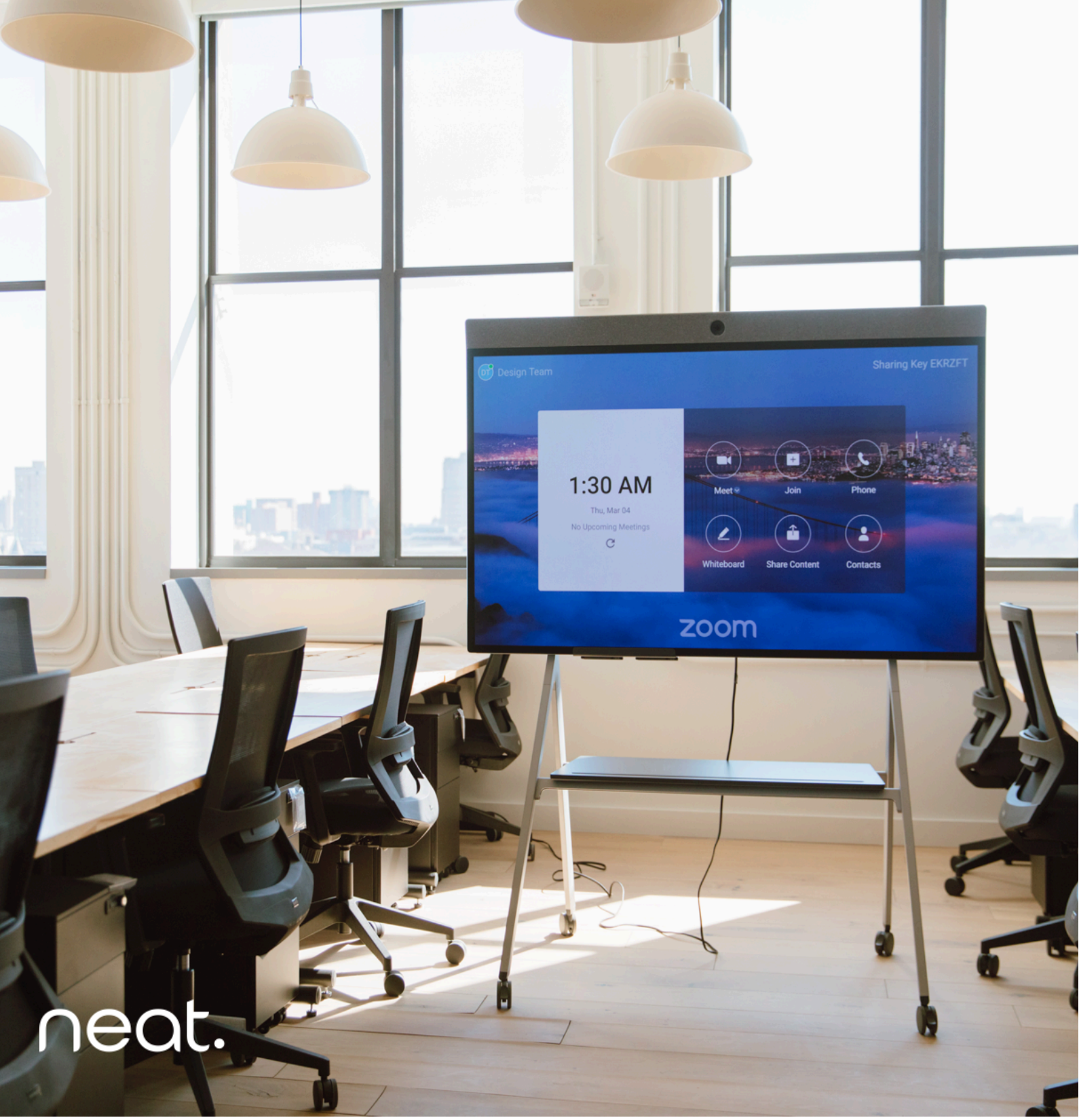


Technical Security Specifications

Version 4.2 - August 2024

1. Revision history

Date	Author	Version	Changes made
January 26, 2021	Bart Jan Voskamp	0.9	Initial draft for first external review
February 12, 2021	Bart Jan Voskamp	1.0	Final version
April 26, 2021	Spencer Wise	1.1	Updates regarding TLS version support on ota.neat.no
Aug 24, 2021	Bart Jan Voskamp	1.2	Android update
Feb 5, 2022	Bart Jan Voskamp	2.0	Microsoft added
April 22, 2022	Bart Jan Voskamp	2.1	Refined version with Microsoft
August 08, 2022	Bart Jan Voskamp	2.2	USB passthrough updates
August 19, 2022	Bart Jan Voskamp, Alexis Bouton	2.3	Release cycle updates
December 13, 2022	Steve Odegaard	2.4	Added section for data analytics / metrics (section 5.9)
January 23, 2023	Bart Jan Voskamp	2.5	Included Neat Pulse, Neat Board pairing
November 23, 2023	Bart Jan Voskamp	3.0	Included Neat Pulse and new releases
February 2024	Bart Jan Voskamp, Steve Odegaard	4.0	Software architecture, Software release cycles, Network requirements
April 2024	Bart Jan Voskamp	4.1	Included Bar 2
August 2024	Steve Odegaard	4.2	Updated section 5.7 Data Storage

2. Table of Contents

3. Disclaimer

This document is created and maintained by NEAT (also known as NEATFRAME) and is under full control of NEAT. The specifications and information regarding the products and services in this document are subject to change without notice. All statements, information and recommendations in this document are believed to be accurate but are presented without warranty of any kind, express or implied. This document is not an agreement and in no event will NEAT be liable for lost profits or loss of business or for any consequential, indirect, special, incidental or punitive damages arising out of or related to this document. This document is intended for NEAT's partners and NDA customers only and not to be distributed without explicit permission from NEAT.

4. Introduction

This whitepaper aims to provide all relevant technical details which have an impact on the security of Neat products. It contains details of the architecture, physical aspects and software aspects of Neat devices.

The information in this document is based on the architecture, features and functionality of the current generally available stable software (Neat devices with normal auto-updated software). Some of the information in this document may be changed, updated or removed in subsequent versions to keep in sync with new features/functionalities in newer releases.

Scope: All the information in this guide is related to Neat Pad, Neat Bar, Neat Bar 2, Neat Board, Neat Board 50, Neat Bar Pro, Neat Center and Neat Frame. The words 'devices', 'products', 'hardware' and 'unit' refer to these devices only.

5. Neat software Architecture

Neat devices are based on an Android operating system. The following APKs can run on top of this, depending on the configuration:

- The platform APK (Microsoft or Zoom)
- The Neat system settings APK
- The Neat Pulse agent APK

This chapter describes these aspects in more detail.

5.1. Android Open Source Project

Neat uses a subset of the full Android Open Source Project (AOSP). Many changes to this AOSP have been made, from kernel modification to removal of unused services. All modifications are aimed at optimizing the software for its task of being a collaboration device, and to lock the unit down.

Neat software does not adhere to Android compatibility standards for OEMs. This also isn't needed, since no standard Android applications like Google Play store are used and no Google certification is needed.

See the Android versions of the devices below

- Neat Pad - Android 10
- Neat Bar - Android 10
- Neat Bar Pro - Android 10
- Neat Board - Android 10
- Neat Board 50 - Android 10
- Neat Frame - Android 10
- Neat Center - Android 13

Locked down

The Neat Android operating system is fully locked down and is not comparable to Android on a phone handset. Neat doesn't make use of Android Kiosk mode, but uses a subset of the AOSP to prevent doing anything else outside the use of the provided platform app (Microsoft Teams Room or Zoom Room). Neat doesn't support any applications other than these platform apps. No other applications can be installed.

There is no keypress or touch-control combination which allows to break out or open up Android controls.

No mechanisms to load other software

One part of securing the Neat device is ensuring no other applications can be loaded.

This is done by Neat owning the operating system, and the ability of Neat software to control what can be installed. No other apps like Google Play are allowed to install apps.

APIs

Neat devices do have APIs built in. These APIs however are only available for the Microsoft/Zoom APKs and other Neat devices/administrators (see 5.4 Web API). There are no public APIs available for the devices.

5.2. The platform APK

Platform vendors provide the relevant APKs to Neat. Neat includes these software APKs in its total software package and tests them thoroughly before this is released to the customer (see 6.1 Release Cycle).

Neat has no access to the source code of this software. The platform app providers are responsible for these packages, and any security concerns towards these APKs should be addressed to them.

The platform APK is signed with the key of the platform provider, which is verified by the operating system. This is the same mechanism Google Play Store uses to verify that a 3rd party developer can upload a new version of an application.

The Neat operating system only trusts properly signed APKs of the supported platforms.

The firmware image is secured by SecureBoot and Android Verified Boot including OTA upgrade signatures.

5.3. Neat system settings

Neat System settings is an APK which contains the interface to view and change device specific settings.

The Neat System settings app can be launched physically from the Zoom or Microsoft application running on the Neat device. Physical access is required during the initial OOB (Out Of Box) device setup; however, after the initial setup, Neat system settings can be managed by Neat's device management platform, Neat Pulse (See 5.4. The Neat Pulse APK).

System Settings access from Zoom app

The access to Neat System Settings is protected by a pin code. The configuration of this pin code can be set in the Zoom admin portal. The policy of this pin code is part of the Zoom platform and outside of Neats responsibility.

Since the pin code resides in the Zoom app, which gets the actual code from its cloud (management setting), a factory reset of the Neat device has no effect on this pincode.

System Settings access from Microsoft app

In Microsoft, most of the Neat system settings are behind the admin access level. To get to these settings, a person should login with administrator credentials.

- The initial password is the last six characters of the serial number
- Once the password is manually changed in the admin settings, then this is the password

The full menu of settings is specified in a separate document 'Neat Technical Details'.

5.4. The Neat Pulse APK

Neat Pulse is the management cloud of Neat. From this cloud platform, Neat devices can be managed remotely. This is disabled by default. Enrolling in Neat Pulse can be done locally from the Neat device itself. Physical access to the Neat device + access to the administrator settings is required to enroll the device to this cloud.

When the device is enrolled to Neat cloud, the Neat Pulse APK will be installed. The Neat Pulse APK will be running in the background, maintaining the connection between the Neat device and Neat Cloud.

When the Neat device is reset, this Neat Pulse APK is removed from the device.

5.5. Web API

Neat devices are equipped with a web API. The web API is used in 2 ways:

- Administrators doing remote management through a web browser

- Neat Pads controlling/configuring Neat Bar, Neat Bar Pro or Neat Board

Having one API for both controllers and remote management also enables Neat to have one point of authentication using a JSON Web Token (JWT). JWT is a token generated for a particular user with some traits which can be used as access control. Towards the future Neat is planning to use this as access control for different kinds of users. At this moment, there is one level of access.

Authentication For administrators

For administrators wanting to access the web interface, the web API server generates a JWT when a user is authenticated. Authentication is done by means of username/password:

- user: "admin"
- password: <specified in SystemSettings>

When remote access is disabled. The server will not provision/generate JWT.

Authentication for Neat Pad with Neat Bar or Neat Bar Pro

At first time pairing of Neat Pad with Neat Bar, Neat Bar Pro, the web API server generates a JWT based on a password-less authentication. For this to work, the following requirements have to be met:

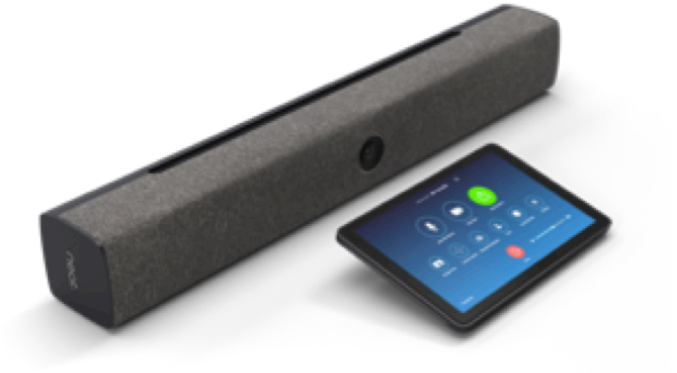
- All devices involved must be on a fresh install (out of box, or after a reset)
- Neat Pad and Neat Bar must be in the same subnet to work together
- The administrator manually selects the right serial from the list of available endpoints to pair with (usually 1, but multiple can be listed)

The JWT token for the Pad is valid for the lifetime of the Neat product. So after a reboot, the Neat Pad will be able to pair automatically with the Neat Bar

Authentication for Neat Pad with Neat Board

Authentication of a Neat Pad with a Neat Board will have the same requirements as for Neat Bar and Bar Pro, however as the Board is configured without the Pad, the situation is little different.

As the Neat Board is already configured standalone, the administrator needs to go into the Neat system settings of the Neat Board, and tap 'pairing'. Then the Neat Board is discoverable for the Pad to pair.



5.6. Remote access

Neat devices have a remote access possibility by means of a web interface. The Web interface is used to remotely configure and troubleshoot the Neat device.
In system settings (see 5.3 Neat system settings), external access to the web interface can be enabled, and an administrator password can be set. By default, this external access is disabled. Having the external access disabled, will prevent the web API server to provision/generate a JSON Web token for the user and will block the login.

To create the web interface on Neat devices, a web framework of which Neat has full control. No Apache is present and no modules are used. The web interface itself is a progressive Web application using javascript to access the underlying Web API.

Remote access security

From the web interface, the password can be changed for this remote access. Also the ability to change the password from the Pad can be disabled. This prevents people locally to disable the remote access, or change the password.

Also there is an account lockout after 5 failed attempts for 5 minutes. After 5 attempts to log in with the wrong password, a timeout of 5 minutes will be applied before the user can attempt to login again. After the timeout expires, users will have 5 more attempts before another timeout is applied.

Log file distribution and encryption

Log files can be generated via the Web interface. This generates an encrypted file which is automatically downloaded, to be sent to support@neat.no. The extension of this file is 'p7m'.

Neat log files are encrypted according to the
https://en.wikipedia.org/wiki/Cryptographic_Message_Syntax standard.

The log file is encrypted using a randomly generated symmetric AES-256-CBC key. This key is then encrypted asymmetrically inside the Neat product using two different 4096-bit RSA public keys, for which Neat exclusively holds both the private keys.

5.7. Data storage

Neat devices have storage. This storage is soldered to the PCB and is therefore non-removable. The user data storage (e.g., System Settings, Microsoft Teams or Zoom Room token, etc.) is fully encrypted using FBE (File Based Encryption) or Full Disk Encryption (FDE), depending upon the device model.

- Neat Bar, Neat Pad and Neat Board use Full Disk Encryption (FDE) with AES-128 ciphers

- Neat Bar 2, Neat Bar Pro, Neat Board 50, Neat Frame, and Neat Center use File Based Encryption (FBE) with AES-256 ciphers
- All keys and certificates on the device are stored encrypted in the device's hardware-based keystore

All data which is sent out from the device is encrypted using security best practices (e.g., TLS 1.2+). Also note that Neat devices do not store personal information.

5.8. Booting process

Neat devices make use of the Android secure boot and Android verified boot process. Tampering mechanisms in place are also part of this Android secure boot. On top of that, there is no possibility to load anything onto the device.

Boot level recovery

Neat is working with an A/B partition system (see 6.3 Software distribution). If the boot of a device fails completely, there is one recovery method to switch back to the old partition again: rebooting the Neat Device 5 times will trigger an emergency slot, which makes the Neat device switch to the other partition to boot from. Rebooting is easiest done by powering off the device, wait 5 seconds, then connect back again and wait approximately 30 seconds (to see if it boots) before powering down again. Repeat this at least 5 times.

5.9. Data Analytics / Metrics

Neat collects system information and sends this data as part of the user agent string in secure web requests to *ota.neat.no*.

The following categories of data are collected and transferred:

- Firmware channel
- Pairing information
- App provider
- Audio settings
- Serial number
- Build number
- Locale (language + country)
- Device up-time

6. Software release cycles, patching and distribution

6.1. Release Cycle

Neat has approximately a bi-monthly release cycle. If emergency patches are required, then hotfixes can be made and verified before the new production (stable) software is provided to customers.

The process for a software release starts with the build selection by Neat R&D.

Subsequently, the Neat firmware is tested against the currently available platform application versions (MS Teams and Zoom applications).

After the tests are successful, the software is shared in our preview channel with customers and partners for exploration and testing. At this point in time, release notes are finished and shared with the customers and partners as well.

If no major issues come to surface, then this release is deployed in the stable channel two weeks later over the weekend.

Microsoft and Zoom have their own release cycles and methods of updating their software (see 6.3. Software distribution. Each new software is tested with the current Neat firmware release.

Neat releases and Microsoft

For devices running Microsoft Teams, the updates are controlled from Microsoft Teams Admin Center(TAC). This usually consists of a manual update.

Neat releases and Zoom

For devices running Zoom: both Neat and Zoom have approximately bi-monthly updates. Neat aims to be validated with the newest release of Zoom software with each new release. This depends if the newest version of software is on time for Neats cutoff for the release (build selection). If required, Neat can also push an individual Zoom software update, without updating the Neat Firmware

So in best case, Neat releases a particular Zoom software release 2 weeks later than Zoom release date. In other cases, it can be a few weeks more.

Individual app updates

Neat is also capable of updating individual platform applications without new Neat firmware. This allows it to deliver platform functionality quickly to the market. In this case the same software release cycle is followed

6.2. Vulnerability patching

Neat closely monitors any security changes or patches required for Android. Any necessary security patches are applied when needed. Security fixes or patches are detailed in our release notes. Release notes can be found at https://support.neat.no.

Penetration tests

Neat works with third-party security consulting companies to perform penetration testing on our hardware, to identify any hardware or software vulnerabilities. As security findings are discovered, they are patched/secured immediately and tests are performed again to verify remediation success.

Neat also has the ability to perform an immediate forced firmware upgrade of the devices if a critical security vulnerability is revealed (e.g. zero-day vulnerability). Devices are required to have their firmware upgrades set to “automatic.”

6.3. Software distribution

Neat devices can subscribe to different software channels. By default, all devices are set to auto update themselves. In doing so, two software channels are available: ‘Stable’ and ‘Preview’. Auto updates can also be turned off to have the update manually initiated from the platform provider. For more information on software channels, see the ‘Neat Technical details’ document

All endpoints (with auto updates enabled) check every hour for new software at https://ota.neat.no. TLS versions 1.2 and 1.3 are allowed in order to connect to ota.neat.no.

If there is new software available, then it is downloaded and held on a memory partition of the Neat device dedicated to storing software updates.

Downloading the software image is done by means of regular HTTPS traffic. The useragent of the Neat device sends its serial number and current sw version to ota.neat.no when requesting for possible new software.

After the OTA upgrade package is downloaded, the signature is validated before the upgrade is started. This means only Neat built and signed OTA upgrades can be installed.

On top of this there are Android Secure Boot and Android Verified Boot mechanisms when the firmware/operating system boots and runs.

As from the June 2023 software release, downgrading is not possible anymore. So if a device is put on Preview channel to see a newer version, reverting back to the n-1 software by means of selecting ‘Stable’ again won’t work. You can still select Stable channel, though it will follow the stable release once the firmware build available in the Stable channel is newer than the current firmware.

6.3.1. Microsoft software distribution

When the unit is configured for Microsoft, only the Neat firmware is distributed via the method above. The total package of firmware consists of:

- The full Android Operating system
- Neat system settings software.

Microsoft software is always distributed via Microsoft TAC.

6.3.2. Zoom software distribution

When the unit is configured for Zoom, both Neat firmware and Zoom software is distributed via the method above. The total package of firmware consists of:

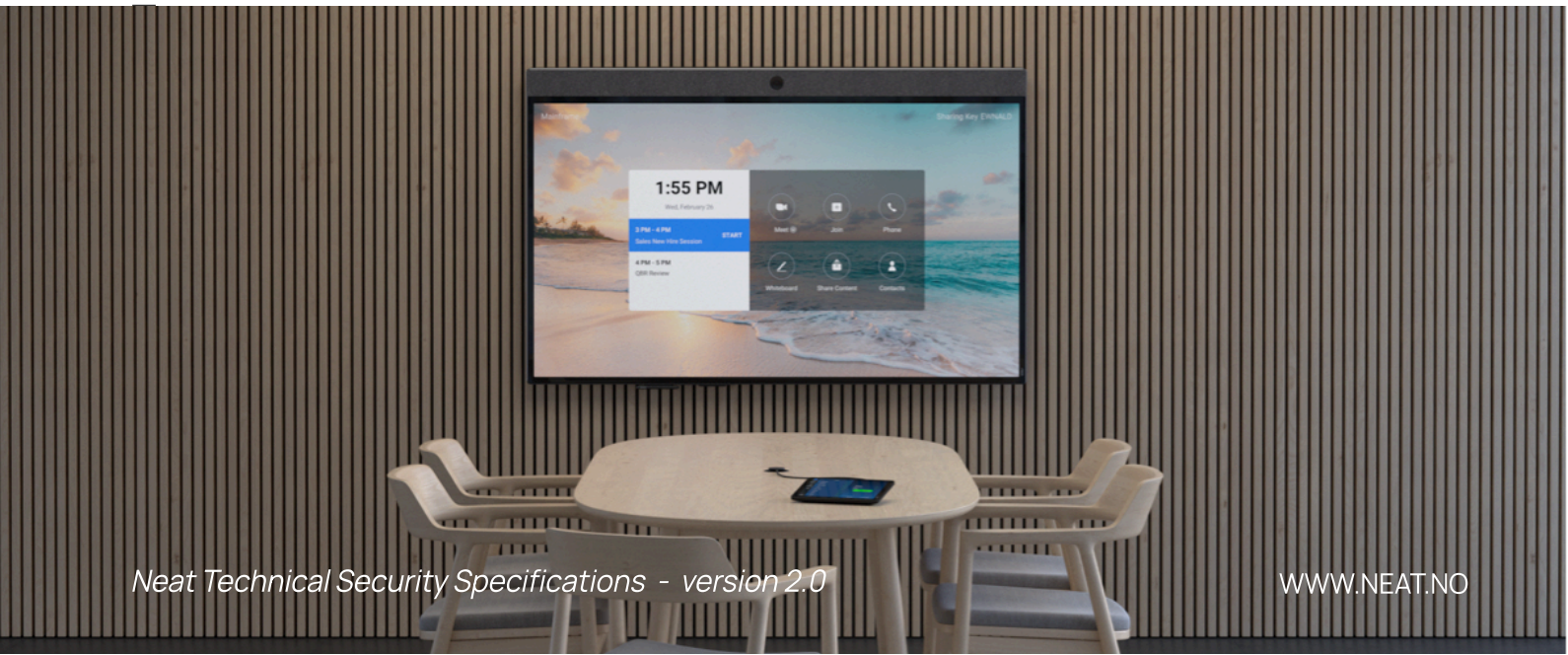
- The full Android Operating system
- Zoom Rooms software
- Neat system settings software.

The total download size for all components is typically around 1 GB.

6.4 Update mechanism

Neat devices work with dual storage partitions on the memory (ie A and B). If Neat Bar is operating from partition A, then the software will be installed on partition B. This installation is done during normal operation of the device.

At the start of the Boot process of the Neat device, it checks if there is a newer software load on the other partition. If there is, then it will boot from this other partition and the upgrade effectively is 'done'.
Apart from restart moment, also at 2hr at night (local time), Neat device checks if there is newer software available on the other partition. If yes, it will reboot.



Network aspects of Neat devices

7.1. Requirements

The network requirements of Neat devices consists of 2 parts, the Neat requirements and the Microsoft Teams/Zoom Room requirements. This chapter handles the Neat requirements.

The Microsoft requirements can be found here:
https://docs.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide#skype-for-business-online-and-microsoft-teams

The Zoom Room requirements can be found at the two links below:
https://support.zoom.us/hc/en-us/articles/203680389-Firewall-Configuration-for-Zoom-Rooms

https://support.zoom.us/hc/en-us/articles/201362683-Network-firewall-or-proxy-server-settings-for-Zoom

Same subnet (for paired Neat devices)

Some Neat devices can pair with each other:

- Neat Pad with Neat Bar, Neat Bar 2, Neat Bar Pro, Neat Board, Neat Board 50
- Neat Center with Neat Bar, Neat Bar 2, Neat Bar Pro, Neat Board or Neat Board 50

For the pairing, the Neat system uses multicast for initial setup and to maintain pairing during ongoing operations. Therefore in order to set up the Neat Bar and Pad, it is required to have both devices in the same subnet, so they can discover and communicate with each other.

Pairing devices find each other using mDNS, which is a multicast message that happens at layer 2; so the Pairing devices are required to be in the same multicast domain (i.e. at layer 2, same VLAN and if the network is NOT using VLANs, then same subnet).

For systems running software older than Jan 2022, TCP ports 46000 and 46001 are used for initial discovery. As Neat devices can pair backwards compatible, these ports are still open to be used in current software

Devices with software load newer than Jan 2022 will use encrypted web traffic (TCP port 443) for setup and communication.

mDNS/multicast messages are used to maintain system pairing on the Neat level. On the App level, the requirements are different.

- No local communication is needed for Microsoft to operate.
- Zoom apps need maintaining communication, done over TCP port 9090.

7.2. Neat Firewall settings

For the latest and most up to date information regarding network and firewall requirements for both Neat devices and Neat Pulse, please visit the following support page.

Network and firewall requirements for Neat - Neat Support

7.3. Proxy

Neat devices support the use of a proxy server without authentication. This proxy is configured at the Neat device level (not the Microsoft/Zoom app level).

Proxy can be configured in two ways:

- Configuring the address of the proxy server manually,
- Using a Proxy Auto Configuration (PAC) file.

From 2021 Feb 18, Neat devices support SSL interception proxy. Security certificates required for this can be uploaded via the web interface.

Neat Center does not support Proxy at this stage

7.4. 802.1x

Neat devices support 802.1x. 802.1x is a standard network authentication protocol that enables port-based access control based on the user's identity and its authentication by the organization's internal authenticator. This offers security within the network to protect organizations from unmanaged devices that find themselves in the workplace.

Neat Center does not support 802.1x at this stage

7.4.1. SCEP (beta)

From the June 2023 firmware, Neat devices support the Simple Certificate Enrollment Protocol (SCEP).SCEP is now supported while setting up Neat devices with 802.1x Wifi network security configurations. SCEP allows for automatic certificate issuing and renewal in a scalable way, and this update will make it easier to roll out a large number of Neat devices with 802.1x configurations.

Neat supports SCEP using EAP-TLS only

More information about setting up 802.1x with SCEP can be found in the following support article: https://support.neat.no/article/how-to-set-up-802-1x-using-scep-on-neat-devices-beta/

7.5. Audio and video traffic between Neat devices

With the introduction of Neat Center, Neat has audio and video traffic flowing between Neat devices.

Audio/ video encryption/data protection

Media is transmitted over Secure Real-Time Transport Protocol (SRTP) and encrypted with the Advanced Encryption Standard (AES-256) in Galois/Counter Mode (GCM). The authentication tag in GCM mode is 8 octets long, often referred to as AEAD_AES_256_GCM_8.

8. Hardware interfaces

In the table below, all hardware interfaces of the Neat devices are shown:

	Neat Pad	Neat Bar/ Neat Bar 2	Neat Board	Neat Bar Pro	Neat Frame	Neat Board 50	Neat Center
Power	-	1 x	1 x	1 x	1 x	1 x	-
Network interface	1 x	1 x	1 x	2 x	-	1 x	1 x
HDMI input	-	1 x	2 x	1 x	-	1 x	-
HDMI output	-	2 x	-	3 x	-	1 x	-
USB-C	1 x	1 x	1 x	1 x	1 x	1 x	1 x
Reset button	1 x	1 x	1 x	1 x	1 x	1 x	1 x
4-pin mini-jack	-	-	-	-	1 x	-	-

Below we will discuss the interfaces which are relevant to security.

8.1. Ethernet interface

The Network interface exists to allow for wired network connections. Neat devices only allow outgoing traffic, apart from TCP ports listed below. These ports are used by paired devices and the web interface.

These ports will always accept TCP connections, however authentication is required before accepting any commands over these ports. Authentication is detailed below:

Incoming TCP Port	**What is it**	**Method of authentication**
80	Redirect to port 443	
443	Https traffic	JWT token
9090	ZR Controller to ZR. See https://support.zoom.us/hc/en-us/articles/203680389-Firewall-Configuration-for-Zoom-Rooms for more info	See Zoom
46000	Neat legacy port -Active for backwards compatibility	None
46001	Neat legacy port -Active for backwards compatibility	None

8.2. Wi-Fi interface

For all Neat devices apart from Neat Frame, The Wifi interface is by default disabled. It can be enabled via Neat System settings to connect the Neat device via Wi-Fi to the network. See 5.3 Neat system settings for more info on the security of these settings.

The access to the ports for this interface are equal to the ones described above at 'Ethernet interface'.

8.3. Bluetooth

Neat devices do have a bluetooth interface. When the Neat device is configured in USB mode or Zoom device, this interface is disabled. If the unit is configured for Microsoft then, the bluetooth is on by default. This is used by the Microsoft app to detect if users are in proximity of the device.

Neat Frame can have Bluetooth enabled both in Zoom and Microsoft, to allow for Bluetooth headset to be connected.

8.4. HDMI input/output

HDMI connections are used for sending/receiving screen content. The HDMI connections support Consumer Electronics Support to control the wake up and sleep of connected screens. Other functions of CEC are disabled.

8.5. USB-C

For the Neat Pad, USB-C is not used and disabled at this moment. On Neat Bar, Bar Pro and Neat Board, USB-C has the following functions:

Connecting Human Interface Devices (HID)

This is used to connect the output of a touch-enabled display into the Neat Bar, which allows the Platform app to be controlled via touch and to allow for example for white-boarding functionality.

As by nature of HID, any device supporting HID like a keyboard and mouse can be connected. The Neat device is locked down in such a way that no commands can be given to the application other than characters can be entered by keyboard where this is allowed in the GUI. An example is the URL of a proxy server in system settings. Nb: the regular way to enter information is via the on screen keyboard of the connected touch panel.

No authentication information is passed along this connection. A keyboard is never required to configure the Neat device. In some rare cases when installing Neat Bar as Microsoft MTR, a mouse might need to be connected to the USB port.

BYOD Mode (beta)

Neat Bar, Neat Bar Pro and Neat Board have a BYOD mode. This allows the high quality components to be used instead of lower quality PC hardware. This is equivalent to a webcam and speakers being connected over USB.

The data streams are:

- Video from Neat device to connected computer (webcam)
- Audio from Neat device to connected computer (microphone)
- Audio from connected computer to Neat device (speaker)
- HID from Neat Board to connected Windows based computer (touch screen)

Display Port

Neat Bar 2 and Neat Board 50 are equipped with a Display Port chip. This allows it to send content to the these devices like a monitor is connected to a laptop via USB-C. As this is technically different from regular USB (but uses the same cable), it is mentioned here separately.

8.6. Reset button

The reset button consists of a microswitch on the Neat device. This is used to system reset the Neat device (by pressing it for more than 7 seconds). By performing this action, the software will stay as-is. It will not revert to the version as loaded in the factory during production. All settings will be erased and the system will be ready as if it is a fresh installation.

9. Acronyms used

AOSP	Android Open Source Project
APK	Android Application package
API	Application Programming Interface
CEC	Consumer Electronics Control)
GUI	Graphical user interface
HID	Human Interface Device
HDCP	High-bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface
JWT	JSON Web Token
LAN	Local Area Network
OTA	Over The Air
PAC	Proxy Auto-Configuration
PCB	Printed circuit board
POE	Power over Ethernet
SOC	System on a Chip
SSID	Service Set IDentifier, usually a name of a Wi-Fi network
TAC	Teams Admin Center
TPM	Trusted Platform Module
ZDM	Zoom Device Management
ZR	Zoom Room
ZRT	Zoom Room Touch

10. Important resources

Our website also provides some frequently asked questions, both on technical and non-technical topics.

Neat support page

This contains FAQ, documents and other resources: https://support.neat.no/

Neat Technical Details document

Contact your Neat Product specialist for this document

Warranty statement

For the most up-to-date Warranty statement, please visit our website: https://neat.no/warranty-statement/

Neat Privacy Policy

For the most up-to-date Privacy Policy, please visit our website: https://neat.no/privacy-policy/

For general queries or sales, you can also talk to one of our team members over chat by visiting our website www.neat.no.