Technical Bulletin CS-17-05

IP DECT Server 400 & 6500 Security Enhancements

This technical bulletin explains security enhancements included in the DECT firmware Q3/2017 release.

System Affected

IP DECT Server 400 & 6500

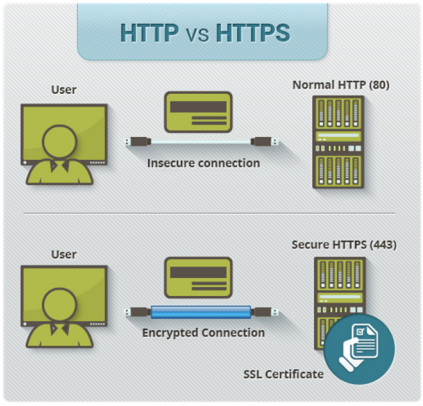
Description

New DECT firmware release Q3/2017

These security enhancements are designed to improve the security around access to our Spectralink IP DECT servers with the goal of providing a higher level of industry standard security and are designed to meet stringent security requirements by modern IT security teams in enterprises large and small. Eventually – these enhancements are designed to provide peace of mind to our end customers – letting them know that the IP DECT servers would continue to work – protected behind a higher layer of security.

Admin Tip: The security enhancements will directly impact how installers/administrators currently log into the DECT servers. If you already have DECT Servers deployed, the following points MUST be understood BEFORE you upgrade the DECT Server with planned Q2 firmware release:

1 When accessing the IP DECT Servers – ONLY HTTPS (https) protocol will be used. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between a web browser and the IP DECT Server you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means that ALL communications between your browser and the IP DECT Server are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking. Web browsers such as Internet Explorer, Firefox and Chrome also display a padlock icon in the address bar to visually indicate that a HTTPS connection is in effect. Note: Changing to HTTPS by default will show a security warning in the web browser when logging in - until a proper security certificate is installed – this may cause concern with some users.



2 HTTP digest authentication has been replaced with a forms and cookies based solution that now allows for storing the admin password salted and strongly hashed. Note: In cryptography, a **salt** is random data that is used as an additional input to a one-way function that "hashes" a password.

3 When you first log into the IP DECT Server with default User ID and Password – you have the added **Option** to change the default user ID and Password, and if you select the new enhanced secure password – it must meet the following conditions:

   a. Minimum length of 8 characters
   b. Must contain characters from at least two of the following classes: upper case letters, lower case letters, numbers and special characters
   c. No simple or dictionary based words (or common numbers such as 12345, 54321, 3.1415, etc.)
   d. New password MUST be different from the last three passwords
   e. Password MUST NOT contain more than two successive identical characters.
      i. *Note: Web Hint would display the password requirements to make it easy to remember the conditions that the enhanced password must meet.*
   f. After being idle for 20 minutes, the logged-in user is automatically logged out of the IP-DECT server web GUI.
   g. The password must be changed every 90 days (or when selecting the enhanced password – you can select the option to Never Expire the password). Note: Even if you select 90 days for password expiry – if no one accesses the DECT Server Web GUI for longer (e.g. 91 days or more) when the DECT Server is accessed next – the user will be prompted to change the password immediately.
      i. *Note: What options are available when password expires at 90 days (and user/admin has lost the password?). Answer: The ONLY option is to do a factory reset – as Spectralink has no back door to access and reset the*

passwords. It is the Installer / IT admin's responsibility to note down and save the password separately.

h. After five successive failed login attempts, the IP-DECT server web GUI will be locked for the next five minutes (to avoid BOT and automated DDOS type attacks)
i. HTTPS is forced by default. HTTP support can be enabled in the Configuration->Security menu (WARNING: Enabling HTTP causes passwords and other sensitive data to be transferred in "clear text" on the network so is NOT recommended/advisable).

4 The IPDECT server now keeps a persistent large FIFO audit log that shows ALL system events:

a. User login / logout
b. System restarts
c. Configuration changes
d. User modifications

Note: This log can only be removed by a factory reset.

Please note that in a future release same security enhancements would also be added to the 2500 / 8000 DECT Servers – however that is not scheduled yet. We would provide a similar communication when firmware for 2500 & 8000 would also be enhanced to support these security enhancements.

Please make a note of these enhanced security requirements and kindly reach out to your Spectralink local partners or support if you have any questions.
Etc

Document Status Sheet

Document Control Number: CS-17-05

Document Title: IP DECT Server 400 and 6500 Security Enhancements

Revision History: Created 08-01-2017

Date: *08/01/2017*

Status: ☐Draft ☒Issued ☐Closed

Distribution Status: ☐Author Only ☐Internal ☐Partner ☒Public

Copyright Notice

Notice

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

Contact Information

US Location
+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com