



Using API Calls for Session Management

Cisco ISE session-management API calls use a Monitoring node to retrieve session-related information. The following sections describe each type of call as well as provide output schema file examples, procedures for issuing each call, a sample of the data returned, and how to remove stale sessions:

- [Session Counter API Calls, page 2-1](#)
- [Session List API Calls, page 2-5](#)
- [Session Attribute API Calls, page 2-10](#)
- [Removing Stale Sessions, page 2-25](#)

Session Counter API Calls

The following API calls let you quickly gather a current count of session-related information on a targeted Monitoring node in your Cisco ISE deployment:

- **ActiveCount**—counts active sessions.
- **PostureCount**—counts postured sessions.
- **ProfilerCount**—counts profiled sessions.

Using ActiveCount API Calls

You use an ActiveCount API call to retrieve a count of active sessions. This section contains the following sections:

- [ActiveCount API Call Schema File, page 2-1](#)
- [Invoking the ActiveCount API Call, page 2-2](#)
- [ActiveCount API Call Data, page 2-2](#)

ActiveCount API Call Schema File

```
<?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="sessionCount" type="activeCount" />
  <xs:complexType name="activeCount">
    <xs:sequence>
      <xs:element name="count" type="xs:int" />
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

```

    </xs:sequence>
  </xs:complexType>
</xs:schema>

```

Invoking the ActiveCount API Call



Note

Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1

Log in to the target Monitoring node.

For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

Step 2

Enter the ActiveCount API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>):

```
https://acme123/ise/mnt/Session/ActiveCount
```



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 the target Monitoring node.

Step 3

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

ActiveCount API Call Data

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

```

-
<sessionCount>
<count>5</count>
</sessionCount>

```

Using PostureCount API Call

You use a PostureCount API call to retrieve a count of active Posture sessions. This section contains the following sections:

- [PostureCount API Call Schema File, page 2-2](#)
- [Invoking a PostureCount API Call, page 2-3](#)
- [PostureCount API Call Data, page 2-3](#)

PostureCount API Call Schema File

```

<?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="sessionCount" type="postureCount"/>

<xs:complexType name="postureCount">
  <xs:sequence>
    <xs:element name="count" type="xs:int"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>

```

Invoking a PostureCount API Call



Note Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1 Log in to the target Monitoring node.
For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

Step 2 Enter the PostureCount API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>):

```
https://acme123/ise/mnt/Session/PostureCount
```



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 the target Monitoring node.

Step 3 Press **Enter** to issue the API call.

PostureCount API Call Data

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

```

-
<sessionCount>
<count>3</count>
</sessionCount>

```

Using ProfilerCount API Call

You use the ProfilerCount API call to retrieve a count of active Profiler sessions. This section contains the following sections:

- [ProfilerCount API Call Schema File, page 2-4](#)
- [Invoking a ProfilerCount API Call, page 2-4](#)
- [ProfilerCount API Call Data, page 2-4](#)

ProfilerCount API Call Schema File

```
<?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="sessionCount" type="profilerCount"/>

  <xs:complexType name="profilerCount">
    <xs:sequence>
      <xs:element name="count" type="xs:int"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

Invoking a ProfilerCount API Call



Note

Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1

Log in to the target Monitoring node.

For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

Step 2

Enter the ProfilerCount API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>):

```
https://acme123/ise/mnt/Session/ProfilerCount
```



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 the target Monitoring node.

Step 3

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

ProfilerCount API Call Data

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

```
-
<sessionCount>
<count>1</count>
</sessionCount>
```

Session List API Calls

The following session list API calls let you quickly gather session-related information such as the MAC address, the network access device (NAD) IP address, username, and session ID associated with a current active session on a target Monitoring node in a Cisco ISE deployment:

- `ActiveList`—lists active sessions
- `AuthList`—lists authenticated sessions

Using ActiveList API Calls

You use an `ActiveList` API call to list all active sessions. This section contains the following sections:

- [ActiveList API Call Schema File, page 2-5](#)
- [Invoking an ActiveList API Call, page 2-6](#)
- [ActiveList API Call Data, page 2-6](#)



Note

In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is 100,000.

ActiveList API Call Schema File

```
<?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="activeSessionList" type="simpleActiveSessionList"/>

<xs:complexType name="simpleActiveSessionList">
  <xs:sequence>
    <xs:element name="activeSession" type="simpleActiveSession" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="noOfActiveSession" type="xs:int" use="required"/>
</xs:complexType>

<xs:complexType name="simpleActiveSession">
  <xs:sequence>
    <xs:element name="user_name" type="xs:string" minOccurs="0"/>
    <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
    <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
    <xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
    <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
    <xs:element name="server" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>
```

Invoking an ActiveList API Call


Note

Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1

Log in to the target Monitoring node.

For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

Step 2

Enter the ActiveList API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>):

```
https://acme123/ise/mnt/Session/ActiveList
```


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 the target Monitoring node.

Step 3

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

ActiveList API Call Data

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

```
-
<activeSessionList noOfActiveSession="5">
-
<activeSession>
<calling_station_id>00:0C:29:FA:EF:0A</calling_station_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<calling_station_id>70:5A:B6:68:F7:CC</calling_station_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>tom_wolfe</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000032</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>graham_hancock</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>0000002C</acct_session_id>
<audit_session_id>0ACB6BA10000002A165FD0C8</audit_session_id>
```

```

<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>ipepvpnuser</user_name>
<calling_station_id>172.23.130.89</calling_station_id>
<nas_ip_address>10.203.107.45</nas_ip_address>
<acct_session_id>A2000070</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>

```

Using AuthList API Calls

You use an AuthList API call to retrieve a list of all active authenticated sessions. This section contains the following sections:

- [AuthList API Call Schema File, page 2-7](#)
- [Invoking an AuthList API Call, page 2-8](#)
- [AuthList API Call Data, page 2-8](#)



Note

In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is 100,000.

AuthList API Call Schema File

```

<?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="activeSessionList" type="simpleActiveSessionList"/>

  <xs:complexType name="simpleActiveSessionList">
    <xs:sequence>
      <xs:element name="activeSession" type="simpleActiveSession" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="noOfActiveSession" type="xs:int" use="required"/>
  </xs:complexType>

  <xs:complexType name="simpleActiveSession">
    <xs:sequence>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="server" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>

```

Invoking an AuthList API Call


Note

Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1

Log in to the target Monitoring node.

For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

Step 2

Enter the AuthList API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>):


Note

The first of the following two examples uses a defined start time and null parameter, which displays a list of the currently active sessions that were authenticated after the specified start time. The second example uses the null/null parameter that displays a list of all currently active authenticated sessions. See [AuthList API Call Data, page 2-8](#), which displays samples of the four parameter setting types for this API call.

```
https://acme123/ise/mnt/Session/AuthList/2010-12-14 15:33:15/null
```

```
https://acme123/ise/mnt/Session/AuthList/null/null
```


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 the targeted Monitoring node.

Step 3

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

AuthList API Call Data

Using the null/null Option

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

```
-
<activeSessionList noOfActiveSession="3">
-
  <activeSession>
    <user_name>ipepwluser</user_name>
    <calling_station_id>00:26:82:7B:D2:51</calling_station_id>
    <nas_ip_address>10.203.107.10</nas_ip_address>
    <audit_session_id>0acb6b0c000000174D07F487</audit_session_id>
    <server>HAREESH-R6-1-PDP2</server>
  </activeSession>
-
  <activeSession>
    <user_name>tom_wolfe</user_name>
    <calling_station_id>00:50:56:8E:28:BD</calling_station_id>
```



```

<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>graham_hancock</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>

```

Using the endtime/null Option

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

```

-
<activeSessionList noOfActiveSession="3">
-
<activeSession>
<user_name>ipepwluser</user_name>
<calling_station_id>00:26:82:7B:D2:51</calling_station_id>
<nas_ip_address>10.203.107.10</nas_ip_address>
<audit_session_id>0acb6b0c0000001F4D08085A</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>hunter_thompson</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>bob_ludlum</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>

```

Using the null/starttime Option

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

```

-
<activeSessionList noOfActiveSession="3">
-
<activeSession>
<user_name>ipepwluser</user_name>
<calling_station_id>00:26:82:7B:D2:51</calling_station_id>
<nas_ip_address>10.203.107.10</nas_ip_address>
<audit_session_id>0acb6b0c0000001F4D08085A</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>

```

```

<user_name>bob_ludlum</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>tom_wolfe</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>

```

Using the starttime/endtime Option

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

```

-
<activeSessionList noOfActiveSession="3">
-
<activeSession>
<user_name>ipepwluser</user_name>
<calling_station_id>00:26:82:7B:D2:51</calling_station_id>
<nas_ip_address>10.203.107.10</nas_ip_address>
<audit_session_id>0acb6b0c0000001F4D08085A</audit_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>graham_hancock</user_name>
<calling_station_id>00:50:56:8E:28:BD</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000035</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
-
<activeSession>
<user_name>hunter_thompson</user_name>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_ip_address>10.203.107.161</nas_ip_address>
<acct_session_id>00000033</acct_session_id>
<server>HAREESH-R6-1-PDP2</server>
</activeSession>
</activeSessionList>

```

Session Attribute API Calls

The following session attribute API calls let you quickly search the latest session for key information, such as the following:

- MAC address session search using a MACAddress API call
- User name session search using a UserName API call
- NAS IP address session search using an IPAddress API call
- Audit Session ID session search

Using MACAddress API Calls

You use a MACAddress API call to retrieve a specified MAC address from an active session on a targeted monitoring node. This section contains the following sections:

- [MACAddress API Call Schema File, page 2-11](#)
- [Invoking a MACAddress API Call, page 2-13](#)
- [MACAddress API Call Data, page 2-13](#)

MACAddress API Call Schema File

```
<?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="sessionParameters" type="restsdStatus"/>

  <xs:complexType name="restsdStatus">
    <xs:sequence>
      <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
      <xs:element name="authn_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
      <xs:element name="access_service" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
      <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_id" type="xs:long" minOccurs="0"/>
      <xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="message_code" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="response" type="xs:string" minOccurs="0"/>
      <xs:element name="service_type" type="xs:string" minOccurs="0"/>
      <xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="use_case" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
      <xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_username" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_role" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
    

```

```

<xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
<xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
<xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="response_time" type="xs:long" minOccurs="0"/>
<xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="acct_id" type="xs:long" minOccurs="0"/>
<xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
<xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
<xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_class" type="xs:string" minOccurs="0"/>
<xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
<xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
<xs:element name="termination_action" type="xs:string" minOccurs="0"/>
<xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
<xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
<xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
<xs:element name="security_group" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
<xs:element name="started" type="xs:anyType" minOccurs="0"/>
<xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
<xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
<xs:element name="type" type="xs:long" minOccurs="0"/>
<xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="vlan" type="xs:string" minOccurs="0"/>
<xs:element name="dacl" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
<xs:element name="interface_name" type="xs:string" minOccurs="0"/>
<xs:element name="reason" type="xs:string" minOccurs="0"/>
<xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

Invoking a MACAddress API Call



Note Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1 Log in to the target Monitoring node.
For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

Step 2 Enter the MACAddress API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>/<macaddress>):

```
https://acme123/ise/mnt/Session/MACAddress/0A:0B:0C:0D:0E:0F
```



Note Make sure that you specify the MAC address using the XX:XX:XX:XX:XX:XX format.



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 the target Monitoring node.

Step 3 Press **Enter** to issue the API call.



Note This API call returns only the session data that is created during the last 5 days.

MACAddress API Call Data

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

```
-
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>hunter_thompson</user_name>
<nas_ip_address>10.203.107.161</nas_ip_address>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_port>50115</nas_port>
<identity_group>Profiled</identity_group>
<network_device_name>Core-Switch</network_device_name>
<acs_server>HAREESH-R6-1-PDP2</acs_server>
<authn_protocol>Lookup</authn_protocol>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2010-12-15T02:11:12.359Z</auth_acs_timestamp>
```

```

<authentication_method>mab</authentication_method>
-
<execution_steps>
11001,11017,11027,15008,15048,15004,15041,15004,15013,24209,24211,22037,15036,15048,15048,
15004,15016,11022,11002
</execution_steps>
<audit_session_id>0ACB6BA1000000351BBFBF8B</audit_session_id>
<nas_port_id>GigabitEthernet1/0/15</nas_port_id>
<nac_policy_compliance>Pending</nac_policy_compliance>
<auth_id>1291240762077361</auth_id>
<auth_acsview_timestamp>2010-12-15T02:11:12.360Z</auth_acsview_timestamp>
<message_code>5200</message_code>
<acs_session_id>HAREESH-R6-1-PDP2/81148292/681</acs_session_id>
<service_selection_policy>MAB</service_selection_policy>
<identity_store>Internal Hosts</identity_store>
-
<response>
{UserName=00-14-BF-5A-0C-03; User-Name=00-14-BF-5A-0C-03;
State=ReauthSession:0ACB6BA1000000351BBFBF8B;
Class=CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681;
Termination-Action=RADIUS-Request; cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT;
cisco-av-pair=url-redirect=https://HAREESH-R6-1-PDP2.cisco.com:8443/guestportal/gateway?se
ssionId=0ACB6BA1000000351BBFBF8B&action=cwa;
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL-DENY-4ced8390; }
</response>
<service_type>Call Check</service_type>
<use_case>Host Lookup</use_case>
<cisco_av_pair>audit-session-id=0ACB6BA1000000351BBFBF8B</cisco_av_pair>
<acs_username>00:14:BF:5A:0C:03</acs_username>
<radius_username>00:14:BF:5A:0C:03</radius_username>
<selected_identity_store>Internal Hosts</selected_identity_store>
<authentication_identity_store>Internal Hosts</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Ethernet</nas_port_type>
<selected_azn_profiles>CWA</selected_azn_profiles>
-
<other_attributes>
ConfigVersionId=44, DestinationIpAddress=10.203.107.162, DestinationPort=1812, Protocol=Radiu
s, Framed-MTU=1500, EAP-Key-Name=, CPMSessionID=0ACB6BA1000000351BBFBF8B, CPMSessionID=0ACB6BA
1000000351BBFBF8B, EndPointMACAddress=00-14-BF-5A-0C-03, HostIdentityGroup=Endpoint Identity
Groups:Profiled, Device Type=Device Type#All Device Types, Location=Location#All
Locations, Model Name=Unknown, Software Version=Unknown, Device IP
Address=10.203.107.161, Called-Station-ID=04:FE:7F:7F:C0:8F
</other_attributes>
<response_time>77</response_time>
<acct_id>1291240762077386</acct_id>
<acct_acs_timestamp>2010-12-15T02:12:30.779Z</acct_acs_timestamp>
<acct_acsview_timestamp>2010-12-15T02:12:30.780Z</acct_acsview_timestamp>
<acct_session_id>00000038</acct_session_id>
<acct_status_type>Interim-Update</acct_status_type>
<acct_session_time>78</acct_session_time>
<acct_input_octets>13742</acct_input_octets>
<acct_output_octets>6277</acct_output_octets>
<acct_input_packets>108</acct_input_packets>
<acct_output_packets>66</acct_output_packets>
-
<acct_class>
CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681
</acct_class>
<acct_delay_time>0</acct_delay_time>
<started xsi:type="xs:boolean">false</started>
<stopped xsi:type="xs:boolean">false</stopped>
</sessionParameters>

```

Using UserName API Calls

You use a UserName API call to retrieve a specified username from an active session. This section contains the following sections:

- [UserName API Call Schema File, page 2-15](#)
- [Invoking a UserName API Call, page 2-17](#)
- [UserName API Call Data, page 2-17](#)

UserName API Call Schema File

```
<?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="sessionParameters" type="restsdStatus"/>

  <xs:complexType name="restsdStatus">
    <xs:sequence>
      <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
      <xs:element name="authen_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
      <xs:element name="access_service" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
      <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_id" type="xs:long" minOccurs="0"/>
      <xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="message_code" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="response" type="xs:string" minOccurs="0"/>
      <xs:element name="service_type" type="xs:string" minOccurs="0"/>
      <xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="use_case" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
      <xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_username" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_role" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```

```

<xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
<xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
<xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
<xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
<xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="response_time" type="xs:long" minOccurs="0"/>
<xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="acct_id" type="xs:long" minOccurs="0"/>
<xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
<xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
<xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_class" type="xs:string" minOccurs="0"/>
<xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
<xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
<xs:element name="termination_action" type="xs:string" minOccurs="0"/>
<xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
<xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
<xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
<xs:element name="security_group" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
<xs:element name="started" type="xs:anyType" minOccurs="0"/>
<xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
<xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
<xs:element name="type" type="xs:long" minOccurs="0"/>
<xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="vlan" type="xs:string" minOccurs="0"/>
<xs:element name="dacl" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
<xs:element name="interface_name" type="xs:string" minOccurs="0"/>
<xs:element name="reason" type="xs:string" minOccurs="0"/>
<xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:schema>

```


Invoking a UserName API Call



Note Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1 Log in to the target Monitoring node.
For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

Step 2 Enter the UserName API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>/<username>):

```
https://acme123/ise/mnt/Session/UserName/graham_hancock
```



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 the target Monitoring node.

Step 3 Press **Enter** to issue the API call.

UserName API Call Data

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

```
-
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>graham_hancock</user_name>
<nas_ip_address>10.203.107.161</nas_ip_address>
<calling_station_id>00:14:BF:5A:0C:03</calling_station_id>
<nas_port>50115</nas_port>
<identity_group>Profiled</identity_group>
<network_device_name>Core-Switch</network_device_name>
<acs_server>HAREESH-R6-1-PDP2</acs_server>
<authn_protocol>Lookup</authn_protocol>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2010-12-15T02:11:12.359Z</auth_acs_timestamp>
<authentication_method>mab</authentication_method>
-
<execution_steps>
11001,11017,11027,15008,15048,15004,15041,15004,15013,24209,24211,22037,15036,15048,15048,
15004,15016,11022,11002
</execution_steps>
<audit_session_id>0ACB6BA1000000351BBFBF8B</audit_session_id>
<nas_port_id>GigabitEthernet1/0/15</nas_port_id>
<nac_policy_compliance>Pending</nac_policy_compliance>
```

```

<auth_id>1291240762077361</auth_id>
<auth_acsview_timestamp>2010-12-15T02:11:12.360Z</auth_acsview_timestamp>
<message_code>5200</message_code>
<acs_session_id>HAREESH-R6-1-PDP2/81148292/681</acs_session_id>
<service_selection_policy>MAB</service_selection_policy>
<identity_store>Internal Hosts</identity_store>
-
<response>
{UserName=graham_hancock; User-Name=graham_hancock;
State=ReauthSession:0ACB6BA1000000351BBFBF8B;
Class=CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681;
Termination-Action=RADIUS-Request; cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT;
cisco-av-pair=url-redirect=https://HAREESH-R6-1-PDP2.cisco.com:8443/guestportal/gateway?se
ssionId=0ACB6BA1000000351BBFBF8B&action=cwa;
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL-DENY-4ced8390; }
</response>
<service_type>Call Check</service_type>
<use_case>Host Lookup</use_case>
<cisco_av_pair>audit-session-id=0ACB6BA1000000351BBFBF8B</cisco_av_pair>
<acs_username>graham_hancock</acs_username>
<radius_username>00:14:BF:5A:0C:03</radius_username>
<selected_identity_store>Internal Hosts</selected_identity_store>
<authentication_identity_store>Internal Hosts</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Ethernet</nas_port_type>
<selected_azn_profiles>CWA</selected_azn_profiles>
-
<other_attributes>
ConfigVersionId=44, DestinationIpAddress=10.203.107.162, DestinationPort=1812, Protocol=Radiu
s, Framed-MTU=1500, EAP-Key-Name=, CPMSessionID=0ACB6BA1000000351BBFBF8B, CPMSessionID=0ACB6BA
1000000351BBFBF8B, EndPointMACAddress=00-14-BF-5A-0C-03, HostIdentityGroup=Endpoint Identity
Groups:Profiled, Device Type=Device Type#All Device Types, Location=Location#All
Locations, Model Name=Unknown, Software Version=Unknown, Device IP
Address=10.203.107.161, Called-Station-ID=04:FE:7F:7F:C0:8F
</other_attributes>
<response_time>77</response_time>
<acct_id>1291240762077386</acct_id>
<acct_acs_timestamp>2010-12-15T02:12:30.779Z</acct_acs_timestamp>
<acct_acsview_timestamp>2010-12-15T02:12:30.780Z</acct_acsview_timestamp>
<acct_session_id>00000038</acct_session_id>
<acct_status_type>Interim-Update</acct_status_type>
<acct_session_time>78</acct_session_time>
<acct_input_octets>13742</acct_input_octets>
<acct_output_octets>6277</acct_output_octets>
<acct_input_packets>108</acct_input_packets>
<acct_output_packets>66</acct_output_packets>
-
<acct_class>
CACS:0ACB6BA1000000351BBFBF8B:HAREESH-R6-1-PDP2/81148292/681
</acct_class>
<acct_delay_time>0</acct_delay_time>
<started xsi:type="xs:boolean">>false</started>
<stopped xsi:type="xs:boolean">>false</stopped>
</sessionParameters>

```

Using IP Address API Calls

You use an IP Address API call to retrieve data for a specified network access server (NAS) IP address from a current session. This section contains the following sections:

- [IP Address API Call Schema File, page 2-19](#)

- [Invoking an IPAddress API Call, page 2-20](#)
- [IPAddress API Call Data, page 2-21](#)

IPAddress API Call Schema File

```
<?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="sessionParameters" type="restsdStatus"/>

  <xs:complexType name="restsdStatus">
    <xs:sequence>
      <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
      <xs:element name="authn_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
      <xs:element name="access_service" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
      <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_id" type="xs:long" minOccurs="0"/>
      <xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="message_code" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="response" type="xs:string" minOccurs="0"/>
      <xs:element name="service_type" type="xs:string" minOccurs="0"/>
      <xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="use_case" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
      <xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_username" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_role" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
    

```

```

<xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
<xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
<xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="response_time" type="xs:long" minOccurs="0"/>
<xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="acct_id" type="xs:long" minOccurs="0"/>
<xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
<xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
<xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_class" type="xs:string" minOccurs="0"/>
<xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
<xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
<xs:element name="termination_action" type="xs:string" minOccurs="0"/>
<xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
<xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
<xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
<xs:element name="security_group" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
<xs:element name="started" type="xs:anyType" minOccurs="0"/>
<xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
<xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
<xs:element name="type" type="xs:long" minOccurs="0"/>
<xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="vlan" type="xs:string" minOccurs="0"/>
<xs:element name="dacl" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
<xs:element name="interface_name" type="xs:string" minOccurs="0"/>
<xs:element name="reason" type="xs:string" minOccurs="0"/>
<xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

Invoking an IPAddress API Call



Note

Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

- Step 1** Log in to the target Monitoring node.
For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:

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

- Step 2** Enter the IPAddress API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/ise/mnt/Session/<specific-api-call>/<nasipaddress>):

```
https://acme123/ise/mnt/Session/IPAddress/10.10.10.10
```



Note Make sure that you specify the NAS IP address using the xxx.xxx.xxx.xxx format.



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 the target Monitoring node.

- Step 3** Press **Enter** to issue the API call.



Note This API call returns only the session data that is created during the last 5 days.

IPAddress API Call Data

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

```
-
<sessionParameters>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">>false</failed>
<user_name>ipepvpnuser</user_name>
<nas_ip_address>10.10.10.10</nas_ip_address>
<calling_station_id>172.23.130.90</calling_station_id>
<nas_port>1015</nas_port>
<identity_group>iPEP-VPN-Group</identity_group>
<network_device_name>iPEP-HA-Routed</network_device_name>
<acs_server>HAREESH-R6-1-PDP2</acs_server>
<authn_protocol>PAP_ASCII</authn_protocol>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2010-12-15T19:57:29.885Z</auth_acs_timestamp>
<authentication_method>PAP_ASCII</authentication_method>
-
<execution_steps>
11001,11017,15008,15048,15048,15004,15041,15004,15013,24210,24212,22037,15036,15048,15048,
15004,15016,11002
</execution_steps>
<audit_session_id>0acb6be400000044D091DA9</audit_session_id>
<nac_policy_compliance>NotApplicable</nac_policy_compliance>
<auth_id>1291240762083580</auth_id>
```

```

<auth_acsview_timestamp>2010-12-15T19:57:29.887Z</auth_acsview_timestamp>
<message_code>5200</message_code>
<acs_session_id>HAREESH-R6-1-PDP2/81148292/693</acs_session_id>
<service_selection_policy>iPEP-VPN</service_selection_policy>
<identity_store>Internal Users</identity_store>
-
<response>
{User-Name=ipepvpuser; State=ReauthSession:0acb6be400000044D091DA9;
Class=CACS:0acb6be400000044D091DA9:HAREESH-R6-1-PDP2/81148292/693;
Termination-Action=RADIUS-Request; }
</response>
<service_type>Framed</service_type>
-
<cisco_av_pair>
audit-session-id=0acb6be400000044D091DA9,ipep-proxy=true
</cisco_av_pair>
<acs_username>ipepvpuser</acs_username>
<radius_username>ipepvpuser</radius_username>
<selected_identity_store>Internal Users</selected_identity_store>
<authentication_identity_store>Internal Users</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Virtual</nas_port_type>
<selected_azn_profiles>iPEP-Unknown-Auth-Profile</selected_azn_profiles>
<tunnel_details>Tunnel-Client-Endpoint=(tag=0) 172.23.130.90</tunnel_details>
-
<other_attributes>
ConfigVersionId=44, DestinationIpAddress=10.203.107.162, DestinationPort=1812, Protocol=Radiu
s, Framed-Protocol=PPP, Proxy-State=Cisco Secure
ACS9e733142-070a-11e0-c000-000000000000-2906094480-3222, CPMSessionID=0acb6be400000044D091
DA9, CPMSessionID=0acb6be400000044D091DA9, Device Type=Device Type#All Device
Types, Location=Location#All Locations, Model Name=Unknown, Software Version=Unknown, Device
IP Address=10.203.107.228, Called-Station-ID=172.23.130.94
</other_attributes>
<response_time>20</response_time>
<acct_id>1291240762083582</acct_id>
<acct_acs_timestamp>2010-12-15T19:57:30.281Z</acct_acs_timestamp>
<acct_acsview_timestamp>2010-12-15T19:57:30.283Z</acct_acsview_timestamp>
<acct_session_id>F1800007</acct_session_id>
<acct_status_type>Start</acct_status_type>
-
<acct_class>
CACS:0acb6be400000044D091DA9:HAREESH-R6-1-PDP2/81148292/693
</acct_class>
<acct_delay_time>0</acct_delay_time>
<framed_protocol>PPP</framed_protocol>
<started xsi:type="xs:boolean">true</started>
<stopped xsi:type="xs:boolean">false</stopped>
</sessionParameters>

```

Using Audit Session ID API Calls

You can use the Audit Session ID API call to retrieve a specified audit session from a current, active session. This API call lists a variety of session-related information drawn from node database tables.

This section contains the following sections:

- [Audit Session ID API Call Schema File, page 2-23](#)
- [Invoking an Audit Session ID API Call, page 2-24](#)
- [Audit Session ID API Call Data, page 2-25](#)

Audit Session ID API Call Schema File

```

<?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="sessionParameters" type="restsdStatus"/>

  <xs:complexType name="restsdStatus">
    <xs:sequence>
      <xs:element name="passed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="failed" type="xs:anyType" minOccurs="0"/>
      <xs:element name="user_name" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="failure_reason" type="xs:string" minOccurs="0"/>
      <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_group" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_name" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_server" type="xs:string" minOccurs="0"/>
      <xs:element name="authen_protocol" type="xs:string" minOccurs="0"/>
      <xs:element name="framed_ip_address" type="xs:string" minOccurs="0"/>
      <xs:element name="network_device_groups" type="xs:string" minOccurs="0"/>
      <xs:element name="access_service" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="authentication_method" type="xs:string" minOccurs="0"/>
      <xs:element name="execution_steps" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_response" type="xs:string" minOccurs="0"/>
      <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_identifier" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port_id" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_policy_compliance" type="xs:string" minOccurs="0"/>
      <xs:element name="auth_id" type="xs:long" minOccurs="0"/>
      <xs:element name="auth_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
      <xs:element name="message_code" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_session_id" type="xs:string" minOccurs="0"/>
      <xs:element name="service_selection_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="authorization_policy" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="response" type="xs:string" minOccurs="0"/>
      <xs:element name="service_type" type="xs:string" minOccurs="0"/>
      <xs:element name="cts_security_group" type="xs:string" minOccurs="0"/>
      <xs:element name="use_case" type="xs:string" minOccurs="0"/>
      <xs:element name="cisco_av_pair" type="xs:string" minOccurs="0"/>
      <xs:element name="ad_domain" type="xs:string" minOccurs="0"/>
      <xs:element name="acs_username" type="xs:string" minOccurs="0"/>
      <xs:element name="radius_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_role" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_username" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_posture_token" type="xs:string" minOccurs="0"/>
      <xs:element name="nac_radius_is_user_auth" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_posture_server" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="authentication_identity_store" type="xs:string" minOccurs="0"/>
      <xs:element name="azn_exp_pol_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="ext_pol_server_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="grp_mapping_pol_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="identity_policy_matched_rule" type="xs:string" minOccurs="0"/>
      <xs:element name="nas_port_type" type="xs:string" minOccurs="0"/>
      <xs:element name="query_identity_stores" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_azn_profiles" type="xs:string" minOccurs="0"/>
      <xs:element name="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
      <xs:element name="selected_query_identity_stores" type="xs:string" minOccurs="0"/>
      <xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
    

```

```

<xs:element name="tunnel_details" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_ssg_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="other_attributes" type="xs:string" minOccurs="0"/>
<xs:element name="response_time" type="xs:long" minOccurs="0"/>
<xs:element name="nad_failure" type="xs:anyType" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
<xs:element name="acct_id" type="xs:long" minOccurs="0"/>
<xs:element name="acct_acs_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="acct_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_status_type" type="xs:string" minOccurs="0"/>
<xs:element name="acct_session_time" type="xs:long" minOccurs="0"/>
<xs:element name="acct_input_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_output_octets" type="xs:string" minOccurs="0"/>
<xs:element name="acct_input_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_output_packets" type="xs:long" minOccurs="0"/>
<xs:element name="acct_class" type="xs:string" minOccurs="0"/>
<xs:element name="acct_terminate_cause" type="xs:string" minOccurs="0"/>
<xs:element name="acct_multi_session_id" type="xs:string" minOccurs="0"/>
<xs:element name="acct_authentic" type="xs:string" minOccurs="0"/>
<xs:element name="termination_action" type="xs:string" minOccurs="0"/>
<xs:element name="session_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="idle_timeout" type="xs:string" minOccurs="0"/>
<xs:element name="acct_interim_interval" type="xs:string" minOccurs="0"/>
<xs:element name="acct_delay_time" type="xs:string" minOccurs="0"/>
<xs:element name="event_timestamp" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_connection" type="xs:string" minOccurs="0"/>
<xs:element name="acct_tunnel_packet_lost" type="xs:string" minOccurs="0"/>
<xs:element name="security_group" type="xs:string" minOccurs="0"/>
<xs:element name="cisco_h323_setup_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_connect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="cisco_h323_disconnect_time" type="xs:dateTime" minOccurs="0"/>
<xs:element name="framed_protocol" type="xs:string" minOccurs="0"/>
<xs:element name="started" type="xs:anyType" minOccurs="0"/>
<xs:element name="stopped" type="xs:anyType" minOccurs="0"/>
<xs:element name="ckpt_id" type="xs:long" minOccurs="0"/>
<xs:element name="type" type="xs:long" minOccurs="0"/>
<xs:element name="nad_acsview_timestamp" type="xs:dateTime" minOccurs="0"/>
<xs:element name="vlan" type="xs:string" minOccurs="0"/>
<xs:element name="dacl" type="xs:string" minOccurs="0"/>
<xs:element name="authentication_type" type="xs:string" minOccurs="0"/>
<xs:element name="interface_name" type="xs:string" minOccurs="0"/>
<xs:element name="reason" type="xs:string" minOccurs="0"/>
<xs:element name="endpoint_policy" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

Invoking an Audit Session ID API Call



Note

Make sure that the target node to which you are issuing an API call is a valid Monitoring node. To verify the persona of a Cisco ISE node, see [Verifying a Monitoring Node, page 1-2](#).

Step 1 Log in to the target Monitoring node.

For example, when you initially log in to a Monitoring node with the hostname acme123, the following URL address field is displayed:


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

- Step 2** Enter the audit session ID API call in the URL address field of the target node by replacing the “/admin/” component with the API call component (/admin/API/mnt/Session/Active/SessionID/<audit-session-id>/0):

```
https://acme123/admin/API/mnt/Session/Active/SessionID/0A000A770000006B609A13A9/0
```



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 the target Monitoring node.

- Step 3** Press **Enter** to issue the API call.

Audit Session ID API Call Data

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

```
--<activeSessionList noOfActiveSession="1">
  <activeSession>
    <calling_station_id>00:50:56:10:13:02</calling_station_id>
    <session_state_bit>0</session_state_bit>
    <session_source>0</session_source>
    <acct_session_time>0</acct_session_time>
    <nas_ip_address>10.0.10.119</nas_ip_address>
    <nas_port_id>GigabitEthernet1/0/15</nas_port_id>
    <auth_method>dot1x</auth_method>
    <auth_protocol>PEAP (EAP-MSCHAPv2)</auth_protocol>
    <posture_status>Compliant</posture_status>
    <endpoint_policy>Undetermined</endpoint_policy>
    <server>acme123</server>
    <paks_in>0</paks_in>
    <paks_out>0</paks_out>
    <bytes_in>0</bytes_in>
    <bytes_out>0</bytes_out>
  </activeSession>
</activeSessionList>
```

Removing Stale Sessions

Some devices, such as wireless LAN controllers (WLCs), may allow stale sessions to linger. In such cases, you use the HTTP DELETE API call to manually delete the inactive sessions. To do so, use cURL, a free 3rd-party command line tool for transferring data with URL (HTTP, HTTPS) syntax, as shown in the following procedure.

Cisco ISE no longer tracks stale sessions. This is to mitigate cases when Cisco ISE loses connectivity to the network for an extended period of time and misses accounting stops from the WLC or network access device (NAD). You can clear such stale information from Cisco ISE using the HTTP DELETE API call.



Note

GNU Wget, the free utility for retrieving files using HTTP and HTTPS, does not support the HTTP DELETE API call.

Step 1 Log in to the target Monitoring node from the command line.



Note API calls are case sensitive and must be entered carefully. The variable <mntnode> represents the target Monitoring node.

Step 2 To manually delete a stale session for a MAC address, issue the following API call on the command line:

```
curl -X DELETE https://<mntnode>/ise/mt/Session/Delete/MACAddress/<macaddress>
```

Step 3 To manually delete a stale session for a session ID, issue the following API call on the command line:

```
curl -X DELETE https://<mntnode>/ise/mt/Session/Delete/SessionID/<sid#>
```

Step 4 To manually delete all sessions on the Monitoring node, issue the following API call on the command line:

```
curl -X DELETE https://<mntnode>/ise/mt/Session/Delete/All
```
