



Jabra Engage

The most powerful professional wireless headsets on the market are also **the most secure***

Taking security in wireless calls to the next level:
256-bit AES encryption. 128-bit authentication.



GN Making Life Sound Better

* Relates to Jabra Engage 75/65 Stereo and Mono variants. February 19, 2018. See facts on [jabra.com/commercial-claims](https://www.jabra.com/commercial-claims)



Eavesdropping nullified. Cut their connection.

Securing business-sensitive conversations

Cybercrime is on the rise, and in a business environment where customer calls are evermore sensitive, making valuable conversations secure is vital.

Jabra meets this challenge head-on, taking communication security to the next level with the Engage Series – the worlds most secure professional wireless headsets – with security features that go above and beyond the leading Jabra Pro 9400 series, and outstripping all other headsets on the market.

Every call counts, but for some businesses and institutions the ability to make secure calls can make or break a company, safeguard the future of others, and even save lives. Whether you're a government, the military, a financial institution, or simply a business where valuable calls are made, you need to be part of a proactive security culture.⁴

The time to Engage is now. Today, customer privacy is rated as the #1 concern (higher than data ownership, and higher than employee privacy).⁵

The cost of hacked calls – Eavesdropping is a major part of today's crime problem

Cybercrime cost businesses an estimated **\$388 billion** in 2016, making it bigger business than the heroin and cocaine trade (\$288 billion)¹

Cybercrime is growing. In four years, attacks increased by **44%**, and each company was impacted, on average, by \$7.5 million ²

75% of all companies have experienced cyber attacks that last 12 months ³

¹ <https://www.helpnetsecurity.com/2011/09/07/global-cost-of-cybercrime-114-billion-annually/>
² https://www.slideshare.net/GGVCapital/securing-the-cloud-58204760/3-Cybercrime_is_a_Growth_IndustrySource
³ <https://www.helpnetsecurity.com/2010/02/22/75-of-organizations-suffered-a-cyber-attack/>
⁴ Economist Intelligence 2016 ⁵ Helpnetsecurity.com





The solution: Jabra Engage headsets

Patented pairing. Absolute authentication. Encryption excellence.

With Jabra Engage, there is increased security of the wireless connection between the wireless headset and its base unit, and rock-solid security is provided in three steps, improving the protection of calls to a category-leading level.

Pairing

The first step is a physical bonding of the base unit and headset. Jabra has patented ‘physical assisted pairing’ to increase security. The Jabra assisted pairing method occurs only when the headset is docked in the base unit, and a secret link-key is then formed when the two pair.

Authentication

At the start of a call, encryption is used to set up secure authentication between the Engage headset and its base. A link is established using a secret key-link formed in the pairing (without this, the headset and base unit will not work together). This means that a “non-paired” headset cannot be used with the base unit. The authentication link is also protected by encryption. The better the encryption level, the more secure the established link.

Encryption

In calls the audio signal between base unit and headset transports data, which is secured via encryption. The higher encryption level, the better the protection of data. With Jabra Engage, the encryption link is renewed every minute to make decryption more difficult.

Increased protection with Jabra Engage Series wireless headsets

Security algorithms are listed in **FIPS 140-2** standards required by the US military and government, and recommended by the National Institute of Standards and Technology for financial institutions demanding the highest degree of security.

The wireless connection is secured with patented pairing – authentication between headset and base is established with **128-bit** level technology compared to the category-standard 64-bit.

The wireless connection is secured using **256-bit** AES encryption – giving a line of defense that goes beyond that of DECT Security Level C.

Security features: Jabra Engage Series compared



Security features	Jabra Engage Series		Jabra Pro 9400 Series	
	Pairing	Physical assisted, patented pairing	Pairing	Physical assisted, patented pairing
	Authentication	128 bit DSAA2 (AES) ²	Authentication	64 bit DSAA
	Encryption	256 bit AES	Encryption	64 bit DSC
	DECT security level	beyond C	DECT security level	A
	FIPS 140-2 listed functions	Yes	FIPS 140-2 listed functions	No

² DSAA and DSC are the authentication and encryption algorithms defined in the DECT security standard ETSI EN 300 175-7 applicable for DECT security and DECT security step A. DSAA2 and DSC2 are the equivalent updated security algorithms for the next steps of DECT security, steps B and C.

Device security
Other security elements take care of protection of PCs, mobile phones etc.



Wireless headset security
Wireless connection between base and headset is secured using 256-bit AES



Bluetooth®
Signals are encrypted with Bluetooth® standards (version 5.0)¹



Wireless connection secured
by FIP140-2 listed functions for providing security beyond DECT level C

To serve and protect

Patented pairing. Absolute authentication. Encryption excellence.



DECT security has evolved over time from the original security definition, to new enhanced definitions called step A, B, and C; each step offering an increased security over the previous step. Each new security level includes all features from a previous level. This means, for example, that Jabra Engage includes all step A, B and C features. For instance, significant features added in step A (such as early encryption derived cipher key updating at least every minute), and peer-side behavior evaluation.

Jabra Engage Series wireless headsets go one step further, taking advantage of encryption algorithms listed in FIPS 140-2 standards required by the US military and government. This level of security goes beyond DECT Level C.

Jabra Engage utilizes AES 256-bit keys for the very strongest level of encryption in a professional headset.

FIPS 140-2 – What’s good for the military, is now good for you

- **Mandatory for US government**, and recommended for financial institutions in US. Adopted by the UK and Canada, and is recommended for use by other private companies
- FIPS 140-2 lists **approved security functions** for encryption, message integrity, and authentication
- Those functions provide **military grade security** (e.g. AES encryption) approved for use by the US government
- FIPS 140-2 is a standard **backed by National Institute of Standards and Technology**

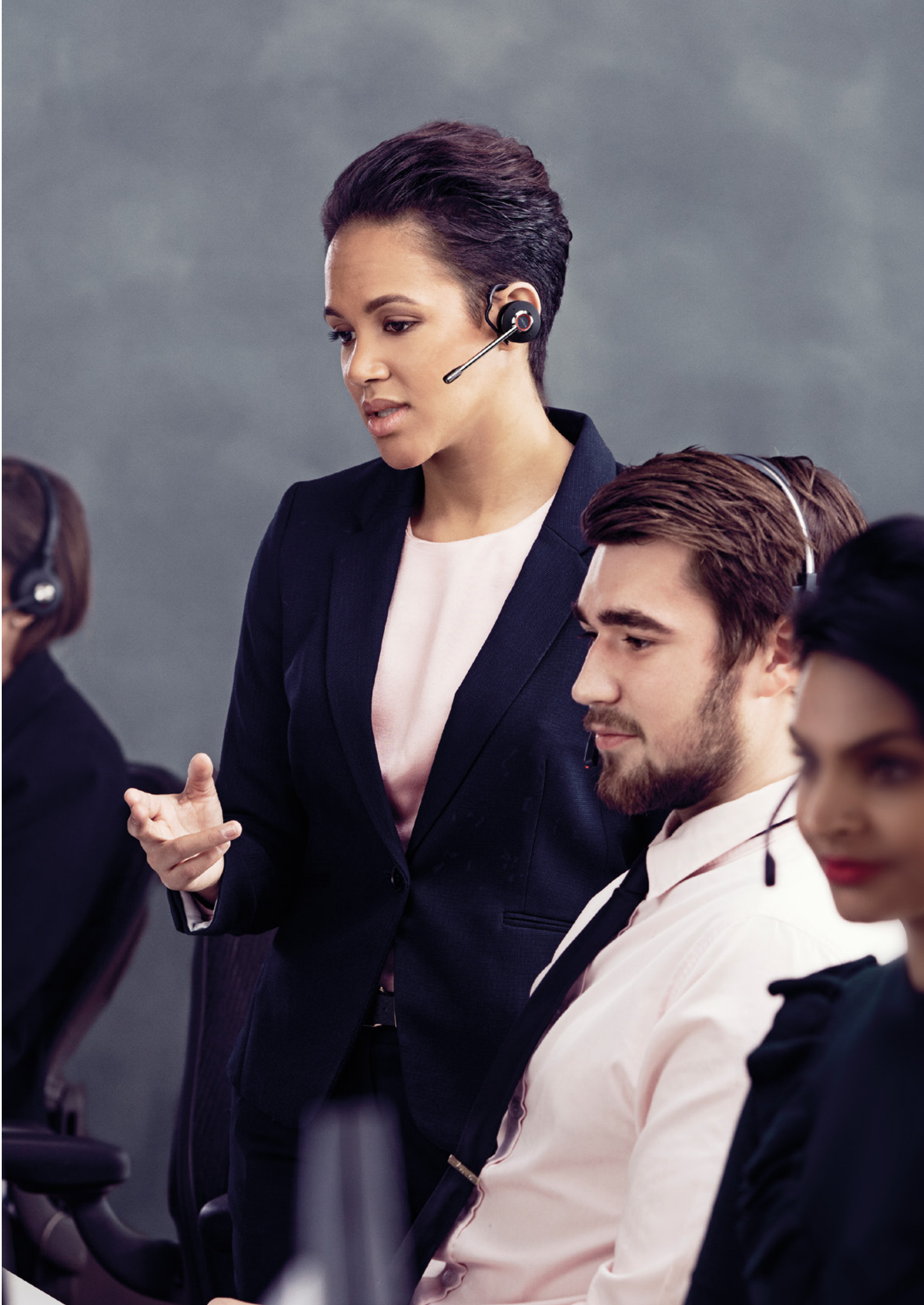


Encryption excellence

Jabra Engage utilizes the very strongest level in a professional headset

Jabra Engage Series				
Jabra Pro 9400 Series				
				Military Standards Engage FIPS algorithms
			DECT security step C	Even stronger encryption of audio stream using AES 256 bit keys
		DECT security step B	Strong encryption of audio stream using AES 128 bit keys (DSC2) ¹	The security level of the Jabra Engage DECT wireless headset has been independently tested and verified by NCC Group/ FortConsult.
	DECT security step A	New authentication using strong AES 128 bit encryption (DSAA2) ¹		
DECT security	New features which correct certain vulnerabilities			
Authentication (DSAA) ¹	Secure DECT certification			
Encryption (DSC, 64 bit keys)				
<div><div>fortconsult</div><div>part of nccgroup</div></div>				

¹ DSAA and DSC are the authentication and encryption algorithms defined in the DECT security standard ETSI EN 300 175-7 applicable for DECT security and DECT security step A. DSAA2 and DSC2 are the equivalent updated security algorithms for the next steps of DECT security, steps B and C.





More about Jabra Engage Series wireless headsets

The world's most powerful professional headset*

- Provides superior wireless connectivity to a range of up to 150 meters/490 feet, enabling up to **3x more users** in the same office space – with no loss in connection quality.
- Advanced noise cancelling microphone and enhanced speakers deliver crystal-clear calls **even in noisy offices**. Meets Skype for Business Open Office requirements.**
- **All day battery life** and a **busylight** that acts as a do-not-disturb sign for colleagues.
- The security level of the Jabra Engage DECT wireless headset has been **independently tested and verified** by NCC Group/FortConsult.



Why Jabra through ScanSource?

Different working environments, office layouts and interiors present an almost infinite variety of challenges to effectively planning and deploying multiple wireless headsets in a limited space. As a global technology solutions supplier, ScanSource can help your customers select and deploy wireless headset solutions that meet the needs of their business, work style, and physical layout. ScanSource has spent decades assembling a team of select suppliers—such as Jabra—whose products enable productivity, security, and customer satisfaction. Learn more by contacting your Jabra ScanSource team at jabra@scansource.com.

[ScanSource.com/JabraEngage](https://scansource.com/JabraEngage)



* Relates to Jabra Engage 75/65 Stereo and Mono variants. February 19, 2018. See facts on jabra.com/commercial-claims ** Variant dependent

Jabra Engage Whitepaper Security update – 10/06/2019

© 2019 GN Audio A/S. All rights reserved. ® Jabra is a registered trademark of GN Audio A/S.

The Bluetooth® word mark and logos are registered trademarks owned by the Bluetooth SIG, Inc. and any use of such marks by GN Audio A/S is under license.