CTOUCH®
The power to engage

Security Note

CTOUCH Neo

Introduction

This document discusses the various security aspects of the CTOUCH displays. It is organized around the various functions and components which make up the CTOUCH Neo product.

Note: this document only briefly discusses Privacy aspects. Privacy aspects are described in detail in the CTOUCH privacy statement which can be found on our website, this document should be seen in conjunction with the CTOUCH privacy statement.

In general

This document describes the security measures that can be taken with the CTOUCH product. Please make yourself aware of the possible security options the product offers. When you order a CTOUCH product in the default setting, the Neo is set up in the most user and privacy friendly way possible. Configurating our products is a balance between security and functionality. The user should always take into account the environment in which the Neo is used when deciding on specific settings and choices.

Please note that the settings on our products are only part of a security solution. We recommend incorporating the security of the screens into your overall security measures and policies. Pay attention to secure behaviour, like changing pincodes and/or passwords on a regular basis and not storing pincodes and/or passwords in places that are not safe. Be aware of who uses your screens for what purposes.

Neo: Secure-by-Design

CTOUCH Neo has been designed from the start with security in mind. This means that while we focus on making a very user-friendly touchscreen, we aim to make choices that are secure by default, while not getting in the way of the user. For example our having settings behind a 6-digit, non-obvious pincode, no user data stored on the screen and automatic browser data removal. With these kind of default settings, we believe that we offer one of the most secure touchscreens on the market, while allowing the administrator to make choices to customise for their organisation.

Secure settings

All Neo settings are default behind a 6-digit pincode. This pincode is set when going through the install wizard. It does not allow for obvious pincodes, such as 000000, 012345, 123456. In addition, there is a rate-limiting implemented: When the wrong pincode is entered, it takes a few seconds before you can enter another one. The more wrong pin codes are typed, the longer it will take to have another attempt.

Neo offers three security levels (Secure, Standard and User friendly) that are set when going through the installation wizard. The most secure level (‘Secure’) does not allow for any data to be stored on the screen. In the ‘Standard’ mode, the USB stick can be accessed for touch, video, sound and data, but the screens internal storage is not accessible. The ‘User friendly’ mode gives the greatest amount of freedom, but at the expense of lesser security: It allows for data access to/from both USB storage as well as the screen’s internal storage.

Applications and data

In order for the Neo to be super user friendly to beginners and advanced users, the Neo screen comes with few built-in applications and tools: CTOUCH Whiteboard, AirServer wireless sharing, (optional) Chromium browser, screenshot tool and annotation tool. These applications have been designed with security in mind and minimal data/network use. The whiteboard, screenshot and annotation tool will not store data on the screen's storage, on USB or in any cloud server outside the screen. Whiteboard, screenshot and annotation contents are being made available for the user through the application's 'save' buttons: When the user presses this button, a QR code and web address are show to the user and a tiny, dedicated server is started on the screen where the user can download a PDF with the contents of the application. As soon as the QR and web address popup is closed, the tiny webserver on the screen is closed.

Neo offers wireless sharing through the AirServer app. This allows a user to share his/her screen through the natively supported protocols in de user's device - Miracast, AirPlay or Google Cast - without having to install any sharing applications or software on the user's device. AirServer does not know what it is sharing, just like the video ports on the Neo it is just transferring video from the user's device onto the screen. In order to limit who can share on the device, Neo's default settings are set to only allow screensharing to a user when an 'OK' button is touched on the screen. This means that not a random person can share on the Neo screen, but only one who is acknowledged by the person in front of the screen. Note that this settings can be changed from the AirServer settings that are accessible from the Neo settings (behind pincode). Sharing traffic from a user to the Neo screen will either go always go straight from the end user's device to the Neo screen: It will never leave your local network or go over the internet.

The installation of the Chromium browser is fully optional and decided upon while going through the installation wizard. In the secure and standard security settings (in the wizard), the Chromium browser will erase all history, bookmarks, user-accounts, cookies and other possible user data after closing the Chrome application or shutting down the screen.

The Neo screen does not allow to install any applications or .APKs , wither by the admin or a user, making leaking of data, credentials, histories, etc. very unlikely.

Physical ports

Many of the Neo's physical ports can be enabled and disabled from the - pincode protected - settings menu. This includes all video interfaces (HDMI, DP, USB-C, OPS), all USB ports (on/off) and all network interfaces (Ethernet ports, Wi-Fi interface, Wi-Fi hotspot and Bluetooth). The Neo screen can therefore have the interfaces configuration desired by the screen's manager/admin, even for (semi-)public spaces such as college or university classrooms.

Other interfaces such as touch, the blue CTOUCH button and remote control interface, and the onscreen buttons in the quick menu (opens when pressing the blue CTOUCH button) can be enabled and disabled from the settings menu, making the screen fully configurable and flexible for many environments.

For physical security, the Neo screen comes with a physical 'Cable lock': an optional steel protection plate that can be screwed over the connector area of the Neo. This allows for physical protection over the connectors and OPS on the side and bottom of the screen, limiting access and preventing insertion and pulling of cables and USB-sticks. This

‘Cable lock’ comes with each Neo screen in the box. This protector is normally secured with the screen’s normal Philips screws, but can be secured with user-provided security screws.

Network connectivity

As mentioned in the Physical Ports chapter, all network interfaces can be enabled and disabled from the settings menu. The Neo limits services on networks ports to only the ones strictly needed for the offered functions. Apart from the Sphere service, these services only run when the function is active (AirServer) or enabled in the settings menu (JSON API):

- Wireless screen sharing: AirServer Miracast, AirPlay and Google Cast service (these can be enabled and disabled from the AirServer settings menu, accessible via the Neo settings)
- Sphere interface: HTTPS encrypted, security token
- JSON control API: Security token, default disabled

Firmware

CTOUCH is committed to offering a secure touchscreen, now and in the future. This means that we will keep offering firmware updates with bugs fixes, new features and security updates for years to come. In order to make it easy for the user to always have the latest firmware and security fixes, by default Neo will show a popup when a new firmware is available and allow for direct install. In the settings menu, it is also possible to set the firmware upgrade (typically call Over-The-Air update or OTA update) to fully automatic: In that case, not even a popup will be shown but the latest firmware will be installed automatically the moment it is available.

With our Sphere management system the IT admin or dealer can check in real-time any of the settings, installed firmware version and change/update these remotely. We believe this will make security a breeze for any organisation.

Independent security assessment

CTOUCH has had independent firm Grant Thornton advise on and assess the security of the Neo screen. Grant Thornton first created a list of area’s to consider and requirements for implementing for security of touch screens. Based on this list (known as the CTOUCH Security Base Line), CTOUCH has designed and implemented security measures to create a screen that will fully pass security assessment and is secure-by-design. As a second step, Grant Thornton has done an independent penetration test (abbreviated pen test), whereby their security try to access the screen in any way possible via any of the physical and network interfaces and try to gain access to the system or data. Results of these pen test are described in a report and can be discussed upon request.

More information/questions

In case you would want to know, more details or have questions regarding Neo security: Please contact CTOUCH service (support@ctouch.eu) or your account manager. We are happy to answer your questions and tell you more…