Cisco DNA Center リリース 2.3.7.0 および 2.3.7.3 リリースノート

初版：2023 年 8 月 11 日

最終更新：2023 年 11 月 28 日

Cisco DNA Center リリース 2.3.7.0 および 2.3.7.3 リリースノート

Cisco DNA Center 2.3.7.0 および 2.3.7.3 は段階的なロールアウトで利用できます。ソフトウェアの一般提供が開始されるまでは、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。段階的なロールアウトが完了すると、Cisco DNA Center はすべてのお客様に一般提供されます。

このドキュメントでは、Cisco DNA Center 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については、Cisco DNA Center 2.3.7 マニュアル [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。

日付	変更内容	参照先
2023 年 11 月 28 日	未解決のバグ CSCwi28419 を追加しました。	未解決のバグ （42 ページ）
2023 年 11 月 22 日	Cisco DNA Center 2.3.7.3 のパッケージのリストを追加しました。	Cisco DNA Center のパッケージバージョン （2 ページ）
	2.3.7.3 の「解決済みのバグ」の表を追加しました。	解決済みのバグ （44 ページ）
	2.3.7.3 の未解決のバグを追加しました。	未解決のバグ （42 ページ）
2023 年 9 月 15 日	デバイス API およびエンリッチメントの詳細 API の機能拡張に関する情報を追加しました。	Cisco DNA Center プラットフォームの新機能および変更された機能 （8 ページ）
2023 年 8 月 22 日	アプリケーションポリシー機能とアプリケーション可視性機能に関する制限を追加しました。	注意事項と制約事項 （32 ページ）

日付	変更内容	参照先
2023 年 8 月 18 日	カスタムアプリケーションに関する制限を追加しました。	注意事項と制約事項 （32 ページ）
2023 年 8 月 11 日	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、検証ツールを使用して Cisco DNA Center のアプライアンスの正常性とアップグレードの準備状況チェックを実行します。アップグレード前チェックを実行するための [Appliance Infrastructure Status] および [Upgrade Readiness Status] 検証セットを選択します。詳細については、『*Cisco DNA Center Administrator Guide*』の「Configure Integration Settings」の章の「Use the Validation Tool」を参照してください。

Cisco DNA Center のパッケージバージョン

パッケージ名	リリース 2.3.7.3	リリース 2.3.7.0
リリースビルドバージョン		
リリースバージョン	2.3.7.3.70332	2.3.7.0.70488
システムアップデート		
システム	1.7.1063	1.7.1011
システム共通	2.1.713.60610	2.1.710.60872
パッケージの更新		
アクセス制御アプリケーション	2.1.713.60610	2.1.710.60872
AI エンドポイント分析	1.11.524	1.11.219
AI ネットワーク分析	3.1.23.315	3.1.20.303
アプリケーション ホスティング	2.3.12309151849	2.3.12307240540
アプリケーションポリシー	2.1.713.117299	2.1.710.117317
アプリケーションレジストリ	2.1.713.117299	2.1.710.117317
アプリケーション可視性サービス	2.1.713.117299	2.1.710.117317

パッケージ名	リリース 2.3.7.3	リリース 2.3.7.0
アシュアランス - 基本	2.3.7.1168	2.3.7.396
アシュアランス - センサー	2.3.7.1141	2.3.7.308
自動化 - 基本	2.1.713.60610	2.1.710.60872
自動化 - インテリジェントキャプチャ	2.1.713.60610	2.1.710.60872
自動化 - センサー	2.1.713.60610	2.1.710.60872
Cisco DNA Center ドキュメント	2.1.713.60610	2.1.710.60872
Cisco DNA Center グローバル検索	1.12.1.18	1.12.1.16
Cisco DNA Center プラットフォーム	1.12.241.40	1.12.1.230
Cisco DNA Center UI	1.7.5.221	1.7.5.201
Cisco Identity Services Engine Bridge	2.1.713.90102	2.1.710.80882
Cisco Umbrella	2.1.713.590143	2.1.710.590223
クラウド接続 - コンテキストコンテンツ	2.8.1.368	2.8.1.368
クラウド接続 - データハブ	1.12.9	1.12.9
クラウド接続 - テザリング	2.33.2.40	2.33.2.34
クラウドデバイス プロビジョニング アプリケーション	2.1.713.60610	2.1.710.60872
コマンドランナー	2.1.713.60610	2.1.710.60872
デバイスのオンボーディング	2.1.713.60610	2.1.710.60872
ディザスタリカバリ	2.1.713.360050	2.1.710.360089
ディザスタリカバリ ー 監視サイト	2.1.713.370022	2.1.710.370026
グループベースポリシーの分析	2.3.7.16	2.3.7.10
イメージ管理	2.1.713.60610	2.1.710.60872
機械推論	2.1.713.210038	2.1.710.210245
NCP - 基本	2.1.713.60610	2.1.710.60872
NCP - サービス	2.1.713.60610	2.1.710.60872
ネットワーク コントローラ プラットフォーム	2.1.713.60610	2.1.710.60872
ネットワーク データ プラットフォーム - 基本分析	2.3.7.10082	2.3.7.137

パッケージ名	リリース 2.3.7.3	リリース 2.3.7.0
ネットワーク データ プラットフォーム - コア	1.9.3085	1.9.3069
ネットワーク データ プラットフォーム - マネージャ	1.9.3016	1.9.3016
ネットワーク エクスペリエンス プラットフォーム - コア	2.1.713.60610	2.1.710.60872
Path Trace	2.1.713.60610	2.1.710.60872
RBAC 拡張	2.1.713.1900008	2.1.710.1900007
不正および aWIPS	2.9.0.26	2.9.0.17
SD-Access	2.1.713.60610	2.1.710.60872
Stealthwatch セキュリティ分析	2.1.713.1090146	2.1.710.1090230
サポート サービス	2.1.713.880009	2.1.710.880043
システム修復	1.1.0	—
Wide Area Bonjour	2.4.713.75128	2.4.710.75209

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

表 *1 : Cisco DNA Center 2.3.7.3* の新機能および変更された機能

機能	説明
2D および 3D ワイヤレスヒートマップのパフォーマンスの向上	Cisco DNA Center は Cisco DNA Assurance を使用して、2D および 3D ワイヤレスヒートマップのパフォーマンスを向上させます。Cisco DNA Center では数秒以内に AP とヒートマップのデータが表示されます。
Cisco Connected Mobile Experiences（CMX）統合の機能強化	Cisco DNA Center では、CMX TLS/SSL 証明書の検証が実行されます。拡張 GUI には、CMX 証明書を確認およびインポートして、新規および既存の CMX 統合の信頼を確立するオプションが用意されています。Cisco DNA Center と CMX の間のサービスの中断を回避するには、Cisco DNA Center 2.3.7.3 アップグレードをインストールする前に、CMX SSL/TLS 証明書を設定し、Cisco DNA Center の信頼できる証明書に CMX 証明書をインポートします。アップグレード後、**[System]** > **[Settings]** > **[Cisco Spaces/CMX Servers]** で CMX 接続ステータスを検証できます。
デバイスの構成ドリフト	ネットワークデバイス用にアーカイブされた最後の構成のタイムスタンプと、デバイスで実行された config-drift 検証のタイムスタンプを確認できます。

機能	説明
SWIM アップグレードワークフローにおける設定の制御のサポート	設定変更の拡張制御を使用すると、計画されたソフトウェアイメージのアップグレードを承認を受けるために ITSM に送信してから展開できます。
スイッチスタックからのスタックメンバーの削除	PnP ダッシュボードの [Delete Member] オプションを使用して、スイッチスタックからスタックメンバーを削除できます。
FlexConnect SSID の VLAN 作成の機能拡張	このリリースでは、FlexConnect SSID の場合、プロビジョニング中に Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで VLAN が自動的に作成されません。ワイヤレス ネットワーク プロファイルにマッピングされたインターフェイスと VLAN は、AP のプロビジョニング時に Flex プロファイルに作成されます。
2D ワイヤレスヒートマップのフロアインポート履歴	正常にインポートされた AP、インポートに失敗した AP、計画済み AP、オーバーレイオブジェクトのログなど、2D ワイヤレスヒートマップのフロアインポート履歴を表示できます。

表 *2 : Cisco DNA Center 2.3.7.0* の新機能および変更された機能

機能	説明
AP Join プロファイルの不正パラメータのサポート	Cisco DNA Center は、次の不正パラメータをサポートしています。 • Rogue detection minimum Received Signal Strength Indicator（RSSI） • Rogue detection transient interval • Rogue detection report interval • Protected Management Frame（PMF）denial
PnP オンボーディング用 AP の場所の設定	PnP オンボーディングの AP の場所として、PnP 要求中に割り当てられたサイトを設定できます。
AP プリイメージのダウンロードの進行状況	デバイスに関連付けられているすべての AP について、AP のプリイメージ ダウンロード タスクに関する詳細を表示できます。
アプリケーション Quality of Service（QoS）のサポート	Cisco DNA Center では、デバイスがプロビジョニングされているサイトに QoS ポリシーを展開する場合、プラグアンドプレイまたはサイト割り当てを介してオンボードされた有線デバイスで、アプリケーション QoS ポリシーをデフォルトで有効にできます。
デバイスでのアプリケーション可視性とコントローラベースのアプリケーション認識（CBAR）の有効化	Cisco DNA Center では、有線で検出されたデバイスと、プラグアンドプレイまたはサイト割り当てを介してオンボードされたデバイスで、アプリケーション可視性と CBAR をデフォルトで有効にできます。
C9800 Day 0 オンボーディング テンプレートのサポート	Cisco DNA Center PnP は、ワイヤレスデバイスのオンボーディング テンプレートをサポートしています。

機能	説明
CAD ファイルからの壁のインポートに関する設定可能な制限	フロアマップとして使用する CAD ファイルをインポートする場合、インポートされる壁の数に制限を設定できます。制限を設定すると、3D ヒートマップの生成にかかる時間を最小限に抑えることができます。
非ファブリック展開用 REP リングからのノードの削除	Cisco DNA Center は、非ファブリック展開 REP リングからのノードの動的な削除をサポートしています。
強化された 2D ワイヤレスヒートマップの生成	デフォルトで有効になっている 3D 計算ヒートマップジェネレータは、2D と 3D の両方のヒートマップの生成をサポートしています。3D 計算ヒートマップジェネレータを無効にして、元のヒートマップジェネレータを使用することもできますが、3D 計算ヒートマップジェネレータを使用することを推奨します。元のヒートマップジェネレータよりも大幅に高速でヒートマップを生成でき、ヒートマップ計算に含まれる壁の数に制限を設定できるため、処理速度も向上します。
セキュリティアドバイザリ、Field Notice、およびネットワークバグ ID 機能の CX ライセンストライアルを有効にする拡張エクスペリエンス	セキュリティアドバイザリ、Field Notice、およびネットワークバグ ID 機能のトライアルを有効にするプロセスが強化されました。これらの機能のトライアルを開始するには、トライアルの利用規約に同意する必要があります。ただし、いずれかのトライアルで 1 回同意すれば、その後は他の機能のトライアルを開始できます。
インベントリの再同期のインサイト	インベントリ内における最後の同期の開始時刻と最後の同期の原因を確認できます。
双方向互換性マトリックスの比較に対するソフトウェアイメージ管理（SWIM）の拡張サポート	Cisco DNA Center SWIM は、In-Service Software Upgrade（ISSU）の互換性に関する意思決定を改善するために、双方向互換性マトリックス ファイルの比較を実行します。 Cisco DNA Center は、cisco.com で入手可能な ISSU 対応デバイスの実行イメージとゴールデンタグ付きイメージの互換性マトリックスファイルを自動的にダウンロードできます。
2D ヒートマップでの稼働中の AP および計画済み AP のサポート	稼働中の AP と計画済み AP の両方を示すカバレッジヒートマップを 2D で表示できます。このオプションは、3D 計算ヒートマップジェネレータが有効になっている場合（デフォルト設定）にのみ使用できます。3D 計算ヒートマップジェネレータを無効にすると、2D ヒートマップは元のヒートマップジェネレータに戻り、稼働中の AP または計画済み AP のヒートマップのみ表示され、両方同時には表示されません。
解決された IP アドレスのツールチップ	デバイスの解決された IP アドレスは、[IP Address] 列で確認できます。
[Design] > [Network Settings] > [Network] ウィンドウのユーザーインターフェイスの更新	[Network Settings] > [Network] ウィンドウが更新され、ユーザー体験が向上しました。

機能	説明
Cisco DNA Center を明るい外観または暗い外観で表示する	Cisco DNA Centerは、明るい外観（デフォルト）または暗い外観で表示できます。**[My Profile and Settings]** > **[Display Settings]** ウィンドウで、明るい外観または暗い外観を適用できます。
コンプライアンス修復の可視性と制御	コンプライアンス違反を修正する際に、計画したネットワーク構成をITサービス管理（ITSM）に送信して、展開前に承認を受けることができます。
構成の可視化と制御	拡張制御を使用すると、計画したネットワーク構成を ITSM に送信して、展開前に承認を受けることができます。制御により、認証および承認された構成のみがネットワークデバイスにプロビジョニングされるため、デバイスのセキュリティが強化されます。

Cisco DNA Assurance の新機能および変更された機能

表 *3*：アシュアランス リリース *2.3.7.3* の新機能および変更された機能

機能	説明
Assurance デバイス 360 からデバイスインベントリへの相互起動	[Device 360] ウィンドウから [Device Inventory] ウィンドウを相互起動して、デバイスの詳細を表示できます。

表 *4*：アシュアランス リリース *2.3.7.0* の新機能および変更された機能

機能	説明
[Event Analytics - Preview] ダッシュボード	syslog メッセージとさまざまなタイプのネットワークイベントの分析データとインサイトデータを確認できます。[Issues and Events] ウィンドウの [Event Analytics - Preview] ダッシュボードから、さまざまなデータソース間のトレンドを特定し、イベントを関連付けられます。ダッシュボードには、syslog メッセージの数と有線およびワイヤレスデバイスからの到達可能性の遷移を含むヒートマップが表示されます。
更新の問題	次の問題は消去時に更新されます。更新期間は28日です。問題ごとにタイムスタンプが更新されるため、次の消去サイクルまで問題が存在します。 • AP の切断 • スイッチ到達不能 • ルータ到達不能 • WLC 到達不能 • スイッチの WLC から AP が切断

機能	説明
RF Insights - Tx Drops チャート	クライアント KPI ごとの [Tx Drops] は、リリース 17.12 以降、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと接続しているクライアントで使用できます。[Device 360] ダッシュボードの [RF] タブには、選択した無線の選択した SSID ごとに、パケットドロップ数が上位 5 つのクライアントを含む [Top Clients with Tx Drops per SSID] チャートが表示されます。 [Client 360] ダッシュボードの [Connected] タブには、パケットドロップのパーセンテージを示す [Tx Drops] チャートが表示されます。
有線 アシュアランス 向けサードパーティ製デバイスのサポート	サードパーティ製デバイスは有線 アシュアランスでサポートされています。[Network] および [Device 360] アシュアランス の正常性ダッシュボードから、サードパーティ製デバイスをモニターおよびトラブルシューティングできます。デフォルトでは、サードパーティ製デバイスは [Core] デバイスファミリカテゴリにマッピングされます。 [Issue Settings] ダッシュボードで、サードパーティ製デバイスによって生じた問題を確認できます。

Cisco DNA Center プラットフォームの新機能および変更された機能

表 *5 : Cisco DNA Center* プラットフォーム、リリース *2.3.7.3* の新機能および変更された機能

機能	説明
新しい API	
サイト API	Cisco DNA Center プラットフォームは、次のサイト API をサポートします。 • GET <cluster-ip>/dna/intent/api/v1/site-member/${id}/member サイトに割り当てられているデバイスを取得します。 新しいサイト API にアクセスするには、メニューアイコンをクリックして、**[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Know Your Network] ドロップダウンリストを展開し、[Sites] を選択します。
API の機能拡張	

機能	説明
taskId データ型	

機能	説明
	応答スキーマでは、taskId パラメータで次の API の `string` データ型がサポートされるようになりました。 • SNMPv3 ログイン情報の更新 • ID によるデバイスの削除 • デバイスの同期 • SNMP 読み取りコミュニティの更新 • Add Device • ID による検出の削除 • HTTP 書き込みログイン情報の作成 • 検出の開始 • SNMP 書き込みコミュニティの作成 • グローバルログイン情報の更新 • SNMP 読み取りコミュニティの作成 • HTTP 読み取りログイン情報の更新 • CLI ログイン情報の作成 • 指定された ID による既存の検出の更新 • SNMPv3 ログイン情報の作成 • SNMP プロパティの作成/更新 • デバイスの詳細の更新 • HTTP 書き込みログイン情報の更新 • デバイスロールの更新 • HTTP 読み取りログイン情報の作成 • 指定された範囲による検出の削除 • NETCONF ログイン情報の更新 • デバイスリストのエクスポート • デバイスで読み取り専用コマンドを実行して、リアルタイムの設定を取得する • すべての検出の削除 • ID によるグローバルログイン情報の削除

機能	説明
	• CLI ログイン情報の更新 • SNMP 書き込みコミュニティの更新 • NETCONF ログイン情報の作成
デバイス API	デバイスの追加 API のタイプ要求パラメータに `FIREPOWER MANAGEMENT CENTER` および `THIRD PARTY DEVICE` デバイスタイプが含まれるようになりました。
廃止された API	
ネットワーク管理 API	次の ネットワーク管理 API は廃止になりました。 • POST <cluster-ip>/dna/intent/api/v1/device-credential デバイスのログイン情報を作成します。 • DELETE <cluster-ip>/dna/intent/api/v1/device-credential/${id} デバイスのログイン情報を削除します。 • PUT <cluster-ip>/dna/intent/api/v1/device-credential デバイスのログイン情報を更新します。 • GET <cluster-ip>/dna/intent/api/v1/device-credential デバイスのログイン情報の詳細を取得します。

表 *6 : Cisco DNA Center* プラットフォーム、リリース *2.3.7.0* の新機能および変更された機能

機能	説明
新しい API	
デバイス API	Cisco DNA Center プラットフォームは、次のデバイス API をサポートします。 POST <cluster-ip>/dna/intent/api/v2/networkDevices/${deviceId}/interfaces/query デバイスインターフェイス統計情報を取得します。 新しい API では、1 分あたり 500 リクエストが許可されます。 新しいデバイス API にアクセスするには、メニューアイコンをクリックして、**[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Know Your Network] ドロップダウンリストを展開し、[Devices] を選択します。

機能	説明
サイト API	Cisco DNA Center プラットフォームは、次のサイト API をサポートします。 • GET <cluster-ip>/dna/intent/api/v2/site サイト V2 を取得します。 • GET <cluster-ip>/dna/intent/api/v2/site/count サイト数 V2 を取得します。 新しいサイト API にアクセスするには、メニューアイコンをクリックして、**[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Know Your Network] ドロップダウンリストを展開し、[Sites] を選択します。
コンプライアンス API	Cisco DNA Center プラットフォームは、次のコンプライアンス API をサポートします。 • GET <cluster-ip>/dna/intent/api/v1/network-device-config/task 設定タスクの詳細を取得します。 • POST <cluster-ip>/dna/intent/api/v1/network-device-config/write-memory デバイス構成をコミットします。 新しいコンプライアンス API にアクセスするには、メニューアイコンをクリックして、 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Know Your Network] ドロップダウンリストを展開し、[Compliance] を選択します。
Configuration Archive API	Cisco DNA Center プラットフォームは、次の Configuration Archive API をサポートします。 GET <cluster-ip>/dna/intent/api/v1/network-device-config 構成アーカイブの詳細を取得します。 新しい Configuration Archive API にアクセスするには、メニューアイコンをクリックして、 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Site Management] ドロップダウンリストを展開し、[Configuration Archive] を選択します。

機能	説明
システム設定 API	Cisco DNA Center プラットフォームは、次のシステム設定 API をサポートします。 • DELETE <cluster-ip>/dna/intent/api/v1/authentication-policy-servers/${id} 認証およびポリシーサーバーアクセス設定を削除します。 • POST <cluster-ip>/dna/intent/api/v1/authentication-policy-servers 認証およびポリシーサーバーアクセス設定を追加します。 • GET <cluster-ip>/dna/intent/api/v1/ise-integration-status Cisco ISE サーバー統合ステータス。 • PUT <cluster-ip>/dna/intent/api/v1/integrate-ise/${id} Cisco ISE サーバー統合用の Cisco ISE サーバー証明書を承認します。 • PUT <cluster-ip>/dna/intent/api/v1/authentication-policy-servers/${id} 認証およびポリシーサーバーアクセスの設定を編集します。 新しい システム設定 API にアクセスするには、メニューアイコンをクリックして、 **[Platform]** > **[Developer Toolkit]** > **[APIs]** > **[System Settings]** の順に選択します。
ユーザー API とロール API	Cisco DNA Center プラットフォームは、次のユーザー API とロール API をサポートします。 • PUT <cluster-ip>/dna/system/api/v1/role ロール API を更新します。 • DELETE <cluster-ip>/dna/system/api/v1/user/${userId} ユーザー API を削除します。 • POST <cluster-ip>/dna/system/api/v1/role ロール API を追加します。 • DELETE <cluster-ip>/dna/system/api/v1/role/${roleId} ロール API を削除します。 新しいユーザー API とロール API にアクセスするには、メニューアイコンをクリックして、 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Cisco DNA Center System] ドロップダウンリストを展開し、[User and Roles] を選択します。

機能	説明
LAN 自動化 API	Cisco DNA Center プラットフォームは、次の LAN 自動化 API をサポートします。 • PUT <cluster-ip>/dna/intent/api/v1/lan-automation/${id} LAN 自動化を停止し、デバイスを更新します。 • PUT <cluster-ip>/dna/intent/api/v1/lan-automation/updateDevice LAN 自動化デバイスを更新します。 新しいLAN自動化APIにアクセスするには、メニューアイコンをクリックして、**[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Site Management] ドロップダウンリストを展開し、[LAN Automation] を選択します。
API の機能拡張	
イベント管理 API	Create Webhook Destination API、Get Webhook Destination API、および Update Webhook Destination API に isProxyRoute 属性が含まれるようになりました。
デバイス API	Cisco DNA Center プラットフォームは、次のデバイス API の機能拡張をサポートします。 • デバイスリストの取得：pendingSyncRequestsCount、pendingSyncRequestsCount、reasonsForDeviceResync、reasonsForPendingSyncRequests、dnsResolvedManagementAddress、および lastDeviceResyncStartTime 応答フィールドを追加しました。 • 指定されたデバイスの物理コンポーネントの詳細を取得：応答スキーマに新しい製造元属性を含めます。 • Get Device Count API：managementIpAddress、macAddress、hostname、および locationName クエリパラメータを追加しました。 • デバイスのシャーシ詳細の取得：応答パラメータ assemblyNumber、assemblyRevision はオプションになりました。 • デバイスインターフェイス VLAN を返す：マスク応答パラメータはオプションフィールドになりました。 • ID によるモジュールの取得とモジュール情報の取得：assemblyNumber、assemblyRevision、moduleIndex、および operationalStateCode 応答パラメータはオプションになりました。 • 属性に完全または部分的に一致するデバイス値の取得：次のサンプル応答スキーマが含まれるようになりました。 `{ "response": [ "string" ], "version": "string" }`

機能	説明
コンプライアンス API	Get Compliance Detail Count API および Get Compliance Detail Intent API の complianceStatus 属性と complianceType 属性に複数値のサポートを追加しました。
エンリッチメントの詳細 API	使いやすさを向上させるために、次の API のレート制限が 1 分あたり 100 リクエストに引き上げられました。 • クライアント エンリッチメントの詳細の取得 • デバイスエンリッチメントの詳細の取得 • 問題エンリッチメントの詳細の取得 • ユーザーエンリッチメントの詳細の取得
サイト API	サイトに割り当てられているデバイスを取得します。 更新された URL：PUT <cluster-ip>/dna/intent/api/v1/site-member/${id}/member
廃止された API	
デバイスオンボーディング（PnP）API	次のデバイスオンボーディング（PnP）API は廃止されました。 • GET <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/sacct/${domain}/vacct/${name}/sync-result バーチャルアカウントの同期結果を取得します。 • POST <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/vacct-sync バーチャル アカウント デバイスを同期します。 • POST <cluster-ip>/dna/intent/api/v1/onboarding/pnp-device/unclaim デバイスの要求を解除します。
新規イベント	

機能	説明
アシュアランス Events	Cisco DNA Center プラットフォームは、次の新しい アシュアランス イベントをサポートします。 • サードパーティ製デバイスの WAN インターフェイスでの高い入出力使用率：このイベントは、WAN インターフェイスで入力または出力の使用率が高い場合に生成されます。 • コントロールプレーンノードのファブリック LISP セッションステータス：このイベントは、コントロールプレーンからファブリックノードへの LISP セッションステータスがダウンすると生成されます。 • ファブリック LISP Pub/Sub セッションステータスダウン：このイベントは、ボーダーノードとコントロールまたはトランジット コントロール プレーン ノード間の LISP Pub/Sub セッションステータスがダウンすると生成されます。ボーダープレーンとコントロールプレーンのペアごとに 1 つのイベントが生成されます。 • ファブリックボーダーノードのインターネットが使用不可：インターネットの可用性では、外部ボーダーのデフォルトルートがモニターされて、LISP または Pub/Sub サイト内のコントロールプレーンノードに登録されます。ボーダープレーンとコントロールプレーンのペアごとに 1 つのイベントが生成されます。 • ピアデバイスでファブリック BGP セッションステータスがダウン：このイベントは、BGP セッションが IP トランジットピアのボーダーノードでダウンしている場合に生成されます。ボーダープレーンとコントロールプレーンのペアごとに 1 つの問題が生成されます。 • ファブリックボーダーノードのリモートインターネットが使用不可：リモートインターネットの可用性では、リモートファブリックサイトが、LISP または Pub/Sub サイト内の SDA トランジット接続ボーダーを介してバックアップインターネットを提供できるかどうかモニターされます。ボーダープレーンとコントロールプレーンのペアごとに 1 つのイベントが生成されます。
イベントの機能拡張	
アシュアランス Events	新しくサポートされるコネクタタイプ SNMP と NO_ENDPOINT が既存の アシュアランス イベントに追加されました。 イベントおよびイベントの通知の設定については、*Cisco DNA Center プラットフォーム ユーザー ガイド* [英語] の「Developer Toolkit GUI」の章を参照してください。
新しいレポート	

機能	説明
AI エンドポイント分析	[AI Endpoint Analytics] レポートタイプには、ロックされたエンドポイント プロファイリング レポートが含まれます。 （注） レポートのロックを解除するには、**[System]** > **[Software Management]** > **[AI Endpoint Analytics]** から [Cisco AI Endpoints Analytics] パッケージをインストールする必要があります。
Long Term	[Long Term] レポートタイプには、次のタイプのロックされたレポートが含まれます。 • AP パフォーマンスレポート • 長期 AP の詳細 • 長期 AP の無線 • 長期 AP の使用状況とクライアントの内訳 • 長期クライアントの詳細 • 長期クライアントセッション • 長期ネットワークデバイス （注） [Long Term] レポートを有効にするには、AI Network Analytics を有効にする必要があります。AI Network Analytics の有効化の詳細については、*Cisco DNA Center* 管理者ガイド [英語] の「Configure Cisco AI Network Analytics」のトピックを参照してください。
レポートの機能拡張	

柔軟なレポート	Cisco DNA Center プラットフォームは、次の柔軟なレポートの機能拡張をサポートします。
	• [Entities] に次の新しいオプションが追加されました。
	  • SWIM：[Summary] レポートタイプをサポートします。
	  • PoE
	• フィールドフィルタには、新しい演算子ベースの選択基準が含まれています。
	詳細については、*Cisco DNA Center* プラットフォーム ユーザー ガイド [英語] の「Reports」の章にある「Generate a Flexible Report」のトピックを参照してください。

Cisco DNA Automation の新機能および変更された機能

表 *7 : Cisco DNA Automation* リリース *2.3.7.3* の新機能および変更された機能

機能	説明
カスタムポリシータグの再利用	カスタムポリシータグは、サイト（エリア、建物、フロア）全体で再利用できます。
FlexConnect SSID の VLAN 作成の機能拡張	このリリースでは、FlexConnect SSID の場合、プロビジョニング中に Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで VLAN が自動的に作成されず、ワイヤレス ネットワーク プロファイルにマッピングされたインターフェイスと VLAN は、AP のプロビジョニング時に Flex プロファイルに作成されます。
ワイヤレスメニューと設定のグローバル検索サポート	Cisco DNA Center は、ネットワーク設定、モデル構成設計、およびワークフローのワイヤレスパラメータのグローバル検索機能をサポートしています。

表 *8 : Cisco DNA Automation* リリース *2.3.7.0* の新機能および変更された機能

機能	説明
PnP 導入準備用の AP の場所設定	PnP オンボーディングの AP の場所として、PnP 要求中に割り当てられたサイトを設定できます。 **[System] > [Settings] > [Device Settings] > [PnP AP Location]** ウィンドウでは、次のようになります。 • [Configure AP Location] チェックボックスをオンにすると、Cisco DNA Center は割り当てられたサイトをPnP 導入準備用の AP の場所として構成します。 • [Configure AP Location] チェックボックスをオフにすると、Cisco DNA Center では PnP オンボーディング中に AP の場所が設定されないため、[Configure Access Points] ワークフローを使用して AP の場所を設定できます。 このチェックボックスは、デフォルトでオフになっています。 （注） これらの設定は、AP プロビジョニングやその他の Day-n 運用中には適用されません。
ワイヤレス用 CLI テンプレートの競合の検出	Cisco DNA Center は、ワイヤレス用 CLI テンプレートでの潜在的な設計の競合とランタイムの競合の検出をサポートしています。 （注） Cisco DNA Center は Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のランタイム競合検出はサポートしていません。
シスコ ワイヤレス コントローラ 設定の処理の機能拡張	シスコ ワイヤレス コントローラ の再プロビジョニング中、Cisco DNA Center は、インテントの一部ではない設定を上書きしないようにします。

機能	説明
ゲスト ワイヤレス ネットワークの中央 Web 認証 SSID に対するアクセス制御リストの機能拡張	このリリースでは、Cisco DNA Center で生成された事前認証アクセス制御リスト（ACL）は、ゲスト ワイヤレス ネットワークの中央 Web 認証（CWA）SSID に設定された AAA または PSN サーバーに対してのみ作成されます。
Cisco AireOS ワイヤレスコントローラ の RF プロファイルにおける無線帯域の管理ステータスの機能拡張	このリリースでは、Cisco AireOS ワイヤレスコントローラ の場合、RF プロファイルで帯域の管理スタータスを無効にして、ワイヤレスコントローラ または AP を再プロビジョニングすると、Cisco DNA Center は、（プロファイルを [None] として設定する代わりに）対応する帯域の RF プロファイルを作成して AP グループにマッピングし、AP で対応する帯域に関するすべての無線の管理ステータスを無効にします。
ワイヤレス ネットワーク プロファイルのテンプレートの関連付けの機能拡張	ワイヤレス ネットワーク プロファイルにオンボーディングテンプレートと Day-n テンプレートを関連付けることができます。オンボーディングテンプレートは、プラグアンドプレイ（PnP）を使用してワイヤレスデバイスをオンボーディングするときに使用されます。
デュアル無線モードの AP におけるチャネル幅選択の機能拡張	以前のリリースでは、デュアル無線モードが AP で有効になっている場合、そのスロット 2 を 160 MHz チャネル幅の [Client-Serving] または [Monitor] 無線ロールにすることはできませんでした。 このリリースでは、デュアル無線モードが AP で有効になっている場合、そのスロット 2 を 160 MHz チャネル幅の [Client-Serving] 無線ロールにすることはできません。
Cisco AireOS ワイヤレスコントローラ の RF プロファイル更新の機能拡張	Cisco AireOS ワイヤレスコントローラ 用のこのリリースでは、ワイヤレスコントローラ ですでにプロビジョニングされている RF プロファイルの DCA チャネルまたはデータレートを変更すると、Cisco DNA Center によって対応する無線がリセットされます。

機能	説明
RF プロファイルの SSID ワークフロー、事前認証 ACL、IP ベースのアクセス契約、および RX SOP しきい値の機能拡張	Cisco DNA Center は、エンタープライズおよびゲストネットワークの SSID 作成ワークフローで、認証キー管理設定、入力および出力 QoS 設定、およびワイヤレス暗号化設定をサポートしています。 （注） 以前のリリースからリリース 2.3.7 にアップグレードする場合： • WPA3-Enterprise SSID の場合、Cisco DNA Center は、SSID の Dot1x-SHA256 認証キー管理設定を有効にします。 • WPA2-WPA3-Enterprise SSID の場合、Cisco DNA Center は、SSID の Dot1x 認証キー管理設定と Dot1x-SHA256 認証キー管理設定の両方を有効にします。 この設定により、Cisco IOS XE リリース 17.6 以前を実行している Cisco AireOS ワイヤレスコントローラおよびワイヤレスコントローラの意図した設定が変更される可能性があります。ワイヤレスコントローラを再プロビジョニングする前に、SSID の**認証キー管理**設定を更新できます。 Cisco DNA Center は、事前認証アクセス制御リストおよび IP ベースのアクセスコントロール契約で追加のプロトコルをサポートしています。 Cisco DNA Center は、[RX-SOP Threshold (dBm) Custom Value] フィールドを使用して、基本および AI RF プロファイルの各帯域のカスタム Receiver Start of Packet Detection（RX-SOP）しきい値をサポートしています。
追加の WLAN パラメータのサポート	Cisco DNA Center は、高度な SSID モデル構成設計の追加の WLAN パラメータをサポートしています。エンタープライズ ネットワークとゲストネットワークの SSID 作成ワークフローは、高度な SSID モデル構成設計の選択をサポートしています。
AP 更新ワークフローで交換ステータスを追跡するための手動データ更新のサポート	[Access Point Refresh] ワークフローでは、最新の AP 交換ステータスを表示するために、[Refresh Data] オプションを使用できます。 （注） このリリースでは、Cisco DNA Center はデータを自動的に更新しません。
新しい国コードのサポート	Cisco DNA Center は、Cisco IOS XE リリース 17.12 以降を実行している Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの新しい国コードをサポートしています。AP 内の無線は、製造時に特定の規制ドメインに割り当てられていますが、国コードを使用すると、規制ドメイン内で稼働する特定の国を指定できます。 サポートされている国コードの製品ごとの完全なリストについては、https://www.cisco.com/c/dam/assets/prod/wireless/wireless-compliance-tool/index.html を参照してください。

機能	説明
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ プロビジョニング時のワイヤレス管理インターフェイス用静的 IP アドレスのサポート	このリリースでは、プロビジョニングの失敗を防ぐために、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でワイヤレス管理インターフェイスの静的 IP アドレスを設定する必要があります。
ワイヤレスデバイス構成の可視性と制御	このリリースでは、Cisco DNA Center はワイヤレスデバイス構成の拡張制御をサポートしています。強化された制御を使用すると、IT サービス管理（ITSM）チェックを通じて、認証および承認された構成のみをネットワークデバイスにプロビジョニングできます。 デフォルトでは、[Configuration Preview] は有効になっており、[ITSM Approval] は無効になっています。これらの設定は、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]** ウィンドウで更新できます。[ITSM Approval] を有効にするには、[Configuration Preview] と ITSM が有効になっていることを確認します。 （注） 計画したネットワーク構成を展開するときに競合する操作が存在する場合、[Pending Operations] ダイアログボックスが表示されます。現在の展開を続行するには、既存、スケジュール済み、またはレビュー保留の操作が完了するまで待つか、この操作を破棄する必要があります。

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

機能	説明
ファブリック構成の可視化と制御	制御機能を使用すると、計画したファブリック構成を ITSM に送信して、ファブリックデバイスに展開する前に承認を受けることができます。 すべてのファブリックワークフローと構成で、可視性と制御機能がサポートされています。
SD-Access の新しい自動化	強化された Cisco SD-Access のユーザーインターフェイスでは、ファブリック要素と各要素の属性の簡潔なビューが表示されます。
AS パスプリペンドのサポート	AS パスプリペンドを変更することで、SD-Access ファブリックの入力ボーダーの選択を操作できます。BGP AS_PATH リストに付加される AS パスの数を定義できます。

機能	説明
Preprefix Affinity	Preprefix Affinity は、SD-Access トランジットを介してリンクされた複数のファブリックサイトが同じデータセンターに接続されているデータセンターのマルチホーミングを可能にします。この設定では、各ファブリックサイトは、データセンターホストに到達するために独自のローカル内部ボーダーを選択できます。ファブリックサイトにデータセンターへのローカル到達可能性がない場合、すべてのサイトボーダーの優先順位が同じであれば、トラフィックはリモートサイトを介して転送されるか、複数のリモートサイト間で負荷分散されます。この動作はデフォルトでイネーブルにされています。 また、データセンターホストがローカル内部ボーダーを介して到達可能であるにもかかわらず、特定のリモートサイトにルーティングされるようにトラフィックを設定できます。この設定は、より効率的なルーティングのためにトラフィックが特定の内部ボーダーを通過する必要がある展開で役立ちます。特定のサイトへのトラフィックのステアリングを有効にする方法については、Cisco Support にお問い合わせください。
SD-Access ファブリックのワイヤレス メッシュ アクセス ポイント	Cisco DNA Center リリース 2.3.7 以降、SD-Access ファブリックでワイヤレスメッシュ AP をオンボードできます。メッシュ AP は、ネットワーク要件に応じて、メッシュアクセスポイント（MAP）またはルートアクセスポイント（RAP）としてプロビジョニングできます。
ワークグループブリッジのサポート	Cisco SD-Access でのワークグループブリッジ（WGB）のサポートにより、ファブリックエッジ、拡張ノード、またはポリシー拡張ノードを展開できないエリアにファブリック接続が拡張されます。WGB はファブリック SSID のファブリック アクセス ポイント（AP）に関連付けられ、有線クライアントは WGB の背後にあるレイヤ 2 スイッチに接続します。クライアントが 802.1X 認証を受ける必要があるシナリオでは、ポートベースの認証を有効にするように WGB を設定します。WGB の設定については、Cisco Support にお問い合わせください。

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
2.3.7.3 の新機能	
新規のウォークスルー	• ウィンドウをお気に入りに追加 • お気に入りの管理
2.3.7.0 の新機能	

機能	説明
新規のウォークスルー	• CLI テンプレートの複製 • CLI テンプレートの作成 • CLI テンプレートのエクスポート • CLI テンプレートのインポート • Field Notice の表示
廃止されたウォークスルー	複合テンプレートの作成

以前のリリースの新機能

前のリリース Cisco DNA Center 2.3.6 の新機能については、「New and Changed Information」[英語] を参照してください。Cisco DNA Center 2.3.6 は、可用性の制限されたリリースです。2.3.6 の機能は 2.3.7 にロールアップされています。

廃止された機能

Cisco DNA Center トラフィック テレメトリ アプライアンス

2.3.7.3 以降、Cisco DNA Center は Cisco DNA Center トラフィック テレメトリ アプライアンスの次の機能をサポートしていません。

- プラグ アンド プレイ（PnP）
- プロファイル
- プロビジョニング

さらに、Cisco DNA Center は、スイッチでテレメトリを有効にする自動ワークフローをサポートしなくなりました。

ネットワーク解析モジュール

2.3.7.3 以降、Network Analysis Module（NAM）または vNAM サーバーは Cisco DNA Center と統合できません。インテリジェントキャプチャは、NAM または vNAM と統合されなくなりました。

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 2.3.7 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(3i)
- アプライアンスモデル DN2-HW-APL-L の Cisco IMC バージョン 4.1(3i)
- アプライアンスモデル DN2-HW-APL-XL の Cisco IMC バージョン 4.1(3i)

Cisco IMC ファームウェアの更新

Cisco IMC ファームウェアを更新する場合は、まず、インストールしている Cisco DNA Center の対応するリリースのリリースノートを参照してください。リリースノートの「サポートされているファームウェア」セクションに、ご使用の Cisco DNA Center リリースの Cisco IMC ファームウェアバージョンが記載されています。

次に、『Cisco Host Upgrade Utility User Guide』のファームウェアの更新手順をご覧ください。

3 ノードクラスタ構成では、クラスタ内の 3 つのノードをすべてシャットダウンしてから Cisco IMC ファームウェアを更新することをお勧めします。ただし、必要に応じて、クラスタノードを個別にアップグレードすることもできます。*Cisco DNA Center* 高可用性ガイド [英語] の「Typical Cluster Node Operations」を参照し、手順に従って 1 つまたはすべてのノードをシャットダウンしてからメンテナンスを実施します。

Cisco DNA Center スケール

Cisco DNA Center のスケールの数値については、*Cisco DNA Center* データシート [英語] 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* 設置ガイド [英語] の「Plan the Deployment」の章の「Required Internet URLs and Fully Qualified Domain Names」を参照してください。

テレメトリ コレクション

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を提供するように設計されています。シスコが収集するデータのカテゴリ：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* のデータシート」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

シスコから購入した Cisco DNA Center ISO イメージがプレインストールされている 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*』[英語] を参照してください。

（注） Group-Based Policy Analytics 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 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。

注意 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ていません）。

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 検出の場合は、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 フィールドのサーバー ID のみ確認し、共通名（CN）フィールドは確認しません。

Web コンテンツ アクセシビリティ ガイドライン 2.1 標準のサポート

Cisco DNA Center 2.3.7 は、AA 適合レベルの Web コンテンツ アクセシビリティ ガイドライン（WCAG）2.1 標準をサポートしますが、次の制限事項があります。

表 *9 : WCAG 2.1* 標準のサポート

WCAG Success Criterion	サポート	制限事項
1.2.4：キャプション（ライブ）	未サポート	—
1.2.5：音声説明（録音済み）	未サポート	—
1.3.4：方向付け	未サポート	—
1.3.5：入力目的の特定	サポート対象	—
1.4.3：コントラスト（最小）	サポート対象	—
1.4.4：テキストのサイズ変更	サポート対象	—
1.4.5：テキストの画像	サポート対象	—

WCAG Success Criterion	サポート	制限事項
1.4.10：リフロー	サポート対象	—
1.4.11：テキスト以外のコントラスト	サポート対象	—
1.4.12：テキストの間隔	サポート対象	—
1.4.13：ホバーまたはフォーカスのコンテンツ	サポート対象	—
2.4.5：複数の方法	サポート対象	—
2.4.6：見出しとラベル	サポート対象	—
2.4.11：フォーカスの外観（最小）	サポート対象	—
2.5.7：ドラッグ移動	一部サポートあり	サードパーティライブラリの制限により、ダッシュボードでは、ドラッグアンドドロップが部分的にサポートされます。
2.5.8：ターゲットサイズ（最小）	サポート対象	—
3.1.2：各部の言語	サポート対象	—
3.2.3：一貫したナビゲーション	サポート対象	—
3.2.4：一貫した識別	サポート対象	—
3.3.3：エラーの提案	サポート対象	—
3.3.4：エラー防止（法的、財務、データ）	未サポート	—

Cisco Wide Area Bonjour のサポートの例外

Cisco Wide Area Bonjour アプリケーションは Cisco DNA Center リリース 2.3.7 で維持されますが、Cisco Wide Area Bonjour アプリケーションは Cisco DNA Center 仮想アプライアンスではサポートされていません。

注意事項と制約事項

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。

（注） 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] 列で、対応するサーバーの横にある [Edit] をクリックします。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 コマンドを手動で入力する必要があります。入力する CLI コマンドについては、対応する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含まれていない場合、復元後、すべてのデバイスで部分的な収集が実行されます。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 アドレスまたは FQDN がプロキシ例外リストに含まれている必要があります。
- 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、Cisco ISE Admin 証明書が CA サーバー A によって発行され、Cisco ISE pxGrid 証明書が CA サーバー B によって発行され、pxGrid ペルソナが Cisco 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。

製品内ヘルプの制限事項

オンラインヘルプおよびインタラクティブヘルプは、ライトモードのみをサポートしており、ダークモードはサポートしていません。

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

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

- エンタープライズ IP アドレスまたは FQDN を変更したら、ライセンス関連のタスクを試行する前に、すべてのサービスが稼働している必要があります。
- 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]** における以下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継承されています。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ネイティブマルチキャストのみをサポートしています。ヘッドエンドレプリケーションは、SD-Access トランジットではサポートされていません。
- Cisco Catalyst 9000 シリーズスイッチは、MACsec スイッチ間接続をサポートしています。

（注） オーバーレイネットワークでは、スイッチからホストへのMACsec接続の使用は推奨されません。

既存のスイッチからホストへのMACsecの実装または設計レビューについては、シスコの営業担当者またはチャネルパートナーにお問い合わせください。

- スイッチからSD-Accessファブリック関連のCLIを手動で削除する場合、Cisco DNA Centerでは通常のデバイスプロビジョニング中にコマンドが適用されないため、ファブリックノードにコマンドを手動で追加する必要があります。または、ファブリックからデバイスを削除してから、そのデバイスをファブリックに再度追加します。

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。

高可用性の制限事項

Cisco DNA Center は Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ の HA をサポートしていません。

ワイヤレスの制限事項

- ワイヤレスポリシーの作成後に AP を移行する場合は、ワイヤレス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。
- Cisco DNA Center は、ワイヤレスマップでの Bluetooth Low Energy（BLE）無線の表示に対応していません。

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、デュアル無線モードの [Disable] オプションはサポートされていません。
- Cisco Catalyst 9124AXE AP では、デュアル無線モードの自動オプションはサポートされていません。

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。

IP デバイストラッキングの制限事項

- トランクポート上の IPDT は、有線ネットワーク上の不正検出の影響を受けます。Cisco DNA Center では、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が表示され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。

- シャーシにラインカードを追加したり、シャーシからラインカードを取り外したりすると、Cisco DNA Center で変更が更新されるまでに数分かかります。IPDT 設定（ある場合）は、新たに追加されたインターフェイスのデバイスに自動的にプッシュされます。
- デバイスをスタックプールに追加したり、スタックプールからデバイスを削除したりすると、Cisco DNA Center で変更が更新されるまでに数分かかります。IPDT 設定（ある場合）は、新たに追加されたインターフェイスのデバイスに自動的にプッシュされます。

  デバイスをスタックに追加したり、スタックから削除したりするには、手動 CLI 設定を使用する必要があります。

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、ダウンロードやインストールはできません。
- 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。
- LAN 自動化はサポートされていません。
- サイトへのデバイスの追加はサポートされていますが、プロビジョニングはサポートされていません。
- ITSM 統合はサポートされていません。
- ワイヤレスデバイスのネットワークプロファイルはサポートされていません。

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。

- Assurance と Cisco Group-Based Policy Analytics 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

- Cisco DNA Center の場合、アプリケーションテレメトリは Cisco Catalyst 9500 シリーズ スイッチではサポートされていません。

- 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-source** コマンドを追加します。**netflow-source** の後には特殊文字とそれに続くスペースを使用できますが、前には使用できません。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

- Infoblox の制限事項：
  - Infoblox には名前属性が表示されないため、Infoblox のコメントフィールドには、同期中に IP プール名が入力されます。
  - プールのインポートでは、コメントフィールドの最初の 50 文字が使用されます。コメントにスペースがある場合は、アンダースコアに置き換えられます。
  - インポートされたプールの IP プール名が更新されると、コメントが上書きされ、新しい名前が反映されます。

- 既存の IPAM 統合を編集するとき、または新しい IPAM 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]** で設定されている 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、次のエラー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。前述の例では、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。

レポートの制限事項

重要なデータを含むレポートが Cisco DNA Center プラットフォームで生成できないことがあります。このような場合は、フィルタを使用してレポートサイズを縮小し、このような障害を防ぐことを推奨します。

カスタムアプリケーションの制限事項

カスタムアプリケーションがデフォルトバケットの一部として設定されている場合、Cisco DNA Center は管理対象デバイスに設定をプッシュしません。

アプリケーションポリシーとアプリケーション可視性の制限事項

Cisco DNA Center からアプリケーションポリシー機能またはアプリケーション可視性機能をプロビジョニングする場合、これらの機能以外で行われた変更は Cisco DNA Center に自動的に反映されません。変更を Cisco DNA Center に反映させるには、これらの機能を再プロビジョニングする必要があります。

サードパーティ製デバイスのサポートの制限事項

Cisco DNA Center によるサードパーティ製デバイスのサポートに関しては、次の点に注意してください。

- サードパーティ製デバイスは、MIB-II（RFC 1213）をサポートするシスコ以外のデバイスとして定義され、Cisco DNA Center に追加できます。
- シスコは、サードパーティ製デバイスに対して新しい権限を発行しません。
- シスコは、サードパーティ製デバイスの一般利用規約を更新しません。
- Cisco DNA Center に追加されたサードパーティ製デバイスは、機能が制限されており（可視性のみ）、Cisco TAC ではサポートされていません。サードパーティ製デバイスで問題が発生した場合は、その製品のベンダーまたはサポート契約を結んでいる担当者に連絡して支援を受ける必要があります。

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
CSCwe38665	インベントリに多数の管理対象デバイスがある場合、インベントリレポートの実行は失敗し、次のエラーが表示されます。 `BAPI Execution Failed.Response Code = 500, Response Content=null`
CSCwe74245	ディザスタ リカバリ フェールオーバー後、ワイヤレスが有効になっている Catalyst 9800 コントローラ、Catalyst 9300 スイッチ、および Catalyst 9400 スイッチの特定のシナリオでは、CBAR プロビジョニングが失敗します。
CSCwe85799	Cisco DNA Center 3 ノードクラスタ：セットアップからプロキシを削除すると、到達可能であっても、ホストとの接続が失われているとノードに表示されます。
CSCwf16863	グローバル LLDP 設定では、ホールド時間とタイマーの値が非常に大きい場合、デバイスの同期中に設定された値はデータベースから破棄されます。
CSCwf17924	3 ノードクラスタのノードをシャットダウン後、一部のサービスインスタンスが非アクティブになります。
CSCwf24189	デバイスの可制御性の設定中に例外が発生しました。
CSCwf56037	2 つのサイト割り当てタスク（1 つはデバイスをサイトに割り当てるタスク、もう 1 つはサイトからデバイスを削除するタスク）が作成された場合、[Tasks] ウィンドウに競合通知が表示されません。
CSCwf59765	Cisco DNA Center で生成された事前認証 ACL には、AAA/ISE サーバーのみが特定の SSID にマッピングされているため、Cisco DNA Center は、追加された他のすべての AAA サーバーを無視します。この変更により、すでに作成されている ACL ルールに ACE の変更が適用されるため、Cisco DNA Center は完全な ACL をデバイスに再プッシュします。WLAN フラップは発生しませんが、ACL 定義に変更が生じます。
CSCwf81439	タスクが破棄されると、Cisco DNA Center と N+1 構成のデバイス構成との間で不一致が発生します。
CSCwf88553	CBAR インターフェイスのコンプライアンス修復が失敗します。次のエラーが生成されます。 `NCSP11000: Error occurred while processing the 'complianceRemediation' request. Additional info for support: taskId: '71d06526-a361-471a-b66c-acc267369e6a'.`

バグ ID	見出し
CSCwf95418	[BAPI Schedule to Publish Inventory Details - ServiceNow Connector] で Cisco DNA Center の基本的な ITSM CMDB 同期がタイムアウトエラーで失敗することがあります。 この問題を回避するには、ServiceNow の REST および JSON Catch All Transaction Quota ルールのタイムアウト値を増やします。増やすことで、同期が正常に完了します。
CSCwh03807	デバイスで設定されている CLI **プロンプト** コマンドに特殊文字、スペース、またはタブが含まれている場合、デバイスは Cisco DNA Centerで [Managed] 状態にならず、Cisco DNA Center の [Syncing] 状態のままになります。
CSCwh16964	3 ノードクラスタがオプションパッケージのインストールが 50% の状態でスタックします。
CSCwh35302	Cisco ISE 統合の目的でデバイスをサイトに割り当てると、デバイスの可制御性とテレメトリ設定の展開が失敗し、Cisco ISE デバイスの統合が失敗します。
CSCwh35343	ファブリック SSID に対する複数のワイヤレス IP プールのサポートを追加するように要求します。
CSCwh45346	インベントリに多数のデバイスがある展開で、CMDB 同期が失敗し、[Schedule to Publish Inventory Details - ServiceNow Connector] が約 3 時間後にタイムアウトします。
CSCwh48163	Wide Area Bonjour アプリケーションがインストールされて動作可能になっても、多くの場合、[Tools] メニューにナビゲーションオプションとして Wide Area Bonjour アプリケーションが表示されません。ダッシュボードには、移動先の Wide Area Bonjour アプリケーション記号も表示されません。
CSCwh59381	NETWORK-NON-FABRIC_WIRELESS-1-150 REST イベント通知で、tenantId、tags、tntId などのキーと値のペアが返されません。
CSCwh63005	Cisco DNA Center インベントリが ServiceNow と同期されていません。ServiceNow のデバイス数は 0 です。
CSCwh88238	Cisco DNA Center のアップグレード後に、デバイスエンリッチメントの詳細の取得 API が機能しません。次のエラーが生成されます。 `The client made a request for a resource that does not exist, for get all devices API while enriching device information.`
CSCwh91534	Cisco DNA Center のアップグレード後にインベントリレポートの生成が失敗します。
CSCwh94858	アシュアランス「sdflow」サービスが予期せず再起動します。
CSCwh96829	Cisco DNA Center GUI にアクセスできません。ほとんどのサービスが「CrashLoopBackOff」状態で、一部のサービスが「CreateContainerConfigError」状態になります。

バグ ID	見出し
CSCwi28259	CLI テンプレートを使用して（かつ、[Force Push Template] オプションを選択せずに）プッシュされたモビリティアンカー設定が、Cisco DNA Center 2.3.5.4 へのアップグレード後に削除されます。 この問題は、CLI テンプレートを使用してモビリティアンカーを設定し、[Force Push Template] オプションを選択せずにコントローラをプロビジョニングした場合に発生します。
CSCwi28419	Cisco DNA Center 2.3.3.7 から Cisco DNA Center 2.3.5.4 にアップグレードすると、Cisco DNA Center インテントによって、AP への SSH アクセスを許可するように初期設定されている default-ap-join プロファイルの CLI テンプレートが上書きされます。Cisco DNA Center では、デバイスのデフォルト値を使用してデフォルトの AP プロファイルを自動的に生成されるため、SSH アクセスが無効になります。

解決済みのバグ

Cisco DNA Center 2.3.7.3

次の表に、Cisco DNA Center リリース 2.3.7.3 で解決されたバグを示します。

バグ ID	見出し
CSCvt57069	Cisco DNA Center カスタムポータルビルダー設定が保存されません。
CSCwd04618	[Edit] オプションを使用してゲストポータルにイメージをアップロードできません。
CSCwd32003	新しい AP をオンボーディングすると、すべての AP が default-ap-profile に戻り、AP がリロードされます。
CSCwd70903	レポートの生成に失敗し、次のエラーが表示されます。 `Maximum running time for the worker pod exceeded.`
CSCwe45252	一部の アシュアランス イベントが通知用に設定されている場合、SNMP が通知用のチャネルとして表示されます。ただし、アシュアランス イベントでは SNMP がサポートされていないため、SNMP 通知は機能しません。
CSCwf31064	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ メッシュロールの SiteTagInfo のエラーで Cisco DNA Center ワイヤレスプロビジョニングが失敗します。
CSCwf39432	/data/maglev/srv/diagnostics/maglev-system/workflow-worker の schema-updater ログで、ProfileAttributeMigrator の実行中に数値形式の例外が発生します。
CSCwf71596	SLAAC モードで、Cisco SD-Access ワイヤレスクライアントに IPv6 スタックの遅延関連付けが示されます。

バグ ID	見出し
CSCwf72802	Cisco DNA Center経由でのモビリティトンネルのピア作成が失敗します。次のエラーが生成されます。 `ERROR: duplicate key value violates unique constraint "mobilitypeerproperty_bk"`
CSCwf73918	Cisco DNA Center 2.3.5.4 からアップグレード後、「Policyprofilename」に関する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの再プロビジョニング設定のプレビューが失敗します。
CSCwf83571	「faultyDeviceId」が使用されている場合、API を介した交換用デバイスのマーク解除が機能しません。
CSCwf86000	AP 更新ワークフローカードが保留中または進行中の状態の場合、AP が表示されません。
CSCwf87650	Cisco DNA Center によって、PnP で取得したデバイスがインベントリから削除されても、そのデバイスが PnP から削除されません。
CSCwf87650	インベントリから PnP デバイスを削除しても、そのデバイスが PnP から削除されません。
CSCwf90876	Cisco IOS-XE 17.9.x を実行している場合、いくつかの国で 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。
CSCwf94495	[Fabric] ページからエッジノードを削除できません。
CSCwh02680	SWIM アップグレードを実行しようとすると、ワークフローの [Schedule Task] および [Clean Up]ページに重大なエラーが表示されます。重大なエラーには無効な入力が示されていますが、実際のページにはエラーも、問題の内容を示唆する内容も表示されていません。
CSCwh07308	ファブリックサイトからファブリックゾーンに切り替えると、ファブリックゾーンビューではなく、ファブリックサイトビューが表示されます。
CSCwh08579	失敗したポート割り当てタスクを表示すると、無限の API コールでブラウザがフラッディングし、タイムアウトします。
CSCwh12140	ワイヤレスコントローラをプロビジョニング後、Cisco DNA Center のコンプライアンスレポートに、そのデバイスがポリシータグ、サイトタグ、およびAP タグマッピングに準拠していないと表示される場合があります。
CSCwh13140	メッシュルート AP モードで Cisco Catalyst 9124AX をプロビジョニングすると障害が発生します。
CSCwh17495	LISP L2 インスタンス下の継承サイトのマップサーバーキーがアンカーサイトと一致しません。
CSCwh28374	Cisco DNA Center 2.3.5.3 へのアップグレードが、メッシュ設定を使用した AireOS AP プロファイルの CommonSettingsApProfileMigrator で失敗します。
CSCwh29152	パーソナル SSID の WLAN パスフレーズの更新が AireOS コントローラにプッシュされません。

バグ ID	見出し
CSCwb41361	膨大な数のベース無線レコードが原因で、Cisco DNA Centerインベントリがメモリ不足状態になる可能性があります。
CSCwh49384	Cisco SD-Access：CiscoSensorProvisioning SSIDが誤ったインターフェイスにマッピングされています。

Cisco DNA Center 2.3.7.0

次の表に、Cisco DNA Center リリース 2.3.7.0 で解決されたバグを示します。

バグ ID	見出し
CSCwb93305	AP 更新ワークフローが次のエラーで失敗します。 `AP already part of another AP refresh task "null".`
CSCwc39603	ユーザーがCisco DNA Centerで新しいイベント通知を設定すると、登録されたイベントの[Try It] オプションで次のエラーが返されることがあります。 `FAILURE - Endpoint Connection Timed Out.`
CSCwc93896	AP とワイヤレスコントローラのプロビジョニングが次のエラーで失敗します。 `NCSP10001: User intent validation failed.`
CSCwd34763	Cisco DNA Center により、ネットワークプロファイルで設定されたサイトタグではなく、デフォルト値の AP タグが設定されることがあります。
CSCwd48297	少なくとも 1 つのフレックス SSID が設定されている場合、非フレックス AP グループを作成できません。
CSCwd50441	失敗したテンプレートが、ポート割り当てプロセス中に再プッシュされます。
CSCwd53101	ワイヤレスコントローラのプロビジョニングが `NCSP11001` エラーで失敗します。
CSCwd64690	ログイン情報検証タスクで、有効なログイン情報の検証がスキップされます。
CSCwd64902	NP エラー応答（コード+パラメータ）でいくつかの NETCONF エラーシナリオの詳細が失われます。
CSCwd66496	新しいスタックメンバーがCisco Catalyst 9400 シリーズスイッチに追加された場合、Cisco DNA Center で新しいインターフェイスの「device-tracking attach-policy IPDT_POLICY」構成が自動的にプッシュダウンされません。
CSCwd77779	認証テンプレートを編集しても、デバイスの CLI が更新されません。
CSCwd96245	device_type「ise」を使用すると、ライセンス使用状況の詳細 API エンドポイントで次のエラーが返されます。 `500 Internal error.`

バグ ID	見出し
CSCwe10186	バルクファブリックゾーンの作成時に、間違ったファブリックゾーンがマルチキャストプールに割り当てられます。
CSCwe14566	ネットワークインテント「RouterProvisioning Failed」の展開で、IE-3200 拡張ノードへの Cisco DNA Center のポート割り当てが失敗します。
CSCwe24079	ライセンスモードの場合、Cisco DNA Center 内のデバイスに対して「該当なし」が表示されます。
CSCwe26616	Catalyst 9410R スイッチおよび関連するハイパーバイザファミリでは、Cisco DNA Center のイメージリポジトリ内のファミリの下に正しいデバイス数が表示されません。
CSCwe27459	バナーに、ISE 統合に関する誤った AI エンドポイント分析警告アラートが表示されます。
CSCwe32559	Cisco DNA Center VLAN レポートに、ゼロまたは 1 つのサイト VLAN レコードが返されます。 `RestApiSourceExecutor - Returned Total count 0/4.`
CSCwe37500	インベントリサービスログから大きな XML が返されると、vManage 統合がフラップします。
CSCwe38622	Meraki MR52/MR53 クラウド管理型 AP にトポロジリンクが表示されません。
CSCwe39344	ウェブフックと REST チャネルのイベント通知を設定しているときに、最初の試行後にイベント通知が機能しません。次のエラーが生成されます。 `Endpoint Connection Timed Out.`
CSCwe42089	Cisco DNA Center 内の外部設定アーカイブにファイルが保存されません。
CSCwe43814	Cisco DNA Center 2.3.5.3 にアップグレード後、（アップグレード後にコントローラをプロビジョニングせずに）フロアを変更して AP を再プロビジョニングしようとすると、プロビジョニングが失敗することがあります。
CSCwe43877	Cisco DNA Center アップグレード後に AP が再プロビジョニングされると、最初にコントローラを再プロビジョニングすることなく、新しいポリシータグとサイトタグが作成され、AP にマッピングされます。
CSCwe46169	ゲスト VN での新しい IP プールの追加が例外で失敗します。Cisco SD-Access ファブリックに、古いリリースのもので、現在はゲストボーダーワークフローをサポートしていない新しいリリースにある専用のゲストボーダー展開があります。
CSCwe52889	Meraki デバイスのシリアル番号に新しい改行文字が含まれているため、[Inventory] ウィンドウが正しくロードされません。
CSCwe54433	2.2.2.9 から 2.3.3.6 ～ 2.3.5.3 にアップグレードされたクラスタに RF プロファイルを保存できません。
CSCwe59569	ソフトウェアイメージベースおよびSMUの配信/有効化で、フラッシュクリーンアップの実行操作がスキップされます。

バグ ID	見出し
CSCwe66749	Meraki AP モデルタイプがインベントリに入力されません。
CSCwe74038	仮想ネットワークの操作によってワイヤレスコントローラのプロビジョニングがトリガーされ、WLAN が置き換えられますが、AP プロビジョニングフローはトリガーされません。
CSCwe82555	すべてのデバイスの詳細が CSV および PDF ファイルにエクスポートされません。
CSCwe89409	Cisco 1100 サービス統合型ルータのイメージ配信が失敗します。
CSCwe92274	他のファブリックデバイスにループバックインターフェイスがないため、デバイスプロビジョニングが失敗する可能性があります。
CSCwe95262	ワイヤレスコントローラ のプロビジョニングが次のエラーで失敗します。 `"NCSP11108: Error occurred while processing the request."`
CSCwe95541	ソフトウェアイメージの更新が [In Progress] 状態でスタックし、成功も失敗もしません。
CSCwe98803	Cisco DNA Center の脆弱性により、認証されていないリモートの攻撃者が、該当デバイスの内部サービスに属するリポジトリ内のデータを読み取り、変更する可能性があります。 この脆弱性は、API リクエストに対するアクセス制御の適用が不十分であることに起因します。攻撃者は、該当デバイスに巧妙に細工された API リクエストを送信することにより、この脆弱性をエクスプロイトする可能性があります。エクスプロイトに成功すると、攻撃者は、該当デバイスの内部サービスによって処理されるデータを読み取り、変更する可能性があります。 この脆弱性に対処するソフトウェア アップデートは、すでに Cisco からリリースされています。脆弱性に対処する回避策があります。 このアドバイザリは、次のリンク先で確認できます。 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ins-acc-con-nHAVDRBZ
CSCwf20392	PnP：AP 要求のプロビジョニングでは、エラーが発生し、デフォルトのサイトタグが残らない必要があります。
CSCwf20970	Cisco DNA Center ライセンスマネージャにバーチャルアカウント名が表示されない場合があります。
CSCwf25120	Cisco DNA Center で生成されたサイトタグからカスタムサイトタグに変更すると、ワイヤレスコントローラのプロビジョニングエラーが発生します。
CSCwf26803	SYSTEM_PERFORMANCE_FILESYSTEM_UTILIZATION の正確な電子メールを Cisco DNA Center が送信できない場合があります。
CSCwf28011	外部リポジトリを使用してデバイスにイメージをコピーしようとすると、NCSW32001 エラーが発生します。

バグ ID	見出し
CSCwf29125	Cisco DNA Center の config-archive-service がメモリ不足状態になり、繰り返し再起動する可能性があります。
CSCwf31445	ネットワークプロファイルで新しい VLAN グループが使用されている場合、WLAN ポリシープロファイルが作成されません。
CSCwf31965	異なるインターフェイスを使用して 2 つのネットワークプロファイルに SSID が追加された場合、非 Flex WLAN ポリシープロファイルが作成されません。
CSCwf36885	Cisco DNA Center 2.3.3.6 へのアップグレード後、多くのデバイスのインベントリ収集ステータスが「内部エラー」に変更される場合があります。
CSCwf38305	Rogue On The Wire アラートに、誤った接続スイッチが表示されます。
CSCwf39680	[Add Fabric Border Device API] の本文メモの ASN 範囲は、2 バイトではなく、4 バイトにする必要があります。
CSCwf40854	ワイヤレスコントローラ のプロビジョニングが次のエラーで失敗する可能性があります。 `NCSP11108 CFS persistence failed.`
CSCwf45762	カスタム RF プロファイルを変更するために、Cisco DNA Center によって無線が無効化されます。
CSCwh58183	Cisco DNA Center でプロトコルパックをバージョン 67 に更新すると、更新が失敗します。

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）について。	*Cisco DNA Center リリースノート（Release Notes）*
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*
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 アップグレードガイド*
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*
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 CenterCisco TelePresence Video Communication Server 管理者ガイド（Administrator Guide）*
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（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）について。	*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]
テクニカルリファレンスと検証済みソリューション。	*Cisco-Validated Solution Profiles*
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。	*Cisco DNA Center プラットフォーム ユーザー ガイド* [英語]

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...
Cisco DNA Center ITSM の統合とサポート。	*Cisco DNA Center ITSM Integration Guide* [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。

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)

© 2023–2024 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。