Change of Authorization REST APIs

This chapter provides examples and describes how to use the following individual Change of Authorization (CoA) REST API calls that are supported in this release of Cisco Identity Services Engine.

Introduction

The CoA API calls provide the means for sending session authentication and session disconnect commands to a specified Cisco Monitoring ISE node in your Cisco ISE deployment.

CoA Session Management API Calls

The CoA session management API calls allow you to send reauthentication and disconnect commands to a specified session on a target Cisco Monitoring ISE node in your Cisco ISE deployment:

- Session reauthentication (Reauth)
- Session disconnection (Disconnect)

Session Reauthentication API Call

The Session Reauthentication API Call constitutes the following types:

- REAUTH_TYPE_DEFAULT = 0
- REAUTH_TYPE_LAST = 1
- REAUTH_TYPE_RERUN = 2

Reauth API Output Schema

This sample schema file is the output of the Reauth API call after sending it to a specified session on the target Cisco Monitoring ISE node:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="remoteCoA" type="coAResult"/>
<xs:complexType name="coAResult">
    <xs:sequence>
      <xs:element name="results" type="xs:boolean" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="requestType" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

Invoking the Reauth API Call

Step 1 Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*).

Step 2 Enter the username and case-sensitive password, that was specified and configured during the initial Cisco ISE setup.

Step 3 Click **Login** or press **Enter**.

For example, when you initially log into a Cisco Monitoring ISE node with the hostname of acme123, this would display the following URL Address field for this node:

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

Step 4 Enter the Reauth API call in the URL Address field of the target node by replacing the "/admin/" component with the API call component (/admin/API/mnt/CoA/<specific-api-call>/<macaddress>/<reauthtype>:

```
https://acme123/admin/API/mnt/CoA/Reauth/server12/00:26:82:7B:D2:51/1
```

Note You must carefully enter each API call in the URL Address field of a target node because these calls are case-sensitive. The use of "mnt" in the API call convention represents a Cisco Monitoring ISE node.

Step 5 Press **Enter** to issue the API call.

Related Topics

- Verifying a Monitoring Node, page 1-2

Sample Data Returned from the Reauth API Call

The following example illustrates the data returned when you invoke a Reauth API call on a target Cisco Monitoring ISE node. Two possible results can be returned from invoking this command:

- True indicates that the command was successfully executed.
- False means that the command was not executed (due to a variety of conditions).

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<remoteCoA requestType="reauth">
<results>true</results>
</remoteCoA>
```

Session Disconnect API Call

The Session Disconnect API call constitutes the following disconnect port option types:

- DYNAMIC_AUTHZ_PORT_DEFAULT = 0
- DYNAMIC_AUTHZ_PORT_BOUNCE = 1
- DYNAMIC_AUTHZ_PORT_SHUTDOWN = 2

Disconnect API Output Schema

This sample schema file is the output of the Disconnect API call after sending it to a specified session on the target Cisco Monitoring ISE node:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <xs:element name="remoteCoA" type="coAResult"/>

  <xs:complexType name="coAResult">
    <xs:sequence>
      <xs:element name="results" type="xs:boolean" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="requestType" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

Invoking the Disconnect API Call

Step 1 Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*).

Step 2 Enter the username and case-sensitive password, that was specified and configured during the initial Cisco ISE setup.

Step 3 Click **Login** or press **Enter**.

For example, when you initially log into a Cisco Monitoring ISE node with the hostname of acme123, this would display the following URL Address field for this node:

```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

Step 4 Enter the Disconnect API call in the URL Address field of the target node by replacing the "/admin/" component with the API call component (/admin/API/mnt/CoA/<Disconnect>/<serverhostname>/<macaddress>/<portoptiontype>/<nasipaddress>/<destinationipaddress>:

```
https://acme123/admin/API/mnt/CoA/Disconnect/server12/00:26:82:7B:D2:51/2/10.10.
10.10/192.168.1.1
```

Note You must carefully enter each API call in the URL Address field of a target node because these calls are case-sensitive. The use of "mnt" in the API call convention represents a Cisco Monitoring ISE node.

Step 5 Press **Enter** to issue the API call.

Related Topics

- Verifying a Monitoring Node, page 1-2

Sample Data Returned from the Disconnect API Call

The following example illustrates the data returned when you invoke a Disconnect API call on a target Cisco Monitoring ISE node. Two possible results can be returned by invoking this command:

- True indicates that the command was successfully executed.
- False means that the command was not executed (due to a variety of conditions).

```
This XML file does not appear to have any style information associated with it. The
document tree is shown below.

-
<remoteCoA requestType="reauth">
<results>true</results>
</remoteCoA>
```