# How to DKIM Sign Emails Sent on Behalf of Other Domains

## Contents



## Introduction

This document describes how to sign emails with DomainKeys Identified Mail (DKIM) on the Email Security Appliance (ESA) and Cloud Email Security (CES) when they are sent on behalf of other domains.

## Background Information

From RFC2822

“The originator fields indicate the mailbox(es) of the source of the message. The "From:" field specifies the author(s) of the message, that is, the mailbox(es) of the person(s) or system(s) responsible for the writing of the message. The "Sender:" field specifies the mailbox of the agent responsible for the actual transmission of the message. For example, if a secretary were to send a message for another person, the mailbox of the secretary would appear in the "Sender:" field and the mailbox of the actual author would appear in the "From:" field. If the originator of the message can be indicated by a single mailbox and the author and transmitter are identical, the "Sender:" field SHOULD NOT be used. Otherwise, both fields SHOULD appear.”

From End-User Guide 14.0

“As messages are received on a listener used to send messages (outbound), the email gateway checks to see if any domain profiles exist. If there are domain profiles created on the email gateway (and implemented for the mail flow policy), the message is scanned for a valid Sender: or From: address. If both are present, the Sender: header is always used for Domain Keys and DKIM Signing, but the From: header is also required even though it is not used for DKIM signing. When only the Sender: header is present, the DomainKeys or DKIM Signing profiles are not matched. The From: header is only used when:

- There is no Sender: header.
- You select the Use From Header for DKIM Signing option in the DKIM Global Setting page in the web interface.”

# Prerequisites

## Requirements

There are no specific requirements for this document.

## Components Used

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

1. Configure DKIM Signing
2. Navigate to **Mail Policies** > **Signing Profiles** > **DKIM Global Settings** > **Use From Header for DKIM Signing: Off**

   **Note**: If **Use From Header for DKIM Signing** is set to **On** the ESA always looks at the **From** header field and messages sent on behalf of other domains are not DKIM signed since the **Sender** header is populated with the **Envelope From** value hence the messages do not match with the domain established in the **DKIM Profile**.

# Verify

1. Initiate an SMPT conversation

```
ESA-C690-K9.MX> telnet 15.0.0.59 25
Trying 15.0.0.59...
Connected to 15.0.0.59.
Escape character is '^]'.
220 mail.mxesa.com ESMTP
hello
250 mail.mxesa.com
MAIL FROM: amacorra@mxesa.com
250 sender <amacorra@mxesa.com> ok
RCPT TO: amacorra@cloudesa.com
250 recipient <amacorra@cloudesa.com> ok
data
354 go ahead
From: amacorra@cloudesa.com
To: amacorra@cloudesa.com
Sender: amacorra@mxesa.com
Subject: Adding Sender Header Manually

Adding Sender Header Manually.
.
250 ok:  Message 640880 accepted
```

2. Verify the logs

**DKIM: pass signature verified (d= mxesa.com s=selector i=@ mxesa.com)**

3. Verify the headers

**dkim=pass (signature verified) header.i=@mxesa.com**

In your inbox, you receive the email with the next line:

**amacorra@mxesa.com <amacorra@ mxesa.com>; on behalf of; amacorra@cloudesa.com <amacorra@cloudesa.com>**

# Related Information

- RFC2822
- End-User Guide 14.0
- Configure DKIM Signing