新機能および変更された機能に関する情報

新機能および変更された機能に関する情報

次の表に、新機能および変更された機能の要約と参照先を示します。

表 *1 : Cisco ISE* リリース *3.3* の新機能および変更された機能

機能	説明
Cisco ISE リリース 3.3 パッチ 1	
多要素認証のための Cisco Duo の統合	Cisco ISE リリース 3.3 パッチ 1 以降では、多要素認証（MFA）ワークフローの外部 ID ソースとして Cisco Duo を直接統合できます。Cisco ISE の以前のリリースでは、Cisco Duo は外部 RADIUS プロキシサーバーとしてサポートされていましたが、この設定は引き続きサポートされます。 この Cisco Duo 統合では、次の多要素認証のユースケースがサポートされています。 **1.** VPN ユーザー認証 **2.** TACACS+ 管理者アクセス認証 多要素認証のための Cisco Duo と Cisco ISE の統合を参照してください。

新機能および変更された機能に関する情報

機能	説明
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に実施することで、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。 カスタマー エクスペリエンス アンケートを参照してください
Cisco ISE リリース 3.3	
エージェントレスポスチャへの IPv6 サポート	Cisco ISE リリース 3.3 では、エージェントレスポスチャへの IPv6 サポートが追加されています。Windows クライアントと Mac クライアントが現在サポートされています。 エージェントレスポスチャを参照してください。
特定の暗号方式を無効にするオプション	次の Cisco ISE コンポーネント（管理 UI、ERS、OpenAPI、セキュア ODBC、ポータル、および pxGrid）との通信用暗号方式を手動で設定する場合は、[Security Settings] ウィンドウの [Manually Configure Ciphers List] チェックボックスをオンにします。 許可された暗号方式がすでに選択された状態で暗号方式リストが表示されます。たとえば、[SHA1暗号方式を許可（Allow SHA1 Ciphers）] オプションが有効になっている場合、このリストの SHA1 暗号方式が有効になります。[Allow Only TLS_RSA_With_AES_128_CBC_SHA] オプションが選択されている場合、この SHA1 暗号方式のみがこのリストで有効になります。[Allow SHA1 Ciphers] オプションが無効になっている場合、このリストの SHA1 暗号方式はどれも有効ではありません。必要に応じて暗号方式を選択したり、選択解除したりできます。 「セキュリティ設定の構成」を参照してください。

新機能および変更された機能に関する情報

機能	説明
ナビゲーションの改善	Cisco ISE ホームページ GUI は、ユーザー体験を向上させるために変更されました。ホームページの左隅にあるメニューアイコンをクリックすると、ペインが表示されます。ペインの各オプションにカーソルを合わせると、次のような選択可能なサブメニューが表示されます。 • **コンテキストの可視性（Context Visibility）** • **動作** • **ポリシー** • **管理（Administration）** • **Work Centers** ホームページで [ダッシュボード（Dashboard）] をクリックします。 左ペインには、最近表示したページを保存できる [ブックマーク（Bookmarks）] タブもあります。メニューアイコンを再度クリックすると、ペインが非表示になります。 左ペインが表示されているときにログアウトし、再度ログインすると、ペインは引き続き表示されます。ただし、ペインが非表示になった後にログアウトし、再度ログインした場合、ペインを再度表示するには、メニューアイコンをクリックする必要があります。 ホームページの アイコンを使用して [Search Pages] オプションにアクセスし、新しいページを検索したり、最近検索したページにアクセスしたりできるようになりました。 基本的なセットアップを参照してください。
多要素分類による拡張エンドポイントの可視化	ネットワークに接続しているエンドポイントからの 4 つの特定の属性を使用して、微妙な差異のある許可ポリシーを作成できるようになりました。多要素分類（MFC）プロファイラは、さまざまなプロファイリングプローブを使用して、Cisco ISE 認証ポリシー作成ワークフローに 4 つの新しいエンドポイント属性（MFC エンドポイントタイプ、MFC ハードウェアメーカー、MFC ハードウェアモデル、MFC オペレーティングシステム）を取り込みます。 多要素分類による拡張エンドポイントの可視化を参照してください。

新機能および変更された機能に関する情報

機能	説明
エンドポイント プロファイリングのための Cisco AI-ML ルール提案	Cisco ISE は、ネットワークからの継続的な学習に基づいてプロファイリングの提案を行い、エンドポイントプロファイリングと管理を強化するのに役立ちます。このような提案を使用して、ネットワーク内の不明なエンドポイントやプロファイリングされていないエンドポイントの数を減らすことができます。 エンドポイント プロファイリングのための Cisco AI-ML ルール提案を参照してください。
ARM64 バージョンのエージェントへのポスチャおよびクライアント プロビジョニングのサポート	Cisco ISE リリース 3.3 から、ポスチャポリシーとクライアントプロビジョニング ポリシーは ARM64 エンドポイントでサポートされます。ARM64 エンドポイント用の ARM64 バージョンのエージェントをアップロードできます。 ARM64 バージョンのエージェントに対するクライアントプロビジョニング ポリシーの設定を参照してください。
RADIUS ステップ遅延ダッシュボード	[RADIUS Step Latency] ダッシュボード（[Analytics] > [Dashboard]）には、指定された期間の RADIUS 認証フローステップの最大遅延と平均遅延が表示されます。また、Active Directory 認証フローステップ（Active Directory がそのノードで設定されている場合）の最大遅延および平均遅延、および最大遅延または平均遅延のうち上位 N 個の RADIUS 認証手順を表示することもできます。 Log Analytics を参照してください。
管理証明書更新後のアプリケーション再起動のスケジュール設定	プライマリ PAN で管理証明書を更新した後、展開内のすべてのノードを再起動する必要があります。各ノードをすぐに再起動することも、後での再起動をスケジュールすることもできます。この機能を使用すると、実行中のプロセスが自動再起動によって中断されないようにすることができ、プロセスをより詳細に制御できます。証明書の更新から 15 日以内にノードの再起動をスケジュールする必要があります。 管理証明書更新後のアプリケーション再起動のスケジュール設定を参照してください。

新機能および変更された機能に関する情報

機能	説明
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 3.3 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 3.3 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。 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。 Cisco pxGrid Direct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。 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を参照してください
TLS 1.3 を使用した Cisco ISE 管理 GUI へのアクセス	Cisco ISE リリース 3.3 からは、TLS 1.3 バージョンを使用して Cisco ISE 管理 GUI にアクセスできます。 「セキュリティ設定の構成」を参照してください。
Cisco ISE でのネイティブ IPSec の設定	Cisco ISE リリース 3.3 からは、ネイティブ IPSec 設定を使用して IPSec を設定できます。IKEv1 および IKEv2 プロトコルを使用して、IPSec トンネルを介した Cisco ISE PSN と NAD 間のセキュリティ アソシエーションを確立するためにネイティブ IPSec を使用できます。ネイティブ IPSec の設定により、Cisco ISE は FIPS 140-3 に準拠します。 Cisco ISE でのネイティブ IPSec の設定を参照してください。
Cisco ISE 展開内のすべてのノードに対するエンドポイント複製の無効化	Cisco ISE リリース 3.3 から、動的に検出されたエンドポイントは、Cisco ISE 展開内のすべてのノードに自動的に複製されません。Cisco ISE 展開内のすべてのノードで動的に検出されたエンドポイントの複製は、有効または無効にするかを選択できるようになっています。 プライマリ Cisco ISE ノードからセカンダリ Cisco ISE ノードへのデータレプリケーションを参照してください。
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 3.3 から、[ダイナミック（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 アイデンティティ グループに割り当てることができます。 「ゲスト タイプの作成または編集」を参照してください。

新機能および変更された機能に関する情報

機能	説明
Cisco ISE ユーザーのパスワードの管理	Cisco ISE リリース 3.3 から、Cisco ISE の内部ユーザーとして、[ネットワークアクセスユーザー（Network Access Users）] ウィンドウの [ネットワークアクセスユーザー（Network Access User）] テーブルに [作成日（Date Created）] 列と [変更日（Date Modified）] 列を追加するか選択できます。 Cisco ISE ユーザー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。 Cisco Meraki ダッシュボードと Cisco ISE の接続を参照してください。
Data Connect	Cisco ISE リリース 3.3 から、Data Connect 機能は、管理者証明書を使用し、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 へのデータベース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。 「Data Connect」を参照してください。

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