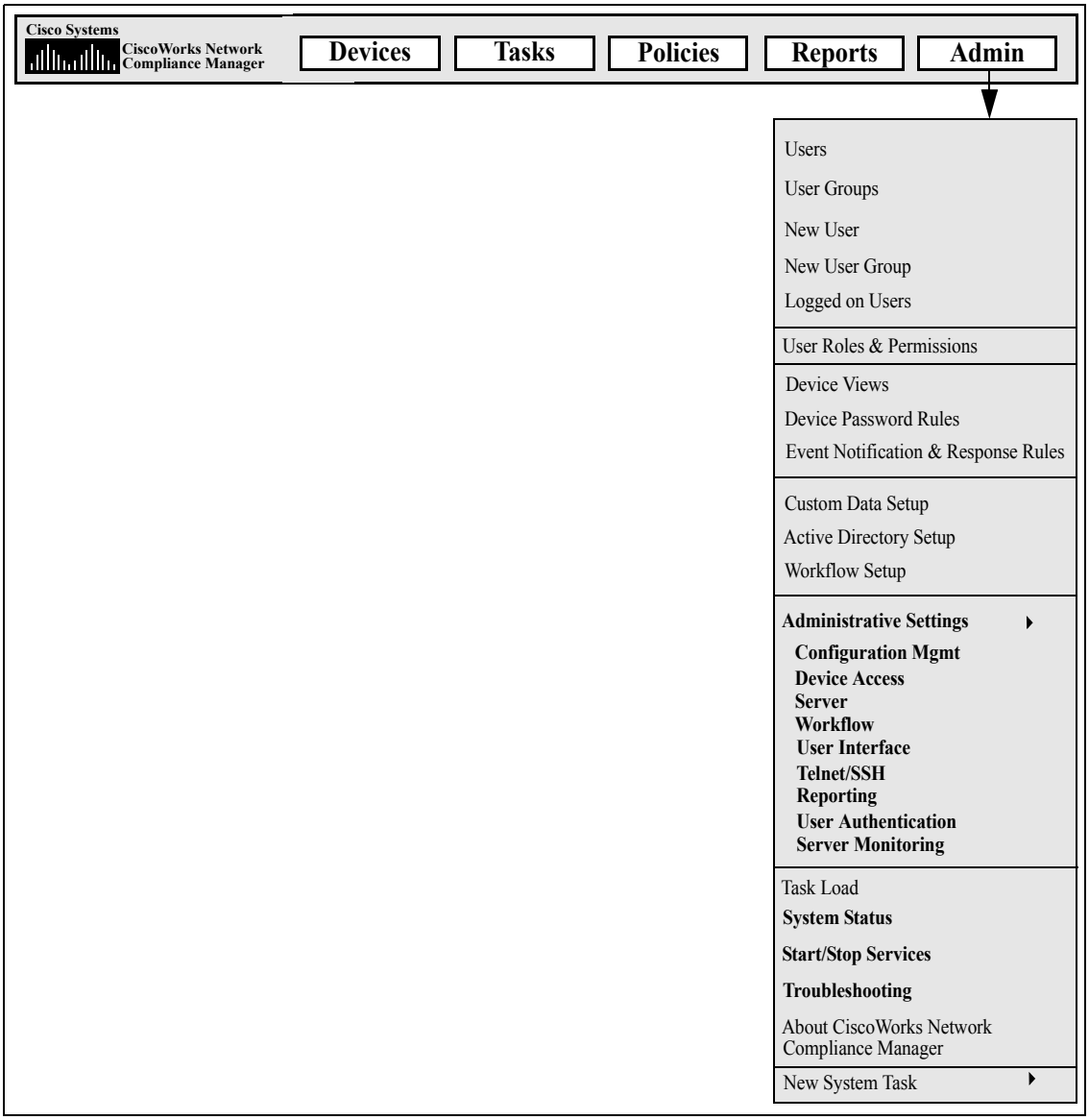
第 2 章：管理設定の構成

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。

トピック	参照先
はじめに	はじめに（P.53）
Configuration Management	Configuration Management（P.54）
Device Access	Device Access ページのフィールド（P.64）
Server	Server（P.72）
Workflow	Workflow（P.78）
User Interface	User Interface（P.80）
Telnet/SSH	Telnet/SSH（P.85）
Reporting	Reporting（P.89）
User Authentication	User Authentication（P.95）
Active Directory 認証の設定	Active Directory 外部認証の設定（P.100）
Server Monitoring	Server Monitoring（P.103）
モニタ結果の表示	モニタ結果の表示（P.107）
サービスの開始と停止	サービスの開始と停止（P.113）
ロギングのイネーブル化	ロギングのイネーブル化（P.115）

管理設定へのナビゲート



はじめに

システム管理者は、CiscoWorks Network Compliance Manager（NCM）の操作に影響する、変更可能な設定の値を定義できます。これらの設定にはインストール時に初期値が入力されますが、その値を変更して機能をカスタマイズすることができます。たとえば、各種の操作に関連付けられた間隔のデフォルト値を変更したり、スクリプト言語のサポートを設定したりすることができます。また、特定のページの表示や内容をカスタマイズすることもできます。

設定オプションを確認して変更を加えるには、メニューバーの Admin の下で、Administrative Settings を選択します。次のオプションを選択できます。

- Configuration Management
- Device Access
- Server
- Workflow
- User Interface
- Telnet/SSH
- Reporting
- User Authentication
- Server Monitoring

Configuration Management

Configuration Mgmt ページでは、次の設定が可能です。

- 設定変更の検出
- ユーザ ID
- スタートアップ コンフィギュレーションと実行コンフィギュレーション
- ACL 解析
- 設定ポリシーの検証
- タスク前およびタスク後のスナップショット
- トポロジ データおよび二重データの収集
- フラッシュ ストレージ スペース
- ブート検出

Configuration Mgmt ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、Configuration Mgmt をクリックします。Configuration Mgmt ページが開きます。Save をクリックして、変更を保存してください。

Configuration Mgmt ページのフィールド

フィールド	説明 / アクション
Change Detection	
Change Detection	次のいずれかのオプションを選択します。 • Enabled : NCM は、変更が検出されるたびに、デバイス設定のスナップショットを取得します（デフォルト）。 • Polling Only : NCM は、デバイス グループのスナップショットの実行中にデバイス設定のスナップショットを取得しますが、変更が検出されたときには取得しません。 • Disabled : 変更が検出されたときも、デバイス グループのスナップショットの実行中も、設定のスナップショットは取得されません。 変更の検出の詳細については、P.60 の「変更の検出」を参照してください。
Change Detection Interval	変更が検出されてからスナップショットが開始するまでの遅延間隔を入力します。デフォルトは 10 分です。NCM が変更を検出した場合、デバイスのスナップショットは、ここで指定された間隔を空けて遅延します。遅延後のスナップショットは、その間隔中に送信された変更通知をすべて反映します。

フィールド	説明 / アクション
Syslog Detection Patterns	NCM に用意されているデフォルト パターンに別のパターンを追加する場合は、右側のボックスにパターンを入力し、Add Pattern << をクリックします。左側のボックスでパターンを選択して Delete Pattern をクリックすると、パターンを削除できます。NCM は、Syslog サーバでこれらのパターンと一致するものを検索します。上記のフィールドで Enabled を選択した場合、一致するものが見つかると、NCM は設定の変更を示し、デバイス設定のスナップショットを取得します（**注**：シスコでは Syslog サーバを提供しています。NCM のインストール時に現在の Syslog サーバを残した場合でも、Syslog メッセージを NCM Syslog サーバに中継するための NCM Syslog サーバをインストールする必要があります）。
Syslog Patterns to Ignore	特定のパターンを無視する場合は、右側のボックスにパターンを入力し、Add Pattern << をクリックします。左側のボックスでパターンを選択して Delete Pattern をクリックすると、パターンを削除できます。
Use IP Address of sender of Syslog Messages	オンの場合、Syslog メッセージの送信者の IP アドレスが使用されます。
Users to Ignore for Change Detection	Syslog または AAA の変更イベントを処理するときに無視するユーザを示します。ユーザを追加するには、右側のボックスにユーザ名を入力し、Add Username << をクリックします。ユーザを削除するには、左側のボックスでユーザ名を選択し、Delete Username をクリックします。
Change User Identification	
Auto-Create Users	オンの場合、NCM は、設定変更を行ったユーザが認識されないときに、新しいユーザを作成します。
Auto-Create User Suffix	NCM が Auto-Create 機能で新しいユーザに追加するサフィックスを入力します。デフォルトは「_auto」です。
Syslog User Identification	オンの場合、NCM は Syslog メッセージからユーザを特定しようとします。
Syslog User Patterns	右側のボックスにパターンを入力し、Add Pattern << をクリックします。左側のボックスでパターンを選択して Delete Pattern をクリックすると、パターンを削除できます。NCM は、Syslog でこれらの正規表現と一致するものを検索します。一致するものが見つかると、NCM はそのテキストをユーザとして取り込みます。通常、これらのパターンは、デバイス ドライバによって入力されます。
Resolve Workstation IP Address from Syslog	オンの場合、NCM は Syslog メッセージから IP アドレスを解決し、そのドメインを当該の設定変更を行ったユーザの名前として処理します。この方法は、Syslog メッセージ以外の方法でユーザ名を特定できない場合にだけ使用されます。

フィールド	説明 / アクション
Store Unresolved IP Addresses	オンの場合、NCM は DNS を使用してホスト名を解決できないときに、IP アドレスをユーザ名として処理します。ピリオドはダッシュで置き換えられます。たとえば、10.10.1.1 は user 10-10-1-1 となります。
Auto-Create Users from Syslog	このオプションと Auto-Create Users がオンの場合、NCM は、Syslog メッセージから特定されたユーザを既存のユーザと照合します。既存のユーザがない場合は、新しいユーザが作成されます。
Startup/Running Configurations	
Capture Startup Config	次のいずれかのオプションを選択します。 • Off : NCM は各スタートアップ コンフィギュレーションを取り込みません。 • Detect Only : NCM は各スタートアップ コンフィギュレーションを取り込み、実行コンフィギュレーションと比較します。ただし、スタートアップ コンフィギュレーションは格納されません。 • On（デフォルト）: NCM は各スタートアップ コンフィギュレーションを取り込み、実行コンフィギュレーションと比較します。その後、スタートアップ コンフィギュレーションを格納します。ベンダーやデバイスの中には、スタートアップ コンフィギュレーションの概念をサポートしないものがあることに留意してください。
Snapshot after Sync	オンの場合、NCM はスタートアップ コンフィギュレーションと実行コンフィギュレーションを同期してから、スナップショットを取得します。
ACL Parsing	
Parse ACL Data with each Snapshot	次のいずれかのオプションを選択します。 • Enabled : NCM は各スナップショットで ACL データを解析し、格納します。 • Disabled : NCM は各スナップショットで ACL データを解析しません。 このオプションで設定されるのは、新しいデバイスを追加する場合のこの機能のデフォルト状態だけであることに留意してください。一括編集を使用すると、デバイス グループの ACL 解析のオンとオフを切り替えることができます（**注** : このオプションは、デバイスごとに上書きできます）。

フィールド	説明 / アクション
ACL Editing	
Show pre-edit application script	オンの場合、ACL を編集または作成するときは、前処理 ACL アプリケーションのスクリプトが表示されます。前処理アプリケーション スクリプトは、デバイス上の既存の ACL アプリケーションを無効にします。新規または更新後の ACL スクリプトにより、編集済みの ACL がデバイスに追加されます。
Show edit preparation script	オンの場合、ACL を編集または作成するときは、編集準備スクリプトが表示されます。編集準備スクリプトは、編集済みの ACL を受け入れるようにデバイスを準備するためのスクリプトをすべて実行します。
Show application script	オンの場合、ACL を編集または作成するときは、ACL アプリケーション スクリプトが表示されます。アプリケーション スクリプトは、ACL を VTY 接続などに適用するときに使用されるスクリプトです。アプリケーション スクリプトにより、ACL が再度適用されます。
Configuration Policy Verification	
Verify Before Deploy by Default	オンの場合、NCM は編集済みの設定を展開する前に、定義済みの設定ポリシーと照合します。
Pattern Timeout	パターンと設定を照合する時間の許容最大値を秒単位で入力します。デフォルトは 30 秒です。
Pre-Task and Post-Task Snapshots	
User Override Pre/Post Task Snapshot	オンの場合、ユーザは個別のタスクを実行するときに、タスク前およびタスク後のスナップショットのデフォルト設定を上書きできます。上書きを許可した場合は、New Task ページの該当する場所に、タスク前およびタスク後のスナップショットのオプションが表示されます。上書きを許可しない場合は、デフォルト設定が使用されます（詳細については、P.62 の「タスク前およびタスク後のスナップショットの設定」を参照してください）。

フィールド	説明 / アクション
Allow Per-Script Pre/Post Task Snapshot Setting Hints	オンの場合、個別のスクリプトによって、タスク前およびタスク後のスナップショットの設定を上書きできます。 **注**：タスク前のスナップショットの設定を上書きする場合、タスク前のスナップショットを要求するときは「tc_pre_snapshot=true」というテキストを、タスク前のスナップショットを要求しないときは「tc_pre_snapshot=false」というテキストを、コメントとしてスクリプトに含めてください。タスク後のスナップショットの設定を上書きする場合、タスク後のスナップショットをタスクの一部として要求するときは「tc_post_snapshot=true」というテキストを、タスク後のスナップショットを別個のタスクとして要求するときは「tc_post_snapshot=task」というテキストを、タスク後のスナップショットを要求しないときは「tc_post_snapshot=false」というテキストを、コメントとしてスクリプトに含めてください。 詳細については、P.62 の「タスク前およびタスク後のスナップショットの設定」を参照してください。
Snapshot Before Run Command Script	次のいずれかのオプションを選択します。 • None • As part of task
Snapshot After Run Command Script	次のいずれかのオプションを選択します。 • None • As part of task • Scheduled as separate task
Snapshot Before Configuration Deployment	次のいずれかのオプションを選択します。 • None • As part of task
Snapshot After Configuration Deployment	次のいずれかのオプションを選択します。 • None • As part of task • Scheduled as separate task
Snapshot Before Run Diagnostic	次のいずれかのオプションを選択します。 • None • As part of task

フィールド	説明 / アクション
Snapshot After Run Diagnostic	次のいずれかのオプションを選択します。 • None • As part of task • Scheduled as separate task
Snapshot Before Delete ACL	次のいずれかのオプションを選択します。 • None • As part of task
Snapshot After Delete ACL	次のいずれかのオプションを選択します。 • None • As part of task • Scheduled as separate task
Snapshot After Synchronize Startup/Running	次のいずれかのオプションを選択します。 • None • As part of task • Scheduled as separate task
Post-Task Snapshot Delay	タスク後のスナップショットを別個のスナップショット タスクとして実行する場合は、その遅延時間を入力します。デフォルトは 30 秒です。
Diagnostics	
Topology Data Gathering Frequency	トポロジ データは、ネットワーク パフォーマンスを維持するためのスロットリングを必要とする、新しい診断クラスに含まれます。ネットワーク ダイアグラムを表示する際に、トポロジ データが使用されます。トポロジ データの収集作業は、NCM サーバに高い負荷をかけるため、できるだけ間隔を空けて行う必要があります。トポロジ データを収集する間隔の許容最小値を時間単位で入力します。デフォルトは 168 時間です。
Stored Topology Data	データベースに現在格納されているトポロジ データの許容存続期間を時間単位で入力します。格納されているデータがこの値より古い場合、デバイスから直接データを取得します。そうでない場合、格納されているデータを使用します。デフォルトは 72 時間です。

フィールド	説明 / アクション
Duplex Data Gathering Frequency	二重化のミスマッチ データは、ネットワーク パフォーマンスを維持するためのスロットリングを必要とする、新しい診断クラスに含まれます。エンドツーエンド パフォーマンスの一般的な問題を特定する際に、二重化のミスマッチ データが使用されます。二重化のミスマッチが頻繁に発生するのは、一方のマシンが全二重に設定され、もう一方のマシンが半二重に設定されている場合です。二重化のミスマッチ データの収集作業は、NCM サーバに高い負荷をかけるため、できるだけ間隔を空けて行う必要があります。二重データを収集する間隔の許容最小値を時間単位で入力します。デフォルトは 168 時間です。
Stored Duplex Data	データベースに現在格納されている二重データの許容存続期間を時間単位で入力します。格納されているデータがこの値より古い場合、デバイスから直接データを取得します。そうでない場合、格納されているデータを使用します。デフォルトは 72 時間です。
Flash Storage Space	
Flash Low Event	オンの場合、検出されたフラッシュ ストレージの空きスペースが不足していると、イベントが生成されます。
Flash Low Threshold	スペース不足イベントの生成基準となる、フラッシュ ストレージ スペースの使用率を入力します。デフォルトは 90% です。
Boot Detection	
Error Margin Factor	デバイス ブートを検出するときのクロック ドリフトの許容量（6 時間あたりの秒数）を入力します。デバイスを確認する最小頻度は、6 時間ごとに 1 回とすることをお勧めします。

変更の検出

NCM は、デバイス設定の変更を検出するときに、次のような方法を使用します。

- Syslog メッセージ
- AAA ログの読み取り
- 内部プロキシ

NCM は、これらの方法から得られるさまざまな入力情報を使用して、デバイスの変更を実際に行ったユーザを特定します。この情報により、変更を行った可能性が最も高いユーザが特定されます。優先度順に、次の情報が使用されます。

- デバイスで実行されたパスワード変更をスケジュールしたユーザ
- デバイスで実行されたソフトウェア アップデートをスケジュールしたユーザ
- デバイスに設定を展開したユーザ
- デバイスでスクリプトを実行したユーザ

- NCM のプロキシを介してデバイスに接続したユーザ
- AAA ログから収集されたユーザ情報
- syslog メッセージから解析されたユーザ情報

NCM は、優先度リストで上位にあるデバイス インタラクションに変更属性を割り当てます。たとえば、あるユーザがパスワード変更をスケジュールし、別のユーザが同じ期間にデバイスにプロキシした場合、変更が検出されたときは、その変更はパスワード変更をスケジュールしたユーザに割り当てられます。

デバイスの設定変更を表示するには、次の手順を実行します。

1. Devices の下のメニューバーで、Inventory をクリックします。現在管理されているすべてのデバイスのリストが開きます。
2. 設定変更を表示するデバイスをクリックします。Device Details ページが開きます。
3. View ドロップダウン メニューから、Configuration Changes をクリックします。
4. User Name カラムで、詳細リンクをクリックします。User Attribution Details ページが開きます。

User Attribution Details ページのフィールド

フィールド	説明 / アクション
Change Event Detail	
User	変更を行ったユーザの名前が表示されます。
Date	変更が行われた日付が表示されます。
Device Interaction	変更を検出するときに使用する方法が表示されます（たとえば、Syslog）。
Additional Details	変更に関する詳細が表示されます（たとえば、変更がコンソールから行われたかどうか）。

タスク前およびタスク後のスナップショットの設定

タスク前およびタスク後のスナップショットを設定すると、次の操作が可能になります。

- さまざまなタスクのタイプに応じた、タスク前およびタスク後のスナップショットの動作を定義する。
- タスク後のスナップショットを別個のタスクとして実行する。
- 特定のタスクを実行するときに、タスク前およびタスク後のスナップショットのデフォルト動作を上書きする。

タスク前およびタスク後のスナップショットのオプションは、次のタスクに対して表示できます。

- Deploy Config（P.172 の「Deploy Config Task ページのフィールド」を参照）
- Run Diagnostics（P.254 の「Run Diagnostics Task ページのフィールド」を参照）
- Delete ACL（P.589 の「Delete ACLs タスクのページ」を参照）
- Synchronized Startup and Running（P.261 の「Synchronize Startup and Running Task ページのフィールド」を参照）
- Run Command Script（P.249 の「Run Command Script Task ページのフィールド」を参照）

コマンド スクリプト内にスナップショットのヒントを含める場合は、コマンド スクリプトに特殊なタグを追加して、そのスクリプトを実行したときの、タスク前およびタスク後のスナップショットの動作を指定します。たとえば、デバイスへの接続または修正を実際には行わない、高度なスクリプトがあるとします。この高度なスクリプトは、NCM API だけを使用してデバイスに関する情報を抽出し、レポートを生成します。この場合は、タスクの実行後にスナップショットを取得する必要がありません。そのため、この高度なスクリプトには、タスク後のスナップショットが不要であることを示すタグを含めることができます。

デバイス グループに対して実行するスクリプトが複数選択されている場合、そのうちの複数のスクリプトにヒントが含まれているときは、指定された動作の中で最も安全な動作が使用されることに留意してください。

Device Access

Device Access ページでは、次の操作を実行できます。

- デバイス接続方式を指定する。
- Detect Network Devices タスクの設定を構成する。
- 要塞ホストの設定を構成する。
- SecurID デバイス アクセスを設定する。
- デバイスへのアクセスに使用するクレデンシャルを、タスクごとに指定する。
- Nortel BayRS MIB/OS バージョンを指定する。
- ゲートウェイ メッシュの情報を入力する。

多くの場合、ネットワーク環境はネットワーク ファイアウォールで保護されています。NCM には、ファイアウォールを介してデバイスにアクセスする方法として、次の 3 つが用意されています。

- ファイアウォールを介したダイレクト アクセスを開始する。
- ファイアウォール上に Network Address Translation（NAT; ネットワーク アドレス変換）を作成し、NAT を使用してデバイスにアクセスするように NCM を設定する。NAT アドレスは、NAT を使用するデバイスのデバイス設定には表示されないことに留意してください。
- ファイアウォールの外側にある既存の要塞ホストを使用して管理要求をプロキシするように、NCM を設定する。要塞ホストでは、ファイアウォールを介したアクセスがすでに許可されているため、要塞ホストの設定を使用すると、要塞ホストのプロキシ接続を介してデバイスを管理できます。

コンソール サーバでは、シリアル リンクを使用した、デバイスへの物理接続が保持されることに留意してください。このリンクは、Telnet を介して、コンソール サーバをホストとした特定の IP ポート番号に接続されています。コンソール サーバの接続は、ネットワーク デバイスがネットワークから切断された場合でも使用できます。

Device Access ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、Device Access をクリックします。Device Access ページが開きます。

Device Access ページのフィールド

フィールド	説明 / アクション
Device Connection Methods	
Password Selection	次のいずれかのオプションを選択します。 • Always try last successful passwords first : オンの場合（デフォルト）、NCM は、デバイスへの前回のアクセスで最後に成功したパスワードを最初に試行します。このパスワードはデータベースに格納されていますが、デバイスへの次回のアクセスでは最初に試行されない可能性もあることに留意してください。その場合は、「最後に使用された規則の変更」イベントが継続的に生成されます。したがって、デバイスが所定のパスワード規則を使用しているかどうかを確認できます。 • Always try passwords in defined order : オンの場合、NCM は、定義された順序でパスワードを常に試行します。NCM では、デバイスとの次回の通信用に、最後に使用された認証クレデンシャルが記録されることに留意してください。このため、デバイス パスワード規則を利用しながら、デバイスへの接続の試行回数を最小限に抑えることができます。詳細については、P.131 の「デバイス パスワード規則の作成」を参照してください。
Default Connection Methods	デバイスへの接続には、次の方式が使用されます。New Device ページおよび Add Device Wizard では、これらの方式はデフォルトでオンになっています。次のオプションを 1 つ以上オンにします。 • Telnet • SSH • SNMP • SCP • FTP • TFTP **注** : NCM は統合 TFTP サーバを備えているため、通常は、SNMP または CLI を介してデバイスにアクセスし、このサーバとの間の転送を設定します。独自の TFTP サーバを備えたデバイスに対しては、NCM は TFTP クライアントとして動作します。一般に、SCP は CLI で使用する必要があります。SCP の場合は、デバイスが SSH を使用できることが条件となります。デバイスが SSH サーバを実行していない場合、SCP は実行できません。

フィールド	説明 / アクション
Bad Login Attempt Delay	不適切なログインが試行された後で、デバイスが回復できるようにするための遅延時間を秒単位で入力します。デフォルトは 5 秒です。
SNMP Timeout	一連の SNMP コマンド（設定のロードなど）をデバイスが動作するまで待機する遅延時間を秒単位で入力します。デフォルトは 40 秒です。
Detect Network Devices Task Settings	
Path to Nmap utility	ネットワーク デバイスをスキャンするための Nmap ユーティリティへのパスを入力します（**注**：Nmap を使用すると、ネットワークをスキャンして、動作中のホストと、そのホストが提供するサービスを特定することができます。Nmap の詳細については、www.Insecure.Org を参照してください）。
Max Addresses to Discover Per Task	検出する IP アドレスの数を入力します。ネットワーク トラフィックを軽減するため、必ず、Detect Network Devices タスクでスキャンするアドレス数を、アドレスの最大数（1,024）までに制限してください。
Max SNMP Scanner Threads	SNMP スキャン方式を使用したデバイス検出の実行中に Detect Network Devices タスクが生成する SNMP スキャナ スレッドの最大数を入力します。デフォルトは 79 です。理論上、SNMP スキャナ スレッドの最大数を大きくすると、タスクの実行速度は上がります。ただし、SNMP スキャナ スレッドが多すぎると、各 SNMP スキャナ スレッドで必要になる CPU オーバーヘッドおよびネットワーク トラフィックが増えるため、システム パフォーマンスに影響を及ぼす場合があります（**注**：Detect Network Devices タスクを設定するときは、SNMP を使用してデバイスを検出するオプションを使用できます。結果として、タスクを実行すると、SNMP を介してデバイスと通信する SNMP スキャナ スレッドが多数生成されます。他のスキャン方式については、P.272 の「Detect Network Devices Task ページのフィールド」を参照してください）。
Network Discovery IP or CIDR Range Exclusions	除外する IP アドレスまたは Classless Inter-Domain Routing（CIDR; クラスレス ドメイン間ルーティング）範囲（たとえば、192.168.1.0-192.168.2.0 または 192.168.31.0/24）を右側のボックスに入力し、Add Pattern << ボタンをクリックします。範囲は、両端の値を含みます。パターンを削除するには、左側のボックスでパターンを選択し、Delete Pattern ボタンをクリックします。
SNMP Timeout	各 SNMP SysOID プローブの SNMP タイムアウト値をミリ秒単位で入力します。デフォルトは 500ms です。

フィールド	説明 / アクション
Bastion Host Settings	
Use Bastion Host by Default	オンの場合、新しいデバイスは、Telnet および SSH アクセス用に要塞ホストを使用します（**注**：要塞ホストの設定は、デバイスごとに上書きできます）。
Default Bastion Host	Telnet アクセスと SSH アクセスに使用する要塞ホストのホスト名または IP アドレスを入力します。
Default Bastion Host Username	Telnet アクセスと SSH アクセスに使用する要塞ホストのユーザ名を入力します。
Default Bastion Host Password	Telnet アクセスと SSH アクセスに使用する要塞ホストのパスワードを入力します。
SecurID Device Access	
SecurID License Usage	次のいずれかのオプションを選択します。 • Use Unique Tokens Per User：オンの場合（デフォルト）、各デバイス アクセスは、タスクまたは Telnet/SSH プロキシ接続を開始したユーザに対応するシード（複数可）だけを使用します。 • Use Software Token Pool：オンの場合、汎用のソフトウェア トークン シードのプールが使用されます。その際は、パフォーマンスが最大になるよう、できるだけ効率的に使用されます。SecurID ソフトウェア トークンのプールを関連付けるユーザ名を入力します。 ユーザごとに一意のソフトウェア トークンを使用すると、より多くのトークンが必要になるため、トークンのメンテナンス作業が増えます。共通ユーザに関連付けられたプールからソフトウェア トークンを使用すると、必要なトークンの数が少なくなるため、タスクのスループットが向上する可能性があります。
Max Software Tokens	NCM を実行するマシンにインポートするソフトウェア トークン ライセンスの最大数を入力します。デフォルトは 1,024 です。
Passcode Lifetime	ソフトウェア トークン パスコードのライフタイムを入力します。デフォルトは 60 秒です。

フィールド	説明 / アクション
Task Credentials	
Allow Standard Device Credentials	次のタスクのうち 1 つ以上を選択します。デフォルトでは、すべてのタスクが選択されています。 • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reload Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software 上記のタスクを使用すると、ユーザは、デバイス固有のパスワードとネットワーク全体のパスワード規則に関する標準処理を選択できます。タスクごとのクレデンシャルについては、P.70 の「タスクごとのクレデンシャル」を参照してください。パスワード規則については、P.131 の「デバイス パスワード規則の作成」を参照してください。

フィールド	説明 / アクション
Allow Per-Task Device Credentials	次のタスクのうち 1 つ以上を選択します。 • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reload Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software オンの場合、上記のタスクを使用すると、ユーザはそのタスク固有のワンタイム デバイス クレデンシャルを入力するように求められます。タスクごとのクレデンシャルについては、P.70 の「タスクごとのクレデンシャル」を参照してください。

フィールド	説明 / アクション
Allow User AAA Credentials	次のタスクのうち 1 つ以上を選択します。 • Configure Syslog • Delete ACLs • Deploy Configuration File • Discover Driver • Deploy Passwords • Reload Device • Run Command Script • Run Diagnostics • Run ICMP Test • Synchronize Startup and Running • Take Snapshot • Update Device Software オンの場合、上記のタスクを使用すると、ユーザは、タスクの実行時に使用するタスク オーナーの AAA クレデンシャルを選択できます（**注**：ユーザは有効な AAA クレデンシャルを定義しておく必要があります）。タスクごとのクレデンシャルについては、P.70 の「タスクごとのクレデンシャル」を参照してください。
Nortel Discovery	
Nortel BayRS MIB/OS Versions	BayRS ドライバを検出する追加の BayRS MIB バージョン / リビジョンのリストが表示されます。縦棒で区切られた一連の <MIB バージョン>/<リビジョン> を使用します（たとえば、14.00/1D12|14.20/）。
Gateway Mesh	
Local Gateway Hostname	NCM Core と同じレルムにあるゲートウェイ システムのホスト名または IP アドレス、およびポートを入力します（たとえば、`gw-vlan10:3001`）。ゲートウェイ メッシュについては、P.145 の「オーバーラップする IP ネットワーク」を参照してください。
Local Gateway Proxy Port	NCM Core と同じレルムにあるゲートウェイ システムのポート名を入力します（たとえば、`gw-vlan10:3001`）。デフォルトは 3002 です。
Local Gateway Admin Port	ローカル レルムにあるゲートウェイの Admin ポート番号を入力します。この番号は、ゲートウェイ メッシュからレルム名を取得するときに使用されます。デフォルトは 9090 です。

フィールド	説明 / アクション
Gateway Admin Private Key Filename	Admin ポートへの接続に必要なゲートウェイの秘密鍵のファイル名を入力します。このファイル名は、絶対パスでも相対パスでもかまいません。相対パスの基準は、NCM インストール ツリーのルートです（通常は *C:\Rendition*）。ゲートウェイの秘密鍵は、ゲートウェイのインストール時に作成されることに留意してください。
Gateway Mesh Delay	ゲートウェイ メッシュを介してリモート レルムに到達するときの遅延時間を秒単位で入力します。デフォルトは 5 秒です。この値は、リモート デバイスとの通信時に使用されるタイムアウトに追加されます。

Save をクリックして、変更を保存してください。

タスクごとのクレデンシャル

タスクごとのクレデンシャルを設定すると、デバイスにアクセスするタスクに対応した一意のクレデンシャルを指定することで、デバイスへのアクセスに使用されるクレデンシャルを指定できます。次の作業を実行できます。

- タスク オーナーの AAA クレデンシャルを使用して、タスクを実行する。
- タスクの作成時に指定したワンタイム クレデンシャルを使用して、タスクを実行する。
- タスクのタイプごとに要求するクレデンシャルのタイプを設定する。

一般に、セキュアな環境では、CiscoSecure ACS TACACS+ サーバなどの AAA サーバが実装されている場合があります。このサーバは、各ユーザが各デバイスで実行できるコマンドを制限します。

たとえば、ユーザ A とユーザ B の両方が、権限のある特定のコマンドを使用してコマンド スクリプトを実行できるとします。NCM を実装したら、ユーザ A とユーザ B の両方がコマンド スクリプトを実行できるようにする必要があります。ただし、ユーザ A とユーザ B の両方が権限のあるコマンドだけを実行するためのクレデンシャルを保持していることを確認する必要があります。

したがって、タスクごとのクレデンシャルを使用すると、ユーザ A とユーザ B の新しいスタティック NCM アカウントにコマンド スクリプトの実行権限を設定する必要がなくなります。各ユーザは、それぞれの現在の権限でコマンド スクリプトを実行できます。ユーザ A とユーザ B のどちらかが権限のないコマンドを使用した場合、NCM はエラーを返します。

AAA クレデンシャルを使用する場合、NCM は次の処理を行います。

- 最後に成功したクレデンシャル、デバイス固有のクレデンシャル、パスワード規則、およびデバイスのアーカイブ済みパスワードなど、標準のクレデンシャル処理をすべて試行します。
- 試行するたびに、NCM はユーザ名とパスワードを、タスク オーナーの AAA ユーザ名とパスワードに置き換えます。試行が失敗した場合、NCM は、ユーザの AAA パスワードを実行パスワードとイネーブル パスワードの両方として使用し、再度試行します。AAA ログインの試行がすべて失敗した場合、タスクは失敗します。

（注）.RCX ファイルで設定できる proxy/auth_fallback_for_aaa_task という非表示の設定があります。true に設定した場合、NCM はフォールバックして、標準のパスワード処理を試行します。

ワンタイム クレデンシャルを設定する場合、NCM は、指定されたタイプのクレデンシャル処理を、そのタスク タイプに基づいて使用します。たとえば、スナップショット タスクに AAA クレデンシャルだけが許可されている場合は、すべてのスナップショット タスクが AAA クレデンシャルを使用します。特定のタスク タイプに複数のクレデンシャル タイプが許可されている場合は、ユーザがどのタイプを使用するかを選択します。

特定のタスクがワンタイム クレデンシャルを使用するように選択されている場合、NCM は、そのタスクの作成時にユーザが指定したクレデンシャルをそのまま使用します。ワンタイム クレデンシャルが失敗した場合、タスクは失敗します。

（注）ワンタイム クレデンシャルが成功しても、NCM は、デバイスに関する最後に成功したクレデンシャルの情報を更新しません。

Server

Server ページでは、次の操作を実行できます。

- CiscoWorks サーバにログインする。
- TFTP および SMTP サーバを指定する。
- NCM タスクの制限を設定する。
- Syslog を設定する。
- デバイス インポートの間隔を設定する。
- ドメインの名前解決を設定する。
- プライマリ IP アドレスの再割り当てと二重化の設定を構成する。
- Resolve FDQN タスク。
- 監査ログをイネーブルにする。
- データベース プルーニングを設定する。
- Advanced Scripting 機能を設定する。
- サーバ パフォーマンスの調整を設定する。

Server ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、Server をクリックします。Server ページが開きます。

Server ページのフィールド

フィールド	説明 / アクション
Servers	
CiscoWorks Server URL	CiscoWorks サーバの URL（たとえば、*http://ciscoworks:1741*）を入力します（**注**：CiscoWorks Device Center オプションと CiscoView オプションを Device Details View メニューに表示する（その後で、My Workspace タブの「My Favorites」セクションに表示する）場合は、CiscoWorks サーバの URL を入力する必要があります）。
TFTP Server IP	NCM が使用する TFTP サーバの IP アドレスを入力します（デフォルトでは、NCM サーバそのものが入力されています）。
TFTP File Path	TFTP サーバが設定ファイルを書き込むパスおよびフォルダを入力します。NCM では、このフォルダに対する読み取り / 書き込み権限が必要になります。デフォルトは、*C:\< インストール ディレクトリ >\server\ext\tftp\tftpdroot* です。

フィールド	説明 / アクション
SMTP Server	NCM が電子メール通知の送信に使用する SMTP サーバのホスト名または IP アドレスを入力します。
SMTP From Address	NCM が電子メールに使用する送信元アドレスを入力します。
Tasks	
Max Concurrent Tasks	同時に実行可能なタスクの最大数を入力します。NCM は、同時タスクを制限することで、ネットワーク パフォーマンスの低下を防止します。デフォルトは 20 です。データベース接続プール内のデータベース接続の数には制限があることに留意してください。同時タスクの最大数は、必ず 50 以下に設定しなければなりません。
Max Concurrent Group Tasks	同時に実行可能なグループ タスクの最大数を入力します。グループ タスクには、デバイス インベントリに対して実行されるスナップショットなどがあります。グループ タスクでは、子タスク（グループ内のデバイスごとに 1 つのタスク）がスケジュールされます。Max Concurrent Group Tasks 設定は、同時に実行可能な子タスクの数を制限します。NCM は、同時子タスクの数を制限することで、システムおよびネットワーク パフォーマンスの低下を防止します。同時子タスクの数のデフォルトは 15 です。 **注**：Max Concurrent Group Tasks の値を Max Concurrent Tasks の値よりも小さく設定すると、大規模なグループ操作の実行中に、NCM が時間依存型の独立したタスクを確実に実行できるようになります。たとえば、大規模なグループ全体のパスワード変更タスクの実行中でも、NCM は、リアルタイム変更検出によってトリガーされるスナップショット タスクをただちに実行します。
Max Task Length	タスクが停止して Failed ステータスになるまでそのタスクを実行できる最大時間を入力します。デフォルトは 3,600 秒（1 時間）です。
Syslog Configuration	
Configure Syslog by Default	オンの場合、NCM は新しいデバイスに対する Syslog 変更の検出を自動的に設定します。
Default Syslog Relay	新しいデバイスに対するリレー ホストのデフォルトのホスト名または IP アドレスを入力します。

フィールド	説明 / アクション
Device Import	
Overwrite Existing Devices	次のいずれかのオプションを選択します。 • Yes：NCM は NCM データベースに格納されている既存のデバイスデータを、インポートしたデータで上書きします（デフォルト）。インポートに含まれていないデバイスは影響を受けません。 • No：NCM は NCM データベースに格納されている既存のデバイスデータを、インポートしたデータで上書きしません。
Missing Device Interval	インポート元から欠落している期間がこの間隔を超えたデバイスを、削除するか、非アクティブのマークを付けるか、または変更しないでそのままにします（Missing/Inaccessible Device Action の設定に基づく）。デフォルトは 45 日です。
Inaccessible Device Interval	この間隔中に NCM からアクセスできなかったデバイスを、削除するか、非アクティブにするか、または変更しないでそのままにします（Missing/Inaccessible Device Action の設定に基づく）。デフォルトは 45 日です。
Missing/Inaccessible Device Action	次のいずれかのオプションを選択します。 • Delete device：欠落している、またはアクセス不能のデバイスを、データベースから削除します。 • Mark device inactive：欠落している、またはアクセス不能のデバイスに、非アクティブのマークを付けます（デフォルト）。通常は、デバイスをデータベースから削除するのではなく、非アクティブに変更して設定履歴を保持することをお勧めします。 • No action：欠落している、またはアクセス不能のデバイスに対して、何のアクションも行いません。
Primary IP Reassignment and Deduplication Settings	
Primary IP Address Reassignment	オンの場合、NCM は、プライマリ IP アドレスなど、デバイスに関連付けられたすべての IP アドレス（およびデバイスに関連付けられた他のすべてのインターフェイス）を調べ、RegEx または他の規則（指定された場合）に一致するプライマリ IP アドレスを設定します。
Interface Name Reassignment RegEx Patterns	右側のボックスに Regular Expression（RegEx; 正規表現）パターンを入力し、Add Pattern << ボタンをクリックします。正規表現は、IP アドレスが準拠する必要のあるインターフェイス名（たとえば、Loopback.*）を指定する特殊なテキスト文字列です。パターンを削除するには、左側のボックスでパターンを選択し、Delete Pattern ボタンをクリックします。

フィールド	説明 / アクション
IP Address Reassignment RegEx Patterns	右側のボックスに正規表現（RegEx）パターンを入力し、Add Pattern << ボタンをクリックします。正規表現は、使用可能なインターフェイス上の IP アドレスと一致する特殊なテキスト文字列です（たとえば、10\.1\..*）。パターンを削除するには、左側のボックスでパターンを選択し、Delete Pattern ボタンをクリックします。
IP Reassignment Order	複数の IP アドレスがインターフェイス名または IP アドレスのパターンと一致した場合の処理として、次のどちらかを選択します。 • Lowest IP address to assign as the primary IP address（デフォルト） • Highest IP address to assign as the primary IP address
Duplication Detection	重複が検出された場合のデバイスに対するオプションとして、次のいずれかを選択します。**注**：複数のデバイスが同一のインターフェイスおよび IP アドレスの情報を持っている場合、それらのデバイスは重複と見なされます。 • Leave Duplicates • Deactivate Duplicates（デフォルト） • Delete Duplicates
Domain Name Resolution	
Overwrite Existing Domain Names	オンの場合、Resolve FQDN タスクを実行すると、手動の FQDN エントリが、DNS で解決された FQDN エントリで上書きされます。
Audit Log	
Audit Logging	次のいずれかのオプションを選択します。 • Enabled：NCM はユーザ アクションの監査ログを格納します。ログを表示するには、View Audit Log をクリックします。 • Disabled：NCM はユーザ アクションの監査ログを格納しません（デフォルト）。
Database Pruning	
Configurations	設定をデータベースに保存する日数を入力します。デフォルトは 365 日です。
Diagnostics	診断をデータベースに保存する日数を入力します。デフォルトは 45 日です。
Events	イベントをデータベースに保存する日数を入力します。デフォルトは 45 日です。

フィールド	説明 / アクション
Tasks	タスクをデータベースに保存する日数を入力します。デフォルトは 365 日です。
Sessions	プロキシ Telnet/SSH セッションをデータベースに保存する日数を入力します。デフォルトは 45 日です。
Log files	サーバ ログ ファイルを保存する日数を入力します。デフォルトは 30 日です。
Diagram files	ダイアグラム ファイルを保存する日数を入力します。デフォルトは 1 日です。
Advanced Scripting	
Scripting Language 1	Advanced Scripting を使用すると、ネットワークで使用されているスクリプト言語で記述したカスタム スクリプトを実行できます。言語ごとにランゲージ インタプリタをインストールし、Advanced Scripting 設定を介してそのパスを言語オプションに関連付ける必要があります。 ここで指定したスクリプト言語は、Advanced Scripting オプションがイネーブルのときに、New Command Script ページの選択リストに表示されます。デフォルトでは、この設定は Expect に事前設定されています。この言語のインタプリタへのパスを、このページ上の対応する Path to Interpreter [#] 設定で指定する必要があります。 Advanced Scripting 機能は最大 5 つの言語に対して設定できます。また、事前設定されたデフォルト言語を使用しない場合は、そのデフォルトを上書きできます。サポートされる言語は、コマンドラインから実行されるものだけです（たとえば、JScript や Python）。 **注**: スロット 1 および 2 は Expect および Perl 用に事前設定されています。ただし、NCM でインストールされるインタプリタは Expect 専用です。ここで指定する言語ごとにインタプリタをインストールし、そのパスを設定してから、その言語で記述されたスクリプトを実行する必要があります。
Path to Interpreter 1	Scripting Language 1 で指定した言語を実行するインタプリタへのパスを入力します。

フィールド	説明 / アクション
Scripting Language [2-5]	スクリプト言語を入力します。ここで指定した言語は、Advanced Scripting オプションがイネーブルのときに、New Command Script ページの Language 選択リストに表示されます。この言語のインタプリタへのパスを、対応する Path to Interpreter [#] 設定で指定する必要があります。 **注**：デフォルトでは、Scripting Language 2 は Perl 用に事前設定されています。ただし、この設定を機能させるには、Perl インタプリタをインストールする必要があります。
Path to Interpreter [2-5]	関連する Scripting Language [#] ボックスで指定した言語を実行するインタプリタへのパスを入力します。 **注**：Windows 環境の場合、デフォルトでは、Path to Interpreter 2 は Perl 用に設定されています。ただし、NCM では Perl インタプリタはインストールされません。この設定を機能させるには、Perl をインストールし、パスを設定する必要があります。
Performance Tuning	
イベントのリストについては、P.345 の「はじめに」を参照してください。	フィルタリングする各イベントのチェックボックスをクリックします。この操作により、システムのパフォーマンスを調整できます。

Save をクリックして、変更を保存してください。

Workflow

Workflow ページでは、次の操作を実行できます。

- ワークフローをイネーブルにする。
- イベント通知および応答規則を設定する。
- Device Reservation System を設定する。
- Telnet/SSH プロキシのデバイス予約を設定する。

Workflow ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、Workflow をクリックします。Workflow ページが開きます。

Workflow ページのフィールド

フィールド	説明 / アクション
Workflow	
Enable Workflow	オンの場合、承認規則を定義したタスクに対して承認が要求されます。
Priority Values	承認を必要とするタスクに設定できる優先度の値を定義します。デフォルト値には、次のものがあります。 • Low • Medium • High 別の値（Urgent や Normal など）を追加するには、その値を入力して Add Value << ボタンをクリックします。値を削除するには、値を選択して Delete Value ボタンをクリックします。 **注**：NCM Scheduler は、この値を参照しません。この値は基本的に、承認をすぐに必要とするタスクを判断するための視覚的なキューです。
Event Notification & Response Rules	
Run Task	オンの場合（デフォルト）、イベント規則によってスケジュールされたタスクはすべて承認されるようになります。たとえば、設定ポリシーに違反したイベントが発生した結果、適切な対応策のタスクがトリガーされた場合、そのタスクは展開前に承認されます。

フィールド	説明 / アクション
Device Reservation System	
Device Reservation System	次のいずれかのオプションを選択します。 • Enabled：Device Reservation System をイネーブルにします（デフォルト）。Device Reservation System については、P.183 の「デバイスの予約」を参照してください。 • Disabled：Device Reservation System をディセーブルにします。
Default Duration	デバイスとデバイス グループを予約状態にできる時間を分単位で入力します。デフォルトは 60 分です。
Max Number of Columns in Activity Calendar	Activity Calendar 内のカラムの最大数を設定します。デフォルト値は 1,024 です。Activity Calendar については、P.183 の「Activity Calendar」を参照してください。
Minimum Overlap for Half-Hour	Activity Calendar 上で、特定の時間の予約を 30 分単位の境界線から延長して表示する最小時間を分単位で設定します。デフォルト値は 5 分です。
Telnet/SSH Proxy Reservation	
Device Reservations for Telnet/SSH Proxy	NCM Telnet/SSH プロキシは、デバイスへのアクセスおよびデバイスの設定に使用できます。このプロキシには、アクセス コントロール機能、キーストローク セッション ロギング機能、およびインライン コメント機能があります。次のいずれかのオプションを選択します。 • Ignore：Telnet/SSH プロキシを介してデバイスにアクセスするときは、デバイス予約を無視します（デフォルト）。Device Reservation System については、P.183 の「デバイスの予約」を参照してください。 • Warn：Telnet/SHH プロキシを介してデバイスに接続するときに、承認されたデバイス予約が存在しない場合は、ユーザに警告します。 • Prevent：承認されたデバイス予約が存在しない場合は、ユーザが Telnet/SHH プロキシを介してデバイスに接続できないようにします。ユーザが無効化権限を持っている場合は、デバイスへのアクセス禁止を無効にするかどうかを尋ねられます。 Warn または Prevent が選択されている場合、NCM は、ユーザ、デバイスまたはデバイス グループ、承認されているかどうか、およびマルチタスク プロジェクト用の予約時間など、条件に一致するデバイス予約を検索します。
No Device Reservation Warning Message	承認されたデバイス予約が存在しないときに表示する警告メッセージを入力します。デフォルトの警告メッセージは、*WARNING: You do not have an approved reservation for this device at this time* です。デフォルトの警告メッセージを削除するオプションを使用できます。

User Interface

User Interface ページでは、次の操作を実行できます。

- ログイン セキュリティを設定する。
- すべてのページに表示される日付の形式を設定する。
- NCM メニューをカスタマイズする。
- View/Edit Modules ページのスロットを追加する。
- New/Edit Templates ページのロールを追加および削除する。
- Edit Command Script ページと Edit Diagnostics ページのテキスト ボックスのサイズをカスタマイズする。
- Device Selector の表示をカスタマイズする。
- 拡張されたカスタム フィールドをイネーブルにする。

User Interface ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、User Interface をクリックします。User Interface 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。

User Interface ページのフィールド

フィールド	説明 / アクション
Security	
Session Timeout	非アクティブな Web セッションを終了するまで NCM が待機する時間を秒単位で入力します。デフォルトは 1800 秒です。変更が有効になるのは、次回のログイン後であることに留意してください。
Check Device Permissions for View Device Configuration	オンの場合、ユーザがデバイス設定を表示できるのは、適切なデバイス権限を持っている場合に限られます。変更を有効にするには、NCM を再起動する必要があります。
Auto-complete user name and password	オンの場合、NCM ログイン ページで、ブラウザの自動補完機能がイネーブルになります。
Cross site scripting check	オンの場合、NCM はユーザ入力を確認して、<script>、<object>、<img>、<input> など、潜在的なクロス サイト スクリプティングの要素を除去します。つまり、このオプションを使用すると、スクリプトから潜在的に悪意のある Javascript コードを削除できます。悪意のある Javascript コードが見つかった場合は、エラーが返されます。

フィールド	説明 / アクション
Date/Time Display	
Date Format	この設定は、Web インターフェイス全体に表示される日付の形式を制御します。デフォルトの形式は、MMM-dd-yy HH:mm:ss です。日付と時刻の要素の順序を変更すること、日付と時刻を入れ替えること、4 桁の年数（yyyy）を入力すること、および月を 2 桁の数値（MM）に変更することが可能です。要素は大文字と小文字が区別されることに留意してください。たとえば、HH は 24 時間制を表し、hh は 12 時間制を表します。
Menu Customization	
Show Summary Reports	オンの場合（デフォルト）、Excel 形式の Summary レポートへのリンクが表示されます。Summary レポートには、システムの使用状況に関する動向データと長期データが Microsoft Excel 形式で含まれています。
Show Custom Menu Link	オンの場合、About オプションの上にユーザ定義の名前が表示されます。チケット アプリケーションのホーム ページなど、特定の HTML ページのメニュー タイトルとリンクを入力します。
Custom Menu Title	表示する名前を入力します。
Custom Menu Page	Show Custom Menu Link を選択した場合は、ユーザがメニュー タイトルをクリックしたときに表示する HTML ページの URL を入力します。このページは、別の HTML アプリケーション内のページでもかまいません。
Configuration Comparison	
Lines of Context for Visual Comparison	2 つの設定を比較するときに各変更の上下に表示する行数を入力します。デフォルトは 3 です。
Lines of Context for Email Comparison	2 つの設定を電子メールのテキストとして比較するときに各変更の上下に表示する行数を入力します。デフォルトは 3 です。
Software Center	
Slots	View/Edit Modules ページに表示されるスロット（カード / ブレード / モジュール用のシャーシ スロット）を追加および削除します。スロットを追加するには、右側のボックスにスロットを入力し、Add Slot << をクリックします。スロットを削除するには、左側のボックスでスロットを選択し、Delete Slot をクリックします。

フィールド	説明 / アクション
Templates	
Template Roles	テンプレートの作成者が New/Edit Template ページで選択するロールを追加および削除します。ロールは、デバイスがネットワークで果たす役割を表すことができます（Border や Core など）。ロールを追加するには、右側のボックスにロールを入力し、Add Role << をクリックします。ロールを削除するには、左側のボックスでロールを選択し、Delete Role をクリックします。
Scripts	
Script Text Height	Edit Command Script ページと Edit Diagnostics ページのテキスト ボックスのサイズ（高さ）を入力します。デフォルトは 12 行です。
Script Text Width	Edit Command Script ページと Edit Diagnostics ページのテキスト ボックスのサイズ（幅）を入力します。デフォルトは 60 文字です。
Device Selector	
Device Selector Maximum Count	Device Selector にロードするデバイスの最大数を入力します。デフォルトは 10,000 です。
Device Selector Maximum Devices Per Page	Device Selector の各ページに表示する項目の数を入力します。デフォルトは 100 です。この数を増やすと、Device Selector の感度に影響を及ぼす場合があります。
Device Selector Initial View	次のいずれかのオプションを選択します。 • All Device Groups（デフォルト） • All Devices
Enhanced Custom Fields	
Enable Enhanced Custom Fields	オンの場合、特定のデータ セット用に拡張されたカスタム フィールドを設定できます。カスタム データ フィールドを使用すると、特定のデバイス、設定、およびユーザなどに有用なデータを割り当てることができます。詳細については、P.430 の「Custom Data Setup ページのフィールド」を参照してください。
Miscellaneous	
Task Page Refresh Interval	Task List ページをリフレッシュする間隔を秒単位で入力します。デフォルトは 60 秒です。

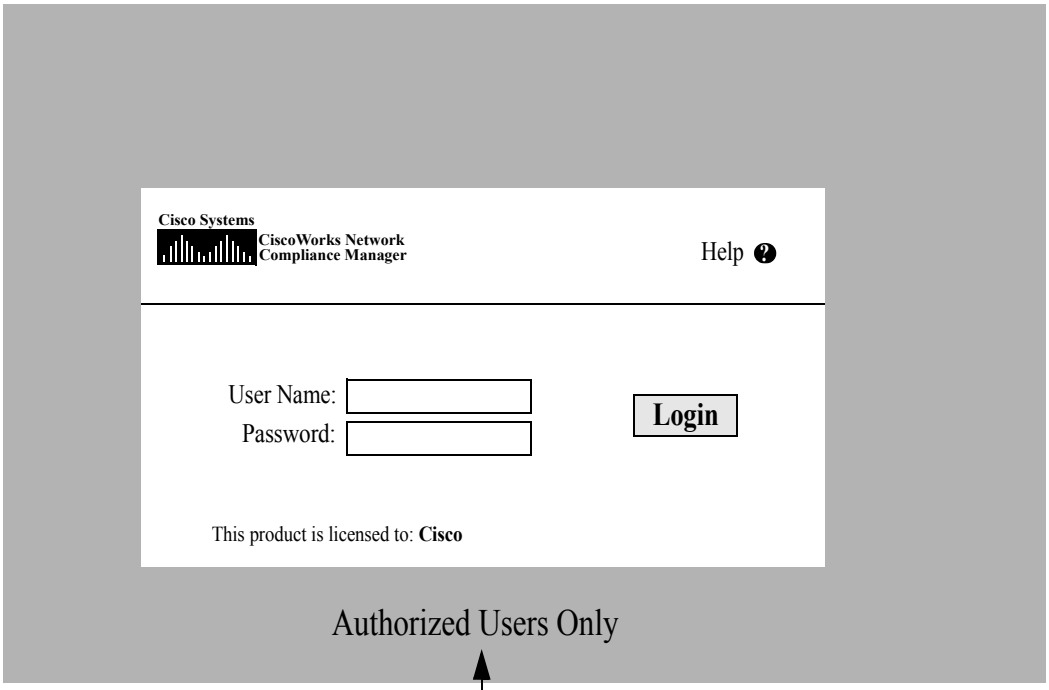
フィールド	説明 / アクション
Config Size Threshold for Displaying as Plain Text	設定を平文形式で表示する場合の設定サイズのしきい値を入力します。デフォルトは 1,000,000 バイトです。一部の設定はサイズが大きすぎるため、行の番号付けなどの特殊な処理を行うと、サーバとブラウザのリソースを大量に消費することに留意してください。設定サイズがデフォルト値を超えている場合、その設定は <pre> タグと </pre> タグを使用して平文形式で表示されます。
Mask Community Strings	オンの場合、コミュニティ ストリングはマスクされます。
Disable hidden stack trace output	オンの場合、非表示のスタック トレースがディセーブルになります。オフの場合、サーバ エラーが発生したときは、NCM は、サーバ ログだけでなく HTML ページでも、スタック トレースを非表示のテキストとして出力します。 **注**：完全な Java スタック トレースは、デフォルトで非表示の HTML として出力されるため、サポート コールで役に立ちます。非表示が潜在的なセキュリティの脆弱性になると思われる場合は、このオプションをオンにしてください。

NCM ログイン ページのカスタマイズ

NCM ログイン ページをカスタマイズして、警告メッセージや企業固有の情報などを表示することができます。

Cisco Login ページをカスタマイズするには、次の手順を実行します。

1. *$NCM_install_dir/resource* ディレクトリで、*customer_banner.html* ファイルを開きます。ファイルが存在しない場合は、この名前のファイルを作成します（注 : *resource* ディレクトリを作成する必要もあります）。
2. このファイルをテキスト エディタ（HTML 対応）で開き、Cisco Login ページに表示するテキストを入力します。
3. ファイルを保存し、NCM にログインします。テキストが Login ボックスの下に表示されます。表示できるワード数に制限はありません。ただし、テキストがページ上で適切に表示されていることを確認する必要があります。次に、サンプルのログイン ページを示します。


Cisco Systems
CiscoWorks Network
Compliance Manager
Help
User Name:
Password:
Login
This product is licensed to: Cisco
Authorized Users Only

カスタム バナー

Telnet/SSH

Telnet/SSH ページでは、次の設定が可能です。

- Telnet/SSH ロギング
- Telnet/SSH プロキシ
- Telnet クライアント
- Telnet サーバ
- SSH サーバ
- デバイスのシングル サインオン

Telnet/SSH ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、Telnet/SSH をクリックします。Telnet/SSH ページが開きます。

デバイスと対話するすべてのタスクは、セッション ロギングをイネーブルにして実行できることに留意してください。このため、タスクで行われたデバイスとの対話の詳細なログを入手することができます。デバイス固有の問題をデバッグするとき、最初のステップとしてセッション ログを参照します。セッション ログには、タスクで実行された CLI、SNMP、およびすべての転送プロトコルの処理の詳細が含まれています。

Telnet/SSH ページのフィールド

フィールド	説明 / アクション
Telnet/SSH Session Logging	
Log Commands	オンの場合、Telnet または SSH セッションの実行中にコマンドが保存されます。コマンドを表示するには、Device Information ページで、View Telnet/SSH Sessions をクリックし、View Commands Only をクリックします。このページの Convert to Script リンクを使用すると、セッションのコマンドをスクリプトにすばやく取り込み、後で使用することができます。
Log Responses	オンの場合、Telnet または SSH セッションの実行中に完全なセッション ログが保存されます。ログを表示するには、Device Information ページで、View Telnet/SSH Sessions をクリックし、View Full Session をクリックします。このページの Convert to Script リンクを使用すると、セッションのコマンドをスクリプトにすばやく取り込み、後で使用することができます。

フィールド	説明 / アクション
Telnet/SSH Proxy	
Enable Telnet/SSH Server	Telnet/SSH プロキシは、デバイスへのアクセスおよびデバイスの設定に使用できます。このプロキシには、アクセス コントロール機能、キーストローク セッション ロギング機能、およびインライン コメント機能があります。オンの場合（デフォルト）、NCM は Telnet/SSH サーバとして動作できます。
Server Inactivity Timeout	NCM Telnet/SSH サーバに接続されているアイドル状態の Telnet または SSH セッションを切断するまでの最大時間を入力します。NCM に接続されている Telnet/SSH クライアントがこの期間にわたって非アクティブであった場合、セッションはタイムアウトします。デフォルトは 30 分です。
Default Connection Method	シングル サインオンを使用しないでデバイスに接続するときの方式として、Telnet または SSH のどちらかを選択します。この接続方式は、Telnet/SSH プロキシの connect コマンドで *-method* オプションが指定されていない場合に使用されます。この方式は、Use Single Sign-on が選択されていない場合または Edit Device ページの Supports リストに同じ接続方式が含まれていない場合には無視されます。 **注**：外部認証に SecurID を使用するように NCM を設定した場合、NCM プロキシに接続するときにシングル サインオン機能はイネーブルになりません。SecurID パスコードを再利用できないため、SecurID クレデンシャルを使用してもう一度認証する必要があります。
Device Inactivity Timeout	NCM がアイドル状態のデバイス セッションを切断するまで開いた状態にしておく時間を分単位で入力します。デフォルトは 30 分です。
SSH Login Timeout	NCM プロキシで「-login」スイッチを使用した SSH ログインのタイムアウト時間を秒単位で入力します。デフォルトは 15 秒です。
Alert for Concurrent Session	次のいずれかのオプションを選択します。 • Warn of Concurrent Sessions：オンの場合（デフォルト）、NCM は、別のユーザがデバイスへの接続を試行したときに警告を発行します。このオプションを使用すると、あるユーザが誤って別のユーザの変更内容を上書きすることを防止できます。警告を無効にできるのは、Admin 権限を持つユーザだけです。これはデフォルトです。 • Prevent Concurrent Sessions：オンの場合、NCM は、すべてのユーザの同時セッションを防止します。 • No Action：オンの場合、NCM は同時セッションを無視します。

フィールド	説明 / アクション
Concurrent Session Handling for Distributed System	次のいずれかのオプションを選択します。 • Allow sessions to non-local devices • Prevent sessions to non-local devices ハイ アベイラビリティ分散処理システムについては、『*High Availability Distributed System Configuration Guide on Oracle for Network Compliance Manager*』を参照してください。
Connect to Unknown Devices	オンの場合（デフォルト）、NCM は、ユーザが管理対象外のデバイスに接続できるようにします。
Max Device Connection List	ワイルドカード検索に基づいてデバイスに接続する場合、一致するデバイスが複数見つかったときに表示するデバイスの最大数を入力します。デフォルトは 20 です。最大数を超えるデバイスが返された場合は、ワイルドカード表現を制限するように求められます。
Device Single Sign-0n	
Use Single Sign-on	オンの場合（デフォルト）、NCM は、自動的にユーザを 1 回認証してから、デバイス変更権限のあるデバイスにログインさせます。 **注**：外部認証に SecurID を使用するように NCM を設定した場合、NCM プロキシに接続するときにシングル サインオン機能はイネーブルになりません。SecurID パスコードを再利用できないため、SecurID クレデンシャルを使用してもう一度認証する必要があります。
Sign-On To Limited Access Mode When No Modify Device Permission	オンの場合、NCM は、ユーザがデバイス変更権限を持っていなくても、制限されたアクセス モード（たとえば、IOS に対する Exec モード）に自動的にログインさせます。
Display Sign-on Banner	オンの場合（デフォルト）、NCM はデバイスへのログイン時に、サインオン バナーが表示されます。
Use AAA Login for Single Sign-on	オンの場合、NCM は AAA ログイン情報を使用します。このオプションは、New/Edit User ページの Use AAA Login for Proxy Interface セクションを参照します。
Use CiscoWorks Network Compliance Manager Login When AAA Login Fails	オンの場合（デフォルト）、AAA ユーザ名とパスワードの情報が無効なときは、NCM ログイン情報が使用されます。

フィールド	説明 / アクション
Telnet Client	
Telnet Client	次のいずれかのオプションを選択します。 • Use NCM's integrated telnet client（デフォルト） • Use standard browser telnet:// URL to NCM’s Telnet proxy • Use standard browser telnet:// URL directly to the indicated device
Telnet Server (changing these setting restarts the Telnet/SHH server)	
Enable Telnet	オンの場合（デフォルト）、NCM は Telnet サーバとして動作します。
Telnet Server Port	NCM がクライアント接続を受け付けるポートを入力します。Windows のデフォルトは 23 です。Unix のデフォルトは 8023 です。
Max Telnet Connections	NCM が同時に受け付ける Telnet クライアント接続の最大数を入力します。デフォルトは 50 です。
SSH Server (changing these setting restarts the Telnet/SHH server)	
Enable SSH	オンの場合（デフォルト）、NCM は SSH サーバとして動作します。
SHH Server Port	NCM がクライアント接続を受け付けるポートを入力します。デフォルトは 22 です。
Max SSH Connections	NCM が同時に受け付ける SSH クライアント接続の最大数を入力します。デフォルトは 50 です。
SSH Fallback Option	
SSH Fallback Order	デバイスへの接続時に試行する SSH バージョンの順序を指定するオプションとして、次のいずれかを選択します。 • SSH v2 then v1（デフォルト） • SSH v1 then v2

Save をクリックして、変更を保存してください。

Reporting

Reporting ページでは、Network Status レポートを組織に応じてカスタマイズできます。レポート カテゴリには、次の 6 つがあります。

- Policy Rule Violations
- Software Compliance Violations
- Startup vs. Running Config Mismatch
- Device Access Failure
- Configuration Change
- Email Report

レポート カテゴリごとに、個別デバイス（およびデバイス グループ）のステータス インジケータを設定できます。設定する際は、リスク レベルの色分けとパラメータの組み合せを使用して、コンプライアンスに違反したデバイスのパーセンテージのしきい値を段階別に指定します。たとえば、外部ネットワーク アクセスとリモート オフィスを制御する境界ルータ グループには、より高いスコアを割り当て、LAN デバイスはデフォルト値のままにすることができます。

ネットワーク内の各イベントの重大度を最もよく反映するように設定すると、問題を特定しやすくなり、設定されたすべてのポリシーに準拠した状態にネットワークを維持することができます。

また、Reporting ページには、ユーザ定義の電子メール通知タスクを介して送信される電子メール レポートの形式および内容に関するオプションや、レポートの保存場所を指定するオプションがあります。さらに、Diagramming パラメータを設定することもできます。Diagramming については、P.471 の「Diagramming ページのフィールド」を参照してください。

（注）違反したデバイスのステータス（リスク レベル）によって、デバイス グループのステータスが決まります。たとえば、1 つの違反デバイスのリスク レベルが黄色に設定された場合、グループ内の 1 つのデバイスが違反し、違反デバイスの数がしきい値に達したときは、デバイス グループのステータスが黄色になります。

Reporting ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、Reporting をクリックします。Reporting ページが開きます。

Reporting ページのフィールド

フィールド	説明 / アクション
Policy Rule Violations	
Device Status Color	デバイス グループ内の 1 つのデバイスが設定ポリシー規則に違反した場合に表示する色を選択します。オプションには、次のものがあります。 • Red（デフォルト） • Yellow • Green
Category Status Color	次のデバイス ステータスの色に対応する、設定ポリシーに違反したデバイスのしきい値パーセンテージを入力します。 • Yellow：デフォルトは 1% です。 • Red：デフォルトは 2% です。
Software Compliance Violations	
Device Status Color	デバイス グループ内の 1 つのデバイスのソフトウェアがコンプライアンスに違反した場合に表示する色を選択します。オプションには、次のものがあります。 • Red（デフォルト） • Yellow • Green 次のリストから、コンプライアンス レベル違反を選択します。 • Security Risk • Pre-production • Obsolete • Bronze • Silver • Gold • Platinum
Category Status Color	ソフトウェア コンプライアンスに違反したデバイスのしきい値パーセンテージを入力します。オプションには、次のものがあります。 • Yellow：デフォルトは 1% です。 • Red：デフォルトは 2% です。

フィールド	説明 / アクション
Startup vs. Running Config Mismatch	
Device Status Color	デバイス グループ内の 1 つのデバイスのスタートアップ コンフィギュレーションが実行コンフィギュレーションと一致していない場合に表示する色を選択します。オプションには、次のものがあります。 • Red • Yellow（デフォルト） • Green
Category Status Color	スタートアップ コンフィギュレーションと実行コンフィギュレーションが一致していないデバイスのしきい値パーセンテージを入力します。オプションには、次のものがあります。 • Yellow：デフォルトは 1% です。 • Red：デフォルトは 2% です。
Device Access Failure	
Device Status Color	デバイス グループ内の 1 つのデバイスがデバイス アクセス障害を報告した場合に表示する色を選択します。オプションには、次のものがあります。 • Red • Yellow（デフォルト） • Green
Category Status Color	アクセス障害が発生したデバイスのしきい値パーセンテージを入力します。オプションには、次のものがあります。 • Yellow：デフォルトは 1% です。 • Red：デフォルトは 2% です。
Configuration Change	
Device Status Color	デバイス グループ内の 1 つのデバイスの設定が変更された場合に表示する色を選択します。オプションには、次のものがあります。 • Red • Yellow（デフォルト） • Green
Category Status Color	設定が変更されたデバイスのしきい値パーセンテージを入力します。オプションには、次のものがあります。 • Yellow：デフォルトは 1% です。 • Red：デフォルトは 2% です。

フィールド	説明 / アクション
Email Report	
Email Report Format	検索結果を電子メール レポートとして送信するときに使用する電子メール形式を選択します。Network Status レポートには適用されないことに留意してください。オプションには、次のものがあります。 • HTML mail（デフォルト） • CSV file attachment • Plain text • HTML mail (without links)
Include Task Results in Email Reports	オンの場合、Comma Separated Value（CSV; カンマ区切り値）ファイル形式のタスク検索の結果を含む完全なタスクの詳細が、電子メール レポートに含められます。Network Status レポートには適用されないことに留意してください。
Email Links	電子メール レポートに含める HTML リンクのアドレス形式を選択します。オプションには、次のものがあります。 • Hostname (if resolvable) • IP Address • Canonical Name (FQDN, if resolvable)（デフォルト） • User Defined：電子メール リンクで使用するユーザ定義のサーバ アドレスを入力します。
SingleView	
Device Change Events to Track	追跡するデバイス変更イベントを選択します。この設定は、SingleView ページに表示するデフォルトのイベント セットを指定します。P.422 の「SingleView ページのフィールド」を参照してください。イベントには、次のものがあります。 • Device Configuration Change • Device Booted • Device Diagnostic Changed • Device Password Change • Module Added • Module Changed • Module Removed • Software Change • User Message

フィールド	説明 / アクション
Diagnostics to Track	追跡する診断を選択します。この設定は、SingleView ページで Device Diagnostic Changed イベント タイプを選択した場合に、どの Device Diagnostic Changed イベントを表示するかを指定します。P.422 の「SingleView ページのフィールド」を参照してください。デフォルトの診断タイプには、次のものがあります。 • Hardware Information • Memory Troubleshooting • CWNCM Detect Device Boot • CWNCM Device File System • CWNCM Flash Storage Space • CWNCM Interfaces • CWNCM Module Status • CWNCM OSPF Neighbors • CWNCM Routing Table **注**：診断の詳細については、P.188 の「View メニュー オプション」を参照してください。
Diagramming	
Maximum Nodes	ダイアグラムに表示するノードの最大数を入力します。デフォルトは 250 ノードです。ダイアグラムを生成すると「Out of Memory」エラーが発生する場合は、この値を小さくします。ダイアグラムに多数のノードを含めると、イメージのサイズが大きくなります。イメージは、非圧縮形式でメモリ内に生成されてから、JPEG 形式で出力されます。ダイアグラムにより多くのノードを含める場合は、この値を増やします。ただし、メモリが不足する可能性があることに留意してください。
Label Font Size	ダイアグラム内のラベルのフォント ポイント サイズを入力します。デフォルトは 8 です。この値を増やすと、ノードのサイズに関連するラベルのサイズが大きくなるため、ラベルが読み取りやすくなる場合があります。
Maximum Layout Duration	レイアウト アルゴリズムを実行する最大期間を入力します。デフォルトは 30 秒です。この最大期間が経過すると、レイアウト アルゴリズムは停止します。この制限に達した場合でも、正確なダイアグラムが生成されることに留意してください。ただし、そのダイアグラムは、レイアウトが十分に最適化されていない場合があります。

フィールド	説明 / アクション
Diagram Compactness	ノード間のスペース量を 0 ～ 100 の範囲で入力します。デフォルトは 90 です。この値は、ダイアグラムを表示する際の密集度を制御します。ダイアグラムの密集度を低くすると、ノードが読み取りやすくなります。ダイアグラムの密集度を高くすると、使用スペース量が削減されますが、ダイアグラムが読み取りにくくなる場合があります。また、密集度の高いダイアグラムは、実行時間が多少長くなる場合があることに留意してください。これは、レイアウトにかかる時間が長くなる傾向があるためです。
Quality-Time Ratio	優先するレイアウト比を 0 ～ 100 の範囲で入力します。デフォルトは 100 です。値を大きくすると、より均整のとれたダイアグラムが生成されます。ただし、レイアウトにかかる時間が長くなり、CPU サイクルの使用量が増えます。
Preferred Edge Length	優先する辺の長さの値を 0 ～ 100 の範囲で入力します。デフォルトは 100 です。一般に、辺を長くすると、ダイアグラム内のノード間のスペースが増えます。ただし、この設定は、レイアウト アルゴリズムが必要に応じて上書きします。値を大きくすると、ダイアグラムの密集度が低くなりますが、メモリの消費量が増えます。また、値を大きくすると、辺がノードやラベルと重なりにくくなるため、ダイアグラムが読み取りやすくなります。
Preferred Minimal Node Distance	優先する最短ノード距離の値を 0 ～ 100 の範囲で入力します。デフォルトは 50 です。この値は、接続されていない状態でのノード間の距離を制御します。値を小さくすると、ダイアグラムの密集度が高くなります。
その他	
Use Excel CSV Format	オンの場合（デフォルト）、検索結果をカンマ区切り値（CSV）ファイルにエクスポートするときは、Microsoft Excel CSV 形式が使用されます。
Save report to file location	すべてのレポート ファイルの保存先となる NCM サーバ上の場所へのパスを入力します。ユーザが Email Report タスクを定義するときに「Save this report to file」オプションを選択した場合は、すべてのファイルがこの場所に自動的に保存されます。デフォルトの場所は *C:\< インストール ディレクトリ >/addins* です。

User Authentication

User Authentication を使用すると、ユーザの認証を 1 か所に集中化できるため、複数のデータベースを保守する必要がなくなります。次のユーザ認証オプションを使用できます。

- Active Directory
- SecurID
- TACACS+
- RADIUS
- Server Automation System

外部認証に失敗し、次に該当する場合は、NCM がローカル ユーザ クレデンシャルへのフォールバックを試行することに留意してください。

- 外部認証サービスがダウンしている、またはアクセス不能である場合
- 外部認証方式を使用して正常にログインされなかったスタティック ユーザ アカウントの場合
- 組み込みの Admin ユーザ アカウントの場合

また、User Authentication を使用すると、NCM 内で組み込みのユーザに対して次のセキュリティ ポリシーを設定することもできます。

- パスワードの最小長を定義する。
- パスワードの複雑性規則を定義する。
- ログイン試行が所定の回数連続して失敗した場合に、ユーザをロックアウトする。

User Authentication ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、User Authentication をクリックします。User Authentication ページが開きます。詳細については、P.97 の「User Authentication ページのフィールド」を参照してください。

Active Directory 認証

組織で Microsoft Active Directory を使用している場合は、グループとユーザの両方を NCM にインポートできます。NCM は Active Directory データベースとのアクティブな交信を維持し、アプリケーションへのログインを許可するユーザと許可しないユーザに関する情報を最新の状態に保ちます。

外部ユーザ認証がイネーブルのときに、ネットワークの問題によって Active Directory サーバが到達不能になった場合でも、NCM へのログインが可能です。NCM が指定の Active Directory サーバに接続できない場合、以前に NCM にログインしたことのあるユーザは、NCM ユーザ パスワードを使用して NCM にログインすることができます。NCM パスワードの設定は My Profile ページで行います。詳細については、P.219 の「My Profile ページのフィールド」を参照してください。

Active Directory ユーザに NCM システム管理者と同じユーザ名が割り当てられていないことを確認してください。デフォルトのシステム管理者のユーザ名は「admin」です。ただし、変更は可能です。デ

フォルトの管理者と別の Active Directory ユーザとの間で名前が競合していると、デフォルトの管理者が NCM にログインできなくなることがあります。

NCM で作成されたユーザが Active Directory で削除された場合でも、そのユーザは自分の NCM パスワード（Active Directory パスワードではない）を使用して、NCM に再度ログインすることができます。

Active Directory に対する外部認証の設定については、P.100 の「Active Directory 外部認証の設定」を参照してください。

SecurID 認証

RSA SecurID® ソリューションは、組織を保護するために、許可されたユーザだけにネットワーク リソースへのアクセス権が付与されることを保証できるように設計されています。一般に、SecurID は 2 つの認証スキーマで構成され、トークンと共にパスワード /PIN を必要とします。トークンは、60 秒ごとに変更されます。詳細については、P.492 の「SecurID ソフトウェア トークンの追加」を参照してください。

TACACS+ 認証

Cisco IOS ソフトウェアでは、現在、TACACS+ を含む複数のバージョンの Terminal Access Controller Access Control System（TACACS）セキュリティ プロトコルがサポートされています。TACACS+ は、詳細なアカウンティング情報を使用して、認証および許可プロセスを柔軟に管理制御することができます。

TACACS+ サーバ（通常は CiscoSecure ACS）を使用してユーザを認証すると、次の利点が得られます。

- NCM ユーザが記憶する必要のあるユーザ名およびパスワードが 1 組だけで済む。
- NCM ユーザの管理を集中化できる。
- TACACS+ パスワード制限を簡単に適用できる。

TACACS+ サーバを使用して、ユーザを NCM に対して認証すると、次のことが可能になります。

- TACACS+ サーバを使用してユーザ ログインを認証する（つまり、ユーザが有効なユーザ名とパスワードのペアを入力したことを確認する）ように NCM を設定する。
- Telnet/SSH プロキシの TACACS+ 認証をサポートする。
- NCM で個別ユーザにフォールバック パスワードを割り当てる。
- TACACS+ ユーザを識別し、TACACS+ サーバがアクセス不能の場合に限ってユーザのフォールバック パスワードが使用されるようにする（ただし、Admin ユーザ以外のユーザが無効な TACACS+ パスワードを入力した場合を除く）。
- フェールオーバー用の複数の TACACS+ サーバを設定する。

（注）TACACS+ は、許可や権限には使用されません。つまり、TACACS+ を介してユーザを認証する前に、ユーザを NCM に手動で追加し、適切な権限を割り当てておく必要があります。NCM でユーザが TACACS+ ユーザとして識別された場合、この指定を削除することはできません。

RADIUS 認証

RADIUS（リモート認証ダイヤルイン サービス）を使用すると、次のことが可能になります。

- ネットワーク アクセス サーバを RADIUS クライアントとして動作させる。RADIUS クライアントは、指定された RADIUS サーバに情報を渡した後、返された応答に対して動作します。
- RADIUS サーバで接続要求を受信し、ユーザを認証して、正しい接続に必要なクライアント設定情報をすべて返す。
- RADIUS サーバを、他の RADIUS サーバまたは他の認証サーバに対するプロキシ クライアントとして動作させる。

（注）RADIUS は、許可や権限には使用されません。つまり、RADIUS を介してユーザを認証する前に、ユーザを NCM に手動で追加し、適切な権限を割り当てておく必要があります。NCM でユーザが RADIUS ユーザとして識別された場合、この指定を削除することはできません。

TACAC+ または RADIUS 認証をイネーブルにするには、次の手順を実行します。

1. メニューバーの Admin の下で、Administrative Settings を選択し、Configuration Mgmt をクリックします。Configuration Mgmt ページが開きます。
2. User Authentication タブをクリックします。User Authentication 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。

User Authentication ページのフィールド

フィールド	説明 / アクション
User Password Security	
Minimum User Password Length	パスワードに含める文字数の最小値を入力します。この文字数に満たないパスワードは無効と見なされます。
User Password Must Contain Upper and Lower Case	オンの場合、ユーザは大文字と小文字の両方の英字を含むパスワードを選択する必要があります。
Additional User Password Restriction	次のいずれかのオプションを選択します。 • No additional restrictions（デフォルト） • Must contain at least one non-alphabetic digit or special character • Must contain both at least one digit and at least one special character
Maximum Consecutive Login Failures	ユーザ認証に連続して失敗できる回数の最大値を入力します。この回数を超えると、ユーザはディセーブルになります。値が 0（ゼロ）の場合、この確認はスキップされます（**注**：この設定が適用されるのは、組み込みのユーザ認証だけで、外部認証方式には適用されません）。

フィールド	説明 / アクション
External Authentication Type	
External Authentication Type	使用する外部認証のタイプを選択します。オプションには、次のものがあります。 • None (Local Auth) • Server Automation System • TACACS+ • RADIUS • SecurID • Active Directory TACACS+ または RADIUS を選択した場合は、下のセクションで詳細を設定できます。Active Directory を選択した場合は、Active Directory Setup リンクをクリックします。詳細については、P.100 の「Active Directory 外部認証の設定」を参照してください。SecurID には、追加の外部認証オプションはありません。
TACACS+ / RADIUS Authentication	
Primary TACACS+ or RADIUS Server	プライマリ TACACS+ または RADIUS サーバのホスト名または IP アドレスを入力します。
Secondary TACACS+ or RADIUS Server	セカンダリ TACACS+ または RADIUS サーバのホスト名または IP アドレスを入力します。このフィールドはオプションです。
TACACS+ or RADIUS Secret	TACACS+ または RADIUS サーバに設定されている NCM ホストの共有秘密を入力します。TACACS+ または RADIUS 共有秘密は、TACACS+ または RADIUS クライアント (NCM) が TACACS+ または RADIUS サーバとの通信を暗号化するときに使用する鍵（パスワード）です。サーバで通信を復号化するには、クライアントとサーバ間で共有秘密が一致する必要があります。
TACACS+ or RADIUS Authentication Method	NCM と TACACS+ または RADIUS サーバ間の通信を暗号化するときに使用する認証方式として、次のいずれかを選択します。 • PAD (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol) • MSCHAP (Microsoft Challenge Handshake Authentication Protocol)
Server Automation System Authentication	
Twist Server	Twist サーバのホスト名または IP アドレスを入力します。
Twist Port Number	Twist サーバに接続する Twist ポート番号（通常は 1032）を入力します。

フィールド	説明 / アクション
Twist Username	接続済みサーバを検索するときに使用する Twist ユーザ名を入力します。
Twist Password	接続済みサーバを検索するときに使用する Twist パスワードを入力します。
OCC Server	接続済みサーバとリンクする OCC サーバのホスト名を入力します。この操作により、NCM Server ページから OCC Server ページにジャンプできるようになります。詳細については、P.198 の「Servers ページのフィールド」を参照してください。
Default User Group	認証ユーザを追加するユーザ グループの名前をドロップダウン メニューから選択します。

Active Directory 外部認証の設定

Active Directory 外部認証をイネーブルにするには、次の手順を実行します。

1. メニューバーの Admin の下で、Administrative Settings を選択し、User Authentication をクリックします。Administrative Settings - User Authentication ページが開きます。
2. External Authentication Type フィールドまでスクロール ダウンします。
3. External Authentication Type フィールドで、Active Directory を選択し、Save をクリックします。
4. Active Directory Setup リンクをクリックします。Active Directory Setup Wizard が開きます。以前に Active Directory 認証を設定していれば、次の情報が表示されます。
    - Active Directory 認証のステータス
    - Active Directory 認証サーバ ホスト
    - ポート番号
    - 接続ユーザの名前
    - 接続ユーザのパスワード
    - 検索ベース
    - セキュア接続を使用しているかどうか

次の表に従って、設定プロセスを実行します。

ステップ	アクション
1	Welcome to the Active Directory Setup Wizard ページで、Next をクリックします。次の情報を入力し、Next をクリックします。 • Server Name：Active Directory サーバのホスト名（つまり、AD/ ドメイン コントローラのホスト名または IP アドレス）を入力します。 • Port：LDAP 要求のポート番号を入力します。Windows 2000 AD ドメイン コントローラはすべて、LDAP 要求をポート 389 で受信することに留意してください。単一のドメイン設定では、ポート 389 またはポート 636（SSL を使用する場合）を使用します。ただし、マルチドメイン AD 環境では、ポート 3268 またはポート 3269（SSL を使用する場合）を使用する必要があります。 • Connection Type：Regular Connection（デフォルト）または Secure Connection (SSL) を選択します。ディレクトリ サーバに接続するときは、必ず Secure Connection を選択してください（**注**：このオプションをイネーブルにする場合、ディレクトリ サーバまたはドメイン コントローラ サーバの証明書が認定済み CA によって署名されていないときは、NCM が動作しているサーバに証明書を手動でインポートする必要があります）。Active Directory の SSL 設定の詳細については、P.101 の「Active Directory の SSL 設定」を参照してください。

ステップ	アクション
2	次の情報を入力し、Next をクリックします。 • Connection User Name : 接続ユーザの名前を入力します。AD サーバに対してユーザ情報をクエリーするには、ドメイン ユーザ アカウント（DN）を使用して NCM を AD サーバにバインドする必要があることに留意してください。DN は、Windows 2000 LDAP 形式または Windows 2000 User Principal Name（UPN; ユーザ プリンシパル名）形式のどちらかです。Windows 2000 UPN 形式は、Active Directory ツリーで DN を一意に識別する簡便な表記法です。UPN には、ユーザ アカウントとそれに対応するドメインの両方が含まれます。Windows 2000 UPN DN の例には、*jsmith@cisco.com* があります。 • Connection User Password：接続ユーザのパスワードを入力します。 • Search Base：検索ベースを入力します。検索ベースは、LDAP 検索を行う場合の LDAP ディレクトリ内の開始点です。できるだけ、検索ベースは、AD フォレスト全体のルートドメインに設定してください。このように設定すると、NCM が Windows 2000 AD フォレスト全体をクエリーできるようになります。検索ベースを特定の OU レベルに設定すると、クエリー対象は、その特定の OU の子オブジェクトに限定されます。同様に、検索ベースを特定のドメイン レベルに設定すると、クエリー対象は、その特定のドメインの子オブジェクトに限定されます。このため、検索ベースはできるだけ汎用にする必要があります。
3	NCM にアクセスできるセキュリティ グループを指定します。Find オプションを使用して Active Directory 内のユーザ グループを検索し、Next をクリックします。
4	外部認証の設定を確認します。確認するには、ユーザ名とパスワードを入力し、Test Login ボタンをクリックします。必ず、Save ボタンをクリックして設定情報を保存してください。エラーがなければ、次のメッセージが表示され、External Authentication Setup Summary ページが更新されます。 `Successfully updated External Authentication settings.`

Active Directory の SSL 設定

Active Directory の SSL を設定するには、次の手順を実行します。

1. Windows 2000 または Windows 2003 Server にエンタープライズ証明機関をインストールします。フォレスト内のドメイン コントローラがすべて自動的に登録され、適切な証明書がインストールされます。
2. Group Policy Editor を使用して Default Domain Controller Policy を開きます。
3. Computer Configuration の下で、Windows Settings をクリックします。
4. Security Settings をクリックし、Public Key Policies をクリックします。
5. Automatic Certificate Request Settings をクリックします。
6. ウィザードを使用してドメイン コントローラ用のポリシーを追加します。

詳細については、Microsoft サポート技術情報の記事 Q247078 を参照してください。

証明書をインポートするには、次の手順を実行します。

1. Certificate Authority 管理コンソール（通常は Active Directory サーバ上にある）を起動します。起動するには、Start → Programs → Administrative Tools → Certification Authority の順にクリックします。
2. Certificate Authority Local の下で、使用するドメイン コントローラの証明書を発行する認証局を検索します。
3. その認証局を右クリックし、Properties を選択します。
4. General タブで、View Certificate をクリックします。
5. Details タブを選択し、Copy to file を選択します。
6. ウィザードを使用して、証明書を Base64 Encoded ファイルにエクスポートします。
7. このファイルを NCM サーバにコピーします。
8. Windows コマンド プロンプトで、次の場所に移動します。
   < インストール ディレクトリ >_Root\jre\bin
9. keytool -import -file PATH_TO_THE_CERT_FILE -alias ADSCert -keystore ..\lib\security\cacert と入力します。

   PATH_TO_THE_CERT_FILE の部分は、ステップ 7 で作成したファイルの絶対パスに置き換えてください。

Server Monitoring

Server Monitoring を使用すると、NCM サーバ全体の状況を確認できます。エラーが検出された場合は、アラート通知とイベント ロギングがトリガーされます。サーバ モニタはすべて、NCM にあらかじめ同梱されています。

モニタがエラーを受信した場合は、NCM Monitor Error イベントがトリガーされ、エラー通知がシステム管理者に送信されます。そのモニタを後で確認したときに引き続きエラー状態にあっても、Monitor Error イベントの送信は続行されないことに留意してください。モニタがエラー状態になり、結果としてイベントがトリガーされたときは、状態が okay に変更された場合に限り、Monitor Okay イベントが送信されます。

（注）システムを再起動した場合、引き続きエラー状態になったときは、新しい Monitor Error イベントがトリガーされます。デバイスがアクセス不能の場合は、その事実が管理者に電子メールで送信されます。

Server Monitoring ページでは、サーバ モニタを設定できます。また、すべてまたは特定のサーバ モニタをイネーブルにするオプションを使用できます。最新のモニタ動作の結果は、Monitor ログ ファイルに格納されます。また、この結果は System Status ページで表示できます。System Status ページについては、P.103 の「Server Monitoring ページのフィールド」を参照してください。

（注）モニタリング タスクの設定を変更する権限を持っているのは、管理者だけです。すべてのユーザは、モニタリング結果を表示できます。

Server Monitoring ページを表示するには、メニューバーの Admin の下で Administrative Settings を選択し、Server Monitoring をクリックします。Server Monitoring ページが開きます。

Server Monitoring ページのフィールド

フィールド	説明 / アクション
Server Monitoring	
Enable Server Monitoring	オンの場合（デフォルト）、Server Monitoring がイネーブルになります。NCM エラーが発生した場合は、電子メール通知が生成されます。最新の結果は、Monitor ログ ファイルに格納されます。また、この結果は System Status ページで表示できます。
Delay on Startup Before Starting Monitoring	Server Monitoring を起動してから開始するまでの遅延時間を分単位で入力します。デフォルトは 2 分です。
Delay Between Monitoring Runs	モニタリング動作の間隔を分単位で入力します。デフォルトは 360 分です。

フィールド	説明 / アクション
Enable the ConfigMonitor	オンの場合、Config モニタがイネーブルになります。このモニタは、インストールされている .rcx ファイルやその他の設定ファイルが正常であることを確認します。このモニタでは、最初にインストールされた .rcx ファイルのバックアップが作成され、正常にインストールされた最新の .rcx ファイルのバックアップが保持されます。
Enable the DatabaseDataMonitor	オンの場合、Database Data モニタがイネーブルになります。このモニタは、重要なシステム コンポーネントがすべてデータベース内に存在することを確認します。たとえば、admin ユーザが存在すること、暗号鍵が 1 つだけ存在すること、および一時停止または保留状態になっているインベントリ スナップショット タスクが 1 つ存在することなどを確認します。このモニタでは、暗号鍵と管理者の電子メール アドレスのバックアップ (データベース サーバがダウンした場合に使用される）が作成されます。
Enable the DatabaseMonitor	オンの場合、Database モニタがイネーブルになります。このモニタは、データベースの接続性について確認します。たとえば、無効なクレデンシャルが存在しないかどうか、または接続が過多になっていないかどうかなどを確認します。
Enable the DiskMonitor	オンの場合、Disk モニタがイネーブルになります。このモニタは、ディスク スペースの不足状況について確認します。
Enable the HTTPMonitor	オンの場合、HTTP モニタがイネーブルになります。このモニタは、NCM Web サーバが正常に動作していることを確認します。
Enable the LDAPMonitor	オンの場合、LDAP モニタがイネーブルになります。このモニタは、Active Directory サーバが使用可能であることを確認します。
Enable the LicenseMonitor	オンの場合、LicenseMonitor がイネーブルになります。このモニタは、使用可能なライセンスが管理対象デバイスのパーセンテージを下回っているかどうかということや、次に満了するライセンスの有効期限が指定の日数を切ったかどうかということを確認します。詳細については、下の「Monitor Configuration」セクションを参照してください。
Enable the MemoryMonitor	オンの場合、Memory モニタがイネーブルになります。このモニタは、メモリの不足状況について確認します。
Enable the RMIMonitor	オンの場合、RMI モニタがイネーブルになります。このモニタは、NCM EJB への RMI アクセスが動作していることを確認します。また、他の EJB コンテナ（Java アプリケーション サーバ）が RMI ポートを占有していないことも確認します。
Enable the RunExternalTaskMonitor	オンの場合、Run External Task モニタがイネーブルになります。このモニタは、NCM サーバが外部の .bat または .sh ファイルを実行できることを確認します。

フィールド	説明 / アクション
Enable the SMTPMonitor	オンの場合、SMTP モニタがイネーブルになります。このモニタは、設定されたメール サーバ上のポート 25 に対する Telnet 接続を確立し、SMTP *QUIT* コマンドを送信して、適切な *221* 応答コードが返されるまで待機します。
Enable the SSHMonitor	オンの場合、SSH モニタがイネーブルになります。このモニタは、NCM に組み込まれている SSH サーバへの接続をテストします。
Enable the SyslogMonitor	オンの場合、Syslog モニタがイネーブルになります。このモニタは、NCM に Syslog メッセージを送信し、メッセージが NCM Management Engine によって受信されたことを確認します。
Enable the TelnetMonitor	オンの場合、Telnet モニタがイネーブルになります。このモニタは、NCM に組み込まれている Telnet サーバが正常に動作していることを確認します。
Enable the TFTPMonitor	オンの場合、TFTP モニタがイネーブルになります。このモニタは、タイムスタンプを含むファイルをローカル マシンに TFTP 送信し、ファイル システムを調べて、ファイルが正しく書き込まれたことを確認します。
Monitor Configuration	
Check the Inventory Snapshot in the DatabaseDataMonitor	オンの場合、Database Data モニタでインベントリ スナップショットが確認されます。
Warning Threshold for Free Disk Space	空きディスク スペースの警告メッセージをトリガーするしきい値を入力します。デフォルトは 20 MB です。
Error Threshold for Free Disk Space	空きディスク スペースのエラー メッセージをトリガーするしきい値を入力します。デフォルトは 10 MB です。
Drives To Monitor for Disk Space	右側のボックスにドライブを入力し、Add Drive << をクリックします。ドライブを削除するには、左側のボックスでドライブを選択し、Delete Drive をクリックします。
Warning Threshold for Managed Devices Count	ライセンス全体のパーセンテージを入力します。使用可能なライセンスがこのパーセンテージを下回った場合は、警告が発行されます。デバイス数のしきい値は、デフォルトで 10% に設定されています。
Warning Threshold for License Expiration	日数を入力します。次に満了するライセンスの有効期限が指定の日数を切った場合は、警告が発行されます。有効期限のしきい値は、デフォルトで 30 日に設定されています。
Warning Threshold for Free RAM	Free RAM 警告メッセージをトリガーするしきい値を入力します。デフォルトは 20 MB です。

フィールド	説明 / アクション
Error Threshold for Free RAM	Free RAM エラー メッセージをトリガーするしきい値を入力します。デフォルトは 10 MB です。
Delay for SSH Thread Check	SSH スレッド チェックの遅延時間を入力します。デフォルトは 15000 ミリ秒です。
Delay for TFTP File Check	TFTP ファイル チェックの遅延時間を入力します。デフォルトは 5000 ミリ秒です。
Delay for Syslog message to show up	Syslog メッセージを表示する際の遅延時間を入力します。デフォルトは 45000 ミリ秒です。

Save をクリックして、変更を保存してください。

モニタ結果の表示

System Status ページには、最新のモニタ動作の結果が表示されます。System Status ページを表示するには、メニューバーの Admin の下で、System Status をクリックします。System Status ページが開きます。

System Status ページのフィールド

フィールド	説明 / アクション
Run All リンク	一覧表示されているモニタをすべて実行します。
Configure Server Monitoring リンク	Configuration Management ページが開きます。詳細については、P.54 の「Configuration Mgmt ページのフィールド」を参照してください。
Monitor Name	モニタ名が表示されます。各モニタは、モニタリング中のサブシステムに関するさまざまなメッセージを返します。P.108 の「モニタのメッセージ」を参照してください。
Status	次のような、モニタのステータスが表示されます。 • Okay • Warning • Error • Disabled
Last Checked	モニタが最後に実行された日時が表示されます。
Result	結果に関する情報が表示されます。
Actions	次のオプションを選択できます。 • Run Now：モニタをただちに実行します。 • View Details : Monitor Details ページが開きます。このページでは、モニタに関する詳細として、モニタの説明、ステータス、結果、追加の診断情報などを表示できます。 • Start/Stop Service：Start/Stop Services ページが開きます。詳細については、P.113 の「サービスの開始と停止」を参照してください。

モニタのメッセージ

各モニタは、モニタリング中のサブシステムに関するさまざまなメッセージを返します。この項では、このようなメッセージの一部を示し、考えられる対応策について説明します。

モニタ	説明 / 解決策
BaseServerMonitor	< スレッド名 > is not running. : NCM の正常動作に必要なスレッドが、何らかの理由で失敗しました。NCM Management Engine を再起動します。
ConfigMonitor	• Missing file < ファイル名 >.rcx：NCM の必須設定ファイルのいずれかが欠落しています。サポート担当者にお問い合せください。 • Error getting required config from < ファイル名 >.rcx：NCM の設定ファイルのいずれかが破損しています。サポート担当者にお問い合せください。 • Exception parsing rcx file: < ファイル名 >：NCM の設定ファイルのいずれかが破損しています。サポート担当者にお問い合せください。
DatabaseMonitor on MySQL	• Cannot connect to the MySQL server on < サーバ名 >:3306.：NCM が接続を試行している場所に、動作中の MySQL サーバがありません。MySQL サービスを再起動するか、または NCM 接続情報が正しいことを確認します。 • Communication link failure: java.io.IOException：MySQL サーバへの接続が失われました。NCM Management Engine または MySQL サービスを再起動します。 • Access denied for user: < ユーザ名 > to database < データベース名 >: NCM が接続を試行しているデータベースに誤りがあるか、または既存のデータベースに対する権限に問題があります。NCM 接続情報が正しいかどうかを確認します。 • Invalid authorization specification: Access denied for user: < ユーザ名 > (Using password: YES)：NCM が接続の試行に使用しているユーザ名またはパスワードに誤りがあります。NCM データベースのユーザ名とパスワードを正しい値にリセットします。 • General error: Table NCM.RN_CRYPTO_KEY doesn't exist：NCM は所定のクレデンシャルを使用してデータベースに接続できますが、データベースが NCM データベースでないか、または破損しています（RN_CRYPTO_KEY テーブルが欠落しているため）。NCM 接続情報が正しいかどうかを確認します。

モニタ	説明 / 解決策
DatabaseMonitor on Oracle	• Error establishing socket.Connection refused: connect：NCM が接続を試行している場所に、動作中の Oracle サーバがありません。Oracle サービスを再起動するか、または NCM 接続情報が正しいことを確認します。 • Connection reset by peer: socket write error. : Oracle サーバへの接続が失われました。NCM Management Engine または Oracle を再起動します。 • ORA-12505 Connection refused, the specified SID (<データベース名>) was not recognized by the Oracle server. : NCM が接続を試行しているデータベースの名前に誤りがあります。NCM 接続情報が正しいかどうかを確認します。 • ORA-01017: invalid username/password; logon denied : NCM が接続の試行に使用しているユーザ名またはパスワードに誤りがあります。NCM データベースのユーザ名とパスワードを正しい値にリセットします。 • ORA-00942: table or view does not exist：NCM は所定のクレデンシャルを使用してデータベースに接続できますが、データベースが NCM データベースでないか、または破損しています（RN_CRYPTO_KEY テーブルが欠落しているため）。NCM 接続情報が正しいかどうかを確認します。
DatabaseMonitor on SQLServer	• Error establishing socket. : NCM が接続を試行している場所に、動作中の SQLServer がありません。SQLServer サービスを再起動するか、または NCM 接続情報が正しいことを確認します。 • Connection reset by peer: socket write error : SQLServer への接続が失われました。NCM Management Engine または SQLServer を再起動します。 • Cannot open database requested in login < データベース名 >.Login fails. : NCM が接続を試行しているデータベースの名前に誤りがあるか、または既存のデータベースに対する権限に問題があります。NCM 接続情報が正しいかどうかを確認します。 • Login failed for user < ユーザ名 >. : NCM が接続の試行に使用しているユーザ名またはパスワードに誤りがあります。NCM データベースのユーザ名とパスワードを正しい値にリセットします。 • Invalid object name RN_CRYPTO_KEY. : NCM は所定のクレデンシャルを使用してデータベースに接続できますが、データベースが NCM データベースでないか、または破損しています（RN_CRYPTO_KEY テーブルが欠落しているため）。NCM 接続情報が正しいかどうかを確認します。

モニタ	説明 / 解決策
DatabaseDataMonitor	• Could not find an administrative user. : NCM で管理ユーザが設定されていません。サポート担当者にお問い合せください。 • Multiple crypto keys exist. : NCM のデータベースに複数の暗号鍵が含まれています。サポート担当者にお問い合せください。 • Current key does not match saved key. : NCM は、異なる暗号鍵を使用しています。サポート担当者にお問い合せください。 • More than one crypto key. : NCM は、異なる暗号鍵を使用しています。サポート担当者にお問い合せください。 • Could not find an Inventory group snapshot. : NCM に、システム内のすべてのデバイスから設定を収集するタスクが含まれていません。Inventory グループに対するスナップショット タスクを作成します。 • Could not find a reporting task. : NCM に、Summary レポートを生成するタスクが含まれていません。Generate Summary Reports タスクを作成します。 • Could not find a pruner task. : NCM に、データベースから古いデータをプルーニングするタスクが含まれていません。Prune Database タスクを作成します。
DiskMonitor	Disk/Filesystem <ファイル システム> has only <スペース> bytes free.Error threshold is < 制限 > bytes. : NCM サーバのディスク ドライブの空き容量が不足しつつあります。ディスク ドライブから不要なファイルを削除します。
HTTPMonitor	Did not get NCM login page. : 設定された HTTP/HTTPS ポートでアプリケーションが動作していますが、そのアプリケーションは NCM Web サーバではないようです。NCM サーバ上で動作している他の Web サーバ（たとえば、IIS）があればすべて停止し、NCM Management Engine を再起動します。
LDAPMonitor	• ActiveDirectory is not in use. : これは、NCM サーバが Active Directory を使用するように設定されていないことを通知する情報メッセージです。 • Exception in LDAPMonitor: javax.naming. CommunicationException: <ホスト名 >:389 : ホスト < ホスト名 > が存在しません。外部認証の Server Name 設定を修正します。 • Exception in LDAPMonitor: javax.naming. CommunicationException: <ホスト名 >:389 : ホスト < ホスト名 > は存在しますが、LDAP ポート（389）上で接続を受け付けません。Server Name 設定が正しいことを確認します。正しい場合は、そのホスト上で LDAP サーバが動作していることを確認します。 • Exception in LDAPMonitor: javax.naming.AuthenticationException : 外部認証の Connection User Name 設定または Connection User Password 設定に誤りがあります。これらの設定が正しいことを確認します。

モニタ	説明 / 解決策
LicenseMonitor	Results カラムに、「License about to expire」や「Device count exceeds the current threshold of available licenses」などの警告が表示されます。警告が表示されない場合は、使用可能なデバイス ライセンスの数が表示されます（たとえば、「3454 of 3600 device licenses remaining」）。View Details リンクをクリックすると、ライセンスの詳細として、使用中および未使用のライセンスや、ライセンスの有効期限などが表示されます（**注**：複数のライセンスが使用されている場合、有効期限は、次に満了するライセンスのものを指します）。
MemoryMonitor	< バイト数 > bytes free.：これはシステムで使用可能なメモリ容量です。エラー状態が発生した場合は、この値が、システムの正常動作に必要な容量を下回りつつあります。サポート担当者にお問い合せください。
RMIMonitor	Could not connect to RMI port 1099.：NCM のクライアントおよび API の正常動作に必要なポート 1099 が、別のアプリケーションによって使用されています。ポート 1099 を使用しているアプリケーションを停止し、NCM Management Engine を再起動します。この方法で問題を解決できない場合は、サポート担当者にお問い合せください。
RunExternalTask Monitor	• CreateProcess: < パス >\tc_test.bat error=5：NCM に、テスト スクリプト（別のスクリプトの可能性もあります）にアクセスする権限がありません。NCM のディレクトリに対するファイル システム権限を確認します。 • CreateProcess: < パス >\tc_test.bat error=2：NCM がテスト スクリプトを見つけることができません。サポート担当者にお問い合せください。 • Running < パス >\tc_test.bat from directory < パス > Got result code: 0 Got output: < テキスト >：テスト スクリプトが破損しています。サポート担当者にお問い合せください。
SMTPMonitor	• SMTP Server name is blank.：NCM で SMTP サーバ名の管理設定がブランクになっています。Administrative Settings ページでメールサーバが設定されていることを確認します。 • Can't open Telnet connection to < ホスト名 > 25 : NCM が < ホスト名 > に接続できないか、またはホストが SMTP ポート（25）上で接続を受け付けません。Administrative Settings ページで正しいメールサーバが設定されていることを確認します。NCM サーバがそのサーバ上のポート 25 にアクセスできることを確認します。 • Timeout waiting Expected: 220 Received.：設定されたメール サーバ上のポート 25 でアプリケーションが動作していますが、そのアプリケーションは適切な SMTP コードに応答しないため、SMTP アプリケーションではないようです。Administrative Settings ページで正しいメールサーバが設定されていることを確認します。

モニタ	説明 / 解決策
SSHMonitor	Unknown problem connecting to SSH server. : NCM SSH サーバが正常に動作していません。NCM が使用している SSH ポートが他のアプリケーションによってリッスンされていないことを確認します。NCM Management Engine を再起動します。
SyslogMonitor	Test syslog message did not get processed. : NCM の組み込み Syslog サーバが動作していないか、またはそのサーバで問題が発生しています。サポート担当者にお問い合せください。
TelnetMonitor	• Can't open Telnet connection to < ホスト名 > 25. : NCM Telnet サーバが正常に動作していません。NCM Management Engine を再起動します。この方法で問題を解決できない場合は、サポート担当者にお問い合せください。 • Timeout waiting Expected: Cisco Login: Received. : 設定された Telnet ポートでアプリケーションが動作していますが、そのアプリケーションは NCM Telnet サーバではないようです。NCM Telnet サーバのリスニングポートを修正します。
TFTPMonitor	• Connection timed out to the TFTP server. : TFTP サーバが動作していないか、または接続を受け付けません。TFTP サーバを再起動します。 • Test TFTP file was written but could not be read successfully.Check TFTP path setting. : TFTP ファイルが TFTP サーバに正常に書き込まれましたが、そのファイルをファイルシステムから読み取ることができません。NCM Management Engine の TFTP パスの設定が正しいことを確認します。 • Found checkpoint file but timestamp is out of date. : 最後に試行したファイル書き込みが失敗しました。また、以前のチェックポイントの試行が見つかりました。これは、過去のある時点で動作していた TFTP サーバが現在は動作していないことを意味します。TFTP サーバを再起動します。

サービスの開始と停止

NCM には、次に示す 4 つの主要な機能ユニットがあります。

- Management Engine
- TFTP サーバ
- Syslog サーバ
- Cisco Connection Online（CCO）

通常、カスタマー サポートと連携するときに行う操作は、サービスの停止、開始、または再起動だけです。

サービスの開始と停止、またはドライバや内容のリロードを行うには、メニューバーの Admin の下で、Start/Stop Services をクリックします。Start/Stop Services ページが開きます。

（注）Web ユーザ インターフェイスを使用して NCM サービスを開始および停止すると、以前のページに移動する機能が失われることがあります。Back ボタンをクリックすると、null というテキストを含むページが表示されます。その場合は、代わりにブラウザの Back ボタンをクリックしてください。

Start/Stop Services ページのフィールド

フィールド	説明 / アクション
Management Engine	次のいずれかのオプションを選択します。 • Stop：Management Engine（別名、NCM サーバ）を停止します。これは、NCM 内のメイン サービスです。 • Restart：Management Engine を再起動します。
TFTP Server	次のいずれかのオプションを選択します。 • Start：TFTP サーバを起動します。NCM は、主に、このサーバを使用して設定の取得と展開を行います（**注**：TFTP を使用すると、最適なパフォーマンスが得られます。TFTP を使用できない場合、NCM は Telnet または SSH を使用して設定を処理します）。 • Stop：TFTP サーバを停止します。 • Restart：TFTP サーバを再起動します。

フィールド	説明 / アクション
Syslog Server	次のいずれかのオプションを選択します。 • Start : Syslog サーバを起動します。NCM を唯一の Syslog サーバにすることができます。または、他の Syslog サーバから NCM にメッセージを転送することもできます。NCM は Syslog メッセージを使用して、リアルタイムの変更イベントを検出し、そのイベントをユーザに関連付けます。 • Stop：Syslog サーバを停止します。 • Restart：Syslog サーバを再起動します。
CCO	次のオプションを選択します。 • Reload Drivers：製品にドライバをリロードできます。Reload Drivers ボタンでは、ドライバは検出されないことに留意してください。 • Reload Content：対象となる内容は、シスコから入手可能な一連の NCM 拡張のうち、製品のアップグレードを必要としないものです。たとえば、NCM では、NCM Alert Center（CAC）を介して、ソフトウェア コンプライアンス ポリシーの内容をインポートできます。CAC の機能を使用してソフトウェア コンプライアンス ポリシーをダウンロードすると、ネットワークの整合性を管理しやすくなります。

ロギングのイネーブル化

ログレベルを変更する場合は、事前にカスタマー サポートに連絡することをお勧めします。ソフトウェア コンポーネントは複雑で、一部のコンポーネントは大量のデータを生成します。

ロギングをイネーブルにするには、メニューバーの Admin の下で、Troubleshooting をクリックします。Troubleshooting ページが開きます。作業が終了したら、必ず Submit をクリックしてください。

Troubleshooting ページのフィールド

フィールド	説明 / アクション
Send Troubleshooting Information リンク	Send Troubleshooting Info ページが開きます。このページでは、電子メールを作成して、システムの情報およびログをカスタマー サポートに送信することができます。詳細については、P.23 の「Send Troubleshooting ページのフィールド」を参照してください。
Send Test Email to Admin User	システム管理者に電子メールを送信します。
Enable logging for	ロギングをイネーブルにするコンポーネントを 1 つ以上選択します。現在のログレベルが、各ソフトウェア コンポーネントの後ろにカッコで囲まれて表示されます。次にコンポーネントの例を示します。 • auth [Error] • changedectection [Error] • Config [Error] • deploy [Error] • user [Error]
and for	リストにないソフトウェア コンポーネントを追加する場合は、ここに入力します。
at level < > and above	ログレベルを選択します。オプションには、次のものがあります。 • Fatal (fewest messages) • Error（デフォルト） • Warning • Info • Debug • Trace (most messages)

フィールド	説明 / アクション
Keep < > days worth of logs	ログ データの保持期間を入力します。デフォルトは 2 日です（**注**: ログ データは、ディスク スペースを大量に必要とする場合があります）。
Reset	オンの場合、Submit ボタンをクリックすると、すべてのログがデフォルト ログレベル（Error）にリセットされます。