CTOUCH®
The power to engage

Security Note

CTOUCH Riva D2

CONTENTS

INTRODUCTION

This document discusses the various security aspects of the CTOUCH displays. This document is organized around the components which make up the CTOUCH Riva D2 product.

Note: this document does not especially touch upon Privacy aspects. Privacy aspects are described in the CTOUCH privacy statement, 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, we will format all settings in the most user and privacy friendly way possible. Configurating our products is a balance between more secure – less functionality. The customer should always take the setting where the CTOUCH product is used into account when choosing its preferable option. Please also note that a number of add-ons are available for CTOUCH products, which can enhance privacy and security of our products.

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 pin codes or passwords on a regular basis and not storing pin codes and/or passwords in places that are not safe. Be aware of who uses your screens for what purposes.

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 PIN codes or passwords on a regular basis and do not store PIN codes and/or passwords at places that are not safe. But also, be aware of who uses your screens for what purposes.

RIVA D2: SECURE-BY-DESIGN

CTOUCH Riva D2 has been designed with security in mind from the start. This means that while we focus on making a very user-friendly touchscreen, we always try to make choices that are secure by default, while not getting in the way of the user. Examples of this are secure default settings, settings behind a – non-obvious - 6-digit pin code, possibility to block network connection, USB and video input ports.

With these 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.

SOFTWARE UPDATES

Keeping the software of your CTOUCH product up to date is very important, since threats are continuously evolving. We offer services to keep your product up to date, this could be part of your organizational security regarding privacy and security. Whether and how you use our updating services depends on the settings of your CTOUCH product. If you have not requested a change of settings, or changed the settings yourself, CTOUCH products will by default update its software automatically. If you do not use the CTOUCH updating services, we strongly recommend using the latest updates of all software and firmware running on your CTOUCH product. Updates are frequently made available by CTOUCH. These updates can be installed "over-the air (OTA)". The OTA URL in the OTA download page cannot be adjusted at any user level. If the customer does not accept over the air updates (which can be activated in the setup menu), a USB key with the newest update can be loaded into the screen through the USB connector. The software update can be collected on the CTOUCH site in the Help Center. This part of the internet site is only accessible for authorised resellers and is secured by an account name with a password.

PASSWORDS AND PIN CODES

CTOUCH offers the option to remind users periodically to update their login credentials and internal passwords. Since some users may find this feature non-convenient, we offer the option to switch this functionality off.

We strongly recommend to CHANGE DEFAULT PIN CODES on your CTOUCH product! Using the factory default PIN codes would make it very easy for unwanted guests. Of course, the possible attackers will still have to obtain physical access to our product to make configuration changes. But the way our products are typically used, makes it vulnerable to these "attacks". We request to create a PIN code when configurating your CTOUCH product but cannot force you to change this PIN code over time.

The applications used on CTOUCH products have a number of safeguards to prevent passwords, PIN codes and other credentials being stored on these devices. Unfortunately, we are unable to prevent this storage entirely. In order to secure that end-user personal information is kept safe, we strongly advise not to store credentials in apps when other users can have access to these apps as well. We request our customers to monitor and inform end-users about storage of personal data on CTOUCH products.

THE DISPLAY SETTINGS

The CTOUCH Riva D2 has a very extensive configuration set. The large number of configuration options provide user the best possible personalized CTOUCH user experience but may also provide extra security options when needed. The configuration data is stored locally in the screen to enable complete stand-alone operation, so even without any network or device connected it can operate.

The configuration data is divided into maximal 5 user access levels, a dealer level, and a factory level. The user access levels are configurable by the admin of the customer. The rights to amend or add things to the CTOUCH product can be amended for every level of access. At the admin/dealer level the following options are available to restrict access and functionality to lower level users:

- Enable/Disable USB ports
- Enable/Disable Network (LAN) ports
- Enable/Disable Wi-Fi
- Enable/Disable Bluetooth
- Enable/Disable Android OS as Source
- Enable/Disable Wake-on-LAN
- Enable/Disable Touch functionality
- Enable/Disable Rooted device
- Enable/Disable Local installation of Apps
- Enable/Disable CTOUCH Button
- Block shortcuts of external keyboards to prevent users without permission to install, open or copy apps or files.

The CTOUCH products standard configuration has almost all functionalities switched on. These settings may be amended according to your answers in the CTOUCH intake. These amendments will be done by CTOUCH or the CTOUCH dealer. In the start-up wizard, the CTOUCH privacy agreement is included, can be opened and read, and should be accepted, before proceeding the configuration.

The dealer menu is protected with a key combination on the standard remote control. Additional to a key on the remote control an additional PIN code can be activated on the screen to have a 2-level authentication. The factory menu is protected with a key combination on a service remote control. There is no separate PIN code on the screen to access the factory menu. This can solely be done through a service remote.

Service and maintenance activities from CTOUCH or support partners, cannot be carried out without being granted access to the screen by the customers Admin. In case of lost passwords, CTOUCH or het service partner can just do a complete reinstall of the screen. All settings, applications as well as local stored content will be lost if user PIN codes are lost. This should be taken into account when choosing a PIN code for the CTOUCH device.

CTOUCH SPHERE

The CTOUCH Riva D2 is offered with a Remote Device Management service called Sphere. We strongly recommend our customers to use this service. Sphere lets you monitor, manage, and control all your connected devices from one easy-to-use platform. This provides you the possibility to monitor the status and configuration of screens very easily from a remote management console. It takes care of the communication with the MDM console at ctouchsphere.eu. During the enrolment procedure at initial installation, a first “handshake”

between screen and the Sphere server will generate a unique authentication token. This token is stored on the server and the screen. Some of the benefits of using Sphere MDM are:

- It analyses device and app usage;
- It centrally manages apps *), OS settings and updates;
- It helps to detect strange usage of the CTOUCH products connected;
- It provides functionality to maintain and secure the Android environment which runs on CTOUCH products;
- It allows you to monitor changes in display settings, detect newly installed apps, usage increase of certain apps etc. and immediately take action to block, remove or restore items *)

*) expected Q1 2024

For all benefits please visit CTOUCH Sphere MDM's website: https://ctouch.eu/nl/sphere

The security architecture of the Sphere Service is described on: https://support.ctouch.eu/hc/en-us/articles/6098774552476-What-are-the-network-requirements-for-Sphere-

ALTERNATIVE MDM

The CTOUCH Riva D2 does also offer Remote Device Management service via VISO MDM as alternative for CTOUCH Sphere. For all benefits please visit VISO MDM's website: https://www.radix-int.com/solution/viso-mdm-emm/

The security architecture of the VISO Service is described on: https://www.radix-int.com/viso-mdm-architecture-overview/

NETWORK CONNECTIVITY (LAN/WI-FI)

For our products to function appropriately, the 802.1x network authentication protocol is by default supported. This means that the CTOUCH product may by default be connected to the internet using a LAN connection. Please note that this means that customers must make sure this LAN environment is safe to connect to.

It is recommended to place the screens in a dedicated network segment protected by firewalls. Please note that if a customer does not have a specialized IT professional that will install the CTOUCH products, that we recommend our dealers to ensure that the product is installed in a safe (digital) environment. Whether or not extra consultancy should be obtained to ensure a secure environment, should follow from the CTOUCH intake.

As described in the section display settings the screen provides options to disable network connectivity interfaces. These portals are switched off by default, we recommended to keep them disabled as long as they are not in use.

The WI-FI settings offer different security protocols like WPA2-PSK. As for all connected devices we strongly recommend not to use open and unencrypted Wi-Fi connections.

As mentioned in the Display Settings chapter, all network interfaces can be enabled and disabled from the settings menu. The services running on these interfaces are protected by the following means:

- Sphere interface: HTTPS encrypted, security token
- JSON control API: Security token, default disabled

INSTALLING APPLICATIONS

Please be aware that some applications that are available online, pose serious risk to the safety and security of your CTOUCH product. To prevent malicious application to be installed on your device, we have taken a number of measures.

Firstly, we have preinstalled a list of applications which are safe to use. The following applications are always pre-installed on your CTOUCH product:

1. UBoardMate
2. E-Share
3. File Commander
4. Office Suite
5. Aqua mail
6. CTOUCH Sphere MDM
7. VISO MDM

Secondly, customers have the option to disable or enable other users besides the admin to also download applications, please be aware that enabling other users to download and install applications comes with a privacy and security risk.

Thirdly, we offer the option to use an MDM solution that allows only organization approved apps on the device.

Fourthly, CTOUCH is currently developed a dedicated CTOUCH App store with apps that have been whitelisted by CTOUCH.

ANDROID SETTINGS

The CTOUCH Riva D2 has an embedded Android module currently running on Android 11. The Android eco-system is working constantly to improve the security level of Android. If you use CTOUCH updating services as indicated above, we will keep track of new updates of your CTOUCH Product.

Please use the CTOUCH Sphere Device Management application (or alternative) as it provides functionality to control, maintain, and secure the Android environment like indicated above.

REMOTE MANAGEMENT & MAINTENANCE

CTOUCH or its dealers may need access to the CTOUCH device to provide support or error connection. Before such access is acquired CTOUCH or its dealers will always request permission from the customer. This way this access cannot be obtained without prior permission.

Remote API – token/timestamp is an extra layer of protection installed by CTOUCH to ensure protection in case of remote management and/or maintenance. This ensures that no external commands can be given to your CTOUCH device that may harm your security.

MORE INFORMATION/QUESTIONS

In case you would want to know, more details or have questions regarding Riva D2 security: Please contact CTOUCH support (support@ctouch.eu) or your account manager.