Email Authentication

Contents

À propos de l’ Email Authentication

L'Email Authentication offre aux administrateurs côté clients différentes possibilités pour authentifier les expéditeurs de courriels (voir Procédures d’ authentification des expéditeurs à la page 6). Les procédures suivantes sont disponibles :

- Validation SPF (Sender Policy Framework) (voir Vérification SPF à la page 6)
- Validation DKIM et signature DKIM (DomainKeys Identified Mail) (voir Validation DKIM et signature DKIM à la page 19)
- Validation DMARC (Domain-based Message Authentication, Reporting and Conformance) (voir Validation DMARC à la page 24)

L'Email Authentication ne peut être utilisée que si la Spam and Malware Protection a été activée (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel). Avant d'activer la procédure, les administrateurs côté clients doivent vérifier les paramètres DNS de leurs propres domaines (voir Vérifier les paramètres DNS d’ un domaine propre à la page 4).

Vérifier les paramètres DNS d’ un domaine propre

Vous avez activé la Spam and Malware Protection (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

REMARQUE :

Vous pouvez vérifier les paramètres DNS uniquement pour les domaines pour lesquels la Spam and Malware Protection est activée.

Avant de paramétrer les procédures pour l'authentification des expéditeurs, vous devez vérifier si les paramètres DNS de vos domaines sont correctement configurés. Le statut des paramètres SPF, DKIM et DMARC de vos domaines est alors vérifié.

IMPORTANT :

Vous pouvez activer la vérification SPF (voir Vérification SPF à la page 6), la validation DKIM (voir Validation DKIM et signature DKIM à la page 19) et la validation DMARC (voir Validation DMARC à la page 24) uniquement pour vos domaines pour lesquels les paramètres DNS correspondants sont correctement configurés.

REMARQUE :

Pour savoir comment définir un enregistrement SPF, voir Définir un enregistrement SPF à la page 9.

Pour savoir comment définir un enregistrement CNAME, voir Définir un enregistrement CNAME à la page 19.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.

4. Cliquez sur **Mettre à jour les paramètres DNS** pour vérifier le statut des paramètres DNS de vos domaines.

Illustration 1 : Actualiser les paramètres DNS

Vous obtenez un aperçu sous forme de tableau du statut des paramètres DNS de vos domaines. Les trois résultats suivants sont possibles#:

✓	Les paramètres du domaine sont configurés correctement.
!	Aucun enregistrement n’est défini pour le domaine.
✗	Les paramètres du domaine ne sont pas configurés correctement.

Les paramètres DNS de vos domaines ont été vérifiés.

Vous pouvez ensuite activer des procédures d'authentification des expéditeurs (voir Procédures d’ authentification des expéditeurs à la page 6).

Procédures d’ authentification des expéditeurs

Les administrateurs côté client peuvent activer différentes procédures d'authentification d'expéditeurs de courriels pour leurs domaines. Les procédures suivantes sont disponibles :

- Vérification SPF à la page 6
- Validation DKIM et signature DKIM à la page 19
- Validation DMARC à la page 24

Ces procédures renforcent la protection de l'infrastructure des courriels des entreprises contre le spam et le phishing. Les administrateurs côté client peuvent utiliser les procédures séparément ou les combiner entre elles.

La combinaison de plusieurs procédures offre une protection supérieure. À titre d'exemple, sur les serveurs utilisant uniquement DKIM, le message indésirable peut être diffusé par un courriel avec une signature DKIM valide. Tant que ce courriel n'est pas modifié, il peut être expédié en masse à différentes personnes avec une signature DKIM valide. Pour éviter cela, il est possible d'utiliser également SPF. SPF vérifie l'origine du courriel. Ainsi, l'adresse IPv4 et le nom du domaine du serveur de messagerie sont vérifiés. SPF refuse les courriels des serveurs non autorisés. Il est alors impossible d'envoyer des messages indésirables par des courriels avec une signature DKIM valide.

En outre, les administrateurs côté client peuvent définir des exceptions aux procédures pour certains de leurs domaines (voir Ajouter des exceptions à la page 39).

Les courriels pour lesquels l'authentification de l'expéditeur a engendré une erreur sont rejetés ou marqués comme spam. Pour les courriels dont la vérification SPF, la validation DKIM ou la validation DMARC a échoué, certaines raisons de catégorisation sont indiquées dans le Control Panel (voir Raisons de catégorisation d’ Email Authentication à la page 40).

Vérification SPF

SPF (Sender Policy Framework) est une procédure d'authentification des expéditeurs qui vérifie si l'adresse des expéditeurs d'un courriel est usurpée. Lors d'une vérification SPF, le serveur entrant vérifie si un courriel entrant provient d'un serveur autorisé. À cet effet, le serveur entrant vérifie si l'adresse IP du serveur sortant est saisie dans une entrée SPF dans la zone DNS du domaine de

l'expéditeur. Dans une entrée SPF sont saisies les adresses IP du serveur qui sont autorisées pour l'envoi de courriels d'un domaine. Pour de plus amples informations sur la logique de la vérification SPF, voir Logique de la vérification SPF à la page 7.

Les administrateurs côté clients peuvent configurer la vérification SPF pour les courriels entrants de leurs domaines. Les administrateurs côté clients doivent définir à cet effet les enregistrements SPF, dans un premier temps, pour tous leurs domaines (voir Définir un enregistrement SPF à la page 9) pour lesquels ils veulent appliquer les vérifications SPF aux courriels entrants. Les administrateurs doivent ensuite activer la vérification SPF (voir Activer la vérification SPF à la page 10) et configurer les options avancées (voir Configurer les options étendues pour la vérification SPF à la page 14).

Le chapitre Élimination des erreurs à la page 17 explique comment les erreurs peuvent être corrigées lors des vérifications SPF.

Logique de la vérification SPF

La logique des vérifications SPF est décrite ci-après.

À la réception d'un courriel sur un serveur destinataire, l'adresse IP du serveur envoyé est synchronisée avec les enregistrements de l'enregistrement TXT du domaine de l'adresse courriel du serveur d'envoi. Si l'adresse IP du serveur d'envoi n'est pas incluse dans l'enregistrement TXT, une erreur est affichée. Lors de la vérification de l'enregistrement TXT, une distinction est faite entre les Hardfails et les Softfails, en fonction de leur gravité.

Les administrateurs côté clients peuvent décider des mesures à appliquer en fonction du type d'erreur (voir Activer la vérification SPF à la page 10). Si aucune erreur ne survient, le courriel est délivré de la manière habituelle.

REMARQUE :

Les exécutions suivantes reposent sur l'hypothèse selon laquelle les informations sur l'expéditeur de l'enveloppe (MAIL FROM) et les informations sur l'expéditeur de l'entête (From) doivent être vérifiées. Si une seule de ces informations doit être vérifiée, un seul contrôle a lieu, et le type d'échec de cette vérification est déterminant.

La logique suivante est prise en compte lors de l'analyse de l'enregistrement TXT :

1. La première étape consiste à vérifier simultanément les domaines indiqués dans l'enveloppe (MAIL FROM) et dans l'entête (From). Si l'une des vérifications contient une erreur, le type d'erreur est pris en compte lors de la prochaine étape. Si les deux vérifications contiennent des erreurs, le type d'erreur la plus grave est pris en compte pour l'étape suivante. Il existe trois possibilités.

Tableau 1 : Possibilité 1 : les deux vérifications SPF entraînent des Softfails

Si les vérifications SPF pour l'enveloppe et l'entête contiennent toutes deux des Softfails, un Softfail est pris en compte à la prochaine étape.

PARTIE DU COURRIEL	CONFIGURATION	TYPE D'ÉCHEC
Enveloppe (MAIL FROM)	~tous	Softfail
Entête (From)	~tous	Softfail

Tableau 2 : Possibilité 2 : les deux vérifications SPF entraînent des Hardfails

Si les vérifications SPF pour l'enveloppe et l'entête contiennent toutes deux des Hardfails, un Hardfail est pris en compte à la prochaine étape.

PARTIE DU COURRIEL	CONFIGURATION	TYPE D'ÉCHEC
Enveloppe (MAIL FROM)	-tous	Hardfail
Entête (From)	-tous	Hardfail

Tableau 3 : Possibilité 3 : les vérifications SPF entraînent différentes erreurs

Si les vérifications SPF pour l'enveloppe et l'en-tête contiennent différentes erreurs, un Hardfail est pris en compte à la prochaine étape.

PARTIE DU COURRIEL	CONFIGURATION	TYPE D'ÉCHEC
Enveloppe (MAIL FROM)	-tous	Hardfail
Entête (From)	~tous	Softfail

2. Lors de la deuxième étape, on vérifie les mesures que vous avez paramétrées pour un Hardfail ou un Softfail. Cette mesure est appliquée.

REMARQUE :

Dans des vérifications SPF, seuls les qualificatifs **-** et **~** sont pris en charge. Le qualificatif **-** représente le code de résultat Hardfail et le qualificatif **~** représente le code de résultat Softfail. Le qualificatif **?** n'est pas pris en charge.

Définir un enregistrement SPF

Vous pouvez définir un enregistrement SPF dans la zone DNS de votre domaine afin d'autoriser nos serveurs à envoyer des courriels au nom de votre domaine. Spam and Malware Protection (voir « Spam and Malware Protection » dans le manuel du Control Panel) peut, grâce à l'enregistrement SPF, reconnaître à temps les tentatives de tromperie, telles que le spoofing. Les destinataires extérieurs à votre organisation peuvent utiliser l'enregistrement SPF pour effectuer des contrôles SPF sur les courriels de votre domaine. En outre, vous avez besoin de l'enregistrement SPF afin que Email Authentication puisse effectuer des vérifications SPF (voir « Vérification SPF » dans le manuel du Control Panel) pour les courriels entrants.

IMPORTANT :

Enregistrez dans l'enregistrement SPF tous les serveurs qui peuvent envoyer des courriels depuis votre domaine.

REMARQUE :

Notre enregistrement SPF n'est pas nécessaire pour les clients qui ont configuré leur environnement principal avec l'option **IP/nom d'hôte**, mais qui n'ont enregistré aucune adresse de serveur de relais pour les courriels sortants. Pour obtenir de plus d'informations sur la configuration de l'environnement primaire, voir .

Vous devez définir vous-même l'enregistrement SPF dans la zone DNS de votre domaine. Pour obtenir de plus amples informations sur la façon dont vous pouvez définir correctement l'enregistrement SPF dans la zone DNS, veuillez contacter le support.

Activer la vérification SPF

Vous avez défini les enregistrements SPF valides dans la zone DNS de vos domaines (voir Définir un enregistrement SPF à la page 9). Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

IMPORTANT :

Les vérifications SPF sont réalisées uniquement pour les domaines avec des enregistrements SPF valides.

IMPORTANT :

La vérification SPF ne peut être activée que si le client remplit l'une des conditions suivantes :

- Le client a configuré son environnement principal avec l'option **IP/nom d'hôte** et a enregistré des adresses de serveurs de relais pour les courriels sortants. Le client a également défini notre enregistrement SPF en plus de ses propres enregistrements SPF dans la zone DNS (voir Définir un enregistrement SPF à la page 9).
- Le client a configuré son environnement principal avec l'option **IP/nom d'hôte** mais n'a pas enregistré d'adresse de serveurs de relais pour les courriels sortants. Le client a défini ses propres enregistrements SPF dans la zone DNS.

Pour plus d'informations concernant la configuration de l'environnement principal, voir le chapitre « Procéder à la configuration de l'environnement principal » dans le manuel du Control Panel.

Vous pouvez activer la vérification SPF pour vérifier si l'adresse IP du serveur sortant d'un courriel entrant est saisie dans les enregistrements SPF du domaine de l'expéditeur et est autorisée à envoyer des courriels du domaine.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Sous **Authentification d’ expéditeur**, cochez la case **Activer la vérification SPF**.

Illustration 2 : Activer la vérification SPF

Un message d’avertissement apparaît.

5. Cliquez sur **Confirmer**.

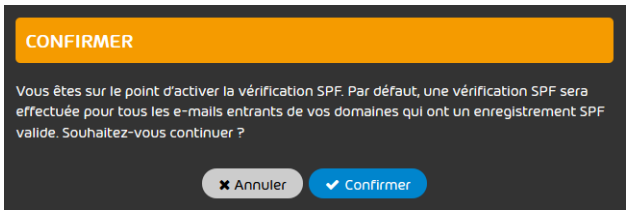

Illustration 3 : Confirmer

La vérification SPF est activée pour tous les domaines qui se trouvent sous le domaine sélectionné et pour lesquels les enregistrements SPF corrects sont définis.

6. Sélectionnez dans quels cas une vérification SPF soit être réalisée.

   - Si tous les courriels entrants pour lesquels un enregistrement SPF est défini pour le domaine de l'expéditeur, sélectionnez **Pour tous les e-mails entrants**.

     REMARQUE :

     Cette variante est recommandée s'il y a, d'une manière générale, de nombreuses usurpations d'adresses provenant de différents domaines d'expéditeurs. L'utilisation de cette variante peut entraîner l'augmentation du nombre de faux positifs si des partenaires de communication n'ont pas défini correctement leurs enregistrements SPF.

   - Si seuls les courriels entrants envoyés par le domaine ou un domaine d'alias du destinataire doivent être vérifiés, sélectionnez **Uniquement pour les e-mails envoyés dans un de vos propres domaines**.

     REMARQUE :

     Seuls les courriels internes sont vérifiés. Cette variante est recommandée pour prévenir les attaques ciblées sous une adresse courriel usurpée de votre propre domaine.

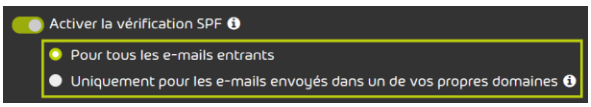

Illustration 4 : Sélectionner des courriels pour la vérification SPF

La vérification SPF est activée.

REMARQUE :

Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La vérification SPF a été activée.

Vous pouvez ensuite configurer les options étendues pour la vérification SPF (voir Configurer les options étendues pour la vérification SPF à la page 14).

Configurer les options étendues pour la vérification SPF

Vous avez activé la vérification SPF (voir Activer la vérification SPF à la page 10).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez configurer la façon de traiter les résultats des vérifications SPF (voir Vérification SPF à la page 6).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Cliquez sur **Options avancées**.

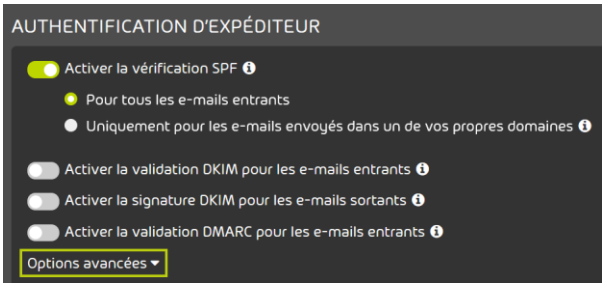

Illustration 5 : Ouvrir les options étendues

Un message d'avertissement apparaît.

5. **IMPORTANT :**

   Les modifications apportées aux options étendues peuvent entraîner la distribution de courriels malveillants.

   Pour modifier les options étendues, cliquez sur **Confirmer**.

Illustration 6 : Confirmer

6. Facultatif : Sous **Comportement après un échec sévère**, indiquez la conduite à tenir après un Hardfail SPF. Vous avez les options suivantes :

   - **Enregistrer le courriel comme spam en quarantaine** : le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
   - **Ne prendre aucune mesure** : le Hardfail SPF ne déclenche aucune action. Le courriel est ensuite vérifié par d'autres filtres de nos services.

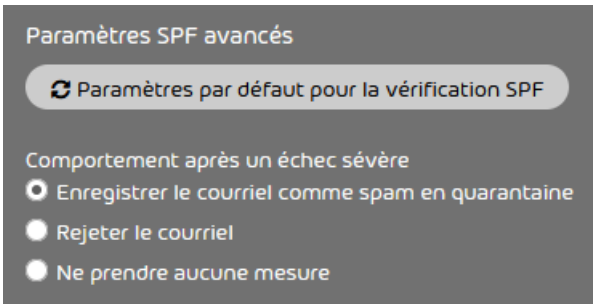

Illustration 7 : Sélectionner la procédure suite à un Hardfail SPF

7. Facultatif : Sous **Comportement après un échec partiel**, indiquez la conduite à tenir après un Softfail SPF. Vous avez trois options :

   - **Enregistrer le courriel comme spam en quarantaine** : le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
   - **Ne prendre aucune mesure** : le Softfail SPF ne déclenche aucune action. Le courriel est ensuite vérifié par d'autres filtres de nos services.

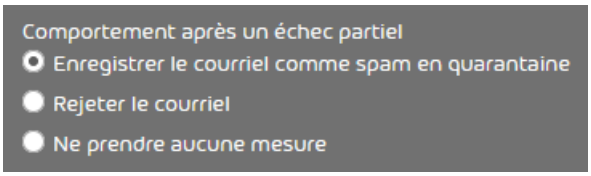

Illustration 8 : Sélectionner la procédure suite à un Softfail SPF

8. Facultatif : Sous **Analyse**, définissez les composants des courriels à analyser. Vous avez les options suivantes :

   - **Analyser uniquement 'envelope from’**
   - **Analyser uniquement 'header from’**
   - **Analyser 'envelope from' et 'header from’**

> **REMARQUE :**
>
> Si les deux indications sont vérifiées, la sécurité est améliorée, mais le nombre de faux positifs augmente également.

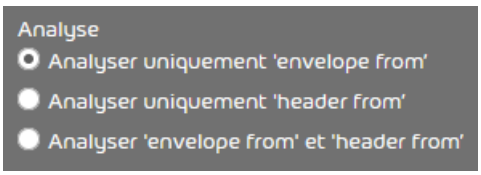

Illustration 9 : Configurer l’ analyse

9. Facultatif : Pour réinitialiser les paramètres SPF aux réglages par défaut, cliquez sur **Paramètres par défaut pour la vérification SPF**.

> **REMARQUE :**
>
> Avec les réglages par défaut, après un Hardfail SPF et un Softfail SPF, les courriels sont mis en quarantaine et seul « Envelope-From » est analysé.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Les options avancées pour la vérification du SPF ont été configurées.

Élimination des erreurs

Les erreurs suivantes lors des vérifications SPF peuvent être corrigées :

- Erreur due aux vérifications SPF lors de l'envoi de courriels (voir Élimination des erreurs : Problèmes lors de l’ envoi de courriels avec une entrée SPF configurée à la page 17)
- Erreur due aux vérifications SPF lors de la réception de courriels (voir Élimination des erreurs : Problèmes lors de la réception de courriels avec des vérifications SPF à la page 18)

Élimination des erreurs : Problèmes lors de l’ envoi de courriels avec une entrée SPF configurée

Condition :

L'une des conditions suivantes est remplie :

- Les vérifications SPF sont exécutées chez vous, uniquement lorsque le domaine de l'expéditeur correspond au domaine du destinataire. Les courriels internes entrants sont identifiés comme non valides par erreur.

- Votre partenaire de communication vous indique que les courriels de votre domaine sont identifiés comme non valides lors des vérifications SPF.

Problème : Enregistrement TXT propre erroné

Les adresses IP saisies dans l'enregistrement TXT de votre serveur de messagerie ne sont pas correctes ou sont manquantes.

Résolution : Modifier l’ enregistrement TXT

Insérez les adresses IPv4 de votre serveur de messagerie à l'enregistrement TXT ou corrigez les adresses IPv4 erronées.

Élimination des erreurs : Problèmes lors de la réception de courriels avec des vérifications SPF

Condition :

Les vérifications SPF sont exécutées pour tous les courriels entrants pour lesquels un enregistrement TXT est défini pour le domaine de l'expéditeur. Les courriels entrants de certains domaines sont identifiés comme non valides par erreur.

Problème : Enregistrement TXT erroné du partenaire de communication

Résolution : Informer le partenaire de communication

Informez le partenaire de communication d'une configuration SPF potentiellement erronée.

Résolution : Autoriser les adresses IP

1. Ouvrez le Control Panel.
2. Sélectionnez le domaine concerné dans la sélection de l'espace.
3. Naviguez vers **Expéditeurs interdits et autorisés**.
4. Sélectionnez l'onglet **Expéditeurs autorisés**.

5. Dans le champ **Ajouter entrée**, saisissez l'adresse IPv4 du partenaire de communication.
6. Cliquez sur **Ajouter** pour confirmer votre saisie.

Validation DKIM et signature DKIM

DKIM (DomainKeys Identified Mail) est une procédure d'authentification de courriels vérifiant si les courriels ont été modifiés sur la voie de transfert. Avec une signature DKIM, une signature DKIM est ajoutée à l'en-tête d'un courriel sortant. Dès qu'un serveur reçoit un courriel avec une signature DKIM et qu'une validation DKIM est effectuée, le serveur destinataire interroge la clé publique saisie dans une entrée TXT dans la zone DNS du domaine de l'expéditeur. Cette clé permet de vérifier si la signature DKIM est correcte. La validation DKIM indique si un courriel a été modifié pendant la distribution.

Les expéditeurs des courriels entrants peuvent être authentifiés avec les validations DKIM. Pour cela, les administrateurs côté clients doivent activer d'abord la validation DKIM (voir Activer la validation DKIM à la page 20) et configurer ensuite les options étendues (voir Configurer les options étendues pour la validation DKIM à la page 21).

Les administrateurs côté client peuvent permettre aux destinataires des courriels sortants de leurs domaines d'effectuer des validations DKIM. Pour ce faire, les administrateurs doivent d'abord définir des enregistrements CNAME dans la zone DNS de leurs domaines, qui renvoient à nos enregistrements DKIM (voir Définir un enregistrement CNAME à la page 19). Les administrateurs doivent ensuite activer les signatures DKIM pour les courriels sortants de leurs domaines (voir Activer la signature DKIM à la page 23). Les courriels sortants qui sont acheminés par notre infrastructure sont alors signés par nos soins avec DKIM.

Définir un enregistrement CNAME

Si vous souhaitez utiliser DKIM (voir Validation DKIM et signature DKIM à la page 19), vous devez définir des enregistrements CNAME dans la zone DNS de votre domaine. Ces enregistrements renvoient à nos enregistrements DKIM. Les destinataires des courriels de votre domaine interrogent ces enregistrements afin d'obtenir la clé publique pour le décryptage de notre signature DKIM et d'autres informations nécessaires pour effectuer la validation DKIM.

1. Contactez le support technique pour obtenir les enregistrements CNAME.
2. Définissez les enregistrements CNAME dans la zone DNS de votre domaine.

Les enregistrements CNAME ont été définis dans la zone DNS de votre domaine.

Vous pouvez ensuite activer la validation DKIM (voir Activer la validation DKIM à la page 20).

Activer la validation DKIM

Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Vous pouvez activer la validation DKIM (voir Validation DKIM et signature DKIM à la page 19) pour vérifier les signatures DKIM des courriels entrants.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l’espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. **IMPORTANT :**

   La validation DKIM peut être activée uniquement pour vos domaines avec des paramètres DKIM valides.

   Cochez la case **Activer la validation DKIM pour les e-mails entrants** sous **Authentification d’ expéditeur**.

Illustration 10 : Activer la validation DKIM

La validation DKIM est activée pour les courriels entrants.

> **REMARQUE :**
>
> Il peut s’écouler jusqu’à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La validation DKIM pour les courriels entrants a été activée pour votre domaine.

Vous pouvez ensuite configurer les options étendues pour la validation DKIM (voir Configurer les options étendues pour la validation DKIM à la page 21).

Configurer les options étendues pour la validation DKIM

Vous avez activé la validation DKIM (voir Activer la validation DKIM à la page 20).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez configurer la façon de traiter les résultats des validations DKIM (voir Validation DKIM et signature DKIM à la page 19).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l’espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Cliquez sur **Options avancées**.

Illustration 11 : Ouvrir les options étendues

Un message d’avertissement apparaît.

5. **IMPORTANT :**

   Les modifications apportées aux options étendues peuvent entraîner la distribution de courriels malveillants.

   Pour modifier les options étendues, cliquez sur **Confirmer**.

Illustration 12 : Confirmer

6. Facultatif : Sous **Paramètres DKIM avancés**, indiquez la conduite à tenir après un échec DKIM. Vous avez les options suivantes :

   - **Enregistrer le courriel comme spam en quarantaine** : le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.

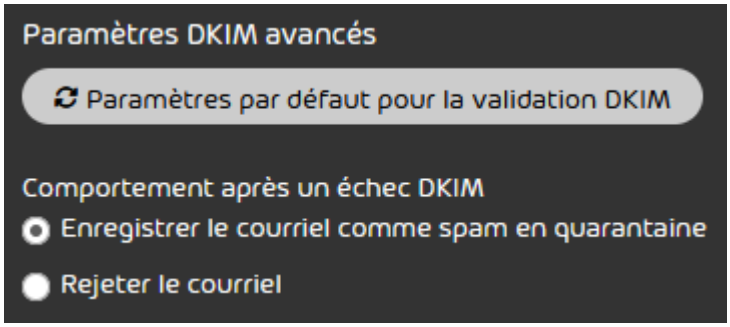

Illustration 13 : Sélectionner les options étendues

7. Facultatif : Pour réinitialiser les paramètres DKIM aux réglages par défaut, cliquez sur **Paramètres par défaut pour la validation DKIM**.

> **REMARQUE :**
>
> Avec les réglages par défaut, les courriels sont mis en quarantaines comme indésirables après un échec DKIM.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> Il peut s’écouler jusqu’à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Les options étendues pour la validation DKIM ont été configurées.

Activer la signature DKIM

Vous avez défini les enregistrements CNAME valides dans la zone DNS de votre domaine (voir Définir un enregistrement CNAME à la page 19). Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez activer la signature DKIM pour les courriels sortants de vos domaines afin que les destinataires des courriels puissent exécuter les validations DKIM.

1. Connectez-vous avec des identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l’espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.

4. **IMPORTANT :**

   La validation DKIM peut être activée uniquement pour vos domaines avec des entrées DKIM valides.

   Cochez la case **Activer la signature DKIM pour les e-mails sortants** sous **Authentification d’ expéditeur**.

Illustration 14 : Activer la signature DKIM

La signature DKIM a été activée pour les courriels sortants.

REMARQUE :

Il peut s’écouler jusqu’à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La signature DKIM a été activée pour les courriels sortants.

Validation DMARC

DMARC (Domain-based Message Authentication, Reporting & Conformance) permet de définir le traitement d’un courriel entrant en fonction des résultats de la vérification SPF et de la validation DKIM ainsi que de l’alignement d’adresses et de domaines.

Une validation DMARC vérifie si un courriel entrant correspond à ce que sait le destinataire de l’expéditeur. Si un enregistrement DMARC a été défini dans la zone DNS du domaine de l’expéditeur, la validation DMARC suit la vérification SPF et la validation DKIM. La validation DMARC décide comment traiter le courriel en fonction des résultats de la vérification SPF et de la validation DKIM ainsi que de l’alignement d’adresses et de domaines dans l’Envelope-From et l’Header-From du courriel (alignement SPF) d’une part et des domaines dans l’Header-From et la signature DKIM

(alignement DKIM) d'autre part. Pour de plus amples informations sur la matrice de décision DMARC, voir Matrice de décision DMARC à la page 29.

Les administrateurs côté clients peuvent configurer la validation DMARC pour les courriels entrants de leurs domaines. Pour cela, les administrateurs doivent d'abord définir un enregistrement DMARC dans la zone DNS de leurs domaines, (voir Définir un enregistrement DMARC à la page 25 et Balises dans les enregistrements DMARC à la page 26), activer la validation DMARC (voir Activer la validation DMARC à la page 34) et enfin configurer les options avancées (voir Configurer les options étendues pour la validation DMARC à la page 35).

Définir un enregistrement DMARC

Un enregistrement DMARC est la condition préalable pour que les validations DMARC (voir Validation DMARC à la page 24) puissent être réalisées pour les courriels d'un domaine. Vous pouvez définir un enregistrement DMARC pour votre domaine.

1. Dans la zone DNS de votre domaine, créez un enregistrement TXT avec le nom suivant. Remplacez **<domaine.tld>** par votre domaine.
   _dmarc.<domaine.tld>

2. Définissez dans l'enregistrement TXT la directive DMARC selon le schéma suivant à titre d'exemple. Remplacez **<utilisateur@domaine.tld>** par une adresse courriel.
v=DMARC1;p=quarantine;pct=100;rua=mailto:<utilisateur@domaine.tld>

> **IMPORTANT :**
>
> Le chapitre Balises dans les enregistrements DMARC à la page 26 contient une prévisualisation et des explications des balises qui peuvent être utilisées dans les enregistrements DMARC.

> **REMARQUE :**
>
> Les informations issues de l'enregistrement DMARC s'appliquent aux courriels expédiés aux destinataires en dehors du domaine. Les paramètres pour les courriels envoyés à des destinataires au sein du domaine peuvent être configurés dans le module **Email Authentication**.

Un enregistrement DMARC a été défini dans la zone DNS.

Balises dans les enregistrements DMARC

Les enregistrements DMARC se composent de balises. Les balises d'un enregistrement DMARC contiennent des exigences pour les validations DMARC de courriels expédiés par le domaine à un destinataire en dehors du domaine.

Le tableau suivant contient une prévisualisation et des explications des balises qui peuvent être utilisées dans les enregistrements DMARC. À l'exception de **v** et **p**, toutes les balises sont facultatives.

> **IMPORTANT :**
>
> Les balises **v** et **p** sont obligatoires.

BALISE	EXPLICATION	VALEURS POSSIBLES
v	Cette balise définit la version de protocole DMARC utilisée.	**v=DMARC1** **REMARQUE :** Pour cette balise, seul **v=DMARC1** est possible.
p	Cette balise définit de quelle manière comment traiter un courriel provenant du domaine si la validation DMARC échoue pour le courriel.	**p=quarantine** : le courriel est mis en quarantaine. **p=reject** : le courriel est refusé. **p=none** : aucune mesure n'est prise pour le courriel. **REMARQUE :** Nous recommandons **p=quarantine**.
pct	Cette balise définit le pourcentage des courriels soumis à des validations DMARC. Des chiffres compris entre 1 et 100 sont possibles pour cette balise.	**pct=100** **REMARQUE :** Nous recommandons **pct=100**, afin que les validations DMARC soient réalisées pour tous les courriels du domaine.

BALISE	EXPLICATION	VALEURS POSSIBLES
rua	Cette balise définit à quelle adresse courriel sont envoyés quotidiennement des rapports combinés sur les validations DMARC qui ont échoué.	**rua=mailto:<utilisateur@domaine.com>** Plutôt que **<utilisateur@domaine.com>**, l'adresse courriel à laquelle les rapports combinés doivent être envoyés est saisie.
ruf	Cette balise définit à quelle adresse courriel les rapports forensiques sont envoyés pour les courriels individuels pour lesquels la validation DMARC a échoué.	**ruf=mailto:<utilisateur@domaine.com>** Plutôt que **<utilisateur@domaine.com>**, l'adresse courriel à laquelle les rapports forensiques combinés doivent être envoyés est saisie.
sp	Cette balise définit comment traiter un courriel provenant d'un sous-domaine du domaine si la validation DMARC échoue pour le courriel.	**sp=quarantine** : le courriel est mis en quarantaine. **sp=reject** : le courriel est refusé. **sp=none** : aucune mesure n'est prise pour le courriel.
adkim	Cette balise définit le mode de calibrage pour les signatures DKIM (voir Validation DKIM et signature DKIM à la page 19). Le mode de calibrage détermine dans quelle mesure un courriel doit correspondre à la signature DKIM pour que le courriel soit accepté.	**adkim=r** : le mode de calibrage est souple. Une concordance partielle suffit. **adkim=s** : le mode de calibrage est strict. Une concordance complète est requise.

BALISE	EXPLICATION	VALEURS POSSIBLES
aspf	Cette balise définit le mode de calibrage pour les domaines de l'en-tête De et de l'envelope De d'un courriel (voir Vérification SPF à la page 6). Le mode de calibrage détermine avec quelle précision les deux domaines doivent correspondre pour que le courriel soit accepté.	**aspf=r** : le mode de calibrage est souple. Une concordance partielle suffit. **aspf=s** : le mode de calibrage est strict. Une concordance complète est requise.

Matrice de décision DMARC

La matrice de décision DMARC indique la conduite à tenir avec les courriels entrants après la réussite ou l'échec des vérifications SPF et des validations DKIM.

Tableau 4 : Matrice de décision DMARC

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Réussi	Réussi	Réussi	Réussi	Réussi	Envoyer
Réussi	Réussi	Réussi	Échec	Réussi	Envoyer
Réussi	Réussi	Échec	Réussi	Réussi	Envoyer

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Réussi	Réussi	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur
Réussi	Échec	Réussi	Réussi	Réussi	Envoyer
Réussi	Échec	Réussi	Échec	Réussi	Envoyer
Réussi	Échec	Échec	Réussi	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Réussi	Échec	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur
Échec	Réussi	Réussi	Réussi	Réussi	Envoyer
Échec	Réussi	Réussi	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur
Échec	Réussi	Échec	Réussi	Réussi	Envoyer

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Échec	Réussi	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur
Échec	Échec	Réussi	Réussi	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur
Échec	Échec	Réussi	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur

VÉRIFICATION SPF	VALIDATION DKIM	ALIGNEMENT SPF	ALIGNEMENT DKIM	RÉSULTAT DMARC	CONSÉQUENCES
Échec	Échec	Échec	Réussi	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur
Échec	Échec	Échec	Échec	Échec	Possibilité de mettre en quarantaine comme spam, de refuser ou de traiter selon la directive DMARC de l’expéditeur

Le résultat DMARC n’est positif que si la vérification SPF (voir Vérification SPF à la page 6) ou la validation DKIM (voir Validation DKIM et signature DKIM à la page 19) ainsi que l’alignement correspondant (SPF ou DKIM) ont réussi. Le courriel est transmis lorsque le résultat DMARC est positif. Autrement, en fonction des réglages dans le module **Email Authentication** (voir Configurer les options étendues pour la validation DMARC à la page 35) (le cas échéant), le courriel est mis en quarantaine comme spam, refusé, ou traité dans le Control Panel selon la directive DMARC du domaine de l’expéditeur.

Activer la validation DMARC

Vous avez défini des enregistrements SPF, DKIM et DMARC valides pour au moins l'un de vos domaines (voir Définir un enregistrement SPF à la page 9, Définir un enregistrement CNAME à la page 19 et Définir un enregistrement DMARC à la page 25). Vous avez activé la Spam and Malware Protection pour votre domaine (voir « Activer la Spam and Malware Protection » dans le manuel du Control Panel).

Vous pouvez activer la validation DMARC pour définir le traitement des courriels entrants en fonction des résultats des vérifications SPF (voir Vérification SPF à la page 6) et des validations DKIM (voir Validation DKIM et signature DKIM à la page 19).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. **IMPORTANT :**

   La validation DMARC peut être activée uniquement pour vos domaines avec des enregistrements SPF, DKIM et DMARC valides.

   Cochez la case **Activer la validation DMARC pour les courriels entrants** sous **Authentification d'expéditeur**.

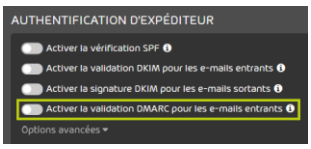

Illustration 15 : Activer la validation DMARC

La validation DMARC est activée pour les courriels entrants.

REMARQUE :

Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

La validation DMARC a été activée pour les courriels entrants.

Vous pouvez ensuite configurer les options étendues en vue de la validation DMARC (voir Configurer les options étendues pour la validation DMARC à la page 35).

Configurer les options étendues pour la validation DMARC

Vous avez activé la validation DMARC (voir Activer la validation DMARC à la page 34).

Dans le module **Paramètres de sécurité** > **Email Authentication**, vous pouvez configurer la façon de traiter les résultats des validations DMARC (voir Validation DMARC à la page 24).

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Cliquez sur **Options avancées**.

Illustration 16 : Ouvrir les options étendues

Un message d’avertissement apparaît.

5.

IMPORTANT :

Les modifications apportées aux options étendues peuvent entraîner la distribution de courriels malveillants.

Pour modifier les options étendues, cliquez sur **Confirmer**.

Illustration 17 : Confirmer

6. Facultatif : Sous **Paramètres DMARC avancés**, indiquez le traitement à appliquer après un échec DMARC. Vous avez les options suivantes :

   - **Enregistrer le courriel comme spam en quarantaine** : Le courriel est classé comme courriel indésirable et mis en quarantaine.
   - **Rejeter le courriel** : Le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
   - **Appliquer la stratégie du domaine de l'expéditeur** : Après un échec DMARC, le comportement défini dans la directive DMARC du domaine expéditeur est appliqué. Il s'agit des paramètres par défaut.

   > **REMARQUE :**
   >
   > Si vous sélectionnez cette option, vous faites confiance aux politiques DMARC de tiers.

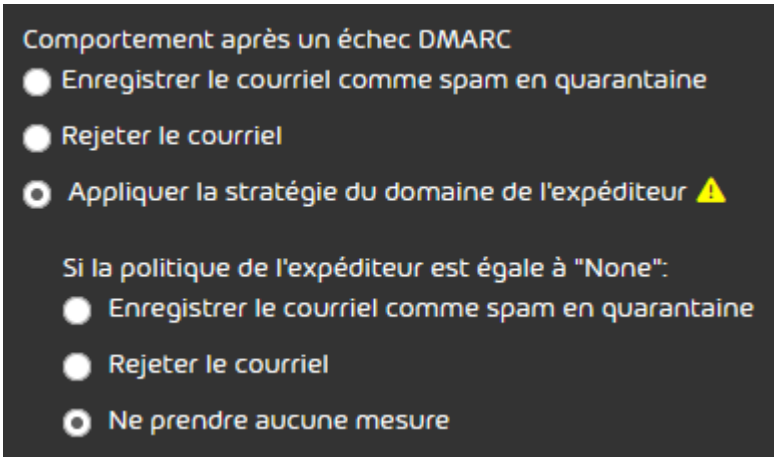

Illustration 18 : Choisir le comportement après un échec DMARC

Si l'option **Appliquer la stratégie du domaine de l'expéditeur** a été sélectionnée, d'autres paramètres s'affichent.

7. Si vous avez sélectionné l'option **Appliquer la stratégie du domaine de l'expéditeur**, passez à **Si la politique de l'expéditeur est égale à "None":** pour spécifier le comportement à

appliquer si la politique DMARC du domaine expéditeur est définie sur « None ». Vous avez les options suivantes :

- **Enregistrer le courriel comme spam en quarantaine** : Le courriel est classé comme courriel indésirable et mis en quarantaine.
- **Rejeter le courriel** : Le courriel est refusé. Le courriel n'est pas remis au destinataire et n'est pas mis en quarantaine.
- **Ne prendre aucune mesure** : L'échec DMARC ne déclenche aucune action. Le courriel est ensuite vérifié par d'autres filtres de nos services.

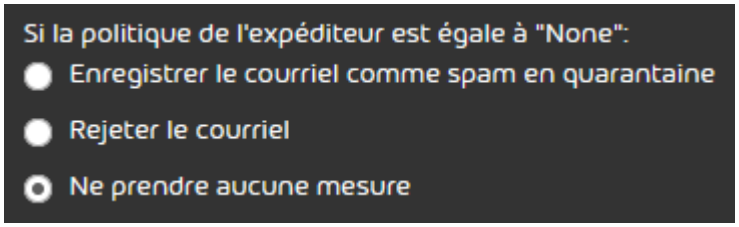

Illustration 19 : Comportement pour les directives d’ expéditeur avec le paramètre « None »

8. Facultatif : Pour réinitialiser les paramètres DMARC aux réglages par défaut, cliquez sur **Paramètres par défaut pour la validation DMARC**.

> **REMARQUE :**
>
> Avec les paramètres par défaut, les courriels sont traités selon un DMARC-Fail conformément à la directive DMARC de l'expéditeur. Si la valeur **None** est entrée pour la directive DMARC de l'expéditeur (voir Définir un enregistrement DMARC à la page 25), aucune action ne sera effectuée par défaut.

Les modifications sont enregistrées.

> **REMARQUE :**
>
> Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Les options avancées pour la validation du DMARC ont été configurées.

Ajouter des exceptions

Vous avez activé des procédures d'authentification des expéditeurs dans le module **Email Authentication** (voir Procédures d’ authentification des expéditeurs à la page 6).

Si vous avez activé la vérification SPF (voir Vérification SPF à la page 6), la validation DKIM (voir Validation DKIM et signature DKIM à la page 19) et/ou la validation DMARC (voir Validation DMARC à la page 24) et si vous souhaitez les désactiver pour l'un de vos domaines, ajoutez une exception.

1. Connectez-vous avec vos identifiants administratifs dans le Control Panel.
2. Sélectionnez votre domaine dans la sélection de l'espace.
3. Naviguez vers **Paramètres de sécurité** > **Email Authentication**.
4. Dans **Exceptions**, cliquez sur **Ajouter exception**.

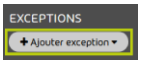

Illustration 20 : Ajouter une exception

Un affichage étendu s'ouvre.

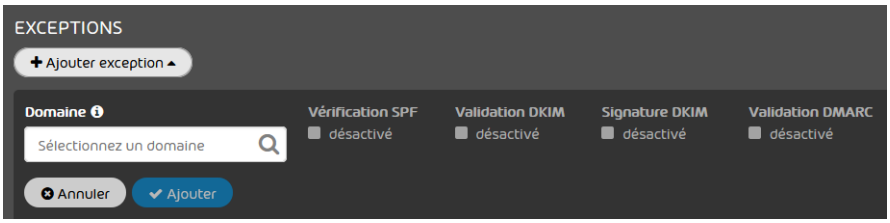

Illustration 21 : Vue élargie

5. Sous **Domaine**, sélectionnez un domaine pour lequel vous souhaitez activer l'exception.

> **REMARQUE :**
>
> Vous pouvez sélectionner uniquement les domaines pour lesquels la Spam and Malware Protection est activée.

6. Cochez la case sous la vérification que vous souhaitez désactiver pour le domaine.

> **REMARQUE :**
>
> Vous pouvez désactiver pour un domaine la vérification SPF, la validation DKIM ou la validation DMARC, uniquement si le domaine dispose des paramètres DNS valides correspondants. Les vérifications ne s'appliquent pas à tous les autres domaines.

7. Cliquez sur **Ajouter**.

L'exception est ajoutée et apparaît dans le tableau ci-dessous.

> **REMARQUE :**
>
> Il peut s'écouler jusqu'à 72 heures avant que les modifications ne deviennent valides dans la zone DNS.

Une exception a été ajoutée à Email Authentication.

Raisons de catégorisation d’ Email Authentication

Pour les courriels pour lesquels l'authentification de l'expéditeur avec Email Authentication a engendré une erreur, certaines raisons de catégorisation sont utilisées dans le Control Panel. Pour des informations sur d'autres raisons de catégorisation, voir le chapitre « Raisons de catégorisation » dans le mode d'emploi du Control Panel.

SPF

Les courriels pour lesquels une vérification SPF a montré qu'ils n'avaient pas été envoyés par un serveur enregistré dans le DNS sont mis en quarantaine comme indésirables, refusés ou distribués en fonction de vos paramètres (voir Configurer les options étendues pour la vérification SPF à la page 14).

Dans le Control Panel, ces courriels sont affichés dans le module **Email Live Tracking**, quelle que soit la mesure exécutée, avec le motif **Envelope SPF Failure** et **Message Header SPF Failure**.

DKIM

Les courriels pour lesquels la validation DKIM a échoué sont mis en quarantaine comme indésirables ou refusés, en fonction de vos paramètres (voir Configurer les options étendues pour la validation DMARC à la page 35).

Dans le Control Panel, ces courriels sont affichés dans le module **Email Live Tracking** avec le motif **DKIM Failure**.

DMARC

Les courriels pour lesquels une validation DMARC a montré qu'ils ne correspondaient pas aux règles saisies pour SPF et/ou DKIM, sont mis en quarantaine comme indésirables ou refusés, en fonction de vos paramètres (voir Configurer les options étendues pour la validation DMARC à la page 35).

Dans le Control Panel, ces courriels sont affichés dans le module **Email Live Tracking** avec le motif **DMARC Failure**.

Index

A

C

D

E

F

P

R

S

V

U.S. SALES 1.800.734.9905

INTERNATIONAL SALES +1.206.613.0895

www.watchguard.com | pandasecurity.com