デバイス アクセスの設定

Configuration > Device Access

この章では、次の項目について説明します。

- AAA Access
- HTTPS/ASDM
- Secure Shell
- Telnet
- Virtual Access

AAA Access

Configuration > Device Access > AAA Access

AAA Access ペインには、管理アクセスの認証、認可、アカウンティングを設定するためのタブが含まれます。AAA サービスの概要については、「AAA サーバの設定」を参照してください。

- Authentication タブ
- Authorization タブ
- Accounting 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
•	•	•	•	—

Authentication タブ

Configuration > Device Access > AAA Access > Authentication タブ

セキュリティ アプライアンスへの管理者アクセスの認証をイネーブルにするには、このタブを使用します。認証では、有効なユーザ名およびパスワードを要求してアクセスを制御します。次の項目を認証するように、セキュリティ アプライアンスを設定できます。

- セキュリティ アプライアンスへのすべての管理接続（この接続は、次の方法を使用します）
  - Telnet
  - SSH
  - HTTPS/ASDM
  - シリアル
- **enable** コマンド

フィールド

- Require authentication to allow use of privileged mode commands：特権モード コマンドへのアクセスを制御するパラメータを指定します。
  - Enable：特権モード コマンドの使用が許可される前のユーザ認証の要求をイネーブルまたはディセーブルにします。
  - Server Group：ユーザの認証に使用するサーバ グループを選択し、特権モード コマンドを使用します。
  - Use LOCAL when server group fails：選択したサーバ グループに障害が発生した場合、ユーザの認証に LOCAL データベースの使用を許可し、特権モード コマンドを使用します。
- Require authentication for the following types of connections：認証を必要とする接続のタイプを指定するとともに、その認証に使用するサーバ グループを指定します。
  - HTTP/ASDM：HTTP/ASDM 接続に認証が必要かどうかを指定します。
  - Server Group：指定した接続タイプの認証に使用するサーバ グループを選択します。
  - Use LOCAL when server group fails：選択したサーバ グループに障害が発生した場合、指定した接続タイプの認証に LOCAL データベースを使用することを許可します。
  - SSH：SSH 接続に認証が必要かどうかを指定します。

- Telnet：Telnet 接続に認証が必要かどうかを指定します。
- Serial：シリアル接続に認証が必要かどうかを指定します。

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
•	•	•	•	—

Authorization タブ

Configuration > Device Access > AAA Access > Authorization タブ

認可では、有効なユーザ名およびパスワードでの認証後、ユーザごとにアクセスを制御します。管理コマンドを認可するようにセキュリティ アプライアンスを設定できます。

認可では、個々のユーザが使用できるサービスおよびコマンドを制御できます。認可では、すべての認証済みユーザにサービスを行う同じアクセスが提供されます。

コマンド認可をイネーブルにすると、（**Advanced** ボタンを使用した）特権レベルを個々のコマンドまたはコマンド グループに手動で割り当てるオプション、または（Restore Predefined User Account Privileges ボタンを使用した）事前定義ユーザ アカウント特権をイネーブルにするオプションが使用できます。

事前定義ユーザ	特権レベル	説明
管理者	15	すべての CLI コマンドへの完全アクセス
読み取り専用	5	すべてのコマンドへの読み取り専用アクセス
監視専用	3	タブの監視のみ

Predefined User Account Privileges Setup ペインには、Yes をクリックした場合、ASDM がセキュリティ アプライアンスに発行するコマンドおよび特権のリストが表示されます。Yes により、ASDM は、管理者、読み取り専用、監視専用の 3 つの特権をサポートします。

Command Privileges Setup ペインには、ASDM がセキュリティ アプライアンスに発行しようとしているコマンドおよび特権のリストが表示されます。リスト内で 1 つまたは複数のコマンドを選択し、Edit ボタンを使用して、選択したコマンドの特権レベルを変更できます。

フィールド

- Enable：セキュリティ アプライアンス コマンド アクセスの認可をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このペインの残りのパラメータがアクティブになります。
- Server Group：コマンドアクセスに対するユーザの認可に使用するサーバ グループを選択します。
- Use LOCAL when server group fails：選択したサーバ グループに障害が発生した場合、ユーザの認可に LOCAL データベースの使用を許可し、特権モード コマンドを使用します。
- Advanced：Command Privileges Setup ペインを開きます。このペインでは、個々のコマンドまたはコマンド グループに特権レベルを手動で割り当てることができます。

- Restore Predefined User Account Privileges：Predefined User Account Command Privilege Setup ペインを開きます。このペインでは、事前定義ユーザ プロファイルを設定するとともに、選択済みのリストになったコマンドの特権レベルを設定できます。

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
•	•	•	•	—

Command Privileges Setup

Configuration > Device Access > AAA Access > Authorization > Command Privileges Setup

個々のコマンドまたはコマンド グループに特権レベルを割り当てるには、このペインを使用します。カラムの先頭をクリックすると、選択したカラムをキー フィールドとして使用し、テーブル全体が英数字順に並び替わります。

- Command Mode : 特定のコマンド モードまたはすべてのモードを選択します。この選択により、リストのすぐ下の Command Modes テーブルに表示される内容が決まります。
- CLI Command：CLI コマンドの名前を指定します。
- Mode：このコマンドに適用されるモードを示します。一部のコマンドには、複数のモードが適用されます。
- Variant : 特権レベルの適用先である特定のコマンドの形式（show または clear など）を示します。
- Privilege：このコマンドに現在割り当てられている特権レベルが表示されます。
- Edit : Select Command(s) Privilege ダイアログボックスを表示します。このダイアログボックスでは、親ウィンドウで選択した 1 つまたは複数のコマンドの特権レベルをリストから選択できます。OK をクリックすると、ただちに変更内容が Command Modes テーブルに反映されます。
- Select All：Command Modes テーブルの内容全体を選択します。

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
•	•	•	•	—

Predefined User Account Command Privilege Setup

Configuration > Device Access > AAA Access > Authorization > Predefined User Account Command Privilege Setup

このペインでは、管理者、読み取り専用、監視専用という名前が付いたユーザ プロファイルを、セキュリティ アプライアンスがセットアップするかどうか尋ねます。このペインには、Authentication/Authorization/Accounting ペインの Authorization タブにある Restore Predefined user Account Privileges をクリックして移動します。

フィールド

- Command List：事前定義ユーザ アカウント特権のセットアップで影響を受ける CLI コマンド、そのモード、バリアント、特権が一覧表示されます。
  - CLI Command：CLI コマンドの名前を指定します。
  - Mode：このコマンドに適用されるモードを示します。一部のコマンドには、複数のモードが適用されます。
  - Variant：特権レベルの適用先である特定のコマンドの形式（show または clear など）を示します。
  - Privilege：このコマンドに現在割り当てられている特権レベルが表示されます。
- Yes：リストされたコマンドをそれぞれの特権レベルでセットアップするように、セキュリティ アプライアンスに指示します。このセットアップでは、User Accounts ペインを介して、特権レベル 15 の管理者、特権レベル 5 の読み取り専用、特権レベル 3 の監視専用というそれぞれの役割でユーザが作成されます。
- No：コマンドおよびユーザの特権レベルを手動で管理します。

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
•	•	•	•	—

Accounting タブ

Configuration > Device Access > AAA Access > Accounting タブ

アカウンティングでは、セキュリティ アプライアンスを通過するトラフィックを追跡し続けます。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウンティングできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウンティングできます。アカウンティング情報には、セッションの開始時刻と終了時刻、AAA クライアント メッセージとユーザ名、そのセッションでセキュリティ アプライアンスを通過したバイト数、使用されたサービス、セッションの継続時間が含まれます。

（注）　アカウンティングを設定できるのは、TACACS+ サーバ グループに対してだけです。 TACACS+ サーバ グループがまだ設定されていない場合は、Configuration > Properties > AAA Setup > AAA Server Groups で移動します。

フィールド

- Require accounting to allow accounting of user activity：ユーザ アクティビティのアカウンティングに関連するパラメータを指定します。
  - Enable：ユーザ　アクティビティのアカウンティングを許可する要求をイネーブルまたはディセーブルにします。
  - Server Group：該当する場合は、ユーザ アカウンティングに使用する選択済みサーバ グループを指定します。TACACS+ サーバ グループが存在しない場合、このリストのデフォルト値は --None-- です。

（注）　サーバ グループ リスト パラメータの定義は、このペインのすべてのグループ ボックスで同じです。

- Require accounting for the following types of connections : アカウンティングを必要とする接続タイプと、それぞれのサーバ グループを指定します。
  - HTTP/ASDM：HTTP/ASDM 接続のアカウンティングを要求します。
  - Serial：シリアル接続のアカウンティングを要求します。
  - SSH：Secure Shell（SSH; セキュア シェル）接続のアカウンティングを要求します。
  - Telnet：Telnet 接続のアカウンティングを要求します。
- Require command accounting for *Security Appliance*：CLI で **show** 以外のコマンドを入力したときに、アカウンティング メッセージを TACACS+ アカウンティング サーバに送信できます。Configuration > Device Access > AAA Access > Authorization > Command Privilege Setup ダイアログボックスを使用してコマンド特権レベルをカスタマイズする場合、最小の特権レベルを指定することにより、セキュリティ アプライアンスがアカウンティングするコマンドを制限できます。セキュリティ アプライアンスは、最小の特権レベル未満のコマンドはアカウンティングしません。
  - Enable：コマンドのアカウンティングをイネーブルにします。
  - Privilege level：コマンド アカウンティングを実行する最小の特権レベルを設定します。

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
•	•	•	•	—

HTTPS/ASDM

Configure > Device Access > HTTPS/ASDM

HTTPS/ASDM ペインには、HTTPS を使用した ASDM へのアクセスを許可するすべてのホストまたはネットワークのアドレスを指定するテーブルが用意されています。このテーブルを使用して、アクセスを許可するホストやネットワークを追加または変更できます。

フィールド

- Interface：デバイス マネージャへの管理アクセスを許可するアクセス元のセキュリティ アプライアンス上のインターフェイスを一覧表示します。
- IP Address：アクセスを許可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。
- Add：新しいホストまたはネットワークを追加するための Add HTTP Configuration ダイアログボックスを表示します。
- Edit：選択したホストまたはネットワークを編集するための Edit HTTP Configuration ダイアログボックスを表示します。
- Delete：選択したホストまたはネットワークを削除します。

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 HTTP Configuration

Configure > Device Access > HTTPS/ASDM > Add/Edit HTTP Configuration

Add/Edit HTTP Configuration ダイアログボックスでは、HTTPS でのセキュリティ アプライアンス デバイス マネージャへの管理アクセスが許可されるホストまたはネットワークを追加できます。

フィールド

- Interface Name：セキュリティ アプライアンス デバイス マネージャへの管理アクセスを許可するアクセス元のセキュリティ アプライアンス上のインターフェイスを指定します。
- IP Address：アクセスを許可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。
- 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。

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 Shell

Configuration > Device Access > HTTPS/ASDM > Secure Shell

Secure Shell ペインでは、特定のホストまたはネットワークが、SSH プロトコルを使用して、管理アクセスのためにセキュリティ アプライアンスへ接続することだけを許可するルールを設定できます。ルールでは、特定の IP アドレスおよびネットマスクへの SSH アクセスが制限されます。ルールに準拠した SSH 接続試行は、次に AAA サーバまたは Telnet パスワードによって認証される必要があります。

SSH セッションは、Monitoring > Administration > Secure Shell Sessions を使用して監視できます。

フィールド

Secure Shell ペインでは、次のフィールドが表示されます。

- Allowed SSH Versions：セキュリティ アプライアンスが受け入れる SSH のバージョンを制限します。デフォルトでは、SSH バージョン 1 および SSH バージョン 2 接続が受け入れられます。
- Timeout (minutes)：セキュリティ アプライアンスが SSH セッションを閉じる前にアイドルでいられる分数を 1 ～ 60 で表示します。デフォルトは 5 分です。
- SSH Access Rule：SSH を使用したセキュリティ アプライアンスへのアクセスが許可されるホストおよびネットワークを表示します。このテーブルの行をダブルクリックすると、選択したエントリを対象とした Edit SSH Configuration ダイアログボックスが開きます。
  - Interface：SSH 接続を許可するセキュリティ アプライアンスのインターフェイスの名前が表示されます。
  - IP Address：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスを表示します。
  - Mask：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスのネットマスクを表示します。
- Add：Add SSH Configuration ダイアログボックスが開きます。
- Edit：Edit SSH Configuration ダイアログボックスが開きます。
- Delete：選択した SSH アクセス ルールを削除します。

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 SSH Configuration

Configuration > Device Access > HTTPS/ASDM > Secure Shell > Add/Edit SSH Configuration

Add SSH Configuration ダイアログボックスでは、新しい SSH アクセス ルールをルール テーブルに追加できます。Edit SSH Configuration ダイアログボックスでは、既存のルールを変更できます。

フィールド

- Interface : SSH 接続を許可するセキュリティ アプライアンス インターフェイスの名前を指定します。
- IP Address : セキュリティ アプライアンスとの SSH 接続の確立が許可されるホストまたはネットワークの IP アドレスを指定します。
- Mask : セキュリティ アプライアンスとの SSH 接続の確立が許可されるホストまたはネットワークのネットマスクです。

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
•	•	•	•	—

Telnet

Configuration > Device Access > Telnet

Telnet ペインでは、ASDM を実行している特定のホストまたはネットワークだけが Telnet プロトコルを使用してセキュリティ アプライアンスに接続できるルールを設定します。

ルールでは、セキュリティ アプライアンス インターフェイスを介した特定の IP アドレスおよびネットマスクへの管理 Telnet アクセスが制限されます。ルールに準拠した接続試行は、事前設定された AAA サーバまたは Telnet パスワードによって認証される必要があります。Telnet セッションは、Monitoring > Telnet Sessions を使用して監視できます。

（注） コンフィギュレーション ファイルには 5 つ以上の Telnet セッションが含まれますが、シングルコンテキスト モードで同時にアクティブになれるのは 5 つまでです。マルチコンテキスト モードでは、コンテキストごとに 5 つの Telnet セッションのみアクティブになれます。

フィールド

Telnet ペインには、次のフィールドが表示されます。

Telnet Rule Table：

- Interface：Telnet 接続を許可するセキュリティ アプライアンス インターフェイス（ASDM を実行している PC またはワークステーションがあるインターフェイス）の名前を表示します。
- IP Address：指定したインターフェイスを介してこのセキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスを表示します。

（注） これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

- Netmask：指定したインターフェイスを介してこの セキュリティ アプライアンスへの接続が許可されている各ホストまたはネットワークの IP アドレスのネットマスクを表示します。

（注） これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

- Timeout：セキュリティ アプライアンスが Telnet セッションを閉じる前にアイドルでいられる分数を 1 ～ 60 で表示します。デフォルトは 5 分です。
- Add：Add Telnet Configuration ダイアログボックスが開きます。
- Edit：Edit Telnet Configuration ダイアログボックスが開きます。
- Delete：選択した項目を削除します。
- Apply：ASDM での変更内容をセキュリティ アプライアンスに送信し、実行中のコンフィギュレーションに適用します。実行中のコンフィギュレーションのコピーをフラッシュ メモリに書き込むには、Save をクリックします。実行中の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、またはフェールオーバー スタンバイ装置に書き込むには、***File*** メニューを使用します。
- Reset：変更内容を破棄し、変更前に表示されていた情報、または ***Refresh*** か ***Apply*** を最後にクリックしたときに表示されていた情報に戻します。Reset をクリックした後は、Refresh を使用して、現在実行中のコンフィギュレーションの情報が表示されていることを確認します。

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
•	•	•	•	—

Add/Edit Telnet Configuration

Configuration > Device Access > Telnet > Add/Edit Telnet Configuration

Telnet ルールの追加

Telnet ルール テーブルにルールを追加するには、次の手順を実行します。

1. **Add** ボタンをクリックし、**Telnet** > **Add** ダイアログボックスを開きます。
2. **Interface** をクリックし、セキュリティ アプライアンス インターフェイスをルール テーブルに追加します。
3. IP Address ボックスに、このセキュリティ アプライアンス インターフェイスを介した Telnet アクセスが許可される、ASDM を実行中のホストの IP アドレスを入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

4. Mask リストで、Telnet アクセスを許可する IP アドレスのネットマスクを選択または入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスのマスクではありません。

5. 前のペインに戻るには、次のいずれかをクリックします。

- **OK**：変更内容を受け入れて、前のペインに戻ります。
- **Cancel**：変更内容を破棄して、前のペインに戻ります。
- **Help**：詳細情報が表示されます。

Telnet ルールの編集

Telnet ルール テーブルのルールを編集するには、次の手順を実行します。

1. **Edit** をクリックし、Telnet > Edit ダイアログボックスを開きます。
2. **Interface** をクリックし、ルール テーブルからセキュリティ アプライアンス インターフェイスを選択します。
3. IP Address フィールドに、このセキュリティ アプライアンス インターフェイスを介した Telnet アクセスが許可される、ASDM を実行中のホストの IP アドレスを入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスではありません。

4. Mask リストで、Telnet アクセスを許可する IP アドレスのネットマスクを選択または入力します。

（注）　これは、セキュリティ アプライアンス インターフェイスの IP アドレスのマスクではありません。

5. 前のウィンドウに戻るには、次のボタンのうちいずれかをクリックします。

- **OK**：変更内容を受け入れて、前のペインに戻ります。
- **Cancel**：変更内容を破棄して、前のペインに戻ります。
- **Help**：詳細情報が表示されます。

Telnet ルールの削除

Telnet テーブルからルールを削除するには、次の手順を実行します。

1. Telnet ルール テーブルからルールを選択します。
2. **Delete** をクリックします。

変更内容の適用

Add、Edit、または Delete を使用してテーブルを変更した内容は、実行中のコンフィギュレーションにただちに適用されるわけではありません。変更内容を適用または破棄するには、次のいずれかのボタンをクリックします。

1. **Apply**：ASDM での変更内容をセキュリティ アプライアンスに送信し、実行中のコンフィギュレーションに適用します。実行中のコンフィギュレーションのコピーをフラッシュ メモリに書き込むには、**Save** をクリックします。実行中の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、またはフェールオーバー スタンバイ装置に書き込むには、**File** メニューを使用します。
2. **Reset**：変更内容を破棄し、変更前に表示されていた情報、または **Refresh** か **Apply** を最後にクリックしたときに表示されていた情報に戻します。Reset をクリックした後は、**Refresh** を使用して、現在実行中のコンフィギュレーションの情報が表示されていることを確認します。

フィールド

- Interface Name：セキュリティ アプライアンスへの Telnet アクセスを許可するインターフェイスを選択します。
- IP Address：セキュリティ アプライアンスへの Telnet が許可されたホストまたはネットワークの IP アドレスを入力します。
- Mask：セキュリティ アプライアンスへの Telnet が許可されたホストまたはネットワークのサブネット マスクを入力します。
- OK：変更内容を受け入れて、前のペインに戻ります。
- Cancel：変更内容を破棄して、前のペインに戻ります。
- 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
•	•	•	•	—

Virtual Access

Configuration > Properties > Device Access > Virtual Access

Virtual Access ペインでは、セキュリティ アプライアンスの仮想 Telnet サーバ アドレスをネットワーク アクセス認証に使用するように設定します。

ネットワーク アクセス認証はあらゆるプロトコルまたはサービスに設定できますが、認証チャレンジは HTTP、Telnet、FTP でのみ提供されます。認証を必要とする他のトラフィックが許可される前に、ユーザはまずこれらのサービスの 1 つを認証する必要があります。

一部のケースでは、セキュリティ アプライアンスを介した HTTP、Telnet、または FTP を許可しない場合もありますが、その場合でもトラフィックの他のタイプを認証する必要があります。その場合は、セキュリティ アプライアンス上に仮想 Telnet サーバを作成します。ユーザが Telnet を使用してセキュリティ アプライアンスを仮想 Telnet IP アドレスに接続すると、セキュリティ アプライアンスは Telnet プロンプトを表示します。認証が済んでいないユーザが仮想 Telnet IP アドレスに接続すると、ユーザはユーザ名とパスワードを尋ねられ、その後 AAA サーバにより認証されます。いったん認証されると、ユーザには「Authentication Successful.」メッセージが表示されます。その後ユーザは認証を必要とする他のサービスにアクセスできます。

セキュリティ アプライアンスからログアウトするには、仮想 IP アドレスに再接続します。ログアウトを尋ねるプロンプトが表示されます。

フィールド

- Virtual Telnet Server：仮想 Telnet サーバ IP アドレスを入力します。

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
•	•	•	•	—