

Cisco Catalyst Center

リリース 3.1.3

リリースノート

目次

Catalyst Center リリース 3.1.3	3
新しいソフトウェア機能	3
動作における変更	9
解決済みの問題	10
未解決の問題	10
既知の問題	10
互換性	13
拡張性	13
サポートされるハードウェア	15
関連技術情報	16
法的情報	16

Catalyst Center リリース 3.1.3

Cisco Catalyst Center は、設計、検出、ポリシー、プロビジョニング、予測分析、インテリジェントな監視、可視性、コンプライアンスといった、最新のネットワーク管理のあらゆる側面に対応する機能を備えた、強力かつ包括的なネットワーク管理ソリューションです。Catalyst Center には、組み込みの自動化と簡素化されたワークフローが含まれており、運用の効率性と一貫性を確保するために役立ちます。

このドキュメントでは、Cisco Catalyst Center リリース 3.1.3 の機能、制限事項、およびバグについて説明します。

注 : Catalyst Center 3.1.3 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、このリリースへのアクセスを要求してください。

表 1. 初回リリース以降のこのドキュメントの変更履歴

日付	変更内容	参照先
2025 年 8 月 28 日	仮想アプライアンスの展開については、Catalyst Center と Cisco TAC のいずれも、サポートされていないハイパーバイザを使用している環境で発生する問題、バグ、または予期しない動作に関するサポートを提供できないことに注意してください。	サポートされる仮想アプライアンス
2025 年 8 月 21 日	SFTP モードが無効になっている場合でも、Catalyst Center はポート 22 経由で ssh-rsa を返すことに注意してください。ただし、キーベースのクライアント認証はサポートされていないため、Catalyst Center に対するリスクはありません。	既知の問題
2025 年 8 月 13 日	Cisco User-Defined Network (UDN) ワークフローはサポートされなくなっていることに注意してください。	推奨されなくなった機能
2025 年 8 月 11 日	Catalyst Center on ESXi の API レート制限の制約事項に関する情報が追加されました。	既知の問題
2025 年 8 月 8 日	アップグレード後にデバイスで Stealthwatch セキュリティ分析をプロビジョニングするための権限要件に関するガイドラインが追加されました。	既知の問題
2025 年 7 月 18 日	Catalyst Center on ESXi の制約事項に関する情報が追加されました。	既知の問題
2025 年 6 月 30 日	ワイヤレスコントローラの設定変更同期プロセスの機能拡張に関する情報が追加されました。	Catalyst Center の自動化
2025 年 6 月 16 日	初回リリース	—

新しいソフトウェア機能

Catalyst Center 3.1.3 のパッケージバージョン

表 2. Catalyst Center 3.1.3 のパッケージバージョン

パッケージ名	リリース 3.1.3
リリースビルドバージョン	
リリースバージョン	3.1.3-75710

パッケージ名	リリース 3.1.3
システムの更新プログラム	
システム	3.1.59
システム共通	2.730.65945
システムアドオン	0.10.35
パッケージの更新	
アクセス制御アプリケーション	2.730.65945
AI エンドポイント分析	1.11.1529
AI ネットワーク分析	4.0.30
アプリケーションおよびサービス修復	3.0.20
アプリケーション ホスティング	2.3.125041411
アプリケーションの可視性およびポリシー	2.730.117956
保証	3.130.480
アシュアランス - センサー	3.130.416
自動化 - インテリジェントキャプチャ	2.730.65945
自動化 - センサー	2.730.65945
b2b-upgrade	2.730.65899
Catalyst Center API カタログ	6.8.80-3
Catalyst Center ゲートウェイサービス	0.10.8
Cisco Catalyst Center グローバル検索	6.9.3
Cisco Catalyst Center プラットフォーム	6.9.39-3
Cisco Catalyst Center UI	3.5.138-3
Cisco Identity Services Engine	3.130.14
クラウド接続	6.10.8
クラウド接続 - コンテキストコンテンツ	7.0.7
クラウド接続 - ダイジェスタ	7.0.4
コアプラットフォーム	0.10.162-3
ディザスタリカバリ	2.730.365227

パッケージ名	リリース 3.1.3
ディザスタリカバリ - 監視	2.1.730.370045
DxHub クラウド接続	6.10.21
グループベースのポリシー分析	3.130.15
アイデンティティ管理とアクセス管理	5.4.36-3
アイデンティティ管理とアクセス管理 - UI	5.4.23-1
マルチ Cisco Catalyst Center	2.730.65945
ネットワーク コントローラ プラットフォーム	2.730.65945
ネットワーク データ プラットフォーム - 基本分析	3.130.150390
ネットワーク データ プラットフォーム - キャッシングインフラ	6.6.9
ネットワーク データ プラットフォーム - コア	6.6.118
ネットワーク データ プラットフォーム - 取り込みインフラ	6.6.10
ネットワーク データ プラットフォーム - マネージャ	6.6.100
ネットワーク データ プラットフォーム - パイプラインインフラ	6.6.119
ネットワーク データ プラットフォーム - ストレージ管理	6.6.38
プラットフォームの更新	1.2.90
RCA スクリプトのパッケージ	0.5.6
不正および aWIPS	3.1.57
SD-Access	2.730.65945
SEA アプリケーション	2.730.685124
共有マネージドサービス	0.10.14
Stealthwatch セキュリティ分析	2.730.1095371
サポート サービス	2.730.885298
システム管理操作	1.6.38
テレメトリ	4.7.15
Wide Area Bonjour	2.730.755051

Catalyst Center

表 3. Catalyst Center 3.1.3 の新機能および変更された機能

製品への影響	機能	説明
基本機能	Parallel Redundancy Protocol の設定	このワークフローは、重要なネットワークシステムで高可用性とゼロパケット損失を確保するために使用される Parallel Redundancy Protocol (PRP) チャネルのセットアップおよび管理に役立ちます。
	エネルギー管理	Catalyst Center のエネルギー管理は、エネルギー消費パターンに関するインサイトを提供します。これにより、より戦略的なエネルギー使用が可能になり、運用コストが大幅に削減されます。また、CO2 排出量も削減され、環境保全に役立ちます。
	ワイヤレスデバイス向けのロールベース アクセス コントロールの機能拡張	Catalyst Center は、特定のネットワークサイトへのユーザーのアクセス範囲を制限するサイトベースのロールベース アクセス コントロール (SRBAC) をサポートしています。ワイヤレス プロビジョニング ワークフローの使用中にサイトとデバイスにアクセスできることを確認する必要があります。
	セキュリティおよび産業用設定	Catalyst Center インベントリ内で次のデバイス設定を表示および編集できます。 - セキュリティ : Cisco Catalyst 9000 シリーズ スイッチおよび Cisco Catalyst IE スイッチでサポートされています。 - 産業用設定 : Cisco Catalyst IE スイッチでのみサポートされています。
	サイトベースのロールベース アクセス コントロールのサポート	特定のネットワークサイトへのアクセスを制限するアクセスグループを作成できます。アクセスグループはロールとサイトの組み合わせです。 Catalyst Center の機能の動作は、アクセスグループで指定されたユーザーロールとサイトによって異なります。
	異なる親サイト間のサイト割り当てに関する検証の機能拡張	ネットワーク階層では、新しい親サイトが現在の親サイトと同じネットワーク設定を共有している場合にのみ、サイトを別の親サイトの下に移動できます。新しい親サイトには、そのサイトと同じネットワークプロファイルがある必要があります。
	トランクポートの VLAN サポート	Catalyst Center は、各トランクポートに関する許可 VLAN 値およびネイティブ VLAN 値の設定をサポートしています。
使いやすさ	検出ダッシュボードの機能拡張	検出ダッシュボードに、スケジュールされたすべてのネットワーク操作を監視および管理するオプションが追加されました。
	ソフトウェア イメージ リポジトリの機能拡張	ソフトウェア イメージ リポジトリの機能が拡張され、イメージ更新のステータスを確認するオプション、特定の日にイメージ更新をスケジュールするオプション、および更新の準備状況レポートをダウンロードするオプションが追加されました。

Cisco Catalyst Assurance

表 4. Cisco Catalyst Assurance 3.1.3 の新機能および変更された機能

製品への影響	機能	説明
基本機能	AP 360 での 6 GHz 無線周波数の AFC サポート	[AP 360] ウィンドウの [Detail Information] > [RF] タブにある [Radio 2] (6-GHz 帯) には、自動周波数調整 (AFC) のサポートが含まれています。この機能により、AP と 6-GHz 無線周波数 (RF) で動作する他のデバイスの間の干渉が軽減され、標準出力 AP 動作の使用が可能になります。

製品への影響	機能	説明
	アシュアランス ダッシュボードの、サイトベースのロールベース アクセス コントロール	アシュアランスは、特定のネットワークサイトへのユーザーのアクセス範囲を制限する、サイトベースのロールベース アクセス コントロール (SRBAC) をサポートしています。範囲またはサイトベースの割り当てに基づいて、ユーザーは、ネットワークダッシュボード、クライアントダッシュボード、問題ダッシュボード、アプリケーション正常性ダッシュボード、ネットワーク サービス ダッシュボード、AI 活用型 RRM ダッシュボード、デバイス、およびクライアントにアクセスして表示できます。 サイトベースおよびロールベース アクセス コントロールが割り当てられた新しいユーザーのみが、それぞれの範囲ベースのダッシュボードおよびウィジェットへのアクセスが制限され、限られた数のデバイス、クライアント、ネットワークトポロジ、グローバルな問題、および正常性スコア設定のみを表示できます。
使いやすさ	有線クライアントおよびワイヤレスクライアントの Cisco ISE 認証失敗に対する可視性の強化	Cisco ISE GUI にログインして、有線クライアントおよびワイヤレスクライアントの Cisco ISE 認証失敗の詳細を表示する代わりに、アシュアランスの次の場所で Cisco ISE 認証失敗の詳細を表示できるようになりました。 • [Client] タブの [Assurance] > [Health] ダッシュボード • [Client 360] ウィンドウ • [Events] タブの [Assurance] > [Issues and Events] ダッシュボード • [Network Services] > [AAA] タブの [Assurance] > [Health] ダッシュボード
	サポートバンドルのコンテキスト RCA	[Activity Logs] からコンテキスト根本原因分析 (RCA) を直接開始したり、プロビジョニングの失敗に関するログをダウンロードしたりできます。
	ThousandEyes Enterprise Agent の機能拡張	[Health] > [Application] ダッシュボードから ThousandEyes Enterprise Agent をインストールおよび管理できます。

Catalyst Center プラットフォーム

表 5. Catalyst Center プラットフォーム 3.1.3 の新機能および変更された機能

製品への影響	機能	説明
基本機能	API 操作	Catalyst Center プラットフォームは、新しい API 操作をサポートしています。 詳細については、『Cisco Catalyst Center Platform User Guide』の「New and changed information」を参照してください。 API 操作の詳細については、Cisco DevNet の『Cisco Catalyst Center APIs』を参照してください。
	ネットワークデバイス レポート	この Catalyst Center プラットフォームリリースでは、新しいエネルギー管理レポートテンプレートがサポートされています。このレポートテンプレートを使用すると、ネットワークデバイスのエネルギー消費、コスト、炭素排出量、および炭素強度データを示す統合されたエネルギー管理レポートを取得でき、完全な可視性が実現されます。 詳細については、『Cisco Catalyst Center Platform User Guide』の「Run a Network Devices Report」を参照してください。

Catalyst Center の自動化

表 6. Catalyst Center 自動化 3.1.3 の新機能および変更された機能

製品への影響	機能	説明
基本機能	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのアクセスポイント (AP) プライミング	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの AP プライミングを使用すると、ユーザーは、特定のワイヤレスコントローラに参加するように AP を事前設定できます。これにより、AP は、起動時に優先ワイヤレスコントローラに自動的に参加できます。
	複数のワイヤレスコントローラ間でのプロファイルのクローン作成	Catalyst Center は、ワイヤレスコントローラ用に作成された既存プロファイルのクローン作成をサポートしています。これにより、ユーザーは、複数のコントローラ間で設定を再利用でき、手動で設定を再作成する時間が削減されます。
	Wi-Fi 7 設定の新しい AP のサポート	Catalyst Center は、Cisco IOS XE リリース 17.17.1 以降の次の AP をサポートしています。 • Cisco Catalyst 9172H シリーズ アクセスポイント • Cisco Catalyst 9172I シリーズ アクセスポイント
	新しい国コードのサポート	Catalyst Center は、Cisco IOS XE リリース 17.17.1 以降を実行しているシスコ ワイヤレスコントローラおよび AP の新しい国コードをサポートしています。 AP 内の無線は、工場出荷時設定で特定の規制ドメインに割り当てられています。国コードを使用すると、その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。
	Cisco Catalyst 9176D1 シリーズ AP および Cisco Catalyst 9176I シリーズ AP での XOR のサポート	Catalyst Center では、Cisco IOS XE リリース 17.17.1 以降を実行している場合、次の AP のスロット 0 で 2.4-GHz と 5-GHz の無線モード間のデュアルバンド (XOR) がサポートされます。 • Cisco Catalyst 9176D1 シリーズ アクセスポイント • Cisco Catalyst 9176I シリーズ アクセスポイント 注：AP が Cisco IOS XE リリース 17.15.2 を実行している場合、スロット 0 は 2.4 GHz 帯域のみをサポートします。
使いやすさ	標準出力モードでの AFC 統合の機能拡張	Catalyst Center は、AP 設定ワークフローによる AP 地理位置情報パラメータの設定をサポートしています。対象となるアクセスポイントの地理位置情報パラメータを表示および編集できます。これらは、自動周波数調整 (AFC) に利用されます。
	Cisco Catalyst 9800 シリーズ ワイヤレスコントローラでのデバイスごとの設定の機能拡張	Catalyst Center でのデバイスごとの設定の機能が拡張され、Cisco IOS XE リリース 17.12 以降を実行する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで、より多くの機能とパラメータをカスタマイズできるようになりました。
	AP 設定ワークフローの機能拡張	アクセスポイント設定ワークフローには、デバイスごとの設定の機能をサポートするために、次の AP 設定が含まれます。 • VLAN タグ • DNS 設定 • LAN ポートパラメータ • BSS カラーの設定

製品への影響	機能	説明
	ワイヤレスコントローラの設定変更同期プロセスの機能拡張	ワイヤレスコントローラ設定変更イベントによってトリガーされる同期プロセスが、パフォーマンスを向上させるために最適化されました。 • 以前のリリースでは、ワイヤレスコントローラの設定変更により、Catalyst Center が、ワイヤレスコントローラとそれに関連付けられた AP を再同期していました。この同期には、設定、動作ステータス、その他の関連データといった AP の詳細情報の更新が含まれていました。 • このリリース以降では、ワイヤレスコントローラの設定変更により、ワイヤレスコントローラの同期のみがトリガーされるようになりました。この同期中、ワイヤレスコントローラに関連付けられている AP の設定とステータスは更新されません。

Cisco Software-Defined Access

表 7. Cisco Software-Defined Access 3.1.3 の新機能および変更された機能

製品への影響	機能	説明
基本機能	Cisco SD-Access ファブリックのカスタムロール	Catalyst Center は、ユーザーが Cisco SD-Access ファブリックを作成および管理することを可能にする SD-Access 機能を使用したカスタムロールの作成をサポートしています。
使いやすさ	Cisco SD-Access ファブリックでのレイヤ 2 仮想ネットワーク設定の機能拡張	レイヤ 2 仮想ネットワークは、次の属性の設定をサポートしています。 • [Resource Guard] : Cisco SD-Access ファブリックで SSDP トラフィックをブロックまたはブロック解除するオプション。 • [Flood Access Tunnel] : レイヤ 2 仮想ネットワークのフラッドアクセストンネルを有効または無効にします。 • [Flooding Address Assignment] : 共有フラッディングアドレスまたはカスタムフラッディングアドレスを選択し、カスタムフラッディングアドレスを設定するオプション。
	Cisco SD-Access ファブリックでのサイト階層変更の機能拡張	サイトがファブリック内にある場合、新しいサイトの下にサイトを移動できます。ファブリックサイトを新しいファブリックまたはファブリック外部のサイトに移動することはできません。
	Cisco SD-Access ファブリックネットワークにおける中継のサイトへのマッピング	エリア、建物、またはフロアなどの地理的サイトに中継（SDA 中継および IP 中継）を関連付けると、サイトユーザーが、中継を効率的に管理できるようになります。

動作における変更

推奨されなくなった機能

表 8. Catalyst Center 3.1.3 の推奨されなくなった機能

機能	説明
Cisco User-Defined Network	2025 年 8 月以降、Cisco User Defined Network Plus は、Catalyst Center でサポートされる UDN ソリューションとして、UDN に取って代わります。この変更の一環として、次の GUI ワークフローはサポートされなくなりました。 • [Provision] > [Service Catalog] > [Cisco User Defined Network] • [Provision] > [Cisco User Defined Network] • [Workflow] > [Configure Cisco UDN]

機能	説明
デバイス設定学習ワークフロー	3.1.3 以降、Catalyst Center は、デバイス設定学習ワークフローをサポートしていません。 既存の設定を持つ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを管理するには、デバイスごとの設定の機能を使用できます。

解決済みの問題

[シスコのバグ検索ツール](#)を使用して、特定のバグを検索したり、このリリースに含まれるすべての解決済みバグを検索したりできます。

未解決の問題

[シスコのバグ検索ツール](#)を使用して、特定のバグを検索したり、このリリースに含まれるすべての未解決バグを検索したりできます。

文書化されたシスコ製品の問題を検索するには、ブラウザに次のように入力します： <bug_number>
site:cisco.com

既知の問題

表 9. Catalyst Center 3.1.3 の注意事項と制約事項

機能	説明
ガイドライン	
AP	このリリース以降では、ワイヤレスコントローラの設定変更により、ワイヤレスコントローラの同期のみがトリガーされます。この同期中に、Catalyst Center は次のことを行います。 - ワイヤレスコントローラ関連の設定を収集します。ただし、 - ワイヤレスコントローラに関連付けられている AP の設定とステータスは更新しません。 ワイヤレスコントローラに関連付けられている AP の更新情報 (AP ステータス、新しい AP の検出、AP 設定など) を表示するには、ワイヤレスコントローラの完全な同期を手動で実行する必要があります。完全同期の場合は、次の手順を実行します。 ステップ 1. [Inventory] ウィンドウで、ワイヤレスコントローラを選択します。 ステップ 2. [Actions] > [Inventory] > [Resync Device] を選択します。
デバイスのオンボーディング	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 デバイスの場合は、メモリ消費量の増加を回避するために、次の点に注意してください。 - デバイスを Catalyst Center に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ます。 - no netconf-yang コマンドを使用して NETCONF を無効にします。

機能	説明
ホストキーアルゴリズムとしての ssh-rsa	SFTP モードが無効になっている場合でも、Catalyst Center はポート 22 経由で ssh-rsa を返します。ただし、キーベースのクライアント認証はサポートされていないため、Catalyst Center に対するリスクはありません。ssh-rsa の SHA-1 使用によるリスクは、サーバー自体ではなく、サーバーを検証するクライアントに影響します。 ssh-rsa は、RFC 4253 で規定された公開キーアルゴリズムの 1 つであり、SSH でサーバーホストキー認証およびユーザー認証に使用されます。これは、デジタル署名に RSA アルゴリズムを使用していることを示します。 ssh-rsa 署名の場合、RFC は、デジタル署名規格 (DSS) [FIPS-186-2] に従って、署名と検証に SHA-1 ハッシュアルゴリズムの使用を義務付けています。 サーバー認証では、ssh-rsa によって採用される SHA-1 ハッシュの使用に関連するリスクの負担は、サーバーではなくクライアントにかかります。これは、クライアントが、Catalyst Center だけではなく、任意のホストになる可能性のあるサーバーの正当性を確立しようとするためです。 キーベースのクライアント認証では、ssh-rsa によって採用される SHA-1 ハッシュの使用に関連するリスクの負担は、クライアントではなくサーバーにかかります。これは、サーバーがクライアントのアイデンティティを確立しようとするためです。Catalyst Center は、キーベースの認証をサポートしていないため、クライアント認証によるリスクはありません。
Stealthwatch セキュリティ分析	以前のリリースから 3.1.3 にアップグレードする場合、デバイスで Stealthwatch セキュリティ分析をプロビジョニングするには、Stealthwatch の書き込み権限が必要です。読み取り権限のみでは、設定を編集またはプロビジョニングできません。設定の編集とプロビジョニングを有効にするために、アップグレードの前または後に権限を更新してください。
制限事項	
AP	[Inventory] ウィンドウで、ライセンス要件を満たしていない Wi-Fi 7 AP が関連付けられたワイヤレスコントローラを追加すると、Catalyst Center に、これらの AP の詳細情報を含むダイアログボックスが表示されます。これらの AP が後で到達不能になった場合でも、Catalyst Center は、引き続きダイアログボックスにそれらを表示します。
アプリケーション テレメトリ	Catalyst 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。

機能	説明
Catalyst Center on ESXi	● Catalyst Center 3.1.3 on ESXi は、次の機能を除き、Catalyst Center 2.3.7.x on ESXi がサポートするすべての機能をサポートしています。 ○ ワイヤレス : Cisco Umbrella ○ システムワークフロー : 次のバックアップおよび復元手法はサポートされていません。 ○ VMware vSphere Client スナップショット機能を使用したバックアップと復元。 ○ Catalyst Center ハードウェアアプライアンスから ESXi 上の Catalyst Center 仮想アプライアンスへのバックアップと復元。 ○ システムパフォーマンス API : 次の API はサポートされていません。 ○ /dna/intent/api/v1/diagnostics/system/performance ○ /dna/intent/api/v1/diagnostics/system/performance/history ● 公式の API ドキュメントに記載されている API レート制限ポリシーが適用されません。その結果、エラー応答 429 でシステムによって自動的にスロットルまたはブロックされることなく、推奨される API リクエスト制限を超える可能性があります。 API レート制限を超えることは推奨されませんが、サービスの中断やセキュリティの脆弱性がすぐに発生することはほとんどありません。ただし、API を過剰に使用すると、次のような問題が発生する場合があります。 ○ パフォーマンスの低下 : API リクエストの量が多いと、Catalyst Center プラットフォームの全体的なパフォーマンスに影響を与え、応答時間が遅くなったり、一時的に使用できなくなったりする可能性があります。 ○ リソースの競合 : API アクティビティが増加すると、追加のシステムリソースが消費され、他のプラットフォーム機能やユーザー体験に影響を与える可能性があります。 ○ 予期しない動作 : 場合によっては、API レート制限を超えると、予期しないプラットフォームの動作やエラーがトリガーされる可能性があります。 最適なプラットフォームのパフォーマンスと安定性を確保するために、ドキュメント化された API レート制限ポリシーに従うことをお勧めします。 ● グループベースのポリシー分析の場合、24 時間および 12 時間の Sankey チャートのサマリーは Catalyst Center on ESXi では使用できません。 ● ESXi 上で動作する Catalyst Center では、3 ノード HA はサポートされていません。vSphere HA クラスターを作成および使用するための VMware vSphere の実装と要件については、VMware vSphere 製品ドキュメントを参照してください。 ● Catalyst Center on ESXi は、次の VMware vSphere 機能をサポートしていません。 ○ 耐障害性 ○ VM の一時停止と再開 ○ VM の複製 ○ スナップショット（バックアップとして） ● 管理インターフェイスとエンタープライズインターフェイスを設定するには、VMware vSphere UI を使用して仮想マシンを手動で作成し、Maglev 設定ウィザードまたはインストール設定ウィザードを使用して両方のインターフェイスを設定します。詳細については、『Cisco Catalyst Center on ESXi Deployment Guide』の「Deploy a Virtual Appliance」を参照してください。
Cisco AireOS ワイヤレスコントローラ	FIPS 対応の Cisco AireOS ワイヤレスコントローラを Catalyst Center にオンボードする際、NA サーバーの CA 証明書の不一致が原因で、デバイスのコンプライアンスチェックが失敗する場合があります。この問題を解決するには、次の手順を実行します。 ステップ 1. Catalyst Center UI から、NA サーバーの CA 証明書をダウンロードします。 証明書ファイルを自動的にダウンロードするには、次の URL を使用します。 <code>http://<Catalyst Center IP address>/ca/pem</code> 注 : CA 証明書ファイルをダウンロードするには、HTTP メソッドを使用します。 ステップ 2. この証明書ファイルを Cisco AireOS ワイヤレスコントローラにダウンロードします。 ● Cisco AireOS ワイヤレスコントローラのメインメニューから、[Commands] > [Download File] を選択します。 ● ファイルタイプとして [NA-Serv-CA-Certificate] を選択します。 ● 必要な転送モードを選択します。 ● 必要な設定の有効なデータを入力し、[Download] をクリックします。

機能	説明
製品内ヘルプ	- オンラインヘルプとインタラクティブヘルプはライトモードでのみ使用でき、ダークモードはサポートされていません。 - インタラクティブヘルプのウィジェットを右上、右中央、および右下の位置に配置している場合、カーソルがウィジェットの右端を超えると、ウィジェットが点滅することがあります。

互換性

Catalyst Center 互換性マトリックス

ルータ、スイッチ、ワイヤレス AP などのデバイス、および Catalyst Center の各アプリケーションでサポートされているソフトウェアリリースについては、[Cisco Catalyst Center 互換性マトリックス](#)を参照してください。

Cisco SD-Access 互換性マトリックス

Catalyst 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 互換性マトリックス](#)』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

Catalyst 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

画面解像度 :

- 最小 : 1368 X 768 ピクセル
- 推奨 : 1920 X 1080 ピクセル

Catalyst 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。

サポートされているアップグレードパス

Catalyst Center の現在のリリースへのアップグレードについては、『[Cisco Catalyst Center Upgrade Guide](#)』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 Catalyst 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 Catalyst Center Administrator Guide](#)』の「Configure System Settings」の章の「Use the Validation Tool」を参照してください。

拡張性

Catalyst Center のスケール

Catalyst Center のスケールの数値については、[Cisco Catalyst Center のデータシート](#)を参照してください。

Cisco Connected Mobile Experiences のサポート

Catalyst Center は、Cisco Connected Mobile Experiences (CMX) リリース 10.6.2 以降をサポートしています。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。
- Catalyst Center は、CMX TLS/SSL 証明書を検証します。Catalyst Center の 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。Catalyst Center と CMX の間のサービスの中断を回避するには、Catalyst Center 3.1.3 にアップ
グレードする前に、CMX SSL/TLS 証明書を設定し、Catalyst 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。認証局（CA）によって署名されていない自己署名サーバー証明
書は、信頼されません。

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

Catalyst Center 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 10. AA 適合レベルの WCAG 2.1 標準と制限事項

WCAG 成功基準	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	－
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	－

WCAG 成功基準	サポート	制限事項
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	—
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	—

サポートされるハードウェア

サポートされ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 **Catalyst Center** を提供しています。次のバージョンの **Catalyst Center** アプライアンスを使用できます。

- 第 2 世代
 - 44 コアアプライアンス : DN2-HW-APL (Cisco UCS C220 M5)
 - 44 コア プロモーション アプライアンス : DN2-HW-APL-U (Cisco UCS C220 M5)
 - 56 コアアプライアンス : DN2-HW-APL-L (Cisco UCS C220 M5)
 - 56 コア プロモーション アプライアンス : DN2-HW-APL-L-U (Cisco UCS C220 M5)
 - 112 コアアプライアンス : DN2-HW-APL-XL (Cisco UCS C480 M5)
 - 112 コア プロモーション アプライアンス : DN2-HW-APL-XL-U (Cisco UCS C480 M5)
- 第 3 世代
 - 32 コアアプライアンス : DN3-HW-APL (Cisco UCS C220 M6)
 - 56 コアアプライアンス : DN3-HW-APL-L (Cisco UCS C220 M6)
 - 80 コアアプライアンス : DN3-HW-APL-XL (Cisco UCS C240 M6)

揮発性に関する報告

物理アプライアンスの揮発性に関するステートメントについては、『[Statement of Volatility for Cisco UCS Hardware](#)』を参照してください。

サポートされる仮想アプライアンス

Catalyst Center 3.1.3 は、オンプレミス環境向けに VMware ESXi 上の仮想アプライアンス (VA) として展開することがサポートされています。Catalyst Center と Cisco TAC のいずれも、他のハイパーバイザを使用している環境で発生する問題、バグ、または予期しない動作に関するサポートを提供できません。

サポートされるファームウェア

Catalyst Center 3.1.3 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 DN2-HW-APL、DN2-HW-APL-L、DN2-HW-APL-XL の Cisco IMC バージョン 4.3(2.240077)
- アプライアンスモデル DN3-HW-APL、DN3-HW-APL-L、DN3-HW-APL-XL の Cisco IMC バージョン 4.3(5.250030)

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 Catalyst 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 Catalyst 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 Catalyst Center High Availability Guide](#)』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。

関連技術情報

Catalyst Center に関するその他のドキュメントについては、『[Cisco Catalyst Center Documentation](#)』を参照してください。

法的情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧については、www.cisco.com/go/trademarks をご覧ください。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語は、シスコと他社との間のパートナーシップ関係を意味するものではありません。(1110R)

このマニュアルで使用している **IP** アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2025 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。