Omitir autenticación en dispositivo web seguro

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Autenticación exenta

Métodos para Eximir la Autenticación en Cisco SWA

Pasos para omitir la autenticación

Información Relacionada

Introducción

En este documento se describen los pasos para eximir la autenticación en el dispositivo web seguro (SWA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA.

Cisco recomienda tener instaladas estas herramientas:

- SWA físico o virtual
- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Autenticación exenta

La exención de la autenticación para determinados usuarios o sistemas en el SWA de Cisco puede ser crucial para mantener la eficacia operativa y cumplir los requisitos específicos. En primer lugar, algunos usuarios o sistemas requieren un acceso ininterrumpido a los recursos o servicios críticos que podrían verse obstaculizados por los procesos de autenticación. Por ejemplo, los sistemas automatizados o las cuentas de servicio que realizan actualizaciones o copias de seguridad periódicas necesitan un acceso sin problemas sin los retrasos o los posibles fallos que introducen los mecanismos de autenticación.

Además, hay situaciones en las que el proveedor de servicios web recomienda no utilizar un proxy para acceder a su servicio. En estos casos, la exención de la autenticación garantiza el cumplimiento de las directrices del proveedor y mantiene la fiabilidad del servicio. Además, para bloquear de forma efectiva el tráfico de determinados usuarios, a menudo es necesario eximirlos primero de la autenticación y, a continuación, aplicar las políticas de bloqueo adecuadas. Este enfoque permite un control preciso de los permisos de acceso.

En algunos casos, el servicio web al que se accede es de confianza y universalmente aceptable, como las actualizaciones de Microsoft. La exención de la autenticación para dichos servicios simplifica el acceso de todos los usuarios. Además, hay situaciones en las que el sistema operativo o la aplicación del usuario no admite el mecanismo de autenticación configurado en el SWA, por lo que es necesario realizar una derivación para garantizar la conectividad.

Por último, los servidores con direcciones IP fijas que no tienen inicios de sesión de usuario y tienen un acceso a Internet limitado y de confianza no requieren autenticación, ya que sus patrones de acceso son predecibles y seguros.

Al exceptuar estratégicamente la autenticación para estos casos, las organizaciones pueden equilibrar las necesidades de seguridad con la eficacia operativa.

Métodos para Eximir la Autenticación en Cisco SWA

La exención de la autenticación en SWA se puede lograr a través de varios métodos, cada uno adaptado a escenarios y requisitos específicos. A continuación se indican algunas formas comunes de configurar excepciones de autenticación:

- Dirección IP o máscara de subred: uno de los métodos más sencillos consiste en eximir de la autenticación a direcciones IP específicas o subredes enteras. Esto resulta especialmente útil para servidores con direcciones IP fijas o segmentos de red de confianza que requieren acceso ininterrumpido a Internet o a recursos internos. Al especificar estas direcciones IP o máscaras de subred en la configuración SWA, puede asegurarse de que estos sistemas omiten el proceso de autenticación.
- Puertos de Proxy: Puede configurar el SWA para eximir el tráfico basado en puertos de proxy específicos. Esto es útil cuando ciertas aplicaciones o servicios utilizan puertos designados para la comunicación. Mediante la identificación de estos puertos, puede configurar el SWA para que omita la autenticación del tráfico en estos puertos, garantizando un acceso sin problemas para las aplicaciones o servicios relevantes.

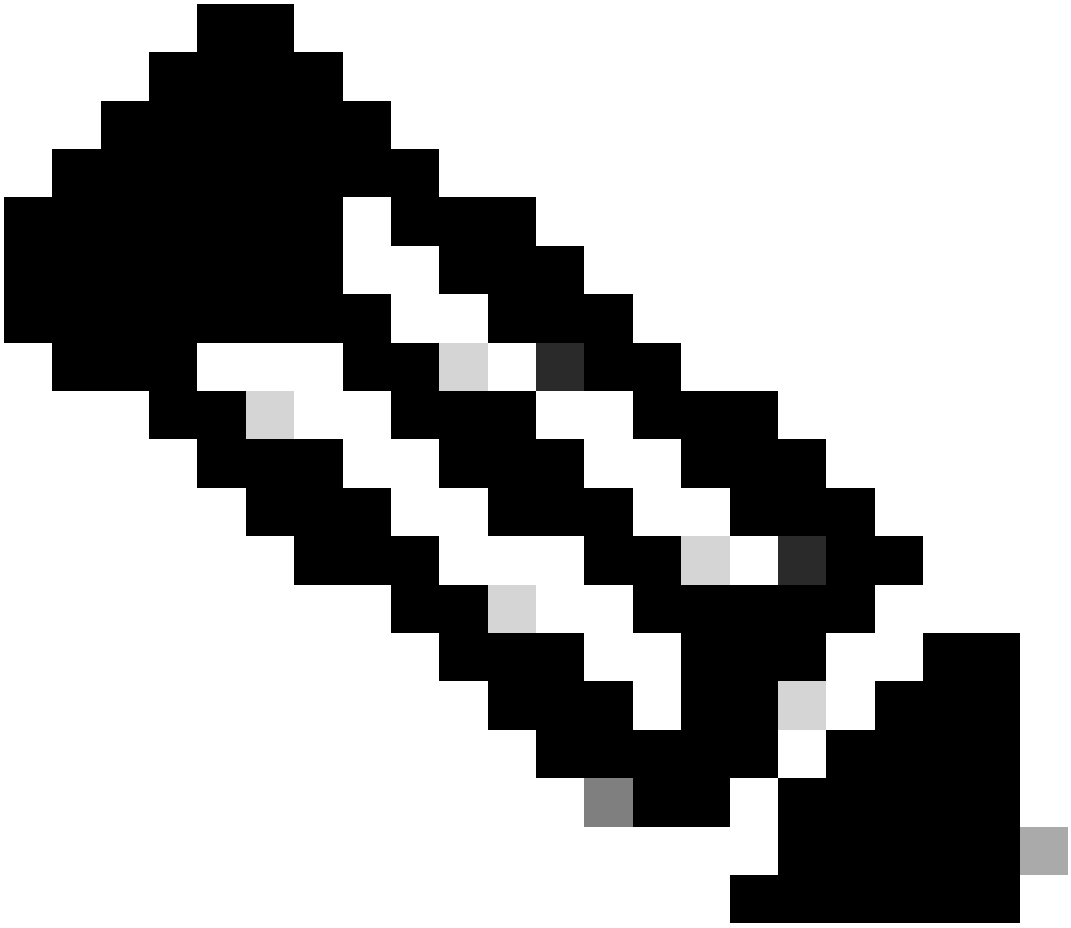
- Categorías de URL: Otro método consiste en eximir la autenticación basada en categorías de URL. Esto puede incluir categorías predefinidas de Cisco y categorías de URL personalizadas que defina en función de las necesidades específicas de su organización. Por ejemplo, si determinados servicios web, como las actualizaciones de Microsoft, se consideran de confianza y universalmente aceptables, puede configurar el SWA para omitir la autenticación para estas categorías de URL específicas. Esto garantiza que todos los usuarios puedan acceder a estos servicios sin necesidad de autenticación.
- Agentes de usuario: la exención de la autenticación basada en agentes de usuario es útil cuando se trata de aplicaciones o dispositivos específicos que no admiten los mecanismos de autenticación configurados. Al identificar las cadenas de agentes de usuario de estas aplicaciones o dispositivos, puede configurar el SWA para que omita la autenticación del tráfico que se origina en ellas, lo que garantiza una conectividad perfecta.

.

Pasos para omitir la autenticación

Estos son los pasos para crear un perfil de identificación que eximir de la autenticación:

Paso 1. En GUI, elija Web Security Manager y, a continuación, haga clic en Perfiles de identificación.
Paso 2. Haga clic en Add Profile para agregar un perfil.
Paso 3. Utilice la casilla de verificación Enable Identification Profile para habilitar este perfil o para deshabilitarlo rápidamente sin eliminarlo.
Paso 4. Asigne un nombre de perfil único.
Paso 5. (Opcional) Agregar descripción.
Paso 6. En la lista desplegable Insertar, elija dónde debe aparecer este perfil en la tabla.

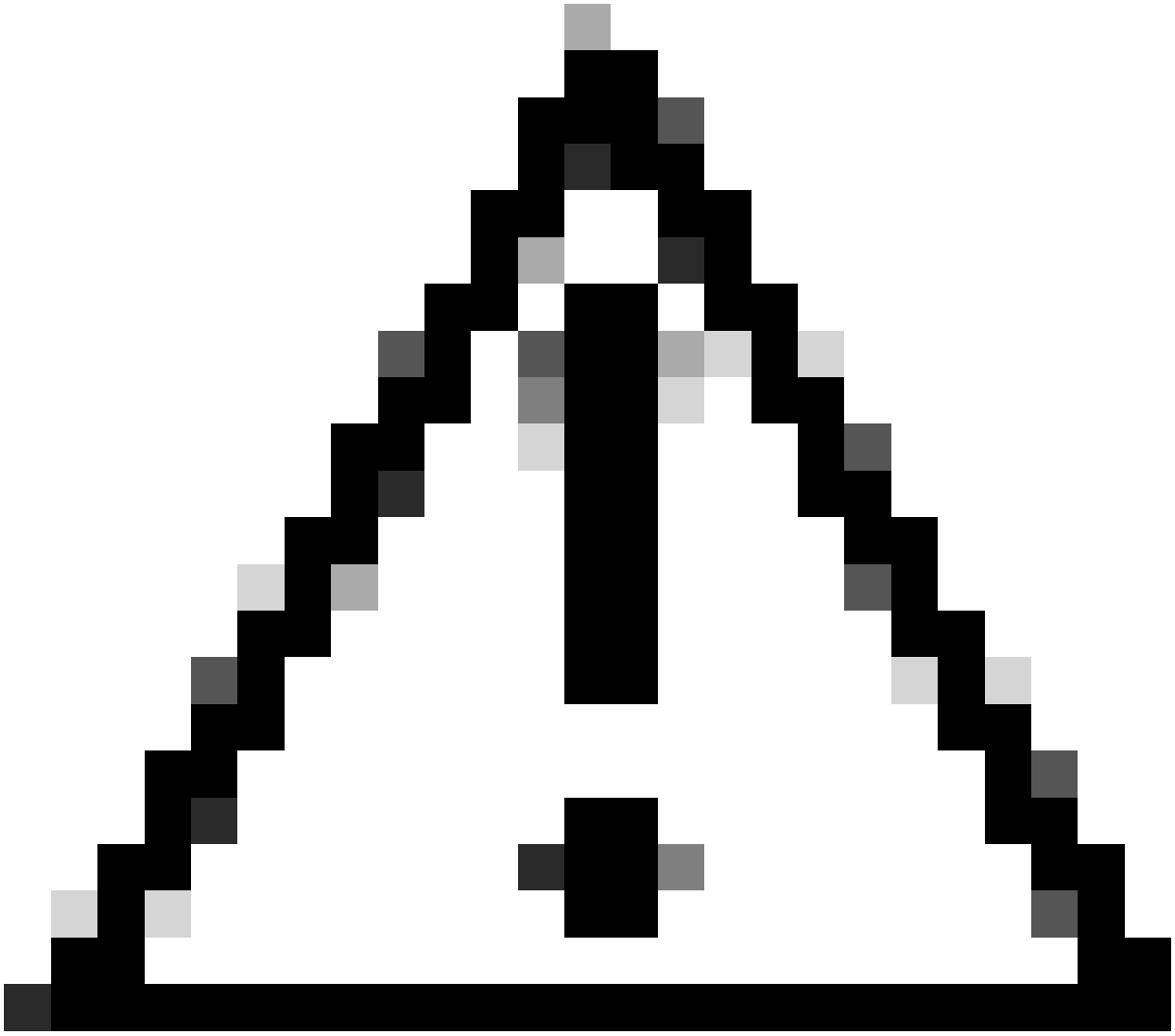


Nota: los perfiles de identificación de puestos que no requieren autenticación se encuentran en la parte superior de la lista. Este enfoque reduce la carga en el SWA, minimiza la cola de autenticación y da como resultado una autenticación más rápida para otros usuarios.

Paso 7. En la sección Método de identificación de usuario, elija Exento de autenticación/identificación.

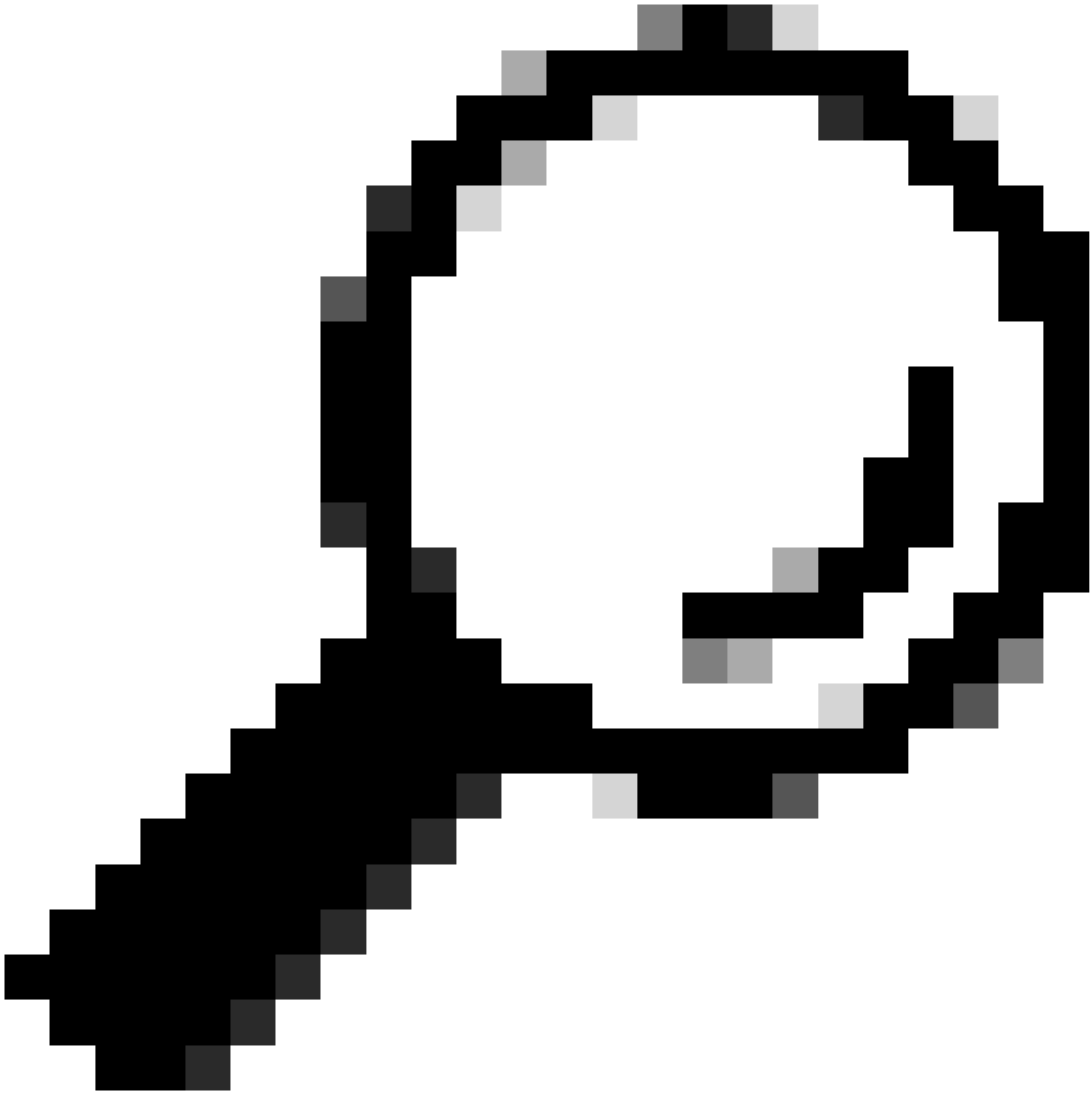
Paso 8. En Definir miembros por subred, introduzca las direcciones IP o las subredes que debe aplicar este perfil de identificación. Puede utilizar direcciones IP, bloques de enrutamiento entre dominios sin clase (CIDR) y subredes.

Paso 9. (Opcional) Haga clic en Avanzado para definir criterios de pertenencia adicionales, como, por ejemplo, Puertos de Proxy, Categorías de URL o Agentes de usuario.



Precaución: en la implementación de proxy transparente, SWA no puede leer los agentes de usuario ni la URL completa para el tráfico HTTPS a menos que se descifre el tráfico. Como resultado, si configura el perfil de identificación mediante agentes de usuario o una categoría de URL personalizada con expresiones regulares, este tráfico no coincide con el perfil de identificación.

Para obtener más información sobre cómo configurar la categoría de URL personalizado, visite: [Configure Custom URL Categories in Secure Web Appliance - Cisco]



Sugerencia: la política utiliza una lógica AND, lo que significa que se deben cumplir todas las condiciones para que el perfil de ID coincida. Cuando se establecen las opciones avanzadas, se deben cumplir todos los requisitos para que se aplique la política.

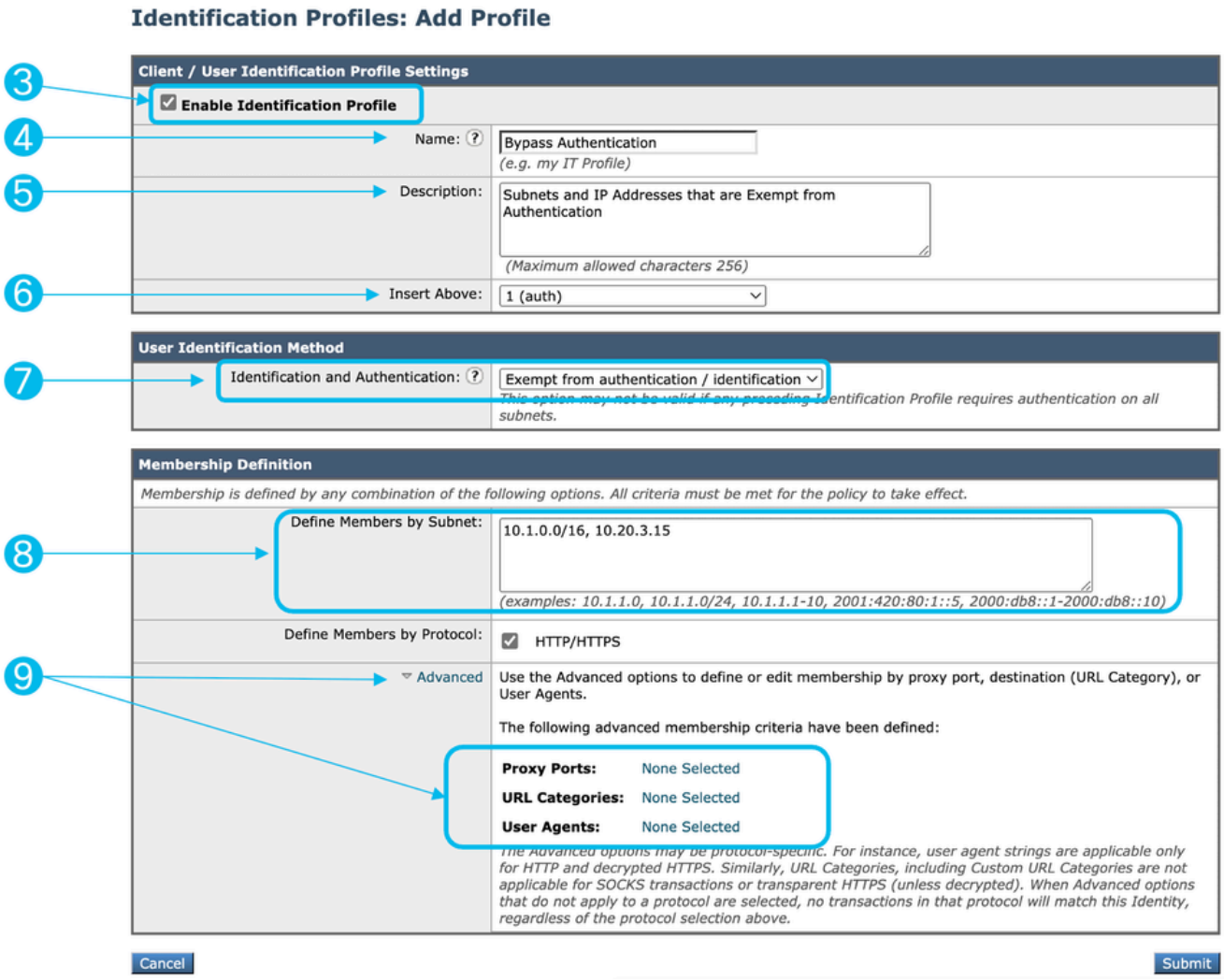


Imagen: Pasos para crear un perfil de ID para omitir la autenticación

Paso 10. Enviar y registrar cambios.

Información Relacionada

- Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - GD(General Deployment) - Clasificación de usuarios finales para la aplicación de políticas [Cisco Secure Web Appliance] - Cisco
- Configurar categorías de URL personalizadas en el dispositivo web seguro - Cisco
- Cómo eximir el tráfico de Office 365 de la autenticación y el descifrado en Cisco Web Security Appliance (WSA): Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).