SOPHOS

Security made simple.

Sophos Mobile Control Network Access Control interface guide

Product version: 7

Document date: January 2017

Contents

1 About this guide

This guide explains how to connect a third-party Network Access Control system to the RESTful web service interface of Sophos Mobile Control.

2 About Sophos Mobile Control

Sophos Mobile Control is a management tool for mobile devices like smartphones and tablets, and also for Windows 10 desktop devices. It helps to keep corporate data safe by managing apps and security.

The Sophos Mobile Control system consists of a server and a client component.

The server is the core component of the Sophos Mobile Control product. It provides a web interface to administer Sophos Mobile Control and to manage the enrolled devices.

The client is an app to be installed onto the devices. It supports over-the-air setup and configuration through the web interface of the Sophos Mobile Control server.

With the Sophos Mobile Control Self Service Portal for your users, you can reduce IT effort by allowing users to enroll devices on their own and to carry out other tasks without contacting the helpdesk.

3 Sophos Mobile Control NAC support

To support Network Access Control (NAC), Sophos Mobile Control manages the network access status of mobile devices based on compliance rules. When a device violates a compliance rule that is assigned to it, the network access status of the device is set to *Deny*. If required, you can set the status of certain devices to a fixed value, independent of their compliance status.

Sophos Mobile Control only manages the network access status of devices. It does not actually restrict network communication. Instead, Sophos Mobile Control offers a web service interface that delivers the MAC addresses and corresponding network access status of the managed devices. Third-party NAC systems can retrieve this information to permit or deny access to network segments.

The connection of the NAC system to the web service interface has to be implemented by the third-party vendor.

4 Prerequisites

The following tasks must be completed in Sophos Mobile Control before you can use the NAC interface:

1. Install and configure Sophos Mobile Control.
   - For on-premise installations, see the *Sophos Mobile Control installation guide* and the *Sophos Mobile Control super administrator guide*.
   - For Sophos Mobile Control as a Service, this has already been performed by Sophos.
2. Enroll your mobile devices with Sophos Mobile Control. See the *Sophos Mobile Control administrator help*.
3. Configure NAC support (page 7).

Note: For information on the Sophos Mobile Control delivery models *on-premise* and *as a Service*, see the *Sophos Mobile Control administrator help*.

5 Configure NAC support

Network Access Control (NAC) support is configured through the Sophos Mobile Control web console.

Unless otherwise noted in the description below, you find detailed information about each step in the *Sophos Mobile Control administrator help*.

To configure network access:

1. For on-premise installations of Sophos Mobile Control, log in to the web console with a super administrator account and then enable NAC support.

   From the menu sidebar, go to **Setup** > **System setup** > **Network Access Control** and then select **Web service** from the list. See the *Sophos Mobile Control super administrator guide* for details.

   Sophos Mobile Control also includes product-specific NAC integration for Sophos UTM, Cisco ISE and Check Point. If you use one of these system, you can select the relevant option from the list. These options also enable the web service interface.

   Note: For Sophos Mobile Control as a Service, this step is not required. NAC support is always enabled.

2. Log in to the web console with a standard administrator account.
3. Configure compliance rules.

   From the menu sidebar, go to **Compliance rules** and then create or edit compliance rules. For each compliance criterion within a rule, you can select the **Deny network** action to block network access for devices that violate the criterion.

4. Assign the compliance rules to device groups.

   From the menu sidebar, go to **Device groups** and then create or edit a device group. Assign compliance rules to the device group. You can select different compliance rules for corporate and personal devices.

5. Assign devices to device groups.

   From the menu sidebar, go to **Devices** and then add or edit a device. Under **Device group**, select the device group that has the relevant compliance rule assigned.

6. In addition to network access based on compliance rules, you can set the network access status of certain devices to a fixed value.

   From the menu sidebar, go to **Devices**. Select the devices for which you want to set network access unconditionally. Then click **Actions** > **Set network access** and select either **Allow** or **Deny**.

When devices synch with Sophos Mobile Control, they are checked for compliance. You can also check the current compliance status of all devices by using **Check now** on the **Compliance rules** page. If a compliance criterion that contains the **Deny network** action is violated, the network access status of the device is set to *Deny*.

6 NAC web service interface

Sophos Mobile Control offers a RESTful web service to retrieve a list of the devices for a customer and their network access status.

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

Basically, you need to implement the following workflow in your third-party NAC system to retrieve the network access status of mobile devices from the web service:

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

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

2. Perform a `GET /rs/nac/mac` request.

   The service returns the MAC addresses of all devices for the customer, divided into devices with network access status *Allow* and *Deny*.

3. Optionally, perform a `GET /rs/nac/denieduser` request.

   The service returns a list of users that are assigned one or more devices with network access status *Denied*.

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

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

7 API description

7.1 Login (`rs/login`)

Login to the Sophos Mobile Control server.

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

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	Customer name
user	Administrator login name
password	Administrator password

Response body

JSON object with the following structure:

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

The administrator must have the `DEVICE_BROWSE` right to be able to retrieve network access status.

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.yourcompany.com
Content-Type: application/x-www-form-urlencoded
customer=your_customer&user=your_admin_name&password=your_password
```

Example response

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

7.2 Logout (`rs/logout`)

Logout from the Sophos Mobile Control 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.yourcompany.com
X-SMCRS-Auth-Session: da81d6d2-3c02-4f18-8115-f4188d84e851
```

7.3 Devices (`rs/nac/mac`)

This resource returns the MAC addresses of all devices for the customer, divided into devices with network access status *Allowed* and *Denied*.

URL

`https://<smc_server_address>/rs/nac/mac`

Method

GET

Request header

Key	Value
x-smcrs-auth-session	Session authentication token from the login response

Request body

empty

Response body

JSON object with the following structure:

Key	Type	Description
allowed	Array of device objects	List of devices with network access status *Allow*
denied	Array of device objects	List of devices with network access status *Deny*

Device objects have the following structure:

Key	Type	Description
deviceId	Integer	Internal device identifier
mac	String	MAC address of the device

Key	Type	Description
deniedReason	String	Possible values: `null`: Network access is allowed. `denied by compliance violation`: Network access is denied because of a compliance violation. `denied by admin`: Network access is unconditionally denied in device settings.

HTTP response status

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

Example request

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

Example response

```
{
   "allowed": [
      {
         "deviceId": 12060,
         "mac": "021111111111",
         "deniedReason": null
      },
      {
         "deviceId": 12066,
         "mac": "022222222222",
         "deniedReason": null
      }
   ],
   "denied": [
      {
```

```
            "deviceId": 12069,
            "mac": "023333333333",
            "deniedReason": "denied by admin"
        },
        {
            "deviceId": 22079,
            "mac": "024444444444",
            "deniedReason": "denied by compliance violation"
        }
    ]
}
```

7.4 Users with denied devices (`rs/nac/denieduser`)

This resource returns a list of device users that are assigned one or more devices with network access status *Deny*.

Only users from an external LDAP directory are listed.

URL

`https://<smc_server_address>/rs/nac/denieduser`

Method

GET

Request header

Key	Value
x-smcrs-auth-session	Session authentication token from the login response

Request body

empty

Response body

JSON array containing objects with the following structure:

Key	Type	Description
userIdentifier	String	User name
deniedDevices	Array of device objects	List of devices with network access status *Deny*

Device objects have the following structure:

Key	Type	Description
deviceId	Integer	Internal device identifier

Key	Type	Description
deniedReason	String	Possible values: `denied by compliance violation`: Network access is denied because of a compliance violation. `denied by admin`: Network access is unconditionally denied in device settings.

Note: For customers with internal user management, the service responds with an empty JSON array `[]`.

HTTP response status

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

Example request

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

Example response

```
[
   {
      "userIdentifier": "a user name",
      "deniedDevices": [
         {
            "deviceId": 12069,
            "mac": "023333333333",
            "deniedReason": "denied by admin"
         },
         {
            "deviceId": 22079,
            "mac": "024444444444",
            "deniedReason": "denied by compliance violation"
         }
```

```
      ]
   }
]
```

8 Migrate to the web service interface

In addition to the RESTful web service interface that is described in this document, Sophos Mobile Control offers a second NAC interface that uses a custom HTTP-based protocol. It is available at `https://<smc_server_address>/servlets/nac/`.

That last-mentioned NAC interface is deprecated and will be removed from Sophos Mobile Control with a future release.

If you have implemented a connection of a third-party NAC system to the deprecated NAC interface, perform the following steps to migrate to the web service interface:

1. Using a REST client implementation of your choice, set up a workflow that connects to the web service interface and retrieves the lists of MAC addresses for devices with network access status *Allow* and *Deny*. See NAC web service interface (page 8).
2. Provide these lists to your third-party NAC system instead of the lists that you retrieved from the deprecated NAC interface.
3. Using the Sophos Mobile Control web console, change the Network Access Control mode from **Custom** to **Web service**. For details, see the *Sophos Mobile Control super administrator guide*.

   You do not need to upload a specific certificate for communication with the web service.

Note: For details about the deprecated NAC interface, see the *Network Access Control interface guide* for Sophos Mobile Control product version 6.

9 Technical 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 knowledgebase 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.

10 Legal notices