Configuration de la journalisation des événements sur un point d'accès sans fil

Objectif

Les événements système sont des activités qui peuvent nécessiter une attention particulière et une action nécessaire pour exécuter le système en douceur et éviter les pannes. Ces événements sont enregistrés sous forme de journaux. Les journaux système permettent à l'administrateur d'effectuer le suivi d'événements particuliers qui se produisent sur le périphérique.

Les journaux d’événements sont utiles pour le dépannage du réseau, le débogage du flux de paquets et la surveillance des événements. Ces journaux peuvent être enregistrés sur la mémoire vive (RAM), la mémoire vive non volatile (NVRAM) et sur des serveurs de journaux distants. Ces événements sont généralement effacés du système au redémarrage. Si le système redémarre de manière inattendue, les événements système ne peuvent pas être affichés, sauf s'ils sont enregistrés dans la mémoire non volatile. Si la fonction de journalisation de persistance est activée, les messages d'événements système sont écrits dans la mémoire non volatile.

Les paramètres de journalisation définissent les règles de journalisation et les destinations de sortie pour les messages, les notifications et d'autres informations à mesure que divers événements sont enregistrés sur le réseau. Cette fonction avertit le personnel responsable afin que l'action nécessaire soit entreprise lorsqu'un événement se produit. Les journaux peuvent également leur être envoyés par e-mail d'alerte.

Ce document a pour but de vous expliquer et de vous guider à travers les différentes configurations pour recevoir les journaux système et d'événements.

Périphériques pertinents

- Série WAP100
- Série WAP300
- Série WAP500

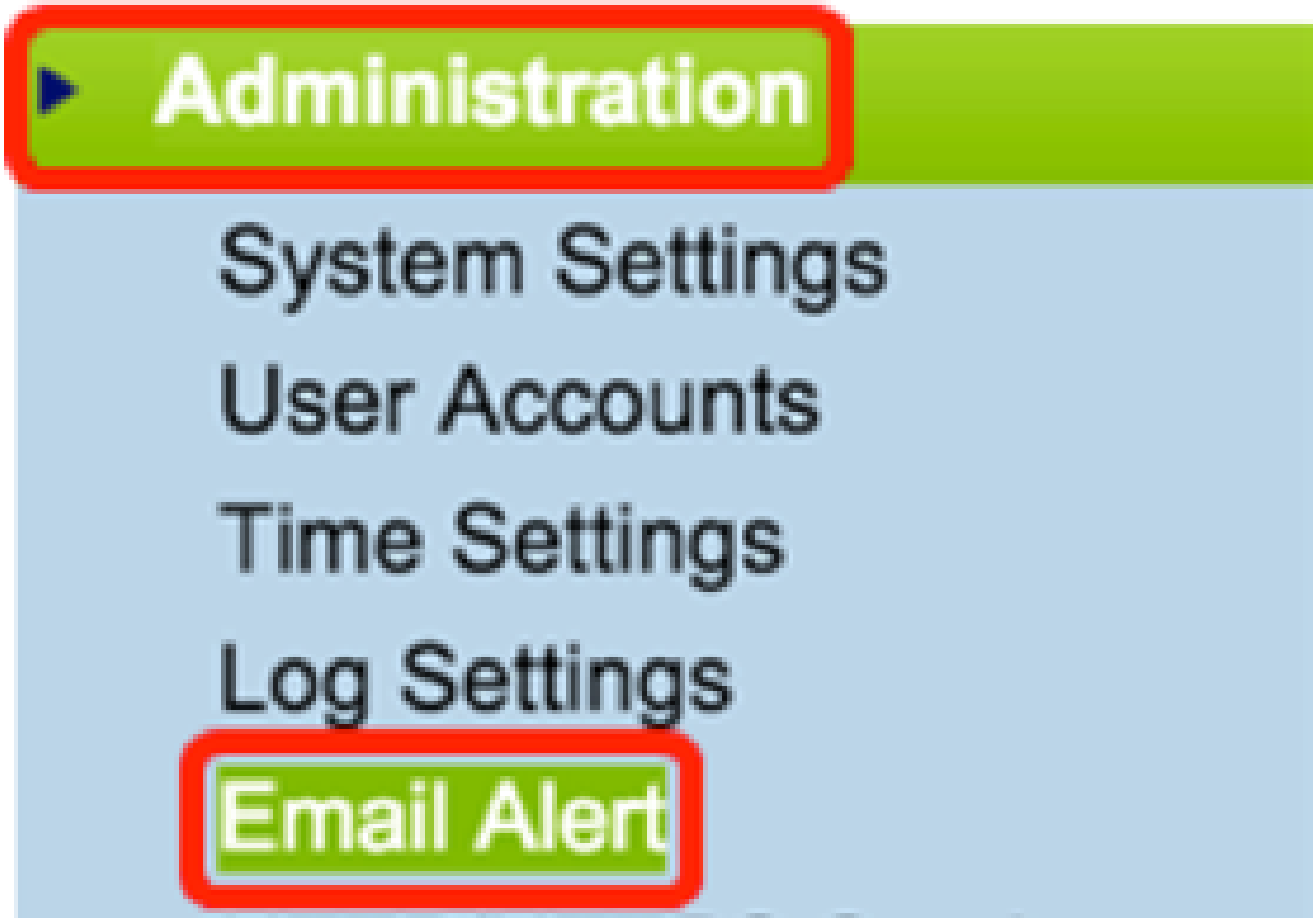
Version du logiciel

- 1.0.1.4 : WAP131, WAP351
- 1.0.6.2 : WAP121, WAP321
- 1.2.1.3 : WAP371, WAP551, WAP561
- 1.0.1.2 : WAP150, WAP361
- 1.0.0.17 - WAP571, WAP571E

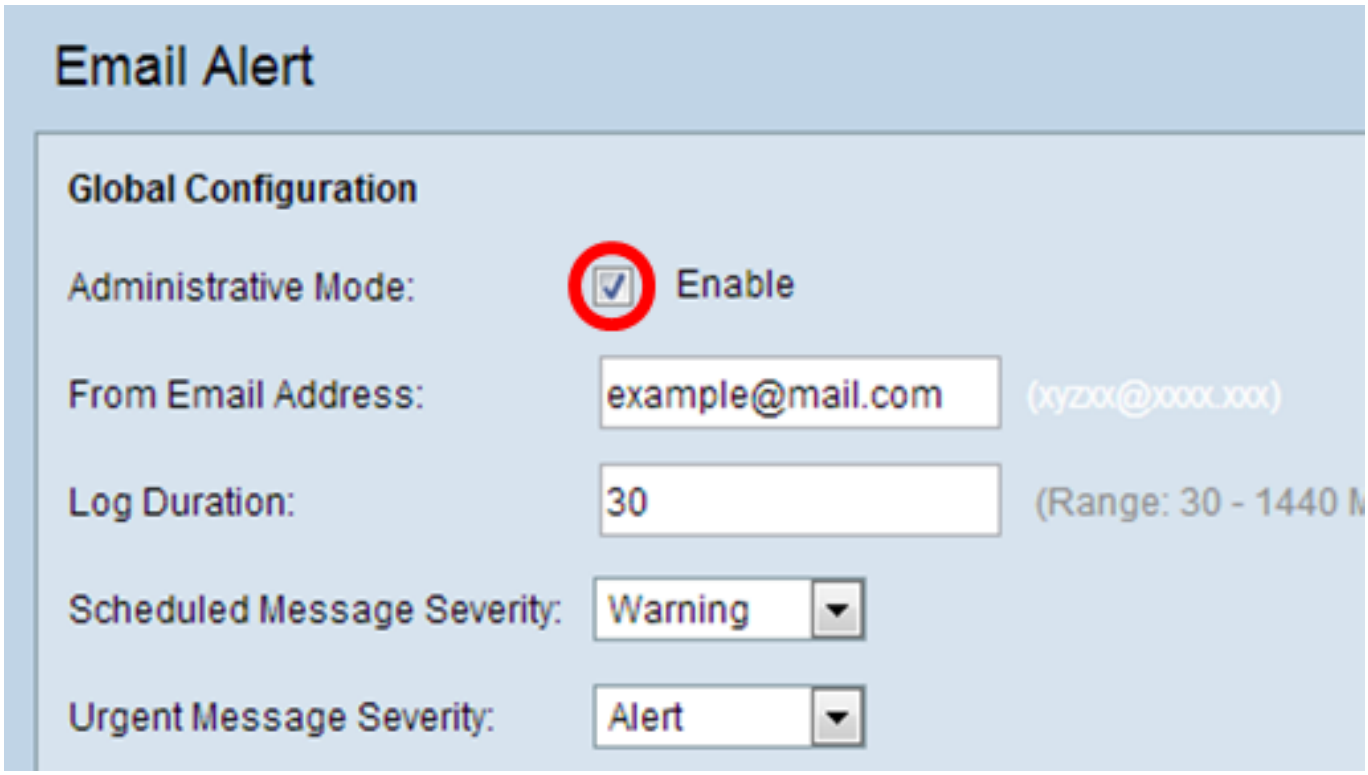
Configurer la consignation des événements

Configurer l'alerte par courrier électronique

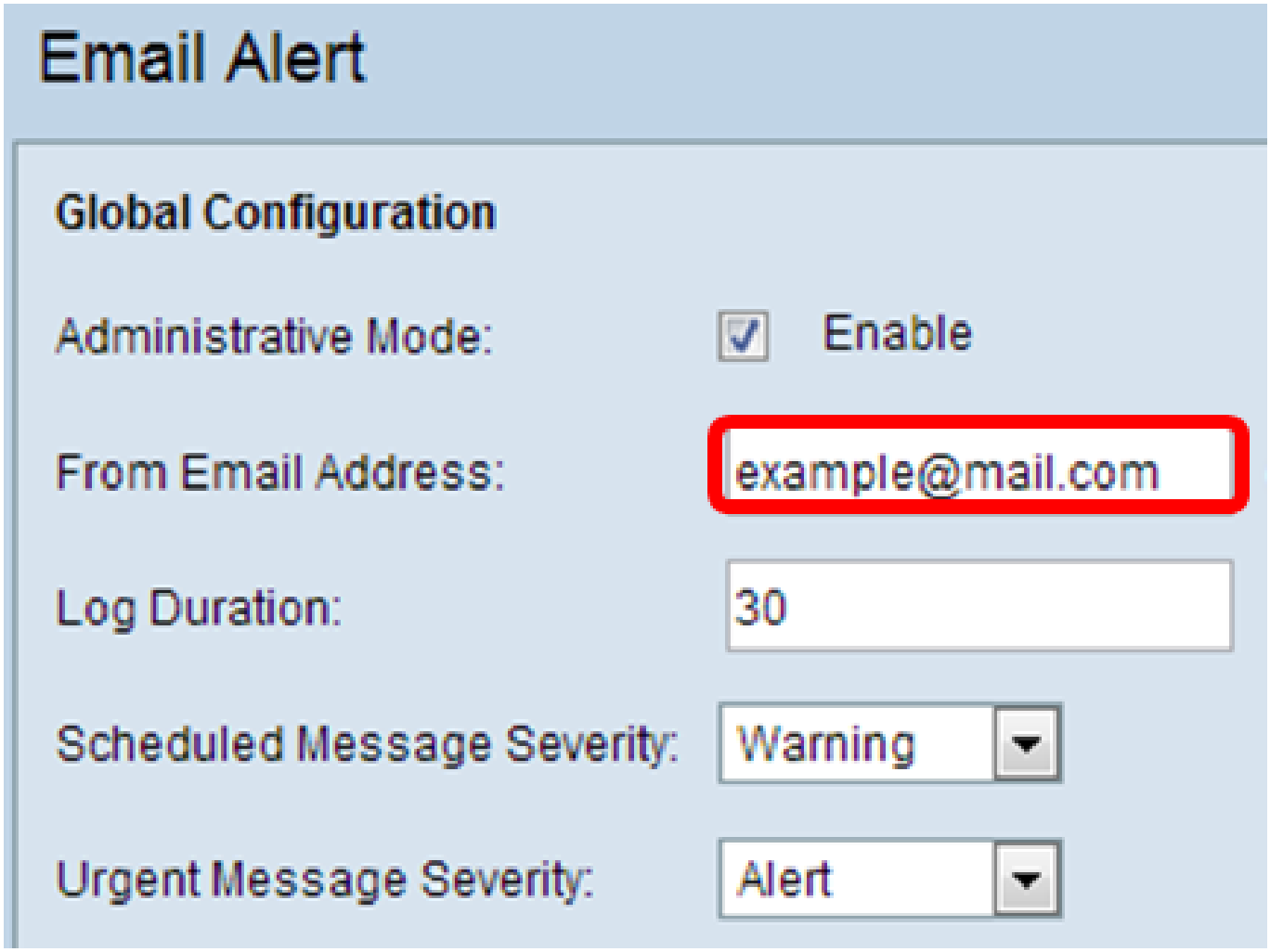
Étape 1. Connectez-vous à l'utilitaire Web et choisissez Administration > Email Alert.



Étape 2. Cochez Enable dans la case Administrative Mode pour activer globalement la fonctionnalité d'alerte par e-mail.

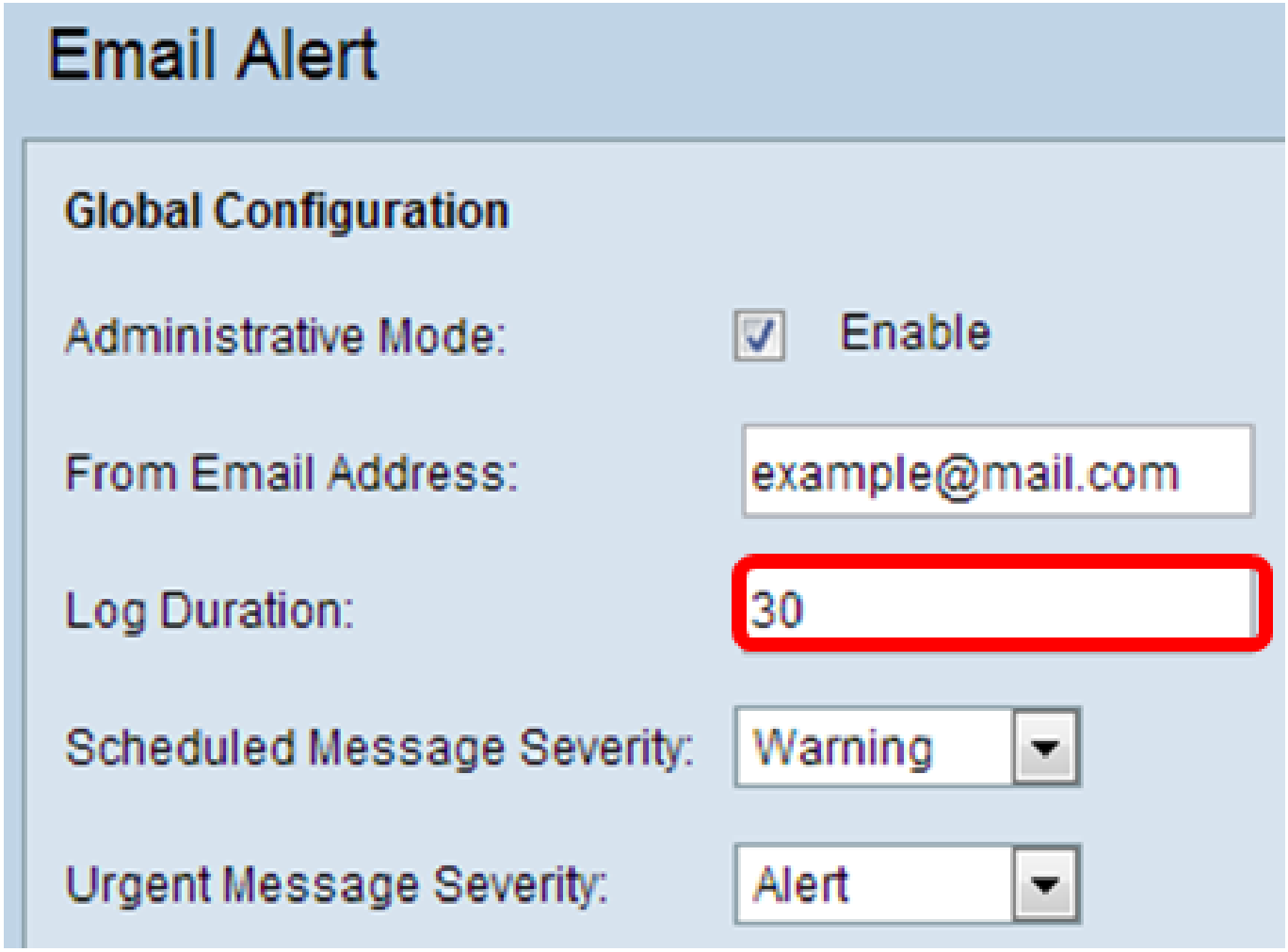


Étape 3. Saisissez une adresse e-mail dans le champ From Email Address. L'adresse s'affiche en tant qu'expéditeur de l'alerte par e-mail. La valeur par défaut est Null.



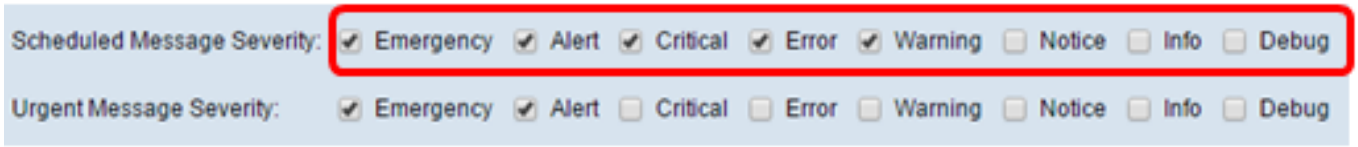
Remarque : il est vivement recommandé d'utiliser un compte de messagerie distinct au lieu d'utiliser votre messagerie personnelle pour préserver la confidentialité.

Étape 4. Dans le champ Log Duration, saisissez l'heure (en minutes) à laquelle les alertes par e-mail doivent être envoyées à l'adresse e-mail configurée. La plage est comprise entre 30 et 1 440 minutes et la valeur par défaut est 30.

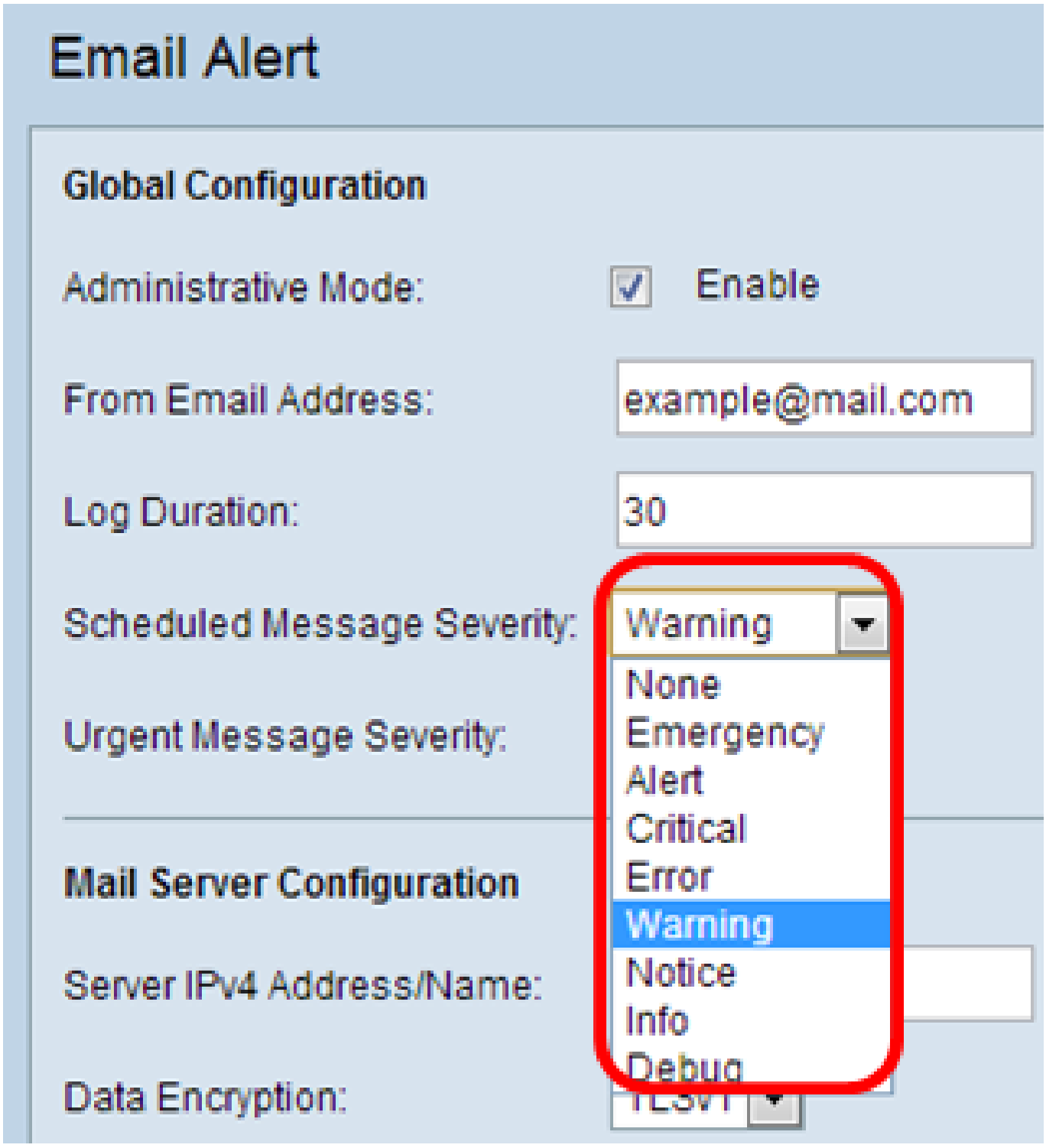


Étape 5. Pour définir la gravité du message planifié, choisissez le type de message approprié à envoyer, par exemple Urgence, Alerte, Critique, Erreur, Avertissement, Avis, Info ou Débogage. Ces messages sont envoyés chaque fois que la durée du journal expire. Ces options s'affichent différemment dans l'utilitaire Web en fonction du modèle du périphérique que vous utilisez.

Pour les protocoles WAP131, WAP150, WAP351 et WAP361, cochez le type de message approprié dans les cases Sévérité des messages planifiés.



Pour WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 et WAP571E, cliquez sur le type de message approprié dans la liste déroulante Gravité planifiée du message.

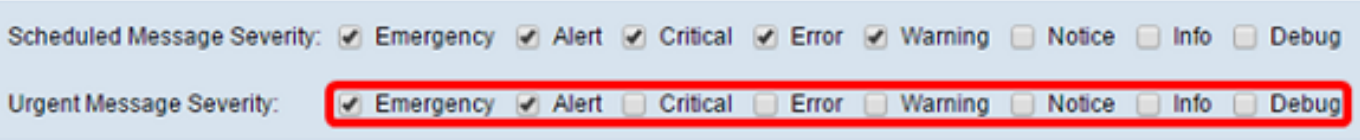


- None : aucun message n'est envoyé.
- Urgence : ce type de message est envoyé à l'utilisateur lorsque le périphérique se trouve dans une situation critique et qu'une attention immédiate est requise.
- Alert : ce type de message est envoyé à l'utilisateur lorsqu'une action différente de la configuration normale se produit.

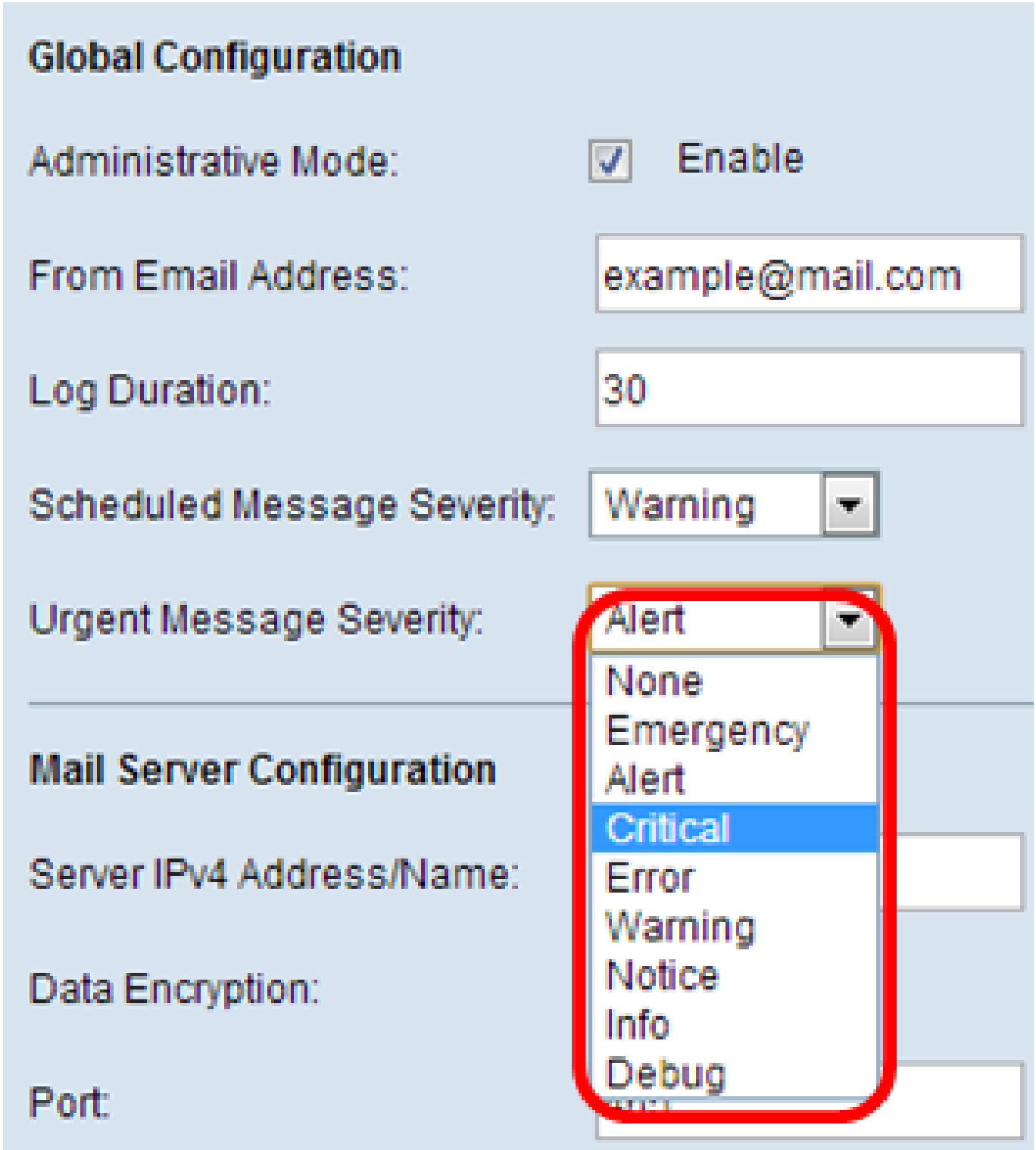
- Critique : ce type de message est envoyé à l'utilisateur lorsqu'un port est en panne ou que l'utilisateur ne peut pas accéder au réseau. Une action immédiate est requise.
- Erreur : ce type de message est envoyé à l'utilisateur en cas d'erreur de configuration.
- Avertissement : ce type de message est envoyé à l'utilisateur lorsqu'un autre utilisateur tente d'accéder aux zones d'accès restreint.
- Notice : ce type de message est envoyé à l'utilisateur en cas de modifications de faible priorité sur le réseau.
- Info : ce type de message est envoyé à l'utilisateur pour décrire le comportement du réseau.
- Debug : ce type de message est envoyé à l'utilisateur avec les journaux du trafic réseau.

Étape 6. Pour définir la gravité du message urgent, choisissez le type de message urgent à envoyer, par exemple Urgence, Alerte, Critique, Erreur, Avertissement, Avis, Info ou Débogage. Ces messages sont envoyés immédiatement. Ces options s'affichent différemment dans l'utilitaire Web en fonction du modèle du périphérique que vous utilisez.

Pour WAP131, WAP150, WAP351 et WAP361, cochez le type de message urgent approprié dans les cases Gravité des messages urgents.



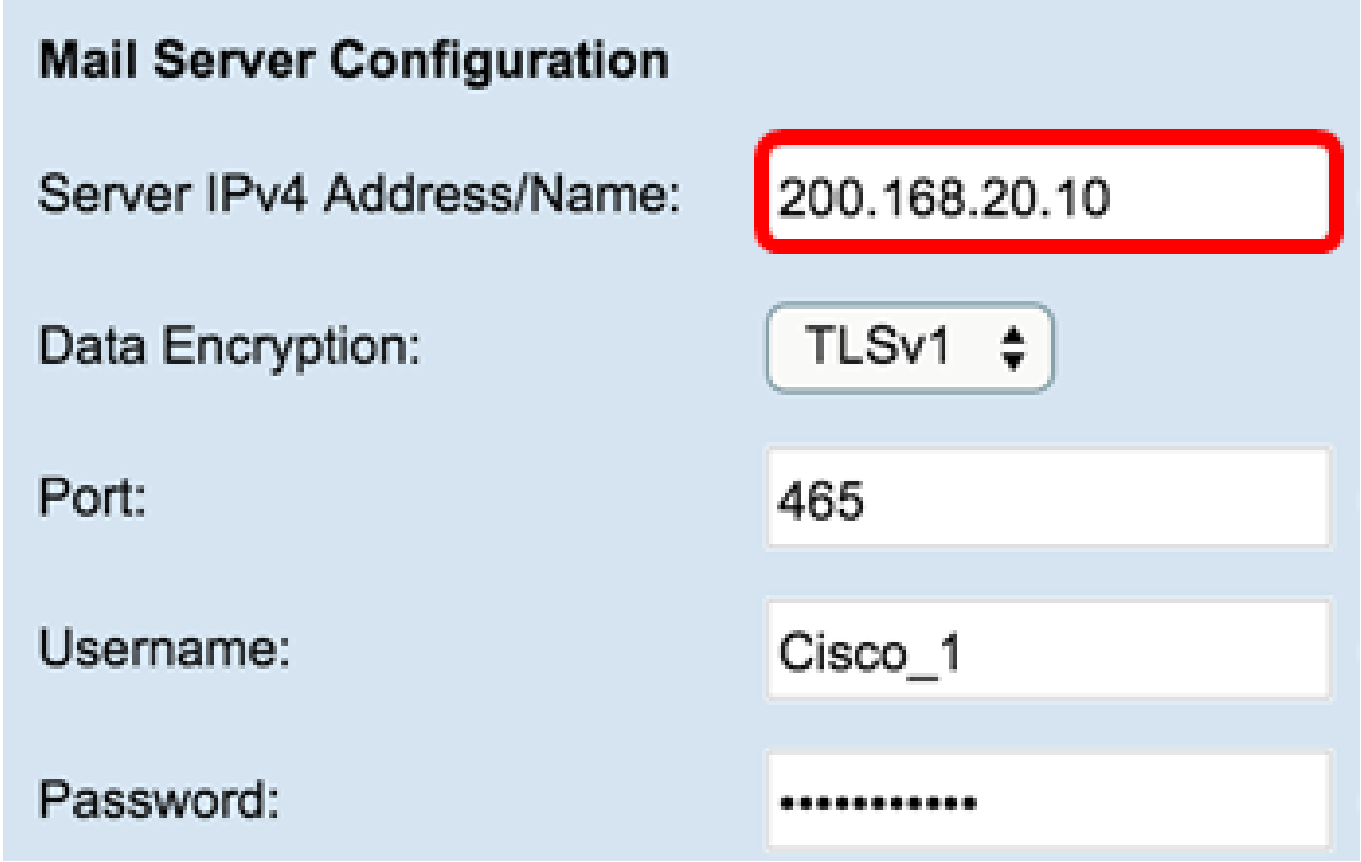
Pour WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 et WAP571E, cliquez sur le type de message urgent approprié dans la liste déroulante Gravité des messages urgents.



Remarque : si l'option est définie sur Aucun, aucun message n'est envoyé.

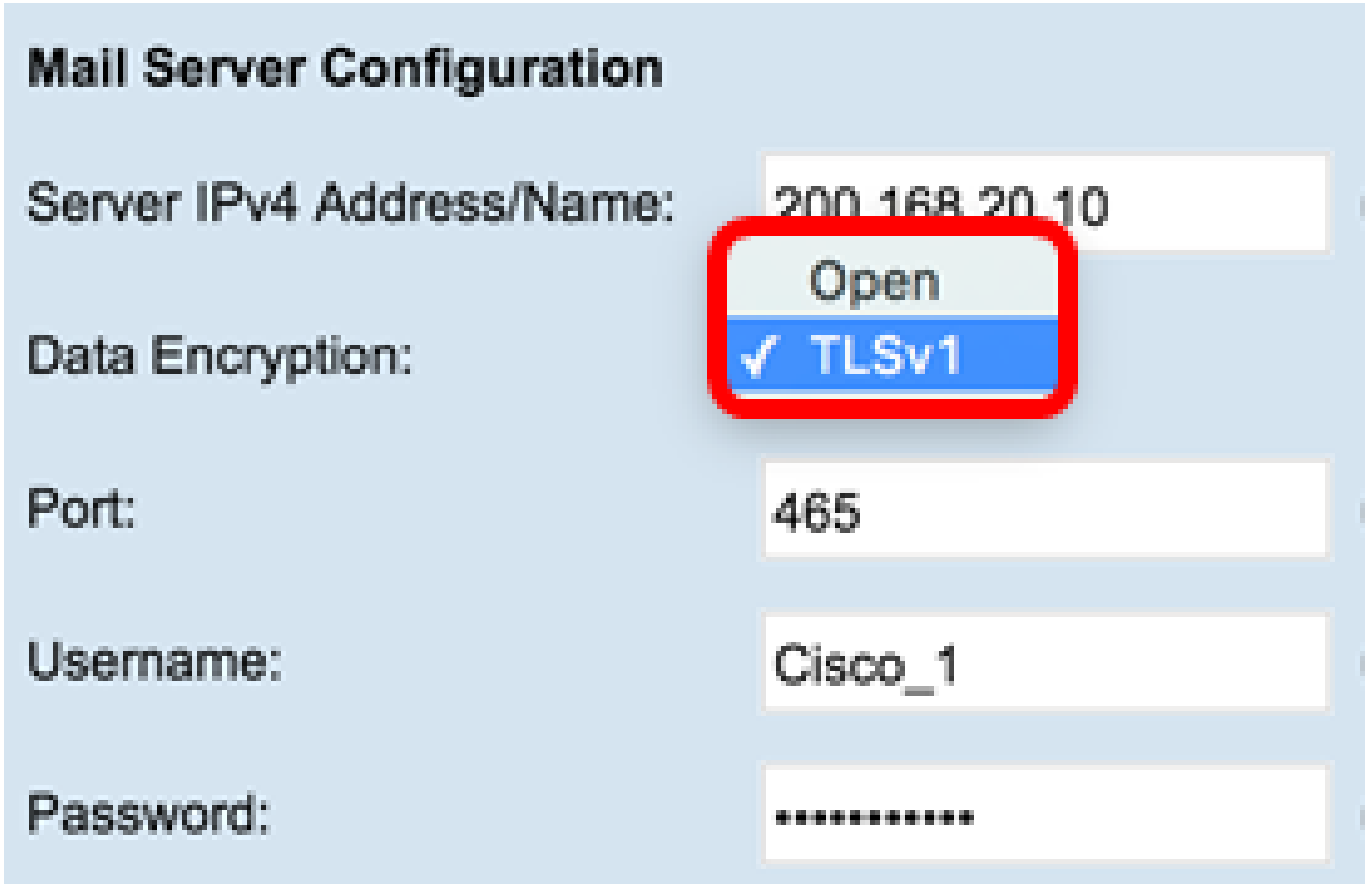
Étape 7. Saisissez le nom d'hôte valide du serveur de messagerie ou l'adresse IP dans le champ Server IPv4 Address/Name.

Remarque : dans l'exemple ci-dessous, 200.168.20.10 est utilisé.



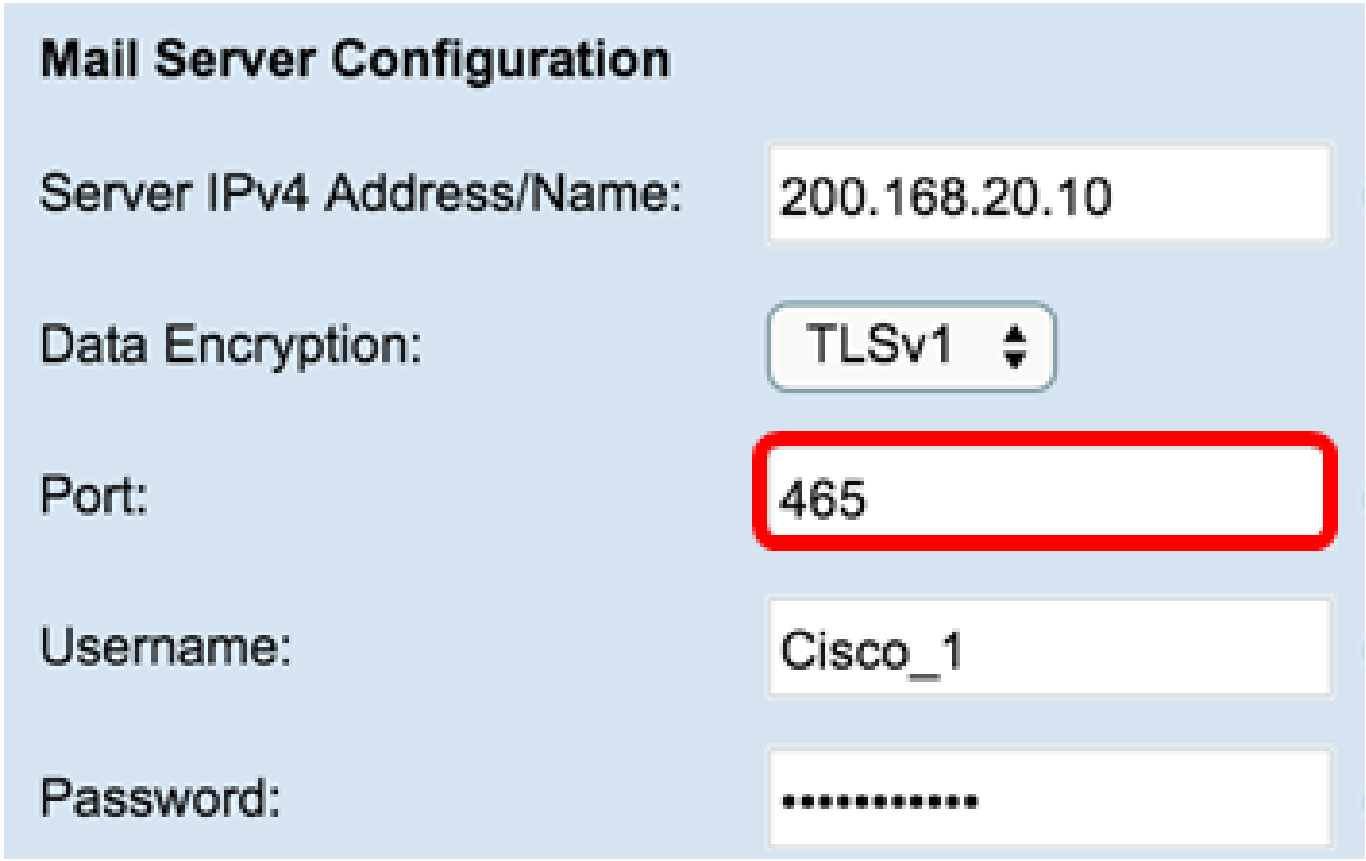
Étape 8. Sélectionnez le mode de sécurité dans la liste déroulante Cryptage des données. Les options disponibles sont les suivantes :

- TLSv1 - Transport Layer Security version 1 est un protocole cryptographique qui assure la sécurité et l'intégrité des données pour les communications sur Internet.
- Open : il s'agit du protocole de cryptage par défaut, mais il ne comporte aucune mesure de sécurité pour le cryptage des données.

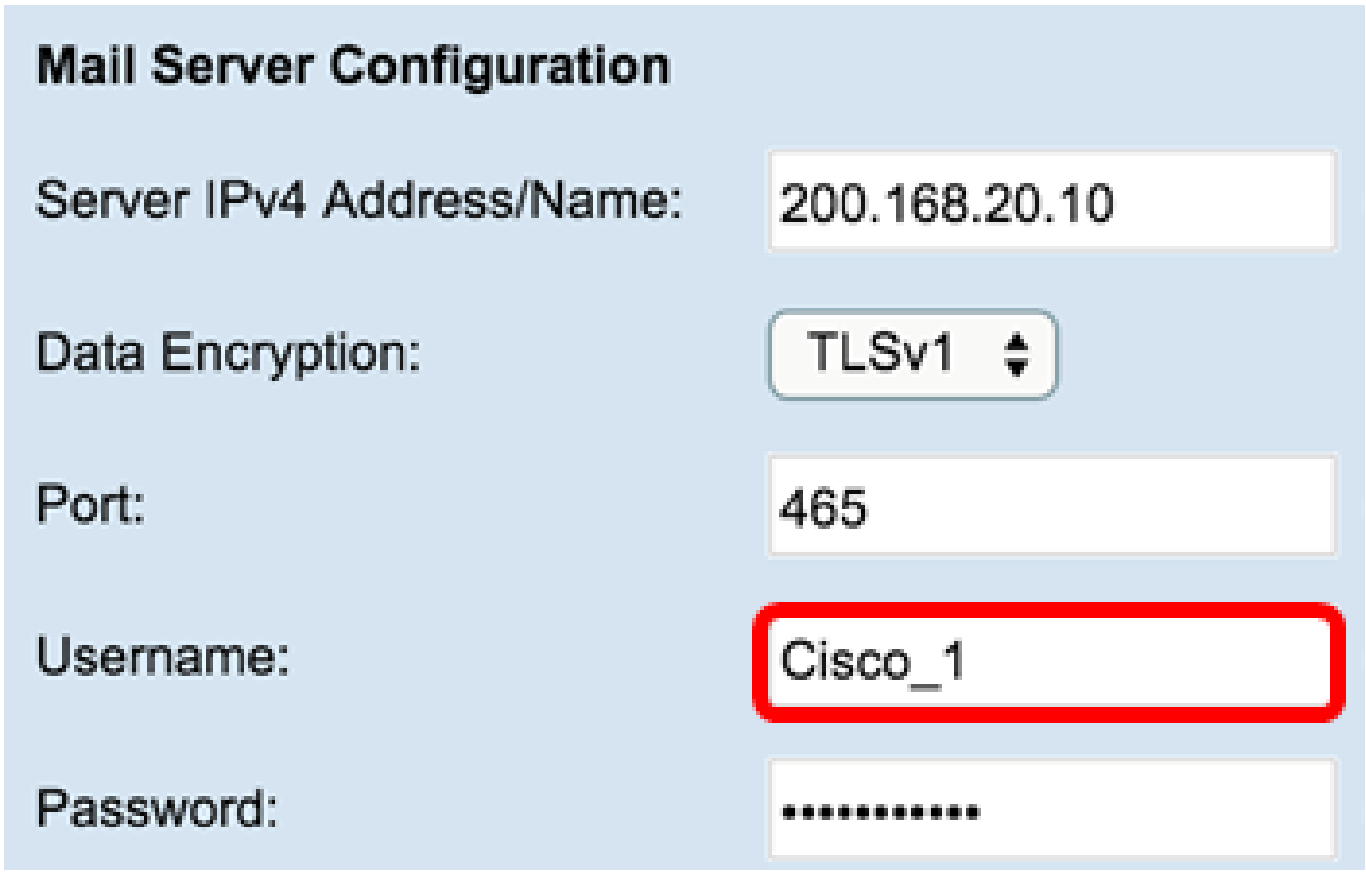


Remarque : dans cet exemple, TLSv1 est sélectionné. Si vous avez sélectionné Ouvrir, passez à l'étape 12.

Étape 9. Saisissez le numéro de port du serveur de messagerie dans le champ Port. Il s'agit d'un numéro de port sortant utilisé pour envoyer des e-mails. La plage de numéros de port valide est comprise entre 0 et 65535 et la valeur par défaut est 465 pour le protocole SMTP (Simple Mail Transfer Protocol).

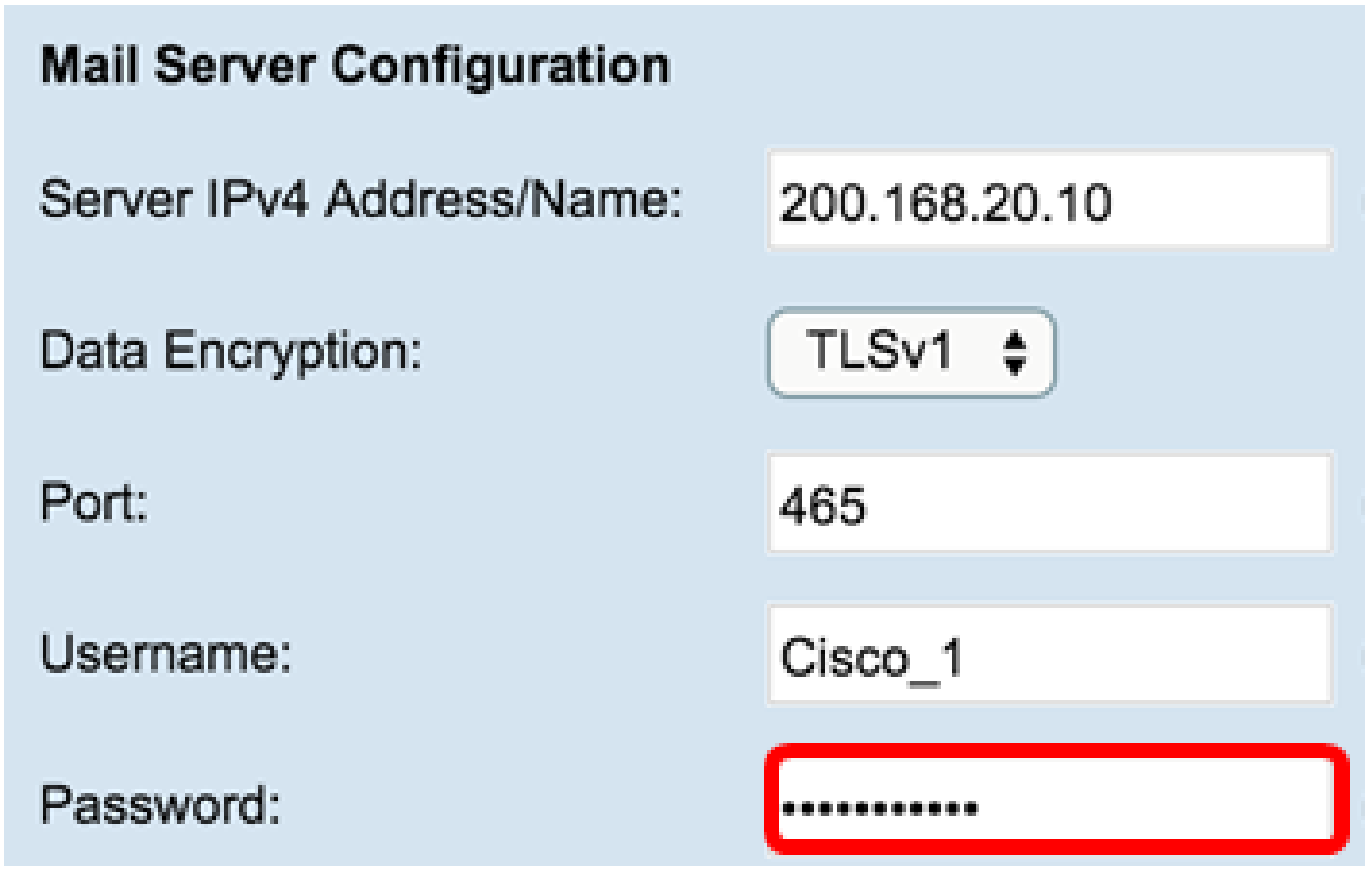


Étape 10. Saisissez le nom d'utilisateur pour l'authentification dans le champ Username.



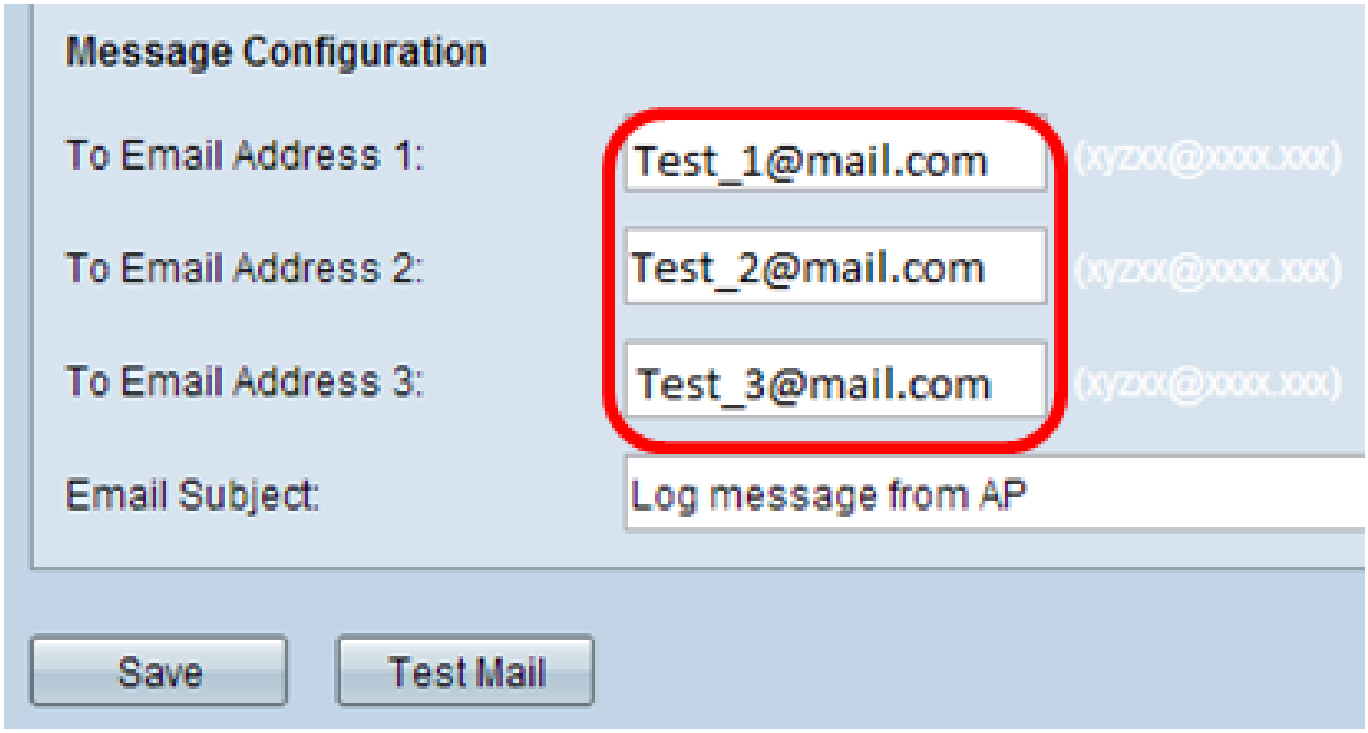
Remarque : Cisco_1 est utilisé à titre d'exemple.

Étape 11. Saisissez le mot de passe d'authentification dans le champ Password.

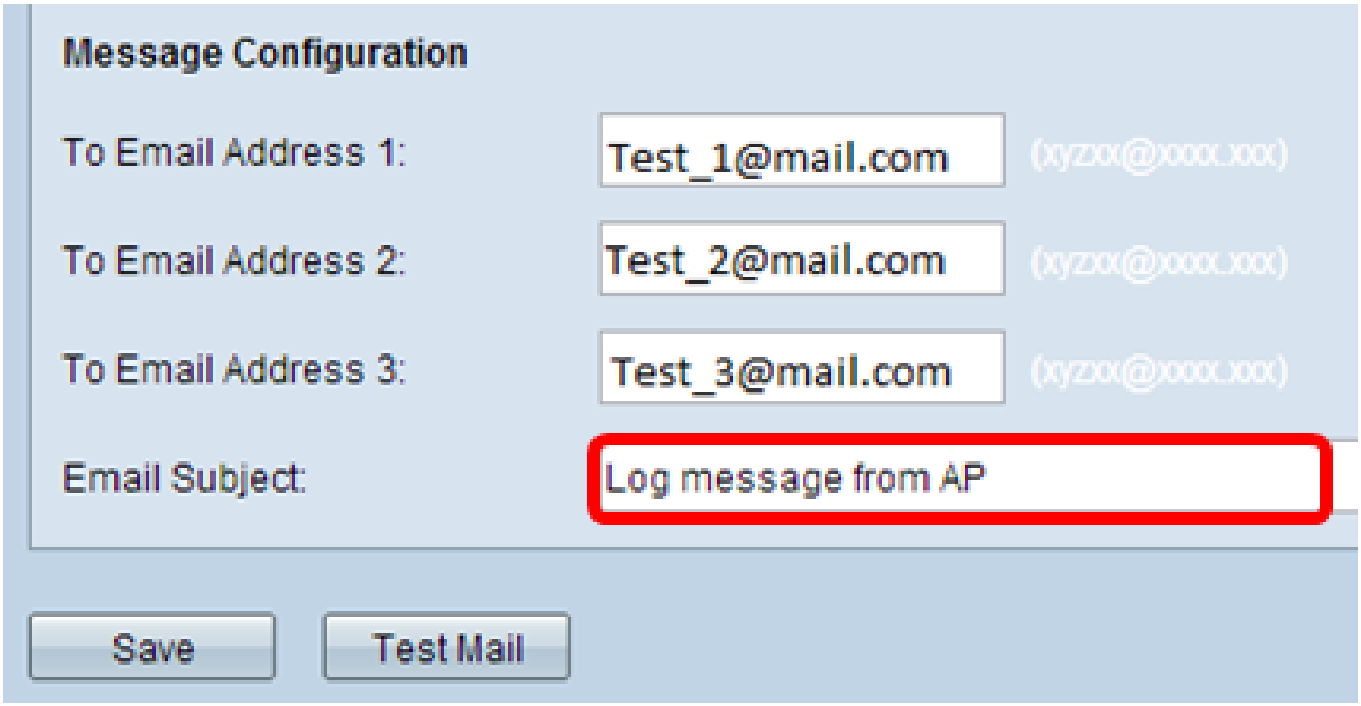


Étape 12. Sous Message Configuration, saisissez l'adresse e-mail requise dans les champs To Email Address 1, 2 et 3.

Remarque : en fonction des besoins, vous pouvez soit saisir des valeurs dans tous les champs Adresse e-mail de destination, soit saisir une seule adresse e-mail et laisser le reste vide.

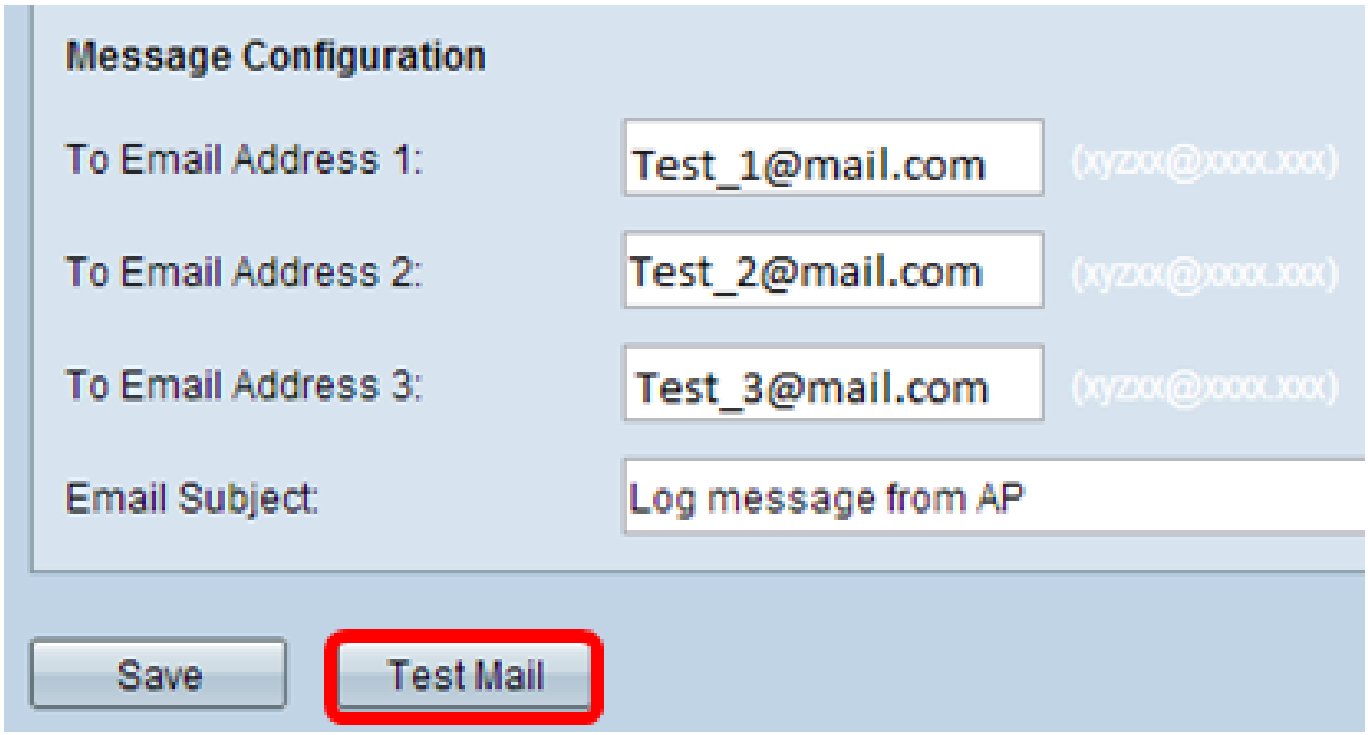


Étape 13. Saisissez l'objet de l'e-mail dans le champ Objet de l'e-mail. L'objet peut contenir jusqu'à 255 caractères alphanumériques.

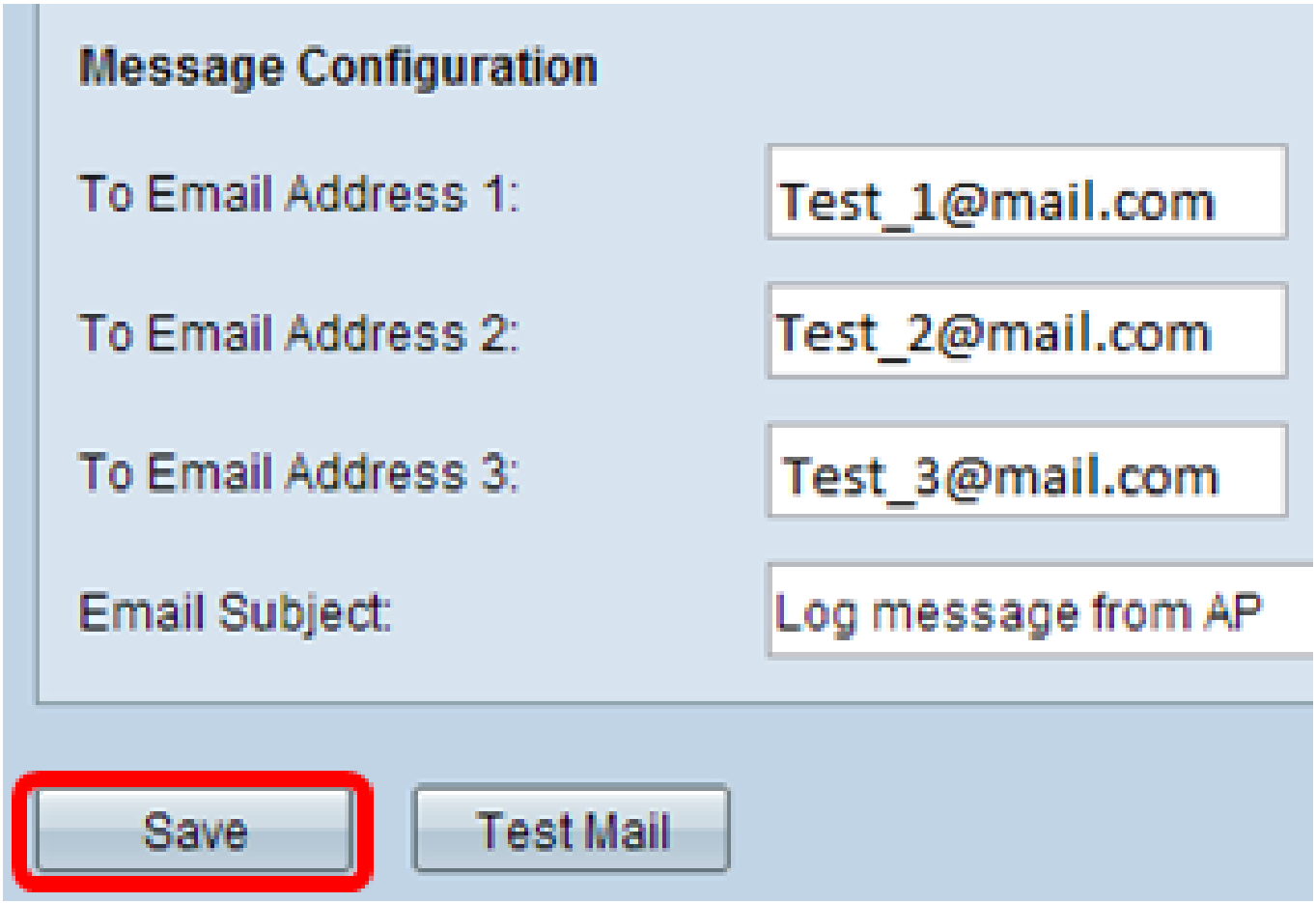


Remarque : dans cet exemple, le message de journalisation du point d'accès est utilisé.

Étape 14. Cliquez sur Test Mail pour valider les informations d'identification du serveur de messagerie configurées. Cette opération envoie un e-mail aux adresses e-mail configurées pour vérifier que la configuration fonctionne.



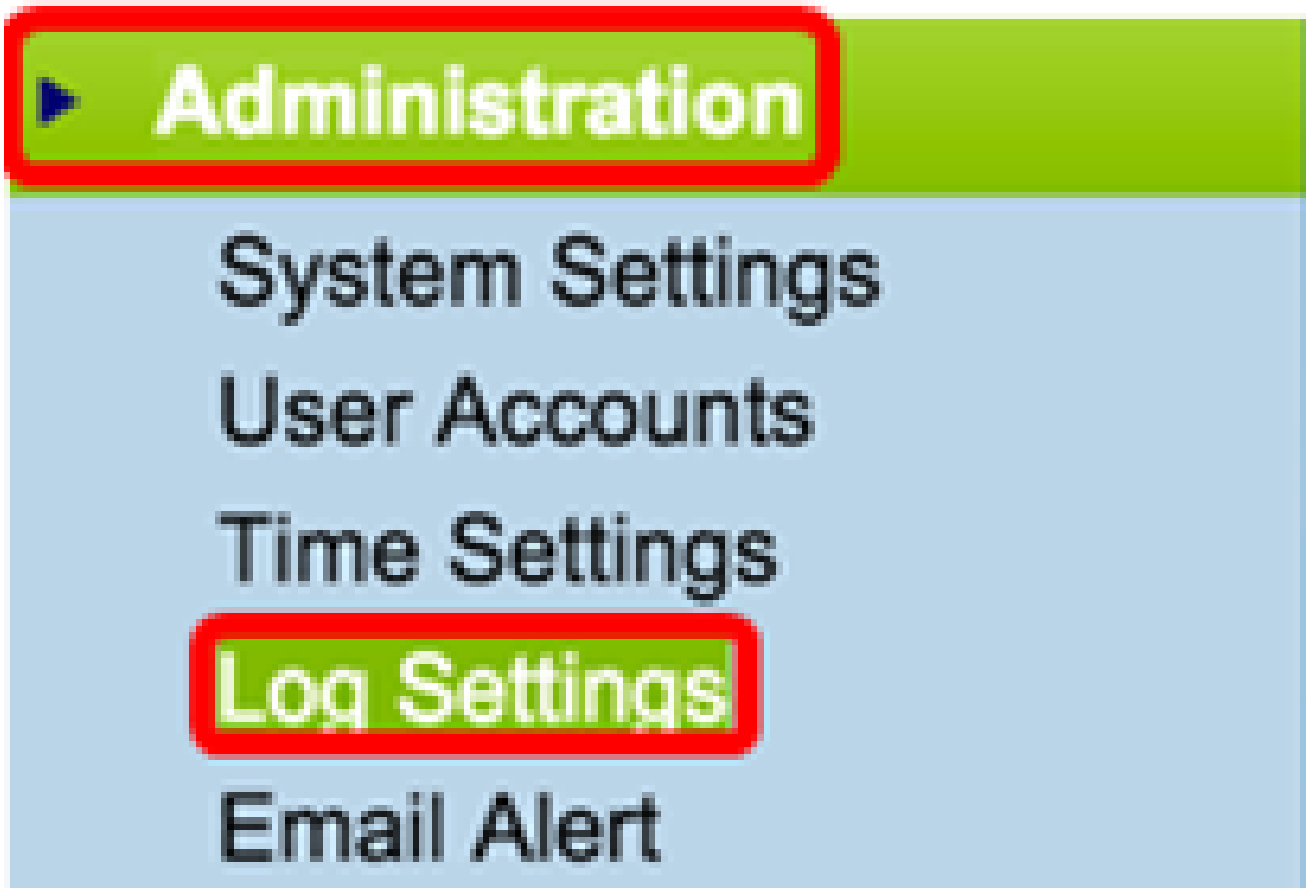
Étape 15. Cliquez sur Save.



Configurer les paramètres du journal

Cette zone configure localement les journaux système et d'événements dans la mémoire volatile et la mémoire NVRAM.

Étape 1. Connectez-vous à l'utilitaire Web du point d'accès pour sélectionner Administration > Log Settings.



Étape 2. (Facultatif) Si vous souhaitez que les journaux soient enregistrés de manière permanente afin que les paramètres restent au moment du redémarrage du WAP, activez Persistence en cochant la case Enable. Ceci est particulièrement utile en cas de redémarrage inattendu du système lorsqu'un événement indésirable ou une panne se produit. Jusqu'à 128 messages de journal peuvent être enregistrés dans la mémoire vive non volatile, après quoi les journaux sont écrasés.

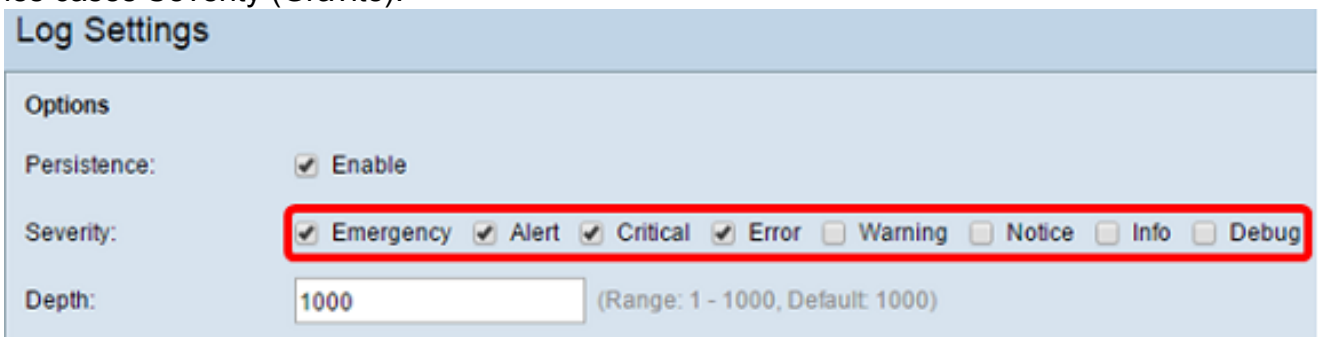


Remarque : si la case Activer est décochée, les journaux sont enregistrés dans la mémoire volatile.

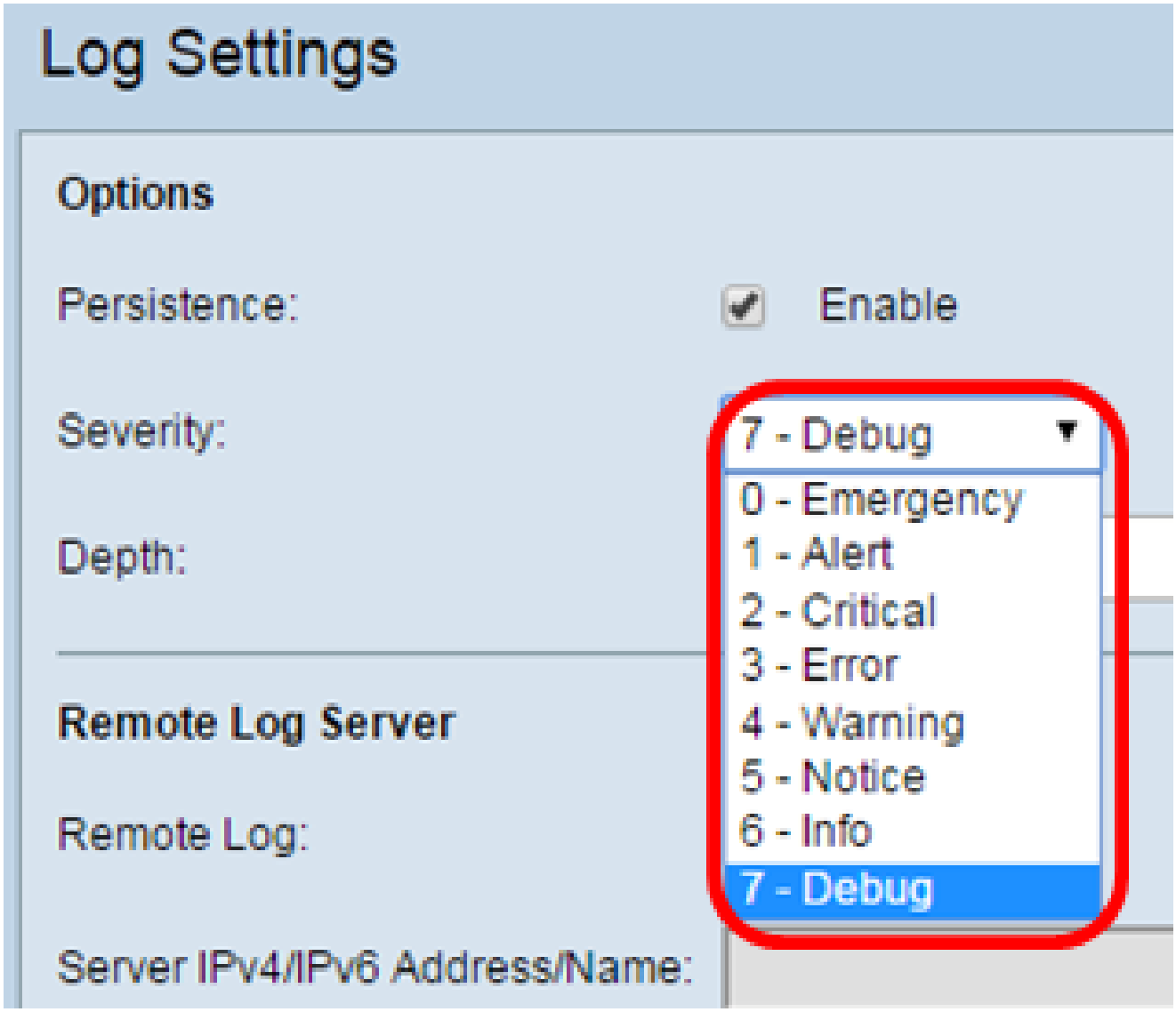
Étape 3. Pour définir la gravité, choisissez le type de message approprié à envoyer, par exemple Urgence, Alerte, Critique, Erreur, Avertissement, Avis, Info ou Débogage. Ces messages sont envoyés chaque fois que la durée du journal expire. Ces options s'affichent

différemment dans l'utilitaire Web en fonction du modèle du périphérique que vous utilisez.

Pour WAP131, WAP150, WAP351 et WAP361, cochez le type de message approprié dans les cases Severity (Gravité).



Pour WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 et WAP571E, cliquez sur le type de message approprié dans la liste déroulante Gravité.



- None : aucun message n'est envoyé.
- Urgence : ce type de message est envoyé à l'utilisateur lorsque le périphérique se trouve dans une situation critique et qu'une attention immédiate est requise.
- Alert : ce type de message est envoyé à l'utilisateur lorsqu'une action différente de la

configuration normale se produit.

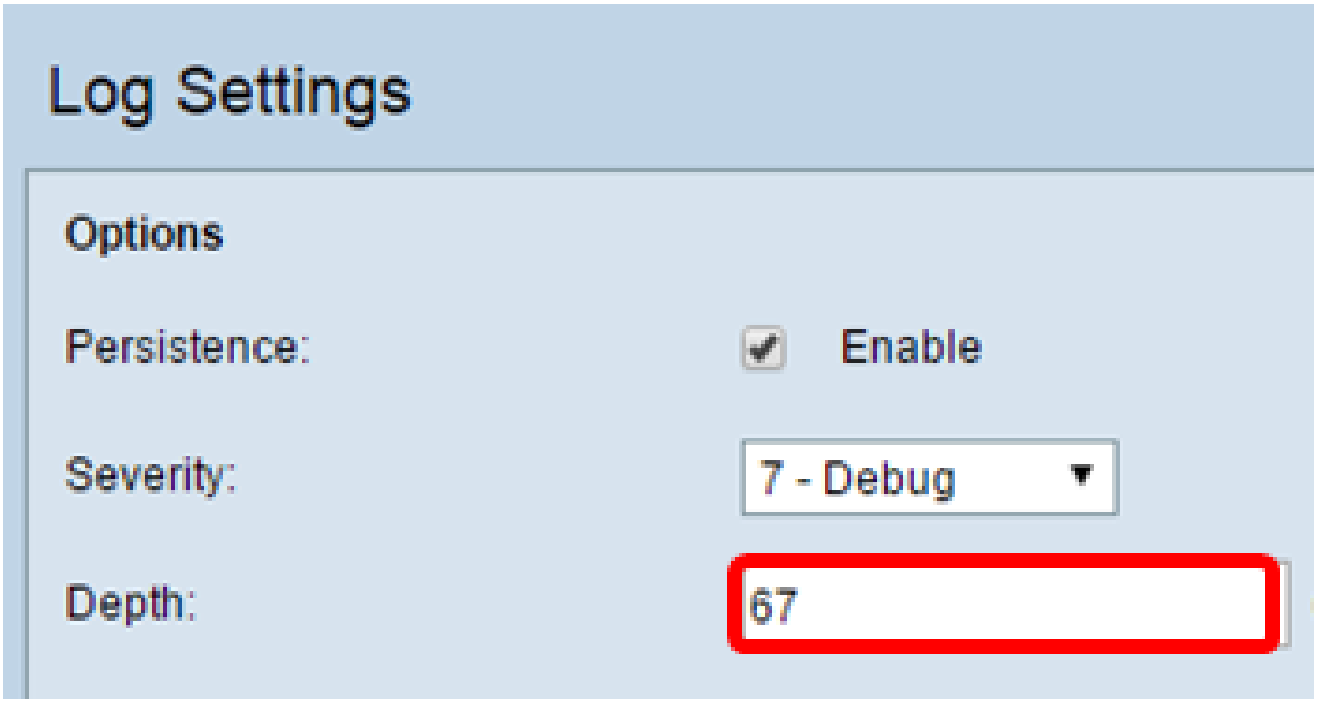
- Critique : ce type de message est envoyé à l'utilisateur lorsqu'un port est en panne ou que l'utilisateur ne peut pas accéder au réseau. Une action immédiate est requise.
- Erreur : ce type de message est envoyé à l'utilisateur en cas d'erreur de configuration.
- Avertissement : ce type de message est envoyé à l'utilisateur lorsqu'un autre utilisateur tente d'accéder aux zones d'accès restreint.
- Notice : ce type de message est envoyé à l'utilisateur en cas de modifications de faible priorité sur le réseau.
- Info : ce type de message est envoyé à l'utilisateur pour décrire le comportement du réseau.
- Debug : ce type de message est envoyé à l'utilisateur avec les journaux du trafic réseau.

Étape 4. Au fur et à mesure de la génération des messages du journal, ceux-ci sont placés dans une file d'attente pour être transmis. Spécifiez le nombre de messages pouvant être mis en file d'attente simultanément dans la mémoire volatile dans le champ Profondeur. Jusqu'à 512 messages peuvent être mis en file d'attente simultanément.

Pour WAP131, WAP150, WAP351 et WAP361, saisissez la plage de profondeur dans le champ Profondeur. La plage est comprise entre 1 et 1 000. La valeur par défaut est 1 000.



Pour WAP121, WAP321, WAP371, WAP551, WAP561, WAP571 et WAP571E, entrez la plage de profondeur dans le champ Profondeur. La plage est comprise entre 1 et 512 et 512 est la valeur par défaut. Dans cet exemple, 67 est utilisé.



Étape 5. Cliquez sur Save.

Remarque : le point d'accès acquiert des informations d'heure et de date à l'aide d'un serveur NTP. Ces données sont au format UTC (Greenwich Mean Time).

Ces configurations doivent propager la journalisation des événements sur votre périphérique local et recevoir des alertes par e-mail.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.