

Configurar o Secure Web Appliance para permitir acesso de convidados

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Visão geral do cenário](#)

[Configuration Steps](#)

[Etapa 1. Criar Perfil de Identificação.](#)

[Etapa 2. \(Opcional\) Criar as categorias de URL personalizadas para URLs permitidas e bloqueadas](#)

[Etapa 3. Criar política decriptografia para dispositivos gerenciados](#)

[Etapa 4. Criar política decriptografia para dispositivos não gerenciados](#)

[Etapa 5. Criar política de acesso para dispositivos gerenciados](#)

[Etapa 6. Criar política de acesso para dispositivos não gerenciados](#)

[Etapa 7. \(Opcional\) Criar política de segurança de dados da Cisco para dispositivos gerenciados](#)

[Etapa 8. \(Opcional\) Criar política de segurança de dados da Cisco para dispositivos não gerenciados](#)

[Etapa 9. Salvando as Alterações](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve as etapas para permitir que os usuários que não instalaram o certificado decriptografia acessem a Internet via Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- SWA físico ou virtual instalado.
- Licença ativada ou instalada.
- O assistente de instalação foi concluído.
- Acesso administrativo à interface gráfica do usuário (GUI) do 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.

Visão geral do cenário

Este artigo aborda um cenário de controle de acesso à rede dentro da sub-rede Wi-Fi 10.10.10.0/24. O ambiente consiste em dois grupos de usuários distintos que exigem políticas de segurança e acesso diferentes:

- Dispositivos gerenciados: Laptops fornecidos pela empresa que são totalmente autenticados e têm o certificado decriptografia SWA instalado. Esses dispositivos são confiáveis e geralmente estão sujeitos às políticas de acesso corporativas padrão.
- Dispositivos não gerenciados/convidados: Laptops pessoais e dispositivos móveis não autenticados e sem o certificado decriptografia SWA.

Objetivo:

A empresa tem como objetivo implementar políticas restritivas de acesso à Web para dispositivos não gerenciados, limitando sua conectividade a um subconjunto específico de URLs permitidos, garantindo que os recursos corporativos permaneçam seguros.



Note: Como o Certificado de descriptografia não é confiável nos dispositivos não gerenciados, você não pode descriptografar o tráfego HTTPS e a ação deve ser definida para passar.

Configuration Steps

Etapa 1. Criar Perfil de Identificação.	Etapa 1.1. Na GUI do SWA, navegue até o Web Security Manager e selecione Identification Profile. Etapa 1.2. Clique em Add Identification Profile. Etapa 1.3. Defina um Nome para o Perfil. Etapa 1.4. (Opcional) Defina a Descrição. Etapa 1.5. Selecione Authenticate Users em Identification and Authentication. Etapa 1.6. Escolha o realm do Active Directory em Selecionar um Realm ou Sequência. Etapa 1.7. Em Select a Scheme, selecione os
---	---

protocolos de autenticação desejados.



Tip: Não escolha Basic Authentication na lista Select a Scheme.

Etapa 1.8. Marque a caixa de seleção Suporte a privilégios de convidado.

Etapa 1.9. (Opcional) Dependendo do seu design, você pode habilitar o Substituto, habilitando Aplicar as mesmas configurações de substituto para solicitações de encaminhamento explícitas.



Caution: Como não é possível descriptografar o tráfego, na implantação transparente, não selecione Cookie persistente ou Cookie de sessão.

Etapa 1.10. Defina a sub-rede do endereço IP em, Definir membros por sub-rede.

Etapa 1.11. Enviar e confirmar as alterações.

Identification Profiles: WiFi IDP

Client / User Identification Profile Settings

☒ Enable Identification Profile

Name: ? WiFi IDP (e.g. my IT Profile)

Description: ? Identification Profile for WiFi Devices (Maximum allowed characters 256)

Insert Above: 1 (Global Profile) v

User Identification Method

Identification and Authentication: ? Authenticate Users

Authentication Realm: ? Select a Realm or Sequence: ? ADDS

Select a Scheme: ? Use Kerberos or NTLMSSP (Scheme setting applies to HTTP/HTTPS only.)

If a user fails authentication: ? ☒ Support Guest privileges ?

Authorization of specific users and groups is defined in subsequent policy layers (see Web Security Manager > Decryption Policies, Routing Policies and Access Policies).

Authentication Surrogates: ?

☒ IP Address

☐ Persistent Cookie

☐ Session Cookie

☒ Apply same surrogate settings to explicit forward requests

If this option is not selected, no surrogates will be used with HTTP/HTTPS explicit forward requests, and NTLM credential caching will not be available to these requests. In addition, re-authentication will not be available for Kerberos.

Membership Definition

Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.

Define Members by Subnet: ? 10.10.10.0/24 (examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1:1:5, 2000:db8:1-2000:db8:1:10)

Define Members by Protocol: ? ☒ HTTP/HTTPS

> Advanced Define additional group membership criteria.

Cancel Submit

Imagem - Definir o perfil de identificação

Etapa 2. (Opcional) Criar as categorias de URL personalizadas para URLs permitidas e bloqueadas

Etapa 2.1. Na GUI, navegue até Web Security Manager e escolha Categorias de URL personalizadas e externas.

Etapa 2.2. Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada.

Etapa 2.3. Digite o nome da nova categoria.

Etapa 2.4. Defina o domínio e/ou subdomínios dos sites que você deseja bloquear o acesso.

Etapa 2.5. Envie as alterações.

Etapa 2.6. Use as mesmas etapas para criar uma categoria de URL para o site ao qual você está permitindo o acesso.

The image displays two screenshots of the 'Custom and External URL Categories: Edit Category' web interface. Both screenshots show the 'Edit Custom and External URL Category' form. In the top screenshot, the 'Category Name' is 'Blocked WiFi Access' and the 'Sites' field contains 'example.com'. In the bottom screenshot, the 'Category Name' is 'Allowed WiFi Access' and the 'Sites' field contains 'cisco.com'. Red circles with numbers 2.3 and 2.4 point to the 'Category Name' and 'Sites' fields respectively in both screenshots. The 'Sort URLs' button is also visible in both screenshots.

Imagem - Definir categoria de URL personalizada

Etapa 3. Criar política de descryptografia para dispositivos gerenciados

Etapa 3.1. Na GUI, navegue até Web Security Manager e escolha Políticas de descryptografia

Etapa 3.2. Clique em Add Policy.

Etapa 3.3. EnterName para a nova política.

Etapa 3.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 3.5. Selecione o Perfil de identificação que foi criado na Etapa 1.

Etapa 3.6. Selecione All Authenticated Users.

Etapa 3.7. Clique em Enviar.

Decryption Policy: WiFi Users DP

Policy Settings

☒ **Enable Policy**

Policy Name:

Description:

Insert Above Policy:

Policy Expires: ☐ Set Expiration for Policy

On Date:

At Time:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

Identification Profile:

Authorized Users and Groups: ☒ All Authenticated Users

☐ Selected Groups and Users (7)
Groups: No groups entered
Users: No users entered

☐ Guests (users failing authentication)

Advanced: ☐ Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (See Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Criar política de descryptografia para dispositivos gerenciados

Etapa 3.8. Na página Políticas de descryptografia, clique no link de Filtragem de URL para a nova política.

Etapa 3.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 3.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

Etapa 3.11. Clique em Submit

Decryption Policies: URL Filtering: WiFi Users DP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	☒	☒	☒	☒	☒	☒	☒
Select Custom Categories...								

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Override Global Settings					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Adult	☒	☒	☒	☒	☒	☒	☒
Advertisements	☒	☒	☒	☒	☒	☒	☒
Alcohol	☒	☒	☒	☒	☒	☒	☒
Arts	☒	☒	☒	☒	☒	☒	☒
Astronomy	☒	☒	☒	☒	☒	☒	☒
Auctions	☒	☒	☒	☒	☒	☒	☒
Business and Industry	☒	☒	☒	☒	☒	☒	☒
Chat and Instant Messaging	☒	☒	☒	☒	☒	☒	☒

Imagem - Configurar Ação para Política de Descryptografia

Etapa 4. Criar política de

Etapa 4.1. Na GUI, navegue até Web Security Manager e escolha Políticas de descryptografia

descriptografia para dispositivos não gerenciados

Etapa 4.2. Clique em Add Policy.

Etapa 4.3. EnterName para a nova política.

Etapa 4.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 4.5. Selecione o Perfil de identificação que foi criado na Etapa 1.

Etapa 4.6. Selecione Convidados (usuários com falha na autenticação).

Etapa 4.7. Clique em Submit.

Decryption Policy: WiFi Guest DP

Policy Settings

☒ Enable Policy

Policy Name: WiFi Guest DP
(e.g. my IT policy)

Description: (Maximum allowed characters 256)

Insert Above Policy: 2 (Global Policy)

Policy Expires: ☐ Set Expiration for Policy
On Date: MM/DD/YYYY
At Time: HH:MM:SS

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: WiFi IDP

Authorized Users and Groups: ☐ All Authenticated Users
☐ Selected Groups and Users (?)
Groups: No groups entered
Users: No users entered
☒ Guests (users failing authentication)

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected
Subnets: None Selected
Time Range: No Time Range Definitions Available
(Use Web Security Manager > Defined Time Ranges)
URL Categories: None Selected
User Agents: None Selected

Cancel Submit

Criar política de descriptografia para dispositivos não gerenciados

Etapa 4.8. Na página Políticas de descriptografia, clique no link de Filtragem de URL para a nova política.

Etapa 4.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 4.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.



Note: Não use Descriptografar como a ação, já que o certificado de descriptografia SWA não é



confiável nos dispositivos não gerenciados.

Decryption Policies: URL Filtering: WiFi Guest DP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Blocked WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Cancel Submit

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Use Global Settings	Override Global Settings					
		Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
Adult	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Advertisements	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Alcohol	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Arts	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Astrotology	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Auctions	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Business and Industry	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Cancel Submit

Imagem - Ação de descryptografia para dispositivos não gerenciados

Etapa 4.11. Role para baixo na seção URLs sem categoria e escolha a ação apropriada.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs: Drop

Default Action for Update Categories: Most Restrictive

Cancel Submit

Imagem - URLs sem categoria



Tip: Para a perspectiva de segurança, é melhor definir a ação como Eliminar, caso qualquer URL precise de acesso, você pode adicioná-los na Categoria de URL personalizada atribuída à Política.

Etapa 4.12. Clique em Submit

Etapa 5. Criar política de acesso para dispositivos gerenciados

Etapa 5.1. Na GUI, navegue até Web Security Manager e escolha Access Policies

Etapa 5.2. Clique em Add Policy.

Etapa 5.3. EnterName para a nova política.

Etapa 5.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 5.5. Selecione o Perfil de identificação que foi criado na Etapa 1.

Etapa 5.6. Selecione All Authenticated Users.

Etapa 5.7.Clique em Submit.

Access Policy: WiFi Users AP

Policy Settings

☒ Enable Policy

Policy Name: WiFi Users AP
(e.g. my IT policy)

Description: (Maximum allowed characters 256)

Insert Above Policy: 1 (WiFi Guest AP)

Policy Expires: ☐ Set Expiration for Policy
On Date: MM/DD/YYYY
At Time: HH:MM:SS

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: WiFi IDP

Authorized Users and Groups: ☒ All Authenticated Users
☐ Selected Groups and Users (Groups: No groups entered, Users: No users entered)
☐ Guests (users failing authentication)

Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile WiFi IDP

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: None Selected

User Agents: None Selected

Cancel Submit

Imagem - Política de acesso para dispositivos gerenciados

Etapa 5.8. Na página Access Policies, clique no link de URL Filtering para a nova política.

Etapa 5.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 5.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

Access Policies: URL Filtering: WiFi Users AP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category: Allowed WiFi Access

Category Type: Custom (Local)

Global Settings: ☒ Use Global Settings

Block: ☒ Redirect: ☐ Allow: ☐ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Select Custom Categories...

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category: Adult

Global Settings: ☒ Use Global Settings

Block: ☒ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Advertisements: ☐ Block: ☐ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Alcohol: ☐ Block: ☐ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Arts: ☐ Block: ☐ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Astrology: ☐ Block: ☐ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Auctions: ☐ Block: ☐ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Business and Industry: ☐ Block: ☐ Monitor: ☐ Warn: ☐ Quota-Based: ☐ Time-Based: ☐

Imagem - Filtragem de URL de política de acesso para dispositivos gerenciados

Etapa 5.11. Clique em Submit.

Etapa 6.1. Na GUI, navegue até Web Security Manager e escolha Access Policies

Etapa 6.2. Clique em Add Policy.

Etapa 6.3. EnterName para a nova política.

Etapa 6.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 6.5. Selecione o Perfil de identificação que foi criado na Etapa 1.

Etapa 6.6. Selecione Convidados (usuários com falha na autenticação).

Etapa 6.7. Clique em Submit.

Etapa 6. Criar política de acesso para dispositivos não gerenciados

Access Policy: WiFi Guest AP

Policy Settings

☒ Enable Policy

Policy Name: WiFi Guest AP
(e.g. my IT policy)

Description:

Insert Above Policy: 2 (Global Policy)

Policy Expires: ☐ Set Expiration for Policy
On Date: MM/DD/YYYY
At Time: HH:MM:SS

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users: Select One or More Identification Profiles

Identification Profile: WiFi IDP

Authorized Users and Groups: ☐ All Authenticated Users
☐ Selected Groups and Users (?)
Groups: No groups entered
Users: No users entered
☒ Guests (users failing authentication)

Advanced

Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Protocols: HTTP/HTTPS/FTP over HTTP in Identification Profile WiFi IDP
Proxy Ports: None Selected
Schemers: None Selected
Time Ranges: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)
URL Categories: None Selected
User Agents: None Selected

Cancel Submit

Imagem - Política de acesso para dispositivos não gerenciados

Etapa 6.8. Na página Access Policies, clique no link de URL Filtering para a nova política.

Etapa 6.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 6.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

Access Policies: URL Filtering: WiFi Guest AP

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Use Global Settings: ☐ Override Global Settings: ☐

Category	Category Type	Block	Redirect	Allow	Monitor	Warn	Quota-Based	Time-Based
Allowed WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	Select all	Select all
Blocked WiFi Access	Custom (Local)	Select all	Select all	Select all	Select all	Select all	Select all	Select all

6.9 6.10

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Use Global Settings: ☐ Override Global Settings: ☐

Category	Block	Monitor	Warn	Quota-Based	Time-Based
Adult	Select all	Select all	Select all	Select all	Select all
Advertisements	Select all	Select all	Select all	Select all	Select all
Alcohol	Select all	Select all	Select all	Select all	Select all
Arts	Select all	Select all	Select all	Select all	Select all
Astrology	Select all	Select all	Select all	Select all	Select all
Auctions	Select all	Select all	Select all	Select all	Select all
Business and Industry	Select all	Select all	Select all	Select all	Select all
Chat and Instant Messaging	Select all	Select all	Select all	Select all	Select all

Imagem - Filtragem de URL de política de acesso para dispositivos não gerenciados

Etapa 6.11. Role para baixo na seção URLs sem categoria e escolha a ação apropriada.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs:

Default Action for Update Categories:

6.11

Imagem - URLs sem categoria da política de acesso

 **Tip:** Para a perspectiva de segurança, é melhor definir a ação como Bloquear, caso qualquer URL precise de acesso, você pode adicioná-los na Categoria de URL personalizada atribuída à política.

Etapa 6.12. Clique em Enviar

Etapa 7. (Opcional) Criar a política de segurança de dados da Cisco para dispositivos gerenciados

 **Note:** Se você não quiser filtrar o tráfego de carregamento para dispositivos gerenciados, ignore esta etapa.

Etapa 7.1. Na GUI, navegue até Web Security Manager e escolha Cisco Data Security.

Etapa 7.2. Clique em Add Policy.

Etapa 7.3. EnterName para a nova política.

Etapa 7.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 7.5. Selecione o Perfil de identificação que foi criado na Etapa 1.

Etapa 7.6. Selecionar Todos os Usuários Autenticados.

Etapa 7.7.Clique em Submit.

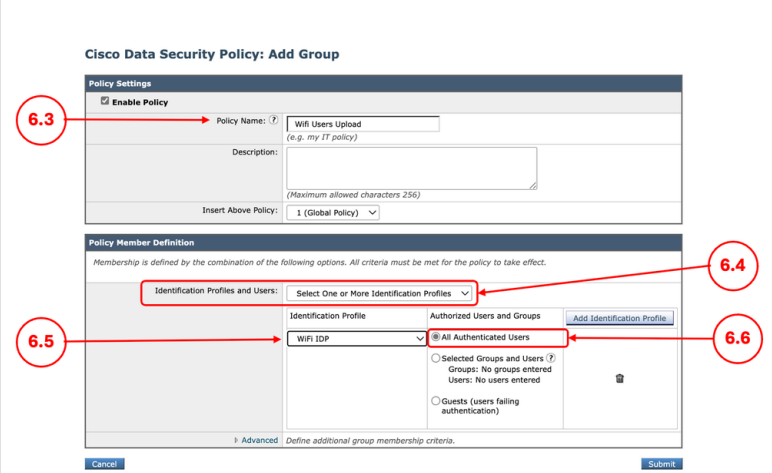


Imagem - Política de segurança de dados da Cisco para dispositivos gerenciados

Etapa 7.8. Na página Cisco Data Security Policies , clique no link de URL Filtering para a nova política.

Etapa 7.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 7.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

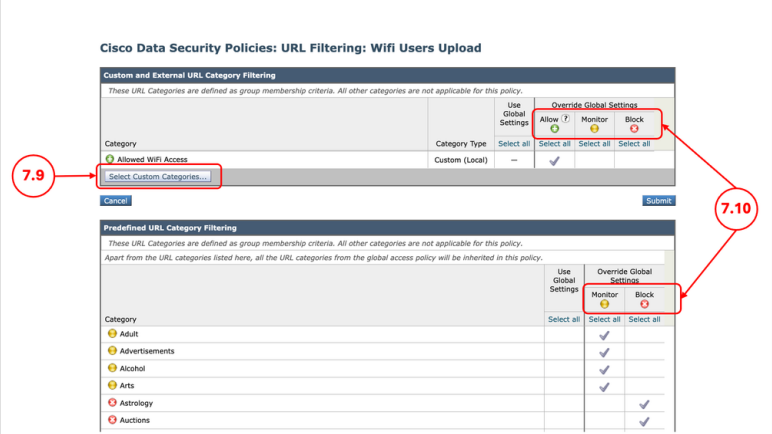


Imagem - Ação de carregamento para dispositivos gerenciados

Etapa 7.11. Clique em Submit.

Etapa 8. (Opcional) Criar a política de segurança de dados da Cisco para dispositivos não gerenciados

Etapa 8.1. Na GUI, navegue até Web Security Manager e escolha Cisco Data Security.
Etapa 8.2.Clique em Add Policy.



Note: Se você não quiser filtrar o tráfego de carregamento para dispositivos não gerenciados, ignore esta etapa.

Etapa 8.3. EnterName para a nova política.

Etapa 8.4. Escolha Selecionar um ou mais perfis de identificação no menu suspenso Perfis de identificação e usuários.

Etapa 8.5. Selecione o Perfil de identificação que foi criado na Etapa 1.

Etapa 8.6. Selecionar Todos os Usuários Autenticados.

Etapa 8.7. Clique em Enviar.

Imagem - Política de segurança de dados da Cisco para dispositivos não gerenciados

Etapa 8.8. Na página Cisco Data Security Policies , clique no link de URL Filtering para a nova política.

Etapa 8.9. (Opcional) Você pode adicionar qualquer Categoria de URL personalizada clicando em Selecionar categorias personalizadas e escolhendo Incluir na política na frente dos nomes de categoria

Etapa 8.10. Configure a Ação para cada Filtragem de Categoria de URL Personalizada e Externa e Filtragem de Categoria de URL Predefinida.

Cisco Data Security Policies: URL Filtering: WiFi Guest Upload

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Select all	Override Global Settings		
			Use Global Settings	Allow	Monitor
Allowed WiFi Access	Custom (Local)	Select all	☒	☐	☐
Blocked WiFi Access	Custom (Local)	Select all	☐	☒	☒

Select Custom Categories...

Cancel

Submit

Predefined URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Apart from the URL categories listed here, all the URL categories from the global access policy will be inherited in this policy.

Category	Select all	Use Global Settings	Override Global Settings	
			Monitor	Block
Adult	Select all	☐	☒	☒
Advertisements	Select all	☐	☒	☒
Alcohol	Select all	☐	☒	☒
Arts	Select all	☐	☒	☒
Astrology	Select all	☐	☒	☒
Auctions	Select all	☐	☒	☒

Imagem - Ação de carregamento para dispositivos não gerenciados

Etapa 8.11. Role para baixo na seção URLs sem categoria e escolha a ação apropriada.

Uncategorized URLs

Specify an action for urls that do not match any category.

Uncategorized URLs:

Block

Default Action for Update Categories:

Use Global Setting (Least Restrictive)

Cancel

Submit

Imagem - Ação de Carregamento para URLs Não Categorizados



Tip: Para a perspectiva de segurança, é melhor definir a ação como Bloquear, caso qualquer URL precise de acesso, você pode adicioná-los na Categoria de URL personalizada atribuída à política.

Etapa 8.12. Clique em Enviar

Etapa 9. Salvando as Alterações

Etapa 9.1. Confirmar as alterações

Informações Relacionadas

- [Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - LD \(implantação limitada\) - Solução de problemas...](#)
- [Bloquear download de arquivo executável em SWA](#)
- [Bloquear tráfego de upload no dispositivo da Web seguro](#)
- [Bloquear o tráfego no Secure Web Appliance](#)
- [Ignorar autenticação no Secure Web Appliance](#)
- [Configurar Restrição de Locatário do Microsoft O365 em SWA](#)
- [Configurar a configuração inicial do 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.