Récupération et personnalisation du tableau de bord Secure Web Appliance

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Mon tableau de bord
  - Vue par défaut
  - Caractéristiques du trafic du proxy Web
  - Utilisation des ressources système
  - Activité totale du proxy Web
  - Résumé du proxy Web
  - Résumé du Moniteur de trafic de couche 4
  - Transactions suspectes
  - Synthèse des transactions suspectes
  - Principales catégories d'URL : Total des transactions
  - Principaux types d'applications : Total des transactions
  - Principales catégories de programmes malveillants : Surveillé ou bloqué
  - Principaux utilisateurs : Transactions bloquées ou averties
- Modifier la plage horaire
- Modifier des jeux de données
- Modifier la conception du tableau de bord
- Restaurer mon tableau de bord par défaut
- Autres informations utiles

Introduction

Ce document décrit les étapes de personnalisation et de restauration du tableau de bord Secure Web Appliance (SWA).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Accès à l'interface graphique utilisateur (GUI) de SWA
- Accès administratif au SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Mon tableau de bord

Par défaut, la page de renvoi SWA est My-Dashboard, c'est-à-dire la page qui s'affiche lorsque l'utilisateur se connecte à l'appliance. Mon tableau de bord contient deux sections principales :

- Présentation du système
- Intervalle de temps

Vous pouvez personnaliser diverses propriétés de ces statistiques et rapports, telles que :

- Type de données
- Intervalle de temps
- Position à afficher sur la page
- Afficher et masquer les jeux de données

Vue par défaut

Par défaut, les rapports et les statistiques de My-Dashboard sont les suivants :

- Présentation du système
    - Présentation > Caractéristiques du trafic du proxy Web
    - Généralités > Utilisation des ressources système
- Intervalle de temps
    - Présentation > Activité totale du proxy Web

- Présentation > Résumé du proxy Web
- Présentation > Résumé du Moniteur du trafic de couche 4 (L4)
- Généralités > Transactions suspectes
- Généralités > Synthèse des transactions suspectes
- Principales catégories d'URL : Total des transactions
- Principaux types d'applications : Total des transactions
- Principales catégories de programmes malveillants : Surveillé ou bloqué
- Principaux utilisateurs : Transactions bloquées ou averties



Image - Tableau de bord SWA

Caractéristiques du trafic du proxy Web

Caractéristiques du trafic du proxy Web répertorie les statistiques relatives aux transactions :

Nombre moyen de transactions par seconde au cours de la dernière minute : XX
Bande passante moyenne (bits/s) au cours de la dernière minute : XX
Temps de réponse moyen (ms) au cours de la dernière minute : XX
Nombre total de connexions actuelles : XX

Utilisation des ressources système

L'utilisation des ressources système répertorie la charge totale de l'unité centrale (UC), la mémoire vive (RAM) et l'utilisation du disque des rapports/journaux.

Cliquez sur System Status Details pour accéder à la page System Status.

(Utilisez la page Reporting > System Status pour surveiller l'état du système. Cette page affiche l'état et la configuration actuels de l'appareil Web sécurisé.)



Remarque : La valeur d'utilisation de l'UC affichée sur cette page et la valeur de l'UC affichée sur la page System Status peuvent différer légèrement, car elles sont lues séparément, à des moments différents.

Activité totale du proxy Web

Vous pouvez afficher l'activité de proxy Web signalée par les appliances Web sécurisées actuellement gérées par l'appliance de gestion de la sécurité.
Cette section affiche le nombre réel de transactions et la date approximative à laquelle l'activité s'est produite sous forme graphique.

Vous pouvez également afficher le pourcentage d'activité de proxy Web suspecte, ou d'activité de proxy propre, et inclure le nombre total de transactions.

Résumé du proxy Web

Permet d'afficher le pourcentage d'activité du proxy Web suspecte ou propre.

Résumé du Moniteur de trafic de couche 4

Vous pouvez afficher tout trafic de couche 4 signalé par les appliances Web sécurisées actuellement gérées par l'appliance de gestion de la sécurité, au format graphique.

Transactions suspectes

Vous pouvez afficher sous forme graphique les transactions Web étiquetées comme suspectes par l'administrateur.
Cette section affiche le nombre réel de transactions et la date approximative à laquelle l'activité s'est produite, sous forme graphique.

Synthèse des transactions suspectes

Vous pouvez également afficher le pourcentage de transactions bloquées ou averties qui sont suspectes.

Vous pouvez voir le type de transactions qui ont été détectées et bloquées, ainsi que le nombre réel de fois où cette transaction a été bloquée.

Principales catégories d'URL : Total des transactions

Vous pouvez afficher les principales catégories d'URL visitées sur le site dans un format graphique.

Principaux types d'applications : Total des transactions

Vous pouvez afficher les principaux types d'application bloqués, qui incluent également le nom du type d'application réel et le nombre de fois où l'application spécifique a été bloquée, au format graphique.

Principales catégories de programmes malveillants : Surveillé ou bloqué

Vous pouvez afficher toutes les catégories de programmes malveillants qui ont été détectés au format graphique.

Principaux utilisateurs : Transactions bloquées ou averties

Vous pouvez afficher les utilisateurs réels qui ont généré les transactions bloquées ou averties, au format graphique. Les utilisateurs peuvent être affichés par adresse IP ou par nom d'utilisateur.

Modifier la plage horaire

Pour modifier la plage de dates Jour à Heure, Semaine, 30 jours, Hier :

Étape 1: Choisir une option (en haut à droite)

Étape 2: Sélectionnez Performances.

Étape 3: Cliquez sur Modifier les préférences.

Étape 4: Remplacez Intervalle de temps de rapport affiché (par défaut) par l'une des options disponibles.

Étape 5 : Envoyer. Il n'est pas nécessaire de valider les modifications.

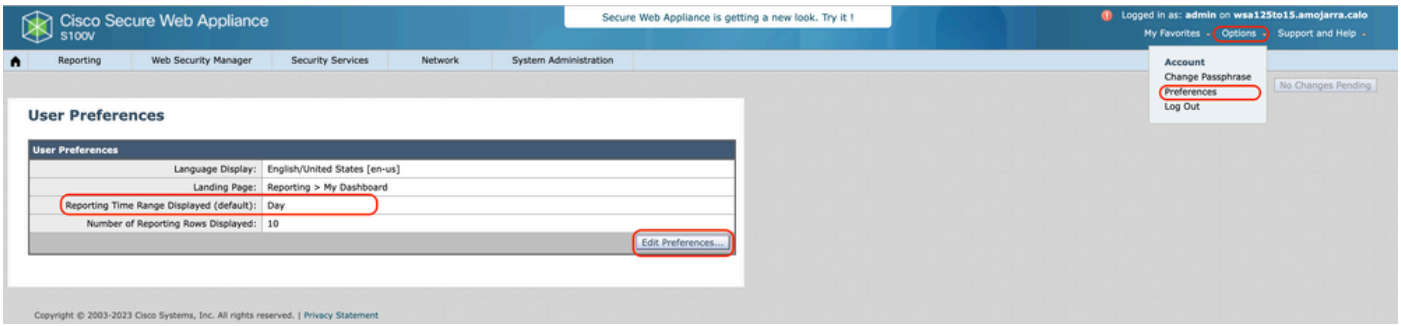


Image - Étapes pour modifier la plage horaire par défaut dans Mon-Tableau de bord

Modifier des jeux de données

Vous pouvez ajouter et supprimer des jeux de données et des rapports dans la page Mon tableau de bord. Utilisez le signe plus (+) pour ajouter des rapports supplémentaires et le signe X en haut à droite de chaque rapport pour les supprimer.

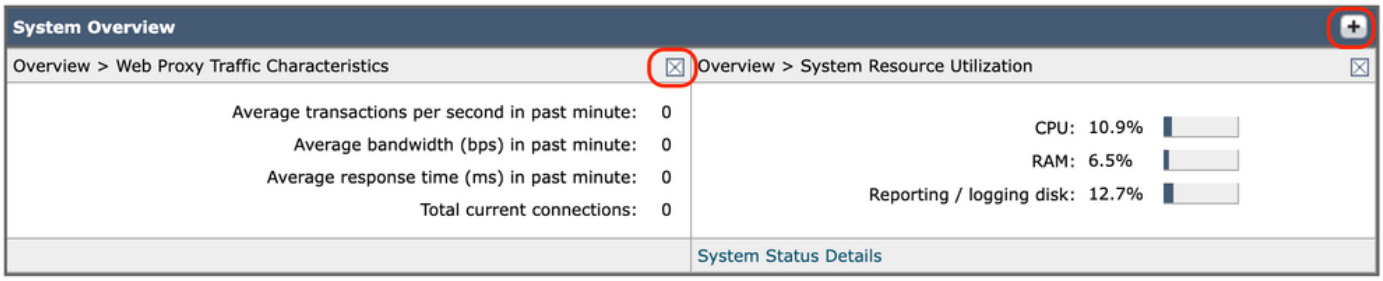


Image - Ajouter et supprimer des rapports dans My-Dashboard.

Mise en garde : Les modifications prennent effet dès que vous les modifiez. Il n'est pas nécessaire d'envoyer.

Modifier la conception du tableau de bord

Vous pouvez modifier l'ordre de chaque jeu de données dans la page Mon tableau de bord. Cliquez sur le ruban bleu en haut de chaque rapport, puis modifiez l'emplacement de ce rapport.

Restaurer mon tableau de bord par défaut

Pour restaurer la valeur par défaut de My-Dashboard, modifiez manuellement le fichier de configuration, en procédant comme suit :

Étape 1: Dans l'interface utilisateur graphique, accédez à Administration système.

Étape 2: Sélectionnez Fichier de configuration.

Étape 3: Téléchargez le dernier fichier de configuration.

Remarque : Sélectionnez Chiffrer les mots de passe dans les fichiers de configuration.

Étape 4 : Modifiez le fichier XML en supprimant tout ce qui se trouve entre <user_reports> et </user_reports>.

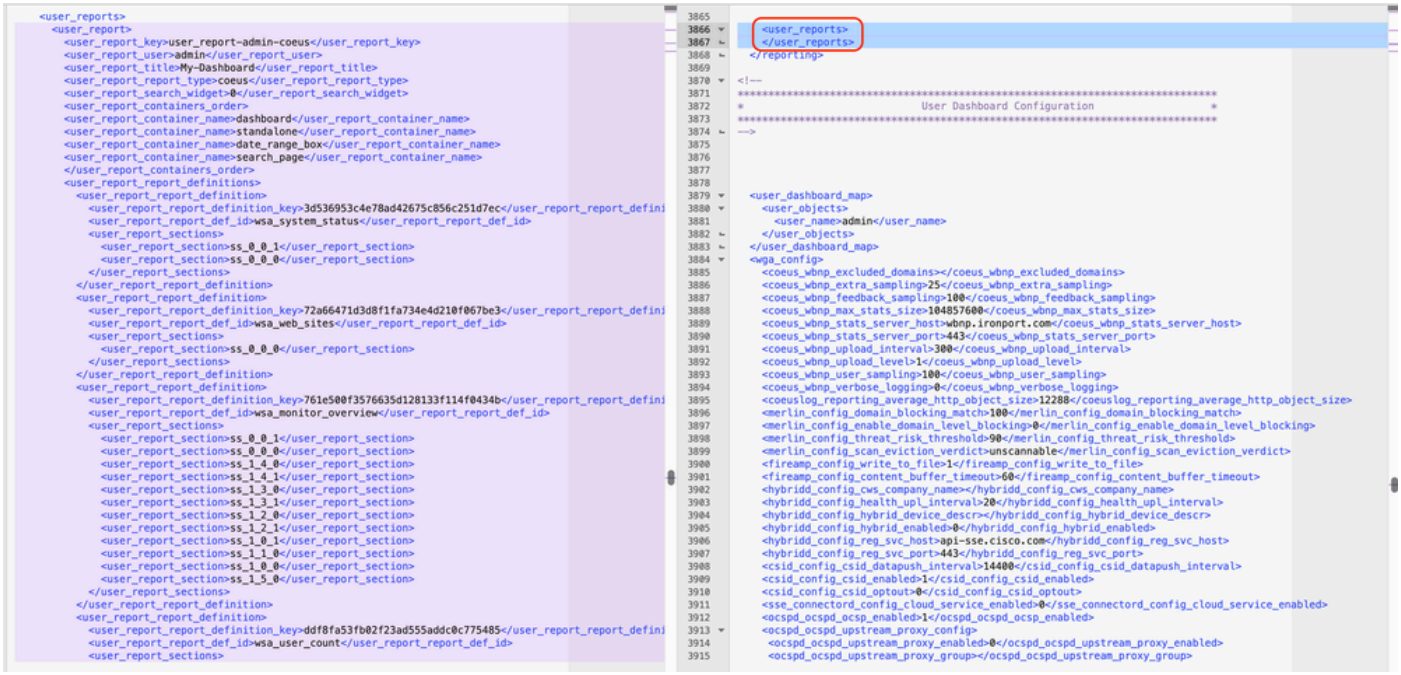


Image - Exemples de fichiers de configuration avec tableau de bord personnalisé (à droite) et fichier de configuration par défaut (à gauche).

Étape 5: Sur la page Fichier de configuration, dans la section Charger la configuration, sélectionnez Charger un fichier de configuration à partir de l'ordinateur local.

Étape 6: Téléchargez le fichier XML modifié.

Étape 7: Cliquez sur Charger et valider les modifications.

Autres informations utiles

Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance - GD (General Deployment)

Assistance - Assistance et téléchargements Cisco - Documentation, outils, dossiers - Cisco

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.