Bluesocket BlueSecure Controller (BSC) FAQ

Updated 11/07/2011

20MB space error when attempting to upload AP firmware to the BSC

When attempting to upload AP firmware to the BSC under wireless>firmware the following error may be received:

"Only 20MB of space is available for upload"

The BSC has 20 MB of space allocated for AP firmware. If the above error is received perform the following:

1. Delete the previous version of AP firmware under wireless>firmware BEFORE attempting to upload new AP firmware.

2. Delete any un-used firmware. For example the BSC software image includes BSAP-1800v2/1840 and BSAP-1800v1 AP firmware. Perhaps you only have BSAP-15XXs. If so you could delete the 18XX firmware to make room for the BSAP-15XX Firmware

3. If you have more than 2 BSAP model types you may be required to swap AP firmware as needed when bringing up new BSAPs for the first time or alternatively configure the BSC to store AP firmware on a TFTP server external to the BSC.

Apple Bonjour (Formerly Rendezvous) is unable to locate devices and services that are on the sameBSC managed network as as each other.

Apple Bonjour (Formerly Renezvous) is Apple Inc.'s trade name for its implementation of Zeroconf, a service discovery protocol. The software comes built into Apple's Mac OS X operating system and iOS for iPhone, iPod touch, and iPad from version 10.2 onward, and can be installed onto computers using Microsoft Windows operating systems. Bonjour is also used by several application such as iTunes.

Bonjour locates devices such as printers, other computers, and the services that those devices offer on a local network using broadcast, and multicast traffic. By default BlueSecure Access Points (BSAPs) tunnel traffic back to the BlueSecure Controller (BSC) in EtherIP (IP Protocol 97). By default the BSC does not send broadcast and multicast traffic back out the EtherIP tunnels therefore other clients will not see the traffic and not be able to locate devices and

services. In order to send broadcast and multicast traffic back out the EtherIP tunnels the following routes must be added under network>routing table>create static route entry for the appropriate managed interface.

Broadcast Traffic
Route Destination
192.168.160.255

Route Gateway
255.255.255.255
Netmask
255.255.255.255

Interface
Managed

This above example assumes we are referring to the managed physical network and the subnet is 192.168.160.0/24. If this is a managed vlan the Interface entry should be populated with the appropriate managed vlan.

Multicast Traffic
Route Destination
224.0.0.0

Route Gateway
255.255.255.255

Netmask
240.0.0.0

Interface
Managed

This above example assumes we are referring to the managed physical network. If this is a managed vlan the Interface entry should be populated with the appropriate managed vlan.

You may also be required to allow services in the firewall policy of the appropriate role specific to the application. For example UDP 5353 for multicast DNS.

WARNING. Configuring these broadcast/multicast routes in networks with large broadcast domains/subnets may cause performance issues.

Are BSAPs counted against the user limits?

No. BSAPs are excluded from the concurrent authenticated user limits and only count against the

BSAP limits.

Are the concurrent authenticated user and BSAP limits of the BSC hard limits or can they be over-subscribed?

The concurrent authenticated user limits are hard limits. For example the BSC-600 supports 64 concurrent authenticated users. The 65th user will not be able to authenticate.

The BSAP limits are not currently hard limits but may be enforced in future releases. If you over-subscribe the BSAP limit you will receive the following message in the web based administrative gui.

"Supported Bluesocket Access Point Limit exceeded. Bluesocket recommends upgrading the hardware, as clients may experience degradation. This limit will be enforced in all future releases."

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.

BSC-600/1200 web server will not start after changing timezone

I changed the timezone on my BSC-600/1200 and after a reboot the web server will not start. How can I recover the BSC-600/1200.

1. Start with the BSC powered off. Connect a laptop with a nine-pin null-modem serial cable to the BSC's serial console port. Use a terminal emulation program such as Microsoft HyperTerminal (9600,8,none,1,none).

2. Power on the BSC. Immediately begin to press control-c repeatedly until the interrupt in the boot process stops at a CFE> prompt. There is only a 2-3 second time frame for the interrupt from the time BSC is powered on.

3. Set the date and time at the CFE prompt - commands are "set date" and "set time".

set date dy/mm/dd/yyyy

where dy is day of week: 1-7 for Sunday through Saturday,
mm is month: 1-12 for Jan through Dec
dd is day of month: 1-31
and yyyy is year: 2000-2099

set time hh:mm:ss

4. Verify time and date with:
show time

5. Push the restart button on the front of the box.

6. After the BSC restores log in to the web based administrative console and go to general>time.

7. Set the BSC to synchronize at boot time and configure a valid NTP server to prevent the issue from re-occurring.

Client is able to access the internet through the BSC without logging in or authenticating.

1. Go to Status>Active Connections>All connections.
2. Look for the client's IP address and or mac address in the connections table.
3. Identify what role the client is in.

If the client is in the un-registered role
Before a client authenticates they are placed in the un-registered role. By default, the un-registered role only allows DNS in it's firewall policy. This is so clients can resolve the host name of their original destination and the login page. If the client is able to access the internet it is likely the un-registered role's firewall policy is allowing HTTP/HTTPS to ANY. Clients will be able to access anything that is allowed in the un-registered role before authenticating. At a minimum, DNS should be allowed.

1. Go to User Roles>Roles>Click to edit the un-registered role.
2. Scroll down to the policies section.
3. Make sure you are not allowing HTTP/HTTPS to ANY in the un-registered role's firewall policy. Clients will be able to access anything allowed before authenticating. At a minimum, DNS should be allowed.

If the client is in a role other than the un-registered role
If the client is in a role other than the un-registered role it is likely there is a default role configured on the managed interface that corresponds to the client. When a default role is

configured, as soon as traffic is received from a client on that interface, the BSC automatically puts the user in that role.

1. Go to Network>Managed.
2. If you have more than 1 managed interface click to edit the appropriate one that corresponds to the client. If you only have 1 managed interface configured the properties of that interface will be displayed.
3. Click the interface tab if not already selected.
4. Scroll down to the default role.
5. Select un-registered. Clients will now be redirected to the login page.

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.

Clients are not able to obtain an IP address on the managed remote subnet of the BSC and I am seeing no free leases errors under status>logs.

Examples of error messages under status>logs:
Time Level Application Function Operation Name Message
779885 7/22/2008 12:22 Error DHCP Server dhcp discover no user DHCPDISCOVER from 00:09:1d:00:ee:84 via 172.31.56.253: network 172.31.56.128/25: no free leases
773989 7/22/2008 10:04 Error DHCP Server dhcp discover no user DHCPDISCOVER from 00:11:85:80:3d:15 via 172.31.56.253: network 172.31.56.128/25: no free leases
779980 7/22/2008 12:25 Error DHCP Server dhcp discover no user DHCPDISCOVER from 00:02:3f:81:ba:fd via 172.31.56.253: network 172.31.56.128/25: no free leases

By default the BSC expects the DHCP requests to be sourced from "Default gateway IP address for remote clients to reach the BSC" configured under the managed remote subnet. If dhcp requests can be sourced from addresses other than the "default gateway address for remote clients to reach the BSC" then the "Additional IP addresses that DHCP relay packets can be sourced from" must be populated with these addresses. For example in the error messages above we can see the dhcp discovers are being sourced from 172.31.56.253. This IP address should be configured in the "Additional IP addresses that DHCP relay packets can be sourced from" field under the 172.31.56.128/25 managed remote subnet. If there are multiple IP addresses add them comma separated. This is common for example with environments that use Hot Standby Router

Protocol (HSRP) with virtual IP addresses.

Do I need an additional power supply to enable POE on the managed interface ports of the BSC-600/1200?

I have enabled Power Over Ethernet (PoE) on each of the 4 managed interface ports of my BSC-600/1200 but the 802.3af compliant access points connected will not power up. Do I need an additional power supply to enable POE on the 4 Managed interface ports of the BSC-600/1200?

Yes, an additional power supply is required to enable POE on the 4 managed interface ports of the BSC-600/1200. The ADTRAN part number is 1700925F1.

Do third party access points, for example Cisco access points, count against the BSAP limits or concurrent authenticated user limits of the BSC?

Third party access points do not count against the BSAP limits however if their management interface is on the BSC's managed network and is authenticated to the BSC into an "access point management" role they will count against the concurrent authenticated user limit. Alternatively the management interface of the third party AP can be placed on a dedicated management vlan so that you could manage it via telnet, ssh, https, etc without having to go through the BSC.

Do users in the Un-registered role count against the concurrent authenticated user limits of the BSC?

Before a user authenticates they are placed into the Un-registered role. While the user is in the Un-registered role they do not count against the concurrent authenticated user limit. When the user transitions to their final role upon successful authentication they will count against the concurrent authenticated user limit.

Does the AP or the BSC's managed interface have to be on a trunk port allowing the appropriate vlans? This may be referred to as tagging vlans on some switches.

I want to deploy multiple ssid assigned to multiple managed side vlans. Does the AP or the BSC's managed interface have to be on a trunk port allowing the appropriate vlans? This may be referred to as tagging vlans on some switches.

BlueSecure Access Points
By default BSAPs tunnel traffic back to the BSC in EtherIP (IP Protocol 97). The 802.1q vlan

tagging is performed inside the tunnel and not exposed to the switch. If you are using BlueSecure access points you are not required to put the BSAPs or the BSC's managed interface on trunk ports. They can be placed on access ports. This may be referred to as untagged ports on some switches. The exception to this is the BSAP-1600. BSAP-1600s do not support EtherIP tunneling.

3rd Party Access Points
If you are using 3rd party access points and you want to deploy multiple ssid assigned to multiple managed side vlans both the 3rd party access points and the BSC's managed interface must be placed on trunk ports. This may be referred to as tagging vlans on some switches. Here is an example vlan setup with the BSC, 3rd Party AP and Cisco switches.

-BSC's protected physical interface on vlan 5. This could be the existing wired network or a dmz.
-BSC's managed physical interface on vlan 10. Vlan 10 is used for 3rd party AP management in this example.
-Employee ssid assigned to managed vlan 15
-Guest ssid assigned to managed vlan 20

BSC's Protected Interface Switchport Configuration
Switchport mode access vlan 5

BSC's Managed Interface Switchport Configuration
Switchport mode trunk
Switchport trunk encapsulation dot1q
Switchport trunk allowed vlan 10,15,20
Switchport trunk native vlan 10

3rd Party APs switchport Configuration
Switchport mode trunk
Switchport trunk encapsulation dot1q
Switchport trunk allowed vlan 10,15,20
Switchport trunk native vlan 10

*****The physical interfaces of the BSC cannot send or receive dot1q tags, only the vlan interfaces can. Notice above the protected physical interface is on an access port (untagged) and the managed physical interface is on the native vlan of the trunk (untagged).**

Here is the same example vlan setup with HP switches.

vlan 5
untagged e10
vlan 10
untagged e11,e12
vlan 15
tagged e11,e12
vlan 20

tagged e11,e12

This example assumes the BSC's Protected interface is plugged into switchport e10, Managed interface into e11, and 3rd Party AP into e12.

*****Notice the protected physical and managed physical interfaces are untagged and the managed vlan interfaces are tagged. The physical interfaces of the BSC cannot send or receive dot1q tags, only the vlan interfaces can.**

Wired Support
If you are required to support wired users on the BSC you may be required to put the BSC's managed interface on a trunk port also. For example you may have a conference room where you could assign switchports to the guest vlan 15 so that visitors can get the BSC's login page and be policed by the BSC's role based authorization. If the wired users were placed on the managed physical network trunking/tagging would not be required.

Edge-to-Edge
The Edge-to-Edge feature essentially disables the EherIP tunnel from the BSAP to the BSC on a per ssid basis. Therefore you may be required to put the BSAP and the managed physical interface on trunk ports if you are using the Edge-to-Edge feature. If the Edge-to-Edge ssid is assigned to the managed physical network (vlan 0) then trunking/tagging would not be required.

How can I allow all users to bypass the login page of the BSC and go straight out to the internet without having to authenticate?

Set the default role under network>managed to an appropriate role. Upon obtaining an IP address users will be placed into that role bypassing the login page and authentication.

How do I default the configuration of the BSC?

From the web based administration console:
-Go to maintenance>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 BSC?

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 "a" for admin password recovery. The password of the default administrator username (admin) will be defaulted to blue.

How do I upload more than 1 intermediate certificate to the BSC?

My certificate authority requires more than 1 intermediate certificate. How do I upload more than 1 intermediate certificate to the BSC?

Please upgrade to BSC software release 6.5.1.03 with the IntermediateCertificate-TG8315-6_5_1_03-1 patch or newer. 6.5.1.03 with this patch adds the ability to upload a chain of intermediate certificates. Prior to 6.5.1.03 you could only upload 1 intermediate certificate.

After making sure you are running the minimum software/patch level you will need to obtain an intermediate certificate bundle for apache from the Certificate Authority or create one with the contents of the two certificates and a text editor. Using a text editor such as Notepad or Vi, copy and paste in the contents of the primary intermediate certificate. Then copy and paste in the contents of the 2nd intermediate certificate. In both cases you should include the BEGIN and END tags. Save the file as a .cer file, for example intermediatebundle.cer. After uploading your certificate, browse for the intermediate certificate bundle by clicking the browse button near the chain certificate upload field. Select the file and click upload intermediate.

Example Intermediate Bundle Text:

-----BEGIN CERTIFICATE-----
MIIE0DCCBDmgAwIBAgIQJQzo4DBhLp8rifcFTXz4/TANBgkqhkiG9w0BAQUFADBf
MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVB
AsT
LkNsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkw
HhcNMDYxMTA4MDAwMDAwWhcNMjExMTA3MjM1OTU5WjCByjELMAkGA1UEBhM
CVVMx
FzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZWZXJpU2lnbiBUcnVz
dCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2lnbiwgSW5jLiAtIEZv
ciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJpU2lnbiBDbGFzcyAz
IFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzUwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAgIKXo1nmAMqudLO07cfLw8
RRy7K+D+KQL5VwijZIUVJ/XxrcgxiV0i6CqqpkKzj/i5Vbext0uz/o9+B1fs70Pb

ZmIVYc9gDaTY3vjgw2IIPVQT60nKWVSFJuUrjxuf6/WhkcIzSdhDY2pSS9KP6HBR
TdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQGBO+QueQA5N06tRn/
Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+rCpSx4/VBEnkjWNH
iDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/NIeWiu5T6CUVAgMB
AAGjggGbMIIBlzAPBgNVHRMBAf8EBTADAQH/MDEGA1UdHwQqMCgwJqAkoCKGIGh0
dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA4GA1UdDwEB/wQEAwIBBjA9
BgNVHSAENjA0MDIGBFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVy
aXNpZ24uY29tL2NwczAdBgNVHQ4EFgQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMwbQYI
KwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCG
gQU
j+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9nby5naWYwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwO
i8v
b2NzcC52ZXJpc2lnbi5jb20wPgYDVR0lBDcwNQYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDAwYJYIZIAYb4QgQBBgpghkgBhvhFAQgBMA0GCSqGSIb3DQEBBQUA
A4GBABMC3fjohgDyWvj4IAxZiGIHzs73Tvm7WaGY5eE43U68ZhjTresY8g3JbT5K
lCDDPLq9ZVTGr0SzEK0saz6r1we2uIFjxfleLuUqZ87NMwwq14lWAyMfs77oOghZ
tOxFNfeKW/9mz1Cvxm1XjRl4t7mi0VfqH5pLr7rJjhJ+xr3/
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIF7DCCBNSgAwIBAgIQbsx6pacDIAm4zrz06VLUkTANBgkqhkiG9w0BAQUFADCB
yjELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQ
QL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJp
U2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxW
ZXJpU2lnbiBDbGFzcyAzIFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0
aG9yaXR5IC0gRzUwHhcNMTAwMjA4MDAwMDAwWhcNMjAwMjA3MjM1OTU5WjCBt
TEL
MAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLE
xZW
ZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2UgYXQg
aHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDEvMC0GA1UEAxMmVmVy
aVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzMwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCxh4QfwgxF9byrJZenraI+nLr2wTm4i8rCrFbG
5btljkRPTc5v7QlK1K9OEJxoiy6Ve4mbE8riNDTB81vzSXtig0iBdNGIeGwCU/m8
f0MmV1gzgzszChew0E6RJK2GfWQS3HRKNKEdCuqWHQsV/KNLO85jiND4LQyUhhDK
tpo9yus3nABINYYpUHjoRWPNGUFP9ZXse5jUxHGzUL4os4+guVOc9cosI6n9FAbo
GLSa6Dxugf3kzTU2s1HTaewSulZub5tXxYsU5w7HnO1KVGrJTcW/EbGuHGeBy0RV
M5l/JJs/U0V/hhrzPPptf4H1uErT9YU3HLWm0AnkGHs4TvoPAgMBAAGjggHfMIIB

2zA0BggrBgEFBQcBAQQoMCYwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcml
z
aWduLmNvbTASBgNVHRMBAf8ECDAGAQH/AgEAMHAGA1UdIARpMGcwZQYLYIZIA
Yb4
RQEHFwMwVjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nw
czAqBggrBgEFBQcCAjAeGhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMDQG
A1UdHwQtMCswKaAnoCWGI2h0dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMtZzUu
Y3JsMA4GA1UdDwEB/wQEAwIBBjBtBggrBgEFBQcBDARhMF+hXaBbMFkwVzBVFglp
bWFnZS9naWYwITAfMAcGBSsOAwIaBBSP5dMahqyNjmvDz4Bq1EgYLHsZLjAlFiNo
dHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvLmdpZjAoBgNVHREEITAfpB0w
GzEZMBcGA1UEAxMQVmVyaVNpZ25NUEtJLTItNjAdBgNVHQ4EFgQUDURcFlNEwYJ+
HSCrJfQBY9i+eaUwHwYDVR0jBBgwFoAUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMwDQYJ
KoZIhvcNAQEFBQADggEBAAyDJO/dwwzZWJz+NrbrioBL0aP3nfPMU++CnqOh5pfB
WJ11bOAdG0z60cEtBcDqbrIicFXZIDNAMwfCZYP6j0M3m+oOmmxw7vacgDvZN/R6
bezQGH1JSsqZxxkoor7YdyT3hSaGbYcFQEFn0Sc67dxIHSLNCwuLvPSxe/20majp
dirhGi2HbnTTiN0eIsbfFrYrghQKlFzyUOyvzv9iNw2tZdMGQVPtAhTItVgooazg
W+yzf5VK+wPIrSbb5mZ4EkrZn0L74ZjmQoObj49nJOhhGbXdzbULJgWOw27EyHW4
Rs/iGAZeqa6ogZpHFt4MKGwlJ7net4RYxh84HqTEy2Y=
-----END CERTIFICATE-----

How many concurrent authenticated users and BSAPs does each model BSC support?

BSC-600: 64 Users/8 BSAP
BSC-1200: 200 Users/25 BSAP
BSC-2100: 400 Users/50 BSAP
BSC-2200: 400 Users/50 BSAP
BSC-3200: 1500 Users/100 BSAP
BSC-5200: 4000 Users/150 BSAP

Although the user licensing is based on concurrent authenticated users, it is recommended you consider and plan for unregistered users, that is users that are connected to the system but not yet authenticated, in your user count when sizing the appropriate controller for your organization as unregistered users consume system resources. For best performance have a mixture of authentication types. For example 802.1X authentication, mac authentication, and web based authentication. Having all web based authentication may have an adverse affect on the BSC?s web server performance.

I am associated to the access point but if I go to Status>Active Connections>APs in the BSC I do not see my client associated.

The BSC polls the BSAPs for the information displayed under Status>Active Connections>APs based on the "Time in minutes between checking APs" setting under wireless>AP. By default this is set to 10 minutes so the BSAPs will be polled every 10 minutes for this information. Adjust to 1 minute.

I am setting up Internal 802.1x Authentication on the BSC. The BSC 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 BSC?

With internal 802.1x both BSAPs and 3rd Party APs are configured to send RADIUS requests to the BSC. The BSC is the RADIUS server and terminates EAP. The BSC then proxies inner methods i.e. PAP, CHAP, MSCHAP, MSCHAPv2 to the external RADIUS server. All RADIUS requests are sourced by the BSC's protected 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 BSC with the protected interface IP address or DNS name.

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

With Transparent 802.1x both BSAPs and 3rd Party APs are configured to send RADIUS requests to the RADIUS server. BSAPs however tunnel these requests in EtherIP (IP Protocol 97) to the BSC and the BSC then forwards them on to the RADIUS server. All RADIUS requests from the BSAPs are sourced by the BSC's protected interface IP address and therefore you are not required to configure a RADIUS client in the RADIUS server for every single BSAP. You only need to configure a RADIUS client in the RADIUS server for the BSC with the protected

interface IP address or DNS name.

3rd Party access points however do not tunnel RADIUS request to the BSC and therefore you are required to configure a RADIUS client in the RADIUS server for every single 3rd Party AP. Alternatively configure a RADIUS client in the RADIUS server for the 3rd Party APs with an IP range.

I am trying to renew my ssl certificate on the BSC but I do not see an option to generate a CSR on the weblogins>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 BSC. 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 BSC 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 BSC that is already in the client's list of trusted root certificate authorities.

I cannot make more than one client connection to a Microsoft file share over the BSC. Are there any known issues with Microsoft file shares and the BSC?

See Microsoft Knowledgebase article: http://support.microsoft.com/kb/301673

When two client computers try to use the server message block (SMB) protocol to connect to the same server across a network address translation (NAT) device, the more recent client connection may reset the earlier client connection. If a client and a server that use the SMB protocol over a NAT device are copying files, that session may be reset when another client uses the SMB protocol over the same NAT device to the same server. By default the BSC NATs the managed networks to the protected interface IP address. Bluesocket¿s recommendation is to disable NAT on the BSC. Go to network>managed>click to edit the appropriate managed interface/vlan and uncheck NAT the addresses to the protected interface address. You will need to add a route back to that managed network in your router on the protected network. For example if the managed network is 192.168.160.0/24 and the protected interface ip address is 192.168.130.1 you would have to add the following route to your router:

ip route 192.168.160.0 255.255.255.0 192.168.130.1

You also need to make sure the managed network for example 192.168.160.0/24 is Natted out your firewall**.**

I have an existing SSL certificate for the Microsoft IIS server platform that I would like to use on the BSC. 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 web 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 general>http in the BSC 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: bsc1.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 BSC's Fully Qualified Domain Name (FQDN) and the protected 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 protected interface IP address. You should be returned the FQDN. Assuming the client is using the same DNS server configured on the protected interface of the BSC. For example C:\>nslookup 192.168.130.1 assuming 192.168.130.1 is the protected interface IP address. If not, add the PTR, test with nslookup to confirm, and then reboot the BSC. The BSC 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 installed a cert provided by a trusted CA on the BSC but I am still receiving a certificate error.

I have installed a certificate provided by a trusted Certificate Authority such as Verisign or Godaddy on the BSC. 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 web logins>ssl>current. Under chain certificate upload Chain CA Certificate: browse for and upload the chain/intermediate certificate obtained from the certificate authority.

I upgraded from one BSC to another for example a BSC-5000 to a BSC-5200. Can I restore the configuration from the BSC-5000 to the BSC-5200?

Yes. On the BSC-5000 for example go to maintenance>configuration backup/restore and backup your configuration. Then on the BSC-5200 for example go to maintenance>configuration>backup/restore and restore the configuration that you previously backed up from the BSC-5000. You can restore a configuration from any BSC model to any BSC model as long as the BSC that you are restoring to is running the same or newer software release. You cannot restore a configuration from a newer software release to an older software release. If you are running version 5.2 or prior, you must upgrade to 5.3.2.6 first to adjust the configuration file before restoring it to a BSC running 6.x.

Maintenance access required to proceed to License Agreement Error Message on BSC

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. If you attempt to upgrade directly to 6.X from 5.2 or prior you may receive the following error when accessing the web based administration console after the upgrade:

"Maintenance access required to proceed to License Agreement".

To recover from this error you will need to 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 the option for switch followed by a reboot to switch back to the partition running 5.2 or prior. Then upgrade to 5.3.2.6 before upgrading to 6.X.

My BSC-2100/2200/3200/5200 will not boot. There is no access to the secure web based administrative console or the serial port console menu. How can I recover the BSC?

Serial port boot interrupt/manual switch of partitions (BSC-2100/2200/3200/5200)

Introduction

This document explains how to perform a serial port boot interrupt to manually switch to the alternate partition when there is no access to the secure web based administrative console or the serial port console menu. This process is typically used for recovery of a BSC-2100/2200/3200/5200 that will not complete a boot of the active partition. If you can successfully boot to the alternate partition you can then perform an upgrade. The upgrade is applied to the alternate partition so it will repair the original partition. For further info on upgrades see BSC software upgrade documentation.

Requirements

Ensure that you meet these requirements before you attempt this process:

-Basic knowledge of how to use a terminal emulation application such as Microsoft HyperTerminal.

- Physical access to the BSC's serial console port.

-A nine pin null-modem serial cable.

-A laptop running a terminal emulation application such as Microsoft HyperTerminal.

Components Used

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

- BSC-2100/2200/3200/5200 running any software image.

- A laptop running Microsoft Windows XP with a terminal emulation application such as Microsoft HyperTerminal.

In summary we will access the BSC via the serial console port. Using a laptop running a terminal emulation application such as Microsoft HyperTerminal we will attempt to interrupt the boot process to get to a boot: prompt where we can manually switch partitions. If we can successfully boot to the alternate partition we can then perform an upgrade. The upgrade is applied to the alternate partition so it will repair the original partition. For further info on upgrades see BSC software upgrade documentation.

1. Start with the BSC powered off. Connect a laptop with a nine-pin null-modem serial cable to the BSC¿s serial console port. Use a terminal emulation program such as Microsoft HyperTerminal (9600,8,none,1,none).

2. Power on the BSC. Immediately begin to press the TAB key repeatedly until the interrupt in the boot process stops at the boot: prompt. There is only a 2-3 second time frame for the interrupt from the time BSC is powered on. You will see:

```
LILO boot
hda5 hda6
boot:
```

-- OR --

```
LILO boot
hda6 hda5
boot:
```

The second line of the boot interrupt indicates the two partitions. The first in list is the ACTIVE partition. The second in list is the ALTERNATE partition.

3. At the boot: prompt type hda5 or hda6 and then press enter. You want to choose the second in the list for the alternate partition.
4. If you can successfully boot to the alternate partition you can then perform an upgrade. The upgrade is applied to the alternate partition so it will repair the original partition. For further info on upgrades see BSC software upgrade documentation.

My BSC-600/1200 did not automatically power back on after several quick power failures. I had to remove the power cord from the power supply, plug it back in, and press the ON/OFF button. Is this normal?

The BSC-600/1200 power supply is designed to protect itself. It has a protected mode feature that often times not only saves the power supply unit from being blown out but also the motherboard and other components from being damaged. If there was an abrupt power spike, or the power went off, came on, went off again, the power supply is put into protected mode. Once it's in protected mode, the normal solution is to remove the power cord from the power supply for roughly 30 seconds, plug it back in, and press the ON/OFF button. It is recommended the BSC-600/1200 be plugged into a UPS (Universal Power Supply).

My BSC-600/1200 will not boot. There is no access to the secure web based administrative console or the serial port console menu. How can I recover the BSC?

Serial port boot interrupt/manual switch of partitions (BSC-600/1200)

Introduction
This document explains how to perform a serial port boot interrupt to manually switch to the alternate partition when there is no access to the secure web based administrative console or the serial port console menu. This process is typically used for recovery of a BSC-600/1200 that will not complete a boot of the active partition. If you can successfully boot to the alternate partition you can then perform an upgrade. The upgrade is applied to the alternate partition so it will repair the original partition. For further info on upgrades see BSC software upgrade documentation.

Requirements
Ensure that you meet these requirements before you attempt this process:
-Basic knowledge of how to use a terminal emulation application such as Microsoft HyperTerminal.

-Physical access to the BSC's serial console port.
-A nine pin null-modem serial cable.
-A laptop running a terminal emulation application such as Microsoft HyperTerminal.

Components Used
The information in this document is based on these hardware and software versions:
-BSC-600/1200 running any software image.
-A laptop running a terminal emulation application such as Microsoft HyperTerminal.

In summary we will access the BSC via the serial console port. Using a laptop running a terminal emulation application such as Microsoft HyperTerminal we will attempt to interrupt the boot process to get to a CFE> prompt where we can manually switch partitions. If we can successfully boot to the alternate partition we can then perform an upgrade. The upgrade is applied to the alternate partition so it will repair the original partition. For further info on upgrades see BSC software upgrade documentation.

1. Start with the BSC powered off. Connect a laptop with a nine-pin null-modem serial cable to the BSC's serial console port. Use a terminal emulation program such as Microsoft HyperTerminal (9600,8,none,1,none).

2. Power on the BSC. Immediately begin to press control-c repeatedly until the interrupt in the boot process stops at a CFE> prompt. There is only a 2-3 second time frame for the interrupt from the time BSC is powered on.

3. Assuming the current runtime is "A" perform the following to switch to the "B" partition:
-At the CFE> boot prompt type setenv -p BSYS B then enter (setenv -p BSYS A to boot from the A partition)
-Then type reset -sysreset -yes then enter
-This will boot to the "B" partition. If your current runtime is B, replace B with an A in the setenv command.

4. If you can successfully boot to the alternate partition you can then perform an upgrade. The upgrade is applied to the alternate partition so it will repair the original partition. For further info on upgrades see BSC software upgrade documentation.

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

Upgrade to the latest software revision. Software version 6.5.0.8 and greater allows you to select

a key bit length of 1024 or 2048 when generating a CSR.

No redirect to the BSC's login page with Windows 7 clients

Allow HTTP outgoing to the OCSP and CRL urls of your SSL certificate in the un-registered role.

The default behavior of many of the browsers today for example Windows 7 with IE8 is if it cannot check the validity of the SSL certificate it considers it invalid. The unfortunate thing is the browser does not display a message or anything to indicate it could not validate the certificate it simply just doesn't display a page or displays a generic page cannot be displayed message. Before a client is authenticated they are placed in the un-registered role. By default the un-registered role only allows DNS outgoing therefore the browser is unable to check the validity of the certificate and doesn't redirect to the login page.

If you go to web logins>ssl certificate on the right hand side you will see the properties of your certificate. There you should see the OCSP (Online Certificate Status Protocol) or CRL (Certificate Revocation List) urls. You may see one or both depending on the certificate. The browser uses these to check the validity of the certificate.

Go to user roles>roles>click to edit the un-registered role>policies and allow HTTP to the OCSP and CRL urls. It is recommended you upgrade to a minimum of 6.5.1.03 before allowing HTTP to the urls as this software release introduces destination hostnames to account for the multiple ip addresses that may resolve to a host name.

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.

Receiving page cannot be displayed when trying to upload AP firmware to the BSC.

Due to the size of the AP firmware, your connection to the BSC's web server may be dropped if you reach the web server hold time before the upload is finished. Temporarily set the web server hold time to 300, upload the ap firmware, and then set back to 10.

1. Go to General>HTTP.
2. Temporarily set Seconds a client is allowed to hold the web server to 300>save.
3. You may be prompted to click here to apply. This will restart the web server. This will be non-intrusive to users on the system. They will not be dropped but you will be dropped for a brief moment from the secure web based administration console.

4. Upload your ap firmware.
5. Now change go back and change the web server hold time back to 10. It is important the web server hold time is set to 10 during normal operation.

Slow or no redirect to the BSC's login page and slow or no access to the BSC's web based administration console

Adjust the seconds a client is allowed to hold the web server under general>http from a default value of 300 to 10.

While clients are in the un-registered role the BSC's job is to redirect their port 80 requests and whatever other ports are being monitored under general>http>HTTP/proxy ports to monitor to the login page. Each client has multiple background processes running for example windows updates, antivirus updates, tool bars, etc that continually perform requests as they are unable to access these services in the un-registered role. Each one of these requests will by default hold onto the BSC's web server for 300 seconds. Adjusting this to 10 will free up web server resources in environments with many users in the un-registered role. It is recommended this setting be adjusted to 300 before an upgrade so that the status of the upgrade may be maintained but to adjust to 10 thereafter. You may be prompted to click here to apply after adjusting this setting. This will restart the web server. This will be non-intrusive to users on the system. They will not be dropped but you will be dropped for a brief moment from the secure web based administration console.

Supported Bluesocket Access Point Limit exceeded. Bluesocket recommends upgrading the hardware, as clients may experience degradation. This limit will be enforced in all future releases error message on the BSC.

Why I am receiving the following error message in the web based administrative console of the BSC after an upgrade:
"Supported Bluesocket Access Point Limit exceeded. Bluesocket recommends upgrading the hardware, as clients may experience degradation. This limit will be enforced in all future releases."

You have exceeded the supported BSAP limit. The supported BSAP limits are not currently hard limits but may be enforced in future releases. If you over-subscribe the supported BSAP limit you will receive the above message in the web based administrative gui.

The BSC is dropping clients from the connection table. I am using DHCP relay.

If you are using DHCP relay the "Time in seconds before idle connections are timed out" under general>misc should be greater than or equal to your dhcp lease time in your external dhcp server. The default value is 600 seconds. If the BSC does not see the dhcp renew at half the lease interval the client will be dropped from the connections table.

This BSC is not associated to a wireless regulatory domain error message

I am receiving the following error: "This BSC is not associated to a wireless regulatory domain. Click here to go to the AP setup to enter the authorization code". All radios are disabled. What is this code for and where can I obtain it?

Based on United States FCC and European DFS and ETSI regulations, Bluesocket now requires customers to validate the country that Bluesocket Access Points are being operated in. The administrator must set the country to the proper country and then enter the corresponding authorization code under wireless>global. Please contact support for your country authentication code. 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.

Troubleshooting NO redirect to the BSC login page

1. Make sure the client is able to resolve DNS.

The client must be able to resolve DNS in order to be redirected to the login page. From a cmd prompt of a client try pinging or performing an nslookup for www.google.com or www.yahoo.com to see if the fully qualified domain name resolves to an ip address.

If you are unable to resolve DNS check the un-registered role to make sure DNS is allowed outgoing to any destination or to your specific dns server(s) (user roles>roles>click to edit un-registered role>policies).

If you are allowing DNS outgoing in the un-registered role but you are still unable to resolve DNS, try statically configuring the DNS settings on the client for public DNS servers for example 4.2.2.1 and 4.2.2.2.

If you are able to resolve DNS and get redirected to a login page after statically configuring the DNS settings on the client, check your DNS server or configure replacement DNS server ip addresses under network>protected or network managed>DHCP server.

2. Check the list of HTTP/proxy ports to monitor under general>http.

By default the BSC monitors requests to port 80 from clients in the un-registered role. If the client makes a request to a port other then 80 they will not be redirected to the login page. For example the client could have their home page set to an https page (443) or the clients browser could be configured for proxy utilizing another port. If that is the case add the ports comma seperated for example 80,443,8081 to the comma separated list of HTTP/proxy ports to monitor under general>http.

3. Allow HTTP outgoing to the OCSP and CRL urls of your SSL certificate in the un-registered role.

The default behavior of many of the browsers today for example Windows 7 with IE8 is if it cannot check the validity of the SSL certificate it considers it invalid. The unfortunate thing is the browser does not display a message or anything to indicate it could not validate the certificate it simply just doesn't display a page or displays a generic page cannot be displayed message. Before a client is authenticated they are placed in the un-registered role. By default the un-registered role only allows DNS outgoing therefore the browser is unable to check the validity of the certificate and doesn't redirect to the login page.

If you go to web logins>ssl certificate on the right hand side you will see the properties of your certificate. There you should see the OCSP (Online Certificate Status Protocol) or CRL (Certificate Revocation List) urls. You may see one or both depending on the certificate. The browser uses these to check the validity of the certificate.

Go to user roles>roles>click to edit the un-registered role>policies and allow HTTP to the OCSP and CRL urls. It is recommended you upgrade to a minimum of 6.5.1.03 before allowing HTTP to the urls as this software release introduces destination hostnames to account for the multiple ip addresses that may resolve to a host name.

4. Adjust the seconds a client is allowed to hold the web server under general>http from a default value of 300 to 10.

While clients are in the un-registered role the BSC's job is to redirect their port 80 requests and whatever other ports are being monitored under general>http>HTTP/proxy ports to monitor to the login page. Each client has multiple background processes running for example windows updates, antivirus updates, tool bars, etc that continually perform requests as they are unable to access these services in the un-registered role. Each one of these requests will by default hold onto the BSC's web server for 300 seconds. Adjusting this to 10 will free up web server resources in environments with many users in the un-registered role. It is recommended this setting be adjusted to 300 before an upgrade so that the status of the upgrade may be maintained but to adjust to 10 thereafter. You may be prompted to click here to apply after adjusting this setting. This will restart the web server. This will be non-intrusive to users on the system. They will not be dropped but you will be dropped for a brief moment from the secure web based administration console.

Unable to see windows file and printer shares of devices that are on the same BSC managed network as as each other.

Windows uses broadcast traffic to resolve the netbios names of file and printer shares that are on the same local subnet. By default BlueSecure Access Points (BSAPs) tunnel traffic back to the BlueSecure Controller (BSC) in EtherIP (IP Protocol 97). By default the BSC does not send broadcast traffic back out

the EtherIP tunnels therefore other clients will not see the traffic and not be able to see file and printer shares. In order to send broadcast traffic back out the EtherIP tunnels the following routes must be added under network>routing table>create static route entry for the appropriate managed interface.

Broadcast Traffic
Route Destination
192.168.160.255

Route Gateway
255.255.255.255

Netmask
255.255.255.255

Interface
Managed

This above example assumes we are referring to the managed physical network and the subnet is 192.168.160.0/24. If this is a managed vlan the Interface entry should be populated with the appropriate managed vlan.

You may also be required to allow services in the firewall policy of the appropriate role. For example TCP port 139 and UDP port 137,138 for NetBIOS and TCP 445 for SMB.

WARNING. Configuring this broadcast route in networks with large broadcast domains/subnets may cause performance issues.

Unable to Transparent Proxy HTTPS on BSC

We have Transparent Proxy enabled in the role with the appropriate proxy server:port and HTTP ports to proxy on the BSC. We are unable to transparently proxy HTTPS. We tried to add port 443 to the list of HTTP ports but received the following error:

"HTTPS (443) is an encrypted protocol and cannot be transparently proxied."

Why can't I transparently proxy HTTPS?

Transparent proxy does not support HTTPS traffic. You cannot transparently proxy HTTPS as a nature of the HTTPS protocol. This would be considered a man in the middle type of attack.

Users that are inactive or have gone out of wireless range for some period of time are getting dropped from active connections of the BSC and have to re-authenticate.

Users that are inactive or have gone out of wireless range for some period of time are getting dropped from active connections of the BSC and have to re-authenticate. An example would be a device that has gone into sleep mode or an employee who has taken their laptop with them outside of the wireless coverage area for a lunch meeting.

You can adjust the "Time in seconds before idle connections are timed out" under general>misc>connection tracking. The default is 600 seconds (10 minutes). This means if a client is inactive or goes away for 10 minutes they will be dropped from the BSC's active connection table and have to re-authenticate. You could adjust this to 4 hours for example, 1/2 of a business day. This must be set to greater than or equal to your DHCP lease. If you are using the BSC's DHCP server you can find the DHCP lease under network>managed>click to edit the appropriate managed network interface>DHCP server tab. If you are using DHCP relay make sure the setting is greater than or equal to your DHCP lease time in your external DHCP server. If the BSC does not see the DHCP renew at half the lease interval the client will be dropped from the connections table.

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

BSC-600/1200
Rack Space: 1U Width: 380 mm (15 in) Depth: 290 mm (11.5 in) Height: 44.5 mm (1.75 in)
Operating Temp: 10 to 35 degrees C (50 to 95 degrees F)
Humidity: 40 to 80%, non-condensing
Power Consumption: 110-240V, 220 Watts
Thermal Output (BTU): 750 BTU/h
*Optional BSC-600/1200 PoE Power Supply (BSC-POE-000-00-00): 100-240V, 80 Watts, 275 BTU/h

BSC-2200/3200/5200
Rack Space: 2U Width: 445 mm (17.5 in) Depth: 450mm (17.7 in) Height: 89 mm (3.5 in)
Operating Temperature: 10 to 35 degrees C (50 to 95 degrees F)
Humidity: 40 to 80%, non-condensing
Power Consumption: 110-240V, 350 Watts
Thermal Output (BTU): 1200 BTU/hr

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

admin/blue

What is the default serial console password of the BSC?

wg1000s

What is the difference between Transparent 802.1x and Internal 802.1x authentication on the BSC?

Transparent 802.1x
-Supports the following EAP types.
-EAP-TLS
-TTLS
-PEAP
-Cisco-LEAP
-MD5
-Supports machine authentication.
-Required to apply group policy, run login scripts, and allow logins by non-cached domain users.
-Access points send RADIUS requests to RADIUS server.
-Requires certificate installed on RADIUS server.

Internal 802.1x
-Supports the following EAP types.
-TTLS
-PEAP
-FAST
-Does NOT support machine authentication.
-Can't apply group policy, run login scripts and non-cached domain users will not be able to login.
-Access points send RADIUS requests to BSC. BSC is the RADIUS server and terminates EAP.
-BSC can authenticate user against local user database.
-Proxy inner method (i.e. PAP, CHAP, MSCHAP, MSCHAPv2) to external RADIUS server.
-*Authenticate user directly against LDAP server if LDAP server has readable attribute containing the MD4 hash of the user's password.
**Microsoft Active Directory does NOT have a readable attribute containing the MD4 hash of the users password and therefore authenticating directly against MS AD is NOT supported. Use IAS or NPS with MS AD.*
-Leverages certificate already installed on BSC.
-Allows you to support 802.1x authentication without deploying a RADIUS server(Local User DB/LDAP) or with a RADIUS server that doesn't support EAP.

What is the IP address of the protected/managed/admin interfaces of a default configuration of the BSC?

Protected
By default the protected interface will obtain an IP address via DHCP. If there is no DHCP server on the protected network the protected interface will fall back to 192.168.130.1/24. The protected interface ip address is displayed on the LCD.

Managed

192.168.160.1/24
DHCP Server enabled

Admin
10.1.1.1/24

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

IP Protocol 97 (EtherIP) - Client Data
TCP/UDP 33333 - Control Channel
UDP 53 - APDiscovery
NAT can NOT be enabled between the BSAP and BSC

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

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

Password
wg1000s

What types of authentication are supported by the BSC?

-Local User Database
-MAC
-802.1x
-LDAP/Active Directory
-Radius
-SIP2
-Transparent NTLM
-NTLM
-CAS
-Cosign
-Kerberos

-Pubcookie

What will cause a primary BSC to failover to a standby BSC?

1. Losing link status on either the protected, managed, or failover interfaces
2. Losing power either abruptly or with a graceful shutdown
3. Internal crash due to a software failure
4. Exceeding preset thresholds

-High Average CPU/Memory Utilization
-Hard Disk Usage

Preset thresholds are configured in the web based administrative console under General>thresholds.

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

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

Where can I find visio stencils for BSC/BSAP product line?

http://www.adtran.com/web/fileDownload/doc/24884

Why am I receiving a license file required error when trying to access the web based administrative console after rebooting or restarting the BSC?

If you refresh the screen a few moments later do you still receive the error? In releases prior to 6.5 the BSC could potentially start the web server before reading the license file. You could therefore access the web based administrative console because the web server had started but you would receive a license file required error because the license file had not yet been read. Wait a few moments, once the license file is read you will no longer receive the error. This is resolved in the latest software release. Upgrade to the latest software release.
