SOPHOS

Cybersecurity made simple.

Sophos Mobile

app groups interface guide

product version: 9.5

Contents

1 About this guide

This guide explains how to manage app groups using the RESTful web service interface of Sophos Mobile.

Typically, this is used by third-party app reputation vendors to integrate app reputation information into Sophos Mobile.

2 App reputation support

In Sophos Mobile you can define list of apps, called app groups, for app reputation purposes. For example:

- Apps that users are allowed to install on their devices (allowed apps).
- Apps that users are not allowed to install on their devices (forbidden apps).

When you define allowed apps, all other apps not included in the app group are forbidden.

When you define forbidden apps, all other apps not included in the app group are allowed.

App groups contain apps for a specific device platform. To cover apps from more than one platform, you need to create separate app groups.

Note
App groups in themselves do not include any app reputation classification. They merely are a collection of apps. The app reputation classification is established within Sophos Mobile by using an app group for a certain purpose, that is, to define allowed or forbidden apps.

3 The app groups web service interface

Sophos Mobile offers a RESTful web service to manage app groups. This interface can be used by third-party app reputation vendors to integrate app reputation information into Sophos Mobile.

For security reasons, the web service only supports HTTPS access. Communication is encrypted with the same SSL/TLS certificate that is used for the Sophos Mobile console and Self Service Portal.

Tip
In Sophos Mobile there is special administrator role **App Group Administrator** that has sufficient rights to create, update and read app groups.

Basically, the management of app groups through the web service interface includes the following workflow:

1. Perform a `POST /rs/login` request, sending the credentials (that is, customer name, login name, password) of a Sophos Mobile administrator account.

   The service returns a session authentication token that is required to access the web service resources.

2. Perform the required requests.
   - To create an app group, use
     - `POST /rs/androidappgroup`
     - `POST /rs/iosappgroup`
     - `POST /rs/macosappgroup`
     - `POST /rs/windowsdesktopappgroup`
     - `POST /rs/windowsphoneappgroup`
   - To retrieve a list of defined app groups, use
     - `GET /rs/androidappgroup`
     - `GET /rs/iosappgroup`
     - `GET /rs/macosappgroup`
     - `GET /rs/windowsdesktopappgroup`
     - `GET /rs/windowphoneappgroup`
   - To retrieve the properties of a certain app group (including the properties of the contained apps), use
     - `GET /rs/androidappgroup/:id`
     - `GET /rs/iosappgroup/:id`
     - `GET /rs/macosappgroup/:id`
     - `GET /rs/windowsdesktopappgroup/:id`
     - `GET /rs/windowsphoneappgroup/:id`

     where `:id` is the internal identifier of the app group.

- To update the properties of an existing app group (for example, to add or remove apps or to change the app group name), use
  - `PUT /rs/androidappgroup/:id`
  - `PUT /rs/iosappgroup/:id`
  - `PUT /rs/macosappgroup/:id`
  - `PUT /rs/windowsdesktopappgroup/:id`
  - `PUT /rs/windowsphoneappgroup/:id`

  where `:id` is the internal identifier of the app group.

3. When you are finished, perform a `POST /rs/logout` request to log out from Sophos Mobile.

For details of the web service API, see API description (page 5).

Note
The session authentication token expires after 60 seconds of inactivity.

4 API description

4.1 Log in

Log in to the Sophos Mobile server.

The `/rs/login` resource returns a session authentication token that is required to access the other web service resources. This token expires after 60 seconds of inactivity.

URL

`https://<smc_server_address>/rs/login`

Method

POST

Request header

Key	Value
Content-Type	`application/x-www-form-urlencoded`

Request body

Form data, containing these properties:

Key	Description
customer	A customer name.
user	An administrator log-in name for that customer.
password	The administrator password.

Response body

JSON object with the following structure:

Key	Type	Description
userName	String	Administrator log-in name.
authToken	String	Session authentication token.
loginDate	Integer	Log-in timestamp in epoch milliseconds.
rights	Array of strings	List of rights that are granted to the administrator.

The administrator must have the following rights to be able to manage app groups:

- `APP_GROUPS_BROWSE`
- `APP_GROUPS_CREATE`
- `APP_GROUPS_SHOW`
- `APP_GROUPS_UPDATE`

HTTP response status

Status code	Description
200 OK	Administrator was successfully logged in.
401 Unauthorized	Administrator is not authorized to access the resource.

Example request

```
POST /rs/login HTTP/1.1
Host: smc.example.com
Content-Type: application/x-www-form-urlencoded
customer=myCustomer&user=myAdminName&password=myPassword
```

Example response

```
{
   "userName": "myAdminName",
   "authToken": "da81d6d2-3c02-4f18-8115-f4188d84e851",
   "loginDate": 1452258438634,
   "rights": [
      <array of granted rights>
   ]
}
```

4.2 Log out

Log out from the Sophos Mobile server.

URL

`https://<smc_server_address>/rs/logout`

Method

POST

Request header

Key	Value
X-SMCRS-Auth-Session	Session authentication token from the login response.

Request body

empty

Response body

empty

HTTP response status

Status code	Description
200 OK	Administrator was successfully logged out.
401 Unauthorized	Administrator is not authorized or the authentication token has expired.

Example request

```
POST /rs/logout HTTP/1.1
Host: smc.example.com
X-SMCRS-Auth-Session: da81d6d2-3c02-4f18-8115-f4188d84e851
```

4.3 Create app group

Create an app group object.

URL

`https://<smc_server_address>/rs/androidappgroup`

`https://<smc_server_address>/rs/iosappgroup`

`https://<smc_server_address>/rs/macosappgroup`

`https://<smc_server_address>/rs/windowsdesktopappgroup`

`https://<smc_server_address>/rs/windowsphoneappgroup`

Method

POST

Request header

Key	Value
X-SMCRS-Auth-Session	The session authentication token from the login response.
Content-Type	`application/json`

Request body

JSON object with the following structure:

Key	Type	Description
name	String	External name of the app group. App groups for the same platform (Android, iOS, Windows Mobile) must have unique names. But it is for example possible to create an Android app group with the same name as an iOS app group.
appList	Array of app objects	See the following table.

App objects have the following structure:

Key	Type	Description
name	String	An arbitrary name that is used to identify the app.
identifier	String	For Android apps, this is the package name. For iOS apps, this is the bundle ID. For Windows Mobile apps, this is the GUID.
fileUrl	String (optional)	The URL of the app in Google Play, in the App Store, or in the Microsoft Store.

Response body

JSON object with the properties of the app group that was created:

Key	Type	Description
appGroupId	Number	ID of the app group.
name	String	External name of the app group.
editable	Boolean	If false, app group cannot be updated.

Key	Type	Description
updateDate	Integer	Update timestamp in epoch milliseconds.
insertDate	Integer	Insertion timestamp in epoch milliseconds.
updatedBy	String	Name of the user that updated the app group.
insertedBy	String	Name of the user that created the app group.
appList	Array of app objects	Same structure as for request.

HTTP response status

Status code	Description
204 OK	App group was successfully created.
401 Unauthorized	User is not authorized or the authentication token has expired.
403 Forbidden	User does not have sufficient rights.
409 Conflict	Another app group for the same platform (Android, iOS, Windows Mobile) with the specified name already exists.

Example request

```
POST /rs/androidappgroup HTTP/1.1
Host: smc.example.com
X-SMCRS-Auth-Session: da81d6d2-3c02-4f18-8115-f4188d84e851
Content-Type: application/json

{
  "name": "myNewAppGroup",
  "appList": [
    {
      "name": "Intercept X",
      "identifier": "com.sophos.smsec",
      "fileUrl":
"https://play.google.com/store/apps/details?id=com.sophos.smsec"
    }
  ]
}
```

Example response

```
{
  "appGroupId": 10042,
  "name": "myNewAppGroup",
  "editable": true,
  "updateDate": null,
  "insertDate": 1467116868245,
  "updatedBy": null,
  "insertedBy": "myAdminName",
  "appList": [
    {
      "name": "Intercept X",
      "identifier": "com.sophos.smsec",
      "fileUrl":
"https://play.google.com/store/apps/details?id=com.sophos.smsec"
    }
  ]
}
```

4.4 Get app groups

Get a list of all app group objects.

URL

`https://<smc_server_address>/rs/androidappgroup`

`https://<smc_server_address>/rs/iosappgroup`

`https://<smc_server_address>/rs/macosappgroup`

`https://<smc_server_address>/rs/windowsdesktopappgroup`

`https://<smc_server_address>/rs/windowsphoneappgroup`

Method

GET

Request header

Key	Value
X-SMCRS-Auth-Session	The session authentication token from the login response.

Response body

JSON object with the list of Android app groups:

Key	Type	Description
appGroupId	Number	ID of the app group.
name	String	External name of the app group.
editable	Boolean	If false, app group cannot be updated.

HTTP response status

Status code	Description
200 OK	Request was successfully processed.
401 Unauthorized	User is not authorized or the authentication token has expired.
403 Forbidden	User does not have sufficient rights.

Example request

```
GET /rs/androidappgroup HTTP/1.1
Host: smc.example.com
X-SMCRS-Auth-Session: da81d6d2-3c02-4f18-8115-f4188d84e851
```

Example response

```
[
  {
    "appGroupId": 10030,
    "name": "myFirstAppGroup",
    "editable": true
  },
  {
    "appGroupId": 10031,
    "name": "mySecondAppGroup",
    "editable": false
  },
  {
    "appGroupId": 10042,
    "name": "myNewAppGroup",
    "editable": true
  }
]
```

4.5 Get app group by ID

Get the properties of an existing app group object.

URL

`https://<smc_server_address>/rs/androidappgroup/:id`

`https://<smc_server_address>/rs/iosappgroup/:id`

`https://<smc_server_address>/rs/macosappgroup/:id`

`https://<smc_server_address>/rs/windowsdesktopappgroup/:id`

`https://<smc_server_address>/rs/windowsphoneappgroup/:id`

Method

GET

URL parameter

Parameter	Description
:id	The internal identifier of the app group. This is the `appGroupId` attribute as returned by, for example `GET /rs/androidappgroup`.

Request header

Key	Value
X-SMCRS-Auth-Session	The session authentication token from the login response.

Response body

JSON object with the properties of the specified app group:

Key	Type	Description
appGroupId	Number	ID of the app group.
name	String	External name of the app group.
editable	Boolean	If false, app group cannot be updated.
updateDate	Integer	Update timestamp in epoch milliseconds.
insertDate	Integer	Insertion timestamp in epoch milliseconds.

Key	Type	Description
updatedBy	String	Name of the user that updated the app group.
insertedBy	String	Name of the user that created the app group.
appList	Array of app objects	See the following table.

App objects have the following structure:

Key	Type	Description
name	String	An arbitrary name that is used to identify the app.
identifier	String	For Android apps, this is the package name. For iOS apps, this is the bundle ID. For Windows Mobile apps, this is the GUID.
fileUrl	String (optional)	If set, the URL of the app in Google Play, in the App Store, or in Microsoft Store.

HTTP response status

Status code	Description
200 OK	Request was successfully processed.
401 Unauthorized	User is not authorized or the authentication token has expired.
403 Forbidden	User does not have sufficient rights.
404 Not Found	App group with specified identifier does not exist.

Example request

```
GET /rs/androidappgroup/10042 HTTP/1.1
Host: smc.example.com
X-SMCRS-Auth-Session: da81d6d2-3c02-4f18-8115-f4188d84e851
```

Example response

```
{
  "appGroupId": 10042,
  "name": "myNewAppGroup",
  "editable": true,
  "updateDate": null,
  "insertDate": 1467116868245,
  "updatedBy": null,
  "insertedBy": "myAdminName",
  "appList": [
    {
      "name": "Intercept X",
      "identifier": "com.sophos.smsec",
      "fileUrl":
"https://play.google.com/store/apps/details?id=com.sophos.smsec"
    }
  ]
}
```

4.6 Update app group

Update an existing app group object.

URL

`https://<smc_server_address>/rs/androidappgroup/:id`

`https://<smc_server_address>/rs/iosappgroup/:id`

`https://<smc_server_address>/rs/macosappgroup/:id`

`https://<smc_server_address>/rs/windowsdesktopappgroup/:id`

`https://<smc_server_address>/rs/windowsphoneappgroup/:id`

Method

PUT

Request header

Key	Value
X-SMCRS-Auth-Session	The session authentication token from the login response.
Content-Type	`application/json`

Request body

JSON object with the updated data of the app group:

Key	Type	Description
name	String	External name of the app group.
appList	Array of app objects	See the following table.

App objects have the following structure:

Key	Type	Description
name	String	An arbitrary name that is used to identify the app.
identifier	String	For Android apps, this is the package name. For iOS apps, this is the bundle ID. For Windows Mobile apps, this is the GUID.
fileUrl	String (optional)	The URL of the app in Google Play, in the App Store, or in Microsoft Store.

Response body

empty

HTTP response status

Status code	Description
204 No Content	App group was successfully updated.
401 Unauthorized	User is not authorized or the authentication token has expired.
403 Forbidden	User does not have sufficient rights.
404 Not Found	App group with specified identifier does not exist.
409 Conflict	Another app group for the same platform (Android, iOS, Windows Mobile) with the specified name already exists.

Example request

```
PUT /rs/androidappgroup/10042 HTTP/1.1
Host: smc.example.com
X-SMCRS-Auth-Session: da81d6d2-3c02-4f18-8115-f4188d84e851
Content-Type: application/json

{
  "name": "myUpdatedAppGroup",
  "appList":[
    {
      "name": "Intercept X",
      "identifier": "com.sophos.smsec",
      "fileUrl":
"https://play.google.com/store/apps/details?id=com.sophos.smsec"
  },
  {
      "name": "Sophos Mobile Control",
      "identifier": "com.sophos.mobilecontrol.client.android",
      "fileUrl":
"https://play.google.com/store/apps/details?
id=com.sophos.mobilecontrol.client.android"
    }
  ]
}
```

5 Support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledge base at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

6 Legal notices