



## **Email Authentication**

# Contents

<b>Über Email Authentication.....</b>	<b>3</b>
<b>DNS-Einstellungen eigener Domains prüfen.....</b>	<b>4</b>
<b>Verfahren zur Absender-Authentifizierung.....</b>	<b>6</b>
SPF-Prüfung.....	6
Logik der SPF-Prüfung.....	7
SPF-Eintrag setzen.....	9
SPF-Prüfung aktivieren.....	10
Erweiterte Optionen zur SPF-Prüfung konfigurieren.....	14
Fehlerbehebung.....	17
DKIM-Validierung und DKIM-Signierung.....	19
CNAME-Eintrag setzen.....	19
DKIM-Validierung aktivieren.....	20
Erweiterte Optionen zur DKIM-Validierung konfigurieren.....	21
DKIM-Signierung aktivieren.....	24
DMARC-Validierung.....	25
DMARC-Eintrag setzen.....	25
DMARC-Entscheidungsmatrix.....	29
DMARC-Validierung aktivieren.....	35
Erweiterte Optionen zur DMARC-Validierung konfigurieren.....	36
Ausnahmen hinzufügen.....	40
Kategorisierungsgründe von Email Authentication.....	41
<b>Index.....</b>	<b>43</b>

## Über Email Authentication

Email Authentication bietet Administratoren auf Kundenebene unterschiedliche Möglichkeiten zur Authentifizierung von E-Mail-Absendern (siehe [Verfahren zur Absender-Authentifizierung](#) auf Seite 6). Die folgenden Verfahren sind verfügbar:

- SPF-Validierung (Sender Policy Framework) (siehe [SPF-Prüfung](#) auf Seite 6)
- DKIM-Validierung und DKIM-Signierung (DomainKeys Identified Mail) (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19)
- DMARC-Validierung (Domain-based Message Authentication, Reporting and Conformance) (siehe [DMARC-Validierung](#) auf Seite 25)

Email Authentication kann nur verwendet werden, falls Spam and Malware Protection aktiviert ist (siehe 'Spam and Malware Protection aktivieren' im Control-Panel-Handbuch). Bevor Administratoren auf Kundenebene die Verfahren zur Absender-Authentifizierung aktivieren, müssen sie die DNS-Einstellungen ihrer eigenen Domains prüfen (siehe [DNS-Einstellungen eigener Domains prüfen](#) auf Seite 4).

## DNS-Einstellungen eigener Domains prüfen



Sie haben Spam and Malware Protection aktiviert (siehe 'Spam and Malware Protection aktivieren' im Control-Panel-Handbuch).



### Hinweis:

Sie können die DNS-Einstellungen nur für die Domains prüfen, für die Spam and Malware Protection aktiviert ist.

Bevor Sie Verfahren für die Absender-Authentifizierung einstellen, müssen Sie prüfen, ob die DNS-Einstellungen Ihrer Domains korrekt konfiguriert sind. Dabei wird der Status der SPF-, DKIM- und DMARC-Einstellungen Ihrer Domains geprüft.



### WICHTIG:

Sie können die SPF-Prüfung (siehe [SPF-Prüfung](#) auf Seite 6), die DKIM-Validierung (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19) und die DMARC-Validierung (siehe [DMARC-Validierung](#) auf Seite 25) nur für Ihre Domains aktivieren, für die die zugehörigen DNS-Einstellungen korrekt konfiguriert sind.



### Hinweis:

Wie Sie einen SPF-Eintrag setzen, erfahren Sie unter [SPF-Eintrag setzen](#) auf Seite 9.

Wie Sie einen CNAME-Eintrag setzen, erfahren Sie unter [CNAME-Eintrag setzen](#) auf Seite 19.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen > Email Authentication**.

4. Klicken Sie auf **DNS-Einstellungen aktualisieren**, um den Status der DNS-Einstellungen Ihrer Domains zu prüfen.

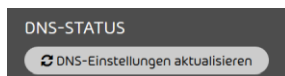


Abbildung 1: DNS-Einstellungen aktualisieren

- ➔ Sie erhalten eine tabellarische Übersicht über den Status der DNS-Einstellungen Ihrer Domains. Die folgenden drei Ergebnisse sind möglich:



Die Einstellungen der Domain sind korrekt konfiguriert.



Für die Domain sind keine Einträge gesetzt.



Die Einstellungen der Domain sind nicht korrekt konfiguriert.



Die DNS-Einstellungen Ihrer Domains sind geprüft worden.

Anschließend können Sie Verfahren zur Absender-Authentifizierung aktivieren (siehe [Verfahren zur Absender-Authentifizierung](#) auf Seite 6).

## Verfahren zur Absender-Authentifizierung

Administratoren auf Kundenebene können verschiedene Verfahren zur Authentifizierung von E-Mail-Absendern für ihre Domains aktivieren. Die folgenden Verfahren stehen zur Verfügung:

- [SPF-Prüfung](#) auf Seite 6
- [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19
- [DMARC-Validierung](#) auf Seite 25

Diese Verfahren erhöhen den Schutz der E-Mail-Infrastruktur von Unternehmen vor Spam und Phishing. Administratoren auf Kundenebene können die Verfahren einzeln verwenden oder miteinander kombinieren.

Eine Kombination mehrerer Verfahren bietet den größten Schutz. Beispielsweise kann bei Servern, die nur DKIM verwenden, über eine E-Mail mit gültiger DKIM-Signatur Spam verbreitet werden. Solange diese E-Mail nicht verändert wird, kann sie mit einer gültigen DKIM-Signatur massenhaft an unterschiedliche Personen versandt werden. Um dies zu verhindern, kann zusätzlich SPF eingesetzt werden. SPF überprüft die Herkunft der E-Mail. Dabei werden die IPv4-Adresse und der Domain-Name des Mail-Servers geprüft. SPF lehnt E-Mails von nicht autorisierten Servern ab. So wird verhindert, dass Spam über E-Mails mit einer gültigen DKIM-Signatur versandt wird.

Administratoren auf Kundenebene können außerdem für einzelne ihrer Domains Ausnahmen von den Verfahren definieren (siehe [Ausnahmen hinzufügen](#) auf Seite 40).

E-Mails, bei denen die Absender-Authentifizierung einen Fehler ergeben hat, werden abgelehnt oder als Spam markiert. Für E-Mails, bei denen die SPF-Prüfung, die DKIM-Validierung oder die DMARC-Validierung fehlgeschlagen ist, werden im Control Panel bestimmte Kategorisierungsgründe angegeben (siehe [Kategorisierungsgründe von Email Authentication](#) auf Seite 41).

### SPF-Prüfung

SPF (Sender Policy Framework) ist ein Verfahren zur Absender-Authentifizierung, das prüft, ob die Absenderadresse einer E-Mail gefälscht ist. Bei einer SPF-Prüfung prüft der Eingangsserver, ob eine eingehende E-Mail von einem autorisierten Server stammt. Dazu prüft der Eingangsserver, ob die IP-Adresse des Ausgangsservers in einem SPF-Eintrag in der DNS-Zone der Absender-Domain

eingetragen ist. In einem SPF-Eintrag sind die IP-Adressen der Server eingetragen, die zum Versand von E-Mails einer Domain autorisiert sind. Für weitere Informationen zur Logik der SPF-Prüfung siehe [Logik der SPF-Prüfung](#) auf Seite 7.

Administratoren auf Kundenebene können die SPF-Prüfung für eingehende E-Mails ihrer Domains einrichten. Hierzu müssen die Administratoren zunächst SPF-Einträge für all ihre Domains setzen (siehe [SPF-Eintrag setzen](#) auf Seite 9), auf deren eingehende E-Mails sie SPF-Prüfungen anwenden möchten. Anschließend müssen die Administratoren die SPF-Prüfung aktivieren (siehe [SPF-Prüfung aktivieren](#) auf Seite 10) und die erweiterten Optionen konfigurieren (siehe [Erweiterte Optionen zur SPF-Prüfung konfigurieren](#) auf Seite 14).

Im Kapitel [Fehlerbehebung](#) auf Seite 17 wird erklärt, wie Fehler bei SPF-Prüfungen behoben werden können.

## Logik der SPF-Prüfung

Die Logik von SPF-Prüfungen wird im Folgenden beschrieben.

Beim Eingang einer E-Mail auf einem Empfängerserver wird die IP-Adresse des sendenden Servers mit den Einträgen aus dem TXT-Eintrag der Domain der E-Mail-Adresse des Absenders verglichen. Falls die IP-Adresse des sendenden Servers nicht im TXT-Eintrag enthalten ist, wird ein Fehler ausgegeben. Bei der Prüfung des TXT-Eintrags wird nach Schwere zwischen Hard- und Softfails unterschieden.

Administratoren auf Kundenebene können entscheiden, welche Maßnahmen bei welcher Art von Fehler angewendet werden sollen (siehe [SPF-Prüfung aktivieren](#) auf Seite 10). Falls keine Fehler auftreten, wird die E-Mail wie gewohnt zugestellt.

### Hinweis:

Die folgenden Ausführungen basieren auf der Annahme, dass sowohl die Absenderangaben aus dem Envelope (MAIL FROM) als auch die Absenderangaben aus dem Header (From) geprüft werden sollen. Falls nur eine dieser Angaben geprüft werden soll, findet eine einzige Prüfung statt und der Failtyp dieser Prüfung ist ausschlaggebend.

Folgende Logik wird beim Überprüfen des TXT-Eintrags berücksichtigt:

1. Im ersten Schritt werden gleichzeitig die Domains geprüft, die im Envelope (MAIL FROM) und im Header (From) angegeben sind. Falls eine der Prüfungen einen Fehler liefert, wird die Art dieses Fehlers beim nächsten Schritt berücksichtigt. Falls beide Prüfungen Fehler liefern, wird für den nächsten Schritt die Art des schwersten Fehlers berücksichtigt. Es gibt drei Möglichkeiten.

**Tabelle 1: Möglichkeit 1 - Beide SPF-Prüfungen liefern Softfails**

Falls die SPF-Prüfungen für Envelope und Header beide Softfails liefern, wird im nächsten Schritt ein Softfail berücksichtigt.

TEIL DER E-MAIL	KONFIGURATION	FAILTYP
Envelope (MAIL FROM)	~all	Softfail
Header (From)	~all	Softfail

**Tabelle 2: Möglichkeit 2 - Beide SPF-Prüfungen liefern Hardfails**

Falls die SPF-Prüfungen für Envelope und Header beide Hardfails liefern, wird im nächsten Schritt ein Hardfail berücksichtigt.

TEIL DER E-MAIL	KONFIGURATION	FAILTYP
Envelope (MAIL FROM)	-all	Hardfail
Header (From)	-all	Hardfail

**Tabelle 3: Möglichkeit 3 - Die SPF-Prüfungen liefern verschiedene Fehler**

Falls die SPF-Prüfungen für Envelope und Header verschiedene Fehler liefern, wird im nächsten Schritt ein Hardfail berücksichtigt.



TEIL DER E-MAIL	KONFIGURATION	FAILTYP
Envelope (MAIL FROM)	-all	Hardfail
Header (From)	~all	Softfail

- Im zweiten Schritt wird überprüft, welche Maßnahmen Sie für einen Hardfail oder Softfail eingestellt haben. Diese Maßnahme wird angewendet.

**i Hinweis:**

Im Rahmen der SPF-Prüfung werden nur die Qualifikatoren - und ~ unterstützt. Der Qualifikator - steht für den Ergebniscode Hardfail und der Qualifikator ~ für den Ergebniscode Softfail. Der Qualifikator ? wird nicht unterstützt.

## SPF-Eintrag setzen

Sie können einen SPF-Eintrag in der DNS-Zone Ihrer Domain setzen, um unsere Server zum Versand von E-Mails im Namen Ihrer Domain zu autorisieren. Spam and Malware Protection (siehe 'Spam and Malware Protection' im Control-Panel-Handbuch) kann anhand des SPF-Eintrags Täuschungsversuche wie Spoofing rechtzeitig erkennen. Empfänger außerhalb Ihrer Organisation können den SPF-Eintrag verwenden, um SPF-Prüfungen für E-Mails von Ihrer Domain durchzuführen. Außerdem benötigen Sie den SPF-Eintrag, damit Email Authentication SPF-Prüfungen (siehe 'SPF-Prüfung' im Control-Panel-Handbuch) für eingehende E-Mails durchführen kann.

**! WICHTIG:**

Hinterlegen Sie in dem SPF-Eintrag alle Server, die E-Mails von Ihrer Domain versenden dürfen.

 **Hinweis:**

Unser SPF-Eintrag ist nicht erforderlich für Kunden, die ihre primäre Umgebung mit der Option **IP/Hostname** eingestellt haben, jedoch keine Adressen von Relay-Servern für ausgehende E-Mails hinterlegt haben. Für weitere Informationen zur Einstellung der primären Umgebung siehe .

Sie müssen den SPF-Eintrag in der DNS-Zone Ihrer Domain selbst setzen. Um weitere Informationen zu erhalten, wie Sie den SPF-Eintrag in der DNS-Zone korrekt setzen, kontaktieren Sie bitte den Support.

## SPF-Prüfung aktivieren



Sie haben gültige SPF-Einträge in der DNS-Zone Ihrer Domains gesetzt (siehe [SPF-Eintrag setzen](#) auf Seite 9). Sie haben Spam and Malware Protection für Ihre Domain aktiviert (siehe 'Spam and Malware Protection aktivieren' im Control-Panel-Handbuch).

 **WICHTIG:**

SPF-Prüfungen werden nur für Domains mit gültigen SPF-Einträgen durchgeführt.

**!** WICHTIG:

Die SPF-Prüfung kann nur aktiviert werden, falls der Kunde eine der folgenden Bedingungen erfüllt:

- Der Kunde hat seine primäre Umgebung mit der Option **IP/Hostname** eingestellt und Adressen von Relay-Servern für ausgehende E-Mails hinterlegt. Der Kunde hat zusätzlich zu seinen eigenen SPF-Einträgen unseren SPF-Eintrag in der DNS-Zone gesetzt (siehe [SPF-Eintrag setzen](#) auf Seite 9).
- Der Kunde hat seine primäre Umgebung mit der Option **IP/Hostname** eingestellt, jedoch keine Adressen von Relay-Servern für ausgehende E-Mails hinterlegt. Der Kunde hat seine eigenen SPF-Einträge in der DNS-Zone gesetzt.

Für weitere Informationen zur Einstellung der primären Umgebung siehe das Kapitel 'Primäre Umgebungseinstellungen vornehmen' im Control-Panel-Handbuch.

Sie können die SPF-Prüfung aktivieren, um zu prüfen, ob die IP-Adresse des Ausgangsservers einer eingehenden E-Mail in den SPF-Einträgen der Domain des Absenders eingetragen und autorisiert ist, E-Mails von der Domain zu verschicken.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen > Email Authentication**.
4. Setzen Sie unter **Absender-Authentifizierung** ein Häkchen in der Checkbox **SPF-Prüfung aktivieren**.

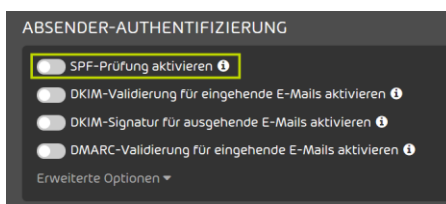
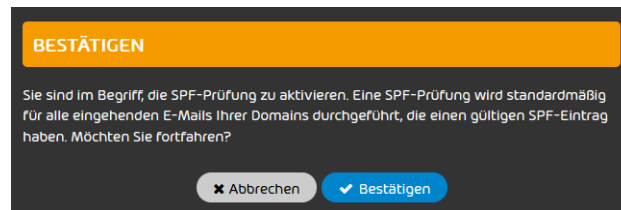


Abbildung 2: SPF-Prüfung aktivieren

- ➔ Eine Warnmeldung wird angezeigt.

5. Klicken Sie auf **Bestätigen**.



**Abbildung 3: Bestätigen**

- ➔ Die SPF-Prüfung wird für alle Domains aktiviert, die unter der ausgewählten Domain liegen und für die korrekte SPF-Einträge gesetzt sind.

6. Wählen Sie aus, in welchen Fällen eine SPF-Prüfung durchgeführt werden soll.
- Falls alle eingehenden E-Mails geprüft werden sollen, für deren Absender-Domain ein SPF-Eintrag gesetzt ist, wählen Sie **Für alle eingehenden E-Mails**



### Hinweis:

Diese Variante wird empfohlen, falls allgemein ein hohes Aufkommen von Adressfälschungen von unterschiedlichen Absenderdomains vorliegt. Die Nutzung dieser Variante kann dazu führen, dass die False-Positive-Rate erhöht wird, falls Kommunikationspartner ihre SPF-Einträge nicht richtig gesetzt haben.

- Falls nur eingehende E-Mails geprüft werden sollen, die von der Domain oder einer Aliasdomain des Empfängers verschickt worden sind, wählen Sie **Nur für E-Mails innerhalb einer Ihrer eigenen Domains**.



### Hinweis:

Es werden nur interne E-Mails geprüft. Diese Variante wird empfohlen, um gezielte Angriffe unter einer gefälschten E-Mail-Adresse der eigenen Domain zu unterbinden.

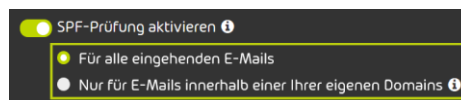


Abbildung 4: E-Mails für SPF-Prüfung wählen

- ➔ Die SPF-Prüfung wird aktiviert.



### Hinweis:

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.



- Die SPF-Prüfung ist aktiviert worden.

Anschließend können Sie die erweiterten Optionen für die SPF-Prüfung konfigurieren (siehe [Erweiterte Optionen zur SPF-Prüfung konfigurieren](#) auf Seite 14).

## Erweiterte Optionen zur SPF-Prüfung konfigurieren

 Sie haben die SPF-Prüfung aktiviert (siehe [SPF-Prüfung aktivieren](#) auf Seite 10).

Im Modul **Sicherheitseinstellungen** > **Email Authentication** können Sie konfigurieren, wie mit den Ergebnissen von SPF-Prüfungen (siehe [SPF-Prüfung](#) auf Seite 6) umgegangen werden soll.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Email Authentication**.
4. Klicken Sie auf **Erweiterte Optionen**

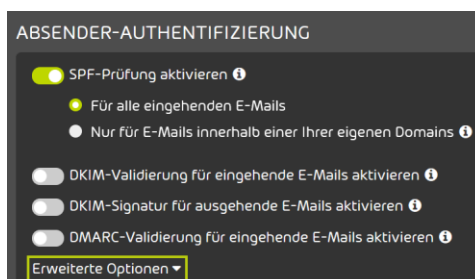


Abbildung 5: Erweiterte Optionen öffnen

-  Eine Warnmeldung wird angezeigt.

5.



### WICHTIG:

Änderungen an den erweiterten Optionen können dazu führen, dass schädliche E-Mails zugestellt werden.

Um die erweiterten Optionen zu ändern, klicken Sie auf **Bestätigen**.

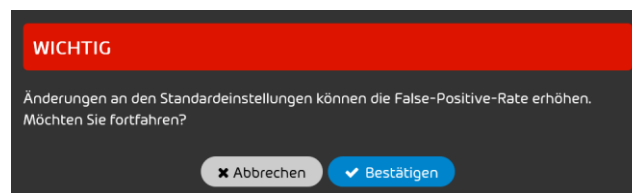


Abbildung 6: Bestätigen

6. Optional: Legen Sie unter **Verhalten nach einem SPF-Hardfail** fest, was nach einem SPF-Hardfail passieren soll. Sie haben die folgenden Optionen:
- **E-Mail als Spam in Quarantäne speichern:** Die E-Mail wird als Spam markiert und in der Quarantäne gespeichert.
  - **E-Mail ablehnen:** Die E-Mail wird abgelehnt. Die E-Mail wird nicht an den Empfänger zugestellt und auch nicht in der Quarantäne gespeichert.
  - **Keine Aktion durchführen:** Der SPF-Hardfail löst keine Aktion aus. Die E-Mail wird anschließend durch weitere Filter unserer Services geprüft.

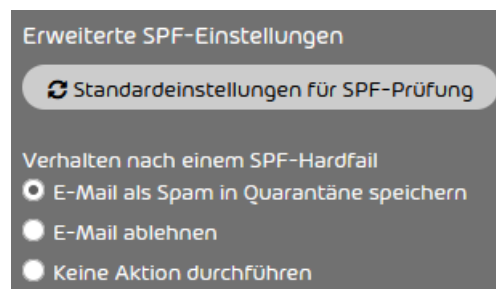


Abbildung 7: Verhalten nach einem SPF-Hardfail auswählen

7. Optional: Legen Sie unter **Verhalten nach einem SPF-Softfail** fest, was nach einem SPF-Softfail passieren soll. Sie haben drei Optionen:
- **E-Mail als Spam in Quarantäne speichern:** Die E-Mail wird als Spam markiert und in der Quarantäne gespeichert.
  - **E-Mail ablehnen:** Die E-Mail wird abgelehnt. Die E-Mail wird nicht an den Empfänger zugestellt und auch nicht in der Quarantäne gespeichert.
  - **Keine Aktion durchführen:** Der SPF-Softfail löst keine Aktion aus. Die E-Mail wird anschließend durch weitere Filter unserer Services geprüft.

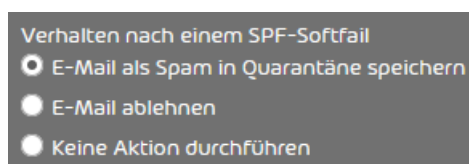


Abbildung 8: Verhalten nach einem SPF-Softfail auswählen

8. Optional: Legen Sie unter **Analyse** fest, welche Bestandteile der E-Mails analysiert werden sollen. Sie haben die folgenden Optionen:
- Nur 'envelope from' analysieren
  - Nur 'header from' analysieren
  - 'envelope from' und 'header from' analysieren



**Hinweis:**

Falls beide Angaben geprüft werden, erhöht das die Sicherheit, aber auch die False-Positive-Rate.

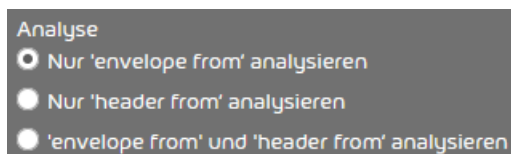


Abbildung 9: Analyse konfigurieren



9. Optional: Um die SPF-Einstellungen auf die Standardeinstellungen zurückzusetzen, klicken Sie auf **Standardeinstellungen für SPF-Prüfung**

**Hinweis:**

Bei den Standardeinstellungen werden E-Mails nach einem SPF-Hardfail und einem SPF-Softfail als Spam in der Quarantäne gespeichert und nur der Envelope-From analysiert.



Die Änderungen werden gespeichert.

**Hinweis:**

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.



Die erweiterten Optionen zur SPF-Prüfung sind konfiguriert worden.

## Fehlerbehebung

Die folgenden Fehler bei SPF-Prüfungen können behoben werden:

- Fehler aufgrund von SPF-Prüfungen beim Versenden von E-Mails (siehe [Fehlerbehebung: Probleme beim Versenden von E-Mails bei eingerichtetem SPF-Eintrag](#) auf Seite 17)
- Fehler aufgrund von SPF-Prüfungen beim Empfangen von E-Mails (siehe [Fehlerbehebung: Probleme beim Empfangen von E-Mails mit SPF-Prüfungen](#) auf Seite 18)

## Fehlerbehebung: Probleme beim Versenden von E-Mails bei eingerichtetem SPF-Eintrag

### Bedingung:

Eine der folgenden Bedingungen ist erfüllt:

- SPF-Prüfungen werden bei Ihnen nur dann durchgeführt, wenn die Absender-Domain mit der Empfänger-Domain übereinstimmt. Eingehende interne E-Mails werden fälschlicherweise als ungültig erkannt.
- Ihr Kommunikationspartner teilt Ihnen mit, dass E-Mails von Ihrer Domain in SPF-Prüfungen als ungültig erkannt werden.

**Problem: Eigener TXT-Eintrag fehlerhaft**

Die im TXT-Eintrag eingetragenen IP-Adressen Ihrer E-Mail-Server sind nicht korrekt oder fehlen.

**Behebung: TXT-Eintrag anpassen**

Fügen Sie die IPv4-Adressen Ihrer E-Mail-Server zum TXT-Eintrag hinzu oder korrigieren Sie die fehlerhaften IPv4-Adressen.

**Fehlerbehebung: Probleme beim Empfangen von E-Mails mit SPF-Prüfungen****Bedingung:**

SPF-Prüfungen werden für alle eingehenden E-Mails durchgeführt, für deren Absender-Domain ein TXT-Eintrag gesetzt ist. Eingehende E-Mails von bestimmten Domains werden fälschlicherweise als ungültig erkannt.

**Problem: Fehlerhafter TXT-Eintrag des Kommunikationspartners****Behebung: Kommunikationspartner informieren**

Informieren Sie den Kommunikationspartner über eine möglicherweise fehlerhafte SPF-Konfiguration.

**Behebung: IP-Adressen auf die Whitelist setzen**

1. Öffnen Sie das Control Panel.
2. Wählen Sie die betroffene Domain aus der Bereichsauswahl aus.
3. Navigieren Sie zu **Black- & Whitelists**.

4. Wählen Sie den Tab **Whitelist** aus.
5. Geben Sie in das Feld **Eintrag hinzufügen** die IPv4-Adresse des Kommunikationspartners ein.
6. Klicken Sie auf **Hinzufügen**, um Ihre Eingabe zu bestätigen.

## DKIM-Validierung und DKIM-Signierung

DKIM (DomainKeys Identified Mail) ist ein Verfahren zur E-Mail-Authentifizierung, das überprüft, ob E-Mails auf dem Übertragungsweg verändert wurden. Bei einer DKIM-Signierung wird dem E-Mail-Header einer ausgehenden E-Mail eine DKIM-Signatur hinzugefügt. Sobald ein Server eine E-Mail mit DKIM-Signatur empfängt und eine DKIM-Validierung durchführt, fragt der empfangende Server den öffentlichen Schlüssel ab, der in einem TXT-Eintrag in der DNS-Zone der Absender-Domain eingetragen wurde. Mit diesem Schlüssel wird überprüft, ob die DKIM-Signatur korrekt ist. Die DKIM-Validierung offenbart, ob eine E-Mail während der Zustellung verändert wurde.

Die Absender eingehender E-Mails können mit DKIM-Validierungen authentifiziert werden. Administratoren auf Kundenebene müssen hierzu zunächst die DKIM-Validierung aktivieren (siehe [DKIM-Validierung aktivieren](#) auf Seite 20) und anschließend die erweiterten Optionen konfigurieren (siehe [Erweiterte Optionen zur DKIM-Validierung konfigurieren](#) auf Seite 21).

Administratoren auf Kundenebene können den Empfängern von ausgehenden E-Mails ihrer Domains ermöglichen, DKIM-Validierungen durchzuführen. Dazu müssen die Administratoren zunächst CNAME-Einträge in der DNS-Zone ihrer Domains setzen, die auf unsere DKIM-Einträge verweisen (siehe [CNAME-Eintrag setzen](#) auf Seite 19). Anschließend müssen die Administratoren DKIM-Signaturen für ausgehende E-Mails ihrer Domains aktivieren (siehe [DKIM-Signierung aktivieren](#) auf Seite 24). Dadurch werden ausgehende E-Mails, die über unsere Infrastruktur geleitet werden, von uns mit DKIM signiert.

### CNAME-Eintrag setzen

Falls Sie DKIM (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19) verwenden möchten, müssen Sie CNAME-Einträge in der DNS-Zone Ihrer Domain setzen. Diese Einträge verweisen auf unsere DKIM-Einträge. Die Empfänger von E-Mails Ihrer Domain fragen diese Einträge ab, um den

öffentlichen Schlüssel zur Entschlüsselung unserer DKIM-Signatur und weitere Informationen zu erhalten, die zur Durchführung der DKIM-Validierung erforderlich sind.

1. Kontaktieren Sie den Support, um die CNAME-Einträge zu erhalten.
2. Setzen Sie die CNAME-Einträge in der DNS-Zone Ihrer Domain.



**CNAME-Einträge sind in der DNS-Zone Ihrer Domain gesetzt worden.**

Anschließend können Sie die DKIM-Validierung aktivieren (siehe [DKIM-Validierung aktivieren](#) auf Seite 20).

## DKIM-Validierung aktivieren



Sie haben Spam and Malware Protection für Ihre Domain aktiviert (siehe "Spam and Malware Protection aktivieren" im Control-Panel-Handbuch).

Sie können die DKIM-Validierung (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19) aktivieren, um die DKIM-Signaturen eingehender E-Mails zu prüfen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen > Email Authentication**.

4.

**WICHTIG:**

Die DKIM-Validierung kann nur für Ihre Domains aktiviert werden, die gültige DKIM-Einstellungen haben.

Aktivieren Sie unter **Absender-Authentifizierung** die Checkbox **DKIM-Validierung für eingehende E-Mails aktivieren**.

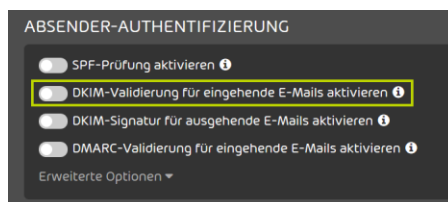


Abbildung 10: DKIM-Validierung aktivieren



Die DKIM-Validierung wird für eingehende E-Mails aktiviert.

**Hinweis:**

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.



Die DKIM-Validierung für eingehende E-Mails ist für Ihre Domain aktiviert worden.

Anschließend können Sie die erweiterten Optionen für die DKIM-Validierung konfigurieren (siehe [Erweiterte Optionen zur DKIM-Validierung konfigurieren](#) auf Seite 21).

## Erweiterte Optionen zur DKIM-Validierung konfigurieren



Sie haben die DKIM-Validierung aktiviert (siehe [DKIM-Validierung aktivieren](#) auf Seite 20).

Im Modul **Sicherheitseinstellungen** > **Email Authentication** können Sie konfigurieren, wie mit den Ergebnissen von DKIM-Validierungen (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19) umgegangen werden soll.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.

2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Email Authentication**.
4. Klicken Sie auf **Erweiterte Optionen**

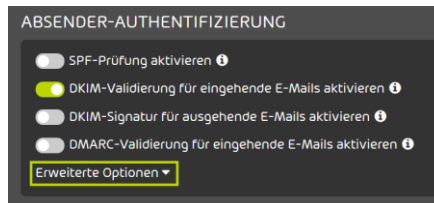


Abbildung 11: Erweiterte Optionen öffnen

- ➔ Eine Warnmeldung wird angezeigt.

5.



**WICHTIG:**

Änderungen an den erweiterten Optionen können dazu führen, dass schädliche E-Mails zugestellt werden.

Um die erweiterten Optionen zu ändern, klicken Sie auf **Bestätigen**

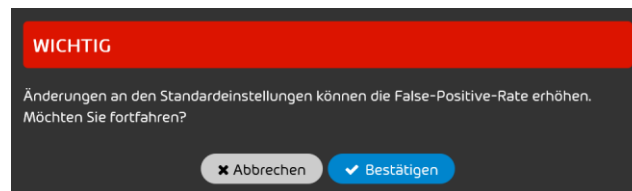


Abbildung 12: Bestätigen

6. Optional: Legen Sie unter **Erweiterte DKIM-Einstellungen** fest, was nach einem DKIM-Fail passieren soll. Sie haben die folgenden Optionen:
  - **E-Mail als Spam in Quarantäne speichern:** Die E-Mail wird als Spam markiert und in der Quarantäne gespeichert.
  - **E-Mail ablehnen:** Die E-Mail wird abgelehnt. Die E-Mail wird nicht an den Empfänger zugestellt und auch nicht in der Quarantäne gespeichert.

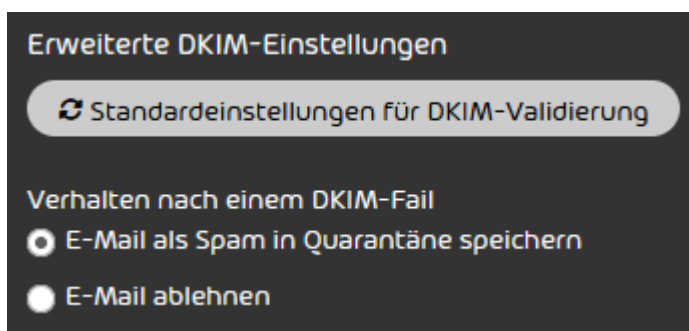


Abbildung 13: Erweiterte Optionen auswählen

7. Optional: Um die DKIM-Einstellungen auf die Standardeinstellungen zurückzusetzen, klicken Sie auf **Standardeinstellungen für DKIM-Validierung**

 **Hinweis:**

Bei den Standardeinstellungen werden E-Mails nach einem DKIM-Fail als Spam in der Quarantäne gespeichert.


-  Die Änderungen werden gespeichert.

 **Hinweis:**

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.

-  Die erweiterten Optionen zur DKIM-Validierung sind konfiguriert worden.

## DKIM-Signierung aktivieren

 Sie haben gültige CNAME-Einträge in der DNS-Zone Ihrer Domain gesetzt (siehe [CNAME-Eintrag setzen](#) auf Seite 19). Sie haben Spam and Malware Protection für Ihre Domain aktiviert (siehe 'Spam and Malware Protection aktivieren' im Control-Panel-Handbuch).

Im Modul **Sicherheitseinstellungen > Email Authentication** können Sie die DKIM-Signierung für ausgehende E-Mails Ihrer Domains aktivieren, damit die Empfänger der E-Mails DKIM-Validierungen durchführen können.

1. Melden Sie sich mit administrativen Anmeldedaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen > Email Authentication**.

4.



### WICHTIG:

Die DKIM-Validierung kann nur für Ihre Domains aktiviert werden, die gültige DKIM-Einträge haben.

Aktivieren Sie unter **Absender-Authentifizierung** die Checkbox **DKIM-Signatur für ausgehende E-Mails aktivieren**.

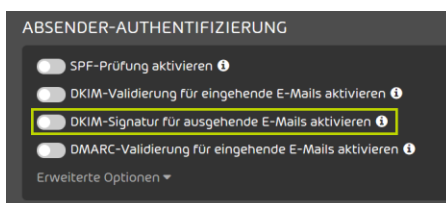


Abbildung 14: DKIM-Signatur aktivieren


-  Die DKIM-Signierung wird für ausgehende E-Mails aktiviert.



### Hinweis:

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.



 Die DKIM-Signierung für ausgehende E-Mails ist aktiviert worden.

## DMARC-Validierung

Mit DMARC (Domain-based Message Authentication, Reporting & Conformance) wird festgelegt, wie eine eingehende E-Mail abhängig von den Ergebnissen der SPF-Prüfung und der DKIM-Validierung sowie weiteren Abgleichen von Adressen und Domains behandelt werden soll.

Eine DMARC-Validierung prüft, ob eine eingehende E-Mail mit dem übereinstimmt, was der Empfänger über den Absender weiß. Falls in der DNS-Zone der Domain des Absenders ein DMARC-Eintrag gesetzt worden ist, folgt die DMARC-Validierung auf die SPF-Prüfung und die DKIM-Validierung. Anhand der Ergebnisse der SPF-Prüfung und der DKIM-Validierung sowie der Ergebnisse von Abgleichen der Adressen im Envelope-From und Header-From der E-Mail (SPF-Abgleich) einerseits und der Domains im Header-From und der DKIM-Signatur (DKIM-Abgleich) andererseits entscheidet die DMARC-Validierung, wie mit der E-Mail umgegangen wird. Für weitere Informationen zur DMARC-Entscheidungsmatrix siehe [DMARC-Entscheidungsmatrix](#) auf Seite 29.

Administratoren auf Kundenebene können die DMARC-Validierung für eingehende E-Mails ihrer Domains einrichten. Hierzu müssen die Administratoren zunächst einen DMARC-Eintrag in der DNS-Zone ihrer Domains setzen (siehe [DMARC-Eintrag setzen](#) auf Seite 25 und [Tags in DMARC-Einträgen](#) auf Seite 26), die DMARC-Validierung aktivieren (siehe [DMARC-Validierung aktivieren](#) auf Seite 35) und abschließend die erweiterten Optionen konfigurieren (siehe [Erweiterte Optionen zur DMARC-Validierung konfigurieren](#) auf Seite 36).

## DMARC-Eintrag setzen

Ein DMARC-Eintrag ist Voraussetzung dafür, dass für E-Mails einer Domain DMARC-Validierungen (siehe [DMARC-Validierung](#) auf Seite 25) durchgeführt werden können. Sie können für Ihre Domain einen DMARC-Eintrag setzen.

1. Erstellen Sie in der DNS-Zone Ihrer Domain einen TXT-Eintrag mit dem folgenden Namen. Ersetzen Sie **<domain.tld>** durch Ihre Domain.  
**\_dmarc.<domain.tld>**

2. Definieren Sie im TXT-Eintrag die DMARC-Richtlinie nach dem folgenden beispielhaften Schema. Ersetzen Sie `<benutzername@domain.tld>` durch eine E-Mail-Adresse.  
`v=DMARC1;p=quarantine;pct=100;rua=mailto:<benutzername@domain.tld>`

 **WICHTIG:**

Das Kapitel [Tags in DMARC-Einträgen](#) auf Seite 26 enthält eine Übersicht und Erklärungen der Tags, die in DMARC-Einträgen verwendet werden können.

 **Hinweis:**

Die Angaben aus dem DMARC-Eintrag gelten für E-Mails, die an Empfänger außerhalb der Domain versendet werden. Die Einstellungen für E-Mails, die an Empfänger innerhalb der Domain versendet werden, können im Modul **Email Authentication** konfiguriert werden.



In der DNS-Zone der Domain ist ein DMARC-Eintrag gesetzt worden.




## Tags in DMARC-Einträgen

DMARC-Einträge bestehen aus Tags. Die Tags eines DMARC-Eintrags enthalten Vorgaben für die DMARC-Validierungen von E-Mails, die von der Domain an Empfänger außerhalb der Domain versandt werden.

Die folgende Tabelle enthält eine Übersicht und Erklärungen der Tags, die in DMARC-Einträgen verwendet werden können. Mit Ausnahme von **v** und **p** sind alle Tags optional.

 **WICHTIG:**

Die Tags **v** und **p** sind Pflichtangaben.

TAG	ERKLÄRUNG	MÖGLICHE WERTE
v	Dieser Tag legt fest, welche DMARC-Protokollversion verwendet wird.	<b>v=DMARC1</b>  <b>Hinweis:</b> Für diesen Tag ist nur <b>v=DMARC1</b> möglich.
p	Dieser Tag legt fest, wie mit einer E-Mail der Domain umgegangen wird, falls die DMARC-Validierung für die E-Mail fehlschlägt.	<b>p=quarantine:</b> Die E-Mail wird in der Quarantäne gespeichert. <b>p=reject:</b> Die E-Mail wird abgelehnt. <b>p=none:</b> Für die E-Mail wird keine Maßnahme durchgeführt.  <b>Hinweis:</b> Wir empfehlen <b>p=quarantine</b> .
pct	Dieser Tag legt fest, für welchen Prozentsatz der E-Mails DMARC-Validierungen durchgeführt werden. Als Wert für diesen Tag sind Zahlen zwischen 1 und 100 möglich.	<b>pct=100</b>  <b>Hinweis:</b> Wir empfehlen <b>pct=100</b> , damit DMARC-Validierungen für alle E-Mails der Domain durchgeführt werden.

**TAG****ERKLÄRUNG****MÖGLICHE WERTE****rua**

Dieser Tag legt fest, an welche E-Mail-Adresse täglich Sammelberichte über fehlgeschlagene DMARC-Validierungen geschickt werden.

**rua=mailto:<benutzername@domain.com>**

Statt

**<benutzername@domain.com>**

wird die E-Mail-Adresse eingegeben, an die die Sammelberichte geschickt werden sollen.

**ruf**

Dieser Tag legt fest, an welche E-Mail-Adresse forensische Berichte über einzelne E-Mails geschickt werden, für die die DMARC-Validierung fehlgeschlagen ist.

**ruf=mailto:<benutzername@domain.com>**

Statt

**<benutzername@domain.com>**

wird die E-Mail-Adresse eingegeben, an die die forensischen Berichte geschickt werden sollen.

**sp**

Dieser Tag legt fest, wie mit einer E-Mail einer Subdomain der Domain umgegangen wird, falls die DMARC-Validierung für die E-Mail fehlschlägt.

**sp=quarantine:** Die E-Mail wird in der Quarantäne gespeichert.**sp=reject:** Die E-Mail wird abgelehnt.**sp=none:** Für die E-Mail wird keine Maßnahme durchgeführt.

TAG	ERKLÄRUNG	MÖGLICHE WERTE
<b>adkim</b>	<p>Dieser Tag legt den Abgleichmodus für DKIM-Signaturen fest (siehe <a href="#">DKIM-Validierung und DKIM-Signierung</a> auf Seite 19). Der Abgleichmodus bestimmt, wie genau eine E-Mail mit der DKIM-Signatur übereinstimmen muss, damit die E-Mail akzeptiert wird.</p>	<p><b>adkim=r</b>: Der Abgleichmodus ist entspannt. Eine Teilübereinstimmung reicht aus.</p> <p><b>adkim=s</b>: Der Abgleichmodus ist streng. Eine vollständige Übereinstimmung ist erforderlich.</p>
<b>aspf</b>	<p>Dieser Tag legt den Abgleichmodus für die Domains aus dem Header-From und Envelope-From einer E-Mail fest (siehe <a href="#">SPF-Prüfung</a> auf Seite 6). Der Abgleichmodus bestimmt, wie genau die beiden Domains miteinander übereinstimmen müssen, damit die E-Mail akzeptiert wird.</p>	<p><b>aspf=r</b>: Der Abgleichmodus ist entspannt. Eine Teilübereinstimmung reicht aus.</p> <p><b>aspf=s</b>: Der Abgleichmodus ist streng. Eine vollständige Übereinstimmung ist erforderlich.</p>

## DMARC-Entscheidungsmatrix

Die DMARC-Entscheidungsmatrix gibt an, wie mit eingehenden E-Mails nach erfolgreichen oder fehlgeschlagenen SPF-Prüfungen und DKIM-Validierungen umgegangen wird.

Tabelle 4: DMARC-Entscheidungsmatrix

<b>SPF-PRÜFUNG</b>	<b>DKIM-VALIDIERUNG</b>	<b>SPF-ABGLEICH</b>	<b>DKIM-ABGLEICH</b>	<b>DMARC-ERGEBNIS</b>	<b>FOLGEN</b>
Pass	Pass	Pass	Pass	Pass	Zustellen
Pass	Pass	Pass	Fail	Pass	Zustellen
Pass	Pass	Fail	Pass	Pass	Zustellen
Pass	Pass	Fail	Fail	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln
Pass	Fail	Pass	Pass	Pass	Zustellen
Pass	Fail	Pass	Fail	Pass	Zustellen

<b>SPF-PRÜFUNG</b>	<b>DKIM-VALIDIERUNG</b>	<b>SPF-ABGLEICH</b>	<b>DKIM-ABGLEICH</b>	<b>DMARC-ERGEBNIS</b>	<b>FOLGEN</b>
Pass	Fail	Fail	Pass	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln
Pass	Fail	Fail	Fail	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln
Fail	Pass	Pass	Pass	Pass	Zustellen

SPF-PRÜFUNG	DKIM-VALIDIERUNG	SPF-ABGLEICH	DKIM-ABGLEICH	DMARC-ERGEBNIS	FOLGEN
Fail	Pass	Pass	Fail	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln
Fail	Pass	Fail	Pass	Pass	Zustellen
Fail	Pass	Fail	Fail	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln



SPF-PRÜFUNG	DKIM-VALIDIERUNG	SPF-ABGLEICH	DKIM-ABGLEICH	DMARC-ERGEBNIS	FOLGEN
Fail	Fail	Pass	Pass	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln
Fail	Fail	Pass	Fail	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln

SPF-PRÜFUNG	DKIM-VALIDIERUNG	SPF-ABGLEICH	DKIM-ABGLEICH	DMARC-ERGEBNIS	FOLGEN
Fail	Fail	Fail	Pass	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln
Fail	Fail	Fail	Fail	Fail	Wahlweise als Spam in der Quarantäne speichern, ablehnen oder gemäß der DMARC-Richtlinie des Absenders behandeln

Das DMARC-Ergebnis fällt nur dann positiv aus, falls sowohl die SPF-Prüfung (siehe [SPF-Prüfung](#) auf Seite 6) oder die DKIM-Validierung (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19) als auch der zugehörige Abgleich (SPF-Abgleich oder DKIM-Abgleich) bestanden worden sind. Bei einem positiven DMARC-Ergebnis wird die E-Mail zugestellt. Ansonsten wird die E-Mail abhängig von den Einstellungen im Modul **Email Authentication** (siehe [Erweiterte Optionen zur DMARC-Validierung konfigurieren](#) auf Seite 36) im Control Panel entweder als Spam in der Quarantäne gespeichert, abgelehnt oder gemäß der DMARC-Richtlinie der Absenderdomain behandelt (sofern vorhanden).

## DMARC-Validierung aktivieren



Sie haben gültige SPF-, DKIM- und DMARC-Einträge für mindestens eine Ihrer Domains gesetzt (siehe [SPF-Eintrag setzen](#) auf Seite 9, [CNAME-Eintrag setzen](#) auf Seite 19 und [DMARC-Eintrag setzen](#) auf Seite 25). Sie haben Spam and Malware Protection für Ihre Domain aktiviert (siehe "Spam and Malware Protection aktivieren" im Control-Panel-Handbuch).

Sie können die DMARC-Validierung aktivieren, um den Umgang mit eingehenden E-Mails in Abhängigkeit von den Ergebnissen von SPF-Prüfungen (siehe [SPF-Prüfung](#) auf Seite 6) und DKIM-Validierungen (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19) festzulegen.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen > Email Authentication**.

4.



### WICHTIG:

Die DMARC-Validierung kann nur für Ihre Domains aktiviert werden, die gültige SPF-, DKIM- und DMARC-Einträge haben.

Aktivieren Sie unter **Absender-Authentifizierung** die Checkbox **DMARC-Validierung für eingehende E-Mails aktivieren**.

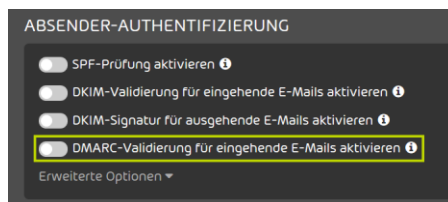


Abbildung 15: DMARC-Validierung aktivieren



Die DMARC-Validierung wird für eingehende E-Mails aktiviert.



### Hinweis:

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.

 Die DMARC-Validierung für eingehende E-Mails ist aktiviert worden.

Anschließend können Sie die erweiterten Optionen zur DMARC-Validierung konfigurieren (siehe [Erweiterte Optionen zur DMARC-Validierung konfigurieren](#) auf Seite 36).

## Erweiterte Optionen zur DMARC-Validierung konfigurieren

 Sie haben die DMARC-Validierung aktiviert (siehe [DMARC-Validierung aktivieren](#) auf Seite 35).

Im Modul **Sicherheitseinstellungen** > **Email Authentication** können Sie konfigurieren, wie mit den Ergebnissen von DMARC-Validierungen (siehe [DMARC-Validierung](#) auf Seite 25) umgegangen werden soll.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen** > **Email Authentication**.
4. Klicken Sie auf **Erweiterte Optionen**.

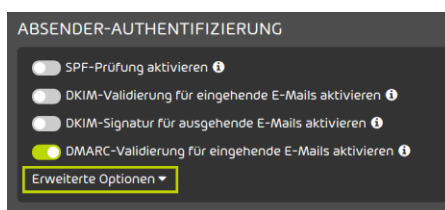



Abbildung 16: Erweiterte Optionen öffnen

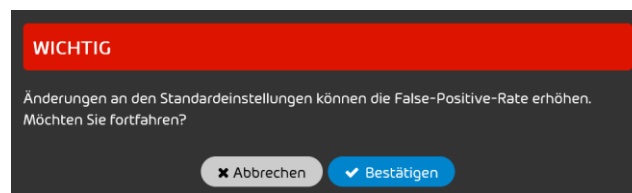
-  Eine Warnmeldung wird angezeigt.

5.

**WICHTIG:**

Änderungen an den erweiterten Optionen können dazu führen, dass schädliche E-Mails zugestellt werden.

Um die erweiterten Optionen zu ändern, klicken Sie auf **Bestätigen**.



**Abbildung 17: Bestätigen**

6. Optional: Legen Sie unter **Erweiterte DMARC-Einstellungen** fest, wie mit einem DMARC-Fail umgegangen werden soll. Sie haben die folgenden Optionen:
- **E-Mail als Spam in Quarantäne speichern:** Die E-Mail wird als Spam markiert und in der Quarantäne gespeichert.
  - **E-Mail ablehnen:** Die E-Mail wird abgelehnt. Die E-Mail wird nicht an den Empfänger zugestellt und auch nicht in der Quarantäne gespeichert.
  - **Richtlinie der Absenderdomain anwenden:** Nach einem DMARC-Fail wird das Verhalten angewendet, das in der DMARC-Richtlinie der Absenderdomain eingestellt ist. Dies ist die Standardeinstellung.


**Hinweis:**

Falls Sie diese Option auswählen, vertrauen Sie den DMARC-Richtlinien Dritter.

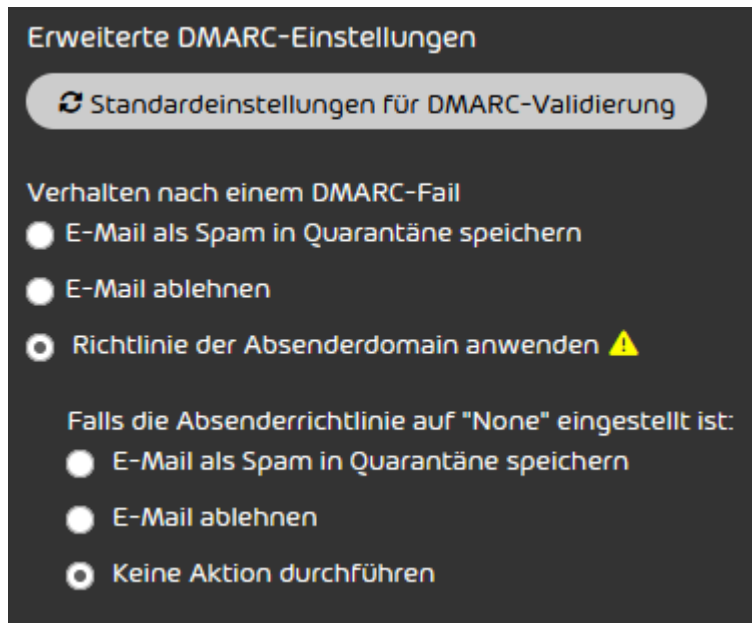


Abbildung 18: Verhalten nach DMARC-Fail auswählen

- ➔ Falls die Option **Richtlinie der Absenderdomain anwenden** ausgewählt worden ist, werden weitere Einstellungen angezeigt.

7. Falls Sie die Option **Richtlinie der Absenderdomain anwenden** ausgewählt haben, legen Sie unter **Falls die Absenderrichtlinie auf "None" eingestellt ist:** fest, welches Verhalten angewendet werden soll, falls die DMARC-Richtlinie der Absenderdomain auf "None" eingestellt ist. Sie haben die folgenden Optionen:
- **E-Mail als Spam in Quarantäne speichern:** Die E-Mail wird als Spam markiert und in der Quarantäne gespeichert.
  - **E-Mail ablehnen:** Die E-Mail wird abgelehnt. Die E-Mail wird nicht an den Empfänger zugestellt und auch nicht in der Quarantäne gespeichert.
  - **Keine Aktion durchführen:** Der DMARC-Fail löst keine Aktion aus. Die E-Mail wird anschließend durch weitere Filter unserer Services geprüft.

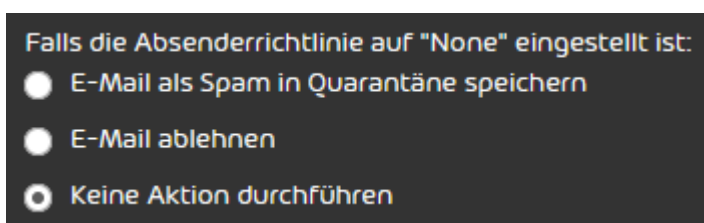


Abbildung 19: Verhalten bei Absenderrichtlinien mit der Einstellung "None"

8. Optional: Um die DMARC-Einstellungen auf die Standardeinstellungen zurückzusetzen, klicken Sie auf **Standardeinstellungen für DMARC-Validierung**

 **Hinweis:**

Bei den Standardeinstellungen werden E-Mails nach einem DMARC-Fail gemäß der DMARC-Richtlinie des Absenders behandelt. Falls für die DMARC-Richtlinie des Absenders der Wert **None** eingetragen ist (siehe [DMARC-Eintrag setzen](#) auf Seite 25), wird standardmäßig keine Aktion durchgeführt.

-  Die Änderungen werden gespeichert.

 **Hinweis:**

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.

 Die erweiterten Optionen zur DMARC-Validierung sind konfiguriert worden.

## Ausnahmen hinzufügen

 Sie haben im Modul **Email Authentication** Verfahren zur Absender-Authentifizierung aktiviert (siehe [Verfahren zur Absender-Authentifizierung](#) auf Seite 6).

Falls Sie die SPF-Prüfung (siehe [SPF-Prüfung](#) auf Seite 6), die DKIM-Validierung (siehe [DKIM-Validierung und DKIM-Signierung](#) auf Seite 19) und/oder die DMARC-Validierung (siehe [DMARC-Validierung](#) auf Seite 25) aktiviert haben und diese für eine Ihrer Domains deaktivieren möchten, fügen Sie eine Ausnahme hinzu.

1. Melden Sie sich mit Ihren administrativen Zugangsdaten im Control Panel an.
2. Wählen Sie Ihre Domain in der Bereichsauswahl aus.
3. Navigieren Sie zu **Sicherheitseinstellungen > Email Authentication**.
4. Klicken Sie unter **Ausnahmen** auf **Ausnahme hinzufügen**.

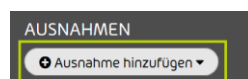


Abbildung 20: Ausnahme hinzufügen

 Eine erweiterte Ansicht öffnet sich.

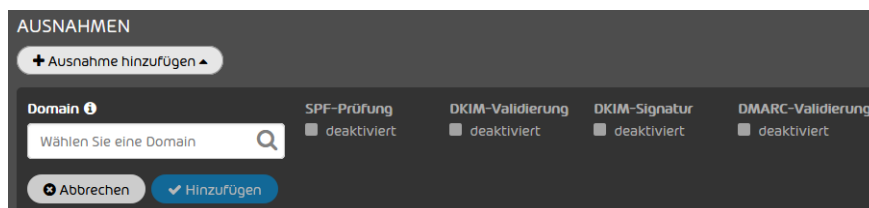


Abbildung 21: Erweiterte Ansicht



- Wählen Sie unter **Domain** eine Domain aus, für die Sie die Ausnahme hinzufügen möchten.

 **Hinweis:**


Sie können nur Domains auswählen, für die Spam and Malware Protection aktiviert ist.

- Aktivieren Sie die Checkbox unter der Prüfung, die Sie für die Domain deaktivieren möchten.

 **Hinweis:**

Sie können für eine Domain die SPF-Prüfung, die DKIM-Validierung oder die DMARC-Validierung nur deaktivieren, falls die Domain die zugehörigen gültigen DNS-Einstellungen hat. Auf alle anderen Domains werden die Prüfungen nicht angewendet.

- Klicken Sie auf **Hinzufügen**

-  Die Ausnahme wird hinzugefügt und erscheint in der unten stehenden Tabelle.

 **Hinweis:**

Aufgrund von DNS-Caching kann es bis zu 72 Stunden dauern, bis die Änderung wirksam wird.

-  Eine Ausnahme ist zu Email Authentication hinzugefügt worden.

## Kategorisierungsgründe von Email Authentication

Für E-Mails, bei denen die Absender-Authentifizierung mit Email Authentication einen Fehler ergeben hat, werden im Control Panel bestimmte Kategorisierungsgründe verwendet. Für Informationen zu weiteren Kategorisierungsgründen siehe das Kapitel "Kategorisierungsgründe" im Control-Panel-Handbuch.

### SPF

E-Mails, bei denen mit einer SPF-Prüfung festgestellt wurde, dass sie nicht von einem im DNS eingetragenen Server versandt wurden, werden abhängig von Ihren Einstellungen als Spam in der

Quarantäne gespeichert, abgelehnt oder zugestellt (siehe [Erweiterte Optionen zur SPF-Prüfung konfigurieren](#) auf Seite 14).

Im Control Panel werden diese E-Mails im Modul **Email Live Tracking** unabhängig von der durchgeführten Maßnahme mit dem Grund **Envelope SPF Failure** und **Message Header SPF Failure** angezeigt.

## DKIM

E-Mails, bei denen die DKIM-Validierung fehlgeschlagen ist, werden abhängig von Ihren Einstellungen als Spam in der Quarantäne gespeichert oder abgelehnt (siehe [Erweiterte Optionen zur DMARC-Validierung konfigurieren](#) auf Seite 36).

Im Control Panel werden diese E-Mails im Modul **Email Live Tracking** mit dem Grund **DKIM Failure** angezeigt.

## DMARC

E-Mails, bei denen mit einer DMARC-Validierung festgestellt wurde, dass sie nicht den eingetragenen Regelungen für SPF und/oder DKIM entsprechen, werden abhängig von Ihren Einstellungen als Spam in der Quarantäne gespeichert oder abgelehnt (siehe [Erweiterte Optionen zur DMARC-Validierung konfigurieren](#) auf Seite 36).

Im Control Panel werden diese E-Mails im Modul **Email Live Tracking** mit dem Grund **DMARC Failure** angezeigt.

# Index

## A

- Absender-Authentifizierung
  - Verfahren [6](#)
- aktivieren
  - DKIM-Signatur [24](#)
  - DKIM-Validierung [20](#)
  - DMARC-Validierung [35](#)
  - SPF-Prüfung [10](#)
- auf Whitelist setzen
  - IP-Adresse [17](#), [18](#)
- Ausnahme
  - Email Authentication [40](#)
- Authentifizierung
  - Absender, **See** Email Authentication Erklärung

## C

- CNAME-Eintrag
  - setzen [19](#)

## D

- DKIM [3](#), [19](#)
- DKIM-Konfiguration
  - prüfen [4](#)
- DKIM-Signatur
  - aktivieren [24](#)
- DKIM-Validierung
  - aktivieren [20](#)
- DMARC [3](#), [25](#)
  - Entscheidungsmatrix [29](#)
- DMARC-Eintrag
  - setzen [25](#)
- DMARC-Konfiguration
  - prüfen [4](#)
- DMARC-Validierung
  - aktivieren [35](#)
- Domain-based Message Authentication, Reporting & Conformance [25](#)
- DomainKeys Identified Mail [19](#)

## E

- E-Mail
  - Kategorisierungsgründe von Email Authentication, **See** Kategorisierungsgründe Email Authentication

Email Authentication

Ausnahme [40](#)

Erklärung [3](#)

Kategorisierungsgründe, *See* Kategorisierungsgründe Email Authentication

## F

False Positives

ausgehende E-Mails [17](#)

eingehende E-Mails [18](#)

Fehlerbehebung

ausgehende E-Mails [17](#)

eingehende E-Mails [18](#)

## I

IP-Adresse

auf Whitelist setzen [17](#), [18](#)

## K

Kategorisierungsgründe

Email Authentication [41](#)

konfigurieren

Verhalten bei SPF-Prüfung [14](#)

Verhalten nach DKIM-Validierung [21](#)

Verhalten nach DMARC-Validierung [36](#)

## P

prüfen

DKIM-Konfiguration [4](#)

DMARC-Konfiguration [4](#)

SPF-Konfiguration [4](#)

## S

Sender Policy Framework [6](#)

setzen

CNAME-Eintrag [19](#)

DMARC-Eintrag, *See* DMARC-Eintrag setzen

SPF-Eintrag [9](#)

TXT-Eintrag für DMARC, *See* TXT-Eintrag für DMARC setzen

TXT-Eintrag für SPF, *See* setzen SPF-Eintrag

SPF [3](#), [6](#)

Logik [7](#)

SPF-Eintrag

setzen [9](#)

SPF-Konfiguration  
  prüfen [4](#)  
SPF-Prüfung  
  aktivieren [10](#)

## T

TXT-Eintrag  
  fehlerhaft [17](#), [18](#)  
  für SPF setzen, **See** SPF-Eintrag setzen  
TXT-Eintrag für DMARC  
  setzen [25](#)

## V

Verfahren  
  Absender-Authentifizierung  
    Absender-Authentifizierung  
      Verfahren [6](#)  
Verhalten bei SPF-Prüfung  
  konfigurieren [14](#)  
Verhalten nach DKIM-Validierung  
  konfigurieren [21](#)  
Verhalten nach DMARC-Validierung  
  konfigurieren [36](#)

