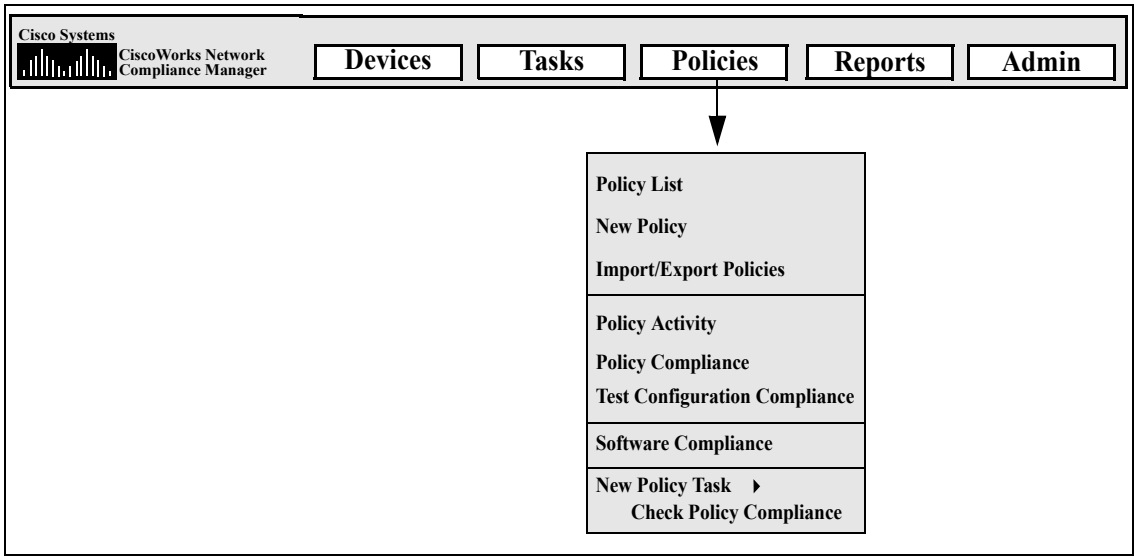
第 8 章：ポリシー保証の管理

次の表を使用すると、情報をすぐに見つけることができます。

ポリシー保証へのナビゲート



はじめに

NCM Policy Manager を使用すると、最高の稼働率と信頼性を保証するネットワーク設定ポリシーとベスト プラクティスを確立できます。さらに、標準化されたデバイス設定を設計することで、個々の設定の差異を減らすことができます。NCM Policy Manager は、承認された設定ポリシーのセットとデバイスの設定を比較することにより、すべてのインフラストラクチャ変更アクティビティを報告することを保証します。

NCM Policy Manager は、NCM が検出したデバイス設定変更に、規則のセット（フィルタ）を適用します。デバイス（またはデバイスのグループ）に対する変更に違反がある場合、NCM Policy Manager はイベントを生成し、通知規則をトリガーします。その結果、違反のある変更を訂正して、準拠性とネットワークのアベイラビリティを維持することができます。

すべての管理対象デバイスについて、ポリシー コンプライアンス ステータスを要約できます。この要約により、ポリシー コンプライアンス ステータスのリスクの度合いに応じたスナップショットを取得して、リスクの高い設定とソフトウェア コンプライアンスの違反を特定し、解決できます。

この項では、次の用語を使用します。

- 設定ポリシー：設定ポリシーは、デバイスまたはデバイス グループに適用する設定規則のセットです。各規則は、デバイスの準拠性を保証するためにデバイスの設定と照合されます。
- 設定規則：設定規則は、設定ポリシーの一部です。*ip name-server* または *interface FastEthernet* のように、正規表現として作成します。設定規則を適用するデバイスの設定と、この表現を照合します。各設定規則は、選択したデバイス ファミリ（BayStack、Cisco IOS など）にのみ適用されます。
- 設定規則の例外：設定規則の例外も、設定規則の一部です。設定規則と同様に、正規表現です。ただし、その目的は、例外テキストがデバイス設定と一致した場合に、この設定規則による処理を行わないようにすることにあります。

（注）設定規則と例外のどちらも、作成するには Administrator または Power User の権限が必要です。

設定ポリシーの作成

設定規則を作成する前に、設定ポリシーを作成する必要があります。設定ポリシーを作成するには、メニューバーの Policies の下で Policy List をクリックします。Policies ページが開きます。このページは、設定ポリシーを作成するまで空です。

NCM の出荷時に、いくつかのデフォルト ポリシー（NSA Router Best Practices ポリシーなど）が設定されています。設定する必要があるポリシーの例を次に示します。

- デバイス グループのすべての設定に Access List 110 を定義する必要があります。
- すべてのファースト イーサネット インターフェイスで、二重化を Auto Negotiate に設定する必要があります。
- すべての境界ルータに、特定の DNS サーバを設定する必要があります。

（注）New policy オプションをクリックするか、既存のポリシーを Policies ページに表示してページの上部にある New Configuration Policy リンクをクリックすると、New Configuration Policy ページに直接移動できます。

Policies ページのフィールド

フィールド	説明
New Configuration Policy リンク	New Configuration Policy ページが開きます。このページでは、新しい設定ポリシーを作成できます。詳細については、P.315 の「New Configuration Policy ページのフィールド」を参照してください。
Check Policy Compliance リンク	Check Policy Compliance task ページが開きます。このページでは、ポリシー コンプライアンスをチェックできます。詳細については、P.280 の「Check Policy Compliance Task ページのフィールド」を参照してください（**注**：メニューバーの Policies/New Policy Task の下で Check Policy Compliance オプションをクリックして、Check Policy Compliance task ページに移動することもできます）。
Import/Export リンク	Import/Export Policies ページが開きます。このページでは、事前設定済みの設定ポリシーをインポートしたり、設定ポリシーをファイルにエクスポートしたりすることができます。詳細については、P.318 の「設定ポリシーのインポートとエクスポート」を参照してください（**注**：Import/Export Policies オプションをクリックして、Import/Export Policies ページに移動することもできます）。

フィールド	説明
チェックボックス	左側のチェックボックスを使用すると、設定ポリシーを管理できます。ポリシーを選択したら、Actions ドロップダウン メニューをクリックして、次のいずれかをクリックします。 • Activate：選択したポリシーでコンプライアンス設定をチェックするように指示します。 • Deactivate：選択したポリシーでコンプライアンス設定をチェックしないように指示します。 • Delete：選択したポリシーを削除します。 隣接する Select ドロップダウン メニューを使用すると、すべてのポリシーを選択または選択解除できます。
Policy Name	ポリシー名が表示されます。
Description	ポリシーの説明が表示されます。
Actions	次のアクションを選択できます。 • View & Edit：Edit Configuration Policy ページが開きます。このページでは、設定ポリシーを編集できます。詳細については、P.319 の「設定ポリシーの編集」を参照してください。 • Test：Test Policy ページが開きます。このページでは、デバイスまたはデバイス グループに対してポリシーをテストできます。詳細については、P.314 の「Test Policy ページのフィールド」を参照してください。

Test Policy ページのフィールド

Test Policy ページでは、デバイスまたはデバイス グループに対してポリシーをテストできます。デバイスを選択した後、Perform Test ボタンをクリックします。

フィールド	説明 / アクション
Select the policies to be tested	ドロップダウン メニューからポリシーを選択します。
Select the devices to test against	Device Selector の使用方法については、P.138 の「Device Selector」を参照するか、Device Selector の右上にある疑問符（?）をクリックしてください。

New Configuration Policy ページのフィールド

New Configuration Policy ページを開くには、メニューバーの Polices の下で New Policy をクリックします。New Configuration Policy ページが開きます。

フィールド	説明 / アクション
Policy Name	ポリシー名を入力します。ポリシーは、デバイスまたはデバイス グループに適用する設定規則のセットです。
Policy Description	ポリシーの説明を入力します。
Applies to these groups	リストから 1 つまたは複数のグループを選択します。複数のグループを選択するには、Shift キーまたは Ctrl キーを押しながらクリックします。
..but not these devices	右側のボックスにデバイスの IP アドレスまたはホスト名を入力し、Add Exception << をクリックします。デバイスを削除するには、左側のボックスでデバイスの IP アドレスまたはホスト名を選択し、Remove Exception をクリックします。
Configuration Rules	設定ポリシーによって適用されるすべての設定規則が、設定規則テーブルに表示されます。設定ポリシーは、この設定ポリシーに対して選択されているデバイスから NCM によって保存された各設定に、すべての設定規則を適用します。設定規則が適用される順序は決まっていないことに留意してください。
New Rule ボタン	この設定ポリシーで使用する新しい規則を作成するには、New Rule ボタンをクリックします。New Configuration Rule ページが開きます。詳細については、P.316 の「New Configuration Rule ページのフィールド」を参照してください。
Detailed Description	設定ポリシーの詳しい説明を入力します。設定ポリシーの簡単な説明は、ポリシーが表示されるすべてのリストに表示されます。このフィールドでは、設定ポリシーの詳しい説明を追加できます。
Policy Status	次のいずれかのオプションをクリックします。 • Active：設定ポリシーをアクティブにします（デフォルト）。 • Inactive：設定ポリシーを非アクティブにします。

終了したら、Save をクリックしてください。

New Configuration Rule ページのフィールド

New Configuration Policy ページの New Rule ボタンをクリックすると、New Configuration Rule ページが開きます。NCM では、正規表現または RegEx（文字列のセットを記述する式）を使用して設定規則を定義することに留意してください。

フィールド	説明 / アクション
New Configuration Rule	
Rule Name	設定規則の名前を入力します。
Rule Description	設定規則の説明を入力します。
Applies to configurations from devices with these drivers	
Device Family	設定規則を適用するデバイス ファミリをドロップダウン メニューから選択します（BayStack、Cisco IOS、Nortel ASF など）。次のいずれかのオプションを選択します。 • All applicable drivers：オンにすると（デフォルト）、該当するすべてのドライバが選択されます。設定規則は、特定のドライバが割り当てられているデバイスの設定にのみ適用されることに留意してください。 • Select specific drivers：オンにした場合は、リストから 1 つ以上のドライバを選択します。設定規則は、特定のドライバが割り当てられているデバイスの設定にのみ適用されることに留意してください。
Apply Rule To	次のいずれかのオプションを選択します。 • Entire Configuration File：設定規則を設定ファイルの全体に適用します（デフォルト）。 • Each Instance of a Block Within the Configuration File：設定規則を設定ファイル内の特定のブロック（Cisco IOS デバイスの単一インターフェイスなど）に適用します。ブロックは、「ブロック開始パターン」と「ブロック終了パターン」の 2 つの正規表現で定義します。設定ファイル内の特定ブロックの各インスタンスに設定規則を適用するには、*interface* .* のようなブロック開始パターンと、*!* のようなブロック終了パターンを入力します。
Each Configuration <must contain> or <must not contain> text that matches the pattern	目的のパターンを入力します。また、そのパターンと一致するテキストを＜含む＞か＜含まない＞かを入力します。「must contain」は、入力したテキストと一致するテキストが含まれている設定ファイルに、この規則を適用することを示します。「must not contain」は、入力したテキストが含まれていない設定ファイルに、この規則を適用することを示します（**注**：Get Help リンクに、正規表現の使用方法に関する情報と例が含まれています）。

フィールド	説明 / アクション
Importance	重大度レベルを選択します。これは、設定ポリシー規則に対する違反リスク レベルを示します。オプションには、次のものがあります。 • Informational：通常は対応する必要がないイベント • Low：時間のあるときに対応すればいよいイベント • Medium：適時（通常、72 時間以内）に対応する必要があるイベント（デフォルト） • High：早急（通常、24 時間以内）に対応する必要があるイベント • Critical：即時に対応する必要があるイベント
Detailed Description	設定規則の説明を入力します。
Rule Exceptions	規則の例外のリストが表示されます（存在する場合）。設定規則の例外も、設定規則の一部です。その目的は、例外テキストがデバイス設定と一致した場合に、この設定規則による処理を行わないようにすることにあります。例外規則を追加するには、New Exception ボタンをクリックします。New Configuration Rule Exception ページが開きます。詳細については、P.320 の「設定規則の例外の追加」を参照してください。

終了したら、Save ボタンをクリックして設定規則を保存するか、Save And Add Another ボタンをクリックして現在の規則を保存してから新しい規則を追加するか、あるいは、New Exception ボタンをクリックして新しい設定規則の例外を追加します。

設定ポリシーのインポートとエクスポート

事前設定済みの設定ポリシーをインポートしたり、設定ポリシーをファイルにエクスポートしたりすることができます。このため、設定ポリシーを簡単に共有できます。

設定ポリシーをインポートまたはエクスポートするには、メニューバーの Policies の下で Import/Export Policies をクリックします。Import/Export Policies ページが開きます。

Import/Export Policies ページのフィールド

フィールド	説明 / アクション
Import Policy	インポートするポリシー ファイルを入力するか、Browse ボタンをクリックしてポリシー ファイルを検索します。ポリシー ファイルが表示されたら、Import ボタンをクリックします。すでにポリシー ファイルが存在する場合は、名前を変更するように要求されます。
Export Policy	現在の設定ポリシーのリストが表示されます。エクスポートする設定ポリシーをクリックし、Export ボタンをクリックします。この設定ポリシーに関連付けられているデバイス グループがある場合でも、デバイス グループはエクスポートされないことに留意してください。また、設定ポリシー例外規則もエクスポートされません。次にポリシーの例を示します。 • Ensure Logging • Ensure Passwords • No Delay on Interfaces • NSA Router Security Best Practices

設定ポリシーの編集

設定ポリシーを編集するには、次の手順を実行します。

1. メニューバーの Policies の下で、Policy List をクリックします。Policies ページが開きます。
2. 編集する設定ポリシーに対応する View & Edit アクションをクリックします。Edit Configuration Policy ページが開きます。終了したら、Save をクリックしてください。

Edit Configuration Policy ページのフィールド

フィールド	説明 / アクション
Policy Name	ポリシー名が表示されます。
Policy Description	ポリシーの説明が表示されます。
Applies to these groups	ポリシーを適用するグループが表示されます。
..but not these devices	デバイスの IP アドレスまたはホスト名を追加するには、右側のボックスにホスト名または IP アドレスを入力し、Add Exception << をクリックします。デバイスを削除するには、左側のボックスでデバイスの IP アドレスまたはホスト名を選択し、Remove Exception をクリックします。
Configuration Rules	この設定ポリシーで適用されるすべての設定規則が表示されます。設定ポリシーは、この設定ポリシーに対して選択されているデバイスから保存した各設定に、すべての設定規則を適用します。設定規則が適用される順序は決まっていないことに留意してください。importance カラムに、Informational、Low、Medium、High、または Critical が表示されます。これは、設定ポリシー規則に対する違反リスク レベルを示します。設定規則を編集するには、Actions カラムで View & Edit リンクをクリックします。
New Rule ボタン	この設定ポリシーで使用する新しい規則を作成するには、New Rule ボタンをクリックします。New Configuration Rule ページが開きます。詳細については、P.316 の「New Configuration Rule ページのフィールド」を参照してください。
Detailed Description	設定ポリシーの詳細な説明が表示されます。
Policy Status	次のいずれかのオプションをクリックします。 • Active：設定ポリシーをアクティブにします（デフォルト）。 • Inactive：設定ポリシーを非アクティブにします。

設定規則の例外の追加

設定規則の例外も、設定規則の一部です。設定規則と同様に、正規表現です。ただし、その目的は、例外テキストがデバイス設定と一致した場合に、この設定規則による処理を行わないようにすることにあります。

例外規則は、通常、設定規則からテキスト パターンまたは特定のデバイス設定を除外します。一般に、例外は、規則に違反するデバイス設定がある場合、同様の設定にすべて適合するように規則を変更できないときに作成します。

設定規則の例外を既存の設定規則に追加するには、次の手順を実行します。

1. メニューバーの Policies の下で、Policy List をクリックします。Policies ページが開きます。
2. 例外規則を追加するポリシーを選択し、View & Edit をクリックします。Edit Configuration Policy ページが開きます。
3. New Rule ボタンをクリックします。New Configuration Rule ページが開きます。
4. ページの下部にある New Exception ボタンをクリックします。New Configuration Rule Exception ページが開きます。

New Configuration Rule Exception ページのフィールド

フィールド	説明 / アクション
Expires on	オンにした場合は、この規則が例外を無視するようになる月、日、年、時、分を選択します。例外規則の有効期限は、例外が規則に対して効力を失う日付です。有効期限を過ぎても例外規則は存在し続けますが、設定ポリシーは例外規則が存在しないものとして規則を適用します。
Ignore this device entirely when checking the configuration rule	オンにした場合は、設定規則のチェック時に NCM はこのデバイスをスキップします。
Ignore text matching this pattern when checking the configuration rule	オンにした場合は、正規表現を入力します。正規表現と一致する設定規則のすべてのテキストが、この設定規則の対象外になります（**注**：Get Help オプションで、例を参照できます）。
Device	この例外規則を適用するデバイスの IP アドレスまたはホスト名を入力します。

終了したら、Save ボタンをクリックしてください。

設定ポリシー アクティビティの表示

設定ポリシーに含まれている設定規則にデバイスの設定が準拠していなかったことを示すイベントを表示できます。イベントは、デバイスの設定に違反があることを NCM が検出し、記録した時間を示します。

Configuration Policy Activity ページを開くには、メニューバーの Polices の下で Policy Activity をクリックします。Configuration Policy Activity ページが開きます。

Configuration Policy Activity ページのフィールド

フィールド	説明 / アクション
For the (time frame)	違反イベントを表示する時間フレームを選択します。デフォルトは、過去 1 時間です。
Current Working Group	違反イベントを表示するグループを選択します。デフォルトは Inventory で、このグループには他のすべてのグループが含まれます。
Event Date	設定ポリシーの違反が検出された日付が表示されます。
Policy Name	設定ポリシーの名前が表示されます。このリンクをクリックすると、Edit Configuration Policy ページが開きます。設定ポリシー、および設定規則に含まれている任意の項目を編集できます。詳細については、P.319 の「設定ポリシーの編集」を参照してください。
Host Name	デバイスのホスト名が表示されます。このリンクをクリックすると、デバイスの基本情報と設定履歴が表示されます。
Device IP	デバイスの IP アドレスが表示されます。このリンクをクリックすると、デバイスの基本情報と設定履歴が表示されます。
Summary	イベント タイプ（Configuration Policy Non-Compliance）が表示されます。このリンクをクリックすると、System Event Detail ページが開きます。このページでは、違反イベントの詳細を表示できます。
Importance	次のように、違反したコンプライアンス規則の重要度を示します。 • Informational：通常は対応する必要がないイベント • Low：時間のあるときに対応すればいよいイベント • Medium：適時（通常、72 時間以内）に対応する必要があるイベント • High：早急（通常、24 時間以内）に対応する必要があるイベント • Critical：即時に対応する必要があるイベント
Added By	設定ポリシーを追加したユーザまたはプロセスが表示されます。

ポリシー コンプライアンスの表示

Policy Compliance ページでは、設定が設定ポリシーに準拠しているデバイス、または準拠していないデバイスを表示できます。Policy Compliance ページを開くには、メニューバーの Polices の下で Policy Compliance をクリックします。Policy Compliance ページが開きます。

Policy Compliance ページのフィールド

フィールド	説明 / アクション
Check Policy Compliance リンク	Check Policy Compliance task ページが開きます。このページでは、設定のコンプライアンスをチェックできます。詳細については、P.280 の「Check Policy Compliance Task ページのフィールド」を参照してください。
Current Working Group	デバイス コンプライアンス ステータスを表示するグループを選択します。
Display only devices that are not in compliance	オンにした場合、違反のないデバイスは表示されません。
Host Name	デバイスのホスト名が表示されます。このリンクをクリックすると、デバイスの基本情報と設定履歴が表示されます。
Device IP	デバイスの IP アドレスが表示されます。このリンクをクリックすると、デバイスの基本情報と設定履歴が表示されます。
Policy Compliance	• Yes : デバイスの設定が、すべての設定ポリシーに準拠していることを示します。 • No : デバイスの設定が、一部の設定ポリシーに準拠していないことを示します。
Importance	現在このデバイスが違反しているすべての設定ポリシー規則の中で、最も重要度が高いものが表示されます。 • Critical : 赤 • Medium : 青 • Low : 黄色
Last Changed Time	デバイスの設定が最後に変更された日時が表示されます。

フィールド	説明 / アクション
Actions	次のオプションを選択できます。 • Policy Events : Configuration Policy Activity ページが開きます。このページでは、違反イベントの詳細を表示できます。 • Policies Applied : Configuration Policies that Apply to Device ページが開きます。このページでは、特定のデバイスの設定ポリシーおよび規則を表示できます。詳細については、P.323 の「Configuration Policies That Apply to Device ページのフィールド」を参照してください。

Configuration Policies That Apply to Device ページのフィールド

Configuration Policies That Apply to Device ページを表示するには、次の手順を実行します。

1. メニューバーの Policies の下で、Policy Compliance をクリックします。
2. 情報を表示するデバイスの Actions カラムで、Policies Applied リンクをクリックします。Configuration Policies That Apply to Device ページが開きます。

フィールド	説明 / アクション
Policy Name	デバイスに適用されている設定ポリシーの名前が表示されます。
Rule Name	デバイスに適用されている設定規則の名前が表示されます。
Out of compliance key	現在デバイスが準拠しているかどうかが表示されます。 • Critical Importance（赤） • High Importance（赤） • Medium Importance（オレンジ） • Low Importance（黄） • Informational（黄）
Actions	次のオプションを選択できます。 • Host name or IP address : Device Information ページが開きます。このページでは、デバイスとその設定履歴に関する基本情報を表示できます。 • Policy Name : Edit Configuration Policy ページが開きます。このページでは、ポリシーの編集および設定規則の追加 / 編集を行うことができます。P.319 の「設定ポリシーの編集」を参照してください。 • Rule Name : Edit Configuration Rule ページが開きます。このページでは、設定規則を編集できます。P.320 の「設定規則の例外の追加」を参照してください。

新しいソフトウエア コンプライアンスの追加

ネットワーク デバイス セキュリティの警告、およびセキュリティ上の脆弱性に関する通知は増え続けているため、多くの組織で、各デバイスに存在する OS バージョン、およびその OS バージョンがセキュリティの問題に対して脆弱かどうかを追跡するという困難な作業が必要になっています。NCM を使用すると、セキュリティの問題の影響を受ける OS バージョンを指定し、そのバージョンが検出されたときに警告または自動対処を生成できます。イメージは「pre-production」、「Obsolete」などのカテゴリにグループ化できます。最近検出された脆弱性に基づいて、「Security Risk」などに分類することもできます。

新しいソフトウェア コンプライアンスの追加、または既存のコンプライアンス定義の確認を行うには、次の手順を実行します。

1. メニューバーの Polices の下で、Software Compliance をクリックします。Software Compliance ページが開きます（Software Compliance ページについては、P.326 の「Software Compliance ページのフィールド」を参照してください。
2. Add Compliance リンクをクリックします。Add Compliance ページが開きます。作業が終了したら、必ず Save をクリックしてください。

Add Compliance ページのフィールド

フィールド	説明 / アクション
Add Compliance	
Policy Name	ポリシー名を入力します。
Status	次のいずれかのオプションが表示されます。 • Active：設定ポリシーをアクティブにします（デフォルト）。 • Inactive：設定ポリシーを非アクティブにします。非アクティブなポリシーは、違反イベントを生成しません。

フィールド	説明 / アクション
Compliance Level	コンプライアンス レベルの名前を選択します。要件と検証手順に応じて、指定されている任意のコンプライアンス定義を使用できます。オプションには、次のものがあります。 • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	コンプライアンスの説明を入力します。
Matching Criteria（照合基準にはワイルドカード演算子の * および ? を使用できます）	
Software Version	現在デバイスで実行しているソフトウェアのバージョンを入力します。
Device Driver	デバイスへのアクセスに使用するデバイス ドライバをドロップダウン メニューから選択します（Any がデフォルトです）。
Device Model	デバイス モデルを入力します。
Configuration Contains	指定されたデバイスにこのコンプライアンスを適用するかどうかを判断するために、現在のデバイス設定と照合するパターンを入力します。
Software Vulnerability Information (for Security Risk compliance level)	
Discloser Date	ソフトウェアの脆弱性にフラグが設定された日付を *yyyy-MM-dd* の形式で入力します。
Importance	次のようなセキュリティ脆弱性の重大度をドロップダウン メニューから選択します。 • Informational • Low • Medium • High • Critical
CVE Name	CVE（Common Vulnerabilities and Exposures）名を入力します。CVE は、脆弱性の標準名およびセキュリティ上の危険性に関するその他の情報のリストです（詳細については、www.cve.mitre.org を参照してください）。
Solution	解決方法に関する詳細な情報を入力します。

フィールド	説明 / アクション
Advisory リンク	脆弱性に関する勧告情報の外部参照への URL を入力します。
Solution リンク	脆弱性に対して適用可能な解決方法に関する詳細情報の外部参照への URL を入力します。

Software Compliance ページのフィールド

Software Compliance ページでは、既存のソフトウェア コンプライアンス定義を確認できます。

フィールド	説明 / アクション
Add Compliance リンク	Add Compliance ページが開きます。このページでは、コンプライアンスを追加できます。P.324 の「Add Compliance ページのフィールド」を参照してください。
Device Software Report リンク	Device Software レポートが開きます。このレポートでは、各デバイスに現在割り当てられているソフトウェア バージョンおよびコンプライアンス レベルを表示できます。P.476 の「Device Software レポートのフィールド」を参照してください。
Software Vulnerabilities Report リンク	Software Vulnerability レポートが開きます。このレポートでは、重大度でソートされたセキュリティ違反のイベントに加え、各デバイスに現在割り当てられているソフトウェア バージョンおよびコンプライアンス レベルを表示できます。P.478 の「Software Vulnerability レポートのフィールド」を参照してください。
View	ドロップダウン メニューから「User-define policies」または「Security Alert Service alerts」を選択します。Security Alert Service alerts は、Security Alert Service から送信された警告です（**注**：Security Alert Service は、加入が必要なサービスです）。
チェックボックス	左側のチェックボックスを使用すると、ソフトウェア コンプライアンス定義を管理できます。コンプライアンス定義を選択したら、Actions ドロップダウン メニューをクリックして、次のいずれかをクリックします。 • Activate：ソフトウェア コンプライアンス定義を有効にするように NCM に指示します。 • Deactivate：ソフトウェア　コンプライアンス定義を無効にするように NCM に指示します。 • Delete：ソフトウェア コンプライアンス定義を削除します。 隣接する Select ドロップダウン メニューを使用すると、すべてのポリシーを選択または選択解除できます。

フィールド	説明 / アクション
Name	コンプライアンスの名前が表示されます。
Version	ソフトウェア バージョンが表示されます。
Device Driver	ドライバ名が表示されます。
Model	デバイスのモデル識別子が表示されます。
Compliance	コンプライアンス レベルの名前が表示されます。レベルには、次のものがあります。 • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Importance	Informational、Low、Medium、High、または Critical が表示されます。これは、違反したコンプライアンス規則の重要度を示します。 • Informational：通常は対応する必要がないイベント • Low：時間のあるときに対応すればいよいイベント • Medium：適時（通常、72 時間以内）に対応する必要があるイベント • High：早急（通常、24 時間以内）に対応する必要があるイベント • Critical：即時に対応する必要があるイベント
Comments	コンプライアンスの説明が表示されます。
Actions	次のオプションを選択できます。 • Edit：Edit Compliance ページが開きます。このページでは、コンプライアンスを編集できます。 • Delete：コンプライアンスを削除できます。

ソフトウェア コンプライアンスの編集

ソフトウェア コンプライアンスを編集するには、次の手順を実行します。

1. メニューバーの Policies の下で、Software Compliance をクリックします。Software Compliance ページが開きます。
2. 編集するソフトウェア コンプライアンスに対応する Edit アクションをクリックします。Edit Compliance ページが開きます。終了したら、Save をクリックしてください。

Edit Compliance ページのフィールド

フィールド	説明 / アクション
Edit Compliance	
Policy Name	ポリシー名が表示されます。
Status	次のいずれかのオプションが表示されます。 • Active：設定ポリシーをアクティブにします（デフォルト）。 • Inactive：設定ポリシーを非アクティブにします。非アクティブなポリシーは、違反イベントを生成しません。
Compliance Level	コンプライアンス レベルの名前が表示されます。要件と検証手順に応じて、指定されている任意のコンプライアンス定義を使用できます。オプションには、次のものがあります。 • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Description	コンプライアンスの説明が表示されます。
Matching Criteria	
Software Version	現在デバイスで実行しているソフトウェアのバージョンが表示されます。
Device Driver	デバイスへのアクセスに使用するデバイス ドライバが表示されます。
Device Model	デバイス モデルが表示されます。

フィールド	説明 / アクション
Configuration Contains	指定されたデバイスにこのコンプライアンス ポリシーを適用するかどうかを判断するために、現在のデバイス設定と照合するパターンが表示されます。
Software Vulnerability Information (for Security Risk compliance level)	
Discloser Date	ソフトウェアの脆弱性にフラグが設定された日付が表示されます。
Importance	セキュリティ上の脆弱性の重大度が表示されます。重大度には、次のものがあります。 • Informational • Low • Medium • High • Critical
CVE Name	CVE（Common Vulnerabilities and Exposures）名が表示されます。CVE は、脆弱性の標準名およびセキュリティ上の危険性に関するその他の情報のリストです（詳細については、www.cve.mitre.org を参照してください）。
Solution	解決方法に関する情報が表示されます。
Advisory リンク	脆弱性に関する勧告情報の外部参照への URL が表示されます。
Solution リンク	脆弱性に対して適用可能な解決方法に関する詳細情報の外部参照への URL が表示されます。

設定のコンプライアンスのテスト

1 つ以上の設定ポリシーに対してデバイス設定のコンプライアンスをテストできます。また、1 つ以上の設定に対して自分の設定ポリシーをテストできます。このため、デバイスの設定のコンプライアンスをテストしたり、展開前に設定ポリシーをテストしたりすることができます。

メニューバーの Policies の下で、Test Configuration Compliance をクリックします。Test Configuration Compliance ページが開きます。

Test Configuration Compliance ページのフィールド

フィールド	説明 / アクション
Policy List リンク	Policies ページが開きます。このページでは、ポリシーのリストを表示できます。詳細については、P.313 の「Policies ページのフィールド」を参照してください。
Select the policies to be applied	次のいずれかのオプションを選択できます。 • All Policies：オンにした場合（デフォルト）、すべての設定ポリシーがテストされます。 • Polices that are applicable to selected device groups：テストを実行するデバイス グループを選択します。複数のデバイス グループを選択するには、Shift キーを押しながらデバイス グループを選択します。 • Selected policies：特定のポリシーを選択します。複数のポリシーを選択するには、Shift キーを押しながらポリシーを選択します。
Test policy against existing devices	このオプションを選択すると、Device Selector が開きます。Device Selector の使用方法については、P.138 の「Device Selector」を参照するか、Device Selector の右上にある疑問符（?）をクリックしてください。
Test policy against configuration	このオプションを選択した場合は、ボックス内に設定テキストを入力するか貼り付けて、その設定テキストのデバイス ファミリをドロップダウン メニューから選択します。

設定が終了したら、Perform Test をクリックします。設定ポリシーのチェックに成功すると、「The configuration is in compliance with all selected policies」というメッセージがページの下部に表示されます。設定ポリシーのチェックに失敗すると、各違反のリストがページの下部に表示されます。このリストには、「View the entire configuration」のような詳細情報へのリンクが含まれています。

（注）Policies ページの Actions カラムの Test オプションをクリックして、設定テキストに対してポリシーをテストすることもできます。Test Policy ページが開きます。詳細については、P.330 の「Test Configuration Compliance ページのフィールド」を参照してください。