

ESA上的例外表如何工作？

目錄

[簡介](#)

[ESA上的例外表如何工作？](#)

[允許操作](#)

[拒絕操作](#)

簡介

本檔案介紹電子郵件安全裝置(ESA)上的例外表如何運作。

ESA上的例外表如何工作？

例外表列出帶有兩種不同行為型別的電子郵件地址（完整或部分地址）：允許或拒絕。在郵件流策略中，需要選中「使用發件人驗證例外表」選項，否則將不會匹配例外表條目。

允許操作

允許異常表中的清單繞過發件人DNS驗證。如果信封發件人的域或電子郵件地址列在「例外表」中，則允許發件人繼續將郵件傳送到ESA，無論是否可以解析信封發件人電子郵件地址的域名。**如果啟用了發件人DNS驗證，並且無法解析域(例如，允許來自內部域或測試域的郵件，即使這些郵件不會以其他方式進行驗證)，這非常有用。**

如果為正在使用的郵件流策略啟用了發件人DNS驗證，並且無法解析信封發件人的域名（該域名不存在、無法解析或格式不正確），則郵件將被拒絕。以下是SMTP響應的示例：

```
SMTP code: 553
```

```
Message: #5.1.8 Domain of sender address <$EnvelopeSender> does not exist
```

如果信封發件人的電子郵件地址或域在「例外表」中列出，並且允許行為，則發件人可以繼續處理郵件的剩餘部分（RCPT TO、DATA等），並且會正常處理郵件：郵件過濾器、反垃圾郵件掃描等）。這樣允許郵件進入裝置，儘管發件人的域名不可驗證。例如，在下列情況下，發件人將被拒絕：

以下是已拒絕傳送者的記錄中的專案：

```
553 #5.1.8 Domain of sender address <user@example.com> does not exist
```

如果新增了@example.com的「允許」清單，則允許該發件人，並且此條目將顯示在日誌中：

```
mail from:<user@example.com>
```

```
250 sender <user@example.com> ok
```

拒絕操作

如果信封發件人與「例外表」中的「拒絕」清單相匹配，則郵件將被拒絕。預設情況下，SMTP響應為：

```
SMTP code: 553
```

```
Message: Envelope sender <${EnvelopeSender}> rejected
```

如果您有一個清單(例如user@example.com)，其中包含「Reject」（拒絕）行為，則當信封發件人為「user@example.com」時傳送的任何郵件都會被拒絕：

```
mail from:<user@example.com>
```

```
553 Envelope sender <user@example.com> rejected
```