

# Quali condizioni determinano quali risultati di autenticazione per DKIM?

## Sommario

[Introduzione](#)

[Risultati](#)

[Informazioni correlate](#)

## Introduzione

In questo documento vengono descritte le condizioni che producono determinati risultati di autenticazione per DKIM.

## Risultati

DomainKeys Identified Mail (DKIM) è un sistema di convalida della posta elettronica progettato per rilevare lo spoofing della posta elettronica fornendo un meccanismo che consente agli scambiatori di posta di ricevere controllare che la posta in arrivo da un dominio sia autorizzata dagli amministratori di quel dominio.

Cisco Email Security Appliance (ESA) può produrre i seguenti risultati con la firma DKIM e la verifica ON/OFF:

Firma DKIM (Fine invio)	Verifica DKIM (Fine ricezione)	Risultato
ON	ON	Pass/Permerror/Temperror/Hardfail
ON	OFF	Nessuna
OFF	OFF	Nessuna
OFF	ON	Neutro

- Superato. Il messaggio ha superato i test di autenticazione.
- Neutro. Autenticazione non eseguita.
- Temperror. Si è verificato un errore reversibile.
- Permerror. Errore irreversibile.
- Hardfail. Test di autenticazione non riusciti.
- Nessuna. Il messaggio non è stato firmato.

Se la verifica di DKIM è disattivata in Mail Flow Policies all'estremità di ricezione, il risultato DKIM non verrà visualizzato nei log di posta. Tuttavia, il risultato di "none" (nessuno) può essere trovato nei filtri dei contenuti.

## Informazioni correlate

- [Guida per l'utente di AsyncOS Email](#)
- [Informazioni di contatto del supporto GLO](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)