Bluesocket virtual Wireless Local Area Network (vWLAN) FAQ

Updated 11/07/2011

Can I disable https on the login page of the BSC or vWLAN and use http instead so I do not get a certificate error?

No, https (http over ssl) is required to encrypt login transactions and cannot be disabled. It is recommended you purchase and install a certificate from a trusted certificate authority such as Verisign or Godaddy.

Does the vWLAN support 3rd party access points?

Using the new wired support feature/license, traffic from 3rd party access points or wired clients can be brought onto the system using 802.11n BlueSecure access points.

Does the vWLAN support BSAP-1500/1540/1700's?

Not natively however using the new wired support feature/license, traffic from BSAP-1500/1540/1700's or wired clients can be brought onto the system using 802.11n BlueSecure access points.

How do I default the configuration of the vWLAN?

From the web based administration console:
-Go to maintain>configuration backup/restore
-Select "Reset to default settings"
-Click reset

From the serial console menu:
-Connect to the serial console port using a 9 pin null modem serial cable and a terminal emulation program (9600, 8, none, 1, none).
-The serial console password is wg1000s.

-Choose option 1 for dbinit

How do I reset the password of the default administrator user name (admin) of the vWLAN?

Connect to the serial console port using a 9 pin null modem serial cable and a terminal emulation program (9600, 8, none, 1, none). The serial console username/ password is vwlan/vwlan. Choose option "a" for admin password recovery. The password of the default administrator username (admin) will be defaulted to blue.

How many concurrent authenticated users and BSAPs does the vWLAN support?

The vWLAN supports 48000 concurrent authenticated users and 1500 BSAPs.

I am setting up Internal 802.1x Authentication on the vWLAN. The vWLAN is configured to proxy to RADIUS. Do I need to configure a RADIUS client in the RADIUS server for every single access point or just the vWLAN?

With internal 802.1x BSAPs are configured to send RADIUS requests to the vWLAN. The vWLAN is the RADIUS server and terminates EAP. The vWLAN then proxies inner methods i.e. PAP, CHAP, MSCHAP, MSCHAPv2 to the external RADIUS server. All RADIUS requests are sourced by the vWLAN's network interface IP address and therefore you are not required to configure a RADIUS client in the RADIUS server for every single AP. You only need to configure a RADIUS client in the RADIUS server for the vWLAN with the network interface IP address or DNS name.

I am setting up Internal 802.1x authentication on the vWLAN. I want to authenticate directly against Microsoft Active Directory so I do not have to install Microsoft's Radius component (IAS or NPS). What is the LDAP Password Attribute Name for Microsoft Active Directory?

Internal 802.1x can authenticate a user directly against an LDAP server if the LDAP server has a readable attribute containing the MD4 hash of the users password. For example Open LDAP has an "ntpassword" attribute that is readable and contains the MD4 hash of the user's password. Microsoft Active Directory however does NOT have a readable attribute containing the MD4 hash of the user's password and therefore authenticating directly against MS AD is NOT supported. Use IAS or NPS with MS AD.

I am setting up RADIUS-802.1x Authentication on the vWLAN. Do I need to configure a RADIUS client in the RADIUS server for every single access point or just the vWLAN?

With RADIUS-802.1x BSAPs are configured to send RADIUS requests to the RADIUS server and therefore you are required to configure a RADIUS client in the RADIUS server for every single BSAP. Alternatively configure a RADIUS client in the RADIUS server with an IP range.

I am trying to renew my ssl certificate on the vWLAN but I do not see an option to generate a CSR on the logins>ssl>renewal tab.

If the renewal setup tab does not have an option to generate a CSR you may have previously generated a CSR or applied a certificate. Simply click delete csr or delete cert as appropriate. Deleting the CSR or cert on the renewal setup tab will not affect the certificate that is currently in operation. After you delete the CSR or cert on the renewal setup tab you will be able to generate a new CSR.

I am using the default ssl certificate that came pre-installed on the vWLAN. Why am I receiving a certificate error from the browser indicating the certificate was not issued by a trusted certificate authority?

Examples of the browser error include:
Internet Explorer: "The security certificate presented by this website was not issued by a trusted certificate authority."
Firefox: "The certificate is not trusted because it is self signed."
Safari: "Authentication failed because the server certificate is not trusted."

By default the vWLAN uses a pre-installed SSL certificate that is self-signed by Bluesocket. You will receive a certificate error from the browser indicating the certificate was not issued by a trusted certificate authority because the certificate is self-signed by Bluesocket and Bluesocket is not a trusted root certificate authority like Verisign or Godaddy for example. There are two ways to stop the generation of this web browser certificate error. Install the Bluesocket self-signed certificate on every client in the browser's list of trusted root certificate authorities, or install an SSL Certificate Provided by a CA such as VeriSign or Godaddy on the vWLAN that is already in the client's list of trusted root certificate authorities.

I have an existing SSL certificate for the Microsoft IIS server platform that I would like to use on the vWLAN. Can this be done?

Yes, you must first export your IIS certificate into a PFX file. Next run openssl to extract the

private key and certificate. Then go to logins>ssl>current. Under Key upload Private key: browse for and upload the private key. After you have uploaded the private key under Certificate upload Signed Certificate browse for and upload the certificate

---

I have enabled redirect to hostname under admin>http of the vWLAN but clients are still being redirected to an ip address. I am receiving a certificate name mismatch error in the browser.

Examples of the browser error:
Internet Explorer: "The security certificate presented by this website was issued for a different website's address".
Firefox: "192.168.130.1 uses an invalid security certificate. The certificate is only valid for: vWLAN.bluesocket.com".
Safari: "This certificate is not valid (host name mismatch)"

Why is redirect to hostname not functioning and why am I receiving a certificate name mismatch error in the browser?

Redirect to hostname requires both an A record (forward) and PTR record (reverse) in your organizations DNS server for the vWLAN's Fully Qualified Domain Name (FQDN) and the network interface IP address. The FQDN entered in your DNS server must match the common name (FQDN) you used when generating the CSR. Check to make sure you have BOTH these records in your organizations DNS server. If redirect to hostname is enabled and not functioning it is likely you are missing the PTR.

To test the PTR perform an nslookup from the command prompt of a client for the network interface IP address. You should be returned the FQDN. Assuming the client is using the same DNS server configured on the network interface of the vWLAN. For example C:\>nslookup 192.168.130.1 assuming 192.168.130.1 is the network interface IP address. If not, add the PTR, test with nslookup to confirm, and then reboot the vWLAN. The vWLAN queries the PTR during boot and redirects users to what is returned going forward. The name in the url bar of the browser must match the common name (FQDN) you used when generating the CSR or you will receive a certificate name mismatch error in the browser.

I have installed a certificate provided by a trusted Certificate Authority such as Verisign or Godaddy on the vWLAN. I have verified the certificate is valid. I have verified that redirect to hostname is functioning and that the name in the url bar of the browser matches the common name of the certificate (FQDN). Why am I still receiving a certificate error from the browser indicating the certificate was not issued by a trusted certificate

authority? Occasionally some browsers will give the error when others do not.

Examples of the browser error include:
IE: "The security certificate presented by this website was not issued by a trusted certificate authority".
Firefox: "The certificate is not trusted because the issuer certificate is unknown. (Error code: sec_error_unknown_issuer)".
Safari: "Authentication failed because the server certificate is not trusted."

You may not have installed a required chain/intermediate certificate. Check with your certificate authority if a chain/intermediate certificate is required. Go to logins>ssl certificate>current. Under chain certificate upload Chain CA Certificate: browse for and upload the chain/intermediate certificate obtained from the certificate authority.

I upgraded from a BSC to a vWLAN. Can I restore the configuration from the BSC to the vWLAN?

No. BSC configurations are not compatible with vWLAN.

My Certificate Authority requires a 2048 bit Certificate Signing Request (CSR). How can I generate a 2048 bit CSR on the vWLAN?

Upgrade to the latest software revision. Software version 2.0.0.10 and greater allows you to select a key bit length of 1024 or 2048 when generating a CSR.

Obtaining 14 Digit Product Serial Numbers of BSC, BSAP, BVMS, and vWLAN

BlueSecure Controller (BSC)
-In the web based administrative console go to Maintenance>Upgrade
-It may be necessary to read the serial number off of the physical hardware if you are unable to access the web based administrative console or the serial number is not displayed under Maintenance>Upgrade.

BlueView Management System (BVMS)
-Read the serial number off of the physical hardware as it is not available electronically.

BlueSecure Access Points (BSAP)

BSAP-15XX, BSAP-1600, and BSAP-1700
-Read the serial number off of the physical hardware as it is not available electronically.

BSAP-18XX
-In the web based administrative console of the BSC go to Wireless>AP. The serial number is located in the serial number column. If the serial number column is not displayed it may be necessary to scroll to the right to click customize to add the serial number column.
-In the web based administrative console of the vWLAN go to Provision>Wireless>AP. The serial number is located in the serial number column. If the serial number column is not displayed it may be necessary to scroll to the right to click customize to add the serial number column.
-It may be necessary to read the serial number off of the physical hardware if the BSAP-18XX has not yet discovered the BSC or the vWLAN. Alternatively the serial number can be obtained remotely via SSH. SSH to the ip address of the BSAP-18XX using port 2335. The default username/password is adm1n/blue1socket. Choose the option for Show Version Information from the console.

Virtual Wireless Lan (vWLAN)
-In the web based administrative console go to Platform>Maintain>Upgrade
-It may be necessary to read the serial number off of the physical hardware if you are unable to access the web based administrative console or the serial number is not displayed under Maintenance>Upgrade.

Obtaining Show_Tech and Configuration Backups of BSC, BVMS, and vWLAN

BSC Show_Tech
-In the web based administrative console go to Maintenance>Config Backup/Restore>Show_Tech

BSC Configuration Backup
-In the web based administrative console go to Maintenance>Config Backup/Restore>Backup

BVMS Show_Tech
-In the web based administrative console go to BlueView>Configuration Backup/Restore> Generate Troubleshooting Information

BVMS Configuration Backup
-In the web based administrative console go to BlueView>Configuration Backup/Restore> Backup the BVMS Configuration. Do not check Controller Firmware, Patches, Configurations or AP firmware.

vWLAN Show_tech
-In the web based administrative console go to Platform>Maintain>Config Backup/Restore>Show_Tech

vWLAN Configuration Backup
-In the web based administrative console go to Platform>Maintain>Config Backup/Restore>Show_Tech

---

Obtaining Software/Firmware and Patch versions of BSC, BSAP, BVMS, and vWLAN

BSC Software
-In the web based administrative console Go to Maintenance>Upgrade and look for Current Version
BSC Patches
-In the web based administrative console go to Maintenance>Patch. Under Installed patches you will find a list of patches installed.

BVMS Software
-In the web based administrative console go to BlueView>upgrade. Under Current Partition Information look for the version.
BVMS Patches
-In the web based administrative console go to BlueView>Patch. Under Installed patches you will find a list of patches installed.

vWLAN Software
-In the web based administrative console go to Platform>Maintain>Upgrade and look for Current Version
vWLAN Patches
-In the web based administrative console go to Platform>Maintain>Patch. Under Installed patches you will find a list of patches installed.

BSAP Firmware
-If connected to BSC go to Wireless>AP and look in the firmware column in the BSC¿s web based administrative console
-If connected to vWLAN go to Provision>Wireless>AP and look in the firmware column in the vWLAN¿s web based administrative console
-If not yet connected to BSC or vWLAN connect to the serial console or ssh to the BSAP. Choose show version information from the console menu. See Salesforce solutions for how to connect to serial console or ssh to the BSAP.

What access points are supported by the vWLAN?

The vWLAN is built upon 802.11n technology and therefore requires 802.11n BlueSecure access

points. The vWLAN supports BSAP-1800v1, BSAP-1800v2, and BSAP-1840 BlueSecure access points. The vWLAN does not support legacy BlueSecure 802.11a/b/g access points i.e. BSAP-1500/1540/1700 or 3rd party access points. BSAP18xx's are backwards compatible to support 802.11a/b/g.

What are the rack space, environmental, power consumption and thermal output (BTU) specifications of the vWLAN appliance?

Rack Space: 1U Width: 430.02 mm (16.93 in) Depth: 508 mm (20 in) Height: 42.42 mm (1.67 in)
Operating Temp: 10 to 30 degrees C (50 to 86 degrees F)
Humidity: 90%, non-condensing
Power Consumption: 110-240V, 350 Watts
Thermal Output (BTU): 1660 BTU/h

What is the default administrator user name/password of the web based administration console of the vWLAN?

admin/blue

What is the IP address of the network/management interfaces of a default configuration of the vWLAN?

Network
By default the network interface will obtain an IP address via DHCP. If there is no DHCP server on the network the interface will fall back to 192.168.130.1/24.

Managment
10.251.252.1/24

What ports and protocols do I need to allow in the firewall between the BSAP and vWLAN?

IP Protocol 97 (EtherIP) - Client Data (vWLAN 1.0 ONLY)
TCP/UDP 33333 - Control Channel
UDP port 53 (DNS) - APDiscovery
UDP port 69 (TFTP) - Firmware
TCP port 28000 - RFIDS Channel (vWLAN 2.0 ONLY)

TCP port 80 (HTTP) - Only if Web Auth and or Blueprotect are enabled (vWLAN 2.0 ONLY)
TCP port 443 (HTTPS) - Only if Web Auth and or Blueprotect are enabled (vWLAN 2.0 ONLY)
NAT can be enabled between the BSAP and vWLAN

What type of cable, what terminal emulation settings, and what default username/password is required to connect to the serial console port of the vWLAN?

Cable
DB9 9 Pin Null Modem Serial Cable Female/Female

Terminal Emulation Settings
Bits per second: 9600
Data bits: 8
Parity: none
Stop bits: 1
Flow control: none

Username/Password
vwlan/vwlan

What types of authentication are supported by the vWLAN?

-Local User Database
-MAC
-802.1x
-LDAP/Active Directory
-Radius
-SIP2
-Radius Admin

When performing an authentication test against my Active Directory or LDAP server under Auth>External>Authentication Test why I am receiving an account resolver login failed error message on the vWLAN?

The LDAP user field should be populated with the "full name" not the login name in active directory. All the name parts are used and simply added to each other to compose the full name. The resulting username when using "John" and "Smith" as the first and last name respectively in active directory would be "John Smith".
Unless the LDAP user is in the root of active directory you must specify where it is. This is

referred to as the distinguished name. For example if John Smith is in the Users container you would enter the following in the LDAP User field:
"CN=John Smith,CN=Users,DC=Bluesocket,DC=com" where the first CN refers to Common Name and the second CN refers to Container. If John Smith was in the root of active directory you could simply enter John Smith.

When submitting the Certificate Signing Request (CSR) to the Certificate Authority for an SSL certificate I am required to select a server platform. What platform should I select?

Apache
