Cisco Identity Services Engine リリース3.1 リリースノート

Cisco Identity Services Engine の概要

Cisco Identity Services Engine（ISE）は、ネットワークリソースへのセキュアなアクセスを提供するセキュリティポリシー管理プラットフォームです。企業は、Cisco ISE を使用して、ネットワーク、ユーザー、およびデバイスからコンテキスト情報をリアルタイムで収集できます。その後、管理者はこの情報を使用して、積極的に管理上の決定を下すことができます。これを行うには、アクセススイッチ、ワイヤレスコントローラ、バーチャルプライベートネットワーク（VPN）ゲートウェイ、5GaaS ネットワーク、データセンタースイッチなどのさまざまなネットワーク要素のアクセスコントロールポリシーを作成します。Cisco ISE は、Cisco TrustSec ソリューションのポリシーマネージャとして機能し、TrustSec ソフトウェアによって定義されたセグメンテーションをサポートします。

Cisco ISE は、異なるパフォーマンス特性を持つセキュアなネットワーク サーバー アプライアンス上で使用できます。また、仮想マシン（VM）上で実行できるソフトウェアとしても使用可能です。パフォーマンス向上のためにアプライアンスを展開に追加できます。

Cisco ISE は、スタンドアロンおよび分散展開をサポートする拡張性の高いアーキテクチャを使用しますが、設定および管理は一元化されています。また、ペルソナとサービスの設定と管理を個別に行うこともできます。このため、ネットワーク内で必要なサービスを作成して適用することができますが、Cisco ISE 展開を完全な統合システムとして運用することもできます。

Cisco ISE の詳細な発注およびライセンス情報については、 *Cisco IdentityServices Engine* 注文ガイド [英語] を参照してください。

システムのモニタリングおよびトラブルシューティングに関する詳細については、『 *Cisco Identity Services Engine* 管理者ガイド』の「Cisco ISE のモニタリングとトラブルシューティング サービス」のセクションを参照してください。

Cisco ISE リリース 3.1 の新機能

このセクションでは、Cisco ISE 3.1 の新機能と変更された機能をすべて示します。

（注） Software Download site [英語] で Cisco ISE 3.1 OVA、ISO、およびアップグレード バンドル ファイルが置き換えられました。詳細については、Cisco ISE ソフトウェア ダウンロード サイトでの Cisco ISE 3.1 ファイルの置き換え （47 ページ）を参照してください。

ネイティブ サプリカント プロファイル向け Android の設定

ネイティブ サプリカント プロファイルに Android 設定が追加されました。Certificate Enrollment Protocol では、次のいずれかのオプションを選択できます。

- Enrollment over Secure Transport（EST）
- Simple Certificate Enrollment Protocol（SCEP）

EST プロトコルを選択した場合、Cisco ISE は、証明書を発行する一方、Android ユーザーに対して追加のパスワードの入力を要求します。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Compliance」の章にある「Native Supplicant Profile Settings」を参照してください。

監査ログの機能強化

次の監査ログが機能強化され、関連するイベントに関してより詳細な情報が含まれるようになりました。

- ポスチャ監査ログには、次に関する情報が含まれるようになりました。
  - ポスチャポリシーの作成と削除。
  - [条件（Conditions）]、[ルール名（Rule Name）] などのフィールドに対する変更など、既存のポスチャポリシーに加えられた変更。
  - [条件（Conditions）]、[修復アクション（Remediation Actions）]、[要件（Requirements）] などのポスチャ設定の追加、削除、または変更。
- RBAC 監査ログに、既存のメニューアクセスおよびデータアクセスコンテンツの作成と削除に関する情報が含まれるようになりました。
- ネットワークアクセスおよび管理ユーザーの監査ログに、ネットワークアクセスおよび管理ユーザーの作成、編集、および削除に関する情報が含まれるようになりました。

双方向ポスチャフロー

ポスチャステータスが準拠していない場合に、指定した間隔で Cisco ISE をプローブするように AnyConnect を設定できます。これにより、クライアントが保留状態でスタックするのを防ぐことができます。

双方向ポスチャフローは、Windows、Linux、および MacOS クライアントでサポートされます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Compliance」の章の「Bidirectional Posture Flow」を参照してください。

Cisco Support Diagnostics Connector を使用した設定バックアップの取得

Cisco Support Diagnostics Connector を使用して、設定のバックアップをトリガーし、バックアップファイルを Cisco Support Diagnostics フォルダにアップロードします。Cisco Support Diagnostics フォルダにバックアップファイルをアップロードした後、そのバックアップファイルは Cisco ISE ローカルディスクから削除できます。この機能を使用するには、Cisco ISE でスマートライセンスと Cisco Support Diagnostics を有効にする必要があります。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Troubleshoot」の章の「Obtain Configuration Backup Using Cisco Support Diagnostics Connector」を参照してください。

認証結果アラームの設定

認証ポリシーの結果に基づいてアラームを設定できるため、エンドポイント認証に対するネットワーキング、インフラストラクチャ、またはアプリケーションの変更の影響をモニターできます。特定のネットワーク デバイス グループ（NDG）を選択して、アラームの範囲を定義できます。選択した NDG ごとに、新しい認証結果アラームが作成されます。

特定の認証プロファイルとセキュリティグループタグ（SGT）を選択することで、このアラームでモニターする認証ログをフィルタリングできます。指定された認証プロファイルおよび SGT を持つ認証ポリシーセットを満たしているエンドポイントのみがアラームによってモニターされます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Troubleshoot」の章の「Configure Authorization Result Alarm」を参照してください。

優先ドメインコントローラの設定

ドメインフェールオーバーの場合に使用するドメインコントローラを指定できます。ドメインが失敗した場合、Cisco ISE は優先リストに追加されたドメインコントローラの優先順位スコアを比較し、優先順位スコアが最も高いドメインコントローラを選択します。そのドメインコントローラがオフラインであるか、何らかの問題により到達不能である場合、優先リスト内で優先順位スコアが次に高いドメインコントローラが使用されます。優先リスト内のすべてのドメインコントローラがダウンしている場合は、リスト外のドメインコントローラが優先順位スコアに基づいて選択されます。フェールオーバーの前に使用されていたドメインコントローラが復元されると、Cisco ISE はそのドメインコントローラに切り替えます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Asset Visibility」の章にある「Configure Preferred Domain Controllers」を参照してください。

コンテキストの可視性の機能拡張

- CSV ファイルを変更せずに Cisco ISE にインポートできる属性のみをエクスポートする場合、[エンドポイントのエクスポート（Export Endpoints）] ダイアログボックスで、[インポート可能のみ（Importable Only）] チェックボックスをオンにできるようになりました。このオプションを使用すると、Cisco ISE にインポートする前に、エクスポートされた CSV ファイルの列またはメタデータを変更する必要がなくなります。

- [クイックフィルタ（Quick Filter）] または [高度なフィルタ（Advanced Filter）] オプションを使用している場合、[フィルタ済みのエクスポート（Export Filtered）] オプションを使用して、フィルタ済みのエンドポイントのみをエクスポートできます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Asset Visibility」の章にある「Export Endpoints Using CSV File」を参照してください。

Cisco ISE GUI に追加されたフルアップグレードと分割アップグレードのオプション

[管理（Administration）] > [システム（System）] > [アップグレード（Upgrade）] > [アップグレードを選択（Upgrade Selection）] ウィンドウで、要件に応じて次のオプションのいずれか 1 つを選択できます。

- [フルアップグレード（Full Upgrade）]：フルアップグレードは、Cisco ISE 展開の連続した完全なアップグレードを可能にするマルチステッププロセスです。これにより、すべてのノードが並行してアップグレードされ、分割アップグレードプロセスよりも短時間でアップグレードされます。すべてのノードが並行してアップグレードされるため、アップグレードプロセス中にサービスがダウンします。
- [分割アップグレード（Split Upgrade）]：分割アップグレードは、アップグレードプロセス中にユーザーがサービスを引き続き利用できるようにしながら、Cisco ISE 展開のアップグレードを可能にするマルチステッププロセスです。分割アップグレードオプションを使用する場合、アップグレードするノードを選択できます。

詳細については、『*Cisco Identity Services Engine Upgrade Journey, Release 3.1*』の「Upgrade Method」の章にある「Upgrade a Cisco ISE Deployment from the GUI」を参照してください。

Amazon Web Service における Cisco ISE

Cloud Formation テンプレート（CFT）または Amazon マシンイメージ（AMI）を使用して、Amazon Web Services（AWS）プラットフォームで Cisco ISE インスタンスを起動できます。

詳細については、『*Cisco Identity Services Engine Installation Guide, Release 3.1*』の「Install Cisco ISE with AmazonWeb Services」の章を参照してください。

仮想アプライアンスのライセンス

Cisco ISE リリース 3.1 以降は ISE VM ライセンスをサポートしています。これは、リリース 3.1 以前にサポートされていた VM Small、VM Medium、および VM Large ライセンスに代わるものです。新しい ISE VM ライセンスは、オンプレミス展開とクラウド展開の両方の Cisco ISE VM ノードを対象としています。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Licensing」の章にある「Cisco ISE Licenses」を参照してください。

ローカルディスクからのファイルのダウンロードまたはアップロード

ローカルディスク管理に使用されるファイルは、簡単に追加、ダウンロード、または削除できます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Maintain and Monitor」の章の「Download and Upload Files from Local Disk」を参照してください。

ポスチャポリシー設定の MacOS バージョン

Cisco ISE 3.0 以前では、MacOS 11.1、MacOS 11.2 などのマイナーな MacOS バージョンでポスチャポリシーと要件を設定できました。Cisco ISE 3.1 では、MacOS 11（All）などのメジャーな MacOS バージョンのみを選択して、ポスチャポリシーと要件を設定できます。

Cisco ISE 3.1 にアップグレードすると、MacOS のマイナーバージョンを含むポスチャ条件は、対応する MacOS のメジャーバージョンに自動的に更新されます。たとえば、MacOS 11.1 用に設定されたポスチャ条件は、MacOS 11（All）に更新されます。

OpenAPI サービス

OpenAPI は、ポート 443 を介して動作する HTTPS に基づく REST API です。Cisco ISE 3.1 以降では、新しい API を OpenAPI 形式で使用できます。Cisco ISE OpenAPI の詳細については、https://<*ise-ip*>/api/swagger-ui/index.html を参照してください。

Cisco ISE 3.1 では、次の OpenAPI が導入されています。

- リポジトリの管理
- 設定データのバックアップと復元
- 証明書の管理
- ポリシー管理
    - RADIUS ポリシー
    - TACACS+ ポリシー

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Basic Setup」の章にある「Enable API Service」を参照してください。

Linux オペレーティングシステムのポスチャサポート

ポスチャは、ネットワークに接続されているすべてのエンドポイントの社内セキュリティポリシーの遵守に関するステートを確認できる、Cisco ISE のサービスです。Cisco ISE 3.1 は、Windows および Mac オペレーティングシステムに加えて、次の Linux オペレーティングシステムのバージョンをサポートします。

- Ubuntu
    - 18.04

- 20.04

- Red Hat
  - 7.5
  - 7.9
  - 8.1
  - 8.2
  - 8.3

- SuSE
  - 12.3
  - 12.4
  - 12.5
  - 15.0
  - 15.1
  - 15.2

Linux オペレーティングシステムでは、次のポスチャ条件がサポートされています。

- ファイル条件
- アプリケーション条件
- マルウェア対策条件
- パッチ管理条件

Linux クライアントのエージェントプロファイルを設定できます。AnyConnect Linux クライアントのクライアント プロビジョニング リソースを追加できます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Compliance」の章を参照してください。

VMware Cloud 環境での ERS サービスの自動有効化

Cisco ISE の Amazon マシンイメージ（AMI）バージョンが VMware クラウド環境に展開されている場合、外部 RESTful サービス（ERS）API サービスはデフォルトで有効になっています。これにより、Cisco ISE GUI から ERS サービスを有効にすることなく、Cisco ISE と他のシスコ製品およびサードパーティ製アプリケーションを簡単に統合できます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Basic Setup」の章にある「Enable API Service」を参照してください。

pxGrid クライアント自動承認 API

Cisco pxGrid を使用して、Cisco ISE セッションディレクトリからの状況依存情報を、Cisco ISE エコシステムのパートナーシステムなどの他のネットワークシステムやシスコの他のプラットフォームと共有できます。PxGrid クライアント自動承認 API を使用して、次のことができます。

- 新しい pxGrid クライアントからの証明書ベースの接続要求の自動承認を有効にします。環境内のすべてのクライアントを信頼している場合にのみ、このオプションを有効にします。
- pxGrid クライアントのユーザー名またはパスワードベースの認証を有効にします。このオプションを有効にした場合、pxGrid クライアントを自動的に承認することはできません。pxGrid クライアントは、REST API を介してユーザー名を送信することで、pxGrid コントローラに自身を登録できます。pxGrid コントローラは、クライアント登録時に pxGrid クライアントのパスワードを生成します。管理者は接続要求を承認または拒否できます。

pxGrid クライアント自動承認 API の詳細については、ERS SDK の「pxGrid Settings」のセクションを参照してください。次の URL で ERS SDK にアクセスできます。

https://<ISE-Admin-Node>:9060/ers/sdk

（注） [ERS 管理者（ERS Admin）] のロールを持つユーザーのみが、ERS SDK にアクセスできます。

Active Directory アカウントに対するパスワードの最大試行回数の設定

不正なパスワードの試行が多すぎることが原因で Active Directory アカウントがロックアウトされるのを防ぐために、badPwdCount 属性を設定できます。Cisco ISE は、ユーザーを認証する前に、Cisco ISE で設定されている不正なパスワードの最大試行回数を Active Directory における badPwdCount 属性の現在の値と比較します。Cisco ISE で設定された不正なパスワードの最大試行回数が badPwdCount 属性の値と等しい場合、認証はドロップされ、Active Directory に送信されません。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Asset Visibility」の章にある「Configure Maximum Password Attempts for AD Account」を参照してください。

モバイルデバイス管理サーバーを使用した、ランダムで変化する MAC アドレスの処理

プライバシー対策として、モバイルデバイスおよび一部のデスクトップのオペレーティングシステムでは、接続先の SSID ごとにランダムで変化する MAC アドレスを使用することが増えています。Cisco ISE では、MAC アドレスの代わりに、GUID と呼ばれる一意のデバイス識別子を使用するように Cisco ISE を設定することで、この問題を回避できます。エンドポイントがモバイルデバイス管理（MDM）サーバーに登録されると、GUID 値を含む証明書が MDM サーバーからエンドポイントに送信されます。エンドポイントでは、Cisco ISE での認証にこの証明書が使用されます。Cisco ISE は、証明書からエンドポイントの GUID を受信します。

Cisco ISE と MDM サーバー間のすべての通信で、GUID を使用してエンドポイントが識別され、2 つのシステム間の精度と一貫性が確保されます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Secure Wired Access」の章にある「Handle Random and Change MAC Addresses With Mobile Device Management Servers」を参照してください。

BYOD の MAC ランダム化

Android 及び iOS デバイスでは、接続先の SSID ごとにランダムで変化する MAC アドレスを使用することが増えています。Cisco ISE および MDM システムは、サービスに接続するために使用する SSID に応じて、同じデバイスの異なる MAC アドレスを認識します。したがって、エンドポイントを識別するため、Cisco ISE プロビジョニングサービスによって一意の識別子が生成されます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Basic Setup」の章にある「MAC Randomization for BYOD」を参照してください。

エンドポイント API の機能拡張

logicalProfileName フィルタを使用して、特定の論理プロファイルに属するエンドポイントを取得できます。logicalProfileNamefilter でサポートされている演算子は EQ（等しい）です。このフィルタを使用して API を呼び出す構文は次のとおりです。

/ers/config/endpoint?filter={ファイル名}.{演算子}.{倫理プロファイル名}

詳細については、『Cisco ISE API Reference Guide』を参照してください。

ポスチャスクリプト修復

ポスチャ修復スクリプトを作成して Cisco ISE にアップロードし、エンドポイントのコンプライアンス違反の問題を解決できます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Compliance」の章にある「Add a Script Remediation」を参照してください。

RHEL 8.2 のサポート

Cisco ISE は、Red Hat Enterprise Linux（RHEL）に基づき、Cisco Application Deployment Engine オペレーティングシステム（ADEOS）で動作します。Cisco ISE 3.1 では、ADEOS は RHEL 8.2 に基づいています。

RHEL 8.2 は、次の VMware ESXi バージョンをサポートしています。

- VMware ESXi 6.5
- VMware ESXi 6.5 U1
- VMware ESXi 6.5 U2
- VMware ESXi 6.5 U3

- VMware ESXi 6.7
- VMware ESXi 6.7 U1
- VMware ESXi 6.7 U2
- VMware ESXi 6.7 U3
- VMware ESXi 7.0
- VMware ESXi 7.0 U1
- VMware ESXi 7.0 U2

詳細については、『*Cisco Identity Services Engine Upgrade Journey, Release 3.1*』の「Overview」の章を参照してください。.

SAML ベースの管理者ログイン

SAML ベースの管理者ログインは、SAML 2.0 標準規格を使用して Cisco ISE にシングルサインオン機能を追加します。Okta などの外部 ID プロバイダーや、SAML 2.0 を導入する任意の ID プロバイダーを使用できます。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Asset Visibility」の章にある「SAML-based Admin Login」を参照してください。

特定ライセンス予約

特定のライセンス予約は、組織のセキュリティ要件で Cisco ISE と Cisco Smart Software Manager（CSSM）間の永続的な接続が許可されていない場合にスマートライセンスを管理するためのスマートライセンス方式です。特定のライセンス予約では、Cisco ISE ノードで特定のライセンス権限を予約できます。

予約する必要があるライセンスのタイプと数を定義して特定のライセンス予約を作成し、Cisco ISE ノードで予約をアクティブ化します。登録して予約を有効にした Cisco ISE ノードは、ライセンスの使用を追跡し、ライセンス消費のコンプライアンスを適用します。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』、『』の「Licensing」の章にある「Specific License Reservation」を参照してください。

pxGrid 2.0 へのアップグレード

Cisco ISE リリース 3.1 以降、すべての pxGrid 接続は pxGrid 2.0 に基づく必要があります。pxGrid 1.0 ベース（XMPP ベース）の統合は、リリース 3.1 以降の Cisco ISE では動作しなくなります。

WebSocket に基づく pxGrid バージョン 2.0 は、Cisco ISE リリース 2.4 で導入されました。統合の中断を防ぐために、他のシステムを計画して pxGrid 2.0 準拠バージョンにアップグレードすることをお勧めします。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「pxGrid」の章を参照してください。

（注） **show application status ise** コマンドの出力には、pxGrid 1.0 サービスのステータスのみが反映されます。

ゼロタッチ プロビジョニング

ゼロタッチプロビジョニング（ZTP）は、手動介入なしで Cisco ISE のインストール、インフラストラクチャ サービスの有効化、パッチ適用、およびホットパッチ適用を自動化するのに役立つ、中断のないプロビジョニングメカニズムを指します。

詳細については、『*Cisco ISE Installation Guide, Release 3.1*』の「Additional Installation Information」の章にある「Zero Touch Provisioning」を参照してください。

Cisco Secure Access Control System から Cisco ISE への移行ツール

Cisco Secure Access Control System から Cisco ISE への移行ツールは、Cisco ISE 3.1 以降ではサポートされていません。Cisco Secure Access Control System のサポート終了日が発表されました。詳細については、「End-of-Life Notice」を参照してください。

システム要件

Cisco ISE の設定を継続使用する場合は、次のシステム要件が満たされていることを確認してください。

この Cisco ISE リリースのハードウェア プラットフォームとインストールの詳細については、『Cisco Identity Services Engine Hardware Installation Guide』を参照してください。

サポート対象ハードウェア

Cisco ISE リリース 3.1 は、次のプラットフォームにインストールできます。

表 *1*: サポートされるプラットフォーム

ハードウェア プラットフォーム	設定
Cisco SNS-3595-K9（大規模）	アプライアンスハードウェアの仕様については、『*Cisco Secure Network Server Appliance Hardware Installation Guide*』を参照してください。
Cisco SNS-3615-K9（小規模）	
Cisco SNS-3655-K9（中規模）	
Cisco SNS-3695-K9（大規模）	

インストール後、上記の表に記載されているプラットフォームで、管理、モニターリング、pxGrid などの特定のコンポーネントペルソナを使用して Cisco ISE を設定できます。これらの

ペルソナに加えて、Cisco ISE では、プロファイリングサービス、セッションサービス、脅威中心型 NAC サービス、TrustSec 用の SXP サービス、TACACS+ デバイス管理サービス、およびパッシブ ID サービスなど、ポリシーサービス内に他のタイプのペルソナが含まれています。

（注）

- Cisco ISE 3.1 は、Cisco Secured Network Server（SNS）3515 アプライアンスをサポートしていません。
- 16 GB 未満のメモリの割り当ては、VM アプライアンスの設定ではサポートされていません。Cisco ISE の動作に問題が発生した場合、すべてのユーザーは、Cisco Technical Assistance Center に連絡する前に、割り当てメモリを 16 GB 以上に変更する必要があります。

サポートされる仮想環境

Cisco ISE は次の仮想環境プラットフォームをサポートしています。

- - ESXi 6.5 の VMware バージョン 9
  - ESXi 6.7 以降の VMware バージョン 14

  次のパブリック クラウド プラットフォーム上の VMware クラウドソリューションに Cisco ISE を展開できます。
  - Amazon Web サービス（AWS）の VMware クラウド：Cisco ISE を AWS の VMware クラウドが提供するソフトウェアデファインド データセンターでホストします。
  - Azure VMware ソリューション：Azure VMware ソリューションは、Microsoft Azure 上でネイティブに VMware ワークロードを実行します。Cisco ISE を VMware 仮想マシンとしてホストできます。
  - Google Cloud VMware Engine：Google Cloud VMware Engine は、Google Cloud 上の VMware によってソフトウェアデファインド データセンターを実行します。VMware Engine によって提供されるソフトウェアデファインドデータセンターで、VMware 仮想マシンとして Cisco ISE をホストできます。
- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V
- QEMU 2.12.0-99 上の KVM
- Nutanix AHV 20201105.2096

（注） Cisco ISE 3.1 以降では、仮想マシン（VM）インスタンス（任意のペルソナを実行）のホスト間での移行に VMware マイグレーション機能を使用できます。Cisco ISE はホットマイグレーションとコールドマイグレーションの両方をサポートします。ホットマイグレーションは、ライブマイグレーションまたは vMotion とも呼ばれます。ホットマイグレーション中に Cisco ISE をシャットダウンしたり、電源をオフにしたりする必要はありません。可用性を損なうことなく、Cisco ISE VM を移行できます。

仮想マシンの要件に関する情報については、お使いの Cisco ISE バージョンの『*Cisco Identity Services Engine インストールガイド*』を参照してください。

連邦情報処理標準（FIPS）モードのサポート

Cisco ISE は、組み込みの連邦情報処理標準（FIPS）140-2 検証済み暗号化モジュール、Cisco FIPS オブジェクト モジュール バージョン 7.2（証明書 #3790）を使用します。FIPS コンプライアンス要求の詳細については、Global Government Certifications を参照してください。

Cisco ISE で FIPS モードが有効になっている場合は、次の点を考慮してください。

- すべての FIPS 非準拠暗号スイートは無効になります。
- 証明書と秘密キーには、FIPS 準拠ハッシュと暗号化アルゴリズムのみを使用する必要があります。
- RSA 秘密キーには、2048 ビット以上を指定する必要があります。
- 楕円曲線デジタル署名アルゴリズム（ECDSA）の秘密キーには、224 ビット以上を指定する必要があります。
- Diffie–Hellman Ephemeral（DHE）暗号方式は 2048 ビット以上の Diffie–Hellman（DH）パラメータを使用して動作します。
- SHA1 は、ISE ローカルサーバー証明書の生成を許可されていません。
- EAP-FAST の匿名 PAC プロビジョニングオプションは無効です。
- ローカル SSH サーバーは FIPS モードで動作します。
- RADIUS の場合、次のプロトコルは FIPS モードではサポートされていません。
  - EAP-MD5
  - PAP
  - CHAP
  - MS-CHAPv1
  - MS-CHAPv2
  - LEAP

検証済みブラウザ

Cisco ISE 3.1 は、次のブラウザで検証済みです。

- Mozilla Firefox 105 以前のバージョン（バージョン 82 以降）
- Mozilla Firefox ESR 91.3 以前のバージョン
- Google Chrome 106 以前のバージョン（バージョン 86 以降）
- Microsoft Edge の最新バージョンと最新バージョンより 1 つ前のバージョン

検証済み外部 ID ソース

（注） サポートされている Active Directory バージョンは、Cisco ISE と Cisco ISE-PIC の両方で同じです。

表 *2 :* 検証済み外部 *ID* ソース

外部 ID ソース	バージョン
Active Directory [1]	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 [2]	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019 [3]	Windows Server 2019
LDAP サーバー	
SunONE LDAP ディレクトリサーバー	バージョン 5.2
OpenLDAP ディレクトリサーバー	バージョン 2.4.23
任意の LDAP v3 準拠サーバー	LDAP v3 準拠のすべてのバージョン
トークンサーバー	
RSA ACE/サーバー	6.x シリーズ
RSA 認証マネージャ	7.x および 8.x シリーズ

外部 ID ソース	バージョン
Any RADIUS RFC 2865 準拠のトークン サーバー	RFC 2865 準拠のすべてのバージョン
セキュリティ アサーション マークアップ言語（SAML）シングルサインオン（SSO）	
Microsoft Azure	最新
Oracle Access Manager（OAM）	バージョン 11.1.2.2.0
Oracle Identity Federation（OIF）	バージョン 11.1.1.2.0
PingFederate サーバー	バージョン 6.10.0.4
PingOne クラウド	最新
セキュア認証	8.1.1
SAMLv2 準拠の ID プロバイダー	SAMLv2 準拠の任意の ID プロバイダバージョン
Open Database Connectivity（ODBC）アイデンティティソース	
Microsoft SQL Server	Microsoft SQL Server 2012
Oracle	Enterprise Edition リリース 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3
ソーシャルログイン（ゲストユーザーアカウントの場合）	
Facebook	最新

[1] Cisco ISE には最大 200 のドメインコントローラのみを追加できます。制限を超えると、次のエラーが表示されます：

```
<DC FQDN> の作成エラー：許可される DC の数が最大数 200 を超えています
```

[2] Cisco ISE は、Microsoft Windows Active Directory 2012 R2 のすべてのレガシー機能をサポートしていますが、保護ユーザーグループなどの Microsoft Windows Active directory 2012 R2 の新機能はサポートされていません。

[3] Cisco ISE 2.6 パッチ 4 は、Microsoft Windows Active Directory 2012 R2 のすべてのレガシー機能をサポートしています。

詳細については、『*Cisco Identity Services Engine Administrator Guide*』を参照してください。

サポート対象のウイルス対策およびマルウェア対策製品

Cisco ISE ポスチャエージェントでサポートされているウイルス対策およびマルウェア対策製品の詳細については、Cisco AnyConnect ISE ポスチャのサポート表を参照してください。

検証済み OpenSSL のバージョン

Cisco ISE 3.1 は、OpenSSL 1.1.1k で検証されています。

OpenSSL の更新には CA 証明書で CA:True であることが必要

証明書を CA 証明書として定義するには、証明書に次のプロパティが含まれている必要があります。

basicConstraints=CA:TRUE

このプロパティは、最近の OpenSSL 更新に準拠するために必須です。

既知の制限事項と回避策

このセクションでは、さまざまな既知の制限と対応する回避策に関する情報を提供します。

誤ったハッシュ値が原因で SNMP ユーザーの認証がアップグレード後に失敗する可能性

Cisco ISE 2.7 以前のリリースから Cisco ISE 3.1 にアップグレードする場合は、アップグレード後に SNMP ユーザーの設定を再設定する必要があります。そうしないと、誤ったハッシュ値が原因で SNMP ユーザーの認証が失敗する可能性があります。

SNMPv3 ユーザーの設定を再設定するには、次のコマンドを使用します。

no snmp-server user <*snmp user*> <*snmp version*> <*auth password*> <*priv password*>

snmp-server user <*snmp user*> <*snmp version*> <*auth password*> <*priv password*>

[名前（Name）]および[説明（Description）]フィールドでの特殊文字の使用に関する制限

- TACACS+ プロファイルおよびデバイス管理ネットワーク条件の [説明（Description）] フィールドでは、特殊文字 [%\<>*^:"|',=/()$.@;&-!#{}.?] は使用できません。サポートされる文字は、英数字、アンダースコア、およびスペースです。
- 認証プロファイルの [名前（Name）] および [説明（Description）] フィールドでは、特殊文字 %\<>*^:\"|',= は使用できません。[名前（Name）] および [説明（Description）] フィールドでサポートされる文字は、英数字、ハイフン、ドット、アンダースコア、およびスペースです。
- 時刻と日付の条件の [名前（Name）] および [説明（Description）] フィールドでは、 特殊文字 [%\#$&()~+*@{}!/?;:',=^`]"<>" は使用できません。[名前（Name）] および [説明

（Description）] フィールドで サポートされる文字は、英数字、ハイフン、ドット、アンダースコア、およびスペースです。

Make a Wish オプションは日本語では利用不可

Cisco ISE で日本語を有効にするようにローカライズ設定をしている場合、**Make a Wish** オプションは日本語では使用できないことに注意してください。

認証の Radius ログ

認証イベントの詳細は、[Radius認証（Radius Authentications）] ウィンドウの [詳細（Details）] フィールドで確認できます。認証イベントの詳細を使用できるのは7日間のみで、その後は認証イベントのデータを表示することはできません。すべての認証ログデータは、パージがトリガーされると削除されます。

Trustsec AAAサーバーリストのサーバー IP の更新

Cisco ISE インスタンスの IP アドレスを CLI を使用して変更すると、Cisco ISE サービスは再起動されます。サービスが起動した後、Trustsec AAA サーバーの IP アドレスを変更する必要があります。Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。**[ワークセンター（Workcenters）]** > **[TrustSec]** > **[コンポーネント（Components）]** > **[Trustsec サーバー（Trustsec Servers）]** > **[TrustSec AAAサーバー（Trustsec AAA Servers）]** を選択します。

EAP-TLS 認証が TPM モジュールを使用した証明書で失敗する

Cisco ISE リリース 3.1 では、Windows 10 で TPM モジュールを使用した証明書で EAP-TLS 認証が失敗することがあります。これは TPM モジュールの問題であり、Cisco ISE の問題ではありません。

回避策として、ルート CLI モードで Cisco ISE にアクセスし、次のスクリプトパスで Disable_RSA_PSS = '1' を設定します。

```
/opt/CSCOcpm/config/cpmenv.sh
```

この修正を適用するには、マシンを再起動してください。

アップグレード情報

リリース 3.1 へのアップグレード

次の Cisco ISE リリースからリリース 3.1 に直接アップグレードできます。

- 2.6
- 2.7
- 3.0

Cisco ISE リリース 2.6 より前のバージョンの場合は、まず上記のリリースのいずれかにアップグレードしてから、リリース 3.1 にアップグレードする必要があります。

アップグレードの開始前に、既存のバージョンで最新のパッチにアップグレードすることをお勧めします。

Cisco ISE 3.1 は、2.6 パッチ 9、2.7 パッチ 4、および 3.0 パッチ 2 と同等です。

アップグレードパッケージ

アップグレードパッケージおよびサポートされているプラットフォームに関する情報は、Cisco ISE Software Download から入手できます。

アップグレード手順の前提条件

- 設定されたデータを必要な Cisco ISE バージョンにアップグレードできるかどうかを確認するには、アップグレードの前にアップグレード準備ツール（URT）を実行します。ほとんどのアップグレードの失敗は、データのアップグレードの問題が原因で発生します。URT により実際のアップグレード前にデータを検証し、問題があれば報告します。URT は Cisco ISE Download Software Center からダウンロードできます。
- アップグレードの開始前に関連するすべてのパッチをインストールすることをお勧めします。

詳細については、『Cisco Identity Services Engine Upgrade Guide』を参照してください。

テレメトリ

インストール後の管理者ポータルへの初回ログイン時には、Cisco ISE テレメトリバナーが表示されます。この機能を使用して、Cisco ISE は、ユーザーの展開、ネットワーク アクセス デバイス、プロファイラ、およびユーザーが使用している他のサービスに関する非機密情報を安全に収集します。このデータは、今後のリリースでサービスを向上させ、より多くの機能を提供するために使用されます。デフォルトでは、テレメトリは有効になっています。アカウント情報を無効または変更するには、[管理（Administration）]>[設定（Settings）]>[ネットワーク設定診断（Network Settings Diagnostics）]>[テレメトリ（Telemetry）] を選択します。アカウントは、各展開に固有です。各管理者ユーザーが個別に提供する必要はありません。

Cisco ISE でテレメトリ機能が無効になり、テレメトリデータの共有が停止するまでに最大 24 時間かかる場合があります。

収集されるデータのタイプには、製品使用状況テレメトリや Cisco Support Diagnostics などがあります。

Cisco Support Diagnostics

Cisco Support Diagnostics Connector は、Cisco Technical Assistance Center（TAC）とシスコのサポートエンジニアがプライマリ管理ノードから展開の情報を取得するのに役立つ。デフォルト

では、この機能は無効になっています。この機能を有効にする手順については、『Cisco Identity Services Engine 管理者ガイド』を参照してください。

Cisco ISE ライブアップデートポータル

Cisco ISE ライブアップデートポータルは、**サプリカント プロビジョニング** ウィザード、AV/AS サポート（コンプライアンスモジュール）、およびクライアントプロビジョニングとポスチャポリシーサービスをサポートするエージェントインストーラ パッケージを自動的にダウンロードするのに役立ちます。このライブアップデートポータルは、Cisco ISE を使用して Cisco.com から該当するデバイスに最新のクライアントプロビジョニングおよびポスチャソフトウェアを直接取得するように、初期展開時に Cisco ISE で設定します。

デフォルトのアップデートポータル URL にアクセスできず、ネットワークにプロキシサーバーが必要な場合は、プロキシを設定します。ライブアップデートポータルにアクセスする前に、[管理（Administration）] > [システム（System）] > [設定（Settings）] > [プロキシ（Proxy）] の順に選択します。Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。プロキシ設定でプロファイラ、ポスチャ、およびクライアント プロビジョニング フィードへのアクセスが許可されている場合、Cisco ISE は MDM 通信のプロキシサービスをバイパスできないため、モバイルデバイス管理（MDM）サーバーへのアクセスがブロックされます。これを解決するには、MDM サーバーとの通信を許可するようにプロキシサービスを設定できます。プロキシ設定の詳細については、『Cisco Identity Services Engine Administrator Guide』の「Specify Proxy Settings in Cisco ISE」の項を参照してください。

クライアント プロビジョニングとポスチャのライブアップデートポータル

次の場所からクライアント プロビジョニング リソースをダウンロードできます。

Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。 **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [クライアント プロビジョニング（Client Provisioning）]**。

次のソフトウェア要素は、次の URL から入手できます。

- Windows および Mac OS X ネイティブサプリカント向けのサプリカント プロビジョニング ウィザード
- 最新の Cisco ISE の永続的なエージェントおよび一時的なエージェントの Windows バージョン
- 最新の Cisco ISE の永続的なエージェントの Mac OS X バージョン
- ActiveX および Java アプレット インストーラ ヘルパー
- AV/AS コンプライアンス モジュール ファイル

クライアント プロビジョニング アップデート ポータルで利用可能なソフトウェアパッケージを Cisco ISE に自動的にダウンロードする方法については、『Cisco Identity Services Engine Administrator Guide』の「Configure Client Provisioning」の章の「Download Client Provisioning Resources Automatically」の項を参照してください。

次の場所からポスチャ更新をダウンロードできます。

Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。 **[ワークセンター（Work Centers）] > [ポスチャ（Posture）] > [設定（Settings）] > [ソフトウェアアップデート（Software Updates）] > [ポスチャ更新（Posture Updates）]**

次のソフトウェア要素は、次の URL から入手できます。

- シスコで事前定義されたチェックとルール
- Windows および Mac OS X の AV/AS サポート表
- Cisco ISE オペレーティングシステムのサポート

このポータルで利用可能なソフトウェアパッケージを Cisco ISE に自動的にダウンロードする方法については、『Cisco Identity Services Engine Administrator Guide』の「Download Posture Updates Automatically」の項を参照してください。

自動ダウンロード機能を有効にしていない場合、更新をオフラインでダウンロードすることができます。

Cisco ISE オフライン更新

このオフライン更新オプションを使用すると、Cisco ISE を使用してデバイスから Cisco.com にインターネット経由で直接アクセスできない場合、またはセキュリティポリシーによって許可されていない場合に、クライアントプロビジョニングおよびポスチャ更新をダウンロードできます。

オフラインのクライアント プロビジョニング リソースをアップロードするには、次の手順を実行します。

手順

ステップ 1 https://software.cisco.com/download/home/283801620/type/283802505/release/3.1.0に進みます。

ステップ 2 ログインクレデンシャルを入力します。

ステップ 3 Cisco Identity Services Engine のダウンロードウィンドウに移動し、リリースを選択します。

次のオフライン インストール パッケージをダウンロードできます。

- **win_spw-**<*version*>**-isebundle.zip**：Windows 向けのオフライン SPW インストールパッケージ
- **mac-spw-**<*version*>**.zip**：Mac OS X 向けのオフライン SPW インストールパッケージ
- **compliancemodule-**<*version*>**-isebundle.zip**：オフライン コンプライアンス モジュール インストール パッケージ
- **macagent-**<*version*>**-isebundle.zip**：オフライン Mac エージェント インストール パッケージ
- **webagent-**<*version*>**-isebundle.zip**：オフライン Web エージェント インストール パッケージ

ステップ 4 [ダウンロード（Download）] または [カートに追加（Add to Cart）] のいずれかをクリックします。

ダウンロードしたインストールパッケージを Cisco ISE に追加する方法については、『Cisco Identity Services EngineAdministrator Guide』の「Add ClientProvisioning Resources from a Local Machine」のセクションを参照してください。

ポスチャ更新を使用して、ローカルシステムのアーカイブから Windows および Mac オペレーティングシステムのチェック、オペレーティングシステム情報、ウイルス対策とスパイウェア対策サポート表を更新できます。

オフライン更新の場合は、アーカイブファイルのバージョンが設定ファイルのバージョンと一致していることを確認します。Cisco ISE を設定した後にオフラインでポスチャ更新を使用し、ポスチャポリシーサービスの動的更新を有効にします。

オフラインのポスチャ更新をダウンロードするには、次のようにします。

手順

ステップ 1 https://www.cisco.com/web/secure/spa/posture-offline.htmlに進みます。

ステップ 2 ローカルシステムに **posture-offline.zip** ファイルを保存します。このファイルを使用すると、Windows および Mac オペレーティングシステムのオペレーティングシステム情報、チェック、ルール、ウイルス対策とスパイウェア対策サポート表が更新されます。

ステップ 3 [管理（Administration）] > [システム（System）] > [設定（Settings）] > [ポスチャ（Posture）]。Cisco ISE GUI で [Menu] アイコン（☰）をクリックして、次の順に選択します。

ステップ 4 矢印をクリックすると、ポスチャの設定が表示されます。

ステップ 5 [更新（Updates）] をクリックします。
[ポスチャ更新（Posture Updates）] ウィンドウが表示されます。

ステップ 6 [オフライン（Offline）] オプションをクリックします。

ステップ 7 [参照（Browse）] をクリックし、システムのローカルフォルダからアーカイブファイル（posture-offline.zip）を検索します。

（注） [更新するファイル（File to Update）] フィールドは必須フィールドです。適切なファイルを含むアーカイブファイル（.zip）を 1 つだけ選択できます。.zip、.tar、.gz 以外のアーカイブファイルはサポートされていません。

ステップ 8 [今すぐ更新（Update Now）] をクリックします。

設定要件

- 関連する Cisco ISE ライセンス料金を支払う必要があります。
- 最新のパッチをインストールする必要があります。

- Cisco ISE ソフトウェア機能がアクティブになっている必要があります。

Cisco ISE を設定するには、次のリソースを参照してください。

- Getting started with Cisco ISE
- YouTube の Cisco ISE チャンネルのビデオ
- *ISE* セキュリティ エコシステム統合ガイド
- *Cisco Identity Services Engine* 管理者ガイド

モニタリングおよびトラブルシューティング

システムのモニタリングおよびトラブルシューティングに関する詳細については、『*Cisco Identity Services Engine* 管理者ガイド』の「Cisco ISE のモニタリングとトラブルシューティング サービス」のセクションを参照してください。

発注情報

Cisco ISE の詳細な発注およびライセンス情報については、 *Cisco IdentityServices Engine* 注文ガイド [英語] を参照してください。

Cisco ISE と Cisco Digital Network Architecture Center との統合

Cisco ISE は Cisco DNA Center と統合できます。Cisco DNA Center と連携するように Cisco ISE を設定する方法については、*Cisco DNA Center* のドキュメントを参照してください。

Cisco ISE と Cisco DNA Center との互換性については、「Cisco SD-Access Compatibility Matrix」を参照してください。

Cisco AI エンドポイント分析

Cisco AI エンドポイント分析は、エンドポイント プロファイリングの忠実度を改善する Cisco DNA Center のソリューションです。きめ細かいエンドポイント識別を提供し、さまざまなエンドポイントにラベルを割り当てます。ディープパケット インスペクション、および Cisco ISE、Cisco SD-AVC、ネットワークデバイスなどのソースからのプローブによって収集された情報は、エンドポイント プロファイリングのために分析されます。

Cisco AI エンドポイント分析は、人工知能（AI）と機械学習機能を使用して、同様の属性を持つエンドポイントを直感的にグループ化します。IT 管理者は、これらのグループを確認してラベルを割り当てることができます。割り当てられたエンドポイントラベルは、Cisco ISE アカウントがオンプレミスの Cisco DNA Center に接続されている場合、Cisco ISE で使用できます。

Cisco AI エンドポイント分析の結果割り当てられたエンドポイントラベルは、Cisco ISE 管理者がカスタム認証ポリシーを作成するために使用できます。それらの認証ポリシーを使用して、

エンドポイントまたはエンドポイントグループに適切なアクセス権限のセットを提供できます。

新しいパッチのインストール

システムへのパッチの適用方法については、『Cisco Identity Services Engine Upgrade Journey』の「Cisco ISE Software Patches」セクションを参照してください。

CLI を使用したパッチのインストール方法については、『*Cisco Identity Services Engine CLI リファレンスガイド*』の「Patch Install」セクションを参照してください。

（注） Cisco ISE 3.1 にホットパッチをインストールしている場合は、パッチをインストールする前にホットパッチをロールバックする必要があります。そうしないと、整合性チェックのセキュリティの問題により、サービスが開始されない可能性があります。

不具合

「不具合」セクションには、バグ ID とそのバグの簡単な説明が含まれています。特定の不具合の症状、条件、および回避策に関する詳細については、シスコのバグ検索ツール（BST）を使用してください。バグ ID は英数字順にソートされます。

（注） 「未解決の不具合」セクションには、現在のリリースに適用され、Cisco ISE 3.1 よりも前のリリースにも適用されている可能性のある未解決の不具合が記載されています。これまでのリリースで未解決で、まだ解決されていない不具合は、解決されるまで、今後のすべてのリリースに適用されます。

BST は Bug Toolkit の後継オンラインツールであり、ネットワークリスク管理およびデバイスのトラブルシューティングにおいて効率性を向上させるように設計されています。製品、リリース、またはキーワードに基づいてソフトウェアのバグを検索し、バグの詳細、製品、バージョンなどの主要データを集約することができます。ツールの詳細については、http://www.cisco.com/web/applicat/cbsshelp/help.html のヘルプ ページを参照してください。

Cisco ISE リリース 3.1 - 累積パッチ 5 の新機能

エンドポイントへの論理プロファイルの自動割り当て

Cisco ISE のプロファイリング ワークフローでエンドポイントが処理される際に、関連付けられた論理プロファイルを持つエンドポイント プロファイリング ポリシーとエンドポイントが一致する場合、その論理プロファイルがエンドポイントに自動的に割り当てられます。

コンテキストインの pxGrid Cloud サポート

Cisco ISE リリース 3.1 累積パッチ 5 から、コンテキストインの pxGrid サポートが利用可能になりました。 pxGrid Cloud コンテキストインサポートは、ERS および Open API を通じて提供されます。

Cisco Secure Client のサポート

Cisco ISE は、Cisco ISE ポスチャ要件の Cisco Secure Client で統合モジュールを使用します。

Cisco ISE をエージェントと統合すると、Cisco ISE は次のように機能します。

- Cisco Secure Client を展開するためのステージングサーバーとして機能
- Cisco ISE ポスチャ要件のエージェント ポスチャ コンポーネントとやり取りする
- エージェントプロファイル、カスタマイズおよび言語パッケージ、および OPSWAT のライブラリ更新の展開をサポートする

Cisco ISE リリース 3.1 - 累積パッチ 5 の解決済みの不具合

次の表に、リリース 3.1 累積パッチ 5 で解決済みの不具合を示します。

ID	見出し
CSCwc74531	ise hourly cron は、95% のメモリ使用量ではなく、キャッシュされたバッファをクリーンアップする必要がある
CSCwc52685	ENH：SMS ゲートウェイ用の Twilio MessagingServiceSid を使用した ISE
CSCwc64346	ISE ERS SDK ネットワークデバイスのバルクリクエストのドキュメントが正しくないです
CSCwc31482	NetworkSetupAssistance.exe デジタル署名証明書が Windows SPW を使用した BYOD フローで期限切れになる
CSCwc76720	ISE 3.1 のみでの SNMPv3 プライバシーパスワードのエラー
CSCwc27765	SYS_EXPORT_SCHEMA_01 が原因で ISE 設定のバックアップが失敗する
CSCwc57240	カスタム属性の追加中に GUI がデフォルト値が検証されません
CSCwb59162	SNMP パスワードパラメータの ISE 3.1 REST API のタイプミス
CSCwc26241	ISE 3.2 で次のエラーが表示される：「TypeError：未定義のプロパティを読み取れません（「attr」の読み取り）（TypeError: Cannot read properties of undefined (reading 'attr')）」
CSCwc21400	SFTP/FTP リポジトリユーザーのパスワードに！（感嘆符）が含まれている場合のリポジトリ OpenAPI での HTTP 400 レスポンス（感嘆符）
CSCwd31405	Session.PostureStatus のクエリ中に遅延が発生する

ID	見出し
CSCwc85920	ISE TrustSec ロギング - SGT 作成イベントが ise-psc.log ファイルに記録されない
CSCwc39614	SYS.DBMS_RCVMAN が古すぎます
CSCwb23853	古い ISE から構成を復元したときに、3.1 p1 で SAML ID プロバイダーを追加できない
CSCwc65802	SAML 構成の保存ボタンがグレー表示される
CSCwc21890	専用 MnT ノードを使用する ISE でパッシブ Easy Connect が機能しない
CSCwc69492	ISE 3.1：メタスペースを使い果たすと ISE ノードでクラッシュが発生する
CSCwb62192	ISE インデックスエンジンのバックアップが失敗するとスケジュール済みバックアップが失敗する
CSCwc65821	ERS API では、「ネットワーク デバイス グループ」名にマイナス文字を使用できません。
CSCwc71060	削除されたネットワーク デバイス グループがポリシーセットに引き続き表示されます
CSCwc62415	Cisco Identity Services Engine の不正ファイルアクセスの脆弱性
CSCwa37580	ISE 3.0 NFS 共有がスタックする
CSCwb84779	親 ID グループ名を変更すると、認証リファレンスが壊れます
CSCwc98833	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCwb88851	VN 値が変更されているときに、複数の再認証後に IP から SGT へのマッピングの一貫性がなくなる
CSCwc80574	参加中に ISE AD コネクタが失敗する
CSCwc79321	ID ソースを内部から外部の RSA/RADIUS トークンサーバーに変更できません
CSCwc64275	ppan の ise-psc.log でオプティミスティックロックが失敗すると、事前チェックがタイムアウトする場合があります
CSCwc61320	ログのダウンロードページがバックグラウンドで読み込まれるため、サポートバンドルページが低速になる。
CSCwc09435	携帯電話番号フォーマットのエラー処理/メッセージが明確でない
CSCwc51219	RADIUS 共有秘密の先頭に += 文字がある場合、CSV NAD インポートが拒否される

ID	見出し
CSCwc24126	プロファイラ条件で属性値が表示されない
CSCwc57294	設定の読み取りに例外がある場合、Duplicate Manager はパケットは削除されません
CSCwc95878	アプリのアクティベーションまたはアプリの断続的な問題によりイベントを受信しない
CSCwd05697	ゲストロケーションが ISE ゲストポータルにロードされない
CSCwb47255	サポートされる HTTP メソッドが表示される
CSCwd03009	2.7 p7 の platform.properties でハードウェアアプライアンスに基づいて制御する RMQForwarder スレッド
CSCvv43120	ISE-2.x：接続に関する Intune MDM アラーム || 401 未承認（401 Unauthorized）
CSCwc81729	フィルタ処理で特定の 1 つの NAD を削除しようとすると、「すべてのデバイスが正常に削除されました（All devices were successfully deleted）」と表示される
CSCwc23997	ISE で [認証プロファイル（Authorization profile）] > [属性詳細（Attributes Details）] に誤った VLAN 割り当て情報が表示される
CSCwc42712	ISE RADIUS および PassiveID セッションのマージ
CSCwc15013	有用性を追加し、ISE 3.0 の「プールが枯渇しているためリソースを取得できませんでした（Could not get a resource since the pool is exhausted）」エラーを修正する
CSCwc59570	ISE が SXP Ver 4 で 4,096 バイトを超えるサイズの SXP メッセージを送信する
CSCwd45843	GC アクティビティによるポリシー評価の認証ステップの遅延
CSCwb53455	内部 Docker IP 169.254.2.2 に関連する RMQ TLS syslog が監査ログに送信される
CSCwa55866	シングル接続が有効になっていると、Tacacs応答が送信されないことがある
CSCwb24002	ISE ERS SDK の authenticationSettings が API 呼び出しを介して無効になっていない
CSCwc95075	ポスチャのファイル条件を設定すると、「[ファイルパス]フィールドには有効なファイル名を含める必要があります（File path field must contain a valid file name）」というエラーが表示される。

ID	見出し
CSCwb36873	ISE-PIC ノードでページにアクセスできないというポップアップメッセージを取得する
CSCvz65945	非 TACACS トラフィックのライブログ内の「無効な長さ」による TACACS 認証の失敗
CSCwb27894	EAP-TLS を使用した EAP-TEAP が「CERTIFICATE.Issuer - Common Name」を持つ条件に一致しない
CSCwc74206	新しいインスタンスの使用時に機能する、新しいパスワードを持つ SCCM MDM サーバーオブジェクトが ISE 3.0 で保存されない
CSCwb48388	CSSM で予約されたライセンスに複数の有効期限がある場合、ライセンス機能で 1 つの予約数しか表示されない
CSCwc50944	プロファイリングポリシー名の変更がポリシーセットの条件に自動的に反映されない
CSCvz91479	3.1 から 3.2.0.804 へのアップグレードの制約を変更中にスキーマのアップグレードが失敗した
CSCwc33850	API を使用して証明書と秘密キーをエクスポートできない
CSCwc60997	ISE：ISE で、トークンの処理が正しくないため、ロードバランサを使用した SAML フローが失敗する
CSCwc49580	ANC CoA がデバイス IP アドレスではなく NAS IP アドレスに送信される
CSCwc23593	LSD によって CPU が高くなる
CSCwc44614	[Network Devices] で [Export Selected] を使用すると、X 回以上の選択でログイン画面が中断されます。
CSCwc48509	Windows Server 2022 が実際には監視対象のドメインコントローラとして機能している
CSCwc93451	プロファイラは、デフォルトの RADIUS プローブからの転送について、否定的な RADIUS Syslog メッセージを無視する必要がある
CSCvv54351	Radius を使用したデバイス管理が基本ライセンスを使用しない
CSCwd30994	ISE：Gig 0 以外のインターフェイスのゲートウェイを使用した静的デフォルトルートにより、ネットワーク接続が切断されます
CSCwc07283	ISE 3.1 で [コンテキストの可視性（Context Visibility）] の [エンドポイント（Endpoints）] の [認証（Authentication）] タブにデータが表示されない

ID	見出し
CSCwc30643	CRUD を実行しないと、ノードのリロード後にデバイスポータルが開かない。
CSCwc11613	証明書署名要求では大文字と小文字を区別すべきでない
CSCwc57939	ISE が大規模な VM をサポート対象外として検出する
CSCwc88848	ISE 3.1 パッチ 1 で Rest ID/ROPC フォルダログが作成されない

Cisco ISE リリース 3.1 - 累積パッチ 5 の未解決の不具合

次の表に、リリース 3.1 - 累積パッチ 5 で未解決の問題を示します。

不具合 ID	説明
CSCwd70346	Cisco ISE リリース 3.1 パッチ 5 に完全にアップグレードすると、選択された古いデータが事前チェックページにロードされ、開始ボタンが無効になります。

Cisco ISE リリース 3.1 - 累積パッチ 4 の新機能

REST ID ストアの [Groups] タブの機能強化

Cisco ISE でリソース所有者のパスワードクレデンシャルを設定するときに、REST ID ストアグループを取得、フィルタリング、および削除できるようになりました。

グループを追加するときに、[Retrieve Groups] をクリックして、接続された ID ソースからユーザーグループをインポートします。選択するグループの隣にあるチェックボックスをオンにし、[保存（Save）] をクリックします。必要に応じて、すべてのグループを選択することもできます。選択したグループが [グループ（Groups）] タブに一覧表示されます。

フィルタオプションを使用して結果をフィルタ処理できます。

ユーザーグループを削除するには、削除するグループの隣にあるチェックボックスをオンにして、[削除（Delete）] をクリックします。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Asset Visibility」の章にある「Configure Resource Owner Password Credentials Flow」を参照してください。

.

IP デフォルトゲートウェイの変更には再起動が必要

Cisco ISE 3.1 パッチ 4 以降では、ゲートウェイを追加または変更すると、CLI は管理者にサービスの再起動が必要になる可能性があることを警告し、[Yes] オプションが選択されている場合にのみコマンドの実行に進みます。

詳細については、『*Cisco ISE CLI Reference Guide, Release 3.1*』の「Cisco ISE CLI Commands in Configuration Mode」の章を参照してください。

Cisco ISE リリース 3.1 - 累積パッチ 4 の解決済みの不具合

次の表に、リリース 3.1 累積パッチ 4 で解決済みの不具合を示します。

問題 ID 番号	説明
CSCwc62413	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCwb22662	64 文字の制限では、ユーザープリンシパル名などの外部ユーザー ID に対応するには不十分です
CSCwb32244	ISE 信頼済み証明書にインポートされた証明書を編集できない
CSCwb75941	パストラバーサルの脆弱性
CSCwb75954	クロスサイト要求偽造の脆弱性
CSCwb75959	保存されたクロスサイト スクリプティングの脆弱性
CSCwb75965	不正なファイルアクセスの脆弱性
CSCwb79353	OS 権限昇格の問題
CSCwa88954	CIAM：python-pip 9.0.3
CSCwb64656	Essential ライセンスが Cisco ISE GUI で無効になっている場合、スマートライセンスポータルはライセンス消費を報告しない。
CSCwb39638	SNMPv3 SHA2 認証で構成されたネットワークデバイスをインポートできない
CSCvy77475	CIAM：libcurl 7.61.1
CSCwa61347	Cisco ISE-PIC から特殊文字で始まるライブセッションが転送されない
CSCwb09824	CIAM：libjpeg-turbo 1.5.3
CSCwa96229	Cisco ISE では、現在のパスワードを検証せずに管理者パスワードを変更できない
CSCwc00162	クライアントまたはブラウザが複数の証明書を送信すると、証明書ベースの管理者ログインが機能しない
CSCwb09881	CIAM：sqlite 3.26.0
CSCwa80499	CIAM: ncurses 6.1
CSCwb33727	属性では特殊文字はサポートされていない
CSCwc30811	ゲストポータルでアンダースコアが脆弱である

問題 ID 番号	説明
CSCvy66496	REST ID は、Azure AD グループの名前または SID に基づいてグループをフィルタ処理しない
CSCwb92006	プロキシ設定でパスワードの途中に一重引用符（'）があると、ページが編集できない
CSCwb56878	複製停止アラームはトリガーされない
CSCwb55232	ERS API を使用してネストされたエンドポイントグループを作成する
CSCwb82814	ネストされた条件の取得時に OpenAPI エラー 400 が発生する
CSCvv87286	ISE 2.7P2 ～ 3.0 で内部 CA とキーをインポートできない
CSCwb92643	ADE-OS CLI TCP パラメータが変更に失敗し、関連性がなくなる
CSCwb88360	アップグレードされたノードで一時的な MnT ペルソナを無効化すると、分割アップグレードで失敗する
CSCwb14106	CIAM：cyrus-sasl 2.1.27
CSCwb75964	PAN 自動フェールオーバーアラームを編集できない
CSCvz71874	CIAM：libdnf 0.39.1
CSCwb19256	Pingnode 呼び出しにより、CRL 検証中にアプリケーションサーバーがクラッシュする（OOM は除く）
CSCwc12303	インスタンスが使用する PGA メモリが MNT ノードで PGA_AGGREGATE_LIMIT を超えている
CSCwa97123	2 つ以上の NTP サーバーが設定されている NTP 同期エラーアラーム。
CSCwa40040	セッションディレクトリの書き込みに失敗する。SQLException：ISE3.0P4 で文字列データの右側が切り捨てられる
CSCwb95433	ポスチャのファイル条件が設定されると、「File path field must contain a valid file name」というエラーが表示される
CSCwa80710	CIAM：jszip 2.5.0
CSCwa06912	認証ポリシーに日付または時刻条件がある TACACS+ 要求で高遅延が発生する
CSCwb29498	高稼働時の DB 使用率アラームのパーセンテージを設定可能にする必要がある。
CSCwb61614	ゲストユーザー（AD または内部）が特定のノードで自分のデバイスを削除または追加できない

問題 ID 番号	説明
CSCwb82141	コンテキストの可視性で、既存の展開のエンドポイントと NAD が復元後に削除されない
CSCvx08772	仮想マシンリソース不足アラームが頻繁に発生する
CSCwb42924	ポスチャ修復アクションでメッセージオプションを取得できない
CSCwc18751	DomainName\UserName 形式を使用してログインしている場合、作成したサポートバンドルを GUI からダウンロードできない
CSCwb25789	SSH ホストキーの処理に関する一貫性のない動作
CSCwb52396	ISE PRA フェールオーバー
CSCwa85010	PAN が展開から削除された場合、SAML 証明書は Stale としてマークできません
CSCwb59170	SHA-2 オプションが REST API での NAD 作成に使用できない
CSCwb91645	TrustSec ダッシュボードの更新コールが原因で MNT の CPU 使用率が高くなる
CSCwb35304	Cisco ISE 3.1 の競合状態が原因で登録または同期が失敗する
CSCwa95892	ui_time_left 変数が間違った期間を示している
CSCwa60903	Cisco ISE で、CRL の nextUpdate の日付に 6 時間追加される
CSCwc06638	パッチロールバックおよびパッチインストール後にシステムサマリーが更新されない
CSCwa83517	電子メールアドレスにアポストロフィが含まれている場合、ゲストポータル登録ページで「ページの読み込みエラー」が表示される
CSCwa89443	DNA Center - ISE 統合：ISE で pxGrid エンドポイントの古い DNAC 証明書が表示される
CSCvz57222	セカンダリインターフェイス GigabitEthernet 1 および Bond 1 で ISE GUI に管理アクセスが許可される
CSCwb05059	TCPDump メニューの P1 古いノード
CSCwb97579	Hyper-V Gen-2 との互換性の問題
CSCwb26965	REST API を使用してネットワーク デバイス グループを作成するときのエラー
CSCwb21669	オンプレミス SSM サーバーの IPv6 アドレスを入力できない

問題 ID 番号	説明
CSCwb79056	ERS コール /ers/config/sgmapping/{id} がカスタム SGT の SGT 値を返さない
CSCwa80488	CIAM：openssh 7.6
CSCvy91805	最大セッション数は EAP-FAST-Chaining では適用されない
CSCwa80480	CIAM：bind 9.11.4
CSCwb34910	Cisco ISE ポータルでのゲスト SMS 通知の複数行の問題
CSCwb55979	NTP サービスの障害（NTP Service Failure）
CSCwa95889	新しい HostKeyAlgorithms（例：RSA-SHA2-512）で SSH/SFTP をホストできない
CSCwb26227	CIAM：jackson-databind 2.9.8
CSCwa73860	ppgrade の後、rabbitmq 証明書ディレクトリ内のファイルに不正なアクセス許可が表示される
CSCwb85456	CIAM：openssl を 1.0.2ze および 1.1.1o にアップグレード
CSCwc12693	ISE ERS 検証エラー：[validDays] 必須フィールドがありません
CSCwb91392	サードパーティの CA 証明書が管理者に使用されている場合、BH ヘルスチェックとフルアップグレードの事前チェックがタイムアウトする
CSCwb70401	パッチ 2：「整合性チェックに失敗しました」エラーによりサービスが開始されない
CSCwc09104	認証仮想 VLAN を使用したゲストリダイレクトが ISE 3.1 で機能しなくなった
CSCwa17925	失敗したアップグレード前チェックを修正しても、[Proceed] ボタンが使用できない
CSCwb86283	ISE 展開：不正な証明書の有効期限チェックの結果として、すべてのノードが OUT_OF_SYNC エラーをスローする
CSCwb09861	CIAM：glib 2.56.4
CSCwb09860	CIAM：openssl 1.1.1g
CSCvy69483	CIAM：libgcrypt 1.5.3
CSCwa79799	sysodbcini ファイルに PermSize 属性がない
CSCwa97357	Cisco ISE が SMTP API 本文で $mobilenumber$ 値を送信しない

問題 ID 番号	説明
CSCwb37760	[Allow kerberos SSO] ポータル設定の有効化時にスポンサーポータルでエラー 500 が表示される
CSCwb94890	重要業績評価指標レポートに毎日午前 8 時と午前 9 時のエントリがない
CSCwb09045	正しくない cryptoLib 初期化が原因で ISE PSN ノードがクラッシュする
CSCwa90930	キューサイズは 3.x の RMQ に制限する必要がある
CSCvz24558	Spring Hibernate TPS アップグレード（Hibernate 5.5.2、Spring 5.3.8）
CSCwa75348	ODBC 動作のフェールオーバーの問題
CSCwb04898	名前にスペースを含まないグループがファイルを所有している場合、Linux SFTP リポジトリから CFG バックアップを復元できない
CSCwb57665	Struts2 CVE-2021-31805 の ISE 評価
CSCwb43007	SAML ログインでポスチャポリシーページが読み込まれない
CSCvz94133	「EDF_DB_LOG」が原因で構成バックアップが失敗する
CSCwc41697	接続エラーが原因でアップグレード中にノード間のデータダンプ転送が失敗する
CSCwa76896	RADIUS 認証レポートで「Failure Reasons」列が重複する
CSCwa47133	ISE 評価 log4j CVE-2021-44228
CSCwb05532	「場所」フィールドと「デバイスタイプ」フィールドの場所は、[Network Devices] タブをクリックするたびに変化し続ける。
CSCvz42996	CIAM：glibc 2.17
CSCwa91335	パッシブ Syslog プロバイダーのデフォルトのドメイン構成が ISE 3.1 で機能しない
CSCwb81416	ログイン後に Cisco ISE GUI がロードされない
CSCwb01854	Cisco ISE 3.0 以降にアップグレードした後、アップグレード外部 Radius サーバーリストが表示されない
CSCwb27857	分散型展開で RSA 2FA を使用して MnT ノードの GUI にログインできない
CSCwc09737	CIAM：cups 1.6.3
CSCwb02129	Cisco ISE への SSH が SSH 公開キーの手動インポートで失敗する

問題 ID 番号	説明
CSCwb36849	Cisco ISE で空の Cisco AV-Pair を access-accept パケットで送信しないようにする必要がある
CSCwb41741	管理者グループの無効な文字エラー
CSCwb32466	説明が設定されていない場合、REST API を介して作成されたエンドポイント ID グループを削除できない
CSCwb57675	「専用 MnT」オプションを有効にした後、GUI から無効にできない
CSCwa82553	ボンディングが設定されている場合、デフォルトルートが間違ったインターフェイス上に配置される
CSCwa04370	アップグレード後にデフォルトルートが削除されるか、間違ったインターフェイスに関連付けられる。
CSCvw90778	展開ページでデバイスの管理プロセスを無効にしても、T+ ポート（49）が開いている
CSCwb11147	仮想ネットワークを使用した SGT-IP マッピングの競合処理で必要なログの改善
CSCwb40942	電子メールの送信元アドレスが .com または .net で終わっていない場合は無効になる
CSCwb96942	構成のバックアップが復元された後、アプリケーションサーバーが初期化中の状態でスタックする
CSCwb98854	SLR ライセンスの更新後に Cisco ISE が有効期限を更新しない
CSCvz43125	CIAM：nettle 3.4.1
CSCwb40349	外部 RADIUS トークン共有秘密の無効な文字。
CSCwb38069	古い ISE バージョン 2.6 からのバックアップの復元後にサービスを開始できない
CSCwb01843	タイムゾーンの更新は自動的に行われる
CSCwb29357	AD ユーザーの SamAccountName パラメータがユーザーセッションで null になる
CSCwb80572	Cisco ISE パッチ 2 に Cisco ISE 3.1 パッチ 3 をインストールした後、アプリケーションサーバーが初期化状態のままになる
CSCwb39964	ISE で外部 ID ソースを持つ無効なシャドウ管理アカウントを使用して GUI にログインできる。

問題 ID 番号	説明
CSCwb07504	ユーザー ID グループに基づいた内部ユーザーの並べ替えが、[Identity Management] > [ID] で機能しない
CSCwb88129	CIAM：samba 4.13.3
CSCwc39844	eth 1 での IP アドレスの変更中に、サービスの自動再起動が内部エラーで失敗する
CSCwa80553	CIAM：samba 4.8.3
CSCwb23028	パスワードの不正確な辞書の単語評価
CSCvk25808	スケジュール設定されたレポートを作成した管理者が利用できなくなった場合、そのスケジュール設定されたレポートを編集または削除できない
CSCwa88948	CIAM：暗号化 2.3
CSCwb93156	TrustCertQuickView がすべての信頼できる証明書について同じ情報を提供する
CSCwb40131	Rest API を使用して外部パスワードタイプで内部ユーザーを有効にしているときに 400 Bad Request が発生する
CSCwb32492	プライマリ PAN の管理証明書を変更した後、すべてのノードでアプリケーションサーバーが再起動する
CSCvv02086	ISE PIC ノードで TLS 1.0 および 1.1 を無効にする機能を追加
CSCwc03220	ISE から IP アクセスリストを削除すると、分散展開が破棄される

Cisco ISE リリース 3.1 の新機能 - 累積パッチ 3.1

Cisco pxGrid クラウドのサポート

Cisco ISE 3.1 パッチ 3 は Cisco pxGrid クラウドをサポートしています。Cisco pxGrid クラウドは、pxGrid および ERS のアクセスをクラウドベースのアプリケーションに拡張する新しい Cisco cloud サービスです。Cisco ISE 展開と Cisco pxGrid クラウド間の接続を許可するには、Cisco ISE 展開内の 1 つ以上の pxGrid ノードで pxGrid クラウドサービスを有効にする必要があります。Cisco pxGrid Cloud の詳細については、『Cisco pxGrid Cloud Solution Guide』を参照してください。

OSCP 証明書の自動更新

Cisco ISE リリース 3.1 累積パッチ 2 以降では、次のルールが OCSP 証明書の更新に適用されます。

- マルチノード Cisco ISE 展開の場合、Cisco ISE GUI を介してパッチをインストールすると、OCSP 証明書が自動的に更新されます。Cisco ISE CLI を介してパッチをインストールする場合は、OCSP 証明書を手動で更新することをお勧めします。
- スタンドアロン Cisco ISE 展開の場合、Cisco ISE GUI、または Cisco ISE CLI のどちらを介してパッチをインストールしたかに関わらず、OCSP 証明書が自動的に更新されます。
- パッチ2をアンインストールする場合は、OCSP証明書を手動で更新する必要があります。

Microsoft Graph の更新による Microsoft Intune の統合の変更

Microsoft は Azure Active Directory（Azure AD）Graph を廃止しており、2022 年 6 月 30 日以降、Azure AD Graph 対応の統合をサポートしません。Azure AD Graph を使用するすべての統合を Microsoft Graph に移行する必要があります。Cisco ISE は通常、エンドポイント管理ソリューション Microsoft Intune との統合に Azure AD Graph を使用します。

Azure AD Graph から Microsoft Graph への移行の詳細については、次のリソースを参照してください。

- Azure AD Graph アプリの Microsoft Graph への移行
- Azure AD Graph から Microsoft Graph への移行に関するよくある質問
- アプリケーションを Microsoft Authentication Library と Microsoft Graph API を使用するように更新する

Cisco ISE リリース 3.1 パッチ 3 は、Microsoft Graph を使用する Microsoft Intune 統合をサポートします。Cisco ISE と Microsoft Intune 間の統合の中断を回避するには、Cisco ISE を Cisco ISE リリース 3.1 パッチ 3 に更新します。次に、2022 年 6 月 30 日までに、Azure AD Graph の代わりに Microsoft Graph を使用するよう、Microsoft Azure の Cisco ISE 統合を更新します。Cisco ISE では、Microsoft Intune 統合を更新して、[自動検出URL（Auto Discovery URL）] フィールドを更新する必要があります。**https://graph.windows.net<*Directory (tenant) ID*>** を **https://graph.microsoft.com** に置き換えます。

設定手順の詳細については、「Connect Microsoft Intune to Cisco ISE as a Mobile Device Management Server」を参照してください。

Cisco ISE での TAC サポートケースのオープン

Cisco ISE GUI から Cisco ISE および他のシスコ製品の TAC サポートケースを開くことができるようになりました。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Troubleshoot」の章の「Open TAC Support Cases in Cisco ISE」を参照してください。

デフォルトで無効になっている SHA1 暗号

Cisco ISE リリース 3.1 パッチ 2 以降、ポート 443 の SHA1 暗号はデフォルトで無効になっています。

Cisco ISE リリース 3.1 の解決済みの不具合 - 累積パッチ 3

次の表に、リリース 3.1 累積パッチ 3 で解決済みの不具合を示します。

問題 ID 番号	説明
CSCwb70401	パッチ 2 をインストールした後、「整合性チェック失敗」エラーが原因でサービスが停止する
CSCwa55996	条件スタジオに新しいオブジェクトが存在しない
CSCwa51150	ISE 3.1 で WLC が EAPOL キー M2 を検証できない
CSCvz91603	ISE 3.0 パッチ 3 にアップグレードした後、ODBC から属性を取得できない
CSCwa07580	ユーザー名に $ が含まれている場合、アイデンティティユーザーを作成できない
CSCwa09113	内部 CA の失敗「OCSP ステータスが不明なため、12557 ユーザー認証に失敗しました（12557 User Auth failed because OCSP status is unknown）」エラーによる単一の Byod フロー
CSCvy99582	外部 RADIUS サーバーが設定されている場合、ISE 2.4 パッチ 13 から ISE 2.7 へのアップグレードが失敗する
CSCwa37040	ISE CLI の公開キー暗号化を使用するバックアップログで、コアファイルのキャプチャが許可されない
CSCvz67479	すべてのフィールドの [ローカルログの設定（Local Log Settings）] ツールチップに、無関係で役に立たない「信頼できる証明書（Trust Certificates）」が表示される
CSCwa17470	ユーザーアサーションに「グループ」クレームに複数の値が含まれている場合、ISE 3.1 SAML 管理認証が失敗する
CSCwa35293	ISE 2.7 認証成功設定が成功/成功 URL を示す
CSCvz88188	セッションキャッシュのユーザー名が null であるため、ユーザー名に対する TACACS 認証ポリシーのクエリ実行に失敗する
CSCwa26210	「GET /ers/config/radiusserversequence」API の JSON 応答に nextPage フィールドがない
CSCwa88845	デバイスポートのネットワーク条件でインターフェイス ID が検証されない
CSCwa11658	CIAM：gnutls 3.6.14
CSCwa11659	CIAM：libx11 1.6.8
CSCwa11657	CIAM：python 3.6.8

問題 ID 番号	説明
CSCwa11654	CIAM：file 5.33
CSCwa11655	CIAM：sysstat 11.7.3
CSCwa78479	CVE-2021-4034 Polkit の Cisco Identity Services Engine 評価
CSCwa20354	[運用データの削除（Operational Data Purging）] > [データベースの使用状況（Database Utilization）] ウィンドウでノードデータベースの使用情報が正しく表示されない
CSCvz79665	Microsoft Intune Graph の URL を graph.windows.net/tenant から graph.microsoft.com に変更
CSCwa16401	Get-By-Id サーバーシーケンスが、GUI を介してシーケンスで最初の変更を行った後に空のサーバーリストを返す
CSCwa48465	複数の値を持つフィールドの処理ミスが原因でレポートが使用できない
CSCvx54894	スポンサーポータル管理者が 1 時間以下のランダムゲストアカウントを作成できない
CSCvz71872	CIAM：nss - 複数のバージョン
CSCvz37241	キューリンクエラー：WARN:{socket_closed_unexpectedly;'connection.start'}
CSCvv04957	GRUB2 の任意のコード実行の脆弱性
CSCvz78841	CIAM：openssh 7.6
CSCvz90468	API フローを使用してユーザーを作成すると、外部パスワードストアを使用する内部ユーザーが無効になる
CSCvy84989	POST /ers/config/internaluser/ の Cookie を有効にすると、「IDグループが存在しません（Identity Group(s) does not exist）」というエラーが発生する
CSCvz56358	ISE 3.0 で最初の SAN エントリのみがチェックされる
CSCwa57705	IP-SGT マッピングが新しいネットワークアクセスのデバイスグループとリンクしない
CSCvx23375	編集/保存中にISE認証プロファイルオプションが切り捨てられる（Chrome のみ）
CSCwa32312	セッションキャッシュが入力されていないため、RCMおよびMDMフローが失敗する
CSCvz65576	CLI リポジトリまたはディスクリポジトリが使用されている場合、パッチでフルアップグレードが機能しない

問題 ID 番号	説明
CSCwa33462	RADIUS 共有シークレットの先頭にある特殊記号 @ により、CSV NAD インポートが拒否される
CSCvz85074	CSCvu35802 の修正により、EAP チェーンのアイデンティティとして証明書属性をもつ AD グループの取得が中断される
CSCwa13696	ISE 3.1 ゲストのユーザー名/パスワードポリシーを変更できない
CSCwa23207	メモリ割り当ての不整合が原因で複数のランタイムがクラッシュする
CSCwa47190	ポスチャポリシーで AD セキュリティグループの OU の末尾をドット文字にできない
CSCwa11678	CIAM：binutils 2.30
CSCwa11679	CIAM：json-c 0.13.1
CSCwa57955	ポスチャファイアウォールの修復アクションを変更できない
CSCwa41166	TACACS コマンドセットの正規表現が間違っている
CSCwa17718	専用の MnT を使用した pxGrid セッションディレクトリでセッションサービスを利用できない
CSCvz18627	PEAP セッションのタイムアウト値が最大で 604800 に制限されている
CSCwa78042	ISE 3.1 がスマートアカウントからの ISE-PIC ライセンスを要求する
CSCwa53231	CIAM：nss - 複数のバージョン
CSCwa08802	AWS 上の ISE 3.1 でヘルスチェックの DNS チェックの検出漏れが生じる
CSCwa49859	属性値 dc-opaque がライブログの問題を引き起こす
CSCwa03126	一部の言語で ISE CPP が正しくロードされない
CSCvz83204	ISE で、ポスチャフロー中に発生した不適切なインデックスから URL 属性値を取得できない
CSCvz74457	ERS API で「ネットワーク デバイス グループ」名にドット文字の使用または作成/更新が許可されていない
CSCvy45345	マシン認証フラグが誤って「true」に設定されているため、Eap チェーン認証が失敗する
CSCvz36192	/ers/config/downloadableacl を使用した DACL の GET が nextPage または previousPage を返さない

問題 ID 番号	説明
CSCwa04454	ISE 3.0 および 3.1：デバイス管理ライセンスだけですべての TACACS メニューへのアクセスを許可する必要がある
CSCwa11662	CIAM：lz4 1.8.3
CSCwa11661	CIAM：glibc 2.28
CSCvy76328	[ネットワークデバイス（Network device）] タブの [複製（duplicate）] オプションを使用すると、IPv6 のサブネットが /128 に変更される
CSCwa20309	「不明な NAD（Unknown NAD）」および「正しく設定されていないネットワークデバイスを検出（Misconfigured Network Device Detected）」アラーム
CSCwa56934	エンドポイントグループに対する ERS API の並べ替えが一貫していない
CSCwa45316	ISE 3.1 で vpn ユーザーの MDM intune 統合が中断する
CSCvz63405	ISE クライアントの pxGrid 証明書が DNAC に配信されない
CSCvn27270	名前、場所、またはデバイスタイプを使用してネットワーク デバイス グループを作成できない
CSCwa15191	エンドポイントがポスチャ不明状態でスタックする
CSCwa13877	ISE が、ライセンスクラウドからの無効な応答を示すアラームを表示する
CSCwa46758	削除されたルート ネットワーク デバイス グループが、ネットワークデバイスのエクスポートされた CSV レポートで引き続き参照されている
CSCvz71284	SNMPv3 COA 要求が ISE 2.7 によって発行されない
CSCwa94984	長いカスタム属性文字列を使用した ISE API のユーザー追加操作に、Curl を使用して約 4 分かかる
CSCvw09460	/erc/config/authorizationprofile/{id} 上の PUT の更新されたフィールドリストが通常空になる
CSCvw90586	ネットワーク デバイス グループの名前と説明を同時に変更できない
CSCvs55875	MTU の変更後、既存のルートがルーティングテーブルにインストールされない
CSCwa47566	ISE 条件スタジオ - [IDグループ（Identity Groups）] ドロップダウンを 1000 個に制限
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} が機能していない。CRUD の例外

問題 ID 番号	説明
CSCvy71309	CIAM：tcp-dump 4.9.3
CSCvy16894	特殊文字を使用すると認証プロファイルでエラーがスローされる
CSCwa47133	ISE 評価 log4j CVE-2021-44228
CSCwa20152	マトリックスが変更されていないスイッチで CoA が開始されなかったため、ポリシーの同期に失敗した
CSCvz83753	認証の高度な属性設定に含まれる空のユーザーカスタム属性により、誤った AVP が発生する
CSCvz75902	ISE 内部 CA の生成時に ISE が pxGrid 証明書を置き換える
CSCwa43187	NAT が使用されたときに「Queue Link Error: Message=From Node1 To Node2; Cause=Timeout」エラーが表示される
CSCwa59924	ISE 3.1 パッチ 1：FIPS が有効な場合、SSH 経由で ISE に接続できない
CSCwa19573	SSL 監査イベントが原因で Catalina.out ファイルが巨大化する
CSCwa52114	CIAM：sqlite 3.18.2
CSCwa52110	ネットワークデバイスにSNMPが設定されると、SNMP レコードの処理中に 20 秒の遅延が発生する
CSCwa59237	200 以上の内部証明書を持つ PAN ノードで、Deployment-RegistrationPoller がパフォーマンスの問題を引き起こす
CSCwa38023	ISE 3.1：Active Directory スーパー管理者で pxGrid 証明書を生成できない
CSCwa32814	15 のコレクションフィルタが設定された ISE で 15 番目のフィルタが非表示になる
CSCwa60873	PAN のパフォーマンスを向上させるために bouncy-castle クラスを最適化する
CSCvz79518	有用性：「DNS 解決の失敗（DNS Resolution Failure）」アラームで ISE サーバーを表示する必要がある
CSCvy96761	EAP チェーンフローで関連する ID を処理する間に、セッションキャッシュを更新する必要がある
CSCwa16291	ゲストポータルフィールドにより Apple VoiceOver の単語が繰り返される
CSCvz90852	[成功（Success）]ページが空白で、ホットスポット ゲスト ポータルの [完了（Done）] ボタンが有効にならない

問題 ID 番号	説明
CSCwa05404	Tacacs+ リクエストで「選択したサービスが見つかりませんでした（Could not find selected service）」エラーが発生した場合に、セッションが削除されない
CSCvz95326	ISE で ACI 統合を有効にしようとすると、複数の ACI IP アドレス/ホスト名を追加できなくなる
CSCwa08018	ISE 3.1 - IPv6 がグローバルに無効になっていると GUI が機能しない
CSCwa11682	CIAM：pcre 8.41
CSCvz93230	Gig0 とは異なるインターフェイスでホストされている場合に、ゲストポータルがロードされない
CSCwa53499	[コネクタ設定（connector settings）] ページが開いていると、REST ID がクラウドからグループを取得する
CSCwa56771	ISE 3.0p2：[すべてをモニター（Monitor All）] 設定が複数のマトリックスと異なるビューで正しく表示されない
CSCwa47221	クライアント プロビジョニング ポリシーの AD セキュリティグループで OU の末尾をドット文字にできない
CSCwa52133	CIAM：libsolv 0.7.16
CSCvz60870	TPS が高いときに Active Directory の遅延が大きいと、ADRT で HOL ブロッキングが発生する
CSCvs95495	サードパーティデバイスで再認証の問題が発生する
CSCwa11633	ISE 3.0 APIC 統合：セキュリティグループの作成に失敗した
CSCwa18443	展開ノードのエンドポイントに 8 オクテット MAC が存在する場合、ポスチャの有効期限を処理する必要がある
CSCwa67433	ISE GUI から SAML プロバイダー情報の XML ファイルをエクスポートできない
CSCwa59621	ID グループに対する ERS API の並べ替えが一貫していない

Cisco ISE リリース 3.1 の未解決の不具合 - 累積パッチ 3

問題 ID 番号	説明
CSCwb30989	ISE UI から再起動後に SXP サービスが開始されない

問題 ID 番号	説明
CSCwb36873	ISE-PIC ノードで「ページにアクセスできません（Page not accessible）」というポップアップメッセージを取得する
CSCwb09045	正しくない cryptoLib 初期化が原因で ISE PSN ノードがクラッシュする

Cisco ISE リリース 3.1 - 累積パッチ 1 の新機能

AWS 上の Cisco ISE

- ソフトウェアバージョン Cisco ISE 3.1 パッチ 1 は、Amazon Web Services で入手できます。
- t3.xlarge という AWS インスタンスで、Cisco ISE を評価モードでインストールできるようになりました。AWS の評価モードで Cisco ISE を使用する詳細については、『*Cisco ISE Installation Guide, Release 3.1*』の「Cisco ISE Evaluation Instance on AWS」のセクションを参照してください。

  t3.xlarge インスタンスは、Cisco ISE リリース 3.1 パッチ 1 以降のリリースのみをサポートします。

OpenAPI サービス

Cisco ISE リリース 3.1 累積パッチ 1 では、次の OpenAPI が導入されています。

- ライセンス
- 自己署名証明書の生成
- パッチおよびホットパッチhttps://developer.cisco.com/docs/identity-services-engine/v1/#!cisco-ise/cisco-ise-api-service
- 導入

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Basic Setup」の章にある「Enable API Service」を参照してください。

Cisco ISE の署名付き SAML 認証要求

Cisco ISE は、署名された SAML 要求とアサーションのみを認証用に受け入れるようになりました。

詳細については、『*Cisco ISE Administrator Guide, Release 3.1*』の「Asset Visibility」の章にある「Configure SAML ID Provider」を参照してください。

Cisco ISE リリース 3.1 - 累積パッチ 1 の解決済みの不具合

次の表に、リリース 3.1 累積パッチ 1 の解決済みの不具合を示します。

問題 ID 番号	説明
CSCvo39514	コレクタログ権限のため、MnT ログプロセッサが動作しない
CSCvq53373	/ers/config/<obj>/bulk/submit が無効なロケーション URI /ers/config/<obj>/bulk/submit/<bulkID> を返す
CSCvs04091	MnT コンポーネントのコード拡張に関する包括的なバグ
CSCvt25277	2.4p12 パッチのインストールが永続的にスタックする
CSCvu47280	oddjo に同梱されている mkhomedir ツールで競合状態が検出された
CSCvu94544	ISE 3.0 BH：TACACS ライブログに、ネットワークデバイス IP の選択オプションが表示されない
CSCvv96532	DOC：この OCSP 応答の更新に対する不明な最大時間差
CSCvw65181	CIAM で POI の脆弱性が検出された
CSCvw78289	50 文字を超えるプロファイル名を使用している場合、認証に成功したことを示すライブログが表示されない
CSCvx14400	glibc の複数の脆弱性
CSCvx43866	3.0P2：アカウンティングレポートのエクスポートの完了に長時間かかる
CSCvx55668	CIAM で netty の脆弱性が検出された
CSCvy14905	CTS-SXP-CONN：デバイスから ISE SXP 接続への ph_tcp_close - Hawkeye
CSCvy43246	[CFD] ユーザーが、ポータルの作成手順でゲスト SSID を作成できない - ISE がビジーエラー
CSCvy53842	特定の証明書監査中に証明書の検証の Syslog メッセージが送信された - ISE
CSCvy69539	CIAM：openjdk - 複数のバージョン
CSCvy71229	CIAM：libx11 1.6.8
CSCvy71232	CIAM：glibc 2.28
CSCvy71238	CIAM：gnupg 2.2.9
CSCvy71239	CIAM：systemd 219
CSCvy71240	CIAM：vim 8.0.1763
CSCvy71261	CIAM：nettle 3.4.1
CSCvy71292	CIAM：unbound 1.7.3

問題 ID 番号	説明
CSCvy71296	CIAM：pcre2 10.32
CSCvy71313	CIAM：cpio 2.12
CSCvy71322	CIAM：libarchive 3.3.2
CSCvy71345	CIAM：network-manager 1.22.8
CSCvy71690	ゲストポータルの [顧客（Customer）] フィールドに & - $ # が含まれる
CSCvy75191	Cisco Identity Services Engine の XML 外部エンティティ インジェクションの脆弱性
CSCvy77472	CIAM：librepo 1.11.0
CSCvy81435	ISE ゲスト SAML 認証が [アクセス権が検証されました（Access rights validated）] HTML ページで失敗する
CSCvy82023	不適切なポスチャ複合条件のホットフィックス
CSCvy88092	スイッチで CTS PAC がアクティブにならない：ISE 3.1 ビルド 3.1.0.477 経由
CSCvy88764	CIAM：go 1.15.7 CVE-2021-33194
CSCvy92040	[ISE復元（ISE restore）] ポップアップメニューに誤ったテキストが表示される
CSCvy92536	ISE 3.0 デバイス管理ライセンスだけで、[管理（Administration）] > [システム（System）] > [ログ記録（Logging）] メニューへのアクセスが許可される必要がある
CSCvy93847	NAD でポリシーペルソナなしで SPAN を選択し、設定変更をデバイス CoA に送信できる
CSCvy94427	2.7 からの eap チェーンのポスチャリースが中断する
CSCvy94511	EPOCH 時間が null になっているため、TACACs レポートに重複したエントリが表示される
CSCvy94553	TACACS 認証レポートに重複したエントリが表示される
CSCvy94818	nmap が積極的な推測を実行したため、EP が「cisco-router」として不適切にプロファイリングされる
CSCvz00258	Tacacs AuthZ で SessionCache がクリアされないエラーのため、ヒープの使用率が高くなり、認証が遅延
CSCvz00659	バナー ブロッキング SFTP リポジトリの特殊文字

問題 ID 番号	説明
CSCvz01485	ISE 2.7 パッチ 4 で、Umbrella セキュリティプロファイルに .json ファイルをアップロードできない
CSCvz05383	P1PNSBaseline：SuperMnT：過去 30 日間の Radius Auth レポートが、フィルタ処理を含めて最大 5 分かかる
CSCvz05966	ISE 2.6 p 9、新しいグループを追加した後、デフォルトの権限がデフォルトのグループ内部に戻らない
CSCvz07191	GUI アクセスに証明書ベースの認証を使用しているときに AD グループが存在しない場合、ISE GUI がロード中にスタックする
CSCvz07823	ise 2.7 がエンドポイントのグループへの追加に失敗した
CSCvz08813	発行された証明書ページで別のページにスクロールできない
CSCvz17020	ISE GUI がすべてのライセンスをコンプライアンス違反として表示する：スマートライセンス
CSCvz18848	ローカルのエージェントレスポスチャが中断する
CSCvz20020	Okta リダイレクトが 1 番目の ID ストアで失敗し、2 番目の ID ストアが割り当てられたときに機能する
CSCvz20770	セカンダリノードの [展開（Deployment）] タブで pxgrid を有効および無効にした場合、[UI pxgrid] ページを表示できない
CSCvz27791	ISE：mdm 設定が原因で、バックアップの復元後にアプリケーションサーバーの初期化がスタックする
CSCvz28133	ユーザーがサポートバンドルを生成できない
CSCvz33839	メニューアクセスのカスタマイズが機能していない
CSCvz35550	ISE ヘルスチェック MDM 検証の誤ったアラーム
CSCvz37623	NTP（' - '）ソースの状態の説明が ISE CLI にない
CSCvz43038	CIAM：libxml 2.9.1
CSCvz43123	CIAM：jspdf 2.3.0
CSCvz43126	CIAM：systemd - 複数のバージョン
CSCvz43154	CIAM：podman 1.6.4
CSCvz43183	「名前による」呼び出しの場合、スポンサーのアクセス許可がゲスト REST API に渡されない。

問題 ID 番号	説明
CSCvz44655	ISE 管理アカウントの選択に関する問題
CSCvz45150	ISE PIC 3.1 が従来のライセンスを要求する
CSCvz46933	CIAM：jsoup 1.10.3
CSCvz49086	SQLException 発生時に ISE 3.0 TimesTen 接続が切断される
CSCvz49871	ISE GUI：net::ERR_ABORTED 404 : /admin/ng/nls/fr-fr/
CSCvz50255	CIAM：bind 9.11.20
CSCvz55258	Cisco:cisco-av-pair AuthZ 条件の機能が停止した
CSCvz57267	SAN フィールド fqdn にもかかわらず、PAN に対して発行された ISE 証明書を他のノードにインポートできない
CSCvz61191	ISE3.1で、CSV ファイルページからのエンドポイントのインポートで[ファイルの選択（choose file）] をクリックしても応答がない。
CSCvz63643	ISE 2.7：EndpointPersister スレッドが停止する
CSCvz64833	CIAM：libgcrypt 1.5.3
CSCvz65182	mtu を 1500 より大きく設定すると、mtu 値は再起動後、永続的に設定されない
CSCvz66289	ファイルをアップロードするためのローカルディスク管理 UI が壊れている
CSCvz67479	すべてのフィールドの [ローカルログの設定（Local Log Settings）] ツールチップに、無関係で役に立たない「信頼できる証明書（Trust Certificates）」が表示される
CSCvz68091	ゲストタイプの設定変更が監査レポートで更新されない
CSCvz72034	ISE 3.1：DNAC からネットワークデバイスを更新している間、共有シークレット/パスワードが空であるかマスクされている
CSCvz72069	Pxgrid が ISE-PIC の [概要（Summary）] ページで無効と表示される
CSCvz72208	ISE 3.1：[認証（Authentication）] タブで、[コンテキストの可視性（Context Visivility）] に空白の結果が表示される
CSCvz72225	検出ホストに FQDN を追加すると、検出ホストの IP アドレスまたはホスト名が無効になる
CSCvz73445	Windows 10 デバイスのエージェントレスポスチャがマルウェア対策チェックに合格しない -

問題 ID 番号	説明
CSCvz77482	ISE 3.0 はゲストの自己登録ポータルの一部として「場所」設定を選択解除できません
CSCvz80829	3.2 のフルアップグレードでバージョンの事前チェックが失敗する
CSCvz85117	ISE ヘルスチェックおよび I/O 帯域幅のパフォーマンスチェックの誤報
CSCvz87476	サポートされていないメッセージコード 91104 および 91105 アラーム
CSCwa00729	特定の NAD 削除により、すべての NAD が削除された
CSCvz86020	「開かれているファイルが多すぎます（too many files open）」エラーにより、ライブログ/セッションに最新のデータが表示されない
CSCwa12273	「操作が許可されていません（Operation is not permitted）」エラーにより、ネットワーク管理者グループの AD ユーザーが管理者ユーザーを作成/編集できない
CSCvz66279	7 日以上前の Radius レポートが空（CSCvw78289 の回帰）
CSCvz91116	Oracle プロセスが増加し、TNS を取得中：接続が切断される

Cisco ISE リリース 3.1 - 累積パッチ 1 の未解決の不具合

問題 ID 番号	説明
CSCwa09113	内部 CA の失敗「OCSP ステータスが不明なため、12557 ユーザー認証に失敗しました（12557 User Auth failed because OCSP status is unknown）」による単一の Byod フロー

Cisco ISE ソフトウェア ダウンロード サイトでの Cisco ISE 3.1 ファイルの置き換え

Cisco ISE ソフトウェア ダウンロード サイトで Cisco ISE 3.1 OVA、ISO、およびアップグレード バンドル ファイルが置き換えられました。

どのような変更が加えられたか

- このビルドでは、次のバグが解決されています。
  - CSCwa04370：ISE 3.1 では、2 つのインターフェイスが IP アドレスで設定されており、デフォルトゲートウェイが eth1 のサブネットを参照している場合、デフォルトインターフェイスの誤った発信インターフェイスが表示されます。
  - CSCwa82553：ボンディングが設定されている場合、ISE 3.1 のデフォルトルートが間違ったインターフェイス上に配置される

- ZTP ツールで ICMP、DNS、および NTP チェックをスキップするオプション。詳細については、『*Cisco ISE Installation Guide, Release 3.1*』の「Additional Installation Information」の章にある「Zero Touch Provisioning」を参照してください。

（注）

- 新しいファイルのファイル名には、ビルド番号に「a」が付加されます（例：ise-3.1.0.518b.SPA.x86_64.iso）。
- SNS 3695 OVA テンプレートを VMware vCenter コンテンツライブラリにインポートする場合は、ISE-3.x.x.xxx-virtual-SNS3695-1800.ova テンプレートを使用できます。この OVA テンプレートは ISE-3.x.x.xxx-virtual-SNS3695-2400.ova テンプレートに似ていますが、ディスクサイズが 2 TB を超える OVA のインポートを防ぐ Vmware vCenter コンテンツライブラリの制限事項を回避するため、予約済みディスクサイズが 2400 GB から 1800 GB に削減されています。
- **show tech-support** コマンドの出力に次の ISE バージョンが表示されます。

  ```
  ZTPBUNDLE
  ```

- 既存の Cisco ISE 3.1 パッチは、このビルドで正常に機能します。

Cisco ISE リリース 3.1 の解決済みの不具合

問題 ID 番号	説明
CSCwa04370	ISE 3.1 では、2 つのインターフェイスが IP アドレスで設定されており、デフォルトゲートウェイが eth1 のサブネットを参照している場合、デフォルトインターフェイスの誤った発信インターフェイスが表示されます。
CSCwa82553	ボンディングが設定されている場合、ISE 3.1 のデフォルトルートが間違ったインターフェイス上に配置される
CSCuo73496	RADIUS 最大 session-timeout 値が 65535 に制限される
CSCvf61114	「認証プロファイル」に対する ERS の作成/更新で XML スキーマの検証が失敗する
CSCvf88737	ポータルビルダーで作成されたポータルに空白のゲストポータルウィンドウが表示される
CSCvg75448	クライアント プロビジョニング ポータルのサポート情報のカスタマイズがない
CSCvg77872	ポータルがスポンサー付きゲストポータルに設定されている場合、ゲスト承認の電子メールにロゴが表示されない
CSCvh04231	「ゲストユーザー情報を保存」の RADIUS アカウンティングおよびアクセス許可でゲストユーザー名が送信されない

問題 ID 番号	説明
CSCvi53134	passive-id サービスが有効になった後、AD 結合に使用されるアカウントがロックされることがある
CSCvi59005	スクロールバーを使用すると、AD グループの完全なリストが表示されない
CSCvk11224	レポートの名前変更に関する問題
CSCvm47584	ポスチャリースが原因で 1 日を超えた猶予期間を設定できない
CSCvn25548	管理者ログイン情報での MnT API 呼び出しによりアカウントが無効になる
CSCvn38371	GUI へのログイン時にセッション情報のポップアップを抑制する機能
CSCvo02275	プロファイリングと条件スタジオがロードされない、または最大 30 分かかる
CSCvo56767	ISE-PIC GUI 管理者ユーザー設定を変更しようとしたときのエラー
CSCvo75723	エンドポイント消去のレポートを実行したとき、消去されたエンドポイント数が 0 の場合、レポートが表示されない
CSCvp88242	デバイスポータルを更新する際の不正な要求エラー
CSCvq44063	DNS の不正な設定により、TACACS 認証または RADIUS 認証に失敗する
CSCvq58506	show running-config を完了できない
CSCvr22065	共有秘密キーに特殊文字が含まれていると、エラーとともに NAD のインポートが失敗する
CSCvr76539	ネットワーク デバイス グループへの変更が Change Audit ログに反映されない
CSCvs24459	ID グループなしの ISE 内部ネットワーク アクセス ユーザーを管理できない
CSCvs27232	[RADIUS認証のトラブルシューティング（RADIUS Authentication Troubleshooting）] ウィンドウが適切にフィルタリングされない
CSCvs29611	Cisco ISE 2.4 パッチ 5 が頻繁にクラッシュしてコアファイルを生成する
CSCvs81248	PassiveID アラームを、各 DC の非アクティブ状態に対して個別にトリガーする必要がある
CSCvs81264	PSN は、PassiveID エージェントからのマッピングの遅延を識別できる必要がある

問題 ID 番号	説明
CSCvt64739	アプリケーションサーバーの初期化に時間がかかる
CSCvt65332	[クライアント プロビジョニング リソース（Client Provisioning Resources）] ウィンドウの [プロファイルの説明（Profile Description）] フィールドを更新しているときに、Enter キーを使用して新しい行を作成すると、「ネットワークエラーが原因でサーバーの応答を受信できません（Fail to receive server response due to the network error）」というメッセージが表示される
CSCvt85370	ポスチャ条件が「vc_visInst_v4_CiscoAnyConnectSecureMobilityのチェックでClient_4_xが見つかりません（Check vc_visInst_v4_CiscoAnyConnectSecureMobility Client_4_x is not found）」エラーで失敗する
CSCvt94587	ISE ルート CA の再生成中に「プラスライセンスはコンプライアンス違反（Plus License is out of compliance）」メッセージが表示される
CSCvu04874	io.netty.buffer.PoolChunk での疑わしいメモリリーク
CSCvu05121	SMTP サーバーの変更後にゲスト電子メールが送信されない
CSCvu14215	AD グループの追加/削除中にスポンサー グループ メンバーシップが削除される
CSCvu22058	DUO を外部 RADIUS プロキシとする ISE で access-reject がドロップされる
CSCvu33861	ISE 2.4 パッチ 6：MAC アドレスでデバイスを取得する REST API MnT クエリに 2 分以上かかる
CSCvu47779	変更設定監査レポートの IP アドレスと CSV エクスポートの変更されたプロパティが欠落している
CSCvu62938	プライマリ PSN または PAN に到達できない場合にポスチャが失敗する
CSCvu84184	ゲストポータルで証明書チェーンが送信されない
CSCvu84773	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCvu87758	ゲストパスワードポリシー設定がアルファベットまたは数字で設定されていると保存できない
CSCvu89715	ISE ヘルスサマリレポートの時間対スループットのチャートで、間違った単位を使用している
CSCvu90761	ISE の [Radiusライブセッション（Radius Live Sessions）] ウィンドウに [データが見つかりません（No Data Found）] と表示される
CSCvu91039	ISE がすべての MAC アドレスのルックアップを行わず、リダイレクトなしのポスチャが失敗する

問題 ID 番号	説明
CSCvu94025	ISE が syslog ターゲットに対してのみ IP を許可するか、DNS キャッシングを提供する
CSCvu97657	エンドポイントのデバッグを有効にすると、ISE 2.4 アプリケーションサーバーが初期化状態になる
CSCvv00951	停止状態への移行中にアプリケーションサーバーがクラッシュする
CSCvv02998	MAC 11 Big sur BYOD フローが失敗した
CSCvv04416	エンドポイントデータがセカンダリ管理ノードに表示されない
CSCvv04957	GRUB2 の任意のコード実行の脆弱性
CSCvv08466	ログ収集エラーアラームが表示される
CSCvv09127	ゲスト API が、制限されたスポンサーに、許可されていないゲストタイプでもゲストアカウントを作成することを許可する
CSCvv10683	ドロップされたセッションのセッションキャッシュがクリアされず、PSN で高い CPU 使用率が発生する
CSCvv14001	共通タスクでセキュリティグループを選択すると、認可プロファイルが適切な属性で保存されない
CSCvv14390	最大セッション数制限がユーザーとグループに対して機能しない
CSCvv15060	ネットワークリストに戻ると、適用されたフィルタが削除される
CSCvv16401	pxGrid 内部クライアントの ping に失敗した
CSCvv19065	[DNACアシュアランス（DNAC Assurance）] ウィンドウでゲスト ID を表示できない
CSCvv25102	ISE で TACACS+ および TCP を強化するための TCP 設定の変更
CSCvv27690	HTTPS、EAP、DTLS、および PORTAL の ISE 証明書を更新すると、PORTAL ロールと Admin ロールのみが適用される
CSCvv29190	iOS 14 beta で BYOD フローが破損している
CSCvv29737	DNA ACA セキュリティグループの同期が JDBCException エラーで失敗する
CSCvv30133	ディスカバリホストの説明テキストが紛らわしい
CSCvv30161	ライブセッション詳細レポートで、VPN ポスチャシナリオについて誤った認証プロファイルと認証ポリシーが表示される

問題 ID 番号	説明
CSCvv30226	Livelog セッションで、VPN ポスチャシナリオに誤った認証ポリシーが表示される
CSCvv30274	[コンテキストの可視性（Context Visibility）] に、VPN ポスチャシナリオの誤った認証プロファイルと認証ポリシーが表示される
CSCvv31500	ISE ゲストポータルの登録と有効期限の電子メールは、ポータルに入力された形式を維持する必要がある
CSCvv35921	内部 ID ストア内の選択したユーザーに対して CSV エクスポートを開始できない
CSCvv36189	無効な IPv6 アドレスが原因で RADIUS の passed-auth ライブログが送信されない
CSCvv38249	カスタムポートのみが有効な場合、手動 NMAP が動作しない
CSCvv39000	LANDESK のポスチャ条件を作成できない
CSCvv41935	キーに < 記号または > 記号が含まれていると、PSK cisco-av-pair がエラーをスローする
CSCvv43383	NFS リポジトリが GUI から機能しない
CSCvv44401	自己署名証明書を生成すると、CSR のデフォルトパラメータが事前にインストールされた自己署名証明書と一致しない
CSCvv45063	ノードが展開から削除されたときに内部 CA 証明書が削除されない
CSCvv45340	running-config の保存エラーにより、スタートアップ設定が失われる
CSCvv46034	TACACS 設定の更新中、デバイス管理サービスが無効になる
CSCvv46958	NDG 列が 255 文字を超えると、TrustSec が有効になった NAD が TrustSec マトリックスに表示されない
CSCvv47849	Cisco DNA Center でセキュリティグループ名が変更された場合、マッピングされた SGT エントリが認証ルールからクリアされる
CSCvv50028	ISE ノードのリセット設定後にヒープダンプの生成が失敗する
CSCvv50168	ISE は 30 日を超えるポスチャの猶予期間を許可する必要がある
CSCvv50721	Aruba ダイナミック URL リダイレクトを使用して NetworkSetupAssistant.exe のダウンロードリンクを取得できない
CSCvv52637	ISE ホットスポット ゲスト ポータル フローが破損している

問題 ID 番号	説明
CSCvv53221	ISE_EST_Local_Host RADIUS 共有シークレットが空の場合、アプリケーションサーバーが「初期化中（Initializing）」としてマークされる
CSCvv54761	現在アクティブなセッションレポートのエクスポートには、午前 0 時以降に更新されたセッションのみが表示される
CSCvv54798	CLI からエクスポートされたコンテキストの可視性 CSV に IP アドレスが表示されない
CSCvv55663	ISE ノードのリロード後に ISE 2.6/2.7 リポジトリが削除される
CSCvv57628	一時停止されたゲストユーザーがエンドポイントグループから自動的に削除されない
CSCvv57639	TACACS コマンドセットでカッコ付きのコマンドを保存するとエラーが発生する
CSCvv57830	コンテキストに空の値が追加されたため、グループのルックアップが失敗した
CSCvv58629	EST サービスを初期化する認証局サービスが ISE 2.7 パッチ 2 へのアップグレード後に実行しない
CSCvv59233	ISE RADIUS ライブログの詳細で、[Other Attributes] セクションに AD グループ名がない
CSCvv60014	/opt フォルダの空き容量が 1 TB 以上の場合、運用バックアップがエラーをスローする
CSCvv60353	合計レコード数が 500 万を超えると、認証概要レポートがスタックする
CSCvv60686	ISE SXP にはセッションから学習した古いマッピングをクリアするメカニズムが必要
CSCvv60923	内部ユーザーのカスタム属性の IP データ型で転送スラッシュを使用する機能の追加が必要
CSCvv61732	異なる SNMP サーバーに対して一意のコミュニティストリングを作成できない
CSCvv62382	プロキシバイパス設定で大文字を使用できない
CSCvv62549	エンドポイントの GUI ページに Clinda のカスタム属性が表示されない
CSCvv62729	存在しないネットワークデバイスを照会すると、ネットワークデバイス API コールがエラー 500 をスローする

問題 ID 番号	説明
CSCvv63548	PSN rmi GC の収集が正しく機能せず、PassiveID フローでメモリリークが発生する
CSCvv64190	ユーザーアイデンティティグループで大文字と小文字が区別されるため、[スポンサーグループメンバーの選択（Select Sponsor Group Members）] ウィンドウがロードされない
CSCvv65036	PSN ノードでのメモリリーク
CSCvv67051	[RADIUSサーバー順序（RADIUS Server Sequences）] ウィンドウに「使用可能なデータがありません（no data available）」と表示される
CSCvv67091	Cisco Identity Services Engine の信頼できないファイルアップロードの脆弱性
CSCvv67743	状態別ポスチャ アセスメント レポートに、状態ステータスフィルタなしのデータが表示される
CSCvv67935	認証プロファイルのセキュリティグループの値が取得直後に表示されない
CSCvv68028	AUP テキストを変更できない
CSCvv68293	ローカルまたはグローバルの例外を使用する場合、ISE がプラスライセンスを使用しない
CSCvv72418	ISE 3.0 REST ID ログファイルがサポートバンドルに含まれていない
CSCvv74361	ISE 3.0 ヘルスチェックライセンス検証の誤ったアラーム
CSCvv77007	ISE が内部のネットワーク管理者ユーザーのリクエストを外部の RADIUS トークンサーバーに絶えず送信する
CSCvv77530	バインドパスワードで % 文字が 2 回以上使用されている場合、LDAP グループ/サブジェクト属性を取得できない
CSCvv77914	[クライアント プロビジョニング（Client Provisioning）] ウィンドウに現在の設定が正しく表示されない
CSCvv77928	プライマリ PAN の障害後、「予期しないエラーが発生しました（An unexpected error occurred）」というメッセージとともに、証明書の一括生成に失敗した
CSCvv78097	ローカルディスクの使用情報がない
CSCvv79940	ISE で SAN の hostname-x を使用して CSR を生成するとエラーになる
CSCvv80113	ポスチャ自動更新が実行されない
CSCvv80297	ROPC の CTL に DigitCert グローバルルート G2 が必要

問題 ID 番号	説明
CSCvv82806	ネットワークデバイス IP フィルタがサブネット内の IP と一致しない
CSCvv83510	RuleResultsSGTUpgradeService ステップでアップグレードが失敗する
CSCvv85588	PassiveID フローを使用した PSN ノードでの高いメモリ使用量
CSCvv91007	接続に失敗すると、[スマートライセンスの権限付与（Smart Licensing Entitlement）] タブが [更新（Refreshing）] でスタックする
CSCvv91234	プライマリ MnT がダウンしていると、ISE 2.6 のスケジュール済みレポートが機能しない
CSCvv91684	ISE コレクションフィルタが GUI に表示されない
CSCvv92203	「Employees」という名前で SGT を作成しようとすると、「入力された名前の NetworkAuthZProfile は既に存在します（NetworkAuthZProfile with entered name already exists）」というメッセージが表示される
CSCvv92613	スポンサーグループに属していないユーザーがスポンサーポータルにログインできる
CSCvv92638	スケジュール設定と運用バックアップを当日と同じ開始日に設定することができない
CSCvv93442	SFTP サーバーのファイルパスに二重スラッシュ「//」が追加された
CSCvv94791	DNAC と ISE の間で GBAC 設定が同期されない
CSCvv95150	Cisco Identity Services Engine のストアドクロスサイトスクリプティングの脆弱性
CSCvv95516	[ISE PICライセンス（ISE PIC Licensing）] ウィンドウがロードされない
CSCvv96532	「thisUpdate of OCSP response」で最大時間差が指定されない
CSCvv99093	ISE ノードが断続的にキューリンクアラームをトリガーする
CSCvw00375	ISE 2.7 パッチ 2 のカスタムビューの [コンテキストの可視性（Context Visibility）] ウィンドウをロードできない
CSCvw01225	ISE の設定復元が 40% で失敗し、「IMPDP を使用した DB の復元が失敗しました（DB Restore using IMPDP failed）」というエラーが表示される
CSCvw01829	Chrome バージョン 85/86 を使用しているときに ISE GUI ログインページにエラーが表示される
CSCvw02887	PassiveID フローに AD グループを追加後のメモリリーク
CSCvw03693	内部ユーザー「chrony」が作成されないため、NTP が機能しない

問題 ID 番号	説明
CSCvw06722	スポンサーが、作成されたゲストユーザーのリストを表示できない
CSCvw08292	削除メッセージの後、ACI マッピングが削除されない
CSCvw08330	サードパーティの NAD のダイナミック リダイレクションでポスチャが機能しない
CSCvw08602	IP オーバーラップの場合にエラーがスローされない
CSCvw09827	PSN ノードの高 CPU 使用率
CSCvw16237	プライマリ MnT のリロード後、スケジュール済みの運用データバックアップがトリガーされない
CSCvw17908	デフォルトルートにタグ付けされている場合、ISE からスイッチへの SGT マッピングに対する IP のプッシュが機能しない
CSCvw19785	外部データ ソースのポスチャ条件を編集すると、常に間違った AD が表示される
CSCvw20021	NAD の場所が [コンテキストの可視性のエラスティック検索（Context Visibility ElasticSearch）] で更新されない
CSCvw20060	Windows ネットワーク インターフェイスよりも先にエージェントサービスが起動した場合、エージェントで DC がダウンとしてマークされる
CSCvw20636	NAD プロファイルが削除された後、認証プロファイルに「No data available（データがありません）」と表示される
CSCvw24227	例外が原因でエンドポイントが消去されない
CSCvw24268	Cisco Identity Services Engine の信頼できないファイルアップロードの脆弱性
CSCvw25285	PassiveID がマルチ接続 syslog クライアントで安定して動作しない
CSCvw26415	ISE 3.0 で CN および SAN が欠落している証明書が信頼できる証明書ストアにインポートされない
CSCvw26570	国際電話番号ドロップダウンボックスが ISE 2.7 で機能しない
CSCvw28441	API の使用中に NAD の共有秘密がログに表示される
CSCvw29490	内部ユーザーのカスタム属性が CoA プッシュで送信されない
CSCvw31269	SAML グループがスポンサーポータルグループで適用した場合に機能しない

問題 ID 番号	説明
CSCvw33115	VPN のユースケースで ISE MnT ライブセッションのステータスが「ポスチャ済み（Postured）」に変わらない
CSCvw34491	Essentials ライセンスを有効にすると、[ネットワークデバイス（Network Devices）] タブへのアクセスのみがブロックされる
CSCvw36486	IP アクセス制限を適用した後、GUI にアクセスできない
CSCvw36743	パスワードに特殊文字を使用すると、ISE サービスアカウントがロックされ、WMI が確立されない
CSCvw37844	ISE で内部コールにホスト名が使用されるため ANC CoA が機能しない
CSCvw38530	[バックアップと復元（Backup and Restore）] ウィンドウのロード中に、リポジトリの ise-psc.log に例外が表示される
CSCvw38853	MAC OSX のマルウェア対策条件に Sophos 10.x の定義がない
CSCvw44120	ISE 3.0 でのゲストポータル作成の失敗
CSCvw46096	ISE 3.0 Syslog プロバイダーが設定を適用できない
CSCvw48396	Cisco ADE-OS のローカル ファイル インクルードの脆弱性
CSCvw48403	エンドポイントについて収集された SNMP 情報が ISE で処理されない
CSCvw48697	API IP SGT マッピングが [No Devices] の結果を返さない
CSCvw49938	TACACS コマンドの前にスペースを含むサードパーティデバイスについて、TACACS コマンド アカウンティング レポートがない
CSCvw50381	猶予アクセスの期限が切れたときに Aruba WLC に対する CoA-disconnect が ISE で発行されない
CSCvw50829	RBAC ポリシーで AD セキュリティグループの OU の末尾をドット文字にできない
CSCvw51787	ISE が、自己署名証明書の上に CA 署名付き証明書をインポートすることを許可しない
CSCvw51801	「ポスチャ済みライブセッション（Postured Live Session）」状態であったセッションが、NAD からアカウンティングの中間更新を受信すると「開始済み（Started）」に移行する
CSCvw53412	SB で Hibernate.log を収集する必要がある
CSCvw54878	日本語の GUI に 50 以上のルールがある場合、ISE が完全認証のルールを表示しない

問題 ID 番号	説明
CSCvw55793	ISE が「ID 割り当てに失敗しました（Identifier Allocation Failed）」というエラーとともに、PSN からの CoA の送信に失敗する
CSCvw61589	ポリシーセットの削除後に RADIUS 要求がドロップされた
CSCvw61786	スキーマオブジェクトをドロップする前に、すべてのプロセスを停止する必要がある
CSCvw63264	ISE 3.0 ポリシー条件スタジオ GUI バグ
CSCvw66483	選択した外部サーバーのリストが変更されると、RADIUS サーバーが間違った順序になる
CSCvw68480	ISE 展開で複数の SXP ノードを使用している場合、マッピングの総数が正しく表示されない
CSCvw68512	ゲスト ユーザーが誤った有効期間で作成される
CSCvw68944	スポンサーポータルで中国語を使用していると、設定日に誤った週情報が表示される
CSCvw69977	「すべての SXP マッピング（All SXP Mapping）」表に、ISE で終了したセッションが含まれる
CSCvw73928	関連しない NTP 同期失敗アラームを変更する必要がある
CSCvw75397	IP アクセスが有効な場合に MnT ノード名が NULL に設定される
CSCvw75563	パスコードフィールドに特殊文字が含まれていると、ホットスポット ゲスト ポータルでページロードエラーが表示される
CSCvw76847	侵入テスト時に ISE 条件ライブラリが破損する
CSCvw77219	Dot1x 認証がマネージャの重複のため失敗した
CSCvw78019	ISE 2.7 へのアップグレード後に NTP が同期しない
CSCvw78269	CWE-20：ノードグループの作成の入力検証が正しくない
CSCvw78289	50 文字を超えるプロファイル名を使用している場合、認証に成功したことを示すライブログが表示されない
CSCvw80520	ISE メッセージングサービスが無効になっている場合、「RADIUS 認証の詳細」レポートに時間がかかる
CSCvw81454	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw82774	ユーザー ID グループでユーザー名に基づくソートが機能しない

問題 ID 番号	説明
CSCvw82784	TACACS+ のエンドステーション ネットワーク条件のスクロールバーが機能しない
CSCvv82815	認証プロファイルの CWA オプションが、一部のネットワーク デバイス プロファイルで正しく機能しない
CSCvw82927	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw83296	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw83334	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw84127	設定監査の詳細に変更されたポリシーセットが表示されない
CSCvw85599	[TACACS+デバイスネットワーク条件（TACACS+ Device Network Conditions）]および[デバイスポートネットワーク条件（Device Port Network Conditions）] タブのスクロールバーが機能しない
CSCvw85860	ISE pxGrid の例外のログレベルは DEBUG ではなく ERROR である必要がある
CSCvw87147	ライブセッションで正しいアクティブセッションが表示されない
CSCvw87173	MAC アドレスを表す AD オブジェクトが「無効（disabled ）」状態の場合、MAB 認証が失敗する
CSCvw87175	Active Directory を使用した MAB 認証が AD オブジェクトが無効でも成功する
CSCvw88881	DB クリーンアップの毎時 cron で DB ロックが取得される結果、展開の登録に失敗する
CSCvw89326	PKI ベースの SFTP の場合、MnT ノードの GUI キーのエクスポートは、PAN として昇格した場合にのみ可能
CSCvw89818	Cisco Identity Services Engine の機密情報の開示における脆弱性
CSCvw90961	RBAC ルールが ISE 2.7 で適用されない
CSCvw93570	ゲストポータルを編集、複製、削除できない
CSCvw94603	ポーリング間隔の変更が外部 MDM サーバー（Microsoft_intune）に反映されない
CSCvw96371	API からカスタム属性を更新すると、EP から静的ポリシーとグループの割り当てが失われる
CSCvw97905	内部ユーザーエクスポート機能で、パスワードに無効な文字が含まれていてもエラーが表示されない

問題 ID 番号	説明
CSCvx00245	MDM ウィンドウで Itune 統合がエラーをスローするが、テスト接続は正常に動作している
CSCvx00345	Azure AD グループを取得できない
CSCvx01272	証明書の一括生成に ISE の自己署名証明書が含まれていない
CSCvx01798	ネットワークデバイスを追加すると、「ネットワークデバイスをロードできません（Unable to load NetworkDevices）」というエラーが表示される
CSCvx04512	login.jsp に直接アクセスすると証明書ベースの認証による管理アクセスがバイパスされる
CSCvx04692	「None」という名前のノードグループを作成すると、レプリケーションが中断される
CSCvx09383	コンテキストの可視性の「実行中のプロセス」でエンドポイントのアプリケーションを並べ替えようとすると、エラーが表示される
CSCvx10186	スマートライセンスに登録した後も ISE が評価期限切れ状態のままになる
CSCvx11857	ISE TrustCert ストアの古い証明書エントリが原因で、特定のページのロードが遅延
CSCvx15427	ヘルスチェックでの DNS 解決可能性：CNAME としての ISE FQDN で誤ったエラー
CSCvx18730	シスコ製品に影響する Sudo 権限昇格の脆弱性：2021 年 1 月
CSCvx22229	結合インターフェイスの IP アドレスを変更すると、「ipv6 address autoconfig」が削除される
CSCvx27632	認証が [ODBCストアドプロシージャ（ODBC Stored-Procedures）] ウィンドウで設定された形式で MAC アドレスをルックアップする必要がある
CSCvx28402	ISE 2.7 以降のサポートバンドルで ise-jedis.log ファイルがキャプチャされない
CSCvx30276	ルート CA の再作成時に Jedis DB 接続プールが再作成されない
CSCvx32666	ポリシーセットのエントリの評価で認証方式の条件が照合されない
CSCvx37149	すべてのペルソナを同じノードで実行している SNS 3515 の SGA 値が under-provisioned になる
CSCvx37297	シングルサインオン/Kerberos ユーザーアカウントでのスポンサーポータル認証でエラー 400 が発生

問題 ID 番号	説明
CSCvx37467	ポータル設定で「携帯電話番号（mobile number）」フィールドにチェックが付いていない場合、スポンサーポータルが「無効な入力」を提供する
CSCvx41826	Tenable SC 5.17 ですべての tenable アダプタリポジトリを取得できない
CSCvx43566	外部のユーザー名と誤ったパスワードを使用している場合に、ログインの失敗がログに記録されない
CSCvx43825	NAS-IP アドレスが指定されていない acct stop を受信した場合に、セッションが「開始（started）」状態のままになる
CSCvx44815	ISE AD ランタイムで a1-a2-a3-a4-a5-a6 から a1a2a3a4a5a6 への書き換えをサポートする必要がある
CSCvx45481	エンドポイントを新規スイッチポートに変更し、エンドポイント ID グループを変更すると、CoA が失敗する
CSCvx46638	EAP チェーンの場合にポスチャポリシーでマシン AD グループメンバーシップを取得できない
CSCvx47691	動的認証後に、セッションディレクトリのトピックがユーザーの SGT 属性を更新しない
CSCvx47891	新しいエンドポイントの AMP イベントが正しくマッピングされない
CSCvx48922	TACACS フローのメモリリーク
CSCvx53205	NIC ボンディングにより、MAR キャッシュが複製されない
CSCvx53905	承認ポリシー条件の形式が正しくありません
CSCvx54213	[デフォルトのネットワークデバイス（Default Network Devices）] ウィンドウで、設定のために Plus ライセンスを要求される
CSCvx57433	TrustSec ポリシーマトリックスにより、ISE 3.0 での制限付きスクロールが許可される
CSCvx57545	isedailycron temp1 のトラッキングにより AWR レポートで遅延が発生する
CSCvx58516	「ネットワークデバイス別上位 N の認証（Top N Authentication by Network Device）」レポートでネットワークデバイスをクリックすると、RADIUS 認証ではなく TACACS 認証にリダイレクトされる
CSCvx60818	ERS 自己登録ポータルの更新により、PSN で期待されるようにフィールドが削除されない
CSCvx61462	ISE ログ収集エラー「セッションディレクトリの書き込みに失敗しました（Session directory write failed）」

問題 ID 番号	説明
CSCvx61664	ISE で AnyConnect 出力設定ファイルの JSON ファイルの情報が更新されない
CSCvx64247	国コードのドロップダウンオプションを使用すると、モバイルデバイスに「無効な電話番号形式（Invalid phone number format）」エラーが表示される
CSCvx69701	データベース接続が利用できないため、展開が同期しなくなった
CSCvx70633	ISE がネットワークデバイス trustsec 設定の EXEC またはイネーブルモードパスワードで % を受け入れない
CSCvx72642	バックアップインターフェイスが設定されている場合、REST 認証サービスが無効になる
CSCvx78643	現在の展開で電子メールアドレスが設定されていない場合でも、レガシーデータを使用してすべてのシステムアラームで電子メールが送信される
CSCvx79693	ISE との Qualys の統合が失敗する
CSCvx82808	CA 署名付き証明書を使用すると、MacOS Big Sur 11.x BYOD が EAP-TLS に失敗する
CSCvx85355	ポスチャ猶予期間の最大許容値を 30 日から 90 日に増やす
CSCvx85391	ログイン文字の大文字小文字が原因で、内部ユーザーの非アクティブタイマーが更新されない
CSCvx85675	ISE が、競合状態が原因の SXP-IP マッピング伝搬の削除/追加を処理できない
CSCvx85807	ISE および ISE-PIC で、登録解除フローのスマートライセンスが機能しない
CSCvx86571	ログインページのメッセージが空の場合は説明のボックスを削除する必要がある
CSCvx86915	TrustSec ウィンドウの UI に問題がある
CSCvx86921	RADIUS トークン ID のソースプロンプトと TACACS 認証の内部ユーザープロンプト
CSCvx94452	ISE 2.7 パッチ 2 以降で EST サービスが実行されない
CSCvx96190	上位認証レポートで、スケジュールされたレポートのフィルタが表示されない
CSCvx97249	PAN はポート 8905 でリッスンすべきではない

問題 ID 番号	説明
CSCvx97501	パスワードに Base64 以外の文字が含まれていると ROPC 認証が失敗する
CSCvx99151	内部 ERS ユーザーが外部 ID ストアを介して認証を試み、REST の遅延が発生する
CSCvx99176	「-」 または「 *」 を使用した NAD IP 定義が完全な IP 比較を実行しない
CSCvy04443	再認証用の MNT REST API が分散型展開で（個別の MnTとともに）使用されると失敗する
CSCvy04665	完全な数値 ID エントリを照合すると、TACACS レポートの詳細フィルタが機能しない
CSCvy05954	[すべてのSXPマッピング（All SXP Mappings）] ウィンドウに、セッション経由で学習した IPv6 マッピングが表示されない
CSCvy06719	「手動アクティブセッション（Manual Active Session）」 レポートが空
CSCvy07088	エージェントレスポスチャがエンドポイントの信頼できるストアに CA 証明書チェーンをインストールしない
CSCvy10026	ISE 管理証明書 CN が FQDN と等しくない場合、エージェントレスポスチャが失敗する
CSCvy11617	Windows ユーザー名にスペースが含まれていると、エージェントレスポスチャが中断する
CSCvy14342	PIP クエリ評価が原因で、ISE 2.6 パッチ 3 以降の PSN ノードで高い CPU が見られる
CSCvy15058	API 経由でドメインを「ブロック/許可する」に更新できない
CSCvy15172	Cisco Identity Services Engine のセルフ クロスサイト スクリプティングの問題
CSCvy17893	ISE REST API が IP-SGT マッピングに重複する値を返す
CSCvy18560	「RADIUS アカウンティングの詳細（RADIUS Accounting Details）」 レポートにアカウンティングの詳細が表示されない
CSCvy20277	一部のオブジェクトの [説明（Descriptions ）] フィールドで以前は許可されていた特殊文字が使用できなくなった
CSCvy23354	FF 88 で、[ISE認証プロファイル（ISE authorization profile）] UI の [説明（Description）] フィールドの最大高が小さすぎる
CSCvy24370	ISE が RADIUS サーバーのシーケンス設定で 6 つを超える属性の変更を受け入れない

問題 ID 番号	説明
CSCvy25533	CLI バックアップ中に「/opt/CSCOcpm/config/cpmenv.sh:line 396:<ipv6>:command not found」エラーが表示される
CSCvy25550	ISE が認証プロファイルの Framed-IPv6-Address でカスタム属性の名前を受け入れない
CSCvy30119	オプションに他の変更を加えると、LDAP グループがスポンサーグループから消える
CSCvy32461	[電話/電子メール（phone/email）] フィールドが入力されている場合、スポンサーユーザーがデータを編集できない
CSCvy34977	証明書テンプレートの曲線タイプ P-192 が原因で、アプリケーションサーバーが「初期化（initializing）」状態でスタックする
CSCvy36868	ISE 2.3 以降のバージョンでは、コマンドセットで「改行」 <cr> 文字をサポートしていない
CSCvy38459	ISE 2.7 パッチ 3 GUI で、すべてのデバイスの管理認証ポリシーが表示されない
CSCvy38896	Framed-IP 値のない AAA 要求により、SXP プロセスで例外が発生する
CSCvy40845	ERS リクエストを通じてカスタム属性を更新すると、別の属性も更新される
CSCvy41066	ポリシーの条件として TACACS カスタム AV ペアが機能していない
CSCvy42885	設定バックアップのキャンセルによる ISE アプリケーションサーバーのクラッシュ/再起動
CSCvy45015	「電話番号をユーザー名として使用（Use Phone number as username）」オプションが有効な場合の、重複ユーザーの ISE ゲスト自己登録エラー
CSCvy46504	ポリシーを展開しようとすると、Cisco DNA Center で断続的にエラーが発生する
CSCvy48766	All Numbers サブドメインが使用されている場合、ISE のインストールが「データベースのプライミングが失敗（Database Priming Failed）」エラーで失敗する
CSCvy51073	ISE 認証プロファイルの ERS 更新が accessType 属性の変更を無視する
CSCvy58771	NAD の編集中に、間違ったデバイスプロファイルがマッピングされる
CSCvy60752	CLI 経由で設定をリセットした後、セットアップウィザードのパスワードでハイフンがサポートされない

問題 ID 番号	説明
CSCvy61564	ISE 2.7 パッチ 3 ERS コールが 3 文字の RADIUS 共有シークレットを受け入れない
CSCvy61894	キーペアの生成はスペースを受け入れるが、キーをエクスポートできない
CSCvy62875	[400] Apple デバイスの SAML SSO OKTA による不正なリクエストエラー
CSCvy63778	CoA の REST API が任意のサーバー IP で動作する
CSCvy65786	% を含む AD アカウントパスワードを使用して WMI を設定するとエラーになる
CSCvy71690	ゲストポータルの [顧客（Customer）] フィールドに & - $ # が含まれる
CSCvy74456	ISE 経由の認証が「無効なログイン情報（Invalid login credentials）」エラーで失敗する
CSCvy74919	非アクティブタイマーに達した後、ISE 内部ユーザーが無効にならない
CSCvy76262	ISE DACL 構文バリデータが ASA のコード要件に準拠していない
CSCvy76601	確認ポップアップでエンドポイントの数が正しくないことを示す「すべて」の機能を削除
CSCvy76617	[NAD] ページのフィルタの有無にかかわらず、[すべてのデバイスを選択（Select ALL device）] オプションが必要
CSCvy82023	不適切なポスチャ複合条件のホットフィックス
CSCvy82114	アップグレード後、[ネットワーク アクセス ユーザー（Network Access Users）] ウィンドウで姓名が中国語の Unicode として誤って表示される
CSCvy90691	RADIUS ベンダー ID が重複すると、PSN がクラッシュすることがある
CSCvz00034	OcspClient のログレベルを WARN ではなく ERROR に変更する必要がある
CSCvx59893	ISE の Syslog レベルとメッセージレベルの不一致

Cisco ISE リリース 3.1 の未解決の不具合

問題 ID 番号	説明
CSCvx43866	アカウンティングレポートのエクスポートの完了により多くの時間がかかっている
CSCwc83059	フルアップグレード後の VCS 情報がない

問題 ID 番号	説明
CSCvy14905	新しい SXP バージョンが ISE で認識できないため、バージョンのネゴシエーションが失敗する
CSCvy76622	EST および StaticIP/ホスト名/FQDN を使用した Android BYOD フローが失敗する
CSCvy88861	ISE HA 後にポリシーの変更がネットワークデバイスにプッシュされない
CSCvz20020	Okta リダイレクトが、最初に追加された SAML 設定が削除され、再設定された後にのみ発生する
CSCvz20770	セカンダリノードの [展開（Deployment）] タブで pxGrid を有効または無効にした後、GUI で [pxGrid] ページを表示できない

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、Cisco Services にアクセスしてください。
- サービスリクエストを送信するには、シスコサポート にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

【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/** ）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。

翻訳について
このドキュメントは、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。