BlueSecure Controller (BSC) Software Upgrade/Patch Instructions

Date: July 2, 2010
Revision: 2.0

***ADVISORY**
OBTAIN COUNTRY CODE BEFORE UPGRADE AS ALL RADIOS WILL BE DISABLED UNTIL COUNTRY CODE IS SET. See requirements below for further details.
***ADVISORY**

Introduction

This document explains the procedure and requirements for upgrading/patching a BlueSecure controller (BSC).

Requirements

Ensure that you meet these requirements before you attempt the upgrade:

- The BSC must be running software version 3.1.1.8 or newer. If it is not running 3.1.1.8 or newer then 3.1.1.8 must be installed prior to upgrading to the latest software release. Software version 3.1.1.8 is available for download at support.bluesocket.com.
- If you are upgrading to version 6.X and are currently running version 5.2 or prior, you must upgrade to 5.3.2.6 first. Software version 5.3.2.6 is also available for download at support.bluesocket.com.
- If you are upgrading from one major version to another, for example 5.X to 6.X, do not "Maintain Current Configuration" during the upgrade but instead backup the configuration and restore it after the upgrade. The BSC's configuration will be defaulted during the upgrade. After the upgrade you will have to restore the configuration.
- The BSC-600/1200 requires a software image/patch with M or MIPS designated in the file name.
- All other platforms (BSC-2100/2200/3200/5200) will either have no special designation in the software image/patch file name or may be designated with i386.
- BlueSecure Access Point (BSAP) firmware for the BSAP-18XX is bundled in the BSC software image and automatically applied during the upgrade. If you have BSAP-15XX's, BSAP-1700's, or Wi-Jack's you will have to download the BSAP firmware separately from support.bluesocket.com, upload it to the BSC and or TFTP server, and then apply it to the BSAPs. You can upload the BSAP firmware to the BSC or specify an external TFTP server under wireless>firmware. After you upload the BSAP firmware or specify an external TFTP server the APs will show up as "modified" under status>AP. You can select them and click "apply" to apply the new firmware.
- If you are upgrading to version 6.4.0.14 with Bluepatch Version 2 or later from any version prior you will be required to populate a country code. Please obtain your country code prior to the upgrade as all radios will be disabled until the country code

is set. You can find the 8 digit Country Authentication Code under your support profile: http://support.bluesocket.com/my-profile.htm. If you are unable to locate a country authentication code under your profile please contact Bluesocket Support. If you are using Failover, you should set the country code on each BSC independently. If you are using Replication and you are not replicating the wireless tab you should set the country code on each BSC independently. If you are replicating the wireless tab, set the country code on the master and perform a snapshot from the nodes to replicate the country code to the nodes. If you are not using Bluesocket Access Points, it is not required you set the Country and you can instead disable the ap service under wireless>service to hide the red warning in the GUI.

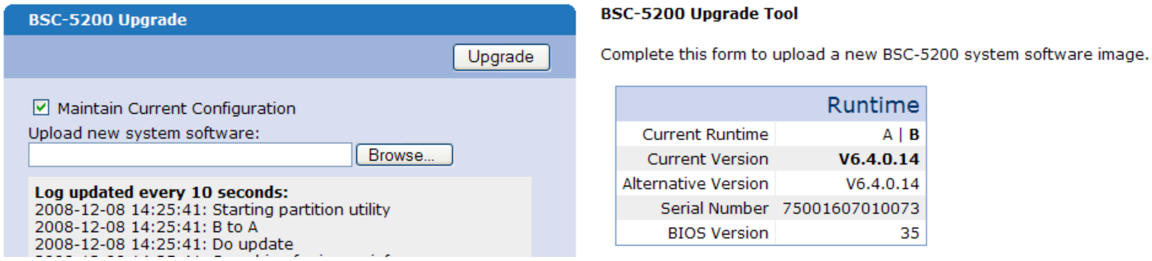
- The BSC will check if it is running as a standalone or the primary of a failover pair. If it is identified as the primary of a failover pair it will automatically upgrade/patch the secondary/failover BSC in standby mode. Alternatively you can break up the failover pair and upgrade each BSC separately. See below for further details. Some patches will require this. Refer to release notes.
- When upgrading multiple BSC's in a replication/loadsharing mesh each BSC should temporarily be configured to act as a master before upgrading. Each BSC should be upgraded independently. After the upgrade is complete the nodes should be re-configured to act as nodes and acquire a snapshot from the master.

Components Used

The information in this document is based on these hardware and software versions:

- All supported hardware platforms running software version 3.1.1.8 or newer.

1. Download current software image and appropriate patches for your hardware platform from support.bluesocket.com.
2. Enter the protected IP address/admin.pl in your browsers address bar to access the BSC's secure web based administrative console. Login with your administrative credentials.
3. Go to Maintenance>Configuration Backup/Restore>backup and save a copy of your current configuration to a safe and secure place.
4. Go to Maintenance>Upgrade.



☑ Maintain Current Configuration

Upload new system software:

```
Log updated every 10 seconds:
2008-12-08 14:25:41: Starting partition utility
2008-12-08 14:25:41: B to A
2008-12-08 14:25:41: Do update
```

BSC-5200 Upgrade Tool

Complete this form to upload a new BSC-5200 system software image.

	Runtime
Current Runtime	A | **B**
Current Version	**V6.4.0.14**
Alternative Version	V6.4.0.14
Serial Number	75001607010073
BIOS Version	35

On the right hand side of the page you will see the current runtime, current version, and alternate version. The current runtime and current version in bold are the runtime/version you are currently running. The BSC contains two runtime software images/partitions, A and B. One runtime image/partition is active (current). When you perform an upgrade it is applied to the alternate partition. When the upgrade is complete the BSC will prompt you to reboot during which the BSC will automatically switch to the alternate partition.

The image that was active becomes the alternate. This allows you to switch back to the original software image using the switch feature under maintenance>switch or via the serial console should you run into any issues with the new software image.

5. If you are prompted with the following message click the link to go to general>http to adjust the “Seconds a client is allowed to hold the web server” to 300. After the upgrade is complete you can adjust it back to your original setting. Bluesocket recommends the client web server hold be set to 300 during an upgrade but 10-30 thereafter.

We have detected a Client Web Server Hold of X seconds. A value of 300 is recommended prior to upgrading, or your upgrade status may be lost.”

6. Browse to the appropriate software image for your hardware platform previously downloaded in step 1.
    a) If you are upgrading from one major version to another, for example 5.3.1.11 to 6.5.0.08 uncheck the “Maintain Current Configuration” check box. The BSC’s configuration will be defaulted during the upgrade. After the upgrade you will have to restore the configuration.
    b) If you are upgrading within the same major version for example 6.4.0.14 to 6.5.0.08, leave the “Maintain Current Configuration” box checked. The configuration database will be maintained while loading the new software image to the alternate partition.
7. Click upgrade. Status of the upgrade will be shown. Wait for the upgrade to complete. The upgrade itself is not service affecting however when the upgrade is complete you will be prompted to reboot or schedule a reboot which will be service affecting.
8. The BSC will check if it is running as a standalone or the primary of a failover pair. If it is identified as the primary of a failover pair it will automatically upgrade the secondary/failover BSC in standby mode. You will see this reflected in the upgrade log for example:

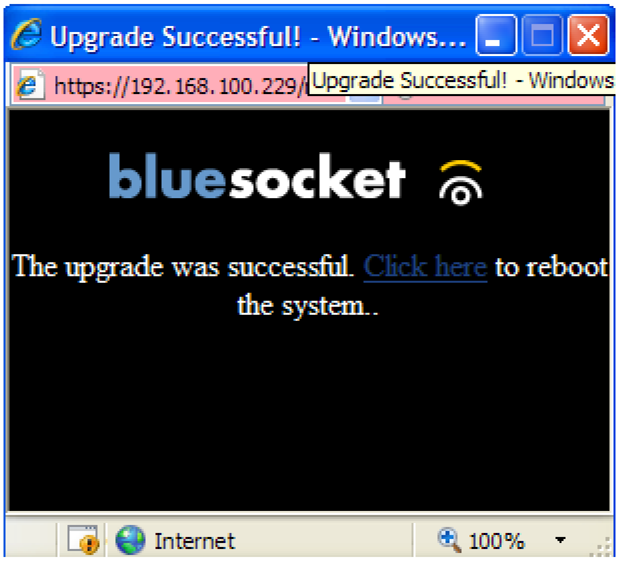
```
2010-06-11 04:14:46: Check if running as standalone,primary,or failover...
2010-06-11 04:14:48: Blueserver running as: primary
2010-06-11 04:14:48: Uploading the image to the Fail-over Secondary
2010-06-11 04:14:54: Starting an upgrade of the Fail-over Secondary.
2010-06-11 04:14:59: Waiting for confirmation from Fail-over Secondary....
2010-06-11 04:14:59: An upgrade of the Fail-over Secondary is started.
2010-06-11 04:18:05: Fail-over Secondary upgraded successfully!
```

Alternatively you can break up the failover pair by disconnecting the cables connected to the managed, protected, and failover interfaces of the secondary/failover BSC and upgrade each BSC separately. After both BSC’s are upgraded/patched you can power the secondary down, reconnect the cables, and power it back up. The failover will automatically synchronize its configuration with the primary.

9. After the upgrade is complete you will be prompted with the following message and *a popup indicating the upgrade was successful. Click on the link to reboot the BSC or schedule a reboot for a later time.

You have made changes which may affect users on the system. After you have made all of your changes, click here to have them take effect.
Alternatively, you may schedule the update to occur at a later time.

*You may not receive the popup if you have a popup blocker enabled.


Upgrade Successful! - Windows...
https://192.168.100.229/
Upgrade Successful! - Windows
bluesocket
Internet
100%

The upgrade was successful. Click here to reboot the system..

10. The BSC will reboot and automatically switch to the alternate partition where the upgrade was applied. The image that was active now becomes the alternate. This allows you to switch back to the original software image under maintenance>switch or from the serial console menu should you run into any issues with the new software image.
11. If the BSC is identified as the primary of a failover pair it will notify the Failover that a reboot has been requested and set the failover to reboot 60 seconds after the primary reboots to give the primary time to launch.

Fail-Over state: primary
Notifying Fail-Over Secondary that reboot has been requested...
Waiting for response...
Fail-Over Secondary is set to reboot. It will reboot 60 seconds after the Primary reboots to give the primary time to launch.

12. BlueSecure Access Point (BSAP) firmware for the BSAP-18XX is bundled in the BSC software image and automatically applied during the upgrade. If you have BSAP-15XX's, BSAP-1700's, or Wi-Jack's you will have to download the BSAP firmware separately from support.bluesocket.com, upload it to the BSC and or TFTP server, and then apply it to the BSAPs. You can upload the BSAP firmware to the BSC or specify an external TFTP server under wireless>firmware. After you upload

the BSAP firmware or specify an external TFTP server the APs will show up as "modified" under status>AP. You can select them and click "apply" to apply the new firmware.

13. If you selected "Maintain Current Configuration" the BSC's configuration database was maintained during the upgrade. Skip to step 19.
14. If you did not select "Maintain Current Configuration" you will have to restore the previously backed up configuration. The BSC's configuration database was defaulted during the upgrade.
    - If you have a DHCP server on the protected network the protected interface will obtain IP settings from the DCHP server. If not the protected interface will fall back to an IP address of 192.168.130.1. The IP address of the protected interface will be displayed in the LCD on the front of the BSC.
    - The managed interface will have an IP address of 192.168.160.1 with the DHCP server enabled.
    - The default username/password is admin/blue.
15. If the protected interface received an IP address via DHCP you can access the web based administrative console via the protected network.
16. Alternatively you can connect a laptop directly to the protected interface and configure it with an IP address in the same subnet for example 192.168.130.2.
17. Alternatively you can connect a laptop directly to the managed interface and configure it for DHCP. By default the managed interface has the DHCP server enabled so the laptop will receive an IP address in the 192.168.160.0/24 subnet from the BSC.
18. Enter the protected IP address/admin.pl in your browsers address bar to access the BSC's secure web based administrative console. Login with the default administrative credentials (admin/blue).
19. Go to Maintenance>Configuration Backup/Restore>Restore and restore the configuration you previously backed up in step 3.
20. You will be prompted to click here to have the configuration changes take effect. Click the link. If you have a laptop directly connected to the protected or managed interface you may now disconnect and restore your connection to your switchport.
21. Enter the protected IP address/admin.pl in your browsers address bar to access the BSC's secure web based administrative console. Login with your administrative credentials.
22. Go to maintenance>patch, browse to the first of your patches to be installed, and click "Install Patch". You will be prompted to click here for changes to take effect. If you have multiple patches to install, continue installing all patches before clicking on the link to reboot. Unlike the software image, patches are applied to the current partition. If the BSC is identified as the primary of a failover pair it will automatically patch the secondary/failover.

Installed patch 'BluePatchRelease' from Bluesocket.
Failover system has successfully been patched

Verify

1. Go to maintenance>upgrade. The current version should be the new software image and the alternate version should be the old pre-upgrade software image.
2. Go to maintenance>patch. All patches installed should be listed.
3. Go to wireless>AP and verify the APs are running the appropriate firmware. Refer to the firmware column.

Troubleshooting

1. Should you run into issues with the new software image that are service affecting you can switch back to the original partition via maintenance>switch or via the serial console. Be sure to gather a show_tech under maintenance>config backup/restore>show_tech before the switch. Report the issue to Bluesocket Support and provide a copy of the show_tech.
2. If the issue is not service affecting a switch back to the original partition may not be necessary. Report the issue to Bluesocket Support.