

ESA/SMA/WSA を工場出荷時のデフォルト設定にリセットする

目次

[はじめに](#)

[ESA/SMA/WSA を工場出荷時のデフォルト設定にリセットする](#)

[ESA/SMA](#)

[WSA](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco E メール セキュリティ アプライアンス (ESA)、Cisco セキュリティ管理アプライアンス (SMA)、または Cisco Web セキュリティ アプライアンス (WSA) を工場出荷時のデフォルト設定にリセットする方法を説明します。

ESA/SMA/WSA を工場出荷時のデフォルト設定にリセットする

場合によっては、お客様からアプライアンスを工場出荷時のデフォルト設定にリセットするよう依頼されることがあります。通常、これはアプライアンスの評価が完了した後に要求されるか、お客様が交換済みのアプライアンスを返品許可(RMA)またはアップグレードの理由で返品します。したがって、お客様の情報をすべて削除するために、アプライアンスを工場出荷時のデフォルト設定にリセットすることを依頼される可能性があります。

注意：このドキュメントで説明するコマンドは、すべてのネットワーク設定を工場出荷時の初期状態に戻します。これにより、CLI からの接続が解除され、アプライアンスへの接続に使用していたサービス (File Transfer Protocol (FTP)、Telnet、セキュア シェル (SSH)、HTTP、HTTPS など) が無効になり、userconfig コマンドを使用して作成した追加のユーザ アカウントが削除される可能性があります。これらのコマンドは、シリアル インターフェイスを使用するか、またはデフォルトの Admin ユーザ アカウントから管理ポート上のデフォルト設定を使用して CLI に再接続できない場合は使用しないでください。

これらのコマンドを使用すると、AsyncOS の使用可能なすべてのバージョンも削除されますが、revert コマンドを使用して AsyncOS にアクセスできる可能性があります。残っている AsyncOS の唯一のバージョンは、現在実行されているリビジョンです。**重要：**revert コマンドは、アプライアンスからすべてをワイプします。ESA の REVERT コマンドは、アプライアンスを以前のバージョンの AsyncOS に戻します。

警告：アプライアンスを元に戻すことは非常に破壊的です。

このデータはプロセスで破棄されます。

- すべての構成設定 (リスナーを含む)
- すべてのログファイル
- すべてのデータベース (ウイルスアウトブレイクおよびポリシー検査のメッセージを含む)
- すべてのレポートデータ (保存済みの定期レポートを含む)
- すべてのメッセージトラッキングデータ

- すべてのIronPortスパム検疫メッセージとエンドユーザセーフリスト/ブロックリストデータ

ネットワーク設定だけが保持されます。

このコマンドを実行する前に、次のことを確認してください。

- このアプライアンスの設定ファイルを保存しました (パスワードはマスクされません)
- IronPortスパム検疫セーフリスト/ブロックリストデータベースを別のマシンにエクスポート (該当する場合)
- メールキューが空になるのを待ちました

デバイスを元に戻すと、すぐにリブートが行われます。リブート後、アプライアンスは自動的に再初期化され、目的のバージョンに再びリブートされます。

注意 : WSA Revertコマンド

このコマンドは、アプライアンスを以前のバージョンのAsyncOSに戻します。

警告 : アプライアンスを元に戻すことは非常に破壊的です。

このデータはプロセスで破棄され、バックアップする必要があります。

- 現在のシステム設定ファイル
- すべてのログファイル
- すべてのレポートデータ (保存されたスケジュール済みレポートとアーカイブ済みレポートを含む)
- カスタムエンドユーザ通知ページ

このコマンドは、現在のネットワーク設定を保持しようとします。

デバイスを元に戻すと、すぐにリブートが行われます。リブート後、アプライアンスは自動的に再初期化され、以前のシステム設定で目的のバージョンに再びリブートされます。

ヒント : 続行する前に、必要に応じて saveconfig または mailconfig コマンドを実行して、現在のアプライアンス設定のコピーを維持しておくことを推奨します。リセットが成功するとアプライアンス設定が削除され、回復できません。

ESA/SMA

Cisco ESA または SMA を元の工場出荷時のデフォルト設定に戻すには、次の手順を実行します。

注 : ネットワーク設定をすべて削除するために systemsetup コマンドを実行する前に、アプライアンスへコンソールからアクセスできるようにしておくことを推奨します。

1. ESA または SMA で diagnostic コマンドを実行し、次に RELOAD 操作を選択します。
2. 続行するかどうかを求められたら Y と入力し、もう一度 Y と入力して処理を完了します。

このプロセスではアプライアンス設定がリセットされ、すべての顧客データ (設定、ログ、

レポート、ユーザ情報など) が削除されます。この時点で、管理者パスワードはデフォルトの *ironport* に戻ります。

```
myesa.local> diagnostic
```

```
Choose the operation you want to perform:
```

```
- RAID - Disk Verify Utility.  
- DISK_USAGE - Check Disk Usage.  
- NETWORK - Network Utilities.  
- REPORTING - Reporting Utilities.  
- TRACKING - Tracking Utilities.  
- RELOAD - Reset configuration to the initial manufacturer values.  
[ ]> RELOAD
```

```
This command will remove all user settings and reset the entire device.
```

```
If this is a Virtual Appliance, all feature keys will be removed,  
and the license must be reapplied.
```

```
Are you sure you want to continue? [N]> y
```

```
Are you *really* sure you want to continue? [N]> y
```

```
Reverting to "testing" preconfigure install mode.
```

この時点でアプライアンスにより現在の接続が閉じられ、アプライアンスが再起動します。

3. ネットワーク設定を削除するには、**systemsetup** コマンドを使用してシステム セットアップ ウィザードを再度実行する必要があります。このウィザードで処理を進め、必要に応じて汎用情報 (管理 IP アドレス *192.168.42.42*、汎用ホスト名、汎用電子メール アドレス *admin@example.com* など) を入力します。

4. セットアップ ウィザードが完了し、変更をコミットするよう求められたら、**Y** と入力します。

```
*****
```

```
Would you like to commit these changes at this time? [Y]> Y
```

```
Congratulations! System setup is complete.
```

この時点で、アプライアンスで以前に設定した設定値はクリアされ、顧客データがアプライアンスから削除されます。

設定が初期の出荷時設定値にリセットされると、ライセンス キーが削除され、*Incoming Mail Handling* の 30 日間デモ キーが復元されます。ESA ハードウェア アプライアンスのライセンス キーは、アプライアンスのシリアル番号に直接関連付けられています。アプライアンスが更新サービスと通信すると、割り当てられた有効な機能キーが呼び出されます。ESA 仮想アプライアンスでは、設定自体に組み込まれている仮想ライセンス番号 (VLN) にライセンス キーが関連付けられているため、これらのライセンス キーが削除されます。仮想アプライアンスでは、**loadlicense** オプションを再実行し、VLN をリロードする必要があります。

注：デモ アプライアンスでこのプロセスを完了する必要があるため、必要な時間が増える場合は、Cisco Global Licensing Operations (GLO) に連絡して、機能拡張または新しいライセンス キーを依頼します。

WSA

Cisco WSA を元の工場出荷時のデフォルト設定に戻すには、次の手順を実行します。

注：ネットワーク設定を削除するために `resetconfig` コマンドまたは `reload` コマンドを実行する前に、アプライアンスへコンソールからアクセスできるようにしておくことを推奨します。

1. アプライアンス CLI から `diagnostic` コマンドを入力し、`[REPORTING] > [DELETEDB]` を選択します。
2. CLI に `resetconfig` コマンドを入力します。

このプロセスでは設定の完全な再インストールが実行されるため、すべての設定が失われます。管理 IP は `192.168.42.42` にリセットされ、管理者パスワードはデフォルトの `ironport` に戻されます。

```
mywsa.local> resetconfig
```

```
Are you sure you want to reset all configuration values? [N]> y
```

```
All settings have been restored to the factory defaults.  
Please run System Setup Wizard at http://192.168.42.42:8080
```

3. ESA では拡張コマンドを入力することもできます。隠しコマンド `reload` を ESA CLI に入力して、`Y` と入力し、次に `YES` と入力して、完了します。このコマンドは、すべての顧客データ (すべての設定、ネットワーク設定、ログ、アーカイブされているスケジュールレポート、ユーザ情報など) を削除します。

```
mywsa.local> reload
```

```
WARNING !!
```

```
This command will erase customer data, reporting and log files,  
erase proxy cache, reset to factory configuration (shipping mode),  
including network settings and IP addresses and reboot the machine.
```

```
This command does NOT extend the feature keys.  
Those must be applied separately.
```

```
If this is a Virtual Appliance, all feature keys will be removed,  
and the license must be reapplied.
```

```
WARNING !!
```

```
This command is primarily intended for Cisco IronPort Field Engineers  
and may delete valuable data. Administrators should normally use  
'resetconfig' instead.
```

```
Are you sure you want to continue? [y|n] y
```

```
Are you *really* sure you want to continue? If so, type 'YES': yes
```

関連情報

- [Cisco E メール セキュリティ アプライアンス - エンド ユーザ ガイド](#)
- [Cisco セキュリティ管理アプライアンス - エンドユーザ ガイド](#)
- [Cisco Web セキュリティ アプライアンス - エンドユーザ ガイド](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)