CHAPTER 1

Introduction to Monitoring REST APIs

The *Cisco Identity Services Engine API Reference Guide, Release 1.1.x*, provides you with guidelines and examples for using the three supported categories of representational state transfer (REST) APIs and related API calls. The REST APIs and calls allow you to gather session and node-specific information by using Cisco Monitoring ISE nodes in your network. A session is defined as the duration between when you start accessing the desired node and completing the set of tasks or operations needed to gather information.

The supported categories of Monitoring REST APIs that are available to users in Cisco ISE, Release 1.1 are as follows:

- Query
  - Session Management
  - Troubleshooting
- Change of Authorization (CoA)

Note You can use only these supported REST API categories to gather information about endpoints being monitored by the Monitoring persona. Monitoring is one of three supported personas that an ISE node type can perform in your Cisco ISE Release 1.1 deployment. For the remainder of this guide, "Monitoring ISE node" will be used to describe the Monitoring persona of a Cisco ISE node.

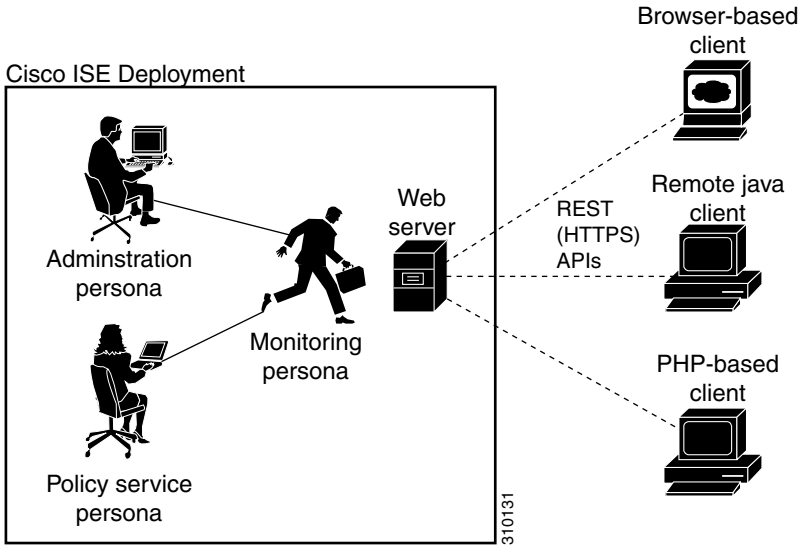
Any attempt to use these APIs to gather information about the Policy Service persona of a Cisco ISE appliance in a Cisco ISE deployment will result in an error. For more information about Cisco ISE nodes and personas, see the *Cisco Identity Services Engine User Guide, Release 1.1.x*.

The REST API calls provide the means for you to locate, monitor, and accumulate important real-time session-based information stored in individual endpoints in your network that you can access through a Cisco Monitoring ISE node.

The real-time session-based information that you gather can prove useful to understand Cisco ISE operations, assist in diagnosing conditions or issues, or be used to troubleshoot error conditions or activity or behavior that you suspect may be affecting your monitoring operations. The role that the REST APIs play in a Cisco ISE distributed deployment is shown in Figure 1-1.

As shown in Figure 1-1, the REST (HTTPS) API calls are used by supported client types: remote Java, browser-based, or PHP (hypertext preprocessor), and for the purpose of accessing the Cisco Monitoring ISE node and retrieving important session-based information that is stored in the Cisco ISE deployment endpoints.

Figure 1-1 Cisco ISE Distributed Deployment and REST APIs



Verifying a Cisco Monitoring ISE Node

Before you can successfully invoke the API calls on a Cisco Monitoring ISE node, you first need to verify that the node you want to monitor is a valid Cisco Monitoring ISE node. To verify this, you need to successfully log into and be authenticated by the Cisco ISE network.

Note To be able to use the public REST APIs, you must first authenticate with Cisco ISE using valid credentials for any of the supported Cisco ISE admin roles (Helpdesk Admin, Identity Admin, Monitoring Admin, Network Device Admin, Policy Admin, RBAC Admin, Super Admin, or System Admin).

To login and be authenticated, complete the following steps:

Step 1 Enter valid login credentials (Username and Password) in the Cisco ISE Login window, and click **Login**.

The Cisco ISE dashboard and user interface appears.

Step 2 Choose **Authorization > System > Deployment**.

The Deployment Nodes page appears, which lists all configured nodes that are deployed.

Step 3 In the Roles column of the Deployment Nodes page, verify that the role for the target node that you want to monitor shows its type as a Cisco Monitoring ISE node.

Supported API Calls

This section introduces the REST APIs, which provide an interface for programmatically issuing calls that retrieve and display the node-specific or session-specific information. The following tables list the API category, type of API call, and provide a brief description and an example of the API call format:

- Table 1-1 on page 1-3—defines the query API calls for session management.
- Table 1-2 on page 1-6—defines the query API calls for troubleshooting.
- Table 1-3 on page 1-7—defines the CoA API calls.

Note Before you can perform any of the API calls described in this guide, you first need to log into and be authenticated by the Cisco ISE network. The authentication requirement for using the public REST APIs is explained in Verifying a Cisco Monitoring ISE Node, page 1-2.

If you intend to use a generic programmatic interface to authenticate with the REST API supported by Cisco ISE, you would need to first create a REST-based client that bridges between Cisco ISE and the specific tool you use. You would then use this REST client to perform authentication with the Cisco ISE REST APIs, marshal and submit the API requests to the Monitoring ISE nodes, and unmarshal the API responses and pass these responses on to the specified tool.

Table 1-1 Cisco ISE Query API Calls - Session Management

Cisco ISE API Call Category	Cisco ISE API Call Description and Example
Session Management	
Session Counters	
• Active sessions counter	Lists the number of currently active sessions: *https://<ISEhost>/ise/mnt/api/Session/ActiveCount*
• Posture sessions counter	Lists the number of currently active Posture service sessions: *https://<ISEhost>/ise/mnt/api/Session/PostureCount* **Note** Posture is a service that aids in checking the state (or posture) for all the endpoints that connect to your Cisco ISE network.
• Profiler sessions counter	Lists the number of currently active Profiler service sessions: *https://<ISEhost>/ise/mnt/api/Session/ProfilerCount* **Note** Profiler is a service that aids in identifying, locating, and determining the capabilities of all attached endpoints on your Cisco ISE network.

Table 1-1 Cisco ISE Query API Calls - Session Management (continued)

Cisco ISE API Call Category	Cisco ISE API Call Description and Example
Simple Session List **Note** A simple session list includes the MAC address, network access switch (NAS) IP address, user name, and session ID information associated with a session.The Cisco Identity Services Engine, Release 1.1, is not compliant with IPv6. **Note** The level of support for IPv6 in Cisco ISE is only as it relates to the node being addressed on an IPv6 network (for example, IPv6 stateless auto-configuration and DHPv6). However, none of the Cisco ISE, Release 1.1, protocol stacks (such as runtime or mgmt) supports IPv6.	
• Active sessions list	Lists all currently active sessions: *https://<ISEhost>/ise/mnt/api/Session/ActiveList* **Note** In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is limited to 100,000.
• Authenticated sessions list	Lists all currently active authenticated sessions: *https://<ISEhost>/ise/mnt/api/Session/AuthList/<parameteroptions>* **Note** The starttime/endtime format is yyyy-mm-dd hh24:MM:ss (for example, 2010-12-10 16:30:00). **Note** You can specify the following parameter options that will return different values: • If null/null is specified, this lists all currently active authenticated sessions. • If null/endtime is specified, this list all currently active authenticated sessions after the specified endtime. • If starttime/null is specified, this lists all currently active authenticated sessions before the specified starttime. • If starttime/endtime is specified, this lists all currently active authenticated sessions between the specified starttime and endtime. See Sample Data Returned from the AuthList API Call, page 2-9, for samples that show all four parameter options. **Note** In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is limited to 100,000.

Table 1-1 Cisco ISE Query API Calls - Session Management (continued)

Cisco ISE API Call Category	Cisco ISE API Call Description and Example
Detailed Session Attributes	
Note This is a timestamp-based search for the latest session that contains the specified search attribute.	
• MAC address session search	Searches the database for the latest session that contains the specified MAC address: *https://<ISEhost>/ise/mnt/api/Session/MACAddress/<macaddress>* **Note** XX:XX:XX:XX:XX:XX is the MAC address format and is not case-sensitive (for example, 0a:0B:0c:0D:0e:0F). **Note** The MAC address serves as the only unique key to finding the correct session you want to monitor. Use the ActiveList API call to list all active sessions and their MAC addresses, from which you can base your MAC address search.
• User name session search	Searches the database for the latest session that contains the specified user name: *https://<ISEhost>/ise/mnt/api/Session/UserName/<username>* **Note** User names must conform to the same Cisco ISE password policy used for network user names. The only invalid character for REST APIs is the backslash (/) character. For details, see "User Password Policy" in the *Cisco Identity Services Engine User Guide, Release 1.1.x*.
• NAS IP address session search	Searches the database for the latest session that contains the specified NAS IP address: *https://<ISEhost>/ise/mnt/api/Session/IPAddress/<nasipaddress>* **Note** xxx.xxx.xxx.xxx is the NAS IP address format (for example, 10.10.10.10).

For specific details about the Cisco ISE query API calls for session management, see Chapter 2, "Using the Query APIs for Session Management".

Table 1-2 Cisco ISE Query API Calls - Troubleshooting

Cisco ISE API Call Category	Cisco ISE API Call Description and Example
Query - Troubleshooting	
Get Version and Type of Node	
• Node version and type	Lists the node version and type: *https://<ISEhost>/ise/mnt/api/Version* Node type can be any of the following values (0-3): STAND_ALONE_MNT_NODE = 0 ACTIVE_MNT_NODE = 1 STAND_BY_MNT_NODE = 2 NOT_AN_MNT_NODE = 3 **Note** STAND_ALONE_MNT_NODE means it is a Cisco Monitoring ISE node that functions not as part of any distributed deployment. ACTIVE_MNT_NODE means it is a primary node in a primary-secondary relationship in a distributed deployment. STAND_BY_MNT_NODE means it is a secondary node in a primary-secondary pair in this same type of deployment. NOT_AN_MNT_NODE means it is not a Cisco Monitoring ISE node. See the *Cisco Identity Services Engine User Guide, Release 1.1* for details about the supported ISE nodes and personas.
Get Failure Reasons Mapping	
• Failure reasons	Lists the reasons for failure: *https://<ISEhost>/ise/mnt/api/FailureReasons* Each failure reason displays an error code (failureReason id), a brief description (code), a failure reason (cause), and a possible response (resolution), as shown in the following example: <failureReason id="100009"> <code> 100009 WEBAUTH_FAIL <cause> This may or may not be indicating a violation. <resolution> Please review and resolve this issue according to your organization's policy. **Note** The use case for which the FailureReasons API call is designed addresses the need for it to be called only once to gather the information from the Monitoring ISE node. You should store the contents of any returned failure reasons into your own file system or database. The returned contents of these API calls are intended to be used for reference purposes. If you experience any issues during authentication, you should compare the failure reason code provided in the authentication response with the list of failure reasons that you have stored in you own file system or database. For a complete list of Cisco ISE failure reasons, see Appendix A, "Using the Cisco ISE Failure Reasons Editor".

Table 1-2 Cisco ISE Query API Calls - Troubleshooting (continued)

Cisco ISE API Call Category	Cisco ISE API Call Description and Example
Get Session Auth Status	
• Session authentication status	Lists the authentication status for all sessions: *https://<ISEhost>/ise/mnt/api/AuthStatus/MACAddress/<macaddress>/<numberofseconds>/<numberofrecordspermacaddress>/All* **Note** The seconds parameter <numberofseconds> is user-configurable, with the range being from a minimum of 0 to a maximum of 432000 seconds (5 days). **Note** Authentication status is defined as when all of the data fields are available in the RADIUS_AUTH table.
Get Session Accounting Status	
• Accounting session status	Lists the accounting status of all sessions within a specific period of time: *https://<ISEhost>/ise/mnt/api/Session/AcctStatusTT/MACAddress/<macaddress>/<numberof seconds>* **Note** The seconds parameter <numberofseconds> is user-configurable, with the range being from a minimum of 0 to a maximum of 432000 seconds (5 days).

For specific details about the Cisco ISE Query API calls for Troubleshooting, see Chapter 2, "Using the Query APIs for Session Management".

Table 1-3 Cisco ISE Change of Authorization API Calls

Cisco ISE API Call Category	Cisco ISE API Call Description and Example
CoA Session Management	
Session Reauth	
• Session reauthentication types	Sends a session reauthentication command and type: *https://<ISEhost>/ise/mnt/api/CoA/Reauth/<serverhostname>/<macaddress>/<reauthtype>/<nasipaddress>/<destinationipaddress>* Reauth type can be any of the following values (0-2): REAUTH_TYPE_DEFAULT = 0 REAUTH_TYPE_LAST = 1 REAUTH_TYPE_RERUN = 2 **Note** If you do not know the NAS IP address, you can enter the required values up to that point and the API will use these values in its search query. However, you must know the MAC address to perform this API call. This API call can only be executed on a Monitoring ISE node, which submits the requests to perform CoA remotely. The Administration ISE node is not involved or required to execute these CoA API calls.

Table 1-3 Cisco ISE Change of Authorization API Calls (continued)

Cisco ISE API Call Category	Cisco ISE API Call Description and Example
Session Disconnect	
• Session disconnect types	Sends a session disconnect command and port option type: *https://<ISEhost>/ise/mnt/api/CoA/Disconnect/<serverhostname>/<macaddress>/<disconnecttype>/<nasipaddress>/<destinationipaddress>* **Note** Port option type can be any of the following values (0-2): DYNAMIC_AUTHZ_PORT_DEFAULT = 0 DYNAMIC_AUTHZ_PORT_BOUNCE = 1 DYNAMIC_AUTHZ_PORT_SHUTDOWN = 2 **Note** If you do not know the NAS IP address, enter the required values up to that point and the API will use these values in its search query. However, you must know the MAC address to perform this API call.

For details about Cisco ISE Change of Authorization API calls, see Chapter 4, "Using the Change of Authorization REST APIs".

Supported API Calls using HTTP PUT

Similar to a Get Session Auth Status API call in Table 1-2, there is an HTTP PUT version of a REST API implemented that allows clients to retrieve account status. The REST APIs support both HTTP PUT and HTTP GET calls, with the examples in this guide documenting HTTP GET calls. The HTTP PUT version addresses the need for APIs that require parameter inputs. The following schema file example is a request for account status:

```
<?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="acctRequest" type="mnTRESTAcctRequest"/>

  <xs:complexType name="mnTRESTAcctRequest">
    <xs:complexContent>
      <xs:extension base="mnTRESTRequest">
        <xs:sequence>
          <xs:element name="duration" type="xs:string" minOccurs="0"/>
        </xs:sequence>
      </xs:extension>
    </xs:complexContent>
  </xs:complexType>
```

```
  <xs:complexType name="mnTRESTRequest" abstract="true">
    <xs:sequence>
      <xs:element name="valueList">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="value" type="xs:string" maxOccurs="unbounded"/>
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      <xs:element name="searchCriteria" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:schema>
```