1. SureLink™ Settings

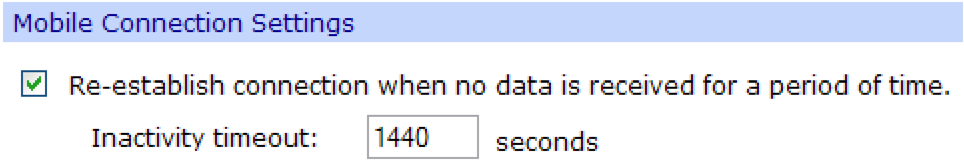
The following options configure the SureLink settings for your Digi device. These settings ensure that your device is in a state where it can connect to the mobile network, and they can be used to monitor the integrity of the established mobile connection.

There are two groups of SureLink settings: Hardware Reset Thresholds and Link Integrity Monitoring. The Hardware Reset Thresholds settings can be configured to clear any error states that were resident in the device's cellular module, so the device can once again connect to the network, if the connection is lost. The Link Integrity Monitoring settings can be configured to perform a selected test to examine the functional integrity of the network connection, and take action to recover the connection in the event that it is lost.

2. The Inactivity Timeout

Re-establish connection when no data is received for a period of time
The Inactivity timeout specifies the time, in seconds, after which if no data has received over the link, the mobile connection will be disconnected and re-established.

Configuration -> Mobile -> Mobile Connection Settings



Mobile Connection Settings

☑ Re-establish connection when no data is received for a period of time.

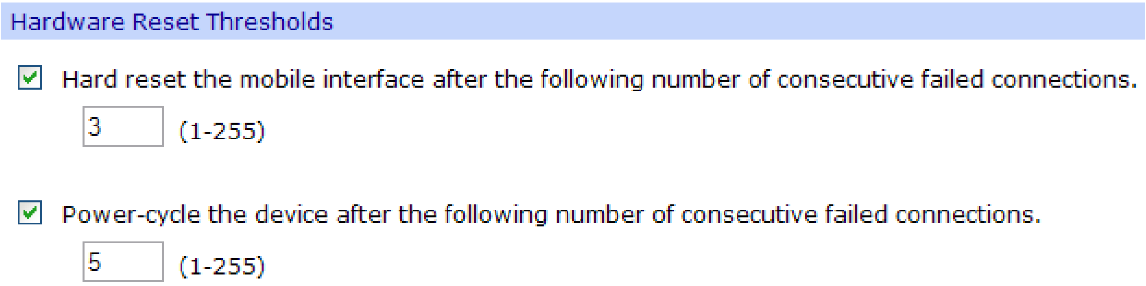
Inactivity timeout: 1440 seconds

3. Hardware Reset Thresholds

Hard reset the mobile interface after the following number of consecutive failed connections.
Enables or disables a hard reset of the cellular modem module after the specified number for failed connection attempts. This value can be a number between 1 and 255. The default is 3.

Power-cycle the device after the following number of consecutive failed connections.
Enables or disables a power-cycle of your Digi device server after the specified number of consecutive failed connection attempts. This value can be a number between 1 and 255. The default is OFF.

Configuration -> Mobile -> SureLink Settings -> Hardware Reset Thresholds



Hardware Reset Thresholds

☑ Hard reset the mobile interface after the following number of consecutive failed connections.

3 (1-255)

☑ Power-cycle the device after the following number of consecutive failed connections.

5 (1-255)

4. Hardware Reset Thresholds

Enable Link Integrity Monitoring using the test method selected below. Enables or disables the link integrity monitoring tests. If this setting is enabled, the other Link Integrity Monitoring settings may be configured and are used to verify the functional integrity of the mobile connection. The default is OFF.

Three different tests are available for selection:

- Ping Test
- TCP Connection Test
- DNS Lookup Test

Each of these tests can be used to demonstrate that two-way communication is working over the mobile connection. This variety of tests is provided because different mobile networks or firewalls may allow or block Internet packets for various services. The appropriate test may be selected according to mobile network constraints and user preference. The link integrity tests are performed only while the mobile connection is established. If the mobile connection is disconnected, the link integrity tests are suspended until the connection is established again. For the link integrity tests to provide meaningful results, the remote or target hosts must be accessible over the mobile connection and not through the LAN interface of the device (if it has one). That is, the settings should be configured to guarantee that the mobile connection is actually being tested.
The link integrity test settings may be modified at any time. The changes are used at the start of the next test interval.

Ping Test
Enables or disables the use of "ping" (ICMP) as a test to verify the integrity of the mobile connection. The test is successful if a valid ping reply is received in response to the ping request sent. The ping test actually sends up to three ping requests, at five second intervals, to test the link. When a valid reply is received, the test completes successfully and immediately. If a reply is received for the first request sent, there is no need to send the other two requests. Two destination hosts may be configured for this test. If the first host fails to reply to all three ping requests, the same test is attempted to the second host. If neither host replies to any of the ping requests sent, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.

Primary Address: First host to test
Secondary Address: Second host to test (if the first host fails)

TCP Connection Test

Enables or disables the creation of a new TCP connection as a test to verify the integrity of the mobile connection. The test is successful if a TCP connection is established to a specified remote host and port number. If the remote host actively refuses the connection request, the test is also considered to be successful, since that demonstrates successful two-way communication over the mobile connection. The TCP connection test waits up to 30 seconds for the connection to be established or refused. When the TCP connection is established, the test completes successfully, and the TCP connection is closed immediately. Two destination hosts may be configured for this test. If the first host fails to establish (or refuse) the TCP connection, the same test is attempted to the second host. If neither host successfully establishes (or refuses) the TCP connection, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.

TCP Port: The TCP port number to connect to on the remote host (default 80)
Primary Address: First host to test
Secondary Address: Second host to test (if the first host fails)

DNS Lookup Test

Enables or disables the use of a Domain Name Server (DNS) lookup as a test to verify the integrity of the mobile connection. The test is successful if a valid reply is received from a DNS server. Typically, this means the hostname is successfully "resolved" to an IP address by a DNS server. But even a reply such as "not found" or "name does not exist" is acceptable as a successful test result, since that demonstrates successful two-way communication over the mobile connection. When a valid reply is received, the test completes successfully and immediately. The DNS servers used in this test for the hostname lookup, are the primary and secondary DNS servers obtained from the mobile network when the mobile PPP connection is first established. These addresses may be viewed in your web browser on the Administration | System Information | Mobile page.

Note that this DNS test is independent of the normal DNS client configuration and lookup cache, which is used for other hostname lookups. This test has been specifically designed to require communication over the mobile connection for each lookup, and to avoid being "short-circuited" by previously cached information. Also, this test does not interfere in any way with the normal DNS client configuration of this device. Two hostnames may be configured for this test. If the first hostname fails to get a reply, the same test is attempted for the second hostname. If no reply is received for either hostname, the test fails. The primary and secondary DNS names should be fully qualified domain names. Note that the reverse lookup of an IP address is possible, but that is usually unlikely to succeed in returning a name. Still, such a reverse lookup can be used to demonstrate the integrity of the mobile connection.

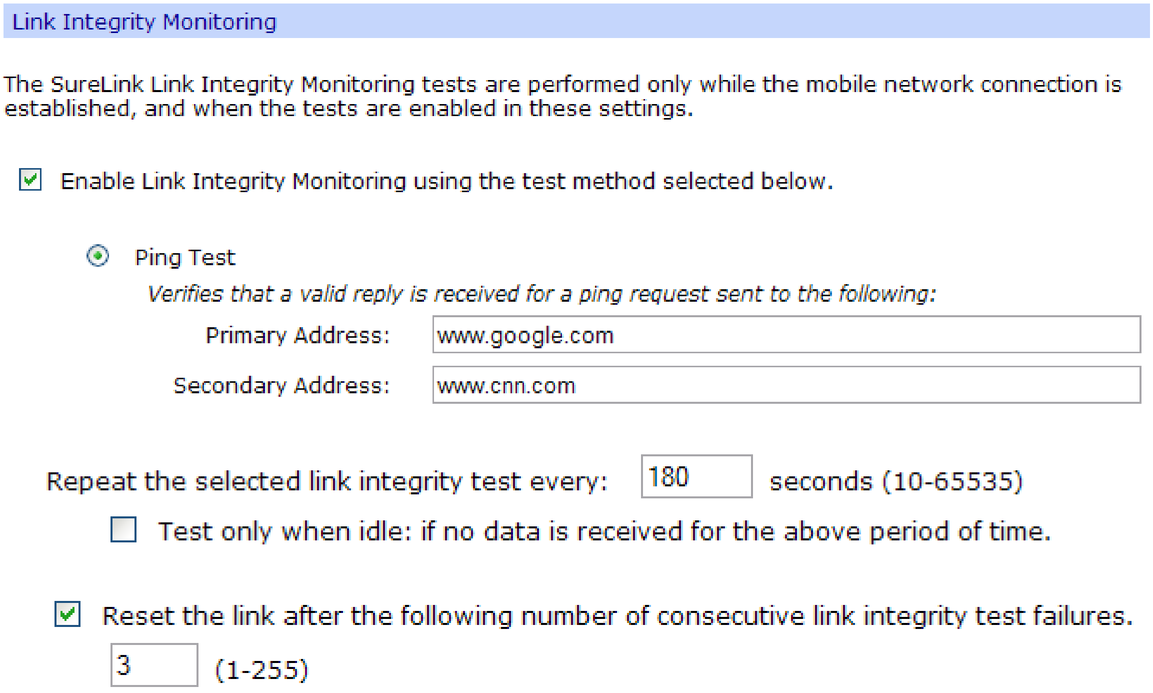
Primary DNS Name: First hostname to look up
Secondary DNS Name: Second hostname to look up (if the first hostname fails)

Repeat the selected link integrity test every *N* seconds
Specifies the interval, in seconds, at which the selected test is initiated (repeated). A new test will be started every *N* seconds while the mobile connection is established. This value must be between 10 and 65535. The default is 240. If the configured interval is less time than it takes a test to complete, the next test will not be initiated until the previous (current) test has completed.

Reset the link after the following number of consecutive link integrity test failures
Specifies that after the configured number of consecutive link integrity test failures, the mobile connection should be disconnected and reestablished. This value must be between 1 and 255. The default is 3. When the mobile connection is reestablished, the "consecutive failures" counter is reset to zero.

Note: if the mobile connection is disconnected for any reason (including not as a result of a link integrity test failure), the consecutive failures count is reset to zero when the mobile connection is reestablished.

Configuration -> Mobile -> SureLink Settings -> Link Integrity Monitoring



Link Integrity Monitoring

The SureLink Link Integrity Monitoring tests are performed only while the mobile network connection is established, and when the tests are enabled in these settings.

☑ Enable Link Integrity Monitoring using the test method selected below.

● Ping Test

Verifies that a valid reply is received for a ping request sent to the following:

Primary Address: www.google.com

Secondary Address: www.cnn.com

Repeat the selected link integrity test every: 180 seconds (10-65535)

□ Test only when idle: if no data is received for the above period of time.

☑ Reset the link after the following number of consecutive link integrity test failures.

3 (1-255)

5. Remote Management

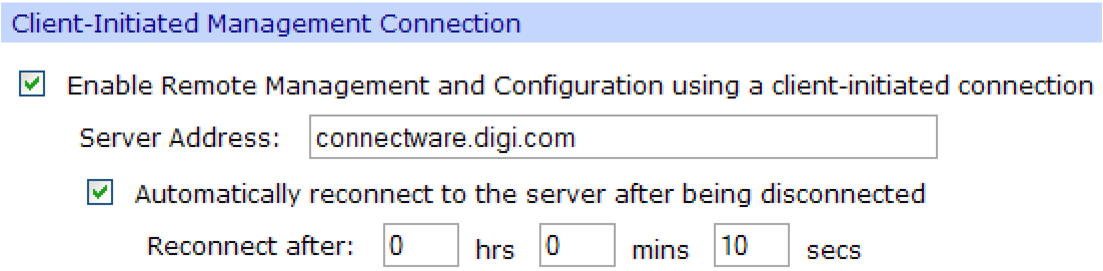
Client-Initiated Management Connection:

Enable Remote Management ... using a client-initiated connection
When enabled, this client device will initiate the connection to the Connectware Manager server. This is the typical connection method.

Server Hostname
The IP address or hostname of the Connectware Manager server.

Automatically reconnect to the server after being disconnected
If enabled, the Digi device server will wait the specified amount of time after a connection to the Connectware Manager server is ended, and then it will reconnect to the Connectware Manager server.

Configuration -> Remote Management -> Connection Settings



Client-Initiated Management Connection

☑ Enable Remote Management and Configuration using a client-initiated connection

Server Address: connectware.digi.com

☑ Automatically reconnect to the server after being disconnected

Reconnect after: 0 hrs 0 mins 10 secs

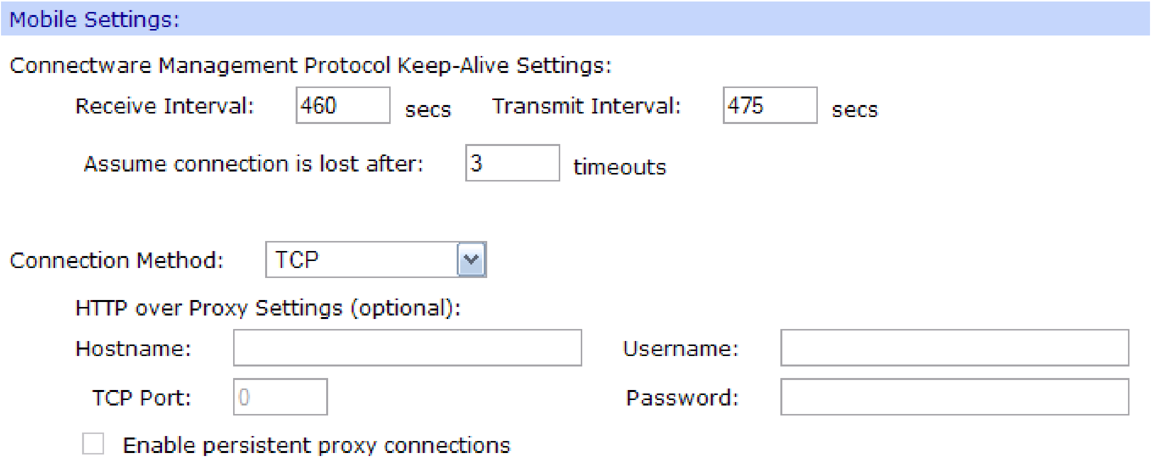
Receive/Transmit Interval

Wait Count
Specifies the keep-alive interval to specify for packets received and packets transmitted. These settings are used in conjunction with the *Wait Count* to signal when the connection has been lost.

Connection Method
Specifies the method by which the associated interface connects to the remote server. The default *TCP* is typically good enough for most connections, and it is the most efficient method of connecting to the remote server in terms of speed and transmitted data bytes. The value *Automatic* is less efficient, but it is useful in situations where a firewall or proxy may prevent direct connection via *TCP*. *Automatic* will try each combination until a connection is made. Note that *None* has the same effect as selecting *TCP*.

HTTP over Proxy Options
Specifies the proxy settings required to communicate over a proxy network using HTTP. These settings only apply when *Automatic* or *HTTP over Proxy* is selected.

Configuration -> Remote Management -> Advanced Settings -> Mobile Settings



Mobile Settings:

Connectware Management Protocol Keep-Alive Settings:

Receive Interval: 460 secs Transmit Interval: 475 secs

Assume connection is lost after: 3 timeouts

Connection Method: TCP

HTTP over Proxy Settings (optional):

Hostname: Username:

TCP Port: 0 Password:

□ Enable persistent proxy connections