



How to enable Portal Page Parameter Signing with version 7.0

Usage: This feature will be beneficial for installations where subscribers are authenticated through a Portal Page or External Web Server (EWS).

NOTE: This document requires knowledge of configuring the Portal Page or EWS feature. Information on these features is available in the User Guide or on the Nomadix Technical Support website under the How to Section – <http://www.nomadix.com/support/howto>.

Function:

The NSE will digitally sign the URL redirection parameters in the query string to prevent subscribers from altering these parameters (maliciously or accidentally) and from gaining unauthorized free access in for-pay rooms. When "Parameter Signing" is activated, the NSE will digitally sign the set of URL redirection parameters prior to redirecting the subscriber in step 2).

The NSE appends five additional redirection parameters to the URL redirection string. These are:

- SIGN=... the digital signature of the URL redirection parameters
- SIGNED=... the URL redirection parameters covered by the signature
- TS=... the timestamp of the URL redirection string, in seconds since Jan 1, 1970.
- NONCE=... a random string that enhances the strength of the signature
- METHOD=... the method used to calculate the signature

The SIGN=... value is calculated using a secret value shared only between the NSE and the Portal Page, so the subscriber will not be able to alter the redirection parameters.

The Portal Page server can then recalculate the digital signature -- entering the timestamp, the set of URL redirection parameters indicated by SIGNED=, the same method used in METHOD=..., the nonce and the shared secret.

The recalculated signature will have to actually match the value in SIGN=... If so, the transaction is valid and the authentication can proceed, otherwise the subscriber has altered the redirection parameters and access has to be denied (or the subscriber has to be challenged for new credentials).



Configuration:

- 1) Navigate to Configuration -> AAA and enable the following services:
AAA Services
Origin Server (OS) parameter encoding for Portal Page
Portal Page and Parameter Passing
- 2) Choose HMAC-MD5 or HASH CRC32 and match the method on the Portal Page Server
- 3) Enable Parameter Signing and choose which values are to be signed by the NSE.
The signature is stronger with each parameter however each requires more computation by the NSE and the web server.
- 4) Enter the Shared Secret phrase
- 5) Select Submit. Note the Shared Secret is not displayed when the changes have been saved.

Internal Web Server

SSL Support Enable
Encrypt only Sensitive Data Enable

Note: To enable, make sure your license includes SSL support and you have all the certificate files on the flash.

Certificate DNS Name

Portal Page Enable

Portal Page URL

Parameter Passing Enable

Parameter Signing	
Method	<input type="radio"/> None <input checked="" type="radio"/> HASH-CRC32 <input type="radio"/> HMAC-MD5
Parameters	<input type="checkbox"/> UI <input checked="" type="checkbox"/> MA <input checked="" type="checkbox"/> RN <input type="checkbox"/> PORT <input checked="" type="checkbox"/> SIP
Shared Secret	<input type="text"/> (write-only)

Manual Passthrough Address Enable

Portal XML POST URL

Portal XML Post Port

Supports GIS Clients Yes

Block IWS Login Page Yes

Sample redirection:

Location: [http://192.168.0.100/default.asp?UI=0197f8&NI=0050e80197f8&UIP=192.168.0.2&MA=00080266D491&RN=Room 10&PORT=10&RAD=no&TUN=no&CC=yes&PMS=no&SIP=10.0.0.13&OS=http://www.google.com%2F&SIGN=iWp0IHvmmYcSSao%2F6q5Ibw%3D%3D&SIGNED=MA,PORT,RN,SIP,UI&TS=1254862934&NONCE=UAbZx5Pn9H2TqP&METHOD=HMAC-MD5](http://192.168.0.100/default.asp?UI=0197f8&NI=0050e80197f8&UIP=192.168.0.2&MA=00080266D491&RN=Room%2010&PORT=10&RAD=no&TUN=no&CC=yes&PMS=no&SIP=10.0.0.13&OS=http://www.google.com%2F&SIGN=iWp0IHvmmYcSSao%2F6q5Ibw%3D%3D&SIGNED=MA,PORT,RN,SIP,UI&TS=1254862934&NONCE=UAbZx5Pn9H2TqP&METHOD=HMAC-MD5)