Configuración de la Autenticación Externa SSO de SAML para la Administración de ESA y SMA

Contenido

Introducción

Este documento describe cómo configurar la autenticación externa SSO de SAML 2.0 para la administración del sistema ESA y SMA.

Entorno

- SOPORTE DE PRODUCTO: Dispositivo de seguridad de correo electrónico (ESA), dispositivo de administración de seguridad (SMA)
- Se aplica a: Administración de sistemas ESA y SMA
- Comportamiento del clúster: Los perfiles de proveedor de servicios (SP) e idP se configuran en el nivel de máquina; la asignación de autenticación externa se configura en el nivel de clúster.

Prerequisites

- Acceso administrativo a la interfaz web ESA/SMA
- Certificado X.509 y clave privada disponibles en formato PKCS #12 (PFX) o PEM (autofirmado o firmado por CA)
- Acceso a una aplicación de proveedor de identidad (IdP) de terceros y sus metadatos SAML/URL SSO

Lista de comprobación de preconfiguración

- Verifique el nombre de host/FQDN de la interfaz de administración que utilizan los administradores para acceder al dispositivo; confirme que la dirección URL de Assertion Consumer Service (ACS) coincide con ese nombre de host.
- Si el dispositivo está en un clúster, planifique configurar SAML en el nivel de equipo para cada miembro antes de activar la autenticación externa SAML.
- Determine si el IdP requiere una aplicación o rango independiente por dispositivo.
- Confirme que los certificados y claves requeridos están disponibles.
- Confirmar que el IdP envía el atributo de grupo o rol requerido para la asignación de roles ESA/SMA.

Precaución: Este documento no se aplica al SSO SAML de cuarentena de usuario final (EUQ).

Antecedentes

- Cisco TAC no proporciona soporte técnico para la configuración de IdP de terceros. Se proporcionan referencias de configuración de ejemplo para los IdPs comunes.

IdPs de SSO SAML

- Duo Access Gateway (DAG) añade autenticación de dos factores, además de servicios en la nube populares que utilizan la federación SAML 2.0.
- Servicios de federación de Active Directory (ADFS): probados con ADFS 2,3,4, Azure Active Directory (Azure AD), SecureAUTH y PingFederate
- Se puede utilizar una autenticación adicional de dos factores si el IdP lo soporta dentro del marco de Single Sign-On de SAML 2.0.
- Okta soporta la autenticación con un IdP que soporta el servicio.

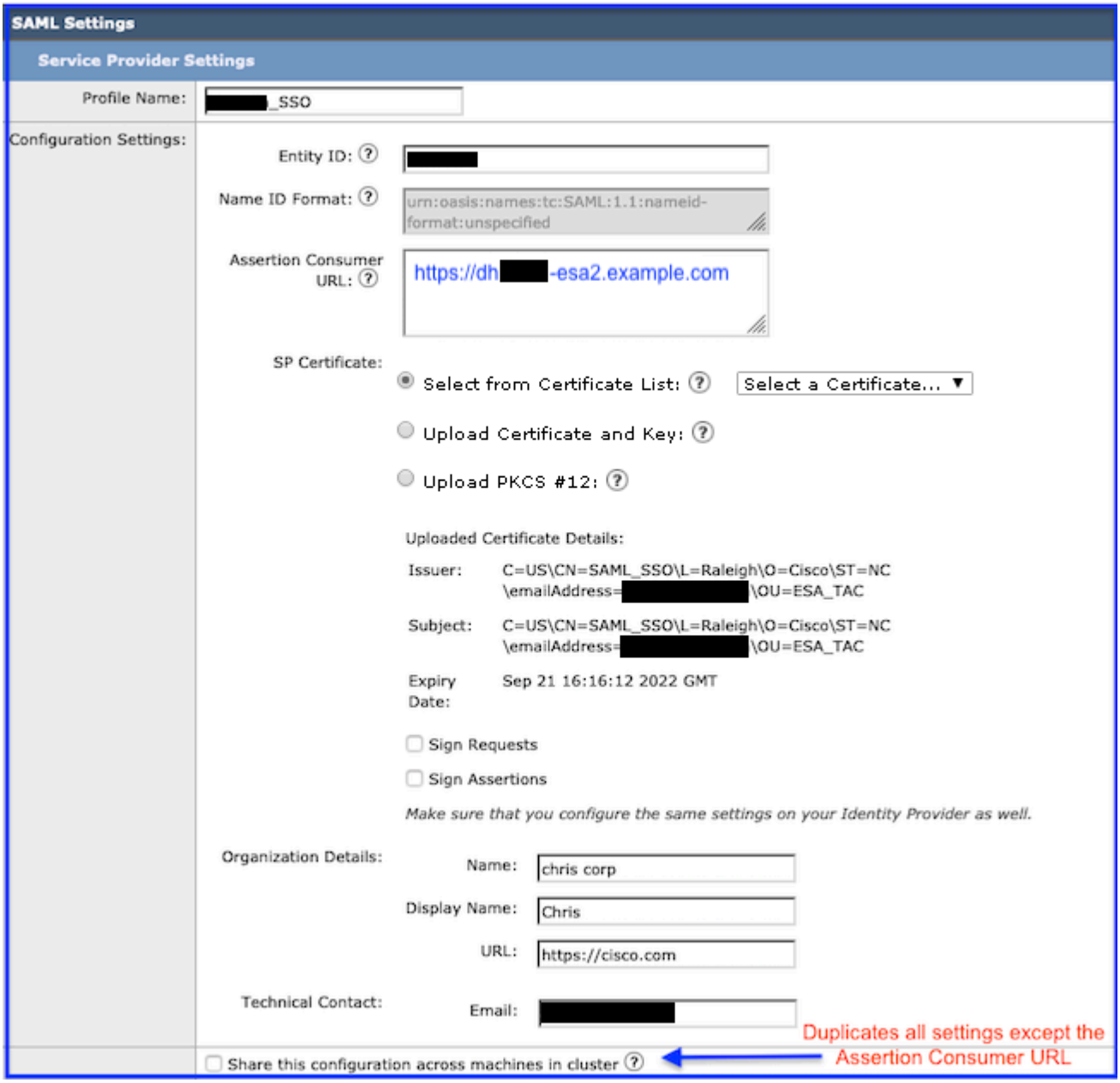
Configuración del ESA/SMA como proveedor de servicios

Vaya a Administración del sistema > SAML > (Nivel de equipo) > Agregar proveedor de servicios.

Nota: Los ESA de un clúster requieren una configuración en el nivel de equipo para todos los miembros del clúster antes de poder habilitar SAML.

- Si la opción de la parte inferior de la página, Compartir esta configuración entre las máquinas del clúster, está seleccionada, se aplicarán estas condiciones:
    - Todos los campos se replican en los miembros del clúster excepto la URL de consumidor de aserción.
    - La URL de Consumidor de Afirmación rellena automáticamente el nombre de host de la interfaz de administración como ACS.
    - Los entornos que utilizan un nombre de host alternativo para acceder al host requieren la configuración manual de cada host, por ejemplo, los dispositivos alojados en CES.
    - Nombre del perfil: Nombre utilizado para etiquetar la instancia SP en la interfaz ESA o SMA.
    - ID de entidad: Nombre utilizado para la instancia SP tal como lo ve el IdP. Este nombre es la etiqueta utilizada por el IdP para representar al SP. Puede ser cualquier nombre, por ejemplo, ESA_SP o ESA_SSO.
    - Formato de ID de nombre: Campo no configurable.
    - URL de consumidor de afirmación o servicio de consumidor de afirmación (ACS): URL utilizada por el IdP para comunicarse con este host ESA/SMA.
    - Certificado SP:
        - Formato: Certificados públicos/privados X.509 en formato PFX/PKCS12 o PEM.
        - Opción 1: Seleccionar de la lista de certificados: Seleccione entre los certificados ya creados en el ESA en Red > Certificados.
        - Opción 2: Cargar certificado y clave: Cargue un certificado y una clave con formato PEM.
        - Opción 3: Cargar PKCS n.º 12: Cargue un archivo PKCS #12.
        - Opcional: Cree un certificado autofirmado en el ESA/SMA para el inicio de sesión único de SAML.
        - Si es necesario, proteja la clave privada con contraseña.

Nota: Si se utilizan certificados con formato PEM, conserve cada certificado y clave privada en archivos independientes.



Página de configuración del proveedor de servicios

Página de configuración del proveedor de servicios

- Firmar solicitudes: Opción para firmar la comunicación SAML ESA/SMA enviada al IdP.
- Firmar aserciones: Opción para requerir que el IdP firme afirmaciones enviadas al ESA/SMA.
- Detalles de la organización: Se puede cumplimentar con los datos de la empresa correspondientes.
- Envíe y confirme los cambios para conservar la configuración.
- Descargue los metadatos SP desde la página de configuración SAML.

Configure el proveedor de identidad (IdP) para que funcione con los dispositivos ESA/SMA

Nota: Algunos IdP requieren aplicaciones o rangos independientes para cada ESA. (Ejemplo: DUO)

Estos vínculos proporcionan configuraciones de ejemplo para varios IdPs en el momento de la publicación.
Cisco TAC no proporciona asistencia técnica para productos de terceros. Estos ejemplos se proporcionan como referencias.

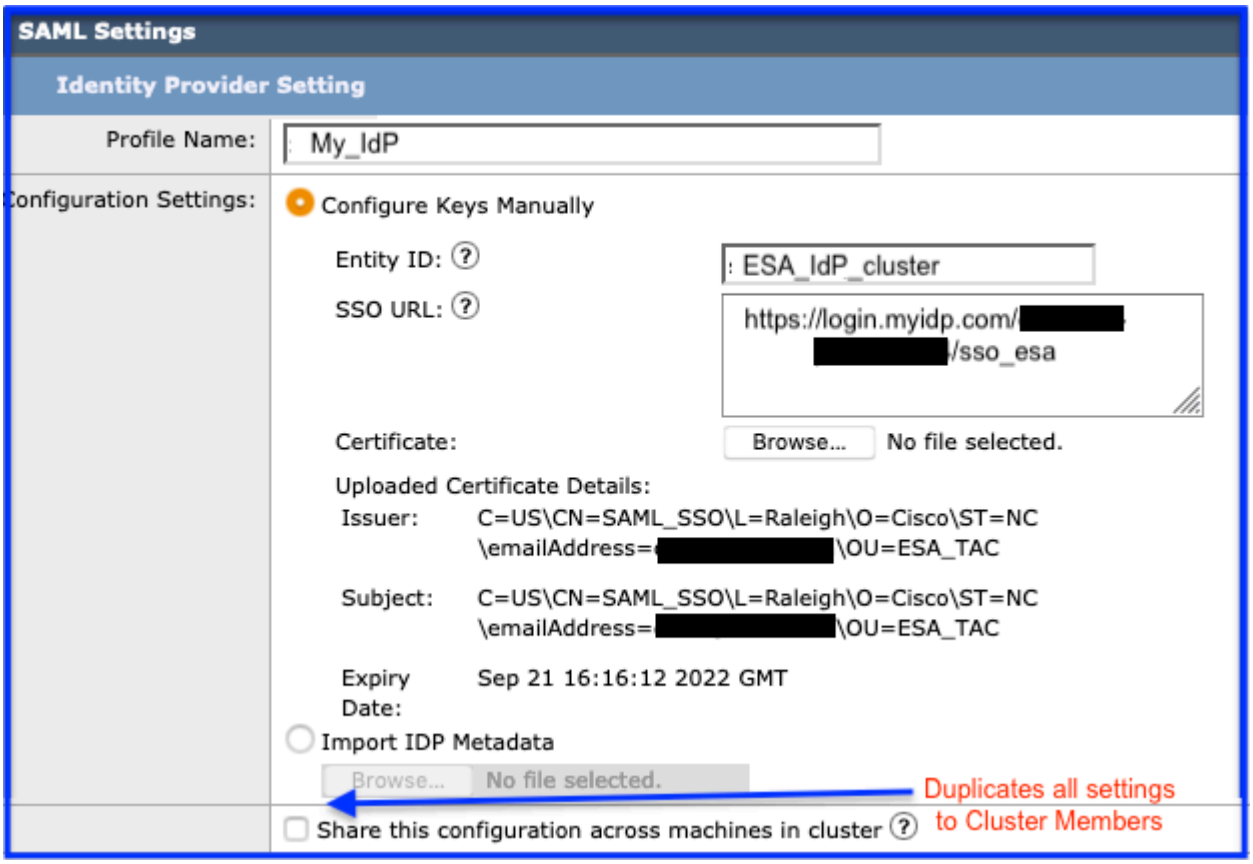
Configuración de los valores IDP en el ESA/SMA

1. Vaya a Administración del sistema > SAML.

2. Seleccione Agregar proveedor de identidad.

- Hay dos opciones disponibles:
- Importar metadatos IdP
- Configurar Llaves Manualmente:
    - ID de entidad: Puede ser cualquier valor utilizado para identificar el IdP
    - URL DE SSO: URL a la que el SP envía solicitudes de autenticación SAML
    - Cargue la clave privada y el certificado público en archivos independientes

3. Comparta esta configuración entre las máquinas del clúster para replicar la configuración en todos los ESA del clúster:

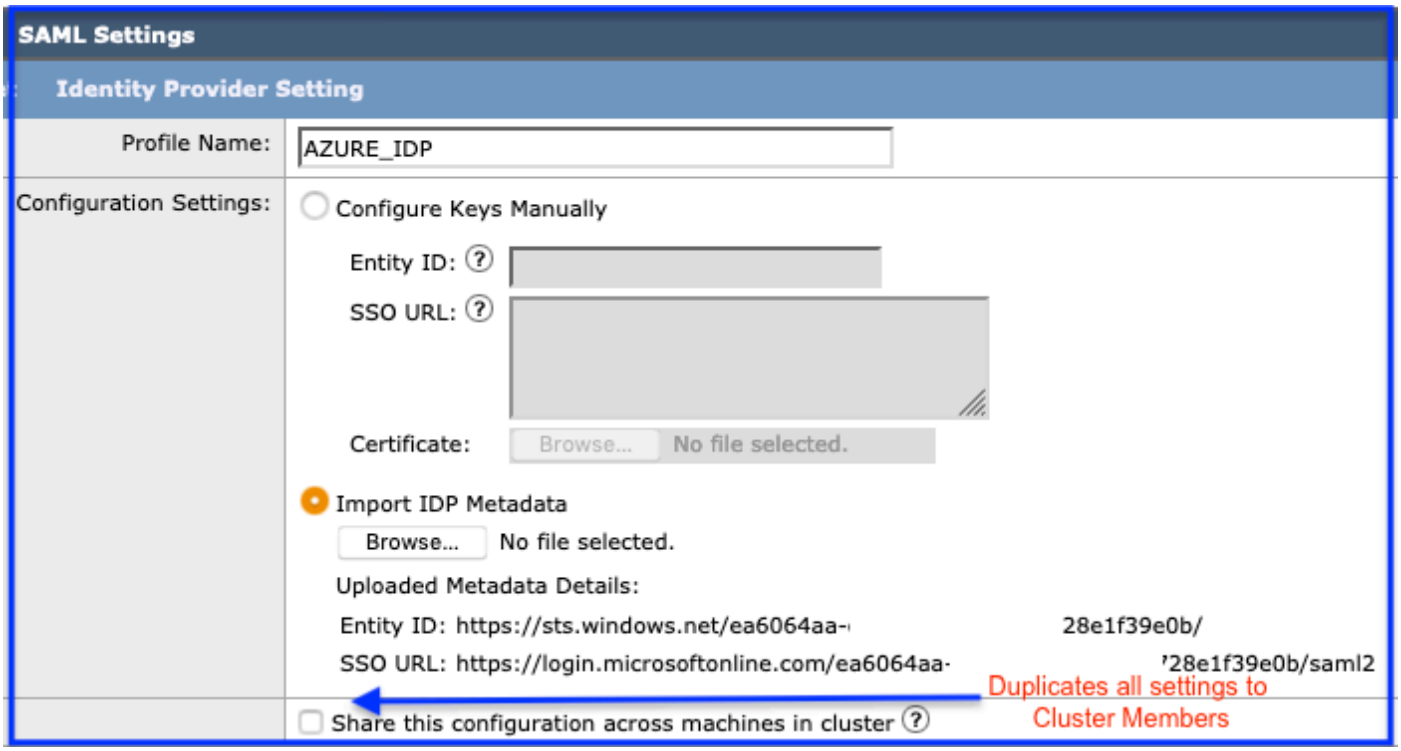


Introducir contenido IdP manualmente

Introducir contenido IdP manualmente

4. Cargar metadatos desde IdP

- Seleccione Importar metadatos IdP.
- Busque el archivo de metadatos guardado desde el IdP y guarde la configuración.
- La opción de compartir esta configuración entre las máquinas de un clúster está disponible si se aplica a la implementación.



Cargar Metadatos Desde Idp

Cargar Metadatos Desde Idp

Habilitación de la Autenticación Externa con SAML en el ESA/SMA

De forma similar a la autenticación externa LDAP, el inicio de sesión único de SAML requiere asignación para asignar grupos a roles administrativos.

1. Vaya a Administración del sistema > Usuarios (nivel de clúster) > Autenticación externa > Activar.

2. Seleccione el tipo de autenticación: SAML.

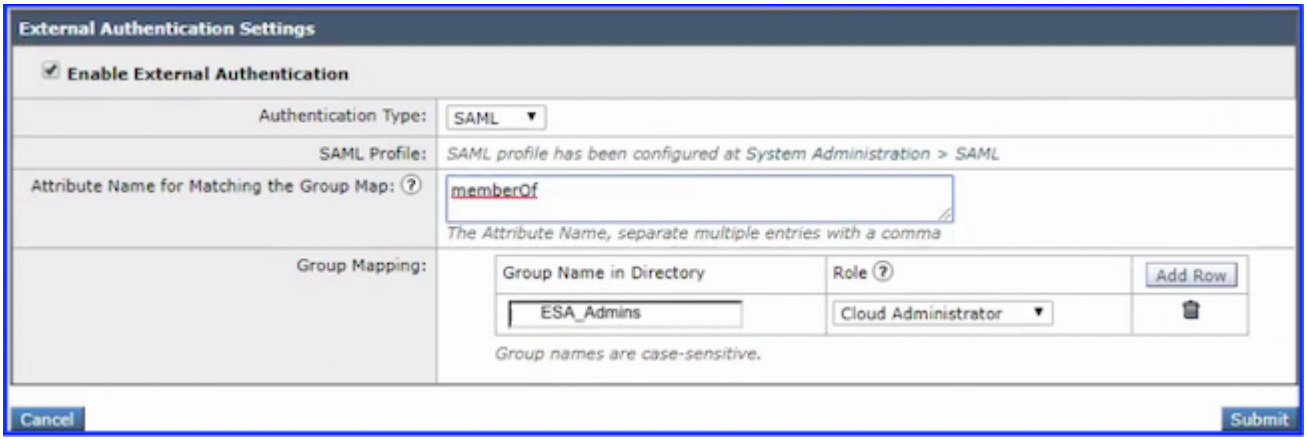
3. Nombre de Atributo para Coincidir con el Mapa de Nombres (Opcional): Introduzca el nombre de atributo que desea buscar en la asignación de grupo.

Nota: El nombre del atributo depende de los atributos configurados para que el proveedor de identidad retransmita en la respuesta SAML. El dispositivo busca entradas coincidentes del nombre de atributo especificado en la respuesta SAML con los atributos configurados en el campo Asignación de grupo. Si este campo no está configurado, el dispositivo busca todos los atributos presentes en la respuesta SAML en el campo Group Mapping configurado.

---

4. Introduzca el atributo de nombre de grupo definido en el directorio SAML en función del rol de usuario predefinido o personalizado.

- El campo Group Mapping debe contener un atributo de grupo. El atributo Unspecified Groups se puede agregar para autenticar afirmaciones o respuestas SAML.



Configuración de autenticación externa

Configuración de autenticación externa

5. Ejecute y confirme los cambios.

Una vez que la configuración se haya realizado correctamente, se mostrará un nuevo vínculo en la parte inferior de la página de inicio de sesión. La página de inicio de sesión de ESA/SMA muestra un enlace Use Single Sign-On que redirige a los administradores al proveedor de identidad corporativo (IdP).

Cuando se selecciona, el administrador se redirige a la página de inicio de sesión SAML corporativa.

Troubleshoot

Utilice estos indicadores para identificar si el problema está relacionado con la configuración del dispositivo o la configuración IdP.

El enlace de redirección de SSO no aparece en la página de inicio de sesión ("Utilizar inicio de sesión único")

Confirme que se haya configurado Administración del sistema > Usuarios > Autenticación externa > SAML.

Redirigir vuelve a la página de inicio de sesión de ESA/SMA con el mensaje "Error en la autenticación de inicio de sesión único". Póngase en contacto con el administrador."

Error: "Error en la autenticación de inicio de sesión único. Póngase en contacto con el administrador."

- Error de autenticación en el IdP.
    - Esto indica que la configuración está funcionando hasta el punto de alcanzar la página de autenticación de Single Sign-On y enviar credenciales.
    - Este fallo se debe a menudo a la configuración del IdP y requiere una verificación adicional de la configuración del IdP.

Redirigir devoluciones a la página de inicio de sesión de ESA/SMA con el mensaje "Error de autorización" Póngase en contacto con el administrador."

Error: "¡Error de autorización! Póngase en contacto con el administrador."

- Se superó la autenticación, pero la autorización falló en el ESA/SMA.
    - Céntrese en la configuración de Users > External Authentication > SAML.
        - Nombre de atributo, Nombre de grupo y Asignación de grupo.

Información Relacionada

- Cisco Email Security Appliance: guías del usuario
- Cisco Content Security Management Appliance: Guías de usuario
- Cisco Web Security: guías del usuario

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).