# Better Security with BenQ

Display solutions designed with security in mind

# Better Security with BenQ

BenQ knows that bringing in new devices to your organization always comes with a few risks. Without sufficient security, these products may leave your networks exposed, increasing chances of data leaks, privacy violations, and operational setbacks.

Trust BenQ to deliver solutions that perfectly fit your current security strategy. When it comes to displays, we not only offer the best in terms of image clarity, color accuracy, sound quality, and interactivity, we also provide top-end security to safeguard your organization.

Our end-to-end solutions—from individual devices to cloud infrastructure—offer multiple levels of security that help you tick every item on your corporate security checklist.

Device Security

Network Security

Cloud Security

**01** We adhere to international standards and uphold your right to data privacy

**02** We help you protect your organization against security threats

**03** We offer secure access to your boards, user accounts, and files

01

## We adhere to international standards and uphold your right to data privacy

BenQ Boards and its related cloud services have gone through rigorous screening and have passed the strict data privacy criteria imposed by the European Union's General Data Protection Regulation (GDPR and GDPR-K), the California Consumer Privacy Act (CCPA), the UK's Product Security and Telecommunications Infrastructure (PSTI) regime, the App Defense Alliance's (ADA) Cloud Application Security Assessment (CASA), the Children's Online Privacy Protection Act (COPPA), and ISO/IEC 27001 security standards.

GDPR

GDPR-K

CCPA

PSTI

ADA

COPPA

# We adhere to international standards and uphold your right to data privacy

## Ethical data collection and usage

Compliant with international data regulations such as GDPR and CCPA, BenQ guarantees that we do not collect or store personal identifiable information (PII) unless permitted by our customers.

BenQ also ensures that any customer data, such as their organization's user directories, will only be used for the purposes explicitly agreed upon by both parties; these may include enabling and improving specific cloud services and device functionalities.

BenQ will not sell or unlawfully share the data of our customers.

## Vetted cloud services and infrastructure

The BenQ Account Management System (AMS) has passed the CASA Tier 2 assessment requirements set by the ADA. Each aspect of AMS such as its cloud architecture, API, and its end-to-end processes including access control, cryptography, and others have undergone thorough scanning and lab testing, and are validated secure against data security threats.

We also host the BenQ service portal and our databases on Amazon web servers (located in Frankfurt, Germany), which are built to meet the highest standards for data security, privacy, and reliability. BenQ cloud services are regularly tested by third-party auditors in line with AWS Compliance programs.

# We adhere to international standards and uphold your right to data privacy

```
    elif _operation == "MIRROR_Y":
        mirror_mod.use_x = False
        mirror_mod.use_y = True
        mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
        mirror_mod.use_x = False
        mirror_mod.use_y = False
        mirror_mod.use_z = True

        #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
        #mirror_ob.select = 0
```

9:41
Search for accounts
BenQ 1 Service (security1@BenQ.com)
940 462
BenQ 2 Service (security2@BenQ.com)
922 356
BenQ 3 Service (security3@BenQ.com)
022 752
BenQ 4 Service (security4@
631 074

## Secure communications

BenQ websites use internet security protocols such as SSL and HTTPS to secure your connection, encrypt any transmitted data, and prevent attackers from intercepting data sent between BenQ online portals and your devices.

## Convenient authorization

BenQ web services make use of OAuth 2.0 and JSON web tokens, industry standards that are utilized for efficient authorization across multiple devices without requiring our users to share their private credentials with BenQ.

## Multi-factor authentication

BenQ allows users to enable multi-factor authentication, which would require them to input a security code sent to their mobile device when logging in. This additional step helps verify their identity and prevents unauthorized access in case their login credentials are compromised.

# We adhere to international standards and uphold your right to data privacy

## Passwords stay private

BenQ Boards never save passwords locally when users log in to their BenQ accounts. This minimizes the risk of unauthorized access to the boards and user data.

BenQ Boards also provide alternative login methods that help prevent users from entering their credentials on screen and ensure that their passwords are not publicly exposed.

### QR code login

Users can scan a QR code displayed on their BenQ Board and then log in from their mobile device.

### NFC login

Some BenQ Board models come with built-in NFC sensors. System administrators can issue NFC cards to each user for controlled access and easy login.

### Single sign-on

BenQ Boards support secure single sign-on services such as Google, Microsoft Azure, and ClassLink that use encrypted tokens to protect user credentials.

02

# We help you protect your organization against security threats

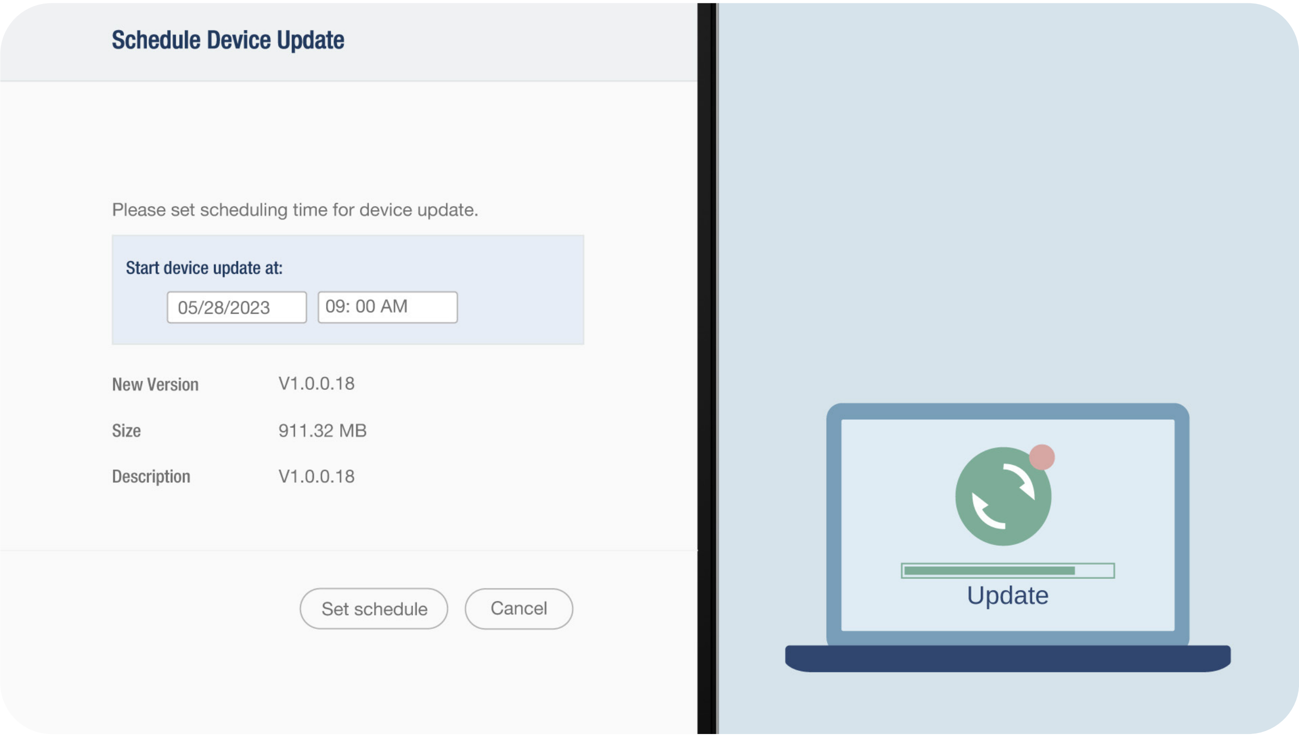
BenQ helps schools and companies safeguard their systems and data against threats such as malware and hacking by providing holistic security options that cover different levels of their data infrastructure.

# We help you protect your organization against security threats

## Protection against exploits

BenQ regularly provides the latest security patches and firmware updates for all rolling models of our BenQ Board. Administrators can take full advantage of their BenQ Board's over-the-air (OTA) update feature and remotely push these patches to all of their boards via the internet.

This not only ensures that their displays will have the necessary and timely protections against exploits and related attacks on their network, it also helps keep their board's operating system and BenQ software functioning at optimal performance.



Schedule Device Update

Please set scheduling time for device update.

Start device update at:

05/28/2023 09: 00 AM

New Version V1.0.0.18

Size 911.32 MB

Description V1.0.0.18

# We help you protect your organization against security threats

## Flexible network security options

BenQ Boards come with flexible network settings, which allow IT administrators to configure their displays to better complement their existing security strategy.

### Enterprise-grade authentication

Set up WPA2-Enterprise for user authentication and more secure communication.

### Encrypted data transmission

Apply certificates to validate other devices and encrypt data.

### Proxy-level protection

Configure proxy settings to restrict access to harmful sites.

## Antimalware and anti-phishing measures

Users of the 04 series BenQ Boards can take advantage of Google Play Protect and Safe Browsing.

**Google Play Protect** ensures that apps are carefully vetted before users can download and install them on the board. It also scans and removes any installed app exhibiting suspicious activity.

Meanwhile, **Google Safe Browsing** safeguards users while they are browsing online as it warns them if they visit potentially harmful sites that involve phishing and other web-based threats.

Google Play
Protect

Google
Safe Browsing

03

# We offer secure access to your boards, user accounts, and files

Through the BenQ AMS and Identity and Access Management (IAM) system, we offer IT administrators a way to create and manage user accounts, allowing them to prevent unauthorized access and possible tampering of BenQ Board settings, user files, and folders.

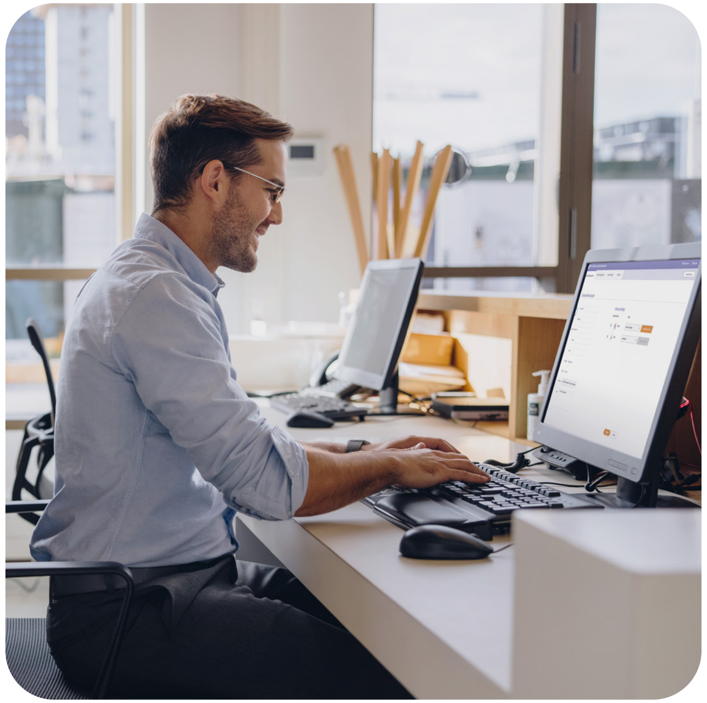
# We offer secure access to your boards, user accounts, and files

| | Guest users | Restricted users | Authenticated users |
|---|---|---|---|
| Login | Not required | Required | Required |
| Modification of settings | Not allowed | Only basic settings | Regular user settings |
| Connected devices<br>(via HDMI or USB-C) | ✓ | ✓ | ✓ |
| Public folder | ✕ | ✓ | ✓ |
| Personal folders | ✕ | ✓ | ✓ |
| Cloud storage | ✕ | ✓ | ✓ |
| EZWrite whiteboard | ✓ | ✓ | ✓ |
| InstaShare wireless screen sharing | ✓ | ✓ | ✓ |
| Web browser | ✕ | ✓ | ✓ |

Get more in-depth information on secure access controls for the BenQ Board.

https://www.benq.com/en-us/education/edtech-blog/access-authority-security-user-roles-settings-benq-board.html

# We offer secure access to your boards, user accounts, and files



## Secure user access

BenQ offers two ways that IT administrators can enforce stricter access controls for their BenQ Boards.

### Authentication mode

This mode offers a higher level of access control as it completely prevents guests from using the board and tampering with its settings. Enabling this mode on AMS ensures that only authenticated users will be able to use the board and its features.

### Restricted user role

Assigning this role ensures the highest level of access control as it restricts even authorized users and groups from making changes to any critical BenQ Board setting while still giving them access to all its essential features and functionalities.

## Idle session logout

Devices that are left unlocked and unattended are one of the most common causes of data leaks. Administrators can prevent this from happening on the BenQ Board by setting an idle session logout time on AMS. If ever a user forgets to log out of their board, AMS automatically logs out of the account.

## How can organizations make their smart devices more secure?

Below is a checklist you can use as a guide to help ensure that your smart devices are safe to use.

- □ Does your organization have smart device usage guidelines?
- □ Are you able to assign and modify user privileges for your devices?
- □ Do you receive firmware updates and security patches for your devices?
- □ Can you install security software?
- □ Does your smart device allow you to configure its network settings to make it more secure?
- □ Does your smart device use secure cloud systems?
- □ Is your smart device and its cloud services compliant with data protection regulations?

BenQ