BenQ IT Management

Best Practices Guide

Follow the steps in this guide to seamlessly set up, monitor, and manage your BenQ smart displays. Discover best practices to keep your devices running smoothly and get the most out of every feature.

Introduction

Managing multiple BenQ smart displays across an organization can be complex, from configuring devices and enforcing security policies to managing user access. This guide helps IT teams streamline these processes.

It focuses on BenQ's three core management platforms:

- **Identity and Access Management (IAM)**
- **Device Management Solution (DMS)**
- **Account Management System (AMS)**

Together, these solutions provide a unified framework for secure, efficient, and scalable management of BenQ smart displays across diverse locations, users, and applications.

You can skip any sections that don't apply to your organization.

Overview

This guide covers the following topics:

BenQ Admin Account

- Create a BenQ admin account.

Identity and Access Management (IAM)

- Create accounts automatically with directory sync.

Device Management Solution (DMS)

- Enroll devices.
- Organize devices.
- Deploy policies.

Account Management System (AMS)

- Configure global user settings.
- Provide instructions for user profile configuration and device login.

Get Started

Create BenQ admin accounts

1. Create an administrator account on service-portal.benq.com.
2. Create additional sub-admin accounts.
   2.1. Log in to iam.benq.com with your admin account.
   2.2. Invite a sub-admin using their email.
   2.3. Select the account, then choose Edit Service Permission to assign sub-admin role.

Identity and Access Management IAM

Effortless user account and access management.

Identity and Access Management

Key benefits

IAM enables quick integration of BenQ smart displays with an organization’s existing identity providers, allowing users to log in securely with their familiar SSO credentials.

- **Secure authentication**: All logins are verified through the organization’s servers.
- **Data privacy**: Sensitive information remains stored within the organization’s own infrastructure.
- **Real-time sync**: Account changes and permissions are automatically updated across all displays.
- **Streamlined management**: Eliminates the need to manually create user accounts.

Identity and Access Management

iam.benq.com

Setting up directory service syncing

Go to: **iam.benq.com: Accounts > SSO settings**

1. Select your organization’s directory service (Google Workspace, Microsoft Entra ID, LDAP, SAML provider, etc.).
2. Follow the on-screen prompts to authenticate and sync IAM with the directory service and ensure that AMS is enabled.

Note: Ensure **BenQ Services** is enabled during the initial setup experience on your BenQ smart display. If it was not enabled and you need directory service sign-in, you’ll have to factory reset the display to enable it.

Device Management Solution DMS

One platform to monitor smart displays, manage apps, execute updates, and more.

Device Management Solution

Key benefits

DMS unifies the control of BenQ smart displays across work sites. IT administrators can remotely monitor device status, deploy policies, push updates, and manage apps from a single platform.

- **Unified control**: Manage all smart displays remotely and securely from a single console.
- **Convenience**: Bundle settings and deploy multiple policies to one or several devices simultaneously.
- **Automation**: Schedule routine tasks such as power management.
- **Firmware updates**: Deploy updates to devices to maintain the latest features and security patches.

Device Management Solution

BenQ DMS Tool app

Enroll devices

Go to: The **BenQ DMS Tool** on your smartphone. (Available on the App Store and Google Play)

1. Log in to the app with your BenQ admin credentials.
2. Use the BenQ DMS Tool app to enroll smart displays by scanning the barcode located on the device or its product packaging. The device will appear in DMS once it’s connected to the internet.
3. Assign distinguishable names, in accordance with your device naming system, to the displays.

Device Management Solution

dms.benq.com

Organize devices

Go to **dms.benq.com: Main menu > Devices**

1. Create groups and tags.
2. Assign your devices to groups and tags.

Note: A device can only be in one group, but have many tags.

Device Management Solution

dms.benq.com

Create a policy

Go to **dms.benq.com: Main menu > Policies**

1. Add a policy.
2. Enter a policy name.
3. Customize policy.
4. Deploy policy to displays after customization.

Continued on next page...

Device Management Solution

dms.benq.com

Customize policy: AMS (to require login for display use) and local admin password

Go to **dms.benq.com: Main menu > Policies > [Select a Policy] > Launcher settings**

1. Enable **Remotely control BenQ AMS settings.**
2. Activate **BenQ AMS.**
3. Change local admin password.

   Important: Change the default admin/admin password to prevent unauthorized access. This password is different from your BenQ admin account credentials, which are used for IAM, AMS, and other BenQ services.
4. Edit **Access Security.**
   - **Authentication mode:** Users must log in to use the BenQ smart display. Access to all functions, including input sources such as HDMI and USB-C, is restricted until login.
   - **Guest mode:** Users can access basic smart display functions without logging in.

Continued on next page...

Device Management Solution

dms.benq.com

Customize policy: Wallpapers

Go to **dms.benq.com: Main menu > Policies > [Select a Policy] > Launcher settings > Wallpaper**

1. Upload wallpaper for login screen.
2. Upload wallpaper for home screen.

Recommended resolution: 3840 x 2160.

Customize policy: Disable notifications

Go to **dms.benq.com: Main menu > Policies > [Select a Policy] > Launcher settings > BenQ notifications**

- Turn off notifications.

Continued on next page...

Device Management Solution

dms.benq.com

Customize policy: Security settings

Go to **dms.benq.com: Main menu > Policies > [Select a Policy] > Security settings**

1. Add **security certificates**.
2. Allow or block apps using the **Apps from Google Play** option.
3. Set **Google Play** permissions for the smart display.
    - **Restrict accounts**: Google Play remains on the display and will auto-update apps, but users cannot sign in and download new apps.
    - **Disable**: Hides Google Play from the smart display and disables all related functions, including updates for apps previously installed through Google Play.

Continued on next page...

Device Management Solution

dms.benq.com

Customize policy: BenQ apps update settings

Go to **dms.benq.com: Main menu > Policies > [Select a Policy] > Update**

1. Turn on **Auto-update**.

Note: This setting doesn’t apply to Google Play apps.

Device Management Solution

dms.benq.com

Create a power schedule

Go to **dms.benq.com: Main menu > Automation**

1. Add an automation.
2. Enter a name.
3. Set a schedule.
4. Deploy schedule to displays.

Device Management Solution

dms.benq.com

Update firmware: Receive the latest features and security updates.

Go to **dms.benq.com: Main menu > Firmware.**

1. Schedule available updates during non-work hours.

Note: If the display is powered off at the scheduled time, updates will run the next time it is powered on.

Account Management System AMS

Secure access to private workspace from any BenQ smart display.

Account Management System

Key benefits

AMS enables secure user login to BenQ smart displays and provides access to personal workspaces.

- **Convenience:** Access cloud storage, bookmarks, apps, and web data.
- **Secure data:** Only the user can access their personal data.
- **Flexible login:** Users can log in using a username and password, NFC card, or QR code.
- **Easy management:** IT can bind NFC cards to accounts or allow users to manage them independently.

Account Management System

ams.benq.com

Set default user settings

Go to **ams.benq.com: Global Settings > Advanced**

1. Set a **global logout timer** or allow users to set their own.
2. **[Optional] Enable Allow users to bind NFC cards on their own** if permitted by your company's security policy, or bind NFC cards in batches by downloading and importing the template file.

Go to **ams.benq.com: Global Settings > Drives**

3. Select the cloud storage providers to be made available to users.

Account Management System

ams.benq.com

User account personalization

Provide these steps to help users get the most out of their BenQ smart displays.

1. Log in to **ams.benq.com.**
2. Go to **Settings > Advanced**, then set the **idle logout timer** if it hasn't already been set by IT.
3. **[Optional]** Bind your NFC card for quick login if permitted by IT.
4. Go to **Settings > Drives**, then link your cloud storage accounts for direct access when you log in to the BenQ smart display.

Choose one of the following methods to log in to a BenQ smart display:

- Username and password
- NFC card (if set previously)
- QR code

Note: Users who sign in with directory-service credentials must select **Sign in with SSO** on the smart display.

You’re All Set!

Your BenQ smart displays can now be managed from a single dashboard. Users can securely sign in using their company’s SSO credentials or NFC cards, access cloud storage files, and start using the devices.

If you have any questions, please contact your BenQ sales representative.

© 2026 BenQ Corp. Specification may vary by region, please visit your local stores for details. Actual product’s features and specifications are subject to change without notice. This material may include corporate names and trademarks of third parties which are the properties of the third parties respectively.