Application Note Security

CTOUCH Leddura 2Meet

Version 1.1 (Released)

Last update: February 28, 2018

Authors

Name	Role	Department
Willem Jan van der Meer	Product Manager Corporate	Product & Innovation

Document History

Date	Version	Document Revision Description	Document Author
16-10-2018	0.1	Draft	W.J. van der Meer
18-10-2018	0.2	Minor layout changes	W.J. van der Meer
23-10-2018	1.0	Released	W.J. van der Meer
28-02-2019	1.1	Fixed broken links	W.J. van der Meer

Table of Contents

1 Introduction

This document describes the security aspects of Leddura 2Meet. The product is built around 3 hardware building blocks:

1. Intel NUC
2. CTOUCH Router (build into the screen)
3. CTOUCH Touch Screen

containing 4 software components:

- Intel NUC: Windows 10 IoT Enterprise
- Intel NUC: Kickle application
- CTOUCH Router: Embedded OS
- CTOUCH Touch Screen: Embedded OS

1.1 Purpose of the document

The purpose of this document is to give insight for IT-personal/installers on how to apply the best security for their environment.

1.2 Scope of the document

The scope of the document is about the hardware and software components as part of Leddura 2Meet. It will not explain on how to apply the different security policies since that is customer and implementation specific.

1.3 Related documents

Please find below the different related documents/websites with regards to Leddura 2Meet:

Component	Name (with link to the document)	Description
OAuth	https://oauth.net/	An open protocol to allow secure authorization in a simple and standard method from web, mobile and desktop applications.
OpenID	https://openid.net/	OpenID allows you to use an existing account to sign in to multiple websites, without needing to create new passwords.
Windows 10	https://www.microsoft.com/en-ww/windowsforbusiness/windows-iot	Windows 10 Internet of Things.
Intel® NUC	https://downloadcenter.intel.com/download/24345/Intel-Driver-Support-Assistant	Intel® Driver & Support Assistant
CTOUCH	http://support.ctouch.eu	Help Center providing FAQs, documentation, firmware etc.
Kickle	http://support.kickleforskype.com/support/signup	Login request
Kickle	http://support.kickle.com/support/home	Deployment Guide

2 Kickle Application

This chapter describes ports and protocols used by Kickle, Office 365 APIs (consent/OpenID), configuration storage and remote access principles.

2.1 Ports and protocols used by Kickle for Skype for Business

Below you'll find the protocol and port used by Kickle:

- For a Skype for Business On-Premises and Exchange On-Premises infrastructure
- For a Skype for Business Online and Exchange Online infrastructure.
- For a hybrid configuration.

http://support.kickle.com/support/solutions/articles/8000073117-protocols-port-requirements-bandwidth

2.2 Ports and protocols used by Kickle for the Cloud platform

Protocols and ports used by Kickle to communicate with the Cloud Platform are detailed here: http://support.kickle.com/support/solutions/articles/8000073117-protocols-port-requirements-bandwidth.

2.3 Ports and protocols used by Kickle for the Wireless Display

Ports and protocols used by Kickle for the Wireless Display are detailed here:
http://support.kickle.com/support/solutions/articles/8000073117-protocols-port-requirements-bandwidth

2.4 Office 365 APIs, OAuth, Consent flow

Kickle uses OpenID authentication to get access to Office 365 resources. Authentication principles are detailed here: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-v2-protocols.

Kickle (i.e. the Skype for Business account used by Kickle) requires the following permissions:

- Read/Write Skype user information
- Initiate conversation and join meetings
- Receive conversation invite
- Read/Write Skype users contacts and groups
- Create Skype meetings

- Sign in and read user profile

These permissions are OAuth standard permissions (based on Azure AD Application specifications). Kickle needs to access your SfB Online instance to initiate a call, read the contact list, etc., as a normal user would do (same "level" permissions than a normal user). The "consent" is an activation in your O365 tenant, to specify that "Kickle is an application and will need to authenticate to the Skype server with a user account". In addition to that, Kickle will always need a Skype user account to authenticate to the Skype server. So there's two security levels: application level AND user level. Without a user account, CTOUCH/Kickle cannot access the Skype server, even if you did the consent.

Note: To use these Office 365 APIs, it is necessary to use a Skype for Business account which is authenticated on the specified Office 365 tenant, and to specify the application ID. **CTOUCH/Kickle employees CANNOT access these APIs.**
Procedure to allow Kickle to use these services is detailed here:

http://support.kickle.com/support/solutions/articles/8000073000-configuring-and-administering-kickle

2.5 Local configuration file

Configuration of each Kickle is stored on a local file. The Skype for Business and Exchange account password is encrypted.

2.6 Cloud platform storage

Configuration of each Kickle is also stored on the Cloud platform (http://portal.kickle.com).
Passwords are not stored on the Cloud platform unless you want to configure an offline Kickle. In this specific case, the password is temporary stored and encrypted. Once the Kickle is back online, the stored password is deleted from the cloud platform.
Cloud platform is based on Windows Azure, using https and authentication.
From December 17th, authentication to the Cloud Platform will be based on Office 365.

2.7 Remote access

Kickle offers remote access for technical support, based on Microsoft Quick Assist: https://support.microsoft.com/en-us/help/20534/windows-10-quick-assist-faq
To allow the remote assistance, it is necessary that someone be in front of the Kickle screen and explicitly initiate the remote assistance procedure. A new code is generated for each new remote assistance session.

3 Windows 10 IoT Enterprise

Windows 10 IoT Enterprise is a full version of Windows 10 that delivers enterprise manageability and security to IoT solutions. Windows 10 IoT Enterprise shares all the benefits of the worldwide Windows ecosystem. It is a binary equivalent to Windows 10 Enterprise, so you can use the same familiar development and management tools as client PCs and laptops. However, when it comes to licensing and distribution, the desktop version and IoT versions differ.

Although the Windows UI is not visible (Kiosk Mode), it can be maintained like any other Windows 10 device (including GPO/AD/Intune etc). For all security settings you will need to enter the Admin Mode (via the Kickle UI, admin login).

3.1 Active Directory

With respect to your IT policies, you wish to join 2Meet/Kickle to the Active Directory. By default, 2Meet/Kickle can be found in Workgroup and is configured with two accounts:

- Kickle: which is the account configured for auto login. It's a simple user.
- Administrator: the default local Windows 10 Administrator.

You can join Kickle either to your local AD or Azure AD. We recommend setting Kickle to a specific OU and blocking inheritance (to avoid deactivation of the local admin account, or configure specific settings for local users).

Useful info for GPO:

Kickle is set up with a local GPO to configure certain settings:

- Computer :
  - Set PowerShell script "execution mode"
  - Power settings to avoid hibernation and sleep mode
  - OneDrive and Cortana are disabled by default
  - Store is disabled
  - Windows Update : Updates are configured by local GPO
  - Explorer : Local Disks are hidden and default shares are disabled

Auto login is not configured by GPO. The keys are added directly to the registry. The above settings are not mandatory but are recommended for a good experience using Kickle.

Procedure to allow Kickle to join AD is detailed here: http://support.kickle.com/support/solutions/articles/8000073118-how-to-join-kickle-to-active-directory-or-azure-active-directory

3.2 Windows Updates

Refer to this article to know more about the Windows Updates settings applied to your Kickle: http://support.kickleforskype.com/support/solutions/articles/8000065990-configuring-windows-updates-and-default-settings

- Feature updates and Quality updates are automatically installed.
- Kickle uses the "semi-annual channel" for the updates.
- Preview build or Feature update deferring: 0 days.
- Quality update deferring: 30 days.

Windows updates are installed every Sunday at 3:00 am.

3.3 Windows Defender

Windows defender is activated by default. There's no specific setting. You're free to set Windows Defender as you need, or disable it and use your own tools.

3.4 Windows Firewall

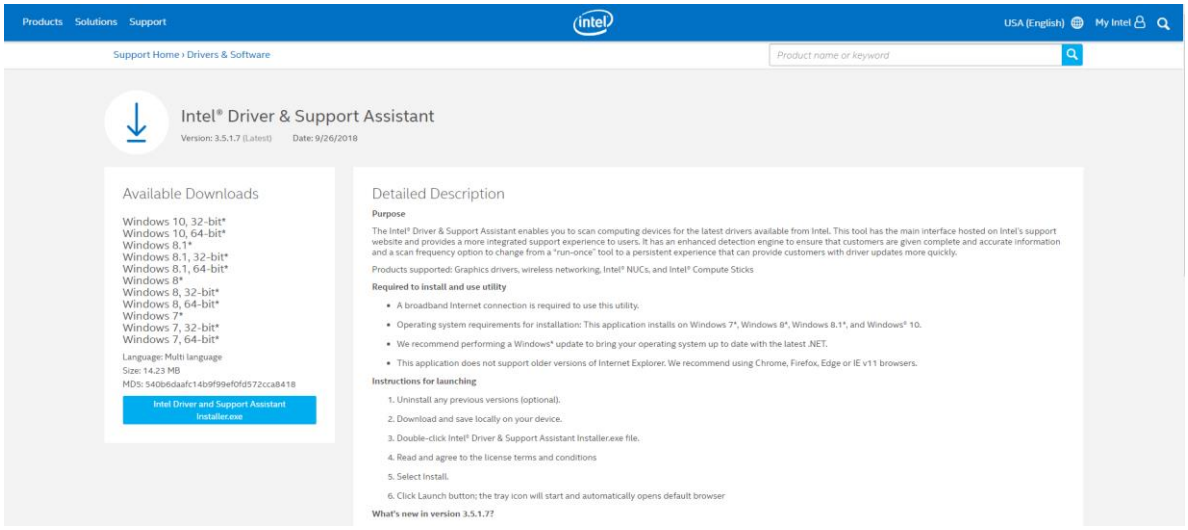
Windows Firewall is activated by default. Virus definitions are automatically updated. Real time protection and periodic scans are not activated.
You're free to set Windows Firewall as you need, or disable it and use your own tools.

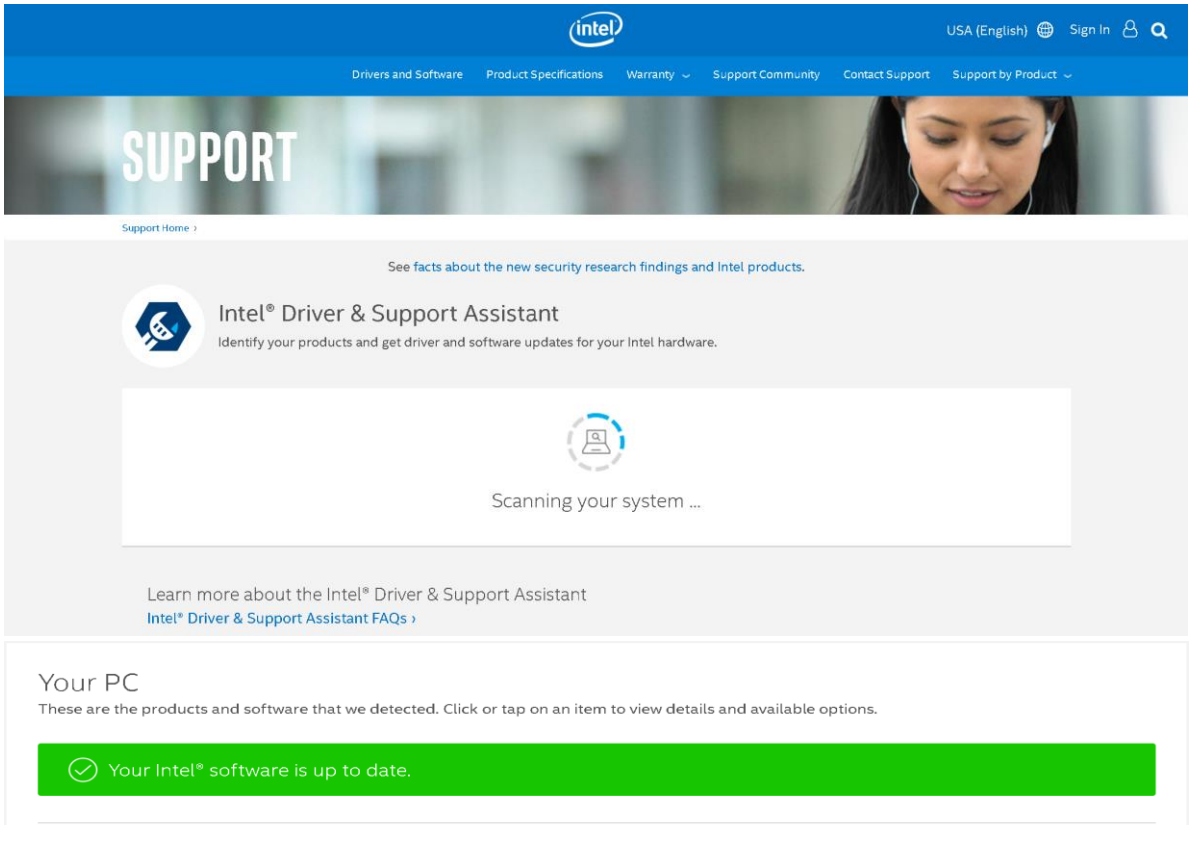
4 Intel® Next Unit of Computing (NUC)

Intel® NUC is used to run the Kickle Application (together with Windows 10 Enterprise).

4.1 Intel® Driver and Support Assistant

Security patches on hardware level can be found on the support website of Intel. It is highly recommended to use the Intel® Driver and Support Assistant to keep up to date on the latest security patches as well as the latest Windows drivers:





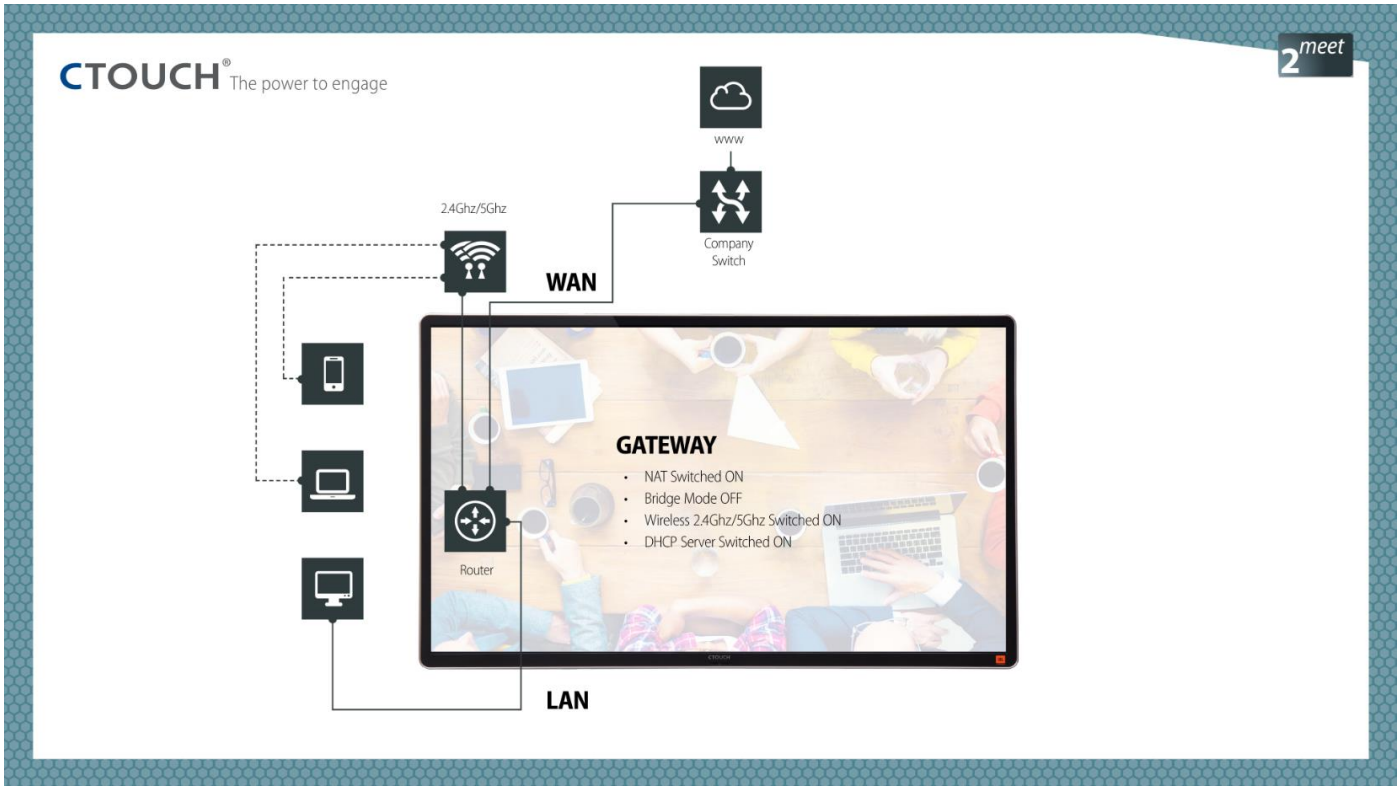
5 CTOUCH Router

The Leddura 2Meet has a build-in router with two Access Points (2.4 & 5GHz) to end users where no wireless network is available.

5.1 Gateway Mode

The router should be connected via the WAN to the corporate LAN where the corporate DCHP server should assign a WAN IP to the router. All devices connected to the LAN side of the router, will get a local IP address in the range 192.168.123.x (standard mode router)

Gateway mode router:

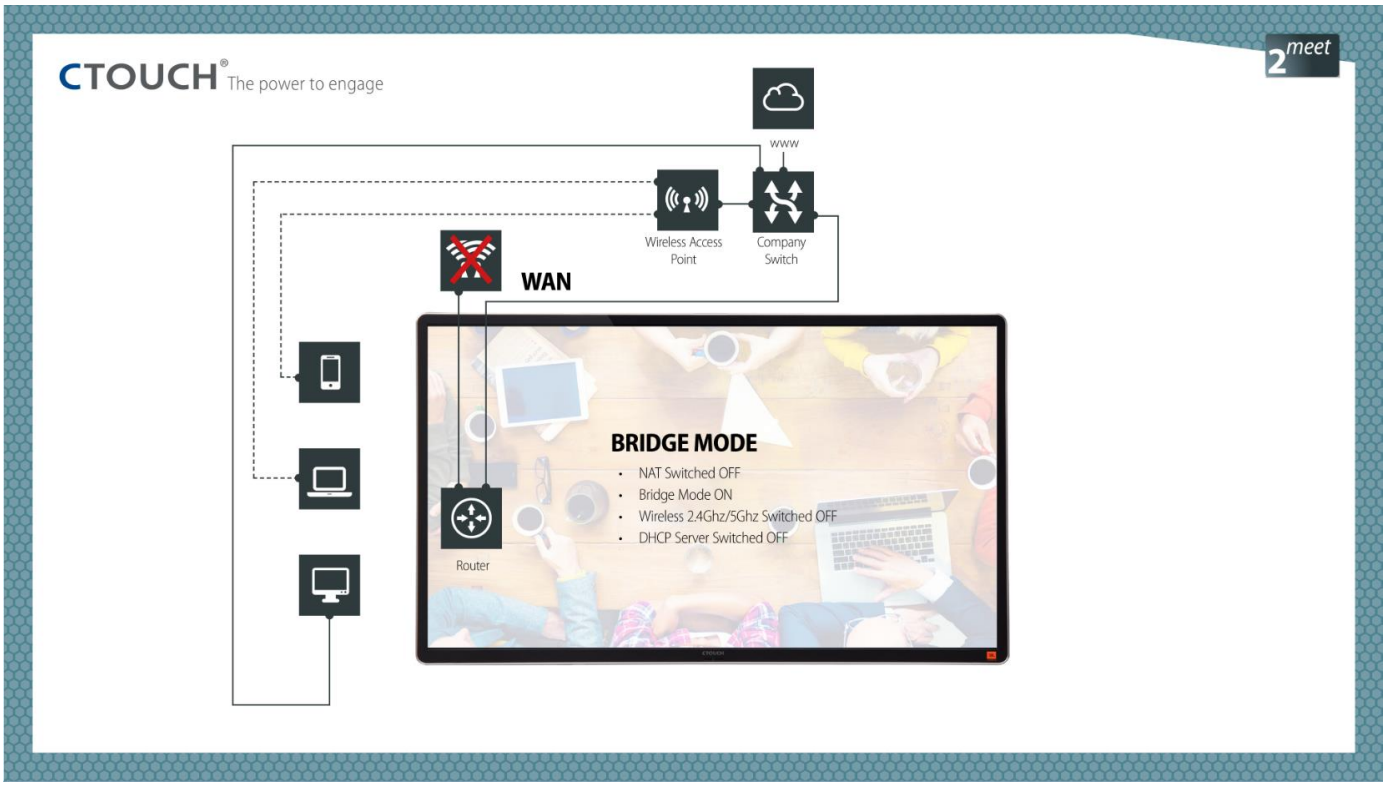


5.2 Bridge Mode

In most corporate environments, the router function is not required as wireless connection is routed already via the corporate network. Also for security reasons is this setup in most cased selected to be able to monitored and secure that data path.

The router mode can be set to Bridge where the Intel NUC will get directly an IP address assigned by the corporate DHCP server.

Bridge Mode router:



5.3 Firmware

New firmwares (in case needed) will be published (including release notes) on the CTOUCH Help Center: http://support.ctouch.eu

6 CTOUCH Touch Screen

The touch screen exists of 2 main parts:

- Touch screen
- Mainboard

6.1 Mainboard

The Leddura 2Meet transfers the touch via the touch screen via USB to the Windows 10 Environment (seen as HID device). Furthermore, the screen provides the possibility to switch sources (HDMI, VGA etc.) and provides sound via the build in JBL speakers. The mainboard with the Embedded OS is providing this functionality. Only in case the build in timer is needed, the mainboard should be able to access the NTP server to sync time. With the router in Gateway mode, this is automatically arranged but when the router is in Bridge Mode, the mainboard will need an IP address from the corporate DHCP server to be able to access the NTP server