APPENDIX D

Cisco ISE のトラブルシューティング

この付録では、Cisco Identity Services Engine（ISE）の使用時に発生する可能性のある問題の識別と解決策に関連するトラブルシューティング情報を、いくつかカテゴリ別に示します。この付録の構成は、次のとおりです。

（注） この付録、および Cisco ISE ソフトウェア アプリケーション自体で提供されるオンライン ヘルプ コンテンツは、Cisco.com 上での公開という点において、可能な限り最新の状態に保たれます。ただし、Cisco Identity Services Engine, Release 1.1.1 以降の最新資料については、スタンドアロンの『*Cisco Identity Services Engine Troubleshooting Guide, Release 1.1.x*』を使用することを推奨します。

インストールとネットワーク接続の問題

ハードウェアに関する複雑な状況が発生していると考えられる場合には、まず展開したすべての Cisco ISE ノードに対して次の点を確認してください。

- 外部電源コードが接続されており、正しい電源が供給されている。
- アプライアンスをネットワークに接続する外部ケーブルが、すべて正しい順序でしっかり装着されている。
- アプライアンスのファンとブロワーが稼働している。
- 不適切な通気、換気の遮断、過剰な埃や汚れ、ファン障害、電源や冷却システムに悪影響を及ぼす可能性のあるすべての環境条件。
- アプライアンスのソフトウェアが正常に起動している。
- アダプタ カード（インストールされている場合）がスロット内に正しく設置されており、それぞれが問題なく初期化されて（アプライアンス ソフトウェアによってイネーブルになって）いる。潜在的な問題の特定を支援するアダプタ カード上のステータス LED を確認する。

電源および冷却要件、および LED の動作を含めて、Cisco ISE ハードウェアのインストールと操作上のトラブルシューティングの詳細については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*』を参照してください。

ヒント　AAA、RADIUS、プロファイラ、および Web 認証を含めて、ネットワーク アクセス デバイス（NAD）設定の潜在的な問題については、[操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [設定評価バリデータ（Evaluate Configuration Validator）] を選択することにより、いくつかの検証分析を実行できます。

現在のインストールおよびネットワーク接続のトラブルシューティングに関するトピック

未知のネットワーク デバイス

症状または問題	Cisco ISE が、指定されたネットワーク アクセス デバイス（NAD）を識別できません。
条件	認証で虫眼鏡アイコンをクリックすると、認証レポートに手順が表示されます。ログに、次のエラー メッセージが表示されます。 • 11007 ネットワーク デバイスまたは AAA クライアント解決を見つけられません（11007 Could not locate Network Device or AAA Client Resolution）
考えられる原因	• 管理者が、Cisco ISE でネットワーク アクセス デバイス（NAD）タイプを正しく設定していません。 • 認証中に IP で NAS にアクセスするときに、ネットワーク デバイスまたは AAA クライアントを見つけられませんでした。
解決策	• Cisco ISE にもう一度 NAD を追加し、NAD タイプと設定を確認します。 • [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワーク デバイス（Network Devices）] で、ネットワーク デバイスまたは AAA クライアントが正しく設定されているか確認します。

CoA がクライアント マシンで開始しない

症状または問題	Cisco ISE ネットワークにログインしているユーザに対して、必要な認可変更（CoA）が実行されません。
条件	Cisco ISE が、サポート対象のネットワーク デバイスからの RADIUS CoA 要求の通信に、デフォルトでポート 1700 を使用します。
考えられる原因	Cisco ISE ネットワーク エンフォースメント ポイント（スイッチ）にキー コンフィギュレーション コマンドが欠落しているか、誤ったポート（たとえば、1700 以外のポート）を割り当てているか、または不正なキーまたは不正に入力されたキーが存在します。
解決策	スイッチ設定ファイル内に、次のコマンドが存在することを確認します（スイッチ上で CoA をアクティブにし、スイッチを設定するのに必要です）。 **aaa server radius dynamic-author** **client** <*Monitoring_node_IP_address*> **server-key** <*radius_key*>

ネットワーク アクセス セッション中にユーザが不正な VLAN に割り当てられる

症状または問題	VLAN 割り当てに関して、クライアント マシンにさまざまなアクセスの問題が発生しています。

条件	認証で虫眼鏡アイコンをクリックすると、認証の詳細が表示されます。認証レポートのセッション イベント セクションに、次の行が含まれています。 • %AUTHMGR-5-FAIL: Authorization failed for client (001b.a912.3782) on Interface Gi0/3 AuditSessionID 0A000A760000008D4C69994E • %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN 666 to 802.1x port FastEthernet1/9 また、認証に対するトラブルシューティング ワークフローを実行できます。このワークフローは、RADIUS スイッチ応答を含む ACL 認証ログとスイッチ メッセージ データベースを比較します。また、次のロギング設定の（グローバルな）詳細も表示されます。 • Mandatory Expected Configuration Found On Device • logging monitor informational Missing • logging origin-id ip Missing • logging source-interface <*interface_id*> Missing • logging <*syslog_server_IP_address_x*> transport udp port 20514 Missing **（注）** ネットワーク デバイスは、syslog メッセージを Monitoring ISE ノード サーバのポート 20514 にも送信する必要があります。
考えられる原因	このスイッチでは、スイッチ上の名前と番号が欠落しています（または、不正なものが含まれています）。
解決策	展開内のネットワーク アクセス/エンフォースメント ポイント（スイッチ）上の VLAN 設定を確認します。

クライアント マシンの URL リダイレクション機能が動作していない

症状または問題	ユーザが、認証用の正しい URL に適切にリダイレクトされていません。
条件	モニタリングおよびトラブルシューティングの設定バリデータが、これを取り込むように設計されています。Web 認証コンフィギュレーション（グローバル）の詳細には、次のような内容が表示されます。 • Mandatory Expected Configuration Found On Device • aaa authorization auth-proxy default group <*radius_group*> aaa authorization auth-proxy default group radius • aaa accounting auth-proxy default start-stop group <*radius_group*> Missing • ip admission name <*word*> proxy http inactivity-time 60 Missing fallback profile <*word*> • ip access-group <*word*> in • ip admission <*word*> Missing • ip http server ip http server • ip http secure-server ip http secure-server
考えられる原因	スイッチに、**ip http server** コマンドまたは **ip http secure-server** コマンドが欠落しています。
解決策	スイッチ上の設定を確認し、（必要な場合には）調整します。

Cisco ISE Profiler がエンドポイントのデータを収集できない

症状または問題	ネットワーク上の既知のデバイスが、Cisco ISE のプロファイラ ポリシーに従ってプロファイルされていません。
条件	モニタリングおよびトラブルシューティング ワークフローが、次のようなデバイス検出設定（グローバル）を取り込みます。 • Mandatory Expected Configuration Found On Device • ip dhcp snooping vlan <*Vlan_ID_for_DHCP_Snooping*> ip dhcp snooping vlan 1-4096 • no ip dhcp snooping information option Missing • ip dhcp snooping ip dhcp snooping • ip device tracking ip device tracking
考えられる原因	1 つまたは複数の Cisco ISE ネットワーク エンフォースメント ポイント（スイッチ）で、Profiler がその機能を実行可能にする **ip dhcp snooping** コマンドまたは **ip device tracking** コマンドが欠落している可能性があります。
解決策	エンドポイントが適切にプロファイルされていないネットワーク セグメントのスイッチ設定を検証して、次の点を確認します。 • エンドポイントをプロファイルするのに必要な情報が、プロファイルを実行するために Cisco ISE に送信されている。 • ネットワーク Policy Service ISE ノード エンティティ上でプローブが設定されている。 • [操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [Tcpdump] で tcpdump 機能を実行することにより、Cisco ISE Profiler モジュールがパケットを受信していることを確認する。 **（注）** HTTP、Netflow、および NMAP で収集された WAN 上のエンドポイントでこの問題が発生する場合、上記のプローブを使用して他の属性を更新する前に、RADIUS/DHCP プローブでエンドポイント IP アドレスが更新されていることを確認します。

RADIUS アカウンティング パケット（属性）がスイッチから着信しない

症状または問題	スイッチが、RADIUS アカウンティング パケット（属性）を RADIUS サーバに送信していません。

条件	認証で虫眼鏡アイコンをクリックすると、認証の詳細が表示されます。認証レポートのセッション イベント セクションには、アカウンティング イベントが示されている必要があります。VSA[1] がブロックされており、スイッチから cisco-av-pair=audit-session-id メッセージが送信されていないため、アカウンティング イベントをクリックすると、audit-session-id フィールドは空白になります。その日のアカウンティング レポートを実行しても、すべての audit-session-id フィールドが空白であるため、同じことが起きます。 **（注）** この問題は、モニタリングおよびトラブルシューティング設定バリデータの RADIUS 設定（グローバル）の詳細により報告されます。 – Mandatory Expected Configuration Found On Device – radius-server attribute 6 support-multiple Missing – radius-server attribute 8 include-in-access-req radius-server attribute 8 include-in-access-req – radius-server host <*radius_ip_address1*> auth-port 1812 acct-port 1813 key <*radius_key*> Missing – radius-server vsa send accounting radius-server vsa send accounting – radius-server vsa send authentication radius-server vsa send authentication **（注）** スイッチ設定には、必ず「radius-server attribute 25 access-request include」を指定してください。
考えられる原因	Cisco ISE ネットワーク エンフォースメント デバイス（スイッチ）に、**radius-server vsa send accounting** コマンドが欠落しています。
解決策	このデバイスのスイッチ RADIUS 設定が正しく、適切なコマンドが備わっていることを確認します。

1. VSA = ベンダー固有属性

Policy Service ISE ノードがトラフィックを渡していない

症状または問題	ネットワーク ポリシー エンフォースメント デバイスがインストールされているネットワーク セグメントを、ネットワーク トラフィックが通過しません。
条件	この問題は、別のネットワーク デバイスと相互運用する Policy Service ISE ノードとして展開されている Cisco ISE およびその他のタイプの NAD に影響を与えることがあります。
考えられる原因	このような問題に対しては、複数の原因が考えられます。
解決策	**1.** NAD コマンドライン インターフェイス（CLI）から **tcpdump** コマンドを使用するか、または [操作（Operations）] > [トラブルシューティング（Troubleshoot）] > [診断ツール（Diagnostic Tools）] > [一般ツール（General Tools）] > [TCP ダンプ（TCP Dump）] の Administration ISE ノード ユーザ インターフェイスから、マシンがネットワークの必要に応じてトラフィックを送受信しているかどうかを確認します。 **2.** TCP ダンプ操作で Cisco ISE または NAD が設定どおりに動作していることが示された場合、他の隣接ネットワーク コンポーネントを確認します。

スタンドアロンの再インストールに続いて Cisco ISE 管理対象リストにノードを登録

症状または問題	Cisco ISE のイメージが再作成され、新しいスタンドアロン ノードとしてインストールされた場合、Administration ISE ノード ユーザ インターフェイスに Policy Service ISE ノードのホスト名および設定情報が表示されます。
条件	これは、関連付けられた 1 つ以上の Policy Service ISE ノードを管理する Administration ペルソナとして、以前展開された Cisco ISE ノードに該当します。
考えられる原因	Policy Service ISE ノードが、当初のセットアップと同様に、Administration ペルソナに syslog アップデートを送信するように引き続き設定されている場合、ノード情報は Administration の個人設定が syslog メッセージを受信した際に収集されます。その情報が、Administration ペルソナのシステム サマリー ページの設定に使用される可能性があります。
解決策	Cisco ISE ノードから Policy Service ISE ノードを「登録解除」していない場合、syslog メッセージを Cisco ISE ノードではなく Policy Service ISE ノード自身に送信するように Policy Service ISE ノードを再設定し、Policy Service ISE ノードを再起動します。 **（注）** Cisco ISE ソフトウェアを再インストールして Administration ペルソナを再設定する前に、関連付けられている Policy Service ISE ノードを登録解除した場合は、Policy Service ISE ノードはスタンドアロン モードで動作し、誤った syslog アップデートを送信しません。

プライマリとセカンダリの Inline Posture ノードのハートビート リンクが機能しない

症状または問題	ハイ アベイラビリティ ピアとして展開されている 2 つの Inline Posture ノードが互いに動作していません。
条件	2 つのインライン ポスチャ ノードが、「連結された」ハイ アベイラビリティ導入で展開されています。
考えられる原因	Inline Posture ノードの eth2 インターフェイスおよび eth3 インターフェイスが接続されていない場合、両方のノードは、展開内の他方のノードに何らかの障害が発生しているかのように動作します。
解決策	ハートビート プロトコルには、2 つのノードの eth3 インターフェイス間の直接ケーブル接続に加えて、ハイ アベイラビリティ ペアの両ノードの eth2 インターフェイス間の直接ケーブル接続が必要です。任意のイーサネット ケーブルを使用して、これらの接続を作成できます。

ライセンスと管理者アクセス

証明書の失効

症状または問題	• 管理者へのアラーム メッセージが、証明書が失効する 30 日前から表示され始めます。 • 証明書が失効した場合は、ユーザは、証明書の更新を完了するまで、Cisco ISE を介してネットワークにログインできません。
条件	この問題は、Cisco ISE 上の失効したすべての証明書に当てはまります。
考えられる原因	Cisco ISE 証明書の有効期限がまもなく切れます。
解決策	Cisco ISE の信頼できる証明書を更新します。

設定と操作（ハイアベイラビリティを含む）

この項では、次のトピックを扱います。

クライアント マシンが認証を実行できない

症状または問題	• クライアント セッションが 802.1X 認証を完了しません。 • 特定 DACL の認証で虫眼鏡アイコンをクリックすると、認証の詳細が表示されます。ACL の内容には、1 つ以上の不正な文字が表示されます。
条件	認証で虫眼鏡アイコンをクリックすると、認証の詳細が表示されます。認証レポートのセッション イベント セクションに、次のエントリが含まれます。 `%EPM-4-POLICY_APP_FAILURE: IP 0.0.0.0| MAC 0002.b3e9.c926| AuditSessionID 0A0002010000239039837B18| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME xACSACLx-IP-acl_access-4918c248| RESULT FAILURE| REASON Interface ACL not configured`
考えられる原因	• DACL 構文が正しくないか、Cisco ISE で設定されていない可能性があります。 • Cisco ISE が DACL を適用し、スイッチで事前認証 ACL が設定されていない場合は、NAD がセッションを停止し、認証が失敗します。
解決策	問題の性質に応じて、次の解決策を実行します。 • Cisco ISE で設定された DACL 構文を修正し、構文に **permit udp any any** コマンドも含まれていることを確認します。 • スイッチ上で適切な事前認証 ACL を設定します。

ユーザが URL に正しくリダイレクトされない

症状または問題	管理者が、1 つ以上の「不正 URL（Bad URL）」エラー メッセージを Cisco ISE から受信します。
条件	このシナリオは、ゲスト アクセス セッションだけでなく、802.1X 認証にも適用されます。 認証で虫眼鏡アイコンをクリックすると、認証の詳細が表示されます。認証レポートには、（スイッチ syslog メッセージを表示する）セッション イベント セクションだけでなく、RADIUS 応答セクションにもリダイレクト URL が存在します。
考えられる原因	無効な構文またはパス コンポーネントの欠落により、リダイレクション URL が正しく入力されていません。

解決策	Cisco-av ペア「URL Redirect」を介して Cisco ISE で指定されたリダイレクション URL が、次の各オプションで正しいことを確認します。 • CWA リダイレクション URL：//ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa • 802.1X リダイレクション URL：url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp

リモート クライアントのプロビジョニング リソースをダウンロードできない

症状または問題	クライアント プロビジョニング リソースのダウンロードを試行すると、管理者は、1 つ以上の「java.net.NoRouteToHostException：ホストへのルートが存在しない（java.net.NoRouteToHostException: No route to host）」エラー メッセージを受信します。
条件	この問題は、外部クライアントのプロビジョニング リソース ストアに接続しているすべての Cisco ISE に適用されます。
考えられる原因	インターネット接続が正常に動作していないか、または信頼性が低い可能性があります。
解決策	• インターネット接続の設定を確認します。 • [管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）] で、Cisco ISE のプロキシを正しく設定したことを確認します。

Policy Service ISE ノードを Administration ISE ノードに登録した後にモニタリングおよびトラブルシューティング データを消失

症状または問題	プロファイリングされたエンドポイントの既知の収集は、オリジナル（プライマリ）Administration ペルソナに登録した場合、セカンダリ Policy Service ISE ノードには表示されません。
条件	この問題は、展開において、登録時まで既知かつプロファイルされたエンドポイントの大規模ストアを持つスタンドアロン Cisco ISE ノードであったノードに、新しい Policy Service ISE ノードを登録すると発生します。
考えられる原因	ノードのサイズが巨大な可能性があるため、新しいノードを元のスタンドアロン Cisco ISE ノードに登録した際に、モニタリングおよびトラブルシューティング データが 2 つのノード間で複製されません。データ ストアのサイズがギガバイトに達すると考えられる場合、展開環境のネットワーク接続に影響を与える可能性があるため、Cisco ISE は、そのようなサイズのデータ ストアを複製しません。
解決策	以前はスタンドアロンの Cisco ISE に新しい Policy Service ISE ノードを登録する*前に*、モニタリングおよびトラブルシューティング情報を確実にエクスポートしてください。

Cisco ISE のモニタリング ダッシュレットが Internet Explorer 8 で表示されない

症状または問題	管理者が Cisco ISE モニタリング ポータルにあるダッシュレットをクリックした後に、1 つ以上の「この Web サイトのセキュリティ証明書には問題があります。(There is a problem with this website's security certificate.)」というメッセージが表示されます。
条件	これは、Internet Explorer 8 に固有の問題です （この問題は、Mozilla Firefox では発生しません)。
考えられる原因	Internet Explorer 8 ブラウザ接続のセキュリティ証明書が無効であるか、または失効しています。
解決策	Internet Explorer 8 を使用して有効なセキュリティ証明書を再インポートし、ダッシュレットを適切に表示します。

データがプライマリ ISE ノードとセカンダリ ISE ノード間で同期しない

症状または問題	管理者に対して、次のいずれかのレプリケーション ステータスまたは同期ステータスが表示されます。 • 同期しない • ノードに到達できない • レプリケーションが無効である
条件	この問題は、プライマリ ノードと ISE セカンダリ ノードのデータベースが同期しない場合に発生します。
考えられる原因	この問題は、次の場合に発生する可能性があります。 • システム時刻の逆方向への変更またはデータベース同期中の中断によって、データベース同期が失敗した場合。 • ノードに到達できない場合。 • 証明書の期限が切れている場合。 • セカンダリ ノードが 6 時間を超えてダウンしている場合。
解決策	次の操作を実行できます • 時刻の変更または NTP 同期問題によって発生する可能性の高い非同期に関する問題を解決するには、システム時刻を修正し、UI を通して手動で同期を実行する必要があります。 • 証明書の有効期限切れの問題に関しては、有効な証明書をインストールし、UI を通して手動で同期を実行する必要があります。 • 6 時間を超えてダウンしているノードに関しては、ノードを再起動して接続の問題を確認し、UI を通して手動で同期を実行する必要があります。

外部認証ソース

この項では、次のトピックを扱います。

ユーザ認証が失敗した

症状または問題	認証レポートの失敗の理由：「認証が失敗しました：22040 パスワードが不正か、または共有秘密が無効です（Authentication failed: 22040 Wrong password or invalid shared secret）」
条件	認証の虫眼鏡アイコンをクリックすると、次のような一連の簡素なメッセージが表示されている認証レポートの手順が表示されます。 • 24210 内部ユーザ IDStore でユーザを検索 - test-radius（24210 Looking up User in Internal Users IDStore - test-radius） • 24212 内部ユーザ IDStore でユーザを検出しました（24212 Found User in Internal Users IDStore） • 22040 パスワードが不正か、または共有秘密が無効です（22040 Wrong password or invalid shared secret）
考えられる原因	ユーザまたはデバイスが、外部認証ソースと一致する正しいクレデンシャルまたは RADIUS キーを提供していない可能性があります。
解決策	クライアント マシンに入力されているユーザ クレデンシャルが正しいことを確認し、RADIUS サーバの共有秘密が NAD と Cisco ISE の両方（これらは同じである必要があります）で正しく設定されていることを確認します。

Cisco ISE ID に RADIUS サーバ テスト ユーザ名のユーザが欠落

症状または問題	管理者に、特定のユーザ ID に関して「認証が失敗しました：22056 該当する ID ストアにサブジェクトが見つかりません（Authentication failed: 22056 Subject not found in the applicable identity store(s)）」のような認証レポート失敗メッセージが通知されます。

条件	認証で虫眼鏡アイコンをクリックすると、認証レポート内のメッセージが表示されます。次のような一連のエントリが表示されます。 • 24210 内部ユーザ IDStore でユーザを検索 - test-radius（24210 Looking up User in Internal Users IDStore - test-radius） • 24216 内部ユーザ ID ストアにユーザが見つかりません（24216 The user is not found in the internal users identity store） • 22056 該当する ID ストアにサブジェクトが見つかりません（22056 Subject not found in the applicable identity store(s)）
考えられる原因	このメッセージは、認証が失敗するたびに表示されます。すべての場合、Cisco ISE にとって未知のユーザであることが原因です。問題は、ローカル データベースに追加されていないゲスト ユーザ、ネットワーク内で適切にプロビジョニングされていない新しい従業員、またはハッカーの可能性さえあります。 さらに、管理者が Cisco ISE 内でユーザ ID を設定していないこともあります。
解決策	ローカルおよび外部 ID ソースを検査して、ユーザ ID が存在すること、および存在する場合には、Cisco ISE および関連付けられたアクセス スイッチの両方がそのユーザを受け入れるように設定されていることを確認します。

ネットワーク アクセス デバイス（スイッチ）と Cisco ISE の接続の問題

症状または問題	認証レポートの失敗の理由：「認証が失敗しました：22040 パスワードが不正か、または共有秘密が無効です（Authentication failed: 22040 Wrong password or invalid shared secret）」
条件	認証で虫眼鏡アイコンをクリックすると、次のような認証レポート エントリが表示されます。 • 24210 内部ユーザ IDStore でユーザを検索 - test-radius（24210 Looking up User in Internal Users IDStore - test-radius） • 24212 内部ユーザ IDStore でユーザを検出しました（24212 Found User in Internal Users IDStore） • 22040 パスワードが不正か、または共有秘密が無効です（22040 Wrong password or invalid shared secret）
考えられる原因	ネットワーク管理者が、Cisco ISE で認証を行うためのスイッチ（または他の NAD）を有効にする、正しいパスワードを指定していない可能性があります。
解決策	Cisco ISE で認証を行うために、NAD 上で設定されたパスワードが正しいことを確認してください。

Active Directory の切断

症状または問題	Cisco ISE と Active Directory サーバの間の接続が切断され、その結果としてユーザ認証が失敗しました。
条件	この問題は、Cisco ISE に接続されるすべての Active Directory ドメイン トポロジに関連しています。

考えられる原因	このシナリオの最も一般的な原因は、VMware 上の NTP[1] を介して時刻が同期していないことによるクロックのずれです。 この問題は、Cisco ISE FQDN[2] が変化すること、またはクライアント マシン上にインポートされた証明書の名前が変更されることによっても発生する可能性があります。
解決策	ユーザの Active Directory ドメインと Cisco ISE が、同じ NTP サーバ ソースに整合していることを確認します。 Active Directory サーバをシャットダウンするか、または一時停止し、ネットワークに対して従業員の認証を試みます。

1. NTP = ネットワーク タイム プロトコル
2. FQDN = Fully-Qualified Domain Name（完全修飾ドメイン名）

Cisco ISE ノードが Active Directory で認証されない

症状または問題	管理者に対して、Administration ISE ノードの認証エラー レポートに「認証エラー（authentication failure）」メッセージが表示されます。
条件	この問題は、既存の AD ドメインに追加される Cisco ISE ポリシー適用ノードに該当します。
考えられる原因	• Cisco ISE ノードを AD ドメインに追加した後、管理者が AD パスワードを変更していない可能性があります。 • Cisco ISE を Active Directory ドメインに追加するのに使用したアカウントで、パスワードの有効期限が切れている可能性があります。
解決策	Cisco ISE を Active Directory に追加した後、AD ドメインに参加するために使用したアカウント パスワードを変更します。

Cisco ISE に RADIUS サーバのエラー メッセージ エントリが表示される

症状または問題	• Cisco ISE で RADIUS 機能または AAA[1] 機能が失敗する • [操作（Operations）] > [認証（Authentication）] イベント エントリでエラー メッセージが表示される
条件	このシナリオでは、Cisco ISE がネットワーク上の外部 ID ソースを介してユーザ認証を実行するように設定されているシステムで問題となる可能性があります。
考えられる原因	外部 ID ソースとの接続を失う場合に考えられる原因は、次のとおりです。 • 該当する ID ソースで、サブジェクトが見つからない • パスワードが不正か、または共有秘密が無効である • ネットワーク デバイスまたは AAA クライアントが見つからない

解決策	Cisco ISE ダッシュボード（[操作（Operations）] > [認証（Authentication）]）で、RADIUS 通信喪失の性質に関する表示を確認します （指定された RADIUS ユーザ名のインスタンスを検索し、エラー メッセージ エントリに関連付けられているシステム メッセージをスキャンします）。 Cisco ISE CLI[2] にログインして次のコマンドを入力し、接続の問題のデバッグに役立つ可能性のある RADIUS 属性出力を生成します。 **test aaa group radius** <*username*> <*password*> **new-code** このテスト コマンドが成功した場合、次の属性が表示されます。 • 接続ポート • 接続 NAD IP アドレス • 接続 Policy Service ISE ノード IP アドレス • 正しいサーバ キー • 認識されているユーザ名またはパスワード • NAD と Policy Service ISE ノード間の接続 また、このコマンドを使用して、コマンドラインに不正なパラメータ値を意図的に指定し、管理者ダッシュボード（[操作（Operations）] > [認証（Authentication）]）に戻って不正なコマンドラインによって生じたエラー メッセージ エントリのタイプと頻度を表示することにより、RADIUS 通信の潜在的な問題に焦点を絞りやすくすることもできます。たとえば、ユーザ クレデンシャルが問題の原因であるかどうかをテストするには、正しくないことが*わかっている*ユーザ名とパスワードまたはそのいずれかを入力して [操作（Operations）] > [認証（Authentications）] ページでユーザ名に関係するエラー メッセージ エントリを検索し、Cisco ISE のレポート内容を確認します。 **（注）** このコマンドでは、NAD が RADIUS を使用するように設定されているかどうか、および NAD が新しい AAA モデルを使用するように設定されているかどうかは検証されません。

1. AAA = 認証、許可、アカウンティング
2. CLI = コマンドライン インターフェイス

RADIUS サーバの接続性に関する問題（Cisco ISE にエラー メッセージ エントリが表示されない場合）

症状または問題	• Cisco ISE で RADIUS 機能または AAA 機能が失敗する • NAD が Policy Service ISE ノードを ping できない
条件	このシナリオは、Cisco ISE がネットワーク上の外部 RADIUS サーバを介してユーザ認証を実行するように設定されているシステムで発生します。
考えられる原因	RADIUS サーバとの接続を失う場合に考えられる原因は、次のとおりです。 • ネットワーク接続に関する 1 つ以上の問題 • 不正サーバ IP アドレス • 不良サーバ ポート

解決策	NAD から Policy Service ISE ノードを ping できない場合は、次のいずれかまたはすべての解決策を実行してください。 • NAD IP アドレスを確認します。 • Traceroute およびその他の適切な「スニファ」タイプのツールを使用し、切断の原因の特定を試みます （デバッグ機能は通常、利用可能な帯域幅と CPU を大量に消費するため、通常のネットワーク動作に影響を与える場合があります。そのため、実働環境では、デバッグ機能を過度に使用しないように注意してください）。 指定された Policy Service ISE ノードの Cisco ISE「TCP ダンプ（TCP Dump）」レポートに記載があるかどうかを確認します。

クライアント アクセス、認証、および許可

この項では、次のトピックを扱います。

プロファイリングされたエンドポイントで認証を実行できない

症状または問題	• IP Phone がプロファイリングされていますが、正しく許可されていません。したがって、音声 VLAN に割り当てられていません。 • IP Phone がプロファイリングされ、正しく許可されているが、正しい音声 VLAN に割り当てられていません。 • エンドポイントが Cisco ISE で正常にプロファイリングされていますが、ユーザ認証が失敗します。
条件	管理者に対して、「22056 該当する ID ストアにサブジェクトが見つかりません（22056 Subject not found in the applicable identity store(s)）」という管理ログ エラー メッセージが表示され、次のエントリが含まれています。 • 24210 内部ユーザ IDStore でユーザを検索 - 00:03:E3:2A:21:4A（24210 Looking up User in Internal Users IDStore - 00:03:E3:2A:21:4A） • 24216 内部ユーザ ID ストアにユーザが見つかりません（24216 The user is not found in the internal users identity store） • 22056 該当する ID ストアにサブジェクトが見つかりません（22056 Subject not found in the applicable identity store(s)）

考えられる原因	• これは、MAB[1] または 802.1X 認証問題のいずれかである可能性があります。 • 許可プロファイルに Cisco av-pair="device-traffic-class=voice" 属性が欠落している可能性があります。そのため、スイッチが音声 VLAN 上のトラフィックを認識しません。 • 管理者がエンドポイントをスタティック アイデンティティとして追加していないか、未登録のエンドポイントの通過を許可していません（障害の発生時に「Continue/Continue/Continue」へのポリシー ルールを作成）。
解決策	• 許可ポリシーがグループおよび条件に対して適切にフレーミングされていることを確認し、IP Phone が「IP phone」または「Cisco-device」のどちらとしてプロファイルされているか確認します。 • マルチドメイン用のスイッチ ポート設定および音声 VLAN 設定を確認します。 • 次のように、continue/continue/continue を追加してエンドポイントの通過を許可します。 **a.** [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [設定（Configurations）] を選択し、[許可されたプロトコル サービス（Allowed Protocol Services）] を選択してプロトコル ポリシーを作成します。MAC 認証は、PAP[2] /ASCII プロトコルおよび EAP-MD5[3] プロトコルを使用します。次の MAB_Protocols 設定をイネーブルにします。 – ホスト ルックアップの処理（Process Host Lookup） – PAP/ASCII – PAP をホスト ルックアップとして検出する（Detect PAP as Host Lookup） – EAP-MD5 – EAP-MD5 をホスト ルックアップとして検出する（Detect EAP-MD5 as Host Lookup） **b.** メイン メニューから、[ポリシー（Policy）] > [認証（Authentication）] を選択します。 **c.** 認証方式をシンプルからルール ベースに変更します。 **d.** アクション アイコンを使用して MAB の新しい認証方式エントリを作成します。 – 名前：MAB – 条件：IF MAB RADIUS:Service-Type == Call Check – プロトコル：MAB_Protocols のプロトコルを許可し、使用する – ID ソース：内部 – ホスト：Continue/Continue/Continue

1. MAB = MAC 認証バイパス
2. PAP = パスワード認証プロトコル
3. EAP = 拡張認証プロトコル、MD5 = メッセージ ダイジェスト 5

隔離済みエンドポイントがポリシー変更の後に認証を更新しない

症状または問題	ポリシー変更または ID の追加後に認証が失敗し、再認証が行われません。問題のエンドポイントが接続不可のままであるか、または認証が失敗します。
条件	この問題は、ユーザ ロールに割り当てられるポスチャ ポリシーごとのポスチャ評価に失敗するクライアント マシンで頻繁に発生します。
考えられる原因	クライアント マシンで認証タイマが正しく設定されていないか、またはスイッチ上で認証間隔が正しく設定されていません。
解決策	この問題には、解決策がいくつか考えられます。 1. Cisco ISE で、指定された NAD またはスイッチの Session Status Summary レポートを検査し、インターフェイスに適切な認証間隔が設定されていることを確認します。 2. NAD/ スイッチ上で「show running configuration」と入力し、適切な「authentication timer restart」設定でインターフェイスが設定されていることを確認します。（たとえば、「authentication timer restart 15」および「authentication timer reauthenticate 15」）。 3. NAD/ スイッチ上で「interface shutdown」および「no shutdown」と入力してポートをバウンスし、Cisco ISE で変更があったと考えられる場合には再認証を適用します。

（注） CoA は MAC アドレスまたはセッション ID を必要とするので、Network Device SNMP レポートに表示されるポートをバウンスしないように推奨しています。

エンドポイントが予期されたプロファイルに整合していない

症状または問題	IP Phone をプラグインすると、プロファイルが「Cisco-Device」として表示されます。
条件	Endpoint Profiler/Endpoint Profiler Summary レポートを起動し、プロファイルされた当該エンドポイントに対応する MAC アドレスの [詳細（Details）] をクリックします。
考えられる原因	• Cisco ISE またはスイッチ、またはその両方に SNMP 設定の問題がある可能性があります。 • プロファイルが正しく設定されていないか、またはすでにエンドポイントの MAC アドレスが含まれている可能性があります。
解決策	• Cisco ISE およびスイッチの両方で SNMP トラップに関する SNMP バージョン設定を確認し、また SNMP サーバの設定も確認します。 • Profiler プロファイルの更新が必要な場合があります。[管理（Administration）] > [ID の管理（Identity Management）] > [ID（Identities）] > [エンドポイント（Endpoints）] に移動し、MAC アドレスでエンドポイントを選択して、[編集（Edit）] をクリックします。

ユーザがローカル Cisco ISE ID ストアに対して認証を実行できない

症状または問題	ユーザがサプリカントから認証できません。
条件	認証レポートの失敗の理由：「認証が失敗しました：22056 該当する ID ストアにサブジェクトが見つかりません（Authentication failed: 22056 Subject not found in the applicable identity store(s)）」 認証で虫眼鏡アイコンをクリックすると、次のように表示された認証レポートが開きます。 • 24210 内部ユーザ IDStore でユーザを検索 - ACSXP-SUPP2\Administrator（24210 Looking up User in Internal Users IDStore - ACSXP-SUPP2\Administrator） • 24216 内部ユーザ ID ストアにユーザが見つかりません（24216 The user is not found in the internal users identity store）
考えられる原因	サプリカントは、ローカル Cisco ISE ユーザ データベースに対して認証を行う名前とパスワードを提供しますが、それらのクレデンシャルがローカル データベースで設定されていません。
解決策	ユーザ クレデンシャルが Cisco ISE ローカル ID ストア内に設定されていることを確認してください。

サプリカントを介した証明書ベースのユーザ認証が失敗

症状または問題	クライアント マシンでユーザ認証が失敗し、「RADIUS Access-Reject」形式のメッセージが表示されます。

条件	（この問題は、証明書の検証を必要とする認証プロトコルで発生します）。 可能性のある認証レポートの失敗の理由： • 「認証が失敗しました：11514 予期しない空の TLS メッセージを受信しました。クライアントによる拒否として取り扱います（Authentication failed: 11514 Unexpectedly received empty TLS message; treating as a rejection by the client）」 • 「認証が失敗しました：12153 クライアントが Cisco ISE ローカル証明書を拒否したため、EAP-FAST が SSL/TLS ハンドシェイクに失敗しました（Authentication failed: 12153 EAP-FAST failed SSL/TLS handshake because the client rejected the Cisco ISE local-certificate）」 認証で虫眼鏡アイコンをクリックすると、認証レポートに次の出力が表示されます。 • 12305 別の PEAP チャレンジで EAP 要求を準備（12305 Prepared EAP-Request with another PEAP challenge） • 11006 RADIUS アクセス チャレンジを返しました（11006 Returned RADIUS Access-Challenge） • 11001 RADIUS アクセス要求を受信しました（11001 Received RADIUS Access-Request） • 11018 RADIUS は既存のセッションを再利用します（11018 RADIUS is reusing an existing session） • 12304 PEAP チャレンジ応答を含む EAP 応答を抽出しました（12304 Extracted EAP-Response containing PEAP challenge-response） • 11514 予期しない空の TLS メッセージを受信しました。クライアントによる拒否として取り扱います（Authentication failed: 11514 Unexpectedly received empty TLS message; treating as a rejection by the client） • 12512 予期しない TLS 確認応答メッセージをクライアントからの拒否として取り扱います（12512 Treat the unexpected TLS acknowledge message as a rejection from the client） • 11504 EAP 障害に対する準備（11504 Prepared EAP-Failure） • 11003 RADIUS アクセス拒否を返しました（11003 Returned RADIUS Access-Reject） • 11006 RADIUS アクセス チャレンジを返しました（11006 Returned RADIUS Access-Challenge） • 11001 RADIUS アクセス要求を受信しました（11001 Received RADIUS Access-Request） • 11018 RADIUS は既存のセッションを再使用しています（11018 RADIUS is re-using an existing session） • 12104 EAP-FAST チャレンジ応答を含む EAP 応答を抽出しました（12104 Extracted EAP-Response containing EAP-FAST challenge-response） • 12815 TLS アラート メッセージを抽出しました（12815 Extracted TLS Alert message） • 12153 クライアントが Cisco ISE ローカル証明書を拒否したため、EAP-FAST が SSL/TLS ハンドシェイクに失敗しました（Authentication failed: 12153 EAP-FAST failed SSL/TLS handshake because the client rejected the Cisco ISE local-certificate） • 11504 EAP 障害に対する準備（11504 Prepared EAP-Failure） • 11003 RADIUS アクセス拒否を返しました（11003 Returned RADIUS Access-Reject） **（注）** これは、クライアントが Cisco ISE 証明書を持っていないか、または信頼していないことを示しています。

考えられる原因	サプリカントまたはクライアント マシンが Cisco ISE からの証明書を受け入れていません。 クライアント マシンは、サーバ証明書を検証するように設定されていますが、Cisco ISE 証明書を信頼するように設定されていません。
解決策	認証を有効にするためには、クライアント マシンが Cisco ISE 証明書を受け入れる必要があります。

802.1X 認証の失敗

症状または問題	クライアント マシンを介してログインしているユーザに、サプリカントから 802.1X 認証が失敗したことを示すエラー メッセージが表示されます。
条件	トラブルシューティングの手順： **1.** [操作（Operations）] > [認証（Authentications）] を選択します。 **2.** 「失敗の理由」をスクロールして検索します。
考えられる原因	失敗した認証レコードの詳細を検索して、[詳細（Details）] > [認証の解決策（Resolution for the Authentication）] 下で失敗の理由のリンクをクリックします。失敗の理由が表示されます。
解決策	• 「考えられる原因」に規定された失敗の理由が見つかるごとに修正します。 • 任意のアクティブ セッションの詳細アイコンをクリックして [AAA プロトコル（AAA Protocol）] > [RADIUS 認証の詳細（RADIUS Authentication Details）] レポートに移動し、そこに表示されている [認証の要約（Authentication Summary）] > [Radius ステータス（Radius Status）] フィールドで、メッセージ コードのハイパーリンクとともに失敗の理由を確認できます。

（注） （モニタリングおよびトラブルシューティングが正しく動作していると想定して）認証が失敗し、検索する認証エントリが存在しない場合には、次の手順を実行します。

1. スイッチ上の RADIUS サーバ設定が Cisco ISE を指していることを確認する。
2. スイッチと Cisco ISE 間のネットワーク接続を確認する。
3. Cisco ISE 上で Policy Service ISE ノードが動作しており、RADIUS 要求を受信できることを確認する。

ユーザから予期しないネットワーク アクセスの問題が報告される

症状または問題	この問題では、次のようないくつかの症状があります。 • ユーザが、予期したエージェント以外のエージェントをダウンロードするように要求されている。 • 完全なネットワーク アクセス権を持つユーザが、制限されたネットワーク アクセスのみ許可される。 • ユーザがポスチャ評価を渡しているにもかかわらず、適切なレベルのネットワーク アクセスを取得できない。 • 会社の（アクセス）VLAN に入ることを許可されているユーザが、認証後も認証 VLAN に残されている。
条件	ユーザは正しく認証されていますが、ネットワークにアクセスできません。
考えられる原因	• 管理者が、正しい許可プロファイルを指定していない可能性があります。 • 管理者が、ユーザのアクセス レベルに該当するポリシー条件を定義していません。 • 許可プロファイル自体が、適切にフレーミングされていない可能性があります。
解決策	該当するユーザ グループに必要な許可プロファイルをサポートするように、ID グループ条件が適切に定義されていることを確認します。 **1.** [操作（Operations）] > [認証（Authentication）] を選択します。 **2.** ユーザが属する ID グループを検索します。 **3.** その ID グループ用に選択された許可プロファイルを検索します。 **4.** [ポリシー（Policy）] > [許可（Authorization）] を選択し、その ID グループに対して正しいルールが一致していることを確認します。 **5.** 一致していない場合には、正しい許可ポリシーが一致していない理由をデバッグします。

許可ポリシーが機能していない

症状または問題	管理者によって指定された許可ポリシーは正しいものですが、エンドポイントは、設定された VLAN IP を受け取っていません。
条件	この問題は、有線環境の標準ユーザ許可セッションに該当します。
考えられる原因	事前許可 ACL が DHCP トラフィックをブロックしている可能性があります。

解決策	• スイッチ上の Cisco IOS リリースが、Cisco IOS Release 12.2.(53)SE と同じか、または新しいリリースであることを確認します。
	• ID グループ条件が適切に定義されていることを確認します。
	• アクセス スイッチ上で **show vlan** コマンドを使用して、クライアント マシン ポート VLAN があるかどうかを確認します。ポートに正しい許可プロファイル VLAN が表示されていない場合、DHCP サーバに到達するためには VLAN エンフォースメントが適切であることを確認します。VLAN が正しい場合には、事前許可 ACL が DHCP トラフィックをブロックしている可能性があります。事前許可 DACL が次のとおりであることを確認します。
	`remark Allow DHCP`
	`permit udp any eq bootpc any eq bootps`
	`remark Allow DNS`
	`permit udp any any eq domain`
	`remark ping`
	`permit icmp any any`
	`permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect`
	`permit tcp any host 80.0.80.2 eq www`
	`permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal port`
	`permit tcp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8906 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`deny ip any any`
	• セッションは、**show epm session summary** コマンドを入力することによって、スイッチ上に作成されることを確認します。表示されたセッションの IP アドレスが「使用できない」場合は、スイッチに次の設定行が表示されることを確認します。
	`ip dhcp snooping vlan 30-100`
	`ip device tracking`

スイッチがアクティブ AAA セッションをドロップしている

症状または問題	802.1X および MAB 認証と許可は成功したが、スイッチがアクティブ セッションをドロップしており、**epm session summary** コマンドでアクティブ セッションが表示されません。
条件	これは、正常にログインした後、スイッチによって終了されるユーザ セッションに適用されます。
考えられる原因	• NAD 上の事前認証 ACL（および Cisco ISE からの後続の DACL エンフォースメント）が、そのセッションに対して正しく設定されていない可能性があります。 • 事前認証 ACL が設定され、DACL が Cisco ISE からダウンロードされていますが、スイッチがセッションをダウンさせます。 • Cisco ISE が（正しい）ポストポスチャ VLAN ではなく、プリポスチャ VLAN 割り当てを適用している可能性があり、そのためセッションがダウンしている可能性があります。

解決策	• スイッチ上の Cisco IOS リリースが、Cisco IOS Release 12.2.(53)SE と同じか、または新しいリリースであることを確認します。
	• Cisco ISE の DACL 名に空白（ハイフン「-」の周辺の場合が多い）が含まれているかどうかを確認します。DACL 名には、スペースを含めないようにする必要があります。次に、DACL 構文が正しく、余分なスペースが含まれていないことを確認します。
	• DACL を適切に解釈するため、スイッチに次の設定が存在することを確認します（設定が有効ではない場合は、スイッチがセッションを終了する可能性があります）。
	`radius-server attribute 6 on-for-login-auth`
	`radius-server attribute 8 include-in-access-req`
	`radius-server attribute 25 access-request include`
	`radius-server vsa send accounting`
	`radius-server vsa send authentication`

クライアント マシン上の URL リダイレクションが失敗する

症状または問題	クライアント マシンのブラウザ内の URL リダイレクション ページで、エンド ユーザが適切な URL に正しくガイドされません。
条件	この問題は、URL リダイレクションを必要とする 802.1X 認証セッション、およびゲスト Centralized Web Authentication（CWA）ログイン セッションで最もよく発生します。
考えられる原因	（この問題には、複数の原因があります。詳細については、「**解決策**」の説明を参照してください）

解決策

- 許可プロファイルで設定されている 2 つの Cisco AV ペアは、次の例と正確に一致している必要があります。（注：「IP」を実際の Cisco ISE IP アドレスで置換しないでください）。
  - url-redirect=https://ip:8443/guestportal/gateway?...lue&action=cpp
  - url-redirect-acl=ACL-WEBAUTH-REDIRECT（この ACL がアクセス スイッチでも定義されていることを確認してください）
- スイッチ上で **show epm session ip** <*session IP*> コマンドを入力することにより、ACL の URL リダイレクション部分がセッションに適用されていることを確認します （ここでセッション IP は、DHCP サーバによってクライアント マシンに渡される IP アドレスです）。

```
Admission feature : DOT1X
AAA Policies : #ACSACL#-IP-Limitedaccess-4cb2976e
URL Redirect ACL : ACL-WEBAUTH-REDIRECT
URL Redirect :
https://node250.cisco.com:8443/guestportal/gateway?sessionId=0A000A72
0000A45A2444BFC2&action=cpp
```

- Cisco ISE 許可プロファイルから適用されるプリポスチャ評価 DACL は、次のコマンドラインを含んでいることを確認します。

```
remark Allow DHCP
permit udp any eq bootpc any eq bootps
remark Allow DNS
permit udp any any eq domain
remark ping
permit icmp any any
permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect
permit tcp any host 80.0.80.2 eq www --> Provides access to internet
permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal
port
permit tcp any host 80.0.80.2 eq 8905 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
permit udp any host 80.0.80.2 eq 8905 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
permit udp any host 80.0.80.2 eq 8906 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
deny ip any any
```

（注） URL リダイレクトに適切な Cisco ISE FQDN が存在することを確認します。

解決策（続き）	• 「ACL-WEBAUTH_REDIRECT」という名前の ACL が、次のスイッチに存在することを確認します。
	`ip access-list extended ACL-WEBAUTH-REDIRECT`
	` deny ip any host 80.80.80.2`
	` permit tcp any any eq www`
	` permit tcp any any eq 443`
	` permit tcp any any eq 8443`
	• スイッチ上で HTTP サーバおよび HTTPS サーバが動作していることを確認します。
	`ip http server`
	`ip http secure-server`
	• クライアント マシンにパーソナル ファイアウォールが導入されている場合は、無効になっていることを確認します。
	• クライアント マシン ブラウザが、プロキシを使用するように設定されていないことを確認します。
	• クライアント マシンと Cisco ISE IP アドレス間の接続を確認します。
	• Cisco ISE が分散環境に展開されている場合は、クライアント マシンが Policy Service ISE ノード FQDN を認識することを確認します。
	• Cisco ISE FQDN が解決され、クライアント マシンから到達可能であることを確認します。

クライアント マシン上のエージェントのダウンロードの問題

症状または問題	ユーザの認証と許可の後、クライアント マシン ブラウザに「ポリシーが一致しません（no policy matched）」のエラー メッセージが表示されます。
条件	この問題は、認証のクライアント プロビジョニング フェーズ中のユーザ セッションに該当します。
考えられる原因	クライアント プロビジョニング リソース ポリシーに必要な設定が欠落している可能性があります。
解決策	• クライアント プロビジョニング ポリシーが Cisco ISE に存在することを確認します。存在する場合は、ポリシー内に定義されているポリシー ID グループ、条件およびエージェントのタイプを確認します （また、すべてデフォルト値のプロファイルも含め、[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [クライアント プロビジョニング（Client Provisioning）] > [リソース（Resources）] > [追加（Add）] > [ISE ポスチャ エージェント プロファイル（ISE Posture Agent Profile）] で設定されたエージェント プロファイルが存在するかどうかについても確認します)。 • アクセス スイッチのポートをバウンスすることにより、クライアント マシンの再認証を試行します。

（注） クライアント プロビジョニング エージェント インストーラのダウンロードには、次の要件を満たす必要があることに注意してください。

- エージェントを初めてクライアント マシンにインストールする場合、ユーザはブラウザ セッションで ActiveX インストーラを許可する必要があります（クライアント プロビジョニング ダウンロード ページでは、この情報の指定を求められます）。
- クライアント マシンには、インターネット アクセスが必要です。

エージェント ログイン ダイアログが表示されない

症状または問題	クライアント プロビジョニングの後にユーザに対して、エージェント ログイン ダイアログボックスが表示されません。
条件	この問題は通常、ユーザ認証セッションのポスチャ評価フェーズで発生します。
考えられる原因	このタイプの問題に対しては、複数の原因が考えられます。詳細については、次の「**解決策**」の説明を参照してください。

解決策	• エージェントがクライアント マシン上で動作していることを確認します。
	• スイッチ上の Cisco IOS リリースが、Cisco IOS Release 12.2.(53)SE と同じか、または新しいリリースであることを確認します。
	• Cisco NAC Agent または Mac OS X Agent の Discovery Host アドレスが、Cisco ISE FQDN を示していることを確認します（**NAC Agent** アイコンを右クリックし、[プロパティ（Properties）] を選択して Discovery Host を確認します）。
	• アクセス スイッチで、Cisco ISE とエンド クライアント マシン間の SWISS 通信が許可されていることを確認します。セッションに適用される制限されたアクセス ACL では、SWISS ポートが許可されている必要があります。
	`remark Allow DHCP`
	`permit udp any eq bootpc any eq bootps`
	`remark Allow DNS`
	`permit udp any any eq domain`
	`remark ping`
	`permit icmp any any`
	`permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect`
	`permit tcp any host 80.0.80.2 eq www --> Provides access to internet`
	`permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal port`
	`permit tcp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`deny ip any any`
	• それでもエージェント ログイン ダイアログが表示されない場合は、証明書に問題がある可能性があります。エンド クライアントの SWISS 通信に使用される証明書が、Cisco ISE の証明書信頼リストにあることを確認します。
	• クライアント マシンからデフォルト ゲートウェイに到達可能であることを確認します。

エージェントがポスチャ評価の開始に失敗する

症状または問題	ユーザに対して「Clean Access Server が使用できません（Clean access server not available）」というメッセージが表示されます。
条件	この問題は、Cisco ISE からのすべてのエージェント認証セッションに適用されます。
考えられる原因	このエラーは、セッションが終了していること、またはネットワーク上で Cisco ISE が到達不可能となったことのいずれかを意味する場合があります。
解決策	• ユーザは、デフォルト ゲートウェイや RADIUS サーバ IP アドレス、またはネットワーク管理者によって提供された FQDN の ping を試みることができます。 • ユーザは、ネットワークに再度ログインを試みることができます。 • 管理者は、ユーザのネットワーク アクセス属性（割り当てられた VLAN、ACL、ルーティング、クライアントでの **nslookup** コマンドの実行、クライアント マシン DNS 接続など）を確認できます。

エージェントに「一時的なアクセス」が表示される

症状または問題	管理者とユーザはフル ネットワーク アクセスを想定していますが、ログインと認証の後にクライアント マシンに「一時的なアクセス」が付与されます。
条件	この問題は、エージェントを使用して接続するクライアント マシンのログイン セッションで発生します。
考えられる原因	クライアントで NAC Agent が動作しているときに、次の状態で問題が発生する可能性があります。 • クライアント マシンのインターフェイスがダウンした場合 • セッションが終了した場合
解決策	ユーザは、ネットワーク接続を確認して再度ログインを試行し（またポスチャ評価を通過し）、接続の再構築を試みる必要があります。

認証の後に Cisco ISE が CoA を発行しない

症状または問題	クライアント マシンのログインと認証の後に、CoA が発行されません。
条件	この特定の問題は、認証を完了するためにクライアント マシンで CoA が必要な有線環境でのみ発生します。
考えられる原因	クライアント マシンの CoA をサポートするのに必要な設定が、アクセス スイッチに存在しない可能性があります。

解決策	• スイッチ上の Cisco IOS リリースが、Cisco IOS Release 12.2.(53)SE と同じか、または新しいリリースであることを確認します。
	• CoA を有効にするのに必要な次のコマンドが、スイッチ設定に装備されていることを確認します。
	`aaa server radius dynamic-author`
	`client 80.0.80.2 server-key cisco456 --> ISE ip.`
	`server-key cisco456`

エラー メッセージ

この項では、次のトピックを扱います。

ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS

説明	この認証失敗メッセージは、ユーザのクレデンシャルが無効であることを示しています。
解決策	Active Directory ドメインへの接続に使用される Active Directory ユーザ アカウントおよびクレデンシャルが正しいか確認します。

ACTIVE_DIRECTORY_USER_AUTH_FAILED

説明	この認証失敗メッセージは、ユーザ認証が失敗したことを示しています。このメッセージは、Active Directory でユーザまたはマシン パスワードが見つからない場合に表示されます。
解決策	Active Directory ドメインへの接続に使用される Active Directory ユーザ アカウントおよびクレデンシャルが正しいか確認します。

ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED

説明	この認証失敗メッセージは、ユーザのパスワードの期限が切れている場合に表示されます。
解決策	Active Directory のユーザ アカウントが有効な場合は、Active Directory 内のアカウントをリセットします。ユーザ アカウントの期限が切れている場合で、そのアカウントがまだ必要である場合は、ユーザ アカウントを更新します。ユーザ アカウントの期限が切れており、すでに有効ではない場合は、試行の理由を調べます。

ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

説明	この認証失敗メッセージは、ユーザが不正なパスワードを入力した場合に表示されます。
解決策	Active Directory ドメインへの接続に使用される Active Directory ユーザ アカウントおよびクレデンシャルが正しいか確認します。

ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED

説明	この認証失敗メッセージは、Active Directory でユーザ アカウントが無効になった場合に表示されます。
解決策	Active Directory のユーザ アカウントが有効な場合は、Active Directory 内のアカウントをリセットします。ユーザ アカウントの期限が切れている場合で、そのアカウントがまだ必要である場合は、ユーザ アカウントを更新します。ユーザ アカウントの期限が切れており、すでに有効ではない場合は、試行の理由を調べます。

ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS

説明	この認証失敗メッセージは、制約のある時間内にユーザがログインした場合に表示されます。
解決策	ユーザ アクセスが有効な場合、Active Directory 内のユーザ アクセス ポリシーを更新します。ユーザ アクセスが無効な（現時点で制限されている）場合、試行の理由を調べます。

ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD

説明	この認証失敗メッセージは、ユーザのパスワードがパスワード ポリシーに準拠していない場合に表示されます。
解決策	Active Directory のパスワード ポリシーに準拠するように、Active Directory 内のパスワードを再設定します。

ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN

説明	この認証失敗メッセージは、Active Directory が指定されたドメインを見つけられない場合に表示されます。
解決策	Administration ISE ノード ユーザ インターフェイスの Active Directory の設定、および Cisco ISE CLI の DNS[1] 設定を確認します。

1. DNS = ドメイン ネーム サービス

ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED

説明	このメッセージは、Active Directory のユーザ アカウントの期限が切れている場合に表示されます。
解決策	ユーザ アカウントの期限が切れている場合で、そのアカウントがまだ必要な場合は、ユーザ アカウントを更新します。ユーザ アカウントの期限が切れており、すでに有効ではない場合は、試行の理由を調べます。

ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT

説明	この認証失敗メッセージは、ユーザ アカウントがロックアウトされている場合に表示されます。
解決策	ユーザが正しいクレデンシャルでログインを試行する場合、ユーザのパスワードをリセットします。それ以外の場合は、ロックアウトの原因となる試行を調査します。

ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED

説明	この認証失敗メッセージは、Active Directory がグループを取得できない場合に表示されます。
解決策	Administration ISE ノード ユーザ インターフェイス内の Active Directory の設定が正しいかどうかを確認します。

ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED

説明	この認証失敗メッセージは、Active Directory でマシン認証が有効になっていない場合に表示されます。
解決策	必要に応じて、Active Directory のマシン認証を有効にします。

ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED

説明	この認証失敗メッセージは、Active Directory が指定された属性を取得できない場合に表示されます。
解決策	Administration ISE ノード ユーザ インターフェイス内の Active Directory の設定が正しいかどうかを確認します。

ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED

説明	この認証失敗メッセージは、Active Directory でパスワード変更オプションが無効になっている場合に表示されます。
解決策	必要に応じて、Active Directory のパスワード変更を有効にします。

ACTIVE_DIRECTORY_USER_UNKNOWN

説明	この無効ユーザ メッセージは、Active Directory でユーザ情報が見つからない場合に表示されます。
解決策	無効な試行の発信元を確認します。発信元が有効なユーザの場合は、Active Directory でユーザ アカウントが正しく設定されていることを確認します。

ACTIVE_DIRECTORY_CONNECTION_FAILED

説明	この外部エラー メッセージは、Cisco ISE が Active Directory との接続を構築できない場合に表示されます。
解決策	Administration ISE ノード ユーザ インターフェイス内の Active Directory の設定が正しいかどうかを確認します。

ACTIVE_DIRECTORY_BAD_PARAMETER

説明	この外部エラー メッセージは、無効な入力を行った場合に表示されます。
解決策	Administration ISE ノード ユーザ インターフェイス内の Active Directory の設定が正しいかどうかを確認します。

ACTIVE_DIRECTORY_TIMEOUT

説明	この外部エラー メッセージは、タイムアウト イベントが発生した場合に表示されます。
解決策	Administration ISE ノード ユーザ インターフェイス内の Active Directory の設定が正しいかどうかを確認します

API のトラブルシューティング

次のトラブルシューティング API を使用して、一般的なトラブルシューティング プロセスで利用できる情報を Cisco ISE に問い合わせることができます。

- **ノードのバージョンとタイプの取得（Version）**
  https://{hostname}/ise/mnt/api/Version
- **障害理由マッピングの取得（FailureReasons）**
  https://{hostname}/ise/mnt/api/FailureReasons
- **セッション認証ステータスの取得（AuthStatus）**
  https://{hostname}/ise/mnt/api/AuthStatus/MACAddress/{mac}/{seconds}/{number of records per MAC Address}/All
- **セッション アカウンティング ステータスの取得（AcctStatusTT）**
  https://{hostname}/ise/mnt/api/AcctStatusTT/MACAddress/{mac}/{seconds}

アクティブ セッション リスト/カウント API

アクティブ セッション カウントを取得する API

- **Session Directory 内のアクティブ セッション カウントの取得（ActiveCount）**
  https://{mnt-node}/ise/mnt/api/Session/ActiveCount
- **ポスチャ サービスを使用する Session ディレクトリ内のアクティブ セッション カウントの取得（PostureCount）**
  https://{mnt node}/ise/mnt/api/Session/PostureCount
- **プロファイラ サービスを使用する Session ディレクトリ内のアクティブ セッション カウントの取得（ProfilerCount）**
  https://{mnt node}/ise/mnt/api/Session/ProfilerCount

アクティブ セッション リストを取得する API

- **Session ディレクトリ内のアクティブ セッション キー情報の取得（ActiveList）**
  https://{mnt node}/ise/mnt/api/Session/ActiveList
- **指定された期間中に認証された Session ディレクトリ内のアクティブ セッション キー情報の取得（AuthList）**
  https://{mnt node}/ise/mnt/api/Session/AuthList/{start time}/{end time}

詳細情報：

- このリリースでのトラブルシューティング API の使用の詳細については、『*Cisco Identity Services Engine API Reference Guide, Release 1.1.x*』を参照してください。

（注） また、『*Cisco Identity Services Engine API Reference Guide, Release 1.1.x*』でも、サポートされているセッション管理および CoA API に関する情報を提供します。

Cisco Technical Assistance Center への問い合わせ

上記の項で問題の原因とその解決策が見つからない場合は、問題を解決するためのその後の最善の処理について製品を購入されたシスコの代理店にお問い合わせください。Cisco Technical Assistance Center（TAC）に関しては、アプライアンスに付属する『*Cisco Information Packet*』を参照するか、または次の Web サイトを参照してください。

http://www.cisco.com/tac/

Cisco TAC に連絡する前に、以下の情報を用意しておいてください。

- アプライアンスのシャーシ タイプおよびシリアル番号。
- 保守契約または保証書（『*Cisco Information Packet*』を参照）。
- ソフトウェアの名前とタイプ、バージョンまたはリリースの番号（該当する場合）。
- 新しいアプライアンスを入手した日付。
- 問題または状況が発生したときの簡単な説明、問題を切り分けまたは再現するための手順、問題を解決するために実行する手順の説明。

（注） カスタマー サービス担当者には、必ず Cisco ISE 3300 シリーズ アプライアンスの初期インストール後に行ったアップグレードまたは保守の情報をすべてお伝えください。サイト ログ情報については、『*Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.1*』の「Creating a Site Log」の項を参照してください。