Cisco Catalyst Center プラットフォーム リリース 2.3.7.x ユーザーガイド

最終更新：2026 年 5 月 14 日

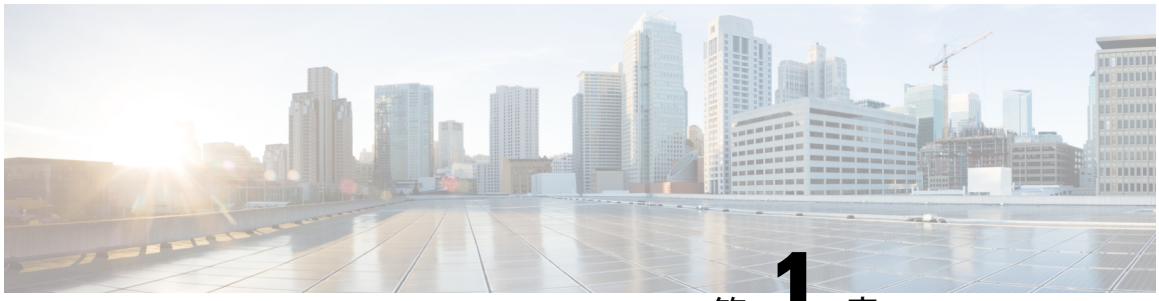
シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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)

© 2023–2025 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

新機能および変更された機能に関する情報

新機能および変更情報

表 *1 : Catalyst Center* プラットフォーム *2.3.7.10* の新機能と変更された機能

機能	説明
新しい API	
なし	—
API の機能拡張	
デバイス API	このリリースでは、到達可能性正常性ステータスパラメータが、次のデバイス API の応答にオプションの属性として含まれています。 • 指定されたデバイス ID（Uuid）のデバイスデータを取得します。 • 指定された複雑なフィルタと集約関数に基づいて、ネットワークデバイスのリストを取得します。 • 指定されたクエリパラメータに基づいてネットワークデバイスの詳細を取得します。
ネットワーク設定 API	このリリースでは、configureDevice 属性がネットワークデバイス同期クレデンシャル API でクエリパラメータとして追加されます。
廃止された API	
なし	—
後方互換性を損なう API の変更	
なし	—

表 *2 : Catalyst Center* プラットフォーム *2.3.7.9* の新機能および変更された機能

機能	説明	記載場所
[インベントリレポート（Inventory Report）]	この Catalyst Center プラットフォーム リリースでは、新しい **インベントリ** レポートテンプレート「**All Data Version 2.0**」がサポートされています。 この新しいすべてのデータビューでは、ネットワークデバイス、時間の経過に伴うデバイスの分散、サイト別のデバイス数、デバイスタイプ別のデバイス数、ソフトウェアバージョン別のデバイス数、ファブリックロール別のデバイス数に関する詳細情報が、より効率的に表示されます。	詳細については、以下を参照してください。 • インベントリレポートの実行 （178 ページ）。 • **新しいレポートテンプレート**は、「Cisco Catalyst Center Release Notes」にあります。
新しい API		
アプリケーション API	Catalyst Center プラットフォーム は、次のアプリケーション API をサポートしています。 • GET <cluster-ip>/dna/data/api/v1/networkApplications ネットワークアプリケーションのリストを、エクスペリエンスおよび正常性メトリックとともに取得します。 • GET <cluster-ip>/dna/data/api/v1/networkApplications/count 基本的なフィルタ処理を適用して、ネットワークアプリケーションの合計数を取得します。 • POST <cluster-ip>/dna/data/api/v1/networkApplications/trendAnalytics ネットワークアプリケーションに関連するトレンド分析データを取得します。 新しいアプリケーション API にアクセスするには、メニューアイコンをクリックし、[**Platform**> **Developer Toolkit** > **APIs**] を選択します。 [**Policy**] ドロップダウンリストを展開し、[**Applications**] を選択します。	

機能	説明	記載場所
アプリケーションポリシー API	Catalyst Center プラットフォーム では、次のアプリケーションポリシー API がサポートされています。 • GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices ネットワークデバイスのリストとアプリケーションの可視性ステータスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/count 指定されたアプリケーション可視性ステータスフィルタのネットワークデバイス数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableAppTelemetry 複数のネットワークデバイスでアプリケーションテレメトリ機能を有効にします。 • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableAppTelemetry 複数のネットワークデバイスでアプリケーションテレメトリ機能を無効にします。 • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/enableCbar 複数のネットワークデバイスで CBAR 機能を有効にします。 • POST <cluster-ip>/dna/intent/api/v1/applicationVisibility/networkDevices/disableCbar 複数のネットワークデバイスで CBAR 機能を無効にします。 • GET <cluster-ip>/dna/intent/api/v1/qosPolicySetting アプリケーション QoS ポリシー設定を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/qosPolicySetting アプリケーション QoS ポリシー設定を更新します。 新しいアプリケーションポリシー API にアクセスするには、メニューアイコンをクリックし、[**Platform** > **Developer Toolkit** > **APIs**] を選択します。 [Policy] ドロップダウンリストを展開し、[Application Policy] を選択します。	

機能	説明	記載場所
Cisco Integrated Management Controller (IMC) APIs	Catalyst Center プラットフォーム は、次の Cisco IMC API をサポートしています。 • GET <cluster-ip>/dna/system/api/v1/ciscoImcs Catalyst Center ノードの Cisco IMC 設定を取得します。 • POST <cluster-ip>/dna/system/api/v1/ciscoImcs Catalyst Center ノードに Cisco IMC 設定を追加します。 • GET <cluster-ip>/dna/system/api/v1/ciscoImcs/${id} Catalyst Center ノードの Cisco IMC 設定を取得します。 • PUT <cluster-ip>/dna/system/api/v1/ciscoImcs/${id} Catalyst Centerノードの Cisco IMC 設定を更新します。 • DELETE <cluster-ip>/dna/system/api/v1/ciscoImcs/${id} Catalyst Center ノードの Cisco IMC 設定を削除します。 新しい Cisco IMC API にアクセスするには、メニューアイコンをクリックし、[**Platform** > **Developer Toolkit** > **APIs**] を選択します。 [**Appliance**] ドロップダウンリストを展開し、[**Cisco IMC**] を選択します。	

機能	説明	記載場所
コンプライアンス API		

機能	説明	記載場所
	Catalyst Center プラットフォーム は、次のコンプライアンス API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v1/networkBugs/trials ネットワークデバイスでバグ検出用のトライアルを作成します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/trials ネットワークデバイスでのバグ検出に関するトライアルの詳細を取得します。 • POST <cluster-ip>/dna/intent/api/v1/networkBugs/triggerScan サポートされているネットワークデバイスのバグスキャンをトリガーします。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs/count ネットワークデバイスに影響するバグの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs ネットワークデバイスに影響するバグを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id} ID でネットワークバグを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id}/networkDevices/count バグのネットワークバグデバイスの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id}/networkDevices バグのネットワークバグデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/bugs/${id}/networkDevices/${networkDeviceId} ネットワークデバイス ID でバグのネットワークバグデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/count ネットワークバグデバイスの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices ネットワークバグデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId} デバイス ID でネットワークバグデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs/count ネットワークデバイスに影響するバグの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs ネットワークデバイスに影響するバグを取得します。	

機能	説明	記載場所
	• GET <cluster-ip>/dna/intent/api/v1/networkBugs/results/networkDevices/${networkDeviceId}/bugs/${id} デバイス ID とバグ ID で、ネットワークデバイスに影響するバグを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/resultsTrend/count 時系列のネットワークバグ数結果のトレンドを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkBugs/resultsTrend 時間の経過に伴うネットワークバグ結果のトレンドを取得します。 • POST <cluster-ip>/dna/intent/api/v1/fieldNotices/trials ネットワークデバイスでフィールド通知検出のトライアルを作成します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/trials ネットワークデバイスでのフィールド通知検出に関するトライアルの詳細を取得します。 • POST <cluster-ip>/dna/intent/api/v1/fieldNotices/triggerScan サポートされているネットワークデバイスのフィールド通知スキャンをトリガーします。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices/count ネットワークデバイスに影響するフィールド通知の数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices ネットワークデバイスに影響するフィールド通知を取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id} ネットワークデバイスに影響する Field Notice を ID で取得できます。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id}/networkDevices/count 通知の Field Notice ネットワークデバイスの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id}/networkDevices 通知用の Field Notice ネットワークデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/notices/${id}/networkDevices/${networkDeviceId} ネットワークデバイス ID で通知の Field Notice ネットワークデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/count Field Notice ネットワークデバイスの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices Field Notice ネットワークデバイスを取得します。	

機能	説明	記載場所
	• GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId} デバイス ID で Field Notice ネットワークデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices/count ネットワークデバイスに影響するフィールド通知の数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices ネットワークデバイスに影響するフィールド通知を取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/results/networkDevices/${networkDeviceId}/notices/${id} デバイス ID と通知 ID で、ネットワークデバイスに影響する Field Notice を取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/resultsTrend/count 時間の経過に伴う Field Notice 結果のトレンドを取得します。 • GET <cluster-ip>/dna/intent/api/v1/fieldNotices/resultsTrend 時間の経過に伴う Field Notice 結果のトレンドを取得します。 • POST <cluster-ip>/dna/intent/api/v1/securityAdvisories/trials ネットワークデバイスでセキュリティアドバイザリ検出用のトライアルを作成します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/trials ネットワークデバイスでのセキュリティアドバイザリ検出に関するトライアルの詳細を取得します。 • POST <cluster-ip>/dna/intent/api/v1/securityAdvisories/triggerScan サポートされているネットワークデバイスのセキュリティ アドバイザリ スキャンをトリガーします。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/count ネットワークデバイスに影響を与えるセキュリティアドバイザリの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories ネットワークデバイスに影響するセキュリティアドバイザリを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id} ネットワークデバイスに影響するセキュリティアドバイザリを ID ごとに取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id}/networkDevices/count セキュリティアドバイザリのセキュリティ アドバイザリ ネットワーク デバイスの数を取得します。	

機能	説明	記載場所
	• GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id}/networkDevices セキュリティアドバイザリのセキュリティ アドバイザリ ネットワーク デバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/advisories/${id}/networkDevices/${networkDeviceId} ネットワークデバイス ID でセキュリティアドバイザリのセキュリティ アドバイザリ ネットワーク デバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/count セキュリティ アドバイザリ ネットワーク デバイスの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices セキュリティ アドバイザリ ネットワーク デバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId} ネットワークデバイス ID でセキュリティ アドバイザリ ネットワーク デバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId}/advisories/count ネットワークデバイスに影響を与えるセキュリティアドバイザリの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId}/advisories ネットワークデバイスに影響するセキュリティアドバイザリを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/results/networkDevices/${networkDeviceId}/advisories/${id} デバイス ID とアドバイザリ ID で、ネットワークデバイスに影響するセキュリティアドバイザリを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/resultsTrend/count 時系列のセキュリティアドバイザリ結果のトレンドを取得します。 • GET <cluster-ip>/dna/intent/api/v1/securityAdvisories/resultsTrend 時系列のセキュリティアドバイザリ結果のトレンドを取得します。 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次を選択します。 **[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。	

機能	説明	記載場所
Configuration Archive API	Catalyst 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/networkDeviceConfigFiles ネットワークデバイス構成ファイルの詳細を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/count ネットワーク デバイス構成ファイルの数。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/${id} 構成ファイルの詳細を ID で取得します。 • POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/${id}/downloadMasked マスクされたデバイス設定をダウンロードします。 • POST <cluster-ip>/dna/intent/api/v1/networkDeviceConfigFiles/${id}/downloadUnmasked マスクなし（未加工）のデバイス設定を ZIP としてダウンロードします。 新しい設定テンプレート 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次を選択します。 [**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 APIs**] を選択します。	

機能	説明	記載場所
設定テンプレート API		

機能	説明	記載場所
	Catalyst Center プラットフォームは、次の Configuration Templates API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites CLI テンプレートに関連付けられたネットワークプロファイルを取得します。 • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/count CLI テンプレートに接続されているネットワークプロファイルの数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites ネットワークプロファイルを Day-N CLI テンプレートに関連付けます。 • POST <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/bulk ネットワークプロファイルのリストを Day-N CLI テンプレートに関連付けます。 • DELETE <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/bulk Day-N CLI テンプレートからネットワークプロファイルのリストを切り離します。 • DELETE <cluster-ip>/dna/intent/api/v1/templates/${templateId}/networkProfilesForSites/${profileId} Day-N CLI テンプレートからネットワークプロファイルを切り離します。 • GET <cluster-ip>/templates/${templateId}/versions テンプレートバージョンを取得します。 • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/versions/${versionId} テンプレートバージョンを取得します。 • GET <cluster-ip>/dna/intent/api/v1/templates/${templateId}/versions/count テンプレートバージョン数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/templates/${templateId}/versions/commit 新しいバージョンのテンプレートをコミットします。 • GET <cluster-ip>/dna/intent/api/v1/projects テンプレートプロジェクトを取得します。 • POST <cluster-ip>/dna/intent/api/v1/projects テンプレートプロジェクトを作成します。 • PUT <cluster-ip>/dna/intent/api/v1/projects/${projectId} テンプレートプロジェクトを更新します。 • GET <cluster-ip>/dna/intent/api/v1/projects/${projectId} テンプレートプロジェクトを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/projects/${projectId}	

機能	説明	記載場所
	テンプレートプロジェクトを削除します。 • GET <cluster-ip>/dna/intent/api/v1/projects/count テンプレートプロジェクト数を取得します。 新しい設定テンプレート 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次を選択します。 [**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 Templates APIs**] を選択します。	

機能	説明	記載場所
デバイス API		

機能	説明	記載場所
	Catalyst Center プラットフォーム は、次のデバイス API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithoutCleanup 設定をクリーンアップせずにネットワークデバイスを削除します。 • POST <cluster-ip>/dna/intent/api/v1/networkDevices/deleteWithCleanup 設定クリーンアップを使用してネットワークデバイスを削除します。 • GET <cluster-ip>/dna/data/api/v1/aaaServices 指定されたパラメータに対して AAA サービスのリストを取得します。 • GET <cluster-ip>/dna/data/api/v1/aaaServices/count 指定されたパラメータの AAA サービスの総数を取得します。 • GET <cluster-ip>/dna/data/api/v1/aaaServices/${id} サービスの ID に一致する特定の AAA サービスの詳細を取得します。 • POST <cluster-ip>/dna/data/api/v1/aaaServices/query 指定された複雑なフィルタのセットに対して AAA サービスのリストを取得します。 • POST <cluster-ip>/dna/data/api/v1/aaaServices/query/count 指定された複雑なフィルタのセットに対する AAA サービスの総数を取得します。 • POST <cluster-ip>/dna/data/api/v1/aaaServices/summaryAnalytics 指定された一連の複雑なフィルタに関する AAA サービスのサマリー分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/aaaServices/topNAnalytics 指定された複雑なフィルタのセットに関する AAA サービスの上位 N の分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/aaaServices/trendAnalytics 指定された一連の複雑なフィルタに関する AAA サービスのトレンド分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/aaaServices/${id}/trendAnalytics サービスの ID に一致する特定の AAA サービスのトレンド分析データを取得します。 • GET <cluster-ip>/dna/data/api/v1/dhcpServices 指定されたパラメータの DHCP サービスのリストを取得します。 • GET <cluster-ip>/dna/data/api/v1/dhcpServices/count 指定されたパラメータの DHCP サービスの総数を取得します。 • GET <cluster-ip>/dna/data/api/v1/dhcpServices/${id}	

機能	説明	記載場所
	サービスの ID に一致する特定の DHCP サービスの詳細を取得します。 • POST <cluster-ip>/dna/data/api/v1/dhcpServices/query 指定された複雑なフィルタのセットに対する DHCP サービスのリストを取得します。 • POST <cluster-ip>/dna/data/api/v1/dhcpServices/query/count 指定された複雑なフィルタのセットに対する DHCP サービスの総数を取得します。 • POST <cluster-ip>/dna/data/api/v1/dhcpServices/summaryAnalytics 指定された一連の複雑なフィルタに関する DHCP サービスの概要分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/dhcpServices/topNAnalytics 指定された複雑なフィルタのセットに関する DHCP サービスの上位 N の分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/dhcpServices/trendAnalytics 指定された一連の複雑なフィルタに関する DHCP サービスのトレンド分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/dhcpServices/${id}/trendAnalytics サービスの ID に一致する特定の DHCP サービスのトレンド分析データを取得します。 • GET <cluster-ip>/dna/data/api/v1/dnsServices 指定されたパラメータの DNS サービスのリストを取得します。 • GET <cluster-ip>/dna/data/api/v1/dnsServices/count 指定されたパラメータの DNS サービスの総数を取得します。 • GET <cluster-ip>/dna/data/api/v1/dnsServices/${id} サービスの ID に一致する特定の DNS サービスの詳細を取得します。 • POST <cluster-ip>/dna/data/api/v1/dnsServices/query 指定された複雑なフィルタのセットに対する DNS サービスのリストを取得します。 • POST <cluster-ip>/dna/data/api/v1/dnsServices/query/count 指定された複雑なフィルタのセットに対する DNS サービスの総数を取得します。 • POST <cluster-ip>/dna/data/api/v1/dnsServices/summaryAnalytics 指定された一連の複雑なフィルタに関する DNS サービスの概要分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/dnsServices/topNAnalytics 指定された複雑なフィルタのセットに関する DHCP サービスの上位 N の分析データを取得します。	

機能	説明	記載場所
	• POST <cluster-ip>/dna/data/api/v1/dnsServices/trendAnalytics 指定された一連の複雑なフィルタに関する DNS サービスのトレンド分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/dnsServices/${id}/trendAnalytics サービスの ID に一致する特定の DNS サービスのトレンド分析データを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules ネットワークデバイスのスケジュールされたメンテナンス期間を取得します。 • POST <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules ネットワークデバイスのメンテナンススケジュールを作成します。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/count スケジュールされたメンテナンスウィンドウの合計数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/${id} メンテナンススケジュール情報を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/${id} メンテナンススケジュール情報を更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/networkDeviceMaintenanceSchedules/${id} メンテナンススケジュールを削除します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices ネットワークデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/${id} 単一のネットワークデバイスの詳細を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/count ネットワークデバイスの数をカウントします。 • POST <cluster-ip>/dna/intent/api/v1/networkDevices/query フィルタを使用してネットワークデバイスをクエリします。 • POST <cluster-ip>/dna/intent/api/v1/networkDevices/query/count フィルタを使用してネットワークデバイスの数をカウントします。 • POST <cluster-ip>/dna/data/api/v1/networkDevices/topNAnalytics ネットワークデバイスに関連する上位 N 分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/interfaces/${id}/trendAnalytics 指定された時間範囲のインターフェイスのトレンド分析データ。	

機能	説明	記載場所
	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、[**Platform**>**Developer Toolkit** > **APIs**] を選択します。 [Know Your Network] ドロップダウンリストを展開し、[Devices] を選択します。	
デバイス交換 API	Catalyst Center プラットフォーム は、次のデバイス交換 API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceReplacements/${id} 障害のあるデバイスを交換用のデバイスに置き換えるデバイス交換ワークフローのステータスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceReplacements すべてのデバイス交換ワークフローのステータスを取得します。 新しいデバイス交換 API にアクセスするには、メニューアイコンをクリックして、[**Platform**> **Developer Toolkit** > **APIs**] を選択します。 [**Site Management**] ドロップダウンリストを展開し、[**Device Replacement**] を選択します。	
ファブリックワイヤレス API	Catalyst Center プラットフォーム は、次のファブリックワイヤレス API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/switchWirelessSetting スイッチから SDA ワイヤレスの詳細を取得します。 • PUT <cluster-ip>//dna/intent/api/v1/sda/fabrics/${fabricId}/wirelessMulticast SDA ワイヤレスマルチキャストを更新します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/wirelessMulticast SDA ワイヤレスマルチキャストを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/switchWirelessSetting スイッチワイヤレス設定およびローリング AP アップグレード管理。 • POST <cluster-ip>//dna/intent/api/v1/sda/fabrics/${fabricId}/switchWirelessSetting/reload ワイヤレスコントローラクリーンアップのためにスイッチをリロードします。 新しいファブリックワイヤレス 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 **[Connectivity]** ドロップダウンリストを展開して、**[Fabric Wireless]** を選択します。	

機能	説明	記載場所
正常性およびパフォーマンス API	Catalyst Center プラットフォーム は、次の正常性およびパフォーマンス API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/diagnosticTasks/${id} 診断タスクを ID で取得します。 • GET <cluster-ip>/dna/intent/api/v1/diagnosticTasks/${id}/detail 診断タスクの詳細を ID で取得します。 新しい正常性およびパフォーマンス 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [**System**] ドロップダウンリストを展開し、[**Health and Performance**] を選択します。	
ライセンス API	Catalyst Center プラットフォーム は、次のライセンス API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/connectionModeSetting CSSM 接続モードを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/connectionModeSetting CSSM 接続モードを更新します。 • GET <cluster-ip>/dna/system/api/v1/license/status システムライセンスのステータス。 • POST <cluster-ip>/dna/system/api/v1/license/register スマートライセンシングの登録。 • POST <cluster-ip>/dna/system/api/v1/license/renew スマートライセンスの更新操作。 • POST <cluster-ip>/dna/system/api/v1/license/deregister スマートライセンシングの登録解除。 • GET <cluster-ip>/dna/system/api/v1/license/lastOperationStatus システムライセンスの直前の操作ステータス。 新しいライセンス 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次を選択します。 **[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、**[Licenses]** を選択します。	

機能	説明	記載場所
ネットワーク設定 API		

機能	説明	記載場所
	Catalyst Center プラットフォーム は、次のネットワーク設定 API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/templates ネットワークプロファイルに関連付けられた CLI テンプレートを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/templates/count ネットワークプロファイルに関連付けられた CLI テンプレートの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools グローバル IP アドレスプールを取得します。 • POST <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools グローバル IP アドレスプールを作成します。 • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${id} グローバル IP アドレスプールを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${id} グローバル IP アドレスプールを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${id} グローバル IP アドレスプールを削除します。 • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${globalIpAddressPoolId}/subpools グローバル IP アドレスプールのサブプール ID を取得します。 • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/${globalIpAddressPoolId}/subpools/count グローバル IP アドレスプールのサブプールをカウントします。 • GET <cluster-ip>/dna/intent/api/v1/ipam/globalIpAddressPools/count グローバル IP アドレスプールをカウントします。 • GET <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools IP アドレスサブプールを取得します。 • POST <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools IP アドレスサブプールを予約（作成）します。 • GET <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/${id} IP アドレスサブプールを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/{id} IP アドレスサブプールを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/{id}	

機能	説明	記載場所
	IP アドレスサブプールをリリースします。 • GET <cluster-ip>/dna/intent/api/v1/ipam/siteIpAddressPools/count IP アドレスサブプールをカウントします。 新しいネットワーク設定 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次を選択します。 **[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、[Network Settings] を選択します。	

機能	説明	記載場所
SD-Access API		

機能	説明	記載場所
	Catalyst Center プラットフォーム は、次の SDA API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/sda/pendingFabricEvents 保留中のファブリックイベントを取得します。 • POST <cluster-ip>/dna/intent/api/v1/sda/pendingFabricEvents/apply 保留中のファブリックイベントを適用します。 • GET <cluster-ip>/dna/data/api/v1/fabricSummary ファブリックエンティティの概要を読み取ります。 • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries 正常性の概要を含むファブリックサイトのリストを読み取ります。 • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries/${id} ID から正常性概要を使用してファブリックサイトを読み取ります。 • GET <cluster-ip>/dna/data/api/v1/fabricSiteHealthSummaries/${id}/trendAnalytics 指定された時間範囲のファブリックサイトのトレンド分析データ。 • GET <cluster-ip> /dna/data/api/v1/fabricSiteHealthSummaries/count ファブリックサイト数を読み取ります。 • GET <cluster-ip> //dna/data/api/v1/virtualNetworkHealthSummaries 正常性の概要を含む仮想ネットワークのリストを読み取ります。 • GET <cluster-ip> /dna/data/api/v1/virtualNetworkHealthSummaries/${id} ID から仮想ネットワークの正常性概要を読み取ります。 • GET <cluster-ip> /dna/data/api/v1/virtualNetworkHealthSummaries/count 仮想ネットワーク数を読み取ります。 • GET <cluster-ip> /dna/data/api/v1/virtualNetworkHealthSummaries/${id}/trendAnalytics 指定された時間範囲の仮想ネットワークの傾向分析データ。 • GET <cluster-ip> //dna/data/api/v1/transitNetworkHealthSummaries 正常性の概要を含むトランジットネットワークのリストを読み取ります。 • GET <cluster-ip> /dna/data/api/v1/transitNetworkHealthSummaries/${id} ID からトランジットネットワークの正常性概要を読み取ります。 • GET <cluster-ip> /dna/data/api/v1/transitNetworkHealthSummaries/count トランジットネットワーク数を読み取ります。 • GET <cluster-ip> /dna/data/api/v1/transitNetworkHealthSummaries/${id}/trendAnalytics	

機能	説明	記載場所
	指定された時間範囲のトランジットネットワークの傾向分析データ。 新しい SD-Access 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次を選択します。 [**Platform** > **Developer Toolkit** > **APIs**] の順に選択します。 [Connectivity] ドロップダウンリストを展開し、[SDA] を選択します。	

機能	説明	記載場所
センサー API		

機能	説明	記載場所
	Catalyst Center プラットフォーム は、次のセンサー API をサポートしています。 • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles 指定された条件に一致する ICAP パケットキャプチャファイルを一覧表示します。 • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles/count 指定された条件に一致するパケットキャプチャファイルの総数を取得します。 • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles/${id} 特定の ICAP パケットキャプチャファイルの詳細を取得します。 • GET <cluster-ip>/dna/data/api/v1/icap/captureFiles/${id}/download 特定の ICAP パケットキャプチャファイルをダウンロードします。 • GET <cluster-ip>/dna/data/api/v1/icap/spectrumSensorReports 指定された AP Mac の WLC によって送信されたスペクトルセンサーレポートを取得します。 • GET <cluster-ip>/dna/data/api/v1/icap/spectrumInterferenceDeviceReports 指定された AP Mac に関して WLC から送信されるスペクトル干渉デバイスレポートを取得します。 • POST <cluster-ip>/dna/data/api/v1/icap/clients/${id}/stats 指定された期間の特定のクライアントの統計情報を取得します。 • POST <cluster-ip>/dna/data/api/v1/icap/radios/${id}/stats 指定された期間の特定の無線統計情報を取得します。 • POST <cluster-ip>/dna/intent/api/v1/icapSettings/deploy 指定された ICAP 設定インテントをプレビューなしで展開します。 • POST <cluster-ip>/dna/intent/api/v1/icapSettings/deploy/${id}/deleteDeploy プレビューなしでデバイスの ICAP 設定を削除します。 • POST <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels プレビュー承認用の ICAP 設定インテントを作成します。 • POST <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${id}/deleteDeploy デバイス上の ICAP 設定を削除するための ICAP インテントのワークフローを作成します。 • GET <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/networkDeviceStatusDetails ネットワークデバイスごとに ICAP 設定ステータスを取得します。 • POST	

機能	説明	記載場所
	<cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/networkDevices/${networkDeviceId}/config ICAP 設定インテントのデバイスの CLI を生成します。 • GET <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/networkDevices/${networkDeviceId}/config ICAP インテントのデバイスの CLI を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId} アクティビティ ID によって ICAP 設定インテントを破棄します。 • DELETE <cluster-ip>/dna/intent/api/v1/icapSettings/configurationModels/${previewActivityId}/deploy アクティビティ ID によって ICAP 設定インテントを展開します。 • GET <cluster-ip>/dna/intent/api/v1/icapSettings/deviceDeployments デバイス展開ステータスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/icapSettings/deviceDeployments/count デバイス展開ステータス数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/icapSettings 基本的なフィルタリングをサポートしながら、展開された ICAP 設定を取得します。 • GET <cluster-ip>/dna/intent/api/v1/icapSettings/count 展開された ICAP 設定の数を取得しますが、基本的なフィルタリングをサポートします。 新しいセンサー 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次を選択します。[**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、[**Sensors**] を選択します。	

機能	説明	記載場所
サイト設計 API	Catalyst Center プラットフォーム は、次のサイト設計 API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/accessPointPositions アクセスポイントの位置を取得します。 • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/accessPointPositions/count アクセスポイント位置数を取得します。 • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/accessPointPositions/bulkChange アクセスポイントの位置を編集します。 • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/bulk 計画されたアクセスポイントの位置を追加します。 • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/bulkChange 計画されたアクセスポイントの位置を編集します。 • DELETE <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/${id} 計画されたアクセスポイントの位置を削除します。 • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions 計画されたアクセスポイントの位置を取得します。 • GET <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/count 計画されたアクセスポイントの位置数を取得します。 • POST <cluster-ip>/dna/intent/api/v2/floors/${floorId}/plannedAccessPointPositions/assignAccessPointPositions 計画済みアクセスポイントを運用中のフロアに割り当てます。 新しいサイト設計 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次を選択します。 **[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、[Site Design] を選択します。	

機能	説明	記載場所
SWIM API	Catalyst Center プラットフォーム は、次の SWIM API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v1/images/ccoSync Cisco.com からソフトウェアイメージの同期を開始します。 • GET <cluster-ip>dna/intent/api/v1/siteWiseImagesSummary 指定されたサイトのイメージサマリーを返します。 • DELETE <cluster-ip>/dna/intent/api/v1/images/${id} イメージを削除します。 • POST <cluster-ip>/dna/intent/api/v1/images/${id}/sites/${siteId}/tagGolden ゴールデンイメージにタグ付けします。 • POST <cluster-ip>/dna/intent/api/v1/images/${id}/sites/${siteId}/untagGolden ゴールデンイメージのタグを解除します。 新しい SWIM 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次を選択します。**[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、[Software Image Management (SWIM)] を選択します。	
タグ API	Catalyst Center プラットフォーム は、次のタグ API をサポートしています。 • PUT <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations/bulk ネットワークデバイスに関連付けられているタグを更新します。 • PUT <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations/bulk インターフェイスに関連付けられたタグを更新します。 新しいタグ 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次を選択します。**[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [**Operational Tasks**] ドロップダウンリストを展開し、[**Tag**] を選択します。	

機能	説明	記載場所
タスク API	Catalyst Center プラットフォーム は、次のタスク API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/activities/${activityId}/triggeredJobs/count トリガーされたジョブの数をアクティビティ ID ごとに取得します。 • GET <cluster-ip>/dna/intent/api/v1/activities アクティビティを取得します。 • GET <cluster-ip>/dna/intent/api/v1/activities/count アクティビティ数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/activities/${id} ID ごとにアクティビティを取得します。 • GET <cluster-ip>/dna/intent/api/v1/activities/${activityId}/triggeredJobs トリガーされたジョブをアクティビティ ID ごとに取得します。 新しいタスク 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次を選択します。**[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Operational Tasks] ドロップダウンリストを展開し、[Task] を選択します。	

機能	説明	記載場所
ワイヤレス API		

機能	説明	記載場所
	Catalyst Center プラットフォーム は、次のワイヤレス API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups アンカーグループを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups アンカーグループを作成します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/${id} ID ごとにアンカーグループを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/${id} アンカーグループを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/${id} ID ごとにアンカーグループを削除します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/anchorGroups/count アンカーグループの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/anchorCapableDevices アンカー対応デバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists AP 認証リストを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists AP 認証リストを作成します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/${id} ID で AP 認証リストを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/${id} AP 認証リストを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/${id} AP 認証リストを削除します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apAuthorizationLists/count AP 承認リスト数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/apAuthorizationLists ネットワークデバイス ID で AP 認証リストを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles	

機能	説明	記載場所
	電力プロファイルを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles 電力プロファイルの作成 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/${id} ID で電力プロファイルを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/${id} ID ごとに電力プロファイルを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/${id} ID で電力プロファイルを削除します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/powerProfiles/count 電力プロファイル数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/meshApNeighbours メッシュ AP ネイバーを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/meshApNeighbours/count メッシュ AP ネイバー数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id}/update SSID を更新またはオーバーライドします。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/ssids/overrideAtSites SSID が上書きされているサイトを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles AP プロファイルを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles AP プロファイルの作成 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} ID で AP プロファイルを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} ID ごとに AP プロファイルを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/${id} ID ごとに AP プロファイルを削除します。	

機能	説明	記載場所
	• GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/apProfiles/count AP プロファイル数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags ワイヤレスプロファイルのすべてのサイトタグを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/bulk ワイヤレスプロファイルの複数のサイトタグを一括で作成します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/${siteTagId} ワイヤレスプロファイルの特定のサイトタグを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/${siteTagId} ワイヤレスプロファイルの特定のサイトタグを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/${siteTagId} ワイヤレスプロファイルから特定のサイトタグを削除します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/siteTags/count ワイヤレスプロファイルのサイトタグの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags ワイヤレスプロファイルのすべてのポリシータグを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/bulk ワイヤレスプロファイルの複数のポリシータグを一括で作成します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/${policyTagId} ワイヤレスプロファイルの特定のポリシータグを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/${policyTagId} ワイヤレスプロファイルの特定のポリシータグを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/${policyTagId} ワイヤレスプロファイルから特定のポリシータグを削除します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id}/policyTags/count ワイヤレスプロファイルのポリシータグの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/${networkDeviceId}/assignAnchorManagedApLocations WLC の アンカー管理対象 AP の場所を割り当てます。 • GET <cluster-ip>/dna/intent/api/v1/wireless/accesspoint-configuration/count アクセスポイント設定数を取得します。	

機能	説明	記載場所
	新しいワイヤレス 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Connectivity] ドロップダウンリストを展開して、[Wireless] を選択します。	
ベータ版 API		

機能	説明	記載場所
有線 API		

機能	説明	記載場所
	このリリースでは、Catalyst Center プラットフォーム には次の Campus Automation ベータ API が含まれています。 • POST <cluster-ip>dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels 有線デバイスの目的の設定の設定モデルを作成します。 • PUT <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature} 有線デバイス上の目的のレイヤ 2 機能の設定を更新します。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/deployed/layer2/${feature} 有線デバイスに展開されたレイヤ 2 機能の設定を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/deployed/layer2/${feature}/count デバイスに展開されたレイヤ 2 機能の設定数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/deploy 有線デバイスに目的の設定機能を展開します。 • PUT <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2 有線デバイスで、目的のレイヤ 2 機能の設定を更新します。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/supported/layer2 有線デバイスでサポートされているレイヤ 2 機能を取得してください。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/serviceDeployments サービス展開ステータスを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId}/config 設定モデルのデバイス設定を生成します。 • POST <cluster-ip>/dna/intent/api/v1/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId}/deploy ネットワークデバイスに設定モデルを展開します。 • DELETE <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature} 有線デバイスの目的のレイヤ 2 機能の設定を削除します。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature}	

機能	説明	記載場所
	有線デバイスで目的のレイヤ 2 機能の設定を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId} 設定モデルを削除します。 • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature} 有線デバイスで目的のレイヤ 2 機能の設定を作成します。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2/${feature}/count 有線デバイス上の目的のレイヤ 2 機能の設定数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/configurationModels/${previewActivityId}/config 設定モデルのデバイス設定を取得します。 • POST <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2 有線デバイスで目的のレイヤ 2 機能の設定を作成します。 • GET <cluster-ip>/dna/intent/api/v1/wired/networkDevices/${networkDeviceId}/configFeatures/intended/deviceDeployments デバイス展開ステータスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/intent/api/v1/wired/networkDevices/${id}/configFeatures/intended/layer2 有線デバイスで目的のレイヤ 2 機能の設定を取得します。 Wired 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次を選択します。[**Platform** > **Developer Toolkit** > **APIs**] を選択します。 [**Connectivity**] ドロップダウンリストを展開して、[**Wired**] を選択します。	
API の機能拡張		
コンプライアンス API	このリリースでは、デバイス API のコンプライアンス詳細のリクエストクエリパラメータに `status` と `remediationSupported` プロパティが追加され、`remediationSupported` という新しい応答パラメータが導入されています。	

機能	説明	記載場所
デバイス API	次のデバイス API に、新しい応答属性 `physicalPortCount` および `virtualPortCount` が含まれます。 • 指定されたデバイス ID（Uuid）のデバイスデータを取得します。 • 指定されたクエリパラメータに基づいてネットワークデバイスの詳細を取得します。 • 指定された複雑なフィルタと集約関数に基づいて、ネットワークデバイスのリストを取得します。	
SD-Access API	• ポートチャネル削除 API に、`PortchannelIds` および `connectedDeviceType` リクエストパラメータが含まれます。`networkDeviceId` パラメータがオプションになりました。 • このリリースでは、`isGlobalAuthenticationProfile` という新しいリクエストパラメータが Get Authentication Profiles API に追加されます。 • `fabricId` リクエスト属性が、Get Authentication Profiles および Update Authentication Profiles API でオプションになりました。	
ワイヤレス API	このリリースでは、以下の通りです。 • `anchorGroupName`、`vlanGroupName`、`additionalInterfaces`、`apZones`、`apZoneName`、`rfProfileName`、および `ssids` 属性は、Update Wireless Profile、Create Wireless Profile、Get Wireless Profiles、および Get Wireless Profile by ID API に含まれています。 • `provisioningStatus` と呼ばれる新しい応答パラメータが、Get Access Point Configuration API に含まれています。	
廃止された API サンセットバナーは、特定の API が廃止されることを示します。 （注） 代替の API がある場合、詳細はそれぞれの廃止された API の [**Features**] タブに記載されています。		
ディスカバリ API	このリリースでは、次のディスカバリ API がサンセットとしてマークされています。 POST <cluster-ip>/dna/intent/api/v1/discovery すべてのディスカバリを削除します。	

機能	説明	記載場所
イベント管理 API	このリリースでは、次のイベント管理 API が「Sunset」としてマークされ、対応する新しい API がサポートされています。	
	廃止された API	**新しい API**
	POST <cluster-ip>/dna/intent/api/v1/event/subscription イベントサブスクリプションを作成します。	POST <cluster-ip>/dna/intent/api/v1/event/subscription/rest Rest/ウェブフック イベントサブスクリプションを作成します。
	PUT <cluster-ip>/dna/intent/api/v1/event/subscription イベントサブスクリプションを更新します。	PUT <cluster-ip>/dna/intent/api/v1/event/subscription/rest Rest/ウェブフック イベントサブスクリプションを取得します。
	GET <cluster-ip>/dna/intent/api/v1/event/subscription イベントサブスクリプションを取得します。	GET <cluster-ip>/dna/intent/api/v1/event/subscription/rest Rest/ウェブフック イベントサブスクリプションを取得します。
ネットワーク設定 API	このリリースでは、次のネットワーク設定 API が廃止されます。 • POST <cluster-ip>/dna/intent/api/v1/global-pool グローバルプールを作成します。 • GET <cluster-ip>/dna/intent/api/v1/global-pool グローバルプールを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/global-pool グローバルプールを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/global-pool/${id} グローバル IP プールを削除します。 • POST <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool/${siteId} IP サブプールを予約します。 • GET <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool 予約済み IP サブプールを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool/${siteId} 予約済み IP サブプールを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/reserve-ip-subpool/${id} 予約済み IP サブプールをリリースします。	

機能	説明	記載場所
SD-Access API		

機能	説明	記載場所
	このリリースでは、次の SD-Access ビジネス API が廃止されます。 ファブリック作成 API • POST <cluster-ip>/dna/intent/api/v1/business/sda/fabric ファブリックサイトを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric SDA ファブリック情報を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/fabric SDA ファブリックを削除します。 SDA ファブリック API のファブリックサイト • POST <cluster-ip>/dna/intent/api/v1/business/sda/fabric-site SDA ファブリックにサイトを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric-site SDA ファブリックからサイトを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/fabric-site SDA ファブリックからサイトを削除します。 SDA ファブリック API のファブリックゾーン • POST <cluster-ip>/dna/intent/api/v1/business/sda/fabric-zone SDA ファブリックにファブリックゾーンを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric-zone SDA ファブリックからファブリックゾーンを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/fabric-zone SDA ファブリックからファブリックゾーンを削除します。 コントロールプレーンデバイス API • POST <cluster-ip>/dna/intent/api/v1/business/sda/control-plane-device コントロールプレーンデバイスを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/control-plane-device コントロールプレーンデバイスを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/control-plane-device SDA ファブリックのコントロールプレーンデバイスを削除します。	

機能	説明	記載場所
	エッジデバイスロール割り当て API • POST <cluster-ip>/dna/intent/api/v1/business/sda/edge-device エッジデバイスを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/edge-device エッジデバイスを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/edge-device エッジデバイスを削除します。 ボーダーデバイスロール割り当て API • POST <cluster-ip>/dna/intent/api/v1/business/sda/border-device SDA ファブリックにボーダーデバイスを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/border-device SDA ファブリックからボーダーデバイスの詳細を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/border-device SDA ファブリックからボーダーデバイスを削除します。 デフォルト認証テンプレート（プロファイル）API • PUT <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile デフォルト認証プロファイルを更新します。 • POST <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile デフォルト認証プロファイルを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile デフォルト認証プロファイルを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/authentication-profile デフォルト認証プロファイルを削除します。 仮想ネットワーク作成 API	

機能	説明	記載場所
	• POST <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network SDA ファブリックに VN を追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network SDA ファブリックから VN を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network SDA ファブリックから VN を削除します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/virtual-network/summary 仮想ネットワークの概要を取得します。 SDA セグメント API • POST <cluster-ip>/dna/intent/api/v1/business/sda/virtualnetwork/ippool SDA 仮想ネットワークに IP プールを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/virtualnetwork/ippool SDA 仮想ネットワークから IP プールを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/virtualnetwork/ippool SDA 仮想ネットワークから IP プールを削除します。 ユーザーデバイスのポート割り当て API • POST <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/user-device ユーザーデバイスのポート割り当てを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/user-device ユーザーデバイスのポート割り当てを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/user-device ユーザーデバイスのポート割り当てを削除します。 アクセスポイントへのポート割り当て API • POST <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/access-point アクセスポイントのポート割り当てを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/access-point アクセスポイントのポート割り当てを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/access-point アクセスポイントのポート割り当てを削除します。 SDA	

機能	説明	記載場所
	マルチキャスト API • POST <cluster-ip>/dna/intent/api/v1/business/sda/multicast マルチキャストを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/multicast マルチキャストを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/multicast マルチキャストを削除します。 有線デバイスプロビジョニング API • POST <cluster-ip>/dna/intent/api/v1/business/sda/provision-device 有線デバイスをプロビジョニングします。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/provision-device プロビジョニングされた有線デバイスを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/provision-device プロビジョニングされた有線デバイスを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/business/sda/provision-device 有線デバイスを再プロビジョニングします。 仮想ネットワーク API • POST <cluster-ip>/dna/intent/api/v1/virtual-network スケーラブルグループを含む仮想ネットワークを追加します。 • GET <cluster-ip>/dna/intent/api/v1/virtual-network スケーラブルグループを含む仮想ネットワークを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/virtual-network スケーラブルグループを含む仮想ネットワークを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/virtual-network スケーラブルグループを使用して仮想ネットワークを更新します。 トランジットネットワークおよびピアネットワーク API	

機能	説明	記載場所
	• POST <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network トランジットピアネットワークを追加します。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network トランジットピアネットワークを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/transit-peer-network トランジットピアネットワークを削除します。 SDA ファブリック API からのデバイス情報の取得 • GET <cluster-ip>/dna/intent/api/v1/business/sda/device SDA ファブリックからデバイス情報を取得します。 指定されたデバイス API の SDA デバイスロールを取得する • GET <cluster-ip>/dna/intent/api/v1/business/sda/device/role SDA ファブリックでデバイスロールを取得します。 ファブリック数の取得 - Cyclops API • GET <cluster-ip>/dna/intent/api/v1/business/sda/fabric/count SDA ファブリック数を取得します。	
セキュリティアドバイザリ API	このリリースでは、次のセキュリティアドバイザリ API が廃止予定としてマークされています。 • GET <cluster-ip>/dna/intent/api/v1/security-advisory/advisory/aggregate アドバイザリの概要を取得します。 • GET <cluster-ip>/dna/intent/api/v1/security-advisory/device/${deviceId} アドバイザリデバイスの詳細を取得します。 • GET <cluster-ip>/dna/intent/api/v1/security-advisory/advisory アドバイザリリストを取得します。 • GET <cluster-ip>/dna/intent/api/v1/security-advisory/device/${deviceId}/advisory デバイスごとにアドバイザリを取得します。 • GET <cluster-ip>/dna/intent/api/v1/security-advisory/advisory/${advisoryId}/device アドバイザリごとにデバイスを取得します。	

機能	説明	記載場所
SWIM API	このリリースでは、次の SWIM API が廃止予定としてマークされています。 • GET <cluster-ip>/dna/intent/api/v1/image/importation ソフトウェアイメージの詳細を取得します。 • GET <cluster-ip>/dna/intent/api/v1/image/importation/device-family-identifiers デバイスファミリ識別子を取得します。 • POST <cluster-ip>/dna/intent/api/v1/image/importation/golden ゴールデンイメージとしてタグ付けします。 • GET <cluster-ip>/dna/intent/api/v1/image/importation/golden/site/${siteId}/family/${deviceFamilyIdentifier}/role/${deviceRole}/image/${imageId}/Swagger doc イメージのゴールデンタグステータスを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/image/importation/golden/site/${siteId}/family/${deviceFamilyIdentifier}/role/${deviceRole}/image/${imageId} イメージのゴールデンタグを削除します。	
後方互換性を損なう API の変更		
なし	—	

表 *3 : Catalyst Center* プラットフォーム リリース *2.3.7.6* の新機能および変更された機能

機能	説明
Catalyst Center アプリへの名前変更	ServiceNow ストアの Cisco DNA Center アプリは、アプリバージョン 2.3.1 以降、Catalyst Center にブランド変更されています。 アプリケーションの以前のバージョンは Cisco DNA Center と呼ばれます。これらのバージョンは、対応する Catalyst Center リリースで引き続き使用できます。
新しい API	

機能	説明
シスコの信頼できる証明書 API	Catalyst Center プラットフォーム は、次の信頼できる証明書のインポート API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v1/trustedCertificates/import 信頼できる証明書をトラストストアにインポートします。.pem または .der ファイルを入力として受け入れます。 新しい信頼できる証明書のインポート 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 **[System]** ドロップダウンリストを展開し、**[Cisco Trusted Certificates]** を選択します。

機能	説明
クライアント API	Catalyst Center プラットフォームは、次のクライアント API をサポートしています。 • GET <cluster-ip>/dna/data/api/v1/clients 基本的なフィルタ処理機能とソート機能も提供しながら、クライアントのリストを取得します。 • GET <cluster-ip>/dna/data/api/v1/clients/${id} MAC アドレスに一致する特定のクライアント情報を取得します。 • GET <cluster-ip>/dna/data/api/v1/clients/count 基本的なフィルタ処理を適用して、クライアントの合計数を取得します。 • POST <cluster-ip>/dna/data/api/v1/clients/query 集約属性もサポートしながら、複雑なフィルタを適用してクライアントのリストを取得します。 • POST <cluster-ip>/dna/data/api/v1/clients/query/count 複雑なフィルタを適用してクライアントの数を取得します。 • POST <cluster-ip>/dna/data/api/v1/clients/trendAnalytics クライアントに関連するトレンド分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/clients/${id}/trendAnalytics 指定された期間の特定のクライアント情報を取得します。 • POST <cluster-ip>/dna/data/api/v1/clients/summaryAnalytics クライアントに関連するサマリー分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/clients/topNAnalytics クライアントに関連する上位 N 個の分析データを取得します。 新しいクライアント 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次を選択します。 **[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、**[Clients]** を選択します。

機能	説明
コンプライアンス API	Catalyst Center プラットフォームは、次のコンプライアンス API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v1/compliance/networkDevices/${id}/issues/remediation/provision コンプライアンス改善。 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次を選択します。 **[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。

機能	説明
デバイス API	

機能	説明
	Catalyst Center プラットフォーム は、次のデバイス API をサポートしています。 • PUT <cluster-ip>/dna/intent/api/v1/networkDevices/resyncIntervalSettings グローバル再同期間隔を更新します。 • PUT <cluster-ip>/dna/intent/api/v1/networkDevices/${id}/resyncIntervalSettings ネットワークデバイスの再同期間隔を更新します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/${id}/resyncIntervalSettings ネットワークデバイスの再同期間隔を取得します。 • POST <cluster-ip>/dna/intent/api/v1/networkDevices/resyncIntervalSettings/override 再同期間隔をオーバーライドします。 • GET <cluster-ip>/dna/data/api/v1/assuranceEvents アシュアランスイベントを照会します。 • GET <cluster-ip>/dna/data/api/v1/assuranceEvents/count イベント数を数えます。 • GET <cluster-ip>/dna/data/api/v1/assuranceEvents/${id} 単一のアシュアランスイベントの詳細を取得します。 • GET <cluster-ip>/dna/data/api/v1/assuranceEvents/${id}/childEvents 指定されたワイヤレス クライアント イベントの子イベントのリストを取得します。 • POST <cluster-ip>/dna/data/api/v1/assuranceEvents/query フィルタを使用してアシュアランスイベントを照会します。 • POST <cluster-ip>/dna/data/api/v1/assuranceEvents/query/count フィルタを使用してイベント数を数えます。 • PUT <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/${id} 指定された ID の正常性スコア定義を更新します。 • GET <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions 指定されたフィルタのすべての正常性スコア定義を取得します。 • GET <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/${id} 指定された ID の正常性スコア定義を取得します。 • GET <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/count 指定されたフィルタに基づいて正常性スコア定義の数を取得します。

機能	説明
	• POST <cluster-ip>/dna/intent/api/v1/healthScoreDefinitions/bulkUpdate 正常性スコア定義を更新します。 • GET <cluster-ip>/dna/data/api/v1/networkDevices 指定されたクエリパラメータに基づいてネットワークデバイスの詳細を取得します。 • GET <cluster-ip>/dna/data/api/v1/networkDevices/{id} 指定されたデバイス ID（Uuid）のデバイスデータを取得します。 • GET <cluster-ip>/dna/data/api/v1/networkDevices/count 指定されたクエリパラメータに基づいてネットワークデバイスの総数を取得します。 • POST <cluster-ip>/dna/data/api/v1/networkDevices/query 指定された複雑なフィルタと集約関数に基づいて、ネットワークデバイスのリストを取得します。 • POST <cluster-ip>/dna/data/api/v1/networkDevices/query/count 指定された複雑なフィルタと集約関数に基づいて、ネットワークデバイスの総数を取得します。 • POST <cluster-ip>/dna/data/api/v1/networkDevices/trendAnalytics トレンド分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/networkDevices/${id}/trendAnalytics 指定した時間範囲のネットワークデバイスのトレンド分析データ。 • POST <cluster-ip>/dna/data/api/v1/networkDevices/summaryAnalytics ネットワークデバイスに関連するサマリー分析データを取得します。 • GET <cluster-ip>/dna/data/api/v1/interfaces すべてのネットワークデバイスからインターフェイスと統計データを取得します。 • GET <cluster-ip>/dna/data/api/v1/interfaces/${id} 指定されたインターフェイス ID（インスタンス Uuid）のインターフェイスデータを統計データとともに取得します。 • GET <cluster-ip>/dna/data/api/v1/interfaces/count 指定した時間範囲のネットワーク デバイス インターフェイスの総数を取得します。開始時刻と終了時刻が指定されていない場合は、最新のインターフェイスの総数を返します。

機能	説明
	• POST <cluster-ip>/dna/data/api/v1/interfaces/query 指定された複雑なフィルタと集約関数に基づいて、ネットワークデバイス全体のインターフェイスのリストを取得します。 • POST <cluster-ip>/dna/data/api/v1/interfaces/query/count ネットワークデバイス全体のインターフェイスの総数。 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次を選択します。 **[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。
ファブリックワイヤレス API	Catalyst Center プラットフォーム は、次のファブリックワイヤレス API をサポートしています。 • PUT <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/vlanToSsids VLAN への SSID マッピングを追加、更新、または削除します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/vlanToSsids/count SSIDからIPプールへのマッピングを持つすべてのファブリックサイトの数を返します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/vlanToSsids VLANからSSIDへのマッピングを持つすべてのファブリックサイトを返します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/vlanToSsids/count ファブリックサイトのSSIDにマッピングされている VLAN の数を返します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabrics/${fabricId}/vlanToSsids ファブリックサイト内の VLAN にマッピングされている VLAN と SSID を取得します。 新しいファブリックワイヤレス 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 **[Connectivity]** ドロップダウンリストを展開して、**[Fabric Wireless]** を選択します。

機能	説明
正常性およびパフォーマンス API	Catalyst Center プラットフォーム は、次の正常性およびパフォーマンス API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationSets すべての検証セットを取得します。 • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationSets/${id} 検証セットの検証の詳細を取得します。 • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows/count 検証ワークフローの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows/${id} 検証ワークフローの詳細を取得します。 • GET <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows 検証ワークフローのリストを取得します。 • POST <cluster-ip>/dna/ intent/api/v1/diagnosticValidationWorkflows 検証を実行するためのワークフローを送信します。 • DELETE <cluster-ip>/dna/intent/api/v1/diagnosticValidationWorkflows/${id} 検証ワークフローを削除します。 新しい正常性およびパフォーマンス 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次を選択します。 **[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、**[Health and Performance]** を選択します。

機能	説明
問題 API	

機能	説明
	Catalyst Center プラットフォーム は、次の問題 API をサポートしています。 • GET <cluster-ip>/dna/data/api/v1/assuranceIssues 指定された一連のフィルタの問題の詳細を取得します。 • GET <cluster-ip>/dna/data/api/v1/assuranceIssues/${id} 指定された問題 ID の問題のすべての詳細と推奨されるアクションを取得します。 • GET <cluster-ip>/dna/data/api/v1/assuranceIssues/count 指定された一連のフィルタの問題の総数を取得します。 • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/query 指定された一連のフィルタの問題の詳細を取得します。 • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/query/count 指定された一連のフィルタの問題の総数を取得します。 • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/topNAnalytics 問題の上位 N 個の分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/summaryAnalytics 問題の概要分析データを取得します。 • POST <cluster-ip>/dna/data/api/v1/assuranceIssues/trendAnalytics 問題のトレンド分析データを取得します。 • POST <cluster-ip>/dna/intent/api/v1/assuranceIssues/resolve 指定された問題のリストを解決します。 • POST <cluster-ip>/dna/intent/api/v1/assuranceIssues/ignore 指定された問題のリストを無視します。 • POST <cluster-ip>/dna/intent/api/v1/assuranceIssues/${id}/update 選択したフィールドを更新して、指定された問題を更新します。 • GET <cluster-ip>/dna/intent/api/v1/customIssueDefinitions 指定されたフィルタに基づいてすべてのカスタム問題定義を取得します。 • POST <cluster-ip>/dna/intent/api/v1/customIssueDefinitions 新しいユーザー定義の問題定義を作成します。 • GET <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/count 指定されたフィルタに基づいて、カスタム問題定義の総数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/${id}

機能	説明
	指定されたカスタム問題定義 ID のカスタム問題定義を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/${id} 指定された ID に基づいて既存のカスタム問題定義を更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/customIssueDefinitions/${id} 既存のカスタム問題定義を削除します。 • GET <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions 指定されたフィルタのすべての問題トリガー定義を返します。 • GET <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions/${id} 指定された ID の問題トリガー定義を取得します。 • GET <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions/count 指定されたフィルタに基づいて、システム定義の問題定義の数を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/systemIssueDefinitions/${id} 問題トリガー定義を更新します。 新しい問題 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次を選択します。 **[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、[Issues] を選択します。
ライセンス API	Catalyst Center プラットフォーム は、次のライセンス API をサポートしています。 • PUT <cluster-ip>/dna/intent/api/v1/licenseSetting ライセンス設定を更新します。 • GET <cluster-ip>/dna/intent/api/v1/licenseSetting ライセンス設定を取得します。 新しいライセンス 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次を選択します。 **[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、**[Licenses]** を選択します。

機能	説明
ネットワーク設定 API	

機能	説明
	Catalyst Center プラットフォーム は、次のネットワーク設定 API をサポートしています。 • PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/timeZoneSettings サイトのタイムゾーンを設定します。 • PUT <cluster-ip>/dna/intent/api/v1/sites/{id}/bannerSettings サイトのバナー設定を行います。 • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/telemetrySettings サイトのテレメトリ設定を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/telemetrySettings サイトのテレメトリ設定を行います。 • POST <cluster-ip>/dna/intent/api/v1/telemetrySettings/apply サイトのテレメトリ設定に準拠するようにデバイスのテレメトリ設定を更新します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/deviceCredentials サイトのデバイスログイン情報の設定を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/deviceCredentials/status 指定されたサイトでネットワークデバイスのログイン情報の同期ステータスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/deviceCredentials/apply ネットワークデバイスのログイン情報を同期します。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/deviceCredentials サイトのデバイスログイン情報の設定を更新します。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/aaaSettings サイトの AAA 設定を行います。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/dnsSettings サイトの DNS 設定を行います。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/dhcpSettings サイトの DHCP 設定を行います。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/ntpSettings サイトの NTP 設定を行います。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${id}/imageDistributionSettings

機能	説明
	サイトのイメージ配信設定を行います。 • GET<cluster-ip>/dna/intent/api/v1/sites/${id}/aaaSettings サイトの AAA 設定を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/dnsSettings サイトの DNS 設定を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/dhcpSettings サイトの DHCP 設定を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/ntpSettings サイトの NTP 設定を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${id}/imageDistributionSettings サイトのイメージ配信設定を取得します。 新しいネットワーク設定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次を選択します。 **[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、[Network Settings] を選択します。

機能	説明
SDA API	

機能	説明
	Catalyst Center プラットフォーム は、次の SDA API をサポートしています。 エクストラネット API • DELETE <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies エクストラネットポリシーを削除します。 マルチキャスト API • GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks マルチキャスト仮想ネットワークを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sda/multicast マルチキャストを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks マルチキャスト仮想ネットワークを更新します。 • GET <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/count マルチキャスト仮想ネットワーク数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks/${id} ID でマルチキャスト仮想ネットワークを削除します。 • POST <cluster-ip>/dna/intent/api/v1/sda/multicast/virtualNetworks マルチキャスト仮想ネットワークを追加します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/multicast マルチキャストを更新します。 ポートチャネル API • POST <cluster-ip>/dna/intent/api/v1/sda/portChannels ポートチャネルを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/portChannels ポートチャネルを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/portChannels ポートチャネルを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/portChannels ポートチャネルを削除します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/portChannels/{id} ID でポートチャネルを削除します。

機能	説明
	• GET <cluster-ip>/dna/intent/api/v1/sda/portChannels/count ポートチャネル数を取得します。 トランジットネットワーク API • GET <cluster-ip>/dna/intent/api/v1/sda/transitNetworks トランジットネットワークを取得します。 • POST <cluster-ip>/dna/intent/api/v1/sda/transitNetworks トランジットネットワークを追加します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/transitNetworks トランジットネットワークを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/transitNetworks/${id} ID でトランジットネットワークを削除します。 • GET <cluster-ip>/dna/intent/api/v1/sda/transitNetworks/count トランジットネットワーク数を取得します。 レイヤ 2 仮想ネットワーク API • PUT <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks レイヤ 2 仮想ネットワークを更新します。 • GET <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks/count レイヤ 2 仮想ネットワーク数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks/${id} ID でレイヤ 2 仮想ネットワークを削除します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks レイヤ 2 仮想ネットワークを削除します。 • POST <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks レイヤ 2 仮想ネットワークを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/layer2VirtualNetworks レイヤ 2 仮想ネットワークを取得します。 レイヤ 3 仮想ネットワーク API

機能	説明
	• POST <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks レイヤ 3 仮想ネットワークを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks レイヤ 3 仮想ネットワークを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks レイヤ 3 仮想ネットワークを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks レイヤ 3 仮想ネットワークを削除します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks/${id} ID でレイヤ 3 仮想ネットワークを削除します。 • GET <cluster-ip>/dna/intent/api/v1/sda/layer3VirtualNetworks/count レイヤ 3 仮想ネットワーク数を取得します。 新しい SDA 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Connectivity] ドロップダウンリストを展開し、[SDA] を選択します。

機能	説明
サイト API	Catalyst Center プラットフォームは、次のサイト API をサポートしています。 • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries サイトの正常性の概要のリストを読み取ります。 • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/${id} サイト ID でサイトの正常性の概要データを読み取ります。 • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/count サイト数を読み取ります。 • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/summaryAnalytics サイトの正常性データの集約された概要を読み取ります。 • POST <cluster-ip>/dna/data/api/v1/siteHealthSummaries/summaryAnalytics サイトの正常性データの集約された概要を照会します。 • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/trendAnalytics ネットワーク内のサイトのグループに関するトレンド分析データを読み取ります。 • GET <cluster-ip>/dna/data/api/v1/siteHealthSummaries/${id}/trendAnalytics ネットワーク内の特定のサイトのトレンド分析データを読み取ります。 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次を選択します。 **[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。

機能	説明
サイト設計 API	

機能	説明
	Catalyst Center プラットフォーム は、次のサイト設計 API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v1/areas エリアを作成します。 • GET <cluster-ip>/dna/intent/api/v1/areas/${id} エリアを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/areas/${id} エリアを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/areas/${id} エリアを削除します。 • POST <cluster-ip>/dna/intent/api/v2/buildings ビルディングを作成します。 • GET <cluster-ip>/dna/intent/api/v2/buildings/${id} ビルディングを取得します。 • PUT <cluster-ip>/dna/intent/api/v2/buildings/${id} ビルディングを更新します。 • DELETE <cluster-ip>/dna/intent/api/v2/buildings/${id} ビルディングを削除します。 • POST <cluster-ip>/dna/intent/api/v2/floors フロアを作成します。 • GET <cluster-ip>/dna/intent/api/v2/floors/${id} フロアを取得します。 • PUT <cluster-ip>/dna/intent/api/v2/floors/${id} フロアを更新します。 • DELETE <cluster-ip>/dna/intent/api/v2/floors/${id} フロアを削除します。 • POST <cluster-ip>/dna/intent/api/v2/floors/${id}/uploadImage フロア画像をアップロードします。 • POST <cluster-ip>/dna/intent/api/v1/sites/bulk サイトを作成します。 • GET <cluster-ip>/dna/intent/api/v1/sites

機能	説明
	サイトを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/count サイト数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/networkDevices/assignToSite/apply ネットワークデバイスをサイトに割り当てます。 • POST <cluster-ip>/dna/intent/api/v1/networkDevices/unassignFromSite/apply サイトからネットワークデバイスの割り当てを解除します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/assignedToSite サイトに割り当てられたネットワークデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/assignedToSite/count サイトに割り当てられたネットワークデバイス数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/notAssignedToSite サイトに割り当てられていないネットワークデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/${id}/assignedToSite サイトに割り当てられたネットワークデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/notAssignedToSite/count サイトに割り当てられていないネットワークデバイス数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDevices/deviceControllability/settings デバイスの可制御性設定を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/networkDevices/deviceControllability/settings デバイスの可制御性設定を更新します。 • GET <cluster-ip>/dna/intent/api/v1/networkProfilesforSites サイトのネットワークプロファイルのリストを取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkProfilesforSites/count サイトのネットワークプロファイル数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkProfilesforSites/${id} ID でサイトのネットワークプロファイルを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/networkProfilesforSites/${id} サイトのネットワークプロファイルを削除します。

機能	説明
	• GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments サイトの指定されたネットワークプロファイルが割り当てられているサイトのリストを取得します。 • POST <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments サイトのネットワークプロファイルを指定されたサイトに割り当てます。 • POST <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/bulk サイトのネットワークプロファイルをサイトのリストに割り当てます。 • DELETE <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/bulk 複数のサイトからサイトのネットワークプロファイルの割り当てを解除します。 • DELETE <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/${id} 1つのサイトからサイトのネットワークプロファイルの割り当てを解除します。 • GET <cluster-ip>/dna/intent/api/v1/networkProfilesForSites/${profileId}/siteAssignments/count サイトの指定されたネットワークプロファイルが割り当てられているサイトの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/profileAssignments 指定されたサイトに割り当てられているネットワークプロファイルのリストを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/profileAssignments/count 指定されたサイトに割り当てられているプロファイルの数を取得します。 新しいサイト設計 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次を選択します。 **[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、[Site Design] を選択します。

機能	説明
SWIM API	

機能	説明
	Catalyst Center プラットフォーム は、次の SWIM API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/images ソフトウェアイメージのリストを返します。 • POST <cluster-ip>/dna/intent/api/v1/images/${id}/download ソフトウェアイメージをダウンロードします。 • GET <cluster-ip>/dna/intent/api/v1/productNames ネットワークデバイス製品名のリストを取得します。 • GET <cluster-ip>/dna/intent/api/v1/productNames/count ネットワーク製品名の数。 • GET <cluster-ip>/dna/intent/api/v1/productNames/${productNameOrdinal} ネットワークデバイスの製品名を取得します。 • GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames サイトのネットワークデバイス製品名を返します。 • POST <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames 指定されたソフトウェアイメージにネットワークデバイスの製品名を割り当てます。 • GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count サイトのネットワークデバイス製品名の数を返します。 • DELETE <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames/${productNameOrdinal} 指定されたソフトウェアイメージからネットワークデバイス製品名の割り当てを解除します。 • PUT <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames/${productNameOrdinal} ソフトウェアイメージに割り当てられているネットワークデバイス製品名のサイトのリストを更新します。 • GET <cluster-ip>/dna/intent/api/v1/images/count ソフトウェアイメージの数を返します。 • GET <cluster-ip>dna/intent/api/v1/images/${id}/addonImages/count 追加イメージの数を返します。 • GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings イメージ配信サーバーを取得します。

機能	説明
	• POST <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings イメージ配信サーバーを追加します。 • GET <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/${id} 特定のイメージ配信サーバーを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/${id} リモートイメージ配信サーバーを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/images/distributionServerSettings/${id} イメージ配信サーバーを削除します。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceImageUpdates ネットワークデバイスイメージの更新を取得します。 • GET <cluster-ip>/dna/intent/api/v1/networkDeviceImageUpdates/count ネットワークデバイスイメージの更新数。 • GET <cluster-ip>/dna/intent/api/v1/images/${imageId}/siteWiseProductNames ソフトウェアイメージに割り当てられているネットワークデバイス製品名を取得します • GET <cluster-ip>/dna/intent/api/v1/siteWiseProductNames/count サイトのネットワークデバイス製品名の数を返します。 新しい SWIM 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次を選択します。 **[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、[Software Image Management (SWIM)] を選択します。

機能	説明
システム設定 API	Catalyst Center プラットフォームは、次のシステム設定 API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v1/ipam/serverSetting 外部 IPAM サーバーの設定の詳細を作成します。外部 IPAM サーバーは 1 つしか作成できません。新しいものを作成する前に、既存の外部サーバーを削除してください。 • GET <cluster-ip>/dna/intent/api/v1/ipam/serverSetting 外部 IPAM サーバーの設定の詳細を取得します。外部 IPAM サーバーが作成されていない場合、このリソースは「404」応答を返します。 • PUT <cluster-ip>/dna/intent/api/v1/ipam/serverSetting 外部 IPAM サーバーの設定の詳細を更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/ipam/serverSetting 外部 IPAM サーバーの設定の詳細を削除します。 • GET <cluster-ip>/dna/intent/api/v1/provisioningSettings プロビジョニング設定を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/provisioningSettings プロビジョニング設定を行います。 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 下にスクロールし、**[System Settings]** をクリックします。

機能	説明
タスク API	Catalyst Center プラットフォームは、次のタスク API をサポートしています。 • GET<cluster-ip>/dna/intent/api/v1/tasks タスクを取得します。 • GET<cluster-ip>/dna/intent/api/v1/tasks/count タスク数を取得します。 • GET<cluster-ip>/dna/intent/api/v1/tasks/${id} ID でタスクを取得します。 • GET<cluster-ip>/dna/intent/api/v1/tasks/${id}/detail ID でタスクの詳細を取得します。 • GET <cluster-ip>/dna/data/api/v1/assuranceTasks/${id} 特定のアシュアランスタスクを ID ごとに取得します。 • GET <cluster-ip>/dna/data/api/v1/assuranceTasks/count 現在存在するアシュアランスタスクの数を取得します。 • GET <cluster-ip>/dna/data/api/v1/assuranceTasks アシュアランスタスクのリストを取得します。 新しいタスク 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Operational Tasks] ドロップダウンリストを展開し、[Task] を選択します。

機能	説明
タグ API	Catalyst Center プラットフォーム は、次のタグ API をサポートしています。 • GET <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations ネットワークデバイスに関連付けられているタグを取得します。 • GET <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations/count 少なくとも 1 つのタグに関連付けられているインターフェイスの数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations/count 少なくとも 1 つのタグに関連付けられているネットワークデバイスの数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/tags/networkDevices/membersAssociations/query ネットワークデバイスに関連付けられているタグを照会します。 • POST <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations/query インターフェイスに関連付けられているタグを照会します。 • GET <cluster-ip>/dna/intent/api/v1/tags/interfaces/membersAssociations インターフェイスに関連付けられているタグを取得します。 新しいタグ 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 **[Operational Tasks]** ドロップダウンリストを展開し、**[Tag]** を選択します。

機能	説明
ワイヤレス API	

機能	説明
	このリリースでは、Catalyst Centerプラットフォーム では次の新しいワイヤレス API が導入されました。 （注） 新しいワイヤレス API は Cisco AireOS ワイヤレスコントローラ をサポートしていません。サポートは、Cisco Catalyst 9800 ファミリのデバイスにのみ拡張されます。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/anchorManagedApLocations 特定のワイヤレスコントローラのアンカー管理対象 AP の場所を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/managedApLocations/count 特定のワイヤレスコントローラの管理対象 AP の場所の数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/primaryManagedApLocations 特定のワイヤレスコントローラのプライマリ管理対象 AP の場所を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/secondaryManagedApLocations 特定のワイヤレスコントローラのセカンダリ管理対象 AP の場所を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups/count モビリティグループ数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups すべてのモビリティグループを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups/mobilityProvision モビリティのプロビジョニング。 • POST <cluster-ip>/dna/intent/api/v1/wirelessControllers/wirelessMobilityGroups/mobilityReset モビリティのリセット。 • GET <cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/ssidDetails 特定のワイヤレスコントローラの SSID の詳細を取得します。 • GET

機能	説明
	<cluster-ip>/dna/intent/api/v1/wirelessControllers/${networkDeviceId}/ssidDetails/count 特定のワイヤレスコントローラの SSID 数を取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/${id} インターフェイスを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/${id} インターフェイスを削除します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces インターフェイスを取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces インターフェイスを作成します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/${id} ID でインターフェイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/interfaces/count インターフェイス数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids SSID を作成します。 • PUT <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id} SSID を更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id} SSID を削除します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids サイトで SSID を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/${id} ID で SSID を取得します。 • GET <cluster-ip>/dna/intent/api/v1/sites/${siteId}/wirelessSettings/ssids/count サイトごとの SSID 数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} ワイヤレスプロファイルを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} ワイヤレスプロファイルを更新します。

機能	説明
	• POST <cluster-ip>/dna/intent/api/v1/wirelessProfiles ワイヤレスプロファイルを作成します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles ワイヤレスプロファイルを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/${id} ID でワイヤレスプロファイルを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessProfiles/count ワイヤレスプロファイル数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/${id} RF プロファイルを削除します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles RF プロファイルを作成します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/${id} RF プロファイルを更新します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles RF プロファイルを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/${id} ID で RF プロファイルを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/rfProfiles/count RF プロファイル数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessAccessPoints/factoryResetRequest/provision アクセスポイントを工場出荷時設定にリセットします。 • GET <cluster-ip>/dna/intent/api/v1/wirelessAccessPoints/factoryResetRequestStatus アクセスポイントの工場出荷時設定へのリセットのステータスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles すべての 802.11be プロファイルを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/${id} 802.11be プロファイルを更新します。

機能	説明
	• DELETE <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/${id} 802.11be プロファイルを削除します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/${id} ID で 802.11be プロファイルを取得します。 • GET <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles/count 802.11be プロファイル数を取得します。 • POST <cluster-ip>/dna/intent/api/v1/wirelessSettings/dot11beProfiles 802.11be プロファイルを作成します。 • POST<cluster-ip>/dna/intent/api/v1/wirelessControllers/${deviceId}/assignManagedApLocations WLC の管理対象 AP の場所を割り当てます。 • POST<cluster-ip>/dna/intent/api/v1/wirelessControllers/${deviceId}/provision ワイヤレスコントローラのプロビジョニング。 • POST <cluster-ip>/dna/intent/api/v1/wirelessAccessPoints/provision AP のプロビジョニング。 新しいワイヤレス 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Connectivity] ドロップダウンリストを展開して、[Wireless] を選択します。
API の機能拡張	
デバイスオンボーディング（PnP）API	このリリースでは、以下の通りです。 • sudiSerialNos 要求パラメータは、デバイスの更新 API とデバイスの追加 API で userSudiSerialNos に名前が変更されました。 • バーチャルアカウントの追加 API および PnP サーバープロファイルの更新 API に、addressIpV6 要求パラメータが追加されました。このパラメータは、クラスタが IPv6 で設定されている場合に必要です。 • isSudiRequired 要求パラメータは、デバイスの一括インポート API で sudiRequired に名前が変更されました。 • サイトへのデバイスの要求 API に、hostname という新しいオプションの要求パラメータが追加されました。 • デバイス要求 API に、authorizationNeeded という新しいオプションの要求パラメータが追加されました。

機能	説明
デバイス API	このリリースでは、デバイスリストの取得 API に `syncRequestedByApp` および `lastManagedResyncReasons` 応答パラメータが導入されました。
イベント管理 API	イベントアーティファクトの取得 API に、オプションの `deprecationMessage` および `deprecated` 応答パラメータが含まれるようになりました。deprecated の値が `true` の場合、イベントアーティファクトは廃止され、廃止メッセージが表示されます。
ファブリックデバイス API	このリリースでは、以下の通りです。 • 要求パラメータ `deviceRoles` は、WIRELESS_CONTROLLER_NODE 値を受け入れます。 • ファブリックデバイス API のサポートがワイヤレスロールに拡張されました。
パストレース API	egressPhysicalInterface、ingressPhysicalInterface、egressInterface、ingressInterface 属性は、以前のパストレースの取得 API のオプション属性になりました。
SDA API	このリリースでは、オプションの `isBpduGuardEnabled` 要求本文パラメータが、認証プロファイルの更新 API に追加されました。`authenticationProfileName` パラメータが [Closed Authentication] に設定されている場合、値を null にすることはできません。
廃止された API	
ファブリックワイヤレス API	このリリースでは、次のファブリックワイヤレス API が廃止予定としてマークされています。 • DELETE <cluster-ip>/dna/intent/api/v1/business/sda/wireless-controller ファブリックドメインからの WLC の削除。 • PUT <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/ssid-ippool SSID から IP プールへのマッピングの更新。 • POST <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/ssid-ippool SSID から IP プールへのマッピングの追加。 • GET <cluster-ip>/dna/intent/api/v1/business/sda/hostonboarding/ssid-ippool SSID から IP プールへのマッピングの取得。 • POST <cluster-ip>/dna/intent/api/v1/business/sda/wireless-controller ファブリックドメインへの WLC の追加。

機能	説明
ネットワーク設定 API	このリリースでは、次のネットワーク設定 API が廃止予定としてマークされています。 • POST <cluster-ip>/dna/intent/api/v1/network/${siteId} ネットワークの作成 • POST <cluster-ip>/dna/intent/api/v2/network/${siteId} ネットワーク V2 を作成します。 • PUT <cluster-ip>/dna/intent/api/v1/network/${siteId} ネットワークを更新します。 • PUT <cluster-ip>/dna/intent/api/v2/network/${siteId} ネットワーク V2 を更新します。 • GET <cluster-ip>/dna/intent/api/v1/network ネットワークを取得します。 • GET <cluster-ip>/dna/intent/api/v2/network ネットワーク V2 を取得します。 • POST <cluster-ip>/dna/intent/api/v1/credential-to-site/${siteId} デバイスのログイン情報をサイトに割り当てます。 • POST <cluster-ip>/dna/intent/api/v2/credential-to-site/${siteId} デバイスのログイン情報をサイト V2 に割り当てます。
サイト設計 API	このリリースでは、次のサイト設計 API が廃止予定としてマークされています。 • POST <cluster-ip>/dna/intent/api/v1/networkprofile/${networkProfileId}/site/${siteId} 関連付けします。 • DELETE <cluster-ip>/dna/intent/api/v1/networkprofile/${networkProfileId}/site/${siteId} 関連付けを解除します。

機能	説明
サイト API	このリリースでは、次のサイト API が廃止予定としてマークされています。 • GET <cluster-ip>/dna/intent/api/v1/site-member/${id}/member サイトに割り当てられているデバイスを取得します。 • POST <cluster-ip>/dna/intent/api/v1/assign-device-to-site/${siteId}/device サイトにデバイスを割り当てます。 • POST <cluster-ip>/dna/intent/api/v1/site サイトを作成します。 • DELETE <cluster-ip>/dna/intent/api/v1/site/${siteId} サイトを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/site/${siteId} サイトを更新します。 • GET <cluster-ip>/dna/intent/api/v1/site サイトを取得します。 • GET <cluster-ip>/dna/intent/api/v2/site サイト V2 を取得します。 • GET <cluster-ip>/dna/intent/api/v1/site/count サイト数を取得します。 • GET <cluster-ip>/dna/intent/api/v1/membership/${siteId} メンバーシップを取得します。 • GET <cluster-ip>/dna/intent/api/v2/site/count サイト数 V2 を取得します。

機能	説明
タスク API	このリリースでは、次のタスク API が廃止予定としてマークされています。 • GET <cluster-ip>/dna/intent/api/v1/task タスクを取得します。 • GET <cluster-ip>/dna/intent/api/v1/task/${taskId} ID でタスクを取得します。 • GET <cluster-ip>/dna/intent/api/v1/task/operation/${operationId}/${offset}/${limit} OperationId でタスクを取得します。 • GET <cluster-ip>/dna/intent/api/v1/task/${taskId}/tree タスクツリーを取得します。 • GET <cluster-ip>/dna/intent/api/v1/task/count タスク数を取得します。

機能	説明
ワイヤレス API	

機能	説明
	このリリースでは、次のワイヤレス API が廃止予定としてマークされています。 • POST <cluster-ip>/dna/intent/api/v1/wireless/profile ワイヤレスプロファイルを作成します。 • GET <cluster-ip>/dna/intent/api/v1/wireless/profile ワイヤレスプロファイルを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/wireless-profile/${wirelessProfileName} ワイヤレスプロファイルを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/wireless/profile ワイヤレスプロファイルを更新します。 • GET <cluster-ip>/dna/intent/api/v1/wireless/rf-profile RF プロファイルを取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/wireless/rf-profile/${rfProfileName} RF プロファイルを削除します。 • POST <cluster-ip>/dna/intent/api/v1/wireless/rf-profile RFプロファイルを作成または更新します。 • GET <cluster-ip>/dna/intent/api/v1/wireless/dynamic-interface ダイナミックインターフェイスを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/wireless/dynamic-interface ダイナミックインターフェイスを作成または更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/wireless/dynamic-interface ダイナミックインターフェイスを削除します。 • POST <cluster-ip>/dna/intent/api/v1/enterprise-ssid エンタープライズ SSID を作成します。 • PUT <cluster-ip>/dna/intent/api/v1/enterprise-ssid エンタープライズ SSID を更新します。 • Delete <cluster-ip>/dna/intent/api/v1/enterprise-ssid/${ssidName} エンタープライズ SSID を削除します。 • GET <cluster-ip>/dna/intent/api/v1/enterprise-ssid エンタープライズ SSID を取得します。 • DELETE

機能	説明
	<cluster-ip>/dna/intent/api/v1/business/ssid/${ssidName}/${managedAPLocations} SSID を削除し、デバイスにプロビジョニングします。 • POST <cluster-ip>/dna/intent/api/v1/business/ssid SSID を作成およびプロビジョニングします。 • GET <cluster-ip>/dna/intent/api/v1/task/count AP のプロビジョニング。 • POST <cluster-ip>/dna/intent/api/v1/wireless/ap-provision プロビジョニングを更新します。 • POST <cluster-ip>/dna/intent/api/v1/wireless/provision プロビジョニングします。
後方互換性を損なう API の変更	
なし	—

表 *4 : Catalyst Center* プラットフォーム *2.3.7.5* の新機能および変更された機能

機能	説明	記載場所
監査ログ レポート	Catalyst Center プラットフォーム リリースでは、新しい**監査ログ**レポートがサポートされています。	詳細については、以下を参照してください。 • 監査ログレポートの実行（159ページ）。 • Cisco Catalyst Center リリースノートの**新規レポート**。
新しい API		

機能	説明	記載場所
LAN 自動化 API	Catalyst Center プラットフォームは、次の LAN 自動化 API をサポートしています。 • POST <cluster-ip>/dna/intent/api/v2/lan-automation LAN 自動化開始 V2。 • PUT <cluster-ip>/dna/intent/api/v2/lan-automation/${id} LAN 自動化の停止とデバイス V2 の更新。 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次を選択します。 **[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。	

機能	説明	記載場所
レポート API	Catalyst Center プラットフォーム は、次のレポート API をサポートしています。 • GET <cluster-ip>/dna/data/api/v1/flexible-report/schedule/${reportId} レポート ID でフレキシブルレポートのスケジュールを取得します。 • GET <cluster-ip>/dna/data/api/v1/flexible-report/report/${reportId}/executions レポート ID で実行 ID を取得します。 • POST <cluster-ip>/dna/data/api/v1/flexible-report/report/${reportId}/execute フレキシブルレポートを実行します。 • PUT <cluster-ip>/dna/data/api/v1/flexible-report/schedule/${reportId} フレキシブルレポートのスケジュールを更新します。 • GET <cluster-ip>/dna/data/api/v1/flexible-report/schedules すべてのフレキシブルレポートのスケジュールを取得します。 • GET <cluster-ip>/dna/data/api/v1/flexible-report/report/content/${reportId}/${executionId} フレキシブルレポートをダウンロードします。 新しいレポート 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 **[Operational Tasks]** ドロップダウンリストを展開し、**[Reports]** を選択します。	

機能	説明	記載場所
SD-Access API		

機能	説明	記載場所
	Catalyst Centerプラットフォームは、次のSDA APIをサポートしています。 エクストラネットポリシー API • GET <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies エクストラネットポリシーを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies エクストラネットポリシーを更新します。 • POST <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies エクストラネットポリシーを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies/count エクストラネットポリシー数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/extranetPolicies/${id} ID でエクストラネットポリシーを削除します。 ポート割り当て API • POST <cluster-ip>/dna/intent/api/v1/sda/portAssignments ポート割り当てを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/portAssignments ポート割り当てを取得します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/portAssignments ポート割り当てを更新します。 • GET <cluster-ip>/dna/intent/api/v1/sda/portAssignments/count ポート割り当て数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/portAssignments/${id}	

機能	説明	記載場所
	ID でポート割り当てを削除します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/portAssignments ポート割り当てを削除します。 ファブリックサイト API • POST <cluster-ip>/dna/intent/api/v1/sda/fabricSites ファブリックサイトを追加します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricSites ファブリックサイトを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricSites/${id} ID でファブリックサイトを削除します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricSites ファブリックサイトを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricSites/count ファブリックサイト数を取得します。 ファブリックゾーン API	

機能	説明	記載場所
	• POST <cluster-ip>/dna/intent/api/v1/sda/fabricZones ファブリックゾーンを追加します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricZones ファブリックゾーンを更新します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricZones/${id} ID でファブリックゾーンを削除します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricZones ファブリックゾーンを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricZones/count ファブリックゾーン数を取得します。 認証プロファイル API • PUT <cluster-ip>/dna/intent/api/v1/sda/authenticationProfiles 認証プロファイルを更新します。 • GET <cluster-ip>/dna/intent/api/v1/sda/authenticationProfiles 認証プロファイルを取得します。 一括デバイスプロビジョニング API	

機能	説明	記載場所
	• GET <cluster-ip>/dna/intent/api/v1/sda/provisionDevices プロビジョニングされたデバイスを取得します。 • POST <cluster-ip>/dna/intent/api/v1/sda/provisionDevices デバイスをプロビジョニングします。 • GET <cluster-ip>/dna/intent/api/v1/sda/provisionDevices/count プロビジョニングされたデバイス数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/provisionDevices プロビジョニングされたデバイスを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/provisionDevices デバイスを再プロビジョニングします。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/provisionDevices/${id} ID でプロビジョニングされたデバイスを削除します。 ファブリックデバイス API	

機能	説明	記載場所
	• POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices ファブリックデバイスを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices ファブリックデバイスを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/count ファブリックデバイス数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices ファブリックデバイスを削除します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/${id} IDでファブリックデバイスを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricDevices ファブリックデバイスを更新します。 ファブリックデバイスレイヤ2ハンドオフ API	

機能	説明	記載場所
	• POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer2Handoffs ファブリックデバイスのレイヤ 2 ハンドオフを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer2Handoffs ファブリックデバイスのレイヤ 2 ハンドオフを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer2Handoffs/count ファブリックデバイスのレイヤ 2 ハンドオフ数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer2Handoffs ファブリックデバイスのレイヤ 2 ハンドオフを削除します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer2Handoffs/${id} ID でファブリックデバイスのレイヤ 2 ハンドオフを削除します。 ファブリックデバイス IP トランジットレイヤ 3 ハンドオフ API	

機能	説明	記載場所
	• POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3HandoffsIpTransits IP トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3HandoffsIpTransits IP トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3HandoffsIpTransits/count IPトランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフの数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3HandoffsIpTransits IP トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを削除します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3HandoffsIpTransits/${id} ID で IP トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3HandoffsIpTransits IP トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを更新します。 ファブリックデバイス SDA トランジットレイヤ 3 ハンドオフ API	

機能	説明	記載場所
	• POST <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/sdaTransits SDA トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/sdaTransits SDA トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを取得します。 • GET <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/sdaTransits/count SDA トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフの数を取得します。 • DELETE <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/sdaTransits SDA トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/fabricDevices/layer3Handoffs/sdaTransits SDA トランジットを使用したファブリックデバイスのレイヤ 3 ハンドオフを更新します。 エニーキャストゲートウェイ API	

機能	説明	記載場所
	• DELETE <cluster-ip>/dna/intent/api/v1/sda/anycastGateways/${id} ID でエニーキャストゲートウェイを削除します。 • PUT <cluster-ip>/dna/intent/api/v1/sda/anycastGateways エニーキャストゲートウェイを更新します。 • GET <cluster-ip>/dna/intent/api/v1/sda/anycastGateways エニーキャストゲートウェイを取得します。 • POST <cluster-ip>/dna/intent/api/v1/sda/anycastGateways エニーキャストゲートウェイを追加します。 • GET <cluster-ip>/dna/intent/api/v1/sda/anycastGateways/count エニーキャストゲートウェイ数を取得します。 新しいSDA 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次を選択します。**[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 [Connectivity] ドロップダウンリストを展開し、[SDA] を選択します。	
API の機能拡張		

機能	説明	記載場所
LAN 自動化 API	• LAN 自動化デバイス更新 API に、新しい要求本文パラメータ `hostnameUpdateDevices` に基づいてデバイスのホスト名を変更するための新しいクエリパラメータ HOSTNAME_UPDATE が含まれるようになりました。 • ID による LAN 自動化ステータス API と LAN 自動化ステータス API に、3 つの追加のオプションパラメータ `discoveryLevel`、`discoveryTimeout`、および `discoveryDevices` が含まれるようになりました。これらは、ユーザーが LAN 自動化開始 V2 API を使用して LAN 自動化を開始するときに、応答本文に表示されます。	

機能	説明	記載場所
デバイス API	• このリリースでは、IPv6 アドレスを指定して、サイトへのデバイスの割り当てAPIでデバイスを割り当てることができます。 • デバイスリストのエクスポート API で、`password` パラメータがオプションになりました。 • このリリースでは、Catalyst Center プラットフォーム は、指定した範囲によるデバイスインターフェイスの取得 API、ID によるインターフェイス情報の取得API、IPによるインターフェイスの取得API、OSPFインターフェイスの取得 API、ISIS インターフェイスの取得API、インターフェイス名によるインターフェイスの取得API、すべてのインターフェイスの取得API、および ID によるインターフェイスの取得APIの応答パラメータにおける、次の変更をサポートしています。 • `addresses`、`lastOutgoingPacketTime`、`lastIncomingPacketTime`、`mtu`、および `name` 応答パラメータが上記の API に含まれるようになりました。 • `poweroverethernet`、`networkdevice_id`、`managedNetworkElementUrl`、`managedNetworkElement`、`managedComputeElementUrl`、および `managedComputeElement` 応答パラメータは、上記の API から削除されました。	

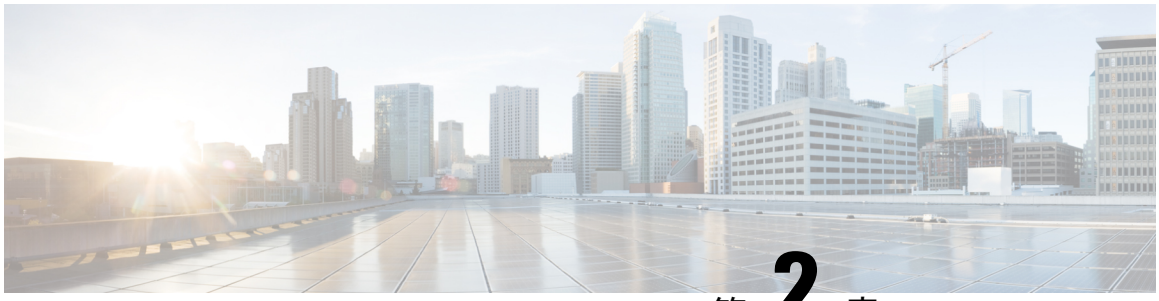
機能	説明	記載場所
ネットワーク設定 API	このリリースでは、予約 IP サブプールの取得 API に新しい `groupName` 要求クエリパラメータが追加されました。`siteId` パラメータはオプションになりました。 （注） `siteId` パラメータを省略すると、次のようになります。 • `ignoreInheritedGroups` パラメータを使用する必要があります。 • 応答の最大ページサイズは 1,000 エントリです。	
廃止された API		
なし	—	
後方互換性を損なう API の変更		
なし	—	

表 *5 : Catalyst Center* プラットフォーム *2.3.7.4* の新機能および変更された機能

機能	説明
Catalyst Center への名称変更	統合プラットフォームを中心に製品を統合するというビジョンの一環として、このリリースでは Cisco DNA Center プラットフォームの名称を Catalyst Center プラットフォーム に変更します。Catalyst Center の機能は Cisco DNA Center と同じままです。
新しい API	

機能	説明
ユーザー API とロール API	Catalyst Center プラットフォーム は、次のユーザーとロール API をサポートしています。 • POST <cluster-ip>/dna/system/api/v1/users/external-servers/aaa-attribute AAA 属性 API を追加および更新します。 • GET <cluster-ip>/dna/system/api/v1/users/external-servers/aaa-attribute AAA 属性 API を取得します。 • DELETE <cluster-ip>/dna/system/api/v1/users/external-servers/aaa-attribute AAA 属性 API を削除します。 • POST <cluster-ip>/dna/system/api/v1/users/external-authentication 外部認証設定 API を管理します。 • GET <cluster-ip>/dna/system/api/v1/users/external-authentication 外部認証設定 API を取得します。 新しいユーザーとロール 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** > **[User and Roles]** の順に選択します。
ITSM 統合 API	Catalyst Center プラットフォーム は、次の ITSM 統合 API をサポートしています。 GET <cluster-ip>/dna/intent/api/v1/integration-settings/status ITSM 統合ステータスを取得します。 新しい ITSM 統合 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次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** の順に選択します。 **[Integration]** ドロップダウンリストを展開し、**[ITSM Integration]** を選択します。
API の機能拡張	
デバイス API	デバイスへのユーザー定義フィールドの追加 API で、`value` 要求パラメータが必須属性になりました。
ディスカバリ API	グローバルログイン情報 V2 の作成 API およびグローバルログイン情報 V2 の更新 API の要求パラメータである `httpRead.name` および `httpWrite.name` は、それぞれ `httpRead.description` および `httpWrite.description`に変更されました。
廃止された API	

機能	説明
デバイス API	すべてのデバイスのデバイス設定の取得 API は廃止されました。



第 2 章

About Catalyst Center プラットフォーム

Catalyst Center プラットフォーム

Catalyst Center は、そのネイティブ機能の上に構築可能な付加価値アプリケーションを作成するために、シスコのお客様とパートナーが使用できる拡張可能なプラットフォームを提供します。Catalyst Center プラットフォームの次の機能を活用し、エンドツーエンドの IT プロセスを最適化し、総所有コスト（TCO）を削減し、新しい価値ネットワークを開発することで、全体的なネットワークエクスペリエンスを高めることができます。

- インテント API：インテント API は Catalyst Center プラットフォームの固有機能を公開するノースバウンド REST API です。インテント API は、ビジネス目的のポリシーベースの抽象化を提供し、成果を実装するためのメカニズムに悩まされることなく、成果に注力できるようになります。API は、REST API アーキテクチャスタイルに準拠しています。API はシンプルで拡張可能で、安全に使用できます。また、HTTPS 経由の GET、POST、PUT および DELETE 操作を含む標準の REST メソッドをサポートしています。
- 統合フロー：統合機能はウエストバウンドインターフェイスの一部です。最新のデータセンターでの運用を拡張および高速化するニーズに応えるため、IT オペレータにはオープン API によるインテリジェントなエンドツーエンドのワークフローが必要です。Catalyst Center プラットフォームは、Assurance ワークフローおよびデータと、サードパーティ製の IT サービスの管理（ITSM）ソリューションを統合するためのメカニズムを提供します。
- イベントおよび通知サービス：サポートされているサービスは、Cisco Catalyst Assurance イベントおよび Catalyst Center SWIM イベントをキャプチャして、サードパーティ製アプリケーションに転送するために使用できます。

（注） SUPER-ADMIN-ROLE のユーザーは、Catalyst Center プラットフォームアプリケーションにアクセスできます。SUPER-ADMIN-ROLE のユーザーとしてログインして Catalyst Center プラットフォーム を表示し、GUI を介してタスクを実行します。さらに、SUPER-ADMIN-ROLE のユーザーは、さまざまなプラットフォーム機能（API、バンドル、イベント、およびレポート）に対する読み取り、書き込み、または拒否権限を持つカスタムロールを作成できます。この機能にアクセスするには、メインメニューから次を選択します。**[System]** > **[Users & Roles]** > **[Role Based Action Access Control]** の順に選択します。

インテント API

インテント API は Catalyst Center プラットフォーム の固有機能を公開するノースバウンド REST API です。インテント API は、ビジネス目的のポリシーベースの抽象化を提供し、成果を実装するためのメカニズムに悩まされることなく、成果に注力できるようになります。

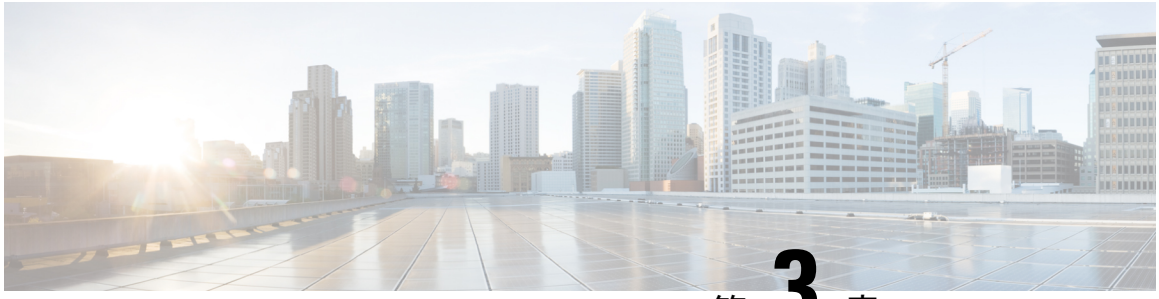
API は、シンプルで拡張可能で、安全な REST API アーキテクチャスタイルに準拠します。また、HTTPS 経由の GET、POST、PUT および DELETE 操作を含む標準の REST メソッドをサポートしています。REST エンドポイントは、JavaScript Object Notation（JSON）ドキュメントを含む HTTPS メッセージを受信して返信します。API メソッドを含むメッセージと JSON ドキュメントの生成には、どのプログラミング言語でも使用できます。これらの API は、Catalyst Center ロールベースアクセス制御（RBAC）ルールによって制御されます。セキュリティ対策として、ユーザーは API を使用する前に正常に認証される必要があります。

インテント API は、Catalyst Center プラットフォーム GUI にある API カタログに一覧表示されています。このカタログを表示するには、[**Platform** > **Developer Toolkit** > **APIs**] に移動します。API のレート制限の詳細については、API の詳細ページにある [**機能**] タブをクリックします。インテント API のデフォルトの API レート制限は 50 リクエストです。

イベントおよび通知について

Catalyst Center プラットフォーム は、特定のイベントがトリガーされた場合にカスタム通知を送信する機能をサポートしています。これは、イベントタイプに基づきビジネスアクションを実行するサードパーティ製システムには役立つ機能です。たとえば、ネットワーク内のデバイスがコンプライアンスに違反している場合、カスタムアプリケーションは通知を受信して、ソフトウェア アップグレードを実行することがあります。

このリリースで使用可能なイベントのリストを表示できます。[Platform]メインメニューから次を選択します。 > [Manage] > [Configurations] の順に選択します。そのようなイベントは、IT サービスの管理（ITSM）のインシデント用にカスタマイズできます。



第 3 章

Catalyst Center プラットフォームの導入

概要

Catalyst Center プラットフォーム を展開するには、次の手順を実行します。

1. Catalyst Center リリース 2.3.7 をインストールします。詳細については、Catalyst Center プラットフォーム のインストール （109 ページ）を参照してください。
2. 統合の設定を行います。詳細については、統合設定の設定 （110 ページ）を参照してください。

Catalyst Center プラットフォーム を展開した後、次のタスクを実行します。

- API の前提条件を確認します。詳細については、API の前提条件 （111 ページ）を参照してください。
- GUI の [**Overview**] に進んで簡単な機能説明を確認し、Catalyst Center プラットフォーム の理解を深めてください。詳細については、プラットフォームの概要について （115ページ）を参照してください。
- GUI の [**Bundles**] に進み、ネットワークに必要なバンドルの有効化、設定、アクティベートを行います。詳細については、バンドル機能 （118 ページ）を参照してください。

Catalyst Center プラットフォーム のインストール

Catalyst Center をインストールすると、Catalyst Center プラットフォーム もインストールされます。Catalyst Center プラットフォーム の個別のインストール手順は不要になりました。Catalyst

Center のインストール方法については、*Cisco Catalyst Center Installation Guide*を参照してください。

SUPER-ADMIN-ROLE のユーザは、Catalyst Center プラットフォームにアクセスできます。SUPER-ADMIN-ROLE のユーザとしてログインすると、Catalyst Center プラットフォーム の機能を表示し、GUI を使用してアクションを実行できます。さらに、SUPER-ADMIN-ROLE のユーザーは、さまざまなプラットフォーム機能（API、バンドル、イベント、およびレポート）に対する読み取り、書き込み、または拒否権限を持つカスタムロールを作成できます。この機能にアクセスするには、メインメニューから次を選択します。**[System]** > **[Users & Roles]** > **[Role Based Action Access Control]** の順に選択します。

統合設定の設定

ファイアウォールなどのルールが、Catalyst Center と、Catalyst Center プラットフォーム に到達する必要があるサードパーティ製アプリケーションの間に存在する場合は、[Integration Settings] を設定する必要があります。Catalyst Center の IP アドレスが、インターネットや外部ネットワークに接続する別の IP アドレスに内部的にマッピングされる場合には、このような事例が発生します。

重要 Catalyst Center のバックアップおよび復元後、[Integration Settings] ウィンドウにアクセスし、（必要に応じて）次の手順を使用して [Callback URL Host Name] または [IP Address] を更新する必要があります。

始める前に

前のセクションの説明に従って Catalyst Center プラットフォームを導入しました。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[System Configuration]** > **[Integration Settings]** の順に選択します。

ステップ 2 [Callback URL Host Name] 、または Catalyst Center プラットフォーム と通信するときにサードパーティ製アプリケーションが接続する必要がある [IP Address] を入力します。

（注）
[Callback URL Host Name] または [IP Address] は、Catalyst Center に内部的にマッピングされている外部向けホスト名または IP アドレスです。3 ノードクラスタセットアップの VIP アドレスを設定します。

ステップ 3 [Apply] をクリックします。

次のタスク

Catalyst Center プラットフォーム が正しく機能させるために必要な API の前提条件を確認してください。

API の前提条件

Catalyst Center API および Catalyst Center プラットフォーム を使用するためには、次の API の前提条件を満たす必要があります。

サポートされているプログラミング言語

生成されたコードプレビューを使用するには、サポートされているプログラミング言語を使用し、必要なタスクを実行する必要があります。

たとえば、Catalyst Center プラットフォーム によって生成された Python スクリプトを使用するには、要求ライブラリをインストールする必要があります。次の CLI コマンドを使用して、pip（Pip Installs Packages）をインストールすることができます。

```
pip install requests
```

Catalyst Center プラットフォーム は、GUI で次の言語のコードプレビューを生成します。

- シェル
- ノード：**HTTP**
- ノード：**Unirest**
- ノード：**Request**
- **Python**
- **Ruby**
- **javascript**
- **JQuery**
- **PHP**
- **Go**
- **Ansible**

認証

Catalyst Center API はトークンベースの認証を使用し、トークンの有効期間は 60 秒です。認証スクリプト（サポートされている任意のプログラミング言語を使用）を使用して API にログインする必要があります。たとえば、次の Python スクリプトを実行してログインします。

```
def get_token():
    token = requests.post(
       'https://<cluster IP>/api/system/v1/auth/token',
```

```
    auth=HTTPBasicAuth(
        username=<username>,
        password=<password>
    ),
headers={'content-type': 'application/json'},
verify=False,
 )
 data = token.json()
 return data['Token']
```

プラットフォーム向けロールベースアクセスコントロールのサポート

Catalyst Center プラットフォーム はロールベース アクセス コントロール（RBAC）をサポートしています。これにより、SUPER-ADMIN-ROLE権限を持つユーザーは、特定のプラットフォーム機能へのユーザーアクセスを許可または制限するカスタムロールを定義できます。

カスタムロールを定義し、定義したロールにユーザーを割り当てるには、次の手順を実行します。

（注） SUPER-ADMIN-ROLE のユーザは、Catalyst Center プラットフォームにアクセスできます。SUPER-ADMIN-ROLE のユーザとしてログインすると、Catalyst Center プラットフォーム の機能を表示し、GUI を使用してアクションを実行できます。NETWORK-ADMIN-ROLE と OBSERVER-ROLE は、Catalyst Center プラットフォームの機能が制限されます。たとえば、それらの 2 つのロールでは、次のアクションは許可されません。

- レポートの生成
- イベントの登録
- イベント設定の構成
- バンドルの有効化と設定
- ユーザーとロールの設定

詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Manage Users」の章を参照してください。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザーのみがこの手順を実行することができます。

手順

ステップ 1 カスタムロールを定義します。

a) メインメニューから次を選択します。**[System]** > **[Users & Roles]** > **[Role Based Access Control]** の順に選択します。

b) [Create a New Role] をクリックします。

[Create a User Role] ウィンドウが表示されます。これが RBAC の最初のイテレーションである場合、新しいロールを作成した後に、ユーザーを新しいロールに割り当てるように求められます。

c) [Let's Do it] をクリックします。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

[Create a New Role] ウィンドウが表示されます。

d) ロール名を入力し、[Next] をクリックします。

[Define the Access] ウィンドウにオプションのリストが表示されます。

e) [Platform] の横にある [>] をクリックして展開します。

次のオプションが表示されます。このオプションを使用して、新しいロールに対して [Deny]（デフォルト）、[Read]、[Write] 権限を設定できます。

- [APIs]：API を表示および試すことができます。
- [Bundles]：バンドルと ITSM の統合設定を設定してアクティブ化できます。
- [Events]：電子メール、REST API エンドポイント、および SNMP トラップのイベント設定を設定できます。
- [Reports]：レポートをスケジュール、表示、およびダウンロードできます。

f) [Next] をクリックします。
[Summary] ウィンドウが表示されます。

g) サマリーを確認します。サマリーの情報が正しい場合は、[Create Role] をクリックします。誤りがある場合は、[Edit] をクリックして適切な変更を行います。

ステップ 2 作成したカスタムロールにユーザーを割り当てるには、[Add Users] をクリックします。

[User Management] > **[Internal Users]** ウィンドウが表示されます。このウィンドウでは、カスタムロールを既存のユーザーまたは新規ユーザーに割り当てることができます。

- 既存のユーザーにカスタムロールを割り当てるには、次の手順を実行します。

  1. [Internal Users] ウィンドウで、カスタムロールを割り当てるユーザーの横にあるオプションボタンをクリックし、次に [Edit] をクリックします。

     [Update Internal User] スライドインペインが表示されます。

  2. [Role List] ドロップダウンリストから、カスタムロールを選択し、[Save] をクリックします。

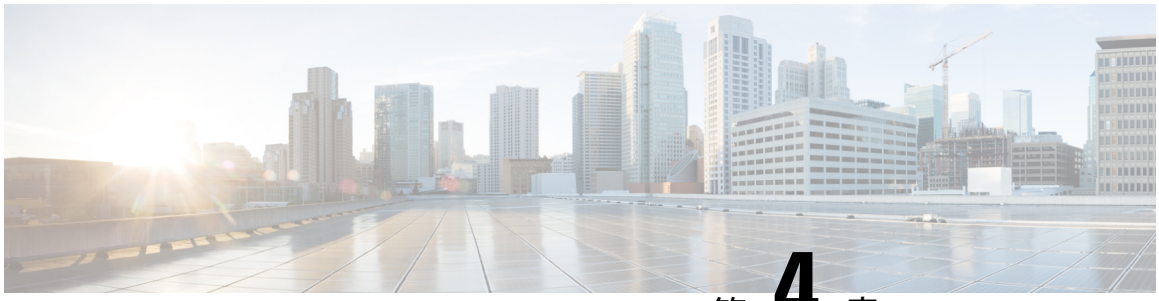
- 新規ユーザーにカスタムロールを割り当てるには、次の手順を実行します。

  1. [Add] をクリックします。

     [Create Internal User] スライドインペインが表示されます。

2. 表示されるフィールドに氏名、電子メール、およびユーザー名を入力します。
3. [Role List] ドロップダウンリストから、新規ユーザーに割り当てるカスタムロールを選択します。
4. 新しいパスワードを入力し、確認のために再度入力します。
5. [Save] をクリックします。

ステップ 3 既存のユーザーがログイン中に、管理者がそのユーザーのアクセス権限を変更した場合、新しい権限設定を有効にするには、ユーザーが Catalyst Center からログアウトして、ログインし直す必要があります。



第 4 章

プラットフォーム概要 GUI

プラットフォームの概要について

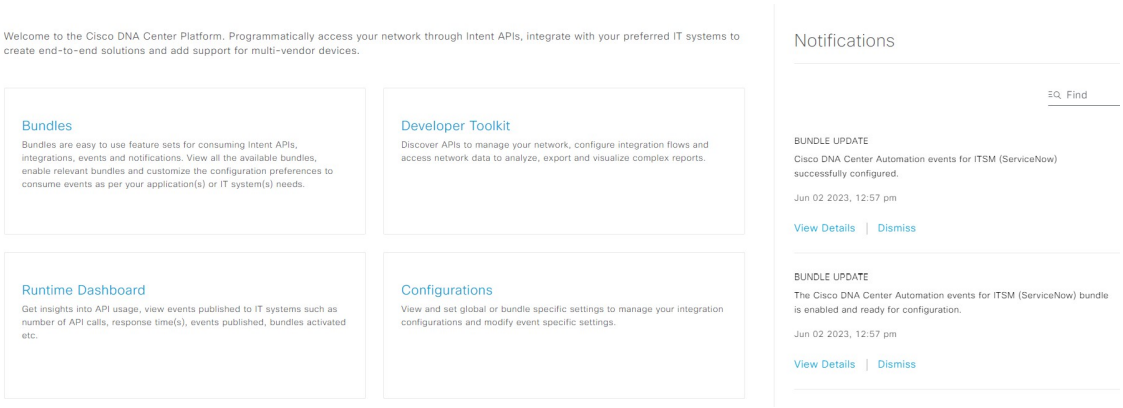
[Overview] ウィンドウにアクセスするには、メニューアイコンをクリックして次を選択します。 **[Platform]** > **[Overview]** の順に選択します。**[Overview]** ウィンドウでは次の機能がサポートされます。

- 次のような Catalyst Center プラットフォームの GUI 機能の概要と直接リンクが表示されます。
  - [Bundles]：独自のアプリケーションを Catalyst Center と統合するために使用できる、または Catalyst Center 自体のパフォーマンスを高めるために使用できるバンドルへのアクセスを提供します。バンドルは、API、イベント、統合フロー、データサービス、またはアプリケーションのグループ化として定義されます。さらに、一般設定またはイベントグローバル設定や複数のバンドルに関する設定を指定できる GUI（[Configurations]）へのアクセスも提供します。
  - [**Developer Toolkit**]：Catalyst Center にアクセスしたり Catalyst Center を他のアプリケーションと統合したりするためのツール（API および統合フロー）を提供します。
  - [Runtime Dashboard]：メトリックが収集されるダッシュボードを提供します。また、API、統合フロー、およびイベントサマリーを確認できます。
  - [Configurations]：ネットワークのイベントのカテゴリ、シビラティ（重大度）、およびタイプを設定したり、インスタンスをバンドルに追加して編集したりすることができるダッシュボードを提供します。
- [Notifications] スライドインペインにアクセスします。ここには Catalyst Center プラットフォームの最新の通知（バンドルの更新など）が示されます。[View Details] をクリックすると、[Bundles] タブにバンドルに関する詳細データが表示されます。[Dismiss] をクリックするとバンドル通知が消去されます。

プラットフォーム GUI の確認

この手順を実行すると、Catalyst Center プラットフォーム の機能と使用可能な機能を確認できます。Catalyst Center GUI の [Overview] ウィンドウを使って、これらの機能を確認できます。

図 *1 : Catalyst Center* プラットフォーム 概要ウィンドウ



手順

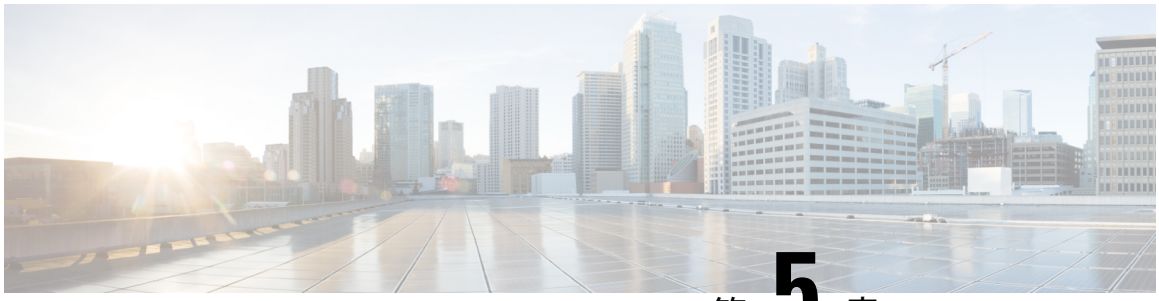
ステップ 1 メインメニューから次を選択します。[Platform] > [Overview] の順に選択します。

ステップ 2 このウィンドウで使用可能なオプションを確認します。

ステップ 3 Catalyst Center プラットフォームの個別の機能に直接アクセスするには、リンクをクリックします。

ステップ 4 [Notifications] スライドインペインを使って、バンドル更新情報を確認します。

（注）
バンドルの更新情報は、バンドルのステータスに関する情報（有効、無効、正常に設定済み、または設定可能）です。



第 5 章

プラットフォーム管理 GUI

管理について

Catalyst Center プラットフォーム [**Manage**] ウィンドウから、次の機能にアクセスできます。

- [Bundles]：Catalyst Center を独自のアプリケーションと統合するために使用できる、または Catalyst Center 自体のパフォーマンスを高めるために使用できるバンドルにアクセスします。バンドルは、API、イベント、統合フロー、データサービス、またはアプリケーションのグループ分けで構成されます。

（注） バンドルのコンポーネントを表示するには、メニューアイコンをクリックして次を選択します。**[Platform]** > **[Developer Toolkit]** > **[APIs]** または **[Platform]** > **[Developer Toolkit]** > **[Integration Flows]** の順に選択します。

- [Configurations]：カスタムプラットフォームエクスペリエンスを実現するために、単一のバンドルまたは複数のバンドルに及ぶグローバル設定を設定できます。

バンドルについて

Catalyst Center プラットフォームは、Catalyst Center をユーザー独自のアプリケーションと統合したり、Catalyst Center 自体のパフォーマンスを向上させたりするために使用できるバンドルへのアクセスを提供します。

GUIを使用して、Catalyst Center プラットフォーム の次の情報にアクセスできます。

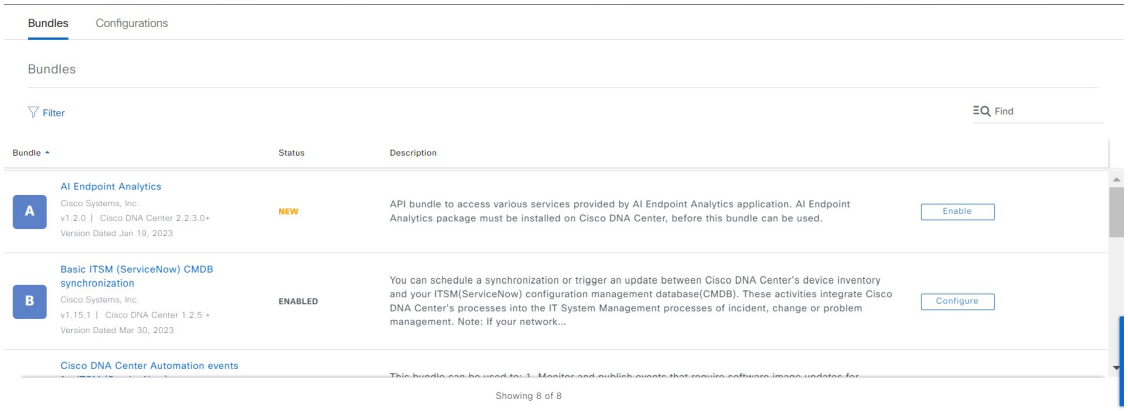
- バンドル名、ベンダー、バージョン、バージョンリリース日、タグ、および説明
- バンドルのステータス：
  - [NEW]：Catalyst Center プラットフォームで利用可能であるものの、まだ有効になっていないバンドル。[Enable] をクリックして、設定とその後のアクティブ化のためにバンドルを有効にしてください。
  - [ENABLE]：有効になっているものの、まだ設定されていないバンドル。有効になっているバンドルの統合フローと API コードは、[Contents] タブで確認できます。[Configure] をクリックして、バンドルレベルで設定します。

    通常、ビジネスマネージャがビジネス上の意思決定として特定のバンドルを有効にするため、バンドルの有効化と設定は2つの個別の手順になります。バンドルの後続の設定は、通常、IT 管理者またはネットワーク管理者によって行われます。
  - [DISABLED]：バンドルの以後の実行が停止されています。
  - [ACTIVE]：バンドルの確認や設定（バンドル固有値の設定）の後に、[Activate] をクリックしてネットワーク内のバンドルをアクティブ化できます。
  - [UPDATE]：あるバージョンの Catalyst Center プラットフォームをより新しいバージョンの Catalyst Center プラットフォームにアップグレードする場合。
  - [ERROR]：バンドルに問題があり、ネットワーク内でアクティブ化できません。

バンドル機能

Catalyst Center GUI の [Bundles] ウィンドウを使用して、バンドルの確認、有効化、および設定をすることができます。

図 *2 : Catalyst Center* プラットフォーム *[Bundles]* ウィンドウ



GUI のバンドルにアクセスして、次のタスクを実行します。

- サポートされている Catalyst Center API を確認し、試してください。詳細については、API での作業 （209 ページ）を参照してください。
- 有線およびワイヤレスの脅威（不正アクセスポイントを含む）を検出するには、不正管理および Cisco Advanced Wireless Intrusion Prevention System（aWIPS）を有効にします。詳細については、API での作業 （209 ページ）を参照してください。
- ServiceNow のイベントを受信するには、宛先（イベント管理または REST API エンドポイント）を設定します。GUI を使用して宛先を設定する方法については、バンドルの設定：イベントを受信する宛先 （120 ページ）を参照してください。
- Catalyst Center から ServiceNow へのアクセス設定（ホスト名、ユーザー名、パスワードなど）を設定します。GUI を使用して ServiceNow へのアクセス設定を設定する方法については、バンドルの設定：ServiceNow のアクセス設定 （123 ページ）を参照してください。
- Catalyst Center と ServiceNow の間のデータ同期設定（動作や送信元の識別子を設定するオプションなど）を設定します。GUI を使用してデータ同期を設定する方法については、バンドルの設定：ServiceNow の CMDB データ同期 （126 ページ）を参照してください。

次のバンドルが利用可能です。

- [Basic ITSM (ServiceNow) CMDB synchronization]：Catalyst Center のデバイスと ServiceNow CMDB システムの間の同期をトリガーまたはスケジュールします。ServiceNow CMDB は、IT のレコードの 1 つのシステムを提供します。

（注） 統合フローと ServiceNow の例については、「ServiceNow Integration」を参照してください。

- **REST API**：Catalyst Centerでサポートされている REST APIが含まれています。この API は、ネットワークの知識のクエリ、およびネットワークプログラミングを開始するための豊富な機能を提供しています。
- [Endpoint Attribute Retrieval with ITSM (ServiceNow)]：詳細なエンドポイント情報を取得し、1 回または定期的なスケジュールで Catalyst Center に公開します。このアクティビティでは、既存の ITSM（ServiceNow）ツールの CI は変更または削除されません。
- [Network Issue Monitor and Enrichment for ITSM (ServiceNow)]：アシュアランスとメンテナンスの問題に対応するためにネットワークを監視する Catalyst Center コンポーネントを含み、ServiceNow システムにイベントの詳細を発行します。ネットワークの豊富なコンテキストデータにアクセスする API も含みます。
- [Rogue and aWIPS]：Catalyst Center for Rogue Management と aWIPS でサポートされている REST API が含まれています。この API は、有線およびワイヤレスの脅威（不正アクセスポイントを含む）を検出するために使用されます。このバンドルとその API を使用するには、**Rogue および aWIPS** パッケージを Catalyst Center にインストールする必要があります。

- [Automation events for ITSM (ServiceNow)]：コンプライアンス、セキュリティ、デバイスのプロビジョニング アクティビティ、またはその他の操作トリガーで、ServiceNow システムのソフトウェアイメージの更新が必要なイベントを監視して発行します。
- [Disaster Recovery API]：ディザスタリカバリでサポートされる REST API が含まれており、ディザスタリカバリシステムをモニターするためのサポートが提供されます。
- [AI Endpoint Analytics]：AI エンドポイント分析アプリケーションによって提供されるさまざまなサービスにアクセスできます。このバンドルを使用するには、**AI Endpoint Analytics** パッケージを Catalyst Center にインストールする必要があります。

[**Filter**] アイコンをクリックしてフィルタを使用するか、[**Find**] フィールドにキーワードを入力することで、GUI に表示されたバンドルを調整することができます。

バンドルの設定：イベントを受信する宛先

ServiceNow のイベント（ネットワークおよびSWIM）を受信するようにバンドル内の宛先を設定するには、次の手順を実行します。

次のバンドル内で ServiceNow のイベントを受信するように宛先を設定します。

- [Network Issue Monitor and Enrichment for ITSM (ServiceNow)]
- [**Automation Events for ITSM (ServiceNow)**]

始める前に

最新の『*Cisco Catalyst Center ITSM Integration Guide*』を参照して、Catalyst Center から ServiceNow への統合を設定する場合、より大きなワークフローにおけるこの手順の位置付けを理解してください。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Manage]** > **[Bundles]**。

ステップ 2 **Network Issue Monitor and Enrichment for ITSM (ServiceNow)** または **Automation Events for ITSM (ServiceNow)** バンドルリンクまたはアイコンのいずれかをクリックします。

次の情報が表示されます。

- [**General information**]：四角いアイコンの下に、ベンダー、バージョン、プラットフォーム、タグが表示されます。

  （注）
  タグは、どの Catalyst Center コンポーネントが使用され、バンドルによって影響を受けるかを示します。

- [Information]：一般的な情報（バンドルの目的、ネットワーク内のバンドルのしくみ）、サンプルスキーマ、マッピングメモ、設定メモ、およびバンドルに関するその他のデータを表示するタブです。
- [Contents]：バンドル内の統合フローに関する情報にアクセスするタブです。
- [Release Notes]：自身のバージョンを含む、バンドルに関する最新のリリース情報を表示するタブです。

ステップ 3 前述の各タブをクリックし、バンドルに関する情報を確認します。

ステップ 4 [Enable] をクリックしてバンドルを有効にします。

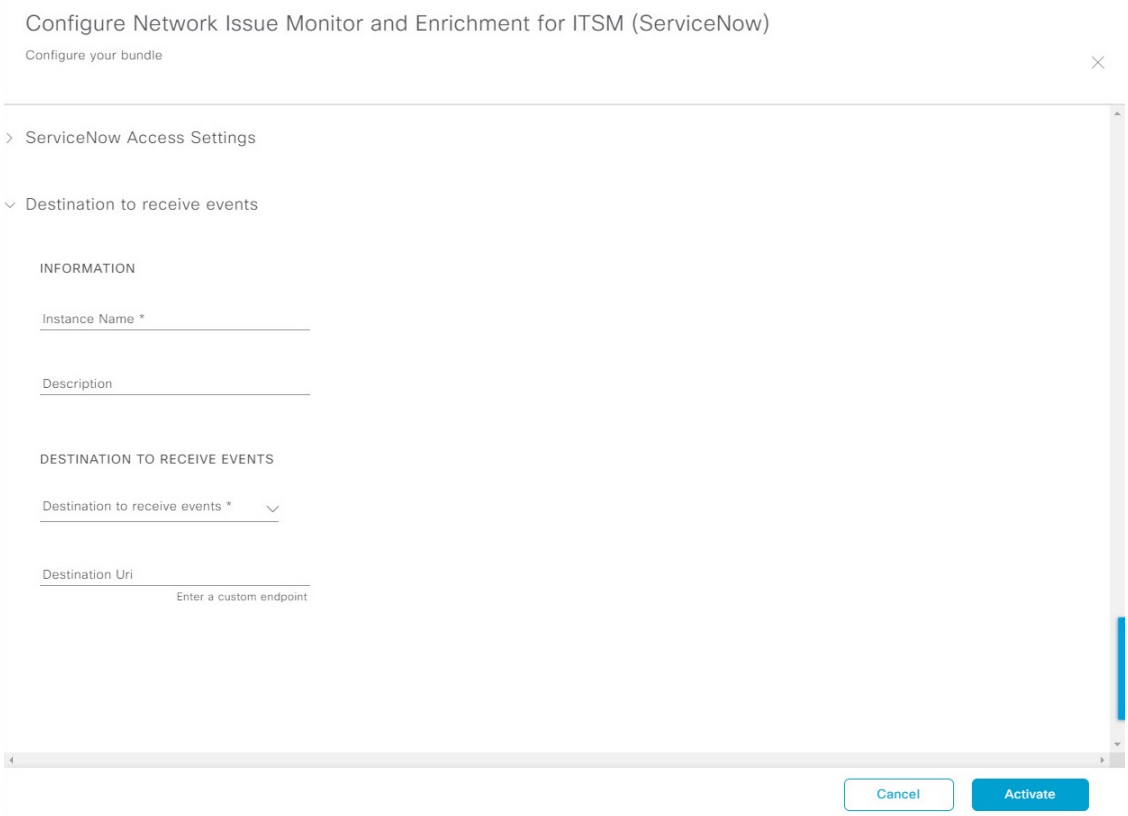
ステップ 5 [nformation] フィールドで、[Enable] をクリックして、バンドルの有効化を確認します。

ステップ 6 成功メッセージの中の [Okay] をクリックします。

ステップ 7 [Configure] をクリックして、バンドルレベルで設定します。

ステップ 8 構成スライドインペインで、[Destination to receive events] をクリックし、宛先インスタンスを設定します。

図 *3 : [Destination to receive events]* 設定フィールドの例



（注）
REST API エンドポイントでネットワークイベントと Catalyst Center 自動化イベントの詳細を受信し、Catalyst Center でユーザーが選択した構成に基づいてインシデント、問題、または変更チケットを作成するには、ServiceNow 用の [**Destination to receive events**] 構成オプションを使用します。ServiceNow を使用

してこれを設定する方法の詳細については、『Cisco Catalyst Center ITSM Integration Guide』を参照してください。

ステップ 9 ラジオボタンをクリックして、既存の宛先インスタンスを設定するか、または新しいインスタンスを設定します。

既存の宛先インスタンスを設定するには、ウィンドウのドロップダウンリストでインスタンスを選択し、[Activate] をクリックします。

ステップ 10 新しい宛先インスタンスを設定するには、次の情報を入力します。

- [Instance Name]：インスタンスの名前。
- [Description]：インスタンスの説明テキスト。
- [**Destination to receive events**]：次のいずれかのオプションを選択します。
  - [Event Management]：Cisco Catalyst アプリを使用せずに Catalyst Center と ServiceNow の統合を設定する場合は、[Event Management] オプションを選択します。[Event Management] オプションを選択する場合、ServiceNow インスタンス内でイベント管理プラグインを設定する必要もあります。
  - [REST API Endpoint]：[REST API Endpoint] オプションは、Cisco Catalyst アプリで使用できます。データは、[REST API Endpoint] オプションを使用して Cisco Catalyst アプリ内の REST API エンドポイントに送信されます。
  - [Generic REST Endpoint in ServiceNow]：[Generic REST Endpoint in ServiceNow] オプションの場合、ServiceNow の別のステージングテーブルにデータを送信できます。

  Catalyst Center と ServiceNow の統合の詳細については、『*Cisco Catalyst Center ITSM Integration Guide*』を参照してください。
- [Destination URI]：[Generic REST Endpoint in ServiceNow] オプションの宛先 Uniform Resource Identifier（URI）を入力します。このオプションでは、このフィールドは必須です。

この情報を入力して、次のステップに進みます。

ステップ 11 [Activate] をクリックし、変更を保存してバンドルを有効化するか、[Cancel] をクリックして設定をキャンセルし、スライドインペインを閉じます。

（注）
[Activate] をクリックすると、バンドルに加えた変更が有効になり、変更は直ちに実施されます。さらに、バンドルのステータスは [ENABLED] から [ACTIVE] に変更されます。

次のタスク

設定を確認するには、**[Manage]** > **[Configurations]** > **[General Settings]** の順に選択し、[Filter] または [Find] ツールを使用して、この手順で設定された特定の宛先インスタンスを探します。

必要であれば、今後は、[General Settings] ウィンドウで、インスタンスの編集、更新、削除ができるようになります。詳細については、全般設定の設定：インスタンスの編集 （139ページ）を参照してください。

バンドルの設定：ServiceNow のアクセス設定

バンドル内の ServiceNow のアクセス設定を設定するには、次の手順を実行します。

次のバンドル内で ServiceNow のアクセス設定を設定します。

- [Endpoint Attribute Retrieval with ITSM (ServiceNow)]
- [Network Issue Monitor and Enrichment for ITSM (ServiceNow)]
- [**Automation Events for ITSM (ServiceNow)**]

始める前に

最新の『*Cisco Catalyst Center ITSM Integration Guide*』を参照して、Catalyst Center から ServiceNow への統合を設定する場合、より大きなワークフローにおけるこの手順の位置付けを理解してください。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Manage]** > **[Bundles]**。

ステップ 2 [**Network Issue Monitor and Enrichment for ITSM (ServiceNow)**]、[**Automation events for ITSM (ServiceNow)**]、または [**Endpoint Attribute Retrieval with ITSM (ServiceNow)**] バンドルリンクまたはアイコンをクリックします。

（注）
ここでは、例として [Endpoint Attribute Retrieval with ITSM (ServiceNow)] を選択しています。

次の情報が表示されます。

- [General information]：四角いアイコンの下に、ベンダー、バージョン、プラットフォーム、タグが表示されます。

  （注）
  タグは、どの Catalyst Center コンポーネントが使用され、バンドルによって影響を受けるかを示します。

- [Information]：一般的な情報（バンドルの目的、ネットワーク内のバンドルのしくみ）、サンプルスキーマ、マッピングメモ、設定メモ、およびバンドルに関するその他のデータを表示するタブです。
- [Contents]：バンドル内の統合フローに関する情報にアクセスするタブです。

  （注）

[Endpoint Attribute Retrieval with ITSM (ServiceNow)] の場合、[Scheduler for ServiceNow Asset Sync] へのアクセスが提供されます。

- [Release Notes]：自身のバージョンを含む、バンドルに関する最新のリリース情報を表示するタブです。

ステップ 3 前述の各タブをクリックし、バンドルに関する情報を確認します。

ステップ 4 [Enable] をクリックして、リンクを有効化します。

ステップ 5 [nformation] フィールドで、[Enable] をクリックして、バンドルの有効化を確認します。

ステップ 6 成功メッセージの中の [Okay] をクリックします。

ステップ 7 [Content] タブをクリックします。

[Endpoint Attribute Retrieval with ITSM (ServiceNow)] の場合、[Scheduler for ServiceNow Asset Sync] へのリンクが表示されます。リンクをクリックして、次のタスクを実行します。

- [Description]、[Tags]、[How to Use this Flow]、およびスケジューラを確認します。
- [Run Now]（スケジューラをすぐに実行する場合）、[Run Later]（後で実行するようにスケジュールする場合）、または [Recurring]（反復スケジュールを設定する場合）をクリックします。

  [Run Later] を選択した場合は、日付、時刻、およびタイムゾーンを選択する必要があります。[Recurring] を選択した場合は、繰り返しの頻度（毎日または毎週）、間隔（分または時間）、開始日と終了日を設定する必要があります。
- [Schedule] をクリックしてスケジューラを有効にします。

  重要
  次の手順に従い、バンドル自体の設定が完了した後にのみ、統合フローのスケジュールを設定および有効化します。統合フローのスケジュールを設定して有効にするには、このビューに戻って [Schedule] をクリックするか、**[Platform]** > **[Developer Toolkit]** > **[Integration Flows]** > **[Scheduler for ServiceNow Asset Sync]** の順に選択します。

他のバンドル（[**Network Issue Monitor and Enrichment for ITSM (ServiceNow)**] と [**Automation events for ITSM (ServiceNow)**]）には、統合フローへのリンクはありません。統合フローに関する情報のみが表示されます。

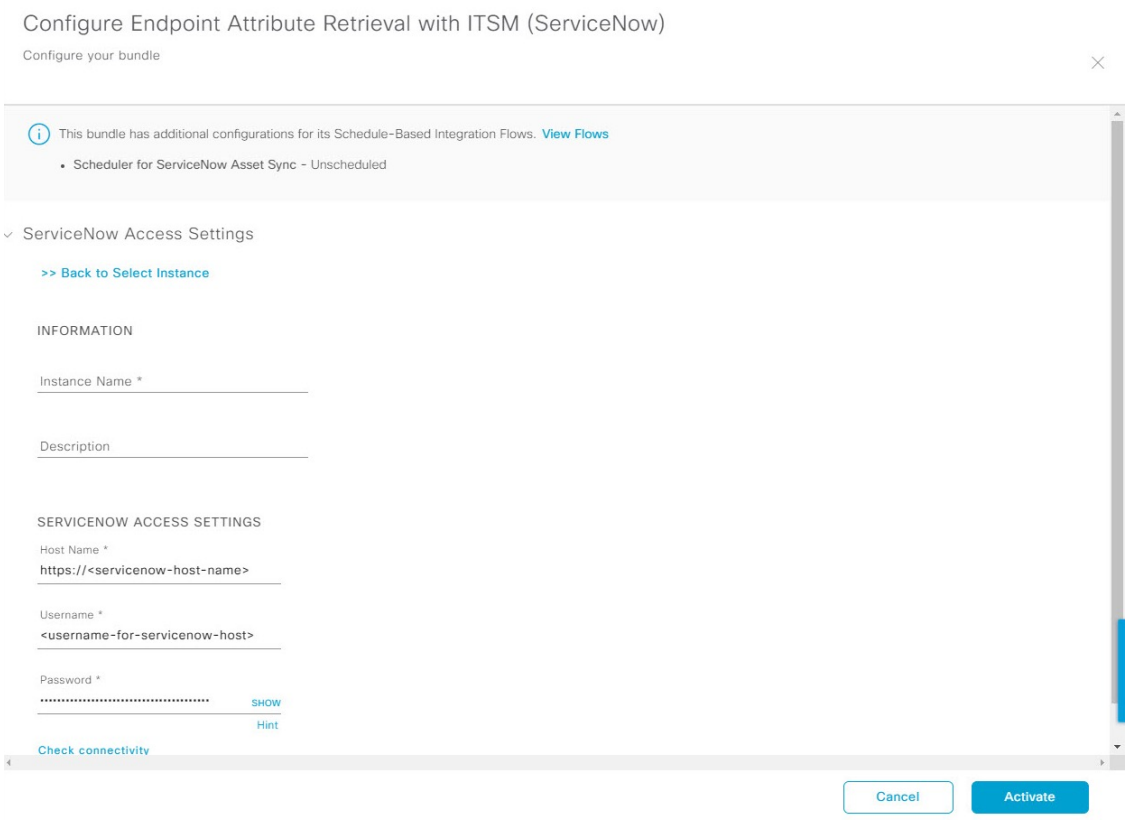
ステップ 8 [**X**] アイコンをクリックしてウィンドウを閉じ、前のバンドルウィンドウに戻ります。

ステップ 9 [Configure] をクリックして、バンドルレベルで設定します。

ステップ 10 設定スライドインペインで、[ServiceNow Access Settings] をクリックして、ServiceNow のインスタンスを設定します。

ステップ 11 ラジオボタンをクリックして、既存の ServiceNow のインスタンスを設定するか、または新しいインスタンスを設定します。

図 *4 : ServiceNow* インスタンスの設定フィールドの例



既存の ServiceNow のインスタンスを設定するには、ドロップダウンリストでそのインスタンスを選択し、[**Activate**] をクリックします。

ステップ 12 新しい ServiceNow インスタンスを設定するには、次の情報を入力します。

- [Instance Name]：インスタンスの名前。
- [Description]：インスタンスの説明テキスト。
- [Host name]：ServiceNow システムのホスト名。
- [Username]：ServiceNow システムへのアクセスに必要なユーザー名。
- [Password]：ServiceNow システムへのアクセスに必要なパスワード。

ステップ 13 [Check Connectivity] をクリックして、エンドポイントが設置されたサーバーへの接続が可能かどうかテストします。

サーバーへの接続テストが成功したら、次の手順に進みます。

ステップ 14 [Activate] をクリックし、変更を保存してバンドルを有効化するか、[Cancel] をクリックして設定をキャンセルし、スライドインペインを閉じます。

（注）

[Activate] をクリックすると、バンドルに加えた変更が有効になり、変更は直ちに実施されます。さらに、バンドルのステータスは [ENABLED] から [ACTIVE] に変更されます。

次のタスク

設定を確認するには、**[Manage]** > **[Configurations]** > **[General Settings]** の順に選択します。[Filter]または [Find] ツールを使用して、この手順で設定された ServiceNow インスタンスを探します。

必要であれば、今後は、[General Settings] ウィンドウで、インスタンスの編集、更新、削除ができるようになります。詳細については、全般設定の設定：インスタンスの編集（139ページ）を参照してください。

バンドルの設定：ServiceNow の CMDB データ同期

バンドル内の Catalyst Center と ServiceNow の間のデータ同期設定（動作や送信元の識別子を設定するオプションなど）を設定するには、次の手順を実行します。

Basic ITSM（ServiceNow）CMDB 同期バンドル内で、データ同期を設定し、ServiceNow の操作制限と識別子を設定します。

始める前に

最新の『Cisco Catalyst Center ITSM Integration Guide』を参照して、Catalyst Center から ServiceNow への統合を設定する場合、より大きなワークフローにおけるこの手順の位置付けを理解してください。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Manage]** > **[Bundles]** の順に選択します。

ステップ 2 [Basic ITSM (ServiceNow) CMDB synchronization] バンドルリンクまたはアイコンをクリックします。

次の情報が表示されます。

- [General information]：四角いアイコンの下に、ベンダー、バージョン、プラットフォーム、タグが表示されます。

  （注）
  タグは、どの Catalyst Center コンポーネントが使用され、バンドルによって影響を受けるかを示します。

- [Information]：一般的な情報（バンドルの目的、ネットワーク内のバンドルのしくみ）、サンプルスキーマ、マッピングメモ、設定メモ、およびバンドルに関するその他のデータを表示するタブです。

- [Contents]：バンドルを構成する統合フローにアクセスするか、バンドルを構成する統合フローに関する情報を提供するタブです。
- [Release Notes]：自身のバージョンを含む、バンドルに関する最新のリリース情報を表示するタブです。

ステップ 3 [Information] タブでバンドルデータを確認し、[Contents] タブをクリックします。

ステップ 4 [Integration Flows] ヘッダーをクリックします。

ヘッダーの下で使用可能な統合フロー（リンク）のリストを確認します。統合フローとその目的の詳細については、統合フローの使用 （212 ページ）を参照してください。

ステップ 5 [Enable] をクリックして、リンクを有効化します。

ステップ 6 [nformation] フィールドで、[Enable] をクリックして、バンドルの有効化を確認します。

ステップ 7 成功メッセージの中の [Okay] をクリックします。

ステップ 8 統合フローのリンクをクリックして、次のタスクを実行します。

- [Description]、[Tags]、[How to Use this Flow]、およびスケジューラを確認します。
- [Run Now]（スケジューラをすぐに実行する場合）、[Run Later]（後で実行するようにスケジュールする場合）、または [Recurring]（反復スケジュールを設定する場合）をクリックします。

  [Run Later] を選択した場合は、日付、時刻、およびタイムゾーンを選択する必要があります。[Recurring] を選択した場合は、繰り返しの頻度（毎日または毎週）、間隔（分または時間）、開始日と終了日を設定する必要があります。
- [Schedule] をクリックしてスケジューラを有効にします。

  重要
  次の手順に従い、バンドル自体の設定が完了した後にのみ、統合フローのスケジュールを設定および有効化します。統合フローのスケジュールを設定して有効にするには、このビューに戻って [Schedule] をクリックします。または、[Configure Basic ITSM (ServiceNow) CMDB synchronization] スライドインペインの [View Flows] リンクをクリックします（次の手順を参照）。あるいは、メニューアイコンをクリックして次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[Integration Flows]** > **[Schedule to Publish Inventory Details-ServiceNow Connector]** の順に選択します。

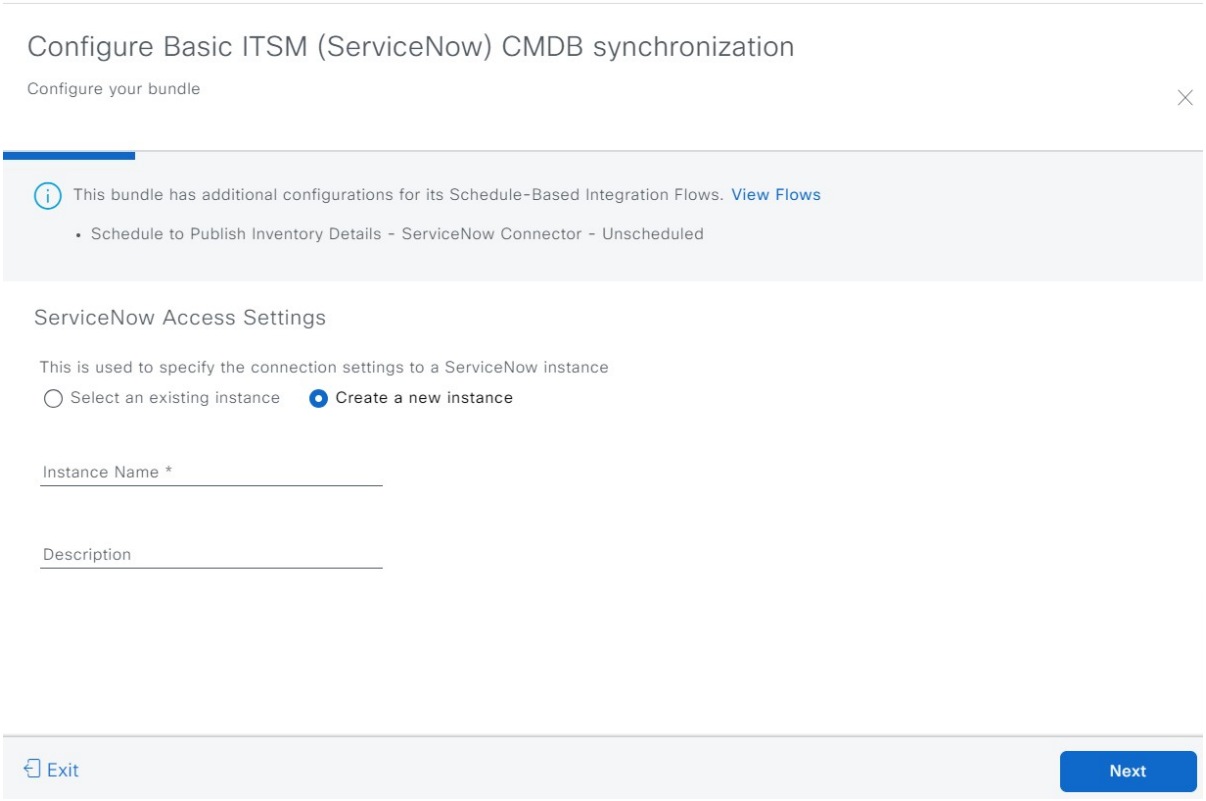
ステップ 9 ウィンドウの右上にある [X] アイコンをクリックして閉じ、前のバンドルウィンドウに戻ります。

ステップ 10 [Configure] をクリックして、バンドルレベルで設定します。

設定 スライドインペイン が表示されます。CMDB 同期情報を確認します。

ステップ 11 オプションボタンをクリックして、CMDB 同期の ServiceNow アクセス設定（既存または新規）を設定します。

図 *5 : [ServiceNow Access Settings]*



既存の設定を設定するには、ウィンドウのドロップダウンメニューで設定を選択し、[Next] をクリックします。

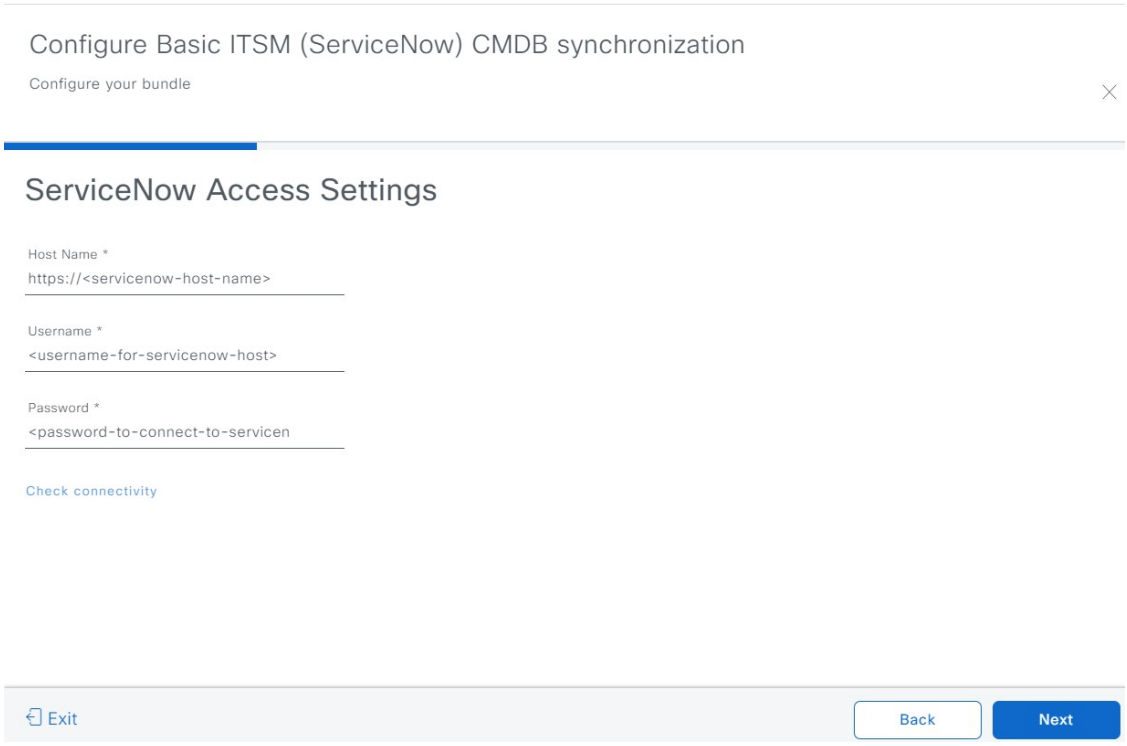
ステップ 12 新しいアクセス設定を設定するには、次のインスタンス情報を入力します。

- [Instance Name]：インスタンスの名前。
- [Description]：インスタンスの説明テキスト。

[Next] をクリックします。

ステップ 13 新しいアクセス設定を設定するには、次の追加の設定情報を入力します。

図 *6 : [ServiceNow Access Settings]*



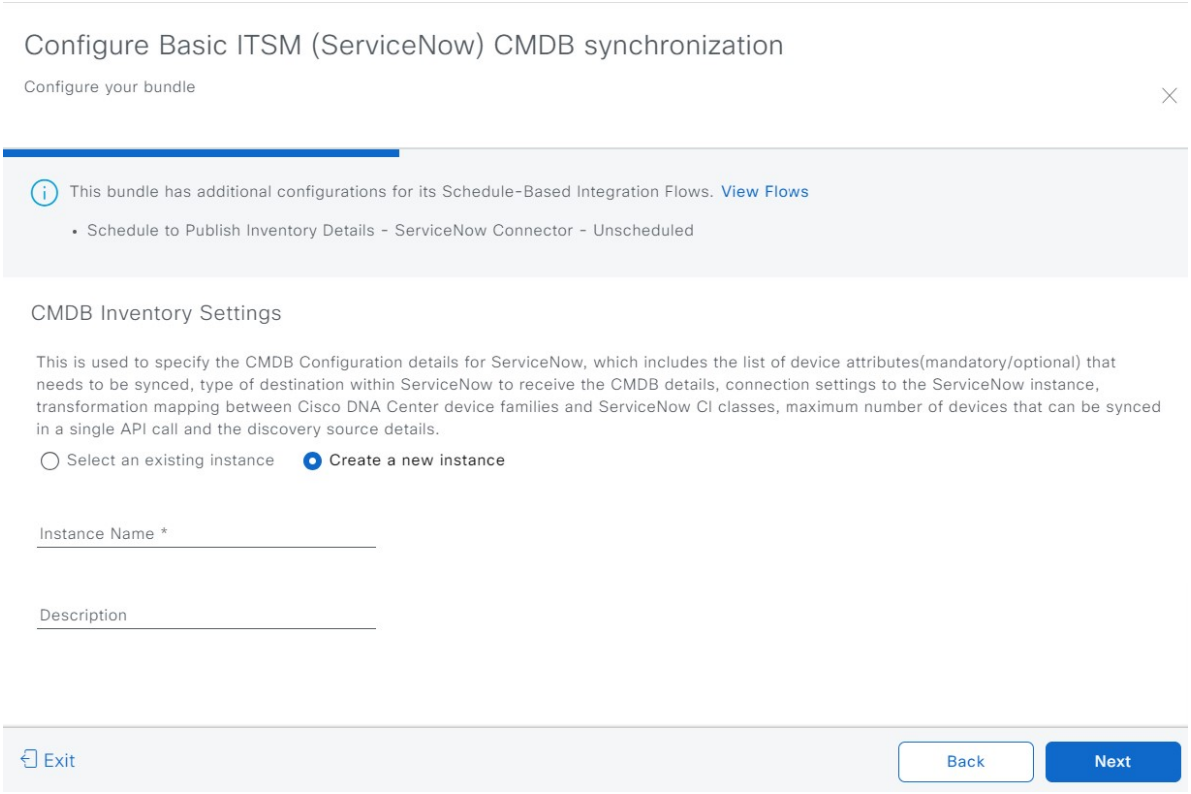
- [Hostname]：ServiceNow サーバーのホスト名または IP アドレス。
- [Username]：ServiceNow サーバーにアクセスするためのユーザー名。
- [Password]：ServiceNow サーバーにアクセスするためのパスワード。

[Check Connectivity] をクリックして、ServiceNow サーバーへのアクセスを確認します。

[Next] をクリックします。

ステップ 14 オプションボタンをクリックして、CMDBインベントリ設定に対して既存のインスタンスを設定するか、または新しいインスタンスを設定します。

図 *7*：*CMDB* インベントリ設定



既存のインスタンスを設定するには、ウィンドウのドロップダウンメニューでインスタンスを選択し、[Configure] をクリックします。

ステップ 15 新しいインスタンスを設定するには、次の追加情報を入力します。

- [Instance Name]：インスタンスの名前。
- [Description]：インスタンスの説明テキスト。

[Next] をクリックします。

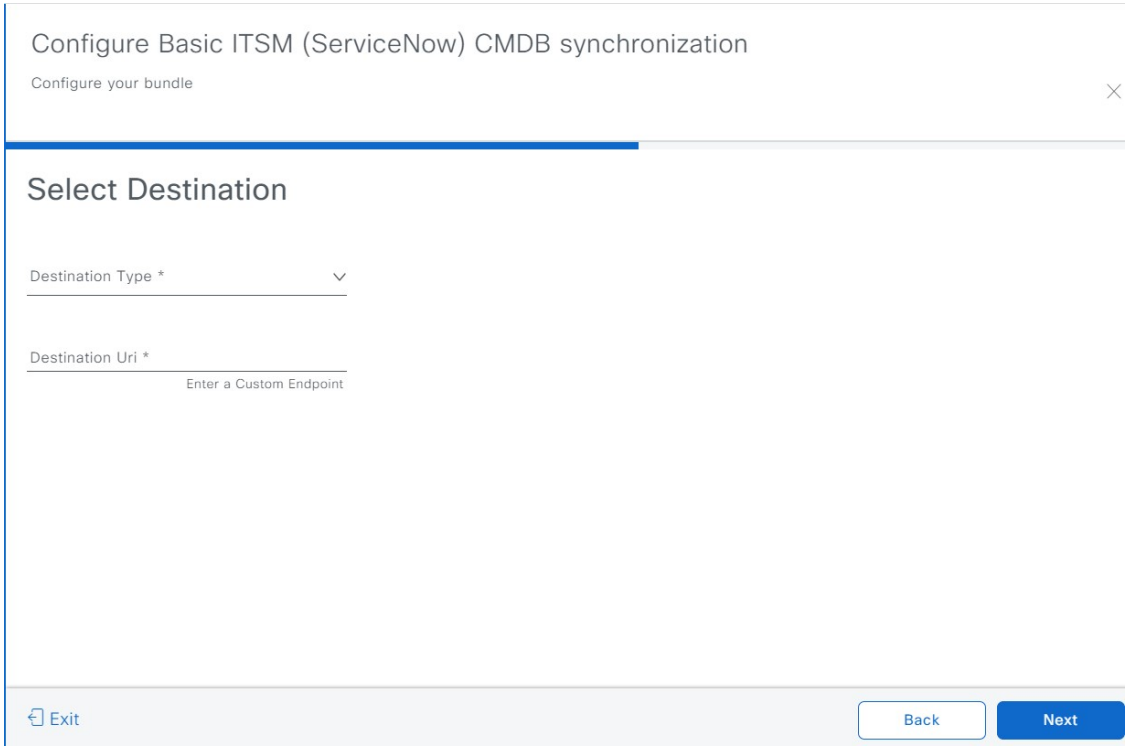
ステップ 16 [Select Destination] ウィンドウで、次の情報を入力します。

- [Destination Type]：次の 2 つの検出ソースオプションから選択できます。
  - **[Synchronize device inventory directly with CMDB]**
  - **[Post device inventory details to a staging table]**

（注）
ステージングテーブルを使用すると、テーブルから値を取得して ServiceNow CMDB にマッピングできます。

- [Destination URL]：ServiceNow サーバー（CMDB）またはステージングテーブルの Uniform Resource Indicator（URI）。

図 *8 : [Select Destination]* ウィンドウ



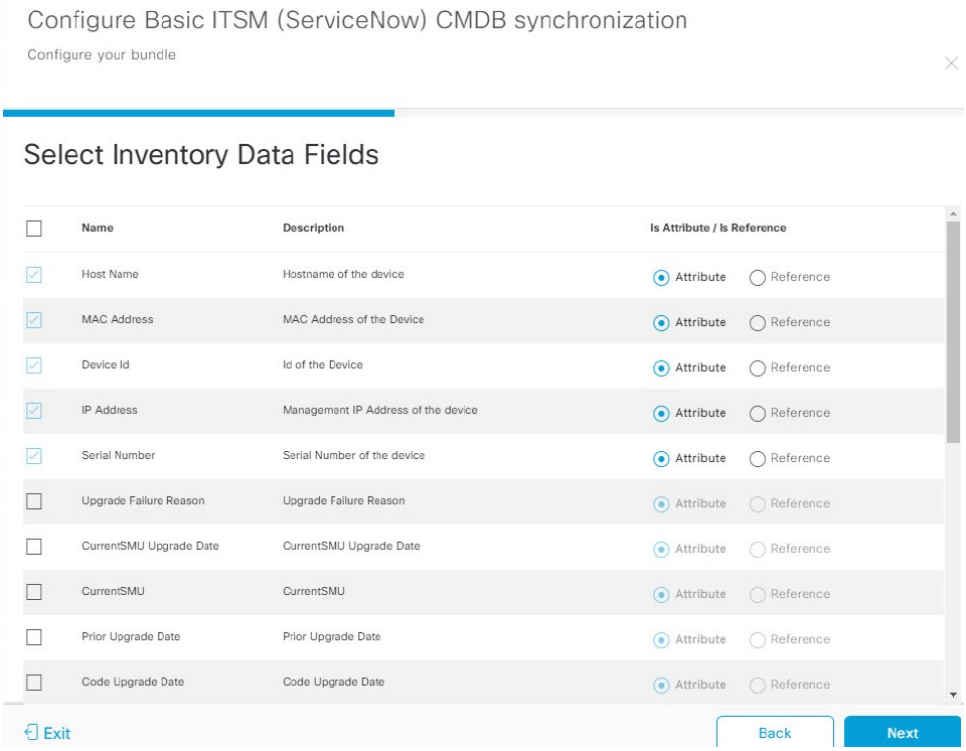
[Next] をクリックします。

ステップ 17 [Select Inventory Data Fields] ウィンドウで、同期するインベントリ データ フィールドを選択します。

（注）
インベントリ データ フィールドは、CMDB またはステージングテーブルに同期される属性または参照として指定できる、シスコが作成したデータタイプです。

[Select Inventory Data Fields] ウィンドウの上部のチェックボックスをクリックすると、同期するすべてのインベントリ データ フィールドが選択されます。すべてのインベントリ データ フィールドを同期する場合は、この上部のチェックボックスをクリックします。すべてを同期しない場合は、チェックボックスを 1 つずつ確認してオンにし、同期するインベントリ データ フィールドの小さなサブセットを作成します。

図 *9 : [Select Inventory Data Fields]* ウィンドウ



[Select Inventory Data Fields] ウィンドウは、次の列で構成されています。

- [Name]：インベントリ データ フィールドの名前。
- [Description]：インベントリ データ フィールドの簡単な説明。
- [Is Attribute/Is Reference]：インベントリ データ フィールドが属性または参照のどちらであるか。参照データフィールドは、データベース内の2つのテーブル間の関係を作成するために使用されます。属性データフィールドは、データベースのテーブルにデータを追加するために使用されます。

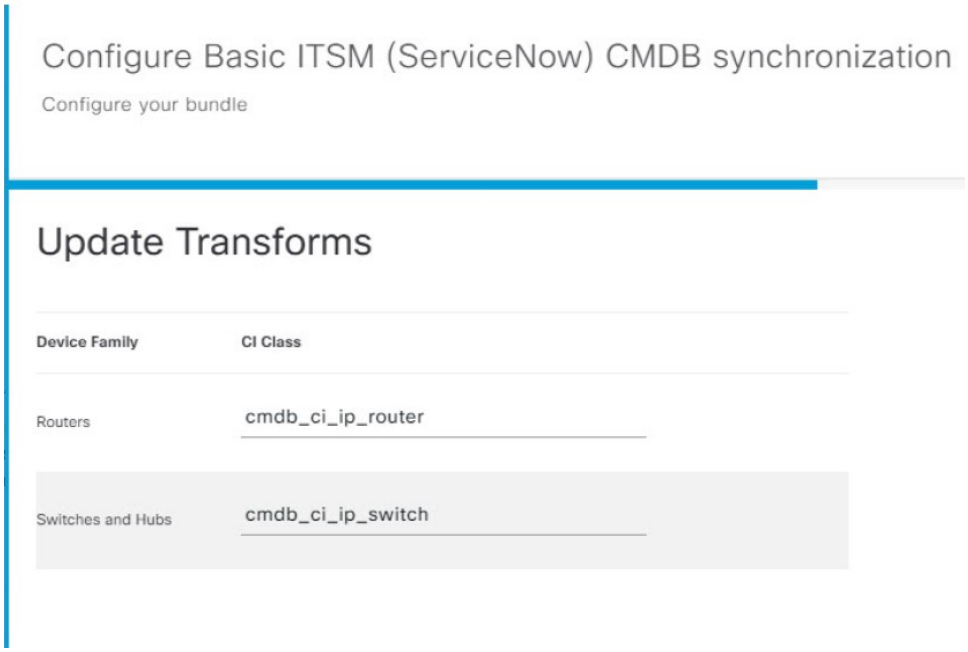
ステップ 18 前のステップで同期対象として選択したデータフィールドについて、デフォルトが属性または参照のどちらで設定されているか確認します。

データフィールドのデフォルトの設定を変更するには、目的のデータフィールドの設定（[Attribute] または [Reference]）をクリックします。

同期するデータフィールドと、データフィールドを属性または参照のどちらにするか選択したら、[Next] をクリックします。

ステップ 19 [Update Transforms] ウィンドウで、Catalyst Center デバイスファミリと ServiceNow CI クラス間の ServiceNow 変換マッピングを受け入れるか、更新します。

図 *10 : [Update Transforms]* ウィンドウ



デバイスファミリは Catalyst Center デバイスの分類（ユニファイド AP、ルータ、ワイヤレスコントローラ、スイッチ、ハブなど）であり、ServiceNow へのインベントリ属性/参照マッピングは ServiceNow の既存の Cisco Catalyst アプリケーションですでに使用できます。デバイスファミリのタイプと数は、ユーザーのネットワーク内のシスコデバイスによって異なります。

（注）
Catalyst Center プラットフォームは、ユーザーの Catalyst Center ネットワーク内のすべてのデバイスファミリを自動的に取得し、この GUI ウィンドウに表示できます。

CI クラスは ServiceNow のデータベーステーブルです（cmdb_ci_wap_network、cmdb_ci_ip_router、cmdb_ci_ip_switchr など）。上記の GUI ウィンドウの [CI Class] 列は、CI クラスをそれぞれのデバイスファミリにマッピングするために使用されます。

次の表に、Catalyst Center のデフォルトの CI クラスをデバイスファミリごとに示します。デフォルトの CI クラスは、ユーザーが変更できます。以下にリストされていない他のデバイスファミリの場合、シスコでは [CI Class] 列にデフォルト値を示しません。ServiceNow アプリケーションユーザーは、対応する CI クラスおよび属性/参照マッピングを手動で作成するか、既存の CI クラスを「親」CI クラスとして使用する必要があります。

表 *6 :* デフォルトのデバイスファミリから *CI* クラスへのマッピングリスト

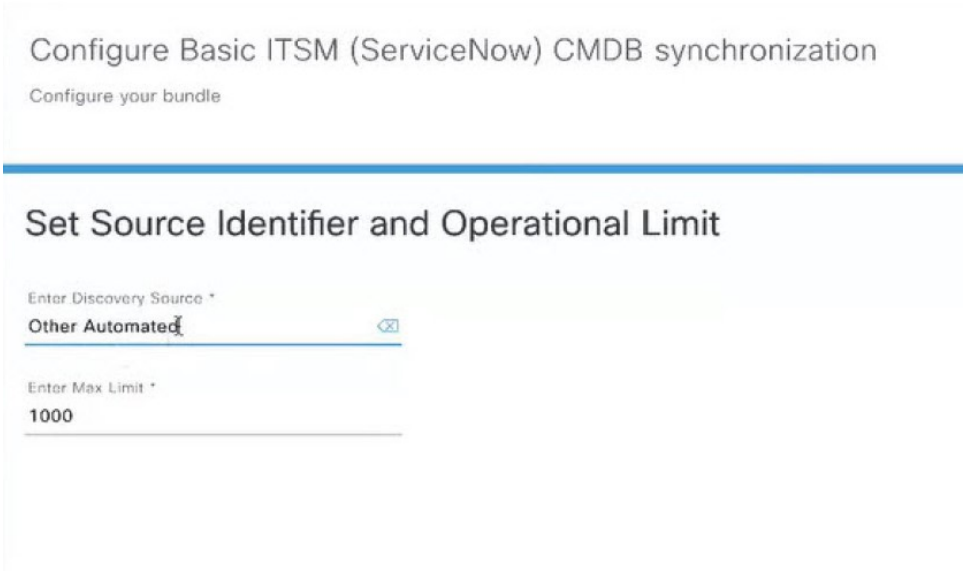
デバイスファミリ	対応する CI クラス
ユニファイド AP	cmdb_ci_wap_network
ワイヤレスコントローラ	x_caci_cisco_dna_wireless_lan_controller
ルータ	cmdb_ci_ip_router

デバイスファミリ	対応する CI クラス
スイッチおよびハブ	cmdb_ci_ip_switch
Meraki アクセスポイント	cmdb_ci_wap_network
Meraki カメラ	cmdb_ci_netgear
Meraki ダッシュボード	cmdb_ci_netgear
Meraki MX セキュリティアプライアンス	cmdb_ci_netgear
Meraki スイッチ	cmdb_ci_ip_switch

このウィンドウの情報を受け入れるか、更新したら、[Next] をクリックします。

ステップ 20 [Set Source Identifier and Operational Limit] ウィンドウで、データソースと最大制限を設定します。

図 *11 : [Set Source Identifier and Operational Limit]* ウィンドウ



次の値を設定します。

- [Enter Discovery Source]：以前に選択した値と同じ値を入力するか、デフォルトの [Other Automated] のままにします。
  - **[Synchronize device inventory directly with CMDB]**
  - **[Post device inventory details to a staging table]**

（注）
[Other Automated] は、OOB ServiceNow インスタンスの検出リソース属性の事前設定値です。これは、ServiceNow CI が検出されたデータソースを示す値です。デフォルトで、シスコは既存の事前設定値の 1 つを統合に使用します。

- [Enter Max Limit] ：反復（単一の API コール）で同期できるデバイスの最大数。

上記の情報を入力したら、[Next] をクリックします。

ステップ 21 [Summary] ウィンドウで、設定の概要を確認します。

情報を確認した後、[Configure] をクリックします。

設定が正常に完了すると、「**Done!**Bundle Configured」メッセージが表示されます。

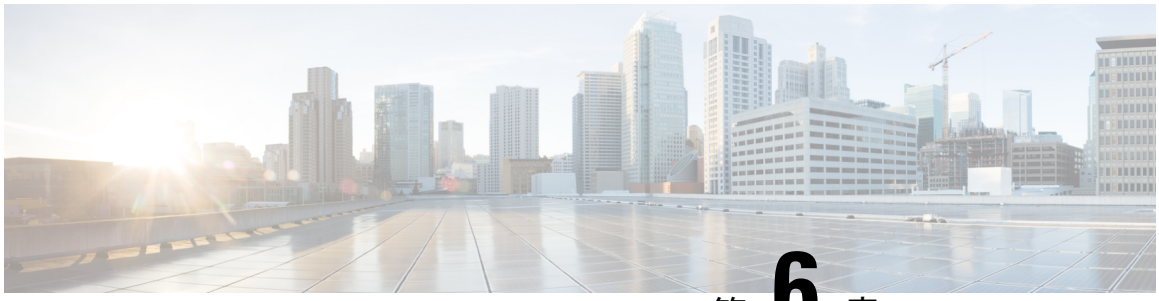
次のタスク

前述のいずれかの方法を使用して、このバンドル（[Schedule to Publish Inventory Details - ServiceNow Connector]）の統合フローを設定します。

設定を確認して、**[Manage]** > **[Configurations]** > **[General Settings]** の順に選択し、[Filter] または [Find] ツールを使用して、この手順で設定されたインスタンスを探します。必要であれば、今後は、[General Settings] ウィンドウで、インスタンスの編集、更新、削除ができるようになります。詳細については、全般設定の設定：インスタンスの編集 （139 ページ）を参照してください。

次のタスクを実行して、CMDB の同期をテストできます。

- Catalyst Center プラットフォーム の GUI で、メニューアイコンをクリックして次を選択します。 **[Platform]** > **[Runtime Dashboard]** > **[Event Summary]** の順に選択します。GUI ビューをリフレッシュするには、[Refresh] をクリックします。ウィンドウの個々のイベントをクリックして、イベントデータを表示し、ServiceNow へのリンクにアクセスします。
- ServiceNow に移動し、同期されたデバイスを検索します。そのデバイスのレコードの同期されたデータの [Configuration] タブと [Other Attributes] タブを確認します。



第 6 章

コンフィギュレーション

設定について

Catalyst Center プラットフォーム が提供する [**Configurations**] を使用すると、次のオプションにより、カスタマイズされたネットワーク エクスペリエンスを設定できます。

- [Event Settings]：Catalyst Center プラットフォームは、ネットワーク内で発生する特定の Cisco Catalyst Assurance イベント（またはインシデント）をサポートします。これは、Catalyst Center プラットフォームがこれらのイベントを認識できることを意味します。また、設定により、それらのイベントを Catalyst Center がレポートするタイプ、カテゴリ、およびシビラティ（重大度）をカスタマイズできます。この情報を GUI で設定することにより、Catalyst Center が ServiceNow などの外部システム（または、多くの場合、ユーザーが設定できる 1 つ以上の REST エンドポイント）に送信する情報をカスタマイズすることもできます。
- [General Settings]：1 つまたは複数のバンドル内の REST および ITSM エンドポイントインスタンスを追加または編集できます。

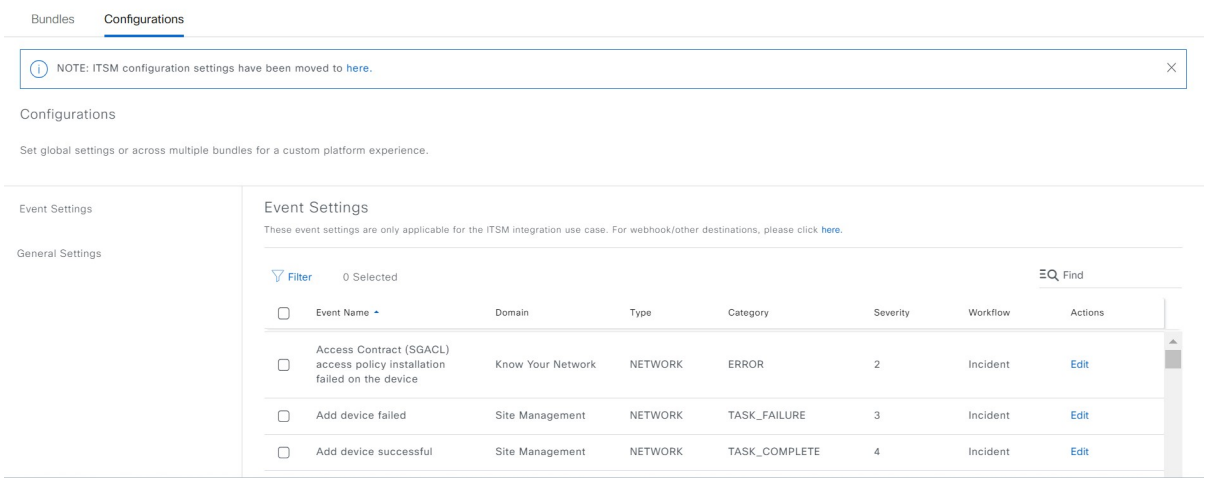
（注） また、各種の宛先を設定して、Catalyst Center プラットフォーム からイベントを配信することもできます。ウェブフック、電子メール、syslog、SNMP トラップ、または ITSM 宛先を設定するため、GUI ウィンドウにアクセスするには、メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** の順に選択します。

イベント設定の構成

ネットワーク内で発生する可能性があるプリセット番号の問題（またはイベント）が、[Configurations] ウィンドウの [Event Settings] にあります。これらのイベントのタイプ、カテゴリ、シビラティ（重大度）、およびワークフローを設定できます。

（注） [Event Settings] ウィンドウの機能は、ITSM（ServiceNow）の統合にのみ適用され、一般的なイベント通知には適用されません。Catalyst Center と ServiceNow の間の ITSM 統合を設定する一連のより大きな手順におけるこの手順の使用方法のガイダンスについては、『Cisco Catalyst Center ITSM Integration Guide』を参照してください。このウィンドウの上部のテキストに表示されるリンク（[here]）をクリックすると、プラットフォームの [Events] ウィンドウにアクセスし、イベントを登録して電子メール、ウェブフック（REST API）、SNMP トラップ、または Syslog サーバーで通知を受け取ることができます。

図 *12 : [Event Settings]* ウィンドウ



手順

ステップ 1 メインメニューから次を選択します。 **[Platform]** > **[Manage]** > **[Configurations]** > **[Event Settings]** の順に選択します。

ステップ 2 表示される [Event Settings] テーブルを確認します。

次の [**Event Settings**] 情報が表示されます。

- [Event Name]：Catalyst Center イベントの名前。
- [Domain]：Catalyst Center イベントのドメイン。
- [Type]：イベントのネットワーク、アプリ、システム、セキュリティ、または統合のタイプ。

- [Category]：エラー、警告、情報、アラート、タスクの進捗状況、タスクの完了。
- [Severity]：1 ～ 5。

（注）
シビラティ（重大度） 1 が最も優先順位が高く、最も重要または重大なイベントに割り当てます。

- [Workflow]：インシデント、問題、イベント、または RFC。
- [Actions]：編集。

[**Filter**] アイコンをクリックしてフィルタを使用するか、[**Find**] フィールドにキーワードを入力することで、テーブルに表示される内容を調整することができます。たとえば、すべてのアクセスポイントの通知を表示するには、[Find] フィールドに「AP」と入力します。すべてのネットワーク通知を表示するには、[Find] フィールドに「Network」と入力します。シビラティ（重大度） 1 のすべての通知を表示するには、[Find] フィールドに「1」と入力します。

その通知をネットワークの標準の表記法に合わせてカスタマイズするように、イベントを編集できます。

ステップ 3 [Actions] カラムの [Edit] をクリックして、イベントを編集します。

下向き矢印をクリックして設定を選択し、値を調整します。たとえば、[Network] をクリックして、[App] に調整します。これにより、イベントタイプはネットワークタイプからアプリケーションタイプに変更されます。[Severity] をクリックし、「5」から「1」に調整します。これにより、シビラティ（重大度）レベルが 5 から 1 に上がります。

ステップ 4 イベント名の横にあるボックスをクリックして、通知を有効にします。

これにより、将来イベントが発生した場合、Catalyst Center により通知が有効になります。

ステップ 5 [Save] をクリックして設定を保存します。

次のタスク

- メインメニューから次を選択します。**[Platform]** > **[Runtime Dashboard]** の順に選択します。

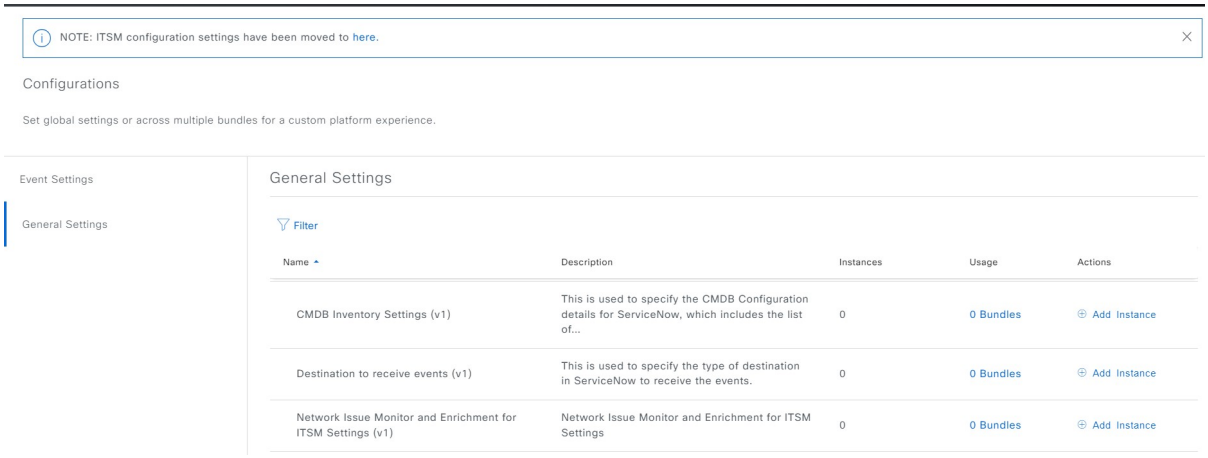
  [Events Summary] フィールドにイベントの通知が表示されます。

- [View Details] をクリックして通知を表示します。

全般設定の設定：インスタンスの編集

[Configurations] を使用して、1 つまたは複数のバンドル内のインスタンスを編集できます。

図 *13 : Catalyst Center* プラットフォーム *Configurations* ウィンドウ



始める前に

[Bundles] でネットワークのバンドルを有効化、設定、アクティベートします。[Bundles] の詳細については、バンドル機能 （118 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。[Platform] > [Manage] > [Configurations] > [General Settings] の順に選択します。

ステップ 2 表示される [General Settings] テーブルを確認します。

次の [**General Settings**] 情報が表示されます。

- [Name]：インスタンスの名前とバージョン。
- [Description]：インスタンスに含まれる設定の説明。
- [Instances]：現在設定されているインスタンスの数。
- [Usage]：1 つまたは複数のインスタンスが使用されるバンドルの数。
- [**Actions**]：設定で実行可能な特定のタスク（設定のためのインスタンスの編集または追加など）。

[**Filter**] アイコンをクリックしてフィルタを使用するか、[**Find**] フィールドにキーワードを入力することで、テーブルに表示される内容を調整することができます。

ステップ 3 表示されたいずれかのインスタンスの矢印をクリックします。たとえば、[CMDB Synchronization Settings (v1)] または [Destination to Receive Events (v1)] の矢印をクリックします。

設定のインスタンスの一覧が表示されます。

ステップ 4 [Usage] 列で、[Bundles] の上にマウス ポインタを重ねます。

Catalyst Center には、指定されたインスタンスを使用するバンドルが表示されます。

ステップ 5 [Actions] カラムの [Edit] アイコン（「パッドとペン」アイコン）をクリックし、既存のインスタンスを編集します。

以降の手順で、要件に合わせて適切なインスタンスを編集します。

ステップ 6 （オプション）[**CMDB Synchronization Settings**] インスタンスの CMDB の同期の詳細を編集するには、[**Edit** > **Actions**] の順にクリックし、表示されるスライドインペインで、次のインスタンスフィールドの 1 つまたは複数を編集します。

- [ServiceNow Access Settings]：ドロップダウンメニューからインスタンスを選択します。
- [CMDB Inventory Settings]：[Instance Name] と [Description] に入力します。
- [Select Destination]：[Destination Type] と [Destination URI] に入力します。オプションには、[Synchronize device inventory directly with CMDB] または [Post device inventory details to staging table] があります。
- [Select Inventory Data Fields]：同期するインベントリ データ フィールドを選択し、データフィールドが属性であるか参照であるかを選択します。
- [Update Transforms]：デバイスファミリに対して CI クラスを承認または更新します。
- [Set Source Identifier and Operational Limit]：検索ソースと上限を設定します。
- [Summary]：構成を確認し、変更を加えてから保存します。

ステップ 7 （オプション）[**Destination to receive events**] インスタンスを編集するには、[**Edit** > **Actions**] の順に選択し、スライドインペイン で、次のフィールドの 1 つまたは複数を編集します。

- [Instance Name]：インスタンスの名前。
- [Description]：インスタンスの説明。
- [**Destination to Receive Events**]：次のいずれかのオプションを選択します。
  - [Event Management]：Cisco Catalyst アプリを使用せずに Catalyst Center と ServiceNow の統合を設定する場合は、[Event Management] オプションを選択します。[Event Management] オプションを選択する場合、ServiceNow インスタンス内でイベント管理プラグインを設定する必要もあります。
  - [REST API Endpoint]：[REST API Endpoint] オプションは、Cisco Catalyst アプリで使用できます。データは、[REST API Endpoint] オプションを使用して Cisco Catalyst アプリ内の REST API エンドポイントに送信されます。
  - [Generic REST Endpoint in ServiceNow]：[Generic REST Endpoint in ServiceNow] オプションの場合、ServiceNow の別のステージングテーブルにデータを送信できます。
- [Destination URI]：[Generic REST Endpoint in ServiceNow] オプションの宛先 URI を入力します。このオプションでは、このフィールドは必須です。

Catalyst Center と ServiceNow の統合の詳細については、このリリースの『Cisco Catalyst Center ITSM Integration Guide』を参照してください。

ステップ 8 [Update] をクリックして編集したものをインスタンスに保存します。

インスタンスへの編集は即座に実行されます。

全般設定の設定：インスタンスの追加

[Configurations] を使用して、1 つまたは複数のバンドル内にインスタンスを追加できます。

始める前に

[Bundles] でネットワークのバンドルを有効化、設定、アクティベートします。[Bundles] の詳細については、バンドル機能 （118 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。[Platform] > [Manage] > [Configurations] > [General Settings] の順に選択します。

ステップ 2 表示される [General Settings] テーブルを確認します。

次の [**General Settings**] 情報が表示されます。

- [Name]：インスタンスの名前とバージョン。
- [Description]：インスタンスに含まれる設定の説明。
- [Instances]：設定のインスタンスの数。
- [Usage]：1 つまたは複数のインスタンスが使用されるバンドルの数。
- [Actions]：設定で実行可能な特定のタスク（設定のためのインスタンスの編集または追加など）。

[**Filter**] アイコンをクリックしてフィルタを使用するか、[**Find**] フィールドにキーワードを入力することで、テーブルに表示される内容を調整することができます。

ステップ 3 表示されたいずれかのインスタンスの矢印をクリックします。たとえば、[CMDB Synchronization Settings (v1)] または [Destination to Receive Events (v1)] の矢印をクリックします。

設定のインスタンスの一覧が表示されます。

ステップ 4 [Usage] 列で、[Bundles] の上にマウス ポインタを重ねます。

Catalyst Center には、指定されたインスタンスを使用するバンドルが表示されます。

ステップ 5 インスタンスを追加するには、[Actions] 列の [Add Instances] リンクをクリックします。

以降の手順で、要件に合わせて適切なインスタンスを追加します。

ステップ 6 （オプション）[**CMDB Synchronization Settings**] インスタンスを追加するには、[**Actions**] 列で [**Add Instance**] をクリックし、表示される スライドインペイン で次のインスタンスフィールドに入力します。

- [ServiceNow Access Settings]：ドロップダウンメニューからインスタンスを選択します。
- [CMDB Inventory Settings]：[Instance Name] と [Description] に入力します。
- [Select Destination]：[Destination Type] と [Destination URI] に入力します。オプションには、[Synchronize device inventory directly with CMDB] または [Post device inventory details to staging table] があります。
- [Select Inventory Data Fields]：同期するインベントリ データ フィールドを選択し、データフィールドが属性であるか参照であるかを選択します。
- [Update Transforms]：デバイスファミリに対して CI クラスを承認または更新します。
- [Set Source Identifier and Operational Limit]：検索ソースと上限を設定します。
- [Summary]：構成を確認し、変更を加えてから保存します。

ステップ 7 （オプション）[**Destination to receive events**] インスタンスを追加するには、[**Actions**] 列で [**Add Instance**] をクリックし、スライドインペイン で次のインスタンスフィールドに入力します。

- [Instance Name]：インスタンスの名前。
- [Description]：インスタンスの説明。
- [**Destination to Receive Events**]：次のいずれかを選択します。
  - [Event Management]：Cisco Catalyst アプリを使用せずに Catalyst Center と ServiceNow の統合を設定する場合は、[Event Management] オプションを選択します。[Event Management] オプションを選択する場合、ServiceNow インスタンス内でイベント管理プラグインを設定する必要もあります。
  - [REST API Endpoint]：[REST API Endpoint] オプションは、Cisco Catalyst アプリで使用できます。データは、[REST API Endpoint] オプションを使用して Cisco Catalyst アプリ内の REST API エンドポイントに送信されます。
  - [Generic REST Endpoint in ServiceNow]：[Generic REST Endpoint in ServiceNow] オプションの場合、ServiceNow の別のステージングテーブルにデータを送信できます。
- [Destination URI]：[Generic REST Endpoint in ServiceNow] オプションの宛先 URI を入力します。このオプションでは、このフィールドは必須です。

Catalyst Center と ServiceNow の統合の詳細については、このリリースの『*Cisco Catalyst Center ITSM Integration Guide*』を参照してください。

ステップ 8 [Add] をクリックしてインスタンスの追加を保存します。

インスタンスへの追加は即座に実行されます。

ウェブフックの宛先の設定

Catalyst Center では、イベントとレポートの両方の宛先としてウェブフックをサポートしています。

イベントまたはレポートのウェブフックの宛先を設定するには、Catalyst Center の GUI を使用して次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destination]** > **[Webhook]** の順に選択します。

ステップ 2 [Webhook] タブを確認します。

次のフィールドが表示されます。

- [Name]：ウェブフックの名前。
- [Description]：ウェブフックの説明（ユーザーが指定）。
- [URL]：ウェブフックの URL（コールバック URL）。
- [Method]：ウェブフックの REST API メソッド（POST）。
- [Edit]：設定済みのウェブフックを編集するためのフィールドを開くリンク。ウェブフック設定を編集したら、[Update] をクリックして変更を保存します。

このリリースでは、[URL] に IPv6 値を設定できます。

ステップ 3 [Add] をクリックしてウェブフックを設定します。

[Add Webhook] スライドインペインが表示されます。

ステップ 4 [Add Webhook] スライドインペインのフィールドに値を入力してウェブフックを設定します。

- [Name]：ウェブフックの名前。
- [Description]：ウェブフックの説明。
- [URL]：ウェブフックの URL アドレス（コールバック URL）。

ステップ 5 ウェブフックの構成に応じて、ウェブフックの URL に信頼できる証明書が関連付けられているかどうかを選択します。

[Trust Certificate] オプションボタンで、[Yes] または [No] をクリックします。

ステップ 6 ウェブフックの構成に応じて、ウェブフックの URL に関連付けられている認証タイプを選択します。

[Authentication] オプションボタンで、次のいずれかのオプションを選択します。

- [Basic]：クライアントが HTTP 要求を送信することで認証を行います。クライアントは、「**Basic**」という単語の後にスペースで区切って「*username:password*」の形式の base64 でエンコードされた文字列を入力した認証ヘッダーを含む HTTP 要求を送信します。GUI で [Basic] を選択すると、[Header Key] フィールドに「Authorization」という値が自動的に入力されます。
- [Token]：サーバーから提供されたセキュリティトークンを使用してユーザーが認証されます。[Token] を選択すると、下の [Header Key] フィールドに [X-Auth-Token] の値が入力されます。
- [No Authentication]：認証が不要になります。

ステップ 7 [Headers] で、[Header Name] と [Header Value] の値を入力します。

[Add] をクリックして、ヘッダーの名前と値を追加します。

（注）
選択する認証のタイプに応じて、ヘッダー名とヘッダー値が自動的に入力されます。

ステップ 8 [Save] をクリックして、ウェブフックの宛先の設定を保存します。

次のタスク

イベントまたはレポートのウェブフックの宛先を設定します。ウェブフックの宛先を使用してイベントまたはレポートを設定する手順については、イベント通知の使用 （214 ページ）および最初のレポートの実行 （152 ページ）を参照してください。

電子メールの宛先の設定

Catalyst Center では、イベントとレポートの両方の電子メール通知をサポートしています。

（注）

- 電子メールに正しい Catalyst Center ハイパーリンクを含めるには、[Integration Settings] ウィンドウで Catalyst Center の IP アドレスまたはホスト名を入力します。GUI を使用してこの情報を入力するには、メニューアイコンをクリックして次を選択します。**[System]** > **[Settings]** > **[System Configuration]** > **[Integration Settings]** の順に選択します。詳細については、統合設定の設定 （110 ページ）を参照してください。
- 電子メールの接続先にユーザー名とパスワードがすでに設定されている場合、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** に移動すると、セキュリティ上の理由からパスワードフィールドが空白になります。パスワードを更新するか、パスワードを変更せずにウィンドウを終了することができます。

この手順で説明するタスクを実行するには、適切な権限が必要になります。Catalyst Center プラットフォーム のロールベース アクセス コントロールの詳細については、プラットフォーム向けロールベース アクセス コントロールのサポート （112 ページ）を参照してください。

Catalyst Center GUI を使用してイベントまたはレポートの電子メールの宛先を設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

ステップ 2 必須の [Primary SMTP Server] フィールドを設定します。

- [Hostname/IP]：プライマリ SMTP サーバーのホスト名または IP アドレスを入力します。
- [Type]：ドロップダウンリストからプロトコルタイプを選択します。
- [Port]：ドロップダウンリストからサーバーのポート番号を選択します。

（注）
デフォルトのポート番号は 25 です。

- [Username]：プライマリ SMTP サーバーを認証するためのユーザー名を入力します。
- [Password]：プライマリ SMTP サーバーを認証するためのパスワードを入力します。

ステップ 3 オプションの [Secondary SMTP Server] フィールドを設定します。

- [Hostname/IP]：セカンダリ SMTP サーバーのホスト名または IP アドレスを入力します。
- [Type]：ドロップダウンリストからプロトコルタイプを選択します。
- [Port]：ドロップダウンリストからサーバーのポート番号を選択します。

（注）
デフォルトのポート番号は 25 です。

- [Username]：セカンダリ SMTP サーバーを認証するためのユーザー名を入力します。
- [Password]：セカンダリ SMTP サーバーを認証するためのパスワードを入力します。

ステップ 4 [Senders and Receivers] でテスト電子メールのフィールドを設定します。

- [From]：テスト電子メールの送信者。
- [To]：テスト電子メールの受信者。
- [Subject]：テスト電子メールの件名行のテキスト（最大 200 文字）を入力します。

ステップ 5 この電子メール構成をテストするには、[Test] をクリックします。

[Test] をクリックすると、設定したパラメータを使用してテスト電子メールが送信されます（プライマリおよびセカンダリの両方の SMTP サーバーの構成について、「Catalyst Center **SMTP configuration test email**」という件名で送信されます）。テスト電子メールの接続結果に基づいて、成功（設定の確認）または失敗のメッセージが表示されます。

ステップ 6 構成を保存するには、[Save] をクリックします。

構成をキャンセルするには、[Cancel] をクリックします。

次のタスク

イベントまたはレポートの電子メールの宛先を設定します。詳細については、イベント通知の使用 （214 ページ）および最初のレポートの実行 （152 ページ）を参照してください。

Syslog サーバーの接続先の設定

Catalyst Center は、イベント通知に関して Syslog サーバーの宛先をサポートしています。

Catalyst Center の GUI を使用してイベント通知に関する Syslog サーバーの宛先を設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。[System] > [Settings] > [External Services] > [Destination] > [Syslog] の順に選択します。 > > > >

ステップ 2 [Syslog] タブを確認します。

次のフィールドが表示されます。

- [Name]：Syslog サーバーの名前。
- [Description]：Syslog サーバーの説明。
- [Hostname/IP]：Syslog サーバーのホスト名または IP アドレス。
- [Port]：Syslog サーバーのポート番号。
- [Protocol]：TCP または UDP プロトコル。

ステップ 3 Syslog サーバーを設定するには、[Addition] アイコン（+）をクリックします。

ステップ 4 [Name] フィールドに、Syslog サーバーの名前を入力します。

ステップ 5 [Description] フィールドに、Syslog サーバーの簡単な説明を入力します。

ステップ 6 [Hostname/IP Address] フィールドに、ホスト名または IP アドレスを入力します。

ステップ 7 [Port] フィールドに、ポート番号を入力します。

ステップ 8 [Protocol] フィールドで、ドロップダウンリストからプロトコルを選択します。

ステップ 9 （任意） 構成をテストするには、[Validate] をクリックします。
設定が成功すると、検証メッセージが表示されます。

ステップ 10 Syslog サーバーの宛先の構成を保存するには、[Save] をクリックします。

構成をキャンセルするには、[Cancel] をクリックします。

次のタスク

イベント通知に関する Syslog サーバーの宛先を設定します。詳細については、イベント通知の使用 （214 ページ）を参照してください。

トラップ通知の設定

Catalyst Center は、SNMP トラップイベント通知をサポートしています。

Catalyst Center GUI を使用して SNMP トラップイベント通知を設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destination]** > **[SNMP]** の順に選択します。

ステップ 2 [SNMP] ウィンドウを確認します。

ステップ 3 [Add] をクリックしてトラップを設定します。

ステップ 4 次のフィールドを設定します。

- [Name]：イベントの名前。
- [Description]：イベントに関する単語またはフレーズ。
- [Hostname/IP Address]：SNMP トラップレシーバ（サーバー）のホスト名または IP アドレスを入力します。

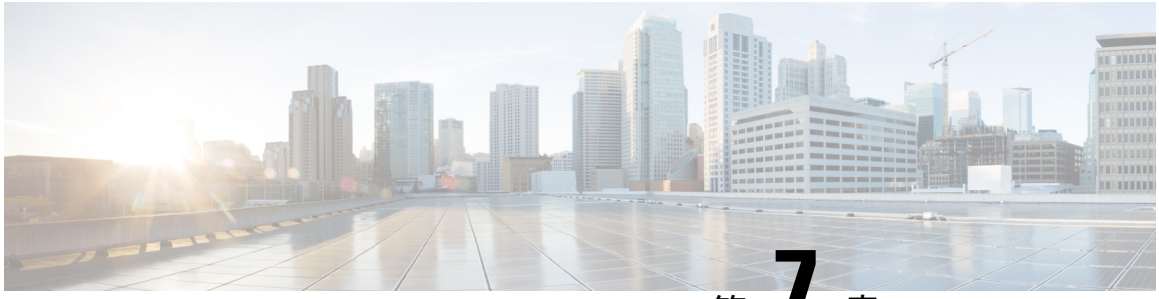
  [Hostname/IP address] に IPv6 値を設定できます。
- [Port]：SNMP トラップレシーバ（サーバー）のポート番号を入力します。
- [SNMP Version]：ドロップダウンリストから、SNMP バージョンを選択します。
  - [SNMP V2C]：SNMP バージョン 2C の場合は、コミュニティストリングを入力します。
  - [SNMP V3]：SNMP バージョン 3 の場合は、次の追加情報を入力します。
    - **ユーザー名（Username）**
    - [Mode]：ドロップダウンリストからモードを選択します。
      - [No Authentication, No Privacy] を選択した場合は、それ以上の設定は必要ありません。
      - [Authentication, No Privacy] の場合は、[Authentication Type]（SHA または MD5）、[Authentication Password]、および [Confirm Authentication Password] を設定します。

- [Authentication and Privacy] の場合は、[Authentication Type]（SHA または MD5）、[Authentication Password]、[Confirm Authentication Password] を設定します。さらに、[Privacy Type]（AES128、DES）、[Privacy Password]、および [Confirm Privacy Password] を設定します。

ステップ 5 [Save] をクリックします。

次のタスク

[Event Notifications] ウィンドウにアクセスして、1 つ以上のイベントを選択し、設定された SNMP トラップの宛先に登録します。メインメニューから次を選択します。**[Platform]** > **[Developer Toolkit]** > **[Event Notifications]** の順に選択します。SNMP トラップの宛先へのサブスクリプションをサポートするイベント（SYSTEM タイプのイベント）を選択し、登録します。



第 7 章

レポート

レポートについて

[Reports] 機能のデータを使用して、ネットワークとその動作に関する洞察を得ることができます。この機能では、運用のニーズに合わせて、さまざまな形式と柔軟なスケジュール オプションを使用してデータとレポートをカスタマイズできます。

[Reports] 機能は、次の使用例をサポートしています。

- キャパシティプランニング：アプリケーションがネットワーク内のデバイスをどのように利用しているのかを理解できます。

- パターンの変更：ネットワーク上の使用率のパターン（クライアント、デバイス、バンド、またはアプリケーション）が変更される方法のトレンドをトラッキング。
- 運用レポート：アップグレード完了やプロビジョニングの失敗などのネットワーク運用に関するレポートを確認します。
- ネットワークの正常性：レポートによってネットワークの全体的な正常性を判断します。

最初のレポートの実行

ネットワークについての専門的なデータレポートの実行を開始するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

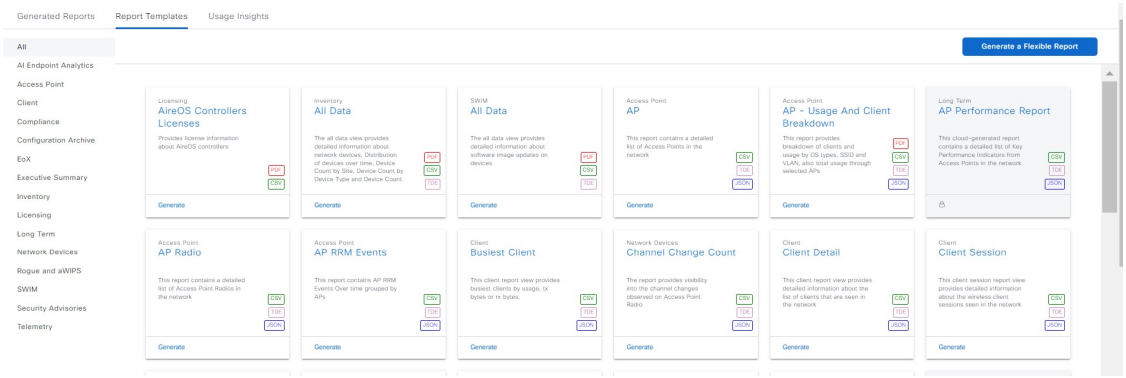
手順

ステップ 1 [Reports]メインメニューから次を選択します。。

ステップ 2 [Run Your First Report] ウィンドウで、[Start] をクリックします。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

図 *14 : [Report Templates]* ウィンドウ



（注）
使用可能なオプションは、選択したレポートのタイプによって異なります。

ステップ 3 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

各タイルはテンプレートを表し、それらのタイルにはレポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプ（PDF、CSV、TDE、JSON）が各タイル内にアイコンで示されます。

ステップ 4 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

そのサンプルレポートの [Preview] ウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、次のデータを示すサンプルレポート全体を確認します。

- 適用されたフィルタ（レポートの構築で使用されたデータフィルタ）。
- データメトリックとサマリー。
- データのグラフィカル表示（回線、バー、円グラフを含む）。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 5 [X] をクリックして、プレビューを閉じます。

ステップ 6 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[Generate] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 7 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックしてウィザードを開始します。

または、メニューアイコンをクリックして次を選択します。**[Workflows]** > **[Generating a New Report]** を選択して、新しいレポートを生成するためのウィザードを起動します。

ステップ 8 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 9 [Setup Report Scope] ウィンドウで、レポートの名前を入力して範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックします。

（注）
[Setup Report Scope] オプションは、選択した [Template Group] に応じて変わります。

[Next] をクリックします。

ステップ 10 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [File Type] オプションを使用できます。

- **PDF**

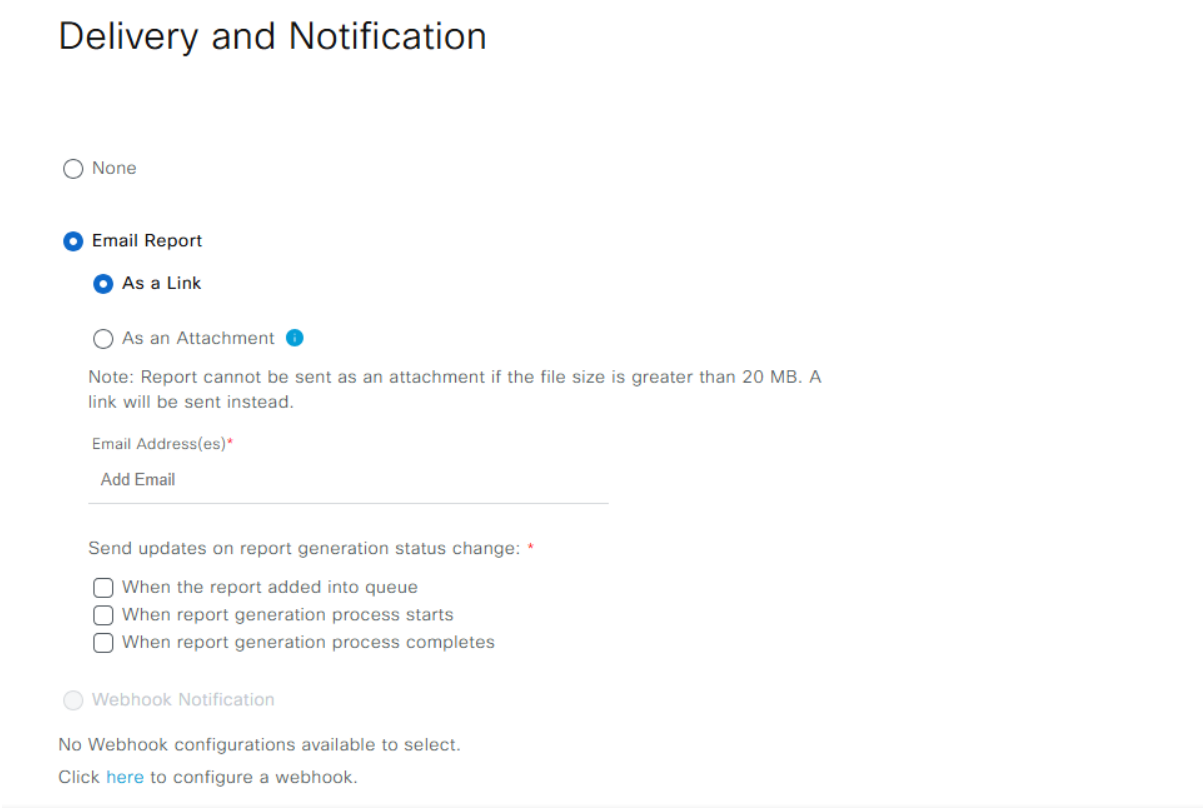
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [CSV]、[JSON]、[Tableau Data Extract] の場合、[Fields] オプションを使用して、CSV、JSON、Tableau Data Extract から作成するレポートの属性を選択します。

ステップ 11 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。次に、[Next] をクリックします。

ステップ 12 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

図 *15 : [Delivery and Notification]* ウィンドウ



- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートをリンクまたは添付ファイルとして受信します。

（注）
電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

- [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

  （注）
  レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

- [Attachment]：レポートが電子メール通知に添付されます。

  （注）
  PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

  （注）
  まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

  ウェブフック通知の形式でレポートのステータス（「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」など）が届きます。これらの通知は、GUI で表示することもできます。

ステップ 13 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 14 [View all Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

アクセスポイントレポートの実行

ネットワークについての [**Access Point**] （AP）レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

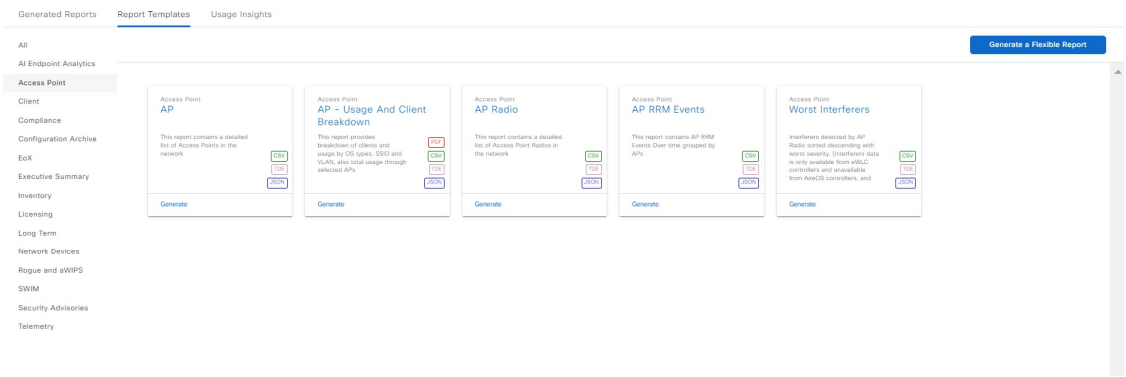
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、選択されたカテゴリでサポートされているレポートが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *16 : AP* レポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。レポートの生成に使用するテンプレートを選びます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[Generate] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、[Template] ドロップダウンリストからテンプレートを選択します。

（注）
[**Template**] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

ステップ 8 **[Next]** をクリックします。

ステップ 9 [**Setup Report Scope**] ウィンドウで、レポートの名前を指定して範囲と時間範囲を選択します。

[**Report Name**] フィールドにレポート名を入力し、[**Scope**] をクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。AP レポートのデータは最大 90 日間保持されます。

ステップ 10 [Next] をクリックします。

ステップ 11 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [CSV]、[JSON]、[Tableau Data Extract] の場合、[Fields] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

ステップ 12 **[Next]** をクリックします。

ステップ 13 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。次に、[Next] をクリックします。

ステップ 14 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。

- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  （注）
  電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [**As a Link**]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[**Reports**] の [**Generated Reports**] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  - [As an Attachment]：レポートが電子メール通知に添付されます。

    （注）
    PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  Catalyst Center は、レポートに関する次の電子メール通知を送信します。

  - レポートは、実行待ちのキュー内にあります。
  - インポートプロセスは進行中です。
  - レポートのコンパイルが正常に完了しました。

  通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

  （注）
  まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

  Catalyst Center は、レポートについて、次のステータスのウェブフック通知を送信します。

  - In Queue
  - In Progress
  - Success

ステップ 15 **[Next]** をクリックします。

ステップ 16 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 17 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

監査ログレポートの実行

ネットワークの [**Audit Log**] レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

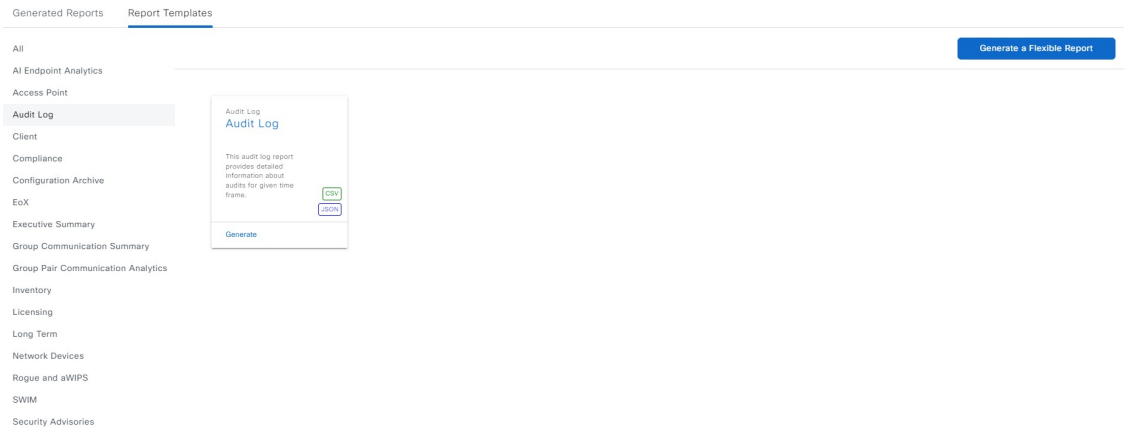
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、選択されたカテゴリでサポートされているレポートが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *17* : 監査ログレポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートがウィンドウに表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[**Template**] リストには、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

ステップ 8 **[Next]** をクリックします。

ステップ 9 [Setup Report Scope] ウィンドウで、レポートの名前を指定して範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。

[Next] をクリックします。

ステップ 10 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

Catalyst Center では、監査ログレポートタイプに次の [**File Type**] オプションが表示されます。

- **CSV**
- **JSON**

ファイルタイプが [**CSV**] および [**JSON**] の場合、[**Fields**] オプションで、[**CSV**] および [**JSON**] の結果についての属性を選択できます。

ステップ 11 [Next] をクリックします。

ステップ 12 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。次に、[Next] をクリックします。

ステップ 13 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

（注）
電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  - [Attachment]：レポートが電子メール通知に添付されます。

    （注）
    PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。

- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [**Webhook Notification**]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリストからウェブフックを選択します（[**Subscription Profile**] フィールド）。

（注）
まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUI で表示することもできます。

ステップ 14 **[Next]** をクリックします。

ステップ 15 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 16 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

クライアントレポートの実行

ネットワークについての専門的な**クライアント**レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択して結果を表示します。

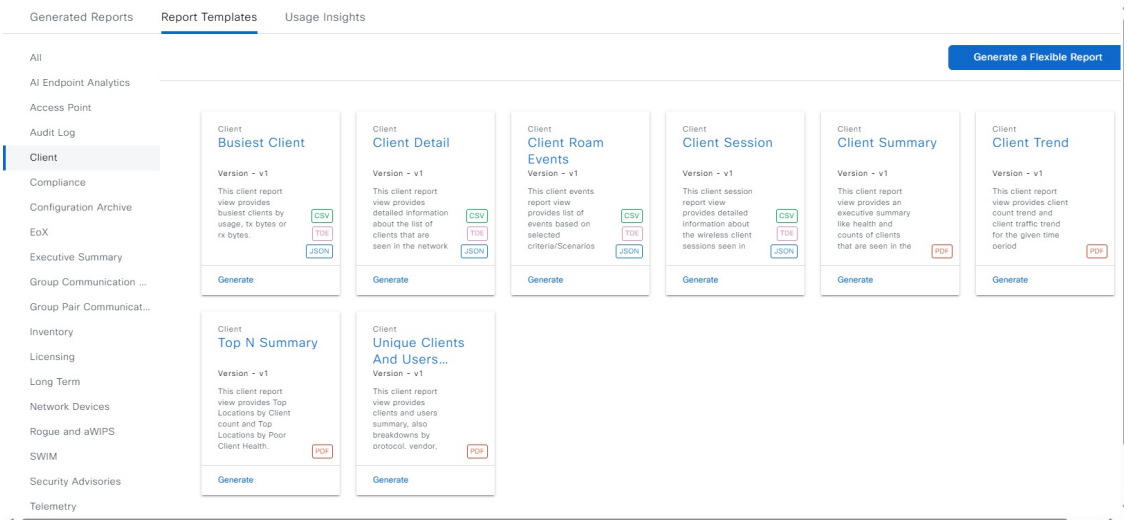
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、選択されたカテゴリでサポートされているレポートが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *18* : クライアントレポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。一部のクライアントレポートで表示されるデータを次に示します。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。
- データメトリックとサマリー。
- データのグラフィカル表示（回線、バー、円グラフを含む）。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

ステップ 8 **[Next]** をクリックします。

ステップ 9 [Setup Report Scope] ウィンドウで、レポートの名前を指定して範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。クライアントレポートのデータは最大 90 日間保持されます。

[Next] をクリックします。

ステップ 10 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [**CSV**]、[**JSON**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

ステップ 11 [Next] をクリックします。

ステップ 12 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。次に、[Next] をクリックします。

ステップ 13 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

（注）
電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

- [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

  （注）
  レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

- [Attachment]：レポートが電子メール通知に添付されます。

  （注）
  PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

  （注）
  まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

  レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUI で表示することもできます。

ステップ 14 **[Next]** をクリックします。

ステップ 15 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 16 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

コンプライアンスレポートの実行

Catalyst Center では、個々のネットワークデバイスのコンプライアンスステータスを示す統合されたコンプライアンス監査レポートを取得できます。このレポートを使用すると、ネットワークを完全に可視化できます。

この手順では、ネットワークに関する [**Compliance**] レポートを設定する方法について説明します。

手順

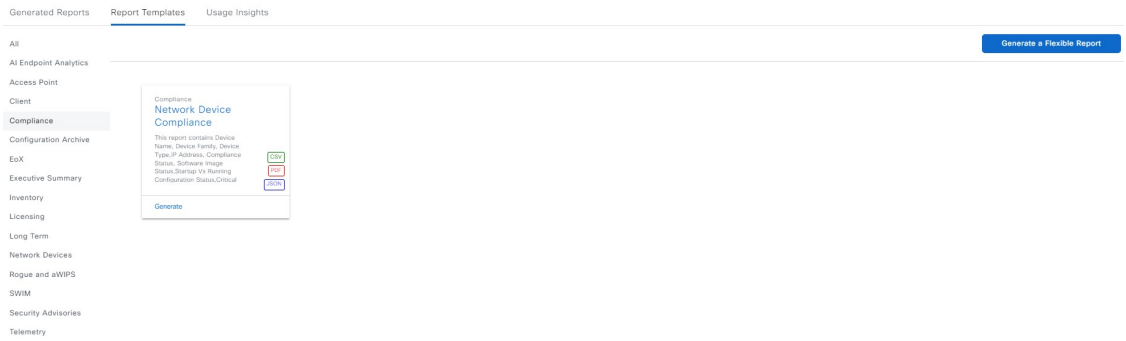
ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。

ステップ 2 左側のペインで、[Compliance] をクリックして、コンプライアンスのテンプレートを表示します。

各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。

図 *19* : コンプライアンスレポート



ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、[Template] ドロップダウンリストからテンプレートを変更できます。

（注）
同じウィンドウで自動生成されたサンプルを確認できます。

ステップ 8 [Next] をクリックします。

[Setup Report Scope] ウィンドウが表示されます。

ステップ 9 [Report Name] フィールドに、レポート名を入力します。

ステップ 10 [Scope] 領域で、レポートに含める [Compliance Status]、[Compliance Category]、[Device Family]、[Device Type] を選択します。

（注）
[Setup Report Scope] オプションは、選択したテンプレートに応じて変わります。

ステップ 11 [Next] をクリックします。

ステップ 12 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

Catalyst Center には、コンプライアンスレポートタイプの次の [**File Type**] オプションが表示されます。

- **PDF**
- **CSV**
- **JSON**

ファイルタイプが [**CSV**] および [**JSON**] の場合、[**Fields**] オプションで、[**CSV**] および [**JSON**] の結果についての属性を選択できます。

ステップ 13 [Next] をクリックします。

ステップ 14 [**Schedule Report**] ウィンドウで、レポートのスケジュールを選択します。次に、[Next] をクリックします。

ステップ 15 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  電子メールの SMTP サーバーが設定されていない場合は、Catalyst Center により、設定するように求められます。リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** で電子メールの宛先を設定します。

  - [As a Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ページへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）

レポートへのリンクが埋め込まれた電子メール通知は、最大20の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームにより電子メールアドレスが検証され、構文が正しくない場合は通知されます。

- [As an Attachment]：レポートが電子メール通知に添付されます。

（注）
PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームにより電子メールアドレスが検証され、構文が正しくない場合は通知されます。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。

（注）
ウェブフックが作成されていない場合は、Catalyst Center により、作成するように求められます。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の [Webhook] タブでリンクをクリックしてウェブフックを設定します。

Catalyst Center は、レポートに関する次のステータスウェブフック通知を送信します。

- In Queue
- In Progress
- Success

[Platform] > **[Runtime Dashboard]** > **[Event Summary]** でイベント通知ステータスを確認できます。

ステップ 16 **[Next]** をクリックします。

ステップ 17 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

ステップ 18 [Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 19 [View the Generated Reports] リンクをクリックします。

[**Generated Reports**] ウィンドウが表示され、スケジュールされたレポートのインスタンスの詳細が示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、「生成されたレポートの表示」を参照してください。

設定アーカイブレポートの実行

ネットワークデバイスの設定変更の統合レポートを取得するには、次の手順を使用します。

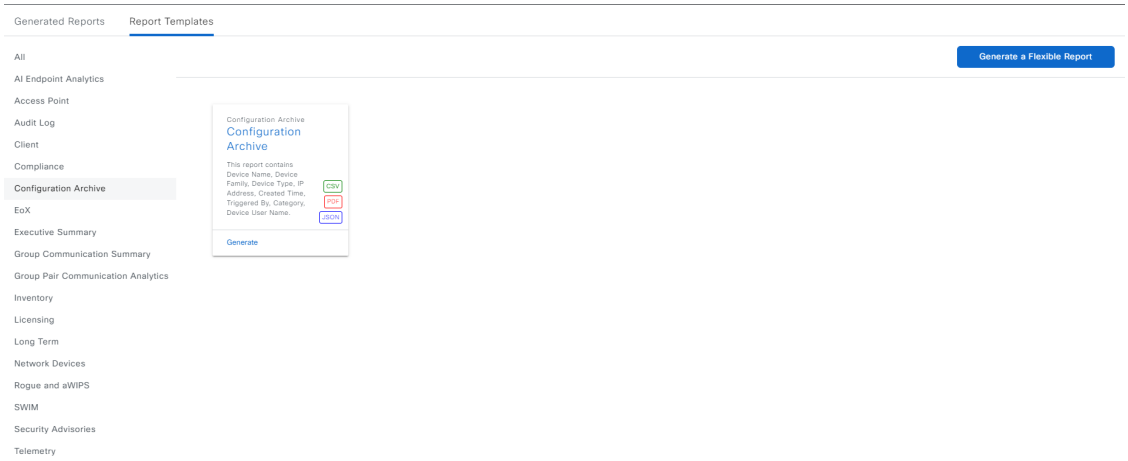
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。

ステップ 2 左側のペインで [Configuration Archive] をクリックしてテンプレートを表示します。

図 *20 :* 設定アーカイブレポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、[Template] ドロップダウンリストからテンプレートを変更できます。

（注）
同じウィンドウで自動生成されたサンプルを確認できます。

ステップ 8 [Next] をクリックします。

[Setup Report Scope] ウィンドウが表示されます。

ステップ 9 [Report Name] フィールドに、レポート名を入力します。

ステップ 10 [**Scope**] エリアで、ドロップダウンリストから [**Category**] を選択します。

[In band] は、Catalyst Center によって行われた設定変更を指します。

[Out Of Band] は、Catalyst Center 外部で行われた設定変更を指します。

ステップ 11 レポートに含める [**Device Family**] と [**Device Type**] を選択します。

（注）
[Setup Report Scope] オプションは、選択したテンプレートに応じて変わります。

ステップ 12 [Next] をクリックします。

ステップ 13 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

Catalyst Center には、構成アーカイブレポートタイプの次の [**File Type**] オプションが表示されます。

- **PDF**
- **CSV**
- **JSON**

ファイルタイプが [**CSV**] および [**JSON**] の場合、[**Fields**] オプションで、[**CSV**] および [**JSON**] の結果についての属性を選択できます。

ステップ 14 [Next] をクリックします。

ステップ 15 [**Schedule Report**] ウィンドウで、レポートのスケジュールを選択します。次に、[Next] をクリックします。

ステップ 16 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  電子メールの SMTP サーバーが設定されていない場合は、Catalyst Center により、設定するように求められます。リンクをクリックし、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** で電子メールの宛先を設定します。

  - [As a Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ページへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

（注）
レポートへのリンクが埋め込まれた電子メール通知は、最大20の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）[Enter] を押す必要があります。Catalyst Centerプラットフォームにより電子メールアドレスが検証され、構文が正しくない場合は通知されます。

- [As an Attachment]：レポートが電子メール通知に添付されます。

（注）
PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）[Enter] を押す必要があります。Catalyst Center プラットフォームにより電子メールアドレスが検証され、構文が正しくない場合は通知されます。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。

（注）
ウェブフックが作成されていない場合は、Catalyst Center により、作成するように求められます。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の [Webhook] タブでリンクをクリックしてウェブフックを設定します。

Catalyst Center は、レポートに関する次のステータスウェブフック通知を送信します。

- In Queue
- In Progress
- Success

[**Platform** > **Runtime Dashboard** > **Event Summary**] でイベント通知ステータスを確認できます。

ステップ 17 **[Next]** をクリックします。

ステップ 18 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

ステップ 19 [Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 20 [View the Generated Reports] リンクをクリックします。

[**Generated Reports**] ウィンドウが表示され、スケジュールされたレポートのインスタンスの詳細が示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、「生成されたレポートの表示」を参照してください。

サポート終了レポートの実行

次の手順では、ネットワークに関する [**End of Life (EoX)**] レポートを設定する方法について説明します。

始める前に

- ソフトウェアをダウンロードする前、またはデバイスをプロビジョニングする前に、エンドユーザーライセンス契約（EULA）に同意する必要があります。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Accept the License Agreement」のトピックを参照してください。
- Cisco CX クラウド接続が有効になっていることを確認します。詳細については、*Cisco Catalyst Center Administrator Guide* の [Update the Machine Reasoning Knowledge Base] を参照してください。
- 正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択して結果を表示します。

手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウが開き、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。

[Report Templates] ウィンドウでは、各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。生成に使用するテンプレートを選びます。

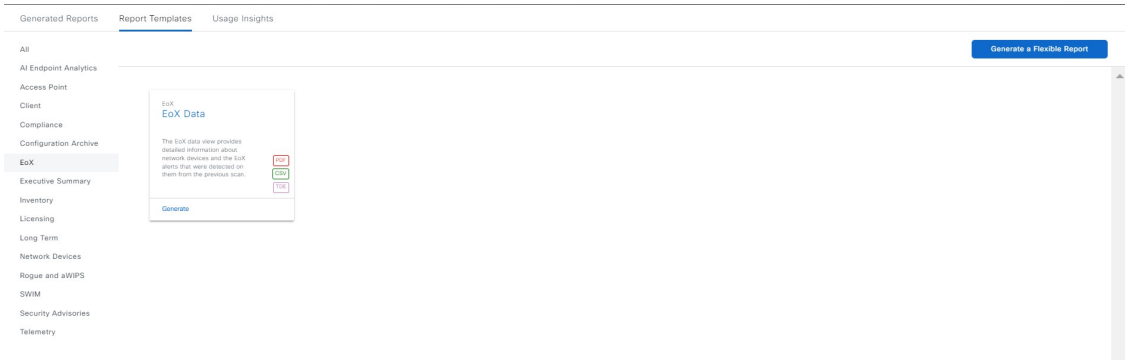
ステップ 2 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。

ステップ 3 [X] をクリックして、プレビューを閉じます。

ステップ 4 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

図 *21 : EoX* レポート



ステップ 5 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 6 [**Select Report Template**] ウィンドウで、[**Template**] ドロップダウンリストからテンプレートを選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

ステップ 7 [Next] をクリックします。

[**Setup Report Scope**] ウィンドウが表示されます。

ステップ 8 [Report Name] フィールドに、レポート名を入力します。

ステップ 9 [**Scope**] 領域で、レポートに含める [**Device Type**] と [**Location**] を選択します。

（注）
[Setup Report Scope] オプションは、選択したテンプレートに応じて変わります。

ステップ 10 [Next] をクリックします。

ステップ 11 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

レポートに基づいて、Catalyst Center には [**File Type**] オプションが表示されます。

- **PDF**
- **CSV**
- **Tableau Data Extract**

ファイルタイプが [**CSV**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、[**CSV**]、[**Tableau Data Extract**] から作成するレポートの属性（追加フィールド）を選択できます。

ステップ 12 [Next] をクリックします。

[Schedule Report] ウィンドウで、レポートのスケジュールを選択します。

ステップ 13 [Next] をクリックします。

ステップ 14 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  Catalyst Center GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。

  電子メールの SMTP サーバーが設定されていない場合は、Catalyst Center により、設定するように求められます。

  - [As a Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ページへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームにより電子メールアドレスが検証され、構文が正しくない場合は通知されます。

  - [As an Attachment]：レポートが電子メール通知に添付されます。

    （注）
    PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームにより電子メールアドレスが検証され、構文が正しくない場合は通知されます。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。

（注）
ウェブフックが作成されていない場合は、Catalyst Center により、作成するように求められます。Catalyst Center GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。

Catalyst Center は、レポートに関する次のステータスウェブフック通知を送信します。

- In Queue
- In Progress

- Success

これらの通知は、GUI で表示できます。

ステップ 15 **[Next]** をクリックします。

ステップ 16 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

ステップ 17 [Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 18 [View the Generated Reports] リンクをクリックします。

[**Generated Reports**] ウィンドウが表示され、スケジュールされたレポートのインスタンスの詳細が示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、「生成されたレポートの表示」を参照してください。

エグゼクティブサマリーレポートの実行

ネットワークについての [**Executive Summary**] レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択して結果を表示します。

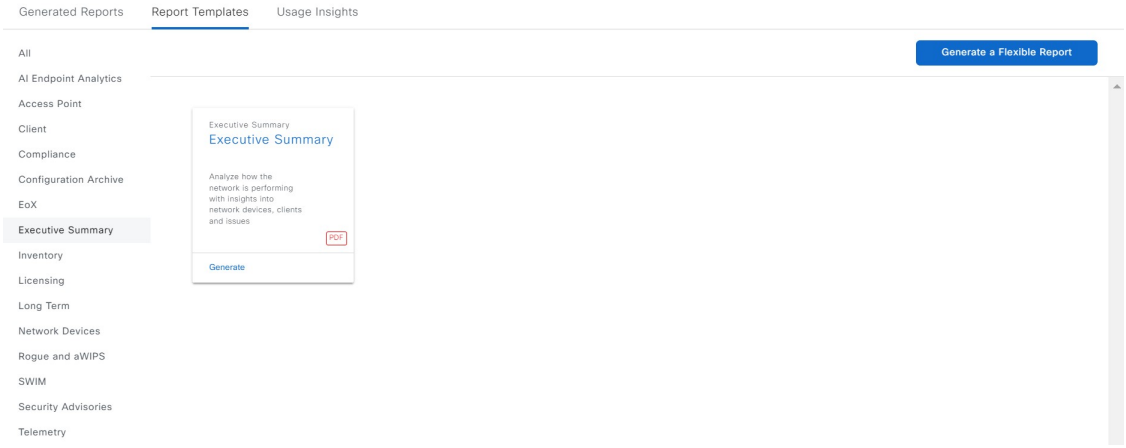
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *22* : エグゼクティブ サマリー レポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプがタイル内にアイコンで示されます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- データメトリックとサマリー。
- データのグラフィカル表示（回線、バー、円グラフを含む）。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 8 [**Setup Report Scope**] ウィンドウで、レポートの名前を指定して範囲と時間範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。[Executive Summary] レポートのデータは最大 90 日間保持されます。

[Next] をクリックします。

ステップ 9 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [**CSV**]、[**JSON**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

[Next] をクリックします。

ステップ 10 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。次に、[Next] をクリックします。

ステップ 11 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  （注）
  電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。[**System** > **Settings** > **External Services** > **Destinations** > **Email**] の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  - [Attachment]：レポートが電子メール通知に添付されます。

（注）
PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

（注）
まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUI で表示することもできます。

[Next] をクリックします。

ステップ 12 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 13 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

インベントリレポートの実行

ネットワークについての [**Inventory**] レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

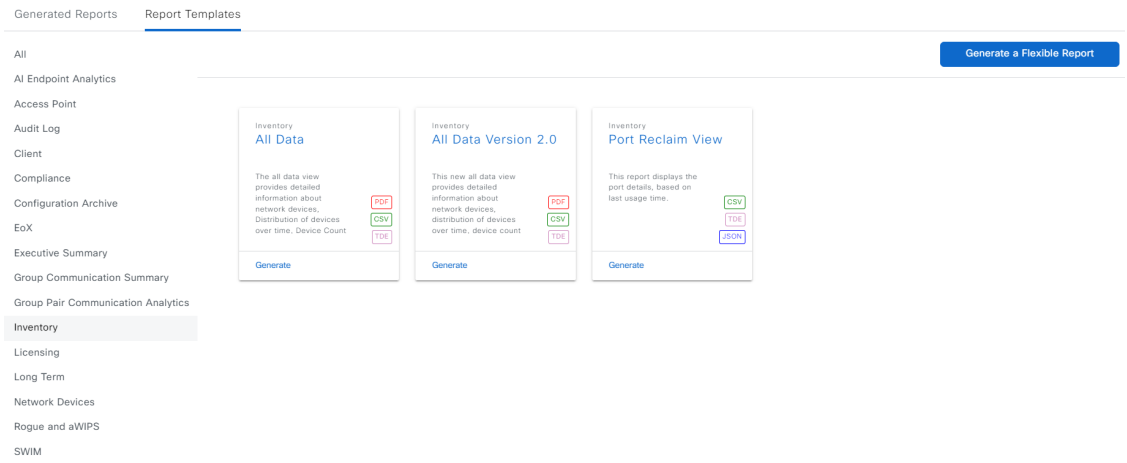
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *23* : インベントリレポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプがタイル内にアイコンで示されます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートがウィンドウに表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。
- データメトリックとサマリー。
- データのグラフィカル表示（回線、バー、円グラフを含む）。
- データの分析を支援するテーブル。

（注）

サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 8 [Setup Report Scope] ウィンドウで、レポートの名前を指定して範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックします。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。

[Next] をクリックします。

ステップ 9 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

ステップ 10 [Next] をクリックします。

ステップ 11 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。

[Next] をクリックします。

ステップ 12 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  （注）
  電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

（注）
レポートへのリンクが埋め込まれた電子メール通知は、最大20の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enterを押す必要があります。Catalyst Centerプラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

- [Attachment]：レポートが電子メール通知に添付されます。

（注）
PDFレポートは、最大20 MBの電子メール通知添付ファイルと最大10の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enterを押す必要があります。Catalyst Centerプラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

Catalyst Centerは、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

（注）
まだウェブフックを作成していない場合は作成するように求められます。GUIの[Webhook]タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUIで表示することもできます。

[Next] をクリックします。

ステップ 13 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 14 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

ライセンスレポートの実行

ネットワークについての [**Licensing**] レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

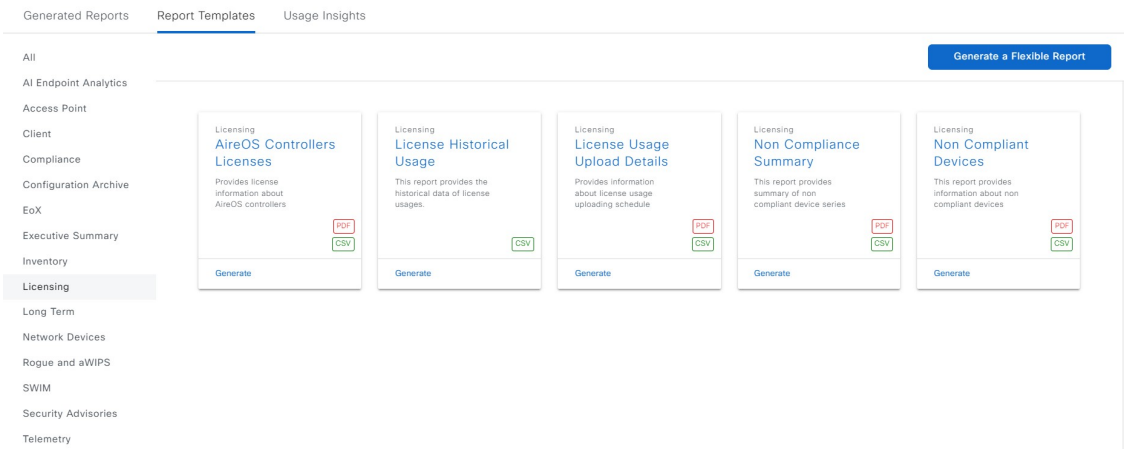
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *24* : ライセンスレポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプがタイル内にアイコンで示されます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。
- データメトリックとサマリー。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 8 [**Setup Report Scope**] ウィンドウで、レポートの名前を指定して範囲と時間範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールド内をクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。

[Next] をクリックします。

ステップ 9 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [**CSV**]、[**JSON**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

[Next] をクリックします。

ステップ 10 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。

[Next] をクリックします。

ステップ 11 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

（注）
電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、レポートへのリンクと、[Reports] の [Generate Reports] ウィンドウへのリンクがあります。ここから、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  - [Attachment]：レポートが電子メール通知に添付されます。

    （注）
    PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  Catalyst Center は、レポートに関する次の電子メール通知を送信します。

  - レポートは、実行待ちのキュー内にあります。
  - インポートプロセスは進行中です。
  - レポートのコンパイルが正常に完了しました。

  通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

（注）
まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

レポートのステータスウェブフック通知（「In Queue」、「In Progress」、「Success」など）が届きます。これらの通知は、GUI で表示することもできます。

[Next] をクリックします。

ステップ 12 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 13 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

ネットワーク デバイス レポートの実行

ネットワークについての [**Network Devices**] レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択して結果を表示します。

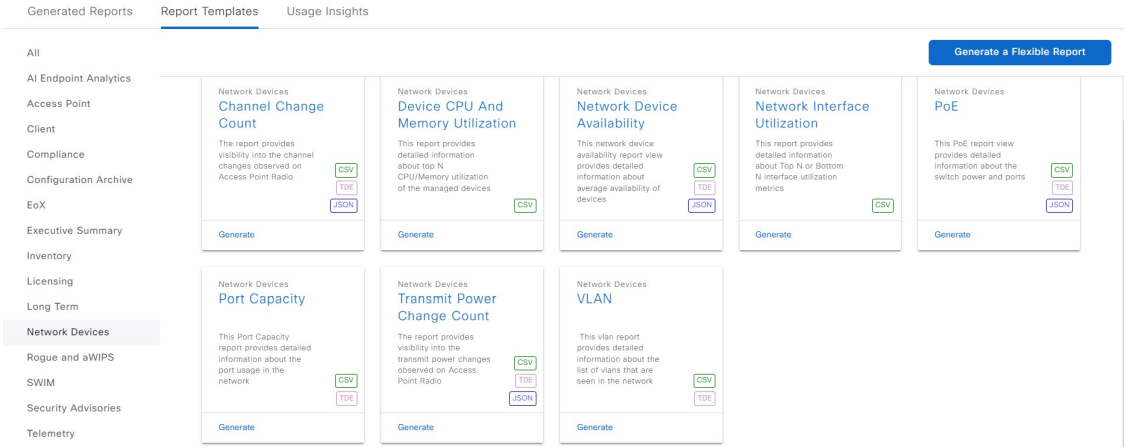
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。各カテゴリはリンクで表されます。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *25* : ネットワーク デバイス レポート



各テンプレートはタイルで表され、レポートに関する情報とレポートを設定（生成）するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプがタイル内にアイコンで示されます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。
- データメトリックとサマリー。
- データのグラフィカル表示（回線、バー、円グラフを含む）。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

ステップ 7 [Setup the Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンメニューから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 8 [**Setup Report Scope**] ウィンドウで、レポートの名前を指定して範囲と時間範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。

[Next] をクリックします。

ステップ 9 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [**CSV**]、[**JSON**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

[Next] をクリックします。

ステップ 10 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。

[Next] をクリックします。

ステップ 11 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

（注）
電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知に、元のレポートと [Reports] の [Generated Reports] ウィンドウへのリンクが含まれます。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

- [Attachment]：レポートが電子メール通知に添付されます。

  （注）
  PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンメニュー（[Subscription Profile] フィールド）からウェブフックを選択します。

  （注）
  まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

  レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUI で表示することもできます。

[Next] をクリックします。

ステップ 12 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 13 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

不正および aWIPS レポートの実行

ネットワークについての [**Rogue and aWIPS**] レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

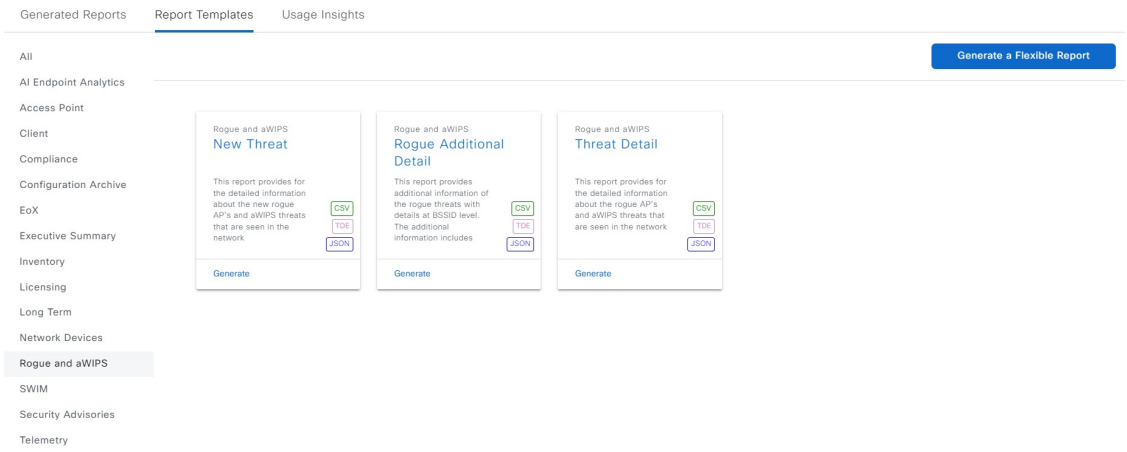
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *26 :* 不正および *aWIPS* レポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプがタイル内にアイコンで示されます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。

- データメトリックとサマリー。
- データのグラフィカル表示（回線、バー、円グラフを含む）。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 8 [**Setup Report Scope**] ウィンドウで、レポートの名前を指定して範囲と時間範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
- [Setup Report Scope] オプションは、選択した [Template] に応じて異なります。
- ネットワーク内のすべての AP がフロアに割り当てられておらず、[**Location**] フィルタで [**Global**] を選択した場合、[**Rogue and aWIPS**] レポートには、グローバル階層の下で割り当てられた AP に関連付けられた脅威のみが表示されます。割り当てられていない AP に関連する脅威を表示するには、[Location] フィルタを空のままにしておく必要があります。

[Next] をクリックします。

ステップ 9 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [**CSV**]、[**JSON**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

[Next] をクリックします。

ステップ 10 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。

[Next] をクリックします。

ステップ 11 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

（注）
電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  - [Attachment]：レポートが電子メール通知に添付されます。

    （注）
    PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  Catalyst Center は、レポートに関する次の電子メール通知を送信します。

  - レポートは、実行待ちのキュー内にあります。
  - インポートプロセスは進行中です。
  - レポートのコンパイルが正常に完了しました。

  通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [**Webhook Notification**]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリストからウェブフックを選択します（[**Subscription Profile**] フィールド）。

（注）
まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUI で表示することもできます。

[Next] をクリックします。

ステップ 12 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 13 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

ROI レポートの実行

Catalyst Center プラットフォームの ROI インサイトレポートは、Catalyst Center によるネットワーク運用の生産性向上、および従来の NMS と比較した ROI に関する知見を示すカスタマイズされたレポートです。

次の手順では、ネットワーク運用に関する ROI レポートを設定する方法について説明します。

手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Usage Insights]** の順に選択します。

[**Usage Insights**] ウィンドウには、次の情報が表示されます。

- [SAVINGS]：選択した時間範囲について、Catalyst Center によるネットワーク運用で節約された時間とコストが表示されます。
- [**ROI Insights**]：[Features]、[Time and Cost Saved]、[Usage KPI]、[Traditional NMS] の時間、[Actions] に基づいて作成された ROI インサイトレポートが表示されます。
- [Savings Trends]：ROI インサイトレポートの [Cost] と [Time] の節約傾向が表示されます。

（注）

[Savings Trends] 領域は、選択した時間範囲が 1 か月を超えている場合にのみ表示されます。

ステップ 2 [Campus Network Assurance]、[Network Device Onboarding]、[Campus Software Image Management]、[Campus Network Segmentation] の各領域で、従来の NMS および Catalyst Center の [Hours] と [Minutes] の名前フィールドに時間の節約を入力します。

- [Traditional NMS]：Catalyst Center なしでネットワークの問題を検出して解決するのに要する平均時間。
- [Catalyst Center]：Catalyst Center でネットワークの問題を検出して解決するのに要する平均時間。

ステップ 3 [Cost Inputs] と [IT Inputs] を変更するには、[Customize ROI Insights] をクリックして変更を加えます。

[Customize ROI Insights] 領域には、事前設定済みの [Cost per IT Staff]、[Currency]、[No. of IT Staff]、[Avg.Annual Hrs Worked] が表示されます。

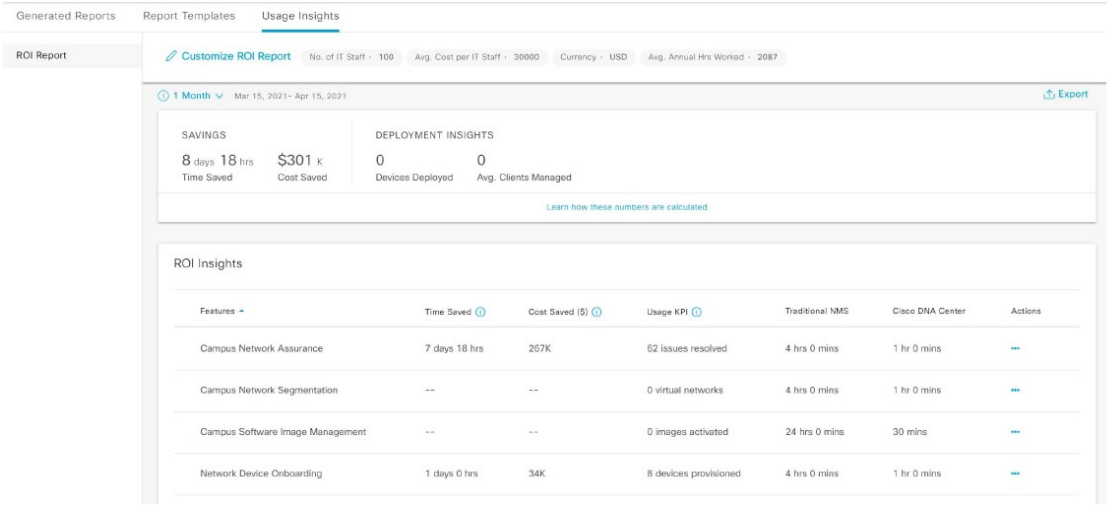
ステップ 4 機能について時間の節約を編集するには、[Actions] 列の下にある対応する [Edit] リンクをクリックし、後続のポップアップウィンドウで時間を更新します。

ステップ 5 ROI レポートを表示する時間範囲を選択するには、[**Customize ROI Insights**] ペインの下にある時間範囲のドロップダウンリストをクリックし、時間範囲のオプションボタンをクリックします。

a) 利用可能な時間範囲オプション：[**1 Month**]、[**3 Months**]、[**6 Months**]、[**1 Year**] から選択します。

b) ROI レポートの時間範囲をカスタマイズするには、時間範囲のドロップダウンリストをクリックし、[Custom] をクリックして、[Start Date] と [End Date] を定義します。

図 *27 : Usage Insights* レポートダッシュボード



ステップ 6 計算の詳細を表示するには、中央のペインの [ROI Insights] テーブルの上にある [Learn how these numbers are calculated] をクリックします。

[Calculation Details] ウィンドウには、[Time Saved] と [Cost Saved] の計算方法が表示されます。

ステップ 7 ROI レポートをエクスポートするには、[Export] をクリックします。

レポートでサポートされているファイルタイプは、PDF と CSV です。

セキュリティ アドバイザリ レポートの実行

ネットワークについての**セキュリティ アドバイザリ** レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

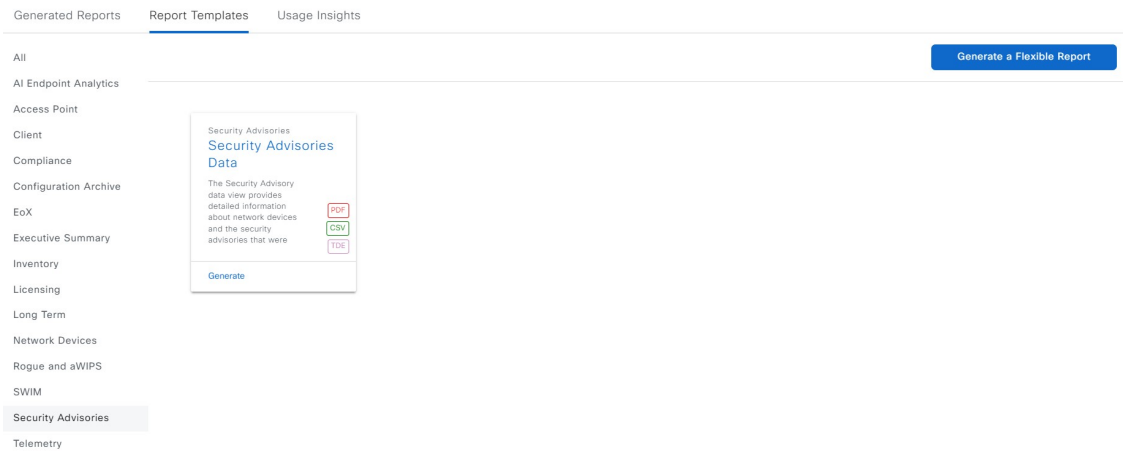
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *28* : セキュリティ アドバイザリ レポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプがタイル内にアイコンで示されます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。
- データメトリックとサマリー。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 8 [**Setup Report Scope**] ウィンドウで、レポートの名前を指定して範囲と時間範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。

[Next] をクリックします。

ステップ 9 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [**CSV**]、[**JSON**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

[Next] をクリックします。

ステップ 10 [Schedule Report] ウィンドウで、レポートのスケジュールを選択します。

[Next] をクリックします。

ステップ 11 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  （注）
  電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  - [Attachment]：レポートが電子メール通知に添付されます。

    （注）
    PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

  Catalyst Center は、レポートに関する次の電子メール通知を送信します。

  - レポートは、実行待ちのキュー内にあります。
  - インポートプロセスは進行中です。
  - レポートのコンパイルが正常に完了しました。

  通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

  （注）
  まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUI で表示することもできます。

[Next] をクリックします。

ステップ 12 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Generate Report] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 13 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

SWIM レポートの実行

ネットワークについての **[SWIM]** レポートを設定するには、次の手順を実行します。

始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]**> **[Inventory]** の順に選択して結果を表示します。

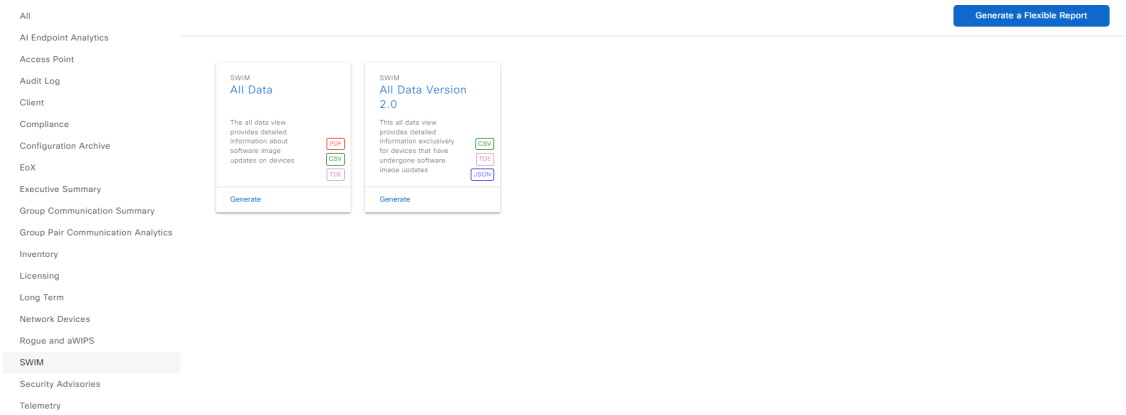
手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

[Report Templates] ウィンドウに、サポートされているレポートカテゴリが表示されます。リンクは各カテゴリを表します。リンクをクリックすると、そのカテゴリでサポートされているレポートのみが表示されます。

ステップ 2 リンクをクリックした後、選択したカテゴリの [Report Templates] ウィンドウを確認します。

図 *29 : SWIM* レポート



各テンプレートはタイル表示され、レポートに関する情報とレポートを生成するためのリンクが含まれています。表示されたテンプレートからレポートの生成に使用するテンプレートを選びます。サポートされるレポートのファイルタイプがタイル内にアイコンで示されます。

ステップ 3 サンプルレポートを表示するには、タイルでヘッダーをクリックします。

サンプルレポートのウィンドウが表示されます。ウィンドウのサイドバーを使用して下にスクロールし、サンプルレポート全体を確認します。次のデータが表示されます。

- 適用されたフィルタ（レポートを構築するために使用されたデータフィルタ）。
- データメトリックとサマリー。
- データの分析を支援するテーブル。

（注）
サンプルレポートを使用して、レポートの表示方法を計画できます。

ステップ 4 [X] をクリックして、プレビューを閉じます。

ステップ 5 レポートを作成するためのパラメータを設定するには、タイルで [Generate] リンクをクリックします。

[**Generate**] ウィンドウでは、レポートのフォーマットタイプを選択し、レポートにデータフィルタを適用し、実際のレポート生成スケジュールを設定することができます。

ステップ 6 [Generate a New Report] ウィンドウで、[Let's Do It] をクリックして生成を開始します。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 7 [Select Report Template] ウィンドウで、レポートのテンプレートを選択します。

ドロップダウンリストから [**Template**] を選択します。

（注）
[Template] には、リリースに対応するカテゴリの個々のレポートタイプが表示されます。

同じウィンドウで自動生成されたサンプルを確認できます。

[Next] をクリックします。

ステップ 8 [**Setup Report Scope**] ウィンドウで、レポートの名前を指定して範囲と時間範囲を選択します。

[Report Name] フィールドにレポート名を入力し、[Scope] フィールドをクリックして使用可能なフィルタを表示します。レポートに使用するフィルタオプションをクリックし、[Time Range] を選択します。

（注）
[Setup Report Scope] オプションは、選択した [Template] に応じて異なります。

[Next] をクリックします。

ステップ 9 [Select File Type] ウィンドウで、レポートのファイルタイプを選択します。

作成しているレポートに応じて、次の [**File Type**] オプションを使用できます。

- **PDF**
- **CSV**
- **Tableau Data Extract**
- **JSON**

ファイルタイプが [**CSV**]、[**JSON**]、[**Tableau Data Extract**] の場合、[**Fields**] オプションで、CSV、JSON、Tableau Data Extract から作成するレポートの属性（追加フィールド）を選択できます。

[Next] をクリックします。

ステップ 10 [Schedule Report] ウィンドウで、レポートの時間範囲とスケジュールを選択します。

[Next] をクリックします。

ステップ 11 [Delivery and Notification] ウィンドウで、レポートの配信方法を選択します。

- [None]：電子メールまたはウェブフックの通知を送信しません。
- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

（注）
電子メールの SMTP サーバーをまだ設定していない場合は、設定するように求められます。GUI の [Email] タブのプロンプトに従って SMTP サーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

  - [Link]：レポートが正常にコンパイルされたことを伝える電子メール通知には、元の通知に戻るリンクと、[Reports] の [Generated Reports] ウィンドウへのリンクがあります。ここからリンクを使用して、レポートを表示およびダウンロードできます。

    （注）
    レポートへのリンクが埋め込まれた電子メール通知は、最大 20 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

- [Attachment]：レポートが電子メール通知に添付されます。

  （注）
  PDF レポートは、最大 20 MB の電子メール通知添付ファイルと最大 10 の電子メールアドレスをサポートします。複数の電子メールアドレスを追加するには、各電子メールアドレスを個別に追加し、追加するたびに（キーボードの）Enter を押す必要があります。Catalyst Center プラットフォームは電子メールアドレスを検証し、シンタックスが正しくない場合は通知します。

Catalyst Center は、レポートに関する次の電子メール通知を送信します。

- レポートは、実行待ちのキュー内にあります。
- インポートプロセスは進行中です。
- レポートのコンパイルが正常に完了しました。

通知の数を減らすには、必要に応じて上記のチェックボックスをオフにします。

- [Webhook Notification]：設定されたウェブフック URL アドレス（コールバック URL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile] フィールド）からウェブフックを選択します。

  （注）
  まだウェブフックを作成していない場合は作成するように求められます。GUI の [Webhook] タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

  レポートのステータスウェブフック通知を受信します。たとえば、「キュー内（In Queue）」、「進行中（In Progress）」、「成功（Success）」のウェブフック通知が届きます。これらの通知は、GUI で表示することもできます。

[Next] をクリックします。

ステップ 12 [Summary] ウィンドウで、構成を確認し、必要に応じてファイルを編集します。

[Next] をクリックします。

レポートが生成されると、成功したことを示すウィンドウが表示されます。

ステップ 13 [View the Generated Reports] リンクをクリックします。

[Generated Reports] ウィンドウに、スケジュールされたレポートのインスタンスの詳細が表示されます。

[Generated Reports] ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

フレキシブルレポートの生成

Catalyst Center では、有線およびワイヤレスネットワーク用にカスタマイズされたレポートを柔軟に生成できます。この手順では、選択したエンティティ、属性、集約、およびフィルタに基づく**柔軟な**レポートを設定する方法について説明します。

Catalyst Center GUI の [Reports] ウィンドウを使用して、柔軟なレポートを設定できます。

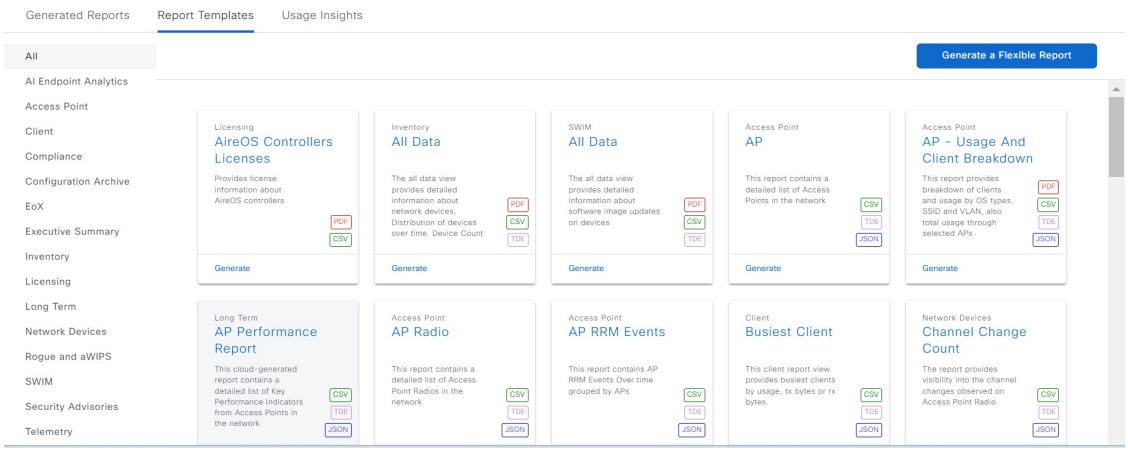
始める前に

正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択して結果を表示します。

手順

ステップ 1 メインメニューから次を選択します。**[Reports]** > **[Report Templates]** の順に選択します。

図 *30 :* フレキシブルレポートの生成



ステップ 2 [Generate a Flexible Report] をクリックします。

（注）
または、メニューアイコンをクリックして次を選択します。 **[Workflows]** > **[Flexible Report]** の順に選択します。

ステップ 3 [Flexible Report] ウィンドウで、[Let's Do it] をクリックして生成を開始します。

[Name Your Report and Select a Time Range for this Report] ウィンドウが表示されます。

（注）
今後 [Flexible Report] ダイアログボックスをスキップするには、[Don't show this to me again] チェックボックスをオンにします。

ステップ 4 [Report Name] フィールドに、レポートの名前を入力します。[**Time Range**] を選択します。

（注）
- **クライアント**レポートでサポートされる時間範囲は 90 日です。
- **ネットワークデバイス**、**PoE**、および **AP** レポートの場合、サポートされる時間範囲は 30 日です。

ステップ 5 [Next] をクリックします。

ステップ 6 [**Create a Subreport**] ウィンドウで [**Subreport Name**] を入力し、エンティティ、レポートタイプ、フィルタ条件、およびそれぞれの属性を選択します。

このリリースでは、[**Select an entity**] ドロップダウンリストで次のオプションを使用できます。

- **ネットワーク デバイス（Network Device）**
- **PoE**
- **AP**
- **[SWIM]**
- **クライアント**

次の [**Report Type**] オプションを使用できます。

- **Trend**
- **Summary**
- **Top N**
- **Distribution**

選択したレポートタイプのフィルタ条件を選択します。

たとえば、[**Trend**] レポートタイプの場合は、ドロップダウンリストから [**Trending Interval**] を選択します。

[**Attributes available for this report type**] エリアから属性を選択します。

各属性で使用可能なグループ別、ソート基準、および集約オプションに基づいてグループを設定できます。

（注）
[Trend] および [Distribution] レポートタイプでは、グループ別および集約オプションをサポートする属性の選択が必須です。[Top N] レポートタイプでは、ソート基準オプションをサポートする属性の選択が必須です。

ステップ 7 **[Next]** をクリックします。

ステップ 8 [**Configure Group By, Aggregates and Sorting Options as Applicable**] ウィンドウで、次の手順を実行します。

- [**Configure Group By**] を選択します。

（注）

[Configure Group By] は、選択したレポートタイプによって必須または任意です。

- サポートされている各属性の [**Aggregate Options**] を、ドロップダウンリストから選択します。
- [**Configure Sorting Option**] では、各サブレポートの [**Target Attributes**] または [**Sort Type**] を選択し、ドロップダウンリストからそれぞれのオプションを選択できます。

ステップ 9 **[Next]** をクリックします。

[Filters for the Current Subreport] ウィンドウが開きます。

- ドロップダウンリストからフィルタオプションを選択し、対応するフィルタの値を設定します。

  必要に応じて、[Apply this filter for the entire report] チェックボックスをオンにします。

- レポートで使用可能なフィールドのフィルタを設定します。

  ドロップダウンリストからフィルタを選択します。選択を基に [**Operator**] オプションと [**Value**] オプションを設定するか、範囲を選択してから、対応する [**Unit**] を選択します。

  （注）
  このリリースでは、演算子ベースのフィルタオプションをクライアント、AP、およびネットワークデバイスの各エンティティで使用できます。

ステップ 10 **[Next]** をクリックします。

[Would you like to add another Subreport] ウィンドウが開きます。

ステップ 11 別のサブレポートを追加するには、[**Yes**] を選択します。

[Subreports Created] エリアで、必要に応じて任意のサブレポートのパラメータを編集できます。

[Next] をクリックします。

ステップ 12 [**Schedule the Report, Select Output Format and Choose the Delivery Method**] ウィンドウで、次の手順を実行します。

- レポートのスケジュールを選択します。
- ファイルの出力形式を選択します。

  （注）
  このリリースでは、サポートされているレポートファイル形式は **CSV**です。フレキシブルレポートを使用すると、サブレポートごとに個別の**CSV** ファイルを生成または表示したり、関連するサブレポートを **ZIP** ファイルとしてまとめてダウンロードまたは表示できます。

- レポートの配信方法を選択します。

  （注）
  配信オプションを有効にするために利用可能なリンクを用いて、統合の設定を構成できます。

  レポートの配信オプションは次のとおりです。

  - [**None**]：レポートのみを表示することもできます。

- [Email Report]：電子メールレポートがリンクまたは添付ファイルとして送信されます。

  （注）
  電子メールのSMTPサーバーをまだ設定していない場合は、設定するように求められます。GUIの[Email]タブのプロンプトに従ってSMTPサーバーを設定します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。

- [Webhook Notification]：設定されたウェブフックURLアドレス（コールバックURL）へのウェブフックとして通知が送信されます。ドロップダウンリスト（[Subscription Profile]フィールド）からウェブフックを選択します。

  （注）
  まだウェブフックを作成していない場合は作成するように求められます。GUIの[Webhook]タブのプロンプトに従ってウェブフックを設定します。一般に、ウェブフックを設定するには、**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。

  Catalyst Centerは、レポートについて、次のステータスのウェブフック通知を送信します。

  - In Queue
  - In Progress
  - Success

これらの通知は、GUIで表示することもできます。

ステップ13 **[Next]** をクリックします。

[Summary]ウィンドウでサブレポートを確認し、必要に応じてパラメータを編集できます。

ステップ14 [Generate Report]をクリックします。

レポートを生成すると、次のオプションを含む成功ウィンドウが表示されます。

- **別のフレキシブルレポートの作成**
- **生成されたレポートの表示**

ステップ15 [View the Generated Reports]をクリックします。

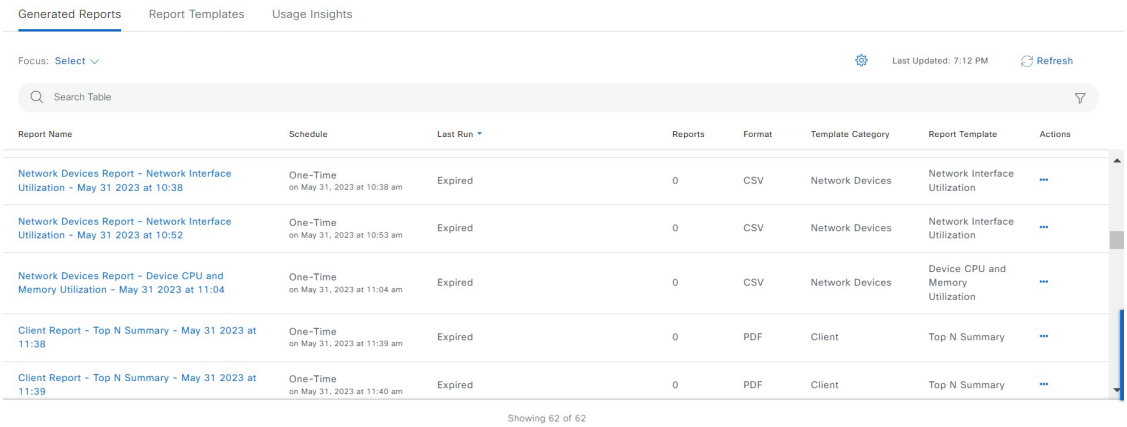
[Generated Reports]ウィンドウに、フレキシブルレポートの詳細が新たに表示されます。

[Generated Reports]ウィンドウで、レポートをダウンロード、確認、編集、複製、または削除できます。詳細については、生成されたレポートの表示 （204 ページ）を参照してください。

生成されたレポートの表示

以前生成したレポートをダウンロード、確認、編集、複製、または削除するには、この手順を実行します。

図 *31* : 生成されたレポート



始める前に

- 正常な**ディスカバリ**ジョブを Catalyst Center で実行します。[Device Inventory] で**ディスカバリ**ジョブが成功しているかどうか確認できます。メインメニューから次を選択します。**[Provision]** > **[Inventory]** の順に選択して結果を表示します。
- [Catalog] の [Schedule] 機能を使って、レポートを作成します。

手順

ステップ 1 メインメニューから次を選択します。[Reports]。

ステップ 2 [Generated Reports] をクリックします。

次の情報が表示されます。

- [Report Name]：レポートの名前。

  レポートに名前を指定しなかった場合は、レポートの日付と時刻とともにレポートタイプを含むデフォルト名がレポートに指定されます。

  （注）
  レポート名はリンクになっており、クリックすると [Generated Reports] ウィンドウ内でそのレポートが表示されます。[Download] リンクを使用すると、レポートのコピーをダウンロードできます。

- [Schedule]：生成された 1 回限りのレポートまたは繰り返しのレポート。レポートの生成スケジュールについての簡単な説明も表示されます。
- [Last Run]：レポートの実行ステータスと詳細が表示されます。次のレポート実行ステータスタイプが表示される可能性があります。
  - [Not Initiated]：スケジュールされたが、まだ開始されていないレポート。
  - [In Queue]：スケジュールされ、実行する処理キュー内にあるレポート。

- [In Progress]：現在実行中のレポート。
- [Completed]：実行が完了したレポート。完了時の日付と時刻が表示されます。

  アイコン（下矢印）をクリックすると、最後に生成されたレポートがダウンロードされます。
- [Expired]：期限切れになり、Catalyst Center で使用できなくなっているレポート。
- [Error]：レポートの実行に失敗しました。

- [Reports]：合計で最大 7 個のレポート数。

  表示されたレポート数にマウスのカーソルを合わせると、[View Report List] が表示されます。レポートダイアログボックスを表示するには、[View Report List] をクリックします。レポートダイアログボックスには、すべてのレポート実行とそのステータス（[Not Initiated]、[In Queue]、[In Progress]、[Completed]、[Expired]、[Error]）、およびコピーをダウンロードするための [Download] ボタンが表示されます。[Error] をクリックすると、レポートの実行に関するエラーと警告が表示されます。

  重要
  Catalyst Center は合計 7 個のレポートを保持します。具体的には、Catalyst Center は、実行された最後の 7 個のレポートと、過去 7 日間（週）に実行された最後の 7 個のレポートを保持します。たとえば、1 日に 8 個のレポートを実行した場合、Catalyst Center は最後の 7 個のレポートのみを保持します。毎日 1 個のレポートをスケジュールすると、Catalyst Center は過去 7 日間（週）にわたる最新の 7 個のレポートのみを保持します。Catalyst Center からさまざまな形式でレポートをエクスポートし、それらを安全な場所にアーカイブすることができます。

- [Format]：PDF や CSV などのファイル形式タイプ。
- [Template Category]：カタログオプション（クライアント、エグゼクティブサマリー、SWIM、インベントリ）に基づくレポートのタイプ。
- [Report Template]：レポートの生成に使用されたテンプレート。
- [Actions]：レポートで実行できるタスクのリスト。

[Filter] アイコンをクリックしてフィルタを使用するか、[Find] フィールドにキーワードを入力することで、GUI に表示されるダウンロードを調整することができます。

ステップ 3 次の 1 つ以上のタスクを実行するには、[Actions] をクリックします。

- [Edit]：レポートに設定されたパラメータ（スケジュールを含む）が表示されるウィンドウを開きます。このウィンドウでは、設定されているレポートパラメータを確認できます。ただし、この読み取り専用ウィンドウでは、レポート設定を変更できません。構成を編集する必要がある場合は、[Edit] をクリックします。[Edit] をクリックすると、レポート設定を表示および編集できます。
- [Edit]：レポートに設定されたパラメータ（スケジュールを含む）が表示されるウィンドウを開きます。このウィンドウでは、パラメータの確認および編集もできます。レポートを編集した後、[Save] をクリックします。

  重要
  レポート構成を編集して更新すると、以降のレポート実行にはこの新しい構成が反映されます。このことは、繰り返しのスケジュールでレポートが生成されている場合に重要です。また、レポート構成

を編集して更新すると、Catalyst Center の以前のレポートはすべて削除されます。[Save] をクリックすると、削除に関する警告が GUI に表示されます。[Save] をクリックして以前のすべてのレポートを削除するために設定で編集を行う必要はありません。

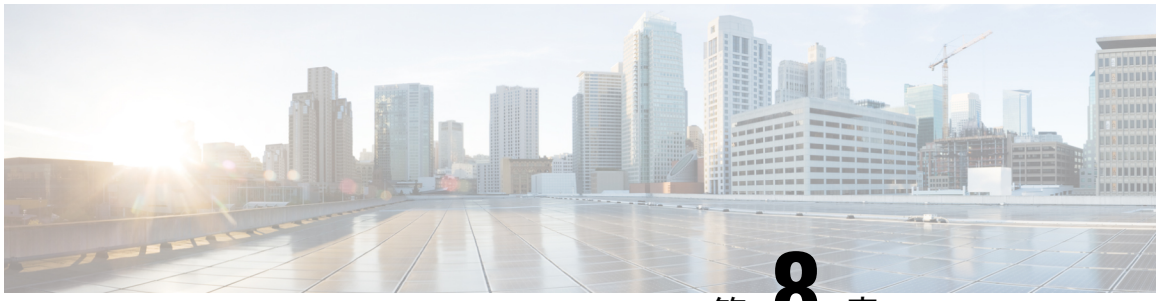
- [Duplicate]：レポートのパラメータを表示または設定できる [Duplicate] ウィンドウが開きます。[Generate Report] をクリックして、レポートを再度生成します。

  （注）
  既存のレポートとその構成に基づいて新しいレポートを作成する場合は、[Duplicate] オプションを使用し、構成を変更します。これにより、既存のレポートとその構成を保持したまま、既存のレポートと同様の新しいレポートを作成できます。既存のレポートを廃棄して新しいレポートに完全に置き換える場合は、前述のように [View Config] オプションと [Edit] オプションを使用します。

- [Run Now]：レポートを実行するプロセスを開始します。レポートの実行が成功すると、成功メッセージが表示されます。

  （注）
  レポートを実行しようとしたときに以前のレポートが 7 個ある場合、最後の 7 個のレポートのみが保存されることを示す警告が GUI に表示されます。レポートの既存のスケジュール以外でレポートを生成する必要がある場合は、[Run Now] オプションを使用します。

- [Delete]：レポートを削除します。レポートを削除する前に、このアクションを確認するよう求められます。



第 8 章

開発者用ツールキット GUI

開発者用ツールキットについて

Catalyst Center プラットフォームは、次のソフトウェア開発者ツールを提供します。これらにより、Catalyst Center でアクセスしてプログラムするとともに、Catalyst Center と他のアプリケーションを統合することができます。

- [APIs]：機能ごとにカテゴリ内で整理された API（[Operational Tasks] API や [Site Management] API など）を利用できます。
- [Integration Flows]：カテゴリ タイプごとに整理された統合フローを利用できます。
- **イベント通知**：ネットワークで発生する可能性のある特定のイベントを表示、登録できます。

API での作業

このプロシージャを実行して、使用可能な API の確認、API を使用するためのコード例の生成、Catalyst Center プラットフォーム上でのインタラクティブな API の試用を行います。

Catalyst Center GUI には、要求方式と URL、クエリパラメータ、リクエスト ヘッダーのパラメータ、応答、およびスキーマ、要求をプレビューまたはテストする方法を含め、各 API コールに関するドキュメントが表示されます。

API の詳細については、Cisco DevNet の 『Cisco Catalyst Center APIs』 を参照してください。

始める前に

- 前のセクションで説明されているとおり、サポートされているプログラミング言語と認証条件を満たしていることを確認してください。詳細については、API の前提条件（111 ページ）を参照してください。
- これらの特定の API を表示するには、まず [Rogue and aWIPS] バンドルを有効にする必要があります。メインメニューから次を選択します。**[Platform]** > **[Manage]** > **[Bundles]** > **[Rogue and aWIPS]** > **[Enable]** の順に選択します。このバンドルを有効にすると、[Contents] タブでバンドル内の API を確認したり、**[Platform]** > **[Developer Toolkit]** > **[APIs]** > **[Know Your Network]** > **[Devices]** の順に選択したりできます。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Developer Toolkit]** > **[APIs]**の順に選択します。

ステップ 2 サポートされている API の一覧を確認します。

必要に応じて、[>] アイコンをクリックして、API サブドメインを表示します。

ステップ 3 API を表示するドメインまたはサブドメインを選択します。

列に表示される各 API に関する情報は、次のとおりです。

- [Method]：サポートされるメソッドには、GET、POST、PUT、および DELETE が含まれます。
- [Name]：スライドインペインおよび説明、機能、タグ、パラメータ、応答、モデルスキーマなどの追加情報にアクセスするためのリンク。[Sunset]、[Deprecated]、または [Intent] バナーは、API のステータスを示します。API の詳細については、Cisco DevNet の『Cisco Catalyst Center APIs』を参照してください。
- [**DESCRIPTION**]：API の簡単な説明。
- [**URL**]：API の URL 値。
- [Actions]：[Try] オプションを使用してコードプレビュースニペットを作成します。

（注）
特定の API 構成が進行中で、後から再度確認することを示す青色のメッセージが表示されることがあります。API が登録されている場合は画面が自動更新されます。その後、API アクティビティを続行できます。きわめて可能性は低いですが、API を設定できないことを示す赤で色分けされたメッセージが表示された場合は、Catalyst Center 管理者に連絡して、問題を解決するための支援をシスコに依頼してください。

ステップ 4 API メソッドの名前（リンク）をクリックします。

API メソッドに関する次の情報が表示されます。

- [**DESCRIPTION**]：API の簡単な説明。
- [TAGS]：API を使用する状況を含む API 識別子。タグがない API もあることに注意してください。

- [PARAMETERS]：説明、データタイプ（ブール値または文字列）、デフォルト値、必要な値を含む API のパラメータ。
- [**FEATURES**]：API 操作の目的、API 操作の廃止またはベータステータスに関連する情報、および代替 API 操作の詳細。
- [RESPONSES]：考えられる HTTP 応答。[**Schema**] はデータモデル（[**Model**] タブ）または実際の応答の JSON 形式（[**Model Schema**] タブ）として応答を提供します。[**Sample**] をクリックすると、サンプルコードが表示されます。
- [POLICIES]：API レート制限機能。ポリシーは特定の API に適用されます。これらのポリシーは、クライアント IP アドレスごとの時間間隔あたりの API コール数を設定します。

ステップ 5 （オプション）[Code Preview] をクリックして、コードプレビューを生成します。

（注）
独自のプログラムを作成している場合は、コードプレビューのサンプルを切り取って、独自のプログラムに貼り付けることができます。

ステップ 6 （オプション）[**Code Preview**] ウィンドウで、ドロップダウンからコードを生成するための言語を選択します。

サポート対象の言語は次のとおりです。

- **シェル**
- **ノード**：**HTTP**
- **ノード**：**Unirest**
- **ノード**：**Request**
- **Python**
- **Ruby**
- **javascript**
- **JQuery**
- **PHP**
- **Go**
- **Ansible**

使用するコードプレビューサンプルを確認またはコピーした後、[Close] をクリックします。

ステップ 7 （オプション）[Try] をクリックして、メソッドを試します。

ステップ 8 （オプション）[Try] ウィンドウで、要求された値（URL アドレスや値など）を入力し、[Run] をクリックします。

応答またはエラーコードを確認した後、[Close] をクリックします。

Catalyst Center が 202（承認）HTTP ステータスコードを返した場合、結果の本文には、元のリクエストが生成した非同期タスクに関する詳細情報のクエリに使用できるタスク ID と URL が含まれます。たとえば、非常に長いタスクが完了したかどうかを判断するためにこの情報を使用できます。

（注）
応答は Catalyst Center 自体からのライブ応答で、結果はネットワークの実際の状態を反映しています。対照的に、コードプレビューは静的で、入力する必要がある値のプレースホルダが含まれています。

統合フローの使用

統合フローは、Catalyst Centerプラットフォームと、ネットワーク問題を追跡、トラブルシューティング、および解決するために使用される ITSM システムなどのサードパーティ製システムとの相互作用を定義します。

Catalyst Center プラットフォーム は、スケジュールベースの統合フローをサポートします。このタイプの統合フローはスケジュールに従って実行され、タスクを実行し、REST エンドポイントまたはその他のベンダーの特定の宛先への情報をプッシュします。スケジュールベースの統合フローは、これらを実行するスケジュールを指定する GUI で [Integration Flows] ウィンドウを使用して編集できます。

（注） [Developer Toolkit] で使用可能な統合フローは、**[Manage]** > **[Bundles]** 内のさまざまなバンドルによって使用されます。バンドルは、ユーザー独自のアプリケーションを Catalyst Center と統合したり、Catalyst Center 自体のパフォーマンスを向上させたりするために使用されます。バンドル内で使用されている統合フローを表示するには、[Manage] 内でバンドルをクリックし、[Contents] タブをクリックします。バンドルの統合フローが、[Contents] タブの下にリストされます。

始める前に

[Integration Flows] ウィンドウで統合フローを表示および管理できるようにするには、それらを有効にする必要があります。Catalyst Centerプラットフォーム で個々のバンドルから統合フローを有効にする必要があります。たとえば、メニューアイコンをクリックして次を選択します。**[Platform]** > **[Manage]** > **[Bundles]** > **[Basic ITSM (ServiceNow) CMDB synchronization]** の順にクリックします。[Contents] タブをクリックし、[Enable] をクリックします。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Developer Toolkit]** > **[Integration Flows]** の順にクリックします。

ステップ 2 GUI によって表示される統合フローを確認します。

ステップ 3 ITSM 統合グループから統合フローを選択します。

次の情報が表示されます。

- [Name]：統合フローと追加情報が入手可能な スライドインペイン にアクセスするリンクの名前。

  統合フローがRESTベースのトリガータイプの場合、統合フロー名をクリックすると、説明、タグ、パラメータ、応答、モデルスキーマ、ポリシーなどの追加データが表示されます。

  統合フローがスケジュールベースのトリガータイプの場合、統合フロー名をクリックすると、スケジュールを設定するための スライドインペイン が表示されます。この スライドインペイン には、[DESCRIPTION]、[TAGS]、および [HOW TO USE THIS FLOW] の内容が表示されます。

- [Description]：統合フローの簡単な説明。
- [Trigger]：RESTベースまたはスケジュールベース。
- アイコン（[...]）：コードプレビューまたは [Try] オプションを作成するためのリンク。統合フローがスケジュールベースの場合、このアイコンは [Schedule Flow] オプションにアクセスします。

ステップ 4 REST ベースの統合フローの場合は、統合フローの名前（リンク）をクリックします。

スライドインペイン が開き、REST ベースの統合フローに関する詳細が表示されます。詳細を確認し、スライドインペイン を閉じます。

ステップ 5 REST ベースの統合フローの場合は、アイコン（[...]）にマウス オーバーして [Generate Code Preview] をクリックし、コードプレビュースニペットを生成します。

これらの選択肢は、RESTベースでトリガーされた統合フローの場合にのみ表示されます。スケジュールベースの統合フローでは、マウスを合わせたときに、[Schedule Flow] メニュー項目が提示されます。

ステップ 6 [**Code Preview**] ウィンドウで、ドロップダウンからコードを生成するためのプログラミング言語を選択します。

使用するコードを確認またはコピーした後、[Close] をクリックします。

ステップ 7 REST リクエストのパスをインタラクティブに試すには、アイコン（[…]）にマウスオーバーして、[Try] をクリックします。

ステップ 8 [Try] ウィンドウで、要求された値（URL アドレスや値など）を入力し、[Run] をクリックします。

メソッドを試した後、[Try] ウィンドウ内で応答/エラーコードを確認し、[Close] をクリックします。

Catalyst Center が 202（承認）HTTP ステータスコードを返した場合、結果の本文には、元のリクエストが生成した非同期タスクに関する詳細情報のクエリに使用できるタスク ID と URL が含まれます。たとえば、非常に長いタスクが完了したかどうかを判断するためにこの情報を使用できます。詳細については、「Getting Information about Asynchronous Operations」を参照してください。

（注）
応答については、Catalyst Center API はタスクベースの応答アーキテクチャを使用するため、複数のリクエストと応答が同時に送信されます。そのため、すべての PUT、POST、および DELETE リクエストでは、タスクベースの応答があります。応答に関する詳細を表示するには、タスク URL に GET リクエストを送信します（スクリプトから、または URL として）。エラーコードの場合、Catalyst Center API は標準の HTTP ステータスコードに従います。

ステップ 9 スケジュールベースの統合フローの場合は、アイコン（[…]）にマウスオーバーして [Schedule Flow] をクリックします。

ステップ 10 次のデータを確認します。

- [DESCRIPTION]：統合フローの説明と目的。
- [TAGS]：タグは、どの Catalyst Center コンポーネントが、バンドルによって使用されるか、または影響を受けるかを示します。
- [HOW TO USE THIS FLOW]：スケジュール設定オプション。

GUI を使用して、統合フローをスケジュールすることができます。

ステップ 11 次の GUI オプションを使用して、統合フローのスケジュールを設定します。

- [**Run Now**]：[**Run Now**] を選択し、[**Schedule**] をクリックして統合フローを実行します。
- [**Run Later**]：[**Run Later**] を選択し、日付、時刻、およびタイムゾーンを入力します。[**Schedule**] をクリックして、指定した日付、時刻、およびタイムゾーンで統合フローを実行します。
- [**Recurring**]：[**Recurring**] を選択し、次のオプションを設定します。
  - [**Repeats**]：統合フローを繰り返す頻度として毎日または毎週を選択します。
  - [Run at Interval]：統合フローを実行する時間間隔を設定します。
  - [Set Schedule Start]：開始日を設定します。
  - [Set Schedule End]：終了日を設定します。

設定された時間に統合を実行するには、[**Schedule**] をクリックします。

イベント通知の使用

ネットワークで発生する可能性のある特定のイベントに通知を関連付けることができます。通知がイベントに関連付けられた後で、イベントが発生した場合でも、REST API または電子メールで通知を受け取ります。Catalyst Center プラットフォーム GUI の [Event Notifications] ウィンドウを使用して、通知をイベントに関連付けます。

始める前に

- REST API 通知の場合は、Catalyst Center の [Webhook] タブでウェブフックの宛先を設定しておきます。[Webhook] タブにアクセスするには、メニューアイコンをクリックして次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。ウェブフックの宛先の設定の詳細については、ウェブフックの宛先の設定（144 ページ）を参照してください。

- イベントの電子メール通知の場合は、Catalyst Center の [Email] タブで電子メールの宛先を設定しておきます。[Email] タブにアクセスするには、メニューアイコンをクリックして次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。電子メールの宛先の設定の詳細については、電子メールの宛先の設定 （145 ページ）を参照してください。
- イベントの Syslog サーバー通知の場合は、Catalyst Center の [Syslog] タブで Syslog サーバーの宛先を設定しておきます。[Syslog] タブにアクセスするには、メニューアイコンをクリックして次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Syslog]** の順に選択します。Syslog サーバーの宛先の設定の詳細については、Syslog サーバーの接続先の設定 （147 ページ）を参照してください。
- イベントの SNMP トラップ通知の場合は、Catalyst Center の [SNMP] タブで SNMP トラップの宛先を設定しておきます。[SNMP] タブにアクセスするには、メニューアイコンをクリックして次を選択します。 **[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[SNMP]** の順に選択します。トラップの宛先の設定に関する詳細については、トラップ通知の設定 （148 ページ）を参照してください。
- [Event Settings] ウィンドウにアクセスして、ネットワークで発生する可能性がある ITSM の統合についてのイベントのリストを確認し、Catalyst Center でキャプチャできるイベントを必要に応じて編集しておきます。[Events Settings] ウィンドウにアクセスするには 、メニューアイコンをクリックして次を選択します。**[Platform]** > **[Manage]** > **[Configurations]** > **[Event Settings]** の順に選択します。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Developer Toolkit]** > **[Event Notifications]**。

[Events Notifications] ウィンドウが表示されます。

ステップ 2 [Notifications] タブをクリックして、通知タイルを表示します。

各通知はタイルで表され、通知の詳細を表示するためのリンクが含まれています。

ステップ 3 左側のペインの [CHANNELS] エリアで、それぞれの通知タイルを表示するチャネルの横にあるオプションボタンをクリックします。

サポートされているチャネルは、[REST]、[PAGERDUTY]、[SNMP]、[SYSLOG]、[WEBEX]、[EMAIL] です。Assurance イベントでは、SNMP はサポートされません。

（注）
- それぞれのチャネルでイベントの通知を作成し、通知をトリガーする必要があります。詳細については、*Cisco Catalyst Center User Guide* の「**イベント通知の作成**」を参照してください。
- 1 つのイベント通知で複数のチャネルがサポートされます。

ステップ 4 通知の詳細を表示する通知タイルリンクをクリックします。

[Notification Details] スライドインペインには、選択したチャネルに基づいて次の通知の詳細が表示されます。

- [Name]：イベントの名前。
- [Description]：イベントの説明
- [Sites]
- [Event]
- [REST]：REST 通知の詳細を表示する場合にのみ表示されます。[REST] エリアには、次の情報が表示されます。
  - [URL]：イベントが送信される REST API エンドポイントの URL アドレス。
  - [Method]：PUT メソッドまたは POST メソッド。
  - [Trust certificate]：REST API エンドポイント通知に信頼できる証明書が必要かどうか。
  - [Headers]：[Header Name] と [Header Value]。
- [PAGERDUTY]：PAGERDUTY 通知の詳細を表示する場合にのみ表示されます。[PAGERDUTY] エリアには、次の情報が表示されます。
  - [PagerDuty Events API URL]
  - [PagerDuty Integration Key]
  - [PagerDuty Events API Version]
- [SNMP]：[SNMP] 通知の詳細を表示する場合にのみ表示されます。
- [SYSLOG]：[SYSLOG] 通知の詳細を表示する場合にのみ表示されます。
- [WEBEX]：[WEBEX] 通知の詳細を表示する場合にのみ表示されます。
- [EMAIL]：[EMAIL] 通知の詳細を表示する場合にのみ表示されます。[EMAIL] エリアには、E メール受信者の [From] と [To] と E メールの [Subject] が表示されます。

ステップ 5 [Notification Details] スライドインペインで、右上隅にあるトグルボタンをクリックして、それぞれの通知を有効または無効にします。

ステップ 6 特定の通知を編集するには、[Actions] ドロップダウンリストをクリックし、[Edit] を選択します。

ステップ 7 [EDIT NOTIFICATION] ウィンドウで、選択したチャネルに基づいて以下の設定を行います。

1. [Name] フィールドに一意の名前を入力します。
2. [Description] フィールドに、それぞれのイベントの説明を入力します。
3. [Site and Events] を展開し、[Select a site] ドロップダウンリストからサイトを選択します。
4. イベントの横にあるプラスアイコンをクリックするか、[Add All] をクリックしてすべてのイベントをそれぞれの通知に追加します。

5. 通知からイベントを削除するには、削除するイベントの横にあるプラスアイコンをクリックするか、[Remove All] をクリックして、それぞれの通知からすべてのイベントを削除します。
6. [Configuration] を展開して、選択した通知チャネルの構成を編集します。

   [Configuration] エリアで詳細を指定するには、『*Cisco Catalyst Center User Guide*』の「**Create an Event Notification**」を参照してください。

   （注）
   [Configuration] エリアに表示されるフィールドは、選択した通知チャネルのタイプによって異なります。

ステップ 8 右上隅にあるトグルボタンをクリックして、タイルビューとリストビューを切り替えます。

ステップ 9 [Event Catalog] タブをクリックして、作成されたイベントのリストを表示します。

（注）
[Search] フィールドにキーワードを入力することで表示されるイベントを調整できます。

ステップ 10 テーブル内の個々のイベントのデータを確認します。

以下の [Event Details] タブのデータが表示されます。

- [Description]：イベントとそれを発生させるトリガーの簡単な説明。
- [Event ID]：イベントの識別番号。
- [Version]：イベントのバージョン番号。
- [Namespace]： イベントの名前空間。
- [Severity]：1 ー 5。

  （注）
  シビラティ（重大度） 1 は最も重要または重大な優先度であり、このタイプのイベントに割り当てる必要があります。

- [Domain]：イベントが属する REST API ドメイン。
- [Subdomain]：イベントが属する REST API ドメインの配下のサブグループ。
- [Category]：エラー、警告、情報、アラート、タスクの進捗状況、タスクの完了。
- [Note]：イベントの理解に役立つ追加情報。
- [Event Link]：REST URL を使用したイベントブロードキャスト。
- [Tags]：イベントの影響を受ける Catalyst Center のコンポーネントを示すタグ。
- [Channels]：イベント通知でサポートされているチャネル（REST API、電子メール、Webex など）。
- [Model Schema]：イベントに関するモデルスキーマが提示されます。
  - [Details]：イベントのモデルスキーマの詳細の例。

- [REST Schema]：イベントの REST スキーマのフォーマット。

ステップ 11 [Notifications] タブをクリックして、それぞれのイベントに関連付けられたアクティブな通知を表示します。

通知をイベントに関連付けると、[Event Catalog] タブに [Try-It Now] ボタンが表示されます。イベント通知シミュレーションを実行するには、[Try-It Now] をクリックします。詳細については、「イベント通知シミュレーションの使用」を参照してください。

イベント通知シミュレーションの使用

Catalyst Center プラットフォーム はイベントシミュレーションをサポートしており、イベントのサブスクリプション（電子メール、REST API、SNMP トラップ通知、syslog サーバー、または Webex）をテストできます。イベントシミュレーションの実行後、結果（成功または失敗）が GUI に表示されます。

始める前に

- イベントの Syslog サーバー通知の場合は、Catalyst Center の [Syslog] タブで Syslog サーバーの宛先を設定しておきます。[Syslog] タブにアクセスするには、メニューアイコンをクリックして次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Syslog]** の順に選択します。Syslog サーバーの宛先の設定の詳細については、Syslog サーバーの接続先の設定 （147 ページ）を参照してください。
- 電子メール通知の場合は、Catalyst Center の [Email] タブで電子メールの宛先を設定しておきます。[Email] タブにアクセスするには、メニューアイコンをクリックして次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Email]** の順に選択します。電子メールの宛先の設定の詳細については、電子メールの宛先の設定 （145 ページ）を参照してください。
- REST API 通知の場合は、Catalyst Center の [Webhook] タブでウェブフックの宛先を設定しておきます。[Webhook] タブにアクセスするには、メニューアイコンをクリックして次を選択します。**[System]** > **[Settings]** > **[External Services]** > **[Destinations]** > **[Webhook]** の順に選択します。ウェブフックの宛先の設定の詳細については、ウェブフックの宛先の設定 （144 ページ）を参照してください。
- [Event Settings] ウィンドウにアクセスして、ネットワークで発生する可能性がある ITSM の統合についてのイベントのリストを確認し、Catalyst Center でキャプチャできるイベントを必要に応じて編集しておきます。[Events Settings] ウィンドウにアクセスするには 、メニューアイコンをクリックして次を選択します。**[Platform]** > **[Manage]** > **[Configurations]** > **[Event Settings]** の順に選択します。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Developer Toolkit]** > **[Event Notifications]** > **[Event Catalog]** の順に選択します。

ステップ 2 [Event Catalog] タブで、イベントをクリックします。Catalyst Center がそのイベントに登録している場合、スライドインペイン に [Try-It Now] ボタンが表示されます。[Try-It Now] をクリックします。

このデータが表示された場合、編集できるのは [Details] フィールドのみです。

- [Event Name]：Catalyst Center におけるイベントのシステム名。
- [Event ID]：イベントの識別番号。
- [Instance ID]：イベントのインスタンスの ID 番号。
- [Name]：イベントの名前。
- [Description]：イベントとそれを発生させるトリガーの簡単な説明。
- [Namespace]： イベントの名前空間。

  このリリースでは、すべてのイベントのデフォルト値は ASSURANCE です。
- [Context]：イベントのコンテキストのフィールド

  デフォルト値は EXTERNAL です。
- [Source]：送信元フィールド。

  デフォルト値は EXTERNAL です。
- [Type]：[Network]、[App]、[System]、[Security]、または [Integrations] のイベントタイプ。
- [Category]：エラー、警告、情報、アラート、タスクの進捗状況、タスクの完了。
- [Severity]：1 ー 5。
- [Domain]：イベントが属する REST API ドメイン。
- [Sub Domain]：イベントが属する REST API ドメインの配下のサブグループ。
- [Details]：イベントに関する追加の詳細のフィールド（ユーザーが入力）。

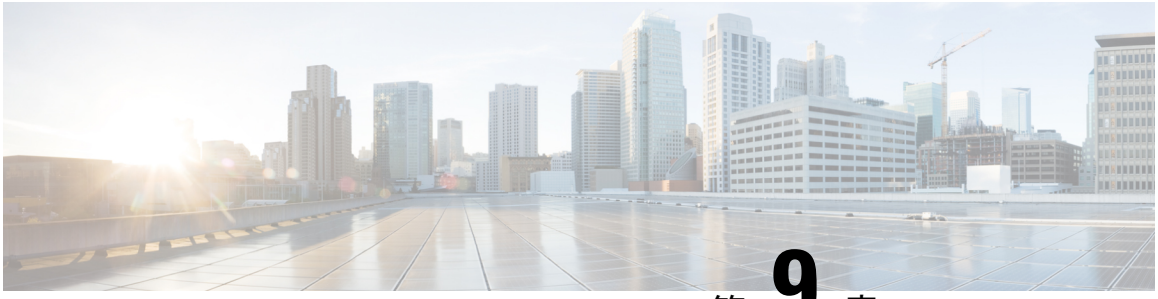
ステップ 3 [X] をクリックしてフィールドを終了します。

ステップ 4 [Publish] をクリックしてイベントシミュレーションを実行し、結果を確認します。

次の結果が表示されます。

- [Subscription Name]：ユーザーが作成したサブスクリプション名。
- [Connector Type]：電子メール、REST API、SNMP トラップ、または Syslog。
- [Status]：ロード中、成功、または失敗。

- [Message]：コネクタタイプが REST（REST API サブスクリプション）の場合、HTTPS 応答が表示されます。



第 9 章

Runtime Dashboard

[Runtime Dashboard] について

高レベルで、APIはビジネスAPI（BAPI）と登録済みAPI（RAPI）に分類されます。ランタイムダッシュボードには、RAPI ではなく BAPI の情報のみが表示されます。このページでは、次の概要について説明します。

- [API Summary]：最近の API コール、結果、およびパフォーマンスの概要。[View Details] をクリックすると、スライドインペインが開き、個別の API コール数およびコール時間に関する情報が表示されます。

  [Runtime Dashboard] には、Catalyst Center から ServiceNow API 統合へのデータのみが表示されます。

- [Event Summary]：REST エンドポイントまたは統合フローを含む Catalyst Center イベント。イベント名（リンク）をクリックすると、スライドインペインが開き、追加の詳細なイベント情報が表示されます。

- [CMDB Synchronization Summary]：**インベントリ**から選択したデバイスの構成管理データベース（CMDB）同期ステータスを表示する概要。

- [**Integration Flow Summary**]：統合フローのインスタンス、結果、およびパフォーマンスの概要。適切なタブをクリックすると、REST ベースまたはスケジュールベースの統合フローに関する追加の詳細情報が表示されます。

イベントの概要の確認

この手順に従って Catalyst Center プラットフォーム [**Event Summary**] を確認します。[Event Summary] には、イベントのタイプに基づいて外部システムに発行されたイベントの合計数が表示されます。[Events Summary] を使用し、Catalyst Center プラットフォームのモニターリングとトラブルシューティング、および他システムとの統合を支援できます。

Catalyst Center GUI の [Runtime Dashboard] ウィンドウで、[Event Summary] を確認します。

始める前に

[Event Summary] フィールドでイベントを表示するには、[Bundles] でバンドルを有効化、設定、アクティベートする必要があります。また、[Event Settings] でバンドルに関連するイベント通知を有効にする必要があります。[Bundles] の詳細については、バンドル機能 （118 ページ）を参照してください。[Event Settings] の情報については、イベント設定の構成 （138 ページ）を参照してください。

手順

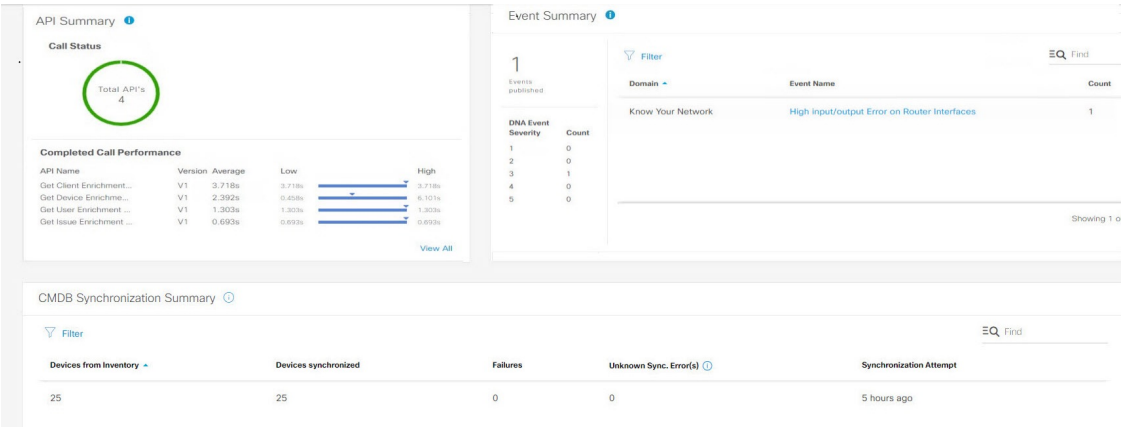
ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Runtime Dashboard]** の順に選択します。

ステップ 2 GUI メニューバーの右上にある [Last 1 Week] をクリックして、[Event Summary] の時間間隔を選択します。

直近の 6、12、24 時間、またはその週のイベントの概要を表示できます。

ステップ 3 [Runtime Dashboard] ウィンドウの [Event Summary] フィールドを確認します。

図 *32 : [Events Summary]* フィールド



次の情報が現在のイベントに表示されます。

- [Events Published]：Catalyst Center プラットフォームによってキャプチャされ発行された（GUI に表示された）イベントの合計数。
- [Event Severity]：重大度（1 ～ 5 の数値）別のイベントの合計数。

- [Count]：イベントの数。
- [Events]：ドメイン（カテゴリ）、イベント名（リンク）、およびカウント（イベント数）別のイベントのリスト。

（注）
リスト全体を表示するには、フィールドの右側にあるスクロールバーを使用して下にスクロールします。

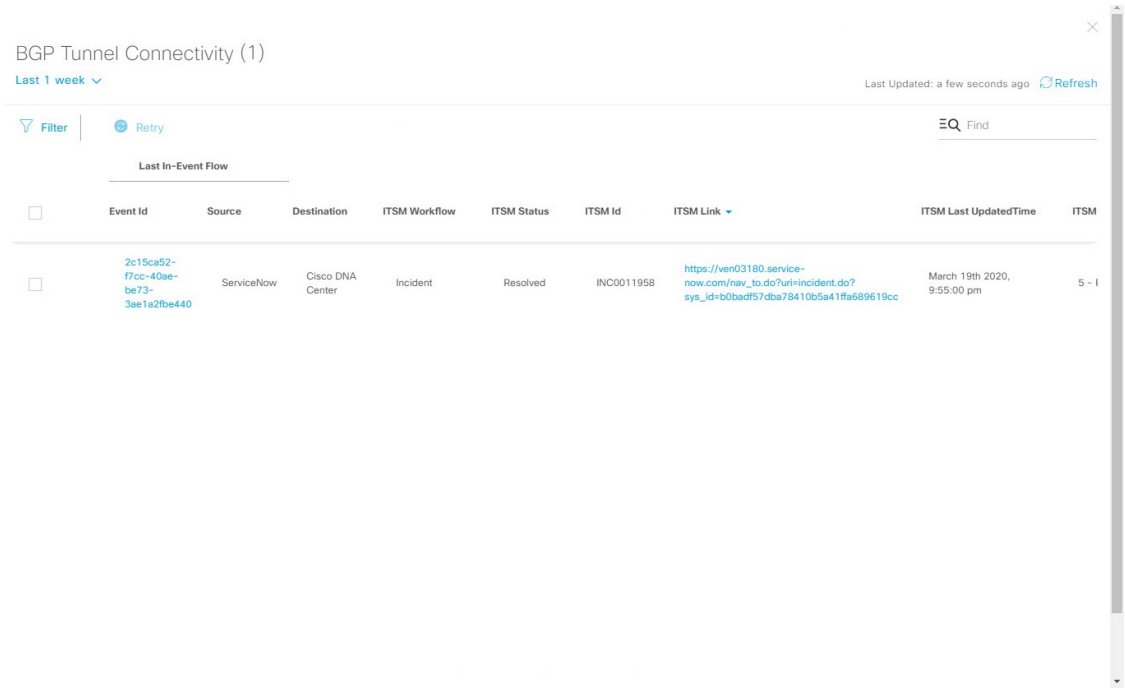
ステップ 4 イベント名（リンク）をクリックして追加の詳細データを確認します。

例として、イベント [Router Unreachable] または [BGP Tunnel Connectivity] が GUI ウィンドウに表示されている場合は、そのリンクをクリックします。

イベント名（リンク）をクリックすると、スライドインペインが開きます。

ステップ 5 このタイプのイベントのリスト（履歴）をスライドインペインで確認します。

図 *33* : イベント履歴



各イベントには次の情報がリストされます。

- [Event ID]：Catalyst Center で生成された Catalyst Center イベント ID 番号。
- [Source]：イベントの発信元の場所。たとえば、Catalyst Center プラットフォーム または ITSM システム（ServiceNow）です。
- [Destination]：イベントの送信先の場所。たとえば、Catalyst Center プラットフォーム または ITSM システム（ServiceNow）です。
- [ITSM Workflow]：ITSM ワークフローのタイプ（[Incident] や [Problem] など）。

- [ITSM Status]：イベントの現在のステータス。イベントのステータスには、[Open]、[New]、[Closed]、[N/A] などがあります。
- [ITSM ID]：ITSM（ServiceNow）で生成された ITSM イベント ID 番号。
- [ITSM Link]：ITSM イベントの ITSM サーバーへのリンク。
- [ITSM Last Updated Time]：イベント更新の最後の日付と時刻。
- [ITSM Entity Severity/Priority]：イベントに割り当てられている ITSM のシビラティ（重大度）または優先度。
- [Event Severity]：Catalyst Center によってイベントに割り当てられた重大度（1 ～ 5）。

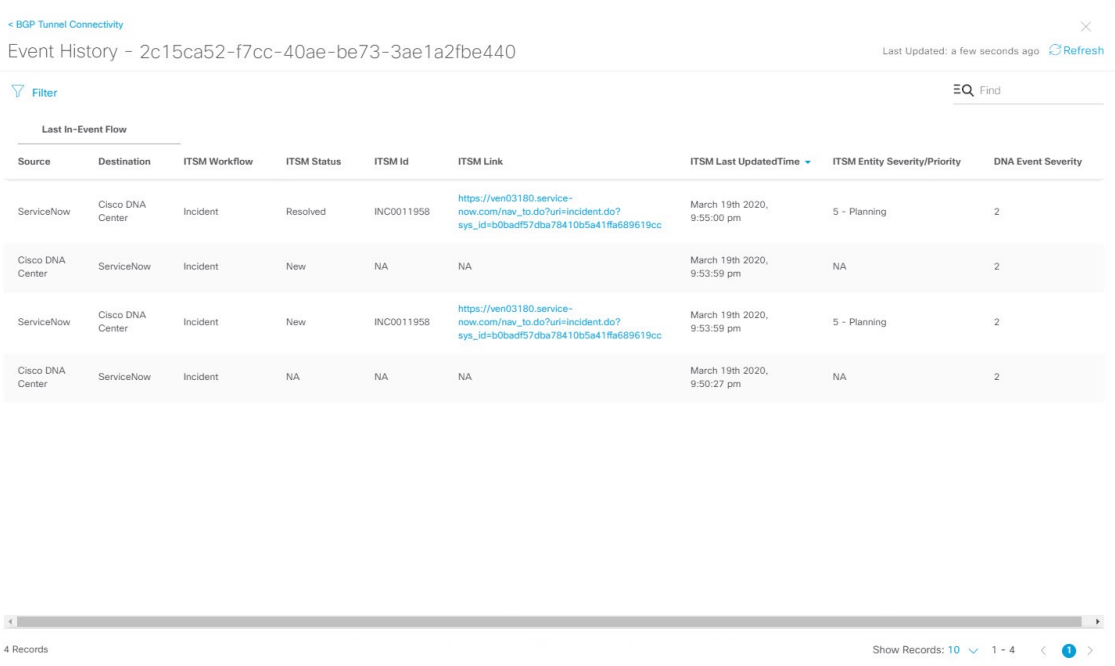
[**Filter**] アイコンをクリックしてフィルタを使用するか、[**Find**] フィールドにキーワードを入力することで、テーブルに表示されるイベントを調整することができます。

ステップ 6 イベント ID 番号（リンク）をクリックすると、その特定のイベントに関連付けられているデータのみが表示されます。

イベント ID 番号（リンク）をクリックすると、スライドインペインが開きます。

ステップ 7 スライドインペインでイベント ID データを確認します。

図 *34* : イベント *ID* データ



次の単一のイベント情報が表示されます。

- [**Source**]：イベントの発信元の場所（Catalyst Center プラットフォーム など）。
- [Destination]：イベントの送信先の場所。REST エンドポイントなどです。

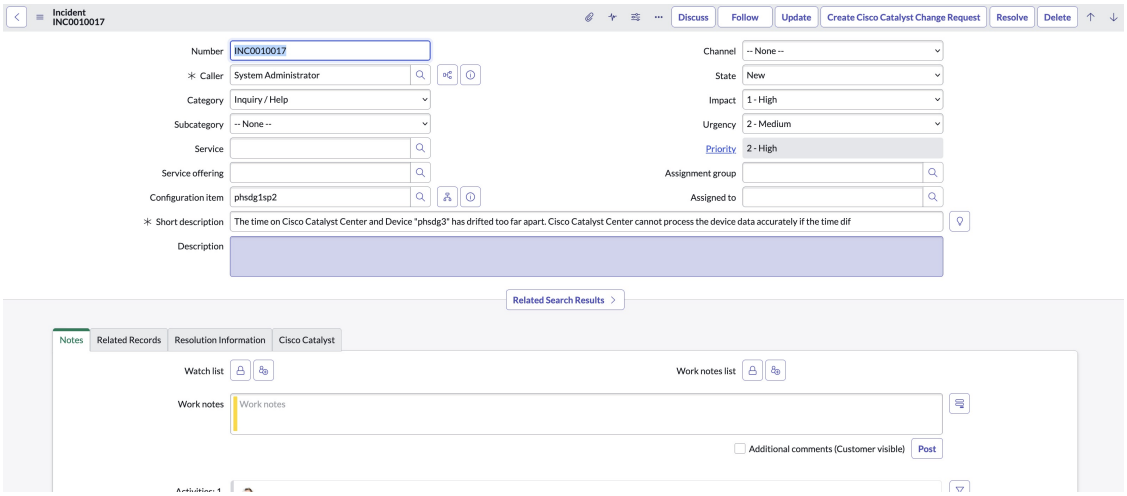
- [ITSM Workflow]：ITSM ワークフローのタイプ（[Incident] や [Problem] など）。
- [ITSM Status]：イベントの現在のステータス。イベントのステータスには、[Open]、[New]、[Resolved] などがあります。
- [ITSM ID]：ITSM イベント ID 番号。
- [ITSM Link]：ITSM（ServiceNow）へのリンク。
- [ITSM Last Updated Time]：イベント更新の最後の日付と時刻。
- [ITSM Entity Severity/Priority]：イベントに割り当てられている ITSM のシビラティ（重大度）または優先度。
- [Event Severity]：Catalyst Center によってイベントに割り当てられた重大度（1 ～ 5）。

スライドインペインを閉じて前のウィンドウに戻るには、ウィンドウの左上にあるイベントのリンクをクリックします。

新しいウィンドウでスライドインペインを閉じて [Runtime Dashboard] に戻るには、もう一度左上のリンクをクリックします。

ステップ 8 （オプション）[ITSM Link] をクリックして、ITSM プログラム（ServiceNow サービス管理 GUI）を起動し、特定のインシデントにアクセスします。

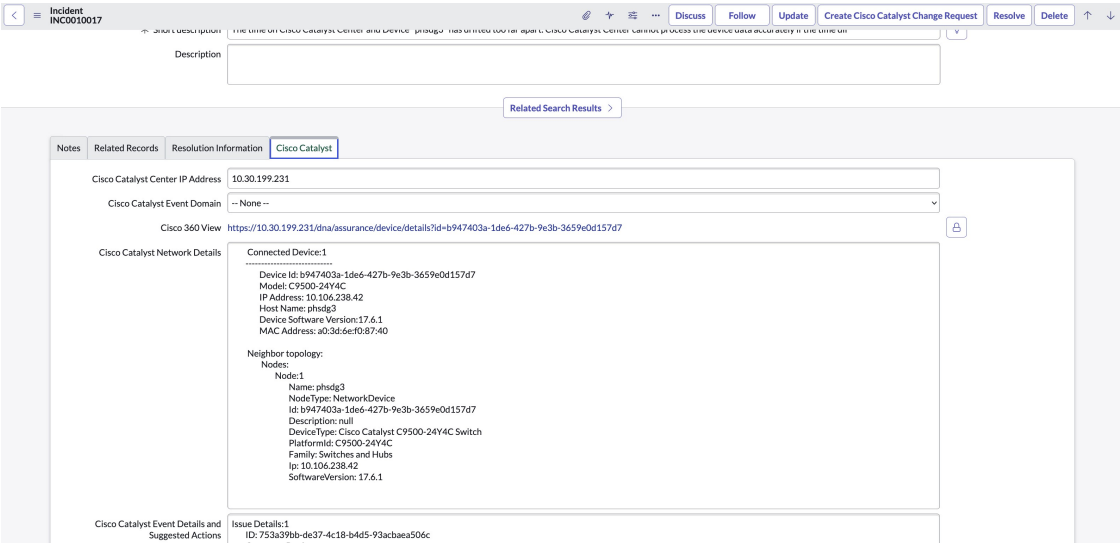
図 *35 : ServiceNow* インシデント



（注）
ITSM プログラムへの [**Runtime**] のイベントリンクを使用するには、『Cisco Catalyst Center ITSM Integration Guide』で説明されている手順に従って Catalyst Center プラットフォームと ServiceNow の統合をセットアップする必要があります。

ステップ 9 （オプション）ServiceNow サービス管理 GUI の [**Cisco Catalyst**] タブをクリックして、イベントの詳細を確認します。

図 *36 : Cisco Catalyst* タブ



この情報は、[**Cisco Catalyst**] タブから確認できます。

- [**Cisco Catalyst Center IP Address**]
- **[Cisco 360 View]**
- [**Cisco Catalyst Network Details**]
- [**Cisco Catalyst Event Domain**]
- **Cisco Catalyst Event Details and Suggested Actions**
- **Cisco Catalyst Event ID**
- **[Approval Status]**

ITSM イベントの再試行

ITSM イベントを再試行するために、Catalyst Center GUI の [**Event Summary**] ウィンドウを使用して Catalyst Center プラットフォーム から ITSM（ServiceNow）にイベントを再送信し、再処理できます。

[Runtime Dashboard] の [Event Summary] ウィンドウには、イベントのタイプに基づいて外部システムに発行されたイベントの合計数が表示されます。[**Events Summary**] を使用し、Catalyst Centerプラットフォーム のモニタリングとトラブルシューティング、および他システムとの統合を支援できます。

始める前に

[Event Summary] フィールドでイベントを表示するには、[Bundles] でバンドルを有効化、設定、アクティベートする必要があります。また、[Event Settings] でバンドルに関連するイベント通知を有効にする必要があります。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Runtime Dashboard]** の順に選択します。

ステップ 2 GUI メニューバーの右上にある [Last 1 Week] をクリックして、[Event Summary] の時間間隔を選択します。

直近の 6、12、24 時間、またはその週のイベントの概要を表示できます。

ステップ 3 [Runtime Dashboard] ウィンドウの [Event Summary] フィールドを確認します。

次の情報が現在のイベントに表示されます。

- [Events Published]：Catalyst Center プラットフォームによってキャプチャされ発行された（GUI に表示された）イベントの合計数。
- [Event Severity]：重大度（1 ～ 5）別のイベントの合計数。
- [Count]：イベントの数。
- [Events]：ドメイン（カテゴリ）、イベント名（リンク）、およびカウント（イベント数）別のイベントのリスト。

（注）
リスト全体を表示するには、フィールドの右側にあるスクロールバーを使用して下にスクロールします。

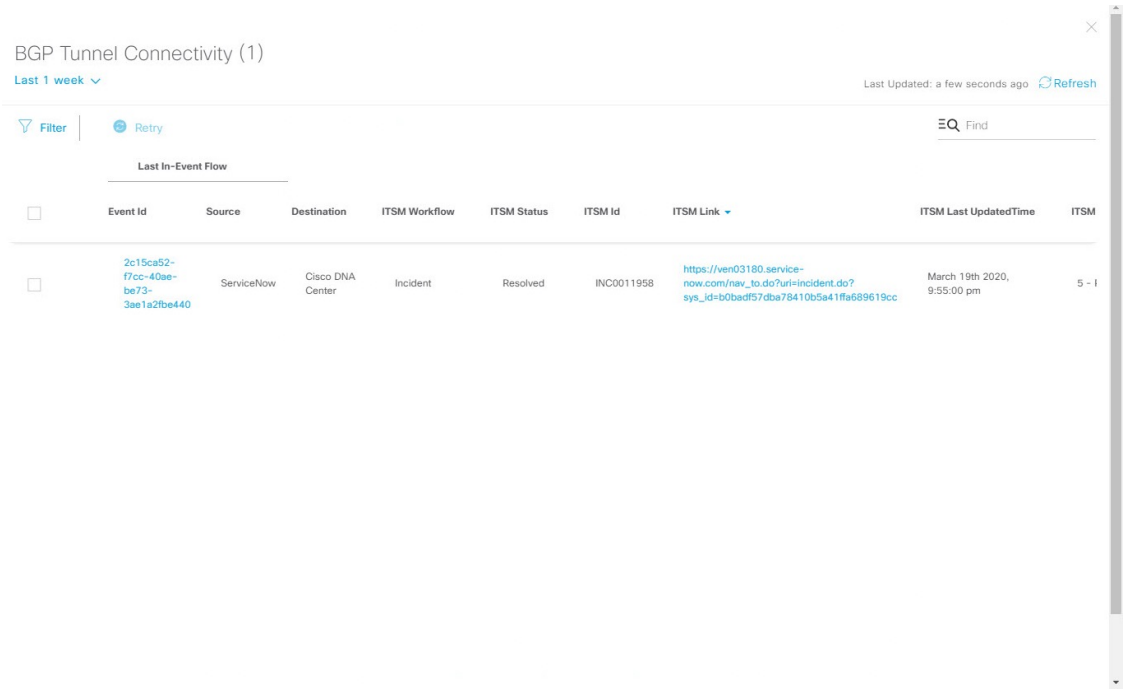
ステップ 4 ITSM イベント名（リンク）をクリックして追加の詳細データを確認します。

たとえば、「SWIMアップグレード要求作成イメージのアクティブ化（SWIM Upgrade Request Creation Image Activation）」のようなITSMイベントがGUIウィンドウに表示されていれば、そのリンクをクリックします。

イベント名（リンク）をクリックすると、スライドインペインが開きます。

ステップ 5 このタイプのイベントのリスト（履歴）をスライドインペインで確認します。

図 *37* : イベント履歴



各イベントには次の情報がリストされます。

- [Event ID]：Catalyst Center で生成された Catalyst Center イベント ID 番号。
- [Source]：イベントの発信元の場所。たとえば、Catalyst Center プラットフォーム または ITSM システム（ServiceNow）です。
- [Destination]：イベントの送信先の場所。たとえば、Catalyst Center プラットフォーム または ITSM システム（ServiceNow）です。
- [ITSM Workflow]：ITSM ワークフローのタイプ（[Incident] や [Problem] など）。
- [ITSM Status]：イベントの現在のステータス。イベントのステータスには、[Open]、[New]、[Closed]、[N/A]、[Resolved] などがあります。
- [ITSM ID]：ITSM（ServiceNow）で生成された ITSM イベント ID 番号。
- [ITSM Link]：ITSM イベントの ITSM サーバーへのリンク。
- [ITSM Last Updated Time]：イベント更新の最後の日付と時刻。
- [ITSM Entity severity/priority]：イベントに割り当てられている ITSM のシビラティ（重大度）または優先度。
- [Event Severity]：イベントに割り当てられた Catalyst Center の重大度（1 ～ 5）。

[Filter] アイコンをクリックしてフィルタを使用するか、[Find] フィールドにキーワードを入力することで、テーブルに表示されるイベントを調整することができます。

ステップ 6 再送信して再処理する必要がある ITSM イベントを特定します。

ITSM イベントの [ITSM Workflow]、[ITSM Status]、または [ITSM ID] の値が [N/A] と表示されている場合（イベントの送信元は ServiceNow でイベントの送信先は Catalyst Center）、再試行が必要な問題であることを示します。また、再試行が必要な ITSM イベントには、[Filter] 列にチェックボックスが表示されます。

ステップ 7 [Filter] 列のチェックボックスをオンにして ITSM イベントを選択すると、[Retry] ボタンが有効になります。

ステップ 8 [Retry] をクリックします。

イベントが送信先の ITSM に再送信されると、次のいずれかの状態になります。

- 再試行成功：イベントの [ITSM Workflow]、[ITSM Status]、および [ITSM ID] の各列に該当する値が表示されます。たとえば、[ITSM Workflow] 列に [RFC]、[ITSM Status] 列に [New]、[ITSM ID] 列に英数字の ID が表示されます。
- 再試行失敗：イベントの再試行に失敗した場合、イベントの [ITSM Workflow]、[ITSM Status]、または [ITSM ID] の値が [N/A] のままになります。2 回目の再試行に失敗した場合の対処方法については、次の手順を参照してください。

ステップ 9 （オプション）再試行に失敗した場合は、Catalyst Center GUI で、メニューアイコンをクリックして次を選択します。 **[Platform]** > **[Developer Toolkit]** > **[APIs]** > **[Ecosystem Integrations]** > **[ITSM]** > **[Get Failed ITSM Events]** の順に選択します。

この API メソッドにアクセスして ITSM 統合のエラーに関する情報を取得できます。

ステップ 10 [Try It] をクリックし、[Runtime] ダッシュボードに表示された失敗したイベントのインスタンス ID（**instanceId**）を入力します。

ステップ 11 [Run] をクリックします。

この API を使用して、次の応答データを取得できます。

- **eventStatus**： ITSM（ServiceNow）イベントのステータス
- **errorCode**：ITSM（ServiceNow）イベントのエラーコード
- **errorDescription**：ITSM（ServiceNow）イベントのエラーの説明
- **responseReceivedFromITSMSystem**：ITSM（ServiceNow）の応答

API で取得した情報を使用して、イベントが失敗した理由を特定して修正します。

API の概要の確認

始める前に

[**API Summary**] フィールドにイベントを表示するには、バンドルを使用します。[**Bundles**] リストでモニターするイベントを提供するバンドルを有効化、設定、およびアクティブ化します。[Bundles] の詳細については、バンドル機能 （118 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Runtime Dashboard]** の順に選択します。

ステップ 2 GUI の右上にある [**Last 1 Week**] をクリックして、[API Summary] の時間間隔を選択します。

直近の 6、12、24 時間、またはその週の API の概要を表示できます。

ステップ 3 [API Summary] フィールドを確認します。

[**API Summary**] フィールドには次の情報が表示されます。

- [Call Status]：API コールの合計数とステータスが表示されます。緑色は成功した API コールを表し、赤色は失敗した API コールを表します。
- [Completed Call Performance]：完了した API コールのパフォーマンス一覧（アルファベット順、単位：秒）（低、平均、高）。
- [View Details]：追加の API 詳細を表示するリンク。

ステップ 4 [View Details] をクリックして、API に関する追加の詳細を確認します。

[All APIs calls] スライドインペインが開きます。

ステップ 5 [All APIs calls] スライドインペインの情報を確認します。

次の情報が表示されます。

- API 名
- API のバージョン
- API コールの合計数、成功した API コール（緑のアイコン）の数、失敗した API コール（赤のアイコン）の数を含む API コールカウントテーブル。
- 最小時間、最大時間、平均時間を含む API 通話時間テーブル

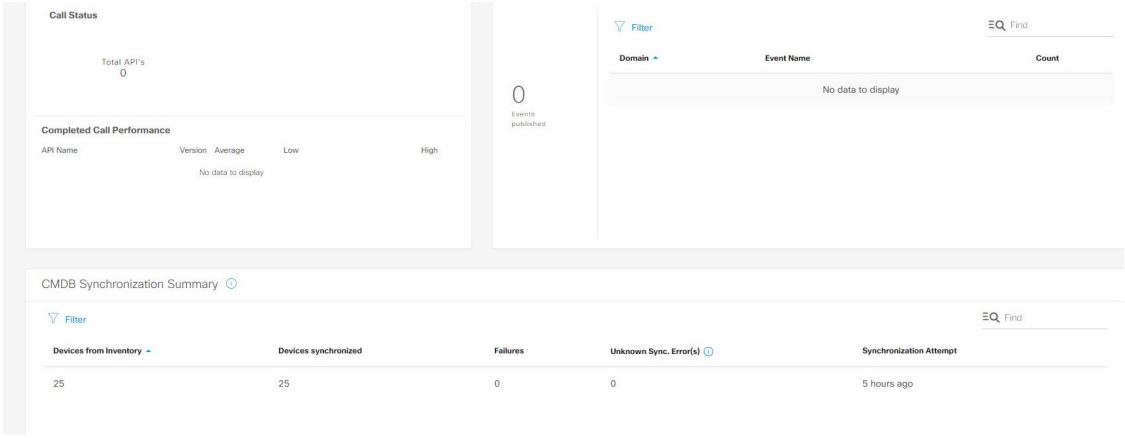
[**Filter**] アイコンをクリックしてフィルタを使用するか、[**Find**] フィールドにキーワードを入力することで、テーブル に表示される API を調整することができます。

CMDB 同期の概要の確認

この手順を実行して Catalyst Center プラットフォーム [**CMDB Synchronization Summary**] を確認します。[CMDB Synchronization Summary] には、ServiceNow に対するインベントリデバイスデータの同期ステータスが表示されます。この概要は、ServiceNow とのデバイスデータ同期をモニターおよびトラブルシューティングするために役立てることができます。

Catalyst Center GUI の [Runtime Dashboard] ウィンドウを使って、[CMDB Synchronization Summary] を確認します。

図 *38 : Catalyst Center* プラットフォーム *Runtime* ウィンドウ



始める前に

[CMDB Synchronization Summary] フィールドでイベントを表示するには、[Bundles] でバンドルを有効化、設定、アクティベートする必要があります。また、[Event Settings] でバンドルに関連するイベント通知を有効にする必要があります。[Bundles] の詳細については、バンドル機能（118 ページ）を参照してください。[Event Settings] の情報については、イベント設定の構成（138 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Runtime Dashboard]** の順に選択します。

ステップ 2 次の情報が表示される [**CMDB Synchronization Summary**] フィールドを確認します。

- [Devices from inventory]：Catalyst Center から収集された [Inventory] からのデバイスの総数。
- [Devices synchronized]：ServiceNow との同期に成功したデバイスのリスト。
- [Failures]：Catalyst Center と ServiceNow の間で失敗した同期試行の回数。

  詳細については、[Learn More...] をクリックしてください。

- [Unknown Synch Errors]：Catalyst Center と ServiceNow の間で部分的に成功した同期試行の回数

  詳細については、[Learn More...] をクリックしてください。

- [Synchronization Attempt]：Catalyst Center と ServiceNow の間で最後に行われた同期試行の日時。

ステップ 3 （オプション）同期の失敗については、[Learn More...] リンクをクリックしてください。

ステップ 4 デバイスの同期失敗に関して表示されたデータを確認します。

次の情報が表に表示されます。

- [Device ID]：デバイス識別番号。
- [Host Name]：デバイスが接続されているホストの名前。
- [Device Type]：スイッチ、ルータ、AP などのデバイスのタイプ。
- [MAC Address]：デバイスの MAC アドレス。
- [Management IP Address]：デバイスのアクセスおよびトラブルシューティングに使用できる、デバイスの管理アドレス。
- [Serial Number]：デバイスのシリアル番号。

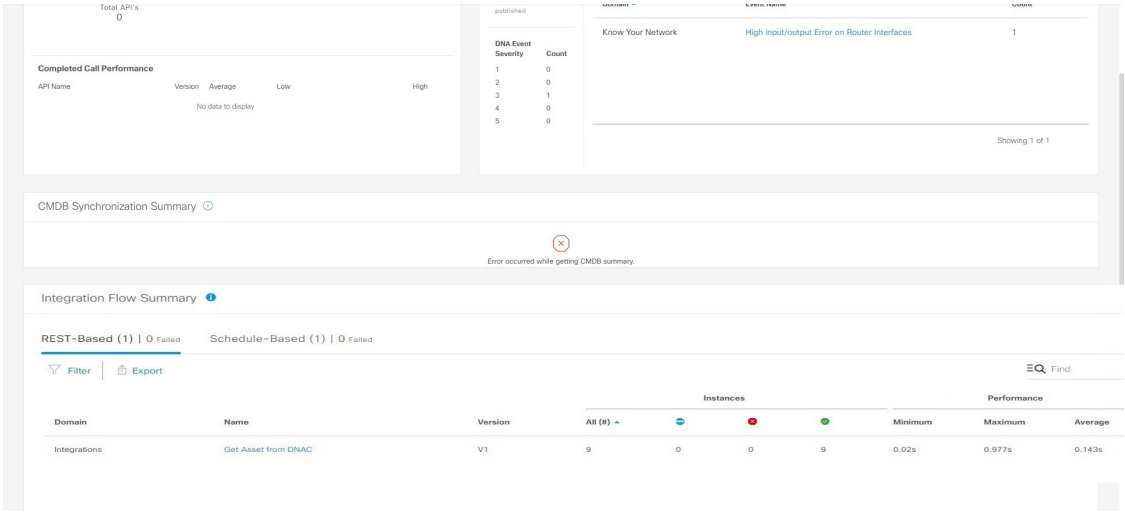
ステップ 5 [DeviceID] リンクをクリックして、[Inventory] ウィンドウでデバイスに関する追加情報を確認します。

統合フローの概要の確認

[Integration Flow Summary]Catalyst Center プラットフォーム を確認するには、この手順を実行します。[Integration Flow Summary] を使って、Catalyst Center プラットフォーム 統合フローのパフォーマンスのモニターリングをサポートできます。この情報は、Catalyst Center プラットフォームのモニターリングやトラブルシューティング、他のシステムとの統合の際に役立ちます。

Catalyst Center GUI の **[Runtime Dashboard]** ウィンドウを使って、[Integration Flow Summary] を確認します。

図 *39 : Catalyst Center* プラットフォーム *Runtime Dashboard* ウィンドウ



始める前に

[Integration Flow Summary] フィールド（2 つのタブ）でデータを表示するには、[Bundles] でモニターするイベントを提供するバンドルを有効化、設定、アクティベートする必要があります。[Bundles] の詳細については、バンドル機能 （118 ページ）を参照してください。

手順

ステップ 1 メインメニューから次を選択します。**[Platform]** > **[Runtime Dashboard]** の順に選択します。

ステップ 2 GUI メニューバーの右上にある [Last 1 Week] をクリックして、[integration flow summary] の時間間隔を選択します。

直近の 6、12、24 時間、またはその週の統合フローの概要を表示できます。

ステップ 3 次の情報が表示される [**Integration Flow Summary**] フィールドを確認します。

- [REST-Based]：ドメイン、統合フロー名とリンク、バージョン、インスタンスの合計、インスタンスのステータス（成功（緑）、失敗（赤）、進行中（青））およびパフォーマンス（最低、最高、平均のコールパフォーマンス時間（ミリ秒））。
- [Schedule-Based]：ドメイン、統合フロー名とリンク、バージョン、インスタンスの合計、インスタンスのステータス（成功（緑）、失敗（赤）、進行中（青））およびパフォーマンス（最低、最高、平均のコールパフォーマンス時間（ミリ秒））。

ステップ 4 REST ベースの統合フローで生成されたデータの概要を表示するには、[REST-Based] タブをクリックします。

ステップ 5 [REST-Based] のデータを確認します。

統合フロー名（リンク）をクリックして、インスタンスに関する追加情報を表示します。この追加情報はスライドインペイン に表示されます。

- [Instance ID]：統合フローへのインスタンスの ID 番号（とリンク）。インスタンスを 1 つ以上の統合フローに設定できます。
- [Status]：インスタンスのステータス（成功または失敗）。
- [Start Time]：インスタンスコールの開始日時。
- [End Time]：インスタンスコールの終了日時。
- [Duration]：コールの時間（秒単位）。

ステップ 6 個々のインスタンス ID（リンク）をクリックして、それぞれに関する詳細な情報を表示します。

この追加情報は スライドインペイン に表示されます。

- [RUN SUMMARY]：開始日時と終了日時、所要時間、ステータス。
- [ERRORS]：エラー応答（ある場合）。
- [LOGS]：ログエントリ（使用可能な場合）。

[X] アイコンをクリックして スライドインペイン を閉じて、前のウィンドウに戻ります。

ステップ 7 スケジュールベースの統合フローで生成されたデータの概要については、[Schedule-Based] タブをクリックします。

ステップ 8 [Schedule-Based] のデータを確認します。

統合フロー名（リンク）をクリックして、インスタンスに関する追加情報を表示します。この追加情報はスライドインペイン に表示されます。

- [Instance ID]：統合フロー内のインスタンスの ID 番号。
- [Status]：インスタンスのステータス（成功または失敗）。
- [Start Time]：インスタンスコールの開始日時。
- [End Time]：インスタンスコールの終了日時。
- [Duration]：コールの時間（秒単位）。

ステップ 9 個々のインスタンス ID（リンク）をクリックして、それぞれに関する詳細な情報を表示します。

この追加情報は スライドインペイン に表示されます。

- [RUN SUMMARY]：開始日時と終了日時、所要時間、ステータス。
- [ERRORS]：エラー応答（ある場合）。
- [LOGS]：ログエントリ（使用可能な場合）。

[X] アイコンをクリックして スライドインペイン を閉じて、前のウィンドウに戻ります。

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。