一般的な管理タスク

この章は、次の項で構成されています。

管理タスクの実行

システム管理タスクのほとんどは、グラフィカル ユーザー インターフェイス（GUI）の [システム管理（System Administration）] メニューを使用して実行できます。ただし、一部のシステム管理機能は、コマンドライン インターフェイス（CLI）からのみ実行できます。

また、 システム ステータスのモニターリング

（注） この章で説明する機能やコマンドの中には、ルーティングの優先順位に影響を及ぼすものがあります。詳細については、IP アドレス、インターフェイス、およびルーティングを参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスのライセンス

機能キーの使用

キーは、アプライアンスのシリアル番号に固有のものであり、またイネーブルする機能にも固有です。1 つのシステムのキーを、別のシステムで再利用することはできません。

ここで説明するタスクをコマンドライン プロンプトから実行するには、featurekey コマンドを使用します。

目的	操作手順
• アプライアンスのアクティブな機能キーをすべて表示する • アクティベーションを保留中のすべての機能キーを表示する • 発行された新しいキーを検索する • 機能キーを手動でインストールする • 機能キーをアクティブ化する	[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）] > [機能キー（Feature Keys）] を選択します。 新しい機能キーを手動で追加するには、[機能キー（Feature Key）]フィールドにキーを貼り付けるか、または入力し、[キーを送信（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（たとえば、キーが正しくない場合など）。それ以外の場合は、機能キーがリストに追加されます。 発行されたときに自動的に新しいキーをダウンロードおよびインストールするようにアプライアンスを設定した場合、[保留中のライセンス（Pending Activation）]リストは常に空白になります。
機能キーの自動ダウンロードおよびアクティベーションを有効または無効にする	[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）] > [機能キーの設定（Feature Key Settings）] を選択します デフォルトでは、アプライアンスは、新しいキーを定期的に確認します。
期限切れ機能キーを更新する	Cisco の担当者にお問い合わせください

仮想アプライアンスのライセンスおよび機能キー

ライセンスおよび機能キーの期限が切れたときのアプライアンスの動作については、http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/products-installation-guides-list.html から入手できる『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。

ライセンス情報を表示するには、コマンドライン インターフェイス（CLI）で show license コマンドを使用します。

スマート ソフトウェア ライセンシング

概要

スマート ソフトウェア ライセンシングを使用すると、Cisco コンテンツ セキュリティ管理アプライアンスのライセンスをシームレスに管理およびモニターできます。スマート ソフトウェア ライセンスをアクティブ化するには、Cisco Smart Software Manager（CSSM）でアプライアンスを登録する必要があります。CSSMは、購入して使用するすべてのシスコ製品についてライセンスの詳細を管理する一元化されたデータベースです。スマート ライセンスを使用すると、製品認証キー（PAK）を使用して Web サイトで個別に登録するのではなく、単一のトークンで登録することができます。

アプライアンスを登録すると、アプライアンスのライセンスを追跡し、CSSMポータル経由でライセンスの使用状況を監視できます。アプライアンスにインストールされているスマート エージェントは、アプライアンスと CSSM を接続し、ライセンスの使用状況に関する情報を CSSM を渡して、CSSM が使用状況を追跡できるようにします。

Cisco Smart Software Manager を理解するには、https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

- ご利用のアプライアンスからインターネットに接続できることを確認します。
- シスコ セールス チームに問い合わせて Cisco Smart Software Manager ポータル（https://software.cisco.com/#module/SmartLicensing）でスマート アカウントを作成するか、Cisco Smart Software Manager サテライトをネットワークにインストールしてください。

  Cisco Smart Software Manager ユーザ アカウントの作成または Cisco Smart Software Manager サテライトのインストールの詳細については、Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

  ライセンスの使用状況に関する情報を直接インターネットに送信したくないユーザの場合、CSSM 機能のサブセットを提供する Smart Software Manager サテライトをオンプレミスにインストールすることもできます。サテライト アプリケーションをダウンロードして導入した後は、インターネットを使用して CSSM にデータを送信せずに、ライセンスをローカルで安全に管理できます。CSSMサテライトは、情報をクラウドに定期的に送信します。

（注） Smart Software Manager サテライトを使用する場合、Smart Software Manager サテライト Enhanced Edition 6.1.0 を使用してください。

- （従来の）クラシック ライセンスの既存ユーザは、クラシック ライセンスをスマート ライセンスに移行する必要があります。

  https://video.cisco.com/detail/video/5841741892001/convert-classic-licenses-to-smart-licenses?autoStart=true&q=classicを参照してください。

- アプライアンスのシステム クロックを CSSM のシステム クロックと同期させる必要があります。アプライアンスのシステム クロックと CSSM のシステム クロックのずれは、スマート ライセンス操作の失敗の原因となります。

（注） インターネットに接続してプロキシ経由でCSSMに接続する場合、[システム管理（System Administration）]>[アップデート設定（Update Settings）] を使用して、アプライアンスに設定されているプロキシと同じプロキシを使用する必要があります

（注） 仮想ユーザーの場合、新しい PAK ファイル（新規または更新）を受信するたびに、ライセンス ファイルを生成し、アプライアンスのファイルをロードします。ファイルをロードした後は、PAK をスマート ライセンスに変換する必要があります。スマート ライセンス モードでは、ファイルのロード中、ライセンス ファイルの機能キー セクションは無視され、証明書情報のみが使用されます。

アプライアンスに対してスマート ソフトウェア ライセンシングを有効にするには、次の手順を実行する必要があります。

	操作内容	詳細情報
ステップ 1	スマート ソフトウェア ライセンシングの有効化	スマート ソフトウェア ライセンシングのイネーブル化 （6 ページ）
ステップ 2	Cisco Smart Software Manager でのアプライアンスの登録	Cisco Smart Software Manager でのアプライアンスの登録 （6 ページ）
ステップ 3	ライセンス（機能キー）の要求	ライセンスの要求 （7 ページ）

スマート ソフトウェア ライセンシングのイネーブル化

ステップ 1 [管理対象アプライアンス（Managed Appliance）] > [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

ステップ 2 [スマート ソフトウェア ライセンシングの有効化（Enable Smart Software Licensing）] をクリックします。

スマート ソフトウェア ライセンシングの詳細については、スマート ソフトウェア ライセンシングの詳細のリンクをクリックします。

ステップ 3 スマート ソフトウェア ライセンシングについての情報を読んだ後、**[OK]** をクリックします。

ステップ 4 変更を保存します。

次のタスク

スマート ソフトウェア ライセンシングを有効すると、クラシック ライセンス モードのすべての機能がスマート ライセンス モードでも自動的に使用可能になります。クラシック ライセンス モードの既存ユーザーの場合、CSSM でアプライアンスを登録せずに、スマート ソフトウェア ライセンシング機能を使用できる 90 日間の評価期間があります。

有効期限および評価期間の期限の前に、一定の間隔（90 日前、60 日前、30 日前、15 日前、5 日前、および最終日）で通知が表示されます。評価期間の間または終了後に、CSSMでアプライアンスを登録できます。

（注） クラシック ライセンス モードにおけるアクティブなライセンスを持たない仮想アプライアンスの新規ユーザーの場合、スマート ソフトウェア ライセンシング機能を有効にしても、評価期間は提供されません。クラシック ライセンス モードにおけるアクティブなライセンスを持つ仮想アプライアンスの既存ユーザーのみに、評価期間が提供されます。新規仮想アプライアンス ユーザーがスマート ライセンス機能の評価を希望する場合には、シスコ セールス チームに連絡し、スマート アカウントに評価ライセンスを追加してください。評価ライセンスは、登録後に評価目的で使用されます。

（注） アプライアンスでスマート ライセンシング機能を有効にすると、スマート ライセンシングからクラシック ラインセンシング モードにロールバックすることができなくなります。

Cisco Smart Software Manager でのアプライアンスの登録

アプライアンスを Cisco Smart Software Manager に登録するには、[システム管理（System Administration）] メニューでスマート ソフトウェア ライセンシング機能を有効にする必要があります。

ステップ 1 [管理対象アプライアンス（Managed Appliance）] > [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] に進みます。

ステップ 2 [スマートライセンスの登録（Smart License Registration）] オプションを選択します。

ステップ 3 [トランスポート設定（Transport Settings）] を変更する場合には、[編集（Edit）] をクリックします。次のオプションを使用できます。

- [直接（Direct）]：アプライアンスを HTTPS 経由で Cisco Smart Software Manager に直接接続します。このオプションは、デフォルトで選択されます。
- [トランスポートゲートウェイ（Transport Gateway）]：アプライアンスをトランスポート ゲートウェイまたは Smart Software Manager サテライト経由で Cisco Smart Software Manager に接続します。このオプションを選択した場合、トランスポート ゲートウェイまたは Smart Software Manager サテライトの URL を入力してから [OK] をクリックする必要があります。このオプションは HTTP および HTTPS をサポートします。FIPS モードの場合、トランスポート ゲートウェイは HTTPS のみをサポートします。トランスポート ゲートウェイについては、Https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

  ログイン クレデンシャルを使用して、Cisco Smart Software Manager ポータル

  （https://software.cisco.com/#module/SmartLicensing）にアクセスします。新しいトークンを作成するには、このポータルの [仮想アカウント（Virtual Account）] ページに移動して [全般（General）] タブにアクセスします。アプライアンス用の製品インスタンス登録トークンをコピーします。

  製品インスタンス登録トークンの作成については、https://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-2/b_Smart_Licensing_Deployment_Guide.html を参照してください。

ステップ 4 アプライアンスに戻り、製品インスタンス登録トークンを貼り付けます。

ステップ 5 [登録（Register）] をクリックします。

ステップ 6 [スマートソフトウェアライセンシング（Smart Software Licensing）] ページで、[すでに登録されている場合は、この製品インスタンスを再登録します（Reregister this product instance if it is already registered）] チェックボックスをオンにして、アプライアンスを再登録することもできます。Cisco Smart Software Manager でのアプライアンスの再登録 （9 ページ）を参照してください。

次のタスク

製品登録プロセスには数分かかります。[スマートソフトウェアライセンシング（Smart Software Licensing）] ページで登録ステータスを表示できます。

ライセンスの要求

登録プロセスが正常に完了した後、アプライアンスの機能のライセンスを要求しなければならない場合があります。

ステップ 1 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ライセンス（Licenses）] を選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 要求するライセンスに対応する [ライセンスの要求/リリース（License Request/Release）] 列のチェック ボックスをオンにします。

ステップ 4 **[送信（Submit）]** をクリックします。

（注） デフォルトでは、メール処理のライセンスが利用可能です。このライセンスは、有効化、無効化、またはリリースすることができません。メール処理ライセンスに評価期間やコンプライアンス違反はありません。

次のタスク

ライセンスは、期限超過また期限切れになるとコンプライアンス違反（OOC）モードになり、各ライセンスに 30 日間の猶予期間が提供されます。有効期限および OOC 猶予期間の期限の前に、一定の間隔（30 日前、15 日前、5 日前、および最終日）で通知が表示されます。

OOC 猶予期間の有効期限が過ぎると、ライセンスは使用できず、機能を利用できなくなります。機能にもう一度アクセスするには、CSSM ポータルでライセンスをアップデートして、認証を更新する必要があります。

ライセンスのリリース

ステップ 1 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ライセンス（Licenses）] を選択します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 リリースするライセンスに対応する [ライセンスの要求（License Request）] 列のチェック ボックスをオフにします。

ステップ 4 **[送信（Submit）]** をクリックします。

（注） メール処理のためにライセンスをリリースすることはできません。

Cisco Smart Software Manager からのアプライアンスの登録解除

ステップ 1 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

ステップ 2 **[アクション（Action）]** ドロップダウン リストから、**[登録解除（Deregister）]** を選択し、**[実行（Go）]** をクリックします。

ステップ 3 **[送信（Submit）]** をクリックします。

Cisco Smart Software Manager でのアプライアンスの再登録

ステップ 1 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

ステップ 2 **[アクション（Action）]** ドロップダウン リストから、**[登録（Register）]** を選択し、**[実行（Go）]** をクリックします。

次のタスク

登録プロセスについては、Cisco Smart Software Manager でのアプライアンスの登録 （6 ページ） を参照してください。

回避できないシナリオにおいては、アプライアンスの設定をリセットした後にアプライアンスを登録することができます。

転送設定の変更

CSSM でアプライアンスを登録する前にのみ、トランスポート設定を変更できます。

（注） スマート ライセンス機能が有効になっている場合にのみ、トランスポート設定を変更することができます。アプライアンスがすでに登録されている場合、トランスポート設定を変更するには、アプライアンスの登録を解除する必要があります。トランスポート設定を変更した後に、アプライアンスを再登録する必要があります。

トランスポート設定を変更する方法については、Cisco Smart Software Manager でのアプライアンスの登録 （6 ページ） を参照してください。

認証と証明書の更新

Cisco Smart Software Manager でアプライアンスを登録した後に、証明書を更新できます。

（注） アプライアンスが正常に登録された後にのみ、認証を更新できます。

ステップ 1 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

ステップ 2 **[アクション（Action）]** ドロップダウン リストから、適切なオプションを選択します。

- 認証を今すぐ更新
- 証明書を今すぐ更新

ステップ 3 **[移動（Go）]** をクリックします。

スマート エージェントの更新

アプライアンスにインストールされているスマート エージェントのバージョンを更新するには、次の手順を実行します。

ステップ 1 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[スマートソフトウェアライセンシング（Smart Software Licensing）] を選択します。

ステップ 2 **[スマートエージェントの更新ステータス（Smart Agent Update Status）]** セクションで、**[今すぐ更新（Update Now）]** をクリックし、プロセスに従います。

（注） CLI コマンド `saveconfig` を使用して、または **[システム管理（System Administration）]>[設定サマリー（Configuration Summary）]** を使用して Web インターフェイス経由で設定変更を保存しようとすると、スマート ライセンス関連の設定は保存されません。

アラート

次のシナリオで通知が送信されます。

- スマート ソフトウェア ライセンシングが正常に有効化された
- スマート ソフトウェア ライセンシングの有効化に失敗した
- 評価期間が開始された
- 評価期間が終了した（評価期間中および期間終了時に一定の間隔で送信）
- 正常に登録された
- 登録に失敗した
- 正常に認証された
- 認証に失敗した
- 正常に登録解除された
- 登録解除に失敗した
- ID 証明書が正常に更新された
- ID 証明書の更新に失敗した

- 認証の有効期限が切れた
- ID 証明書の有効期限が切れた
- コンプライアンス違反猶予期間の期限が切れた（コンプライアンス違反猶予期間中および期間終了時に一定の間隔で送信）
- 機能の有効期限に関する最初のインスタンスが発生した
- [SLR および PLR のみに適用（Applicable for SLR and PLR only）]：リクエストコードの生成後に認証コードがインストールされます。
- [SLR および PLR のみに適用（Applicable for SLR and PLR only）]：認証コードがインストールされます。
- [SLR および PLR のみに適用（Applicable for SLR and PLR only）]：リターンコードが正常に生成されました。

コマンドライン インターフェイス

license_smart

説明

スマート ソフトウェア ライセンス機能の設定

使用方法

確定：このコマンドは「commit」が必要です。

バッチ コマンド：このコマンドはバッチ形式をサポートしています。詳細については、`help license_smart` コマンドを入力して、インライン ヘルプを参照してください。

例：スマート エージェント サービス用ポートの設定

```
example.com> license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
- SETAGENTPORT - Set port to run Smart Agent service.
[]> setagentport

Enter the port to run smart agent service.
[65501]>
```

例：スマート ライセンスの有効化

```
mail.example.com > license_smart
Choose the operation you want to perform:
- ENABLE - Enables Smart Licensing on the product.
 []> enable
After enabling Smart Licensing on your appliance, follow below steps to activate
the feature keys (licenses):

a) Register the product with Smart Software Manager using license_smart > register command
 in the CLI.
b) Activate the feature keys using license_smart > requestsmart_license command in the
CLI.

Note: If you are using a virtual appliance, and have not enabled any of the
features in the classic licensing mode; you will not be able to activate the
licenses, after you switch to the smart licensing mode. You need to first register
your appliance, and then you can activate the licenses (features) in the smart licensing
 mode.
Commit your changes to enable the Smart Licensing mode on your appliance.
All the features enabled in the Classic Licensing mode will be available in the Evaluation
 period.
Type "Y" if you want to continue, or type "N" if you want to use the classic licensing
mode [Y/N] []> y

> commit

Please enter some comments describing your changes:
[]>
Do you want to save the current configuration for rollback? [Y]>
```

例：*Smart Software Manager* でのアプライアンスの登録

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> register
Reregister this product instance if it is already registered [N]> n

Enter token to register the product:
[]>
ODRlOTM5MjItOTQzOS00YjY0LWExZTUtZTdmMmY3OGNlNDZmLTE1MzM3Mzgw%0AMDEzNTR8WlpCQ1lMbGVMQWRx
```

```
OXhuenN4OWZDdktFckJLQzF5V3VIbzkyTFgx%0AQWcvaz0%3D%0A
Product Registration is in progress. Use license_smart > status command to check status
 of registration.
```

例：スマート ライセンスのステータス

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

例：スマート ライセンスのステータスの概要

```
mail.example.com > license_smart
To start using the licenses, please register the product.
Choose the operation you want to perform:
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> summary

FeatureName                                  LicenseAuthorizationStatus
Mail Handling                                                In Compliance
Content Security Management Master ISQ                       In Compliance
```

例：スマート トランスポート *URL* の設定

```
mail.example.com > license_smart

Choose the operation you want to perform:
- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> url
```

```
1. DIRECT - Product communicates directly with the cisco license servers
2. TRANSPORT_GATEWAY - Product communicates via transport gateway or smart software
manager satellite.

Choose from the following menu options:
[1]> 1
Note: The appliance uses the Direct URL
(https://smartreceiver.cisco.com/licservice/license) to communicate with Cisco
Smart Software Manager (CSSM) via the proxy server configured using the updateconfig
command.
Transport settings will be updated after commit.
```

例：ライセンスの要求

（注） 仮想アプライアンスのユーザーは、ライセンスを要求またはリリースする場合、そのアプライアンスを登録する必要があります。

```
mail.example.com > license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> requestsmart_license

Feature Name                                    License Authorization Status
1. Content Security Management Centralized Tracking     Not Requested
2. Content Security Management Master ISQ               Not requested

Enter the appropriate license number(s) for activation.
Separate multiple license with comma or enter range:
[]> 1
Activation is in progress for following features:
Security Management Centralized Tracking
Use license_smart > summary command to check status of licenses.
```

例：ライセンスのリリース

```
mail.example.com > license_smart
Choose the operation you want to perform:

- REQUESTSMART_LICENSE - Request licenses for the product.
- RELEASESMART_LICENSE - Release licenses of the product.
- REGISTER - Register the product for Smart Licensing.
- URL - Set the Smart Transport URL.
- STATUS - Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing status summary.

[]> releasesmart_license

Feature Name                                  License Authorization Status
1. Content Security Management Centralized          In Compliance
   Tracking
2. Content Security Management Master ISQ           In Compliance
```

show_license

説明

スマート ライセンスのステータスとステータスの概要を表示します。

例：スマート ライセンスのステータス

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.
[]> status
Smart Licensing is: Enabled

Evaluation Period: In Use

Evaluation Period Remaining: 89 days 23 hours 53 minutes
Registration Status: Unregistered

License Authorization Status: Evaluation Mode

Last Authorization Renewal Attempt Status: No Communication Attempted

Product Instance Name: mail.example.com

Transport Settings: Direct (https://smartreceiver.cisco.com/licservice/license)
```

例：スマート ライセンスのステータスの概要

```
example.com> showlicense_smart
Choose the operation you want to perform:
- STATUS- Show overall Smart Licensing status.
- SUMMARY - Show Smart Licensing summary.

[]> summary

FeatureName                          LicenseAuthorizationStatus
Mail Handling                                        In Compliance
Content Security Management Master ISQ               In Compliance
```

CLI コマンドを使用したメンテナンス作業の実行

ここで説明する操作とコマンドを利用すると、セキュリティ管理アプライアンス上でメンテナンスに関連する作業を実行できます。ここでは、次の操作とコマンドについて説明します。

- shutdown
- reboot
- suspend
- suspendtransfers

- 復帰
- resumetransfers
- resetconfig
- version

セキュリティ管理アプライアンスのシャットダウン

セキュリティ管理アプライアンスをシャット ダウンするには、次の手順を実行します。

- [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[シャットダウン/再起動（Shutdown/Reboot）] ページを使用します。

  または

- コマンドライン プロンプトで `shutdown` コマンドを使用します。

アプライアンスをシャットダウンすると、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。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。

セキュリティ管理アプライアンスのリブート

セキュリティ管理アプライアンスをリブートするには、GUI の [システム管理（System Administration）] メニューで利用可能な [シャットダウン/再起動（Shutdown/Reboot）] ページを使用するか、CLI で reboot コマンドを使用します。

アプライアンスをリブートすると、AsyncOS が再起動されるため、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。デフォルト遅延値は 30 秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が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。

セキュリティ管理アプライアンスの停止

システム メンテナンスを実行する場合など、アプライアンスをオフラインにするには、次のコマンドのいずれかを使用します。

コマンド	説明	永続化
suspend	• E メール セキュリティ アプライアンスからセキュリティ管理アプライアンスへの隔離されたメッセージの転送を一時停止します。 • 隔離からリリースされたメッセージの配信を一時停止します。 • 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。	リブート後も永続化されます。
suspendtransfers	管理対象の電子メールおよび Web Security Appliances から Content Security Management Appliance へのレポーティング データおよびトラッキング データの転送を一時停止します。 このコマンドでは、E メール セキュリティ アプライアンスからの隔離されたメッセージの受信も一時停止されます。 バックアップ アプライアンスをプライマリ アプライアンスとして再開するための準備段階でこのコマンドを使用します。	リブート後も維持されます。

これらのコマンドの使用時には、アプライアンスの遅延値を入力する必要があります。デフォルト遅延値は30秒です。AsyncOS では、その遅延値の間はオープン中の接続を完了できます。その遅延値を超えると、オープン中の接続が強制的に閉じられます。オープン中の接続が存在しない場合は、すぐにサービスが停止されます。

suspend または suspendtransfers コマンドで停止したサービスを再アクティブ化するには、resume または resumetransfers コマンドをそれぞれ使用します。

管理アプライアンスの現在のステータス（オンラインまたは一時停止）を特定するには、Web インターフェイスで [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [シャットダウン/再起動（Shutdown/Reboot）] を選択します。

関連項目：

- お使いの E メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプの「Suspending Email Delivery」、「Resuming Email Delivery」、「Suspending Receiving」、および「Resuming Receiving」。

CLI の例：suspend および suspendtransfers コマンド

```
sma.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.
sma.example.com>
sma.example.com> suspendtransfers

Transfers suspended.
sma.example.com>
```

一時停止状態からの再開

resume コマンドは、suspend または suspenddel コマンドの使用後にアプライアンスを通常の動作状態に戻します。

resumetransfers コマンドは、suspendtransfers コマンドの使用後にアプライアンスを通常の動作状態に戻します。

CLI の例：resume および resumetransfers コマンド

```
sma.example.com> resume
Receiving resumed.
Mail delivery resumed.
sma.example.com>
sma.example.com> resumetransfers

Receiving resumed.
Transfers resumed.
sma.example.com>
```

工場出荷時の初期状態への設定のリセット

アプライアンスを物理的に転送するとき、または構成の問題を解決する最後の手段として、工場出荷時の初期状態にアプライアンスをリセットすることもできます。

⚠

注意 設定をリセットすると CLI から切り離すことになり、アプライアンス（FTP、Telnet、SSH、HTTP、HTTPS）への接続に使用しているサービスが無効になり、ユーザーアカウントが削除されます。

目的	操作手順
• 工場出荷時の初期状態へすべての設定をリセット • すべてのレポート カウンタをクリア ただし、 • ログ ファイルを保持 • 隔離メッセージを保持	1. デフォルトの admin ユーザー アカウントとパスフレーズを使用し、シリアル インターフェイスを使用して CLI に接続するかまたはデフォルト設定を使用して管理ポートに接続して、リセット後にアプライアンスに接続できることを確認します。デフォルト設定のアプライアンスへのアクセスの詳細については、セットアップ、インストール、および基本設定を参照してください。 2. アプライアンスのサービスを一時停止します。 3. **[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [設定ファイル（Configuration File）]** を選択し、**[リセット（Reset）]** をクリックします。 （注） リセット後、アプライアンスがオフライン状態に自動的に戻ります。リセット前に電子メールの送信が中断されている場合、配信はリセット後に再試行されます。
• 工場出荷時の初期状態へすべての設定をリセット • すべてのデータを削除	`diagnostic > reload` CLI コマンドを使用します。 **注意** このコマンドは、Cisco ルータまたはスイッチで使用される類似のコマンドと同じではありません。

resetconfig コマンド

```
mail3.example.com> suspend
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

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システム ステータス（System Status）] を選択します。

ステップ 3 ページの下部までスクロールして、[バージョン情報（Version Information）] で、現在インストールされている AsyncOS のバージョンを確認します。

あるいは、コマンドライン プロンプトで **version** コマンドを使用することもできます。

リモート電源再投入の有効化

アプライアンス シャーシの電源をリモートでリセットする機能は、80 および 90 シリーズ ハードウェアでのみ使用できます。

アプライアンスの電源をリモートでリセットする場合は、このセクションで説明されている手順を使用して、この機能を事前に有効にし、設定しておく必要があります。

始める前に

- 専用のリモート電源再投入（RPC）ポートをセキュア ネットワークに直接、ケーブル接続します。詳細については、ご使用のモデルのハードウェア マニュアルを参照してください（資料に記載されている場所から入手できます）。
- ファイアウォールを通過するために必要なポートを開くなど、アプライアンスがリモート アクセス可能であることを確認します。
- この機能を使用するには、専用のリモート電源再投入インターフェイスの一意の IPv4 アドレスが必要です。このインターフェイスは、このセクションで説明されている手順でのみ設定可能です。`ipconfig` コマンドを使用して設定することはできません。
- アプライアンスの電源を再投入するには、Intelligent Platform Management Interface（IPMI）バージョン2.0 をサポートするデバイスを管理できるサードパーティ製ツールが必要です。このようなツールを使用できるように準備されていることを確認します。
- コマンドライン インターフェイスへのアクセスに関する詳細については、CLI のリファレンス ガイドを参照してください。

ステップ 1 SSH、Telnet、またはシリアル コンソール ポートを使用して、コマンドライン インターフェイスにアクセスします。

ステップ 2 管理者権限を持つアカウントを使用してログインします。

ステップ 3 以下のコマンドを入力します。

```
remotepower
setup
```

ステップ 4 プロンプトに従って、以下の情報を指定します。

- この機能専用の IP アドレスと、ネットマスクおよびゲートウェイ。
- 電源の再投入コマンドを実行するために必要なユーザー名とパスフレーズ。

これらのクレデンシャルは、アプライアンスへのアクセスに使用する他のクレデンシャルに依存しません。

ステップ 5 commit を入力して変更を保存します。

ステップ 6 設定をテストして、アプライアンスの電源をリモートで管理できることを確認します。

ステップ 7 入力したクレデンシャルが、将来、いつでも使用できることを確認します。たとえば、この情報を安全な場所に保管し、このタスクを実行する必要がある管理者が、必要なクレデンシャルにアクセスできるようにします。

次のタスク

アプライアンスの電源のリモート リセット

SNMP を使用したシステムの状態のモニタリング

AsyncOS は、Simple Network Management Protocol（SNMP）バージョン v1、v2、および v3 を使用したシステム ステータスのモニタリングをサポートします。

- SNMP を有効にし、設定するには、コマンドライン インターフェイスで `snmpconfig` コマンドを使用します。
- MIB は http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html から入手できます（使用可能な最新ファイルを使用）。
- このサービスをイネーブルにするには、パスフレーズ認証と DES 暗号化を伴う SNMPv3 の使用が必須です。（SNMPv3 の詳細については、RFC 2571 ～ 2575 を参照してください）。SNMP システム ステータスのモニタリングをイネーブルにするには、少なくとも 8 文字の SNMPv3 パスフレーズを設定する必要があります。最初に SNMPv3 パスフレーズを入力するときは、確認のためにそのパスフレーズを再入力する必要があります。次に `snmpconfig` コマンドを実行するときは、コマンドにこのフレーズが「記憶」されています。
- 接続をモニタするように SNMP を設定する場合：

  connectivityFailure SNMP トラップの設定時に url-attribute を入力する場合、URL がディレクトリまたはファイルのいずれを指すかを決定します。

  - ディレクトリの場合は、末尾にスラッシュ（/）を追加します。
  - ファイルの場合は、末尾にスラッシュを追加しません。

- AsyncOS での SNMP の使用の詳細については、Web または Email Security Appliance のオンライン ヘルプを参照してください。

例：snmpconfig コマンド

```
sma.example.com> snmpconfig
```

```
Current SNMP settings:
SNMP Disabled.
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]> SETUP
Do you want to enable SNMP?
[Y]>
Please choose an IP interface for SNMP requests.
1. Management (198.51.100.1: sma.example.com)
[1]>
Which port shall the SNMP daemon listen on interface "Management"?
[161]>
Please select SNMPv3 authentication type:
1. MD5
2. SHA
[1]> 2
Please select SNMPv3 privacy protocol:
1. DES
2. AES
[1]> 2
Enter the SNMPv3 authentication passphrase.
[]>
Please enter the SNMPv3 authentication passphrase again to confirm.
[]>
Enter the SNMPv3 privacy passphrase.
[]>
Please enter the SNMPv3 privacy passphrase again to confirm.
[]>
Service SNMP V1/V2c requests?
[N]> Y
Enter the SNMP V1/V2c community string.
[ironport]> public
Shall SNMP V2c requests be serviced from IPv4 addresses?
[Y]>
From which IPv4 networks shall SNMP V1/V2c requests be allowed? Separate
multiple networks with commas.
[127.0.0.1/32]>
Enter the Trap target as a host name, IP address or list of IP
addresses separated by commas (IP address preferred). Enter "None" to disable traps.
[127.0.0.1]> 203.0.113.1
Enter the Trap Community string.
[ironport]> tcomm
Enterprise Trap Status
1. CPUUtilizationExceeded       Disabled
2. FIPSModeDisableFailure       Enabled
3. FIPSModeEnableFailure        Enabled
4. FailoverHealthy              Enabled
5. FailoverUnhealthy            Enabled
6. RAIDStatusChange             Enabled
7. connectivityFailure          Disabled
8. fanFailure                   Enabled
9. highTemperature              Enabled
10. keyExpiration               Enabled
11. linkUpDown                  Enabled
12. memoryUtilizationExceeded   Disabled
13. powerSupplyStatusChange     Enabled
14. resourceConservationMode    Enabled
15. updateFailure               Enabled
Do you want to change any of these settings?
[N]> Y
Do you want to disable any of these traps?
[Y]> n
Do you want to enable any of these traps?
[Y]> y
```

```
Enter number or numbers of traps to enable.  Separate multiple numbers with
commas.
[]> 1,7,12
What threshold would you like to set for CPU utilization?
[95]>
What URL would you like to check for connectivity failure?
[http://downloads.ironport.com]>
What threshold would you like to set for memory utilization?
[95]>
Enter the System Location string.
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #30, position 3
Enter the System Contact string.
[snmp@localhost]> SMA.Administrator@example.com
Current SNMP settings:
Listening on interface "Management" 198.51.100.1  port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 127.0.0.1/32 .
SNMP v1/v2 Community String: public
Trap target: 203.0.113.1
Location: Network Operations Center - west; rack #30, position 3
System Contact: SMA.Administrator@example.com
Choose the operation you want to perform:
- SETUP - Configure SNMP.
[]>
sma.example.com> commit
Please enter some comments describing your changes:
[]> Enable and configure SNMP
Changes committed: Fri Nov 06 18:13:16 2015 GMT
sma.example.com>
```

セキュリティ管理アプライアンスのデータのバックアップ

バックアップされるデータ

すべてのデータをバックアップすること、または次のデータの任意の組み合わせをバックアップすることを選択できます。

- メッセージ、メタデータを含むスパム隔離
- メッセージおよびメタデータを含んでいる集約されたポリシー、ウイルス、およびアウトブレイク隔離
- メッセージ、メタデータを含む電子メール トラッキング（メッセージ トラッキング）
- Web トラッキング
- レポーティング（電子メールおよび Web）
- セーフリスト/ブロックリスト

データの転送が完了すると、2 つのアプライアンスのデータが同一になります。

この処理を行っても、設定とログはバックアップされません。これらの項目をバックアップする方法については、その他の重要なバックアップ タスク （30 ページ）を参照してください。

最初のバックアップ後の各バックアップは、前回のバックアップ後に生成された情報のみをコピーします。

バックアップの制約事項および要件

バックアップをスケジュール設定する前に、次の制約事項および要件を考慮してください。

制約事項	要件
AsyncOS バージョン	ソース セキュリティ管理アプライアンスおよびターゲット セキュリティ管理アプライアンスの AsyncOS バージョンが同じである必要があります。バージョンの非互換性がある場合、バックアップをスケジュールする前に、同じリリースにアプライアンスをアップグレードします。
ネットワーク上のターゲット アプライアンス	ターゲット アプライアンスがネットワーク上に設定されている必要があります。 ターゲット アプライアンスが新規の場合は、システム セットアップ ウィザードを実行して必要な情報を入力します。手順については、セットアップ、インストール、および基本設定を参照してください。

制約事項	要件
ソース アプライアンスとターゲット アプライアンス間の通信	ソースおよびターゲットのセキュリティ管理アプライアンスは、SSH を使用して通信できるようになっている必要があります。したがって、次のようにします。 • 両方のアプライアンスのポート 22 を開いておく必要があります。デフォルトでは、このポートはシステム セットアップ ウィザードを実行すると開きます。 • ドメイン ネーム サーバ（DNS）で、A レコードと PTR レコードの両方を使用して、両方のアプライアンスのホスト名を解決できる必要があります。
ターゲット アプライアンスを停止する必要があります。	プライマリ アプライアンスのみが、管理対象の電子メールおよび Web Security Appliances からデータを取得する必要があります。確実に実行するために、ターゲット アプライアンスによる管理対象アプライアンスからのデータの直接取得の防止 （27 ページ）を参照してください。 また、バックアップ アプライアンスでスケジュール設定されている設定公開ジョブをキャンセルしてください。
アプライアンス キャパシティ	ターゲットアプライアンスのディスク領域キャパシティが、ソース アプライアンスのキャパシティと同等以上である必要があります。ターゲットアプライアンスで各データ タイプ（レポーティング、トラッキング、隔離など）に割り当てるディスク領域は、ソース アプライアンスの対応する割り当てより少なくすることはできません。 各データ タイプのすべてのデータのバックアップに十分なスペースがターゲット アプライアンス上にあれば、大きいソースから小さいターゲットセキュリティ管理アプライアンスへのバックアップをスケジュール設定できます。ソースアプライアンスがターゲットアプライアンスよりも大きい場合、ターゲット アプライアンスで使用可能な領域に合わせて、ソース アプライアンスで割り当てられている領域を削減します。 ディスク領域の割り当てとキャパシティを表示および管理するには、ディスク領域の管理 （79 ページ）を参照してください。 仮想アプライアンスのディスク容量については、『Cisco Content Security Virtual Appliance Installation Guide』を参照してください。

制約事項	要件
複数、同時、およびチェーン バックアップ	バックアップ プロセスは一度に 1 つだけ実行できます。前のバックアップが完了する前に実行がスケジュールされているバックアップはスキップされ、警告が送信されます。 セキュリティ管理アプライアンスからのデータは、単一のセキュリティ管理アプライアンスにバックアップできます。 チェーン バックアップ（バックアップへのバックアップ）はサポートされていません。

バックアップ期間

最初の完全バックアップでは、800GB のバックアップに最大 10 時間かかります。毎日のバックアップは、それぞれ最大3時間かかります。毎週または毎月のバックアップはより長くかかる場合があります。これらの数は場合によって異なります。

初期バックアップ後のバックアップ プロセスでは、最後のバックアップから変更されたファイルのみが転送されます。このため、その後のバックアップにかかる時間は初期バックアップの場合よりも短くなります。後続のバックアップに必要な時間は、累積されたデータ量、変更されたファイル数、および最後のバックアップ以降どの程度のファイルが変更されたかによって異なります。

バックアップ中のサービスのアベイラビリティ

セキュリティ管理アプライアンスをバックアップすると、「ソース」セキュリティ管理アプライアンスから「ターゲット」セキュリティ管理アプライアンスにアクティブ データ セットがコピーされます。このとき、コピー元の「ソース」アプライアンスの中断は最小限に抑えられます。

バックアップ プロセスのフェーズと、それらがサービスのアベイラビリティに及ぼす影響は次のとおりです。

- フェーズ 1：バックアップ プロセスのフェーズ 1 は、ソース アプライアンスとターゲット アプライアンス間のデータの転送で開始されます。データの転送中、ソース アプライアンスでのサービスは実行されたままになるため、データ収集をそのまま継続できます。ただし、ターゲット アプライアンスではサービスがシャットダウンされます。ソースからターゲット アプライアンスへのデータの転送が完了すると、フェーズ 2 が開始されます。
- フェーズ 2：フェーズ 2 が始まると、ソース アプライアンスでサービスがシャットダウンされます。最初のシャットダウン以降、ソース アプライアンスとターゲット アプライアンス間でのデータ転送中に収集された相違点がターゲット アプライアンスにコピーされ、ソース アプライアンスとターゲット アプライアンスの両方で、サービスがバックアップ開始時の状態に戻ります。これにより、ソース アプライアンス上で最大の稼働時間を維持でき、いずれかのアプライアンスのデータが損失することがなくなります。

バックアップ中に、データ アベイラビリティ レポートが機能しなくなる場合があります。また、メッセージ トラッキング結果を表示すると、各メッセージのホスト名に「未解決（unresolved）」というラベルが付くことがあります。

レポートをスケジュール設定しようとしているときに、バックアップが進行中であることを忘れていた場合は、[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] を選択して、システムのステータスを確認できます。このウィンドウでは、ページの上部にシステムのバックアップが進行中であるという警告が表示されます。

バックアップ プロセスの中断

（注） バックアップの実行中にソース アプライアンスの予期しないリブートがあっても、ターゲット アプライアンスはこの停止を認識しません。ターゲット アプライアンスでバックアップをキャンセルする必要があります。

バックアッププロセスの中断があり、そのバックアッププロセスが完了していない場合、バックアップを次に試行したときに、セキュリティ管理アプライアンスは停止した部分からバックアップ プロセスを開始できます。

進行中のバックアップをキャンセルすることは推奨されません。これは、既存のデータが不完全になり、エラーが発生した場合は、次のバックアップが完了するまで使用できないことがあります。進行中のバックアップのキャンセルが必要な場合は、できるだけ早く完全バックアップを実行し、常に使用可能な現在のバックアップを確保してください。

ターゲットアプライアンスによる管理対象アプライアンスからのデータの直接取得の防止

ステップ 1 ターゲットアプライアンスのコマンドラインインターフェイスにアクセスします。この説明については、コマンドライン インターフェイスへのアクセス を参照してください。

ステップ 2 `suspendtransfers` コマンドを実行します。

ステップ 3 プロンプトが再表示されるまで待ちます。

ステップ 4 `suspend` コマンドを実行します。

ステップ 5 プロンプトが再表示されるまで待ちます。

ステップ 6 ターゲット アプライアンスのコマンドライン インターフェイスを終了します。

バックアップ ステータスに関するアラートの受信

バックアップの完了時に問題を通知するアラートを受信するには、タイプが [システム（System）] で重大度が [情報（Info）] のアラートを送信するようにアプライアンスを設定します。アラートの管理 （52 ページ） を参照してください。

単一または定期バックアップのスケジュール設定

単一または定期バックアップを事前設定した時間に行うようにスケジュール設定できます。

（注） リモート マシンに実行中のバックアップがある場合、バックアップ プロセスは開始されません。

始める前に

- バックアップの制約事項および要件 （24 ページ）の項目に対処します。
- バックアップ プロセスを開始する前に、ターゲット アプライアンスで一時的に二要素認証を無効にするかどうかを確認します。バックアップ プロセスが完了すると、ターゲット アプライアンスの二要素認証を有効にできます。

ステップ 1 ソース アプライアンスのコマンドライン インターフェイスに、管理者としてログインします。

ステップ 2 コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステップ 3 ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4 **Schedule** と入力して、Enter を押します。

ステップ 5 ターゲット セキュリティ管理アプライアンスの IP アドレスを入力します。

ステップ 6 ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7 ターゲット アプライアンスの管理ユーザの名前およびパスフレーズを入力します。

ステップ 8 バックアップするデータに関するプロンプトに応答します。

ステップ 9 単一バックアップをスケジュール設定するには、Schedule a single backup に **2** を入力して、Enter を押します。

ステップ 10 定期バックアップをスケジュール設定する場合は、次の手順を実行します。

a) 繰り返しバックアップをスケジュール設定するには、**1** を入力して、Enter を押します。

b) 定期バックアップの頻度を選択し、Enter を押します。

ステップ 11 バックアップを開始する特定の日付または日および時間を入力して、Enter を押します。

ステップ 12 バックアップ プロセスの名前を入力します。

ステップ 13 バックアップが正常にスケジュール設定されたことを確認します。コマンド プロンプトで **View** と入力して、Enter を押します。

ステップ 14 その他の重要なバックアップ タスク （30 ページ）も参照してください。

即時バックアップの開始

（注） ターゲット マシンでバックアップが実行中の場合、バックアップ プロセスは開始されません。

始める前に

バックアップの制約事項および要件 （24 ページ）のすべての要件を満たします。

ステップ 1 ソース アプライアンスのコマンドライン インターフェイスに、管理者としてログインします。

ステップ 2 コマンド プロンプトで `backupconfig` と入力し、Enter を押します。

ステップ 3 ソース アプライアンスおよびターゲット アプライアンス間の接続が低速である場合は、データ圧縮をオンにします。

setup と入力して、Y を押します。

ステップ 4 **Schedule** と入力して、Enter を押します。

ステップ 5 ターゲット セキュリティ管理アプライアンスの IP アドレスを入力します。

ステップ 6 ターゲット アプライアンスを識別する有効な名前を入力します（最大 20 文字）。

ステップ 7 ターゲット アプライアンスの管理ユーザの名前およびパスフレーズを入力します。

ステップ 8 バックアップするデータに関するプロンプトに応答します。

ステップ 9 単一バックアップをすぐに開始するため、**3** を入力して Enter を押します。

ステップ 10 バックアップ ジョブの有効な名前を入力します。

バックアップ プロセスが数分で開始されます。

ステップ 11 （任意）バックアップの進捗状況を表示するには、コマンドライン プロンプトで **Status** と入力します。

ステップ 12 その他の重要なバックアップ タスク （30 ページ）も参照してください。

バックアップ ステータスの確認

ステップ 1 プライマリ アプライアンスのコマンドライン インターフェイスに、管理者としてログインします。

ステップ 2 コマンド プロンプトで **backupconfig** と入力し、Enter を押します。

ステータスの確認対象	操作手順
スケジュール設定されたバックアップ	View 操作を選択します。
進行中のバックアップ	Status 操作を選択します。 アラートを設定している場合は、電子メールを確認するか、最新アラートの表示 （54 ページ）を参照してください。

次のタスク

関連項目

ログ ファイルのバックアップ情報 （30 ページ）

ログ ファイルのバックアップ情報

バックアップ ログはバックアップ プロセスを開始から終了まで記録します。

バックアップ スケジューリングに関する情報は、SMA ログ内にあります。

関連項目

- バックアップ ステータスの確認 （29 ページ）

その他の重要なバックアップ タスク

ここで説明されているバックアップ プロセスではバックアップされない項目が失われることを防止するため、およびアプライアンスの障害が発生した場合にセキュリティ管理アプライアンスの交換を速めるため、次のことを検討してください。

- プライマリ セキュリティ管理アプライアンスから設定を保存するには、設定の保存とインポート （70 ページ）を参照してください。プライマリ セキュリティ管理アプライアンスとは別の安全な場所にコンフィギュレーション ファイルを保存します。
- Configuration Master の設定に使用した、Web 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 ファイルをすべて保存します。
- セキュリティ管理アプライアンスから別の場所にログ ファイルを保存する方法については、ログ サブスクリプションを参照してください。

さらに、バックアップ ログのログ サブスクリプションを設定できます。GUI でのログ サブスクリプションの作成 を参照してください。

バックアップ アプライアンスのプライマリ アプライアンスとしての使用

アプライアンス ハードウェアをアップグレードする場合、またはその他の理由でアプライアンスを切り替える場合は、次の手順を使用します。

始める前に

セキュリティ管理アプライアンスのデータのバックアップ （23 ページ）の情報を確認してください。

ステップ 1 旧/プライマリ/ソース アプライアンスのコンフィギュレーション ファイルのコピーを、新しいアプライアンスから到達できる場所に保存します。設定の保存とインポート （70 ページ）を参照してください。

ステップ 2 新規/バックアップ/ターゲット アプライアンスでシステム セットアップ ウィザードを実行します。

ステップ 3 バックアップの制約事項および要件 （24 ページ）の要件を満たします。

ステップ 4 旧/プライマリ/ソース アプライアンスからバックアップを実行します。即時バックアップの開始 （29 ページ）の手順を参照してください。

ステップ 5 バックアップが完了するまで待ちます。

ステップ 6 旧/プライマリ/ソース アプライアンスで suspendtransfers および suspend コマンドを実行します。

ステップ 7 2 番目のバックアップを実行して、旧/プライマリ/ソース アプライアンスから新規/バックアップ/ターゲット アプライアンスに直前のデータを転送します。

ステップ 8 コンフィギュレーション ファイルを新規/バックアップ/ターゲット アプライアンスにインポートします。

ステップ 9 新規/バックアップ/ターゲット アプライアンスで resumetransfers および resume コマンドを実行します。

旧/元プライマリ/ソース アプライアンスでこのコマンドを実行しないでください。

ステップ 10 新規/バックアップ/ターゲット アプライアンスと管理対象の電子メールおよび Web Security Appliances の間の接続を確立します。

ステップ 11
a) （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。
b) **[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）]** を選択します。
c) アプライアンス名をクリックします。
d) **[接続の確立（Establish Connection）]** ボタンをクリックします。
e) **[テスト接続（Test Connection）]** をクリックします。
f) アプライアンスのリストに戻ります。
g) 管理対象の各アプライアンスに対して、この手順を繰り返します。

ステップ 12 新規/ターゲット アプライアンスがプライマリ アプライアンスとして機能していることを確認します。

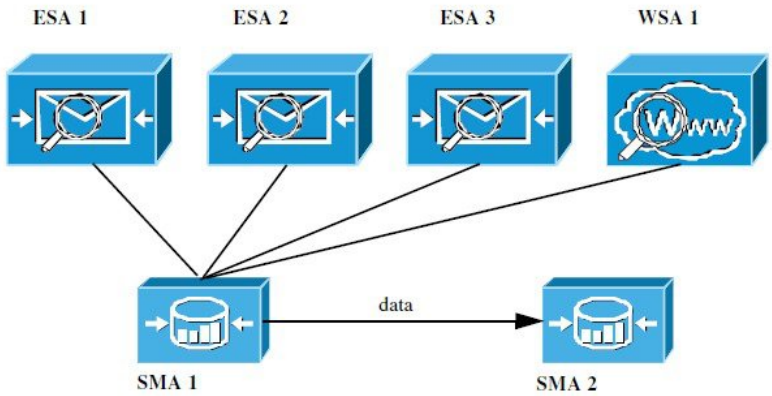
[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [システムステータス（System Status）] を選択し、データ転送の状態を確認します。

セキュリティ管理アプライアンスでのディザスタ リカバリ

セキュリティ管理アプライアンスが予期せず失敗した場合は、次の手順を使用して、セキュリティ管理サービスおよびバックアップしたデータを復元します。これはセキュリティ管理アプライアンスのデータのバックアップ （23 ページ）の情報を使用して定期的に保存しています。

典型的なアプライアンス設定は、次の図に示すようになります。

図 *1*: ディザスタ リカバリ：一般的な環境



この環境で、SMA 1 は ESA 1 ～ 3 および WSA 1 からデータを受信しているプライマリ セキュリティ管理アプライアンスです。SMA 2 は SMA1 からバックアップ データを受信しているバックアップ セキュリティ管理アプライアンスです。

失敗した場合は、SMA 2 がプライマリ セキュリティ管理アプライアンスになるように設定する必要があります。

SMA 2 を新しいプライマリ セキュリティ管理アプライアンスとして設定し、サービスを復元するには、次の手順を実行します。

手順

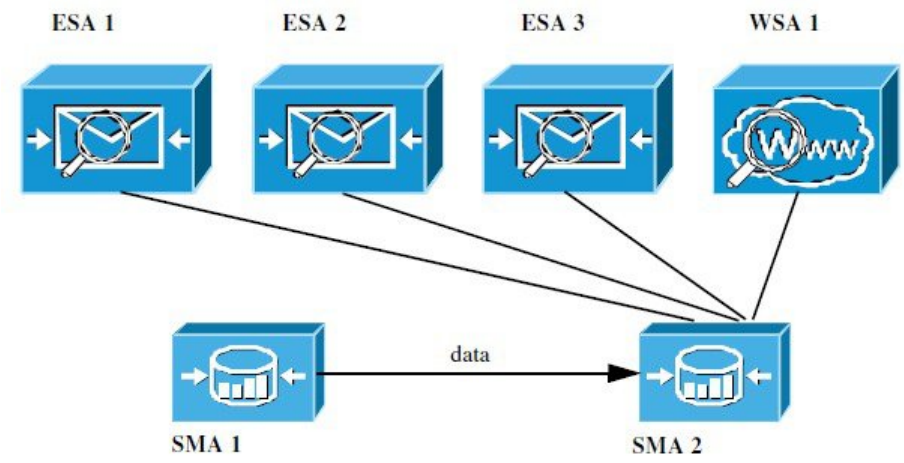
	コマンドまたはアクション	目的
ステップ 1	集約ポリシー、ウイルス、およびアウトブレイク隔離を使用している場合は以下を実行します。 • 各 E メール セキュリティ アプライアンスで、集約隔離を無効にします。	E メール セキュリティ アプライアンスのマニュアルで集約されたポリシー、ウイルス、およびアウトブレイク隔離を無効にする方法を参照してください。 これは各 E メール セキュリティ アプライアンスで内部隔離を作成し、それを後で新しいセキュリティ管理アプライアンスに移行します。

	コマンドまたはアクション	目的
ステップ 2	プライマリ セキュリティ管理アプライアンス（SMA1）から保存した設定ファイルを、バックアップセキュリティ管理アプライアンス（SMA2）にロードします。	コンフィギュレーション ファイルのロード（72ページ）を参照してください。
ステップ 3	障害が発生した SMA 1 から IP アドレスを再作成し、SMA 2 の IP アドレスに設定します。	1. SMA 2 で、[ネットワーク（Network）]>[IPインターフェイス（IP Interfaces）]>[IPインターフェイスの追加（Add IP Interfaces）] を選択します。 2. [IPインターフェイスの追加（Add IP Interfaces）] ページで、障害が発生した SMA1 のすべての関連 IP 情報をテキスト フィールドに入力して、SMA 2 のインターフェイスを再作成します。 IP インターフェイスの追加の詳細については、IP インターフェイスの設定を参照してください。
ステップ 4	変更を送信し、保存します。	
ステップ 5	新しいセキュリティ管理アプライアンス（SMA 2）で、適用可能なすべての中央集中型サービスを有効にします。	セキュリティ管理アプライアンスでのサービスの設定を参照してください。
ステップ 6	すべてのアプライアンスを新しいセキュリティ管理アプライアンス（SMA 2）に追加します。 • アプライアンスへの接続を確立し、その接続をテストすることで、各アプライアンスがイネーブルとなり、機能していることをテストして確認します。	管理対象アプライアンスの追加についてを参照してください。
ステップ 7	集約ポリシー、ウイルス、およびアウトブレイク隔離を使用している場合、新しいセキュリティ管理アプライアンス上に隔離の移行を設定し、その後必要な E メール セキュリティ アプライアンスごとに移行を有効にして設定します。	ポリシー、ウイルス、およびアウトブレイク隔離の集約を参照してください。
ステップ 8	必要に応じて、追加データを復元します。	その他の重要なバックアップ タスク （30 ページ）を参照してください。

次のタスク

このプロセスが完了した後、SMA 2 がプライマリ セキュリティ管理アプライアンスになります。これで、次の図に示すように、ESA 1 ～ 3 と WSA 1 からもすべてのデータが SMA 2 に送られるようになりました。

図 *2:* ディザスタ リカバリ：最終結果



アプライアンス ハードウェアのアップグレード

バックアップ アプライアンスのプライマリ アプライアンスとしての使用 （31 ページ） を参照してください。

AsyncOS のアップグレード

アップグレード用のバッチ コマンド

アップグレード手順用のバッチ コマンドの詳細については、AsyncOS for Email の CLI リファレンス ガイドを参照してください http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html

アップグレードとアップデートのネットワーク要件の決定

Cisco コンテンツ セキュリティ アプライアンスのアップデート サーバは、ダイナミック IP アドレスを使用します。ファイアウォール ポリシーを厳しく設定している場合、AsyncOS アッ

プグレードに対して静的な参照先を設定する必要がある場合があります。アップグレードに関して、ファイアウォール設定にスタティック IP が必要であると判断した場合は、Cisco カスタマー サポートに連絡して、必要な URL アドレスを取得してください。

（注） 既存のファイアウォール ルールで upgrades.cisco.com ポート（22、25、80、4766 など）からのレガシー アップグレードのダウンロードが許可されている場合は、それらを削除するか、修正したファイアウォール ルールに置き換える必要があります。

アップグレード方式の選択：リモートまたはストリーミング

Cisco はアプライアンスでの AsyncOS のアップグレード用に、以下の 2 種類の方法（または「ソース」）を提供しています。

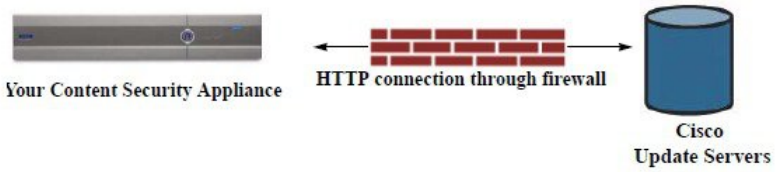
- ストリーミング アップグレード：各アプライアンスは Cisco コンテンツ セキュリティ アップグレード サーバから HTTP を介して AsyncOS アップグレードを直接ダウンロードします。
- リモート アップグレード：Cisco からアップグレード イメージを 1 回だけダウンロードし、アプライアンスに保存します。次に、アプライアンスは、ネットワーク内のサーバから AsyncOS アップグレードをダウンロードします。

アップグレードおよびサービス アップデートの設定 （38 ページ）にある、アップグレード方式を設定します。オプションで、CLI で **updateconfig** コマンドを使用します。

ストリーミング アップグレードの概要

ストリーミング アップグレードでは、各 Cisco コンテンツ セキュリティ アプライアンスが直接 Cisco コンテンツ セキュリティ アップデート サーバーに接続して、アップグレードを検索してダウンロードします。

図 *3:* ストリーミング アップデートの方法



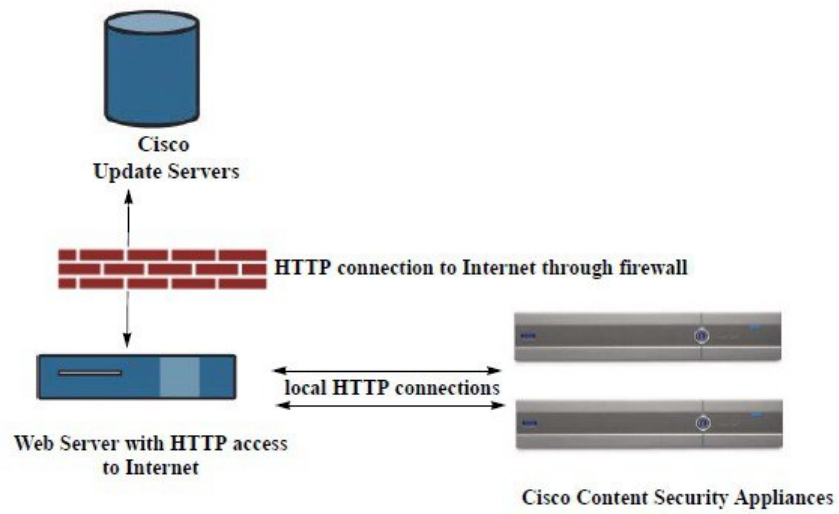
この方式では、アプライアンスが Cisco コンテンツ セキュリティ アップデート サーバーにネットワークから直接接続する必要があります。

リモート アップグレードの概要

また、Cisco アップデート サーバから直接アップデートを取得する（ストリーミング アップグレード）のではなく、ネットワーク内からローカルで AsyncOS にアップデートをダウンロードおよびホストする（リモート アップグレード）こともできます。この機能を使用して、イン

ターネットにアクセスできるネットワーク上のすべてのサーバにHTTPで暗号化されたアップデート イメージをダウンロードします。アップデート イメージをダウンロードする場合は、内部HTTPサーバ（アップデートマネージャ）を設定し、セキュリティ管理アプライアンスでAsyncOSイメージをホスティングできます。

図 *4*: リモート アップデートの方法



基本的なプロセスは、次のとおりです。

ステップ 1 リモート アップグレードのハードウェア要件およびソフトウェア要件 （37 ページ）およびリモート アップグレード イメージのホスティング （37 ページ）の情報をお読みください。

ステップ 2 アップグレード ファイルを取得および供給するようにローカル サーバを設定します。

ステップ 3 アップグレード ファイルをダウンロードします。

ステップ 4 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 5 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定の選択（Update SettingsChoose）] を選択します。

このページで、ローカル サーバを使用するようにアプライアンスを設定することを指定します。

ステップ 6 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システムのアップグレード（System Upgrade）] を選択します

ステップ 7 [利用可能なアップグレード（Available Upgrades）] をクリックします。

（注） コマンドライン プロンプトから **updateconfig** コマンドを実行し、次に **upgrade** コマンドを実行することもできます。

詳細については、AsyncOS のアップグレード （34 ページ）を参照してください。

リモート アップグレードのハードウェア要件およびソフトウェア要件

AsyncOS アップグレード ファイルのダウンロードでは、次の要件を備えた内部ネットワークにシステムを構築する必要があります。

- Cisco コンテンツ セキュリティ アプライアンスのアップデート サーバへのインターネット アクセス。
- Web ブラウザ。

（注） 今回のリリースでアップデート サーバのアドレスへの HTTP アクセスを許可するファイアウォール設定値を設定する必要がある場合、特定の IP アドレスではなく DNS 名を使用する必要があります。

AsyncOS アップデート ファイルのホスティングでは、次の要件を備えた内部ネットワークにサーバを構築する必要があります。

- Web サーバ。たとえば、次のような Microsoft IIS（Internet Information Services）または Apache オープン ソース サーバ。
  - 24 文字を超えるディレクトリまたはファイル名の表示をサポートしていること
  - ディレクトリの参照ができること
  - 匿名認証（認証不要）または基本（「シンプル」）認証用に設定されていること
  - 各 AsyncOS アップデート イメージ用に最低 350 MB 以上の空きディスク領域が存在すること

リモート アップグレード イメージのホスティング

ローカル サーバの設定が完了したら、**http://updates.ironport.com/fetch_manifest.html** にアクセスしてアップグレード イメージの zip ファイルをダウンロードします。イメージをダウンロードするには、Cisco コンテンツ セキュリティ アプライアンスのシリアル番号とバージョン番号を入力します。利用可能なアップグレードのリストが表示されます。アップグレード イメージの zip ファイルをダウンロードするアップグレード バージョンをクリックします。AsyncOS アップグレードのアップグレード イメージを使用するには、ローカル サーバの基本 URL を [更新設定を編集（Edit Update Settings）] ページに入力します（または CLI の updateconfig を使用します）。

ネットワーク上の Cisco コンテンツ セキュリティ アプライアンスに使用可能なアップグレードを、http://updates.ironport.com/fetch_manifest.html で選択したバージョンに限定する XML ファイルを、ローカル サーバでホスティングすることもできます。この場合でも、Cisco コンテンツ セキュリティ アプライアンスはアップグレードをシスコ サーバからダウンロードします。アップグレード リストをローカル サーバにホスティングする場合は、zip ファイルをダウンロードして、asyncos/phoebe-my-upgrade.xml ファイルをローカル サーバのルート ディレクトリに展開します。AsyncOS アップグレードのアップグレード リストを使用するには、XML ファイルの完全 URL を [更新設定を編集（Edit Update Settings）] ページに入力します（または CLI の updateconfig を使用します）。

リモートアップグレードの詳細については、ナレッジベース（ナレッジベースの記事を参照）を確認するか、サポート プロバイダーにお問い合わせください。

リモート アップグレード方式における重要な違い

ストリーミング アップグレード方式と比較して、AsyncOS をローカル サーバーからアップグレード（リモートアップグレード）する場合には、次の違いがあることに注意してください。

- ダウンロード中に、アップグレードによるインストールがすぐに実行されます。
- アップグレード プロセスの最初の 10 秒間、バナーが表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

アップグレードおよびサービス アップデートの設定

Cisco コンテンツ セキュリティ アプライアンスがセキュリティ サービス アップデート（時間帯ルールなど）および AsyncOS アップグレードをダウンロードする方法を設定できます。たとえば、イメージを利用できる場所にシスコ サーバまたはローカル サーバのどちらからアップグレードおよびアップデートを動的にダウンロードするかを選択したり、アップデート間隔を設定したり、自動アップデートを無効にしたりすることができます。

AsyncOS は、新しい AsyncOS アップグレードを除く、すべてのセキュリティ サービス コンポーネントへの新しいアップデートがないか、定期的にアップデート サーバに問い合わせます。AsyncOS をアップグレードするには、AsyncOS が使用可能なアップグレードを問い合わせるよう、手動で要求する必要があります。

アップグレードおよびアップデート設定は、GUI（次の 2 つの項を参照）で、または CLI で updateconfig コマンドを使用して設定できます。

アップグレード通知を設定することもできます。

アップグレードとアップデートの設定

次の表に、設定可能なアップデートおよびアップグレード設定を示します。

表 *1*: セキュリティ サービスのアップデート設定

設定	説明
アップデート サーバ（イメージ）（Update Servers (images)）	シスコ サーバまたはローカル Web サーバのどちらから、AsyncOS アップグレードおよびサービス アップデート ソフトウェア イメージ（時間帯ルールや機能キーのアップデートなど）をダウンロードするかを選択します。デフォルトでは、アップグレードおよびアップデートの両方でシスコ サーバが選択されます。 次の場合、ローカル Web サーバを使用する場合があります。 • スタティック アドレスからアプライアンスにイメージをダウンロードする必要がある。厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定 （40 ページ）を参照してください。 • 適宜、アプライアンスに AsyncOS アップグレード イメージをダウンロードする（この場合でも、Cisco アップデート サーバからサービス アップデート イメージを動的にダウンロードできます）。 ローカル アップデート サーバを選択した場合は、アップグレードおよびアップデートのダウンロードに使用するサーバのベース URL とポート番号を入力します。サーバが認証を必要とする場合、有効なユーザ名とパスフレーズも入力します。 詳細については、アップグレード方式の選択：リモートまたはストリーミング （35 ページ）およびリモート アップグレードの概要 （35 ページ）を参照してください。
アップデートサーバ（リスト）（Update Servers (lists)）	利用可能なアップグレードおよびサービス アップデートのリスト（マニフェスト XML ファイル）を、シスコ サーバとローカル Web サーバのどちらからダウンロードするかを選択します。 アップグレードおよびアップデートの両方で、デフォルトはシスコ サーバです。アップグレードとアップデートには、それぞれ異なる設定を選択できます。 該当する場合は、厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定 （40 ページ）を参照してください。 ローカル アップデート サーバを選択した場合、サーバのファイル名およびポート番号を含む、各リストのマニフェスト XML ファイルのフル パスを入力します。ポートのフィールドを空のままにした場合、AsyncOS はポート 80 を使用します。サーバが認証を必要とする場合、有効なユーザ名とパスフレーズも入力します。 詳細については、アップグレード方式の選択：リモートまたはストリーミング （35 ページ）およびリモート アップグレードの概要 （35 ページ）を参照してください。
自動更新	時間帯ルールの自動アップデートをイネーブルにするかどうかを選択します。イネーブルにする場合は、アップデートを確認する間隔を入力します。分の場合は **m**、時間の場合は **h**、日の場合は **d** を末尾に追加します。

設定	説明
インターフェイス（**Interface**）	時間帯ルールやAsyncOSアップグレードなどをアップデート サーバに問い合わせるときに、どのネットワーク インターフェイスを使用するかを選択します。利用可能なプロキシデータ インターフェイスが表示されます。デフォルトでは、アプライアンスは使用するインターフェイスを選択します。
HTTP プロキシ サーバ（HTTP Proxy Server）	アップストリームの HTTP プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスフレーズをここに入力します。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。 このプロキシ サーバは、クラウドからファイル分析レポートの詳細を取得するためにも使用されます。ファイル分析レポートの詳細の要件（Web レポート）、またはファイル分析レポートの詳細の要件（電子メール レポート）も参照してください。
HTTPS プロキシ サーバ（HTTPS Proxy Server）	アップストリームの HTTPS プロキシ サーバが存在し、認証が必要な場合は、サーバ情報、ユーザ名、およびパスフレーズをここに入力します。 プロキシ サーバを指定すると、GUI にリストされているサービスへのアクセスおよびアップデートにそれが使用されます。 このプロキシ サーバは、クラウドからファイル分析レポートの詳細を取得するためにも使用されます。ファイル分析レポートの詳細の要件（Web レポート）、またはファイル分析レポートの詳細の要件（電子メール レポート）も参照してください。

厳格なファイアウォール ポリシーを適用している環境のスタティック アップグレードおよびアップデート サーバ設定

AsyncOS アップデート サーバは、ダイナミック IP アドレスを使用します。環境にスタティック IP アドレスが必要な厳格なファイアウォール ポリシーを適用している場合は、[アップデート設定（Update Settings）] ページで次の設定を使用します。

図 *5 : [*アップデートサーバ*(*イメージ*)*（***Update Servers (images)***）*]*設定のスタティック ***URL***

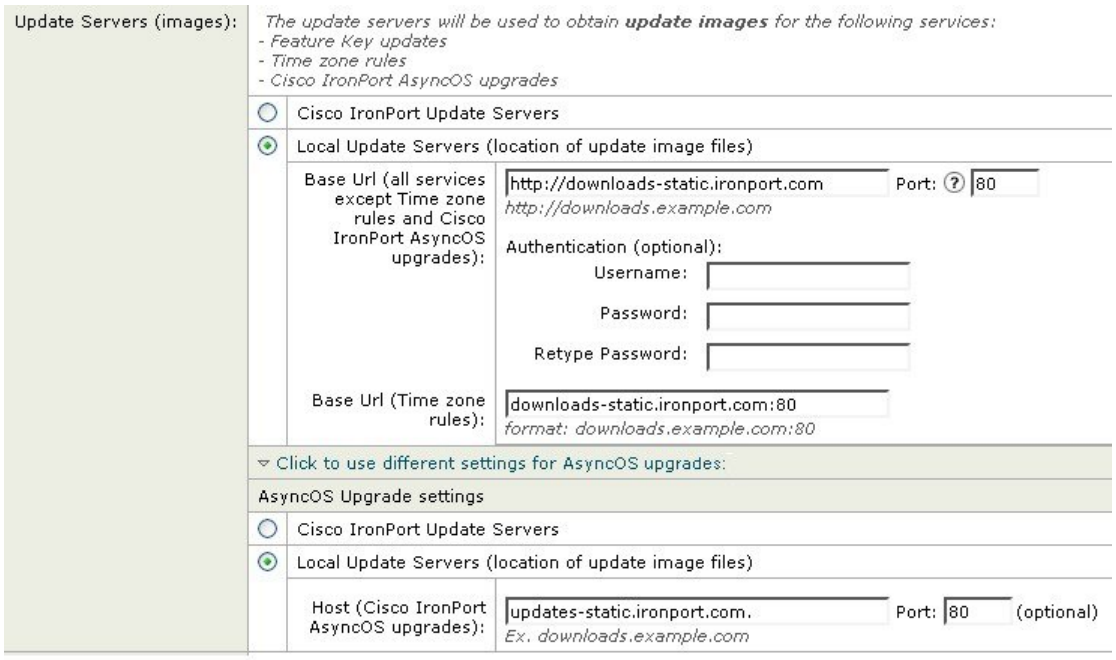


図 *6 : [*アップデートサーバ*(*リスト*)*（***Update Servers (list)***）*]*設定のスタティック ***URL***

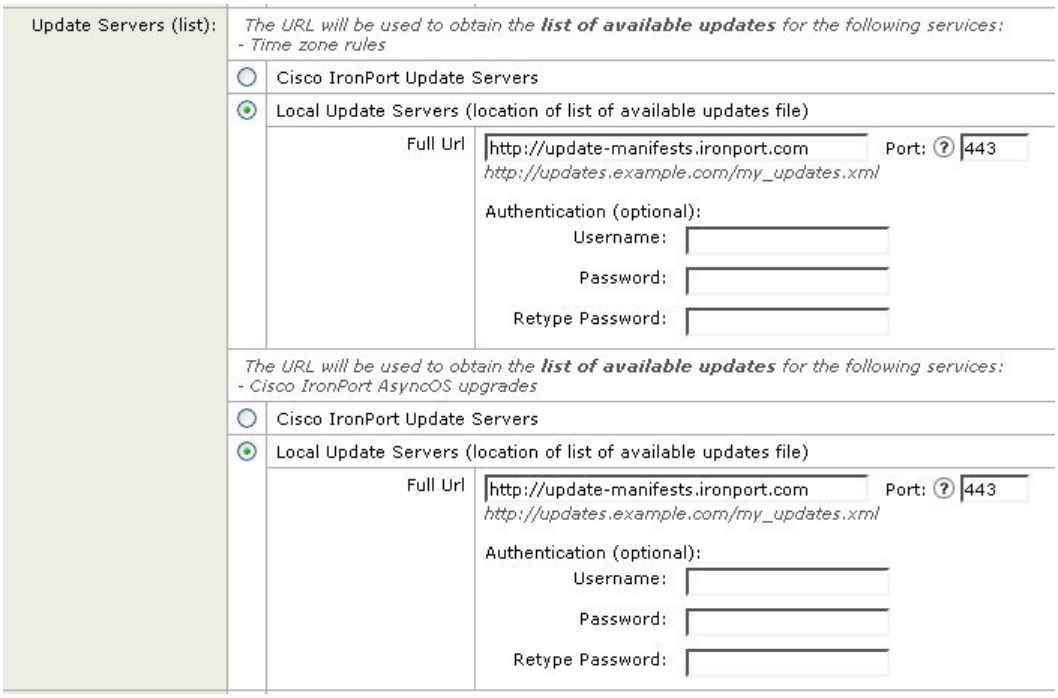


表 *2:* 厳格なファイアウォール ポリシーを適用している環境のスタティック アドレス

セクション	設定	スタティック URL/IP アドレスおよびポート
Update Servers (images)	ベースURL（タイムゾーンルールおよびAsyncOSアップグレード以外のすべてのサービス）（Base URL (all services except Time zone rules and AsyncOS upgrades)）	http://downloads-static.ironport.com 204.15.82.8 Port 80
	ベースURL（タイムゾーンルール）（Base URL (Time zone rules)）	downloads-static.ironport.com 204.15.82.8 Port 80
	ホスト（AsyncOSアップグレード）（Host (AsyncOS upgrades)）	updates-static.ironport.com 208.90.58.25 Port 80
Update Servers (list):	物理ハードウェア アプライアンスでのアップデート用： フルURL（Full URL）	update-manifests.ironport.com 208.90.58.5 Port 443
	仮想アプライアンスでのアップデート用：フル URL（For updates on virtual appliances: Full URL）	update-manifests.sco.cisco.com Port 443
	アップグレード用：フルURL（For upgrades: Full URL）	update-manifests.ironport.com 208.90.58.5 Port 443

重要 CLI で `updateconfig` コマンドの `dynamichost` サブコマンドを使用して、`update-manifests` URL とポート番号を設定する必要があります。これにより、サービスの更新が検証されます。

GUI からのアップデートおよびアップグレード設定値の設定

ステップ 1 （新しいWebインターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[アップデート設定（Update Settings）] を選択します。

ステップ 3 [更新設定を編集（Edit Update Settings）] をクリックします。

アップグレードとアップデートの設定（38ページ）の説明を使用して、この手順の設定を構成します。

ステップ 4 [アップデートサーバー(イメージ)（Update Servers (images)）] セクションで、アップデートのイメージのダウンロード元のサーバーを指定します。

ステップ 5 AsyncOS アップグレードのイメージをダウンロードする元のサーバーを指定します。

a) 同じセクションの下部で、[クリックして AsyncOS アップグレードの異なる設定を使用する（Click to use different settings for AsyncOS upgrades）] リンクをクリックします。

b) AsyncOS アップグレードのイメージをダウンロードするためのサーバー設定を指定します。

ステップ 6 [アップデートサーバー(リスト)（Update Servers (list)）] セクションで、使用可能なアップデートおよび AsyncOS アップグレードのリストを取得するサーバーを指定します。

上部のサブセクションはアップデートに適用されます。下部のサブセクションはアップグレードに適用されます。

ステップ 7 時間帯ルールおよびインターフェイスの設定を指定します。

ステップ 8 （任意）プロキシ サーバーの設定を指定します。

ステップ 9 変更を送信し、保存します。

ステップ 10 結果が予定通りか確認します。

[アップデート設定（Update Settings）] ページが表示されていない場合は、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アップデート設定（Update Settings）] を選択します。

一部の URL では、サーバー URL に「asyncos」ディレクトリが追加されます。この不一致は無視してかまいません。

アップグレードの通知

デフォルトでは、AsyncOS アップグレードがアプライアンスで使用可能な場合、管理者および技術者の権限を持つユーザーには、Web インターフェイスの上部に通知が表示されます。

目的	操作手順
最新のアップグレードの詳細情報を表示する	アップグレード通知にカーソルを合わせます。
使用できるすべてのアップグレードのリストを表示する	通知の下向き矢印をクリックします。
現在の通知を閉じる 新しいアップグレードが入手可能になるまで、アプライアンスは別の通知を表示しません。	下向き矢印をクリックして [通知を消去（Clear the notification）] を選択してから、[閉じる（Close）] をクリックします。

目的	操作手順
今後の通知を中止する（管理者権限を持つユーザのみ）	[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[システムアップグレード（System Upgrade）] に移動します。

アップグレードする前に：重要な手順

始める前に

アップグレードとアップデートのネットワーク要件の決定 （34 ページ）でネットワーク要件を参照してください。

ステップ 1 次のようにして、データの消失を防止する、または最小限に抑えます。

- 新しいアプライアンスに十分なディスク容量があり、転送される各データ タイプに同等以上のサイズが割り当てられていることを確認します。最大ディスク領域と割り当てについて （80 ページ）を参照してください。
- ディスク領域についての何らかの警告を受け取った場合は、アップグレードを開始する前に、ディスク領域に関する問題をすべて解決してください。

ステップ 2 アプライアンスから、XML コンフィギュレーション ファイルを保存します。現在の設定ファイルの保存およびエクスポート （71 ページ）で説明する警告を参照してください。

何らかの理由でアップグレード前のリリースに戻す場合は、このファイルが必要です。

ステップ 3 セーフリスト/ブロックリスト機能を使用している場合は、リストをボックスからエクスポートします。

[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[設定ファイル（Configuration File）] をクリックしてスクロール ダウンします。

ステップ 4 CLI からアップグレードを実行している場合は、**suspendlistener** コマンドを使用してリスナーを停止します。GUI からのアップグレードを実行する場合は、リスナーの停止が自動的に実行されます。

ステップ 5 メール キューとデリバリ キューを解放します。

ステップ 6 アップグレード設定が希望どおりに設定されていることを確認します。アップグレードおよびサービス アップデートの設定 （38 ページ） を参照してください。

AsyncOS のアップグレード

1 回の操作でダウンロードとインストールを行うか、またはバックグラウンドでダウンロードし後でインストールできます。

（注） AsyncOS を Cisco サーバーからではなくローカル サーバーから 1 回の操作でダウンロードとアップグレードする場合は、アップグレードはダウンロード中に即座に実行されます。アップグレードプロセスの開始時に、バナーが 10 秒間表示されます。このバナーが表示されている間は、Ctrl を押した状態で C を押すと、ダウンロードの開始前にアップグレード プロセスを終了できます。

始める前に

- Cisco から直接アップグレードをダウンロードするか、またはネットワーク上のサーバからアップグレードイメージをホストするかを選択します。次に、選択した方式をサポートするようにネットワークをセットアップします。そして、選択した入手先からアップグレードを入手するためにアプライアンスを設定します。アップグレード方式の選択：リモートまたはストリーミング （35 ページ）およびアップグレードおよびサービス アップデートの設定 （38 ページ）を参照してください。
- アップグレードをインストールする前に、アップグレードする前に：重要な手順 （44 ページ）の手順を実行してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システムのアップグレード（System Upgrade）] を選択します。

ステップ 3 [アップグレードオプション（Upgrade Options）] をクリックします。

ステップ 4 次のオプションを選択します。

目的	操作手順
1 回の操作でアップグレードのダウンロードとインストールを実行する	[ダウンロードしてインストール（Download and Install）] をクリックします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。
アップグレードインストーラをダウンロードする	[ダウンロードのみ（Download only）] をクリックします。 すでにインストーラをダウンロードしている場合、既存のダウンロードを上書きするよう求められます。 インストーラはサービスを中断することなく、バックグラウンドでダウンロードします。

目的	操作手順
ダウンロードしたアップグレードインストーラをインストールする	[Install（インストール）] をクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。 インストールする AsyncOS のバージョンは、[インストール（Install）] オプションの下に表示されます。

ステップ 5 以前にダウンロードしたインストーラでインストールする場合を除き、利用可能なアップグレードのリストから AsyncOS のバージョンを選択します。

ステップ 6 インストール中の場合、次に従います。

a) 現在の設定をアプライアンス上の configuration ディレクトリに保存するかどうかを選択します。

b) コンフィギュレーション ファイルでパスフレーズをマスクするかどうかを選択します。

（注） マスクされたパスフレーズが記載されたコンフィギュレーション ファイルは、GUI の [設定ファイル（Configuration File）] ページや CLI の `loadconfig` コマンドからロードできません。

c) コンフィギュレーション ファイルのコピーを電子メールで送信する場合は、ファイルを送信する電子メール アドレスを入力します。複数の電子メール アドレスを指定する場合は、カンマで区切ります。

ステップ 7 [続行（Proceed）] をクリックします。

ステップ 8 インストール中の場合、次に従います。

a) プロセス中のプロンプトに応答できるようにしてください。

応答するまでプロセスは中断されます。

ページの上部の近くに、経過表示バーが表示されます。

b) プロンプトで、[今すぐ再起動（Reboot Now）] をクリックします。

（注） リブートしてから少なくとも 20 分経過するまで、いかなる理由があっても（アップグレードの問題をトラブルシューティングするためであっても）アプライアンスの電源を中断しないでください。

c) 約 10 分後、アプライアンスにアクセスしてログインします。

次のタスク

- プロセスが中断された場合、プロセスを再開する必要があります。
- アップグレードをダウンロードしてインストールしなかった場合は次のとおりです。

  アップグレードをインストールする準備ができたら、「始める前に」の項の前提条件も含め次の手順を最初から実行しますが、[インストール（Install）]オプションを選択します。
- アップグレードをインストールしている場合は、アップグレード後 （47 ページ）を参照してください。

バックグラウンドダウンロードのキャンセルまたは削除ステータスの表示

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システムのアップグレード（System Upgrade）] を選択します。

ステップ 3 [アップグレードオプション（Upgrade Options）] をクリックします。

ステップ 4 次のオプションを選択します。

目的	操作手順
ダウンロード ステータスの表示	ページの中央を確認してください。 進行中のダウンロードおよびダウンロードが完了してインストールされるのを待っているものがない場合は、ダウンロードのステータス情報は表示されません。 アップグレードのステータスは upgrade_logs でも確認できます。
ダウンロードのキャンセル	ページの中央にある、[ダウンロードをキャンセル（Cancel Download）] ボタンをクリックします。 このオプションは、ダウンロード進行中にのみ表示されます。
ダウンロードされたインストーラの削除	ページの中央にある、[ファイルを削除（Delete File）] ボタンをクリックします。 このオプションは、インストーラがダウンロードされている場合にのみ表示されます。

アップグレード後

アップグレードが完了したら、次の手順を実行します。

- （関連する E メール セキュリティ アプライアンスのある導入環境の場合）リスナーを再度イネーブルにします。
- （関連する Web セキュリティ アプライアンスのある導入環境の場合）最新の Configuration Master をサポートするようにシステムを設定します。Configuration Master を使用して中央集中型で Web セキュリティ アプライアンスを管理するを参照してください。
- 設定を保存するかどうか判断します。詳細については、設定の保存とインポート （70 ページ）を参照してください。

- アップグレード後オンライン ヘルプを表示するには、ブラウザ キャッシュをクリアし、ブラウザを終了してもう一度開きます。これにより、期限切れのコンテンツのブラウザ キャッシュがクリアされます。

AsyncOS の以前のバージョンへの復元について

緊急時には、前の認定バージョンの AsyncOS に戻すことができます。

アプライアンス上のすべてのデータをクリアし、新しい、クリーンな設定から始める場合は、現在実行中のビルドに戻すこともできます。

関連項目

- 復元の影響に関する重要な注意事項 （48 ページ）
- AsyncOS の復元 （48 ページ）

復元の影響に関する重要な注意事項

Cisco コンテンツ セキュリティ アプライアンスにおける revert コマンドの使用は、非常に破壊的な操作になります。このコマンドはすべての既存の設定およびデータを永久破壊します。さらに、復元ではアプライアンスが再設定されるまでメール処理が中断されます。

復元によって機能キーまたは仮想アプライアンス ライセンスの有効期限日に影響が及ぶことはありません。

AsyncOS の復元

始める前に

- 保持する必要があるデータをアプライアンス以外の場所にバックアップまたは保存します。
- 戻し先のバージョンのコンフィギュレーション ファイルが必要です。コンフィギュレーション ファイルに下位互換性はありません。
- このコマンドはすべての設定を破壊するため、復元を実行する場合は、アプライアンスへの物理的なローカル アクセスを必ず用意するようにしてください。
- お使いの E メール セキュリティ アプライアンスで隔離が有効になっている場合は、それらのアプライアンスでローカルにメッセージが隔離されるように集約化を無効にします。

ステップ 1 戻し先のバージョンのコンフィギュレーション ファイルがあることを確認してください。コンフィギュレーション ファイルに下位互換性はありません。

ステップ 2 アプライアンスの現在の設定のバックアップ コピーを、（パスフレーズをマスクしない状態で）別のマシンに保存します。コンフィギュレーションファイルを取得するには、ファイルを電子メールでユーザー

自身に送信するか、ファイルを FTP で取得します。簡単に行うには、`mailconfig` CLI コマンドを実行すると、アプライアンスの現在のコンフィギュレーション ファイルが指定したメールアドレスに送信されます。

（注） このコピーは、バージョンを戻した後にロードする設定ファイルではありません。

ステップ 3 セーフリスト/ブロックリスト機能を使用する場合は、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します。

ステップ 4 Email Security Appliances で、すべてのリスナーを一時停止します。

ステップ 5 メール キューが空になるまで待ちます。

ステップ 6 バージョンを戻すアプライアンスの CLI にログインします。

`revert` コマンドの実行時には、いくつかの警告プロンプトが発行されます。これらの警告プロンプトに同意すると、すぐにバージョンを戻す動作が開始します。このため、復元前の手順を完了するまで、復元プロセスを開始しないでください。

ステップ 7 コマンドライン プロンプトから **revert** コマンドを入力し、プロンプトに応答します。

次に、**revert** コマンドの例を示します。

例：

```
m650p03.prep> revert
This command will revert the appliance to a previous version of AsyncOS.
WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy
quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
- all Cisco Spam Quarantine message and end-user safelist/blocklist data
Only the network settings will be preseved.
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passphrases
unmasked)
- exported the Cisco Spam Quarantine safelist/blocklist database
   to another machine (if applicable)
- waited for the mail queue to empty
Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots again to the desired version.
Do you want to continue? yes
Are you sure you want to continue? yes
Available versions
=================
 1. 7.2.0-390
 2. 6.7.6-020
Please select an AsyncOS version: 1
You have selected "7.2.0-390".
Reverting to "testing" preconfigure install mode.
The system will now reboot to perform the revert operation.
```

ステップ 8 アプライアンスが 2 回リブートするまで待ちます。

ステップ 9 CLI を使用してアプライアンスにログインします。

ステップ 10 少なくとも 1 つの Web セキュリティ アプライアンスを追加し、URL カテゴリ アップデートがそのアプライアンスからダウンロードされるまで数分待ちます。

ステップ 11 URL カテゴリのアップデートが完了したら、戻し先のバージョンのコンフィギュレーション ファイルをロードします。

ステップ 12 セーフリスト/ブロックリスト機能を使用する場合は、セーフリスト/ブロックリスト データベースをインポートして復元します。

ステップ 13 Email Security Appliances で、すべてのリスナーを再びイネーブルにします。

ステップ 14 変更を保存します。

これで、復元が完了した Cisco コンテンツ セキュリティ アプライアンスは、選択された AsyncOS バージョンを使用して稼働します。

（注） 復元が完了して、Cisco コンテンツ セキュリティ アプライアンスへのコンソール アクセスが再び利用可能になるまでには、15 ～ 20 分かかります。

アップデートについて

サービス アップデートは定期的にダウンロード可能にできます。これらのダウンロードの設定を指定するには、アップグレードおよびサービス アップデートの設定 （38 ページ）

関連項目

- アップグレードおよびサービス アップデートの設定 （38 ページ）

Web 使用率制御の URL カテゴリ セット アップデートについて

- URL カテゴリ セットの更新の準備および管理
- URL カテゴリ セットの更新とレポート

プロキシサーバーとの通信を信頼するようにアプライアンスを設定

透過的でないプロキシサーバーを使用している場合、プロキシ証明書の署名に使用する CA 証明書を電子メールゲートウェイに追加できます。これにより、電子メールゲートウェイはプロキシサーバー通信を信頼します。

Cisco Secure Email and Web Manager がアップデータサーバーと通信して更新を受信する場合、使用されている証明書に対して証明書が信頼できるかどうかの検証が実行されます。使用されている証明書を正常に検証するには、そのアップデータサーバーの認証局証明書を Cisco Secure Email and Web Manager に含めて、通信を成功させる必要があります。これを実行するには、**updateconfig** > **trusted_certificates**を使用します。コマンドのオプションは次のとおりです。

- 追加：CA に証明書を追加します

- リスト：CA 内のすべての証明書を一覧にします
- 削除：CA の証明書を削除します

このオプションを構成するには、updateconfig コマンドを使用します。次の例は、このオプションを構成する方法を示しています。

```
SMA> updateconfig

Service (images): Update URL:
-------------------------------------------------------------------------------
Feature Key updates http://downloads.ironport.com/asyncos
Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Service (list): Update URL:
-------------------------------------------------------------------------------
Timezone rules Cisco Servers
Support Request updates Cisco Servers
Smart License Agent Updates Cisco Servers
Notifications component Updates Cisco Servers
Cisco AsyncOS upgrades Cisco Servers

Update interval: 5m

Proxy server: not enabled

HTTPS Proxy server: not enabled

Choose the operation you want to perform:
- SETUP - Edit update configuration.
- VALIDATE_CERTIFICATES - Validate update server certificates
- TRUSTED_CERTIFICATES - Manage trusted certificates for updates
[]> trusted_certificates


Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]> add

Paste certificates to be trusted for secure updater connections, blank to quit
Trusted Certificate for Updater:
paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDxTCCAq2gAwIBAgIIOUMAFHhzRskwDQYJKoZIhvcNAQELBQAwczELMAkGA1UE
BhMCSU4xCzAJBgNVBAgTAlROMQwwCgYDVQQHEwNDaG4xETAPBgNVBAoTCENBQ053
aWxkMREwDwYDVQQLEwhDQUNOd2lsZDEjMCEGA1UEAwwaKi5jczIxLmRldml0LmNp
c2NvbGFicy5jb20wHhcNMjExMjE1MTE0NzAwWhcNMjIxMjE1MTE0NzAwWjBzMQsw
CQYDVQQGEwJJTjELMAkGA1UECBMCVE4xDDAKBgNVBAcTA0NobjERMA8GA1UEChMI
Q0FDTndpbGQxETAPBgNVBAsTCENBQ053aWxkMSMwIQYDVQQDDBoqLmNzMjEuZGV2
aXQuY2lzY29sYWJzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AJPPBRGq0wHv/6ZLPOZ3jdEgzVS+dzXJSyhtMsgm/XrvIvjRH0MK3r++dtUgHMzz
le/WrxPKGphjtNsvF7ss58RRg3fiQCSQPX6nfBYc9v4A7rSdmKzYYFbBkGPeijLB
qwVyseMa3rifjv4Bucxw0M3ZrUqq7YfcZtxZhSEtxx8rT3A/uReIm/n1ERcZDclW
+GkfRxEdY3ZLpen/2sFiOAVMvAHlKRtK7kEhmo1TPQZ0h0UQFNDbl2ZWZZ6Nuv0I
Z6pUDNj1/+GoJyvSwl0qpetHxhdMtubMAAM8JQNvNkHgzOswsbN18F5at7cZ/KFI
HuvBUXKHV5pEX3hOdJxbuocCAwEAAaNdMFswDAYDVR0TBAUwAwEB/zAdBgNVHQ4E
FgQUCNlXseZ5qBjqJtYv3sdCujJuqnAwHwYDVR0jBBgwFoAUCNlXseZ5qBjqJtYv
```

```
3sdCujJuqnAwCwYDVR0PBAQDAgGGMA0GCSqGSIb3DQEBCwUAA4IBAQBaq5KXw/wX
nzJpBnKPZuO4KNcIz9/A2Hil2ikWNBjfla1x/37OdTbh3IpHJ6n1OCeAkE5Ww7uX
amlUcWxvDk3Zn+tKysCU2Q1PYSxUHXtqH3rvWZDRglPkJUu420tnCg2fV1bulcJ1
xx6E95a9D1vCarfxvuINU50076gnypTMv9+lOFXCkvDgBOmkQpqswR5l519kmDZi
mt8CoknJN/iAENxM8b47262yXEc1X6ZN/OWa/xl4OS3X0C0hikyg9HpUGDq+CigE
s5CBCOLDfe8G9kAPoTg2mVNT10xxQF1juobb6djmdB1Of8kqgKs2eWsD+MfKvNbG
ZzPGx4SUS2RZ
-----END CERTIFICATE-----
.
Do you want to check if Common Name or SAN:dNSName or both are in Fully Qualified Domain
 Name(FQDN) format ? [N]> y


Choose the operation you want to perform:
- ADD - Upload a new trusted certificate for updates.
- LIST - List trusted certificates for updates.
- DELETE - Delete a trusted certificate for updates.
[]>
```

生成されたメッセージの返信アドレスの設定

次の場合に対して、AsyncOS で生成されたメールのエンベロープ送信者を設定できます。

- バウンス メッセージ
- レポート

返信アドレスの表示、ユーザ、およびドメイン名を指定できます。ドメイン名に仮想ゲートウェイ ドメインの使用を選択することもできます。

GUI の [システム管理（System Administration）] メニューから利用できる [返信先アドレス（Return Addresses）] ページを使用するか、CLI で **addressconfig** コマンドを使用します。

システムで生成された電子メール メッセージの返信アドレスを GUI で変更するには、[返信先アドレス（Return Addresses）] ページで [設定の編集（Edit Settings）] をクリックします。1 つまたは複数のアドレスを変更して [送信（Submit）] をクリックし、変更を保存します。

アラートの管理

アプライアンスから、アプライアンスで発生しているイベントに関する電子メールアラートが送信されます。

目的	操作手順
タイプの異なるアラートが別の管理ユーザに送信されるようにする	[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[アラート（Alerts）]を選択します。 システムのセットアップ時に AutoSupport をイネーブルにした場合、指定した電子メールアドレスはデフォルトで、すべての重大度およびクラスのアラートを受信します。この設定はいつでも変更できます。 複数のアドレスを指定する場合は、カンマで区切ります。
次のようなアラートのグローバル設定を行う • アラート送信者（FROM:）アドレス • 重複したアラートの制御 • AutoSupport 設定	[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[アラート（Alerts）]を選択します。 重複したアラートについて （55 ページ）を参照してください Cisco AutoSupport （55 ページ）を参照してください
最近のアラートのリストを表示する このリストの設定を管理する	最新アラートの表示 （54 ページ）を参照してください
アラートのリストと説明を表示する	参照先： ハードウェア アラートの説明 （55 ページ）。 システム アラートの説明 （56 ページ）
アラートの配信メカニズムを理解する	アラートの配信 （54 ページ）を参照してください

アラート タイプおよび重大度

アラート タイプは次のとおりです。

- ハードウェア アラート。ハードウェア アラートの説明 （55 ページ）を参照してください。
- システム アラート。システム アラートの説明 （56 ページ）を参照してください。
- アップデータ アラート。

アラートの重大度は次のとおりです。

- Critical：すぐに対処が必要な問題
- Warning：今後モニターリングが必要な問題またはエラー。すぐに対処が必要な可能性もあります
- Info：このデバイスのルーティン機能で生成される情報

アラートの配信

アラート メッセージは Cisco コンテンツ セキュリティ アプライアンス内の問題の通知に使用されるため、送信に AsyncOS の標準メール配信システムを使用しません。代わりに、アラート メッセージは AsyncOS で重大なシステム故障が発生しても動作するように設計された、個別に並行動作する電子メール システムで処理されます。

アラート メール システムは、AsyncOS と同一の設定を共有しません。このため、アラート メッセージは、次のように他のメール配信とは若干異なる動作をする可能性があります。

- アラート メッセージは、標準の DNS MX レコードおよび A レコードのルックアップを使用して配信されます。
  - アラート メッセージは DNS エントリを 30 分間キャッシュし、そのキャッシュは 30 分ごとにリフレッシュされます。このため、DNS 障害時にもアラートが出力されます。
- 導入環境に E メール セキュリティ アプライアンスが含まれている場合：
  - アラート メッセージはワーク キューを通過しないため、ウイルスまたはスパムのスキャン対象外です。メッセージ フィルタまたはコンテンツ フィルタの処理対象にも含まれません。
  - アラート メッセージは配信キューを通過しないため、バウンスのプロファイルまたは送信先制御の制限には影響を受けません。

最新アラートの表示

目的	操作手順
最近のアラートのリストを表示する	管理者およびオペレータのアクセス権のあるユーザは、[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [アラート（Alerts）] を選択し、[上位アラートを表示（View Top Alerts）] ボタンをクリックします。 アラートは、電子メールで通知する問題があっても表示されます。
リストをソートする	列の見出しをクリックします。
このリストに保存するアラートの最大数を指定する	コマンドライン インターフェイス（CLI）で alertconfig コマンドを使用します。
この機能を無効にする	コマンドライン インターフェイス（CLI）で alertconfig コマンドを使用してアラートの最大数をゼロ（0）に設定します。

重複したアラートについて

AsyncOSが重複したアラートを送信するまでに待機する秒数の初期値を指定できます。この値を0に設定した場合、重複したアラートのサマリーは送信されず、代わりにすべての重複したアラートがリアルタイムに送信されます（短時間に大量の電子メールを受信する可能性があります）。重複したアラートを送信するまでに待機する秒数は、アラートを送信するたびに増加します。増加する秒数は、前回の待機間隔の2倍の値を足した秒数です。つまり、待機時間が5秒間の場合、アラートは5秒後、15秒後、35秒後、75秒後、155秒後、315秒後といった間隔で送信されます。

最終的に、送信間隔は非常に長くなります。[重複するアラートを送信する前に待機する最大秒数（Maximum Number of Seconds to Wait Before Sending a Duplicate Alert）] フィールドを使用して、待機間隔の秒数に制限を設けることができます。たとえば、初期値を5秒に設定し、最大値を60秒に設定すると、アラートは5秒後、15秒後、35秒後、60秒後、120秒後といった間隔で送信されます。

Cisco AutoSupport

シスコによる十分なサポートと今後のシステム変更の設計を可能にするため、システムで生成されたすべてのアラートメッセージをシスコに送信するようにCiscoコンテンツセキュリティアプライアンスを設定できます。「AutoSupport」と呼ばれるこの機能は、カスタマー サポートによるお客様のニーズへのプロアクティブな対応に役立ちます。また、AutoSupportはシステムの稼働時間、**status**コマンドの出力、および使用されているAsyncOSバージョンを通知するレポートを毎週送信します。

デフォルトでは、アラート タイプがSystemで重大度レベルがInformationのアラートを受信するように設定されているアラート受信者は、Ciscoに送信される各メッセージのコピーを受信します。内部にアラートメッセージを毎週送信しない場合は、この設定をディセーブルにできます。この機能を有効または無効にするには、[管理アプライアンス（Management Appliance）] >[システム管理アラート（System Administration Alerts）] を選択し、[設定の編集（Edit Settings）] をクリックします。

AutoSupportが有効の場合、Informationレベルのシステム アラートを受信するように設定されたアラート受信者に、デフォルトで毎週AutoSupportレポートが送信されます。

ハードウェア アラートの説明

表 *3:* ハードウェア アラートの説明

アラート名	説明	重大度
INTERFACE.ERRORS	インターフェイス エラーを検出した場合に送信されます。	警告
MAIL.MEASUREMENTS_FILESYSTEM	ディスク パーティションが75％の使用率に近づいた場合に送信されます。	警告

アラート名	説明	重大度
MAIL.MEASUREMENTS_FILESYSTEM.CRITICAL	ディスク パーティションが 90 % の使用率に達した場合（95 %、96 %、97 % など）に送信されます。	クリティカル
SYSTEM.RAID_EVENT_ALERT	重大な RAID-event が発生した場合に送信されます。	警告
SYSTEM.RAID_EVENT_ALERT_INFO	RAID-event が発生した場合に送信されます。	情報

システム アラートの説明

表 *4:* システム アラートの説明

アラート名	説明	重大度
COMMON.APP_FAILURE	不明なアプリケーション障害が発生した場合に送信されます。	クリティカル（Critical）
COMMON.KEY_EXPIRED_ALERT	機能キーの有効期限が切れた場合に送信されます。	警告
COMMON.KEY_EXPIRING_ALERT	機能キーの有効期限が切れる場合に送信されます。	警告
COMMON.KEY_FINAL_EXPIRING_ALERT	機能キーの有効期限が切れる場合の最後の通知として送信されます。	警告
DNS.BOOTSTRAP_FAILED	アプライアンスがルート DNS サーバに問い合わせることができない場合に送信されます。	警告
COMMON.INVALID_FILTER	無効なフィルタが存在する場合に送信されます。	警告

アラート名	説明	重大度
IPBLOCKD.HOST_ADDED_TO_ALLOWED LIST IPBLOCKD.HOST_ADDED_TO_BLOCKED LIST IPBLOCKD.HOST_REMOVED_FROM_BLOCKED LIST	アラート メッセージ： • <IP address>のホストがSSH DoS 攻撃のためブロックリストに追加されました。（The host at <IP address> has been added to the blocked list because of an SSH DOS attack） • <IP address>のホストがSSH許可リストに追加されました。（The host at <IP address> has been permanently added to the ssh allowed list.） • <IP address>のホストがブロックリストから削除されました（The host at <IP address> has been removed from the blocked list） SSH を介してアプライアンスへの接続を試みているが、有効なクレデンシャルを提示しない IP アドレスは、2 分以内に 11 回以上試行に失敗した場合、SSH のブロックリストに追加されます。 同じ IP アドレスからユーザが正常にログインすると、その IP アドレスは許可リストに追加されます。 許可リストのアドレスは、それらがブロックリストに含まれていてもアクセスが許可されます。	警告
LDAP.GROUP_QUERY_FAILED_ALERT	LDAP グループ クエリに失敗した場合に送信されます。	クリティカル（Critical）

アラート名	説明	重大度
LDAP.HARD_ERROR	LDAP クエリが（すべてのサーバで試行した後）完全に失敗した場合に送信されます。	クリティカル（Critical）
LOG.ERROR.*	さまざまなロギング エラー。	クリティカル
MAIL.PERRCPT.LDAP_GROUP_QUERY_FAILED	各受信者のスキャン時に LDAP グループ クエリーに失敗した場合に送信されます。	クリティカル
MAIL.QUEUE.ERROR.*	メール キューのさまざまなハード エラー。	クリティカル
MAIL.RES_CON_START_ALERT.MEMORY	メモリ使用率がシステム リソース節約しきい値を超過した場合に送信されます。	クリティカル
MAIL.RES_CON_START_ALERT.QUEUE_SLOW	メール キューが過負荷となり、システム リソース節約がイネーブルになった場合に送信されます。	クリティカル
MAIL.RES_CON_START_ALERT.QUEUE	キュー使用率がシステム リソース節約しきい値を超過した場合に送信されます。	クリティカル
MAIL.RES_CON_START_ALERT.WORKQ	ワーク キューのサイズが大きすぎるため、リスナーが一時停止された場合に送信されます。	クリティカル
MAIL.RES_CON_START_ALERT	アプライアンスが「リソース節約」モードになった場合に送信されます。	クリティカル
MAIL.RES_CON_STOP_ALERT	アプライアンスの「リソース節約」モードが解除された場合に送信されます。	クリティカル
MAIL.WORK_QUEUE_PAUSED_NATURAL	ワーク キューが中断された場合に送信されます。	クリティカル

アラート名	説明	重大度
MAIL.WORK_QUEUE_UNPAUSED_NATURAL	ワーク キューが再開された場合に送信されます。	クリティカル（Critical）
NTP.NOT_ROOT	root として NTP が実行されていないためにアプライアンスが時刻を調整できない場合に送信されます。	警告
PERIODIC_REPORTS.DOMAIN_REPORT.DOMAIN_FILE_ERRORS	ドメイン指定ファイルでエラーが検出された場合に送信されます。	クリティカル
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_EMPTY	ドメイン指定ファイルが空の場合に送信されます。	クリティカル
PERIODIC_REPORTS.DOMAIN_REPORT.FILE_MISSING	ドメイン指定ファイルが見つからない場合に送信されます。	クリティカル
REPORTD.DATABASE_OPEN_FAILED_ALERT	レポート エンジンがデータベースを開けない場合に送信されます。	クリティカル（Critical）
REPORTD.AGGREGATION_DISABLED_ALERT	システムのディスク領域が不足している場合に送信されます。ログ エントリに関するディスク使用率がログ使用率のしきい値を超過すると、reportd は集約をディセーブルにし、アラートを送信します。	警告
REPORTD.DATABASE_DELETION_ALERT	システムがエクスポート ディレクトリをチェックし、空でないことがわかると送信され、ログラインを出力して、次の反復でディレクトリの削除を試みます。	情報
REPORTING.CLIENT.UPDATE_FAILED_ALERT	レポート エンジンがレポート データを保存できなかった場合に送信されます。	警告

アラート名	説明	重大度
REPORTING.CLIENT.JOURNAL.FULL	レポート エンジンが新規データを保存できない場合に送信されます。	クリティカル
REPORTING.CLIENT.JOURNAL.FREE	レポート エンジンが再び新規データを保存できるようになった場合に送信されます。	情報
PERIODIC_REPORTS.REPORT_TASK。BUILD_FAILURE_ALERT	レポート エンジンがレポートを作成できない場合に送信されます。	クリティカル
PERIODIC_REPORTS.REPORT_TASK。EMAIL_FAILURE_ALERT	レポートを電子メールで送信できなかった場合に送信されます。	クリティカル
PERIODIC_REPORTS.REPORT_TASK。ARCHIVE_FAILURE_ALERT	レポートをアーカイブできなかった場合に送信されます。	クリティカル（Critical）
SENDERBASE.ERROR	SenderBase からの応答を処理中にエラーが発生した場合に送信されます。	情報
SMAD.ICCM.ALERT_PUSH_FAILED	1 台以上のホストでコンフィギュレーションのプッシュに失敗した場合に送信されます。	警告
SMAD.TRANSFER.TRANSFERS_STALLED	SMA ログがトラッキング データを 2 時間取得できなかった場合、またはレポーティング データを 6 時間取得できなかった場合に送信されます。	警告
SMTPAUTH.FWD_SERVER_FAILED_ALERT	SMTP 認証転送サーバが到達不能である場合に送信されます。	警告
SMTPAUTH.LDAP_QUERY_FAILED	LDAP クエリが失敗した場合に送信されます。	警告

アラート名	説明	重大度
SYSTEM.HERMES_SHUTDOWN_FAILURE。REBOOT	リブート中のシステムをシャットダウンしている際に問題が発生した場合に送信されます。	警告
SYSTEM.HERMES_SHUTDOWN_FAILURE。SHUTDOWN	システムをシャットダウンしている際に問題が発生した場合に送信されます。	警告
SYSTEM.RCPTVALIDATION.UPDATE_FAILED	受信者検証のアップデートに失敗した場合に送信されます。	クリティカル
SYSTEM.SERVICE_TUNNEL.DISABLED	シスコ サポート サービス用に作成されたトンネルが無効の場合に送信されます。	情報
SYSTEM.SERVICE_TUNNEL.ENABLED	シスコ サポート サービス用に作成されたトンネルが有効の場合に送信されます。	情報

ネットワーク設定値の変更

このセクションでは、アプライアンスのネットワーク操作の設定に使用する機能について説明します。これらの機能では、システム セットアップ ウィザードの実行でシステム セットアップ ウィザードを利用して設定したホスト名、DNS、およびルーティングの設定値に直接アクセスできます。

ここでは、次の機能について説明します。

- `sethostname`
- DNS 設定（GUI で設定。および CLI で `dnsconfig` コマンドを使用して設定）
- ルーティング設定（GUI で設定。および CLI で `routeconfig` コマンドと `setgateway` コマンドを使用して設定）
- `dnsflush`
- パスフレーズ

システム ホスト名の変更

ホスト名は、CLIプロンプトでシステムを識別する際に使用されます。完全修飾ホスト名を入力する必要があります。sethostname コマンドは、コンテンツ セキュリティ アプライアンスの名前を設定します。新規ホスト名は、commit コマンドを発行して初めて有効になります。

sethostname コマンド

```
oldname.example.com> sethostname
[oldname.example.com]> mail3.example.com
oldname.example.com>
```

ホスト名の変更を有効にするには、commit コマンドを入力する必要があります。ホスト名の変更を確定すると、CLI プロンプトに新しいホスト名が表示されます。

```
oldname.example.com> commit
Please enter some comments describing your changes:
[]> Changed System Hostname
Changes committed: Mon Jan 04 12:00:01 2010
```

プロンプトに新規ホスト名が次のように表示されます。mail3.example.com>

ドメイン ネーム システムの設定

コンテンツ セキュリティ アプライアンスのドメイン ネーム システム（DNS）は、GUI の [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [DNS] ページ、または dnsconfig コマンドを使用して設定できます。

次の設定値を設定できます。

- インターネットの DNS サーバーまたはユーザー独自の DNS サーバーのどちらを使用するか、および使用するサーバー
- DNS トラフィックに使用するインターフェイス
- 逆引き DNS ルックアップがタイムアウトするまで待機する秒数
- DNS キャッシュのクリア

DNS サーバの指定

AsyncOS では、インターネットのルート DNS サーバー、ユーザー独自の DNS サーバー、またはインターネットのルート DNS サーバーと指定した信頼できる DNS サーバーを使用できます。インターネットのルート サーバーを使用するときは、特定のドメインに使用する代替サーバーを指定することもできます。代替 DNS サーバーは単一のドメインに適用されるため、該当ドメインに対する信頼できるサーバー（最終的な DNS レコードを提供）になっている必要があります。

AsyncOS では、インターネットの DNS サーバを使用しない場合に「スプリット」DNS サーバをサポートしています。ユーザ独自の内部サーバを使用している場合は、例外のドメインおよび関連する DNS サーバを指定することもできます。

「スプリットDNS」を設定する場合は、in-addr.arpa（PTR）エントリも同様に設定する必要があります。このため、たとえば「.eng」クエリをネームサーバー1.2.3.4にリダイレクトする際に、すべての .eng エントリが 172.16 ネットワークにある場合、スプリット DNS 設定に「eng,16.172.in-addr.arpa」をドメインとして指定する必要があります。

複数エントリとプライオリティ

入力する各 DNS サーバーに、数値でプライオリティを指定できます。AsyncOS では、プライオリティが 0 に最も近い DNS サーバーの使用を試みます。その DNS サーバーが応答しない場合、AsyncOS は次のプライオリティを持つサーバーの使用を試みます。同じプライオリティを持つ DNS サーバーに複数のエントリを指定する場合、システムはクエリを実行するたびに同じプライオリティを持つ DNS サーバーをリストからランダムに選びます。次にシステムは最初のクエリが期限切れになるか、「タイムアウト」になるまで短時間待機した後、さらにそれよりわずかに長い秒数待機するという動作を続けます。待機時間の長さは、DNS サーバーの実際の総数と、設定されたプライオリティによって異なります。タイムアウトの長さはプライオリティに関係なく、すべての IP アドレスで同じです。最初のプライオリティには最も短いタイムアウトが設定されており、次のプライオリティにはより長いタイムアウトが設定されています。最終的なタイムアウト時間は約 60 秒です。1 つのプライオリティを設定している場合、該当のプライオリティに対する各サーバーのタイムアウトは 60 秒になります。2 つのプライオリティを設定している場合、最初のプライオリティに対する各サーバーのタイムアウトは 15 秒になり、次のプライオリティに対する各サーバーのタイムアウトは 45 秒になります。プライオリティが 3 つの場合、タイムアウトは 5 秒、10 秒、45 秒になります。

たとえば、4 つの DNS サーバを設定し、2 つにプライオリティ 0 を、1 つにプライオリティ 1 を、もう 1 つにプライオリティ 2 を設定したとします。

表 *5 : DNS* サーバ、プライオリティ、およびタイムアウト間隔の例

プライオリティ	サーバ	タイムアウト（秒）
0	1.2.3.4、1.2.3.5	5、5
1	1.2.3.6	10
2	1.2.3.7	45

AsyncOS は、プライオリティ 0 に設定された 2 つのサーバーをランダムに選択します。プライオリティ 0 のサーバーの 1 つがダウンしている場合は、もう 1 つのサーバーが使用されます。プライオリティ 0 のサーバが両方ダウンしている場合、プライオリティ 1 のサーバ（1.2.3.6）が使用され、最終的にプライオリティ 2（1.2.3.7）のサーバが使用されます。

タイムアウト時間はプライオリティ 0 のサーバは両方とも同じであり、プライオリティ 1 のサーバにはより長い時間が設定され、プライオリティ 2 のサーバにはさらに長い時間が設定されます。

インターネット ルート サーバの使用

AsyncOS DNS リゾルバは、高性能な電子メール配信に必要な大量の同時 DNS 接続を収容できるように設計されています。

（注） デフォルト DNS サーバにインターネット ルート サーバ以外を設定することを選択した場合、設定されたサーバは権威サーバとなっていないドメインのクエリを再帰的に解決できる必要があります。

逆引き DNS ルックアップのタイムアウト

Cisco コンテンツ セキュリティ アプライアンスは電子メールの送受信の際、リスナーに接続しているすべてのリモート ホストに対して「二重 DNS ルックアップ」の実行を試みます。つまり、ダブル DNS ルックアップを実行することで、システムはリモート ホストの IP アドレスの正当性を確保および検証します。これは、接続元ホストの IP アドレスに対する逆引き DNS（PTR）ルックアップと、それに続く PTR ルックアップ結果に対する正引き DNS（A）ルックアップからなります。その後、システムは A ルックアップの結果が PTR ルックアップの結果と一致するかどうかをチェックします。結果が一致しないか、A レコードが存在しない場合、システムはホスト アクセス テーブル（HAT）内のエントリと一致する IP アドレスのみを使用します。この特別なタイムアウト時間はこのルックアップにのみ適用され、複数エントリとプライオリティ （63 ページ）で説明されている一般的な DNS タイムアウトには適用されません。

デフォルト値は 20 秒です。秒数に「0」を入力することで、すべてのリスナーに対してグローバルに逆引き DNS ルックアップのタイムアウトを無効にできます。値を 0 秒に設定した場合、逆引き DNS ルックアップは試行されず、代わりに標準のタイムアウト応答がすぐに返されます。

DNS アラート

アプライアンスの再起動時に、まれにメッセージ「DNSキャッシュのブートストラップに失敗しました（Failed to bootstrap the DNS cache）」が付与されたアラートが生成される場合があります。このメッセージは、システムによるプライマリ DNS サーバーへの問い合わせができなかったことを示しています。この事象は、ネットワーク接続が確立される前に DNS サブシステムがオンラインになった場合、ブートのタイミングで発生します。このメッセージが別のタイミングで表示された場合、ネットワーク問題が発生しているか、または DNS 設定で有効なサーバが指定されていないことを示しています。

DNS キャッシュのクリア

GUI の [キャッシュを消去（Clear Cache）] ボタン、または dnsflush コマンドを使用して、DNS キャッシュのすべての情報をクリアします（dnsflush コマンドの詳細については、資料に指定された場所で入手可能な『IronPort AsyncOS CLI Reference Guide』を参照してください）。ローカル DNS システムが変更された際に、この機能を使用できます。コマンドはすぐに実行され、キャッシュの再投入中に一時的に性能が低下する可能性があります。

グラフィカル ユーザ インターフェイスを使用した DNS 設定値の設定

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[ネットワーク（Network）]>[DNS] ページを選択し、[設定の編集（Edit Settings）] ボタンをクリックします。

ステップ 3 インターネットのルート DNS サーバーまたはユーザー独自の内部 DNS サーバーのどちらを使用するかを選択して、権威 DNS サーバーを指定します。

ステップ 4 ユーザー独自の DNS サーバーを使用するか、権威 DNS サーバーを指定する場合は、サーバー ID を入力し [行の追加（Add Row）] をクリックします。各サーバでこの作業を繰り返します。ユーザ独自の DNS サーバを入力する場合は、プライオリティも同時に指定します。詳細については、DNS サーバの指定 （62 ページ）を参照してください。

ステップ 5 DNS トラフィック用のインターフェイスを選択します。

ステップ 6 逆引き DNS ルックアップをキャンセルするまでに待機する秒数を入力します。

ステップ 7 必要に応じて、[キャッシュのクリア（Clear Chashe）] をクリックして、DNS キャッシュをクリアします。

ステップ 8 変更を送信し、保存します。

TCP/IP トラフィック ルートの設定

一部のネットワーク環境では、標準のデフォルト ゲートウェイ以外のトラフィック ルートを使用する必要があります。スタティック ルートの管理は、GUI の [管理アプライアンス（Management Appliance）]>[ネットワーク（Network）]>[ルーティング（Routing）] ページ、または CLI の **routeconfig** コマンドを使用して行います。

- GUI でのスタティック ルートの管理 （65 ページ）
- デフォルト ゲートウェイの変更（GUI） （66 ページ）

GUI でのスタティック ルートの管理

[管理アプライアンス（Management Appliance）]>[ネットワーク（Network）]>[ルーティング（Routing）] ページを使用して、スタティック ルートの作成、編集、または削除を行えます。このページからデフォルト ゲートウェイの変更もできます。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[ネットワーク（Network）]>[ルーティング（Routing）] ページで、ルート リストの [ルートを追加（Add Route）] をクリックします。ルートの名前を入力します。

ステップ 3 宛先 IP アドレスを入力します。

ステップ 4 ゲートウェイの IP アドレスを入力します。

ステップ 5 変更を送信し、保存します。

デフォルト ゲートウェイの変更（GUI）

ステップ 1 [ルーティング（Routing）] ページのルート リストで [デフォルトルート（Default Route）] をクリックします。

ステップ 2 ゲートウェイの IP アドレスを変更します。

ステップ 3 変更を送信し、保存します。

デフォルト ゲートウェイの設定

GUI の [管理アプライアンス（Management Appliance）] > [ネットワーク（Network）] > [ルーティング（Routing）] ページ（デフォルト ゲートウェイの変更（GUI） （66 ページ）を参照してください）、または CLI の setgateway コマンドを使用して、デフォルト ゲートウェイを設定できます。

セキュア通信プロトコルの指定

- TLSv1.0 が有効になっている下位の AsyncOS バージョン（例：13.6.x）から AsyncOS 13.8.x 以降にアップグレードすると、デフォルトで TLSv1.0 が無効になり TLSv1.1 および TLSv1.2 が有効になります。アップグレード後にアプライアンスで TLSv1.0 方式を有効にする必要があります。
- AsyncOS 13.8.x 以降では、SSLv2 方式および SSLv3 方式はサポートされません。
- SSLv3 および TLSv1.0 ではなく、TLSv1.1 方式および TLSv1.2 方式を使用することを推奨します。 SSLv3 は安全ではないため、使用しないでください。
- 次のそれぞれに対して、使用する通信プロトコルを選択できます。
  - アップデート サーバー
  - アプライアンスの Web ベース管理インターフェイス
  - LDAPS

（注） デフォルトでは、新規に設置したアプライアンスのアップデートサーバー、Web インターフェイス、および LDAP サーバーで TLSv1.1 および TLSv1.2 方式を使用します。スパム隔離へのエンドユーザーのアクセスについては、SSLv3 は無効になっています。

- 現在選択されているプロトコルと利用可能なオプションを表示する場合、またはプロトコルを変更する場合は、コマンドライン インターフェイスで `sslconfig` コマンドを使用します。
- Cisco アップデートサーバーでは SSLv3 をサポートしていません。
- ローカル（リモート）アップデート サーバーを使用する場合、他のすべてのサービスおよび Web ブラウザに選択するプロトコルは、使用しているサーバーとツールでサポートされて有効にされていなければなりません。
- 使用するサーバーごとに、利用可能なオプションのいずれかを有効にする必要があります。
- `sslconfig` コマンドを使用して変更した場合は、変更をコミットする必要があります。
- `sslconfig` コマンドを使用して行った変更をコミットした後、該当するサービスが短時間中断されます。

システム時刻の設定

（注） セキュリティ管理アプライアンスは、レポートのデータを収集する際に、セキュリティ管理アプライアンス上で時間設定を行った際に設定した情報からタイム スタンプを適用します。詳細については、セキュリティ管理アプライアンスによるレポート用データの収集方法を参照してください。

コマンドライン インターフェイスを使用して時間に関連する設定を行うには、ntpconfig、settime、および settz コマンドを使用します。

目的	操作手順
システム時刻を設定する	**[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [時刻設定（Time Settings）] を選択します。** ネットワーク タイム プロトコル（NTP）サーバの使用 （68 ページ）も参照してください。
時間帯を設定する	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [タイムゾーン（Time Zone）] を選択します。 関連項目： • GMT オフセットの選択 （68 ページ） • 時間帯ファイルの更新 （69 ページ）

ネットワーク タイム プロトコル（NTP）サーバの使用

ネットワーク タイム プロトコル（NTP）サーバを使用して、セキュリティ管理アプライアンスのシステム クロックをネットワークまたはインターネット上の他のコンピュータと同期できます。

デフォルトの NTP サーバは time.sco.cisco.com です。

デフォルトの NTP サーバを含め、外部 NTP サーバを使用する場合は、ファイアウォールで必要なポートを開きます。ファイアウォール情報を参照してください

関連項目

- システム時刻の設定 （67 ページ）
- 時間帯ファイルの手動更新 （69 ページ）

（推奨）ネットワーク タイム プロトコル（NTP）を使用したアプライアンスのシステム時刻の設定

これは、特にアプライアンスが他のデバイスに統合されている場合に推奨される、時刻の設定方法です。統合されたデバイスはすべて、同じの NTP サーバーを使用する必要があります。

NTP サーバーを使用して時間を設定するには、CLI の `ntpconfig` コマンドを使用します。

ステップ 1 **[システム管理（System Administration）] > [時刻設定（Time Settings）]** ページに移動します。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 [時刻の設定方法（Time Keeping Method）] セクションで、[NTP（Network Time Protocol）を使用（Use Network Time Protocol）] を選択します。

ステップ 4 NTP サーバのアドレスを入力し、[行を追加（Add Row）] をクリックします。複数の NTP サーバを追加できます。

ステップ 5 NTP サーバをリストから削除するには、サーバのゴミ箱アイコンをクリックします。

ステップ 6 NTP クエリー用のインターフェイスを選択します。これは、NTP クエリーが発信される IP アドレスになります。

ステップ 7 [NTP認証の使用（Use NTP Authentication）] チェック ボックスをオンにすると、タイムスタンプが信頼できるソースによって生成され、NTP が悪意のあるアクティビティや傍受から保護されます。

ステップ 8 変更を送信し、保存します。

GMT オフセットの選択

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[タイムゾーン（Time Zone）] を選択します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 地域のリストから [GMTオフセット（GMT Offset）] を選択します。[タイムゾーンの設定（Time Zone Setting）] ページが更新され、[タイムゾーン（Time Zone）] フィールドに GMT オフセットが含まれるようになります。

ステップ 5 [タイムゾーン（Time Zone）] フィールドでオフセットを選択します。オフセットとは、グリニッジ子午線のローカル時間であるグリニッジ標準時（GMT）に、加算または減算する時間のことです。時間の前にマイナス記号（「-」）が付いている場合、グリニッジ子午線の西側にあたります。プラス記号（「+」）の場合、グリニッジ子午線の東側にあたります。

ステップ 6 変更を送信し、保存します。

時間帯ファイルの更新

いずれかの国の時間帯ルールに変更があった場合は必ず、アプライアンスの時間帯ファイルを更新する必要があります。

- 時間帯ファイルの自動更新　（69 ページ）
- 時間帯ファイルの手動更新　（69 ページ）

時間帯ファイルの自動更新

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[アップデート設定（Update Settings）] を選択します。

ステップ 3 [時間帯ルールの自動アップデートを有効にする（Enable automatic updates for Time zone rules）] チェックボックスをオンにします。

ステップ 4 間隔を入力します。重要な情報については、ページ上の [?] ヘルプをクリックします。

ステップ 5 変更を送信し、保存します。

時間帯ファイルの手動更新

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[時刻設定（Time Settings）] を選択します。

ステップ 3 [タイムゾーンファイルの更新（Time Zone File Updates）] セクションを確認します。

ステップ 4 使用可能な時間帯ファイルの更新がある場合、[今すぐ更新（Update Now）] をクリックします。

[設定ファイル（Configuration File）] ページ

次のセクションの詳細について	参照先
現在の設定の保存	設定の保存とインポート （70 ページ）
保存されている設定のロード	設定の保存とインポート （70 ページ）
エンドユーザー セーフリスト/ブロックリスト データベース（スパム隔離）	セーフリスト/ブロックリストのバックアップと復元
設定のリセット	工場出荷時の初期状態への設定のリセット （18 ページ）

設定の保存とインポート

（注） ここで説明されている設定ファイルは、セキュリティ管理アプライアンスの設定に使用されます。

セキュリティ管理アプライアンス内の大部分の設定は、1 つの設定ファイルで管理できます。このファイルは Extensible Markup Language（XML）フォーマットで保持されます。

このファイルは次の複数の方法で使用できます。

- プライマリ セキュリティ管理アプライアンスで予期しない障害が発生した場合に、2 番目のセキュリティ管理アプライアンスをすばやく設定し、サービスを復元できます。
- 設定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間違えた場合、保存し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（新しいブラウザの多くに、XML ファイルを直接レンダリングする機能が含まれています）。現在の設定にマイナーエラー（誤入力など）があった場合、この機能がトラブルシューティングに役立つことがあります。
- 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 を介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 ファイルの一部を CLI に直接貼り付けたりすることができます。
- このファイルは XML 形式になっているため、設定ファイルのすべての XML エンティティが記述された、関連する文書型定義（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）。
- コンフィギュレーションファイルを使用して、別のアプライアンス（クローン作成された仮想アプライアンスなど）を迅速に設定できます。

コンフィギュレーション ファイルの管理

- セーフリスト/ブロックリストのバックアップと復元
- 工場出荷時の初期状態への設定のリセット （18 ページ）
- 以前コミットしたコンフィギュレーションへのロールバック （74 ページ）

現在の設定ファイルの保存およびエクスポート

[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [設定ファイル（Configuration File）] ページの [現在の構成（Current Configuration）] 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 ルートの設定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。

パスフレーズのマスク

必要に応じてチェック ボックスをオンにして、ユーザのパスフレーズをマスクします。パスフレーズをマスクすると、元の暗号化されたパスフレーズが、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。

（注） パスフレーズがマスクされたコンフィギュレーション ファイルをロードして AsyncOS に戻すことはできません。

パスフレーズの暗号化

[設定ファイル内のパスフレーズを隠す（Encrypt passphrases in the Configuration Files）] チェックボックスをクリックして、ユーザのパスフレーズをマスクできます。次に、暗号化される、設定ファイル内の重要なセキュリティ パラメータを示します。

- 証明書の秘密キー
- RADIUS パスワード
- LDAP バインドのパスワード
- ローカル ユーザのパスワードのハッシュ
- SNMP パスワード
- 発信 SMTP 認証パスワード

- PostX 暗号化キー
- PostX 暗号化プロキシ パスワード
- FTP プッシュ ログ サブスクリプションのパスワード
- IPMI LAN パスワード
- アップデータ サーバの URL

これは、saveconfig コマンドを使用してコマンドライン インターフェイスでも構成できます。

コンフィギュレーション ファイルのロード

コンフィギュレーション ファイルは、設定をロードするアプライアンスと同じバージョンの AsyncOS を実行しているアプライアンスから保存される必要があります。

パスフレーズ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。

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、Cisco コンテンツ セキュリティ アプライアンスの configuration ディレクトリにある 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。設定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、設定ファイルを検証できます。

いずれのインポート方法でも、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（上記の宣言タグを含み、<config></config> タグ内に存在する場合）をインポートできます。

「complete（完全）」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、次のコードをアップロードまたは貼り付けると、検証エラーが発生します。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
  <autosupport_enabled>0</autosu
</config>
```

しかし、次のコードをアップロードまたは貼り付けても、検証エラーは発生しません。

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<config>
```

```
  <autosupport_enabled>0</autosupport_enabled>
</config>
```

「unique（一意）」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てないため、次のコード（宣言および <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>
```

しかし、システムにはそれぞれ異なる受信者アクセステーブルが定義された複数のリスナーが定義されている可能性があるため、次のコードのみをアップロードすることは多義的であると見なされます。

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

多義的であるため、「完全」な構文であっても許可されません。

注意 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。

空のタグと省略されたタグ

設定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、次のコード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。

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

注意 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。管理ポートで別のプロトコル、シリアル インターフェイス、または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フレーズのロードについての注意事項

パスフレーズが必要なログ 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フレーズ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フレーズ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 設定ファイルの「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ます。

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

現在の設定のリセット

現在の設定をリセットすると、Cisco コンテンツ セキュリティ アプライアンスは設定を元の出荷時デフォルト値に戻します。リセットする前に設定を保存してください。

工場出荷時の初期状態への設定のリセット （18 ページ） を参照してください。

以前コミットしたコンフィギュレーションへのロールバック

以前コミットされた設定にロール バックできます。

コマンドライン インターフェイスで rollbackconfig コマンドを使用して、直近の 10 件のコミットから 1 件を選択します。

ロール バックをコミットすることを促されたときに No を入力した場合、このロール バックは、次回変更をコミットする際にコミットされます。

管理者アクセス権を持つユーザーだけが rollbackconfig コマンドを使用できます。

（注） 以前の設定が復元されてもログ メッセージまたはアラートは生成されません。

（注） 既存のデータを保持する十分なサイズにディスク領域を再割り当てするなどの一部のコミットでは、データ漏洩が発生する可能性があります。

設定ファイル用の 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
- rollbackconfig
- resetconfig（工場出荷時の初期状態への設定のリセット （18 ページ）を参照）
- publishconfig
- backupconfig （セキュリティ管理アプライアンスのデータのバックアップ （23 ページ）を参照）
- trailblazerconfig

showconfig、mailconfig、および saveconfig コマンド

設定コマンドの 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フレーズを含めるかどうか選択することを求められます。パスフレーズを含めないことを選択すると、パスフレーズフィールドが空白のままになります。セキュリティ違反を心配する場合は、パスフレーズ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、パスフレーズ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フレーズのロードについての注意事項 （74 ページ）を参照してください。

（注） 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に、パスフレーズを含めることを選択すると（「Do you want to include passphrases?」に「yes」と回答した場合）、パスフレーズは暗号化されます。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 passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig.
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: 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ー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 passphrases? Please be aware that a configuration
```

```
without passphrases will fail when reloaded with loadconfig.  [N]> y
The configuration file has been sent to administrator@example.com.
```

セキュリティ管理アプライアンスで saveconfig コマンドを使用すると、一意のファイル名を使用して、すべての Configuration Master ファイル（ESA）が configuration ディレクトリに保存されます。

```
mail3.example.com> saveconfig
Do you want to include passphrases? Please be aware that a configuration without
passphrases
will fail when reloaded with loadconfig.  [N]> y
The file C650-00065B8FCEAB-31PM121-20030630T130433.xml has been saved in the configuration
 directory.
mail3.example.com>
```

loadconfig コマンド

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

- configuration ディレクトリに情報を格納し、アップロードする。
- 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 （72 ページ）を参照してください。

rollbackconfig コマンド

以前コミットしたコンフィギュレーションへのロールバック （74 ページ） を参照してください。

publishconfig コマンド

変更を Configuration Master に公開するには、publishconfig コマンドを使用します。構文は次のようになります。

publishconfig *config_master* [*job_name*] [*host_list* | *host_ip*

ここで、*config_master* は、サポートされている Configuration Master です。これらの Configuration Master のリストは、このリリースのリリース ノートの「Compatibility Matrix」（http://www.cisco.com/en/US/products/ps10155/prod_release_notes_list.html）にあります。このキーワードは必須です。キーワード *job_name* は省略可能で、指定しなかった場合は生成されます。

キーワード *host_list* は、公開される WSA アプライアンスのホスト名または IP アドレスのリストで、指定しなかった場合は、Configuration Master に割り当てられているすべてのホストに公開されます。オプションの *host_ip* には、カンマで区切って複数のホスト IP アドレスを指定できます。

publishconfig コマンドが成功したことを確認するには、smad_logs ファイルを調べます。[ウェブ（Web）] > [ユーティリティ（Utilities）] > [Webアプライアンスステータス（Web Appliance Status）] を選択することで、セキュリティ管理アプライアンスの GUI から公開履歴が成功だったことを確認することもできます。このページから、公開履歴の詳細を調べる Web アプライ

アンスを選択します。また、[ウェブ（Web）]>[ユーティリティ（Utilities）]>[公開（Publish）]>[公開履歴（Publish History）] により、[公開履歴（Publish History）] ページに進むことができます。

trailblazerconfig コマンド

`trailblazerconfig` コマンドを使用すると、新しい Web インターフェイスで HTTP と HTTPS のポートを介して受信接続と送信接続をルーティングできます。

インライン ヘルプを参照するには、CLI で `help trailblazerconfig` コマンドを使用します。

構文は次のようになります。

```
trailblazerconfig enable <https_port> <http_port>

trailblazerconfig disable

trailblazerconfig status
```

ここで、

`'enable'` は、デフォルトのポート（HTTPS: 4431）で trailblazer 設定を実行します。

`'disable'` は、trailblazer 設定を無効にします。

`'status'` は trailblazer 設定のステータスをチェックします。

重要 デフォルトで、`trailblazerconfig` のCLI コマンドはアプライアンスで有効になっています。HTTPS ポートがファイアウォールで開かれていることを確認します。また、アプライアンスにアクセスするために指定したホスト名を DNS サーバが解決できることを確認します。

`trailblazerconfig` コマンドを使用すると、次の問題を回避できます。

- 特定のブラウザで API ポートの複数の証明書を追加する必要がある。
- スパム隔離、セーフリスト、またはブロックリストのページを更新するときに、レガシー Web インターフェイスにリダイレクトされる。
- 高度なマルウェア防御レポート ページのメトリック バーにデータが含まれない。

（注） アプライアンスで `trailblazerconfig` コマンドを有効にすると、リクエスト URL にはホスト名に付加された `trailblazerconfig` HTTPS ポート番号が含まれます。

updatepvocert コマンド

2048 ビットの CA 証明書を更新し、FIPS モードの管理対象 Cisco E メール セキュリティ アプライアンスで一元化されたポリシー、ウイルス、および隔離を有効にするには、CLI で updatepvocert コマンドを使用する必要があります。

管理対象の E メール セキュリティ アプライアンスで、FIPS を有効にすると、一元化されたポリシー、ウイルス、アウトブレイク隔離は無効になります。AsyncOS 13.0 以降、 FIPS モードでは、2048 ビットの証明書を使用して、ポリシー、ウイルス、およびアウトブレイク検疫の一元管理設定が有効になります。以前の AsyncOS バージョンには、サイズが 1024 ビットの証明書があります。

```
example.mail.com> updatepvocert
This command will recreate the PVO certificate and key of strength 2048 bits.
Also, the new certificate will be signed by a CA of strength 2048 bits.
Hermes process will restart post certificate update. No commit will be required.
Do you want to proceed with the certificate update? [Y]>

Certificate updated successfully. Hermes restart needed for the changes to be effective.
Do you want to restart hermes? []> Y

Enter the number of seconds to wait before abruptly closing connections. [30]>

Waiting for listeners to exit... Receiving suspended for euq_listener, cpq_listener.
Waiting for outgoing deliveries to finish... Mail delivery suspended. Receiving resumed
 for euq_listener, cpq_listener. Mail delivery resumed.
Hermes will be up in a moment. Run the status command for hermes.

example.mail.com >
```

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、IP インターフェイスおよびアプライアンスへのアクセスを参照してください。

ステップ 2 設定ファイル全体または設定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。

例：

```
mail3.example.com>
l
oadconfig
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、システムセットアップ 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、およびゲートウェイ情報を変更します（詳細については、システムセットアップ ウィザードの実行を参照してください）。最後に、変更を確定します。

例：

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

ディスク領域の管理

組織で使用する各機能に、使用可能な最大量まで、使用可能なディスク領域を割り当てることができます。

（仮想アプライアンスのみ）使用可能なディスク領域の拡大

ESXi 5.5 および VMFS 5 を実行する仮想アプライアンスの場合、2 TB を超えるディスク領域を割り当てることができます。ESXi 5.1 を実行するアプライアンスの場合は 2 TB に制限されます。

（注） ESXi でのディスク領域の削減はサポートされません。詳細については、VMware のマニュアルを参照してください。

仮想アプライアンス インスタンスにディスク領域を追加するには、次の手順を実行します。

始める前に

必要な追加ディスク領域を慎重に検討します。

ステップ 1 Cisco コンテンツ セキュリティ管理アプライアンス インスタンスを停止します。

ステップ 2 VMware が提供するユーティリティまたは管理ツールを使用してディスク領域を増やします。

VMware のマニュアルで仮想ディスク設定の変更に関する情報を参照してください。

ESXi 5.5 の情報は、次のサイトから入手できます。 http://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-81629CAB-72FA-42F0-9F86-F8FD0DE39E57.html

ステップ 3 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 4 [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ディスク管理（Disk Management）] に移動して、変更が反映されていることを確認します。

ディスク領域、クォータ、および使用状況の表示

目的	操作手順
アプライアンスで利用可能な合計ディスク領域を表示する	[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ディスク管理（Disk Management）] を選択します。 [合計割当て容量（Total Space Allocated）] に示されている値（例：184G of 204G）を確認します。
セキュリティ管理アプライアンスのモニタリング サービスごとに、割り当てられているディスク領域および現在使用されているディスク領域の量を表示する	[管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[ディスク管理（Disk Management）] を選択します。
現在使用されている隔離のクォータの割合を表示する	[管理アプライアンス（Management Appliance）]>[集約管理サービス（Centralized Services）]>[システムステータス（System Status）] を選択して、[集約管理サービス（Centralized Services）] セクションで確認します。

最大ディスク領域と割り当てについて

（注） セキュリティ管理アプライアンスの中央集中型レポーティングディスク領域は、電子メールと Web の両方のデータに使用されます。中央集中型電子メール レポーティングと中央集中型 Web レポーティングのどちらか一方をイネーブルにすると、すべての領域がイネーブルにした機能専用になります。両方をイネーブルにした場合、電子メールおよび Web レポーティング データは領域を共有し、領域はファースト カム ベースで割り当てられます。

- 中央集中型 Web レポーティングをイネーブルにしているが、レポーティングにディスク領域が割り当てられていない場合、ディスク領域が割り当てられるまで、中央集中型 Web レポーティングが機能しません。
- その他のクォータを現在の使用量より少なくする前に、不要なデータを削除する必要があります。その他のクォータのディスク領域の管理 （81 ページ）を参照してください。
- ポリシー、ウイルス、およびアウトブレイク隔離のディスク領域を管理する方法については、ポリシー、ウイルス、およびアウトブレイク隔離へのディスク領域の割り当ておよび隔離内のメッセージの保持期間を参照してください。
- 他のすべてのデータ タイプでは、既存の割り当て量を現在の使用量より少なくした場合、新しい割り当て量内にすべてのデータが収まるまで、最も古いデータから削除されます。
- 新しいクォータが現在使用されているディスク領域よりも大きい場合、データは失われません。
- 割り当て量をゼロに設定すると、データは保持されなくなります。

ディスク領域に関するアラートの受信の確認

その他のディスク使用量がクォータの 75% に達すると、警告レベルのシステム アラートを受信します。これらのアラートを受信した場合は、対処する必要があります。

確実にアラートが届くようにするには、アラートの管理 （52 ページ）を参照してください。

その他のクォータのディスク領域の管理

その他のクォータにはシステム データとユーザ データが含まれます。システム データは削除できません。管理できるユーザ データには次のファイル タイプがあります。

管理対象	手順
ログ ファイル	[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] に移動して、以下を実行します。 • [サイズ（Size）]列見出しをクリックして、最も多くのディスク領域を消費しているログを確認します。 • 生成されるすべてのログ サブスクリプションが必要であることを確認します。 • 必要以上に詳細なログ レベルになっていないかを確認します。 • 可能な場合は、ロールオーバー ファイル サイズを小さくします。

管理対象	手順
パケット キャプチャ	[ヘルプとサポート（Help and Support）]（画面上部の右側付近）> [パケットキャプチャ（Packet Capture）] に移動します。不要なキャプチャを削除します。
コンフィギュレーション ファイル （これらのファイルが多くのディスク領域を消費する可能性は低いと考えられます）。	アプライアンスの /data/pub ディレクトリに FTP でアクセスします。 アプライアンスへの FTP アクセスを設定するには、次を参照してください。 FTP 経由でのアプライアンスへのアクセス
クオータ サイズ	[システム管理（System Administration）]> [ディスク管理（Disk Management）] に移動します。

ディスク領域量の再割り当て

ディスク領域が使用していない機能に割り当てられている場合、または、アプライアンスで特定の機能については頻繁にディスク領域が不足するものの他の機能については過剰な領域がある場合は、ディスク領域量の割り当てを変更できます。

すべての機能にさらに領域が必要な場合は、ハードウェアのアップグレード、または仮想アプライアンスへの追加ディスク領域の割り当てを検討してください。「（仮想アプライアンスのみ）使用可能なディスク領域の拡大 （79 ページ）」を参照してください。

始める前に

- ディスク割り当てを変更すると、既存のデータまたは機能のアベイラビリティに影響する場合があります。最大ディスク領域と割り当てについて （80 ページ）で情報を参照してください。
- 隔離からメッセージを手動で解放または削除することで、隔離用の領域を一時的に作成できます。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]> [システム管理（System Administration）]> [ディスク管理（Disk Management）] を選択します。

ステップ 3 [ディスククォータの編集（Edit Disk Quotas）] をクリックします。

ステップ 4 [ディスククォータの編集（Edit Disk Quotas）] ページで、各サービスに割り当てるディスク領域の量（ギガバイト単位）を入力します。

ステップ 5 **[送信（Submit）]** をクリックします。

ステップ 6 確認ダイアログボックスで、[新しいクオータの設定（Set New Quotas）] をクリックします。

ステップ 7 [確定する（Commit）] をクリックして変更を保存します。

Eメール セキュリティ アプライアンスのシステムの状態グラフの参照のしきい値の調整

（注） これらのしきい値に関連するアラートを受信するには、各管理対象Eメールセキュリティアプライアンスのしきい値を設定します。詳細については、お使いの E メール セキュリティ アプライアンス リリースのユーザ ガイドまたはオンライン ヘルプで、システムの状態のしきい値の設定に関する情報を参照してください。個々のアプライアンスからオンデマンドのシステムの状態チェックを実行できます。アプライアンスの状態のチェックについては、お使いの E メール セキュリティ アプライアンス リリースのユーザ ガイドまたはオンライン ヘルプを参照してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 **[管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [システムの状態（System Health）]** をクリックします。

ステップ 3 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 4 オプションを設定します。

オプション	説明
全体のCPU使用率（Overall CPU Usage）	デフォルト：85%
メモリページスワップ（Memory Page Swapping）	デフォルト：5000 ページ
ワークキュー内の最大メッセージ（Maximum Messages in Work Queue）	デフォルト：500 メッセージ

ステップ 5 変更を送信し、保存します。

SAML 2.0 による SSO

• Cisco セキュリティ管理アプライアンスでの SSO の設定方法 （85 ページ）

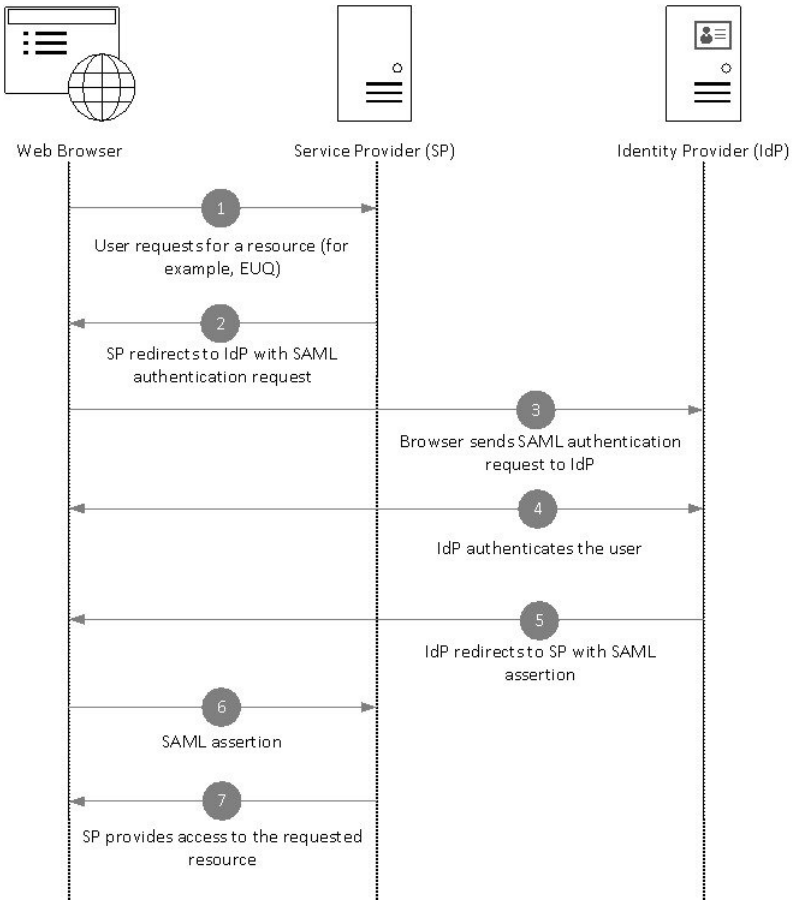
SSO および SAML 2.0 について

Cisco コンテンツ セキュリティ管理アプライアンスは SAML 2.0 SSO をサポートするようになりました。これによりエンドユーザはその組織内で他の SAML 2.0 SSO 対応サービスへのアクセスに使用している同じクレデンシャルを使用してスパム隔離にアクセスできます。たとえば、SAML ID プロバイダー（IdP）として Ping 認証を有効にしており、SAML 2.0 SSO 対応の Rally、Salesforce、および Dropbox のアカウントを持っています。サービス プロバイダー（SP）として SAML 2.0 SSO をサポートするように Cisco コンテンツ セキュリティ管理アプライアンスを構成すると、エンドユーザーは一度サインインするだけでスパム隔離を含むすべてのサービスにアクセスできるようになります。

SAML 2.0 SSO のワークフロー

SAML 2.0 SSO ワークフローを、次の図に表示します。

図 *7: SAML 2.0 SSO* のワークフロー



ワークフロー

1. エンドユーザは、Web ブラウザを使用して、サービス プロバイダー（アプライアンス）からリソースを要求します。たとえば、エンドユーザは、スパム通知のスパム隔離リンクをクリックします。
2. サービスプロバイダーは、SAML 認証要求で Web ブラウザに要求をリダイレクトします。
3. Web ブラウザは、ID プロバイダーに SAML 認証要求をリレーします。
4. ID プロバイダーは、エンドユーザを認証します。ID プロバイダーはエンドユーザにログイン ページを表示し、エンドユーザがログインします。
5. ID プロバイダーは、SAML アサーションを生成して、Web ブラウザに送り返します。
6. Web ブラウザは、サービス プロバイダーに SAML アサーションをリレーします。
7. サービス プロバイダーは、要求されたリソースへのアクセスを付与します。

SAML 2.0 に関する注意事項と制約事項

ログアウト

エンドユーザが、スパム隔離からログアウトしても、他の SAML 2.0 SSO が有効なアプリケーションからはログアウトされません。

一般

Cisco コンテンツ セキュリティ管理アプライアンス上では、サービス プロバイダーと ID プロバイダーのインスタンスを 1 つのみ構成できます。

管理者のスパム隔離へのアクセス

スパム隔離用の SSO を有効にしている場合、管理者はスパム隔離の URL（http://<appliance_hostname>:<port>）を使用してスパム隔離へアクセスできなくなることを覚えておいてください。管理者は Web インターフェイスを使用してスパム隔離にアクセスできます（[メール（Email）] > [メッセージの隔離（Message Quarantine）] > [スパム隔離（Spam Quarantine）]）。

Cisco セキュリティ管理アプライアンスでの SSO の設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	前提条件を確認します。	前提条件 （86 ページ）

	コマンドまたはアクション	目的
ステップ 2	サービス プロバイダーとして、アプライアンスを設定します。	サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定（87ページ）
ステップ 3	[IDP で] アプライアンスを操作するように ID プロバイダーを設定します。	Cisco セキュリティ管理アプライアンスと通信するための ID プロバイダーの設定 （89 ページ）
ステップ 4	アプライアンスで ID プロバイダーを設定します。	Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成 （92 ページ）
ステップ 5	アプライアンスで SAML を使用して外部認証を有効にします。	SAML 認証の有効化 （93 ページ）

前提条件

- サポートされるアイデンティティ プロバイダー （86 ページ）
- セキュアな通信の証明書 （86 ページ）

サポートされるアイデンティティ プロバイダー

組織で使用する ID プロバイダーが Cisco E メール セキュリティ アプライアンスでサポートされているかどうかを確認します。次に、サポートされる ID プロバイダーを示します。

- Microsoft Active Directory Federation Services（AD FS）2.0 以降
- Duo Access Gateway
- Azure AD

セキュアな通信の証明書

アプライアンスと ID プロバイダーの間の通信をセキュリティで保護するために必要な次の証明書を取得します。

- アプライアンスで SAML 認証要求に署名する、または ID プロバイダーで SAML アサーションを暗号化する場合、自己署名証明書または信頼できる CA の証明書、および関連付けられている秘密キーを取得します。
- ID プロバイダーで SAML アサーションに署名する場合は、ID プロバイダーの証明書を取得してアプライアンスにインポートします。アプライアンスはこの証明書を使用して、署名済み SAML アサーションを確認します。

証明書の変換

通常、アプライアンスから取得した証明書は .pfx 形式であり、アプライアンスをサービス プロバイダーとして設定するときには .pem 形式に変換する必要があります。

証明書を .pfx 形式から .pem 形式に変換するには、次の操作を行います。

- OpenSSL ツールをダウンロードしてインストールし、アプライアンスから取得した証明書ファイル（.pfx）をインポートします。
- 次のコマンドを実行して、証明書を .pem 形式でエクスポートします。`openssl pkcs12 -in <certname>.pfx -nokeys -out cert.pem`
- 次のコマンドを実行して、秘密キーを .pem 形式でエクスポートします。`openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes`
- 次のコマンドを実行して、秘密キーからパスフレーズを削除します。`openssl rsa -in key.pem -out server.key`

サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定

始める前に

「前提条件 （86 ページ）」を確認してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [SAML] を選択します。

ステップ 3 [サービスプロバイダー（Service Provider）] セクションで [サービスプロバイダーの追加（Add Service Provider）] をクリックします。

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	サービス プロバイダー プロファイルの名前を入力します。
コンフィギュレーション設定	
エンティティ ID	サービスプロバイダー（この場合、ご使用のアプライアンス）のグローバルな固有の名前を入力します。通常、サービスプロバイダーエンティティ ID の形式は URI です。
名前 ID の形式	ID プロバイダーが SAML アサーションでユーザを指定するのに使用する形式。 このフィールドは設定できません。ID プロバイダーを設定する際にこの値が必要になります。

フィールド	説明
アサーション コンシューマ URL	認証が正常に完了した後で、ID プロバイダーが SAML アサーションを送信する URL。この場合、スパム隔離の URL です。 このフィールドは設定できません。IDプロバイダーを設定する際にこの値が必要になります。
SP 証明書	（注）　秘密キーは .pem 形式である必要があります。 **認証要求の署名** アプライアンスで SAML 認証要求に署名する場合、 **1.** 証明書と関連付けられている秘密キーをアップロードします。 **2.** 秘密キーのパスフレーズを入力します。 **3.** [署名要求（Sign Request）] を選択します。 **暗号化されたアサーションの復号** SAMLアサーションを暗号化するようにIDプロバイダーを設定する場合、 **1.** 証明書と関連付けられている秘密キーをアップロードします。 **2.** 秘密キーのパスフレーズを入力します。
署名アサーション	SAML アサーションに署名するように ID プロバイダーを設定する場合、[署名アサーション（Sign Assertions）] を選択します。 このオプションを選択すると、アプライアンスに ID プロバイダーの証明書を追加する必要があります。Cisco セキュリティ管理アプライアンスと通信するための ID プロバイダーの設定 （89 ページ）を参照してください。
組織詳細	組織の詳細を入力します。 ID プロバイダーは、エラー ログでこの情報を使用します。
技術的な問い合わせ先	技術的な問い合わせ先の電子メール アドレスを入力します。 ID プロバイダーは、エラー ログでこの情報を使用します。

ステップ 5 **[送信（Submit）]** をクリックします。

ステップ 6 [SSOの設定（SSO Settings）] ページに表示されるサービス プロバイダーのメタデータ（エンティティ ID とアサーション顧客 URL）と、[サービスプロバイダー設定（Service Provider Settings）] ページに表示される名前 ID の形式を書き留めます。ID プロバイダーでサービス プロバイダーを設定するときに、これらの詳細が必要になります。

必要に応じて、メタデータをファイルとしてエクスポートできます。[メタデータのエクスポート（Export Metadata）] をクリックして、メタデータ ファイルを保存します。一部の ID プロバイダーでは、メタデータ ファイルからサービス プロバイダーの詳細をロードできます。

次のタスク

アプライアンスと通信するようにIDプロバイダーを設定します。Cisco セキュリティ管理アプライアンスと通信するための ID プロバイダーの設定 （89 ページ） を参照してください。

Cisco セキュリティ管理アプライアンスと通信するための ID プロバイダーの設定

始める前に

次の内容について確認してください。

- アプライアンスがサービス プロバイダーとして構成されている。サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定 （87 ページ）を参照してください。
- サービスプロバイダーのメタデータの詳細がコピーされているか、またはメタデータ ファイルがエクスポートされている。サービスプロバイダーとしてのCiscoコンテンツセキュリティ管理アプライアンスの設定 （87 ページ）を参照してください。

ステップ 1 ID プロバイダーで、次のいずれかを実行します。

- サービス プロバイダー（アプライアンス）の詳細を手動で構成します。
- ID プロバイダーがメタデータ ファイルからサービス プロバイダーの詳細をロードすることを許可している場合は、メタデータ ファイルをインポートします。

アプライアンスがSAML認証要求に署名するように構成済みの場合、またはSAMLアサーションを暗号化する予定の場合は、必ず関連する証明書を ID プロバイダーに追加します。

ID プロバイダー固有の手順については、以下を参照してください。

- Cisco セキュリティ管理アプライアンスと通信するための AD FS の設定 （90 ページ）。
- Cisco セキュリティ管理アプライアンスと通信するための Azure AD の設定 （91 ページ）。
- Cisco セキュリティ管理アプライアンスと通信するための Duo Access Gateway の設定 （91 ページ）。

ステップ 2 ID プロバイダーのメタデータを書き留めるかまたはメタデータをファイルとしてエクスポートします。

次のタスク

アプライアンス上でIDプロバイダーの設定を構成します。Ciscoセキュリティ管理アプライアンスと通信するための ID プロバイダーの設定 （89 ページ） を参照してください。

Cisco セキュリティ管理アプライアンスと通信するための AD FS の設定

以下は、お使いのアプライアンスと通信するように AD FS（2.0 以降）を設定するために実行する必要があるタスクの概要です。完全かつ詳細な手順については、*Microsoft* のマニュアルを参照してください。

- リレー パーティとしてサービス プロバイダー（アプライアンス）のアサーション コンシューマ URL を追加します。
- [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [ID（Identifiers）] > [リレー パーティ ID（Relaying Party Identifier）] で、サービス プロバイダー（アプライアンス）のエンティティ ID を入力します。この値が、アプライアンスのサービス プロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービス プロバイダー（アプライアンス）を構成済みの場合は、サービスプロバイダーの証明書（認証要求を署名するために使用される）を [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [署名（Signature）] の下で .cer 形式でアップロードします。
- 暗号化された SAML アサーションを送信するように AD FS を構成する場合は、サービスプロバイダー（アプライアンス）の証明書を [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [暗号化（Encryption）] の下で .cer 形式でアップロードします。
- [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [詳細（Advanced）] の下で、セキュアハッシュ アルゴリズムを SHA-1 に設定します。
- 応答に SPNameQualifier を含めるためのカスタム ルールを追加します。次のファイルは、サンプルのカスタム ルールです。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>

issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer=
c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties ["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
 =
"urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified");
```

- 要求ルールを編集し、電子メール アドレスの LDAP 属性を発信要求タイプ（電子メール アドレス）として送信する発行変換規則を追加します。また、発行変換規則を追加して、グループ属性の LDAP 属性を送信要求タイプ（未指定のグループ）として送信するようにします。

Cisco セキュリティ管理アプライアンスと通信するための Azure AD の設定

以下は、お使いのアプライアンスと通信するように Azure AD を設定するために実行する必要があるタスクの概要です。完全かつ詳細な手順については、Microsoft Azure AD のマニュアルを参照してください。

- SAML アサーションを受信および処理するサービス プロバイダー識別子として、サービス プロバイダーの（アプライアンスの）アサーション コンシューマー URL を追加します。
- [エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [基本SAML設定（Basic SAML Configuration）] にある Azure ポータルにサービス プロバイダーの（アプライアンスの）エンティティ ID を入力します。この値が、アプライアンスのサービス プロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービス プロバイダー（アプライアンス）を構成済みの場合は、[SAML署名証明書（SAML Signing Certificate section）] セクション（[エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [SAML署名証明書（SAML Signing Certificate）]）で、サービス プロバイダーの証明書（認証要求を署名するために使用される）をアップロードします。
- [ユーザ属性とクレーム（User Attributes and Claims）] セクション（[エンタープライズアプリケーション（Enterprise Application）] > [新しいアプリケーション（New Application）] > [ギャラリー以外のアプリケーション（Non-gallery application）] > [シングルサインオン（Single Sign-On）] > [ユーザ属性とクレーム（User Attributes and Claims）]）でグループ クレームを設定し、グループ属性を追加します。
- ユーザが SAML アサーションまたは応答に基づいてアプリケーションにログインできるようにするには、[企業アプリケーション（Enterprise Application）] > [新規アプリケーション（New Application）] > [非ギャラリーアプリケーション（Non-gallery application）] > [ユーザとグループ（Users & Groups）] の下にユーザとグループを追加します。

Cisco セキュリティ管理アプライアンスと通信するための Duo Access Gateway の設定

以下は、お使いのアプライアンスと通信するように Duo Access Gateway を設定するために実行する必要があるタスクの概要です。完全かつ詳細な手順については、Duo Security のマニュアルを参照してください。

- SAML アサーションを受信および処理するサービス プロバイダー エンドポイントとして、サービス プロバイダーの（アプライアンスの）アサーション コンシューマー URL を追加します。
- [Duo管理パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）] > [SAMLサービスプロバイダー（SAML Service Provider）] で、サービス プロバイダー（アプライアンス）のエンティティ ID を入力しま

す。この値が、アプライアンスのサービス プロバイダー設定のエンティティ ID 値と同じかどうかを確認します。

- 署名入りの SAML 認証要求を送信するようにサービス プロバイダー（アプライアンス）を構成済みの場合は、Duo Access Gateway に認証ソースを設定する際に、サービス プロバイダーの証明書（認証要求を署名するために使用される）を .cer 形式でアップロードします。
- 暗号化された SAML アサーションを送信するように Duo を構成する計画の場合は、Duo Access Gateway に認証ソースを設定する際に、サービス プロバイダーの（アプライアンスの）証明書を .cer 形式でアップロードします。
- [Duo管理パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）] > [SAMLサービスプロバイダー（SAML Service Provider）] で、NameID 形式として [未指定（unspecified）] を選択します。
- [Duo管理パネル（Duo Admin Panel）] > [アプリケーション（Applications）] > [アプリケーションの保護（Protect an Application）] > [SAMLサービスプロバイダー（SAML Service Provider）] で、セキュア ハッシュ アルゴリズムを SHA-256 に設定します。
- [Duo管理パネル（Duo Admin Panel）] で [SAML-サービスプロバイダー設定（SAML - Service Provider Setting）] を設定ファイルとして保存し、Duo Access Gateway でその設定ファイルを SAML アプリケーションとしてインポートします。

Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成

始める前に

次の内容について確認してください。

- アプライアンスとの通信のための ID プロバイダーが構成されている。Cisco セキュリティ管理アプライアンスと通信するための ID プロバイダーの設定 （89 ページ）を参照してください。
- ID プロバイダーのメタデータの詳細またはエクスポートされたメタデータ ファイルがコピーされている。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [SAML] を選択します。

ステップ 3 [ID プロバイダー（Identity Provider）] セクションで、[ID プロバイダーの追加（Add Identity Provider）] をクリックします。

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	ID プロバイダー プロファイルの名前を入力します。
構成設定（ID プロバイダー設定の手動構成）	
エンティティ ID	IDプロバイダーのグローバルに一意の名前を入力します。通常、ID プロバイダー エンティティ ID の形式は URI です。
SSO URL	サービスプロバイダーがSAML認証要求を送信する必要があるURLを指定します。
証明書	ID プロバイダーが SAML アサーションに署名する場合、ID プロバイダーの署名証明書をアップロードする必要があります。
構成設定（ID プロバイダー メタデータのインポート）	
IDP メタデータのインポート	[メタデータのインポート（Import Metadata）] をクリックして、メタデータ ファイルを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

SAML 認証の有効化 （93 ページ）

SAML 認証の有効化

SAML を使用したシングル サインオンを有効化し、ユーザを認証してユーザのグループをシスコのルールに割り当てることができます。

始める前に

サービス プロバイダーおよびIDプロバイダーの設定を含むSAMLプロファイルが設定済みである必要があります。「Ciscoセキュリティ管理アプライアンスでのSSOの設定方法 （85ページ）」を参照してください。

ステップ 1 [管理アプライアンス（Management Appliances）] > [システム管理（System Administration）] > [ユーザ（Users）] に移動します。

ステップ 2 **[Web 認証（Web Authentication）]** セクションまでスクロールします。

ステップ 3 **[有効（Enable）]** をクリックします。

ステップ 4 **[外部認証を有効にする（Enable External Authentication）]** チェックボックスをオンにします。

ステップ 5 ドロップダウンリストから、認証タイプとして [SAML] を選択します。

ステップ 6 （任意）[外部認証属性名マップ（External Authentication Attribute Name Map）] フィールドに、グループマッピングから検索する属性名を入力します。

属性名は、IDプロバイダーに対して設定する属性によって異なります。アプライアンスは、[グループマッピング（Group Mapping）] フィールドで、属性名の一致するエントリを検索します。これは省略可能であり、設定しない場合、アプライアンスは[グループマッピング（Group Mapping）] フィールドに存在するすべての属性の一致するエントリを検索します。

ステップ 7 [グループマッピング（Group Mapping）] フィールドに、事前定義済みまたはカスタムのユーザ ロールに基づいて SAML ディレクトリで定義されているグループ名属性を入力します。[行の追加（Add Row）] をクリックして複数のロール マッピングを追加できます。

グループ マッピングには、グループ属性を含める必要があります。「未指定のグループ（Unspecified Groups）」属性を追加して、SAML アサーションまたは応答を認証できます。

ユーザ ロール タイプの詳細については、[ユーザー（Users）] ページを参照してください。

ステップ 8 変更を送信し、保存します。

次のタスク

SAML 外部認証を有効にした後は、アプライアンスのログイン ページの [シングルサインオンを使用（Use Single Sign On）] リンクを使用し、ユーザ名を入力してアプライアンスにログインできます。

スパム隔離用の SSO の設定方法

	操作内容	詳細
ステップ 1	前提条件を確認します。	前提条件 （95 ページ）
ステップ 2	サービスプロバイダーとして、アプライアンスを設定します。	サービスプロバイダーとしてのCisco コンテンツ セキュリティ管理アプライアンスの設定 （95 ページ）
ステップ 3：	[IDP で] アプライアンスを操作するように ID プロバイダーを設定します。	Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成
ステップ 4：	アプライアンスで ID プロバイダーを設定します。	Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成 （99 ページ）
ステップ 5	アプライアンスでスパム隔離用の SSO を有効にします。	スパム隔離のための SSO の有効化 （100 ページ）
ステップ 6：	エンドユーザに新しい認証メカニズムについて通知します。	

前提条件

- 組織で使用される ID プロバイダーが Cisco コンテンツ セキュリティ管理アプライアンスでサポートされているかどうかを確認します。次に、サポートされる ID プロバイダーを示します。
  - Microsoft Active Directory Federation Services（AD FS）2.0
  - Ping Identity PingFederate 7.2
  - Cisco Web Security Appliance 9.1
- アプライアンスと ID プロバイダーの間の通信をセキュリティで保護するために必要な次の証明書を取得します。
  - アプライアンスで SAML 認証要求に署名する、または ID プロバイダーで SAML アサーションを暗号化する場合、自己署名証明書または信頼されている CA と関連付けられている秘密キーから証明書を取得します。
  - ID プロバイダーで SAML アサーションに署名する場合は、ID プロバイダーの証明書を取得します。アプライアンスはこの証明書を使用して、署名済み SAML アサーションを確認します。

サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定

始める前に

「前提条件 （95 ページ）」を確認してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [SAML] を選択します。

ステップ 3 [サービスプロバイダー（Service Provider）] セクションで [サービスプロバイダーの追加（Add Service Provider）] をクリックします。

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	サービス プロバイダー プロファイルの名前を入力します。
コンフィギュレーション設定	

フィールド	説明
エンティティ ID	サービス プロバイダー（この場合、ご使用のアプライアンス）のグローバルな固有の名前を入力します。通常、サービス プロバイダー エンティティ ID の形式は URI です。
名前 ID の形式	ID プロバイダーが SAML アサーションでユーザを指定するのに使用する形式。 このフィールドは設定できません。IDプロバイダーを設定する際にこの値が必要になります。
アサーション コンシューマ URL	認証が正常に完了した後で、ID プロバイダーが SAML アサーションを送信する URL。この場合、スパム隔離の URL です。 このフィールドは設定できません。IDプロバイダーを設定する際にこの値が必要になります。
SP 証明書	（注）　秘密キーは .pem 形式である必要があります。 **認証要求の署名** アプライアンスで SAML 認証要求に署名する場合、 **1.** 証明書と関連付けられている秘密キーをアップロードします。 **2.** 秘密キーのパスフレーズを入力します。 **3.** [署名要求（Sign Request）] を選択します。 **暗号化されたアサーションの復号** SAMLアサーションを暗号化するようにIDプロバイダーを設定する場合、 **1.** 証明書と関連付けられている秘密キーをアップロードします。 **2.** 秘密キーのパスフレーズを入力します。
署名アサーション	SAML アサーションに署名するように ID プロバイダーを設定する場合、[署名アサーション（Sign Assertions）] を選択します。 このオプションを選択すると、アプライアンスに ID プロバイダーの証明書を追加する必要があります。Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成 （97 ページ）を参照してください。
組織詳細	組織の詳細を入力します。 ID プロバイダーは、エラー ログでこの情報を使用します。
技術的な問い合わせ先	技術的な問い合わせ先の電子メール アドレスを入力します。 ID プロバイダーは、エラー ログでこの情報を使用します。

ステップ 5 **[送信（Submit）]** をクリックします。

ステップ 6 [SSOの設定（SSO Settings）] ページに表示されるサービス プロバイダーのメタデータ（エンティティ ID とアサーション顧客 URL）と、[サービスプロバイダー設定（Service Provider Settings）] ページに表示される名前 ID の形式を書き留めます。ID プロバイダーでサービス プロバイダーを設定するときに、これらの詳細が必要になります。

必要に応じて、メタデータをファイルとしてエクスポートできます。[メタデータのエクスポート（Export Metadata）] をクリックして、メタデータ ファイルを保存します。一部の ID プロバイダーでは、メタデータ ファイルからサービス プロバイダーの詳細をロードできます。

次のタスク

アプライアンスと通信するように ID プロバイダーを設定します。Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成 （97 ページ） を参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成

始める前に

次の内容について確認してください。

- アプライアンスがサービス プロバイダーとして構成されている。サービス プロバイダーとしての Cisco コンテンツ セキュリティ管理アプライアンスの設定 （95 ページ）を参照してください。
- サービスプロバイダーのメタデータの詳細がコピーされているか、またはメタデータ ファイルがエクスポートされている。サービスプロバイダーとしてのCiscoコンテンツセキュリティ管理アプライアンスの設定 （95 ページ）を参照してください。

ステップ 1 ID プロバイダーで、次のいずれかを実行します。

- サービス プロバイダー（アプライアンス）の詳細を手動で構成します。
- ID プロバイダーがメタデータ ファイルからサービス プロバイダーの詳細をロードすることを許可している場合は、メタデータ ファイルをインポートします。

アプライアンスがSAML認証要求に署名するように構成済みの場合、またはSAMLアサーションを暗号化する予定の場合は、必ず関連する証明書を ID プロバイダーに追加します。

ID プロバイダー固有の手順については、以下を参照してください。

- Cisco コンテンツ セキュリティ管理アプライアンスとの通信のための AD FS 2.0 の構成 （98 ページ）
- PingFederate 7.2 を Cisco コンテンツ セキュリティ管理アプライアンスと通信させるための設定 （99 ページ）

- 『*User Guide for AsyncOS for Cisco Web Security Appliances* http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html』の「**Configuring the Appliance as an Identity Provider**」セクション

ステップ 2 ID プロバイダーのメタデータを書き留めるかまたはメタデータをファイルとしてエクスポートします。

次のタスク

アプライアンス上で ID プロバイダーの設定を構成します。Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成 （99 ページ） を参照してください。

Cisco コンテンツ セキュリティ管理アプライアンスとの通信のための AD FS 2.0 の構成

次に示すのは、アプライアンスと通信する AD FS 2.0 を構成するために実行する必要がある高レベルのタスクです。完全かつ詳細な手順については、Microsoft のマニュアルを参照してください。

- リレー パーティとしてサービス プロバイダー（アプライアンス）のアサーション コンシューマ URL を追加します。
- [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [ID（Identifiers）] > [リレー パーティ ID（Relaying Party Identifier）] で、サービス プロバイダー（アプライアンス）のエンティティ ID を入力します。この値が、アプライアンスのサービス プロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名入りの SAML 認証要求を送信するようにサービス プロバイダー（アプライアンス）を構成済みの場合は、サービスプロバイダーの証明書（認証要求を署名するために使用される）を [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [署名（Signature）] の下で .cer 形式でアップロードします。
- 暗号化された SAML アサーションを送信するように AD FS を構成する場合は、サービス プロバイダー（アプライアンス）の証明書を [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [暗号化（Encryption）] の下で .cer 形式でアップロードします。
- [リレー パーティ トラスト（Relaying Party Trusts）] > [プロパティ（Properties）] > [詳細（Advanced）] の下で、セキュアハッシュ アルゴリズムを SHA-1 に設定します。
- 要求ルールを編集し、電子メール アドレスの LDAP 属性を発信要求タイプ（電子メール アドレス）として送信する発行変換規則を追加します。
- 応答に SPNameQualifier を含めるためのカスタム ルールを追加します。次のファイルは、サンプルのカスタム ルールです。

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"] =>
issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer =
 c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties
["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"https://<appliance-hostname>:83");
```

PingFederate 7.2 を Cisco コンテンツ セキュリティ管理アプライアンスと通信させるための設定

以下は、お使いのアプライアンスと通信するように PingFederate 7.2 を設定するために実行する必要があるタスクの概要です。包括的かつ詳細な手順については、Ping Identity のマニュアルを参照してください。

- お使いのサービス プロバイダー（アプライアンス）のアサーション コンシューマ URL を、プロトコル設定におけるエンドポイントとして追加します。
- [SP Connection] > [General Info] > [Partner's Entity ID (Connection ID)] にサービス プロバイダー（アプライアンス）のエンティティ ID を入力します。この値が、アプライアンスのサービス プロバイダー設定のエンティティ ID 値と同じかどうかを確認します。
- 署名付き SAML 認証要求を送信するようにサービス プロバイダー（アプライアンス）を設定している場合、[Signature Verification] セクション（[SP Connection] > [Credentials] > [Signature Verification] > [Signature Verification Certificate]）で、サービス プロバイダーの証明書をアップロードします。
- 暗号化された SAML アサーションを送信するように PingFederate を設定する場合は、[Signature Verification] セクション（[SP Connection] > [Credentials] > [Signature Verification] > [Select XML Encryption Certificate]）で、サービス プロバイダー（アプライアンス）の証明書をアップロードします。
- 属性コントラクトを編集し、LDAP 属性の電子メール アドレスを送信するようにします（[Attribute Sources & User Lookup] > [Attribute Contract Fulfillment]）。

Cisco コンテンツ セキュリティ管理アプライアンスでの ID プロバイダーの設定の構成

始める前に

次の内容について確認してください。

- アプライアンスとの通信のための ID プロバイダーが構成されている。Cisco コンテンツ セキュリティ管理アプライアンスと通信するための ID プロバイダーの構成（97 ページ）を参照してください。
- ID プロバイダーのメタデータの詳細またはエクスポートされたメタデータ ファイルがコピーされている。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [SAML] を選択します。

ステップ 3 [ID プロバイダー（Identity Provider）] セクションで、[ID プロバイダーの追加（Add Identity Provider）] をクリックします。

ステップ 4 次の詳細を入力します。

フィールド	説明
プロファイル名（Profile Name）	ID プロバイダー プロファイルの名前を入力します。

フィールド	説明
構成設定（ID プロバイダー設定の手動構成）	
エンティティ ID	ID プロバイダーのグローバルに一意の名前を入力します。通常、ID プロバイダー エンティティ ID の形式は URI です。
SSO URL	サービス プロバイダーが SAML 認証要求を送信する必要がある URL を指定します。
証明書	ID プロバイダーが SAML アサーションに署名する場合、ID プロバイダーの署名証明書をアップロードする必要があります。
構成設定（ID プロバイダー メタデータのインポート）	
IDP メタデータのインポート	[メタデータのインポート（Import Metadata）] をクリックして、メタデータ ファイルを選択します。

ステップ 5 変更を送信し、保存します。

次のタスク

スパム隔離のための SSO の有効化 （100 ページ）

スパム隔離のための SSO の有効化

始める前に

次の内容について確認してください。

- [管理アプライアンス（Management Appliance）]>[システム管理（System Administration）]>[SAML] ページですべての設定が構成済みである。
- スパム隔離が有効になっている。「スパム隔離」を参照してください。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）]>[集約管理サービス（Centralized Services）]>[スパム隔離（Spam Quarantine）] に移動します。

ステップ 3 [設定の編集（Edit Settings）] をクリックして、[エンドユーザ隔離アクセス（End-User Quarantine Access）] セクションまでスクロールします。

ステップ 4 エンドユーザ隔離アクセスが有効になっていることを確認します。

ステップ 5 エンドユーザ認証方式を **SAML2.0** に設定します。

ステップ 6 （任意）メッセージが解放される前に、メッセージ本文を表示するかどうかを指定します。

ステップ 7 変更を送信し、保存します。

次のタスク

エンドユーザに新しい認証メカニズムについて通知します。

AsyncOS API の Cisco コンテンツセキュリティ管理での OpenID Connect 1.0 の設定

概要

Cisco コンテンツセキュリティ管理アプライアンスは、OpenID Connect 1.0 認証で ID プロバイダ（IDP）を使用するアプリケーションまたはクライアントとの統合をサポートし、アプライアンスで使用可能な AsyncOS API とシームレスに接続します。現在、お使いのアプライアンスは、Microsoft AD FS のみを使用して OpenID Connectで認定されています。

ワークフロー

次のワークフローでは、AD FS を ID プロバイダ、外部アプリケーションをクライアント、アプライアンスをリソースプロバイダとして使用しています。

手順：

1. 次のワークフローでは、AD FS を ID プロバイダ、外部アプリケーションをクライアント、アプライアンスをリソースプロバイダとして使用しています。アプライアンスでの OpenID Connect の設定 （103 ページ） を参照してください。
2. （1 回限りのアクティビティ）アプライアンスは、OpenID Connect の設定メタデータと必要なキーを取得して、ステップ 1 で行った設定に基づいてアクセストークンを検証します。

3. AD FS で外部アプリケーションを認証した後、アクセストークンを取得します。アクセストークンを認証および受信する方法の詳細については、認証プロバイダーまたは ID プロバイダーのマニュアルを参照してください。
4. API 要求をアクセストークンとともにアプライアンスに送信します。
5. アプライアンスは、ステップ 2 で取得したキーセットを使用して API 要求のアクセストークンを検証します。
6. アプライアンスは、アクセストークン内の必要な要求（発行者、対象者）を検証します。
7. アプライアンスは、ロール要求値を使用して、AsyncOS API にアクセスするためのユーザーロール権限を許可し、割り当てます。
8. アプライアンスは、AsyncOS API 要求に適切な応答を提供します。

サンプルアクセストークン

次に、サンプルアクセストークンの形式を示します。

ヘッダー

alg:RSA256

typ:JWT

[….]

ペイロード

claim:aud: CiscoEmailAPICaller

claim:iss:http://adfsserver/adfs/services/trust

claim:iat: 1594712147

claim:exp: 1594712807

claim: CustomOrgIdentifier: MyCustomOrgId

claim: LastName: Fernandes

claim: FirstName: Erik

claim: Email: http://erik.fernandes@customorg.com

claim: Role: LogCollector

claim: Role: ReadOnly

[…..]

アプライアンスは、次のアルゴリズムによって署名されたアクセストークンの検証のみをサポートします。

- RSA256
- RSA384
- RSA512

前提条件

OpenID Connect でアプライアンスを設定する前に、次の前提条件を満たしていることを確認します。

- 組織で使用される認証プロバイダはアプライアンスでサポートされている。
- アプリケーションは認証プロバイダで認証し、アクセストークンを取得できる。
- アプライアンスは、HTTP 経由で認証プロバイダに接続して、OpenID Connect メタデータ設定を取得できる。

アプライアンスでの OpenID Connect の設定

始める前に

次の情報について確認してください。

- （認証プロバイダーの設定に基づいて）認証プロバイダーによって発行された有効なアクセストークン。
- アクセストークンには、アプライアンスが必要な許可チェックを実行できるようにするためのロール情報が含まれている必要があります。

ステップ 1 **[システム管理（System Administration）] > [OpenID Connect]**をクリックします。

ステップ 2 **[設定の編集（Edit Settings）]** をクリックします。

ステップ 3 以下の表に記載される必須パラメータを入力して、OpenID Connect を設定します。

OpenID Connect パラメータ	説明
[IDプロバイダーのメタデータのURL（Identity Provider Metadata URL）]	OpenID Connect の設定メタデータを取得するために使用する ID プロバイダの URL を入力します。メタデータは、アクセストークンの検証に使用されます。 次に、ID プロバイダの URL の例を示します。https://example.com/adfs/.well-known/openid-configuration
発行元（Issuer）	アクセストークンの発行者の値を入力します。 （注） この値は、アクセストークンの検証時にアクセストークンの発行者要求値と一致する必要があります。 次に、発行者の例を示します。http://example.com/adfs/services/trust

OpenID Connect パラメータ	説明
対象読者	アクセストークンの対象者要求値と一致する必要がある対象者の値を入力します。 （注） 複数の対象者値を追加する場合は、[行を追加（Add Row）]をクリックします。
[要求名（Claim Name）]	ユーザロール情報を含むアクセストークンの要求の名前を入力します。要求名は、アクセストークンからロール情報を取得するために使用されます。
ID プロバイダーとアプライアンスロールのマッピング	ID プロバイダサーバーで定義されたユーザーグループロールを入力し、アプライアンスで設定された対応するローカルユーザーロールを選択して、両方のロールをマッピングします。 （注） 複数のロールマッピングレコードを追加する場合は、[行を追加（Add Row）] をクリックします。

ステップ 4 変更を送信し、保存します。

次のタスク

AsyncOS API コールの Authorization Bearer ヘッダーにアクセストークンを含め、API 要求を送信します。

次に、API の Authorization Bearer ヘッダーにアクセストークンを含めた AsynOS API を呼び出す例を示します。

```
curl --location --request
GET 'https://sma.com/sma/api/v2.0/config/logs/subscriptions?retrievalMethod=manual'
--header 'Authorization: Bearer <add access_token here>'
```

CLI を使用したアプライアンスでの OpenID Connect の設定

次のタスクを実行するには、**oidcconfig** コマンドを使用します。

- AsyncOS API の電子メールゲートウェイで OpenID Connect を設定します。
- 電子メールゲートウェイで OpenID Connect 構成設定を削除します。

ビューのカスタマイズ

お気に入りページの使用

（ローカル認証された管理ユーザ限定）よく利用するページのクイック アクセス リストを作成できます。

目的	操作手順
お気に入りリストにページを追加する	追加するページに移動し、ウィンドウの右上隅付近にある [お気に入り（My Favorites）] メニューから [このページをお気に入りに追加（Add This Page To My Favorites）] を選択します。 お気に入りへの変更では確定操作は必要ありません。
お気に入りの順序を変更する	[お気に入り（My Favorites）] > [お気に入りをすべて表示（View All My Favorites）] を選択し、適切な順序にお気に入りをドラッグします。
お気に入りページ、名前、または説明を編集する	[お気に入り（My Favorites）] > [すべてのお気に入りを表示（View All My Favorites）] を選択し、編集するお気に入りの名前をクリックします。
お気に入りを削除する	[お気に入り（My Favorites）] > [お気に入りをすべて表示（View All My Favorites）] を選択し、お気に入りを削除します。
お気に入りページに移動する	ウィンドウの右上隅付近にある [お気に入り（My Favorites）] からページを選択します。
-メインインターフェイスに戻る	お気に入りを選択するか、ページ下部の [前のページに戻る（Return to previous page）] をクリックします。

プリファレンスの設定

セキュリティ管理アプライアンスで設定された管理ユーザ

ローカル認証されたユーザは次のプリファレンスを選択できます。このプリファレンスは、ユーザがセキュリティ管理アプライアンスにログインするたびに適用されます。

- 言語（GUI に適用）
- ランディング ページ（ログイン後に表示されるページ）
- レポート ページのデフォルトの時間範囲（使用可能なオプションは、電子メールおよび Web レポーティング ページのサブセットです）
- レポート ページの表に表示する行数

実際のオプションは、ユーザ ロールによって異なります。

これらのプリファレンスを設定するには、[オプション（Options）]>[環境設定（Preferences）]を設定します。（[オプション（Options）] メニューは、GUI ウィンドウの上部右側にあります）。完了したら変更を送信します。確定する必要はありません。

ヒント [環境設定（Preferences）] ページにアクセスする前に表示していたページに戻るには、ページ下部の [前のページに戻る（Return to previous page）] リンクをクリックします。

外部認証されたユーザ

外部認証されたユーザは、[オプション（Options）] メニューで表示言語を直接選択できます。

全般設定

Web 使用状況分析のモニタリング

[使用状況分析（Usage Analytics）] は、分析統計情報のためにサイトアクティビティデータへのインサイトを得るために使用します。[使用状況分析（Usage Analytics）] が有効になっている場合、アプライアンスは新しい Web インターフェイスでアプライアンスの機能の使用状況データを収集します。使用状況の統計情報は、分析して、アプライアンスのユーザエクスペリエンスを向上させるためのインサイトを得るために使用します。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [全般設定（General Settings）] を選択します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [使用状況分析（Usage Analytics）] フィールドで [有効（Enable）] チェック ボックスをオンにします。

ステップ 5 変更を送信し、保存します。

Web インターフェイスのレンダリングの改善

優れた Web インターフェイスのレンダリングのために、Internet Explorer 互換モードのオーバーライドを有効にすることを推奨します。

（注） この機能を有効にすることが組織のポリシーに違反する場合は、この機能を無効にすることができます。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [管理アプライアンス（Management Appliance）] > [システム管理（System Administration）] > [全般設定（General Settings）] を選択します。

ステップ 3 [設定の編集（Edit Settings）] をクリックします。

ステップ 4 [IE互換モードの上書き（Override IE Compatibility Mode）] フィールドで [有効（Enable）] チェック ボックスをオンにします。

ステップ 5 変更を送信し、保存します。

アプライアンスで有効なサービスの再起動とステータスの表示

CLI で `diagnostic > services` サブコマンドを使用して、以下を実行できます。

- アプライアンスで有効になっているサービスを再起動します。アプライアンスを再起動する必要はありません。
- アプライアンスで有効になっているサービスのステータスを表示します。

例：レポート サービスのステータスの表示

次の例では、`services` コマンドを使用して、アプライアンスで有効になっているレポート サービスのステータスを表示します。

```
mail.example.com> 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.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> reporting
```

```
Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> status

Reporting has been up for 28d 20h 45m 35s.
```

例：メッセージ トラッキング サービスの再起動

次の例では、services コマンドを使用して、アプライアンスで有効になっているメッセージ トラッキング サービスを再起動します。

```
mail.example.com> 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.
- SERVICES - Service Utilities.
[]> services

Choose one of the following services:
- REPORTING - Reporting associated services
- TRACKING - Tracking associated services
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> tracking

Choose the operation you want to perform:
- RESTART - Restart the service
- STATUS - View status of the service
[]> restart
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。