Configurar Restrição de Locatário do Microsoft O365 em SWA

Contents

Introdução

Este documento descreve o processo de configuração da Restrição de Usuário do Microsoft O365 no 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.

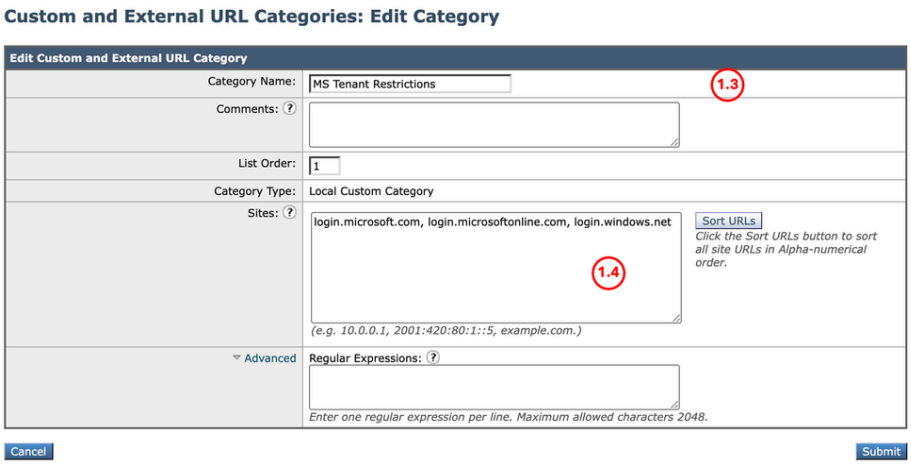
Componentes Utilizados

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.

Configuration Steps

Etapa 1. Crie uma Categoria	Etapa 1.1. Na GUI, navegue até Web Security Manager e escolha

de URL Personalizada para o site.	Custom and External URL Categories. Etapa 1.2. Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada. Etapa 1.3. Digite Nome para a nova categoria. Etapa 1.4. Defina esses URLs na seção Sites: `login.microsoft.com, login.microsoftonline.com, login.windows.net` Etapa 1.5.Envie as alterações.  Imagem - Categoria de URL personalizada Tip: Para obter mais informações sobre como configurar categorias de URL personalizadas, acesse: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
Etapa 2. Descriptografe o tráfego.	Etapa 2.1. Na GUI, navegue até o Web Security Manager e escolha Políticas de descriptografia Etapa 2.2. Clique em Add Policy. Etapa 2.3. Digite Nome para a nova política. Etapa 2.4. Selecione o Perfil de identificação ao qual você precisa que essa política se aplique.

Tip: Se você tiver ignorado as Autenticações para URLs da Microsoft e estiver configurando esta política para Todos os usuários, escolha: Todos os perfis de identificação > Todos os usuários

Etapa 2.5. Na seção Definição de membro de política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada.

Etapa 2.6. Selecione a Categoria de URL que foi criada na Etapa 1.

Etapa 2.7. Clique em Submit.

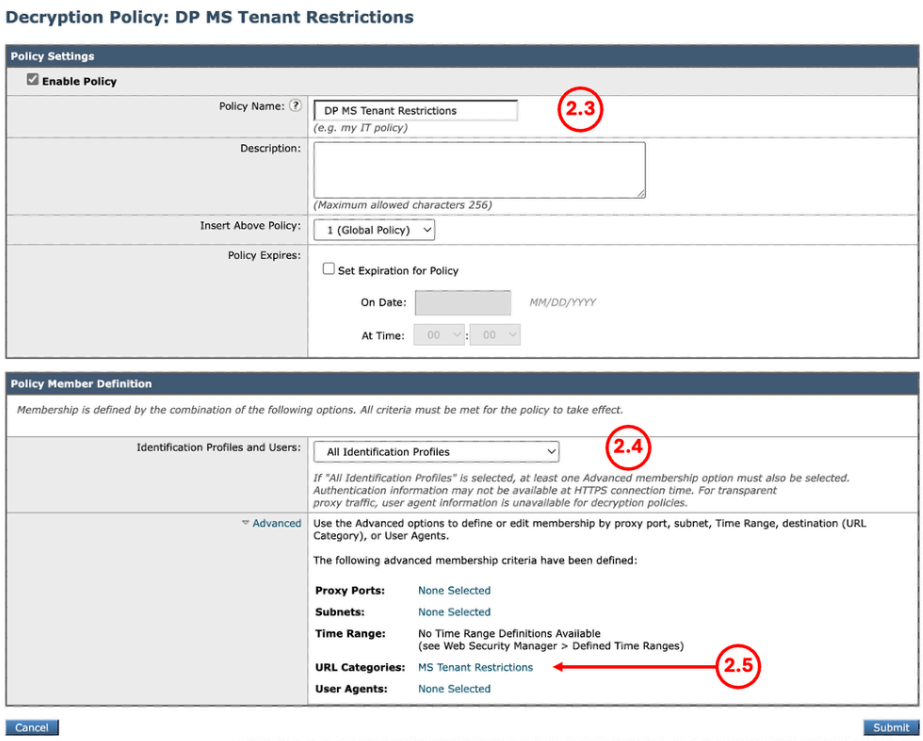
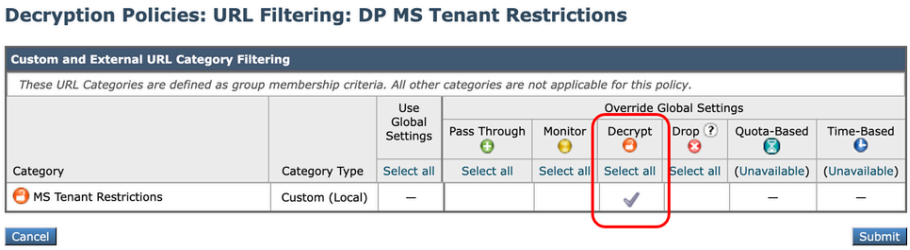
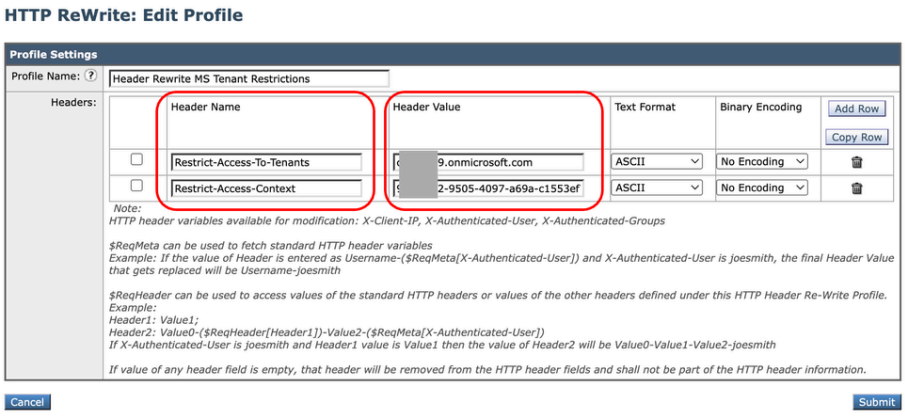


Imagem - Configurar política de descriptografia

Etapa 2.8. Na página Políticas de descriptografia, clique no link de Filtragem de URL para a nova política.

Imagem - Editar ação de filtragem de URL

	Etapa 2.9. Escolha Descriptografar como a ação para Categoria de URL Personalizada. Etapa 2.10. Clique em Submit.  Imagem - Descriptografar a categoria de URL personalizada
Etapa 3. Criar Perfil de Regravação HTTP.	Etapa 3.1. Na GUI, navegue até o Web Security Manager e escolha HTTP ReWrite Profiles. Etapa 3.2. Clique em Add Profile. Etapa 3.3. Digite Name para o novo perfil. Etapa 3.4. Use Restrict-Access-To-Tenants para o primeiro Nome do Cabeçalho. Etapa 3.5. Para a configuração Restrict-Access-To-Tenants, use um valor de <lista de espaços permitidos>, que deve ser uma lista separada por vírgulas dos espaços que os usuários têm permissão para acessar. Etapa 3.6. Clique em Adicionar linha Etapa 3.7. Use Restrict-Access-Context como o segundo Header Name. Etapa 3.8. Para a configuração Restrict-Access-Context, use o valor de um único ID de diretório para especificar o espaço que está definindo as restrições de espaço. Etapa 3.9. Clique em Submit.

	 Imagem - Adicionar perfil de regravação HTTP Tip: Para obter mais informações sobre Restrição de Locatário e como coletar suas informações de locatário, acesse: Microsoft Learn - Restringir o acesso a um espaço.
Etapa 4. Criar Política de Acesso.	Etapa 4.1. Na GUI, navegue até o Web Security Manager e escolha Access Policies Etapa 4.2. Clique em Add Policy. Etapa 4.3. Digite Nome para a nova política. Etapa 4.4. Selecione o Perfil de identificação ao qual você precisa que essa política se aplique. Tip: Se tiver ignorado as Autenticações para URLs da Microsoft e estiver configurando esta política para Todos os usuários, escolha: Todos os perfis de identificação > Todos os usuários. Etapa 4.5. Na seção Definição de membro de política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada. Etapa 4.6. Selecione a Categoria de URL que foi criada na Etapa 1. Etapa 4.7. Clique em Submit.

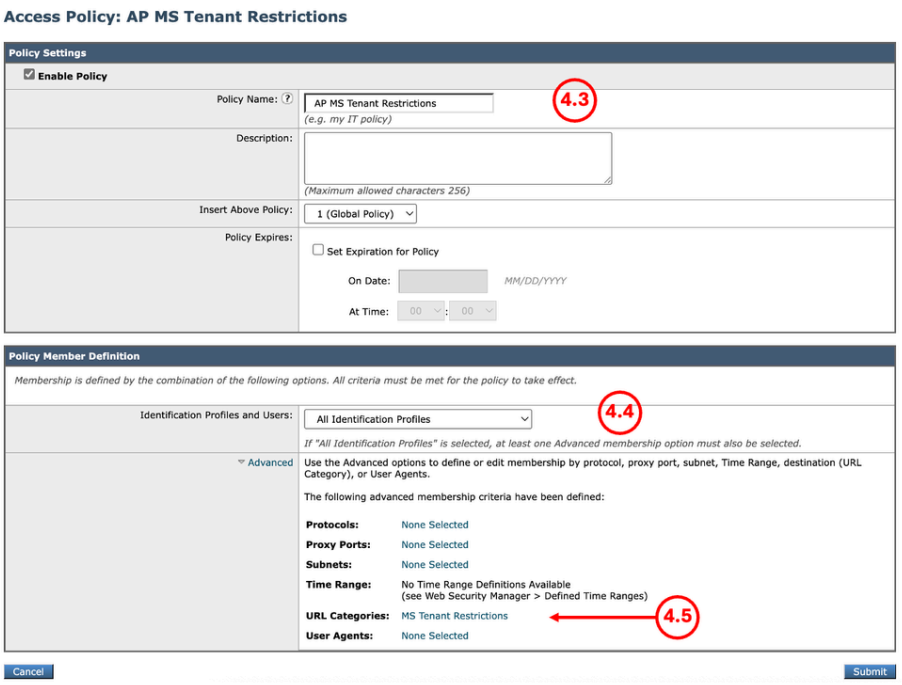


Imagem - Criar política de acesso

Etapa 4.8. Na página Access Policies, certifique-se de que a ação da filtragem de URL esteja definida como Monitor.

Etapa 4.9. Clique no link em HTTP ReWrite Profile para adicionar o Perfil do Cabeçalho HTTP a esta política.

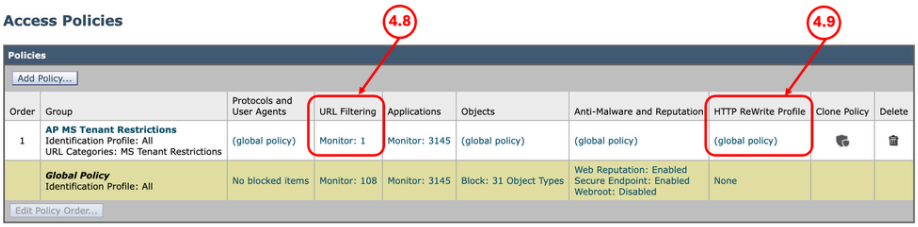


Imagem - Propriedades da política de acesso

Etapa 4.10. Escolha os perfis de regravação HTTP, criados na Etapa [3].

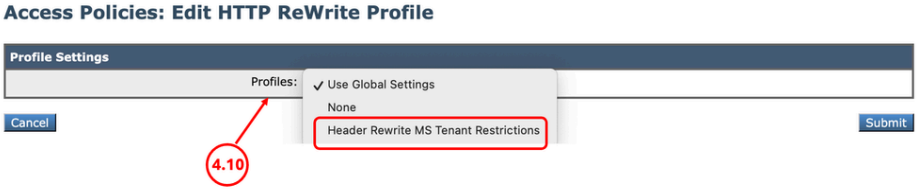


Imagem - Adicionar perfil de regravação HTTP

Etapa 4.11. Clique em Submit.

Etapa 4.12. Confirmar alterações.

Relatórios e registros

Logs

Você pode adicionar um campo personalizado aos logs de acesso ou aos logs W3C para exibir o nome do perfil de regravação do cabeçalho HTTP.

Especificador de Formato em Logs de Acesso	Campo Log nos Logs W3C	Descrição
%]	x-http-rewrite-profile-name	Nome do perfil de regravação do cabeçalho HTTP.

Relatórios

Você pode gerar o relatório de Rastreamento da Web para exibir os relatórios do tráfego pelo nome da política de acesso.

Siga estas etapas para gerar os relatórios:

Etapa 1. Na GUI, selecione Reporting e escolha Web Tracking.

Etapa 2. Escolha o intervalo de tempo desejado.

Etapa 3. Clique no link Avançado para pesquisar transações usando critérios avançados.

Etapa 4. Na seção Política, selecione Filtrar por política e digite o nome da Política de acesso que foi criada anteriormente.

Etapa 5. Clique em Pesquisar para revisar o relatório.

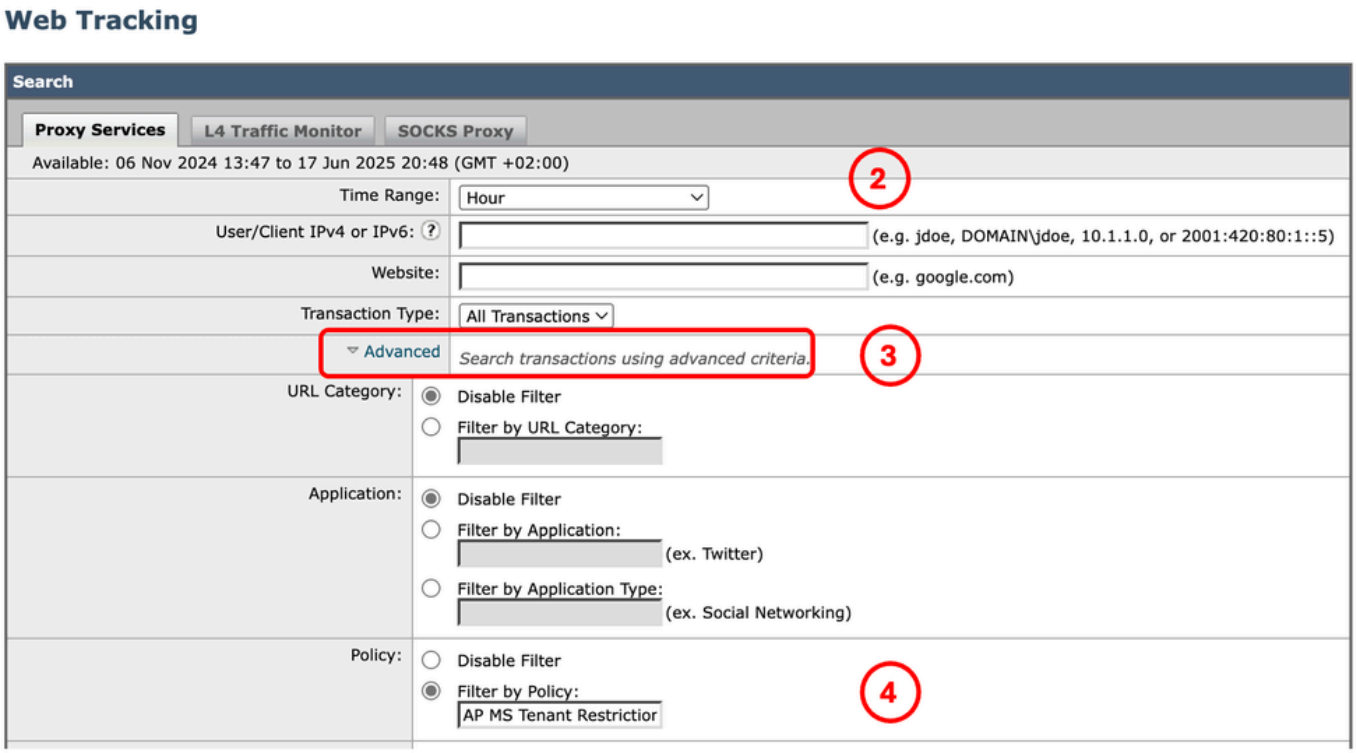


Imagem - Relatório de rastreamento da Web

Informações Relacionadas

- Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance
- Guia de instalação do Cisco Secure Email and Web Virtual Appliance
- Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco
- Use as práticas recomendadas de dispositivos da Web seguros
- Configurar firewall para dispositivo seguro da Web
- Configurar certificado de descriptografia no aplicativo da Web seguro
- Configurar e solucionar problemas de SNMP em SWA
- Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server
- Habilitar canal/vídeo específico do YouTube e bloquear o restante do YouTube no SWA
- Entender o formato do registro de acesso HTTPS no Secure Web Appliance
- Acessar logs do dispositivo da Web seguro
- Ignorar autenticação no Secure Web Appliance
- Bloquear o tráfego no Secure Web Appliance
- Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance

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.