ネットワークデバイスのコンプライアンス監査

コンプライアンスの概要

コンプライアンスは、元のコンテンツに影響を与えることなく注入または再設定される可能性があるネットワークのインテントの逸脱や**帯域外**の変更を特定するのに役立ちます。

ネットワーク管理者は、Cisco DNA Center でソフトウェアイメージ、PSIRT、ネットワークプロファイルなどコンプライアンスのさまざまな側面のコンプライアンス要件を満たさないデバイスを簡単に特定できます。

コンプライアンスチェックは、自動化することも、オンデマンドで実行することもできます。

- 自動コンプライアンスチェック：Cisco DNA Center でデバイスから収集された最新のデータを使用します。このコンプライアンスチェックは、インベントリやSWIMなどさまざまなサービスからのトラップと通知をリッスンして、データを評価します。
- 手動コンプライアンスチェック：Cisco DNA Center でユーザーが手動でコンプライアンスをトリガーできるようにします。
- スケジュールされたコンプライアンスチェック：スケジュールされたコンプライアンスジョブは、毎週実行されるコンプライアンスチェック（毎週土曜日の午後 11 時に実行）です。

手動コンプライアンスの実行

Cisco DNA Center では、コンプライアンスチェックを手動でトリガーできます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Inventory]** の順に選択します。

ステップ 2 一括してコンプライアンスチェックを行う場合は、次の手順を実行します。

a) 該当するすべてのデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

ステップ 3 デバイスごとにコンプライアンスチェックを行う場合は、次の手順を実行します。

a) コンプライアンスチェックを実行するデバイスを選択します。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

c) または、[Compliance] 列（使用可能な場合）をクリックし、[Run Compliance] をクリックします。

ステップ 4 デバイスの最新のコンプライアンスステータスを表示するには、次の手順を実行します。

a) デバイスとインベントリを選択します。デバイス情報の再同期を参照してください。

b) [Actions] ドロップダウンリストから、**[Compliance]** > **[Run Compliance]** の順に選択します。

（注）
- 到達不能のデバイスやサポートされていないデバイスに対してコンプライアンスの実行をトリガーすることはできません。
- デバイスに対してコンプライアンスを手動で実行しない場合、コンプライアンスチェックはコンプライアンスのタイプに応じて一定期間後に実行されるように自動的にスケジュールされます。

コンプライアンスサマリーの表示

インベントリページには、デバイスごとにコンプライアンスの集約ステータスが表示されます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Inventory]** の順に選択します。

コンプライアンス列には、デバイスごとに集約コンプライアンスステータスが表示されます。

ステップ 2 コンプライアンスステータスをクリックすると、コンプライアンス サマリー ウィンドウが開きます。このウィンドウには、選択したデバイスに適用可能な次のコンプライアンスチェックが表示されます。

- スタートアップ設定と実行中の設定
- ソフトウェア イメージ

- 重大なセキュリティの脆弱性
- ネットワークプロファイル
- ファブリック
- アプリケーションの可視性

（注） [Network Profile]、[Fabric]、および [Application Visibility] はオプションであり、デバイスが必要なデータでプロビジョニングされている場合にのみ表示されます。

コンプライアンスのタイプ

コンプライアンスタイプ	コンプライアンスチェック	コンプライアンスステータス
スタートアップ設定と実行中の設定	このコンプライアンスチェックは、デバイスのスタートアップ設定と実行中の設定が同期しているかどうかを識別するために役立ちます。デバイスのスタートアップ設定と実行中の設定が同期していない場合は、コンプライアンスがトリガーされ、アウトオブバンド変更の詳細レポートが表示されます。スタートアップ設定と実行中の設定の比較に関するコンプライアンスは、**アウトオブバンド**変更の5分以内にトリガーされます。	• [Noncompliant]：スタートアップ設定と実行中の設定は同じではありません。詳細ビューには、スタートアップと実行中との違いか、または実行中と以前の実行中との違いが表示されます。 • [Compliant]：スタートアップ設定と実行中の設定は同じです。 • [NA (Not Applicable)]：このコンプライアンスタイプのデバイスはサポートされていません（たとえば、AireOS）。
ソフトウェアイメージ	このコンプライアンスチェックは、Cisco DNA Centerのタグ付きのゴールデンイメージがデバイスで実行されているかどうかをネットワーク管理者が確認するのに役立ちます。これにより、デバイスのゴールデンイメージと実行中のイメージとの違いがわかります。ソフトウェアイメージに変更があると、遅延なくすぐにコンプライアンスチェックがトリガーされます。	• [Noncompliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行していません。 • [Compliant]：デバイスは、デバイスファミリのタグ付きのゴールデンイメージを実行しています。 • [NA (Not Applicable)]：選択したデバイスファミリではゴールデンイメージを使用できません。

重大なセキュリティ（PSIRT）	PSIRT コンプライアンスチェックでは、ネットワークデバイスが重大なセキュリティの脆弱性なしで実行されているかどうかを確認できます。	• [Noncompliant]：デバイスに重要なアドバイザリがあります。詳細レポートには、その他のさまざまな情報が表示されます。 • [Compliant]：デバイスに重大な脆弱性はありません。 • [NA (Not Applicable)]：Cisco DNA Center でネットワーク管理者がセキュリティ アドバイザリ スキャンを実行していないか、デバイスがサポートされていません。
ネットワークプロファイル	Cisco DNA Center では、ネットワークプロファイルでインテント設定を定義して、プロビジョニングでデバイスにプッシュできます。デバイスでインテントが実行されている必要があります。**アウトオブバンドの変更**のために任意の時点で違反が検出された場合、コンプライアンスはそれを特定し、評価してオフのフラグを立てます。違反は、コンプライアンスサマリーページの [Network Profiles] でユーザーに対して表示されます。自動コンプライアンスチェックは、5時間後に実行されるようにスケジュールされます。 （注） ネットワーク プロファイル コンプライアンスは、ルータおよびワイヤレス LAN コントローラにのみ適用され、スイッチには適用されません。	• [Noncompliant]：デバイスでプロファイルのインテント設定が実行されていません。 • [Compliant]：デバイスでインテント設定が実行されています。 • [Error]：根本的なエラーのため、コンプライアンスがステータスを計算できませんでした。詳細については、エラーログを参照してください。
ファブリック（SDA プロファイル）	ファブリック コンプライアンスは、ファブリックインテント違反（ファブリック関連の設定のアウトオブバンド変更など）の識別に役立ちます。	• [Noncompliant]：デバイスでインテント設定が実行されていません。 • [Compliant]：デバイスでインテント設定が実行されています。
アプリケーションの可視性	Cisco DNA Center では、アプリケーション可視性インテントを作成して、CBAR および NBAR を介してデバイスにプロビジョニングできます。デバイスにインテント違反がある場合、コンプライアンスにより違反が識別されて評価され、[Application Visibility] に準拠または非準拠として表示されます。自動コンプライアンスチェックは、5 時間後に実行されるようにスケジュールされます。	• [Noncompliant]：デバイスで CBAR/NBAR 設定が実行されていません。 • [Compliant]：デバイスで CBAR/NBAR のインテント設定が実行されています。

デバイスのアップグレード後のコンプライアンス動作

- デバイスのアップグレードが正常に完了すると、該当するすべてのデバイス（システムでコンプライアンスが実行されたことがないデバイス）のコンプライアンスチェックがトリガーされます。
- コンプライアンスは、[Startup vs Running] タイプを除き、インベントリに含まれるデバイスのステータスを計算して表示します。
- アップグレード後、[Startup vs Running] タイルに [NA] が「Configuration data is not available」というテキストとともに表示されます。
- アップグレードが正常に完了してから 1 日後に、1 回限りのスケジューラが実行され、デバイスで構成データを使用できるようになります。[Startup vs Running] タイルに、正しいステータス（[Compliant]/[Non-Compliant]）と詳細データが表示され始めます。
- トラップを受信すると、設定アーカイブサービスが構成データを収集し、コンプライアンスチェックが再度実行されます。

（注） アップグレードセットアップでは、[Flex Profile] インターフェイスのコンプライアンスの不一致は無視してください。インターフェイス名の場合、[1] が [management] にマッピングされます。

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。