



SAS[®] Viya[®] Platform: Mobile Device Administration

2020.1 - 2024.11

This document might apply to additional versions of the software. Open this document in [SAS Help Center](#) and click on the version in the banner to see all available versions.

Mobile: Overview	2
Mobile: How To	3
Manage Mobile Devices	3
Limit Functionality	5
Adjust Passcode Constraints	6
Adjust the Time-Out Interval	6
Configure an Additional External URL	7
Mobile: How To (CLI)	7
Examples	7
Mobile: Concepts	8
Prerequisites for Managing Mobile Devices	8
Allowlist and Denylist Features	9
Passcode Feature	10
Cache Report Data Feature	11
Offline-Access Time-Out Feature	12
Report State	12
Natural Language	12
Mobile: Reference	13
Device ID Criteria	13
Device Logon Information	13
Rules to Control Access to SAS Visual Analytics App Functionality	14
Mobile: Troubleshooting	16

<i>Mobile: Interfaces</i>	17
Interfaces to Mobile	18
<i>Mobile: Software Development Kits</i>	18

Mobile: Overview

The SAS Visual Analytics App (previously called SAS Mobile BI) 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 personal computers. For information about how to use the SAS Visual Analytics App, see [SAS Visual Analytics Apps](#).

As an administrator, you can control how a mobile device running the SAS Visual Analytics 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.

Note: These settings and features can also be used to manage custom mobile apps that you create using Software Development Kits (SDKs), SAS SDK for Android or SAS SDK for iOS. For more information, see [“Mobile: Software Development Kits” on page 18](#).

Allowlist and denylist feature

You can manage whether a device can access servers through the SAS Visual Analytics App, either by inclusion or exclusion.

Note: The device ID that is added to the allowlist or denylist is validated, not the device itself.

Passcode properties and rule

You can require SAS Visual Analytics 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 Visual Analytics App for a specified number of days, you can require the user to 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 Visual Analytics 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 Visual Analytics App by applying one or more rules to a user or group of users. Functionality includes whether a user can do the following:

- add reports to the app 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

Navigate to 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 allowlist or denylist by completing the following steps:

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

- 1 On the Mobile Devices page, 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 Allowlist or Denylist

- 1 On the Mobile Devices page, click the **Allowlist** or **Denylist** tab, depending on which list you want to add devices to.
- 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 AllowlistAdd to Allowlist or Add to Denylist window.

- To add multiple devices to a list, click .

In the Add to Allowlist or Add to Denylist 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 allowlist to the denylist).

- 1 On the Mobile Devices page, 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 .
- 3 In the Move Device window, click **Yes**.

Remove One or More Devices from a List

- 1 On the Mobile Devices page, 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 .
- 3 In the Confirm Remove window, click **Yes**.

View Logon Event Information

- 1 On the Mobile Devices page, click the **Last Access** tab.
- 2 View the device logon event information, including status. For more information, see [“Device Logon Information”](#).

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

View Previous Logon Events

- 1 On the Mobile Devices page, click 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 allowlist or denylist 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.”
- On the **Dashboard**, look on the **Mobile Devices** tile.
- Run the following command-line interface (CLI) command and look at the output:

```
sas-viya devices enforcement status
```

For more information about how to run the device management CLI, see [“Command-Line Interface: Instructions when Downloading the CLI” in SAS Viya Platform: Using the Command-Line Interface](#).

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 Visual Analytics App. Adding a device to the denylist deletes all existing connections and reports from that device.

- 1 Verify that the list that you intend to enforce is appropriately populated.
 - If you enforce the allowlist, the allowlist should contain all eligible devices. The denylist is ignored.
 - If you enforce the denylist, the denylist should contain all excluded devices. The allowlist is ignored.
- 2 On the **Mobile Devices** page, click the tab that corresponds to the list that you want to enforce.
- 3 To change the list that is enabled, click **Enable**.
- 4 In the confirmation window, click **Yes** to enable the new list.

Limit Functionality

Initially, all authenticated users can access all functionality in the SAS Visual Analytics App. To change this behavior:

- 1 Locate the relevant authorization rule. For a list of the mobile-specific rules, see [“Rules to Control Access to SAS Visual Analytics App Functionality”](#) on page 14.
- 2 Choose one of the following:
 - Disable the rule.
 - Change the principal type 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.

For information about functionality, see [“Access to Functionality: How To \(Basic Approach\)”](#) in *SAS Viya Platform: Access to Functionality*.

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**.

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 Visual Analytics App again.
- 8 Click **Save**.

Configure an Additional External URL

In the SAS Viya platform, the `sas.url.external.viya` value might need to be configured. This is because SAS Visual Analytics alert and report distribution emails contain a report link for `localhost` if the value for `sas.url.external.viya` is not configured. To use a different URL prefix for external URLs, you can modify the initial `kustomization.yaml` file prior to deployment. Below is an example `kustomization.yaml` file:

```
name: sas-shared-config
behavior: merge
literals:
- SAS_SERVICES_URL=external-URL
- SAS_URL_EXTERNAL_VIYA=external-proxy-URL
```

For detailed information about `kustomization.yaml`, see [“Initial kustomization.yaml File” in SAS Viya Platform: Deployment Guide](#).

If you have already deployed the SAS Viya platform and need to modify the `sas.url.external.viya` value, you can modify the customization by repeating the steps of your initial deployment. For more information see [“Modify Existing Customizations in a Deployment” in SAS Viya Platform: Deployment Guide](#).

Mobile: How To (CLI)

The following examples assume that you have already signed in to the SAS Viya platform at the command line. See [“Command-Line Interface: Instructions when Downloading the CLI” in SAS Viya Platform: Using the Command-Line Interface](#).

Examples

Example: Determine whether the device with ID `device1` is authorized for use in the environment.

```
sas-viya devices authorized-devices validate --device-id device1
```

Example: Show whether the allowlist or denylist is being enforced.

```
sas-viya devices enforcement status
```

Example: Add the device with ID device1 to the allowlist.

```
sas-viya devices allowlist add --device-id device1
```

Example: List the devices that are enabled in the allowlist.

```
sas-viya devices allowlist list
```

Example: Add the device with ID device1 to the denylist.

```
sas-viya devices denylist add --device-id device1
```

Example: Remove the device with ID device1 from the denylist.

```
sas-viya devices denylist delete --device-id device1
```

Example: From a list of the devices of type iPhone that have connected or attempted to connect to the server, add a specific iPhone to the denylist.

```
1 sas-viya devices last-access list --device-type iPhone
2 sas-viya devices denylist add --device-id device-id
```

- 1 List the last-access attempts of all devices of type iPhone.
- 2 Add a device to the denylist using the device ID that was identified in the previous step.

Example: List in fulljson output the last access attempts to the server for all devices.

```
sas-viya --output fulljson devices last-access list
```

See Also

[“Command-Line Interface: Overview” in SAS Viya Platform: Using the Command-Line Interface](#)

Mobile: Concepts

The SAS Viya platform provides ways to manage mobile devices and the security of reports and data. You can manage mobile devices by using a combination of configuration properties for the server and authorization rules 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 authorization rules for mobile devices. Initially, the SAS Administrators group has Read and Write access to the `/deviceManagement_capabilities/manageMobileDevices` object URI.

Allowlist and Denylist Features

Overview

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

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

IMPORTANT To help ensure that unauthorized individuals do not gain access to your servers through the allowlist feature, ensure that a password policy is enforced with strict password controls.

Considerations

Here are the key points for managing mobile devices:

- You can manage devices either by exclusion or by inclusion.
 - If you manage by inclusion, only devices that are on the allowlist can access servers through the SAS Visual Analytics App. An allowlist is a list of mobile devices that are authorized to use the SAS Visual Analytics App.
 - If you manage by exclusion, all devices can access servers through the SAS Visual Analytics App, except those that are on the denylist. A denylist is a list of mobile devices that are not authorized to use the SAS Visual Analytics App.
- A deployment enforces only one list (either the allowlist or the denylist) at a time.
- In a new deployment, the denylist is enforced and contains no items. Therefore, all devices can access servers through the SAS Visual Analytics App.
- You can modify both lists. Making changes to a list that is not currently enforced can help accommodate a future change.
- The allowlist and denylist affect devices, not users. As an administrator, you authorize what a particular user can see or do. For more information, see [SAS Viya Platform: General Authorization](#).
- The device ID that is added to the allowlist or denylist is validated, not the device itself.

Add Devices by User ID

The easiest way to add a device to the allowlist or denylist 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.

Passcode Feature

Overview

The passcode feature locks the SAS Visual Analytics 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 Visual Analytics 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 Visual Analytics 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 [SAS Visual Analytics Apps](#). Be sure to view the Help for the platform (iOS or Android) and release that you are using.

Cache Report Data Feature

Cache Report Data

When a user adds a report to the SAS Visual Analytics App, the report appears in **My Reports**. 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 **My Reports** displays the cloud icon.

How Cache Report Data Works

Each time a user opens a cached report, 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 the user views the report.

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

This feature affects the user ID that is used to access the server. When the user accesses the server via the SAS Visual Analytics App using that user ID, all reports on that server use the caching 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 authorization rule 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 Visual Analytics 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 downloaded 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 allowlist and denylist 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.

Report State

When you view reports located on servers running SAS Visual Analytics 8.3 or later, the state of your report is saved when you close the report.

Note: This feature also applies to the report viewer.

The *report state* can include selections that you have made in charts and graphs, interactions between objects, navigation into a hierarchy or Esri map, and much more.

If you use multiple devices (for example, a tablet and a phone) to view and update reports, the report state on the server reflects the most recent updates made before closing the report on any device.

Note: Large reports might require additional time to close because the SAS Visual Analytics App is saving many selections.

For more information about the report state, see the Report and Data Interactions section of [“URIs for Applications” in SAS Viya Platform: Access to Functionality](#).

Natural Language

The voice assistant feature enables you to interact with the SAS Visual Analytics App by using voice commands. The voice assistant recognizes voice commands that are spoken in English only.

Note: The voice assistant is available only when the app is connected to a server running SAS Visual Analytics 8.3 or later.

Mobile: Reference

Device ID Criteria

To add one or more devices to the allowlist or denylist, 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 allowlist or denylist 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 1 *Status Icons and Descriptions*

Icon	Description
	Indicates that the authentication was a success.
	Indicates that the authentication was a failure.
	Indicates that the device is not in the allowlist.

Icon	Description
	Indicates that the device is in the denylist.
	Indicates that the device is in an unknown state. Note: This icon indicates that there may be a failure to authenticate.

Rules to Control Access to SAS Visual Analytics App Functionality

You can limit the functionality of the SAS Visual Analytics 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 Visual Analytics App:

CAUTION

Rule Modification Most of the rules in the table are not specific to the SAS Visual Analytics App. Therefore, careful consideration should be taken before making modifications to those rules that affect other applications. For more information, see [SAS Viya Platform: Access to Functionality](#).

Table 2 Rules and Descriptions

Object URI	Description	Rule Specific to SAS Visual Analytics App
/comments/comments	Create permission enables users to add comments to a report or its contents. Read permission enables users to view the comments that are associated with a report or its content.	No
/deviceManagement_capabilities/manageMobileDevices	Enables users to manage mobile device denylist, allowlist, and device access history. Initially granted to SAS administrators.	Yes
/folders/folders/@myFavorites	Create permission enables users to add a report to the Favorites view. Delete permission enables users to remove a report from the Favorites view. Read permission enables users to view items for a particular server in the	No

Object URI	Description	Rule Specific to SAS Visual Analytics App
	Favorites view. It also enables the user, in Add Reports, to see the contents of the Favorites folder for that server. Note: When Read permission is granted, it takes precedence over Create and Delete permissions. If a user is not authorized to view favorites, the user cannot add or remove favorites, even if the user was granted Create and Delete permission.	
/folders/folders/@myHistory	Enables users 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.	No
/reportAlerts/*	Enables users to view alerts in a report and add reports to the app.	No
/reportData_capabilities/exportData	Enables users to export data for a report object.	No
/reportData_capabilities/exportDetailData	Enables users to select the Detailed data option (if applicable) in the Export Data window. Note: 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.	No
/reportRenderer/reports	Enables users to access PDF printing of reports.	No
/reportViewerNaturalLanguageUnderstanding/interpretations	Enables users to process natural language on an iOS app. Note: Current support for this feature is provided only by the iOS version of SAS Visual Analytics App.	No
/SASMobileBI/**	Enables users to add reports to the app and view reports. It also controls whether the user can define a connection to the server within the SAS Visual Analytics App.	Yes
/SASMobileBI_capabilities/allowWebContent	Enables users to render reports with web content.	Yes
/SASMobileBI_capabilities/cacheMobileReportData	Enables users to cache mobile report data from within the SAS Visual Analytics App. This is required for offline access to reports. For users who do not have this capability, report data is retained on the device only while the report is open.	Yes

Object URI	Description	Rule Specific to SAS Visual Analytics App
	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.	
/SASMobileBI_capabilities/exemptFromOfflineTimeLimit	Enables users to be exempt from the SAS Visual Analytics App offline time-out. Initially, no users are subject to time-outs for offline access. 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.	Yes
/SASMobileBI_capabilities/exemptFromPasscodeRequirements	Enables users to be exempt from the requirement to enter a passcode to access the SAS Visual Analytics App. Initially, use of a passcode is not required. However, you can require passcodes or adjust passcode constraints. Note: If any of the mobile server connections require a passcode, then it is still required to access the application. This is true even if the exemption rule is in effect. In addition, users can enable a passcode even if the exemption rule is in effect.	Yes
/SASVisualAnalyticsCommon_capabilities/shareReport	Enables users to share links to reports (and screen captures) by using email, text messaging, or other functionality.	No
/webDataAccess/esri/user/token	Enables mobile users to view Esri maps.	No

Mobile: Troubleshooting

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 [“Cache 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 Visual Analytics App. See [“Offline-Access Time-Out Feature”](#).

A user is prompted for an application passcode.

Explanation:

The user is required to secure the SAS Visual Analytics App with a passcode. See [“Passcode Feature”](#).

Resolution:

To learn how to create a required passcode in the SAS Visual Analytics App, see [SAS Visual Analytics Apps](#).

Note: Be sure to view the Help for the platform (iOS or Android) and release the user is accessing.

On the Mobile Devices page, a message indicates that a list is not currently in use.

Explanation:

By design, only one list (either the allowlist or the denylist) is in use.

As an administrator, you are unable to change the allowlist or denylist using the Enable or Disable button.

TIP For more troubleshooting information about the SAS Visual Analytics App, see [SAS Visual Analytics Apps](#).

Be sure to view the Help for the platform (iOS or Android) and release the user is accessing.

Mobile: Interfaces

There are multiple interfaces available to administer mobile devices. In the following table, the shaded part of each circle is an approximation of the amount of mobile functionality that a particular interface exposes. The shading indicates relative coverage. The shading does not indicate alignment of functional coverage across interfaces.

Table 3 *Interfaces to Mobile*

Coverage Amount	Interface	Description
	Command-line interface	A simple scriptable interface that provides commands for accessing the Device Management command-line interface. For details, see “ Mobile: How To (CLI) ” on page 7.
	SAS Environment Manager	A graphical enterprise web application used to access Mobile Devices. For details, see “ Mobile: How To ” on page 3.

Mobile: Software Development Kits

The Software Development Kits (SDKs), SAS SDK for Android or SAS SDK for iOS, enable your mobile apps to include SAS Visual Analytics content. You can preconfigure, customize, and manage the app experience by doing the following:

- Creating custom mobile apps for viewing and interacting with SAS Visual Analytics report content.
- Substituting your organization’s name and branding in the SAS Visual Analytics App.
- Displaying SAS Visual Analytics reports in a custom-designed app.
- Integrating the mobile app with your mobile device management (MDM) service.

Your customized apps can connect to SAS Viya platform servers and can be managed by your organization’s SAS administrators. The SAS SDK is free and available for iOS and Android operating systems. It can be downloaded from <https://developer.sas.com>.