

# 10  
Use  
case

**SecuriConnect®**

**Video conferencing  
complemented with  
encryption approved  
to handle classified  
information**



**Video conferencing makes business sense today, improving collaboration and operational efficiency while cutting costs and environmental impact. However, digitalisation in general increases attack vectors, with video conference deployments particularly susceptible to cyber-attacks.**

# Video conferencing complemented with encryption approved to handle classified information

## Securing all the benefits of video conferencing

For government agencies such as the police or courts of law, and for others communicating valuable, sensitive and/or classified information, implementing secure video conferencing needs to be a priority. Existing video conferencing device can be leveraged if complemented with SecuriConnect network encryption.

## Easy to set up and scale up

The SecuriConnect system is a plug-and-play encryption solution designed according to IP networking standards, guaranteeing sustainable future-proof communications privacy secure. Therefore, it is easy to deploy into your existing network infrastructure. It supports network features such as NAT, QoS, DHCP, Access List, and NTP. Also, all end user applications are supported, including time critical real-time information.

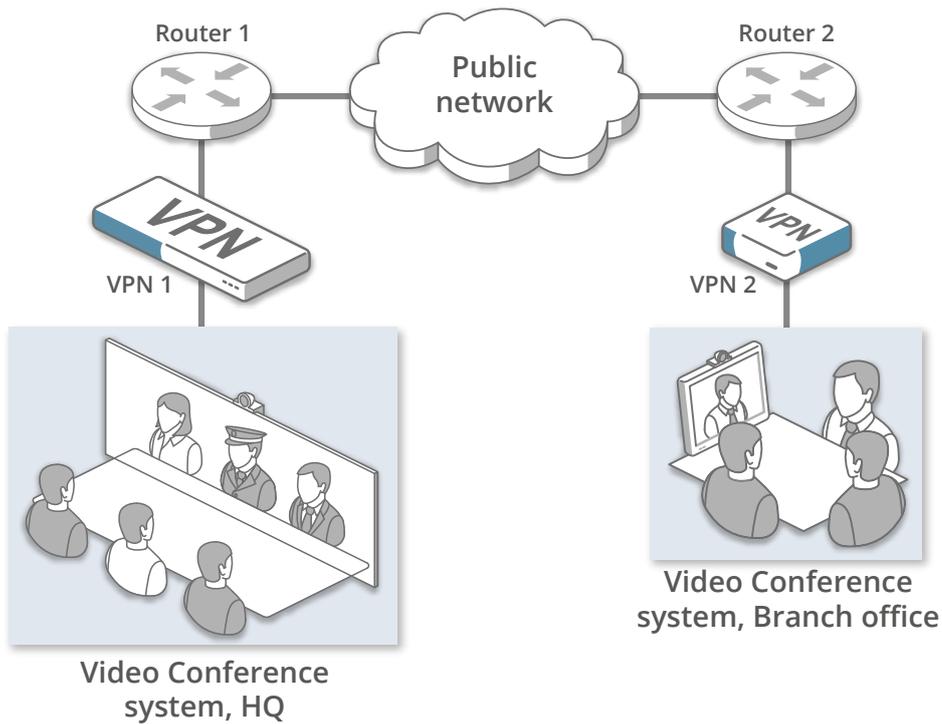
## How SecuriConnect works

Placing a SecuriConnect device between the video conference (VC) system and both sides of the carrier network has the same effect as a dedicated secure point-to-point connection. Communication is carried out via cryptographically protected tunnels through the carrier IP network rendering vital network security functionalities such as authentication of information origin, integrity control and anti-replay mechanism. To ensure the best possible user experience, the SecuriConnect system utilises Quality of Service (QoS) on every tunnel.

## Flexible layout

The illustration shows a simple SecuriConnect protected VC design with a point-to-point encrypted tunnel between VC system 1 and VC system 2. VC system 1 can call VC system 2 and vice versa. The design can be used for up to 512 VC sites, each protected by SecuriConnect devices and interconnected via encrypted tunnels (full-mesh network).

The SecuriConnect device ED140 can also protect multiple VC systems within the same network site. Depending on the video quality and the video codec used, approximately 120 simultaneous video conference connections can be maintained with the same high quality.



Extensive SecuriConnect protected video conferencing deployment can be facilitated by using a key server and central administration with remote configuration, network monitoring and extensive logging.

### Encrypted communication, uncompromising quality

Encrypted point-to-point and multipoint VC calls can easily be achieved with SecuriConnect network encryptor without compromising the quality of the call. It is also easy to integrate encryption to an already deployed VC system.

### SecuriConnect benefits

- Superior communication privacy with Advenica's advanced technologies, quantum secure algorithms and Three Domain Separation.
- Easy to deploy into existing network infrastructure – operational within minutes.
- Easy to use and intuitive to manage.
- Flexible and fully scalable – can accommodate multiple VC systems.
- Provides maximum protection in line with national and international regulations.



Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

**Read more at [advenica.com](https://advenica.com)**



© Copyright 2020 Advenica AB. All rights reserved. Advenica and the Advenica logo are trademarks of Advenica AB. All registered and unregistered trademarks included in this publication are the sole property of their respective owner. Our policy of continuous development may cause the information and specifications contained herein to change without notice. Doc. no.: T7852 v1.2

ISO 9001  
CERTIFIED  
ISO 14001  
CERTIFIED