

# Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Descripción del flujo](#)

[Flujo previsto para este caso del uso:](#)

[Configurar](#)

[Paso 1. Prepare el ISE para utilizar un proveedor externo de la identidad de SAML](#)

[Paso 2. Configure el portal del invitado para utilizar un proveedor externo de la identidad](#)

[Paso 3. Configure PingFederate para actuar como proveedor de la identidad para el portal del invitado ISE](#)

[Paso 4. Importe los meta datos de IdP en el perfil externo del proveedor ISE SAML IdP](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar la versión 2.1 de Engine(ISE) de los servicios de la identidad de Cisco a las solas capacidades de On(SSO) de la muestra del proveedor para los usuarios porta del invitado con el margen de beneficio Language(SAML) de la aserción de la Seguridad.

## Prerrequisitos

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicios del invitado del Cisco Identity Services Engine.
- Conocimiento básico sobre SAML SSO.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 2.1 del Cisco Identity Services Engine
- Servidor de PingFederate 8.1.3.0 de la identidad del ping como identidad Provider(IdP) de SAML

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 su red está viva, asegúrese que usted entiende el impacto potencial de cualquier configuración aplicada.

## Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

## Descripción del flujo

El lenguaje de marcado de la aserción de la Seguridad (SAML) es un estándar XML basado para intercambiar los datos de la autenticación y autorización entre los dominios de seguridad.

SAML la especificación define tres papeles: el director (Usuario invitado), el [IdP] del proveedor de la identidad (servidor federado de IPing), y el proveedor de servicio [SP] (ISE).

En un flujo típico de SAML SSO, el SP pide y obtiene una aserción de la identidad del IdP. De acuerdo con este resultado, el ISE puede realizar las decisiones de políticas mientras que el IdP puede incluir los atributos configurables que el ISE puede utilizar (es decir grupo y dirección de correo electrónico asociados al objeto AD).

### Flujo previsto para este caso del uso:

1. El WLC o el switch de acceso se configura para un flujo central típico de la autenticación Web (CWA).

Consejo: Encuentre por favor los ejemplos de configuración para CWA fluye en la **sección de información relacionada** en la parte inferior del artículo

2. El cliente conecta y la sesión consigue autenticada contra el ISE. El acceso a la red Device(NAD) aplica los pares del valor de atributos de la reorientación (AVP) vueltos por el ISE (el URL-reorientar-ACL y URL-reorienta).

3. ¿El cliente abre al navegador, genera el tráfico HTTP o HTTPS y consigue reorientado al ISE? portal del invitado s.

4. Una vez en el portal el cliente podrá ingresar las credenciales previamente asignadas del invitado (**patrocinador creado**), la uno mismo-disposición una nueva cuenta del invitado o utilizar sus credenciales AD para iniciar sesión (**login del empleado**) que proporcionen la sola muestra en las capacidades a través SAML.

5. ¿Una vez que el usuario selecciona la opción de? ¿Login del empleado? ¿El ISE verifica si hay una aserción activa asociada a este cliente? gainst de la sesión del buscador s el IdP. Si no hay sesiones activas, el IdP aplicará el ingreso del usuario al sistema. En este paso se indicará al usuario que ingrese las credenciales AD en el portal de IdP directamente.

6. El IdP autentica al usuario vía el LDAP y crea una nueva aserción que permanezca viva por un tiempo configurable.

Nota: El ping federado por abandono aplicará un **tiempo de espera de la sesión de 60**

minutos (éste significa que si no hay pedidos de registro SSO del ISE en 60 minutos después de autenticación inicial la sesión está borrada) y un **descanso máximo de la sesión de 480 minutos** (incluso si el IdP ha estado recibiendo los pedidos de registro constantes SSO del ISE para este usuario que la sesión expirará en 8 horas).

Mientras la sesión de la aserción sea todavía activa, el empleado experimentará el SSO cuando portal del invitado del gthe del usin. Una vez los tiempos de la sesión hacia fuera que una autenticación de usuario nuevo será aplicada por el IdP.

## Configurar

La sección siguiente discutirá los pasos para la configuración para integrar el ISE con el ping federado y cómo habilitar al navegador SSO para el portal del invitado.

Nota: Aunque existan las diversas opciones y posibilidades cuando usted autentica a los Usuarios invitados, no todas las combinaciones se describen en este documento. Sin embargo, este ejemplo provee de usted la información necesaria entender cómo modificar el ejemplo a la configuración exacta que usted quiere alcanzar.

### Paso 1. Prepare el ISE para utilizar un proveedor externo de la identidad de SAML

1. En Cisco ISE navegue a la **administración > a la Administración de la identidad > las fuentes externas de la identidad > SAML los proveedores identificación**.
2. El tecleo **agrega**
3. Bajo lengüeta de **General** ingrese un **nombre del proveedor identificación**. Haga clic en la **salvaguardia**. El resto de la configuración en esta sección dependerá de los meta datos que necesite ser importada del IdP en pasos posteriores.

### Paso 2. Configure el portal del invitado para utilizar un proveedor externo de la identidad

1. Navegue a los **centros de trabajo > al acceso de invitado > a la configuración > a los portales del invitado**
2. Cree un nuevo **portal Uno mismo-registrado porta** y selecto del invitado.

Nota: Éste no será el portal principal que el usuario experimentará solamente un subportal que obrará recíprocamente con el IdP para verificar el estatus de la sesión. Llamaré este SSOSubPortal porta.

3. Amplíe las **configuraciones porta** y seleccione **PingFederate** para el **método de autenticación**.
4. Seleccione de la **secuencia de la fuente de la identidad el defined(PingFederate)** externo de SAML IdP previamente.
5. Amplíe las secciones de las **paginaciones del banner de Acceptable Use Policy(AUP)** y del **Poste-login** y inhabilite ambos.

Flujo porta:

6. Guarde los cambios.

7. Vuelva a los portales del invitado y cree un nuevo usando la opción **Uno mismo-registradoa del portal del invitado**.

Nota: Éste será el visible porta primario al cliente. El portal primario utilizará el SSOSubportal como interfaz entre el ISE y el IdP. Nombraremos este PrimaryPortal porta.

8. ¿Amplíe las **paginaciones del login** y seleccione el **SSOSubPortal** creado previamente debajo? **Permita que el portal siguiente del invitado del identidad-proveedor sea utilizado para el login?**

9. Amplíe las **paginaciones del banner AUP** y del **Poste-login del Acceptable Use Policy** y desmarquelas.

En este momento el flujo porta debe parecer esto:

10. Haga clic en el **arreglo para requisitos particulares > las páginas > el login porta**. Debemos ahora tener la opción para personalizar las **opciones alternativas del login** (icono, texto, etc).

Nota: Note eso en el lado derecho, bajo avance porta, la opción adicional del login es visible.

11. Haga clic en Save (Guardar).

Ahora ambos portales deben aparecer conforme a la lista del portal del invitado.

### **Paso 3. Configure PingFederate para actuar como proveedor de la identidad para el portal del invitado ISE**

1. En el ISE, navegue a la **administración > a la Administración de la identidad > las fuentes externas de la identidad > SAML los proveedores > PingFederate identificación** y haga clic la **información del proveedor de servicio**
2. Bajo **exportación del tecleo de la información del proveedor de servicio de la exportación**
3. Salve y extraiga archivo zip generado. El archivo XML contenido aquí será utilizado mientras que crea el perfil en PingFederate en los siguientes pasos.

Nota: Desde aquí, cubriremos la configuración de PingFederate. Esta configuración será lo mismo para las soluciones múltiples como el portal del patrocinador, MyDevices y los portales BYOD. (Esas soluciones no se cubren en este artículo)

4. Abra el portal de PingFederate admin (típicamente <https://ip:9999/pingfederate/app>).

5. Bajo sección de la **ficha de configuración de IdP > de las conexiones SP** selecta cree nuevo.

6. Bajo el **Tipo de conexión** haga clic **después**

7. Bajo **opciones de conexión** haga clic **después**

8. Bajo **meta datos de la importación**, el **archivo** selecto, eligió el archivo y selecciona el archivo XML exportado previamente del ISE.

el **resumen de los meta datos** 9. Under, hace clic en **después**.

la página de la información general 10. On, bajo nombre de la conexión ingresa un nombre (IE. ISEGuestWebAuth) y hace clic **después**.

11. Bajo **navegador SSO de la configuración del teclado del navegador SSO** y bajo **perfiles de SAML** marque las opciones siguientes y haga clic después:

tecleo del **curso de la vida de la aserción** 12. On **después**

**creación de la aserción de la configuración del teclado de la creación de la aserción** 13. On

**estándar** selecto y teclado de la **asignación de la identidad** 14. Under **después**

15. En el **contrato del atributo** > extienda el contrato ingresan el **correo de los atributos** y el teclado del **memberOf and agrega**. Entonces haga clic **después**

Configurar esta opción permitirá que el proveedor de la identidad pase el **MemberOf** y **envíe por correo electrónico los atributos** proporcionados por el Active Directory al ISE, que el ISE puede utilizar más adelante como condición durante la decisión de políticas.

**caso del adaptador del mapa del teclado de la asignación de la fuente de la autenticación** 16. Under **nuevo**.

**adaptador** selecto de la **forma del caso HTML del adaptador** 17. On. Teclado **después**

18. Bajo **asignación los métodos** seleccionan la segunda opción abajo y hacen clic **después**:

19. En el **atributo las fuentes** y el teclado de las **operaciones de búsqueda del usuario** agregan el **cuadro de la fuente del atributo**

20. Bajo el **almacén de los datos** ingrese una descripción, y después selecciónela de los **datos activos** **salvan** su caso de la **conexión LDAP** y definen qué tipo de servicio de directorio es éste. Si no hay **almacenes de datos** configurados con todo el teclado **maneja los almacenes de datos** para agregar la nueva instancia.

21. Bajo la **búsqueda del directorio LDAP** defina la **base DN** para las operaciones de búsqueda del usuario LDAP en el dominio y haga clic **después**.

Nota: Esto es importante pues definirá la base DN durante las operaciones de búsqueda del usuario LDAP. La base incorrectamente definida DN dará lugar al objeto no encontrado en el esquema LDAP.

el **filtro** 22. Under **LDAP** agrega la cadena **sAMAccountName=\$ {nombre de usuario}** y hace clic **después**.

23. Bajo **cumplimiento del contrato del atributo** seleccione las opciones siguientes y haga clic **después**.
24. Verifique la configuración en la sección de resumen y haga clic **hecho**.
25. Apoye en tecleo de las **operaciones de búsqueda de las fuentes y del usuario del atributo después**.
26. Bajo **fuentes a prueba de averías del atributo** haga clic **después**.
27. Bajo **cumplimiento del contrato del atributo** seleccione estas opciones y haga clic **después**:
28. Verifique la sección y el tecleo de la configuración en resumen **hechos**.
29. Apoye en el tecleo de la **asignación de la fuente de la autenticación después**.
30. Una vez que la configuración se ha verificado bajo el tecleo de la **página de resumen hecho**.
31. Apoye en el tecleo de la **creación de la aserción después**.
32. Bajo **configuraciones del protocolo de la configuración del clickNext** de las **configuraciones del protocolo**. En este momento debe haber 2 entradas pobladas ya. Haga clic en Next (Siguiente).
33. Bajo SLO mantenga el tecleo URL después
34. En los atascamientos permisibles de SAML, desmarque las opciones ARTEFACTO y JABÓN y haga clic **después**.
35. Bajo directiva de la firma haga clic **después**.
36. Bajo política de encriptación haga clic **después**.
37. Revise la configuración en la página de resumen y haga clic **hecho**.
38. Apoye en el navegador SSO > tecleo de las configuraciones del protocolo después, valide la configuración y haga clic **hecho**.
39. Esto nos traerá de nuevo al tecleo del navegador SSO cuadro **después**.
40. Bajo las **credenciales** haga clic las **credenciales de la configuración** y elija el certificado de firma que se utilizará durante IdP a la comunicación ISE y marque la opción **incluyen el certificado en la firma**. Luego haga clic en Next (Siguiente).

Nota: Si no hay tecleo configurado los Certificados **maneje los Certificados** y siga los prompts para generar un **certificado autofirmado** que se utilizará para firmar IdP a las comunicaciones ISE.

41. Valide la configuración conforme a la página de resumen y haga clic **hecho**.
42. Apoye en el tecleo de la lengüeta de las **credenciales después**.

43. Conforme a la **activación y al resumen** selectos en el **ACTIVE** del estado de la conexión, valide el resto de la configuración y haga clic **hecho**.

#### **Paso 4. Importe los meta datos de IdP en el perfil externo del proveedor ISE SAML IdP**

1. Bajo la consola de administración de PingFederate navegue a la **Configuración del servidor > a las funciones administrativas > a la exportación de los meta datos**. Si el servidor se ha configurado para los papeles múltiples (IdP y SP) seleccione la opción que **soy la identidad Provider(IdP)**. Haga clic **después**
2. ¿Bajo modo de los **meta datos** seleccione? **Seleccione la información para incluir en los meta datos manualmente?**. Haga clic en Next (Siguiente).
3. Bajo **protocolo** haga clic **después**.
4. En el **contrato del atributo** haga clic **después**.
5. Bajo **clave de firma** seleccione el certificado configurado previamente en el perfil de la conexión. Haga clic en Next (Siguiente).
6. ¿Bajo **firma de los meta datos** seleccione el certificado de firma y el control **incluye este certificado? clave pública s en el elemento de información fundamental**. Haga clic en Next (Siguiente).
7. Bajo tecleo del **certificado del cifrado XML** después.

Nota: La opción para aplicar el cifrado aquí está hasta la red Admin.

8. Bajo la **exportación del** tecleo de la **sección de resumen**. Salve el archivo de metadatos generado y después haga clic **hecho**.

9. Bajo el ISE navegue a la **administración > a la Administración de la identidad > las fuentes externas de la identidad > SAML los proveedores > PingFederate identificación**.

10. **Los Config del proveedor de la identidad del** tecleo **> hojean** y proceden a importar los meta datos guardados de la operación de la exportación de los meta datos de PingFederate.

11 La lengüeta selecta de los **grupos**, bajo **atributo de la membresía del grupo** agrega el **memberOf** y después hace clic **agrega**

Bajo el nombre **en la aserción** agregue el nombre distintivo que el **IdP** debe volver detrás cuando el atributo del **memberOf** es autenticación extraída de la forma LDAP. En este caso conectan al grupo configurado al grupo del patrocinador de TOR y el DN para este grupo es como sigue:

¿Una vez que usted agrega el DN y? ¿Nombre en el ISE? **AUTORIZACIÓN** del tecleo de la descripción.

12. Lengüeta selecta y haga click en Add de los **atributos**

¿En este paso agregaremos el atributo? ¿correo? ¿eso se contiene en el token de SAML pasajero del IdP que basó en el ping? interrogación s sobre el LDAP, debe contener el atributo del

correo electrónico para ese objeto.

Nota: Los pasos 11 y 12 se aseguran de que el ISE reciba el correo electrónico del objeto AD y los atributos de MemberOf a través del IdP inicia sesión la acción.

## Verificación

1. Inicie el portal del invitado usando la prueba porta URL o siguiendo el CWA fluya. El usuario tendrá las opciones para ingresar las credenciales del invitado, crea su propia cuenta y login del empleado.
2. **Login del empleado del teclado.** Puesto que no hay sesiones activas reorientarán al usuario al portal del login de IdP.
3. Ingrese las credenciales AD y haga clic la **muestra encendido**.
4. La pantalla de inicio de IdP reorientará al usuario a la página porta del éxito del invitado.
5. ¿En este momento, cada vez que el usuario vuelve al portal del invitado y selecciona? ¿**Login del empleado**? serán permitidos en la red mientras la sesión sea todavía activa en el IdP.

## Troubleshooting

Cualquier problema de la autenticación de SAML será registrado bajo ise-psc.log. Hay un componente dedicado (SAML) bajo **configuración del registro de la administración > del registro > del debug > selecciona el nodo en la pregunta > fijó SAML el componente al nivel de debug**.

Podemos acceder el ISE con el CLI y publicar el comando? ¿muestre la cola de ise-psc.log de la aplicación del registro? y monitoree los eventos de SAML, o podemos descargar ise-psc.log para el análisis adicional bajo las **operaciones > los registros del Troubleshooting > de la descarga > seleccionamos la lengüeta de los registros del nodo > del debug ISE > el teclado ise-psc.log** para descargar los registros.

## Información Relacionada

- [Autenticación Web central con el ejemplo de configuración del WLC y ISE de Cisco.](#)
- [Autenticación Web central con un ejemplo de configuración del Switch y del Identity Services Engine.](#)
- [Release Note para el Cisco Identity Services Engine, 2.1 de la versión](#)
- [Guía del administrador del Cisco Identity Services Engine, 2.1 de la versión](#)