デバイス プロパティの設定

ここでは、次の項目について説明します。

Management IP

Configuration > Properties > Management IP

Management IP ウィンドウで、セキュリティ アプライアンスの管理 IP アドレスまたは透過ファイアウォール モードのコンテキストの管理 IP アドレスを設定できます。透過ファイアウォールは、IP ルーティングに参加しません。セキュリティ アプライアンスで必要とされる唯一の IP コンフィギュレーションは、管理 IP アドレスの設定です。例外として、Management 0/0 管理専用インターフェイスに IP アドレスを設定できますが、トラフィックはこのインターフェイスを通過できません。Management 0/0 の IP アドレスの設定については、「インターフェイスの設定」を参照してください。

このアドレスは、システム メッセージまたは AAA サーバとの通信など、セキュリティ アプライアンス上で発信されるトラフィックの送信元アドレスとしてセキュリティ アプライアンスが使用するために必要です。このアドレスは、リモート管理アクセスにも使用できます。

フィールド

- Management IP Address：管理 IP アドレスを設定します。
- Subnet Mask：サブネット マスクを設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
—	•	•	•	—

Device Administration

Device Administration で、セキュリティ アプライアンスに基本的なパラメータを設定できます。ここでは、次の項目について説明します。

Banner

Configuration > Properties > Device Administration > Banner

Banner パネルで、当日のお知らせメッセージ、ログイン、セッション バナーを設定できます。

バナーを作成するには、該当するボックスにテキストを入力します。テキストに入力したスペースはそのまま表示されます。タブは ASDM インターフェイスで入力します。コマンドラインから入力できません。トークンの $(domain) および $(hostname) は、セキュリティ アプライアンスのドメイン名およびホスト名に置き換えられます。

$(hostname) および $(domain) トークンを使用すると、特定のコンテキストで指定したホスト名とドメイン名を画面に表示できます。$(system) トークンを使用して、特定のコンテキストのシステム スペースで設定したバナーを画面に表示できます。

バナーが複数行の場合、行ごとに入力したテキストが既存のバナーの最後に追加されます。テキストが空の場合、復帰記号（CR）がバナーに追加されます。RAM やフラッシュ メモリの容量が許す限り、バナーの長さに制限はありません。ASCII 文字のみ使用できます。改行（Enter キー。2 文字に相当）も使用できます。

Telnet または SSH でセキュリティ アプライアンスにアクセスしたとき、システム メモリが不足してバナー メッセージを表示できなかったり、バナー メッセージを表示するときに TCP 書き込みエラーが発生したりするとセッションは終了します。

バナーを置き換えるには、該当するボックスの内容を変更して **Apply** をクリックします。バナーをクリアするには、該当するボックスの内容をクリアして **Apply** をクリックします。

システム コンテキストでは ASDM のパネルからバナー コマンドを使用できませんが、**Tools > Command Line Interface** から設定できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Boot Image/Configuration

Configuration > Properties > Device Administration > Boot Image/Configuration

Boot Image/Configuration で選択したイメージ ファイルからセキュリティ アプライアンスをブートできます。また、起動時に使用するコンフィギュレーション ファイルもここで選択できます。

起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバのイメージを 1 つ指定し、そこからデバイスをブートできます。TFTP サーバのイメージ ファイルを指定する場合、リストの先頭に指定してください。TFTP サーバにアクセスできず、イメージ ファイルをそこからロードできない場合は、リストでその次に指定されたイメージ ファイルがフラッシュ メモリからロードされます。

ブート変数を指定しなければ、内部フラッシュ メモリの先頭にある有効なイメージからシステムがブートされます。

フィールド

Boot Configuration

- ***Boot Order***：ブート時に使用されるバイナリ イメージ ファイルの順序を表示します。
- ***Boot Image Location***：ブート ファイルの物理的な場所とパスを表示します。
- ***Boot Config File Path***：コンフィギュレーション ファイルの場所を表示します。
- ***Add***：ブート時に使用するフラッシュ メモリまたは TFTP サーバのブート イメージ エントリを追加します。
- ***Edit***：フラッシュ メモリまたは TFTP サーバのイメージ エントリを編集します。
- ***Delete***：フラッシュ メモリまたは TFTP サーバのイメージ エントリを選択して、削除します。
- **Move Up**：フラッシュ メモリまたは TFTP サーバのイメージ エントリを選択して、ブート順序を上に移動します。
- ***Move Down***：フラッシュ メモリまたは TFTP サーバのイメージ エントリを選択して、ブート順序を下に移動します。
- ***Browse Flash***：ブート イメージ ファイルまたはコンフィギュレーション ファイルの場所を指定します。

ASDM Image Configuration

- ***ASDM Image File Path***：起動時に使用するコンフィギュレーション ファイルの場所を表示します。
- ***Browse Flash***：ブート イメージ ファイルまたはコンフィギュレーション ファイルの場所を指定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Add Boot Image

Configuration > Properties > Device Administration > Boot Image/Configuration > Add Boot Image

ブート イメージ エントリをブート順序リストに追加するには、**Boot Image/Configuration** パネルの ***Add*** をクリックします。

フラッシュ メモリまたは TFTP サーバのイメージを選択して、ブート イメージをブート順序リストに追加できます。

イメージのパスを入力するか ***Browse Flash*** をクリックして、イメージの場所を指定します。TFTP の場合、イメージの場所のパスを入力する必要があります。

フィールド

- **Flash Image**：フラッシュ ファイル システムのブート イメージを選択して追加します。
  - **Path**：フラッシュ ファイル システムにあるブート イメージのパスを指定します。
- **TFTP Image**：TFTP サーバのブート イメージを選択して追加します。
  - **[Path]**：TFTP サーバのブート イメージ ファイルのパスを入力します。サーバの IP アドレスも指定します。
- **OK**：変更を有効にして、直前のパネルに戻ります。
- **Cancel**：変更を無効にして、直前のパネルに戻ります。
- **Help**：詳細情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Clock

Configuration > Properties > Device Administration > Clock

Clock パネルで、日付と時刻をセキュリティ アプライアンスに手動で設定します。時刻は ASDM メイン ウィンドウの下部のステータスバーに表示されます。

マルチコンテキスト モードでは、時刻はシステム コンフィギュレーションのみに設定してください。

NTP サーバを利用して時刻をダイナミックに設定するには、**NTP** パネルを参照して NTP サーバから時刻を取得すると **Clock** で手動で設定した時刻をいつでも上書きできます。

フィールド

- **Time Zone**：時間帯は、適切な数値を GMT に追加または削除して設定します。Eastern Time、Central Time、Mountain Time、または Pacific Time を時間帯として選択すると、4 月の第一日曜日の午前 2 時と 10 月の最終日曜日の午前 2 時に夏時間が自動的に設定されます。

（注） セキュリティ アプライアンスの時間帯を変更すると、インテリジェント SSM との接続がドロップされる場合があります。

- **Date**：日付を設定します。リストから年と日付を選択して、カレンダーの日をクリックします。
- **Time**：時刻を 24 時間制で設定します。
  - **hh**、**mm**、および **ss** ボックス：時間、分、秒を設定します。
- **Update Display Time**：ASDM ウィンドウの右下の表示時刻が更新されます。現在時刻は 10 秒ごとに自動更新されます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Console

Configuration > Properties > Device Administration > Console

Console パネルで、管理コンソールの表示時間（分単位）を指定できます。ここで指定した時間が経過すると、コンソールは自動的にシャットダウンします。

Console Timeout テキストボックスに時間を入力します。制限しない場合は 0 を入力します。デフォルト値は 0 です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Device

Configuration > Properties > Device Administration > Device

Device パネルで、ホスト名とドメイン名をセキュリティ アプライアンスに設定できます。

ホスト名はコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。ホスト名はシステム メッセージでも使用されます。

マルチコンテキスト モードでは、システム実行スペースで設定したホスト名がすべてのコンテキストのコマンドライン プロンプトに表示されます。コンテキストで設定したホスト名を、コマンドラインに表示せず、バナーに表示するオプションもあります。

セキュリティ アプライアンスは、ドメイン名を未修飾名に拡張子として追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバに未修飾名「jupiter」を指定すると、セキュリティ アプライアンスは、この名前を「jupiter.example.com」に限定します。

フィールド

- *Platform* **Host Name**：ホスト名を設定します。デフォルトのホスト名は、プラットフォームの種類によって決まります。
- **Domain Name**：ドメイン名を設定します。デフォルトのドメイン名は、default.domain.invalid です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	•

FTP Mode

Configuration > Properties > Device Administration > FTP Mode

FTP Mode パネルで、FTP モードをアクティブまたはパッシブに設定できます。セキュリティ アプライアンスがイメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバにアップロードしたり、FTP サーバからダウンロードできるようになります。パッシブ FTP クライアントは、コントロール接続とデータ接続を両方とも起動できます。サーバはパッシブ モードでデータ接続の宛先になり、特定の接続の受信時にポート番号に応答します。

フィールド

- **Specify FTP mode as passive**：FTP モードをアクティブまたはパッシブに設定します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

ICMP Rules

Configuration > Properties > Device Administration > ICMP Rules

ICMP Rules パネルで、ICMP ルール テーブルを表示し、セキュリティ アプライアンスに ICMP でアクセスするすべてのホストまたはネットワークの許可 / 拒否を指定します。このテーブルでホストまたはネットワークを追加、変更すると、セキュリティ アプライアンスに送信された ICMP メッセージを許可または禁止できます。

ICMP ルールは、セキュリティ アプライアンス インターフェイスに ICMP トラフィックが着信した場合の制御方法を表示します。ICMP コントロール リストが設定されていない場合、セキュリティ アプライアンスは外部インターフェイスも含め、インターフェイスに着信した ICMP トラフィックをすべて許可します。ただし、デフォルトでは、セキュリティ アプライアンスはブロードキャスト アドレスへの ICMP エコー要求に応答しません。

（注）　**Security Policy** パネルで ICMP トラフィックのアクセス ルールを設定すると、宛先のインターフェイスが保護されていてもセキュリティ アプライアンスを *通過* ルートにできます。

ICMP の到達不能メッセージ タイプ（type 3）の権限は、常に許可にすることをお勧めします。ICMP の到達不能メッセージを拒否すると、ICMP の Path MTU Discovery 機能がディセーブルになり、IPSec および PPTP トラフィックが停止する場合があります。Path MTU Discovery の詳細については、RFC 1195 および RFC 1435 を参照してください。

ICMP コントロール リストを設定すると、セキュリティ アプライアンスでは最初に一致した条件を ICMP トラフィックに適用し、暗黙的にすべてを拒否します。したがって、最初に一致したエントリが許可の場合は、ICMP パケットはそのまま処理されます。最初に一致したエントリが拒否の場合または一致しなかった場合は、セキュリティ アプライアンスで ICMP パケットは破棄され、syslog メッセージが出力されます。例外は ICMP コントロール リストが設定されていない場合です。その場合、**許可**が設定されているものとして処理されます。

フィールド

- **Interface**：ICMP アクセスが許可されるセキュリティ アプライアンスのインターフェイスを一覧表示します。
- **Action**：指定したネットワークまたはホストの ICMP 受信メッセージの許可/拒否を表示します。
- **IP Address**：アクセスを許可 / 拒否するネットワークまたはホストの IP アドレスを一覧表示します。
- **Mask**：アクセスを許可するネットワークまたはホストに関連付けられたネットワーク マスクを一覧表示します。
- **ICMP Type**：ルールを適用する ICMP メッセージ タイプを一覧表示します。表 8-1 に示す ICMP タイプがサポートされます。
- **Add**：**Add ICMP Rule** ダイアログボックスが表示され、新規の ICMP ルールをテーブルの最後に追加できます。
- **Insert Before**：ICMP ルールを選択中のルールの前に追加します。
- **Insert After**：ICMP ルールを選択中のルールの後に追加します。
- **Edit**：**Edit ICMP Rule** ダイアログボックスが表示され、選択したホストまたはネットワークを編集できます。
- **Delete**：選択したホストまたはネットワークを削除します。

表 8-1　ICMP タイプ リテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit ICMP Rule

Configuration > Properties > Device Administration > ICMP Rules > Add/Edit ICMP Rule

Add/Edit ICMP Rule ダイアログボックスで、ICMP ルールの追加または変更ができます。ICMP ルールでは、セキュリティ アプライアンスへの ICMP アクセスが許可 / 拒否されるホストまたはネットワークのアドレスをすべて指定できます。

フィールド

- **ICMP Type**：ルールを適用する ICMP メッセージ タイプを指定します。表 8-2 に示す ICMP タイプがサポートされます。
- **Interface**：ICMP アクセスが許可されるセキュリティ アプライアンスのインターフェイスを識別します。
- **IP Address**：アクセスを許可 / 拒否するネットワークまたはホストの IP アドレスを指定します。
- **Any Address**：指定したインターフェイスのすべての受信アドレスにアクションを適用します。
- **Mask**：アクセスを許可するネットワークまたはホストに関連付けられたネットワーク マスクを指定します。
- **Action**：指定したネットワークまたはホストの ICMP 受信メッセージの許可/拒否を指定します。
  - **Permit**：指定したホストまたはネットワークと、アクセス許可されたインターフェイスの ICMP メッセージを作成します。
  - **Deny**：指定したホストまたはネットワークと、ドロップされたインターフェイスの ICMP メッセージを作成します。

表 8-2　ICMP タイプ リテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request

表 8-2　ICMP タイプ リテラル（続き）

ICMP タイプ	リテラル
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Management Access

Configuration > Properties > Device Administration > Management Access

Management Access パネルで、高度なセキュリティ インターフェイスの管理アクセスをイネーブル / ディセーブルに切り換え、セキュリティ アプライアンスの管理機能を実行できます。管理アクセスをイネーブルにすると、IPSec VPN トンネルで固定された IP アドレスを持つ内部インターフェイスで、ASDM を実行できます。この機能を使用する場合は、VPN をセキュリティ アプライアンスで設定し、外部インターフェイスにダイナミック IP アドレス割り当てを適用します。たとえば、セキュリティ アプライアンスを自宅から VPN クライアントでアクセスするような場合のセキュリティ管理で役立ちます。

フィールド

- **Management Access Interface** : セキュリティ アプライアンスの管理インターフェイスを指定します。**None** の場合、管理アクセスはディセーブルです。これはデフォルトです。管理アクセスをイネーブルにするには、インターフェイスのセキュリティを最も高く設定し、内部インターフェイスにします。一度に 1 つのインターフェイスだけの管理アクセスをイネーブルにできます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	—	•	—	—

NTP

Configuration > Properties > Device Administration > NTP

NTP パネルで、NTP サーバを定義して、セキュリティ アプライアンスに時刻をダイナミックに設定できます。時刻は ASDM メイン ウィンドウの下部のステータスバーに表示されます。

Clock パネルで手動設定した時刻はすべて、NTP サーバから取得された時刻によって上書きされます。

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。セキュリティ アプライアンスは一番下の階層からサーバを選択し、データ信頼度の尺度にします。

フィールド

- **NTP Server List**：定義されている NTP サーバを示します。
  - **IP Address**：NTP サーバの IP アドレスを示します。
  - **Interface**：NTP パケットの発信インターフェイスが設定されている場合、そのインターフェイスを示します。システムにインターフェイスがない場合、管理コンテキスト インターフェイスが使用されます。インターフェイスが空白の場合、セキュリティ アプライアンスが使用するデフォルトの管理コンテキスト インターフェイスは、ルーティング テーブルによって決まります。
  - **Preferred?**：この NTP サーバが優先サーバかどうかを Yes または No で示します。NTP はアルゴリズムを使用して最も精度の高いサーバを判別し、そのサーバに同期します。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバよりはるかに精度の高いサーバがある場合は、セキュリティ アプライアンスはその精度の高いサーバを使用します。たとえば、セキュリティ アプライアンスはより精度の高いサーバを使用し、優先サーバの精度が低ければ使用しません。
  - **Key Number**：認証キーの ID 番号を示します。
  - **Trusted Key?**：キーが trusted key かどうかを Yes または No で示します。trusted key だけが認証されます。
- **Enable NTP Authentication**：すべてのサーバの認証をイネーブルにします。
- **Add**：NTP サーバを追加します。
- **Edit**：NTP サーバを編集します。
- **Delete**：NTP サーバを削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Add/Edit NTP Server Configuration

Configuration > Properties > Device Administration > NTP > Add/Edit NTP Server Configuration

Add/Edit NTP Server Configuration ダイアログボックスで、NTP サーバを追加または編集できます。

フィールド

- **IP Address**：NTP サーバの IP アドレスを設定します。
- **Preferred**：このサーバを優先サーバに設定します。NTP は、アルゴリズムを使用して最も精度の高いサーバを判別し、そのサーバに同期します。精度が同じ程度であれば、優先サーバを使用します。ただし、優先サーバよりはるかに精度の高いサーバがある場合は、セキュリティ アプライアンスはその精度の高いサーバを使用します。たとえば、セキュリティ アプライアンスはより精度の高いサーバを使用し、優先サーバの精度が低ければ使用しません。
- **Interface**：NTP パケットの発信インターフェイスを設定します。ルーティング テーブルによるデフォルト インターフェイスを変更できます。システムにインターフェイスがない場合、管理コンテキスト インターフェイスが使用されます。管理コンテキスト（使用できるインターフェイス）を変更する場合は、安定性のために **None**（デフォルト インターフェイス）を選択してください。
- **Authentication Key**：MD5 認証で NTP サーバと通信する場合に、認証キーのアトリビュートを設定します。
  - **Key Number**：認証キーのキー ID を設定します。NTP サーバのパケットもこのキー ID を使用する必要があります。他のサーバのキー ID が設定済みの場合は、リストから選択できます。入力する場合は、1 ～ 4294967295 の範囲の値を指定します。
  - **Trusted**：このキーを trusted key として設定します。このチェックボックスをオンにしないと、認証されません。
  - **Key Value**：認証キーを 32 文字以内で設定します。
  - **Reenter Key Value**：正しいキーであることを確認するため、キーを 再度入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

Password

Configuration > Properties > Device Administration > Password

Password パネルで、ログイン パスワードとイネーブル パスワードを設定できます。

セキュリティ アプライアンスに接続して Telnet または SSH セッションを実行している場合、ログイン パスワードで EXEC モードにアクセスできます。（Telnet または SSH のアクセスにユーザ認証を設定すると、ユーザは自分のパスワードを使用し、ログイン パスワードを使用しません。**AAA Access** パネルを参照してください）。

イネーブル パスワードでログインすると、特権 EXEC モードにアクセスできます。また、このパスワードは、デフォルト ユーザ名で ASDM にアクセスする場合にも使用します。デフォルト ユーザ名は空白になっています。デフォルト ユーザ名は **User Accounts** パネルに「enable_15」と表示されます（イネーブル アクセスにユーザ認証を設定すると、ユーザは自分のパスワードを使用し、イネーブル パスワードを使用しません。**AAA Access** パネルを参照してください。さらに、HTTP/ASDM アクセスにも認証を設定できます）。

フィールド

- **Enable Password**：イネーブル パスワードを設定します。デフォルトでは空白になっています。
  - **Change the privileged mode password**：イネーブル パスワードを変更します。
  - **Old Password**：変更前のパスワードを入力します。
  - **New Password**：変更後のパスワードを入力します。
  - **Confirm New Password**：変更後のパスワードを確認します。
- **Telnet Password**：ログイン パスワードを設定します。デフォルトでは「cisco」です。このグループのボックスは Telnet Password になっていますが、このパスワードで Telnet と SSH にアクセスできます。
  - **Change the password to access the** *platform* **console**：ログイン パスワードを変更します。
  - **Old Password**：変更前のパスワードを入力します。
  - **New Password**：変更後のパスワードを入力します。
  - **Confirm New Password**：変更後のパスワードを確認します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Secure Copy

Configuration > Properties > Device Administration > Secure Copy

Secure Copy パネルで、セキュリティ アプライアンスのセキュア コピー サーバをイネーブルにします。SSH を利用するセキュリティ アプライアンスのアクセスを許可されたクライアントだけが、セキュア コピー接続を確立できます。

制限事項

セキュア コピー サーバの実装には、次の制限事項があります。

- サーバはセキュア コピー接続の受け入れと終了はできますが、起動はできません。
- サーバは、ディレクトリの指定をサポートしていません。そのため、リモート クライアント アクセスでセキュリティ アプライアンスの内部ファイル参照はできません。
- サーバは、バナーをサポートしていません。
- サーバは、ワイルドカードをサポートしていません。
- SSH バージョン 2 で接続するには、セキュリティ アプライアンスのライセンスに VPN-3DES-AES 機能が必要です。

フィールド

- **Enable Secure Copy Server**：セキュリティ アプライアンスのセキュア コピー サーバをイネーブルにします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	•

SMTP

Configuration > Properties > Device Administration > SMTP

SMTP パネルで、発生した重要イベントを電子メールで通知する SMTP クライアントをイネーブル / ディセーブルにできます。ここで追加できるのは SMTP サーバの IP アドレスで、オプションとしてバックアップ サーバの IP アドレスも設定できます。ASDM は IP アドレスが有効かどうかをチェックしません。アドレスを正確に入力してください。

警告を受信する電子メール アドレスは、***Configuration*** > ***Properties*** > ***Logging*** > ***Email Setup*** で設定します。

フィールド

- **Remote SMTP Server**：プライマリ SMTP サーバとセカンダリ SMTP サーバを設定します。
- **Primary Server IP Address**：SMTP サーバの IP アドレスを入力します。
- **Secondary Server IP Address (Optional)**：セカンダリ SMTP サーバの IP アドレスを入力します（オプション）。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP

Configuration > Properties > Device Administration > SNMP

SNMP パネルで、セキュリティ アプライアンスを簡易ネットワーク管理プロトコル（SNMP）管理ステーションから監視できるように設定できます。

ネットワーク管理ステーションを PC またはワークステーションで実行し、スイッチ、ルータ、セキュリティ アプライアンスなど、さまざまなタイプのデバイスのステータスとヘルスを監視する標準的な方法を SNMP で定義できます。

SNMP の用語

- **Management station** : PC またはワークステーションで実行されるネットワーク管理ステーションです。SNMP プロトコルを使用して、管理対象デバイスの標準データベースを管理します。ハードウェアの障害など注意が必要なイベントのメッセージも受信できます。

- **Agent**：SNMP コンテキストでは、管理ステーションが*クライアント*、セキュリティ アプライアンスで動作する SNMP エージェントが*サーバ*になります。
- **OID**：SNMP 規格では、システム オブジェクト ID（OID）を設定して、管理ステーションが SNMP エージェントがあるネットワーク デバイスを一意に識別したり、ユーザに分かるように監視情報の発生元を表示したりします。
- **MIB**：エージェントは Management Information Databases（MIB; 管理情報データベース）と呼ばれる標準データ構造を保持します。これが管理ステーションに蓄積されます。MIB は、パケット、接続、エラー カウンタ、バッファの使用状況、フェールオーバー ステータスなどの情報を収集します。MIB は製品ごとに定義され、通常のネットワーク デバイスで使用される一般的なプロトコルとハードウェア規格も MIB に定義されています。SNMP 管理ステーションから MIB を参照したり、特定のフィールドだけを要求したりできます。一部のアプリケーションでは、管理目的で MIB データを変更する場合があります。
- **Trap**：エージェントはアラーム条件も監視します。リンク アップ、リンク ダウン、syslog イベントなどトラップに定義したアラーム条件が発生すると、エージェントは指定された管理ステーションにただちに通知します。この通知は SNMP トラップとも呼ばれます。

SNMP

シスコの MIB ファイルおよび OID については、
http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。OID は、次の URL からダウンロードすることもできます。
ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz

MIB のサポート

セキュリティ アプライアンスは、次の SNMP MIB をサポートしています。

（注）　セキュリティ アプライアンスは、Cisco syslog MIB のブラウジングはサポートしません。

- MIB-II の System グループと Interface グループをブラウジングできます。MIB のブラウジングはトラップの送信とは違います。ブラウジングとは、管理ステーションから MIB ツリーの snmpget や snmpwalk を実行し、値を決定することです。
- Cisco MIB および Cisco Memory Pool MIB を使用できます。
- セキュリティ アプライアンスは、次の Cisco MIB をサポートしていません。
- cfwSecurityNotification NOTIFICATION-TYPE
- cfwContentInspectNotification NOTIFICATION-TYPE
- cfwConnNotification NOTIFICATION-TYPE
- cfwAccessNotification NOTIFICATION-TYPE
- cfwAuthNotification NOTIFICATION-TYPE
- cfwGenericNotification NOTIFICATION-TYPE

SNMP CPU 使用状況

セキュリティ アプライアンスは、SNMP を利用する CPU 使用状況のモニタリングをサポートしています。セキュリティ アプライアンスの CPU 使用状況を監視する際、HP OpenView などの SNMP 管理ソフトウェアを利用すると、ネットワーク管理者は容量プランを作成できます。

この機能は、Cisco Process MIB（CISCO-PROCESS-MIB.my）の cpmCPUTotalTable のサポート機能によって組み込まれています。MIB には他に 2 つのテーブル（cpmProcessTable、cpmProcessExtTable）がありますが、今回のリリースではサポートされていません。

cpmCPUTotalTable の各行には、CPU のインデックスと次のオブジェクトが含まれます。

MIB オブジェクト名	説明
cpmCPUTotalPhysicalIndex	このオブジェクトの値は 0 になります。Entity MIB の entPhysicalTable of Entity MIB をセキュリティ アプライアンスの SNMP エージェントがサポートしていないためです。
cpmCPUTotalIndex	このオブジェクトの値は 0 になります。Entity MIB の entPhysicalTable of Entity MIB をセキュリティ アプライアンスの SNMP エージェントがサポートしていないためです。
cpmCPUTotal5sec	直前 5 秒間の CPU 全体のビジー率
cpmCPUTotal1min	直前 1 分間の CPU 全体のビジー率
cpmCPUTotal5min	直前 5 分間の CPU 全体のビジー率

（注）　現在のセキュリティ アプライアンス ハードウェア プラットフォームは単一 CPU だけサポートしているため、セキュリティ アプライアンスが返す cpmCPUTotalTable は 1 行だけで、インデックスは常に 1 になります。

直前の 3 要素の値は、show cpu usage コマンドの出力値と同じです。

次の新しい MIB オブジェクトが cpmCPUTotalTable にありますが、セキュリティ アプライアンスではサポートされていません。

- cpmCPUTotal5secRev
- cpmCPUTotal1minRev
- cpmCPUTotal5minRev

フィールド

- **Community string (default)**：パスワードを入力します。SNMP 管理ステーションはセキュリティ アプライアンスに要求を送信するとき、このパスワードを使用します。SNMP のコミュニティ ストリングは、SNMP 管理ステーションと管理対象ネットワーク ノード間で共有される秘密情報です。セキュリティ アプライアンスはパスワードを参照して、受信する SNMP 要求が有効かどうかを決定します。パスワードは、大文字と小文字が区別される最大 32 文字の値です。スペースは使用できません。デフォルトは「public」です。SNMPv2c では、管理ステーションごとに別のコミュニティ ストリングを設定できます。コミュニティ ストリングがどの管理ステーションにも設定されていない場合、ここで設定した値がデフォルトとして使用されます。
- **Contact**：セキュリティ アプライアンスのシステム管理者の名前を入力します。テキストは最大 127 文字で、大文字と小文字を区別します。スペースは使用できますが、連続するスペースは 1 桁のスペースに縮められます。
- **Security Appliance Location**：セキュリティ アプライアンスの場所を指定します。テキストは最大 127 文字で、大文字と小文字を区別します。スペースは使用できますが、連続するスペースは 1 桁のスペースに縮められます。
- **Listening Port**：SNMP トラフィックが送信されるポートを指定します。デフォルトは 161 です。
- **Configure Traps**：イベントを設定すると、SNMP トラップを利用して通知できます。
- **SNMP Management Station** ボックス
  - **Interface**：SNMP 管理ステーションが存在するセキュリティ アプライアンスのインターフェイス名を表示します。

- **IP Address**：SNMP 管理ステーションの IP アドレスを表示します。セキュリティ アプライアンスはこのアドレスを使ってトラップ イベントを送信したり、要求またはポーリングを受信したりします。
- **Community string**：管理ステーションでコミュニティ ストリングを指定しない場合、**Community String (default)** フィールドの設定値が使用されます。
- **SNMP Version**：管理ステーションに設定されている SNMP のバージョンを表示します。
- **Poll/Trap**：この管理ステーションの通信方式を表示します。ポーリングのみ、トラップのみ、ポーリングとトラップがあります。ポーリングとは、一定間隔で繰り返し送信される管理ステーションの要求をセキュリティ アプライアンスが待つことをいいます。トラップを設定すると、発生した syslog イベントが送信されます。
- **UDP Port**：SNMP ホストの UDP ポートです。デフォルト ポートは 162 です。

- **Add**：**Add SNMP Host Access Entry** が開き、次のフィールドを設定できます。
- **Interface Name**：管理ステーションが存在するインターフェイスを選択します。
- **IP Address**：管理ステーションの IP アドレスを指定します。
- **Server Poll/Trap Specification**：**Poll** または **Trap** を選択します。両方を選択することもできます。
- **UDP Port**：SNMP ホストの UDP ポートです。このフィールドを指定すると、SNMP ホストのデフォルト UDP ポート番号 162 が上書きされます。
- **Help**：詳細情報を表示します。
- **Edit**：**Edit SNMP Host Access Entry** ダイアログボックスが開き、追加の場合と同じフィールドが表示されます。
- **Delete**：選択した項目を削除します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit SNMP Host Access Entry

Configuration > Properties > Device Administration > SNMP > Add/Edit SNMP Host Access Entry

SNMP 管理ステーションの追加

SNMP 管理ステーションを追加するには、次の手順を実行します。

1. **Add** をクリックし、**SNMP Host Access Entry** ダイアログボックスを開きます。
2. **Interface Name** から SNMP 管理ステーションが存在するインターフェイスを選択します。
3. 管理ステーションの IP アドレスを **IP Address** に入力します。
4. SNMP ホストの UDP ポートを入力します。デフォルトは 162 です。
5. SNMP ホストの Community String パスワードを入力します。管理ステーションでコミュニティ ストリングを指定しない場合、SNMP Configuration 画面の **Community String (default)** フィールドに設定した値が使用されます。
6. **Poll** または **Trap** をクリックして選択します。両方を選択することもできます。

7. 次のボタンをクリックすると、直前のパネルに戻ります。
   - **OK**：変更を有効にして、直前のパネルに戻ります。
   - **Cancel**：変更を無効にして、直前のパネルに戻ります。
   - **Help**：詳細情報を表示します。

SNMP 管理ステーションの編集

SNMP 管理ステーションを編集するには、次の手順を実行します。

1. **SNMP** パネルで SNMP 管理ステーション テーブルのリスト項目を選択します。
2. **Edit** をクリックし、**Edit SNMP Host Access Entry** を開きます。
3. **Interface Name** から SNMP 管理ステーションが存在するインターフェイスを選択します。
4. 管理ステーションの IP アドレスを **IP Address** に入力します。
5. SNMP ホストの Community String パスワードを入力します。管理ステーションでコミュニティ ストリングを指定しない場合、SNMP Configuration 画面の **Community String (default)** フィールドに設定した値が使用されます。
6. SNMP ホストの UDP ポートを入力します。デフォルトは 162 です。
7. **Poll** または **Trap** をクリックして選択します。両方を選択することもできます。
8. SNMP のバージョンを選択します。
9. 次のボタンをクリックすると、直前のパネルに戻ります。
   - **OK**：変更を有効にして、直前のパネルに戻ります。
   - **Cancel**：変更を無効にして、直前のパネルに戻ります。
   - **Help**：詳細情報を表示します。

SNMP 管理ステーションの削除

テーブルから SNMP 管理ステーションを削除するには、次の手順を実行します。

1. **SNMP** パネルで SNMP 管理ステーション テーブルの項目を選択します。
2. **Delete** をクリックします。

フィールド

- **Interface name**：SNMP ホストが存在するインターフェイスを選択します。
- **IP Address**：SNMP ホストの IP アドレスを入力します。
- **UDP Port**：SNMP アップデートの送信先にする UDP ポートを入力します。デフォルトは 162 です。
- **Community String**：SNMP サーバのコミュニティ ストリングを入力します。
- **SNMP Version**：SNMP のバージョンを選択します。
- **Server Port/Trap Specification**
  - **Poll**：ポーリング情報を送信します。ポーリングとは、一定間隔で繰り返し送信される管理ステーションの要求をセキュリティ アプライアンスが待つことをいいます。
  - **Trap**：トラップ情報を送信します。トラップを設定すると、発生した syslog イベントが送信されます。
- **OK**：変更を有効にして、直前のパネルに戻ります。
- **Cancel**：変更を無効にして、直前のパネルに戻ります。
- **Help**：詳細情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

SNMP Trap Configuration

Configuration > Properties > Device Administration > SNMP > SNMP Trap Configuration

トラップ

トラップはブラウジングと異なり、特に要求しなくても、リンク アップ、リンク ダウン、syslog イベントなど特定のイベントが発生すると、管理対象デバイスから管理ステーションに「コメント」が送信されます。

セキュリティ アプライアンスの SNMP オブジェクト ID（OID）が、セキュリティ アプライアンスから送信される SNMP イベントに表示されます。セキュリティ アプライアンスのシステム OID は、SNMP のイベント トラップと SNMP の mib-2.system.sysObjectID に表示されます。

セキュリティ アプライアンスで実行される SNMP サービスには、2 つの異なる機能があります。

- 管理ステーション（または SNMP クライアント）が送信した SNMP 要求に応答を返します。
- 管理ステーション、またはセキュリティ アプライアンスの通知を受信するように登録されたその他のデバイスに、トラップ（イベント通知）を送信します。

セキュリティ アプライアンスは、3 タイプのトラップをサポートします。

- ファイアウォール
- ジェネリック
- syslog

トラップの設定

SNMP Trap Configuration を開くと、次のフィールドが表示されます。

- **Standard SNMP Traps**：送信する標準トラップを選択します。
  - **Authentication**：認証の標準トラップをイネーブルにします。
  - **Cold Start**：コールド スタートの標準トラップをイネーブルにします。
  - **Link Up**：リンク アップの標準トラップをイネーブルにします。
  - **Link Down**：リンク ダウンの標準トラップをイネーブルにします。
- **Entity MIB Notifications**
  - **FRU Insert**：現場交換可能ユニット（FRU）が挿入された場合のトラップ通知をイネーブルにします。
  - **FRU Remove**：現場交換可能ユニット（FRU）が取り外された場合のトラップ通知をイネーブルにします。
  - **Configuration Change**：ハードウェア変更が行われた場合のトラップ通知をイネーブルにします。
- **IPSec Traps**：IPSec トラップをイネーブルにします。
  - **Start**：IPSec が開始した場合のトラップをイネーブルにします。
  - **Stop**：IPSec が停止した場合のトラップをイネーブルにします。

- **Remote Access Traps**：リモート アクセス トラップをイネーブルにします。
  - **Session threshold exceeded**：リモート アクセスを開こうとしたセッション数が、設定されているセッション数のしきい値を超過した場合のトラップをイネーブルにします。
- **Enable Syslog traps**：SNMP 管理ステーションへの syslog メッセージの送信をイネーブルにします。
- **OK**：変更を有効にして、直前のパネルに戻ります。
- **Cancel**：変更を無効にして、直前のパネルに戻ります。
- **Help**：詳細情報を表示します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

TFTP Server

Configuration > Properties > Device Administration > TFTP

TFTP Server パネルでセキュリティ アプライアンスを設定すると、TFTP を利用してファイル サーバにコンフィギュレーションを保存できます。

（注） このパネルでは、サーバにファイルを書き込みません。このパネルでセキュリティ アプライアンスを TFTP サーバで使用できるように設定してから、***File*** > ***Save Running Configuration to TFTP Server*** をクリックします。

TFTP サーバとセキュリティ アプライアンス

TFTP は RFC783 および RFC1350 Rev. 2 で規定されているシンプルなクライアント / サーバ ファイル転送プロトコルです。このパネルでセキュリティ アプライアンスを TFTP *クライアント*に設定すると、実行コンフィギュレーションのコピーを TFTP *サーバ*に転送できます。転送するには、***File*** > ***Save Running Configuration to TFTP Server*** をクリックするか ***Tools*** > ***Command Line Interface*** をクリックします。この方法でコンフィギュレーション ファイルをバックアップし、複数のセキュリティ アプライアンスにプロパゲートできます。

configure net コマンドで TFTP サーバの IP アドレスを指定し、**tftp-server** コマンドでサーバのインターフェイスとパス / ファイル名を指定すると、そこに実行コンフィギュレーション ファイルが書き込まれます。この情報を実行コンフィギュレーションに設定すれば、ASDM で ***File*** > ***Save Running Configuration*** をクリックするだけで、**copy** コマンドで TFTP サーバにファイル転送できます。

セキュリティ アプライアンスでサポートされる TFTP サーバは 1 つだけです。TFTP サーバのフルパスを **Configuration > Properties > Administration > TFTP Server** で指定します。ここで設定すると、CLI の **configure net** および **copy** コマンドにコロン（:）で IP アドレスを指定できます。ただし、セキュリティ アプライアンスと TFTP サーバの通信に必要な、中間デバイスの認証またはコンフィギュレーションは、この機能とは別に実行されます。

show tftp-server コマンドで、現在のコンフィギュレーションに含まれている **tftp-server** コマンド文を一覧表示できます。**no tftp server** コマンドで、サーバへのアクセスをディセーブルにします。

フィールド

TFTP パネルには次のフィールドがあります。

- **Enable**：選択すると、コンフィギュレーションに含まれる TFTP サーバの設定がイネーブルになります。
- **Interface Name**：セキュリティ アプライアンスのインターフェイス名を選択します。このインターフェイスで TFTP サーバの設定を使用します。
- **IP Address**：TFTP サーバの IP アドレスを入力します。
- **Path**：TFTP サーバのパスを入力します。先頭にスラッシュ（/）を付け、最後にファイル名を指定します。ここに実行コンフィギュレーションが書き込まれます。

  TFTP サーバのパスの例：**/tftpboot/**security appliance**/config3**

（注）　パスの先頭には必ずスラッシュ (/) を付けます。

詳細情報

TFTP の詳細については、使用するソフトウェア バージョンのセキュリティ アプライアンスの技術マニュアルを参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

User Accounts

Configuration > Properties > Device Administration > User Accounts

User Accounts パネルで、ローカル ユーザ データベースを管理できます。ローカル ユーザ データベースは、次の機能で使用されます。

- ユーザごとの ASDM アクセス

  デフォルトでは、空白のユーザ名とイネーブル パスワードを指定して ASDM にログインできます（「**Password**」を参照）。ただし、（空白ユーザ名を使用しないで）ログイン画面でユーザ名とパスワードを入力すると、ASDM はローカル データベースをチェックして照合します。

（注）　ローカル データベースを参照する HTTP 認証を設定できますが（「**Authentication タブ**」を参照）、この機能はデフォルトで常にイネーブルです。RADIUS または TACACS+ サーバを認証に使用する場合は、HTTP 認証だけを設定します。

- コンソール認証（「**Authentication タブ**」を参照）。

- Telnet および SSH 認証（「**Authentication タブ**」を参照）。
- **enable** コマンド認証（「**Authentication タブ**」を参照）。

  CLI アクセスのみの設定です。ASDM ログインには影響しません。
- コマンド認可（「**Authorization タブ**」を参照）。

  ローカル データベースを使用するコマンド認可をイネーブルにすると、セキュリティ アプライアンスはユーザ特権レベルを参照して、どのコマンドが使用できるか確認します。コマンド認可がディセーブルの場合、通常特権レベルは参照されません。デフォルトでは、コマンドの特権レベルは 0 または 15 のどちらかになっています。ASDM にはイネーブルにできる特権レベルがあらかじめ定義されています。指定できるレベルは、15（管理）、5（読み取り専用）、3（監視専用）の 3 種類です。あらかじめ定義されたレベルを使用するには、3 種類の特権レベルのいずれかにユーザを設定します。

（注） CLI へのアクセス権を取得できるユーザを特権 EXEC モードに入れないようにするには、そのユーザをローカル データベースに追加する際にコマンド認可をイネーブルにする必要があります。コマンド認可を行わないと、ユーザは、特権レベルが 2 以上（2 がデフォルト）の場合、CLI で自分のパスワードを使用して特権モード（およびすべてのコマンド）にアクセスできます。あるいは、コンソール アクセスに RADIUS または TACACS+ 認証を使用して、ユーザが login コマンドを使用できないようにすることも、すべてのローカル ユーザをレベル 1 に設定して、システム イネーブル パスワードを使用して特権モードにアクセスできるユーザを制御することもできます。

- ネットワーク アクセス認証
- VPN クライアント認証

ネットワーク アクセス認可には、ローカル データベースは使用できません。

マルチコンテキスト モードの場合、システム実行スペースでユーザ名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する **aaa** コマンドは設定できません。

（注） VPN 機能は、マルチモードでサポートされていません。

（**Password** でなく）このパネルでイネーブル パスワードを設定するには、ユーザ名 enable_15 のパスワードを変更します。ユーザ名 enable_15 は常時このパネルに表示されます。これがデフォルトのユーザ名です。ASDM のシステム コンフィギュレーションでは、この方法だけがイネーブル パスワードを設定する方法です。CLI で他のイネーブル レベル パスワードを設定すると（**enable password 10** など）、そのユーザ名は enable_10 のようになります。

フィールド

- **User Name**：ここに示すパラメータを適用するユーザ名を指定します。
- **Privilege (Level)**：ユーザに設定する特権レベルを指定します。特権レベルは、ローカル コマンド認可で使用されます。詳細については、「**Authorization タブ**」を参照してください。
- **VPN Group Policy**：ユーザに適用する VPN グループ ポリシー名を指定します。マルチモードでは使用できません。
- **VPN Group Lock**：ユーザに適用するグループ ロック ポリシーがあれば、それを指定します。マルチモードでは使用できません。
- **Add**：Add User Account ダイアログボックスを表示します。
- **Edit**：Edit User Account ダイアログボックスを表示します。

- **Delete**：選択した行をテーブルから削除します。確認されず、やり直しもできません。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit User Account > Identity タブ

Configuration > Properties > Device Administration > User Accounts > Add/Edit User Account > Identity タブ

このタブで指定したパラメータでユーザ アカウントを識別し、追加または変更ができます。変更は、OK をクリックすると User Accounts テーブルにただちに表示されます。

フィールド

- **Username**：アカウントのユーザ名を指定します。
- **Password**：ユーザの一意のパスワードを指定します。パスワードは 4 文字以上にする必要があります。また、最大 32 文字です。パスワードは、大文字と小文字を区別します。フィールドには、アスタリスクだけが表示されます。

（注）　セキュリティ保護のため、パスワードは 8 文字以上にすることをお勧めします。

- **Confirm Password**：確認のためユーザ パスワードを再入力します。フィールドには、アスタリスクだけが表示されます。
- **Privilege Level**：ローカル コマンド認可でユーザに適用する特権レベルを選択します。0（最低）～ 15（最高）の範囲の値を指定します。詳細については、「**Authorization タブ**」を参照してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit User Account > VPN Policy タブ

Configuration > Properties > Device Administration > User Accounts > Add/Edit User Account > VPN Policy タブ

このタブで指定した VPN ポリシーをユーザに適用します。Inherit チェックボックスを選択すると、対応する設定の値をグループ ポリシーから取得できます。

フィールド

- **Group Policy**：利用できるグループ ポリシーを一覧表示します。
- **Tunneling Protocols**：ユーザが使用できるトンネル プロトコルを指定します。また、グループ ポリシーのデータを継承するかどうかも指定します。必要な **Tunneling Protocols** のチェックボックスをオンにし、ユーザが使用できる VPN トンネル プロトコルを選択します。ユーザは、選択されているプロトコルのみを使用できます。選択肢は次のとおりです。

  IPSec：IP セキュリティ プロトコル。最もセキュアなプロトコルであるとされている IPSec は、VPN トンネルの最も完全なアーキテクチャを提供します。IPSec は、LAN 間（ピアツーピア）接続と、クライアントと LAN の接続の両方で使用できます。

  WebVPN：SSL/TLS を利用する VPN。Web ブラウザを使用して、VPN コンセントレータへのセキュアなリモートアクセス トンネルを確立し、ソフトウェアまたはハードウェアのクライアントを必要としません。WebVPN を使用すると、HTTPS インターネット サイトを利用できるほとんどすべてのコンピュータから、企業の Web サイト、Web 対応アプリケーション、NT/AD ファイル共有（Web 対応）、電子メール、およびその他の TCP ベース アプリケーションなど、幅広い企業リソースに簡単にアクセスできるようになります。

  L2TP over IPSec：いくつかの一般的な PC およびモバイル PC のオペレーティング システムで提供される VPN クライアントを使用しているリモート ユーザが、パブリック IP ネットワークを介してセキュリティ アプライアンスおよびプライベート企業ネットワークへのセキュアな接続を確立できるようにします。

  （注）　プロトコルを選択しなかった場合、エラー メッセージが表示されます。

- **Filter**：使用するフィルタを指定します。また、グループ ポリシーのデータを継承するかどうかも指定します。フィルタは、セキュリティ アプライアンスを経由して着信したトンネリングされたデータ パケットを、送信元アドレス、宛先アドレス、プロトコルなどの基準によって、許可するか拒否するかを決定するルールで構成されます。フィルタおよびルールを設定するには、Configuration > VPN > VPN General > Group Policy パネルを参照してください。
- **Manage**：ACL Manager パネルを表示します。アクセス コントロール リスト（ACL）および拡張アクセス コントロール リスト（ACE）の追加、編集、削除ができます。
- **Tunnel Group Lock**：トンネル グループ ロックがある場合、それを継承するかどうか、または選択したトンネル グループ ロックを使用するかどうかを指定します。特定のロックを選択すると、ユーザのリモート アクセスはこのグループだけに制限されます。トンネル グループ ロックは、VPN クライアントで設定されたグループが、そのユーザが割り当てられているグループと同じかどうかをチェックすることによって、ユーザを制限します。同じでない場合、セキュリティ アプライアンスは、ユーザが接続できないようにします。Inherit チェックボックスがオフの場合、デフォルト値は --None-- です。
- **Store Password on Client System**：この設定をグループから継承するかどうかを指定します。Inherit チェックボックスをオフにすると、Yes/ No のオプション ボタンが有効になります。Yes を選択すると、ログイン パスワードがクライアント システムに保存されます（セキュリティが低下する恐れのあるオプションです）。No（デフォルト）を選択すると、ユーザ接続時ごとにパスワード入力が求められます。最大限のセキュリティを確保するには、パスワードの保存は許可しないことをお勧めします。VPN 3002 の場合、このパラメータは対話型ハードウェア クライアント認証や個別ユーザ認証では動作しません。

- **Connection Settings**：接続設定パラメータを指定します。
  - **Access Hours**：Inherit チェックボックスがオフの場合、既存のアクセス時間ポリシーがあれば、その名前を選択してこのユーザに適用できます。また、新規のアクセス時間ポリシーを作成することもできます。デフォルトは Inherit です。また、Inherit チェックボックスがオフの場合のデフォルトは --Unrestricted-- です。
  - **New**：Add Time Range ダイアログボックスが開き、アクセス時間の新規セットを指定できます。
  - **Simultaneous Logins**：Inherit チェックボックスがオフの場合、同時にログインできる最大ユーザ数を指定します。デフォルト値は 3 です。最小値は 0 で、この場合ログインがディセーブルになり、ユーザ アクセスを禁止します。

（注） 最大値を設定して制限しない場合、多くの同時接続が許可され、セキュリティとパフォーマンスの低下を招く恐れがあります。

  - **Maximum Connect Time**：Inherit チェックボックスがオフの場合、ユーザの最大接続時間（分単位）を指定します。ここで指定した時間が経過すると、システムは接続を終了します。最短時間は 1 分で、最長時間は 2147483647 分（4000 年超）です。接続時間を無制限にするには、Unlimited チェックボックスを選択します（デフォルト）。
  - **Idle Timeout**：Inherit チェックボックスがオフの場合、ユーザのアイドル タイムアウト時間（分単位）を指定します。この期間、ユーザ接続に通信アクティビティがなかった場合、システムは接続を終了します。最短時間は 1 分で、最長時間は 10080 分です。この値は WebVPN ユーザには適用されません。
- **Dedicated IP Address (Optional)**
  - **IP Address** ボックス：専用 IP アドレスを指定します（オプション）。
  - **Subnet Mask** リスト：専用 IP アドレスのサブネット マスクを指定します。

Group Lock チェックボックスを選択すると、ユーザのリモート アクセスはこのグループだけに制限されます。グループ ロックは、VPN クライアントで設定されたグループが、そのユーザが割り当てられているグループと同じかどうかをチェックすることによって、ユーザを制限します。同じでない場合、VPN Concentrator は、ユーザが接続できないようにします。

このチェックボックスがオフの場合（デフォルト）、ユーザが割り当てられているグループと関係なく、ユーザを認証します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Add/Edit User Account > WebVPN タブ

Configuration > Properties > Device Administration > User Accounts > Add/Edit User Account > WebVPN タブ

Add User Account パネルまたは **Edit User Account** パネルの **WebVPN** タブには 6 つのタブがあり、WebVPN のユーザ アトリビュートを設定できます。

フィールド

- **Inherit** : 対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。
- **Functions**：WebVPN ユーザが使用できる機能を設定します。
  - **Enable URL entry**：ホームページに URL 入力ボックスを配置します。イネーブルにすると、ユーザは URL 入力ボックスに Web アドレスを入力し、WebVPN を使用してこれらの Web サイトにアクセスできます。

    WebVPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。WebVPN は、企業ネットワーク上のリモート PC やワークステーションとセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

    WebVPN 接続では、セキュリティ アプライアンスはエンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。WebVPN ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、SSL 証明書を検証します。エンド ユーザのブラウザは提示された SSL 証明書を受信しないため、この証明書を検証することはできません。現在の WebVPN の実装では、有効期限が切れた証明書を提供するサイトとの通信は許可されません。また、セキュリティ アプライアンスは信頼できる CA 証明書の検証も実行しません。そのため、WebVPN ユーザは、SSL 対応 Web サーバと通信する前に、提供される証明書を分析できません。

    WebVPN ユーザのインターネット アクセスを制限するには、Enable URL Entry フィールドを選択解除します。これによって、WebVPN ユーザは、WebVPN 接続中に Web サーフィンができなくなります。

  - **Enable file server access**：HTTPS を介した Windows ファイル アクセス（SMB/CIFS ファイルのみ）をイネーブルにします。このボックスを選択すると、ユーザはネットワーク上の Windows ファイルにアクセスできるようになります。WebVPN のファイル共有用にこのパラメータだけをイネーブルにした場合、Servers and URLs グループ ボックスで設定されたサーバにのみアクセスできます。ユーザがサーバに直接アクセスしたり、ネットワーク上のサーバを参照できるようにするには、Enable file server entry および Enable file server browsing パラメータの説明を参照してください。

    ファイルのダウンロード、編集、削除、名前変更、移動ができます。ファイルとフォルダの追加もできます。

    適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、ファイルにアクセスする前に、ユーザの認証が必要になります。

    ファイル アクセス、サーバ / ドメイン アクセス、および参照を行うには、WINS サーバまたはマスター ブラウザ（通常、セキュリティ アプライアンスと同じネットワーク、またはそのネットワークから到達可能なネットワークに存在）を設定する必要があります。WINS サーバまたはマスター ブラウザは、セキュリティ アプライアンスにネットワーク上のリソースのリストを提供します。代わりに DNS サーバを使用することはできません。

（注） ダイナミック DNS を同時に使用している場合、Active Native Directory 環境でファイル アクセスはサポートされません。WINS サーバを同時に使用している場合にサポートされます。

- **Enable file server entry**：ポータル ページにファイル サーバの入力ボックスを配置します。ファイル サーバ アクセスをイネーブルにする必要があります。

  このチェックボックスを選択すると、ユーザは Windows ファイルのパス名を直接入力できるようになります。ファイルのダウンロード、編集、削除、名前変更、移動ができます。ファイルとフォルダの追加もできます。ここでも、適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、ファイルにアクセスする前に、ユーザの認証が必要になります。

- **Enable file server browsing**：Windows ネットワークからドメイン / ワークグループ、サーバ、共有を参照できます。ファイル サーバ アクセスをイネーブルにする必要があります。

  このチェックボックスを選択すると、ユーザがドメインおよびワークグループを選択し、そのドメイン内のサーバおよび共有を参照できるようになります。適切な Windows サーバへのユーザ アクセスを行うために、共有も設定する必要があります。ネットワーク要件によっては、サーバにアクセスする前に、ユーザの認証が必要になります。

- **Enable port forwarding**：WebVPN ポート転送を使用すると、グループ内のリモート ユーザが既知の固定 TCP/IP ポートで通信するクライアント/サーバ アプリケーションにアクセスできるようになります。リモート ユーザは、ローカル PC にインストールされたクライアント アプリケーションを使用して、そのアプリケーションをサポートするリモート サーバに安全にアクセスできます。シスコでは、Windows Terminal Services、Telnet、Secure FTP（FTP over SSH）、Perforce、Outlook Express、および Lotus Notes についてテストしています。その他の TCP ベースのアプリケーションの一部も機能すると考えられますが、シスコではテストしていません。

（注）　ポート転送は、一部の SSL/TLS バージョンでは機能しません。

  このチェックボックスを選択すると、ローカルおよびリモート システムの TCP ポートをマッピングすることによって、ユーザがクライアント / サーバ アプリケーションにアクセスできるようになります。

（注）　デジタル証明書を使用してユーザを認証する場合、TCP ポート転送 JAVA アプレットは機能しません。JAVA は Web ブラウザのキーストアにアクセスできません。そのため JAVA は、ブラウザがユーザ認証に使用する証明書を使用できず、アプリケーションを起動できません。アプリケーションにアクセスできるようにする場合は、WebVPN ユーザの認証にデジタル証明書を使用しないでください。

- **Enable Outlook/Exchange proxy**：Outlook/Exchange 電子メール プロキシをイネーブルにします。
- **Apply Web-type ACL**：定義されている WebVPN のアクセス コントロール リストをこのグループのユーザに適用します。
- **Enable HTTP Proxy**：クライアントへの HTTP アプレット プロキシの転送をイネーブルにします。プロキシは、Java、ActiveX、Flash など、適切なマングリングを妨げる技術に対して有用です。セキュリティ アプライアンスを使用しながら、マングリングをバイパスします。転送プロキシは、ブラウザの古いプロキシ設定を自動的に修正し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、Java など、事実上すべてのクライアント サイド テクノロジーをサポートします。サポートされるブラウザは Microsoft Internet Explorer だけです。

- **Content Filtering**：Web サイトのうち Java または Active X を使用する部分、スクリプトを使用する部分、画像を表示する部分、およびクッキーを配信する部分をブロックまたは削除します。デフォルトでは、これらのパラメータは無効になっていて、フィルタリングは行われません。
  - **Filter Java/ActiveX**：HTML から <applet>、<embed>、<object> タグを削除します。
  - **Filter scripts**：HTML から <script> タグを削除します。

  - **Filter images**：HTML から <img> タグを削除します。画像を削除すると、Web ページの配信が大幅に高速化されます。
  - **Filter cookies from images**：画像で配信されるクッキーを削除します。広告主はクッキーを使用して訪問者を追跡するため、これによってユーザのプライバシーが保護されます。
- **Homepage**：ホームページで使用するものがあれば設定します。
  - **Specify URL**：後続のフィールドにプロトコルを設定する場合に指定します。http または https と、ホームページに使用する Web ページの URL を設定できます。
  - **Protocol**：ホームページの接続プロトコルとして、http または https を指定します。
  - **://**：Web ページの URL をホームページとして指定します。
  - **Use none**：ホームページが設定されません。
- **Port Forwarding**：ポート転送パラメータを設定します。
  - **Port Forwarding List**：ポート転送リストをデフォルト グループ ポリシーから継承するか、リストから選択するか、新しいポート転送リストを作成するかを指定します。
  - **New**：新規ポート転送リストを追加できる新しいパネルが表示されます。Add/Edit Port Forwarding List パネルの説明を参照してください。
  - **Applet Name**：アプレット名を継承するか、ボックスで指定した名前を使用するかを指定します。この名前を指定して、エンド ユーザに対してポート転送を識別します。設定した名前は、エンド ユーザ インターフェイスにホットリンクとして表示されます。このリンクをクリックすると Java アプレット ウィンドウが開き、ユーザに設定されたポート転送アプリケーションが表示され、ここからアプリケーションにアクセスできます。デフォルトのアプレット名は Application Access です。
- **Other**：サーバおよび URL リスト、Web タイプの ACL ID を設定します。
  - **Servers and URL Lists**：サーバおよび URL のリストを継承するか、既存のリストを選択するか、新しいリストを作成するかを指定します。
  - **New**：新規ポート転送リストを追加できる新しいパネルが表示されます。
  - **Web-Type ACL ID**：使用する Web タイプ ACL の識別子を指定します。
- **SSL VPN Client タブ**：セキュリティ アプライアンスを設定して、SSL VPN クライアント（SVC）をリモート コンピュータにダウンロードできます。

  SVC は、ネットワーク管理者が IPSec VPN クライアントをリモート コンピュータにインストールし、設定しなくても、リモート ユーザが IPSec VPN を利用できるようにする VPN トンネリング技術です。SVC は、すでにリモート コンピュータにある SSL 暗号化と、セキュリティ アプライアンスの WebVPN ログインおよび認証を使用します。

  SVC セッションを確立するには、リモート ユーザはセキュリティ アプライアンスの WebVPN インターフェイスの IP アドレスをブラウザに入力します。ブラウザはそのインターフェイスに接続して WebVPN のログイン画面を表示します。ユーザがログインと認証を終了し、セキュリティ アプライアンスがこのユーザを SVC が必要なユーザとして識別した場合、セキュリティ アプライアンスはリモート コンピュータに SVC をダウンロードします。セキュリティ アプライアンスがこのユーザを SVC がオプションで使用できるユーザとして識別した場合、セキュリティ アプライアンスは SVC のインストールをスキップするリンクをユーザ画面に表示して、リモート コンピュータに SVC をダウンロードします。

  ダウンロード後、SVC は自己インストールおよび設定を行い、接続が終了したときに、（設定に応じて）リモート コンピュータに残るか、自己アンインストールします。

  セキュリティ アプライアンスは、異なるリモート コンピュータのオペレーティング システム用に、複数の一意の SVC イメージをキャッシュ メモリに常駐させることができます。ユーザが接続しようとしたとき、セキュリティ アプライアンスは、イメージとオペレーティング システムが一致するまで、これらのイメージの一部を連続してダウンロードします。一致すると、SVC の全体をダウンロードします。リモート コンピュータのオペレーティング システムと最も一致する可能性が高いイメージが最初にダウンロードされるように SVC イメージを並べ替えて、接続セットアップ時間を最小にできます。

  - **Inherit**：対応する設定が、その後に続く明示的な指定ではなく、デフォルト グループ ポリシーから値を取得することを示します。

- **Keep Installer on Client System**：永続的な SVC インストールをイネーブルにし、SVC の自動アンインストール機能をディセーブルにします。後続の SVC 接続では、SVC がリモート コンピュータにインストールされたままの状態になるため、リモート ユーザの SVC への接続時間が短縮されます。
- **Keepalive Messages**：キープアライブ メッセージの頻度を 15 ～ 600 秒の範囲で調整します。デフォルトでは、キープアライブ メッセージはディセーブルです。

  プロキシ、ファイアウォール、または NAT デバイスが接続のアイドル時間を制限する場合でも、これらのデバイスを経由する SVC 接続が開いたままになるように、キープアライブ メッセージの頻度を調整できます。また、頻度を調整すると、リモート ユーザが Microsoft Outlook や Microsoft Internet Explorer などのソケットベース アプリケーションをアクティブに実行していない場合に、切断して再接続することがなくなります。
- **Compression**：SVC 接続での圧縮をイネーブルにします。デフォルトでは、圧縮はイネーブルになっています。

  SVC 圧縮を行うと、転送されるパケットのサイズが減少するため、セキュリティ アプライアンスと SVC 間の通信パフォーマンスが向上します。
- **Rekey Negotiation Settings** グループ ボックス：セキュリティ アプライアンスと SVC が鍵を再生成するときは、暗号鍵と初期ベクトルを再ネゴシエーションして、接続セキュリティを強化します。

  Renegotiation Interval は、セッション開始から鍵の再生成までの時間（分単位）を 1 ～ 10080（1 週間）の範囲で指定します。

  Renegotiation Method は、SVC 鍵の再生成の際に SVC が新しいトンネルを確立するかどうかを指定します。*none* を選択すると、SVC 鍵の再生成はディセーブルになります。*ssl* を選択すると、SVC 鍵の再作成の際に、SSL の再ネゴシエーションが実行されます。
- **Dead Peer Detection**：Dead Peer Detection（DPD）は、ピアが応答していないために失敗した接続をセキュリティ アプライアンス（ゲートウェイ）または SVC で迅速に検出できるようにします。

  Gateway Side Detection は、セキュリティ アプライアンス（ゲートウェイ）による DPD 実行をイネーブルにし、セキュリティ アプライアンスが DPD を実行する頻度を 30 ～ 3600 秒（1 時間）の範囲で指定します。*disable* を選択すると、セキュリティ アプライアンスによる DPD の実行がディセーブルになります。

  Client Side Detection は、SVC（クライアント）による DPD の実行をイネーブルにし、SVC が DPD を実行する頻度を 30 ～ 3600 秒（1 時間）の範囲で指定します。*disable* を選択すると、SVC による DPD の実行がディセーブルになります。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	•	—

Auto Update

Configuration > Properties > Auto Update

Auto Update ペインでセキュリティ アプライアンスの管理リモート サーバを設定すると、リモート サーバで Auto Update 仕様をサポートできます。Auto Update を利用すると、セキュリティ アプライアンスにコンフィギュレーションの変更を適用したり、離れた場所からソフトウェア アップデートを取得したりできます。

Auto Update は、セキュリティ アプライアンスの管理者が直面するさまざまな課題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点を解決します。
- 基本アクションのコンフィギュレーション変更を確実に反映します。
- 信頼度の高い方式でソフトウェアを更新します。
- 十分に実績のある方式を応用し、高い拡張性があります。
- オープン インターフェイスで、きわめて高い開発自由度があります。
- サービス プロバイダー環境のセキュリティ ソリューションに容易に対応できます。
- 高い信頼性と豊富なセキュリティ管理機能を、さまざまな製品により幅広くサポートします。

Auto Update の概要

Auto Update 仕様は、中央、または複数の場所から、リモート管理アプリケーションによりセキュリティ アプライアンスのコンフィギュレーションやソフトウェア イメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update 仕様に従うことで、Auto Update サーバはセキュリティ アプライアンスにコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりできます。また、セキュリティ アプライアンスから Auto Update サーバへ定期的にポーリングさせ、最新のコンフィギュレーション情報を送ることもできます。また、Auto Update サーバはいつでもセキュリティ アプライアンスにコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバとセキュリティ アプライアンスの通信では、通信パスとローカル CLI コンフィギュレーションをすべてのセキュリティ アプライアンスに設定する必要があります。

セキュリティ アプライアンスの Auto Update 機能は、シスコのセキュリティ製品と併用できますが、サード パーティ製品でセキュリティ アプライアンスを管理することもできます。

特記事項

- セキュリティ アプライアンスのコンフィギュレーションが Auto Update で更新されても、ASDM には通知されません。**Refresh** または **File > Refresh ASDM with the Running Configuration on the Device** をクリックして、最新のコンフィギュレーションを取得する必要があります。また、ASDM でコンフィギュレーションに加えた変更は失われます。
- Auto Update サーバとの通信プロトコルとして HTTPS を選択すると、セキュリティ アプライアンスは SSL を使用します。その場合、セキュリティ アプライアンスに DES または 3DES のライセンスが必要です。

フィールド

Auto Update ペインには、Auto Update Servers テーブルの他に Timeout エリアと Polling エリアがあります。

Auto Update Servers テーブルで、Auto Update サーバにすでに設定されているパラメータを確認できます。セキュリティ アプライアンスは、テーブルの一番上にあるサーバを最初にポーリングします。テーブルのサーバ表示位置を変更するには、Move Up または Move Down ボタンをクリックします。Auto Update Servers テーブルには次のカラムがあります。

- Server：Auto Update サーバの名前または IP アドレス名。
- User Name：Auto Update サーバのアクセス時に使用されるユーザ名。
- Interface：Auto Update サーバへの要求送信時に使用されるインターフェイス。
- Verify Certificate：Auto Update サーバが返した証明書を、セキュリティ アプライアンスで認証局（CA）のルート証明書と照合するかどうかを指定します。その場合、Auto Update サーバとセキュリティ アプライアンスは、同じ CA を使用する必要があります。

Auto Update Server テーブルの行のいずれかをダブルクリックすると、Edit Auto Update Server ダイアログが開き、Auto Update サーバのパラメータを変更できます。変更はテーブルにただちに表示されますが、Apply をクリックしないと、コンフィギュレーションに保存されません。

Timeout エリアで、セキュリティ アプライアンスが Auto Update サーバのタイムアウトを待つ時間を設定できます。Timeout エリアには次のフィールドがあります。

- Enable Timeout Period：セキュリティ アプライアンスは、Auto Update サーバから応答を受信しなかった場合、タイムアウトします。
- Timeout Period (Minutes)：Auto Update サーバから応答がなかった場合のセキュリティ アプライアンスのタイムアウト時間（分単位）を指定します。

Polling エリアで、セキュリティ アプライアンスから Auto Update サーバの情報をポーリングする頻度を設定できます。Polling エリアには次のフィールドがあります。

- Polling Period (minutes)：セキュリティ アプライアンスから Auto Update サーバに新しい情報をポーリングするときの待ち時間（分単位）。
- Poll on Specified Days：ポーリングのスケジュールを設定します。
- Set Polling Schedule：Set Polling Schedule ダイアログボックスが表示され、Auto Update をポーリングする日と時刻を設定できます。
- Retry Period (minutes)：サーバのポーリングに失敗した場合、セキュリティ アプライアンスから Auto Update サーバに新しい情報をポーリングするまでの待ち時間（分単位）。
- Retry Count：セキュリティ アプライアンスから Auto Update サーバに新しい情報をポーリングするときの再試行回数。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Set Polling Schedule

Configuration > Properties > Auto Update > Set Polling Schedule

Set Polling Schedule ダイアログボックスで、セキュリティ アプライアンスから Auto Update サーバをポーリングする特定の日と時刻を設定します。

フィールド

Set Polling Schedule ダイアログボックスには次のフィールドがあります。

Days of the Week：セキュリティ アプライアンスから Auto Update サーバをポーリングする曜日のチェックボックスを選択します。

Daily Update Window グループで、セキュリティ アプライアンスから Auto Update サーバをポーリングする時刻を設定します。次のフィールドがあります。

- Start Time：Auto Update のポーリング開始時刻を入力します。
- Enable Randomize:セキュリティ アプライアンスから Auto Update サーバをランダムに選択した時刻にポーリングします。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add/Edit Auto Update Server

Configuration > Properties > Auto Update > Add/Edit Auto Update Server

Edit Auto Update Server ダイアログボックスには次のフィールドがあります。

- URL : Auto Update サーバがセキュリティ アプライアンスと通信する際に使用する、http または https のプロトコルと Auto Update サーバのパス。
- Interface：Auto Update サーバに要求を送信する際に使用するインターフェイス。
- Verify Certificate：セキュリティ アプライアンスは Auto Update サーバが返した証明書を認証局（CA）のルート証明書と比較して検証します。その場合、Auto Update サーバとセキュリティ アプライアンスは、同じ CA を使用する必要があります。

User エリアには次のフィールドがあります。

- User Name (Optional)：Auto Update サーバのアクセス時に必要なユーザ名を入力します。
- Password：Auto Update サーバのユーザ パスワードを入力します。
- Confirm Password：Auto Update サーバのユーザ パスワードを再入力します。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Advanced Auto Update Settings

Configuration > Properties > Auto Update > Advanced Auto Update Settings

フィールド

- Use Device ID to uniquely identify the ASA : デバイス ID による認証をイネーブルにします。デバイス ID により、セキュリティ アプライアンスが Auto Update サーバで一意に識別できます。
- Device ID：使用するデバイス ID のタイプを入力します。
  - Hostname：ホストの名前です。
  - Serial Number：デバイスのシリアル番号です。
  - IP Address on interface：選択したインターフェイスの IP アドレス。セキュリティ アプライアンスを Auto Update サーバが一意に識別する場合に使用します。
  - MAC Address on interface：選択したインターフェイスの MAC アドレス。セキュリティ アプライアンスを Auto Update サーバが一意に識別する場合に使用します。
  - User-defined value：一意のユーザ ID です。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Client Update

Configuration > Properties > Client Update

Client Update ペインで、Auto Update サーバとして設定したセキュリティ アプライアンスに関連付けた Auto Update クライアントのパラメータを設定します。

Auto Update サーバの場合、Auto Update クライアントに設定されたセキュリティ アプライアンスにプラットフォームと ASDM のイメージを指定できます。イメージのリビジョン番号と場所、使用するデバイス ID、デバイス ファミリ、クライアントのデバイス タイプなどが含まれます。

Auto Update Server と Client Update の概要

Auto Update 仕様は、中央から、リモート管理アプリケーションによりセキュリティ アプライアンスのコンフィギュレーションやソフトウェア イメージをダウンロードしたり、基本的な監視機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update サーバの仕様に従うことで、Auto Update サーバはセキュリティ アプライアンスにコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりできます。また、セキュリティ アプライアンスから Auto Update サーバへ定期的にポーリングさせ、最新のコンフィギュレーション情報を送ることもできます。また、Auto Update サーバはいつでもセキュリティ アプライアンスにコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバとセキュリティ アプライアンスの通信では、通信パスとローカル CLI コンフィギュレーションをすべてのセキュリティ アプライアンスに設定する必要があります。

フィールド

Client Update ペインには次のフィールドがあります。

- Enable Client Update：セキュリティ アプライアンスは、Auto Update クライアントに設定された他のセキュリティ アプライアンスが使用しているイメージを更新します。
- Client Images テーブル：設定済みの Client Update エントリを表示します。次のカラムがあります。
  - Device：クライアントのデバイス ID に対応するテキスト文字列を表示します。
  - Device Family：クライアントのファミリ名を表示します。asa、pix、テキスト文字列のいずれかです。
  - Device Type：クライアントのタイプ名を表示します。
  - Image Type：イメージ タイプを指定します。ASDM イメージまたは Boot イメージのいずれかです。
  - Image URL：ソフトウェア コンポーネントの URL を指定します。
  - Client Revision：ソフトウェア コンポーネントのリビジョン番号を指定します。

  Client Images テーブルの行のいずれかをダブルクリックすると、Edit Client Update Entry ダイアログが開き、クライアント パラメータを変更できます。変更はテーブルにただちに表示されますが、Apply をクリックしないと、コンフィギュレーションに保存されません。
- Live Client Update エリア：トンネル経由で現在セキュリティ アプライアンスに接続されている Auto Update クライアントを、ただちに更新します。
  - Tunnel Group：「all」を選択すると、すべてのトンネル グループ上で接続している Auto Update クライアントをすべて更新します。また、トンネル グループを指定してクライアントを更新することもできます。
  - Update Now：ただちに更新を開始します。

（注） Live Client Update は、セキュリティ アプライアンスがルーテッド モードに設定されている場合のみ使用できます。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—

Add/Edit Client Update

Configuration > Properties > Add/Edit Client Update

フィールド

Add/Edit Client Update ダイアログボックスには次のフィールドがあります。

- Device Identification グループ
  - Device ID：クライアントの識別を一意の文字列で行う設定になっている場合に、イネーブルにします。クライアントが使用している同じ文字列を指定します。最大長は 63 文字です。
  - Device Family：クライアントの識別をデバイス ファミリで行う設定になっている場合に、イネーブルにします。クライアントが使用している同じデバイス ファミリを指定します。asa、pix、または 7 文字以内のテキスト文字列を指定します。
  - Device Type：クライアントの識別をデバイス タイプで行う設定になっている場合に、イネーブルにします。クライアントが使用している同じデバイス タイプを指定します。指定できるタイプは、pix-515、pix-515e、pix-525、pix-535、asa5505、asa5510、asa5520、asa5540 です。また、15 文字以内のテキスト文字列を指定します。
  - Not Specified：クライアントが上記に該当しない場合に、選択します。
- Image Type：イメージ タイプを指定します。ASDM イメージまたは Boot イメージのいずれかです。必ず、このクライアントに適したファイルのある URL を指定してください。最大 255 文字です。
- Client Revision：ソフトウェア コンポーネントのリビジョン番号に対応するテキスト文字列を指定します。たとえば 7.1(0)22 のように指定します。
- Image URL：ソフトウェア コンポーネントの URL を指定します。必ず、このクライアントに適したファイルのある URL を指定してください。

モード

次の表に、この機能を使用できるモードを示します。

ファイアウォール モード		セキュリティ コンテキスト		
			マルチ	
ルーテッド	透過	シングル	コンテキスト	システム
•	•	•	—	—