start Address	End Address	SNMP	Status	un-sort	customize
<input type="checkbox"/>	Initial Discovery	1	192.168.168.1	192.168.171.254	V3			
Check All Clear All								<input type="button" value="Delete"/>
1 row								

Figure 3-9: Defined Discovery Job

Click the  icon to run the discovery job. Use the  icon to edit the job, the  icon to delete the job, and the  icon to schedule the job.

As the discovery job runs, its percentage complete is reported in the Status field and the binoculars icon changes to  indicating that the job is in progress and will be stopped if you click on the  icon.

Upon completion of the job, its status field is blank.

Click **Devices/Controllers** to see a list of the BlueSecure Controllers BlueView.





Actions	Status	Name	Address	Group	SNMP	un-sort	customize
<input type="checkbox"/>	All	All	All	All	All		un-filter
<input type="checkbox"/>		192.168.100.143	192.168.100.143	Default	V3		
<input type="checkbox"/>		192.168.100.142	192.168.100.142	Default	V3		
<input type="checkbox"/>		wlan.eng.bluesocket.com	wlan.eng.bluesocket.com	Default	V3		
<input type="checkbox"/>		192.168.100.135	192.168.100.135	Default	V3		
Check All Clear All						<input type="button" value="Delete"/>	
4 rows download							

Figure 3-10: BlueSecure Controllers List

The discovered BlueSecure Controllers now are in the default group; regroup as described in “Organizing Your Bluesocket Devices into Groups” on page 3-15.

After you have discovered BlueSecure Controllers or manually added BlueSecure Controllers to the BlueView managed device list, any BlueSecure Access Points (BSAPs) or stand alone Access Points (APs) connected to the BSCs under BlueView management will be listed in the navigation pane of any BlueView status window. Additionally, all BSAP configurations stored on BSCs under BlueView management will be listed on the **Devices/Access Points** page.

Click **Devices/Access Points** from any BlueView administrator console page to see the BSAP configurations stored on BSCs managed by BlueView.

Actions	In Sync	Status	MAC	Enabled	Name	Home Controller	un-sort	customize
<input type="checkbox"/>	All	All	All	All	All	All	un-filter	
<input type="checkbox"/>	Yes		00:12:cf:09:fd:e6	Yes		192.168.102.230		
<input type="checkbox"/>	Yes		00:12:cf:14:b4:d8	Yes		192.168.102.230		
<input type="checkbox"/>	Yes		00:12:cf:09:fd:cb	Yes		No Home Controller		
<input type="checkbox"/>	Yes		00:12:cf:11:22:33	Yes	mimo-12	No Home Controller		
<input type="checkbox"/>	Yes		00:12:cf:07:d4:85	Yes	ap3	No Home Controller		

[Check All](#) | [Clear All](#) | [Assign template...](#) | [Apply](#) | [Enable](#) | [Disable](#) | [Delete](#) | [Reboot](#) | [Calibrate Dynamic RF](#)

5 rows [download](#)

Figure 3-11: Listing BSAPs

See “Managing BSAP Configurations” on page 7-26 for information about displaying, editing, and deleting BSAP configurations.

Additionally, any SSIDs stored on the BSCs under BlueView management will be listed on the **Devices/AP SSIDs** page.

Click **Devices/AP SSIDs** from any BlueView administrator console page to see a list of SSIDs configured on BSCs under management by BlueView.

Actions	In Sync	Enabled	SSID	VLAN	Home Controller	un-sort	customize
<input type="checkbox"/>							
<input type="checkbox"/>	Yes	Yes	Default	0	192.168.100.135		
<input type="checkbox"/>	Yes	Yes	mySSID66	66	192.168.100.144		
<input type="checkbox"/>	Yes	Yes	JMnet	0	192.168.100.29		
<input type="checkbox"/>	Yes	Yes	jby	0	192.168.100.144		

[Check All](#) | [Clear All](#) | [Apply](#) | [Enable](#) | [Disable](#) | [Delete](#)

4 rows

Figure 3-12: Listing BSAP SSIDs

See “Managing BSAP SSIDs” on page 7-37 for information about displaying, editing, adding, and deleting BSAP SSIDs.

Stand Alone APs connected to the BSCs discovered on your network will be listed on the **Stand Alone APs/Access Points** page.

Actions	In Sync	Status	MAC	Template	Hostname	Location	Home Controller
<input type="checkbox"/>	All	All	All	All	All	All	All
<input type="checkbox"/>	Yes		00:0e:d7:94:c2:60		jby-Cisco1100.bluesocket.com	Burlington	192.168.100.143
<input type="checkbox"/>	Yes		00:20:a6:58:d3:c8		JCSWIRELESS	Selma Middle	No Home Controller
<input type="checkbox"/>	Yes		00:20:a6:5e:43:8c		ORINOCO-AP-4000-5e-43-8c	here	No Home Controller
<input type="checkbox"/>	Yes		00:15:c7:80:07:40		ap1242		192.168.100.143
<input type="checkbox"/>	Yes				3Com Access Point	here	No Home Controller

5 rows [download](#)

Figure 3-13: Listing Stand Alone APs

See Chapter 5 for complete information about manually adding and fully configuring stand alone APs for management by BlueView.

Manually Adding BSCs for Management by BlueView

In addition to running a discovery job, you can make BlueSecure Controllers on your network available for management by BlueView by manually adding specific BSCs to BlueView’s managed device list.

To manually add a controller to BlueView’s managed device list:

1. Click **Devices/Controllers** from any Administrator Console page, and then click . The Create New Controller page appears (see Figure 3-8).
2. Enter a meaningful name identifying the BlueSecure Controller in the **Display Name** field.

Leave the **Display Name** field blank to use the hostname associated with the controller’s IP address for identification purposes.

3. Enter the controller’s IP address in the **IP Address** field.
4. Mark the **Ignore "Managed Interface Down" warnings from this BSC** checkbox if all BSAPs are connected to the BSC's protected interface.
5. Select the default group into which to place the BlueSecure Controller from the **Default Group** drop-down menu.

Until you create your own device groups, the only group available for selection will be the Default group.

6. Specify the SNMP (Simple Network Management Protocol) version BlueView is to use when querying the BlueSecure Controller.



Note: Although the BSC supports both SNMP v2c and V3, we recommend that you configure the BSC to communicate with BlueView using SNMP V3, as a greater number of BSC maintenance and provisioning jobs are supported with SNMP v3.

Mark the **V2c** radio button and enter a community string to communicate with the BlueSecure Controller using SNMP version 2c.

Alternatively, mark the **V3** radio button and enter a Username and Password to communicate with the BlueSecure Controller using SNMP version 3.

7. The **API Port** must match the **Admin web server port** on the BSC’s HTTP Settings page. Specify **API Port** to block admin access at the interface level. The default port is 443. If the value is different than 443, the web server will listen on the new port and deny

access via port 443 to the admin entry points. For example, if you specify port 8083, admin access is available at <https://IP:8083/admin.pl>.

8. Mark the **Set the controller's syslog server to the BVMS?** checkbox to configure the BSC to send its event data to BlueView to be logged.
9. Mark the **Add the BVMS as an SNMP Trap Management Station?** checkbox to configure the BSC to send its SNMP trap data to BlueView.

Create new Controller

Back Reset Save Save and create another

Name
Display Name
IP Address
Leave blank to use the hostname of the below address.
 Ignore "Managed Interface Down" warnings from this BSC
Select this option if all BSAPs are connected to the BSC's protected interface.

Group
Device Group
Default
Container to manage this device.

Access Settings
SNMP Version
 v2c
SNMPv3/API are needed to run jobs.
Community String
public
 v3
SNMPv3/API Username Password Confirm password
API Port
443
Port 443 is recommended.

Set the controllers syslog server to the BVMS?
 Add the BVMS as a SNMP Trap Management Station?
Addressable Interface
Ethernet 1

Secure Mobility Matrix
 Opt out of group's Secure Mobility Matrix?

RF Power Management
 Enable Dynamic RF Power Management?

Bandwidth Limit
Bandwith Limit for uploading firmware, patches, etc. in kbps
Unlimited 0
Rate for uploading data in kbps, 0 is for unlimited

Notes

Back Reset Save Save and create another

Figure 3-14: Create New Controller Page

10. Define the IP address configured for the primary or secondary BVMS network interface as the BSC's syslog server/SNMP trap management station address by selecting Ethernet 1 or Ethernet 2 from the **Addressable Interface** drop-down menu.

11. Optional. Enter meaningful information about the BlueSecure Controller in the **Notes** field.
12. Optional. Mark the **Opt out of group's Secure Mobility Matrix** checkbox to prevent this BSC from being added to the Secure Mobility Matrix associated with the group to which this BSC is added.
13. Optional. Define a bandwidth limit (in kbps) for the BSC when it uploads files to BlueView by selecting a value from the **Bandwidth Limit** drop-down menu. By default, there is no bandwidth limit on the BSC when it uploads files to BlueView.
14. Click **Save** to add the specified Controller to BlueView's managed device list or **Save and Create Another** to add the specified controller to BlueView's managed device list and then identify another controller for management by BlueView.
The added controller is listed on the Devices/Controllers page (see Figure 3-10).
You should now organize your discovered/added controllers into logical groups as described in "Organizing Your Bluesocket Devices into Groups" on page 3-15.

Organizing Your Bluesocket Devices into Groups


After BlueView has discovered the BlueSecure devices on your network or you have manually added devices to BlueView's managed device list, you should organize these devices into logical groups that have meaning for your network.

BlueView supports creation of two types of groups, static device groups and dynamic virtual groups. Both static and dynamic groups can be referenced when defining provisioning and maintenance jobs, or status reports.

Creating Static Groups

Static device groups are logical groupings of the BlueSecure Controllers on your network. Generally, you will group Bluesocket devices together in a static group by geographical location, network location, function, etc. BSCs and Centralized Sensors in a static group are identified by their IP address.

You can create hierarchies of static groups by creating groups within groups.

 **Note:** You can reassign a controller or sensor from one group to another, but a controller or sensor can reside only in a single static device group.

To create a static device group:

1. Click **Devices/Groups**, and then click .

The Create New Device Group page appears as shown in Figure 3-17.

Create new Device Group

Back Reset Save Save and create another

Settings

Name

Parent Group Default

Group Type
 Static Dynamic

Polling Intervals

Connectivity Rate
1
In minutes. Determines device connection status (0 = off).

Status Rate
10
In minutes. Determines device uptime, network status, etc. (0 = off)

Configuration Rate
6
In hours. Determines device modal, version, patches, etc. (0 = off)

Active Connection Rate
0
In minutes. Determines active connections (0 = off).

Devices

Controllers:

Available Items	Selected Items
<div style="border: 1px solid #ccc; padding: 2px; min-height: 100px;"> 192.168.100.135 192.168.100.142 192.168.100.143 wlan.eng.bluesocket.com </div>	<div style="border: 1px solid #ccc; padding: 2px; min-height: 100px;"> (Empty) </div>

Add highlighted Items Remove highlighted Items
Add all Items in list Remove all Items in list

Removing a device will place it in the Default group.

Centralized Sensors:

Available Items	Selected Items
<div style="border: 1px solid #ccc; padding: 2px; min-height: 100px;"> 192.168.100.249 </div>	<div style="border: 1px solid #ccc; padding: 2px; min-height: 100px;"> (Empty) </div>

Add highlighted Items Remove highlighted Items
Add all Items in list Remove all Items in list

Removing a sensor will place it in the Default group.

Secure Mobility Matrix

Join parent group's Secure Mobility Matrix?

Join controllers in a Secure Mobility Matrix?

Node list sync time
6
In hours. Gaurantees nodes are in sync. Select 0 to stop BVMS from adjusting the controllers settings.

Default 3rd Party Access Point Credentials

Read-only Community String (required)

Read-write Community String

Needed to update AP settings
 Telnet User

Needed to update Cisco APs running IOS
 Telnet Password

Telnet Enable Password

Figure 3-15: Create New Device Group Page - Static Groups

2. Enter a meaningful name for the device group in the **Name** field.
3. Select the existing static group within which to create this new static group from the **Parent Group** drop-down menu.

You can create hierarchies of static groups by nesting groups within groups.
4. Mark the **Static** radio button.
5. Select the rate in seconds at which BlueView is to poll the devices in the group for connectivity status from the **Connectivity Rate** drop-down menu.

The default setting is 1 minute. A setting of 0 disables BlueView from polling for this information.
6. Select the rate in minutes at which BlueView is to poll the devices in the group for uptime and network status from the **Status Rate** drop-down menu.

The default setting is 10 minutes. A setting of 0 disables BlueView from polling for this information.
7. Select the rate in hours at which BlueView is to poll the devices in the group for model number, software version, and software patch status from the **Configuration Rate** drop-down menu.

The default setting is 0—BlueView does not poll for this information.
8. Select the rate in minutes at which BlueView is to poll the devices in the group for active connection status from the **Active Connection Rate** drop-down menu.

The default setting is 2 minutes. A setting of 0 disables BlueView from polling for this information.
9. Select one or more controllers from the **Available Items** list to include in the device group, and then click **add Highlighted Items**.

The selected controllers are added to the **Selected Items** list.

To add all available controllers to the group, simply click **Add all items in list**.

Click **Remove highlighted items** or **Remove all items in list** to remove controllers from the group. Removed devices are placed in the Default group.
10. Define the group's Secure Mobility Matrix settings.

Optional. Mark the **Join parent group's Secure Mobility Matrix?** checkbox to add all group BSCs to the Secure Mobility Matrix defined for the parent group.

If you unmark the **Join parent group's Secure Mobility Matrix?** checkbox, the **Join controllers in a Secure Mobility Matrix** checkbox appears. Mark this checkbox to create a Secure Mobility Matrix for all BSCs in the group.

Enter a text string in the **Secure Mobility mesh key** field. The mesh key is a common shared password that you provide for all BSCs participating in the Secure Mobility setup. The BSCs exchange the key when communicating with each other, thus providing an extra layer of security. The key can be any text string you choose.

Define the frequency (in hours) at which BlueView is to synchronize the Secure Mobility Matrix node list on all BSCs in the group, by selecting a value from the **Node list sync time** drop-down menu. Select 0 to prevent BlueView from adjusting BSC Secure Mobility Matrix settings.

If you wish to add any stand alone access points as members of the group that are connected to BSCs in the group, then you must complete the following steps to define the default access credentials.

 - a) Define the SNMP v2 passwords that will enable BlueView to access and manage discovered APs via SNMP.

Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-only Community String** field, and then re-enter the password in the **Confirm** field.

Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-Write Community String** field, and then re-enter the password in the **Confirm** field.

- b) Define the authentication information required for telnet access to the AP. Telnet access to the AP is required to update the firmware on Cisco IOS model APs. Enter the telnet session username in the **Telnet User** field.
Enter the telnet session password in the **Telnet Password** field.
Enter the telnet session enable mode password in the **Telnet Enable Password** field.

- 11. Optional. Enter a meaningful description of the static device group in the **Notes** field.
- 12. Click **Save** to store the group information to the BlueView database or **Save and create another** to continue defining controller groups.

After you have discovered the BlueSecure Controllers on your network and organized these devices into logical groupings, you should set up BlueView for use on your network as described in the next chapter.

Visually Organizing Bluesocket Devices within Static Groups

You can visually organize the composition of existing static groups by dragging and dropping Bluesocket device icons in the BlueView administrator console.

To visually organize the devices on your network within existing static device groups:

- 1. Click **Devices/Groups**, and then click .

The Device Organization page appears as shown in Figure 3-17.

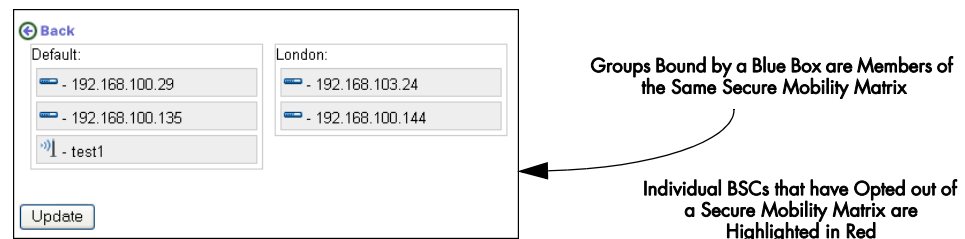


Figure 3-16: Visually Organizing Devices within Static Groups

- 2. Drag and drop the device icons between the displayed static groups until the group composition you desire is achieved.
- 3. Click to update the BlueView database with the modified static group memberships.
- 4. Click to return to the Device Groups page.
The new static group composition is reflected in the displayed group list.

Creating Dynamic Groups

Dynamic groups are virtual groups that do not contain devices but instead contain device properties in which you are interested, e.g., model number, firmware version, CPU

usage, etc. Create dynamic groups when you wish to target a particular segment of your network devices to receive the action of a provisioning or maintenance job, or when you wish to track the segment's behavior in a status report.

To create a dynamic group:

1. Click **Devices/Groups**, and click **Add** and then mark the Dynamic radio button. The Create New Device Group page looks as shown in Figure 3-17.

Figure 3-17: Create New Device Groups Page - Dynamic

2. Enter a meaningful name for the dynamic group in the **Name** field.
3. Define the properties of the devices on your network that you wish to receive the action of a provisioning or maintenance job, or that you wish to track in a status report by following these steps:
 - a) Select the device property, e.g., model number, you wish to track from the **Property** drop-down menu.
 - b) Select the boolean operator to use to relate the selected property to its specified value from the **Operator** drop-down menu.
 - c) Select the device property's value from the **Value Options** drop-down menu. The selected value is used to fill the **Value** field.
 - d) Repeat steps a to c until you have defined all properties you wish to associate with the dynamic group.
4. Optional. Enter a meaningful description of the dynamic virtual group in the **Notes** field.
5. Click **Save** to store the group information to the BlueView database or **Save and create another** to continue defining controller groups.

After you have discovered the BlueSecure Controllers on your network and organized these devices into logical groupings, you should set up BlueView for use on your network as described in the next chapter.

4)))

Configuring BlueView

BlueView provides several settings that enable you to optimize BlueView for your network. This chapter provides procedures for configuring BlueView for your network and includes:

- Managing Administrator User Accounts
- Configuring the BlueView Network Interfaces
- Adding Static Routes
- Configuring BlueView's Time and Date Settings
- Configuring the Log and Alarm Database
- Configuring the BlueView SNMP Agent and Remote Diagnostics
- Specifying the BlueView Email Server

Managing Administrator User Accounts

BlueView enables you to manage administrator accounts by:

- Adding a New Administrator Account
- Changing an Administrator Password
- Deleting Administrator Accounts
- Defining Administrator Authentication Servers

Adding a New Administrator Account

In addition to the default administrator account, admin, you can define additional administrator accounts, each with their own login, password, and specified event notifications. These administrator accounts are stored in the BlueView database.

To add a new administrator account:


1. Click **BlueView/Setup** from any administrator console page, and then click **Administrative Users** in the navigation pane.
The Administrative Users page appears.
2. Click .
- The Create New Administrative User page appears (see Figure 4-1).
3. Mark the **Enable user** checkbox to enable this administrator.
4. Enter the administrator's login name in the **Name** field.
5. Enter the administrator's password in the **New password** field, and then re-enter it in the **Confirm new password** field.
6. Optional. Mark the **Force password change next login?** checkbox to force the Administrator to change his or her password on the next login.
7. Optional. Mark the **Restrict admin from changing their password on the login screen?** checkbox to disable the Change password? link for this administrator on the BlueView login screen.
8. Optional. To limit the administrator's access to a single device group (and all of its child groups), select a device group from the **Restrict Admin to specified group** drop-down menu.
The administrator will only be able to see and manage devices in the selected group from BlueView.
9. Specify what level of write access the administrator is to receive by marking the appropriate radio button:
 - **Full** - The administrator has full write access to all data.
 - **Intermediate** - The administrator has write access to only the checked data items.
 - **Read only** - The administrator can read but not modify any data.
10. Optional. Mark the **Allow admin to access using SNMP** checkbox to enable this administrator to access BlueView via SNMP V3 (typically via another network management package).
If you enable this option, then you must enable and run an SNMP agent on BlueView as described in "Configuring the BlueView SNMP Agent and Remote Diagnostics" on page 4-13.

Figure 4-1: Create New Administrative User Page

11. Optional. Enter a meaningful description of the administrator and their assigned write access to functions in the **Notes** field.
12. Click **Save** to save the administrator information to the BlueView database, or click **Save and Create Another** to continue adding administrator accounts.

Changing an Administrator Password


To change the password for an administrator account:

1. Click **BlueView/Setup** from any administrator console page, and then click **Administrative Users** in the navigation pane.
The administrative users page appears.
2. Click the  icon corresponding to the administrator whose password you wish to change.
3. The Add/Edit Administrative User page appears (see Figure 4-1).

4. Enter the administrator's new password and password confirmation in the fields provided.
5. Click **Save** to store the modified administrator information to the BlueView database.

Deleting Administrator Accounts

To delete a BlueView administrator account:

1. Click **BlueView/Setup** from any administrator console page, and then click **Administrative Users** in the navigation pane.
The administrative users page appears.
2. Click the  icon corresponding to the administrator whose account you wish to delete.

Defining Administrator Authentication Servers

In addition to defining administrator accounts in the BlueView database, you can define external LDAP or RADIUS authentication servers against which BlueView will authenticate administrators who attempt to log into the system.

Separate procedures for configuring LDAP and RADIUS authentication servers are given in this section.

Defining an LDAP Server

LDAP uses a database schema to store user information and authentication credentials. The database uses a hierarchical tree structure with a root at the base of the tree and branches as the top of the tree.

Objects in the tree are classified based upon the LDAP schema.

dc= domain container or domain controller
cn= common name
ou=organizational unit

The base entry specifies the level of the tree where BlueView starts to look at the database. The base entry field value should specify a level low enough in the tree to allow the BlueView to search for all the user credentials at or above the level of the base entry.

The unique ID attribute field specifies the unique identifier that is used to distinguish each user record in the LDAP database. `userid` is a common unique identifier that is use by many LDAP servers. The Microsoft Active Directory Server LDAP implementation uses `sAMAccountName` as the unique identifier.

BlueView must bind to the LDAP server to look up the user in the LDAP database. BlueView can use anonymous binding when it is supported by the LDAP server. The LDAP user is used to bind to LDAP servers that do not support anonymous binding. The LDAP user field must contain the distinguished name of the LDAP user. An LDAP distinguished name is equivalent to a DNS fully qualified domain name or a disk operating system explicit directory path. The Microsoft Active Directory Server LDAP implementation does not support anonymous binding.

Administrator accounts are automatically assigned based upon the attributes configured on the LDAP server. The dynamic account assignment logic operates on a first match basis. If there is no match, the administrator will be assigned to the default account. The default account can also be used when dynamic account assignment is not configured.

To define an LDAP authentication server against which to authenticate BlueView administrators:

1. Click **BlueView/Setup** from any administrator console page, and then click **External Administrative Users, LDAP/RADIUS** in the navigation pane.
2. Mark the **Enable LDAP** radio button.
The External Administrative Users page expands to display the external LDAP authentication server settings (see Figure 4-2).

Figure 4-2: Defining an External LDAP Authentication Server

3. Enter the server's IP address or fully qualified domain name in the **Server address** field.
4. Enter the server's port number in the **Port** field.
5. Configure the following LDAP parameters:
 - **Base entry** - Enter the base name entry, for example, cn=Users,dc=acme,dc=com. This entry serves as the starting point for the search in the server database.
 - **Unique ID attribute** - Enter a unique attribute to search for in the server database, for example uid.

- **LDAP user** and **LDAP password** - Enter the LDAP/active directory account identifiers in the **LDAP user** and **LDAP password** fields. Re-enter the password in the **Confirm LDAP password** field.
 - **LDAP Filters** - Optional. Enter LDAP Filters to apply to entries within the specified scope of the search, e.g., objectClass=Person. You can use a filter on any property of an object. All entered filters are case sensitive and must follow the syntax specified in RFC1960.
6. Specify what user credentials to base the LDAP search upon.
Mark the **User Login Information** radio button to search the LDAP/Active Directory server for the user using the information entered when the user logs in. This is the default setting.
Alternatively, mark the **LDAP User** radio button to search the LDAP/Active Directory server for the user using the information you have defined on this page.
 7. Define the rules to determine if the user is authenticated. For each rule:
 - a) Enter the appropriate LDAP attribute in the **Attribute** field.
 - b) Select the appropriate logic operator (equal to, not equal to, starts with, ends with, greater than, less than, or contains) from the **Logic** drop-down list.
 - c) Enter the appropriate value to check against the specified attribute in the **Value** field.
 - d) Select the administrator account to assign to the user if the rule evaluates as true and the user is authenticated from the **then Administrator is** drop-down list.
 8. Optional. Use the commands included in the **Row Management** drop-down list to change the order of rules, add new blank rules, clear rule data, or delete a rule, etc. Remember, BlueView evaluates rules in the order in which they are listed here on the External Administrative Users server page.
 9. Select the default administrator account from the **Default Administrator** drop-down list. The selected default account is the account BlueView assigns the administrator if none of the rules is true.
 10. Optional. Enter a meaningful description for the external LDAP/active directory authentication server in the **Notes** field.
 11. Click **Save** to store the LDAP authentication server information to the BlueView database.

Defining a RADIUS Server

The BlueView Management System must be configured on the RADIUS server as a network access server (NAS) with a shared secret before the RADIUS server will communicate with the BlueView. RADIUS authentication can use the IANA assigned port of 1812 or the well known port of 1645.

Administrator accounts are automatically assigned based upon the attributes configured on the RADIUS server. The dynamic account assignment logic operates on a first match basis. If there is no match, the administrator will be assigned to the default account. The default account can also be used when dynamic account assignment is not configured.

To define a RADIUS authentication server against which to authenticate BlueView administrators:

1. Click **BlueView/Setup** from any administrator console page, and then click **External Administrative Users, LDAP/RADIUS** in the navigation pane.
2. Mark the **Enable RADIUS** radio button.

The External Administrative Users page expands to display the external RADIUS authentication server settings (see Figure 4-3).

External Administrative Users

Disable LDAP/RADIUS
 Enable LDAP
 Enable RADIUS

Radius Settings

Server Address Port

The IP address or DNS Name of the server

Password/Shared Secret Confirm Password/Shared Secret

Timeout

Timeout in seconds for RADIUS Server Response.

NAS Identifier

NAS Identifier

Name of the NAS Identifier attribute for RADIUS.

Mapping LDAP/Active Directory fields

When a user successfully authenticates against the server the following rules are checked in numerical order. If a rule matches then the user is assigned that administrative user, and no further rule is checked. If no rules match, the user is assigned the default administrative user.

if	Attribute	logic	Value	then Administrator is	Row Management...
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Default Administrator

Notes

Figure 4-3: Defining an External RADIUS Authentication Server

3. Enter the server's port number in the **Port** field.
4. Enter the known secret shared between the BSC and the RADIUS authentication server in the **Shared secret** field, and then confirm the shared secret by entering it in the **Confirm shared secret** field.
5. Enter the number of seconds by which the RADIUS server must respond to BlueView's query before the request times out in the **Timeout** field. You must enter a value greater than zero in this field.
6. Optional. Enter a Network Access Server identifier string used to access the RADIUS server in the **NAS Identifier** field. The default string is Hostname.
7. Define the rules to determine if the administrative user is authenticated. For each rule:
 - a) Enter the appropriate LDAP attribute in the **Attribute** field.
 - b) Select the appropriate logic operator (equal to, not equal to, starts with, ends with, greater than, less than, or contains) from the **Logic** drop-down list.
 - c) Enter the appropriate value to check against the specified attribute in the **Value** field.

- d) Select the administrator account to assign to the user if the rule evaluates as true and the user is authenticated from the **then Administrator is** drop-down list.
8. Optional. Use the commands included in the **Row Management** drop-down list to change the order of rules, add new blank rules, clear rule data, or delete a rule, etc. Remember, BlueView evaluates rules in the order in which they are listed here on the External Administrative Users server page.
9. Select the default administrator account from the **Default Administrator** drop-down list. The selected default account is the account BlueView assigns the administrator if none of rules is true.
10. Optional. Enter a meaningful description for the external RADIUS authentication server in the **Notes** field.
11. Click **Save** to store the RADIUS authentication server information to the BlueView database.
12. Enter the server's IP address or fully qualified domain name in the **Server address** field.

Configuring the BlueView Network Interfaces

You must configure BlueView to communicate with the BSCs on your network by configuring its network interfaces appropriately for your network.

1. Click **BlueView/Setup** from any administrator console page, and then click **Network** in the navigation pane.
The Network Interface page appears as shown in Figure 4-4.
The current settings for the BlueView network interfaces are listed in the status panes on the right side of the page.
2. Select the primary BlueView network interface, Ethernet 1, from the **Network Interface** drop-down menu.
3. Clear the **Obtain IP settings from a DHCP server for the interface** checkbox if you are assigning IP settings manually.



Note: Even if you are using dynamic host configuration protocol (DHCP) to dynamically assign IP settings, we recommend that you clear the **Obtain IP settings from a DHCP server for the interface** checkbox and enter default IP settings for the interface. These defaults will become the fallback settings for the interface if DHCP should fail for any reason.

Enter the appropriate network interface information for the following fields:

You may simply click to populate the following fields with the values currently displayed in the status panes.

Network Interface

Back Reset Save

Network Interface
Ethernet 1

Obtain IP settings from a DHCP server for the interface?

Fill Up

Fill with the current values

IP Address
192.168.100.131

Netmask
255.255.252.0

Gateway
192.168.100.1

Primary DNS
192.168.100.1

Secondary DNS

Default Domain
bluesocket.com

Hostname
blueview

Port settings

Interface speed
 Auto 10 100 Max

Duplex
 Auto Half Full

Back Reset Save

MAC Address	00:0E:0C:33:0A:D2
Link Up	true
DHCP Type	Fixed IP
IP Address	192.168.100.131
Netmask	255.255.252.0
Broadcast	192.168.103.255
Bytes Out	414667030
Bytes In	1107343348
Duplex	Full
Speed	100Mb/s

Default Gateway	192.168.100.1
Primary DNS	192.168.100.1
Secondary DNS	

Figure 4-4: Network Interface Page

- **IP Address** - Enter the IP address of the BlueView network interface in four-byte dotted-decimal format.
 - **Netmask** - Enter a subnet mask specifying which bits in the IP address correspond to the network address and which bits correspond to the subnet portion of the address.
 - **Gateway** - Enter the IP address of the host serving as the BlueView network interface's IP gateway.
 - **Primary DNS** - Enter the IP address of the primary domain name system (DNS) server.
 - **Secondary DNS** - Optional. Enter the IP address of the secondary domain name system (DNS) server.
 - **Default Domain** - Optional. Enter the domain name to append to a hostname when its domain is not specified. For example, if the hostname myhost is received, and the default domain is widgetsrus.com, then the fully qualified domain name becomes myhost.widgetsrus.com.
 - **Hostname** - Optional. Enter the hostname for BlueView. Leaving the Hostname blank means that a hostname is not sent to the Dynamic DNS service.
4. Optional. Mark the **Obtain IP settings from a DHCP server for the interface** checkbox if you are using a DHCP server to dynamically assign IP settings.

Enter the appropriate DHCP server settings for BlueView in the following fields:

- **DHCP timeout** - Maximum time in seconds between a client request and the client acknowledgement of a response to that request from the DHCP server.
- **Hostname** - Optional. Enter the hostname for BlueView. Leaving the Hostname blank means that a hostname is not sent to the Dynamic DNS service.

5. Define the Port Settings for the network interface:
By default, BlueView's network interfaces automatically negotiate bit rate and duplex type for connections. However, if required, you can specify **Interface Speed** and **Duplex** type here. Max indicates the highest speed supported by the interface (1Gbps).
6. Click **Save** to save the network interface settings to the BlueView database.
7. Optional. If you are also using BlueView's secondary network interface to connect to your Bluesocket network, select Ethernet 2, from the **Network Interface** drop-down menu, and then repeat steps 3 to 6.

Adding Static Routes

BlueView automatically builds and maintains its own internal routing table to keep track of addresses and interfaces used to reach BSC destinations.

To display BlueView's internal routing table, click **BlueView/Setup** from any administrator console page, and then click **Routes** in the navigation pane.

Actions	Name	Destination	Gateway	Netmask	Interface	un-sort customize
<input type="checkbox"/>	System Route	192.168.168.0	0.0.0.0	255.255.252.0	i1	
	System Route	169.254.0.0	0.0.0.0	255.255.0.0	i1	
	System Route	0.0.0.0	192.168.168.240	0.0.0.0	i1	
Check All Clear All						<input type="button" value="Delete"/>
3 rows						

Figure 4-5: Sample BlueView Routing Table

Rarely, you may need to add a static route to a special network destination that is not normally included in the routing table.



Caution: This is an advanced BlueView configuration function. Do not add static routes unless you have a thorough understanding of network and routing concepts.

To add a static route to the BlueView routing table:

1. To display BlueView's internal routing table, click **BlueView/Setup** from any administrator console page, and then click **Routes** in the navigation pane.
2. Click .
The Create New Route page appears as shown in Figure 4-6.
3. Enter the IP address of the destination network in the **Route Destination** field.
4. Enter the IP address of the gateway through which traffic is routed to the destination network in the **Route Gateway** field. This gateway must be on the same subnet as the IP address of the specified **Interface**.
5. Enter a bit mask specifying which bits in the IP address correspond to the network address and which bits correspond to the subnet portion of the destination network IP address.
6. Specify the BlueView interface through which traffic is routed to the destination network.
7. Click **Save** to store the static route settings to the BlueView database.

Figure 4-6: Create New Route Page

Configuring BlueView's Time and Date Settings

To configure the BlueView system clock or to set up BlueView to use network time protocol (NTP) synchronization:

1. Click **BlueView/Setup** from any administrator console page, and then click **Time** in the navigation pane.

The BlueView Time Settings page appears as shown in Figure 4-7.

Figure 4-7: BlueView Time Settings Page


2. Configure the following BlueView time settings as appropriate:

- **System settings** - Change the current time zone, date, or time on BlueView. The date entries must be in MMDDYYYY format and the time entries in 24-hour format (HHMMSS).
To prevent manual update of the time, leave the date or time fields blank, respectively. Default values: America/New_York time zone and factory time/date setting.
 - **NTP settings** - Enter Network Time Protocol (NTP) server(s) to set the date and time on BlueView. When specifying more than one server, use a comma-delimited list of IP addresses or fully qualified domain names.
You can set the frequency of NTP synchronization to either hourly, daily, weekly, or monthly. Whenever NTP performs an update, it overrides the current BlueView time and date setting. Default value: Never (i.e., no NTP synchronization is used).
 - **Query the NTP server now?** - If this checkbox is marked and you click **Update**, the specified NTP server(s) is checked immediately and BlueView's date and time settings are updated, if necessary. This option is useful when you need to update the BlueView time settings now, rather than waiting for the selected NTP update interval.
If cleared, the BlueView time and date settings are updated at the next selected NTP update interval.
3. Click **Update** to update the BlueView system time as specified and to save the configured time settings to the BlueView database.

Configuring the Log and Alarm Database

BlueView maintains a log and alarm database in non-volatile memory that contains event records received from managed BlueSecure Controllers.

BlueView automatically manages its log and alarm database based on maximum size (MB) and entry count parameters you configure as described in this section.

 **Note:** By default, the BSCs on your network are not configured to send log messages to BlueView. Follow the procedure given in “Configuring the BSCs on Your Network to Support BlueView” on page 3-2 to configure the BSCs on your network to send their log data to BlueView. Managed BSCs will automatically send their alarms to BlueView.

To configure how BlueView stores log and alarm data received from BSCs:

1. Click **BlueView/Setup** from any administrator console page, and then click **Logging and Storage** in the navigation pane.
The BlueView Logging and Storage Settings page appears as shown in Figure 4-8.
2. Configure the following BlueView log record settings as appropriate:
 - **Maximum number of log entries to keep** - Specify the maximum number of log entries (lines) permitted in the BlueView database. Default value: 1,000,000.
 - **Number of log entries to delete when reaching maximum** - Number of event log entries to automatically delete when the number specified in Maximum number of log entries to keep is reached. Default value: 200,000.

The screenshot shows the 'Logging and Storage Settings' configuration page. It features a blue header with the title and three buttons: 'Back', 'Reset', and 'Save'. The main content area is light blue and contains three sections: 'Log Records', 'Alarm Records', and 'Storage'. Each section has input fields for numerical values and a 'Save' button at the bottom.

Section	Setting	Value
Log Records	Maximum number of log entries to keep in local database	1000000
	Number of log entries to delete when reaching maximum	200000
Alarm Records	Maximum number of alarm entries to keep in local database	100000
	Number of alarm entries to delete when reaching maximum	20000
Storage	Max number of Non-Preserved Controller Backups	0

Figure 4-8: Logging and Storage Settings Page

3. Configure the following BlueView alarm record settings as appropriate:
 - **Maximum number of alarm entries to keep** - Specify the maximum number of alarm entries (lines) permitted in the BlueView database. Default value: 1,000,000.
 - **Number of alarm entries to delete when reaching maximum** - Number of event alarm entries to automatically delete when the number specified in Maximum number of alarm entries to keep is reached. Default value: 200,000.
 - **Max number of Non-Preserved Controller Backups** - After a backup completes, delete any backups matching the IP/Hostname that are older than this number. A value of 0 means no limit.
4. Click **Save** to save the log settings to the BlueView database.

Configuring the BlueView SNMP Agent and Remote Diagnostics

You may run an SNMP agent on BlueView to enable BlueView to be managed by a network management system. The SNMP agent page also provides a setting to enable/disable remote access to the BlueView via SSHv2.

To modify the settings for the BlueView SNMP agent:

1. Click **BlueView/Setup** from any administrator console page, and then click **SNMP Agent & Remote Diagnostics** in the navigation pane.

The BlueView SNMP Settings and Remote Diagnostics page appears:

The screenshot shows a web interface for configuring SNMP settings. The title bar reads "SNMP Settings and Remote Diagnostics". At the top right are buttons for "Back", "Reset", and "Save". The main content area is divided into two sections. The first section, "SNMP Agent Settings", contains a dropdown menu for "SNMP Agent" currently set to "Off". Below this are two pairs of text input fields: "Read-Only Community String" and "Confirm", and "Read-Write Community String" and "Confirm". Further down are two more text input fields: "System Location" (with the value "unknown") and "System Contact" (with the value "unknown"). The second section, "Remote Diagnostics", contains a single checkbox labeled "Enable Remote SSH Diagnostics?". At the bottom right of the form area are another set of "Back", "Reset", and "Save" buttons.

Figure 4-9: SNMP Settings and Remote Diagnostics Page

2. Configure the following BlueView SNMP agent settings as appropriate for your network:
 - **SNMP Agent** - Start the selected version of SNMP agent (v2c, v3, or both) on the BlueView, or shut down the agent. To enable administrator access to SNMP v3, which requires a user ID and password, see "Adding a New Administrator Account" on page 4-2 of this guide.
Default value: Off (SNMP agent shut down).
 - **Read Only Community String** - Enter and confirm the SNMP v2c community string that enables a remote device to retrieve read-only SNMP information from BlueView.
 - **Read-Write Community String** - Enter and confirm the SNMP v2c community string that enables a remote device to read SNMP information from and modify SNMP settings on BlueView.
 - **System Location and System Contact** - Optional comment fields that describe physical location and contact information for BlueView.
3. Optional. Mark the **Enable Remote SSH Diagnostics** checkbox to enable Bluesocket personnel to access the BVMS via SSHv2 to perform remote diagnostics.
4. Click **Save** to save the SNMP agent settings to the BlueView database.

Specifying the BlueView Email Server

When you set up an administrator account, you can configure BlueView to send event notifications to the administrator as described on "Adding a New Administrator Account" on page 4-2.

To enable BlueView to login to your mail server securely and to email notifications, specify the email server BlueView is to use by completing the following steps:

1. Click **BlueView/Setup** from any administrator console page, and then click **Email** in the navigation pane.

The BlueView Email Settings page appears as shown in Figure 4-10.


Figure 4-10: Email Settings Page

2. Enter the host name or IP address of the Simple Mail Transfer Protocol server that BlueView is to use to send event notifications to administrators in the **SMTP Server** field.
3. **Port:** Enter the mail server port. Defaults to 25.
4. **SMTP Authentication method:** Defaults to None. Specify Login to pass the user name and password through a secure tunnel.
5. **SMTP Username:** Optionally, specify the username to authenticate with the mail server.
6. **SMTP Password:** Optionally, specify a password to authenticate with the mail server.
7. Enter the email address that is to be used to identify the sender in event notification messages sent from BlueView in the **Return Address** field. This should be a valid email address to which bounce notifications can be sent
8. Click **Save** to save the email settings to the BlueView database.

Configuring Administrator Notifications

You can configure BlueView to notify administrators that an event has occurred within the protected RF airspace that warrants their attention.

To configure administrator notifications:

1. Click **BlueView/Setup/Notifications** from any Administrator Console page.
2. Click the  icon corresponding to the administrator notification you want to edit. The **Edit Global Notification Configuration** page appears
3. Mark the **Enable** checkbox to enable this notification.
4. Enter the email address to which notifications are to be sent in the **Email To** field.
5. Enter the IP address of the SNMP trap receiver to which BlueView is to send notifications in the **Host IP Address** field.
6. Enter the community string required to gain access to the SNMP trap recover in the **Community String** field.

7. Enter the IP address of the syslog server to which BlueView is to send notifications in the **SysLog IP Address** field.
8. Specify the category of RF Alarm by marking the appropriate checkbox: **Information**, **Warning**, or **Severe**.
9. Specify what event notifications the administrator is to receive by marking the checkbox next to one or more of the following events:
 - **Connectivity Lost to AP or Controller** - connectivity from a BSC or AP to another device has been lost.
 - **Controller or AP Down** - a BSC or AP is unreachable from BlueView.
 - **Link Down on Controller** - a Bluesocket network link is down.
 - **Controller Failover** - a primary BSC has failed over to its backup BSC.
10. Click **Save** to save the notification settings to the BlueView database.

Specifying Refresh Rates

You can customize refresh rates, controlling how fast the Status page Jobs page, Device Discovery page, and BlueView Upgrade page are refreshed with the latest status data.

1. Click **BlueView/Setup** from any administrator console page, and then click **GUI** in the navigation pane.

The BlueView GUI Settings page appears as shown in Figure 4-11.
2. Configure the following refresh rates in seconds. In all cases, values must be greater than 10 seconds:
 - Refresh Rate for Status Pages
 - Refresh Rate for Jobs Pages
 - Refresh Rate for Device Discovery Page
 - Refresh Rate for BlueView Upgrade Page
3. Click **Save** to save the refresh settings to the BlueView database.

The screenshot shows a web interface titled "GUI Settings". At the top right, there are three buttons: "Back", "Reset", and "Save". Below this is a section titled "Refresh Rates". It contains four rows of configuration, each with a label, a text input field, and a small note: "The Refresh rate in seconds. Values must be greater than 10." The values entered in the input fields are 30, 15, 15, and 15 respectively. At the bottom right of the form area, there are three buttons: "Back", "Reset", and "Save".

Figure 4-11: GUI Settings Page

5

Configuring Stand Alone Access Points with BlueView

In addition to managing and monitoring Bluesocket devices on your network, you can use BlueView to manage, monitor, and update the firmware on access points manufactured by Cisco, Proxim/Avaya/Orinoco, 3COM, Netgear, Symbol, and Enterasys.

To support management of stand alone APs on your network, BlueView enables you to define the Service Set Identifiers (SSIDs) you will use on the stand alone APs as well as the RADIUS servers to which the stand alone APs will link for user authentication.

This chapter provides the procedures you should follow to configure stand alone APs for management by BlueView including:

- Overview
- Listing Stand Alone Access Points
- Editing Stand Alone Access Point Configurations
- Creating a Stand Alone AP Configuration Template
- Adding a Stand Alone AP for Management by BlueView
- Configuring Stand Alone AP SSIDs
- Configuring Stand Alone AP RADIUS Authentication Servers

Overview

In addition to managing and monitoring Bluesocket devices on your network, you can use BlueView to manage, monitor, and update the firmware on access points manufactured by Cisco, Proxim/Avaya/Orinoco, 3COM, Netgear, and Symbol.

- Cisco Aironet access points:
 - Model 350 IOS and VxWorks.
 - Model 1100
 - Model 1200/1210/1220/1230/1240 IOS and 1200/1220 VxWorks
 - Model 1300
 - Model 1400
- Proxim/Avaya/Orinoco access points:
 - Model AP-2000
 - Model AP-4000
- 3COM access points:
 - Model 8750
 - Model 8750 (Only credentials, SNMP location and contact, and radio settings may be edited)
- Netgear access points:
 - Model WG102
 - Model WG302
 - Model WAG302
- Symbol access points:
 - Model 4131
- Enterasys access points:
 - Roamabout RBT-4102

To enable a stand alone access point to be fully manageable from BlueView, you must configure:

- general AP setup information
- 802.11 b/g radio settings
- 802.11a radio settings
- credentials used to access the AP

You can also define the Service Set Identifiers (SSIDs) used on the stand alone APs as well as the RADIUS servers to which the stand alone APs will link for user authentication.

The following APs are displayed within BVMS, but their configurations cannot be edited.

- Cisco:
 - Model 340
- Proxim/Avaya/Orinoco:
 - Model AP-600
 - Model AP-700
 - Model AP-1000
 - Model AP-2500
- Bluesocket:
 - AP-1600

Listing Stand Alone Access Points

After you have run a device discovery job to discover stand alone Access Points (APs) as described in “Discovering WLAN Devices on Your Network” on page 3-8, any APs connected to BSCs under BlueView management will be listed in the navigation pane of any BlueView status window.

To display a list of the stand alone APs connected to BSCs under BlueView management, click **Stand Alone APs/Access Points** from any Administrator Console page. The stand alone access points page appears as shown in Figure 5-1.

Actions	In Sync	Status	MAC	Template	Hostname	Location	Home Controller
<input type="checkbox"/>	All	All	All	All	All	All	All
<input type="checkbox"/>	Yes		00:0e:d7:94:c2:60		jby-Cisco1100.bluesocket.com	Burlington	192.168.100.143
<input type="checkbox"/>	Yes		00:20:a6:58:d3:c8		JCSWIRELESS	Selma Middle	No Home Controller
<input type="checkbox"/>	Yes		00:20:a6:5e:43:8c		ORINOCO-AP-4000-5e-43-8c	here	No Home Controller
<input type="checkbox"/>	Yes		00:15:c7:80:07:40		ap1242		192.168.100.143
<input type="checkbox"/>	Yes				3Com Access Point	here	No Home Controller

[Check All](#) | [Clear All](#) | Assign template... | [Apply](#) | [Delete](#) | [Reboot](#) | [Mark synched and poll](#) | [Poll](#)

5 rows [download](#)

Figure 5-1: Listing Stand Alone APs

The following information is displayed for stand alone APs:

- **In Sync** - Does the AP configuration stored on BlueView match the AP's current configuration? Yes or No. If the configurations are out of sync, then click [Apply](#) to synchronize the configurations.
- **Status** - The AP's current status, Up or Down .
- **MAC** - The AP's configured MAC address.
- **Template** - Configuration template used to configure the AP's settings.
- **Hostname** - The hostname assigned to the AP in its BlueView configuration.
- **Location** - The location assigned to the AP in its BlueView configuration.
- **Home Controller** - The BSC to which the AP is connected.
- **Address** - The AP's IP address.
- **Vendor** - The vendor that manufactured the stand alone AP, Cisco, Proxim, etc.
- **Model** - The AP's model number.
- **Version** - The AP's firmware version number.
- **Description** - A description of the AP's firmware.

Click the icon to edit the credentials used to access an AP.

Click the icon to edit a AP's setup, and 802.11a and 802.11b/g radio configuration as described in the next section.

Click [Apply](#) to apply an AP configuration you have edited/saved on BlueView to the AP.

Click or [Delete](#) to delete an AP configuration.

Click [Reboot](#) to reboot the selected APs. You should only need to reboot an AP if it is hung or you have otherwise lost communications to it.

Click [Mark synched and poll](#) to change the AP's In Synch status to yes and then poll the AP.

If you have defined Stand Alone AP configuration templates as described in “Creating a Stand Alone AP Configuration Template” on page 5-11, click to assign/remove a template to/from the selected AP.

Editing Stand Alone Access Point Configurations


To enable a stand alone access point to be fully manageable from BlueView, you must configure:


- General Settings
- 802.11b/g Radio Settings
- 802.11a Radio Settings
- Access Credentials

Procedures to configure the above settings for stand alone AP models supported by BlueView are provided in the sections that follow.

General Settings

To define the general information that BlueView will use to identify a stand alone AP:

 **Note:** If the AP is associated with a Template, you click **Save**, only changes to the Name, IP Address, Location and Contact will be saved. All other changes must be made on the Template itself and will apply to every AP associated with the Template.

1. Click **Stand Alone APs/Access Points** from any Administrator Console page, and then click the  icon corresponding to the AP configuration you wish to edit. The Edit AP Access Point page appears as shown in Figure 5-2.

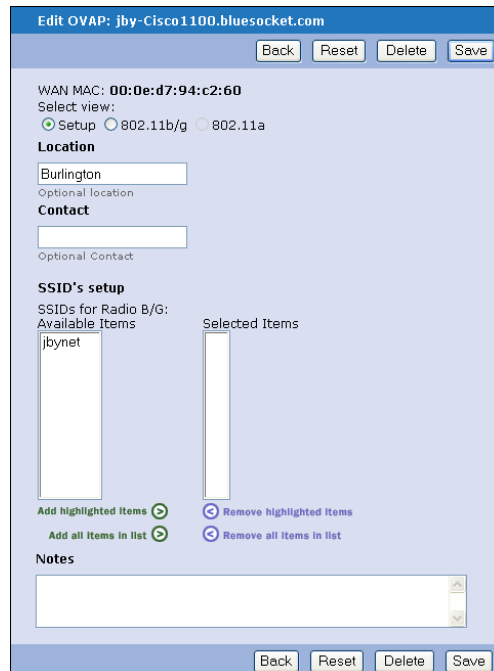



Figure 5-2: Defining Stand Alone AP Setup Information

2. Mark the **Setup** radio button at the top of the page.
3. Optional. Enter identifying information for the AP in the **Location** and **Contact** fields.

4. Optional. Enter meaningful information about the stand alone AP in the **Notes** field.
5. Define the configured SSIDs the AP is to use by selecting the SSIDs in the **Available Items** pane and then clicking **Add highlighted items** to move the selected SSIDs to the **Selected Items** pane.
See "Configuring Stand Alone AP SSIDs" on page 5-14 for information about Configuring Stand Alone AP SSIDs.
6. Click **Save** to save the specified stand alone AP configuration settings to the BlueView database and send the SSID to the AP.
You are returned to the Stand Alone APs/Access Points page.
7. Mark the checkbox corresponding to the AP configuration you just updated and then click to apply the configuration changes to the AP.

802.11b/g Radio Settings

To define the 802.11b/g radio settings on a stand alone AP on your network:

1. Click **Stand Alone APs/Access Points** from any Administrator Console page, and then click the  icon corresponding to the AP configuration you wish to edit.
2. Mark the **802.11 b/g** radio button at the top of the page.
The Edit AP page appears as shown in Figure 5-3.
3. Mark the **Enable Radio 1** checkbox to enable the 802.11b/g radio on the AP.
4. Use the **Data Rates** setting to choose the data transmission rates. The rates are expressed in megabits per second. For Cisco devices only, you can select multiple data rates and the device always attempts to transmit at the highest rate selected; if there are obstacles or interference, the device steps down to the highest rate that enables data transmission. All other devices support just a single data rate, so for these APs, only the the *lowest* valid data rate specified will be used.
5. When selecting multiple Required Datarates, Access Points which only support a single value (all Access Points except Cisco) will use the LOWEST valid value specified. For each of the rates, choose Require, Enable, or Disable.
 - **Require** - Enables transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to Require. A client must support a required rate before it can associate.
 - **Enable** - Enables transmission at this rate for unicast packets only.
 - **Disable** - Does not allow transmission at this rate.



Note: The client must support the basic rate you select or it cannot associate with the access point.

6. Configure the radio's Orthogonal Frequency Division Multiplexing transmitter power level in milliWatts or dBm by selecting a value from the **OFDM Transmitter Power** drop-down menu.
7. Specify the default channel on which the radio operates by selecting a value from the **Default Radio Channel** drop-down menu. By default, the radio is configured to operate on the least congested frequency.
8. Configure the **Radio Preamble** to short or long by marking the radio button.
The radio preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. You can set the radio preamble to long or short as described below:
 - **Short** - A short preamble improves throughput performance.

- **Long** - A long preamble ensures compatibility between the access point and all early models of Wireless LAN Adapters. If these client devices do not associate to your access points, you should use short preambles.

Edit AP: KR-WG102

WAN MAC: **00:14:6c:68:99:b2**

Select view:
 Setup 802.11b/g 802.11a

Enable Radio 1
Not supported for 3COM (pre v3.1).

Data Rates

1.0Mb/sec
 Require Enable Disable

2.0Mb/sec
 Require Enable Disable

5.5Mb/sec
 Require Enable Disable

6.0Mb/sec
 Require Enable Disable

9.0Mb/sec
 Require Enable Disable

11.0Mb/sec
 Require Enable Disable

12.0Mb/sec
 Require Enable Disable

18.0Mb/sec
 Require Enable Disable

24.0Mb/sec
 Require Enable Disable

36.0Mb/sec
 Require Enable Disable

48.0Mb/sec
 Require Enable Disable

54.0Mb/sec
 Require Enable Disable

Power and Channel Setup

OFDM Transmitter Power

Default Radio Channel

Packet Options

Radio Preamble
 Short Long
Not supported for Proxim and 3COM (pre v3.1).

Receive Antenna
 Diversity Left Right
Not supported for Proxim and 3COM.

Transmit Antenna
 Diversity Left Right
Not supported for Proxim and 3COM (pre v3.1).

Beacon Period

Interval in kilomicroseconds, Values (20-4000).
 Not supported for Proxim AP-2000.

RTS Threshold

Packet length in bytes when RTS/CTS are used, Values (0-2347).

Fragmentation Threshold

Packet length in bytes when packet gets fragmented, Values (256-2346).
 Not supported for Proxim.

DTIM Period

Send broadcast and multicast every (DTIM * Beacon Interval), Values (1-100)

Data Retries

Maximum number of attempts the device makes to send a packet before giving up, Values (1-128). Not supported for 3COM.

RTS Retries

Maximum number of times the device issues an RTS before stopping the attempt, Values (1-128). Not supported for 3COM.

Figure 5-3: Defining Stand Alone AP 802.11b/g Radio Settings

9. Select the antenna the access point uses to receive and transmit data. There are three options for both the receive and the transmit antenna:
 - **Diversity** - This default setting tells the access point to use the antenna that receives the best signal. If your access point has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
 - **Right** - If your access point has removable antennas and you install a high-gain antenna on the access point's right connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the right antenna is on the right.
 - **Left** - If your access point has removable antennas and you install a high-gain antenna on the access point's left connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the left antenna is on the left.
10. Configure the radio **Beacon Period** and **DTIM Period** settings.

The beacon period is the amount of time between access point beacons in Kilomicroseconds. One Kµsec equals 1,024 microseconds. The DTIM Period, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

If the beacon period is set at 100, its default setting, and the DTIM period is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kµsecs. One Kµsec equals 1,024 microseconds.
11. Configure the radio **RTS Threshold** and **RTS Retries** settings.

The RTS threshold determines the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other. You can enter a setting ranging from 0 to 2339 bytes.

RTS Retries is the maximum number of times the access point issues an RTS before stopping the attempt to send the packet over the radio. Enter a value from 1 to 128. The default RTS threshold is 2312, and the default **RTS Retries** setting is 32.
12. Configure the radio **Fragmentation Threshold** setting.

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

The default setting is 2338 bytes.
13. Configure the radio **Data Retries** setting.

The maximum data retries setting determines the number of attempts the access point makes to send a packet before giving up and dropping the packet.

The default setting is 32.
14. Optional. Enter meaningful information about the stand alone AP in the **Notes** field.
15. Click **Save** to save the specified stand alone AP settings to the BlueView database. You are returned to the Stand Alone APs/Access Points page.
16. Mark the checkbox corresponding to the AP configuration you just updated and then click to apply the configuration changes to the AP.

802.11a Radio Settings

Edit AP: KR RBT-4102

Back Reset Delete Save

WAN MAC: **00:11:88:5a:50:a9**

Select view:
 Setup 802.11b/g 802.11a

Enable Radio 2
Not supported for 3COM (pre v3.1).

Data Rates

6.0Mb/sec
 Require Enable Disable

9.0Mb/sec
 Require Enable Disable

12.0Mb/sec
 Require Enable Disable

18.0Mb/sec
 Require Enable Disable

24.0Mb/sec
 Require Enable Disable

36.0Mb/sec
 Require Enable Disable

48.0Mb/sec
 Require Enable Disable

54.0Mb/sec
 Require Enable Disable

Power and Channel Setup

Transmitter Power
 Minimum

Default Radio Channel
 Least Congested Frequency

Packet Options

Receive Antenna
 Diversity Left Right
Not supported for Proxim and 3COM.

Transmit Antenna
 Diversity Left Right
Not supported for Proxim and 3COM.

Beacon Period
 100
Interval in kilomicroseconds, Values (20-4000).
 Not supported for Proxim AP-2000.

RTS Threshold
 2347
Packet length in bytes when RTS/CTS are used, Values (0-2347).

Fragmentation Threshold
 2346
Packet length in bytes when packet gets fragmented, Values (256-2346).
 Not supported for Proxim and 3COM (pre v3.1).


DTIM Period
 3
Send broadcast and multicast every (DTIM * Beacon Interval), Values (1-100)

Data Retries
 64
Maximum number of attempts the device makes to send a packet before giving up, Values (1-128). Not supported for 3COM.

RTS Retries
 4
Maximum number of times the device issues an RTS before stopping the attempt, Values (1-128). Not supported for 3COM.

Figure 5-4: Defining Stand Alone AP 802.11a Radio Settings

To define the 802.11a radio settings on a stand alone AP on your network:

1. Click **Stand Alone APs/Access Points** from any Administrator Console page, and then click the  icon corresponding to the AP configuration you wish to edit.
2. Mark the **802.11 a** radio button at the top of the page.
 The Edit AP page appears as shown in Figure 5-4.

3. Mark the **Enable Radio 2** checkbox to enable the 802.11a radio on the AP.
4. Complete the remaining AP 802.11a radio settings and then click **Save** to save the specified stand alone AP configuration settings to the BlueView database.

When configuring the 802.11a radio settings for the stand alone AP, refer to the 802.11 b/g radio setting descriptions given starting in "802.11b/g Radio Settings" on page 5-5, as these settings match those for the 802.11a radio.


You are returned to the Stand Alone APs/Access Points page.

5. Mark the checkbox corresponding to the AP configuration you just updated and then click to apply the configuration changes to the AP.

Access Credentials

To enable BlueView to fully manage an AP via SNMP and update the AP's firmware file, you must define the SNMP and telnet credentials BlueView can use to access the AP.

To define a stand alone AP's access credential's:

1. Click **Stand Alone APs/Access Points** from any Administrator Console page, and then click the  icon corresponding to the AP configuration you wish to edit. The Edit AP page appears as shown in Figure 5-5.



The screenshot shows the 'Edit AP: netgear6f2900' configuration page. At the top, there are buttons for 'Back', 'Reset', 'Delete', and 'Save'. Below the title, the WAN MAC is '00:14:6c:6f:29:00'. The 'Name' field contains 'netgear6f2900'. The 'Device Group' is a dropdown menu. Below it, there is a note: 'Container to manage this device.' The 'AP Template' is another dropdown menu. A note states: 'All config items will be controlled via the template.' Under the 'IP Address' section, the IP Address field contains '192.168.5.120'. The 'SNMP V2' section has two rows: 'Read-Only Community String' and 'Read-Write Community String', each with a 'Confirm' field. The 'Telnet' section has three rows: 'User', 'Password', and 'Enable Password', each with a 'Confirm' field. At the bottom, there is a 'Notes' section with a large text area. Navigation buttons 'Back', 'Reset', 'Delete', and 'Save' are at the bottom of the page.

Figure 5-5: Configuring a Stand Alone AP's Access Credentials

2. Enter the AP's hostname in the **Name** field.
3. Enter the AP's IP address in the **IP Address** field.

4. Select a configuration template for the AP from the **AP Template** drop-down menu. The selected template will be used to configure the AP's setup and 802.11 a and 802.11b/g radio settings. Creating stand alone AP configuration templates is described in the next section.
5. Specify to which device group the stand alone AP belongs by selecting a group from the **Device Group** drop-down menu.
6. Define the SNMP v2 passwords for BlueView to access/manage the AP via SNMP. Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-only Community String** field, and then re-enter the password in the **Confirm** field. Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-Write Community String** field, and then re-enter the password in the **Confirm** field.
7. Define the authentication information required for telnet access to the AP. Telnet access to the AP is required to update the AP's firmware. Enter the telnet session username in the **User** field. Enter the telnet session password in the **Password** field, and then re-enter the password in the **Confirm** field. Enter the telnet session enable mode password in the **Enable Password** field, and then re-enter the password in the **Confirm** field.
8. Optional. Enter meaningful information about the stand alone AP in the **Notes** field.
9. Click **Save** to save the stand alone AP configuration settings to the database. You are returned to the Stand Alone APs/Access Points page.
10. Mark the checkbox corresponding to the AP configuration you just updated and then click to apply the configuration changes to the AP.


Creating a Stand Alone AP Configuration Template

BlueView enables you to create to configuration templates to simplify and speed up the configuration of stand alone APs on your network for management by BlueView. You may want to create a configuration template for each stand alone AP model on your network.

The screenshot shows a web form titled "Empty list, create new AP Template". At the top, there are four buttons: "Back", "Reset", "Save", and "Save and create another". Below the buttons, there is a "Select view:" section with four radio buttons: "Credentials" (selected), "Setup", "802.11b/g", and "802.11a". The form is divided into several sections: "Name" with a text input field; "SNMP V2" with two pairs of fields: "Read-Only Community String" and "Confirm", and "Read-Write Community String" and "Confirm"; "Telnet" with three pairs of fields: "User" and "Confirm", "Password" and "Confirm", and "Enable Password" and "Confirm"; and "Notes" with a large text area. At the bottom, there are four buttons: "Back", "Reset", "Save", and "Save and create another".

Figure 5-6: Creating a Stand Alone AP Template


To create a stand alone AP configuration template:

-  **Note:** Associating a Template with a Stand Alone AP will override any Credentials which had been set on that AP with those specified in the Template.
1. Click **Stand Alone APs/AP Templates** from any Administrator Console page.
The Create a New AP Template page appears (see Figure 5-5).
 2. Mark the **Credentials** radio button and then configure the AP template credential settings as described in “Access Credentials” on page 5-10.
 3. Mark the **Setup** radio button and then configure the AP template general setup settings as described in “General Settings” on page 5-4.
 4. Mark the **802.11 b/g** radio button and then configure the AP template 802.11 b/g radio settings as described in “802.11b/g Radio Settings” on page 5-5.
 5. Mark the **802.11 a** radio button and then configure the AP template 802.11 b/g radio settings as described in “802.11a Radio Settings” on page 5-9.
 6. Click **Save** to save the AP configuration template to the BlueView database.

Adding a Stand Alone AP for Management by BlueView

After you have discovered BlueSecure Controllers or manually added BlueSecure Controllers to the BlueView managed device list, any stand alone Access Points (APs) connected to the BSCs under BlueView management will be listed in the navigation pane of any BlueView status window. To display a list of the stand alone APs connected to BSCs under BlueView management, click **Stand Alone APs/Access Points** from any Administrator Console window.

You can also manually add a stand alone AP to the BlueView managed device list by completing these steps:

1. Click **Stand Alone APs/Access Points** from any Administrator Console page.
The stand alone access points page appears (see Figure 5-1).
2. Click  at the top of the stand alone access points page.
The Create New AP page appears (see Figure 5-5).
3. Enter the AP's hostname in the **Name** field.
4. Enter the AP's IP address in the **IP Address** field.
5. Specify to which device group the stand alone AP belongs by selecting a group from the **Device Group** drop-down menu.
6. Select the configuration template from which to configure the AP's settings from the **AP Template** drop-down menu.

You must upload a stand alone AP configuration template as described in “Creating a Stand Alone AP Configuration Template” on page 5-11 before this menu is populated with selections.

If you select a configuration template for the stand alone AP, then skip to step 9 of this procedure.

7. Define the SNMP v2 passwords that will enable BlueView to access and manage the AP via SNMP.

Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-only Community String** field, and then re-enter the password in the **Confirm** field.

Enter the password that gives BlueView read-only access to the AP's MIB in the **Read-Write Community String** field, and then re-enter the password in the **Confirm** field.

- Define the authentication information required for telnet access to the AP. Telnet access to the AP is required to update the AP's firmware.

Enter the telnet session username in the **User** field.

Enter the telnet session password in the **Password** field, and then re-enter the password in the **Confirm** field.

Enter the telnet session enable mode password in the **Enable Password** field, and then re-enter the password in the **Confirm** field.

The screenshot shows a web-based configuration form titled "Create new AP". At the top, there are four buttons: "Back", "Reset", "Save", and "Save and create another". The form is organized into several sections:

- Name:** A text input field.
- Device Group:** A dropdown menu.
- AP Template:** A dropdown menu. Below it, a note states: "All config items will be controlled via the template."
- IP Address:** A text input field.
- SNMP V2:** Two pairs of fields. The first pair is "Read-Only Community String" and "Confirm". The second pair is "Read-Write Community String" and "Confirm".
- Telnet:** Four pairs of fields. The first pair is "User" and a text input. The second pair is "Password" and "Confirm". The third pair is "Enable Password" and "Confirm".
- Notes:** A large text area for entering additional information.

At the bottom of the form, there are four buttons: "Back", "Reset", "Save", and "Save and create another".

Figure 5-7: Adding a Stand Alone AP

- Optional. Enter meaningful information about the stand alone AP in the **Notes** field.
- Click **Save** to save the specified stand alone AP configuration settings to the BlueView database.
You are returned to the Stand Alone APs/Access Points page.
The newly added AP is listed on the stand alone access points page
- Mark the checkbox corresponding to the AP configuration you just updated and then click **Apply** to apply the configuration changes to the AP.
- if you haven't specified a configuration template for the stand alone AP, then you must complete the following steps to fully configure the AP for management by BlueView:
 - Configure the AP's general setup information as described in "General Settings" on page 5-4.

- b) Configure the AP's 802.11b/g radio settings as described in "802.11b/g Radio Settings" on page 5-5.
- c) Configure the AP's 802.11a radio settings as described in "802.11a Radio Settings" on page 5-9.

Configuring Stand Alone AP SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSIDs.

You can configure up to 16 SSIDs on your stand alone access point and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of its configured SSIDs.

You must configure the following settings for each AP:

- VLAN
- Client authentication method

To define the Service Set Identifiers (SSIDs) you will use on the stand alone APs:

1. Click **Stand Alone APs/SSIDs** from any Administrator Console page.
A list of previously configured stand alone AP SSIDs appears.
2. Click at the top of the stand alone AP SSIDs page.
The SSID page appears as shown in Figure 5-8.
3. Enter the Service Set Identifier to enable on the AP in the **SSID** field.
4. Optional. Assign the SSID to a virtual LAN (VLAN) interface by entering the VLAN ID in the **VLAN** field.

If your network uses VLANs, you can assign one SSID to a VLAN, and client devices using the SSID are grouped in that VLAN. Enter 0 if you are not using VLANs on your network.

5. Enter a network identifier for the SSID in the **Network ID** field.
6. Enter the maximum number of wireless clients that may associate to the AP in the **Association Limit** field. Valid limit settings are 1 to 56. Enter 0 if you do not wish to limit client associations.
7. Configure an authentication method for the SSID by marking one of the following checkboxes.
 - **Open Authentication** - Open authentication allows any device to authenticate and then attempt to communicate with the access point. You can configure the following additional authentication options:
 - **MAC authentication** - The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network.
 - **EAP** - The access point forces all client devices to perform EAP authentication before they are allowed to join the network.
 - **MAC authentication and EAP**
 - **MAC authentication or EAP**
 - **Shared Authentication** - Set the authentication type for the SSID to shared key. You can configure the following authentication options:
 - **MAC authentication** - The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network.

- **EAP** - The access point forces all client devices to perform EAP authentication before they are allowed to join the network.
- **MAC authentication and EAP**

Create new SSID

Back Reset Save Save and create another

General

SSID VLAN
0 for untagged, 1 - 4095.

Broadcast SSID

Primary SSID
Cisco VxWorks, Proxim and Enterasys RBT-4102 only

Network ID
Enter 0 for no network id.

Association Limit
Enter 0 for no association limit.

Authentication

Open Authentication:

Shared Authentication:

Network EAP:

Pre-Shared Key:
Alphanumeric 8-63 characters, Hex: 64 characters

EAP Authentication Servers

Priority 1

Priority 2

Priority 3

MAC Authentication Servers

Priority 1

Priority 2

Priority 3

Data Encryption

None

Cipher

Cipher

Encryption Keys

Encryption Key 1

Encryption Key (Hexadecimal) Key Size

Encryption Key 2

Encryption Key (Hexadecimal) Key Size

Encryption Key 3

Encryption Key (Hexadecimal) Key Size

Encryption Key 4

Encryption Key (Hexadecimal) Key Size

Back Reset Save Save and create another

Figure 5-8: Defining Stand Alone AP SSIDs

- **Network EAP** - Set the authentication type for the SSID to Network-EAP. Using the Extensible Authentication Protocol (EAP) to interact with an EAP-compatible

RADIUS server, the access point helps a wireless client device and the RADIUS server to perform mutual authentication and derive a dynamic unicast WEP key. However, the access point does not force all client devices to perform EAP authentication. You can configure the following authentication options:

- **MAC authentication** - The access point forces all client devices to perform MAC-address authentication before they are allowed to join the network.
8. Define the **EAP Authentication Servers** to use when performing EAP authentication on wireless clients. You may define up to three servers by selecting from the **Priority 1**, **Priority 2**, and **Priority 3** drop-down menus. The defined priority 1 server is queried before the priority 2 server, and the priority 2 server is queried before the priority 3 server.
 9. Define the **MAC Authentication Servers** to use when performing MAC address authentication on wireless clients. You may define up to three servers by selecting from the **Priority 1**, **Priority 2**, and **Priority 3** drop-down menus. The defined priority 1 server is queried before the priority 2 server, and the priority 2 server is queried before the priority 3 server.
 10. Define the encryption mode for the stand alone AP by marking the appropriate radio button:
 - **None** - Communication between the access point and client devices is in the clear.
 - **Cipher** - Communication between the access point and client devices is encrypted.
Select the encryption method to use from the **Cipher** drop-down menu.
 11. Optional. Define static WEP keys for use on the AP.

You need to configure static WEP keys only if your access point needs to support client devices that use static WEP. If all the client devices that associate to the access point use key management (WPA, CCKM, or 802.1x authentication) you do not need to configure static WEP keys.

Enter the key in the **Encryption Key** field and select the size of the key, 40-bit, 64 bit, 128 bit, or 128-bit, from the **Key Size** field.

40-bit keys contain 10 hexadecimal digits; 128-bit keys contain 26 hexadecimal digits.
 12. Click **Save** to save the specified stand alone AP SSID settings to the BlueView database.

You are returned to the Stand Alone APs/SSIDs page.
 13. Mark the checkbox corresponding to the SSID configuration you just updated and then click to apply the configuration changes.

Configuring Stand Alone AP RADIUS Authentication Servers

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software.

If user authentication to your stand alone access point is controlled by a RADIUS server, then you must configure the login information for that RADIUS server.

To configure a stand alone AP RADIUS authentication server:

1. Click **Stand Alone APs/RADIUS Servers** from any Administrator Console page.

A list of previously configured stand alone AP RADIUS authentication servers appears.

2. Click **Add** at the top of the stand alone AP RADIUS authentication servers page. The RADIUS server page appears as shown in Figure 5-9.
3. Enter the IP address of the remote RADIUS server host in the **IP Address** field.
4. Enter the UDP destination port for RADIUS authentication requests in the **Authentication Port** field.
5. Enter the UDP destination port for RADIUS accounting requests in the **Accounting Port** field.
6. Enter the authentication and encryption key used between the access point and the RADIUS daemon running on the RADIUS server in the **Secret** field.
7. Enter the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly in the **Retries** field. The range is 1 to 1000.
8. Enter the time interval in seconds that the access point waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000 seconds.

The screenshot shows a web-based configuration form for a RADIUS server. The form is titled "Radius Server" and has a blue header. Below the header, there are four buttons: "Back", "Reset", "Delete", and "Save". The form is divided into two main sections: "Network" and "Settings".

Network Section:

- IP Address:** A text input field.
- Authentication Port:** A text input field.
- Accounting Port:** A text input field, labeled as "Optional".

Settings Section:

- Secret:** A text input field.
- Retries:** A text input field with the value "8".
- Timeouts:** A text input field with the value "8".

At the bottom of the form, there are four buttons: "Back", "Reset", "Delete", and "Save".

Figure 5-9: Defining Stand Alone AP RADIUS Authentication Servers

6

Monitoring WLAN Devices

After discovering the BlueSecure devices and stand alone APs on your network, organizing them into groups, configuring the stand alone APs for management by BlueView, and setting up BlueView for your network, you are ready to monitor the WLAN devices for status information using BlueView. Additionally, if you have BlueSecure Centralized Sensors or BSAPs operating in sensor mode on your network, you can monitor your protected airspace using BlueView. This chapter includes:

- Displaying Summary Information
- Monitoring Your Protected Airspace
- Monitoring Active User Connections
- Displaying BSC Logs
- Displaying BSC Alarms
- Displaying Sensor Alarms
- Generating Status Reports
- Displaying and Saving Status Reports
- Generating and Displaying RF Heat Maps
- Monitoring Devices in RF Autocontainment


Displaying Summary Information

BlueView displays summary information about itself and the BlueSecure devices and stand alone access points it is managing on your network. Devices under management are listed in the navigation pane of the BlueView screens.

- Displaying BlueView Summary Information
- Displaying Bluesocket BSC Summary Information
- Displaying AP Summary Information

Displaying BlueView Summary Information

To display summary information about your BlueView Management System:

1. Click **Status/Summary** from any Administrator Console page.
2. Click the  **BlueView** link in the navigation pane. BlueView summary information is displayed, for example.

Sign out, admin | Site Map | Help

Status Jobs Devices Stand Alone APs RF Sensor BlueView

2007-07-24 17:51:33

Summary Active Connections RF View Logs Alarms RF Alarms Reports Maps Contained Devices

This page will refresh in 6 seconds.

Ethernet 1 Status		edit
MAC Address	00:0E:0C:2D:1D:12	
Link Up	true	
IP Address	192.168.100.142	
Netmask	255.255.252.0	
Broadcast	192.168.103.255	
Bytes Out	998449912	
Bytes In	2252775867	
Duplex	Full	
Speed	100Mb/s	

Available Disk Space	
Current Partition (System)	1.3G
Current Partition (Data)	3.6G
Alternative Partition (System)	1.7G
Alternative Partition (Data)	3.4G
Shared Data	169G

System Status	
Users Logged In	4
Free Memory	990277192
CPU	Unavailable

Ethernet 2 Status		edit
MAC Address	00:0E:0C:22:60:54	
Link Up	false	
IP Address	192.168.160.1	
Netmask	255.255.252.0	
Broadcast	192.168.160.255	
Bytes Out	0	
Bytes In	0	
Duplex	Unknown! (255)	
Speed	Unknown! (65535)	

Percentage Disk Space Used	
Current Partition (System)	40%
Current Partition (Data)	12%
Alternative Partition (System)	20%
Alternative Partition (Data)	17%
Shared Data	2%

Figure 6-1: BlueView Summary Information



The displayed BlueView Management System summary information includes:

- Network Interface Status (Ethernet 1 and Ethernet 2)
 - **MAC Address** - The network interface's Media Access Control address.

- **Link Up** - "True" when the network interface is up and "False" when the network interface is down.
- **IP Address** - The network interface's configured IP address.
- **Netmask** - The network interface's subnet mask setting.
- **Broadcast** - The network interface's broadcast address calculated from its IP address and Netmask settings.
- **Bytes Out** - Count of bytes transmitted since last network restart.
- **Bytes In** - Count of bytes received since last network restart.
- **Duplex** - Half duplex or full duplex Ethernet communications.
- **Speed** - Data transmission rate over Ethernet link in Megabits per second.
- Available Disk Space
 - **Current Partition (System)** - Disk space available for use by BlueView system files on active partition.
 - **Current Partition (Data)** - Disk space available for use by BlueView data files on active partition.
 - **Alternate Partition (System)** - Disk space available for use by BlueView system files on inactive partition.
 - **Alternate Partition (Data)** - Disk space available for use by BlueView data files on inactive partition.
 - **Shared Data** - Disk space available to store shared data including: firmware/patches/backup images, as well as logs and alarms.
- Percentage Disk Spaced Used
 - **Current Partition (System)** - Percentage of total available disk space used by BlueView system files on active partition.
 - **Current Partition (Data)** - Percentage of total available disk space used by BlueView data files on active partition.
 - **Alternate Partition (System)** - Percentage of total available disk space used by BlueView system files on inactive partition.
 - **Alternate Partition (Data)** - Percentage of total available disk space used by BlueView data files on inactive partition.
 - **Shared Data** - Percentage of available disk space used to store shared data including: firmware/patches/backup images, logs and alarms.
- System Status
 - **Users Logged In** - Count of administrative users logged into the system.
 - **Free Memory** - Count of available memory in bytes.
- Click the [edit](#) link to modify BlueView's network interface configuration as described in "Configuring the BlueView Network Interfaces" on page 4-8.

Displaying Bluesocket BSC Summary Information

To display summary information about your BlueSecure Controllers:

1. Click **Status/Summary** from any Administrator Console page.
2. Click on the  **All BlueSecure Controllers** link or a group link, , in the navigation pane to display summary information for all of the BSCs on your network or for a specific group of BSCs.

BSC group summary information is displayed in the information pane as shown in Figure 6-2.

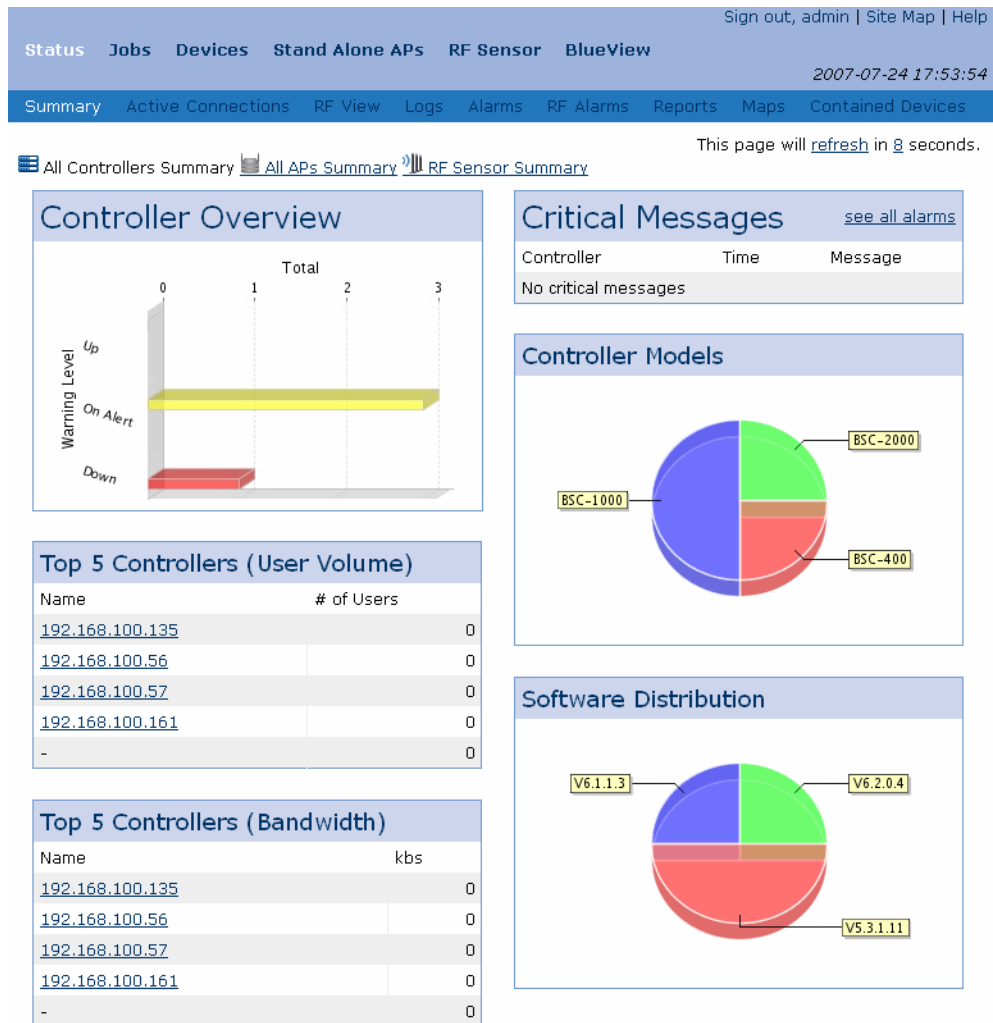



Figure 6-2: BlueView BSC Summary Information (Group)

Alternatively, click on an individual BSC link, , in the navigation pane to display summary information for that particular BSC in a separate browser window as shown in Figure 6-3.


Pass the cursor over the pie charts to see which BSCs comprise the model types and software distribution.




BSC Group Summary Information


Information presented on the BSC group summary page includes:

- **Controller Overview** - A concise visual summary of BSCs in the group since the last network poll. Counts are provided for BSCs UP (running and communicating with BlueView), On Alert (i.e., having sent alarms to the BSC), and Down (i.e., unreachable by BlueView).

- **Top 5 Controllers (User Volume)** - The five BSCs in the group with the most active user sessions. BSCs are identified by their protected port IP address.
- **Top 5 Controllers (Bandwidth)** - The five BSCs in the group using the most bandwidth (Kilobits). BSCs are identified by their protected port IP address.
- **Critical Messages** - A list of critical messages received. Each message is identified by the source BSC and is time-stamped.
- **BSC Model Types** - A concise visual summary of the BSC models (BSC-600, BSC-1200, BSC-2100 and BSC-5200) in the group.
- **Software Distribution** - A concise visual summary of system software releases installed on BSCs in the group.

The group folder icon, , in the navigation pane conveys the following status the following status information at a glance:

-  - All BSCs in the group are up and operational.
-  - All BSCs in the group are up, but at least one BSC in the group has sent an alert message to BlueView. Possible BSC alerts include that its managed interface is down or that its CPU is operating at 80% or more.
-  - One or more BSCs in the group is down (unreachable from BlueView).

Pass the cursor over a group folder icon, , to display a text summary listing group status, a brief description of that status, links to status windows for any Controllers in the group that are on alert, and links to the group's status, logs, and alarms displays.



Individual BSC Summary Information

Information presented on the BSC summary page (see Figure 6-3) includes:

- **Polling Option**
 Click to poll the selected BSC immediately and refresh the display.
- **Status**
 - **System** - Either "Up" (running and communicating with BlueView) or "Down" (i.e., unreachable by BlueView).
 - **System Uptime** - Total time BSC has been up, i.e., reachable from BlueView. The uptime count is reset anytime connectivity to the BSC is lost.
 - **Last Successful Poll** - The time BlueView last collected data from the BSC. When the System state is "Down", the Last successful poll time stamps are displayed in red.
 - **Last Error** - The time an error condition was last detected on the BSC.
 - **Managed Interface** - Current state of BSC's managed interface, either "Up" or "Down." The BSC receives data traffic from wireless users on its managed interface.
 - **Protected Interface** - Current state of BSC's protected interface (Up or Down). The BSC uses this interface to communicate with BlueView.
 - **Failover Unit** - Either "Connected" or "Not Connected." The BSC may fail over to another BSC connected via its failover interface if the BSC should fail to function properly.
 - **Disk Space Total** - Byte count of the BSC's total available storage space.
 - **Disk Space Used** - Byte count of the BSC's storage space currently used.
 - **CPU** - Percentage of BSC's CPU in use.

Sign out, admin | Site Map | Help

Status **Jobs** **Devices** **Stand Alone APs** **RF Sensor** **BlueView**

2007-07-24 17:58:07

Summary Active Connections RF View Logs Alarms RF Alarms Reports Maps Contained Devices

This page will [refresh](#) in 22 seconds.

[Controller Summary](#)
 [Controller's APs Summary](#)
 [RF Sensor Summary](#)

Status

System	Up
System Uptime	5 days, 3 hours, 35 minutes, 23 seconds.
Last successful poll	2007-07-24 17:57:29
Last Error	
Managed Interface	Down
Protected Interface	Up
Failover Unit	Not Connected
Disk Space Total	8436 MB
Disk Space Used	363 MB
CPU	<div style="width: 5%; height: 10px; background-color: green; display: inline-block;"></div> 5%



Specifications

Name	192.168.100.135
Address	192.168.100.135
Model	BSC-2000
Sys Contact	Unknown
Sys Location	Unknown
Running Software	V6.2.0.4
Alternate Software	V6.2.0.3
Patches Installed	DevPatch Thu Jul 19 00:42:45 2007 V6 R.1
Group	Default
Last successful poll	2007-07-24 16:30:50
Last Error	

User Activity

[see all logs](#)

Total Number of Users	0
Users Logged In	0
Users with VPN	0
Total Bandwidth	0 kbs
Attached APs	3
Last successful poll	2007-07-24 17:50:39
Last Error	

Alarm Summary

[see all alarms](#)


	Last Hour	Last Day	Total
Emergency	0	0	0
Alert	0	0	0
Critical	0	0	0
Error	0	0	0
Warning	0	0	0
Notice	0	0	0
Info	0	0	0
Debug	0	0	0




Figure 6-3: BlueView BSC Summary Information (Single BSC)


- Specifications
 - **Name** - The BSC's hostname or protected interface IP address.
 - **Address** - Hyperlink to the BSC's protected interface IP address. You may click this link to access the BSC's administrator interface.
 - **Model** - BSC-600, BSC-1200, BSC-2100, or BSC-5200. The model type is represented visually in the upper right corner of the summary page.
 - **Sys Contact** - Contact information for this BSC (optional, admin supplied).
 - **Sys Location** - Location of this BSC (optional - administrator supplied).
 - **Running Software** - Version number of the BSC's system software.

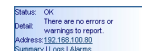
- **Alternate Software** - Version number of the system software stored on the BSC's inactive partition.
 - **Patches Installed** - Click the [Patches](#) link to see a listing of the version numbers of the software patches installed on the BSC.
 - **Group** - BlueView group to which the BSC is assigned.
 - **Last Poll** - The time BlueView last collected data from the BSC.
 - **Last Error** - The time an error condition was last reported by the BSC.
 - **User Activity**
 - **Total Number of Users** - Total number of BSC users.
 - **Users Logged In** - Number of users currently logged into the BSC.
 - **Users with VPN** - Number of users that opened a Virtual Private Network (VPN) tunnel (e.g., IPSec) to the BSC.
 - **Total Bandwidth** - Count of kilobytes consumed by user data traffic.
 - **Attached APs** - Access Points connected to this BSC.
 - **Last Poll** - Last Poll - The time BlueView last collected data from the BSC.
 - **Last Error** - The time an error condition was last reported by the BSC.

Click the [see all logs](#) link to display a filtered view of log entries received from this BSC. (filtered views of log entries are described in the next section).
 - **Alarm Summary** - Table summarizing types of alarm received by BlueView over the last day, over the last hour, and in total.
- Click the [see all alarms](#) link to display a filtered view of alarms received from this BSC. Filtered views of BSC alarms are described in "Displaying BSC Alarms" on page 6-22.

The individual BSC icon, , in the navigation pane conveys the following status the following status information at a glance:





-  - The BSC is up and operational.
-  - The BSC is up, but it has sent an alert message to BlueView. Possible BSC alerts include that its managed interface is down or its CPU is operating at 80% or more.
-  - The BSC is down, i.e. unreachable from BlueView.

Pass the cursor over an individual BSC link, , in the navigation pane to show a summary of BSC status, a description of that status, a link to the BSC's administrator console, and links to the BSC's active connections, logs, alarms, and edit configuration displays.



Displaying AP Summary Information

To display summary information about your BlueSecure access points connected to BSCs on your network:

1. Click **Status/Summary** from any Administrator Console page.
2. Click on the  **All BlueSecure Controllers** link in the navigation pane and then click on the  **All APs Summary** link at the top of the summary page to display summary information for all APs. Alternatively, click on an individual controller icon  in the navigation pane, then the  **All Controller's APs** link at the top of the summary

page to display summary information for all of APs configured on that BSC. For example:

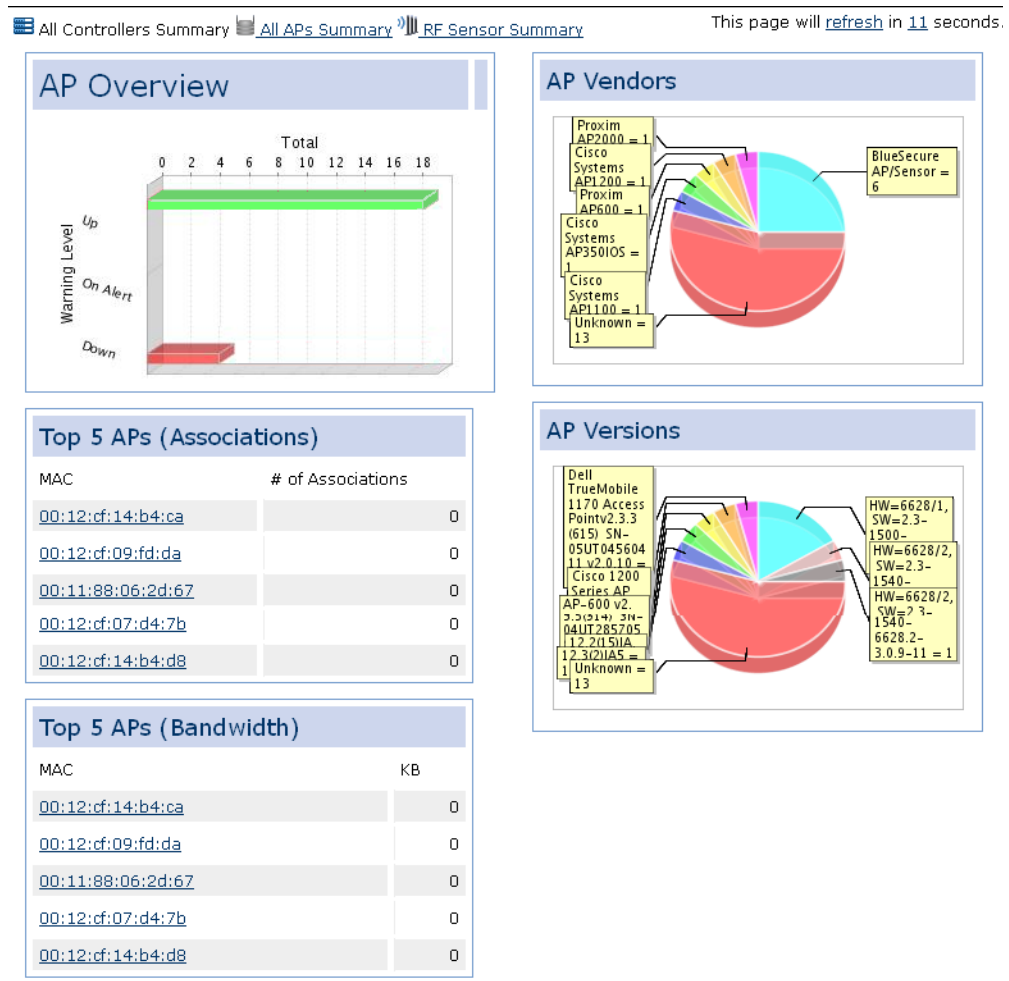



Figure 6-4: BlueView AP Summary Information (All)

Alternatively, click on an individual AP link, , in the navigation pane to display summary information for that particular AP in a separate browser window (see Figure 6-5).

All APs Summary Information

Information presented on the All APs summary page includes:

- **AP Overview** - A concise visual summary of APs associated to the BSC since the last network poll. Counts are provided for APs UP (running, configured, and communicating with the BSC), On Alert (i.e., up but not configured by the BSC), and Down (i.e., unreachable by the BSC).
- **Top 5 APs (Associations)** - The five APs connected to the BSC with the most user associations. APs are identified by their MAC address.
- **Top 5 APs (Bandwidth)** - The five APs connected to the BSC using the most bandwidth, measured in KiloBytes. APs are identified by their MAC address.

- **AP Vendors** - A concise visual summary of the AP types (by manufacturer) connected to the BSC.
- **AP Versions** - A concise visual summary of the AP models in the group.

Single AP Summary Information

Click on a hyper-linked BSAP or stand alone AP label to display summary information about the AP in the information panel (see Figure 6-5).

Information presented on the BSAP summary page includes:

- **Status**
 - **Status** - Either "Up" (communicating with its home BSC) or "Down" (unreachable from the BSC). Status for a BSAP that has been configured on a BSC but has not yet connected to the BSC is listed as "No runtime data is known about this AP."
 - **Name** - Hostname assigned to this AP.
 - **Address** - Configured IP address of the AP, i.e. the public address that BVMS uses to communicate with the AP.
 - **NAT Private Address** - The address that the Controller used to discover the AP. Typically BVMS is configured to have a Static Route through the Controller to gain access to the Managed-side APs. However when that is not possible (for example, the Controller is multiple hops away from BVMS and corporate security prevents Static Routes on other routers), configuring the Controller with one-to-one NAT provides a secure mechanism for BVMS to communicate directly with the APs. NAT is generally not required with BSAPs since the Controller already acts as a Proxy Agent.
 - **SSID** - Service Set Identifier assigned to the AP.
 - **Channel** - Channel on which the AP's 802.11a and 802.11b/g radios are operating.
 - **Power** - Configured transmission power level for the 802.11a and 802.11b/g radios.
 - **Memory** - Available memory on AP (in bytes).
- **Specifications**
 - **MAC** - AP media access control address.
 - **Vendor** - Vendor and model number of AP.
 - **Firmware** - Version number of the firmware installed and running on the AP.
 - **Type** - BAP = BlueSecure Access Point.
 - **Location** - Configured location of the AP.
 - **Security** - Configured security for the AP:
 - Open system
 - Shared Key
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK
 - WPA + WPA2
 - WPA-PSK + WPA2-PSK


AP Summary [RF Sensor Summary](#) This page will refresh in 18 seconds.

Status

Status	Up
Address	192.168.100.212
SSID	MacGrill
Channel	BG=8, A=140
Power	BG=0, A=0
Memory	0

Specifications

MAC	00:12:cf:09:fd:e9
Vendor	BlueSecure AP/Sensor-1500
Firmware	HW=6628/1, SW=2.3-375-6628.1-1.0.9-27
Type	BAP
Location	
Security	Default=Open System



Radio - b/g

MAC	00:12:cf:0a:0b:10
State	1
Associations	1
Adjacent APS	0
Channel	8
Auto Channel?	0
Tx Power	0
Tx Rate	100
Beacon Rate	100

Adjacent APs on radio 1:

MAC	SSID	RSSI	Beacon	Security
No adjacent APs				

Radio - a

MAC	00:12:cf:0a:0b:11
State	1
Associations	0
Adjacent APS	14
Channel	140
Auto Channel?	0
Tx Power	0
Tx Rate	100
Beacon Rate	100

Adjacent APs on radio 2:

MAC	SSID	RSSI	Beacon	Security
00:04:e2:aa:a9:c5	Picnic	12	49718	0
00:04:e2:aa:a9:b7	Picnic	49	49702	0
00:12:cf:0a:07:31	Wicklow	27	49792	0
00:12:cf:0a:06:51	chariot	26	49849	0
00:04:e2:aa:a8:c2	Picnic	40	49804	0
00:04:e2:aa:a9:82	Picnic	12	49829	0
00:12:cf:0a:05:f1	MacGrill	32	49768	0
00:04:e2:a1:5d:2f	Picnic	23	49853	0
00:04:e2:aa:a9:b0	Picnic	15	49804	0
00:12:cf:0a:06:c1	Valhalla	22	49829	0
00:11:20:ee:7c:97	QA-Fast	34	49833	1
00:12:cf:0a:06:f1	pf0y01	43	49808	0
00:12:cf:0a:06:a1	QA_TA_TEST3	35	49849	0
00:12:cf:0a:06:e1	QA_TA_TEST3	31	49837	0

www.bluesocket.com

Figure 6-5: BlueView AP Summary Information (Single BSAP)

- Radio b/g and Radio a
 - **MAC** - Individual MAC address of 802.11a/802.11b/g radios.

- **State** - Operating (1) or not operating (0).
- **Associations** - Count of wireless clients associated to the radio.
- **Adjacent APs** - APs operating within range of the AP.
- **Channel** - Channel on which the AP is operating.
- **Auto Channel?** - Is automatic channel selection enabled on radio, Yes/No.
- **Tx Power** - Transmission power of the radio (0 to 8).
- **Tx Rate** - Data transmission rate in Mbps.
- **Beacon Rate** - Milliseconds between radio's beacon signal transmissions.
- Adjacent APs on Radio a and Radio b/g
 - **MAC** - MAC address of radio operating within range of the AP.
 - **SSID** - Service Set Identifier assigned to adjacent radio.
 - **RSSI** - Receive Signal Strength Indication calculated for adjacent AP.
 - **Beacon** - Beacon identifier broadcast by adjacent AP.
 - **Security** - Possible values are: Open system; Shared Key; WPA; WPA-PSK; WPA2; WPA2-PSK; WPA + WPA2; WPA-PSK + WPA2-PSK

Information presented on the stand alone AP summary page includes:

This page will [refresh](#) in 5 seconds.

Poll now

Status	
Status	Up
Name	ap-jm.bluesocket.com
Address	192.168.18.106
SSID	
Channel	0
Power	

Specifications	
MAC	00:08:21:31:4f:2b
Vendor	Cisco Systems AP350IOS
Firmware	Cisco AP IOS Version 12.2(15)JA
Type	Other
Location	
Security	0

Adjacent APs

MAC
Adjacent AP information unavailable






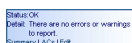
Figure 6-6: BlueView AP Summary Information (Single Stand Alone AP)


- Status
 - **Status** - Either "Up" (communicating with its home BSC) or "Down" (unreachable from the BSC). Status for a BSAP that has been configured on a BSC but has not yet connected to the BSC is listed as "No runtime data is known about this AP."
 - **Name** - Hostname assigned to this AP.

- **Address** - Configured IP address of the AP.
- **SSID** - Service Set Identifier assigned to the AP.
- **Channel** - Channel on which the AP's 802.11a and 802.11b/g radios are operating.
- **Power** - Configured transmission power level for the 802.11a and 802.11b/g radios.
- Specifications
 - **MAC** - AP media access control address.
 - **Vendor** - Vendor and model number of AP.
 - **Firmware** - Version number of the firmware running on the AP.
 - **Type** - Other= Stand Alone AP.
 - **Location** - Configured location of the AP.
 - **Security** - Configured security for the AP.
- Radio b/g and Radio a
 - **MAC** - Individual MAC address of 802.11a/802.11b/g radios.
 - **State** - Operating (1) or not operating (0).
 - **Associations** - Count of wireless clients associated to the radio.
 - **Adjacent APs** - APs operating within range of the AP.
 - **Channel** - Channel on which the AP is operating.
 - **Auto Channel?** - Is automatic channel selection enabled on the radio? Yes/No.
 - **Tx Power** - Transmission power of the radio (0 to 8).
 - **Tx Rate** - Data transmission rate in Mbps.
 - **Beacon Rate** - Interval at which radio's beacon signal is transmitted in milliseconds.
- Adjacent APs on Radio a and Radio b/g
 - **MAC** - MAC address of radio operating within range of the AP.
 - **SSID** - Service Set Identifier assigned to adjacent radio.
 - **RSSI** - Receive Signal Strength Indication calculated for adjacent AP and expressed as a percentage.
 - **Beacon** - Beacon identifier broadcast by adjacent AP.
 - **Security** - Configured security for the adjacent AP.

Status for APs connected to individual BSCs on your network is represented using the following icons in the navigation pane:

-  - The AP is up and configured by the BSC.
-  - The AP is up but has not been configured by the BSC. The AP's configuration may reside on the BSC, but the AP is connected elsewhere.
-  - The AP is down, i.e. unreachable from the BSC.



Pass the cursor over an individual AP link, , in the navigation pane to display a summary listing AP status and a brief description of that status. Links are provided to display the AP's summary and active connections information, and edit the AP's configuration.

Monitoring Your Protected Airspace

BlueView provides two informative displays for monitoring the airspace the covered by BSAPs operating in Sensor or Dual mode installed on your network:


- Displaying an RF Summary View - Display high-level statistics about the RF devices operating in your protected airspace in a graphical dashboard-style format.
- Displaying a Detailed RF View - Display detailed statistics about all of the RF devices operating in your protected airspace in a tabular format.

Displaying an RF Summary View


To display summary information about the RF devices operating within the coverage area of BSAPs operating in Sensor or Dual mode installed on your network:

1. Click **Status/Summary** from any Administrator Console page.

The Summary page appears.

2. Click on the  **RF Sensor Summary** link at the top of any summary page to display summary information for all of the RF devices operating within the coverage area of the BSAPs operating in Sensor or Dual mode installed on your network.

The RF summary information is displayed in the information pane as shown in Figure 6-7.

Alternatively, click on an individual BSAP operating in sensor mode link  in the navigation pane to display summary information for that sensor in a separate browser window.

The displayed RF summary information includes:

- **RF Stations** - The count of 802.11a, 802.11b, and 802.11g RF devices operating within range of your BSAPs operating in sensor or dual mode.
- **RF Network Inventory** - A count of the 802.11a/b/g RF station types operating within range of your BSAPs operating in sensor or dual mode. A device is classified as an AP, Client or Ad-hoc, and is further designated as one of the following: Unknown (Unk), Ignored (Ign), Rogue (Rog), Authorized (Aut), or Neighbor (Nei). Rogue devices are devices that are not in the authorized list. Ignored devices are those that are in the user configurable Ignore List. You can define the authorized RF stations on your network as described in "Identifying Authorized RF Stations on Your Network" on page 8-2.
- **Alarms View** - A concise visual summary of the eight alarms most frequently issued by the your BSAPs operating in sensor or dual mode on your network.
- **Top 5 Alarms** - A list of the five alarms most frequently issued by the BSAPs operating in sensor or dual mode.
- **Last 5 Alarms** - A list of the five most recent alarms issued by the BSAPs operating in sensor or dual mode.

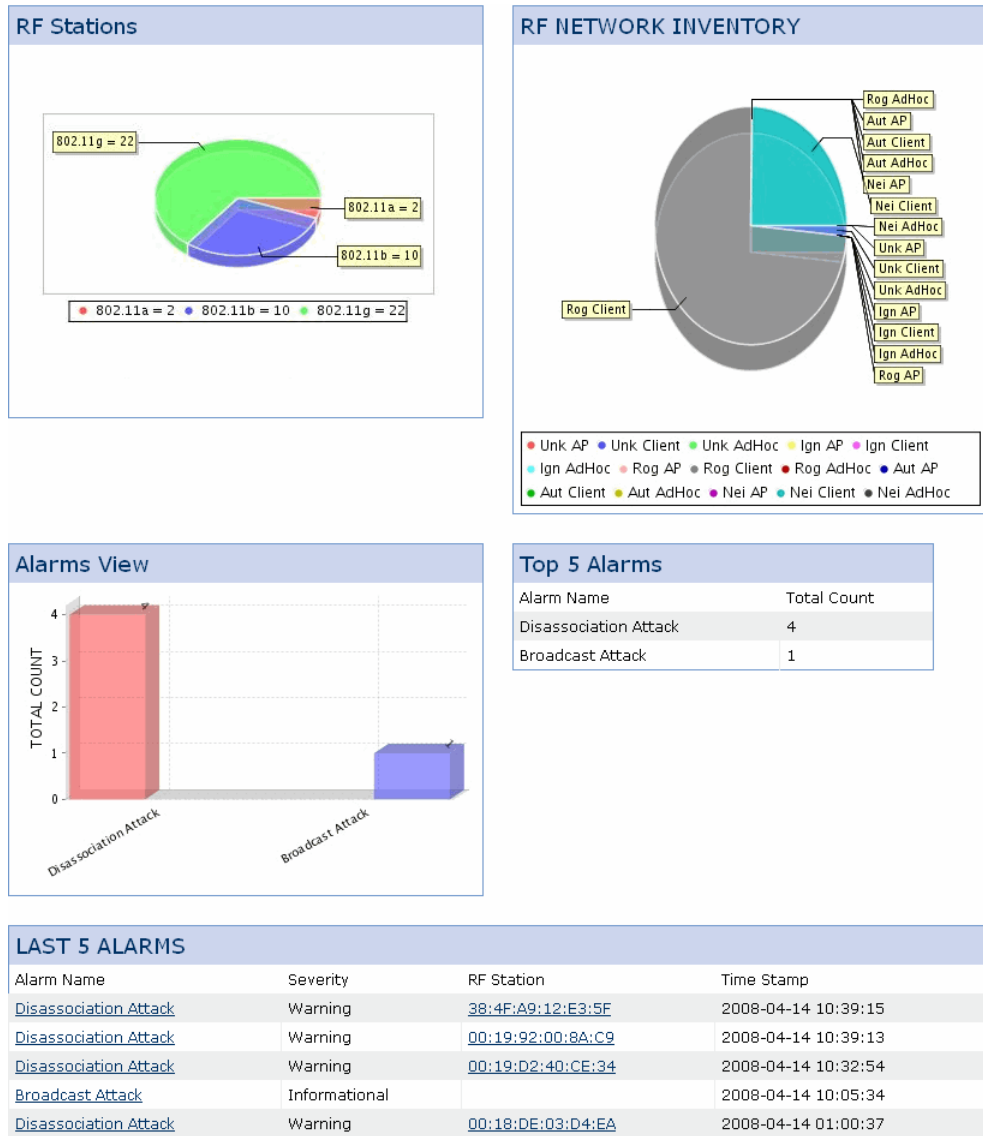


Figure 6-7: RF Summary Information

Displaying a Detailed RF View

Click **Status/RF View** from any Administrator Console page to list details about all of the RF devices operating within the coverage area of the BSAPs operating in Sensor or Dual mode installed on your network: The RF View page appears as shown in Figure 6-8.
























Type	MAC	SSID	Radio (a/b/g)	Channel	Signal	Packets Rx/Tx	Last Seen	un-sort customize
All	All	All	All	All	All		All	un-filter
	00:0E:0C:6C:2E:59	containme	802.11b/g	11		0	2006-06-06 13:00:05	
	00:0D:88:A5:03:38	waf	802.11b/g	11		49	2006-06-06 11:39:34	
	00:12:CF:0C:0D:E3	Guest	802.11a	165		87	2006-06-06 13:00:14	
	00:0E:0C:7F:80:BE	apengqtest	802.11b/g	6		2	2006-07-14 18:19:12	
	00:12:CF:0C:0D:E5	Eng	802.11a	165		111	2006-06-06 16:05:08	
	00:12:CF:0F:36:46	QA	802.11g	1		1	2006-06-27 21:08:07	
	00:12:CF:14:B4:06	QA	802.11g	11		424	2006-06-06 16:05:08	
	00:12:CF:14:B4:27	QA	802.11a	149		156	2006-06-06 13:00:14	
	00:0F:B5:3B:43:4C	apengqtest	802.11b/g	6		5	2006-07-14 18:20:00	
	00:12:CF:0F:36:4A	Picnic	802.11g	1		5	2006-06-27 21:08:10	

Figure 6-8: RF View

The RF View page lists the following information about each of the RF devices operating within the coverage area of the BSAPs operating in Sensor or Dual mode:

- **Type** - Icons are used to represent three general classes of RF devices.  icons represent access points,  icons represent wireless clients and  icons represent wireless clients operating in ad-hoc mode.
- **MAC** - Media Access Control address of device.
- **Station Name** - Hostname of detected wireless device.
- **SSID** - Service Set Identifier device is using, if any.
- **Sensor** - Name of the Sensor that detected the device.
- **Radio (a/b/g)** - 802.11 spectrum on which device was detected.
- **Channel** - Channel on which device was operating when was detected.
- **Signal** - Graphical representation of the device's relative signal strength. Hover the mouse over the graphic to display the detected signal strength.
- **Packets Rx/Tx** - Count of packets transmitted/received by the device.
- **Last Seen** - Date and time at which the device was last detected.

Click to purge all wireless device listings.

Click an RF device icon to display additional detailed information about that device as shown in Figure 6-9.

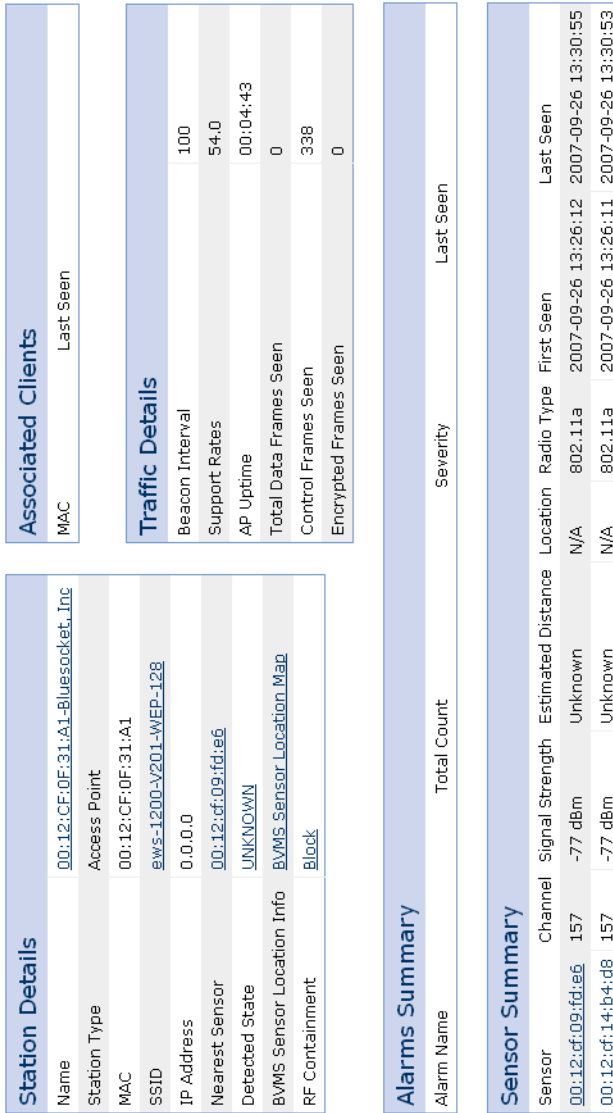



Figure 6-9: Detailed RF View

Detailed information displayed for access points includes: Station details, a list of clients associated to the access point, traffic details, alarm summary, and sensor summary. Additional device details are provided for wireless clients and clients operating in ad hoc mode.

Displaying a Location Map

Click the [BVMS Sensor Location Map](#) link within the detailed RF View to display a graphical representation of the location of the RF device relative to the RF Sensor from which it was detected as shown in Figure 6-10.

 **Note:** Before attempting to generate a location map for a wireless device, ensure that you have imported a floorplan and have properly positioned BSAPs operating in sensor mode on the floorplan.

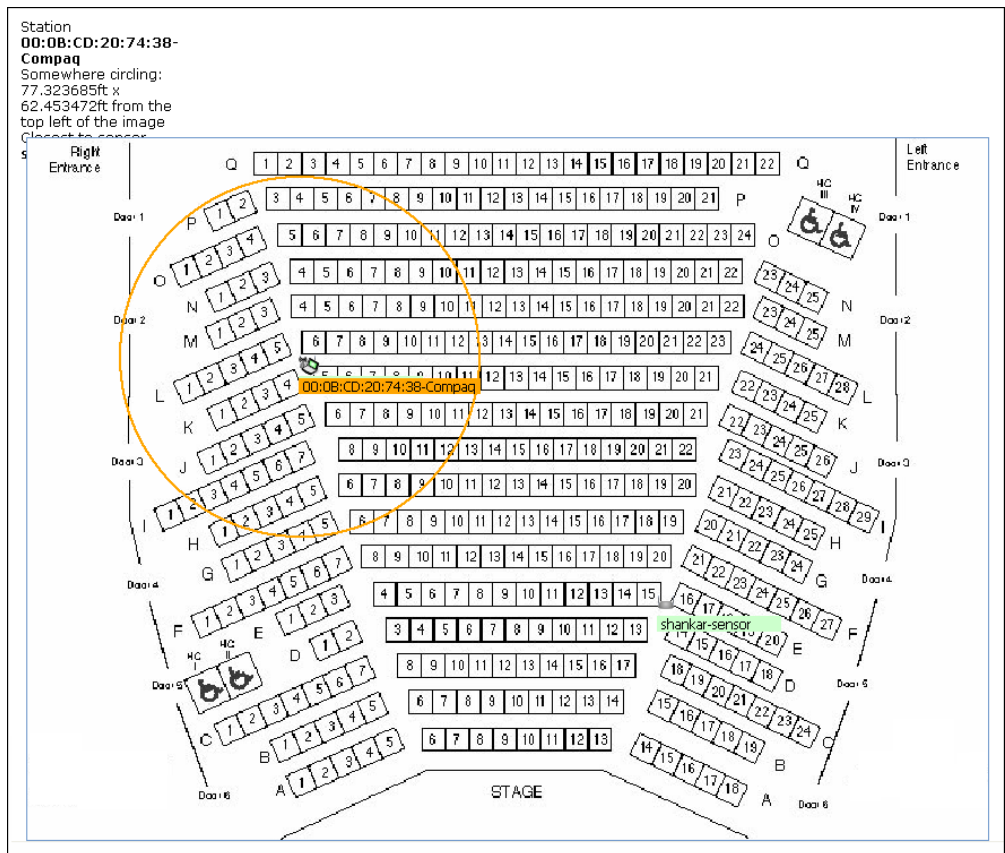


Figure 6-10: Sample Location Map

Blocking a Device

Click the [Block](#) link within the detailed RF View to place the detected wireless device in active RF containment. The device is now blocked from accessing the WLAN.

See “Monitoring Devices in RF Autocontainment” on page 6-34 for procedures to list all devices in active RF containment and selectively remove devices from active RF containment (i.e., unblock devices).

See “Configure RF Autocontainment” on page 8-6 for information about configuring the RF containment feature.


Monitoring Active User Connections

BlueView enables you to display and monitor active user connection status and other user information, such as IP address, assigned role, and throughput statistics, in both text and graphical formats.

The BlueSecure Controller provides an administrator-configurable Intrusion Detection System (IDS) to defend itself and the network it is protecting from intruders, worms, and


other targeted attacks. If you have configured the BSC IDS, you can also track the IDS status of each user connected to the BSC using BlueView:

- Displaying BSC Active Connection Status
- Displaying AP Associations

 **Note:** You must configure an active connection rate of other than 0 as part of a static group's configuration to enable active connection polling. See "Creating Static Groups" on page 3-15 for details.

Displaying BSC Active Connection Status

To view connection information for users logged onto a BSC:

Click **Status/Active Connections** from any Administrator Console page, and then click a BSC icon,  in the navigation pane.

The BSC Active Connections page appears as shown in Figure 6-11.



Figure 6-11: Active Connections Page

The Active Connections page displays the following information for each user actively connected to a BSC on your network:

- **Home** - The BSC to which the user is connected.
- **Name** - User's login name - brackets are used to indicate a static DHCP entry
- **Address** - IP address of the user's wireless device
- **Hostname** - Hostname of the user's wireless device
- **MAC address** - Hardware (MAC) address of the wireless device's NIC card
- **Role** - Role assigned to this connection
- **AP** - Access point to which user has associated
- **Authentication** - Authentication type (Local = BSC user database)
- **Current/Average Kbps** - Current/average user data traffic.
- **Bytes In/Bytes Out** - Current data throughput in bytes per second
- **Packets In/Packets Out** - Current packet throughput counts
- **IDS State** - IDS-designated state for user host. Possible states are: Normal, Pre-monitoring, Monitoring, and Blocked.

- **Packets Dropped** - Count of packets dropped due to blocked port(s).
- **Port N** - Count of packets dropped on this blocked port.
- **Start Time** - Start date and time of the connection session

Click to refresh the displayed information.

Note that In the Role column, a bold underlined role indicates a secure connection. Positioning the mouse pointer over the role indicates its secure connection type (i.e., IPsec, PPTP, or L2TP/IPsec).


Each active IPsec, PPTP, or L2TP/IPsec user is represented by two rows of information. The top row is the original connection and looks similar to other non-secure connections. The bottom row describes the secure tunnel connection. One asterisk (*) denotes the IP address of the secure tunnel. Two asterisks (**) denote a Transparent NTLM Windows login waiting for the secure tunnel to become active.

You can use column data filters to limit the display of active user connections to selected user Names, Roles, or session Start times within certain time periods such as Today or Last Month. Additionally, you can sort the displayed data by clicking a column heading link. The displayed data is sorted in ascending or descending order based on the data contained in the column. The Rows per page control restricts the number of rows displayed per page for easy viewing.

Brackets around a hostname indicate a fixed, i.e., static DHCP entries.


Forcing a User Logout

To log out a user and terminate their connection to the BSC:

1. Click **Status/Active Connections** from any Administrator Console page.
The Active Connections page appears as shown in Figure 6-11.
2. Click the  icon in the **Actions** column that corresponds to the user you wish to log out.
The BSC logs out the selected user and drops the user's connection.


Terminating a User's Secure Connection

To terminate a user's secure VPN connection to a BSC on your network without logging the user out:

1. Click **Status/Active Connections** from any Administrator Console page.
The Active Connections page appears as shown in Figure 6-11.
2. Click the  icon in the Actions column that corresponds to the user whose secure VPN connection you wish to terminate.
The BSC drops the selected user's VPN connection but does not log the user out.

Displaying Active Connection Details

To display active connection details for a specific user:

1. Click **Status/Active Connections** from any Administrator Console page.
The Active Connections page appears as shown in Figure 6-11.
2. Click the  icon in the Actions column that corresponds to the user for which you wish to display detailed information.

Additional detail, location, and traffic information is displayed as shown in Figure 6-12.

Detail	
Name	[00:12:cf:09:fd:c2]
Address	192.168.86.100
Hostname	my-bap
MAC	00:12:cf:09:fd:c2
Start Time	2005-10-21 18:29:40
Role	wide_open
Secure	
Authentication	


Location	
Group	Default
Device	192.168.100.144
AP	

Traffic	
Packets In/Out	0/0
Total Bytes	0
Bytes In/Out	0/0
Dropped Packets	0
IDS State	normal
Ports Blocked	0/0/0/0/0


Figure 6-12: Active Connection Details

Displaying AP Associations

To view connection information for wireless clients associated to a AP:

Click **Status/Active Connections** from any Administrator Console page, and then click a AP icon, , in the navigation pane.

The AP Active Connections page displays the following information for each wireless client actively connected to a AP on your network:

 **Note:** For third party APs, just the IP Address, MAC Address, Signal Strength, and Signal Quality is displayed.

- **Identifier** - Media Access Control address of associated wireless client.
- **RSSI** - Receive Signal Strength Indication calculated for wireless client expressed as a percentage.
- **Tx KB** - Count of bytes transmitted by wireless client.
- **Rx KB** - Count of bytes received by wireless client.
- **Tx KPkts** - Count of packets transmitted by wireless client (in thousands).
- **Rx Pkts** - Count of packets received by wireless client (in thousands).
- **Tx KB/s** - Transmission rate of wireless client expressed in KiloBytes per second.
- **Rx KB/s** - Receive rate of wireless client expressed in KiloBytes per second.
- **Tx Kerrors** - Count (in thousands) of transmission errors generated by wireless client.
- **Rx Kerrors** - Count (in thousands) of receive errors generated by wireless client.
- **Association Time** - Time (in seconds) has been associated to the AP.
- **Re-associations** - Number of times this client has re-associated to the AP.
- **Authenticated** - Is the client authenticated? Yes (1) or no (0).
- **VLAN** - Client's VLAN association.

Displaying BSC Logs

BlueView maintains a log database in non-volatile memory that serves as a central repository for log records received from managed BlueSecure Controllers.

Note: By default, the BSCs on your network are not configured to send log messages to BlueView. Follow the procedure given in “Configuring the BSCs on Your Network to Support BlueView” on page 3-2 to configure the BSCs on your network to send their log data to BlueView. Managed BSCs will automatically send their alarms to BlueView.

Click **Status/Logs** from any Administrator Console page and then click the **All BlueSecure Controllers** link in the navigation pane to display a BSC log summary for all BSCs on your network as shown in Figure 6-14.

Click Column Headings to Sort Logs

next > Page 1 Rows per page 10

#	Created	Source	Level	Application	Message	Un-Sort
	All	All	All	All	All	Un-Filter
147666	2005-03-04 15:05:22.0	192.168.0.210	info	wg_system	System_Performance cpu_load=1 disk_used=9 mei	
147665	2005-03-04 15:05:22.0	192.168.0.210	info	user_tracking	User_Counts total=0 logged_in=0 passing_traffic=	
147659	2005-03-04 15:05:07.0	192.168.0.23	info	wg_system	System_Performance cpu_load=2 disk_used=2 mei	
147658	2005-03-04 15:05:07.0	192.168.0.23	info	user_tracking	User_Counts total=8 logged_in=8 passing_traffic=	
147541	2005-03-04 15:03:33.0	192.168.0.211	info	wg_system	System_Performance cpu_load=31 disk_used=29 r0	
147540	2005-03-04 15:03:33.0	192.168.0.211	info	user_tracking	User_Counts total=7 logged_in=5 passing_traffic=	
147199	2005-03-04 15:00:22.0	192.168.0.210	info	wg_system	System_Performance cpu_load=4 disk_used=9 mei	
147198	2005-03-04 15:00:22.0	192.168.0.210	info	user_tracking	User_Counts total=0 logged_in=0 passing_traffic=	
147197	2005-03-04 15:00:08.0	192.168.0.23	info	wg_system	System_Performance cpu_load=3 disk_used=2 mei	
147196	2005-03-04 15:00:08.0	192.168.0.23	info	user_tracking	User_Counts total=8 logged_in=8 passing_traffic=	

10 rows on page Delete

3891 total rows

Purge all log records



next > Page 1 Rows per page 10

Click to Purge all Logs in Database

Select Log Filters from Drop-down Menus

Click to Delete Selected Records

Figure 6-13: BSC Log Summary


Click a BSC group icon, , to display logs received by BlueView from all BSCs in the group. Click an individual BSC icon, , to display only logs received from that BSC.

Log table entries include:

- **#** - incrementing counter of received log records
- **Created** - Date and time of the event.
- **Source** - IP address of the BSC that sent the log record to BlueView.
- **Level** - Type of event message. Warning and Error messages signal possible system malfunctions. Emergency and Critical indicate potentially more serious failures. Notice and Info messages display higher level events such as user login/logout times or the addition or modification of user information.
- **Application** - BSC application that generated the event, such as Database, DHCP Server, or PPTP Tunneling.
- **Message** - Description of the event, such as Login admin user #1 Full access at 208.192.100.113 as role #0.

Displaying BSC Alarms

BlueView serves as an SNMP trap receiver for all managed BSCs on the network. BlueView intelligently interprets received traps and generates a sortable and filterable alarm table for administrator review.

Click **Status/Alarms** from any Administrator Console page and then click the  **All BlueSecure Controllers** link in the navigation pane to display a BSC alarm summary for all BSCs installed on your network as shown in Figure 6-14.

Click Column Headings to Sort Select Filters next > Page 1 Rows per page 10



#	Ack	Created	Source	Level	Application	Message	Un-Sort	Un-Filter
<input type="checkbox"/>	All	All	All	All	All			
<input type="checkbox"/> 147666	N	2005-03-04 15:05:22.0	192.168.0.210	alert	btLinkDown	Managed interface link down.		
<input type="checkbox"/> 147665	N	2005-03-04 15:05:22.0	192.168.0.210	alert	btLinkUp	e100: eth1 NIC Link is Up 100 Mb		
<input type="checkbox"/> 147659	N	2005-03-04 15:05:07.0	192.168.0.23	alert	btLinkDown	e100: eth1 NIC Link is Down		
<input type="checkbox"/> 147658	N	2005-03-04 15:05:07.0	192.168.0.23	alert	btLinkUp	e100: eth1 NIC Link is Up 100 Mb		
<input type="checkbox"/> 147541	N	2005-03-04 15:03:33.0	192.168.0.211	alert	btLinkUp	e100: eth1 NIC Link is Up 100 Mb		
<input type="checkbox"/> 147540	N	2005-03-04 15:03:33.0	192.168.0.211	alert	btLinkDown	e100: eth1 NIC Link is Down		
<input type="checkbox"/> 147199	N	2005-03-04 15:00:22.0	192.168.0.210	alert	btLinkUp	e100: eth1 NIC Link is Up 100 Mb		
<input type="checkbox"/> 147198	N	2005-03-04 15:00:22.0	192.168.0.210	alert	btLinkDown	e100: eth1 NIC Link is Down		
<input type="checkbox"/> 147197	N	2005-03-04 15:00:08.0	192.168.0.23	alert	btLinkUp	e100: eth1 NIC Link is Up 100 Mb		
<input type="checkbox"/> 147196	N	2005-03-04 15:00:08.0	192.168.0.23	alert	btLinkDown	e100: eth1 NIC Link is Down		

Check All | Clear All Acknowledge

Purge all alarm records next > Page 1 Rows per page 10

Click to Purge all Alarms in Database Click to Acknowledge Checked Alarms

Figure 6-14: BSC Alarm Summary































Click a BSC group icon, , to display alarms received by BlueView from all BSCs in the group. Click an individual BSC icon, , to display only alarms received from that BSC.

Alarm table entries include:

- **#** - incrementing counter of received alarm records
- **Ack** - Y, Yes the alarm has been acknowledged or N, No, the alarm has not been acknowledged at the administrator console.
- **Created** - Date and time BlueView created the alarm record in its database.
- **Source** - IP address of BSC that sent the alarm to BlueView.
- **Level** - Alarm severity. Possible values include: critical, error, warning, and informational.
- **Type** - Alarm type. Possible values include: cold start, warm start, link up/down, enterprise message.
- **Message** - Alarm description as generated by the BSC.

Displaying Sensor Alarms

Click **Status/Alarms**, and then click the  **All RF Sensors** link in the navigation pane from any Administrator Console page to list the alarms received from BSAPs operating in Sensor Mode installed on your network. The Alarms page appears (see Figure 6-1).

<input type="checkbox"/>	Name	Severity	Time Stamp	Device	Sensor IP	Status	Note	Un-Sort
<input type="checkbox"/>	 Network Probe	Informational	2005-07-14 08:49:39.0	(00:0F:20:E2:F7:C)	192.168.100.150			
<input type="checkbox"/>	 AP Channel Change	Warning	2005-07-14 09:15:08.0	(00:0F:20:E2:F7:C)	192.168.100.150			
<input type="checkbox"/>	 Network Probe	Informational	2005-07-14 09:19:46.0	(00:0F:20:E2:F7:C)	192.168.100.150			
<input type="checkbox"/>	 Network Probe	Informational	2005-07-14 09:17:42.0	(00:0F:B5:94:34:2)	192.168.100.150			
<input type="checkbox"/>	 Network Probe	Informational	2005-07-14 09:20:14.0	(00:0E:6A:D7:46:8)	192.168.100.150			
<input type="checkbox"/>	 Network Probe	Informational	2005-07-14 09:19:55.0	(00:0F:B5:60:38:6)	192.168.100.150			
<input type="checkbox"/>	 AP Channel Change	Warning	1980-04-14 05:32:19.0	(00:0F:B5:60:38:6)	192.168.100.150			
<input type="checkbox"/>	 Network Probe	Informational	1980-04-14 05:32:20.0	(00:0F:B5:94:34:2)	192.168.100.150			
<input type="checkbox"/>	 Network Probe	Informational	2005-07-13 16:28:45.0	(00:0E:6A:D7:46:8)	192.168.100.150			
<input type="checkbox"/>	 Network Probe	Informational	1980-04-14 05:33:25.0	(00:0E:6A:D7:47:9)	192.168.100.150			







|

10 rows on page
55 total rows

Figure 6-15: Received RF Sensor Alarms

The received alarms are listed with any configuration settings you may have applied to them as described in “Configuring Sensor Alarms and RF Autocontainment” on page 8-3.

The following information is provided about received alarms:

- **Icon** - Icons are used to represent the configured severity level for the alarm.  icons represent informational alarms,  icons represent warning alarms and  icons represent severe alarms.
- **Name** - Name of WLAN vulnerability responsible for alarm.
- **Severity** - The configured severity level for the alarm:
 - Severe - This is the highest alert level and is usually associated with a WLAN intrusion, e.g., a broadcast attack.
 - Warning - This alert level is usually associated with a security vulnerability, e.g., a client association change.
 - Informational - This alert level is usually associated with a change in network operational status, e.g., an authorized AP is down.
- **Time Stamp** - The date and time the alarm was received.
- **Device** - MAC address of RF device associated with alarm.
- **Sensor IP** - IP address of BSAP that issued the alarm.
- **Status** - Alarm status,  acknowledged or  unacknowledged.
- **Note** - Click the note icon, , to enter a notation about the alarm for future reference.

Click on a column heading to sort the list of received alarms. Click to acknowledge the selected alarm(s), click to unacknowledge the selected alarm(s), and to delete the selected alarm(s).


Generating Status Reports

BlueView enables you to generate and display status reports on the Bluesocket devices on your network. Specifically, BlueView enables you to generate reports detailing:

- inventory - Inventory reports list and describe the Bluesocket devices on your entire network or within a specified device group. Inventory reports provide device counts, IP addresses, model numbers, and system software versions.
- user - User reports detail user activity over a specified period of time for the Bluesocket devices on your entire network or within a specified device group.
- sensor - Sensor reports detail RF activity/events detected by BSAP 1500/1540s operating in sensor mode installed on your network.

You may display and save generated reports in HTML, Adobe Acrobat (.pdf), and Microsoft Excel (.xls) formats.

Additionally, you may create a job to send a generated report to an individual via email. Refer to "Sending a BlueView Report via Email" on page 7-23 for details.

 **Note:** For the reports to generate, you should add the BVMS as your syslog server to each managed BSC (also include the Active Connection Syslog). On the BVMS side, you should enable all four polls.

To generate a status report:

1. Click **Status/Reports** from any Administrator Console page.

If no reports have been previously generated, the Report page appears as shown in Figure 6-16.



Figure 6-16: Report Page

If one or more reports have been generated previously, then you must click to add a new report to the table of generated reports before the Report page appears.

2. Enter a meaningful name for the report in the **Name** field.
3. Select the type of status report to generate from the **Report Type** drop-down menu:

Table 6-1: Status Reports

Report	Description
Controller Inventory	A table of all the devices per Group (or all groups) with the following information: Device, hostname, model, software version, software version in the alternative partition, number of users associated to the BSC, number of logged users, number of APs connected to this BSC, the CPU usage, and list of patches on the BSC running version. In multiple CPU environment report includes both CPU values. This report needs to have polling enabled. There are also two pie charts: the distribution of models controlled by the BVMS; and the distribution of software in the BSCs controlled by the BVMS.
Controller Bandwidth over Time	A chart with the total bandwidth (per time period (days, hours, etc) in the time period specified. This report needs to have polling enabled. This report can be customized as all Groups, one specific Group or one specific BSC.
System Performance over Time	A set of tables and graphs (CPU Average usage and disk average usage) that display the BSC system performance over time. To accommodate large amounts of data, the data is grouped in sets up to 4 BSCs. In each set of data, 1 table and 2 graphs are displayed. Only one set of data is displayed per page. The table contains the device name, the IP, the minimum CPU Usage, the Maximum CPU Usage, the Minimum Disk Usage and the Maximum Disk Usage. Graph 1 displays the Average CPU usage (as a percentage) over time (for up to 4 BSCs). Graph 2 displays the Average Disk Usage (as a percentage) over time (for up to 4 BSCs). This report needs to have polling enabled.
AP Inventory	Displays a table and 2 pie charts. The report can be customized per Group (or all groups), or a specific BSC. The tables are organized by groups, and the entries are APs in each group, grouped by controller. Each table displays the APs Mac address, Name, IP Address, Vendor, Model, and Location, as well as information about the firmware. Graph 1 displays the model types in a pie chart. Graph 2 displays the firmware software in a pie chart. This report needs to have polling enabled.
AP Bandwidth over Time	A graph of the total AP bandwidth over time. This report needs to have polling enabled.
AP Users over Time	A graph with the total number of users connected to the APs over time. It can be customized as per group (or all groups), a specific controller or a specific AP.
Unique Users Per SSID	A table and a graph per page. Each page contains up to 8 SSIDs. The table displays the following data: the SSID, the number of users connected to that SSID, if this SSID is enabled by default on the BG radio, if this SSID is enabled by default on the A radio, the VLAN it corresponds to, if the SSID is broadcasted or not, the type of authentication and the cipher used in the SSID. The bar graph displays the number of users authenticated in each SSID.
Coverage	The coverage of the APs in a map. The user needs to create in Status/Maps one entry with the map of the building and place the APs in that map. This report will display 4 graphs per floor: The current BG coverage, the current A Coverage, the pre-configured BG coverage, and the pre-configured A coverage.
Users over Time	Displays a graph with the number of users (could be either authenticated or not) over time. Can customize the data to be all groups, one specific group or one specific BSC.
Users Summary	A table with the following data: Device, User-Name, how many times the user connected to the BSC, how long the user stayed connected to the BSC, the total bytes received and the total bytes sent. At the end of the report is displayed the total of each of the previous quantities and the average of these quantities by user and by day. This report requires the user to send the syslog messages from the BSC (they need to add the BVMS to the syslog server).

Table 6-1: Status Reports

Report	Description
Users Association Summary	<p>This report has 5 varieties. They all display the same data, the only difference is how the data is grouped:</p> <p>Group - This report displays the users connected to a specific Group of BSCs. The Group (or Groups) could be selected from a Group, a Device or just a specific AP. For each user we display the hostname, MAC address, the IP address, the role, the SSID, the Current Kbps and Average Kbps. A graph shows the number of users connected to each Group.</p> <p>Device - This report displays the users connected to a specific Device (BSC). The BSC (or BSCs) could be selected from a Group, a Device or just a specific AP. For each user we display the hostname, MAC address, the IP address, the role, the SSID and the Current Kbps and Average Kbps. A graph shows the number of users connected to each BSC.</p> <p>AP - This report displays the users connected to a specific AP. The AP (or APs) could be selected from a Group, a Device or just a specific AP. For each user we display the hostname, MAC address, the IP address, the role, the SSID and the Current Kbps and Average Kbps. A graph shows the number of users connected to each AP.</p> <p>Role - This report displays the users connected to a specific Role. The Role (or Roles) could be selected from a Group, a Device or just a specific AP. For each user we display the hostname, MAC address, the IP address, the role, the SSID and the Current Kbps and Average Kbps. A graph shows the number of users connected to each Role.</p> <p>SSID - This report displays the users connected to a specific SSID. The SSID (or SSIDs) could be selected from a Group, a Device or just a specific AP. For each user we display the hostname, MAC address, the IP address, the role, the SSID and the Current Kbps and Average Kbps. A graph shows the number of users connected to each SSID.</p>
Total User Logins over Time	A bar chart that displays how many uses logged in on a specific date. This report requires that the BSC sends syslog information, specifically the log out message.
RF AP Inventory	A list of all the APs inventory that the collector detects in the vicinity. The table includes the following data: Mac Address, the manufacturer of the device, the SSID that is broadcasting the AP, which sensor detected it, the channel it is broadcasting, the state and the number of clients connected to it.
RF Client Inventory	This report displays a list of all the clients that the collector detects in the vicinity. The table includes the following data: MAC address, manufacturer of the wireless card, the SSID it is connected to, which sensor detected it, the channel it is broadcasting, the state and to which access point it is connected to.
RF IDS Alarm Summary	A list of all the alarms detected (the alarms have to be enabled under Status/RF Alarms). The table includes the alarm type, how many times the alarm occurred, the sensor that detected that type of alarm, and the severity of the alarm.

4. If you select either RF AP Inventory or RF Client Inventory, mark one or more of the **Station State** checkboxes to include just stations in those states in the Inventory report.
5. Specify whether the report is to apply to all Bluesocket devices on your network or to a specific group by selecting from the **Device Group** menu.
6. If you select any report other than Coverage and Controller Inventory, you can mark the checkbox next to Specific Controller or Specific AP and then select a Controller or AP from the drop down list.

Note: Three reports (RF IDS Alarm Summary, RF AP Inventory, and RF Client Inventory) allow selection of a specific AP. If the user selects an AP that is not in sensor mode, the report will contain no data. If the user selects an AP that is a Stand Alone AP, the report will indicate that Stand Alone AP's are not supported.
7. **Reporting interval** – Date and time span of data records to include in the report. Typically, you will want to set up recurring reports that are automatically delivered. To do this, select one of the following options from the Time Period drop down: Today, Yesterday, This Week, Last Week, This Month, Last Month, or This Year. The schedule for recurrent delivery is as follows:
 - Today / Yesterday: Deliver the report every day after midnight.
 - This week / Last week: Deliver the report Saturday night after midnight.
 - This month / Last month: Deliver the report the first day of the month after midnight.
 - This year: Deliver the report the first day of the year after midnight.

Alternatively, you can generate a report for a specific time period. To do so, select **Specific Time Period** from the drop down and then indicate the **Start Time** and **End Time**. The ending date and time you select is also the date/time that the report is automatically delivered via the selected delivery options

8. Optional. Enter a report description in the **Notes** field.
9. Click **Save** to save the report data to the BlueView database.
Clicking **Save and create another** stores the report data to the BlueView database and enables you to continue creating reports.

Displaying and Saving Status Reports

To display and save status reports, click **Status/Reports**. If no reports have been previously generated, the Report page appears as shown in Figure 6-16. If a report has been generated, then the Generated Reports page appears as shown in Figure 6-17.

Actions	Name	Type	Group	un-sort customize
<input type="checkbox"/>				
<input type="checkbox"/>	Boston Devices	Inventory	Boston	
<input type="checkbox"/>	January User Activity	User	All	
Check All Clear All				<input type="button" value="Delete"/>
2 rows				

Figure 6-17: Generated Reports Page

Information on generated reports includes:

- **Name** - The administrator-assigned name of the report.
- **Type** - The report type, inventory or user.
- **Group** - The device group to which the report applies, all groups or a specific device group.

You may manage the reports listed on the Generated Reports as follows:

- Click to edit the corresponding report. Refer to the section entitled “Generating Status Reports” on page 6-24 when editing a report.
- Click to delete the corresponding report.
- Click to define a job to email the corresponding report as described in “Sending a BlueView Report via Email” on page 7-23.
- Click to display or save the corresponding report in HTML format.
- Click to display or save the corresponding report in Adobe Acrobat (.pdf) format.
- Click to display or save the corresponding report in Microsoft Excel (.xls) format.

Generating and Displaying RF Heat Maps

BlueView enables you to manage BlueSecure Access Points on your wireless networks. As an administrator, you need to know where to locate and how to configure these access points within your premises to provide optimal RF coverage with adequate signal strength for all wireless user space.

To assist you with these tasks, BlueView enables you to create RF “heat maps” (RF coverage maps):

- Sample Heat Map
- Importing Floor Plans
- Generating RF Heat Maps
 - General Procedure
 - Calibrating Heat Map Dimensions

Sample Heat Map

A heat map is created from imported floor plans of buildings in which you have installed or plan to install WLANs secured and managed with Bluesocket devices.

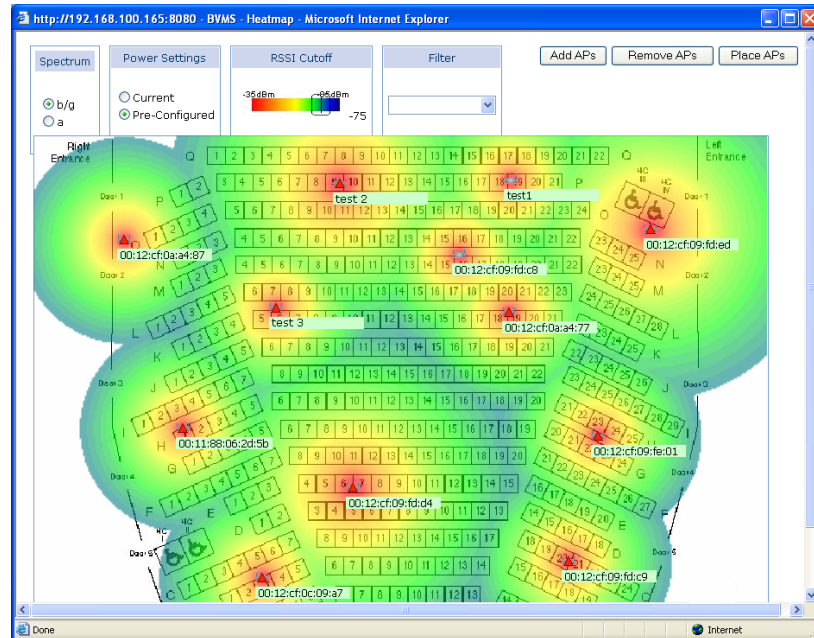


Figure 6-18: Sample RF Heat Map

Importing Floor Plans

The first step in generating an RF heat map is to import a floor plan of the area for which you wish to determine optimal RF coverage. If you plan to or already have installed WLANs in a multi-story building, you should import a floor plan for each floor on which a WLAN is planned or installed.

The imported floor plan must be in a Portable Network Graphic (.png), Joint Photographic Experts Group (.jpg), or CompuServe Graphics Interchange (.gif) file format.

You should also know the dimensions of the area represented by the floor plan. If the area dimensions are not known to you, then you should measure the distance between two objects represented in the floor plan. BlueView can calculate the represented area dimensions using this known calibration value.

To import a floor plan from which to generate an RF heat map:

1. Click **Status/Maps** from any Administrator Console page.
A list of previously generated RF heat maps appears.

2. Click to add a new RF heat map to the list.
The Create New Map Location page appears as shown in Figure 6-19.

Figure 6-19: Map Configuration Page

3. Enter a meaningful name for the Building for which you will be importing floor plans in the **Name** field.
4. Specify the number of floors in the building by selecting a value from the **Initial number of floors** drop-down menu.
5. Click **Browse...** and select the floor plan image file to import.
Again, the imported floor plan must be in either a .gif, .jpg, or .png file format. Initially, BlueView will use the first floorplan you import for all floors in the building. You can later edit the maps associated with each floor to import a custom floorplan for each floor if applicable.
6. Characterize the environment of the area represented by the imported floor plan by marking the appropriate radio button:
 - **Open Space**
 - **Cubicles**
 - **Cubicles and Interior Office Walls**
 - **Interior Office Walls**

The more accurately you characterize the environment of the space for which you are supplying RF coverage, the more accurate your heat map will be.

7. Specify the known dimensions of the area represented by the floor plan.
 - a) Mark the radio button indicating the map units, **FEET** or **METERS**.
 - b) Enter width of the floor plan in the **Width** field.
The width of the floor plan is the distance from the left to the right edge of the image as the floor plan image is displayed on your computer screen.
 - c) Optional. If your floor plan image is to scale, mark the **Keep the Image Ratio** checkbox to enable BlueView to automatically calculate the height dimension of the floor plan based on the entered width value.
 - d) Enter height of the floor plan in the **Height** field.
The height of the floor plan is the distance represented from the top edge of the image to the bottom edge of the image as the floor plan image is displayed on your computer screen.
8. Optional. If you don't know the dimensions of the area represented by the floor plan image, then mark the **Calibrate dimensions on screen** checkbox.
The first time you generate the RF heat map, you will be prompted to enter a known calibration distance. BlueView's map calibration function is described in "Calibrating Heat Map Dimensions" on page 6-33.
9. Optional. Add any meaningful notes or descriptions about the RF heat map in the **Notes** field.
10. Click **Save** to save the RF heat map to the BlueView database.
The added map is listed on the Maps page as shown in Figure 6-20.












Actions	Building	Floor	Floor Image	Dimensions	AP Count	Sensor Count	customize
<input type="checkbox"/>							
<input type="checkbox"/>    	Library						
<input type="checkbox"/>   		Floor 1	libraryfloorone.jpg	300' x 236'	0	0	
Check All Clear All							<input type="button" value="Delete"/>
1 row							

Figure 6-20: RF Heat Maps List


Click the  icon to edit the corresponding RF heat map, click the  icon to delete the corresponding RF heat map, or click the  icon to generate the corresponding RF heat map. Click the  icon to add another floor to a building and then import a floorplan for that floor.

Generating RF heat maps is described in the next section.

Generating RF Heat Maps

General Procedure

To generate an RF heat map from an imported floor plan:

1. Click **Status/Maps** from any administrator console page.
A list of RF heat maps appears as shown in Figure 6-20.
2. Click the  icon corresponding to the RF heat map you wish to generate.
The selected RF heat map is displayed as shown in Figure 6-21.

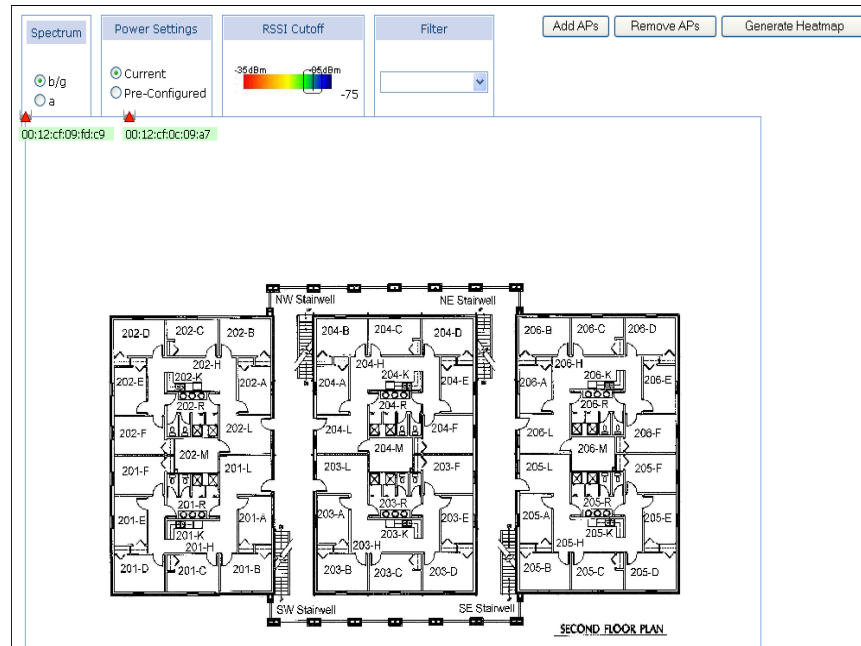


Figure 6-21: RF Heat Map: Initial Display

Note that the BlueSecure Access Points that you added to the RF heat map when you imported the floor plan are displayed at the top of the map.

3. Specify the RF spectrum to display on the generated RF heat map:
 - **b/g** - Display only BSAPs operating in the 802.11b or g (2.4 GHz) RF spectrum.
 - **a** - Display only BSAPs operating in the 802.11a (5 GHz) RF spectrum.
4. Specify the access point power settings to use when generating the RF heat map:
 - **Current** - Generate the RF heat map based on the power settings of access points that have downloaded their configurations from BlueSecure Controllers.
 - **Pre-Configured** - Generate the RF heat map based on the access points' default power settings. This selection may be useful when you are planning the layout of a WLAN but have not fully configured all access points.
5. Specify the **Receive Signal Strength Indication Cut Off** value by dragging the slide control to the appropriate setting.
This value sets the weakest signal strength to display on the RF heat map. The default setting is -75 dBm.
6. Optional. Filter the RF heat map to display only those APs corresponding to the item (SSID or radio channel) selected from the **Filter** drop-down menu.

7. Click **Add APs** to add BSAPs to the RF Heat Map.
8. Optional. Click **Remove APs** to remove BlueSecure Access Points from the RF Heat Map.
9. Drag the access point icons to their possible installation locations on the floor plan, and then click **Generate Heatmap**.

The generated heat map is displayed as shown in Figure 6-22.

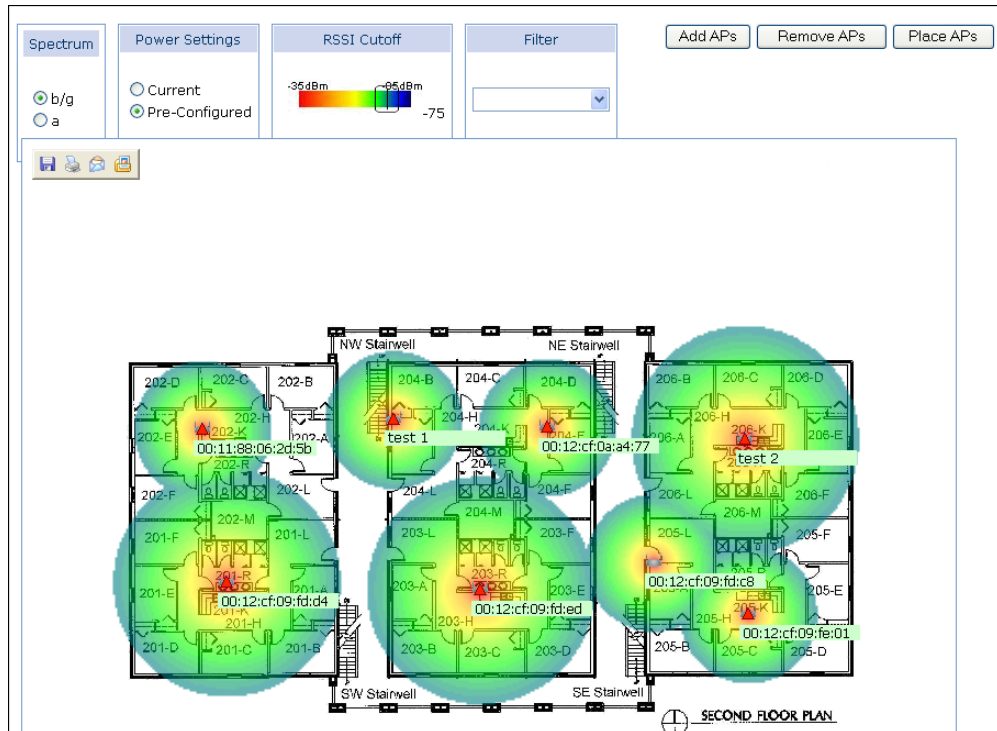


Figure 6-22: Generated RF Heat Map Display

Any movement of the AP icons or change to the spectrum, power, RSSI Cutoff, or filter settings will result in the heat map being redrawn automatically.

If you wish to relocate multiple APs on the map, click **Place APs**, move the AP icons to their new locations, and then click **Generate Heatmap**.

RF signal strength is represented on the heat map using the following colors:



Table 6-2:

Signal Strength (dBm)	Color
-35 or greater	Red
-50	Orange
-60	Yellow
-70	Green
-80	Blue
-85	Dark Blue
Less than -85	Clear

Calibrating Heat Map Dimensions

If you enabled the **Calibrate dimensions on screen** option when you imported a floor plan, then you are prompted to enter a dimensions calibration value the first time you attempt to generate a heat map using that floor plan.

To calibrate heat map dimensions:

1. Click **Status/Maps** from any administrator console page.
A list of RF heat maps appears (see Figure 6-20).
2. Click the  icon corresponding to the RF heat map you wish to generate.
3. If you have not entered dimensions for the floor plan, you will be prompted to entered a calibration value as shown in Figure 6-23.
4. Drag and drop each of the calibration points, , onto objects represented in the floor plan.
5. Enter the distance between the two objects marked with the calibration points in the **Distance between two points** field.
6. Mark the **FEET** or **METERS**, corresponding to the entered distance.
7. Click **Calibrate**.

BlueView calculates the width and height dimensions of the imported floor plan, and then displays the scaled floor plan as a background on which to place your BlueSecure Access Points.

Continue with step three of the procedure presented in “Calibrating Heat Map Dimensions” on page 6-33 to generate the heat map.

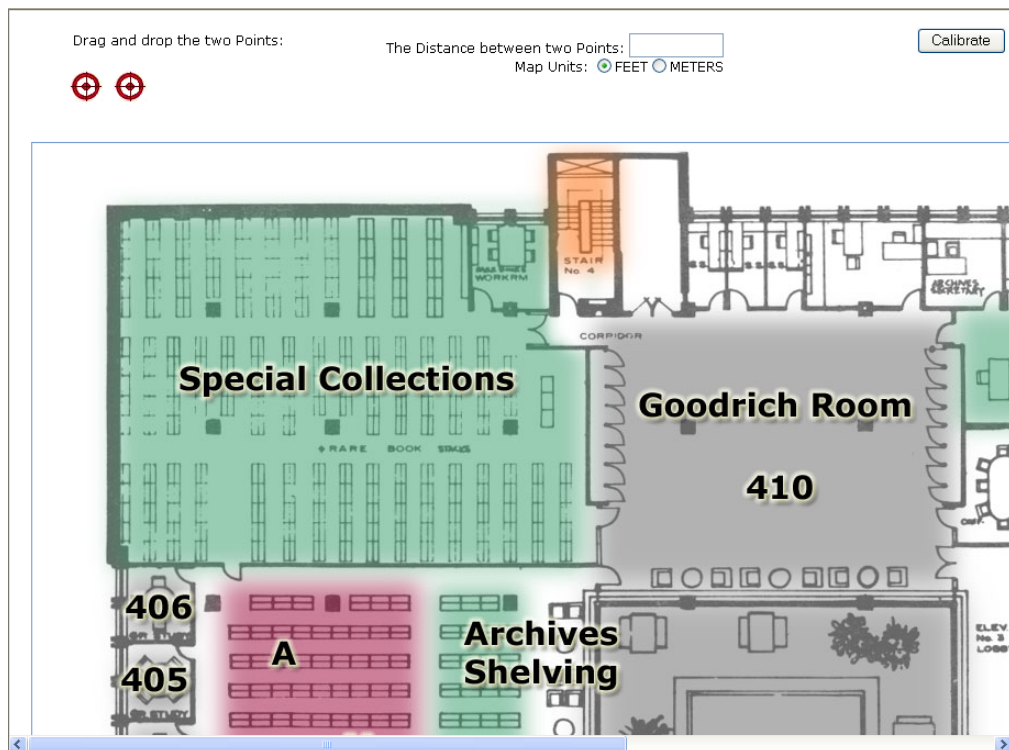


Figure 6-23: Entering a Dimensions Calibration Value

Monitoring Devices in RF Autocontainment

Click the **Status/Contained Devices** from any administrator console window to list the rogue wireless devices that are in active RF containment by or that were previously in containment. The Contained Devices page appears as shown in Figure 6-24.

	Device Mac	Containment Start Time	Duration (min)	customize
<input type="checkbox"/>				
<input type="checkbox"/>	00:07:E9:1A:FA:68	2005-12-02 15:49:40.0	5	

[Check All](#) | [Clear All](#)

1 row

Figure 6-24: Contained Devices Page

The following information is provided about contained devices:

- **Device MAC** - MAC address of contained RF device.
- **Containment Start Time** - The date and time that the BSC initiated containment on the device.
- **Duration** - Period of time device was in RF containment.

To remove a device from active RF containment, mark the device's corresponding checkbox, and then click .

See "Blocking a Device" on page 6-17 for procedures to place a device in active RF containment manually.

See "Configure RF Autocontainment" on page 8-6 for information about configuring the RF containment feature.

7

Maintaining and Provisioning WLAN Devices

BlueView enables you to run jobs to maintain and provision the Bluesocket devices and stand alone APs on your network. This chapter provides procedures for maintaining and provisioning network devices and includes:

- Maintaining and Provisioning Your Bluesocket Devices
- Creating Job Elements
- Editing a BSC Configuration Template
- Running Jobs on BlueView
- Reviewing Pending Jobs
- Reviewing Job History
- Managing BSAP Configurations
- Managing BSAP SSIDs

Maintaining and Provisioning Your Bluesocket Devices

BlueView simplifies the administration of your WLANs by providing you the ability to schedule and run jobs to complete the following BlueSecure Controller and BlueSecure Access Point maintenance and provisioning tasks from a single location:

- restart all BSC services
- reboot BSCs
- shutdown BSCs
- back up a BSC configuration
- restore a BSC configuration
- push a configuration template out to BSCs
- upgrade BSCs, BSAPs, or stand alone APs with new firmware
- switch BSC runtime images
- install a new BSC system software patch
- remove a BSC system software patch

As a prerequisite for four of these jobs, restoring a BSC configuration, pushing out a BSC configuration template, upgrading BSCs, BSAPs, or stand alone APs with new firmware, and installing a new system software patch, you must upload BSC, BSAP, or stand alone AP software to BlueView (i.e., create a job element) before running the job.

Creating job elements is described in the next section.

Creating Job Elements

You must upload software to your BlueView Management System before you can execute the following jobs:

- restoring a BSC configuration
- upgrading BSCs, BSAPs, or stand alone APs with new firmware
- installing a new BSC system software patch

Additionally, before you push out a BSC configuration template, you must generate the template from an uploaded BSC configuration file.

Follow the procedures given in this section to create the job elements required to complete the four BSC maintenance and provisioning jobs listed above:

“Uploading BSC Configuration Files to BlueView” on page 7-2.

“Uploading BSC Image Files to BlueView” on page 7-3.

“Uploading BSAP Image Files to BlueView” on page 7-4.

“Uploading Stand Alone AP Image Files to BlueView” on page 7-5.

“Uploading BSC Patch Files to BlueView” on page 7-6.

“Generating a BSC Configuration Template” on page 7-6.

Uploading BSC Configuration Files to BlueView

Follow these steps to upload a BSC configuration file to BlueView:

1. Click **Jobs/Job Elements** from any Administrator Console page, and then click **Controller Configurations** in the navigation pane.

The Configurations page appears as shown in Figure 7-1.

2. Mark the **Import a new device backup?** checkbox.

- The **Backup File** field appears.
- Enter the pathname of the BSC configuration file you wish to upload to BlueView in the **Backup File** field.
You may search for the BSC configuration file to upload by clicking **Browse**.
Note that by default, BSC configuration files have a .blue file extension.
 - Click **Import** to upload the specified configuration file.
Upon completion of the configuration file upload, the file is added to the configurations listed on the Configurations page.

Import a new device backup?

Max Number of Non Preserved Configurations per Host
Max number of Non Preserved Configurations per Host is (0 means no limit): 0
To change the Max number of Configurations Preserved, go to: [Change Max Configs](#)

Actions	Preserve	Product	Version	Version Creation Date	Hostname	Admin	Backup Creation Date
<input type="checkbox"/>							
<input type="checkbox"/>	No	BSC-1100	V5.1.0.1	2005-10-20 02:35:33	192.168.100.161	API	2005-01-31 07:18:29
<input type="checkbox"/>	No	BSC-5000	V5.0.0.5A	2005-06-29 15:51:06	192.168.103.22	admin	2005-01-05 09:57:55
<input type="checkbox"/>	No	WG-2100	V4.0.0.2	2003-11-21 12:09:41	192.168.168.37	admin	2005-01-07 17:43:45
<input type="checkbox"/>	No	WG-1000	V4.1.0.9A	2005-02-18 00:30:51	192.168.100.144	moe	2005-01-25 09:11:30
<input type="checkbox"/>	No	BSC-1000	V5.1.0.1	2005-10-19 02:23:00	192.168.100.144	API	2005-01-31 12:23:44
<input type="checkbox"/>	No	BSC-2000	V5.0.0.11	2005-08-12 02:20:53	192.168.100.135	API	2005-01-31 12:22:11
<input type="checkbox"/>	No	BSC-2000	V5.0.0.6	2005-07-12 02:14:32	192.168.100.135	admin	2005-01-12 15:49:47
<input type="checkbox"/>	No	BSC-2000	V5.1.1.1	2006-02-08 08:16:16	192.168.100.135	API	2006-01-07 10:37:42

Check All | Clear All | | | |

8 rows [download](#)

Figure 7-1: BlueView Configurations Page

This file is now available to restore a BSC's configuration or to be used as the source file from which to create a configuration template.

- Optional. Select the [Change Max Configs](#) link to go to the Logging and Storage Settings Page (see Figure 4-8), to change the **Max Number of Non Preserved Configurations per Host**. This limits the number of automated backups for each Controller (defaults to 5, 0 means no limit). When a backup job completes for a BSC, each backup (matching the IP/Hostname) that is older than the max is deleted. To prevent an older backup from being deleted, mark its checkbox and select **Preserve**.
You can manage the files listed on the Configurations page by clicking the icon corresponding to a configuration file you wish to delete, by clicking the icon corresponding to the configuration file you wish to include in a job, or by clicking the icon corresponding to the configuration file you wish to download from the BlueView Management System. Running BlueView jobs is described in detail in "Running Jobs on BlueView" on page 7-10.

Uploading BSC Image Files to BlueView

Follow these steps to upload a BSC system software image file to BlueView:

- Click **Jobs/Job Elements** from any Administrator Console page, and then click **Controller Upgrades** in the navigation pane.
The BSC Firmware page appears as shown in Figure 7-2.
- Mark the **Upload new firmware?** checkbox.

The **Upgrade Image** field appears.

3. Enter the pathname of the BSC image file you wish to upload to BlueView in the **Upgrade Image** field.
You may search for the BSC image file to upload by clicking **Browse**.
Note that by default, BSC image files have a .img file extension.
4. Click **Upload** to upload the specified BSC system software image file.

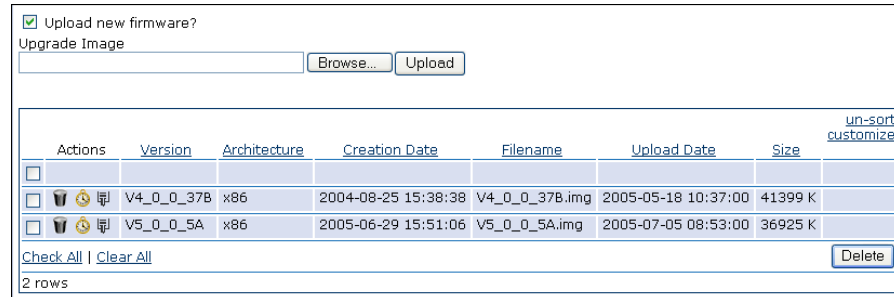


Figure 7-2: BlueSecure Controller Firmware Page

Upon completion of the image file upload, the file is added to the images listed on the BSC firmware page.

This file is now available to upgrade the system software on BSCs on your network.

You may manage the files listed on the BSC Firmware page by clicking the icon corresponding to an image file you wish to delete, by clicking the icon corresponding to the image file you wish to include in a job, or by clicking the icon corresponding to the BSC firmware file you wish to download from the BlueView Management System. Running BlueView jobs is described in detail in “Running Jobs on BlueView” on page 7-10.

Uploading BSAP Image Files to BlueView

Follow these steps to upload a BSAP system software image file to BlueView:

1. Click **Jobs/Job Elements** from any Administrator Console page, and then click **BSAP Upgrades** in the navigation pane.
The BSAP firmware page appears as shown in Figure 7-3.
2. Mark the **Upload new firmware?** checkbox.
The **Upgrade Image** field appears.

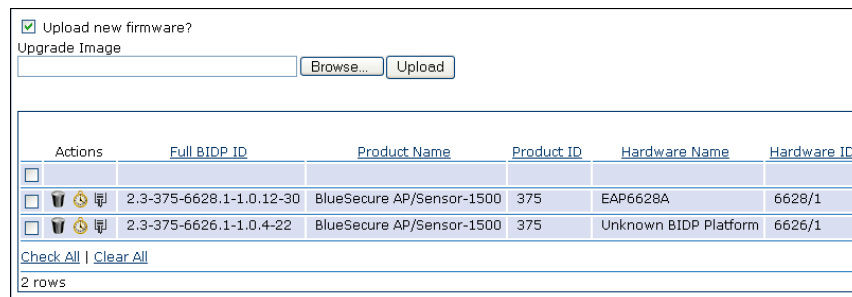





Figure 7-3: BlueSecure Access Point Firmware Page

3. Enter the pathname of the BSAP image file you wish to upload to BlueView in the **Upgrade Image** field.
You may search for the BSAP image file to upload by clicking **Browse**.
Note that by default, BSAP image files have a .img file extension.
4. Click **Upload** to upload the specified BSAP system software image file.
Upon completion of the image file upload, the file is added to the images listed on the Firmware page.
This file is now available to upgrade the system software on BSAPs on your network.
You may manage the files listed on the BSAP Firmware page by clicking the  icon corresponding to an image file you wish to delete, by clicking the  icon corresponding to the image file you wish to include in a job, or by clicking the  icon corresponding to the BSAP image file you wish to download from the BlueView Management System. Running BlueView jobs is described in detail in "Running Jobs on BlueView" on page 7-10.

Uploading Stand Alone AP Image Files to BlueView

Follow these steps to upload a stand alone AP system software image file to BlueView:

1. Click **Jobs/Job Elements** from any Administrator Console page, and then click **Stand Alone AP Upgrades** in the navigation pane.
The Vendor AP Upgrades page appears as shown in Figure 7-4.
2. Mark the **Upload new firmware?** checkbox.
The **Upgrade Image** field appears.









<input type="checkbox"/> Upload new firmware?							
	un-sort						
	customize						
Actions	Vendor Name	Model Number	Filename	Upload Date	Size		
<input type="checkbox"/>							
<input type="checkbox"/>    	Cisco	Cisco AP-1100IOS	c1100-k9w7-mx.123-2JA.tar	2005-12-20 15:50:00	4152 K		
Check All Clear All <input type="button" value="Delete"/>							
1 row download							

Figure 7-4: Stand Alone Access Point Firmware Page

3. Enter the pathname of the stand alone AP image file you wish to upload to BlueView in the **Upgrade Image** field.
You may search for the AP image file to upload by clicking **Browse**.
4. Click **Upload** to upload the specified AP system software image file.
Upon completion of the image file upload, the file is added to the images listed on the Vendor AP Upgrades page.
This file is now available to upgrade the system software on stand alone APs.
You may manage the files listed on the Vendor AP Upgrades page by clicking the  icon corresponding to an image file you wish to delete, by clicking the  icon corresponding to the image file you wish to edit, clicking the  icon corresponding to the image file you wish to include in a job, or by clicking the  icon corresponding to the AP image file you wish to download from the BlueView Management System. Running BlueView jobs is described in detail in "Running Jobs on BlueView" on page 7-10.

Uploading BSC Patch Files to BlueView

Follow these steps to upload a BSC system software patch file to BlueView:

1. Click **Jobs/Job Elements** from any Administrator Console page, and then click **Controller Patches** in the navigation pane.

The BSC Patches page appears as shown in Figure 7-2.

Actions	Name	Version	Architecture	Summary	Release	Creation Date
<input type="checkbox"/>	Version	V4_0_1_6	arm_xscale_le	Changes the version to 4016XP.	1	2004-08-18 00:00:00
<input type="checkbox"/>	V4_0-gMoney	V4_0	x86_pentium3	MC Test Patch.	1	2004-09-24 00:00:00




Figure 7-5: BlueView Patches Page

2. Mark the **Upload a new patch?** checkbox.
The **Blue Patch** field appears.
3. Enter the pathname of the BSC patch file you wish to upload to BlueView in the **Blue Patch** field.

Note that by default, BSC patch files have a .bpf file extension.

4. Click **Upload** to upload the specified BSC system software patch file.
Upon completion of the patch file upload, the file is added to the patches listed on the Patches page.

This file is now available to install on BSCs on your network.

You may manage the files listed on the BSC Patches page by clicking the  icon corresponding to an image file you wish to delete, by clicking the  icon corresponding to the image file you wish to include in a job, or by clicking the  icon corresponding to the BSC patch file you wish to download from the BlueView Management System. Running BlueView jobs is described in detail in "Running Jobs on BlueView" on page 7-10.

Generating a BSC Configuration Template

BlueView enables you to generate configuration templates from a BSC configuration file you have uploaded. After you have generated configuration templates, you can push them out to BSCs on you network.

Follow these steps to generate a BSC configuration template from a configuration file you have uploaded to BlueView:

1. Click **Jobs/Job Elements** from any Administrator Console page, and then click **Controller Templates** in the navigation pane.

The Templates page appears as shown in Figure 7-6.

Actions	Name	Filename	un-sort	customize
<input type="checkbox"/>	All	All	un-filter	
<input type="checkbox"/>	v5.1 Cfg Template	192.168.100.144_v5.1.0.1_20051031122344.backup.blue		

[Check All](#) | [Clear All](#)

1 row [download](#)

Figure 7-6: BSC Configuration Templates Page

- Click .
The BSC Configuration Template page appears as shown in Figure 7-7.

BSC Configuration Template

Name

Import template from backup configuration

Available Backup Configurations

Notes

Figure 7-7: BSC Configuration Template Page

- Enter a descriptive name for the configuration template in the **Name** field.
- Select the previously uploaded configuration file from which to generate the template from the **Available Backup Configurations** drop-down menu.

Uploading configurations to BlueView is described in "Uploading BSC Configuration Files to BlueView" on page 7-2.

- Click **Save** to store the configuration template in the BlueView database.

Clicking **Save and create another** stores the configuration template and enables you to create another.

When BlueView has finished generating the configuration template, the file is added to the templates listed on the Templates page.

This file is now available to update BSC configurations on your network.

You may manage the files listed on the Configurations page by clicking the icon corresponding to a configuration file you wish to delete or by clicking the icon corresponding to a configuration file you wish to include in a job. Running BlueView jobs is described in detail in "Running Jobs on BlueView" on page 7-10.

Additionally, you can click the icon to edit the configuration template's file name or click the icon to launch the BSC configuration template editor as described in the next section.

Editing a BSC Configuration Template

BlueView provides a configuration template editor that enables you to customize any BSC template you have uploaded. The template editor provides the familiar look and feel of the BSC administrator console and enables you to configure the following BSC settings:

- Authentication
 - Server Authentication
 - Local Authentication
 - External Accounting
 - Administrative Users
- Roles
 - Create, Edit, or Delete Roles
- Role Elements
 - Services
 - Destinations
 - Schedules
 - Locations
- VPN
 - IPsec
 - IPsec Policies
 - Certificates
 - Subnet VPN
 - Certificate Enrollment
 - Certificate Validation
 - Contivity Client Configuration
 - PPTP
 - L2TP
- Voice
 - General
 - IP Phones
- General
 - HTTP
 - IDS
 - SNMP Agent
 - Auto Backups
 - Time
 - Email
 - Public Access
 - Logging
 - Thresholds
 - DNS
 - Misc

Refer to the *BlueSecure Controller Setup and Administration Guide* included with your BSC distribution for complete BSC configuration setting descriptions and procedures.

Follow these steps to launch the configuration template editor:

1. Click **Jobs/Job Elements** from any Administrator Console page, and then click **Controller Templates** in the navigation pane.

The templates page appears (see Figure 7-6).

Authentication Roles Role Elements VPN Voice General

HTTP IDS SNMP Agent Auto Backups Time Email Public Acc

HTTP Settings Back Reset Save

Login redirects
 Comma separated list of HTTP/proxy ports to monitor
 80
 Web requests on these ports will be redirected to the login page
 Port of HTTP redirection for user login
 8080
 Adjust if 8080 is in use on your network
 Redirect to hostname
 Will cause unregistered users to be redirected to the hostname, not the IP address
 Typically required when installing a 3rd party SSL certificate
 Automatic redirect enabled
 If checked, users will be redirected to the default URL, not their original destination
 Default redirect URL
 http://www.bluesocket.com/
 Pause in seconds before redirecting user after login
 1
 If 0, users will be kept at the Thank You page
 Seconds a client is allowed to hold the web server
 10
 A value of 300 is recommended prior to doing an upgrade.
 Root CA URL
 0
 Adjust if your custom SSL is a chain certificate


Admin Login options
 Admin web server port
 0
 The recommended port is 443.
 An example port is 8083. Admin access would then be https://IP:8083/admin.pl
 Admin Access Allow Control List
 all
 Comma separated list of IP addresses to allow administrative access. Use partial address to allow an address space, e.g. 10.1.1 allows 10.1.1.0 through 10.1.1.225.
 Disable access to the BSC API

Default language
 Language code
 en
 Default language for admin pages (e.g. en-US).
 Character set
 ISO-8859-1
 Default charset for admin pages (e.g. GB2312).

Clientless Endpoint Scanning
 Enable ICS Scanning Support

Back Reset Save

Figure 7-8: Configuration Template Editor Window

2. Click the  icon corresponding to the configuration template you wish to edit. The configuration template editor runs in a separate browser window, having the familiar look and feel of the BSC administrator console as shown in Figure 7-8.

3. Navigate the configuration template editor interface to change and save any BSC settings you wish to edit.
4. After you have finished editing the configuration template, click the **Close** link in the upper right corner of the editor window.
The edited configuration template is now available for distribution to BSCs on your network.

Running Jobs on BlueView

Follow the procedures given in this section to run the following BSC, BSAP, and BlueView maintenance and provisioning jobs:

- “Restarting BSC Services” on page 7-10 - Restart all services on the BSC, but do not reboot it.
- “Rebooting BSCs” on page 7-12 - Shutdown and then reboot the BSC.
- “Shutting Down BSCs” on page 7-13 - Shutdown the BSC.
- “Backing Up BSC Configurations” on page 7-14 - Upload the BSC’s configuration file to BlueView.
- “Restoring a BSC Configuration” on page 7-14 - Restore a BSC’s configuration from a previously uploaded configuration file.
- “Pushing Out a Configuration Template to a BSC” on page 7-15 - Push a configuration template out to a BSC and then reboot the BSC so that the new configurations settings take effect.
- “Upgrading BSCs with New System Software” on page 7-16 - Upgrade the BSC with a new image file and then reboot the device so that the new system software image runs.
- “Switching the BSC Runtime Image” on page 7-17- Switch from the active to the standby system software image on the BSC, and then reboot the BSC so that former standby image runs as the active image.
- “Installing a System Software Patch on a BSC” on page 7-18 - Install a system software patch file on the BSC and then reboot the BSC so that installed patch takes effect.
- “Removing a System Software Patch on a BSC” on page 7-19 - Remove a system software patch file on the BSC and then reboot the BSC so that installed patch takes effect.
- “Upgrading BSAPs with New Firmware” on page 7-20 - Upgrade the BSAP system software with a new image file and then reboot the device so that the new system software image runs.
- “Upgrading Stand Alone APs with New System Software” on page 7-21 - Upgrade the stand alone AP system software with a new image file and then reboot the device so that the new system software image runs.
- “Applying Stand Alone AP Configuration Changes” on page 7-22 - Apply stand alone configuration changes at the group, BSC, or individual AP level.
- “Sending a BlueView Report via Email” on page 7-23
- “Backing Up a BVMS Configuration” on page 7-24

The procedure to run a BSC discovery job is given in “Discovering WLAN Devices on Your Network” on page 3-8.

Restarting BSC Services

Follow these steps to run a job to restart services on specified BSCs on your network:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears as shown in Figure 7-9. If a previously scheduled job is pending, then you must click **Add** to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.

Empty list, create new Job

Name

Name
20080304070248

Start Time/Recurrence

Hour Minute
07 02

When
 Date
 Time Shortcut

Year Month Day
2008 March 4

Daily
 Recur on the...
 On Demand

Actions

BlueSecure Controller Actions

Restart all Services
 Reboot the devices
 Shutdown the devices
 Backup Controller configuration
 Restore a configuration
 Push a template
 Upgrade with new firmware
 Switch Controller runtime
 Install a new patch
 Remove a patch

BlueSecure Access Point Actions

Upgrade with new local firmware
 Upgrade with new external firmware
 Apply configuration changes
 Calibrate Dynamic RF
 Reboot

Stand Alone Access Point Actions

Upgrade with new firmware
 Apply configuration changes

BlueView Actions

Run a discovery
 Email a Report
 Backup BVMS Configuration

Action Detail
No detail required for action


Notes

Figure 7-9: Job Action Page

4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - Twelve Hours
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.

Mark the **Daily** radio button and then specify on which days to run the job.

Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.

Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Restart all Services** action.

This action will restart all services on the specified BSCs, but will not reboot them.
7. Select the **Device Group** to which to apply the action from the drop-down.

Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
8. Optional. Enter meaningful notes about the job in the **Notes** field.
9. Click **Save** to save the pending job.


The job appears on the Pending jobs list and will run at its scheduled time.

Alternatively, click **Save and Create Another** to save the job and creating another.

Rebooting BSCs

Follow these steps to run a job to reboot (i.e., shutdown and then restart) specified BSCs:


1. Click **Jobs/Pending** from any Administrator Console page.

If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click  to add a new job to the list of pending jobs before the Job Action page appears (see Figure 7-9).
2. Enter a meaningful name for the job in the **Name** field.

By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - Twelve Hours
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.



Mark the **Daily** radio button and then specify on which days to run the job.

Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.

- Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Reboot the devices** action.
This action will reboot (i.e., shutdown and then restart) the specified BSCs.
 7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
 8. Optional. Enter meaningful notes about the job in the **Notes** field.
 9. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and creating another.


Shutting Down BSCs

Follow these steps to run a job to shut down specified BSCs on your network:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click  to add a new job to the list of pending jobs before the Job Action page appears (see Figure 7-9).
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Shutdown the devices** action.
This action will shut down (i.e., stop operation of) the specified BSCs.
7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
8. Optional. Enter meaningful notes about the job in the **Notes** field.
9. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and creating another.

Backing Up BSC Configurations

Follow these steps to run a job to back up the configurations of (i.e., upload configuration files from) specified BSCs on your network:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click **Add** to add a new job to the list of pending jobs before the Job Action page appears (see Figure 7-9).
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Backup BSC configuration** action.
This action will upload the configuration file from the specified BSCs.
7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
8. Optional. Enter meaningful notes about the job in the **Notes** field.
9. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and create another.

Restoring a BSC Configuration

 **Note:** You must have uploaded a BSC configuration file to BlueView as described in the previous section and in "Uploading BSC Configuration Files to BlueView" on page 7-2 before you can run this job type.


Follow these steps to run a job to restore the configuration of a single BSC:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click **Add** to add a new job to the list of pending jobs before the Job Action page appears (see Figure 7-9).
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.

3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - Twelve Hours
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.

Mark the **Daily** radio button and then specify on which days to run the job.

Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.

Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Restore a configuration** action.


This action will download the specified configuration file from BlueView to the specified BSC.
7. Select the single BSC to which to apply the action from the **Controller** drop-down menu.
8. Select the configuration file to download to the BSC from the **Available Backup Configurations** drop-down menu.
9. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot the BSC after the configuration file has been uploaded to it.

Although, the new configuration will not take effect until the BSC is restarted, you may opt to reboot the BSC at a later, more convenient time.
10. Optional. Enter meaningful notes about the job in the **Notes** field.
11. Click **Save** to save the pending job.

The job appears on the Pending jobs list and will run at its scheduled time.


Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Pushing Out a Configuration Template to a BSC


 **Note:** You must have created a BSC configuration template from an uploaded BSC configuration file as described in “Generating a BSC Configuration Template” on page 7-6 before you can run this job type.

Follow these steps to run a job to push out a configuration template to one or more BSCs on your network:

1. Click **Jobs/Pending** from any Administrator Console page.


If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click  to add a new job to the list of pending jobs before the Job Action page appears (see Figure 7-9).
2. Enter a meaningful name for the job in the **Name** field.


By default, the Name field is filled with the current yyyyymmddhhmm timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:


- **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - Twelve Hours
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Push a template** action.
This action will download the specified configuration file from BlueView to the specified BSCs.
7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
8. Select the configuration template to push out to the selected BSCs from the **Configuration Template** drop-down menu.
9. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot each BSC after the configuration template has been uploaded.
Although, the new configuration will not take effect until each BSC is restarted, you may opt to reboot the BSCs at a later, more convenient time.
10. Optional. Enter meaningful notes about the job in the **Notes** field.
11. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Upgrading BSCs with New System Software

Follow these steps to run a job to upgrade the system software on specified BSCs on your network:


 **Note:** If you downgrade a BSC's firmware, the current configuration will not be carried over.


1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click  to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current yyyyymmddhhmm timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.

- **One Hour**
 - Twelve Hours
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
 6. Mark the radio button corresponding to the **Upgrade with new firmware** action.
This action will download the specified system software image file from BlueView to the specified BSCs.
 7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
 8. Select the firmware image to push out to the selected BSCs from the **Available Firmware** drop-down menu.
 9. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot each BSC after the software image has been uploaded to it.
Although, the new image will not run until each BSC is restarted, you may opt to reboot the BSCs at a later, more convenient time.
 10. Optional. Enter meaningful notes about the job in the **Notes** field.
 11. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Switching the BSC Runtime Image


Follow these steps to run a job to switch from the active to the standby system software image on a single BSC so that former standby image runs as the active image:


1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click  to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - Twelve Hours
 - **1 Day**
 - **1 Week**

- **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
 6. Mark the radio button corresponding to the **Switch BSC runtime** action.
This action will cause the selected BSC to switch from its active to its standby system software image so that former standby image runs as the active image.
 7. Select the individual BSC or BSC group to which to apply the action from the **Device Group** drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
 8. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot the BSC after the image has been switched.
Although, the image switch will not take effect until the BSC is rebooted, you may opt to reboot the BSC at a later, more convenient time.
 9. Optional. Enter meaningful notes about the job in the **Notes** field.
 10. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Installing a System Software Patch on a BSC

Follow these steps to install a system software patch file on one or more BSCs on your network:


1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click  to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.

- Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Install a new patch** action.
This action will install a selected patch file on the specified BSCs.
 7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
 8. Select the system software patch file to install on the selected BSC from the **Available patches** drop-down menu.
 9. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot each BSC after the patch file has been installed on it.
Although, some patch files will not take effect until each BSC is restarted, you may opt to reboot the BSCs at a later, more convenient time.
 10. Optional. Enter meaningful notes about the job in the **Notes** field.
 11. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Removing a System Software Patch on a BSC

You may need to un-install a system software patch if it does not provide the functionality updates you need for your BSC or as a prerequisite to installing a newer software patch.


Follow these steps to remove a system software patch file on one or more BSCs on your network:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Remove a patch** action.

- This action will remove a selected patch file from the specified BSCs.
7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
 8. Enter the complete filename of the system software patch to remove from the specified BSCs in the **Patch name to remove** field.
Note that by default, BSC patch files have a .bpf file extension.
 9. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot each BSC after the patch file has been removed from it.
Although, some patch file deletions will not take effect until each BSC is restarted, you may opt to reboot the BSCs at a later, more convenient time.
 10. Optional. Enter meaningful notes about the job in the **Notes** field.
 11. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Upgrading BSAPs with New Firmware

You can update the firmware on BSAPs on your network by pushing out the new firmware file to BSCs on your network. The BSCs will then subsequently upgrade BSAPs that they have configured with the new firmware file. Follow these steps to run a job to upgrade the firmware on specified BSAPs on your network:


1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click **Add** to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Upgrade with new local firmware** action or the **Upgrade with new external firmware** action under the **BlueSecure Access Point Actions** heading.

This action will download the specified system software image file from BlueView to the specified BSAPs.

7. Select the **Device Group** to which to apply the action from the drop-down menu. Alternatively, mark the **Specific Controller...?** checkbox, and then select the single BSC to which to apply the action from the **Controller** drop-down menu.
8. Select the firmware image to push out to the selected BSCs from the **Available Firmware** drop-down menu.
9. Optional. Enter meaningful notes about the job in the **Notes** field.
10. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Upgrading Stand Alone APs with New System Software


Follow these steps to run a job to upgrade the system software on specified stand alone APs on your network:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current yyymmddhhmm timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the **Upgrade with new firmware** radio button under the **Stand Alone Access Point Actions** heading.
This action will download the specified system software image file from BlueView to the specified stand alone APs.
7. Select the **Device Group** to which to apply the action from the drop-down menu. Alternatively, select the individual AP to which to apply the action from the from the **Stand Alone APs** drop-down menu.
8. Select the firmware image to push out to the selected stand alone APs from the **Available Stand Alone Firmware** drop-down menu.

9. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot each stand alone AP after the software image has been uploaded to it.
Although, the new image will not run until each stand alone AP is restarted, you may opt to reboot the APs at a later, more convenient time.
10. Optional. Enter meaningful notes about the job in the **Notes** field.
11. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Applying Stand Alone AP Configuration Changes

Follow these steps to run a job to apply configuration changes you have made to stand alone APs at the group or individual AP level:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click **Add** to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the **Apply configuration changes** radio button under the **Stand Alone Access Point Actions** heading.
This action will apply the configuration changes you have made to the selected AP(s).
7. Select the **Device Group** to which to apply the action from the drop-down menu.
Alternatively, select the individual AP to which to apply the action from the **Stand Alone APs** drop-down menu.
8. Optional. Mark the **Restart/Reboot automatically if necessary?** checkbox to automatically reboot each stand alone AP after the firmware image has been uploaded to it.
Although, the new image will not run until each stand alone AP is restarted, you may opt to reboot the APs at a later, more convenient time.


9. Optional. Enter meaningful notes about the job in the **Notes** field.
10. Click **Save** to save the pending job.
The job appears on the Pending jobs list and will run at its scheduled time.
Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Sending a BlueView Report via Email

You may send out a report that you have generated on BlueView via email to an administrator or other interested party.

See “Generating Status Reports” on page 6-24 for information about generating reports on BlueView.

Follow these steps to send out a generated report via email:

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current yyymmddhhmm timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Email a report** action under the **BlueView Actions** heading.
This action will send a specified report to an individual via email.
7. Select the report to send from the **Available Reports** drop-down menu.
8. Specify the file format for the report by marking the appropriate radio button:
 - **Email the report in .pdf format**
 - **Email the report in excel format**
9. Enter the email address(es) to which to send the report in the **Destination Email Address** field. Separate email addresses with a semicolon (;)
10. If you have not previously set up an email server on the BlueView Setup Email page:
 - a) Enter the IP address of the Simple Mail Transfer Protocol server that BlueView is to use to send event notifications to administrators in the **SMTP Server** field.

- b) Enter the email address that is to be used to identify the sender in event notification messages sent from BlueView in the **Return Address** field.

This should be a valid email address to which bounce notifications can be sent.

11. Optional. Enter meaningful notes about the job in the **Notes** field.


12. Click **Save** to save the pending job.

The job appears on the Pending jobs list and will run at its scheduled time.

Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Backing Up a BVMS Configuration

Follow these steps to generate a backup BVMS configuration on BlueView and then download it to a specified server via file transfer protocol (FTP) or secure copy protocol (SCP):

1. Click **Jobs/Pending** from any Administrator Console page.
If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9). If a previously scheduled job is pending, then you must click **Add** to add a new job to the list of pending jobs before the Job Action page appears.
2. Enter a meaningful name for the job in the **Name** field.
By default, the Name field is filled with the current `yyyymmddhhmm` timestamp.
3. Select a start time for the job using the **Hour** and **Minute** picklists.
4. Select the time at which to run the job from the **Time Shortcut** menu:
 - **Date shown below** - You must set the date and time at which BlueView is to run the job using the Year, Month, Day, Hour, and Minute drop-down menus.
 - **One Hour**
 - **Twelve Hours**
 - **1 Day**
 - **1 Week**
 - **1 Month**
5. Optional. Specify how often the job is to recur.
Mark the **Daily** radio button and then specify on which days to run the job.
Mark the **Recur on the ...** radio button, and then specify the frequency at which to run the job using the three provided drop-down menus.
Mark the **On Demand** radio button to add the job to the Pending Jobs list without running it. Run from the Pending Jobs list by clicking the corresponding  icon.
6. Mark the radio button corresponding to the **Backup BVMS Configuration** action under the **BlueView Actions** heading.
This action will generate a backup configuration file and enable you to download it to a specified server via ftp or scp.
7. Enter the URL of the destination FTP server in the **FTP server hostname** field.
8. Enter the directory to which to write the file on the destination server in the **Destination directory** field.
9. Enter the username to use to access the specified server host in the **Username** field.
10. Enter the password to access the specified server host in the **Password** field and then re-enter it in the **Confirm Password** field.
11. Specify the protocol to use when transferring the BVMS configuration backup file to the specified server by marking the appropriate radio button:

- **FTP** - transfer the backup BVMS configuration file using File Transfer Protocol.
 - **SCP** - transfer the backup BVMS configuration file using Secure Copy Protocol.
12. Enter the email address to which to send the report in the **Destination Email Address** field.
 13. Optional. Enter meaningful notes about the job in the **Notes** field.
 14. Click **Save** to save the pending job.
 The job appears on the Pending jobs list and will run at its scheduled time.
 Alternatively, click **Save and Create Another** to save the job and continue creating additional jobs.

Reviewing Pending Jobs

Jobs that have yet to be run at their scheduled time or that could not be run completely are labeled as pending in the BlueView administrator console.

To view pending jobs, Click **Jobs/Pending** from any Administrator Console page.

If no previously scheduled jobs are pending, the Job Action page appears (see Figure 7-9) enabling you to create a job.










Action	Name	Detail	Start Time	un-sort	customize
<input type="checkbox"/>					
<input type="checkbox"/>   	Install BluePatch 1.8	Patch device '192.168.168.37'	Fri Jan 14 15:37:00 EST 2005		
<input type="checkbox"/>   	Restart Lobby BSC	Restart device '192.168.168.37'	Wed Jan 12 18:40:00 EST 2005		
Check All Clear All					<input type="button" value="Delete"/>
2 rows					

Figure 7-10: Pending Jobs Page

If a previously scheduled job is pending, then the Pending Jobs page appears as shown in Figure 7-10.

The displayed job history information includes:

- **Name** - The job's configured name.
- **Detail** - A brief summary of the task the job is to complete.
- **Start Time** - The date and time at which BlueView is scheduled to run the job.

You may manage the files listed on the Pending Jobs page by clicking the  icon corresponding to a job file you wish to delete, clicking the  icon corresponding to a job file you wish to edit, or clicking the  icon corresponding to a job file you wish to run immediately. Refer to the section entitled "Running Jobs on BlueView" on page 7-10 when editing a BlueView job.

Reviewing Job History

You can display a concise summary of BlueView jobs that have run.

To view a history of run jobs, Click **Jobs/History** from any Administrator Console page.

The Jobs History page appears as shown in Figure 7-11.




Action	Name	State	Detail	Date
<input type="checkbox"/>				
<input type="checkbox"/> 	Floor Discovery	Success	Discover '2'	At 16:14 on 2005-06-28
<input type="checkbox"/> 	Lab Discovery	Success	Discover '3'	At 16:22 on 2005-06-28
Check All Clear All				<input type="button" value="Delete"/>
2 rows				

Figure 7-11: Jobs History Page

The displayed job history information includes:

- **Name** - The configured name of the job.
- **State** - Possible job states are: Success, Competed With Error, Competed With Some Errors, and Running.
- **Date** - The date and time at which BlueView ran the job.
- **Detail** - Click the Show detail icon,  , to display detailed status messages about the job

You may manage the files listed on the Jobs History page by marking the checkbox corresponding to a job history you wish to delete from the database, and then clicking Delete. You can delete all displayed job histories from the database by clicking **Purge all job history**.

Managing BSAP Configurations

Bluesocket manufactures a line of a next-generation, “thin” access points (AP) that works in conjunction with BlueSecure Controllers for enterprise wireless LAN (WLAN) deployments. BlueSecure Access Points (BSAPs) feature dual radios supporting 802.11a/b/g in a plenum-rated housing with fixed omni-directional antennas.

BlueSecure Access Points can be configured to operate in AP mode for standard wireless client access, sensor mode to perform RF scanning to detect WLAN intrusion, attack, or vulnerability, or dual AP/sensor mode where the device alternates between access point and RF sensor operation on a continual basis.

After you have discovered BlueSecure Controllers or manually added BlueSecure Controllers to the BlueView managed device list, any APs connected to the BSCs under BlueView management will be listed in the navigation pane of any BlueView status window. Additionally, all BSAP configurations stored on BSCs under BlueView management will be listed on the Access Points page. These BSAP configurations will also be listed in the navigation pane.

In general, we recommend that you store a BSAP’s configuration only on its home BSC.

You can manage BSAP configurations from BlueView, by:

- Listing BSAP Configurations
- Editing BSAP Configurations
- Deleting BSAP Configurations
- Adding/Removing BSAP Configurations to/from a BSC
- Creating a BSAP Configuration Template

Listing BSAP Configurations

Click **Devices/Access Points** from any BlueView administrator console page to see a list of BSAP configurations stored on BSCs under management by BlueView as shown in Figure 7-12.

	Actions	In Sync	Status	MAC	Enabled	Hostname	Location	Home Controller	un-sort	customize
<input type="checkbox"/>										
<input type="checkbox"/>		Yes		00:12:cf:0a:a4:7a	Yes	jmcubebap	jm cube	192.168.100.29		
<input type="checkbox"/>		Yes		11:11:11:11:11:11	No			192.168.100.135		
<input type="checkbox"/>		Yes		00:12:cf:09:fd:c2	Yes	jby	cube	192.168.100.144		
<input type="checkbox"/>		Yes		22:22:22:22:22:22	Yes			192.168.100.135		
<input type="checkbox"/>		Yes		00:12:cf:09:fd:cb	Yes	shankar	cube	192.168.100.161		

|

5 rows

Figure 7-12: Displaying BSAPs

The following information is displayed for BSAPs:

- **In Sync** - Does the BSAP configuration stored on BlueView match the BSAP's current configuration? Yes or No. If the configurations are out of sync, then click to synchronize the configurations.
- **Status** - The BSAP's current status, Up or Down .
- **MAC** - The BSAP's configured MAC address.
- **Enabled** - Is the BSAP's service enabled? Yes/No. The BSAP's service must be enable to allow it to be configured and managed by its home BSC.
- **Template** - Configuration template used to configure the BSAP's identification and radio settings.
- **Name** - The hostname assigned to the BSAP in its configuration.
- **Location** - The location assigned to the BSAP in its configuration.
- **Home Controller** - The BSC to which the BSAP is connected and by which it is configured.

Click the icon to edit a BSAP's configuration as described in the next section.

Click to apply a BSAP configuration you have edited and saved on BlueView to the BSAP's home BSC.

Click or to selectively enable or disable BSAPs on a BSC. Click or to delete a BSAP's configuration from its home BSC.

Click to assign/remove a template to/from the selected BSAP.


Click to reset the selected BSAP configurations. Resetting a BSAP configuration means that the configuration is deleted locally on BlueView and then updated with the first matching BSAP configuration (i.e., a configuration having a matching MAC address) found on a BSC under management by BlueView. If no matching BSAP is found, then the BSAP configuration remains deleted on BlueView.


Click to reboot the selected BSAPs. You should only need to reboot a BSAP if it is hung or you have otherwise lost communications to it.

Editing BSAP Configurations

Editing BSAP configuration requires that you edit the following settings:


- BSAP identification settings
- 802.11a radio settings
- 802.11b/g radio settings

 **Note:** Once you have edited and saved a BSAP configuration on BlueView, you must apply the edited configuration to BSAP's home controller.

 **Note:** Fields displayed in blue are using the settings from the AP Template specified in the System View. You can reset all the configuration fields to use the Template settings by clicking on the Default button.

Editing BSAP Identification Settings

To edit a BSAP's identification settings:

1. Click **Devices/Access Points** from any BlueView administrator console page. A list of BSAPs configured on BSCs under management by BlueView appears (see Figure 7-12).
2. Click the  icon corresponding to the BSAP configuration you wish to edit.
3. Mark the **System** radio button to display the BSAP identification settings. The Edit AP page appears, for example as shown in Figure 7-13 for a BSAP-1800.

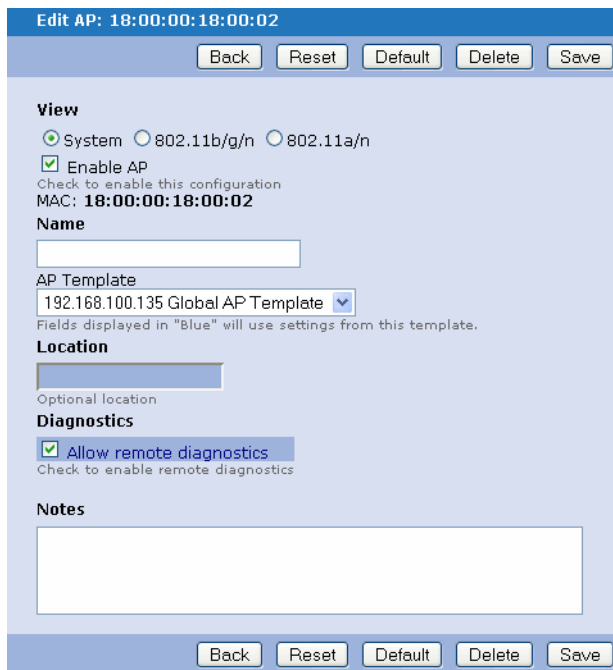


Figure 7-13: Edit AP Page (ID Settings)

4. Mark the **Enable setting** checkbox to enable the BSAP configuration.
5. Enter a unique hostname for the BSAP in the **Name** field.
6. Optional. Select the template used to configure the BSAP's identification and radio settings from the **AP Template** drop-down menu.


You must create a BSAP configuration template as described in “Creating a BSAP Configuration Template” on page 7-36 before this menu is populated with selections.

7. Optional. Enter a location for the AP in the **Location** field.
8. Optional (not supported on 1700). Mark the **Allow remote diagnostics** checkbox to allow Bluesocket service personnel to reach the BSAP via SSH to perform remote diagnostics.
9. Optional. Enter a meaningful description of the BSAP in the **Notes** field.
10. Click **Save** to save the BSAP configuration to the BlueView database.
11. Click from the Access Points page to apply the BSAP configuration you have edited to the BSAP’s home BSC.

Editing 802.11b/g Radio Settings

The IEEE 802.11g standard operates within the 2.4 GHz band at up to 54 Mbps. Also note that because the IEEE 802.11g standard is an extension of the IEEE 802.11b standard, it allows clients with 802.11b wireless network cards to associate to an 802.11g access point.

To edit a BSAP’s 802.11b/g radio settings:

1. Click **Devices/Access Points** from any BlueView administrator console page.
A list of BSAPs configured on BSCs under management by BlueView appears (see Figure 7-12).
2. Click the  icon corresponding to the BSAP configuration you wish to edit.
3. Mark the **802.11b/g** radio button to display the BSAP 802.11b/g radio settings.
The Edit AP page appears. For example, if you edit a BSAP-1800, the available settings are as shown in Figure 7-14.
4. Mark the **Enable 802.11b/g Radio** checkbox at the top of the page to enable the 802.11b/g radio in the BSAP.
5. Set the BSAP’s operational mode by selecting one of the following options from the **Operational Mode** drop-down menu:
 - **AP Mode** - BSAP provides standard wireless client access.
 - **Sensor Mode** - BSAP performs RF scanning to detect WLAN intrusion, attack, or vulnerability.
 - **Dual (AP/Sensor) Mode** - BSAP alternates between access point and RF sensor operation on a continual basis.
6. Set the **Wireless Mode And Rate**.
 - a) Select 802.11b/g, 802.11b, or 802.11g from the **Wireless Mode** drop-down menu.
The 802.11b/g and 802.11g modes provide connections up to 54 Mbps.
 - b) Select the BSAP’s data transmit rate from the **Transmit Rate** drop-down menu.
Select the Auto setting to enable the BSAP to determine and use its optimal transmit rate. (Default: Auto)

Edit AP: 18:00:00:18:00:02

Back Reset Default Delete Save

View

System
 802.11b/g/n
 802.11a/n

Enable 802.11b/g/n radio

Operational Mode

Dual(AP/Sensor) Mode ▾

Wireless Mode and Rate

Wireless Mode: 802.11g/n ▾ Minimum Transmit Rate: 54 Mbps ▾

The BSAP-1700 will always use the best rate

Channel Options

Auto Channel Select

Automatically determine optimal channel

Channel: Auto ▾

Manually setting channel

Transmit Power

Minimum = 0 mW ▾ 0%

Radio output power level

SSID Settings

Use default SSIDs ▾

Advanced Settings for the 802.11b/g/n Radio

Display Advanced Settings for the 802.11b/g/n Radio?

Load Balancing

Average user count per AP: Enforcement: Low ▾

Average number of associations per AP before balancing clients.
BSAP-1500 and BSAP-1540: 1-56. BSAP-1700 and BSAP-1800: 1-64

Voice Call Admission Control

Enable Voice Call Admission Control?

Check to enable WMM Settings

Enable SVP?

Check to enable Spectralink/Avaya Voice Protocol(SVP)

WMM Settings

Voice Sessions:

Maximum number of voice sessions per radio. '0' means unlimited.

Video Sessions:

Maximum number of video sessions per radio. '0' means unlimited.

BSAP-1800 MIMO Settings

Channel Bandwidth: 20 Mhz ▾

Whether to use the secondary channel setting for MIMO client, and when to disable this feature if a non-MIMO network is detected

Packet Aggregation: Disable ▾

Used to transmit multiple data packets in a single 802.11 frame, without any delay.

MIMO Secondary Channel: Auto ▾

Manually set MIMO secondary channel - a second frequency that AP will use for higher throughput. This channel must be at exactly four channels away from primary (e.g. channel 1 or 9 if the AP is on channel 5).

Back Reset Default Delete Save

Figure 7-14: Edit AP Page - (802.11b/g Radio Settings)

7. Mark the **Auto Channel Select** checkbox to enable automatic radio channel selection. This is the default and recommended setting.

Alternatively, set the channel the BSAP 802.11b/g radio is to operate on in the **Channel** field.

When multiple BSAPs are deployed in the same area, set the channel on neighboring BSAPs at least five channels apart to avoid interference with each other. For example, in the United States you can deploy up to three BSAPs in the same area (e.g., channels 1, 6, 11).

Also note that the channel for wireless clients is automatically set to the same as that used by the BSAP to which it is linked.

8. Adjust the power of the radio signals transmitted from the BSAP by selecting a **Transmit Power** level from the drop-down menu.

The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (Default: 100% transmission power for the selected country/region)

You can also adjust the transmission power level settings using the (+) and (-) buttons to the right of the drop-down menu.

9. To Define the SSIDs a BSAP is to use, select an option from the **SSID Settings** menu:

- **Use default SSIDs** - The BSAP will use only the default SSIDs.
- **Exclude selected SSIDs** - The BSAP will use only those SSIDs not selected in the Select SSID picklist.
- **Only Use Selected SSIDs** - The BSAP will use only those SSIDs selected in the Select SSID picklist.



Note: Only one SSID is supported on the BSAP-1700's "a" radio. Instead of the following three options, the drop-down for the BSAP 1700's a radio allows you to select just a single SSID.

Advanced Settings

10. Mark the **Display Advanced Settings** checkbox to specify the following:

- **Beacon Interval** – Enter the rate in milliseconds at which beacon signals are transmitted from the BSAP.

The beacon signals allow wireless clients to maintain contact with the BSAP. They may also carry power-management information. (Default: 100 milliseconds)

- **Fragmentation Threshold** – Enter the maximum length (in bytes) of the frame, beyond which payload must be broken up (fragmented) into two or more frames. (Range: 256-2346 bytes, Default: 2346 bytes)

Collisions occur more often for long frames because sending them occupies the channel for a longer period of time, increasing the chance that another station will transmit and cause collision. Reducing Fragmentation Threshold results in shorter frames that "busy" the channel for shorter periods, reducing packet error rate and resulting retransmissions. However, shorter frames also increase overhead, degrading maximum possible throughput, so adjusting this parameter means striking a good balance between error rate and throughput.

- **RTS Threshold** – Set the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. (Range: 256-2346 bytes: Default: 2346 bytes)

The BSAP sends RTS frames to a receiving station to negotiate the sending of data. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 0, the BSAP never sends RTS signals. If set to 2347, the BSAP always sends RTS signals. If set to any other value, and the packet size

equals or exceeds the RTS threshold, the RTS/CTS (Request to Send /Clear to Send) mechanism will be enabled.

The BSAPs contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem."

- **DTIM** – Enter the rate at which stations in sleep mode must wake up to receive broadcast/multicast transmissions. (Range: 1-255 beacons; Default: 1 beacon) Delivery Traffic Indication Map (DTIM) interval, it indicates how often the MAC layer forwards broadcast/multicast traffic, which is necessary to wake up stations that are using Power Save mode. The default value of 2 indicates that the BSAP will save all broadcast/multicast frames for the Basic Service Set (BSS) and forward them after every second beacon.

Using smaller DTIM intervals delivers broadcast/multicast frames in a more timely manner, causing stations in Power Save mode to wake up more often and drain power faster. Using higher DTIM values reduces the power used by stations in Power Save mode, but delays the transmission of broadcast/multicast frames.

11. (15xx only) Specify the **Antenna Type** by marking the appropriate radio button:
 - **Internal** - The BSAP uses its fixed omni antennas for communications.
 - **External** - The BSAP uses connected external antennas for communications. External antennas are available only for model BSAP-1540s. A BSAP-1500 will always use its fixed antennas for communications regardless of the configured antenna type. Selecting External disables antenna diversity controls, since only antenna B is used.
12. (15xx only) Mark the **Antenna Diversity** radio button to specify whether the antenna is automatically selected based on best signal reception (i.e., Diversity mode), or is fixed to use one of the BSAP's antennas, A or B. (Default: Diversity mode is enabled).
13. **Load Balancing**: Enter the maximum number of wireless devices that may associate to the BSAP in the **Average user count per AP** field. Valid values for this setting are 1 to 56.

Set the relative strength of the BSAP's enforcement of the maximum AP client count from low (BSAP rejects a client device once before allowing it to associate), medium (BSAP rejects a client device up to three times before allowing it to associate) or high (BSAP rejects a client device up to five times before allowing it to associate) by selecting a value from the **Enforcement** drop-down menu.
14. **Voice Call Admission Control**: BlueSecure Controller system software release 5.2 (and higher) enables IP phone voice traffic to pass through the BSC, providing support of widely used voice over IP protocols (SIP and H.323), vendor-specific IP phone configuration (Spectralink/Avaya, Cisco, Skype, and Vocera), and system-level QoS for voice traffic.
 - VoIP is highly sensitive to the network delay, jitter, errors, lost, and retransmitted packets. To enable call admission control for this BSAP, mark the **Enable Voice Call Admission Control?** checkbox.
 - Mark the **Enable SVP** checkbox if your wireless clients are passing Spectralink/Avaya IP phone traffic through the BSC.
15. Optional. Specify **WMM settings**, advanced BSAP radio Wi-Fi multimedia settings. These settings determine the Quality of Service (QoS) function that is used for multimedia applications, such as Voice-over-IP (VoIP) and video, and allows the network packets of the multimedia application to have priority over regular data network packets, enabling multimedia applications to run smoother and with fewer errors.

Note: To enable the WMM QoS settings on a BSAP, you must mark the **Use WMM to apply QoS** checkbox on the Create/Edit SSID page and then assign that SSID to the BSAP.

Enter the maximum number of voice clients that may associate to the BSAP in the **Voice Sessions** field.

Enter the maximum number of video clients that may associate to the BSAP in the **Video Sessions** field.

The above maximum voice and video sessions settings affect only SSIDs that have voice and video QoS enabled. Note that a BSAP's system-level QoS and the Wi-Fi multimedia QoS that you enable for voice and video SSIDs are complementary. We recommend that you enable both QoS methods when passing voice or video traffic on the BSAP.

MIMO Settings

For BSAP-1700s and BSAP-1800s, specify the following:

- **Adaptive Channel Expansion 1700/Channel Bandwidth (1800)**

Only supported on b/g/n card – Airgo Gen-3 card. Provides increased data rates by increasing the RF bandwidth from 20 MHz to 40 MHz by combining adjacent channels. Adaptive Channel Expansion/Channel Bandwidth enables the following rates –48, 72, 84, 96, 144, 160, 168, 192, 216, 240 Mbps.

Here is an example of the channel usage in ACE: - primary and secondary channels are separated by 4 channels.

- 1 is primary, 5 is secondary
- 6 is primary, 2 is secondary
- 7 is primary, 11 is secondary
- 11 is primary, 7 is secondary
- 9 is primary, 13 is secondary

The BSAP automatically determines the secondary channel based on channel set in the UI. If you enable auto channel selection, the BSAP first determines the primary through an auto channel selection algorithm and then sets the secondary 4 channels away.

Before you enable this feature, make sure that the channels are available in your RF network. Otherwise, you could experience degraded performance with MIMO Concatenation Mode/ Packet Aggregation. All 20Mhz traffic and the management frames are always sent on the primary channel.

- 0 = Disabled
- 1 = Enabled
- 2 = Enable if no legacy BSS (i.e. no legacy AP detected)
- 3 = Enabled if no legacy device (i.e. no legacy station is detected)
- **MIMO Concatenation Mode(1700)/Packet Aggregation(1800):** Used to transmit multiple data packets in a single 802.11 frame, without any delay. If concatenation is enabled, there will be a maximum limit of 14 clients.
- **MIMO Secondary Channel (1800 only):** Manually set a second frequency that the BSAP will use for higher throughput. This channel must be at exactly four channels away from primary (e.g. channel 1 or 9 if the AP is on channel 5).
- **MIMO Compression Mode (1700 only):** (b/g/n card – Airgo Gen3 card)
Data frames are compressed by hardware, which can increase data throughput. An Airgo Gen-3 MIMO client is required for this feature.

- 0 = Disabled
- 1 = Enabled
- **MIMO Network Density (1700 only):** Network Density refers to how many wireless networks are deployed in your surroundings. This setting provides a mechanism to tell the AP how noisy to expect the environment so the AP can then adjust its noise threshold accordingly. The settings are subjective (i.e. there is no static range of devices associated with the settings high, medium, and low) and might require some experimentation to determine the optimal setting. A site survey should help determine the network density in your environment. Adjusting the network density affects transmit power and overall system performance.

16. Click **Save** to save the BSAP radio settings to the BlueView database.

17. Click from the Access Points page to apply the BSAP configuration you have edited to the BSAP's home BSC.

You may be prompted to restart the BSC. We recommend that you do not restart the BSC until you have completely finished configuring the BSC for use in your network.


Editing 802.11a Radio Settings

The IEEE 802.11a interface operates within the 5 GHz band, at up to 54 Mbps in normal mode or up to 108 Mbps in Turbo mode.



Note: Complete 802.11a radio settings not discussed in this section by referring to the instructions given in "Editing 802.11b/g Radio Settings" on page 7-29, as these settings match those for the BSAP 802.11a radio.

To edit a BSAP's 802.11a radio settings:

1. Click **Devices/Access Points** from any BlueView administrator console page.
A list of BSAPs configured on BSCs under management by BlueView appears (see Figure 7-12).
2. Click the  icon corresponding to the BSAP configuration you wish to edit. The Edit-AP page appears. For example, when editing the settings for a BSAP-1800, the Edit AP page appears as shown in Figure 7-15.
3. Mark the **802.11a** radio button to display the BSAP 802.11a radio settings.
4. Mark the **Enable 802.11a Radio** checkbox at the top of the page to enable the 802.11a radio in the BSAP.
5. Set the wireless mode and rate.
 - a) Select 802.11a or 802.11 Turbo A from the **Wireless Mode** drop-down menu.
The normal 802.11a wireless operation mode provides connections up to 54 Mbps. Turbo Mode is an enhanced mode (not regulated in IEEE 802.11a) that provides a higher data rate of up to 108 Mbps. Enabling Turbo Mode allows the BSAP to provide connections up to 108 Mbps. (Default: Normal 802.11a mode)
In normal mode, the BSAP provides a channel bandwidth of 20 MHz, and supports the maximum number of channels permitted by local regulations (e.g., 11 channels for the United States). In Turbo Mode, the channel bandwidth is increased to 40 MHz to support the increased data rate. However, this reduces the number of channels supported (e.g., 5 channels for the United States).
 - b) Select the BSAP's data transmit rate from the **Transmit Rate** drop-down menu.
Select the Auto setting to enable the BSAP to determine and use its optimal transmit rate. (Default: Auto)
6. **SSID** - Select a single from the drop-down (the BSAP-1700 supports just one SSID for "a" radios, unlike the BSAP-1500/1540).

Edit AP: 18:00:00:18:00:02

Back Reset Default Delete Save

View

System
 802.11b/g/n
 802.11a/n

Enable 802.11a/n radio

Operational Mode

Sensor Mode

Wireless Mode and Rate

Wireless Mode: 802.11a Minimum Transmit Rate: No Minimum

The BSAP-1700 will always use the best rate

Channel Options

Auto Channel Select

Allow algorithm to determine optimal channel

Channel: Auto

Manually setting channel

Maximum Transmit Power

20 dBm = 100 mW 100%

Radio output power level

SSID Settings

Use default SSIDs

Advanced Settings for the 802.11a/n Radio

Display Advanced Settings for the 802.11a/n Radio?

Load Balancing

Average user count per AP: 64 Enforcement: Low

Average number of associations per AP before balancing clients.
BSAP-1500 and BSAP-1540: 1-56, BSAP-1700 and BSAP-1800: 1-64

Voice Call Admission Control

Enable Voice Call Admission Control?

Check to enable WMM Settings

Enable SVP?

Check to enable Spectralink/Avaya Voice Protocol(SVP)

WMM Settings

Voice Sessions: 3

Maximum number of voice sessions per radio. '0' means unlimited.

Video Sessions: 3

Maximum number of video sessions per radio. '0' means unlimited.

BSAP-1800 MIMO Settings

Channel Bandwidth: 20 Mhz

Whether to use the secondary channel setting for MIMO client, and when to disable this feature if a non-MIMO network is detected

Packet Aggregation: Disable

Used to transmit multiple data packets in a single 802.11 frame, without any delay.


Back Reset Default Delete Save

Figure 7-15: Edit AP Page (802.11a Radio Settings)

7. Click **Save** to save the BSAP radio settings to the BlueView database.
8. Click **Apply** from the Access Points page to apply the BSAP configuration you have edited to the BSAP's home BSC.

Deleting BSAP Configurations













To delete a BSAP configuration:

1. Click **Devices/Access Points** from any BlueView administrator console page.
A list of BSAPs connected to and configured by BSCs under management by BlueView appears (see Figure 7-12).
2. Click the  icon corresponding to the BSAP configuration you wish to delete.
A dialog appears prompting you to confirm the deletion.
3. Click **OK** to remove the BSAP configuration to the BlueView database.

Adding/Removing BSAP Configurations to/from a BSC

To add or remove BSAP configurations to or from a BSC:


1. Click **Devices/Controllers** from any Administrator Console page. The list of BlueSecure Controllers managed by BlueView appears as shown in Figure 7-16.

Actions	Status	Name	Address	Group	SNMP	un-sort	customize
<input type="checkbox"/>	All	All	All	All	All		un-filter
<input type="checkbox"/>   		192.168.100.143	192.168.100.143	Default	V3		
<input type="checkbox"/>   		192.168.100.142	192.168.100.142	Default	V3		
<input type="checkbox"/>   		wlan.eng.bluesocket.com	wlan.eng.bluesocket.com	Default	V3		
<input type="checkbox"/>   		192.168.100.135	192.168.100.135	Default	V3		

Check All | Clear All

4 rows [download](#)

Figure 7-16: BlueSecure Controllers List

2. Click the  icon corresponding to the BSC configuration you wish to edit.
3. The Edit Controller page appears.
4. Add or remove BSAP configurations to/from the BSC.
All BSAP Configurations on BSCs currently under management by BlueView are listed in the **Available Items** pane. Copy any of these configurations to the BSC by moving the configurations to the **Selected Items** pane.
Select one or more BSAP configurations from the **Available Items** list to copy to the BSC, and then click **add Highlighted Items**.
To add all available BSAP configurations to the BSC, simply click **Add all items in list**.
To remove BSAP configurations from the BSC, select the BSAP configurations in the Selected Items pane, and then click **Remove highlighted items**. Click **Remove all items in list** to delete all BSAP configurations on the BSC.
5. Click **Save** to save the BSC configuration changes you have made.

Creating a BSAP Configuration Template

BlueView enables you to simplify and speed up the BSAP configuration process by creating templates to configure a BSAP's identification and radio settings.

To create or edit a BSAP configuration template:

1. Click **Devices/AP Templates** from any Administrator Console page.
If no BSAP configuration templates have been created, the Create new AP template page appears. If you have already created one or more templates, click the pencil



icon for the template you want to edit. The Edit AP Template page appears, for example as shown in Figure 7-17.

If BSAP configurations have been created, click **Add** to add a new template to the list of configuration templates before the Create new AP template page appears.

Figure 7-17: Editing a BSAP Configuration Template

2. Mark the **Setup** radio button and then configure the BSAP identification settings as described starting in “Editing BSAP Identification Settings” on page 7-28.
3. Mark the **802.11 a** radio button and then configure the BSAP 802.11a radio settings as described starting in “Editing 802.11a Radio Settings” on page 7-34.
4. Mark the **802.11 b/g** radio button and then configure the BSAP 802.11 b/g radio settings as described starting in “Editing 802.11b/g Radio Settings” on page 7-29.
5. Optional. Enter a meaningful description of the BSAP configuration in the **Notes** field.
6. Click **Save** to save the BSAP configuration template to the BlueView database.

The newly created BSAP configuration template is added to the list of templates displayed on the AP templates page.

You may manage the BSAP configuration templates listed on the AP templates page by clicking the  icon corresponding to a template you wish to delete or clicking the  icon corresponding to a template you wish to edit.

Refer to the section entitled “Editing BSAP Identification Settings” on page 7-28 to apply a configuration template to a BSAP.

Managing BSAP SSIDs

A Service Set Identifier (SSID) is an identifier that is attached to packets sent over the wireless LAN and functions as a password for joining a particular radio cell, i.e. WLAN. All wireless clients must use a BSAP’s assigned SSID to associate with the BSAP.

After you have discovered BlueSecure Controllers or manually added BlueSecure Controllers to the BlueView managed device list, any SSIDs on the BSCs under BlueView

management will be listed on the AP SSIDs page. You can manage BSAP SSIDs from BlueView, by:

- Listing BSAP SSIDs
- Editing BSAP SSIDs
- Adding BSAP SSIDs
- Deleting BSAP SSIDs
- Adding/Removing SSID Configurations to/from a BSC

Listing BSAP SSIDs

Click **Devices/AP SSIDs** from any BlueView administrator console page to see a list off SSIDs configured on BSCs under management by BlueView as shown in Figure 7-18.










Actions	In Sync	Enabled	SSID	VLAN	Home Controller	un-sort customize		
<input type="checkbox"/>								
<input type="checkbox"/>  	Yes	Yes	Default	0	192.168.100.135			
<input type="checkbox"/>  	Yes	Yes	mySSID66	66	192.168.100.144			
<input type="checkbox"/>  	Yes	Yes	JMnet	0	192.168.100.29			
<input type="checkbox"/>  	Yes	Yes	jby	0	192.168.100.144			
Check All Clear All					<input type="button" value="Apply"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Delete"/>
4 rows								


Figure 7-18: Displaying BSAP SSIDs

The following information is displayed for SSIDs:

- **In Sync** - Does the SSID configuration stored on BlueView match the configuration on BSCs under management by BlueView? Yes or No. If the configurations are out of sync, then click to synchronize the configurations.
- **Enabled** - Is the SSID configuration enabled for use? Yes or No.
- **SSID** - The configured SSID name.
- **VLAN** - The virtual LAN assigned to the SSID.
- **Home Controller** - BSC on which SSID configuration is stored.

Click the  icon to edit an SSID configuration as described in the next section.

Click to apply an SSID configuration you have edited and saved on BlueView.

Click or to selectively enable or disable SSIDs. Click  or to delete an SSID configuration.

Click to reset the selected SSID configurations. Resetting an SSID configuration means that the configuration is deleted locally on BlueView and then updated with the first matching configuration (i.e., a configuration having a matching Service Set Identifier) found on a BSC under management by BlueView. If no matching SSID is found, then the SSID configuration remains deleted on BlueView.

Editing BSAP SSIDs

As part of the SSID configuration, you must define how wireless clients connecting to the BSAP are to be authenticated and how data transmitted from the BSAP is to be encrypted. You should familiarize yourself with the BSAP authentication and data encryption options before editing the BSAP SSID configuration.

BSAP Authentication Options

Possible BSAP authentication options are:

- **Open System** - The BSAP is configured by default as an “open system,” that broadcasts a beacon signal including the configured SSID. Wireless clients can read the SSID from the beacon, and automatically reset their SSID to allow immediate connection to the nearest BSAP.
- **Shared Key** - Sets the BSAP to use WEP shared keys. If this option is selected, you must configure at least one key on the BSAP and all clients.
- **WPA** - Wi-Fi Protected Access (WPA) provides improved data encryption, which was weak in WEP, and user authentication, that was largely missing in WEP. WPA uses the following security mechanisms.
 - Temporal Key Integrity Protocol (TKIP). TKIP provides data encryption enhancements including per-packet key hashing (i.e., changing the encryption key on each packet), a message integrity check, an extended initialization vector with sequencing rules, and a re-keying mechanism.
 - Enterprise-level User Authentication via 802.1x and EAP - To strengthen user authentication, WPA uses 802.1x and the Extensible Authentication Protocol (EAP). Used together, these protocols provide strong user authentication via a central RADIUS authentication server that authenticates each user on the network before they join it. WPA also employs “mutual authentication” to prevent a wireless client from accidentally joining a rogue network.

When the Authentication Type is set to WPA, clients are authenticated using 802.1x via a RADIUS server. Each client has to be WPA-enabled or support 802.1x client software. A RADIUS server must also be configured and be available in the wired network.

With this authentication type, keys are generated for each wireless client associating with the BSAP. These keys are regenerated periodically, and also each time the wireless client is re-authenticated.

- **WPA-PSK** - For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the BSAP and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks. When the WPA mode is set to “pre-shared-key,” the key must first be generated and distributed to all wireless clients before they can successfully associate with the BSAP.
- **WPA2** - Wi-Fi Protected Access 2 (WPA2) is the second generation of WPA security and is based on the final IEEE 802.11i amendment to the 802.11 standard.

When the Authentication Type is set to WPA2, clients are authenticated using 802.1x via a RADIUS server. Each client has to be WPA2-enabled or support 802.1x client software. A RADIUS server must also be configured and be available in the wired network.

With this authentication type, keys are generated for each wireless client associating with the BSAP. These keys are regenerated periodically, and also each time the wireless client is re-authenticated.
- **WPA2-PSK** - The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the BSAP and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks. When

the WPA2 mode is set to "pre-shared-key," the key must first be generated and distributed to all wireless clients before they can successfully associate with the BSAP.

- **WPA + WPA2** - Use both WPA and WPA2 authentication as described above.
- **WPA-PSK + WPA2-PSK** - Use both WPA-PSK and WPA2-PSK authentication as described above.

BSAP Data Encryption Options

Possible BSAP data encryption options are:

- **WEP** - Wired Equivalent Privacy (WEP) WEP provides a basic level of security, preventing unauthorized access to the network and encrypting data transmitted between wireless clients and the BSAP. WEP uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. Unfortunately, WEP has been found to be seriously flawed and cannot be recommended for a high level of network security.

Setting up shared keys enables the basic IEEE 802.11 Wired Equivalent Privacy (WEP) on the BSAP to prevent unauthorized access to the network.

If you choose to use WEP shared keys instead of an open system, be sure to define at least one static WEP key for user authentication and data encryption. Also, be sure that the WEP shared keys are the same for each client in the wireless network.

- **AES-OCB** - Advanced Encryption Standard - Offset Code Book (AES-OCB). This new encryption standard is a version of the AES standard recently adopted by the U.S. government as the replacement for 3DES. WPA specifies AES encryption as an optional alternative to TKIP and WEP. AES provides very strong encryption using a completely different ciphering algorithm to TKIP and WEP. The developing IEEE 802.11i wireless security standard has specified AES as an eventual replacement for TKIP and WEP. However, because of the difference in ciphering algorithms, AES requires new hardware support in client network cards that is currently not widely available.
- **AES-CCM** - AES-CCM mode is an alternative mode to OCB mode for AES encryption. CCM mode is the combination of Cipher Block Chaining Counter mode (CBC-CTR mode) and CBC Message Authenticity Check (CBC-MAC). The functions are combined to provide encryption and message integrity in one solution.
- **CKIP** - CKIP (Cisco Key Integrity Protocol) - Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- **TKIP** - Temporal Key Integrity Protocol (TKIP): WPA specifies TKIP as the data encryption method to replace WEP. TKIP avoids the problems of WEP static keys by dynamically changing data encryption keys. Basically, TKIP starts with a master (temporal) key for each user session and then mathematically generates other keys to encrypt each data packet. TKIP provides further data encryption enhancements by including a message integrity check for each packet and a re-keying mechanism, which periodically changes the master key.


SSID Editing Procedure

To edit a BSAP SSID configuration:

1. Click **Devices/AP SSIDs** from any BlueView administrator page. A list of SSIDs configured on BSCs under management by BlueView appears (see Figure 7-18).

The screenshot shows the 'Edit SSID: Default' configuration page. At the top, there are buttons for 'Back', 'Reset', 'Delete', and 'Save'. Below these are two checked checkboxes: 'Enable by default on the b/g radio' and 'Enable by default on the a radio'. The 'General Settings' section contains 'SSID' (Default) and 'VLAN' (0) fields. The 'Broadcast SSID' section has a checked 'Enable' checkbox. The 'Edge-to-Edge' section has an unchecked 'Enable' checkbox. The 'Standby Mode' section has an unchecked 'Enable this SSID ONLY when BSC connectivity is lost' checkbox. The 'Security Types' section has 'Authentication Type' set to 'Open System' and 'Cipher Type' set to 'Disabled'. The 'BSAP-1540 and BSAP-1500' section has 'Default QoS for SSID' set to 'Best Effort' and a checked 'Use WMM to apply QoS' checkbox. At the bottom, there is a 'Notes' text area and another set of 'Back', 'Reset', 'Delete', and 'Save' buttons.

Figure 7-19: Edit SSID Page

2. Click the  icon corresponding to the SSID configuration you wish to edit. The Edit SSID page appears as shown in Figure 7-19.
3. Mark **Enable by default on the b/g radio** to enable this SSID for radio b/g.
4. Mark the **Enable by default on the a radio** checkbox to enable this SSID for radio a.
5. Mark the **Enable SSID** checkbox to enable the Service Set Identifier and make it available for assignment to a BSAP you have created.
6. Enter the Service Set Identifier in the **SSID** field that all wireless clients must use to associate with the BSAP.
The SSID is case sensitive and can consist of up to 32 alphanumeric characters (0 means no VLAN, Range 2 to 4095).
7. Optional. Enter a VLAN identifier in the **VLAN** field.
Entering a VLAN ID enables VLAN tagging support on the BSAP. If enabled, the BSAP will tag traffic passing from wireless clients to the BSC with the VLAN ID.
8. Optional. Mark the **Enable** checkbox to broadcast the BSAP's SSID.
When enabled, the BSAP will include its SSID in beacon messages, and it will respond to probe requests from clients that do not include the correct SSID. You can

disable this option to hide the BSAP's SSID to prevent access to clients without a pre-configured SSID. (Default: Enabled, i.e. the BSAP's SSID is broadcast in the clear)

9. If **Edge-to-Edge** is enabled, wireless traffic will not be tunneled through the BSC. This can compromise security and should be used with caution. Client to client traffic will not be blocked.
10. **Standby Mode** - Mark to indicate that this SSID should only be enabled if BSC connectivity is lost.
11. Define how the BSAP is to authenticate users by selecting an authentication method from the **Authentication Type** drop-down menu. Possible BSAP authentication methods are:
 - Open System
 - Shared Key
 - WPA (Wi-Fi Protected Access)
 - WPA-PSK (Wi-Fi Protected Access with Pre-Shared Key)
 - WPA2 (Wi-Fi Protected Access 2)
 - WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key)
 - WPA + WPA2
 - WPA-PSK + WPA2-PSK

See "BSAP Authentication Options" on page 7-38 for descriptions of these options.

12. Define how data transmitted from the BSAP is to be encrypted by selecting a data encryption method from the **Cipher Type** menu. Possible BSAP data encryption methods are:
 - WEP (Wired Equivalent Privacy)
 - AES-OCB (Advanced Encryption Standard - Offset Code Book)
 - AES-CCM (Advanced Encryption Standard - in Counter with CBC-MAC)
 - CKIP (Cisco Key Integrity Protocol)
 - TKIP (Temporal Key Integrity Protocol)

See "BSAP Data Encryption Options" on page 7-40 for descriptions of these options.

13. (*Shared Key Authentication only*) If you have configured Shared Key authentication, then you must define the WEP shared keys the BSAP is to use.
 - a) Select the key length from the **WEP Key Size** drop-down menu.

Note that the same size of encryption key must be supported on all wireless clients. (11b/g: 64/128 Bits; 11a: 64/128/152 Bits)
 - b) Enter keys as 10 hexadecimal digits (0 to 9 and A to F) for 64 bit keys, 26 hexadecimal digits for 128 bit keys, or 32 hexadecimal digits for 152 bit keys. Be sure to specify a default key (0 to 3) when entering 64-bit keys.
14. (*WPA or WPA2 Authentication only*) If you have configured WPA or WPA2 authentication, then you must configure access to the RADIUS authentication server that is to authenticate each user on the network before the user is able to join it.
 - a) Enter IP address or fully qualified domain name of the RADIUS server in the **Address** field.
 - b) Enter the RADIUS server's port number in the **Port** field.
 - c) Enter the known secret shared between the BSAP and the RADIUS authentication server in the **Secret** field, and then confirm the shared secret by entering it in the **Confirm secret** field.
 - d) (For BSAP-15x0 only) Mark the **Enable 802.11i preauth bit** checkbox to enable clients to establish an 802.11i Pairwise Master Key (PMK) security association to

- a BSAP (configured with this SSID) with which the client has yet not been associated.
15. (*WPA-PSK or WPA2-PSK Authentication only*) If you have configured WPA-PSK or WPA2-PSK authentication, then you must configure the key that all wireless clients will use to communicate with the BSAP.
 - a) Enter the interval in minutes at which the WPA group key is to be regenerated in the **Rekey Time** field.
 - b) Enter the WPA pre-shared key in the **Passphrase** field, and then enter the same pre-shared key in the **Confirm passphrase** field.
Enter a key as an easy-to-remember string of letters and numbers. The string must be from 8 to 63 characters and can include spaces.
 16. (BSAP-15x0 only) Define the default Quality of Service the BSAP is to apply by selecting a class of service option from the **Default QoS for SSID** drop-down menu. Best Effort is the default QoS setting. Select Voice when this SSID handles IP Phone traffic.
Alternatively, mark the **Use WMM** checkbox to use the Wi-Fi multimedia QoS settings that have been defined on the BSC using the Global Settings page.
 17. Click **Save** to save the BSAP SSID settings to the BlueView database.
 18. Click from the SSIDs page to apply the SSID configuration edits to the BSC on which the configuration resides.


Adding BSAP SSIDs

To add a BSAP SSID configuration:

1. Click **Devices/AP SSIDs** from any BlueView administrator console page.
A list of SSIDs configured on BSCs under management by BlueView appears (see Figure 7-18).
2. Click to create a new SSID configuration.
The Edit SSID page appears.
3. Complete the Edit SSID page settings, following the instructions for the Create New SSID page described in the previous section (the Edit SSIC page is identical to the Create New SSID page).
4. Click **Save** to save the BSAP SSID configuration to the BlueView database.
5. Click from the SSIDs page to add the SSID configuration to the selected BSC.

Deleting BSAP SSIDs

To delete a BSAP SSID configuration:

1. Click **Devices/AP SSIDs** from any BlueView administrator console page.
A list of SSIDs configured on BSCs under management by BlueView appears (see Figure 7-18).
2. Click the  icon corresponding to the SSID configuration you wish to delete.
A dialog appears prompting you to confirm the deletion.
3. Click **OK** to remove the BSAP SSID configuration to the BlueView database.

Adding/Removing SSID Configurations to/from a BSC

To add or remove SSID configurations to or from a BSC:

1. Click **Devices/Controllers** from any Administrator Console page.

The list of BlueSecure Controllers under management by BlueView appears as shown in Figure 7-20.

Actions	Status	Name	Address	Group	SNMP	un-sort	customize
<input type="checkbox"/>	All	All	All	All	All		un-filter
<input type="checkbox"/>		192.168.100.143	192.168.100.143	Default	V3		
<input type="checkbox"/>		192.168.100.142	192.168.100.142	Default	V3		
<input type="checkbox"/>		wlan.eng.bluesocket.com	wlan.eng.bluesocket.com	Default	V3		
<input type="checkbox"/>		192.168.100.135	192.168.100.135	Default	V3		

Check All | Clear All | Delete

4 rows [download](#)

Figure 7-20: BlueSecure Controllers List

- Click the icon corresponding to the BSC configuration you wish to edit.
- Add or remove SSID configurations to/from the BSC.
All SSID Configurations on BSCs currently under management by BlueView are listed in the **Available Items** pane, as shown in Figure 7-21. You may copy any of these configurations to the BSC by moving the configurations to the **Selected Items** pane. Select one or more SSID configurations from the **Available Items** list to copy to the BSC, and then click **add Highlighted Items**.
To add all available SSID configurations to the BSC, simply click **Add all items in list**.
To remove SSID configurations from the BSC, select the SSID configurations in the Selected Items pane, and then click **Remove highlighted items**. Click **Remove all items in list** to delete all SSID configurations on the BSC.
- Optional. Mark the **Automatically add newly created SSID configs to this controller** checkbox to enable BlueView to send any SSID configurations that are added to BlueView to the Controller automatically.
- Click **Save** to save the BSC configuration changes you have made.

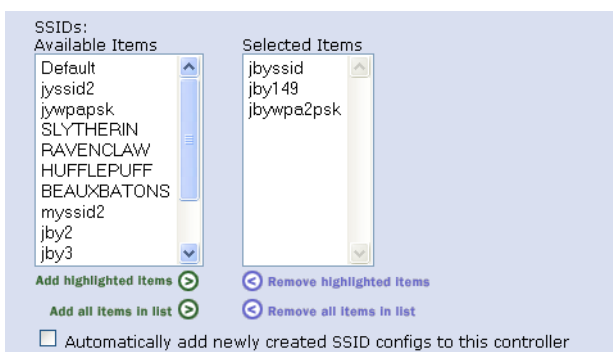


Figure 7-21: Edit Controller Page

8

Configuring RF Intrusion Detection and Containment

This chapter provides procedures for configuring BlueView to perform RF intrusion detection and containment services using the BSAPs operating in sensor mode, and includes:

- Overview
- Identifying Authorized RF Stations on Your Network
- Configuring Sensor Alarms and RF Autocontainment
- Defining Approved SSIDs
- Importing Bulk RF Configuration Data Files
- Exporting Bulk RF Configuration Data Files

Overview

The BlueView Management System detects and protects against rogue devices, ad-hoc networks, and a large number of WLAN Denial of Service (DoS) and spoofing attacks.

BlueView provides RF intrusion detection by analyzing the data collected from BSAPs operating in dual AP/sensor mode or sensor-only mode to detect attacks, vulnerabilities, and rogue devices in the protected RF space.

Should a rogue AP or client be discovered, BlueView configures the BSAP nearest the rogue device to initiate containment using 802.11 de-authentication and/or disassociation messages. Up to five Bluesocket devices can participate in the containment if range permits. The BSAPs participating in the RF containment remain online for wireless access during the containment period.

All RF IDS alarms issued by a Bluesocket BSAP automatically generate a corresponding SNMP trap message and syslog message.

Identifying Authorized RF Stations on Your Network

To better track rogue devices on your network, BlueView enables you to create a “white list” of known authorized RF stations. RF devices not appearing on the authorized list will be identified as rogue or intruding devices.

To add an RF device to BlueView’s list of known authorized RF stations:

1. Click **RF Sensor/Stations** from any Administrator Console page.
A list of previously configured authorized RF stations appears.
2. Click to add an RF station to the authorized list.

The Create New Station Configuration page appears as shown in Figure 8-1.

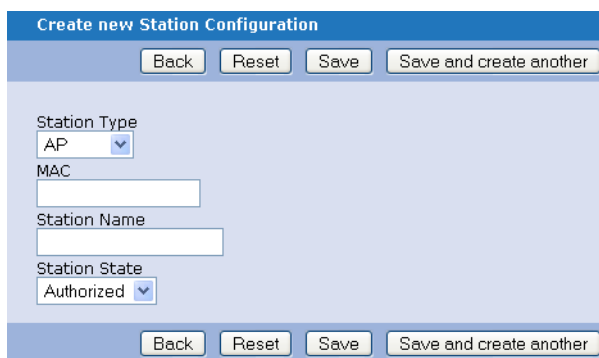


Figure 8-1: Create New Station Configuration Page

3. Identify the station by selecting one of the following device types from the **Station Type** menu:
 - AP - The RF station is an access point.
 - Ad Hoc - The RF station is communicating in an ad hoc mode, i.e., a peer-to-peer connection mode in which wireless PC cards communicate directly with one another.
 - Client - The RF station is a wireless client.
4. Enter the RF station’s Media Access Code address in the **MAC address** field.

Acceptable MAC address delimiters are colons (00:03:4a:3b:4f:02) or hyphens (00-03-4a-3b-4f-02).

5. Enter a meaningful name for the RF station in the **Station Name** field.
6. Select the authorization level for the RF station from the **Station State** drop-down menu:
 - **Authorized** - This station is authorized to be on the network and no alarms will be generated if it is detected.
 - **Rogue** - This station is not authorized to be on the network and an alarm will be generated if it is detected.
 - **Neighbor** - This station is not part of the internal network, but is always present.
 - **Ignore** - Ignore this station and do not generate an alarm if this station is detected on the network.
7. Click **Save** to save the RF station settings to the BlueView database.

Configuring Sensor Alarms and RF Autocontainment

By default, the BSAPs operating in sensor mode are configured to issue alarms on 22 different WLAN security threats. You can configure how BlueView processes these alarms by selectively disabling alarms and setting the severity level associated with the alarm.

The following table describes the RF sensor alarms that are configurable with this release of BlueView.

Table 8-1: RF Sensor Alarms

Alarm	Description	Dual/Sensor Mode
Adhoc SSID same as AP	A mobile station in Adhoc mode is using an approved AP SSID.	D
AirJack Attack	Airjack is a toolset that allows attackers to inject fake 802.11 packets in order to gain network access or create a DoS attack. Information on the tool and its variant (wlan-jack, monkey-jack, ssid-jack, cracker-jack) can be found here: http://sourceforge.net/projects/airjack/	S
AP Broadcasting Multiple SSID	The AP is broadcasting multiple SSIDs. This can indicate a spoof attempt	S
AP Channel Change	The Access Point has changed channels.	D
AP Denied Association	An authorized AP denied an association request from client.	D
AP Denied Authentication	An authorized AP denied client access due to authentication failure.	D
AP Down	The AP is down.	S
AP in WDS Mode	AP is operating in WDS (bridge) mode.	D
AP Low Signal Strength	An AP with low signal strength is detected by BAP sensor.	S
AP Overloaded	An overloaded AP refuses new clients from associating with it.	D
AP Restarted	The AP has restarted.	S
AP SSID Changed	An AP has changed its SSID, if this was not authorized then there is a possible spoof in progress.	D
AP Using Default SSID	The Access Point is using its factory default SSID. This may indicate a mis-configured AP and it should be changed to an SSID appropriate to the installation.	D
AP Using Hotspot SSID	An AP is using a hotspot SSID.	D
ASLEAP Attack	ASLEAP is a tool that exploits a weakness in CISCO proprietary LEAP protocol.	S
Authorized AP Down	An authorized Access Point can no longer be heard by the sensor. This may indicate that the AP has failed or been Removed from service.	D

Table 8-1: RF Sensor Alarms

Alarm	Description	Dual/ Sensor Mode
Broadcast Attack	Many attacks use broadcast disassociate or deauthenticate frames to disconnect all users on the network, either to redirect them to a fake network or to cause a Denial of Service attack or disclose a cloaked SSID.	S
Client Association Change	Client has changed its association to a different Access Point. This might be due to a Rogue AP in the vicinity.	D
Client BSSID Changed	Mobile station has changed its BSSID.	D
Client Limit	Maximum client limit per AP has been reached. Could be due to a MAC spoofing client or real network density increase.	D
Client Rate Support Mismatch	Specified mandatory data rate in Probe Request does not match with the values advertised by the AP.	D
Client To Rogue AP	An authorized client is connected to a rogue AP.	D
Deauthentication Flood	An attacker is conducting a Denial of Service (DoS) attack by flooding the network with 802.11 de-authentication frames in an attempt to disconnect users from Access Points. This can result in a Denial of Service (DoS) attack	S
Disassociation Traffic	This alarm indicates that a client is continuing to send traffic within 10 seconds of being disassociated from an AP.	S
Duration Attack	An attacker sends 802.11 frame with 0xFF in the duration field. This forces other mobile nodes in the range to wait till the value reaches zero. If the attacker sends continuous packets with huge durations, it prevents other nodes from operating for a long time, results in an Denial-of-Service attack.	S
EAPOL ID Flood	Attacker tries to bring down an AP by consuming the EAP Identifier space (0-255).	S
EAPOL Logoff Storm	An attacker floods the air with EAPOL logoff frames. It may result in Denial of Service to all legitimate stations.	S
EAPOL Spoofed Failure	Spoofed EAP failure messages detected.	S
EAPOL Spoofed Success	Spoofed EAP success messages detected.	S
EAPOL Start Storm	Attacker floods air with EAPOL start frames; may result in Denial of Service to all legitimate stations.	S
Fata-Jack Attack	A Fata-jack device sends an authentication failure packet to a mobile node to prevent the client from getting any WLAN services.	S
Invalid Deauthentication Code	Unknown deauthentication reason code. Some access points and drivers can not handle improper reason codes.	D
Invalid Disconnect Code	Unknown disassociation reason code. Some access points and drivers can not handle improper reason codes.	D
Invalid Probe Response	An Access Point has responded to a client probe with a 0-length SSID, which is an invalid response which has been shown to create a fatal error with some client cards. This could be a faulty AP or an attacker specifically crafting the packet to disrupt the network.	D
Link Test	Some Lucent/Orinoco/Proxim/Agere products provide link testing capability which could use network bandwidth.	D
MSF Broadcom Exploit	MSF-style poisoned exploit packet for Broadcom drivers, this can be used for client hijacking.	D
MSF D-Link Exploit	MSF-style poisoned 802.11 rate field in beacon for D-Link driver, this can be used for client hijacking.	D
MSF Netgear Exploit	MSF-style poisoned 802.11 over-sized options beacon for Netgear driver attack, this can be used for client hijacking.	S
Netstumbler Probe	Netstumbler is a wireless network scanning tool available for download at: http://www.netstumbler.com . This could be the precursor to a more serious attack	D
Network Probe	A Client is probing the network looking for a wireless AP, but is not connecting. Many wireless cards and operating systems (i.e. Windows XP) do this by default in an attempt to automatically find Access Points, but this could be an operational issue indicating a misconfigured client because it cannot associate	D

Table 8-1: RF Sensor Alarms

Alarm	Description	Dual/Sensor Mode
Possible AP Spoof	A BSS timestamp mismatch in beacon or probe frames is likely to indicate an attempt to spoof the BSSID or SSID of an AP.	S
Rogue Client	A rogue client has been detected.	D
Rogue Client To AP	A rogue client is connected to an authorized AP.	D
Rogue AP	A Rogue AP has been detected. Check that this is not a newly installed Access Point or an AP belonging to a nearby organization.	D
Rogue Ad-Hoc Client	A rogue client in Ad-Hoc mode has been detected.	D
Spoofed MAC Address	A spoofed MAC address has been detected. If you are using any MAC-based authentication/access control, the user may be attempting to bypass this protection or hijack another user's session	D
SSID too long	SSID length exceeds 32 bytes which is larger than allowed by the 802.11 standard. This is indicative of a SSID handling exploit.	D
Unapproved Manufacturer	A device is from a unapproved manufacturer.	D
Using Unauthorized SSID	An authorized client is using an unauthorized SSID.	D
Wellenreiter Probe	Wellenreiter is a wireless network scanning tool available for download at: http://www.wellenreiter.net/ .	D
WEP Disabled	An AP is not using WEP encryption.	D

To configure how BlueView processes alarms issued by RF sensors on your network:

1. Click **RF Sensor/Alarms** from any Administrator Console page, and then click in the navigation pane.

The list of configured RF sensor alarms appears as shown in Figure 8-2.

Actions	Name	Enabled	Severity	Auto Containment	un-sort	customize
<input type="checkbox"/>	All	All	All	All		un-filter
<input type="checkbox"/>	Deauthentication Flood	Enabled	Severe	Disabled		
<input type="checkbox"/>	Link Test	Enabled	Informational	Disabled		
<input type="checkbox"/>	Wellenreiter Probe	Enabled	Informational	Disabled		
<input type="checkbox"/>	Broadcast Attack	Enabled	Severe	Disabled		
<input type="checkbox"/>	AirJack Attack	Enabled	Severe	Disabled		
<input type="checkbox"/>	Disassociation Attack	Enabled	Severe	Disabled		
<input type="checkbox"/>	AP Channel Change	Enabled	Warning	Disabled		
<input type="checkbox"/>	Possible AP Spoof	Enabled	Warning	Disabled		
<input type="checkbox"/>	Network Probe	Enabled	Informational	Disabled		
<input type="checkbox"/>	Invalid Probe Response	Enabled	Informational	Disabled		

[Check All](#) | [Clear All](#) | [Enable Alert Type](#) | [Disable Alert Type](#) | [Enable Auto Containment](#) | [Disable Auto Containment](#)

10 rows on page

52 total rows [download](#) [next >](#) Page Rows per page

Figure 8-2: Configured RF Sensor Alarms

2. Click [Enable](#) or [Disable](#) to enable or disable the selected alarm(s).
3. Click to edit the severity level associated with the corresponding alarm.

The Edit Alarm Configuration page appears for the alarm, for example the the Deauthentication Flood alarm as shown in Figure 8-3.

Mark the **Enable** checkbox and then specify the severity level you wish to associate with the alarm by marking the appropriate radio button:

- **Severe** - This is the highest alert level and is usually associated with a WLAN intrusion, e.g., a broadcast attack.
- **Warning** - This alert level is usually associated with a security vulnerability, e.g., a client association change.
- **Informational** - This alert level is usually associated with a change in network operational status, e.g., an authorized AP is down.

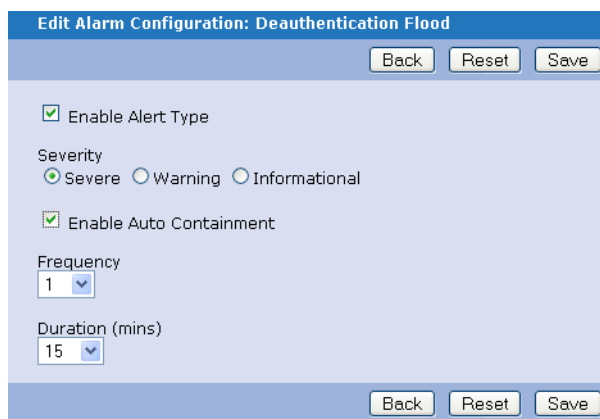


Figure 8-3: Edit Alarm Configuration Page

4. Configure RF Autocontainment

Any rogue device that triggers an alarm can be automatically “contained”, i.e. blocked, i.e., contain rogue RF devices. If you enable the BlueView’s autocontainment feature for this alarm, and a rogue AP or client is detected within your protected airspace, BlueView configures the BSAP (operating in sensor or dual mode) nearest the rogue device to initiate containment using 802.11 de-authentication and/or disassociation messages. Up to five RF sensors can participate in the containment if range permits. Any BSAPs participating in the RF containment remain online for wireless access during the containment period.

To configure RF Autocontainment

- a) Mark the **Auto Containment** checkbox to enable the BlueView’s RF autocontainment feature for this alarm.
- b) Select the **Frequency**, i.e., successive times BlueView will perform autocontainment on a rogue device, from the Frequency drop-down menu.
- c) Select the duration (in minutes) that BlueView will perform active containment on the rogue device from the **Duration** drop-down menu.

See “Monitoring Devices in RF Autocontainment” on page 6-34 for information about displaying a list of devices currently in active containment.



Note: BlueView will perform active containment using BSAPs operating in sensor or dual mode.

5. Click **Save** to save the alarm configuration settings to the BlueView database.

Defining Approved SSIDs

You can define the Service Set Identifiers (SSIDs) approved for use in the coverage area of the BSAPs operating in Sensor or Dual mode. The BSAP will generate an alarm for any wireless client or access point that broadcasts a non-approved SSID.

To define Service Set Identifiers approved for use in the BSAP's coverage area:

1. Click **RF Sensor/Approved SSIDs** from any Administrator Console page.
The list of configured approved SSIDs appears.
2. Click **Add** to add an approved SSID.
The Create new Assid Configuration page appears as shown in Figure 8-4.

Figure 8-4: Create New SSID Configuration Page

3. Enter the approved Service Set Identifier in the **Approved SSID** field.
4. Click **Save** to save the approved SSID configuration settings to the BlueView database.

Defining Manufacturer MAC Addresses

1. Click **RF Sensor/Manufacturer-MAC** from any Administrator Console page.
The list of configured approved Manufacturer MAC addresses appears.
2. Click **Add** to add an approved Manufacturer MAC address.
The Create new Manufacturer MAC Configuration page appears as shown in Figure 8-4.

Figure 8-5: Create New Manufacturer MAC Configuration Page

Creating New Hotspot SSID Configuration

1. Click **RF Sensor/Hotspot-SSID** from any Administrator Console page.
The list of configured approved Hotspot SSIDs appears.
2. Click **Add** to add an approved Hotspot SSID.

The Create new Hotspot SSID Configuration page appears as shown in Figure 8-4.

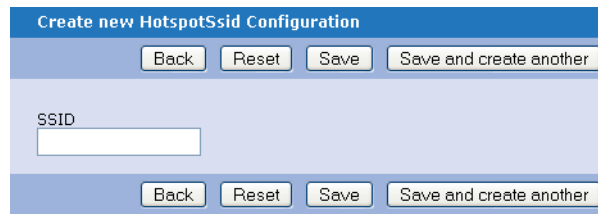



Figure 8-6: Create New Hotspot SSID Configuration Page

Importing Bulk RF Configuration Data Files

You can import bulk RF configuration data files to simplify and speed up the BlueView RF IDS and containment configuration process:

 **Note:** You can only import .CSV formatted files to the BlueView database.

To import a bulk RF configuration data file into the BlueView database:

1. Click **RF Sensor/Bulk Import** from any Administrator Console page.
The Bulk Import page appears as shown in Figure 8-7.

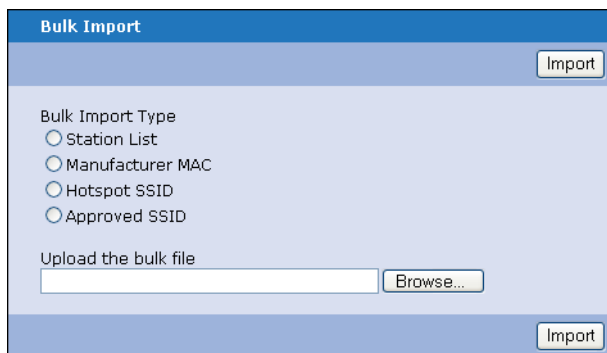


Figure 8-7: Bulk RF Configuration Data Import Page

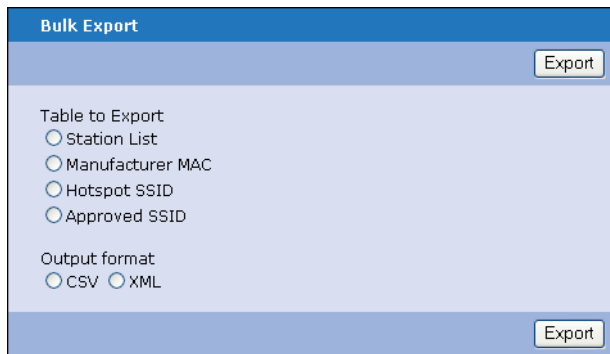
2. Mark the radio button corresponding to the type of configuration data you wish to import:
 - **Station List**
 - **Manufacturer MAC**
 - **Hotspot SSID**
 - **Approved SSID**
3. Click **Browse** and select the .CSV formatted file to import.
4. Click **Import** to import the specified file to the BlueView database.

Exporting Bulk RF Configuration Data Files

You can import bulk RF configuration data files to simplify and speed up the BlueView RF IDS and containment configuration process:

To export a bulk RF configuration data file from the BlueView database:

1. Click **RF Sensor/Bulk Export** from any Administrator Console page.
The Bulk Export page appears as shown in Figure 8-8.



The screenshot shows a web form titled "Bulk Export". The form is set against a light blue background. At the top, there is a dark blue header bar with the text "Bulk Export" in white. Below the header, there is a light blue area containing two sections. The first section is labeled "Table to Export" and contains four radio buttons: "Station List", "Manufacturer MAC", "Hotspot SSID", and "Approved SSID". The second section is labeled "Output format" and contains two radio buttons: "CSV" and "XML". There are two "Export" buttons: one in the top right corner and one in the bottom right corner of the form area.

Figure 8-8: Bulk Configuration Data Export Page

2. Mark the radio button corresponding to the type of configuration data you wish to export:
 - **Station List**
 - **Manufacturer MAC**
 - **Hotspot SSID**
 - **Approved SSID**
3. Mark the radio button corresponding to the file format in which the configuration data should be exported:
 - **CSV** - Export data to a comma separated values file.
 - **XML** - Export data to extensible markup language file.
4. Click **Export** to export the specified data table from the BlueView database.

9

Administering Your BlueView System

This chapter describes BlueView system software administration tasks including:

- Restarting, Rebooting, and Shutting Down BlueView
- Backing Up and Restoring the BlueView Database
- Upgrading to a New Version of Runtime Software
- Installing and Uninstalling Software Patches
- Switching Between BlueView Runtime Software Versions
- Running Diagnostics
- Capturing Network Traffic Data
- Accessing BlueView Functions via the BlueView Serial Port

Restarting, Rebooting, and Shutting Down BlueView

Many configuration settings in BlueView do not take effect until you restart certain services or reboot BlueView.

Additionally, you may need to restart BlueView services, reboot BlueView, or shut down BlueView manually for other system maintenance reasons.

As a matter of definition, restarting BlueView means that services running on BlueView are stopped and then restarted without interrupting power, dropping user connections or restarting the OS. Rebooting the BlueView means that BlueView is powered off and all network connections are dropped, and then BlueView is powered back on and its OS is restarted.

To restart BlueView services, reboot BlueView, or shut down BlueView manually:

1. Click **BlueView/Restart Services** from any administrator console page.
The BlueView restart page appears as shown in Figure 9-1.

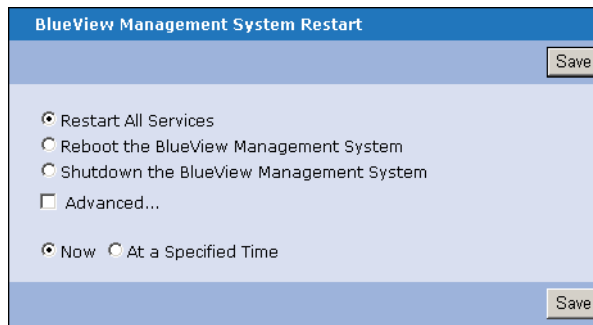


Figure 9-1: BlueView Management System Restart Page

2. Select the appropriate BlueView action by marking one of the following radio buttons:
 - **Restart All Services** - Restarts all BlueView services, but does not reboot the BlueView.
 - **Reboot BlueView** and **Shutdown BlueView** - Reboots and shuts down BlueView, respectively.
 - **Advanced** - If checked, you can choose to restart a single service: network interface, SNMP, logging, or sensor.
 - **Now** - Perform the selected action immediately.
 - **At a Specified Time** - Perform the selected action at the specified date and time. Use the **Time Shortcut** drop-down list or the **Year**, **Month**, **Day**, **Hour**, and **Minute** drop-down lists to specify the date and time.
3. Click **Save** to perform the BlueView action immediately or at the specified time.

Backing Up and Restoring the BlueView Database

All BlueView configuration information along with received BSC log and alarm data is stored in its internal database. We strongly recommended that you routinely back up the BlueView database, so that you can restore the original settings if the current database becomes corrupted or unusable.

- “Backing Up the BlueView Database” on page 9-3
- “Restoring the Database” on page 9-4
- “Creating a Debug File” on page 9-4
- “Resetting BlueView to its Default Settings” on page 9-4

We also recommend that you back up the firmware and patches you have installed so that the BlueView system software can be restored if it should become corrupted for some reason.

Backing Up the BlueView Database

To back up the BlueView database:

1. Click **BlueView/Configuration Backup/Restore** from any administrator console page. The Configuration Backup and Restore page appears as shown in Figure 9-2.

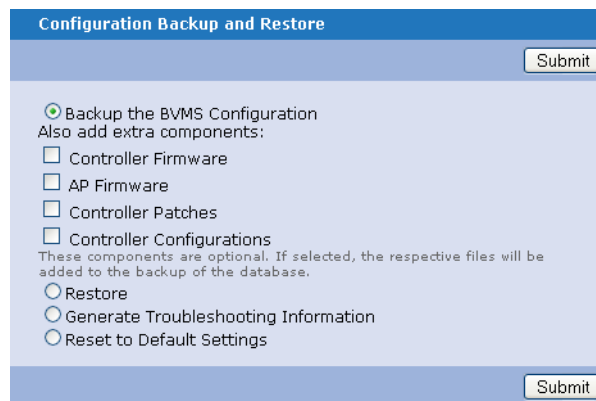


Figure 9-2: Configuration Backup and Restore Page

2. Mark the **Backup the BVMS Configuration** radio button and then mark the radio buttons next to any additional software components you wish to back up, **Controller Firmware**, **AP Firmware**, **Controller Patches**, or **Controller Configurations**.
3. Click **Save**.

BlueView creates the backup file as specified and then displays the following message on the right side of the page:

To backup the configuration select Backup the BVMS Configuration. When the backup is finished, download the .bvb file to your computer

Backups available for Download.

Host_Version_DateTime_backup.bvb

where Host_Version_DateTime_backup.bvb is a link to the backup file.

4. Click the link, and then specify a directory location on your computer where you want to download the .bvb file.

The BlueView database file is downloaded and saved with a .bvb file extension.



Caution: Never directly edit the BlueView database backup file, as doing so will corrupt the file. The backup file is around 1MB in size and can easily be mailed to Bluesocket Customer Support if required.

Restoring the Database

To restore the BlueView database from a configuration backup file:

1. Click **BlueView/Configuration Backup/Restore** from any administrator console page. The Configuration Backup and Restore page appears (see Figure 9-2).
2. Mark the **Restore** radio button.
3. Enter the pathname of the .bvb backup file in the **Restore** field or click **Browse** to search your computer's file system for the file.
4. Click **Save** to upload the backup file to the BlueView Management System to which you are connected.

As BlueView restores its database from the backup file, it displays the message:

BlueView backup restore in progress, please wait

You will be redirected to the login page when restore completes

The BlueView Management System reboots itself and you are directed to the administrator console login page.

5. Log into the administrator console using your username and password.

Creating a Debug File

If you encounter trouble configuring BlueView, you may contact Bluesocket customer support for assistance (See Appendix A, "Contacting Bluesocket, Inc.," for Customer Support contact information). Your Bluesocket customer support representative may ask you to send him a debug file that contains your BSC's configuration along with troubleshooting information.

To create a BlueView debug file:

1. Click **BlueView/Configuration Backup/Restore** from any administrator console page. The Configuration Backup and Restore page appears (see Figure 9-2).
2. Mark the **Generate Troubleshooting Information** radio button. A dialog appears prompting you to open or save the file.
3. Select **Save**, and then specify a directory location on your computer to which to store the file.

The debug/troubleshooting file is downloaded and saved with a .bvd file extension.



Caution: Never directly edit the BlueView debug file, as doing so will corrupt the file. The debug file is around 1MB in size and can easily be mailed to Bluesocket Customer Support.

Resetting BlueView to its Default Settings

You can reset BlueView to its default configuration (i.e. factory default settings) via the administrator console. Note that resetting BlueView to its default values also resets the default admin account to a password of blue and deletes all other administrator accounts.

To reset all BlueView configuration settings back to their default values:

1. Click **BlueView/Configuration Backup/Restore** from any administrator console page. The Configuration Backup and Restore page appears (see Figure 9-2).


2. Mark the **Reset to default settings** radio button, and then click **Reset**.
3. You are prompted to confirm your intention to restore BlueView’s default settings.
4. Click **OK**.
5. BlueView reboots. Upon completion of the reboot, all BlueView configuration settings are reset to their default values.


Upgrading to a New Version of Runtime Software

BlueView contains two runtime software images, A and B. One runtime image is active and the other image is in standby mode. When Bluesocket releases a new runtime version of BlueView software, you will need to upload it to your BlueView Management System.

When you upload a new runtime image:

- The runtime image that was active becomes the standby image.
- The uploaded runtime image becomes the new active image.

 **Note:** After uploading the new software image to BlueView, you will be able to login to the BlueView administrator console using only the default **admin** administrator account. Be sure you know the password for the **admin** account before upgrading BlueView to a new software image.

 **Note:** Before starting the upgrade, make sure that popups are allowed in your browser.

Before beginning the software upgrade, copy the new BlueView software image file to the computer on which you are running your web browser to connect to the BlueView administrator console.

To install a new runtime image on BlueView:

1. Back up your BlueView database as described on “Backing Up the BlueView Database” on page 9-3.
2. After the database is backed up, click **BlueView/Upgrade** from any administrator console page.

The BlueView update page appears as shown in Figure 9-3.

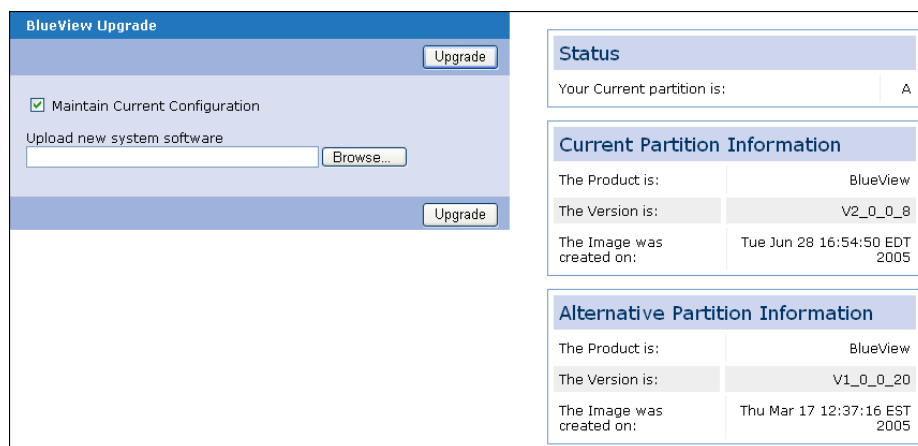


Figure 9-3: BlueView Update Page

The current active image, either A or B, is shown in boldface on the right side of the page.

3. Optional. Mark the **Maintain Current Configuration** checkbox to maintain the current database configuration while loading the new system software image.

If this checkbox is not marked, you will need to restore the database manually and then reboot BlueView after the runtime image uploads.

4. Enter the pathname of the new runtime image you wish to load onto BlueView in the **Upload new system software** field.
5. Click **Upgrade** to upload the runtime image to BlueView.

The size of the image is approximately 175 Mb, so the process may take some time to complete. If the upload is interrupted or cancelled, you must repeat this step.

Installing and Uninstalling Software Patches

Bluesocket may occasionally release small software fixes, known as patches. These are not the same as BlueView runtime software upgrades, which usually involve major changes in functionality or performance.

Also, unlike upgrades, patches overwrite just the changed files in the current runtime software, not the entire image. Finally, although a backup of the BlueView database is always recommended, it is not a pre-requisite for installing a patch.

When Bluesocket releases a new BlueView software patch, you will need to install it on your BlueView Management System.

Installing a Patch

To install a BlueView software patch:

1. Click **BlueView/Patch** from any administrator console page.
The Manage Patches page appears as shown in Figure 9-4.

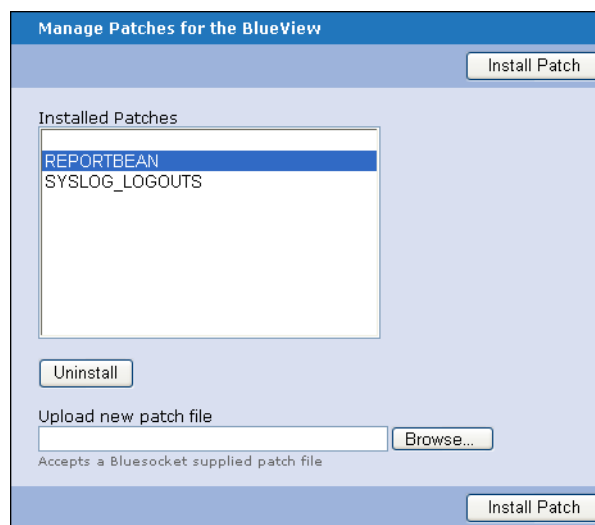


Figure 9-4: Manage Patches Page

Any previously installed patches are listed in the **Installed Patches** listbox.

2. Use the **Browse** button to enter the pathname where the patch file resides on your local computer in the **Upload new patch** field.
3. Click **Install Patch** to install the patch on BlueView.

The **Installed Patches** listbox will list the name of the patch when the installation is complete. To view patch information, such as release number and date, highlight the patch in the box, and then click **View**.



Note: Patches do not take effect until BlueView is rebooted.

Uninstalling a Patch

You may need to uninstall a patch if it doesn't provide the functionality updates you need for your BlueView Management System.

To uninstall a patch:

1. Click **BlueView/Patch** from any administrator console page.
The Manage Patches for BlueView page appears as shown in Figure 9-4.
2. Select the patch that you want to uninstall in the **Installed Patches** listbox.
3. Click **Uninstall** to remove the patch from BlueView.

Switching Between BlueView Runtime Software Versions

It is possible to switch between the currently active and standby versions of the BlueView runtime image. For example, if you find there is a problem with a recently uploaded runtime image, use this function to switch back to the standby image.

To switch between software runtime images:

1. Click **BlueView/Switch** from any administrator console page.
The BlueView switch page appears as shown in Figure 9-5.

Figure 9-5: BlueView Switch Page

The current active runtime image (A or B) is shown on the right of the page.

2. Mark the **Destination** radio button corresponding to the image, either **A** or **B**, that you want to switch to.
3. Click **Switch**.
BlueView will reboot automatically and come up running the selected image.

Running Diagnostics

The BlueView administrator console enables you to access several standard network diagnostic tests directly from your web browser including:

- ping - Use the standard Packet InterNet Groper utility to determine if BlueView can reach a specified IP address over a specified network interface.
- traceroute - Use the standard TCP/IP utility to determine the route packets are taking from BlueView to a specified host over a specified interface.
- netstat - List statistics about the network including socket status, interfaces that have been auto-configured, memory statistics, etc.
- arp - Use address resolution protocol to determine the Ethernet address of the BlueView's protected interface (eth0).

Additionally, you can execute these tasks from the BlueView administrator console running on your web browser:

- list the status (running/not running) of all BlueView processes

To run a network diagnostic test:

1. Click **BlueView/Diagnostics** from any administrator console page. The Task execution menu page appears as shown in Figure 9-6.

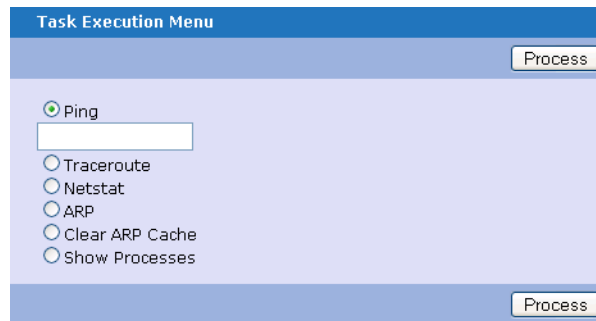


Figure 9-6: Task Execution Menu Page

2. Select a test to execute by marking the appropriate radio button.

Ping - Use the standard Packet InterNet Groper utility to determine if the BSC can reach a specified IP address over a specified network interface. Provide an IP address or fully qualified domain name for the target host and specify the originating Ethernet port on the BSC. Select Any to let the Controller decide based on routes.

Traceroute - Use the standard TCP/IP utility to determine the route packets are taking from the BSC to a specified host over a specified interface. Provide an IP address or fully qualified domain name for the target host and specify the originating Ethernet port on the BlueView, Ethernet 1 or Ethernet 2. Select Any to let the BVMS decide based on routes.

Netstat - List statistics about the network including socket status, interfaces that have been auto-configured, memory statistics, etc.

ARP - Use address resolution protocol to determine the Ethernet address of the BSC's protected interface (eth0).

Clear ARP Cache - Aids in the resolution of problems caused by an incorrect or sticky ARP cache.

Show Processes - List the status (running/not running) of all BSC processes.

3. Click **Process** to execute the selected test.
Test results are displayed on the right side of the screen.



Note: It may take several minutes for results from the traceroute test to appear, especially if devices cannot be reached.

Capturing Network Traffic Data

BlueView enables you to capture network traffic data on any of its physical interfaces, filter the packets using specified criteria, and then save the data to a file.

You can then either display the data file on screen or import the file into any network analyzer program, such as Ethereal or TCP Dump.

To capture BlueView network traffic:

1. Click **BlueView/Traffic Capture** from any administrator console page.
The Traffic capture page appears as shown in Figure 9-7.

Figure 9-7: Traffic Capture Page

2. Configure the following traffic capture options as appropriate:
 - **Name** - Name for the traffic capture file. BlueView appends a .DMP extension to the saved file name when you stop the capture operation.
 - **Interface** - BlueView network interface from which to capture packet data.
 - **Filter** - Restrict the type of packets captured to provide more meaningful results. You can filter packets by a selected protocol, port, and source or destination IP, netmask, and MAC addresses.
 - **Number of Records** - Specify the maximum number of packets to capture. Use this setting to prevent excessive file size.






Note: You can run multiple traffic captures simultaneously.

3. Click **Save** to store the configured traffic capture job in the BlueView database.

Clicking **Save and create another** stores the traffic capture job and enables you to create another.

Clicking **Capture/Save** stores the configured traffic capture job and runs it immediately.





The configured traffic capture job appears on the BlueView/Traffic Capture page as shown in Figure 9-8.

Actions	Name	Interface	Status
<input type="checkbox"/>			
<input type="checkbox"/>   	TrafficCapture1	TrafficCapture1	Stopped

Check All | Clear All Delete

1 row

Figure 9-8: Defined Traffic Capture Job

- Click the  icon to launch the traffic capture job.
As the traffic capture job runs, the binoculars icon changes to  indicating that the job is in progress and will be stopped if you click on the  icon.
Upon completion of the job, its status returns to Stopped.
Click the  icon to download the completed traffic capture file.
By default, BlueView saves the traffic capture file using a .dmp file extension.

Accessing BlueView Functions via the BlueView Serial Port

On a rare occasion, you may temporarily lose access to the BlueView's web browser interface due to a misplaced password or an ISP service outage. In this case, BlueView provides serial port access to the following essential functions:

- 1) `initdb` - Restore all values in the BlueView database back to their defaults. Requires a restart to take effect.
- 2) `Network`: Access the Network sub-menu to:
 - * Modify and display the NIC settings.
 - * Enable ssh remote diagnostics
 - * Disable ssh remote diagnostics
- 3) `processes` - Show a list of all running processes.
- 4) `BVMS` - Access the BVMS sub-menu to start, stop, or restart the BVMS.
- 5) `switch` - Switch to the alternate runtime software image. You must subsequently issue the `reboot` command for the switch to take effect.
- 6) `reboot` - Reboot the BlueView machine (required after image switch).
- 7) `clean` - Access the Clean sub-menu to clean up old database and log files; delete BSC firmware, patches, or configurations; delete BSAP firmware; or delete BVMS backups.
- 8) `specials` - [Reserved for Bluesocket use only].
- 9) `exit` - Exit the serial port session.

To access the BlueView serial port functions:

1. Connect a nine-pin null-modem serial cable between the nine-pin serial port on the back of the BlueView chassis and your laptop computer (see Figure 9-9).

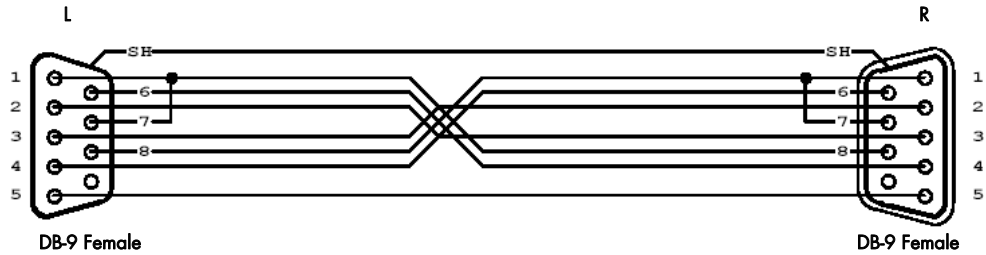


Table 9-1:

Pin Connections	
L-SH	R-SH
L-1	L-7, R-8
L-2	R-3
L-3	R-2
L-4	R-6
L-5	R-5
L-6	R-4
L-8	R-1, R-7

Use the above cable for RS-232 asynchronous communications between BlueView and a laptop computer.

In this cable, Request-to-Send (RTS, pin 7) asserts the Carrier Detect (pin 1) on the same side and the Clear-to-Send (CTS, pin 8) on the other side of the cable.

Figure 9-9: Recommended Null-modem Serial Cable Pinout

2. Run a terminal emulation program on your laptop computer configured with the following settings:
 - Port - COM1
 - bps - 9600
 - Data bits - 8
 - Stop bits - 1
 - Parity - None
 - Flow control - None
3. Initiate the connection to BlueView.
4. Press the Enter key, and then enter the following password at the displayed password prompt:


```
blueviews
```

A menu appears listing the commands described above.
5. Enter a command at the prompt, or exit the serial port session.

BVMS Central Guest Access

With the introduction of the 6.4 release, Bluesocket's BlueView Management System (BVMS) is used to centrally manage Guest accounts. Guest accounts are created from a central web based GUI. Guest authentication is done via a RADIUS directory server, residing on the BVMS. While a tight integration is available for Bluesocket Controllers, the BVMS can be used with any 3rd party Controller that can authenticate against RADIUS. Finally, reports are available based on Guest creation and usage.

- Benefits
- Operation
- Configuration
- Group Configuration
- Controller Configuration
- User Configuration
- Location Configuration
- Limiting Access
- Reporting

Benefits

- Scalability across multiple controllers, administrators and locations.
- Centralized management and configuration of Guest accounts
- Separation of guests into groups, for tracking and usage.
- Able to determine policy (role, session limits, total time) based on group.
- No need to install software on administrator PCs.
- Singular reports of Guest Activities across the installation.

Operation

Guest accounts are created by any staff member in an organization authorized to do so. This could include receptionists, hotel staff, event organizers etc., all of whom could access the system and create Guest accounts – and print receipts for them.

The accounts reside on a Radius server on BVMS and then Controllers are configured to query this Radius server when a user attempts to authenticate to that BSC.

When a super-admin decided to run reports, they are available at the BVMS.

Configuration

1. Log into the BVMS (<https://IPAddress>)
2. Go to the Guest Access View:



Figure 10-1: Guest Access View

Group Configuration

1. Go to the Guest Groups View:

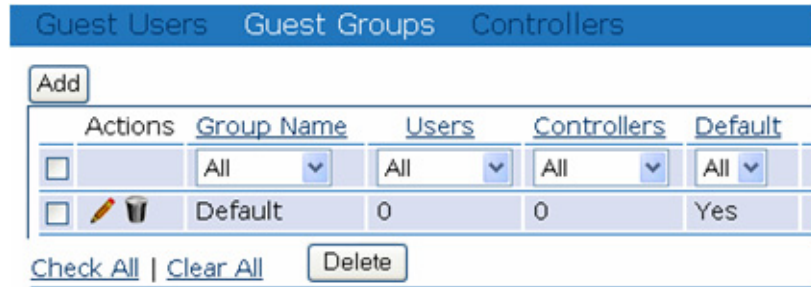


Figure 10-2: Guest Groups View

2. The Default group is called 'Default'. All Guest users created will belong to this group. If desired, created additional groups for different locations, buildings or departments within the organization. For now, open the Default group.
3. The group name (and whether it's the default group) can be changed:



Figure 10-3: Guest Access Group Settings

4. A default password for all group users can be specified, or the BVMS can generate a random password for each user:

Password Setting

Generate Unique Passwords

Use Default Password

Figure 10-4: Password Setting

5. Account settings determine when the account expires (to remove unused accounts) and when the user time runs out (to limit the time a guest can access the network). In addition the Role passed back to the controller during a successful authentication is configurable. Finally, the BVMS can limit the Guest credentials to a single user, to prevent multiple logins:

Account Settings

Account Expiration
1440
Enter in minutes guest account remains valid since account creation.

Account Duration
60
Enter in minutes the duration of valid session time after login.

Guest Role
 Custom Role

Guest

Enable simultaneous login
Select this option to allow guest to login to multiple sessions at the same time.

Figure 10-5: Account Settings

6. Guest Access Controllers maps the IP addresses of the controllers that can authenticate Guests in this group. By default it is empty until you create a Guest Access Controller:

Guest Access Controllers

No configured *guest access device*.

Figure 10-6: Guest Access Controllers

7. Role attributes – allow the administrator to configure the RADIUS server for 3rd party configurations, like PPP authentication.

Attribute	Operator	Value Options	Value	Row Management...
Service Type	:=	Login-User	Login-User	
Framed Compression	:=	Van-Jacobsen-TCP-IP	Van-Jacobsen-TCP-IP	
Framed Protocol	:=	PPP	PPP	
Framed MTU	:=		1500	

Figure 10-7: Role Attributes

Controller Configuration

1. Click on Controllers
2. You will be prompted to create a Guest Access controller. Pick one from the drop down list:

Empty list, create new Guest Access Devices

Back Reset Save Save and create another

Controllers
192.168.102.40

Figure 10-8: Create New Guest Access Devices

3. Confirm the port numbers to be used for Authentication and Accounting, and the retries for the Radius Server:

Port
1812
Guest Access Manager port (default is 1812)

Accounting Port
1813
Guest Access Manager accounting port (default is 1813)

Retry Count
3
Number of retries to authenticate with BVMS (default is 3)

Timeout
10
Timeout in seconds for RADIUS Server Response. Value must be greater than 0, default is 10.

Figure 10-9: Authentication and Accounting Port Numbers

4. Enter a shared secret – the Controller will be added as a RADIUS client to the BVMS, with this shared secret.

Shared Secret

••••••••

The shared secret passphrase to be used in authentication with BVMS.

Confirm Shared Secret

••••••••

Enter the same passphrase as in Shared Secret.

Figure 10-10: Shared Secret

5. Click save, and the Controller (in this case a BSC) will show up in the list:

✓ Successfully created Guest Access Devices: "192.168.102.40".

Add

Actions	Controller Name	Device IP Address	Groups
<input type="checkbox"/>	All	All	All
<input type="checkbox"/>	192.168.102.40	192.168.102.40	0

Check All | Clear All | Delete

Figure 10-11: Authentication and Accounting Port Numbers

6. Now go to the Bluesocket Controller UI, under Authentication Server. The BVMS is automatically added to the Authentication Server list.

Status | User Authentication | User Roles | Voice | General | Web Logins | Wireless | Network | Mobility Matrix | Maintenance

Authentication Servers | Internal_B02_1x Authentication | Local Users | MAC Device Authentication | Accounting Servers | Administrative Users | Create...

Servers | Authentication Test

Actions	Enabled	Name	Default role	Type	Address	Precedence	Accounting server
<input type="checkbox"/>	Yes	BVMS Guest Access Manager	Guest	RADIUS	192.168.100.139	97	BVMS Guest Access Accounting

Check All | Clear All | Enable | Disable | Delete

Figure 10-12: Authentication Server List

- The BVMS has pre-populated the Authentication server fields:

Name
 BVMS Guest Access Manager
 Name to identify this server

RADIUS server settings
 Server address: 192.168.100.139 [See hosts...](#) Port: 1812
The IP address or DNS name of the RADIUS server. NOTE: IP Address only if used for VPN Authentication.
 Shared secret: [redacted] Confirm shared secret: [redacted]

Accounting
 Accounting server: BVMS Guest Access Accounting
For accounting logging with authentication.

Figure 10-13: Authentication Server Fields Prepopulated

- The Role assignment is via the default role, or an override role at the BVMS (using a Bluesocket RADIUS Vendor Attribute):

if	Attribute	logic	Value	then Role is	Row Management...
1	[input]	[dropdown]	[input]	[dropdown]	[dropdown]

Default role: Guest

Figure 10-14: Authentication and Accounting Port Numbers

- See the Accounting Server was also created (for reporting):

Navigation: Status | **User Authentication** | User Roles | Voice | General | Web Logins | Wireless | Network | Mob...

Authentication Servers | Internal 802.1x Authentication | Local Users | MAC Device Authentication | Accounting Servers | Adminis Users

Actions	Enabled	Name	Type	Address
<input type="checkbox"/>	All [dropdown]	[dropdown]	All [dropdown]	
<input type="checkbox"/> [edit] [trash]	Yes	BVMS Guest Access Accounting	RADIUS Accounting	192.168.100.139

Figure 10-15: Authentication Server Created

- Return to the Guest Groups page, and edit the Default Group. Select the controller to be available for use by the default group:



Figure 10-16: Default Group Controller

User Configuration

- Click on Guest Users:
- By default, Single Creation of users is selected. Bulk user creation is also possible (specifying a username prefix):



Figure 10-17: Create Guest User

- Enter the user's credentials:

Guest Information	
Guest Company	Bluesocket
Guest Name	Mimo Joe
Guest Email	mjoe@bluesocket.com

Figure 10-18: Guest Information

- The user name and password is generated by BVMS:

Guest Login

User Name
3273100268

Password
ISUEF8cdV4

Figure 10-19: Guest Login

- The Guest's access policies can be determined by a group, or overridden here (similar to the Group view). The group is chosen here:

Guest Group

Guest belongs to a guest group

Default

Figure 10-20: Guest Group

- Click save, the list view shows the newly created user. You can print the user's login information from this screen, by clicking the printer icon.

Actions	Active	Enabled	User Name	Group Name	Guest Name	Company Name	Creator	Creation Date	Expiration Date
	All	All	All	All	All	All	All	All	All
	No	Yes	3273100268	Default	Mimo Joe	Bluesocket	admin	2008-08-03 20:50:55	2008-08-04 20:50:55

- Test the newly created user at the BSC's external authentication test:

External Authentication Test

Submit

User name
3273100268

Password
●●●●●●●●

External server
BVMS Guest Access Manager

Figure 10-21: External Authentication Test

Location Configuration

1. Combining groups with controllers can be an effective means of tailoring access needs in terms of location, network access and bandwidth usage.
2. Here three groups exist:







Actions	Group Name	Users	Controllers	Default
<input type="checkbox"/>	All	All	All	All
<input type="checkbox"/>  	Default	1	1	Yes
<input type="checkbox"/>  	Finance	10	0	No
<input type="checkbox"/>  	Marketing	0	1	No

Figure 10-22: Authentication and Accounting Port Numbers

3. The Finance group has 10 users, but no controller yet – so the Finance guests cannot authenticate until they are associated with a controller
4. Marketing has a controller, but no users yet – new marketing guests will be able to associate to the marketing controller but not others.
5. Bandwidth, session time-out, and reports are granular to the group level.

Limiting Access

Given that the Guest Access tool is targeted to non-admin users, the BVMS allows a full admin to create an admin account that can only access Guest Access Services.

1. As a full admin, click BlueView Setup Administrative Users

2. Create an administrative user, limiting the user to Write Access of Guest Access:

Create new Administrative User

Back Reset Save Save and create another

Enable user

Admin user settings

Name
MrFrontDesk

New password
●●●●●●

Confirm new password
●●●●●●

Force password change next login?

Access

Restrict admin from changing their password on the login screen?

Restrict Admin to specified group?
Boston

The selected group would be the admins default group.

Write Access

Full Status
 Intermediate Jobs
 Read Only Jobs Elements
 Guest Access Templates
 Device Discovery

Figure 10-23: Create New Administrative User

3. Sign out as admin.
4. Sign in as the new admin. Only the Guest Access tabs are shown:

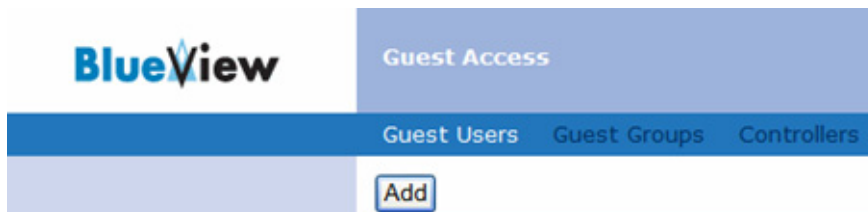


Figure 10-24: Guest Access Tabs

5. This Guest Access admin can create a user, as above.

6. Only a full admin can modify the groups or the controllers. So the full admin should build the groups and controllers tab.

Guest Access

Guest Users Guest Groups Controllers

 You only have read only permission.

Actions	Group Name	Users	Controllers	Default
<input type="checkbox"/>	All ▾	All ▾	All ▾	All ▾
<input type="checkbox"/> 	Default	1	0	Yes

[Check All](#) | [Clear All](#)

1 row [download](#)

Figure 10-25: Admin only can modify groups or controllers

Reporting

Three new reports are available for Guest Access users:

- Guest User Creation over time (per Admin)
- Guest User Bandwidth over time
- Guest User Bandwidth per Controller

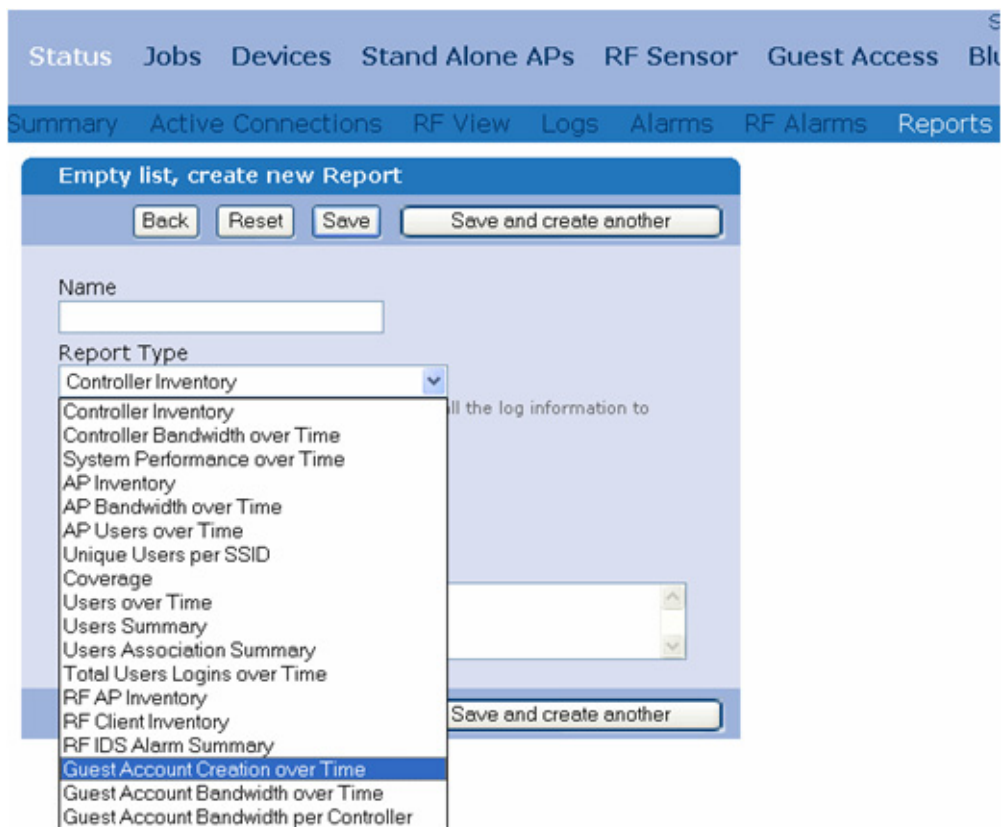


Figure 10-26: Create New Report - Select Report Type

Empty list, create new Report

Back Reset Save Save and create another

Name
UserCreation

Report Type
Guest Account Creation over Time

All user reports need the controllers to send all the log information to BVMS.

Data Range

Time Period
Choose from Below

From

Year Month Day Hour Minute
2008 August 3 00 00

To

Year Month Day Hour Minute
2008 August 3 21 01

Figure 10-27: Create New Report - Completed Fields

And the resulting report shows the creation of one user:

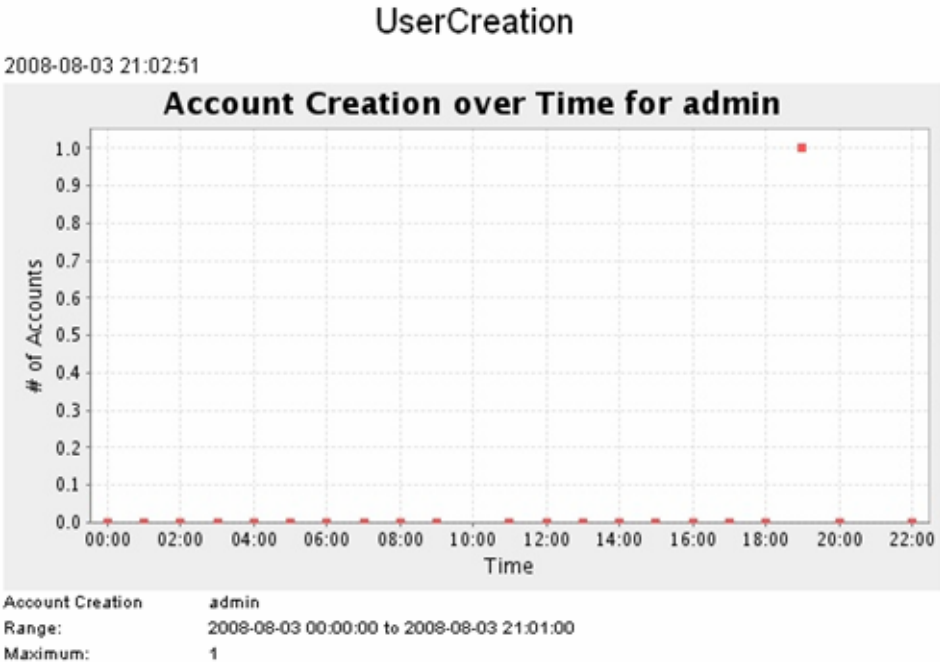
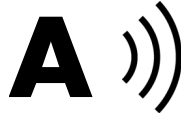


Figure 10-28: Reports - User Creation over Time



Contacting Bluesocket, Inc.

This appendix provides complete information for contacting Bluesocket and includes:

- Obtaining Technical Support
- Contacting Bluesocket Customer Support

Obtaining Technical Support

Bluesocket is committed to providing complete technical support to its customers.

If you have a question concerning your Bluesocket product, refer to the technical documentation, including release notes, supplied with your distribution. You should be able to find the answer to your question in these documents.

If you need further assistance, please first contact your authorized Bluesocket value-added reseller from whom you purchased your product. Your Bluesocket reseller is familiar with you and your particular installation, and has technical support staff ready to assist you.

Contacting Bluesocket Customer Support

If you require further assistance, and you are a BLUE STANDARD or BLUE PREMIUM service contract customer, you can reach our support department directly using the following information:

- **e-mail:** support@bluesocket.com
- **telephone:** In the US, dial toll-free 1-866-633-3358 and then press 2 at the prompt to reach Bluesocket customer support personnel from 8:00 a.m. to 6:00 p.m. eastern time.

From locations outside of the US, dial +1-781-328-0888 and then press 2 at the prompt to reach Bluesocket customer support personnel.

Live telephone support is available 24 hours per day, 7 days a week for BLUE PREMIUM customers.

- **Internet:** www.bluesocket.com
- **postal mail:** Bluesocket, Inc.
10 North Avenue
Burlington, MA 01803 USA



Index

Symbols

.BPF file 7-6, 7-20
.BVB file 9-3, 9-4
.bvd file 9-4
.DMP file 9-9
.IMG file 7-4, 7-5

Numerics

802.11a radio settings, configuring 7-34
802.11a radio settings, editing 7-34
802.11b/g radio settings, editing 7-29
802.11i preauthentication, enabling for an SSID 7-42

A

About this guide xi
AC power requirements 2-6
AC power, connecting BlueView to 2-8
Acknowledging alarms 6-22
ACT/LINK LEDs 2-4
Active Connection Rate 3-17
Active RF containment, manually placing a device in 6-17
Active user connections, monitoring 6-17
Administrator accounts
 adding 4-2
 adding a new 4-2
 changing password for 4-3
 defining authentication servers for 4-4
 defining external authentication servers for 4-4
 deleting 4-4
 forcing password change upon next login 4-2
 restricting access to specified groups 4-2
Administrator console
 accessing 3-4
 logging into for the first time 3-4
 logging out of 3-7
Administrator notifications, configuring for RF sensors 4-15
Administrator password, changing 4-3
Agent, SNMP 4-13
Alarms
 acknowledging 6-22
 displaying 6-22

- interpreting 6-22
- purging 6-22

Allow admin to access using SNMP 3-3

- Allow admin to access using SNMP 4-2
- Antenna type, configuring fixed or external for BSAPs 7-32
- AP bandwidth over time reports, generating 6-25
- AP inventory reports, generating 6-25
- AP users over time reports, generating 6-25
- Approvals, safety and emissions 1-6
- Approved SSIDs, identifying 8-7
- APs, placing on a heat map 6-32
- Arp utility, executing from the BlueView administrator console 9-8
- Audience for this guide xi
- Authorized wireless devices, identifying 8-2
- Auto-discovery
 - feature description 1-3
- Automatically add newly created SSID configs to this controller 7-44**

B

- Backing up BSC configurations 7-14
- Backing up the BlueView database 9-3, 9-4
- Bandwidth limit, defining for the BSC for file uploads to BlueView 3-15
- Binoculars icon 3-11
- Blocking a detected RF device 6-17
- BlueSecure Access Points (BSAPs)
 - configuring 802.11a radio settings 7-34
 - configuring 802.11bg radio settings 7-29
 - deleting configurations on BSCs 7-36
 - displaying status information for 6-12
 - displaying summary information for 6-7
 - editing 802.11a settings 7-34
 - editing 802.11b/g settings 7-29
 - editing configurations on BSCs 7-28
 - editing identification settings 7-28
 - limiting client connections to 7-32
 - listing BSC configurations 7-27
 - listing configurations on BSCs 3-12
 - manageable by BlueView 1-3
 - managing configurations on BSCs 7-26
 - managing SSID configurations 7-37
 - upgrading with new system software 7-20, 7-21
- BlueSecure controllers, manageable by BlueView 1-3
- Bluesocket BlueSecure Access Point 1500 Quick Start Guide xiii
- Bluesocket BlueSecure Controller Quick Start Guide xiii
- Bluesocket BlueSecure Setup and Administration Guide xiii
- Bluesocket SSL certificate, installing 3-5
- Bluesocket, contacting A-1
- BlueView™ Management System
 - administering 9-1
 - configuring 4-1
 - connecting to remotely 3-4
 - diagram of 1-2
 - installation procedures 2-1

- overview of 1-1
- Brackets, mounting 2-8
- BSAP configurations
 - deleting 7-36
 - editing 7-28
 - listing 7-27
- BSAP image files, uploading to BlueView 7-4, 7-5
- BSAP system software required by BlueView 1-3
- BSC configuration files, uploading to BlueView 7-2
- BSC configuration template
 - editing 7-8
 - generating 7-6
- BSC configurations
 - backing up 7-14
 - restoring 7-14
- BSC image files, uploading to BlueView 7-3
- BSC models, manageable by BlueView 1-3
- BSC patch files, uploading to BlueView 7-6
- BSC system software, required by BlueView 1-3
- Bulk RF configuration data files, importing 8-8
- Bytes in, count 6-3
- Bytes out, count 6-3

C

- Calibrate dimensions on screen** 6-30, 6-33
- Capturing network traffic data 9-9
- Chassis cap, installing 2-7
- Cipher** 5-16
- Communication protocols 1-6
- Community strings, defining the BlueView's for SNMP v2 4-14
- Configuration Rate** 3-17
- Configuration template
 - editing 7-8
 - generating 7-6
 - pushing out 7-15
- Configuration templates, creating for stand alone APs 5-11
- Configuration to restore** 9-4
- Configurations
 - backing up BSCs 7-14
 - managing on BSAPs 7-26
- Configuring BlueView 4-1
- Connectivity Rate** 3-17
- Contained devices, listing 6-34
- Controller bandwidth over time reports, generating 6-25
- Controller inventory reports, generating 6-25
- Controllers
 - auto-discovering 3-8
 - configuring to send logs to BlueView 3-2
 - discovering for management 3-8
 - maintaining and provisioning 7-1
 - manually adding to BlueView for management 3-13
 - monitoring 6-1
 - organizing into static groups 3-17

- preparing for management by BlueView 3-2
- rebooting 7-12
- restarting 7-10
- shutting down 7-13
- switching the runtime image 7-17
- upgrading with new system software 7-16

Controllers list 3-11, 7-36, 7-44

Conventions used in this guide xii

Copyright information ii

Coverage reports, generating 6-25

D

Data Retries 5-8

Database

- backing up manually 9-3
- configuring 4-12
- restoring from backup file 9-4

Date setting, configuring BlueView's 4-11

Debug file, creating 9-4

Debugging BlueView 9-4

Default Group for discovered controllers 3-9

Defaults, resetting all BlueView parameters to 9-4, 9-10

Deleting administrator or user accounts 4-4

Desktop bumpers, installing on BlueView chassis 2-6

Desktop mounting procedures 2-6

Devices in RF containment, listing 6-34

DHCP, configuring BlueView to use 4-9

Diagnostic tests, running from the BlueView administrator console 9-8

Discovering stand alone APs 3-9

Discovery job, creating 3-8

DISK LED on front panel 2-4

Display, liquid crystal 2-4

Document organization xi

Download file icon 9-10

Download icon 7-3, 7-4, 7-5, 7-6

DTIM 7-32

Dynamic groups, creating 3-18

E

Editing a BSC configuration template 7-8

Email server, specifying for event notifications 4-14

Enable 802.11i preauth bit 7-42

Enable Remote SSH Diagnostics 4-14

Enforcement 7-32

Environmental requirements for BlueView 2-5

Environmental specifications 1-6

Ethernet 1, use as default network connection 2-5

External antennas, configuring use of for BSAP-1540s 7-32

External antennas, configuring use of on BSAP-1540s 7-32

F

Fault monitoring 1-3

Features and functions 1-3

Floor plans, importing for BlueView heat maps 6-28
 Forcing a user to logout 6-19
Fragmentation Threshold 5-8

G

Getting Started page 3-5
 Graceful shutdown, performing 2-9
 Groups

- creating dynamic virtual 3-19
- creating hierarchies of 3-17
- creating static device 3-15
- visually organizing 3-18

H

Heat maps

- calibrating 6-33
- generating 6-31
- overview of 6-27

 History of jobs 7-25
 HTML-based administrator console 3-4
 Humidity, operating 2-5

I

Icon

- binoculars 3-11
- download 7-3, 7-4, 7-5, 7-6
- download file 9-10
- letter 6-27
- pencil 7-7, 7-9
- red hand 3-11
- wastebasket 6-27, 7-3, 7-4, 7-5, 7-6, 7-7, 7-25, 7-37
- watch 7-3, 7-4, 7-5, 7-6, 7-7

 image files uploading BSAP 7-4, 7-5
Import a new device backup? 7-2
 Importing floor plans for heat maps 6-28
 Installation location, selecting 2-5
 Installation procedures

- connecting BlueView to your network 2-8
- mounting the BlueView chassis 2-6
- overview of 2-2
- powering up BlueView 2-8
- safety considerations 2-2
- selecting an installation location 2-5

 Inventory reports, generating and displaying 6-24
 IP address

- assigning to the protected interface 4-9

J

Job elements, creating 7-2
 Jobs

- backing up a BVMS configuration 7-24
- backing up BSC configurations 7-14

- history 7-25
- installing a BSC patch 7-18
- pending 7-25
- pushing out a BSC configuration template 7-15
- removing a BSC patch 7-19
- restarting Controllers 7-10
- restoring a BSC configuration 7-14
- running 7-10
- scheduling 7-12
- sending a BlueView report via email 7-23
- shutting down BSCs 7-13
- switching the BSC runtime image 7-17
- upgrading BSCs with new system software 7-16, 7-20, 7-21

L

- LCD 2-4
- LDAP server, authenticating administrators against 4-4
- LEDs 2-4
- Letter/email icon 6-27
- Load balancing clients on a BSAP 7-32
- Location map, displaying for a detected RF device 6-16
- Logging, configuring 4-12
- Login name for administrator account 3-5
- Logs
 - displaying 6-20
 - interpreting 6-18, 6-19, 6-20, 6-21

M

- Maintain Current Configuration** 9-6
- Manageable devices 1-3
- Manually adding devices for management by BlueView 3-13
- Maps, generating RF heat 6-31
- Maps, overview of 6-27
- Maximum number of alarm entries to keep 4-13
- Maximum number of log entries to keep 4-12
- Mounting procedures
 - desktop 2-6
 - two-post rack 2-7

N

- Netstat, executing from the BlueView administrator console 9-8
- Network diagnostic tests, running from the BlueView administrator console 9-8
- Network interfaces, configuring 4-8
- Network ports, description of 2-5
- Network time protocol (NTP) synchronization, configuring 4-11
- Network traffic data, capturing 9-9
- Network, preparing for use with BlueView 2-5
- Notational conventions xii
- Null-modem cable, serial port connection 9-11

O

- Obtain IP settings from a DHCP server for the interface** 4-9

- Obtain IP settings from a DHCP server for the interface 4-8
- OFDM Transmitter Power** 5-5
- Online help, displaying 3-7
- Operating humidity 2-5
- Operating temperature 2-5
- Opt out of group's Secure Mobility Matrix** 3-15
- Organization of this guide xi
- Overview of BlueView 1-1

P

- Parent Group** 3-17
- Password
 - administrator account 3-5
 - changing an administrator's 4-3
 - recovering lost or forgotten administrator account 3-5
- Patches
 - installing a system software patch on BlueView 9-6
 - installing on a BSC 7-18
 - removing an installed BlueView system software patch 9-7
 - removing from a BSC 7-19
- Pencil icon 7-7, 7-9
- Pending jobs, reviewing 7-25
- Ping, executing from the BlueView administrator console 9-8
- Poll now button, using 6-5
- Power control 2-4
- Power source requirements 2-6
- Power supply 1-6
- Powering down BlueView 2-9
- Powering up BlueView 2-8
- Preauthentication, enabling 802.11i 7-42
- Preface xi
- Processes, displaying the status of all BlueView 9-8
- Purge all job history 7-26
- Purging logs 6-21
- Pushing Out a Configuration Template to a BSC 7-15
- PWR LED on front panel 2-4

Q

- Query the NTP server now?** 4-12

R

- Rack requirements 2-5
- Rack-mounting procedures 2-7
- RADIUS authentication server, using with stand alone APs 5-16
- RADIUS server, authenticating administrators against 4-6
- Rebooting BlueView 9-2
- Rebooting Controllers 7-12
- Refresh rates 4-16
- Related Documents xiii
- Remote access to the BVMS, enabling 4-14
- Reports, emailing to a user 6-27
- Reports, generating and displaying 6-24
- Resetting all configuration settings to their default values 9-4

- Resetting all parameters to default values 9-10
- Restart control 2-4
- Restart/Reboot automatically if necessary? 7-15
- Restarting BlueView 9-2
- Restarting BSCs 7-10
- Restoring a BSC Configuration 7-14
- Restoring the database from a backup file 9-4
- Return Address 4-15, 7-24
- RF IDS alarm summary reports, generating 6-26
- RF intrusion and containment
 - configuring autocontainment 8-6
 - defining approved SSIDs 8-7
 - identifying administrator notifications 4-15
 - identifying authorized stations 8-2
 - importing bulk configuration data files 8-8
 - overview of 8-2
- Rf intrusion and containment
 - manually blocking a detected device 6-17
- RF sensors
 - configuring alarms from 8-3
- RF signal strength, heat map colors used to represent 6-32
- RF station inventory reports, generating 6-26
- RF stations (devices), identifying 8-2
- Rogue devices, containing 8-6
- Rogue, identifying an RF station as 8-3
- Route Destination 4-10
- Route Gateway 4-10
- Routing table, displaying BlueView's 4-10
- Routing table, displaying the BlueView's 4-10

S

- Safety considerations when installing BlueView 2-2
- Secure connection, terminating a user's 6-19
- Secure Mobility Matrix, configuring a BSC to opt out of its group's 3-15
- Security alert, preventing display of 3-6
- Serial port
 - accessing BlueView functions via 9-10
 - description 2-5
- Show Processes** 9-8
- Shutting down BlueView 2-9, 9-2
- Shutting Down Controllers 7-13
- Sign Out link 3-7
- Site Map link 3-7
- SMTP Server 4-15, 7-23
- SNMP agent setting 4-14
- SNMP Agent, configuring 4-13
- SNMP agent, configuring BlueView's 4-13
- Space requirements 2-5
- Spectralink IP phone traffic, passing through the BSC 7-32
- SSH access to the BVMS, enabling 4-14
- SSID configurations
 - adding on BSCs 7-43
 - defining for stand alone APs 5-14

- deleting from BSCs 7-43
- editing 7-38, 7-40
- listing 7-38
- managing 7-37
- SSID, listing configurations on BSCs 3-12
- SSIDs, defining approved in RF sensor coverage area 8-7
- SSL certificate, installing Bluesocket 3-5
- Stand alone APs
 - configuring a RADIUS server for 5-16
 - creating configuration templates for 5-11
 - defining access credentials 5-10
 - defining radio settings for 5-5, 5-9
 - defining SSIDs for 5-14
 - discovering 3-8
 - editing configurations 5-4
 - listing 5-3
 - managing 5-2
 - manually adding for management 5-12
- Static groups, creating 3-15
- Static routes, configuring for BlueView 4-10
- Status LEDs 2-4
- Status Rate** 3-17
- Status reports, generating and displaying 6-24
- Storage space 1-6
- Summary information
 - BlueView 6-2
 - BSAP 6-7
 - BSC group 6-3
 - displaying 6-2
 - RF sensors 6-13
 - single BSC 6-5
- Support, obtaining technical A-1
- Switching the BSC Runtime Image 7-17
- System software
 - installing and uninstalling patches on BlueView 9-6
 - switching between BlueView runtime versions 9-7
 - upgrading BlueView to a new version 9-5

T

- Technical specifications 1-6
- Technical support, obtaining A-1
- Temperature, operating 2-5
- Terminal emulation program settings to access BlueView serial port 9-11
- Terminating a user's secure connection to a BSC 6-19
- Terminology, used in this document xiii
- Time setting, configuring BlueView's 4-11
- Total user logins over time reports, generating 6-26
- Traceroute, executing from the BlueView administrator console 9-8
- Traffic, capturing network interface 9-9
- Troubleshooting your BlueView configuration 9-4

U

- Upgrading BSAPs with New System Software 7-20, 7-21

Upgrading BSCs with New System Software 7-16

Upload a new patch? 7-6

Upload new firmware? 7-3, 7-4, 7-5

URL, to connect to BlueView 3-4

Use WMM to apply QoS 7-33

User connections, monitoring 6-17

User logout, forcing a 6-19

User reports, generating and saving 6-24

Users Logged In 6-3

Users over time reports, generating 6-25

Users summary reports, generating 6-25

Users with VPN 6-7

V

VPN connection, terminating a user's 6-19

W

Wastebasket icon 6-27, 7-3, 7-4, 7-5, 7-6, 7-7, 7-25, 7-37

Watch icon 7-3, 7-4, 7-5, 7-6, 7-7