CHAPTER 8

一般的な管理タスク

Framemaker テンプレートの内容は次のとおりです。

Cisco IronPort アプライアンスの管理

以下のタスクでは、Cisco IronPort アプライアンス内の一般的な機能を簡単に管理できます。次の操作とコマンドについて説明します。

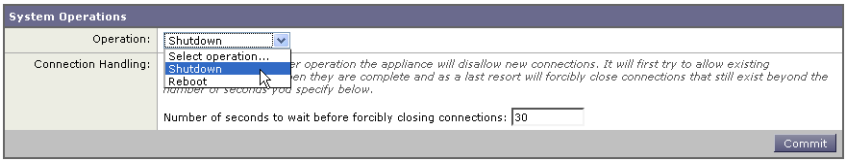
- `shutdown`
- `reboot`
- `suspend`
- `offline`
- `resume`
- `resetconfig`
- `version`
- `updateconfig`
- `upgrade`

Cisco IronPort アプライアンスのシャットダウン

IronPort アプライアンスをシャットダウンするには、GUI の [System Administration] メニューで利用可能な [Shutdown/Suspend] ページを使用するか、CLI で shutdown コマンドを使用します。図 8-1 に、[Shutdown/Suspend] ページを使用してアプライアンスをシャットダウンする方法を示します。

アプライアンスをシャットダウンすると、IronPort AsyncOS が終了し、アプライアンスの電源を安全にオフにできます。アプライアンスは、配信キューのメッセージを失わずに後で再起動できます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルトの遅延値は 30 秒です。IronPort AsyncOS では、その遅延値の間にオープンな接続が完了します。その遅延値を超えると、オープンな接続は強制的に閉じられます。

図 8-1　　GUI によるアプライアンスのシャットダウン

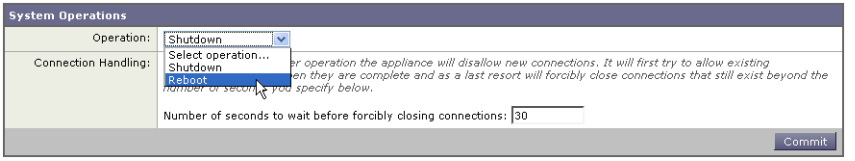


Cisco IronPort アプライアンスのリブート

IronPort アプライアンスをリブートするには、GUI の [System Administration] メニューで利用可能な [Shutdown/Suspend] ページを使用するか、CLI で reboot コマンドを使用します。図 8-2 に、[Shutdown/Suspend] ページを使用してアプライアンスをリブートする方法を示します。

アプライアンスをリブートすると、IronPort AsyncOS が再起動され、アプライアンスの電源を安全にオフにし、アプライアンスをリブートできます。アプライアンスをシャットダウンする遅延値を入力する必要があります。デフォルトの遅延値は 30 秒です。IronPort AsyncOS では、その遅延値の間にオープンな接続が完了します。その遅延値を超えると、オープンな接続は強制的に閉じられます。アプライアンスは、配信キュー内のメッセージを失わずに再起動できます。

図 8-2　GUI を使用したアプライアンスのリブート



IronPort アプライアンスをメンテナンス状態にする

システム メンテナンスを実行する場合は、Cisco IronPort アプライアンスをオフライン状態にする必要があります。suspend コマンドと offline コマンドを実行すると、IronPort AsyncOS オペレーティング システムがオフライン状態になります。オフライン状態の特徴は次のとおりです。

- 着信電子メール接続が許可されません。
- 発信電子メール配信は停止されます。
- ログ転送が停止されます。
- CLI はアクセス可能のままになります。

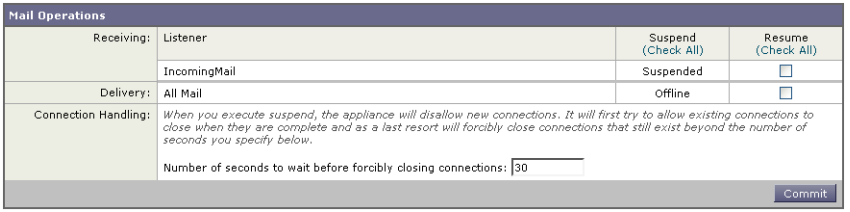
アプライアンスがオフライン状態になる遅延値を入力する必要があります。デフォルトの遅延値は 30 秒です。IronPort AsyncOS では、その遅延値の間にオープンな接続が完了します。その遅延値を超えると、オープンな接続は強制的に閉じられます。オープンな接続がない場合は、すぐにオフライン状態になります。

（注）suspend コマンドと offline コマンドの違いは、suspend コマンドはマシンのリブート後でもその状態を保持することです。suspend コマンドを発行し、アプライアンスをリブートする場合は、resume コマンドを使用してシステムをオンライン状態に戻す必要があります。

GUI で [System Administration] > [Shutdown/Suspend] ページを使用して、アプライアンスでの電子メールの送受信を中断できます。アプライアンスに複数のリスナーが存在する場合は、個々のリスナーに対して電子メールの受信を中断および再開できます。電子メールの送受信を中断するために、[Commit] をクリックします。

図 8-3 に、電子メールの送受信が中断された電子メール セキュリティ アプライアンスの例を示します。

図 8-3　アプライアンスで中断された電子メールの処理



suspend コマンドと offline コマンド

```
mail3.example.com> suspend


Enter the number of seconds to wait before abruptly closing
connections.

[30]> 45


Waiting for listeners to exit...

Receiving suspended.

Waiting for outgoing deliveries to finish...

Mail delivery suspended.


mail3.example.com> offline


Enter the number of seconds to wait before abruptly closing
connections.

[30]> 45
```

```
Waiting for listeners to exit...

Receiving suspended.

Waiting for outgoing deliveries to finish...

Mail delivery suspended.
```

オフライン状態からの再開

AsyncOS CLI で resume コマンドを実行すると、IronPort AsyncOS オペレーティング システム（suspenddel または suspend コマンドの使用後）が通常の動作状態に戻ります。

また、GUI で [System Administration] > [Shutdown/Suspend] ページを使用して、アプライアンスでの電子メールの送受信を再開できます。アプライアンスに複数のリスナーが存在する場合は、個々のリスナーに対して電子メールの受信を再開できます。電子メールの送受信を再開するために、[Commit] をクリックします。

resume コマンド

```
mail3.example.com> resume


Receiving resumed.

Mail delivery resumed.

mail3.example.com>
```

出荷時デフォルト値へのリセット

物理的にアプライアンスを移動したときに、出荷時デフォルト値に戻したい場合があります。[System Administration] > [Configuration File] ページの [Reset Configuration] セクションまたは resetconfig コマンドを使用すると、すべての

IronPort AsyncOS の設定値が出荷時デフォルト値にリセットされます。このコマンドは非常に破壊的であるため、ユニットを移動する場合や、設定の問題を解決する最後の手段としてのみ使用してください。設定のリセット後にシステム設定ウィザードまたは systemsetup コマンドを実行することが推奨されます。

FIPS 準拠のアプライアンスの場合、HSM カードにある既存のすべての秘密キーは、そのペアの証明書が削除されるために孤立します。resetconfig コマンドを実行する前に fipsconfig -> init コマンドを実行することが推奨されます。

（注） resetconfig コマンドは、アプライアンスがオフライン状態にあるときにのみ動作します。resetconfig コマンドが完了すると、systemsetup コマンドを再び実行する前であってもアプライアンスがオフライン状態に戻ります。resetconfig コマンドを実行する前に電子メールの送信が中断された場合は、resetconfig コマンドが完了したときに電子メールの送信が再試行されます。

警告 **resetconfig コマンドを実行すると、すべてのネットワーク設定が出荷時デフォルト値に戻ります。場合によっては、CLI から切断され、アプライアンスに接続するために使用したサービス（FTP、Telnet、SSH、HTTP、HTTPS）がディセーブルにされ、userconfig コマンドで作成した追加のユーザ アカウントが削除されます。このコマンドは、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。**

resetconfig コマンド

```
mail3.example.com> offline


Delay (seconds, minimum 30):

[30]> 45


Waiting for listeners to exit...

Receiving suspended.

Waiting for outgoing deliveries to finish...

Mail delivery suspended.


mail3.example.com> resetconfig


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


All settings have been restored to the factory default.
```

AsyncOS のバージョン情報の表示

Cisco IronPort アプライアンスに現在インストールされている AsyncOS のバージョンを確認するには、GUI の [Monitor] メニューから [System Overview] ページを使用するか（「[System Status]」（P.2-67）を参照）、CLI で `version` コマンドを使用します。

サポート コマンド

アプライアンスをアップグレードする場合やサポート プロバイダーに連絡する場合に役に立つコマンドと機能は次のとおりです。

- テクニカル サポート（[Support Request] ページと [Remote Access] ページ）
- 機能キー

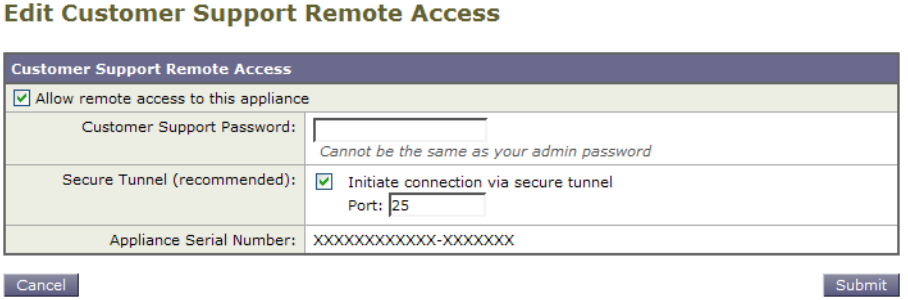
テクニカル サポート

[System Administration] メニューの [Technical Support] セクションには、[Support Request] と [Remote Access] の 2 つのページが含まれます。

リモート アクセス

IronPort アプライアンスへの IronPort カスタマー サポート リモート アクセスを許可するには、[Remote Access] ページを使用します。

図 8-4　[Remote Access] ページ



リモート アクセスをイネーブルにすると、デバッグとシステムへの一般的なアクセスのための、IronPort カスタマー サポートにより使用される特別なアカウントが有効になります。これは、IronPort カスタマー サポートにより、顧客がシステムを設定したり、設定を理解したり、障害レポートを調査したりするのを支援するために使用されます。また、CLI で `techsupport` コマンドを使用することもできます。

「セキュアなトンネル」の使用をイネーブルにすると、アプライアンスにより指定済みポートを介してサーバ upgrades.ironport.com への SSH トンネルが作成されます。デフォルトでは、この接続はポート 25 を介します（システムでは電子メール メッセージを送信するためにこのポートを介して一般的なアクセスが必要になるため、このポートの使用はほとんどの環境で問題ありません）。upgrades.ironport.com への接続が確立されたら、IronPort カスタマー サポートは SSH トンネルを使用してアプライアンスへのアクセスを取得できます。ポート 25 を介した接続が許可される限り、ほとんどのファイアウォールの制限は適用されません。また、CLI で techsupport tunnel コマンドを使用することもできます。

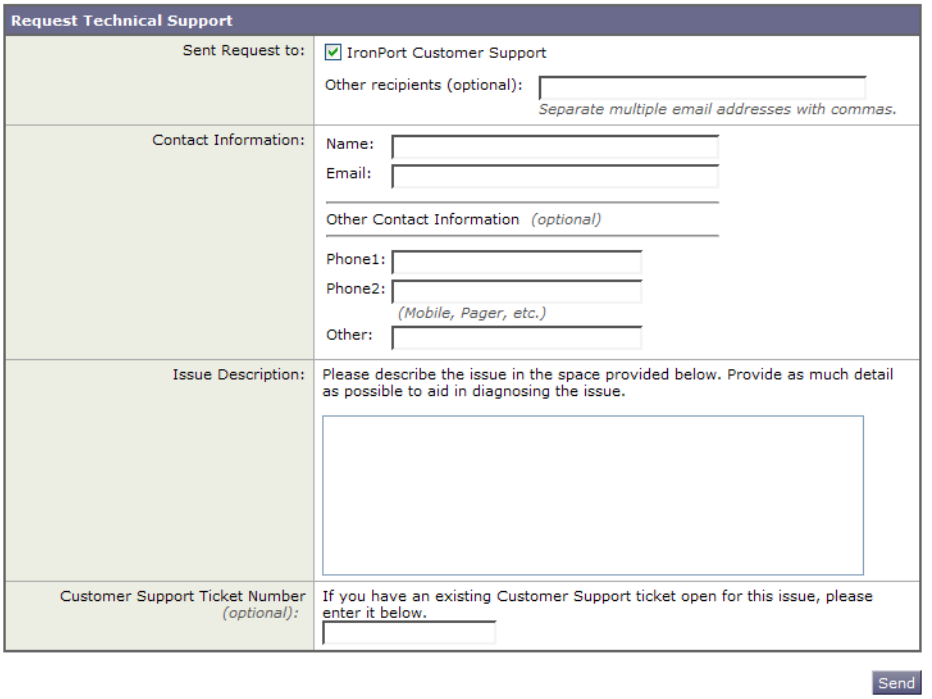
「リモート アクセス」と「トンネル」の両方のモードでは、パスワードが必要です。これはシステムにアクセスするために使用されるパスワード *ではない* ことを理解することが重要です。パスワードとシステムのシリアル番号がカスタマー サポート担当者に提供された後で、プライアンスにアクセスするために使用されるパスワードが生成されます。

techsupport トンネルがイネーブルになると、upgrades.ironport.com に 7 日間接続されたままになります。7 日間後に、確立された接続は切断されませんが、いったん切断されるとトンネルに再接続できません。SSH トンネル接続に設定されたタイムアウトはリモート アクセス アカウントに適用されません。リモート アクセス アカウントは特に非アクティブ化するまではアクティブです。

サポート要求

[Help] > [Support Request] ページまたは supportrequest コマンド（supportrequest コマンドの詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください）を使用すると、アプライアンスの設定を IronPort カスタマー サポート チームや追加ユーザに電子メールで送信したり、サポートが必要な問題に関するコメントを入力したりできます。このコマンドを使用するには、アプライアンスがインターネットに電子メールを送信できる必要があります。

図 8-5　[Support Request] ページ



ステップ 1　連絡先情報（名前、電子メール アドレス、電話番号など）を入力します。

ステップ 2　問題の内容を入力します。

ステップ 3　デフォルトでは、サポート要求（コンフィギュレーション ファイルを含む）は IronPort カスタマー サポートに送信されます（フォーム上部のチェックボックスを使用）。また、他の電子メール アドレス（複数のアドレスはカンマで区切ります）にコンフィギュレーション ファイルを電子メールで送信することもできます。

ステップ 4　この問題に関するカスタマー サポート チケットをすでに持っている場合は、それを入力してください。

ステップ 5　[Send] をクリックします。

ステップ 6　トラブル チケットが作成されます。詳細については、「IronPort Customer Support」（P.1-7）を参照してください。

パケット キャプチャ

場合によっては、問題発生時に IronPort カスタマー サポートに問い合わせたときに、電子メール セキュリティ アプライアンスとのネットワーク状況について尋ねられることがあります。アプライアンスでは、アプライアンスが接続されたネットワークで送受信されている TCP/IP と他のパケットを傍受および表示できます。

パケット キャプチャを実行すると、ネットワーク設定をデバッグしたり、アプライアンスに到達しているネットワーク トラフィックやアプライアンスから送信されているネットワーク トラフィックを確認したりできます。

アプライアンスはキャプチャされたパケットの状態をファイルに保存し、ファイルをローカルで保持します。パケット キャプチャ ファイルの最大サイズ、パケット キャプチャの実行時間、およびキャプチャを実行するネットワーク インターフェイスを設定できます。また、フィルタを使用して、特定のポートからのトラフィックや特定のクライアントまたはサーバの IP アドレスからのトラフィックにパケット キャプチャを制限することもできます。

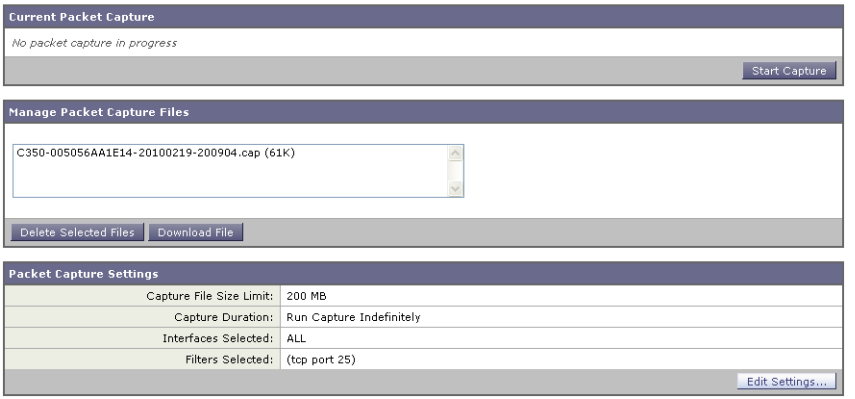
GUI の [Support and Help] > [Packet Capture] ページには、ハード ドライブに格納された完全なパケット キャプチャ ファイルの一覧が表示されます。パケット キャプチャが実行されている場合、[Packet Capture] ページには、実行中のキャプチャのステータス（ファイル サイズや経過時間などの現在の統計情報）が表示されます。

パケット キャプチャ ファイルは [Download File] ボタンを使用してダウンロードし、デバッグやトラブルシューティングのために IronPort カスタマー サポートに電子メールで送信できます。また、1 つまたは複数のファイルを選択し、[Delete Selected Files] をクリックすることにより、パケット キャプチャ ファイルを削除することもできます。

CLI で、`packetcapture` コマンドを使用します。

図 8-6 に、GUI の [Packet Capture] ページを示します。

図 8-6　[Packet Capture] ページ



（注）　パケット キャプチャ機能は UNIX の tcpdump コマンドに似ています。

パケット キャプチャの開始

CLI でパケット キャプチャを開始するには、`packetcapture` > `start` コマンドを実行します。実行されているパケット キャプチャを停止する必要がある場合は、`packetcapture` > `stop` コマンドを実行します。アプライアンスで、セッション終了時にパケット キャプチャが停止します。

GUI でパケット キャプチャを開始するには、[Support and Help] メニューの [Packet Capture] オプションを選択し、[Start Capture] をクリックします。実行されているキャプチャを停止するには、[Stop Capture] をクリックします。GUI で開始されたキャプチャはセッション間で維持されます。

（注）　GUI に表示されるのは GUI で開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。キャプチャは一度に 1 つだけ実行できます。

パケット キャプチャ設定の編集

CLI でパケット キャプチャ設定を編集するには、`packetcapture` > `setup` コマンドを実行します。

GUI でパケット キャプチャ設定を編集するには、[Support and Help] メニューの [Packet Capture] オプションを選択し、[Edit Settings] をクリックします。

表 8-1 に、設定可能なパケット キャプチャの項目を示します。

表 8-1　パケット キャプチャ設定オプション

オプション	説明
[Capture file size limit]	すべてのパケット キャプチャ ファイルの最大ファイル サイズ（メガバイト単位）。

表 8-1　パケット キャプチャ設定オプション（続き）

オプション	説明
[Capture Duration]	パケット キャプチャの実行時間を選択します。 • [Run Capture Until File Size Limit Reached]。パケット キャプチャは、ファイル サイズ制限に到達するまで実行されます。 • [Run Capture Until Time Elapsed Reaches]。パケット キャプチャは、設定された時間が経過するまで実行されます。時間は秒単位（s）、分単位（m）、または時間単位（h）で入力できます。単位を指定せずに時間を入力すると、AsyncOS ではデフォルトで秒単位が使用されます。このオプションは GUI でのみ使用できます。 （注）　パケット キャプチャ ファイルは 10 個の部分に分割されます。全体の時間が経過する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャ データで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。 • [Run Capture Indefinitely]。パケット キャプチャは、手動で停止するまで実行されます。 （注）　手動でパケット キャプチャを停止する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャ データで新しい部分が開始されます。 パケット キャプチャはいつでも手動で停止できます。

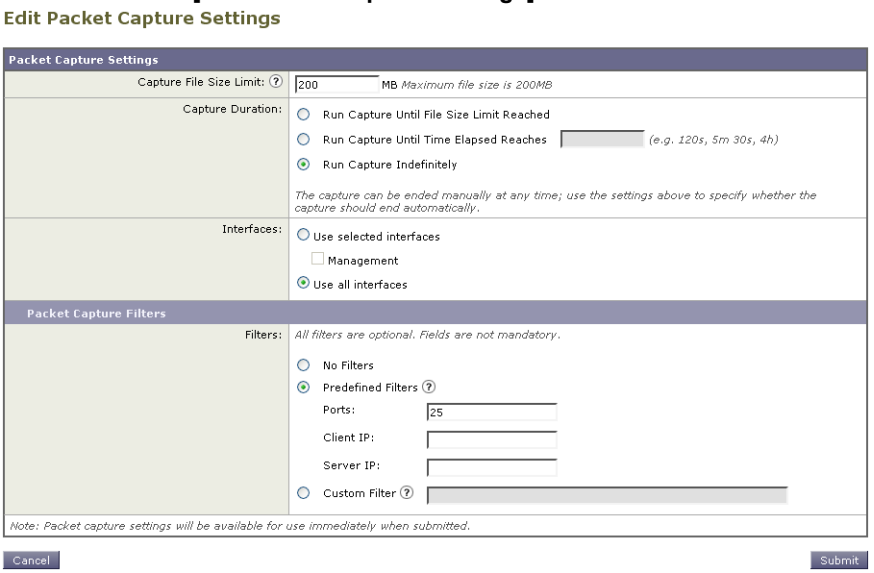
表 8-1　パケット キャプチャ設定オプション（続き）

オプション	説明
[Interface]	パケット キャプチャを実行するネットワーク インターフェイスを選択します。
[Filters]	パケット キャプチャで保存されるデータの量を削減するために、パケット キャプチャにフィルタを適用するかどうかを選択します。 事前定義されたフィルタを使用してポート、クライアント IP、またはサーバ IP でフィルタリングしたり（GUI のみ）、UNIX の tcpdump コマンドでサポートされた構文（`host 10.10.10.10 && port 80` など）を使用してカスタム フィルタを作成したりできます。

AsyncOS は新しいパケット キャプチャ設定を使用します（これらを送信後）。変更を保存する必要はありません。

図 8-7 に、GUI でパケット キャプチャ設定を編集する例を示します。

図 8-7　[Edit Packet Capture Settings] ページ



機能キーの使用

場合によっては、サポート チームが、システムで特定の機能をイネーブルにするキーを提供することがあります。GUI で [System Administration] > [Feature Keys] ページ（または CLI で `featurekey` コマンド）を使用し、キーを入力して、関連付けられた機能をイネーブルにします。

キーはアプライアンスのシリアル番号とイネーブルにされる機能に固有です（あるシステムのキーを別のシステムで再使用することはできません）。キーを間違って入力した場合は、エラー メッセージが生成されます。

機能キーの機能は [Feature Keys] と [Feature Key Settings] の 2 つのページに分割されます。

[Feature Keys] ページ

GUI にログインし、[System Administration] タブをクリックします（GUI へのアクセス方法については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Overview」の章を参照してください）。左側のメニューの [Feature Keys] リンクをクリックします。[Feature Keys] ページの内容は次のとおりです。

- アプライアンスのすべてのアクティブな機能キーが表示されます。
- アクティベーション待ちのすべての機能キーが表示されます。
- 発行された新しいキーを検索できます（これは任意であり、キーをインストールすることもできます）。

現在イネーブルな機能の一覧が表示されます。[Pending Activation] セクションは、アプライアンスに対して発行され、まだアクティベートされていない機能キーの一覧です。設定に応じてアプライアンスが新しいキーを定期的に確認することがあります。[Check for New Keys] ボタンをクリックすると、待機状態のキーの一覧が更新されます。

機能キーの設定

[Feature Key Settings] ページは、新しい機能キーを確認およびダウンロードするかどうかや、これらのキーを自動的にアクティベートするかどうかを制御するために使用します。

図 8-8　[Feature Key Settings] ページ

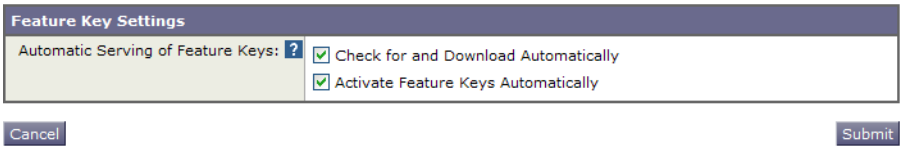
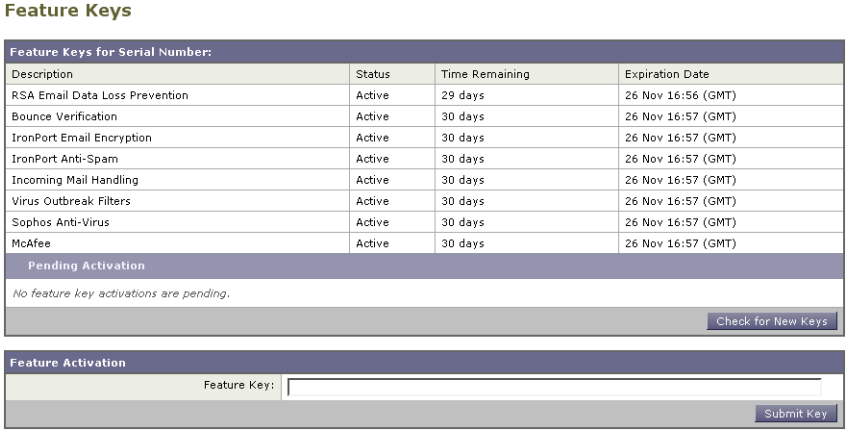


図 8-9　[Feature Keys] ページ



新しい機能キーを手動で追加するには、[Feature Key] フィールドにキーを貼り付けるか、または入力し、[Submit Key] をクリックします。機能が追加されない場合は、エラー メッセージが表示されます（キーが正しくない場合など）。それ以外の場合は、機能キーが画面に追加されます。

[Pending Activation] 一覧の新しい機能キーをアクティベートするには、そのキーを選択し（[Select] チェックボックスをオンにします）、[Activate Selected Keys] をクリックします。

新しいキーが発行されたときにキーを自動的にダウンロードおよびインストールするよう IronPort アプライアンスを設定できます。この場合、[Pending Activation] 一覧は常に空白になります。[Feature Key Settings] ページで自動確認をディセーブルにした場合であっても、[Check for New Keys] ボタンをクリックすることにより、新しいキーを検索するよう AsyncOS にいつでも指示できます。

期限切れ機能キー

（GUI から）アクセスしようとしている機能の機能キーの有効期限が切れている場合は、IronPort 担当者またはサポート組織までご連絡ください。

ユーザの追加

IronPort アプライアンスには、ユーザ アカウントを追加する 2 つの方法があります。IronPort アプライアンス自体でユーザ アカウントを作成する方法と、LDAP または RADIUS ディレクトリなどの独自の中央認証システムを使用してユーザ認証をイネーブルにする方法です。ユーザと外部認証ソースへの接続を管理するには、[System Administration] > [Users] ページを使用します（または、CLI で `userconfig` コマンドを使用します）。ユーザを認証するために外部ディレクトリを使用することについては、「外部認証」（P.8-340）を参照してください。

システムのデフォルトのユーザ アカウントである admin はすべての管理権限を持っています。admin ユーザ アカウントは編集または削除できません（ただし、パスワードを変更できます）。デフォルトの admin ユーザ アカウントのパスワードを変更するには、GUI で [Edit User] ページを使用するか（詳細については、「ユーザの編集」（P.8-337）を参照してください）、CLI で `password` または `passwd` コマンドを使用します。admin ユーザ アカウントのパスワードを忘れた場合は、パスワードをリセットするためにカスタマー サポート プロバイダーにご連絡ください。

IronPort アプライアンスで作成する新しいユーザ アカウントごとに、ユーザ名と氏名を指定し、ユーザを Administrator、Operator、Guest、Read-Only Operator、または Help Desk User のいずれかのユーザ ロールに割り当てます。各ロールには、システム内での異なるレベルの権限が含まれます。ロールを割り当てた後で、ユーザのパスワードを指定します。

表 8-2　ユーザ タイプの一覧

ユーザ ロール	説明
Administrator	Administrator ロールを持つユーザ アカウントはシステムのすべての設定に対する完全なアクセス権を持っています。ただし、`resetconfig` コマンドと `upgrade` コマンドを発行できるのは admin ユーザだけです。 **（注）** AsyncOS は、GUI から電子メール セキュリティ アプライアンスを同時に設定する複数の管理者をサポートしません。
Operator	Operator ロールを持つユーザ アカウントは次のことができません。 • ユーザ アカウントの作成または編集 • `resetconfig` コマンドの発行 • `systemsetup` コマンドの発行またはシステム設定ウィザードの実行 • `adminaccessconfig` コマンドの発行 • 一部の検疫機能の実行（検疫の作成および削除を含む） これら以外は、Administrator ロールと同じ権限を持ちます。
Guest	Guest ロールを持つユーザ アカウントはステータス情報だけを参照できます。また、Guest ロールを持つユーザは IronPort スパム検疫とシステム検疫でメッセージを管理することもできます（アクセスがイネーブルな場合）。Guest ロールを持つユーザはメッセージ トラッキングにアクセスできません。

表 8-2　ユーザ タイプの一覧（続き）

ユーザ ロール	説明
Read-Only Operator	Read-Only Operator ロールを持つユーザは、設定情報を参照するアクセス権を持っています。Read-Only Operator ロールを持つユーザは、機能の設定方法を確認するために変更を行って送信できますが、保存できません。また、このロールを持つユーザは IronPort スパム検疫とシステム検疫でメッセージを管理できます（アクセスがイネーブルな場合）。このロールを持つユーザはファイル システム、FTP、または SCP にアクセスできません。
Help Desk User	Help Desk User ロールを持つユーザがアクセスできるのは次のものに制限されます。 • メッセージ トラッキング • IronPort スパム検疫およびシステム検疫の管理 このロールを持つユーザは、CLI を含めたこれ以外のシステムにはアクセスできません。このロールを持つユーザが IronPort スパム検疫とシステム検疫を管理できるようにするには、これらへのアクセスをイネーブルにする必要があります。

Help Desk User ロールは CLI にアクセスできず、それ以外のロールは GUI と CLI の両方にアクセスできることに注意してください。

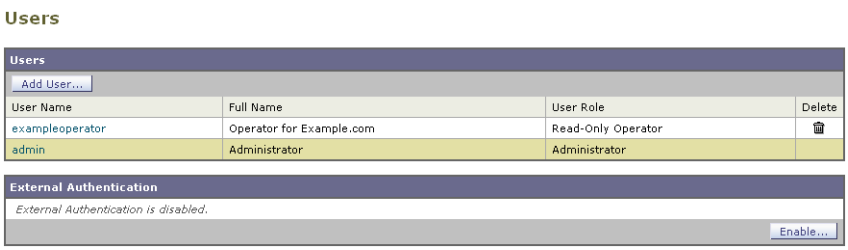
アプライアンスで作成できるユーザ アカウントの数には制限がありませんが、システムにより予約された名前ではユーザ アカウントを作成できません。たとえば、「operator」や「root」などの名前のユーザ アカウントは作成できません。

ユーザを認証するために LDAP ディレクトリを使用する場合は、ユーザ ロールに個々のユーザではなくディレクトリ グループを割り当てます。ユーザ ロールにディレクトリ グループを割り当てると、そのグループの各ユーザはそのユーザ ロールで定義された権限を受け取ります。詳細については、「外部認証」（P.8-340）を参照してください。

ユーザの管理

GUI にログインし、[System Administration] メニューで [Users] を選択します。

図 8-10　[Users] ページ



[Users] ページには、システムの既存のユーザが一覧（ユーザ名、氏名、およびユーザ タイプまたはグループを含む）で表示されます。

[Users] ページからは、次の操作が行えます。

- 新しいユーザの追加
- ユーザの削除
- ユーザの編集（admin ユーザのパスワードの変更を含む）

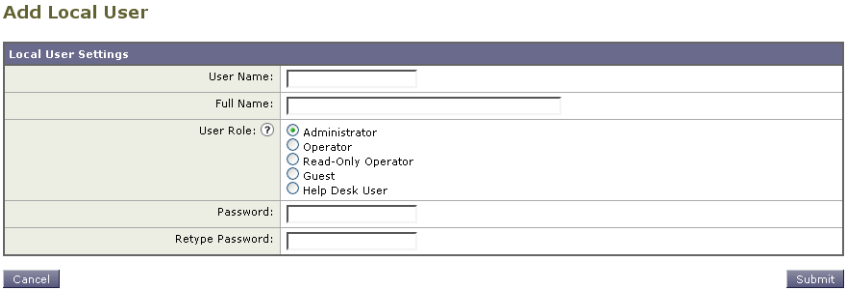
また、ユーザを認証するために LDAP または RADIUS ディレクトリを使用するようアプライアンスをイネーブルにすることもできます。詳細については、「外部認証」（P.8-340）を参照してください。

ユーザの追加

ユーザを追加するには、次の手順を実行します。

ステップ 1　[Add User] をクリックします。[Add User] ページが表示されます。

図 8-11　ユーザの追加



ステップ 2　ユーザの名前を入力します。一部の単語（「operator」や「root」など）は予約されています。

ステップ 3　ユーザの氏名を入力します。

ステップ 4　ユーザ タイプを選択します（ユーザ タイプの詳細については、表 8-2 を参照してください）。

ステップ 5　パスワードを入力し、パスワードを再入力します。パスワードは、6 文字以上にする必要があります。

ステップ 6　変更を送信し、保存します。

ユーザの編集

ユーザを編集（パスワードの変更など）するには、次の手順を実行します。

ステップ 1　[Users] 一覧でユーザの名前をクリックします。[Edit User] ページが表示されます。

ステップ 2　ユーザに対して変更を行います。

ステップ 3　変更を送信し、保存します。

ユーザの削除

ユーザを削除するには、次の手順を実行します。

ステップ 1　[Users] 一覧でユーザの名前に対応するゴミ箱のアイコンをクリックします。

ステップ 2　表示される警告ダイアログで [Delete] をクリックして削除を確認します。

ステップ 3　変更を保存します。

パスワードの変更

ユーザは GUI の上部にある [Options] > [Change Password] リンクを使用して自分のパスワードを変更できます。

古いパスワードを入力し、次に新しいパスワードを入力して確認のためにそのパスワードを再入力します。[Submit] をクリックします。ログアウトされ、画面にログが表示されます。

複数のユーザをサポートする追加コマンド：who、whoami、last

次に、アプライアンスへの複数ユーザ アクセスをサポートするコマンドを示します。

- who コマンドは、CLI からシステムにログインしたすべてのユーザ、ログイン時間、アイドル時間、およびユーザがログインしたリモート ホストを一覧表示します。

```
mail3.example.com> who


Username  Login Time  Idle Time  Remote Host  What

========  ==========  =========  ===========  ====

admin     03:27PM     0s         10.1.3.201   cli
```

- whoami コマンドは、現在ログインしているユーザのユーザ名および氏名と、ユーザが属しているグループを表示します。

```
mail3.example.com> whoami


Username: admin

Full Name: Administrator

Groups: admin, operators, config, log, guest
```

- last コマンドは、アプライアンスに最近ログインしていたユーザを表示します。また、リモート ホストの IP アドレス、ログイン時間、ログアウト時間、および合計時間も表示されます。

```
mail3.example.com> last


Username  Remote Host  Login Time        Logout Time       Total Time
========  ===========  ================  ================  ==========
Username  Remote Host  Login Time        Logout Time       Total Time
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
```

```
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m

admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m

admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m

admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

外部認証

ネットワークの LDAP または RADIUS ディレクトリにユーザ情報を保存する場合は、外部ディレクトリを使用してアプライアンスにログインするユーザを認証するよう IronPort アプライアンスを設定できます。認証のために外部ディレクトリを使用するようアプライアンスを設定するには、GUI で [System Administration] > [Users] ページを使用するか、CLI で `userconfig` コマンドと `external` サブコマンドを使用します。

外部認証がイネーブルであり、ユーザが電子メール セキュリティ アプライアンスにログインすると、アプライアンスは最初に、ユーザがシステム定義の「admin」アカウントであるかどうかを確認します。ユーザがシステム定義の「admin」アカウントでない場合、アプライアンスは最初に設定された外部サーバをチェックしてユーザがそこで定義されたかどうかを確認します。アプライアンスが最初の外部サーバに接続できなければ、アプライアンスは一覧の次の外部サーバをチェックします。

LDAP サーバの場合は、ユーザが外部サーバで認証に失敗すると、アプライアンスは電子メール セキュリティ アプライアンスで定義されたローカル ユーザとしてユーザを認証しようとします。そのユーザが外部サーバまたはアプライアンスに存在しない場合、またはユーザが間違ったパスワードを入力した場合は、アプライアンスへのアクセスが拒否されます。

外部 RADIUS サーバに接続できなければ、一覧の次のサーバが試行されます。すべてのサーバに接続できない場合、アプライアンスは電子メール セキュリティ アプライアンスで定義されたローカル ユーザとしてユーザを認証しようとします。ただし、外部 RADIUS サーバが何らかの理由（パスワード間違いやユーザ未登録など）でユーザを拒否すると、アプライアンスへのアクセスは拒否されます。

図 8-12　外部認証の確立

LDAP 認証のイネーブル化

ユーザを認証するために LDAP ディレクトリを使用する以外に、LDAP グループを IronPort ユーザ ロールに割り当てることができます。たとえば、IT グループのユーザを Administrator ユーザ ロールに割り当てたり、Support グループのユーザを Help Desk User ロールに割り当てたりできます。ユーザが異なるユーザ ロールを持つ複数の LDAP グループに属する場合は、AsyncOS がユーザに最も制限されたロールの権限を割り当てます。たとえば、ユーザが Operator 権限を持つグループと Help Desk User 権限を持つグループに属する場合、AsyncOS はユーザに Help Desk User ロールの権限を割り当てます。

（注）　外部ユーザが LDAP グループのユーザ ロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

LDAP を使用して外部認証をイネーブルにする前に、LDAP サーバ プロファイルと LDAP サーバの外部認証クエリーを定義します。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「LDAP Queries」の章を参照してください。

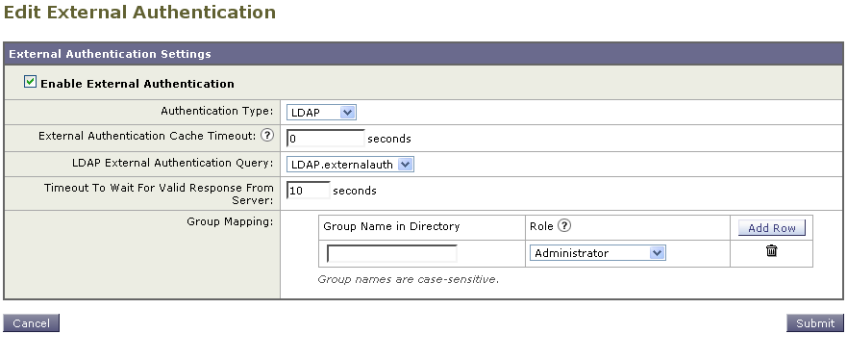
LDAP を使用して外部認証をイネーブルにするには、次の手順を実行します。

ステップ 1　[System Administration] > [Users] ページで、[Enable] をクリックします。[Edit External Authentication] ページが表示されます。

ステップ 2　[Enable External Authentication] チェックボックスをオンにします。

ステップ 3　認証タイプとして LDAP を選択します。

図 8-13　LDAP を使用した外部認証のイネーブル化



ステップ 4　Web ユーザ インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

ステップ 5　ユーザを認証する LDAP 外部認証クエリーを選択します。

ステップ 6　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 7　アプライアンスで認証する LDAP ディレクトリからのグループ名を入力し、グループのユーザに対するロールを選択します。

ステップ 8　また、[Add Row] をクリックして別のディレクトリ グループを追加することもできます。アプライアンスが認証する各ディレクトリ グループに対してステップ 7 とステップ 8 を繰り返します。

ステップ 9　変更を送信し、保存します。

RADIUS 認証のイネーブル化

ユーザを認証するために RADIUS ディレクトリを使用し、ユーザのグループを IronPort ロールに割り当てることもできます。RADIUS サーバは CLASS 属性をサポートする必要があります（AsyncOS は RADIUS ディレクトリのユーザを IronPort ユーザ ロールに割り当てるために CLASS 属性を使用します）。AsyncOS は、RADIUS サーバと通信するために Password Authentication Protocol（PAP; パスワード認証プロトコル）と Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェイク認証プロトコル）の 2 つの認証プロトコルをサポートします。

RADIUS ユーザを IronPort ユーザ ロールに割り当てるには、最初に RADIUS サーバで `<radius-group>` という文字列値を使用して CLASS 属性を設定します（これは IronPort ユーザ ロールにマップされます）。CLASS 属性には文字、数字、およびダッシュを含めることができますが、先頭にダッシュを使用すること

はできません。AsyncOS は CLASS 属性で複数の値をサポートしません。CLASS 属性またはマップされていない CLASS 属性がないグループに属する RADIUS ユーザはアプライアンスにログインできません。

アプライアンスが RADIUS サーバと通信できない場合、ユーザはアプライアンスのローカル ユーザ アカウントでログインできます。

（注）　外部ユーザが RADIUS グループのユーザ ロールを変更する場合、外部ユーザはアプライアンスからログアウトし、再びログインする必要があります。このユーザは新しいロールの権限を持ちます。

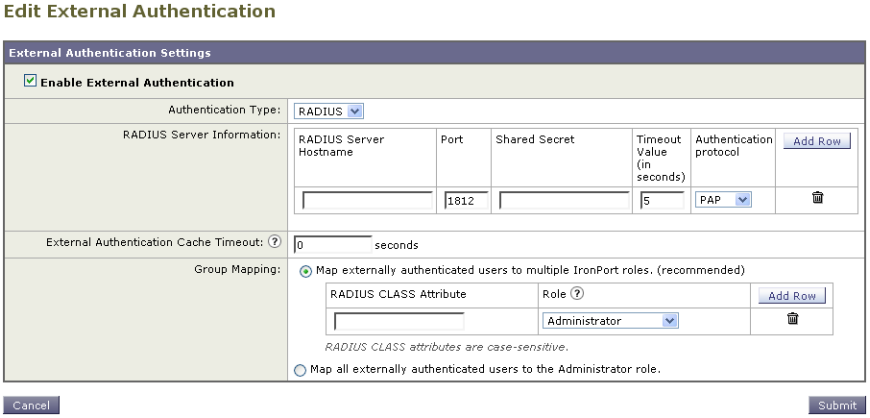
RADIUS を使用して外部認証をイネーブルにするには、次の手順を実行します。

ステップ 1　[System Administration] > [Users] ページで、[Enable] をクリックします。[Edit External Authentication] ページが表示されます。

ステップ 2　[Enable External Authentication] チェックボックスをオンにします。

ステップ 3　認証タイプとして RADIUS を選択します。

図 8-14　RADIUS を使用した外部認証のイネーブル化



ステップ 4　RADIUS サーバのホスト名を入力します。

ステップ 5　RADIUS サーバのポート番号を入力します。デフォルトのポート番号は 1812 です。

ステップ 6　RADIUS サーバの共有秘密パスワードを入力します。

（注）　IronPort アプライアンスのクラスタに対して外部認証をイネーブルにするには、クラスタ内のすべてのアプライアンスで同じ共有秘密パスワードを入力します。

ステップ 7　タイムアウトするまでアプライアンスがサーバからの応答を待つ時間を秒単位で入力します。

ステップ 8　RADIUS 認証として PAP を使用するか、CHAP を使用するかを選択します。

ステップ 9　また、[Add Row] をクリックして別の RADIUS サーバを追加することもできます。認証のためにアプライアンスで使用する各 RADIUS サーバに対してステップ 6 とステップ 7 を繰り返します。

ステップ 10　Web ユーザ インターフェイスで、外部認証クレデンシャルを保存する時間を入力します。

ステップ 11　RADIUS ユーザのグループを IronPort ロールにマップするかどうか、またはすべての RADIUS ユーザに Administrator ロールを割り当てるかどうかを選択します。RADIUS グループを IronPort ロールにマップすることを推奨します。

ステップ 12　RADIUS グループを IronPort ロールにマップすることを選択した場合は、グループの RADIUS CLASS 属性を入力し、その CLASS 属性を持つユーザのロールを選択します。

ステップ 13　また、[Add Row] をクリックして別のグループを追加することもできます。アプライアンスが認証するユーザの各グループに対してステップ 12 とステップ 13 を繰り返します。

ステップ 14　変更を送信し、保存します。

コンフィギュレーション ファイルの管理

Cisco IronPort アプライアンス内のすべての設定は、1 つのコンフィギュレーション ファイルで管理できます。このファイルは Extensible Markup Language（XML）形式で保持されます。

このファイルは次の複数の方法で使用できます。

- コンフィギュレーション ファイルを別のシステムに保存し、重要な設定データをバックアップおよび保持できます。アプライアンスの設定を誤った場合は、保存された最新のコンフィギュレーション ファイルに「ロールバック」できます。
- 既存のコンフィギュレーション ファイルをダウンロードし、アプライアンスの全体の設定を素早く確認できます（多くの新しいブラウザは XML ファイルを直接レンダリングできます）。これにより、現在の設定に存在する可能性がある小さなエラー（タイピング エラーなど）のトラブルシューティングを行えるようになります。
- 既存のコンフィギュレーション ファイルをダウンロードし、変更を行い、そのファイルを同じアプライアンスにアップロードできます。この場合は、実質的に設定の変更を行うために CLI と GUI の両方が「バイパス」されます。
- FTP アクセスを使用してコンフィギュレーション ファイル全体をアップロードしたり、コンフィギュレーション ファイルの一部または全体を CLI に貼り付けたりできます。
- ファイルは XML 形式であるため、コンフィギュレーション ファイルのすべての XML エンティティを定義する、関連付けられた Document Type Definition（DTD）も提供されます。XML コンフィギュレーション ファイルをアップロードする前にこの DTD をダウンロードして XML コンフィギュレーション ファイルを検証できます（XML 検証ツールはインターネットで簡単に入手できます）。

XML コンフィギュレーション ファイルを使用した複数のアプライアンスの管理

- ある Cisco IronPort アプライアンスから既存のコンフィギュレーション ファイルをダウンロードし、変更を行い、別のアプライアンスにアップロードできます。これにより、複数の IronPort アプライアンスのインストールを簡単に管理できるようになります。現時点では、コンフィギュレーション ファイルを C/X-Series アプライアンスから M-Series アプライアンスにロードできません。
- ある Cisco IronPort からダウンロードされた既存のコンフィギュレーション ファイルを複数のサブセクションに分割できます。（複数のアプライアンス環境の）すべてのアプライアンスで共通するこれらのセクションを変更し、サブセクションの更新時にこれらのセクションを他のアプライアンスにロードできます。

たとえば、Global Unsubscribe コマンドをテストするためにテスト環境でアプライアンスを使用できます。グローバル配信停止リストを適切に設定した場合は、テスト アプライアンスのグローバル配信停止設定セクションをすべての実稼動アプライアンスにロードできます。

GUI を使用したコンフィギュレーション ファイルの管理

GUI を使用して IronPort アプライアンスでコンフィギュレーション ファイルを管理するには、[System Administration] タブの [Configuration File] リンクをクリックします。

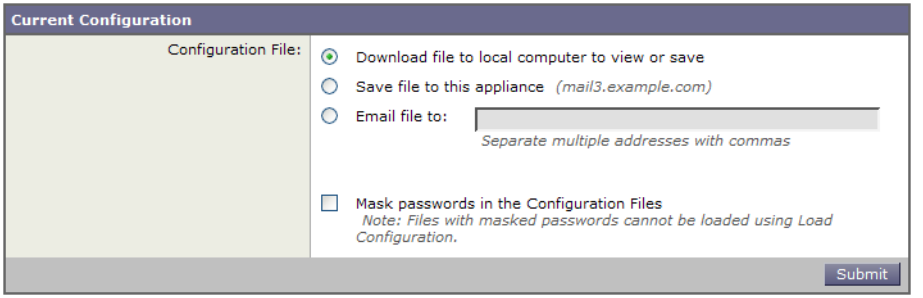
[Configuration File] ページには次の 3 つのセクションがあります。

- [Current Configuration]：現在のコンフィギュレーション ファイルを保存およびエクスポートするために使用します。
- [Load Configuration]：コンフィギュレーション ファイルの全体または一部をロードするために使用します。
- [Reset Configuration]：現在の設定を出荷時デフォルト値にリセットするために使用します（リセット前に設定を保存する必要があります）。

現在のコンフィギュレーション ファイルの保存およびエクスポート

[System Administration] > [Configuration File] ページの [Current Configuration] のセクションを使用すると、現在のコンフィギュレーション ファイルを、ローカル マシンに保存したり、アプライアンスで保存したり（FTP/SCP ルートの `configuration` ディレクトリに保存されます）、指定されたアドレスに電子メールで送信したりできます。

図 8-15　現在のコンフィギュレーション ファイル



チェックボックスをクリックすることにより、ユーザのパスワードをマスクできます。パスワードをマスクすると、元の暗号化されたパスワードが、エクスポートまたは保存されたファイルで「*****」に置き換えられます。ただし、パスワードがマスクされたコンフィギュレーション ファイルを AsyncOS に再びロードすることはできないことに注意してください。

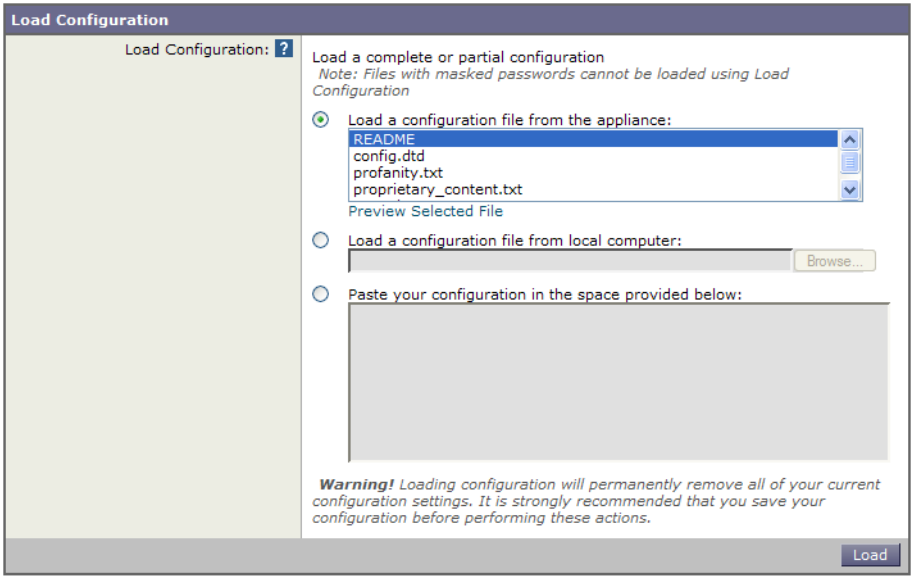
コンフィギュレーション ファイルのロード

[System Administration] > [Configuration File] ページの [Load Configuration] のセクションを使用して新しい設定情報を Cisco IronPort アプライアンスにロードします。情報は次の 3 つのいずれかの方法でロードできます。

- `configuration` ディレクトリに情報を格納し、アップロードする。
- コンフィギュレーション ファイルをローカル マシンから直接アップロードする。
- GUI に設定情報を直接貼り付ける。

パスワードがマスクされたコンフィギュレーション ファイルはロードできません。

図 8-16　コンフィギュレーション ファイルのロード



どの方法の場合でも、設定の上部に次のタグを含める必要があります。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

 ... your configuration information in valid XML

</config>
```

`</config>` 閉じタグは設定情報の後に指定する必要があります。XML 構文の値は、IronPort アプライアンスの `configuration` ディレクトリにある Document Type Definition（DTD）を使用して解析および検証されます。DTD ファイルの名前は `config.dtd` です。`loadconfig` コマンドを使用したときにコマンド ラインで検証エラーが報告された場合、変更はロードされません。コンフィギュレーション ファイルをアップロードする前に、アプライアンスの外部で DTD をダウンロードし、コンフィギュレーション ファイルを検証できます。

いずれの方法の場合でも、コンフィギュレーション ファイル全体（最上位のタグである <config></config> 間で定義された情報）またはコンフィギュレーション ファイルの *complete* および *unique* サブセクション（上記の宣言タグが含まれ、<config></config> タグ内に存在する場合）をインポートできます。

「complete」とは、DTD で定義されたサブセクションの開始タグおよび終了タグ全体が含まれることを意味します。たとえば、次の内容をアップロードまたは解析します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

  <autosupport_enabled>0</autosu

</config>
```

この場合は、アップロード中に検証エラーが発生します。ただし、

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">

<config>

  <autosupport_enabled>0</autosupport_enabled>

</config>
```

この場合は、検証エラーが発生しません。

「unique」とは、アップロードまたは貼り付けられるコンフィギュレーション ファイルのサブセクションが、設定として多義的でないことを意味します。たとえば、システムは 1 つのホスト名しか持つことができないため、次の内容（宣言と <config></config> タグを含む）をアップロードすることは可能です。

```
<hostname>mail4.example.com</hostname>
```

ただし、システムでは複数のリスナーを定義できるため（リスナーごとに異なる受信者アクセス テーブルが定義されます）、

```
<rat>
   <rat_entry>
     <rat_address>ALL</rat_address>
     <access>RELAY</access>
   </rat_entry>
 </rat>
```

上記の内容だけをアップロードすることは多義的と見なされ、「完全」な構文であっても許可されません。

警告　コンフィギュレーション ファイルまたはコンフィギュレーション ファイルのサブセクションをアップロードまたは解析する場合は、待機中の可能性がある、保存されていない変更が破棄されることがあります。

空白タグと省略されたタグ

コンフィギュレーション ファイルのセクションをアップロードまたは解析する場合は注意が必要です。タグを含めないと、コンフィギュレーション ファイルのアップロード時に設定の値が変更されません。ただし、空白タグを含めると、設定の問題が解消されます。

たとえば、

```
<listeners></listeners>
```

上記の内容をアップロードすると、システムからすべてのリスナーが削除されます。

警告　コンフィギュレーション ファイルのサブセクションをアップロードしたり、貼り付けたりした場合、GUI または CLI から切断され、大量の設定データが破壊されることがあります。別のプロトコル、シリアル インターフェイス、または管理ポートのデフォルト設定を使用してアプライアンスに再接続できない場合は、このコマンドでサービスをディセーブルにしないでください。また、DTD で定義された設定構文がよくわからない場合は、このコマンドを使用しないでください。新しいコンフィギュレーション ファイルをアップロードする前に、必ず設定データをバックアップしてください。

ログ サブスクリプションのパスワードのロードについての注意事項

パスワードが必要なログ サブスクリプションを含むコンフィギュレーション ファイルをロードしようとしても（たとえば、FTP プッシュを使用）、`loadconfig` コマンドは不明なパスワードについて警告しません。FTP プッシュが失敗し、`logconfig` コマンドを使用して正しいパスワードを設定するまで警告が生成されます。

文字セット エンコーディングについての注意事項

XML コンフィギュレーション ファイルの「encoding」属性は、ファイルをオフラインで操作するために使用している文字セットに関係なく、「`ISO-8859-1`」である必要があります。`showconfig` コマンド、`saveconfig` コマンド、または `mailconfig` コマンドを発行するたびにエンコーディング属性がファイルで指定されることに注意してください。

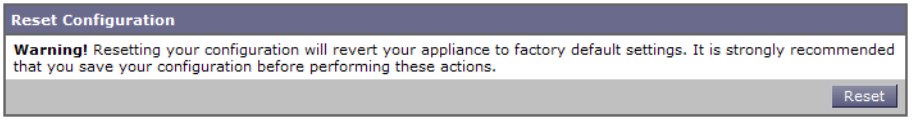
```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

現時点では、このエンコーディングを持つコンフィギュレーション ファイルだけをロードできます。

現在の設定のリセット

現在の設定をリセットすると、IronPort アプライアンスが元の出荷時デフォルト値に戻ります。リセットする前に設定を保存する必要があります。GUI でこのボタンを使用して設定をリセットすることは、クラスタリング環境ではサポートされていません。

図 8-17　コンフィギュレーション ファイルのリセット



「出荷時デフォルト値へのリセット」（P.8-319）を参照してください。

コンフィギュレーション ファイル用の CLI コマンド

次のコマンドを使用すると、コンフィギュレーション ファイルを操作できます。

- showconfig
- mailconfig
- saveconfig
- loadconfig
- resetconfig（「出荷時デフォルト値へのリセット」（P.8-319）を参照）

showconfig、mailconfig、および saveconfig コマンド

コンフィギュレーション コマンドの showconfig、mailconfig、および saveconfig の場合は、電子メールで送信されるファイルまたは表示されるファイルにパスワードを含めるかどうか選択することを求められます。パスワードを含めないことを選択すると、パスワード フィールドが空白のままになります。セキュリティの問題を心配する場合は、パスワードを含めないことを選択できます。ただし、loadconfig コマンドを使用してロードされた場合、パスワードがないコンフィギュレーション ファイルは失敗します。「ログ サブスクリプションのパスワードのロードについての注意事項」（P.8-351）を参照してください。

（注）　パスワードを含めることを選択した場合（「Do you want to include passwords?」に「yes」と回答します）にコンフィギュレーション ファイルを保存、表示、または電子メールで送信するとき、パスワードは暗号化されます。ただし、秘密キーと証明書は暗号化されない PEM 形式で含められます。

Showconfig コマンドは現在の設定を画面に出力します。

```
mail3.example.com> showconfig



Do you want to include passwords? Please be aware that a
configuration without passwords will fail when reloaded with
loadconfig.



<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE config SYSTEM "config.dtd">



<!--

  Product: IronPort model number Messaging Gateway Appliance(tm)

  Model Number: model number

  Version: version of AsyncOS installed

  Serial Number: serial number

  Current Time: current time and date

[The remainder of the configuration file is printed to the screen.]
```

mailconfig コマンドを使用して現在の設定をユーザに電子メールで送信します。メッセージには config.xml という名前の XML 形式のコンフィギュレーション ファイルが添付されます。

```
mail3.example.com> mailconfig



Please enter the email address to which you want to send
```

```
the configuration file.

[]> administrator@example.com



Do you want to include passwords? Please be aware that a
configuration without passwords will fail when reloaded with
loadconfig.  [N]> y



The configuration file has been sent to administrator@example.com.
```

Saveconfig コマンドは、一意のファイル名を使用してコンフィギュレーション ファイルを configuration ディレクトリに保存します。

```
mail3.example.com> saveconfig



Do you want to include passwords? Please be aware that a
configuration without passwords will fail when reloaded with
loadconfig.  [N]> y



The file C60-00065B8FCEAB-31PM121-20030630T130433.xml has been saved
in the configuration directory.

mail3.example.com>
```

loadconfig コマンド

Cisco IronPort アプライアンスに新しい設定情報をロードするには loadconfig を使用します。情報は次の 2 つのいずれかの方法でロードできます。

ステップ 1　configuration ディレクトリに情報を格納し、アップロードする。

ステップ 2　CLI に設定情報を直接貼り付ける。

詳細については、「コンフィギュレーション ファイルのロード」（P.8-347）を参照してください。

CLI を使用した設定変更のアップロード

ステップ 1　CLI の外部で、アプライアンスの configuration ディレクトリにアクセスできることを確認します。詳細については、Appendix A, “Accessing the Appliance” を参照してください。

ステップ 2　コンフィギュレーション ファイル全体またはコンフィギュレーション ファイルのサブセクションをアプライアンスの configuration ディレクトリに格納するか、saveconfig コマンドで作成した既存の設定を編集します。

ステップ 3　CLI 内で、loadconfig コマンドを使用して、ステップ 2 で示されたディレクトリに格納したコンフィギュレーション ファイルをロードするか、テキスト（XML 構文）を CLI に直接貼り付けます。

この例では、changed.config.xml という名前のファイルがアップロードされ、変更が保存されます。

```
mail3.example.com> loadconfig



1. Paste via CLI

2. Load from file

[1]> 2



Enter the name of the file to import:

[]> changed.config.xml



Values have been loaded.
```

```
Be sure to run "commit" to make these settings active.

mail3.example.com> commit
```

この例では、新しいコンフィギュレーション ファイルをコマンド ラインに直接貼り付けます（空白行で Ctrl+D を押すと貼り付けコマンドが終了します）。次に、システム設定ウィザードを使用して、デフォルトのホスト名、IP アドレス、およびデフォルトのゲートウェイ情報を変更します（詳細については、『*Cisco IronPort AsyncOS for Email Configuration Guide*』の「Setup and Installation」を参照してください）。最後に、変更を保存します。

```
mail3.example.com> loadconfig


1. Paste via CLI

2. Load from file

[1]> 1


Paste the configuration file now. Press CTRL-D on a blank line when
done.


[The configuration file is pasted until the end tag </config>.
Control-D is entered on a separate line.]


Values have been loaded.

Be sure to run "commit" to make these settings active.

mail3.example.com> systemsetup
```

```
[The system setup wizard is run.]

mail3.example.com> commit

Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings via
systemsetup
```

セキュア シェル（SSH）キーの管理

sshconfig コマンドを使用すると、システムで設定されたユーザ アカウント（admin アカウントを含む）の authorized_keys ファイルに Secure Shell（SSH; セキュア シェル）公開ユーザ キーを追加したり、それらのキーを削除したりできます。これにより、パスワード チャレンジではなく SSH キーを使用してユーザ アカウントを認証できるようになります。RSA ベース認証と DSA キー タイプを持つ SSH プロトコル バージョン 1（SSH1）と SSH プロトコル バージョン 2（SSH2）の両方がサポートされます。SSH1 は setup サブコマンドを使用してディセーブルにできます。

（注） Cisco IronPort アプライアンスから他のホスト マシンへのログ ファイルの SCP プッシュを実行する場合に使用されるホスト キーを設定するには、logconfig -> hostkeyconfig を使用します。詳細については、第 5 章「ロギング」を参照してください。

hostkeyconfig を使用すると、リモート ホストのキーをスキャンし、Cisco IronPort アプライアンスに追加できます。

（注） CLI に新しいキーを直接貼り付ける場合は、空白行で Enter または Return を押してキーの入力を終了します。

次の例では、admin アカウントに対して新しい公開キーがインストールされます。

```
mail3.example.com> sshconfig


Currently installed keys for admin:


Choose the operation you want to perform:

- NEW - Add a new key.

- USER - Switch to a different user to edit.

- SETUP -  Configure general settings.

[]> new


Please enter the public SSH key for authorization.

Press enter on a blank line to finish.


[cut and paste public key for user authentication here]


Currently installed keys for admin:

1. ssh-dss AAAAB3NzaC1kc3MAA...CapRrgxcY= (admin@example.com)


Choose the operation you want to perform:

- NEW - Add a new key.
```

```
- EDIT - Modify a key.

- DELETE - Remove a key.

- PRINT - Display a key.

[]>
```

SSH1 のディセーブル化

SSH1 をディセーブル（またはイネーブル）にするには、sshconfig コマンドの setup サブコマンドを使用します。

```
mail3.example.com> sshconfig


Currently installed keys for admin:


Choose the operation you want to perform:

- NEW - Add a new key.

- USER - Switch to a different user to edit.

- SETUP -  Configure general settings.

[]> setup




Choose the operation you want to perform:

- DISABLE - Disable SSH v1

[]> disable
```

```
Currently installed keys for admin:


Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings
[]>


mail3.example.com> commit
```

リモート SSH コマンド実行

CLI では、リモート SSH コマンド実行を使用してコマンドを実行できます。コマンドの一覧については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の付録 A「AsyncOS Quick Reference Guide」を参照してください。たとえば、IronPort アプライアンスで admin アカウントに対して SSH 公開キーが設定されている場合は、チャレンジされないリモート ホストから次のコマンドを実行できます。

```
# ssh admin@mail3.example.com status
Enter "status detail" for more information.
Status as of: Mon Jan 20 17:24:15 2003
Last counter reset: Mon Jan 20 17:08:21 2003
System status: online
[rest of command deleted]
```