



コマンド：参考例

この章は、次の項で構成されています。

- [リストの読み方](#) (2 ページ)
- [高度なマルウェア防御](#) (2 ページ)
- [スパム対策](#) (11 ページ)
- [グレイメールの検出と安全な購読解約](#) (17 ページ)
- [アンチウイルス](#) (19 ページ)
- [コマンドラインの管理](#) (22 ページ)
- [コンフィギュレーション ファイルの管理](#) (25 ページ)
- [クラスタの管理](#) (30 ページ)
- [データ損失の防止](#) (32 ページ)
- [S/MIME セキュリティ サービス](#) (34 ページ)
- [ドメイン キー](#) (36 ページ)
- [DMARC 検証](#) (47 ページ)
- [DNS](#) (52 ページ)
- [一般的な管理/トラブルシューティング](#) (61 ページ)
- [コンテンツ スキャン](#) (120 ページ)
- [LDAP](#) (121 ページ)
- [メール配信の設定/モニタリング](#) (127 ページ)
- [ネットワーキング設定とネットワーク ツール](#) (161 ページ)
- [アウトブレイク フィルタ](#) (181 ページ)
- [ポリシーの適用](#) (183 ページ)
- [ロギングとアラート](#) (220 ページ)
- [レポート](#) (236 ページ)
- [Senderbase](#) (239 ページ)
- [SMTP サービスの設定](#) (240 ページ)
- [システムのセットアップ](#) (275 ページ)
- [URL フィルタリング](#) (278 ページ)
- [ユーザ管理](#) (285 ページ)
- [仮想アプライアンスの管理](#) (292 ページ)

- [位置情報](#) (293 ページ)

リストの読み方

コマンドごとに説明と1つ以上の使用例が示されています。「使い方」の欄には、以下のコマンド属性についての説明があります。

手順

-
- ステップ1** そのコマンドは、アプライアンス上で **commit** コマンドを実行して確定する必要があるかどうか。
- ステップ2** そのコマンドは特定のモード（クラスタ、グループ、またはマシン）でのみ実行可能か。
- ステップ3** そのコマンドをバッチ形式で実行できるか。

集中管理の詳細については、『*User Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

バッチ形式の詳細については、[コマンドラインインターフェイスの概要](#)を参照してください。

高度なマルウェア防御

- [ampconfig](#) (2 ページ)
- [ampstatus](#) (10 ページ)

ampconfig

ファイルレピュテーションフィルタリングとファイル分析Cisco TACの指導なしで詳細オプションを変更しないでください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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 ampconfig` 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

- [ファイルレピュテーションとファイル分析の有効化](#) (3 ページ)

- [ファイル分析用のファイル タイプの選択 \(4 ページ\)](#)
- [パブリック クラウドのファイル分析サーバを使用するための E メール セキュリティ アプライアンスの設定 \(5 ページ\)](#)
- [\(パブリック クラウド ファイル分析サービスのみ\) アプライアンス グループの設定 \(6 ページ\)](#)
- [オンプレミスのファイル分析サーバを使用するための E メール セキュリティ アプライアンスの設定 \(7 ページ\)](#)
- [オンプレミスのファイル レピュテーション サーバを使用するための E メール セキュリティ アプライアンスの設定 \(8 ページ\)](#)
- [ローカル ファイルのレピュテーション キャッシュのクリア \(9 ページ\)](#)
- [ファイル レピュテーション判定結果値のキャッシュ有効期間の設定 \(9 ページ\)](#)
- [ファイル レトロスペクティブ アラートの抑制 \(10 ページ\)](#)

ファイル レピュテーションとファイル分析の有効化

```
mail.example.com> ampconfig

File Reputation: Disabled

Choose the operation you want to perform:

- SETUP - Configure Advanced-Malware protection service.

[>] setup

File Reputation: Disabled

Would you like to use File Reputation? [Y]>

Would you like to use File Analysis? [Y]>

File types supported for File Analysis:

1. Microsoft Executables

Do you want to modify the file types selected for File Analysis? [N]>

Specify AMP processing timeout (in seconds)

[120]>

Advanced-Malware protection is now enabled on the system.

Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure advanced malware scanning behavior for
default and custom Incoming Mail Policies.

This is recommended for your DEFAULT policy.
```

```

File Reputation: Enabled

File Analysis: Enabled

File types selected for File Analysis:

1. Microsoft Executables

Choose the operation you want to perform:

- SETUP - Configure Advanced-Malware protection service.

- ADVANCED - Set values for AMP parameters (Advanced configuration).

- CLEARCACHE - Clears the local File Reputation cache.

[]>

```

ファイル分析用のファイルタイプの選択

```

mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> setup

File Reputation: Enabled
Would you like to use File Reputation? [Y]> yes

Would you like to use File Analysis? [Y]> yes

Do you want to modify the file types selected for File Analysis? [N]> yes

Enter comma separated serial numbers from the list of groups to select file types associated with the group.

1. Archived and compressed
2. Configuration
3. Database
4. Document
5. Email
6. Encoded and Encrypted
7. Executables [partly selected]
8. Font & Graphics and Images
9. Microsoft Documents
10. Miscellaneous
11. Multimedia
[]> 9
File types belonging to the group "Microsoft Documents":
1. Access.Extension.14(mda)
2. Access.MDBFile(mdb)
3. Access.MDEFile.14(mde)
4. Access.Shortcut.DataAccessPage.1(maw)
5. Access.Shortcut.Form.1(maf)
6. ....
Choose the operation you want to perform:

```

```
- PRINT - Print the file types for File Analysis
- ADD - Add the file type(s) for File Analysis
[]> add
Choose the file type(s) to be added for File Analysis from the list
File types that are not selected for File Analysis from group "Microsoft Documents":
1. Access.Extension.14(mda)
2. Access.MDBFile(mdb)
3. Access.MDEFile.14(mde)
4. Access.Shortcut.DataAccessPage.1(maw)
5. Access.Shortcut.Form.1(maf)
6. ....
[]> 1-3, 5
Choose the operation you want to perform:
- PRINT - Print the file types for File Analysis
- DELETE - Delete the file type(s) for File Analysis
- ADD - Add the file type(s) for File Analysis
[]> print
File types belonging to the group:
1. Access.Extension.14(mda) [selected]
2. Access.MDBFile(mdb) [selected]
3. Access.MDEFile.14(mde) [selected]
4. Access.Shortcut.DataAccessPage.1(maw)
5. Access.Shortcut.Form.1(maf) [selected]
6. ....
Choose the operation you want to perform:
- PRINT - Print the file types for File Analysis
- DELETE - Delete the file type(s) for File Analysis
- ADD - Add the file type(s) for File Analysis
Specify AMP processing timeout (in seconds)
[120]>

Advanced-Malware protection is now enabled on the system.

Please note: you must issue the 'policyconfig' command (CLI) or Mail Policies (GUI) to
configure advanced malware
scanning behavior for default and custom Incoming Mail Policies.
This is recommended for your DEFAULT policy. File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File
Analysis reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]>
```

パブリック クラウドのファイル分析サーバを使用するための E メール セキュリティ アプライアンスの設定

```
mail.example.com> ampcnfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
```

(パブリック クラウド ファイル分析サービスのみの) アプライアンス グループの設定

```
[ ]> advanced
Enter cloud query timeout?
[15]>
Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>
Enter cloud domain?
[cloud-domain.com]>
Do you want use the recommended analysis threshold from cloud service? [Y]>
Enter analysis threshold?
[50]>
Enter heartbeat interval?
[15]>
Do you want to enable SSL communication (port 443) for file reputation? [N]>
Do you want to suppress the verdict update alerts for all messages that are
not delivered to the recipient? [N]>
Choose a file analysis server:
1. AMERICAS (https://americas-fa.com)
2. Private Cloud
[1]>
...
```

(パブリック クラウド ファイル分析サービスのみの) アプライアンス グループの設定

組織内のアプライアンスから分析用に送信されたファイルに関するクラウド内の詳細な分析結果を、組織のすべてのコンテンツ セキュリティ アプライアンスで表示するには、すべてのアプライアンスを同じアプライアンス グループに結合する必要があります。

詳細については、ユーザ ガイドの「File Reputation Filtering and File Analysis」を参照してください。

```
mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[ ]> setgroup
Does your organization have multiple Cisco Email, Web, and/or Content Security Management
appliances? [N]> Y
Do you want this appliance to display detailed analysis reports for files uploaded to
the cloud from other appliances in your organization,
and vice-versa?
[Y]> Enter an Analysis Group name. This name is case-sensitive and must be configured
identically on each appliance in the Analysis Group.
[ ]> FA_Reporting
Registration is successful with the group name. This does not require commit
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: FA_Reporting
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
```

```
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- VIEWGROUP - view the group members details.
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```



(注) アプライアンスグループの設定後は、**setgroup** サブコマンドを使用できません。グループを何らかの理由で変更する必要がある場合は、Cisco TAC でケースを開く必要があります。アプライアンスグループの詳細は、**viewgroup** サブコマンドを使用して表示できます。

オンプレミスのファイル分析サーバを使用するためのEメールセキュリティアプライアンスの設定

```
mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced
Enter cloud query timeout?
[15]>
Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.sourcefire.com)
2. Private reputation cloud
[1]>
Enter cloud domain?
[a.immunet.com]>
Do you want use the recommended analysis threshold from cloud service? [Y]>
Enter analysis threshold?
[50]>
Enter heartbeat interval?
[15]>
Do you want to enable SSL communication (port 443) for file reputation? [N]>
Do you want to suppress the verdict update alerts for all messages that are
not delivered to the recipient? [N]>
Choose a file analysis server:
1. AMERICAS (https://panacea.threatgrid.com)
2. Private Cloud
[1]> 2
Enter file analysis server url?
[]> https://mycloud.example.com
Certificate Authority:
1. Use Cisco Trusted Root Certificate List
2. Paste certificate to CLI
[1]>
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
```

```
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```

オンプレミスのファイルレピュテーションサーバを使用するためのEメールセキュリティアプライアンスの設定

```
mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File
Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> advanced
Enter cloud query timeout?
[15]>
Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.domain.com)
2. Private reputation cloud
[1]> 2
Enter AMP reputation server hostname or IP address?
[]> myamp.domain.com
Paste the public key followed by a . on a new line
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKuk01De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0
FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZKjeGcjDOL5UlsuusFncCzWBQ7RKNUSesmQRMSGkVb1/
3j+skZ6UtW+5u09lHNSj6tQ51s1SPrcBkedbNf0Tp0GbMJdyR4e9T04ZZwIDAQAB
-----END PUBLIC KEY-----
.
Enter cloud domain?
[immunet.com]>
Do you want use the recommended analysis threshold from cloud service? [Y]>
Enter heartbeat interval?
[15]>
Do you want to enable SSL communication (port 443) for file reputation? [N]>
Choose a file analysis server:
1. AMERICAS (https://threatgrid.com)
2. Private analysis cloud
[1]>
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File
Analysis reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```


ローカル ファイルのレピュテーション キャッシュのクリア

```
mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]> clearcache
Do you want to clear File Reputation Cache? [N]> y
Cache cleared successfully.
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CLEARCACHE - Clears the local File Reputation cache.
[]>
```

ファイル レピュテーション判定結果値のキャッシュ有効期間の設定

次の例では、modifytimeout サブ コマンドを使用して、悪意のあるファイルのキャッシュ有効期間を設定します。



(注) キャッシュ有効期間は 15 分から 7 日の間に設定してください。

```
mail.example.com> ampconfig
File Reputation: Enabled
File Analysis: Enabled
File types selected for File Analysis:
    Microsoft Windows / DOS Executable
Appliance Group ID/Name: Not part of any group yet
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> cachesettings
Choose the operation you want to perform:
- MODIFYTIMEOUT - Configure the cache expiry period based on File Reputation disposition.
- CLEARCACHE - Clears the local File Reputation cache.
[]> modifytimeout
Choose the operation you want to perform:
- CLEAN - Configure the cache expiry period for clean files.
- MALICIOUS - Configure the cache expiry period for malicious files.
- UNKNOWN - Configure the cache expiry period for unknown files.
[]> malicious
```

```
Specify the cache expiry period for this file disposition (use 'd' for days, 'h' for
hours, or 'm' for minutes). If you
specify a value without a unit, it is always treated as days.
[1d]> 5d
```

ファイルレトロスペクティブアラートの抑制

```
mail.example.com> ampconfig

File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet

Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis
  reporting details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> advanced

Enter cloud query timeout?
[15]>

Choose a file reputation server:
1. AMERICAS (cloud-sa.amp.domain.com)
2. Private reputation cloud
[1]>

Do you want use the recommended reputation threshold from cloud service? [Y]>

Enter heartbeat interval?
[15]>

Do you want to enable SSL communication (port 443) for file reputation? [N]>

Do you want to suppress the file retrospective verdict alerts for the messages that are
  not delivered to the recipient
[N]> yes
```

ampstatus

説明

さまざまな Advanced Malware Protection（ファイルレピュテーションおよび分析）コンポーネントのバージョンを表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail.example.com> ampstatus
Component                               Version    Last Updated
AMP Client Settings                     1.0       Never updated
AMP Client Engine                       1.0       Never updated
```

スパム対策

ここでは、次のコマンドについて説明します。

- [antispamconfig](#) (11 ページ)
- [antispamstatus](#) (12 ページ)
- [antispamupdate](#) (13 ページ)
- [incomingrelayconfig](#) (13 ページ)

antispamconfig

説明

Anti-Spam ポリシーを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次に、Anti-Spam 機能の設定例を示します。

```
mail3.example.com> antispamconfig
Choose the operation you want to perform:
- IRONPORT - Configure IronPort Anti-Spam.
- CLOUDMARK - Configure Cloudmark Service Provider Edition.
- MULTISCAN - Configure IronPort Intelligent Multi-Scan.
[]> ironport
IronPort Anti-Spam scanning: Disabled
Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[]> setup
IronPort Anti-Spam scanning: Disabled
Would you like to use IronPort Anti-Spam scanning? [Y]> Y
The IronPort Anti-Spam License Agreement is displayed (if you have not already accepted it).
Do you accept the above IronPort Anti-Spam license agreement? []> Y
Increasing the following size settings may result in decreased performance. Please consult
```

```
documentation for size
recommendations based on your environment.
Never scan message larger than: (Add a trailing K for kilobytes, M for megabytes, or no
letters for bytes.)
[1M]>
Always scan message smaller than: (Add a trailing K for kilobytes, M for megabytes, or
no letters for bytes.)
[512K]>
Please specify the IronPort Anti-Spam scanning timeout (in seconds)
[60]>
Would you like to enable regional scanning? [N]>
IronPort Anti-Spam scanning is now enabled on the system. Please note: you must issue
the 'policyconfig' command (CLI)
or Mail Policies (GUI) to configure
Cisco IronPort scanning behavior for default and custom Incoming and Outgoing Mail
Policies. This is recommended for your DEFAULT policy.
IronPort Anti-Spam scanning: Enabled
Choose the operation you want to perform:
- SETUP - Edit IronPort Anti-Spam settings.
[]>
```

antisipamstatus

説明

Anti-Spam ステータスを表示します。

使用方法

確定 : このコマンドに「commit」は必要ありません。

クラスタ管理 : このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> antisipamstatus
Choose the operation you want to perform:
- IRONPORT - Display IronPort Anti-Spam version and rule information.
- CLOUDMARK - Display Cloudmark Service Provider Edition version and rule information.
- MULTISCAN - Display Intelligent Multi-Scan version and rule information.
[]> ironport
Component                Last Update                Version
CASE Core Files           Never updated              3.4.0-013
CASE Utilities            Never updated              3.4.0-013
Structural Rules          Never updated 3.3.1-009-20141210_214201
Web Reputation DB         Never updated              20141211_111021
Web Reputation Rules      Never updated 20141211_111021-20141211_170330
Content Rules             Never updated              unavailable
Content Rules Update      Never updated              unavailable
Last download attempt made on: Never
```

antispamupdate

説明

Anti-Spamルールおよび関連するCASEコンポーネントの即時更新を手動で要求します。Intelligent Multi-Scan (IMS) が使用する Anti-Spam ルールおよび CASE コンポーネントも対象となります。ただし、IMS が使用するサードパーティ製アンチスパム エンジン対象外です。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログイン ホスト（ユーザがログインしたマシン）でのみ使用できます。

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せん。

例

```
mail3.example.com> antispamupdate
Choose the operation you want to perform:
- MULTISCAN - Request updates for Intelligent Multi-Scan
- IRONPORT - Request updates for IronPort Anti-Spam
- CLOUDMARK - Request updates for Cloudmark Anti-Spam
[]> ironport
Requesting check for new CASE definitions
```

incomingrelayconfig

説明

incomingrelayconfig コマンドは、着信リレー機能をイネーブルにして設定するために使用します。次の例では、まず着信リレー機能をイネーブルにし、2つのリレーを追加してから、一方を変更し、もう一方を削除しています。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例：着信リレーのイネーブル化と設定

```
mail3.example.com> incomingrelayconfig
Incoming relays: Disabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
```

```

- RELAYLIST - Configure incoming relays.
[> setup
This command helps your Cisco IronPort appliance determine the sender's
originating IP address.
You should ONLY enable this command if your Cisco IronPort appliance is NOT
directly connected to the Internet as the "first hop" in your email
infrastructure.
You should configure this feature if other MTAs or servers are configured at
your network's perimeter to relay mail to your Cisco IronPort appliance.
Do you want to enable and define incoming relays? [N]> y
Incoming relays: Enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
- RELAYLIST - Configure incoming relays.
[> relaylist
There are no relays defined.
Choose the operation you want to perform:
- NEW - Create a new entry
[> new
Enter a name for this incoming relay (Ex: "first-hop")
[> first-hop
Enter the IP address of the incoming relay. IPv4 and IPv6 addresses are supported.
For IPv4, CIDR format subnets such as 10.1.1.0/24, IP address ranges such as 10.1.1.10-20,
and subnets such as 10.2.3. are allowed.
For IPv6, CIDR format subnets such as 2001:db8::/32 and IP address ranges such as
2001:db8::1-2001:db8::11 are allowed.
Hostnames such as crm.example.com and partial hostnames such as .example.com are allowed.
[> 192.168.1.1
Do you want to use the "Received:" header or a custom header to determine the originating
IP address?
1. Use "Received:" header
2. Use a custom header
[1]> 1
Within the "Received:" header, enter the special character or string after which to begin
parsing for the originating IP address:
[from]> [
Within the headers, enter the position of the "Received:" header that contains the
originating IP address:
[1]> 1
There is 1 relay defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[> print
Incoming
relay name:      IP address:      Header      Match
-----
first-hop      192.168.1.1      Received    [      1
There is 1 relay defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[> new
Enter a name for this incoming relay (Ex: "first-hop")
[> second-hop
Enter the IP address of the incoming relay. IPv4 and IPv6 addresses are supported.
For IPv4, CIDR format subnets such as 10.1.1.0/24, IP address ranges such as 10.1.1.10-20,
and subnets such as 10.2.3. are allowed.
For IPv6, CIDR format subnets such as 2001:db8::/32 and IP address ranges such as
2001:db8::1-2001:db8::11 are allowed.

```

```
Hostnames such as crm.example.com and partial hostnames such as .example.com are allowed.
[]> 192.168.1.2
Do you want to use the "Received:" header or a custom header to determine the originating
IP address?
1. Use "Received:" header
2. Use a custom header
[1]> 2
Enter the custom header name that contains the originating IP address:
[]> x-Connecting-IP
There are 2 relays defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]> print
Incoming
relay name:      IP address:      Header      Match      Hops:
-----
first-hop        192.168.1.1      Received    [          1
second-hop        192.168.1.2      x-Connecting-IP n/a        n/a
There are 2 relays defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]> delete
1. first-hop:      192.168.1.1
2. second-hop:      192.168.1.2
Enter the number of the entry you wish to delete:
[1]> 1
Incoming relay "first-hop" deleted.
There is 1 relay defined.
Choose the operation you want to perform:
- NEW - Create a new entry
- EDIT - Modify an entry
- DELETE - Remove an entry
- PRINT - Display the table
[]>
```

sblconfig

説明

エンドユーザのセーフリスト/ブロック リストを設定します。



(注) セーフリスト/ブロック リストを GUI を使用してアプライアンスでイネーブルにし、このコマンドを実行する必要があります。

使用方法

確定：このコマンドに「commit」は必要ありません。

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。

バッチ形式 - インポート

バッチ形式

エンドユーザのセーフリスト/ブロック リストすべてのエントリを、指定のファイルの現在のエントリと置き換えます。

```
slblconfig import <filename> <ignore invalid entries>
```

- **filename** : インポートする必要があるファイルの名前。ファイルは、アプライアンスの /configuration ディレクトリに格納する必要があります。
- **ignore invalid entries** : 無効なエントリを無視するかどうかを指定します。「はい (Yes)」または「いいえ (No)」。

バッチ形式 - エクスポート

エンドユーザのセーフリスト/ブロックリストすべてのエントリをアプライアンスのファイルにエクスポートします。

```
slblconfig export
```

アプライアンスは、次の命名規則を使用して /configuration ディレクトリに CSV ファイルを保存します。

slbl<timestamp><serial number>.csv.

例：セーフリスト/ブロック リスト エントリのインポート

```
mail.example.com>
slblconfig
End-User Safelist/Blocklist: Enabled
Choose the operation you want to perform:
- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.
[ ]>
import
Currently available End-User Safelist/Blocklist files:
1. slbl.csv
Choose the file to import from.
[1]>
1
Do you want to ignore invalid entries? [Y]>
Y
End-User Safelist/Blocklist import has been initiated...
Please wait while this operation executes.
End-User Safelist/Blocklist successfully imported.
Choose the operation you want to perform:
- IMPORT - Replace all entries in the End-User Safelist/Blocklist.
- EXPORT - Export all entries from the End-User Safelist/Blocklist.
[ ]>
```


グレイメールの検出と安全な購読解約

タスク	コマンド
グレイメールの検出と安全な配信停止のグローバル設定	graymailconfig (17 ページ)
グレイメールの検出と安全な配信停止の着信メール ポリシーの設定	policyconfig (190 ページ)
既存のグレイメール ルールの詳細の表示	graymailstatus (18 ページ)
手動でグレイメール ルールの更新の要求	graymailupdate (18 ページ)

graymailconfig

説明

グレイメール検出と安全な配信停止のグローバル設定を設定します。



(注) グレイメール検出と安全な配信停止を有効にするには、アンチスパム スキャンをグローバルに有効にする必要があります。これは、IronPort Anti-Spam または Intelligent Multi-Scan 機能のいずれかになります。

グレイメール検出と安全な配信停止のポリシー設定を設定するには、`policyconfig` コマンドを使用します。詳細については、一括 E メールまたはソーシャル ネットワークの E メールであると識別されたメッセージをドロップする着信ポリシーの作成 (209 ページ) を参照してください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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 graymailconfig` 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

```
Graymail Detection: Disabled

Choose the operation you want to perform:
- SETUP - Configure Graymail.
[> setup
```

```

Would you like to use Graymail Detection? [Y]>

Increasing the following size settings may result in decreased performance.
Please consult documentation for size recommendations based on your
environment.

Maximum Message Size to Scan (Add a trailing K for kilobytes, M for megabytes,
or no letters for bytes.):
[1M]>

Timeout for Scanning Single Message(in seconds):
[60]>

Would you like to enable automatic updates for Graymail engine? [Y]> Y

Graymail Safe Unsubscribe: Disabled

Would you like to use Graymail Safe Unsubscribe? [Y]>

Graymail Detection and Safe Unsubscribe is now enabled. Please note: The global
settings are recommended only for your DEFAULT mail policy. To configure policy
settings, use the incoming or outgoing policy page on web interface or the
'policyconfig' command in CLI.

```

graymailstatus

説明

既存のグレイメール ルールの詳細を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```

mail.example.com> graymailstatus
Component      Version      Last Updated
Graymail Engine 01.378.53    Never Updated
Graymail Rules  01.378.53#15 Never updated
Graymail Tools  1.0.03       Never updated

```

graymailupdate

説明

手動でグレイメール ルールの更新を要求します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> graymailupdate
```

新しいグレイメール更新の検査を要求します。

アンチウイルス

ここでは、次の CLI コマンドについて説明します。

- [antivirusconfig](#) (19 ページ)
- [antivirusstatus](#) (21 ページ)
- [antivirusupdate](#) (22 ページ)

antivirusconfig

説明

Anti-Virus ポリシーを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例では、antivirusconfig コマンドを使用して、システム上で Sophos ウイルス スキャンをイネーブルにし、タイムアウト値を60秒に設定しています。アップデートサーバ、アップデート間隔、およびオプションのプロキシ サーバを設定する方法については、[updateconfig](#) (113 ページ) を参照してください。



- (注) `systemsetup` コマンドの実行時にライセンス契約に同意しなかった場合、`antivirusconfig` コマンドを初めて実行するときにライセンス契約書が表示されます。ライセンス契約に同意しなければ、Sophos ウィルス スキャン エンジン はアプライアンスでイネーブルになりません。

```
mail3.example.com> antivirusconfig

Choose the operation you want to perform:
- SOPHOS - Configure Sophos Anti-Virus.
- MCAFEE - Configure McAfee Anti-Virus.
[]> sophos

Sophos Anti-Virus: Disabled

Choose the operation you want to perform:

- SETUP - Configure Sophos Anti-Virus.

[]> setup

Sophos Anti-Virus scanning: Disabled

Would you like to use Sophos Anti-Virus scanning? [Y]> y

(First time users see the license agreement displayed here.)

Please specify the Anti-Virus scanning timeout (in seconds)
[60]> 60

Would you like to enable automatic updates for Sophos engine? [Y] > Y

Sophos Anti-Virus scanning is now enabled on the system.

Please note: you must issue the 'policyconfig' command (CLI) or Mail
Policies (GUI) to configure Sophos Anti-Virus scanning behavior for default and custom
Incoming and Outgoing Mail Policies.
This is recommended for your DEFAULT policy.

Sophos Anti-Virus: Enabled
Choose the operation you want to perform:

- SETUP - Configure Sophos Anti-Virus.
[]>
```

Anti-Virus IDE の詳細の表示

AsyncOS では、アプライアンスがダウンロードしたアンチウイルス シグニチャ (IDE ファイル) の詳細なステータスを確認できます。この詳細を表示するには、**`antivirusconfig -> detail`** サブコマンドを使用します。次に例を示します。

```
mail3.example.com> antivirusconfig

Choose the operation you want to perform:
- SOPHOS - Configure Sophos Anti-Virus.
- MCAFEE - Configure McAfee Anti-Virus.
[]> sophos

Sophos Anti-Virus: Enabled
Choose the operation you want to perform:
```

```
- SETUP - Configure Sophos Anti-Virus.
- STATUS - View Sophos Anti-Virus status.
- DETAIL - View Sophos Anti-Virus detail.
[> detail
Sophos Anti-Virus:
Product - 3.87
Engine - 2.25.0
Product Date - 01 Nov 2004
Sophos IDEs currently on the system:
'Mkar-E.Ide'          Virus Sig. - 23 Dec 2004 01:24:02
'Rbot-Sd.Ide'         Virus Sig. - 22 Dec 2004 19:10:06
'Santy-A.Ide'         Virus Sig. - 22 Dec 2004 06:16:32
'Bacbanan.Ide'        Virus Sig. - 21 Dec 2004 18:33:58
'Rbot-Sb.Ide'         Virus Sig. - 21 Dec 2004 14:50:46
'Rbotry.Ide'          Virus Sig. - 21 Dec 2004 06:13:40
'Sdbot-Si.Ide'        Virus Sig. - 20 Dec 2004 20:52:04
'Odbbob-A.Ide'        Virus Sig. - 19 Dec 2004 23:34:06
'Rbot-Rw.Ide'         Virus Sig. - 19 Dec 2004 00:50:34
'Worltd.Ide'          Virus Sig. - 18 Dec 2004 07:02:44
'Delf-Jb.Ide'         Virus Sig. - 17 Dec 2004 22:32:08
[...command continues...]
```

antivirusstatus

説明

Anti-Virus ステータスを表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> antivirusstatus
Choose the operation you want to perform:
- MCAFEE - Display McAfee Anti-Virus version information
- SOPHOS - Display Sophos Anti-Virus version information
[> sophos
SAV Engine Version      3.85
IDE Serial              2004101801
Engine Update           Mon Sep 27 14:21:25 2004
Last IDE Update         Mon Oct 18 02:56:48 2004
Last Update Attempt     Mon Oct 18 11:11:44 2004
Last Update Success     Mon Oct 18 02:56:47 2004
```

antivirusupdate

説明

ウイルス定義を手動で更新します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログイン ホスト（ユーザがログインしたマシン）でのみ使用できます。

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せん。

例

```
mail3.example.com> antivirusupdate
Choose the operation you want to perform:
- MCAFEE - Request updates for McAfee Anti-Virus
- SOPHOS - Request updates for Sophos Anti-Virus
[]> sophos
Requesting update of virus definitions
mail3.example.com>
```

コマンド ラインの管理

ここでは、次の CLI コマンドについて説明します。

- [commit](#) (22 ページ)
- [commitdetail](#) (23 ページ)
- [clearchanges](#) または [clear](#) (23 ページ)
- [help](#) または [h](#) または [?](#) (24 ページ)
- [rollbackconfig](#) (24 ページ)
- [quit](#) または [q](#) または [exit](#) (25 ページ)

commit

説明

変更を確定します。commit コマンドの後のコメントの入力は任意です。

使用方法

確定：該当なし

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Changed "psinet" IP Interface to a different IP ad dress
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

commitdetail

説明

最後の確定に関する詳細情報を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> commitdetail
Commit at Mon Apr 18 13:46:28 2005 PDT with comments: "Enabled loopback".
mail3.example.com>
```

clearchanges または clear

説明

clear コマンドは、commit または clear コマンドが最後に実行された以降に設定に対して行われた変更をすべてクリアします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> clear
Are you sure you want to clear all changes since the last commit? [Y]> y
Changes cleared: Mon Jan 01 12:00:01 2003
mail3.example.com>
```

help または h または ?

説明

help コマンドを実行すると、使用可能なすべての CLI コマンドが表示され、各コマンドの簡単な説明を参照できます。**help** コマンドは、コマンドプロンプトで **help** と入力するか、疑問符 (?) を 1 つ入力して実行できます。

使用方法

確定：このコマンドに「**commit**」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> help
Displays the list of all available commands.
```

rollbackconfig

rollbackconfig コマンドを使用すると、直前に確定した 10 の設定のうち 1 つをロールバックできます。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail.example.com> rollbackconfig
Previous Commits:
  Committed On      User      Description
-----
1. Fri May 23 06:53:43 2014  admin    new user
2. Fri May 23 06:50:57 2014  admin    rollback
```



```
3. Fri May 23 05:47:26 2014      admin
4. Fri May 23 05:45:51 2014      admin      edit user
Enter the number of the config to revert to.
[]> 2
Are you sure you want to roll back the configuration? [N]> y
Reverted to Fri May 23 06:50:57 2014      admin      rollback
Do you want to commit this configuration now? [N]> y
Committed the changes successfully
```

quit または q または exit

説明

quit コマンドを実行すると、CLI アプリケーションからログアウトします。確定されていない設定変更はクリアされます。**quit** コマンドは電子メール操作には影響しません。ログアウトはログ ファイルに記録されます（**exit** の入力、**quit** の入力と同じです）。

使用方法

確定：このコマンドに「**commit**」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> quit
Configuration changes entered but not committed.  Exiting will lose changes.
Type 'commit' at the command prompt to commit changes.
Are you sure you wish to exit?  [N]> y
```

コンフィギュレーション ファイルの管理

ここでは、次の CLI コマンドについて説明します。

- [loadconfig](#) (25 ページ)
- [mailconfig](#) (27 ページ)
- [resetconfig](#) (27 ページ)
- [saveconfig](#) (29 ページ)
- [showconfig](#) (29 ページ)

loadconfig

説明

コンフィギュレーション ファイルをロードします。



- (注) クラスタ化されたマシンへの設定のロードは GUI を使用する場合にのみサポートされます。手順については、『*User Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

この例では、新しいコンフィギュレーション ファイルをローカルな場所からインポートします。

```
mail3.example.com> loadconfig
1. Paste via CLI
2. Load from file
[1]> 2
Enter the name of the file to import:
[]> changed.config.xml
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> commit
Please enter some comments describing your changes:
[]> loaded new configuration file
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

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。最後に、変更を確定します。

```
mail3.example.com> loadconfig
1. Paste via CLI
2. Load from file
[1]> 1
Paste the configuration file now.
Press CTRL-D on a blank line when done.
[The configuration file is pasted until the end tag
</config>
. Control-D is entered on a separate line.]
Values have been loaded.
Be sure to run "commit" to make these settings active.
mail3.example.com> systemsetup
[The system setup wizard is run.]
mail3.example.com> commit
Please enter some comments describing your changes:
[]> pasted new configuration file and changed default settings via
```

systemsetup

```
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

mailconfig

説明

設定をテストする際は、**mailconfig** コマンドを使用して、**systemsetup** コマンドで作成したばかりのシステム設定データを含むテスト電子メールをただちに送信できます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> mailconfig
Please enter the email address to which you want to send the configuration file.
Separate multiple addresses with commas.
[ ]> user@example.com
Choose the passphrase option:
1. Mask passphrases (Files with masked passphrases cannot be loaded using loadconfig
command)
2. Encrypt passphrases
3. Plain passphrases
[1]> 2
The configuration file has been sent to user@example.com.
```

利用可能なメールボックスに設定を送信して、システムでネットワーク上に電子メールを送信できることを確認します。



(注)

セキュリティを強化するために、アプライアンスの機密データの暗号化を **fipsconfig** コマンドでイネーブルにしている場合、Plain passwords オプションは使用できません。

resetconfig

説明

アプライアンスを物理的に移動する際、出荷時の初期状態で始めなければならない場合があります。**resetconfig** コマンドは、すべての設定値を出荷時の初期状態にリセットします。このコマンドを実行すると元に戻せないため、ユニットを移動する場合や、設定の問題を解決する最

後の手段としてのみ使用してください。**resetconfig** コマンドの実行後に CLI に再接続してから **systemsetup** コマンドを実行することを推奨します。



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



危険 **resetconfig** コマンドを実行すると、すべてのネットワーク設定が出荷時デフォルト値に戻ります。場合によっては、CLI から切断され、アプライアンスに接続するために使用したサービス（FTP、Telnet、SSH、HTTP、HTTPS）がディセーブルにされ、**userconfig** コマンドで作成した追加のユーザ アカウントが削除されます。このコマンドは、シリアル インターフェイスを使用するか、またはデフォルトの Admin ユーザ アカウントから管理ポート上のデフォルト設定を使用して CLI に再接続できない場合は使用しないでください。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカル ファイル システムにアクセスする必要があります。

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せん。

例

```
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.
```

saveconfig

説明

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



- (注) クラスタ化した環境の場合、このコマンドは、完全なクラスタ設定を保存します。クラスタ化したマシンでこのコマンドを実行するには、コンフィギュレーションモードをクラスタに変更します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例では、コンフィギュレーション ファイルのパスフレーズは暗号化され、configuration ディレクトリに保存されます。

```
mail.example.com> saveconfig
Choose the passphrase option:
1. Mask passphrases (Files with masked passphrases cannot be loaded using loadconfig command)
2. Encrypt passphrases

[1]> 2
File written on machine "mail.example.com" to the location
"/configuration/C100V-4232116C4E14C70C4C7F-7898DA3BD955-20140319T050635.xml".
Configuration saved.
```



- (注) セキュリティを強化するために、アプライアンスの機密データの暗号化を fipsconfig コマンドでイネーブルにしている場合、Plain passwords オプションは使用できません。

showconfig

説明

showconfig コマンドは、現在の設定を画面に出力します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例では、設定が CLI に表示され、設定のパスフレーズは暗号化されています。

```
mail.example.com> showconfig
Choose the passphrase display option:
1. Mask passphrases (Files with masked passphrases cannot be loaded using loadconfig
command)
2. Encrypt passphrases
3. Plain passphrases
[1]> 2
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE config SYSTEM "config.dtd">
<!--
  Product: Cisco C100V Email Security Virtual Appliance
  Model Number: C100V
  Version: 9.0.0-038
  Serial Number: 4232116C4E14C70C4C7F-7898DA3BD955
  Number of CPUs: 2
  Memory (MB): 6144
  Current Time: Wed Mar 19 05:30:05 2014
-->
<config>
<!--
*****
*                               Network Configuration                               *
*****
-->[The remainder of the configuration file is printed to the screen.]
```



(注) セキュリティを強化するために、アプライアンスの機密データの暗号化を `fipsconfig` コマンドでイネーブルにしている場合、Plain passwords オプションは使用できません。

クラスタの管理

ここでは、次の CLI コマンドについて説明します。

- [clusterconfig](#) (31 ページ)

clusterconfig

説明

clusterconfig コマンドは、クラスタ関連の設定を指定するために使用します。クラスタに属していないマシンで **clusterconfig** を実行した場合は、既存のクラスタに参加するか、新しいクラスタを作成するかを選択できます。

clusterconfig コマンドには、次のサブコマンドが用意されています。

非クラスタ コマンド

次のコマンドは、クラスタに属していない場合に使用できます。

- **clusterconfig new <name>** : 指定された名前で新しいクラスタを作成します。このマシンは、このクラスタおよび「Main Group」と呼ばれるデフォルトのクラスタグループのメンバになります。

<name> : 新しいクラスタの名前。

- **clusterconfig join [--port=xx] <ip_of_remote_cluster> [<admin_password>]<groupname>** : このマシンをクラスタに追加します。

引数の説明

<ip_of_remote_cluster> : クラスタ内の別のマシンの IP アドレス。

<admin_password> : クラスタの admin パスワード。CCS を使用してクラスタに参加する場合、

このパラメータを指定する必要はありません。

<groupname> : 参加するグループの名前。

<port> : 接続するリモート マシンのポート（デフォルトは 22）。

- **clusterconfig prepjoin print**

このマシンを CCS ポート経由でクラスタに参加させるための準備に必要な情報を表示します。

クラスタ コマンド

次のコマンドは、クラスタに属している場合に使用できます。

- **clusterconfig addgroup <groupname>** : 新しいクラスタ グループを作成します。グループはメンバが含まれていない空の状態で作成されます。
- **clusterconfig renamegroup <old_groupname> <new_groupname>** : クラスタ グループの名前を変更します。
- **clusterconfig deletigroup <groupname> [new_groupname]** : クラスタ グループを削除します。
 <groupname> : 削除するクラスタ グループの名前。
 <new_groupname> : 元のグループのマシンを追加するクラスタ グループ。

- `clusterconfig setgroup <machinename> <groupname>`：マシンが属するグループを設定（または変更）します。
`<machinename>`：設定するマシンの名前。
`<groupname>`：マシンを設定するグループ。
- `clusterconfig removemachine <machinename>`：クラスタからマシンを削除します。
- `clusterconfig setname <name>`：クラスタの名前を指定された名前に変更します。
- `clusterconfig list`：現在クラスタに属しているすべてのマシンを表示します。
- `clusterconfig connstatus`：現在クラスタに属しているすべてのマシンを表示し、切断されたマシンのルーティングの詳細を追加します。
- `clusterconfig disconnect <machinename>`：マシンを一時的にクラスタから切断します。
`<machinename>`：切断するマシンの名前。
- `clusterconfig reconnect <machinename>`：「disconnect」コマンドによって切断されていたマシンとの接続を復元します。
- `clusterconfig prepjoin new <serial_number> <hostname> <user_key>`：CCS ポート経由でクラスタに参加する新しいホストを追加します。
`<serial_number>`：追加するマシンのシリアル番号。
`<hostname>`：追加するマシンのホスト名。
`<user_key>`：参加マシンから「prepjoin print」コマンドによって取得された SSH ユーザキー。
- `clusterconfig prepjoin delete <serial_number|hostname>`：追加対象として指定されていたホストを「prepjoin new」コマンドから削除します。このパラメータが必要となるのは、後でホストを追加しないことにした場合だけです。ホストが正常にクラスタに追加されると、そのホストの prepjoin 情報が自動的に削除されます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはクラスタ モードでのみ使用できます。

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せん。

例

clusterconfig コマンドとその使用方法の説明については、『*User Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

データ損失の防止

ここでは、次の CLI コマンドについて説明します。

- [dlpstatus](#) (33 ページ)
- [dlpupdate](#) (33 ページ)

dlpstatus

DLP エンジンの要求バージョン情報。



- (注) **dlpstatus** コマンドを使用する前に、GUI の DLP Global Settings ページで DLP を設定しておく必要があります。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、クラスタ、グループ、またはマシンの各モードで使用できます。

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せん。

例

```
mail.example.com> dlpstatus
```

Component	Version	Last Updated
DLP Engine	3.0.2.31	Never updated

dlpupdate

説明

DLP エンジンを更新します。



- (注) **dlpupdate** コマンドを使用する前に、GUI の DLP Global Settings ページで DLP を設定しておく必要があります。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、クラスタ、グループ、またはマシンの各モードで使用できます。

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。

バッチ形式

変更が検出されない場合でも `dlpupdate` コマンドのバッチ形式が DLP エンジンを強制的に更新します。

```
dlpupdate [force]
```

例

```
mail.example.com> dlpupdate
```

```
Checking for available updates. This may take a few seconds..
```

```
Could not check for available updates. Please check your Network and Service Updates settings and retry.
```

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

```
- SETUP - Enable or disable automatic updates for DLP Engine.
```

```
[ ]> setup
```

```
Automatic updates for DLP are disabled
```

```
Do you wish to enable automatic updates for DLP Engine? [N]> y
```

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

```
- SETUP - Enable or disable automatic updates for DLP Engine.
```

```
[ ]>
```

S/MIME セキュリティ サービス

smimeconfig

説明

送信プロファイル、公開キーの設定など、S/MIME の設定を設定します。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

- 署名と暗号化のための送信プロファイルの作成 (35 ページ)
- 暗号化の公開キーの追加 (36 ページ)

署名と暗号化のための送信プロファイルの作成

次の例では、S/MIME を使用する署名および暗号化メッセージの送信プロファイルを作成方法を示しています。

```
mail.example.com> smimeconfig
Choose the operation you want to perform:
- GATEWAY - Manage S/MIME gateway configuration.
[]> gateway
Choose the operation you want to perform:
- VERIFICATION - Manage S/MIME Public Keys.
- SENDING - Manage S/MIME gateway sending profiles.
[]> sending
Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[]> new
Enter a name for this profile:
> hr_sign_and_encrypt
1. Encrypt
2. Sign
3. Sign/Encrypt
4. Triple
Enter S/MIME mode:
[2]> 3
1. smime_signing
Select S/MIME certificate to sign:
[1]>
1. Detached
2. Opaque
Enter S/MIME sign mode:
[1]>
1. Bounce
2. Drop
3. Split
Enter S/MIME action:
[1]> 3
Choose the operation you want to perform:
- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[]> print
S/MIME Sending Profiles
Name          Certificate      S/MIME Mode    Sign Mode    Action
-----
hr_sign_a     smime_signing    Sign/Encrypt    Detached     Split
Choose the operation you want to perform:
```

```

- NEW - Create a new S/MIME sending profile.
- EDIT - Edit a S/MIME sending profile.
- RENAME - Rename a S/MIME sending profile.
- DELETE - Delete a S/MIME sending profile.
- IMPORT - Import a S/MIME sending profile from a file
- EXPORT - Export a S/MIME sending profile to a file
- PRINT - Display S/MIME sending profiles.
[]>

```

暗号化の公開キーの追加

次に、メッセージの暗号化のために、アプライアンスに受信者の S/MIME 証明書の公開キーを追加する例を示します。

```

mail.example.com> smimeconfig
Choose the operation you want to perform:
- GATEWAY - Manage S/MIME gateway configuration.
[]> gateway
Choose the operation you want to perform:
- VERIFICATION - Manage S/MIME Public Keys.
- SENDING - Manage S/MIME gateway sending profiles.
[]> verification
Choose the operation you want to perform:
- NEW - Create a new S/MIME Public Key.
- IMPORT - Import the list of S/MIME Public Keys from a file.
[]> new
Enter a name for this profile:
> hr_signing
1. Import
2. Paste
Choose one of the options for the certificate introducing:
[2]>
Paste public certificate in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDdDCCAlYgAwIBAgIBDTANBgkqhkiG9w0BAQUFADCBljELMAkGA1UEBhMCSU4x
CzAJBgNVBAG...
-----END CERTIFICATE-----
.
C=IN,ST=KA,L=BN,O=Cisco,OU=stg,CN=cert_for_enc,emailAddress=admin@example.com
Choose the operation you want to perform:
- NEW - Create a new S/MIME Public Key.
- EDIT - Edit a S/MIME Public Key.
- RENAME - Rename a S/MIME Public Key.
- DELETE - Delete a S/MIME Public Key.
- IMPORT - Import the list of S/MIME Public Keys from a file.
- EXPORT - Export the list of S/MIME Public Keys to a file.
- PRINT - Display S/MIME Public Keys.
[]> print
S/MIME Public Keys

```

Name	Emails	Domains	Remaining
hr_signin	admin@vm30bsd0008.ibqa	dns.vm30bsd0008.ibqa	145 days

ドメインキー

ここでは、次の CLI コマンドについて説明します。

- [domainkeysconfig \(37 ページ\)](#)

domainkeysconfig

説明

DomainKeys/DKIM のサポートを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。



(注) セキュリティ強化のため、FIPS モードでのアプライアンスの機密データの暗号化を有効にすると、秘密キーを表示できなくなります。秘密キーを編集する場合は、既存の秘密キーを入力するか、または新しい秘密キーを作成できます。

バッチ形式：署名プロファイル

domainkeysconfig コマンドのバッチ形式は、署名プロファイルの作成、編集、または削除で使用できます。

- DomainKeys/DKIM 署名プロファイルの追加

```
domainkeysconfig profiles signing new <name> <type> <domain> <selector> <user-list>
[options]
```

表 1: domainkeysconfig の新しい署名プロファイル引数

引数	説明
<name>	ドメイン プロファイルの名前。
<type>	ドメインのタイプ。dk または dkim です。
<domain>	ドメインプロファイルのドメインフィールド。これは、DomainKeys 署名の d タグを形成します。
<selector>	ドメインプロファイルのセレクタフィールド。これは、DomainKeys 署名の s タグを形成します。
<user-list>	ドメイン プロファイル ユーザのカンマ区切りリスト。ユーザは、特定のドメインプロファイルを使用して電子メールに署名する必要があるかどうかを判断するために、電子メールアドレスとの照合に使用されます。すべてのドメインユーザと一致させるには、特別なキーワード all を使用します。

引数	説明
[options]	
--key_name	署名に使用する秘密キーの名前。
--canon	DK で署名するときに使用する標準化アルゴリズム。現在サポートされているアルゴリズムは <code>simple</code> と <code>nofws</code> です。デフォルトは <code>nofws</code> です。
--body_canon	DKIMで署名するときに使用する、本文の標準化アルゴリズム。現在サポートされているアルゴリズムは <code>simple</code> と <code>relaxed</code> です。デフォルトは <code>simple</code> です。
--header_canon	DKIMで署名するときに使用する、ヘッダーの標準化アルゴリズム。現在サポートされているアルゴリズムは <code>simple</code> と <code>relaxed</code> です。デフォルトは <code>simple</code> です。
--body_length	署名の計算に使用する、標準化した本文のバイト数。DKIMプロファイルでのみ使用します。この値は、使用すると署名の1タグになります。デフォルトでは使用されません。
--headers_select	署名のヘッダーを選択する方法を指定します。DKIMプロファイルでのみ使用します。 <code>all</code> 、 <code>standard</code> 、 <code>standard_and_custom</code> のいずれかです。 <code>all</code> はすべての非反復ヘッダーに署名することを意味します。 <code>standard</code> は、 <code>Subject</code> 、 <code>From</code> 、 <code>To</code> 、 <code>Sender</code> 、 <code>MIME</code> などの既知のヘッダーの事前定義のセットに署名することを意味します。 <code>standard_and_custom</code> は、既知のヘッダーおよびユーザ定義のヘッダーのセットに署名することを意味します。デフォルトは <code>standard</code> です。
--custom_headers	署名するヘッダーのユーザ定義セット。 <code>headers_select</code> が <code>standard_and_custom</code> の場合に、DKIMプロファイルでのみ使用します。デフォルトは空のセットです。
--i_tag	署名に <code>i</code> タグを追加するかどうかを指定します。指定できる値は <code>yes</code> または <code>no</code> です。デフォルトは <code>yes</code> です。
--agent_identity	ユーザまたはユーザの代わりにこのメッセージに署名する代理人の ID。構文は標準の電子メールアドレスですが、ローカル部分は省略してもかまいません。このアドレスのドメイン部分は、 <code><domain></code> またはそのサブドメインとする必要があります。このオプションは、 <code>--i_tag</code> の値を <code>yes</code> に設定している場合にのみ適用されます。デフォルトは、ローカル部分を空にして、その後には <code>@</code> と <code><domain></code> を続けて記述した値です。
--q_tag	署名に <code>q</code> タグを追加するかどうかを指定します。指定できる値は <code>yes</code> または <code>no</code> です。デフォルトは <code>yes</code> です。
--t_tag	署名に <code>t</code> タグを追加するかどうかを指定します。指定できる値は <code>yes</code> または <code>no</code> です。デフォルトは <code>yes</code> です。

引数	説明
--x_tag	署名に x タグを追加するかどうかを指定します。指定できる値は yes または no です。デフォルトは yes です。
--expiration_time	署名が失効するまでの時間（秒）です。DKIM プロファイルでのみ使用します。この値は、署名の x タグと t タグの差になります。このオプションは、--x_tag の値を yes に設定している場合にのみ適用されます。デフォルトは 31536000 秒（1 年）です。
--z_tag	署名に z タグを追加するかどうかを指定します。指定できる値は yes または no です。デフォルトは no です。

- 署名プロファイルの編集：

```
domainkeysconfig profiles signing edit <name> [signing-profile-options]
```

署名プロファイルのオプション：

- rename <name>
- domain <domain>
- selector <selector>
- canonicalization <canon>
- canonicalization <header_canon> <body_canon>
- key <key_name>
- bodylength <body_length>
- headersselect <header_select>
- customheaders <custom_headers>
- itag <i_tag> [<agent_identity>]
- qtag <q_tag>
- ttag <t_tag>
- xtag <x_tag> [<expiration_time>]
- ztag <z_tag>
- new <user-list>
- delete <user-list>
- print
- クリア
- 署名プロファイルの削除：

```
domainkeysconfig profiles signing delete <name>
```

- 署名プロファイルの一覧表示：

```
domainkeysconfig profiles signing list
```

- 署名プロファイルの詳細出力：

```
domainkeysconfig profiles signing print <name>
```

- 署名プロファイルのテスト：

```
domainkeysconfig profiles signing test <name>
```

- 署名プロファイルのローカル コピーのインポート：

```
domainkeysconfig profiles signing import <filename>
```

- アプライアンスにある署名プロファイルのコピーのエクスポート：

```
domainkeysconfig profiles signing export <filename>
```

- アプライアンスにあるすべての署名プロファイルの削除：

```
domainkeysconfig profiles signing clear
```

バッチ形式：検証プロファイル

- 新しい DKIM 検証プロファイルの作成：

```
domainkeysconfig profiles verification new <name> <verification-profile-options>
```

表 2: *domainkeysconfig* の検証プロファイル オプション

引数	説明
--name	DKIM 検証プロファイルの名前。
--min_key_size	受け入れる最小キー。指定できるキーの長さは512、768、1024、1536、および2048です（単位はビット）。デフォルトは512です。
--max_key_size	受け入れる最大キー。指定できるキーの長さは512、768、1024、1536、および2048です（単位はビット）。デフォルトは2048です。
--max_signatures_num	メッセージの中で検証できる署名の最大数。任意の正数を指定できます。デフォルトは5です。
--key_query_timeout	キークエリーがタイムアウトするまでの時間（秒）です。任意の正数を指定できます。デフォルトは10です。

引数	説明
--max_systemtime_divergence	送信者の時計と検証者の時計との間に許容できる非同期量（秒）です。任意の正数を指定できます。デフォルトは 60 です。
--use_body_length	本文の長さのパラメータを使用するかどうかを指定します。指定できる値は yes または no です。デフォルトは yes です。
--tempfail_action	一時的な障害の場合は、SMTP のアクションを実行します。指定できる値は accept または reject です。デフォルトは accept です。
--tempfail_response_code	一時的な障害が発生した場合、拒否されたメッセージの SMTP 応答コードです。指定できる値は 4XX 形式の番号です。デフォルトは 451 です。
--tempfail_response_text	一時的な障害が発生した場合、拒否されたメッセージの SMTP 応答テキストです。デフォルトは、「#4.7.5 Unable to verify signature - key server unavailable（署名を検証できません。キー サーバが見つかりません）」です。
--permfail_action	永続的な障害の場合は、SMTP のアクションを実行します。指定できる値は accept または reject です。デフォルトは accept です。
--permfail_response_code	永続的な障害が発生した場合、拒否されたメッセージの SMTP 応答コードです。指定できる値は 5XX 形式の番号です。デフォルトは 550 です。
--permfail_response_text	永続的な障害が発生した場合、拒否されたメッセージの SMTP 応答テキストです。デフォルトは「#5.7.5 DKIM unauthenticated mail is prohibited（DKIM 未認証のメールは禁止されています）」です。

- 検証プロファイルの編集：

```
domainkeysconfig profiles verification edit <name> <verification-profile-options>
```

- 検証プロファイルの削除：

```
domainkeysconfig profiles verification delete <name>
```

- 既存の検証プロファイルの詳細出力：

```
domainkeysconfig profiles verification print <name>
```

- 既存の検証プロファイルの一覧表示：

```
domainkeysconfig profiles verification list
```

- ローカルマシンにある検証プロファイルファイルのインポート：

```
domainkeysconfig profiles verification import <filename>
```

- アプライアンスにある検証プロファイルのインポート：

```
domainkeysconfig profiles verification export <filename>
```

- アプライアンスにあるすべての既存検証プロファイルの削除：

```
domainkeysconfig profiles verification clear
```

バッチ形式：署名キー

- 新しい署名キーの作成：

```
domainkeysconfig keys new <key_name> <key-options>
```

表 3: *domainkeysconfig* の署名キー オプション

引数	説明
<code>--generate_key</code>	秘密キーを生成します。指定できるキーの長さは512、768、1024、1536、および2048です（単位はビット）。
<code>--use_key</code>	指定された秘密キーを使用します。
<code>--public_key</code>	指定された秘密キーに一致する公開キーを取得して画面に出力するためのフラグ。 <code>--generate_key</code> を先に指定している場合は、まず新しい秘密キーが生成され、続いてそれに一致する公開キーが表示されます。

- 署名キーの編集：

```
domainkeysconfig keys edit <key_name> key <key-options>
```

- 既存の署名キーの名前変更：

```
domainkeysconfig keys edit <key_name> rename <key_name>
```

- 公開キーを指定するには：

```
domainkeysconfig keys publickey <key_name>
```

- キーの削除：

```
domainkeysconfig keys delete <key_name>
```

- すべての署名キーの一覧表示：

```
domainkeysconfig keys list
```

- 指定の署名キーに関するすべての情報の表示：

```
domainkeysconfig keys print <key_name>
```

- ローカル マシンにある署名キーのインポート：

```
domainkeysconfig keys import <filename>
```

- アプライアンスにある署名キーのエクスポート：

```
domainkeysconfig keys export <filename>
```

- アプライアンスにあるすべての署名キーの削除：

```
domainkeysconfig keys clear
```

バッチ形式：キーまたはプロファイルの検索

- プロファイルの署名キーの検索

```
domainkeysconfig search <search_text>
```

バッチ形式：グローバル設定

- アプライアンスでの DomainKeys/DKIM のグローバル設定の変更：

```
domainkeysconfig setup <setup_options>
```

指定できるオプションは次のとおりです。

- `--sign_generated_msgs`：システムで生成されたメッセージに署名するかどうかを指定します。指定できる値は `yes` または `no` です。

例：CLI によるドメイン キーの設定

アプライアンス上のドメイン キーを設定するには、CLI で **domainkeysconfig** コマンドを使用します。

domainkeysconfig コマンドは、[メールポリシー (Mail Policies)]->[ドメインキー (Domain Keys)] ページ内の機能をすべて備えています。このコマンドでは、サンプルドメインキー DNS TXT レコードを生成することもできます。サンプルドメインキー DNS TXT レコードの生成の詳細については、[サンプルドメインキー DNS TXT レコードの作成 \(46 ページ\)](#) を参照してください。

この例では、キーを生成し、ドメインプロファイルを作成します。

```
mail3.example.com> domainkeysconfig
Number of DK/DKIM Signing Profiles: 0
Number of Signing Keys: 0
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> keys
No signing keys are defined.
Choose the operation you want to perform:
- NEW - Create a new signing key.
- IMPORT - Import signing keys from a file.
[]> new
Enter a name for this signing key:
[]> testkey
1. Generate a private key
2. Enter an existing key
[1]>
Enter the size (in bits) of this signing key:
1. 512
2. 768
3. 1024
4. 1536
5. 2048
[3]>
New key "testkey" created.
There are currently 1 signing keys defined.
Choose the operation you want to perform:
- NEW - Create a new signing key.
- EDIT - Modify a signing key.
- PUBLICKEY - Create a publickey from a signing key.
- DELETE - Delete a signing key.
- PRINT - Display signing keys.
- LIST - List signing keys.
- IMPORT - Import signing keys from a file.
- EXPORT - Export signing keys to a file.
- CLEAR - Clear all signing keys.
[]>
Number of DK/DKIM Signing Profiles: 0
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> profiles
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
```

```

- VERIFICATION - Manage verification profiles.
[]> signing
No domain profiles are defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- IMPORT - Import domain profiles from a file.
[]> new
Enter a name for this domain profile:
[]> Example
Enter type of domain profile:
1. dk
2. dkim
[2]>
The domain field forms the basis of the public-key query. The value in
this field MUST match the domain of the sending email address or MUST
be one of the parent domains of the sending email address. This value
becomes the "d" tag of the DomainKeys signature.
Enter the domain name of the signing domain:
[]> example.com
Selectors are arbitrary names below the "_domainkey." namespace. A
selector value and length MUST be legal in the DNS namespace and in
email headers with the additional provision that they cannot contain a
semicolon. This value becomes the "s" tag of the DomainKeys
Signature.
Enter selector:
[]> test
The private key which is to be used to sign messages must be entered.
A corresponding public key must be published in the DNS following the
form described in the DomainKeys documentation. If a key is not
immediately available, a key can be entered at a later time.
Select the key-association method:
1. Create new key
2. Paste in key
3. Enter key at later time
4. Select existing key
[1]> 4
Enter the name or number of a signing key.
1. testkey
[1]>
The canonicalization algorithm is the method by which the headers and
content are prepared for presentation to the signing algorithm.
Possible choices are "simple" and "relaxed".
Select canonicalization algorithm for body:
1. simple
2. relaxed
[1]> 1
How would you like to sign headers:
1. Sign all existing, non-repeatable headers (except Return-Path header).
2. Sign "well-known" headers (Date, Subject, From, To, Cc, Reply-To, Message-ID, Sender,
  MIME headers).
3. Sign "well-known" headers plus a custom list of headers.
[2]>
Body length is a number of bytes of the message body to sign.
This value becomes the "l" tag of the signature.
Which body length option would you like to use?
1. Whole body implied. No further message modification is possible.
2. Whole body auto-determined. Appending content is possible.
3. Specify a body length.
[1]>
Would you like to fine-tune which tags should be used in the
DKIM Signature? (yes/no) [N]>
Finish by entering profile users. The following types of entries are
allowed:
- Email address entries such as "joe@example.com".

```

```

- Domain entries such as "example.com".
- Partial domain entries such as ".example.com". For example, a partial
  domain of ".example.com" will match "sales.example.com". This
  sort of entry will not match the root domain ("example.com").
- Leave blank to match all domain users.
Enter user for this signing profile:
[]> sales.example.com
Do you want to add another user? [N]>
There are currently 1 domain profiles defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]>
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]>
Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]>

```

サンプルドメインキー DNS TXT レコードの作成

```

mail3.example.com> domainkeysconfig
Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]> profiles
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]> signing
There are currently 1 domain profiles defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.

```

```
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]> dnstxt
Enter the name or number of a domain profile.
1. Example
[1]>
The answers to the following questions will be used to construct DKIM text
record for DNS. It can be used to publish information about this profile.
Do you wish to constrain the local part of the signing identities
("i=" tag of "DKIM-Signature" header field) associated with this
domain profile? [N]>
Do you wish to include notes that may be of interest to a human (no
interpretation is made by any program)? [N]>
The "testing mode" can be set to specify that this domain is testing DKIM and
that unverified email must not be treated differently from verified email.
Do you want to indicate the "testing mode"? [N]>
Do you wish to disable signing by subdomains of this domain? [N]>
The DKIM DNS TXT record is:
test._domainkey.example.com. IN TXT "v=DKIM1;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDX5dOG9J8rXreA/uPtYr5lrCTCqR+qlS5Gm
1f0QpLazSUE2BOnxZ5Nr+se0T+k7mYDF0FSUHyWaoX+Cum7fFRjS3B0F9glbIdH5vz0Kp/w7hdjPy3q6PSgJvtqQ6v9E8k5Ui7C+DF6wUimDSY5sbu2
zmm9rKAH5m7FwIDAQAB;"
There are currently 1 domain profiles defined.
Choose the operation you want to perform:
- NEW - Create a new domain profile.
- EDIT - Modify a domain profile.
- DELETE - Delete a domain profile.
- PRINT - Display domain profiles.
- LIST - List domain profiles.
- TEST - Test if a domain profile is ready to sign.
- DNSTXT - Generate a matching DNS TXT record.
- IMPORT - Import domain profiles from a file.
- EXPORT - Export domain profiles to a file.
- CLEAR - Clear all domain profiles.
[]>
Choose the operation you want to perform:
- SIGNING - Manage signing profiles.
- VERIFICATION - Manage verification profiles.
[]>
Number of DK/DKIM Signing Profiles: 1
Number of Signing Keys: 1
Number of DKIM Verification Profiles: 1
Sign System-Generated Messages: Yes
Choose the operation you want to perform:
- PROFILES - Manage domain profiles.
- KEYS - Manage signing keys.
- SETUP - Change global settings.
- SEARCH - Search for domain profile or key.
[]>
```

DMARC 検証

ここでは、次の CLI コマンドについて説明します。

- [dmarcconfig](#) (48 ページ)

dmarcconfig

説明

DMARC の設定値を設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式：DMARC 検証プロファイル

dmarcconfig のバッチ形式は、検証プロファイルの作成、編集、削除、およびグローバル設定の変更で使用できます。

DMARC 検証プロファイルの追加

dmarcconfig profiles new <name> [options]

引数	説明
<name>	DMARC プロファイルの名前。
[options]	
--rejectpolicy_action	DMARC レコード内のポリシーが「拒否」のときに AsyncOS が実行する必要があるメッセージアクション。可能な値は、“reject”、“quarantine”、または“none”です。
--rejectpolicy_response_code	拒否されたメッセージの SMTP 応答コード。デフォルト値は 550 です。
--rejectpolicy_response_text	拒否されたメッセージの SMTP 応答テキスト。デフォルト値は“#5.7.1 DMARC unauthenticated mail is prohibited.”です。
--rejectpolicy_quarantine	DMARC 検証に失敗したメッセージの隔離。
--quarantinepolicy_action	DMARC レコード内のポリシーが隔離のときに AsyncOS が実行する必要があるメッセージアクション。可能な値は、“quarantine”または“none”です。
--quarantinepolicy_quarantine	DMARC 検証に失敗したメッセージの隔離。

引数	説明
--tempfail_action	DMARC 検証中に一時的な障害が発生したメッセージに対して AsyncOS が実行する必要があるメッセージアクション。指定できる値は“accept”または“reject”です。
--tempfail_response_code	一時的な障害が発生した場合、拒否されたメッセージの SMTP 応答コードです。デフォルト値は 451 です。
--tempfail_response_text	一時的な障害が発生した場合、拒否されたメッセージの SMTP 応答テキストです。デフォルト値は“#4.7.1 Unable to perform DMARC verification”です。
--permfail_action	DMARC 検証中に永続的な障害が発生したメッセージに対して AsyncOS が実行する必要があるメッセージアクション。指定できる値は“accept”または“reject”です。
--permfail_response_code	永続的な障害が発生した場合、拒否されたメッセージの SMTP 応答コードです。デフォルト値は 550 です。
--permfail_response_text	永続的な障害が発生した場合、拒否されたメッセージの SMTP 応答テキストです。デフォルト値は“#5.7.1 DMARC verification failed”です。

DMARC 検証プロファイルの編集

```
dmARCconfig profiles edit <name> [options]
```

DMARC 検証プロファイルの削除

```
dmARCconfig profiles delete <name>
```

すべての DMARC の検証プロファイルの削除

```
dmARCconfig profiles clear
```

DMARC 検証プロファイルの詳細の表示

```
dmARCconfig profiles print <name>
```

DMARC 検証プロファイルのエクスポート

```
dmARCconfig profiles export <filename>
```

DMARC 検証プロファイルのインポート

```
dmARCconfig profiles import <filename>
```

グローバル設定の変更

```
dmARCconfig setup [options]
```

オプション	説明
--report_schedule	AsyncOS が DMARC 集計レポートを生成する時間。
--error_reports	DMARC 集計レポート サイズが 10 MB または DMARC レコードの RUA タグで指定されたサイズを超えた場合に、配信エラーレポートをドメイン所有者に送信する。
--org_name	DMARC 集計レポートを生成するエンティティ。これにはドメイン名を指定する必要があります。
--contact_info	DMARC 集計レポートを受け取ったドメイン所有者がレポートを生成したエンティティと連絡を取る場合の、追加の連絡先情報（組織のカスタマー サポートの詳細など）。
--copy_reports	すべての DMARC 集計レポートのコピーを特定のユーザ（集計レポートの分析を実行する内部ユーザなど）に送信します。電子メールアドレスを入力します。複数の場合はカンマで区切ります。
--bypass_addresslist	特定の送信者から受信したメッセージの DMARC 検証をスキップします（アドレス リスト）。 (注) 完全な E メール アドレスで作成されるアドレス リストのみを選択できます。
--bypass_headers	特定のヘッダー フィールド名を含むメッセージの DMARC 検証をスキップします。たとえば、メーリングリストや信頼できるフォワーダからのメッセージの DMARC 検証をスキップするには、このオプションを使用します。ヘッダーを入力します。複数の場合はカンマで区切ります。

例

次に、DMARC 検証プロファイルを設定し、DMARC 検証プロファイルのグローバル設定を編集する例を示します。

```
mail.example.com> dmarccconfig
Number of DMARC Verification Profiles: 1
Daily report generation time is: 00:00
Error reports enabled: No
Reports sent on behalf of:
Contact details for reports:
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: None Specified
Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]> profiles
There are currently 1 DMARC verification profiles defined.
Choose the operation you want to perform:
```

```

- NEW - Create a new DMARC verification profile.
- EDIT - Modify a DMARC verification profile.
- DELETE - Delete a DMARC verification profile.
- PRINT - Display DMARC verification profiles.
- IMPORT - Import DMARC verification profiles from a file.
- EXPORT - Export DMARC verification profiles to a file.
- CLEAR - Clear all DMARC verification profiles.
[]> new
Enter the name of the new DMARC verification profile:
[]> dmarc_ver_profile_1
Select the message action when the policy in DMARC record is reject:
1. No Action
2. Quarantine the message
3. Reject the message
[3]> 1
Select the message action when the policy in DMARC record is quarantine:
1. No Action
2. Quarantine the message
[2]> 2
Select the quarantine for messages that fail DMARC verification (when the DMARC policy
is quarantine).
1. Policy
[1]> 1
What SMTP action should be taken in case of temporary failure?
1. Accept
2. Reject
[1]> 2
Enter the SMTP response code for rejected messages in case of temporary failure.
[451]>
Enter the SMTP response text for rejected messages in case of temporary failure. Type
DEFAULT to use the default response text
'#4.7.1 Unable to perform
DMARC verification.'
[#4.7.1 Unable to perform DMARC verification.]>
What SMTP action should be taken in case of permanent failure?
1. Accept
2. Reject
[1]> 2
Enter the SMTP response code for rejected messages in case of permanent failure.
[550]>
Enter the SMTP response text for rejected messages in case of permanent failure. Type
DEFAULT to use the default response text
'#4.7.1 Unable to perform
DMARC verification.'
[#5.7.1 DMARC verification failed.]>
There are currently 2 DMARC verification profiles defined.
Choose the operation you want to perform:
- NEW - Create a new DMARC verification profile.
- EDIT - Modify a DMARC verification profile.
- DELETE - Delete a DMARC verification profile.
- PRINT - Display DMARC verification profiles.
- IMPORT - Import DMARC verification profiles from a file.
- EXPORT - Export DMARC verification profiles to a file.
- CLEAR - Clear all DMARC verification profiles.
[]>
Number of DMARC Verification Profiles: 2
Daily report generation time is: 00:00
Error reports enabled: No
Reports sent on behalf of:
Contact details for reports:
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: None Specified
Choose the operation you want to perform:

```

```

- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]> setup
Would you like to modify DMARC report settings? (Yes/No) [N]> y
Enter the time of day to generate aggregate feedback reports. Use 24-hour format (HH:MM).
[00:00]>
Would you like to send DMARC error reports? (Yes/No) [N]> y
Enter the entity name responsible for report generation. This is added to the DMARC
aggregate reports.
[]> example.com
Enter additional contact information to be added to DMARC aggregate reports. This could
be an email address,
URL of a website with additional help, a phone number etc.
[]> http://dmarc.example.com
Would you like to send a copy of all aggregate reports? (Yes/No) [N]>
Would you like to bypass DMARC verification for an addresslist? (Yes/No) [N]>
Would you like to bypass DMARC verification for specific header fields? (Yes/No) [N]> y
Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
[]> add
Enter the header field name
[]> List-Unsubscribe
DMARC verification is configured to bypass DMARC verification for messages containing
the following header fields.
1. List-Unsubscribe
Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
- REMOVE - Remove a header field from the list.
[]> add
Enter the header field name
[]> List-ID
DMARC verification is configured to bypass DMARC verification for messages containing
the following header fields.
1. List-Unsubscribe
2. List-ID
Choose the operation you want to perform:
- ADD - Add a header field to the verification-bypass list.
- REMOVE - Remove a header field from the list.
[]>
Number of DMARC Verification Profiles: 2
Daily report generation time is: 00:00
Error reports enabled: Yes
Reports sent on behalf of: example.com
Contact details for reports: http://dmarc.example.com
Send a copy of aggregate reports to: None Specified
Bypass DMARC verification for senders from addresslist: None Specified
Bypass DMARC verification for messages with header fields: List-Unsubscribe, List-ID
Choose the operation you want to perform:
- PROFILES - Manage DMARC verification profiles.
- SETUP - Change global settings.
[]>

```

DNS

ここでは、次の CLI コマンドについて説明します。

- [dig \(53 ページ\)](#)
- [dnsconfig \(54 ページ\)](#)
- [dnsflush \(58 ページ\)](#)

- [dnshostprefs](#) (59 ページ)
- [dnslistconfig](#) (59 ページ)
- [dnslisttest](#) (60 ページ)
- [dnsstatus](#) (61 ページ)

dig

説明

DNS サーバ上でレコードをルックアップします

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式

dig コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- DNS サーバ上でレコードをルックアップします

```
dig [options] [@<dns_ip>] [qtype] <hostname>
```

- DNS サーバ上で、指定された IP アドレスに対する逆ルックアップを実行します。

```
dig -x <reverse_ip> [options] [@<dns_ip>]
```

これらは dig コマンドのバッチ形式で利用可能なオプションです。

-s <source_ip>	Specify the source IP address.
-t	Make query over TCP.
-u	Make query over UDP (default).
dns_ip	Query the DNS server at this IP address.
qtype	Query type: A, PTR, CNAME, MX, SOA, NS, TXT.

```
hostname - Record that user want to look up.
```

```
reverse_ip - Reverse lookup IP address.
```

```
dns_ip - Query the DNS server at this IP address.
```

例

次の例では、ルックアップする DNS サーバを明示的に指定しています。

```
mail.com> dig @111.111.111.111 example.com MX
; <<>> DiG 9.4.3-P2 <<>> @111.111.111.111 example.com MX
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18540
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 3
;; QUESTION SECTION:
;example.com.                IN      MX
;; ANSWER SECTION:
mexample.com.                10800   IN      MX      10 mexample.com.
;; AUTHORITY SECTION:
example.com.                  10800   IN      NS      test.example.com.
;; ADDITIONAL SECTION:
example.com. 10800 IN      A      111.111.111.111
example.com. 10800 IN      AAAA   2620:101:2004:4201::bd
example.com. 300  IN      A      111.111.111.111
;; Query time: 6 msec
;; SERVER: 10.92.144.4#53(10.92.144.4)
;; WHEN: Fri Dec 9 23:37:42 2011
;; MSG SIZE rcvd: 143
```



(注) このコマンドを使用するときに DNS サーバを明示的に指定しない場合は、**dig** コマンドによって Authority セクションと Additional セクションの情報が絞り込まれます。

dnsconfig

説明

DNS のセットアップを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式

dnsconfig コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- ローカル ネーム サーバ キャッシュを使用するための DNS の設定：

```
dnsconfig parent new <ns_ip> <priority>
```

コマンドの引数：

- <ns_ip>：ネーム サーバの IP アドレス。複数の IP アドレスはカンマで区切って指定します。
- <priority>：このエントリの優先順位。
- ローカル ネーム サーバ キャッシュの削除：

```
dnsconfig parent delete <ns_ip>
```

- 特定のドメインに使用するための代替 DNS キャッシュの設定：

```
dnsconfig alt new <domains> <ns_ip>
```



(注) インターネットのルート ネーム サーバを使用している場合は使用できません。

コマンドの引数：

- <ns_ip>：ネーム サーバの IP アドレス。複数の IP アドレスはカンマで区切って指定します。
- <domains>：ドメインのカンマ区切りリスト。
- 特定のドメインの代替 DNS キャッシュの削除：

```
dnsconfig alt delete <domain>
```

- インターネットのルート ネーム サーバを使用するための DNS の設定：

```
dnsconfig roots new <ns_domain> <ns_name> <ns_ip>
```

ネーム サーバの引数：

- <ns_domain>：優先して使用するドメイン。
- <ns_name>：ネーム サーバの名前。
- <ns_ip>：ネーム サーバの IP アドレス。



(注) ドメインに対する代替ネームサーバを指定することで、特定のドメインよりも優先させることができます。

- ネームサーバの削除：

```
dnsconfig roots delete <ns_domain> [ns_name]
```



(注) 削除するときに `ns_name` を指定しないと、該当のドメインのすべてのネームサーバが削除されます。

- すべての DNS 設定の消去、およびインターネットのルートサーバを使用するためのシステムの自動設定：

```
dnsconfig roots
```

現在の DNS 設定の表示

```
dnsconfig print
```

例

各ユーザ指定の DNS サーバには、次の情報が必要です。

- ホスト名
- IP アドレス
- 権限のあるドメイン（代替サーバのみ）

dnsconfig コマンドでは、次の 4 つのサブコマンドを使用できます。

表 4: *dnsconfig* コマンドのサブコマンド

構文	説明
<code>new</code>	特定のドメインに使用する新しい代替 DNS サーバまたはローカル DNS サーバを追加します。
<code>delete</code>	代替サーバまたはローカル DNS サーバを削除します。
<code>edit</code>	代替サーバまたはローカル DNS サーバを変更します。
<code>setup</code>	インターネット ルート DNS サーバまたはローカル DNS サーバを切り替えます。


```
mail3.example.com> dnsconfig
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]> setup
Do you want the Gateway to use the Internet's root DNS servers or would you like
it to use your own DNS servers?
1. Use Internet root DNS servers
2. Use own DNS cache servers
[1]> 1
Choose the IP interface for DNS traffic.
1. Auto
2. Management (10.92.149.70/24: mail3.example.com)
[1]>
Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>
Enter the minimum TTL in seconds for DNS cache.
[1800]>
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
```

特定のドメインの代替 DNS サーバの追加

特定のローカルドメインを除き、すべてのDNSクエリーでインターネットルートサーバを使用するようにアプライアンスを設定できます。

```
mail3.example.com> dnsconfig
Currently using the Internet root DNS servers.
No alternate authoritative servers configured.
Choose the operation you want to perform:
- NEW - Add a new server.
- SETUP - Configure general settings.
[]> new
Please enter the domain this server is authoritative for. (Ex: "com").
[]> example.com
Please enter the fully qualified hostname of the DNS server for the domain "example.com".
(Ex: "dns.example.com").
[]> dns.example.com
Please enter the IP address of dns.example.com.
[]> 10.1.10.9
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[]>
```

独自の DNS キャッシュ サーバの使用

独自の DNS キャッシュ サーバを使用するようにアプライアンスを設定できます。

```
mail3.example.com> dnsconfig
Currently using the Internet root DNS servers.
Alternate authoritative DNS servers:
1. com: dns.example.com (10.1.10.9)
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[ ]> setup
Do you want the Gateway to use the Internet's root DNS servers or would you like
it to use your own DNS servers?
1. Use Internet root DNS servers
2. Use own DNS cache servers
[1]> 2
Please enter the IP address of your DNS server.
Separate multiple IPs with commas.
[ ]> 10.10.200.03
Please enter the priority for 10.10.200.3.
A value of 0 has the highest priority.
The IP will be chosen at random if they have the same priority.
[0]> 1
Choose the IP interface for DNS traffic.
1. Auto
2. Management (192.168.42.42/24)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Enter the number of seconds to wait before timing out reverse DNS lookups.
[20]>
Enter the minimum TTL in seconds for DNS cache.
[1800]>
Currently using the local DNS cache servers:
1. Priority: 1 10.10.200.3
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
[ ]>
```

dnsflush

説明

DNS キャッシュからすべてのエントリをクリアします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> dnsflush
Are you sure you want to clear out the DNS cache? [N]> Y
```

dnshostprefs

説明

IPv4/IPv6 DNS を設定します

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> dnshostprefs
Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]> new
Enter the domain you wish to configure.
[]> example.com
How should the appliance sort IP addresses for this domain?
1. Prefer IPv4
2. Prefer IPv6
3. Require IPv4
4. Require IPv6
[2]> 3
Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]> setdefault
How should the appliance sort IP addresses?
1. Prefer IPv4
2. Prefer IPv6
3. Require IPv4
4. Require IPv6
[2]> 1
Choose the operation you want to perform:
- NEW - Add new domain override.
- SETDEFAULT - Set the default behavior.
[]>
```

dnslistconfig

説明

DNS リスト サービスのサポートを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> dnslistconfig
Current DNS List Settings:
Negative Response TTL: 1800 seconds
DNS List Query Timeout: 3 seconds
Choose the operation you want to perform:
- SETUP - Configure general settings.
[]> setup
Enter the cache TTL for negative responses in seconds:
[1800]> 1200
Enter the query timeout in seconds:
[3]>
Settings updated.
Current DNS List Settings:
Negative Response TTL: 1200 seconds
DNS List Query Timeout: 3 seconds
Choose the operation you want to perform:
- SETUP - Configure general settings.
[]>
```

dnslisttest

説明

DNS ベースのリスト サービスの DNS ルックアップをテストします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> dnslisttest
Enter the query server name:
[]> mail4.example.com
Enter the test IP address to query for:
[127.0.0.2]> 10.10.1.11
Querying: 10.10.1.11.mail4.example.com
Result: MATCHED
```

dnsstatus

説明

DNS 統計情報を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> dnsstatus
Status as of: Mon Apr 18 10:58:07 2005 PDT
Counters:
DNS Requests      1,115      1,115      1,115
Network Requests  186        186        186
Cache Hits        1,300      1,300      1,300
Cache Misses      1          1          1
Cache Exceptions  0          0          0
Cache Expired     185        185        185
```

一般的な管理/トラブルシューティング

ここでは、次の CLI コマンドについて説明します。

- [addressconfig](#) (62 ページ)
- [adminaccessconfig](#) (64 ページ)
- [certconfig](#) (69 ページ)
- [date](#) (73 ページ)
- [diagnostic](#) (73 ページ)
- [diskquotaconfig](#) (79 ページ)
- [ecconfig](#) (80 ページ)
- [ecstatus](#) (81 ページ)
- [ecupdate](#) (81 ページ)
- [encryptionconfig](#) (82 ページ)
- [encryptionstatus](#) (85 ページ)
- [encryptionupdate](#) (85 ページ)
- [enginestatus](#) (86 ページ)
- [featurekey](#) (87 ページ)
- [featurekeyconfig](#) (88 ページ)
- [generalconfig](#) (89 ページ)

- [healthcheck](#) (89 ページ)
- [healthconfig](#) (90 ページ)
- [ntpconfig](#) (91 ページ)
- [portalregistrationconfig](#) (92 ページ)
- [reboot](#) (93 ページ)
- [repengstatus](#) (93 ページ)
- [resume](#) (94 ページ)
- [resumedel](#) (94 ページ)
- [resumelistener](#) (95 ページ)
- [revert](#) (95 ページ)
- [settime](#) (96 ページ)
- [settz](#) (97 ページ)
- [shutdown](#) (97 ページ)
- [sshconfig](#) (99 ページ)
- [status](#) (102 ページ)
- [supportrequest](#) (103 ページ)
- [supportrequeststatus](#) (105 ページ)
- [supportrequestupdate](#) (106 ページ)
- [suspend](#) (106 ページ)
- [suspenddel](#) (107 ページ)
- [suspendlistener](#) (107 ページ)
- [tcpservices](#) (108 ページ)
- [techsupport](#) (109 ページ)
- [tlsverify](#) (110 ページ)
- [trace](#) (110 ページ)
- [trackingconfig](#) (112 ページ)
- [updateconfig](#) (113 ページ)
- [updatenow](#) (117 ページ)
- [upgrade](#) (119 ページ)
- [version](#) (118 ページ)
- [wipedata](#) (119 ページ)

[仮想アプライアンスの管理](#) (292 ページ) も参照してください。

addressconfig

説明

addressconfig コマンドは、From: アドレス ヘッダーを設定するために使用します。From: 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。次の状況では、AsyncOSによって生成されたメールには **addressconfig** コマンドを使用します。

- Anti-Virus 通知
- バウンス
- DMARC フィードバック レポート (DMARC Feedback Reports)
- 通知 (notify() および notify-copy() フィルタの動作)
- 隔離メッセージ (および隔離管理機能における「コピー送信」)
- レポート
- その他のすべてのメッセージ

次の例では、通知の From: アドレスを Mail Delivery System [MAILER-DAEMON@domain] (デフォルト) から Notifications [Notification@example.com] に変更します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> addressconfig
Current anti-virus from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current bounce from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current notify from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current quarantine from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current DMARC reports from: "DMARC Feedback" <MAILER-DAEMON@domain>
Current all other messages from: "Mail Delivery System" <MAILER-DAEMON@domain>
Choose the operation you want to perform:
- AVFROM - Edit the anti-virus from address.
- BOUNCEFROM - Edit the bounce from address.
- NOTIFYFROM - Edit the notify from address.
- QUARANTINEFROM - Edit the quarantine bcc from address.
- DMARCFROM - Edit the DMARC reports from address.
- OTHERFROM - Edit the all other messages from address.
[]> notifyfrom
Please enter the display name portion of the "notify from" address
["Mail Delivery System"]> Notifications
Please enter the user name portion of the "notify from" address
[MAILER-DAEMON]> Notification
Do you want the virtual gateway domain used for the domain? [Y]> n
Please enter the domain name portion of the "notify from" address
[]> example.com
Current anti-virus from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current bounce from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current notify from: Notifications <Notification@example.com>
Current quarantine from: "Mail Delivery System" <MAILER-DAEMON@domain>
Current DMARC reports from: "DMARC Feedback" <MAILER-DAEMON@domain>
Current all other messages from: "Mail Delivery System" <MAILER-DAEMON@domain>
Choose the operation you want to perform:
- AVFROM - Edit the anti-virus from address.
- BOUNCEFROM - Edit the bounce from address.
- NOTIFYFROM - Edit the notify from address.
- QUARANTINEFROM - Edit the quarantine bcc from address.
- DMARCFROM - Edit the DMARC reports from address.
```

```
- OTHERFROM - Edit the all other messages from address.
[]>
```

adminaccessconfig

説明

次を設定する場合に **adminaccessconfig** コマンドを使用します。

- 管理者のログイン メッセージ（バナー）。
- アプライアンスの管理インターフェイスへの IP ベースのアクセス。
- Web インターフェイスのクロスサイト リクエスト偽造保護。
- HTTP 要求でホスト ヘッダーを使用するオプション。
- Web インターフェイスおよび CLI セッションの非アクティブ タイムアウト。
- 最大 HTTP ヘッダー サイズ。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式

adminaccessconfig コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- すべての IP アドレスにアクセスを許可するか、特定の IP アドレス/サブネット/範囲にアクセスを制限するかを選択

```
adminaccessconfig ipaccess <all/restrict/proxyonly/proxy>
```

- 新しい IP アドレス/サブネット/範囲の追加

```
adminaccessconfig ipaccess new <address>
```

- 既存の IP アドレス/サブネット/範囲の編集

```
adminaccessconfig ipaccess edit <oldaddress> <newaddress>
```

- 既存の IP アドレス/サブネット/範囲の削除

```
adminaccessconfig ipaccess delete <address>
```


- IP アドレス/サブネット/範囲のリストの出力

```
adminaccessconfig ipaccess print
```

- 既存のすべての IP アドレス/サブネット/範囲の削除

```
adminaccessconfig ipaccess clear
```

- ログイン バナーの出力

```
adminaccessconfig banner print
```

- アプライアンス上にあるファイルからのログイン バナーのインポート

```
adminaccessconfig banner import <filename>
```

- 既存のログイン バナーの削除

```
adminaccessconfig banner clear
```

- 初期画面バナーの出力

```
adminaccessconfig welcome print
```

- アプライアンス上にあるファイルからの初期画面バナーのインポート

```
adminaccessconfig welcome import <filename>
```

- 既存の初期画面バナーの削除

```
adminaccessconfig welcome clear
```

- 初期画面バナーのエクスポート

```
adminaccessconfig welcome export <filename>
```

- 許可されたプロキシの IP アドレスの追加

```
adminaccessconfig ipaccess proxylist new <address>
```

- 許可されたプロキシの IP アドレスの編集

```
adminaccessconfig ipaccess proxylist edit <oldaddress> <newaddress>
```

- 許可されたプロキシの IP アドレスの削除

```
adminaccessconfig ipaccess proxylist delete <address>
```

- すべての既存の許可されたプロキシの IP アドレスの削除

```
adminaccessconfig ipaccess proxylist clear
```

- 送信元 IP アドレスを含むヘッダー名の設定

```
adminaccessconfig ipaccess proxy-header <header name>
```

- Web インターフェイスのクロスサイト リクエスト偽造保護の有効化または無効化

```
adminaccessconfig csrf <enable|disable>
```

- Web インターフェイスのクロスサイト リクエスト偽造保護が有効かどうかの確認

```
adminaccessconfig csrf print
```

- Web インターフェイスのセッション タイムアウトの設定

```
adminaccessconfig timeout gui <value>
```

- CLI セッション タイムアウトの設定

```
adminaccessconfig timeout gui <value>
```

例：ネットワーク アクセス リストの設定

E メールセキュリティ アプライアンスにアクセスするユーザの IP アドレスを制御できます。ユーザは、定義したアクセス リストの IP アドレスを持つすべてのマシンから、アプライアンスにアクセスできます。ネットワーク アクセス リストを作成する際は、IP アドレス、サブネット、または CIDR アドレスを指定できます。

AsyncOS では、現在のマシンの IP アドレスがネットワーク アクセス リストに含まれていない場合に警告を表示します。現在のマシンの IP アドレスがリストにない場合、変更をコミットするとアプライアンスにアクセスできなくなります。

次の例では、アプライアンスへのネットワーク アクセスを 2 つの IP アドレス セットに制限します。

```
mail.example.com> adminaccessconfig
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator
```

```

login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSIZE - Configure maximum HTTP header field size.
[> ipaccess
Current mode: Allow All.
Please select the mode:
- ALL - All IP addresses will be allowed to access the administrative interface.
- RESTRICT - Specify IP addresses/Subnets/Ranges to be allowed access.
- PROXYONLY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy.
- PROXY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy or
directly.
[> restrict
List of allowed IP addresses/Subnets/Ranges:
Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
[> new
Please enter IP address, subnet or range.
[> 192.168.1.2-100
List of allowed IP addresses/Subnets/Ranges:
1. 192.168.1.2-100
Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
- EDIT - Modify an existing entry.
- DELETE - Remove an existing entry.
- CLEAR - Remove all the entries.
[> new
Please enter IP address, subnet or range.
[> 192.168.255.12
List of allowed IP addresses/Subnets/Ranges:
1. 192.168.1.2-100
2. 192.168.255.12
Choose the operation you want to perform:
- NEW - Add a new IP address/subnet/range.
- EDIT - Modify an existing entry.
- DELETE - Remove an existing entry.
- CLEAR - Remove all the entries.
[>
Warning: The host you are currently using [72.163.202.175] is not included in the User
Access list. Excluding it will prevent your
host from connecting to the administrative interface. Are you sure you want to continue?
[N]> Y
Current mode: Restrict.
Please select the mode:
- ALL - All IP addresses will be allowed to access the administrative interface.
- RESTRICT - Specify IP addresses/Subnets/Ranges to be allowed access.
- PROXYONLY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy.
- PROXY - Specify IP addresses/Subnets/Ranges to be allowed access through proxy or
directly.
[>

```

例：ログインバナーの設定

ユーザが SSH、Telnet、FTP、または Web UI からログインしようとした際に、「ログインバナー」と呼ばれるメッセージを表示するように E メールセキュリティ アプライアンスを設定できます。ログインバナーは、CLI でログインプロンプトの上部に表示され、GUI でログインプロンプトの右側に表示されるカスタマイズ可能なテキストです。ログインバナーを使用して、内部のセキュリティ情報またはアプライアンスのベストプラクティスに関する説明を表示できます。たとえば、許可しないアプライアンスの使用を禁止する簡単な注意文言を作成し

例：Web インターフェイスおよび CLI セッションタイムアウトの設定

たり、ユーザがアプライアンスに対して行った変更を確認する企業の権利に関する詳細な警告を作成したりできます。

ログインバナーは、80 x 25 のコンソールに収まるように最大 2000 文字になっています。ログインバナーは、アプライアンスの /data/pub/configuration ディレクトリにあるファイルからインポートできます。バナーを作成したら、変更内容を確定します。

次の例では、アプライアンスにログインバナー「Use of this system in an unauthorized manner is prohibited」を追加します。

```
mail.example.com> adminaccessconfig
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSIZE - Configure maximum HTTP header field size.
[]> banner
A banner has not been defined.
Choose the operation you want to perform:
- NEW - Create a banner to display at login.
- IMPORT - Import banner text from a file.
[]> new
Enter or paste the banner text here. Enter CTRL-D on a blank line to end.
Use of this system in an unauthorized manner is prohibited.
^D
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[]> banner
Banner: Use of this system in an unauthorized manner is prohibited.
Choose the operation you want to perform:
- NEW - Create a banner to display at login.
- IMPORT - Import banner text from a file.
- DELETE - Remove the banner.
[]>
```

例：Web インターフェイスおよび CLI セッションタイムアウトの設定

次の例では、Web インターフェイスと CLI セッションタイムアウトを 32 分に設定します。



(注) CLIセッションタイムアウトは、セキュアシェル (SSH)、SCP、および直接シリアル接続を使用する接続にだけ適用されます。CLIセッションタイムアウト時に未確定の設定変更は失われます。設定を変更したらすぐに確定してください。

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

```
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
- MAXHTTPHEADERFIELDSize - Configure maximum HTTP header field size.
[]> timeout
Enter WebUI inactivity timeout(in minutes):
[30]> 32
Enter CLI inactivity timeout(in minutes):
[30]> 32
Choose the operation you want to perform:
- BANNER - Configure login message (banner) for appliance administrator login.
- WELCOME - Configure welcome message (post login message) for appliance administrator login.
- IPACCESS - Configure IP-based access for appliance administrative interface.
- CSRF - Configure web UI Cross-Site Request Forgeries protection.
- HOSTHEADER - Configure option to use host header in HTTP requests.
- TIMEOUT - Configure GUI and CLI session inactivity timeout.
[]>
mail.example.com> commit
Please enter some comments describing your changes:
[]> Changed WebUI and CLI session timeout values
Do you want to save the current configuration for rollback? [Y]>
Changes committed: Wed Mar 12 08:03:21 2014 GMT
```



(注) 変更を確定した後、新しいCLIセッションタイムアウトは次回以降のログイン時にだけ反映されます。

certconfig

説明

セキュリティの証明書とキーを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例：証明書の貼り付け

次の例では、証明書と秘密キーを貼り付けることによって証明書をインストールします。

```
mail3.example.com> certconfig
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
```

```

- CRL - Manage Certificate Revocation Lists
[]> certificate
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
Demo          Cisco Appliance Demo   Cisco Appliance Demo   Active          3467 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- PRINT - View certificates assigned to services
[]> paste
Enter a name for this certificate profile:
> partner.com
Paste public certificate in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIICLDCCAdYCAQAwDQYJKoZIhvcNAQEEBQAwgAxCzAJBgNVBAYTA1BURMRWwEQYD
VQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNlb2ExFzAVBgNVBAoTDk5ldXJv
bmlvLlCBMzGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZG
dXR1cy5uZXVyb25pby5wdDEhMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZpMB4X
DTk2MDkwNTAzNDI0M1oXDTEk2MTAwNTAzNDI0M1owGAxCzAJBgNVBAYTA1BURMRW
EQYDVQQIEwpRdWVlbnNsYW5kMQ8wDQYDVQQHEwZMaXNlb2ExFzAVBgNVBAoTDk5ldXJv
bmlvLlCBMzGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZGZG
EmJydXR1cy5uZXVyb25pby5wdDEhMBkGCSqGSIb3DQEJARYMc2FtcG9AaWtpLmZp
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNw
L4lYKbpzzlmc5beaQXeq2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAATAN
BgkqhkiG9w0BAQQQFAANBAFqPEKFjk6T6CKTHvaQeEAsX0/8YHPHQH/9AnhSjrwuX
9EBc0n6bVGhN7XaXd6sJ7dym9sbsWxb+pJdurnkxjx4=
-----END CERTIFICATE-----
.
C=PT,ST=Queensland,L=Lisboa,O=Neuronio,
Lda.,OU=Desenvolvimento,CN=brutus.partner.com,emailAddress=admin@example.com
Paste private key in PEM format (end with '.'):
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAL7+aty3S1iBA/+yxjxv4q1MUTd1kjNwL4lYKbpzzlmc5beaQXeq
2RmGMTXU+mDvuqItjVHOK3DvPK7lTcSGftUCAwEAAQJBALjkK+jc2+iihI98riEF
oudmkNziSRTYjnwjx8mCoAjPWviB3c742e03FG4/soiljD9A5alihEOXFUzloenr
8IECIQD3B5+0l+68BA/6d76iUNqAAV8djGTzvxnCxycnxPQydQIhAMXt4trUI3nc
a+U8YL2HPFA3gmhBsSICbq2OptOCnM7hAiEA6Xi3JIQECob8Ywkrj29DU3/4WYD7
WLPgsQpwo1GuSpECICGsnWH5oaeD9t9jbFoSfhJvv0IZmxcLpRcpslpeWBBaiEA
6/5B8J0GHdJq89FHWEG/H2eVVUYu5y/aD6sgcm+0Avg=
-----END RSA PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
partner.c brutus.partner.com   brutus.partner     Active          30 days
Demo          Cisco Appliance Demo   Cisco Appliance Demo   Active          3467 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]>

```

```
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Installed certificate and key for receiving, delivery, and https
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

例: 自己署名証明書の作成

次の例では、自己署名証明書を作成します。

```
mail3.example.com> certconfig
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certificate
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
partner.c     brutus.neuronio.pt    brutus.neuronio.pt Expired          -4930
days
Demo          Cisco Appliance Demo  Cisco Appliance Demo Active           3467 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]> new
1. Create a self-signed certificate and CSR
2. Create a self-signed SMIME certificate and CSR
[1]> 1
Enter a name for this certificate profile:
> example.com
Enter Common Name:
> example.com
Enter Organization:
> Example
Enter Organizational Unit:
> Org
Enter Locality or City:
> San Francisoc
Enter State or Province:
> CA
Enter Country (2 letter code):
> US
Duration before expiration (in days):
[3650]>
1. 1024
2. 2048
Enter size of private key:
[2]>
Do you want to view the CSR? [Y]> y
-----BEGIN CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDELMakGA1UEBhMCVVMxFDASBgNVBAMTC2V4YW1wbGUuY29t
MRYwFAYDVQQHEw1TYW4gRnJhbmNpc29jMRAwDgYDVQQKEwdleGFtcGxlMQswCQYD
VQIQIEWJDQTEEMMAoGA1UECxb3JnMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEANwamZyX7VgTZka/x1I5HHrN9V2MPKXoLq7FjzUtiIDwznElrKIuJovw
Svonle6GvF1UHfjv8B3WobOzk5Ny6btKjwPrBfaY+qr7rzM4lAQKHM+P6l+1ZnPU
P05N9RCkLP4XsUuyY6CalWLTiPIgaq2fR8Y0JX/kesZcGOqlde66pN+xJIHHYadD
```

例：自己署名 S/MIME 署名証明書の作成

```

oopOgqi6SLNfAzJu/HEu/fnSujG4nhF0ZG1OpVUx4fg33NwZ4wVl0XBk3GrOjbbA
ih9ozAwfNzxb57amtxEJk+pW+co3uEHLJIOpdiH9SHzn/UVU4hiu8rSQR19sDApp
kfdWcfadLF9tnQJPWSYoCh0USGcC8QIDAQABAAAwDQYJKoZIhvcNAQEFBQADggEB
AG1VhyMAZuHSv9yA08kJCmrgO89yRlnDUXDDo6IrODVKx4hHTiOanOPulnsThSvH
7xV4xR35T/QV0U3yPrL6bJbbwMySOLIRTjsUcwZNjOE1xMM5EkBM2BOI5rs4l59g
FhHVejhG1LyyUDL0U82wsSLMqLFH1IT63tzwVmRiIXmAu/lHYci3+vctb+sopnN1
lY1OIuj+EgqWNrRBNnKXLtdXkzhELOd8vZEqSAfBWyjZ2mECzC7SG3evqkw/OGLk
AILNXHayiGjeY+UfWzF/HBSeKsJtQu6hIv6JpBSY/MnYU4tllExqD+GX3lru4xc4
zDas2rS/Pbpn73Lf503nmsw=
-----END CERTIFICATE REQUEST-----
List of Certificates

```

Name	Common Name	Issued By	Status	Remaining
example.c	example.com	example.com	Valid	3649 days
partner.c	brutus.partner.com	brutus.partner.com	Valid	30 days
Demo	Cisco Appliance Demo	Cisco Appliance Demo	Active	3467 days

```

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>

```

例：自己署名 S/MIME 署名証明書の作成

次に、署名メッセージの自己署名 S/MIME 証明書を作成する例を示します。

```

vm10esa0031.qa> certconfig
Choose the operation you want to perform:
- CERTIFICATE - Import, Create a request, Edit or Remove Certificate Profiles
- CERTAUTHORITY - Manage System and Customized Authorities
- CRL - Manage Certificate Revocation Lists
[]> certificate
List of Certificates

```

Name	Common Name	Issued By	Status	Remaining
Demo	Cisco Appliance Demo	Cisco Appliance Demo	Active	3329 days

```

Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- PRINT - View certificates assigned to services
[]> new
1. Create a self-signed certificate and CSR
2. Create a self-signed SMIME certificate and CSR
[1]> 2
Enter a name for this certificate profile:
> smime_signing
Enter Common Name:
> CN
Enter Organization:
> ORG
Enter Organizational Unit:
> OU
Enter Locality or City:
> BN
Enter State or Province:
> KA
Enter Country (2 letter code):

```



```
> IN
Duration before expiration (in days):
[3650]>
1. 1024
2. 2048
Enter size of private key:
[2]>
Enter email address for 'subjectAltName' extension:
[]> admin@example.com
Add another member? [Y]> n
Begin entering domain entries for 'subjectAltName'.
Enter the DNS you want to add.
[]> domain.com
Add another member? [Y]> n
Do you want to view the CSR? [Y]> n
List of Certificates
Name          Common Name          Issued By          Status          Remaining
-----
smime_sig     CN                    CN                  Valid           3649 days
Demo          Cisco Appliance Demo Cisco Appliance Demo Active           3329 days
Choose the operation you want to perform:
- IMPORT - Import a certificate from a local PKCS#12 file
- PASTE - Paste a certificate into the CLI
- NEW - Create a self-signed certificate and CSR
- EDIT - Update certificate or view the signing request
- EXPORT - Export a certificate
- DELETE - Remove a certificate
- PRINT - View certificates assigned to services
[]>
```

date

説明

現在の日時を表示します

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> date
Tue Mar 10 11:30:21 2015 GMT
```

diagnostic

説明

diagnostic コマンドは次のために使用します。

- さまざまなユーティリティを使用した、ハードウェアとネットワークの問題のトラブルシューティング
- RAID の状態のチェック
- ARP キャッシュの表示
- LDAP、DNS、および ARP キャッシュのクリア
- SMTP テスト メッセージの送信
- アプライアンスで有効になっているサービス エンジンのステータスの再起動と表示

diagnostic コマンドの使用

diagnostic サブメニューでは、次のコマンドを使用できます。

表 5: *diagnostic* サブコマンド

オプション	サブコマンド	アベイラビリティ
RAID	1. ディスク 検証の実行	C30 および C60 でのみ使用可能。
	2. 実行中のタスクのモニタ	
	3. ディスク 検証結果の表示	
DISK_USAGE (廃止)	サブコマンドなし	このコマンドはすでに廃止されています。代わりに、 diskquotaconfig コマンドを使用します。
NETWORK	FLUSH	C-Series、X-Series、M-Series
	ARPSHOW	
	SMTPPING	
	TCPDUMP	
REPORTING	DELETEDB	C-Series、X-Series、M-Series
	DISABLE	
TRACKING	DELETEDB	C-Series、X-Series、M-Series
	DEBUG	
RELOAD	サブコマンドなし	C-Series、X-Series、M-Series
SERVICES	RESTART	C-Series、X-Series、M-Series
	STATUS	

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカルファイルシステムにアクセスする必要があります。

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。

バッチ形式

diagnostic コマンドのバッチ形式を使用すると、RAID の状態のチェック、キャッシュのクリア、ARP キャッシュの内容の表示を実行できます。バッチ コマンドとして実行するには、次の形式を使用します。

次の操作のためにバッチ形式を使用します。

- RAID の状態のチェック

```
diagnostic raid
```

- ARP キャッシュの内容の表示

```
diagnostic network arpshow
```

- NDP キャッシュの内容の表示

```
diagnostic network ndpshow
```

- LDAP、DNS、ARP、および NDP キャッシュのクリア

```
diagnostic network flush
```

- レポート データベースのリセットおよび削除

```
diagnostic reporting deletedb
```

- レポート デーモンの有効化

```
diagnostic reporting enable
```

- レポート デーモンの無効化

```
diagnostic reporting disable
```

- トラッキング データベースのリセットおよび削除

例：ARP キャッシュの表示とクリア

```
diagnostic tracking deletedb
```

- 最初の製造元の値に設定をリセット

```
diagnostic reload
```

例：ARP キャッシュの表示とクリア

次の例では、**diagnostic** コマンドを使用して、ARP キャッシュの内容を表示し、ネットワークに関連するすべてのキャッシュをフラッシュします。

```
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.
[]> network
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> arpshow
System ARP cache contents:
(10.76.69.3) at 00:1e:bd:28:97:00 on em0 expires in 1193 seconds [ethernet]
(10.76.69.2) at 00:1e:79:af:f4:00 on em0 expires in 1192 seconds [ethernet]
(10.76.69.1) at 00:00:0c:9f:f0:01 on em0 expires in 687 seconds [ethernet]
(10.76.69.149) at 00:50:56:b2:0e:2b on em0 permanent [ethernet]
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTPPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> flush
Flushing LDAP cache.
Flushing DNS cache.
Flushing system ARP cache.
10.76.69.3 (10.76.69.3) deleted
10.76.69.2 (10.76.69.2) deleted
10.76.69.1 (10.76.69.1) deleted
10.76.69.149 (10.76.69.149) deleted
Flushing system NDP cache.
fe80::250:56ff:feb2:e2d%em2 (fe80::250:56ff:feb2:e2d%em2) deleted
fe80::250:56ff:feb2:e2c%em1 (fe80::250:56ff:feb2:e2c%em1) deleted
fe80::250:56ff:feb2:e2b%em0 (fe80::250:56ff:feb2:e2b%em0) deleted
Network reset complete.
```

例：別のメールサーバとの接続の検証

次の例では、**diagnostic** コマンドを使用して別のメールサーバとの接続をチェックします。メールサーバをテストするには、サーバに対してメッセージを送信するか、**ping** を実行します。

```
mail.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[]> network
Choose the operation you want to perform:
- FLUSH - Flush all network related caches.
- ARPSHOW - Show system ARP cache.
- NDPSHOW - Show system NDP cache.
- SMTTPING - Test a remote SMTP server.
- TCPDUMP - Dump ethernet packets.
[]> smtpping
Enter the hostname or IP address of the SMTP server:
[mail.example.com]> mail.com
The domain you entered has MX records.
Would you like to select an MX host to test instead? [Y]> y
Select an MX host to test.
1. mx00.gmx.com
2. mx01.gmx.com
[1]>
Select a network interface to use for the test.
1. Management
2. auto
[2]> 1
Do you want to type in a test message to send? If not, the connection will be tested
but no email will be sent. [N]>
Starting SMTP test of host mx00.gmx.com.
Resolved 'mx00.gmx.com' to 74.208.5.4.
Unable to connect to 74.208.5.4.
```

例：最初の製造元の値にアプライアンス設定をリセット

次に、最初の製造元の値にアプライアンスの設定をリセットする例を示します。

```
mail.example.com> diagnostic
Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
[]> reload
This command will remove all user settings and reset the entire device.
If this is a Virtual Appliance, all feature keys will be removed,
and the license must be reapplied.
Are you sure you want to continue? [N]> Y
Are you *really* sure you want to continue? [N]> Y
Do you want to wipe also? [N]> Y
```

サービス エンジン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 エンジンを再起動します。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 エンジンのステータスを表示します。

例：DLP エンジン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 DLP エンジン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:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- SBRS - Reputation Engine services
- TRACKING - Tracking associated services
- URLFILTERING - URL Filtering
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[]> dlp

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

Cisco Data Loss Prevention has been up for 3s.
```

例：Graymail エンジンの再起動

次の例では、`services` コマンドを使用して、アプライアンスの Graymail エンジンを再起動します。

```
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:
- ANTISPAM - Anti-Spam services
- ANTIVIRUS - Anti-Virus services
- DLP - Cisco Data Loss Prevention services
- ENCRYPTION - Encryption services
- GRAYMAIL - Graymail services
- REPORTING - Reporting associated services
- SBRS - Reputation Engine services
- TRACKING - Tracking associated services
- URLFILTERING - URL Filtering
- EUQWEB - End User Quarantine GUI
- WEBUI - Web GUI
[> graymail

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

diskquotaconfig

レポートと追跡、隔離、ログ ファイル、パケット キャプチャ、およびコンフィギュレーション ファイル用のディスク領域割り当てを表示または設定します。

この機能の詳細については、『*User Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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。

バッチ形式

```
diskquotaconfig <feature> <quota> [<feature> <quota> [<feature> <quota>[<feature> <quota>]]]
```

<feature> の有効値は、euq、pvo、tracking、reporting です。

<quota> の有効値は整数です。

例

```
mail.example.com> diskquotaconfig
Service                               Disk Usage (GB)  Quota (GB)
-----
Spam Quarantine (EUQ)                 1                1
Policy, Virus & Outbreak Quarantines 1                3
Reporting                             5               10
```

```

Tracking 1 10
Miscellaneous Files 5 30
    System Files Usage : 5 GB
    User Files Usage : 0 GB
Total 13 54 of 143
Choose the operation you want to perform:
- EDIT - Edit disk quotas
[]> edit
Enter the number of the service for which you would like to edit disk quota:
1. Spam Quarantine (EUQ)
2. Policy, Virus & Outbreak Quarantines
3. Reporting
4. Tracking
5. Miscellaneous Files
[1]> 1
Enter the new disk quota -
[1]> 1
Disk quota for Spam Quarantine (EUQ) changed to 1
Service Disk Usage(GB) Quota(GB)
-----
Spam Quarantine (EUQ) 1 1
Policy, Virus & Outbreak Quarantines 1 3
Reporting 5 10
Tracking 1 10
Miscellaneous Files 5 30
    System Files Usage : 5 GB
    User Files Usage : 0 GB
Total 13 54 of 143
Choose the operation you want to perform:
- EDIT - Edit disk quotas
[]>

```

ecconfig

URLフィルタリング機能で使用する証明書の取得に使用する登録クライアントを設定またはクリアします。

シスコのサポートから指示がない場合は、このコマンドを使用しないでください。

エントリは、<hostname:port> または <IPv4 address:port> の形式にする必要があります。ポートはオプションです。

デフォルト サーバを指定するには、ecconfig server default と入力します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、クラスタ内のすべてのレベルで使用できます。

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。

バッチ形式

- デフォルト以外の登録クライアント サーバを指定するには：

```
> ecconfig server <server_name:port>
```


デフォルトの登録クライアント サーバを使用するには：

```
> ecconfig server default
```

例

```
mail.example.com> ecconfig
Enrollment Server: Not Configured (Use Default)
Choose the operation you want to perform:
- SETUP - Configure the Enrollment Server
[]> setup
Do you want to use non-default Enrollment server?
WARNING: Do not configure this option without the assistance of Cisco Support.
Incorrect configuration can impact the services using certificates from the Enrollment
server. [N]> y
[]> 192.0.2.1
Choose the operation you want to perform:
- SETUP - Configure the Enrollment Server
[]>
```

ecstatus

URL フィルタリング機能で使用する証明書を自動的に取得するのに使用される、登録クライアントの現在のバージョンを表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail.example.com> ecstatus
Component      Version      Last Updated
Enrollment Client  1.0.2-046  Never updated
```

ecupdate

URL フィルタリング機能で使用する証明書を自動的に取得するのに使用される、登録クライアントを手動で更新します。通常、この更新は自動的に行われます。シスコのサポートから指示がない場合は、このコマンドを使用しないでください。

force パラメータ（ecupdate [force]）を使用した場合、変更が検出されなくても、クライアントが更新されます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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。

バッチ形式

```
> ecupdate [force]
```

例

```
mail.example.com> ecupdate
Requesting update of Enrollment Client.
```

encryptionconfig

電子メール暗号化を設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

次に、暗号化プロファイルを変更する例を示します。

```
mail.example.com> encryptionconfig
IronPort Email Encryption: Enabled
Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> setup
PXE Email Encryption: Enabled
Would you like to use PXE Email Encryption? [Y]>
WARNING: Increasing the default maximum message size(10MB) may result in
decreased performance. Please consult documentation for size recommendations
based on your environment.
Maximum message size for encryption: (Add a trailing K for kilobytes, M for
megabytes, or no letters for bytes.)
[10M]>
Enter the email address of the encryption account administrator
[administrator@example.com]>
IronPort Email Encryption: Enabled
Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> profiles
Proxy: Not Configured
Profile Name          Key Service          Proxied          Provision Status
-----
```

```

HIPAA                Hosted Service                No                Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]> edit
1. HIPAA
Select the profile you wish to edit:
[1]> 1
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated
Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLETT - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[]> security
1. High Security (Recipient must enter a passphrase to open the encrypted
message, even if credentials are cached ("Remember Me" selected).)
2. Medium Security (No passphrase entry required if recipient credentials are
cached ("Remember Me" selected).)
3. No passphrase Required (The recipient does not need a passphrase to open the
encrypted message.)
Please enter the envelope security level:
[1]> 1
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: No
Secure Reply All enabled: No
Suppress Applet: No

```

```

URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated
Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLET - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[]> forward
Would you like to enable "Secure Forward"? [N]> y
Profile name: HIPAA
External URL: https://res.cisco.com
Encryption algorithm: ARC4
Payload Transport URL: http://res.cisco.com
Envelope Security: High Security
Return receipts enabled: Yes
Secure Forward enabled: Yes
Secure Reply All enabled: No
Suppress Applet: No
URL associated with logo image: <undefined>
Encryption queue timeout: 14400
Failure notification subject: [ENCRYPTION FAILURE]
Failure notification template: System Generated
Filename for the envelope: securedoc_${date}T${time}.html
Use Localized Envelope: No
Text notification template: System Generated
HTML notification template: System Generated
Choose the operation you want to perform:
- NAME - Change profile name
- EXTERNAL - Change external URL
- ALGORITHM - Change encryption algorithm
- PAYLOAD - Change the payload transport URL
- SECURITY - Change envelope security
- RECEIPT - Change return receipt handling
- FORWARD - Change "Secure Forward" setting
- REPLYALL - Change "Secure Reply All" setting
- LOCALIZED_ENVELOPE - Enable or disable display of envelopes in languages
other than English
- APPLET - Change applet suppression setting
- URL - Change URL associated with logo image
- TIMEOUT - Change maximum time message waits in encryption queue
- BOUNCE_SUBJECT - Change failure notification subject
- FILENAME - Change the file name of the envelope attached to the encryption
notification.
[]>
Proxy: Not Configured
Profile Name           Key Service           Proxied           Provision Status

```

```

-----
HIPAA                Hosted Service          No          Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]>
IronPort Email Encryption: Enabled
Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]>

```

encryptionstatus

説明

encryptionstatus コマンドは、E メールセキュリティ アプライアンス上の PXE エンジンとドメインマッピング ファイルのバージョンとコンポーネントが最後に更新された日時を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```

mail3.example.com> encryptionstatus
Component          Version      Last Updated
PXE Engine         6.7.1       17 Nov 2009 00:09 (GMT)
Domain Mappings File 1.0.0       Never updated

```

encryptionupdate

説明

encryptionupdate コマンドは、E メールセキュリティ アプライアンス上の PXE エンジンの更新を要求します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログイン ホスト（ユーザがログインしたマシン）でのみ使用できます。

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せん。

例

```
mail3.example.com> encryptionupdate
Requesting update of PXE Engine.
```

enginestatus

説明

enginestatus コマンドは、アプライアンス上でイネーブルになっている各種エンジンのステータスと CPU 使用率を表示するために使用されます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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 enginestatus 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

次の例は、アプライアンス上でイネーブルになっているすべてのエンジンのステータスと CPU 使用率を表示する方法を示しています。

```
vm30esa0086.ibqa> enginestatus
Choose the operation you want to perform:
- GRAYMAIL - View Graymail engine status
- SOPHOS - View Sophos engine status
- CASE - View CASE engine status
- AMP - View AMP engine status
- MCAFEE - View McAfee engine status
- ALL - View status of All engines
[]> ALL
CASE Status: UP CPU: 0.0%
Component                                Version                                Last Updated
CASE Core Files                          3.5.0-008                            Never updated
CASE Utilities                          3.5.0-008                            Never updated
Structural Rules                        3.3.1-009-20141210_214201            Never updated
Web Reputation DB                       20141211_111021                      Never updated
Web Reputation Rules                    20141211_111021-20141211_170330      Never updated
Content Rules                           unavailable                           Never updated
Content Rules Update                    unavailable                           Never updated
SOPHOS Status: UP CPU: 0.0%
Component                                Version                                Last Updated
Sophos Anti-Virus Engine                 3.2.07.365.2_5.30                   Never updated
Sophos IDE Rules                         0                                    Never updated
```

```
GRAYMAIL Status: UP CPU: 0.0%
Component                Version                Last Updated
Graymail Engine          01-392.68             N10 Nov 2016 07:08
(GMT +00:00) updated
Graymail Rules           01-392.68#121         Never updated
Graymail Tools           1.0.03                Never updated
MCAfee Status: UP CPU: 0.0%
Component                Version                Last Updated
McAfee Engine            5700                  Never updated
McAfee DATs              7437                  Never updated
AMP Status: UP CPU: 0.0%
Component                Version                Last Updated
AMP Client Settings      1.0                   Never updated
AMP Client Engine        1.0                   Never updated
```

featurekey

説明

featurekey コマンドは、システム上でキーによってイネーブルになっているすべての機能とキーに関連する情報を表示します。また、キーを使用して機能を有効にしたり、新しい機能キーをチェックしたりすることもできます。

仮想アプライアンスについては、[loadlicense \(292 ページ\)](#) および [showlicense \(293 ページ\)](#) も参照してください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

この例では、**featurekey** コマンドを使用して新しい機能キーをチェックします。

```
mail3.example.com> featurekey
Module                Quantity  Status  Remaining  Expiration Date
Outbreak Filters      1        Active  28 days    Tue Feb 25 06:40:53
  2014
IronPort Anti-Spam    1        Dormant  30 days    Wed Feb 26 07:56:57
  2014
Sophos Anti-Virus     1        Active  26 days    Sun Feb 23 02:27:48
  2014
Bounce Verification   1        Dormant  30 days    Wed Feb 26 07:56:57
  2014
Incoming Mail Handling 1        Active  20 days    Sun Feb 16 08:55:58
  2014
IronPort Email Encryption 1        Dormant  30 days    Wed Feb 26 07:56:57
  2014
Data Loss Prevention  1        Active  25 days    Fri Feb 21 10:07:10
  2014
McAfee                1        Dormant  30 days    Wed Feb 26 07:56:57
  2014
Choose the operation you want to perform:
```

```
- ACTIVATE - Activate a (pending) key.
- CHECKNOW - Check now for new feature keys.
[]> checknow
No new feature keys are available.
```

featurekeyconfig

説明

featurekeyconfig コマンドでは、使用可能なキーのダウンロードとマシン上のキーの更新を自動的に行うようにマシンを設定できます。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

この例では、featurekeyconfig コマンドを使用して autoactivate および autocheck 機能をイネーブルにします。

```
mail3.example.com> featurekeyconfig
Automatic activation of downloaded keys: Disabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- SETUP - Edit feature key configuration.
[]> setup
Automatic activation of downloaded keys: Disabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- AUTOACTIVATE - Toggle automatic activation of downloaded keys.
- AUTOCHECK - Toggle automatic checking for new feature keys.
[]> autoactivate
Do you want to automatically apply downloaded feature keys? [N]> y
Automatic activation of downloaded keys: Enabled
Automatic periodic checking for new feature keys: Disabled
Choose the operation you want to perform:
- AUTOACTIVATE - Toggle automatic activation of downloaded keys.
- AUTOCHECK - Toggle automatic checking for new feature keys.
[]> autocheck
Do you want to periodically query for new feature keys? [N]> y
Automatic activation of downloaded keys: Enabled
Automatic periodic checking for new feature keys: Enabled
```


generalconfig

説明

generalconfig コマンドを使用するとブラウザを設定できます。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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 generalconfig** 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：Internet Explorer 互換性モードのオーバーライドの設定

次に、IE 互換性モードをオーバーライドする例を示します。

```
mail.example.com> generalconfig
Choose the operation you want to perform:
- IEVERRIDE - Configure Internet Explorer Compatibility Mode Override
[]> ieoverride
    For better web interface rendering, we recommend that you enable Internet Explorer Compatibility Mode Override. However, if enabling this feature is against your organizational policy, you may disable this feature.
    Internet Explorer Compatibility Mode Override is currently disabled.
Would you like to enable Internet Explorer Compatibility Mode Override? [N]y
Choose the operation you want to perform:
- IEVERRIDE - Configure Internet Explorer Compatibility Mode Override
[]>
```

healthcheck

説明

E メールセキュリティ アプライアンスの状態を確認します。ヘルス チェックにより現在のステータス ログの履歴データ（最大 3 カ月）が分析され、アプライアンスの状態が判断されます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> healthcheck
Analyzing the system to determine current health of the system.
The analysis may take a while, depending on the size of the historical data.
System analysis is complete.
The analysis indicates that the system has experienced the following issue(s) recently:
Entered Resource conservation mode
Delay in mail processing
High CPU usage
High memory usage
Based on this analysis,
we recommend you to contact Cisco Customer Support before upgrading.
```

healthconfig

説明

CPU 使用率、ワーク キューの最大メッセージ数など、アプライアンスのさまざまな健全性パラメータのしきい値を設定します

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> healthconfig
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> workqueue
Number of messages in the workqueue : 0
Current threshold on the workqueue size : 500
Alert when exceeds threshold : Disabled
Do you want to edit the settings? [N]> y
Please enter the threshold value for number of messages in work queue.
[500]> 550
Do you want to receive alerts if the number of messages in work queue exceeds
threshold value? [N]> n
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> cpu
Overall CPU usage : 0 %
Current threshold on the overall CPU usage: 85 %
Alert when exceeds threshold : Disabled
Do you want to edit the settings? [N]> y
Please enter the threshold value for overall CPU usage (in percent)
```

```
[85]> 90
Do you want to receive alerts if the overall CPU usage exceeds threshold value? [N]> n
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]> swap
Number of pages swapped from memory in a minute : 0
Current threshold on the number of pages swapped from memory per minute : 5000
Alert when exceeds threshold : Disabled
Do you want to edit the settings? [N]> y
Please enter the threshold value for number of pages swapped from memory in a
minute.
[5000]> 5500
Do you want to receive alerts if number of pages swapped from memory in a
minute exceeds the threshold? [N]> n
Choose the operation you want to perform:
- WORKQUEUE - View and edit workqueue-health configuration.
- CPU - View and edit CPU-health configuration.
- SWAP - View and edit swap-health configuration.
[]>
```

ntpconfig

説明

ntpconfig コマンドでは、ネットワーク タイム プロトコル (NTP) を使用してシステム クロックを他のコンピュータと同期するように、AsyncOS を設定します。NTP をオフにするには、**settime** コマンドを使用します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com>
ntpconfig
Currently configured NTP servers:
1. time.ironport.com
Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should originate.
- AUTH - Configure NTP authentication.
[]> new
Please enter the fully qualified hostname or IP address of your NTP server.
[]> ntp.example.com
Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi
Choose the operation you want to perform:
```

```

- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should
originate.
- AUTH - Configure NTP authentication.
[> sourceint

When initiating a connection to an NTP server, the outbound IP address
used is chosen automatically.
If you want to choose a specific outbound IP address, please select
its interface name now.
1. Auto
2. Management (172.19.0.11/24: elroy.run)
3. PrivateNet (172.19.1.11/24: elroy.run)
4. PublicNet (172.19.2.11/24: elroy.run)
[1]> 1
Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi
Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should originate.
- AUTH - Configure NTP authentication.
[> auth

Would you like to enable NTP authentication? [N]>yes
Currently configured NTP servers:
1. time.ironport.com
2. bitsy.mit.edi
Authentication is on
Choose the operation you want to perform:
- NEW - Add a server.
- DELETE - Remove a server.
- SOURCEINT - Set the interface from whose IP address NTP queries should
originate.
- AUTH - Configure NTP authentication.

mail3.example.com> commit
Please enter some comments describing your changes:
[> Added new NTP server
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

portalregistrationconfig

Cisco Spam Submission Tracking Portal は、電子メール管理者が組織からのスパムの報告を追跡し、間違って分類された新規メッセージをシスコに報告できる、Web ベースのツールです。このポータルでは、使用するすべてのアプライアンスが共通登録 ID を持つ必要があります。

登録 ID を設定するには、CLI で **portalregistrationconfig** コマンドを使用します。アプライアンスがクラスタの一部でない場合、使用するすべてのアプライアンスに共通の登録 ID を設定する必要があります。

ポータルの詳細については、ユーザ ガイドまたはオンライン ヘルプのアンチスパムの章を参照してください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> portalregistrationconfig

Choose the operation you want to perform:

- REGISTRATION_ID - Set up the Registration ID.
  []> registration_id
  Enter the new value of the Registration ID.
  []> registrationidexample1234
```

reboot

説明

アプライアンスを再起動します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> reboot
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

repengstatus

説明

レピュテーション エンジンのバージョン情報を要求します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail.example.com> repengstatus
Component                Last Update                Version
Reputation Engine        28 Jan 2014 23:47 (GMT +00:00) 1
Reputation Engine Tools  28 Jan 2014 23:47 (GMT +00:00) 1
```

resume

説明

受信と配信を再開します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> resume
Receiving resumed for Listener 1.
Mail delivery resumed.
Mail delivery for individually suspended domains must be resumed individually.
```

resumedel

説明

配信を再開します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail.example.com> resumedel
Currently suspended domains:
1. domain1.com
2. domain2.com
3. domain3.com
Enter one or more domains [comma-separated] to which you want to resume delivery.
[ALL]> domain1.com, domain2.com
Mail delivery resumed.
```

resumelister

説明

リスナーでの受信を再開します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> resumelister
Choose the listener(s) you wish to resume.
Separate multiple entries with commas.
1. All
2. InboundMail
3. OutboundMail
[1]> 1
Receiving resumed.
mail3.example.com>
```

revert

説明

以前のリリースに戻します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> 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 IronPort Spam Quarantine message and end-user safelist/blocklist data
Only the network settings will be preserved.
Before running this command, be sure you have:
- saved the configuration file of this appliance (with passphrases unmasked)
- exported the IronPort 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.
    Available versions
    =====
    1. 9.1.0-019
Please select an AsyncOS version [1]:
Do you want to continue? [N]>
```

settime

説明

settime コマンドでは、NTP サーバを使用していない場合に時刻を手動で設定できます。このコマンドを実行すると、NTP を停止して手動でシステム クロックを設定するかどうか尋ねられます。時刻は **MM/DD/YYYY HH:MM:SS** の形式で入力します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> settime
WARNING: Changes to system time will take place immediately
and do not require the user to run the commit command.
Current time 09/23/2001 21:03:53.
This machine is currently running NTP.
In order to manually set the time, NTP must be disabled.
Do you want to stop NTP and manually set the time? [N]> Y
Please enter the time in MM/DD/YYYY HH:MM:SS format.
[]> 09/23/2001 21:03:53
Time set to 09/23/2001 21:03:53.
```


settz

説明

ローカル タイム ゾーンを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> settz
Current time zone: Etc/GMT
Current time zone version: 2010.02.0
Choose the operation you want to perform:
- SETUP - Set the local time zone.
[]> setup
Please choose your continent:
1. Africa
2. America
[ ... ]
11. GMT Offset
[2]> 2
Please choose your country:
1. Anguilla
[ ... ]
45. United States
46. Uruguay
47. Venezuela
48. Virgin Islands (British)
49. Virgin Islands (U.S.)
[45]> 45
Please choose your timezone:
1. Alaska Time (Anchorage)
2. Alaska Time - Alaska panhandle (Juneau)
[ ... ]
21. Pacific Time (Los_Angeles)
[21]> 21
Current time zone: America/Los_Angeles
Choose the operation you want to perform:
- SETUP - Set the local time zone.
[]>
```

shutdown

説明

システムをシャットダウンして電源を切ります。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail.example.com> shutdown
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System shutting down. Please wait while the queue is being closed...
Closing CLI connection.
The system will power off automatically.
Connection to mail.example.com closed.
```

smaconfig

- [説明 \(98 ページ\)](#)
- [使用法 \(98 ページ\)](#)
- [例 \(98 ページ\)](#)

説明

smaconfig コマンドを使用すると、SMA 接続パラメータとキーの追加、削除、または表示を行うことができます。

使用法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

例

次の例で、smaconfig コマンドを使用すると、コンテンツ セキュリティ管理アプライアンス（SMA）に E メールセキュリティアプライアンスを事前共有キーを使用して追加し、SMA 接続の詳細（ホスト名とユーザ キー）を表示できます。

```
mail.example.com> smaconfig
Choose the operation you want to perform:
- ADD - Add a new SMA Connection Parameter and Key.
[]> add

Enter the hostname of the system that you want to add.
[]> m380q03.ibqa
```

```
[>] print
1. Hostname: m380q03.lbqa Keys: SSH2:dsl0.76.71.107 ssh-dss
#####
j24inBqBlisDPrs9ZwGfZKw0d0rQVnE1TpwWBg9gP202dWf5tA92BRvYAFm//SbmJyXSS6TJMPC5PB5SySSSgPW42CZWNg
j98HRGjHnM3GPGenK4VF43SLGiwVEXCSDF9smLtLaMRBLR6Qcz/Tbn9UMLz48KS2L7N3hCjyRHXDAgAtJCPE5Mucl5Uw0BrFzhG=
Choose the operation you want to perform:
- ADD - Add a new SMA Connection Parameter and Key.
- DELETE - Remove an existing SMA Connection Parameter and Key.
- PRINT - Display all SMA Parameters and Keys.
[>]
```

SSH サーバおよびユーザ キー設定を設定します。

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せん。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
```

```

- USERKEY - Edit SSH User Key settings
[]> sshd
ssh server config settings:
Public Key Authentication Algorithms:
    rsa1
    ssh-dss
    ssh-rsa
Cipher Algorithms:
    aes128-ctr
    aes192-ctr
    aes256-ctr
    arcfour256
    arcfour128
    aes128-cbc
    3des-cbc
    blowfish-cbc
    cast128-cbc
    aes192-cbc
    aes256-cbc
    arcfour
    rijndael-cbc@lysator.liu.se
MAC Methods:
    hmac-md5
    hmac-sha1
    umac-64@openssh.com
    hmac-ripemd160
    hmac-ripemd160@openssh.com
    hmac-sha1-96
    hmac-md5-96
Minimum Server Key Size:
    1024
KEX Algorithms:
    diffie-hellman-group-exchange-sha256
    diffie-hellman-group-exchange-sha1
    diffie-hellman-group14-sha1
    diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup
Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,
rijndael-cbc@lysator.liu.se]>
Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96]>
Enter the Minimum Server Key Size do you want to use
[1024]>
Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1]>
ssh server config settings:
Public Key Authentication Algorithms:
    rsa1
    ssh-dss
    ssh-rsa
Cipher Algorithms:
    aes128-ctr
    aes192-ctr
    aes256-ctr
    arcfour256
    arcfour128
    aes128-cbc
    3des-cbc
    blowfish-cbc

```

```

cast128-cbc
aes192-cbc
aes256-cbc
arcfour
rijndael-cbc@lysator.liu.se
MAC Methods:
  hmac-md5
  hmac-sha1
  umac-64@openssh.com
  hmac-ripemd160
  hmac-ripemd160@openssh.com
  hmac-sha1-96
  hmac-md5-96
Minimum Server Key Size:
  1024
KEX Algorithms:
  diffie-hellman-group-exchange-sha256
  diffie-hellman-group-exchange-sha1
  diffie-hellman-group14-sha1
  diffie-hellman-group1-sha1
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>

```

例：管理者アカウントの新しい公開キーのインストール

次の例では、管理者アカウントの新規公開キーをインストールします。

```

mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>

```

例：永続的なブラックリストまたはホワイトリストとして IP アドレスを分類

アプライアンスまたは `ipblockd` サービスが再起動されても、永続的なブラックリストまたはホワイトリストとして分類された IP アドレスは保持されます。



(注) AsyncOS 11.0.2 以降でのみ、IP アドレスを永続的なブラックリストまたはホワイトリストとして分類できます。

次の例は、IP アドレスを永続的なホワイトリストとして分類する方法を示しています。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[]> access control

Choose the operation you want to perform:
- WHITELIST - Manage the persistent whitelist
- BLACKLIST - Manage the persistent blacklist
[]> whitelist

Choose the operation you want to perform:
- ADD - Add address(es)
- REMOVE - Remove address(es)
- PRINT - Print addresses
[]> add

Enter an IP address or a comma-separated list of addresses.
Addresses already in the Whitelist will be ignored.
[]> 10.8.85.77
```

The addresses were successfully added to the Whitelist

次の例は、IP アドレスを永続的なブラックリストとして分類する方法を示しています。

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[]> access control

Choose the operation you want to perform:
- WHITELIST - Manage the persistent whitelist
- BLACKLIST - Manage the persistent blacklist
[]> blacklist

Choose the operation you want to perform:
- ADD - Add address(es)
- REMOVE - Remove address(es)
- PRINT - Print addresses
[]> add

Enter an IP address or a comma-separated list of addresses.
Addresses already in the Whitelist will be ignored.
[]> 10.8.85.77
```

The addresses were successfully added to the blacklist

status

説明

システム ステータスを表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> status

Status as of:                Thu Oct 21 14:33:27 2004 PDT
Up since:                    Wed Oct 20 15:47:58 2004 PDT (22h 45m 29s)
Last counter reset:         Never
System status:              Online
Oldest Message:             4 weeks 46 mins 53 secs
Feature - McAfee:           161 days
[....]
Feature - Outbreak Filters:  161 days

Counters:
  Receiving
    Messages Received        62,049,822      290,920      62,049,822
    Recipients Received      62,049,823      290,920      62,049,823
  Rejection
    Rejected Recipients      3,949,663       11,921       3,949,663
    Dropped Messages         11,606,037        219       11,606,037
  Queue
    Soft Bounced Events     2,334,552       13,598       2,334,552
  Completion
    Completed Recipients     50,441,741     332,625     50,441,741
  Current IDs
    Message ID (MID)                                99524480
    Injection Conn. ID (ICID)                        51180368
    Delivery Conn. ID (DCID)                        17550674

Gauges:
  Connections
    Current Inbound Conn.      0
    Current Outbound Conn.    14
  Queue
    Active Recipients          1
    Messages In Work Queue     0
    Kilobytes Used             92
    Kilobytes Free             8,388,516
  Quarantine
    Messages In Quarantine
      Policy, Virus and Outbreak 0
    Kilobytes In Quarantine
      Policy, Virus and Outbreak 0
```

supportrequest

説明

シスコのカスタマーサポートにメッセージを送信します。このコマンドを使用するには、アプライアンスがインターネットに電子メールを送信する必要があります。トラブルチケットが

自動的に作成されます。また、サポート要求を既存のトラブルチケットに関連付けることもできます。

アプライアンスからシスコ テクニカル サポートに直接アクセスするには、Cisco.com ユーザ ID がこのアプライアンスのサービス契約に関連付けられている必要があります。Cisco.com プロファイルに現在関連付けられているサービス契約の一覧を参照するには、Cisco.com Profile Manager (<https://sso.cisco.com/autho/forms/CDClogin.html>) にアクセスしてください。Cisco.com のユーザ ID がない場合は、登録して ID を取得してください。オンライン ヘルプのアカウントの登録に関する情報か、お使いのリリースのユーザガイドを参照してください。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカル ファイル システムにアクセスする必要があります。

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せん。

例

次に、既存のサポート チケットに関連しないサポート要求の例を示します。

```
mail.example.com> supportrequest
Please Note:
If you have an urgent issue, please call one of our worldwide Support Centers
(www.cisco.com/support). Use this command to open a technical support request
for issues that are not urgent, such as:
- Request for information.
- Problem for which you have a work-around, but would like an alternative
solution.
Do you want to send the support request to supportrequest@mail.qa?
[Y]>
Do you want to send the support request to additional recipient(s)?
[N]>
Is this support request associated with an existing support ticket?
[N]>
Please select a technology related to this support request:
1. Security - Email and Web
2. Security - Management
[1]> 1
Please select a subtechnology related to this support request:
1. Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - Misclassified
Messages
2. Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - SBRS
3. Cisco Email Security Appliance (C1x0,C3x0, C6x0, X10x0) - Other
4. Email Security Appliance - Virtual
[1]> 3
Please select the problem category:
1. Upgrade
2. Operate
3. Configure
4. Install
[1]> 3
Please select a problem sub-category:
1. Error Messages, Logs, Debugs
```



```

2. Software Failure
3. Interoperability
4. Configuration Assistance
5. Install, Uninstall or Upgrade
6. Hardware Failure
7. Licensing
8. Data Corruption
9. Software Selection/Download Assistance
10. Passphrase Recovery
[1]> 5
Please enter a subject line for this support request:
[]> <Subject line for support request>
Please enter a description of your issue, providing as much detail as possible
to aid in diagnosis:
[]> <Description of issue>
It is important to associate all your service contracts with your Cisco.com profile (CCO
ID) in order for you to receive complete
access to support and services from Cisco. Please follow the URLs below to associate
your contract coverage on your Cisco.com profile.
If you do not have a CCO ID, please follow
the URL below to create a CCO ID.
How to create a CCO ID:
https://tools.cisco.com/RPF/register/register.do
How to associate your CCO ID with contract:
https://tools.cisco.com/RPFA/profile/profile_management.do
Frequently Asked Question:
http://www.cisco.com/web/ordering/cs_info/faqs/index.html
Select the CCoid
1. New CCoid
[1]>
Please enter the CCoid of the contact person :
[]> your name
The CCO ID may contain alphabets, numbers and '@', '.', '-' and '_' symbols.
Please enter the CCoid of the contact person :
[]> me@example.com
Please enter the name of the contact person :
[]> yourname
Please enter your email address:
[]> me@example.com
Please enter the contract ID:
[]> 1234
Please enter any additional contact information (e.g. phone number):
[]>
Please wait while configuration information is generated...
Do you want to print the support request to the screen?
[N]>

```

supportrequeststatus

説明

Cisco TAC のサポートを要求するための、サポート要求キーワードバージョン情報を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> supportrequeststatus
Component          Version      Last Updated
Support Request    1.0         Never updated
```

supportrequestupdate

説明

Cisco TAC のサポートを要求するための、サポート要求キーワードの手動アップデートを要求します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> supportrequestupdate
Requesting update of Support Request Keywords.
```

suspend

説明

受信と配信を中断します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> suspend
```

```
Enter the number of seconds to wait before abruptly closing connections.
[30]> 45
Waiting for listeners to exit...
Receiving suspended for Listener 1.
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
mail3.example.com>
```

suspenddel

説明

配信を中断します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail.example.com> suspenddel
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Enter one or more domains [comma-separated] to which you want to suspend delivery.
[ALL]> domain1.com, domain2.com, domain3.com
Waiting for outgoing deliveries to finish...
Mail delivery suspended.
```

suspendlistener

説明

受信を中断します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> suspendlistener
Choose the listener(s) you wish to suspend.
Separate multiple entries with commas.
1. All
```

```

2. InboundMail
3. OutboundMail
[1]> 1
Enter the number of seconds to wait before abruptly closing connections.
[30]>
Waiting for listeners to exit...
Receiving suspended.
mail3.example.com>

```

tcpservices

説明

プロセスによって開かれているファイルに関する情報を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```

mail.cisco.com> tcpservices
System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw          - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon
Feature Processes
  euq_webui    - GUI for ISQ
  gui          - GUI process
  hermes       - MGA mail server
  postgres    - Process for storing and querying quarantine data
  splunkd      - Processes for storing and querying Email Tracking data
COMMAND      USER      TYPE  NODE  NAME
interface    root      IPv4  TCP   127.0.0.1:53
postgres     pgsql     IPv4  TCP   127.0.0.1:5432
qabackdoo    root      IPv4  TCP   *:8123
ftpd.main    root      IPv4  TCP   10.1.1.0:21
euq_webui    root      IPv4  TCP   10.1.1.0:83
euq_webui    root      IPv6  TCP   [2001:db8::]:83
gui          root      IPv4  TCP   172.29.181.70:80
gui          root      IPv4  TCP   10.1.1.0:80
gui          root      IPv6  TCP   [2001:db8::]:80
gui          root      IPv4  TCP   172.29.181.70:443
gui          root      IPv4  TCP   10.1.1.0:443
gui          root      IPv6  TCP   [2001:db8::]:443
ginetd       root      IPv4  TCP   172.29.181.70:22
ginetd       root      IPv4  TCP   10.1.1.0:22
ginetd       root      IPv6  TCP   [2001:db8::]:22

```

```
ginetd      root      IPv4 TCP    10.1.1.0:2222
ginetd      root      IPv6 TCP    [2001:db8::]:2222
hermes      root      IPv4 TCP    172.29.181.70:25
splunkd     root      IPv4 TCP    127.0.0.1:8089
splunkd     root      IPv4 TCP    127.0.0.1:9997
api_serve   root      IPv4 TCP    10.1.1.0:6080
api_serve   root      IPv6 TCP    [2001:db8::]:6080
api_serve   root      IPv4 TCP    10.1.1.0:6443
api_serve   root      IPv6 TCP    [2001:db8::]:6443
java        root      IPv6 TCP    [::127.0.0.1]:9999
```

techsupport

説明

Cisco TAC がシステムにアクセスできるようにします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> techsupport
Service Access currently disabled.
Serial Number: XXXXXXXXXXXX-XXXXXXX
Choose the operation you want to perform:
- SSHACCESS - Allow a Cisco IronPort Customer Support representative to remotely access
  your system, without establishing a tunnel.
- TUNNEL - Allow a Cisco IronPort Customer Support representative to remotely access
  your system, and establish a secure tunnel
  for communication.
- STATUS - Display the current techsupport status.
[> sshaccess
A random seed string is required for this operation
1. Generate a random string to initialize secure communication (recommended)
2. Enter a random string
[1]> 1
Are you sure you want to enable service access? [N]> y
Service access has been ENABLED. Please provide the string:
QT22-JQZF-YAQL-TL8L-8@2L-95
to your Cisco IronPort Customer Support representative.
Service Access currently ENABLED (0 current service logins).
Tunnel option is not active.
Serial Number: XXXXXXXXXXXX-XXXXXXX
Choose the operation you want to perform:
- DISABLE - Prevent customer service representatives from remotely accessing your system.
- STATUS - Display the current techsupport status.
[>
```

tlsverify

説明

発信 TLS 接続を必要に応じて確立し、宛先ドメインに関する TLS 接続の問題をデバッグします。接続を確立するには、検証するドメインと宛先ホストを指定します。AsyncOS は、必要な（検証）TLS 設定に基づいて TLS 接続を確認します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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。

バッチ形式

tlsverify コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行し、特定のホスト名との TLS 接続をチェックできます。

```
tlsverify <domain> <hostname>[:<port>]
```

例

```
mail3.example.com> tlsverify
Enter the TLS domain to verify against:
[]> example.com
Enter the destination host to connect to. Append the port (example.com:26) if you are
not connecting on port 25:
[example.com]> mxe.example.com:25
Connecting to 1.1.1.1 on port 25.
Connected to 1.1.1.1 from interface 10.10.10.10.
Checking TLS connection.
TLS connection established: protocol TLSv1, cipher RC4-SHA.
Verifying peer certificate.
Verifying certificate common name mxe.example.com.
TLS certificate match mxe.example.com
TLS certificate verified.
TLS connection to 1.1.1.1 succeeded.
TLS successfully connected to mxe.example.com.
TLS verification completed.
```

trace

説明

システムを通過するメッセージのフローを追跡します。

使用方法

確定: このコマンドに「commit」は必要ありません。

クラスタ管理: このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> trace
Enter the source IP
[]> 192.168.1.1
Enter the fully qualified domain name of the source IP
[]> example.com
Select the listener to trace behavior on:
1. InboundMail
2. OutboundMail
[]> 1
Fetching default SenderBase values...
Enter the SenderBase Org ID of the source IP. The actual ID is N/A.
[N/A]>
Enter the SenderBase Reputation Score of the source IP. The actual score is N/A.
[N/A]>
Enter the Envelope Sender address:
[]> pretend.sender@example.net
Enter the Envelope Recipient addresses. Separate multiple addresses by commas.
[]> admin@example.com
Load message from disk? [Y]> n
Enter or paste the message body here. Enter '.' on a blank line to end.
Subject: Hello
This is a test message.
.
HAT matched on unnamed sender group, host ALL
- Applying $ACCEPTED policy (ACCEPT behavior).
- Maximum Message Size: 100M (Default)
- Maximum Number Of Connections From A Single IP: 1000 (Default)
- Maximum Number Of Messages Per Connection: 1,000 (Default)
- Maximum Number Of Recipients Per Message: 1,000 (Default)
- Maximum Recipients Per Hour: 100 (Default)
- Use SenderBase For Flow Control: Yes (Default)
- Spam Detection Enabled: Yes (Default)
- Virus Detection Enabled: Yes (Default)
- Allow TLS Connections: No (Default)
Processing MAIL FROM:
- Default Domain Processing: No Change
Processing Recipient List:
Processing admin@ironport.com
- Default Domain Processing: No Change
- Domain Map: No Change
- RAT matched on admin@ironport.com, behavior = ACCEPT
- Alias expansion: No Change
Message Processing:
- No Virtual Gateway(tm) Assigned
- No Bounce Profile Assigned
Domain Masquerading/LDAP Processing:
- No Changes.
Processing filter 'always_deliver':
Evaluating Rule: rcpt-to == "@mail.qa"
Result = False
Evaluating Rule: rcpt-to == "ironport.com"
```

```

Result = True
Evaluating Rule:  OR
Result = True
Executing Action:  deliver()
Footer Stamping:
- Not Performed
Inbound Recipient Policy Processing: (matched on Management Upgrade policy)
Message going to:  admin@ironport.com
AntiSpam Evaluation:
- Not Spam
AntiVirus Evaluation:
- Message Clean.
- Elapsed Time = '0.000 sec'
Outbreak Filter Evaluation:
- No threat detected
Message Enqueued for Delivery
Would you like to see the resulting message? [Y]> y
Final text for messages matched on policy Management Upgrade
Final Envelope Sender:  pretend.sender@example.doma
Final Recipients:
- admin@ironport.com
Final Message Content:
Received: from remotesite.example.com (HELO TEST) (1.2.3.4)
by stacy.qa with TEST; 19 Oct 2004 00:54:48 -0700
Message-Id: <3i93q9$@Management>
X-IronPort-AV: i="3.86,81,1096873200";
d="scan'208"; a="0:sNHT0"
Subject: hello
This is a test message.
Run through another debug session? [N]>

```



(注) **trace** を使用するときには、貼り付けられたメッセージのヘッダーと本文の両方を CLI に含める必要があります。

trackingconfig

説明

トラッキング システムを設定します。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```

mail.example.com> trackingconfig
Message Tracking service status: Message Tracking is enabled.
Choose the operation you want to perform:

```



```
- SETUP - Enable Message Tracking for this appliance.
[]> setup
Would you like to use the Message Tracking Service? [Y]>
Do you want to use Centralized Message Tracking for this appliance? [N]>
Would you like to track rejected connections? [N]>
Message Tracking service status: Local Message Tracking is enabled.
Rejected connections are currently not being tracked.
Choose the operation you want to perform:
- SETUP - Enable Message Tracking for this appliance.
[]>
```

tzupdate

説明

タイムゾーンルールを更新します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。

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。

バッチ形式

tzupdate コマンドのバッチ形式を使用すると、変更が検出されない場合でも、すべてのタイムゾーンルールが強制的に更新されます。

```
tzupdate [force]
```

例

```
mail.example.com> tzupdate
Requesting update of Timezone Rules
```

updateconfig

説明

システム更新パラメータを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

- アップデータ サーバから更新プログラムをダウンロードするようにアプライアンスを設定 (114 ページ)
- アップデータ サーバの証明書の有効性を検証するようにアプライアンスを設定 (116 ページ)
- プロキシ サーバとの通信を信頼するようにアプライアンスを設定 (117 ページ)

アップデータ サーバから更新プログラムをダウンロードするようにアプライアンスを設定

次の例では、`updateconfig` コマンドを使用して、アプライアンスがシスコサーバからアップデータ イメージをダウンロードし、ローカル サーバから使用可能な AsyncOS アップグレードのリストをダウンロードするように設定します。

```
mail.example.com> updateconfig
Service (images): Update URL:
-----
Feature Key updates http://downloads.ironport.com/asyncos
Timezone rules Cisco IronPort Servers
Enrollment Client Updates Cisco IronPort Servers
Support Request updates Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
Service (list): Update URL:
-----
Timezone rules Cisco IronPort Servers
Enrollment Client Updates Cisco IronPort Servers
Support Request updates Cisco IronPort Servers
Service (list): Update URL:
-----
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
Update interval: 5m
Alert Interval for Disabled Automatic Engine Updates: 30d
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
[1]> setup
For the following services, please select where the system will download updates from:
Service (images): Update URL:
-----
Feature Key updates http://downloads.ironport.com/asyncos
1. Use Cisco IronPort update servers (http://downloads.ironport.com)
2. Use own server
[1]>
For the following services, please select where the system will download updates from
(images):
Service (images): Update URL:
-----
Timezone rules Cisco IronPort Servers
Enrollment Client Updates Cisco IronPort Servers
Support Request updates Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own server
[1]>
For the following services, please select where the system will download updates from
```

```
(images):
Service (images):                                Update URL:
-----
Cisco IronPort AsyncOS upgrades                  Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own server
[1]>
For the following services, please select where the system will download the list of
available
updates from:
Service (list):                                Update URL:
-----
Timezone rules                                  Cisco IronPort Servers
Enrollment Client Updates                      Cisco IronPort Servers
Support Request updates                        Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own update list
[1]>
For the following services, please select where the system will download the list of
available
updates from:
Service (list):                                Update URL:
-----
Cisco IronPort AsyncOS upgrades                  Cisco IronPort Servers
1. Use Cisco IronPort update servers
2. Use own update list
[1]>
Enter the time interval between checks for new:
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
Use a trailing 's' for seconds, 'm' for minutes or 'h' for hours. The minimum
valid update time is 30s or enter '0' to disable automatic updates (manual
updates will still be available for individual services).
[5m]>
When initiating a connection to the update server the originating IP interface
is chosen automatically. If you want to choose a specific interface, please
specify it now.
1. Auto
2. Management (10.76.69.149/24: vm30esa0086.ibqa)
[1]>
Do you want to set up a proxy server for HTTP updates for ALL of the following
services:
- Feature Key updates
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
- Cisco IronPort AsyncOS upgrades
[N]>
Do you want to set up an HTTPS proxy server for HTTPS updates for ALL of the following
services:
- Feature Key updates
- Timezone rules
- Enrollment Client Updates (used to fetch certificates for URL Filtering)
- Support Request updates
- Cisco IronPort AsyncOS upgrades
- SenderBase Network Participation sharing
[N]>
Service (images):                                Update URL:
-----
Feature Key updates                            http://downloads.ironport.com/asyncos
Timezone rules                                Cisco IronPort Servers
Enrollment Client Updates                    Cisco IronPort Servers
Support Request updates                      Cisco IronPort Servers
```

アップデータ サーバの証明書の有効性を検証するようにアプライアンスを設定

```

Cisco IronPort AsyncOS upgrades                               Cisco IronPort Servers
Service (list):                                              Update URL:
-----
Timezone rules                                              Cisco IronPort Servers
Enrollment Client Updates                                Cisco IronPort Servers
Support Request updates                                    Cisco IronPort Servers
Service (list):                                              Update URL:
-----
Cisco IronPort AsyncOS upgrades                               Cisco IronPort 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
[]>

```

アップデータ サーバの証明書の有効性を検証するようにアプライアンスを設定

このオプションを設定すると、アプライアンスがシスコのアップデータサーバと通信するたびに、アップデータサーバの証明書の有効性が確認されます。検証に失敗した場合は、更新プログラムはダウンロードされず、詳細がアップデータのログに記録されます。次に、このオプションを設定する例を示します。

```

mail.example.com> updateconfig
Service (images):                                              Update URL:
-----
Feature Key updates                                          http://downloads.ironport.com/asyncos
Timezone rules                                              Cisco IronPort Servers
Enrollment Client Updates                                Cisco IronPort Servers
Support Request updates                                    Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                            Cisco IronPort Servers
Service (list):                                              Update URL:
-----
Timezone rules                                              Cisco IronPort Servers
Enrollment Client Updates                                Cisco IronPort Servers
Support Request updates                                    Cisco IronPort Servers
Service (list):                                              Update URL:
-----
Cisco IronPort AsyncOS upgrades                               Cisco IronPort Servers
Update interval: 5m
Alert Interval for Disabled Automatic Engine Updates: 30d
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
[]> validate_certificates
Should server certificates from Cisco update servers be validated?
[Yes]>
Service (images):                                              Update URL:
-----
Feature Key updates                                          http://downloads.ironport.com/asyncos
Timezone rules                                              Cisco IronPort Servers
Enrollment Client Updates                                Cisco IronPort Servers
Support Request updates                                    Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades                            Cisco IronPort Servers
Service (list):                                              Update URL:
-----
Timezone rules                                              Cisco IronPort Servers

```

```

Enrollment Client Updates                                Cisco IronPort Servers
Support Request updates                                Cisco IronPort Servers
Service (list):                                         Update URL:
-----
Cisco IronPort AsyncOS upgrades                        Cisco IronPort 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
[]>

```

プロキシサーバ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証明書をアプライアンスに追加できます。これにより、アプライアンスはプロキシサーバ通信を信頼します。次に、このオプションを設定する例を示します。

```

...
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.
[]> 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-----
MMIICiDCCAfGgAwIBAgIBATANBgqhkiG9w0BAQUFADCBgDELMAkGA1UEBhMCSU4x
DDAKBgNVBAGTA0tBUjENM.....
-----END CERTIFICATE-----
.
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.
[]>

```

updatenow

説明

すべてのシステム サービス コンポーネントの更新を要求します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。

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。

バッチ形式

updatenow コマンドのバッチ形式を使用すると、変更が検出されない場合でも、アプライアンス上のすべてのコンポーネントを更新できます。

```
updatenow [force]
```

例

```
mail3.example.com> updatenow
Success - All component updates requested
```

version

説明

システムのバージョン情報を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> version
Current Version
=====
Product: Cisco C100V Email Security Virtual Appliance
Model: C100V
Version: 9.1.0-019
Build Date: 2015-02-17
Install Date: 2015-02-19 05:17:56
Serial #: 421C73B18CFB05784A83-B03A99E71ED8
BIOS: 6.00
CPUs: 2 expected, 2 allocated
Memory: 6144 MB expected, 6144 MB allocated
RAID: NA
RAID Status: Unknown
RAID Type: NA
BMC: NA
```

wipedata

説明

ディスクのコア ファイルを消去し、最後のコアダンプ操作のステータスを確認するのに **wipedata** コマンドを使用します。



(注) データサイズに応じて、消去アクションは、時間がかかることがあり、操作が完了するまで、システム パフォーマンスに影響を与えることがあります。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail.example.com> wipedata
Wiping data may take a while and can affect system performance till it completes.
Choose the operation you want to perform:
- STATUS - Display status of last command run
- COREDUMP - Wipe core files on disk
[]> coredump
wipedata: In progress
mail.example.com> wipedata
Wiping data may take a while and can affect system performance till it completes.
Choose the operation you want to perform:
- STATUS - Display status of last command run
- COREDUMP - Wipe core files on disk
[]> status
Last wipedata status: Successful
```

upgrade

説明

upgrade CLI コマンドは、使用可能なアップグレードのリストを表示し、ユーザが指定したバージョンに AsyncOS システムをアップグレードします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> upgrade
Upgrades available:
1. AsyncOS (***DON'T TOUCH!**) 4.0.8 upgrade, 2005-05-09 Build 900
2. AsyncOS 4.0.8 upgrade, 2005-08-12 Build 030
.....
45. SenderBase Network Participation Patch
[45]>
Performing an upgrade will require a reboot of the system after the upgrade is applied.
Do you wish to proceed with the upgrade? [Y]> Y
```

コンテンツ スキャン

- [contentscannerstatus](#) (120 ページ)
- [contentscannerudpate](#) (120 ページ)

contentscannerstatus

コンテンツ スキャン エンジンのバージョン情報を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail.example.com> contentscannerstatus
Component          Version          Last Updated
Content Scanner Tools 11.2.1884.970097 Never updated
```

contentscannerudpate

コンテンツ スキャン エンジンの手動アップデートを要求します。「force」パラメータを使用すると、更新は変更が検出されなくても実行されます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログイン ホスト（ユーザがログインしたマシン）でのみ使用できます。

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せん。

例

```
mail.example.com> contentscannerupdate force
Requesting forced update for Content Scanner.
```

LDAP

ここでは、次の CLI コマンドについて説明します。

- [ldapconfig](#) (121 ページ)
- [ldapflush](#) (125 ページ)
- [ldaptest](#) (125 ページ)
- [sievechar](#) (126 ページ)

ldapconfig

説明

LDAP サーバを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例：新しい LDAP サーバ プロファイルの作成

次の例では、`ldapconfig` コマンドを使用して、アプライアンスのバインド先となる LDAP サーバを定義し、受信者受け入れ (`ldapaccept` サブコマンド)、ルーティング (`ldaprouting` サブコマンド)、マスカレード (`masquerade` サブコマンド)、スパム隔離のエンドユーザ認証 (`isqauth` サブコマンド)、およびスパム通知のエイリアス統合 (`isqalias` サブコマンド) のクエリーを設定します。

まず、「PublicLDAP」というニックネームを `mldapserver.example.com` LDAP サーバに与えます。クエリの送信先は、ポート 3268 (デフォルト値) です。example.com の検索ベースが定義され (`dc=example,dc=com`)、受信者受け入れ、メール再ルーティング、およびマスカレードのクエリーが定義されます。この例のクエリーは、期限切れのインターネット ドラフト *draft-lachman-laser-ldap-mail-routing-xx.txt* で定義された `inetLocalMailRecipient` 補助オブジェクトクラス (「Laser 仕様」) としても知られる) を使用する、OpenLDAP ディレクトリ設定に似ています。(このドラフトのバージョンは、OpenLDAP のソース ディストリビューションに含まれています)。この例では、メールの再ルーティングクエリーで照会される受信者に使用する代替メールホストが `mailForwardingAddress` であることに注意してください。クエリー名で

は、大文字と小文字が区別されます。正しい結果が返されるようにするには、正確に一致している必要があります。

```
mail3.example.com> ldapconfig
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]> new
Please create a name for this server configuration (Ex: "PublicLDAP"):
[]> PublicLDAP
Please enter the hostname:
[]> myldapserver.example.com
Use SSL to connect to the LDAP server? [N]> n
Select the authentication method to use for this server configuration:
1. Anonymous
2. Passphrase based
[1]> 2
Please enter the bind username:
[cn=Anonymous]>
Please enter the bind passphrase:
[]>
Connect to LDAP server to validate setting? [Y]
Connecting to the LDAP server, please wait...
Select the server type to use for this server configuration:
1. Active Directory
2. OpenLDAP
3. Unknown or Other
[3]> 1

Please enter the port number:
[3268]> 3268
Please enter the base:
[dc=example,dc=com]> dc=example,dc=com
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- TEST - Test the server configuration.
- LDAPACCEPT - Configure whether a recipient address should be accepted or
bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- CERTAUTH - Configure certificate authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> ldapaccept
Please create a name for this query:
[PublicLDAP.ldapaccept]> PublicLDAP.ldapaccept
Enter the LDAP query string:
[(proxyAddresses=smtp:{a})]> (proxyAddresses=smtp:{a})
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
```

```

Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> ldaprouting
Please create a name for this query:
[PublicLDAP.routing]> PublicLDAP.routing
Enter the LDAP query string:
[(mailLocalAddress={a})]> (mailLocalAddress={a})
The query requires one of the attributes below. Please make a selection.
  [1] Configure MAILROUTINGADDRESS only - Rewrite the Envelope Recipient (and
leave MAILHOST unconfigured)?
  [2] Configure MAILHOST only - Send the messages to an alternate mail host
(and leave MAILROUTINGADDRESS unconfigured)?
  [3] Configure both attributes
[]> 1
Enter the attribute which contains the full rfc822 email address for the
recipients.
[mailRoutingAddress]> mailRoutingAddress
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> masquerade
Please create a name for this query:
[PublicLDAP.masquerade]> PublicLDAP.masquerade
Enter the LDAP query string:
[(mailRoutingAddress={a})]> (mailRoutingAddress={a})
Enter the attribute which contains the externally visible full rfc822 email address.
[]> mailLocalAddress
Do you want the results of the returned attribute to replace the entire friendly portion
of the original recipient? [N]> n
Do you want to test this query? [Y]> n
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
MASQUERADE: PublicLDAP.masquerade
Choose the operation you want to perform:

```

例 : グローバル設定の指定

```

- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]> isqauth
Please create a name for this query:
[PublicLDAP.isqauth]> PublicLDAP.isqauth
Enter the LDAP query string:
[(sAMAccountName={u})]> (sAMAccountName={u})
Enter the list of email attributes.
[]> mail,proxyAddresses
Do you want to activate this query? [Y]> y
Do you want to test this query? [Y]> y
User identity to use in query:
[]> admin@example.com
Passphrase to use in query:
[]> passphrase
LDAP query test results:
LDAP Server: myldapserver.example.com
Query: PublicLDAP.isqauth
User: admin@example.com
Action: match positive
LDAP query test finished.
Name: PublicLDAP
Hostname: myldapserver.example.com Port 3268
Server Type: Active Directory
Authentication Type: passphrase
Base: dc=example,dc=com
LDAPACCEPT: PublicLDAP.ldapaccept
LDAPROUTING: PublicLDAP.routing
MASQUERADE: PublicLDAP.masquerade
ISQAUTH: PublicLDAP.isqauth [active]
Choose the operation you want to perform:
- SERVER - Change the server for the query.
- LDAPACCEPT - Configure whether a recipient address should be accepted or bounced/dropped.
- LDAPROUTING - Configure message routing.
- MASQUERADE - Configure domain masquerading.
- LDAPGROUP - Configure whether a sender or recipient is in a specified group.
- SMTPAUTH - Configure SMTP authentication.
- EXTERNALAUTH - Configure external authentication queries.
- ISQAUTH - Configure Spam Quarantine End-User Authentication Query.
- ISQALIAS - Configure Spam Quarantine Alias Consolidation Query.
[]>
Current LDAP server configurations:
1. PublicLDAP: (myldapserver.example.com:3268)
Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
- EDIT - Modify a server configuration.
- DELETE - Remove a server configuration.
[]>

```

例 : グローバル設定の指定

この例では、TLS 接続の証明書を含む LDAP グローバル設定を指定します。

```
mail3.example.com> ldapconfig
```

```
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]> setup
Choose the IP interface for LDAP traffic.
1. Auto
2. Management (10.92.145.175/24: esx16-esa01.qa)
[1]> 1
LDAP will determine the interface automatically.
Should group queries that fail to complete be silently treated as having
negative results? [Y]>
Validate LDAP server certificate? [Y]>
The "Demo" certificate is currently configured. You may use "Demo", but this will not
be secure.
1. partner.com
2. Demo
Please choose the certificate to apply:
[1]> 1
No LDAP server configurations.
Choose the operation you want to perform:
- NEW - Create a new server configuration.
- SETUP - Configure LDAP options.
[]>
```

ldapflush

説明

キャッシュされている LDAP の結果をフラッシュします。

使用方法

確定: このコマンドに「commit」は必要ありません。

クラスタ管理: このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> ldapflush
Are you sure you want to flush any cached LDAP results? [N]> y
Flushing cache
mail3.example.com>
```

ldaptest

説明

1 つの LDAP クエリー テストを実行します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

この例では、`ldaptest` コマンドを使用して、設定済みの LDAP サーバ設定の受信者受け入れクエリーだけをテストします。受信者アドレス「`admin@example.com`」はこのテストに合格しますが、受信者アドレス「`bogus@example.com`」は不合格になります。

```
mail3.example.com> ldaptest
Select which LDAP query to test:
1. PublicLDAP.ldapaccept
[1]> 1
Address to use in query:
[]> admin@example.com
LDAP query test results:
    Query: PublicLDAP.ldapaccept
    Argument: admin@example.com
    Action: pass
LDAP query test finished.
mail3.example.com> ldaptest
Select which LDAP query to test:
1. PublicLDAP.ldapaccept
[1]> 1
Address to use in query:
[]> bogus@example.com
LDAP query test results:
    Query: PublicLDAP.ldapaccept
    Argument: bogus@example.com
    Action: drop or bounce (depending on listener settings)
    Reason: no matching LDAP record was found
LDAP query test finished.
mail3.example.com>
```

sievechar

説明

RFC 3598に規定されている Sieve 電子メールフィルタリングに使用する文字を設定またはディセーブルにします。Sieve 文字は LDAP 承認クエリーと LDAP 再ルーティング クエリーでのみ認識されることに注意してください。システムの他の部分は、完全な電子メールアドレスを操作対象とします。

使用できる文字は、`-_=/^#` です。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

この例では、`sievechar` コマンドを使用して、+を承認クエリーおよびLDAP再ルーティングクエリーで認識される Sieve 文字として定義します。

```
mail3.example.com> sievechar
Sieve Email Filtering is currently disabled.
Choose the operation you want to perform:
- SETUP - Set the separator character.
[]> setup
Enter the Sieve Filter Character, or a space to disable Sieve Filtering.
[]> +
Sieve Email Filter is enabled, using the '+' character as separator.
This applies only to LDAP Accept and LDAP Reroute Queries.
Choose the operation you want to perform:
- SETUP - Set the separator character.
[]>
```

メール配信の設定/モニタリング

ここでは、次の CLI コマンドについて説明します。

- [addresslistconfig](#) (128 ページ)
- [aliasconfig](#) (129 ページ)
- [archivemessage](#) (132 ページ)
- [altsrchoost](#) (132 ページ)
- [bounceconfig](#) (134 ページ)
- [bouncerecipients](#) (137 ページ)
- [bvconfig](#) (138 ページ)
- [deleterecipients](#) (139 ページ)
- [deliveryconfig](#) (140 ページ)
- [delivernow](#) (141 ページ)
- [destconfig](#) (141 ページ)
- [hostrate](#) (149 ページ)
- [hoststatus](#) (149 ページ)
- [imageanalysisconfig](#) (150 ページ)
- [oldmessage](#) (151 ページ)
- [rate](#) (152 ページ)
- [redirectrecipients](#) (153 ページ)
- [resetcounters](#) (154 ページ)
- [removemessage](#) (154 ページ)
- [showmessage](#) (155 ページ)

- [showrecipients](#) (155 ページ)
- [status](#) (102 ページ)
- [tophosts](#) (157 ページ)
- [topin](#) (158 ページ)
- [unsubscribe](#) (159 ページ)
- [workqueue](#) (160 ページ)

addresslistconfig

説明

アドレス リストを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式

addresslistconfig コマンドのバッチ形式を使用して、新しいアドレス リストの作成、既存のアドレス リストの編集、アドレス リストの一覧出力、アドレス リストの削除、アドレス リストの中で競合しているアドレスの検出が可能です。

- 新しいアドレス リストの追加：

```
addresslistconfig new <name> --descr=<description> --addresses=<address1,address2,...>
```

- 既存のアドレス リストの編集：

```
addresslistconfig edit <name> --name=<new-name> --descr=<description>
--addresses=<address1,address2,...>
```

- アドレス リストの削除：

```
addresslistconfig delete <name>
```

- アドレス リストの一覧出力：

```
addresslistconfig print <name>
```

- アドレス リストの中で競合しているアドレスの検出：

```
addresslistconfig conflicts <name>
```


例

```
mail.example.com> addresslistconfig
No address lists configured.
Choose the operation you want to perform:
- NEW - Create a new address list.
[]> new
Enter a name for the address list:
> add-list1
Enter a description for the address list:
> This is a sample address list.
Do you want to enter only full Email Addresses? [N]> Y
Enter a comma separated list of addresses:
(e.g.: user@example.com)
> user1@example.com, user2@example.com
Address list "add-list1" added.
Choose the operation you want to perform:
- NEW - Create a new address list.
- EDIT - Modify an address list.
- DELETE - Remove an address list.
- PRINT - Display the contents of an address list.
- CONFLICTS - Find conflicting entries within an address list.
[]>
```

aliasconfig

説明

電子メールエイリアスを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式

aliasconfig のバッチ形式を使用すると、新しいエイリアス テーブルの追加、既存のエイリアス テーブルの編集、電子メールエイリアスのリストの出力、エイリアス テーブルのインポート/エクスポートを実行できます。バッチ コマンドとして実行するには、aliasconfig コマンドを次の形式で入力し、以下の変数を指定します。

- 新しい電子メールエイリアスの追加

```
aliasconfig new <domain> <alias> [email_address1] [email_address2] ...
```



(注) 存在しないドメインに対して「aliasconfig new」コマンドを実行すると、そのドメインが作成されます。

- 既存の電子メールエイリアスの編集

```
aliasconfig edit <domain> <alias> <email_address1> [email_address2] ...
```

- 電子メールエイリアスの表示

```
aliasconfig print
```

- ローカルエイリアスリストのインポート

```
aliasconfig import <filename>
```

- アプライアンスのエイリアスリストのエクスポート

```
aliasconfig export <filename>
```

例

```
mail3.example.com> aliasconfig
Enter address(es) for "customercare".
Separate multiple addresses with commas.
[>] bob@example.com, frank@example.com, sally@example.com
Adding alias customercare: bob@example.com,frank@example.com,sally@example.com
Do you want to add another alias? [N]> n
There are currently 1 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[>] new
How do you want your aliases to apply?
1. Globally
2. Add a new domain context
3. example.com
[1]> 1
Enter the alias(es) to match on.
Separate multiple aliases with commas.
Allowed aliases:
- "user@domain" - This email address.
```

```

- "user" - This user for any domain
- "@domain" - All users in this domain.
- "@.partialdomain" - All users in this domain, or any of its sub domains.
[]> admin
Enter address(es) for "admin".
Separate multiple addresses with commas.
[]> administrator@example.com
Adding alias admin: administrator@example.com
Do you want to add another alias? [N]> n
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]> print
admin: administrator@example.com
[ example.com ]
customercare: bob@example.com, frank@example.com, sally@example.com
There are currently 2 mappings defined.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- PRINT - Display the table.
- IMPORT - Import aliases from a file.
- EXPORT - Export table to a file.
- CLEAR - Clear the table.
[]>

```

表 6:エイリアス設定用の引数

引数	説明
<domain>	エイリアスを適用するドメインコンテキスト。「Global」はグローバル ドメイン コンテキストを指定します。
<alias>	<p>設定するエイリアスの名前。</p> <p>グローバル ドメイン コンテキストで使えるエイリアスは次のとおりです。</p> <p>"user@domain" : この E メール アドレス。</p> <p>"user" : 任意のドメインのこのユーザ</p> <p>'@domain' : このドメインのすべてのユーザ。</p> <p>'@.partialdomain' : このドメインまたはその任意のサブドメインのすべてのユーザ。</p> <p>特定のドメイン コンテキストで使えるエイリアスは次のとおりです。</p> <p>'User' : このドメイン コンテキストのこのユーザ</p> <p>'User@domain' : この E メール アドレス</p>

引数	説明
<email_address>	エイリアスをマッピングする電子メール アドレス。1 つのエイリアスを複数の電子メール アドレスにマッピングできます。
<filename>	エイリアス テーブルのインポート/エクスポートに使用するファイル名。

archivemessage

説明

キュー内の古いメッセージをアーカイブします。

使用方法

確定：このコマンドに **commit** は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

次の例では、古いメッセージをアーカイブします。

```
mail3.example.com>
archivemessage
Enter the MID to archive.
[0]> 47
```

```
MID 47 has been saved in file oldmessage_47.mbox in the configuration
```

altsrhost

説明

Virtual Gateway™ のマッピングを設定します。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例では、**altsrchost** テーブルが出力されて、既存のマッピングがないことが示されます。その後、2つのエントリが作成されます。

- グループウェアサーバホスト **@exchange.example.com** からのメールは、**PublicNet** インターフェイスにマッピングされます。
- 送信者 IP アドレス **192.168.35.35** からのメールは、**AnotherPublicNet** インターフェイスにマッピングされます。

最後に、確認のために **altsrchost** マッピングが出力されて、変更が確定されます。

```
mail3.example.com> altsrchost
There are currently no mappings configured.
Choose the operation you want to perform:
- NEW - Create a new mapping.
- IMPORT - Load new mappings from a file.
[]> new
Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping.
Partial addresses such as "@example.com" or "user@" are allowed.
[]> @exchange.example.com
Which interface do you want to send messages for @exchange.example.com from?
1. AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[]> 4
Mapping for @exchange.example.com on interface PublicNet created.
Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> new
Enter the Envelope From address or client IP address for which you want to set up a
Virtual Gateway mapping.
Partial addresses such as "@example.com" or "user@" are allowed.
[]> 192.168.35.35
Which interface do you want to send messages for 192.168.35.35 from?
1. AnotherPublicNet (192.168.2.2/24: mail4.example.com)
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail4.example.com)
[]> 1
Mapping for 192.168.35.35 on interface AnotherPublicNet created.
Choose the operation you want to perform:
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]> print
1. 192.168.35.35 -> AnotherPublicNet
2. @exchange.example.com -> PublicNet
Choose the operation you want to perform:
```

```
- NEW - Create a new mapping.
- EDIT - Modify a mapping.
- DELETE - Remove a mapping.
- IMPORT - Load new mappings from a file.
- EXPORT - Export all mappings to a file.
- PRINT - Display all mappings.
- CLEAR - Remove all mappings.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added 2 altsrghost mappings
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

bounceconfig

説明

バウンスの動作を設定します。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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、CLIのインラインヘルプを参照してください。このコマンドのインラインヘルプにアクセスするには、**help** コマンドを使用します。

例

次の例では、**bounceconfig** コマンドを使用して、**bounceprofile** という名前のバウンス プロファイルを作成します。このプロファイルでは、ハードバウンスされたすべてのメッセージが代替アドレスである **bounce-mailbox@example.com** に送信されます。遅延警告メッセージはイネーブルです。受信者あたり警告メッセージが1つ送信されます。警告メッセージ間のデフォルト値は4時間（14400秒）です。

```
mail3.example.com> bounceconfig
Current bounce profiles:
1. Default
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
[]> new
Please create a name for the profile:
[]> bounceprofile
Please enter the maximum number of retries.
[100]> 100
Please enter the maximum number of seconds a message may stay in the queue before being
hard bounced.
[259200]> 259200
Please enter the initial number of seconds to wait before retrying a message.
[60]> 60
```

```
Please enter the maximum number of seconds to wait before retrying a message.
[3600]> 3600
Do you want a message sent for each hard bounce? (Yes/No/Default) [Y]> y
Do you want bounce messages to use the DSN message format? (Yes/No/Default) [Y]> y
Enter the subject to use:
[Delivery Status Notification (Failure)]>
Select default notification template:
1. System Generated
2. bounce_english
3. bounce_russian
[1]>
Do you want to configure language specific templates? [N]>
Do you want to parse the DSN "Status" field received from bounce
responses to include in the DSN generated by the appliance?
(Yes/No/Default) [N]>
If a message is undeliverable after some interval, do you want to send a delay warning
message? (Yes/No/Default) [N]> y
Enter the subject to use:
[Delivery Status Notification (Delay)]>
Select default notification template:
1. System Generated
2. bounce_english
3. bounce_russian
[1]> 1
Do you want to configure language specific templates? [N]>
Please enter the minimum interval in seconds between delay warning messages.
[14400]> 14400
Please enter the maximum number of delay warning messages to send per
recipient.
[1]> 1
Do you want hard bounce and delay warning messages sent to an alternate address, instead
of the sender? [N]> y
Please enter the email address to send hard bounce and delay warning.
[]> bounce-mailbox@example.com
Do you want bounce messages to be signed (Yes/No/Default)? [N]>
Current bounce profiles:
1. Default
2. bounceprofile
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Remove a profile.
[]>
mail3.example.com>
```

リスナーへのバウンス プロファイルの適用

バウンス プロファイルを設定したら、`listenerconfig -> bounceconfig` コマンドを使用し、変更を確定することにより、そのプロファイルを各リスナーに適用できます。



(注) バウンスプロファイルは、メッセージを受信したリスナーに基づいて適用できます。ただし、そのリスナーはメッセージが最終的にどのように配信されるかには関係しません。

この例では、`OutboundMail` プライベート リスナーを編集し、このリスナーに `bouncepr1` というバウンス プロファイルを適用します。

```
mail3.example.com> listenerconfig
```

```

Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 2
Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> bounceconfig
Please choose a bounce profile to apply:
1. Default
2. bouncepr1
3. New Profile
[1]> 2
Name: OutboundMail
Type: Private
Interface: PrivateNet (192.168.1.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 600 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: bouncepr1
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]>
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private
Choose the operation you want to perform:

```



```
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Enabled the bounceprl profile to the Outbound mail listener
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

bouncerecipients

説明

キューからメッセージをバウンスします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

バウンスされる受信者は、宛先受信者ホストによって、またはメッセージエンベロープの **Envelope From** 行に指定された特定のアドレスで識別されるメッセージ送信者によって識別されます。または、配信キュー内のすべてのメッセージを一度にバウンスすることもできます。

受信者ホストによるバウンス

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1
Please enter the hostname for the messages you wish to bounce.
[]> example.com
Are you sure you want to bounce all messages being delivered to "example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

Envelope From アドレスによるバウンス

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2
Please enter the Envelope From address for the messages you wish to bounce.
[]> mailadmin@example.com
```

```
Are you sure you want to bounce all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Bouncing messages, please wait.
100 messages bounced.
```

すべてバウンス

```
mail3.example.com> bouncerecipients
Please select how you would like to bounce messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]>
Are you sure you want to bounce all messages in the queue? [N]> Y
Bouncing messages, please wait.
1000 messages bounced.
```

bvconfig

説明

バウンス検証の設定を行います。このコマンドは、キーおよびバウンスされた無効な電子メールを設定するために使用します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次に、キー設定とバウンスされた無効な電子メールの設定の例を示します。

```
mail3.example.com> bvconfig
Behavior on invalid bounces: reject
Key for tagging outgoing mail: key
Previously-used keys for verifying incoming mail:
  1. key (current outgoing key)
  2. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)
Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]> key
Enter the key to tag outgoing mail with (when tagging is enabled in the Good
Neighbor Table)
[]> basic_key
Behavior on invalid bounces: reject
Key for tagging outgoing mail: basic_key
Previously-used keys for verifying incoming mail:
  1. basic_key (current outgoing key)
```

```

    2. key (last in use Wed May 31 23:22:49 2006 GMT)
    3. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)
Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]> setup
How do you want bounce messages which are not addressed to a valid tagged
recipient to be handled?
1. Reject.
2. Add a custom header and deliver.
[1]> 1
Behavior on invalid bounces: reject
Key for tagging outgoing mail: basic_key
Previously-used keys for verifying incoming mail:
    1. basic_key (current outgoing key)
    2. key (last in use Wed May 31 23:22:49 2006 GMT)
    3. goodneighbor (last in use Wed May 31 23:21:01 2006 GMT)
Choose the operation you want to perform:
- KEY - Assign a new key for tagging outgoing mail.
- PURGE - Purge keys no longer needed for verifying incoming mail.
- CLEAR - Clear all keys including current key.
- SETUP - Set how invalid bounces will be handled.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Configuring a new key and setting reject for invalid email bounces
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

deleterecipients

説明

キューからメッセージを削除します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンのモードでのみ使用できます。

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せん。

例

アプライアンスには、必要に応じて受信者を削除するための各種のオプションが用意されています。次に、受信者ホスト別の受信者の削除、Envelope From アドレスによる削除、およびキュー内のすべての受信者の削除の例を示します。

受信者ドメインによる削除

```

mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.

```

Envelope From アドレスによる削除

```

3. All.
[1]> 1
Please enter the hostname for the messages you wish to delete.
[]> example.com
Are you sure you want to delete all messages being delivered to "example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.

```

Envelope From アドレスによる削除

```

mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 2
Please enter the Envelope From address for the messages you wish to delete.
[]> mailadmin@example.com
Are you sure you want to delete all messages with the Envelope From address of
"mailadmin@example.com"? [N]> Y
Deleting messages, please wait.
100 messages deleted.

```

すべて削除

```

mail3.example.com> deleterecipients
Please select how you would like to delete messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 1
Are you sure you want to delete all messages in the queue? [N]> Y
Deleting messages, please wait.
1000 messages deleted.

```

deliveryconfig

説明

メール配信を設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例では、**deliveryconfig** コマンドを使用し、[配信可能性あり (Possible Delivery)] をイネーブルにして、デフォルトのインターフェイスを[自動 (Auto)] に設定します。システム全体の最大発信メッセージ配信は、9000 接続です。

```
mail3.example.com> deliveryconfig
Choose the operation you want to perform:
- SETUP - Configure mail delivery.
[ ]> setup
Choose the default interface to deliver mail.
1. Auto
2. AnotherPublicNet (192.168.3.1/24: mail4.example.com)
3. Management (192.168.42.42/24: mail3.example.com)
4. PrivateNet (192.168.1.1/24: mail3.example.com)
5. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Enable "Possible Delivery" (recommended)? [Y]> y
Please enter the default system wide maximum outbound message delivery
concurrency
[10000]> 9000
mail3.example.com>
```

delivernow

説明

メッセージのスケジュールを即時配信用に再設定します。ユーザは、1 つの受信者ホストと、配信用に現在スケジュールされているすべてのメッセージのいずれかを選択できます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> delivernow
Please choose an option for scheduling immediate delivery.
1. By recipient domain
2. All messages
[1]> 1
Please enter the recipient domain to schedule for delivery.
[ ]>foo.com
Scheduling all messages to foo.com for delivery.
```

destconfig

以前の **setgoodtable** コマンドです。テーブルは、現在、宛先制御テーブルと呼ばれています。このテーブルを使用して、指定したドメインの配信制限を設定します。

destconfig コマンドの使用

destconfig サブメニューでは、次のコマンドを使用できます。

表 7: destconfig サブコマンド

構文	説明
SETUP	グローバル設定を変更します。
NEW	ドメインの新しい制限を追加します。
EDIT	ドメインの制限を変更します。
DELETE	ドメインの制限を削除します。
DEFAULT	指定されていないドメインのデフォルトの制限を変更します。
LIST	ドメインとその制限のリストを表示します。
DETAIL	1 つの宛先またはすべてのエントリの詳細を表示します。
CLEAR	テーブルからすべてのエントリを削除します。
IMPORT	.INI コンフィギュレーションファイルから宛先制御エントリのテーブルをインポートします。
EXPORT	宛先制御エントリのテーブルを .INI コンフィギュレーションファイルにエクスポートします。

destconfig コマンドには、宛先制御テーブルの各行を構成する以下の情報を指定する必要があります。

- ドメイン（受信者ホスト）
- ドメインへの最大同時接続数
- 接続ごとの最大メッセージ数
- 受信者制限
- システム全体または仮想ゲートウェイ スイッチ
- ドメインごとの制限を適用します。
- 受信者制限の期間（分単位）
- バウンス検証
- ドメインで使用するバウンス プロファイル

サンプル宛先制御テーブル

次の表に、宛先制御テーブルのエントリを示します。

表 8:宛先制御テーブルのエントリ例

ドメイン	Conn. Limit	Rcpt. Limit	Min. Prd.	Enforce MX/DOM
(デフォルト)	500	なし	1	ドメイン
表示されていないドメインの接続数は 500、1 時間あたりの受信者数は無制限				
(デフォルト)	500	なし	1	MXIP
表示されていないドメインのメール ゲートウェイの最大接続数は 500、1 時間あたりの受信者数は無制限				
partner.com	10	500	60	ドメイン
partner.com のすべてのゲートウェイが 10 個の接続を共有、1 分間の最大受信者数は 500				
101.202.101.2	500	なし	[0]	MXIP
IP アドレスの指定				

バッチ形式

destconfig コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- 新しい宛先制御テーブルの作成

```
destconfig new <profile> [options]
```

- 既存の宛先制御テーブルの編集

```
destconfig edit <default|profile> [options]
```

- 既存の宛先制御テーブルの削除

```
destconfig delete <profile>
```

- 宛先制御エントリの一覧表示

```
destconfig list
```

- 1 つの宛先またはすべてのエントリの詳細の表示

```
destconfig detail <default|profile|all>
```

- 既存の宛先制御テーブルからすべてのエントリを削除

```
destconfig clear
```

- ファイルからのテーブルのインポート

```
destconfig import <filename>
```

- テーブルのファイルへのエクスポート

```
destconfig export <filename>
```

edit および **new** バッチ コマンドでは、変数名と等号を使用して値を示すことにより、以下のオプションの一部またはすべてを指定できます。指定しなかったオプションは、**edit** を使用した場合は変更されず、**new** を使用した場合はデフォルト値に設定されます。

<code>concurrency_limit=<int></code>	- The maximum concurrency for a specific host.
<code>concurrency_limit_type=<host MXIP></code>	- Maximum concurrency is per host or per MX IP.
<code>concurrency_limit_apply=<system VG></code>	- Apply maximum concurrency is system wide or by Virtual Gateway(tm).
<code>max_messages_per_connection=<int></code>	- The maximum number of messages that will be sent per connection.
<code>recipient_limit_minutes=<int></code>	- The time frame to check for recipient limits in minutes.
<code>recipient_limit=<int></code>	- The number of recipients to limit per unit of time.
<code>use_tls=<off on require on_verify require_verify></code>	- Whether TLS should be on, off, or required for a given host.
<code>bounce_profile=<default profile></code>	- The bounce profile name to use.
<code>bounce_verification=<off on></code>	- Bounce Verification option.

例：新しい **destconfig** エントリの作成

次の例では、現在の **destconfig** エントリを画面に出力します。さらに、ドメイン **partner.com** の新しいエントリを作成します。このドメインについては、最大同時接続数が 100、60 分あたりの受信者制限が 50 に設定されます。したがって、システムはドメイン **partner.com** に対し、1

時間に 100 を超える接続を確立せず、50 を超える受信者にメッセージを配信しません。このドメインにバウンス プロファイルは割り当てられず、TLS 設定は設定されません。最後に、変更が確認のために出力され、確定されます。

```
mail3.example.com> destconfig
There are currently 2 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[>] list
1
Domain          Rate          TLS          Bounce          Bounce
Limiting        Verification  Profile
=====
(Default) On      Off      Off      (Default)
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[>] new
Enter the domain you wish to configure.
[>] partner.com
Do you wish to configure a concurrency limit for partner.com? [Y]> y
Enter the max concurrency limit for "partner.com".
[500]> 100
Do you wish to apply a messages-per-connection limit to this domain? [N]> n
Do you wish to apply a recipient limit to this domain? [N]> y
Enter the number of minutes used to measure the recipient limit.
[60]> 60
Enter the max number of recipients per 60 minutes for "partner.com".
[>] 50
Select how you want to apply the limits for partner.com:
1. One limit applies to the entire domain for partner.com
2. Separate limit for each mail exchanger IP address
[1]> 1
Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)
[1]> 1
Do you wish to apply a specific TLS setting for this domain? [N]> n
Do you wish to apply a specific bounce verification address tagging setting for
this domain? [N]> n
Do you wish to apply a specific bounce profile to this domain? [N]> n
There are currently 3 entries configured.
mail3.example.com> commit
Please enter some comments describing your changes:
[>] Throttled delivery to partner.com in the destconfig table
```

```
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

例：バウンス プロファイルと TLS 設定

この例では、ドメイン `newpartner.com` に新しい `destconfig` エントリを設定します。TLS 接続が必要です。また、この例では、ドメイン `bouncepr1` ([リスナーへのバウンス プロファイルの適用 \(135 ページ\)](#)) を参照) というバウンス プロファイルをドメイン `newpartner.com` へのすべての電子メール配信に使用されるように設定します。

```
mail3.example.com> destconfig
There is currently 1 entry configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> new
Enter the domain you wish to configure.
[]> newpartner.com
Do you wish to configure a concurrency limit for newpartner.com? [Y]> n
Do you wish to apply a messages-per-connection limit to this domain? [N]> n
Do you wish to apply a recipient limit to this domain? [N]> n
Do you wish to apply a specific TLS setting for this domain? [N]> y
Do you want to use TLS support?
1. No
2. Preferred
3. Required
4. Preferred(Verify)
5. Required(Verify)
[1]> 3
You have chosen to enable TLS. Please use the 'certconfig' command to ensure that there
  is a valid certificate configured.
Do you wish to apply a specific bounce verification address tagging setting for this
domain? [N]> y
Perform bounce verification address tagging? [N]> y
Do you wish to apply a specific bounce profile to this domain? [N]> y
Please choose a bounce profile to apply:
1. Default
2. New Profile
[1]> 1
There are currently 2 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[]> detail
```

Rate	Bounce	Bounce

```

Domain          Limiting  TLS      Verification  Profile
=====
newpartner.com  Default  Req      On             Default
(Default)       On       Off      Off            (Default)
Enter the domain name to view, or enter DEFAULT to view details for the
default, or enter ALL to view details for all:
[]> all
newpartner.com
Maximum messages per connection: Default
Rate Limiting: Default
TLS: Required
Bounce Verification Tagging: On
Bounce Profile: Default
Default
Rate Limiting:
500 concurrent connections
No recipient limit
Limits applied to entire domain, across all virtual gateways
TLS: Off
Bounce Verification Tagging: Off
There are currently 2 entries configured.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> enabled TLS for delivery to newpartner.com using demo certificate
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

例：着信「緩衝装置」

この例では、メールを内部グループウェアサーバ `exchange.example.com` にスロットリングする別の **destconfig** エントリを作成します。この内部サーバ用の「緩衝装置」エントリを指定することで、トラフィックが特に増大する時間帯には着信が内部グループウェアサーバにスロットリングされます。この例では、アプライアンスは、内部グループウェアサーバ `exchange.example.com` に対し、1 分間に 10 を超える同時接続を確立せず、1000 を超える受信者にメッセージを配信しません。バウンス プロファイルと TLS 設定は設定されません。

```

mail3.example.com> destconfig
There are currently 2 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- CLEAR - Remove all entries.
[]> new
Enter the domain you wish to configure.
[]> exchange.example.com
Do you wish to configure a concurrency limit for exchange.example.com? [Y]> y
Enter the max concurrency limit for "exchange.example.com".
[500]> 10
Do you wish to apply a recipient limit to this domain? [N]> y
Enter the number of minutes used to measure the recipient limit.
[60]> 1
Enter the max number of recipients per 1 minutes for "exchange.example.com".

```

```
[ ]> 1000
Select how you want to apply the limits for exchange.example.com:
1. One limit applies to the entire domain for exchange.example.com
2. Separate limit for each mail exchanger IP address
[1]> 1
Select how the limits will be enforced:
1. System Wide
2. Per Virtual Gateway(tm)
[1]> 1
Do you wish to apply a specific TLS setting for this domain? [N]> n
Do you wish to apply a specific bounce verification address tagging setting for this
domain? [N]> n
Do you wish to apply a specific bounce profile to this domain? [N]> n
There are currently 3 entries configured.
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- CLEAR - Remove all entries.
[ ]>
mail3.example.com> commit
Please enter some comments describing your changes:
[ ]> set up shock absorber for inbound mail
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

例 : グローバル設定

この例では、TLS 接続の TLS アラートおよび証明書を設定します。

```
mail3.example.com> destconfig
Choose the operation you want to perform:
- SETUP - Change global settings.
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- DEFAULT - Change the default.
- LIST - Display a summary list of all entries.
- DETAIL - Display details for one destination or all entries.
- CLEAR - Remove all entries.
- IMPORT - Import tables from a file.
- EXPORT - Export tables to a file.
[ ]> setup
The "Demo" certificate is currently configured. You may use "Demo", but this will not
be secure.
1. partner.com
2. Demo
Please choose the certificate to apply:
[1]> 1
Do you want to send an alert when a required TLS connection fails? [N]> n
```

hostrate

説明

特定のホストのアクティビティをモニタします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> hostrate
Recipient host:
[]> aol.com
Enter the number of seconds between displays.
[10]> 1
  Time      Host  CrtCncOut  ActvRcp  ActvRcp  DlvRcp  HrdBncRcp  SftBncEvt
      Status                Delta      Delta      Delta      Delta
23:38:23    up        1          0          0          4          0          0
23:38:24    up        1          0          0          4          0          0
23:38:25    up        1          0          0         12          0          0
^C
```

hostrate コマンドを停止するには、Ctrl+C を使用します。

hoststatus

説明

特定のホスト名のステータスを取得します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> hoststatus

Recipient host:
[]> aol.com
Host mail status for: 'aol.com'
Status as of:      Fri Aug  8 11:12:00 2003
Host up/down:      up
```

```

Counters:
  Queue
    Soft Bounced Events          0
  Completion
    Completed Recipients          1
    Hard Bounced Recipients      1
    DNS Hard Bounces              0
    5XX Hard Bounces              1
    Filter Hard Bounces           0
    Expired Hard Bounces          0
    Other Hard Bounces            0
    Delivered Recipients          0
    Deleted Recipients            0
Gauges:
  Queue
    Active Recipients             0
    Unattempted Recipients        0
    Attempted Recipients          0
  Connections
    Current Outbound Connections  0
    Pending Outbound Connections  0
Oldest Message      No Messages
Last Activity       Fri Aug  8 11:04:24 2003
Ordered IP addresses: (expiring at Fri Aug  8 11:34:24 2003)
  Preference  IPs
    15        64.12.137.121    64.12.138.89    64.12.138.120
    15        64.12.137.89     64.12.138.152   152.163.224.122
    15        64.12.137.184    64.12.137.89    64.12.136.57
    15        64.12.138.57     64.12.136.153   205.188.156.122
    15        64.12.138.57     64.12.137.152   64.12.136.89
    15        64.12.138.89     205.188.156.154 64.12.138.152
    15        64.12.136.121    152.163.224.26  64.12.137.184
    15        64.12.138.120    64.12.137.152   64.12.137.121
MX Records:
  Preference  TTL      Hostname
    15        52m24s   mailin-01.mx.aol.com
    15        52m24s   mailin-02.mx.aol.com
    15        52m24s   mailin-03.mx.aol.com
    15        52m24s   mailin-04.mx.aol.com
Last 5XX Error:
-----
550 REQUESTED ACTION NOT TAKEN: DNS FAILURE
(at Fri Aug  8 11:04:25 2003)
-----
Virtual gateway information:
=====
example.com (PublicNet_017):
  Host up/down:  up
  Last Activity  Wed Nov 13 13:47:02 2003
  Recipients    0
=====
example.com (PublicNet_023):
  Host up/down:  up
  Last Activity  Wed Nov 13 13:45:01 2003
  Recipients

```

imageanalysisconfig

説明

IronPort イメージ分析の設定値を設定します

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com>imageanalysisconfig
IronPort Image Analysis: Enabled
Image Analysis Sensitivity: 65
Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)
Skip small images with size less than 100 pixels (width or height)

(First time users see the license agreement displayed here.)
Choose the operation you want to perform:
- SETUP - Configure IronPort Image Analysis.
[]> setup
IronPort Image Analysis: Enabled
Would you like to use IronPort Image Analysis? [Y]>
Define the image analysis sensitivity. Enter a value between 0 (least sensitive) and 100
(most sensitive). As sensitivity increases, so does the false
positive rate. The default setting of 65 is recommended.
[65]>
Define the range for a CLEAN verdict. Enter the upper bound of the CLEAN range by entering
a value between 0 and 98. The default setting of 49 is
recommended.
[49]>
Define the range for a SUSPECT verdict. Enter the upper bound of the SUSPECT range by
entering a value between 50 and 99. The default setting of 74 is
recommended.
[74]>
Would you like to skip scanning of images smaller than a specific size? [Y]>
Please enter minimum image size to scan in pixels, representing either height or width
of a given image.
[100]>
IronPort Image Analysis: Enabled
Image Analysis Sensitivity: 65
Verdict Ranges: Clean (0-49), Suspect(50-74), Inappropriate (75+)
Skip small images with size less than 100 pixels (width or height)
Choose the operation you want to perform:
- SETUP - Configure IronPort Image Analysis.
[]>
```

oldmessage

説明

システム上の最も古い非隔離メッセージの MID とヘッダーを表示します。

使用方法

確定：このコマンドに commit は必要ありません。

クラスタ管理 : このコマンドはマシンモードでのみ使用できます。

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せん。

例

次の例では、古いメッセージを表示します。

```
mail3.example.com>
oldmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from test02.com ([172.19.0.109])
by test02.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@test02.com
To: 4031@example.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@test02.com>
```

rate

説明

メッセージのスループットをモニタします。

使用方法

確定 : このコマンドに「commit」は必要ありません。

クラスタ管理 : このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> rate

Enter the number of seconds between displays.
[10]> 1
Hit Ctrl-C to return to the main prompt.
Time      Connections Recipients      Recipients      Queue
          In    Out   Received    Delta  Completed    Delta    K-Used
23:37:13   10    2   41708833     0   40842686     0       64
23:37:14    8    2   41708841     8   40842692     6      105
23:37:15    9    2   41708848     7   40842700     8       76
23:37:16    7    3   41708852     4   40842705     5       64
23:37:17    5    3   41708858     6   40842711     6       64
23:37:18    9    3   41708871    13   40842722    11       67
23:37:19    7    3   41708881    10   40842734    12       64
23:37:21   11    3   41708893    12   40842744    10       79
^C
```


redirectrecipients

説明

すべてのメッセージを別のリレー ホストにリダイレクトします。



危険

メッセージを、/dev/null を宛先とする受信側ドメインにリダイレクトすると、メッセージが失われます。メールをこのようなドメインにリダイレクトしても、CLI に警告は表示されません。メッセージをリダイレクトする前に、受信側ドメインがあるかどうかSMTP ルートを確認してください。



危険

このホストから大量の SMTP メールを受信できるように準備されていないホストまたは IP アドレスに受信者をリダイレクトすると、メッセージがバウンスされ、メールが失われる可能性があります。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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。

バッチ形式

redirectrecipients コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- すべてのメールを別のホスト名または IP アドレスにリダイレクトします。

```
redirectrecipients host <hostname>
```

例

次に、すべてのメールを example2.com ホストにリダイレクトする例を示します。

```
mail3.example.com> redirectrecipients
Please enter the hostname or IP address of the machine you want to send all mail to.
[]> example2.com
WARNING: redirecting recipients to a host or IP address that is not prepared to accept
large volumes of SMTP mail from this host
will cause messages to bounce and possibly result in the loss of mail.
Are you sure you want to redirect all mail in the queue to "example2.com"? [N]> y
Redirecting messages, please wait.
246 recipients redirected.
```

resetcounters

説明

システム内のすべてのカウンタをリセットします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> resetcounters
Counters reset: Mon Jan 01 12:00:01 2003
```

removemessage

説明

特定のメッセージ ID のメッセージを安全に削除します。

removemessage コマンドでは、作業キュー、再試行キュー、または宛先キュー内のメッセージのみを削除できます。システムの状態によっては、これらのキューに有効でアクティブなメッセージが含まれていない場合があります。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
example.com>
removemessage
Enter the MID to remove.
[]> 1
MID 1: 19 secs old
Received: from example2.com ([172.16.0.102])
    by test02.com with SMTP; 01 Mar 2007 19:50:41 -0800
From: user123@test02.com
To: 9526@example.com
Subject: Testing
Message-Id: <20070302035041.67424.53212@test02.com>
Remove this message? [N]> y
```

showmessage

説明

指定されたメッセージ ID のメッセージとメッセージ本文を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
example.com> showmessage
MID 9: 1 hour 5 mins 35 secs old
Received: from example2.com([172.19.0.109])
    by test02.com with SMTP; 14 Feb 2007 22:11:37 -0800
From: user123@test02.com
To: 4031@example.com
Subject: Testing
Message-Id: <20070215061136.68297.16346@test02.com>
This is the message body.
```

showrecipients

説明

キュー内のメッセージを受信者ホスト別または Envelope From アドレス別に表示するか、すべてのメッセージを表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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。

バッチ形式

showrecipients コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- 受信者ホスト名でのメッセージの検索

```
showrecipients host <hostname>
```

- Envelope From アドレスでのメッセージの検索

```
showrecipients [sender_options] <sender_email>
```

次の **sender_option** を使用できます。

--match-case アドレスのユーザ名部分の大文字と小文字を区別した一致。

- すべてのメッセージの検索

```
showrecipients all
```

例

次に、すべての受信者ホストへのキュー内のメッセージの例を示します。

```
mail3.example.com> showrecipients
Please select how you would like to show messages:
1. By recipient host.
2. By Envelope From address.
3. All.
[1]> 3
Showing messages, please wait.
MID/      Bytes/      Sender/      Subject
[RID]     [Atmps]    Recipient
1527      1230      user123456@ironport.com Testing
[0]       [0]       9554@example.com
1522      1230      user123456@ironport.com Testing
[0]       [0]       3059@example.com
1529      1230      user123456@ironport.com Testing
[0]       [0]       7284@example.com
1530      1230      user123456@ironport.com Testing
[0]       [0]       8243@example.com
1532      1230      user123456@ironport.com Testing
[0]       [0]       1820@example.com
1531      1230      user123456@ironport.com Testing
[0]       [0]       9595@example.com
1518      1230      user123456@ironport.com Testing
[0]       [0]       8778@example.com
1535      1230      user123456@ironport.com Testing
[0]       [0]       1703@example.com
1533      1230      user123456@ironport.com Testing
[0]       [0]       3052@example.com
1536      1230      user123456@ironport.com Testing
[0]       [0]       511@example.com
```

status

使用方法

確定：このコマンドに「**commit**」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

mail.example.com> status detail

```
Status as of:                Mon Sep 08 00:01:44 2014 GMT
Up since:                  Tue Aug 26 17:24:16 2014 GMT
(12d 6h 37m 28s)
Last counter reset:        Never
System status:              Online
Oldest Message:             No Messages
Feature - IronPort Anti-Spam: 1459 days
Feature - Incoming Mail Handling: Perpetual
Feature - Outbreak Filters: 1459 days

Counters:
Receiving
  Messages Received          2
  Recipients Received        2
Rejection
  Rejected Recipients        0
  Dropped Messages           0
Queue
  Soft Bounced Events       0
Completion
  Completed Recipients        0
Current IDs
  Message ID (MID)           2
  Injection Conn. ID (ICID)   0
  Delivery Conn. ID (DCID)    13

Gauges:
Current
Connections
  Current Inbound Conn.      0
  Current Outbound Conn.     0
Queue
  Active Recipients          2
  Messages In Work Queue     0
  Kilobytes Used              184
  Kilobytes Free              8,388,424
Quarantine
  Messages In Quarantine
    Policy, Virus and Outbreak 0
  Kilobytes In Quarantine
    Policy, Virus and Outbreak 0
```

tophosts

説明

電子メールキューに関する現在の情報を取得し、特定の受信者ホストに配信の問題（キューの増大など）があるかどうかを判断するには、**tophosts** コマンドを使用します。**tophosts** コマンドは、キュー内の上位 20 の受信者のリストを返します。リストは、アクティブ受信者、発信接続、配信済み受信者、ソフトバウンスイベント、およびハードバウンスされた受信者など、さまざまな統計情報別にソートできます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> tophosts
Sort results by:
1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]> 1
Status as of: Fri Mar 13 06:09:18 2015 GMT
Hosts marked with '*' were down as of the last delivery attempt.
```

#	Recipient Host	Active Recip.	Conn. Out	Deliv. Recip.	Soft Bounced	Hard Bounced
1*	example.com	2	0	0	0	0
2	the.encryption.queue	0	0	0	0	0
3	the.euq.queue	0	0	0	0	0
4	the.euq.release.queue	0	0	0	0	0

topin

説明

着信接続の数の順に上位のホストを表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> topin

Status as of: Sat Aug 23 21:50:54 2003
```

#	Remote hostname	Remote IP addr.	listener	Conn. In
1	mail.remotedomain01.com	172.16.0.2	Incoming01	10
2	mail.remotedomain01.com	172.16.0.2	Incoming02	10
3	mail.remotedomain03.com	172.16.0.4	Incoming01	5
4	mail.remotedomain04.com	172.16.0.5	Incoming02	4
5	mail.remotedomain05.com	172.16.0.6	Incoming01	3
6	mail.remotedomain06.com	172.16.0.7	Incoming02	3
7	mail.remotedomain07.com	172.16.0.8	Incoming01	3
8	mail.remotedomain08.com	172.16.0.9	Incoming01	3
9	mail.remotedomain09.com	172.16.0.10	Incoming01	3
10	mail.remotedomain10.com	172.16.0.11	Incoming01	2
11	mail.remotedomain11.com	172.16.0.12	Incoming01	2
12	mail.remotedomain12.com	172.16.0.13	Incoming02	2
13	mail.remotedomain13.com	172.16.0.14	Incoming01	2

14	mail.remotedomain14.com	172.16.0.15	Incoming01	2
15	mail.remotedomain15.com	172.16.0.16	Incoming01	2
16	mail.remotedomain16.com	172.16.0.17	Incoming01	2
17	mail.remotedomain17.com	172.16.0.18	Incoming01	1
18	mail.remotedomain18.com	172.16.0.19	Incoming02	1
19	mail.remotedomain19.com	172.16.0.20	Incoming01	1
20	mail.remotedomain20.com	172.16.0.21	Incoming01	1

unsubscribe

説明

グローバル配信停止リストを更新します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

この例では、アドレス `user@example.net` がグローバル配信停止リストに追加され、メッセージをハードバウンスするように機能が設定されます。このアドレスに送信されるメッセージはバウンスされます。配信の直前にメッセージがバウンスされます。

```
mail3.example.com> unsubscribe
Global Unsubscribe is enabled. Action: drop.
Choose the operation you want to perform:
- NEW - Create a new entry.
- IMPORT - Import entries from a file.
- SETUP - Configure general settings.
[]> new
Enter the unsubscribe key to add. Partial addresses such as "@example.com"
or "user@" are allowed, as are IP addresses. Partial hostnames such as "@.example.com"
are allowed.
[]> user@example.net
Email Address 'user@example.net' added.
Global Unsubscribe is enabled. Action: drop.
Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]> setup
Do you want to enable the Global Unsubscribe feature? [Y]> y
Would you like matching messages to be dropped or bounced?
1. Drop
2. Bounce
[1]> 2
Global Unsubscribe is enabled. Action: bounce.
```

```

Choose the operation you want to perform:
- NEW - Create a new entry.
- DELETE - Remove an entry.
- PRINT - Display all entries.
- IMPORT - Import entries from a file.
- EXPORT - Export all entries to a file.
- SETUP - Configure general settings.
- CLEAR - Remove all entries.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added username "user@example.net" to global unsubscribe
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

workqueue

説明

作業キューの一時停止ステータスを表示および変更します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```

mail3.example.com> workqueue
Status: Operational
Messages: 1243
Manually pause work queue? This will only affect unprocessed messages. [N]> y
Reason for pausing work queue:
[]> checking LDAP server
Status: Paused by admin: checking LDAP server
Messages: 1243

```



(注) 理由の入力は任意です。理由を入力しない場合、理由を「operator paused」としてログが記録されます。

次の例では、ワーク キューが再開されます。

```

mail3.example.com> workqueue
Status: Paused by admin: checking LDAP server
Messages: 1243
Resume the work queue? [Y]> y
Status: Operational
Messages: 1243

```


ネットワーク設定とネットワーク ツール

ここでは、次の CLI コマンドについて説明します。

- [etherconfig](#) (161 ページ)
- [interfaceconfig](#) (163 ページ)
- [nslookup](#) (165 ページ)
- [netstat](#) (166 ページ)
- [packetcapture](#) (167 ページ)
- [ping](#) (168 ページ)
- [ping6](#) (169 ページ)
- [routeconfig](#) (170 ページ)
- [setgateway](#) (172 ページ)
- [sethostname](#) (173 ページ)
- [smtproutes](#) (173 ページ)
- [sslconfig](#) (175 ページ)
- [sslv3config](#) (178 ページ)
- [telnet](#) (178 ページ)
- [traceroute](#) (179 ページ)
- [traceroute6](#) (180 ページ)

etherconfig

説明

メディア設定、NIC ペアリング、VLAN 設定、DSR 設定などのイーサネット設定を行います。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> etherconfig
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> vlan
VLAN interfaces:
```

```

Choose the operation you want to perform:
- NEW - Create a new VLAN.
[]> new
VLAN tag ID for the interface (Ex: "34") :
[]> 12
Enter the name or number of the ethernet interface you wish bind to:
1. Data 1
2. Data 2
3. Management
[1]> 1
VLAN interfaces:
1. VLAN 12 (Data 1)
Choose the operation you want to perform:
- NEW - Create a new VLAN.
- EDIT - Edit a VLAN.
- DELETE - Delete a VLAN.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> loopback
Currently configured loopback interface:
Choose the operation you want to perform:
- ENABLE - Enable Loopback Interface.
[]>
Choose the operation you want to perform:
- MEDIA - View and edit ethernet media settings.
- VLAN - View and configure VLANs.
- LOOPBACK - View and configure Loopback.
- MTU - View and configure MTU.
- MULTICAST - Accept or reject ARP replies with a multicast address.
[]> mtu
Ethernet interfaces:
1. Data 1 default mtu 1500
2. Data 2 default mtu 1500
3. Management default mtu 1500
4. VLAN 12 default mtu 1500
Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]> edit
Enter the name or number of the ethernet interface you wish to edit.
[]> pair1
That value is not valid.
Enter the name or number of the ethernet interface you wish to edit.
[]> 12
That value is not valid.
Enter the name or number of the ethernet interface you wish to edit.
[]> 2
Please enter a non-default (1500) MTU value for the Data 2 interface.
[]> 1200
Ethernet interfaces:
1. Data 1 default mtu 1500
2. Data 2 mtu 1200
3. Management default mtu 1500
4. VLAN 12 default mtu 1500
Choose the operation you want to perform:
- EDIT - Edit an ethernet interface.
[]>

```

interfaceconfig

説明

インターフェイスを設定します。インターフェイスを作成、編集、削除できます。FTP をイネーブルにし、IP アドレスを変更し、イーサネット IP アドレスを設定できます。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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。

バッチ形式

interfaceconfig コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- 新しいインターフェイスの作成

interfaceconfig new <name>
<ethernet interface>
<hostname>
--ip=IPv4 Address/Netmask
--ip6=IPv6 Address/Prefix Lenght
[--ftp[=<port>]]
[--telnet[=<port>]]
[--ssh[=<port>]]
[--http[=<port>]]
[--https[=<port>]]
[--euq_http[=<port>]]
[--euq_https[=<port>]]

```
[--ccs[=<port>]].
```

```
FTP is available only on IPv4.
```

• インターフェイスの削除

```
interfaceconfig delete <name>
```

例 : インターフェイスの設定

```
mail.example.com> interfaceconfig
Currently configured interfaces:
1. Management (10.76.69.149/24 on Management: mail.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[]> edit
Enter the number of the interface you wish to edit.
[]> 1
IP interface name (Ex: "InternalNet"):
[Management]>
Would you like to configure an IPv4 address for this interface (y/n)? [Y]>
IPv4 Address (Ex: 192.168.1.2 ):
[1.1.1.1]>
Netmask (Ex: "24", "255.255.255.0" or "0xffffffff00"):
[0xffffffff]>
Would you like to configure an IPv6 address for this interface (y/n)? [N]> n
Ethernet interface:
1. Data 1
2. Data 2
3. Management
[3]>
Hostname:
[mail.example.com]>
Do you want to enable SSH on this interface? [Y]>
Which port do you want to use for SSH?
[22]>
Do you want to enable FTP on this interface? [N]>
Do you want to enable Cluster Communication Service on this interface? [N]>
Do you want to enable HTTP on this interface? [Y]>
Which port do you want to use for HTTP?
[80]>
Do you want to enable HTTPS on this interface? [Y]>
Which port do you want to use for HTTPS?
[443]>
Do you want to enable Spam Quarantine HTTP on this interface? [N]>
Do you want to enable Spam Quarantine HTTPS on this interface? [N]>
Do you want to enable AsyncOS API (Monitoring) HTTP on this interface? [N]> y
Which port do you want to use for AsyncOS API (Monitoring) HTTP?
[6080]>
Do you want to enable AsyncOS API (Monitoring) HTTPS on this interface? [N]> y
Which port do you want to use for AsyncOS API (Monitoring) HTTPS?
[6443]>
The "Demo" certificate is currently configured. You may use "Demo", but this will not
be
```

```
secure. To assure privacy, run "certconfig" first.
Both HTTP and HTTPS are enabled for this interface, should HTTP requests redirect to the
secure service? [Y]>
You have edited the interface you are currently logged into. Are you sure you want to
change it? [Y]>
Currently configured interfaces:
1. Management (10.76.69.149/24 on Management: mail.example.com)
Choose the operation you want to perform:
- NEW - Create a new interface.
- EDIT - Modify an interface.
- GROUPS - Define interface groups.
- DELETE - Remove an interface.
[ ]>
```

nslookup

説明

nslookup コマンドを使用すると、DNS の機能を検査できます。

nslookup コマンドでは、アプライアンスが、動作している DNS（ドメイン ネーム サービス）サーバからホスト名と IP アドレスを解決して到達できることを確認できます。

表 9: **nslookup** コマンドのクエリー タイプ

クエリーのタイプ	説明
	ホストのインターネット アドレス
CNAME	エイリアスの正規の名前
MX	メール エクスチェンジャ
NS	指定したゾーンのネーム サーバ
PTR	クエリーがインターネット アドレスの場合はホスト名、そうでない場合は他の情報に対するポインタ
SOA	ドメインの「権限開始」情報
TXT	テキスト情報

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> nslookup
Please enter the host or IP address to resolve.
[]> vm30esa0086.ibqa
Choose the query type:
1. A      the host's IP address
2. AAAA   the host's IPv6 address
3. CNAME  the canonical name for an alias
4. MX     the mail exchanger
5. NS     the name server for the named zone
6. PTR    the hostname if the query is an Internet address,
otherwise the pointer to other information
7. SOA    the domain's "start-of-authority" information
8. TXT    the text information
[1]> 2
AAAA=2001:420:54ff:ff06::95 TTL=30m
```

netstat

説明

netstat コマンドを使用すると、ネットワーク接続（着信および発信）、ルーティングテーブル、およびさまざまなネットワークインターフェイス統計情報を表示できます。このバージョンではすべての引数がサポートされるわけではないことに注意してください。特に、**-a**、**-A**、**-g**、**-m**、**-M**、**-N**、**-s** は使用できません。このコマンドはインタラクティブモードでの実行を目的としているため、**netstat** を入力した後でレポートの対象を5つのオプションから選択できます。また、リッスンするインターフェイスと表示の間隔も指定できます。

使用方法

確定：このコマンドに「**commit**」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
example.com> netstat
Choose the information you want to display:
1. List of active sockets.
2. State of network interfaces.
3. Contents of routing tables.
4. Size of the listen queues.
5. Packet traffic information.
[1]> 2
Select the ethernet interface whose state you wish to display:
1. Data 1
2. Data 2
3. Management
4. ALL
[]> 1
Show the number of bytes in and out? [N]>
```

```
Show the number of dropped packets? [N]> y
Name      Mtu Network      Address      IpKts Ierrs      OpKts
Oerrs  Coll Drop
Data 1 1500 197.19.1/24  example.com      30536      -      5      -
-      -
example.com>
```

packetcapture

説明

netstat コマンドを使用すると、ネットワーク接続（着信および発信）、ルーティングテーブル、およびさまざまなネットワーク インターフェイス統計情報を表示できます。このバージョンではすべての引数がサポートされるわけではないことに注意してください。特に、**-a**、**-A**、**-g**、**-m**、**-M**、**-N**、**-s** は使用できません。このコマンドはインタラクティブ モードでの実行を目的としているため、**netstat** を入力した後でレポートの対象を 5 つのオプションから選択できます。また、リッスンするインターフェイスと表示の間隔も指定できます。

使用方法

確定：このコマンドに「**commit**」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> packetcapture
Capture Information:
  Status:                No capture running
Current Settings:
  Maximum File Size:     200 MB
  Limit:                 None (Run Indefinitely)
  Interface(s):          ALL
  Filter:                (tcp port 25)
Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> start
Success - Packet Capture has started
Capture Information:
  File Name:             C100V-421C73B18CFB05784A83-B03A99E71ED8-20150312-105256.cap
  File Size:              0 of 200M
  Duration:              0s
  Limit:                 None (Run Indefinitely)
  Interface(s):          ALL
  Filter:                (tcp port 25)
Choose the operation you want to perform:
- STOP - Stop packet capture.
- STATUS - Display current capture status.
- SETUP - Change packet capture settings.
[]> stop
Success - Packet Capture has stopped
Capture Information:
```

```

File Name:          C100V-421C73B18CFB05784A83-B03A99E71ED8-20150312-105256.cap
File Size:          24 of 200M
Duration:           10s
Limit:              None (Run Indefinitely)
Interface(s):       ALL
Filter:              (tcp port 25)
Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]> setup
Enter maximum allowable size for the capture file (in MB)
[200]>
Do you want to stop the capture when the file size is reached? (If not, a new file will
be started and the older capture data will be discarded.)
[N]>
The following interfaces are configured:
1. Management
2. ALL
Enter the name or number of one or more interfaces to capture packets from, separated
by commas (enter ALL to use all interfaces):
[2]>
Select an operation. Press enter to continue with the existing filter.
- PREDEFINED - PREDEFINED filter.
- CUSTOM - CUSTOM filter.
- CLEAR - CLEAR filter.
[]>
Capture settings successfully saved.
Current Settings:
  Maximum File Size: 200 MB
  Limit:             None (Run Indefinitely)
  Interface(s):      ALL
  Filter:             (tcp port 25)
Choose the operation you want to perform:
- START - Start packet capture.
- SETUP - Change packet capture settings.
[]>

```

ping

説明

ping コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストできます。

使用方法

確定： このコマンドに「commit」は必要ありません。

クラスタ管理： このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカル ファイル システムにアクセスできる必要があります。

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せん。

例

```
mail3.example.com> ping
```



```
Which interface do you want to send the pings from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Please enter the host you wish to ping.
[]> anotherhost.example.com
Press Ctrl-C to stop.
PING anotherhost.example.com (
x.x.x.x
): 56 data bytes
64 bytes from 10.19.0.31: icmp_seq=0 ttl=64 time=1.421 ms
64 bytes from 10.19.0.31: icmp_seq=1 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=2 ttl=64 time=0.118 ms
64 bytes from 10.19.0.31: icmp_seq=3 ttl=64 time=0.115 ms
64 bytes from 10.19.0.31: icmp_seq=4 ttl=64 time=0.139 ms
64 bytes from 10.19.0.31: icmp_seq=5 ttl=64 time=0.125 ms
64 bytes from 10.19.0.31: icmp_seq=6 ttl=64 time=0.124 ms
64 bytes from 10.19.0.31: icmp_seq=7 ttl=64 time=0.122 ms
64 bytes from 10.19.0.31: icmp_seq=8 ttl=64 time=0.126 ms
64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms
64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms
^C
--- anotherhost.example.com ping statistics ---
11 packets transmitted, 11 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
^C
```



(注) ping コマンドを終了するには、Ctrl+C を使用する必要があります。

ping6

説明

IPv6 を使用するネットワーク ホストに ping を実行します

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカル ファイル システムにアクセスできる必要があります。

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せん。

例

```
mail.example.com> ping6
Which interface do you want to send the pings from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
[1]> 1
```

```
Please enter the host you wish to ping.
[]> anotherhost.example.com
Press Ctrl-C to stop.
```



(注) **ping6** コマンドを終了するには、Ctrl+C を使用します。

routeconfig

説明

routeconfig コマンドを使用すると、TCP/IP トラフィックのスタティックルートを作成、編集、削除できます。デフォルトでは、トラフィックは **setgateway** コマンドで設定されたデフォルトゲートウェイ経由でルーティングされます。ただし、AsyncOS では特定の宛先へのルーティングも可能です。

ルートは、ニックネーム（参照用）、宛先、およびゲートウェイで構成されます。ゲートウェイ（ネクストホップ）は、10.1.1.2 などの IP アドレスです。宛先は次のいずれかになります。

- IP アドレス（192.168.14.32 など）
- CIDR 表記法によるサブネットたとえば、192.168.5.0/24 は 192.168.5.0 から 192.168.5.255 までのクラス C ネットワーク全体を意味します。

IPv6 アドレスの場合は、次の形式を使用できます。

- 2620:101:2004:4202::0-2620:101:2004:4202::ff
- 2620:101:2004:4202::
- 2620:101:2004:4202::23
- 2620:101:2004:4202::/64

このコマンドでは、現在設定されている TCP/IP ルートのリストが表示されるので、そこからルートを選択して **edit** および **delete** サブコマンドを使用できます。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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。

バッチ形式

smtproutes コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。ルートに IPv4 アドレスまたは IPv6 アドレスのどちらを使用するかを選択できます。

- スタティック ルートの作成：

```
routeconfig new 4|6 <name> <destination_address> <gateway_ip>
```

表 10: routeconfig の引数

引数	説明
4 6	このコマンドを適用する IP のバージョン（IPv4 または IPv6）。clear を指定した場合および print を指定した場合、このオプションは省略可能で、コマンドは両方のバージョンに適用されます。
name	ルートの名前。
destination_address	発信 IP トラフィックの場合に照合する IP アドレスまたは CIDR アドレス。
gateway_ip	このトラフィックの送信先とする IP アドレス。

- スタティック ルートの編集：

```
routeconfig edit 4|6 <name> <new_name> <destination_address> <gateway_ip>
```

- スタティック ルートの削除：

```
routeconfig delete 4|6 <name>
```

- すべてのスタティック ルートの削除：

```
routeconfig clear [4|6]
```

- スタティック ルートの一覧出力：

```
routeconfig print [4|6]
```

例

```
mail3.example.com> routeconfig
Configure routes for:
1. IPv4
2. IPv6
[1]>
Currently configured routes:
Choose the operation you want to perform:
- NEW - Create a new route.
[]> new
Please create a name for the route:
[]> EuropeNet
Please enter the destination IPv4 address to match on.
CIDR addresses such as 192.168.42.0/24 are also allowed.
[]> 192.168.12.0/24
Please enter the gateway IP address for traffic to 192.168.12.0/24:
[]> 192.168.14.4
Currently configured routes:
```

```

1. EuropeNet Destination: 192.168.12.0/24 Gateway: 192.168.14.4
Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[]>
mail3.example.com> routeconfig
Configure routes for:
1. IPv4
2. IPv6
[1]> 2
Currently configured routes:
Choose the operation you want to perform:
- NEW - Create a new route.
[]> new
Please create a name for the route:
[]> EuropeIPv6Net
Please enter the destination IPv6 address to match on.
CIDR addresses such as 2001:db8::/32 are also allowed.
[]> 2620:101:2004:4202::/6
Please enter the gateway IP address for traffic to 2620:101:2004:4202::/6:
[]> 2620:101:2004:4202::23
Currently configured routes:
1. EuropeIPv6Net Destination: 2620:101:2004:4202::/6 Gateway:
2620:101:2004:4202::23
Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Modify a route.
- DELETE - Remove a route.
- CLEAR - Clear all entries.
[]>

```

setgateway

説明

setgateway コマンドでは、パケットをルーティングするときに経由するデフォルトのネクストホップを設定します。代替（デフォルトではない）ゲートウェイは、routeconfig コマンドを使用して設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```

mail3.example.com> setgateway
Warning: setting an incorrect default gateway may cause the current connection to be
interrupted when the changes are committed.
Enter new default gateway:
[10.1.1.1]> 192.168.20.1

```

```
mail3.example.com> commit
Please enter some comments describing your changes:
[]> changed default gateway to 192.168.20.1
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

sethostname

説明

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、Eメール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。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
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
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

次のように新しいホスト名がプロンプトに表示されます。

```
mail3.example.com>
```

smtproutes

説明

永続的なドメイン転送を設定します。

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式

`smtproutes` コマンドのバッチ形式を使用すると、従来の CLI コマンドのすべての機能を実行できます。

- 新しい SMTP ルートの作成

```
smtproutes new <source> <destination> [destination] [destination] [...]
```

- 既存の SMTP ルートの削除

```
smtproutes delete <source>
```

- SMTP ルートのリストのクリア

```
smtproutes clear
```

- SMTP ルートのリストの出力

```
smtproutes print
```

- SMTP ルートのリストのインポート

```
smtproutes import <filenames>
```

- SMTP ルートのリストのエクスポート

```
smtproutes export <filenames>
```

例

次の例では、`smtproutes` コマンドを使用して、ドメイン `example.com` の `relay1.example.com`、`relay2.example.com`、および `backup-relay.example.com` へのルート（マッピング）を作成します。宛先のプライオリティを指定するには、`/pri=#` を使用します。# には 0 ～ 65535 の値を指定します。値が大きいほどプライオリティは低くなります。プライオリティを指定しない場合、デフォルトの 0 に設定されます。

（`systemsetup` コマンドの実行時、`InboundMail` パブリック リスナーを設定するときに同じマッピングを作成している場合があることに注意してください。）

```
mail3.example.com> smtproutes
```

```

There are no routes configured.
Choose the operation you want to perform:
- NEW - Create a new route.
- IMPORT - Import new routes from a file.
[]> new
Enter the domain for which you want to set up a permanent route.
Partial hostnames such as ".example.com" are allowed.
Use "ALL" for the default route.
[]> example.com
Enter the destination hosts, separated by commas, which you want mail
for example.com to be delivered.
Enter USEDNS by itself to use normal DNS resolution for this route.
Enter /dev/null by itself if you wish to discard the mail.
Enclose in square brackets to force resolution via address (A)
records, ignoring any MX records.
[]> relay1.example.com/pri=10, relay2.example.com, backup-relay.example.com
Mapping for example.com to relay1.example.com, relay2.example.com,
backup-relay.example.com/pri=10 created.
There are currently 1 routes configured.
Choose the operation you want to perform:
- NEW - Create a new route.
- EDIT - Edit destinations of an existing route.
- DELETE - Remove a route.
- PRINT - Display all routes.
- IMPORT - Import new routes from a file.
- EXPORT - Export all routes to a file.
- CLEAR - Remove all routes.
[]>

```

sslconfig

説明

アプライアンスの SSL 設定を指定します。



(注) FIPS 140-2 準拠モードでサーバおよびクライアントのメソッドは変更できません。

使用方法

確定： このコマンドは「commit」が必要です。

クラスタ管理： このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```

mail.example.com> sslconfig

sslconfig settings:
  GUI HTTPS method:  tlsv1_1tlsv1_2
  GUI HTTPS ciphers:
    AES128

```

```

        AES256
        !SRP
        !AESGCM+DH+aRSA
        !AESGCM+RSA
        !aNULL
Inbound SMTP method:  tlsv1_1tlsv1_2
Inbound SMTP ciphers:
        AES128
        AES256
        !SRP
        !AESGCM+DH+aRSA
        !AESGCM+RSA
        !aNULL
Outbound SMTP method:  tlsv1_1tlsv1_2
Outbound SMTP ciphers:
        ECDH+aRSA
        ECDH+ECDSA
        DHE+DSS+AES
        AES128
        AES256
        !SRP
        !AESGCM+DH+aRSA
        !AESGCM+RSA
        !aNULL
        !eNULL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> gui
Enter the GUI HTTPS ssl method you want to use.
1. TLS v1.0
2. TLS v1.1
3. TLS v1.2
4. SSL v3
[2, 3]> 1
Enter the GUI HTTPS ssl cipher you want to use.
[AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL]>
sslconfig settings:
  GUI HTTPS method:  tlsv1_0
  GUI HTTPS ciphers:
        AES128
        AES256
        !SRP
        !AESGCM+DH+aRSA
        !AESGCM+RSA
        !aNULL
Inbound SMTP method:  tlsv1_1tlsv1_2
Inbound SMTP ciphers:
        AES128
        AES256
        !SRP
        !AESGCM+DH+aRSA
        !AESGCM+RSA
        !aNULL
Outbound SMTP method:  tlsv1_1tlsv1_2
Outbound SMTP ciphers:
        ECDH+aRSA
        ECDH+ECDSA
        DHE+DSS+AES
        AES128
        AES256

```



```

!SRP
!AESGCM+DH+aRSA
!AESGCM+RSA
!aNULL
!eNULL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound
Enter the inbound SMTP ssl method you want to use.
1. TLS v1.0
2. TLS v1.1
3. TLS v1.2
4. SSL v3
[2, 3]> 2
Enter the inbound SMTP ssl cipher you want to use.
[AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL]>
  sslconfig settings:
  GUI HTTPS method:  tlsv1_0
  GUI HTTPS ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
  Inbound SMTP method:  tlsv1_1
  Inbound SMTP ciphers:
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
  Outbound SMTP method:  tlsv1_1tlsv1_2
  Outbound SMTP ciphers:
    ECDH+aRSA
    ECDH+ECDSA
    DHE+DSS+AES
    AES128
    AES256
    !SRP
    !AESGCM+DH+aRSA
    !AESGCM+RSA
    !aNULL
    !eNULL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>

[]>

```

ssl3config

説明

アプライアンスの SSLv3 設定を有効または無効にします。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例は、エンド ユーザ隔離に対して SSLv3 を無効にする方法を示しています。

```
mail.example.com> ssl3config
Current SSLv3 Settings:
-----
                UPDATER      :      Enabled
        WEBSECURITY      :      Enabled
                EUQ        :      Enabled
                LDAP       :      Enabled
-----

Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]> setup
Choose the service to toggle SSLv3 settings:
1. EUQ Service
2. LDAP Service
3. Updater Service
4. Web Security Service
[1]>
Do you want to enable SSLv3 for EUQ Service ? [Y]>n
Choose the operation you want to perform:
- SETUP - Toggle SSLv3 settings.
[]>
```

telnet

説明

リモート ホストに接続します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカルファイルシステムにアクセスする必要があります。

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せん。

例

```
mail3.example.com> telnet
Please select which interface you want to telnet from.
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 3
Enter the remote hostname or IP.
[]> 193.168.1.1
Enter the remote port.
[25]> 25
Trying 193.168.1.1...
Connected to 193.168.1.1.
Escape character is '^'.
```

traceroute

説明

traceroute コマンドを使用すると、アプライアンスから IPV4 を使用するネットワーク ホストへの接続をテストして、ネットワークのホップに関するルーティングの問題をデバッグできます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカルファイルシステムにアクセスする必要があります。

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せん。

例

```
mail3.example.com> traceroute
Which interface do you want to trace from?
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Please enter the host to which you want to trace the route.
[]> 10.1.1.1
Press Ctrl-C to stop.
```

```
tracert6 to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets
 1  gateway
   (192.168.0.1)  0.202 ms  0.173 ms  0.161 ms
 2  hostname
   (10.1.1.1)  0.298 ms  0.302 ms  0.291 ms
mail3.example.com>
```

tracert6

説明

tracert6 コマンドを使用すると、アプライアンスから IPV6 を使用するネットワーク ホストへの接続をテストして、ネットワークのホップに関するルーティングの問題をデバッグできます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカル ファイル システムにアクセスできる必要があります。

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せん。

例

```
mail.example.com> tracert6
Which interface do you want to trace from?
1. Auto
2. D1 (2001:db8::/32: example.com)
[1]> 1
Please enter the host to which you want to trace the route.
[]> example.com
Press Ctrl-C to stop.
connect: No route to host
vm10esa0031.qa> tracert6
Which interface do you want to trace from?
1. Auto
2. D1 (2001:db8::/32: example.com)
[1]> 2
Please enter the host to which you want to trace the route.
[]> example.com
Press Ctrl-C to stop.
tracert6 to example.com (2606:2800:220:1:248:1893:25c8:1946) from 2001:db8::, 64 hops
max, 12 byte packets
sendto: No route to host
 1 tracert6: wrote example.com 12 chars, ret=-1
 *sendto: No route to host
tracert6: wrote example.com 12 chars, ret=-1
 *sendto: No route to host
tracert6: wrote example.com 12 chars, ret=-1
```

アウトブレイク フィルタ

ここでは、次の CLI コマンドについて説明します。

- [outbreakconfig](#) (181 ページ)
- [outbreakflush](#) (182 ページ)
- [outbreakstatus](#) (182 ページ)
- [outbreakupdate](#) (183 ページ)

outbreakconfig

説明

outbreakconfig コマンドを使用すると、アウトブレイク フィルタ機能を設定できます。このコマンドを使用して次のアクションを実行できます。

- アウトブレイク フィルタをグローバルにイネーブルにします。
- アダプティブ ルールのスキャンをイネーブルにします。
- スキャンするファイルの最大サイズを設定します（サイズをバイトで入力することに注意してください）。
- アウトブレイク フィルタのアラートをイネーブルにします。
- URL のロギングをイネーブルにします。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> outbreakconfig
Outbreak Filters: Enabled
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]> setup
Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>
Outbreak Filters enabled.
Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or
back down below), meaning that new messages of
certain types could be quarantined or will no longer be quarantined, respectively.
Would you like to receive Outbreak Filter alerts? [N]>
What is the largest size message Outbreak Filters should scan?
[524288]>
Do you want to use adaptive rules to compute the threat level of messages? [Y]>
```

```

Logging of URLs is currently disabled.
Do you wish to enable logging of URL's? [N]> Y
Logging of URLs has been enabled.
The Outbreak Filters feature is now globally enabled on the system.  You must use the
'policyconfig' command in the CLI or the Email
Security Manager in the GUI to enable Outbreak Filters for the desired Incoming and
Outgoing Mail Policies.
Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
[]>

```

outbreakflush

説明

キャッシュされている発生ルールをクリアします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```

mail3.example.com> outbreakflush
Warning - This command removes the current set of Outbreak Filter Rules, leaving your
network exposed until the next rule download.
Run "outbreakupdate force" command to immediately download Outbreak Filter Rules.
Are you sure that you want to clear the current rules? [N]> y
Cleared the current rules.
mail3.example.com>

```

outbreakstatus

説明

outbreakstatus コマンドは、感染フィルタ機能をイネーブルにするかどうか、発生ルール、現在のしきい値など、感染フィルタ機能の現在の設定を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> outbreakstatus
Outbreak Filters: Enabled

Component                Last Update                Version
CASE Core Files          26 Jan 2014 06:45 (GMT +00:00)  3.3.1-005
CASE Utilities           26 Jan 2014 06:45 (GMT +00:00)  3.3.1-005
Outbreak Rules           26 Jan 2014 07:00 (GMT +00:00)  20140126_063240

Threat Outbreak          Outbreak
Level  Rule Name            Rule Description
-----
5      OUTBREAK_0002187_03    A reported a MyDoom.BB outbreak.
5      OUTBREAK_0005678_00    This configuration file was generated by...
3      OUTBREAK_0000578_00    This virus is distributed in pictures of...

Outbreak Filter Rules with higher threat levels pose greater risks.
(5 = highest threat, 1 = lowest threat)

Last update: Mon Jan 27 04:36:27 2014

mail3.example.com>
```

outbreakupdate

説明

CASE ルールおよびエンジン コアの即時更新を要求します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログイン ホスト（ユーザがログインしたマシン）でのみ使用できます。

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せん。

例

```
elroy.run> outbreakupdate
Requesting updates for Outbreak Filter Rules.
```

ポリシーの適用

ここでは、次の CLI コマンドについて説明します。

- [dictionaryconfig](#) (184 ページ)
- [exceptionconfig](#) (187 ページ)
- [filters](#) (188 ページ)

- [policyconfig](#) (190 ページ)
- [quarantineconfig](#) (212 ページ)
- [scanconfig](#) (214 ページ)
- [stripheaders](#) (217 ページ)
- [textconfig](#) (218 ページ)

dictionaryconfig

説明

コンテンツ デictionary を設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

dictionaryconfig -> new を使用して Dictionary を作成し、**dictionaryconfig -> delete** を使用して Dictionary を削除します。

Dictionary の作成

```
example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new
Enter a name for this content dictionary.
[]> HRWords
Do you wish to specify a file for import? [N]>
Enter new words or regular expressions, enter a blank line to finish.
<list of words typed here>
Currently configured content dictionaries:
1. HRWords
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> delete
Enter the number of the dictionary you want to delete:
1. HRWords
[]> 1
Content dictionary "HRWords" deleted.
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]>
```


ディクショナリの作成 2

この例では、用語「codename」を含む「secret_words」という名前の新しいディクショナリが作成されます。ディクショナリを入力したら、**edit->settings** サブコマンドを使用して、ディクショナリ内の単語の大文字と小文字の区別や単語境界の検出を定義します。

```
mail3.example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new
Enter a name for this content dictionary.
[]> secret_words
Do you wish to specify a file for import? [N]>
Enter new words or regular expressions, enter a blank line to finish.
codename
Currently configured content dictionaries:
1. secret_words
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> edit
Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1
Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> settings
Do you want to ignore case when matching using this dictionary? [Y]>
Do you want strings in this dictionary to only match complete words? [Y]>
Enter the default encoding to be used for exporting this dictionary:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[2]>
Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]>
Currently configured content dictionaries:
1. secret_words
```

```

Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> Added new dictionary: secret_words
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT

```

ディクショナリのインポート

次の例では、**dictionaryconfig** コマンドを使用して、profanity.txt テキスト ファイル内の 84 個の用語を Unicode (UTF-8) としてディクショナリ profanity にインポートします。

```

mail3.example.com> dictionaryconfig
No content dictionaries have been defined.
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
[]> new
Enter a name for this content dictionary.
[]> profanity
Do you wish to specify a file for import? [N]> y
Enter the name of the file to import:
[]> profanity.txt
Enter the encoding to use for the imported file:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[2]>
84 entries imported successfully.
Currently configured content dictionaries:
1. profanity
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.

```

ディクショナリのエクスポート

次の例では、**dictionaryconfig** コマンドを使用して、secret_words ディクショナリをテキスト ファイル secret_words_export.txt にエクスポートします。

```

mail3.example.com> dictionaryconfig
Currently configured content dictionaries:
1. secret_words
Choose the operation you want to perform:

```

```
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> edit
Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1
Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> export
Enter a name for the exported file:
[]> secret_words_export.txt
mail3.example.com> dictionaryconfig
Currently configured content dictionaries:
1. secret_words
Choose the operation you want to perform:
- NEW - Create a new content dictionary.
- EDIT - Modify a content dictionary.
- DELETE - Remove a content dictionary.
- RENAME - Change the name of a content dictionary.
[]> edit
Enter the number of the dictionary you want to edit:
1. secret_words
[]> 1
Choose the operation you want to perform on dictionary 'secret_words':
- NEW - Create new entries in this dictionary.
- IMPORT - Replace all of the words in this dictionary.
- EXPORT - Export the words in this dictionary.
- DELETE - Remove an entry in this dictionary.
- PRINT - List the entries in this dictionary.
- SETTINGS - Change settings for this dictionary.
[]> export
Enter a name for the exported file:
[]> secret_words_export.txt
```

exceptionconfig

説明

exceptionconfig コマンドを CLI で使用することにより、ドメイン例外テーブルを作成できます。この例では、E メールアドレス「admin@zzzaazzz.com」をドメイン例外テーブルに追加し、ポリシーを「Allow」に設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```

mail3.example.com> exceptionconfig
Choose the operation you want to perform:
- NEW - Create a new domain exception table entry
[]> new
Enter a domain, sub-domain, user, or email address for which you wish to
provide an exception:
[]> mail.partner.com
Any of the following passes:
- @[IP address]
    Matches any email address with this IP address.
- @domain
    Matches any email address with this domain.
- @.partial.domain
    Matches any email address domain ending in this domain.
- user@
    Matches any email address beginning with user@.
- user@domain
    Matches entire email address.
Enter a domain, sub-domain, user, or email address for which you wish to
provide an exception:
[]> admin@zzzaaazzz.com
Choose a policy for this domain exception:
1. Allow
2. Reject
[]> 1
Choose the operation you want to perform:
- NEW - Create a new domain exception table entry
- EDIT - Edit a domain exception table entry
- DELETE - Delete a domain exception table entry
- PRINT - Print all domain exception table entries
- SEARCH - Search domain exception table
- CLEAR - Clear all domain exception entries
[]>

```

filters

説明

メッセージ処理オプションを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

この例では、filter コマンドを使用して 3 つの新しいフィルタを作成します。

- 最初のフィルタの名前は、**big_messages** です。これは body-size ルールを使用して、10 MB より大きいメッセージをドロップします。

- 2 番目のフィルタの名前は、**no_mp3s** です。これは **attachment-filename** ルールを使用して、.mp3 ファイル拡張子が付いた添付ファイルを含むメッセージをドロップします。
- 3 番目のフィルタの名前は、**mailfrompm** です。これは **mail-from** ルールを使用して、**postmaster@example.com** からのメールをすべて調べ、**administrator@example.com** のブラインドカーボンコピーを作成します。

filter -> list サブコマンドを使用し、フィルタのリストを表示して、フィルタがアクティブで有効であることを確認します。次に、**move** サブコマンドを使用して、最初と最後のフィルタの位置を入れ替えます。最後に、変更を確定してフィルタを有効にします。

```
mail3.example.com> filters
Choose the operation you want to perform:
- NEW - Create a new filter.
- IMPORT - Import a filter script from a file.
[]> new
Enter filter script. Enter '.' on its own line to end.
big_messages:
    if (body-size >= 10M) {
        drop();
    }
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
no_mp3s:
    if (attachment-filename == '\\.mp3$') {
        drop();
    }
.
1 filters added.
Choose the operation you want to perform:
- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> new
Enter filter script. Enter '.' on its own line to end.
mailfrompm:
    if (mail-from == "^postmaster$")
    { bcc ("administrator@example.com"); }
.
1 filters added.
Choose the operation you want to perform:
```

```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.
[]> list

```

policyconfig

説明

受信者単位または送信者ベースのポリシーを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

- 一括 E メールまたはソーシャル ネットワークの E メールであると識別されたメッセージをドロップする着信ポリシーの作成 (209 ページ)
- 販売チームのポリシーの作成 (193 ページ)
- エンジニアリング チームのポリシーの作成 (194 ページ)
- scan_for_confidential コンテンツ フィルタの作成 (196 ページ)
- no_mp3s および ex_employee コンテンツ フィルタの作成 (199 ページ)
- 特定のポリシーに対するコンテンツ フィルタのイネーブル化 (203 ページ)
- デフォルトの発信ポリシーの DLP ポリシー (207 ページ)
- スпам メッセージをドロップし、陽性と疑わしいスパム メッセージをアーカイブする着信メール ポリシーの作成 (190 ページ)
- AMP エンジンによってスキャン不能としてマークされたメッセージを処理する着信ポリシーの設定 (210 ページ)

スパム メッセージをドロップし、陽性と疑わしいスパム メッセージをアーカイブする着信メール ポリシーの作成

この例では、policyconfig->edit->antispam サブコマンドを使用して、デフォルトの着信メールポリシーのスパム対策設定を編集します（これと同じ設定が電子メール セキュリティ マネージャ機能の GUI にもあります）。

- まず、スパムとして陽性判定されたメッセージはアーカイブの対象から除外され、ドロップされます。

- スパムの疑いがあるメッセージはアーカイブ対象となります。このようなメッセージは、`quarantine.example.com` というサーバにインストールされたスパム隔離にも送信されます。件名行の先頭にテキスト `[quarantined: possible spam]` が追加され、このような疑わしいメッセージには `X-quarantined: true` という特別なヘッダーが追加されます。このシナリオでは、管理者およびエンドユーザは隔離でないかどうかを確認でき、管理者は必要に応じて疑わしいスパムのしきい値を調整できます。

最後に、変更を確定します。

```
mail3.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 1
Incoming Mail Policy Configuration
```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```
Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[>] edit
```

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1.	DEFAULT	Ironport	Mcafee	N/A	N/A	Off	Enabled

```
Enter the name or number of the entry you wish to edit:
[>] 1
Policy Summaries:
Anti-Spam: IronPort - Deliver, Prepend "[SPAM] " to Subject
Suspect-Spam: IronPort - Deliver, Prepend "[SUSPECTED SPAM] " to Subject
Anti-Virus: Off
Content Filters: Off (No content filters have been created)
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- OUTBREAK - Modify Outbreak Filters policy
[>] antis spam
Choose the operation you want to perform:
- EDIT - Edit Anti-Spam policy
- DISABLE - Disable Anti-Spam policy (Disables all policy-related actions)
[>] edit
Begin Anti-Spam configuration
Some messages will be positively identified as spam. Some messages will be
identified as suspected spam. You can set the IronPort Anti-Spam Suspected Spam Threshold
```

```

below.
The following configuration options apply to messages POSITIVELY identified as spam:
What score would you like to set for the IronPort Anti-Spam spam threshold?
[90]> 90
1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as spam?
[1]> 2
Do you want to archive messages identified as spam? [N]>
Do you want to enable special treatment of suspected spam? [Y]> y
What score would you like to set for the IronPort Anti-Spam suspect spam threshold?
[50]> 50
The following configuration options apply to messages identified as SUSPECTED spam:
1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as SUSPECTED spam?
[1]> 4
Do you want to archive messages identified as SUSPECTED spam? [N]> y
1. PREPEND
2. APPEND
3. NONE
Do you want to add text to the subject of messages identified as SUSPECTED spam?
[1]> 1
What text do you want to prepend to the subject?
[[SUSPECTED SPAM] ]> [quarantined: possible spam]
Do you want to add a custom header to messages identified as SUSPECTED spam? [N]> y
Enter the name of the header:
[]> X-quarantined
Enter the text for the content of the header:
[]> true
Anti-Spam configuration complete
Policy Summaries:
Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Content Filters: Off (No content filters have been created)
Outbreak Filters: Enabled. No bypass extensions.
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- OUTBREAK - Modify Outbreak Filters policy
[]>

```

Name:	Anti-Spam:	Anti-Virus:	Advanced Malware Protection:	Graymail:	Content Filter:	Outbreak Filters:
-----	-----	-----	-----	-----	-----	-----
DEFAULT	Ironport	Mcafee	N/A	N/A	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]>
mail3.example.com> commit
Please enter some comments describing your changes:

```



```
[ ]> configured anti-spam for Incoming Default Policy
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```

販売チームのポリシーの作成

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
DEFAULT	Ironport	Mcafee	N/A	N/A	Off	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters

```
[ ]> new
```

Enter the name for this policy:

```
[ ]> sales_team
```

Begin entering policy members. The following types of entries are allowed:
Username entries such as joe@, domain entries such as @example.com, sub-domain
entries such as @.example.com, LDAP group memberships such as ldap(Engineers)
Enter a member for this policy:

```
[ ]> ldap(sales)
```

Please select an LDAP group query:

1. PublicLDAP.ldapgroup

```
[1]> 1
```

Is this entry a recipient or a sender?

1. Recipient
2. Sender

```
[1]> 1
```

Add another member? [Y]> n

Would you like to enable Anti-Spam support? [Y]> y

Use the policy table default? [Y]> n

Begin Anti-Spam configuration

Some messages will be positively identified as spam. Some messages will be
identified as suspected spam. You can set the IronPort Anti-Spam Suspected Spam Threshold
below.

The following configuration options apply to messages POSITIVELY identified as spam:

What score would you like to set for the IronPort Anti-Spam spam threshold?

```
[90]> 90
```

1. DELIVER
2. DROP
3. BOUNCE
4. IRONPORT QUARANTINE

What do you want to do with messages identified as spam?

```
[1]> 2
```

Do you want to archive messages identified as spam? [N]> n

Do you want to enable special treatment of suspected spam? [Y]> y

What score would you like to set for the IronPort Anti-Spam suspect spam
threshold?

```
[50]> 50
```

The following configuration options apply to messages identified as SUSPECTED
spam:

1. DELIVER
2. DROP

エンジニアリングチームのポリシーの作成

```

3. BOUNCE
4. IRONPORT QUARANTINE
What do you want to do with messages identified as SUSPECTED spam?
[1]> 4
Do you want to archive messages identified as SUSPECTED spam? [N]> n
1. PREPEND
2. APPEND
3. NONE
Do you want to add text to the subject of messages identified as SUSPECTED
spam?
[1]> 3
Do you want to add a custom header to messages identified as SUSPECTED spam? [N]> n
Anti-Spam configuration complete
Would you like to enable Anti-Virus support? [Y]> y
Use the policy table default? [Y]> y
Would you like to enable Outbreak Filters for this policy? [Y]> y
Use the policy table default? [Y]> y
Incoming Mail Policy Configuration

```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>

```

次に、エンジニアリングチーム（3人のEメール受信者）のポリシーを作成し、.dwg ファイルをアウトブレイク フィルタ スキャンの対象外に指定します。

エンジニアリングチームのポリシーの作成

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy

```

```
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> new
Enter the name for this policy:
[]> engineering
Begin entering policy members. The following types of entries are allowed:
Username entries such as joe@, domain entries such as @example.com, sub-domain entries
such as @.example.com,
LDAP group memberships such as ldap(Engineers)
Enter a member for this policy:
[]> bob@example.com
Is this entry a recipient or a sender?
1. Recipient
2. Sender
[1]> 1
Add another member? [Y]> y
Enter a member for this policy:
[]> fred@example.com
Is this entry a recipient or a sender?
1. Recipient
2. Sender
[1]> 1
Add another member? [Y]> y
Enter a member for this policy:
[]> joe@example.com
Is this entry a recipient or a sender?
1. Recipient
2. Sender
[1]> 1
Add another member? [Y]> n
Would you like to enable Anti-Spam support? [Y]> y
Use the policy table default? [Y]> y
Would you like to enable Anti-Virus support? [Y]> y
Use the policy table default? [Y]> y
Would you like to enable Outbreak Filters for this policy? [Y]> y
Use the policy table default? [Y]> n
Would you like to modify the list of file extensions that bypass
Outbreak Filters? [N]> y
Choose the operation you want to perform:
- NEW - Add a file extension
[]> new
Enter a file extension:
[]> dwg
Choose the operation you want to perform:
- NEW - Add a file extension
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]> print
The following file extensions will bypass Outbreak Filter processing:
dwg
Choose the operation you want to perform:
- NEW - Add a file extension
- DELETE - Delete a file extension
- PRINT - Display all file extensions
- CLEAR - Clear all file extensions
[]>
Incoming Mail Policy Configuration
```

scan_for_confidential コンテンツ フィルタの作成

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies

[]>

次に、[受信メール概要ポリシー（Incoming Mail Overview policy）] テーブルで使用する 3 つの新しいコンテンツ フィルタを作成します。

CLI では、policyconfig コマンドの filters サブコマンドは [受信コンテンツ フィルタ（Incoming Content Filters）] GUI ページと同じ機能を持ちます。CLI でコンテンツ フィルタを作成するときには、save サブコマンドを使用してフィルタを保存し、policyconfig コマンドに戻る必要があります。

まず、scan_for_confidential コンテンツ フィルタを作成します。

scan_for_confidential コンテンツ フィルタの作成

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy

```

- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> filters
No filters defined.
Choose the operation you want to perform:
- NEW - Create a new filter
[]> new
Enter a name for this filter:
[]> scan_for_confidential
Enter a description or comment for this filter (optional):
[]> scan all incoming mail for the string 'confidential'
Filter Name: scan_for_confidential
Conditions:
Always Run
Actions:
No actions defined yet.
Description:
scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[]> add
1. Condition
2. Action
[1]> 1
1. Message Body Contains
2. Only Body Contains (Attachments are not scanned)
3. Message Body Size
4. Subject Header
5. Other Header
6. Attachment Contains
7. Attachment File Type
8. Attachment Name
9. Attachment MIME Type
10. Attachment Protected
11. Attachment Unprotected
12. Attachment Corrupt
13. Envelope Recipient Address
14. Envelope Recipient in LDAP Group
15. Envelope Sender Address
16. Envelope Sender in LDAP Group
17. Reputation Score
18. Remote IP
19. DKIM authentication result
20. SPF verification result
[1]> 1
Enter regular expression or smart identifier to search message contents for:
[]> confidential
Threshold required for match:
[1]> 1
Filter Name: scan_for_confidential
Conditions:
body-contains("confidential", 1)
Actions:
No actions defined yet.
Description:
scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- RENAME - Rename this filter

```

```

- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 1
Enter the email address(es) to send the Bcc message to:
[]> hr@example.com
Do you want to edit the subject line used on the Bcc message? [N]> y
Enter the subject to use:
[$Subject]> [message matched confidential filter]
Do you want to edit the return path of the Bcc message? [N]> n
Filter Name: scan_for_confidential
Conditions:
body-contains("confidential", 1)
Actions:
bcc ("hr@example.com", "[message matched confidential filter]")
Description:
scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type

```

```

12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 14
1. Policy
[1]> 1
Filter Name: scan_for_confidential
Conditions:
body-contains("confidential", 1)
Actions:
bcc ("hr@example.com", "[message matched confidential filter]")
quarantine ("Policy")
Description:
scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- MOVE - Reorder the conditions or actions
- SAVE - Save filter
[> save
Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- RENAME - Rename a filter
[>

```

no_mp3s および ex_employee コンテンツ フィルタの作成

```

Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- RENAME - Rename a filter
[> new
Enter a name for this filter:
[> no_mp3s
Enter a description or comment for this filter (optional):
[> strip all MP3 attachments
Filter Name: no_mp3s
Conditions:
Always Run
Actions:
No actions defined yet.
Description:
strip all MP3 attachments
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description

```

```

- ADD - Add condition or action
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 12
Enter the file type to strip:
[]> mp3
Do you want to enter specific text to use in place of any stripped attachments?[N]> n
Filter Name: no_mp3s
Conditions:
Always Run
Actions:
drop-attachments-by-filetype("mp3")
Description:
strip all MP3 attachments
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- SAVE - Save filter
[]> save
Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments
Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter
[]> new
Enter a name for this filter:
[]> ex_employee
Enter a description or comment for this filter (optional):
[]> bounce messages intended for Doug
Filter Name: ex_employee
Conditions:
Always Run
Actions:
No actions defined yet.

```



```

Description:
bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
[]> add
1. Condition
2. Action
[1]> 1
1. Message Body Contains
2. Only Body Contains (Attachments are not scanned)
3. Message Body Size
4. Subject Header
5. Other Header
6. Attachment Contains
7. Attachment File Type
8. Attachment Name
9. Attachment MIME Type
10. Attachment Protected
11. Attachment Unprotected
12. Attachment Corrupt
13. Envelope Recipient Address
14. Envelope Recipient in LDAP Group
15. Envelope Sender Address
16. Envelope Sender in LDAP Group
17. Reputation Score
18. Remote IP
19. DKIM authentication result
20. SPF verification result
[1]> 13
Enter regular expression to search Recipient address for:
[]> doug
Filter Name:  ex_employee
Conditions:
rcpt-to == "doug"
Actions:
No actions defined yet.
Description:
bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine

```

```

16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 2
Enter the email address(es) to send the notification to:
[]> joe@example.com
Do you want to edit the subject line used on the notification? [N]> y
Enter the subject to use:
[]> message bounced for ex-employee of example.com
Do you want to edit the return path of the notification? [N]> n
Do you want to include a copy of the original message as an attachment to the
notification? [N]> y
Filter Name: ex_employee
Conditions:
rcpt-to == "doug"
Actions:
notify-copy ("joe@example.com", "message bounced for ex-employee of
example.com")
Description:
bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> add
1. Condition
2. Action
[1]> 2
1. Bcc
2. Notify
3. Redirect To Alternate Email Address
4. Redirect To Alternate Host
5. Insert A Custom Header
6. Insert A Message Tag
7. Strip A Header
8. Send From Specific IP Interface
9. Drop Attachments By Content
10. Drop Attachments By Name
11. Drop Attachments By MIME Type
12. Drop Attachments By File Type
13. Drop Attachments By Size
14. Send To System Quarantine
15. Duplicate And Send To System Quarantine
16. Add Log Entry
17. Drop (Final Action)
18. Bounce (Final Action)
19. Skip Remaining Content Filters (Final Action)
20. Encrypt (Final Action)
21. Encrypt on Delivery
22. Skip Outbreak Filters check
[1]> 18
Filter Name: ex_employee
Conditions:
rcpt-to == "doug"
Actions:
notify-copy ("joe@example.com", "message bounced for ex-employee of
example.com")
bounce()

```

```

Description:
bounce messages intended for Doug
Choose the operation you want to perform:
- RENAME - Rename this filter
- DESC - Edit filter description
- ADD - Add condition or action
- DELETE - Delete condition or action
- SAVE - Save filter
[]> save
Defined filters:
1. scan_for_confidential: scan all incoming mail for the string 'confidential'
2. no_mp3s: strip all MP3 attachments
3. ex_employee: bounce messages intended for Doug
Choose the operation you want to perform:
- NEW - Create a new filter
- EDIT - Edit an existing filter
- DELETE - Delete a filter
- PRINT - Print all filters
- MOVE - Reorder a filter
- RENAME - Rename a filter
[]>
Incoming Mail Policy Configuration

```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>

```

特定のポリシーに対するコンテンツ フィルタのイネーブル化

次に示すのは、もう一度ポリシーをイネーブルにして一部のポリシーのコンテンツ フィルタだけをイネーブルにする方法です。

Incoming Mail Policy Configuration

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----

sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Choose the operation you want to perform:

- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies

[> edit

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1.	sales_team	IronPort	Default	Default	Default	Default	Default
2.	engineering	Default	Default	Default	Default	Default	Enabled
3.	DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

Enter the name or number of the entry you wish to edit:

[> 3

Policy Summaries:

Anti-Spam: IronPort - Drop

Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.

Anti-Virus: McAfee - Scan and Clean

Graymail Detection: Unsubscribe - Disabled

Content Filters: Off

Outbreak Filters: Enabled. No bypass extensions.

Choose the operation you want to perform:

- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters

[> filters

Choose the operation you want to perform:

- ENABLE - Enable Content Filters policy

[> enable

1. scan_for_confidential

2. no_mp3s

3. ex_employee

Enter the filter to toggle on/off, or press enter to finish:

[> 1

1. Active scan_for_confidential

2. no_mp3s

```

3.          ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 2
1. Active scan_for_confidential
2. Active no_mp3s
3.          ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3
1. Active scan_for_confidential
2. Active no_mp3s
3. Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>
Policy Summaries:
Anti-Spam: IronPort - Drop
Suspect-Spam: IronPort - Quarantine - Archiving copies of the original message.
Anti-Virus: McAfee - Scan and Clean
Graymail Detection: Unsubscribe - Disabled
Content Filters: Enabled. Filters: scan_for_confidential, no_mp3s, ex_employee
Outbreak Filters: Enabled. No bypass extensions.
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]>
Incoming Mail Policy Configuration

```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Default	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Enabled	Enabled

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]> edit

```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----

1	sales_team	IronPort	Default	Default	Default	Default	Default
2	engineering	Default	Default	Default	Default	Default	Enabled
3	DEFAULT	Ironport	Mcafee	N/A	Off	Off	Enabled

```

Enter the name or number of the entry you wish to edit:
[]> 2
Policy Summaries:
Anti-Spam: Default
Anti-Virus: Default
Graymail Detection: Unsubscribe - Default
Content Filters: Default
Outbreak Filters: Enabled. Bypass extensions: dwg
Choose the operation you want to perform:
- NAME - Change name of policy
- NEW - Add a new member
- DELETE - Remove a member
- PRINT - Print policy members
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- FILTERS - Modify filters
[]> filters
Choose the operation you want to perform:
- DISABLE - Disable Content Filters policy (Disables all policy-related
actions)
- ENABLE - Enable Content Filters policy
[]> enable
1. scan_for_confidential
2. no_mp3s
3. ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 1
1. Active scan_for_confidential
2. no_mp3s
3. ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]> 3
1. Active scan_for_confidential
2. no_mp3s
3. Active ex_employee
Enter the filter to toggle on/off, or press enter to finish:
[]>
Policy Summaries:
Anti-Spam: Default
Anti-Virus: Default
Graymail Detection: Unsubscribe - Default
Content Filters: Enabled. Filters: scan_for_confidential, ex_employee
Outbreak Filters: Enabled. Bypass extensions: dwg
Choose the operation you want to perform:
- NAME - Change name of policy
- NEW - Add a new member
- DELETE - Remove a member
- PRINT - Print policy members
- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy

```

```
- FILTERS - Modify filters
[]>
Incoming Mail Policy Configuration
```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
sales_team	IronPort	Default	Default	Default	Default	Default
engineering	Default	Default	Default	Default	Enabled	Enabled
DEFAULT	Ironport	Mcafee	N/A	Off	Enabled	Enabled

```
Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- DELETE - Remove a policy
- PRINT - Print all policies
- SEARCH - Search for a policy by member
- MOVE - Move the position of a policy
- FILTERS - Edit content filters
- CLEAR - Clear all policies
[]>
```



(注) この CLI には、個々のポリシーに新しいコンテンツ フィルタを追加する機能はありません。
filters サブコマンドでは、policyconfig コマンドの 1 つのサブセクションからすべてのコンテンツ
フィルタを管理することになります。そのため、この例では drop_large_attachments の追加
を省略しています。

デフォルトの発信ポリシーの DLP ポリシー

次に、デフォルトの発信ポリシーで DLP ポリシーをイネーブルにする方法を示します。

```
mail3.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 2
Outgoing Mail Policy Configuration
```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----	DLP: -----
DEFAULT	N/A	N/A	N/A	Off	Off	Off	Off

```
Choose the operation you want to perform:
- NEW - Create a new policy
```

デフォルトの発信ポリシーの DLP ポリシー

```
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[> edit
```

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----	DLP: -----
1	DEFAULT	N/A	N/A	N/A	Off	Off	Off	Off

Enter the name or number of the entry you wish to edit:

```
[> 1
```

Policy Summaries:

Anti-Spam: Off

Anti-Virus: Off

Graymail Detection: Unsubscribe - Disabled

Content Filters: Off (No content filters have been created)

Outbreak Filters: Off

DLP: Off

Choose the operation you want to perform:

- ANTISPAM - Modify Anti-Spam policy
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- DLP - Modify DLP policy

```
[> dlp
```

Choose the operation you want to perform:

- ENABLE - Enable DLP policy

```
[> enable
```

1. California AB-1298
2. Suspicious Transmission - Zip Files
3. Restricted Files

Enter the policy to toggle on/off, or press enter to finish:

```
[> 1
```

1. Active California AB-1298
2. Suspicious Transmission - Zip Files
3. Restricted Files

Enter the policy to toggle on/off, or press enter to finish:

```
[> 2
```

1. Active California AB-1298
2. Active Suspicious Transmission - Zip Files
3. Restricted Files

Enter the policy to toggle on/off, or press enter to finish:

```
[> 3
```

1. Active California AB-1298
2. Active Suspicious Transmission - Zip Files
3. Active Restricted Files

Enter the policy to toggle on/off, or press enter to finish:

```
[>
```

Policy Summaries:

Anti-Spam: Off

Anti-Virus: Off

Graymail Detection: Unsubscribe - Disabled

Content Filters: Off (No content filters have been created)

Outbreak Filters: Off

DLP: Enabled. Policies: California AB-1298, Suspicious Transmission - Zip Files, Restricted Files

Choose the operation you want to perform:

- ANTISPAM - Modify Anti-Spam policy


```
- ANTIVIRUS - Modify Anti-Virus policy
- GRAYMAIL - Modify Graymail policy
- OUTBREAK - Modify Outbreak Filters policy
- DLP - Modify DLP policy
[]>
```

一括 E メールまたはソーシャル ネットワークの E メールであると識別されたメッセージをドロップする着信ポリシーの作成

```
mail.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 1
Incoming Mail Policy Configuration
```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
DEFAULT	Off	N/A	N/A	Off	Off	N/A

```
Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[]> edit
```

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1.	DEFAULT	Off	N/A	N/A	Off	Off	N/A

```
Enter the name or number of the entry you wish to edit:
[]> 1
Policy Summaries:
Anti-Spam: Off
Graymail Detection: Off
Content Filters: Off (No content filters have been created)
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- GRAYMAIL - Modify Graymail policy
- FILTERS - Modify filters
[]> graymail
Choose the operation you want to perform:
- ENABLE - Enable Graymail policy
[]> enable
Begin Graymail configuration
Do you want to enable Safe Unsubscribe? [N]> y
Do you want to perform Safe Unsubscribe action only for unsigned messages (recommended)?
[Y]>
Do you want to enable actions on messages identified as Marketing Email? [N]>
Do you want to enable actions on messages identified as Social Networking Email? [N]> y
1. DELIVER
```

AMP エンジンによってスキャン不能としてマークされたメッセージを処理する着信ポリシーの設定

```

2. DROP
3. BOUNCE
What do you want to do with messages identified as Social Networking Email?
[1]> 2
Do you want to archive messages identified as Social Networking Email? [N]>
Do you want to enable actions on messages identified as Bulk Email? [N]> y
1. DELIVER
2. DROP
3. BOUNCE
What do you want to do with messages identified as Bulk Email?
[1]> 2
Do you want to archive messages identified as Bulk Email? [N]>
Graymail configuration complete.
Policy Summaries:
Anti-Spam: Off
Graymail Detection: Unsubscribe - Enabled
    Social Networking mails : Drop
    Bulk mails : Drop
Content Filters: Off (No content filters have been created)
Choose the operation you want to perform:
- ANTISPAM - Modify Anti-Spam policy
- GRAYMAIL - Modify Graymail policy
- FILTERS - Modify filters
[ ]>

```

AMP エンジンによってスキャン不能としてマークされたメッセージを処理する着信ポリシーの設定

```

mail.example.com> policyconfig
Would you like to configure Incoming or Outgoing Mail Policies?
1. Incoming
2. Outgoing
[1]> 1
Incoming Mail Policy Configuration

```

Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
DEFAULT	Off	N/A	N/A	Off	Off	N/A

```

Choose the operation you want to perform:
- NEW - Create a new policy
- EDIT - Edit an existing policy
- PRINT - Print all policies
- FILTERS - Edit content filters
[ ]> edit

```

	Name: -----	Anti-Spam: -----	Anti-Virus: -----	Advanced Malware Protection: -----	Graymail: -----	Content Filter: -----	Outbreak Filters: -----
1.	DEFAULT	Off	N/A	N/A	Off	Off	N/A

```

Enter the name or number of the entry you wish to edit:
[ ]> 1
Policy Summaries:

```

```

Advanced Malware Protection: Malware Action - drop , Message Error Unscannable Action -
  deliver , Rate Limit Unscannable Action - deliver , AMP Service Not
Available Unscannable Action - deliver , File Analysis Action - Deliver , Mailbox Auto
Remediation (MAR) - Disabled
Content Filters: Off
Outbreak Filters: Off

Choose the operation you want to perform:
- OUTBREAK - Modify Outbreak Filters policy
- ADVANCEDMALWARE - Modify Advanced Malware Protection policy
- FILTERS - Modify filters
[> advancedmalware

Choose the operation you want to perform:
- EDIT - Edit Advanced-Malware protection policy
- DISABLE - Disable Advanced-Malware protection policy (Disables all policy-related
actions)
[> edit

Begin AMP configuration

Do you want to enable File Analysis? [Y]>

Do you like the system to automatically insert an X-header with the anti-malware scanning
results? (Recommended for trouble-shooting) [Y]>

Unscannable Message Handling

Current actions to take if any of the attachments could not be scanned due to message
errors:
- WARNING: Delivering Unscannable due to Message Errors messages normally
- Prepending subjects with "[WARNING: ATTACHMENT UNSCANNED]"
- Archiving copies of the original message.
Do you want to edit the actions for Unscannable Message due to message errors? [N]> yes

Current actions to take if any of the attachments could not be scanned due to rate limit
hit:
- WARNING: Delivering Unscannable due to Rate Limit messages normally
- Prepending subjects with "[WARNING: ATTACHMENT UNSCANNED]"
- Archiving copies of the original message.
Do you want to edit the actions for Unscannable Message due to rate limit hit? [N]> yes

Current actions to take if any of the attachments could not be scanned due to AMP Service
not available:
- WARNING: Delivering Unscannable due to AMP Service Not Available messages normally
- Prepending subjects with "[WARNING: ATTACHMENT UNSCANNED]"
- Archiving copies of the original message.
Do you want to edit the actions for Unscannable Message due to AMP Service not available?
[N]> yes

```

例: [差出人 (From)] ヘッダーの優先度の設定

次の例では、`policyconfig > match headers` 優先順位サブ コマンドを使用して、アプライアンスで着信および発信メッセージを照合するための、[差出人 (From)] メッセージヘッダーの優先順位を設定します。

```
mail1.example.com > policyconfig
```

```
Would you like to configure Incoming Mail Policy or Outgoing Mail Policies or
Match Headers Priority?
```

```
1. Incoming Mail Policies
```

```

2. Outgoing Mail Policies
3. Match Headers Priority
[1]> 3

Match Headers Priority Configuration
Priority:      Headers:
-----      -
P1            Envelope Sender

Choose the operation you want to perform:
- ADD - Add match priority for headers
- EDIT - Edit an existing match priority for headers
- REMOVE - Remove an existing match priority for headers
[1]> add

Choose headers for priority 2
Add header "From" Header:
1. Yes
2. No
[1]> 1

Add header "Reply-To" Header:
1. Yes
2. No
[1]> 2

Add header "Sender" Header:
1. Yes
2. No
[1]> 2

Match Headers Priority Configuration
Priority:      Headers:
-----      -
P1            Envelope Sender
P2            "From" Header

```

quarantineconfig

説明

システムの隔離を設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```

mail3.example.com> quarantineconfig
Currently configured quarantines:
#  Quarantine Name      Size (MB)  % full  Messages  Retention  Policy
1  Outbreak              3,072      0.0      1         12h      Release

```

```

2 Policy          1,024      0.1      497      10d      Delete
3 Virus           2,048      empty      0      30d      Delete
2,048 MB available for quarantine allocation.
Choose the operation you want to perform:
- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- OUTBREAKMANAGE - Manage the Outbreak Filters quarantine.
[]> new
Please enter the name for this quarantine:
[]> HRQuarantine
Retention period for this quarantine. (Use 'd' for days or 'h' for hours or 'm' for
'minutes'.):
[]> 15d
1. Delete
2. Release
Enter default action for quarantine:
[1]> 2
Do you want to modify the subject of messages that are released because
"HRQuarantine" overflows? [N]>
Do you want add a custom header to messages that are released because
"HRQuarantine" overflows? [N]>
Do you want to strip all attachments from messages that are released
because "HRQuarantine" overflows? [N]>
Do you want default action to apply automatically when quarantine space fills up? [Y]>
Currently configured quarantines:
#  Quarantine Name      Size (MB) % full  Messages  Retention  Policy
1  HRQuarantine         1,024    N/A      N/A       15d      Release
2  Outbreak             3,072    0.0      1         12h      Release
3  Policy               1,024    0.1      497       10d      Delete
4  Virus                2,048    empty     0         30d      Delete
(N/A: Quarantine contents is not available at this time.)
1,024 MB available for quarantine allocation.
Choose the operation you want to perform:
- NEW - Create a new quarantine.
- EDIT - Modify a quarantine.
- DELETE - Remove a quarantine.
- OUTBREAKMANAGE - Manage the Outbreak Filters quarantine.

```

ユーザと隔離

ユーザの追加に関する質問に“y”つまり「はい」と答えると、ユーザ管理が開始され、ユーザリストを管理できます。これにより、隔離設定に関する他の質問に答えなくても隔離に対して複数のユーザを追加または削除できます。ユーザ管理セクションから出て隔離の設定を続行するには、空のプロンプト（[]>）で Enter を押します。



(注) システム上にゲスト ユーザまたはオペレータ ユーザが作成されている場合は、ユーザへの隔離に対するアクセスの付与だけが要求されます。

隔離のユーザ リストには、Operators グループまたは Guests グループに属するユーザだけが含まれます。Administrators グループ内のユーザは、常に隔離に対してすべてのアクセス権限を持ちます。ユーザ リストを管理するときには、すべてのオペレータ/ゲスト ユーザがすでに隔離のユーザ リストに含まれている場合、NEW コマンドは使用不可となります。同様に、削除の対象となるユーザが存在しない場合、DELETE コマンドは使用不可となります。

scanconfig

説明

添付ファイルのスキャン ポリシーを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

例

この例では、scanconfig コマンドで以下のパラメータを設定します。

- video/*、audio/*、image/* の MIME タイプはスキップされます（コンテンツはスキャンされません）。
- ネストされた（再帰的な）アーカイブ添付ファイルは、最大 10 レベルまでスキャンされます。（デフォルトは 5 レベル）。
- スキャンされる添付ファイルの最大サイズは、25MB です。これより大きいファイルはすべてスキップされます。（デフォルトは 5 MB）。
- ドキュメントのメタデータがスキャンされます。
- 添付ファイルのスキャンのタイムアウトは、180 秒に設定されます。
- スキャンされなかった添付ファイルは、検索パターンに一致しないと見なされます。（デフォルトの動作）。
- プレーン テキストの本文や MIME タイプの plain/text または plain/html 部分に何も指定されていない場合は、ASCII エンコードが使用されます。



(注) [assume the attachment matches the search pattern] を「Y」に設定すると、スキャンできないメッセージはメッセージ フィルタ ルールによって true と評価されます。これにより、辞書に一致しないメッセージの検疫など、予想外の動作が発生することがあります。このようなメッセージは、コンテンツが正しくスキャンできないという理由で検疫されていました。この設定は DLP スキャンには適用されません。

```
mail3.example.com> scanconfig
There are currently 5 attachment type mappings configured to be SKIPPED.
Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
```

```

- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
[> setup
1. Scan only attachments with MIME types or fingerprints in the list.
2. Skip attachments with MIME types or fingerprints in the list.
Choose one:
[2]> 2
Enter the maximum depth of attachment recursion to scan:
[5]> 10
Enter the maximum size of attachment to scan:
[5242880]> 10m
Do you want to scan attachment metadata? [Y]> y
Enter the attachment scanning timeout (in seconds):
[30]> 180
If a message has attachments that were not scanned for any reason (e.g.
because of size, depth limits, or scanning timeout), assume the attachment matches the
search pattern? [N]> n
If a message could not be deconstructed into its component parts in order to remove
specified attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[1]>
Configure encoding to use when none is specified for plain body text or
anything with MIME type plain/text or plain/html.
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[1]> 1
Scan behavior changed.
There are currently 5 attachment type mappings configured to be SKIPPED.
Choose the operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
- SMIME - Configure S/MIME unpacking.
[> print
1. Fingerprint    Image
2. Fingerprint    Media
3. MIME Type      audio/*
4. MIME Type      image/*
5. MIME Type      video/*

```

例：スキャンできないメッセージのメッセージ処理アクションの設定

次の例では、scanconfig > setup コマンドを使用して、添付ファイルの抽出に失敗したために、コンテンツスキャナによってスキャンされないメッセージのメッセージ処理アクションを有効にし、設定します。

例：スキャンできないメッセージのメッセージ処理アクションの設定

```

mail3.example.com> scanconfig
There are currently 5 attachment type mappings configured to be SKIPPED. Choose the
operation you want to perform:
- NEW - Add a new entry.
- DELETE - Remove an entry.
- SETUP - Configure scanning behavior.
- IMPORT - Load mappings from a file.
- EXPORT - Save mappings to a file.
- PRINT - Display the list.
- CLEAR - Remove all entries.
-[]>SMIMEsetup- Configure S/MIME unpacking.
[] > setup

1. Scan only attachments with MIME types or fingerprints in the list.
2. Skip attachments with MIME types or fingerprints in the list.

Choose one: [2]>

Enter the maximum depth of attachment recursion to scan: [5]>

Enter the maximum size of attachment to scan: [5242880]>

Do you want to scan attachment metadata? [Y]>

Enter the attachment scanning timeout (in seconds): [30]>

If a message has attachments that were not scanned for any reason (e.g.
because of size, depth limits, or scanning timeout), assume the attachment matches the
search pattern? [N]>

In case of a content or message filter error, should all filters be bypassed? [Y]>

Assume zip file to be unscannable if files in the archive cannot be read? [0]>

If a message could not be deconstructed into its component parts in order
to remove specified attachments, the system should:
1. Deliver
2. Bounce
3. Drop
[1]>

Configure encoding to use when none is specified for
plain body text or anything with MIME type plain/text or plain/html.

1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)

[]> Do you want to enable actions on unscannable messages due to an extraction failure?
y/n [Y]> Yes

1. Drop Message
2. Deliver As Is
3. Quarantine

```



```

Action applied to original message: [2]> 2

Do you want to deliver mail to an alternate mailhost ? [N]> yes

Enter the mailhost to deliver to: []> mail.example.com

Do you want to redirect mail to an alternate email address ? [N]> yes

Enter the address to deliver to:
[]> user@mail.example.com

Do you want to add a custom header? [N]> yes

Enter the header name: []> Unscannable Messages

Enter the header content:
[]> Actions taken on Unscannable Messages

Do you want to modify the subject? [N]> yes

1. Prepend
2. Append

Select position of text: [1]> 1

Enter the text to add:
[[WARNING: UNSCANNABLE EXTRACTION FAILED]]> [WARNING: UNSCANNABLE FILE EXTRACTION FAILURE]

```

stripheaders

説明

削除するメッセージヘッダーのリストを定義します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```

mail3.example.com> stripheaders
Not currently stripping any headers.
Choose the operation you want to perform:
- SETUP - Set message headers to remove.
[]> setup
Enter the list of headers you wish to strip from the messages before they are delivered.
Separate multiple headers with commas.
[]> Delivered-To
Currently stripping headers: Delivered-To
Choose the operation you want to perform:
- SETUP - Set message headers to remove.

```

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

textconfig

説明

DLP、バウンス、暗号化通知を含め、アンチウイルス アラート テンプレート、メッセージ免責事項、通知テンプレートなどのテキスト リソースを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

textconfig -> NEW を使用してテキスト リソースを作成し、**textconfig > delete** を使用してテキスト リソースを削除します。

```
mail3.example.com> textconfig
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
[ ]> new
What kind of text resource would you like to create?
1. Anti-Virus Container Template
2. Anti-Virus Notification Template
3. DLP Notification Template
4. Bounce and Encryption Failure Notification Template
5. Message Disclaimer
6. Encryption Notification Template (HTML)
7. Encryption Notification Template (text)
8. Notification Template
[1]> 5
Please create a name for the message disclaimer:
[ ]> disclaimer 1
Enter the encoding for the message disclaimer:
1. US-ASCII
2. Unicode (UTF-8)
3. Unicode (UTF-16)
4. Western European/Latin-1 (ISO 8859-1)
5. Western European/Latin-1 (Windows CP1252)
6. Traditional Chinese (Big 5)
7. Simplified Chinese (GB 2312)
8. Simplified Chinese (HZ GB 2312)
9. Korean (ISO 2022-KR)
10. Korean (KS-C-5601/EUC-KR)
11. Japanese (Shift-JIS (X0123))
12. Japanese (ISO-2022-JP)
13. Japanese (EUC)
[1]>
Enter or paste the message disclaimer here. Enter '.' on a blank line to end.
```

This message was sent from an IronPort(tm) Email Security appliance.

```
.
Message disclaimer "disclaimer 1" created.
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[> delete
Please enter the name or number of the resource to delete:
[> 1
Message disclaimer "disclaimer 1" has been deleted.
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
[>
```

textconfig -> EDITを使用して既存のテキストリソースを変更します。エンコードを変更したり、選択したテキストリソースのテキストを置換したりできます。

テキストリソースのインポート

テキストファイルをテキストリソースとしてインポートするには、**textconfig -> IMPORT**を使用します。インポートするテキストファイルは、アプライアンス上のconfigurationディレクトリに存在する必要があります。

```
mail3.example.com> textconfig
Current Text Resources:
1. footer.2.message (Message Footer)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[> import
What kind of text resource would you like to create?
1. Anti-Virus Container Template
2. Anti-Virus Notification Template
3. DLP Notification Template
4. Bounce and Encryption Failure Notification Template
5. Message Disclaimer
6. Encryption Notification Template (HTML)
7. Encryption Notification Template (text)
8. Notification Template
[1]> 8
Please create a name for the notification template:
[> strip.mp3files
Enter the name of the file to import:
[> strip.mp3.txt
Enter the encoding to use for the imported file:
1. US-ASCII
[ list of encodings ]
[1]>
Notification template "strip.mp3files" created.
Current Text Resources:
```

```

1. disclaimer.2.message (Message Disclaimer)
2. strip.mp3files (Notification Template)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]>

```

テキストリソースのエクスポート

テキストリソースをテキストファイルとしてエクスポートするには、**textconfig -> EXPORT**を使用します。テキストファイルは、アプライアンス上のconfigurationディレクトリに作成されます。

```

mail3.example.com> textconfig
Current Text Resources:
1. footer.2.message (Message Footer)
2. strip.mp3 (Notification Template)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]> export
Please enter the name or number of the resource to export:
[]> 2
Enter the name of the file to export:
[strip.mp3]> strip.mp3.txt
Enter the encoding to use for the exported file:
1. US-ASCII
[ list of encoding types ]
[1]>
File written on machine "mail3.example.com" using us-ascii encoding.
Current Text Resources:
1. footer.2.message (Message Footer)
2. strip.mp3 (Notification Template)
Choose the operation you want to perform:
- NEW - Create a new text resource.
- IMPORT - Import a text resource from a file.
- EXPORT - Export text resource to a file.
- PRINT - Display the content of a resource.
- EDIT - Modify a resource.
- DELETE - Remove a resource from the system.
- LIST - List configured resources.
[]>

```

ロギングとアラート

ここでは、次のCLIコマンドについて説明します。

- [alertconfig \(221 ページ\)](#)

- [displayalerts](#) (222 ページ)
- [findevent](#) (223 ページ)
- [grep](#) (225 ページ)
- [logconfig](#) (226 ページ)
- [rollovernow](#) (232 ページ)
- [snmpconfig](#) (233 ページ)
- [tail](#) (235 ページ)

alertconfig

説明

電子メール アラートを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例：新しいアラートの作成

この例では、新しいアラート受信者（`alertadmin@example.com`）を作成し、重大度が **Critical** である、システム、ハードウェア、およびディレクトリハーベスト攻撃のアラートを受け取るように設定します。

```
vm30esa0086.ibqa> alertconfig
Not sending alerts (no configured addresses)
Alerts will be sent using the system-default From Address.
Cisco IronPort AutoSupport: Disabled
Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[]> new
Please enter a new email address to send alerts.
(Ex: "administrator@example.com")
[]> alertadmin@example.com
Choose the Alert Classes. Separate multiple choices with commas.
1. All
2. System
3. Hardware
4. Updater
5. Outbreak Filters
6. Anti-Virus
7. Anti-Spam
8. Directory Harvest Attack Prevention
9. Release and Support Notifications
[1]> 2,3,8
Select a Severity Level. Separate multiple choices with commas.
```

```

1. All
2. Critical
3. Warning
4. Information
[1]> 2
Sending alerts to:
  alertadmin@example.com
    Class: Hardware - Severities: Critical
    Class: Directory Harvest Attack Prevention - Severities: Critical
    Class: System - Severities: Critical
Initial number of seconds to wait before sending a duplicate alert: 300
Maximum number of seconds to wait before sending a duplicate alert: 3600
Maximum number of alerts stored in the system are: 50
Alerts will be sent using the system-default From Address.
Cisco IronPort AutoSupport: Disabled
Choose the operation you want to perform:
- NEW - Add a new email address to send alerts.
- EDIT - Modify alert subscription for an email address.
- DELETE - Remove an email address.
- CLEAR - Remove all email addresses (disable alerts).
- SETUP - Configure alert settings.
- FROM - Configure the From Address of alert emails.
[1]>

```

displayalerts

説明

アプライアンスから送信された最後の **n** 個のアラートを表示します

使用方法

確定 : このコマンドに「commit」は必要ありません。

クラスタ管理 : このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```

> displayalerts
Date and Time Stamp      Description
-----
10 Mar 2015 11:33:36 +0000  The updater could not validate the server certificate.
Server certificate not validated - unable to get local issuer
certificate
Last message occurred 28 times between Tue Mar 10 10:34:57 2015 and Tue Mar 10 11:32:24
2015.
10 Mar 2015 11:23:39 +0000  The updater has been unable to communicate with the update
server for at least 1h.
Last message occurred 8 times between Tue Mar 10 10:29:57 2015 and Tue Mar 10 11:18:24
2015.
10 Mar 2015 10:33:36 +0000  The updater could not validate the server certificate.
Server certificate not validated - unable to get local issuer
certificate
Last message occurred 26 times between Tue Mar 10 09:33:55 2015 and Tue Mar 10 10:29:57
2015.

```

```
10 Mar 2015 10:23:39 +0000      The updater has been unable to communicate with the update
server for at least 1h.
Last message occurred 9 times between Tue Mar 10 09:26:54 2015 and Tue Mar 10 10:22:56
2015.
```

findevent

説明

メール ログ ファイルのイベントを検索します

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例：エンベロープ送信者による検索

```
mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 1
Enter the regular expression to search for.
[]> "
Currently configured logs:
-----
Log Name          Log Type          Retrieval          Interval
-----
1. mail_logs      IronPort Text Mail Logs      Manual Download      None
Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 3
No matching message IDs were found
```

例：メッセージ ID による検索

```
mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 2
Enter the Message ID (MID) to search for.
[]> 1
Currently configured logs:
```

例：件名による検索

Log Name	Log Type	Retrieval	Interval
1. mail_logs	IronPort Text Mail Logs	Manual Download	None

Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 1

例：件名による検索

```
mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 3
Enter the regular expression to search for.
[]> "
Currently configured logs:
```

Log Name	Log Type	Retrieval	Interval
1. mail_logs	IronPort Text Mail Logs	Manual Download	None

Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file
[3]> 2
Available mail log files, listed by log file start time.
Specify multiple log files by separating with commas or specify a range with a dash:
1. Thu Feb 19 05:18:02 2015
[1]>
No matching message IDs were found

例：エンベロープ受信者による検索

```
mail.example.com> findevent
Please choose which type of search you want to perform:
1. Search by envelope FROM
2. Search by Message ID
3. Search by Subject
4. Search by envelope TO
[1]> 4
Enter the regular expression to search for.
[]> '
Currently configured logs:
```

Log Name	Log Type	Retrieval	Interval
1. mail_logs	IronPort Text Mail Logs	Manual Download	None

Enter the number of the log you wish to use for message tracking.
[1]> 1
Please choose which set of logs to search:
1. All available log files
2. Select log files by date list
3. Current log file


```
[3]> 3  
No matching message IDs were found
```

grep

説明

ログ ファイル内のテキストを検索します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカル ファイル システムにアクセスする必要があります。

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せん。

grep コマンドを使用すると、ログ内の文字列を検索できます。grep コマンドを実行するときには、次の構文を使用します。

```
grep [-C count] [-e regex] [-i] [-p] [-t] [regex] log_name
```



(注) 結果を返すには、**-e regex** または **regex** を入力する必要があります。

grep コマンドを実行するときには、次のオプションを使用します。

表 11: **grep** コマンドのオプション

オプション	説明
-C	見つかった grep パターンのコンテキストを示す周辺の行を表示します。表示する行数を入力します。
-e	正規表現を入力します。
-i	大文字と小文字の区別を無視します。
-p	出力に改ページを追加します。
-t	grep コマンドをログ ファイルの末尾まで実行します。
regex	正規表現を入力します。

grep の例

次に、アンチウイルスログの中で文字列「clean」または「viral」を検索する例を示します。この **grep** コマンドには **regex** 表現が含まれています。

```
mail3.example.com> grep "CLEAN\\|VIRAL" antivirus
Fri Jun 9 21:50:25 2006 Info: sophos antivirus - MID 1 - Result 'CLEAN' ()
Fri Jun 9 21:53:15 2006 Info: sophos antivirus - MID 2 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 3 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 4 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 5 - Result 'CLEAN' ()
Fri Jun 9 22:47:41 2006 Info: sophos antivirus - MID 6 - Result 'CLEAN' ()
Fri Jun 9 22:47:42 2006 Info: sophos antivirus - MID 12 - Result 'CLEAN' ()
Fri Jun 9 22:53:04 2006 Info: sophos antivirus - MID 18 - Result 'VIRAL' ()
Fri Jun 9 22:53:05 2006 Info: sophos antivirus - MID 16 - Result 'VIRAL' ()
Fri Jun 9 22:53:06 2006 Info: sophos antivirus - MID 19 - Result 'VIRAL' ()
Fri Jun 9 22:53:07 2006 Info: sophos antivirus - MID 21 - Result 'VIRAL' ()
Fri Jun 9 22:53:08 2006 Info: sophos antivirus - MID 20 - Result 'VIRAL' ()
Fri Jun 9 22:53:08 2006 Info: sophos antivirus - MID 22 - Result 'VIRAL' ()
mail3.example.com>
```

logconfig

説明

ログファイルへのアクセスを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

FTP プッシュ ログ サブスクリプションの例

次の例では、**logconfig** コマンドを使用して、myDeliveryLogs と呼ばれる新しい配信ログを設定します。次に、ログがFTPによってリモートホストにプッシュされるように設定します。

```
mail3.example.com> logconfig
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
```

```
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[1]> new
Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. gmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. Anti-Spam Archive
17. Anti-Virus Logs
18. Anti-Virus Archive
19. Scanning Logs
20. IronPort Spam Quarantine Logs
21. IronPort Spam Quarantine GUI Logs
22. Reporting Logs
23. Reporting Query Logs
24. Updater Logs
25. Tracking Logs
26. Safe/Block Lists Logs
27. Authentication Logs
[1]> 8
Please enter the name for the log:
[1]> myDeliveryLogs
Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> 2
Hostname to deliver the logs:
[1]> yourhost.example.com
Username on the remote host:
[1]> yourusername
Passphrase for your user:
[1]> thepassphrase
Directory on remote host to place logs:
[1]> /logs
```

SCP プッシュ ログ サブスクリプションの例

```

Filename to use for log files:
[conversation.text]>
Maximum time to wait before transferring:
[3600]>
Maximum filesize before transferring:
[10485760]>
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "myDeliveryLogs" Type: "SMTP Conversation Logs" Retrieval: FTP Push - Host
    yourhost.example.com
16. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
17. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
18. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
19. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
20. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
21. "status" Type: "Status Logs" Retrieval: FTP Poll
22. "system_logs" Type: "System Logs" Retrieval: FTP Poll
23. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
24. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll

```

SCP プッシュ ログ サブスクリプションの例

次の例では、**logconfig** コマンドを使用して、LogPush と呼ばれる新しい配信ログを設定します。このログは、SCP によって IP アドレスが 10.1.1.1 のリモートホストにユーザ **logger** としてプッシュされ、ディレクトリ **/tmp** に保存されるように設定します。ログ取得方法が SCP プッシュである場合は **logconfig** コマンドから自動的に **sshconfig** コマンドが呼び出されることに注意してください。（ホストキーの詳細については「Configuring Host Keys」、ユーザキーの詳細については「Managing Secure Shell (SSH) Keys」を、『*User Guide for AsyncOS for Cisco Email Security Appliances*』で参照してください）。また、IP アドレスをホスト名プロンプトで使用できることに注意してください。

```

mail3.example.com> logconfig
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll

```

```
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[> new
Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. Anti-Spam Archive
17. Anti-Virus Logs
18. Anti-Virus Archive
19. Scanning Logs
20. IronPort Spam Quarantine Logs
21. IronPort Spam Quarantine GUI Logs
22. Reporting Logs
23. Reporting Query Logs
24. Updater Logs
25. Tracking Logs
26. Safe/Block Lists Logs
27. Authentication Logs
[1]> 3
Please enter the name for the log:
[> LogPush
Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
[1]> 3
Hostname to deliver the logs:
[> 10.1.1.1
Port to connect to on the remote host:
[22]>
Username on the remote host:
[> logger
Directory on remote host to place logs:
[> /tmp
Filename to use for log files:
[delivery.log]>
```

```

Maximum time to wait before transferring:
[3600]>
Maximum filesize before transferring:
[10485760]>
Protocol:
1. SSH1
2. SSH2
[2]> 2
Do you want to enable host key checking? [N]> y
Do you want to automatically scan the host for its SSH key, or enter it
manually?
1. Automatically scan.
2. Enter manually.
[1]> 1
SSH2:dsa
10.1.1.1 ssh-dss
AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwEsArt9LVE2ts5yE9JBTSdUwLvoq0G3FRqifrc92zgyHtc/
ZWYxavUTIM3XdlbpiEcscMp2XKpSnPPx21y8bqkpJsSQcM8zZMDjnOPm8ghiwHXYh7oNEUJCCPnPxAy44rlJ5Yz4x9eIoAlp0dHU0GR
+j1NAAAFQDQi5GY/X9PlDM3fPMvEx7wc0edlwAAAIb9cgMTEFP1WIAGrlRtbowZP5zWZtVDTxLhdXzjlo4+hbB4hBR7DKuc80+naAFnThyH/
JER3WLJVF79M5geKUbXzuJGK3ZwL3UyefPcBqXp20LzIFQSUxdlWwYz/rooqNlBnF4sh12mtq3tde1176oQgtwQAwKO15k3zQvSPwAAIAicRYat3y+Blv/
V6wDE6Bk+oULv3ek38gafuip4WMBxkG9G06EQi8nss82oznwMBy/pITRQfh4MBnLxTF4VEY00sARrlZtuUJC1QQvCgh7Nd3YNais2CSbEKBEaIOTf6+
SX2RNpcUF3Wg5yggw92xtqQPKMcZeLtK2ZJRkhC+Vw==
Add the preceding host key(s) for 10.1.1.1? [Y]> y
Currently installed host keys:
1. 10.1.1.1 1024 35 12260642076447444117847407996206675325...3520565607
2. 10.1.1.1 ssh-dss AAAAB3NzaC1kc3MAAACBALwGi4IlWLDVndbIwE...JRkhC+Vw==
Choose the operation you want to perform:
- NEW - Add a new key.
- EDIT - Modify a key.
- DELETE - Remove a key.
- SCAN - Automatically download a host key.
- PRINT - Display a key.
- HOST - Display this machine's host keys.
[>
Maximum filesize before transferring:
[10485760]>
Protocol:
1. SSH1
2. SSH2
[2]> 2
Do you want to enable host key checking? [N]> y
Currently installed host keys:
Choose the operation you want to perform:
- NEW - Add a new key.
- SCAN - Automatically download a host key.
- HOST - Display this machine's host keys.
[> scan
Choose the ssh protocol type:
1. SSH1:rsa
2. SSH2:rsa
3. SSH2:dsa
4. All
[4]> 4
SSH1:rsa
10.1.1.1 1024 35
122606420764474441178474079962066753259278682648965870690129496065430424463013457294798980627829828033793152226
44869451431621827281445398693161250828232800881574007210997563235647853212881618780683074632823432777810013112817667266624451119
1783747965898000855947022484692079466697707373948871554575173520565607

```

Syslog プッシュ ログ サブスクリプションの例

次の例では、**logconfig** コマンドを使用して、MailLog SyslogPush と呼ばれる新しい配信ログを設定します。このログは、UPD を使用して IP アドレスが 10.1.1.2 のリモート syslog サーバに「メール」ファシリティでプッシュされ、所定のディレクトリに保存されるように設定します。

```
mail3.example.com> logconfig
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> new
Choose the log file type for this subscription:
1. IronPort Text Mail Logs
2. qmail Format Mail Logs
3. Delivery Logs
4. Bounce Logs
5. Status Logs
6. Domain Debug Logs
7. Injection Debug Logs
8. SMTP Conversation Logs
9. System Logs
10. CLI Audit Logs
11. FTP Server Logs
12. HTTP Logs
13. NTP logs
14. LDAP Debug Logs
15. Anti-Spam Logs
16. Anti-Spam Archive
17. Anti-Virus Logs
18. Anti-Virus Archive
19. Scanning Logs
20. IronPort Spam Quarantine Logs
```

```

21. IronPort Spam Quarantine GUI Logs
22. Reporting Logs
23. Reporting Query Logs
24. Updater Logs
25. Tracking Logs
26. Safe/Block Lists Logs
27. Authentication Logs
[1]> 1
Please enter the name for the log:
[]> MailLogSyslogPush
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 2
Choose the method to retrieve the logs.
1. FTP Poll
2. FTP Push
3. SCP Push
4. Syslog Push
[1]> 4
Hostname to deliver the logs:
[]> 10.1.1.2
Which protocol do you want to use to transfer the log data?
1. UDP
2. TCP
[1]> 1
Which facility do you want the log data to be sent as?
1. auth
2. authpriv
3. console
4. daemon
5. ftp
6. local0
7. local1
8. local2
9. local3
10. local4
11. local5
12. local6
13. local7
14. mail
15. ntp
16. security
17. user
[14]> 14
Currently configured logs:
1. "MailLogSyslogPush" Type: "IronPort Text Mail Logs" Retrieval: Syslog Push -
Host 10.1.1.2

```

rollovernow

説明

ログファイルをロールオーバーします。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail3.example.com> rollovernow
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
24. All Logs
Which log would you like to roll over?
[]> 2
Log files successfully rolled over.
mail3.example.com>
```

snmpconfig

説明

SNMP を設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例では、`snmpconfig` コマンドを使用して、ポート 161 の「PublicNet」インターフェイスで SNMP をイネーブルにしています。バージョン 3 のパスフレーズが入力され、確認のために再入力されています。システムは、バージョン 1 および 2 要求を処理するように設定されており、これらのバージョン 1 および 2 からの GET 要求に対してコミュニティ スtring `public` が入力されています。トラップターゲット `snmp-monitor.example.com` が入力されています。最後に、システムの場所と連絡先情報が入力されています。

```
mail3.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? [N]> y
Please choose an IP interface for SNMP requests.
1. Data 1 (192.168.1.1/24: buttercup.run)
2. Data 2 (192.168.2.1/24: buttercup.run)
3. Management (192.168.44.44/24: buttercup.run)
[1]>
Enter the SNMPv3 passphrase.
>
Please enter the SNMPv3 passphrase again to confirm.
>
Which port shall the SNMP daemon listen on?
[161]>
Service SNMP V1/V2c requests? [N]> y
Enter the SNMP V1/V2c community string.
[]> public
From which network shall SNMP V1/V2c requests be allowed?
[192.168.2.0/24]>
Enter the Trap target (IP address). Enter "None" to disable traps.
[None]> snmp-monitor.example.com
Enterprise Trap Status
1. RAIDStatusChange           Enabled
2. fanFailure                  Enabled
3. highTemperature             Enabled
4. keyExpiration               Enabled
5. linkDown                    Enabled
6. linkUp                      Enabled
7. powerSupplyStatusChange     Enabled
8. resourceConservationMode     Enabled
9. updateFailure               Enabled
Do you want to change any of these settings? [N]> y
Do you want to disable any of these traps? [Y]>
Enter number or numbers of traps to disable. Separate multiple numbers with commas.
[]> 1,8
Enterprise Trap Status
1. RAIDStatusChange           Disabled
2. fanFailure                  Enabled
3. highTemperature             Enabled
4. keyExpiration               Enabled
5. linkDown                    Enabled
6. linkUp                      Enabled
7. powerSupplyStatusChange     Enabled
8. resourceConservationMode     Disabled
9. updateFailure               Enabled
Do you want to change any of these settings? [N]>
Enter the System Location string.
```

```
[Unknown: Not Yet Configured]> Network Operations Center - west; rack #31, position 2
Enter the System Contact string.
[snmp@localhost]> Joe Administrator, x8888
Current SNMP settings:
Listening on interface "Data 1" 192.168.2.1/24 port 161.
SNMP v3: Enabled.
SNMP v1/v2: Enabled, accepting requests from subnet 192.168.2.0/24.
SNMP v1/v2 Community String: public
Trap target: snmp-monitor.example.com
Location: Network Operations Center - west; rack #31, position 2
System Contact: Joe Administrator, x8888
mail3.example.com>
```

tail

説明

ログファイルの最新部分を継続的に表示します。tail コマンドには、表示するログの名前または番号をパラメータ tail 9 または tail mail_logs として指定することもできます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカルファイルシステムにアクセスする必要があります。

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せん。

例

```
mail3.example.com> tail
Currently configured logs:
1. "antispam" Type: "Anti-Spam Logs" Retrieval: FTP Poll
2. "antivirus" Type: "Anti-Virus Logs" Retrieval: FTP Poll
3. "asarchive" Type: "Anti-Spam Archive" Retrieval: FTP Poll
4. "authentication" Type: "Authentication Logs" Retrieval: FTP Poll
5. "avarchive" Type: "Anti-Virus Archive" Retrieval: FTP Poll
6. "bounces" Type: "Bounce Logs" Retrieval: FTP Poll
7. "cli_logs" Type: "CLI Audit Logs" Retrieval: FTP Poll
8. "encryption" Type: "Encryption Logs" Retrieval: FTP Poll
9. "error_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
10. "euq_logs" Type: "IronPort Spam Quarantine Logs" Retrieval: FTP Poll
11. "euqgui_logs" Type: "IronPort Spam Quarantine GUI Logs" Retrieval: FTP Poll
12. "ftpd_logs" Type: "FTP Server Logs" Retrieval: FTP Poll
13. "gui_logs" Type: "HTTP Logs" Retrieval: FTP Poll
14. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
15. "reportd_logs" Type: "Reporting Logs" Retrieval: FTP Poll
16. "reportqueryd_logs" Type: "Reporting Query Logs" Retrieval: FTP Poll
17. "scanning" Type: "Scanning Logs" Retrieval: FTP Poll
18. "slbld_logs" Type: "Safe/Block Lists Logs" Retrieval: FTP Poll
19. "sntpd_logs" Type: "NTP logs" Retrieval: FTP Poll
20. "status" Type: "Status Logs" Retrieval: FTP Poll
21. "system_logs" Type: "System Logs" Retrieval: FTP Poll
22. "trackerd_logs" Type: "Tracking Logs" Retrieval: FTP Poll
23. "updater_logs" Type: "Updater Logs" Retrieval: FTP Poll
```

```

Enter the number of the log you wish to tail.
[]> 19
Press Ctrl-C to stop.
Sat May 15 12:25:10 2008 Info: PID 274: User system commit changes: Automated Update for
Quarantine Delivery Host
Sat May 15 23:18:10 2008 Info: PID 19626: User admin commit changes:
Sat May 15 23:18:10 2008 Info: PID 274: User system commit changes: Updated filter logs
config
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Receiving suspended.
Sat May 15 23:46:06 2008 Info: PID 25696: User admin commit changes: Suspended receiving.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving resumed.
Sat May 15 23:46:35 2008 Info: PID 25696: User admin commit changes: Receiving resumed.
Sat May 15 23:48:17 2008 Info: PID 25696: User admin commit changes:
Sun May 16 00:00:00 2008 Info: Generated report: name b, start time Sun May 16 00:00:00
2004, size 2154 bytes
^C
mail3.example.com>

```

レポート

ここでは、次の CLI コマンドについて説明します。

- [reportingconfig](#) (236 ページ)

reportingconfig

reportingconfig コマンドの使用

reportingconfig サブメニューでは、以下のサブコマンドを使用できます。

表 12: *reportingconfig* サブコマンド

構文	説明	アベイラビリティ
filters	セキュリティ管理アプライアンスのフィルタを設定します。	M-Series のみ
alert_timeout	レポートデータを取得できなかった場合にアラートを受け取るまでの時間を設定します。	M-Series のみ
domain	ドメイン レポート設定を指定します。	M-Series のみ
mode	セキュリティ管理アプライアンスで中央集中型レポートングをイネーブルにします。E メールセキュリティアプライアンスの中央集中型またはローカルレポートングをイネーブルにします。	C-Series、M-Series

構文	説明	アベイラビリティ
mailsetup	Eメールセキュリティアプライアンスのレポーティングを設定します。	C-Series のみ

使用方法

確定：このコマンドは「commit」が必要です。

例：レポーティングフィルタのイネーブル化（M-Series のみ）

```
mail3.example.com> reportingconfig
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> filters
Filters remove specific sets of centralized reporting data from the "last year" reports.

Data from the reporting groups selected below will not be recorded.
All filtering has been disabled.
1. No Filtering enabled
2. IP Connection Level Detail.
3. User Detail.
4. Mail Traffic Detail.
Choose which groups to filter, you can specify multiple filters by entering a comma separated list:
[]> 2, 3
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]>
```

ドメイン レポートの HAT REJECT 情報のイネーブル化（M-Series のみ）

```
mail3.example.com> reportingconfig
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> domain
If you have configured HAT REJECT policy on all remote appliances providing reporting data to this appliance to occur at the message recipient level then of domain reports.
Use message recipient HAT REJECT information for domain reports? [N]> y
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting data
- DOMAIN - Configure domain report settings.
```

```
- MODE - Enable/disable centralized reporting.
[]>
```

タイムアウト アラートのイネーブル化 (M-Series のみ)

```
mail3.example.com> reportingconfig
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting
data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]> alert_timeout
An alert will be sent if reporting data has not been fetched from an appliance after 360
minutes.
Would you like timeout alerts to be enabled? [Y]> y
After how many minutes should an alert be sent?
[360]> 240
Choose the operation you want to perform:
- FILTERS - Configure filtering for the SMA.
- ALERT_TIMEOUT - Configure when you will be alerted due to failing to get reporting
data
- DOMAIN - Configure domain report settings.
- MODE - Enable/disable centralized reporting.
[]>
```

E メールセキュリティ アプライアンスでの中央集中型レポーティングのイネーブル化

```
mail3.example.com> reportingconfig
Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]> mode
Centralized reporting: Local reporting only.
Do you want to enable centralized reporting? [N]> y
Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]>
```

レポーティング データに対する記憶域の制限の設定 (C-Series のみ)

```
mail.example.com> reportingconfig
Choose the operation you want to perform:
- MAILSETUP - Configure reporting for the ESA.
- MODE - Enable centralized or local reporting for the ESA.
[]> mailsetup
SenderBase timeout used by the web interface: 5 seconds
Sender Reputation Multiplier: 3
The current level of reporting data recording is: unlimited
No custom second level domains are defined.
Legacy mailflow report: Disabled
Choose the operation you want to perform:
- SENDERBASE - Configure SenderBase timeout for the web interface.
- MULTIPLIER - Configure Sender Reputation Multiplier.
- COUNTERS - Limit counters recorded by the reporting system.
- THROTTLING - Limit unique hosts tracked for rejected connection reporting.
- TLD - Add customer specific domains for reporting rollup.
- STORAGE - How long centralized reporting data will be stored on the C-series before
```

```
being overwritten.
- LEGACY - Configure legacy mailflow report.
[]> storage
While in centralized mode the C-series will store reporting data for the M-series to collect.
If the M-series does not collect that data then eventually the C-series will begin to overwrite the oldest data with new data.
A maximum of 24 hours of reporting data will be stored.
How many hours of reporting data should be stored before data loss?
[24]> 48
SenderBase timeout used by the web interface: 5 seconds
Sender Reputation Multiplier: 3
The current level of reporting data recording is: unlimited
No custom second level domains are defined.
Legacy mailflow report: Disabled
Choose the operation you want to perform:
- SENDERBASE - Configure SenderBase timeout for the web interface.
- MULTIPLIER - Configure Sender Reputation Multiplier.
- COUNTERS - Limit counters recorded by the reporting system.
- THROTTLING - Limit unique hosts tracked for rejected connection reporting.
- TLD - Add customer specific domains for reporting rollup.
- STORAGE - How long centralized reporting data will be stored on the C-series before being overwritten.
- LEGACY - Configure legacy mailflow report.
[]>
```

Senderbase

ここでは、次の CLI コマンドについて説明します。

- [sbstatus](#) (239 ページ)
- [senderbaseconfig](#) (240 ページ)

sbstatus

説明

SenderBase クエリーのステータスを表示します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> sbstatus
SenderBase host status
Status as of:      Tue Oct 21 10:55:04 2003
Host up/down:      up
```

アプリケーションが SenderBase 評価サービスに接続できない場合、つまりこのサービスへの接続が成功しなかった場合は、次のように表示されます。

```
mail3.example.com> sbstatus
SenderBase host status
Host up/down:           Unknown (never contacted)
```

senderbaseconfig

説明

SenderBase の接続設定を指定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> senderbaseconfig
Share statistics with SenderBase Information Service: Enabled
Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings
[]> setup
Do you want to share statistical data with the SenderBase Information Service
(recommended)? [Y]>
Share statistics with SenderBase Information Service: Enabled
Choose the operation you want to perform:
- SETUP - Configure SenderBase Network Participation settings
[]>
```

SMTP サービスの設定

ここでは、次の CLI コマンドについて説明します。

- [callaheadconfig](#) (241 ページ)
- [listenerconfig](#) (242 ページ)
- [localeconfig](#) (272 ページ)
- [smtpauthconfig](#) (274 ページ)

callaheadconfig

説明

SMTP コールアヘッド プロファイルを追加、編集、または削除します

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次に、配信ホストの新しい SMTP コールアヘッド プロファイルを作成する例を示します。

```
> callaheadconfig
No SMTP Call-Ahead profiles are configured on the system.
Choose the operation you want to perform:
- NEW - Create a new profile.
[]> new
Select the type of profile you want to create:
1. Delivery Host
2. Static Call-Ahead Servers
[1]> 1
Please enter a name for the profile:
[]> delhost01
Advanced Settings:
  MAIL FROM Address: <>
  Interface: Auto
  Timeout Value: 30
  Validation Failure Action: ACCEPT
  Temporary Failure Action: REJECT with same code
  Maximum number of connections: 5
  Maximum number of validation queries: 1000
  Cache size: 10000
  Cache TTL: 900
Do you want to change advanced settings? [N]> n
Currently configured SMTP Call-Ahead profiles:
1. delhost01 (Delivery Host)
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[]>
```

次に、コールアヘッド サーバの新しい SMTP コールアヘッド プロファイルを作成する例を示します。

```
> callaheadconfig
Currently configured SMTP Call-Ahead profiles:
```

```

1. delhost01 (Delivery Host)
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[]> new
Select the type of profile you want to create:
1. Delivery Host
2. Static Call-Ahead Servers
[1]> 2
Please enter a name for the profile:
[]> Static
Enter one or more Call-Ahead servers hostname separated by commas.
[]> 192.168.1.2
Advanced Settings:
    MAIL FROM Address: <>
    Interface: Auto
    Timeout Value: 30
    Validation Failure Action: ACCEPT
    Temporary Failure Action: REJECT with same code
    Maximum number of connections: 5
    Maximum number of validation queries: 1000
    Cache size: 10000
    Cache TTL: 900
Do you want to change advanced settings? [N]> n
Currently configured SMTP Call-Ahead profiles:
1. Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)
Choose the operation you want to perform:
- NEW - Create a new profile.
- EDIT - Modify a profile.
- DELETE - Delete a profile.
- PRINT - Display profile information.
- TEST - Test profile.
- FLUSHCACHE - Flush SMTP Call-Ahead cache.
[]> print
Select the profile you want to print:
1. Static (Static Call-Ahead Servers)
2. delhost01 (Delivery Host)
[1]>

```

listenerconfig

説明

listenerconfig コマンドでは、リスナーを作成、編集、削除できます。AsyncOS では、メッセージを受信し、受信ホストやネットワークの内部またはインターネット上の外部の受信者のいずれかにリレーするための条件を指定する必要があります。

これらの対象となる条件はリスナーで定義されます。これらの条件が一括されてメールフローポリシーが定義され、適用されます。リスナーでは、アプライアンスでEメールを送信するシステムと通信する方法も定義されます。

表 13: *listenerconfig* コマンド

名前	リスナーには、簡単に参照できるように一意の名前を付けてください。リスナー用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、複数のリスナーに同一の名前を付けることはできません。
IP インターフェイス	リスナーは IP インターフェイスに割り当てられます。リスナーを作成し割り当てる前に、 <code>systemstartup</code> コマンドまたは <code>interfaceconfig</code> コマンドを使用して、すべての IP インターフェイスを設定する必要があります。
メール プロトコル	電子メールの受信に使用されるメールプロトコルであり、ESMTP と QMQP のいずれかです。
IP ポート	リスナーへの接続に使用する特定の IP ポート。デフォルトでは、SMTP ではポート 25 を使用し、QMQP ではポート 628 を使用します。
リスナー タイプ： パブリック プライベート ブラックホール	パブリック リスナーおよびプライベート リスナーは、ほとんどの設定に使用されます。一般的に、プライベート リスナーはプライベート（内部）ネットワークに使用されます。パブリック リスナーには、インターネット経由の電子メールの受信のためのデフォルトの特性があります。 テストまたはトラブルシューティングの目的で、「ブラックホール」リスナーを使用できます。ブラックホール リスナーの作成時に、メッセージを削除する前にそのメッセージをディスクに書き込むかどうかを選択します（詳細については『 <i>User Guide for AsyncOS for Cisco Email Security Appliances</i> 』の「Testing and Troubleshooting」の章を参照してください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

バッチ形式：一般的な *listenerconfig*

listenerconfig コマンドのバッチ形式を使用すると、特定のインターフェイスに対してリスナーを追加および削除できます。listenerconfig コマンドのバッチ形式では、リスナーの HAT および RAT を設定することもできます。

- 新しいリスナーの追加：

```
listenerconfig new <name> <public|private|blackhole|blackholequeueing>
<interface_name> <smtp|qmqp>
```

- リスナーの削除：

```
listenerconfig delete <name>
```

バッチ形式：HAT

次に、`listenerconfig` のバッチ形式を使用して HAT 関連の各種作業を実行する例を示します。引数の詳細については、次の表：*listenerconfig* 引き数値：HAT を参照してください。

- HAT への新しい送信者グループの追加

```
listenerconfig edit <name> hostaccess new sendergroup <name> <host_list> <behavior>
[options [--comments]]
```

- HAT への新しいポリシーの追加

```
listenerconfig edit <name> hostaccess new policy <name> <behavior> [options]
```

- 送信者グループへの新しいホスト リストの追加

```
listenerconfig edit <name> hostaccess edit sendergroup <name> new <host_list>
```

- 送信者グループからのホストの削除

```
listenerconfig edit <name> hostaccess edit sendergroup <name> delete <host>
```

- 送信者グループ リストでのホストの移動

```
listenerconfig edit <name> hostaccess edit sendergroup <name> move <host>
<host-to-insert-before>
```

- 送信者グループのポリシーの変更

```
listenerconfig edit <name> hostaccess edit sendergroup <name> policy <behavior>
[options]
```

- 送信者グループ リストの出力

```
listenerconfig edit <name> hostaccess edit sendergroup <name> print
```

- 送信者グループ名の変更

```
listenerconfig edit <name> hostaccess edit sendergroup <name> rename <name>
```

- HAT ポリシーの編集

```
listenerconfig edit <name> hostaccess edit policy <name> <behavior> [options]
```

- HAT からの送信者グループの削除

```
listenerconfig edit <name> hostaccess delete sendergroup <name>
```

- ポリシーの削除

```
listenerconfig edit <name> hostaccess delete policy <name>
```

- HAT での送信者グループの移動

```
listenerconfig edit <name> hostaccess move <group> <group-to-insert-before>
```

- HAT デフォルト オプションの変更

```
listenerconfig edit <name> hostaccess default [options]
```

- ホスト アクセス テーブルの出力

```
listenerconfig edit <name> hostaccess print
```

- HAT のローカル コピーのインポート

```
listenerconfig edit <name> hostaccess import <filename>
```

- アプライアンスからの HAT のコピーのエクスポート

```
listenerconfig edit <name> hostaccess export <filename>
```

- HAT からユーザ定義のすべての送信者グループおよびポリシーを削除

```
listenerconfig edit <name> hostaccess clear
```

- 特定の送信者グループについて、送信者の出身国を追加します。

```
listenerconfig edit incoming hostaccess edit sendergroup WHITELIST  
country add India Nepal Cyprus
```

- 特定の送信者グループについて、送信者の出身国を削除します。

```
listenerconfig edit incoming hostaccess edit sendergroup WHITELIST
country delete Cyprus
```

- 特定の送信者グループについて、送信者の出身国を印刷します。

```
listenerconfig edit incoming hostaccess edit sendergroup WHITELIST
country print
```

表 14: *listenerconfig* 引数値：HAT

引数	説明
<behavior>	“Accept”、“Relay”、“Reject”、“TCP Refuse”、または“Continue”。送信者グループで使用する動作を選択するときは、“Policy: FOO”（“FOO”はポリシー名）という形式で追加の動作も選択できます。
<filename>	ホスト アクセス テーブルのインポートおよびエクスポートで使用するファイル名。
<group>	送信者グループの <name>。
<host>	<host_list> の 1 つのエンティティ。
<host_list>	追加するホストを入力します。ホストは次のようなフォーマットにできます。 CIDR アドレス (10.1.1.0/24) IP アドレス範囲 (10.1.1.10 ~ 20) IP サブネット (10.2.3) ホスト名 (crm.example.com) 部分ホスト名 (.example.com) SenderBase 評価スコア範囲 (7.5:10.0) SenderBase ネットワーク オーナー IDS (SBO:12345) リモート ブラックリスト クエリー (dnslist[query.blacklist.example]) (注) 複数のホストを指定する場合は、カンマで区切ります。
<name>	送信者グループまたはポリシーの名前。HAT ラベルは、文字または下線で開始する必要がある、その後に任意の数の文字、数字、下線、またはハイフンを追加します。
[options]	
--max_size	最大メッセージサイズ。最後に、単位がキロバイトの場合はk、メガバイトの場合はMを追加します。単位がバイトの場合、末尾の文字は不要です。

引数	説明
--max_conn	1 つのホストから確立できる接続の最大数。
--max_msgs	接続あたりの最大メッセージ数。
--max_rcpt	メッセージあたりの最大受信者数。
--override	SMTP バナーのホスト名を上書きします。“No” または SMTP バナー文字列。
--cust_acc	カスタム SMTP 受け入れ応答を指定します。“No” または SMTP 受け入れ応答文字列。
--acc_code	カスタム SMTP 受け入れ応答コード。デフォルトは 220 です。
--cust_rej	カスタム SMTP 拒否応答を指定します。“No” または SMTP 拒否応答文字列。
--rej_code	カスタム SMTP 拒否応答コード。デフォルトは 554 です。
--rate_lim	ホスト単位のレート制限をイネーブルにします。“No”、“default”、またはホストごとの受信者の 1 時間あたり最大数を指定します。
--cust_lim	カスタム SMTP 制限超過応答メッセージを指定します。“No” または SMTP 拒否応答文字列。デフォルトは “No” です。
--lim_code	カスタム SMTP 制限超過応答コード。デフォルトは 452 です。
--use_sb	デフォルトでフロー制御に SenderBase を使用します。“Yes”、“No”、または “default”。
--as_scan	anti-spam スキャンをイネーブルにします。“Yes”、“No”、“Default”。
--av_scan	アンチウイルス スキャンをイネーブルにします。“Yes”、“No”、“Default”。
--dhap	ディレクトリ ハーベスト攻撃防止 “No”、“default”、またはリモートホストからの無効な受信者の 1 時間あたり最大数を指定します。
--tls	サポートされていません。TLS を設定するには、メニューシステムを使用します。
--sig_bits	IP アドレスの有意ビット数。0～32、“No”、または “default”。
--dkim_signing	DKIM 署名をイネーブルにします。“Yes”、“No”、“Default”。
--dkim_verification	DKIM 検証をイネーブルにします。“Yes”、“No”、“Default”。
--dkim_verification_profile <name>	DKIM 検証プロファイルの名前。このオプションは、--dkim_verification の値を “Yes” に設定した場合にのみ適用されます。

引数	説明
--spf	SPF 検証をイネーブルにします。“Yes”、“No”、“Default”。
--spf_conf_level	SPF 適合レベル。“--spf Yes”の場合にのみ使用します。“spf_only”、“sidf_compatible”、“sidf_strict”。
--spf_downgrade_pra	SPF PRA 検証結果をダウングレードします。“--spf Yes”および“--spf_conf_level sidf_compatible”の場合にのみ使用します。“Yes”、“No。”
--spf_helo_test	SPF HELO テスト。“--spf Yes”および“--spf_conf_level sidf_compatible,”または“--spf_conf_level spf_only”の場合に使用します。“Yes”、“No”。
--dmarc_verification	DMARC 検証をイネーブルにします。“Yes”、“No”、“Default”。
--dmarc_verification_profile <name>	DMARC 検証プロファイルの名前。このオプションは、--dmarc_verification の値を“Yes”に設定した場合にのみ適用されます。
--dmarc_agg_reports	DMARC 集計レポートの有効化。“Yes”、“No”、“Default”。このオプションは、--dmarc_verification の値を“Yes”に設定した場合にのみ適用されます。

バッチ形式：RAT

次に、listenerconfig のバッチ形式を使用して RAT 関連の各種作業を実行する例を示します。引数に関する詳細については、次の表：listenerconfig 引き数値：RAT を参照してください。

- RAT への新しい受信者の追加

```
listenerconfig edit <name> rcptaccess new <rat_addr> [options]
```

- RAT 内の受信者の編集

```
listenerconfig edit <name> rcptaccess edit <rat_addr> [options]
```

- RAT からの受信者の削除

```
listenerconfig edit <name> rcptaccess delete <rat_addr>
```

- RAT のコピーの出力

```
listenerconfig edit <name> rcptaccess print
```

- ローカル RAT のアプライアンスへのインポート


```
listenerconfig edit <name> rcptaccess import <filename>
```

- RAT のエクスポート

```
listenerconfig edit <name> rcptaccess export <filename>
```

- デフォルト アクセスのクリア

```
listenerconfig edit <name> rcptaccess clear <default_access>
```

表 15: *listenerconfig* 引数値：RAT

引数	説明
<rat_addr>	追加するホストを入力します。ホストは次のようなフォーマットにできます。 CIDR アドレス (10.1.1.0/24) ホスト名 (crm.example.com) 部分ホスト名 (.example.com) ユーザ名 (postmaster@) 完全な電子メール アドレス (joe@example.com, joe@[1.2.3.4]) (注) 複数のホストを指定する場合は、カンマで区切ります。
<options>	
--action	アドレスに適用するアクション。“Accept” または “Reject” のどちらか。デフォルトは “Accept” です。
--cust_resp	カスタム SMTP 応答を指定します。“No” または SMTP 受け入れ応答文字列。
--resp_code	カスタム SMTP 応答コード。“Accept” の場合は 250 がデフォルト、“Reject” の場合は 550 がデフォルトです。
--bypass_rc	受信制御をバイパスします。デフォルトは “No” です。
--bypass_la	LDAP 承認クエリーをバイパスします。“Yes” または “No” のどちらか。
--bypass_ca	SMTP コールアヘッドをバイパスします。デフォルトは [いいえ (No)] です。

例：リスナーの追加

次の例では、`listenerconfig` コマンドを使用して、エンタープライズゲートウェイ構成に必要な B リスナーに使用できる、**OutboundMail** と呼ばれる新しいプライベート リスナーを作成します。（注：このプライベート リスナーは、GUI の **System Setup Wizard** または CLI の **systemsetup** コマンドを実行するときに追加することもできます）。

プライベート リスナー タイプを選択し、名前を **OutboundMail** に設定します。このリスナーは、**PrivateNet** IP インターフェイス上でポート 25 の SMTP プロトコルを使用して動作するように指定します。このリスナーのホスト アクセス ポリシーのデフォルト値が受け入れられます。

```
mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[1]> new
Please select the type of listener you want to create.
1. Private
2. Public
3. Blackhole
[2]> 1
Please create a name for this listener (Ex: "OutboundMail"):
[1]> OutboundMail
Please choose an IP interface for this Listener.
1. Management (192.168.42.42/24: mail3.example.com)
2. PrivateNet (192.168.1.1/24: mail3.example.com)
3. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 2
Choose a protocol.
1. SMTP
2. QMQP
[1]> 1
Please enter the TCP port for this listener.
[25]> 25
Please specify the systems allowed to relay email through the IronPort C60.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[1]> .example.com
Do you want to enable rate limiting for this listener? (Rate limiting defines the maximum
number of recipients per hour you are
willing to receive from a remote domain.) [N]> n
Default Policy Parameters
=====
Maximum Message Size: 100M
Maximum Number Of Connections From A Single IP: 600
Maximum Number Of Messages Per Connection: 10,000
Maximum Number Of Recipients Per Message: 100,000
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: No
Spam Detection Enabled: No
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
```

```
Require TLS To Offer SMTP authentication: No
Would you like to change the default host access policy? [N]> n
Listener OutboundMail created.
Defaults have been set for a Private listener.
Use the listenerconfig->EDIT command to customize the listener.
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[ ]>
```

例: 送信者の出身国を送信者グループに追加する

次の例では、`listenerconfig` コマンドを使用してリスナーを変更します。このリスナーは、特定の送信者グループについて送信者の出身国を追加します。

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.

[ ]> edit

Enter the name or number of the listener you wish to edit.

[ ]> 1

Name: InboundMailhostacce

Type: Public

Interface: PublicNet (192.168.2.1/24) TCP Port 25

Protocol: SMTP

Default Domain:

Max Concurrency: 1000 (TCP Queue: 50)

Domain map: disabled

TLS: No

SMTP Authentication: Disabled
```

例：送信者の出身国を送信者グループに追加する

```
Bounce Profile: Default

Use SenderBase For Reputation Filters and IP Profiling: Yes

Footer: None

LDAP: off

Choose the operation you want to perform:

- NAME - Change the name of the listener.

- INTERFACE - Change the interface.

- LIMITS - Change the injection limits.

- SETUP - Configure general options.

- HOSTACCESS - Modify the Host Access Table.

- RCPTACCESS - Modify the Recipient Access Table.

- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.

- MASQUERADE - Configure the Domain Masquerading Table.

- DOMAINMAP - Configure domain mappings.

[> hostaccess

Default Policy Parameters

=====

Maximum Message Size: 10M

Maximum Number Of Concurrent Connections From A Single IP: 10

Maximum Number Of Messages Per Connection: 10

Maximum Number Of Recipients Per Message: 50

Directory Harvest Attack Prevention: Enabled

Maximum Number Of Invalid Recipients Per Hour: 25

Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control: Yes

Spam Detection Enabled: Yes

Virus Detection Enabled: Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

DKIM/DomainKeys Signing Enabled: No

DKIM Verification Enabled: No
```

```

SPF/SIDF Verification Enabled: No

DMARC Verification Enabled: No

Envelope Sender DNS Verification Enabled: No

Domain Exception Table Enabled: No

Accept untagged bounces: No

There are currently 4 policies defined.

There are currently 5 sender groups.

Choose the operation you want to perform:

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.

[ ]> edit

1. Edit Sender Group
2. Edit Policy

[1]>1

Currently configured HAT sender groups:

1. WHITELIST (My trusted senders have no anti-spam scanning or rate limiting)
2. BLACKLIST (Spammers are rejected)
3. SUSPECTLIST (Suspicious senders are throttled)
4. UNKNOWNLIST (Reviewed but undecided, continue normal acceptance)
5. MyList
6. (no name, first host = ALL) (Everyone else)

Enter the sender group number or name you wish to edit.

[ ]> 1

Choose the operation you want to perform:

- NEW - Add a new host.

```

例：送信者の出身国を送信者グループに追加する

```

- DELETE - Remove a host.

- COUNTRY - Add and delete countries.

- POLICY - Change the policy settings and options.

- PRINT - Display the current definition.

- RENAME - Rename this sender group.

[]> country

Choose the operation you want to perform:

- ADD - Add countries

[]>ADD

1. Afghanistan [af]

2. Aland Islands [ax]

3. Albania [al]

4. Algeria [dz]

5. American Samoa [as]

6. Andorra [ad]

7. Angola [ao]

8. Anguilla [ai]

9. ...

Enter the indices separated by commas or specify the range.

[]>1,4,8

Choose the operation you want to perform:

- NEW - Add a new host.

- DELETE - Remove a host.

- MOVE - Reorder the hosts.

- COUNTRY - Add and delete countries.

- POLICY - Change the policy settings and options.

- PRINT - Display the current definition.

- RENAME - Rename this sender group.

[]> country

Choose the operation you want to perform:

- ADD - Add countries

- DELETE - Delete countries

```

```
- PRINT - Print countries

[> print

Afghanistan [af]

Algeria [dz]

Anguilla [ai]
```

例：エクスポートおよびインポートによるリスナーのホストアクセステーブル（HAT）のカスタマイズ

listenerconfig コマンドのサブコマンドの多くでは、データのインポートとエクスポートによって大規模な設定変更ができるため、CLI にデータを少しずつ入力する必要がありません。

この手順では、CLI を使用して、ファイルをエクスポートし、変更を加えてインポートすることにより、リスナーのホストアクセステーブル（HAT）を変更します。HAT CLI エディタまたは GUI を使用してリスナーの HAT をカスタマイズすることもできます。詳細については、『*User Guide for AsyncOS for Cisco Email Security Appliances*』の「Configuring the Gateway to Receive Mail」と「Using Mail Flow Monitor」の章を参照してください。

エクスポートとインポートによって定義した、リスナーの HAT をカスタマイズするには：

手順

ステップ 1 listenerconfig の hostaccess -> export サブコマンドを使用して、デフォルトの HAT をファイルにエクスポートします。

次の例では、パブリック リスナー InboundMail の HAT を出力し、さらに inbound.HAT.txt というファイルにエクスポートします。

例：

```
mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[> edit
Enter the name or number of the listener you wish to edit.
[> 1
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain map: disabled
TLS: No
```

例 : エクスポートおよびインポートによるリスナーのホスト アクセス テーブル (HAT) のカスタマイズ

```
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[> hostaccess
Default Policy Parameters
=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[> print
$BLOCKED
    REJECT {}
$TRUSTED
    ACCEPT {
        tls = "off"
        dhap_limit = 0
        max_rcpts_per_hour = -1
        virus_check = "on"
        max_msgs_per_session = 5000
        spam_check = "off"
        use_sb = "off"
        max_message_size = 104857600
        max_rcpts_per_msg = 5000
```



```

        max_concurrency = 600
    }
$ACCEPTED
    ACCEPT {}
$THROTTLED
    ACCEPT {
        tls = "off"
        dhap_limit = 0
        max_rcpts_per_hour = 1
        virus_check = "on"
        max_msgs_per_session = 10
        spam_check = "on"
        use_sb = "on"
        max_message_size = 1048576
        max_rcpts_per_msg = 25
        max_concurrency = 10
    }
WHITELIST:
    $TRUSTED (My trusted senders have no anti-spam or rate limiting)
BLACKLIST:
    $BLOCKED (Spammers are rejected)
SUSPECTLIST:
    $THROTTLED (Suspicious senders are throttled)
UNKNOWNLIST:
    $ACCEPTED (Reviewed but undecided, continue normal acceptance)
ALL
    $ACCEPTED (Everyone else)
Default Policy Parameters
=====
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[> export
Enter a name for the exported file:
[> inbound.HAT.txt
File written on machine "mail3.example.com".

```

例：

ステップ2 コマンドラインインターフェイス（CLI）の外部で、ファイルinbound.HAT.txtを取得します。

ステップ3 テキストエディタを使用して、このファイルに新しいHATエントリを作成します。

例：エクスポートおよびインポートによるリスナーのホストアクセス テーブル (HAT) のカスタマイズ

この例では、HAT 内の ALL エントリの上に以下のエントリを追加します。

spamdomain.com	REJECT
.spamdomain.com	REJECT
251.192.1.	TCPREFUSE
169.254.10.10	RELAY

- 最初の 2 つのエントリは、ドメイン spamdomain.com および spamdomain.com のサブドメイン内のリモート ホストからの接続をすべて拒否します。
- 3 つ目のエントリは、IP アドレスが 251.192.1.x であるホストからの接続を拒否します。
- 4 つ目のエントリによって、IP アドレスが 169.254.10.10 であるリモート ホストは、インターネットへのすべての発信電子メールについて、E メールセキュリティ アプライアンスを SMTP リレーとして使用できます。

(注) HAT 内でのルールの順序は重要な意味を持ちます。リスナーに接続しようとするホストごとに、HAT は上から下へ順番に読み込まれます。接続元ホストにルールが一致する場合、その接続に対してすぐにアクションが実行されます。HAT では、すべてのカスタム エントリを ALL ホスト定義より上に配置する必要があります。HAT CLI エディタまたは GUI を使用してリスナーの HAT をカスタマイズすることもできます。詳細については、『*User Guide for AsyncOS for Cisco Email Security Appliances*』の「Configuring the Gateway to Receive Mail」と「Using Mail Flow Monitor」の章を参照してください。

ステップ 4 ファイルを保存してインターフェイスの configuration ディレクトリに配置し、インポートできるようにします。(詳細については、付録 B「Accessing the Appliance」を参照してください)。

ステップ 5 listenerconfig の hostaccess -> import サブコマンドを使用して、編集済みのホストアクセス テーブル ファイルをインポートします。

次の例では、編集済みのファイル inbound.HAT.txt を InboundMail リスナーの HAT にインポートします。print サブコマンドを使用して新しいエントリを出力します。

例：

```
mail3.example.com> listenerconfig
Currently configured listeners:
1. InboundMail (on PublicNet, 192.168.2.1) SMTP TCP Port 25 Public
2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP TCP Port 25 Private
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: InboundMail
Type: Public
Interface: PublicNet (192.168.2.1/24) TCP Port 25
Protocol: SMTP
Default Domain:
Max Concurrency: 1000 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
```

```
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[> hostaccess
Default Policy Parameters
=====
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[> import
Enter the name of the file to import:
[> inbound.HAT.txt
9 entries imported successfully.
Default Policy Parameters
=====
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
```

例 : エクスポートおよびインポートによるリスナーのホストアクセス テーブル (HAT) のカスタマイズ

```
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]> print
$ACCEPTED
    ACCEPT
$THROTTLED
    ACCEPT {
        spam_check = "on"
        max_msgs_per_session = 10
        max_concurrency = 10
        max_rcpts_per_msg = 25
        max_rcpts_per_hour = 1
        dhap_limit = 0
        virus_check = "on"
        max_message_size = 1048576
        use_sb = "on"
        tls = "off"
    }
$TRUSTED
    ACCEPT {
        spam_check = "off"
        max_msgs_per_session = 5000
        max_concurrency = 600
        max_rcpts_per_msg = 5000
        max_rcpts_per_hour = -1
        dhap_limit = 0
        virus_check = "on"
        max_message_size = 104857600
        use_sb = "off"
        tls = "off"
    }
$BLOCKED
    REJECT
WHITELIST:
    $TRUSTED (My trusted senders have no anti-spam scanning or rate limiting)
BLACKLIST:
    $BLOCKED (Spammers are rejected)
SUSPECTLIST:
    $THROTTLED (Suspicious senders are throttled)
UNKNOWNLIST:
    $ACCEPTED (Reviewed but undecided, continue normal acceptance)
spamdomain.com
    REJECT (reject the domain "spamdomain.com")
.spamdomain.com
    REJECT (reject all subdomains of ".spamdomain.com")
251.192.1.
    TCPREFUSE (TCPREFUSE the IP addresses in "251.192.1")
169.254.10.10
    RELAY (RELAY the address 169.254.10.10)
ALL
    $ACCEPTED (Everyone else)
Default Policy Parameters
=====
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
Maximum Concurrency Per IP: 1,000
Maximum Message Size: 100M
Maximum Messages Per Connection: 1,000
Maximum Recipients Per Message: 1,000
```

```
Maximum Recipients Per Hour: Disabled
Use SenderBase For Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- CLEAR - Remove all entries.
[]>
```

インポート後には、設定変更を有効にするために、必ず **commit** コマンドを発行します。

例：公開キーのハーベストおよび S/MIME の復号化と検証のイネーブル化

次の例は、下記のことを行う方法を示します。

- 着信 S/MIME 署名済みメッセージから公開キーを取得（ハーベスト）します。
- S/MIME の復号化と検証をイネーブルにします。

```
mail.example.com> listenerconfig
Currently configured listeners:
1. MyListener (on Management, 172.29.181.70) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: MyListener
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 50 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
```

- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.

[> hostaccess

Default Policy Parameters

=====

Maximum Message Size: 10M

Maximum Number Of Concurrent Connections From A Single IP: 10

Maximum Number Of Messages Per Connection: 10

Maximum Number Of Recipients Per Message: 50

Directory Harvest Attack Prevention: Enabled

Maximum Number Of Invalid Recipients Per Hour: 25

Maximum Number Of Recipients Per Hour: Disabled

Maximum Number of Recipients per Envelope Sender: Disabled

Use SenderBase for Flow Control: Yes

Spam Detection Enabled: Yes

Virus Detection Enabled: Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

DKIM/DomainKeys Signing Enabled: No

DKIM Verification Enabled: No

S/MIME Public Key Harvesting Enabled: No

S/MIME Decryption/Verification Enabled: No

SPF/SIDF Verification Enabled: No

DMARC Verification Enabled: No

Envelope Sender DNS Verification Enabled: No

Domain Exception Table Enabled: No

Accept untagged bounces: No

There are currently 4 policies defined.

There are currently 5 sender groups.

Choose the operation you want to perform:

- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.

[> default

Enter the default maximum message size. Add a trailing k for kilobytes, M for megabytes, or no letter for b

[10M]>

Enter the maximum number of concurrent connections allowed from a single IP address.

[10]>

Enter the maximum number of messages per connection.

[10]>

Enter the maximum number of recipients per message.

[50]>

Do you want to override the hostname in the SMTP banner? [N]>

Would you like to specify a custom SMTP acceptance response? [N]>

Would you like to specify a custom SMTP rejection response? [N]>

Do you want to enable rate limiting per host? [N]>

Do you want to enable rate limiting per envelope sender? [N]>

Do you want to enable Directory Harvest Attack Prevention per host? [Y]>

Enter the maximum number of invalid recipients per hour from a remote host.

[25]>

Select an action to apply when a recipient is rejected due to DHAP:

1. Drop

```

2. Code
[1]>
Would you like to specify a custom SMTP DHAP response? [Y]>
Enter the SMTP code to use in the response. 550 is the standard code.
[550]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
custom_response
Would you like to use SenderBase for flow control by default? [Y]>
Would you like to enable anti-spam scanning? [Y]>
Would you like to enable anti-virus scanning? [Y]>
Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>
Would you like to enable DKIM/DomainKeys signing? [N]>
Would you like to enable DKIM verification? [N]>
Would you like to enable S/MIME Public Key Harvesting? [N]> y

Would you like to harvest certificate on verification failure? [N]>

Would you like to harvest updated certificate? [Y]>

Would you like to enable S/MIME gateway decryption/verification? [N]> y

Select the appropriate operation for the S/MIME signature processing:
1. Preserve
2. Remove
[1]>
Would you like to change SPF/SIDF settings? [N]>
Would you like to enable DMARC verification? [N]>
Would you like to enable envelope sender verification? [N]>
Would you like to enable use of the domain exception table? [N]>
Do you wish to accept untagged bounces? [N]>
Default Policy Parameters
=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number Of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
S/MIME Public Key Harvesting Enabled: Yes
S/MIME Decryption/Verification Enabled: Yes
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:

```

例：HATの詳細パラメータ

```
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]>
```

例：HATの詳細パラメータ

次の表では、HAT 詳細パラメータの構文を定義しています。次の値は数値であり、後に **k** を追加してキロバイトで表すか、後に **M** を追加してメガバイトで表すことができます。文字のない値はバイトと見なされます。アスタリスクが付いたパラメータは、次の表に示す変数構文をサポートしています。

表 16：HAT 詳細パラメータの構文

パラメータ	構文	値	値の例
接続あたりの最大メッセージ数	max_msgs_per_session	番号	1000
メッセージあたりの最大受信者数	max_rcpts_per_msg	番号	10000 1k
最大メッセージサイズ (Maximum message size)	max_message_size	番号	1048576 20M
このリスナーに許可された最大同時接続数	max_concurrency	番号	1000
SMTP バナー コード	smtp_banner_code	番号	220
SMTP バナー テキスト (*)	smtp_banner_text	文字列	Accepted
SMTP 拒否バナー コード	smtp_banner_code	番号	550
SMTP 拒否バナー テキスト (*)	smtp_banner_text	文字列	Rejected
SMTPバナーホスト名を上書き	use_override_hostname	on off default	default
	override_hostname	文字列	newhostname
TLS を使用	tls	on off required	on
スパム対策スキャンの使用	spam_check	on off	off

パラメータ	構文	値	値の例
Sophos ウィルス スキャンの使用	virus_check	on off	off
1 時間あたりの最大受信者数	max_rcpts_per_hour	番号	5k
1 時間あたりのエラー コードの最大受信者数	max_rcpts_per_hour_code	番号	452
1 時間あたりのテキストの最大受信者数 (*)	max_rcpts_per_hour_text	文字列	Too many recipients
SenderBase の使用	use_sb	on off	on
SenderBase レピュテーション スコアの定義	sbrs[value1:value2]	-10.0 ~ 10.0	sbrs[-10:-7.5]
ディレクトリ獲得攻撃防止：1 時間あたりの最大無効受信大数	dhap_limit	番号	150

listenerconfig への bypass_ca 引数の追加

次の例では、listenerconfig への bypass_ca 引数の追加を示しています。

```
esa.example.com (SERVICE)> help listenerconfig.
```

```
rcptaccess_options are the following:
  new <rat_addr> [options]
  edit <rat_addr> [options]
  delete <rat_addr>
  print
  import <filename>
  export <filename>
  clear <default_access>

default_access - Default access for empty RAT.  Either "ACCEPT"
                or "REJECT".
rat_addr - Hostnames such as "example.com" and "[1.2.3.4]" are
           allowed. Partial hostnames such as ".example.com"
           are allowed. Usernames such as "postmaster@" are
           allowed. Full email addresses such as
           "joe@example.com" or "joe@[1.2.3.4]" are allowed.
           Separate multiple entries with commas.
options - Various options to modify a host access policy:
  --action      Action to apply to address(es).  Either
                "Accept" or "Reject".  Default is "Accept".
  --cust_resp   Specify a custom SMTP response.  "No" or SMTP
                acceptance response string.
  --resp_code   Custom SMTP response code.  Default is 250 for
                "Accept" actions, 550 for "Reject".
  --bypass_rc   Bypass receiving control.  Default is "No".
  --bypass_la   Bypass LDAP Accept queries for this Recipient.  Default is "No".
```

```
--bypass_ca Bypass SMTP Call-Ahead. Default is "No".
```

例：SPF および SIDF の設定

リスナーのホストアクセステーブルのデフォルトの設定をする場合、リスナーの SPF/SIDF 準拠レベルと、アプライアンスが SPF/SIDF 検証結果に基づいて実行する SMTP アクション（ACCEPT または REJECT）を選択できます。アプライアンスがメッセージを拒否する場合に送信する SMTP 応答を定義することもできます。

準拠レベルに応じて、アプライアンスは HELO ID、MAIL FROM ID、または PRA ID に対してチェックを実行します。アプライアンスが、次の各 ID チェックの各 SPF/SIDF 検証結果に対し、セッションを続行する（ACCEPT）か、セッションを終了する（REJECT）かを指定できます。

- [None]。情報の不足のため、検証を実行できません。
- [Neutral]。ドメイン所有者は、クライアントに指定された ID を使用する権限があるかどうかをアサートしません。
- [SoftFail]。ドメイン所有者は、ホストが指定された ID を使用する権限がないと思うが、断言を避けたいと考えています。
- [失敗]：クライアントは、指定された ID でメールを送信する権限がありません。
- [TempError]。検証中に一時的なエラーが発生しました。
- [PermError]。検証中に永続的なエラーが発生しました。

アプライアンスは、メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、PRA ID の Pass 結果を None にダウングレードするように SIDF 互換準拠レベルを設定していない限り、Pass 結果のメッセージを受け入れます。アプライアンスは PRA チェックで None が返された場合に指定された SMTP アクションを実行します。

ID チェックに対して SMTP アクションを定義していない場合、アプライアンスは Fail を含むすべての検証結果を自動的に受け入れます。

イネーブルにされたいずれかの ID チェックの ID 検証結果が REJECT アクションに一致する場合、アプライアンスはセッションを終了します。たとえば、管理者は、すべての HELO ID チェック結果に基づいてメッセージを受け入れるようにリスナーを設定しますが、MAIL FROM ID チェックからの Fail 結果に対してはメッセージを拒否するようにリスナーを設定するとします。メッセージが HELO ID チェックに失敗しても、アプライアンスはその結果を受け入れるため、セッションが続行します。次に、メッセージが MAIL FROM ID チェックで失敗した場合、リスナーはセッションを終了し、REJECT アクションの SMTP 応答を返します。

SMTP 応答は、アプライアンスが SPF/SIDF 検証結果に基づいてメッセージを拒否する場合に返すコード番号とメッセージです。TempError 結果は、他の検証結果と異なる SMTP 応答を返します。TempError の場合、デフォルトの応答コードは 451 で、デフォルトのメッセージテキストは「#4.4.3 Temporary error occurred during SPF verification」です。他のすべての検証結果では、デフォルトの応答コードは 550 で、デフォルトのメッセージテキストは「#5.7.1 SPF unauthorized mail is prohibited」です。TempError や他の検証結果に独自の応答コードとメッセージテキストを指定できます。

任意で、Neutral、SoftFail、または Fail 検証結果に対して REJECT アクションが実行された場合に、SPF パブリッシャドメインから、サードパーティの応答を返すように、アプライアンスを設定することができます。デフォルトで、アプライアンスは次の応答を返します。

550-#5.7.1 SPF unauthorized mail is prohibited.

550-The domain example.com explains:

550 <Response text from SPF domain publisher>

これらの SPF/SIDF 設定をイネーブルにするには、`listenerconfig -> edit` サブコマンドを使用し、リスナーを選択します。次に、`hostaccess -> default` サブコマンドを使用して、ホストアクセステーブルのデフォルトの設定を編集します。次のプロンプトに **yes** と答えて、SPF 制御を設定します。

```
Would you like to change SPF/SIDF settings? [N]> yes

Would you like to perform SPF/SIDF Verification? [Y]> yes
```

ホスト アクセス テーブルでは、次の SPF 制御設定を使用できます。

表 17: SPF 制御設定

準拠レベル	使用可能な SPF 制御設定
SPF のみ (SPF Only)	<ul style="list-style-type: none"> • HELO ID チェックを実行するかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション • HELO ID (イネーブルの場合) • MAIL FROM ID • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト
SIDF 互換 (SIDF Compatible)	<ul style="list-style-type: none"> • HELO ID チェックを実行するかどうか • メッセージに Resent-Sender: または Resent-From: ヘッダーが存在する場合に、検証で PRA ID の Pass 結果を None にダウングレードするかどうか • 次の ID チェックの結果に基づいて実行される SMTP アクション • HELO ID (イネーブルの場合) • MAIL FROM ID • PRA Identity • REJECT アクションに対して返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト

例：SPF/SIDF 設定

準拠レベル	使用可能な SPF 制御設定
SIDF 厳格 (SIDF Strict)	<ul style="list-style-type: none"> • 次の ID チェックの結果に基づいて実行される SMTP アクション • MAIL FROM ID • PRA Identity • SPF REJECT アクションの場合に返される SMTP 応答コードとテキスト • 秒単位の検証タイムアウト

次に、ユーザが SPF Only 準拠レベルを使用して、SPF/SIDF 検証を設定する例を示します。アプライアンスは HELO ID チェックを実行し、None および Neutral 検証結果を受け入れ、その他の結果を拒否します。SMTP アクションの CLI プロンプトはすべての ID タイプで同じです。ユーザは MAIL FROM ID の SMTP アクションを定義しません。アプライアンスは、その ID のすべての検証結果を自動的に受け入れます。アプライアンスはすべての REJECT 結果に対して、デフォルトの拒否コードとテキストを使用します。

例：SPF/SIDF 設定

```

Would you like to change SPF/SIDF settings? [N]> yes
Would you like to perform SPF/SIDF Verification? [N]> yes
What Conformance Level would you like to use?
1. SPF only
2. SIDF compatible
3. SIDF strict
[2]> 1
Would you like to have the HELO check performed? [Y]> y
Would you like to change SMTP actions taken as result of the SPF verification? [N]> y
Would you like to change SMTP actions taken for the HELO identity? [N]> y
What SMTP action should be taken if HELO check returns None?
1. Accept
2. Reject
[1]> 1
What SMTP action should be taken if HELO check returns Neutral?
1. Accept
2. Reject
[1]> 1
What SMTP action should be taken if HELO check returns SoftFail?
1. Accept
2. Reject
[1]> 2
What SMTP action should be taken if HELO check returns Fail?
1. Accept
2. Reject
[1]> 2
What SMTP action should be taken if HELO check returns TempError?
1. Accept
2. Reject
[1]> 2
What SMTP action should be taken if HELO check returns PermError?
1. Accept
2. Reject
[1]> 2
Would you like to change SMTP actions taken for the MAIL FROM identity? [N]> n
Would you like to change SMTP response settings for the REJECT action? [N]> n
Verification timeout (seconds)
[40]>

```

次に、リスナーのデフォルトのポリシーパラメータに SPF/SIDF 設定がどのように表示されるかを示します。

例：デフォルトポリシーパラメータの SPF/SIDF

```
SPF/SIDF Verification Enabled: Yes
Conformance Level: SPF only
Do HELO test: Yes
SMTP actions:
  For HELO Identity:
    None, Neutral: Accept
    SoftFail, Fail, TempError, PermError: Reject
  For MAIL FROM Identity: Accept
SMTP Response Settings:
  Reject code: 550
  Reject text: #5.7.1 SPF unauthorized mail is prohibited.
  Get reject response text from publisher: Yes
  Defer code: 451
  Defer text: #4.4.3 Temporary error occurred during SPF verification.
Verification timeout: 40
```

例：DMARC 検証の有効化

次に、DMARC 検証を有効にする例を示します。

```
mail.example.com> listenerconfig
Currently configured listeners:
1. Listener 1 (on Management, 172.29.181.70) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]> edit
Enter the name or number of the listener you wish to edit.
[]> 1
Name: Listener 1
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 300 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
```

```

- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]> hostaccess
Default Policy Parameters
=====
Maximum Message Size: 20M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.
There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]> default
Enter the default maximum message size. Add a trailing k for kilobytes, M for megabytes,
or no letter for bytes.
[20M]>
Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>
Enter the maximum number of messages per connection.
[10]>
Enter the maximum number of recipients per message.
[50]>
Do you want to override the hostname in the SMTP banner? [N]>
Would you like to specify a custom SMTP acceptance response? [N]>
Would you like to specify a custom SMTP rejection response? [N]>
Do you want to enable rate limiting per host? [N]>
Do you want to enable rate limiting per envelope sender? [N]>
Do you want to enable Directory Harvest Attack Prevention per host? [Y]>
Enter the maximum number of invalid recipients per hour from a remote host.
[25]>
Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>
Would you like to specify a custom SMTP DHAP response? [Y]>
Enter the SMTP code to use in the response. 550 is the standard code.
[550]>
Enter your custom SMTP response. Press Enter on a blank line to finish.

```

```

Would you like to use SenderBase for flow control by default? [Y]>
Would you like to enable anti-spam scanning? [Y]>
Would you like to enable anti-virus scanning? [Y]>
Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>
Would you like to enable DKIM/DomainKeys signing? [N]>
Would you like to enable DKIM verification? [N]>
Would you like to change SPF/SIDF settings? [N]>
Would you like to enable DMARC verification? [N]> Y
Select the DMARC verification profile to use:
1. DEFAULT
[1]> 1
Would you like to send aggregate reports? [N]> Y
Note: DMARC reports should be DMARC compliant.
      Secure delivery is recommended for delivery of DMARC reports.
      Please enable TLS support using the `destconfig` command.
Would you like to enable envelope sender verification? [N]> Y
Would you like to specify a custom SMTP response for malformed envelope senders? [Y]>
Enter the SMTP code to use in the response. 553 is the standard code.
[553]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
Would you like to specify a custom SMTP response for envelope sender domains which do
not resolve? [Y]>
Enter the SMTP code to use in the response. 451 is the standard code.
[451]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
Would you like to specify a custom SMTP response for envelope sender domains which do
not exist? [Y]>
Enter the SMTP code to use in the response. 553 is the standard code.
[553]>
Enter your custom SMTP response. Press Enter on a blank line to finish.
Would you like to enable use of the domain exception table? [N]>
Do you wish to accept untagged bounces? [N]>
Default Policy Parameters
=====
Maximum Message Size: 20M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: Yes
      DMARC Verification Profile: DEFAULT
      Aggregate reports: Yes
Envelope Sender DNS Verification Enabled: Yes
Domain Exception Table Enabled: No
Accept untagged bounces: No
There are currently 4 policies defined.

```

```

There are currently 5 sender groups.
Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
[]>
Name: Listener 1
Type: Public
Interface: Management (172.29.181.70/24) TCP Port 25
Protocol: SMTP
Default Domain: <none configured>
Max Concurrent Connections: 300 (TCP Queue: 50)
Domain Map: Disabled
TLS: No
SMTP Authentication: Disabled
Bounce Profile: Default
Use SenderBase For Reputation Filters and IP Profiling: Yes
Footer: None
Heading: None
SMTP Call-Ahead: Disabled
LDAP: Off
Choose the operation you want to perform:
- NAME - Change the name of the listener.
- INTERFACE - Change the interface.
- CERTIFICATE - Choose the certificate.
- LIMITS - Change the injection limits.
- SETUP - Configure general options.
- HOSTACCESS - Modify the Host Access Table.
- RCPTACCESS - Modify the Recipient Access Table.
- BOUNCECONFIG - Choose the bounce profile to use for messages injected on this listener.
- MASQUERADE - Configure the Domain Masquerading Table.
- DOMAINMAP - Configure domain mappings.
[]>
Currently configured listeners:
1. Listener 1 (on Management, 172.29.181.70) SMTP TCP Port 25 Public
Choose the operation you want to perform:
- NEW - Create a new listener.
- EDIT - Modify a listener.
- DELETE - Remove a listener.
- SETUP - Change global settings.
[]>
mail.example.com>

```

localeconfig

説明

多言語対応の設定値を設定します。

使用方法

確定 : このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> localeconfig
```

```
Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading
encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the
message body is added as an attachment.
```

```
Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[]> setup
```

```
If a header is modified, encode the new header in the same encoding as the message body?
```

```
(Some MUAs incorrectly handle headers encoded in a different encoding than the body.
However, encoding a modified header in the same encoding as the message body may cause
certain
characters in the modified header to be lost.) [Y]>
```

```
If a non-ASCII header is not properly tagged with a character set and is being used or
modified,
impose the encoding of the body on the header during processing and final representation
of the message?
(Many MUAs create non-RFC-compliant headers that are then handled in an undefined way.
Some MUAs handle headers encoded in character sets that differ from that of the main
body in an incorrect way.
Imposing the encoding of the body on the header may encode the header more precisely.
This will be used to interpret the content of headers for processing, it will not modify
or rewrite the
header unless that is done explicitly as part of the processing.) [Y]>
```

```
Disclaimers (as either footers or headings) are added in-line with the message body
whenever possible.
However, if the disclaimer is encoded differently than the message body, and if imposing
a single encoding
will cause loss of characters, it will be added as an attachment. The system will always
try to use the
message body's encoding for the disclaimer. If that fails, the system can try to edit
the message body to
use an encoding that is compatible with the message body as well as the disclaimer.
Should the system try to
re-encode the message body in such a case? [Y]>
```

```
If the disclaimer that is added to the footer or header of the message generates an error
when decoding the message body,
it is added at the top of the message body. This prevents you to rewrite a new message
content that must merge with
the original message content and the header/footer-stamp. The disclaimer is now added
as an additional MIME part
that displays only the header disclaimer as an inline content, and the rest of the message
content is split into
separate email attachments. Should the system try to ignore such errors when decoding
the message body? [N]>
```

```

Behavior when modifying headers: Use encoding of message body
Behavior for untagged non-ASCII headers: Impose encoding of message body
Behavior for mismatched footer or heading encoding: Try both body and footer or heading encodings
Behavior when decoding errors found: Disclaimer is displayed as inline content and the message body is added as an attachment.

Choose the operation you want to perform:
- SETUP - Configure multi-lingual settings.
[> mail3.example.com

```

smtpauthconfig

説明

SMTP 認証発信および転送プロファイルを設定します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

次の例では、**smtpauthconfig** コマンドを使用して、サーバ「smtp2.example.com」の新しい転送ベースのプロファイルを作成します。

```

mail3.example.com> smtpauthconfig
Choose the operation you want to perform:
- NEW - Create a new SMTP Auth profile
[> new
Choose the type of profile you wish to create:
- FORWARD - Create an SMTP Auth forwarding server group profile
- OUTGOING - Create an outgoing SMTP Auth profile
[> forward
Enter a name for this profile:
[> forwarding-based
Please begin entering forwarding servers for this group profile.
Enter a hostname or an IP address for the forwarding server:
[> smtp2.example.com
Enter a port:
[25]>
Choose the interface to use for forwarding requests:
1. Auto
2. Data 1 (192.168.1.1/24: mail3.example.com)
3. Data 2 (192.168.2.1/24: mail3.example.com)
4. Management (192.168.42.42/24: mail3.example.com)
[1]>
Require TLS? (issue STARTTLS) [Y]> y
Enter the maximum number of simultaneous connections allowed:
[10]>
Use SASL PLAIN mechanism when contacting forwarding server? [Y]>

```

```
Use SASL LOGIN mechanism when contacting forwarding server? [Y]>
Would you like to enter another forwarding server to this group? [N]>
Choose the operation you want to perform:
- NEW - Create a new SMTP Auth profile
- EDIT - Edit an existing SMTP Auth profile
- PRINT - List all profiles
- DELETE - Delete a profile
- CLEAR - Delete all profiles
[]>
mail3.example.com> commit
Please enter some comments describing your changes:
[]> created SMTP auth profile
Do you want to save the current configuration for rollback? [Y]> n
Changes committed: Fri May 23 11:42:12 2014 GMT
```



(注) 認証済みのユーザには、RELAY HAT ポリシーが許可されます。

1 つのプロファイル内で複数の転送サーバを指定することもできます。SASL メカニズム CRAM-MD5 と DIGEST-MD5 は、E メールセキュリティ アプライアンスと転送サーバの間ではサポートされません。

システムのセットアップ

systemsetup

説明

初回のシステム セットアップおよびシステムの再インストール。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> systemsetup
WARNING: The system setup wizard will completely delete any existing
'listeners' and all associated settings including the 'Host Access Table' -
mail operations may be interrupted.
Are you sure you wish to continue? [Y]> y
Before you begin, please reset the administrator passphrase to a new value.
Old passphrase:
New passphrase:
Retype new passphrase:
*****
```

```

You will now configure the network settings for the IronPort C100.
Please create a fully qualified hostname for the IronPort C100 appliance
(Ex: "ironport-c100.example.com"):
[]> ironport-c100.example.com
*****
You will now assign an IP address for the "Data 1" interface.
Please create a nickname for the "Data 1" interface (Ex: "Data 1"):
[]> Data 1
Enter the static IP address for "Data 1" on the "Data 1" interface? (Ex:
"192.168.1.1"):
[]> 192.168.1.1
What is the netmask for this IP address? (Ex: "255.255.255.0" or "0xffffffff"):
[255.255.255.0]>
You have successfully configured IP Interface "Data 1".
*****
Would you like to assign a second IP address for the "Data 1" interface? [Y]> n
What is the IP address of the default router (gateway) on your network?:
[192.168.1.1]> 192.168.2.1
*****
Do you want to enable the web interface on the Data 1 interface? [Y]> y
Do you want to use secure HTTPS? [Y]> y
Note: The system will use a demo certificate for HTTPS.
Use the "certconfig" command to upload your own certificate.
*****
Do you want the IronPort C100 to use the Internet's root DNS servers or would
you like it to use your own DNS servers?
1. Use Internet root DNS servers
2. Use my own DNS servers
[1]> 2
Please enter the IP address of your DNS server.
[]> 192.168.0.3
Do you want to enter another DNS server? [N]>
You have successfully configured the DNS settings.
*****
You are now going to configure how the IronPort C100 accepts mail by creating a
"Listener".
Please create a name for this listener (Ex: "MailInterface"):
[]> InboundMail
Please choose an IP interface for this Listener.
1. Data 1 (192.168.1.1/24: ironport-c100.example.com)
[1]> 1
Enter the domain names or specific email addresses you want to accept mail for.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
Usernames such as "postmaster@" are allowed.
Full email addresses such as "joe@example.com" or "joe@[1.2.3.4]" are allowed.
Separate multiple addresses with commas.
[]> example.com, .example.com
Would you like to configure SMTP routes for example.com, .example.com? [Y]> n
Please specify the systems allowed to relay email through the IronPort C100.
Hostnames such as "example.com" are allowed.
Partial hostnames such as ".example.com" are allowed.
IP addresses, IP address ranges, and partial IP addresses are allowed.
Separate multiple entries with commas.
[]> example.com, .example.com
Do you want to enable filtering based on SenderBase Reputation Service (SBRS)
Scores for this listener? (Your selection will be used to filter all incoming
mail based on its SBRS Score.) [Y]> y
Do you want to enable rate limiting for this listener? (Rate limiting defines
the maximum number of recipients per hour you are willing to receive from a
remote domain.) [Y]> y
Enter the maximum number of recipients per hour to accept from a remote domain.
[]> 1000
Default Policy Parameters

```

```

=====
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: 1,000
Maximum Recipients Per Hour SMTP Response:
    452 Too many recipients received this hour
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No
Would you like to change the default host access policy? [N]> n
Listener InboundMail created.
Defaults have been set for a Public listener.
Use the listenerconfig->EDIT command to customize the listener.
*****
Do you want to use Anti-Spam scanning in the default Incoming Mail policy? [Y]> y
Would you like to enable IronPort Spam Quarantine? [Y]> y
IronPort Anti-Spam configured globally for the IronPort C100 appliance. Use the
policyconfig command (CLI) or Mail Policies (GUI) to customize the IronPort
settings for each listener.
IronPort selected for DEFAULT policy
*****
Do you want to use Anti-Virus scanning in the default Incoming and Outgoing
Mail policies? [Y]> y
1. McAfee Anti-Virus
2. Sophos Anti-Virus
Enter the number of the Anti-Virus engine you would like to use on the default
Incoming and Outgoing Mail policies.
[]> 2
Sophos selected for DEFAULT policy
*****
Do you want to enable Outbreak Filters? [Y]> y
Outbreak Filters enabled.
Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or
back down below),
meaning that new messages of certain types could be quarantined or will no longer be
quarantined, respectively.
Allow the sharing of limited data with SenderBase? [Y]> y
You have successfully configured Outbreak Filters and SenderBase.
*****
You will now configure system alerts.
Please enter the email address(es) to send alerts.
(Ex: "administrator@example.com")
Separate multiple addresses with commas.
[]> administrator@example.com
Would you like to enable IronPort AutoSupport, which automatically emails
system alerts and weekly status reports directly to IronPort Customer Support?
You will receive a complete copy of each message sent to IronPort.
(Recommended) [Y]> y
*****
You will now configure scheduled reporting.

```

```

Please enter the email address(es) to deliver scheduled reports to.
(Leave blank to only archive reports on-box.)
Separate multiple addresses with commas.
[]> administrator@example.com
*****
You will now configure system time settings.
Please choose your continent:
1. Africa
2. America
...
11. GMT Offset
[11]> 2
Please choose your country:
1. Anguilla
...
47. United States
48. Uruguay
49. Venezuela
50. Virgin Islands (British)
51. Virgin Islands (U.S.)
[]> 47
Please choose your timezone:
1. Alaska Time (Anchorage)
...
26. Pacific Time (Los_Angeles)
[]> 26
Do you wish to use NTP to set system time? [Y]> y
Please enter the fully qualified hostname or IP address of your NTP server, or
press Enter to use time.ironport.com:
[time.ironport.com]>
*****
Would you like to commit these changes at this time? [Y]> y
Congratulations! System setup is complete.
For advanced configuration, please refer to the User Guide.

```

URL フィルタリング

ここでは、次の CLI コマンドについて説明します。

- [aggregatorconfig](#) (278 ページ)
- [urllistconfig](#) (279 ページ)
- [webcacheflush](#) (280 ページ)
- [websecurityadvancedconfig](#) (280 ページ)
- [websecurityconfig](#) (284 ページ)
- [websecuritydiagnostics](#) (284 ページ)

aggregatorconfig

説明

E メールセキュリティ アプライアンスでシスコのアグリゲータ サーバのアドレスを設定します。このサーバは、リライトされた URL と、各ユーザのクリックに関連付けられたアクション（許可、ブロック、または不明）をクリックしたエンドユーザの詳細を提供します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail.example.com> aggregatorconfig
Choose the operation you want to perform:
- EDIT - Edit aggregator configuration
[]> edit
Edit aggregator address:
[aggregator.organization.com]> org-aggregator.com
Successfully changed aggregator address to : org-aggregator.com
```

urllistconfig

説明

URL フィルタリング機能によって評価されない URL のホワイトリストを設定またはインポートします。このリストは、アウトブレイク フィルタ機能には使用されません。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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。

例

```
> urllistconfig
No URL lists configured.
Choose the operation you want to perform:
NEW - Create a new URL list-
[]> new
Do you want to import a URL list?
[N]>
Enter a name for the URL list
[]> sample
Enter the URL domains that need to be skipped from scanning for URL Filtering.
Enter one URL domain per line and '.' to finish.
cisco.com
ironport.com/*
*.example.com
10.2.4.5/24
[2001:DB8::1]
URL list sample added.
```

```

There are currently 4 URL lists configured.
Choose the operation you want to perform:
- NEW - Create a new URL whitelist.
- EDIT - Modify an existing URL whitelist.
- DELETE - Delete an existing URL whitelist.
[]>EDIT
Choose the operation to edit the URL whitelist:
- IMPORT - Import a file into an existing URL whitelist
- EXPORT - Export an existing URL whitelist into a file
- RENAME - Rename an existing URL whitelist
[]>IMPORT
Assign new name to the imported list? (By default, name stored in the
file will be applied to the list)
[N] > Y
Enter name of the list > new_list
Enter filename to import from > URLfile
NOTE: These files will be stored in /pub/configuration
URL list "new_list" added.

```

webcacheflush

説明

URL フィルタリング機能で使用するキャッシュをフラッシュします。シスコの Web セキュリティサービスとの通信に使用される証明書を変更した場合は、このコマンドを使用します。通常、シスコ サポートから指示された場合にのみ、このコマンドを使用します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```

> webcacheflush
Web Security cache has been flushed.

```

websecurityadvancedconfig

説明

次の URL フィルタリングの詳細設定を設定します。

- [URLルックアップのタイムアウト (URL Lookup Timeout)] : URL で特定のドメイン名の IP アドレスを要求するためにかかる時間。
- [URLキャッシュサイズ (URL Cache Size)] : URL フィルタリングを設定するために必要な URL の数。

- [DNSルックアップの無効化 (Disable DNS Lookup)] : DNS ルックアップはドメイン名を IP アドレスに解決し、テレメトリ情報の更新にかかる時間を予測します。
- [スキャンするURLの最大数 (Maximum number of URLs to scan)] : メッセージ本文またはメッセージ添付ファイルでスキャンされる URL の最大数。
- [ホスト名 (Hostname)] : Web セキュリティ サービスのホスト名。
- [未処理リクエストのしきい値 (Threshold Value for Outstanding Requests)] : 未処理のリクエストのしきい値。
- [サーバ証明書の検証 (Verify Server Certificate)] : ドメインのサーバ証明書を検証します。
- [存続可能時間値 (Time-to-live Value)] : アプライアンスが URL レピュテーション サービスから URL のレピュテーションを取得した後、URL レピュテーションはキャッシュに保持されます。デフォルトの存続可能時間値は、URL レピュテーションがキャッシュ内に保持される秒数を示します。この値は、URL レピュテーション サービスによって上書きされる可能性があります。
- [メッセージ内のURLテキストとHREFの書き換え (Rewrite URL text and HREF in the message)] : 完全に書き換えられた URL をメッセージ本文に表示するか、書き換えられた URL を HTML メッセージの HREF にのみ表示するかを選択できます。
- [追加ヘッダー (Additional Header)] : 必要に応じて、メッセージにカスタム ヘッダーを含めます。
- [RPCサーバのデフォルトログレベル (Default Log Level for RPC Server)] : RPC サーバのデフォルト ログ レベル。
- [URLキャッシュのデフォルトログレベル (Default Log Level for URL Cache)] : URL キャッシュのデフォルト ログ レベル。
- [HTTPクライアントのデフォルトログレベル (Default Log Level for HTTP Client)] : HTTP クライアントのデフォルト ログ レベル。



(注) トラブルシューティングの目的でタイムアウト値を変更する場合以外は、シスコのサポートから指示があった場合にのみこのコマンドを使用します。

タイムアウト値は、URL の評価およびカテゴリを提供するクラウドサービスとの通信用の秒単位の値です。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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。

バッチ形式

バッチ形式については、CLI インライン ヘルプを参照してください。

例

```
> websecurityadvancedconfig
Enter URL lookup timeout (includes any DNS lookup time) in seconds:
[15]>
Enter the URL cache size (no. of URLs):
[1215000]>
Do you want to disable DNS lookups? [N]>
Enter the maximum number of URLs that should be scanned:
[100]>
Enter the Web security service hostname:
[example.com]>
Enter the threshold value for outstanding requests:
[20]>
Do you want to verify server certificate? [Y]>
Enter the default time-to-live value (seconds):
[30]>
Do you want to include additional headers? [N]>
Enter the default debug log level for RPC server:
[Info]>
Enter the default debug log level for SDS cache:
[Info]>
Enter the default debug log level for HTTP client:
[Info]>
```

例 : 短縮 URL の URL フィルタリングの有効化

次の例では、websecurityadvancedconfig コマンドを使用して、短縮 URL の URL フィルタリングを有効にします。

```
mail1.example.com> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds: [5]>

Enter the URL cache size (no. of URLs): [810000]>

Do you want to disable DNS lookups? [N]>

Enter the maximum number of URLs that should be scanned: [100]>

Enter the Web security service hostname: [v2.sds.cisco.com]>

Enter the threshold value for outstanding requests: [50]>

Do you want to verify server certificate? [Y]>

Do you want to enable URL filtering for shortened URLs? [Y]> yes

For shortened URL support to work, please ensure that ESA is able to connect to the
following domains:
bit.ly, tinyurl.com, ow.ly, tumblr.com, post/ly .....

Enter the default time-to-live value (seconds): [30]>
```

```
Do you want to rewrite both the URL text and the href in the message?
Y indicates that the full rewritten URL will appear in the email body.
N indicates that the rewritten URL will only be visible in the href for HTML messages.
[N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server: [Info]>

Enter the default debug log level for URL cache: [Info]>

Enter the default debug log level for HTTP client: [Info]>
```

例 : メッセージの添付ファイルの URL に対するスキャン制限の設定

次の例では、websecurityadvancedconfig コマンドを使用して、メッセージの添付ファイル内でスキャンできる URL の最大数を設定します。

```
mail1.example.com> websecurityadvancedconfig

Enter URL lookup timeout (includes any DNS lookup time) in seconds: [5]>

Enter the URL cache size (no. of URLs): [810000]>

Do you want to disable DNS lookups? [N]>

Enter the maximum number of URLs that can be scanned in a message body: [100]>

Enter the maximum number of URLs that can be scanned in the attachments in a message:
[25]>

Enter the Web security service hostname: [v2.sds.cisco.com]>

Enter the threshold value for outstanding requests: [50]>

Do you want to verify server certificate? [Y]>

Do you want to enable URL filtering for shortened URLs? [Y]>

Enter the default time-to-live value (seconds): [30]>

Do you want to rewrite both the URL text and the href in the message?
Y indicates that the full rewritten URL will appear in the email body.
N indicates that the rewritten URL will only be visible in the href for HTML messages.
[N]>

Do you want to include additional headers? [N]>

Enter the default debug log level for RPC server: [Info]>

Enter the default debug log level for URL cache: [Info]>

Enter the default debug log level for HTTP client: [Info]>
```

websecurityconfig

説明

URL フィルタリングの基本設定（URL レピュテーションおよび URL カテゴリ機能）を設定します。

通常、証明書管理は自動です。Cisco TAC から Yes にすることを指示されていない限り、証明書の設定を要求されたときに No を選択してください。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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、CLI のインライン ヘルプを参照してください。このコマンドのインライン ヘルプにアクセスするには、help コマンドを使用します。

例

```
mail.example.com> websecurityconfig
Enable URL Filtering? [N]> y
Do you wish to enable Web Interaction Tracking? [N]> y
Web Interaction Tracking is enabled.
Do you want to whitelist URLs using a URL list? [N]> y
1. urllist1
2. urllist2
3. No URL list
Enter the number of URL list
[1]> 1
URL list 'urllist1' added
mail.example.com> websecurityconfig
URL Filtering is enabled.
URL list 'urllist1' used.
System provided certificate used.
Web Interaction Tracking is enabled.
```

websecuritydiagnostics

説明

URL フィルタリングに関連する診断統計情報を表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシン モードでのみ使用できます。

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せん。

例

```
mail.example.com> websecuritydiagnostics
Cache Size: 254
Cache Hits: 551
Response Time
  Minimum: None
  Average: 0.0
  Maximum: None
DNS Lookup Time
  Minimum: 9.4198775
  Average: 10.1786801765
  Maximum: 10.544356
```

ユーザ管理

ここでは、次の CLI コマンドについて説明します。

- [userconfig](#) (285 ページ)
- [passphrase](#) または [passwd](#) (290 ページ)
- [last](#) (290 ページ)
- [who](#) (291 ページ)
- [whoami](#) (291 ページ)

userconfig

説明

ユーザ アカウントと外部の認証ソースへの接続を管理します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはクラスタ モードでのみ使用できます。

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、CLI のインライン ヘルプを参照してください。このコマンドのインライン ヘルプにアクセスするには、`help` コマンドを使用します。例：

```
mail.example.com> userconfig help
```

例：新しいユーザ アカウントの作成

次に、Help Desk User ロールを持つ新しいユーザ アカウントの作成例を示します。

```
mail.example.com> userconfig
```

例：RADIUS サーバを外部認証用にセットアップ

```

Users:
1. admin - "Administrator" (admin)
External authentication: Disabled
Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change passphrase and account policy settings.
- PASSPHRASE - Change the passphrase for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
- URLTRACKING - Configure URL tracking privileges.
[]> new
Enter your Passphrase to make changes:
Enter the new username.
[]> helpdesk
Enter the full name for helpdesk.
[]> HELP DESK
Assign a role to "helpdesk":
1. Administrators - Administrators have full access to all settings of the system.
2. Operators - Operators are restricted from creating new user accounts.
3. Read-Only Operators - Read-Only operators may only view settings and status information.
4. Guests - Guest users may only view status information.
5. Technicians - Technician can only manage upgrades and feature keys.
6. Help Desk Users - Help Desk users have access only to ISQ and Message Tracking.
[1]> 6
Would you like to get a system generated passphrase? [N]>
Enter the passphrase for helpdesk
[]>
Please enter the new passphrase again:
Users:
1. admin - "Administrator" (admin)
2. helpdesk - "HELP DESK" (helpdesk)
External authentication: Disabled
Choose the operation you want to perform:
- NEW - Create a new account.
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change passphrase and account policy settings.
- PASSPHRASE - Change the passphrase for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
- URLTRACKING - Configure URL tracking privileges.
[]>

```

例：RADIUS サーバを外部認証用にセットアップ

次に、RADIUS サーバを外部認証用にセットアップする例を示します。RADIUS サーバをセットアップするには、ホスト名、ポート、および共有パスフレーズを入力し、認証プロトコルとして CHAP と PAP のどちらを使用するかを指定します。

```

mail.example.com> userconfig
Users:
1. admin - "Administrator" (admin)
2. hdesk_user - "Helpdesk User" (helpdesk)
External authentication: Disabled
Choose the operation you want to perform:
- NEW - Create a new account.

```

```
- EDIT - Modify an account.
- DELETE - Remove an account.
- POLICY - Change passphrase and account policy settings.
- PASSPHRASE - Change the passphrase for a user.
- ROLE - Create/modify user roles.
- STATUS - Change the account status.
- EXTERNAL - Configure external authentication.
- DLPTRACKING - Configure DLP tracking privileges.
- URLTRACKING - Configure URL tracking privileges.
[]> external
Choose the operation you want to perform:
- SETUP - Set up global settings.
[]> setup
Do you want to enable external authentication? [N]> Y
Please enter the timeout in seconds for how long the external authentication credentials
will be cached. (Enter '0' to disable expiration of
authentication credentials altogether when using one time passphrases.)
[0]> 30
Choose a mechanism to use:
LDAP is unavailable because no LDAP queries of type EXTERNALAUTH are configured
1. RADIUS
[1]> 1
Configured RADIUS servers:
- No RADIUS servers configured
Choose the operation you want to perform:
- NEW - Add a RADIUS server configuration.
[]> new
Please enter host name or IP address of the RADIUS server:
[]> radius.example.com
Please enter port number of the RADIUS server:
[1812]>
Please enter the shared passphrase:
>
Please enter the new passphrase again.
>
Please enter timeout in seconds for receiving a valid reply from the server:
[5]>
1. CHAP
2. PAP
Select authentication type:
[2]>
Configured RADIUS servers:
Host Port Timeout (s) Auth type
-----
radius.example.com 1812 5 pap
Choose the operation you want to perform:
- NEW - Add a RADIUS server configuration.
- EDIT - Modify a RADIUS server configuration.
- DELETE - Remove a RADIUS server configuration.
- CLEAR - Remove all RADIUS server configurations.
[]>
```

例：特定のユーザ ロールに対する二要素認証の有効化

次の例では、twofactorauth サブ コマンドを使用して、特定のユーザ ロールに対して二要素認証を有効にします。

```
mail.example.com> userconfig

Users:

1. admin - "Administrator" (admin)
```

```
2. hdesk_user - "Helpdesk User" (helpdesk)

External authentication: Disabled

Two-Factor Authentication: Disabled

Choose the operation you want to perform:

- NEW - Create a new account.

- EDIT - Modify an account.

- DELETE - Remove an account.

- POLICY - Change passphrase and account policy settings.

- PASSPHRASE - Change the passphrase for a user.

- ROLE - Create/modify user roles.

- STATUS - Change the account status.

- EXTERNAL - Configure external authentication.

- TWOFACTORAUTH - Configure Two-Factor Authentication.

- DLPTRACKING - Configure DLP tracking privileges.

- URLTRACKING - Configure URL tracking privileges.

[]> twofactorauth

Choose the operation you want to perform:

- SETUP - Set up global settings.

- PRIVILEGES - Configure Two-Factor Authentication based on User Role Privileges.

[]> setup

Do you want to enable external authentication? [N]> y

Choose the operation you want to perform:

- NEW - Add a two-factor authentication server configuration.

- EDIT - Modify two-factor authentication server configuration.

- DELETE - Remove a two-factor authentication server configuration.

- CLEAR - Remove all two-factor authentication server configurations.

[]> new

Please enter host name or IP address of the RADIUS server:

[]> radius.example.com

Please enter port number of the RADIUS server:

[1812]> 1800

Please enter the shared passphrase:
```



```

>

Please enter the new passphrase again.

>

Please enter timeout in seconds for receiving a valid reply from the server:

[5]> 10

1. CHAP
2. PAP

Select authentication type:

[2]> 2

Choose the operation you want to perform:

- SETUP - Set up global settings.
- PRIVILEGES - Configure Two-Factor Authentication based on Role Privileges.

[> privileges

Role Privileges:

Choose the operation you want to perform:

1. Add

[> 1

Select Predefined Roles to allow the privileges

1. Administrators
2. Guests
3. Help Desk Users
4. Operators
5. Read-Only Operators
6. Technicians

Enter the numbers (comma separated) to add privilege.

[> 1

Role Privileges:

Predefined:

Administrators

Choose the operation you want to perform:

1. Add
2. Delete

```

[]>

passphrase または passwd

説明

パスフレーズを変更します。

使用方法

確定：このコマンドは「commit」が必要です。

クラスタ管理：このコマンドはクラスタ モードでのみ使用できます。



(注) passwd コマンドは、マシンモードしか使用できないゲストユーザが使用できるようにするための特例です。ゲストユーザがクラスタ内のマシン上で passwd コマンドを実行すると、警告メッセージは表示されず、ユーザのモードを変更せずにクラスタレベルのデータに対して操作が行われます。他のすべてのユーザに対しては、上記の（他の制限されるコンフィギュレーション コマンドと同じ）動作が行われます。

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せん。

例

```
mail3.example.com> passphrase
Old passphrase: your_old_passphrase
New passphrase: your_new_passphrase
Retype new passphrase: your_new_passphrase
passphrase changed.
```

last

説明

last コマンドは、システムに最近ログインしたユーザを表示します。デフォルトでは、システムにログインしているすべてのユーザを表示します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
elroy.run> last
=====
Username Remote Host Login Time Logout Time Total Time
=====
admin 10.251.23.186 Thu Sep 01 09:14 still logged in 1h 5m
admin 10.251.23.186 Wed Aug 31 14:00 Wed Aug 31 14:01 1m
admin 10.251.16.231 Wed Aug 31 13:36 Wed Aug 31 13:37 0m
admin 10.251.23.186 Wed Aug 31 13:34 Wed Aug 31 13:35 0m
admin 10.251.23.142 Wed Aug 31 11:26 Wed Aug 31 11:38 11m
admin 10.251.23.142 Wed Aug 31 11:05 Wed Aug 31 11:09 4m
admin 10.251.23.142 Wed Aug 31 10:52 Wed Aug 31 10:53 1m
admin 10.251.60.37 Tue Aug 30 01:45 Tue Aug 30 02:17 32m
admin 10.251.16.231 Mon Aug 29 10:29 Mon Aug 29 10:41 11m
shutdown Thu Aug 25 22:20
```

who

説明

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

使用方法

確定：このコマンドに「**commit**」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。このコマンドを使用するには、ローカル ファイル システムにアクセスする必要があります。

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せん。

例

```
mail3.example.com> who
=====
Username Login Time Idle Time Remote Host What
=====
admin 03:27PM 0s 10.1.3.201 cli
```

whoami

説明

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

使用方法

確定：このコマンドは「**commit**」が必要です。

クラスタ管理：このコマンドは、すべてのマシンモード（クラスタ、グループ、マシン）で使用できます。

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せん。

例

```
mail3.example.com> whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

仮想アプライアンスの管理

- [loadlicense](#) （292 ページ）
- [showlicense](#) （293 ページ）

loadlicense

説明

仮想アプライアンスの XML ライセンスをロードします。ファイルからロードするか、コピーアンドペーストできます。詳細については、『*Cisco Content Security Virtual Appliance Installation Guide*』を参照してください。このドキュメントは、<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html> から入手できます。

このコマンドは、管理者またはオペレータ権限を持つユーザが使用できます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログイン ホスト（ユーザがログインしたマシン）でのみ使用できます。

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せん。

例

```
mail.example.com> loadlicense
1 Paste via CLI
2 Load from file
How would you like to load a license file?
[1]> 2
Enter the name of the file in /configurations to import:
[]> <filename>
TERMS AND CONDITIONS OF USE
<Terms and conditions>
Do you accept the above license agreement?
```

```
[ ]> y
The license agreement was accepted.
The following feature key have been added:
<feature keys>
```

エラーやハードウェアの設定ミスが表示されることもあります。

showlicense

説明

現在の仮想アプライアンスライセンスに関する情報を表示します。詳細については、[featurekey](#) コマンドを使用すると分かります。

このコマンドは、管理者またはオペレータ権限を持つユーザが使用できます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。さらに、このコマンドはログインホスト（ユーザがログインしたマシン）でのみ使用できます。

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。

バッチ形式

このコマンドの構文：showlicense

例

```
mail.example.com> showlicense
company: Example Inc.
org: Widget Division
unit: Portland Data Center
seats: 1000
city: Portland
state: Oregon
country: US
email: mailadmin@example.com
begin_date: Tue Dec 6 17:45:19 2011
end_date: Mon Sep 1 17:45:19 2014
vln: ABC-123423123
serial: 1003385
```

位置情報

ここでは、次の CLI コマンドについて説明します。

- [geolocationupdate](#) (294 ページ)
- [geolocationstatus](#) (294 ページ)

geolocationupdate

説明

地理位置情報リストを手動で更新します。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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 generalconfig` 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

```
mail3.example.com> geolocationupdate

Requesting update of Geo Countries List.
```

geolocationstatus

説明

地理位置情報リストの現在のバージョンが表示されます。

使用方法

確定：このコマンドに「commit」は必要ありません。

クラスタ管理：このコマンドはマシンモードでのみ使用できます。

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せん。

例

```
mail3.example.com> geolocationstatus

Component          Version      Last Updated
Geo Countries List  1.0.48      26 Feb 2017 04:22 (GMT +00:00)
```