



## **Cisco Identity Services Engine Release 1.1.x API リファレンス ガイド**

2012 年 7 月

**【注意】シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。**

**本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報  
につきましては、日本語版掲載時点で、英語版にアップデートがあ  
り、リンク先のページが移動 / 変更されている場合がありますこと  
をご了承ください。  
あくまでも参考和訳となりますので、正式な内容については米国サ  
イトのドキュメントを参照ください。**

**また、契約等の記述については、弊社販売パートナー、または、弊  
社担当者にご確認ください。**

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

*Cisco Identity Services Engine Release 1.1.x API リファレンス ガイド*

© 2012 Cisco Systems, Inc.

All rights reserved.

Copyright © 2012, シスコシステムズ合同会社.

All rights reserved.



## CONTENTS

はじめに	vii
Cisco Identity Services Engine の概要	vii
目的	viii
対象読者	viii
マニュアルの構成	ix
ドキュメントの表記法	ix
マニュアルの更新	x
製品に関する資料	x
関連資料	x
このリリースのマニュアル	x
プラットフォーム別のマニュアル	xi
マニュアルの入手方法およびテクニカル サポート	xii

---

### PART 1

---

## Cisco ISE Monitoring REST API

---

### CHAPTER 1

<b>Monitoring REST API の概要</b>	1-1
Cisco Monitoring ISE ノードの確認	1-2
サポートされる API コール	1-3
HTTP PUT を使用したサポート対象の API コール	1-9

---

### CHAPTER 2

<b>セッション管理のためのクエリー API の使用</b>	2-1
セッション カウンタ API コールの使用	2-1
アクティブ セッション カウンタ	2-1
ActiveCount API の出カスキーマ	2-2
ActiveCount API コールの呼び出し	2-2
ActiveCount API コールから返されるサンプル データ	2-2
ポスチャ セッション カウンタ	2-3
PostureCount API の出カスキーマ	2-3
PostureCount API コールの呼び出し	2-3
PostureCount API コールから返されるサンプル データ	2-4
プロファイラ セッション カウンタ	2-4
ProfilerCount API の出カスキーマ	2-4
ProfilerCount API コールの呼び出し	2-4
ProfilerCount API コールから返されるサンプル データ	2-5

単純なセッション リスト API コールの使用	2-5
アクティブなセッション リスト	2-5
ActiveList API の出カスキーマ	2-6
ActiveList API コールの呼び出し	2-6
ActiveList API コールから返されるサンプル データ	2-7
認証セッション リスト	2-8
AuthList API の出カスキーマ	2-8
AuthList API コールの呼び出し	2-8
AuthList API コールから返されるサンプル データ	2-9
詳細なセッション属性 API コールの使用	2-11
MAC アドレス セッションの検索	2-12
MACAddress API の出カスキーマ	2-12
MACAddress API コールの呼び出し	2-14
MACAddress API コールから返されるサンプル データ	2-14
ユーザ名のセッションの検索	2-16
UserName API の出カスキーマ	2-16
UserName API コールの呼び出し	2-18
UserName API コールから返されるサンプル データ	2-18
NAS IP アドレス セッションの検索	2-20
IPAddress API の出カスキーマ	2-20
NAS IPAddress API コールの呼び出し	2-22
IPAddress API コールから返されるサンプル データ	2-22
エンドポイントの IP アドレスのセッションの検索	2-24
EndPointIPAddress API の出カスキーマ	2-24
EndPointIPAddress API コールの呼び出し	2-26
EndPointIPAddress API コールから返されるサンプル データ	2-26
古いセッションの削除	2-28

---

**CHAPTER 3**

トラブルシューティング用のクエリー API の使用	3-1
クエリー API を使用した Cisco ISE のトラブルシューティング	3-1
ノードのバージョンおよびタイプの API コール	3-2
バージョン API の出カスキーマ	3-2
バージョン API コールの呼び出し	3-2
バージョン API コールから返されるサンプル データ	3-3
障害理由 API コール	3-3
FailureReasons API の出カスキーマ	3-4
FailureReasons API コールの呼び出し	3-4
FailureReasons API コールから返されるサンプル データ	3-5
認証ステータス API コール	3-7

AuthStatus API の出カスキーマ	3-8
AuthStatus API コールの呼び出し	3-10
AuthStatus API コールから返されるサンプル データ	3-11
アカウント ステータス API コール	3-15
AcctStatus API の出カスキーマ	3-15
AcctStatus API 呼び出しを呼び出すこと	3-16
AcctStatus API コールから返されるサンプル データ	3-17

---

**CHAPTER 4****認可変更 REST API の使用 4-1**

CoA セッション管理 API コールの使用	4-1
セッション再認証 API コール	4-1
Reauth API の出カスキーマ	4-2
Reauth API コールの呼び出し	4-2
Reauth API コールから返されるサンプル データ	4-3
セッション切断 API コール	4-3
Disconnect API の出カスキーマ	4-3
Disconnect API コールの呼び出し	4-3
Disconnect API コールから返されるサンプル データ	4-4

---

**PART 2****参考資料**

---

**APPENDIX A****Cisco ISE Failure Reasons Editor の使用 A-1**

理由の表示および編集	A-1
------------	-----





## はじめに

---

ここでは、『Cisco Identity Services Engine Release 1.1 および 1.1.1 API リファレンス ガイド』の目的、対象読者、および構成について説明します。また、指示を記述する表記法について説明し、次のセクションでは他の種類の情報を説明します。

- 「Cisco Identity Services Engine の概要」 (P.vii)
- 「目的」 (P.viii)
- 「対象読者」 (P.viii)
- 「マニュアルの構成」 (P.ix)
- 「ドキュメントの表記法」 (P.ix)
- 「マニュアルの更新」 (P.x)
- 「製品に関する資料」 (P.x)
- 「関連資料」 (P.x)
- 「マニュアルの入手方法およびテクニカル サポート」 (P.xii)

## Cisco Identity Services Engine の概要

Cisco Identity Services Engine (ISE) は、次世代アイデンティティおよびアクセス制御ポリシープラットフォームとして、企業でのコンプライアンスの順守、インフラストラクチャのセキュリティの強化、サービス オペレーションの合理化を実現します。Cisco ISE の固有のアーキテクチャにより、企業は、アクセス スイッチ、Wireless LAN Controller (WLC)、バーチャルプライベートネットワーク (VPN) ゲートウェイ、およびデータセンター スイッチなど、さまざまなネットワーク要素に ID を結びつけることで予防的な管理を決定するために、ネットワーク、ユーザ、およびデバイスからリアルタイムのコンテキスト情報を収集することができるようになります。

Cisco ISE は Cisco Security Group Access Solution の重要なコンポーネントです。Cisco ISE は、統合ポリシー ベースのアクセス コントロール ソリューションで、次の機能があります。

- 認証、許可、アカウントिंग (AAA)、ポスチャ、プロファイル、およびゲストの管理サービスを 1 つのアプライアンスに統合します。
- 802.1X 環境を含むネットワークにアクセスしているすべてのエンドポイントのデバイス ポスチャをチェックして、エンドポイントへの準拠を強制します。
- ネットワーク上のエンドポイントの検出、プロファイリング、ポリシー ベースの配置、モニタリングのサポートを提供します。
- 集中型展開および分散型展開で一貫性ポリシーを有効にし、必要な箇所にサービスを配布できるようにします。

- セキュリティグループタグ (SGT) およびセキュリティグループ (SG) アクセスコントロールリスト (ACL) の使用により、セキュリティグループアクセス (SGA) などの高度な適用機能を使用します。
- 小規模なオフィス環境から大規模な企業環境まで、多くの導入シナリオをサポートするスケーラビリティをサポートします。

Cisco ISE のアーキテクチャは、集中型ポータルからネットワークを設定して管理できるように、スタンドアロンの導入と分散型の導入をサポートします。Cisco ISE の機能の詳細については、『[Cisco Identity Services Engine User Guide, Release 1.1.1](#)』を参照してください。

## 目的

このアプリケーションプログラミングインターフェイス (API) リファレンスガイドは、サポート対象の API が提供する機能の概要だけを説明します。この API リファレンスガイドの目的は、Cisco ISE 展開内で概説された API を使用するための基本的な注意事項を、開発者、システム管理者やネットワーク管理者、またはシステムインテグレータに提供することです。

API コールは、次の種類のデータを確認するためにクエリーを使用します。

- アクティブセッションの数
- アクティブセッションのタイプ
- アクティブセッションの認証ステータス
- 使用中の MAC アドレス
- 使用中の NAS の IP アドレス
- ノードのバージョンとタイプ
- ノードのセッション障害の理由



(注)

この API リファレンスガイドは、『[Cisco Identity Services Engine User Guide, Release 1.1.1](#)』に代わるものではありません。Cisco ISE ネットワークとそのノードおよびペルソナ、動作または用途の概念、Cisco ISE ユーザインターフェイスの使用法の詳細については、『[Cisco Identity Services Engine User Guide, Release 1.1.1](#)』を参照してください。たとえば、用語集には Cisco ISE ネットワークで使用される主な用語と概念の完全なリストが含まれています。

## 対象読者

この API リファレンスガイドは、ネットワーク環境内で Cisco ISE アプライアンスを管理する経験豊富なシステム管理者、API を利用するシステムインテグレータ、Cisco ISE 導入の管理やトラブルシューティングの役割を持つサードパーティ製パートナーを対象としています。この API リファレンスガイドを使用する前提条件として、トラブルシューティングと診断方法について、API コールの作成および解釈方法について、基礎を理解しておく必要があります。



## マニュアルの構成

このマニュアルは、次の章で構成されています。

- Part 1 — Cisco ISE Monitoring REST API
  - 第 1 章「Monitoring REST API の概要」
  - 第 2 章「セッション管理のためのクエリー API の使用」
  - 第 3 章「トラブルシューティング用のクエリー API の使用」
  - 第 4 章「認可変更 REST API の使用」
- Part 2 — 参考資料
  - 付録 A「Cisco ISE Failure Reasons Editor の使用」

## ドキュメントの表記法

ここでは、このマニュアル全体で使用されている表記法について説明します。



**注意**

「**要注意**」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



**(注)**

「**注釈**」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

この API リファレンス ガイドは次の表記法を使用して、指示と情報を伝送します。

項目	表記法
手順で選択する必要があるコマンド、キーワード、特殊な用語、およびオプション	<b>太字</b>
ユーザが値を指定する変数、および新しい用語や重要な用語	<i>イタリック体</i>
表示されるセッション情報、システム情報、パス、およびファイル名	screen フォント
ユーザが入力する情報。	<b>太字の screen</b> フォント
ユーザが入力する変数。	<i>イタリック体の screen</i> フォント
選択するメニュー項目を、選択する順序で示します。	[ <b>オプション (Option)</b> ] > [ <b>ネットワーク プリファレンス (Network Preferences)</b> ]

## マニュアルの更新

表 1 に、このマニュアルの初版と、更新の履歴、および最新の更新が示されます。

表 1 『Cisco Identity Services Engine Release 1.1.x API リファレンス ガイド』の更新

日付	説明
2012 年 7 月 10 日	Cisco Identity Services Engine, Release 1.1.1
2012 年 3 月 19 日	Cisco Identity Services Engine, Release 1.1

## 製品に関する資料



(注)

初版発行後、印刷物または電子マニュアルのアップデートを行う場合があります。マニュアルの更新については、<http://cisco.com> で確認してください。

表 2 に、[www.cisco.com](http://www.cisco.com) で入手可能な Cisco ISE Release 1.1 の関連製品のマニュアルを示します。[www.cisco.com](http://www.cisco.com) ですべての製品のエンド ユーザ マニュアルを検索するには、次のサイトにアクセスしてください。

<http://www.cisco.com/go/techdocs>

## 関連資料

ここでは、このリリースのマニュアルと、このプラットフォームのマニュアルの情報を提供します。

## このリリースのマニュアル

表 2 に、Cisco ISE リリースで利用可能な製品マニュアルを示します。Cisco ISE の一般的な製品に関する情報は、<http://www.cisco.com/go/ise> で入手できます。エンド ユーザ マニュアルは、[http://www.cisco.com/en/US/products/ps11640/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html) にある Cisco.com から入手できます。

表 2 Cisco Identity Services Engine の製品マニュアル

マニュアル名	参照先
<ul style="list-style-type: none"> <li>『Release Notes for the Cisco Identity Services Engine, Release 1.1』</li> <li>『Release Notes for the Cisco Identity Services Engine, Release 1.1.1』</li> </ul>	<a href="http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html">http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html</a>
<ul style="list-style-type: none"> <li>『Cisco Identity Services Engine Network Component Compatibility, Release 1.1』</li> <li>『Cisco Identity Services Engine Network Component Compatibility, Release 1.1.1』</li> </ul>	<a href="http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html">http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html</a>

表 2 Cisco Identity Services Engine の製品マニュアル (続き)

マニュアル名	参照先
<ul style="list-style-type: none"> <li>『Cisco Identity Services Engine User Guide, Release 1.1』</li> <li>『Cisco Identity Services Engine User Guide, Release 1.1.1』</li> </ul>	<a href="http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html">http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html</a>
<ul style="list-style-type: none"> <li>『Cisco Identity Services Engine Hardware Installation Guide, Release 1.1』</li> <li>『Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1』</li> </ul>	<a href="http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html</a>
『Cisco Identity Services Engine Upgrade Guide, Release 1.1.1』	<a href="http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html</a>
『Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.x』	<a href="http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html</a>
『Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.x』	<a href="http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html">http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html</a>
『Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x』	<a href="http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html">http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html</a>
『Cisco Identity Services Engine API Reference Guide, Release 1.1.x』	<a href="http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html">http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html</a>
『Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x』	<a href="http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html">http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html</a>
『Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler』	<a href="http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html">http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html</a>
『Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card』	<a href="http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html">http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html</a>

## プラットフォーム別のマニュアル

Policy Management Business Unit マニュアルへのリンクは、次の場所にある [www.cisco.com](http://www.cisco.com) で利用できます。

- Cisco ISE  
[http://www.cisco.com/en/US/products/ps11640/prod\\_installation\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html)
- Cisco Secure ACS  
[http://www.cisco.com/en/US/products/ps9911/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html)
- Cisco NAC アプライアンス  
[http://www.cisco.com/en/US/products/ps6128/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html)
- Cisco NAC プロファイラ  
[http://www.cisco.com/en/US/products/ps8464/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html)

- Cisco NAC ゲスト サーバ  
[http://www.cisco.com/en/US/products/ps10160/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html)

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



## **PART 1**

# **Cisco ISE Monitoring REST API**





# CHAPTER 1

## Monitoring REST API の概要

『Cisco Identity Services Engine API リファレンス ガイド』には、サポート対象の 3 つのカテゴリの Representational State Transfer (REST) API および関連 API コール使用のガイドラインと使用例が記載されています。REST API とコールでは、ネットワークで Cisco Monitoring ISE ノードを使用することにより、セッションおよびノード固有の情報を収集することができます。セッションは、目的のノードへのアクセスの開始から情報の収集に必要なタスクまたは操作のセットの完了までの期間として定義されます。

Cisco ISE Release 1.1.1 でユーザが使用できる、サポート対象の Monitoring REST API のカテゴリは、次のとおりです。

- クエリー
  - セッション管理
  - トラブルシューティング
- 認可変更 (CoA)



(注)

Monitoring ペルソナによって監視されているエンドポイントに関する情報を収集するためには、これらのサポート対象の REST API カテゴリだけを使用できます。Monitoring は、ISE のノードタイプが Cisco ISE リリース 1.1 の展開で実行できる、サポート対象の 3 つのペルソナの 1 つです。このガイドの残りの部分では、Cisco ISE ノードの Monitoring ペルソナを説明するため、「Monitoring ISE ノード」を使用します。

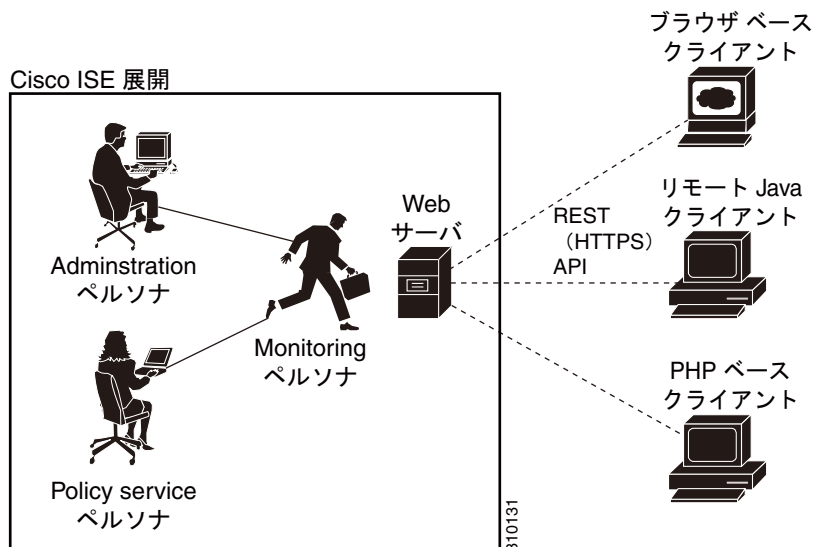
これらの API を Cisco ISE 展開における Cisco ISE アプライアンスの Policy service ペルソナに関する情報の収集に使用しようとすると、エラーが発生します。Cisco ISE ノードおよびペルソナに関する詳細については、『Cisco Identity Services Engine User Guide, Release 1.1.1』を参照してください。

REST API コールは、ユーザが Cisco Monitoring ISE ノードを通じてアクセスできるネットワークで、個々のエンドポイントに格納されている重要なリアルタイムのセッションベースの情報を検索、監視、収集する手段を提供します。

ユーザが収集するリアルタイムのセッションベースの情報は、Cisco ISE 操作の理解、状態や問題の診断の支援に役立ちます。また、モニタリング業務に影響を与える可能性のあるエラー状態、アクティビティ、動作などのトラブルシューティングに使用することもできます。REST API が Cisco ISE 分散展開で果たす役割を [図 1-1](#) に示します。

[図 1-1](#) に示すように、REST (HTTPS) API コールは、サポートされているクライアントのタイプ (リモート Java、ブラウザベース、または PHP (ハイパーテキストプリプロセッサ)) によって使用され、Cisco Monitoring ISE ノードにアクセスして Cisco ISE 展開のエンドポイントに格納されている重要なセッションベースの情報を取得する目的で使用されます。

図 1-1 Cisco ISE の分散展開および REST API



## Cisco Monitoring ISE ノードの確認

API コールを Cisco Monitoring ISE ノードで正常に呼び出す前に、監視するノードが有効な Cisco Monitoring ISE ノードであることを確認しておく必要があります。これを確認するには、正常にログインして、Cisco ISE ネットワークによって認証を受ける必要があります。



(注)

パブリック REST API を使用できるようにするには、サポート対象の Cisco ISE 管理ロール (Helpdesk Admin、Identity Admin、Monitoring Admin、Network Device Admin、Policy Admin、RBAC Admin、Super Admin、System Admin) の有効なクレデンシヤルを使用して、最初に Cisco ISE で認証を受ける必要があります。

ログインして認証を受けるには、次の手順を実行します。

- ステップ 1** 有効なログインクレデンシヤル (ユーザ名とパスワード) を [Cisco ISE ログイン (Cisco ISE Login) ] ウィンドウに入力し、[ログイン (Login) ] をクリックします。
- Cisco ISE ダッシュボードとユーザインターフェイスが表示されます。
- ステップ 2** [許可 (Authorization) ] > [システム (System) ] > [展開 (Deployment) ] の順に選択します。
- 展開されたすべての設定済みノードがリストされた [展開ノード (Deployment Nodes) ] ページが表示されます。
- ステップ 3** [展開ノード (Deployment Nodes) ] ページの [ロール (Roles) ] カラムに、監視するターゲットノードのロールが Cisco Monitoring ISE ノードタイプとして表示されていることを確認します。



## サポートされる API コール

ここでは、ノード固有またはセッション固有の情報を取得して表示するコールをプログラムで発行するためのインターフェイスを提供する REST API の概要を説明します。次の表に、API カテゴリと API コールのタイプ、API コールの形式の簡単な説明および例を示します。

- 表 1-1 (P.1-3) : セッション管理用のクエリー API コールを定義します。
- 表 1-2 (P.1-6) : トラブルシューティング用のクエリー API コールを定義します。
- 表 1-3 (P.1-8) : CoA API コールを定義します。



(注)

このマニュアルで説明する API コールを実行するには、最初に Cisco ISE ネットワークにログインして認証を受けておく必要があります。パブリック REST API を使用するための認証要件については、「Cisco Monitoring ISE ノードの確認」(P.1-2) を参照してください。

Cisco ISE でサポートされる REST API を使用して認証を受けるため、汎用プログラマチック インターフェイスを使用する計画の場合、Cisco ISE と使用するツールとの間を接続する REST ベースのクライアントを最初に作成する必要があります。次に、この REST クライアントを使用して Cisco ISE REST API での認証を実行し、API 要求を変換して Monitoring ISE ノードに送信します。そして、API 応答を再変換し、これらの応答を指定されたツールに引き渡します。

表 1-1 Cisco ISE クエリー API コール : セッション管理

Cisco ISE API コール カテゴリ	Cisco ISE API コールの説明と例
セッション管理	
セッション カウンタ	
<ul style="list-style-type: none"> <li>• アクティブ セッション カウンタ</li> </ul>	現在アクティブなセッションの数をリストします。 <i>https://&lt;ISEhost&gt;/ise/mnt/api/Session/ActiveCount</i>
<ul style="list-style-type: none"> <li>• ポスチャ セッション カウンタ</li> </ul>	現在アクティブなポスチャ サービス セッションの数をリストします。 <i>https://&lt;ISEhost&gt;/ise/mnt/api/Session/PostureCount</i> <b>(注)</b> ポスチャとは、Cisco ISE ネットワークに接続しているすべてのエンドポイントの状態（またはポスチャ）の確認を支援するサービスです。
<ul style="list-style-type: none"> <li>• プロファイラセッション カウンタ</li> </ul>	現在アクティブなプロファイラ サービス セッションの数をリストします。 <i>https://&lt;ISEhost&gt;/ise/mnt/api/Session/ProfilerCount</i> <b>(注)</b> プロファイラとは、Cisco ISE ネットワークにあるすべての接続エンドポイントの機能の識別、検索、確認を支援するサービスです。

表 1-1 Cisco ISE クエリー API コール : セッション管理 (続き)

Cisco ISE API コール カテゴリ	Cisco ISE API コールの説明と例
<p>単純なセッションのリスト</p> <p>(注) 単純なセッション リストには、MAC アドレス、ネットワーク アクセス スイッチ (NAS) の IP アドレス、ユーザ名、セッションに関連付けられているセッション ID 情報が含まれます。Cisco Identity Services Engine Release 1.1.1 は、IPv6 に準拠していません。</p> <p>(注) Cisco ISE における IPv6 のサポートの度合いは、IPv6 ネットワーク (IPv6 ステートレス自動設定および DHPv6 など) でアドレス指定されたノードに関係している場合だけです。ただし、Cisco ISE Release 1.1.1 プロトコル スタック (ランタイムや mgmt など) のいずれも IPv6 をサポートしません。</p>	
<ul style="list-style-type: none"> <li>アクティブなセッション リスト</li> </ul>	<p>現在アクティブなすべてのセッションをリストします。</p> <p><code>https://&lt;ISEhost&gt;/ise/mnt/api/Session/ActiveList</code></p> <p>(注) Cisco ISE のこのリリースでは、アクティブな認証済みエンドポイント セッションの表示可能な最大数は、100,000 に制限されています。</p>
<ul style="list-style-type: none"> <li>認証済みセッション リスト</li> </ul>	<p>現在アクティブなすべての認証済みセッションをリストします。</p> <p><code>https://&lt;ISEhost&gt;/ise/mnt/api/Session/AuthList/&lt;parameteroptions&gt;</code></p> <p>(注) starttime/endtime の形式は、yyyy-mm-dd hh24:MM:ss (例 : 2010-12-10 16:30:00) です。</p> <p>(注) 異なる値を返す次のパラメータ オプションを指定できます。</p> <ul style="list-style-type: none"> <li>null/null が指定されると、現在アクティブなすべての認証済みセッションがリストされます。</li> <li>null/endtime が指定されると、指定された endtime の後にアクティブなすべての認証済みセッションがリストされます。</li> <li>starttime/null が指定されると、指定された starttime の前にアクティブなすべての認証済みセッションがリストされます。</li> <li>starttime/endtime が指定されると、指定された starttime と endtime の間で認証されたすべてのセッションがリストされます。</li> </ul> <p>4 つのパラメータ オプションをすべて示すサンプルについては、「AuthList API コールから返されるサンプル データ」(P.2-9) を参照してください。</p> <p>(注) Cisco ISE のこのリリースでは、アクティブな認証済みエンドポイント セッションの表示可能な最大数は、100,000 に制限されています。</p>

表 1-1 Cisco ISE クエリー API コール：セッション管理（続き）

Cisco ISE API コール カテゴリ	Cisco ISE API コールの説明と例
詳細なセッション属性 (注) これは、指定された検索属性を含む最新のセッションのタイムスタンプに基づいた検索です。	
<ul style="list-style-type: none"> <li>MAC アドレス セッションの検索</li> </ul>	指定した MAC アドレスを含む最新のセッションについてデータベースを検索します。 <code>https://&lt;ISEhost&gt;/ise/mnt/api/Session/MACAddress/&lt;macaddress&gt;</code> (注) XX:XX:XX:XX:XX:XX は MAC アドレス形式です。大文字と小文字は区別されません（例：0a: 0B: 0c: 0D: 0e: 0F）。 (注) MAC アドレスは、監視対象の正しいセッションを検索する唯一の一意のキーとして機能します。MAC アドレスの検索のベースとすることが可能なアクティブなすべてのセッションと MAC アドレスをリストするには <b>ActiveList</b> API コールを使用します。
<ul style="list-style-type: none"> <li>ユーザ名セッション検索</li> </ul>	指定したユーザ名を含む最新のセッションについてデータベースを検索します。 <code>https://&lt;ISEhost&gt;/ise/mnt/api/Session/UserName/&lt;username&gt;</code> (注) ユーザ名は、ネットワーク ユーザ名に使用しているのと同じ Cisco ISE パスワード ポリシーに準拠している必要があります。REST API の唯一の無効な文字はバックスラッシュ (/) 文字です。詳細については、『 <a href="#">Cisco Identity Services Engine User Guide, Release 1.1.1</a> 』の「User Password Policy」を参照してください。
<ul style="list-style-type: none"> <li>NAS IP アドレスセッションの検索</li> </ul>	指定した NAS IP アドレスを含む最新のセッションについてデータベースを検索します。 <code>https://&lt;ISEhost&gt;/ise/mnt/api/Session/IPAddress/&lt;nasipaddress&gt;</code> (注) xxx.xxx.xxx.xxx は NAS IP アドレス形式（例：10.10.10.10）です。

セッション管理用の Cisco ISE クエリー API コールの詳細については、第 2 章「セッション管理のためのクエリー API の使用」を参照してください。

表 1-2 Cisco ISE クエリー API コール : トラブルシューティング

Cisco ISE API コール カテゴリ	Cisco ISE API コールの説明と例
クエリー : トラブルシューティング	
ノードのバージョンとタイプの取得	
<ul style="list-style-type: none"> <li>ノードのバージョンとタイプ</li> </ul>	<p>ノードのバージョンおよびタイプをリストします。</p> <p><i>https://&lt;ISEhost&gt;/ise/mnt/api/Version</i></p> <p>ノードのタイプは、次の値 (0 ~ 3) のいずれかです。</p> <p>STAND_ALONE_MNT_NODE = 0  ACTIVE_MNT_NODE = 1  STAND_BY_MNT_NODE = 2  NOT_AN_MNT_NODE = 3</p> <p>(注) STAND_ALONE_MNT_NODE は、分散展開の一部としてではなく機能する Cisco Monitoring ISE ノードであることを意味します。</p> <p>ACTIVE_MNT_NODE は、分散展開におけるプライマリ - セカンダリ関係のプライマリ ノードであることを意味します。</p> <p>STAND_BY_MNT_NODE は、この同じタイプの展開におけるプライマリ - セカンダリ関係のセカンダリ ノードであることを意味します。</p> <p>NOT_AN_MNT_NODE は、Cisco Monitoring ISE ノードではないことを意味します。サポート対象の ISE ノードおよびペルソナの詳細については、『<i>Cisco Identity Services Engine User Guide, Release 1.1.1</i>』を参照してください。</p>

表 1-2 Cisco ISE クエリー API コール：トラブルシューティング（続き）

Cisco ISE API コール カテゴリ	Cisco ISE API コールの説明と例
<b>障害理由マッピングの取得</b>	
<ul style="list-style-type: none"> <li>障害理由</li> </ul>	<p>障害の理由をリストします。</p> <p><code>https://&lt;ISEhost&gt;/ise/mnt/api/FailureReasons</code></p> <p>各障害理由は、次の例に示すように、エラーコード (failureReason id)、簡単な説明 (code)、障害理由 (cause)、および可能な対処 (resolution) を表示します。</p> <pre>&lt;failureReason id="100009"&gt; &lt;code&gt; 100009 WEBAUTH_FAIL &lt;cause&gt; This may or may not be indicating a violation. &lt;resolution&gt; Please review and resolve this issue according to your organization's policy.</pre> <p><b>(注)</b> FailureReasons API コールの設計用途は、Monitoring ISE ノードから情報を収集するために一度だけ呼び出す必要がある場合に対処するものです。使用しているファイルシステムまたはデータベースに、返された障害理由の内容を保存する必要があります。これらの API コールの返信内容はあくまでも参照用に使用することを目的としています。認証中に問題が発生した場合、認証応答で提供される障害理由コードと、ユーザのファイルシステムまたはデータベースに保存している障害理由のリストと比較する必要があります。</p> <p>Cisco ISE 障害理由の完全なリストについては、<a href="#">付録 A 「Cisco ISE Failure Reasons Editor の使用」</a> を参照してください。</p>
<b>セッションの認証ステータスの取得</b>	
<ul style="list-style-type: none"> <li>セッションの認証ステータス</li> </ul>	<p>すべてのセッションの認証ステータスをリストします。</p> <p><code>https://&lt;ISEhost&gt;/ise/mnt/api/AuthStatus/MACAddress/&lt;macaddress&gt;/&lt;numberofseconds&gt;/&lt;numberofrecordspermacaddress&gt;/All</code></p> <p><b>(注)</b> seconds パラメータ &lt;numberofseconds&gt; は、最短 0 秒から最長 432000 秒 (5 日) の範囲でユーザが設定できます。</p> <p><b>(注)</b> 認証ステータスは、すべてのデータ フィールドが RADIUS_AUTH テーブルで使用可能なときに定義されます。</p>
<b>セッション アカウンティング ステータスの取得</b>	
<ul style="list-style-type: none"> <li>アカウンティングセッションステータス</li> </ul>	<p>特定の期間内のすべてのセッションのアカウンティングステータスを示します。</p> <p><code>https://&lt;ISEhost&gt;/ise/mnt/api/Session/AcctStatusTT/MACAddress/&lt;macaddress&gt;/&lt;numberofseconds&gt;</code></p> <p><b>(注)</b> seconds パラメータ &lt;numberofseconds&gt; は、最短 0 秒から最長 432000 秒 (5 日) の範囲でユーザが設定できます。</p>

トラブルシューティング用の Cisco ISE クエリー API コールの詳細については、[第 2 章 「セッション管理のためのクエリー API の使用」](#) を参照してください。

表 1-3 Cisco ISE 認可変更 API コール

Cisco ISE API コール カテゴリ	Cisco ISE API コールの説明と例
CoA セッション管理	
セッション再認証	
<ul style="list-style-type: none"> <li>セッション再認証タイプ</li> </ul>	<p>セッション再認証コマンドとタイプを送信します。</p> <pre>https://&lt;ISEhost&gt;/ise/mnt/api/CoA/Reauth/&lt;serverhostname&gt;/&lt;macaddress&gt;/&lt;reauthtype&gt;/&lt;nasipaddress&gt;/&lt;destinationipaddress&gt;</pre> <p>再認証タイプは次の値 (0 ~ 2) のいずれかです。  REAUTH_TYPE_DEFAULT = 0  REAUTH_TYPE_LAST = 1  REAUTH_TYPE_RERUN = 2</p> <p><b>(注)</b> NAS IP アドレスが不明な場合は、この時点までに必要な値を入力できます。API はこれらの値を検索クエリーに使用します。ただし、この API コールを実行するには、MAC アドレスを知っている必要があります。</p> <p>この API コールは、CoA をリモートで実行する要求を送信する Monitoring ISE ノードでしか実行できません。Administration ISE ノードは、これらの CoA API コールの実行には関係ないか、必要がありません。</p>
セッション切断	
<ul style="list-style-type: none"> <li>セッション切断タイプ</li> </ul>	<p>セッション切断コマンドおよびポート オプション タイプを送信します。</p> <pre>https://&lt;ISEhost&gt;/ise/mnt/api/CoA/Disconnect/&lt;serverhostname&gt;/&lt;macaddress&gt;/&lt;disconnecttype&gt;/&lt;nasipaddress&gt;/&lt;destinationipaddress&gt;</pre> <p><b>(注)</b> ポート オプション タイプは次の値 (0 ~ 2) のいずれかです。  DYNAMIC_AUTHZ_PORT_DEFAULT = 0  DYNAMIC_AUTHZ_PORT_BOUNCE = 1  DYNAMIC_AUTHZ_PORT_SHUTDOWN = 2</p> <p><b>(注)</b> NAS IP アドレスが不明な場合は、この時点までに必要な値を入力します。API はこれらの値を検索クエリーに使用します。ただし、この API コールを実行するには、MAC アドレスを知っている必要があります。</p>

Cisco ISE 認可変更 API コールに関する詳細については、[第 4 章「認可変更 REST API の使用」](#)を参照してください。

## HTTP PUT を使用したサポート対象の API コール

表 1-2 のセッションの認証ステータス取得 API コールと同様に、クライアントがアカウント ステータスを取得できるようにする REST API 実装の HTTP PUT バージョンがあります。REST API は、HTTP GET コールについて記述したこのマニュアルの例で示すように、HTTP PUT と HTTP GET の両方のコールをサポートします。HTTP PUT のバージョンは、パラメータの入力が必要な API の必要性に対処します。次のスキーマ ファイルの例は、アカウント ステータスの要求です。

```
<?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>
```







## CHAPTER 2

# セッション管理のためのクエリー API の使用

この章では、Cisco ISE のこのリリースでサポートされる次の個々のセッション管理 REST API コールを使用する方法について例をあげながら説明します。セッション管理 API コールは、Cisco ISE 展開において、Cisco Monitoring ISE ノード内から重要なセッション関連の情報を取得する手段を提供します。

次の項では、API の出力スキーマ ファイルの例、各 API コール発行の手順、および各 API コールによって返されるデータのサンプルについて説明します。

- 「セッション カウンタ API コールの使用」 (P.2-1)
- 「単純なセッション リスト API コールの使用」 (P.2-5)
- 「詳細なセッション属性 API コールの使用」 (P.2-11)
- 「古いセッションの削除」 (P.2-28)

## セッション カウンタ API コールの使用

次のセッション カウンタ API コールによって、Cisco ISE 展開におけるターゲット Cisco Monitoring ISE ノードのセッション関連情報の現在のカウントをすぐに収集できるようになります。

- アクティブ セッション (ActiveCount)
- ポスチャ セッション (PostureCount)
- プロファイラ セッション (ProfilerCount)

## アクティブ セッション カウンタ

現在アクティブなすべてのセッション カウントを取得するために ActiveCount API コールを使用できます。ここでは、スキーマ ファイルの出力例、ActiveCount API コールを呼び出すことにより、すべてのアクティブ セッションをカウントする手順、この API コール発行後に返されるアクティブ セッション データのサンプルについて説明します。

## ActiveCount API の出力スキーマ

このサンプル スキーマ ファイルは、ISE のノードのターゲット Monitoring ペルソナでアクティブ セッションのカウントを取得するための ActiveCount API コールの出力です。

```
<?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>
```


## ActiveCount API コールの呼び出し



(注)

API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**ActiveCount API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。
- たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。
- ```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```
- ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/ <specific-api-call>) に置き換えて、ターゲット ノードの URL アドレス フィールドに ActiveCount API コールを入力します。
- ```
https://acme123/ise/mnt/api/Session/ActiveCount
```
-  (注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、ターゲット Cisco Monitoring ISE ノードを表します。
- ステップ 3** Enter キーを押して API コールを発行します。

## ActiveCount API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで ActiveCount API コールを呼び出すときに返されるデータ (アクティブ セッション数) を示します。

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>
```

## ポスチャ セッションカウンタ

現在アクティブなすべてのポスチャセッションの現在のカウントを取得するために PostureCount API コールを使用できます。ここでは、スキーマファイルの出力例、PostureCount API コールを呼び出すことにより、現在のすべてのアクティブポスチャセッションをカウントする手順、この API コール発行後に返されるポスチャセッションデータのサンプルについて説明します。

### PostureCount API の出力スキーマ

このサンプルスキーマファイルは、ターゲット Cisco Monitoring ISE ノードで現在アクティブなポスチャセッションのカウントを取得するための PostureCount API コールの出力です。

```
<?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>
```

### PostureCount API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2)を参照してください。

**PostureCount API コールを発行するには、次の手順を実行します。**

**ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

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

**ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/Session/<specific-api-call>) に置き換えて、ターゲット ノードの URL アドレス フィールドに PostureCount API コールを入力します。

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



(注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、ターゲット Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。

## PostureCount API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで PostureCount API コールを呼び出すときに返されるデータ（現在アクティブなポスチャセッション数）を示します。

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>
```

## プロファイラ セッション カウンタ

現在アクティブなすべてのプロファイラセッションカウントを取得するために ProfilerCount API コールを使用できます。ここでは、スキーマ ファイルの出力例、ProfilerCount API コールを呼び出すことにより、現在のすべてのアクティブ プロファイラセッションをカウントする手順、この API コール発行後に返されるプロファイラセッションデータのサンプルについて説明します。

## ProfilerCount API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードで現在アクティブなプロファイラセッションのカウントを取得するための ProfilerCount API コールの出力です。

```
<?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>
```

## ProfilerCount API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**ProfilerCount API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。
- たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。
- ```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```

**ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/Session/<specific-api-call>) に置き換えて、ターゲット ノードの URL アドレス フィールドに ProfilerCount API コールを入力します。

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



**(注)** これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。

## ProfilerCount API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで ProfilerCount API コールを呼び出すときに返されるデータ（現在アクティブなプロファイラセッション数）を示します。

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>
```

## 単純なセッション リスト API コールの使用

次の単純なセッション リスト API コールによって、Cisco ISE 展開におけるターゲット Cisco Monitoring ISE ノードの現在のアクティブセッションに関連付けられた MAC アドレス、ネットワーク アクセス スイッチ (NAS) の IP アドレス、ユーザ名、セッション ID などのセッション関連の情報をすぐに収集できるようになります。

- アクティブなセッション リスト (ActiveList)
- 認証セッション リスト (AuthList)

## アクティブなセッション リスト

現在アクティブなすべてのセッションをリストするには ActiveList API 呼び出しを使用できます。ここでは、スキーマ ファイルの出力例、ActiveList API コールを呼び出すことにより、すべてのアクティブセッションをリストする手順、この API コール発行後に返されるアクティブセッション関連のデータのサンプルについて説明します。



**(注)** Cisco ISE のこのリリースでは、アクティブな認証済みエンドポイントセッションの表示可能な最大数は、100,000 に制限されています。

## ActiveList API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードで現在アクティブなセッション（およびセッション関連情報）のリストを取得するための ActiveList API コールの出力です。

```
<?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>
```

## ActiveList API コールの呼び出し



(注)

API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**ActiveList API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。
- たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。
- ```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```
- ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/Session/<specific-api-call>) に置き換えて、ターゲット ノードの URL アドレス フィールドに ActiveList API コールを入力します。
- ```
https://acme123/ise/mnt/api/Session/ActiveList
```



(注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API 呼び出しを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。

## ActiveList API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで ActiveList API コールを呼び出すときにアクティブセッションのリストから返されるセッション関連データを示します。

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>
```

## 認証セッション リスト

現在アクティブなすべての認証セッションのリストを取得するために AuthList API コールを使用できます。ここでは、スキーマ ファイルの出力例、AuthList API コールを呼び出すことにより、現在のすべてのアクティブな認証セッションをリストする手順、この API コール発行後に返されるアクティブな認証セッションのサンプルについて説明します。



(注) Cisco ISE のこのリリースでは、アクティブな認証済みエンドポイント セッションの表示可能な最大数は、100,000 に制限されています。

## AuthList API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードでの、指定した期間内（または「null/null」パラメータを使用して期間を指定しない場合）現在アクティブなすべての認証セッションのリストを取得するための AuthList API コールの出力です。

```
<?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>
```

## AuthList API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。



**AuthList API コールを発行するには、次の手順を実行します。**

**ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が `acme123` の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

**ステップ 2** `https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash`  
「/admin/」コンポーネントを API コールのコンポーネント (`/ise/mnt/api/Session/<specific-api-call>`) に置き換えて、ターゲット ノードの URL アドレス フィールドに AuthList API コールを入力します。



**(注)** 次の 2 種類の例では、定義済みの開始時刻パラメータおよび `null` パラメータを使用し、開始時刻以降に認証された現在アクティブなセッションのリストを表示します。2 番目の例は、現在アクティブなすべての認証済みセッションのリストを表示する「`null/null`」パラメータを使用します。この API コールに対する 4 種類のパラメータ設定の例については、「[AuthList API コールから返されるサンプル データ](#)」(P.2-9) を参照してください。

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

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



**(注)** これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「`mnt`」の使用は、Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。

## AuthList API コールから返されるサンプル データ

次に、サポートされているパラメータ オプションの 1 つを使用して、ターゲット Cisco Monitoring ISE ノードで AuthList API コールを呼び出すときに返される、現在アクティブな認証済みセッションのリストを示します。

### null/null オプションの使用

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>

```

### endtime/null オプションの使用

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>0acb6b0c000001F4D08085A</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>

```

### null/starttime オプションの使用

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>0acb6b0c000001F4D08085A</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>
```

### starttime/endtime オプションの使用

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>
```

## 詳細なセッション属性 API コールの使用

次の詳細なセッション属性 API コールによって、次のようなキー情報の最新のセッションをすぐに検索することができますようになります。

- MAC アドレス セッションの検索 (MACAddress)
- ユーザ名のセッションの検索 (UserName)
- NAS IP アドレス セッションの検索 (ターゲット Monitoring ISE ノードに関連付けられた IP アドレス)
- エンドポイントの IP アドレスのセッションの検索 (EndPointIPAddress)

## MAC アドレス セッションの検索

現在のアクティブなセッションから指定された MAC アドレスを取得するために MACAddress API コールを使用できます。ここでは、スキーマ ファイルの出力例、MACAddress API コールを呼び出すことより、指定された MAC アドレスが含まれる最新のアクティブ セッションに対応するノード データベースを検索する手順、API コールの後に返された MAC アドレス関連データのサンプルについて説明します。この API コールは、ノード データベース テーブルから供給されるさまざまなセッション関連の情報をリストします。

### MACAddress API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードで現在アクティブなセッションから指定された MAC アドレスを取得するための MACAddress API コールの出力です。

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

```
<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>
```

## MACAddress API コールの呼び出し



- (注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**MACAddress API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

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

- ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/<specific-api-call>/<macaddress>) に置き換えて、ターゲット ノードの URL アドレスフィールドに MACAddress API コールを入力します。

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



- (注) XX:XX:XX:XX:XX:XX 形式を使用して MAC アドレスを指定していることを確認します。



- (注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレスフィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

- ステップ 3** Enter キーを押して API コールを発行します。

## MACAddress API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで ActiveList API コールを呼び出すときにアクティブセッションのリストから返されるセッション関連データを示します。

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>

```

## ユーザ名のセッションの検索

現在のアクティブなセッションから指定されたユーザ名を取得するために `UserName` API コールを使用できます。ここでは、スキーマ ファイルの出力例、`UserName` API コールを呼び出すことより、指定されたユーザ名が含まれる最新のアクティブセッションに対応するノードデータベースを検索する手順、API コールの後に返されたユーザ名関連データのサンプルについて説明します。この API は、ノードデータベース テーブルから供給されるさまざまなセッション関連の情報をリストします。

### UserName API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット `Cisco Monitoring ISE` ノードで現在アクティブなセッションから指定されたユーザ名を取得するための `UserName` API コールの出力です。

```

<?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:sequence>
  </xs:complexType>

```



```
<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>

```

## UserName API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**UserName API コールを発行するには、次の手順を実行します。**

**ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

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

**ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/<specific-api-call>/<username>) に置き換えて、ターゲット ノードの URL アドレスフィールドに UserName API コールを入力します。

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



(注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。

## UserName API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで UserName API コールを呼び出すときにアクティブセッションのリストから返されるセッション関連データを示します。

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
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>

```

## NAS IP アドレス セッションの検索

現在のセッションから指定された NAS IP アドレスを取得するために IPAddress API コールを使用できます。ここでは、スキーマ ファイルの出力例、IPAddress API コールを呼び出すことより、指定された NAS IP アドレスが含まれる最新のアクティブセッションに対応するノードデータベースを検索する手順、API コールの後に返された NAS IP アドレス関連データのサンプルについて説明します。この API は、ノードデータベース テーブルから供給されるさまざまなセッション関連の情報をリストします。

### IPAddress API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードで現在アクティブなセッションから指定された NAS IP アドレスを取得するための IPAddress API コールの出力です。

```

<?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:sequence>
  </xs:complexType>

```

```
<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>

```

## NAS IPAddress API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**NAS IPAddress API コールを発行するには、次の手順を実行します。**

**ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

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

**ステップ 2** 「/admin/」 コンポーネントを API コールのコンポーネント (/ise/mnt/api/<specific-api-call>/<nasipaddress>) に置き換えて、ターゲット ノードの URL アドレスフィールドに IPAddress API コールを入力します。

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



(注) xxx.xxx.xxx.xxx の形式を使用して NAS IP アドレスを指定していることを確認します。



(注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレスフィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。

## IPAddress API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで IPAddress API コールを呼び出すときにアクティブセッションのリストから返されるセッション関連データを示します。

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=ipepvpnuser; 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>ipepvpnuser</acs_username>
<radius_username>ipepvpnuser</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>

```

## エンドポイントの IP アドレスのセッションの検索

現在のアクティブなセッションからセッションディレクトリ情報を取得するために EndPointIPAddress API コールを使用できます。ここでは、スキーマファイルの出力例、EndPointIPAddress API コールを呼び出すことより、指定された IP アドレスが含まれる最新のアクティブセッションに対応するノードデータベースを検索する手順、API コールの後に返されたエンドポイント関連データのサンプルについて説明します。この API コールは、ノードデータベーステーブルから供給されるさまざまなセッションディレクトリ情報をリストします。

### EndPointIPAddress API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードで現在アクティブなセッションから指定されたエンドポイントに関するセッションディレクトリ情報を取得するための EndPointIPAddress API コールの出力です。

```

<?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>

```

## EndPointIPAddress API コールの呼び出し



- (注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**EndPointIPAddress API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

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

- ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/Session/EndPointIPAddress/<endpoint\_ip>) に置き換えて、ターゲット ノードの URL アドレス フィールドに EndPointIPAddress API コールを入力します。

```
https://acme123/ise/mnt/api/Session/EndPointIPAddress/A.B.C.D
```



- (注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

- ステップ 3** Enter キーを押して API コールを発行します。

## EndPointIPAddress API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで EndPointIPAddress API コールを呼び出すときにアクティブセッションのリストから返されるセッション関連データを示します。

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>00:0C:29:95:A5:C1</user_name>
<nas_ip_address>10.77.152.139</nas_ip_address>
<calling_station_id>00:0C:29:95:A5:C1</calling_station_id>
<nas_port>50109</nas_port>

```

```

<identity_group>RegisteredDevices</identity_group>
<network_device_name>switch</network_device_name>
<acs_server>ise248</acs_server>
<authen_protocol>Lookup</authen_protocol>
<framed_ip_address>10.20.40.10</framed_ip_address>
-
<network_device_groups>
Device Type#All Device Types,Location#All Locations
</network_device_groups>
<access_service>RADIUS</access_service>
<auth_acs_timestamp>2012-03-13T17:02:22.169+05:30</auth_acs_timestamp>
<authentication_method>mab</authentication_method>
-
<execution_steps>
11001,11017,11027,15008,15048,15048,15004,15041,15006,15013,24209,24211,22037,15036,15048,
15004,15016,11022,11002
</execution_steps>
<audit_session_id>0A4D988B000000E337B8D983</audit_session_id>
<nas_port_id>GigabitEthernet1/0/9</nas_port_id>
<nac_policy_compliance>Pending</nac_policy_compliance>
<auth_id>1331101769985927</auth_id>
<auth_acsview_timestamp>2012-03-13T17:02:22.171+05:30</auth_acsview_timestamp>
<message_code>5200</message_code>
<acs_session_id>ise248/120476308/97</acs_session_id>
<service_selection_policy>MAB</service_selection_policy>
<authorization_policy>wired_redirect</authorization_policy>
<identity_store>Internal Endpoints</identity_store>
-
<response>
{UserName=00:0C:29:95:A5:C1; User-Name=00-0C-29-95-A5-C1;
State=ReauthSession:0A4D988B000000E337B8D983;
Class=CACS:0A4D988B000000E337B8D983:ise248/120476308/97;
Termination-Action=RADIUS-Request; Tunnel-Type=(tag=1) VLAN; Tunnel-Medium-Type=(tag=1)
802; Tunnel-Private-Group-ID=(tag=1) 30;
cisco-av-pair=url-redirect-acl=ACL-WEBAUTH-REDIRECT;
cisco-av-pair=url-redirect=https://ise248.cisco.com:8443/guestportal/gateway?sessionId=0A4
D988B000000E337B8D983&action=cwa;
cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-cwa_wired-4f570619;
cisco-av-pair=profile-name=WindowsXP-Workstation; }
</response>
<service_type>Call Check</service_type>
<use_case>Host Lookup</use_case>
<cisco_av_pair>audit-session-id=0A4D988B000000E337B8D983</cisco_av_pair>
<acs_username>00:0C:29:95:A5:C1</acs_username>
<radius_username>00:0C:29:95:A5:C1</radius_username>
<selected_identity_store>Internal Endpoints</selected_identity_store>
<authentication_identity_store>Internal Endpoints</authentication_identity_store>
<identity_policy_matched_rule>Default</identity_policy_matched_rule>
<nas_port_type>Ethernet</nas_port_type>
<selected_azn_profiles>wired_cwa_redirect</selected_azn_profiles>
<response_time>17</response_time>
<destination_ip_address>10.77.152.248</destination_ip_address>
-
<other_attributes>
ConfigVersionId=15, DestinationPort=1812, Protocol=Radius, Framed-MTU=1500, EAP-Key-Name=, cisc
o-nas-port=GigabitEthernet1/0/9, CPMSessionID=0A4D988B000000E337B8D983, EndPointMACAddress=0
0-0C-29-95-A5-C1, EndPointMatchedProfile=WindowsXP-Workstation, HostIdentityGroup=Endpoint
Identity Groups:RegisteredDevices, Device Type=Device Type#All Device
Types, Location=Location#All Locations, Device IP
Address=10.77.152.139, Called-Station-ID=EC:C8:82:55:2E:09
</other_attributes>
<acct_id>1331101769985928</acct_id>
<acct_acs_timestamp>2012-03-13T17:02:22.365+05:30</acct_acs_timestamp>
<acct_acsview_timestamp>2012-03-13T17:02:22.366+05:30</acct_acsview_timestamp>

```

```
<acct_session_id>000000FC</acct_session_id>
<acct_status_type>Interim-Update</acct_status_type>
<acct_session_time>16411</acct_session_time>
<acct_input_octets>3053882</acct_input_octets>
<acct_output_octets>2633472</acct_output_octets>
<acct_input_packets>20166</acct_input_packets>
<acct_output_packets>20297</acct_output_packets>
<acct_class>CACS:0A4D988B000000E337B8D983:ise248/120476308/97</acct_class>
<acct_delay_time>0</acct_delay_time>
<started xsi:type="xs:boolean">>false</started>
<stopped xsi:type="xs:boolean">>false</stopped>
<vlan>30</vlan>
<dacl>#ACSACL#-IP-cwa_wired-4f570619</dacl>
<endpoint_policy>WindowsXP-Workstation</endpoint_policy>
</sessionParameters>
```

## 古いセッションの削除

一部のデバイスでは、Wireless LAN Controller (WLC) など、古いセッションを保持できるようにする場合があります。このような場合、手動で非アクティブなセッションを削除するには、HTTP **DELETE** API コールを使用できます。これを行うには、URL (HTTP、HTTPS) 構文のデータを転送するための無償のサードパーティ製のコマンドラインツールである **cURL** を使用します。



(注)

HTTP および HTTPS を使用してファイルを取得するための無償ユーティリティである GNU Wget は、HTTP **DELETE** API コールをサポートしません。

古いセッションを削除するには、次の手順を実行します。

**ステップ 1** コマンドラインからターゲット Cisco Monitoring ISE ノードにログインします。



(注) API コールは大文字と小文字が区別され、慎重に入力する必要があります。変数 `<mntnode>` は Cisco Monitoring ISE ノードを表します。

**ステップ 2** 手動で MAC アドレスの古いセッションを削除するには、コマンドラインで次の API コールを発行します。

```
curl -X DELETE https://<mntnode>/ise/mnt/api/Session/Delete/MACAddress/<madaddress>
```

**ステップ 3** 手動でセッション ID の古いセッションを削除するには、コマンドラインで次の API コールを発行します。

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

**ステップ 4** 手動ですべてのセッションを削除するには、コマンドラインで次の API コールを発行します。

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



## CHAPTER 3

# トラブルシューティング用のクエリー API の使用

この章では、このリリースでサポートされている個々の Cisco Prime Network Control System (NCS) REST API コールを使用する方法について説明します。Cisco Prime NCS API コールはノードのバージョンおよびタイプ、障害の理由、認証ステータスとアカウント ステータスを含むターゲット Cisco Monitoring ISE ノードのセッションに関する主要なトラブルシューティング情報を取得するためのメカニズムを提供します。

次の項では、クエリー API コールを使用して取得してトラブルシューティング情報を提供します。この情報の形式は、出力スキーマ ファイルの例、各 API コールの発行の手順、各 API コールによって返されるデータのサンプルです：

- 「クエリー API を使用した Cisco ISE のトラブルシューティング」 (P.3-1)
- 「ノードのバージョンおよびタイプの API コール」 (P.3-2)
- 「障害理由 API コール」 (P.3-3)
- 「認証ステータス API コール」 (P.3-7)
- 「アカウント ステータス API コール」 (P.3-15)

## クエリー API を使用した Cisco ISE のトラブルシューティング

次の項では、Cisco ISE 展開で指定したターゲット Cisco Monitoring ISE ノードにステータス要求を送信し、次の診断関連情報を取得する主要な Cisco Prime NCS トラブルシューティング API コールを提供します。

- ノードのバージョンおよびタイプ (Version API コールを使用)
- 障害理由 (FailureReasons API コールを使用)
- 認証ステータス (AuthStatus API コールを使用)
- アカウンティング ステータス (AcctStatus API コールを使用)

## ノードのバージョンおよびタイプの API コール

各ノードの RETS Programmatic インターフェイス (PI) サービスとクレデンシャルをテストするには Version API コールを使用できます。ここでは、スキーマ ファイルの出力例、この API コールを呼び出すことにより、Cisco ISE ソフトウェアのバージョンおよびノードタイプを要求する手順、この API コール発行後に返されるノードのバージョンとタイプのサンプルについて説明します。

ノードタイプは次のいずれかになります。

- STANDALONE\_MNT\_NODE = 0
- ACTIVE\_MNT\_NODE = 1
- BACKUP\_MNT\_NODE = 2
- NOT\_AN\_MNT\_NODE = 3

## バージョン API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードへの送信後の、バージョン API コールの出力です。

```
<?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="product" type="product"/>

  <xs:complexType name="product">
    <xs:sequence>
      <xs:element name="version" type="xs:string" minOccurs="0"/>
      <xs:element name="type_of_node" type="xs:int"/>
    </xs:sequence>
    <xs:attribute name="name" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

## バージョン API コールの呼び出し



**(注)** API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

バージョン API コールを発行するには、次の手順を実行します。

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。
- たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。
- ```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```
- ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/ <specific-api-call>) に置き換えて、ターゲット ノードの URL アドレス フィールドにバージョン API コールを入力します。
- ```
https://acme123/ise/mnt/api/Version
```



(注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

ステップ 3 Enter キーを押して API コールを発行します。

## バージョン API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードでバージョン API コールを呼び出すときに返されるデータを示します。この API コールでは、ターゲット ノードについて次の 2 種類の値が返されます。

- ノードのバージョン (この例では、1.0.3.032 を表示します)。
- Cisco Monitoring ISE ノードのタイプ (この例では、アクティブな Cisco Monitoring ISE ノードが 1 つであることを意味する「1」を表示します)。

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

```
-
<product name="Cisco Identity Services Engine">
<version>1.0.3.032</version>
<type_of_node>1</type_of_node>
</product>
```

## 障害理由 API コール

ターゲット ノードで行われた認証ステータスのチェックで返された障害理由のリストを返すために FailureReasons API コールを使用できます。ここでは、スキーマ ファイルの出力例、この API コールを呼び出すことにより、Cisco Monitoring ISE ノードで記録される障害理由のリストを要求する手順、この API コール発行後に返される障害理由のサンプルについて説明します。返される障害理由には、それぞれ表 3-1 に示す次の要素で構成されます。



(注) Cisco ISE Failure Reasons Editor を使用して障害理由の完全なリストにアクセスする方法に関する詳細については、「[Cisco ISE Failure Reasons Editor の使用](#)」(P.A-1) を参照してください。

表 3-1 Cisco Identity Services Engine の製品マニュアル

障害理由の要素	例
障害理由 ID	<failureReason id="11011">
コード	<11011 RADIUS listener failed>
原因	<Could not open one or more of the ports used to receive RADIUS requests>
解決策	<Ensure that the ports 1812, 1813, 1645 and 1646 are not being used by another process on the system>



(注) Cisco ISE ユーザ インターフェイスを使用して ([ モニタ (Monitor) ] > [ レポート (Reports) ] > [ カタログ (Catalog) ] > [ 障害理由 (Failure Reasons) ]) をクリックして) 障害理由レポートがあるかどうかを確認します。障害理由レポートが表示されます。

## FailureReasons API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードへの要求の送信後の、FailureReasons API コールの出力です。

```
<?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="failureReasonList" type="failureReasonList"/>

  <xs:complexType name="failureReasonList">
    <xs:sequence>
      <xs:element name="failureReason" type="failureReason" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="failureReason">
    <xs:sequence>
      <xs:element name="code" type="xs:string" minOccurs="0"/>
      <xs:element name="cause" type="xs:string" minOccurs="0"/>
      <xs:element name="resolution" type="xs:string" minOccurs="0"/>
    </xs:sequence>
    <xs:attribute name="id" type="xs:string"/>
  </xs:complexType>
</xs:schema>
```

## FailureReasons API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**FailureReasons API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。
- たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。
- `https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash`



- ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/ <specific-api-call>) に置き換えて、ターゲットノードの URL アドレス フィールドに FailureReasons API コールを入力します。

https://acme123/ise/mnt/api/FailureReasons



- (注)** これらのコールは、大文字小文字を区別するため、ターゲットノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

- ステップ 3** Enter キーを押して API コールを発行します。

## FailureReasons API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで FailureReasons API コールを呼び出すときに返されるデータを示します。この API コールは、ターゲットノードから障害理由のリストを返します。障害理由は、それぞれ、障害 ID、障害コード、原因、対処法（既知の場合）によって定義されます。



- (注)** 次の FailureReasons API コールの例は、返されるデータの小規模なサンプルを表示しています。

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

```
-
<failureReasonList>
-
<failureReason id="100001">
-
<code>
100001 AUTHMGR-5-FAIL Authorization failed for client
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100002">
-
<code>
100002 AUTHMGR-5-SECURITY_VIOLATION Security violation on the interface
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100003">
-
<code>
100003 AUTHMGR-5-UNAUTHORIZED Interface unauthorized
</code>
<cause>This may or may not be indicating a violation</cause>
-
```

```

<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100004">
-
<code>
100004 DOT1X-5-FAIL Authentication failed for client
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100005">
<code>100005 MAB-5-FAIL Authentication failed for client</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100006">
-
<code>
100006 RADIUS-4-RADIUS_DEAD RADIUS server is not responding
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>
-
<failureReason id="100007">
-
<code>
100007 EPM-6-POLICY_APP_FAILURE Interface ACL not configured
</code>
<cause>This may or may not be indicating a violation</cause>
-
<resolution>
Please review and resolve according to your organization's policy
</resolution>
</failureReason>

```

### 詳細情報

Cisco ISE Failure Reasons Editor の詳細については、[付録 A 「Cisco ISE Failure Reasons Editor の使用」](#) を参照してください。

## 認証ステータス API コール

ターゲット ノードのセッションの認証ステータスをチェックするために AuthStatus API 呼び出しを使用できます。この API コールに関連付けられたクエリーには、一致の検索対象である MAC アドレスが少なくとも 1 つ必要です。指定の MAC アドレスが返されるように、最新レコードに、ユーザ設定が可能な制限を付けます。

ここでは、スキーマ ファイルの出力例、この API コールを呼び出すことにより、ターゲットのモニタリング モードでセッション認証のステータスを検索する要求を送信する手順、この API コール発行後に返されるデータのサンプルについて説明します。

AuthStatus API コールにより、次の検索関連パラメータを設定できるようになります。

- **期間** : 指定された MAC アドレスに関連付けられた認証ステータス レコードの検索と取得が試行される秒数を定義します。ユーザが設定可能な値の有効範囲は 1 ~ 864000 秒 (10 日) です。0 秒の値を入力した場合は、デフォルト期間の 10 日を指定します。
- **レコード** : MAC アドレスごとに検索するセッションのレコード数を定義します。ユーザが設定可能な値の有効範囲は 1 ~ 500 レコードです。0 を入力した場合は、デフォルト設定の 200 レコードを指定します。



**(注)** 期間およびレコード パラメータの両方に値 0 を指定すると、この API コールは、指定された MAC アドレスに関連付けられている最新の認証セッション レコードのみを返します。

- **属性** : AuthStatus API コールを使用して認証ステータスの検索で返された認証ステータスのテーブルの属性数を定義します。有効な値は 0 (デフォルト)、All、または user\_name+acs\_timestamp です (AuthStatus スキーマの例「AcctStatus API の出力スキーマ」(P.3-15) を参照)。
  - 「0」を入力すると、表 3-2 で定義された属性が返されます。これらは出力スキーマの restAuthStatus のセクションに記載されています。
  - 「All」を入力すると、より詳しい属性セットが返されます。これらは出力スキーマの fullRESTAuthStatus のセクションに記載されています。
  - user\_name+acs\_timestamp のスキーマに示されている値を入力すると、それらの属性だけが返されます。user\_name 属性と acs\_timestamp 属性は、出力スキーマ restAuthStatus のセクションに記載されています。

表 3-2 認証ステータス テーブルの属性

属性	説明
name="passed"	2 種類の可能な認証ステータスの結果の 1 つが: <ul style="list-style-type: none"> <li>• 合格</li> </ul>
name="failed"	2 種類の可能な認証ステータスの結果の 1 つが: <ul style="list-style-type: none"> <li>• 不合格</li> </ul>
name="user_name"	ユーザ名
name="nas_ip_address"	ネットワーク アクセス スイッチの IP アドレス / ホスト名
name="failure_reason"	セッション認証エラーの原因
name="calling_station_id"	ソース IP アドレス
name="nas_port"	ネットワーク アクセス サーバのポート
name="identity_group"	関係ユーザおよびホストからなる論理グループ
name="network_device_name"	ネットワーク デバイス名

表 3-2 認証ステータス テーブルの属性 (続き)

属性	説明
name="acs_server"	Cisco ISE アプライアンス名
name="eap_authentication"	認証要求に使用される拡張認証プロトコル (EAP) メソッド
name="framed_ip_address"	指定ユーザに設定されるアドレス
network_device_groups"	関係ネットワーク デバイスからなる論理グループ
name="access_service"	適用されたアクセス サービス
name="acs_timestamp"	Cisco ISE 認証要求に関連付けられたタイム スタンプ
name="authentication_method"	認証に使用されるメソッドを識別する
name="execution_steps"	要求の処理中にロギングされる各診断メッセージのメッセージコードリスト
name="radius_response"	RADIUS 応答のタイプ (VLAN や ACL など)
name="audit_session_id"	認証セッションの ID
name="nas_identifier"	特定のリソースに関連付けられたネットワーク アクセス サーバ (NAS)
name="nas_port_id"	使用された NAS ポートの ID
name="nac_policy_compliance"	ポスチャの状態を反映する (準拠、または非準拠)
name="selected_azn_profiles"	承認に使用されたプロファイルを識別する
name="service_type"	フレームド ユーザを表す
name="eap_tunnel"	EAP 認証に使用されるトンネルまたは外部メソッド
name="message_code"	処理された要求の結果を定義する監査メッセージの識別子
name="destination_ip_address"	宛先 IP アドレスを識別する

## AuthStatus API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードでの指定されたセッションへの送信後の、AuthStatus API コールの実出力です。

```
<?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="authStatusOutputList" type="fullRESTAuthStatusOutputList"/>

  <xs:complexType name="fullRESTAuthStatusOutputList">
    <xs:sequence>
      <xs:element name="authStatusList" type="fullRESTAuthStatusList" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
```

```

<xs:complexType name="fullRESTAuthStatusList">
  <xs:sequence>
    <xs:element name="authStatusElements" type="fullRESTAuthStatus" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="key" type="xs:string"/>
</xs:complexType>

<xs:complexType name="fullRESTAuthStatus">
  <xs:complexContent>
    <xs:extension base="restAuthStatus">
      <xs:sequence>
        <xs:element name="id" type="xs:long" minOccurs="0"/>
        <xs:element name="acsview_timestamp" type="xs:dateTime" 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="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="sel_exp_azn_profiles" type="xs:string" minOccurs="0"/>
        <xs:element name="selected_query_identity_stores" 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:sequence>
    </xs:extension>
  </xs:complexContent>
</xs:complexType>

<xs:complexType name="restAuthStatus">
  <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:sequence>
</xs:complexType>

```

```

<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="eap_authentication" 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="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_identifer" 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="selected_azn_profiles" type="xs:string" minOccurs="0"/>
<xs:element name="service_type" type="xs:string" minOccurs="0"/>
<xs:element name="eap_tunnel" type="xs:string" minOccurs="0"/>
<xs:element name="message_code" type="xs:string" minOccurs="0"/>
<xs:element name="destination_ip_address" type="xs:string" minOccurs="0"/>
</xs:sequence>
</xs:complexType>
</xs:schema>

```

## AuthStatus API コールの呼び出し



**(注)** API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**AuthStatus API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。
- たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。
- ```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```
- ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/<specific-api-call>/MACAddress/<macaddress>/<seconds>/<numberofrecordspermacaddress>/All) に置き換えて、ターゲット ノードの URL アドレス フィールドに AuthStatus API コールを入力します。
- ```
https://acme123/ise/mnt/api/AuthStatus/MACAddress/00:50:56:10:13:02/120/100/All
```
- (注)** これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。
- ステップ 3** Enter キーを押して API コールを発行します。

## AuthStatus API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで AuthStatus API コールを呼び出すときに返されるデータを示します。

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

```
-
<authStatusOutputList>
-
<authStatusList key="00:25:9C:A3:7D:48">
-
<authStatusElements>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>hareesh6</user_name>
<nas_ip_address>10.203.107.10</nas_ip_address>
<calling_station_id>00:25:9C:A3:7D:48</calling_station_id>
<nas_port>1</nas_port>
<identity_group>iPEP-WLC-Group</identity_group>
<network_device_name>iPEP3</network_device_name>
<acs_server>HAREESH-R6-1-PDP1</acs_server>
<eap_authentication>EAP-MSCHAPv2</eap_authentication>
-
<network_device_groups>
Device Type#All Device Types#iPEP,Location#All Locations
</network_device_groups>
<access_service>Default Network Access</access_service>
<acs_timestamp>2010-12-20T01:38:49.566Z</acs_timestamp>
<authentication_method>MSCHAPV2</authentication_method>
-
<execution_steps>
11001,11017,15008,15048,15048,15004,11507,12500,11006,11001,11018,12101,12100,11006,11001,
11018,12102,12800,12175,12805,12806,12801,12802,12105,11006,11001,11018,12104,12804,12816,
12132,12125,11806,12105,11006,11001,11018,12104,11808,15041,15006,15013,24210,24212,22037,
11824,12105,11006,11001,11018,12104,11810,11814,11519,12128,12105,11006,11001,11018,12104,
12126,12127,15036,15048,15048,15004,15016,12171,12105,11006,11001,11018,12104,12106,11503,
15036,15048,15048,15004,15016,11002
</execution_steps>
<audit_session_id>0acb6b0b0000000D4D0EB3A9</audit_session_id>
<nas_identifier>Cisco_4d:c0:a0</nas_identifier>
<nac_policy_compliance>NotApplicable</nac_policy_compliance>
<selected_azn_profiles>iPEP-Compliant-Authz-Profile</selected_azn_profiles>
<service_type>Framed</service_type>
<eap_tunnel>EAP-FAST</eap_tunnel>
<message_code>5200</message_code>
<destination_ip_address>10.203.107.150</destination_ip_address>
<id>1292549379215912</id>
<acsview_timestamp>2010-12-20T01:38:49.567Z</acsview_timestamp>
<acs_session_id>HAREESH-R6-1-PDP1/81999140/50</acs_session_id>
<service_selection_policy>iPEP-WLC</service_selection_policy>
<authorization_policy>iPEP-WLC-Compliant-Policy</authorization_policy>
<identity_store>Internal Users</identity_store>
-
<response>
{User-Name=hareesh6; State=ReauthSession:0acb6b0b0000000D4D0EB3A9;
Class=CACS:0acb6b0b0000000D4D0EB3A9:HAREESH-R6-1-PDP1/81999140/50;
Termination-Action=RADIUS-Request;
MS-MPPE-Send-Key=04:11:2d:bf:8b:5f:c1:b0:14:b1:73:ad:48:90:65:e0:c2:a3:f7:66:2d:dc:70:f1:a
b:56:cd:09:c4:b0:b7:ae;
MS-MPPE-Recv-Key=7e:38:94:72:e2:a3:8a:e4:90:18:45:61:91:c0:44:ea:0c:21:39:14:2f:7c:9f:55:d
6:52:af:fd:55:48:3f:34; }
```

```

</response>
-
<cisco_av_pair>
audit-session-id=0acb6b0b0000000D4D0EB3A9,ipep-proxy=true
</cisco_av_pair>
<acs_username>hareesh6</acs_username>
<radius_username>anonymous</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>Wireless - IEEE 802.11</nas_port_type>
-
<tunnel_details>
Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0)
208
</tunnel_details>
-
<other_attributes>
ConfigVersionId=18,DestinationPort=1812,Protocol=Radius,Framed-MTU=1300,State=37CPMSession
ID=0acb6b0b0000000D4D0EB3A9;39SessionID=HAREESH-R6-1-PDP1/81999140/50;,Proxy-State=Cisco
Secure
ACS53e5cfac-0a31-11e0-c000-000000000000-2905701264-3372,Airespace-Wlan-Id=2,CPMSessionID=0
acb6b0b00000000D4D0EB3A9,IssuedPacInfo=Issued PAC type=Authorization with expiration time:
Mon Dec 20 02:38:49
2010,CPMSessionID=0acb6b0b0000000D4D0EB3A9,EndPointMACAddress=00-25-9C-A3-7D-48,Device
Type=Device Type#All Device Types#iPEP,Location=Location#All Locations,Model
Name=Unknown,Software Version=Unknown,Device IP
Address=10.203.107.11,Called-Station-ID=00-24-c4-1b-36-70:i pep3
</other_attributes>
<response_time>3</response_time>
</authStatusElements>
-
<authStatusElements>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>hareesh6</user_name>
<nas_ip_address>10.203.107.10</nas_ip_address>
<calling_station_id>00:25:9C:A3:7D:48</calling_station_id>
<nas_port>1</nas_port>
<identity_group>iPEP-WLC-Group</identity_group>
<network_device_name>iPEP3</network_device_name>
<acs_server>HAREESH-R6-1-PDP1</acs_server>
<eap_authentication>EAP-MSCHAPv2</eap_authentication>
-
<network_device_groups>
Device Type#All Device Types#iPEP,Location#All Locations
</network_device_groups>
<access_service>Default Network Access</access_service>
<acs_timestamp>2010-12-19T01:32:39.220Z</acs_timestamp>
<authentication_method>MSCHAPV2</authentication_method>
-
<execution_steps>
11001,11017,15008,15048,15048,15004,11507,12500,11006,11001,11018,12101,12100,11006,11001,
11018,12102,12800,12175,12805,12806,12801,12802,12105,11006,11001,11018,12104,12804,12816,
12132,12125,11806,12105,11006,11001,11018,12104,11808,15041,15006,15013,24210,24212,22037,
11824,12105,11006,11001,11018,12104,11810,11814,11519,12128,12105,11006,11001,11018,12104,
12126,12127,15036,15048,15048,15004,15016,12171,12105,11006,11001,11018,12104,12106,11503,
15036,15048,15048,15004,15016,11002
</execution_steps>
<audit_session_id>0acb6b0b0000000C4D0D60B6</audit_session_id>
<nas_identifier>Cisco_4d:c0:a0</nas_identifier>
<nac_policy_compliance>NotApplicable</nac_policy_compliance>
<selected_azn_profiles>iPEP-Compliant-Authz-Profile</selected_azn_profiles>
<service_type>Framed</service_type>

```



```

<eap_tunnel>EAP-FAST</eap_tunnel>
<message_code>5200</message_code>
<destination_ip_address>10.203.107.150</destination_ip_address>
<id>1292549379206881</id>
<acsview_timestamp>2010-12-19T01:32:39.218Z</acsview_timestamp>
<acs_session_id>HAREESH-R6-1-PDP1/81999140/46</acs_session_id>
<service_selection_policy>iPEP-WLC</service_selection_policy>
<authorization_policy>iPEP-WLC-Compliant-Policy</authorization_policy>
<identity_store>Internal Users</identity_store>
-
<response>
{User-Name=hareesh6; State=ReauthSession:0acb6b0b0000000C4D0D60B6;
Class=CACS:0acb6b0b0000000C4D0D60B6:HAREESH-R6-1-PDP1/81999140/46;
Termination-Action=RADIUS-Request;
MS-MPPE-Send-Key=f0:f4:5d:38:c4:5d:e8:85:51:65:ea:9e:ad:27:9f:c6:50:ae:11:ae:f8:8c:9d:c2:5
c:d3:33:06:36:be:14:79;
MS-MPPE-Recv-Key=d3:4a:2b:e6:6b:f8:31:ef:cc:84:d0:57:96:24:ab:e4:9b:45:3a:43:a7:1a:05:e7:5
d:a0:46:33:02:63:ef:39; }
</response>
-
<cisco_av_pair>
audit-session-id=0acb6b0b0000000C4D0D60B6,ipep-proxy=true
</cisco_av_pair>
<acs_username>hareesh6</acs_username>
<radius_username>anonymous</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>Wireless - IEEE 802.11</nas_port_type>
-
<tunnel_details>
Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0)
208
</tunnel_details>
-
<other_attributes>
ConfigVersionId=18, DestinationPort=1812, Protocol=Radius, Framed-MTU=1300, State=37CPMSession
ID=0acb6b0b0000000C4D0D60B6;39SessionID=HAREESH-R6-1-PDP1/81999140/46;; Proxy-State=Cisco
Secure
ACS53e5cfac-0a31-11e0-c000-000000000000-2905701264-3372, Airespace-Wlan-Id=2, CPMSessionID=0
acb6b0b00000000C4D0D60B6, IssuedPacInfo=Issued PAC type=Authorization with expiration time:
Sun Dec 19 02:32:39
2010, CPMSessionID=0acb6b0b0000000C4D0D60B6, EndPointMACAddress=00-25-9C-A3-7D-48, Device
Type=Device Type#All Device Types#iPEP, Location=Location#All Locations, Model
Name=Unknown, Software Version=Unknown, Device IP
Address=10.203.107.11, Called-Station-ID=00-24-c4-1b-36-70:ipep3
</other_attributes>
<response_time>3</response_time>
</authStatusElements>
-
<authStatusElements>
<passed xsi:type="xs:boolean">true</passed>
<failed xsi:type="xs:boolean">false</failed>
<user_name>hareesh6</user_name>
<nas_ip_address>10.203.107.10</nas_ip_address>
<calling_station_id>00:25:9C:A3:7D:48</calling_station_id>
<nas_port>1</nas_port>
<identity_group>iPEP-WLC-Group</identity_group>
<network_device_name>iPEP3</network_device_name>
<acs_server>HAREESH-R6-1-PDP1</acs_server>
<eap_authentication>EAP-MSCHAPv2</eap_authentication>
-
<network_device_groups>
Device Type#All Device Types#iPEP, Location#All Locations

```

```

</network_device_groups>
<access_service>Default Network Access</access_service>
<acs_timestamp>2010-12-18T01:26:22.089Z</acs_timestamp>
<authentication_method>MSCHAPV2</authentication_method>
-
<execution_steps>
11001,11017,15008,15048,15048,15004,11507,12500,11006,11001,11018,12101,12100,11006,11001,
11018,12102,12800,12805,12806,12807,12810,12105,11006,11001,11018,12104,12812,12804,12801,
12802,12816,12149,12105,11006,11001,11018,12104,12125,11521,12105,11006,11001,11018,12104,
11522,11806,12105,11006,11001,11018,12104,11808,15041,15006,15013,24210,24212,22037,11824,
12105,11006,11001,11018,12104,11810,11814,11519,12128,12105,11006,11001,11018,12104,12126,
12127,15036,15048,15048,15004,15016,12169,12105,11006,11001,11018,12104,12651,12107,11503,
15036,15048,15048,15004,15016,11002
</execution_steps>
<audit_session_id>0acb6b0b0000000B4D0C0DBD</audit_session_id>
<nas_identifier>Cisco_4d:c0:a0</nas_identifier>
<nac_policy_compliance>NotApplicable</nac_policy_compliance>
<selected_azn_profiles>iPEP-Compliant-Authz-Profile</selected_azn_profiles>
<service_type>Framed</service_type>
<eap_tunnel>EAP-FAST</eap_tunnel>
<message_code>5200</message_code>
<destination_ip_address>10.203.107.150</destination_ip_address>
<id>1292549379197803</id>
<acsview_timestamp>2010-12-18T01:26:22.042Z</acsview_timestamp>
<acs_session_id>HAREESH-R6-1-PDP1/81999140/30</acs_session_id>
<service_selection_policy>iPEP-WLC</service_selection_policy>
<authorization_policy>iPEP-WLC-Compliant-Policy</authorization_policy>
<identity_store>Internal Users</identity_store>
-
<response>
{User-Name=hareesh6; State=ReauthSession:0acb6b0b0000000B4D0C0DBD;
Class=CACS:0acb6b0b0000000B4D0C0DBD:HAREESH-R6-1-PDP1/81999140/30;
Termination-Action=RADIUS-Request;
MS-MPPE-Send-Key=d3:94:df:2b:fc:18:12:91:ad:4f:3b:09:d1:76:93:83:21:83:33:3a:14:b9:9b:c0:a
0:81:71:96:95:64:2c:ed;
MS-MPPE-Recv-Key=3b:c2:31:58:81:8a:34:24:d4:55:03:cd:a2:91:85:49:7f:16:36:30:d9:8d:24:a7:5
0:ec:3e:df:7a:85:ea:5c; }
</response>
-
<cisco_av_pair>
audit-session-id=0acb6b0b0000000B4D0C0DBD,ipep-proxy=true
</cisco_av_pair>
<acs_username>hareesh6</acs_username>
<radius_username>anonymous</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>Wireless - IEEE 802.11</nas_port_type>
-
<tunnel_details>
Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0)
208
</tunnel_details>
-
<other_attributes>
ConfigVersionId=18, DestinationPort=1812, Protocol=Radius, Framed-MTU=1300, State=37CPMSession
ID=0acb6b0b0000000B4D0C0DBD;39SessionID=HAREESH-R6-1-PDP1/81999140/30;, Proxy-State=Cisco
Secure
ACS53e5cfac-0a31-11e0-c000-000000000000-2905701264-3372,Airespace-Wlan-Id=2,CPMSessionID=0
acb6b0b0000000B4D0C0DBD,IssuedPacInfo=Issued PAC type=Tunnel V1 with expiration time: Fri
Mar 18 01:26:22
2011,CPMSessionID=0acb6b0b0000000B4D0C0DBD,EndPointMACAddress=00-25-9C-A3-7D-48,Device

```

```

Type=Device Type#All Device Types#iPEP,Location=Location#All Locations,Model
Name=Unknown,Software Version=Unknown,Device IP
Address=10.203.107.11,Called-Station-ID=00-24-c4-1b-36-70:i pep3
</other_attributes>
<response_time>3</response_time>
</authStatusElements>
</authStatusList>
</authStatusOutputList>

```

## アカウント ステータス API コール

ターゲット ノードの最新のデバイスおよびセッションのアカウント情報を取得するために **AcctStatus** API コールを使用できます。ここでは、スキーマ ファイルの出力例、この API コールを呼び出すことにより、最新のデバイスおよびセッション情報の要求を送信する手順、この API コール発行後に返されるデータのサンプルについて説明します。**AcctStatus** API コールにより、時間関連パラメータを設定できるようになります。

- 期間：指定された MAC アドレスに関連付けられた最新アカウントのデバイス レコードの検索と取得が試行される秒数を定義します。ユーザが設定可能な値の有効範囲は 1 ~ 432000 秒 (5 日) です。
  - 2400 秒 (40 分) の値を入力した場合は、過去 40 分間に使用可能な指定 MAC アドレスの最新アカウントのデバイス レコードが必要であることを意味します。
  - 0 秒の値を入力した場合は、デフォルト期間の 15 分 (900 秒) を指定します。これは、この時間内に使用可能な指定 MAC アドレスの最新アカウントのデバイス レコードが必要であることを意味します。

**AcctList** API コールは、API 出力として、次のアカウント ステータスのデータ フィールドを提供します (表 3-3 を参照)。

**表 3-3 アカウンティング ステータスのデータ フィールド**

データ フィールド	説明
MAC アドレス	クライアントの MAC アドレス
audit-session-id	認証セッション ID
パケット入力	総受信パケット数
パケット出力	総送信パケット数
バイト入力	総受信バイト数
バイト出力	総送信バイト数
セッション時間	現在のセッションの存続時間

## AcctStatus API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードでの指定されたセッションへの送信後の、**AcctStatus** API コールの出力です。

```

<?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="acctStatusOutputList" type="restAcctStatusOutputList"/>

  <xs:complexType name="restAcctStatusOutputList">
    <xs:sequence>

```

```

    <xs:element name="acctStatusList" type="restAcctStatusList" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="restAcctStatusList">
  <xs:sequence>
    <xs:element name="acctStatusElements" type="restAcctStatus" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="macAddress" type="xs:string"/>
  <xs:attribute name="username" type="xs:string"/>
</xs:complexType>

<xs:complexType name="restAcctStatus">
  <xs:sequence>
    <xs:element name="calling_station_id" type="xs:string" minOccurs="0"/>
    <xs:element name="audit_session_id" type="xs:string" minOccurs="0"/>
    <xs:element name="paks_in" type="xs:long" minOccurs="0"/>
    <xs:element name="paks_out" type="xs:long" minOccurs="0"/>
    <xs:element name="bytes_in" type="xs:long" minOccurs="0"/>
    <xs:element name="bytes_out" type="xs:long" minOccurs="0"/>
    <xs:element name="session_time" type="xs:long" minOccurs="0"/>
    <xs:element name="username" type="xs:string" minOccurs="0"/>
    <xs:element name="server" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>

```

## AcctStatus API 呼び出しを呼び出すこと



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**AcctStatus API コールを発行するには、次の手順を実行します。**

**ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が `acme123` の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

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

**ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント  
(`/ise/mnt/api/<specific-api-call>/MACAddress/<macaddress>/<durationofcurrenttime>`) に置き換えて、ターゲット ノードの URL アドレス フィールドに AcctStatus API コールを入力します。

```
https://acme123/ise/mnt/api/AcctStatus/MACAddress/00:26:82:7B:D2:51/1200
```



(注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。

---

## AcctStatus API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで AcctStatus API コールを呼び出すときに返されるデータを示します。

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

```
-  
<acctStatusOutputList>  
-  
<acctStatusList macAddress="00:25:9C:A3:7D:48">  
-  
<acctStatusElements>  
<calling_station_id>00:25:9C:A3:7D:48</calling_station_id>  
<audit_session_id>0acb6b0b0000000B4D0C0DBD</audit_session_id>  
<paks_in>0</paks_in>  
<paks_out>0</paks_out>  
<bytes_in>0</bytes_in>  
<bytes_out>0</bytes_out>  
<session_time>240243</session_time>  
<server>HAREESH-R6-1-PDP1</server>  
</acctStatusElements>  
</acctStatusList>  
</acctStatusOutputList>
```





## CHAPTER 4

# 認可変更 REST API の使用

この章では、Cisco Identity Services Engine のこのリリースでサポートされている次の個々の認可変更 (CoA) REST API コールの使用法について例をあげながら説明します。CoA API コールは、Cisco ISE 導入で指定された Cisco Monitoring ISE ノードセッションに認証コマンドおよびセッション切断コマンドを送信する方法を提供します。

次の項では、API の出力スキーマ ファイルの例、各 API コール発行の手順、および各 API コールによって返されるデータのサンプルについて説明します。

- 「セッション再認証 API コール」 (P.4-1)
- 「セッション切断 API コール」 (P.4-3)

## CoA セッション管理 API コールの使用

CoA セッション管理 API コールにより、Cisco ISE 導入において、ターゲット Cisco Monitoring ISE ノードの指定セッションに再認証コマンドおよび切断コマンドを送信できるようにします。

- セッション再認証 (Reauth)
- セッション切断 (Disconnect)

## セッション再認証 API コール

ここでは、スキーマ ファイルの出力例、Reauth API コールを呼び出すことにより、セッション再認証コマンドおよび Reauth タイプを送信する手順、この API コール発行後に返されるデータのサンプルについて説明します。再認証のタイプには次のいずれかを割り当てることができます。

- REAUTH\_TYPE\_DEFAULT = 0
- REAUTH\_TYPE\_LAST = 1
- REAUTH\_TYPE\_RERUN = 2

## Reauth API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードで指定セッションへの送信後の Reauth API コールの出力です。

```
<?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>
```

## Reauth API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2) を参照してください。

**Reauth API コールを発行するには、次の手順を実行します。**

**ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。  
たとえば、ホスト名が acme123 の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。

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

**ステップ 2** 「/admin/」コンポーネントを API コールのコンポーネント (/ise/mnt/api/CoA/<specific-api-call>/<macaddress>/<reauthtype>/<nasipaddress>/<destinationipaddress>) に置き換えて、ターゲット ノードの URL アドレス フィールドに Reauth API コールを入力します。

```
https://acme123/ise/mnt/api/CoA/Reauth/server12/00:26:82:7B:D2:51/2/10.10.10
```



(注) これらのコールは、大文字小文字を区別するため、ターゲット ノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。

**ステップ 3** Enter キーを押して API コールを発行します。



## Reauth API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで Reauth API コールを呼び出すときに返されるデータを示します。このコマンドの呼び出しから、次の2種類の結果が返されます。

- 「True」はコマンドが正常に実行されたことを示します。
- 「False」は（さまざまな条件により）コマンドが実行されなかったことを意味します。

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>
```

## セッション切断 API コール

ここでは、スキーマ ファイルの出力例、Disconnect API コールを呼び出すことにより、セッション接続解除コマンドおよびポート オプション タイプを送信する手順、この API コール発行後に返されるデータのサンプルについて説明します。接続解除のポート オプション タイプには、次のいずれかを割り当てることができます。

- DYNAMIC\_AUTHZ\_PORT\_DEFAULT = 0
- DYNAMIC\_AUTHZ\_PORT\_BOUNCE = 1
- DYNAMIC\_AUTHZ\_PORT\_SHUTDOWN = 2

## Disconnect API の出力スキーマ

このサンプル スキーマ ファイルは、ターゲット Cisco Monitoring ISE ノードで指定セッションへの送信後の Disconnect API コールの出力です。

```
<?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>
```

## Disconnect API コールの呼び出し



(注) API コールを発行するターゲット ノードが、有効な Cisco Monitoring ISE ノードであることを確認している必要があります。Cisco ISE ノードのペルソナを確認するには、「[Cisco Monitoring ISE ノードの確認](#)」(P.1-2)を参照してください。

**Disconnect API コールを発行するには、次の手順を実行します。**

- ステップ 1** ターゲット Cisco Monitoring ISE ノードにログインします。
- たとえば、ホスト名が `acme123` の Cisco Monitoring ISE ノードに最初にログインする場合、このノードの URL アドレスが次のように表示されます。
- ```
https://acme123/admin/LoginAction.do#pageId=com_cisco_xmp_web_page_tmpdash
```
- ステップ 2** 「/admin/」 コンポーネントを API コールのコンポーネント (/ise/mnt/api/CoA/<Disconnect>/<serverhostname>/<macaddress>/<portoptiontype>/<nasipaddress>/<destinationipaddress>) に置き換えて、ターゲットノードの URL アドレス フィールドに Disconnect API コールを入力します。
- ```
https://acme123/ise/mnt/api/CoA/Disconnect/server12/00:26:82:7B:D2:51/2/10.10.10.10
```
-  **(注)** これらのコールは、大文字小文字を区別するため、ターゲットノードの URL アドレス フィールドに慎重に各 API コールを入力する必要があります。API コール規則での「mnt」の使用は、Cisco Monitoring ISE ノードを表します。
- ステップ 3** Enter キーを押して API コールを発行します。

## Disconnect API コールから返されるサンプル データ

次に、ターゲット Cisco Monitoring ISE ノードで Disconnect API コールを呼び出すときに返されるデータを示します。このコマンドの呼び出しから、次の 2 種類の結果が返されます。

- 「True」はコマンドが正常に実行されたことを示します。
- 「False」は (さまざまな条件により) コマンドが実行されなかったことを意味します。

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>
```



## **PART 2**

### **参考資料**





# APPENDIX A

## Cisco ISE Failure Reasons Editor の使用

この付録では、Cisco ISE Failure Reasons Editor にアクセスするための手順を提供します。Cisco ISE Failure Reasons Editor は検出できる障害理由すべてに関する情報を提供する Cisco ISE ユーザ インターフェイスのオプションです。API を解決する Cisco ISE クエリーを使用すると Get 障害理由のマッピングのコールから出力として返されるオプションをチェックする場合に使用できます。

Cisco ISE Failure Reasons Editor を使用すると、Cisco ISE ソフトウェアによって定義された Cisco Monitoring ISE ノード動作に適用する障害理由の全リストにアクセスできるようになります。次の手順により、定義された障害理由のリストを表示または編集することができます。障害理由を表示し、ここにアクセスするには、宛先 Cisco Monitoring ISE ノードの Cisco ISE ユーザ インターフェイスにログインする必要があります。ロギングに関する詳細については、「[Cisco Monitoring ISE ノードの確認 \(P.1-2\)](#)」を参照してください。



(注)

Cisco ISE 障害理由に関する詳細または一般的なトラブルシューティングに関する問題については、『[Cisco Identity Services Engine User Guide, Release 1.1.1](#)』の第 22 章「Monitoring and Troubleshooting」および付録 D を参照してください。

## 理由の表示および編集

Cisco ISE Failure Reason Editor を使用すると、障害理由のリストを表示し、障害理由の説明を編集することができます。さらに問題を解決する方法も提供します。

**障害理由を表示および編集するには、次の手順を実行します。**

- ステップ 1** [管理 (Administration)] > [システム (System)] > [設定 (Settings)] の順に選択します。
- ステップ 2** ナビゲーション パネルの [モニタリング (Monitoring)] を展開し、[障害理由エディタ (Failure Reason Editor)] を選択します。  
障害理由のリストが右側のパネルに表示されます。
- ステップ 3** 既知の障害理由を表示または障害理由を検索するには、次の作業を実行します。
  - 既知の障害理由を表示する場合：
    - [障害理由エディタ (Failure Reason Editor)] ページにあるリストから、障害の原因に対応するオプション ボタンか名前リンクを選択します。
  - 障害理由を検索する場合：
    - テキスト文字列を [フィルタ (Filter)] テキスト ボックスに入力し、[フィルタ (Filter)] をクリックします。

- 検索結果として表示される、一致する障害理由の 1 つ（またはそれ以上）を選択します。

**ステップ 4** 障害理由を編集するには、次の手順を実行します。

- 名前の左側にあるオプション ボタンをクリックします（選択されるとボタンは緑に変わります）。
  - [編集 (Edit) ] をクリックします。
  - 適切なフィールドに説明を入力または変更してから、解決手順を入力するか、変更します。
  - 変更を保存するには、[送信 (Submit) ] をクリックします。変更を保存せずに終了する場合は [キャンセル (Cancel) ] をクリックします。
-