Configure Incoming Filter Based on DKIM Verification in ESA

Introduction

This document describes how to configure the Email Security Appliance (ESA) in order to take any action on Domain Keys Identified Email (DKIM) verification through an incoming content filter or message filter configuration.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ESA
- Basic knowledge of content filter configuration
- Basic knowledge of message filters configuration
- Centralizing Policy, Virus, and Outbreak Quarantine configuration knowledge

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Step 1. Configure DKIM Verification

Ensure DKIM verification is enabled. Navigate to **Mail Policies > Mail Flow Policies**.

In order to configure DKIM verification on the ESA is similar to SPF verification. In the **Default Policy Parameters** of Mail Flow Policies, simply turn DKIM Verification to **On**.

Step 2. Verify Final Action

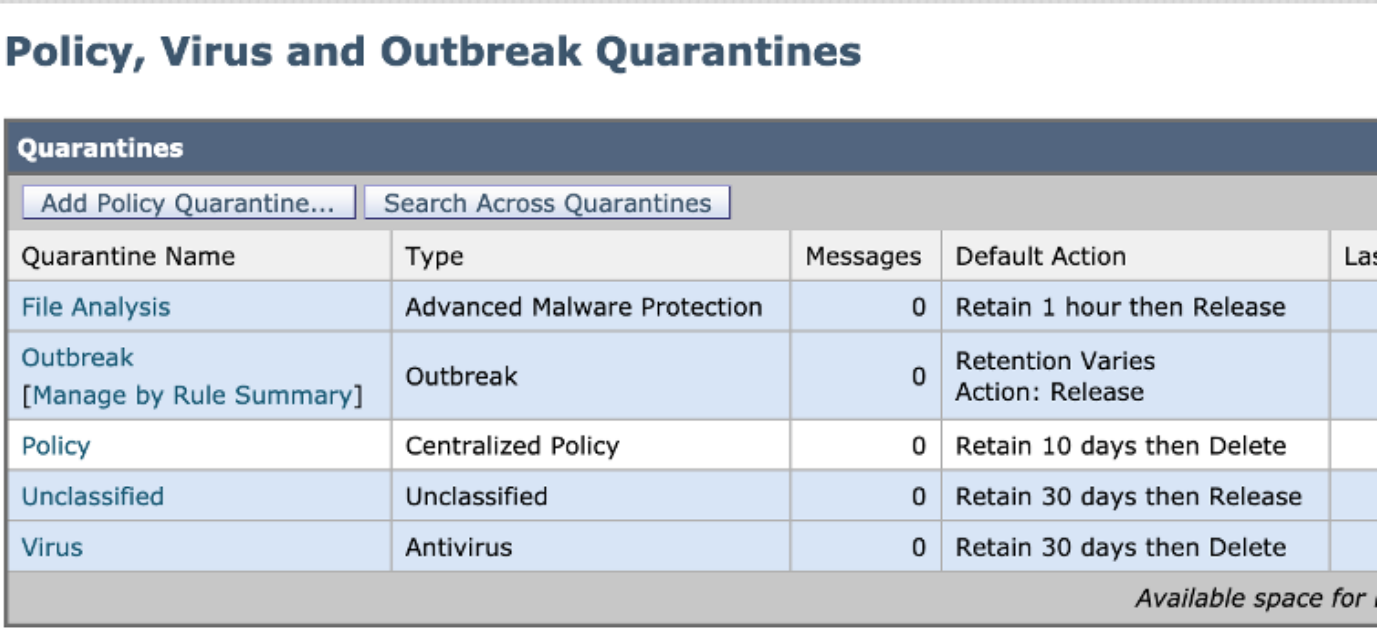
First, identify the action to be taken as per to DKIM verification. Ex: drop, add a tag or quarantine. If the final action is to quarantine the mail, review the configured Quarantines.

- If you do not use centralized management:

Navigate to **ESA >Monitor> Policy, Virus and Outbreak Quarantines**.

- If you have configured centralized management (SMA):

Navigate to **SMA >Email >Message Quarantine >Policy, Virus and Outbreak Quarantines**, as shown in the image:

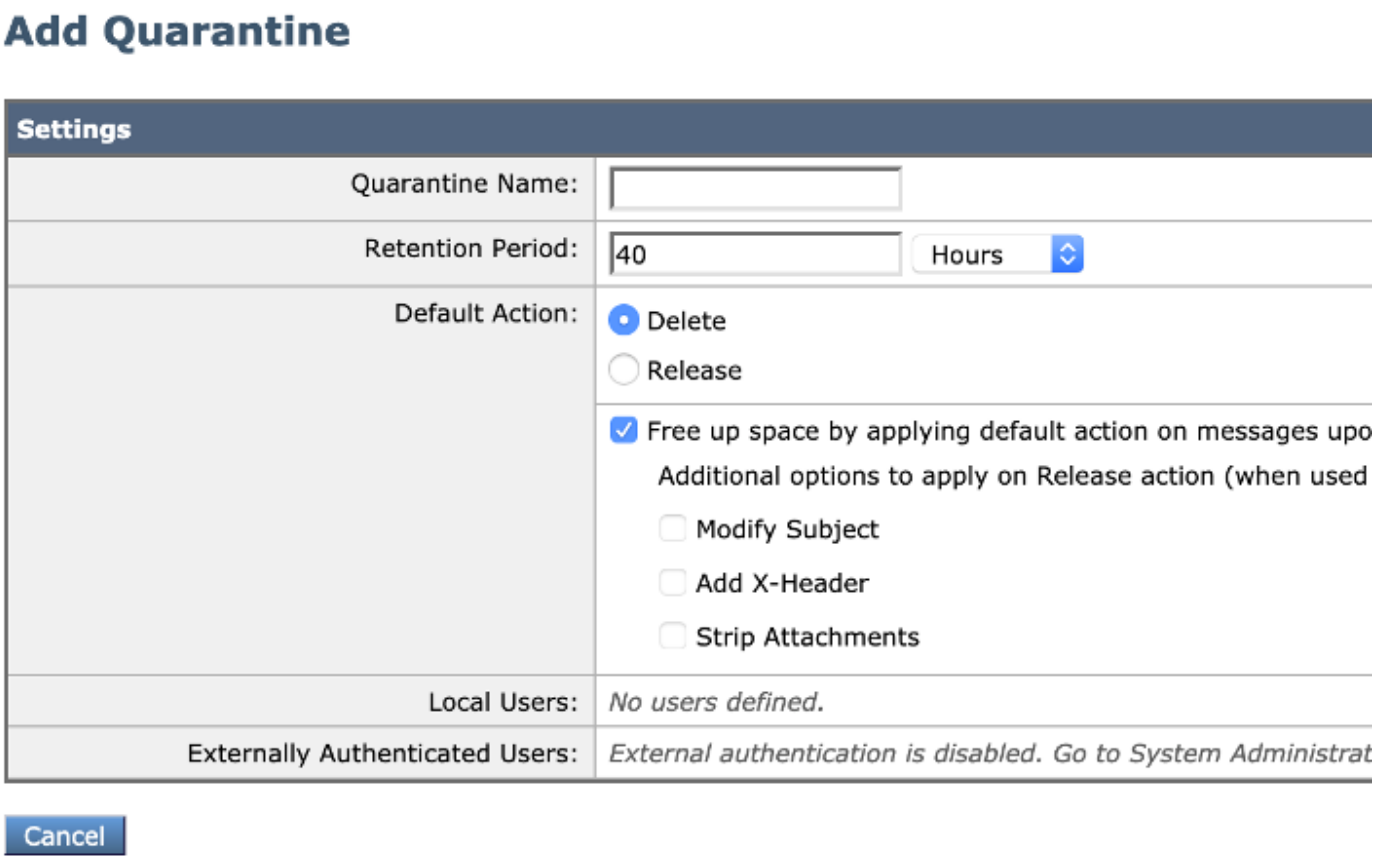


If there are no specific quarantine for **DKIM**/Domain-based Message Authentication, Reporting & Conformance (DMARC)/Sender Policy Framework (SPF) services. It is recommended to create one.

While on Policy, Virus and Outbreak Quarantines, select **Add Policy Quarantine**:

Here, you can set up:

- Quarantine Name: For ex, **DkimQuarantine**
- Retention Period: It is up to you and depends on your organization's needs, and Default action. After retention period to the email will be deleted or release and delivered, determined by your selection, as shown in the image:



Step 3. Incoming Filter for ESA

a. Create an incoming content filter for ESA:

Navigate to **ESA > Mail Policies > Incoming Content Filters > Add Filter**.

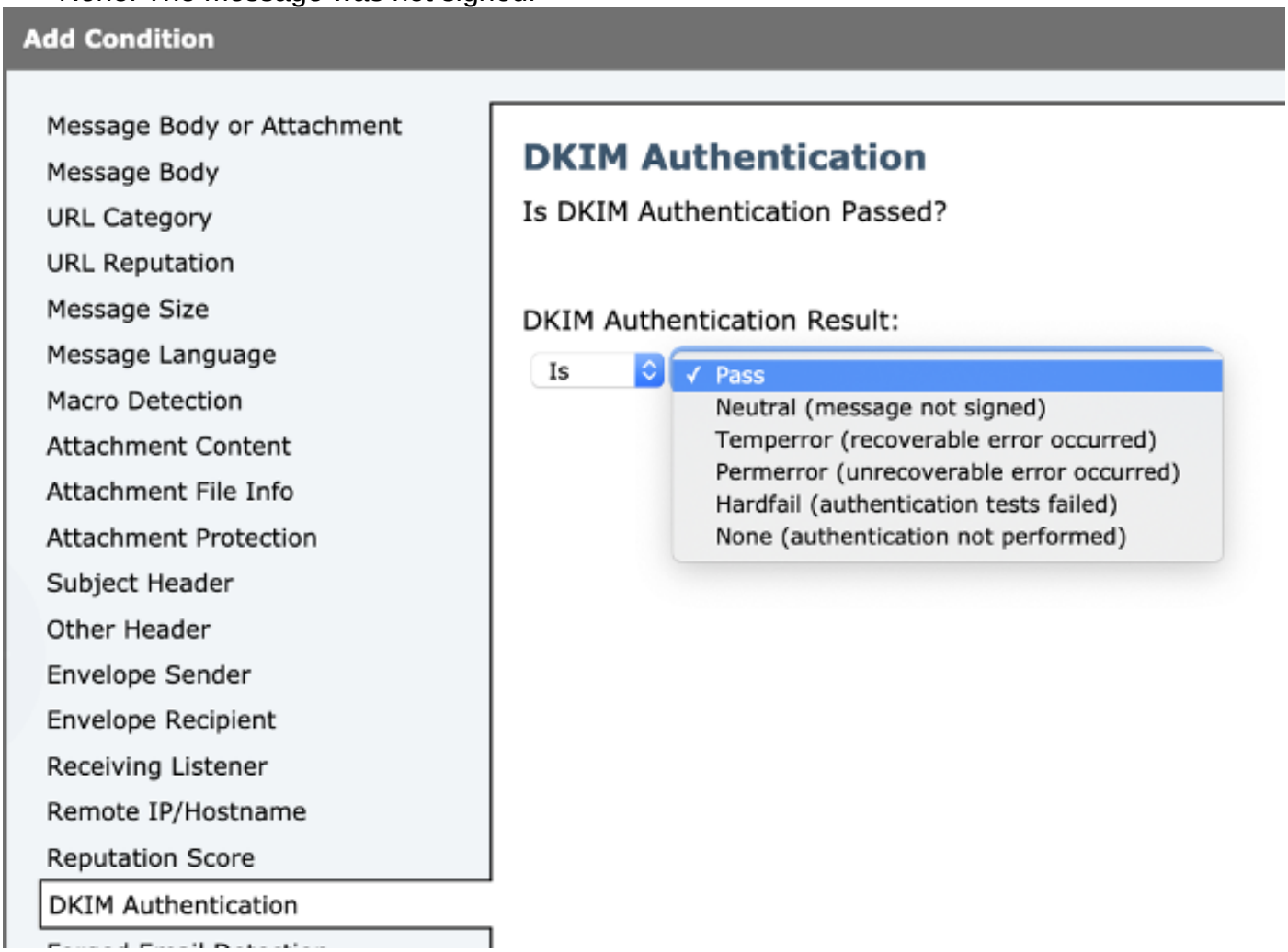
- First section: You can configure the **Name**, **Description**, and **Order** of the filter:

- Second section: Add Condition. You can add, more than one condition and you can configure more content filters in order to take action on DKIM verification:

Authentication-Results expected and meaning:

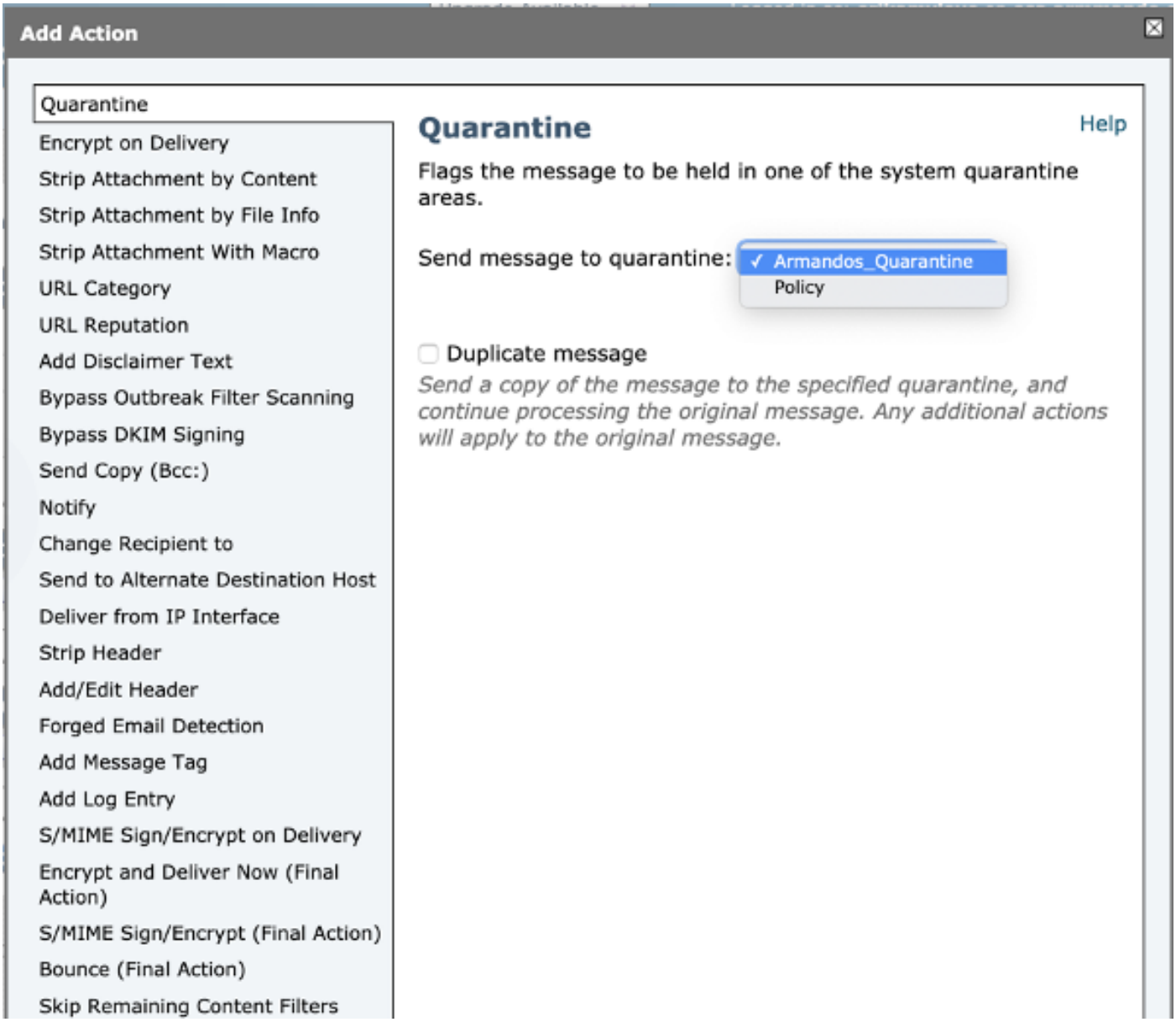
- Pass: The message passed the authentication tests.

- Neutral: Authentication was not performed.
- Temperror: A recoverable error occurred.
- Permerror: An unrecoverable error occurred.
- Hardfail: The authentication tests failed.
- None. The message was not signed.



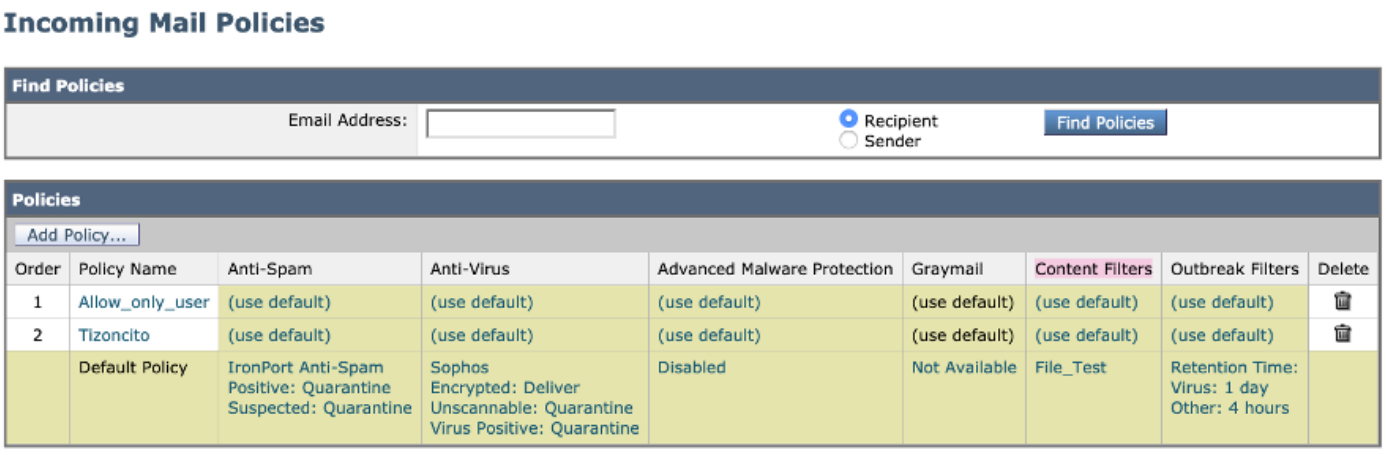
Note: DKIM verification requirements: The sender must sign the message before it can be verified. The sending domain must have a public key available in DNS for verification.

- Third section: Select an action. You can add more than one action like add a log entry, send to quarantine, drop the email, notify, etc. In this case, select the previously configured quarantine, as shown in the image:



Add New Filter to Mail flow policy:

Once a filter has been created. From ESA add the filter on each mail flow policy where you want to verify DKIM with a final action. Navigate to **ESA> Mail Policies >Incoming Mail Policies**, as shown in the image:



Click on the **Content filters** column and **Mail flow policy** row.

> **Note**: (use default) action does not mean that it is configured as Default Policy settings. Configure each mail flow policy with filters needed.

b. Create a message filter for ESA:

All message filter is configured from ESA CLI. Enter the command **Filters** and follow the instructions:

```
ESA. 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.
DKIM_Filter:
If (dkim-authentication == "hardfail" )
{
quarantine("DkimQuarantine");
}
.
1 filters added.
```

Once the filter is created, review the legend: **1 filters added**.

The conditions and actions to configure are the same as those used by the incoming content filter.

Verify

Use this section to confirm that your configuration works properly.

Incoming content filter:

- From ESA Web User Interface (WebUI)

a. Check if the filter is configured:

Navigate to **ESA >Mail Policies >Incoming Content Filters.** The filter must be configured according to the order previously selected in the displayed list.

b. Check if the filter is applied:

Navigate to **ESA>Mail Policies >Incoming mail policies**.

The name of the filter must be shown in the Content filters column and Mail flow policy row. If the list is wide and you can't see the name, click on the filter list in order to identify the filters applied to the policy.

Message Filter:

```
From ESA CLI:
ESA. com> filters
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

Num Active Valid Name

  1           Y      Y     DKIM_Filter
```

The list shows if the filter is configured and active.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Verify configuration:

You must ensure that:

- The mail flow policy has dkim: on verification
- There is an action configured in a content filter or message filter
- In the case of a content filter, validate that the filter is associated with a mail flow

Verify message tracking:

Message tracking allows us to observe:

- The result of the DKIM verification, ex: permfail
- The configured log entry (if one was configured)
- The filter applied (name and action taken)

Tracking from ESA:

```
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 From: <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 ICID 98 RID 0 To: <userb@domainb.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 Message-ID '<3903af$2r@mgt.esa.domain.com>Fri Apr 26
11:33:44 2019 Info: MID 86 DKIM: permfail body hash did not verify [final]
Fri Apr 26 11:33:44 2019 Info: MID 86 Subject "Let's go to camp!"
Fri Apr 26 11:33:44 2019 Info: MID 86 ready 491 bytes from <user@domain.com>
Fri Apr 26 11:33:44 2019 Info: MID 86 matched all recipients for per-recipient policy
Allow_only_user in the inbound table
Fri Apr 26 11:33:46 2019 Info: MID 86 interim verdict using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: CASE spam negative
Fri Apr 26 11:33:46 2019 Info: MID 86 interim AV verdict using Sophos CLEAN
Fri Apr 26 11:33:46 2019 Info: MID 86 antivirus negative
Fri Apr 26 11:33:46 2019 Info: MID 86 AMP file reputation verdict : UNSCANNABLE
Fri Apr 26 11:33:46 2019 Info: MID 86 using engine: GRAYMAIL negative
Fri Apr 26 11:33:46 2019 Info: MID 86 Custom Log Entry: The content that was found was:
DkimFilter
Fri Apr 26 11:33:46 2019 Info: MID 86 Outbreak Filters: verdict negative
Fri Apr 26 11:33:46 2019 Info: MID 86 quarantined to "DkimQuarantine" by add-footer filter
'DkimFilter '
```

```
Fri Apr 26 11:33:46 2019 Info: Message finished MID 86 done
```

Related Information

- **Best Practices ESA-SPF-DKIM-DMARC**
- **Email Security Appliance End User Guide**
- **DKIM RFC4871**
- **DKIM RFC8301**
- **DKIM RFC8463**
- **Technical Support & Documentation - Cisco Systems**