ASDM の概要

ASDM はブラウザの Java アプレットを利用して、セキュリティ アプライアンスのソフトウェアの設定およびモニタリングを行います。また、ASDM をセキュリティ アプライアンスからロードすると、デバイスを設定、監視、管理できます。

今回のリリースの詳細については、次の項目を参照してください。

特記事項

- **CLI コマンドのサポート**：いくつかの例外を除き、ほとんどすべての CLI コマンドが ASDM でサポートされています。ASDM がサポートしていないコマンドのリストについては、「サポートされていないコマンド」を参照してください。
- **多重 ASDM セッション**：ASDM では複数の PC やワークステーションでそれぞれブラウザ セッションを開き、同じセキュリティ アプライアンス ソフトウェアを使用できます。1 つのセキュリティ アプライアンスで、シングル ルーテッド モードの ASDM 並行セッションを 5 つまでサポートできます。PC またはワークステーションはそれぞれ、特定のセキュリティ アプライアンスのセッションを 1 つだけブラウザで実行できます。マルチコンテキスト モードの場合、コンテキストあたり 5 つの ASDM 並行セッションを実行でき、セキュリティ アプライアンスあたり最大 32 セッションまで接続できます。
- **セキュリティ アプライアンスのリリース バージョン**：今回リリースされた ASDM に必要なバージョンは 7.1 です。これより以前にリリースされたバージョンのセキュリティ アプライアンスでは実行できません。
- **警告**：Cisco.com の Bug Toolkit を利用して、現在の警告情報を確認してください。Bug Toolkit は次のアドレスからアクセスできます。

  http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl
- **OS カラー スキームの変更方法**：ASDM の実行時にオペレーティング システムのカラー スキームを変更した場合は、ASDM を再起動してください。そうしない場合、一部の ASDM 画面が正常に表示されないことがあります。

今回のリリースで追加された機能

ここでは、次の項目について説明します。

プラットフォームと ASDM に追加された機能がすべて記載されたリストについては、Cisco.com の『*Cisco ASDM Release Notes*』を参照してください。

リリース 5.2（1）で追加された機能

リリース 5.2（1）の新しい機能の詳細については、次の項目を参照してください。

- 機能強化された、新しい検査エンジン。P.21-2 の「Service Policy Rules」および P.6-1 の「グローバル オブジェクト」を参照してください。
- サブセカンド フェールオーバー、高可用性、およびスケーラビリティ ウィザード。P.12-1 の「フェールオーバー」を参照してください。
- パケット トレーサ ツール。P.1-13 の「Packet Tracer」を参照してください。
- トレースルート ツール。P.1-16 の「Traceroute」を参照してください。
- VPN サポートの向上
  - ZoneLabs Integrity サーバ。P.28-65 の「Zone Labs Integrity Server」を参照してください。
  - Easy VPN Remote。P.28-67 の「Easy VPN Remote」を参照してください。
  - Online Certificate Status Protocol（OCSP; オンライン認証ステータス プロトコル）のサポート。P.33-12 の「Add/Edit Trustpoint Configuration > Revocation Check タブ」および P.33-15 の「Add/Edit Trustpoint Configuration > OCSP Rules タブ」を参照してください。
- RIP ルーティング機能の向上。P.14-23 の「RIP」を参照してください。
- スタティック ルート トラッキング / デュアル ISP のサポート。P.14-30 の「スタティック ルート」を参照してください。
- Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）のサポート。P.25-3 の「WCCP」を参照してください。
- ASA 5505 対応セキュリティ アプライアンス Power over Ethernet ポートのサポート。P.5-1 の「Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定」を参照してください。

リリース 5.2（2）で追加された機能

リリース 5.2（2）で追加された機能の詳細については、次の項目を参照してください。

- IDM の統合。P.35-2 の「ASDM からの IDM へのアクセス」を参照してください。
- AIP SSM パスワードのリセット。P.35-3 の「AIP SSM パスワードのリセット」を参照してください。
- CSC SSM パスワードのリセット。P.36-14 の「Restoring the Default Password」を参照してください。
- マルチキャストの追加機能のサポート
  - PIM neighbor-filter。P.15-15 の「Neighbor Filter」を参照してください。
  - PIM bidir-neighbor-filter。P.15-17 の「Bidirectional Neighbor Filter」を参照してください。
  - PIM old-register-checksum。P.15-18 の「Rendezvous Points」で、Generate IOS 互換の登録メッセージのチェックボックスを参照してください。
  - マルチキャスト境界。P.15-11 の「MBoundary」を参照してください。
  - MFIB 転送。PIM bidir-neighbor-filter を参照してください。P.15-13 の「MForwarding」を参照してください。

- HTTP/HTTPS インタラクティブ認証のサポート。P.19-13 の「高度な AAA 機能の設定」を参照してください。
- トンネル グループのプライマリ DN フィールドに追加された UPN（User Principle Name）。P.28-49 の「Add/Edit Tunnel Group > General タブ > Authorization タブ」を参照してください。
- トンネル グループのインターフェイス単位認可サーバ グループ。P.28-49 の「Add/Edit Tunnel Group > General タブ > Authorization タブ」を参照してください。
- 仮想 Telnet サーバのサポート。P.11-13 の「Virtual Access」を参照してください。

サポートされていないコマンド

セキュリティ アプライアンスのコマンドはほとんどすべて ASDM でサポートされますが、既存のコンフィギュレーションのコマンドが ASDM で無視される場合があります。通常、無視されるコマンドはユーザのコンフィギュレーションに記述されています。無視されるコマンドについては、「Show Commands Ignored by ASDM on Device」を参照してください。

alias コマンドの場合、コンフィギュレーションからコマンドを削除しないと ASDM はモニタリング専用モードになります。

ここでは、次の項目について説明します。

無視される表示専用コマンド

次の表のコマンドを CLI で追加したコンフィギュレーションは ASDM で使用できますが、ASDM でコマンドの追加および編集はできません。ASDM で無視されるコマンドは ASDM の GUI に一切表示されません。表示専用コマンドは GUI に表示されますが、編集はできません。

サポートされていないコマンド	ASDM の動作
access-list	未使用の場合は無視
capture	無視
dns-guard	無視
established	無視
failover timeout	無視
ipv6 （IPv6 アドレスの場合）	無視
object-group icmp-type	表示のみ
object-group network	ネストされたグループを表示のみ
object-group protocol	表示のみ
object-group service	ネストされたグループの追加は不可
pager	無視
pim accept-register route-map	無視。**list** オプションを除き、ASDM では設定不可
prefix-list	OSPF 領域で使用されていない場合は無視
route-map	無視

service-policy global	**match access-list** クラスで使用されている場合は無視次の例を参考にしてください。
	
	`access-list myacl line 1 extended permit ip any any`
	`class-map mycm`
	`match access-list mycl`
	`policy-map mypm`
	`class mycm`
	`inspect ftp`
	`service-policy mypm global`

sysopt nodnsalias	無視
sysopt uauth allow-http-cache	無視
terminal	無視
virtual	無視

サポートされていないコマンドによる影響

- 既存の実行コンフィギュレーションを ASDM にロードし、そこに IPv6 関連のコマンドがある場合、ASDM のダイアログボックスに IPv6 はサポートされていないというメッセージが表示されます。ASDM では IPv6 コマンドを一切設定できませんが、その他のコンフィギュレーションは使用できます。
- 既存の実行コンフィギュレーションを ASDM にロードし、そこにサポートされていないコマンドがあっても、ASDM の操作には影響しません。サポートされていないコマンドを表示するには、デバイスで ASDM の Options > Show Commands Ignored を実行します。
- 既存の実行コンフィギュレーションを ASDM にロードし、そこに **alias** コマンドがあると、モニタリング専用モードになります。

  モニタリング専用モードの場合、次の機能にアクセスできます。

  － モニタリング エリア

  － CLI ツール（Tools > Command Line Interface）。ここから CLI コマンドを実行できます。

  モニタリング専用モードを終了させるには、CLI ツールを使用するか、セキュリティ アプライアンスのコンソールで **alias** コマンドを削除します。**alias** コマンドの代わりに外部 NAT を使用できます。詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

（注） モニタリング専用モードになる場合が他にもあります。ASDM のメイン ウィンドウ下部のステータス バーに表示される ユーザ アカウント権限レベルを、システム管理者が 3 以下に設定すると、モニタリング専用モードにできるためです。詳細については、Configuration > Properties > Device Administration > User Accounts and Configuration > Device Access > AAA Access を参照してください。

CLI のその他の制限事項

ASDM では、255.255.0.255 のように連続していないサブネット マスクはサポートされていません。たとえば、次のような記述はできません。

```
ip address inside 192.168.2.1 255.255.0.255
```

ASDM ウィンドウについて

ASDM ウィンドウからセキュリティ アプライアンスのさまざまな機能に簡単にアクセスできます。ASDM ウィンドウには、次のような機能があります。

- メニュー：ファイル、ツール、オプション、およびヘルプにすぐにアクセスできます。
- ツールバー：ASDM をナビゲーションできます。ツールバーからホームページ、コンフィギュレーション パネル、およびモニタリング パネルにアクセスできます。また、機能の検索、コンフィギュレーションの保存、ヘルプの参照、パネル間の前後ナビゲーションもできます。Home、Configuration、Monitoring ボタンをクリックすると、開いたパネルから各種の便利なツールを使用できます。ホームページにはさまざまな情報が表示され、一目で確認できます。コンフィギュレーション パネルとモニタリング パネルには、左側のフレームに使いやすいカテゴリ ツリーがあり、そこから詳細なコンフィギュレーション データまたはモニタリング情報にアクセスできます。
- ステータスバー：時刻、接続ステータス、特権レベルを表示します。

メニュー

ASDM には、次のメニューがあります。

- File メニュー
- Options メニュー
- Tools メニュー
- Wizards メニュー
- Help メニュー

File メニュー

File メニューからセキュリティ アプライアンスのコンフィギュレーション データを管理できます。また、次のメニュー項目もあります。

- Refresh ASDM with the Running Configuration on the Device：実行コンフィギュレーションのコピーを ASDM にロードします。リフレッシュを実行すると、ASDM に現在の実行コンフィギュレーションのコピーがあるかどうかを確認できます。
- Reset Device to the Factory Default Configuration：コンフィギュレーションを工場出荷時のデフォルトに戻します。詳細については、Reset Device to the Factory Default Configuration ダイアログボックスを参照してください。
- Show Running Configuration in New Window：現在の実行コンフィギュレーションを別のウィンドウに表示します。
- Save Running Configuration to Flash：実行コンフィギュレーションのコピーをフラッシュ メモリに書き込みます。
- Save Running Configuration to TFTP Server：実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。詳細については、Save Running Configuration to TFTP Server ダイアログボックスを参照してください。
- Save Running Configuration to Standby Unit：プライマリ装置の実行コンフィギュレーション ファイルのコピーを、フェールオーバー スタンバイ装置の実行コンフィギュレーションに送信します。
- Save Internal Log Buffer to Flash：ログ バッファをフラッシュ メモリに保存します。
- Print：現在のパネルを印刷します。ルールを印刷する場合、ページを横方向にすることをお勧めします。ASDM を Netscape Communicator で使用している場合、ユーザが Java アプレットに対する印刷権限を持っていないとセキュリティ ダイアログボックスが表示され、印刷権限を要求されます。**Grant** をクリックすると、アプレットの印刷権限が与えられます。Internet Explorer の場合は、署名付きアプレットを最初に承認した時点で印刷権限が与えられています。

- Clear ASDM Cache : ASDM のローカル イメージをクリアします。ASDM に接続すると、イメージがローカルにダウンロードされます。
- Clear Internal Log Buffer：システム ログ メッセージのバッファをクリアします。
- Exit：ASDM を終了します。

Reset Device to the Factory Default Configuration

デフォルト コンフィギュレーションには、ASDM からセキュリティ アプライアンスに接続できる最小限のコマンドが含まれています。この機能は、ルーテッド ファイアウォール モードでのみ利用可能です。透過モードではインターフェイスの IP アドレスはサポートされていません。また、インターフェイス IP アドレスはデフォルト設定の中で設定します。また、この機能はシングル コンテキスト モードでのみ利用可能です。コンフィギュレーションがクリアされたセキュリティ アプライアンスには、設定済みのコンテキストがなく、リセット後のデフォルト コンフィギュレーションでは自動設定されません。

この機能を実行すると、現在の実行コンフィギュレーションがクリアされ、コマンドがいくつか設定されます。設定されるインターフェイスは、使用するプラットフォームによって異なります。プラットフォームが専用の管理インターフェイスの場合、インターフェイス名は「management」になります。他のプラットフォームには Ethernet 1 のインターフェイスが設定され、インターフェイス名は「inside」になります。

次のコマンドが専用の管理インターフェイス Management 0/0 に適用されます（プラットフォームが専用の管理インターフェイスでない場合、インターフェイスは Ethernet 1 になります）。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

このダイアログボックスで IP アドレスを設定すると、**http** コマンドは指定されたサブネットを参照します。また、**dhcpd address** コマンドの範囲も、指定されたサブセットの範囲内のアドレスになります。

工場出荷時のデフォルト コンフィギュレーションの復元後、File > Save Running Configuration to Flash 項目で内部フラッシュ メモリに保存します。別の場所に Boot Image/Configuration を事前に設定した場合でも、実行コンフィギュレーションはスタートアップ コンフィギュレーションのデフォルトの場所に保存されます。設定をクリアすると、このパスもクリアされます。

（注）　また、Add Boot Image のコンフィギュレーションもあれば、他のコンフィギュレーションとともにこのコマンドでクリアされます。Add Boot Image ペインで設定すると、外部フラッシュ メモリ カード上のイメージなど、特定のイメージからブートできます。工場出荷時のデフォルト コンフィギュレーションの復元後に、セキュリティ アプライアンスをリロードすると、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、セキュリティ アプライアンスはブートしません。

フィールド

- Use this address for the “Interface_ID” interface which will be named as “name”：デフォルト アドレス 192.168.1.1 を使用する代わりに、管理インターフェイスの IP アドレスを手動で設定します。プラットフォームが専用の管理インターフェイスの場合、インターフェイス名は「management」になります。他のプラットフォームには Ethernet 1 のインターフェイスが設定され、インターフェイス名は「inside」になります。
- Management IP Address：管理インターフェイスの IP アドレスを設定します。
- Management subnet mask：インターフェイスのサブネット マスクを設定します。サブネット マスクを設定しない場合は、IP アドレス クラスに適切なマスクがセキュリティ アプライアンスで使用されます。

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
•	—	•	—	—

Save Running Configuration to TFTP Server

File > Save Running Configuration to TFTP Server > Save Running Configuration to TFTP Server

ダイアログボックスで、現在の実行コンフィギュレーションのコピーを TFTP サーバに保存します。

フィールド

- TFTP Server IP Address：TFTP サーバの IP アドレスを入力します。
- Configuration File Path：ファイルを保存する TFTP サーバのパスを入力します。

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
•	•	•	•	•

Enter Log File Name

File > Save Internal Log Buffer to Flash > Enter Log File Name

ログ バッファをフラッシュ メモリに保存します。

フィールド

- Use default file name：ログ バッファの保存ファイル名は LOG-YYYY-MM-DD-hhmmss.txt になります。
- Use user-specified file name：ログ バッファを指定したファイル名で保存します。
- Field Name：保存したログ バッファのファイル名を入力します。

Options メニュー

Options メニューで ASDM のプリファレンスを設定できます。

- Show Commands Ignored by ASDM on Device：ASDM で無視された、サポートされていないコマンドを表示します。詳細については、Show Commands Ignored by ASDM on Device ダイアログボックスを参照してください。
- Preferences：ASDM の機能の一部を、Web ブラウザのクッキー機能を使用してセッション間で変更します。詳細については、Preferences ダイアログボックスを参照してください。

Show Commands Ignored by ASDM on Device

Options > Show Commands Ignored by ASDM on Device > Show Commands Ignored by ASDM on Device

一部のコマンドは ASDM でサポートされていません。通常、サポートされないコマンドは ASDM の実行時に無視されます。Show Commands Ignored by ASDM on Device を実行すると、未解析コマンドの一覧が表示されます。

ASDM がコンフィギュレーションのコマンドを変更、削除することはありません。詳細については、「サポートされていないコマンド」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
•	•	•	•	•

Preferences

Options > Preferences > Preferences

Preferences ダイアログボックスでは、ASDM の機能の一部を、Web ブラウザのクッキー機能を使用してセッション間で変更します。

フィールド

- General タブ：汎用プリファレンスを設定します。
  - Preview commands before sending to the device チェックボックス：ASDM により生成された CLI コマンドを表示できます。
  - Enable Large Fonts (Requires ASDM Restart) チェックボックス：ASDM を閉じて再接続した後に、ASDM のアイコンのフォント サイズを拡大します。すべてのフォントが大きくなるとは限りません。
  - Confirm before exiting from ASDM チェックボックス：ASDM を閉じるとき、プロンプトを表示して終了を確認します。このオプションは、デフォルトでオンになっています。
- Rules Table タブ：Rules テーブルのプリファレンスを設定します。
  - Display settings：Rules テーブルのルール表示方法を変更します。
    - Auto expand network and service object groups with specified prefix：ネットワークとサービス オブジェクト グループを、Auto Expand-Prefix により自動展開して表示します。
    - Auto Expand-Prefix：ネットワークおよびサービス オブジェクトのプレフィックスを指定して、自動展開して表示します。

- Show members of network and service object groups : ネットワークおよびサービス オブジェクト グループのメンバおよび Rules テーブルのグループ名を選択して表示します。チェックボックスがオフの場合、グループ名だけが表示されます。
- Limit members to : 表示するネットワークおよびサービス オブジェクト グループの数を入力します。オブジェクト グループ メンバの場合、最初の *nn* 個のメンバだけが表示されます。
- Show all actions for service policy rules : Rules テーブルのアクションをすべて表示します。クリアされている場合、サマリーが表示されます。

— Deployment Settings : Rules テーブルに変更内容を適用する場合に、セキュリティ アプライアンスの動作を設定できます。

- Issue clear xlate command when deploying access lists : アクセスリストを新規に適用するとき NAT テーブルがクリアされます。したがって、セキュリティ アプライアンスに設定されているアクセスリストが、すべての変換アドレスに対して確実に適用されます。
- Show filter panel by default : デフォルトで、フィルタ パネルを表示します。
- Show rule diagram panel by default : デフォルトで、ルール ダイアグラム パネルを表示します。

- Applications Inspections タブ : アプリケーション検査マップのオプションを設定します。
  - — Prompt to add inspect map before applying changes : 検査マップが未設定の場合は、警告します。
  - — Make advanced view the default inspect view : アプリケーション検査のデフォルト表示を詳細表示に設定します。
    - Ask to make advanced view the default view : アプリケーション検査のデフォルト表示を詳細表示にするかどうかを確認するダイアログボックスを表示します。ダイアログボックスを表示しない場合、チェックボックスをオフにします。
- Syslog Color Settings タブ : ホームページの背景色とシステム ログ メッセージの色を設定します。
  - — Severity column : 重大度を表示します。
  - — Background Color column : 重大度メッセージの背景色を設定します。色を変更するには、その行をクリックします。Pick a Color ダイアログボックスが表示されます。
  - — Foreground Color column : 重大度のメッセージの前景色（テキスト色）を設定します。色を変更するには、その行をクリックします。Pick a Color ダイアログボックスが表示されます。
  - — Restore Default button : デフォルトの設定に戻し、白の背景色に色つきのテキストで表示します。

（注） プリファレンスのチェックボックスのオン / オフを切り替えると、そのたびに変更結果が .conf ファイルに書き込まれ、ワークステーションで実行中の他のすべての ASDM セッションで使用可能になります。ASDM をリスタートすると、設定したプリファレンスが反映されます。

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
•	•	•	•	•

Tools メニュー

Tools メニューには ASDM のトラブルシューティング ツールがあります。ここから、別のソフトウェアを ASDM にアップロードしたり、接続状態を確認したり、コマンドラインからコマンドを実行したりできます。

- Command Line Interface：テキスト ベース ツールでセキュリティ アプライアンスにコマンドを送信し、結果を確認できます。詳細については、Command Line Interface ダイアログボックスを参照してください。
- Packet Tracer：指定した送信元アドレスとインターフェイスから宛先まで、パケットをトレースできます。プロトコルおよびポートをデータ タイプに関わりなく指定でき、そこで実行された処理の詳細データを含むパケットの一部始終を表示することができます。詳細については、Packet Tracer ダイアログボックスを参照してください。
- Ping：セキュリティ アプライアンスおよび関係する通信リンクのコンフィギュレーションや動作を検証できる便利なツールで、他のネットワーク デバイスの基本的なテストにも使用できます。詳細については、Ping ダイアログボックスを参照してください。
- Traceroute：宛先までのパケット ルートを決定できます。詳細については、Traceroute ダイアログボックスを参照してください。
- File Management：フラッシュ メモリに保存されたファイルを表示、移動、コピー、削除できます。また、フラッシュ メモリにディレクトリを作成することもできます。詳細については、File Management を参照してください。また、File Transfer ダイアログボックスで、TFTP、フラッシュ メモリ、ローカル PC などさまざまなファイル システム間のファイル転送ができます。
- Upload ASDM Assistant Guide：フラッシュ メモリに XML ファイルをアップロードし、ASDM Assistant が使用するデータを格納できます。これらのファイルは Cisco.com からダウンロードできます。
- Upgrade Software：セキュリティ アプライアンスのイメージや ASDM のイメージなどのイメージ ファイルをユーザ PC にダウンロードし、フラッシュ メモリにアップロードできます。詳細については、「Upload Image from Local PC」を参照してください。
- System Reload：システムをリスタートし、保存したコンフィギュレーションをメモリにリロードします。詳細については、System Reload ダイアログボックスを参照してください。
- IPS/CSC Password Reset：AIP SSM や CSC SSM に設定されているパスワードをデフォルト（cisco）にリセットします。詳細については、P.35-3 の「AIP SSM パスワードのリセット」および P.36-14 の「Restoring the Default Password」を参照してください。
- ASDM Java Console：Java コンソールを表示します。

Command Line Interface

Tools > Command Line Interface > Command Line Interface

Command Line Interface ダイアログボックスのテキスト ベース ツールでセキュリティ アプライアンスにコマンドを送信し、結果を表示できます。

（注）　ASDM の CLI ツールからコマンドを入力すると、セキュリティ アプライアンスの接続ターミナルからコマンドを入力したときと動作が異なる場合があります。

コマンド エラー

誤った入力コマンドによってエラーが発生した場合、問題が生じたコマンドは実行されず、その他のコマンドはエラーを無視して実行されます。エラーが発生した場合は、Response ボックスの表示メッセージでエラー内容とその関連情報を確認できます。

（注）　コマンドのリストについては、『*Cisco Security Appliance Command Reference*』を参照してください。いくつかの例外を除き、ほとんどすべての CLI コマンドが ASDM でサポートされています。

インタラクティブ コマンド

インタラクティブ コマンドは Command Line Interface ダイアログボックスでサポートされていません。これらのコマンドを ASDM で使用するには、次のように、**noconfirm** キーワード（使用できる場合）を指定します。

```
crypto key generate rsa modulus 1024 noconfirm
```

管理者間の競合の回避

管理者権限を持つ複数のユーザがセキュリティ アプライアンスの実行コンフィギュレーションをアップデートできます。ASDM の CLI ツールでコンフィギュレーションを変更する場合は、アクティブな管理セッションが他にないことを事前に確認してください。複数のユーザが同時にセキュリティ アプライアンスを設定すると、最後に加えられた変更が反映されます （**Monitoring** タブをクリックすると、同じセキュリティ アプライアンスで現在アクティブな他の管理セッションを確認できます)。

ASDM のコンフィギュレーション変更の表示

CLI ツールでコンフィギュレーションを変更した場合、**Refresh** ボタンをクリックすると、ASDM の変更結果を表示できます。

前提条件

CLI ツールで実行できるコマンドは、ユーザ権限によって異なります。「Authorization タブ」を参照してください。ASDM のメイン ウィンドウの下にあるステータス バーの権限レベルで、CLI 特権コマンドの実行権限の有無を確認できます。

フィールド

- Command：セキュリティ アプライアンスにコマンドを送信します。
  - Single Line：一度に 1 コマンドだけ入力します。直前に入力したコマンドが表示されていますが、別のコマンドを入力することもできます。
  - Multiple Line：複数のコマンドラインを入力します。
  - Enable context sensitive help (?)：コマンドの CLI ヘルプを表示するには、コマンドの後に「?」を入力します。Enter キーを押さなくても「?」を入力するだけでヘルプが表示されます。

    このチェックボックスをオフにすると、デバイスに送信する前に ASDM は「?」文字をエスケープし、テキスト文字列として「?」を入力することができます。したがって、コマンドのヘルプは表示されません。
- Response：コマンド ボックスに入力したコマンドの実行結果を表示します。
- Send：すべてのコマンドをセキュリティ アプライアンスに送信します。
- Clear Response：Response ボックスのテキストをすべてクリアします。

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
•	•	•	•	•

Packet Tracer

パケット トレーサ ツールを実行すると、パケット スニファおよびネットワークの分離障害をトレースできます。

このツールは、パケットの詳細、およびセキュリティ アプライアンスでのパケット処理方法に関して、詳細な情報を提供します。コンフィギュレーションのコマンドでパケットがドロップされない限り、パケット トレーサ ツールでその原因に関する情報が分かりやすく表示されます。たとえば、無効なヘッダー検証が原因でパケットがドロップした場合、「packet dropped due to bad ip header (reason)」と、メッセージが表示されます。

パケットを取得するだけでなく、パケットの一部始終をトレースし、セキュリティ アプライアンスが想定どおり動作しているかどうかを確認することもできます。パケット トレーサ ツールでは次のことができます。

- ネットワーク上でのすべてのパケット ドロップのデバッグ
- コンフィギュレーションが意図したとおりに機能しているかどうかの検証
- パケットに適切なルールとルールを追加する CLI 行の表示
- データ パスでのパケット変更のタイム ラインの表示
- トレーサ パケットのデータ パスへの挿入

フィールド

- ***Interface***：パケット トレースの発信元インターフェイスを指定します。
- ***Packet type***：パケット トレースのプロトコル タイプを指定します。指定できるプロトコル タイプは、*icmp*、*rawip*、*tcp*、および *udp* です。
  - ***Source IP***：パケット トレースの送信元アドレスを指定します。
  - ***Source Port***：パケット トレースの送信元ポートを指定します。
  - ***Destination IP***：パケット トレースの宛先アドレスを指定します。
  - ***Destination Port***：パケット トレースの宛先ポートを指定します。
- ***Start***：パケット トレースを開始します。
- ***Clear***：すべてのフィールドをクリアします。
- ***Show animation***：チェックボックスをオンにして、パケット トレースをグラフィック表示します。
- ***Information Display Area***：パケット トレースの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
•	•	•	•	•

Ping

Tools > Ping > Ping

Ping ダイアログボックスの便利なツールでセキュリティ アプライアンスおよび関係する通信リンクのコンフィギュレーションおよび動作を検証でき、他のネットワーク デバイスの基本的なテストもできます。

ping は、潜水艦の音波探知機と同等のネットワーク ツールです。ping を IP アドレスに送信すると、エコーまたは応答が返されます。この簡単なプロセスで、ネットワーク デバイスどうしの検出、識別、およびテストができます。

Ping ツールは、RFC-777 と RFC-792 で規定された ICMP というプロトコルを使用します。ICMP で定めたのは、2 つのネットワーク デバイス間で送受される*エコー*と*エコー応答*のトランザクションで、これは ping として知られています。*エコー*（要求）パケットをネットワーク デバイスの IP アドレスに送信します。受信側のデバイスは送信元と宛先のアドレスを逆にしてから、パケットを *エコー応答*として送り返します。

Ping ツールの使い方

管理者は ASDM の Ping ツールを利用し、次のようにさまざまな方法でインタラクティブな診断ができます。

- インターフェイス間のループバック テスト：同じセキュリティ アプライアンスで一方のインターフェイスから相手側のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- セキュリティ アプライアンスインターフェイスへの ping 送信：他のセキュリティ アプライアンスのインターフェイスに対して Ping ツールまたは別の送信元から ping を送信すると、相手側がアップしていて応答することを確認できます。
- セキュリティ アプライアンスを通過する ping 送信：Ping ツールの送信 ping パケットがデバイスに到達する途中で、中間のセキュリティ アプライアンスを通過する場合があります。エコーパケットは、返されるときにそのインターフェイスを両方とも通過します。この手順によって、中間にある装置のインターフェイス、動作、応答時間についての基本的なテストができます。
- ネットワーク デバイスの動作に疑問がある場合:セキュリティ アプライアンスのインターフェイスから正常に機能していないと思われるネットワーク デバイスに ping を送信する場合があります。インターフェイスの設定が正常にもかかわらずエコーを受信しない場合、デバイスに問題があると考えられます。
- 中間の通信状態をテストする場合：エコー要求を返すことが分かる、動作が正常なネットワーク デバイスにセキュリティ アプライアンスのインターフェイスから ping を送信する場合があります。エコーを受信すると、中間にあるデバイスはすべて正常に動作し、物理的に正しく接続されていることを確認できます。

Ping ツールのトラブルシューティング

ping でエコーを受信できない場合、おそらく原因はセキュリティ アプライアンスのコンフィギュレーションまたは動作にエラーがあると考えられます。必ずしも ping に対する「NO response」の IP アドレスが原因とは限りません。Ping ツールを利用する前に次の点を確認してから、セキュリティ アプライアンスの*インターフェイスから*または*インターフェイス*へ、あるいは*インターフェイス経由で* ping を送信してください。

インターフェイスの基本的な確認事項

- インターフェイスが正常に設定されていることを、Configuration > Properties > Interfaces で確認します。
- スイッチやルータなど通信パスの中間デバイスで、他のタイプのネットワーク トラフィックが正常に配信されているかどうかを確認します。
- 「既知の正常な」送信元を使用して、他のタイプのトラフィックが正常に通過するかどうかを確認します。Monitoring > Interface Graphs を使用してください。

セキュリティ アプライアンス インターフェイスから ping を送信

インターフェイスの基本的なテストを行う場合、セキュリティ アプライアンスのインターフェイスからネットワーク デバイスに ping を送信する方法があります。その場合、他の方法でネットワーク デバイスが正常に動作し、中間通信パス経由でエコーが返されることを事前に確認しておきます。

- セキュリティ アプライアンスから送信した ping を「既知の正常な」デバイスで受信して確認します。受信できない場合、おそらくインターフェイスの送信側ハードウェアまたはコンフィギュレーションに問題があります。
- セキュリティ　アプライアンスのインターフェイス設定が正しいにもかかわらず「既知の正常な」デバイスのエコーを受信できない場合、インターフェイスの受信側ハードウェアに問題があると考えられます。インターフェイスを「既知の正常な」受信機能に変更し、「既知の正常な」デバイスから ping のエコーを受信できれば、変更前のインターフェイスは受信側ハードウェアに問題があると確認できます。

セキュリティ アプライアンス インターフェイスへ ping を送信

セキュリティ アプライアンスのインターフェイスへ *ping を送信*する場合、Configuration > Properties > Administration > ICMP パネルのインターフェイスで ping 応答（ICMP の*エコー応答*）がイネーブルになっているかどうかを確認します。ping 機能がディセーブルになっていると、セキュリティ アプライアンスは他のデバイスやソフトウェア アプリケーションから検出されず、ASDM の Ping ツールにも応答しません。

セキュリティ アプライアンス インターフェイス経由で ping を送信

- まず、「既知の正常な」送信元からセキュリティ アプライアンスを経由し、他のタイプのネットワーク トラフィックが通過することを確認します。Monitoring > Interface Graphs、または SNMP 管理ステーションを使用します。
- イネーブルにした内部ホストから外部ホストに ping を送信するには、Configuration > Access Rules で内部および外部インターフェイスの ICMP アクセスを正しく設定する必要があります。

フィールド

- IP Address：ICMP エコー要求パケットの宛先 IP アドレス。

（注）　**Configuration > Hosts/Networks > Basic Information > Host Name** パネルで設定したホスト名がある場合、IP アドレスとして使用できます。

- Interface :（オプション）エコー要求パケットを送信するセキュリティ アプライアンス インターフェイスを指定します。指定しない場合、セキュリティ アプライアンスはルーティング テーブルを調べ、宛先アドレスを見つけて必要なインターフェイスを使用します。
- Ping Output：ping の実行結果。**Ping** をクリックすると、IP アドレスには ping が 3 回送信され、次のフィールドに実行結果が 3 つ表示されます。
  - Reply IP address/Device name : ping が送信されたデバイスの IP アドレスまたはデバイス名（設定されている場合）。ホストやネットワークに割り当てたデバイス名は、結果が「**NO response**」でも表示される場合があります。
  - Response time/timeout (ms) : ping を送信すると、ミリ秒タイマーが開始します。ここで指定する最大値がタイムアウト値になります。たとえば、異なるルートやアクティビティ レベルの相対応答時間を比較するテストで役立ちます。

    ping の実行結果の例：

    ```
    Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
    ```

    ping に失敗すると、実行結果は次のようになります。

    ```
    Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
    ?????
    Success rate is 0 percent (0/5)
    ```

- Ping : ICMP のエコー要求パケットを、指定したインターフェイスまたはデフォルトのインターフェイスから指定した IP アドレスへ送信し、応答タイマーを開始します。
- Clear Screen：これまでに実行した ping コマンドの実行結果を画面でクリアします。

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
•	•	•	•	•

Traceroute

Traceroute ダイアログボックスのツールで、宛先までのパケット ルートを簡単に決定できます。

トレースルートの出力

トレースルート ツールは、プローブを送信するたびに結果を表示します。出力結果の各行は、TTL 値の上昇順に対応します。トレースルート ツールの出力に表示される記号を説明します。

出力記号	説明
*	プローブがタイムアウトするまでに応答がなかった
nn msec	指定したプローブ数のノードごとのラウンドトリップ時間（ミリ秒単位）
!N.	ICMP ネットワークに到達不能
!H	ICMP ホストに到達不能
!P	ICMP プロトコルに到達不能
!A	管理上の禁止 ICMP
?	不明な ICMP エラー

フィールド

- Hostname or IP address：ルート トレースの対象になるホスト名を指定します。ホスト名が指定されている場合、***Configuration*** > ***Global Objects*** > ***IP Names*** で定義するか、DNS サーバを設定してトレースルートがホスト名の IP アドレスを解決できるようにします。
- Timeout : 応答を待機しているときの接続タイムアウト時間を秒単位で指定します。デフォルトは 3 秒です。
- Port : UDP プローブ メッセージで使用される宛先ポートを指定します。デフォルトは 33434 です。
- Probe：各 TTL レベルで送信されるプローブ数を指定します。デフォルトは 3 個です。
- Min & Max TTL：最初のプローブのデータ表示時間の最小値と最大値を指定します。デフォルトの最小値は 1 です。値を大きくすると、始めに表示される既知のホップが少なくなります。デフォルトの最大値は 30 です。トレースルート パケットが宛先に到達するか、この最大値に達するとツールは終了します。
- Destination Port：UDP プローブ メッセージで使用される宛先ポートを指定します。デフォルトは 33434 です。
- Specify Source Interface or IP Address：パケットをトレースする発信元インターフェイスまたは送信元 IP アドレスを指定します。この IP アドレスは、少なくとも 1 つのインターフェイスの中に含まれている必要があります。透過モードの場合は、セキュリティ アプライアンスの管理 IP アドレスを指定します。
- Reverse Resolve：チェックボックスをオンにすると、名前解決が設定されている場合、使用されたホップ名が出力結果に表示されます。チェックボックスがオフの場合、出力結果には IP アドレスが表示されます。
- Use ICMP：UDP プローブ パケットでなく ICMP プローブ パケットを使用します。
- Traceroute Output：トレースルートの詳細メッセージを表示します。
- Traceroute：トレースルートを開始します。
- Clear：すべてのフィールドをクリアします。

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
•	•	•	•	•

File Management

Tools > File Management > File Management

フラッシュ メモリに保存されたファイルの表示、移動、コピー、削除ができます。また、フラッシュ メモリにディレクトリを作成することもできます。

マルチコンテキストモードの場合、このツールはシステムでのみ使用できます。

フィールド

- Folders：ディスクにあるフォルダを表示します。
  - Flash Space：フラッシュ メモリのサイズと空き容量を示します。
    Total：フラッシュ メモリの全体のサイズを示します。
    Available：空き容量を示します。

- Files：選択したフォルダに含まれるファイルの情報を表示します。
  - Path：選択されたパスを示します。
  - Filename
  - Size (bytes)
  - Time Modified
  - Status
- View：選択したファイルをブラウザに表示します。
- Cut：選択したファイルを切り取り、他のディレクトリに貼り付けられます。
- Copy：選択したファイルをコピーし、他のディレクトリに貼り付けられます。
- Paste：コピーしたファイルを選択した場所に貼り付けます。
- Delete：選択したファイルをフラッシュ メモリから削除します。
- Rename：ファイルの名前を変更します。
- New Directory：ファイルを保存するディレクトリを新規作成します。
- File Transfer：File Transfer ダイアログボックスを開きます。

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
•	•	•	—	•

Upload Image from Local PC

Tools > Upgrade Software > Upload Image from Local PC

Upload Image from Local PC ダイアログボックスで、セキュリティ アプライアンスのイメージ ファイル、ASDM のイメージ、PC 上のその他のイメージを選択し、フラッシュ メモリにアップロードできます。

フィールド

- Image to upload：アップロードするイメージ タイプを選択します。
- Local File Path：ユーザの PC 上のファイルのパスを入力します。
  - Browse Local：選択して PC 上のファイルを参照します。
- Flash File System Path：ファイルのコピー先となるフラッシュ メモリのパスを入力します。
  - Browse Local：選択してフラッシュ メモリのディレクトリやファイルを参照します。

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
•	•	•	•	•

File Transfer

Tools > File Management > File Management > File Transfer

File Transfer により、HTTPS、TFTP、FTP を使用するかローカル イメージを参照して、セキュリティ アプライアンスとの間でファイルを相互にコピーすることができます。

フィールド

- Source File：転送対象になるソース ファイルを選択します。
  - Remote Server：リモート サーバからファイルを転送する場合に選択します。

    Path：ファイルの場所のパスを入力します。サーバの IP アドレスを含めます。

    Port/Type：リモート サーバのポート番号またはタイプ（FTP の場合）を入力します。次の FTP タイプが有効です。

    ap：パッシブ モードの ASCII ファイル

    an：非パッシブ モードの ASCII ファイル

    ip：パッシブ モードのバイナリ イメージ ファイル

    in：非パッシブ モードのバイナリ イメージ ファイル
  - Flash File System：フラッシュ メモリのファイルをコピーする場合に選択します。

    Path：ファイルの場所のパスを入力します。

    Browse Flash：選択して、セキュリティ アプライアンスでコピーされたファイルの場所を参照します。
  - Local Computer：ローカル PC からファイルをコピーする場合に選択します。

    Path：ファイルの場所のパスを入力します。

    Browse Localhost：ローカル PC を参照し、転送対象ファイルを検索します。
- Destination File：転送先のファイルを選択します。送信元の場所によって、Flash File System と Remote Server のどちらかが自動選択されます。
  - Flash File System：ファイルをフラッシュ メモリに転送します。

    Path：ファイルの場所のパスを入力します。

    Browse Flash：選択して、セキュリティ アプライアンスでファイルが転送される場所を参照します。
  - Remote Server：リモート サーバにファイルを転送します。

    Path：ファイルの場所のパスを入力します。

    Type：FTP 転送の場合、タイプを入力します。次のタイプが有効です。

    ap：パッシブ モードの ASCII ファイル

    an：非パッシブ モードの ASCII ファイル

    ip：パッシブ モードのバイナリ イメージ ファイル

    in：非パッシブ モードのバイナリ イメージ ファイル
- Transfer File：ファイル転送を開始します。

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
•	•	•	—	•

Upload ASDM Assistant Guide

Tools > Upload ASDM Assistant Guide

Upload ASDM Assistant Guide を実行すると、フラッシュ メモリに XML ファイルをアップロードして、タスクに応じて ASDM の使用方法のヘルプを格納できます。これらのファイルは Cisco.com から取得できます。ファイルをロードすると、File メニューの Search フィールドから参照できます。

フィールド

- File to upload：ユーザのコンピュータ上にある XML ファイルの名前で、通常 Cisco.com から取得されます。
- Flash File System Path：XML ファイルを保存するフラッシュ メモリのパスを示します。
- Upload File：アップロードを開始します。

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
•	•	•	—	•

System Reload

Tools > System Reload > System Reload

System Reload を実行すると、システムをリスタートし、保存されたコンフィギュレーションをメモリにリロードします。System Reload ダイアログボックスで、システムのリロードのタイミング、実行コンフィギュレーションをフラッシュ メモリに保存する / しない、リロード時に接続しているユーザにメッセージを送信する / しない、を選択できます。

フィールド

- Reload Scheduling：リロードを実行するタイミングを設定します。
  - Configuration State：リロード時に実行コンフィギュレーションを保存するかしないかを選択します。

    Save the Running Configuration at Time of Reload：リロード時に実行コンフィギュレーションを保存します。

    Reload Without Saving the Running Configuration：リロード時に実行コンフィギュレーションに加えられた変更を破棄します。
- Reload Start Time：リロードのタイミングを選択します。
  - Now：リロードをただちに実行します。
  - Delay by：指定した時間だけ遅延させてリロードします。リロード開始までの経過時間を、時間と分、または分で入力します。
  - Schedule at：リロードする時刻と日付を指定してスケジュールを設定します。リロードの実行時刻を入力し、リロードのスケジュール日を選択します。
- Reload Message：リロード時に ASDM のインスタンスを開いたときに送信されるメッセージを入力します。
- On Reload Failure Force Immediate Reload after：リロードに失敗した場合、もう一度リロードを実行するまでの経過時間を、時間と分、または分で指定します。
- Schedule Reload：設定に従ってリロードをスケジュールします。

- Reload Status：リロードのステータスを表示します。
- Cancel Reload：スケジュールされたリロードをキャンセルします。
- Refresh：Reload Status 画面をリフレッシュします。
- Details：スケジュールされたリロードの詳細を表示します。

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
•	•	•	—	•

Wizards メニュー

Wizards メニューで、さまざまな機能を設定するウィザードを実行できます。

- Startup Wizard：ASDM Startup Wizard を利用して、セキュリティ アプライアンスの初期コンフィギュレーションを段階的に設定することができます。設定画面をクリックすると表示されるプロンプトに従って、使用するセキュリティ アプライアンスの情報を入力できます。Startup Wizard で設定すると、セキュリティ アプライアンスの使用をすぐに開始できます。
- VPN Wizard：このウィザードを使用して、VPN ポリシーをセキュリティ アプライアンスに簡単に設定します。
- High Availability and Scalability Wizard：このウィザードを使用して、セキュリティ アプライアンスにフェールオーバーを設定します。

Help メニュー

Help メニューでは、オンライン ヘルプへのリンクの他に、ASDM とセキュリティ アプライアンスの情報へのリンクも提供されます。

- Help Topics：新しいブラウザ ウィンドウが開き、左側のフレームに目次、画面の名前、索引で整列されたヘルプが表示されます。この画面で必要な項目のヘルプを見つけるか、上部の Search タブで検索します。
- Help for Current Screen：その時点で開いている画面、パネル、ダイアログボックスの文脈依存ヘルプが開きます。また、「?」マークのヘルプ アイコンをクリックして文脈依存ヘルプを表示することもできます。
- Release Notes：Web サイトから最新バージョンの『*Cisco ASDM Release Notes*』を開きます。リリース ノートには、ASDM のソフトウェアとハードウェア要件の最新情報、およびソフトウェア変更に関する最新情報が記載されています。
- Getting Started：スタートアップ ガイドのヘルプ項目が表示され、ASDM の使用をすぐに開始できます。
- Glossary：用語および略語の定義が記載されています。
- Feature Matrix：Web サイトから最新バージョンの『*Cisco ASDM Release Notes*』を開きます。最新のライセンス情報が記載されています。
- Feature Search：ASDM の機能を検索できます。各パネルのタイトルをすべて検索して一致項目を表示します。ハイパーリンクをクリックすると、パネルがただちに表示されます。検索された異なる 2 種類のパネルをすばやく切り換えるには、Back または Forward ボタンをクリックします。ASDM のツールバーにある Search アイコンをクリックすることもできます。

- How do I? : ASDM Assistant が開いて、Cisco.com からダウンロード可能なコンテンツを検索できます。特定のタスクの実行に関する詳細が分かります。
- Legend : ASDM にあるアイコンとそれらの機能を説明したリストを表示します。
- About Cisco Platform : セキュリティ アプライアンスに関するさまざまな情報を一覧表示します。ソフトウェア バージョン、ハードウェア構成、スタートアップ時にロードされるコンフィギュレーション ファイルやソフトウェア イメージなどが含まれます。これらはトラブルシューティングの際に役立つ情報です。
- About Cisco ASDM 5.2 : ASDM に関する情報を表示します。ASDM ソフトウェア バージョン、ホスト名、特権レベル、オペレーティング システム、ブラウザのタイプ、Java のバージョンなどが含まれます。

ツールバー

ツールバーは ASDM ウィンドウ上部のメニュー項目の下にあり、ここからホームページ、コンフィギュレーション ページ、モニタリング ページにアクセスできます。また、マルチコンテキスト モードでシステムとセキュリティ コンテキストを選択したり、ナビゲーションなどよく使用する機能を実行したりできます。

- System/Contexts : 下矢印をクリックすると左側のペインにコンテキストのリストが開いて表示され、上矢印をクリックするとコンテキストのドロップダウン リストが元に戻ります。リストが展開されているときに左向き矢印をクリックすると、ペイン全体は左側に折りたたまれます。右向き矢印をクリックすると、ペインが元に戻ります。システムを管理するには、リストから System を選択します。コンテキストを管理するには、リストから該当するコンテキストを選択します。
- Home : ホームページを表示します。インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、セキュリティ アプライアンスの重要な情報を一目で確認できます。詳細については、「ホームページ」を参照してください。マルチモードの場合、システムのホームページはありません。
- Configuration : セキュリティ アプライアンスを設定します。左側のペインで、設定する機能のボタンをクリックします。
- Monitoring : セキュリティ アプライアンスを監視します。左側のペインで、監視する機能のボタンをクリックします。
- Back : 直前に表示した ASDM パネルに戻ります。
- Forward : 直前に表示した ASDM パネルに進みます。
- Search : ASDM の機能を検索できます。各パネルのタイトルをすべて検索して一致項目を表示します。ハイパーリンクをクリックすると、パネルがただちに表示されます。検索された異なる 2 種類のパネルをすばやく切り換えるには、Back または Forward をクリックします。
- Refresh : 選択すると、現在の実行コンフィギュレーションで ASDM をリフレッシュします。監視中のグラフはリフレッシュされません。
- Save : 実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存します。書き込みアクセスが禁止されているコンテキストの場合（HTTP にあるなど）、実行コンフィギュレーションは保存されません。
- Help : その時点で表示されている画面の文脈依存ヘルプを開きます。

ステータスバー

ステータスバーは ASDM ウィンドウの下部に表示されます。ステータスバーの左から右に、次のようなエリアが表示されます。

- Status：コンフィギュレーションのステータスが、「Device configuration loaded successfully」のように表示されます。
- User Name：ASDM を使用しているユーザの名前が表示されます。ユーザ名なしでログインするとユーザ名は「admin」になります。
- User Privilege：ASDM を使用しているユーザの権限レベルが表示されます。
- Commands Ignored by ASDM：アイコンをクリックすると、ASDM で実行されなかったコンフィギュレーションのコマンドのリストが表示されます。これらのコマンドはコンフィギュレーションから削除されません。詳細については、「Show Commands Ignored by ASDM on Device」を参照してください。
- Status of Connection to Device：ASDM とセキュリティ アプライアンスの接続ステータスを表示します。詳細については、「Connection to Device」を参照してください。
- Save to Flash Needed：ASDM のコンフィギュレーションを変更したが、実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存していないことを示します。
- Refresh Needed：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変更された場合、ASDM のコンフィギュレーションをセキュリティ アプライアンスからリフレッシュする必要があるかどうかを示します。コンフィギュレーションを CLI で変更したような場合です。
- SSL Secure：ASDM への接続に SSL を使用し、安全であることを示します。
- Time：セキュリティ アプライアンスのスイッチで設定された時刻を示します。

Connection to Device

Status Bar > Status of Connection to Device icon > Connection to Device

ASDM はセキュリティ アプライアンスとの接続を常に保ち、最新のモニタリング データおよびホームページ データを表示します。このダイアログボックスに接続ステータスが表示されます。コンフィギュレーションを変更する場合、変更している間 ASDM は接続をもう一つ開き、変更が終わるとその接続を閉じます。その場合の接続はこのダイアログボックスに表示されません。

パネル共通のボタン

ほとんどの ASDM パネルで使用できるボタンを次に示します。

- Apply：ASDM で加えた変更データをセキュリティ アプライアンスに送信し、実行コンフィギュレーションに適用します。**Save** をクリックすると、実行コンフィギュレーションのコピーがフラッシュ メモリに書き込まれます。File メニューでは、実行コンフィギュレーションのコピーをフラッシュ メモリ、TFTP サーバ、フェールオーバー スタンバイ装置に書き込むことができます。
- **Reset**：変更データを無効にして、変更前、または **Refresh** や **Apply** を最後にクリックした時点の表示情報に戻します。Reset したら Refresh を実行し、現在の実行コンフィギュレーション データが表示されることを確認してください。
- **Cancel**：変更を無効にして、直前のパネルに戻ります。
- **Help**：選択したパネルのヘルプを表示します。

ヘルプ ウィンドウについて

ここでは、次の項目について説明します。

ヘッダー ボタン

ヘッダー ボタンを使用すると、ヘルプをナビゲーションして目的の項目を探し出せます。

- About ASDM：ASDM に関する情報を表示します。
- Search：ヘルプ項目を検索します。
- Using Help：オンライン ヘルプの活用方法を説明します。
- Glossary：ASDM およびネットワークの用語集を表示します。

左側のペインのタブ：オンライン ヘルプのナビゲーションを容易にします。

- Contents：目次を表示します。
- Screens：ヘルプ ファイルを画面の名前ごとに表示します。
- Index：ASDM のオンライン ヘルプにあるヘルプ項目の索引を表示します。

右側のペインのヘルプ項目：選択した項目のヘルプを表示します。

注意

ヘルプをアプレット モードで起動したときヘルプ ページを表示中のウィンドウがあれば、同じブラウザのウィンドウ上に次のヘルプ ページを表示します。ヘルプ ページを表示中のウィンドウがなければ、新規のブラウザ ウィンドウに表示します。

Netscape がデフォルト ブラウザの場合、ヘルプをアプリケーション モードで起動すると、ヘルプを起動するたびに新規のブラウザ ウィンドウが開いてヘルプ ページが表示されます。IE がデフォルト ブラウザの場合、ユーザの設定により、ヘルプ ページが直前に使用していたウィンドウに表示される場合と、新しいウィンドウが開いて表示される場合があります。表示方法を IE に設定するには、オプションの Tools > Internet Options > Advanced > Reuse window でショートカットを実行します。

ホームページ

ASDM の Home ペインからセキュリティ アプライアンスの重要な情報を一目で確認できます。SSM をセキュリティ アプライアンスにインストールしている場合は、ホームページにタブが追加されます。追加されたタブをクリックすると、SSM のソフトウェアに関するステータス情報を表示できます。

この領域の設定の詳細については、次を参照してください。

- Home
- Home > Content Security タブ

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
•	•	•	•	—

Home

Home

ASDM の Home ペインから、インターフェイスのステータス、実行中のバージョン、ライセンス情報、パフォーマンスなど、セキュリティ アプライアンスの重要な情報を一目で確認できます。

ASDM のホームページに表示される詳細のほとんどは、ASDM の実行中に他の場所から確認できますが、Home ペインではセキュリティ アプライアンスの実行状態をすぐに確認できるので便利です。Home ペインのステータス情報は 10 秒ごとに更新されます。

フィールド

- Device Information：デバイス情報を表示するタブが 2 つあります。
  - General：次の情報が表示されます。

    Host Name：表示のみ。セキュリティ アプライアンスのホスト名を示します。ホスト名の設定方法については、「Device」を参照してください。

    Platform Version：表示のみ。セキュリティ アプライアンス ソフトウェアのバージョンを示します。

    Device Uptime：表示のみ。セキュリティ アプライアンスの実行経過時間を示します。

    ASDM Version：表示のみ。ASDM のバージョンを示します。

    Device Type：表示のみ。セキュリティ アプライアンスのモデルを示します。

    Firewall Mode：表示のみ。ファイアウォール モードを示します。「ルーテッド」または「透過」です。詳細については、「ファイアウォール モードの概要」を参照してください。

    Context Mode：表示のみ。コンテキスト モードを示します。「シングル」または「マルチ」です。詳細については、「セキュリティ コンテキストの概要」を参照してください。

    Total Flash：表示のみ。フラッシュ メモリの全体容量、内部フラッシュ メモリと外部フラッシュ メモリ カード（使用できる場合）の合計サイズを MB 単位で表示します。

    Total Memory：表示のみ。RAM の全体の容量を示します。
  - License：表示のみ。セキュリティ アプライアンスでライセンスされた機能のサポート レベルを示します。

- VPN Status：ルーテッド、シングルモードの場合のみ。次の情報が表示されます。
  - IKE Tunnels：表示のみ。接続されている IKE トンネル数を示します。
  - IPSec Tunnels：表示のみ。接続されている IPSec トンネル数を示します。
- System Resources Status：CPU およびメモリの使用状況に関する次の統計値を示します。
  - CPU：表示のみ。現在の CPU 使用率を示します。
  - CPU Usage (percent)：表示のみ。直前 5 分間の CPU 使用状況を示します。
  - Memory：表示のみ。現在のメモリ使用サイズを MB 単位で示します。
  - Memory Usage (MB)：表示のみ。直前 5 分間のメモリ使用状況を MB 単位で示します。
- Interface Status：インターフェイスごとにステータスが表示されます。インターフェイスの行を選択すると、入力と出力が Kbps でテーブルの下に表示されます。
  - Interface：表示のみ。インターフェイス名を示します。
  - IP Address/Mask：表示のみ。ルーテッド モードのみです。インターフェイスの IP アドレスとサブネット マスクを示します。
  - Line：表示のみ。インターフェイスの管理ステータスを示します。アイコンが赤の場合は回線がダウン、緑の場合は回線がアップしています。
  - Link：表示のみ。インターフェイスのリンク ステータスを示します。アイコンが赤の場合はリンクがダウン、緑の場合はリンクがアップしています。
  - Current Kbps：表示のみ。現在のインターフェイス 通過速度を Kbps で示します。
- Traffic Status：インターフェイス全体の接続数 / 秒と、最も遅いセキュリティ インターフェイスのトラフィック スループットのグラフを示します。
  - Connections per Second Usage：表示のみ。直前 5 分間の UDP および TCP の接続数 / 秒を示します。グラフには、現在の接続数が UDP と TCP のタイプごとに表示され、また合計値も表示されます。
  - Name Interface Traffic Usage (Kbps)：表示のみ。最も低いセキュリティ インターフェイスのトラフィック スループットを示します。同じレベルのインターフェイスが複数ある場合、ASDM にはアルファベット順で先頭のインターフェイスが表示されます。グラフには、現在のスループットが入力 Kbps と出力 Kbps のタイプごとに表示されます。
- Latest ASDM Syslog Messages：セキュリティ アプライアンスから直前に出力されたシステム メッセージです。
  - Stop Message Display：ASDM のロギングを停止します。
  - Resume Message Display：ASDM のロギングを再開します。

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
•	•	•	•	—

Home > Content Security タブ

Home > Content Security

Content Security タブから、CSC（Content Security and Control）SSM に関する重要な情報を確認できます。このパネルは、CSC SSM をセキュリティ アプライアンスにインストールしないと表示できません。

CSC SSM の概要については、「CSC SSM について」を参照してください。

（注）　Configuration > Trend Micro Content Security > CSC Setup の Setup Wizard を実行しないと、Home > Content Security でこのパネルにアクセスできません。代わりにダイアログボックスが表示され、Home > Content Security から Setup Wizard に直接アクセスできます。

フィールド

- Device Information：次の情報が表示されます。

  Model：セキュリティ アプライアンスにインストールされている SSM のタイプです。

  Mgmt IP：CSC SSM の管理インターフェイスの IP アドレスを示します。

  Version：CSC SSM のソフトウェア バージョンを示します。

  Last Update：Trend Micro のソフトウェアを前回更新した日付を示します。

  Daily Node #：過去 24 時間の間に CSC SSM のサービス対象になったネットワーク デバイス数を示します。ASDM によって深夜 0 時に更新されます。

  Base License：アンチウイルス、アンチスパイウェア、FTP ファイル ブロッキング機能など CSC SSM の基本機能に関するライセンス ステータスを表示します。ライセンス有効期限の日付が表示されます。ライセンスの有効期限が過ぎている場合は、終了日が表示されます。ライセンスが設定されていない場合、このフィールドには「Not Available」と表示されます。

  Plus License：アンチスパム、アンチフィッシング、電子メール コンテンツ フィルタリング、URL のブロッキングやフィルタリングなど、CSC SSM の高度な機能に関するライセンス ステータスが表示されます。ライセンス有効期限の日付が表示されます。ライセンスの有効期限が過ぎている場合は、終了日が表示されます。ライセンスが設定されていない場合、このフィールドには「Not Available」と表示されます。

  Licensed Nodes：CSC SSM がライセンスによってサービス提供可能なネットワーク デバイスの最大数を示します。

- System Resources Status：CSC SSM の CPU およびメモリの使用状況に関する次の統計値を示します。
  - CPU：現在の CPU 使用率を示します。
  - CSC SSM CPU Usage (percent)：直前 5 分間の CPU 使用状況を示します。
  - Memory：現在のメモリ使用サイズを MB 単位で示します。
  - CSC SSM Memory Usage (MB)：直前 5 分間のメモリ使用状況を MB 単位で示します。
- Threat Summary：CSC SSM が検出した脅威に関する集約データを示します。
  - Threat Type：ウイルス、スパイウェア、フィルタ処理された URL、ブロックされた URL の 4 つのタイプの脅威を示します。
  - Today：過去 24 時間に検出された脅威の数が、脅威タイプごとに表示されます。
  - Last 7 Days：過去 7 日間に検出された脅威の数が、脅威タイプごとに表示されます。
  - Last 30 Days：過去 30 日間に検出された脅威の数が、脅威のタイプごとに表示されます。

- Email Scan：スキャンされた電子メール数と、検出されたウイルスやスパイウェアをグラフに表示します。
  - Email Scanned Count：スキャンされた電子メール数です。電子メール プロトコル（SMTP または POP3）で区分したグラフと、両方のプロトコルを合計したグラフで表示されます。グラフのデータは 10 秒間隔で表示されます。
  - Email Virus and Spyware：電子メール スキャンで検出されたウイルスと電子メールの数です。グラフは脅威のタイプ（ウイルス または スパイウェア）で区分して表示されます。グラフのデータは 10 秒間隔で表示されます。
- Latest CSC Security Events：CSC SSM から取得したセキュリティ イベント メッセージをリアルタイムで表示します。
  - Time：イベントの発生時刻を表示します。
  - Source：脅威が検出された IP アドレスまたはホスト名を表示します。
  - Threat/Filter：イベントをトリガーした脅威のタイプを表示します。URL フィルタ イベントの場合はフィルタが表示されます。
  - Subject/File/URL：脅威を含む電子メールの件名、脅威またはブロックされた URL、フィルタ処理された URL を含む FTP ファイル名を表示します。
  - Receiver/Host：脅威を含む電子メールの受信者、または脅威が検出されたノードの IP アドレスやホスト名を表示します。
  - Sender：脅威を含む電子メールの送信者を表示します。
  - Content Action：メッセージやファイルのコンテンツの対処の結果を示します。コンテンツを変更せずに配信、添付ファイルを削除、添付ファイルを検疫してから配信、などです。
  - Msg Action：メッセージの対処の結果を示します。メッセージを変更せずに配信、添付ファイルを削除してからメッセージを配信、メッセージの配信を停止、などです。

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
•	•	•	•	—