

# Cisco Identity Services Engine リリース 3.2

## リリースノート

初版：2022年8月16日

最終更新：2024年5月23日

## 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、ローカル 5G 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 グループベースポリシー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 Cisco Secure Network Server アプライアンス、仮想マシン (VM)、またはパブリッククラウドで使用できます。

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 Identity Services 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 3.2 の新機能

このセクションでは、Cisco ISE 3.2 の新機能と変更された機能をすべて示します。

## Cisco Private 5G

Cisco ISE リリース 3.2 以降、Cisco ISE は Cisco Private 5G をサポートします。Cisco ISE は、RADIUS 認証のみおよびアカウントングフローで実装される 5G と 5G 認証のポリシー設定を提供します。

詳細については、『Cisco ISE Administrator Guide, Release 3.2』の「Secure Access」の章にある「[Configure Cisco Private 5G as a service](#)」[英語]を参照してください。

## Cisco AnyConnect のブランド変更

Cisco AnyConnect は、Cisco Secure Client としてブランド変更されました。

Cisco ISE 3.2 は、Windows OS に対してのみ Cisco Secure クライアントをサポートします。Windows OS は、AnyConnect (バージョン 4.10.5075 以降) と Cisco Secure クライアント (バージョン 5.00529 以降) の両方をサポートしています。Windows OS では両方のエンドポイントを構成できますが、エンドポイントの実行時に考慮されるのは 1 つのポリシーのみです。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「[Compliance](#)」の章 [英語] を参照してください。

## Cisco pxGrid Direct

Cisco pxGrid Direct は、エンドポイント属性の JSON データを提供する外部 REST API に接続するのに役立ちます。収集されるデータは、pxGrid Direct 構成で指定した属性に基づいています。次に、pxGrid Direct は収集したデータを Cisco ISE データベースに保存します。

このデータは、認証ポリシーで使用できます。pxGrid Direct はエンドポイントをより迅速に評価および認証するのに役立ちます。取得されたデータが認証ポリシーで使用されるためです。これにより、エンドポイントを承認する必要があるたびにエンドポイント属性データをクエリする必要がなくなります。

## PassiveID ログインユーザーの認証ポリシーの構成

PassiveID ログインユーザーの認証ポリシーを設定する場合は、[Active Directoryの詳細設定 (Active Directory Advanced Settings)] ウィンドウの [認証フロー (Authorization Flow)] チェックボックスをオンにします。

AD グループメンバーシップに基づいて SGT をユーザーに割り当てる認証ポリシーを設定できます。設定すると、PassiveID 認証に対しても TrustSec ポリシールールを作成できるようになります。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Asset Visibility」の章にある「[Active Directory Settings](#)」[英語]を参照してください。

## Data Connect

Data Connect 機能は、オープンデータベース コネクティビティ (ODBC) または Java Database Connectivity (JDBC) ドライバを使用して Cisco ISE へのアクセスを提供するため、データベー

スサーバーを直接照会して、選択したレポートを生成できます。データへの読み取り専用アクセスのみが提供されます。

ビジネス要件に応じて、ネットワークに関する構成または運用データを抽出し、それを使用して洞察に富んだレポートとダッシュボードを生成できます。



- (注) Cisco ISE リリース 3.2 限定提供リリースで Data Connect 機能がアクティブになっている場合、Cisco ISE リリース 3.2 一般提供リリースにアップグレードするときに、Data Connect 機能を無効にしてから有効にする必要があります。

## クラウドプラットフォームへの Cisco ISE のネイティブな展開

Cisco ISE リリース 3.2 は、クラウドプラットフォーム (Amazon Web Services (AWS)、Azure Cloud、および Oracle Cloud Infrastructure (OCI)) でネイティブに利用できます。クラウドプラットフォームでの Cisco ISE の設定については、『[Deploy Cisco Identity Services Engine Natively on Cloud Platforms](#)』 [英語] を参照してください。

## Azure AD での EAP-TLS および TEAP 認証のサポート

Cisco ISE は、証明書ベースの認証と Microsoft Entra ID 認証をサポートしています。証明書ベースの認証は、内部方式として EAP-TLS または EAP-TLS を使用した TEAP のいずれかです。次に、Microsoft Entra ID から属性を選択し、それらを Cisco ISE デクショナリに追加できます。これらの属性は、認証に使用できます。

## エンドポイントプロファイルと論理プロファイルの概要レポート

このレポートには、論理プロファイルとエンドポイントプロファイル、およびそれらのプロファイルに一致するエンドポイントの数が表示されます。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Maintain and Monitor」の章にある「[Available Reports](#)」 [英語] を参照してください。

## ERS API の Open API 仕様

ERS API の Open API 仕様 (JSON ファイル) は、Cisco ISE GUI の [API設定 (API Settings)] ウィンドウの [概要 (Overview)] セクションでダウンロードできます ([管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [API設定 (API Settings)] > [概要 (Overview)])。

この Open API JSON ファイルは、Python、Java などのプログラミング言語を使用した API クライアントコードの自動生成に使用できます。Open API の仕様とツールの詳細については、<https://openapi.tools/> [英語] を参照してください。

## ERS API PATCH 要求のサポート

Cisco ISE は、ERS API の PATCH 要求をサポートするようになりました。PATCH 要求は、リソースの属性のサブセットを更新するのに役立ちます。そのリソースの構成全体を更新するのではなく、要求の一部として送信された属性のみが更新されます。詳細については「[API Reference Guide](#)」を参照してください。

## Cisco ISE ユーザーのパスワードの管理

Cisco ISE リリース 3.2 以降、Cisco ISE の内部ユーザーとして、[パスワードのライフタイム (Password Lifetime)] オプションを使用して、有効化パスワードとログインパスワードのライフタイムを管理できます。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Asset Visibility」の章にある「[Cisco ISE Users](#)」[英語]を参照してください。

## モバイルデバイス管理の機能拡張

エンドポイントがプライマリ MDM または UEM サーバーに登録されていない場合、またはプライマリ MDM もしくは UEM サーバーに到達できない場合、[一般的なMDMまたはUEM設定 (General MDM or UEM Settings)] を構成して、複数の MDM サーバーにクエリを実行できます。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Secure Access」の章にある「[Configure General MDM or UEM Settings](#)」[英語]を参照してください。

## ポスチャ条件スクリプトのサポート

ポスチャ条件スクリプトを作成およびアップロードして、エンドポイントであらゆる種類のポスチャチェックを実行できます。次のプラットフォームとスクリプトタイプがサポートされています。

プラットフォーム	サポートされるスクリプトタイプ
Windows	PowerShell スクリプト (.ps1)
macOS	シェルスクリプト (.sh)
Linux	シェルスクリプト (.sh)

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Compliance」の章にある「[Add a Script Condition](#)」[英語]を参照してください。

## スマートライセンスに必要な URL

Cisco ISE リリース 3.2 は、<https://smartreceiver.cisco.com> を使用してスマートライセンス情報を取得します。

## セキュリティ設定の機能拡張

[SHA-1暗号の許可 (Allow SHA-1 Ciphers) ] オプション ([管理 (Administration) ] > [システム (System) ] > [設定 (Settings) ] > [セキュリティ設定 (Security Settings) ] の下) が有効になっている場合、Cisco ISE は次の Cisco ISE コンポーネントとの通信に SHA-1 暗号を許可します。

- 管理者アクセス UI
- Cisco ISE ポータル
- ERS
- pxGrid

これらのコンポーネントの通信には、次のポートが使用されます。

- 管理者アクセス : 443
- Cisco ISE ポータル : 9002、8443、8444、8445、8449
- ERS : 9060、9061、9063
- pxGrid : 8910

このオプションはデフォルトでは無効になっています。

Cisco ISE リリース 3.2 にアップグレードすると、アップグレード前に有効にした場合でも、[SHA-1暗号化を許可 (Allow SHA-1 Ciphers) ] オプションは無効になります。クライアントが SHA-1 暗号化のみを使用して Cisco ISE と通信できるようにする場合は、アップグレード後にこのオプションを有効にできます。このオプションを有効または無効にした後、展開内のすべてのノードを再起動する必要があります。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Segmentation」の章にある「[Configure Security Settings](#)」 [英語] を参照してください。

## エンドポイントコンテキストの可視性ウィンドウの GUID を持つエンドポイントの単一エントリ

ランダムな MAC アドレスを使用するエンドポイントが Cisco ISE に接続し、次の条件を満たす場合、[エンドポイントコンテキストの可視性 (Endpoint Context Visibility) ] ウィンドウには、エンドポイントの最新の MAC アドレスのみが表示されます。

- エンドポイントは、証明書ベースの認証方法 (EAP-TLS など) を介して Cisco ISE に接続します。
- エンドポイントは、MDM サーバーを介して Cisco ISE に接続します。

上記の条件を満たすエンドポイントは、MAC アドレスではなく GUID と呼ばれる一意の属性によって識別されます。Cisco ISE GUI の [コンテキストの可視性 (Context Visibility) ] > [エンドポイント (Endpoints) ] ウィンドウで、GUID を持つエンドポイントは、最新のランダム MAC アドレスとともに 1 回だけリストされます。

[MDM-GUID] 列には、エンドポイントに割り当てられている一貫性のある GUID が表示されます。

以前の MAC アドレスエントリで使用できたすべてのエンドポイントデータは、新しいエントリに引き継がれます。

## 極小規模な仮想マシン展開のサポート

Cisco ISE 3.2 は、極小規模な仮想マシンの展開をサポートしています。このノードでは PSN ペルソナのみを有効にできます。このノードでは、PAN ペルソナと MnT ペルソナはサポートされていません。

表 1: オンプレミス展開での極小規模な仮想マシンの要件

要件のタイプ	仕様
CPU コア数	8
メモリ	32 GB
ハード ディスク	300 GB

表 2: クラウド展開での極小規模な仮想マシンの要件

クラウド	タイプ/サイズ/形状	vCPU	メモリ
AWS	m5.2xlarge	8	32 GB
Azure	Standard_D8s_v4	8	32 GB
OCI	Standard3.Flex	8 (4 OCPU。1 つの Oracle Compute Unit (OCPU) は 2 つの vCPU に相当)	32 GB

詳細については、『[Cisco Identity Services Engine Installation Guide, Release 3.2](#)』 [英語] を参照してください。

## システム 360

システム 360 には、[モニタリング (Monitoring)] と [Log Analytics] が含まれています。

[モニタリング (Monitoring)] 機能を使用すると、一元化されたコンソールから、展開内のすべてのノードの幅広いアプリケーションとシステム統計、および重要業績評価指標 (KPI) を監視できます。KPI は、ノード環境の全体的な状態を把握するのに役立ちます。統計は、システム構成と使用率固有のデータを簡略化して表示します。

Cisco ISE 3.2 以降のリリースは、Grafana および Prometheus と統合されています。Grafana は、サードパーティのメトリクスダッシュボードおよびグラフエディタです。これは、Prometheus データベースで収集された統計とカウンタをグラフィックまたはテキストベースで表示しま

す。Prometheus は、KPI を時系列形式で格納するためのデータストアとして使用されます。Grafana の詳細については、Grafana のドキュメントを参照してください。

Grafana ダッシュボードは、システムメトリックを分析し、情報に基づいた意思決定を行うのに役立つ、量的および質的データの包括的なセットを表示します。カスタマイズされた Grafana ダッシュボードを作成して、必要なシステムメトリックを分析および監視できます。カスタマイズされた Grafana ダッシュボードを作成するには、[操作 (Operations)] > [システム360 (System 360)] > [モニタリング (Monitoring)] を選択します。

Prometheus データソースから必要なデータを取得するため、組み込みクエリまたはカスタムクエリを使用できます。Grafana ダッシュボードを作成しながら、新しいダッシュボードパネルを追加し、Prometheus データの取得に使用するクエリを [クエリ (Queries)] タブで指定できます。

モニタリングサービスはデフォルトで有効になっています。このサービスは、[操作 (Operations)] > [システム360 (System 360)] > [設定 (Settings)] から無効または有効にすることができます。

[Log Analytics] は、エンドポイントの認証、許可、アカウントティング (AAA) およびポスチャ syslog データを詳細に分析するための柔軟な分析システムを提供します。ISE 正常性サマリーと ISE プロセスステータスを分析することもできます。ISE カウンタと正常性サマリーレポートと同様のレポートを生成できます。Log Analytics サービスは、MnT ノードでのみ実行されます。

オープンソースのデータ可視化プラットフォームである Kibana を使用して、syslog データを分析および可視化し、Elasticsearch を使用して、syslog データを保存およびインデックス化します。

Log Analytics を有効にするには、[操作 (Operations)] > [システム360 (System 360)] > [設定 (Settings)] の順に選択し、[Log Analytics] サービスを有効にします。

詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Maintain and Monitor」の章にある「[System 360](#)」 [英語] を参照してください。

## デフォルトモードまたはダークモードで Cisco ISE を表示する

Cisco ISE をデフォルト (ライト) モードまたはダークモードで表示できるようになりました。Cisco ISE 管理者ポータル [アカウント設定 (Account Settings)] ダイアログボックスから、デフォルトモードまたはダークモードを選択します。

『Cisco ISE Administrator Guide, Release 3.2』の「Basic Setup」の章にある「[Apply Default or Dark Mode in Cisco ISE](#)」のトピック [英語] を参照してください。

## ゼロタッチプロビジョニング – セキュリティ更新

ゼロタッチプロビジョニング (ZTP) を介して Cisco ISE をプロビジョニングする場合、次のセキュリティ機能を使用できます。

- **公開キー認証** : パスワードの代わりに秘密キーを使用して Cisco ISE CLI にログインできます。詳細については、「[Public Key Authentication](#)」 [英語] を参照してください。

- **初回のログインパスワードの変更** : Cisco ISE GUIへの初回ログイン時に、管理者パスワードをリセットするように求められます。詳細については、「[First Login Password Change](#)」[英語]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 3.2 は、次の Secure Network Server (SNS) ハードウェア プラットフォームにインストールできます。

表 3: 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、『 <a href="#">Cisco Secure Network Server Appliance Hardware Installation Guide</a> 』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)	
Cisco SNS-3715-K9 (小規模)	
Cisco SNS-3755-K9 (中規模)	
Cisco SNS-3795-K9 (大規模)	

SNS 3600 シリーズ アプライアンスには、次の OVA テンプレートを使用できます。

- ISE-3.2.0.542a-virtual-SNS3615-SNS3655-300.ova
- ISE-3.2.0.542a-virtual-SNS3615-SNS3655-600.ova
- ISE-3.2.0.542a-virtual-SNS3655-SNS3695-1200.ova
- ISE-3.2.0.542a-virtual-SNS3695-1800.ova
- ISE-3.2.0.542a-virtual-SNS3695-2400.ova

SNS 3700 シリーズ アプライアンスには、次の OVA テンプレートを使用できます。

- ISE-3.2.0.542b-virtual-SNS3715-SNS3755-300.ova
- ISE-3.2.0.542b-virtual-SNS3715-SNS3755-600.ova



- ISE-3.2.0.542b-virtual-SNS3755-SNS3795-1200.ova
- ISE-3.2.0.542b-virtual-SNS3795-2400.ova



(注) Cisco ISE 3.1 パッチ 6 以降および Cisco ISE 3.2 パッチ 2 以降は、Cisco SNS 3700 シリーズ アブライアンスをサポートします。

## 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。

- Cisco ISE リリース 3.0 以降のリリースでは、VMware ESXi 7.0.3 以降のリリースに更新することを推奨します。
  - OVA テンプレート : ESXi 6.7 および ESXi 7.0、では VMware バージョン 14 以降。
  - ISO ファイルは ESXi 6.7 以降のリリース ESXi 6.7、ESXi 7.0、および ESXi 8.0 をサポートしています。

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。



(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。

- Microsoft Windows Server 2012 R2 以降の Microsoft Hyper-V

- QEMU 2.12.0-99 上の KVM



(注) Cisco ISE は OpenStack にインストールできません。

- Nutanix AHV 20220304.392

次のパブリック クラウドプラットフォーム上に Cisco ISE をネイティブに展開できます。

- Amazon Web Services (AWS)
- Microsoft Azure クラウド
- Oracle Cloud Infrastructure (OCI)

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

## 対応ブラウザ

Cisco ISE 3.2 は、次のブラウザでサポートされています。

- Mozilla Firefox バージョン 102、103、104、105、106、107、108、110、113、114、119、123、および 125
- Google Chrome バージョン 103、104、105、106、107、108、109、110、112、114、116、117、119、122、および 124
- Microsoft Edge バージョン 103、104、106、107、108、109、112、115、117、119、122 および 125



(注) 現在、モバイルデバイスで Cisco ISE GUI にアクセスすることはできません。

## 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 4: 検証済み外部 ID ソース

外部 ID ソース	バージョン
<b>Active Directory</b>	
Microsoft Windows Active Directory 2012	Windows Server 2012
Microsoft Windows Active Directory 2012 R2 <a href="#">1</a>	Windows Server 2012 R2
Microsoft Windows Active Directory 2016	Windows Server 2016
Microsoft Windows Active Directory 2019	Windows Server 2019
Microsoft Windows Active Directory 2022	Windows Server 2022 (パッチ Windows10.0-KB5025230-x64-V1.006.msu 適用 済み)

外部 ID ソース	バージョン
<b>LDAP サーバー</b>	
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
LDAP としての AD	Windows Server 2022 (パッチ Windows10.0-KB5025230-x64-V1.006.msu 適用済み)
<b>トークンサーバー</b>	
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
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
<b>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)</b>	
Microsoft Azure MFA	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
<b>Open Database Connectivity (ODBC) アイデンティティソース</b>	
Microsoft SQL Server	Microsoft SQL Server 2012 Microsoft SQL Server 2022
Oracle	Enterprise Edition リリース 12.1.0.2.0
PostgreSQL	9.0
Sybase	16.0
MySQL	6.3

外部 ID ソース	バージョン
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

<sup>1</sup> 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。

## 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 3.2 は、OpenSSL 1.1.1k で検証済みです。

### 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。

### pxGrid Direct コネクタが無効になっている場合の Cisco ISE の再起動の制限

無効な pxGrid Direct コネクタがある状態で Cisco ISE を再起動すると、再起動後に pxGrid Direct コネクタを使用する同期操作をスケジュールする際に問題が発生します。Cisco ISE を再起動する前に、無効になっているすべての pxGrid Direct コネクタを有効にし、再起動してからコネクタを再度無効にすることをお勧めします。または、この問題の回避策として、Cisco ISE を再起動する前に、無効になっているコネクタの属性を編集する（アクティブなコネクタにする）こともできます。

この問題は、Cisco ISE リリース 3.2 累積パッチ 5 および Cisco ISE リリース 3.3 累積パッチ 2 で解決されています。

## イーサネット MAC アドレスベースの API に対する Microsoft コンプライアンス取得 API のサポート

Microsoft コンプライアンス取得 API は現在、MAC アドレスベースの API のイーサネット MAC 属性をサポートしていません。この制限は 2024 年 1 月、Microsoft により対処されます。有線で展開する場合は、次のパッチにアップグレードする前に、GUID 埋め込み証明書に移行することをお勧めします：Cisco ISE リリース 3.1 パッチ 8、Cisco ISE リリース 3.2 パッチ 4、または Cisco ISE リリース 3.3 パッチ 1。

## RADIUS ライブログ遅延のホットパッチ

Cisco ISE リリース 3.2 累積パッチ 2、3、および 4 では、[CSCwi06794](#) で説明されている RADIUS ライブログ遅延が発生する可能性があります。この問題を修正するには、ホットパッチ `ise-apply-CSCwi06794_3.1.x_patchall-SPA.tar.gz` をインストールする必要があります。

## Hyper-V でのインストールでは、eth0 インターフェイス上で DHCP が有効化される

Cisco ISE 3.2 のメインリリースまたはパッチリリースが Microsoft Hyper-V にインストールされると（新規インストール）、DHCP が eth0 インターフェイスで有効になります。この問題は、Cisco ISE 3.2 のメインリリースまたはパッチリリースにアップグレードする場合は発生しません。

Cisco ISE が Hyper-V にインストールされている場合、次の問題が発生する可能性があります。

- Hyper-V で実行している Cisco ISE 3.2 ノードに、初期セットアップ時に設定された静的 IP に加えて DHCP アドレスが割り当てられる。
- ゲートウェイと NTP の ping が一貫して失敗する可能性がある。
- Cisco ISE GUI にアクセスできない場合がある。
- ネットワーク通信の問題が原因で、展開やその他の操作が失敗する可能性がある。

この問題を修正するには、次のホットパッチをインストールする必要があります。

`ise-apply-CSCwf02093_3.2.x_patchall-SPA.tar.gz`

ホットパッチをインストールするには、以下の手順を実行します。

1. Cisco ISE CLI にログインします。
2. 次のコマンドを実行して、ホットパッチを適用するバンドルをインストールします。

```
application install ise-apply-CSCwf02093_3.2.x_patchall-SPA.tar.gz <Repository_Name>
```
3. ホットパッチが正常にインストールされたら、Hyper-V 管理コンソールで `reset-config` コマンドを実行して、IP アドレス/マスク/ゲートウェイ、ホスト名、ドメイン名、DNS サーバー、NTP サーバーなどのネットワーク設定をリセットします。このコマンドでは、Cisco ISE の設定データはリセットされません。



- (注)
- Hyper-V 管理コンソールで **reset-config** コマンドを実行する必要があることに注意してください。
  - **application reset-config ise** コマンドは使用しないでください。

4. 必要なセットアップの詳細を入力して、reset-config 操作を完了します。

## ClamWin 製品のマルウェア対策条件

ClamWin Pty Ltd ベンダーのマルウェア対策条件を追加しようとすると、次のエラーメッセージが表示される場合があります。

```
class com.cisco.cpm.posture.exceptions.PostureException:Check am_linux_def_v4_ClamWinPtyLtd
is not found
```

バージョン 0.x の複数の ClamWin 製品が [Baseline Condition] タブにリストされている場合、それらの製品のいずれかを選択してマルウェア対策条件を設定すると、上記のエラーメッセージが表示されることがあります。

このようなシナリオでは、ポストチャフィードの更新を 1 回以上実行して、バージョン 0.x の複数のエントリを削除する必要があります。

回避策として、[Advanced Condition] タブから製品を選択し、ClamWin Pty Ltd ベンダーのマルウェア対策条件を設定できます。

## インターフェイスで IPv6 アドレスが設定されている場合、ホストエイリアスが自動的に追加または削除されない

Cisco ISE リリース 3.2 以降、インターフェイスで IPv6 アドレスが設定されている場合、対応する IP アドレスのホストエイリアスは自動的に追加または削除されません。次の **ip host** コマンドを実行して、ホストエイリアスを手動で追加または削除する必要があります。

ホストエイリアスを追加するには、次を実行します。

```
ip host 2001:420:54ff:4::456:00 demo demo.cisco.com
```

ホストエイリアスを削除するには、次を実行します。

```
no ip host 2001:420:54ff:4::456:00 demo demo.cisco.com
```

## 3.2P5 SLR 登録済みノードでパッチロールバック後に SL 登録済みと表示される

Cisco ISE リリース 3.2 パッチ 5 以降のリリースを Cisco ISE ノードにインストールし、特定ライセンス登録 (SLR) を有効にしてから以前のリリースにロールバックすると、ノードは SLR ではなくスマートライセンス (SL) に自動的に登録されます。この場合、ライセンス設定が正しくないために登録解除または更新操作が機能しないので、SLR を返却することはできません。この問題は、TAC の介入によって解決できます。

これを回避するには、以前のリリースにロールバックする前に SLR を返却する必要があります。各ノードには、SLR を返却するために Cisco Smart Software Manager (CSSM) で送信する必要がある一意のコードが設定されています。Cisco ISE リリース 3.2 パッチ 5 以降をインストールする前に SLR を有効にしていた場合は、以前のリリースにロールバックする前に SLR を返却する必要はありません。

## アップグレード情報



(注) ネイティブクラウド環境に展開された Cisco ISE ノードではアップグレードを実行できません。新しいバージョンの Cisco ISE を使用して新しいノードを展開し、古い Cisco ISE 展開の設定をそのノードに復元する必要があります。

### リリース 3.2 へのアップグレード

次の Cisco ISE リリースからリリース 3.2 に直接アップグレードできます。

- 2.7
- 3.0
- 3.1

Cisco ISE リリース 2.7 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 3.2 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。

### 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。

[Cisco ISE Software Download](#) サイトで Cisco ISE リリース 3.2 の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。

これには以下が含まれます。

- バグ [CSCwj43362](#) および [CSCwj55392](#) の解決。
- 新しいファイルのファイル名には、「c」がビルド番号に追加されます（たとえば、`ise-upgradebundle-2.7.x-3.1.x-to-3.2.0.542c.SPA.x86_64.tar.gz`）。
- 既存の Cisco ISE リリース 3.2 累積パッチは、この新しいアップグレードバンドルで引き続き機能します。



## 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。

## Cisco ISE の Cisco Catalyst Center との統合

Cisco ISE は Cisco Catalyst Center との統合が可能です。Catalyst Center と連携するように Cisco ISE を設定する方法については、[Cisco Catalyst Center のドキュメント](#)を参照してください。

Cisco ISE と Catalyst Center との互換性については、「[Cisco SD-Access Compatibility Matrix](#)」[英語]を参照してください。

## 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 Reference Guide](#)』の「Patch Install」セクション [英語] を参照してください。



- 
- (注) 以前の Cisco ISE リリース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。



(注) 「未解決の不具合」セクションには、現在のリリースに該当し、Cisco ISE 3.2 よりも前のリリースにも該当す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。

## Cisco ISE リリース 3.2 の解決済みの不具合：累積パッチ 6

問題 ID 番号	説明
CSCwf47838	コマンド引数のスペース文字が TACACS+ コマンドセットの CSV エクスポート後に保持されない。
CSCwi60778	エンドポイントが再認証後にスタティック アイデンティティ グループの割り当てを失う。
CSCwf24553	SR-Insights : [Licensing] ページで使用される用語情報の提供に関する Cisco Umbrella の不具合。
CSCwf24554	SR-Insights : SL 登録の失敗に関する詳細情報の表示に関する Cisco Umbrella の不具合。
CSCwi89466	Cisco ISE 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 (3.2 P3 以降)。
CSCwi58699	Cisco ISE で DNAC/EA ディクショナリ属性が更新されると、ゲストフローを介して CoA がトリガーされる。
CSCwi62078	組み込みの認証プロファイル Block_Wireless_Access を使用すると、[404] Resource Not Found エラーが返される。
CSCwi58421	ポスチャリースが有効になっている場合、PSN ノードは正しいポスチャ有効期限で DB を更新しない。
CSCwi34405	認証中に IdentityAccesss Restricted 属性を適用できない。
CSCwi61491	メタスペースの枯渇によりアプリケーションサーバーがクラッシュする。
CSCwi29253	Cisco ISE AD 診断ツールをアップグレードすると動作が停止し、使用可能なテストのリストを取得できない。
CSCwh33160	Cisco ISE は、設定された SNMP サーバーに SNMPv3 ディスクトラップを送信しない。
CSCwi53104	1 か月を超えるレポートをエクスポートすると、データが生成されない。
CSCwf61673	Cisco ISE CLI 読み取り専用ユーザーは show CPU usage コマンドを実行できない。
CSCwi54722	リダイレクト URL は IP で終わる FQDN を使用し、IP は Cisco ISE ホスト名で置き換えられる。
CSCwi15793	Cisco Identity Services Engine のカスタム属性の特殊文字エラー。

問題 ID 番号	説明
CSCwa15336	Cisco ISE PIC 3.1：終了したセッションはライブセッションに表示されるべきではない。
CSCwi59868	スポンサード ゲスト アカウントの延長が最大日数を超えて機能する。
CSCwi45090	Cisco ISE：REST API ERS：downloadableacl：フィルタフィールド「name」がサポートされない。
CSCwi89082	Cisco ISE ポータル（デフォルト）が SAML の設定に必要なデータベースから削除された。
CSCwi42628	MAR キャッシュの複製が、NIC および非 NIC ボンディング インターフェイスの両方のピア ノード間で失敗した。
CSCwi36040	Cisco ISE リリース 3.2 の IP アクセスリスト制御が表示されない。
CSCwi34117	Grafana UI と Kibana では Identity Services Engine に RBAC を実装する必要がある。
CSCwh67500	Cisco ISE 3.2 で選択した認証プロファイルが見つからない。
CSCvs77939	AnyConnect 設定およびポスチャ エージェント プロファイルの編集集中にエラーが発生する。
CSCwj21203	「Dashboard System Status」クエリが原因で 1,000 件の DB 接続が使い果たされた。
CSCwj03747	特定の論理グループでは抑制 CoA があるにもかかわらず、プロファイリングで CoA が抑制されない。
CSCwi32576	cpmSessionId の割り当て中に PSN ノードがクラッシュする。
CSCwj16540	Cisco ISE 3.2 パッチ 4 の Context Visibility がライブログまたはセッションと一致しない。
CSCwi45879	既存の認証プロファイルまたは重複した認証プロファイルが選択されている場合、ホットスポットポータルを選択できない。
CSCwi53915	高度なフィルタの [Save] オプションが、クライアント プロビジョニング リソースのフィルタリングで機能しない。
CSCwf89224	クライアントから受信したセッションチケットの復号化が Cisco ISE で失敗する。
CSCwh99772	子項目がいずれかのグループから削除された後、すべてのネットワーク デバイス グループが削除される。
CSCwi86161	[ESXi VA] 機能：mDNAC ロールが未定義であり、Cisco ISE 統合後に ACA 移行を開始できない。
CSCwj47769	Cisco ISE リリース 3.2 パッチ 5 の無効な要求ページ。
CSCwh41977	Cisco ISE 3.2：Cisco ISE 設定でのユーザーごとの dACL の存在の確認。
CSCwh56565	MNT ノード（ライブログ、レポート）への PSPAN REST コールはロードバランシングすべきでない。

問題 ID 番号	説明
CSCwj44477	アップグレードの問題：「Database upgrade failed」というメッセージが表示される。
CSCwi57903	スケジュール済みバックアップが失敗してもアラームが生成されない。
CSCwj07319	API ers/config/sessionservicenode が誤った合計を返す。
CSCwi73984	Cisco ISE 3.1P8 の [Installed Patches] メニューにすべてのパッチが表示されない。
CSCwi33361	Cisco ISE CLI のアクセスの問題：サーバーへの接続に失敗しました。
CSCwi21020	Cisco ISE メッセージング証明書の生成では、セカンダリノードで完全な証明書チェーンが複製されない。
CSCwh72754	Cisco ISE Active Directory プロセス (lwsmd) が「Updating」でスタックし、CPU を 90～100% 消費する。
CSCwi66126	Cisco ISE ERS API：DACL を更新しても最終更新日のタイムスタンプが変更されない。
CSCwc85211	Cisco ISE パッシブアイデンティティエージェントのエラー「id to load is required for loading」。
CSCwi57950	Cisco ISE 3.2：Nexpose Rapid 7：Strict-Transport-Security 形式が正しくない。
CSCwi98793	プロファイラが誤った値を持つ mdm 属性をキャッシュしている。
CSCwi17694	Cisco ISE：10,000 以上に設定されている場合、synflood-limit が有効にならない。
CSCwd67833	ERS API が単一のエンドポイントを更新するのに数秒かかる。
CSCwi67639	コマンド show cpu usage が Cisco ISE 3.X の情報を表示しない。
CSCwi30707	Cisco ISE 3.1 パッチ 7：削除されたデバイスタイプがポリシーセットで引き続き選択可能。
CSCwi73981	大文字の FQDN を使用して追加されたアイデンティティストアを CLI から削除できない。
CSCwi89689	Cisco ISE：無効な IP またはホスト名エラー。
CSCwi94938	フィルタを使用すると、Cisco ISE 3.2 ゲストユーザー API で誤った結果が返される。
CSCwi59216	[Contact Support] をクリックすると、スポンサーポータルが 400 Bad Request を返す。
CSCwi59567	CoA 再試行カウントを「0」に更新する際の問題。
CSCwi52264	Cisco ISE SAML アイデンティティプロバイダーの設定属性が参照されているにもかかわらず削除される。
CSCvt75833	トークンサーバーが FQDN の場合、Cisco ISE は nslookup を再度実行する必要がある。
CSCwi17200	Cisco ISE：TROUBLESHOOTING.EncryptionOffPeriod が原因で RPC netlogon が失敗する。
CSCwi48806	デュオポータルのエントリが原因で認証ポリシーのロードに時間がかかる。

問題 ID 番号	説明
CSCwi96581	3.4.2 に脆弱性があるため、CXF バージョンをアップグレードする。
CSCwi88504	Cisco ISE リリース 3.2P5：属性のライブログに手順と解決策の文章が不足している。
CSCwi59230	Cisco ISE に 1,000 を超えるアイデンティティグループがある場合、スーパー管理者以外のユーザーはエンドポイントを編集または削除できない。
CSCwf80386	パッチのインストール時に、Disable_RSA_PSS 環境値の現在の値が保持されない。
CSCwi63725	SNMPD プロセスが原因で Cisco ISE でメモリリークが発生する。
CSCwi25755	Cisco ISE 3.2 以降。SAML プロバイダーを追加できない。
CSCwh25160	スワップクリーンアップスクリプトがスワップ領域をドロップし、cron をプログラムする。
CSCwf51766	Cisco ISE で、OpenAPI を介して DenyAccess アイデンティティソースを使用する認証ポリシーを作成できない。
CSCwj06401	エンドポイントの属性セクションに null のキーと値のペアがあり、ページフローが中断される。
CSCwd14523	「accountEnabled」属性により、Azure AD での EAP-TLS の認証問題が発生する。
CSCwh61339	90,000 を超えるネットワークデバイスのエクスポートがタイムアウトする。
CSCwa32407	ENH：すべてまたは特定のゲストユーザーのユーザーアカウントの詳細をスポンサーに再送信する。
CSCwh92366	3.1P8：3.1P8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。
CSCwf17714	Cisco ISE 3.3 BH：レポートに DockerMetric の複数のエントリが表示される。

## Cisco ISE リリース 3.2 の新機能：累積パッチ 5

### Cisco ISE での TAC サポートケースのオープン

Cisco ISE リリース 3.2 パッチ 5 以降、Cisco ISE GUI から直接 Cisco ISE の TAC サポートケースを開くことができます。

詳細については、『Cisco ISE Administrator Guide, Release 3.2』の「Troubleshoot」の章の「[Open TAC Support Cases in Cisco ISE](#)」[英語]を参照してください。

### ローカライズされた ISE のインストール

Cisco ISE の再インストール中に、**application configure ise** コマンドで [Localized ISE Install] オプション（オプション 36）を使用して、インストール時間を短縮できます。このオプションを使用すると、再インストール時間を平均 5～7 時間から約 1～2 時間に短縮できます。

このオプションは、Cisco Secure Network Server と仮想アプライアンスの両方に使用できますが、Cisco Secure Network Server の再インストール時間を大幅に短縮します。

詳細については、『Cisco ISE CLI Reference Guide, Release 3.2』の「Cisco ISE CLI Commands in EXEC Mode」の章にある「[Localized ISE Installation](#)」[英語]を参照してください。

### 「今すぐ同期」を使用したオンデマンドの pxGrid 直接データ同期

[Sync Now] 機能を使用して、pxGrid Direct URL フェッチャコネクタのデータのオンデマンド同期を実行できます。完全同期と増分同期の両方をオンデマンドで実行できます。オンデマンドのデータ同期は、Cisco ISE GUI または OpenAPI を使用して実行できます。

詳細については、『Cisco ISE Administrator Guide, Release 3.2』の「Asset Visibility」の章にある「[On-demand pxGrid Direct Data Synchronization using Sync Now](#)」[英語]を参照してください。

## Cisco ISE リリース 3.2 の解決済みの不具合：累積パッチ 5

警告 ID	説明
<a href="#">CSCwb57672</a>	RSA4096 証明書を使用した SHA384 の GCMP256 認証に失敗した。
<a href="#">CSCwh36544</a>	pxGrid にトピック登録の詳細が表示されない。
<a href="#">CSCwh42683</a>	SAML ユーザーの読み取り専用権限。
<a href="#">CSCwh64195</a>	データ破損により FailureReason=11007 または FailureReason=15022 が発生。
<a href="#">CSCwh99534</a>	エンドポイントプローブが SXP マッピングをクリーンアップしない。
<a href="#">CSCwh24823</a>	非必須属性が PUT 要求に含まれていない場合、それらの値が空またはデフォルトにリセットされる。
<a href="#">CSCwd48787</a>	ISE : SSL バッファがクリアされず、PAC 復号に影響する。
<a href="#">CSCwh90691</a>	show CLI コマンドが、ログレベルを 5 に設定した後に例外をスローする。
<a href="#">CSCwh83323</a>	カスタムの「SMTPAPI宛先アドレス」が使用されている場合、「パスワードのリセット」フローで SMS が送信されない。
<a href="#">CSCwe25050</a>	PPAN にインポートされたワイルドカード証明書が展開内の他のノードに複製されない。
<a href="#">CSCwi18005</a>	Cisco ISE 3.2 にアップグレードした後、外部 RADIUS サーバーリストが表示されない。
<a href="#">CSCwd21798</a>	Cisco ISE-PIC ライセンスの期限切れアラーム。
<a href="#">CSCvj75157</a>	Cisco ISE API がユーザーアカウントの作成中にアイデンティティグループを認識しない。
<a href="#">CSCwh63501</a>	log4net 2.0.8.0 の脆弱性。
<a href="#">CSCwi37249</a>	エンドポイントが Android デバイスとして誤ってプロファイリングされる。
<a href="#">CSCvz86688</a>	Aruba-MPSK-Passphrase に暗号化のサポートが必要。

警告 ID	説明
CSCwh58768	ISE 2.7 バージョンからの復元後に、デバイスポータルで既存のデバイスを削除できない。
CSCwh47601	40 文字の auth および priv パスワードを持つ SNMPv3 ユーザーを作成できない。
CSCwh18899	ISE OpenAPI でマルチノードクラスターのシステム証明書インポートのサポートが必要。
CSCwc04447	ネットワークデバイス IP を介して TACACS ライブログをフィルタ処理できない。
CSCwh17285	インターフェイス上の IPv6 コマンドが IPv6 有効化だけである場合、ポータルの初期化に失敗する。
CSCwh70696	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。
CSCwi04514	ディクショナリ属性に「-」が含まれている場合のポスチャクライアントプロビジョニングリソース HTTP エラー。
CSCwh24754	スポンサーグループにマッピングされた AD グループの数が多すぎるため、スポンサーログインで遅延が発生する。
CSCwh81035	PAN で PSN からのエンドポイントの重要ではない属性更新が欠落している。
CSCwh10401	CSR を利用して pxGrid クライアント証明書を生成できない。
CSCwh60726	ISE lwsm 復号化が正しく行われない。
CSCwh77574	Cisco ISE が証明書のインポート中にパスワードに特殊文字を使用できない。
CSCwh55667	期限切れまたは無効なライセンスによるポスチャ障害が、AnyConnect ISE ポスチャレポートで内部システムエラーとして報告される。
CSCwh88801	すべてのインターフェイスで設定されている 0.0.0.0 のデフォルトスタティックルートがリロード後に削除される。
CSCwf10516	認証ポリシーの検索機能が動作しない。
CSCwi45131	シスコ製品に影響を与える Apache Struts の脆弱性：2023 年 12 月。
CSCwi27497	ISE ノードで REST 認証サービスが実行されていない。
CSCwh52589	Acs.Username が最初のデバイス接続の際、ゲストユーザー名で更新されない。
CSCwh30723	ISE のコンテキストの可視性で、コロンなどの区切り文字がない場合、スタティック MAC エントリが検証されない。
CSCwh92185	[Operational Data Purging] ページからエクスポートされた RADIUS 認証レポートが空である。
CSCwh83482	ISE データベースがスポンサーアカウントの電子メールフィールドを更新しない。

警告 ID	説明
CSCwh96018	同じ名前で大文字と小文字が異なる新しい MDM が作成された場合に、大文字と小文字を区別するチェックが原因で失敗する。
CSCwh99772	子項目がいずれかのグループから削除されると、すべてのネットワーク デバイス グループが削除される。
CSCwh93498	デバイスポータルに重複オプションが使用されている場合、エンドポイント消去ルールが自動的に作成される。
CSCwh90610	ISE 放棄された Jedis 接続が threadPool に返送されない。
CSCvo60450	MS-RPC コールの AES256 のみを送信するための暗号化の機能拡張。
CSCwi03961	ポリシーセットにロケーショングループ情報がない。
CSCwh41977	ISE 設定でのユーザーごとの dACL の存在の確認。
CSCwh79938	高度な調整で PreferredDCs レジストリ値を設定できない。
CSCwh30893	プロファイリングで、「xxxxxxxxxxx」の形式の発信側ステーション ID の値が処理されない。
CSCwh84446	アカウントの有効期限通知に特殊文字または改行文字が含まれている場合、ゲストタイプの保存が機能しない。
CSCwh45472	PKI キーペアのパスフレーズに「+」が含まれている場合、GUI から SFTP リポジトリへの運用バックアップが失敗する。
CSCwh38464	ISE CLI 管理者ユーザーが 2 カ月の非アクティブ期間の後にログインできない。
CSCwi06794	CSCwe00424 の RADIUS ライブログ遅延回帰。
CSCwh71117	「User Services」のみを有効にすると、管理 GUI アクセスも有効になる。
CSCwh95022	日本語の UI を使用すると、スポンサーポータルの [Setting date] タブに誤った曜日情報が表示される。
CSCwf25955	SGT、VN 名、Vlan フィールドが空のマッチング認証プロファイルを使用すると、prrt がクラッシュする。
CSCwf61657	スポンサー FQDN の TCP ハンドシェイクに常に Gig0 が関与する。
CSCwd34467	EAP チェーンおよび Azure AD グループを使用した試行で、承認ルールの評価が失敗する。
CSCwi15914	SXP Add 操作から IPv6 リンクローカルアドレス用の追加の IPV6-SGT セッションバインディングが作成される。
CSCwh70275	登録解除から残った証明書を使用してノードを登録すると、使用中の証明書が削除される可能性がある。



警告 ID	説明
CSCwh69045	内部ユーザーのパスワードの大部分が、グローバルパスワードの有効期限を超過している。
CSCwh26698	pxGrid コネクタのユーザーデータを取得する方法の追加。
CSCwf98849	クライアント プロビジョニング ポータルへの変更の保存中に重大なエラーが表示される。
CSCwh71273	Essentials ライセンスが無効になっている場合、GUI アクセスが制限される/ルート CA を再生成できない。
CSCwi23166	パッチ管理条件の変更を保存できない。
CSCwh51156	破損した NAD プロファイルがロードされず、FailureReasons 11007 および 15022 で認証が失敗する。
CSCwi59555	xx:xx:xx:xx:xx:xx 形式の MAC アドレスの検索が無視される。
CSCwh47299	Cisco ISE アラームとダッシュボードの概要がロードされない。
CSCwf64662	SXP で、IP アドレスと SGT 間にマッピングの不整合が発生する可能性がある。
CSCwh26288	pxGrid Direct：コネクタの追加に Premier ライセンスを要求されるが、この機能には Advantage のみ必要なはず。
CSCwc53824	ISE で、AMP AMQP サービスへの接続が TLSv1.0 に制限される。
CSCwi05905	ISE ERS API - /ers/config/deploymentinfo/getAllInfo がマルチノード展開で異なるデータを返す。
CSCwh23367	ISE 3.2 自己登録電子メールの件名の行で、スポンサーゲストポータルの「=」記号以降がすべて切り捨てられる。
CSCwh53159	「\$」が含まれている場合、管理者パスワードを変更できない。
CSCwh71435	ERS API で指定されていない場合でも、内部ユーザーの有効パスワードが作成される。
CSCwf38083	ISE サービスが、Secure SysLog で初期化状態のままになる。
CSCwh93925	複数のスタティック デフォルト ルートが設定されている場合、ISE が RADIUS トラフィックを誤ってルーティングする。
CSCwi28131	[Never Purge] ルールで使用されているカスタム属性を持つエンドポイントがまだ消去される。
CSCwf55795	ADE-OS の復元後、3.2P1 以降で ISE UI と CLI にアクセスできない。
CSCwi36954	MnT データベースの使用率がしきい値を超えると、RADIUS に設定された保持日数に基づいてデータベースが消去される。
CSCwf72037	管理者ログインレポートに 5 分ごとに「Administrator authentication failed」と表示される。
CSCwh21038	サードパーティのポストチャフロー中に、セッション情報が時間指定セッションキャッシュに保存されない。

警告 ID	説明
<a href="#">CSCwi19099</a>	いずれかのコネクタが無効になっている場合、設定フォルダへのデータの挿入中に問題が発生する。

## Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 5

これらは、Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 5 です。

問題 ID 番号	説明
<a href="#">CSCwh92366</a>	3.1 パッチ 8 : 3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。

## Cisco ISE リリース 3.2 の新機能：累積パッチ 4

### カスタマー エクスペリエンス アンケート

Cisco ISE では、管理ポータル内でユーザーに顧客満足度アンケートが表示されるようになりました。顧客満足度アンケートを定期的実施することで、シスコではお客様の Cisco ISE のエクスペリエンスをより深く理解し、何が良好に機能しているかを追跡し、改善すべき領域を特定することができます。アンケートを送信すると、その後 90 日間は別のアンケートは表示されません。

アンケートは、すべての Cisco ISE の展開においてデフォルトで有効になっています。アンケートはユーザーレベルで、あるいは Cisco ISE の展開に対して無効にできます。

詳細については、『[Cisco ISE Administrator Guide, Release 3.2](#)』の「Basic Setup」の章にある「Customer Experience Surveys」[英語]を参照してください。

### Microsoft Intune が MDM 統合における UDID ベースのクエリのサポートを終了

2024 年 3 月 24 日以降、Microsoft Intune では MDM 統合の UDID ベースのクエリのサポートを終了します。詳細はこの [Field Notice](#) をご確認ください。このサポート終了に対応して、Microsoft Intune MDM 統合から必要なエンドポイント情報を取得するための Cisco ISE API が変更されました。

Cisco ISE リリース 3.2 パッチ 4 以降、Microsoft Intune ではコンプライアンス API に対応して次のエンドポイントの詳細のみを提供します。

- デバイス コンプライアンス ステータス
- Intune による管理
- MAC アドレス
- 登録ステータス

変更の詳細については、『[Integrate MDM and UEM Servers with Cisco ISE](#)』を参照してください。

## Cisco Catalyst 9800 ワイヤレス LAN コントローラからの Wi-Fi デバイス分析データ

Cisco ISE に統合されたシスコ ワイヤレス LAN コントローラからのデバイス分析データを使用して、Apple、Intel、および Samsung エンドポイントのプロファイリングポリシー、許可条件、および認証条件とポリシーを作成できます。

詳細については、『[Cisco Identity Services Engine Administration Guide, Release 3.2](#)』の「Asset Visibility」の章にある「Wi-Fi Device Analytics Data from Cisco Catalyst 9800 Wireless LAN Controller」[英語]を参照してください。

## Cisco ISE リリース 3.2 の解決済みの不具合：累積パッチ 4

警告 ID	説明
<a href="#">CSCwf80509</a>	Cisco ISE パッシブ ID セッションのエージングタイムは、設定に関係なく常に 1 時間です。
<a href="#">CSCwc71060</a>	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る。
<a href="#">CSCwe37377</a>	Cisco ISE CRL 取得失敗アラームには、CRL のダウンロードが失敗したサーバーを表示する必要がある。
<a href="#">CSCwc33290</a>	カスタムエンドポイント属性を削除できない。
<a href="#">CSCwf83193</a>	AD ログイン情報を使用してセカンダリ管理ノードの GUI にログインできない。
<a href="#">CSCwf32641</a>	Cisco ISE リリース 3.3 BH SNMP エンジン ID がすべてのノードで同じ。
<a href="#">CSCwh17386</a>	専用 MNT ノードが SMTP 設定を複製しない。
<a href="#">CSCwe89459</a>	エンドポイントグループの作成時にスクリプトによって提供される ISE REST API ドキュメントが間違っている。
<a href="#">CSCwe15576</a>	KRON ジョブを設定できない。
<a href="#">CSCwh18487</a>	期限切れのゲストアカウントが、アカウントを再アクティブ化しても SMS を受信しない。
<a href="#">CSCwd82539</a>	ローカルおよびグローバルの例外ルールでは、結果で SecGroup のみが選択されている場合、ルールが一致しない。
<a href="#">CSCwh06338</a>	クライアント プロビジョニング ポータルの設定を編集するときに Cisco ISE GUI がロードされない。
<a href="#">CSCwf68108</a>	OpenAPI を介した「Asset」属性と pxGrid コンテキストイン。
<a href="#">CSCwe54318</a>	バインディングのクエリでの H2 DB の遅延が原因で、SXP サービスが初期化状態でスタックする。
<a href="#">CSCwd12453</a>	Cisco ISE リリース 3.1 ポータルタグには、特殊文字の検証に関する問題がある。

警告 ID	説明
CSCwb63834	MNT ログプロセッサが非管理 admin Cisco ISE ノードで実行される。
CSCwf27484	Azure へのクエリにページングがないため、認証で Azure AD グループを照合できない。
CSCwf19811	Cisco ISE 3.1 SXP バインディングレポートにデータが見つからないと表示される。
CSCwf22794	VLAN ID と名前の不一致「Error: Not a valid ODBC dictionary」。
CSCvq79397	カスタム管理メニューのワークセンター権限で UI ページが正しくロードされない。
CSCuz65708	Mozilla Firefox 45 および Google Chrome 72 : DACL の行番号が正しくない。
CSCwf59005	Cisco ISE リリース 3.2 パッチ 3 : PEAP および EAP-TLS が FIPS モードで機能しない。
CSCwh51548	Cisco ISE 3.2.0.542 : パッチとホットパッチの両方が ZTP 設定にある場合、ホットパッチがインストールされない。
CSCwc26835	RADIUS サーバーのシーケンス設定が破損する。
CSCwf44906	設定バックアップの復元後、ログイン情報を使用してリポジトリを再設定する必要がある。
CSCwf39620	ユーザー名が \$ (ドル記号) で始まる場合、Windows エージェントレスポスチャが機能しない。
CSCwh17448	Cisco ISE リリース 3.1 : ドメインユーザーがエンドポイントログイン用に設定されている場合、エージェントレス ポスチャ フローが失敗する。
CSCwf72918	Cisco ISE リリース 3.2 で、実行コンフィギュレーション内の IP ネームサーバーの順序に誤りがある。
CSCwd57628	Cisco ISE リリース 3.1 NAD Radius は、アポストロフィ記号で始まる秘密鍵を誤って共有する。
CSCwh46669	管理証明書の変更後、ボンドインターフェイスが設定されている場合、Cisco ISE がサービスを再起動しない。
CSCwh26288	pxGrid Direct : コネクタの追加に Premier ライセンスを要求される。この機能には Advantage ライセンスのみ必要。
CSCwe10898	ゲストポータルで猶予アクセスを使用すると、エンドポイントの MAC アドレスがエンドポイント ID グループに追加されない。
CSCwh42009	Cisco ISE リリース 3.2 パッチ 3 : アダプタログの問題。
CSCwf22527	Context Visibility : エンドポイントのカスタム属性を特殊文字でフィルタリングできない。
CSCwf88944	ゲストポータルの FQDN がデータベース内のノードの IP アドレスにマッピングされる。

警告 ID	説明
CSCwd38766	「-」または「_」文字が含まれる SNMPv3 ユーザー名を削除すると、Cisco ISE から 16 進数のユーザー名が削除されない。
CSCwe74135	Cisco ISE リリース 3.1 パッチ 5：ゲストポータル削除に失敗する：ORA-02292：完全性の制約。
CSCwf10773	「no ip name-server」は、プロンプトなしでサービスを直接再起動する。
CSCvw81130	Cisco ISE リリース 2.7：Active Directory 診断ツールのスケジュール済みテストを無効にできない。
CSCwd34685	Cisco ISE メッセージングサービスが「Not running」と「Initializing」の間で揺れている。
CSCwf30570	コンピュータが AC 電源に接続されていない場合、エージェントレススクリプトが実行されない。
CSCwf24158	Portal Builder を Cisco ISE リリース 3.0 以降のリリースで使用すると、[Terms and Conditions] チェックボックスが表示されない。
CSCwf94289	Cisco ISE リリース 3.0 パッチ 6：ポリシーのエクスポートでポリシーがエクスポートされない。
CSCwa08802	AWS 上の Cisco ISE リリース 3.1 で正常性チェックのための DNS チェックで検出漏れが生じる。
CSCwe15945	ゲストアカウントが特定のスポンサーグループのスポンサーに表示されない。
CSCwf34391	PassiveID がアクティブ認証の前に発生した場合、Cisco ISE Easyconnect ステッチングは機能しない。
CSCwh42442	Cisco ISE リリース 3.2 パッチ 3：CRL のダウンロードに失敗する。
CSCvy88380	既存の証明書の Cisco ISE メッセージングの使用状況を選択できない（グレー表示される）。
CSCwf21585	安全でない可能性のあるメソッドの使用：HTTP PUT メソッドが受け入れられた。
CSCwh14249	API ゲートウェイ設定で Cisco ISE 3.x のスペルミスがある。
CSCwf09364	ユーザーおよびエンドポイント ID グループの説明フィールドは、長いテキストでは編集できない。
CSCwf47038	pxGrid ポリシーの [Trash all] または [selected] が、内部グループのエントリに影響しないようにする必要がある。
CSCwh04251	Cisco ISE エージェントレスポスチャで、「:」文字を含むパスワードがサポートされない。
CSCvu56500	Cisco ISE がすべてのネットワークデバイスをエクスポートし、空のファイルを提供する。
CSCwf66237	Cisco ISE リリース 2.7 以降、Cisco ISE の「Get All Endpoints」要求の実行に時間がかかる。

警告 ID	説明
CSCwf59058	管理メニューが非表示の場合、カスタム権限を持つ RBAC ポリシーが機能しない。
CSCwd97984	Cisco ISE アプリケーションサーバーの再起動直後に Meraki 同期サービスが実行されない。
CSCwf66880	エンドポイントの .csv ファイルのインポートで、ファイルを選択した後に「No file chosen」と表示される。
CSCwf26951	プロファイラ CoA が誤ったセッション ID で送信される。
CSCwd17322	AWS の Cisco ISE：正常性チェック入出力帯域幅のパフォーマンスとチェックの誤報。
CSCwe27438	パッチ管理、アップグレード、およびヘルスチェックで起動ページレベルのヘルプが機能しない。
CSCwf40265	Cisco ISE の最大セッションカウンタの時間制限が機能しない。
CSCwb18744	説明に複数のバックスラッシュ文字が連続して含まれる SG とコントラクトは、Cisco ISE と同期できない。
CSCwh48026	pxGrid direct-connector.log で、実際のクロック時刻とログの出力時刻が一致しない。
CSCwf37679	プライマリ PAN からアクセスすると、スポンサーポータルでスポンサー権限が無効になる。
CSCwf96294	Cisco ISE リリース 3.0：許可されていないドメインへの接続試行。
CSCwf23981	Cisco ISE 認証プロファイルに誤ったセキュリティグループと VN 値が表示される。
CSCwf61939	[First Name] と [Last name] フィールドにアポストロフィを使用すると、名前が無効である旨のエラーが表示される。
CSCwd36753	スクリプトの条件名にピリオドが含まれている場合、AnyConnect ポスチャスクリプトが実行されない。
CSCwc36589	Intune からの MAC アドレスベースの API のサポート終了により、Cisco ISE Intune MDM 統合が中断される可能性がある。
CSCwh18731	アップグレード前に LSD を無効にして Cisco ISE リリース 3.2 にアップグレードすると、EP プロファイラ例外が発生する。
CSCwc53824	Cisco ISE で、AMP AMQP サービスへの接続が TLSv1.0 に制限される。
CSCwf36285	[Manage SXP Domain filters] の行には、最大 25 しか表示されない。
CSCwf07855	コールが失敗した場合、Cisco ISE SXP バインディング API コールが 2xx 応答を返す。
CSCwf82055	パッシブ ID エージェントに関連付けられたポートの SHA1 を無効にできない。
CSCwf62744	ENH：「Disable EDR Internet Check」タグの追加。

警告 ID	説明
CSCwh28098	Cisco ISE リリース 3.2 パッチ 3 : RSD が無効になっているポスチャアセスメント中に、CoA プッシュの代わりに CoA 切断が送信される。
CSCwf14365	ログ分析ページで「Configuration Missing」という警告が表示される。
CSCwe82004	TCP ソケットの枯渇。
CSCwe53550	Cisco ISE および CVE-2023-24998。
CSCwf71870	0 日間の評価期間で TACACS 展開を行った場合、スマートライセンスの登録後に動作しない。
CSCwh46877	PORT_BOUNCE を使用して ANC ポリシーを削除する際、CoA ポートバウンズが必要となる。
CSCwf62987	Antisamy 1.5.9 に存在する脆弱性。
CSCwh32290	リセット設定の実行後、GUI と CLI の FQDN 値が一致しない。
CSCwf42496	「Is IPSEC Device」NDG を削除しようとする、後続のすべての RADIUS/T+ 認証が失敗する。
CSCwc44622	NAD (Meraki) が誤動作したときに再起動するまで、セッションが無期限に停止する。
CSCwh51136	Cisco ISE が RADIUS 要求をドロップし、「Request from a non-wireless device was dropped」というメッセージが表示される。
CSCwf33018	バグ CSCwd35608 の修正により、UI からの CoA コールが誤った IP アドレスに送信される。
CSCwf44942	最大ユーザーセッション認証フロー中に TACACS:PSN がクラッシュする。
CSCwf19039	Cisco ISE リリース 3.1 パッチ 5 : エージェントレスポスチャの失敗により、/tmp/ フォルダのサイズが増加する。
CSCwf31477	スイッチポートに複数のセッションが存在する場合、プロファイラがポートバウンズをトリガーする。
CSCwf55641	ドイツ語とイタリア語の電子メールがゲストタイプのアカウント有効期限通知に保存されない。
CSCwh28528	TACACS 着信メッセージが 1 日あたり 4,000 万レコードを超えると、TopN デバイス管理レポートが機能しなくなる。
CSCwe96739	TLS 1.0 および TLS 1.1 は、Cisco ISE リリース 3.0 管理者ポータルで受け入れられる。
CSCwe95624	ノードの再起動後に Cisco ISE リリース 3.2 SNMP が機能しない。
CSCwe03624	スマートライセンスの登録に失敗し、「communication send error」アラームが断続的に発生する。

警告 ID	説明
CSCwf81550	Cisco ISE で、必要ない場合でも、選択した MAC アドレス形式に従って MAC アドレス形式が変更される。
CSCwf54680	名前に括弧が含まれている認証プロファイルを編集または削除できない。
CSCwh38484	Cisco ISE リリース 3.0 パッチ 7 で、スタティックルートを手動で削除すると、Cisco ISE が誤った MAC のパケットを送信する。
CSCwf35760	ct_engine の CPU 使用率が 100% になる。
CSCwh39008	構成バックアップのスケジュールを設定または編集できない。
CSCwf60904	ANC の修復が AnyConnect VPN で機能しない。
CSCwh03227	認証プロファイルルールを使用せず認証すると、Cisco ISE がライセンスを使用しない。
CSCwf80951	「xwt.widget.repeater.DataRepeater」エラーにより、管理者ユーザーを編集または作成できない。
CSCwe98676	ZAP の実行中に脆弱な JavaScript ライブラリの問題が見つかった。
CSCwd20521	Active Directory コネクタが停止しない。
CSCwf59310	Cisco ISE リリース 3.1 パッチ 7 : Context Visibility : pxGrid コンテキストイン : カスタム属性が存在しない。
CSCwh05647	IPv6 のスタティックルートが、Cisco ISE リリース 3.2 でのリロード後に削除される。
CSCwh41693	Cisco ISEaaS : AWS : IMDS v2 の問題をサポート。
CSCwh00049	Cisco ISE の保存されたクロスサイトスクリプティングの脆弱性。

## Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 4

これらは、Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 4 です。

問題 ID 番号	説明
CSCwh92366	3.1 パッチ 8 : 3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。



## Cisco ISE リリース 3.2 の新機能 : 累積パッチ 3

### 外部 LDAP ユーザーを Cisco ISE エンドポイントグループにリンクする

Cisco ISE リリース 3.2 パッチ 3 以降では、[Dynamic] オプションを使用して、外部 LDAP ユーザーグループをゲストデバイスのエンドポイント ID グループに割り当てることができます。詳細については、『Cisco Identity Services Engine Administrator Guide, Release 3.2』の「Guest and Secure WiFi」の章の「[Create or Edit Guest Types](#)」[英語]を参照してください。

### GUI からの Cisco ISE 展開の分割アップグレード

分割アップグレードは、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では、ノードを反復またはバッチでアップグレードすることでダウンタイムを制限できますが、プロセスには完全アップグレードよりも時間がかかる場合があります。

詳細については、『Cisco Identity Services Engine Upgrade Guide, Release 3.2』の「Perform the Upgrade」の章にある「Split Upgrade of Cisco ISE Deployment from GUI」を参照してください。

### ポータルでのウクライナ語のサポート

ゲスト、スポンサー、デバイス、およびクライアントプロビジョニングポータルに、サポートされるローカリゼーション言語としてウクライナ語が含まれるようになりました。

## Cisco ISE リリース 3.2 の解決済みの不具合 : 累積パッチ 3

警告 ID	説明
<a href="#">CSCwe61215</a>	パスワードが 16 文字を超えて設定されている場合、CLI を介した SFTP および FTP 検証が失敗する。
<a href="#">CSCwf15717</a>	ISE 3.2 : システム 360 が、デバイス管理ライセンスでのみ使用できない。
<a href="#">CSCvr79992</a>	Session.CurrentDate 属性が認証時に正しく計算されない。
<a href="#">CSCwe68336</a>	条件別ポスチャ評価で ORA-00904: "SYSTEM_NAME": invalid identifier が生成される。
<a href="#">CSCwe15315</a>	ネットワークデバイスの CSV テンプレートファイルをインポートすると、TrustSec PAC 情報フィールドの属性値が失われる。
<a href="#">CSCwf14957</a>	ISE で日本語の UI を使用している場合、TrustSec ステータスを変更できない。
<a href="#">CSCwe69085</a>	デバイス管理ライセンスのみが有効になっている場合、PSN GUI にアクセスできない
<a href="#">CSCwd97022</a>	ISE-PIC 3.2 p3 のスマートライセンスが無効化された PIC アップグレードはコンプライアンス違反である。

警告 ID	説明
CSCwd46505	ISE-PIC がキューリンクのエラーを表示しない。
CSCwe24932	エンドポイントログイン設定で複数のドメインユーザーを使用すると、エージェントレスポスタチャが失敗する。
CSCwe54318	バインディングのクエリでの H2 DB の遅延が原因で、SXP サービスが初期化でスタックする。
CSCvt62460	LDAP がノードごとに定義されている場合、異なる LDAP からグループまたは属性を取得できない。
CSCwe49261	ISE PassiveID エージェントは、passiveID が設定されていないドメインを含むすべてのドメインのステータスをプローブする。
CSCwd47111	ISE が音声 VLAN のサブネットまたは IP アドレス プール名を保存できない。
CSCwd79277	同期に最大数の TrustSec オブジェクトが選択されている場合、同期ステータスが失敗と表示される。
CSCwf26973	管理者アカウントが読み取り専用の場合、ネットワーク デバイス グループ情報が欠落している。
CSCwd97606	異なるセッション ID を持つ同じ IP + VN + VPN の組み合わせに対する複数のリクエストにより、重複するレコードが作成される。
CSCwe07822	ISE の最後の消去日付のタイムスタンプが正しくない。
CSCwd90613	[RADIUS Server Sequences] ページに「no data available」と表示される。
CSCwf28229	VLAN 検出間隔を 30 秒以下にする必要がある。
CSCwd12357	ポート 9644 での例外が原因で、SXP サービスが初期化中にスタックする。
CSCwe59587	日本語表示で、一部の項目に [Test] と表示される。
CSCwe37978	巨大なサイズのスケジュールされたレポートが、エクスポート時にリポトリで空として表示される。
CSCwe92640	ISE 3.1 および 3.2 : CLI 設定時に既存のルートの検証が失敗する。
CSCwe43002	読み取り専用管理者を、ISE 管理 SAML 認証で使用できない。
CSCwe93253	ISE : フィルタが1つのネットワークデバイスに一致する場合にのみ、ネットワークデバイス CAPTCHA が入力を要求する。
CSCwe64558	ネットワークアクセスユーザーから作成された管理者アカウントは、ダークモード設定を変更できない。

警告 ID	説明
CSCwf19463	条件スタジオのドラッグアンドドロップ階層化。
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。
CSCwe85828	新しい管理証明書を生成した後、信頼ストアが管理証明書を更新しない。
CSCwc47015	CSCvz85074 の修正により、ISE での AD グループの取得が中断される。
CSCwe52296	ISE MNT 認証ステータス API クエリを最適化する必要がある。
CSCwf33128	RADIUS の使用済みスペースで、いくつかの TACACS テーブルも考慮されるため、誤った使用状況が報告される。
CSCwb83304	カスタム セキュリティ グループが原因で ISE のアップグレードが失敗する。
CSCwc47799	パスワードに % が含まれている場合、証明書と秘密キーをインポートするときに ISE にエラーが表示されない。
CSCwe11676	Cisco ISE ダッシュボード [Threat for TC-NAC] の [Total Compromised Endpoints] にアクセスすると、データが失われる。
CSCwe41695	ISE 3.1P4 および P5：管理アクセス制限を削除した後に再起動すると、スタンドアロン ISE がクラッシュする。
CSCwe80760	パラメータに二重引用符 ("" ) が含まれている場合、プログラム起動修復を保存できない。
CSCwe17954	Cisco Identity Services Engine 情報開示の脆弱性。
CSCwe70402	ISE 3.2 は、単一行の JavaScript コメントを含むポータル カスタマイズ スクリプトを処理できない。
CSCwf40128	CiscoSSL ルールに則った KU 目的の検証なしでクライアント証明書を受け入れる。
CSCwe52461	ISE 3.1 でファイアウォール条件を有効にできない。
CSCwe96633	サポートバンドルに terrors.log および times.log が含まれない。
CSCwf22799	コンプライアンスモジュールが Secure Client と互換性がない場合、遅延更新条件が機能しない。
CSCwd39746	MS が ADAL を廃止しているため、SCCM と ISE の統合に MSAL のサポートが必要。
CSCwe97989	ISE 3.2 が認証プロファイルの VN でクラッシュする。

警告 ID	説明
CSCwe38800	hibernate-validator の脆弱性 - 複数のバージョン。
CSCwe49167	ISE 3.2 SAML 署名認証要求の設定が保存時にオフになる。
CSCwf33881	ISE 3.2 P1 が、ISE ポートまたはリソースのリファレンスガイドに記載されていないサーバーへの接続を確立する。
CSCwf13630	Mnt ログプロセッササービスが毎晩停止する。
CSCwe12098	ISE 3.2 : ゲストポータル設定用のポートが、AWS ノードにインストールされた ISE ノードで開かない。
CSCwe86793	REST ID ストアグループの ISE フィルタに「Error Processing this request」と表示される。
CSCwe40577	API リソース要求の処理に失敗する：条件の変換に失敗する。
CSCwe70975	ISE で、SMS JavaScript のカスタマイズが SMS 電子メールゲートウェイで機能しない。
CSCwe69179	ISE : 最新の IP アクセス制限設定により、以前の設定が削除される。
CSCwf31073	ISE 3.1 : デバイス管理ネットワーク条件が取得されると、OpenAPI エラー 400 が発生する。
CSCwf33421	タイムゾーンの変更中に更新警告メッセージが表示される。
CSCwe49422	ISE 3.2 以降で、identity-store コマンドにクリアテキストパスワードを入力する必要がある。
CSCwf09393	古い ISE バージョン 2.7 からのバックアップの復元後に ISE 3.1 のサービスを開始できない
CSCwc70197	ISE 証明書 API は、フレンドリ名にハッシュ文字を含む信頼できる証明書を返すことができない。
CSCwf15130	Collector.log ファイルの権限が、自動的に root として設定される。
CSCwe38610	MDM API V3 証明書文字列で大文字と小文字が区別されないようにする。
CSCwe57240	カスタム属性の追加中に GUI でデフォルト値が検証されない。
CSCwe55215	ISE スマートライセンスが Smart Transport を使用するようになった。
CSCwf05309	ISE SAML 証明書が他のノードに複製されない。
CSCwe83868	spring-framework 5.1.3 の脆弱性
CSCwf34596	[User Custom Attributes] がレンダリングでスタックする。

警告 ID	説明
CSCwe78540	[Get All Endpoints] が呼び出されると、iotAsset 情報が欠落する。
CSCwe43468	VN 参照を使用したスタティック IP-SGT マッピングにより、DNAC グループベースのポリシーの同期が失敗する。
CSCwc13859	「System Admin」管理者グループの管理者ユーザーで、スケジュールされたバックアップを作成できない。
CSCwf26226	EP 消去呼び出しに伴うメモリークによる CPU スパイク。
CSCwc20314	ISE-PIC 3.1 : PIC ライセンス : 消費 0。
CSCwf40861	UI に、コマンドセット内の文字の HTML 16 進数コードが表示される。
CSCwd55061	既存の NDG の作成中に ERS API 内部エラーが発生する。
CSCwe86494	ISE で特定の URL を使用すると、tomcat スタックトレースが表示される。
CSCwd41098	pxGrid の無効化後に ise-psc.log で pxGrid のエラーログが記録される。
CSCwe41824	ISE 3.2 で PKI ベースの SFTP の S-PAN キーが存在しない。
CSCwd82119	ISE 3.1 で ECDSA 証明書を使用した EAP-TLS 認証が失敗する。
CSCwf26482	ISE 3.1 からバージョン 3.2 へのアップグレード後に REST AUTH サービスが実行されない。
CSCwd05040	展開への登録後にセカンダリノードに証明書をインポートできない。
CSCwf10004	ISE の IP SGT スタティックマッピングを別のマッピンググループに移動するときこのマッピングが SXP ドメインに送信されない。
CSCwe36242	TACACS コマンド アカウンティング レポートのエクスポートが機能しない。
CSCwc85867	ISE の変更構成監査レポートに、SGT の作成および削除イベントが明確に表示されない
CSCwd70658	ネットワーク アクセス デバイスを追加できない。理由：「There is an overlapping IP Address in your device」（デバイスに重複する IP アドレスがある）。
CSCwe99961	ドイツのスポンサードポータル - カレンダーに木曜日（Donnerstag）が Di not Do と表示される。
CSCwf23981	ISE 認証プロファイルに誤ったセキュリティグループと VN 値が表示される。

警告 ID	説明
CSCwd73282	ISE 3.1 パッチ 3：スポンサーポータル：[Session Cookie] の SameSite 値が none に設定される。
CSCwf09674	登録済みエンドポイントレポートに、未登録のゲストデバイスが表示される。
CSCwc85546	ISE 3.1 ENH 「Illegal hex characters in escape (%) pattern ? for input string: ^F"」が表示される。
CSCwf17490	SL 更新後、ISE ライセンスページに、消費されたライセンスの評価コンプライアンスステータスが表示される。
CSCwe30235	jszip 3.0.0 の脆弱性。
CSCwe84210	LicenseConsumptionUtil.java の NullPointerException が原因で、認証ポリシーの評価が失敗する。
CSCwe69189	LSD により、帯域幅の使用率が高くなる。
CSCwb44638	機能拡張：MNT DB メトリックを含む別のログファイルを生成。
CSCwd31414	[Reason for Visit] フィールドに特殊文字が含まれていると、ゲストポータルで「Error Loading Page」エラーが表示される。
CSCwf21960	アップグレード中、登録解除コールでデータベースからのすべてのノードの削除に失敗する。
CSCwe18371	ISE 3.2 の管理アクセス制限に関する問題。
CSCwe36063	[Advanced Tuning] ページで PBIS 登録キー設定が検証されない。
CSCwe63873	Qualys アダプタがナレッジベースをダウンロードできない。ナレッジのダウンロードが進行中のままスタックする。
CSCwd97551	EAP-TLS セッションの再開時に ISE がクライアント証明書から OU 属性を取得できない。
CSCwc80574	ISE AD コネクタが参加の処理中に失敗する。
CSCwd68070	SAML メタデータのインポートが失敗する。
CSCvx15522	FQDN syslog ポップアップの DNSCache 有効化コマンドを修正する必要がある。
CSCwe37826	ポスチャポリシー条件で条件演算子を AND から OR に変更できない。
CSCwe71729	ISE 3.2：Data Connect パスワードの期限切れ間近アラームが 1 分ごとに表示される。

警告 ID	説明
<a href="#">CSCwc57162</a>	証明書ベースの GUI 管理者ログインがスタックする。
<a href="#">CSCwe39262</a>	パッシブ AD エージェントが誤った時刻形式のイベントを送信する。
<a href="#">CSCwd38136</a>	Cisco Identity Services Engine GUI のサービス拒否 (DoS) の脆弱性。
<a href="#">CSCwd54844</a>	ネットワーク デバイス グループ作成のための ERS API スキーマ。
<a href="#">CSCwe49183</a>	署名付き認証要求の ISE SAML 宛先属性がない。
<a href="#">CSCwe36788</a>	ISE 3.2 で、IP アクセスルールの追加時に追加されたルールを削除できない。
<a href="#">CSCvz86446</a>	ISE レプリケーション：SyncRequest タイムアウト モニター スレッドがタイムアウト後にファイル転送を強制終了しない。
<a href="#">CSCwe12618</a>	ISE 3.2：APIC 統合：com.cisco.cpm.apic.ConfImporter:521 - Failed to get EPs null。
<a href="#">CSCwe71804</a>	ISE 3.1：サードパーティのネットワーク デバイス プロファイルが使用されている場合、SessionCache にキー属性がない。
<a href="#">CSCwe34566</a>	ROPC ID ストアに対する認証が RSA キー生成エラーで失敗する。
<a href="#">CSCwb79496</a>	エージェントプロトコルから WMI プロトコルへのマッピング後に WMI ステータスに進行状況が表示される。
<a href="#">CSCwe49504</a>	ISE 3.2 の identity-store コンフィギュレーション コマンドで、16 文字を超えるパスワードがサポートされていない。
<a href="#">CSCwe39781</a>	CoA 後に SGT が変更されると、ISE は SXP マッピングを削除しない。
<a href="#">CSCwe30606</a>	GUI から 1GB を超えるサイズのサポートバンドルをダウンロードできない。
<a href="#">CSCvv99093</a>	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： Cause=Timeout。
<a href="#">CSCwf16165</a>	15 文字を超える NTP 認証キーで % ERROR: bad hashed key が発生する。
<a href="#">CSCwd89797</a>	Meraki コネクタでデバッグログレベルが有効になっている場合に、例外エラーメッセージが表示される。

## Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 3

これらは、Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 3 です。

問題 ID 番号	説明
<a href="#">CSCwf59005</a>	PEAP と EAP-TLS は FIPS モードでは機能しない。
<a href="#">CSCwh92366</a>	3.1 パッチ 8 : 3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。

## Cisco ISE リリース 3.2 の新機能 : 累積パッチ 2

### pxGrid Cloudでのコンテキストイン API の一括更新と一括削除のサポート

Cisco ISE リリース 3.2 パッチ 2 から、pxGrid Cloudでコンテキストイン API がサポートされ、エンドポイントの一括更新および一括削除が可能になります。詳細については、『[Cisco pxGrid Cloud Onboarding Guide](#)』[英語] および『[Cisco ISE API Reference Guide](#)』[英語] を参照してください。

### pxGrid Direct の機能拡張

pxGrid Direct は、制御された導入機能ではなくなりました。Cisco ISE リリース 3.2 または 3.2 パッチ 1 から Cisco ISE リリース 3.2 パッチ 2 にアップグレードする前に、設定済みのすべての pxGrid Direct コネクタと、pxGrid Direct コネクタからのデータを使用する認証プロファイルおよび認証ポリシーを削除することを推奨します。Cisco ISE リリース 3.2 パッチ 2 にアップグレードした後、pxGrid Direct コネクタを再設定してください。



(注) 設定済みの pxGrid Direct コネクタを削除しない場合、コネクタはアップグレード中に自動的に削除されます。この削除により、編集も使用も不可能な認証プロファイルと認証ポリシーが作成されます。これらを削除して新しいものに置き換える必要があります。

pxGrid Direct 機能の変更の詳細については、『[Cisco Identity Services Engine Administration Guide, Release 3.2](#)』の「Asset Visibility」の章にある「[pxGrid Direct](#)」[英語] を参照してください。

### Cisco Secure Network Server 3700 シリーズ アプライアンスのサポート

Cisco Secure Network Server (SNS) 3700 シリーズ アプライアンスは、Cisco Unified Computing System (Cisco UCS) C220 ラックサーバーに基づいており、特に Cisco ISE をサポートするように構成されています。Cisco SNS 3700 シリーズ アプライアンスは、幅広いワークロードで高いパフォーマンスと効率性を提供するように設計されています。

Cisco SNS 3700 シリーズ アプライアンスには次のモデルがあります。

- Cisco SNS 3715 (SNS-3715-K9)
- Cisco SNS 3755 (SNS-3755-K9)
- Cisco SNS 3795 (SNS-3795-K9)



Cisco SNS 3715 アプライアンスは、小規模な展開向けに設計されています。Cisco SNS 3755 および Cisco SNS 3795 アプライアンスには、ハードディスクや電源などの複数の冗長コンポーネントがあり、信頼性の高いシステム構成を必要とする大規模な展開に適しています。

詳細については、『[Cisco Secure Network Server 3700 Series Appliance Hardware Installation Guide](#)』を参照してください。



- (注) Cisco ISE 3.2 パッチ 2 以降のバージョンで、Cisco SNS 3700 シリーズ アプライアンスがサポートされます。したがって、SNS 3700 シリーズ アプライアンスに最初のパッチ (ISE 3.2 パッチ 2 以降) をインストールした後は、ISE 3.2 にロールバックできません。



- (注) [Cisco ISE ソフトウェアダウンロードサイト](#)で Cisco ISE 3.2 アップグレードバンドルが置き換えられました。SNS 3700 シリーズ アプライアンスで Cisco ISE 3.1 から Cisco ISE 3.2 にアップグレードするには、新しいアップグレードバンドル (ise-upgradebundle-2.7.x-3.1.x-to-3.2.0.542b.SPA.x86\_64.tar.gz) を使用する必要があります。

## Cisco ISE リリース 3.2 の解決済みの不具合：累積パッチ 2

ID	見出し
<a href="#">CSCwe25138</a>	ユーザーのカスタム属性に \$ または ++ 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
<a href="#">CSCwd45783</a>	P-PIC がダウンしている間に FMC を再統合すると、pxGrid セッションのパブリッシュが停止する
<a href="#">CSCwd70902</a>	マージを回避するために IMS が有効になっている場合、PRRT はフラグメント化されていないメッセージを MnT に送信する必要がある
<a href="#">CSCwd92324</a>	ISE 3.2 ROPC の基本的な有用性の改善
<a href="#">CSCwd84055</a>	ISE 3.1 で MDM API V3 の Azure AD 自動検出が正しくない
<a href="#">CSCwd41218</a>	Cisco Identity Services Engine のコマンドインジェクションの脆弱性
<a href="#">CSCwd27865</a>	エンドポイントをグループに割り当てるときに、変更された設定が機能しない
<a href="#">CSCwd39056</a>	ISE 3.1 P4 のパッシブ DC 設定でユーザー名を正しく保存できない
<a href="#">CSCwc91917</a>	TACACS 認証プロファイルに引用文字を追加できない
<a href="#">CSCwc62716</a>	IndexRebuild.sql スクリプトが MnT で実行される
<a href="#">CSCwe18371</a>	ISE 3.2 の管理アクセス制限に関する問題

ID	見出し
CSCwd63661	GUIで誤ったパスワードを入力すると、エンドユーザーの同意が表示される
CSCwd97353	自動バックアップが3～5日後に停止する
CSCwd71574	エージェントレスポスチャが設定されている場合にCPU使用率が高くなる
CSCwe27146	ISE 3.2 パッチ 1：「-」（ハイフン/ダッシュ）を含む CLI 管理ユーザー名を解析できない
CSCwd26845	APIC 統合に fvIP サブスクリプションがない
CSCwc65821	ERS API で、「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ない
CSCwc39302	シャットダウン後もインターフェイスのステータスが UP と表示される
CSCwd63749	大量の AD グループ（400 以上）をロードすると、[AD Retrieve Groups] に空白のページが表示される
CSCwd71496	ISE が [All SXP Mapping] テーブルからセッションを削除しない
CSCwd92835	[Network Device Profile ] に HTML コードが名前として表示される
CSCwe07406	アカウント登録ゲストポータルでゲストアカウントを作成すると、「Error Loading Page」エラーが表示される
CSCwd79277	同期に最大数の TrustSec オブジェクトが選択されている場合、同期ステータスが失敗と表示される
CSCwa52678	GUI TCPDUMP が Stop_In_Progress でスタックする
CSCwe00424	ISE : NAS-Port-id の長さが原因で収集失敗アラームに SQLException が送信される
CSCwe14808	ISE が msRASSavedFramedIPAddress の AD 属性の変換に失敗する
CSCwd98296	[Network Device Port Conditions] ページの [IP Addresses/Device Groups] フィールドに有効なポート文字列を入力できない
CSCwd57978	IP とロケーションでネットワークデバイスをフィルタリングすると、すべての NAD が削除される
CSCwe37041	元の PPAN が削除されると、内部 CA 証明書チェーンが無効になる
CSCwc64480	同じサブジェクトを使用し、外部 CA（CSR なし）によって署名された新しい証明書がポータルにインポートされると、ISE によるセキュアな接続の確立が失敗する

ID	見出し
CSCwd22790	ISE 3.1/3.2 で、URI が Group 属性または Name として SAML IdP の属性のアサーションに受け入れられない
CSCvy69943	{ } 文字を含むコンテンツヘッダーを含むゲストポータル HTTP リクエストが許可される
CSCwe07354	RADIUS トークンサーバー設定がセカンダリサーバーの空のホスト IP を受け入れる
CSCwd57071	自己登録ポータルが、スポンサーに送信される承認/拒否リンクのノード FQDN をサポートしない
CSCwd24286	ISE が DNAC にホスト名属性を送信しない
CSCwe44750	フィールド増分更新後に再プロファイリング結果が Oracle および VCS DB に保存されない
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
CSCwd74560	DNAC を介した ISE (ERS) へのペイロードで PUT 操作が失敗する
CSCwe63320	ISE で「Get All Endpoints」レポートに不一致の情報が表示される
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
CSCwe33360	異常な動作の検出が期待どおりに機能しない
CSCwd82134	ISE で不正な SLR コンプライアンス違反エラーが報告される
CSCwe37018	ISE 信頼ストアに無効な証明書がある場合、ISE-DNAC 統合が失敗する
CSCwc48311	IMS を使用した ISE vPSN のパフォーマンスが、UDP syslog と比較して 30 ~ 40% 低下する
CSCwe13780	特定の OU を設定すると、REST API によってノードを AD に参加させることができない
CSCwd93002	グループを編集し、SAML でアサーションに Name を追加すると、Null システムエラーが発生する
CSCwd31524	16 文字のパスワードが、ISE 3.2 の sftp 設定でサポートされない
CSCwe02315	ISE GUI の Meraki コネクタページのオンラインページレベルのヘルプ ID
CSCwd41651	ISE 3.1 の垂直スクロールバーのバグ

ID	見出し
<a href="#">CSCwd69072</a>	ユーザー定義 NAD プロファイルを使用した Cisco NAD でのセッションディレクトリ書き込み失敗アラーム
<a href="#">CSCwe15576</a>	KRON ジョブを設定できない
<a href="#">CSCwc55529</a>	証明書の秘密キーが見つからないため、認証に失敗する
<a href="#">CSCwc07082</a>	csv ファイルからユーザーをインポートしようとする時、「The phone number is invalid」エラーメッセージが表示される
<a href="#">CSCwd87161</a>	デバイス管理ライセンスのみが有効になっている場合、証明書ベースのログインでライセンスファイルが要求される
<a href="#">CSCwe34204</a>	パッチのインストール後に ISE アップグレードタブにアップグレードが進行中であると表示される
<a href="#">CSCwe22934</a>	MAC アドレスのないデバイスからの ISE 認証遅延
<a href="#">CSCwd63717</a>	PKI 対応の SFTP リポジトリが ISE 3.2 で機能しない
<a href="#">CSCwb85502</a>	CIAM : xstream 1.4.17
<a href="#">CSCwe99816</a>	CLI コマンド「show restore status」で Completed_With_Success が表示される 25 分前に、ISE openAPI 復元でこのメッセージが表示される
<a href="#">CSCwe45245</a>	スマートライセンスの登録が正しく機能していない
<a href="#">CSCwd51812</a>	証明書ベースの認証を使用している場合、ISE GUI にアクセスしようすると、アクセス許可エラーが発生する
<a href="#">CSCwe13110</a>	プライマリ MnT ノードで設定バックアップが実行される
<a href="#">CSCvg66764</a>	ISE PIC エージェントによるセッションスティッチングのサポート
<a href="#">CSCwd74898</a>	「Posture Configuration detection」アラームは「INFO」レベルであり、言い回しを変更する必要がある
<a href="#">CSCwd64649</a>	複数の内部 CA 証明書による Cisco DNA Center 統合の問題
<a href="#">CSCwe13947</a>	EP 作成/更新の OpenAPI は、ERS API と同じように動作する必要があるのに加え、より多くの機能を提供する必要がある
<a href="#">CSCwe57764</a>	CVE-2021-26414 の Windows DCOM サーバー強化後に Microsoft SCCM への MDM 接続が失敗する
<a href="#">CSCvo61351</a>	ライブセッションが「認証済み」状態でスタックする
<a href="#">CSCwe74108</a>	Cisco AI Analytics が IP アドレスとして設定されたプロキシで機能しない

ID	見出し
CSCwd97582	ISE 3.1p5 で CA 証明書 EKU が検証され、「unsupported certificate」エラーが発生する

## Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 2

これらは、Cisco ISE リリース 3.2 の未解決の不具合：累積パッチ 2 です。

問題 ID 番号	説明
CSCwf25955	SGT、VN 名、VLAN フィールドが空の match 認証プロファイルを使用すると、ポートがクラッシュする。
CSCwf40128	CiscoSSL ルールに則った KU 目的の検証なしでクライアント証明書を受け入れる。
CSCwf02093	Cisco ISE リリース 3.2 では、Hyper-V のインストールで DHCP が有効になっている。
CSCwe92640	Cisco ISE リリース 3.1 および 3.2：CLI 設定時に既存のルートを検証が行われない。
CSCwf32255	Cisco ISE リリース 3.2 パッチ 2 で「snmp-server host」が設定されている場合、SNMP サーバーから応答を受信しない。
CSCwe95624	Cisco ISE リリース 3.2 で、ノードの再起動後に SNMP が機能しない。
CSCwe69179	最新の IP アクセス制限設定により、Cisco ISE で以前の設定が削除される。
CSCwe36788	Cisco ISE リリース 3.2 では、ユーザーは IP アクセスルールの追加工中に追加されたルールを削除できない。
CSCwe41695	Cisco ISE リリース 3.1 パッチ 4 および 5 では、管理者アクセス制限を削除した後に再起動すると、スタンドアロン Cisco ISE ノードがクラッシュします。
CSCwf55795	Cisco ISE リリース 3.2 パッチ 1 で、ADE-OS を使用した設定の復元後、Cisco ISE GUI および CLI にアクセスできない。
CSCwd97551	EAP-TLSセッションでCiscoISEがクライアントの証明書から複数の属性値を取得できない。
CSCwh92366	3.1 パッチ 8：3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。

## Cisco ISE リリース 3.2 - 累積パッチ 1 の新機能



- (注) アプリケーション内のオンラインヘルプには、Cisco ISE リリース 3.2 パッチ 1 の機能と拡張機能に関する情報は含まれていません。次の新機能と拡張機能の設定情報については、『[Cisco Identity Services Engine Administrator Guide, Release 3.2](#)』を参照してください。

### Cisco Secure Client の延長サポート

Cisco ISE 3.2 パッチ 1 は、Windows、MacOS、Linux オペレーティングシステム用の AnyConnect と Cisco Secure Client の両方をサポートしています。これらのオペレーティングシステムでは、次の Cisco Secure Client バージョンがサポートされています。

- Windows : Cisco Secure Client バージョン 5.00529 以降
- MacOS : Cisco Secure Client バージョン 5.00556 以降
- Linux : Cisco Secure Client バージョン 5.00556 以降

これらのオペレーティングシステムではエンドポイントに対して AnyConnect と Cisco Secure Client の両方を構成できますが、エンドポイントでの実行時に考慮されるのは 1 つのポリシーのみです。



- (注) Cisco ISE 3.2 は、Windows OS に対してのみ Cisco Secure クライアントをサポートします。

詳細については、『[Cisco Identity Services Engine Administrator Guide, Release 3.2](#)』の「[Compliance](#)」の章 [英語] を参照してください。

### Cisco ISE の Meraki コネクタ

Cisco ISE およびクラウドベースの Cisco Meraki は、TrustSec ポリシーのポリシー管理ポイントである TrustSec 対応システムです。Cisco と Meraki の両方のネットワークデバイスを使用している場合、1 つ以上の Cisco Meraki ダッシュボードを Cisco ISE に接続して、TrustSec ポリシーおよび要素を Cisco ISE から各組織に属する Cisco Meraki ネットワークに複製できます。

Meraki コネクタの設定の詳細については、『[Cisco Identity Services Engine Administrator Guide, Release 3.2](#)』の「[Segmentation](#)」の章にある「[Connect Cisco Meraki Dashboards with Cisco ISE](#)」を参照してください。

### コンテキストインの pxGrid Cloud サポート

Cisco ISE リリース 3.2 累積パッチ 1 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。詳細については、『[pxGrid Cloud Onboarding Guide](#)』 [英語] を参照してください。

## Cisco AI 分析のサポート

Cisco ISE 3.2 パッチ 1 以降は Cisco AI 分析をサポートしています。Cisco AI Analytics エージェントは、Cisco ISE からエンドポイントのデータに対してクエリを実行し、そのデータを定期的に AI クラウドに送信します。このデータを使用して、AI ベースのエンドポイントグループ化、自動化されたカスタム プロファイリング ルール、クラウドソーシングされたエンドポイントラベルを提供することにより、ネットワーク内の不明なエンドポイントの数を減らすことができます。

詳細については、『[Cisco ISE Administrator Guide, Release 3.2](#)』の「Asset Visibility」の章にある「[Cisco ISE Administrator Guide, Release 3.2](#)」を参照してください。

## OpenAPI を使用した SGT 予約

Cisco ISE 3.2 パッチ 1 以降では、OpenAPI を使用した SGT 予約がサポートされています。詳細については、『[Cisco Identity Services Engine API Reference Guide](#)』を参照してください。

## Cisco ISE リリース 3.2 - 累積パッチ 1 の解決済みの不具合

警告 ID	説明
<a href="#">CSCwd13425</a>	UI からのパッチのインストールが失敗する
<a href="#">CSCwc74531</a>	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
<a href="#">CSCwc80243</a>	リポジトリが選択されていない場合、ISE TCPDUMP が「COPY_REPO_FAILED」状態でスタックする
<a href="#">CSCwc85920</a>	ISE TrustSec ログイン - SGT 作成イベントが ise-psc.log ファイルに記録されない
<a href="#">CSCwc33751</a>	ISE 3.1 の TFTP コピーがタイムアウトする
<a href="#">CSCwc53895</a>	アクティブな PSN がダウンしている場合、ISE 3.1 パッチ 3 SAML SSO が機能しない
<a href="#">CSCwc65802</a>	SAML 構成の保存ボタンがグレー表示される
<a href="#">CSCwc99178</a>	アクティブセッションのアラーム設定で多数の認証プロファイルを追加できない
<a href="#">CSCwd10997</a>	ノードの syncup が、ポータルロールでワイルドカード証明書の複製に失敗する
<a href="#">CSCwc69492</a>	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
<a href="#">CSCwb62192</a>	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

警告 ID	説明
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
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
CSCwb77915	許可されるプロトコルのポリシーに基づいて RSA PSS 暗号の有効/無効を切り替える
CSCvv10712	Sec_txnlog_master テーブルは、レコード数が 200 万を超えたら切り捨てる必要がある
CSCwc62413	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCwc76720	ISE 3.1 での SNMPv3 プライバシーパスワードのエラー
CSCwd35608	ポートバウンス CoA が成功した後も、ISE が reath CoA で古い監査セッション ID を送信している
CSCwc62419	Cisco Identity Services Engine の不十分なアクセス制御の脆弱性
CSCwc44580	ISE 3.1 で IP 10.88.0.1 および 10.88.0.0/16 の IP ルートを持つ cni-podman0 インターフェイスが作成される
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
CSCwc98833	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性
CSCwc98831	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
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
CSCwd13555	ISE がサードパーティの Syslog サーバーからの passive-id セッションの使用を突然停止する
CSCwd32591	[キーペアの生成 (generate key pairs)] をクリックした後、ISE 3.2 SFTP リポジトリが GUI から操作できない
CSCwd51409	ISE は Tenable Security Center のリポジトリとスキャンポリシーを取得できない
CSCwd24304	ISE 3.2 ERS POST /ers/config/networkdevicegroup が破損した属性 othername/type/ndgtype が原因で失敗する
CSCwd03009	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



警告 ID	説明
CSCw81729	フィルタリングによって NAD を削除しようとする時、「すべてのデバイスが正常に削除されました (All devices were successfully deleted)」というメッセージが表示される
CSCwb16640	ISE 3.2 の認証プロファイルで SDA SG-VN-VLAN ユースケースの VLAN 名文字列が保持されない
CSCw42712	ISE RADIUS および PassiveID セッションのマージ
CSCwd15888	ERS API で時刻設定構成のエクスポートにアクセスできない
CSCw15013	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 (Could not get a resource since the pool is exhausted)」エラーを修正する
CSCw87670	SAML が使用されている場合、ISE 3.1 パッチ 3 で csv ファイルからエンドポイントをインポートできない
CSCwa55233	IMS にサードパーティの署名付き証明書を使用している場合の「不明な CA」キューリンクエラー
CSCwd73787	「password」コマンドの後、CLI パスワードの変更が Confd DB に保持されない
CSCwd42311	GUI のダウンロードログから rest-id-store をダウンロードできない
CSCw50392	ROPC AD グループの取得が 53000 以上のグループで機能しない
CSCw50944	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反映されない
CSCw95075	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。
CSCw75572	PPAN アプリケーションサーバーが初期化状態でスタックする
CSCwd22790	ISE 3.2 で SAML サービスプロバイダーの Group Membership 属性を保存できない
CSCwd27506	ISE 3.0 パッチ 6 でスケジュールされたレポートが欠落している
CSCw74206	ISE 3.0 が SCCM MDM サーバーオブジェクトを新しいパスワードとともに保存せず、新しいインスタンスが使用されると機能する
CSCwd31405	Session.PostureStatus のクエリ中に遅延が発生する
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

警告 ID	説明
<a href="#">CSCwc60997</a>	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
<a href="#">CSCwc49580</a>	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
<a href="#">CSCwb26965</a>	REST API を介してネットワーク デバイス グループを作成中にエラーが発生する
<a href="#">CSCwc23593</a>	LSD によって CPU 使用率が高くなる
<a href="#">CSCwc48509</a>	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
<a href="#">CSCwb72948</a>	ISE 3.0 パッチ 4 が登録済みノードのシステム証明書ページにアクセスできない
<a href="#">CSCwc93451</a>	プロファイラは、デフォルトの RADIUS プロンプト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
<a href="#">CSCwc98828</a>	Cisco Identity Services Engine インターフェイス機能の不十分なアクセス制御の脆弱性
<a href="#">CSCwd24089</a>	ISE 3.2 セーフモードが有効になっていない
<a href="#">CSCwd16837</a>	ディレクトリリストが無効になっていると、ISE openAPI HTTP リポジトリパッチのインストールが失敗する
<a href="#">CSCwd31137</a>	SFTP リポジトリへのエクスポート中に ISE のスケジュール RADIUS 認証レポートが失敗する
<a href="#">CSCwc98824</a>	ポスチャ要件はデフォルトエントリのみを表示する
<a href="#">CSCwd30994</a>	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る
<a href="#">CSCwc98823</a>	Cisco Identity Services Engine のコマンドインジェクションの脆弱性
<a href="#">CSCwd41773</a>	5 MB 以上のサイズの CRL が頻繁にダウンロードされると、アプリケーションサーバーがクラッシュする
<a href="#">CSCwc88848</a>	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 3.2 の未解決の不具合：累積パッチ 1

警告 ID	説明
CSCwd79277	同期に最大数の TrustSec オブジェクトが選択されている場合、同期ステータスが失敗と表示される。
CSCwd89797	Meraki コネクタでデバッグログレベルが有効になっている場合に、例外エラーメッセージが表示される。
CSCwd93002	グループを編集し、SAML でアサーションに Name を追加すると、「System Error : Null」が発生する。
CSCwd93209	Meraki コネクタが ISE から削除されても、同期サイクルが終了しない。
CSCwe02315	Meraki コネクタのページレベルのオンラインヘルプを使用できない。
CSCwe01771	変更された [Time] フィールドを使用して作成されたダッシュボード：acs_timestamp がパッチのインストール後に表示されない。
CSCwh92366	3.1 パッチ 8 : 3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。

## Cisco ISE リリース 3.2 - 累積パッチ 1 の既知の制限事項

### パッチのインストール後にカスタムログ分析ダッシュボードが表示されない

Cisco ISE リリース 3.2 で作成されたカスタムログ分析ダッシュボードは、Cisco ISE リリース 3.2 パッチ 1 のインストール後に表示されません。これらのダッシュボードを表示するには、Cisco ISE 3.2 パッチ 1 にアップグレードする前にすべてのカスタムダッシュボードを Kibana から (json ファイルとして) エクスポートし、Cisco ISE 3.2 パッチ 1 のインストール後に MnT ノードにインポートする必要があります。

これらのダッシュボードは、Cisco ISE 3.2 パッチ 1 ノードで Cisco ISE 3.2 の運用バックアップを復元しても表示されません。前述のように、ダッシュボードを Kibana からエクスポートし、パッチのインストール後にインポートする必要があります。

Cisco ISE 3.2 パッチ 1 をインストールした後、次の属性を使用して作成された可視化を含むログ分析ダッシュボードにエラーが表示される場合があります。

- acs\_timestamp
- acsview\_timestamp (TACACS を除くすべてのインデックス用)
- TACACS インデックスの generated\_time
- すべてのインデックスの IP アドレスフィールド

このエラーを修正するには、次の手順を実行します。

- acs\_timestamp を logs\_at\_timezone に置き換える

- acsview\_timestamp を logging\_at に置き換える
- generated\_time を logs\_at\_timezone に置き換える
- ipaddress をテキストフィールドと見なす

## Cisco ISE ソフトウェア ダウンロード サイトでの Cisco ISE 3.2 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 [英語] で Cisco ISE 3.2 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。

### 変更内容

このビルドでは、次のバグが解決されています。

- CSCwd13425 : ISE 3.2 GUI でのパッチのインストールが失敗する。



(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-3.2.0.542a.SPA.x86\_64.iso)。

## Cisco ISE リリース 3.2 の未解決の不具合

次の表に、リリース 3.2 では解決されていない不具合を示します。

警告 ID	説明
<a href="#">CSCwc75986</a>	Cisco ISE リリース 3.2 のエンドポイント デバッグ レポートに「No Data Available」というエラーが表示される。
<a href="#">CSCwb16640</a>	Cisco ISE リリース 3.2 で、認証プロファイルが SDA SG-VN-VLAN ユースケースの VLAN 名文字列で保持されない。
<a href="#">CSCwc54812</a>	負荷が高いため、アップグレードの準備でスレッドダンプが発生する。
<a href="#">CSCwc73330</a>	Cisco ISE リリース 3.2 でユーザーを作成しているときに、内部ユーザーの姓が正しく追加されない。
<a href="#">CSCwc83059</a>	フルアップグレード後、VCS 情報がない。
<a href="#">CSCwc41697</a>	セカンダリ PAN のアップグレード後に Cisco ISE リリース 3.1 パッチ 3 から Cisco ISE リリース 3.2.0.483 にアップグレードすると、PSN でレガシー分割アップグレードが失敗する。
<a href="#">CSCwc74251</a>	PRRT - OCSP チェックの実行時に pxGrid クライアントで応答署名の検証エラーが発生する。
<a href="#">CSCwe99609</a>	タイムゾーンが変更されるたびにタイムスタンプを再調整する必要がある。

警告 ID	説明
<a href="#">CSCwe99666</a>	PSN および MnT ノードでタイムゾーンが変更されると、ライブログとライブセッションのページが誤ったソート順序で表示される。
<a href="#">CSCwe99706</a>	複数の PSN が異なるタイムゾーンにある場合、セッションデータが下部に表示される。
<a href="#">CSCwh18731</a>	アップグレード前に LSD を無効にして Cisco ISE リリース 3.2 にアップグレードすると、EP プロファイラ例外が発生する。
<a href="#">CSCwh36667</a>	Cisco ISE モニタリング GUI ページが「Welcome to Grafana」のままになる。
<a href="#">CSCwh92366</a>	3.1 パッチ 8 : 3.1 パッチ 8 の寿命設定で、不十分な仮想マシンリソースのアラームが発生。

## Cisco ISE リリース 3.2 の解決済みの不具合

Cisco ISE リリース 3.2 で解決済みの不具合は、Cisco ISE パッチリリース (2.7 パッチ 7、3.0 パッチ 6、3.1 パッチ 3) と同等です。

不具合 ID	理由
<a href="#">CSCwd13425</a>	Cisco ISE GUI からのパッチのインストールが失敗する。
<a href="#">CSCvz91603</a>	Cisco ISE を Cisco ISE リリース 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。
<a href="#">CSCvy75191</a>	Cisco ISE XML 外部エンティティ インジェクションの脆弱性。
<a href="#">CSCvz55293</a>	セカンダリ管理 Cisco ISE ノードにより、プライマリ管理ノードでサービスが再起動される。これにより、ドキュメントで不一致が発生する。
<a href="#">CSCvq53373</a>	/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
<a href="#">CSCvz87476</a>	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。
<a href="#">CSCwa12273</a>	ネットワーク管理者グループの AD ユーザーは、管理者ユーザーを作成または編集できない。「Operation is not permitted」というエラーが表示される。
<a href="#">CSCvz66279</a>	7 日以上前の RADIUS レポートが空 (CSCvw78289 の回帰)。
<a href="#">CSCvz37623</a>	NTP ('-') ソースの状態の説明が Cisco ISE CLI にない。
<a href="#">CSCwa25539</a>	Oracle DB での CVE-2021-35599 の脆弱性評価。

不具合 ID	理由
CSCwc12303	インスタンスが使用する PGA メモリがモニタリングノードで PGA_AGGREGATE_LIMIT を超えている。
CSCwc33751	Cisco ISE リリース 3.1 の TFTP コピーがタイムアウトする。
CSCwb29357	Cisco ISE 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
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。
CSCvx48922	TACACS フローのメモリリーク。
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。
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。
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。
CSCwa56934	エンドポイントグループに対する Cisco ISE ERS API の並べ替えが一貫していない。
CSCwb55232	Cisco ISE 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。
CSCwb77915	許可されるプロトコルのポリシーに基づいて RSA PSS 暗号の有効/無効を切り替える。
CSCvz85117	Cisco ISE ヘルスチェックの I/O 帯域幅パフォーマンスチェックで誤ったアラームが発生する。
CSCwb29140	nss rpm が更新された最新のパッチに移行した後、スレッドが枯渇する。
CSCwb59357	Cisco ISE ova ztp がコンテンツの HTTP ダイレクトリスティングを試行する。
CSCvz18848	ロケールのエージェントレスポスタチャが中断する。
CSCwb82814	Cisco ISE リリース 3.1 でネストされた条件の取得時に OpenAPI で 400 エラーが発生する。
CSCwa61347	Cisco ISE-PIC が特殊文字で始まるライブセッションを転送しない。
CSCvz13747	SystemTest : PAN フェールオーバー後に Cisco ISE プライマリ管理ノードの GUI ページが開かない。

不具合 ID	理由
CSCVz66577	SMS Javascript のカスタマイズが SMS 電子メールゲートウェイで機能しない。
CSCVy81435	Cisco 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。
CSCwb23853	古い Cisco ISE リリースから設定の復元を実行すると、Cisco ISE 3.1 パッチ 1 で SAML ID プロバイダーを追加できない。
CSCvy99582	外部 RADIUS サーバーが設定されている場合に、Cisco ISE 2.4 パッチ 13 から Cisco ISE リリース 2.7 へアップグレードすると失敗する。
CSCwa96229	Cisco ISE では、ユーザー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可能。
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。
CSCwa20152	マトリックスが変更されていないスイッチの Cisco ISE 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。
CSCvy94553	TACACS 認証レポートに重複したエントリが表示される。
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。
CSCVz50059	Cisco ISE GC_APP ログがローカルディスクから自動ローテーションしない、または削除されない。
CSCwc99178	アクティブセッションのアラーム設定で多数の認証プロファイルを追加できない。
CSCvu21809	EAP チェーン付きの TEAP (EAP-TLS) で AD ルックアップに設定された CN が使用されない。
CSCVz79665	Microsoft Intune Graph の URL を graph.windows.net/tenant から graph.microsoft.com に変更。
CSCwc39320	CLI 方式によってアップグレードされた Cisco ISE ノードがプライマリ管理ノードの GUI で「Upgrading」の状態でスタックする。
CSCwa35293	Cisco ISE 2.7 : 認証成功設定が成功/成功 URL を示す。
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くなる。
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。

不具合 ID	理由
<a href="#">CSCwc50944</a>	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。
<a href="#">CSCvw58039</a>	Cisco ISE を介してエンドポイントで AC が更新されるとき、Cisco ISE でクライアント プロビジョニングのレポートが表示されない。
<a href="#">CSCwb33727</a>	Cisco ISE 3.1 : 属性の特殊文字がサポートされていない。
<a href="#">CSCwa26210</a>	「GET/ers/config/radiusserversequence」 API の JSON 応答に next page フィールドがない。
<a href="#">CSCwc18751</a>	DomainName\UserName の形式を使用してログインすると、作成されたサポートバンドルを Cisco ISE の GUI からダウンロードできない。
<a href="#">CSCwb24002</a>	Cisco ISE ERS SDK の認証設定が API 呼び出しを介して無効になっていない。
<a href="#">CSCwa88845</a>	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。
<a href="#">CSCvy66496</a>	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できない。
<a href="#">CSCwa94984</a>	長いカスタム属性文字列を使用した Cisco ISE API のユーザー追加操作に、Curl を使用して 4 分かかる
<a href="#">CSCvz44655</a>	Cisco ISE 管理アカウントの選択に関する問題。
<a href="#">CSCwb56878</a>	レプリケーションの停止アラームが Cisco ISE でトリガーされる。
<a href="#">CSCvz77905</a>	Cisco ISE RADIUS のサービス拒否の脆弱性。
<a href="#">CSCwa11653</a>	CIAM : linux-kernel 4.18.0。
<a href="#">CSCwa78479</a>	CVE-2021-4034 Polkit の Cisco Identity Services Engine 評価
<a href="#">CSCwa20354</a>	運用データの消去とデータベース使用率のノード情報が断続的に表示されない。
<a href="#">CSCvv87286</a>	Cisco ISE リリース 2.7 パッチ 2 から Cisco ISE リリース 3.0 への内部 CA およびキーのインポートに失敗する。
<a href="#">CSCvz08813</a>	[Issued Certificates] ページで別のページにスクロールできない。
<a href="#">CSCvz07191</a>	Cisco 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、Cisco ISE GUI がロード中にスタックする。
<a href="#">CSCwb92643</a>	Cisco ISE ADE-OS CLI TCP パラメータが変更失敗し、関連性がなくなる。



不具合 ID	理由
CSCVz28133	ユーザーがサポートバンドルを生成できない。
CSCwa55996	条件スタジオに新しいオブジェクトが存在しない。
CSCwc09435	携帯電話番号フォーマットのエラー処理またはメッセージが明確でない。
CSCvx59893	Cisco ISE の Syslog レベルとメッセージレベルの不一致。
CSCwa16401	Get-By-ID サーバーシーケンスが Cisco ISE 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。
CSCwc40959	ダークモードの Cisco ISE リリース 3.2 では、内部ユーザーの色がわかりにくい。
CSCwc26241	Cisco ISE リリース 3.2 で次のエラーが表示される：「TypeError: Cannot read properties of undefined (reading 'attr')」。
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。
CSCwb01843	DST/TZ は自動的に更新される必要がある。
CSCvx54894	スポンサーポータル管理者が 60 分間または 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。
CSCwb75964	Cisco ISE リリース 3.0：プライマリ管理ノードの自動フェールオーバーアラームを編集できない。
CSCwb32244	Cisco ISE の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。
CSCwa89443	Cisco DNA Center - Cisco ISE 統合：Cisco ISE で pxGrid エンドポイントの古い Cisco DNA Center 証明書が表示される。
CSCVz27791	Cisco 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。
CSCwa14268	Oracle DB での CVE-2021-35619 の脆弱性評価。
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。
CSCvy51210	Cisco ISE リリース 2.7 でネットワーク アクセス デバイスの IP デフォルトラベルを Cisco ISE GUI で削除しようとする、エラーが表示される。
CSCVz37241	キューリンクエラーを警告から重大に移動し、タイムアウトが発生した場合は再起動する。
CSCwa40040	セッションディレクトリの書き込みに失敗する。SQLException：Cisco ISE 3.0 パッチ 4 での文字列データの右側が切り捨てられる。

不具合 ID	理由
<a href="#">CSCvy53842</a>	Cisco ISE で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。
<a href="#">CSCvz01485</a>	Cisco ISE 2.7 パッチ 4 で、ユーザーが 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。
<a href="#">CSCwc23997</a>	Cisco ISE で認証プロファイルと属性詳細に誤った VLAN 割り当て情報が表示される。
<a href="#">CSCwb95433</a>	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。
<a href="#">CSCvz78841</a>	CIAM : openssh 7.6。
<a href="#">CSCvz90468</a>	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。
<a href="#">CSCwa06912</a>	認証ポリシーに日時条件がある TACACS+ 要求で高遅延が発生する。
<a href="#">CSCwb01568</a>	AWS 上の Cisco ISE : 運用 DB が大きな OS ディスクに基づいて適切にサイジングされない。
<a href="#">CSCvy76328</a>	[Network device] タブの [duplicate] オプションを使用すると、IPV6 の [Subnet] が /128 に変更される。
<a href="#">CSCvz56358</a>	Cisco ISE リリース 3.0 で最初の SAN エントリのみがチェックされる。
<a href="#">CSCwc85920</a>	Cisco 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。
<a href="#">CSCwc61320</a>	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。
<a href="#">CSCvw93570</a>	Cisco ISE リリース 2.4 パッチ 8 でゲストポータルを編集、複製、削除できない。
<a href="#">CSCwa20309</a>	不明な 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というアラーム。
<a href="#">CSCwc21890</a>	専用モニタリングノードを使用する Cisco ISE でパッシブ Easy Connect が機能しない。
<a href="#">CSCwb29498</a>	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。
<a href="#">CSCwc69492</a>	Cisco ISE 3.1 : メタスペースを使い果たすと Cisco ISE ノードでクラッシュが発生する。

不具合 ID	理由
CSCwb48707	[Endpoint Purge] タブを読み込めない。
CSCvz44488	同じローカルユーザーが存在する場合、Cisco ISE 3.0 エージェントレスポスチャでドメイン認証が使用されない。
CSCvt25277	Cisco ISE 2.4 パッチ 12 のインストールが停止する。
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。
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。
CSCwa37040	Cisco 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。
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。
CSCvs95495	Aruba サードパーティデバイスでの再認証の問題。
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。
CSCvz49871	Cisco ISE GUI : net::ERR_ABORTED 404: /admin/ng/nls/fr-fr/。
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。
CSCwc44580	Cisco ISE 3.1 で IP 10.88.0.1 および 10.88.0.0/16 の IP ルートを持つ cni-podman0 インターフェイスが作成される。
CSCvx23375	編集または保存中に Cisco ISE 認証プロファイルオプションが切り捨てられる（Google Chrome のみ）。
CSCwb41741	Cisco ISE : 管理者グループの無効な文字エラー。
CSCwb27857	Cisco ISE リリース 3.0 パッチ 5 : 分散型展開で RSA 2FA を使用して MnT ノードの Cisco ISE GUI にログインできない。
CSCwa09060	Cisco ISE 3.1 パッチ 1 の CSR によってバインドされた外部署名済みシステム証明書にロールを割り当てることができない。
CSCvz72225	ディスカバリホストに FQDN を追加すると、ディスカバリホストの IP アドレスまたはホスト名が無効になる。
CSCwa13696	Cisco ISE リリース 3.1 ゲストのユーザー名またはパスワードポリシーを変更できない。

不具合 ID	理由
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。
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。
CSCwb52396	Cisco ISE PRA フェールオーバー。
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。
CSCvz77482	Cisco ISE リリース 3.0 はゲストの自己登録ポータルの一部として「location」設定を選択解除できない。
CSCwb59170	Cisco ISE リリース 3.1 SHA-2 オプションが REST API での NAD 作成に使用できない。
CSCwc62415	Cisco Identity Services Engine の不正ファイルアクセスの脆弱性。
CSCwc76720	Cisco ISE リリース 3.1 のみでの SNMPv3 プライバシーパスワードのエラー。
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。
CSCwb35304	Cisco ISE リリース 3.1 : 競合状態が原因で登録/同期が失敗する。
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。
CSCvz57222	Cisco ISE リリース 3.0 : セカンダリインターフェイス GigabitEthernet 1 および Bond 1 で Cisco ISE GUI に管理アクセスが許可される。
CSCwb52092	Cisco ISE リリース 3.1 の AWS Cloud Formation スタックが非常に強力な管理者パスワードで失敗する。
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。
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「error loading page」が表示される。
CSCvi35653	Cisco ISE と AnyConnect Cisco ISE ポスチャ間の双方向通信/UDP ハートビート。
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)。
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。
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。

不具合 ID	理由
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。
CSCwa25731	レポートで過去 7 日間のフィルタが機能しない。
CSCwb97579	Hyper-V Gen-2 との Cisco ISE リリース 3.1 の互換性の問題。
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 Cisco ISE リリース 3.0 で保存されない。
CSCvy33393	Cisco ISE 3.1 BH のコンテキストの可視性でユーザー名に \ が表示されるが、ライブログでは正しい単一の \ が表示される。
CSCwb26965	Cisco ISE リリース 3.1 : REST API を介してネットワークデバイス グループを作成中にエラーが発生する
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	Cisco ISE リリース 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。
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 Cisco ISE リリース 3.1 で機能しない。
CSCvz73445	エージェントレスポスタチャがマルウェア対策チェックに合格しない。
CSCvz63643	Cisco ISE リリース 2.7 : EndpointPersister スレッドが停止する。
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。
CSCwa17470	グループクレームに 2 つ以上のグループがある場合、アクセスが拒否され、Cisco ISE リリース 3.1 SAML 管理認証が失敗する。
CSCwa49859	属性値 dc-opaque がライブログの問題を引き起こす
CSCvz72034	Cisco ISE リリース 3.1 : Cisco DNA Center からネットワークデバイスを更新している間、共有秘密/パスワードが空であるかマスクされている。
CSCvz83204	Cisco ISE でポスタ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。
CSCwc53577	親ユーザー ID グループを CSV ファイル経由で作成できる。
CSCwb71505	Cisco ISE リリース 3.1 : ACE ライブラリのエラーにより、アプリケーションサーバーが初期化状態でスタックする。
CSCvz74457	Cisco ISE 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または更新が許可されていない。

不具合 ID	理由
<a href="#">CSCwc07283</a>	Cisco ISE リリース 3.1 で [Context visibility endpoint authentication] タブにデータが表示されない。
<a href="#">CSCvy94427</a>	Cisco ISE リリース 2.7 で EAP チェーンのポスチャリースが中断する。
<a href="#">CSCvy71690</a>	ゲストポータルの [Customer] フィールドに & - \$ # が含まれる。
<a href="#">CSCwa95889</a>	Cisco ISE : 新しいホストキーアルゴリズムを使用したホストへの SSH/SFTP (rsa-sha2-512 など) 。
<a href="#">CSCvy91805</a>	Cisco ISE の EAP-FAST-Chaining で最大セッション数が適用されない。
<a href="#">CSCwd05697</a>	ゲストロケーションが Cisco ISE ゲストポータルにロードされない。
<a href="#">CSCwc88848</a>	Cisco ISE リリース 3.1 パッチ 1 で Rest ID/ROPC フォルダログが作成されない。
<a href="#">CSCvy69539</a>	CIAM : openjdk - 複数のバージョン。
<a href="#">CSCwb34910</a>	Cisco ISE ポータルでのゲスト SMS 通知の複数行の問題。
<a href="#">CSCvy92536</a>	Cisco ISE リリース 3.0 : デバイス管理ライセンスだけで、[Administration] > [System] > [Logging] メニューへのアクセスが許可される必要がある。
<a href="#">CSCwb02129</a>	手動でインポートした SSH 公開キーで Cisco ISE への SSH が失敗する。
<a href="#">CSCwb32466</a>	Cisco ISE リリース 3.1 : 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。
<a href="#">CSCvy86859</a>	Mac OS Beta Monterey (MacOS 12 beta 2) で NSP MacOSXSPWizard v3.1.0.2 に失敗する。
<a href="#">CSCwa04454</a>	Cisco ISE リリース 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 必須メニューへのアクセスが許可される必要がある。
<a href="#">CSCwc08484</a>	TAC ケースのオープンを無効にすると、Cisco ISE サービスの再起動時に Cisco ISE 完全性チェックが失敗する。
<a href="#">CSCvz07823</a>	Cisco ISE リリース 2.7 でエンドポイントをグループに追加できない。
<a href="#">CSCwc49580</a>	ANCCoA 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。
<a href="#">CSCwc87670</a>	SAML が使用されている場合、Cisco ISE リリース 3.1 パッチ 3 で csv ファイルからエンドポイントをインポートできない。
<a href="#">CSCwd31405</a>	Session.PostureStatus のクエリ中に遅延が発生する。
<a href="#">CSCwb30941</a>	CVE-2022-0778 - Cisco ISE リリース 3.1 以降が影響を受ける。

不具合 ID	理由
CSCwb85456	CIAM : OpenSSL を 1.0.2ze および 1.1.1o にアップグレード。
CSCwc65802	SAML 構成の保存ボタンがグレー表示される。
CSCvy84989	POST /ers/config/internaluser/ の Cookie を有効にすると、「Identity Group(s) does not exist」というエラーが発生する。
CSCwc12693	Cisco ISE ERS 検証エラー - 必須フィールドがありません : [validDays]。
CSCvz33839	メニューアクセスのカスタマイズが機能していない。
CSCwb91392	サードパーティの CA 証明書が管理者用に使用されている場合、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。
CSCvz75902	Cisco ISE 内部 CA の生成時に Cisco ISE が pxGrid 証明書を置き換える。
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。
CSCvu94544	Cisco 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。
CSCwc09104	認証 VLAN を使用したゲストリダイレクトが Cisco ISE リリース 3.1 で機能しなくなった。
CSCvz17020	Cisco 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。
CSCwa45316	Cisco ISE リリース 3.1 で vpn ユーザーの MDM intune 統合が中断する。
CSCwd10840	Cisco ISE CLI がスタックする。
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。
CSCvz63405	Cisco ISE クライアントの pxGrid 証明書が Cisco DNA Center に配信されない。
CSCwb75093	CIAM : linux-kernel 4.18.0
CSCvy92040	[Cisco 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。
CSCvz72208	Cisco ISE リリース 3.1 : [Authentication] タブで、[Context Visibility] に空白の結果が表示される。
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。
CSCwa79799	sysodbcini ファイルに PermSize 属性がない。

不具合 ID	理由
CSCvn27270	Cisco ISE : 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。
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。
CSCwc59570	Cisco ISE が SXP バージョン 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。
CSCwa67433	Cisco 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。
CSCwc24126	プロファイラ条件で属性値が表示されない。
CSCwa97357	Cisco ISE が SMTP API 本文で「mobilenumber」値を送信しない。
CSCvz61191	Cisco ISE リリース 3.1 : 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 [choose file] をクリックしても応答がない。
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 Cisco ISE ポリシーサービスノードがクラッシュする。
CSCwb11147	VN 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。
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で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。
CSCwc81729	フィルタ処理で特定の 1 つの NAD を削除しようとする、「All devices were successfully deleted」と表示される。
CSCvz20851	Cisco Identity Services Engine の機密情報の開示における脆弱性。
CSCvu94025	Cisco 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。
CSCvz71284	SNMPv3 COA 要求が Cisco ISE リリース 2.7 によって発行されない。
CSCwa90930	RMQ にハード Q キャップが必要。
CSCvx85675	Cisco 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。
CSCwb04898	名前にスペースを含む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 Cisco ISE 評価。



不具合 ID	理由
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。
CSCvz94133	「EDF_DB_LOG」が原因で構成バックアップが失敗する。
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。
CSCwa51150	Cisco ISE 3.1 で WLC が EAPOL キー M2 を検証できない。
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。
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	Cisco ISE 条件スタジオ : [Identity Groups] ドロップダウンを 1000 個に制限。
CSCwb91645	Cisco ISE 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。
CSCvz34849	DELETE /ers/config/networkdevicegroup/{id} が機能しない、CRUD の例外。
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。
CSCwb38069	Cisco ISE リリース 3.1 : 古い Cisco ISE リリース 2.6 からのバックアップの復元後、サービスを開始できない。
CSCvy16894	一部の記号を使用すると、認証プロファイルでエラーが発生する。
CSCwa13877	Cisco ISE スマートライセンス認証更新の失敗 : 詳細 = ライセンスクラウドからの無効な応答。
CSCwa76896	RADIUS 認証レポートの「Failure Reasons」列が重複する。
CSCwa47133	Cisco ISE 評価 log4j CVE-2021-44228。
CSCvy66598	MAB 認証の場合は MAR 機能を無視する必要がある。
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。
CSCwc05718	Cisco ISE デバッグウィザードのポスチャプロファイルに、デバッグするための client-webapp コンポーネントが含まれていない。
CSCwb05532	「場所」と「デバイスタイプ」の場所が、[Network Devices] > [Add] をクリックするたびに交換される。

不具合 ID	理由
CSCwb22662	64 文字の制限は、ユーザープリンシパル名などの外部ユーザー ID に対応するには小さすぎる。
CSCvz83753	AuthZ 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。
CSCwa75348	ODBC 動作のフェールオーバーの問題。
CSCwb81416	Cisco ISE リリース 3.1 GUI がログイン後にロードしない。
CSCwb40349	Cisco ISE 3.X : 外部 RADIUS トークン共有秘密の無効な文字。
CSCvz67073	Cisco Identity Services Engine の認証バイパスの脆弱性。
CSCwb62192	CiscoISE 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。
CSCwb01854	Cisco ISE リリース 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。
CSCvz05704	ディスクサイズが 1TB を超える Cisco ISE のプラットフォームチェックが失敗する。
CSCwa43187	Cisco ISE キューリンクエラー : Message=From Node1 To Node2, Cause=Timeout in NAT'ed deployment。
CSCwb47255	サポートされる HTTP メソッドが表示される。
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、認証の遅延が発生する。
CSCwb86283	CiscoISE 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 をスローする。
CSCwa19573	SSL 監査イベントが原因で Catalina.out ファイルが巨大化する。
CSCwb82469	Windows 11 Pro for Workstations は最新のポストチャフィード更新では実際にはまだサポートされていない。
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。
CSCvz55258	Cisco:cisco-av-pair AuthZ 条件の機能が停止した。
CSCwa52110	ネットワークデバイスに設定された SNMP 構成で SNMP レコードの処理中に 20 秒の遅延が発生する。
CSCvz00659	バナーで特殊文字を使用すると、SFTP リポジトリがブロックされる。

不具合 ID	理由
CSCwvc65711	MAC - CSC 5.0554 ウェブ展開パッケージが [ISE]>[CP]>[resources] [100MB] へのアップロードに失敗する。
CSCvz45150	Cisco ISE リリース 3.1 が従来のライセンスを要求する。
CSCwvc27765	SYS_EXPORT_SCHEMA_01 が原因で Cisco ISE 設定のバックアップが失敗する。
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	Cisco ISE リリース 3.1 : Active Directory のネットワーク管理者で pxGrid 証明書を生成できない。
CSCwb57675	[Dedicated MnT] オプションを有効にすると、Cisco ISE 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、Cisco ISE リリース 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。
CSCwa04370	Cisco ISE リリース 3.1 : 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。
CSCwa32814	15 のコレクションフィルタが設定された Cisco ISE で 15 番目のフィルタが非表示になる。
CSCwa60873	プライマリ管理ノード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。
CSCwvc42712	Cisco ISE RADIUS および PassiveID セッションのマージ。
CSCvz46560	jquery v1.10.2 を使用する Cisco ISE が脆弱になっている。
CSCwvc53895	Cisco ISE リリース 3.1 パッチ 3 で、アクティブなポリシーサービスノードがダウンした場合、SAML SSO は機能しない。
CSCvz79518	有用性 : 「DNS Resolution Failure」アラームで Cisco ISE サーバーを表示する必要がある
CSCvz08319	EAP TLS のバッファ長が 0 であるため、Cisco ISE のアプリケーションサーバー プロセスが Dot1X 時に再起動する。
CSCwa08484	セッションに IPv4 アドレスと IPv6 アドレスの両方がある場合に、IPv4 マッピングがない
CSCwb23028	パスワードの不正確なディクショナリの単語評価。

不具合 ID	理由
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。
CSCvz38266	Okta と同じ FQDN で動作する ADFS SAML ログイン。
CSCwd10997	ノードの syncup が、ポータルロールでワイルドカード証明書の複製に失敗する。
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。
CSCvy96761	EAP チェーンフローを実行して関連する ID を処理する際に、セッションキャッシュを更新する必要がある。
CSCvy69900	CIAM : linux-kernel 4.18.0。
CSCwa37580	Cisco ISE リリース 3.0 の 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る。
CSCwb00530	Android VPN と InTune MDM の統合が Cisco ISE リリース 3.1 で機能しない。
CSCvx85064	スポンサーゲストによるパスワードのセルフリセット時に SMS コンテンツを変更できるようにする。
CSCwa16291	ゲストポータルのボタンのテキスト要素により、Apple VoiceOver の単語が繰り返される。
CSCwa03126	一部の言語で Cisco ISE CPP が正しくロードされない。
CSCwa36350	ホットパッチ API の詳細に空白のタイムスタンプがある。
CSCvz90852	CNA のホットスポットゲストポータルで [Success] が空白であり、iDevice で [Done] に切り替わらない。
CSCwc57939	Cisco ISE が大規模な VM をサポート対象外として検出する。
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
CSCvz92898	管理者ログイン時の SCM js ファイルのブラウザダウンロード。
CSCwa05404	「Stale Sessions observed for Tacacs Could not find selected service (TACACS で確認された古いセッションで選択したサービスが見つかりませんでした)」というエラー。
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 が発生する。

不具合 ID	理由
CSCVz72069	pxGrid が Cisco ISE-PIC の [Summary] ページで無効と表示される。
CSCwd13555	Cisco ISE がサードパーティの syslog サーバーからの passive-id セッションの使用を突然停止する。
CSCVz95326	Cisco ISE で ACI 統合を有効にしようとする、複数の ACI IP アドレスまたはホスト名を追加できなくなる。
CSCwa08018	Cisco ISE リリース 3.1 : IPV6 がグローバルに無効になっている場合、Cisco ISE GUI が機能しない。
CSCvy76622	SystemTest : 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。
CSCwb03479	hotpatch.log をサポートバンドルに含める必要がある。
CSCvv43120	Cisco ISE 2.x : 接続に関する Intune MDM アラーム    401 Unauthorized (401 未承認)。
CSCwb84440	エンドポイントグループの削除後にスポンサーポータルが中断する
CSCwa00729	1 つの特定の NAD を削除すると、すべての NAD が削除される。
CSCwa82247	Cisco ISE キューリンクエラー : Cisco ISE IPtables の 169.254.2.0/25 による Cause=Timeout。
CSCwb39964	Cisco 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 Cisco ISE GUI にログインできる。
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] > [Identities] で機能しない。
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	[connector settings] ページが開くと、REST ID がクラウドからグループを取得する。
CSCwa56771	Cisco ISE リリース 3.0 パッチ 2 : [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。
CSCwa60903	ISE で、CRL の nextUpdate の日付に 6 時間追加される
CSCwa41166	T+ コマンドの安全でない文字が 16 進数の文字参照に格納される。
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。
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

不具合 ID	理由
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。
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
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。
CSCvz57267	SAN フィールド FQDN にもかかわらず、プライマリ管理ノードに対して発行された Cisco ISE 証明書を他のノードにインポートできない。
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。
CSCwc51219	RADIUS 共有秘密の先頭に += 文字がある場合、CSVNAD インポートが拒否される。
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。
CSCwb02346	Cisco Identity Services Engine の機密情報の開示における脆弱性。
CSCvy43246	ユーザーがポータルで作成手順でゲスト SSID を作成できない : Cisco ISE がビジーというエラーが表示される。
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。
CSCvz86020	「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。
CSCwa95892	間違った期間を示す \$ui_time_left\$ 変数
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。
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。
CSCwc60997	Cisco ISE : Cisco 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。
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
CSCwa11633	Cisco ISE リリース 3.0 : APIC 統合 : secGroup を作成できない。
CSCwb32492	プライマリ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。

不具合 ID	理由
<a href="#">CSCwc00162</a>	クライアント/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ログインが機能しない。
<a href="#">CSCwb79056</a>	Cisco ISE リリース 3.1 ERS コール <code>/ers/config/sgmapping/{id}</code> がカスタム SGT の SGT 値を返さない。
<a href="#">CSCwc62413</a>	Cisco Identity Services Engine クロスサイト スクリプティングの脆弱性。
<a href="#">CSCvv02086</a>	Cisco 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。
<a href="#">CSCvy94818</a>	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。
<a href="#">CSCvz35550</a>	Cisco ISE ヘルスチェック MDM 検証の誤ったアラーム。
<a href="#">CSCwc03220</a>	Cisco 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。
<a href="#">CSCwc30811</a>	ゲストポータルでアンダースコアが脆弱である。
<a href="#">CSCvz05966</a>	Cisco ISE リリース 2.6 パッチ 9 で、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。
<a href="#">CSCwc30643</a>	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。
<a href="#">CSCwa47221</a>	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。
<a href="#">CSCwa59621</a>	ID グループに対する Cisco ISE ERS API の並べ替えが一貫していない。

## その他の参考資料

Cisco ISE を使用するときには活用できるその他のリソースについては、『[Cisco ISE End-User Resources](#)』を参照してください。

## 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](#) [英語] 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、[Cisco Support](#) [英語] 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 DevNet](#) にアクセスしてください。
- 一般的なネットワーク、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。

## シスコバグ検索ツール

[シスコバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

## マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



---

【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/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご承ください。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。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

## 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。