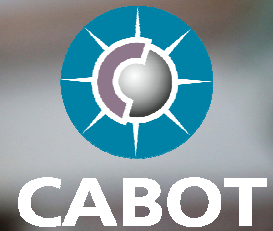


Software Upgrade



Cabot's software upgrade mechanism is available as part of an integrated middleware solution or as a component plug-in. It has been designed and tested to provide Cabot customers with a secure and efficient way to make product upgrades both before and after deployment.

Continuous and seamless product upgrades - any time, any place

The constant evolution of new standards and functionality means that, without a software upgrade mechanism, products can become out of date soon after deployment. Cabot's upgrade solution, known as Callisto, is fully compliant with ETSI SSU and Enhanced SSU standards as well as the UK D-Book. Callisto automatically configures itself to the correct OAD protocol on detecting the appropriate network and will switch automatically depending on the location of the device. The DSM-CC data and object carousel enable seamless upgrades to be carried out whether the device is still in the factory or in-situ in the field. This enables customers to maintain critical market windows by delivering enhanced functionality after the product has been released and to easily fix any field issues even after deployment.

Upgrades with the customer in mind

Callisto provides a range of options for how upgrades can be managed. Forced downloads can be set to take place at specified dates and times or user interactive downloads can be activated via on-screen messages sent directly to the viewer. In addition, the following enhancements have recently taken place to improve the upgrade experience:

- **One DSM-CC per tuner is now supported, allowing for the simultaneous download of more than one carousel. This enables, for example, an OAD to take place on a twin tuner platform without impacting on any shared resources (e.g. a running MHEG application).**
- **OADs can now be tailored for download and verification in several parts, rather than one contiguous image. This not only provides more flexibility about how downloads can be performed but also minimises upgrade time and any platform-specific memory constraints**

As part of Cabot's continuous development roadmap, Cabot is also integrating the ability to use a local update mechanism such as USB, as required by the D-Book v6. Further upgrade mechanisms, such as via the internet, are also in development.



Complete the digital experience

Complete software security for deployed receivers with SEA Manager

As there is currently no default security provided in the current OAD standards, unprotected deployed receivers can be exposed to erroneous field upgrades. The Security, Encryption and Authentication (SEA) Manager enables receivers to be protected from malicious, corrupted or misdirected upgrades, whether over air or via hardware interface. The SEA includes a PC toolkit which enables the digital signing of software upgrades using public key cryptography. It works by embedding key pairs in the receiver so that only authenticated and authorised upgrades will be re-flashed by the receiver. In addition, to protect from possible corruption over the network, the SEA PC toolkit generates a specialised and rigorous checksum to be verified by the receiver before upgrade acceptance.

Cabot's product road maps are continually evolving so for the most up-to-date information regarding product functionality please visit our web site www.cabot.co.uk or contact us via any of the methods listed below:



Cabot Communications Ltd
Verona House, Filwood Road
Bristol BS16 3RY, UK
Tel: +44 (0) 117 958 4232
Fax: +44 (0) 117 958 4168
Email: info@cabot.co.uk