Recupere e personalize o painel do Secure Web Appliance

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Meu painel
  - Exibição padrão
  - Características de tráfego do Web Proxy
  - Utilização de recursos do sistema
  - Atividade total do Web Proxy
  - Resumo do Web Proxy
  - Resumo do L4 Traffic Monitor
  - Transações suspeitas
  - Resumo de transações suspeitas
  - Principais categorias de URL: Total de transações
  - Principais tipos de aplicativos: Total de transações
  - Principais categorias de malware: Monitorado ou Bloqueado
  - Principais usuários: Transações bloqueadas ou com aviso
- Modificar intervalo de tempo
- Modificar Conjuntos de Dados
- Alterar Design do Painel
- Restaurar Meu Painel para o Padrão
- Conteúdo relacionado

Introdução

Este documento descreve as etapas para personalizar e restaurar o painel do Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface gráfica do usuário (GUI) do SWA
- Acesso administrativo ao SWA.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Meu painel

Por padrão, a página inicial do SWA é Meu painel, que é a página exibida quando o usuário faz login no equipamento. Meu painel contém duas seções principais:

- Visão geral sobre o sistema
- Intervalo de tempo

Você pode personalizar várias propriedades dessas estatísticas e relatórios, como:

- Tipo de dados
- Intervalo de tempo
- Posição a ser mostrada na página
- Mostrar e ocultar conjuntos de dados

Exibição padrão

Por padrão, os relatórios e as estatísticas em Meu painel são:

- Visão geral sobre o sistema
  - Visão geral > Características de tráfego do Web Proxy
  - Visão geral > Utilização de recursos do sistema
- Intervalo de tempo

- Visão Geral > Atividade Total do Web Proxy
- Visão geral > Resumo do Web Proxy
- Visão geral > Resumo do monitor de tráfego da camada 4 (L4)
- Visão geral > Transações suspeitas
- Visão Geral > Sumário de Transações Suspeitas
- Principais categorias de URL: Total de transações
- Principais tipos de aplicativos: Total de transações
- Principais categorias de malware: Monitorado ou Bloqueado
- Principais usuários: Transações bloqueadas ou com aviso



Imagem - Painel SWA

Características de tráfego do Web Proxy

As Características de Tráfego do Web Proxy listam as estatísticas sobre a transação:

Média de transações por segundo no último minuto: XX
Largura de banda média (bps) no último minuto: XX
Tempo médio de resposta (ms) no último minuto: XX
Total de conexões atuais: XX

Utilização de recursos do sistema

A Utilização de Recursos do Sistema lista a Carga Geral da Unidade Central de Processamento (CPU), a Memória de Acesso Aleatório (RAM) e o uso do disco de Relatório/Log atuais.

Clique em System Status Details para alternar para a página System Status.

(Use a página Relatórios > Status do sistema para monitorar o Status do sistema. Esta página exibe o status atual e a configuração do Secure Web Appliance.)



Note: O valor de utilização da CPU mostrado nesta página e o valor da CPU mostrado na página Status do sistema podem diferir um pouco porque são lidos separadamente, em momentos diferentes.

Atividade total do Web Proxy

Você pode exibir a atividade de proxy da Web relatada pelos dispositivos da Web seguros que são gerenciados atualmente pelo dispositivo de gerenciamento de segurança.
Esta seção exibe o número real de transações e a data aproximada em que a atividade ocorreu no formato gráfico.

Você também pode exibir a porcentagem de atividades de proxy da Web suspeitas ou limpar a atividade de proxy, incluindo o número total de transações.

Resumo do Web Proxy

Permite exibir a porcentagem de atividades do Web Proxy suspeitas ou limpas.

Resumo do L4 Traffic Monitor

Você pode exibir qualquer tráfego L4 relatado pelos dispositivos da Web seguros que são atualmente gerenciados pelo dispositivo de gerenciamento de segurança, em formato gráfico.

Transações suspeitas

Você pode exibir as transações da Web que foram rotuladas como suspeitas pelo administrador em um formato gráfico.
Esta seção exibe o número real de transações e a data aproximada em que a atividade ocorreu, em formato gráfico.

Resumo de transações suspeitas

Você também pode exibir a porcentagem de transações bloqueadas ou avisadas que são suspeitas.

Você pode ver o tipo de transações que foram detectadas e bloqueadas e o número real de vezes que essa transação foi bloqueada.

Principais categorias de URL: Total de transações

Você pode exibir as principais categorias de URL visitadas no site em um formato gráfico.

Principais tipos de aplicativos: Total de transações

Você pode exibir os principais tipos de aplicativos bloqueados, que também incluem o nome do tipo de aplicativo real e o número de vezes que o aplicativo específico foi bloqueado, em formato gráfico.

Principais categorias de malware: Monitorado ou Bloqueado

Você pode exibir todas as categorias de malware que foram detectadas no formato gráfico.

Principais usuários: Transações bloqueadas ou com aviso

Você pode exibir os usuários reais que geraram as transações bloqueadas ou avisadas, no formato gráfico. Os usuários podem ser exibidos por endereço IP ou por nome de usuário.

Modificar intervalo de tempo

Para modificar a data do intervalo de tempo de Dia para Hora, Semana, 30 dias, Ontem:

Passo 1: Escolha Option (superior direito)

Passo 2: Escolha Performance.

Passo 3: Clique em Edit Preferences.

Passo 4: Altere Intervalo de tempo do relatório Exibido (padrão) para uma das opções disponíveis.

Etapa 5: Enviar. Não há necessidade de confirmar as alterações.

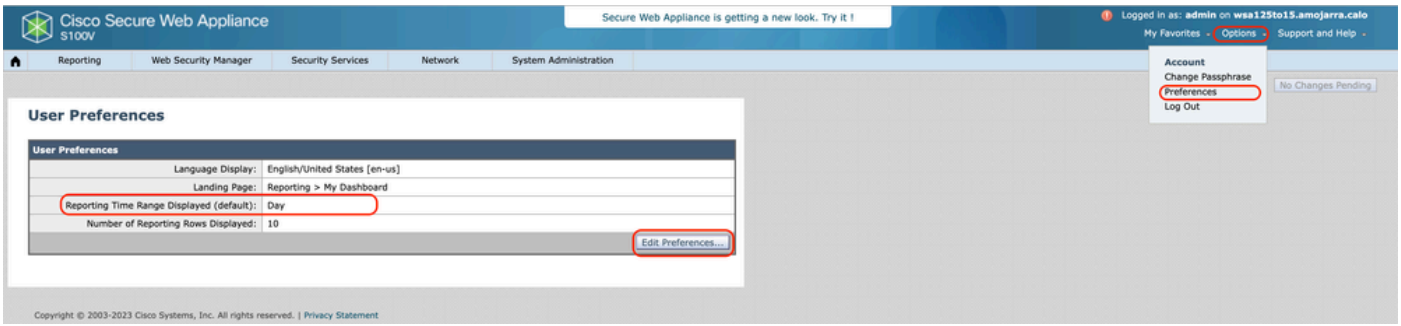


Imagem - Etapas para editar o intervalo de tempo padrão em Meu Painel

Modificar Conjuntos de Dados

Você pode adicionar e remover conjuntos de dados e relatórios na página Meu Painel. Use o sinal de adição (+) para adicionar outros relatórios e use o sinal de X na parte superior direita de cada relatório para removê-los.

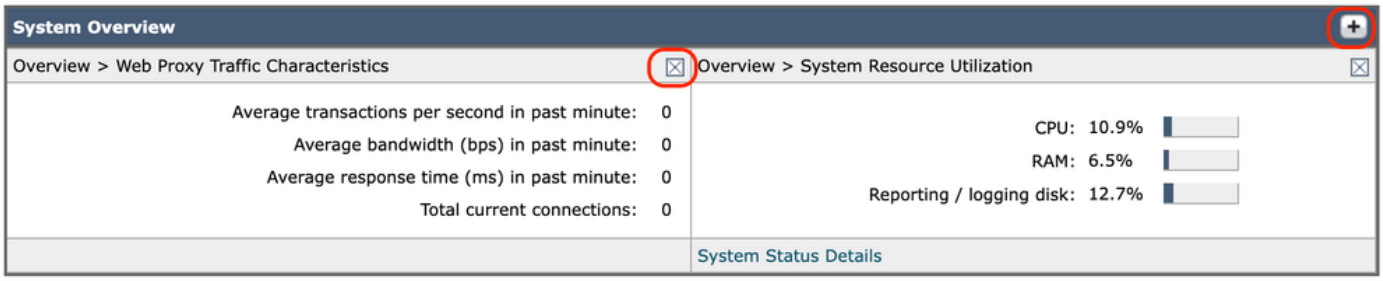


Imagem - Adicionar e remover relatórios em Meu painel.

Caution: As alterações entram em vigor assim que são alteradas. Não há necessidade de Enviar.

Alterar Design do Painel

Você pode alterar a ordem de cada conjunto de dados na página Meu painel. Clique na faixa azul na parte superior de cada relatório e altere o local do relatório.

Restaurar Meu Painel para o Padrão

Para restaurar o valor padrão do My-Dashboard, edite manualmente o arquivo de configuração, com estas etapas:

Passo 1: Na GUI, navegue até System Administrations.

Passo 2: Selecione Configuration File.

Passo 3: Faça o download do arquivo de configuração mais recente.

Note: Selecione Criptografar senhas nos arquivos de configuração.

Etapa 4: Modifique o arquivo XML removendo tudo entre <user_reports> e </user_reports>.

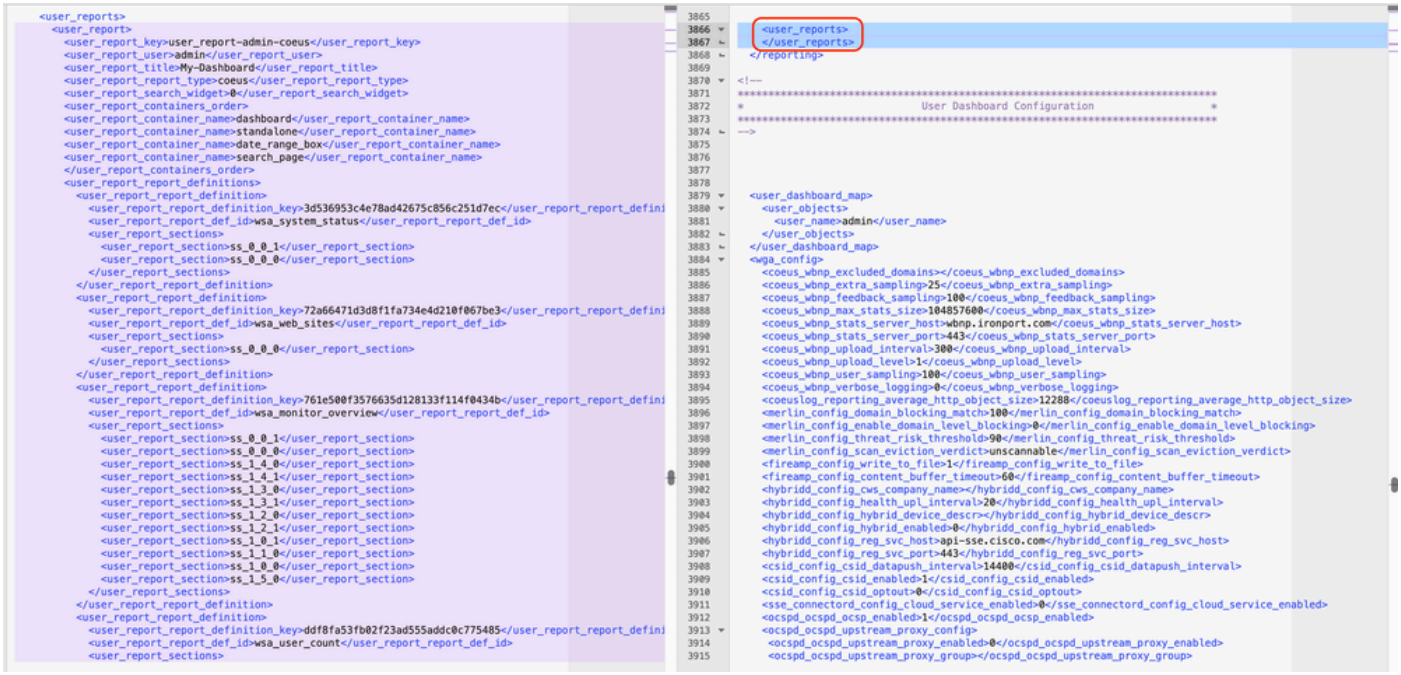


Imagem - Arquivos de configuração de exemplo com painel personalizado (direita) e arquivo de configuração padrão (esquerda).

Passo 5: Na página Arquivo de configuração, na seção Carregar configuração, selecione Carregar um arquivo de configuração do computador local.

Passo 6: Carregue o arquivo XML modificado.

Passo 7: Clique em Load e commit.

Conteúdo relacionado

Guia do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD (General Deployment, implantação geral)

Suporte - Suporte e downloads da Cisco - Documentação, ferramentas, casos - Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.