

SMART Remote Management

Device management guide



Was this document helpful?
smarttech.com/docfeedback/171798





Learn more

This guide and other resources for SMART Remote Management are available in the Support section of the SMART website (smarttech.com/support). Scan this QR code to view these resources on your mobile device.

Trademark notice

SMART Board, SMART Notebook, SMART Meeting Pro, SMART Ink, smarttech, the SMART logo and all SMART taglines are trademarks or registered trademarks of SMART Technologies ULC in the US and/or other countries. Apple, iOS, and macOS are trademarks of Apple Inc., registered in the US and other countries. Google, Android, Chrome, Chrome OS, and Google Play are trademarks of Google Inc. Windows is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The Bluetooth word mark is owned by the Bluetooth SIG, Inc. and any use of such marks by SMART Technologies ULC is under license. All other third-party product and company names may be trademarks of their respective owners.

Copyright notice

© 2021–2022 SMART Technologies ULC. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without the prior written consent of SMART Technologies ULC. Information in this manual is subject to change without notice and does not represent a commitment on the part of SMART.

This product and/or use thereof is covered by one or more of the following US patents:

www.smarttech.com/patents

December 8, 2022

Contents

Chapter 1 Welcome	5
About SMART Remote Management	5
About this guide	6
More information	7
Chapter 2 Managing devices	8
Monitoring devices	9
Using tags and groups	19
Remotely viewing and controlling devices	24
Connecting to devices using the Terminal feature	26
Removing devices	27
Chapter 3 Installing and managing apps on devices	28
Installing apps	28
Enabling, disabling, and stopping apps	35
Clearing app data	39
Uninstalling apps	40
Installing and uninstalling apps on iOS and macOS devices using VPP	42
Viewing app usage data	44
Chapter 4 Deploying policies and managing settings	50
About policies and settings	50
Deploying policies	51
Deploying kiosk policies	54
Managing settings	57
Returning devices to factory settings and resetting their authentication tokens	63
Chapter 5 Running other commands on devices	65
Sending custom commands and scripts to devices	66
Sending files to devices	71
Sending messages and sounding the siren	74
Locking and unlocking devices	80
Restarting, shutting down, and waking devices	83
Changing devices' agent passwords	88
Running device-type-specific commands	90

Contents

Chapter 6 Running ad-hoc sessions	96
Chapter 7 Managing commands, schedulers, triggers, and workflows	98
Managing commands	99
Managing schedulers and triggers	104
Managing workflows	118
Appendix A Troubleshooting	123

Chapter 1 **Welcome**

About SMART Remote Management	5
About this guide	6
More information	7

About SMART Remote Management

SMART Remote Management is a cloud-based device-management tool you can use to remotely maintain, support, control, and secure devices in your organization. You can manage SMART Board[®] interactive displays and Android[™], iOS, macOS, Windows[®], and Chrome OS[™] devices all from a central location.

When you create a SMART Remote Management domain account for your organization and register for the first time, you receive a free 30-day trial automatically. To continue using SMART Remote Management after the trial period ends, activate the domain account with a product key. You can obtain a product key in two ways:

- Purchasing a product key from a SMART reseller
- Using the SMART Remote Management subscription included with your purchase of a SMART Board interactive display

After you create the domain account for your organization, you can create users and enroll your SMART Board interactive displays and other devices. You and other SMART Remote Management users can then perform a variety of actions with enrolled devices:

- Monitor and locate devices
- Use tags and groups to manage devices
- Remotely view and control devices
- Remove devices from SMART Remote Management
- Install and manage apps on devices
- Deploy policies to devices
- Manage device settings
- Send remote execution commands to devices

- Send files to devices
- Send messages and sound the siren
- Lock and unlock devices
- Restart, shut down, and wake devices
- Return devices to factory settings

Tip

For an overview of the SMART Remote Management user interface, see the *SMART Remote Management quick tour* (smarttech.com/kb/171797).







About this guide

This guide explains how to manage enrolled SMART Board interactive displays and other devices in SMART Remote Management. It also explains how to troubleshoot common issues with SMART Remote Management.

This guide assumes you have created and activated a domain account, created users, and enrolled your organization's devices as documented in the *SMART Remote Management setup guide* (smarttech.com/kb/171333).

Note

Some SMART Remote Management features are available on only certain devices. The documentation for each feature in this guide includes a table that shows which devices the feature supports. The header rows in these tables represent devices with the following icons:

Icon	Description
	SMART Board interactive displays with iQ
	SMART Board GX and MX100 series interactive displays and Android devices
	iOS devices
	macOS devices
	Windows devices
	Chrome OS devices

In addition, *SMART Remote Management feature compatibility* (smarttech.com/kb/171722) includes a complete list of features and the device types each feature supports.

More information

This guide is part of a set of documentation for SMART Remote Management.

Other documentation for SMART Remote Management includes:

Document	Link
Quick tour	smarttech.com/kb/171797
Setup guide	smarttech.com/kb/171333
Release notes	smarttech.com/kb/171799
Feature compatibility	smarttech.com/kb/171722

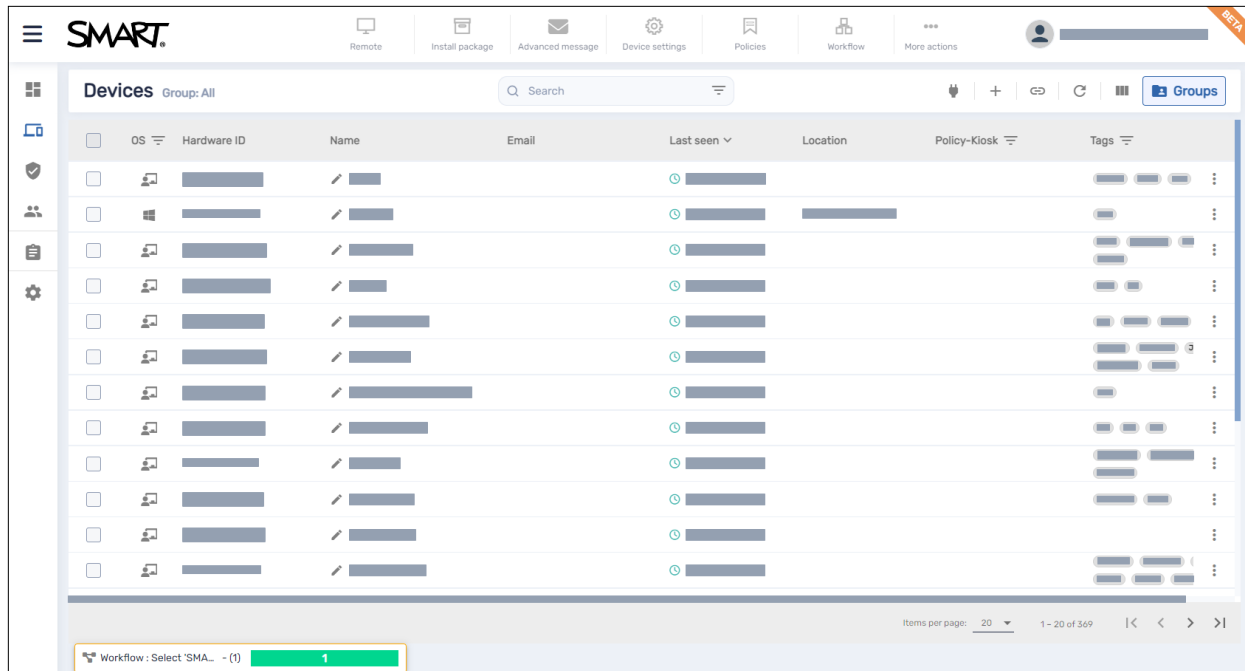
Scan the QR code on the inside front cover of this guide to view links to this documentation and other SMART Remote Management support resources.


Chapter 2 **Managing devices**

Monitoring devices	9
Showing and hiding columns	10
Finding devices	11
Using filters	12
Renaming devices	14
Identifying which devices are online	15
Viewing device details	15
Locating devices	17
Exporting device details to CSV files	18
Using tags and groups	19
Using tags	19
Using groups	22
Remotely viewing and controlling devices	24
Connecting to devices using the Terminal feature	26
Removing devices	27

Monitoring devices

The *Devices* view displays information about all devices enrolled in SMART Remote Management for which you have access. It is the main view in SMART Remote Management for monitoring and managing devices.

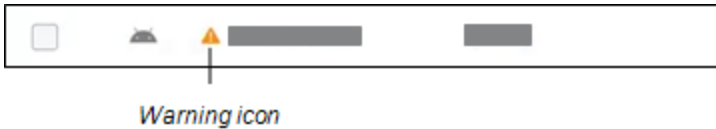


To open the *Devices* view from anywhere in SMART Remote Management, click **Devices**  in the menu. In the *Devices* view, you can:

- Show and hide columns
- Filter devices
- Identify which devices are online
- View device details
- Locate devices
- Export device details to CSV files

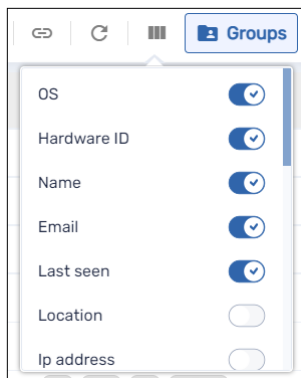
! **Important**

If a warning icon appears next to a device's ID, you need to reset the device's authentication token. Click the icon to learn more and reset the device's authentication token.



Showing and hiding columns

You can choose which columns appear in the *Devices* view by clicking **Columns** . Enable columns you want to show, and disable columns you want to hide:



Typically, you'd want to show these columns for SMART Board interactive displays with iQ:

Column	Description	Notes
OS	An icon representing the device's type (operating system)	For SMART Board interactive displays with iQ, the icon is .
Hardware ID	A unique identifier assigned by the device's manufacturer	For SMART Board interactive displays with iQ, the unique identifier is the same as the display's serial number.
Name	A name you give to the device to identify it in SMART Remote Management	For more information about changing a device's name, see <i>Renaming devices</i> on page 14.
Last seen	The date and time the device was last active	[N/A]

Column	Description	Notes
Policy-Kiosk	Any policies applied to the device	For more information about policies, see <i>Deploying policies</i> on page 51.
Tags	Any tags applied to the device	For more information about tags, see <i>Using tags</i> on page 19.
SMART Build Number	The build number of iQ software running on the SMART Board interactive display	For devices other than SMART Board interactive displays with iQ, this column is blank.

Tips

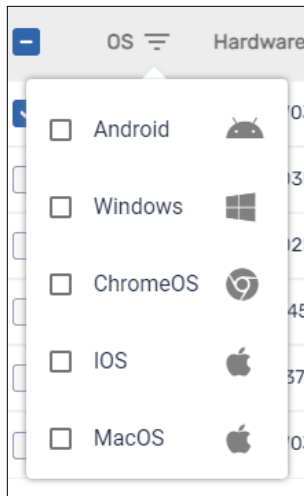
- You can sort devices by clicking the **Last Seen** column header.
- You can change the order of columns by dragging a column's header to its new position.
- You can filter the list of devices based on values in some columns (see *Finding devices* below).

Finding devices

To find a specific device or devices quickly, filter the devices in the *Devices* view in one of the following ways:

- Use the *Search* bar at the top of the *Devices* view

- Use column filtering.



Notes

- Column filtering is available for the *OS*, *Policy-Kiosk*, and *Tags* columns.
 - For the OS column, selecting **Android** displays all SMART Board interactive display and Android devices, not just Android devices.
- Use filters (see *Using filters* below)
 - Use groups (see *Using groups* on page 22)

Using filters

You can use filters to filter devices in the *Devices* view and run commands on all devices that meet filter criteria. You can create and save a filter for future use, or you can create a one-time quick filter.

Tip

Filters are useful when applying policies to a group of devices. Because policies are created for specific operating systems, create a filter for devices that have the same operating system. For more information about policies, see *Deploying policies* on page 51.

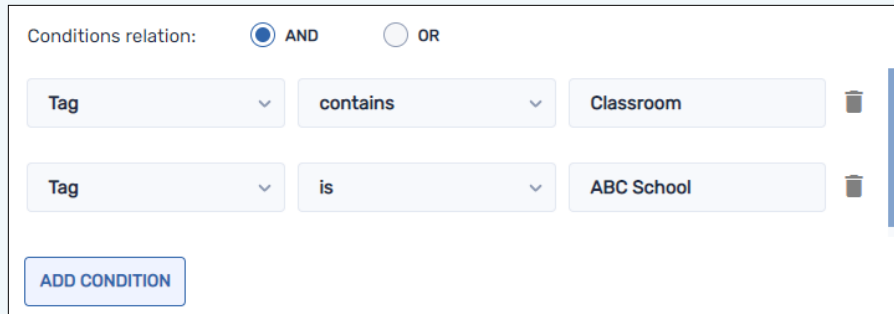
To create and save a filter

1. Click **Filters** .
2. Create the conditions for the filter.

Note

Click **ADD CONDITION** to add multiple conditions as needed.

Example



The screenshot shows a filter configuration window. At the top, it says 'Conditions relation:' with two radio buttons: 'AND' (selected) and 'OR'. Below this are two rows of conditions. The first row has a dropdown menu with 'Tag' selected, followed by a dropdown menu with 'contains' selected, and a text input field with 'Classroom'. To the right of the text input is a trash icon. The second row has a dropdown menu with 'Tag' selected, followed by a dropdown menu with 'is' selected, and a text input field with 'ABC School'. To the right of the text input is a trash icon. At the bottom left of the window is a blue button labeled 'ADD CONDITION'.

3. Click **SAVE FILTER**.
The *Save filter* window appears.
4. Type a name in the *Filter name* box.
5. (Optional) Select the following options for the filter:


Option	Description
Set as private	Make this filter available only to you.
Select color	Assign a color to the filter's icon.
Select icon	Assign an icon to the filter.

6. Click **SAVE**.

Tip

You can edit the filter by selecting it in the list, modifying its conditions, and clicking **EDIT FILTER**.

To filter devices using filters

1. Click **Filters** .
2. Select the saved filter you want to use.

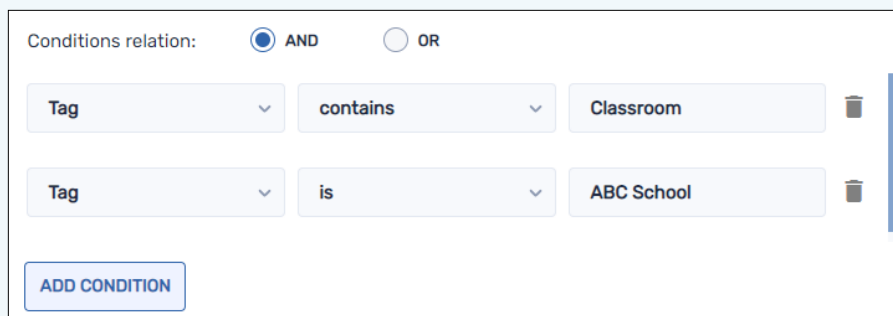
OR

Create the conditions for a one-time quick filter and click **QUICK SEARCH**.


Note


Click **ADD CONDITION** to add multiple conditions as needed.

Example



Conditions relation: AND OR

Tag contains Classroom 



Tag is ABC School 

ADD CONDITION

3. Click outside the filter drop-down menu.

The devices that meet the filter's criteria appear in the *Devices* view.

To run a command on all devices that meet a saved filter's criteria

1. Click **Filters** .
2. Click **Actions**  next to a saved filter and select the command you want to run on the devices that meet the filter's criteria.

Tip



You can pin a frequently used command to the top of the menu by hovering over it and clicking

Pin to favorites .


Renaming devices

You may need to change a device's name if its current name doesn't accurately describe its status or purpose. You can rename devices from the *Devices* view.



To rename a device

1. Click **Edit device name**  beside the device's name.
2. Type a new name for the device and click **save changes** .

Tips

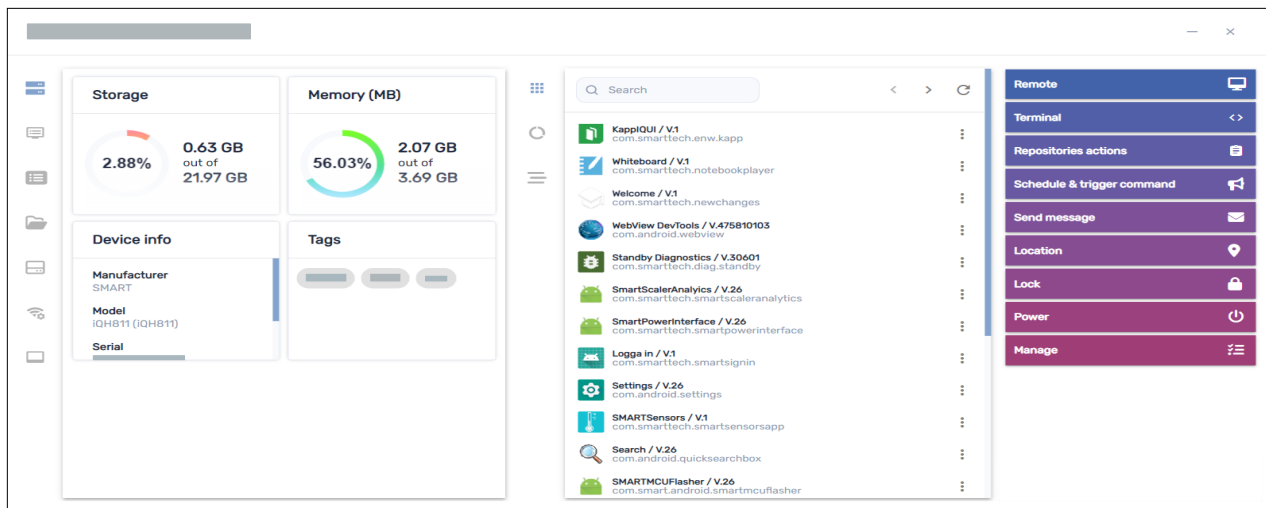
- To revert to the existing name, click **cancel** .
- You can also rename a device from the device dashboard (see *Viewing device details* below) by clicking **Manage** and then **RENAME**.

Identifying which devices are online

You can quickly identify which devices are online by clicking **Who is online?**  in the *Devices* view. The OS icon for any online devices turns blue (.

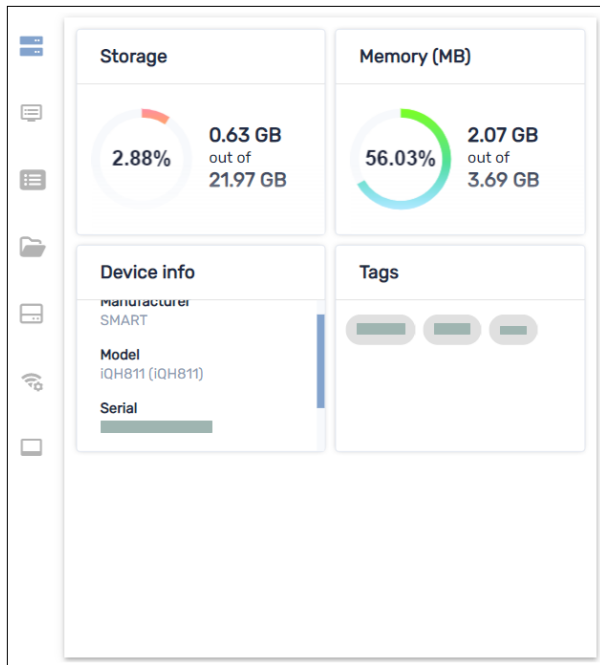
Viewing device details

When you click a device's row in the *Devices* view, a device dashboard similar to this appears:


















From this dashboard, you can view general information about the device, see a list of apps installed on the device, and device usage. The device dashboard also offers management tools, such as starting a remote session, applying settings and policies, and more.

The general details section on the dashboard's left side shows you device information, such as memory, storage, resolution, battery life, and more.





Click the other tabs to see additional information for the device:

Icon	Tab	Description						
	Info	More details about the device, such as Wi-Fi, IP address, Bluetooth availability, model number, operating system version, MAC address, permissions, CPU, serial number, and time zone	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Properties	Properties for the device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	File system	Contents of the device's file system	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Storage stats	Storage statistics for the device	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Network	Network information, such as Wi-Fi state, Wi-Fi SSID, Wi-Fi allowed protocols, IP address, subnet mask, and more	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Icon	Tab	Description						
	Smartboard	Basic information about the SMART Board interactive display with iQ, such as information about the touch controller and scaler firmware version, display build number, and display name	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Bios	Information about the device's BIOS	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Processor	Information about the device's CPU	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Manufacture model	Information about the device's model	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Hot fixes	Information about Windows hot fixes applied to the device	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	OS	Information about the device's operating system	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Disks	Information about the device's hard drive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Logged on users	Information about users currently logged on to the device	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Browsing	the device's browsing history	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Tip

In the *Properties*, *File system*, *Storage stats*, and *Browsing* tabs, you can do the following:

- Search for specific information using the *Search* box.
- Export information to a CSV file by clicking **Export to CSV** .
- Display the information in the tab in an expanded view by clicking **Expand** .

Locating devices

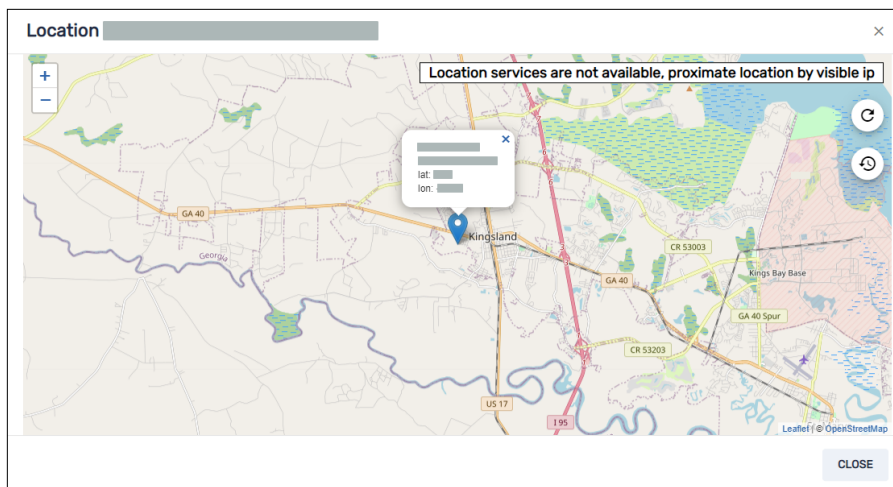
You can see a device's current location from the *Devices* view. This is particularly useful for finding mobile devices.

Notes

- Before SMART Remote Management can locate a device, you must set up the network as described in the *SMART Remote Management setup guide* (smarttech.com/kb/171333).
- If location services are not available, SMART Remote Management shows an approximate location for the device based on its IP address.

To locate a device

1. Click the row of the device you want to locate.
The device's dashboard window appears.
2. Click **Location** to open the *Location* window.

**Exporting device details to CSV files**

From the *Devices* view, you can create a CSV file with the following information for selected devices:

- The unique identifier assigned by the device's manufacturer
- The device's current location (by latitude and longitude)
- Whether the device is locked
- An email account associated with the device
- The device's IMEI
- The date and time the device was last active
- The device's type (operating system)
- The device's name

- Tags applied to the device (see *Using tags* below)
- The device's serial number
- The device's operating system version
- The device's model
- Permissions for the device
- The public and local IP addresses for the device
- The device's SIM
- The device's Wi-Fi network
- The build number of iQ software running on the device (if it is a SMART Board interactive display with iQ)

To export a CSV file

1. Select the check boxes of the devices you want to include in the CSV file.
2. Click **More actions** *** and select **Export to CSV**.
Your browser downloads a CSV file from SMART Remote Management.
3. Open the CSV file in a spreadsheet application.

Using tags and groups

You can use tags and groups to organize devices in SMART Remote Management.

Using tags

Tags are a way of classifying devices enrolled in SMART Remote Management. For example, you could use tags to identify:

- Which devices are SMART Board interactive displays, which are computers, and which are mobile devices
- Where devices are located
- The intended purposes of the devices
- The department, team, or group that uses the devices

Tip

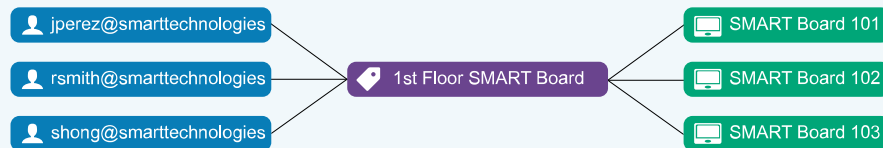
You can assign more than one tag to a device.

Assigning tags to devices is a prerequisite for creating groups (see *Using groups* on page 22). You can also use tags, along with groups, to filter devices in the *Devices* view (see *Finding devices* on page 11).

You can also assign tags to SMART Remote Management users to control which devices and other users those users can access in SMART Remote Management.


Example

If you assign the tag “1st Floor SMART Board” to the users `jperez@smarttechnologies`, `rsmith@smarttechnologies`, and `shong@smarttechnologies`, those users can only access devices with the tag “1st Floor SMART Board,” and they can only access each other and not other SMART Remote Management users:



Typically, you assign tags to devices when you first enroll those devices in SMART Remote Management. After enrolling devices, you can also assign tags to them in the *Devices* view.

To add tags to a single device

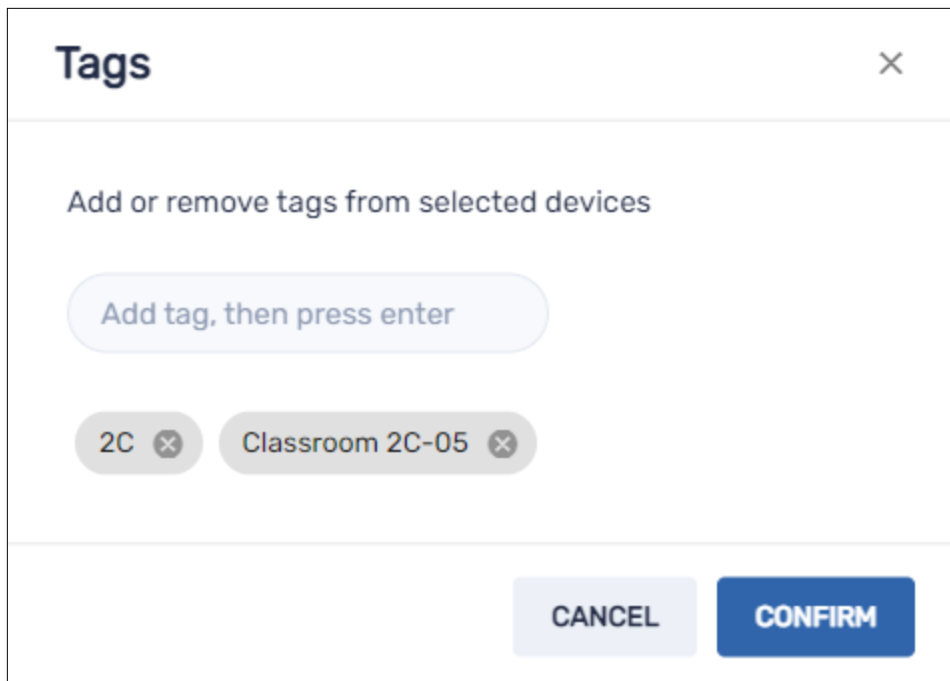
1. Click **Devices**  to open the *Devices* view.
2. Click the row of the device to which you want to add a tag.

The device’s dashboard window appears.

3. Click **Manage**, and then click **TAGS**.

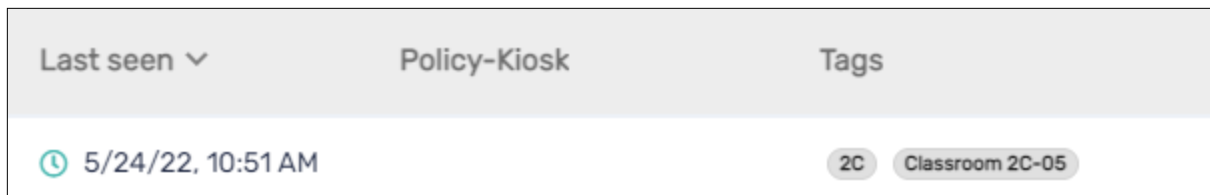
The *Tags* window appears.

4. For each tag you want to add to the device, type a name for the tag in the *Add tag, then press enter* box and press ENTER.





5. Click **CONFIRM**.

You'll see the tags added for the device in the *Tags* column.



To assign tags to multiple devices

1. Click **Devices**  to open the *Devices* view.
2. Select the devices' check boxes.
3. Click **More actions**  and select **Tags**.
The *Tags* window appears.
4. For each tag you want to add to the devices, type the name for the tag in the *Add tag, then press enter* box and press ENTER.
5. Click **CONFIRM**.

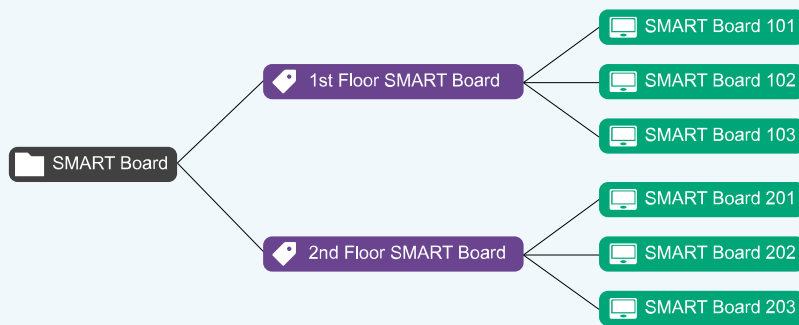
Using groups

Groups are a way of organizing devices enrolled in SMART Remote Management. By default, all enrolled devices are included in the All group, and any new devices you enroll are included in the New Devices group.

You can create additional groups using tags.

Example

If you create a group called “SMART Board” and assign it the tags “1st Floor SMART Board” and “2nd Floor SMART Board,” the group will contain all devices with those tags:



The relationship between tags and groups is many-to-many: You can assign multiple tags to a single group and a single tag to multiple groups. This allows you to create groups that are as simple or as complex as your organization needs.




Most of the commands you can run for a single device or multiple devices you can also run for a group. In addition, you can make commands persistent: if you assign a new device to a group in the future (by adding one of the group’s tags to the device), any persistent commands for that group run on the device automatically.

Note

For more information about making existing group commands persistent, see *Making group commands persistent* on page 103.

You can create, edit, and delete groups from the *Devices* view. When you create a group, you assign it at least one tag and, optionally, one or more installation packages. SMART Remote Management automatically deploys a group’s installation packages to any devices you add to the group (by adding one of the group’s tags to the device).

To create a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Add new group** .
The *Create new group* window appears.
4. Type a name and description in the *Group name* and *Group description* boxes.
5. Click **Tags** .
6. For each tag you want to add to the device, type the name for the tag in the *Add tag, then press enter* box and press ENTER.

Note

You must assign at least one tag to the group.


7. (Optional) Click **Packages** , click **ADD PACKAGES**, select the installation packages you want to assign to the group, and click **UPDATE**.

Notes


- For information about creating installation packages, see *Installing apps* on page 28.
- Installation packages you assign to the group are persistent: if you assign a new device to the group in the future, SMART Remote Management deploys the installation packages to the device automatically.
- SMART Board interactive displays with iQ support persistent installation packages.
- Other devices require version 11.5.1.1 or later of the Viso MDM agent to support persistent installation packages.

8. Click **CONFIRM**.

Tip



To edit or delete an existing group, click **Actions**  in the group's row and select **Edit** or **Delete**. (You can't delete the All or New Devices groups.)

To filter devices using groups

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Select the group you want to use.

The devices that meet the group's criteria appear in the *Devices* view.

To run commands on all devices in a group







1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  next to a group and select the command you want to run on the devices in the group.

Tip

You can pin a frequently used command to the top of the menu by hovering over it and clicking

Pin to favorites .

Remotely viewing and controlling devices

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> ¹

You can use SMART Remote Management to start a remote view or control session with a device. You can see and interact with a device's screen as if you were in the room with the device. A remote view or control session is particularly useful when you need to help a user troubleshoot an issue with a device.

Whether you can remotely control a device or only view its screen depends on the following:

- The type of device

Type of device	Level of access
SMART Board interactive displays with iQ	View and control
SMART Board GX and MX100 series interactive displays and Android devices	View and control
Windows devices	View and control
Chrome OS devices	View only



- Whether you have permission to view or control devices remotely

Note


If the *Require users permission for remote control* option is enabled as described below, the user must grant permission before you can interact with the device.

¹Remote view only

To require user permission before starting a remote view or control session

1. Click **Account settings**  .
The *Account settings* window appears.
2. Click **Remote control**  .
3. Enable **Require users permission for remote control**.
4. Click **SAVE**.

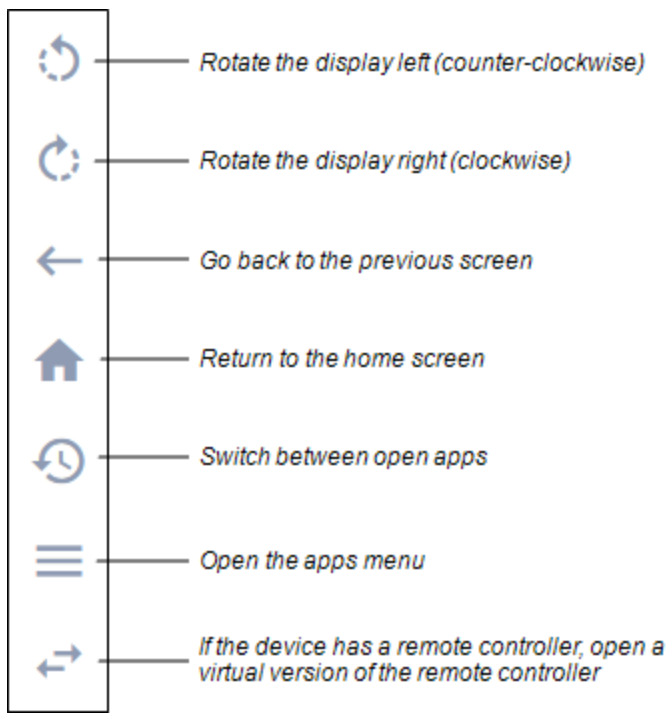
To start a remote view or control session

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Remote**.

The remote window appears, and you can view or control the device.

Tip





Use the buttons on the left side of the window to navigate the device:



To end a remote view or control session

Click the X in the top right corner of the remote window.

Connecting to devices using the Terminal feature


					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

You can use SMART Remote Management's Terminal feature to open direct Android Debug Bridge (ADB) shell connections to SMART Board interactive displays and Android devices. This allows you to remotely execute commands and pull logs in real time.

Important

The Terminal feature is available only on request. Contact a SMART representative if you would like to enable the Terminal feature for your organization.

To connect to a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.



The device's dashboard window appears.

4. Click **Terminal**.

The *Terminal* window appears.

5. Use the *Terminal* window to connect to the device and enter commands.

Tips

- To run the terminal session as a system administrator, click **Enable run as system** .
- To download a log file for the terminal session, click **Get log** , and then click the link that appears in the *Terminal* window.


6. Click **CLOSE** when you're done.

Removing devices

You may need to remove a device from SMART Remote Management for a number of reasons:

- You are replacing the device (as part of SMART's RMA program or otherwise)
- You no longer need to monitor, manage, or control the device remotely

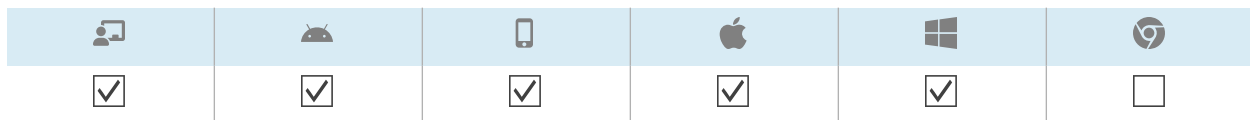
To remove a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Manage**, and then click **REMOVE**.
5. Click **YES**.

Chapter 3 Installing and managing apps on devices

Installing apps	28
Creating installation packages	29
Deploying installation packages	32
Creating an activation command	33
Unsupported apps for SMART Board interactive displays with iQ	34
Enabling, disabling, and stopping apps	35
Enabling apps	35
Disabling apps	36
Stopping apps	38
Clearing app data	39
Uninstalling apps	40
Installing and uninstalling apps on iOS and macOS devices using VPP	42
Viewing app usage data	44

Installing apps



You can remotely install apps on devices using SMART Remote Management by completing these steps:

1. Create an installation package.
2. Deploy the installation package.
3. Create an activation command (if required).

! **Important**





- For SMART Board interactive displays with iQ:
 - Review the list of unsupported apps (see *Unsupported apps for SMART Board interactive displays with iQ* on page 34).
 - Different SMART Board interactive displays with iQ support different Android versions:

Displays	Supported Android version
Displays with AM30 appliances	4.4
Displays with AM40 and AM50 appliances	7.1
SMART Board MX (V2), 6000S, 7000 (V2), and 7000R series interactive displays	8


- Install apps only from sources that you trust.
- Take care when installing apps that change Wi-Fi settings, Ethernet settings, VPNs, and alarms.
- Review required permissions for apps before installing them. For SMART Board interactive displays and Android devices, visit the Android developer site (developer.android.com/guide/topics/permissions/overview#perm-groups) for app permission guidelines.
- Test apps before installing them.
- Some apps depend on other apps and will not run unless other packages are deployed first.

Creating installation packages


The first step in using SMART Remote Management to install an app is to create an installation package for the app. The procedure for creating an installation package depends on the app's source:

Source						
Online file	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File saved on your computer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Google Play™ app	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
iOS enterprise app	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


To create an installation package using an online file

1. Click **Repositories**  and select **Packages**.
The *Packages* window appears.
2. Click **ADD NEW**.
3. Select **File from Url** from the *Select upload method* drop-down list.
4. Type the file's URL in the *File url* box.
5. Type a name and description in the *Repository name* and *Package description* boxes.
6. (Optional) Type appropriate values in the remaining boxes.
7. Click **CONFIRM**.

To create an installation package using a file saved on your computer

1. Click **Repositories**  and select **Packages**.
The *Packages* window appears.
2. Click **ADD NEW**.
3. Select **Upload file** from the *Select upload method* drop-down list.
4. Click **ADD FILE**.
5. Browse to and select the file, and click **Open**.
The file uploads and the *Repository name* box updates to include the file name.
6. Type a description in the *Package description* box.
7. (Optional) Type appropriate values in the remaining boxes.
8. Click **CONFIRM**.

To create an installation package using a Google Play app

1. Click **Repositories**  and select **Packages**.
The *Packages* window appears.
2. Click **ADD NEW**.
3. Select **Package from play store** from the *Select upload method* drop-down list.
4. Click **Play store**.
The Google Play store opens in a separate browser tab.
5. Search or browse for the app you'd like to use.

6. Copy the webpage's URL from the address bar.

Example

The URL to the WPS Office app is

`https://play.google.com/store/apps/details?id=cn.wps.moffice_eng`.

7. Return to the SMART Remote Management tab and paste the URL you copied in step 4 in the *Copy app URL from Play store* box.
8. Select the country where the devices on which you want to install the app are located in the *Select country* drop-down list.
9. Select the type of device in the *Device type* drop-down list.

Note

For SMART Board interactive displays, select **Interactive flat panel (Android)**.

10. Click **SYNC**.
11. (Optional) Modify the name and description in the *Repository name* and *Package description* boxes.
12. (Optional) Modify the values in the remaining boxes.
13. Click **CONFIRM**.

To create an installation package using an iOS enterprise app

1. Click **Repositories**  and select **Packages**.

The *Packages* window appears.

2. Click **ADD NEW**.
3. Select **iOS enterprise application** from the *Select upload method* drop-down list.

4. Complete one of the following procedures (based on the file’s source):

Source	Procedure
Online file	<ol style="list-style-type: none"> Select File from Url from the second <i>Select upload method</i> drop-down list. Type the file’s URL in the <i>File url</i> box. Type a name, description, and version in the <i>Repository name</i>, <i>Package description</i>, and <i>Package version number</i> boxes. (Optional) Type appropriate values in the remaining boxes.
File saved on your computer	<ol style="list-style-type: none"> Select Upload file from the second <i>Select upload method</i> drop-down list. Click ADD FILE. Browse to and select the file, and click Open. The file uploads and the <i>Repository name</i> box updates to include the file name. Type a description and version in the <i>Package description</i> and <i>Package version number</i> boxes. (Optional) Type appropriate values in the remaining boxes.


5. Click **CONFIRM**.

Deploying installation packages

You can deploy an installation package to a single device, multiple devices, all devices that match a saved filter’s criteria, or a group. Alternatively, you can:

- Assign the installation package to a group so the package is automatically deployed to devices added to the group (see *Using tags and groups* on page 19).
- Use a trigger to initiate the deployment of the installation package at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the deployment of the installation package in a workflow (see *Managing workflows* on page 118).

To deploy an installation package to a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device’s row.


The device’s dashboard window appears.

4. Click **Repositories actions**, and then click **INSTALL PACKAGES**.

The *Install package* window appears.

5. Select the installation package from the list and click **APPLY**.

To deploy an installation package to multiple devices




1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.

4. Click **Install package** .

The *Install package* window appears.

5. Select the installation package from the list and click **APPLY**.



To deploy an installation package to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Install package**.

The *Install package* window appears.

4. Select the installation package from the list and click **APPLY**.

To deploy an installation package to a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Install package**.

The *Install package* window appears.

4. Select the installation package from the list and click **APPLY**.

Creating an activation command

If an app requires activation and supports centralized activation, you can create a command or script in SMART Remote Management to activate it on the device (see *Sending remote execution commands and scripts to SMART Board interactive displays and Android and Windows devices* on page 66).

! **Important**

For SMART Notebook[®] software, provisioning email addresses is the recommended method for activating. To learn more about this and the differences between activation methods, see [Determining the best activation method](#).

Notes

- Not all SMART software, such as SMART Ink[®] and Product Drivers, requires activation.
- Commands for activating SMART software are provided in the products' system administrator or deployment guides. Refer to the *Documents* page on support.smarttech.com.







Unsupported apps for SMART Board interactive displays with iQ

Some apps can cause issues with SMART Board interactive displays with iQ and are not supported on these displays as a result:

Unsupported apps	Issues
Launchers	Launcher apps can interfere with the home screen app and cause the Input, Screen Share, and SMART Notebook Player apps to stop working.
Web browsers	Third-party web browsers allow users to download APKs and other files from the internet. Pages that are visited are not added to the home screen recent list.
File managers	File managers can allow access to hidden system files and settings.
Keyboards	Third-party keyboards can cause a wide variety of issues with the iQ experience.
Setup wizards, system setting tuners, and apps that allow the system to be rooted	These apps grant access to the operating system and can cause a wide variety of issues.
Online music players	Online music players can operate in the background. The interface is hidden and you can't stop unintended music from playing.
Apps requiring Google Play Services	Google [™] policies do not permit Google Play Services to be used on interactive display products. Apps requiring Google Play Services will not run on SMART Board interactive displays with iQ, and attempts to do so could cause problems.
Apps with GPS	Hardware limitations prevent apps from working.
Apps with NFC	Hardware limitations prevent apps from working.
Apps with Bluetooth [®] LE (low energy)	SMART Board interactive displays with iQ use Bluetooth LE, and apps that require Bluetooth LE will cause issues.

Unsupported apps	Issues
Apps that require portrait orientation	Apps that require portrait orientation don't fit the landscape screen. Install only apps that allow landscape orientation.

Enabling, disabling, and stopping apps

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Three common app management activities are enabling, disabling, and stopping apps. You can complete these activities—as well as clearing app data (see *Clearing app data* on page 39) and uninstalling apps (see *Uninstalling apps* on page 40)—for a single device from the device's dashboard.

You can also enable and disable apps using SMART Remote Management commands.


Enabling apps

Apps are enabled by default. If you or another administrator disabled apps on one or more devices (see *Disabling apps* on the next page), you can re-enable them from SMART Remote Management.

You can enable apps on a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the enabling of apps at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the enabling of apps in workflows (see *Managing workflows* on page 118).





To enable apps on a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.




The device's dashboard window appears.

4. For each app you want to enable, click  in the app's row and select **Enable app**.




To enable apps on all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Enable apps**.
The *Enable apps* window appears.
4. Click **Add to list**  for each app you want to enable.
5. Click **ENABLE**.

To enable apps on multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Enable apps**.
The *Enable apps* window appears.
5. Click **Add to list**  for each app you want to enable.
6. Click **ENABLE**.

To enable apps in a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Enable apps**.
The *Enable apps* window appears.
4. Click **Add to list**  for each app you want to enable.
5. Click **ENABLE**.

Disabling apps

If you want to prevent users from using an app but don't want to remove the app entirely from devices, you can disable the app from SMART Remote Management.



You can disable apps on a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the disabling of apps at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the disabling of apps in workflows (see *Managing workflows* on page 118).




Important

Take care when disabling an app because devices might not work correctly without the app.




To disable apps on a single device


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. For each app you want to disable, click  in the app's row and select **Disable app**.

To disable apps on multiple devices



1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Disable apps**.
The *Disable apps* window appears.
5. Click **Add to list**  for each app you want to disable.
6. Click **DISABLE**.

To disable apps on all devices that match a saved filter's criteria


1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Disable apps**.
The *Enable apps* window appears.

4. Click **Add to list**  for each app you want to disable.
5. Click **DISABLE**.

To disable apps in a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Disable apps**.

The *Disable apps* window appears.

4. Click **Add to list**  for each app you want to disable.
5. Click **DISABLE**.



Stopping apps

You can stop any apps currently running on a device from SMART Remote Management. This is particularly useful when you are working with users to troubleshoot issues with their devices.







Important

Take care when stopping an app because devices might not work correctly without the app.

To stop apps

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. For each app you want to stop, click  in the app's row and select **Stop app**.

Clearing app data

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

You can clear app data using SMART Remote Management. This is particularly useful when you are working with users to troubleshoot issues with their devices.



Important

Take care when clearing app data because apps might not work as expected after data is cleared.




You can clear app data on a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the clearing of app data at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the clearing of app data in workflows (see *Managing workflows* on page 118).





To clear app data on a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. For each app for which you want to clear data, click  in the app's row and select **Clear app data**.





To clear app data on multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Clear apps data**.
The *Clear apps data* window appears.
5. Click **Add to list**  for each app for which you want to clear data.
6. Click **CLEAR**.




To clear app data on all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Clear apps data**.
The *Clear apps data* window appears.
4. Click **Add to list**  for each app for which you want to clear data.
5. Click **CLEAR**.

To clear app data on a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups**  to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Clear apps data**.
The *Clear apps data* window appears.
4. Click **Add to list**  for each app for which you want to clear data.
5. Click **CLEAR**.

Uninstalling apps

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

On occasion, you might need to uninstall one or more apps on a single device or multiple devices. You can do this from SMART Remote Management.



You can uninstall apps on a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the removal of apps at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the removal of apps in workflows (see *Managing workflows* on page 118).




Important

Take care when uninstalling an app because devices might not work correctly without the app.





To uninstall apps on a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. For each app you want to uninstall, click  in the app's row and select **Uninstall app**.



To uninstall apps on multiple devices


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Uninstall packages**.
The *Uninstall packages* window appears.
5. Click **Add to list**  for each app you want to uninstall.
6. Click **UNINSTALL**.

To uninstall apps on all devices that match a saved filter's criteria

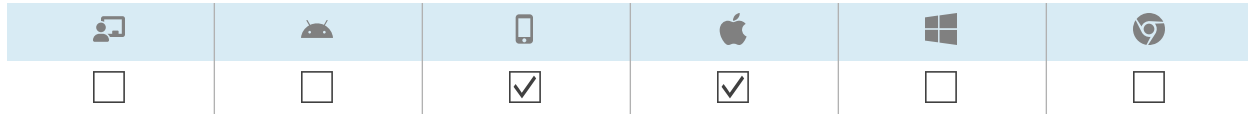
1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Uninstall package**.
The *Uninstall packages* window appears.
4. Click **Add to list**  for each app you want to uninstall.
5. Click **UNINSTALL**.

To uninstall apps on a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Uninstall packages**.
The *Uninstall packages* window appears.

4. Click **Add to list**  for each app you want to uninstall.
5. Click **UNINSTALL**.

Installing and uninstalling apps on iOS and macOS devices using VPP



Apple School Manager and Apple Business Manager are online services that include the ability to install and uninstall apps on your organization’s iOS and macOS devices in SMART Remote Management and other mobile device management software.

Note

Apple School Manager and Apple Business Manager replace the Volume Purchase Program (VPP). However, the term “VPP” is still used in SMART Remote Management and in this documentation.

For more information on these Apple programs, see [Getting started using Apple Business Manager or Apple School Manager with mobile device management](#).


To use these Apple programs with SMART Remote Management to install or uninstall apps, follow these three steps:


1. If you haven’t already, enroll in the appropriate program for your organization:

Program	Link
Apple School Manager	school.apple.com
Apple Business Manager	business.apple.com



2. Add a VPP account to SMART Remote Management as described in the *SMART Remote Management setup guide* (smarttech.com/kb/171333).
3. Install or uninstall apps on a single device, multiple devices, or a group.

To install or uninstall apps on a single device




1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).

3. Click **Actions**  in the device's row and select **VPP install/uninstall**.
The *VPP install* window appears.
4. Select the VPP account in the *Select VPP account* drop-down list.
5. Select **Install** or **Uninstall**.
6. Use the remaining controls to select the apps you want to install or uninstall and set options for those apps.
7. Click **CONFIRM**.



To install or uninstall apps on multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **VPP install/uninstall**.
The *VPP install* window appears.
5. Select the VPP account in the *Select VPP account* drop-down list.
6. Select **Install** or **Uninstall**.
7. Use the remaining controls to select the apps you want to install or uninstall and set options for those apps.
8. Click **CONFIRM**.







To install or uninstall apps on all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **VPP install/uninstall**.
The *VPP install* window appears.
4. Select the VPP account in the *Select VPP account* drop-down list.
5. Select **Install** or **Uninstall**.
6. Use the remaining controls to select the apps you want to install or uninstall and set options for those apps.
7. Click **CONFIRM**.

To install or uninstall apps on a group

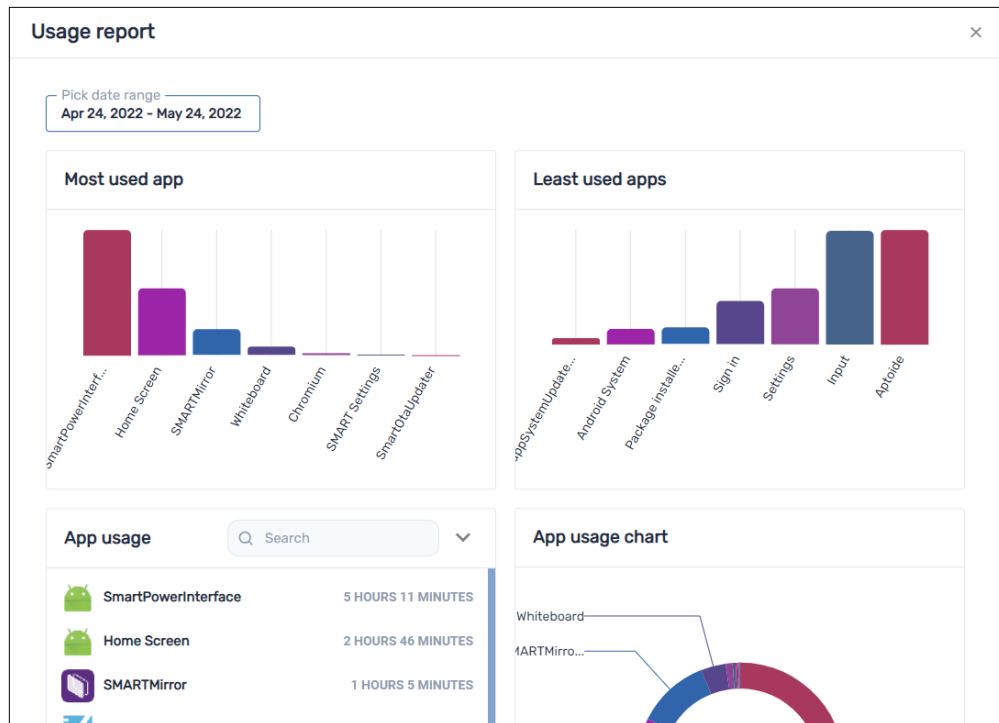
1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **VPP install/uninstall**.
The *VPP install* window appears.
4. Select the VPP account in the *Select VPP account* drop-down list.
5. Select **Install** or **Uninstall**.
6. Use the remaining controls to select the apps you want to install or uninstall and set options for those apps.
7. Click **CONFIRM**.

Viewing app usage data

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

You can view apps currently running on a device and detailed app information for the device using SMART Remote Management.

Alternatively, you can create an app usage report for a single device, multiple devices, all devices that match a saved filter's criteria, or a group. This report displays app usage data, including the most- and least-used apps on the devices. Usage data is helpful for determining which apps are being used in your organization and which aren't and can be either disabled (see *Disabling apps* on page 36) or uninstalled (see *Uninstalling apps* on page 40).



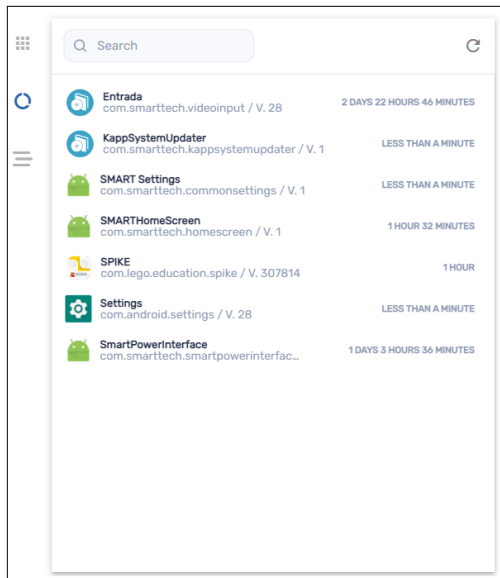
To view apps currently running on a device

1. Click **Devices** to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.


The device's dashboard window appears.

4. Click **Usage** .

A list of all apps currently running on the device appears.



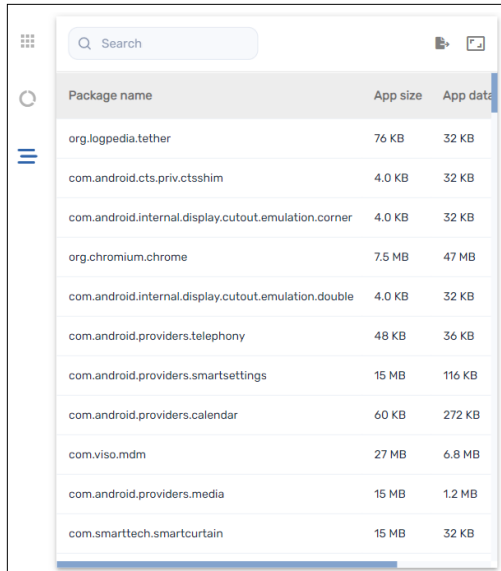
To view detailed app information for a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.

The device's dashboard window appears.

4. Click **Advanced stats** .



A table with detailed app information for the device appears.





Package name	App size	App data
org.logpedia.tether	76 KB	32 KB
com.android.cts.priv.ctsshim	4.0 KB	32 KB
com.android.internal.display.cutout.emulation.corner	4.0 KB	32 KB
org.chromium.chrome	7.5 MB	47 MB
com.android.internal.display.cutout.emulation.double	4.0 KB	32 KB
com.android.providers.telephony	48 KB	36 KB
com.android.providers.smartsettings	15 MB	116 KB
com.android.providers.calendar	60 KB	272 KB
com.viso.mdm	27 MB	6.8 MB
com.android.providers.media	15 MB	1.2 MB
com.smarttech.smartcurtain	15 MB	32 KB

Tip

You can do the following:

- Search for specific information using the *Search* box.
- Export information to a CSV file by clicking **Export to CSV** .
- Display the information in the tab in an expanded view by clicking **Expand** .

To create an app usage report for a single device




1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click **Actions**  in the device's row and select **App usage report**.

The app usage report for the device appears. By default, the report displays app usage data for the last month.



4. (Optional) Change the report's start and end dates using the calendar.

Tip

In the *App usage* section of the report, you can do the following:

- Search for specific information using the *Search* box.
- Export information to a CSV file by clicking **Export to CSV** .
- Sort the list of apps by clicking **Sort ascending**  or **Sort descending** .

To create an app usage report for multiple devices




1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **App usage report**.

The app usage report for the devices appears. By default, the report displays app usage data for the last month.




5. (Optional) Change the report's start and end dates using the calendar.

Tip

In the *App usage* section of the report, you can do the following:

- Search for specific information using the *Search* box.
- Export information to a CSV file by clicking **Export to CSV** .
- Sort the list of apps by clicking **Sort ascending**  or **Sort descending** .

To create an app usage report for all devices that match a saved filter's criteria




1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **App usage report**.

The app usage report for the devices appears. By default, the report displays app usage data for the last month.



4. (Optional) Change the report's start and end dates using the calendar.

Tip

In the *App usage* section of the report, you can do the following:

- Search for specific information using the *Search* box.
- Export information to a CSV file by clicking **Export to CSV** .
- Sort the list of apps by clicking **Sort ascending**  or **Sort descending** .

To create an app usage report for a group




1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **App usage report**.

The app usage report for the devices appears. By default, the report displays app usage data for the last month.

4. (Optional) Change the report's start and end dates using the calendar.

Tip

In the *App usage* section of the report, you can do the following:

- Search for specific information using the *Search* box.
- Export information to a CSV file by clicking **Export to CSV** .
- Sort the list of apps by clicking **Sort ascending**  or **Sort descending** .

Chapter 4 Deploying policies and managing settings

About policies and settings	50
Deploying policies	51
Deploying kiosk policies	54
Managing settings	57
Managing settings	57
Locking settings for SMART Board interactive displays with iQ	60
Returning devices to factory settings and resetting their authentication tokens	63
Returning devices to factory settings	63
Resetting devices' authentication tokens	63







About policies and settings







You can control users' access to apps and websites on devices by deploying policies to those devices. You can also manage device settings remotely.

SMART Remote Management includes three repository item types you use for deploying policies and managing settings:

- Policies
- Kiosk
- Device settings

This table defines the purpose of these repository item types and the device types each supports:







Repository item type	Purpose						
Policies	Control what users can and can't do on devices	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Repository item type	Purpose						
Kiosk	Set devices as kiosks (devices with limited user control, such as information terminals in shopping malls and other public places) and control what users can and can't do on kiosks	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device settings	Manage device settings remotely	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Notes

- For SMART Board interactive displays with iQ, you can lock settings by deploying a policy (see *Locking settings for SMART Board interactive displays with iQ* on page 60).
- For SMART Board GX and MX100 series interactive displays and Android devices, you can add settings to a policy (see *Deploying policies* below). This allows you to deploy policies and manage settings in a single step.


Deploying policies

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>














You can deploy policies to your organization’s devices using SMART Remote Management. Policies control what users can and can’t do using your organization’s devices.

You can deploy a policy to a single device, multiple devices, all devices that match a saved filter’s criteria, or a group. Alternatively, you can use a trigger to deploy a policy at a scheduled time or when a specific event takes place (for SMART Board GX and MX100 series interactive displays, Android devices, and Windows devices only).


To create a policy


1. Click **Repositories**  and select **Policies**.
The *Policies* window appears.
2. Click **ADD NEW** and select the type of device for which you want to create the policy.
3. Type a name and description in the *Policy name* and *Policy description* boxes.

4. Enter the appropriate information in the remaining tabs:

Icon	Tab	Description						
	Restrictions	Allow or block features of iOS	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Passcode	Enable or disable passcodes on iOS and macOS devices and set requirements for passcodes if enabled	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Content filter	Prevent access to adult content or allow or block specific website URLs	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Single app	Enable single app mode on iOS devices and select the app to use in this mode	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Block list	Allow or block apps	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Web	Allow or block websites	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Settings lockdown	Lock SMART Board interactive display with iQ settings (see <i>Locking settings for SMART Board interactive displays with iQ</i> on page 60)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


5. (Optional) For SMART Board GX and MX100 series interactive displays, Android devices, and Windows devices, use a trigger to start or stop the deployment of the policy (see *Managing schedulers and triggers* on page 104):

- a. Click **General** .
- b. Turn on **Activate policy by trigger**.
- c. Click **SELECT TRIGGER**.
The *Scheduler & triggers* window appears.
- d. Select the trigger from the list and click **APPLY**.

6. (Optional) For SMART Board GX and MX100 series interactive displays and Android devices, add settings to the policy (see *Managing settings* on page 57):
 - a. Click **General** .
 - b. Turn on **Add settings to policy**.
 - c. Click **SELECT SETTINGS**.

The *Settings* window appears.
 - d. Select the settings from the list and click **APPLY**.
7. Click **CONFIRM**.


To deploy a policy to a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.

The device's dashboard window appears.
4. Click **Repositories actions**, and then click **POLICIES**.


The *Policies* window appears.
5. Select a policy from the list and click **APPLY**.

To deploy a policy to multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the device's check boxes.

Note




Policies are created for specific device types, so select devices of the same type.

4. Click **Policies** .

The *Policies* window appears.

5. Select a policy from the list and click **APPLY**.

To deploy a policy to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Policies**.



The *Policies* window appears.

Note

Policies are created for specific device types, so select a filter with devices that are of the same type.

4. Select the policy from the list and click **APPLY**.

To deploy a policy to a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Policies**.







The *Policies* window appears.

Note

Policies are created for specific device types, so select a group with devices that are of the same type.

4. Select the policy from the list and click **APPLY**.

Deploying kiosk policies

					
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

A kiosk is a device with limited user control, such as information terminals in shopping malls and other public places. You can create policies for kiosks in SMART Remote Management that do the following:

- Set allowed apps for kiosks
- Specify which allowed app is the launcher app (in other words, the app that appears when users first interact with kiosks)

- Set allowed and blocked websites for kiosks
- Set a wallpaper (background) for kiosks






You can deploy a kiosk policy to a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can use a trigger to deploy a kiosk policy at a scheduled time or when a specific event takes place.


To create a kiosk policy

1. Click **Repositories**  and select **Kiosk**.


The *Kiosk* window appears.

2. Click **ADD NEW** and select the type of device for which you want to create the kiosk policy.
3. Type a name and description in the *Kiosk name* and *Kiosk description* boxes.
4. Enter the appropriate information in the remaining tabs:

Icon	Tab	Description		
	Allow list	Allow apps and select an allowed app as the launcher.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Web	Allow or block website URLs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Wallpaper	Set a wallpaper for the kiosk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

5. (Optional) Use a trigger to start or stop the deployment of the kiosk policy (see *Managing schedulers and triggers* on page 104):
 - a. Click **General** .
 - b. Turn on **Activate kiosk by trigger**.
 - c. Click **SELECT TRIGGER**.
The *Scheduler & triggers* window appears.
 - d. Select the trigger from the list and click **APPLY**.
6. Click **CONFIRM**.

To deploy a kiosk policy to a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.


The device's dashboard window appears.

4. Click **Repositories actions**, and then click **KIOSK**.

The *Kiosk* window appears.

5. Select a kiosk policy from the list and click **APPLY**.

To deploy a kiosk policy to multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the device's check boxes.

Note




Policies are created for specific device types, so select devices of the same type.

4. Click **More actions**  and select **Kiosk**.

The *Kiosk* window appears.

5. Select a kiosk policy from the list and click **APPLY**.

To deploy a kiosk policy to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Kiosk**.


The *Kiosk* window appears.

Note

Kiosk policies are created for specific device types, so select a filter with devices that are of the same type.

4. Select the kiosk policy from the list and click **APPLY**.

To deploy a policy to a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.

3. Click **Actions**  in the group's row and select **Kiosk**.

The *Kiosk* window appears.

Note







Kiosk policies are created for specific device types, so select a group with devices that are of the same type.

4. Select the kiosk policy from the list and click **APPLY**.

Managing settings

You can use SMART Remote Management to manage settings for SMART Board interactive displays and Android devices remotely. You can also lock access to settings from SMART Board interactive displays with iQ so that users do not inadvertently change them.

Managing settings

					
<input checked="" type="checkbox"/> ¹	<input checked="" type="checkbox"/> ²	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

To manage a device's settings remotely using SMART Remote Management, you need to first create settings in SMART Remote Management. You can then apply the settings to an individual device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to apply settings at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the application of settings in workflows (see *Managing workflows* on page 118).

Note

Not all SMART Board interactive display with iQ settings can be changed from SMART Remote Management. If there is a setting you want to be able to change from SMART Remote Management, [submit a feature request](#) to add this setting to a future version.

To create settings









1. Click **Repositories**  and select **Device settings**.

The *Device settings* window appears.

¹SMART Board interactive displays with iQ don't support all settings available in SMART Remote Management.


²SMART Board GX and MX100 series interactive displays don't support all settings available in SMART Remote Management.

2. Click **ADD NEW**.
3. Type a name and description in the *Name* and *Description* boxes.
4. Enter the appropriate information in the remaining tabs:

Icon	Tab	Description
	Wifi	<p>Enable Set device wifi to enter the device's Wi-Fi settings.</p> <p>Notes</p> <p>SMART doesn't recommend connecting SMART Board interactive displays with iQ to hidden networks using SMART Remote Management settings. If you do, you might need to apply settings twice to connect the display to the network successfully, particularly if the display is connected to the internet through Ethernet (rather than Wi-Fi).</p>
	Security	<p>Enable security settings you want to apply to the device, such as maximum allowed log in attempts, password settings, and so on.</p>
	General	<p>Control various settings for the device, such as allowing users to be added locally, volume adjustments, and so on.</p> <p>Tip</p> <p>Search for specific settings using the <i>Search</i> box at the top of the tab.</p>
	APN	<p>Turn on Access Point Name (APN) settings and enter APN details.</p>
	Wallpaper	<p>Set a wallpaper for the device.</p>
	Certificates	<p>Install certificates on the device. To do this</p> <ol style="list-style-type: none"> a. Turn on Install CA Certificate. b. Select one of the following from the <i>User certificate</i> drop-down list: <ul style="list-style-type: none"> o User trusted credentials o User wifi CA certificate o VPN and apps certificate c. If you selected User wifi CA certificate or VPN and apps certificate in step b, type the alias for the certificate in the <i>Certificate alias</i> box. d. Copy the body text of the certificate and paste it into the <i>CA certificate body</i> box.
	Smartboard settings	<p>Control general display settings, such as the apps visible in the display's apps library, whiteboard settings, and so on.</p>
	Lock screen	<p>Set a password and message for the device's lock screen.</p>

5. Click **CONFIRM**.

To apply settings to a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.


The device's dashboard window appears.

4. Click **Repositories actions**, and then click **DEVICE SETTINGS**.

The *Device settings* window appears.

5. Select the settings from the list and click **APPLY**.

To apply settings to multiple devices




1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.

4. Click **Device settings** .

The *Device settings* window appears.

5. Select the settings from the list and click **APPLY**.


To apply settings to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Device settings**.

The *Device settings* window appears.

4. Select the settings from the list and click **APPLY**.

To apply settings to a group

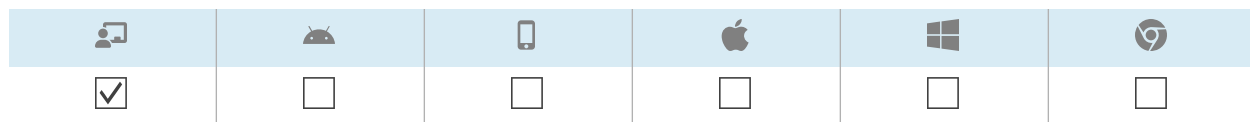
1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.

3. Click **Actions**  in the group's row and select **Device settings**.

The *Device settings* window appears.

4. Select the settings from the list and click **APPLY**.

Locking settings for SMART Board interactive displays with iQ



To lock access to settings on a SMART Board interactive display with iQ, connect a USB drive to a display and create a lockdown certificate. After you obtain the lockdown certificate, create a lockdown policy and apply it to a display, multiple displays, all displays that match a saved filter's criteria, or a group.

To create a lockdown policy

1. Connect a USB drive to a SMART Board interactive display with iQ and create a lockdown certificate (see [Locking down the iQ experience Settings app](#)).

2. Connect the USB drive to your computer.

3. Click **Repositories**  and select **Policies**.

The *Policies* window appears.

4. Click **ADD NEW** and select **Smartboard**.

The *New custom policy* window appears.

5. Type a name and description in the *Policy name* and *Policy description* boxes.

6. Click **Settings lockdown** .

7. Click the **Set key** slider to enable it.

8. Click **Add key** .

The *Open* window appears.

9. Browse to and select the .key file on the USB drive, and click **Open**.

10. Click **CONFIRM**.



To lock settings on a single display

1. Click **Devices**  to open the *Devices* view.




2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).

3. Click the display's row.
The display's dashboard window appears.
4. Click **Repositories actions**, and then click **POLICIES**.
The *Policies* window appears.
5. Select the lockdown policy from the list and click **APPLY**.

To lock settings on multiple displays

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the displays' check boxes.
4. Click **Policies** .
The *Policies* window appears.
5. Select the lockdown policy from the list and click **APPLY**.

To lock settings on all displays that match a saved filter's criteria


1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Policies**.
The *Policies* window appears.

Note

Select a filter that selects only SMART Board interactive displays with iQ.

4. Select the lockdown policy from the list and click **APPLY**.

To lock settings on a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.

3. Click **Actions**  in the group's row and select **Policies**.

The *Policies* window appears.







Note

Select a group that contains only SMART Board interactive displays with iQ.

4. Select the lockdown policy from the list and click **APPLY**.

Returning devices to factory settings and resetting their authentication tokens

Returning devices to factory settings


					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

You can return a device to its factory settings (or “wipe it”) as described below. Alternatively, you can use a trigger to initiate the wiping of a device at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).



Important

If you return a device to factory settings, the authentication token that was generated when you first enrolled the device will be lost. You will need to generate a new authentication token following the instructions in *Resetting devices’ authentication tokens* below.

To return a device to factory settings

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device’s row.
The device’s dashboard window appears.
4. Click **Lock** or **Power**, and then click **WIPE**.
5. Click **YES**.

Resetting devices’ authentication tokens

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>


For security reasons, the first handshake between a device and SMART Remote Management generates an authentication token. This token is stored on SMART Remote Management and on the device.

You can generate a new authentication token for a device if the original authentication token was lost. This is useful if you’ve performed a factory reset on the device and need to reconnect it to SMART Remote Management.

Note

If you've never enrolled a device in SMART Remote Management, it should not have an authentication token. However, in rare situations, such as when you receive a replacement SMART Board interactive display that was previously enrolled in SMART Remote Management on another domain, a device that you haven't enrolled in SMART Remote Management might have an authentication token. In these situations, contact SMART support (smarttech.com/contactsupport) to reset the device's authentication token.

To reset a device's authentication token







1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Manage**, and then click **RESET AUTH TOKEN**.
5. Click **RESET AUTH TOKEN**.

Chapter 5 Running other commands on devices

Sending custom commands and scripts to devices	66
Sending remote execution commands and scripts to SMART Board interactive displays and Android and Windows devices	66
Sending custom MDM commands to iOS and macOS devices	70
Sending files to devices	71
Sending messages and sounding the siren	74
Sending text-only messages	74
Sending advanced messages	76
Sounding the siren	78
Locking and unlocking devices	80
Locking and unlocking SMART Board GX and MX100 series interactive displays and Android, Windows, and Chrome OS devices	80
Locking and unlocking iOS and macOS devices	81
Restarting, shutting down, and waking devices	83
Restarting devices	83
Shutting down devices	84
Waking devices	86
Changing devices' agent passwords	88
Running device-type-specific commands	90
Removing Google accounts from Android devices	90
Deploying DEP profiles to iOS and macOS devices	92
Clearing passcodes from iOS and macOS devices	94
Retrieving the default password for Chrome OS devices	95

Sending custom commands and scripts to devices

Sending remote execution commands and scripts to SMART Board interactive displays and Android and Windows devices

					
<input checked="" type="checkbox"/> ¹	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>


You can create remote execution commands and scripts in SMART Remote Management and send them to devices for a variety of purposes, including:

- Enabling or disabling automatic over-the-air (OTA) updates on SMART Board interactive displays with iQ
- Activating software, such as SMART Notebook or SMART Meeting Pro[®], on computers

You can send remote execution commands and scripts to a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to send a remote execution command at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the sending of remote execution commands and scripts in workflows (see *Managing workflows* on page 118).

To create a remote execution command

1. Click **Repositories**  and select **Remote execute**.

The *Remote execute* window appears.

2. Click **ADD NEW**.

The *New remote execution* window appears.

3. Type a name in the *Name* box.
4. Select **Command line**.
5. Type the command in the *Command* box.
6. (Optional) Type arguments in the *Arguments* box.

¹SMART Board interactive displays with iQ don't fully support remote execution commands.

Example

This command enables automatic OTA updates on SMART Board interactive displays with iQ:

New remote execution ×

Name

Command

Arguments

Example

This command disables automatic OTA updates on SMART Board interactive displays with iQ:

New remote execution ×

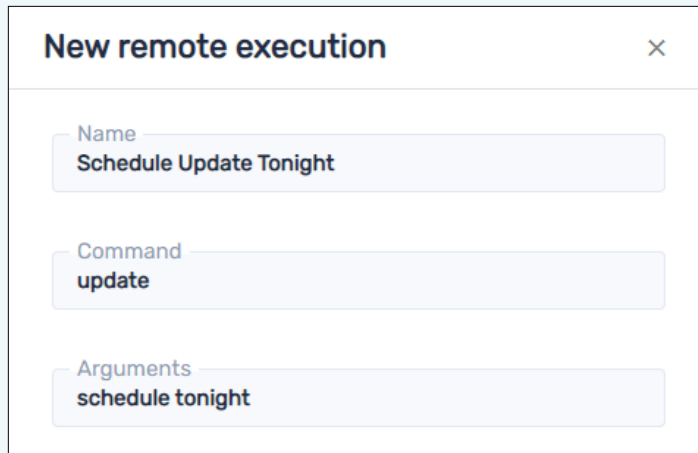
Name

Command

Arguments

Example

This command causes SMART Board interactive displays with iQ to check for OTA updates tonight:



The screenshot shows a dialog box titled "New remote execution" with a close button (X) in the top right corner. The dialog contains three input fields:

- Name:** Schedule Update Tonight
- Command:** update
- Arguments:** schedule tonight


Other schedule options:

- none (checks for OTA updates immediately)
- tomorrow night
- this weekend

7. Click **CONFIRM**.

The remote execution command is added to the repository.

To create a remote execution script

1. Click **Repositories**  and select **Remote execute**.

The *Remote execute* window appears.


2. Click **ADD NEW**.

The *New remote execution* window appears.



3. Type a name in the *Name* box.
4. Select **Script**.
5. Type the script in the *Script* box.
6. Click **CONFIRM**.

The remote execution script is added to the repository.




To send a remote execution command or script to a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Repositories actions**, and then click **REMOTE EXECUTE**.
The *Remote execute* window appears.
5. Select a command or script from the list and click **APPLY**.



To send a remote execution command or script to multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Remote execute**.
The *Remote execute* window appears.
5. Select a command or script from the list and click **APPLY**.







To send a remote execution command or script to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Remote execute**.
The *Remote execute* window appears.
4. Select a command or script from the list and click **APPLY**.

To send a remote execution command or script to a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Remote execute**.
The *Remote execute* window appears.
4. Select a command or script from the list and click **APPLY**.

Sending custom MDM commands to iOS and macOS devices

					
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


The Mobile Device Management (MDM) protocol allows you to send commands to iOS and macOS devices enrolled in SMART Remote Management. For more information about the MDM protocol, see the [Mobile Device Management protocol reference](#).

You can create custom MDM commands to perform a variety of actions on iOS and macOS devices:

- Inspect, install, or remove profiles
- Remove passcodes
- Begin secure erase

You can run custom MDM commands on a single device, multiple devices, all devices that match a saved filter's criteria, or a group.


To create a custom MDM command

1. Click **Repositories**  and select **Apple custom command**.

The *Apple custom command* window appears.

2. Click **ADD NEW**.
3. Type a name in the *Name* box.
4. Type the command in the *Plist text* box.
5. Click **CONFIRM**.

To run a custom MDM command on a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.



The device's dashboard window appears.

4. Click **Repository actions**, and then click **APPLE CUSTOM COMMAND**.




The *Apple custom command* window appears.

5. Select the custom MDM command from the list and click **APPLY**.



To run a custom Apple MDM command on multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Apple custom command**.
The *Apple custom command* window appears.
5. Select the custom MDM command from the list and click **APPLY**.

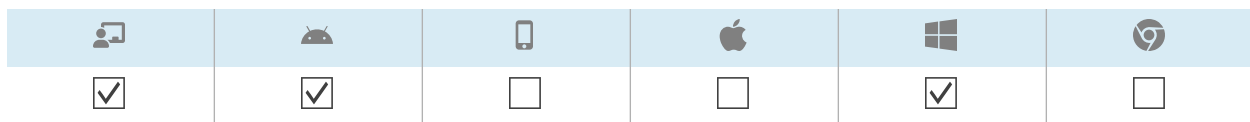
To run a custom Apple MDM command on all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Apple custom command**.
The *Apple custom command* window appears.
4. Select the custom MDM command from the list and click **APPLY**.

To run a custom MDM command on a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Apple custom command**.
The *Apple custom command* window appears.
4. Select the custom MDM command from the list and click **APPLY**.

Sending files to devices



You can upload files from your computer or a URL and use SMART Remote Management to send those files to devices in your organization. This is useful when you want all devices to have the same wallpaper or otherwise share common files.

You can send files to a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the sending of files at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the sending of files in workflows (see *Managing workflows* on page 118).

To upload files from your computer

1. Click **Repositories**  and select **Files**.

The *Files* window appears.

2. Click **ADD NEW**.

The *New file* window appears.

3. Select **Upload File** in the *Select upload method* drop-down list.

4. Type a name for the files in the *Name* box.

5. Type the path where you want to send the files in the *Destination* box.

Tip

For SMART Board interactive displays with iQ:

- Place files in `/sdcard/download` to have them appear in the **Downloads** folder.
- Place files in `/sdcard/Android/obb/SMART/shared/files` to have them appear in the **Board Files** folder.

For information on viewing files in these folders, see [Using the Files Library](#).

6. Click **ADD FILES**.

The *Open* dialog box appears.

7. Browse to and select the first file you want to upload, and click **Open**.

8. Repeat steps 6 and 7 for all other files you want to upload.

9. Click **Upload all** .

10. Click **CONFIRM**.

To upload files from a URL

1. Click **Repositories**  and select **Files**.

The *Files* window appears.

2. Click **ADD NEW**.

The *New file* window appears.

3. Select **File from Url** in the *Select upload method* drop-down list.
4. Type the URL you are uploading the files from in the *File url* box.
5. Type a name for the files in the *Name* box.
6. Type the path where you want to send the files in the *Destination* box.

Tip


For SMART Board interactive displays with iQ:

- Place files in `/sdcard/download` to have them appear in the **Downloads** folder.
- Place files in `/sdcard/Android/obb/SMART/shared/files` to have them appear in the **Board Files** folder.

For information on viewing files in these folders, see [Using the Files Library](#).

7. Click **CONFIRM**.

To send files to a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.



The device's dashboard window appears.

4. Click **Repositories actions**, and then click **FILES**.

The *Files* window appears.

5. Select the files from the list and click **APPLY**.




To send files to multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Send files**.



The *Files* window appears.

5. Select the files from the list and click **APPLY**.

To send files to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Send files**.
The *Files* window appears.
4. Select the files from the list and click **APPLY**.

To send files to a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Send files**.
The *Files* window appears.
4. Select the files from the list and click **APPLY**.

Sending messages and sounding the siren







You can send messages and sound the siren using SMART Remote Management. These features are useful when you need to communicate information with specific users or all users across your organization quickly.

You can send two types of messages using SMART Remote Management:

- Text-only
- Advanced

Text-only messages can be sent to all devices. You can send advanced messages to only SMART Board interactive displays and Android devices.

Sending text-only messages


					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Text-only messages consist of a title and body.



You can send text-only messages to a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to send a text-only message at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the sending of text-only messages in workflows (see *Managing workflows* on page 118).




To send a text-only message to a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Send message**.
The *Send message* window appears.
5. Type the message title and body text in the *Message title* and *Message body* boxes.
6. Click **CONFIRM**.

To send a text-only message to multiple devices



1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Send message**.
The *Send message* window appears.
5. Type the message title and body text in the *Message title* and *Message body* boxes.
6. Click **CONFIRM**.

To send a text-only message to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Send message**.
The *Send message* window appears.

4. Type the message title and body text in the *Message title* and *Message body* boxes.
5. Click **CONFIRM**.







To send a text-only message to a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Send message**.

The *Send message* window appears.

4. Type the message title and body text in the *Message title* and *Message body* boxes.
5. Click **CONFIRM**.

Sending advanced messages



					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Unlike text-only messages, advanced messages consist of text, images, and sounds.


You can send advanced messages to a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to send advanced messages at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the sending of advanced messages in workflows (see *Managing workflows* on page 118).

To create an advanced message


1. Click **Repositories**  and select **Advanced messaging**.
The *Advanced messages* window appears.
2. Click **ADD NEW**.
3. Type a name and description in the *Name* and *Description* boxes.
4. Click **Content** .

- Provide text, image, and sound for the advanced message:



Component	Procedure
Text	<ol style="list-style-type: none"> Type text in the <i>Text to display</i> box. Click  and select a color for the text.
Image	<ol style="list-style-type: none"> Click ADD IMAGE ASSET. The <i>Assets</i> window appears. <div data-bbox="565 548 1424 695" style="border-left: 2px solid #0070C0; padding-left: 10px; margin: 10px 0;"> <p>Note</p> <p>If the image you want to use for the advanced message isn't already available in SMART Remote Management, click ADD NEW and follow the on-screen instructions to upload the image.</p> </div> Select the image and click APPLY. (Optional) Select Stretch on screen to stretch the image to fill the screen. (Optional) Select Horizontal or Vertical to keep the width or height of the image proportional.
Sound	<ol style="list-style-type: none"> Click ADD AUDIO ASSET. The <i>Assets</i> window appears. <div data-bbox="565 974 1424 1121" style="border-left: 2px solid #0070C0; padding-left: 10px; margin: 10px 0;"> <p>Note</p> <p>If the sound you want to use for the advanced message isn't already available in SMART Remote Management, click ADD NEW and follow the on-screen instructions to upload the sound.</p> </div> Select the sound and click APPLY. (Optional) Select Loop audio to replay the sound while the message is visible on the device.

- Click **CONFIRM**.




To send an advanced message to a single device

- Click **Devices**  to open the *Devices* view.
- (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
- Click the device's row.
The device's dashboard window appears.
- Click **Repository actions**, and then click **ADVANCED MESSAGING**.
The *Advanced messaging* window appears.
- Select the advanced message from the list and click **APPLY**.



To send an advanced message to multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **Advanced message** .
The *Advanced messaging* window appears.
5. Select the advanced message from the list and click **APPLY**.

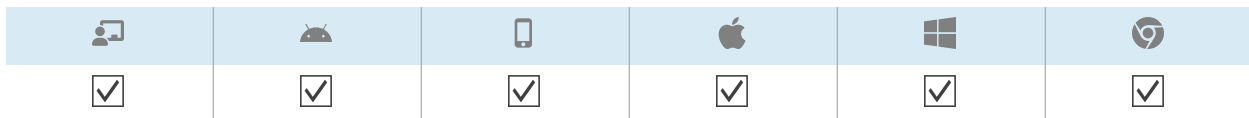
To send an advanced message to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Advanced messaging**.
The *Advanced messaging* window appears.
4. Select the advanced message from the list and click **APPLY**.

To send an advanced message to a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Advanced messaging**.
The *Advanced messaging* window appears.
4. Select the advanced message from the list and click **APPLY**.

Sounding the siren




To inform device users of an emergency, you can sound the siren on a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to sound the siren at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the sounding of the siren in workflows (see *Managing workflows* on page 118).



 **Warning**

The siren causes devices' screens to flash at approximately 7 Hz. If any users are sensitive to rapidly flashing screens, consider sending messages instead.




To sound the siren on a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Lock**, and then click **SIREN**.
A message appears, asking if you want to sound the siren.
5. Click **CONFIRM**.


To sound the siren on multiple devices


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Sound siren**.
A message appears, asking if you want to sound the siren.
5. Click **CONFIRM**.

To sound the siren on all devices that match a saved filter's criteria







1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Sound siren**.
A message appears, asking if you want to sound the siren.
4. Click **CONFIRM**.

To sound the siren on a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.

3. Click **Actions**  in the group's row and select **Sound siren**.
A message appears, asking if you want to sound the siren.
4. Click **CONFIRM**.

Locking and unlocking devices


					
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

If a device is lost or stolen, you can lock it from SMART Remote Management to secure it, provided the device still has wireless connectivity.


You can lock and unlock devices as described below. Alternatively, you can lock and unlock devices at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).

Locking and unlocking SMART Board GX and MX100 series interactive displays and Android, Windows, and Chrome OS devices

To lock a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Lock**, and then click **LOCK**.
5. For an iOS and macOS device, type a message and phone number in the appropriate boxes to display on the screen of the device.
6. Click **CONFIRM**.

To unlock a device


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).

3. Click the device's row.

The device's dashboard window appears.


4. Click **Lock**, and then click **UNLOCK**.
5. Click **CONFIRM**.

To retrieve the password from a locked device


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Lock**, and then click **GET PASSWORD**.
5. Click **PRESS TO RETRIEVE PASSWORD**.

Locking and unlocking iOS and macOS devices

To enable Lost Mode


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Lost mode**, and then click **ENABLE LOST MODE**.
5. Type a message, phone number, and footnote in the appropriate boxes to display on the screen of the device when it is locked.
6. Click **CONFIRM**.

To disable Lost Mode


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.

4. Click **Lost mode**, and then click **DISABLE LOST MODE**.
5. Click **YES**.


To lock a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Lost mode**, and then click **LOCK**.
5. Type a message and phone number in the appropriate boxes to display on the screen of the device.
6. Click **CONFIRM**.

To unlock a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Lost mode**, and then click **UNLOCK**.
5. Click **CONFIRM**.







To sound the siren on a device with Lost Mode enabled

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Lost mode**, and then click **PLAY LOST MODE SOUND**.
5. Click **CONFIRM**.

Restarting, shutting down, and waking devices

You can restart, shut down, and wake devices from SMART Remote Management. This is useful when you are troubleshooting issues with device users and when you are installing apps on devices and need to wake and restart (or shut down) those devices as part of the installation.


Restarting devices

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>



You can restart a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the restarting of devices at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the restarting of devices in workflows (see *Managing workflows* on page 118).




To restart a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Power**, and then click **RESTART**.
5. Click **YES**.



To restart multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Restart**.
5. Click **YES**.







To restart all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Restart**.
4. Click **YES**.

To restart a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Restart**.
4. Click **YES**.


Shutting down devices

					
<input type="checkbox"/>	<input checked="" type="checkbox"/> ²	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

You can shut down a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:



- Use a trigger to initiate the shutdown of devices at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the shutdown of devices in workflows (see *Managing workflows* on page 118).

To shut down a single device




1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Power**, and then click **SHUTDOWN**.
5. Click **YES**.

²SMART Board GX series interactive displays can't be shut down from SMART Remote Management.



To shut down multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Shutdown**.
5. Click **YES**.







To shut down all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Shutdown**.
4. Click **YES**.

To shut down a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Shutdown**.
4. Click **YES**.

Waking devices

					
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

You can wake devices from SMART Remote Management if those devices support Wake on LAN (WOL).


You can wake devices from a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the waking of devices at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the waking of devices in workflows (see *Managing workflows* on page 118).

Notes

- Make sure devices support WOL before completing the following procedures.
- The devices that send the WOL command must be running and on the same network as the devices you're waking.
- It's better to send a WOL command from multiple devices or a group than from a single device because it's possible the single device may not be running when you send the WOL command.



To send a WOL command from a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Power**, and then click **WAKE ON LAN**.
The *Wake on lan* window appears.
5. Select **Filter** or **Group** and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see *Finding devices* on page 11).
OR
Select **Device** and type a device's ID in the *Device ID* box to wake a single device.
6. (Optional) Turn on **Advanced wake-on-lan settings** and specify the broadcast address and port

for execution if your network requires this information to be provided.

7. Click **CONFIRM**.

To send a WOL command from multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Wake on lan**.

The *Wake on lan* window appears.




5. Select **Filter** or **Group** and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see *Finding devices* on page 11).

OR

Select **Device** and type a device's ID in the *Device ID* box to wake a single device.

6. (Optional) Turn on **Advanced wake-on-lan settings** and specify the broadcast address and port for execution if your network requires this information to be provided.
7. Click **CONFIRM**.

To send a WOL command from all devices that match a saved filter's criteria



1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Wake on lan**.
4. Select **Filter** or **Group** and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see *Finding devices* on page 11).

OR

Select **Device** and type a device's ID in the *Device ID* box to wake a single device.

5. (Optional) Turn on **Advanced wake-on-lan settings** and specify the broadcast address and port for execution if your network requires this information to be provided.
6. Click **CONFIRM**.

To send a WOL command from a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Wake on lan**.

The *Wake on lan* window appears.







4. Select **Filter** or **Group** and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see *Finding devices* on page 11).

OR

Select **Device** and type a device's ID in the *Device ID* box to wake a single device.

5. (Optional) Turn on **Advanced wake-on-lan settings** and specify the broadcast address and port for execution if your network requires this information to be provided.
6. Click **CONFIRM**.


Changing devices' agent passwords

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Agent passwords are used to lock SMART Remote Management settings on devices.

You can change the agent password on a single device, multiple devices, all devices that match a saved filter's criteria, or a group as described below. Alternatively, you can use a trigger to initiate the change of the agent password when a specific event takes place (see *Managing schedulers and triggers* on page 104).

To change the agent password on a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.



The device's dashboard window appears.

4. Click **Manage**, and then click **CHANGE AGENT PASSWORD**.




The *Change agent password* window appears.

5. Type the new agent password in the *Password* and *Confirm password* boxes.
6. Click **CONFIRM**.



To change the agent password on multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Change agent password**.
The *Change agent password* window appears.
5. Type the new agent password in the *Password* and *Confirm password* boxes.
6. Click **CONFIRM**.

To change the agent password on all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Change agent password**.
The *Change agent password* window appears.
4. Type the new agent password in the *Password* and *Confirm password* boxes.
5. Click **CONFIRM**.







To change the agent password on a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Change agent password**.
The *Change agent password* window appears.
4. Type the new agent password in the *Password* and *Confirm password* boxes.
5. Click **CONFIRM**.

Running device-type-specific commands

Although most commands in SMART Remote Management can be run on multiple types of devices, some commands are specific to certain device types.

Removing Google accounts from Android devices


					
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

You can use SMART Remote Management to remove all Google accounts (except those you explicitly choose not to remove) from your organizations' Android devices.

You can remove Google accounts on a single device, multiple devices, all devices that match a saved filter's criteria, or a group. Alternatively, you can:

- Use a trigger to initiate the removal of Google accounts when a specific event takes place (see *Managing schedulers and triggers* on page 104).
- Include the removal of Google accounts in workflows (see *Managing workflows* on page 118).

To remove Google accounts from a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.

The device's dashboard window appears.

4. Click **Manage**, and then click **REMOVE GOOGLE ACCOUNTS**.

The *Remove accounts* window appears.


5. Select **Remove all accounts** to remove all Google accounts.


OR

Select **Keep one account** to retain one Google account and type that account's email address in the *Email account* box.

6. Click **CONFIRM**.

To remove Google accounts from multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).

3. Select the devices' check boxes.
4. Click **More actions**  and select **Remove Google accounts from device**.

The *Remove accounts* window appears.




5. Select **Remove all accounts** to remove all Google accounts.

OR

Select **Keep one account** to retain one Google account and type that account's email address in the *Email account* box.

6. Click **CONFIRM**.

To remove Google accounts from all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Remove Google accounts from device**.

The *Remove accounts* window appears.



4. Select **Remove all accounts** to remove all Google accounts.

OR

Select **Keep one account** to retain one Google account and type that account's email address in the *Email account* box.

5. Click **CONFIRM**.

To remove Google accounts from a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Remove Google accounts from device**.

The *Remove accounts* window appears.







4. Select **Remove all accounts** to remove all Google accounts.

OR

Select **Keep one account** to retain one Google account and type that account's email address in the *Email account* box.

5. Click **CONFIRM**.

Deploying DEP profiles to iOS and macOS devices

					
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apple School Manager and Apple Business Manager are online services that include the ability to automate the enrollment and configuration of your organization’s iOS and macOS devices in SMART Remote Management and other mobile device management software.

Note

Apple School Manager and Apple Business Manager replace the Device Enrollment Program (DEP). However, the term “DEP” is still used in SMART Remote Management and in this documentation.

For more information on these Apple programs, see [Getting started using Apple Business Manager or Apple School Manager with mobile device management](#).

To use these Apple programs with SMART Remote Management to enroll and configure devices, follow these four steps:

1. If you haven’t already, enroll in the appropriate program for your organization:

Program	Link
Apple School Manager	school.apple.com
Apple Business Manager	business.apple.com

2. Add a DEP server account to SMART Remote Management as described in the *SMART Remote Management setup guide* (smarttech.com/kb/171333).
3. Create DEP profiles.
4. Deploy DEP profiles to a single device, multiple devices, all devices that match a saved filter’s criteria, or a group.

To add a DEP server account to SMART Remote Management




See the *SMART Remote Management setup guide* (smarttech.com/kb/171333).

To create a DEP profile

1. Click **Repositories**  and select **Dep Apple profile**.


The *DEP Apple profile* window appears.

2. Click **ADD NEW**.
3. Type a name and description in the *Name* and *Description* boxes.
4. Select a DEP server account in the *DEP server account* drop-down list.
5. Enter the appropriate information in the remaining tabs:


Icon	Tab	Description
	General	Enable and disable general settings for the DEP profile.
	Support info	Enter support contact information for the DEP profile.
	Setup assistant	Enable and disable setup assistant features for the DEP profile.

6. Click **CONFIRM**.




To deploy a DEP profile to a single device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Repository actions**, and then click **DEP APPLE PROFILE**.
The *Dep Apple profile* window appears.
5. Select the DEP profile from the list and click **APPLY**.



To deploy a DEP profile to multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions** ******* and select **Dep Apple profile**.
The *Dep Apple profile* window appears.
5. Select the DEP profile from the list and click **APPLY**.







To deploy a DEP profile to all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Dep Apple profile**.
The *Dep Apple profile* window appears.
4. Select the DEP profile from the list and click **APPLY**.

To deploy a DEP profile to a group


1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Dep Apple profile**.
The *Dep Apple profile* window appears.
4. Select the DEP profile from the list and click **APPLY**.

Clearing passcodes from iOS and macOS devices


					
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Using SMART Remote Management, you can clear the passcode and the restrictions passcode from an iOS or macOS device.

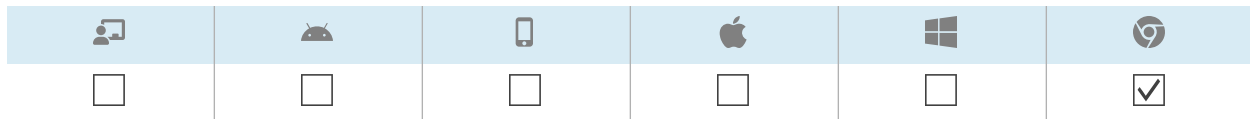
To clear a passcode from a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Power**, and then click **CLEAR PASSCODE**.
5. Click **YES**.

To clear a restrictions passcode from a device


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Power**, and then click **CLEAR RESTRICTIONS PASSCODE**.
5. Click **YES**.

Retrieving the default password for Chrome OS devices









Using SMART Remote Management, you can retrieve the default password for a Chrome OS device.

To retrieve the default password for a device

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.
The device's dashboard window appears.
4. Click **Manage**, and then click **GET DEFAULT PASSWORD**.
5. Click **PRESS TO RETRIEVE PASSWORD**.

Chapter 6 Running ad-hoc sessions

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

On occasion, you might want to manage a device that is on a different account or domain. For these occasions, you can run an ad-hoc session.

Running an ad-hoc session involves two steps:

1. Starting the ad-hoc session on the device
2. Connecting to the ad-hoc session from SMART Remote Management

You can end an ad-hoc session from SMART Remote Management, or the device's user can end it from the device.

Tip

If you are working with SMART support to troubleshoot an issue with a SMART Board display with iQ, you can start an ad-hoc session on the display following the procedure below, then provide the token ID to the SMART support agent. The SMART support agent will then be able to connect to the display to diagnose the issue.


To start an ad-hoc session on a SMART Board interactive display with iQ

1. Open the display's settings and browse to **System > Remote Management > Launch Remote Management Settings**.

Note


For information about opening the display's settings, see the display's documentation.

The remote management settings window appears.



2. Tap  in the top-right corner of the screen and select **Start Ad-Hoc session**.

The *Session Token* screen appears, displaying a session token ID.

To start an ad-hoc session on an Android device

1. If the Viso MDM agent is not already installed on the device, download and install it from radix-int.com/radix-viso-mdm-download-links.
2. Open the Viso MDM agent on the device.
3. Tap  in the top-right corner of the screen and select **Start Ad-Hoc session**.
The *Session Token* screen appears, displaying a session token ID.

To connect to an ad-hoc session from SMART Remote Management

1. Click **Devices**  to open the *Devices* view.
2. Click **Ad-hoc session**  to open the *Ad-hoc session* window.
3. In the *Token ID* box, type the session token ID generated by the user in the previous procedures and click **START**.

The ad-hoc session window appears. You can manage the device like you do enrolled devices:

- *Chapter 2 Managing devices* on page 8
- *Chapter 3 Installing and managing apps on devices* on page 28
- *Chapter 5 Running other commands on devices* on page 65

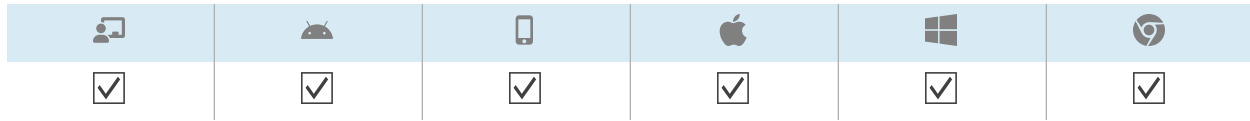
To end an ad-hoc session

Click **Stop session** in the ad-hoc session window.

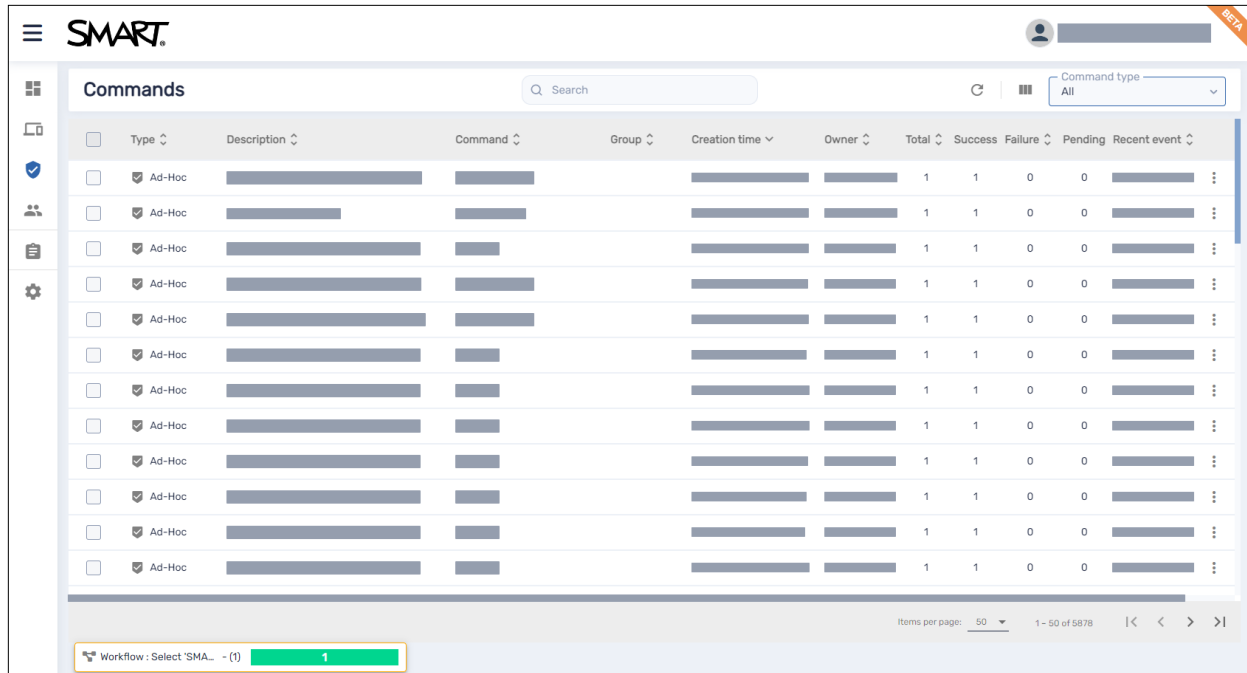
Chapter 7 **Managing commands, schedulers, triggers, and workflows**

- Managing commands 99
 - Showing and hiding columns100
 - Finding commands100
 - Viewing command details101
 - Stopping, restarting, and editing commands102
 - Resending commands103
 - Deleting commands103
 - Making group commands persistent103
- Managing schedulers and triggers104
 - Creating schedulers and triggers105
 - Initiating commands using schedulers and triggers108
- Managing workflows118

Managing commands



The *Commands* view provides a centralized list of all the commands currently running, previously run, and set to run by trigger on devices for which you have access.



Note


The color of each command's icon indicates its status:

Icon color	Command status
	Applies to a single device or multiple devices
	Applies to a group but is not persistent
	Applies to a group and is persistent


For more information about groups and persistent commands, see *Making group commands persistent* on page 103.

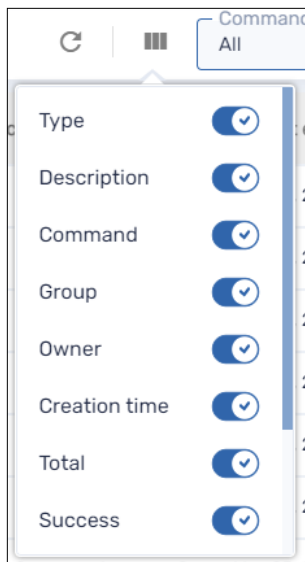
From this view, you can:

- Filter commands
- View command details
- Stop, restart, and edit currently running or trigger commands
- Resend commands to all devices for which the commands apply or only to those devices for which the commands previously failed
- Delete commands
- Make group commands persistent


To open the *Commands* view from anywhere in SMART Remote Management, click **Commands**  in the menu.

Showing and hiding columns

You can choose which columns appear in the *Commands* view by clicking **Columns** . Enable columns you want to show, and disable columns you want to hide:



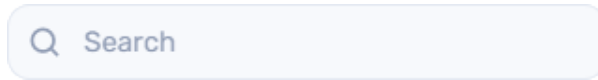
Tips

- You can sort commands by clicking  beside the column headers.
- You can change the order of columns by dragging a column's header to its new position.

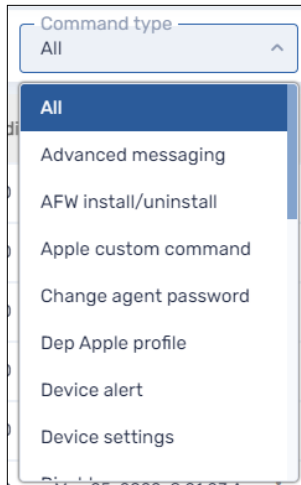
Finding commands

To find a specific command or commands quickly, filter the commands in the *Commands* view in one of the following ways:

- Use the *Search* bar at the top of the *Commands* view




- Filter commands by type by using the *Command type* drop-down list

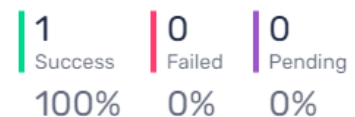
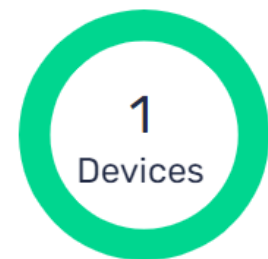


Viewing command details

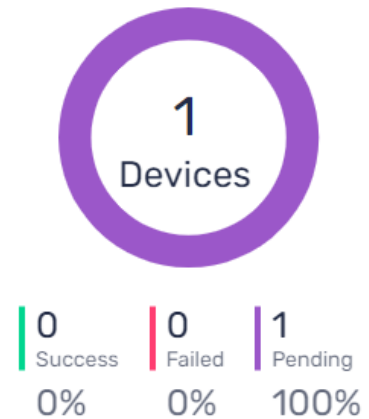
To view the status of a command

1. Click **Commands**  to open the *Commands* view.
2. Click the command's row.

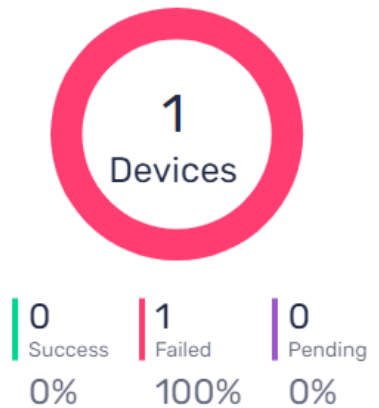
The command's status window appears.
Successful commands appear in green.



Pending commands appear in purple.



Failed commands appear in red.



Tip

Click **More info** in a command's row to see why it failed.

Stopping, restarting, and editing commands

You can stop, restart, and edit currently running, scheduled, or trigger commands from the *Commands* view.

To stop a command

1. Click **Actions**  in the command's row and select **Stop command**.
2. Click **YES**.

To restart a command

1. Click **Actions**  in the command's row and select **Start command**.
2. Click **YES**.

To edit a command

1. Click **Actions**  in the command's row and select **Edit command**.

The *Scheduler & trigger commands* window appears.

2. Make any desired changes to the command.
3. Click **CONFIRM**.


Resending commands

You can resend previously run commands from the *Commands* view. You can resend the commands to all devices for which it applies or only to devices for which it previously failed.

To resend a command to all devices for which it applies

1. Click **Actions**  in the command's row and select **Resend command**.
2. Click **YES**.

To resend a command to only devices for which it previously failed

1. Click **Actions**  in the command's row and select **Resend command to failed devices**.
2. Click **YES**.

Deleting commands

You can delete commands from the *Commands* view.

To delete a command

1. Click **Actions**  in the command's row and select **Delete command**.
2. Click **YES**.

Making group commands persistent

You can make group commands persistent from the *Commands* view. If you assign a new device to a group in the future (by adding one of the group's tags to the device), the persistent commands for that group automatically run on the device.

Notes


- For information about groups, see *Using groups* on page 22.
- SMART Board interactive displays with iQ support persistent commands.


- Other devices require version 11.5.1.1 or later of the Viso MDM agent to support persistent commands.

Tip

If you want to run a command, such as deploying an installation package, on each new device you enroll in SMART Remote Management, run the command on the New Devices group and make it persistent.



To make a group command persistent

1. Click **Actions**  in the command's row and select **Persist**.
2. Click **YES**.

The command's icon changes from blue () to green ()

To stop a group command's persistence

1. Click **Actions**  in the command's row and select **Stop persistence**.
2. Click **YES**.

The command's icon changes from green () to blue ()

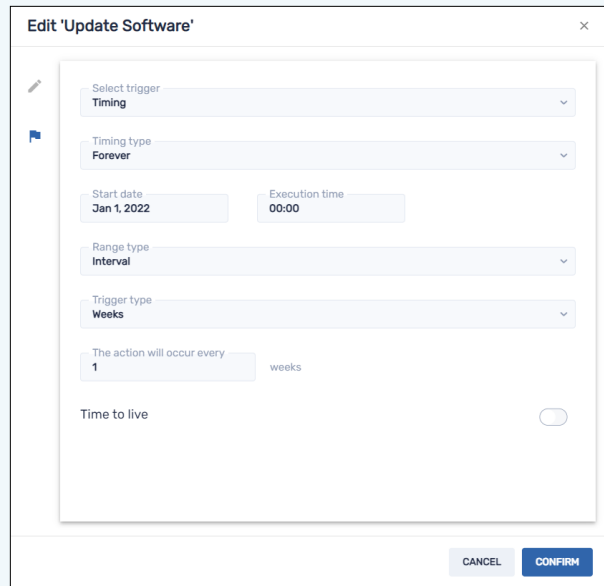
Managing schedulers and triggers

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Although you can run commands whenever you want on demand, you might prefer to initiate them at a scheduled time or in response to a specific event. Schedulers and triggers allow you to do this for all types of commands, including workflows (see *Managing workflows* on page 118).

Example

If you need to update software on devices every week, you can create a scheduler that deploys the appropriate software installation package during off-hours.



Creating schedulers and triggers

You can create three types of schedulers and triggers:

Type	Description
Scheduler (also known as “timing trigger”)	Run a command at a scheduled time once or at regular intervals
Geofencing trigger	Run a command when a device enters or leaves a specified area
Wi-Fi trigger	Run a command when a device joins or leaves a Wi-Fi network

Tip


Use geofencing and Wi-Fi triggers with mobile devices that you want to maintain in a specific area or on a specific Wi-Fi network.

To create a scheduler

1. Click **Repositories**  and select **Scheduler & triggers**.

The *Scheduler & triggers* window appears.


2. Click **ADD NEW**.



3. Type a name and description for the scheduler in the *Name* and *Description* boxes.
4. Click **Add trigger** .
5. Select **Timing** in the *Select trigger* drop-down list.
6. Complete one of the procedures below (depending on when you'd like the command to run):

Option	Procedure
Run the command once	<ol style="list-style-type: none"> a. Select Once in the <i>Timing type</i> drop-down list. b. Select the date you want to run the command in the <i>Start date</i> drop-down list. c. Select the time you want to run the command in the <i>Execution time</i> drop-down list.
Run the command regularly for a specific length of time	<ol style="list-style-type: none"> a. Select From/To date in the <i>Timing type</i> drop-down list. b. Select the date you want to first run the command in the <i>Start date</i> drop-down list. c. Select the time you want to run the command in the <i>Execution time</i> drop-down list. d. Select the date you want to last run the command in the <i>End date</i> drop-down list. e. Select an interval type in the <i>Range type</i> drop-down list and use the resulting drop-down list to specify the interval.
Run the command regularly indefinitely	<ol style="list-style-type: none"> a. Select Forever in the <i>Timing type</i> drop-down list. b. Select the date you want to first run the command in the <i>Start date</i> drop-down list. c. Select the time you want to run the command in the <i>Execution time</i> drop-down list. d. Select an interval type in the <i>Range type</i> drop-down list and use the resulting drop-down list to specify the interval.

7. (Optional) Enable **Time to live** and type the maximum time in seconds for the command to go live in the *Time to live (seconds)* box.
8. Click **CONFIRM**.

To create a geofencing trigger

1. Click **Repositories**  and select **Scheduler & triggers**.
The *Scheduler & triggers* window appears.
2. Click **ADD NEW**.
3. Type a name and description for the trigger in the *Name* and *Description* boxes.



4. Click **Add trigger** .
5. Select **Geofencing** in the *Select trigger* drop-down list.
6. Using the map, zoom in to the area you want to use for the trigger.
7. Click **Draw a circle**  and draw a circle around the area.

Note

The area must be at least 40 m in diameter.

8. Specify what happens when the device enters the area by selecting the appropriate option under *On enter*:
 - Select **Start** to start running the command when the device enters the area.
 - Select **End** to stop running the command when the device enters the area.
 - Select **Nothing** to do nothing when the device enters the area.
9. Specify what happens when the device leaves the area by selecting the appropriate option under *On exit*:
 - Select **Start** to start running the command when the device leaves the area.
 - Select **End** to stop running the command when the device leaves the area.
 - Select **Nothing** to do nothing when the device leaves the area.
10. Click **CONFIRM**.

To create a Wi-Fi trigger


1. Click **Repositories**  and select **Scheduler & triggers**.
The *Scheduler & triggers* window appears.
2. Click **ADD NEW**.
3. Type a name and description for the trigger in the *Name* and *Description* boxes.
4. Click **Add trigger** .
5. Select **Wifi** in the *Select trigger* drop-down list.
6. Type the Wi-Fi network's SSID in the *SSID* box.

7. Specify what happens when the device joins the Wi-Fi network by selecting the appropriate option under *On enter*:
 - Select **Start** to start running the command when the device joins the Wi-Fi network.
 - Select **End** to stop running the command when the device joins the Wi-Fi network.
 - Select **Nothing** to do nothing when the device joins the Wi-Fi network.
8. Specify what happens when the device leaves the Wi-Fi network by selecting the appropriate option under *On exit*:
 - Select **Start** to start running the command when the device leaves the Wi-Fi network.
 - Select **End** to stop running the command when the device leaves the Wi-Fi network.
 - Select **Nothing** to do nothing when the device leaves the Wi-Fi network.
9. Click **CONFIRM**.

Initiating commands using schedulers and triggers

After you have created schedulers and triggers, you can use them to initiate commands on a single device, multiple devices, all devices that match a saved filter's criteria, or a group.


To initiate commands on a single device using a scheduler or trigger

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Click the device's row.

The device's dashboard window appears.
4. Click **Schedule & trigger command**.

The *Schedule & trigger command* window appears.
5. Type a name for the scheduler- or trigger-based commands in the *Command name* box.
6. Click **SELECT TRIGGER**.



The *Scheduler & triggers* window appears.
7. Select a scheduler or trigger from the list and click **ADD**.
8. Click **SELECT COMMAND** and select from the following options:

Option	Subsequent steps
Advanced messaging	<ol style="list-style-type: none"> Select an advanced message. Click ADD.
AFW install/uninstall	<ol style="list-style-type: none"> Select Install or Uninstall. Select the apps you want to install or uninstall. Click CONFIRM. <p>Note</p> <p>You need to enroll in Android for Work to use this option (see Android for Work (AFW)—Google EMM enrollment).</p>
Change agent password	<ol style="list-style-type: none"> Type the new agent password in the <i>Password</i> and <i>Confirm password</i> boxes. Click CONFIRM.
Clear apps data	<ol style="list-style-type: none"> Click Add to list ⁺ for each app for which you want to clear data. Click CONFIRM.
Device alert	<ol style="list-style-type: none"> For each email address to which you want to send the alert, type the email address in the <i>Add email, then press Enter</i> box and press ENTER. <p>Tips</p> <ul style="list-style-type: none"> ◦ Your SMART Remote Management user account's email address is included by default. ◦ You can delete an email address by clicking its  button. Type the alert message in the <i>Message</i> box. Click CONFIRM.
Device settings	<ol style="list-style-type: none"> Select settings. Click ADD.
Disable apps	<ol style="list-style-type: none"> Click Add to list ⁺ for each app you want to disable. Click CONFIRM.
Enable apps	<ol style="list-style-type: none"> Click Add to list ⁺ for each app you want to enable. Click CONFIRM.
Install package	<ol style="list-style-type: none"> Select an installation package. Click ADD.
Lock	[N/A]

Option	Subsequent steps
Remote execute	<ol style="list-style-type: none"> Select a remote execution command. Click ADD.
Remove Google accounts from device	<ol style="list-style-type: none"> Select Remove all accounts to remove all Google accounts. OR Select Keep one account to retain one Google account and type that account's email address in the <i>Email account</i> box. Click CONFIRM.
Restart	[N/A]
Send files	<ol style="list-style-type: none"> Select files. Click ADD.
Send message	<ol style="list-style-type: none"> Type the message title and body text in the <i>Message Title</i> and <i>Message Body</i> boxes. Click CONFIRM.
Shutdown	[N/A]
Sound siren	[N/A]
Uninstall packages	<ol style="list-style-type: none"> Click Add To List \oplus for each app you want to uninstall. Click UNINSTALL SELECTED.
Wake on lan	<ol style="list-style-type: none"> Select Filter or Group and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see <i>Finding devices</i> on page 11). OR Select Device and type a device's ID in the <i>Device ID</i> box to wake a single device. (Optional) Turn on Advanced wake-on-lan settings and specify the broadcast address and port for execution if your network requires this information to be provided. Click CONFIRM.
Wipe	[N/A]
Workflow	<ol style="list-style-type: none"> Select a workflow. Click ADD.

9. Click **CONFIRM**

To initiate commands on multiple devices using a scheduler or trigger


1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **More actions**  and select **Scheduler & triggers command**.




The *Scheduler & triggers command* window appears.


5. Type a name for the scheduler- or trigger-based commands in the *Command name* box.
6. Click **SELECT TRIGGER**.

The *Scheduler & triggers* window appears.

7. Select a scheduler or trigger from the list and click **ADD**.
8. Click **SELECT COMMAND** and select from the following options:




Option	Subsequent steps
Advanced messaging	<ol style="list-style-type: none"> a. Select an advanced message. b. Click ADD.
AFW install/uninstall	<ol style="list-style-type: none"> a. Select Install or Uninstall. b. Select the apps you want to install or uninstall. c. Click CONFIRM. <p>Note You need to enroll in Android for Work to use this option (see Android for Work (AFW)—Google EMM enrollment).</p>
Change agent password	<ol style="list-style-type: none"> a. Type the new agent password in the <i>Password</i> and <i>Confirm password</i> boxes. b. Click CONFIRM.
Clear apps data	<ol style="list-style-type: none"> a. Click Add to list  for each app for which you want to clear data. b. Click CONFIRM.


Option	Subsequent steps
Device alert	<p>a. For each email address to which you want to send the alert, type the email address in the <i>Add email, then press Enter</i> box and press ENTER.</p> <p>Tips</p> <ul style="list-style-type: none"> ◦ Your SMART Remote Management user account's email address is included by default. ◦ You can delete an email address by clicking its  button. <p>b. Type the alert message in the <i>Message</i> box.</p> <p>c. Click CONFIRM.</p>
Device settings	<p>a. Select settings.</p> <p>b. Click ADD.</p>
Disable apps	<p>a. Click Add to list  for each app you want to disable.</p> <p>b. Click CONFIRM.</p>
Enable apps	<p>a. Click Add to list  for each app you want to enable.</p> <p>b. Click CONFIRM.</p>
Install package	<p>a. Select an installation package.</p> <p>b. Click ADD.</p>
Lock	[N/A]
Remote execute	<p>a. Select a remote execution command.</p> <p>b. Click ADD.</p>
Remove Google accounts from device	<p>a. Select Remove all accounts to remove all Google accounts. OR Select Keep one account to retain one Google account and type that account's email address in the <i>Email account</i> box.</p> <p>b. Click CONFIRM.</p>
Restart	[N/A]
Send files	<p>a. Select files.</p> <p>b. Click ADD.</p>
Send message	<p>a. Type the message title and body text in the <i>Message Title</i> and <i>Message Body</i> boxes.</p> <p>b. Click CONFIRM.</p>
Shutdown	[N/A]

Option	Subsequent steps
Sound siren	[N/A]
Uninstall packages	<ol style="list-style-type: none"> Click Add To List  for each app you want to uninstall. Click UNINSTALL SELECTED.
Wake on lan	<ol style="list-style-type: none"> Select Filter or Group and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see <i>Finding devices</i> on page 11). OR Select Device and type a device's ID in the <i>Device ID</i> box to wake a single device. (Optional) Turn on Advanced wake-on-lan settings and specify the broadcast address and port for execution if your network requires this information to be provided. Click CONFIRM.
Wipe	[N/A]
Workflow	<ol style="list-style-type: none"> Select a workflow. Click ADD.

- Click **CONFIRM**

To initiate commands on all devices that match a saved filter's criteria using a scheduler or trigger



- Click **Devices**  to open the *Devices* view.
- Click **Filters** .
- Click **Actions**  in the saved filter's row and select **Scheduler & triggers command**.
The *Scheduler & triggers command* window appears.
- Type a name for the scheduler- or trigger-based commands in the *Command name* box.
- Click **SELECT TRIGGER**.
The *Scheduler & triggers* window appears.
- Select a scheduler or trigger from the list and click **ADD**.
- Click **SELECT COMMAND** and select from the following options:


Option	Subsequent steps
Advanced messaging	<ol style="list-style-type: none"> Select an advanced message. Click ADD.
AFW install/uninstall	<ol style="list-style-type: none"> Select Install or Uninstall. Select the apps you want to install or uninstall. Click CONFIRM. <p>Note</p> <p>You need to enroll in Android for Work to use this option (see Android for Work (AFW)—Google EMM enrollment).</p>
Change agent password	<ol style="list-style-type: none"> Type the new agent password in the <i>Password</i> and <i>Confirm password</i> boxes. Click CONFIRM.
Clear apps data	<ol style="list-style-type: none"> Click Add to list ⁺ for each app for which you want to clear data. Click CONFIRM.
Device alert	<ol style="list-style-type: none"> For each email address to which you want to send the alert, type the email address in the <i>Add email, then press Enter</i> box and press ENTER. <p>Tips</p> <ul style="list-style-type: none"> ◦ Your SMART Remote Management user account's email address is included by default. ◦ You can delete an email address by clicking its  button. Type the alert message in the <i>Message</i> box. Click CONFIRM.
Device settings	<ol style="list-style-type: none"> Select settings. Click ADD.
Disable apps	<ol style="list-style-type: none"> Click Add to list ⁺ for each app you want to disable. Click CONFIRM.
Enable apps	<ol style="list-style-type: none"> Click Add to list ⁺ for each app you want to enable. Click CONFIRM.
Install package	<ol style="list-style-type: none"> Select an installation package. Click ADD.
Lock	[N/A]




Option	Subsequent steps
Remote execute	<ol style="list-style-type: none"> Select a remote execution command. Click ADD.
Remove Google accounts from device	<ol style="list-style-type: none"> Select Remove all accounts to remove all Google accounts. OR Select Keep one account to retain one Google account and type that account's email address in the <i>Email account</i> box. Click CONFIRM.
Restart	[N/A]
Send files	<ol style="list-style-type: none"> Select files. Click ADD.
Send message	<ol style="list-style-type: none"> Type the message title and body text in the <i>Message Title</i> and <i>Message Body</i> boxes. Click CONFIRM.
Shutdown	[N/A]
Sound siren	[N/A]
Uninstall packages	<ol style="list-style-type: none"> Click Add To List + for each app you want to uninstall. Click UNINSTALL SELECTED.
Wake on lan	<ol style="list-style-type: none"> Select Filter or Group and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see <i>Finding devices</i> on page 11). OR Select Device and type a device's ID in the <i>Device ID</i> box to wake a single device. (Optional) Turn on Advanced wake-on-lan settings and specify the broadcast address and port for execution if your network requires this information to be provided. Click CONFIRM.
Wipe	[N/A]
Workflow	<ol style="list-style-type: none"> Select a workflow. Click ADD.

8. Click **CONFIRM**.

To initiate commands on a group using a scheduler or trigger

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Scheduler & triggers command**.
The *Scheduler & triggers command* window appears.
4. Type a name for the scheduler- or trigger-based commands in the *Command name* box.
5. Click **SELECT TRIGGER**.
The *Scheduler & triggers* window appears.
6. Select a scheduler or trigger from the list and click **ADD**.
7. Click **SELECT COMMAND** and select from the following options:

Option	Subsequent steps
Advanced messaging	<ol style="list-style-type: none"> a. Select an advanced message. b. Click ADD.
AFW install/uninstall	<ol style="list-style-type: none"> a. Select Install or Uninstall. b. Select the apps you want to install or uninstall. c. Click CONFIRM. <p>Note You need to enroll in Android for Work to use this option (see Android for Work (AFW)—Google EMM enrollment).</p>
Change agent password	<ol style="list-style-type: none"> a. Type the new agent password in the <i>Password</i> and <i>Confirm password</i> boxes. b. Click CONFIRM.
Clear apps data	<ol style="list-style-type: none"> a. Click Add to list  for each app for which you want to clear data. b. Click CONFIRM.

Option	Subsequent steps
Device alert	<p>a. For each email address to which you want to send the alert, type the email address in the <i>Add email, then press Enter</i> box and press ENTER.</p> <p>Tips</p> <ul style="list-style-type: none"> ◦ Your SMART Remote Management user account's email address is included by default. ◦ You can delete an email address by clicking its  button. <p>b. Type the alert message in the <i>Message</i> box.</p> <p>c. Click CONFIRM.</p>
Device settings	<p>a. Select settings.</p> <p>b. Click ADD.</p>
Disable apps	<p>a. Click Add to list  for each app you want to disable.</p> <p>b. Click CONFIRM.</p>
Enable apps	<p>a. Click Add to list  for each app you want to enable.</p> <p>b. Click CONFIRM.</p>
Install package	<p>a. Select an installation package.</p> <p>b. Click ADD.</p>
Lock	[N/A]
Remote execute	<p>a. Select a remote execution command.</p> <p>b. Click ADD.</p>
Remove Google accounts from device	<p>a. Select Remove all accounts to remove all Google accounts. OR Select Keep one account to retain one Google account and type that account's email address in the <i>Email account</i> box.</p> <p>b. Click CONFIRM.</p>
Restart	[N/A]
Send files	<p>a. Select files.</p> <p>b. Click ADD.</p>
Send message	<p>a. Type the message title and body text in the <i>Message Title</i> and <i>Message Body</i> boxes.</p> <p>b. Click CONFIRM.</p>
Shutdown	[N/A]







Option	Subsequent steps
Sound siren	[N/A]
Uninstall packages	<ol style="list-style-type: none"> Click Add To List + for each app you want to uninstall. Click UNINSTALL SELECTED.
Wake on lan	<ol style="list-style-type: none"> Select Filter or Group and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see <i>Finding devices</i> on page 11). OR Select Device and type a device's ID in the <i>Device ID</i> box to wake a single device. (Optional) Turn on Advanced wake-on-lan settings and specify the broadcast address and port for execution if your network requires this information to be provided. Click CONFIRM.
Wipe	[N/A]
Workflow	<ol style="list-style-type: none"> Select a workflow. Click ADD.

8. Click **CONFIRM**.

Tip

If you want to initiate the command on any new devices added to the group, see *Making group commands persistent* on page 103.

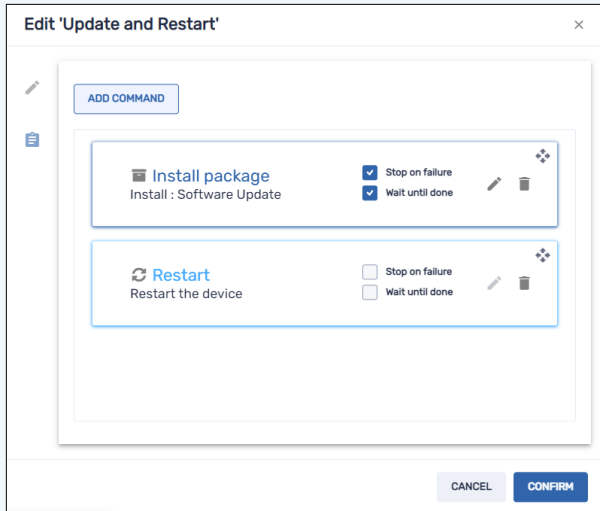
Managing workflows

					
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

A workflow allows you to run a series of commands on one or more devices in a single step. Workflows are particularly useful when you need to run commands in sequence.

Example

If you need to update software on devices then restart the devices to complete the installation, you can create a workflow that first deploys the appropriate software installation package then restarts the devices.







You can then run the workflow on appropriate devices enrolled in SMART Remote Management.


You can run a workflow on a single device, multiple devices, all devices that match a saved filter’s criteria, or a group. Alternatively, you can use a trigger to initiate a workflow at a scheduled time or when a specific event takes place (see *Managing schedulers and triggers* on page 104).

To create a workflow

1. Click **Repositories** and select **Workflow**.
The *Workflow* window appears.
2. Click **ADD NEW**.
3. Type a name and description for the workflow in the *Workflow name* and *Workflow description* boxes.
4. Click **Commands** .
5. Click **ADD COMMAND** and select from the following options:


Option	Subsequent steps
Advanced messaging	<ol style="list-style-type: none"> a. Select an advanced message. b. Click ADD.

Option	Subsequent steps
Clear apps data	<ol style="list-style-type: none"> Click Add to list  for each app for which you want to clear data. Click CONFIRM.
Device alert	<ol style="list-style-type: none"> For each email address to which you want to send the alert, type the email address in the <i>Add email, then press Enter</i> box and press ENTER. <ul style="list-style-type: none"> Tips <ul style="list-style-type: none"> ◦ Your SMART Remote Management user account's email address is included by default. ◦ You can delete an email address by clicking its  button. Type the alert message in the <i>Message</i> box. Click CONFIRM.
Device settings	<ol style="list-style-type: none"> Select settings. Click ADD.
Disable apps	<ol style="list-style-type: none"> Click Add to list  for each app you want to disable. Click CONFIRM.
Enable apps	<ol style="list-style-type: none"> Click Add to list  for each app you want to enable. Click CONFIRM.
Install package	<ol style="list-style-type: none"> Select an installation package. Click ADD.
Remote execute	<ol style="list-style-type: none"> Select a remote execution command. Click ADD.
Remove Google accounts from device	<ol style="list-style-type: none"> Select Remove all accounts to remove all Google accounts. OR Select Keep one account to retain one Google account and type that account's email address in the <i>Email account</i> box. Click CONFIRM.
Restart	[N/A]
Send files	<ol style="list-style-type: none"> Select files. Click ADD.
Send message	<ol style="list-style-type: none"> Type the message title and body text in the <i>Message Title</i> and <i>Message Body</i> boxes. Click CONFIRM.

Option	Subsequent steps
Shutdown	[N/A]
Sound siren	[N/A]
Time out	<ol style="list-style-type: none"> Type the time in minutes and seconds before devices should time out. Click CONFIRM.
Uninstall packages	<ol style="list-style-type: none"> Click Add To List  for each app you want to uninstall. Click UNINSTALL SELECTED.
Wake on lan	<ol style="list-style-type: none"> Select Filter or Group and select a filter or group in the drop-down list to wake all the devices that match the filter's or group's criteria (see <i>Finding devices</i> on page 11). OR Select Device and type a device's ID in the <i>Device ID</i> box to wake a single device. (Optional) Turn on Advanced wake-on-lan settings and specify the broadcast address and port for execution if your network requires this information to be provided. Click CONFIRM.


- For each command you added in step 4:
 - Select **Stop on failure** to stop the workflow if the command fails.
 - Select **Wait until done** to allow the command to finish running before the workflow continues to the next command.

Tip

To move a command higher or lower in the order of execution, click **Press to drag**  and drag the command up or down.

- Click **CONFIRM**.



To run a workflow on a single device

- Click **Devices**  to open the *Devices* view.
- (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
- Click the device's row.
The device's dashboard window appears.
- Click **Repository actions**, and then click **WORKFLOW**.

The *Workflow* window appears.

5. Select the workflow from the list and click **APPLY**.




To run a workflow on multiple devices

1. Click **Devices**  to open the *Devices* view.
2. (Optional) Filter the devices shown in the *Devices* view (see *Finding devices* on page 11).
3. Select the devices' check boxes.
4. Click **Workflow** .

The *Workflow* window appears.

5. Select the workflow from the list and click **APPLY**.



To run a workflow on all devices that match a saved filter's criteria

1. Click **Devices**  to open the *Devices* view.
2. Click **Filters** .
3. Click **Actions**  in the saved filter's row and select **Workflow**.

The *Workflow* window appears.

4. Select the workflow from the list and click **APPLY**

To run a workflow on a group

1. Click **Devices**  to open the *Devices* view.
2. Click **Groups** to open the *Groups* panel.
3. Click **Actions**  in the group's row and select **Workflow**.

The *Workflow* window appears.

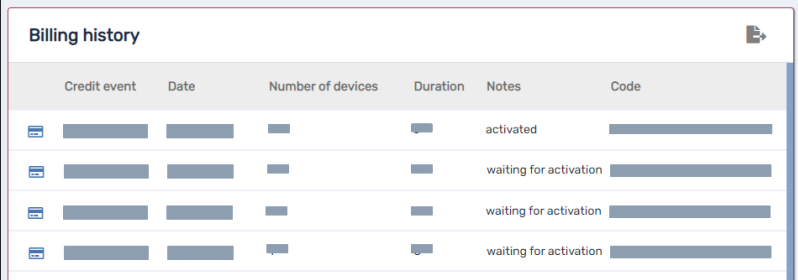
4. Select the workflow from the list and click **APPLY**

Tip

To run the workflow on any new devices added to the group, see *Making group commands persistent* on page 103.

Appendix A Troubleshooting

The following describes how to troubleshoot the most common issues encountered in SMART Remote Management. If the issue you're experiencing isn't listed or none of the solutions help resolve it, check out the [knowledge base](#), which contains articles to help with advanced troubleshooting. Search for your issue to see if any of the published resources offer a solution.

Issue	Solution																														
Forgot password	<p>If you forgot your password and can't sign in to SMART Remote Management, use these steps to reset your password.</p> <ol style="list-style-type: none">1. In a Chrome or Firefox browser, browse to the SMART Remote Management sign-in screen.2. Click Forgot password.3. Type your user name in the <i>Username</i> box and click RESET PASSWORD. An email is sent to your email address with a link to reset your password.																														
Can't enter more than one active product key OR Receive email messages about exceeding the number of devices allowed	<p>If you enter more than one unique product key, SMART Remote Management marks the first product key as "active" and all subsequent product keys as "waiting for activation."</p>  <table border="1"><caption>Billing history</caption><thead><tr><th>Credit event</th><th>Date</th><th>Number of devices</th><th>Duration</th><th>Notes</th><th>Code</th></tr></thead><tbody><tr><td></td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>activated</td><td>[redacted]</td></tr><tr><td></td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>waiting for activation</td><td>[redacted]</td></tr><tr><td></td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>waiting for activation</td><td>[redacted]</td></tr><tr><td></td><td>[redacted]</td><td>[redacted]</td><td>[redacted]</td><td>waiting for activation</td><td>[redacted]</td></tr></tbody></table>	Credit event	Date	Number of devices	Duration	Notes	Code		[redacted]	[redacted]	[redacted]	activated	[redacted]		[redacted]	[redacted]	[redacted]	waiting for activation	[redacted]		[redacted]	[redacted]	[redacted]	waiting for activation	[redacted]		[redacted]	[redacted]	[redacted]	waiting for activation	[redacted]
Credit event	Date	Number of devices	Duration	Notes	Code																										
	[redacted]	[redacted]	[redacted]	activated	[redacted]																										
	[redacted]	[redacted]	[redacted]	waiting for activation	[redacted]																										
	[redacted]	[redacted]	[redacted]	waiting for activation	[redacted]																										
	[redacted]	[redacted]	[redacted]	waiting for activation	[redacted]																										
	<p>If you enroll more devices in SMART Remote Management than are allowed for the activated product key, you might receive email messages from SMART Remote Management informing you that you have exceeded the number of devices allowed for your organization.</p> <p>In these situations, contact SMART support (smarttech.com/contactsupport). SMART support can create a single product key for all your organization's devices.</p>																														

Issue	Solution
Can't enroll a device	<p>When you enroll a device in SMART Remote Management, an authentication token is created. If you uninstall the remote management agent or perform a factory reset on the device, you'll need to reset the authentication token before you can connect the device.</p> <p>If you reset a device to its factory settings or used a wipe command in SMART Remote Management, reset the authentication token for the device (see <i>Resetting devices' authentication tokens</i> on page 63).</p>
Can't enroll a SMART Board interactive display with iQ	<p>On a SMART Board interactive display with iQ, go to Settings > Diagnostics and ensure that SMART Cloud Status is listed as operational.</p> <p>Contact SMART Support (smarttech.com/contactsupport) if SMART Cloud Status isn't operational.</p>
Can't manage a SMART Board MX100 interactive display from SMART Remote Management even though it is enrolled	<p>SMART Board MX100 interactive displays will not respond to commands from SMART Remote Management when in a low-power sleep state. The display must be fully on before it will respond to commands from SMART Remote Management.</p>
Can't install 64-bit apps on SMART Board MX (V3) and 6000S (V3) series interactive displays	<p>Download a version of the app's APK (not XAPK) file that supports the armeabi and armeabi-v7a ABI from a third-party website. Use that version of the APK file to install the app on SMART Board MX (V3) and 6000S (V3) series interactive displays.</p> <p>Example</p> <p>These are example versions of common apps that support the armeabi and armeabi-v7a ABI:</p> <ul style="list-style-type: none"> • Adobe® Acrobat® Reader® • Spotify® Premium <p>Note</p> <p>SMART Board MX (V3) and 6000S (V3) series interactive displays will support 64-bit apps by late 2022.</p>
Can't start a remote control session	<p>Disable the user permission requirement for remote control (see <i>Remotely viewing and controlling devices</i> on page 24).</p>
Running a remote control session on a SMART Board MX (V3) or 6000S (V3) series interactive display causes the display to stop responding.	<p>Stop the remote control session and restart the display. Do not run remote control sessions on SMART Board MX (V3) and 6000S (V3) series interactive displays in the future.</p> <p>Note</p> <p>SMART Board MX (V3) and 6000S (V3) series interactive displays will support remote control sessions by late 2022.</p>

Issue	Solution
Can't see devices in the <i>Devices</i> view OR Can't see users in the <i>Users</i> view	Check to see if your user account has been assigned one or more tags. If your user account has been assigned one or more tags, you can only view other users and devices assigned those same tags. If your user account is not assigned any tags, you can view all users and devices in SMART Remote Management.

SMART Technologies

smarttech.com/support

smarttech.com/contactsupport

smarttech.com/kb/171798