Updated 2026-11-11

AbittiCandidate Application for ChromeOS - Documentation for School IT Administration

For a quick start, see Installation.

Table of Contents

- The purpose of AbittiCandidate application
- How the application works
- Installation
  - Pinning a specific version
- Technical monitoring
  - Why technical monitoring exists
  - What technical monitoring observes
  - Implementation
  - How monitoring reacts and appears in different situations
- Closing remarks

The purpose of AbittiCandidate application

Abitti 2 works in a client-server model. The server provides an HTML5 desktop with the test and the applications the candidate can use during the test. The client (AbittiCandidate) consists of two parts:

- **Kiosk app.** The candidate application is a progressive web app that runs in ChromeOS kiosk mode. The Google Admin console configuration locks the candidate into the app, so that they can only access the test and its materials.
- **Extension.** A companion extension lets the app talk to the operating system. It is needed for monitoring and for OS-specific features such as volume control.

How the application works

The candidate uses the AbittiCandidate application as follows:

1. The candidate signs out from their own user account.
2. At the bottom of the sign-in screen, the candidate clicks Apps and selects Abitti2. This starts the AbittiCandidate application as well as the technical monitoring.
3. When the candidate has participated to the test, they exit from the AbittiCandidate application.
4. When the AbittiCandidate application exits for any reason, the candidate is taken back to the sign-in screen.

Installation

A Google Workspace administrator can install the application as a kiosk app by following these steps:

1. Add the Kiosk by URL

Navigate to Google Workspace Admin Console at https://admin.google.com/. Go to **Devices** > **Chrome** > **Apps & Extensions** > **Kiosks**, click the + icon and add by URL:

```
https://chromeos.abitti.fi/index.html
```

2. Add the Extension

Click **Add extension** > **Add from a custom URL** from the sidepanel. Enter the following details.

Extension ID:

```
ednjaikaedogelbafimghlbnilijpnpf
```

URL:

```
https://chromeos.abitti.fi/extension/update.xml
```

The aforementioned URLs always serve the latest AbittiCandidate version, so the kiosk and the extension update automatically.

Pinning a specific version

Most installations should use the URLs above and stay on the latest version. If you do need to keep a kiosk on a specific version, follow the same steps but use versioned URLs. The extension ID stays the same.

An example versioned kiosk URL (for version 1.2.3):

```
https://chromeos.abitti.fi/versions/chromeos-v1.2.3/index.html
```

An example versioned extension URL (for version 1.2.3):

```
https://chromeos.abitti.fi/versions/chromeos-v1.2.3/extension/update.xml
```

Configure Chromebooks for Abitti

After installing the Abitti kiosk app and companion extension, complete the settings below in Google Admin and Tutkintopalvelu.

1. Configure Google Admin

The Google administrator configures the organizational unit containing the exam Chromebooks:

1. Open Google Admin → **Devices → Chrome → Settings → Device settings** and select the relevant organizational unit.
2. Under **Verified mode**, select **Require verified mode boot for verified access**.
3. Add this YTL service-account address to **Services with full access**, preserving existing entries:

   ```
   sayo-va-production@abitti2-508212.iam.gserviceaccount.com
   ```

4. Click **Save** to save the device settings.
5. Navigate to **Devices → Chrome → Apps & extensions → Kiosks**. In the organizational-unit list on the left, select the unit containing the exam Chromebooks.

6. Select the **Abitti2** kiosk app configured under **Installation**. Its settings open in a panel on the right.
7. Scroll down to the companion extensions. Find the entry with ID `ednjaikaedogelbafimghlbnilijpnpf` and click the arrow beside it to expand its settings. If the entry is missing, complete **Add the Extension** under **Installation** first.
8. In the expanded extension settings, find **Certificate management** and turn on **Allow enterprise challenge**.
9. Click **Save** in the upper-right corner.
10. Keep the Chromebooks online so they receive the updated settings, then restart the kiosk session.

2. Add the allowed Google organizations in Tutkintopalvelu

A staff member with access to the school's settings opens Tutkintopalvelu, selects the correct school, and opens **Asennuskoodit**.

Under **Sallitut Google-organisaatiot (vain Chromebook-lukiot)**, enter:

Field	Value
Organisaation Google-verkkotunnus	The organization's Google domain, for example `school.example.fi`.
Asiakastunnus	The organization's Google Customer ID.

Find the Customer ID in Google Admin under **Account → Account settings → Profile**, as described in Google's instructions.

Click **Lisää uusi organisaatio**. Check that the entry appears under **Sallitut** and remains after refreshing the page. To correct an entry, use its **Poista** button and add the corrected values.

Add every Google organization whose Chromebooks will be used with this school's server. For example, if school A hosts candidates using school B's devices, add B's organization to A's list too. Each organization's Google administrator must also complete the Google Admin settings above.

3. Check the result in the invigilator's view

Test the settings before the exam:

1. Start the Abitti kiosk app from the Chromebook sign-in screen's **Apps** menu.
2. Sign in to a practice exam using a test candidate.
3. Open **Aloita ja valvo kokeita** on the server. Expand the candidate's **ChromeOS-tarkistus** result.
4. Confirm that both **Laite** and **Kioskitila** show **Varmennettu**. Test devices from each organization that will participate.

Result	Meaning
ChromeOS-tarkistus: varmennettu	Both device and kiosk checks passed.

ChromeOS-tarkistus: hylätty	A check was rejected. The details indicate the reason, such as an organization or boot-mode mismatch.
ChromeOS-tarkistus ei onnistunut	The check could not finish. Check the Google Admin and Tutkintopalvelu settings, network connection and installed app versions.

Technical monitoring

To ensure fairness in the matriculation tests, AbittiCandidate includes a comprehensive technical monitoring feature. Technical monitoring is a software-based solution that observes events in the test environment and collects evidence of possible cheating attempts.

This chapter explains why monitoring is carried out, what it observes, and how it affects (or does not affect) the candidate's experience. The details of monitoring are not disclosed, based on the Act on the Openness of Government Activities (621/1999), 24 § paragraph 7.

Why technical monitoring exists

In digital tests, there is always a risk of cheating (e.g., unauthorized use of online resources, programmatic communication with outsiders, etc.). Traditional invigilation (an invigilator walking around the room) is not sufficient to detect all forms of digital cheating. Technical monitoring has been developed to support the test as follows:

- **Preventing** many types of cheating in advance by discouraging attempts when candidates are aware of monitoring.
- **Detecting** suspicious activity in real time, if something obvious happens.
- **Enabling** evidence collection to confirm cheating afterwards using concrete data.

What technical monitoring observes

Without listing every detail, technical monitoring may observe key activities in the kiosk session, such as:

- Screen contents or changes on the screen
- Keyboard events
- Mouse and other peripheral device usage
- Clipboard contents
- Audio device usage
- Network traffic and connections
- System state

This list is presented as an example only and does not restrict MEB in developing monitoring.

Implementation

When launching the kiosk application, its extension runs a monitoring program (or several) in the background to collect information. The programs are optimised so that the quality of the test performance is not affected (they consume very few resources and operate silently in the background).

These programs get the monitoring tasks from the server during the test so the activities may vary during the exams. Furthermore, the activities cannot be analysed by decompiling the monitoring applications.

Before executing the monitoring tasks the digital signature of the tasks is verified to prevent malicious code execution.

How monitoring reacts and appears in different situations

There are three possible operation modes, and AbittiCandidate may apply one or more depending on the situation:

1. **Real-time warning to the candidate**: If something clearly prohibited is detected, the system may display a warning on the screen. Such warnings are intended mainly to protect the candidate from unintentional fraudulent behaviour.
2. **Alert to the test invigilator**: In certain serious cases, the system can send a notification to the party monitoring the test (e.g., the invigiltors' view). For example, if the monitoring system is not functioning on the candidate's device, an alert may appear in the invigilators' view. The alert may block the candidate from continuing until the reason for the warning has been clarified.
3. **Post-test review**: In most cases, all monitoring data is stored without interfering in real time. After the test, the MEB specialists review the output produced by the monitoring. Furthermore, if a new cheating method is discovered in one test, recordings can be searched afterwards to find all candidates with similar activity.

From the candidate's perspective, technical monitoring is almost unnoticeable. In rare cases, they may receive a warning on screen, as mentioned above.

ChromeOS Flex

ChromeOS Flex is Google's product where ChromeOS is installed to traditional 64-bit workstation. Since this hardware lacks Chromebook's hardware security layer, the ChromeOS Flex devices cannot utilise ChromeOS Verified Access feature. ChromeOS Verified Access is used to make sure the device is administered by a trusted party.

On the Abitti 2 server's invigilator screen, a warning is displayed for candidates whose Verified Access check has failed. In practice, this warning is shown for all candidates using ChromeOS Flex because of missing hardware security layer.

In schools' own practice tests, this warning can be ignored. In the matriculation examinations, however, such devices must be started using an Abitti 2 candidate USB drive. In that case, a Linux operating system is loaded from the USB flash drive and the ChromeOS operating system is bypassed for the duration of the examination.

Closing remarks

This document aims to cover all the key aspects of the Abitti 2 ChromeOS application from the perspective of school IT administration and information security – from installation to monitoring. The

MEB is committed to designing and implementing a secure, isolated, and manageable system that contributes to a fair matriculation examination.

By following the instructions given here you should be able to deploy the application without problems and respond to concerns raised by teaching staff or candidates.

If there are still questions or exceptional situations not addressed here, we recommend contacting the Matriculation Examination Board’s Abitti support. The contact information can be found at abitti.fi. The website contains updated version of this document and other up-to-date information about AbittiCandidate and Abitti 2.

With thorough planning and trialing, you can ensure smooth and fair matriculation examinations for all candidates.