Mobile Devices: Overview

As an administrator, you can manage a device’s access to SAS Mobile BI, either by exclusion or inclusion. If you manage by exclusion, all devices can use the mobile reporting application, except those that are on the blacklist. If you manage by inclusion, only devices that are on the whitelist can use the mobile reporting application.

SAS Mobile BI enables users to view certain types of relational reports on iPad, iPhone, and Android devices. Supported reports are displayed in the native format of the device.

Mobile Devices: How To

Navigation

To navigate to the Mobile Devices page, from the side menu \(\equiv\), under SAS Environment Manager, click Security ⇒ Mobile Devices.

Note: This menu item is available only if you are a member of the SAS Administrators group.

Add One or More Devices to the Blacklist or Whitelist

1 On the Mobile Devices page, select the Blacklist or Whitelist tab, depending on the list to which you want to add devices.

2 To add one device to a list, click \(+\). Otherwise, to add multiple devices to a list, click \(+\).
In the Add to Blacklist or Add to Whitelist window, enter one or more device IDs. To add multiple devices, enter each device ID on a new line.

Note: No validation is performed on the information that you supply.

Click Save.

See Also
Device ID Criteria on page 4

Move One or More Devices between Lists
You can move devices from one list to the other (for example, from the blacklist to the whitelist):

1 On the Mobile Devices page, select the tab that corresponds to the list from which you want to move a device.
2 Select one or more devices that you want to move, and click.
3 In the Move Device window, click Yes.

Remove One or More Devices from a List

1 On the Mobile Devices page, select the tab that corresponds to the list from which you want to remove a device.
2 Select one or more devices that you want to remove, and click.
3 In the Confirm Remove window, click Yes.

Add a Device to a List from Last Access
You can add a device that has already connected (or attempted to connect) to the blacklist or whitelist:

1 On the Mobile Devices page, select the Last Access tab.
2 Select the device and click.
3 Select the list to which you want to add the device.
4 In the Add Device window, click Yes.

View Previous Logon Events

1 On the Mobile Devices page, select the Last Access tab.
2 To view records that were captured from devices on a prior application version or operating system version, select the Include device history option.
Determine Which List Is Enforced

There are several ways to determine whether the blacklist or whitelist is being enforced. On the Mobile Devices page, look for the following indicators:

- The list that is being enforced has a ● next to the list name.
- The list that is being enforced displays the following message above the Device ID table: ".fi This list is currently being enforced."
- The list that is not being enforced displays the following message above the Device ID table: ".fa This list is not currently being enforced."

Change How Devices Are Managed

**CAUTION!** These are deployment-level instructions that affect user access. If you change how devices are managed, you might disrupt existing users by changing which devices are eligible to connect to SAS Mobile BI.

1. Verify that the list that you intend to enforce is appropriately populated.
   - If you enforce the whitelist, the whitelist should contain all eligible devices. The blacklist is ignored.
   - If you enforce the blacklist, the blacklist should contain all excluded devices. The whitelist is ignored.

2. On the Mobile Devices page, select the tab that corresponds to the list that you want to enforce.

3. To change the list that is enabled, select the Enable blacklist or Enable whitelist option. In the confirmation window, click Yes to enable the new list.

Mobile Devices: Concepts

About Managing Mobile Devices

Here are the key points:

- You can manage devices either by exclusion or by inclusion.
  - If you manage by exclusion, all devices have access to SAS Mobile BI, except those that are on the blacklist. A blacklist is a list of mobile devices that are not authorized to use the mobile reporting application.
  - If you manage by inclusion, only devices that are on the whitelist have access to SAS Mobile BI. A whitelist is a list of mobile devices that are authorized to use the mobile reporting application.
- A deployment enforces only one list (either the blacklist or the whitelist) at a time.
- In a new deployment, the blacklist is enforced and contains no items. Therefore, all devices can access SAS Mobile BI.
- You can modify both lists. Making changes to a list that is not currently enforced can help accommodate a future change.
- The blacklist and whitelist affects devices, not users. As an administrator, you authorize what a particular user can see or do. For more information, see SAS Viya Administration: Orientation to Authorization.
About the Mobile Devices Window

Here are some details about the Mobile Devices window:

- On the Last Access tab, you can filter by selecting an item from the Filter by drop-down list.
- The Last Access tab displays logon events. A device might appear multiple times if a different user ID attempts to log on with a device that has already been captured. The following occurrences are logon events:
  - a connection attempt that comes from a new source (a unique combination of device ID and user ID)
  - a connection attempt that comes from an existing source (existing device ID and new user ID)
  - a connection attempt that is accompanied by a device change (such as a new operating system version or application version)
- On the Last Access tab, the option to add a device ID to the blacklist or whitelist will be disabled if the ID already exists on the respective list.
- On the Last Access tab, the Status column provides information about a logon event. The following table lists the status icons that might be displayed:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>●</td>
<td>Indicates that the authentication was a success.</td>
</tr>
<tr>
<td>◆</td>
<td>Indicates that the authentication was a failure.</td>
</tr>
<tr>
<td>■</td>
<td>Indicates that the device is in the blacklist.</td>
</tr>
<tr>
<td>▲</td>
<td>Indicates that the device is not in the whitelist.</td>
</tr>
</tbody>
</table>

Device ID Criteria

To add one or more devices to the blacklist or whitelist, you must enter valid device IDs. If an invalid ID is entered, you will not be able to add devices to the lists. In order for an ID to be valid, the following four conditions must be met:

- non-empty string
- length of 36 characters or less
- alphanumeric characters and hyphens
- not a duplicate of an existing device ID

Mobile Devices Service Configuration

You can customize the Mobile Devices service configuration properties. For SAS Mobile BI, you can configure which approach (whitelist or blacklist) is used to manage mobile devices. For other mobile reporting applications, you can configure the following information:

- time before the mobile application goes offline, in days
number of sequential failed attempts to enter a passcode before the user is locked out of the mobile application

how frequently a user must re-enter his or her passcode in the mobile application, in minutes

See Also
“Device Management Service” in SAS Viya Administration: Configuration Properties