Auto Update Server 4.2 ユーザ ガイド

Text Part Number: OL-25317-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Auto Update Server 4.2 ユーザ ガイド

CONTENTS

Cisco Security Manager 4.2 ユーザ ドキュメンテーション ガイド

78-20303-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Security Manager は、Cisco Security Management Suite の一部として、Cisco Self-Defending Network においてポリシーを包括的に管理および適用する機能を提供します。また、このスイートには、個別に使用できる Cisco Security Monitoring, Analysis, and Response System（MARS）も含まれています。

このマニュアルでは、Cisco Security Manager（Security Manager）、Auto Update Server（AUS）、および Performance Monitor に関する入手可能な資料について説明し、これらの資料へのリンクを示します。このマニュアルの構成は、次のとおりです。

ドキュメント セット

Cisco Security Manager のドキュメント セットには、次の URL からアクセスできます。

http://www.cisco.com/en/US/products/ps6498/tsd_products_support_series_home.html。

このドキュメント セットの内容は次のとおりです。

データ シート

データシートには、新機能を含め、Cisco Security Manager の機能と利点の概要が記載されています。

http://www.cisco.com/en/US/products/ps6498/products_data_sheets_list.html:

- *Cisco Security Manager 4.2 データ シート*

リリース ノート

リリース ノートには、製品概要、重要事項、および既知の問題が記載されています。

http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html:

- 『*Release Notes for Cisco Security Manager 4.2*』

インストレーション ガイドおよびアップグレード ガイド

これらのガイドには、導入を計画するための情報、Security Manager を Windows サーバ上や、ハイ アベイラビリティ設定またはディザスタ リカバリ設定でインストールするための要件と手順が記載されています。インストレーション ガイドは、Security Manager、AUS、および Performance Monitor のインス

トール、アップグレード、およびアンイストール手順について説明します。また、イストール前およびインストール後のガイドラインおよびトラブルシューティング情報も含まれています。

http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html:

- 『*Installation Guide for Cisco Security Manager 4.2*』

（注） インストールに関する重要事項については、『*Release Notes for Cisco Security Manager 4.2*』を参照してください。

- 『*High Availability Installation Guide for Cisco Security Manager 4.0-4.2*』

ユーザ ガイドとオンライン ヘルプ

Security Manager、AUS、および Performance Monitor の個々のユーザ ガイドおよびオンライン ヘルプには、概念および手順に関する情報が記載されています。

http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html:

- 『*User Guide for Cisco Security Manager 4.2*』

ヒント 状況依存オンライン ヘルプには、『*User Guide for Cisco Security Manager 4.2*』の内容が含まれており、[Help] メニューからアクセスするか、または任意のページやダイアログボックスの [Help] をクリックしてアクセスできます。

- 『*User Guide for Auto Update Server 4.2*』
- 『*User Guide for Cisco Performance Monitor 4.2*』

ビデオ

『Introduction to the Cisco Security Manager Event Viewer』ビデオには、Cisco Security Manager 4.0 で導入された Event Viewer 機能の簡単な紹介が収録されています。

- 『Video: Introduction to the Cisco Security Manager Event Viewer』

設定例

これらのドキュメントには、特定の設定シナリオに関する情報および Cisco Security Manager を使用してそれらのシナリオを実装する方法が記載されています。設定例は特定の Security Manager リリースに固有ですが、関心のある機能がサポートされている他のリリースで使用できます。

http://www.cisco.com/en/US/products/ps6498/prod_configuration_examples_list.html:

- 『Managing a Cluster of Cisco Security Manager 4.1 Servers』
- 『Getting Started with Cisco Security Manager 4.0』
- 『Configuring Botnet Traffic Filtering Using Cisco Security Manager 4.0』
- 『Applying Zone-based Firewall Policies in Cisco Security Manager』
- 『Migrating from 1800/2800/3800 ISRs to 1900/2900/3900 ISRs Using Cisco Security Manager 3.3.1』
- 『Configuring Cisco IOS Content Filtering Using Cisco Security Manager Version 3.3 in Cisco IOS Software Releases 12.4(15)XZ and Later』

サポートされるデバイスの表

このドキュメントには、Security Manager、AUS、および Performance Monitor でサポートされるデバイスとソフトウェアの完全なリストが記載されています。

http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html:

- 『*Supported Devices and Software Versions for Cisco Security Manager 4.2*』

Security Manager の起動方法

Security Manager をすばやく起動して実行するには、次の方法を推奨します。

- **インストールの計画を立てます。**

  インストール可能なアプリケーションを確認したり、インストールの計画を立てたりするには、まず次の URL で入手できる『*Installation Guide for Cisco Security Manager 4.2*』の「Overview」を参照することを推奨します。

  http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

- **Cisco Security Manager の概要を理解します。**

  製品概要については、次の URL で入手できる『*User Guide for Cisco Security Manager 4.2*』の「Product Overview」を参照してください。

  http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

ヒント Security Manager 機能の対話形式の概要については、Security Manager を最初に起動したときに開く対話形式の JumpStart チュートリアルを参照してください。JumpStart チュートリアルには、[Help] > [JumpStart] を選択してアクセスすることもできます。

- **Getting Started チェックリストを確認します。**

  Security Manager を最も効率的に起動して実行するには、次の URL で入手できる『*User Guide for Cisco Security Manager 4.2*』の「Getting Started with Security Manager」を参照してください。

  http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

- **基本的な設定を定義します。**

  Security Manager を使用して、展開方式など、作業環境をカスタマイズする多くのアプリケーション全体の設定を定義します。次の URL で入手できる『*User Guide for Cisco Security Manager 4.2*』の「Completing the Initial Security Manager Configuration」を参照してください。

  http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

- **ユーザの認証および認可を管理します。**

  - ユーザ ロールとユーザ権限を定義するには、次の URL で入手できる『*Installation Guide for Cisco Security Manager 4.2*』の「Managing User Accounts」の章を参照してください。

    http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

  - Security Manager を Cisco Secure ACS と統合するには、次の URL で入手できる『*Installation Guide for Cisco Security Manager 4.2*』の「Managing User Accounts」の章を参照してください。

    http://www.cisco.com/en/US/products/ps6498/prod_installation_guides_list.html.

- デバイスをブートストラップします。

  Security Manager とデバイスとの間の通信をイネーブルにするには、デバイスをインベントリに追加する前にデバイスに転送設定を行う必要があります。次の URL で入手できる『*User Guide for Cisco Security Manager 4.2*』の「Preparing Devices for Management」を参照してください。

  http://www.cisco.com/en/US/products/ps6498/products_user_guide_list.html.

はじめに

このマニュアルでは、Auto Update Server（AUS）を使用する方法について説明します。ネットワーク管理および構成に精通したユーザ、および PIX ファイアウォールと Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスのコンフィギュレーションと管理の責任者が対象です。

表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
コマンドまたはキーワード	**boldface** フォント
ユーザが値を指定する変数	*italic* フォント
セッション情報およびシステム情報の表示出力	`screen` フォント
本文中のメニュー項目の選択	[Option]>[Network Preferences]

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

製品マニュアル

Cisco Security Management Suite のマニュアル一覧を参照するには、http://www.cisco.com/en/US/products/ps6498/products_documentation_roadmaps_list.html にある、お使いの製品のマニュアル ロードマップにアクセスしてください。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

AUS の紹介

Auto Update Server（AUS）を使用すると、自動アップデート機能を使用する PIX ファイアウォールおよび Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）上でデバイス コンフィギュレーション ファイルやソフトウェア イメージをアップグレードする際に Web ベースのインターフェイスを利用できます。

自動更新機能を使用するセキュリティ アプライアンスは、定期的に AUS に接続して、デバイス コンフィギュレーション ファイルを更新し、デバイスおよびステータス情報を渡します。

（注） AUS およびその他の関連サーバ アプリケーションのインストール方法については、『*Installation Guide for Cisco Security Manager*』を参照してください。

次に、AUS の基本的な使用方法について説明します。

Auto Update Server の概要

Cisco Security Management Suite のコンポーネントである Auto Update Server（AUS）は、PIX ファイアウォール ソフトウェア イメージ、ASA ソフトウェア イメージ、PIX Device Manager（PDM）イメージ、Adaptive Security Device Manager（ASDM）イメージ、および PIX ファイアウォールと ASA の各コンフィギュレーション ファイルを更新するツールです。

ASA または PIX デバイスすべてのソフトウェアおよび ASDM/PDM イメージを更新できますが、コンフィギュレーション ファイルの更新には、Security Manager アプリケーションを使用してコンフィギュレーションを作成および展開する必要があります。

AUS は Security Manager でサポートされている任意の ASA または PIX デバイスおよびオペレーティング システムのバージョンで使用できます（デバイスのリストについては、Cisco.com の『*Supported Devices and Software Versions for Cisco Security Manager*』を参照してください）。ただし、デバイスはシングルコンテキスト モードで実行されている必要があります。セキュリティ コンテキストをホストするデバイスでは AUS は使用できません。AUS サーバ 1 台でデバイスを 1000 台まで管理できます。

AUS はスタティック IP アドレスを使用するデバイスまたは DHCP を介してダイナミックに IP アドレスを取得するデバイスで使用できます。DHCP を使用するデバイスでコンフィギュレーションを更新する場合は、AUS を使用してください。ネットワーク管理サーバでは IP アドレスを事前に知ることができないため、DHCP を使用してインターフェイス アドレスを取得するデバイスとは直接通信を開始できません。さらに、管理システムで変更が必要な場合にこれらのデバイスが実行されていないか、ファイアウォールおよび NAT 境界をまたいで実行されている可能性があります。

自動更新機能を使用するように設定した場合、デバイスがスタティックまたはダイナミック IP アドレスのいずれを使用していても、デバイスは定期的に AUS に接続します。デバイスによって AUS に現在の状態とデバイス情報が提供されます。それに対して AUS は、デバイスで実行するべきソフトウェア イメージおよびコンフィギュレーション ファイルのバージョン リストを提供してデバイスに答えます。デバイスによってファイル バージョンは、実行しているファイル バージョンと比較されます。バージョンが異なる場合は、デバイスによって新しいバージョンが AUS によって提供された URL からダウンロードされます。新しいファイル バージョンによってデバイスが最新の状態になると、デバイスによって AUS に状態およびデバイス情報が再度送信されます。

また、AUS を使用して、デバイスがサーバに接続するのを待たず、オンデマンドでデバイスのコンフィギュレーションまたはソフトウェア イメージを更新できます。この機能は、緊急の驚異に対応するためデバイスを更新する場合に有用です。

次のトピックでは、AUS に関する詳細を説明します。

NAT 境界をまたいだ AUS の展開

NAT 境界をまたいで企業ネットワーク内またはエンタープライズ DMZ 内のいずれかで AUS を展開する場合、AUS によって管理される PIX ファイアウォールおよび ASA デバイスは NAT 境界をまたぐことはできません。たとえば、NAT 境界をまたいだ DMZ で AUS を展開して、インターネット上でのみ展開されたデバイスを管理できますが、一部のデバイスが境界内でプライベート アドレスを使用し、一部のデバイスがインターネット上の外部にある場合、NAT 境界をまたいだ DMZ 上に AUS を展開できません。

AUS が NAT 境界をまたいでいる場合、デバイスが AUS への接続に使用するアドレスは多くの場合、AUS サーバの実際の IP と異なります。したがって、NAT 境界のパブリック側のデバイスが AUS のアクセスに使用する IP アドレスを指定する必要があります。たとえば、通常の設定は次のようになります。

AUS のパブリック アドレス 209.165.201.1 で、AUS の内部アドレス、192.168.0.1 に対応します。

デバイスはすべてパブリック アドレスに接続するため、[NAT Settings] ページの IP アドレスを 209.165.201.1 に設定する必要があります。NAT 境界がかかわらない場合は、ローカル マシンの IP アドレスであるデフォルト値のままにします。

（注）　デバイスはすべて NAT 境界をまたぐことはできません。NAT 境界をまたいだデバイスのコンフィギュレーションでは、AUS サーバが 2 台必要です。

ステップ 1　[Admin] > [NAT Settings] を選択します。[NAT Settings] ページが表示されます。

ステップ 2　[NAT Address] を選択して、サーバの IP アドレスに変換される IP アドレスを入力します。

（NAT を使用しない場合、または後で NAT の使用をやめる場合は [Actual Host Address] を選択します）

ステップ 3　[OK] をクリックして変更を適用します。

デバイスの AUS への追加

Security Manager を使用してデバイスに AUS を介してコンフィギュレーションを展開する場合、デバイスが正常に AUS に接続してコンフィギュレーションを取得した後、デバイスは自動的に AUS インベントリに追加されます。これは、デバイスを追加する通常の方法です。

ただし、AUS を使用して Security Manager によって管理されていないデバイスのソフトウェアおよび ASDM/PDM イメージの更新を管理する場合、またはトラブルシューティングする場合には、手動でデバイスを追加できます。詳細については、「デバイスを直接 AUS に追加する」を参照してください。

デバイスを AUS に追加する場合、Security Manager にはイネーブル パスワードおよび HTTP ユーザ名/パスワード（AUS では TACACS+ ユーザ名およびパスワードとして定義）が含まれます。これらのクレデンシャルは、デバイスで即時にコンフィギュレーションを更新するために [Update Now] アクションを実行する場合（即時自動更新）に使用されます。詳細については、「即時自動更新の要求」（P.2-6）を参照してください。

AUS データベースのバックアップおよび復元

AUS データベースをバックアップおよび復元するには、標準の Security Manager/CiscoWorks バックアップおよび復元ユーティリティを使用します。データベース バックアップは、AUS をサーバ新しいサーバにインストールして、データベースを復元する場合に使用できます。

これらのツールの使用方法については、『*User Guide for Cisco Security Manager*』を参照してください。

ユーザ ロールおよび権限について

AUS では、CiscoWorks Server または Cisco Secure Access Control Server（ACS）を使用した 2 種類の認証方式がサポートされます。AUS および Security Manager をインストールすると、使用する方式を設定できます。詳細については、付録 B「ユーザ ロールおよび権限」を参照してください。

自動アップデート サーバへのログインと終了

Auto Update Server には、Cisco Security Management Suite のホーム ページからログインできます。また、ホーム ページから Security Manager クライアントをインストールしたり、Common Services、Performance Manager、RME、および Common Services にインストールされたその他のソフトウェアにアクセスしたりできます。

手順

ステップ 1　Web ブラウザで、次のいずれかの URL を開きます。*AUSServer* は AUS がインストールされたコンピュータの名前を表します。いずれかのセキュリティ アラート ウィンドウで [Yes] をクリックします。

- SSL を使用しない場合は、http://*AUSServer*:1741 を開きます。
- SSL を使用する場合は、https://*AUSServer*:443 を開きます。

Cisco Security Management Suite のログイン画面が表示されます。ページ上で、JavaScript と cookie がイネーブルになっていることと、サポートされているバージョンの Web ブラウザを実行していることを確認します。Security Manager を実行するためのブラウザの設定方法については、『*Installation Guide for Cisco Security Manager*』を参照してください。

（注）　セキュリティを確保するためには SSL の使用を推奨します。また、Security Manager と AUS 間で適切に通信できるようにするため、AUS を実行するマシンのブラウザのセキュリティ モードをイネーブルにしてください。詳細については、「ブラウザとサーバ間のセキュリティの設定」（P.1-5）を参照してください。

ステップ 2　ユーザ名とパスワードを使用して、Cisco Security Management Suite サーバにログインします。初めてサーバをインストールする場合は、ユーザ名の **admin** と製品のインストール中に定義されたパスワードを使用してログインできます。

ステップ 3　ログインすると Cisco Security Management Suite のホームページが開きます。このホームページには、サーバにインストールされているスイートのアプリケーションがリストされます。AUS を実行するサーバでは、少なくとも次の機能を使用できます。製品のインストール内容によっては、他の機能も使用できる場合があります。

- Auto Update Server：この項目をクリックすると、Auto Update Server インターフェイスが開きます。
- Server Administration：この項目をクリックすると、CiscoWorks Common Services Server のページが開きます。CiscoWorks Common Services は、サーバを管理する基盤ソフトウェアです。このソフトウェアを使用して、サーバの保守とトラブルシューティングやローカル ユーザ定義などのバックエンド サーバ機能を設定して管理します。
- CiscoWorks リンク（ページ右上）：このリンクをクリックすると、CiscoWorks Common Services のホームページが開きます。このページからは AUS にもアクセスできます。

ステップ 4　アプリケーションを終了するには、画面右上にある [Logout] をクリックします。サーバのいずれかのウィンドウ（[AUS] ウィンドウまたは Security Manager ホーム ページなど）からログアウトすると、すべてのウィンドウからログアウトされます。

ログイン セッションは、非アクティブな状態が 2 時間続くとタイムアウトになります。

ブラウザとサーバ間のセキュリティの設定

Security Manager で AUS に適切にコンフィギュレーション ファイルを展開するため、Security Manager デバイス インベントリに追加する、AUS によって管理されるデバイスでは、ブラウザとサーバ間のセキュリティ モードがイネーブルである必要があります。

Common Services では、クライアント ブラウザと AUS 間および AUS とデバイス間でセキュアなアクセスを提供するため、SSL を使用します。Common Services では次でセキュアなアクセスを実現します。

- クライアント ブラウザおよび管理サーバ（AUS）間。
- AUS および Security Manager 間。
- AUS およびデバイス間。

SSL はアプリケーションレベルのプロトコルで、プライバシー、認証、およびデータ整合性により、データのセキュアなトランザクションを実現します。SSL は、証明書、公開キー、および秘密キーに依存しています。SSL によってクライアントとサーバ間の転送チャネルが暗号化されます。CiscoWorks サーバでは、クライアント ブラウザと管理サーバ間のセキュア アクセスの認証に証明書を使用します。

クライアント ブラウザと管理サーバ間および AUS と Security Manager 間のアクセスをセキュアにするには、SSL をイネーブルにしてください。ただし、スタンドアロン AUS アプリケーション（Security Manager に統合されていない AUS）を実行する場合は、SSL をディセーブルにできます。

手順

ステップ 1　Cisco Security Management Suite ホーム ページで、[Server Administration] をクリックして、Common Services を開きます。

ステップ 2　Common Services で、[Server] > [Security] > [Browser-Server Security Mode Setup] を選択します。

ステップ 3　[Enable] チェックボックスをオンにします。

ステップ 4　[Apply] をクリックします。

ステップ 5　CiscoWorks セッションからログアウトして、すべてのブラウザ セッションを終了します。

ステップ 6　CiscoWorks サーバ CLI を使用して Daemon Manager を再起動します。

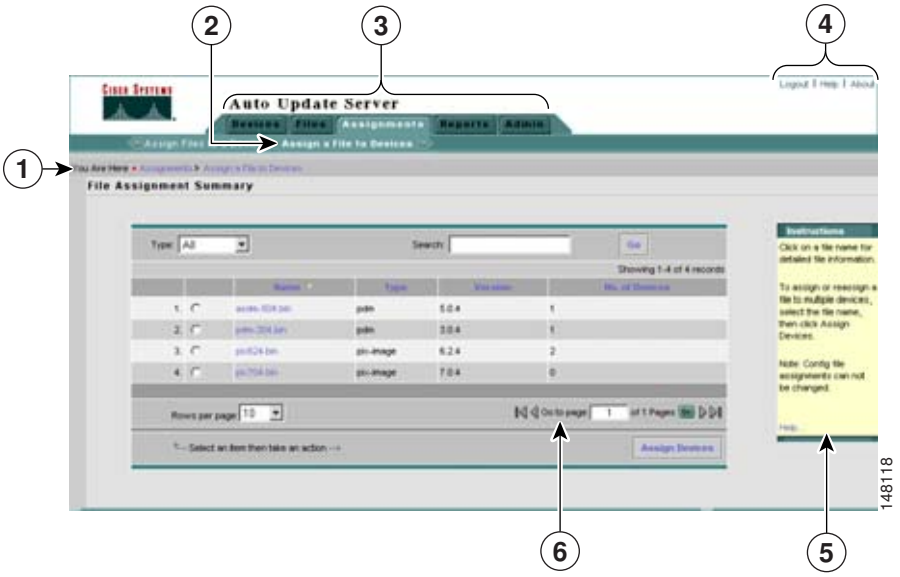
a. **net stop crmdmgtd** を入力

b. **net start crmdmgtd** を入力

ユーザ インターフェイスについて

Auto Update Server アプリケーションはブラウザ上で実行されます。アプリケーションの操作には、ブラウザのボタンではなく、インターフェイスのリンクおよびボタンを使用します。図 1-1 にインターフェイスの図と、詳細な説明を示します。

図 1-1　AUS GUI



参照番号	場所	説明
1	パス バー	表示されたページのコンテキストが表示されます。タブ、オプション、および現在のページが表示されます。リンクをクリックすると階層の中のそのページに移動できます。
2	オプション バー	選択したタブで利用可能なオプションが表示されます。オプションをクリックすると、そのページが表示されます。
3	タブ	製品の主な機能にアクセスできます。タブをクリックしてそのオプションにアクセスします。 • Devices：AUS によって管理されているデバイスに関する概要情報が表示されます。詳細については、第 2 章「デバイスおよび更新スケジュールの管理」を参照してください。 • Files：ソフトウェア イメージ、PDM と ASDM イメージ、およびコンフィギュレーション ファイルに関する情報を表示し、ソフトウェア イメージとデバイス マネージャ イメージを追加および削除できます。詳細については、第 3 章「ファイルの管理」を参照してください。 • Assignments：割り当て情報を表示し、デバイスからイメージへの割り当て、およびイメージからデバイスへの割り当てを変更できます。詳細については、第 4 章「ファイル割り当ての管理」を参照してください。 • Reports：レポートを表示します。詳細については、第 5 章「レポートの表示」を参照してください。 • Admin：NAT 設定を実行できます。詳細については、「NAT 境界をまたいだ AUS の展開」（P.1-2）を参照してください。

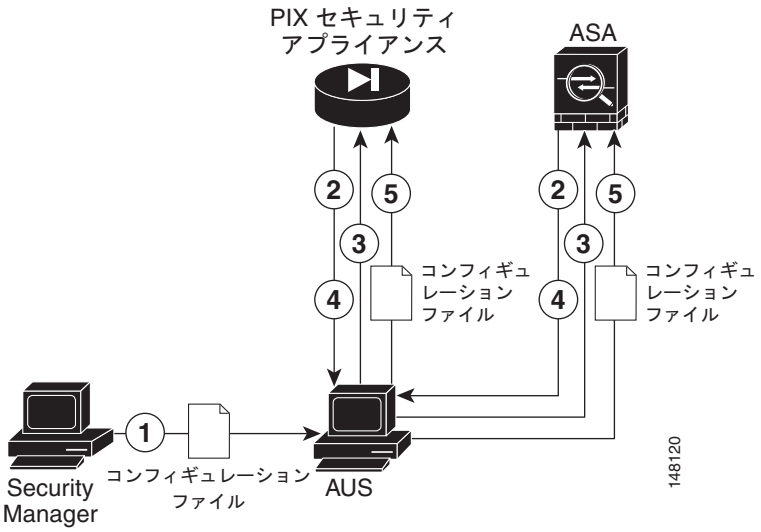
参照番号	場所	説明
4	リンク	次のリンクを使用できます。 • Logout：CiscoWorks からログアウトします。 • Help：新しいウィンドウを開きます。このウィンドウには、表示されたページの状況依存型ヘルプが表示されます。 • About：アプリケーションのバージョンを表示します。
5	指示ボックス	ページの使用方法の概要が表示されます。[Help] リンクをクリックすると追加情報を参照できます。
6	ページ	アプリケーション タスクを実行する領域が表示されます。 画像で示すような多くのページには表があります。表の項目を操作するには、左端のカラムにあるチェックボックスをオンにして、表の下にある実行したいアクションに対応するボタンをクリックします。 ソートするカラムの見出しをクリックすると、表をソートできます。検索文字列を入力して、[Go] をクリックすると、表の項目を検索できます。 また、表の上にあるフィールドを選択することで、表の項目をフィルタ（関心のある項目のみを表示する）できます。この操作によって、表のみがフィルタされ、データベースからデータは削除されません。

コンフィギュレーション ファイルの更新

Security Manager では、管理されている PIX ファイアウォールおよび ASA デバイスのコンフィギュレーションを更新する媒体として AUS が使用されます。これらのコンフィギュレーションの作成および展開には、Security Manager を使用する必要があります。AUS のみを使用して、コンフィギュレーションの展開を実行できません。

図 1-2 に仕組みを示します。また、後続の手順では、Security Manager および AUS を併用して、コンフィギュレーションを展開する方法を説明します。

図 1-2　Security Manager および AUS を使用したコンフィギュレーション ファイルの更新



参照番号	説明
1	Security Manager では、PIX ファイアウォールまたは ASA コンフィギュレーション ファイルを AUS に展開します。
2	設定されたスケジュールに基づいて、デバイスは更新のため、AUS に接続します。
3	AUS によってイメージ ファイルまたはコンフィギュレーション ファイル（または両方）の URL リストと一緒にデバイスで実行すべきファイルのチェックサムが送信されます。
4	デバイスによって AUS から受信したチェックサムが参照され、実行中のファイルが正しいことが検証されます。正しくない場合は、AUS にファイルが要求されます。
5	ファイルがデバイスにダウンロードされます。

手順

ステップ 1　AUS サーバを使用するようにデバイスを設定します。付録 C「AUS と連動するためのデバイスのブートストラップ」を参照してください。

ステップ 2　Security Manager で New Device ウィザードで利用できる任意の方法を使用してデバイスを追加します。

- [Add New Device] または [Add Device from File] を選択すると、ウィザード上でデバイスを管理する AUS サーバを選択できます。これは、ブートストラップ時に設定したサーバと同じです。AUS サーバがインベントリですでに定義されていない場合は、デバイスの追加時に定義できます。
- [Add Device from Network] または [Add from Configuration Files] を選択すると、ウィザード上で AUS サーバを選択できません。代わりに、デバイスを追加した後に、[Tools] > [Device Properties] を選択して、[General] タブで AUS サーバを選択します。AUS サーバがインベントリですでに定義されていない場合は、デバイスのプロパティから定義できます。

デバイスを管理する AUS サーバを指定する他に、次の情報をウィザードまたはデバイスのプロパティで定義してください。

- デバイス ID：デバイスをブートストラップする際、ID として使用する文字列を設定します。これは通常、デバイスのホスト名です。ウィザードまたはデバイスのプロパティのいずれかに ID を入力します。

- クレデンシャル：イネーブル パスワードを入力します。AAA を使用してデバイスへのアクセスを制御している場合、デバイスで要求される HTTP のユーザ名およびパスワードを入力してください。

デバイスおよび AUS サーバをインベントリに追加する手順、およびこの手順で説明したその他の Security Manager のタスクについては、Security Manager のオンライン ヘルプを参照してください。

ステップ 3　Security Manager でデバイスの AUS ポリシーを設定します。次のいずれかを実行します。

- 単一のデバイスのポリシーを設定します。デバイス ビューで、デバイスを選択し、デバイス ポリシー セレクタから [Platform] > [Device Admin] > [Server Access] > [AUS] を選択します。
- 同じ AUS を共有する多くのデバイスに割り当てることができる共有ポリシーを設定します。ポリシー ビューで、ポリシー タイプ セレクタから [PIX/ASA/FWSM Platform] > [Device Admin] > [Server Access] > [AUS] を選択します。[AUS] を右クリックし、[New AUS Policy] を選択してポリシーを作成するか、またはポリシー セレクタから既存のポリシーを選択してポリシーを変更します。[Assignments] タブを選択して、ポリシーを特定のデバイスに割り当てます。

必要に応じてデバイスに展開するコンフィギュレーションを実装するために、他のポリシーも設定します。

ヒント　AUS を使用するために Security Manager が他のファイルをデバイスにダウンロードする必要がある場合、その AUS には設定を正常に展開できません。たとえば、リモート アクセス VPN ポリシーによっては、プラグイン、Anyconnect クライアント、および Cisco Secure Desktop 設定を設定できます。このようなファイルは AUS に送信されません。このようなタイプのポリシーを設定する場合は、AUS を使用しないでください。

ステップ 4　Security Manager で、[Deploy to Device] 展開方式を使用して設定を展開します。Security Manager によってコンフィギュレーションが AUS に送信され、そこでネットワーク デバイスによって取得されます。

デバイスを初めて展開すると、Security Manager によってデバイスが AUS インベントリに追加されます。デバイスで AUS インターフェイスを使用して即時自動更新などの（Update Now アクション）操作を実行する前に、AUS を介してデバイスを正常に展開する必要があります。正常に展開するには、デバイスが AUS に接続して、コンフィギュレーションを取得する必要があります。

ステップ 5　コンフィギュレーションが更新されたことを確認します。Event Report を表示すると、AUS に接続したデバイスに関する情報を表示できます。「Event Report の表示」（P.5-4）を参照してください。

デバイスの更新には少し時間がかかる場合があります。更新情報が表示されない場合は、数分待機してから再度レポートを確認してください。それでも情報が更新されない場合は、付録 A「AUS のトラブルシューティング」を参照してください。

関連項目

- 「PIX セキュリティ アプライアンス、ASA、ASDM、および PDM イメージの更新」
- 「デバイスの AUS への追加」（P.1-3）
- 「デバイスを直接 AUS に追加する」

PIX セキュリティ アプライアンス、ASA、ASDM、および PDM イメージの更新

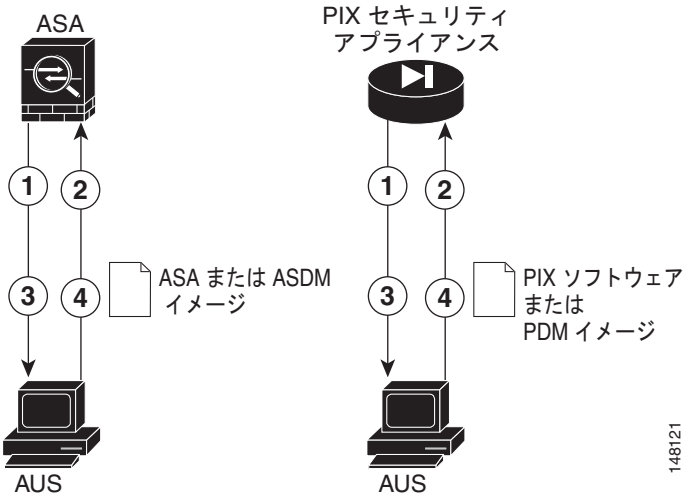
AUS を使用して PIX ファイアウォール ソフトウェア、ASA ソフトウェア、ASDM、および PDM イメージを更新できます。これらのイメージ更新には、Security Manager は使用しません。したがって、更新は Security Manager でコンフィギュレーションが管理されていないデバイスで実行できます。

ソフトウェアまたはデバイス マネージャ イメージを更新する際、次の点に注意してください。

- 新しい PIX または ASA ソフトウェア イメージがデバイスで実行されているコンフィギュレーション ファイルで使用できることを確認します。互換性のないソフトウェア イメージがダウンロードされると、デバイスによってすべてのサポートされないコマンドがドロップされ、コンフィギュレーション エラーが発生する場合があります。
- 新しい PDM または ASDM イメージが、デバイスで実行されている既存のソフトウェア イメージで使用できることを確認します。互換性のない PDM または ASDM イメージがダウンロードされると、PDM または ASDM が起動しない可能性があります。

（注）　AUS を使用して ASDM および ASA ソフトウェア イメージを管理するには、**asdm image** および **boot system** コマンドを使用して ASA デバイスをブートストラップする必要があります。詳細については、「起動するソフトウェア イメージおよび ASDM イメージのコンフィギュレーション」（P.C-3）を参照してください。

図 1-3　AUS を使用した PIX セキュリティ アプライアンス、ASA、ASDM、および PDM イメージの更新



参照番号	説明
1	設定されたスケジュールに基づいて、デバイスは更新のため、AUS に接続します。
2	AUS によってイメージ ファイルまたはコンフィギュレーション ファイル（または両方）の URL リストと一緒にデバイスで実行すべきファイルのチェックサムが送信されます。
3	デバイスによって AUS から受信したチェックサムが参照され、実行中のファイルが正しいことが検証されます。正しくない場合は、AUS にファイルが要求されます。
4	ファイルがデバイスにダウンロードされます。

手順

ステップ 1　AUS サーバを使用するようにデバイスを設定します。付録 C「AUS と連動するためのデバイスのブートストラップ」を参照してください。

ステップ 2　デバイスが Security Manager によるコンフィギュレーションの展開時、または「デバイスを直接 AUS に追加する」（P.2-3）の手順に従って手動で AUS に追加されたことを確認してください。

ステップ 3　イメージを AUS に追加します。詳細については、「ソフトウェア イメージの追加」（P.3-2）を参照してください。

ステップ 4　ファイルを 1 つ以上のデバイスに追加します。

- ファイルを単一のデバイスに追加する方法ついては、「単一デバイスへのファイルの割り当て / 割り当て解除」（P.4-3）を参照してください。
- ファイルを複数のデバイスに追加する方法ついては、「複数のデバイスへのファイルの割り当て / 割り当て解除」（P.4-4）を参照してください。

設定したスケジュールに基づいてセキュリティ アプライアンスは AUS に接続して、新しいソフトウェア、ASDM、または PDM イメージをダウンロードします。これらのアクションにはユーザの介入は不要です。

ソフトウェア イメージを更新すると、デバイスは自動的に再起動されます。再起動によって接続が切断され、ファイアウォールを通じたすべての既存のセッションは中断されます。

このことから、トラフィックのピークを避けた時間帯にセキュリティ アプライアンス イメージ更新してください。すべてのファイアウォールがピークを避けた時間帯に更新されるようにするため、制限のあるポーリング時間を設定できます。たとえば、3 時間のポーリング時間を設定して、更新が午前 12 時に実行されるように設定できます。ファイアウォールはすべて午前 12 時から午前 3 時の間に更新されます。ポーリング間隔の設定に関する詳細については、「セキュリティ アプライアンスのブートストラップ」（P.C-1）を参照してください。デバイスが Security Manager によって管理されている場合は、これらの設定を AUS ポリシーで設定してください（「コンフィギュレーション ファイルの更新」（P.1-7）を参照）。

ステップ 5　イメージが更新されたことを確認します。Event Report を表示すると、AUS に接続したデバイスに関する情報を表示できます。「Event Report の表示」（P.5-4）を参照してください。

デバイスの更新には少し時間がかかる場合があります。更新情報が表示されない場合は、数分待機してから再度レポートを確認してください。それでも情報が更新されない場合は、付録 A「AUS のトラブルシューティング」を参照してください。

CHAPTER 2

デバイスおよび更新スケジュールの管理

[Device] タブには、AUS に定義されたデバイスのリストが表示されます。このページで自動更新スケジュールの設定、即時更新の開始、更新のブロックを実行できます。次のトピックでは、[Device Summary] ページとその使用方法を説明します。

[Device Summary] ページの表示

[Device Summary] ページを表示するには、[Device] タブをクリックします。このページには、管理されているすべてのデバイスが表示され、デバイス ID、デバイス タイプ、デバイスが最新の状態であるか、およびデバイスが最後に AUS に接続した日時などのデバイスに関する情報が含まれます。[Device Summary] ページでは、デバイスの追加と削除、即時自動更新、更新スケジュールの設定と変更、PIX Device Manager（PDM）または Adaptive Security Device Manager（ASDM）アプリケーションの起動を実行できます。

カラム名をクリックすると、そのカラムを基準として表をソートできます。また、表に表示される情報をフィルタしたり、デバイスを検索したりできます。

表 2-1 では、[Device Summary] ページのフィールドについて説明します。

表 2-1　[Device Summary] ページ

要素	説明
Check box	機能を実行するデバイスを選択します。

表 2-1　[Device Summary] ページ （続き）

要素	説明
Device ID	AUS で識別に使用されるデバイスの名前です。ホスト名とは異なる場合があります。デバイス ID に使用される名前は、デバイスのブートストラップ時または Security Manager で AUS ポリシーを変更する際にユーザが決定します（「セキュリティ アプライアンスのブートストラップ」（P.C-1）を参照）。 デバイス ID をクリックすると、そのデバイスの詳細および割り当てられたファイルを示す表が新しいウィンドウで開かれます。詳細には、デバイス名、IP アドレス、シリアル番号、sysObjectID、ソフトウェア バージョン、PDM/ASDM バージョン、およびデバイスで利用できる RAM およびフラッシュ メモリ、この表の一部の情報などが表示されます。
Family	常に PIX を表示します。[Type] フィールドのモデル タイプを確認することで、デバイスが PIX ファイアウォールまたは ASA デバイスであるかを確認できます。
Type	デバイスのタイプです（PIX-535 または ASA-5540 など）。
Up-to-Date	デバイスで最新のファイルが実行されているかを示します。 • No（最新ではない）：デバイスでは、AUS に展開された最新のファイルが実行されていません。 • Up-to-date：デバイスで、AUS に展開された最新のファイルが実行されています。 • NA（該当しない）：デバイスは上記いずれのカテゴリにも一致しません。ファイルが割り当てられていない可能性があります。 • Not Contacted AUS：デバイスは一度も AUS に接続していません。
Update Type	デバイスが更新ファイルを受信するスケジュールされた方法です。 • Any Time：デバイスはデバイスのコンフィギュレーションで定義されたポーリング スケジュールに従って更新されます。 • One Time：デバイスはユーザによって定義された日時に基づいて 1 回のみ更新されます。 • Daily：デバイスはユーザによって定義された日時に基づいて毎日更新されます。 • Weekly：デバイスはユーザによって定義された日時に基づいて毎週更新されます。 • Never：デバイスは更新されません（更新がブロックされます）。
Last Contact	デバイスが最後に AUS 接続した日時です。
[Add] ボタン	このボタンをクリックすると、デバイスを表に手動で追加できます。Security Manager によって管理されているデバイスは追加する必要はありません。詳細については、「デバイスを直接 AUS に追加する」（P.2-3）を参照してください。
[Update Now] ボタン	このボタンをクリックすると、デバイスが即時に AUS に接続して、新しいファイルを取得します（即時自動更新）。詳細については、「即時自動更新の要求」（P.2-6）を参照してください。
[Launch Device Manager] ボタン	このボタンをクリックすると、PDM または ASDM アプリケーションを起動します（デバイスによって異なる）。Security Manager を使用してデバイスを管理している場合は、デバイス コンフィギュレーションの変更にこのアプリケーションを使用しないでください。詳細については、「デバイス マネージャの起動」（P.2-8）を参照してください。
[Update Schedule] ボタン	このボタンをクリックしてデバイスの更新スケジュールを設定します。詳細については、「更新スケジュールの設定」（P.2-4）を参照してください。

表 2-1　[Device Summary] ページ （続き）

要素	説明
[Update Any Time] ボタン	このボタンをクリックして、デバイスの既存の更新スケジュールをキャンセルし、デフォルトの Any Time スケジュールに変更します。このオプションでは、デバイスに定義されたポーリング時間が使用されます。詳細については、「更新スケジュールのキャンセル」（P.2-5）を参照してください。
Block Updates	このボタンをクリックして、選択したデバイスの自動更新をディセーブルにします。これにより更新スケジュールが Never に設定されます。詳細については、「自動更新のディセーブルまたはブロック」（P.2-7）を参照してください。
[Delete] ボタン	このボタンをクリックして、デバイスを削除します。デバイスを削除しても、Security Manager からは削除されません。詳細については、「デバイスの削除」（P.2-6）を参照してください。

デバイスを直接 AUS に追加する

Security Manager を使用してデバイスに AUS を介してコンフィギュレーションを展開する場合、デバイスが正常に AUS に接続してコンフィギュレーションを取得した後、デバイスは自動的に AUS インベントリに追加されます。これは、デバイスを追加する通常の方法です。

ただし、デバイスを手動で AUS に追加することもできます。この方法は次の目的の場合に便利です。

- AUS を使用して Security Manager によって管理されていないデバイスのソフトウェアおよび ASDM/PDM イメージの更新を管理する場合。
- 発生した問題をトラブルシューティングする場合。

手動で AUS に追加したデバイスは Security Manager インベントリに追加されません。

ヒント　デバイスの追加後はプロパティを編集できません。プロパティを変更する場合（クレデンシャルを更新する場合など）、デバイスを削除して再度追加してください。

手順

ステップ 1　[Devices] を選択します。[Device Summary] ページが表示されます（「[Device Summary] ページの表示」（P.2-1）を参照）。

ステップ 2　[Add] をクリックします。[Add Device] ページが表示されます。

ステップ 3　デバイスを識別する次の情報を入力します。

- [Device ID]：デバイスが AUS で自身を識別する ID です。

  ID のタイプは、デバイスで AUS 設定を実行する際（「セキュリティ アプライアンスのブートストラップ」（P.C-1）を参照）、または Security Manager でデバイスの [Platform] > [Device Admin] > [Server Access] > [AUS] ポリシーを設定する際に設定します。通常、ID はデバイスのホスト名です。
- [Auto Update Username and Password]：AUS との認証にデバイスが使用するユーザ名およびパスワードです。このユーザ アカウントは、ブートストラップ時に設定するか、Security Manager の AUS ポリシーから取得します。

ステップ 4　即時自動更新（[Update Now] ボタンを使用。「即時自動更新の要求」（P.2-6）を参照）を実行できるようにするには、[Request Auto Update Credentials] を設定します。次のいずれかを選択します。

- [None]：クレデンシャルがありません。デバイスで即時自動更新を実行できません。
- [TACACS]：デバイスへのアクセス制御に AAA を使用している場合は、デバイスの TACACS+ ユーザ名およびパスワードを入力します。
- [Enable Password]：デバイスでイネーブル モード、または特権 EXEC モードに入るパスワードです。このクレデンシャルはデバイス マネージャ（ASDM または PDM）を AUS から起動した場合にデバイス マネージャによって使用されます。

（注）　Security Manager でこれらの設定を実行した場合は、Security Manager から追加されたすべてのデバイスの TACACS+ およびイネーブル パスワードが AUS に提供されます。Security Manager では、HTTP クレデンシャルを TACACS+ クレデンシャルとして使用します。

ステップ 5　[OK] をクリックして、デバイスを追加します。

更新スケジュールの設定

AUS で使用するデバイスを設定する場合、デバイスが AUS への接続に使用するポーリング時間を設定します。デバイスに設定されたこのポーリング時間は、AUS で **Any Time** スケジュールと呼ばれます。つまり、デバイスはデバイスの設定に基づいて AUS にいつでも接続できます。

デフォルトのポーリング時間は 720 分です。Security Manager クライアントを使用して、デバイスに定義されたポーリング スケジュールを変更する手順については、「デバイスが AUS に接続するポーリング間隔の変更」（P.2-5）を参照してください。

AUS では、デバイスで定義されたスケジュールより優先されるスケジュールを作成できます。次の手順に従ってスケジュールを作成すると、「更新スケジュールのキャンセル」（P.2-5）の説明に従ってキャンセルすることができます。

手順

ステップ 1　[Devices] を選択します。[Device Summary] ページが表示されます（「[Device Summary] ページの表示」（P.2-1）を参照）。

ステップ 2　更新スケジュールを設定するデバイスを選択します。

ステップ 3　[Update Schedule] をクリックします。[Configure Update] ウィンドウが表示されます。

ステップ 4　[Allow Updates] リストからスケジュールのタイプを選択して、必須フィールドを入力します。次のオプションがあります。

- [One Time]：デバイスは 1 回のみ更新されます。日付を入力し、更新ウィンドウの開始時刻を HH:MM の形式（24 時間）で入力して、ウィンドウの時間を入力します。デバイスによって、このウィンドウ内で更新が要求されます。
- [Daily]：デバイスは毎日更新されます。更新ウィンドウの開始時刻と時間を入力します。
- [Weekly]：デバイスは週に一度更新されます。更新ウィンドウの開始時刻と時間を入力して、更新が発生する曜日を選択します。

- [Never]：デバイスは更新されません。これにより、自動更新がブロックされ、[Device Summary] ページで [Block Updates] ボタンをクリックした場合と同じ結果が得られます。詳細については、「自動更新のディセーブルまたはブロック」（P.2-7）を参照してください。

ステップ 5　[OK] をクリックします。[Device Summary] ページに戻り、新しいスケジュールが [Update Schedule] カラムに表示されます。

デバイスが AUS に接続するポーリング間隔の変更

AUS によって定義されているスケジュール（Any Time スケジュールと呼ばれる）の代わりに、デバイスで定義されたスケジュールに基づいてデバイスの AUS への接続を許可している場合、Security Manager クライアントを使用してポーリング スケジュールを変更できます。

手順

ステップ 1　Security Manager クライアントで次のいずれかの手順を実行します。

- （デバイス ビュー）デバイスで共有ポリシーを使用していない場合は、デバイスを選択して [Platform] > [Device Admin] > [Server Access] > [AUS] ポリシーを選択します。
- （ポリシー ビュー）デバイスで共有ポリシーを使用している場合は、[PIX/ASA/FWSM Platform] > [Device Admin] > [Server Access] > [AUS] ポリシー フォルダからポリシーを選択します。

ステップ 2　頻度または特定のスケジュールに基づくことができる [Poll Type] を選択して、スケジュール、ポーリング回数、および再試行回数を定義します。

コンフィギュレーションを展開して、デバイスが AUS から更新を取得するまで変更は適用されません。したがって、このポリシーを展開してから最初に実行される展開は、前回のバージョンのポリシーに基づきます。

更新スケジュールのキャンセル

AUS でデバイスの更新スケジュールを設定した場合、キャンセルすることができます。これにより、更新スケジュールが Any Time に変更されます。つまり、デバイスではデバイスのコンフィギュレーションで定義されたポーリング時間を使用して、AUS に接続して更新します。

スケジュールをキャンセルする以外に次を実行できます。

- デバイスで更新の受信を停止する場合は、「自動更新のディセーブルまたはブロック」（P.2-7）を参照してください。
- デバイスで更新を即時に受信する場合は、「即時自動更新の要求」（P.2-6）を参照してください。

手順

ステップ 1　[Devices] を選択します。[Device Summary] ページが表示されます（「[Device Summary] ページの表示」を参照）。

ステップ 2　更新スケジュールをキャンセルするデバイスを選択します。

ステップ 3　[Update Any Time] をクリックします。AUS から更新スケジュールを削除するか確認されます。

デバイスの削除

AUS でデバイスを管理する必要がなくなった場合、AUS からデバイスを削除できます。Security Manager で引き続きデバイスを管理する場合は、デバイスが AUS を使用しないようにしたまま、コンフィギュレーションを展開すると、AUS にデバイスを再び追加することができます。

デバイスは AUS と Security Manager で個別に削除する必要があります。デバイスを一方のアプリケーションから削除しても、もう一方のアプリケーションからは削除されません。

手順

ステップ 1　[Devices] を選択します。[Device Summary] ページが表示されます（「[Device Summary] ページの表示」を参照）。

ステップ 2　削除するデバイスを選択します。

ステップ 3　[Delete] をクリックします。デバイスを削除するか確認されます。

即時自動更新の要求

場合によっては、スケジュールに従って AUS に接続されるのを待たず、デバイスで確実に最新のファイルが実行されているようにするため、デバイスを即時に AUS に接続する必要があります。たとえば、ネットワークのセキュリティが侵害された場合にデバイスの AUS への接続を要求したり、Security Manager でコンフィギュレーションを更新し、AUS に展開したにもかかわらず、デバイスがコンフィギュレーションを許容される時間内に取得するようにスケジュールされていない場合などが挙げられます。

即時自動更新を実行するには、次の要件を満たしていることを確認してください。

- 更新スケジュールが Never ではない。Never の場合は、最初にデバイスを選択して、[Update Any Time] をクリックするか、更新スケジュールを定義します。
- デバイスの HTTPS ポートがデフォルト 443 である。デバイスの HTTPS ポート番号をデフォルトの 443 以外の任意の番号に変更すると、即時自動更新を実行できません。スケジュールされた間隔以外にデバイスで AUS に接続する場合は、デバイスの HTTPS ポート番号をデフォルト値のままにします。
- TACACS+ クレデンシャル（AAA 認証を使用する場合）またはイネーブル パスワードがデバイスに定義されている。これらのクレデンシャルは追加したデバイスについて Security Manager によって自動的に AUS に提供されます。ただし、Security Manager で設定した場合に限ります（Security Manager では、HTTP クレデンシャルを TACACS+ クレデンシャルとして使用します）。詳細については、「デバイスを直接 AUS に追加する」（P.2-3）を参照してください。

- デバイスが直接接続でき、NAT 境界をまたいでいない。
- デバイスですでに AUS に正常に接続できている。

手順

ステップ 1　[Devices] を選択します。[Device Summary] ページが表示されます（「[Device Summary] ページの表示」を参照）。

ステップ 2　即時更新するデバイスを選択します。

ヒント　大量のデバイスを即時 AUS に接続するように要求すると、パフォーマンスの問題が発生します。大量のデバイスを更新する場合は、小規模のグループ単位で行ってください。

ステップ 3　[Update Now] をクリックします。要求の確定が求められます。

AUS では、最初に TACACS+ クレデンシャル（HTTP ユーザ名およびパスワード）を使用してデバイスへの接続が試行されます。接続に失敗すると、イネーブル パスワードが使用されます。

Event Report を使用して、正常に更新されたかを確認できます（[Reports] > [Events] を選択）。詳細については、「Event Report の表示」（P.5-4）を参照してください。

自動更新のディセーブルまたはブロック

デバイスの自動更新をディセーブルまたはブロックできます。更新をディセーブルにすると、デバイスのコンフィギュレーションは変更されません。更新スケジュールを作成するか（「更新スケジュールの設定」（P.2-4）を参照）、デバイスでいつでも更新を取得できるようにすることで（[Device Summary] ページでデバイスを選択し、[Update Any Time] をクリック）更新を再度イネーブルにできます。

手順

ステップ 1　[Devices] を選択します。[Device Summary] ページが表示されます（「[Device Summary] ページの表示」を参照）。

ステップ 2　自動更新をディセーブルにするデバイスを選択します。

ステップ 3　[Block Updates] をクリックします。更新スケジュールをブロックするか確認されます。これにより、更新スケジュールが Never に変更されます。

デバイス マネージャの起動

デバイスに ASDM または PDM がインストールされている場合、AUS から ASDM または PDM を起動して、デバイスの特定の設定を表示または変更できます。デバイスのデバイス マネージャを起動するには、デバイスがすでに AUS に接続している必要があります。デバイスの設定に Security Manager を使用している場合は、コンフィギュレーションの変更に ASDM または PDM を使用しないでください。

（注）　デバイスの HTTPS ポート番号をデフォルトの 443 以外の任意の番号に変更していると、デバイス マネージャを起動できません。デバイス マネージャを AUS 自体から起動する場合は、デフォルト値の 443 を変更しないでください。

手順

ステップ 1　[Devices] を選択します。[Device Summary] ページが表示されます（「[Device Summary] ページの表示」（P.2-1）を参照）。

ステップ 2　デバイス マネージャを起動するデバイスを選択します。

ステップ 3　[Launch Device Manager] をクリックします。

アプリケーションにログインするよう要求され、デバイス マネージャが新しいウィンドウで開きます。使用方法については、アプリケーションのオンライン ヘルプを参照してください。

CHAPTER 3

ファイルの管理

AUS では、PIX ソフトウェア イメージ、ASA ソフトウェア イメージ、PDM イメージ、ASDM イメージ、ASA コンフィギュレーション ファイル、および PIX コンフィギュレーション ファイルという 6 タイプのファイルを管理できます。

次のトピックでは、AUS を使用して、さまざまなタイプのファイルを管理する方法について説明します。

[File Summary] ページの表示

[Files] タブをクリックして、[File Summary] ページ表示します。このページでは、AUS データベースにあるファイルに関する情報が表示されます。このページから、次の操作を実行できます。

- ソフトウェア イメージ、ASDM イメージ、および PDM イメージの追加または削除
- コンフィギュレーション ファイルの表示または削除

カラム名をクリックすると、そのカラムを基準として表をソートできます。また、表に表示される情報をフィルタしたり、ファイルを検索したりできます。

AUS を使用して ASDM および ASA ソフトウェア イメージを管理するには、**asdm image** および **boot system** コマンドを使用して ASA デバイスをブートストラップする必要があります。詳細については、「起動するソフトウェア イメージおよび ASDM イメージのコンフィギュレーション」（P.C-3）を参照してください。

[File Summary] ページの要素に関する説明については、表 3-1 を参照してください。

表 3-1　[File Summary] ページ

要素	説明
Check box	機能を実行するファイルを選択します。
Name	ファイルの名前です。 名前をクリックすると、ファイルおよびファイルに割り当てられたデバイスに関する情報の表が表示されます。

表 3-1　[File Summary] ページ （続き）

要素	説明
Type	次のファイル タイプを選択できます。 • pix-config：ASA または PIX コンフィギュレーション ファイル。 • pix-image：ASA または PIX ソフトウェア イメージ ファイル。 • asdm-image：ASDM ソフトウェア イメージ。 • pdm-image：PDM ソフトウェア イメージ。
Version	ファイルのソフトウェア バージョンです。コンフィギュレーション ファイルの場合、コンフィギュレーションが作成された OS バージョンが表示されます。
Create Timestamp	ファイルが AUS に追加された日時です。
No.of References	ファイルに割り当てられたデバイスの数です。デバイスの割り当てに関する詳細については、第 4 章「ファイル割り当ての管理」を参照してください。
[Add] ボタン	このボタンをクリックして、ファイルを追加します。詳細については、「ソフトウェア イメージの追加」（P.3-2）を参照してください。
[View Config] ボタン	このボタンをクリックして、選択したコンフィギュレーション ファイルを表示します。詳細については、「コンフィギュレーション ファイルの表示」（P.3-3）を参照してください。
[Delete] ボタン	このボタンをクリックして、選択したファイルを削除します。詳細については、「ソフトウェア ファイルの削除」（P.3-3）を参照してください。

ソフトウェア イメージの追加

ASA または PIX ソフトウェア イメージ、Adaptive Security Device Manager（ASDM）ソフトウェア イメージ、または PIX Device Manager（PDM）ソフトウェア イメージを追加できます。

（注）　コンフィギュレーション ファイルは AUS から追加できません。デバイスにコンフィギュレーションを導入するには、Security Manager を使用してください。詳細については、「コンフィギュレーション ファイルの更新」（P.1-7）を参照してください。

はじめる前に

Cisco.com からファイルをお使いのワークステーションにダウンロードします。シスコの命名規則に従わないファイルは AUS に追加できないため、ファイル名は変更しないでください。

手順

ステップ 1　[Files] を選択します。[File Summary] ページが表示されます（「[File Summary] ページの表示」（P.3-1）を参照）。

ステップ 2　[Add] をクリックします。[Add File] ページが表示されます。

ステップ 3　追加するファイルのタイプを次から選択します。

- pdm：PIX Device Manager（PDM）ソフトウェア イメージ。
- asdm：Adaptive Security Device Manager（ASDM）ソフトウェア イメージ。

- pix-image : ASA または PIX ソフトウェア イメージ。

ステップ 4　[Browse] をクリックして、追加するファイルを選択し、[Open] をクリックします。

ステップ 5　[OK] をクリックして、ファイルを追加します。通常のシスコ命名規則に従わないファイルを追加しようとしても、ファイルは追加できません。

ソフトウェア ファイルの削除

不要になったファイルはすべて削除できます。デバイスに割り当てられたファイルを削除すると、デバイスの割り当てもすべて削除されます。ファイルを削除する前に、デバイスを他のファイルに割り当てることを検討してください（第 4 章「ファイル割り当ての管理」を参照）。

ファイルを削除しても、ファイルをダウンロードした割り当て済みデバイスからファイルが削除されることはありません。

手順

ステップ 1　[Files] を選択します。[File Summary] ページが表示されます（「[File Summary] ページの表示」（P.3-1）を参照）。

ステップ 2　削除するファイルを選択します。

ステップ 3　[Delete] をクリックします。削除の確認が求められます。

コンフィギュレーション ファイルの表示

Security Manager によって AUS に展開されたコンフィギュレーション ファイルを表示することができます。

手順

ステップ 1　[Files] を選択します。[File Summary] ページが表示されます（「[File Summary] ページの表示」（P.3-1）を参照）。

ステップ 2　表示するコンフィギュレーション ファイルを選択します。同時に実行できるコンフィギュレーションは、1 つのみです。

ステップ 3　[View Config] をクリックします。コンフィギュレーション ファイルが新しいウィンドウで開きます。

CHAPTER 4

ファイル割り当ての管理

[Assignments] タブのオプションを使用して、デバイスおよびファイルの割り当てを管理します。たとえば、新しい ASA ソフトウェア イメージが利用可能な場合、ファイルをダウンロードして、AUS に追加し、1 つ以上のデバイスに割り当てられます（イメージの追加に関する詳細については、「ソフトウェア イメージの追加」（P.3-2）を参照してください）。

単一のデバイスに複数のファイルを割り当てることができます。たとえば、ASA ソフトウェア イメージ、ASDM イメージ、および ASA コンフィギュレーション ファイルを単一の ASA デバイスに割り当てることができます。図 4-1 を参照してください。

また単一のファイルを複数のデバイスに割り当てることもできます。たとえば、同じ ASA ソフトウェア イメージまたは ASDM イメージを複数の ASA デバイスに割り当てることができます。図 4-2 を参照してください。

（注） コンフィギュレーション ファイルを複数のデバイスに割り当てることはできません。

図 4-1　　複数のファイルを単一のデバイスに割り当てる

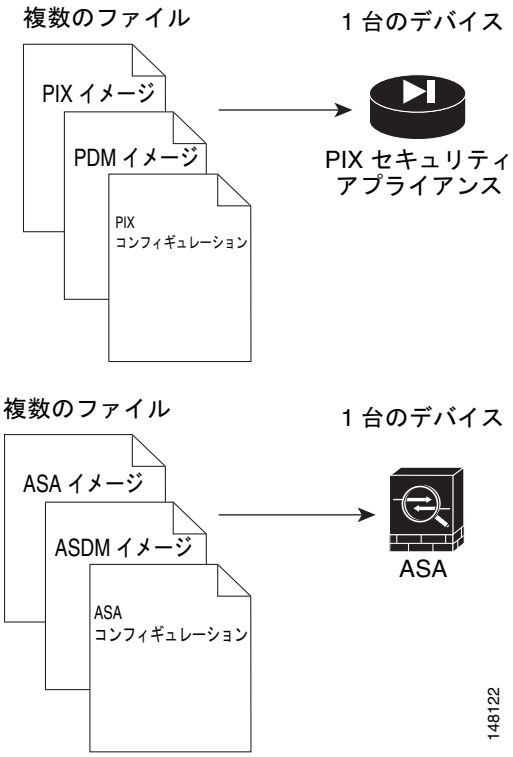
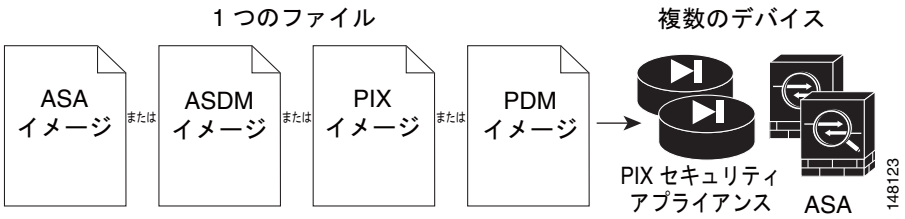


図 4-2　複数のデバイスを単一のファイルに割り当てる



次のトピックでは、デバイスおよびイメージの割り当てを管理する方法を説明します。

- 「デバイス割り当て概要の表示」（P.4-2）
- 「単一デバイスへのファイルの割り当て/割り当て解除」（P.4-3）
- 「ファイル割り当て概要の表示」（P.4-3）
- 「複数のデバイスへのファイルの割り当て/割り当て解除」（P.4-4）

デバイス割り当て概要の表示

[Assignments] タブから、[Assign File to a Device] オプションを選択して、デバイス割り当て概要の表を表示します（表 4-1）。表には、各デバイスに割り当てられたファイルに関する情報が表示されます。

カラム名をクリックすると、そのカラムを基準として表をソートできます。また、表に表示される情報をフィルタしたり、デバイスを検索したりできます。

表 4-1　デバイス割り当て概要

要素	説明
Radio button	ファイルに割り当てるデバイスのボタンをクリックします。
Device ID	AUS で識別に使用されるデバイスの名前です。 デバイス ID をクリックすると、そのデバイスの詳細および割り当てられたファイルを示す表が新しいウィンドウで開かれます。詳細には、デバイス名、IP アドレス、シリアル番号、sysObjectID、ソフトウェア バージョン、PDM/ASDM バージョン、およびデバイスで利用できる RAM およびフラッシュ メモリ、この表の一部の情報などが表示されます。
Family	常に PIX を表示します。[Type] フィールドのモデル タイプを確認することで、デバイスが PIX ファイアウォールまたは ASA デバイスであるかを確認できます。
Type	デバイスのタイプです（PIX-535 または ASA-5540 など）。
PDM Image	デバイスに割り当てられた PDM または ASDM イメージ ファイルの名前です。
PIX Image	デバイスに割り当てられた PIX ファイアウォールまたは ASA イメージ ファイルの名前です。
PIX Config	デバイスに割り当てられた PIX ファイアウォールまたは ASA コンフィギュレーション ファイルの名前です。
[Assign File] ボタン	このボタンをクリックして、選択したデバイスにファイルを割り当てます。詳細については、「単一デバイスへのファイルの割り当て/割り当て解除」（P.4-3）を参照してください。

関連項目

- 「ソフトウェア イメージの追加」（P.3-2）
- 「ファイル割り当て概要の表示」
- 「複数のデバイスへのファイルの割り当て / 割り当て解除」

単一デバイスへのファイルの割り当て / 割り当て解除

[Device Assignment Summary] ページでは、デバイスに割り当てるファイルを変更できます。デバイスで実行されているソフトウェア イメージを更新する場合など、ファイルの割り当てを解除して、新しいファイルを割り当てることができます。

（注）　ASA または PIX ソフトウェア イメージを変更する場合は、既存のコンフィギュレーション ファイルを新しいイメージで使用できることを必ず確認してください。互換性のないソフトウェア イメージがダウンロードされると、セキュリティ アプライアンスによってサポートされないコマンドがすべてドロップされ、コンフィギュレーション エラーが発生する場合があります。

手順

ステップ 1　[Assignments] > [Assign File to a Device] を選択します。[Device Assignment Summary] ページが表示されます（「デバイス割り当て概要の表示」（P.4-2）を参照）。

ステップ 2　ファイルを割り当てるデバイスを選択します。

ステップ 3　[Assign File] をクリックします。[Select Images to Assign] ページが表示されます。

ステップ 4　デバイスに割り当てるコンフィギュレーション ファイル、PIX/ASA ソフトウェア イメージ ファイル、または PDM/ASDM イメージ ファイルを選択します。3 タイプすべてのファイルを割り当てることができます。リストには、AUS に追加したファイルのみが含まれます。

特定のファイル タイプを割り当てない場合は、[none] を選択します。

ステップ 5　[OK] をクリックしてファイルをデバイスに割り当てます。

関連項目

- 「ソフトウェア イメージの追加」（P.3-2）
- 「ファイル割り当て概要の表示」
- 「複数のデバイスへのファイルの割り当て / 割り当て解除」

ファイル割り当て概要の表示

[Assignments] タブから、[Assign a File to Devices] オプションを選択して、ファイル割り当て概要の表を表示します（表 4-2）。表には、ファイルおよび各ファイルに割り当てられているデバイスの数がリスト表示されます。

カラム名をクリックすると、そのカラムを基準として表をソートできます。また、表に表示される情報をファイル タイプでフィルタしたり、ファイルを検索したりできます。

表 4-2　ファイル割り当ての概要

要素	説明
Radio button	デバイスに割り当てるファイルのボタンをクリックします。
Name	ファイルの名前です。 ファイル名をクリックすると、そのデバイスの詳細および割り当てられたデバイスの表が新しいウィンドウで開かれます。
Type	次のファイル タイプを選択できます。 • pdm：PIX Device Manager（PDM）ソフトウェア イメージ。 • asdm：Adaptive Security Device Manager（ASDM）ソフトウェア イメージ。 • pix-image：ASA または PIX ソフトウェア イメージ。 • pix-config：ASA または PIX コンフィギュレーション ファイル。
Version	ファイルのソフトウェア バージョンです。コンフィギュレーション ファイルの場合、コンフィギュレーションが作成された OS バージョンが表示されます。
No.of Devices	ファイルに割り当てられたデバイスの数です。
[Assign Devices] ボタン	このボタンをクリックして、デバイスを選択したファイルに割り当てます。詳細については、「複数のデバイスへのファイルの割り当て/割り当て解除」（P.4-4）を参照してください。

関連項目

- 「ソフトウェア イメージの追加」（P.3-2）
- 「デバイス割り当て概要の表示」
- 「単一デバイスへのファイルの割り当て/割り当て解除」

複数のデバイスへのファイルの割り当て/割り当て解除

[File Assignment Summary] ページでは、ファイルに割り当てるデバイスを変更できます。たとえば、新しい ASA ソフトウェア イメージを導入する場合、ASA デバイスすべてに一括して割り当てることができます。

コンフィギュレーション ファイルを複数のデバイスに割り当てることはできません。

（注）　デバイスの ASA または PIX ソフトウェア イメージを変更する場合は、デバイスで実行されている既存のコンフィギュレーション ファイルを新しいイメージで使用できることを必ず確認してください。互換性のないソフトウェア イメージがダウンロードされると、セキュリティ アプライアンスによってサポートされないコマンドがすべてドロップされ、コンフィギュレーション エラーが発生する場合があります。

手順

ステップ 1　[Assignments] >[Assign a File to Devices] を選択します。[File Assignment Summary] ページが表示されます（「ファイル割り当て概要の表示」（P.4-3）を参照）。

ステップ 2　割り当てを変更するファイルを選択します。

ステップ 3　[Assign Devices] をクリックします。[Select Device Assignments] ページが表示されます。

カラム名をクリックすると、そのカラムを基準として表をソートできます。また、表に表示される情報をフィルタしたり、デバイスを検索したりできます。

ステップ 4　ファイルに割り当てるデバイスを選択します。割り当てを解除するには、デバイスのチェックボックスをオフにします。

表示されたデバイスをすべて選択するには、表の見出しにあるチェックボックスをオンにします。

ステップ 5　[OK] をクリックして、割り当てを更新します。

関連項目

- 「ソフトウェア イメージの追加」（P.3-2）
- 「単一デバイスへのファイルの割り当て / 割り当て解除」
- 「デバイス割り当て概要の表示」

CHAPTER 5

レポートの表示

レポートでは、AUS に関する有益な情報を得ることができます。たとえば、AUS がどれくらい混雑しているか、エラーの有無、AUS にアクセスしたデバイスに関する情報を表示できます。

次のトピックでは、AUS のレポートについて説明します。

System Information Report の表示

システム情報レポートを表示するには、[Reports] タブで、[System Info] オプションを選択します（表 5-1）。

レポートには、AUS に関する基本情報、サーバの混雑状況、過去 24 時間のアクティビティに関する統計情報が表示されます。

表 5-1　System Info Report

行	説明
General System Information	
Auto Update Server URL	デバイスによって AUS にアクセスするために使用される URL です。AUS を Security Manager に追加する場合、この情報を使用して URN を確認します。
No.of Devices Managed	AUS データベースにあるデバイスの数です。
No.of Devices That Never Contacted AUS	AUS に一度も接続していない AUS データベースにあるデバイスの数です。
Percentage of Devices Up-to-date	AUS への接続および新しいイメージまたはコンフィギュレーション ファイルのダウンロードに成功したデバイスの比率です。
Percentage of Devices Not Up-to-date	AUS に一度も接続していない、または AUS への接続に失敗して、新しいイメージまたはコンフィギュレーション ファイルをダウンロードできなかったデバイスの比率です。
No.of Files	AUS データベースにあるファイルの数です。

表 5-1　System Info Report （続き）

行	説明
No.of Assignments	デバイスに割り当てられたイメージの数およびイメージに割り当てられたデバイスの数です。
Statistics For Last 24 Hours	
次の統計情報の値はすべて、過去 24 時間の情報に基づきます。	
No.of Successful Auto Updates	デバイスが AUS に接続し、自動更新の取得に成功した回数です。
No.of Failed Auto Updates	デバイスが AUS に接続し、自動更新の取得に失敗した回数です。
Percentage of Devices that Contacted AUS	AUS への接続および新しいイメージまたはコンフィギュレーション ファイルのダウンロードに成功したデバイスの比率です。
Device That Contacted AUS Most	AUS に最も多く接続したデバイスです。
Most Downloaded File	デバイスによって AUS から最も多くダウンロードされたファイルです。
No.of Unique Files Downloaded	デバイスが AUS から最も多くダウンロードしたファイルのユニーク数です。
No.of Successful File Downloads	ファイルが正常にダウンロードされた回数です。
No.of Failed File Downloads	デバイスの自動更新中にエラーが発生した回数です。
No.of Bytes Downloaded	ダウンロードされたバイト数です。
No.of New Assignments	新たにデバイスに割り当てられたイメージの数およびイメージに割り当てられたデバイスの数です。

関連項目

- 「Event Report の表示」（P.5-4）
- 「Event Failure Summary Report の表示」（P.5-4）
- 「Event Success Summary Report の表示」（P.5-5）
- 「No Contact Since Report の表示」（P.5-6）

AUS イベント タイプについて

任意のイベント レポートを表示すると、レポートの各エントリには、イベント タイプが含まれます。このタイプは基本的にイベント中に何が発生したかを表します。説明カラムでは、より詳細な情報が表示されます。

レポートの表はこれらのイベントに基づいてフィルタできます。Event Failures および Event Successes レポートでは、失敗または成功タイプの情報についてのみ提供される一方、Events レポートでは、すべてのタイプの情報が表示されます。表 5-2 では、すべてのイベント タイプについて説明します。

イベント レポートの表示方法については、次のトピックを参照してください。

- 「Event Report の表示」（P.5-4）
- 「Event Failure Summary Report の表示」（P.5-4）
- 「Event Success Summary Report の表示」（P.5-5）

表 5-2　イベント タイプの説明

イベント タイプ	説明
CONNECT_SUCCESS	デバイスは AUS に正常に接続して、インベントリの詳細をレポートしました。
CONNECT_FAILURE	自動更新の試行時に問題が発生しました。可能性のある原因は次のとおりです。 • XML の解析中にエラーが発生した。 • クレデンシャルが無効である。 • デバイスが AUS に追加されていない。 • 接続の問題。 • レコードの追加時にデータベースがダウンしていた。
DEVICE_CONFIG_ERROR	デバイスからサーバにエラーが報告されたか、またはデバイスが割り当てられたコンフィギュレーション ファイルのロード時にエラーが発生しました。コンフィギュレーションの問題をデバッグする場合に、これらのエラーを使用してください。デバイスでコンフィギュレーション ファイルをダウンロード中にエラーが発生した場合、実行中のコンフィギュレーションによってスタートアップ コンフィギュレーションに戻されます。
GENERAL_DEVICE_ERROR	デバイスから AUS に報告されたコンフィギュレーション ファイル以外のエラーです。可能性のある原因は次のとおりです。 • Auto Update サーブレットへの接続の問題。 • ダウンロードされたイメージの問題（無効なチェックサム）。セキュリティ アプライアンスに複数のソフトウェア イメージまたは ASDM イメージがインストールされている場合に特定のものを使用するように設定するには、または、ソフトウェア イメージまたは ASDM イメージを外付けフラッシュ メモリにインストールするには、「起動するソフトウェア イメージおよび ASDM イメージのコンフィギュレーション」（P.C-3）を参照してください。
DOWNLOAD_SUCCESS	ファイルはリモート デバイスに正常に送信されました。これは、デバイスでイメージが正常に実行されていることを意味するものではありません。このメッセージの後に、DEVICE_CONFIG_ERROR または GENERAL_DEVICE_ERROR のいずれかが続く場合があります。
DOWNLOAD_FAILURE	イメージまたはコンフィギュレーション ファイルのダウンロード中にエラーが発生しました。可能性のある原因は次のとおりです。 • クレデンシャルが無効である。 • 通信の問題。 • データベースの問題。
AUS_IMMEDIATE_SUCCESS	[Update Now] を選択して、即時自動更新を実行したときに、AUS によってデバイスへの接続および更新が正常に実行されました。
AUS_IMMEDIATE_FAILURE	デバイスの即時自動更新中にエラーが発生しました。可能性のある原因は次のとおりです。 • サーバがデバイスに直接接続できません（NAT 境界をまたぐ場合など）。AUS を NAT と連携するように設定する方法については、「NAT 境界をまたいだ AUS の展開」（P.1-2）を参照してください。 • デバイスが AUS で認証される場合に使用するイネーブルまたは TACACS+ ユーザ名およびパスワードが正しくありません。これらのクレデンシャルの詳細については、「デバイスを直接 AUS に追加する」（P.2-3）を参照してください。 • 内部エラーが発生しました。
SYSTEM_ERROR	内部エラーが発生しました。

Event Report の表示

[Reports] タブで、[Events] オプションを選択してイベント レポートを表示します。このレポートには、成功または失敗にかかわらず、すべてのイベントが表示されます。

レポートには、AUS に接続したデバイスに関する情報が表示されます。情報には、イベント タイプ、イベントの結果、イベントの日時、問題が発生した場合に修復を支援する詳細な説明などが含まれます。発生するイベント タイプの詳細については、「AUS イベント タイプについて」（P.5-2）を参照してください。

レポートには、デバイスから AUS に送信された通知に関する情報も表示されます。たとえば、ASA デバイスによってコンフィギュレーション ファイルがダウンロードされ、エラーが検出されると、AUS にアラートが送信されます。このアラートがレポートに表示されます。デバイスによって AUS に接続されるたび、またはファイルがダウンロードされるたびにエントリが追加されます。

レポートは次の方法で操作できます。

- レポートには、1 日に発生したイベントのみが表示されます。[Date] フィールド（過去 7 日間からのみ選択可能）で日付を選択して、その日のイベントを表示します。
- カラム名をクリックすると、カラムの情報を基準として表をソートできます。Device ID カラムを基準に表をソートすると、表は最初にデバイス ID を基準にソートされ、次にタイムスタンプを基準にソートされます。
- 表の上にあるフィールドを使用すると、表をフィルタして、特定のデバイス ID を表で検索できます。

関連項目

- 「System Information Report の表示」（P.5-1）
- 「Event Failure Summary Report の表示」（P.5-4）
- 「Event Success Summary Report の表示」（P.5-5）
- 「No Contact Since Report の表示」（P.5-6）

Event Failure Summary Report の表示

エラーが発生したイベントの概要レポートを表示するには、[Reports] タブで、[Event Failures] オプションを選択します。

このレポートには、イベント エラーが発生したデバイスがリストされます。デバイスの情報には、デバイスで各タイプのエラーが発生した回数が含まれます（カラムにエントリがない場合は、そのタイプのエラーは発生していません）。レポートを分析するには、次を実行します。

- [Date] フィールド（過去 7 日間からのみ選択可能）で日付を選択して、その日のイベントを表示します。
- デバイス ID をクリックすると、その日にそのデバイスで発生したすべてのイベントを表示する詳細なレポートが開きます。
- いずれかのエラー カラムの番号をクリックすると、そのタイプのエラーのみにフィルタされた詳細なレポートが表示されます。次のエラー タイプがあります。詳細については、「AUS イベント タイプについて」（P.5-2）を参照してください。
  - **Auto Update**：CONNECT_FAILURE イベントが発生した回数（デバイスの AUS への接続エラー）。
  - **Download**：DOWNLOAD_FAILURE イベントが発生した回数（デバイスのファイル ダウンロード エラー）。

  - **Request Update**：AUS_IMMEDIATE_FAILURE イベントが発生した回数（即時自動更新の実行エラー）。
  - **Configuration**：DEVICE_CONFIG_ERROR イベントが発生した回数（ダウンロードされたコンフィギュレーションのエラー）。
  - **General**：GENERAL_DEVICE_ERROR イベントが発生した回数。
  - **System**：SYSTEM_ERROR イベントが発生した回数（AUS システム エラー）。
- カラム名をクリックすると、カラムの情報を基準として表をソートできます。Device ID カラムを基準に表をソートすると、表は最初にデバイス ID を基準にソートされ、次にタイムスタンプを基準にソートされます。
- 表の上にあるフィールドを使用すると、表をフィルタして、特定のデバイス ID を表で検索できます。

関連項目

- 「Event Report の表示」（P.5-4）
- 「Event Success Summary Report の表示」（P.5-5）
- 「No Contact Since Report の表示」（P.5-6）

Event Success Summary Report の表示

成功したイベントの概要レポートを表示するには、[Reports] タブで、[Event Success] オプションを選択します。

レポートには、アクションを正常に実行したデバイスがリストされます。デバイスの情報には、デバイスで各タイプのイベントを正常に実行した回数が含まれます（カラムにエントリがない場合は、そのタイプのエラーが発生していません）。レポートを分析するには、次を実行します。

- [Date] フィールド（過去 7 日間からのみ選択可能）で日付を選択して、その日のイベントを表示します。
- デバイス ID をクリックすると、その日にそのデバイスで発生したすべてのイベントを表示する詳細なレポートが開きます。
- いずれかの成功カラムの番号をクリックすると、そのタイプの成功のみにフィルタされた詳細なレポートが表示されます。次の成功タイプがあります。詳細については、「AUS イベント タイプについて」（P.5-2）を参照してください。
  - **Auto Update**：CONNECT_SUCCESS イベントに成功した回数（デバイスが AUS に正常に接続）。
  - **Download**：DOWNLOAD_SUCCESS イベントに成功した回数（デバイスにファイルを正常にダウンロード）。
  - **Request Update**：AUS_IMMEDIATE_SUCCESS イベントに成功した回数（即時自動更新を正常に実行）。
- カラム名をクリックすると、カラムの情報を基準として表をソートできます。Device ID カラムを基準に表をソートすると、表は最初にデバイス ID を基準にソートされ、次にタイムスタンプを基準にソートされます。
- 表の上にあるフィールドを使用すると、表をフィルタして、特定のデバイス ID を表で検索できます。

関連項目

- 「Event Report の表示」（P.5-4）
- 「Event Failure Summary Report の表示」（P.5-4）
- 「No Contact Since Report の表示」（P.5-6）

No Contact Since Report の表示

最後に接続された日付レポートを表示するには、[Reports] タブで、[No Contact Since] オプションを選択します。

レポートには、指定した日付以降 AUS に接続していないデバイスがリストされ、最後に正常に接続が実行された日時が表示されます。レポートを分析するには、次を実行します。

- 必要に応じて、[Select Date] フィールドに接続情報を表示する他の日付を指定して、[Go] をクリックします。
- デバイス ID をクリックすると、そのデバイスで発生したすべてのイベントを表示する詳細なレポートが開きます。過去 7 日間のイベントを表示できます。詳細レポートで表示できるイベントタイプの詳細については、「AUS イベント タイプについて」（P.5-2）を参照してください。
- カラム名をクリックすると、カラムの情報を基準として表をソートできます。
- 表の上にあるフィールドを使用すると、特定のデバイス ID を表で検索できます。

関連項目

- 「System Information Report の表示」（P.5-1）
- 「Event Report の表示」（P.5-4）
- 「Event Failure Summary Report の表示」（P.5-4）
- 「Event Success Summary Report の表示」（P.5-5）

APPENDIX A

AUS のトラブルシューティング

次のトピックでは、AUS のトラブルシューティングについて説明します。

デバイス概要にデバイスが表示されません

デバイスがデバイス概要に表示されない場合は、Security Manager インベントリにデバイスが正常に追加されていません。Security Manager を使用してデバイスを追加する方法については、「コンフィギュレーション ファイルの更新」（P.1-7）を参照してください。

このトピックの説明に従ってコンフィギュレーションを展開したら、Security Manager の展開結果を表示して、正常に展開されていることを確認してください。また、AUS イベント レポートを表示して、デバイスが正常に AUS に接続し、コンフィギュレーションを取得したことを確認します。

正常に展開され、デバイスによってコンフィギュレーションが正常にダウンロードされると、AUS デバイス リストに表示されます。

デバイスが AUS に接続されていません

デバイスが AUS に一度も接続されていない場合、次が考えられます。

- デバイスに正しい AUS URL が設定されていない。
- デバイスがネットワークに接続されていない。
- AUS のデバイスのクレデンシャルが正しくない。
- デバイスは正常に設定されているが、AUS をポーリングしていない。
- 使用している PIX ファイアウォール ソフトウェアのバージョンが正しくない（6.3 以降が必要）。ASA のバージョンはすべてサポートされています。

デバイスを AUS に接続するには、次の 1 つ以上を実行します。

- ポーリング時間が終了するのを待ちます。
- ポーリング時間が終了してもデバイスが AUS に接続しない場合は、デバイスのコンソールを使用してデバイスにログインし、AUS を ping してデバイスが AUS に接続できるかを確認します。
- デバイスが展開された環境で動作できるように設定されていることを確認します。DHCP 向けに展開されている場合は、DHCP サーバが存在しており、デバイスにネットワーク アドレスを提供できることを確認します。デバイスがスタティック IP アドレスを使用して展開されている場合は、IP アドレスが正しいことを確認してください。
- AUS で [Reports] > [Events] を選択して、デバイスで認証エラーが発生していないかをイベント レポートで確認してください。認証エラーが発生している場合は、[Event Type] カラムに CONNECT_FAILURE と表示され、詳細カラムにデバイスで認証エラーが発生しているというメッセージが表示されます。
- [Auto Update URL] を表示して、システム情報の URL と一致していることを確認します（[Report] > [System Info]）。デバイスにログインして、イネーブル モードに入り、show auto-update と入力してデバイスに設定された AUS 設定を表示します。

  URL がシステム情報レポートに表示された URL と一致しない場合は、次を入力して AUS の URL を新しく設定します。

  ```
  conf t
  auto-update server
  https://username:password@AUSServerAddress:port/autoupdate/AutoUpdateServlet
  ```

- エラーが発生していないか AUS ログを確認します。

AUS で認証エラーが発生します。どのように対応したらいいでしょうか

認証エラーはデバイスの AUS への接続時に発生します。認証エラーはイベント レポート（「Event Report の表示」（P.5-4）を参照）またはデバイス コンソールで表示できます（コンソールでデバッグがイネーブルの場合）。

デバイス コンソールでデバッグをイネーブルにするには、デバイスにログインして、イネーブル モードに入り、次のコマンドを設定します。

```
conf t
logging on
logging console debug
```

誤った認証情報を使用した場合にも認証エラーが発生します。

- デバイスを AUS に追加する際、デバイスでサーバに接続するためのクレデンシャルを入力しました。ユーザ名 / パスワードのクレデンシャルが誤っています。このようなクレデンシャルは、追加したデバイスの Security Manager から取得されます（HTTP ユーザ名 / パスワードおよびイネーブル パスワード）。
- コマンド ラインを使用してユーザが、デバイスが AUS への接続に使用していたクレデンシャルの組み合わせを変更しました。これにより、サーバのクレデンシャルと一致しなくなりました。

この問題を解決するには、次の 1 つ以上を実行します。

- デバイスが AUS に接続して、新しいコンフィギュレーション ファイルがレポートされるまで待ちます。
- デバイスにアクセスして認証の問題を解決します。該当するデバイスのマニュアルを参照してください。
- デバイスにログインして、コマンド ラインからユーザ名およびパスワードを変更します。次のように入力します。

```
enable
conf t
auto-update server
https://username:password@AUSServerAddress:port/autoupdate/AutoUpdateServelet
```

自動更新を要求した後も、デバイスが最新の状態ではありません

デバイスで即時に AUS に接続して自動更新を要求したにもかかわらず、（「即時自動更新の要求」（P.2-6）を参照）デバイスが最新の状態ではない場合は、次の原因が考えられます。

- 要求がキューを通過していない。複数のデバイスについて AUS への即時接続を要求した場合、AUS では 1 件ずつ要求が処理されるため、要求が受け入れられるまでに時間がかかる場合があります。
- デバイスにアクセスできない。
- 設定されたポリシー定義に対して Security Manager によって生成された CLI コマンドが正しくない。

この問題を解決するには、次の 1 つ以上を実行します。

- 要求がキューを通過するまで少し待機します。
- デバイスがファイアウォールまたは NAT 境界をまたいでいないことを確認します。このようなデバイスでは、Update Now コマンドは使用できません。デバイスのポーリング時間が終了してデバイスが更新を取得するまで待機してください。
- Security Manager のインベントリで設定されたデバイスの ID がデバイスにコンフィギュレーションされたデバイス ID と一致することを確認します。HTTP ユーザ名およびパスワードとイネーブル パスワードが正しいことを確認します。
- イベント レポートを表示して、ポリシー設定に対して誤ったコマンドが生成されていないことを確認します。

イメージ ファイルの追加を試行すると、AUS でエラーが発生する原因を教えてください

PDM、ASDM、ASA、または PIX ソフトウェア イメージ ファイルを AUS に追加して、エラー メッセージが表示される場合、次の原因が考えられます。

- ファイルの割り当てに選択したイメージ タイプが正しくない。
- 追加するイメージ ファイルが正しくないか、破損している。
- ファイル名が予期されるファイル命名規則に従っていない。

この問題を解決するには、次の 1 つ以上を実行します。

- ファイルを追加する際、正しいイメージ タイプを選択してください。
- Cisco.com からファイルをダウンロードする際にファイル名を変更しないでください。
- イメージ ファイルが破損していないことを確認します。イメージ ファイルの MD5 チェックサムを確認してください。チェックサム値を確認するには、[Files] を選択して、[Name] カラムでイメージ ファイル名をクリックします。チェックサム値を含むファイルに関する情報がポップアップ ウィンドウが表示されます。詳細については、「[File Summary] ページの表示」（P.3-1）を参照してください。

  このチェックサム値をイメージのダウンロード時に取得した値と比較します。値が異なる場合は、イメージ ファイルが破損しています。

コンフィギュレーション ファイルを追加できません

追加できるのは、ASDM、PDM、ASA、および PIX ソフトウェア イメージ ファイルのみです。コンフィギュレーション ファイルを追加するには、Security Manager を使用してデバイスを設定して、コンフィギュレーションを AUS に展開します。手順の説明については、「コンフィギュレーション ファイルの更新」（P.1-7）を参照してください。

イメージ ファイルを割り当てても、最新の状態になりません

イメージ ファイルをデバイスに割り当てても、デバイスにこのファイルが含まれない場合は、次の原因が考えられます。

- デバイスは AUS に接続してイメージ ファイルを実行していることをレポートする必要がある。デバイスのポーリング時間によっては、更新されるまで数時間かかる場合があります。
- デバイスが AUS に接続できない問題が発生している。
- イメージ ファイルが破損している。

この問題を解決するには、次のいずれかまたは両方を実行します。

- AUS タイムスタンプを確認して、最後にデバイスが AUS に接続した時間を検証します。ポーリング時間が終了していない場合、デバイスは AUS に接続して最新情報をレポートしていません。ポーリング時間の終了まで待てない場合は、デバイスに対して即時に AUS に接続することを要求できます（「即時自動更新の要求」（P.2-6）を参照）。

- イベント レポートを確認して（[Report] > [Events]）、エラーを探します。デバイスに破損したイメージ ファイルが割り当てられている場合、レポートに DEVICE_CONFIG_ERROR イベント タイプが表示されます。これは、イメージ ファイルのダウンロード時にエラーが発生したことを示します。新しいイメージ ファイルをデバイスに割り当てるか、割り当てを解除して、以前に設定されたデバイスのイメージ ファイルに戻します。

  デバイスが AUS に接続して、イメージ ファイルが実行されていることをレポートしていない場合は、「デバイスが AUS に接続されていません」（P.A-2）を参照してください。

1 つのデバイスに同じタイプのイメージ ファイルを 2 つ割り当てられません

デバイスで同時に実行できるのは、ASA ソフトウェア イメージ、PIX ソフトウェア イメージ、ASDM ファイル、または PDM ファイル 1 つのみです。したがって、デバイスに割り当てられる各タイプのファイルは 1 つのみです。

新しい PIX または ASA ソフトウェア イメージをデバイスに割り当てると、デバイスが再起動します

新しい ASA または PIX ソフトウェア イメージをデバイスに割り当てた場合、デバイスを再起動する必要があります。再起動は自動的に実行されます。

デバイスで同じファイルが繰り返しダウンロードされます

デバイスで繰り返し同じファイルがダウンロードされる場合、デバイスでイメージの実行に問題が発生しています。イベント レポート（[Report] > [Events]）でエラーが発生していないか確認してください。エラーがある場合は、新しいイメージ ファイルを割り当てます。

一部のボタンがグレーアウトしています

一部の AUS の画面でボタンがグレーアウトされている場合、このコマンドを実行する適切な権限がありません。付録 B「ユーザ ロールおよび権限」を参照してください。

マシンの再起動後、AUS を起動できません

マシンの再起動後、AUS の起動には数分かかります。次のいずれかを実行します。

- 数分待ってから AUS を起動します。
- AUS エラー ログですべてのプロセスが正常に実行していることを確認します。

破損したまたは正しくないコンフィギュレーション ファイルをデバイスでダウンロードしないようにする方法を教えてください

コンフィギュレーション ファイルの割り当てを解除します。詳細については、「単一デバイスへのファイルの割り当て/割り当て解除」（P.4-3）を参照してください。コンフィギュレーション ファイルの割り当てを解除したら、Security Manager を使用してファイルを修正し、再度展開します。

AUS と PIX または ASA デバイス間の接続を確認する方法を教えてください

Security Manager をインストールしていない場合、または単に AUS とデバイスの接続を確認する場合は、デバイスを手動で AUS に追加できます。詳細については、「デバイスを直接 AUS に追加する」（P.2-3）を参照してください。

デバイスは、定義された間隔で AUS に接続されます。デバイスが AUS に接続されたかをイベント レポートで確認します。「Event Report の表示」（P.5-4）を参照してください。

AUS とデバイス間の接続が正常であることが確認できたら、デバイスを AUS から削除します。

コンフィギュレーション エラーがレポートされた場合の対応方法を教えてください

イベントのエラー概要レポートにコンフィギュレーション エラーが表示された場合、原因と考えられるコンフィギュレーション ファイルを表示して問題の原因をさぐります。「コンフィギュレーション ファイルの表示」（P.3-3）を参照してください。

コンフィギュレーション エラーの行数を使用して、コンフィギュレーション ファイルのエラーを特定します。

エラー メッセージについて

エラーの情報について、次のログを確認できます。

- *NMSROOT*¥MDC¥log¥operation¥autoupdate.log：AUS アプリケーションからのメッセージをすべて格納する AUS ログ。
- *NMSROOT*¥MDC¥tomcat¥logs¥stdout.log：tomcatServletEngine で実行されてる任意のアプリケーションからのメッセージを格納する Tomcat 出力ログ。
- *NMSROOT*¥MDC¥tomcat¥logs¥stderr.log：java コードが破損した場合にスタック トレースを格納する Tomcat 標準エラー ログ。

表 A-1 に一般的なエラー メッセージ、考えられる原因、および考えられる解決策を示します。

表 A-1　AUS エラー メッセージ

メッセージ	考えられる原因	考えられる解決策
CALLHOME-DB-ADD_FILE_FAILURE	ファイルを AUS に追加中にエラーが発生しました。 データベースで通信の問題が発生しました。	ファイルを再度 AUS に追加してください。それでも解決されない場合は、AUS を再起動します。
CALLHOME-FILE-INVALID_FILE_NAME	ファイル名が正しくありません。 ファイルの名前が長すぎるか短すぎます。または、予測される命名規則に従っていません。	正しいファイル名を入力します。
CALLHOME-FILE-INVALID_FILE_CONTENTS	破損しているまたはファイル タイプが正しくないファイルを追加しました。	ファイルを交換するか、他のファイルを追加してみてください。
CALLHOME-FILE_NOT_FOUND	選択されたファイルが見つかりません。 このファイルは、データベースからすでに削除されています。	[Files] タブをクリックして、画面を更新します。
CALLHOME-FILE-BAD_FILE_NAME	AUS のファイルへのアクセス時にエラーが発生しました。 ファイルが存在していないか、読み込めません。	ファイルが存在しており、破損していないことを確認します。
CALLHOME-FILE-INVALID_IMAGE	ファイルを AUS に追加できません。ファイルが破損しているか、AUS で指定されているのとは異なるタイプのファイルを追加しようとしています。	新しいバージョンのイメージ ファイルをダウンロードして、ファイルを AUS に追加します。
CALLHOME-DEVICE-NOT_CALLED_HOME_YET	デバイスが AUS に接続されませんでした。AUS で、デバイスの IP アドレスが認識されていません。	デバイスが AUS に接続し、自動更新を要求するまで待機します（「即時自動更新の要求」（P.2-6）を参照）。
CALLHOME-SECURITY-NOT_AUTHENITCATED	AUS でユーザ名 / パスワードのクレデンシャルを認証できません。 クレデンシャルが間違っているか、セッションがタイムアウトしました。	ユーザ名およびパスワードを再度入力して、AUS にログインします。
CALLHOME-COMMON-AUDIT_FAILED	AUS で、ACS または Core 監査ログに書き込めません。 通信エラーが発生しました。	AUS を再起動します。問題が続く場合は、Technical Assistance Center（TAC）にご連絡ください。
CALLHOME-DEVICE_NOT_FOUND	AUS で選択したデバイスが見つかりません。 デバイスは、すでにデータベースから削除されています。	[Devices] タブをクリックして、画面を更新します。
CALLHOME-FILE-CANNOT_DELETE_FILE	このファイルは削除できません。 ファイルは使用中です。	ファイルの削除を再試行してください。ファイルを削除できない場合は、AUS を再起動します。

表 A-1　AUS エラー メッセージ （続き）

メッセージ	考えられる原因	考えられる解決策
CALLHOME-DEVICE-BAD_ CALLHOME_IMMEDIATE_ RESPONSE	自動更新時にエラーが発生しました。 イネーブルまたは AAA クレデンシャルが正しくないか、デバイスで HTTP アクセスが許可されていません。	デバイスで AUS に対する HTTP アクセスが許可されており、AUS AAA およびイネーブルクレデンシャルが正しいことを確認してください。「デバイスを直接 AUS に追加する」（P.2-3）を参照してください。
CALLHOME-FILE-MOVE_ERROR	ファイルの追加に使用した一時ファイルを削除できません。 指定したファイル名には、無効または不正な文字が含まれているか、ストレージ領域に同じファイルが存在しています。	ファイルが存在していないか、ストレージ ディレクトリを確認します。タスクを再度実行して、問題が解決されない場合は、AUS を再起動して、コンフィギュレーション ファイルを再度追加してください。エラーがないか、ログ ファイルを確認します。
CALLHOME-DEVICE-CH_ IMMEDIATE_NO_CREDENTIALS	AUS で、自動更新を実行できません。 イネーブル パスワードまたは AAA クレデンシャルがデバイスに入力されていないため、AUS では、デバイスの通信に使用するクレデンシャルが認識されません。	デバイスに正しいクレデンシャルを入力してエントリを修正し、タスクを再度実行します。「デバイスを直接 AUS に追加する」（P.2-3）を参照してください。
CALLHOME-INVALID_UPLOAD_ FILE	ファイルが無効です。	有効なファイル名を入力してください。
CALLHOME-DB-NO_CONNECTION	AUS がデータベースに接続できません。 データベース サーバが停止しています。	AUS を再起動して、タスクを再試行します。
CALLHOME-DB-BAD_PASSWORD_ STATE	データベース パスワードの変更中にエラーが発生しました。 AUS db.prop ファイルに含まれるデータベースのユーザ名およびパスワードが正しくないか、入力したパスワードが正しくありません。	AUS db.prop ファイルにデータベースの正しいユーザ名およびパスワードが含まれていることを確認して、ユーザ名およびパスワードを再度入力します。
CALLHOME-DB-COMMIT_ERROR	AUS でデータベースにデータを書き込めません。	AUS を再起動して、タスクを再試行します。
CALLHOME-DB-POOL_ERROR	AUS でデータベースに接続できません。	AUS を再起動して、タスクを再試行します。
CALLHOME-DB-DISK_FULL	空きディスク容量が不足しています。	不要な情報をハード ドライブから削除するか、新しいハード ドライブを追加します。
CALLHOME-DB-ADD_DEVICE_ FAILURE	システムにデバイスを追加中にエラーが発生しました。 データベースで通信の問題が発生しました。	デバイスの追加を再試行してください。それでもデバイスを AUS に追加できない場合は、AUS を再起動します。
CALLHOME-DB-ADD_FILE_ FAILURE	ファイルにデバイスを追加中にエラーが発生しました。 データベースで通信の問題が発生しました。	ファイルの追加を再試行してください。それでもファイルを AUS に追加できない場合は、AUS を再起動します。

表 A-1　AUS エラー メッセージ （続き）

メッセージ	考えられる原因	考えられる解決策
CALLHOME-DB-DUPLICATE_ VALUE	AUS にすでに存在するファイルを追加しようとしています。	既存のエントリを使用するか、既存のエントリを削除して、タスクを再試行します。
CALLHOME-DB-DEVICE_NOT_ FOUND	要求したデバイスが AUS で見つかりません。 AUS に追加されたデバイスで AUS への接続を試行しました。	正しいデバイス ID が入力されていることを確認して、タスクを再試行します。
CALLHOME-DEVICE-INVALID_ AUTHORIZATION	デバイスによって無効な認証情報が渡されました。 デバイスのユーザ名およびパスワードを確認してください。	デバイスのユーザ名およびパスワードを更新してください。
CALLHOME-FILE-CHECKSUM_ MISMATCH	ファイルがデータベースに追加された後に、ファイルのチェックサムが変更されました。 他のユーザがファイルを変更したか、システムが侵害されています。	マシンがセキュアであることを確認してください。次にイメージ ファイルを削除して、ファイルの新しいコピーを AUS に追加します。
CALLHOME-INVALID_UPLOAD_ FILE	ファイル名が無効です。	アップロードする有効なファイル名を入力してください。
CALLHOME-UI_CANNOT_MODIFY_ CONFIG_MAPPING	コンフィギュレーション ファイルの割り当てを変更できません。	Security Manager を使用してコンフィギュレーション ファイルを変更します。
CALLHOME-UI_INVALID_ IPADDRESS	IP アドレスが無効です。 無効な IP アドレスが入力されました。	有効な IP アドレスを入力してください。
CALLHOME-UI_MULTICAST_ ADDRESS	マルチキャスト アドレスが RFC マルチキャスト範囲（224.0.0.0 ～ 239.255.255.255）外です。 無効なマルチキャスト アドレスが入力されました。	有効なマルチキャスト IP アドレスを入力してください。
CALLHOME-UI_NO_DEVICE_EXIST	デバイスが存在していません。 すでにデバイスを削除した可能性があります。	[Devices] タブをクリックして、画面を更新します。
CALLHOME-BOUNDS-INVALID_ EMPTY_START_UPDATE_WINDOW_ TIME	自動更新スケジュールの開始時刻が未入力です。 自動更新の開始時刻が入力されていません。	HH:MM の形式で、開始時刻を入力してください。
CALLHOME-BOUNDS-INVALID_ EMPTY_END_UPDATE_WINDOW_ TIME	自動更新スケジュールの期間が未入力です。 自動ウィンドウの期間が入力されていません。	HH:MM の形式で、期間を入力してください。
CALLHOME-BOUNDS-INVALID_ EMPTY_UPDATE_WINDOW_DAY_ INFO	週間自動更新が発生する曜日が未入力です。 自動更新が発生する曜日が選択されていません。	毎週更新する曜日を選択します。

表 A-1　AUS エラー メッセージ （続き）

メッセージ	考えられる原因	考えられる解決策
CALLHOME-COMMON-MISSING_ UPDATE_WINDOW	更新スケジュール タイプが指定されていません。 ヌルまたは無効なデバイス ID オブジェクトが渡されました。	デバイス ID が正しく渡されていることを確認してください。
CALLHOME-BOUNDS-INVALID_ UPDATE_WINDOW_TYPE	設定された更新スケジュール タイプが無効です。 無効な更新スケジュール タイプが設定されています。	更新スケジュール タイプが正しく設定されていることを確認してください。
CALLHOME-UPDATE_WINDOW_ NOT_CONFIGURED	自動更新スケジュールを削除できません。 更新スケジュールが設定されていません。	削除する前に、コンフィギュレーションの更新をスケジュールしてください。
CALLHOME-UPDATE_WINDOW_ UNSUCCESSFUL	更新スケジュールのコンフィギュレーションに失敗しました。 デバイスには、すでに更新スケジュール タイプが設定されています。	既存の更新スケジュールを削除してください。

APPENDIX B

ユーザ ロールおよび権限

AUS を使用するには、ユーザ名およびパスワードが認証される必要があります。ユーザ名およびパスワードの組み合わせは、AUS で使用するようにコンフィギュレーションで選択された、CiscoWorks Server または Cisco Secure Access Control Server（ACS）データベースのいずれかと比較されます。

認証後、割り当てられた権限に基づいて許可されます。権限は、アプリケーション内で定義されたタスクまたは操作です。ユーザに割り当てられた権限セットによって、ユーザのロールが定義され、システムへのアクセス権の範囲とタイプを示します。

次のトピックでは、2 タイプの認証方式に関連したユーザ ロールおよび許可に関する詳細を説明します。

AUS 権限

AUS 権限は、ユーザが実行できる主要なアクションです。AUS によって提供される権限を表 B-1 に示します。これらの権限は CiscoWorks Server および次の項で説明する ACS ロールに割り当てられます。

表 B-1　　AUS 権限

権限	説明
API_View_Device GUI_View_Device	デバイス情報を表示できます。
API_View_Images GUI_View_Images	ソフトウェア イメージに関する情報を表示できます。
API_View_Assignment GUI_View_Assignment	デバイスからファイルへの割り当ておよびファイルからデバイスへの割り当てに関する情報を収集および表示できます。
API_View_Reports GUI_View_Reports	システム概要情報およびイベント レポートを表示できます。
API_View_Admin GUI_View_Admin	AUS 管理情報を表示できます。
API_Modify_Device GUI_Modify_Device	デバイスを強制的に AUS に接続できます。

表 B-1　AUS 権限 （続き）

権限	説明
API_Modify_Images GUI_Modify_Image	AUS でイメージを追加および削除できます。
API_Modify_Assignment GUI_Modify_Assignment	ファイルをデバイスに割り当てる、またはデバイスをファイルに割り当てることができます。
API_Modify_Admin GUI_Modify_Admin	AUS 管理コンフィギュレーション設定を変更できます。

CiscoWorks Server ロールおよび AUS 権限

CiscoWorks Server 認証方式を使用してデバイスに対してアクションを実行すると、アクションは選択したデバイスに応じて認証されます。

CiscoWorks Server には、組織内で想定される職務に対応するロールが 5 つ定義されています。

表 B-2 に AUS とともに使用できるロールを示します。

表 B-2　CiscoWorks のロール

ロール	説明
System Administrator	CiscoWorks Server および AUS タスクをすべて実行できます（ユーザの追加、ユーザ パスワードの設定、イメージの追加または削除、割り当ての解除など）。
Network Administrator	CiscoWorks Server の管理をタスクを実行し、システム管理者と同じ権限があります。
Network Operator	AUS の情報すべてに読み取り専用の権限があります。
Approver	デバイスを変更できます。イメージ、割り当て、レポート、および管理タスクに対して読み取り専用の権限があります。
Help Desk	AUS の情報すべてに読み取り専用の権限があります。

表 B-3 に AUS ロールおよびサポートされる権限を示します。権限の詳細については、表 B-1 を参照してください。

表 B-3　CiscoWorks ロールおよび AUS 権限

	CiscoWorks ロール				
AUS 権限	System Admin	Network Admin	Network Operator	Approver	Help Desk
API_View_Device GUI_View_Device	X	X	X	X	X
API_View_Images GUI_View_Images	X	X	X	X	X
API_View_Assignment GUI_View_Assignment	X	X	X	X	X
API_View_Reports GUI_View_Reports	X	X	X	X	X

表 B-3　CiscoWorks ロールおよび AUS 権限 （続き）

AUS 権限	CiscoWorks ロール				
	System Admin	Network Admin	Network Operator	Approver	Help Desk
API_View_Admin GUI_View_Admin	X	X	X	X	X
API_Modify_Device GUI_Modify_Device	X	X	–	X	–
API_Modify_Images GUI_Modify_Image	X	X	–	–	–
API_Modify_Assignment GUI_Modify_Assignment	X	X	–	–	–
API_Modify_Admin GUI_Modify_Admin	X	X	–	–	–

Cisco Secure ACS ロールおよび AUS 権限

Cisco Secure ACS では、アプリケーション固有のロールがサポートされます。上位ロールには、下位ロールに関連付けられたすべての権限が含まれます。ACS を認証に使用する他のアプリケーションとは異なり、AUS では、デバイス単位ではなく、AUS 自体で認証を確認します。

ACS ですでに定義されている AUS ロールを使用することも、独自のカスタマイズ ロールを作成することもできます。

ACS の使用方法および、ACS のセキュリティに関するメリットについては、『*User Guide for Cisco Secure ACS for Windows Server*』を参照してください。

表 B-4 に AUS とともに使用できるデフォルトのロールを示します。

表 B-4　ACS ロール

ロール	説明
System Administrator	フル権限（スーパーユーザ）。
Network Administrator	フル権限（スーパーユーザ）。
Network Operator	GUI の読み取り権限。
AUS リモート インターフェイス	外部インターフェイスのみのアクセスが許可され、GUI へのアクセスは許可されません。
Help Desk	機密ではないデータの読み取り専用権限。
API Reader	外部インターフェイスの読み取り権限。
API Writer	外部インターフェイスの読み取り / 書き込み権限。
GUI Reader	GUI の情報を表示する読み取り権限。
GUI Writer	GUI の情報を表示および変更する読み取り / 書き込み権限。

（注）　Security Manager および AUS 間で正常に通信するには、Security Manager で AUS に対して入力したユーザ名およびパスワードを API_Writer ロール、同様の権限があるロール、または AUS リモート インターフェイスと関連付ける必要があります。

表 B-5 にデフォルトの AUS ロールおよびサポートされる権限を示します。権限の詳細については、表 B-1 を参照してください。

表 B-5　ACS ロールおよび AUS 権限

AUS 権限	ACS ロール							
	System Admin	Network Admin	Network Operator	Help Desk	API Reader	GUI Reader	API Writer	GUI Writer
API_View_Device	X	X	X	–	X	–	X	–
GUI_View_Device	X	X	X	X		X	–	X
API_View_Images	X	X	X	–	X	–	X	–
GUI_View_Images	X	X	X	X		X	–	X
API_View_Assignment	X	X	X	–	X	–	X	–
GUI_View_Assignment	X	X	X	X		X	–	X
API_View_Reports	X	X	X	–	X	–	X	–
GUI_View_Reports	X	X	X	X		X	–	X
API_View_Admin	X	X	X	X	X	–	X	–
GUI_View_Admin	X	X	X	–	–	X	–	X
API_Modify_Device	X	X	–	–	–	–	X	–
GUI_Modify_Device	X	X	–	–	–	–	–	X
API_Modify_Images	X	X	–	–	–	–	X	–
GUI_Modify_Images	X	X	–	–	–	–	–	X
API_Modify Assignment	X	X	–	–	–	–	X	–
GUI_Modify_Assignment	X	X	–	–	–	–	–	X
API_Modify_Admin	X	X	–	–	–	–	X	–
GUI_Modify_Admin	X	X	–	–	–	–	–	X

APPENDIX C

AUS と連動するためのデバイスのブートストラップ

AUS とデバイス間で通信できるようにするには、デバイスのトランスポートを設定してから、AUS または Security Manager のインベントリに追加します。デバイスは必要に応じて設定してください。

セキュリティ アプライアンスのブートストラップ

AUS を使用して PIX ファイアウォールまたは ASA デバイスを管理する前に、デバイスで基本的な接続ができるように最低限のコンフィギュレーションをデバイスで行います。基本的な接続の設定に関する詳細については、『*User Guide for Cisco Security Manager*』を参照してください。

基本的な接続に加えて、AUS 固有の設定を行う必要があります。次の手順では、デバイスのコマンドライン インターフェイスを使用してこの設定を実行および検証する方法を説明します。また、PIX Firewall Device Manager（PDM）セットアップ ウィザード（PIX バージョン 6.3 デバイスの場合）または Adaptive Security Device Manager（ASDM）セットアップ ウィザード（PIX 7.0+ または ASA デバイスの場合）を使用して設定できます。詳細については、ASA、ASDM、および PDM のマニュアルを参照してください。

（注） AUS を使用して ASDM および ASA ソフトウェア イメージを管理するには、**asdm image** および **boot system** コマンドを使用して ASA デバイスをブートストラップする必要があります。詳細については、「起動するソフトウェア イメージおよび ASDM イメージのコンフィギュレーション」（P.C-3）を参照してください。

PIX または ASA デバイスを AUS と連動するようにブートストラップするには、デバイスのコンソール ポートに接続されたコンソール端末から次の手順を実行します。

	コマンド	目的
ステップ 1	**enable** *password*	特権 EXEC モードに入ります。
ステップ 2	**config terminal**	設定モードを開始します。
ステップ 3	**http server enable**	デバイスの HTTP サーバを有効にして、ブラウザまたは HTTP 接続からコンフィギュレーションをモニタまたは変更できるようにします。

	コマンド	目的
ステップ 4	**http** *ip_address* [*netmask*] [*if_name*]	デバイスへの HTTP 接続を開始する権限を与えられたホストまたはネットワークを指定します。HTTP アクセスを許可するホストそれぞれにこのコマンドを入力します。 • *ip_address*：デバイスへの HTTP 接続を開始する権限を与えられたホストまたはネットワークの IP アドレスです。このコマンドを使用して少なくとも AUS および Security Manager サーバのアドレスを指定してください。 • *netmask*：IP アドレスのネットワーク マスクです。 • *if_name*：デバイスのインターフェイス名（デフォルトは **inside**）です。これを介して AUS または Security Manager によって HTTP 接続が開始されます。 **（注）** 即時自動更新を実行するには、これを設定してください。この設定によって、ASDM/PDM またはその他の HTTP 接続を介してデバイスにアクセスできるホストも決定されます。
ステップ 5	**auto-update server https://***username***:***password***@***AUSserver_IP_address***:***port***/autoupdate/AutoUpdateServlet**	デバイスを AUS に接続します。 • *username*：AUS サーバに入るためのログイン名です。 • *password*：ユーザのパスワードです。 • *AUSserver_IP_address*：AUS サーバの IP アドレスです。 • *port*：AUS サーバのポート番号です（通常は 443）。
ステップ 6	**auto-update poll-period** *poll_period [retry_count] [retry_period]*	AUS のポーリング時間を設定します。 • *poll_period*：2 つの更新の間のポーリング期間間隔。デフォルトは 720 分（12 時間）です。 • *retry_count*：サーバへの接続が失敗した場合に再試行する回数です。デフォルトは 0 です。 • *retry_period*：再試行の間隔です（分）。デフォルトは 5 です。
ステップ 7	**auto-update device-id [hardware-serial | hostname | ip_address** [*if_name*] | **mac-address** [*if_name*] | **string** *text* **]**	指定したデバイス ID を使用して自身を識別するようにデバイスが設定されます。 • *if_name*：デバイス インターフェイス名です（デフォルトは **inside**）。 • *text*：デバイスを識別するテキストです。 次の例では、ホスト名がデバイス ID として使用されています。 `auto-update device-id hostname`
ステップ 8	**write memory**	コンフィギュレーションを保存します。
ステップ 9	**show auto-update**	AUS URL、ポーリング時間、タイムアウト、およびデバイス ID を表示します。設定を確認できます。
ステップ 10	**exit**	設定モードを終了します。

起動するソフトウェア イメージおよび ASDM イメージのコンフィギュレーション

デフォルトでは、セキュリティ アプライアンスによって内蔵フラッシュ メモリで最初に検出されたソフトウェア イメージが使用されます。また、内蔵フラッシュ メモリで最初に検出された ASDM イメージまたは、イメージがない場合は次に、外付けフラッシュ メモリで最初に検出されたイメージが起動されます。複数のイメージがある場合は、起動するイメージを指定してください。ASDM イメージの場合、起動するイメージを指定しないと、イメージが 1 つのみインストールされている場合でも、セキュリティ アプライアンスによって **asdm image** コマンドが実行されているコンフィギュレーションに挿入されます。自動更新で発生する問題を回避するため（設定されている場合）、または起動時に毎回イメージが検索されないようにするためには、スタートアップ コンフィギュレーションで起動する ASDM イメージを指定してください。

AUS を使用してデバイスにダウンロードされたイメージのバージョンをセキュリティ アプライアンスで **boot system** および **asdm image** コマンドを使用して示す必要があります。これを実行しないと、セキュリティ アプライアンスのイメージは、AUS からダウンロードされた最新のバージョンによって上書きされ、ASDM イメージの更新に失敗する場合があります。

また、セキュリティ アプライアンスに割り当てられたコンフィギュレーション ファイルは、デバイスに設定された同じブート ソフトウェア イメージおよび ASDM イメージを示す必要があります。示されていない場合、セキュリティ アプライアンスにある既存のイメージは、AUS からダウンロードされる最新のバージョンによって上書きされます。

セキュリティ アプライアンスで次のメッセージが表示された場合、セキュリティ アプライアンスの ASDM イメージが現行のバージョンと互換性があることを確認してください。この条件は、デバイスで **show run** コマンドの出力を表示することで確認できます。

```
Auto-update client: Sent DeviceDetails to /autoupdate/AutoUpdateServlet of server
10.1.1.200
Auto-update client: Processing UpdateInfo from server 10.1.1.200
Auto-update client: Failed to contact: https://10.1.1.200/autoupdate/AutoUpdateServlet,
reason: ErrorList error code: CALLHOME-PARSER-ERROR, description: The XML parser
encountered an error: The content of element type "DeviceDetails" must match
"(DeviceID,HostName,PlatformFamily,PlatformType,SerialNumber,SysObjectId,IPAddress+,Versio
nInfo*,Memory*)
```

次では、これらをデバイスのコマンド ラインを使用して設定する手順を説明します。また、Security Manager で [Platform] > [Device Admin] > [Boot Image/Configuration] ポリシーを使用しても設定できます。

- 起動するソフトウェア イメージを設定するには、次のコマンドを入力します。

  ```
  hostname(config)# boot system url
  ```

  url に次のいずれかを入力します。

  - {**flash:/** | **disk0:/** | **disk1:/**}[*path/*]*filename*

    flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内蔵フラッシュ メモリを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内蔵フラッシュ メモリには、**flash:/** または **disk0:/** と入力できます。**disk1:/** キーワードは、ASA の外付けフラッシュ メモリを示します。

  - **tftp://**[*user*[**:*password***]**@**]*server*[:*port*]/[*path/*]*filename*

    このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみサポートされます。

  boot system コマンド エントリを最大 4 つ入力して、順番に起動する異なるイメージを指定できます。セキュリティ アプライアンスによって最初に検索されたイメージが起動されます。**boot system tftp:** コマンドは 1 つのみ設定でき、最初に設定する必要があります。

- 起動する ASDM イメージを設定するには、次のコマンドを入力します。

  hostname(config)# **asdm image** {**flash:/** | **disk0:/** | **disk1:/**}[*path***/**]*filename*

INDEX

A

C

D

G

H

N

P

と

に

ね

ふ

へ

ほ

め

も

ゆ

れ