



ASAv の設定

ASAv の導入により、ASDM アクセスが事前設定されます。導入時に指定したクライアント IP アドレスから、Web ブラウザで ASAv 管理 IP アドレスに接続できます。この章では、他のクライアントが ASDM にアクセスできるようにする方法と CLI アクセスを許可する方法 (SSH または Telnet) についても説明します。この章で取り上げるその他の必須の設定作業には、ASDM でウィザードが提供するライセンスのインストールおよび一般的な設定作業が含まれます。

- [ASDM の開始\(61 ページ \)](#)
- [ASDM を使用した初期設定の実行\(62 ページ \)](#)
- [高度な設定\(63 ページ \)](#)

ASDM の開始

手順

1. ASDM クライアントとして指定した PC で次の URL を入力します。

https://asa_ip_address/admin

次のボタンを持つ ASDM 起動ページが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

2. ランチャをダウンロードするには、次の手順を実行します。

- a. [Install ASDM Launcher and Run ASDM] をクリックします。
- b. ユーザ名とパスワードのフィールドを空のままにし (新規インストールの場合) [OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名および **イネーブル** パスワード (デフォルトで空白) を入力しないで ASDM にアクセスできます。注: HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。
- c. インストーラを PC に保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
- d. 管理 IP アドレスを入力し、ユーザ名とパスワードを空白のままにし (新規インストールの場合) [OK] をクリックします。注: HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

3. Java Web Start を使用するには:

- a. [Run ASDM] または [Run Startup Wizard] をクリックします。
- b. プロンプトが表示されたら、ショートカットを PC に保存します。オプションで、アプリケーションを保存せずに開くこともできます。
- c. ショートカットから Java Web Start を起動します。
- d. 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。
- e. ユーザ名とパスワードを空白のままにし (新規インストールの場合) [OK] をクリックします。注: HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。

ASDM を使用した初期設定の実行

次の ASDM ウィザードおよび手順を使用して初期設定を行うことができます。CLI の設定については、CLI コンフィギュレーション ガイドを参照してください。

- [Startup Wizard の実行 \(62 ページ\)](#)
- [\(オプション\)ASAv の背後のパブリック サーバへのアクセス許可 \(62 ページ\)](#)
- [\(オプション\)VPN ウィザードの実行 \(62 ページ\)](#)
- [\(オプション\)ASDM の他のウィザードの実行 \(63 ページ\)](#)

Startup Wizard の実行

導入環境に応じてセキュリティ ポリシーをカスタマイズできるように、**Startup Wizard** ([Wizards] > [Startup Wizard]) を選択して実行します。Startup Wizard を使用して、次の項目を設定できます。

- ホスト名
- ドメイン名
- 管理パスワード
- インターフェイス
- IP アドレス
- スタティック ルート
- DHCP サーバ
- ネットワーク アドレス変換規則
- その他

(オプション)ASAv の背後のパブリック サーバへのアクセス許可

[Configuration] > [Firewall] > [Public Servers] ペインでは、インターネットから内部サーバにアクセスできるようにするためのセキュリティ ポリシーが自動的に設定されます。ビジネス オーナーとして、内部ネットワーク サービス(Web サーバや FTP サーバなど)に外部ユーザがアクセスできるようにする必要がある場合があります。これらのサービスは、ASAv の背後にある、Demilitarized Zone(DMZ; 非武装地帯)と呼ばれる別のネットワーク上に配置できます。DMZ にパブリック サーバを配置すると、パブリック サーバに対する攻撃は内部ネットワークには影響しません。

(オプション)VPN ウィザードの実行

次のウィザード ([Wizards] > [VPN Wizards]) を使用して、VPN を設定できます。

- **Site-to-Site VPN Wizard:** 2 台の ASAv 間で、IPsec サイト間トンネルを作成します。
- **AnyConnect VPN Wizard:** Cisco AnyConnect VPN クライアントに対する SSL VPN リモート アクセスを設定します。AnyConnect は ASA へのセキュアな SSL 接続を提供し、これにより、リモート ユーザによる企業リソースへのフル VPN トンネリングが可能となります。ASA ポリシーは、リモート ユーザがブラウザを使用して最初に接続するときに、AnyConnect クライアントをダウンロードするように設定できます。AnyConnect 3.0 以降を使用する場合、クライアントは、SSL または IPsec IKEv2 VPN プロトコルを実行できます。
- **Clientless SSL VPN Wizard:** ブラウザにクライアントレス SSL VPN リモート アクセスを設定します。クライアントレス ブラウザベース SSL VPN によって、ユーザはブラウザを使用して ASA へのセキュアなリモート アクセス VPN トンネルを確立できます。認証されると、ユーザにはポータル ページが表示され、サポートされる特定の内部リソースにアクセスできるようになります。ネットワーク管理者は、グループ単位でユーザにリソースへのアクセス権限を付与します。ACL は、特定の企業リソースへのアクセスを制限したり、許可するために適用できます。
- **IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard:** Cisco IPsec クライアント用の IPsec VPN リモート アクセスを設定します。

(オプション) ASDM の他のウィザードの実行

- High Availability and Scalability Wizard: フェールオーバーまたは VPN ロード バランシングを設定します。
- Packet Capture Wizard: パケット キャプチャを設定し、実行します。このウィザードは、入出力インターフェイスのそれぞれでパケット キャプチャを 1 回実行します。パケットをキャプチャすると、PC にパケット キャプチャを保存し、パケット アナライザでチェックおよびリプレイできます。

高度な設定

ASAv の設定を続行するには、『[Navigating the Cisco ASA Series Documentation](#)』を参照してください。

