

# Configuration de la sécurité des ports sur les commutateurs empilables de la gamme Sx500

## Objectif

La sécurité des ports peut être utilisée avec des adresses MAC apprises dynamiquement et statiques pour limiter le trafic d'entrée d'un port, car elle limite les adresses MAC qui sont autorisées à envoyer du trafic au port. Lorsqu'une adresse MAC sécurisée est attribuée à un port sécurisé, le port ne transfère pas le trafic d'entrée pour ceux qui ont des adresses MAC source qui ne sont pas similaires aux adresses définies.

L'objectif de ce document est d'expliquer la configuration de la sécurité des ports sur les commutateurs de la gamme Sx500.

## Périphériques pertinents

Commutateurs Empilables · Sx500

## Version du logiciel

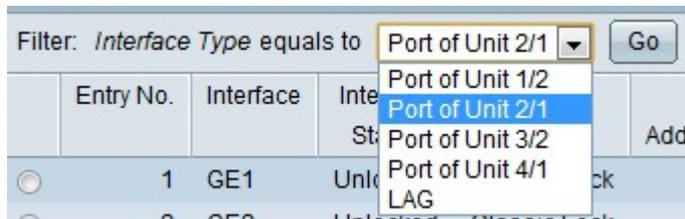
•v 1.2.7.76

## Configuration de la sécurité des ports

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > Port Security**. La page *Sécurité des ports* s'ouvre :

Entry No.	Interface	Interface Status	Learning Mode	Max No. of Address Allowed	Action on Violation	Trap	Trap Frequency (sec.)
<input type="radio"/>	1 GE1	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	2 GE2	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	3 GE3	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	4 GE4	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	5 GE5	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	6 GE6	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	7 GE7	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	8 GE8	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	9 GE9	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	10 GE10	Unlocked	Classic Lock	1	Disabled	10	

Étape 2. À partir du filtre : Liste déroulante Type d'interface, sélectionnez le type d'interface sur lequel le paquet est attendu.



Étape 3. Cliquez sur **Go**, qui affiche l'état des interfaces.

Étape 4. Cliquez sur l'interface à modifier et cliquez sur **Modifier**. La fenêtre *Modifier les paramètres de l'interface de sécurité des ports* s'affiche.

Entry No.	Interface	Interface Status	Learning Mode	Max No. of Address Allowed	Action on Violation	Trap	Trap Frequency (sec.)
<input checked="" type="radio"/>	1 GE1	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	2 GE2	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	3 GE3	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	4 GE4	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	5 GE5	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	6 GE6	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	7 GE7	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	8 GE8	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	9 GE9	Unlocked	Classic Lock	1	Disabled	10	
<input type="radio"/>	10 GE10	Unlocked	Classic Lock	1	Disabled	10	

Buttons: Copy Settings... Edit..

Étape 5. (Facultatif) Pour modifier l'interface que vous configurez, cliquez sur la case d'option souhaitée dans le champ *Interface* et sélectionnez l'interface souhaitée dans la liste déroulante.

Interface:  Unit/Slot 1/1 Port GE1  LAG 1

Interface Status:  Lock

Learning Mode:  Classic Lock  Limited Dynamic Lock  Secure Permanent  Secure Delete on Reset

Max No. of Address Allowed: 10 (Range: 0 - 256, Default: 1)

Action on Violation:  Discard  Forward  Shutdown

Trap:  Enable

Trap Frequency: 15 sec. (Range: 1 - 1000000, Default: 10)

Buttons: Apply Close

· unité/logement — Dans les listes déroulantes Unité/logement, sélectionnez l'unité/logement approprié. L'unité identifie si le commutateur est actif ou membre de la pile. Le logement identifie le commutateur auquel est connecté le logement (le logement 1 est SF500 et le logement 2 est SG500). Si vous ne connaissez pas les termes utilisés, consultez [Cisco Business : Glossaire des nouveaux termes](#).

· Port : dans la liste déroulante Port, sélectionnez le port approprié à configurer.

·LAG : sélectionnez le LAG dans la liste déroulante LAG. Un LAG (Link Aggregate Group) est utilisé pour relier plusieurs ports entre eux. Les LAG multiplient la bande passante, augmentent la flexibilité des ports et assurent la redondance des liaisons entre deux périphériques pour optimiser l'utilisation des ports

Étape 6. (Facultatif) Pour verrouiller le port immédiatement et ne pas apprendre de nouvelles adresses MAC, cochez **Verrouiller** dans le champ *État de l'interface*.

**Économiseur de temps** : Si cette case est cochée, passez à l'étape 9.

Étape 7. Cliquez sur la case d'option correspondant au type de verrouillage de port souhaité requis dans le champ *Mode apprentissage*. Il existe quatre options.

·Classic Lock : verrouille instantanément le port sans tenir compte du nombre d'adresses déjà acquises. Le port n'apprend aucune nouvelle adresse MAC. Les adresses apprises ne peuvent pas être réappries ou vieilles.

·Limited Dynamic Lock : verrouille le port, supprime les adresses MAC dynamiques actuelles associées au port, puis le port apprend les adresses jusqu'à sa limite maximale. Le port peut être réappris et vieilli.

·Secure Permanent : l'adresse MAC dynamique actuelle associée au port est conservée et elle apprend le nombre maximal d'adresses autorisées sur le port. Ce champ est défini par le champ *Nombre max. d'adresses autorisées*. Relearning et Aging sont activés.

·Secure Delete on Reset : une fois le port réinitialisé, il supprime l'adresse MAC dynamique actuelle. Les adresses MAC peuvent être apprises en fonction du nombre d'adresses autorisées sur le port. Ce champ est défini par le champ *Nombre max. d'adresses autorisées*. La régénération et le vieillissement sont désactivés.

Étape 8. Si vous ne cliquez pas sur Verrouillage classique à l'étape 7, entrez le nombre maximal d'adresses MAC pouvant être apprises sur un port si vous cliquez sur le mode d'apprentissage de verrouillage dynamique limité. Le nombre 0 indique que seules les adresses statiques sont prises en charge sur l'interface.

Étape 9. Si Verrouiller est coché à l'étape 6, cliquez sur une case d'option dans le champ *Action en cas de violation* pour choisir l'action à effectuer sur les paquets reçus au port verrouillé.

·Discard : rejette les paquets de toute source non apprise.

·Forward : transfère les paquets d'une source inconnue sans connaître l'adresse MAC.

·Shutdown : supprime les paquets de toute source non apprise et le port est arrêté. Ce port est arrêté jusqu'à sa réactivation ou jusqu'au redémarrage du commutateur.

Étape 10. (Facultatif) Pour activer les déroutements lorsqu'un port verrouillé reçoit un paquet, activez **Enable** dans le champ *Trap*. Il s'applique aux violations de verrous. En cas de verrouillage classique, il s'agit de toute nouvelle adresse reçue. En cas de verrouillage dynamique limité, il s'agit de toute nouvelle adresse qui dépasse le nombre d'adresses autorisées.

**Économiseur de temps** : Si l'option Activer n'est pas cochée à l'étape 10, passez à l'étape 12.

Étape 11. Entrez la durée minimale, en secondes, qui passe entre les interruptions dans le champ *Fréquence de déroutement*.

Étape 12. Cliquez sur **Apply** pour appliquer les paramètres.

## Paramètres de copie

Étape 1. Cliquez sur l'interface à modifier et cliquez sur **Copier les paramètres**. La fenêtre *Copy Settings* s'affiche.

Entry No.	Interface	Interface Status	Learning Mode	Max No. of Address Allowed	Action on Violation	Trap	Trap Frequency (sec.)
<input checked="" type="radio"/>	1	GE1	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	2	GE2	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	3	GE3	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	4	GE4	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	5	GE5	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	6	GE6	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	7	GE7	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	8	GE8	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	9	GE9	Unlocked	Classic Lock	1	Disabled	10
<input type="radio"/>	10	GE10	Unlocked	Classic Lock	1	Disabled	10

Étape 2. Saisissez les interfaces ou plages d'interfaces auxquelles la configuration doit être copiée dans le champ fourni.

Copy configuration from entry 1 (GE1)

to:  (Example: 1,3,5-10 or: GE1,GE3-GE5)

Étape 3. Cliquez sur **Apply** pour modifier la sécurité des ports et mettre à jour le fichier de configuration en cours.