Cisco DNA Centerリリース 2.3.4.x リリースノート

初版：2022 年 9 月 21 日

最終更新：2023 年 2 月 17 日

Cisco DNA Center リリース 2.3.4.x リリースノート

Cisco DNA Center 2.3.4.x は段階的なロールアウトで利用できます。シスコの営業担当者に連絡して、このリリースをリクエストしてください。

このドキュメントでは、Cisco DNA Center リリース 2.3.4.x の機能、制限事項、およびバグについて説明します。

このリリースのすべてのガイドへのリンクは、Cisco DNA Center 2.3.4 Documentation [英語] を参照してください。

変更履歴

次の表に、このドキュメントの最初のリリース以降の変更点を示します。

表 *1*: マニュアルの変更履歴

日付	変更内容	参照先
2023 年 2 月 17 日	In-Service Software Upgrade（ISSU）に関する制限を追加しました。	制限事項と制約事項 （25 ページ）
2022-12-14	Cisco DNA Center 2.3.4.3 のパッケージのリストを追加しました。	Cisco DNA Center リリース 2.3.4.x のパッケージバージョン （2 ページ）
	2.3.4.3 の「解決済みのバグ」の表を追加しました。	解決済みのバグ （21 ページ）
	未解決のバグ CSCwc17228 を追加しました。	未解決のバグ （19 ページ）
2022-09-21	初回リリース	—

最新の Cisco DNA Center リリースへのアップグレード

Cisco DNA Center の現在のリリースへのアップグレードの詳細については、『*Cisco DNA Center Upgrade Guide*』 [英語] を参照してください。

アップグレードする前に、Audit & Upgrade Readiness Analyzer（AURA）の事前チェックを実行します。AURA は、Cisco DNA Center とファブリックネットワークの正常性、スケーリング、アップグレードの準備状況チェックを実行するコマンドラインツールです。詳細については、『Enhanced Visibility into Cisco DNA Center Using AURA』[英語] を参照してください。

Cisco DNA Center リリース 2.3.4.x のパッケージバージョン

パッケージ名	リリース 2.3.4.3	リリース 2.3.4.0
リリースビルドバージョン		
リリースバージョン	2.3.4.3.70172	2.3.4.0.70523
システムアップデート		
システム	1.7.808	1.7.774
システム共通	2.1.563.60229	2.1.560.60835
パッケージの更新		
アクセス制御アプリケーション	2.1.563.60229	2.1.560.60835
AI エンドポイント分析	1.8.576	1.8.525
AI ネットワーク分析	2.10.16.314	2.10.10.294
アプリケーション ホスティング	2.0.02209080642	2.0.02205161126
アプリケーションポリシー	2.1.563.170211	2.1.560.117594
アプリケーションレジストリ	2.1.563.170211	2.1.560.117594
アプリケーション可視性サービス	2.1.563.170211	2.1.560.117594
アシュアランス - 基本	2.3.4.336	2.3.4.277
アシュアランス - センサー	2.3.4.333	2.3.4.217
自動化 - 基本	2.1.563.60229	2.1.560.60835
自動化 - インテリジェントキャプチャ	2.1.563.60229	2.1.560.60835
自動化 - センサー	2.1.563.60229	2.1.560.60835
Cisco DNA Center グローバル検索	1.9.1.6	1.9.1.6
Cisco DNA Center プラットフォーム	1.9.1.90	1.9.1.78
Cisco DNA Center UI	1.7.2.312	1.7.2.306
Cisco Identity Services Engine	2.1.563.1018	2.1.560.451

パッケージ名	リリース 2.3.4.3	リリース 2.3.4.0
Cisco Umbrella	2.1.563.590131	2.1.560.590253
クラウド接続 - コンテキストコンテンツ	2.5.1.345	2.5.1.345
クラウド接続 - データハブ	1.9.47	1.9.38
クラウド接続 - テザリング	2.30.1.72	2.30.1.72
クラウド デバイス プロビジョニング アプリケーション	2.1.563.60229	2.1.560.60835
コマンドランナー	2.1.563.60229	2.1.560.60835
デバイスのオンボーディング	2.1.563.60229	2.1.560.60835
ディザスタ リカバリ	2.1.563.360021	2.1.560.360043
ディザスタリカバリ ー 監視サイト	2.1.563.370016	2.1.560.370025
グループベースポリシーの分析	2.3.4.17	2.3.4.17
イメージ管理	2.1.563.60229	2.1.560.60835
機械推論	2.1.563.210158	2.1.560.210319
NCP - 基本	2.1.563.60229	2.1.560.60835
NCP - サービス	2.1.563.60229	2.1.560.60835
ネットワーク コントローラ プラットフォーム	2.1.563.60229	2.1.560.60835
ネットワーク データ プラットフォーム - 基本分析	1.9.134	1.9.96
ネットワーク データ プラットフォーム - コア	1.9.212	1.9.175
ネットワーク データ プラットフォーム - マネージャ	1.9.59	1.9.59
ネットワーク エクスペリエンス プラットフォーム - コア	2.1.563.60229	2.1.560.60835
[Path Trace]	2.1.563.60229	2.1.560.60835
RBAC 拡張	2.1.563.1900001	2.1.560.1900006
不正および aWIPS	2.6.0.37	2.6.0.36
SD-Access	2.1.563.60229	2.1.560.60835
Stealthwatch セキュリティ分析	2.1.563.1090110	2.1.560.1090244
サポート サービス	2.1.563.880007	2.1.560.880041

パッケージ名	リリース 2.3.4.3	リリース 2.3.4.0
Wide Area Bonjour	2.4.563.75063	2.4.560.75194

新機能および変更された機能に関する情報

Cisco DNA Center の新機能および変更された機能

機能	説明
NBAR クラウドコネクタの設定	プロトコルパックの自動更新を有効にできるようになりました。
EoX スキャンの開始	[Inventory] ウィンドウから EoX スキャンを開始できます。
証明書失効確認	証明書失効の状態を確認を設定できます。
2D ワイヤレスマップへの吹き抜け（アトリウム）の追加	吹き抜け（アトリウムとも呼ばれます）を 2D マップに追加できます。
ワイヤレスカバレッジオプティマイザ	ワイヤレスカバレッジが SLA を満たしていない場合に、オプティマイザツールを実行できます。このツールは、移動および追加の準備ができている AP の最大数を入力として受け取り、ワイヤレスカバレッジが最大化される構成を計算します。
アプリケーションとエンドポイントの可視性の無効化	アプリケーションとエンドポイントの可視性はデフォルトで有効になっています。この設定は無効にできます。
ワイヤレスマップ GUI の機能強化	GUI の堅牢性と一貫性を高めるために、マイナーな機能強化が実装されました。たとえば、ワイヤレスマップから要素（センサー、壁など）を削除した場合、その要素はマップから取り除かれるだけです。Cisco DNA Center からは削除されません。このアクションをより正確に表すために、GUI の用語が [Delete] から [Remove] に変更されました。
非ファブリックデバイスの Resilient Ethernet Protocol（REP）リング	非ファブリックデバイスの REP リングを設定できます。
ポート利用情報	デバイスポートの場合、デバイスの [Details] ウィンドウで、最後に受信した入力と最後に送信した出力のタイムスタンプを確認できます。
セキュアトンネルの作成	ブランチロケーションの新しいエッジデバイスへアクセスできる、自動化された、セキュアな IPSec トンネルを作成できます。これにより、クラウドセキュリティ（Umbrella および Zscaler）への高速で安全な IPsec WAN 接続、およびエンタープライズ接続が提供されます。
返品許可（RMA）のサポート	RMA のサポートが次のように拡張されています。 • シスコのスイッチスタック（ハードウェアスタッキング）：Cisco DNA Center では、フルスタックのスイッチを交換できます。 • サプリカントベースの拡張ノード（SBEN）。

機能	説明
RMA の準備状況チェック	RMA フローには、デバイスが交換できる状態かどうかを評価する準備状況チェックが含まれています。
SSID用の個別のアカウンティングサーバーの構成のサポート	SSID用に認証および許可サーバーとは異なる個別のアカウンティングサーバーを構成できます。
SSID での CCKM 構成のサポート	Cisco DNA Center での認証キー管理オプションとして CCKM を有効にすることができます。
SSID ブロードキャストのスケジューリングのサポート	SSID スケジューラを作成して、タイムゾーンに基づいて WLAN を有効または無効にすることができます。
リモート LAN ポートのフォールバックメカニズムのサポート	リモート ローカルエリアネットワーク（LAN）ポートには、Dot1x の障害から MAC フィルタリングに、また MAC フィルタリングの障害から Dot1x にフォールバックするメカニズムがあります。
検出ワークフローの機能強化	このリリースから、次の拡張機能を利用できます。 • [Provide Credentials] ウィンドウで、[HTTP（S）Read] および [HTTP（S）Write] のログイン情報を追加できます。 • [Schedule Task] ウィンドウで、トグルボタンをクリックして、[Discover new devices only] オプションを有効または無効にすることができます。
モデル化されたアクセス契約	基盤となるセキュリティグループ ACL（SGACL）の有効なコマンドを Cisco DNA Center によって生成する場合は、アクセス契約の作成時に [Modeled Access Contract] オプションを有効にします。このオプションを有効にすると、アクセス契約は、基盤となるコマンドラインシンタックスを知らなくても作成および編集できるモデルに基づくようになります。 SGACL コマンドラインを直接入力し、アクセス契約をテキストとして保存する場合は、このオプションを無効にすることができます。
モビリティピア構成の機能強化	モビリティグループの構成時に、Cisco DNA Center によって管理されていないワイヤレスコントローラをモビリティピアとして追加できます。
複数アンカー構成のサポート	最大 3 つのアンカー ワイヤレスコントローラでアンカーグループを構成し、アンカーの優先順位を設定できます。アンカーを SSID に追加し、ワイヤレス用のネットワークプロファイルに構成済みのアンカーグループを選択できます。
外部ゲスト アンカー シスコ ワイヤレス コントローラ構成のサポート	外部アンカー ワイヤレスコントローラをアンカーグループに追加できます。
EoX（サポート終了）のコンプライアンスサポート	EoX デバイスのハードウェア、ソフトウェア、およびモジュールについて、コンプライアンスサポートが拡張されました。

機能	説明
ソフトウェアイメージのコンプライアンスサポート	シスコのスイッチスタックについてソフトウェアイメージのコンプライアンスを確認できます。
コンプライアンス違反の確認	重要度の低いコンプライアンス違反を確認し、コンプライアンスステータスの計算から違反をオプトアウトできます。
APのトライラジオ構成のサポート	トライラジオ構成をサポートするAPのトライラジオパラメータを設定できます。
カスタムWLANプロファイル構成のサポート	ゲストおよびエンタープライズワイヤレスネットワークのSSIDを作成する際に、カスタム WLAN プロファイルを構成できます。
AP でのゼロ待機動的周波数選択（DFS）のサポート	5 GHz 無線帯域のカスタム無線周波数（RF）プロファイル構成の一部として、ゼロ待機 DFS を設定できます。ゼロ待機 DFS を使用すると、5 GHz 無線帯域の AP が待機時間なしで新しいチャネルに切り替えることができます。 ゼロ待機 DFS は、Cisco RF ASIC を備えた次の AP でサポートされています。 • Cisco Catalyst 9120AX シリーズ アクセスポイント • Cisco Catalyst 9124AX シリーズ アクセスポイント • Cisco Catalyst 9130 Wi-Fi 6 アクセスポイント
RF プロファイル：6 GHz 無線帯域のサポート	6 GHz 無線帯域は、次の RF 機能でサポートされています。 • 基本 RF プロファイル • AI 無線周波数プロファイル • [Configure AI RF Profile] ワークフロー
リモートテレワーカー構成向けの他の AP モデルのサポート	Cisco DNA Center は、既存の Cisco Aironet 1815T（テレワーカー）AP に加えて、リモートテレワーカー構成向けに次の AP モデルをサポートしています。 • Cisco Aironet 2800 シリーズ アクセス ポイント • Cisco Aironet 3800 シリーズ アクセスポイント • Cisco Catalyst 9100 シリーズ アクセスポイント
新しい AP のサポート	Cisco DNA Centerは、次の AP をサポートしています。 • Cisco Catalyst 9164I シリーズ アクセスポイント • Cisco Catalyst 9166I シリーズ アクセスポイント
MREワークフローを使用したワイヤレス AP のトラブルシューティング	MRE ワークフローを使用して、ワイヤレス AP の問題をトラブルシュートできます。

機能	説明
デフォルト ホームページ	Cisco DNA Center のデフォルトホームページのヘルプメニューのサポートが Cisco CX Cloud Success Tracks に拡張されており、新しいウィンドウで Cisco CX Cloud Success Tracks の Web サイトにアクセスできます。

リモートサポート許可ダッシュボードの表示	[Remote Support Authorization] ダッシュボードで、次の事ができます。
	• [Manage SSH Credentials]：Cisco DNA Center への SSH 接続を確立できます。
	• [Configure SSH Credential]：トラブルシューティングのためにシスコスペシャリストが Cisco DNA Center セットアップにアクセスできるようにします。
	• [Access Permission Agreement] ウィンドウのサポートが、次のチェックボックスを使用できるように拡張されています。
	  • ネットワークデバイスへのアクセス
	  • Cisco DNA Center セットアップへのアクセス

ユーザーインターフェイスの機能強化	[Inventory] ユーザーインターフェイスの機能が強化され、フィルタとレイアウトがより使いやすくなりました。
セキュリティアドバイザリの表示	• Cisco DNA Center のセキュリティアドバイザリのサポートが、Cisco IOS ソフトウェア イメージ バージョン 8.5.120.0 以降で実行される Cisco AireOS ワイヤレスコントローラに拡張されています。 • Cisco DNA Center のセキュリティアドバイザリは [FAILED DEVICES] エリアをサポートしています。このエリアには、将来の日時にスケジュールされているデバイススキャンに関する情報が表示されます。
拡張ノードのデバイスサポート	スタックされた IE9300 スイッチは、プラグ アンド プレイを通じて拡張ノードまたはポリシー拡張ノードとしてオンボードできます。

Cisco DNA Assurance の新機能および変更された機能

機能	説明
サイト分析	構成されたパフォーマンスのしきい値を満たさないサイトの KPI 統計を表示できます。
MS Teams アプリケーション	**MS Teams** アプリケーションの正常性をモニターおよびトラブルシューティングできます。

機能	説明
新しい AP 切断の問題	新しいグローバル AP 切断の問題が導入されました。同じスイッチで発生する AP 切断の問題は、影響を受ける AP のリストとともに集約され、1 つの問題として提起されます。新しく集約された AP 切断の問題は、[Device 360] ウィンドウとグローバルダッシュボードの両方に記録されます。 以前の AP 切断の問題は引き続き記録されます。ただし、これはグローバルな [Issue] ダッシュボードではなく、[Device 360] ウィンドウにのみ表示されます。
組み込み型 シスコ ワイヤレス コントローラ の新規チャート	[Device 360] ウィンドウ組み込みの ワイヤレスコントローラ の多数の新規チャートを選択して表示できます。新規チャートには、電波品質、チャネル使用率、合計フレームエラー数などの KPI が含まれています。
AP の RF チャート	[Device 360] ウィンドウで、AP の RF チャートを選択して表示できます。新規チャートには、スループットやクライアント数、チャネル使用率、クライアント/パケット数別の上位 SSID などの KPI が含まれます。
組み込み型 シスコ ワイヤレス コントローラ の新規グローバルクライアント数	組み込み型 ワイヤレスコントローラ の [Device 360] ウィンドウで、クライアント数チャートには次の新しい数が表示されます。 **Anchor entries**：最近別の ワイヤレスコントローラ にローミングしたクライアントの数。クライアントは既に、このデータを報告している ワイヤレスコントローラ に接続されていません。 **Foreign entries**：最近 ワイヤレスコントローラ にローミングしたクライアントの数。このデータを報告しているワイヤレスコントローラに接続されているクライアントは、現在接続されていない可能性があります。 **Local entries**：現在 ワイヤレスコントローラ に接続しているクライアントの数。 **Idle State entries**：一時的なアイドル状態にあるクライアントの数。
新しい BGP ダウンの問題	ルーター、コア、流通、アクセスの問題に、新しい BGP ダウンの問題が追加されました。BGP ダウンの問題は、BGP 接続がそのネイバーとダウンしているときにトリガーされます。発行トリガー条件は、最長 10 分間に変更できます。
自動問題解決	このリリースでは、システムは次の問題タイプの問題を自動的に解決します。 • スイッチ電源の障害 • スイッチファンの障害
エンドポイントイベント	アシュアランス の [Events] ダッシュボードは、エンドポイントのよりコンテキストに応じたビューを提供します。イベントに関連する他のデバイスに接続されているエンドポイントによってトリガーされたイベントを検索する代わりに、アシュアランス がこれらの詳細を提供します。

機能	説明
クライアントダッシュボードの強化	アシュアランス [Client] ダッシュボードでは、[Client Devices] ダッシュレットの [Excluded Clients] オプションを使用して、特定の シスコ ワイヤレス コントローラのクライアントを除外できます。 [Client 360] ウィンドウで、[Client Details] の [Device Info] タブにある [Excluded] ステータスのハイパーリンクを使用して、特定のワイヤレスコントローラデバイスを除外できます。
PoE 電力使用量ダッシュレットの強化	アシュアランス [PoE] ダッシュボードの、[Allocation] ビューと [Consumption] ビューで、電力使用量ダッシュレットが強化されました。最新およびトレンドのタブには、選択したビューに基づき、デバイスの消費電力と割り当てデータが表示されます。
ファブリック用クライアント 360 の機能強化	このリリースでは、クライアントデバイスの詳細に、セキュリティグループ（タグ値）やブリッジモード（仮想マシン）などのファブリック属性が含まれます。
Cisco AI Network Analytics：ネットワークヒートマップの機能強化	このリリースでは、**スイッチ**の**ネットワークヒートマップ**を生成できます。KPI と特定の**スイッチファミリ**に基づいてヒートマップデータをフィルタリングして、直接比較することができます。 スイッチでは、次の温度 KPI がサポートされています。 • **温度**：**すべてのセンサー** • **温度**：**コア** • **温度**：**ホットスポット** • **温度**：**入口** • **温度**：**出口**
6-GHz 無線帯域サポート	6 GHz 無線帯域サポートが**拡張 RRM** ダッシュボードに追加されました。
RF シミュレータ	AI RF シミュレータを使用して、現在の RF プロファイル構成への変更をシミュレートし、[Enhanced RRM] ダッシュボードの拡張 RRM ダッシュレットに対して予測される結果を視覚化できます。

Cisco DNA Automation の新機能および変更された機能

機能	説明
制限付きシェル	セキュリティを強化するため、Cisco DNA Center のこのリリースからルートシェルへのアクセスは無効になっています。制限付きシェルでは、ユーザーは基礎となるオペレーティングシステムとファイルシステムにアクセスできないため、運用上のリスクが軽減されます。 制限付きシェルは、セキュリティ上の理由から有効になっています。ただし、ルートシェルに一時的にアクセスする場合は、Cisco TAC に連絡して問い合わせる必要があります。
MS Teams 統合の構成	Microsoft Teams との統合を構成できるようになりました。統合を有効にすると、Cisco DNA Center では、アプリケーション 360 ダッシュボードとクライアント 360 ダッシュボードに通話品質メトリック情報が提供されます。
デバイス証明書	[Device Certificate] ウィンドウに [Device Name] 列が含まれるようになり、証明書をデバイス名でフィルタリングできるようになりました。

新機能および変更された機能 Cisco Software-Defined Access

機能	説明
Cisco SD-Access Zero Trust ワークプレイス	Cisco SD-Access は、ワークプレイス向けの Zero Trust セキュリティソリューションを提供します。Cisco SD-Access Zero Trust セキュリティソリューションは、ネットワーク全体のあらゆる場所からすべてのユーザーとデバイスに安全にアクセスできるようにします。エンドポイントの可視化、トラスト評価、およびネットワークのセグメンテーションを実装し、ネットワーク アクセス ポリシーを自動化できます。 [SD-Access Zero-Trust Overview] ダッシュボードで、ワークプレイス全体でゼロトラストが確立されていく様子を把握できます。
ファブリックサイトのリモート LAN サポート	Cisco DNA Center は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでのファブリックサイト用のリモート LAN（RLAN）構成をサポートします。ファブリックサイトの AP に RLAN ポートを構成できます。シスコ ワイヤレス コントローラは有線クライアントを認証し、ネットワークへの接続を許可します。Cisco IOS XE リリース 17.7 以降を実行する ワイヤレスコントローラ ではファブリックサイトに RLAN を設定できます。

機能	説明
SD-Access Transit を使用した、シングルおよびマルチサイトファブリックでのエクストラネットをサポートする仮想ネットワークポリシー	ピアデバイスを介さず、レイヤー 3 VN 間のルート リークを許可する仮想ネットワーク（VN）ポリシーを作成します。DNA Center で自動的に VN ポリシーを作成し、エンドポイント（ホストまたはユーザー）から DHCP、DNS サーバ、インターネットアクセスなどの共有サービスへアクセスできるようになります。共有サービスはプロバイダー VN に接続します。共有サービスを使用するエンドポイントは、サブスクライバ VN 内に存在します。VN ポリシーは、ファブリック内のサブスクライバー VN 間の通信を許可することなく、プロバイダー VN とサブスクライバー VN 間の通信を確立します。 Cisco SD-Access のこのリリースは、ユニキャスト通信に対してのみ VN ポリシーをサポートします。 次の展開では、VN ポリシーの作成、VN ポリシーの編集、および VN ポリシーの削除を行うことができます。 • IP トランジットを使用した単一サイトファブリック • SD-Access トランジットを使用したマルチサイトファブリック
ボーダーノードのアフィニティ ID	Cisco DNA Center では、ボーダーノードのアフィニティ ID 属性を設定できます。アフィニティ ID は、ボーダーノードの相対的な地理的位置を指定します。アフィニティ ID 属性を使用して、ファブリックサイトにネットワークアクセスがない場合にトラフィックをルーティングする優先ボーダーノードを選択できるようになりました。
カスタム ボーダー レイヤ 3 ハンドオフ IP アドレスの割り当て	Cisco DNA Centerのこれまでのリリースでは、レイヤー 3 ハンドオフ 時の仮想ネットワークの IP アドレス割り当てが自動化されていました。Cisco DNA Center のこのリリースでは、レイヤー 3 ハンドオフする仮想ネットワークにそれぞれ IP アドレスとサブネットマスクを手動で割り当てられるオプションがつきました。ボーダーノードとピア間の IP ルーティングを自動化するか、IP アドレスを手動で構成するかを選択できます。両方を行うことはできません。
LAN 自動化タスクビューとステータス	Cisco DNA Centerのこのリリースでは、プライマ デバイスとピアデバイスを含む各デバイスの詳細なステータスビューとログビューが把握できるようになったことで、LAN オートメーションの全体的なエクスペリエンスが向上しました。 [LAN Automation Status] ウィンドウには、デバイスのログと構成を表示するためのオプションがあります。構成の成功や失敗を確認することもできます。構成が失敗した場合、Cisco DNA Centerは対処の手がかりを示したエラーメッセージを表示し、問題解決に向け支援します。

機能	説明
拡張ノードおよびポリシー拡張ノードに対応したフル Flexible NetFlow	すでにプロビジョニングされている拡張ノードとポリシー拡張ノードでアプリケーションテレメトリを有効にできるようになりました。テレメトリを有効にすると、拡張ノードとポリシー拡張ノードのすべてのインターフェースでフローモニターが有効になります。 デバイスでテレメトリを有効にする方法の詳細については、『*Cisco DNA Center User Guide*』の「Configure Telemetry」の章を参照してください。 以下は、アプリケーション テレメトリをサポートする拡張ノードまたはポリシー拡張ノードデバイスです。 • Cisco IOS 15.2(7)E0 以降が動作する Cisco Industrial Ethernet（IE）4000、5000 シリーズ スイッチ。 • Cisco IOS 15.2(7)E2 以降のリリースが動作する Cisco IE 4010 シリーズ スイッチ。 • Cisco IOS XE 17.3.1 以降が動作する Cisco Catalyst IE 3300 シリーズ スイッチ。 • Cisco Catalyst IE 3400 および IE 3400H シリーズ スイッチ。どちらも拡張ノードまたはポリシー拡張ノードとして構成され、Cisco IOS XE 17.3.1 以降のリリースで動作します。 • Cisco IOS XE 17.8.1 以降が動作する Cisco Catalyst IE9300 シリーズ スイッチ。 • Cisco IOS XE 17.3.1 以降が動作する Cisco ESS 3300 シリーズ スイッチ。
レイヤー 3 仮想ネットワーク、レイヤー2仮想ネットワーク、エニーキャスト ゲートウェイ ワークフローの強化	レイヤー 3 仮想ネットワーク、レイヤー 2 仮想ネットワーク、エニーキャストゲートウェイ ワークフローが強化されました。 レイヤー 3 仮想ネットワーク、レイヤー 2 仮想ネットワーク、エニーキャストゲートウェイを1 つのワークフローで最大 5 つまで選択、編集できるようになりました。

インタラクティブヘルプの新機能および変更された機能

機能	説明
新規のウォークスルー	次のウォークスルーが追加されました。 • フロアへの包含リージョンの追加 • フロアへのカバレッジエリアの追加 • フロアへの GPS マーカーの追加 • フロアへのマーカーの追加 • フロアへの開口部の追加 • ボーダーノードの IP ベースのカスタムハンドオフの設定 • 認証テンプレートの変更 • ワイヤレス カバレッジ オプティマイザの実行
新しいリソース	次のリソースを追加しました。 • コミュニティ • ガイド付きセットアップ

Cisco DNA Center の互換性マトリクス

ルータ、スイッチ、ワイヤレス AP、NFVIS プラットフォームなどのデバイス、および Cisco DNA Center の各アプリケーションでサポートされるソフトウェアリリースについては、『*Cisco DNA Center Compatibility Matrix*』[英語] を参照してください。

Cisco SD-Access の互換性マトリクス

Cisco DNA Center での Cisco SD-Access ハードウェアおよびソフトウェアのサポートについては、『*Cisco SD-Access Hardware and Software Compatibility Matrix*』[英語] を参照してください。この情報は、Cisco SD-Access を展開する際に役立ちます。

互換性のあるブラウザ

Cisco DNA Center の GUI は次の HTTPS 対応ブラウザと互換性があります。

- Google Chrome：バージョン 93 以降
- Mozilla Firefox：バージョン 92 以降

Cisco DNA Center へのログインに使用するクライアント システムは、64 ビット オペレーティング システムとブラウザを装備していることが推奨されます。

（注） Cisco DNA Center 2.3.4 へのアップグレードには、Firefox ではなく Chrome を使用することをお勧めします。

サポートされているファームウェア

Cisco Integrated Management Controller（Cisco IMC）のバージョンは、Cisco DNA Center リリースから独立しています。Cisco DNA Center のこのリリースは、次のファームウェアに対してのみ検証されています。

- アプライアンスモデル DN1-HW-APL の Cisco IMC バージョン 3.0(3f) および 4.1(2g)
- アプライアンスモデル DN2-HW-APL の Cisco IMC バージョン 4.1(3d)
- アプライアンスモデル DN2-HW-APL-L の Cisco IMC バージョン 4.1(3d)
- アプライアンスモデル DN2-HW-APL-XL の Cisco IMC バージョン 4.1(3d)

Cisco DNA Center のスケール

Cisco DNA Center のスケールの数値については、*Cisco DNA Center* のデータシート https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/datasheet-listing.html を参照してください。

IP アドレスと FQDN ファイアウォールの要件

既存のネットワーク ファイアウォールを介して Cisco DNA Center からアクセスできるようにする必要がある IP アドレスと完全修飾ドメイン名（FQDN）を特定する方法については、『*Cisco DNA Center Installation Guide*』の「Plan the Deployment」の章の「Required Internet URLs and Fully Qualified Domain Names」 [英語] を参照してください。

テレメトリコレクションについて

Cisco DNA Center ではデフォルトでテレメトリデータが収集されますが、一部のデータ収集をオプトアウトできます。データ収集は、製品機能の開発を支援し、運用上の問題に対処して、より優れた価値と投資回収率（ROI）を実現することを目的としています。シスコが収集するデータの種類は、Cisco.com ID、システム、機能の使用状況、ネットワーク デバイス インベントリ、およびソフトウェア利用資格です。収集されるデータの詳しいリストについては、『*Cisco DNA Center Data Sheet*』 [英語] を参照してください。一部のデータ収集をオプトアウトするには、シスコのアカウント担当者および Cisco TAC にお問い合わせください。

サポートされているハードウェアアプライアンス

シスコは、ラックマウント可能な物理アプライアンスの形で Cisco DNA Center を提供しています。次のバージョンの Cisco DNA Center アプライアンスを使用できます。

- 第 1 世代
  - 44 コアアプライアンス：DN1-HW-APL
- 第 2 世代
  - 44 コアアプライアンス：DN2-HW-APL
  - 44 コア プロモーション アプライアンス：DN2-HW-APL-U
  - 56 コアアプライアンス：DN2-HW-APL-L
  - 56 コア プロモーション アプライアンス：DN2-HW-APL-L-U
  - 112 コアアプライアンス：DN2-HW-APL-XL
  - 112 コア プロモーション アプライアンス：DN2-HW-APL-XL-U

Cisco DNA Center のインストール

Cisco DNA Center ISO イメージがプレインストールされている、シスコから購入した Cisco DNA Center を専用の物理アプライアンスとしてインストールします。インストールと展開の手順については、『*Cisco DNA Center Installation Guide*』を参照してください。

（注） グループベースポリシー分析など、特定のアプリケーションは、デフォルトでは Cisco DNA Center にインストールされないオプションのアプリケーションです。オプションのアプリケーションが必要な場合は、パッケージを個別に手動でダウンロードしてインストールする必要があります。

パッケージのダウンロードとインストールの詳細については、『*Cisco DNA Center Administrator Guide*』の「Manage Applications」 [英語] を参照してください。

Cisco DNA Center プラットフォーム サポート

新機能、インストール、アップグレード、未解決および解決済みのバグに関する情報を含む、Cisco DNA Center プラットフォーム に関する情報については、『*Cisco DNA Center Platform Release Notes*』 [英語] を参照してください。

Cisco Connected Mobile Experiences のサポート

Cisco DNA Center は Cisco Connected Mobile Experiences（CMX）リリース 10.6.2 以降をサポートします。それ以前のバージョンの Cisco CMX はサポートされていません。

（注） CMX設定を構成するときは、CMX管理者パスワードに「#」記号を含めないでください。CMX管理者パスワードに「#」記号を含めると、CMX 統合は失敗します。

プラグアンドプレイに関する考慮事項

一般的な機能のサポート

プラグアンドプレイは、デバイスの Cisco IOS ソフトウェアリリースに応じて、次の機能をサポートします。

- AAA デバイスログイン情報のサポート：AAA ログイン情報はデバイスに安全に渡され、パスワードはログに記録されません。この機能により、**aaa authorization** コマンドを含む構成でデバイスをプロビジョニングできます。この機能を使用するには、デバイスにソフトウェアリリース Cisco IOS 15.2(6)E1、Cisco IOS 15.6(3)M1、Cisco IOS XE 16.3.2、または Cisco IOS XE 16.4 以降が必要です。
- Cisco Catalyst 9200 シリーズ、Catalyst 9300 シリーズ、Catalyst 9400 シリーズ、Catalyst 9500 シリーズ、Catalyst 3650 シリーズ、および Catalyst 3850 シリーズ スイッチのイメージのインストールとアップグレードは、スイッチがインストールモードで起動されている場合にのみサポートされます。（バンドルモードで起動されたスイッチでは、イメージのインストールとアップグレードはサポートされません。）

セキュアな固有デバイス識別子のサポート

安全なデバイス認証を可能にするセキュアな固有デバイス識別子（SUDI）機能は、次のプラットフォームで使用できます。

- Cisco ルータ：
  - ソフトウェアリリース Cisco IOS XE 17.5.1 以降を搭載した Cisco Catalyst IR 1800 シリーズ
  - ソフトウェアリリース Cisco IOS XE 16.6.2 を搭載した Cisco ISR 1100 シリーズ
  - ソフトウェアリリース Cisco IOS XE 3.16.1 以降を搭載した Cisco ISR 4000 シリーズ（ただし、リリース Cisco IOS XE 16.4.1 以降が必要な ISR 4221 は除く）。
  - ソフトウェアリリース Cisco IOS XE 16.6.1 を搭載した Cisco ASR 1000 シリーズ（ASR 1002-x を除く）
- Cisco スイッチ：
  - ソフトウェアリリース Cisco IOS XE 3.6.3E または Cisco IOS XE 16.1.2E 以降を搭載した Cisco Catalyst 3850 シリーズ
  - Supervisor 7-E/8-E と、ソフトウェアリリース 3.6.3E、Cisco IOS XE 3.7.3E、または Cisco IOS XE 16.1.2E 以降を搭載した Cisco Catalyst 3650 シリーズおよび 4500 シリーズ
  - Supervisor 8L-E と、ソフトウェアリリース XE 3.8.1E 以降を搭載した Cisco Catalyst 4500 シリーズ
  - Supervisor 9-E と、ソフトウェアリリース XE 3.10.0E 以降を搭載した Cisco Catalyst 4500 シリーズ

- ソフトウェアリリース Cisco IOS XE 16.6.1 以降を搭載した Cisco Catalyst 9300 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.6.1 以降を搭載した Cisco Catalyst 9400 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.6.1 以降を搭載した Cisco Catalyst 9500 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.10.1e 以降を搭載した Cisco Catalyst IE3300 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.11.1a 以降を搭載した Cisco Catalyst IE3400 シリーズ
- Cisco IOS XE 17.8.1 以降を搭載した Cisco Catalyst IE9300 シリーズ

• NFVIS プラットフォーム：

- ソフトウェアリリース 3.7.1 以降を搭載した Cisco ENCS 5400 シリーズ
- ソフトウェアリリース 3.7.1 以降を搭載した Cisco ENCS 5104

（注） SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号（デバイスラベルのライセンス SN と呼ばれる）の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加する際には、[Serial Number] フィールドに SUDI のシリアル番号を入力する必要があります。次のデバイスモデルには、シャーシのシリアル番号とは異なる SUDI シリアル番号があります。

- Cisco ルータ：Cisco ISR 43xx、Cisco ISR 44xx、Cisco ASR1001-X/HX、および Cisco ASR1002-HX
- Cisco スイッチ：Supervisor 8-E/8L-E/9-E を搭載した Cisco Catalyst 4500 シリーズ、および Catalyst 9400 シリーズ

管理インターフェイスの VRF サポート

プラグアンドプレイは、次のプラットフォームのデバイス管理インターフェイスで動作します。

• Cisco ルータ：

- ソフトウェアリリース Cisco IOS XE 16.3.2 以降を搭載した Cisco ASR 1000 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.3.2 以降を搭載した Cisco ISR 4000 シリーズ

• Cisco スイッチ：

- ソフトウェアリリース Cisco IOS XE 16.6.1 以降を搭載した Cisco Catalyst 3650 シリーズおよび 3850 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.6.1 以降を搭載した Cisco Catalyst 9300 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.6.1 以降を搭載した Cisco Catalyst 9400 シリーズ
- ソフトウェアリリース Cisco IOS XE 16.6.1 以降を搭載した Cisco Catalyst 9500 シリーズ

4G インターフェイスのサポート

プラグアンドプレイは、次のシスコルータの 4G ネットワーク インターフェイス モジュール上で動作します。

- ソフトウェアリリース Cisco IOS XE 16.6.2 以降を搭載した Cisco 1100 シリーズ ISR
- Cisco Catalyst IR 1800 シリーズ

サーバー ID の設定

シスコデバイスで Cisco DNA Center の検出を成功させるには、Cisco Plug and Play IOS エージェントがサーバーの ID を確認できるように、SSL ハンドシェイク中に、Cisco DNA Center によって提供されるサーバー SSL 証明書に適切なサブジェクト代替名（SAN）値が含まれる必要があります。これにより、管理者は適切な SAN 値を持つ新しいサーバー SSL 証明書を Cisco DNA Center にアップロードすることが必要になる場合があります。**[System]** > **[Settings]** > **[Trust & Privacy]** > **[System Certificates]** で新しい証明書署名要求（CSR）を生成できます。詳細については、『Cisco DNA Center Administrator Guide』の「Update the Cisco DNA Center Server Certificate」[英語] を参照してください。

SAN の要件は、次の Cisco IOS リリースを実行しているデバイスに適用されます。

- Cisco IOS リリース 15.2(6)E2 以降
- Cisco IOS リリース 15.6(3)M4 以降
- Cisco IOS リリース 15.7(3)M2 以降
- Cisco IOS XE Denali 16.3.6 以降
- Cisco IOS XE Everest 16.5.3 以降
- Cisco IOS Everest 16.6.3 以降
- 16.7.1 以降のすべての Cisco IOS リリース

次のように、デバイスによって使用されているディスカバリのタイプに基づいて Cisco DNA Center 証明書の SAN フィールドの値を設定する必要があります。

- IPv4 または IPv6 の明示アドレスを使用する DHCP オプション 43 または オプション 17 の検出の場合は、Cisco DNA Center の特定の IPv4 または IPv6 アドレスに SAN フィールドを設定します。
- ホスト名を使用する DHCP オプション 43 またはオプション 17 の検出の場合は、Cisco DNA Center のホスト名に SAN フィールドを設定します。
- DNS ディスカバリの場合は、pnpserver.domain の形式で、Plug and Play のホスト名に SAN フィールドを設定します。
- Cisco Plug and Play Connect のクラウド ポータル ディスカバリの場合で、Cisco Plug and Play Connect のプロファイルに IP アドレスが使用されている場合は、Cisco DNA Center の IP アドレスに SAN フィールドを設定します。プロファイルに Cisco DNA Center のホスト名を使用している場合は、コントローラの FQDN に SAN フィールドを設定する必要があります。

Plug and Play プロファイルで使用される Cisco DNA Center の IP アドレスがネットワークアドレス変換（NAT）ルータによって割り当てられたパブリック IP アドレスの場合は、サーバー証明書の SAN フィールドにこのパブリック IP アドレスを含める必要があります。

デバイスと Cisco DNA Center 間に HTTP プロキシサーバーが使用されている場合は、プロキシ証明書が適切な IP アドレスまたはホスト名と同じ SAN フィールドを持つことを確認します。

検出方法が異なる場合、証明書に複数の SAN 値を含めることを推奨します。たとえば、SAN フィールドに、Cisco DNA Center FQDN と IP アドレス（または NAT IP アドレス）の両方を含めることができます。両方を含める場合は、最初の SAN 値として FQDN、その後に IP アドレスを設定します。

Cisco DNA Center 証明書の SAN フィールドに適切な値が含まれていない場合、デバイスは Plug and Play プロセスを正常に完了できません。

（注） Cisco Plug and Play IOS エージェントは、証明書 SAN フィールドでサーバ ID のみ確認します。共通名（CN）フィールドは確認しません。

バグ

未解決のバグ

次の表に、このリリースの Cisco DNA Center で未解決になっているバグを示します。

バグ ID	見出し
CSCwa19027	Cisco DNA Center は、その標準の Cisco SD-Access 設定の一部として、コマンド「automate-tester username dummy ignore-acct-port probe-on」をプッシュします。Cisco DNA Center では、RADIUS 要求が RADIUS サーバーに定期的に送信されるように、「automate-tester」設定をプッシュします。デバイスが応答を受信すると、サーバーはUpとマークされます。デバイスが応答を受信しない場合、サーバーは Down とマークされます。 認証が成功したか失敗したかにかかわらず、デバイスは RADIUS サーバーからの応答を探すだけなので、ユーザーが Cisco ISE に存在するかどうかは関係ありません。 ユーザーが存在しない場合に、対応するCisco ISE認証ポリシーがデフォルトの「Access-Reject」アクションではなく「Drop」アクションを使用すると、Cisco ISE がパケットをドロップしたときに AAA サーバーは Dead としてマークされることがあります（ダミーユーザーが Cisco ISE に存在しないことが原因）。これは、CTS 操作に影響を与える可能性があり、次のログが毎分生成されます。 `%CTS-3-AAA_NO_RADIUS_SERVER: No RADIUS servers available for CTS AAA request for CTS env-data SM`
CSCwb28054	カスタム設定された RF プロファイル（カスタムベースの RF プロファイルとすべての AI RF プロファイルを含む）を使用している場合、 バージョン 17.7 の ワイヤレスコントローラ のプロビジョニングは、Cisco DNA Center2.3.4 では失敗します。client-aware-fra パラメータ設定のRPC のプロビジョニングが失敗しました。
CSCwb85510	[SYSTEM-SOFTWARE-UPGRADE]イベントでは、複数の DNS 名で同じ IP アドレスを設定した場合、またはCisco DNA Centerでホスト名を設定していない場合、[System Upgrade alert] がソース設定ではなく DNS を使用します。 この問題を回避するには、Cisco DNA Centerアプライアンスにホスト名を 1 つだけ設定します。加えて、このホスト名を対応する DNS サーバーエントリにマップします。これにより、Cisco DNA Centerが生成するどのシステムイベント通知の [Instance] フィールドにも、アプライアンスが適切に参照されます。
CSCwc37682	アシュアランス デザスタリカバリの後、データが GUI に正しく反映されません。 データ cob ログには、コレクター SDK からのブローカーエージェント接続の例外（「5000 ミリ秒後に再試行」など）が反映され、最終的にスタック オーバーフロー例外が発生します。
CSCwc39022	「スイッチの WLC から AP が切断されました」の警告は、Cisco DNA Centerにスイッチを追加した後に AP がゼロであることを示しています。AP 切断の問題では、[Suggested Action] は [empty] です。 AP 切断の問題はスイッチごとにグループ化され、自動解決として処理されます。AP 切断の問題がトリガーされた後にスイッチがCisco DNA Centerに追加された場合は、問題を手動で解決する必要があります。それ以外の場合は、自動解決として処理されます。

バグ ID	見出し
CSCwc42371	[Outlook Web Access] のセンサーテストで [Login Fail] エラーが発生しました。 ほとんどの電子メール サーバーは、サードパーティ アプリケーションが通常のパスワードで直接アクセスすることを許可していないため、 [Outlook Web Access] のセンサーテストが失敗します。たとえば、Gmail と Yahoo は、サードパーティ アプリケーションによる電子メール サーバーへのアクセスに制限を設けています。たとえば、Google では、ユーザー名とパスワードのみで Google アカウントにサインインできるサードパーティアプリケーションやデバイスの使用をサポートしていません。
CSCwc62887	Cisco DNA Center2.2.3 から 2.3.4 にアップグレードした直後、GUI には、ダウンロード可能なリリースバージョンとして最も古いバージョンナンバーが表示されます。これは混乱します。
CSCwc70685	ディザスターリカバリーのフェイルオーバーワークフローが完了するまでに 1 時間以上かかります。
CSCwc74941	Mozilla Firefox を使用して証明書をアップロードする場合（**[System]** > **[Settings]** > **[PKI Certificates]**）、[Choose a file] をクリックしても、拡張子が .cer および .pem のファイルはそれらのファイル形式がサポートされていてもグレー表示されます。 または、ファイル形式が無効であることを示す [File type not supported] が表示されます。 この問題を回避するには、PKI 証明書のアップロードに、Mozilla Firefox ではなく Google Chrome を使用してください。または、ファイルを参照せずに、ファイルをアップロードボックスにドラッグアンドドロップすることもできます。
CSCwc85038	システムの更新がポストフック インストール フェーズで失敗し、失敗後にリリースのアップグレードが再試行されます。リリースのアップグレードは、ポストシステムフックを完全にインストールする前に、アプリケーションパッケージに直接進みます。
CSCwd17228	SSID にアンバインドされた IP プールは、デバイスまでプロビジョニングされません。
CSCwd74259	大きなファブリック サイトをロードできません。

解決済みのバグ

次の表に、Cisco DNA Center リリース 2.3.4.3 で解決されたバグを示します。

バグ ID	見出し
CSCwb57629	プラグアンドプレイで新しいデバイスを追加すると、プロセスが完了し、状態とオンボーディングの進行状況に [Provisioned] と表示されます。ただし、次のエラーメッセージが表示され、デバイスはインベントリに見当たりません。 `NCOB02064: Device not added to Inventory - No CLI credentials provided` この問題を回避するには、すべてのグローバルクレデンシャル（CLI だけでなく、HTTP、SNMP なども含）を削除して再入力します。次に、プラグアンドプレイプロセスを再試行します。

バグ ID	見出し
CSCwc23153	IOX インターフェイス TenGigabitEthernet4/0/48 をプロビジョニングしようとして、Cisco Catalyst 9000 シリーズ スイッチでプロビジョニング タスクが失敗しました。Cisco DNA Center
CSCwc40992	Provision-Fabric ページの Fabric インスタンスにアクセスできません。
CSCwc48881	トライ無線モードをサポートする AP を持つワイヤレスコントローラで AP をプロビジョニングしている間にトライ無線がグローバルで有効化される
CSCwc49833	ディザスタリカバリ：ファイルサービスは、Mongo から消去されたファイルを削除しません。
CSCwc53593	ファブリックホスト オンボーディング ページからのポートの静的割当ては、リクエストが無効なために失敗しました。`[Provisioning failed due to invalid request.]` インターフェイスの `[Connected Device Type]` は変更できません。デバイスタイプを変更するには、インターフェイスをクリアしてからもう一度お試しください。
CSCwc53951	Cisco DNA Center の一部のフロアでは、[Matlab connection timeout] エラーで、ワイヤレスヒートマップが表示されない場合があります。
CSCwc56341	Cisco DNA Centerが予約した IP プール API が 2つ目のグローバル IP プールを認識しません。
CSCwc59647	Cisco DNA Center - VM：VN をファブリックに追加している間、RD の古いエントリがデータベースに残っています。
CSCwc60578	Cisco DNA Centerの事前検証ステータスで Prime Data Migration Tool を使ったマップの移行が完了できません。REST API のエラーです。
CSCwc61000	ディザスタリカバリ：ソフトウェアのアップグレード後に監視VMがディザスタリカバリ設定に再接続しようとすると、再参加操作が失敗します。
CSCwc62677	外部キー制約違反により、Cisco DNA Center のインベントリからのデバイス削除に失敗しました。
CSCwc66513	Cisco DNA Center では、ワイヤレスデバイスがプロビジョニングされているときにインフラストラクチャ セグメントの L3 VNID を 0 に設定する場合があり、その結果、ファブリックネットワークから AP の関連付けが解除されます。
CSCwc69467	Cisco DNA Center 2.3.3.3 では、同じサイト内の AP に異なるサイトタグが割り当てられます。
CSCwc73983	ワイヤレス ファブリック コントロール プレーンの IP アドレスは、ワイヤレスコントローラ から削除されます。

バグ ID	見出し
CSCwc78951	Cisco DNA Centerのインベントリサービスが不安定であるため、インベントリ Web ページの読み込みが遅くなるか、デバイスの同期の実行に時間がかかります。
CSCwc83710	ネットワークプロファイルの詳細設定にアクセスしてカスタムタグを作成すると、Cisco DNA Center GUI にエラーメッセージが表示されます。
CSCwc86109	ファイルシステムは、融合に対して 100% の使用率を示しています。Web GUI が断続的であり、サービスが正しく動作していません。
CSCwc94852	[NCSP11108 CFS persistence failed] のため、ワイヤレス コントローラーをプロビジョニングまたは削除できません。
CSCwc98658	Cisco DNA Centerワイヤレス LAN コントローラのプロビジョニングとコンプライアンス動作がほぼ同時に開始された場合、プロビジョニングが失敗する可能性があります。これが SPF サービスのメモリの枯渇を引き起こす原因とみられます。
CSCwd02734	IP プールをファブリックゾーンに追加すると、[NCSP11108: Error occurred while processing the request] が表示されます。
CSCwd07407	Cisco DNA Center を使い Catalyst 2960-Plus シリーズ 15.2(7)E6 でテレメトリの設定をプロビジョニングまたは更新すると、NetFlow がサポートされていない場合でもエラーが発生します。

次の表に、Cisco DNA Center リリース 2.3.4.0 で解決されたバグを示します。

バグ ID	見出し
CSCwa21212	LAN 自動化を開始できません。次のエラーが生成されます。 `NCND00050: An internal error occurred while processing the request.`
CSCwa29973	デバイスの CTS クレデンシャルがCisco DNA Centerの NAD エントリと同期されません。
CSCwa68838	Cisco DNA Center 2.1.2.7 へのアップグレード後に sspf-service-manager-service が開始されません。
CSCwa77904	シスコ ワイヤレス コントローラのプロビジョニングは、オブジェクトを処理中に内部エラー [NCSP10246] が発生したため失敗します。
CSCwa90595	無効な $apMac 構成要素が原因で、Cisco DNA Center2.2.3.4 のシスコ ワイヤレス コントローラのプロビジョニングが失敗します。
CSCwa97774	名前空間のスナップショットが存在しないため、シスコ ワイヤレス コントローラ のプロビジョニングは失敗します。
CSCwb02969	Cisco Catalyst 9500 スイッチスタックをプロビジョニングし、ファブリック構成をプッシュすると、スイッチのステータスが [Managed Internal error.] に変わります。

バグ ID	見出し
CSCwb28540	Cisco DNA Center 2.2.2.8：プライマリコントローラとセカンダリコントローラの間でタグの不一致が見られます。
CSCwb29770	ファブリックセットアップで、Dot11 の設定の不一致が原因で Cisco 9840 ワイヤレス コントローラのプロビジョニングが失敗します。
CSCwb40106	Cisco DNA Center 2.2.3.4：ソフトウェアイメージ管理（SWIM）は、イメージの転送が成功した後でもアクティベーションタスクを表示しません。
CSCwb42071	重複するキー値が一意の制約「manageddcs_unique_key」に違反するため、スイッチのプロビジョニングが失敗します。
CSCwb47791	イメージリポジトリ：デバイスファミリの割り当て GUI には、Cisco Catalyst 9300X モデル（mdfdata.xml）の特定の PID が必要です
CSCwb57463	単一の RF プロファイルをプロビジョニングすると、サイトのすべての AP が接続/接続解除されます。
CSCwb70550	Cisco DNA Center 2.2.3：重複する Meraki デバイスをインベントリから削除すると、インベントリに割り当てられていないデバイスの数が間違って表示されます。
CSCwb72776	Cisco DNA Center デバイスは、[icppolicymapaction_bk constraint] エラーで同期に失敗します。
CSCwb73232	SNMP ステータスが Success と表示されているのに、デバイスのホスト名は検出結果に表示されません。
CSCwb88023	Cisco DNA Center 2.2.3.4：無効な LAN ポート ID：AP3800、ポート 128 でプロビジョニングが失敗します。
CSCwb96201	Cisco DNA Center 2.2.3.5：Application Visibility ウィンドウが部分的にロードされ、同じ IP アドレスを持つ 2 つの異なるデバイスが表示されます。
CSCwc10284	Cisco DNA Center は、SWIM の配布中に、スイッチで実行されているイメージパッケージの一部を削除しました。
CSCwc11245	API を介して 500 を超えるデバイスを同時に追加しようとすると、Cisco DNA Centerのインベントリサービスが失敗します。
CSCwc13096	postgres が大きなオブジェクトを見つけられないため、AP をプロビジョニングできません。
CSCwc18059	サイトと AP の数が多数ある場合、シスコ ワイヤレス コントローラ のプロビジョニングは [stack overflow error] が発生し失敗します。
CSCwc20229	アプリケーションは RabbitMQ からメッセージを受信できません。RabbitMQ 管理 GUI にログインしてそれぞれの交換を開くと、キューバインドが断続的に表示されます。それ以外の場合、何も表示されません。

バグ ID	見出し
CSCwc28641	Cisco DNA Center 2.2.3.5：Cisco Catalyst 9300 シリーズ スタックスイッチの再同期が、内部エラー（[arpDetails_feature]）のために失敗します。

制限事項と制約事項

SSL インターセプトによるクラウド接続のガイドライン

Cisco DNA Center アプライアンスの Cisco AI Network Analytics エージェントなど、一部の Cisco DNA Center アプリケーションでは、X.509 証明書を使用した相互認証でクラウドへのセキュア通信を確立する必要があります。

直接接続に加えて、SSL 通信がエージェントとクラウドエンドポイントで直接終了し、間に SSL インターセプトデバイスがない限り、プロキシの使用もサポートされます。

SSL インターセプトデバイスを介したクラウド接続はサポートされていないため、接続エラーが発生する可能性があります。

バックアップと復元に関するガイドライン

- Cisco DNA Center のあるバージョンのバックアップを作成し、Cisco DNA Center の別のバージョンにそのバックアップを復元することはできません。バックアップは、バックアップが行われたアプライアンスおよびアプリケーションと同じ Cisco DNA Center ソフトウェアバージョン、アプリケーション、およびアプリケーションバージョンを実行しているアプライアンスにのみ復元できます。
- 復元操作を実行した後、Cisco ISE と Cisco DNA Center の統合を更新します。復元操作の後、Cisco ISE と Cisco DNA Center が同期していない可能性があります。Cisco ISE と Cisco DNA Center の統合を更新するには、**[System]** > **[Settings]** > **[Authentication and Policy Servers]** の順に選択します。[Actions] 列から、サーバーに対応する [Edit] を選択します。更新する Cisco ISE のパスワードを入力します。
- 復元操作の実行後、ネットワーク内のデバイスの構成が復元されたデータベースと同期していない場合があります。このようなシナリオでは、ネットワークデバイスの認証、許可、およびアカウンティング（AAA）と構成のためにプッシュされた CLI コマンドを手動で元に戻す必要があります。入力する CLI コマンドについては、個々のネットワークデバイスのマニュアルを参照してください。
- 復元されたデータベースにデバイスのログイン情報を再入力します。データベースの復元前にサイトレベルのログイン情報を更新していて、復元中のバックアップにログイン情報の変更情報がない場合、すべてのデバイスは、復元後に部分的な収集に移行します。次に、Cisco DNA Center との同期のためにデバイス上のデバイスログイン情報を手動で更新するか、それらのデバイスの再検出を実行してデバイスログイン情報を学習する必要があります。

- 復元されたデータベースへのネットワークデバイスの差分変更を調整した後にのみ、AAA プロビジョニングを実行します。そうしないと、デバイスのロックアウトが発生する可能性があります。
- 自動化データのみ、または自動化データとアシュアランスデータの両方をバックアップおよび復元できます。ただし、GUI または CLI を使用してアシュアランスデータのみをバックアップまたは復元することはできません。

Cisco ISE 統合のガイドライン

- ECDSA キーは、Cisco ISE SSH アクセスの SSH キーとしても、Cisco DNA Center と Cisco ISE の証明書でもサポートされません。
- 既存の証明書を置き換える際には、完全な証明書チェーンを Cisco DNA Center にアップロードする必要があります。Cisco DNA Center 証明書がルート CA のサブ CA によって発行された場合、Cisco DNA Center 証明書の置き換え中に Cisco DNA Center にアップロードされる証明書チェーンには、3 つの証明書すべてが含まれている必要があります。
- Cisco DNA Center に適用される自己署名証明書では、cA:TRUE (RFC5280 section-4.2.19) の基本制約の拡張を使用する必要があります。
- Cisco ISE と Cisco DNA Center の両方の IP アドレスまたは FQDN は、対応する証明書の [Subject Name] フィールドまたは [Subject Alt Name] フィールドのいずれかに存在する必要があります。
- Cisco ISE または Cisco DNA Center のいずれかで証明書が置換または更新された場合は、信頼を再確立する必要があります。
- Cisco DNA Center と Cisco ISE の間に Web プロキシがある場合は、Cisco DNA Center と Cisco ISE の IP または FQDN がプロキシ例外リストに存在する必要があります。
- Cisco DNA Center および Cisco ISE ノードを NAT デバイスの背後に置くことはできません。
- ISE Admin および ISE pxGrid 証明書が異なるエンタープライズ認証局によって発行されている場合は Cisco DNA Center と Cisco ISE を統合できません。

  具体的には、ISE Admin 証明書が *CA* サーバー *A* によって発行され、ISE pxGrid 証明書が *CA* サーバー *B* によって発行され、pxGrid パーソナル機能が ISE PPAN 以外のノードで実行されている場合、Cisco DNA Center から Cisco ISE への pxGrid セッションは機能しません。

デバイスのオンボーディングのガイドライン

Cisco IOS XE 17.8.1 以降を使用する IE-3200-8P2S-E/A、IE-3200-8T2S-E/A、IE-3300-8P2S-E/A、および IE-3300-8T2S-E/A デバイスの場合、デバイスをオンボードする前にインストールモードで起動することをお勧めします。

オンボードされた IE3200 または IE3300 デバイスを Cisco IOS XE 17.8.1 以降にアップグレードする場合は、アップグレードする前に、デバイスがインストールブートモードになっていることを確認してください。

アップグレードの制限事項

- Cisco DNA Center にアップグレードする場合で、次のすべての条件が当てはまるとき、アップグレードは開始されません。
  - Cisco ISE が Cisco DNA Center ですでに構成されている。
  - Cisco ISE のバージョンが 2.6 パッチ 1、2.4 パッチ 7、またはそれ以降ではない。
  - Cisco DNA Center に既存のファブリックサイトが含まれている。
  - DNS サーバーの数は 3 を超えてはならない。

  GUI にはアップグレードの開始に失敗したことが示されませんが、ログにはアップグレードの失敗に関連するメッセージが含まれています。

  この問題を回避するには、Cisco ISE を 2.6 パッチ 1、2.4 パッチ 7、またはそれ以降にアップグレードし、Cisco DNA Center のアップグレードを再試行します。
- In-Service Software Upgrade（ISSU）は、Cisco SD-Access の展開ではサポートされていません。

ライセンスの制限事項

- Cisco DNA Center License Manager は、Cisco IOS XE を実行するワイヤレスコントローラモデルに対してのみスマートライセンスをサポートします。License Manager は、接続モードがスマートプロキシの場合、Cisco 5500 シリーズ AireOS ワイヤレスコントローラのスマートライセンス登録をサポートしません。
- Cisco DNA Center License Manager は、Cisco IOS 17.3.2 以降では、**[Actions]** > **[Manage License Reservation]** での次の操作をサポートしません。
  - ライセンス予約の有効化
  - ライセンス予約の更新
  - ライセンス予約のキャンセル/返却
  - ファクトリライセンス予約

ファブリックの制限事項

- エリアレベルで予約されている IP アドレスプールは、**[Design]** > **[Network Settings]** > **[IP Address Pools]** ウィンドウの建物レベルで [Inherited] として表示されます。ただし、ファブリックサイトが建物レベルで定義されている場合、これらの IP アドレスプールは [Host Onboarding] ウィンドウにリストされません。ファブリックサイトが建物レベルで定義されている場合は、建物レベルで IP アドレスプールを予約する必要があります。ファブリッ

クサイトがエリアレベルで定義されている場合は、エリアレベルで IP アドレスプールを予約する必要があります。

この問題を回避するには、ファブリックサイトと同じレベル（エリアまたは建物）で IP アドレスプールを解放して予約するか、予約済み IP アドレスプールと同じレベルでファブリックサイトを再構成します。

- Cisco DNA Center は、SD-Access トランジットネットワークによって接続されている複数のファブリックサイト間でのマルチキャストをサポートしていません。
- IP ダイレクトブロードキャスト機能は、サイレントホスト（つまり、リモート SD-Access サイトに存在するが、コントロールプレーンに登録されていないホスト）宛ての不明なユニキャストトラフィックに対してのみ、SD-Access トランジットでサポートされています。SD-Access トランジットの下での IP ダイレクトブロードキャストでは、ブロードキャストパケットは使えません。

既存の機能関連の制限事項

- Cisco DNA Center は、デバイスのログイン情報を学習できません。
- インポートフローの一部として、AAA サーバーの事前共有キー（PSK）または共有秘密を入力する必要があります。
- Cisco DNA Center は、DNS、WebAuth リダイレクト URL、syslog に関する詳細は学習しません。
- Cisco DNA Center は、コントローラごとに 1 回だけデバイス構成を学習できます。
- Cisco DNA Center が一度に学習できるワイヤレスコントローラは 1 つだけです。
- サイトプロファイルの作成では、AP および SSID エントリを持つ AP グループのみが考慮されます。
- 自動サイト割り当てはできません。
- サポートされていないセキュリティタイプと無線ポリシーの SSID は破棄されます。
- 認証サーバーとアカウンティングサーバーの場合、RADIUS サーバーがデバイスに存在すると、それが優先されます。RADIUS サーバーが存在しない場合は、TACACS サーバーが設計に考慮されます。
- Cisco ISE サーバー（AAA）構成は、既存のデバイスプロビジョニングを通じて学習できません。
- 認証サーバーとアカウンティングサーバーは、既存のデバイスプロビジョニングを通じて学習されるように、同じ IP アドレスを持っている必要があります。
- SSID が異なる AP グループの異なるインターフェイスに関連付けられている場合、プロビジョニング中に、SSID を使用して新しく作成された AP グループは同じインターフェイスに関連付けられます。
- ワイヤレスの競合は、SSID 名のみに基づいており、他の属性は考慮されません。

ワイヤレスポリシーの制限事項

ポリシーの作成後に AP を移行する場合は、ポリシーを手動で編集し、ポリシーを展開する前に、ポリシーを適切な AP の場所にポイントする必要があります。それ以外の場合は、「`Policy Deployment failed`」メッセージが表示されます。

AP の制限事項

- ローカルにスイッチされる WLAN をプロビジョニングする前に FlexConnect モードで AP を設定すると、AP プロビジョニングエラーがバイパスされます。そうしないと、ローカルで切り替えられた WLAN が Cisco DNA Center によってワイヤレスコントローラまたは AP でプロビジョニングされたときに、AP プロビジョニングが失敗します。

  プロビジョニングの失敗後、AP はワイヤレスコントローラに再参加します。正常なプロビジョニングのために AP を再プロビジョニングできます。

- C-ANT9104 アンテナを備えた Cisco Catalyst 9130AXE AP では、デュアル ラジオ モードの [Disable] オプションは使えません。

- Cisco Catalyst 9124AXE AP では、デュアルラジオモードの自動オプションは使えません。

リリース間コントローラモビリティ（IRCM）の制限事項

インターフェイスまたは VLAN 設定は、外部コントローラとアンカーコントローラの間で区別されません。Cisco DNA Center で提供される VLAN またはインターフェイスは、外部コントローラとアンカーコントローラの両方で設定されます。

トランクポートでの IP デバイストラッキングの制限事項

有線ネットワーク上の不正検出は影響を受けます。Cisco DNA Center は、ブリッジモードのアクセスポイントを介してスイッチに接続されているすべてのクライアントを表示するわけではありません。トランクポートは、すべての VLAN 情報を交換するために使用されます。トランクポートで IP デバイストラッキングを有効にすると、ネイバースイッチに接続されているクライアントも表示されます。Cisco DNA Center は、接続されたインターフェイスがトランクポートであり、ネイバーがスイッチである場合、クライアントデータを収集しません。ベストプラクティスとして、トランクポートでの IP デバイストラッキングを無効にします。トランクポートで IP デバイストラッキングが有効になっている場合、有線ネットワーク上の不正は検出されません。詳細については、「Disabling IP Device Tracking」 [英語]を参照してください。

SNMPv3 での暗号化の制限事項

AES192 および AES256 暗号化は、SNMPv3 構成では完全にはサポートされていません。AES192 または AES256 暗号化を使用して Cisco DNA Center にデバイスを追加すると、それらのデバイスの アシュアランスデータは収集されません。

回避策として、アシュアランスデータを収集するには、AES128 暗号化を備えたデバイスを追加します。Cisco DNA Center は AES128 をサポートし、AES128 暗号化を使用してデバイスのアシュアランスデータを収集します。

IPv6 の制約事項

IPv6 モードで Cisco DNA Center を実行することを選択した場合：

- Access Control Application、Group-Based Policy Analytics、SD-Access、および Cisco AI Endpoint Analytics パッケージは無効になっており、ダウンロードまたはインストールできません。
- Cisco ISE pxGrid は IPv6 をサポートしていないため、Cisco ISE pxGrid を介した通信は無効になっています。

Cisco プラグアンドプレイの制限事項

- 仮想スイッチングシステム（VSS）はサポートされていません。
- Cisco プラグアンドプレイ モバイル アプリは、Cisco DNA Center のプラグアンドプレイではサポートされていません。
- スタック ライセンス ワークフロー タスクは、Cisco IOS XE 16.7.1 以降を実行する Cisco Catalyst 3650 および 3850 シリーズ スイッチでサポートされています。
- スイッチのプラグアンドプレイ エージェントは、デフォルトで VLAN 1 で開始されます。ほとんどの展開では、VLAN 1 を無効にすることをお勧めします。PnP の開始時に VLAN 1 を使用しない場合は、アップストリームデバイスで次のコマンドを入力します。

  pnp startup-vlan *<vlan_number>*

シスコのグループベースポリシー分析の制限事項

- シスコのグループベースポリシー分析は、現実的な顧客データに基づいて、最大 5 つの同時要求をサポートします。GUI 操作は 5 秒以内に応答することが望ましいですが、現実的なデータに基づく極端なケースでは、最大 20 秒かかることがあります。一度に 5 つ以上の同時要求を防止するメカニズムはありませんが、発生すると、一部の GUI 操作が失敗する可能性があります。1 分以上かかる操作はタイムアウトします。
- データの集約は、シスコのグループベースポリシー分析の UTC からの 1 時間ごとのオフセットで発生します。ただし、一部のタイムゾーンは UTC から 30 分または 45 分のオフセットがあります。Cisco DNA Center サーバーが UTC から 30 分または 45 分のオフセットがあるタイムゾーンにあり、クライアントが UTC からの 1 時間ごとのオフセットがあるタイムゾーンにある場合、またはその逆の場合、シスコのグループベースポリシー分析でのクライアントのデータ集約の時間範囲は正しくありません。

  たとえば、Cisco DNA Center サーバーがカリフォルニア PDT（UTC-7）にあり、データ集約が時間単位のオフセット（午前 8:00、午前 9:00、午前 10:00 など）で発生するとします。インドの IST（UTC+5.30）にあるクライアントが、カリフォルニアの時間範囲 9:30 ～ 10:30 a.m. PDT に対応する 10:00 ～ 11:00 p.m. IST のデータを表示しようとした場合、集約は表示されません。
- 1 時間以内に発生したグループの変更はキャプチャされません。エンドポイントが別のセキュリティグループに変更されると、シスコのグループベースポリシー分析は次の 1 時間までこの変更を認識しません。

- [Search Results] ウィンドウで [Security Group] 列と [Stealthwatch Host Group] 列を並べ替えることはできません。
- Cisco DNA アシュアランスとシスコのグループベースポリシー分析の間で、ネットワークアクセスデバイスに関連する情報（場所を含む）に不一致が見られる場合があります。

アプリケーションテレメトリの制限事項

デバイスでアプリケーションテレメトリを設定するときに、Cisco DNA Center は NetFlow データのソースとして間違ったインターフェイスを選択する可能性があります。

Cisco DNA Center で特定のインターフェイスを強制的に選択するには、インターフェイスの記述に Netflow ソースを追加します。Netflow ソースの前ではなく後ろに特殊文字とそれに続くスペースを使用できます。たとえば、次の構文は有効です。

```
netflow-source
MANAGEMENT netflow-source
MANAGEMENTnetflow-source
netflow-source MANAGEMENT
netflow-sourceMANAGEMENT
netflow-source & MANAGEMENT
netflow-source |MANAGEMENT
```

次の構文は無効です。

```
MANAGEMENT | netflow-source
* netflow-source
netflow-source|MANAGEMENT
```

IP アドレスマネージャの制限事項と回避策

- 既存の IPAM 統合を編集するとき、または新しい IPAM マネージャを追加するときに、次のエラーが表示される場合があります。

  ```
  NCIP10283: The remote server presented a certificate with an incorrect CN of the
  owner
  ```

  これを修正するには、IPAM の新しい証明書を再生成し、次の条件のいずれかが満たされていることを確認します。

  - 証明書の SAN フィールドに値が設定されていません。
  - 値が設定されている場合、値とタイプ（IP アドレスまたは FQDN）は、**[System]** > **[Settings]** > **[External Services]** > **[IP Address Manager]** ウィンドウに設定されている URL と一致する必要があります。

- Cisco DNA Center は、信頼できる証明書を持つ外部 IPAM サーバーとの統合をサポートします。Cisco DNA Center GUI の **[System]** > **[Settings]** > **[External Services]** > **[IP Address Manager]** で、次のメッセージが表示される場合があります。

  ```
  NCIP10282: Unable to find the valid certification path to the requested target.
  ```

  自己署名証明書のこのエラーを修正するには、次の手順を実行します。

1. OpenSSL を使用して、次のいずれかのコマンドを入力し、IPAM タイプに応じた自己署名証明書をダウンロードします。（コマンドでは FQDN [ドメイン名] または IP アドレスを指定できます。）

   ```
   openssl s_client -showcerts -connect Infoblox-FQDN:443
   ```

   ```
   openssl s_client -showcerts -connect Bluecat-FQDN:443
   ```

2. 出力の ---BEGIN CERTIFICATE--- から ---END CERTIFICATE--- までの内容を使用して、新しい .pem ファイルを作成します。

3. **[System]** > **[Settings]** > **[Trust & Privacy]** > **[Trustpool]**に移動し、[Import] をクリックして、証明書（.pem ファイル）をアップロードします。

4. **[System]** > **[Settings]** > **[External Services]** > **[IP Address Manager]**に移動し、外部 IPAM サーバーを構成します。（IPAM サーバーがすでに構成されている場合は、この手順をスキップしてください。）

CA 署名付き証明書のこのエラーを修正するには、IPAM にインストールされている CA のルート証明書と中間証明書を Cisco DNA Center trustpool（**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Trustpool]**）にインストールします。

- CA 署名付き証明書が認証局によって取り消された場合、次のエラーが表示されることがあります。

  ```
  NCIP10286: The remote server presented with a revoked certificate. Please verify the
   certificate.
  ```

  これを修正するには、認証局から新しい証明書を取得し、それを**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Trustpool]**にアップロードします。

- 外部 IPAM の詳細を設定した後、次のエラーが表示される場合があります。

  ```
  IPAM external sync failed:
  NCIP10264: Non Empty DNAC parent pool <CIDR> exists in external ipam.
  ```

  これを修正するには、次の手順を実行します。

  1. 外部 IPAM サーバー（BlueCat など）にログインします。

  2. 親プールの CIDR が外部 IPAM サーバーに存在することを確認し、その親プールの下に構成されているすべての子プールを削除します。

  3. Cisco DNA Center GUI に戻り、**[System]** > **[Settings]** > **[External Services]** > **[IP Address Manager]** で IPAM サーバーを再構成します。

- IP アドレスマネージャを使用して外部 IPAM を構成しているときに、次のエラーが表示される場合があります。

  ```
  NCIP10114: I/O error on GET request for "https://<IP>/wapi/v1.2/":
  Host name '<IP>' does not match the certificate subject provided by the peer
  (CN=www.infoblox.com, OU=Engineering, O=Infoblox, L=Sunnyvale, ST=California, C=US);
  nested exception is javax.net.ssl.SSLPeerUnverifiedException: Host name '<IP>'
  does not match the certificate subject provided by the peer (CN=www.infoblox.com,
  OU=Engineering,
  O=Infoblox, L=Sunnyvale, ST=California, C=US) |
  ```

これを修正するには、次の手順を実行します。

1. 外部 IPAM サーバー（Infoblox など）にログインします。
2. 有効なホスト名または IP アドレスとして共通名（CN）値を使用して外部 IPAM 証明書を再生成します。前の例では、CN 値は www.infoblox.com ですが、これは外部 IPAM の有効なホスト名または IP アドレスではありません。
3. 有効な CN 値を使用して証明書を再生成したら、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Trustpool]**に移動します。
4. [Import] をクリックして、新しい証明書（.pem ファイル）をアップロードします。
5. **[System]** > **[Settings]** > **[External Services]** > **[IP Address Manager]** に移動し、有効なホスト名または IP アドレス（証明書の CN 値としてリストされている）としてサーバー URL を使用し、外部 IPAM サーバーを構成します。

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

Cisco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。

関連資料

Cisco DNA Center の参照ドキュメントとして以下をお勧めします。

情報のタイプについては、	このドキュメントを参照してください...
リリース情報（新機能、制限事項、未解決および解決済みのバグなど）。	*Cisco DNA Center Release Notes* [英語]
Cisco DNA Center のインストールと設定（設置作業を含む）について。	*Cisco DNA Center Installation Guide* [英語]
Cisco DNA Center の最新リリースに関するアップグレード情報。	*Cisco DNA Center Upgrade Guide* [英語]
Cisco DNA Center GUI とアプリケーションの使用について。	*Cisco DNA Center User Guide* [英語]
ユーザアカウント、セキュリティ証明書、認証およびパスワードポリシー、バックアップと復元の設定について。	*Cisco DNA Center Administrator Guide* [英語]
セキュリティの機能、強化、ベストプラクティスを通じて安全に展開する方法について。	*Cisco DNA Center Security Best Practices Guide* [英語]
サポートされているデバイスについて（ルータ、スイッチ、ワイヤレス AP、ソフトウェアリリースなど）。	*Cisco DNA Center Compatibility Matrix* [英語]
Cisco SD-Access 向けハードウェアおよびソフトウェアのサポートについて。	*Cisco SD-Access Compatibility Matrix* [英語]
Cisco DNA アシュアランス GUI の使用について。	*Cisco DNA Assurance User Guide* [英語]
Cisco DNA Center プラットフォーム GUI とアプリケーションの使用について。	*Cisco DNA Center Platform User Guide* [英語]
Cisco DNA Center プラットフォーム リリース情報（新機能、展開、バグなど）。	*Cisco DNA Center Platform Release Notes* [英語]
Cisco Wide Area Bonjour アプリケーション GUI の使用について。	*Cisco Wide Area Bonjour Application User Guide* [英語]
Cisco DNA Center での Stealthwatch Security Analytics Service の使用について。	*Cisco Stealthwatch Analytics Service User Guide* [英語]
Cisco DNA Center での不正および aWIPS 機能を使用した脅威の監視について。	*Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide* [英語]

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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