# Table of Contents

1 INTRODUCTION ........................................................................................................... 3

2 APP INSTALLATION ........................................................................................................ 4
   2.1 PREREQUISITES ....................................................................................................... 4
      2.1.1 Operating system .............................................................................................. 4
      2.1.2 G Suite for Education or Clever ....................................................................... 4
      2.1.3 Networking considerations .............................................................................. 4
   2.2 ON CHROME OS ...................................................................................................... 5
      2.2.1 Sign into the Google Administration Console ............................................... 5
      2.2.2 Enable Chrome Web Store ............................................................................ 5
      2.2.3 Deploying through the Chrome Store ............................................................ 6
      2.2.4 Deploying without the Chrome store ............................................................. 9
   2.3 ON WINDOWS ........................................................................................................ 10
   2.4 ON MACOS ........................................................................................................... 11

3 ADMINISTRATION ......................................................................................................... 12
   3.1 CONFIGURING ACCESS TO THE VISION PORTAL WEBSITE ..................... 12
      3.1.1 Additional configuration for access with GSuite accounts ......................... 12
         3.1.1.1 Authorize Vision Portal for the required API scopes ............................ 12
         3.1.1.2 Create a domain-wide delegation user account for Vision ................. 15
   3.2 CONFIGURE THE RELAY SERVER ..................................................................... 20
   3.3 USING APPLICATION POLICIES ...................................................................... 20
      3.3.1 For Chrome OS ............................................................................................... 20
      3.3.2 For Windows .................................................................................................. 24
      3.3.3 For macOS ..................................................................................................... 25
      3.3.4 Application Policy options ............................................................................ 25
         3.3.4.1 Keepalive Signal (deprecated) ................................................................. 25
            • For Chrome OS ......................................................................................... 26
            • For Windows ............................................................................................. 26
            • For macOS ................................................................................................. 26
         3.3.4.2 Disable Analytics (deprecated) ................................................................. 26
            • For Chrome OS ......................................................................................... 26
            • For Windows ............................................................................................. 26
            • For macOS ................................................................................................. 26
         3.3.4.3 Add Relay Server for Restricted Networks ........................................... 26
            • For Chrome OS ......................................................................................... 27
            • For Windows ............................................................................................. 27
            • For macOS ................................................................................................. 27
         3.3.4.4 Add On Premise Signaling Server (deprecated) ...................................... 28
            • For Chrome OS ......................................................................................... 28
            • For Windows ............................................................................................. 28
            • For macOS ................................................................................................. 28
         3.3.4.5 Enable Clever authentication ................................................................. 28
            • For Chrome OS ......................................................................................... 28
            • For Windows ............................................................................................. 28
            • For macOS ................................................................................................. 29
         3.3.4.6 Enable Edlink authentication ................................................................. 29
            • For Chrome OS ......................................................................................... 29
            • For Windows ............................................................................................. 29
            • For macOS ................................................................................................. 29
         3.3.4.7 Modify refresh interval for student screen capture (deprecated) ........... 29
            • For Chrome OS ......................................................................................... 30
         3.3.4.8 Enforce student screen capture mode (deprecated) .............................. 30
            • For Chrome OS ......................................................................................... 30
            • For Windows ............................................................................................. 30
            • For Mac ...................................................................................................... 30
   3.4 DISABLE INCognito MODE ..................................................................................... 30
Vision for Chromebooks – Administrator's Guide

3.5 MANAGE THE TASK MANAGER GOOGLE DOMAIN POLICY ................................................................. 31
3.6 LOGGING .............................................................................................................................................. 31
  3.6.1 For Chrome OS ................................................................................................................................. 31
  3.6.1.1 Retrieve Extension Logs ................................................................................................................. 31
  3.6.1.2 Retrieve detailed logs ...................................................................................................................... 31
  3.6.2 For Windows ..................................................................................................................................... 32
  3.6.3 For macOS ....................................................................................................................................... 33

4 ADMIN REPORTS .................................................................................................................................. 34

5 ADMIN POLICIES ................................................................................................................................... 39
  5.1 STUDENT MONITORING ...................................................................................................................... 40
  5.2 IP ADDRESS RESTRICTIONS ............................................................................................................... 41
  5.3 APP BEHAVIOUR ................................................................................................................................. 41
  5.4 NETWORKING ...................................................................................................................................... 42
1 Introduction

This document is intended to guide school IT administrators through the deployment and configuration of the Vision for Chromebooks solution.

Vision for Chromebooks includes four components:

- **Netop Vision Teacher** – the teacher’s User Interface
- **Netop Vision Student** – the student’s User Interface
- **Netop Vision Student Extension** – a Chrome extension to manage teacher control features
- **Netop Vision Portal** – a website that provides additional functionality and configuration options for teachers and administrators

**NOTE:** The extension is located in the browser, at `chrome://extensions`: 

![Netop Vision Student Extension](image-url)
2 App Installation

2.1 Prerequisites

This section is intended to describe the technical specifications necessary to execute the applications.

2.1.1 Operating system

Vision Teacher is supported on the following operating system platforms:
- On Chrome OS: the latest version of Chrome OS
- On Windows: Windows 7 or later
- On macOS: macOS 10.9 or later

For more information in regards to the system requirements, refer to the following link.

Vision Student:
- The latest version of Chrome OS

2.1.2 G Suite for Education or Clever

G Suite for Education or Clever is required. By default, the Vision for Chromebooks application uses the G Suite authentication.

To switch to the Clever authentication, refer to the Enable Clever authentication sub-chapter.

2.1.3 Networking considerations

Vision for Chromebooks uses WebRTC connectivity, a collection of protocols and interfaces that makes real-time peer-to-peer audio and video communication more efficient.

WebRTC uses the STUN protocol to establish peer-to-peer connections, even when the endpoints are not in the same network.

To protect the student’s privacy and to prevent accidental connections from outside your organization, Vision does not allow students to join classes. Vision allows them to join if the Students’ and Teacher’s external IP addresses are in the same range, sharing the same first two address octets (i.e., a 255.255.0.0 netmask is used for matching). You can configure the following setting in the Admin policy section > Student monitoring.

Ports are allocated dynamically, and, in most cases, there is no need for any port configuration. However, if your current network configuration is preventing direct connectivity through the use of firewalls, or if you are using a restricted NAT model (i.e. restricted cone, symmetric NAT), make sure that you apply additional settings to allow Vision traffic.

NOTE: To allow Vision traffic in a restricted network, you can use the WebRtcUdpPortRange Chromium Policy to force Chrome to use WebRTC ports from within a given range, then configure your network equipment accordingly, allowing UDP traffic through those ports. For a list of active policies, refer to
chrome://policy > Chrome policies. For Windows and macOS, verify the firewall and proxy considerations, available here.

2.2 On Chrome OS

2.2.1 Sign into the Google Administration Console

Go to admin.google.com and sign in using your administrator account.

2.2.2 Enable Chrome Web Store

Before you can install Vision apps or extensions for your school users, make sure that you turn ON their Chrome Web Store service in your Administration console. Refer to the Turn Additional Google services on or off section for more information.
2.2.3 Deploying through the Chrome Store

To deploy the Vision Teacher and Student applications on the user Chromebooks through the Chrome Store, proceed as follows:

1. Go the Google Admin console.
2. In the Admin console, click on the More button.
3. Click on Devices.
4. Expand the **Chrome** option.

5. Click on **Apps & Extensions**.

6. Create your Organizational Units where to deploy the **Vision Teacher** and **Student** applications.

   **NOTE:** It is recommended to have separate Organizational Units for the teachers’ and students’ devices.
7. In the respective Organizational Unit, click on the + button.

8. Click on the **Add from Chrome Web Store** button.

9. In the search entry field, specify **Netop Vision**.
10. To add the application to the Organization Unit, click on the **Select** button.

11. To deploy the applications, select either **Force install + pin** or **Force install** from the drop-down menu of the application.

   After you select an option, the applications are deployed on the devices.

### 2.2.4 Deploying without the Chrome store

To deploy the **Vision** components (Teacher or Student) on the user Chromebooks, proceed as follows:

1. From the **Admin console dashboard**, click on the **Device Management** button.
2. From the **Devices Settings** menu on the left, click on the **Chrome Management** button.
3. Click on the **App Management** button.
4. In the upper right corner of the **Admin console**, click on the **** button.
5. Select **Add Custom App**. You are prompted to specify the **app ID** and **URL**.

![Add custom app dialog box]

The following table describes the information required for the Vision apps:

- **Vision Teacher**
  
<table>
<thead>
<tr>
<th>Fields</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>ncbcbpchojjmcjajfdhehmpmioohndg</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://clients2.google.com/service/update2/crx">https://clients2.google.com/service/update2/crx</a></td>
</tr>
</tbody>
</table>

- **Vision Student**
  
<table>
<thead>
<tr>
<th>Fields</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>hfpdkhblendlpcghglcmncbicbkappp</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://clients2.google.com/service/update2/crx">https://clients2.google.com/service/update2/crx</a></td>
</tr>
</tbody>
</table>

- **Vision Student extension**
  
<table>
<thead>
<tr>
<th>Fields</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>hppkmolfplapacolakfekieiedjapl</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://clients2.google.com/service/update2/crx">https://clients2.google.com/service/update2/crx</a></td>
</tr>
</tbody>
</table>

6. Click on the **Add** button.

7. To add all of the **Vision** components in the Admin console, repeat steps 3 and 4.

Based on the policies you have set in the **Google Admin** console the components are automatically installed on the users’ Chromebooks.

Refer to the **Manage Chrome Apps Individually** for more information on installations for specific users.

### 2.3 On Windows

Only the **Teacher** app can be installed on Windows devices.

To manually install the **Teacher** app, use one of the following options:

- Go to the **Microsoft Store** and install the **Teacher** application; or
- Download the **.EXE** file from the **Netop site** and install it.
To mass deploy the **Teacher** app, proceed as follows:

- Mass deploy the **Teacher** app using the [Microsoft Store app](#) (check Microsoft article [here](#)).
- Mass deploy the **Teacher** app using the available `.MSI` files (more info [here](#)).

### 2.4 On macOS

Only the **Teacher** app can be installed on the macOS devices.

To install the **Teacher** app go to the [Mac App Store app](#).
3 Administration

3.1 Configuring access to the Vision Portal website

Vision Portal offers a Filter Web configurator and additional application settings and provides domain admins with access to usage reports.

The website can be accessed by opening the link [https://vision.netop.com](https://vision.netop.com) from any modern browser. The Teacher app provides direct links to the Vision Portal.

3.1.1 Additional configuration for access with GSuite accounts

By default, when using GSuite authentication, all accounts have access to Vision Portal and usage reports are unavailable. In order to limit access to Teachers (members of the Classrooms Teachers group) and Admins (users with an Administrative role), as well as to grant admins access to usage reports, make sure that you perform the following configuration steps using a GSuite admin account:

- Authorize Vision Portal for the required API scopes
- Create a domain-wide delegation user account for Vision, with limited administrative privileges (netop-vision / Read Groups Admin and Read Users)

**NOTE:** Refer to the following link for more information about the Administrator roles in GSuite.

3.1.1.1 Authorize Vision Portal for the required API scopes

Vision Portal requires API permissions to read users and groups, in order to determine the roles of users logging in.

To delegate domain-wide authority to Vision Portal, with the required API scopes, proceed as follows:

1. Go to [admin.google.com](https://admin.google.com).
2. Click on the Security icon.
3. Scroll down to **API controls**.

4. Click on **API Controls**.

5. Click on the **Manage Domain Wide Delegation** button.
6. Click on the **Add new** button.

7. In the **Client ID** entry field specify the following **application ID** 107208250793970984385.

8. In the **OAuth scopes** entry field, specify the following **API scopes** (comma-delimited):
   - https://www.googleapis.com/auth/admin.directory.user.readonly,
   - https://www.googleapis.com/auth/admin.directory.group.readonly
9. To save your changes, click on the Authorize button.

3.1.1.2 Create a domain-wide delegation user account for Vision

**Vision Portal** requires that a specific domain-wide delegation user account with administrative privileges to read users and groups that exist in the **GSuite** domain. The account is used for querying the roles of users logging in to the website.

To create this user account, proceed as follows:

A. **Create the netop-vision user account.**

To create the **netop-vision** delegated admin account, proceed as follows:

1. Go to **admin.google.com**.
2. Click on the Users icon.
3. Click on the Add new user button.
4. Specify **Netop** as the first name in the First name entry field.
5. Specify **Vision** as the last name in the Last name entry field.
6. Specify `netop-vision` as the primary email address.

**NOTE**: Selecting the **Organizational unit** is optional.

7. Click on the **ADD NEW USER** button to save your changes.

---

**B.** Optional: create a custom administrative role for the `netop-vision` account (**Read Groups Admin**)

This step is optional but recommended. You can skip this step if you plan to use a pre-existing administrative role for the `netop-vision` account.

To create the **Read Groups Admin** user custom role, proceed as follows:

1. Go to `admin.google.com`. 
2. Click on the Admin roles icon.

3. Click on the CREATE A NEW ROLE button.

4. In the name field, specify Read Groups Admin as the name of the group. The Privileges tab is displayed.

5. Scroll down to the Admin API Privileges area.

6. From the Users drop-down list, check the Read checkbox.
7. From the **Groups** drop-down list, check the **Read** checkbox.

**NOTE:** Refer to the following link for more information about creating custom administrator roles.

**C. Assign the required admin privileges to the netop-vision user delegated account**

The following steps make use of the custom role created in step B – if you skipped that step, you may use any other administrative role with the required privileges.

To assign the user-created role, proceed as follows:

1. Go to `admin.google.com`.
2. Click on the **Users** icon.
3. Click on the **Netop Vision (netop-vision)** account.

4. Click on the **Admin roles and privileges** card.
5. To assign the role, click on the toggle button for the **Read Groups Admin** role.

Refer to the following link for more information about assigning administrator roles to a user.

### 3.2 Configure the Relay Server

Vision for Chromebooks has its own relay TURN server to help achieve a successful connection between Teachers and Students when peer-to-peer connections are not possible.

Make sure that you allow communication on the following ports:

- TCP and UDP – 3478
- TLS and DTLS – 5349
- Relay ports: 49152 – 65535

### 3.3 Using Application Policies

Please note that the following application policies and settings are now available in the **Vision Portal**:

- Modify refresh interval for student screen capture
- Disable Google Analytics
- Enable Keepalive Signal
- Add On Premise Signaling Server
- Enforce student screen capture mode

**NOTE:** These application policies will soon be discontinued. They will be supported for a short period in order to provide you with sufficient time to migrate them to the **Vision Portal**.

For more information refer to the Admin policies chapter.

#### 3.3.1 For Chrome OS

Through Google Administration, you can add files that contain various configurations for your apps running on Chrome OS (Teacher and/or Student side).
A configuration file begins with "{" and ends with "}". Between the brackets, multiple policy settings can be added.

This is a sample configuration file:

```
{"WebRTCPingIntervalDurationMs" : { "Value" : 30000 },
"DisableAnalytics": { "Value" : true }
}
```

To upload a configuration file to an application or to specify a policy, proceed as follows:

1. **Log in the Google Admin console.**

2. **Click on the More button.**

3. **Go to Devices.**
4. Go to Chrome.

5. Go to Apps & extensions.

6. Go to the Organizational Unit where the Vision for Chromebook applications are installed.
7. Click on the **Vision Teacher** application.

8. Specify the policies that you want to add in the **Policy for extensions** entry field.

9. To upload a configuration file, click on the **Upload configuration file** button.
10. To save your changes, click on the **Save** button.

To remove the file, you can click on the **X** button or click on the **Inherit to default** button to inherit the settings of the previous user groups.

You can view active configurations by browsing to `chrome://policy` for each user, under the app name.

Sample configuration files can be retrieved [here](#).

### 3.3.2 For Windows

Custom configuration is available on Windows using the registry. Registry keys can be updated individually on a device or deployed on several devices using tools like the **Group Policy**.

To update a device individually, create a `.REG` file containing information on the registry items that require to be updated.

The configuration information starts at `"{" and ends with "}"`. You can between the brackets, multiple policy settings (**all " need to be escaped using the \ sign)**.

Here is a sample reg file (`test.reg`):

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Netop\Vision\Chromebooks]
@=""
"ManagedStorage"="{\"WebRTCSignalingServerHost\":{\"Value\":\"testserver.com \"}}"
```

To manually execute a `.reg` file, double click on the file, and accept the changes.

For deployment using a **Group Policy**, refer to the following [Microsoft article](#).
Sample configuration files can be retrieved from the following link.

3.3.3 For macOS

Custom configuration is available on macOS using .plist files. This is a custom .plist file (myfile.plist):

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>ManagedStorage</key>
    <dict>
      <key>WebRTCSignalingServerHost</key>
      <dict>
        <key>Value</key>
        <string>peerserver.school.org</string>
      </dict>
      <key>WebRTCPingIntervalDurationMs</key>
      <dict>
        <key>Value</key>
        <integer>120000</integer>
      </dict>
    </dict>
  </dict>
</plist>
```

The configuration information starts after the first <dict> tag.

To import a .plist file on a device, open a Terminal, type the following and then press Enter.

```bash
defaults import com.netop.visionteacher <path to the .plist file>
```

<path to the .plist file> is the location of the .plist file on the device.

To view the current configuration of the application, open a Terminal, type the following and then press Enter.

```bash
defaults read com.netop.visionteacher
```

Sample configuration files can be retrieved here.

3.3.4 Application Policy options

3.3.4.1 Keepalive Signal (deprecated)

**NOTE:** The following option will be discontinued and is now a part of the Admin policies feature in the Netop Vision Portal. For more information about the Admin policies feature refer to the WebRTC settings section.

If your network uses a proxy that disconnects the idle WebSocket connections after a timeout, this is a Keepalive signal mechanism that verifies the connection between the Teacher and Student application. Setting this option to a value close to the proxy timeout ensures that the connection remains open. Make sure that the value you set is at least 30000 (default value 30 seconds).
• For Chrome OS
"WebRTCPingIntervalDurationMs" : { "Value" : 30000 }

• For Windows
"WebRTCPingIntervalDurationMs" : { "Value" : 30000 }

• For macOS

<key>WebRTCPingIntervalDurationMs</key>
<dict>
  <key>Value</key>
  <integer>120000</integer>
</dict>

3.3.4.2 Disable Analytics (deprecated)

NOTE: The following option will be discontinued and is now a part of the Admin policies feature in the Netop Vision Portal. For more information about the Admin policies feature refer to the Application settings section.

By default, Netop Vision sends information such as clicks and view count to Google Analytics, which we use to make our product better. This option makes the application stop sending this kind of information.

• For Chrome OS
"DisableAnalytics": { "Value" : true }

• For Windows
"DisableAnalytics": { "Value" : true }

• For macOS

<key>DisableAnalytics</key>
<dict>
  <key>Value</key>
  <true/>
</dict>

3.3.4.3 Add Relay Server for Restricted Networks

This option allows adding one or multiple relay servers to channel network traffic between the Teacher and Student in case that direct connections are not possible.
Each section contains an URL, username, and password to connect to either a **TURN** or **STUN** server.
3.3.4.4 Add On Premise Signaling Server (deprecated)

**NOTE:** The following option will be discontinued and is now a part of the Admin policies feature in the Netop Vision Portal. For more information about the Admin policies feature refer to the WebRTC settings section.

In the scenario where due to the firewall and/or proxy conditions, WSS (Web secure sockets) are not allowed between the applications and the Netop servers, there is the option of setting up a signaling server locally. The following option needs to be added to use an on-premise signaling server.

- **For Chrome OS**
  ```json
  "WebRTCSignalingServerHost": {"Value": "mysite.local" }
  ```

- **For Windows**
  ```json
  \"WebRTCSignalingServerHost\": {"Value": \"mysite.local\"}
  ```

- **For macOS**
  ```xml
  <key>WebRTCSignalingServerHost</key>
  <dict>
    <key>Value</key>
    <string>mysite.local</string>
  </dict>
  ```

Replace `mysite.local` with the domain for the signaling server. For instructions on how to set up the on-premise signaling server, refer to the following Knowledge Base article.

3.3.4.5 Enable Clever authentication

In order to provide easy integration with your Student Information System (SIS), we use the integration with Clever (www.clever.com). In order to enforce that the students and the teachers need to use Clever authentication, the following setting needs to be applied (you need to modify the DISTRICT_ID with the ID provided by us).

- **For Chrome OS**
  ```json
  {"CustomSISOOptions": { 
    "Value" : { 
      "Type": "clever", 
      "Organization": "DISTRICT_ID"
    }
  }}
  ```

- **For Windows**
  ```json
  {"CustomSISOOptions": {"Type": \"clever\", \"Organization": \"DISTRICT_ID\"}}
  ```
3.3.4.6 Enable Edlink authentication

Edlink is a platform that allows synchronization with well-known LMS/SIS systems such as Canvas, Blackboard, Moodle, Schoology, or Microsoft Teams for Education.

In order to enforce that the students and the teachers need to use Edlink authentication, the following setting needs to be applied:

- For Chrome OS

```json
{ "CustomSISOptions": { 
    "Value": { 
        "Type": "edlink",
    }
}
}
```

- For Windows

```
"CustomSISOptions": { "Type": "edlink"}
```

- For macOS

```xml
<key>Value</key>
<dict>
    <key>Type</key>
    <string>edlink</string>
</dict>
```

**NOTE:** During the login process, some LMS platforms may request you to authorize the Edlink application.

3.3.4.7 Modify refresh interval for student screen capture (deprecated)

**NOTE:** The following option will be discontinued and is now a part of the Admin policies feature in the Netop Vision Portal. For more information about the Admin policies feature refer to the Student monitoring section.

The rate at which the student desktop is captured as well as the interval at which updates are sent to the Teacher application can be modified in order to save network resources. The refresh interval value can
be specified in milliseconds and needs to be larger than 5000 (5 seconds). You need to apply the policy to the Vision Student application.

- For Chrome OS

```json
"ThumbnailCaptureIntervalDurationMs": {
   "Value": 5000
}
```

### 3.3.4.8 Enforce student screen capture mode (deprecated)

**NOTE:** The following option will be discontinued and is now a part of the Admin policies feature in the Netop Vision Portal. For more information about the Admin policies feature refer to the [Admin policies](#) chapter.

Teachers have the option of configuring the way the student desktops are shared, via the Teacher Settings section in the Netop Vision Portal.

The option within the Teacher Portal – “Monitoring students” - can be overridden by a policy set by an admin. You need to enable this policy on the Vision Teacher application. The policy takes any one of the following two values:

- **“tab”** – for capturing and sharing the active browser tabs
- **“desktop”** – for capturing the full desktop, with sound. The “desktop” option requires the student’s approval.

- For Chrome OS

```json
"StudentDesktopCaptureMode": { "Value" : "tab" }
```

- For Windows

```xml
<key>StudentDesktopCaptureMode</key>
<dict>
   <key>Value</key>
   <string>screen</string>
   <string>screen</string>
</dict>
```

- For Mac

```xml
<key>StudentDesktopCaptureMode</key>
<dict>
   <key>Value</key>
   <string>screen</string>
</dict>
```

### 3.4 Disable Incognito Mode

Incognito mode disables by default all the preinstalled extensions. To override this and allow teacher access if students are using Incognito mode, proceed as follows:

1. From the Admin console dashboard, click on Device Management.
2. From the Devices Settings menu on the left, click on Chrome Management.
3. Click on User Settings.
4. From the **Incognito Mode** drop-down, select the **Disallow incognito mode** option.

![Incognito Mode](image)

3.5 Manage the Task Manager Google Domain Policy

**Task Manager** is a new Google domain policy allows you to block students from ending tasks with the Task Manager utility. This setting is available from the Google Admin Console, by browsing to **Devices > Chrome Management > User Settings**, and then searching for **Task Manager**.

**NOTE**: The Task Manager Google domain policy applies only to Chromebook devices that are running version 52 and above.

3.6 Logging

3.6.1 For Chrome OS

3.6.1.1 Retrieve Extension Logs

To retrieve the extension logs, access from the browser the following links:

- **For the Teacher**: https://vision.netop.com/apps/chrome/teacher/logs
- **For the Student**: https://vision.netop.com/apps/chrome/student/logs

This triggers a log file download.

**NOTE**: The corresponding applications (Teacher or Student) are necessary for this to work.

3.6.1.2 Retrieve detailed logs

To view the **Netop Vision for Chromebooks** logs (for each component), proceed as follows:

1. In Chrome, click on the ** Collegium button.**
2. Select **More Tools**.
3. Select **Extensions**.
4. Tick the **Developer Mode** checkbox to obtain access to developer tools.
5. Click on the URL from the Inspect views section. The **Developer Tools window** is displayed.
An example is displayed below:

6. Select the **Console** tab.

3.6.2 For Windows

Retrieve the logs by copy and pasting `%APPDATA%\Vision Teacher for Chromebooks\logs\` into the Windows file explorer.

If the **Vision for Chromebooks** application is downloaded and installed from the Microsoft Store, you can retrieve the logs from the following location:

`%AppData%\Local\Packages\NetopSolutions.VisionTeacherforChromebooks_m7p600ccwap2t\LocalCache\Roaming\Vision Teacher for Chromebooks\logs`. 
3.6.3 For macOS

You can retrieve the logs from the following path:

(Your username here)/Library/Containers/com.netop.visionteacher/Data/Library/Application Support/Vision Teacher for Chromebooks/logs/
4 Admin reports

The Admin reports page in the Vision Portal provides organization admins with an overview of the Vision applications usage.

NOTE: To use the Admin reports feature in the Vision Portal with GSuite accounts, you need to go through the additional configuration steps for the Vision Portal, as detailed previously in this document. Only Administrator accounts have access to the Admin reports.

The Admin reports page contains usage reports over a time span, for domain administrators, that displays how the teachers and students use and interact with the Vision for Chromebooks application.

The data used in generating the usage reports is gathered from all the organizations using the domains associated with your account.

You find the domains used in generating the usage reports at the bottom of the page.

You can select the time span for the usage reports from the top of the page:

The time span values that you can select are:
- Last 7 days
- Last 14 days
- Last 30 days
- Last 60 days
- Last 90 days
NOTE:

- For the last 7, 14, and 30 days the usage reports display **daily** unique users, active teachers, active classes, class sessions, class features, and most active teachers.
- For the last 60 and 90 days, the usage reports display **weekly** unique users, active teachers, active classes, class sessions, class features, and most active teachers.

The following table describes the displayed values:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total unique users</td>
<td>This value represents the total number of users that have logged in the Vision app.</td>
</tr>
<tr>
<td>Total class sessions</td>
<td>This value represents the total number of times a class has been started.</td>
</tr>
<tr>
<td>Total active teachers</td>
<td>This value represents the total number of unique teachers that started a class.</td>
</tr>
<tr>
<td>Total active students</td>
<td>This value represents the total number of unique students that joined an active class.</td>
</tr>
</tbody>
</table>

Several usage report charts are available:

- **Unique users** – displays the total number of unique logins to the Vision app, per day or per week, during the selected time span.
• **Active Teachers** – displays the total number of *Teachers* that started a class, per day or week, during the selected time span.

![Active teachers chart](chart1)

• **Active classes** – displays the total number of classes that were started at least once, per day or per week, during the selected time span. Multiple start class events for the same class are counted only once per interval.

![Active classes chart](chart2)
- **Class sessions** – displays the total number of times classes were started per day or week, during the selected time span. All start class events for all classes are counted per interval.

- **Class features** – displays the total number of times each class feature was used during the selected time span.

- **Teachers by feature usage** – displays the top 10 teachers based on the number of features used in an active class.
To download the usage reports, click on the **Export report data** button. The exported report data are `.csv` files and they contain the following data:

- Active classes
- Active teachers
- Class features
- Class sessions
- Metric
- Teachers by feature usage
- Unique users

You can use the browser's default **Print** function in order to print the usage reports or save them as a **PDF** file.
With the **Admin policies** feature, admins can configure the following:

- **Student monitoring**

  ![Student monitoring screenshot](image1)

  - **Refresh interval for the student cards**
    - Interval in seconds
    - 5 - 180 seconds; leave empty for application default.
  
  - **Monitoring mode**
    - **Not configured**
      - Teachers may configure monitoring according to their own preference.
    - **View the Chromebook main screen**
      - Show all activity on device. Students are prompted to accept.
    - **View the active Chrome tab**
      - Show the browser activity only. No prompt is issued to students.

- **IP address restrictions**

  ![IP address restrictions screenshot](image2)

  - **No restriction**
    - Students join classes regardless of their IP address. This may be a privacy risk.
  
  - **Match the teacher IP address**
    - Students join classes only if the first half of their external IP address is the same as the teacher's.
  
  - **Match the teacher IP address or a whitelisted network**
    - Students join classes only if the first half of their external IP address is the same as the teacher's or it matches one of the whitelisted networks.

  - **Match a whitelisted network**
    - Students join classes only if their IP address matches one of the whitelisted networks.

  - **Whitelisted networks**

  ![Whitelisted networks screenshot](image3)

  - **Add a new network**

- **App behaviour**

  ![App behaviour screenshot](image4)

  - **Send anonymous data to Google Analytics from Vision Student**
    - **Enabled**
5.1 Student monitoring

From the **Student monitoring** section, you can change the following:

**Refresh interval for the student cards**

The rate at which the student desktop is captured as well as the interval at which updates are sent to the Teacher application can be modified in order to save network resources. The refresh interval value is specified in seconds and needs to be larger than the default value (default value is set to 5 seconds).

**NOTE:** The refresh rate interval applies to both Student thumbnails and Student browser tabs.

**Monitoring mode**

The following options are available:

- **Not configured**
  Each Teacher can modify the student monitoring option from the **Teacher settings** tab.

- **View the Chromebook main screen**
  All Student browser tab activity is displayed. Students are prompted to accept sharing their screen.

- **View the active Chrome tab**
  Only the browser activity is displayed. Students are not prompted to accept sharing their screen.

**NOTE:** If the option is set from the **Admin policies**, Teachers cannot change the Student monitoring option from the Teachers settings.
5.2 IP address restrictions

From the IP address restrictions section, you can select one of the following options:

- **No restriction** - no IP address restriction is applied. This means that Students can connect to the Teachers’ class regardless of their public IP address.

- **Match the teacher IP address** – the first two octets of the Teacher and Student IP addresses must match for a successful connection.

- **Match the teacher IP address or a whitelisted network** – the following setting allows admins to add a whitelisted network IP addresses and masks using the CIDR notation. The first two octets of the Teacher and Student IP addresses must match, or the Student IP address must match one of the whitelisted networks for a successful connection between Teacher and Student devices.

- **Match a whitelisted network** – the following setting allows admins to manually add the whitelisted network IP. The Student IP address must match one of the whitelisted networks in order to have a successful connection between Teacher and Student devices.

5.3 App behaviour

From the Application settings you can Enable or Disable Google Analytics. **Netop Vision** sends information such as clicks and view count to Google Analytics, which we use to improve our product. This option makes the application stop sending this kind of information.

By default, the option is set to **Enabled**. To disable the policy, click on the **Enabled** button and click on **Disabled**.
5.4 Networking

Depending on the products that you have, you can modify the following settings:

**NOTE:** These settings apply to the Vision 365 application.

- **Demo quality level** - This setting allows admins to modify the demo quality and bandwidth consumption of the Demo feature.
  
  You can select from the following options:
  
  - **High** - high demo quality and bandwidth consumption
  - **Medium** - medium demo quality and bandwidth consumption
  - **Low** - low demo quality and bandwidth consumption

- **Connection timeout** - this setting specifies the maximum period of network inactivity after which the Student application disconnects from the Teacher application. A higher value can solve connection issues on slower or congested Wi-Fi networks. The connection timeout value is specified in seconds and needs to be larger than the default value (the default value is set to 10 seconds).

**NOTE:** These settings apply to the Vision for Chromebooks application.

- The **WebRTC keep-alive interval** – If your network uses a proxy that disconnects the idle WebSocket connections after a timeout, this signal mechanism verifies the connection between the Vision applications and the Signaling Server. Setting this option to a value close to the proxy timeout ensures that the connection remains open. The default value is set to 30 seconds.

- The **WebRTC signaling server** – you specify the address of your signaling server. You can specify it as a domain (i.e., www.mydomain.org:443), or as an IPv4 address (10.10.20.30:443), or an IPv6 address (for a valid IPv6 address, you must specify it between square brackets “[”, “]”, i.e., [2001:0db8:85a3:0000:0000:8a2e:0370:7334]:443).