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
チェックボックス	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.2-7）を参照してください。

表 2-1　[Device Summary] ページ（続き）

要素	説明
[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。
[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変更できません。プロパティを変更する場合（資格情報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]：資格情報がありません。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。この資格情報はデバイス 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 資格情報を TACACS+ 資格情報として使用します。

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]：デバイスは毎週更新されます。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+ 資格情報（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。これらの資格情報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 資格情報を TACACS+ 資格情報として使用します）。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+ 資格情報（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。