Now.WAP Proxy v2011

NowMobile.com Limited
Bourne House
475 Godstone Road
Whyteleafe, CR3 0BL, UK

http://www.nowsms.com
http://www.nowwap.com

E-Mail: nowsms@nowsms.com
UK Telephone : +44 1883 621100

Now.WAP Proxy

The Now.WAP Proxy is a high performance WAP Gateway that is designed to meet the needs of WAP 2.x and multimedia applications, especially MMS (Multimedia Messaging Service) and Java downloads. With WAP providing the underlying protocol support for multimedia object delivery to mobile clients, the explosive growth of MMS services is placing heavy demands on conventional WAP gateways. The Now.WAP Proxy was designed to meet the needs of new MMS services, as well as legacy WAP applications.

The Now.WAP Proxy provides full WAP gateway support for WAP v1.1, v1.2, v1.2.1, v1.3 and v2.0 WAP clients.

The Now.WAP Proxy can support WAP 2.0 clients using either Wireless Profiled HTTP/TCP (W-HTTP and W-TCP), or the WSP protocol stack.

Segmentation and re-assembly (SAR) is supported to provide support for larger object delivery to MMS (Multimedia Messaging Service) clients.

To implement WAP Push and MMS services in conjunction with Now.WAP, we recommend the use of the Now SMS/MMS Gateway. More information regarding the Now SMS/MMS Gateway can be found at http://www.nowsms.com.

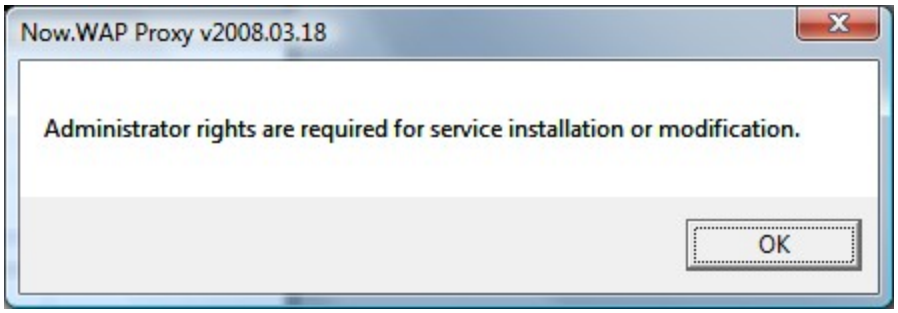
The Now.WAP Proxy can be installed on Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 2003 Server and Windows 2008 Server platforms. Both 32-bit and 64-bit platforms are supported. A 64-bit service version of the Now.WAP service is automatically installed on 64-bit platforms to provide increased speed and scalability.

This help file provides details for configuring the Now.WAP Proxy.

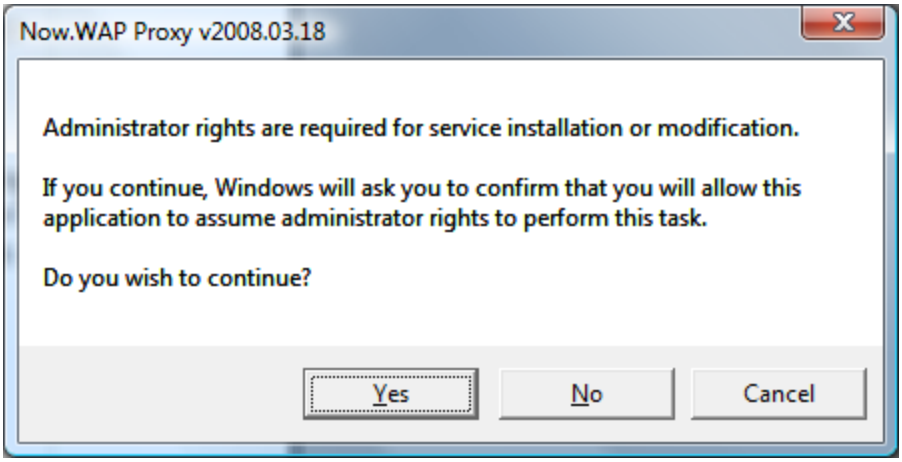
Installing Now.WAP as a Service

For automatic operation, Now.WAP is best installed as a service. Services are automatically started by Windows when the machine is started. When Now.WAP is configured to run as a service, it will always be available, as long as the machine running Now.WAP is powered on and connected to the network.

In order to operate as a service, ***Now.WAP must be installed when logged into Windows with a user account that has administrative privileges for the local machine***. At startup, the Now.WAP configuration program will check to see that it has the required privileges to install or modify services. If these privileges are not available, Now.WAP will display an error message indicating that "Administrator rights are required for service installation or modification". To correct this error, you must login to Windows with a user account that has administrative privileges.



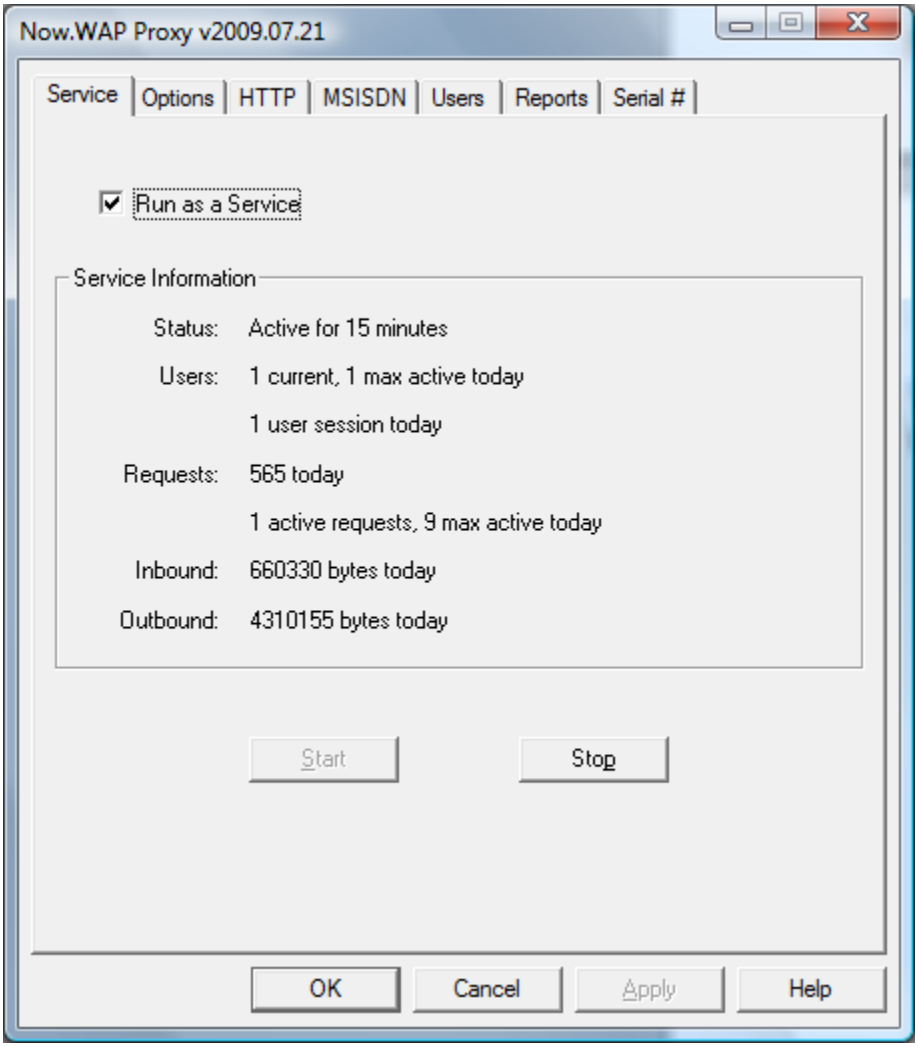
In Windows Vista and Windows Server installations, even though you are logged in with an administrator account, Now.WAP may have to ask for further permission to access administrative tasks. In this case, Now.WAP will display the following dialog:



After you confirm this dialog by pressing the "Yes" button, Windows will blank the screen and display a further dialog indicating that wap3gx.exe is requesting administrative privileges. It is necessary to select "Allow" to continue with the Now.WAP installation or configuration.

Assuming that the necessary rights are available, the Now.WAP configuration can continue.

The “Service” tab of the configuration dialog provides setup options for installing Now.WAP as a service.



Check “Run as a service” to install and start the Now.WAP service.

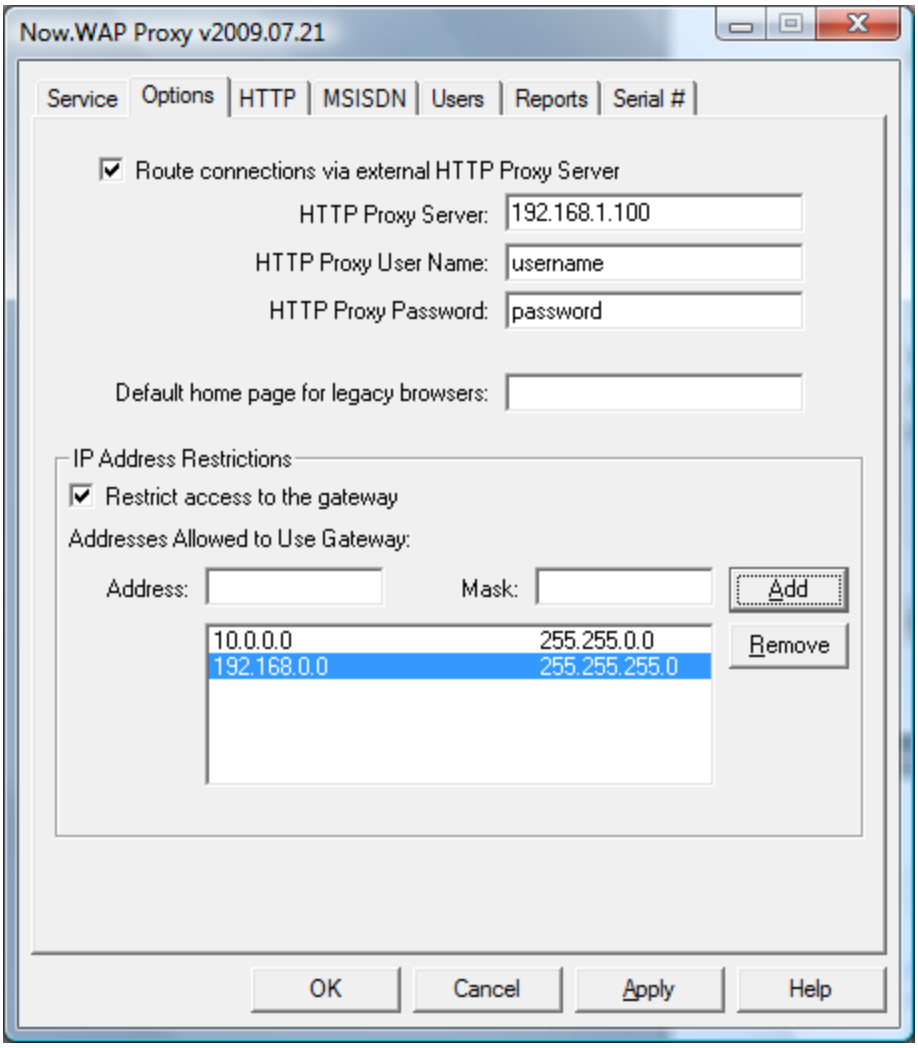
The “Start” and “Stop” buttons can be used to start and stop the service.

To remove the Now.WAP service from the Windows services registry, uncheck “Run as a service”.

The “Service” tab of the configuration dialog also displays information about the status of the currently running service, indicating how long the service has been running, the number of currently active users, and the number of requests processed by the gateway.

General Configuration Options

The “Options” tab of the configuration dialog is used for setting some of the more commonly used configuration options for the gateway.



Check the “Use HTTP Proxy Server” checkbox if the gateway should forward all HTTP requests through an HTTP proxy server. Provide the IP address of the HTTP proxy server in the “HTTP Proxy Server” field. If a port number other than 80 is used by the proxy server, add a colon (:) and the port number to the proxy server IP address (e.g., 192.168.1.1:2080). If the HTTP Proxy Server requires a username and password for access, supply these settings in the “HTTP Proxy User Name” and “HTTP Proxy Password” fields.

Older versions of the OpenWave/Phone.com browser installed on some phone models do not allow the home page to be set on the phone. For these legacy browsers, a default home page can be specified in the "Default home page for legacy browsers" field. Please specify a complete URL such as http://wap.mydomain.com/home.wml.

The "IP Address Restrictions" settings can be used to restrict access to the gateway to a pre-defined set of IP addresses. If "Restrict access to the Gateway" is checked, then only the IP addresses listed in the "Addresses Allowed to Use Gateway" table will be allowed to access the gateway. If "Restrict access to the Gateway" is not checked, then any device can connect to the gateway.

When adding IP Address restrictions, both an IP address and mask are specified. For example, to restrict access to only the IP address of 192.168.1.101, specify that address and a mask of 255.255.255.255. To restrict access to all IP addresses in the range 192.168.1.1 thru 192.168.1.254, specify any address within that range, and a mask of 255.255.255.0.

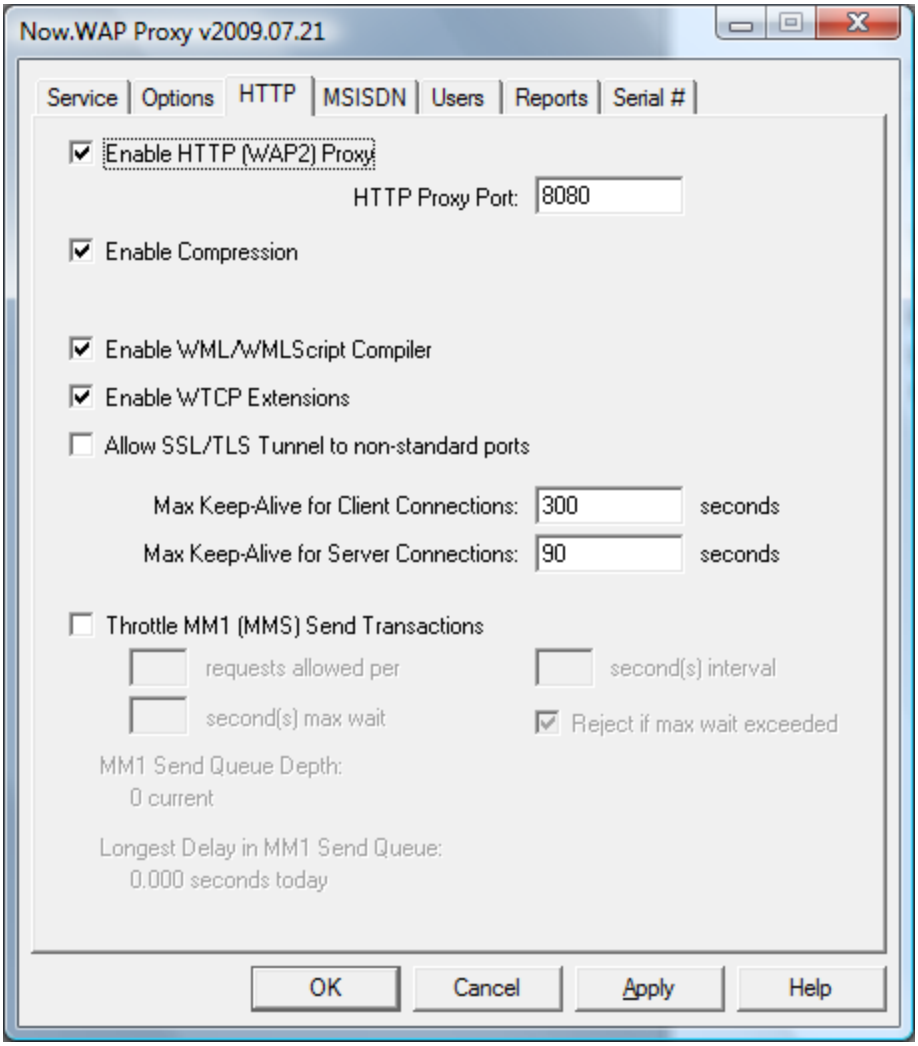
After entering an IP address and mask, click "Add" to add the entry to the list.

To remove an address from the allowed list, highlight the entry and click "Remove".

Note that after making any configuration changes in this dialog, it is necessary to click "Apply" or "OK" for the changes to be saved.

HTTP Proxy Options

The Now.WAP Proxy includes an HTTP Proxy Server interface that can be utilised by WAP 2.0 clients which support Wireless Profiled HTTP and TCP (W-HTTP and W-TCP). This interface can also be used as an HTTP proxy to provide speed enhancements for web browsing via a PC over a GPRS modem or other wireless connection.



The HTTP (WAP2) Proxy server interface is enabled by checking “Enable HTTP (WAP2) Proxy”, and specifying an available port number on the local PC to be used as the “HTTP Proxy Port”. HTTP and WAP2 clients must then be configured to connect to the Now.WAP Proxy on this port to use the proxy services.

When the “Enable Compression” setting is enabled, the Now.WAP Proxy will automatically compress requested files before transmitting them to the receiving client (when compression is supported by the receiving client).

When the “Enable WTCP Extensions” setting is enabled, the Now.WAP Proxy will enable certain Wireless Profile TCP extensions to provide optimum performance for wireless clients.

Both the “Enable Compression” and “Enable WTCP Extensions” settings are enabled by default. It is recommended that these settings only be changed for troubleshooting purposes.

The Now.WAP Proxy supports SSL/TLS tunneling, to support end-to-end encryption between WAP2 and HTTP clients and content servers. By default, the Now.WAP Proxy only supports SSL/TLS tunneling to content servers via the standard HTTP SSL/TLS port of 443. If you wish to enable SSL/TLS tunneling to other ports, check the “Allow SSL/TLS Tunnel to non-standard ports” setting.

To help achieve optimum performance, the Now.WAP Proxy uses HTTP “Keep-Alive” connections whenever possible. By default, Now.WAP will allow a client device to maintain a “Keep-Alive” connection to the proxy for up to 300 seconds. This means that a connected device can remain connected to the proxy for up to 300 seconds without making a request, eliminating the need to re-connect for each request. This value can be changed by entering a new value in the “Max Keep-Alive for Client Connections” field. A value of “0” can be used to disable all “Keep-Alive” connections to client devices.

Similarly, the Now.WAP Proxy will maintain “Keep-Alive” connections to content servers whenever possible. By default, after issuing a request to a content server that supports “Keep-Alive”, Now.WAP will keep that connection alive for up to 90 seconds, and will re-use the connection for any additional requests. This value can be changed by entering a new value in the “Max Keep-Alive for Server Connections” field. A value of “0” can be used to disable all “Keep-Alive” connections to content servers.

Throttle MM1 (MMS) Send Transactions

Now.WAP is frequently used as a WAP Proxy front-end for an MMSC that facilitates MMS messaging services.

Some MMSC configurations may have limits on the number of MMS send transactions that are allowed per second.

Now.WAP can be configured to throttle MM1 send transactions, delaying them from being forwarded to the MMSC, in order to stay within licensing thresholds.

This throttling functionality is enabled by checking "Throttle MM1 (MMS) Send Transactions".

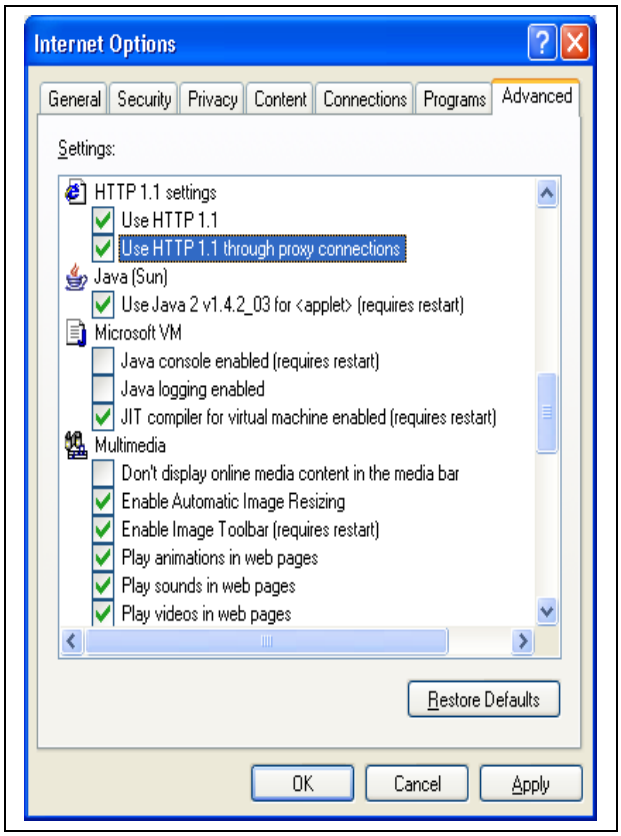
Throttling restrictions are defined as a number of messages (requests) allowed per second. To define a threshold of 3 messages per second, specify "3 requests allowed per 1 second(s) interval". To define a a threshold of 1 message every 2 seconds, specify "1 requests allowed per 2 second(s) interval".

Most MMS clients will timeout if a response is not received within a timeout value that is specific to the MMS client. Therefore, it is necessary to specify a maximum amount of time that Now.WAP will hold the request if too many requests are already being throttled. In most instances, you will not want to allow a request to be held for more than 60 seconds, in order to prevent unnecessary client retries. When the maximum timeout is reached, the default behaviour of Now.WAP is to forward the request to the MMSC, even though the threshold has been exceeded. Alternatively, if "Request if max wait is exceeded" is checked, Now.WAP will return an error to the MMS client indicating that the network is busy and the request should be retried at a later time.

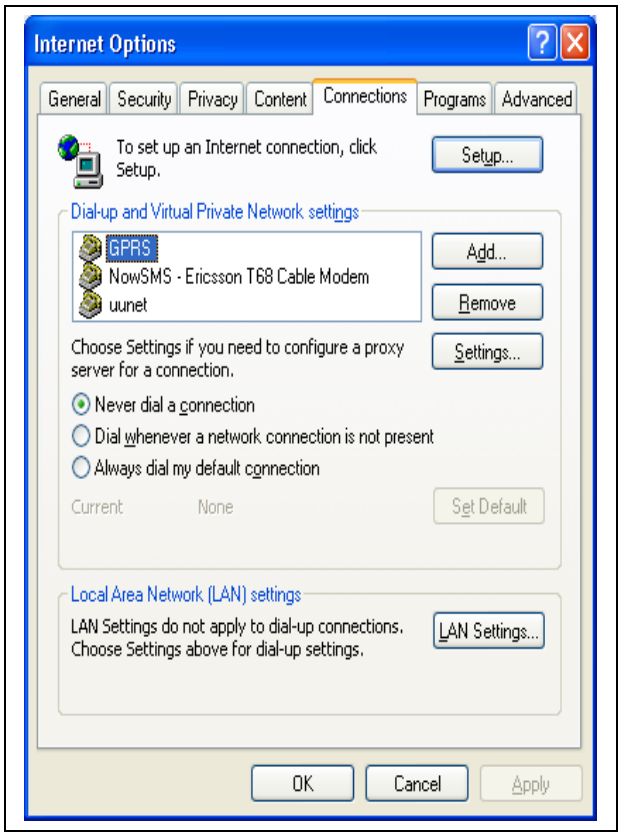
Now.WAP Proxy for PC Web Browser Connections

To use the Now.WAP Proxy to provide increased speed for connections from a web browser running on a PC, it is necessary to configure the web browser to use the Now.WAP Proxy as an HTTP 1.1 proxy for HTTP (and optionally HTTPS) connections. To configure these settings in Internet Explorer, follow these steps:

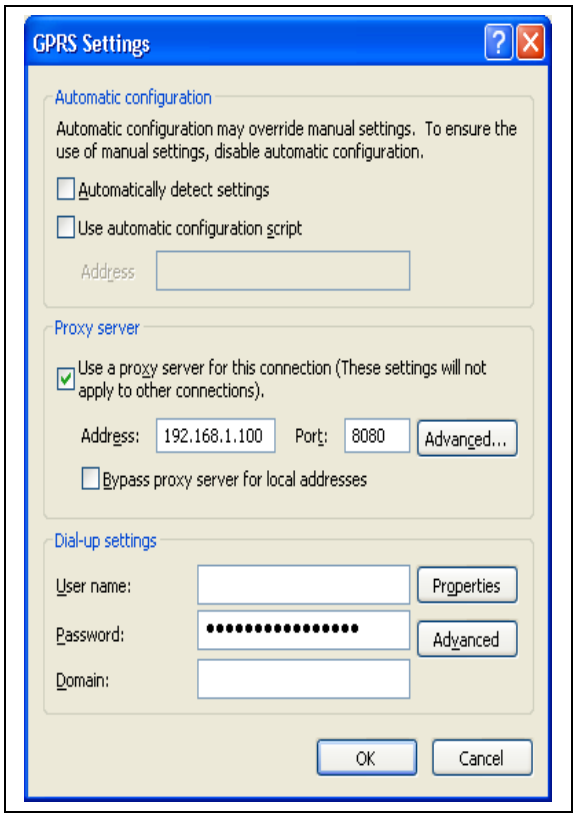
Under Tools/Internet Options/Advanced, find the entry "Use HTTP 1.1 through proxy connections" and make sure this setting is checked. (Compression of content is only supported in the HTTP 1.1 interface.)



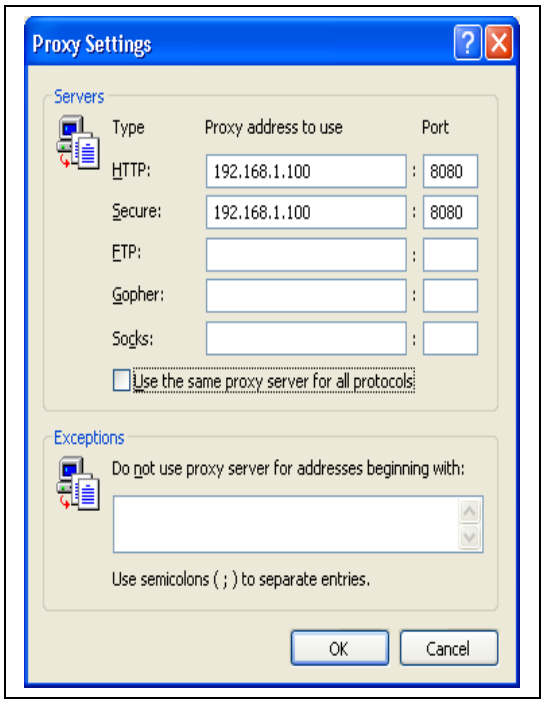
Next, it is necessary to define the address of the proxy server to the web browser. This definition is applied under Tools/Internet Options/Connections.



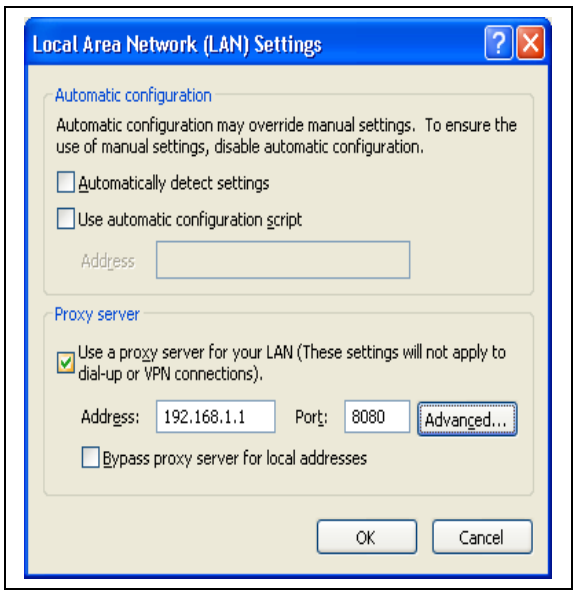
If you are using a dial-up connection for GPRS, highlight the dial-up definition in the "Dial-up and Virtual Private Network Settings" list, and select "Settings". Check "Use Proxy Server", and enter the IP address and port of the Now WAP Proxy.



As the Now WAP Proxy does not support HTTP or Gopher, you may wish to go into the "Advanced" settings, and enable the proxy only for "HTTP" and "Secure", as shown below:



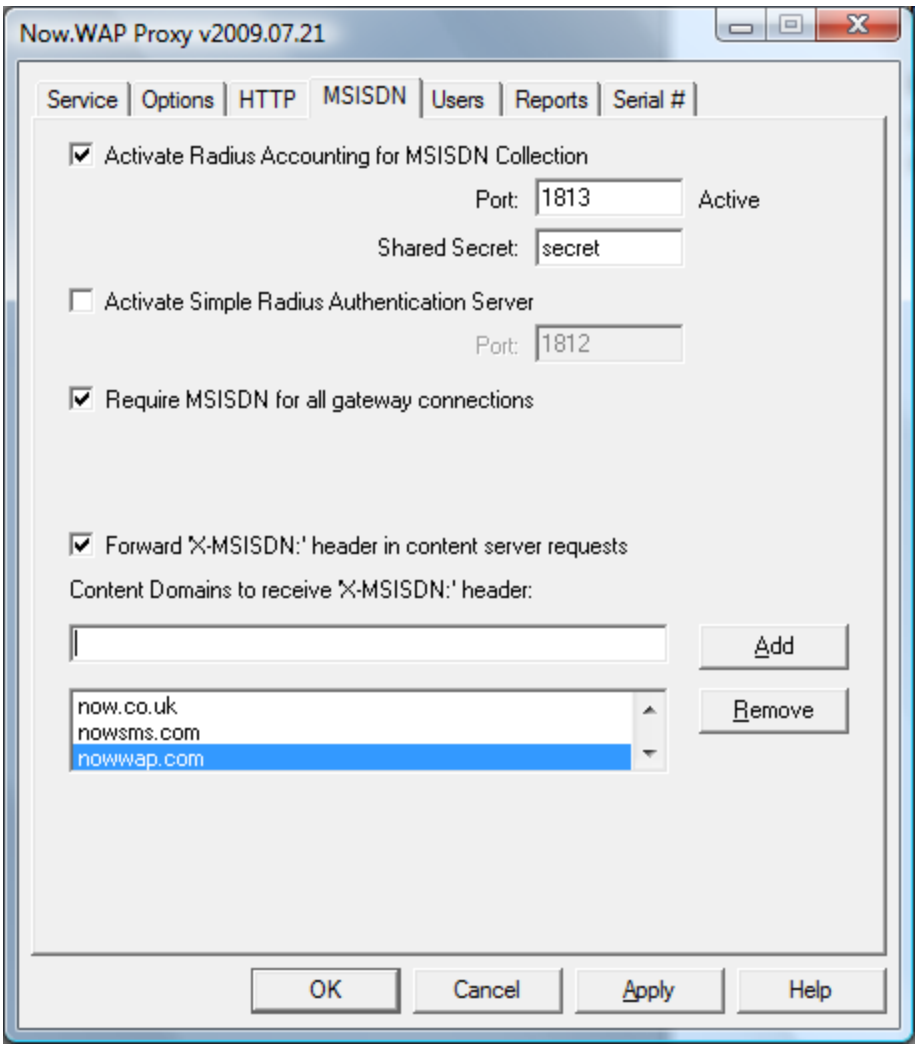
If you are using a PC card that provides a GPRS connection using a network driver instead of dial-up (such as the Sierra Aircard), then the proxy server settings are defined under "LAN Settings" in Tools/Internet Options/Connections. Unfortunately, in this configuration, the proxy server settings apply to all network card connections, which can be inconvenient.



MSISDN Options

The “MSISDN” tab of the configuration dialog allows the gateway to interface with a Radius accounting server that is integrated with the service provider’s data network. This allows the gateway to determine the MSISDN (phone number) of a connected user.

Note that this configuration is typically used only inside of a service provider’s data network, requiring that the WAP gateway be able to receive a Radius accounting feed from the provider’s dial-in server and/or GPRS network.



Check “Activate Radius Accounting for MSISDN Collection” to enable a Radius accounting server that is built into the Now.WAP Proxy, and specify the port number on the local PC to be utilised. The default port number is 1813,

although some older Radius services expect Radius accounting to listen to port 1646. You will also need to configure a "Shared Secret" that is common to the Radius server.

Once the "Radius accounting server" is enabled, the Radius servers on the service provider's network should be configured to forward Radius Accounting packets to the Now.WAP Proxy on the specified port.

Check "Activate Simple Radius Authentication Server" to enable a simple Radius authentication server built into the Now.WAP Proxy. By default, this Radius authentication server accepts all logins, regardless of user name and password, although it is possible to configure this server to authenticate against the user name and password list defined on the "Users" page of the Now.WAP Proxy configuration. This interface is provided primarily for environments where a Radius proxy is unable to separate the Radius accounting and Radius authentication feeds. By default, Radius authentication services listen to port 1812, although some older Radius services expect Radius authentication services to listen to port 1645.

Check "Require MSISDN for all gateway connections" if you wish to only accept WAP connections where the MSISDN (phone number) of the device can be reliably determined. Note that this setting would normally only be used in an environment where the Now.WAP Proxy is tightly integrated with the service provider network.

The gateway can forward the MSISDN of the WAP device to content servers via the "X-MSISDN:" HTTP header. Check "Forward 'X-MSISDN:' Header in content server requests" to enable this capability. For privacy reasons, it is possible to explicitly list the content servers and/or domains that will receive the "X-MSISDN:" header. When a content domain is added to the list, a host name that exactly matches the content domain, as well as any host names within the content domain will receive the "X-MSISDN:" header. For example, if "now.co.uk" is added to the content domain list, the "X-MSISDN:" header would be forwarded to a host named "now.co.uk" as well as for "www.now.co.uk" and "mms.now.co.uk". If you wish to have the "X-MSISDN" header forwarded to all content servers, define a content domain named "*".

For privacy reasons, it may be desirable to use alternative HTTP headers for user identification, without divulging the user's MSISDN to third-party content providers. This capability is discussed in the section titled **HTTP Header Enrichment**.

HTTP Header Enrichment

HTTP Header Enrichment (HHE) capability provides solutions for a content provider to identify a subscriber.

Basic HHE allows the subscriber to be identified by their MSISDN.

Aliased HHE allows the subscriber to be identified without divulging the subscriber's MSISDN.

A standard feature of the NowWAP Proxy is to provide Basic HTTP Header Enrichment to facilitate operator billing for HTTP based services, including Multimedia Messaging Services (MMS).

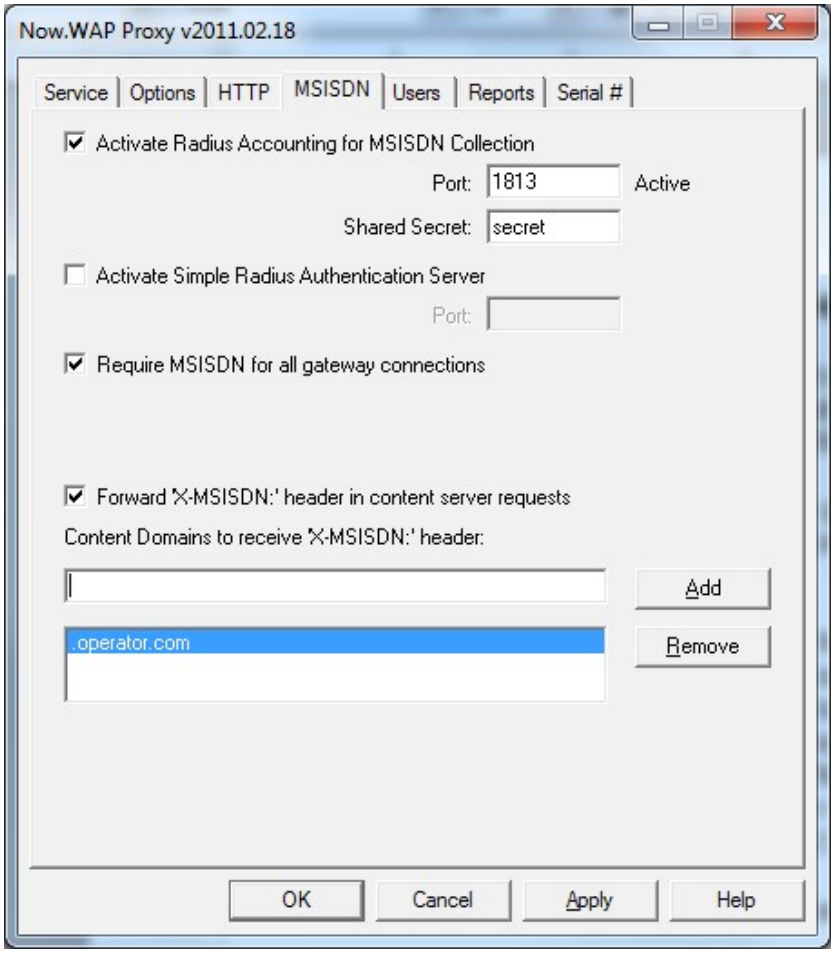
Basic HHE is enabled for all subscriber HTTP transactions that are forwarded to a configurable list of content provider hosts and/or domains (most frequently these are hosts within the operator domain, such as the operator MMSC). Depending on the information available from the RADIUS accounting feed, this basic information can include the subscriber MSISDN, SGSN IP Address, SGSN MCC & MNC (useful for determining if the client is currently roaming), client IP address (useful for identifying which operator APN was accessed), IMSI, and radio access type (4G, 3G or 2.5G) .

Basic HHE can result in the following HTTP headers being inserted:

X-MSISDN: xxxxxxxxxxxxxxxx
X-WAP-3GPP-SGSN-MCC-MNC: xxxxx
X-WAP-3GPP-SGSN-ADDRESS: 1.2.3.4
X-WAP-3GPP-IMSI: xxxxxxxxxxxxxx
X-WAP-3GPP-RAT-TYPE: 1 or 2 (1 = 3G, 2 = EDGE/GPRS)
X-WAP-Client-IP: 7.8.9.0

The list of content provider hosts and/or domains that receive this basic HHE is configurable. Host names can be listed here explicitly, such as mmsc.operator.com, or all hosts within a particular domain can be included by adding the domain name to the list prefaced with a ".", for example .operator.com means that all hosts within the operator.com domain would receive basic HHE (for example, both www.operator.com and mmsc.operator.com).

Hosts that receive Basic HHE are configured on the "MSISDN" page of the Now.WAP configuration dialog.



In many instances, it is useful to provide similar identifying information to content provider partners, but without divulging the subscriber MSISDN. A new feature of the NowWAP Proxy 2011 release is to provide Aliased HTTP Header Enrichment to meet this need.

Content provider hosts and domains that are to receive Aliased HHE are configured with a list that is similar, but separate from, the existing Basic HHE content provider domain/host list that is configured on the “MSISDN” page of the NowWAP configuration program.

NowWAP does not directly generate the Aliased HHE. Instead, it provides an HTTP callback interface to allow the customer to generate customized Aliased HHE that is appropriate for the target operator environment.

A customer-defined Aliased HHE callback interface (running on a separate web server at the customer presmises) is defined to NowWAP by adding the following configuration setting to the [WAPGW] header of WAPGW.INI:
HHECallbackURL=http://server/path

When the HHE callback is configured in NowWAP, each time NowWAP receives a RADIUS notification of a new user connecting, NowWAP will make an HTTP GET request to the HHE callback to request HHE/alias information for the user account.

The HHE callback request will include MSISDN, and other RADIUS information, if available.

Example:

http://server/path?PhoneNumber=xxxx&UserName=xxxxx&
AssignedIP=a.b.c.d&3GPP-SGSN-MCC-MNC=xxxxx&
3GPP-SGSN-ADDRESS=xx&3GPP-IMSI=xxxxxxxxxxxxxxx&
3GPP-RAT-TYPE=x

(Line breaks have been inserted in the URL above for readability only. There are no line breaks in the actual HHE callback URL.)

The “PhoneNumber” (MSISDN) and “AssignedIP” (X-WAP-Client-IP) parameters will always be present. The 3GPP parameters would be present only if they were presented to NowWAP by the RADIUS feed.

The HHE callback response should be a text response containing enriched HTTP headers to be included in all requests that are processed on behalf of this device.

Example:

HTTP/1.1 200 OK
Content-Type: text/plain
X-MSISDN-Alias: xxxxxxxxxxxxxxxxxxxx
X-HHE-Extra-Info: xxxxxxxxxxxxxxxxxxxx

As NowWAP processes subsequent requests, if the request is directed to a content domain that receives Aliased HHE, these headers would be included in the HTTP request that is forwarded to the content provider. (Basic HHE would not be forwarded to these content providers.)

The list of content domains to receive Aliased HHE is defined in the WAPGW.INI file, under the [WAPGW] header, using keyword value pairs of the following format:

IncludeHHEForDomain1=.domain1.name
IncludeHHEForDomain2=host.domain2.name
IncludeHHEForDomain3=host.domain3.name

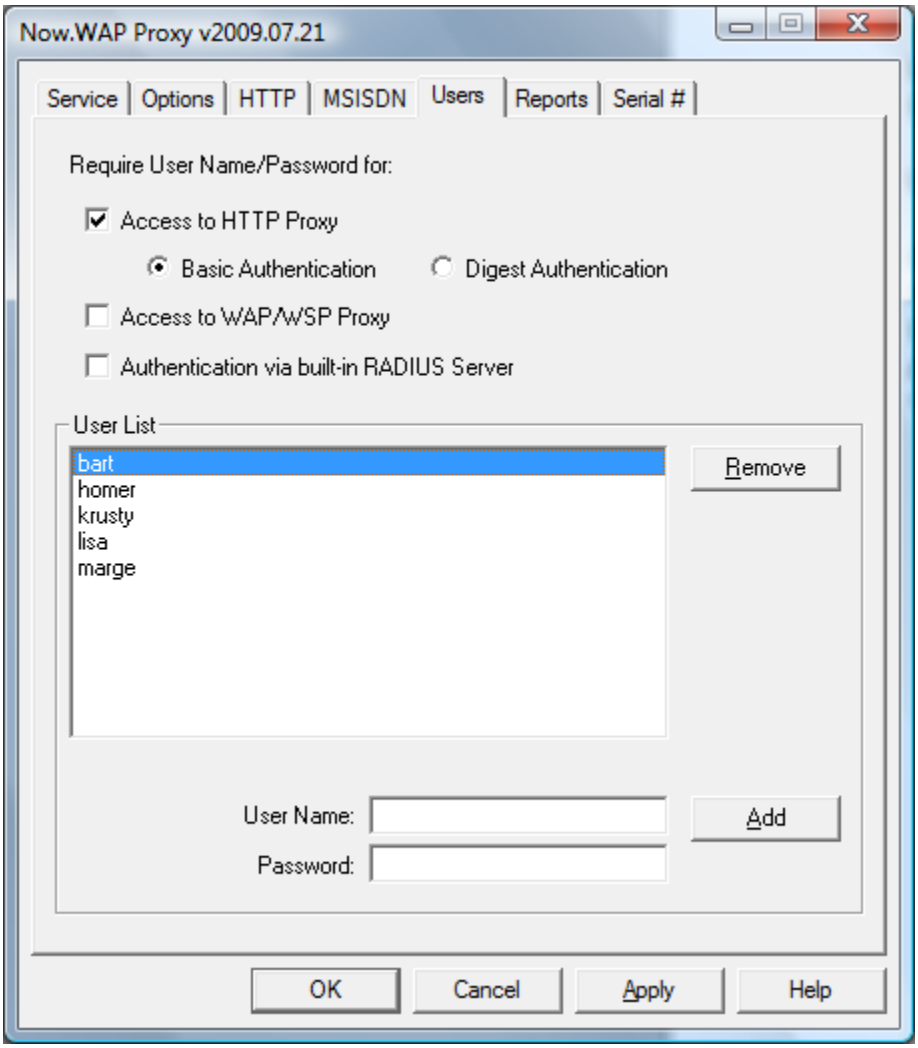
Host names can be listed explicitly, such as www.contentprovider.com, or all hosts within a particular domain can be included by adding the domain name to the list prefaced with a ".", for example .contentprovider.com means that all hosts within the contentprovider.com domain would receive aliased HHE (for example, both www.contentprovider.com and www2.contentprovider.com).

User Accounts

In smaller configurations, it may be desirable to configure user accounts, so that a username and password are required for access to the Now.WAP Proxy.

User accounts are defined on the “Users” page of the configuration dialog.

A single user account list is supported. This user account list can be used to restrict access to the HTTP Proxy functions, the WAP/WSP Proxy functions, or it can be used for user account/password validation for the built-in RADIUS Authentication Server (the RADIUS Authentication Server is defined on the “MSISDN” page of the configuration).



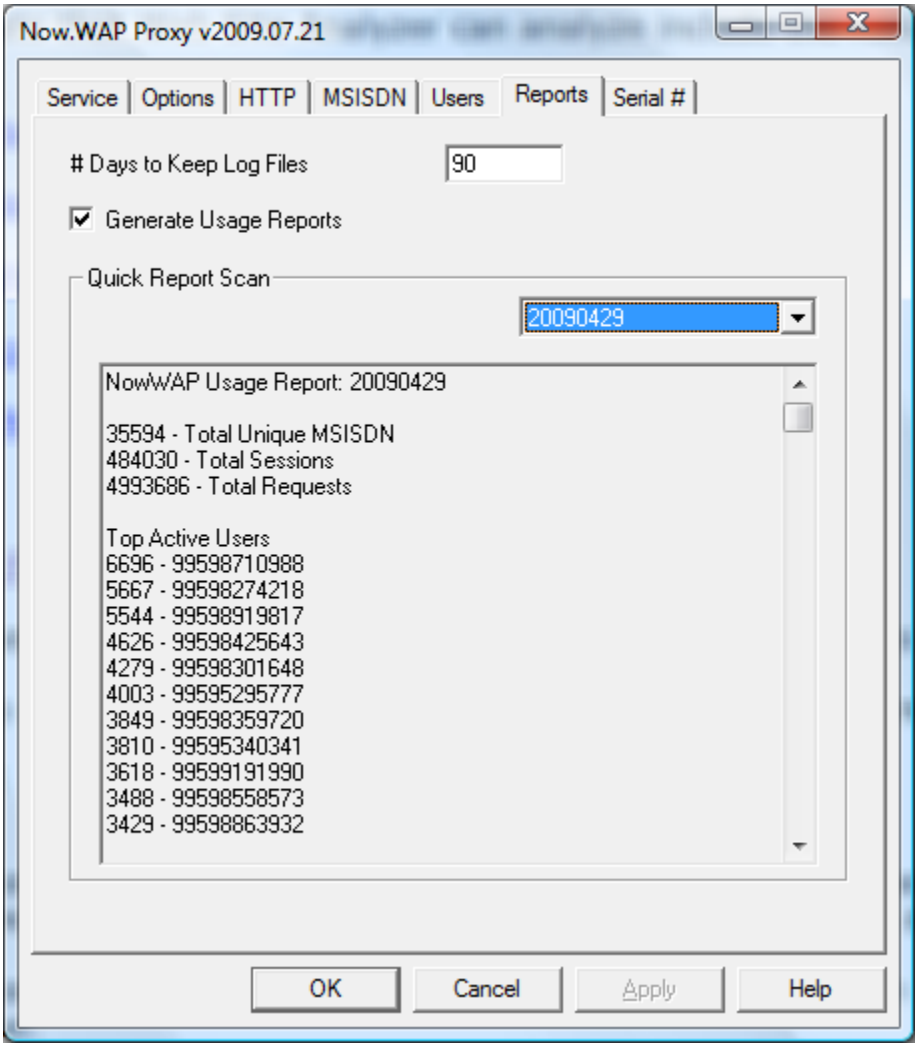
The user account list is stored as a text file in the Now.WAP Proxy gateway directory under a file name of USERS.TXT. This file can be edited outside of the Now.WAP Proxy. Each line of the text file should consist of a user name, followed by a comma, followed by the password for the account.

Reports and Log Files

The log files created by NowWAP are of a text format that follows the common log format for web servers.

These log files are stored on the NowWAP server, with one log file created for each day, using a file naming convention of WAPGW-yyyymmdd.LOG, where yyyymmdd is the 4-digit year, 2-digit month and 2-digit day.

NowWAP 2011 has optional functionality which can convert these log files into a database format for further analysis. This functionality is enabled by checking "Generate Usage Reports" on the "Reports" page of the configuration dialog.



When usage reports are enabled, NowWAP will automatically generate daily and monthly usage reports.

These reports are located in the REPORTS subdirectory of the NowSMS installation.

REPORTS\LOGDB contains SQLite format databases with one database per month.

REPORTS\TEXT contains text format summary reports of NowWAP usage. Daily reports have file names of YYYYMMDD.TXT and monthly reports have file names of YYYYMM.TXT. Every night at midnight, a new daily report and updated monthly report for the current month will be generated.

The format of the text report will be similar to the following:

```
NowWAP Usage Report: YYYYMMDD

#### - Max Active Users
#### - Max Active Requests
#### - Total Unique MSISDN
#### - Total Sessions
#### - Total Requests

Top Active Users
#### - Phone Number 1
#### - Phone Number 2
etc...

Top Content Domains
#### - Domain 1
#### - Domain 2
etc...

Top Content Servers
#### - Server 1
#### - Server 2
etc...
```

REPORTS\XML contains XML formatted summary reports of NowWAP usage. Daily reports have file names of YYYYMMDD.XML and monthly reports have file names of YYYYMM.XML. Every night at midnight, a new daily report and updated monthly report for the current month will be generated.

The format of the XML report will be similar to the following. Note that some XML elements may not be present, depending on NowWAP configuration issues. Also note that additional XML elements may be added in future releases.

```
<NowWAPUsageReport>
<ReportDate>YYYYMMDD</ReportDate>
<MaxActiveUsers>####</MaxActiveUsers>
<MaxActiveRequests>####</MaxActiveRequests>
<TotalUniqueMsisdn>####</TotalUniqueMsidn>
<TotalSessions>####</TotalSessions>
<TotalRequests>####</TotalRequests>
<TopActiveMsisdn>
<Name>Phone Number 1</Name><Requests>####</Requests>
<Name>Phone Number 2</Name><Requests>####</Requests>
</TopActiveMsisdn>
<TopContentDomains>
<Name>Domain 1</Name><Requests>####</Requests>
<Name>Domain 2</Name><Requests>####</Requests>
</TopContentDomains>
<TopContentServers>
<Name>Server 1</Name><Requests>####</Requests>
<Name>Server 2</Name><Requests>####</Requests>
</TopContentServers>
</NowWAPUsageReport>
```

ReportDate – YYYYMMDD for a daily report or YYYYMM for a monthly report.

MaxActiveUsers – The maximum number of active (concurrent) users recorded during the report period. (Note: This information cannot be obtained from log files created by earlier versions of NowWAP.)

MaxActiveRequests – The maximum number of simultaneous requests recorded during the report period. (Note: This information cannot be obtained from log files created by earlier versions of NowWAP.)

TotalUniqueMsisdn – The number of unique MSISDN (phone numbers) that made requests of the proxy. (Note: Requires MSISDN/RADIUS integration.)

TotalSessions – The number of user sessions during the report period.

TotalRequests – The number of user requests serviced during the report period.

TopActiveMsisdn – A list of the most active mobile terminals and the number of requests generated by that mobile terminal during the report period. (Note: Requires MSISDN/RADIUS integration.)

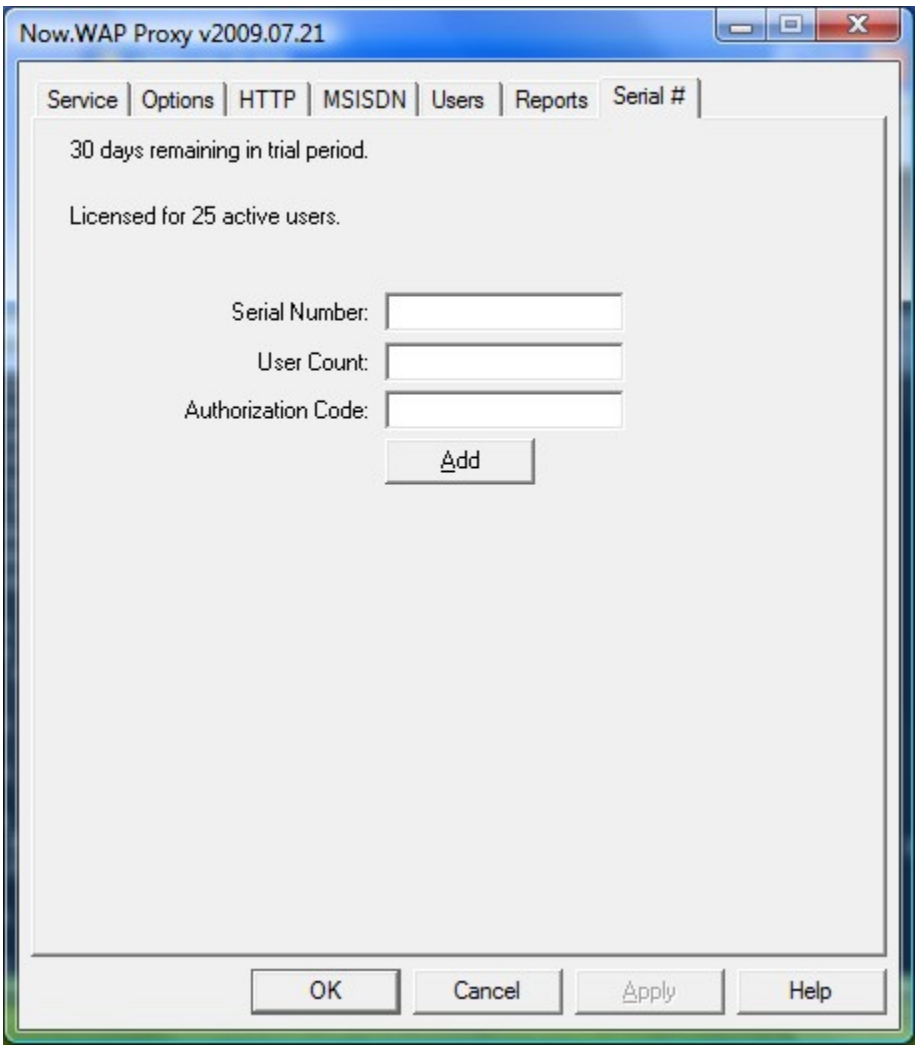
TopContentDomains – A list of the content domains which recorded the most requests (hits) during the report period.

TopContentServers – A list of the content servers which recorded the most requests (hits) during the report period.

Serialisation and Serial Numbers

The Now.WAP Proxy is licensed by active (or concurrent) users.

When the Now.WAP Proxy is purchased, you will be provided with a serial number, user count and authorization code that must be entered into the "Serial #" tab of the configuration dialog. Enter this information and press "Add" to serialise the Now.WAP product.



Fault Tolerant Configurations

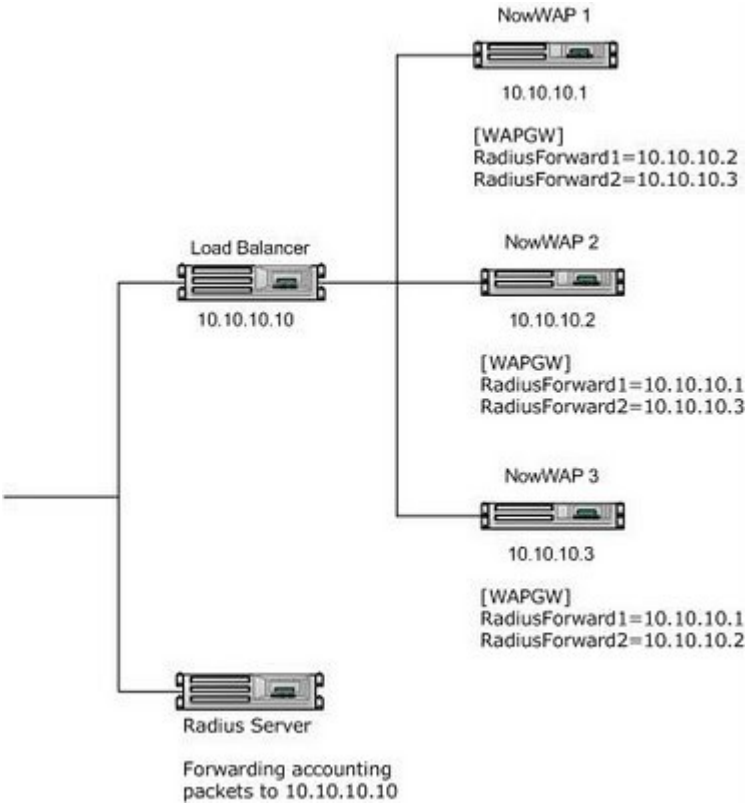
For many configurations, it is desirable to install Now.WAP on multiple servers in order to achieve fault tolerance and/or improved throughput and performance.

Note that each Now.WAP server requires a unique serial number. Use of the same serial number on multiple servers will prevent fault tolerant configuration options from functioning correctly.

The primary configuration concern when running Now.WAP in a clustered configuration is when Now.WAP is configured to use RADIUS accounting to supply MSISDN information to one or more content servers, such as an MMSC.

This section describes how to configure multiple Now.WAP gateways to share this MSISDN information.

To run Now.WAP in a load balanced configuration, the Now.WAP program files are installed locally on each server.



A load balancer is used to route network traffic to any of the Now.WAP servers.

In this type of environment, there is one shared IP address for which the load balancer accepts requests and routes them to any of the available Now.WAP servers.

In addition to the single shared IP address, each of the Now.WAP servers has a unique local IP address that is not shared.

The access server is configured to send RADIUS accounting packets to the shared IP address. Based upon server availability, the load balancer will route the RADIUS accounting packet to one of the Now.WAP servers. The RADIUS accounting packet could be routed to any of the Now.WAP servers.

All of the Now.WAP servers are configured to listen for RADIUS accounting packets, with "Activate Radius Accounting for MSISDN Collection" checked on the "MSISDN" page of the Now.WAP configuration. The same "Port" number and "Shared Secret" should be configured on all Now.WAP servers, using the values expected by the access server.

Manual edits must then be applied to the WAPGW.INI file of each Now.WAP server.

Under the [WAPGW] section header of this file, configuration parameters must be added to specify that any RADIUS accounting packets received by this server should also be forwarded to the other server(s). The syntax of the configuration parameter is RadiusForward#=ip.address:port, where "#" is an incrementing number for each definition beginning with 1, "ip.address" is the non-shared IP address of another Now.WAP server, and "port" is the Radius Accounting port number (if not specified, the default is 1813).

As an example of this configuration, assume a configuration where 3 Now.WAP servers are load balanced with a shared IP address of 10.10.10.10. The non-shared (local) IP addresses for the 3 servers are 10.10.10.1, 10.10.10.2, and 10.10.10.3.

The access server is configured to send RADIUS accounting packets to 10.10.10.10 (the shared IP address).

The Now.WAP server on 10.10.10.1 has the following configuration settings under the [WAPGW] header of WAPGW.INI:

RadiusForward1=10.10.10.2
RadiusForward2=10.10.10.3

The Now.WAP server on 10.10.10.2 has the following configuration settings under the [WAPGW] header of WAPGW.INI:

RadiusForward1=10.10.10.1
RadiusForward2=10.10.10.3

The Now.WAP server on 10.10.10.3 has the following configuration settings under the [WAPGW] header of WAPGW.INI:

RadiusForward1=10.10.10.1
RadiusForward2=10.10.10.2

Troubleshooting Notes

1.) For troubleshooting purposes, it may be easiest to first configure the access server to send the RADIUS Accounting packets to the non-shared IP address of just one of the Now.WAP servers. Once that is working properly, change the access server to send the RADIUS Accounting packets to the shared IP address of the load balanced cluster.

2.) Now.WAP logs all received RADIUS transactions in log files named RADIUS-yyyymmdd.LOG (yyyymmdd is the current date). Refer to these log files for details regarding RADIUS Accounting packets received by Now.WAP.

3.) For further troubleshooting, it may be helpful to use a network traffic analyzer, such as Wireshark (formerly known as Ethereal).

Advanced Configuration Options

Several additional configuration options may be applied by directly editing the WAPGW.INI file, located in the Now.WAP program directory.

The configuration settings described in this section may be entered into the WAPGW.INI file under the [WAPGW] section header.

SessionTimeout=####

This setting specifies a timeout value, in minutes, after which a gateway session will be automatically timed out. The default value is 10 minutes. Use caution when setting this value to lower values, as while most clients will automatically reconnect after a session timeout, some clients will report an error message.

DaysToKeepLogFile=####

This setting specifies the number of days to keep log files. The default value is 90 days. These are the WAPGW-YYYYMMDD.LOG files that the gateway maintains to track access. Note that the log files follow the standard format for a web server log file.

ResponseSizeLimits=Yes/No

When this setting is set to No, the gateway will not enforce any limits on the response size of data that is sent back to a mobile device. By default this setting is set to Yes, and the gateway will not sent any responses to a mobile device which exceed the response size that the device indicates that it will accept. The default setting is No.

AcceptAllMimeTypes=Yes/No

When this setting is set to Yes, the gateway will not reject responses from content servers that are in a MIME type that the client has not indicated that it will accept. By default this setting is set to No, and the gateway will return an error if a content server returns a MIME type that the client has not indicated that it will accept.

DefaultCharSet=####

This setting specifies a default Windows character set to be assumed for WAP content. By default, the gateway assumes that the UTF-8 character set is used, unless a "charset" header exists within a WML page. The mapping of MIME character sets to Windows character sets is automatically read from the Windows registry (HKEY_CLASSES_ROOT\MIME\Database\Charset). Additional character set mappings can be defined in a CHARSET.INI file, an example of which is shown below. Note that if the DefaultCharSet setting is used to specify a default character set, you must specify the Windows code page number, and not the MIME character set name.

```
[Charset]
us-ascii=1252
iso-8859-1=1252
iso-8859-2=1250
iso-8859-4=1257
iso-8859-5=1251
iso-8859-6=1256
iso-8859-7=1253
iso-8859-8=1255
iso-8859-9=1254
big5=950
big-5=950
gbk=936
gb2312=936
gb2312-80=936
shift-jis=932
shift_jis=932
iso-2022-kr=949
korean=949
ks_c_5601=949
KSC_5601=949
KSC5601=949
KSC-5601=949
```

WTPSarSegmentSize=####

This setting specifies the maximum segment size in bytes to be used in segmentation and reassembly (SAR) responses generated by the gateway. The default setting is 1400 bytes.

WTPSarWindowSize=####

This setting specifies the window size (number of packets sent without acknowledgement) to be used in segmentation and reassembly (SAR) responses generated by the gateway. The default setting is 3.

AllowHttpsWithoutWtls=Yes/No

Available in the WTLS version only, when this setting is set to Yes, the gateway will make HTTPS (SSL/TLS) connections to content servers, even when the client device did not use WTLS to connect to the gateway. The default setting for this parameter is No, meaning that the gateway will only make HTTPS connections on behalf of clients that have used WTLS to connect to the gateway.

LogTruncateUrlQuery=Yes/No

By default, URL GET parameters are not included in the URL requests written to the log files. To include URL GET parameters in the log file, this parameter should be set to Yes.

TunnelSmtpPort=Yes/No

The SSL/TLS tunnel functionality of the HTTP Proxy allows clients to use any protocol, not just HTTP SSL/TLS, to connect to external content servers. To prevent abuse of this functionality, by default the Now.WAP Proxy only supports tunnel connections to the standard HTTP SSL/TLS port of 443. A menu based configuration setting allows tunnel connections to be enabled for other non-standard ports. However, by default, the Now.WAP Proxy will still not allow connections to port 25 (the standard SMTP port) via the HTTP tunnel facility unless this configuration parameter is present in the INI file with a setting value of Yes.

SARTimeout=###

When receiving a segmented request from a WSP client, this setting specifies the maximum number of minutes that the server will wait for a client to send the next segment before considering the request aborted. The default value is 5.

WTPSarAckTimeout=###

When sending a segmented response to a client, this is the maximum number of seconds that the server will wait for an acknowledgment before aborting the response. The default value is 90 seconds.

WTPSarAckTimeoutResend=###

When sending a segmented response to a client, this is the maximum number of seconds that the server will wait for an acknowledgment for any segment that requires acknowledgment before resending the current segment. The default value is 8 seconds.

WTPAckTimeout=###

When sending a simple (non-segmented) response to a client, this is the maxmium number of seconds that the server will wait for an acknowledgment before aborting the response. The default value is 90 seconds.

WTPAckTimeoutResend=###

When sending a simple (non-segmented) response to a client, this is the maximum number of seconds that the server will wait for an acknowledgment of the response before resending the response. The default value is 5 seconds.

DisableConnectionLess=Yes/No

This setting can be set to Yes to disable support for legacy WAP/WSP connectionless requests on UDP port 9200. The connectionless protocol is limited to a single packet and does not work well for requests larger than 1500 bytes. The default value is No (connectionless support enabled).

MethodMOR=###

This setting sets the maximum value that the server will return for the "Maximum Outstanding Method Requests" field in a WAP/WSP connection request. The default value is 50. This value specifies the maximum number of concurrent transactions allowed between the client and the server. Note that Now.WAP does not enforce this MOR connection limit, and sets this value merely as advice for the client.

IncludeMSISDNConnectOnly=Yes/No

Setting this value to "Yes" indicates that Now.WAP should only allow proxy requests to connect to domains and hosts that are listed in the "Content

Domains to receive X-MSISDN header" list on the "MSISDN" page of the Now.WAP configuration dialog. Any attempts to connect to a domain or host name that is not in this list will result in the proxy returning an "Access Denied" error. This setting is active even if RADIUS support has not been enabled for MSISDN collection. This setting is intended primarily for configurations where the WAP proxy is acting only to support a single service, such as an MMSC. The default value for this setting is "No".

IncludeMSISDNConnectOnlyGWIP=ip.addr1,ip.addr2,...

This setting works similar to the IncludeMSISDNConnectOnly=Yes setting, however it applies this setting only for selected server IP addresses, if the Now.WAP server is running as a multi-homed server will multiple IP addresses. For example, if the Now.WAP server is running on multiple network interfaces with IP addresses of 10.0.0.100 and 192.168.1.100, you may want Now.WAP to act as an open proxy for connections to the 10.0.0.100 server, while restricting connections to the 192.168.1.100 server. In this case, define IncludeMSISDNConnectOnlyGWIP=192.168.1.100, and any connections that the Now.WAP server receives on the 192.168.1.100 interface will be restricted to the domains and/or host names in the "Content Domains to receive X-MSISDN header" list on the "MSISDN" page of the Now.WAP configuration dialog.

IncludeMSISDNConnectOnlySourceIP=ip.addr1,ip.addr2,...

This setting works similar to the IncludeMSISDNConnectOnly=Yes setting, however it applies this setting only for selected client IP addresses. For example, if the Now.WAP server is supporting clients that are assigned to multiple different IP address ranges, you may want Now.WAP to act as an open proxy for clients from one IP address range, while limiting access for other clients to selected hosts. For example, assume that you have two APNs, one for browser connections, and another only for MMS traffic. The browser APN assigns client IP addresses in the 10.0.0.0 network, and the MMS APN assigns client IP addresses in the 192.168.0.0 network. In this case, define IncludeMSISDNConnectOnlySourceIP=192.168.*.*, and any connections that the Now.WAP server receives from clients on the 192.168.0.0 network will be restricted to the domains and/or host names in the "Content Domains to receive X-MSISDN header" list on the "MSISDN" page of the Now.WAP configuration dialog. Note that this setting does not support address masks, but the "*" wildcard character can be used as a placeholder in any part of the IP address. This setting allows for a comma delimited list of multiple client source IP addresses.

HHECallbackURL=http://server/path

This setting enables an HTTP callback for supporting ***aliased*** HTTP Header Enrichment. For further information, refer to the section of this document titled **HTTP Header Enrichment**.

IncludeHHEForDomain#=domain.name

When ***aliased*** HTTP Header Enrichment is enabled with an HHECallbackURL, this setting specifies a host or domain name that should receive aliased HTTP Header Enrichment. # is a numeric index that starts with 1, and is increased for each additional defined host or domain name. For example:

IncludeHHEForDomain1=www.contentprovider1.com
IncludeHHEForDomain2=.contentprovider2.com
IncludeHHEForDomain3=host.contentprovider3.com

Host names can be listed explicitly, such as www.contentprovider1.com, or all hosts within a particular domain can be included by adding the domain name to the list prefaced with a ".", for example .contentprovider2.com means that all hosts within the contentprovider2.com domain would receive aliased HHE (for example, both www.contentprovider2.com and m.contentprovider2.com).

URLREWRITE.TXT

The URLREWRITE.TXT file is a special file that can be created in the Now.WAP program directory.

The URLREWRITE.TXT file is a standard text file that can be created and edited with a basic text editor such as Windows Notepad.

Each line of this file can contain the start of a URL, and how it should be translated/redirected.

For example, if you have clients that are pre-configured to start at a homepage of http://homepage, you can define a redirection in this file to redirect the request to a different server, such as:

http://homepage=http://domain.name/path/page