デバイス通信および展開のトラブルシューティング

Security Manager がデバイスにログインする必要がある処理を行うときに、問題が発生する可能性が高くなります。このようなタイプの処理には、動作中デバイスを使用したポリシーの検出と展開や、デバイスから情報を取得する際の関連処理などがあります。

重要な点として、通信パスが Security Manager サーバからデバイスまでであること、つまり、Security Manager クライアントが動作しているワークステーションはデバイス通信に関連していないこと（サーバが同じマシン上にインストールされている場合を除きます）に注意してください。通信を正常に行うには、Security Manager サーバに、デバイスへのネットワーク パスと、デバイスに対して認証を行うための適切なクレデンシャルおよび証明書が必要です。

次の各項は、デバイス通信およびポリシー展開の一般的な問題のトラブルシューティングに役立ちます。

デバイス接続のテスト

Security Manager は、デバイスを管理するために、デバイスに接続してログインできる必要があります。この目的で Security Manager 内に定義したクレデンシャルおよびトランスポート方式を、Security Manager が使用できるかどうかをテストできます。

接続をテストできるのは、スタティック IP アドレスを持つデバイスだけです。トランスポート プロトコルとして Token Management Server（TMS）を使用するデバイスに対しては、接続をテストできません。

ネットワークまたはインベントリ ファイルからインベントリにデバイスを追加すると、Security Manager によって自動的に接続がテストされます。

デバイスの接続は、インベントリ内のデバイス、または手動で追加する新しいデバイスに対して、手動でテストできます。ここでは、すでにインベントリ内に存在するデバイスに対して接

続をテストする方法について説明します。デバイスを手動で追加する場合、[新規デバイス（New Device）] ウィザードの [デバイスのログイン情報（Device Credentials）] ページで [接続テスト（Test Connectivity）] をクリックして、次に示すテストを実行します。手動でのデバイスの追加方法については、手動定義によるデバイスの追加を参照してください。

はじめる前に

Security Manager は、[Device Communication] ページの設定を使用して、接続タイムアウト、接続を再試行する頻度、トランスポートプロトコル、および使用するクレデンシャルを決定します。これらの設定を行うには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します。

関連項目

- デバイス ビューについて
- デバイス プロパティの表示または変更
- [Device Communication] ページ

ステップ 1 デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

ステップ 2 コンテンツテーブルから [ログイン情報（Credentials）] を選択します。

ステップ 3 [接続のテスト（Test Connectivity）] をクリックします。

[Device Connectivity Test] ダイアログボックスが開き、使用中のプロトコルなど、テストの経過が表示されます（ [Device Connectivity Test] ダイアログボックス （3 ページ）を参照）。テストは実行中に中断できます。テストが完了したら、[詳細（Details）] をクリックして、次の情報を確認します。

- テストが成功した場合、 **show version** コマンドまたは **getVersion** コマンド（IPS センサーおよび Cisco IOS IPS センサーの場合）の出力が表示されます。テキストを選択し、Ctrl+C を押してテキストをクリップボードにコピーすると、あとで分析するために別のファイルに貼り付けることができます。
- テストが失敗した場合は、エラー情報が表示されます。次のような問題が一般的です。
  - ユーザ名またはパスワードが間違っている。
  - 間違ったプロトコルが選択されている。たとえば、選択されているプロトコルに応答するようにデバイスが設定されていない可能性があります。
  - デバイスが接続を正しく受け入れるように設定されていない。サポートされているプロトコルが少なくとも 1 つ設定されていることを確認してください。

- デバイスに間違ったオペレーティング システムが指定されている（ASA デバイスに PIX を指定した場合など）。
- ACS 認証を使用していて、デバイスへの接続が完了している場合、Control 認可がなければ、Security Manager がバージョン情報の取得を試行するときにエラーが発生することがある。
- 一般的なネットワーク設定の問題が存在する。Security Manager の外部からデバイスへの接続をテストしてください。ハードウェア エラー、メディア エラー、ブーティング エラー、キューのオーバーフローを引き起こす超過トラフィック、デバイス上の重複する MAC または IP アドレス、物理的な不一致（リンク、デュプレックス、速度の不一致など）、または論理的な不一致（VLAN や VTP の不一致、ATM ネットワークの設定の誤りなど）がないかどうかを調べます。

[Device Connectivity Test] ダイアログボックス

[Device Connectivity Test] ダイアログボックスを使用して、Security Manager が設定済みのクレデンシャルを使用してデバイスに接続できるかどうかを確認します。

ナビゲーション パス

デバイス接続テストを開始するには、次のいずれかの領域の [ログイン情報（Credentials）] ページから [接続のテスト（Test Connectivity）] をクリックします。

- 手動でデバイスを追加するときの New Device ウィザード。手動定義によるデバイスの追加を参照してください。
- [Device Properties]。このページを開くには、デバイス セレクタ内のデバイスをダブルクリックするか、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択します。

ネットワークからデバイスを追加するときの [ログイン情報（Credentials）] ページで [次へ（Next）] または [完了（Finish）] をクリックすると、接続テストが自動的に実行されます。

関連項目

- デバイス接続のテスト （1 ページ）
- [Device Credentials] ページ
- デバイス プロパティの表示または変更

フィールド リファレンス

表 *1 : [Device Connectivity Test]* ダイアログボックス

要素	説明
接続プロトコル（Connectivity Protocol）	デバイスへのログインに使用されているトランスポート プロトコル。Security Managerは、デバイスのデバイス プロパティで指定されているプロトコルを使用します。通常は、[Device Communications] ページ（[Device Communication] ページを参照）で設定されているデフォルト プロトコルです。
Connectivity Status	テストのステータスと、テスト開始後の経過時間が表示されます。
[Details] ボタン	このボタンをクリックすると、テスト結果の詳細情報が表示されます。 • [合格したテスト（Passed tests）]：**show version** コマンドの出力（PIX ファイアウォール、適応型セキュリティアプライアンス（ASA）、ファイアウォール サービス モジュール（FWSM）、Cisco IOS ルータ、および VPN サービスモジュール（VPNSM）の場合）または**getVersion** コマンドの出力（IPS センサーおよびCisco IOS IPS センサーの場合）の詳細が表示されます。コマンド出力をコピーして、分析のためにファイルに貼り付けることができます。 • [Failed tests]：詳細なエラー メッセージです。
[Abort] ボタン	完了前に接続テストを停止します。

デバイス通信設定および証明書の管理

デバイスインベントリおよびポリシーをデバイスから直接検出する場合、またはファイルではなくデバイスに設定を展開する場合は、デバイスで使用されるトランスポートプロトコルを使用するように Security Manager を設定する必要があります。一部のデバイス タイプは、1 つのトランスポートプロトコルしかサポートしていません。この場合、選択を行う必要はありません。使用するプロトコルを選択できるデバイスもあります（Cisco IOS ルータなど）。

Security Managerには、各デバイス タイプで最もよく使用されるプロトコルであるトランスポート プロトコルのデフォルト設定が用意されています。これらの設定を変更するには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します（[Device Communication] ページを参照）。

ほとんどのユーザの場合、管理が必要となる通信設定は、SSL（HTTPS）通信に使用される証明書と、SSH接続に使用される公開キーです。デバイスの証明書およびキーは更新できます。この場合、Security Manager で古いコピーが保持されます。

次の各項では、証明書およびキーの管理と、デバイス通信のトラブルシューティングの方法について説明します。

- SSL 証明書：[Device Communication] ページで、デバイスから取得した証明書で自動的に証明書を置換するように Security Manager を設定できます。SSL 証明書ストアを手動で管理する場合は、HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （6 ページ）を参照してください。次のトピックでは、証明書エラーに関する詳細を説明します。
  - デバイス検出時にセキュリティ証明書が拒否される （7 ページ）
  - デバイス検出中の無効な証明書のエラー （8 ページ）
  - IPS 証明書の管理

ヒント　Security Manager を使用して管理するすべての PIX ファイアウォールおよび適応型セキュリティアプライアンスに、3DES/AES のライセンスがあることを確認してください。デバイスの通信要件についてを参照してください。

- SSH 公開キー：デフォルトでは、Security Manager により、公開キーが SSH 接続中に取得された新しい公開キーに置換されます。SSH 通信に関する問題が発生した場合は、SSH 接続の問題のトラブルシューティング （9 ページ）を参照してください。
- デバイス通信の一般的なトラブルシューティング：発生する可能性のあるその他の問題については、デバイス通信障害のトラブルシューティング （9 ページ）を参照してください。

複数証明書認証のサポート

バージョン 4.13 以降、Cisco Security Manager は、VPN 接続の複数証明書認証に関する ASA 9.7.1 の機能をサポートします。ASA のリリース 9.7.1 では、VPN クライアントのお客様に対する複数証明書認証のサポートが導入されました。その結果、クライアントは 2 つのクライアント証明書を使用してリモート VPN ユーザーを認証できるようになりました。2 つのクライアント証明書は、1 つのユーザー証明書と 1 つのマシン証明書の組み合わせ、または 2 つのユーザー証明書の組み合わせにすることができます。セキュリティを考慮して、2 つのマシン証明書による認証はサポートされていません。複数証明書認証は、SSL VPN と IPsec VPN の両方で機能します。

Cisco Security Manager 4.13 で複数証明書認証のサポートを有効にするには、AAA 認証方式を適切に指定し（[AAA] タブ（[Connection Profiles]）を参照）、DAP ポリシーを設定する必要があります（[DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）]を参照）。

HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加

（注） このトピックで説明されている方法に加えて、IPS デバイスでは IPS Certificates ユーティリティを使用して、Cisco Security Manager の証明書データストアにある証明書を管理できます。詳細については、IPS 証明書の管理を参照してください。

IPS、PIX、ASA、または FWSM の各デバイスとの通信、あるいは Cisco IOS ルータとの通信にトランスポート プロトコルとして SSL（HTTPS）を使用する場合は、デバイスの追加時にデバイス認証証明書を自動的に取得するように Security Manager を設定できます（[Device Communication] ページを参照）。

ヒント HTTPS 通信を正常に行うには、適切な証明書が必要です。適切な証明書がないと、Security Manager はデバイスと通信できず、設定は展開されません。自己署名証明書を使用している場合は、Security Manager が間違った証明書を使用してデバイスにアクセスしようとすると、デバイスによって新しい証明書が作成されることがあります。このため、常にデバイスから証明書を取得するように Security Manager を設定しておくことを推奨します。

ネットワーク セキュリティのレベルを上げるために、証明書を自動取得するように Security Manager を設定せずに、手動で証明書を追加することもできます。[デバイス通信（Device Communication）]ページで、デバイスタイプのデバイス認証を [証明書を手動で追加（Manually add certificates）] として設定します。

デバイスの証明書を手動で更新するには、デバイスから証明書を取得する方法が最も簡単です。デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。[ログイン情報（Credentials）] をクリックして [ログイン情報（Credentials）] ページを開き、[認証証明書のサムプリント（Authentication Certificate Thumbprint）] フィールドの右側にある [デバイスから取得（Retrieve From Device）] をクリックします。Security Manager により証明書が取得され、ユーザは証明書を受け入れるように要求されます。設定の展開中に証明書の問題が発生した場合には、この操作を行う必要があることがあります（証明書を自分で入力してこのフィールドに貼り付けることもできます）。

また、Security Manager からデバイスにログインせずに、証明書のサムプリントを手動で入力またはコピー アンド ペーストすることもできます。手動で追加した証明書を必要とするようにデバイス タイプを設定した場合、そのデバイスの SSL 証明書サムプリントを手動で入力するには、次の手順を使用します。

ヒント Cisco Security Manager では、**[メガメニュー（Megamenu）] > [サーバー管理（Server Administration）] > [サーバー（Server）] > [セキュリティ（Security）] > [単一サーバー管理（Single Server Management）] > [証明書セットアップ（Certificate Setup）]** で 2048 ビットの自己署名証明書を生成できます。

ヒント [メガメニュー（Megamenu）] にアクセスするには、サーバーのデスクトップにある [Cisco Security Manager] アイコンをダブルクリックしてログオンします。[メガメニュー（Megamenu）] にアクセスする別の方法は次のとおりです。Windows > [スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Security Manager] > [Cisco Security Manager] > [ログオン（log on）]。この 2 番目のナビゲーションパスは、Windows Server のインストール時の個人用設定の内容によって若干異なる場合があります。

はじめる前に

デバイスの証明書サムプリント（16 進ストリング）を取得します。

ヒント サムプリントをすぐに使用できない場合、ネットワークからデバイスを追加したときに表示されるエラーメッセージから、またはエクスポートファイルから、サムプリントをコピーできます。

ステップ 1 **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択し、目次から [デバイス通信（Device Communication）] を選択して [デバイス通信（Device Communication）] ページを開きます（[Device Communication] ページを参照）。

ステップ 2 [証明書の追加（Add Certificate）] をクリックして、[証明書の追加（Add Certificate）] ダイアログボックスを開きます（[Add Certificate] ダイアログボックスを参照）。

ステップ 3 デバイスの DNS ホスト名または IP アドレス、証明書サムプリントを 16 進形式で入力し、[OK] をクリックします。サムプリントが証明書ストアに追加されます。

ヒント 既存のサムプリントを消去するには、[Certificate Thumbprint] フィールドを空のままにしておきます。

デバイス検出時にセキュリティ証明書が拒否される

デバイスを検出しようとするとエラーが発生し、デバイスから取得したセキュリティ証明書が拒否されたことがエラーメッセージに示される場合、証明書を更新する必要があります。これには、次のいずれかの方法を使用できます。

- IPS デバイスの場合にのみ、**[管理（Manage）] > [IPS] > [IPS証明書（IPS Certificates）]** を選択して、証明書を同期します。また、証明書の再生成が必要になる場合があります。詳細については、IPS 証明書の管理を参照してください。
- 次のいずれかの操作を実行して、証明書に必要なサムプリントを手動で入力します。
  - **[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバイス通信（Device Communication）]** を選択します。[証明書の追加（Add Certificate）] をクリックし、デバイスの IP アドレスを入力してから、エラーメッセー

ジに表示されたサムプリントをコピーして [証明書サムプリント（Certificate Thumbprint）] フィールドに貼り付けます。

- デバイスを右クリックし、**[デバイスのプロパティ（Device Properties）] > [資格情報（Credentials）]** を選択します。エラー メッセージに表示されたサムプリントをコピーして、[Authentication Certificate Thumbprint] フィールドに貼り付けます。

[Add New Device] または [Add From Configuration File] オプションを使用して新しいデバイスを追加するとき、および再検出を実行するときは、サムプリントを手動で入力する必要があります。[Add New Device From Network] または [Add Device From File] オプションを使用して新しいデバイスを追加するときには、この操作は不要です。

- デバイスの追加時に証明書を自動的に取得するようにSSL証明書を設定します。IPS、ルータ、およびASA/PIX/FWSMデバイスには、それぞれ異なる設定を選択できます。これらの設定を行うには、**[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバイス通信（Device Communication）]** を選択し、[SSL証明書パラメータ（SSL Certificate Parameters）] グループを参照します。

関連項目

- HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加　（6 ページ）
- デバイス インベントリへのデバイスの追加
- デバイスを管理するための準備
- [Device Communication] ページ
- [Device Credentials] ページ

デバイス検出中の無効な証明書のエラー

デバイスと Security Manager の時刻設定が同期していない場合、（インベントリにデバイスを追加したり、インベントリ内にすでに存在するデバイス上のポリシーを再検出して）デバイス上のポリシーを検出しようとすると、証明書がまだ有効になっていないというエラー メッセージが表示されることがあります。

Security Manager サーバの設定時刻がデバイスの設定時刻よりも遅れている場合、有効期間の開始時刻が Security Manager の時刻設定よりも進んでいると、Security Manager はデバイス証明書を検証できません。設定されているタイム ゾーンがデバイスと Security Manager で同じであっても、夏時間（サマータイム）の設定が異なっていると、無効な証明書のエラーが発生します。この問題を解決するには、タイム ゾーンが同じであるかどうかにかかわらず、夏時間の時刻設定がデバイスと Security Manager で同じになっていることを確認します。夏時間の設定後に、デバイスのクロックを Security Manager と同期して、どちらにも同じ時刻が表示されるようにします。

最善の結果を得るために、デバイスと Security Manager で同じタイム ゾーンを設定し、証明書の検出後に、必要に応じてあとからタイム ゾーンを変更することを推奨します。

関連項目

- HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （6 ページ）
- IPS 証明書の管理
- デバイス インベントリへのデバイスの追加
- デバイスを管理するための準備

SSH 接続の問題のトラブルシューティング

トランスポート プロトコルとして SSH を使用するデバイスの場合、Security Manager は、各デバイスで使用する適切な SSH バージョン（1.5 または 2）を自動的に検出します。SSH バージョン 2 の接続中、Security Manager は暗号化アルゴリズムまたは暗号をデバイスと自動的にネゴシエートします。また、キーが変更された場合、Security Manager はデバイスの SSH 公開キーを自動的に上書きします。このため、通常は SSH 接続の問題が発生することはありません。

実際に SSH 接続の問題が発生した場合は、次の修正策を考慮してください。

- デバイスの公開キーが変更され、キーの問題が原因で SSH 接続が失敗する場合は、Security Manager サーバ上の Program Files/CSCOpx/MDC/be/tmp/.shh/known_hosts ファイルからデバイスのキーを削除してから、操作を再試行します。
- Security Manager は、デフォルトの暗号化アルゴリズムとして Triple Data Encryption Standard（3DES; トリプルデータ暗号規格）を使用します。このアルゴリズムが使用中のデバイスに適していない場合は、デバイスの設定を変更するか、DCS.ssh.encipher プロパティで適切なアルゴリズムを指定するように Program Files/MDC/athena/config/DCS.properties ファイルを更新します（不明な点があれば、Cisco TAC にお問い合わせください）。このファイルを変更した場合は、Security Manager デーモン マネージャを再起動する必要があります。

関連項目

- デバイスを管理するための準備
- [Device Communication] ページ
- [Device Credentials] ページ

デバイス通信障害のトラブルシューティング

Security Manager がデバイスと通信できない場合（デバイスのログイン、検出、展開、その他の処理で失敗するなど）、次の領域を確認し、問題を特定して解決してください。

- デバイスが動作していることを確認します。
- どのトランスポート プロトコルが選択されているかを確認します。デバイスで受け入れるように設定されているプロトコルを選択する必要があります。ほとんどのデバイスの場合、プロトコルは [デバイスプロパティ（Device Properties）] の [全般（General）] ページ

（[ツール（Tools）] > [デバイスプロパティ（Device Properties）] > [全般（General）] を選択）で選択します。IPS デバイスの場合は、デバイス プロパティの [Credentials] ページで [IPS RDEP] モードが選択されています。

K8 または K9 暗号イメージを持たない IOS デバイスの場合は、プロトコルとして Telnet を選択する必要があります。

デバイスを追加する方法によっては、デフォルト以外のトランスポートプロトコルを選択することもできます。デバイスクラスに対してデフォルトのトランスポートプロトコルを設定するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communications）] を選択します。

- [Device Properties General] ページで、ホスト名、ドメイン名、および IP アドレスが正しいことを確認します。デバイスのホスト名、アカウント、およびクレデンシャルのポリシーによって、デバイスで設定される実際の名前およびクレデンシャルが定義されます。ただし、ポリシーはデバイス通信には使用されません。デバイス通信に使用しているクレデンシャルに影響を与えるポリシーを変更した場合は、デバイスプロパティも手動で更新する必要があります。
- Security Manager サーバから DNS 名を解決できることを確認します。サーバ上の DNS 設定を修正する必要があることもあります。
- Security Manager でデバイスのクレデンシャルを調べて、クレデンシャルが正しいこと、およびサーバとデバイスの間にルートが存在することを確認します。デバイスを右クリックし、[デバイスプロパティ（Device Properties）] を選択します。次に [クレデンシャル（Credentials）] タブを選択して、[テスト接続（Test Connectivity）] ボタンをクリックします。接続が失敗した場合は、エラーメッセージを確認して、接続の問題かクレデンシャルの問題かを判断します。必要に応じて、デバイスプロパティ内のクレデンシャルを更新します。

デバイスを追加する方法でクレデンシャルが必要とされる場合は、新しいデバイスを追加するときに、New Device ウィザードでクレデンシャルが定義されます。次の点を考慮してください。

- SSH 接続および Telnet 接続にはプライマリ クレデンシャルが使用される。
- HTTP 接続および SSL 接続には、HTTP/HTTPS クレデンシャルが使用されます。ただし、[プライマリクレデンシャルを使用（Use Primary Credentials）] を選択した場合は例外で、これらの接続にもプライマリクレデンシャルが使用されます。
- バージョン 4.11 以降、Security Manager は、MD5 アルゴリズムを使用するデバイス SSL 証明書をサポートしていません。デバイスの SSL が MD5 アルゴリズムを使用している場合、デバイスを Security Manager に追加しようとすると、Security Manager にエラーが表示されます。このエラーは、セキュリティの脆弱性を理由として、JRE がデフォルトで MD5 アルゴリズムを無効にするために発生します。これを解決するには、デバイスの SSL 証明書により高度な暗号化アルゴリズムを使用する必要があります。
- バージョン 4.19 以降、Cisco Security Manager は、DES アルゴリズムを使用したデバイス SSL 証明書をサポートしていません。デバイスの SSL が DES アルゴリズムを使用してい

る場合、デバイスを Security Manager に追加しようとすると、Security Manager にエラーが表示されます。このエラーは、セキュリティの脆弱性を理由として、JRE がデフォルトで DES アルゴリズムを無効にするために発生します。これを解決するには、デバイスの SSL 証明書により高度な暗号化アルゴリズムを使用するか、以下の手順に従う必要があります。

- Security Manager サーバーサービスを停止します。
- 必ず MDC\vms\jre\lib\security\java.security プロパティのバックアップを取ってください。
- プロパティで、「jdk.tls.disabledAlgorithms=SSLv3, DES, MD5withRSA, DH keySize <1024, \ EC keySize < 224, RC4_40, 3DES_EDE_CBC」を見つけ、リストから「DES」を削除します。
- Security Manager サーバーサービスを再度開始します。

関連項目

- デバイス インベントリへのデバイスの追加
- デバイスの通信要件について
- デバイスを管理するための準備
- [Device Credentials] ページ

デバイス セレクタ内の赤い X マークの解決

デバイス ビューのデバイス セレクタ内でデバイスに赤い X マークが付いている場合は、3.2.0 以前の Security Manager リリースからのアップグレード中に、そのデバイスに対する Auto Update Server（AUS）または Configuration Engine サーバの割り当てが失われたことを意味しています。AUS と Configuration Engine は、3.1.x からのアップグレード中に移行されません。アップグレード後に次の手順を使用して、これらによって管理されるデバイスを再び割り当てる必要があります。

ステップ 1 デバイス ビューで、次のいずれかを実行します。

- デバイスセレクタから、赤い X アイコンの付いたデバイスを右クリックし、[サーバー情報の更新（Update Server Info）] を選択します。
- デバイス選択ツリー内の赤い X アイコンをクリックします。アップグレード プロセス後に、AUS および Configuration Engine の情報が移行されなかったという警告メッセージが表示されます。[はい（Yes）] をクリックして、これらのサーバーを手動で追加します。

[Device Server Assignment] ダイアログボックスが開きます。

ステップ 2 [使用可能なデバイス（Available Devices）] リストから、同じ AUS または Configuration Engine サーバーを使用するすべてのデバイスを選択し、[>>] をクリックして選択済みリストに移動します。[Available Devices] リストには、赤い X マークの付いた AUS または Configuration Engine により管理されるすべてのデバイスが含まれます。

ステップ 3 [Server] リストから、選択されたデバイスを管理する AUS または Configuration Engine を選択します。目的のサーバが表示されていない場合は、[Server Properties] ダイアログボックスを使用して、[+サーバーの追加...（+ Add Server...）] を選択して、インベントリにそのサーバーを追加します。

AUS または Configuration Engine サーバをインベントリに追加する方法については、Auto Update Server または Configuration Engine の追加、編集、または削除を参照してください。

ステップ 4 赤い X マークの付いたデバイスがなくなるまで、このプロセスを繰り返します。

展開のトラブルシューティング

展開プロセスは、Security Manager の使用中に問題が発生する可能性が高い領域の 1 つです。展開には、展開ジョブの成否を決めるさまざまなプロセスが多数関連しています。

- Security Manager 自体。
- ネットワークの安定性と可用性（リモート管理されるデバイスへのリンクを含む）。
- Security Manager が展開しようとするコマンドに影響を与えるネットワーク デバイスで使用中のオペレーティング システム バージョン固有のバグ（Security Manager は、これらのバグの影響を受けます）。
- デバイスでイネーブルにしたライセンス。多くのセキュリティ コマンドでは、固有のデバイス ライセンスが必要となるためです。
- デバイスでサポートされている特定の機能。Security Manager が常に事前にこれらを判別できるとはかぎりません。たとえば、デバイスに特定の最小 RAM がある場合にかぎってこれらの機能がサポートされるプラットフォームもあれば、特定のインターフェイス カードに対してだけ使用可能なインターフェイス設定もあります。
- 中間アプリケーション（AUS、Configuration Engine、TMS サーバなど）の正常な動作。

展開が失敗する場合は、展開ステータス ウィンドウ内のメッセージをよく調べてください。さらに、次の各項で、発生する可能性のあるいくつかの問題について説明します。

- Security Manager のデバイス メッセージへの応答方法の変更 （13 ページ）
- ASA 8.3+ デバイスのメモリ違反展開エラー （15 ページ）
- 展開後に Security Manager がデバイスと通信できない （16 ページ）
- ルーティング プロセスを組み込む VPN の更新 （17 ページ）
- ルータ ポリシーおよび VPN ポリシーを使用した展開方式の混合 （17 ページ）
- ルータへの展開の失敗 （19 ページ）

• Catalyst スイッチおよびサービス モジュールへの展開の失敗 （20 ページ）
• AUS により管理されるデバイスへの展開が失敗する （23 ページ）
• Configuration Engine により管理されるデバイスのセットアップのトラブルシューティング （24 ページ）

Security Manager のデバイス メッセージへの応答方法の変更

Security Manager には、デバイス設定時に表示される可能性のある多くの応答メッセージに対する、組み込みの応答があります。Security Manager でエラーとして処理されるメッセージが、無視してよいメッセージ、または通知メッセージとして処理してよいメッセージであることがあります。エラーが無視されるように展開ジョブを設定することもできますが、プロパティ ファイルを使用して、特定のメッセージを別の方法で処理するように Security Manager を更新することもできます。

エラーが無視されるようにプロパティ ファイルを設定するだけでは必ずしも十分ではないことを理解してください。[エラー時のダウンロードを許可する（Allow Download on Error）] チェックボックス（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] ページにある）がデフォルトで選択されていないため、展開が失敗する可能性があります。次の表に、展開中にエラーが発生した場合、[エラー時のダウンロードを許可する（Allow Download on Error）] オプションが選択されている場合と選択されていない場合、および [変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] オプションが選択されている場合と選択されていない場合の Security Manager の動作について説明します。

表 *2 : PIX* ファイアウォール、*ASA*、および *Cisco IOS* ルータでの *SSL* および *SSH* に対する展開デバイス エラー処理

Allow Download on Error	エラー発生	警告表現を使用してエラーを無視	展開ステータス	メモリ書き込みの実行
オン	対応	×	失敗しました（Failed）	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。
オン	対応	対応	[成功 (Success)]	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。
オン	非対応	該当なし	[成功 (Success)]	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。

Allow Download on Error	エラー発生	警告表現を使用してエラーを無視	展開ステータス	メモリ書き込みの実行
オフ	対応	×	Failed（「Deploy not Completed」メッセージ）	番号
オフ	対応	対応	SSL（ASA、PIX、IOS デバイス）：Failed SSH（IOS デバイス）：Success	SSL：なし。 SSH（IOS デバイス）：[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。
オフ	非対応	該当なし	[成功 (Success)]	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。

（注） SSL プロトコルを使用する Cisco IOS ルータでは、コマンド構文エラーでデバイスでの展開が停止されます。設定関連のエラーが発生しても、展開は停止されません。

Security Manager でのメッセージの処理方法を変更するには、インストール ディレクトリ（通常は c:\Program Files）の \CSCOpx\MDC\athena\config フォルダ内の DCS.properties ファイルを更新する必要があります。メモ帳などのテキストエディタを使用して、ファイルを更新します。

無視してよいメッセージを判断するには、次の手順を使用して、エラーの原因となった展開ジョブのトランスクリプトを調べるのが最も簡単です。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 エラー メッセージのあるジョブを選択します。

ステップ 3 [展開の詳細（Deployment Details）] タブの [トランスクリプト（Transcript）] ボタンをクリックして、トランスクリプトを開きます。

ステップ 4 無視してよいエラー テキストを特定します。

ステップ 5 DCS.properties ファイル内で適切な警告表現プロパティを見つけます。たとえば、PIX デバイスの場合、プロパティの名前は **dev.pix.warningExpressions** ですが、IOS デバイスの場合、プロパティの名前は **dev.ios.warningExpressions**です。

ヒント 逆に、プレフィックス Error が付かないデバイス応答をエラー メッセージとして表示することもできます。このためには、メッセージを [エラー表現（Error Expressions）] リスト（dev.pix.ErrorExpressions など）に追加します。

ステップ 6 エラーテキストを警告表現リストに追加します。警告メッセージは、汎用の正規表現ストリングにする必要があります。最後の表現を除いて、すべての表現を「$\」で区切る必要があります。たとえば、「Enter a public key as a hexadecimal number」というメッセージを無視する場合は、次の文字列を入力します。

.*Enter a public key as a hexadecimal number .*$

ステップ 7 CiscoWorks Daemon Manager を再起動します。

ASA 8.3+ デバイスのメモリ違反展開エラー

ASA ソフトウェア リリース 8.3+ では、旧バージョンの ASA ソフトウェアに比べ、必要なデバイス メモリが大幅に増加しています。最小メモリ要件を満たしていない ASA デバイスをアップグレードすると、アップグレードプロセスで問題が通知され、デバイスは、最小メモリ要件が満たされるまで syslog メッセージを定期的に送信します。

最小メモリ要件を満たしていない ASA デバイスは正常に動作できないため、インベントリへのデバイスの追加、およびインベントリからのポリシーの検出がユーザに許可されていても、Security Manager は設定をこれらのデバイスに展開しません。ただし、メモリを追加する前にポリシーをデバイスに展開しようとすると、デバイスが最小メモリ要件を満たしていないことを示す展開エラーが発生し、展開は失敗します。

エラーを解決する最善の方法は、メモリをデバイスに追加することです。ASA デバイスおよびメモリアップグレードの可能性の詳細については、https://www.cisco.com/c/ja_jp/products/security/asa-firepower-services/index.html を参照してください。

また、ASA ソフトウェア バージョンをダウングレードすることもできます。この場合は、インベントリからデバイスを削除してから再びインベントリに追加したあと、ポリシーを検出する必要があります。

未参照のオブジェクトを削除しようとしたときのエラー

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] ページで [未参照のオブジェクトグループをデバイスから削除（Remove Unreferenced Object Groups from Device）] オプションを有効にすると、Security Manager は、Security Manager によって管理または検出されたポリシーで使用されていないオブジェクトを展開中に削除します。Security Manager によって検出または管理されていないポリシーがそのようなオブジェクトを使用している場合、Security Manager は展開中にそのオブジェクトを削除しようとします。このような場合、オブジェクトが使用されているためオブジェクトを削除

できなかったことを示すトランスクリプトエラーが表示されて、展開が失敗します。正常に展開するには、[未参照のオブジェクトグループのデバイスからの削除を無効化（disable the Remove Unreferenced Object Groups from Device）] オプションを無効にします。

展開後に Security Manager がデバイスと通信できない

Security Manager で設定可能な、デバイスへのアクセスを妨げるようなポリシーが数多くあります。これがセキュリティのポイントであり、望ましくないホストがネットワークやネットワーク デバイスに侵入できないようにします。

ただし、間違って Security Manager サーバがデバイスからロックアウトされてしまうと、Security Manager が設定をデバイスに展開できなくなったり、デバイスを管理できなくなることがあります。展開後に Security Manager がデバイスにアクセスできなくなっていることが判明した場合は、デバイスが動作中であること、またはデバイスが正常に機能していることを確認してから、次のポリシーをよく調べて、ポリシーがロックアウトの原因となっていないかどうかを確認します。

- **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] または [ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]**：これらのポリシーを使用する場合は、ルールが Security Manager サーバーからの管理トラフィックを許可する必要があります。少なくとも、HTTP、HTTPS、SSH、および Telnet を許可することを検討してください。Security Manager に対する必要なアクセスを定義する共有ポリシーを作成して、すべてのデバイスにそれを適用することを検討してください。これらのポリシー内にルールを作成した場合、明示的に許可されていないトラフィックはすべて拒否されるという暗黙のルールがポリシーの最後に追加されます。
- [NATポリシー（NAT policies）]：デバイス上で変換対象の元のアドレスとしてローカルアドレスを使用していないことを確認します。このアドレスを変換すると、Security Manager とデバイス間で送信される管理トラフィックが変換されて、中断されることがあります。
- [ルータ上のデバイスアクセスポリシー（Device Access policies on routers）]：デバイスへのデバイスアクセスポリシーの割り当てを解除して再展開したあと、Security Manager がデバイスとの接続を解除することがあります。デバイス アクセス ポリシーを使用して、デバイスにアクセスするためのイネーブルパスワードを定義できます。このポリシーの割り当てを解除して再展開すると、パスワードがデバイスから削除されます。この場合は通常、デバイスによってパスワードがデフォルトに戻されます。ただし、Security Manager に認識されない追加パスワード（ライン コンソール パスワードなど）がデバイスに含まれる場合もあります。この追加パスワードが存在する場合は、デフォルトパスワードではなくこのパスワードに戻されます。この場合、Security Manager はこのデバイスを設定できません。このため、デバイス アクセス ポリシーを使用してデバイス上にイネーブル パスワードやイネーブル シークレット パスワードを設定する場合は、ポリシーの割り当てを解除してから、次の展開までに新しいポリシーを割り当ててください。
- [サイト間VPN（Site-to-Site VPNs）]：VPN 内のスポークとの通信を失った場合、Security Manager サーバーがハブの保護対象ネットワーク内からスポーク上の外部インターフェイスと通信するときに、問題が発生する可能性があります。ハブデバイスを Security Manager

に追加するときは、ハブの保護対象ネットワークの外側にある管理 IP アドレスを定義することを推奨します。

- **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [許可ホスト（Allowed Hosts）]**：IPS デバイスの場合、[許可ホスト（Allowed Hosts）] ポリシーでは、センサーに接続できるホストを指定します。このポリシーには、Security Manager サーバを含める必要があります。

関連項目

- デバイス通信障害のトラブルシューティング （9 ページ）
- デバイス通信設定および証明書の管理 （4 ページ）
- IPS 証明書の管理
- デバイスの通信要件について

ルーティング プロセスを組み込む VPN の更新

問題：（Site-to-Site VPN Manager またはルーティングポリシーを使用して）VPN トポロジによって使用されているルーティングプロセスへの変更を定義および展開した場合、行った変更は、デバイスで設定されている CLI コマンドには反映されません。

解決策：ルーティングプロセスを組み込む VPN トポロジ（GRE 完全メッシュなど）を検出した場合、Security Manager は、Site-to-Site VPN Manager に GRE Modes ポリシーおよび関連するルーティングポリシーを移入します。ただし、Security Manager でこれらのポリシーの 1 つに対して行われた変更が他のポリシーに自動的に反映されることはないため、展開後に予期しない結果が起こることがあります。したがって、Site-to-Site VPN Manager で保護対象の IGP に変更を行った場合は、[プラットフォーム（Platform）] > [デバイスでのルーティング（Routing in Device）] ビューを選択してデバイスのルーティングポリシーに必要な変更を行ってください。同様に、ルーティング ポリシーを直接変更した場合も、Site-to-Site VPN Manager で必要な変更を行ってください。

関連項目

- サイト間 VPN の管理：基本
- ルータの管理
- ファイアウォール デバイスの管理

ルータ ポリシーおよび VPN ポリシーを使用した展開方式の混合

ルータ プラットフォーム ポリシーおよび VPN ポリシーを、設定ファイルにすでに展開したあとで動作中のデバイスに展開すると、予期しない結果が発生することがあります。

この問題は、ルータ プラットフォーム ポリシーと VPN ポリシーを使用した展開方式（デバイスへの展開およびファイルへの展開）を混合して使用すると、発生することがあります。Security Manager では、これらのポリシー タイプに対する使用可能なすべての CLI コマンドが管理されるわけではないため、設定されたコマンドのスナップショットが維持され、他のすべてのコマンド（Security Manager でサポートされていないコマンドや、Security Manager で設定されていないポリシー内のサポート対象コマンドを含む）はデバイスでその状態のまま残ります。

展開が終わるたびに、Security Manager では、各デバイスに展開されたポリシーのスナップショットが作成されます。このスナップショットは、次の展開時に、デバイスに展開される設定変更リストを生成するために使用されます。デバイス 1 つにつき、一度に 1 つだけスナップショットが維持されます。

この例に示すように、ルータ プラットフォーム ポリシーと VPN ポリシーを使用した展開方式を混合すると、予期しない結果が発生することがあります。

1. 動作中のデバイスに対してルータ プラットフォーム ポリシー A を設定します。展開が完了すると、Security Manager によって、ポリシー A を持つそのデバイスのスナップショットが作成されます。
2. 次に、ポリシー A に置き換わるポリシー B を設定します。ただし、ポリシー B は、デバイスではなくファイルに展開します。この展開が完了すると、Security Manager によって、ポリシー A を持つ以前のスナップショットに置き換わるポリシー B を持つスナップショットが作成されます。ただし、ポリシー B をデバイスに展開していないため、ポリシー A を無効にするために必要な CLI コマンドは展開されていません。ポリシー A はデバイス上に展開されたままです。
3. 設定ファイル内の変更をデバイスにコピーせずに、再びデバイスに展開します。ポリシー A を持つスナップショットはもう存在しないため、Security Manager は、デバイスからポリシー A を無効にするために必要なコマンドを生成できません。

ポリシー A はルータ プラットフォーム ポリシーであるため、次のいずれの結果になる可能性があります。

- 最後の展開のポリシーによってポリシー A が上書きされる。
- デバイスで両方のポリシーが定義されることになる。
- 2 つのポリシーが共存できないため、展開が失敗する。

このため、動作中のデバイスでの作業中にファイルに展開する場合は、設定変更をファイルからデバイスにコピーしてから、デバイスへの追加の展開を実行することを強く推奨します。

関連項目

- サイト間 VPN の管理：基本
- ルータの管理

ルータへの展開の失敗

次に、設定を Cisco IOS ルータに展開するときに発生する可能性のある問題を示します。

インターフェイス設定の展開に失敗

問題：ルータへのインターフェイス設定の展開が失敗します。

解決策：Security Manager は、インターフェイスポリシーをサポートするための適切なタイプのインターフェイスカードまたは共有ポートアダプタ（SPA）がルータにインストールされているか、または適切なライセンスが設定されているかどうかを検証できません。インターフェイス ポリシーを変更せずにインターフェイス カードを追加または削除すると、展開エラーが発生することがあります。ベストプラクティスとして、Security Manager が適切なインターフェイス機能を検出できるように、インターフェイス モジュールまたは SPA を変更するたびに必ずルータからインベントリを検出することを推奨します。

レイヤ 2 インターフェイス定義の展開

問題：インターフェイスポリシーにレイヤ2インターフェイスの定義が含まれていると、展開に失敗します。

解決策：レイヤ2インターフェイスは、IP アドレスなどのレイヤ3インターフェイス定義をサポートしていません。レイヤ2インターフェイスにレイヤ3を定義していないことを確認してください。

VPN トラフィックが暗号化されずに送信される

問題：VPN を介して暗号化して送信する必要のあるトラフィックが、暗号化されずに送信されます。

解決策：VPN トラフィックに対して NAT を実行していないことを確認してください。VPN トラフィックに対してアドレス変換を実行すると、トラフィックが暗号化されなくなり、VPN トンネル経由で送信されなくなります。ダイナミック NAT ルールを定義する際は、IPSec に対して NAT を実行する場合でも、[Do Not Translate VPN Traffic] チェックボックスが選択されていることを確認してください（このオプションを設定しても、重複するネットワークから到着したアドレスの変換は行われます）。

このオプションは、サイト間 VPN に対してだけ使用できます。リモート アクセス VPN の場合は、VPN トラフィックを含むフローを明示的に拒否する ACL オブジェクトを作成し、この ACL を NAT ポリシー内にダイナミック ルールの一部として定義する必要があります。詳細については、[NAT] ページ - [Dynamic Rules]を参照してください。

ADSL または PVC ポリシーを展開できない

問題：ADSL または PVC ポリシーの展開が失敗します。

解決策：ポリシー定義で適切な ATM インターフェイス カード タイプを選択していることを確認してください。Security Manager は、適切なカード タイプが不明な場合、ポリシー定義を正しく検証できません。これにより、展開が失敗することがあります。

DHCP トラフィックが送信されない

問題：DHCP ポリシーをデバイスに展開した後も、DHCP トラフィックが送信されません。

解決策：デバイス上のアクセスルールによりブートストラッププロトコル（BootP）トラフィックがブロックされていないかどうかを確認してください。このようなルールが設定されていると、DHCP トラフィックは送信されません。

NAC がルータ上に実装されない

問題：NAC ポリシーがルータに展開されているにもかかわらず、ネットワーク アドミッション コントロールがルータ上に実装されません。

解決策：ルータ上のデフォルト ACL で、EAP over UDP トラフィックの NAC ポリシーで定義されているポートを経由する UDP トラフィックが許可されていることを確認してください。これは、NAC が Cisco Trust Agent（CTA）とネットワーク アクセス デバイス（NAD）の間の通信に使用するプロトコルです。CTA は、インストールされているエンドポイント デバイスのポスチャ クレデンシャルを提供する NAC クライアントであり、NAD は、検証のためにポスチャ クレデンシャルを AAA サーバに中継するデバイス（この場合はルータ）です。EAP over UDP トラフィックに使用されるデフォルト ポートは 21862 ですが、このポートは NAC ポリシーの一部として変更できます。デフォルト ACL により UDP トラフィックがブロックされている場合、EAP over UDP トラフィックも同様にブロックされるため、NAC は実装されません。

「Error Writing to Server」または「HTTP Response Code 500」メッセージとともに展開が失敗する

問題：Cisco IOS ルータへの展開が失敗し、「Error Writing to Server」または「Http Response Code 500」というエラーメッセージが表示されます。

解決策：SSL をトランスポートプロトコルとして使用して設定を Cisco IOS ルータに展開する場合、設定は複数の設定バルクに分割されます。この設定バルクのサイズは、プラットフォームによって異なります。Security Manager が、そのデバイスで設定されている SSL チャンクサイズを超える設定バルクを展開しようとすると、展開は失敗し、「Error Writing to Server」または「Http Response Code 500」というエラーメッセージが表示されます。

これを解決するには、次の手順を実行します。

1. Security Manager サーバで、インストール先ディレクトリ（通常は C:\Program Files）\CSCOpx\MDC\athena\config フォルダから DCS.properties ファイルを開きます。
2. **DCS.IOS.ssl.maxChunkSize=**<*value of the configuration bulk*> を見つけます。
3. 設定バルクの値を小さくします。
4. CiscoWorks Daemon Manager を再起動します。

Catalyst スイッチおよびサービス モジュールへの展開の失敗

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、拡張機能はサポートしていません。

次に、Catalyst スイッチおよび Catalyst 6500/7600 サービス モジュールに設定を展開するときに発生する可能性のある問題を示します。

インターフェイス設定の展開に失敗

問題：Catalyst 6500/7600 デバイスへのインターフェイス設定の展開が失敗します。

解決策：一部のインターフェイス設定（速度、デュプレックス、MTU 設定など）は特定のカードタイプに固有のものであり、展開の前に検証されません。展開が正常に行われるように、特定のカード タイプには適切な値を入力してください。

インターフェイス ポリシーの変更後に FWSM セキュリティ コンテキストの展開が失敗する

問題：セキュリティコンテキストとともに FWSM を追加し、そのポリシーを検出します。設定にはインターフェイス エイリアス（allocate interface コマンド）が含まれます。コンテキストのインターフェイス ポリシーを変更したあと、展開が失敗します。

解決策：FWSM に直接接続し、システム実行領域設定から、マッピングされているすべてのインターフェイス名を削除します。また、他のすべてのコンテキストで、マッピングされている名前へのインターフェイス参照を、インターフェイスの VLAN ID で置き換えます。これにより、Security Manager インベントリから FWSM を削除し、再検出できるようになります。

複数のコンテキストを持つ FWSM への展開が失敗する

問題：複数のセキュリティコンテキストを持つ FWSM に展開しようとすると、展開が失敗したり、FWSM のパフォーマンスが一時的に低下したりすることがあります。

解決策：問題は、Security Manager が設定を 1 つのデバイス上にある複数のセキュリティコンテキストに同時に展開しようとしている点です。設定変更によっては、これによりデバイスでエラーが発生して、展開が失敗することがあります。マルチ コンテキスト モードで FWSM を使用する場合は、Security Manager でマルチ コンテキストの FWSM に設定を展開する方法の変更 （22 ページ）の説明に従って、一度に 1 つずつコンテキストが設定され、設定がシリアルにデバイスに展開されるように、Security Manager を設定します。

内部 VLAN への展開の失敗

問題：Security Manager がデバイスの内部 VLAN リストの範囲に含まれる ID で VLAN を作成しようとすると、展開が失敗します。

解決策：Security Manager は内部 VLAN を検出できません。このため、デバイスの内部 VLAN リストの範囲外にある VLAN ID をユーザーが定義する必要があります。デバイスで **show vlan internal usage** コマンドを使用して、内部 VLAN のリストを表示します。

IDSM データ ポート VLAN の動作モードの変更時に展開が失敗する

問題：データポート VLAN の動作モードを [Trunk（トランク）]（IPS）から [Capture（キャプチャ）]（IDS）に変更しようとすると、展開が失敗し、次のエラーメッセージが表示されます。

Command Rejected: Remove trunk allowed vlan configuration from data port 2 before configuring capture allowed-vlans

解決策：一部のソフトウェアリリース（12.2(18)SFX4 など）には、正常な変更を妨げるバグがあります。この問題を解決するには、デバイスをリロードしてください。

多数の ACL が含まれる FWSM 設定で展開が失敗する

問題：設定に多数の ACL が含まれている場合、FWSM デバイスへの展開が失敗します。

解決策：これは、ACL コンパイル中に CPU 使用率が高くなったために発生する可能性があります。これを解決するには、次の手順を実行して、CPU 使用率のしきい値制限を再設定します。

1. Security Manager サーバで、インストール先ディレクトリ（通常は C:\Program Files）\CSCOpx\MDC\athena\config フォルダから DCS.properties ファイルを開きます。
2. **DCS.FWSM.checkThreshold=False** プロパティを見つけます。
3. 値を true に変更します（**DCS.FWSM.checkThreshold=True**）。
4. CiscoWorks Daemon Manager を再起動します。
5. 設定を再びデバイスに展開します。

値を true に設定したあと、検出および展開によって CPU 使用率が確認されます。CPU 使用率が DCS.FWSM.minThresholdLimit プロパティ内に設定されている値の範囲を超えていると、エラー メッセージが生成されます。デフォルト値は 85 です。

Security Manager でマルチ コンテキストの FWSM に設定を展開する方法の変更

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、拡張機能はサポートしていません。

FWSM で複数のセキュリティ コンテキストをホストするために、マルチ コンテキスト モードで動作するように Firewall Services Module（FWSM; ファイアウォール サービス モジュール）を設定した場合は、設定がシリアルに FWSM に展開されるように Security Manager を設定する必要があります。FWSM には、複数のコンテキストが同時に更新された場合に正常な展開を妨げる可能性のある、いくつかの制限があります。このため、シリアル展開を使用しない場合、展開が失敗することがあります。また、シリアル展開を使用しないと、展開中の FWSM のパフォーマンスが低下することもあります。

Security Manager でマルチ コンテキストの FWSM に設定を展開する方法を変更するには、DCS.properties ファイルを更新する必要があります。個々のセキュリティ コンテキストを追加するのではなく、FWSM 管理コンテキストを使用して FWSM コンテキストをインベントリに追加する必要があります。

次に、FWSM 展開をシリアルに行うためのエンドツーエンド プロセスについて説明します。

ステップ 1 通常は、管理コンテキストの管理 IP アドレスを使用して FWSM セキュリティ コンテキストを追加してください。コンテキストの管理は、管理コンテキストを介して行います。

各コンテキストの管理 IP アドレスを使用して FWSM のセキュリティコンテキストを個別に追加することも可能ですが、Security Manager は、個別に追加されたこれらのコンテキストを、同じ物理デバイス上でホ

スティングされるコンテキストとして認識できません。この場合、Security Manager ではコンテキストへのシリアル展開を実行できません。

セキュリティ コンテキスト管理 IP を使用して追加した FWSM セキュリティ コンテキストがある場合は、インベントリからコンテキストおよびFWSMを削除してから、管理コンテキストを使用してそれらを追加します（すべてのポリシーを検出します）。デバイス インベントリへのデバイスの追加を参照してください。

ヒント これらのコンテキストに対する未展開の変更を保持する必要がある場合、まず変更を展開して、デバイスの設定が完了していることを確認します。コンテキスト展開は、一度に 1 つずつ行ってください。

ステップ 2 Security Manager サーバーで Windows にログインし、インストールディレクトリ（通常は c:\Program Files）の \CSCOpx\MDC\athena\config フォルダ内の **DCS.properties** ファイルを編集します。メモ帳などのテキスト エディタを使用して、ファイルを更新します。

ステップ 3 DCS.properties ファイル内の DCS.doSerialAccessForFWSMVCs プロパティを見つけて、true に設定します。

DCS.doSerialAccessForFWSMVCs=true

ステップ 4 CiscoWorks Daemon Manager を再起動します。

AUS により管理されるデバイスへの展開が失敗する

Auto Update Server（AUS）を起動してから、完全に動作可能になる前に展開を実行すると、AUS により管理される複数のデバイスに展開するとき、展開が失敗することがあります。次の操作の実行後は、AUS が起動するまでに時間がかかります。

- 新規インストールまたはアップグレード
- 手動による再起動（停電後など）
- 手動による Cisco Security Manager Daemon Manager サービスの再起動

AUS が完全に動作可能になったかどうかを確認するには、Windows サービスのステータスを確認します。このためには、**[スタート（Start）] > [コントロールパネル（Control Panel）] > [管理サービス（Administrative Services）] > [サービス（Services）]** を選択してから、CiscoWorks AUS Database Engine サービスのステータスを確認します。このサービスがすでに開始されていれば、展開を再試行してください。

デバイス通信の展開

CSM 管理対象デバイスでデバッグが有効になっている場合、展開が失敗する

問題：CSM で管理されているデバイスで debug コマンドが有効になっていると、展開が失敗します。

解決策：展開時に、CSM によって管理されているデバイスで debug コマンドが有効になっていないことを確認します。

認識できない文字を入力すると展開が失敗する

問題：VPN トポロジの説明に認識できない文字が含まれていると、設定の展開とプレビューが失敗することがあります。

解決策：VPN トポロジの説明に認識されない文字を使用しないようにします。他のアプリケーションまたは Web ページからテキストをコピーする場合は、テキストをワードパッドに貼り付け、ワードパッドから CSM テキストボックスにテキストをコピーします。

Configuration Engine により管理されるデバイスのセットアップのトラブルシューティング

次の質問と回答で、Cisco Configuration Engine（CNS）により管理されるデバイスのセットアップ時に発生する可能性のある問題と、その解決方法について説明します。

質問：Configuration Engine の展開が失敗するのはなぜですか。

回答：Configuration Engine のすべてのバージョンが互換性をもって機能するわけではありません。Configuration Engine をデバイス インベントリに追加するとき、Security Manager では Configuration Engine 上で動作しているソフトウェア バージョンを確認できないため、サポートされていないバージョンをユーザがインベントリに追加してしまう可能性があります。この場合、展開しようとすると、予期しないエラーが発生することがあります。サポートされている Configuration Engine バージョンを実行していることを確認してください（バージョン情報については、http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html にあるこのバージョンの Security Manager のリリースノートを参照してください）。

質問：Configuration Engine の Web ページで IOS デバイスをクリックすると、InvalidParameterException が発生するのはなぜですか。

回答：これは想定された動作です。IOS デバイスの場合、Security Manager は展開ジョブを使用して、設定を Configuration Engine の IOS デバイスに関連付けるのではなく、設定を Configuration Engine に展開します。このため、Configuration Engine の Web ページでデバイス名をクリックしても、関連付けられた設定は表示されません。ASA/PIX デバイスの場合、Security Manager は設定を Configuration Engine のデバイスに関連付けます。このため、デバイス名をクリックすると、関連付けられた設定が表示されます。

質問：「com.cisco.netmgmt.ce.websvc.exec.ExecServiceException: [002-01003]]deviceName does not exists?」というエラーが発生するのはなぜですか。

回答：このエラーは、デバイスがまだ Configuration Engine に追加されていないことを示します。Security Manager でロールバックも展開も（いずれもデバイスが自動的に追加されます）実行しておらず、手動でも Configuration Engine にデバイスを追加していない場合、このエラーが表示されます。

質問：「com.cisco.netmgmt.ce.websvc.config.ConfigServiceException: [002-01003]]Device device id is not connected」というエラーが発生するのはなぜですか。

回答：回答は、実行しているセットアップのタイプによって異なります。

- イベントモードセットアップ：Security Manager の [デバイスのプロパティ（Device Properties）] ウィンドウで定義されている Configuration Engine デバイス ID が、ルータで設定されているデバイス ID と一致していることを確認してください（**cns id string** コマンドを使用）。
- Call Home モードセットアップ：このモードでは、デバイスは Configuration Engine に接続されません。このため、Configuration Engine を使用してデバイス設定を取得することが必要となる Security Manager 操作はいずれもサポートされません。これには、検出、プレビュー設定、表示実行設定、および接続テスト（IOS デバイスの場合はロールバックも）が含まれます。

質問：Configuration Engine により管理される ASA/PIX デバイスへの展開が正常に行われないのはなぜですか。

回答：いくつかの原因が考えられます。

- 設定に無効なコマンドが含まれている。このことをテストするには、Configuration Engine で ASA/PIX デバイスに関連付けられている設定をコピーして、デバイスに直接貼り付けます。
- **auto-update server** コマンドに無効なユーザー名およびパスワードが含まれている。
- 設定を ASA/PIX デバイスにポーリングするための待機時間が足りなかった。次回のポーリングサイクルがいつ開始されるかを確認するには、**show auto** コマンドを使用します。
- 以前に同じ ASA/PIX デバイスに対して Configuration Engine サーバを使用していて、現在の作業を開始する前に Configuration Engine サーバからそのデバイスを削除しなかった場合、新しい設定をユーザがデバイスに展開する前に、デバイスがサーバから以前の設定を取得した可能性があります。
- 上記のいずれによっても問題が解決しない場合は、ASA/PIX デバイスで Configuration Engine デバッグ モードを有効にし、次のポーリング サイクル終了後にログでエラーを確認します。

質問：Configuration Engine により管理される ASA/PIX デバイスへの展開が最初は成功したのに、2 回め以降は成功しないのはなぜですか。

回答：最初の展開でプッシュされた設定に自動更新機能に対する不適切な CLI コマンドが含まれていた場合、このようなエラーが発生することがあります。次の点をチェックします。

- **auto-update** コマンドで Configuration Engine サーバーのユーザー名およびパスワードが適切に定義されてることを確認します。
- デバイス CLI を使用して自動更新サーバーを設定する際に **name** コマンドを使用した場合、必要な **name** コマンドを含む FlexConfig を定義したことを確認します。このコマンドは Security Manager で直接サポートされていないため、FlexConfig が必要となります。こ

のため、このコマンドが検出されても、完全な設定には表示されません。Security Manager を使用して AUS ポリシーを設定する場合は、**name** コマンドは必要ありません。

質問：ASA/PIX デバイスで Configuration Engine をデバッグするにはどうすればよいですか。

回答：次の CLI コマンドを入力します。

```
logging monitor debug
terminal monitor
logging on
```

Configuration Engine サーバ上の PIX ログで関連情報を確認することもできます。

質問：IOS デバイスで Configuration Engine をデバッグするにはどうすればよいですか。

回答：次の CLI コマンドを入力します。

```
debug cns all
debug kron exec-cli
terminal monitor
```

イベント モードの場合は、Configuration Engine サーバ上のイベント ログで関連情報を確認することもできます。Call Home モードの場合は、Configuration Engine サーバ上の config server ログを確認してください。

質問：Configuration Engine を介した IOS デバイスの検出およびその設定の取得に失敗したのはなぜですか。

回答：デバッグモードで、次のエラーが表示されているかどうかを確認します。

*Feb 23 21:42:15.677: CNS exec decode: Unknown hostname cnsServer-lnx.cisco.com ... 474F6860: 72726F72 2D6D6573 73616765 3E584D4C error-message>XML 474F6870: 5F504152 53455F45 52524F52 3C2F6572 _PARSE_ERROR

次のことを確認してください。

- CNS コマンドで完全修飾ホスト名（ホスト名およびドメイン名）が使用されている。
- デバイスに **ip domain name** コマンドが含まれている。
- デバイスに、**ip host** コマンドと、Configuration Engine の完全修飾ホスト名およびその IP アドレスが含まれている。

質問：イベントモードルータが Configuration Engine の [デバイスの検出（Discover Device）] ページに表示されない、または Configuration Engine の Web ページに緑色で表示されるのはなぜですか。

回答：次のことを確認してください。

- ルータと Configuration Engine サーバで相互に ping が実行できることを確認します。
- 次のいずれかのコマンドを使用して、Configuration Engine サーバでイベント ゲートウェイが動作していることを確認します。

プレーンテキストモードのステータス：**/etc/init.d/EvtGateway**

SSL 暗号化モードのステータス：**/etc/init.d/EvtGatewayCrypto**

- **cns event** コマンドをクリアしてから、ポート番号を指定せずにコマンドを再入力します。

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。