

# 警告メッセージ「Potential Directory Harvest Attack detected」は何を意味しますか。

## 目次

[はじめに](#)

[GUI](#)

[CLI](#)

[関連情報](#)

## 概要

この資料は Cisco E メール セキュリティ アプライアンス (ESA) で受け取られるように「潜在的なディレクトリ収穫不正侵入」エラーメッセージを記述したものです。

## 警告メッセージ「Potential Directory Harvest Attack detected」は何を意味しますか。

ESA のための管理者は次のディレクトリ収穫不正侵入防止 (DHAP) 警告メッセージを受け取りました:

The Warning message is:

```
Potential Directory Harvest Attack detected. See the system mail logs for more information about this attack.
```

```
Version: 8.0.1-023
```

```
Serial Number: XXBAD1112DYY-008X011
```

```
Timestamp: 22 Sep 2014 21:21:32 -0600
```

これらのアラートは情報と考慮され、処置をとる必要があるべきではありません。外部メールサーバは余りにも多くの無効な受信者を試み、DHAP (ディレクトリ収穫不正侵入防止) アラートを引き起こしました。ESA はメール ポリシー 設定に基づいて設定されるように機能しています。

これはリスナーがリモートホストから受け取る 1 時間あたりの無効な受信者の最大数です。このしきい値は SMTP メッセージ交換で廃棄されるか、または作業待ち行列で跳ねられる無効な LDAP 受信者にメッセージの総数によって結合される RATS 拒絶および SMTP コール前方サーバ拒絶の総数を表します (LDAP の設定によって関連するリスナーの設定を受け入れて下さい)。LDAP のための DHAP の設定に関する詳細については「LDAP が」[E メール セキュリティ ユーザガイド](#)の章を問い合わせることをクエリを、見ます受け入れて下さい。

これらのアラートを受け取りたくない場合これらをフィルタ・アウトするために alertconfig とのアラート プロファイルを調節できます:

```
myesa.local> alertconfig
```

```
Sending alerts to:
```

```
robert@domain.com
```

```
Class: All - Severities: All
```

```
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: Enabled
```

```
You will receive a copy of the weekly AutoSupport reports.
```

```
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.

```
[ ]> edit
```

```
Please select the email address to edit.
```

```
1. robert@domain.com (all)
```

```
[ ]> 1
```

```
Choose the Alert Class to modify for "robert@domain.com".
```

```
Press Enter to return to alertconfig.
```

```
1. All - Severities: All
```

```
2. System - Severities: All
```

```
3. Hardware - Severities: All
```

```
4. Updater - Severities: All
```

```
5. Outbreak Filters - Severities: All
```

```
6. Anti-Virus - Severities: All
```

```
7. Anti-Spam - Severities: All
```

```
8. Directory Harvest Attack Prevention - Severities: All
```

または GUI システム 管理から >> 受信者のアドレス警告し、受け取った重大度を修正するかまたは完全に警告 します。

## GUI

GUI からの DHAP コンフィギュレーションパラメータを表示することは、**かデフォルトポリシーパラメータを > 編集し、メール フロー制限/ディレクトリへの変更に必要に応じて不正侵入防止 (DHAP) セクションを収穫させます、メール ポリシー > メール フロー ポリシーによってクリックするために > ポリシー名をクリックします:**

GUI への変更を入れ、保存して下さい。

## CLI

CLI からの DHAP コンフィギュレーションパラメータを表示するために、`listenerconfig > Edit` を (編集するためにリスナーの数を選択する) > DHAP 設定を編集する `hostaccess > デフォルト` 使用して下さい:

```
myesa.local> alertconfig
```

```
Sending alerts to:
```

```
robert@domain.com
```

```
Class: All - Severities: All
```

```
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: Enabled
```

```
You will receive a copy of the weekly AutoSupport reports.
```

```
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.

```
[> edit
```

```
Please select the email address to edit.
```

```
1. robert@domain.com (all)
```

```
[> 1
```

```
Choose the Alert Class to modify for "robert@domain.com".
```

```
Press Enter to return to alertconfig.
```

```
1. All - Severities: All
```

```
2. System - Severities: All
```

```
3. Hardware - Severities: All
```

```
4. Updater - Severities: All
```

```
5. Outbreak Filters - Severities: All
```

```
6. Anti-Virus - Severities: All
```

```
7. Anti-Spam - Severities: All
```

```
8. Directory Harvest Attack Prevention - Severities: All
```

更新を行うか、または変更する場合、主要な CLI プロンプトに戻し、すべての変更を保存して下さい。

## 関連情報

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