

Contenu

[Introduction](#)

[Prerequistes](#)

[Informations générales](#)

[Pratiques recommandées pour l'installation virtuelle de permis ESA/Virtual WSA/Virtual SMA](#)

[Obtenez un permis virtuel \(VLN\)](#)

[Chargez le permis virtuel sur votre appliance](#)

[Vérifiez](#)

[Informations connexes](#)

Introduction

Ce document décrit des pratiques recommandées, comment obtenir un permis, et l'installation du permis de Cisco pour l'appliance virtuelle de sécurité du courrier électronique (vESA), l'appliance virtuelle de sécurité Web (vWSA), ou l'appliance virtuelle de Gestion de la sécurité (vSMA).

Prerequistes

- Vous avez un compte de Cisco.com attaché à un [contrat](#) actif de [Cisco](#).
- Vous avez une appliance entièrement autorisée de sécurité du courrier électronique de Cisco (ESA), l'
- Vous avez lu et avez reconnu le [guide d'installation virtuel d'appareils de sécurité du contenu de Cisco](#).
- Le vESA/vWSA/vSMA a été installé dans votre environnement virtuel, l'assistant de configuration de système est terminé, et vous avez émis la commande de **saveconfig** du CLI sur l'appliance virtuelle.

[Informations générales](#)

Les diverses références pourraient répertorier l'ESA virtuel comme VESA, vESA, ou ESAV, et le WSA virtuel comme VWSA, vWSA, ou WSAV, ou SMA virtuel comme VSMA, vSMA, et SMAV. Soyez sûr d'utiliser ces acronymes l'un pour l'autre, comme nécessaire.

Pratiques recommandées pour l'installation virtuelle de permis ESA/Virtual WSA/Virtual SMA

Avant que vous vous terminiez la configuration pour votre vESA/vWSA/vSMA, vous êtes requis de demander et installer un permis virtuel d'appareils.

Obtenez un permis virtuel (VLN)

Un numéro de licence virtuel (VLN) doit être créé des exécutions globales de permis de Cisco (GLO). Vous devrez avoir vos clés d'activation de votre ESA, WSA ou SMA, et votre compte de

Cisco.com afin de compléter ce processus. (Si vous n'avez pas déjà un compte de Cisco.com, inscription à un compte chez www.tools.cisco.com/RPF/register/register.do.)

1. Allez à www.cisco.com/go/license.
2. Procédure de connexion avec votre ID de compte Cisco.
3. De l'obtenir l'autre liste déroulante de permis, choisissez le processus de permis de partage...

Tools & Resources

Product License Registration

Hello [User Name] [User Profile]

[View in French](#) [Contact Us](#) [Feedback](#) [Help](#) [My Profile](#) [Related Tools](#)

[Did You Know?](#) [System Messages](#) [Supported Browsers](#)

Get New Licenses

Enter 1 to 10 PAKs or token IDs, separated by commas

[Fulfill...](#) [Get Other Licenses](#)

Manage

[PAKs/Tokens](#) | [Licenses](#) | [Devices](#) | [Transactions History](#)

[Add New PAKs/Tokens](#) | [Actions](#) | [Filters](#) | [Export to CSV](#)

<input type="checkbox"/>	PAK/Token ID	Status	Product Family	SKU	Available	Used
<input type="checkbox"/>	[blurred]	Fulfilled	Iron Port Product - SW ...	SMA-EMGT-LIC=	0	10000
<input type="checkbox"/>	[blurred]	Fulfilled	Iron Port Product - SW ...	SMA-EMGT-LIC=	0	52456
<input type="checkbox"/>	[blurred]	Fulfilled	Iron Port Product - SW ...	ESA-ESI-LIC=	0	52456

1 show 10 records

#1 → [Get Other Licenses](#)

#2 → [Share License Process...](#)

- Demo and Evaluation...
- TelePresence Software Release Key...
- TelePresence License to Resend...
- IPS, Crypto, Other...
- [Share License Process...](#)
- Main to Backup...
- Register ROSA HA as Pair...
- Migration...

4. Choisissez l'option de codes de lancement d'obtenir.

Get Other Licenses

- Demo and Evaluation...
- TelePresence Software Release Key...
- TelePresence License to Resend...
- IPS, Crypto, Other...
- [Share License Process...](#)
- Main to Backup...
- Register ROSA HA as Pair...
- Migration...

Get Activation Codes

Use Activation Codes

→

5. Vous serez présenté avec une fenêtre externe. Choisissez le produit d'IronPort - Paquets de SW (si vous avez un lot de logiciels existant) ou produit d'IronPort - comité technique (si vous avez différents Produits).

License for Email & Web Security Appliance



Apply the licensed features of an existing device to additional devices. If intending to use an activation code but find it has expired, request another code.

* Product:

A dropdown menu is shown with the following options: "Select One", "Select One", "Cisco FirePOWER Product - Perpetual", "Cisco FirePOWER Product - Term", "Iron Port Product - Perpetual", "Iron Port Product - SW Bundles" (highlighted in blue), "Iron Port Product - TC", and "Iron Port Product - Third Party". A red arrow points to the "Iron Port Product - SW Bundles" option.

6. Écrivez un numéro de série existant ESA/WSA/SMA dans le champ d'identification de numéro de série de source/périphérique virtuel. Si vous avez plusieurs ESAs, WSAs, ou SMAs, choisissez un qui a les mêmes permis que vous voulez activé sur votre appliance virtuelle.
7. Pour l'option choisie de type d'appareils de destination, choisissez le bouton virtuel.
8. Laissez le blanc de champ d'identification de numéro de série de cible/périphérique virtuel.
9. Dans l'envoi à mettre en place, écrivez l'adresse e-mail à laquelle le code de lancement devrait être envoyé.
10. Code de demande de clic.

License for Email & Web Security Appliance

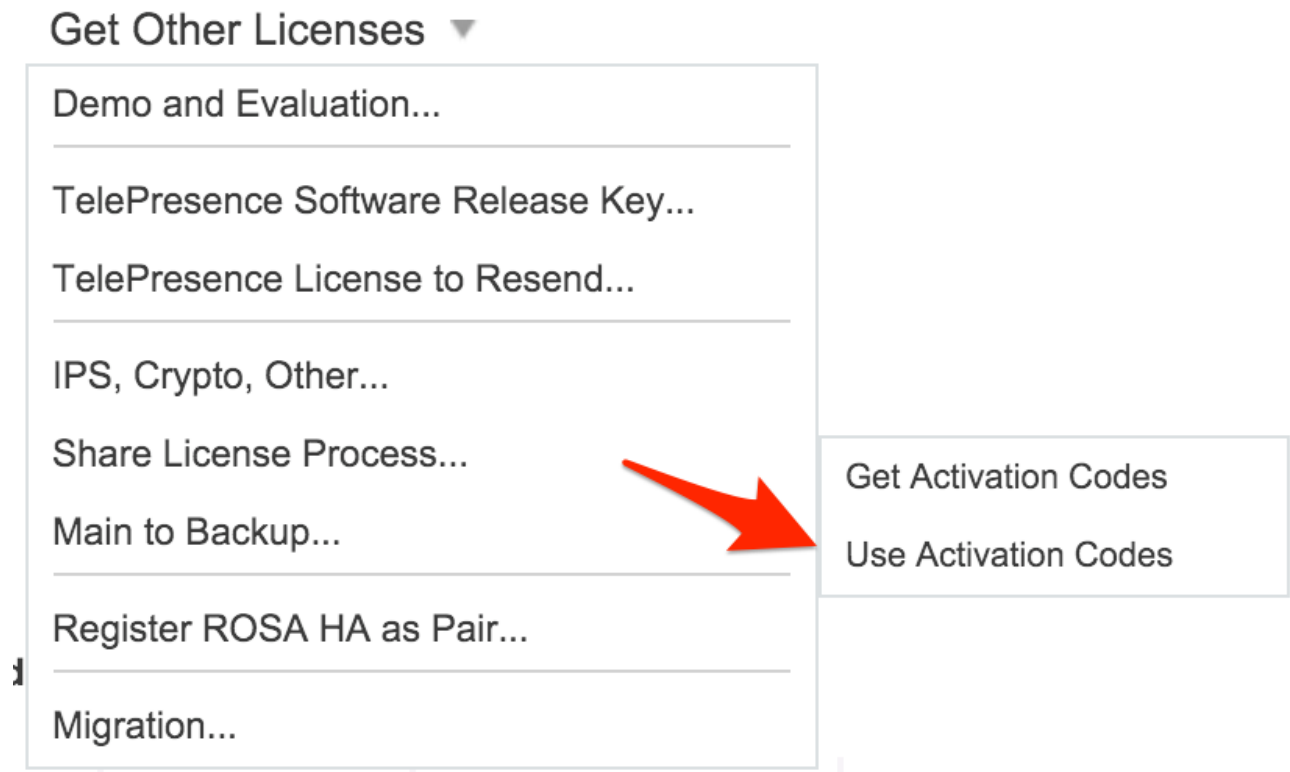


Apply the licensed features of an existing device to additional devices. If intending to use an activation code but find it has expired, request another code.

The screenshot shows the license application form with the following fields and annotations:

- Product:** A dropdown menu set to "Iron Port Product - SW Bundles".
- Source Serial Number / Virtual Device Identifier:** A text input field with a red arrow and the number "1" pointing to it.
- Select Destination Appliance Type:** Radio buttons for "Physical" and "Virtual". The "Virtual" option is selected, with a red arrow and the number "2" pointing to it.
- Target Serial Number / Virtual Device Identifier:** A text input field.
- Send to:** A text input field with a red arrow and the number "3" pointing to it.
- Select an Existing VLN:** A dropdown menu set to "-Select an Existing VLN-".
- VLN License File:** A text input field.
- Buttons:** "Reset" and "Request Code" buttons at the bottom. A red arrow and the number "4" point to the "Request Code" button.

11. Après que vous recevez le code, répétez l'étape 3 (répertoriée ci-dessus). Une fois que vous atteignez l'étape 4, choisissez l'option de **codes de lancement d'utilisation**.



12. Utilisant le code fourni de lancement, cliquez sur Next, et puis choisissez le logiciel UGS de Cisco ESA/WSA qui devrait être inclus sur le permis virtuel de Cisco ESA/virtual WSA/virtual SMA. Cliquez sur **Next** (Suivant).
13. Écrivez l'adresse e-mail à laquelle le permis devrait être envoyé.
14. En conclusion, le clic **obtiennent le permis**.

Remarque: Votre fichier de licence virtuel devrait être envoyé et reçu dans un délai de trois heures à l'adresse e-mail car vous avez spécifié dans l'étape 13. Remarque: Le fichier de licence virtuel sera introduit le format XML.

Chargez le permis virtuel sur votre appliance

- Le fichier de licence virtuel en tant que reçu doit être chargé avec le **loadlicense de** commande CLI, et alors **le collez du CLI ou chargez à partir du fichier**.
- Vous devrez écrire **CTRL-D** une fois que le permis a été entré. (*Highlighted en jaune dans l'exemple ci-dessous.)
- Après le chargement réussi du fichier de licence, vous serez présenté avec la pleine extrémité - utilisateur - le contrat de licence (CLUF) de recevoir. Vous devrez écrire **Y** afin de recevoir le CLUF et se terminer chargeant le permis sur l'appliance virtuelle.

Remarque: Vous pouvez charger le fichier XML dans Notepad++, ou tout autre éditeur de texte semblable qui est capable du rendu XML.

Exemple de sortie de **pâte par l'intermédiaire de CLI** :

Exemple de sortie de **chargement à partir de fichier** :

Remarque: Si vous choisissez **de charger à partir du fichier**, vous devrez employer le Protocole FTP (File Transfer Protocol) afin de placer le fichier de licence sur l'appliance virtuelle. Ceci pourrait exiger la configuration de l'interface du CLI avec la commande **d'interfaceconfig**, ou le GUI, **réseau > interfaces IP**. Assurez-vous que le FTP est activé sur l'interface exigée, et **soumettez/validation** toutes les modifications.

Un FTP d'exemple de votre localhost, avec le FTP standard commande, est affiché ici :

Vérifiez

En ce moment, le fichier de licence devrait être chargé sur votre appliance virtuelle. Vous pouvez employer la commande de **featurekey** afin d'obtenir le plein affichage des touches de fonction qui ont été attachées au permis et qui sont maintenant en activité.

Remarque: Des touches de fonction sont incluses en tant qu'élément du permis. Les touches de fonction expirent en même temps que le permis, même si la caractéristique n'a pas été lancée. Acheter de nouvelles touches de fonction exigera de vous de télécharger et installer un nouveau fichier de licence virtuel d'appareils. Ceci est spécifié dans le [guide d'installation virtuel d'appareils de sécurité du contenu de Cisco](#).

Vous pouvez également utiliser la commande de **showlicense** et voir les dates de nombre VLN et de validité de permis :

Informations connexes

- [Appliance virtuelle de sécurité du courrier électronique de Cisco - Page de support](#)
- [Appliance de sécurité du courrier électronique de Cisco - Page de support](#)
- [Appliance virtuelle de sécurité Web de Cisco - Page de support](#)
- [Appliance de sécurité Web de Cisco - Page de support](#)
- [Support et documentation techniques - Cisco Systems](#)