Mobile: Overview

The SAS Mobile BI app enables mobile device users to view and interact with reports that can contain a variety of charts, graphs, gauges, tables, and other report objects. Supported mobile devices include iPads, iPhones, Android tablets and smartphones, and Windows 10 tablets. For information about how to use the SAS Mobile BI app, see the SAS Mobile BI Help.

As an administrator, you can control how a mobile device running the SAS Mobile BI app can access reports and data located on a SAS Visual Analytics server. You can use the following features, rules, and properties (alone or in combination) to control access to the server data and reports from the app:

Blacklist and whitelist feature
   You can manage whether a device can access servers through the SAS Mobile BI app, either by exclusion or inclusion.

Passcode properties and rule
   You can require SAS Mobile BI app users to lock the app with a passcode. You can configure two properties that control the behavior of the passcode.

Offline access time-out property and rule
   If a user has not opened the SAS Mobile BI app for a specified number of days, you can require that he or she must enter the user ID and password to access the server. The time-out is specified by a server property. You can use a rule to identify users who are exempt from the time-out.

Remote report data rule
   You can specify that when users view a report in the SAS Mobile BI app, the mobile device must maintain a network connection to the server.

Limit functionality in the app
   You can limit the functionality of the SAS Mobile BI app by applying one or more rules to a user or group of users. Functionality includes whether a user can subscribe to and view reports; share links to reports (and screen captures) by using email, text messaging, or other functionality; add or view comments; see and use the Favorites or Recent views; and view alerts.
Mobile: How To

Manage Mobile Devices

Who Can Manage Mobile Devices?
Only members of the SAS Administrators group can manage mobile devices.

Navigate to the Mobile Devices Page
Blacklists and whitelists are managed on the Mobile Devices page.
Note: This page is available only if you are a member of the SAS Administrators group.

1. Click and select Manage Environment.
2. In the navigation bar, click .

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.

TIP This option is disabled if the ID already exists on the respective list.

Complete the following steps on the Mobile Devices page:
1. Click 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.

Add One or More Devices to the Blacklist or Whitelist
Complete the following steps on the Mobile Devices page:
1. Click the Blacklist or Whitelist tab, depending on which list you want to add devices.
2. You can add one device or multiple devices to a list:
   ■ To add one device to a list, click .
     Enter the Device ID in the Add to Whitelist window.
   ■ To add multiple devices to a list, click .
     In the Add to Whitelist window, enter each Device ID to create a new line.
     Note: Validation is not performed on the device IDs as they are added to the list.
3. Click Save.

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).
Complete the following steps on the Mobile Devices page:
1. Click 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 the move button.
3. In the Move Device window, click Yes.

Remove One or More Devices from a List

Complete the following steps on the Mobile Devices page:
1. Click 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 the remove button.
3. In the Confirm Remove window, click Yes.

View Logon Event Information

Complete the following steps on the Mobile Devices page:
1. Click the Last Access tab.
2. View the device logon event information, including status. See “Device Logon Information”.

TIP: Use the Filter by drop-down list to filter the information about the tab.

View Previous Logon Events

You can view records that were captured from devices on a prior application version or operating system version.

Complete the following steps on the Mobile Devices page:
1. Click the Last Access tab.
2. 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:
  “This list is currently being enforced.”.
- The list that is not being enforced displays the following message above the Device ID table:
  “This list is not currently being enforced.”.

Change How Devices Are Managed

CAUTION! These are deployment-level instructions that affect user access. Changing how devices are managed can disrupt existing users by changing which devices are eligible to connect to servers through the SAS Mobile BI app.

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, click the tab that corresponds to the list that you want to enforce.
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.

**Limit Functionality**

Initially, all authenticated users can access all functionality in the SAS Mobile BI app.

1. To limit access to functionality, locate the relevant authorization rule.
2. Change the principal from its initial value (Authenticated Users) to a different value (for example, the group ID for a custom group).

   **Note:** Users who are within the scope of a revised rule have access to the functionality that the rule provides. Other users do not have access to the functionality that the rule provides.


**Limit Caching of Report Data**

Initially, all mobile devices cache report data. To change this behavior:

1. Locate and adjust the following predefined authorization rule:

   - **Object URI:** /SASMobileBI_capabilities/cacheMobileReportData
   - **Principal:** Authenticated Users

2. Choose one of the following:

   - To prevent all caching of report data, disable the rule.
   - To selectively prevent caching of report data, change the principal from its initial value (Authenticated Users) to an alternate value (for example, the group ID for a custom group).

   **Note:** For users who are within the scope of the revised rule, report data is cached. For users who are outside the scope of the revised rule, report data is downloaded when a report is open and purged when the report is closed. Offline access to reports is not supported for users who are outside the scope of the revised rule.

For details, see “Adjust Rules for Access to Functionality” in SAS Viya Administration: Identity Management.

**Manage Passcode Requirements**

Initially, use of a passcode is not required. However, you can require passcodes or adjust passcode constraints.

**Require Passcodes**

1. Locate and adjust the following predefined authorization rule:

   - **Object URI:** /SASMobileBI_capabilities/exemptFromPasscodeRequirements
   - **Principal:** Authenticated Users

2. Choose one of the following:

   - To require all users to use a passcode, disable the rule.
   - To require some users to use a passcode, change the principal from its initial value (Authenticated Users) to an alternate value (for example, the group ID for a custom group).

   **Note:** Users who are within the scope of the revised rule can choose to use a passcode, but they are not required to do so. Users who are outside the scope of the revised rule must use a passcode.
Adjust Passcode Constraints
To adjust the passcode constraints, use the passcodeAttempts and passcodeTimeoutMinutes properties in the sas.devicemanagement configuration definition.
1 Click and select Manage Environment.
2 In the navigation bar, click .
3 In the View list, choose Definitions.
4 In the Filter field, type device.
5 Select sas.devicemanagement from the results. The configuration properties appear in the right pane.
6 Click .
7 Edit the value in the passcodeAttempts field to configure the passcode lock-out behavior.
8 Edit the value in the passcodeTimeoutMinutes field to configure the passcode time-out behavior.
9 Click Save.

Manage Offline-Access Time-Outs
Initially, no users are subject to time-outs for offline access. However, you can prevent time-outs and adjust the time-out interval.

Prevent Time-Outs
To implement time-outs for offline access:
1 Locate and adjust the following predefined authorization rule:
   Object URI: /SASMobileBI_capabilities/exemptFromOfflineTimeLimit
   Principal: Authenticated Users
2 Choose one of the following:
   ■ To make all users subject to time-outs, disable the rule.
   ■ To make some users subject to time-outs, change the principal from its initial value (Authenticated Users) to an alternate value (for example, the group ID for a custom group).
   Note: Users who are within the scope of the revised rule are exempt from time-outs. Users who are outside the scope of the revised rule are subject to time-outs.
For details, see “Adjust Rules for Access to Functionality” in SAS Viya Administration: Identity Management.

Adjust the Time-Out Interval
To adjust the time limit, set the offlineLimitDays property in the sas.devicemanagement configuration definition.
1 Click and select Manage Environment.
2 In the navigation bar, click .
3 In the View list, choose Definitions.
4 In the Filter field, type device.
5 Select sas.devicemanagement from the results. The configuration properties appear in the right pane.
6 Click .
7 Edit the value in the offlineLimitDays field. Specify, in days, how many days a device can be offline without requiring the user log on to the server when opening SAS Mobile BI app again.
8 Click Save.
Mobile: Concepts

SAS Viya provides ways to manage mobile devices and the security of reports and data accessed by means of a SAS Viya server. You can manage mobile devices by using a combination of configuration properties for the server and rule authorizations that control the access of mobile device users to the server.

Prerequisites for Managing Mobile Devices

To manage mobile devices, you must be a SAS administrator, and your user ID must have the device management rule authorization for mobile devices. By default, SAS administrators already are granted authorization for the /deviceManagement_capabilities/manageMobileDevices rule.

Prerequisites for Mobile Device Access

The SAS Mobile BI app uses the /SASMobileBI/** authorization rule to identify those who can log on to the server from the app. By default, all authenticated users are added to this rule. A SAS administrator can choose to update the rule to identify users or groups of users to prohibit from using the app.

Blacklist and Whitelist Features

Overview

The whitelist manages the devices that can access servers by using the SAS Mobile BI app. A device must be on the whitelist in order to use SAS Mobile BI on your network. The whitelist affects devices, not users. If a device is lost, a SAS administrator can remove the device from the whitelist and prevent access to the reports and data.

The blacklist manages the devices that cannot access servers by using the SAS Mobile BI app. All devices can use SAS Mobile BI on your network except those that are on the blacklist. The blacklist affects devices, not users. If a device is lost, a SAS administrator can add the device to the blacklist and prevent access to the reports and data.

Considerations

Here are the key points for managing mobile devices:

- You can manage devices either by exclusion or by inclusion.
  - If you manage by exclusion, all devices can access servers through the SAS Mobile BI app, except those that are on the blacklist. A blacklist is a list of mobile devices that are not authorized to use the SAS Mobile BI app.
  - If you manage by inclusion, only devices that are on the whitelist can access servers through the SAS Mobile BI app. A whitelist is a list of mobile devices that are authorized to use the SAS Mobile BI app.
- 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 servers through the SAS Mobile BI app.
- 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 affect devices, not users. As an administrator, you authorize what a particular user can see or do. For more information, see “SAS Viya Administration: General Authorization” in SAS Viya Administration: General Authorization.

Add Devices by User ID

The easiest way to add a device to the whitelist or blacklist is to add a device that has already connected (or attempted to connect) to the server. When the attempt is made, the Last Access tab logs the device owner’s user ID, device ID, device type, and other information. You can sort the User ID column to locate the user ID of the person whom you want to add.

Restricting and enabling devices by user ID is a best practice because users can have more than one device. By identifying the user ID, you can be sure to add all devices used by that person.

TIP The only way to add a device running Windows 10 is by user ID.

Passcode Feature

Overview

The passcode feature locks the SAS Mobile BI app. This feature is separate from and in addition to the passcode feature that is provided by mobile devices. There are two types of app passcodes: required and optional.

A required passcode is a passcode that is required by the server. When the app first connects to the affected server, the server forces the app to require that the app user create a passcode. Then, whenever the app user opens the app or views a report that is associated with that server, the user must enter the passcode.

Note: By using an additional rule, the SAS administrator can exempt app users from using a passcode. By using a combination of two rules, all mobile devices that access the server must use a passcode except for those separately exempted.

An optional passcode is a passcode that the app user can choose to use to lock the app. The passcode is not required to access the server. The app user can disable the passcode at any time.

Considerations

Here are some key points to remember when working with passcodes:

- The passcode should be known only to the app user. If the app user loses the mobile device, no one else should be able to guess the passcode and use it to open the app.

- The passcode has a time-out feature. The SAS administrator can customize the passcodeTimeoutMinutes setting to configure this feature. This setting specifies, in minutes, how long a user must wait before re-entering his or her passcode in the SAS Mobile BI app. The default is 15.

  If the app user (or another person) provides an incorrect passcode a specific number of times (passcodeAttempts), the app locks itself for a length of time (passcodeTimeoutMinutes). The app user can enter the passcode again after the time-out expires.

- The passcode has a lock-out feature. The SAS administrator can customize the passcodeAttempts setting to configure this feature. The setting limits the number of sequential, failed attempts to enter a passcode for the SAS Mobile BI app. The default is 5.

  If a user reaches the specified limit (passcodeAttempts), the user is timed out of the app for 15 minutes (or the value set for passcodeTimeoutMinutes). After the time-out interval, the user can make one more attempt to enter his or her passcode. If the password fails again, all custom content (data, reports, settings, and connection information) is removed from the mobile device. The app is reset to its default settings.
If the app user forgets the passcode, the app user must delete and re-install the app on the device. Doing so deletes the reports and data.

For information about how app users set a passcode, see the SAS Mobile BI Help. Be sure to view the Help for the platform (iOS, Android, or Windows 10) and release that you are using.

Remote Report Data Feature

Remote Report Data

When you subscribe to a report, it appears in the Subscriptions view of SAS Mobile BI. However, depending on the security assigned to the user ID, the report data might not exist on the mobile device. Report data can be local or remote:

- **Local** data is stored on the mobile device.
- **Remote** data exists on the mobile device only while the report is open and the device is connected to a Wi-Fi or cellular network. If a report uses remote data, the report tile in the Subscriptions view displays the cloud icon.

How Remote Data Works

Each time you open a report with remote data, the app connects to the server. The Prepare Data notification is displayed while the data is downloaded. The report opens when the data is available on the mobile device. The data is available only while you view the report.

After you close the report, the data is removed from the device. The thumbnail image on the report tile no longer appears. If you are not connected to a network and you try to open the report, it does not open.

This feature affects the user ID that is used to access the server. When you access the server via SAS Mobile BI using that user ID, all reports on that server use the remote report data feature.

Prevent Mobile Devices from Storing Report Data

The /SASMobileBI_capabilities/cacheMobileReportData rule specifies that a mobile device can store (or cache) report data on the device when it is not connected to a network. By default, all authenticated users’ mobile devices can cache report data.

If you want to enforce additional security by preventing mobile devices from storing report data, then you must prohibit the rule authorization that is applied to a user or group of users.

Offline-Access Time-Out Feature

If a user has been offline for a specified number of days, he or she must sign in to the server used by the SAS Mobile BI app. For example, if the user attempts to browse reports on the server or open a report in the report viewer, the app requires the user to enter the password for the requested server connection. If the user fails to sign in, then the app no longer downloads reports, updates subscribed reports, or opens reports for viewing.

This feature is not only useful when the device is missing. It also provides security when the employee leaves the organization but keeps the device. The blacklist and whitelist features require that the device must access the server before the list can look up the device to deny or permit access. The offline access time-out feature denies access by checking the employee’s credentials, which the IT organization revokes when the employee leaves the organization.
Mobile: Reference

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 cannot add devices to the lists. In order for an ID to be valid, the following conditions must be met:
- non-empty string
- length of 36 characters or less
- contains alphanumeric characters and hyphens
- is not a duplicate of an existing device ID

Device Logon Information
A device might appear multiple times in the blacklist or whitelist 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)

The following table lists the device status icons that might be displayed:

Table A.1 Status Icons and Descriptions

<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>

Rules to Control Access to SAS Mobile BI App Functionality
You can limit the functionality of the SAS Mobile BI app by applying one or more rules to a user or group of users.

The following table lists the rules that enable you to limit a user’s access to functionality in the SAS Mobile BI app:
**Table A.2  Rules and Descriptions**

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCESS_MOBILE_BI</td>
<td>Enables a user to subscribe to and view reports.</td>
</tr>
<tr>
<td>ACCESS_RECENTS</td>
<td>Enables a user to see items for a particular server in their Recent view. It also enables the user, in Add Reports, to see the contents of the Recent folder for that server.</td>
</tr>
<tr>
<td>ADD_COMMENTS</td>
<td>Enables a user to add comments to a report or its contents.</td>
</tr>
<tr>
<td>EMAIL</td>
<td>Enables a user to share links to reports (and screen captures) by using email, text messaging, or other functionality.</td>
</tr>
<tr>
<td>EXPORT_DATA</td>
<td>Enables a user to export data for a report object.</td>
</tr>
<tr>
<td>EXPORT_DETAILED_DATA</td>
<td>Enables a user to select the <strong>Detailed data</strong> option (if applicable) in the Export Data window.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>The EXPORT_DATA rule takes precedence over this rule. If a user ID is not authorized to use the EXPORT_DATA rule, then authorizing the EXPORT_DETAIL_DATA rule to that user ID has no effect.</td>
</tr>
<tr>
<td>MANAGE_FAVORITES</td>
<td>Enables a user to add a report to the Favorites view or to remove a report from the Favorites view.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>The VIEW_FAVORITES rule takes precedence over this rule. If a user ID is not authorized to view favorites, the user cannot add or remove favorites, even if the user is authorized to use the MANAGE_FAVORITES rule.</td>
</tr>
<tr>
<td>SUBSCRIBE_TO_REPORT_ALERTS</td>
<td>Enables a user to view alerts in a report and to subscribe to them.</td>
</tr>
<tr>
<td>VIEW_COMMENTS</td>
<td>Enables a user to view the comments that are associated with a report or its content.</td>
</tr>
<tr>
<td>VIEW_FAVORITES</td>
<td>Enables a user to see items for a particular server in the Favorites view. It also enables the user, in Add Reports, to see the contents of the Favorites folder for that server.</td>
</tr>
</tbody>
</table>

**Mobile: Troubleshooting**

**TIP** For more troubleshooting information about the SAS Mobile BI app, see the SAS Mobile BI Help. Be sure to view the Help for the platform (iOS, Android, or Windows 10) that you are using.

**A user cannot open reports on an offline device.**

**Explanation:**
- The user ID might be required to use remote report data.
- The user ID might be affected by the offline-access time out.
Resolution:
If the user ID is subject to the remote report data authorization rule, make sure the user understands that he or she must be connected to a network while viewing the report. See “Remote Report Data Feature”.

If the user ID is subject to the offline-access time out authorization rule, make sure the user can log on to the server connection in the SAS Mobile BI app. See “Offline-Access Time-Out Feature”.

A user is prompted for an application passcode.

Explanation:
The user is required to secure the SAS Mobile BI app with a passcode. See “Passcode Feature”.

Resolution:
To learn how to create a required passcode in the SAS Mobile BI app, see the SAS Mobile BI Help.

Note: Be sure to view the Help for the platform (iOS, Android, or Windows 10) that you are using.

In the Mobile Devices window, a message indicates that a list is not currently in use.

Explanation:
By design, only one list (either the blacklist or the whitelist) is in use.

Blacklist and whitelist status displays 'status unknown'.

Explanation:
If you are working in a multi-tenant environment, then device configuration properties are not available to display the status of the blacklist and whitelist. These properties are available only in the provider tenant configuration. Other locations show a status of 'unknown' unless the administrator specifically sets configuration properties for the individual tenant locations.