vivitek®

Digital Signage | NovoDS

NovoDS Security Whitepaper

The importance of an integral approach to security in Digital Signage - from device access to network and data security

vivitek

TABLE OF CONTENTS

1. INTRODUCTION

Digital signage deployments have grown rapidly in recent years, appearing everywhere from shopping malls and restaurants to office buildings and schools. However, security or protection against unauthorised users and data hacks is often overlooked in the design of many products currently on the market. This white paper describes the design and implementation of the security measures integrated into Vivitek's NovoDS products, which provide data protection for digital signage applications.

The Vivitek NovoDS product family was launched in 2014, as part of Vivitek's Novo Ecosystem. All Novo products are based on four guaranteed principles: simplicity, security, integration and centralisation. This white paper will focus on the principle of security. From the outset, data security has been one of the major design goals in developing these products, from device access to data encryption.

The Novo Ecosystem includes all-in-one displays and add-on devices (to upgrade your existing screen) which make up a flexible and scalable wireless collaboration and/or digital signage solution. It can be configured easily in any venue and provides a very simple user interface that is identical across the entire ecosystem.

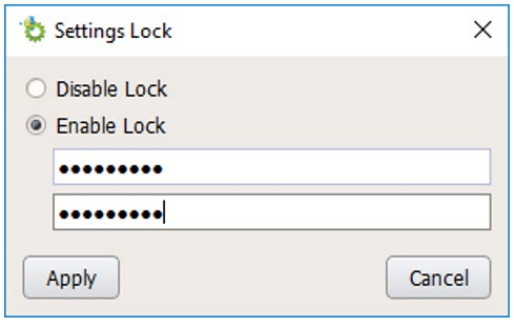
This white paper will address the data security of the NovoDS solutions in detail.

2. DEVICE ACCESS

Security does not only apply to how secure your data encryption algorithm is. In fact, security often starts from something much more basic, such as device access control.

NovoDS provides a "Settings Lock" to prevent unauthorised users from accessing the actual devices. In doing so, unauthorised users will not be able to tamper with the device settings or install any malicious Apps on NovoDS devices.

Users can enable the "Settings Lock" on the device or from NovoDS Studio or NovoDS Cloud, as illustrated in the figure below.



3. NETWORK SECURITY

Most of NovoDS devices have both Ethernet and WiFi connections to allow a configuration that suits your deployment and security requirements. The only exception is NovoDSmini which has Ethernet only.

1. **Ethernet**

   By connecting the NovoDS' Ethernet port to your organisation's Intranet, the NovoDS device becomes a standard network device on your Intranet. This means that all your network policies, such as the firewall, will apply to the NovoDS device, ensuring it is under the full control of the network administrators. As a result, the Ethernet connection eliminates any concern when it comes to network security.

2. **WiFi**

   WiFi security has been under intense scrutiny from the early days of WEP protocol. Modern security protocols like WPA2 greatly improve WiFi's security level. In particular, WPA2-Enterprise with 802.1x authentication has become the norm for corporate WiFi deployment. NovoDS supports a range of WiFi protocols, including WPA2 and WPA2-Enterprise with 802.1x authentication. This ensures that NovoDS' WiFi connection matches the protection of your company's WiFi infrastructure.

In addition, it is worth mentioning that:

1. NovoDSmini doesn't have WiFi capability which makes it free from the risk of being tampered by malicious users via a wireless network. This is of great importance when deploying NovoDS solutions in public space.
2. NovoDS (DS200) and NovoDS4K do support WiFi connection. However, when the Ethernet is connected, the WiFi connection is disabled automatically.

4. COMMUNICATION SECURITY

NovoDS not only comply with existing network security policies, but also takes a step further when it comes to communication and content security.

When communicating with NovoDS devices over the network, two options are available - NovoDS Public Cloud, and NovoDS Studio software.

1. **NovoDS Public Cloud (https://www.novods.com)**

   NovoDS Public Cloud allows users to control and manage their NovoDS devices over the Internet. All communications are conducted using HTTPS and WSS (Web-Socket over SSL) protocols, which are the de facto communication protocols adopted by the Internet, and eCommerce in particular. In other words, a proven security mechanism is used by NovoDS Public Cloud.

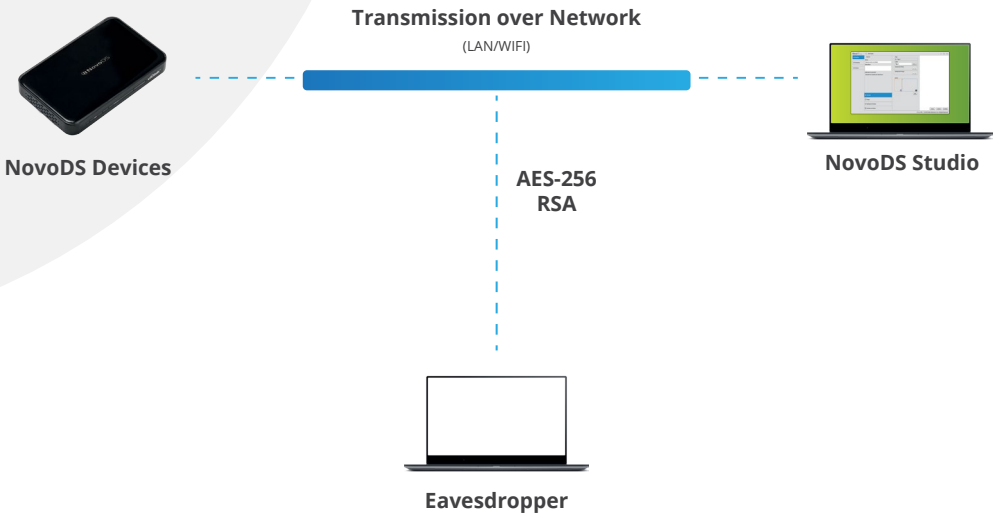
2. **NovoDS Studio**

   NovoDS Studio enables users to control and manage their NovoDS devices within an internal network. This includes in-office networks and VPN connections.

   As explained in Section 3, the communications to and from NovoDS devices are managed by your IT/network administrators. In addition, two additional encryption mechanisms are implemented.

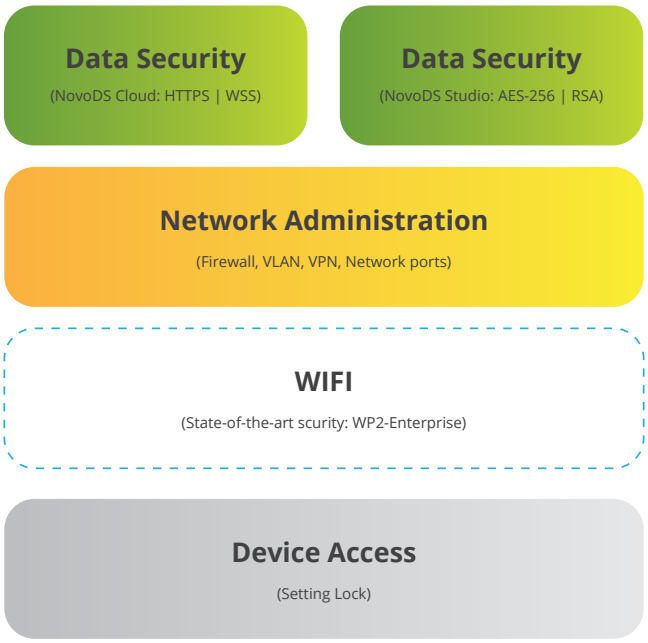
   - Commands and responses between NovoDS Studio and NovoDS devices are encrypted by AES-256
   - Playlist transfers from NovoDS Studio to NovoDS devices are encrypted by RSA

   Suppose someone has authorised network access like you do (for instance, an employee having legitimate network access, or a “hacker” breaking into your internal network). They could try to ‘eavesdrop’ on the communication. With AES-256 and RSA in place, the ‘eavesdropper’ is not able to ‘siphon’ any useful information.



5. CONCLUSION

The following figure summarises the security mechanism implemented in NovoDS devices, from the user managed “Device Access” settings to “Data Security”.



In conclusion, the protection built into NovoDS devices, in combination with company firewalls and state-of-the-art encryption mechanisms, provide a high level of security for digital signage applications.

FOR MORE INFORMATION, PLEASE CONTACT:

Vivitek EMEA

Zandsteen 15 | 2132 MZ Hoofddorp | The Netherlands

tel: +31 20 800 3960 | fax: +31 20 655 0999

e-mail: info@vivitek.eu

website: www.vivitek.eu

File version 01.00-mdu