HP Engage Console User Guide

SUMMARY

HP Engage Console pushes apps to and configures settings for devices in an enterprise setting.

Legal information

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

First Edition: July 2020

Document Part Number: M03762-001

Table of contents

1 Getting started

You can use HP Engage Console to remotely configure and manage devices. For instance, you can manage HP Retail Point of Sale devices running the Android® operating system. You can also use this cloud-based software to configure and manage devices running Android, iOS, macOS®, and Windows ® 10 operating systems (OS).

Administrators and roles

Use the **Admins and Roles** section to add new administrators, manage existing ones, or change their roles and sign-in settings.

Adding new administrators

Follow these steps to add new administrators.

1. Go to **Admins and Roles**.
2. Select **Administrators**.
3. Select **Add New Admin**.
4. Enter the administrator's name and email, and assign a role to the user.
5. Select **Submit**. The user name is displayed on the administrator window, and a confirmation email is sent to the user.

NOTE: If you need to resend the confirmation email, select the email icon in the administrator's list.

Creating a new role

Follow these steps to create a custom role.

1. Go to the **Admins and Roles** page, and select the **Roles & Permissions** tab.
2. Select **CREATE NEW** under the **CUSTOM ROLES** section.
3. **NOTE:** You can assign any feature with all access or read-only permissions.

   A new page opens where you can enter a role name, choose whether you want to create roles for all devices or for device groups, and set the following permissions.

   - **VISIBILITY**—To display or hide a particular feature on the dashboard, toggle this button on or off.
   - **ALL ACCESS**—Provides both read and write permissions to the administrator.
   - **READ ONLY**—Provides read-only permission to the administrator.
4. Select **SAVE ROLE**. The custom role opens under the **CUSTOM ROLES** section.

Changing roles for administrators

Follow these steps to change an administrator role.

1. Select the **Administrators** tab, and select the gear icon in front of an existing administrator. Select **Edit**.
2. When the **Edit Admin User** window opens, go to the **Role** section, and choose the role within the drop-down menu.
3. Select **Submit**.

Two-step verification

Two-step verification provides an additional layer of security to HP Engage Console dashboard login. Only owner and co-owner accounts can enable two-step verification.

HP Engage Console supports two types of two-step verification:

- **Email-based two-step verification**—Sends a one-time password to the administrator's email address that you must enter to complete the login.
- **Google Authenticator two-step verification**—Uses the Google Authenticator app to create a code that must be entered to complete the login.

When either type of two-step verification is enabled, all accounts assigned as owner, co-owner, or administrator must follow the specified two-step verification method in order to log in.

Enabling two-step verification with email

Follow these steps to enable two-step verification with email.

1. Sign in to HP Engage Console.
2. Navigate to **Admins and Roles**.
3. Select **Sign In Settings** tab.
4. Select **Enable 2-Step Verification**. The email option is selected by default.
5. Select **SAVE**. The **Confirm password to continue** window opens.
6. Enter your password and select **SUBMIT**. The **Two-step Verification Enabled** section opens, and a notification window opens after enabling two-step verification successfully.

NOTE: Enabling two-step verification will not sign you or others out of a session, but it will enable at the next login attempt.

Enabling two-step verification with Google Authenticator

Follow these steps to enable two-step verification with Google Authenticator.

1. Sign in to HP Engage Console.
2. Select **Admins and Roles**, and select **Sign In Settings** tab.
3. Select the **Enable 2-Step Verification** button and select **Google Authenticator**.
4. Select **SAVE**. The **Confirm password to continue** window opens.

5. Enter your password, and select **SUBMIT**.

6. Follow the instructions displayed to register for Google authentication:

   a. A QR code is displayed on the dashboard. Download and install Google Authenticator application on your phone and launch the app.

   b. Select **Scan barcode** to launch the device camera.

   c. Point the device camera to the QR code displayed on the dashboard. The account is added to your authenticator app, and the dashboard displays a success message with back-up codes.

   NOTE: HP recommends downloading and saving the backup codes in case you lose or switch devices.

7. Select **DONE**. The two-step verification with Google authenticator is enabled for you and other administrator accounts of your HP Engage Console dashboard.

2 Device and user enrollment

You can enroll devices and users through the software directly or through a QR code.

Enrolling users

Follow these steps to add new users.

1. Under the **Device & User Enrollment** tab, select **User Management** .
2. Select **Add User**.
3. Create a user name for the user, enter their email and phone number, and select the number of devices to assign to the user.
4. Select **Add** to add the user.

Enrolling Android devices with QR code

Use this procedure to create a QR code that you can use to enroll Android devices.

1. Under the **Device & User Enrollment** tab, select **QR Code**.
2. Select **Create**. The **Create Device Enrollment Configuration** window opens.
3. Under the **Basic** tab, enter a name to identify the QR code.
4. Select an enrollment type:
   - **Kiosk/Agent**—For corporate-owned devices.
   - **Personal (BYOD)**—For user-owned devices.
5. Enter the device naming options.
6. Select **Next**; the **Group/Profile** tab opens.
7. Select either a user group or device profile for each of your platforms, and then select **Next**.
8. When the **License** tab opens, select a device license, if needed.

   NOTE: This step is optional.

9. Select **Save** to create the QR code. The QR code appears on the list.
10. Select the Android button from the list.
11. Select **Show Android QR** to view the QR code.
12. You can perform the following actions:
    - **Download**—Downloads the configuration file you can copy to an SD card for enrolling devices.

- **Email**—Sends the QR code to your account email.
- **Edit**—Edits the QR code configuration. Editing does not affect already enrolled devices.
- **Deactivate**—Deactivates the current QR code configuration.
- **Rotate**—Generates a new QR code and URL, and deactivates the previous QR Code and URL. Use if you think the current QR code configuration is compromised.

Enrolling Windows devices

Follow these steps to enroll Windows devices.

1. Under **Device & User Enrollment**, select **QR Code**.
2. Find and select the device enrollment configuration that you want.
3. Select the **Windows 10** button.
4. Select **SHOW ENROLLMENT URL**, and follow the on-screen instructions.

Enrolling devices with config file

Follow these steps to enroll devices with config file.

1. Select **Device & User Enrollment**, and then select **QR Code**.
2. Select the configuration that you want to use.
3. Select the download icon.
4. Save the `config.mlp` file to your local PC, and then copy it to the folder location on the target device within either `/`, `/sdcard/`, or `/Downloads/` folder.
5. Launch the HP Engage Console client, and select **Other Enrollment Options**. Then choose the **Auto Enroll** option.

NOTE: You must copy the file to each device's storage.

6. To enroll a Windows device, select **SHOW ENROLLMENT URL**. The Enrollment URL window displays the URL and enrollment code that you need to enroll the device. Follow the on-screen instructions to enroll the target device.

NOTE: Note the browser requirements.

3 Devices

The **Devices** tab allows you to see detailed information and perform some actions at the device level on enrolled devices.

Device information

This section outlines how to view detailed information about individual devices.

1. Select the **Devices** tab to view a list of enrolled devices.
2. Find the device whose information you want to see, and then select **View Details**.
3. A device specific page is displayed that contains the following information.
   - **Name and last seen**—The name of the device and the last time that it was active. HP Engage Console pings the device every 5 minutes to determine if it is active.
   - **Inactive alert**—If the device is inactive, an inactive alert message is displayed at the top of the information page. Whether or not this alert is displayed depends on the inactivity duration you set in the **Alerts** section of **Reports and Alerts** and the response to the device pings that HP Engage Console sends to the device every 5 minutes.
   - **Management removed alert**—If management is removed from the device, an alert displays at the top of the information page.
   - **Basic device information**—Other device information such as its device group name, battery level, Wi-Fi state and more information is displayed here.
4. To view additional detailed information about the device, select the gear icon and then select **Full Device Information**.

Device-level actions

This section outlines the device-level actions available in the **Devices** tab.

1. Select the **Devices** tab.
2. Find the device you want to work with and select **View Details**.
3. Select the gear icon to access the options listed here:
   - **Lock/Unlock**—This option applies only to Android devices. The **Lock** option applies the device profile to the device. The **Unlock** option allows the device user to use the device without the device profile policies applied. After you make your selection, refresh the page to verify that your selected option is enabled.
   - **Refresh Device**—This option applies changes made to the device profile to the device. Use this option if you see that the device profile changes you made were not applied. This option is available only if the device is locked.
   - **Add Notes**—Use this option to create custom notes that will appear in the **Full Device Information** page.

- **Factory Reset Device**—Resets the device to factory settings. This options works on any device that is enrolled as a corporate device, however, it is not available for user enrolled devices.
- **Delete Device**—This option removes management for and completely deletes the device. If you want to manage the device in the future, you must re-enroll it to HP Engage Console.
- **Change Device Name**—This option changes the name of the device.
- **Clear Browser Cache**—Clears browser cache for the selected device.
- **Nudge Device**—Use this option to ping an inactive device.
- **Send Message**—Use this option to send a message to the device.
- **Add to Device Group**—Use this option to add the device to a previously created device group.

4 Device Management options

You can use the Device Management options to create device profiles and device groups.

Branding

Branding allows you to create a set of customized features that you can apply to device profiles and groups. With branding, you can customize the lock-screen wallpaper, lock-screen message, and home-screen wallpaper. You can apply branding only to device groups or profiles, not to individual devices.

Creating a brand

Follow these steps to create a brand.

1. Log in to your HP Engage Console dashboard.
2. Select the **Device Management** tab and select **Branding**.
3. Select **CREATE NEW BRAND**.
4. A window opens with the following four tabs:
    - **GENERAL**—You can name your brand, choose to set as default brand, and enter a lock-screen message.
    - **ANDROID**—Select **Basic** or **Advanced** buttons to customize top bar color, wallpaper, logo, and app icons.
    - **IOS**—You can choose a home-screen wallpaper, lock-screen wallpaper, and preview the wallpapers.
    - **WINDOWS 10**—You can choose a home-screen wallpaper and lock-screen wallpaper and preview the wallpapers.
5. Select **SAVE**.

Publishing from branding

Follow the steps to publish from branding.

1. Select **Device Management**. Then select **Branding**. A list of saved brands opens.
2. Select **Apply Brand** on the brand that you want to apply.
3. From the window that opens, select the device profiles that you want to apply your brand to.
4. Select **APPLY**.

NOTE: HP Engage Console does not support branding individual devices.

Device Profiles

The Device Profile feature helps you group your policies together.

With Device Profiles you can create a group of policies and settings to assign to your devices. You can apply the device profile to individual devices or to a device group. Changes made in Device Profiles automatically apply to all the devices assigned to that profile. You can create custom device profiles or choose from the QuickStart options that contain preloaded settings based on the OS of the target device.

Creating a new profile for corporate-owned Android devices

Follow these steps to create a new device profile for corporate-owned Android devices.

1. From your HP Engage Console dashboard, go to **Device Management** and select **Device Profiles**.
2. Select **CREATE NEW PROFILE** in the upper-right corner.
3. Select **Kiosk/Agent** option.
4. Enter a name for the profile and an exit passcode. Select **Submit** to redirect yourself to the profile creator view.
5. After the **SELECT APPS** window opens, select from the following options.
   - **Set HP Engage Console as launcher**—Replaces the home launcher of your device and displays a custom home screen.
   - **Set HP Engage Console as agent**—Runs in the background and silently applies policies. You can use the native launcher.
6. Choose which applications you want to use on the device.
   - **Enabled**—Allows you to use the application on the device.
   - **Visible**—Allows you to display or hide the application on the home screen.
   - **Allow Lock Task**—Allows the app to pin itself to the screen for a custom amount of time and achieve single-app-mode state.
7. Select **NEXT**. The **SELECT BROWSER SHORTCUTS** window opens. You can select the previously whitelisted websites.

   For more information about how to whitelist a website, see Whitelisting websites on page 12.
8. Select **NEXT** and the **SELECT BRAND / APP ORDER** window opens. You can apply a previously selected brand, and select the order of the enabled apps.

   For more information about branding, see Creating a brand on page 8.
9. Select **NEXT**. When the **KIOSK/LAUNCHER SETTINGS** window opens, you can view the settings that are applicable when HP Engage Console is set to launcher.
   - **Single App Mode**—Allows you to turn your Android tablets or phones into a kiosk that runs one app only.
   - **Home Screen settings**—Allows you to customize HP Engage Console home screen behavior.
10. Select **NEXT**. When the **RESTRICTIONS** window opens, you see a collection of policies that allow you to control and manage your devices better.
    - **Volume Settings**—Allows you to control the volume attributes of your devices.
    - **Wifi Settings**—Allows you to manage the WiFi configuration of your devices.

- **Mobile Network**—Allows you to mange the mobile data configuration of your devices.
- **Display Settings**—Allows you to manage the display attributes of your devices.
- **EMM Settings**—Additional settings that provide additional security and control for your EMM-managed devices. You can give your users access to Systems Settings in a controlled fashion.
- **VPN Settings**—You can select one app from the list of applications and mark it as Always On VPN with an additional flag to lock down the network.
- **Compliance**—You can use Safety Net API to check the device compliance.
- **Secure Settings**—You can override the Global or Device level Secure Settings.

NOTE: These settings only work with Samsung, Sony, and LG devices. Options that are marked by an asterisk work when HP Engage Console is set as device owner via EMM management.

- **Exchange**—Allows you to configure an Exchange account on the device and select a previously created Exchange configuration.

Creating a new profile for user-owned Android devices

Follow these steps to create a new profile for personal Android devices.

1. Under **Device Management** tab, select **Device Profile**, and select the **CREATE NEW PROFILE** button.
2. Select **Create New Profile**.
3. In the **Create New Profile** dialog box, select the **Android** tab. Then select the **Personal (BYOD)** option.
4. Enter a name for your profile, and select **SUBMIT**. The Profile Creator wizard launches, and the device profile creation is divided into three sections:
    - **Select Apps** —Select the apps that you want installed to the device.
    - **Whitelist Websites** —Select to enable access to previously whitelisted websites.
    - **Restrictions** —Configure security and account management policy controls.
5. For security, account management, data sharing, and app management settings, go to the **Restrictions** tab, and select **General Settings**.
6. To set up an Exchange account on the device, go to **Restrictions** tab, select **Exchange Settings** .
7. To configure Wi-Fi settings, select **Wifi Settings**.

NOTE: This creates the Wi-Fi configuration on the device but does not enforce it.

8. To create a separate profile for your work apps, select **Work Profile Password** section. To enable, select **Require Passcode**.
9. To configure VPN settings, go to the **Restrictions** tab, and select **VPN settings** tab.
10. To configure compliance levels and actions for compromised devices, select **Compliance.**
11. After you select all the necessary configuration options, select **Create Profile** to complete the profile setup.

Creating new Windows device profile

Follow these steps to create a new Windows device profile.

1. Under **Device Management** tab, select **Device Profile**, and select **CREATE NEW PROFILE** button.
2. Select **Create New Profile**.
3. In the **Create New Profile** dialog box, select the **Windows** tab. Then, enter a name for your profile and select **SUBMIT**. The Profile Creator wizard launches, and the device profile creation is divided into the following four sections.
   - **Select Apps**—Section to configure your application policy.
   - **Whitelist Websites**—Section to whitelist websites to be used with **Google Chrome**.
   - **Chrome Configurations**—Additional settings for Google Chrome.
   - **Settings**— Section to configure additional settings based on categories.
4. To configure the application policy in **Select Apps**, select an application policy and select **NEXT**.
   - **Application Blacklisting**—Block selected Windows applications from running.

     NOTE: You can block only UWP apps or apps installed from Microsoft Store. Use Device Profile to select the apps to block.
   - **Skip Configuring Apps**—Select this feature if you do not want to define an application policy for your Windows devices.
   - **Application Whitelisting**—Select the list of applications that should be allowed.

     NOTE: You can whitelist both UWP and Win32 bit apps.
5. In the **Whitelist Websites** section, configure the URLs that a user is allowed to browse on Google® Chrome™ or Windows Kiosk Browser app.
6. In the **Chrome Configurations** section, configure Google Chrome settings.
7. To set an application to run always and set the Windows device in kiosk app mode, go to the **Settings** tab, and select **Kiosk App**.
8. To apply a home-screen wallpaper, lock-screen wallpaper, or both to your enterprise devices, go to the **Settings** tab, and select **Branding**.

   NOTE: To create a custom branding, go to **Device Management** tab, and select **Branding**, and then apply it to device profile.

   You can select branding that is compatible with Windows.
9. To configure Wi-Fi and network settings, go to **Settings**, and select **Wifi & Network**.
10. After you select all the necessary configuration options, select **Create Profile** to complete profile set up.

Device Groups

You can use the Device Group feature to organize your devices into distinct groups.

The Device Groups feature gives you the following options:

- Group together devices using different operating systems.
- Reboot all devices that belong to a group.
- Refresh all the devices that belong to a group so that you can be sure that device profile policies are actively applied.
- Set or change device profiles for all the devices in a group.
- Create and assign group administrators.

Creating a device group

Follow the instructions outlined here to create a device group.

1. Under the **Device Management** tab, select **Device Groups**, and then select **Create New**.
2. Enter a name for the group, and then select **Submit**. A new window opens.
3. In the **Select Devices** tab, only devices that do not already belong to a group are listed. Select the devices you want to add, and then select **Next**.
4. Select the profiles you want to apply based on OS type, and select **Next**. If you have not created any device profiles, you will see only the default option.
5. In the **Add Admin** tab, you can select group administrators.
6. Select **Create Device Group** to create the group.

Device group actions

You can apply changes and perform actions for all devices in a device group.

You can perform the following device group actions:

- **Set Install Window**—You can set an installation window for the applications that you push to this device group from the enterprise store. The applications are installed or updated when the device time matches the time you specify here.
- **Rename Device Group**—Use this to change the name of the group.
- **Delete the Device Group**—Deletes the device group. All devices retain their profiles and are locked.
- **Reboot Devices**—Use to reboot all devices in a group.
- **Refresh Devices**—Use this to refresh the device to ensure that all the required policies are enforced on the device.
- **Clear Browser Cache**—Use to clear the browser cache on all the devices in the group.

Whitelisting websites

Follow the instructions here to create a list of whitelisted websites that you can apply to device profiles and groups.

1. Under **Device Management** tab, select **Whitelist Websites**.

2. Select the **Whitelist A Website** button.

3. In the **Whitelist a Website** window, the **Details** tab opens first. Enter the website name and URL here. You can also choose whether you want the site to be visible on the home screen.

4. Select **Next**.

5. Under the **Android Settings** tab, choose from the available options.

6. Select **Next**.

7. Under the **Apple Settings** tab, choose from the available options.

8. Select **Save** to whitelist the site.

5 Content Management

The Content Management feature allows you to publish content to devices managed by HP Engage Console.

Uploading content to the dashboard

Follow these steps to upload content to the dashboard.

1. Within the dashboard, select **Content Management** and then select **Content**.
2. Select **ADD NEW** and then select **Files**. The file upload window opens with two separate tabs:
   - **Upload from Computer**—You can drag and drop files here, or select **UPLOAD FILES** and select a file to upload.
   - **Upload Using External Link**—You can upload files using an external link by following the onscreen directions on this tab.

NOTE: To upload content, Android and Windows devices must have the FileDock app installed. iOS devices must have the HP Engage Console app installed. You can download both the FileDock app and the HP Engage Console app from **Enterprise/My Apps/Recommended Apps**.

Creating a presentation

Follow these steps to create a presentation.

1. From the dashboard, select **Content Management**, and then select **Content**. Be sure that you have content uploaded.
2. Select the **Presentations** section, and select **CREATE PRESENTATION**.
3. Enter your presentation name, and select **SAVE**. A presentation creator window opens with the following panels:
   - Content panel—Displays the content you uploaded in a tree format. You can select your files and move them to the presentation panel.
   - Presentation panel—Displays the files that are part of the presentation and additional properties that you can set for the presentation.
4. Select the arrows next to the file to move it from the content panel to the presentation panel. Unsupported files have a red exclamation mark next to them.
5. Drag the files in any order that you choose within the presentation panel.
6. Select the **PROPERTIES** tab to select the properties of your presentation:
   - **Enforce Landscape mode**—Select this option to lock the presentation in landscape mode.
   - **Use As A Screensaver**—Select this option to use the presentation as a screensaver.

   NOTE: This feature is available only for Android devices.

- **Loop Continuously**—Select this option to play the presentation in a continuous loop.
- **Choose an Interval Time**—Select this option to set a time duration to delay between two files. The minimum time is 5 seconds and the maximum time is 1 minute.

7. Select **UPDATE** to save the presentation.

6 Remote Cast & Control

Remote Cast & Control grants you remote access to devices registered to HP Engage Console. This allows you to remotely view, control, and troubleshoot devices.

Remote cast supports the following functions:

- Cast device screen—Mirrors the screen of a remote device.
- Remote control—Allows you to control the device screen.

NOTE: Not available on iOS devices. Available on most Android devices and all HP Engage devices.

- VoIP Calling—Allows you to make a voice call to the device.
- Keyboard and clipboard redirection—Allows you to type in the input fields for the target device.

Setting up Remote Cast & Control for Android devices

Follow these steps to set up Remote Cast and Control for Android devices.

1. Under the **Enterprise**, go to **My App**.
2. Under **Recommended Apps**, find the Remote Cast & Control app for Windows (indicated by the Android logo in the app tile).
3. Select the profiles and devices where you want to install the app.
4. Select **Publish** to install the app.
5. After download is complete on the target device, select the Remote Cast & Control app to launch it.
6. Follow the on-screen instructions to grant permission to use the features of the app on the device.

Initiating a Remote Cast & Control session for Android devices

Follow these steps to initiate a Remote Cast and Control session for Android devices.

1. Select **Remote Cast & Control** to display the list of devices that support Remote Cast & Control.
2. Find the device that you want to start a Remote Cast & Control session with, and select **Start Session**. The screen casting page displays the following components:
   - **CREATE TICKET**—Create a service desk ticket. This option is supported only if you have integrated an IT Management Tool (ITSM).
   - **Allow User to Stop Session**—When enabled, the users see a stop button which allows them to quit the session.
   - **Enable Voice Call**—When enabled, allows the use of VoIP call during the remote cast session.
   - **Start Session**—Select this button to start the session.

- **Start Recording**—Select this button to record the session.

3. Select **Start Session** to start the session. The device user must select **Okay** and **Start Now** on the Android device to accept the remote session.

4. Select **START NOW** to start a remote cast session. During a session, the following options are displayed:

   - **Control**—If supported, allows you to control the screen.
   - **Back**—Select to replicate back key behavior.
   - **Home**—Select to replicate home key behavior.
   - **App Switcher/Recent App**—Select to replicate app switcher or recent key behavior.
   - **Power Off**—Select to replicate power button behavior.
   - **Full screen**—Select to go full screen.
   - **Snapshot**—Select to take a snapshot.
   - **Lock/Unlock**—Select to lock or unlock device.
   - **Stop Session**—Select to stop the session.
   - **Start Recording**—Select to start recording the screen cast session.

Setting up Remote Cast and Control for Windows devices

Follow these steps to set up Remote Cast and Control for Windows devices.

1. Under the **Enterprise** tab, select **My Apps**.

2. Under **Recommended Apps**, find the Remote Cast app for Windows (indicated by the Windows logo in the app tile).

3. Select the profiles and devices where you want to install the app.

4. Select **Publish** to install the app.

5. After download is complete on the target device, go to **Start** search for `Remote Case and Control`, then select to launch the app.

NOTE: You must run the app at least one time on the target device in order to get the device listed on the **Remote Cast and Control** page on your dashboard.

6. A message displays on the device which indicates that it is waiting for an HP Engage Console administrator to initiate a session.

Initiating a Remote Cast & Control session for Windows devices

Follow these steps to initiate a Remote Cast & Control session for Android devices.

1. Select **Remote Cast & Control** to display the list of devices that support Remote Cast & Control.

2. Find the device that you want to start a Remote Cast & Control session with, and select **Start Session**. The screen casting page displays the following components:

   - **Session Details**—Displays the Windows device name and model.
   - **Create Ticket**—Create a service desk ticket. This option is supported only if you have integrated an IT Management Tool (ITSM).
   - **Start Session**—Select this to send the device user a request to start a Remote Cast & Control session.

3. Select **Start Session** to start the session.

4. The device user must accept the request to start the session.

NOTE: If the device user does not accept the request within 1 minute, the session times out and you must send another request.

5. After the device user accepts the request, the session launches in the Edge browser. A dialog box is displayed that shows the device user the following options:

   - **Your entire screen**—If the device user selects this option, you see their entire screen.
   - **Application window**—If the device user selects this option, you see only the application that they have open. If the application window is minimized, you see a black screen.
   - **Microsoft Edge tab**—If the device user selects this option, you see only the tab that they have selected.

6. After the device user makes their selection, you will see the section displayed on the HP Engage Console dashboard. The options available to you during an active Remote Cast & Control session are:

   - **Full Screen**—Select this option to expand the shared screen to full screen.
   - **Take Screenshot**—Select this option to take a screenshot of the shared screen.
   - **Stop Session**—Select this option to stop the session. The device user also has this option.

7 Eva Communication Suite

Eva Communication Suite allows you to communicate with device users through different methods.

Eva Communication Suite contains the following features:

- **Messenger**—This service allows device users to communicate with other users and administrators within their device groups via text or voice. Users can also send and receive files.
- **Phone**—Use this feature to manage contact lists and incoming and outcoming calls.
- **Channel Management**—Allows you to create and manage communication channels that devices or device groups can subscribe to.

NOTE: Devices must have the Eva app installed in order to use the Eva Communication Suite. The Eva app is available in the recommended apps section of the **Enterprise** tab. For more information, see Enterprise store on page 23.

Enabling device-to-device chat

Follow these steps to enable the device-to-device chat feature and VoIP calls.

1. Under the **Eva Communication Suite** tab, select **Settings**.
2. In the **Device to Device chat** section, select the slider to enable.
3. Select **Save Settings**. When enabled, devices that have the Eva client installed can chat with other devices within their device group.

Enabling Eva Phone

Follow these steps to enable the Eva Phone feature.

1. Under **Eva Communication Suite**, tap select **Settings**.
2. In the **Eva Phone** section, select the slider to enable.
3. Select **Save Settings**.

Adding and uploading contacts

After you have set up Eva Phone, you can add or upload contacts.

1. Under the **Eva Communication Suite**, select **Phone**. The **Contact** tab opens.
2. There are two ways to add contacts:
   - **Add Contact**—Use this option to upload one contact at a time.
   - **Upload CSV**—Use this to upload multiple contacts via a CSV file.

3. **NOTE:** Steps 3 and 4 are instructions on how to add contacts with the **Add Contact** option. For instructions on uploading multiple contacts at once, go to step 5.

   Select **Add Contact** and type the contact details.

4. - **Contact Number**—Use this to enter a full contact number including the country code.
   - **USSD**—Use this to enter a USSD number.
   - **Starts With**—Use this option if you want to blacklist or whitelist a group of numbers. For example, if you enter '1234', any contact that starts with that number can be blacklisted or whitelisted.

4. Select **Save**. The contact number is now listed on the dashboard.

5. To upload contacts, you must properly format the CSV file. To obtain a template you can use for uploads, select **Download Sample CSV**.

6. Open the file in a text editor such as Notepad.

7. The CSV file has three column headers; name,contact number, and USSD. It also has some sample numbers. Delete the sample numbers, but do not delete the headers.

8. Type your contact numbers and save the file. If you are not entering a USSD, type `false` in the column.

9. Select **Upload CSV**. A dialog box opens. To upload the CSV, you can either select **Browse File** to find it on your computer, or drag and drop the file into the dialog box.

Sending a file from dashboard to device

Follow these steps to send a file from dashboard to device.

1. Sign in to HP Engage Console.

2. Select **EVA Communication Suite**. Select **Messenger**. A window opens that contains four tabs. Select **Contacts**. Contacts and devices are listed on the left side of the window. Select the contact or device that you want to transfer your files to. After selecting the device, the chat view is displayed on the right side of the window.

3. Select the **Attachment** icon within the chat view.

4. Select **Files**.

5. Browse for your file, choose it, and select **Open**. The image sends to the device.

   NOTE: A double-tick mark indicates the status of the file sent.

   - Grey color—The file is delivered.
   - Blue color—The file is seen by the recipient.

Sending a file from a device to dashboard

Follow these steps to send files from a device to the dashboard.

1. Open the Eva app.

2. Select the contact that you want to send a file to. The chat view opens.

3. Select the attachment icon at the bottom of the chat view. The options open. Select **File**.

4. Select the file that you want to send. The file sends to the dashboard under Eva Messenger.

Eva Channels

Eva Channels allows you to create public or closed communication channels. Administrators and users can communicate with other members who are subscribed or visible to the channel.

You can create two types of channels:

- **Public**—A channel that is available to all users who have installed Eva and HP Engage Console apps on their devices.
- **Close**—A channel available only to users that are added to the channel by an administrator. Only the administrator who created the channel can remove or add users; users cannot remove or add themselves.

Creating a public channel

Follow these steps to create a public channel:

1. Go to the **Eva Communication Suite** tab, and select **Channel Management**.
2. Select **Add Channel**. The **Add Channel** window opens.
3. Enter the **Channel Name**.
4. Under **Choose Channel Type**, select **Public**, and then select **Submit**.
5. Select **Public** in **Channel Type**, and select **SUBMIT**.
6. When the channel is created and visible on the device. Select **Join Channel** to join the public channel. Users who have joined the channel can chat, send images, files, and voice messages to other users within the channel. Within the dashboard, you can perform the following tasks:
   - **Edit**—You can edit the name of the channel.
   - **Deactivate**—Deactivated channels go in read-only mode for all users. You can reactivate a deactivated channel.
   - **Delete**—You can delete a channel to remove it from the devices and the dashboard.
7. To leave the channel, select the three vertical dots next to the channel name, and select channel info. A new window opens. Select **Leave Channel**.

Creating a close channel

Follow these steps to create a close channel.

1. Go to **Eva Communication Suite** tab, and then select **Channel Management**.
2. Select **ADD CHANNEL**. The **Add a Channel** window opens.
3. Enter the **Channel Name**.
4. Under **Choose Channel Type**, select **Close**, and then select **SUBMIT**. A window opens.

5. Select the devices and users that you want to add as subscribers to the channel and select **NEXT**. Then, select administration users to add as a subscriber and select **SAVE**. Invited users can chat and send images, files, and voice messages to other users within the channel.

8 Enterprise

This section outlines the options available under the **Enterprise** tab.

My Apps

Use the My Apps feature, located under the **Enterprise** tab, to upload, update, and publish apps to devices. You can publish apps from several sources, such as those recommended by HP Engage Console or those from the Apple® App Store. You can also upload and update your own custom apps. Play-for-work apps are not supported for HP Engage Console at this time.

Enterprise store

The Enterprise store allows you to upload your own third-party apps into HP Engage console. This section outlines how to upload apps for Android, iOS, and Windows onto HP Engage Console.

Uploading an Android app

Follow the instructions here to upload an Android app.

1. Under the **Enterprise** tab, select **My Apps**.
2. Select **Enterprise Store**.
3. Select **Upload Android app**.
4. Select one option from the **Upload Android app** window:
   - **Upload APK file**—Select **Browse files** to find your APK file.
   - **Link to External APK**—Copy and paste an APK URL into the entry field and refresh.

NOTE: All APKs must have a digitally signed certificate to be uploaded onto devices and updated when installed. HP Engage Console supports APKs signed with version V1, or both V1 and V2. However, it does not support APKs signed only with V2. You can find more information in Android developer documentation available online.

Uploading an iOS app

Follow the instructions here to upload a iOS app.

1. Under the **Enterprise** tab, select **My Apps**.
2. Select **Enterprise Store**.
3. Select **Upload iOS App**.
4. To upload using an IPA file, select **Upload Using IPA File** . Select **Browse Files** to find the IPA from your computer.

   - or -

   To upload using a Plist link, select the **Upload Using Plist Link** tab. Copy and paste the `.plist` file

Uploading a Windows app

Follow the instructions here to upload a Windows app.

1. Under the **Enterprise** tab, select **My Apps**.
2. Select **Enterprise Store**.
3. Select **Upload Windows App**.
4. The **Basic Details** tab opens, type the information requested on-screen. Scroll down to see certificate and app size requirements.
5. Select **Next** to go to the **App Bundle** tab.
6. Select **Upload file** to upload an APPX or MSIX bundle from your computer.

   - or -

   Select **Provide URL** to copy and paste the `.appxbundle` or `.msixbundle` file link.
7. Select the **Choose File** button to upload the `.cer` certificate file .
8. Select **Save** to finish the upload.

Recommended Apps

HP recommends the apps in this section to enhance the functionality of HP Engage Console.

Table 8-1 Recommended apps

App	Description	OS compatibility
Bluetooth Manager	This app allows users to send and receive files using Bluetooth while in kiosk mode.	Android
Call Assist	This app allows users to view and end incoming calls to their device through the notification panel while in kiosk mode.	Android
Eva Eva Messenger	This app allows users to communicate with other users and administrators within their device groups via text or voice. This app also allows users to send and receive files. See Eva Communication Suite on page 19 for more information.	Android and iOS
FileDock	This app enables the ability to upload content to the dashboard and then publish it to user devices. See Content Management on page 14 for more information.	Android, iOS, and Windows
HP Engage Console	Installs HP Engage Console to devices, and allows you to update HP Engage Console from the dashboard.	Android
Mobilock LG Guard	This app provides extra security for LG devices enrolled to HP Engage Console. To enable this feature, you must publish the LG Guard APK from the dashboard to the devices, and then manually activate it on the devices.	Android
Remote Cast & Control	This app allows you to remotely view and control devices. See Remote Cast & Control on page 16 for more information.	Android and Windows
WingMan	This app enables the Remote Cast & Control feature for selected Lenovo devices.	Android
ProSurf - Kiosk Browser	This app allows you to create a customized and secure browser for iOS users.	iOS

Table 8-1 Recommended apps (continued)

App	Description	OS compatibility
Brew Survey	Use this app to create customized surveys and collect feedback from customers using phones and tablets.	Android
Brew Survey - Offline	This app allows you to create offline surveys.	iOS

Creating a password policy

Follow these steps to create a password policy for device users .

1. Select **Enterprise**. Then select **Passcode Policy**.
2. Select the tab of the OS that you want to create a policy for.
3. Select **Require Password**. Configure the **Password Type** policy and settings. The options listed here will vary depending on which OS you are creating a policy for.
   - **Select Password Type**—Select from the options available in the dropdown menu.
   - **Minimum Password Length**—Select a minimum password length.
   - **Enforce Complex Password**—Select to enable a complex password.
   - **Minimum number of symbols**—Select to choose a minimum amount of symbols in the password.
   - **Minimum number of lowercase characters**—Select to choose a minimum amount of lower-case characters in the password.
   - **Minimum number of alphabets**—Select to choose a minimum amount of alphabetical characters in the password.
   - **Minimum number of uppercase characters**—Select to choose a minimum amount of upper-case characters in the password.
   - **Minimum number of digits**—Select to choose a minimum amount of digits in the password.
4. Configure **Password Management Settings**.
   - **Password Expiry Period**—Select how often the user must change the password.
   - **Maximum Password History List**—Select the amount of previously used passwords that the user cannot use when setting a new password.
   - **Maximum Failed Attempts to Factory Reset**—Select the number of failed login attempts before device factory resets.
   - **Set Idle time for Auto Lock (in minutes)**—Select the amount of time to pass before the device auto locks.
   - **Maximum Grace Period for Device Lock**—Select the amount of time the user can use the device without entering a password before it locks the device. This option is available only for iOS devices.
5. Select **SAVE**.

Removing a password policy

Follow these steps to remove a password policy.

1. In the **Enterprise** tab, select **Passcode Policy**.
2. Select the tab of the OS you want to remove the password policy for.
3. Select **REMOVE**. The **Remove Password policy** dialog box opens.
4. Select either the **Device Profiles** tab or the **Devices** tab to remove the policy from. HP Engage Console attempts to remove the password and will not enforce a future password on the device.

Security incidents

The Security Incidents feature creates a log entry each time there is a failed attempt to unlock a device. A failed attempt entry is created when a device user attempts to exit HP Engage Console and enters an incorrect passcode more than three consecutive times. This feature is available only for Android devices.

Secure Settings

This option allows you to control security features on KNOX-compatible Samsung devices, and Sony and LG devices that have OS version 5.0 and later.

9 Utilities

This section outlines the options available in the **Utilities** tab.

APN settings

Access Point Name (APN) settings are provided by cellular carriers to allow devices to connect to the internet using cellular data (a SIM card). Here you can enter custom APN settings provided by the carrier to restrict the use of cellular data on corporate-owned devices and devices that use a corporate-owned SIM card. Some APN settings allow for the direct access of corporate devices without the need of a VPN.

Nudging inactive devices

You can reactivate devices that are idle or inactive. Follow these steps to nudge inactive devices.

1. Select **Utilities**. Then select **Nudge Inactive Devices**. A list of inactive devices opens.
2. Select your devices and select **Nudge**.

Broadcast messages

Broadcast Messages allows you to send messages directly to any device.

1. Under the **Utilities** tab, select **Broadcast Messages**.
2. Select **Create New Message**.
3. When a new window opens, enter the sender's name and the message, and then select **Next**.
4. All the registered devices and device groups appear in a new window. Select the device or device groups and then select **Send Message** to send the message to the selected devices or device groups.

Buzzing devices

Follow these steps to buzz (send an alarm to) devices.

1. Select **Utilities**. Select **Buzz Devices**.
2. Select the device that you want to send an alarm to. Select **Buzz**. A confirmation message opens.
3. Select **OK**. The device rings, and the alarm remains on until you engage in other activity on the device.

NOTE: The Buzz Devices feature works for devices already active.

Publishing Wi-Fi settings to devices

The Wi-Fi settings feature allows you to publish Wi-Fi configurations to enrolled devices.

1. Under the **Utilities** tab, select **Wifi settings**.

2. Select **Create New** and then select **Basic**.

3. When a new window opens, type the following information:

   - **Name**—Type a name to identify the configuration.
   - **SSID**—Type a name to identify the Wi-Fi network.
   - **Security Type**—Select an option from the dropdown menu.
   - **Password**—Create a password that must be entered to access the Wi-Fi network.

4. Select **Submit** to create the configuration.

5. To publish the configuration to devices, select the arrow icon located to the right of the Wi-Fi configuration name. Then select the devices and device profiles.

Locking and unlocking Android devices from the dashboard

Follow these steps to lock or unlock Android devices remotely from the dashboard.

1. Under the **Utilities** tab, select **Lock Unlock Devices**.

2. Select the device that you want to lock or unlock from the list of enrolled devices. You can now select either the **Lock** or **Unlock** button, depending on the current status of the device.

   If the device is locked, you can select the **Unlock** button. If the device is unlocked, you can select the **Lock** button. If the device is inactive, both the **Lock** and **Unlock** options are available.

10 Android Utilities

The **Android Utilities** tab allows you to manage and create a variety of settings for Android devices.

Global settings

The **Global Settings** feature, is located under the **Android Utilities** tab. It allows you to configure app notifications, password settings, and other options for Android devices without a device profile.

You can configure the settings listed here:

- **Enable/Disable app notifications**—Enables or disables app notifications on your devices. If enabled, apps with notifications are marked with a small icon.
- **Play Sound for Incoming Notifications**—If app notifications are enabled, use this option to assign sounds to play for each notification type.
- **Lock Screen**—Use this option to enable or disable the HP Engage Console lockscreen on devices. This option is enabled by default.
- **Capture IP Address**—Enable this option to capture the full IP address of device. After this feature is enabled, you can find the IP address in the **Devices** tab.
- **Password Protect Safe Mode**—Enable this option to force the user to enter a password when a device boots in Safe Mode. This additional layer of security prevents the user from uninstalling HP Engage Console. Follow the on-screen instructions and select **I Agree** to enable.
- **Internet Connectivity Indicator**—Enable this option so that a notification shows on the device when there is no internet connection.
- **Show OS Upgrade Menu Option**—This option allows the user to upgrade the OS on the device.
- **Password Protect HP Engage Console Upgrade**—If enabled, when HP Engage Console runs in Single App Mode, the user is asked for a password to upgrade the HP Engage Console app.
- **Access Root Privileges** —Enable this option to allow HP Engage Console to access root privileges on rooted devices.
- **Auto-Publish Whitelist Websites**—Enable this option to automatically publish whitelisted websites on devices that do not have a profile applied.

Clearing app data

Follow these steps to clear app data.

1. Select **Android Utilities**, and then select **Clear App Data**.
2. Select **Devices / Device Groups** tab, and then select **Next**.
3. In the **Select Apps** tab, select the apps whose data you want to clear.

11 Email Utilities

The **Email Utilities** tab allows you to create email exchange settings for devices managed by HP Engage Console.

Creating Email Exchange settings

This section outlines how to create Email Exchange settings for Android devices.

1. Under the **Email Utilities** tab, select **Exchange Settings.**
2. Select **Add New**. The **New Exchange Settings** window opens.
3. In the **Basics** tab, configure the required settings, and then select **Next.**
4. In the **Advanced** tab, configure additional settings, such as email sync settings (optional).
5. Select **Save**. The configuration appears in the **Exchange ActiveSync Settings** list.

Publishing an Email Exchange configuration

This section outlines how to publish an Email Exchange configuration to devices.

1. Under the **Email Utilities** tab, select **Exchange Settings.**
2. Previously created configurations are listed here. Find the configuration you want.
3. Select the publish icon located in the **Action** column. A new window opens that lists your device profiles.
4. Select the check box for the profile that you want to apply the email exchange configuration to, and then select **Publish**.
5. For the devices in the device profile, the Gmail client is configured with the selected configuration. Users who open the Gmail client on their device are asked to type their password in order to sync emails.

12 Workflows

The **Workflows** feature allows you to schedule repeated tasks and assign actions to occur when the tasks are carried out. The scheduled tasks run like scripts. Detailed reports are generated for the scheduled tasks.

There are two main types of workflows:

- Scheduled tasks—These tasks act on the apps published to the devices or change the state of the devices. The devices must be online at the scheduled time for the task. Scheduled tasks are based on your selected dashboard time zone.
- Compliance tasks—These tasks are based on device data and metrics. For example, an email alert can be sent to a device user to act when a certain metric, such as battery usage, is reached.

Creating a new workflow

Use this procedure to create a new workflow.

1. Go to the **Reports and Workflow** tab.
2. Select **Workflows**.
3. Select **Create Flow**.
4. Choose from the OS options , or select **Global** for workflow options that operate independent of OS type.

Creating a Workflow for device reports

Follow the steps outlined here to create a Workflow that automatically emails you a report of selected device properties.

1. Under **Reports & Workflows**, select **Create New**. The **Create a Flow** window opens.
2. Select the **Global** tab, and then select **Device Reports.**
3. Enter the following information—
   - **Name**—Create a name to identify the workflow.
   - **Select Devices/Groups**—Choose whether this workflow should work for all devices or only for the devices that you specify.

   NOTE: You can create only one workflow for all devices or device group.

   - **Select Device Properties**— Select the properties that you want to include in the report.
   - **Email Settings**— Choose the email addresses that will receive the report.
   - **Time & Timezone**— Select the time and timezone in which the report is sent.
   - **Frequency**— Select how often the device report is sent.
4. Select **Save** to create the workflow.

Managing existing workflows

Follow these steps to manage existing workflows.

1. Go to the **Reports & Workflow** tab.
2. Find the workflow that you want under the list of workflows.
3. To edit the workflow, expand the **Action** tab to find the **Edit** button.