

Tech Note

LHM

SonicWALL Lightweight Hotspot Messaging

Introduction

SonicWALL Lightweight Hotspot Messaging (LHM) defines the method and syntax for communications between a SonicWALL wireless access device (such as a SOHO TZW, a TZ170 Wireless, or a SonicPoint with a management SonicWALL security appliance) and an Authentication Back-End (ABE) for the purpose of authenticating Hotspot users and providing them parametrically bound network access. The following illustration depicts a generic configuration:

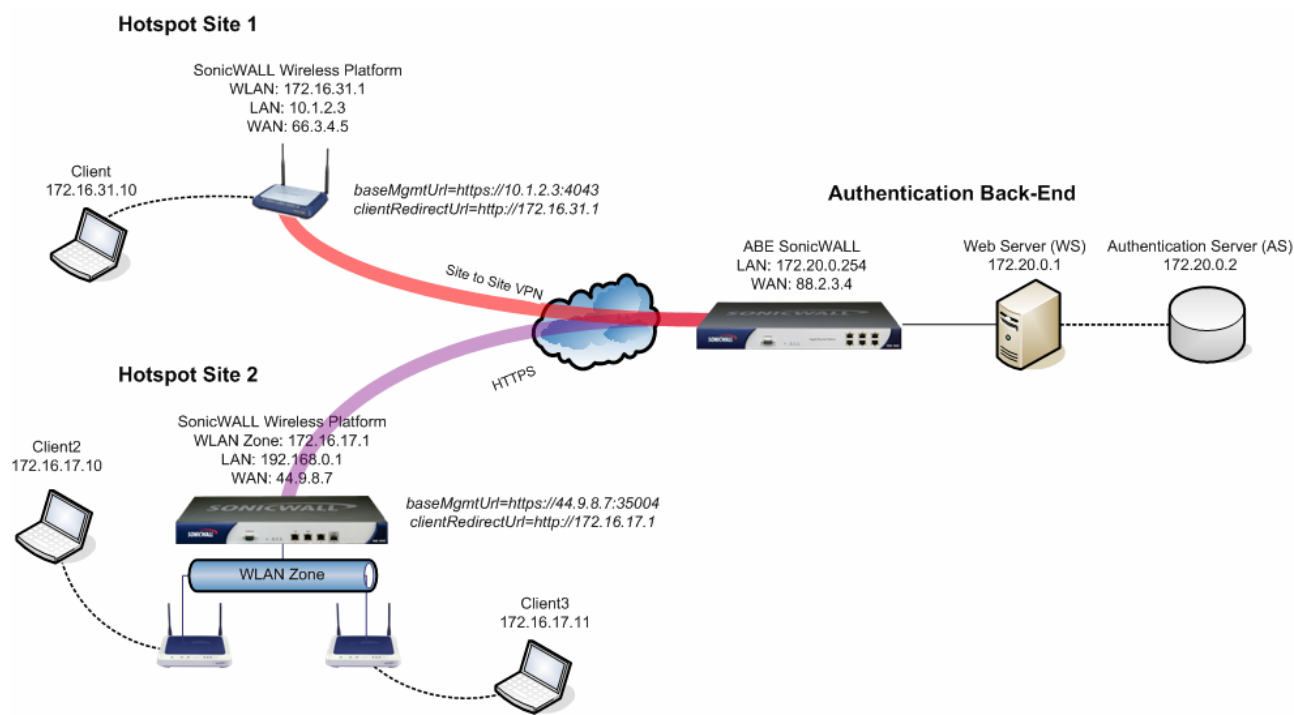


Figure 1 – Configuration Example

LHM allows network operators to provide centralized management of multiple Hotspot locations by providing an interface between SonicWALL's Wireless Guest Services and any existing ABE. LHM is an adaptation of the generalized WISPr¹ and GIS² specifications. LHM was designed to satisfy the requirements of a particularly common operational environment rather than a broad set of environments. Specifically, LHM allows for Hotspot user management and authentication to occur entirely on the network operator's ABE, supporting any method of account creation and management, and any extent of site customization and branding. This approach enables integration into any existing environment without dependencies upon particular billing, accounting or database systems, and also provides the network operator with unrestricted control of the site's design, from look-and-feel to redirection.

Description

The ABE consists of a Web Server (WS) to host content for user interaction and an (optional) Authentication Server (AS) to provide directory services authentication. The AS can be any kind of user database, including, but not limited to RADIUS, LDAP, or AD; the only requirement is that the WS can communicate with the AS for authentication purposes. The WS and AS can be administered on a single server or on separate servers.

¹ WISPr document reference: http://www.wi-fi-allyance.org/opensections/downloads/WISPr_V1.0.pdf

² GIS document reference: http://www.ipass.com/pdfs/gis_doc_v1.3.pdf

Tech Note

LHM also provides the ability for the AS to use the SonicWALL security appliance's internal user database for user authentication. Refer to the Message Format – Local Authentication Request and Reply sections for details on the messaging.

The ABE will need to communicate with the Hotspot SonicWALL to exchange result codes and session information. All communications will be HTTPS and can occur either directly (such as to the LAN, WAN, X0 interface of the SonicWALL security appliance) or over a VPN tunnel to one of the SonicWALL security appliance's management interface addresses. The LHM management interface will be selectable, and only the selected interface will accept LHM management messaging through automatically added Access Rules.

LHM communications will occur on a specific LHM management port that must be defined on the SonicWALL security appliance, and the LHM management port must be different from the standard HTTPS Management port. The default LHM port will be set to TCP 4043. To further secure communications between the SonicWALL and the ABE, it will be possible to optionally use HMAC authentication for exchanged data. Refer to the Message Authentication section for syntax.

To allow the ABE to communicate with the SonicWALL, and to redirect clients to the appropriate interface on the SonicWALL, two parameters will be constructed by the SonicWALL and passed to the ABE. The following communication parameters should be used for all communications between the ABE and the SonicWALL.

- *baseMgmtUrl* - The IP address and the port that the ABE uses to communicate with the SonicWALL. It contains the HTTPS protocol designator, the IP of the selected LHM management interface, and the LHM port (e.g. <https://10.1.2.3:4043>).
- *clientRedirectUrl* - The IP address (and optionally, the port) on the SonicWALL to which clients are redirected during various phases of the session, i.e. the LAN management IP on the TZW, or the WLAN IP on a SonicOS Enhanced device (e.g. <http://172.16.31.1>).

The parameter values will be passed to the ABE by the SonicWALL during Session Creation (see below) and during the Session State Sync (see the Message Format section), and should be used by the ABE as the base in the construction of all relevant URLs. The following are the pages on the SonicWALL that will be referenced by the ABE:

- [wirelessServicesUnavailable.html](#) – ABE is unavailable message. This redirect will typically be sent by the SonicWALL, but can also be referenced by the ABE. Text is configurable (see 'Web Content' tab in Figure 2).
- [externalGuestRedirect.html](#) – Initial redirect message provided by the SonicWALL on session creation. Text is configurable (see Web Content tab in Figure 2).
- [externalGuestLogin.cgi](#) – The page to which the ABE POSTs session creation data.
- [externalGuestLogout.cgi](#) – The page to which the ABE POSTs session termination data.
- [localGuestLogin.cgi](#) – The page to which the ABE POSTs for authenticating user credentials against the SonicWALL's internal user database.
- [createGuestAccount.cgi](#) – The page to which the ABE POSTs to create a guest account in the SonicWALL's internal user database.



Tech Note

For communications from the SonicWALL to the ABE, URLs (including host, port, and page/resource) hosted on the ABE will be fully configurable at the SonicWALL (see the General and Auth Pages tabs in Figure 2 below). The host can be specified using either an IP address or Fully Qualified Domain Name (FQDN). When using FQDN, the name will be resolved upon first use and will be stored by the SonicWALL as an IP address.

The figure displays four screenshots of the SonicWALL LHM Configuration pages, arranged in a 2x2 grid. Each screenshot is a Microsoft Internet Explorer window titled "External Guest Authentication - Microsoft Internet Explorer provid...".

- Top Left Screenshot (Local Web Server Settings):** Shows the "General" tab. It includes sections for "Local Web Server Settings" (Secure Communications Port: 4043, Client Redirect Protocol: HTTPS), "External Web Server Settings" (Web Server: HTTP, Host: 10.0.67.64, Port: 80, Connection Timeout: 15 Seconds), and "Message Authentication" (Enable Message Authentication: checked, Authentication Method: HMAC - MD5, Shared Secret: Shared Secret).
- Top Right Screenshot (External Authentication Pages):** Shows the "Auth Pages" tab. It includes a section for "External Authentication Pages" with fields for Login Page (login.asp?rc=1), Session Expiration Page (login.asp?rc=2), Idle Time Out Page (login.asp?rc=3), and Max Sessions Page (login.asp?rc=4).
- Bottom Left Screenshot (Redirect Message):** Shows the "Auth Pages" tab. It includes sections for "Redirect Message" (Use default selected, Customize: [text area], Note: Text may include HTML formatting, Preview button) and "Server Down Message" (Use default selected, Customize: [text area], Note: Text may include HTML formatting, Preview button).
- Bottom Right Screenshot (Auto-Session Logout):** Shows the "Auth Pages" tab. It includes sections for "Auto-Session Logout" (Enable Auto-Session Logout: checked, Auto-logout Expired Sessions Every: 5 Minutes, Logout CGI: autoLogout.asp), "Server Status Check" (Enable Server Status Check: checked, Check Status Every: 1 Minutes, Server Status CGI: statusCheck.asp), and "Session Synchronization" (Enable Session Synchronization: checked, Synchronize Every: 5 Minutes, Session Sync CGI: sessionSync.asp).

Figure 2 – SonicWALL LHM Configuration pages

Tech Note

The phases of a session lifecycle are described in the following sections:

- Session Creation
 - Session Window Popup
- Idle Timeout
- Session Timeout
- User Logout
- Administrator Logout
- WS Server Status Check
- Session State Sync

The Session Popup Window and WS Server Status Check components will also be described.

Tech Note

Session Creation

Occurs when a wireless client attempts access, and the SonicWALL has no active session information for that client based upon MAC address.

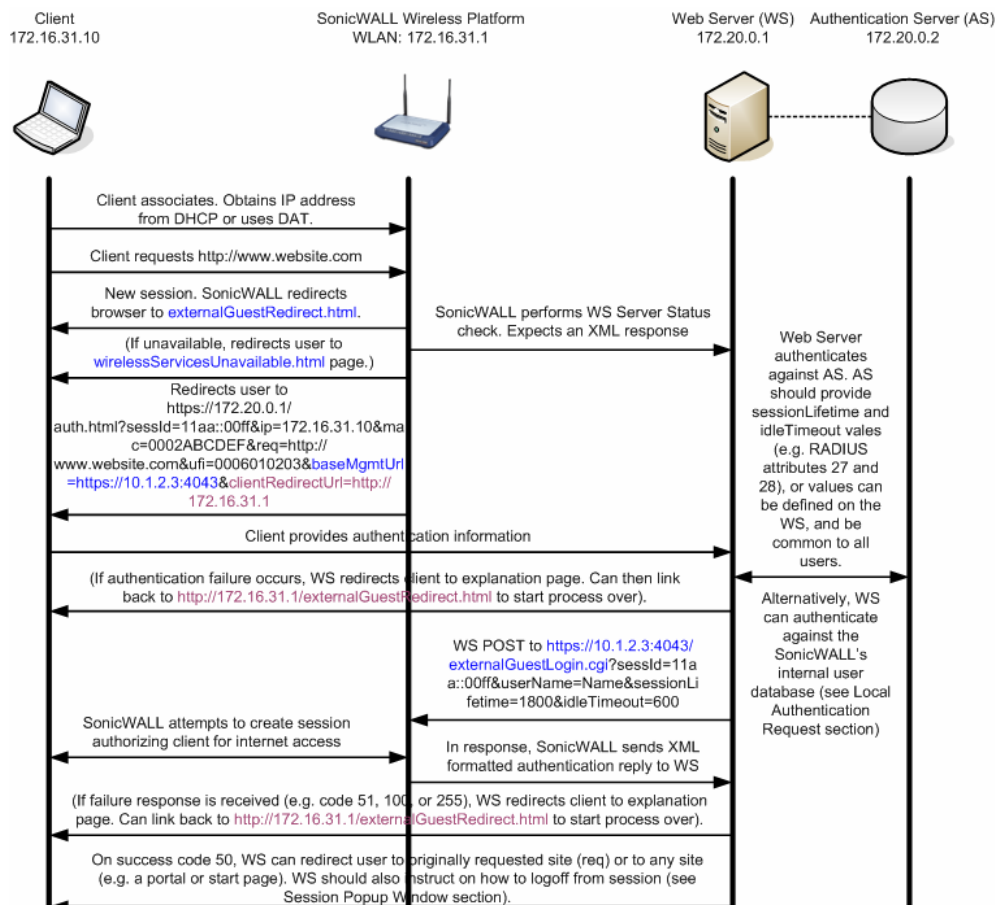


Figure 3 – Session Creation flow

- Wireless client associates with SonicWALL. Obtains IP Address from internal DHCP server, or uses static addressing with Dynamic Address Translation (DAT) feature.
- Client requests web-resource <http://www.website.com>
 - SonicWALL determines that this is a new session.
- SonicWALL redirects client to internally hosted externalGuestRedirect.html page. The externalGuestRedirect.html page provides administrator configurable text explaining that the session is being redirected for authentication.
- During this redirect, the SonicWALL checks the availability of the ABE via a JavaScript redirect attempt to the configured target redirect page.
 - If the redirect to the WS fails to occur within a specified period (the value will be configurable on the SonicWALL, between 1 and 30 seconds) the SonicWALL will redirect the session the internal "wirelessServicesUnavailable.html" page.
- In addition to the JavaScript availability check, an optional full "WS Server Status Check" will be available from the SonicWALL (see 'WS Server Status Check'). This option can be configured to run at a configurable interval between 1 and 60 minutes. In the event of an error response code (1, 2, or 255), the SonicWALL will log the response and will redirect the browser to the internal "wirelessServicesUnavailable.html" page. This page will provide administrator configurable text explaining recourse.

Tech Note

6. If available, the SonicWALL redirects client to authentication portal hosted on AS at:
<https://172.20.0.1/auth.html?sessId=11aa::00ff&ip=172.16.31.10&mac=0002ABCDEF&req=http://www.website.com&ufi=0006010203&baseMgmtUrl=https://10.1.2.3:4043&clientRedirectUrl=http://172.16.31.1>
 - a. "sessId" — A 32 byte hex representation of a 16 byte MD5 hash value generated by the SonicWALL, which will be used by the SonicWALL and the WS for indexing clients (e.g. "11aa3e2f5da3e12ef978ba120d2300ff").
 - b. "ip" — The client IP address.
 - c. "mac" is the client MAC address.
 - d. "req" — The originally requested web-site is passed as an argument to the authentication server)
 - e. "ufi" — The SonicWALL Unique Firewall Identifier. To be used for site identification, if desired.
 - f. "baseMgmtUrl" — The protocol, IP address, and port on the SonicWALL with which the IP will subsequently communicate.
 - g. "clientRedirectUrl" — The protocol, IP address (and optionally port) on the SonicWALL that the ABE will use for client redirection.
7. Client provides authentication information (e.g. username, password, token, etc.).
8. WS validates user against AS.
 - a. AS provides session specific information, namely, Session Timeout and Idle Timeout values.
 - b. Session specific values can optionally be applied globally by the WS rather than obtained from the AS; some value simply needs to be passed to the SonicWALL.
 - c. Timeout values will be presented in seconds and can range from 1 to 863,913,600 (equal to 9999 days).
9. If authentication fails, the WS should redirect the client to a page explaining the failure. A link should be provided back to [http\(s\)://172.16.31.1/externalGuestRedirect.html](http(s)://172.16.31.1/externalGuestRedirect.html) to restart the process.
10. If successful, the WS connects to the SonicWALL either via HTTPS or via VPN and POSTs
<https://10.1.2.3:4043/externalGuestLogin.cgi?sessId=11aa::00ff&userName=Name&sessionLifetime=1800&idleTimeout=600>
 - a. The SonicWALL will attempt to create the session and will send a result to the WS in the same connection. Results are described in the "Message Format" section.
11. If failure response is received (e.g. code 51, 100, or 255), WS should redirect client to a page explaining the failure. A link can be provided back to: [http\(s\)://172.16.31.1/externalGuestRedirect.html](http(s)://172.16.31.1/externalGuestRedirect.html) to start process over.
12. If successful (code 50), WS can redirect user to the originally requested site (req) or to any site (e.g. a portal or start page). WS should also instruct on how to logoff from session (e.g. bookmark a page, popup window, URL, etc.).

Tech Note

Session Popup Window

It is recommended that sessions be managed via a Session Popup window. This should be a browser window instantiated at the time of Session Creation providing session time information (e.g. lifetime, idle timeout value, timer countdowns, etc.) and a “Logout” button. Sample code will be provided.

- Clicking the “Logout” button ends the session and triggers a “User Logout” event.
- Attempting to close the window should provide a warning message that closing the window will end the session.
- Closing the window ends the session and triggers a “User Logout” event.

Idle Timeout

Event occurs when the idle timeout (specified in Session Creation step 10) is exceeded.

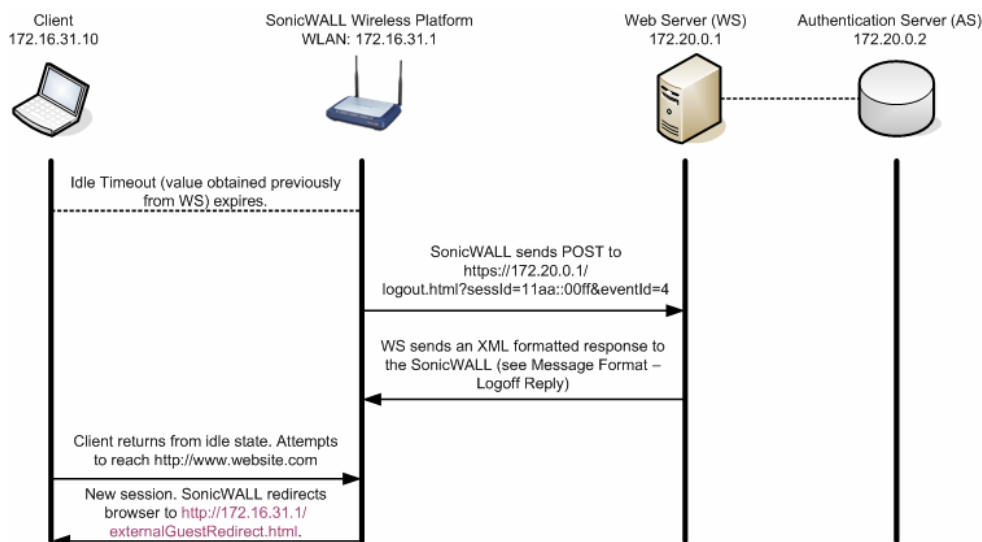


Figure 4 – Session Idle Timeout flow

1. Idle timer (as set during Session Creation) expires.
2. Since the client's browser may not be open at this time, we do not initiate this process with a redirect. Instead, the SonicWALL sends a POST to the WS at: `https://172.20.0.1/logout.html?sessId=11aa::00ff&eventId=4` (see “Message Format” section for Logoff event ID's).
 - a. The resource to which the POST will be sent will be configurable on the SonicWALL.
 - b. The WS hosted page must expect and interpret the sessId and eventId values.
3. The WS will send an XML result to the WS in the same connection. Results are described in the Message Format – Logoff Reply section.
4. If the client returns from the idle state and attempts to reach a web resource, the SonicWALL will redirect the user to the internal `externalGuestRedirect.html` page, starting the Session Creation process over.

Note: To conserve resources, it is recommended that the idle timeout be set to a maximum of 10 minutes.

Session Timeout

Event occurs when the Session lifetime expires. The exchange is the same as the Idle Timeout above, except the Session Timeout eventId value is “3” (instead of “4” for an Idle Timeout).

Tech Note

User Logout

Event occurs when the user actively ends the session by closing their Session Popup window or by using the “Logout” button provided on the Session Popup window. The Session Popup window is the preferred method for user logout, however the same result can be achieved without this method by allowing the session’s lifetime to expire. The latter removes the dependency on the popup window, but manages resources less efficiently.

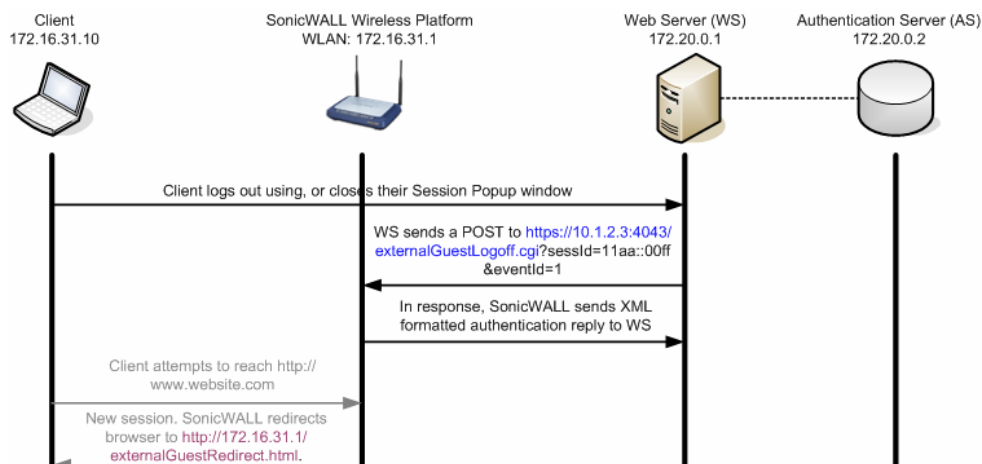


Figure 5 – Active User Logout flow

1. Client logs out using, or closes the session popup window.
2. The WS sends a POST to: <https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=1>. (see “Message Format” section for Logoff event ID’s).
 - a. “sessId” — The value generated during Session Creation by the SonicWALL, which is used by the SonicWALL and the WS for indexing clients.
 - b. “eventId” — Describes the logoff request event.
3. The SonicWALL responds with a result to the WS in the same connection. Results are described in the Message Format – Logoff Reply section.
4. If the client attempts to reach a web resource, the SonicWALL will redirect the user to the internal <http://172.16.31.1/externalGuestRedirect.html> page, starting the Session Creation process over.

Tech Note

Administrator Logout (Optional)

Event occurs when the ABE administrator logs out from a Guest session from the management interface. It will not be possible at this time to terminate ABE-established Guest Sessions from the SonicWALL interface itself. ABE-established Guest Sessions will be represented as such (i.e. distinctly from internal WGS Guest Sessions) on the SonicWALL management UI, and will not be editable.

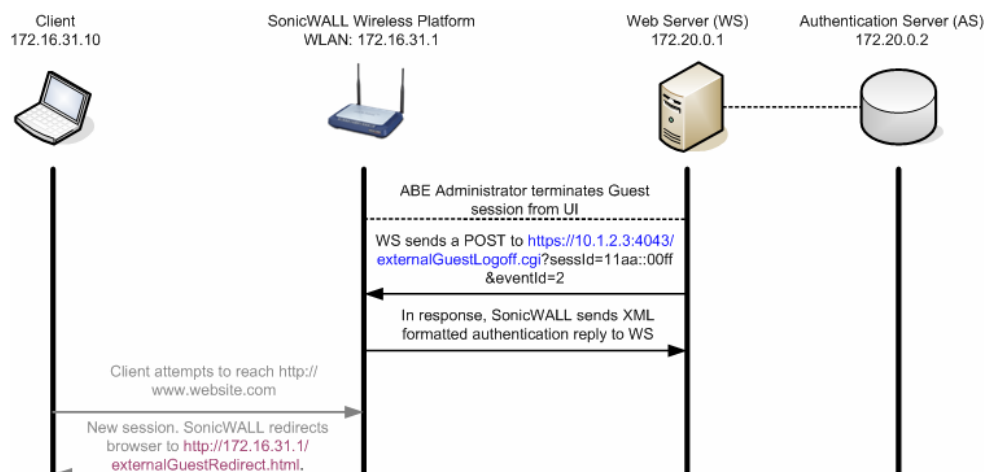


Figure 6 – ABE Administrator User Logout flow

1. ABE administrator terminates the Guest session from the management UI.
2. The WS sends a POST to the SonicWALL:
`https://10.1.2.3:4043/externalGuestLogoff.cgi?sessId=11aa::00ff&eventId=2`. (see “Message Format” section for Logoff event ID’s).
 - a. “sessId” — The value generated during Session Creation by the SonicWALL, which is used by the SonicWALL and the WS for indexing clients.
 - b. “eventId” — Describes the logoff request event.
3. The SonicWALL sends a result to the WS in the same connection. Results are described in the Message Format – Logoff Reply section.
4. If the client returns from the idle state and attempts to reach a web resource, the SonicWALL redirects the user to the internal `http://172.16.31.1/externalGuestRedirect.html` page, starting the Session Creation process over.

WS Server Status Check

To provide more granular ABE status than simple WS availability (as is provided by the mandatory step 4 of ‘Session Creation’, the JavaScript redirect), the SonicWALL can optionally send a secure HTTP GET operation to the WS in order to determine server operational status. The target URL will be configurable, as will the interval of the query (between 1 and 60 minutes). The WS responds back in an XML format listing the server’s current state. Refer to Message Format section for details.

If an error response code (1, 2, or 255) is received (indicating that the WS itself is available, but that some other ABE error condition has occurred), the SonicWALL logs the response and redirects all subsequent authentication requests to an internal “wirelessServicesUnavailable.html” page. This page will provide administrator configurable text explaining recourse.

The SonicWALL will continue to attempt to query the ABE at the configured interval and will resume redirection to the WS (rather than to the wirelessServicesUnavailable.html page) when a response code of 0 (‘Server Up’) is received.

Session State Sync

At a configurable interval (between 1 and 60 minutes), the SonicWALL will optionally send a secure HTTP POST operation to the WS containing an XML list of all currently active guest sessions:

- The feature itself will be enabled via a checkbox on the SonicWALL and will be disabled by default.
- The target URL will be configurable.
- The CGI post will provide the “sessionList” as an XML list of all active guest sessions.
- Refer to Message Format section for detail.

Tech Note

Message Authentication

This feature ensures that the CGI data exchanged between both the SonicWALL and ABE originated from the SonicWALL/ABE device, and that it has not been tampered with. If enabled, an additional CGI parameter named "hmac" will be added to all CGI data exchanged. The following is an example of what the redirect URL now looks like with message authentication enabled:

```
https://10.1.2.3/login.asp?sessionId=faad7f12ac26d5c2fe3236de2c149a22&ip=172.16.31.2&mac=00:90:4b:6a:37:32&ufi=0006B1020148&mgmtBaseUrl=https://10.0.61.222:4043/&clientRedirectUrl=http://192.168.168.168:80/&req=http://www.google.com/&hmac=cd2399aeff26d5c2fe3236d211549acc
```

In the preceding example, the HMAC signature was generated using the following data:

```
HMAC(
    faad7f12ac26d5c2fe3236de2c149a22 +
    172.16.31.2 +
    00:90:4b:6a:37:32 +
    0006B1020148 +
    https://10.0.61.222:4043/ +
    https://10.0.61.222:4043/ +
    http://www.google.com/
)
```

If message authentication is enabled then the SonicWALL device will expect an HMAC signature as part of the CGI post data originating from the ABE. If the SonicWALL detects that the HMAC is missing or incorrect, then an error code of 251 is returned, and the requested operation (e.g. guest login, account creation, etc) is aborted.

Message Format

Notes: The XML Schema location is subject to change.

The SonicWALL IP address and port will be defined in the baseMgmtUrl variable.

External Authentication Request

The WS shall send a secure HTTP POST operation to: <https://sonicwall.ip.add.ress:port/externalGuestLogin.cgi>. The post parameters include the following arguments:

- **sessId:** Session ID
- **userName:** The full user ID
- **sessionLifetime:** The session lifetime of the user (in seconds)
- **idleTimeout:** The max idle timeout (in seconds)

External Authentication Reply

The SonicWALL returns an XML response in the following format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWALLAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWALLAccessGatewayParam.xsd">
  <AuthenticationReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
  </AuthenticationReply>
</SonicWALLAccessGatewayParam>
```



Tech Note

The *{response code}* includes one of the values listed in the following table:

Response Code	Response Meaning
50	Login succeeded
51	Session limit exceeded
100	Login failed -- access reject
251	Msg. Auth failed -- Invalid HMAC
253	Invalid session ID
254	Invalid or missing CGI parameter
255	Internal error

Local Authentication Request

The WS sends a secure HTTP POST operation to: <https://sonicwall.ip.add.ress:port/localGuestLogin.cgi>. The post parameters includes the following arguments:

- **sessId:** Session ID
- **userName:** The full user ID
- **passwd:** The guest's clear-text password

Local Authentication Reply

The SonicWALL returns an XML response in the following format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWALLAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWALLAccessGatewayParam.xsd">
  <AuthenticationReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
  </AuthenticationReply>
</SonicWALLAccessGatewayParam>
```

The *{response code}* includes one of the values listed in the following table:

Response Code	Response Meaning
50	Login succeeded
51	Session limit exceeded
52	Invalid username/password
100	Login failed -- access reject
251	Msg. Auth failed -- Invalid HMAC
253	Invalid session ID
254	Invalid or missing CGI parameter
255	Internal error

Tech Note

Logoff Request

The WS shall send a secure HTTP POST operation to: <https://sonicwall.ip.add.ress:port/externalGuestLogoff.cgi>. The post parameters includes the following arguments:

- **sessId**: GW Session ID
- **eventId**: Logoff event ID. Must be one of the following:
- **rxBytes**: total bytes received
- **txBytes**: total bytes transmitted

Logoff Event ID	Event Meaning
1	Guest logged out manually
2	Admin logged off the specified guest
3	Guest session expired
4	Guest idle timeout expired

Logoff Reply

The SonicWALL returns an XML response in the following format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWALLAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
SonicWALLAccessGatewayParam.xsd">
  <LogoffReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
    <rxBytes>{total bytes received}</rxBytes>
    <txBytes>{total bytes transmitted}</txBytes>
  </LogoffReply>
</SonicWALLAccessGatewayParam>
```

NOTE: <ReplayMessage> tag is only available when logout fails
<rxBytes> and <txBytes> tags are only available when logout success

The {response code} includes one of the values listed in the following table:

Response Code	Response Meaning
150	Logoff succeeded
251	Msg. Auth failed -- Invalid HMAC
253	Invalid session ID
254	Invalid or missing CGI parameter
255	Internal error

Tech Note

WS Server Status Check

The WS returns an XML response in the following format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWALLAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWALLAccessGatewayParam.xsd">
  <ServerStatus >{status code}</ ServerStatus >
</SonicWALLAccessGatewayParam>
```

The *{response code}* includes one of the values listed in the following table:

Response Code	Response Meaning
0	Server Up
1	DB down
2	Configuration error
255	Internal error

Tech Note

Session State Sync

Periodically, the GW will send a secure HTTP POST operation to the AS containing an XML list of all currently active guest sessions. Both the target URL and time period will be configurable by the GW admin.

The CGI post parameters includes the following argument:

- **sessionList:** XML list of all active GW guest sessions.

The session list returns an XML response in the following format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWALLAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
SonicWALLAccessGatewayParam.xsd">
<SessionSync>
  <baseMgmtUrl>[https://ip.add.re.ss:port]</baseMgmtUrl>
  <clientRedirectUrl> http://ip.add.re.ss:port</clientRedirectUrl>
  <SessionCount>{Session Count}</SessionCount>
  <SessionList>
    <Session>
      <ID>{Session ID}</ID>
      <UserName>{User Name}</UserName>
      <IP>{IP Address}</IP>
      <MAC>{MAC Address}</MAC>
      <Idle>
        {Time Idle (expressed in seconds)}
      </Idle>
      <SessionRemaining>
        {Session Remaining (expressed in seconds)}
      </SessionRemaining>
      <RxBytes>
        {total bytes received}
      </RxBytes>
      <TxBytes>
        {totl bytes transmitted}
      </TxBytes>
    </Session>
  </SessionList>
</SessionSync>
</SonicWALLAccessGatewayParam>
```

Session State Sync Reply

The WS returns an XML response in the following format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWALLAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
SonicWALLAccessGatewayParam.xsd">
<SessionSync>
  <ResponseCode>{response code}</ResponseCode>
</SessionSync>
</SonicWALLAccessGatewayParam>
```



Tech Note

The *{response code}* includes one of the values listed in the following table:

Response Code	Response Meaning
200	Sync successful
201	Sync failed
255	Internal error

Local Account Creation Request

The WS sends a secure HTTP POST operation to: <https://sonicwall.ip.add.ress:port/createGuestAccount.cgi>. The post parameters includes the following arguments:

- **userName:** The full user id (max length: 32)
- **passwd:** The guest's clear-text password (max length: 64)
- **comment:** Optional (max length: 16). Default=NULL
- **enforceUniqueLogin:** Optional: 1=true, 0=false. Default=1
- **activateNow:** Optional: 1=true, 0=false. Default=0
- **autoPrune:** Optional: 1=true, 0=false. Default=1
- **accountLifetime:** The account lifetime of the user (expressed in seconds)
- **sessionLifetime:** The session lifetime of the user (expressed in seconds)
- **idleTimeout:** The max idle timeout (expressed in seconds)

Local Account Creation Reply

The SonicWALL returns an XML response in the following format:

```
<?xml version="1.0" encoding="UTF-8">
<SonicWALLAccessGatewayParam
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="http://www.sonicwall.com/
  SonicWALLAccessGatewayParam.xsd">
  <AccountCreationReply>
    <ResponseCode>{response code}</ResponseCode>
    <ReplyMessage>{reply message}</ReplyMessage>
  </AccountCreationReply>
</SonicWALLAccessGatewayParam>
```

The *{response code}* includes one of the values listed in the following table:

Response Code	Response Meaning
10	Account creation succeeded
11	Max account limit
12	Account Exists
251	Msg. Auth failed -- Invalid HMAC
254	Invalid or missing CGI parameter
255	Internal error

Date: October 7, 2005
Version 1.6.2

