Manual de Usuario del Gestor de Metadatos

Preparado para:	**Proyecto CONFIA**
Preparado por:	**Yaco Sistemas S.L.**
Versión:	1
Fecha:	15/08/2009
Ref. YACO:	P174MAN090965

Yaco Sistemas S.L. Inscrita en el Registro Mercantil de Sevilla, tomo 3.496 de Sociedades, folio 16, hoja SE-48.825, inscripción 3ª. CIF:

Control de Versiones del Documento			
Versión	**Fecha**	**Descripción del Cambio**	**Autor**
1	15/09/09	Versión inicial	G. Rodríguez
2	29/0909	Incorporación de nuevas funcionalidades	Isabel Muñoz

Índice de contenido

1.- Definición del sistema....4
2.- Objeto del documento....4
3.- Autenticación y salida del sistema....4
3.1.- Ingreso en el sistema....4
3.2.- Salida del sistema....5
4.- Cambiar la descripción del usuario....6
5.- Crear conexiones....6
5.1.- Crear conexión con un Service Provider (SP)....6
5.2.- Crear conexión con un Identity Provider (IdP)....7
6.- Configurar conexiones....7
6.1.- Cambiar el tipo de una conexión....7
6.2.- Añadir metadatos a una conexión....8
6.3.- Importar metadatos en formato XML....9
6.4.- Importar metadatos a través de una URL....10
6.5.- Historial de cambios....11
6.6.- Exportar metadatos....12
7.- Acceso como usuario Lector....13

1.- Definición del sistema

El objetivo general del gestor de metadatos es centralizar el control de los metadatos de la federación en un mismo sitio. Se ha decidido no partir de cero en el desarrollo de este sistema y tras una serie de estudios se decidió utilizar Janus.

Janus es un módulo de Simplesamlphp capaz de gestionar una infraestructura común y publicar de forma segura los metadatos de la federación que incluyen los sistemas de autenticación de cada universidad y los servicios (LMS y otros), así como los procedimientos para incorporar nuevos servicios, nuevas organizaciones y nuevos usuarios que registren los diferentes IdPs y Sps.

El objetivo final del gestor de metadatos es que la unidad organizativa de la federación se encargue de mantener la lista de las organizaciones miembros, así como sus IdPs y los servicios accesibles utilizando esta herramienta. Todos los integrantes de la federación descargarán periódicamente estos metadatos que permiten que cada SP sepa en qué IdPs confiar y cada IdP a qué SP puede proporcionar datos. También permiten que el servicio WAYF pueda ofrecer una lista de organizaciones y sus IdPs. La federación publica periódicamente estos datos en formato XML digitalmente firmado.

Adicionalmente, el gestor de metadados podrá en un futuro ofrecer un servicio de comprobación de validez de certificados o listas de revocación de certificados para responder mejor en caso que un IdP haya sido comprometido.

2.- Objeto del documento

Este documento enseña cómo hacer uso del gestor de metadatos desde los roles de Administrador de Entidad y Lector que, respectivamente, pueden gestionar los SPs e IdPs de una entidad y obtener lista de los IdPs y SPs .

3.- Autenticación y salida del sistema

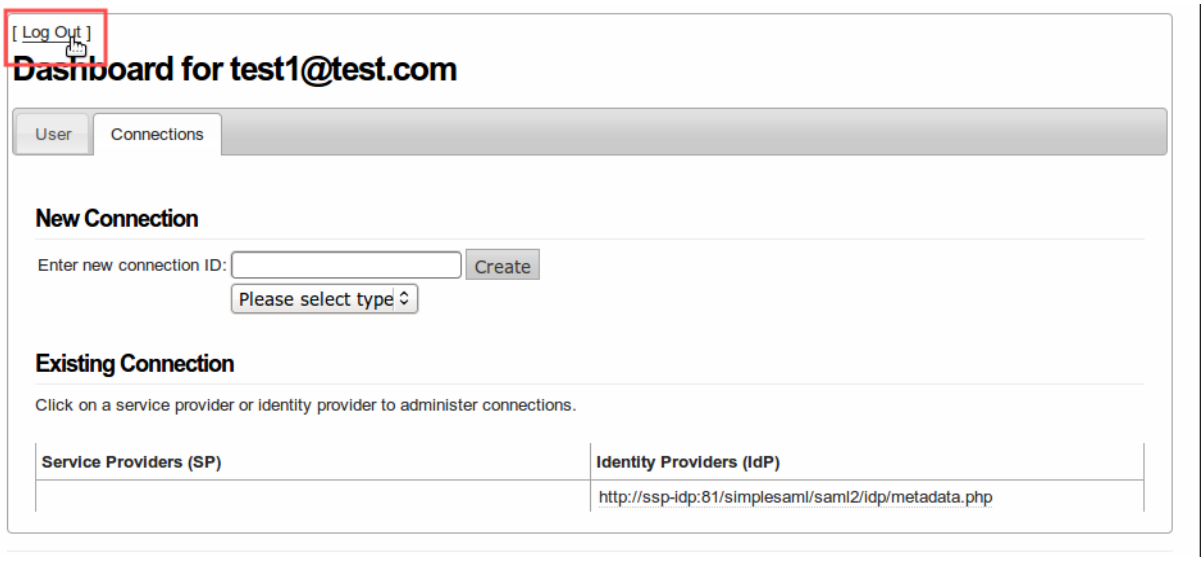
3.1.- Ingreso en el sistema

Para ingresar en el gestor de metadatos, una vez en la página principal de simpleSAMLphp, hay que pinchar en la pestaña **Federación** y, a continuación, en el enlace **JANUS module**.

A continuación, introduzca su nombre de usuario y su contraseña y pulse en el botón de acceso.

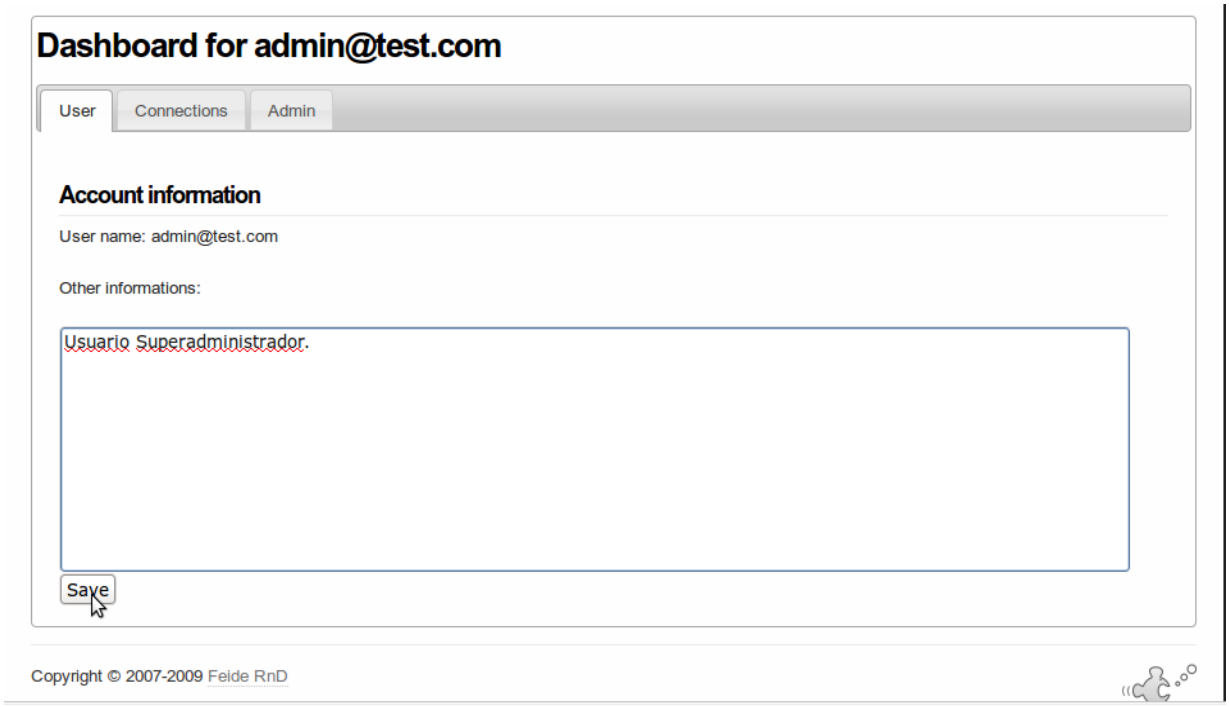
3.2.- Salida del sistema

Para salir del sistema, hay que pulsar en el enlace **[Log Out]** que aparece en la página principal de Janus.



4.- Cambiar la descripción del usuario

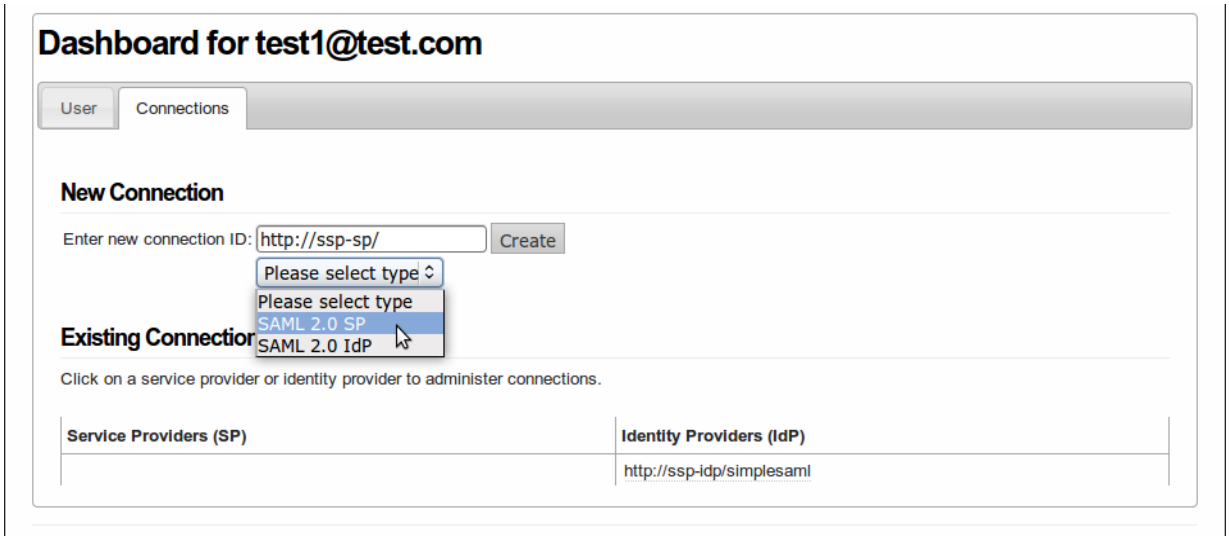
Para cambiar la descripción del usuario hay que pinchar en la pestaña **User**, editar el área de texto **Other informations** y pulsar en el botón de guardar.



5.- Crear conexiones

5.1.- Crear conexión con un Service Provider (SP)

Para crear una conexión con un SP, pinche en la pestaña **Connections**. A continuación, introduzca el identificador de entidad del SP: una URL que identifica unívocamente al SP. Luego seleccione **SAML 2.0 SP** y pulse en el botón **Create**.



5.2.- Crear conexión con un Identity Provider (IdP)

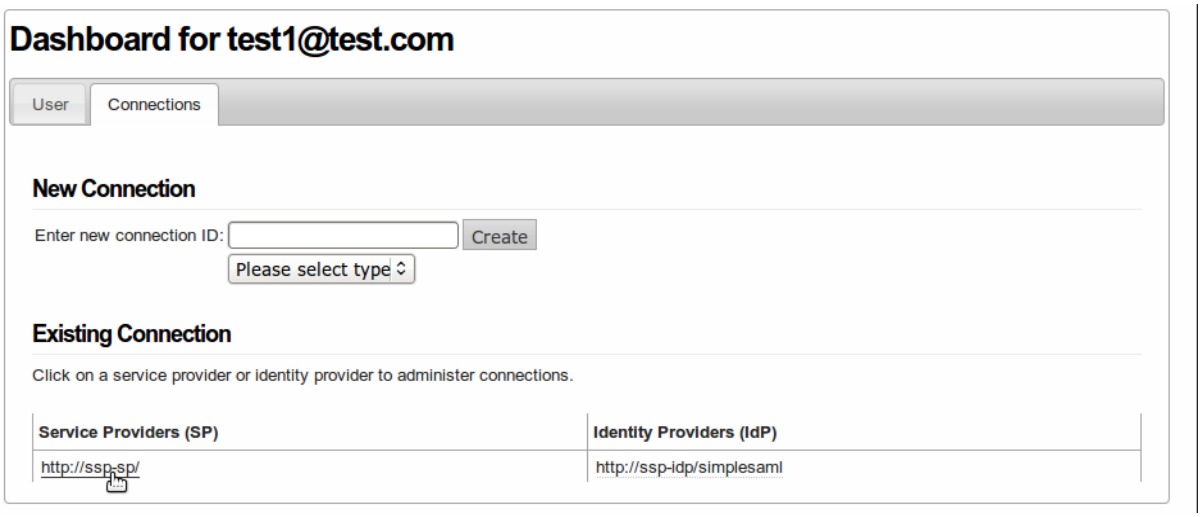
El procedimiento es idéntico al de la creación de un SP, con la salvedad de que hay que seleccionar **SAML 2.0 IdP** en el selector de tipo de conexión.

6.- Configurar conexiones

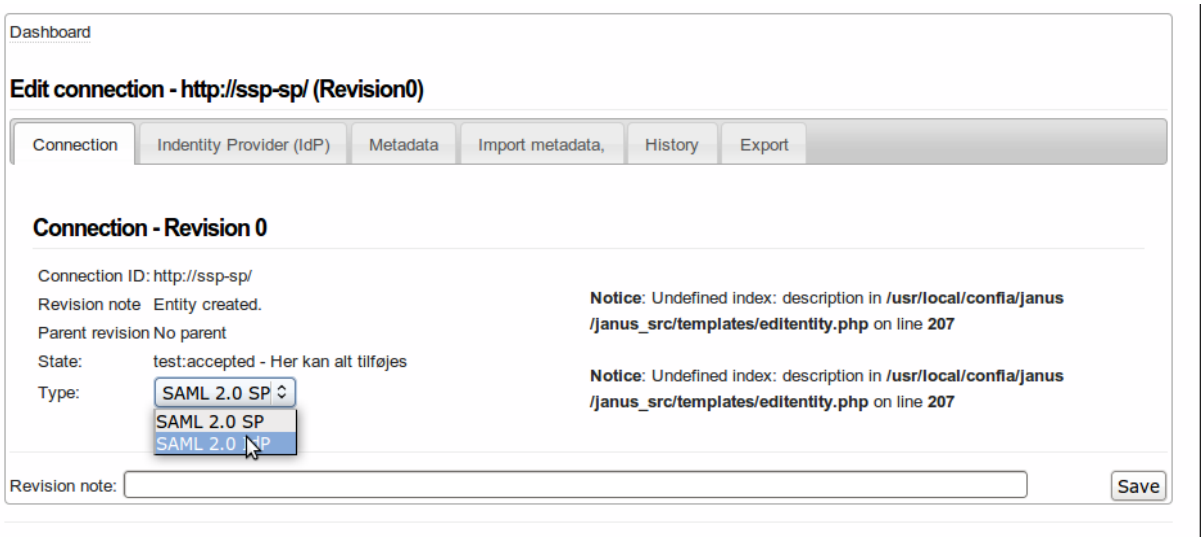
Todos los cambios que se efectúan en una conexión se registran como una revisión. Cada revisión puede tener un comentario explicativo que se puede rellenar en el campo de texto **Revision note** que aparece en la parte inferior de todas las pestañas.

6.1.- Cambiar el tipo de una conexión

El procedimiento es el mismo para las conexiones SP e IdP. Hay que pinchar en la conexión, dentro de la lista de conexiones que aparece en la página principal ("Dashboard") de Janus (a la derecha los SP y a la izquierda los IdP).

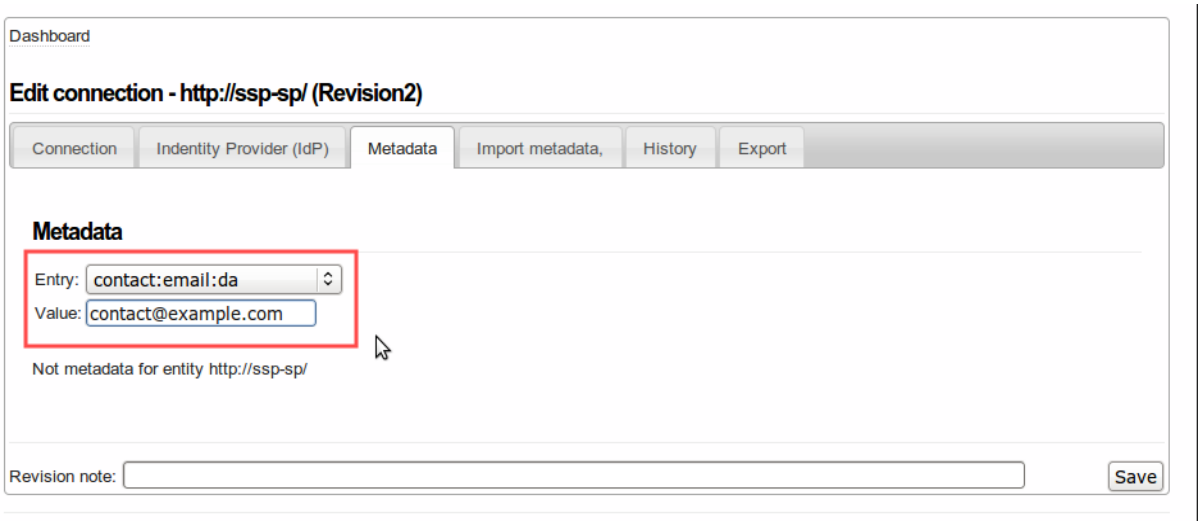


Una vez dentro, se puede cambiar el tipo de conexión seleccionándolo del desplegable con la etiqueta **Type** y pulsando en el botón **Save**.



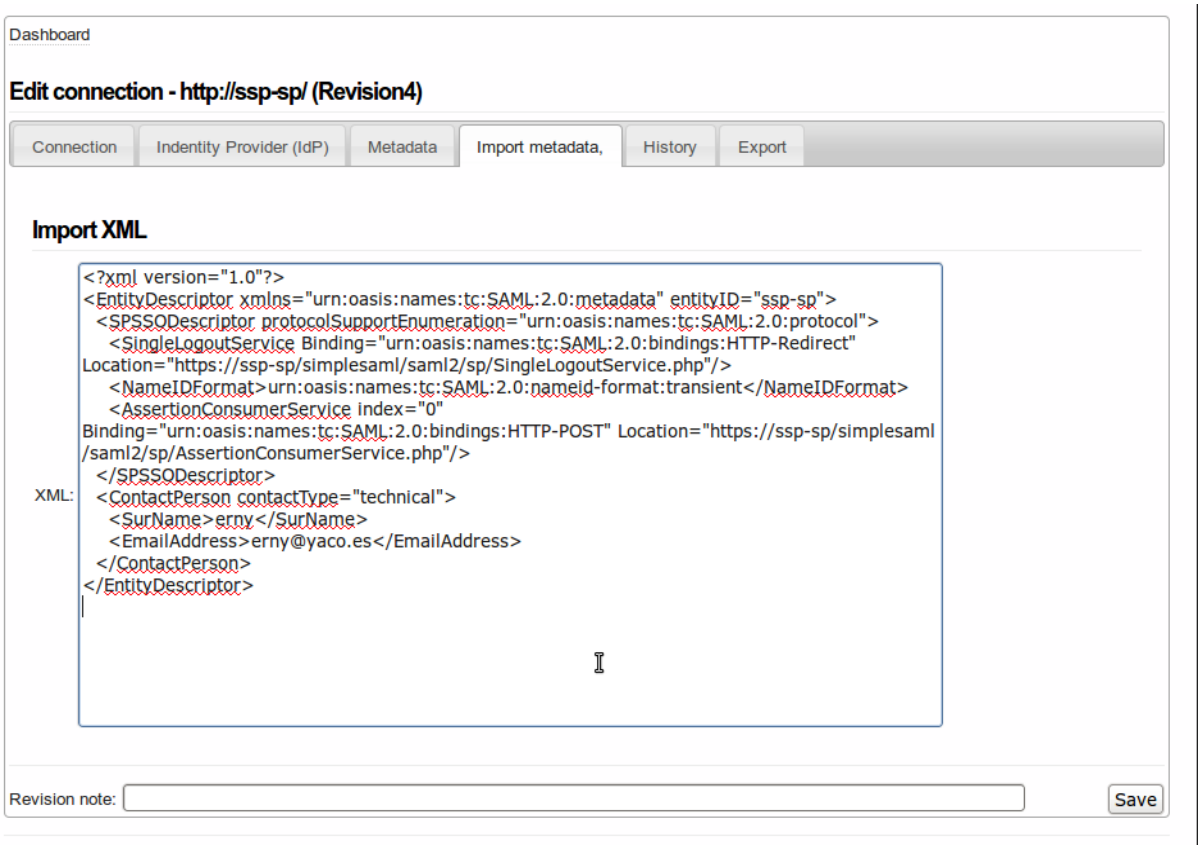
6.2.- Añadir metadatos a una conexión

Para añadir metadatos a una conexión, acceda a la pestaña **Metadata** en la pantalla de modificación de una conexión. Una vez dentro, seleccione el tipo de metadato que quiere añadir en el selector desplegable **Entry**, y el valor del metadato en el cuadro de texto **Value**.



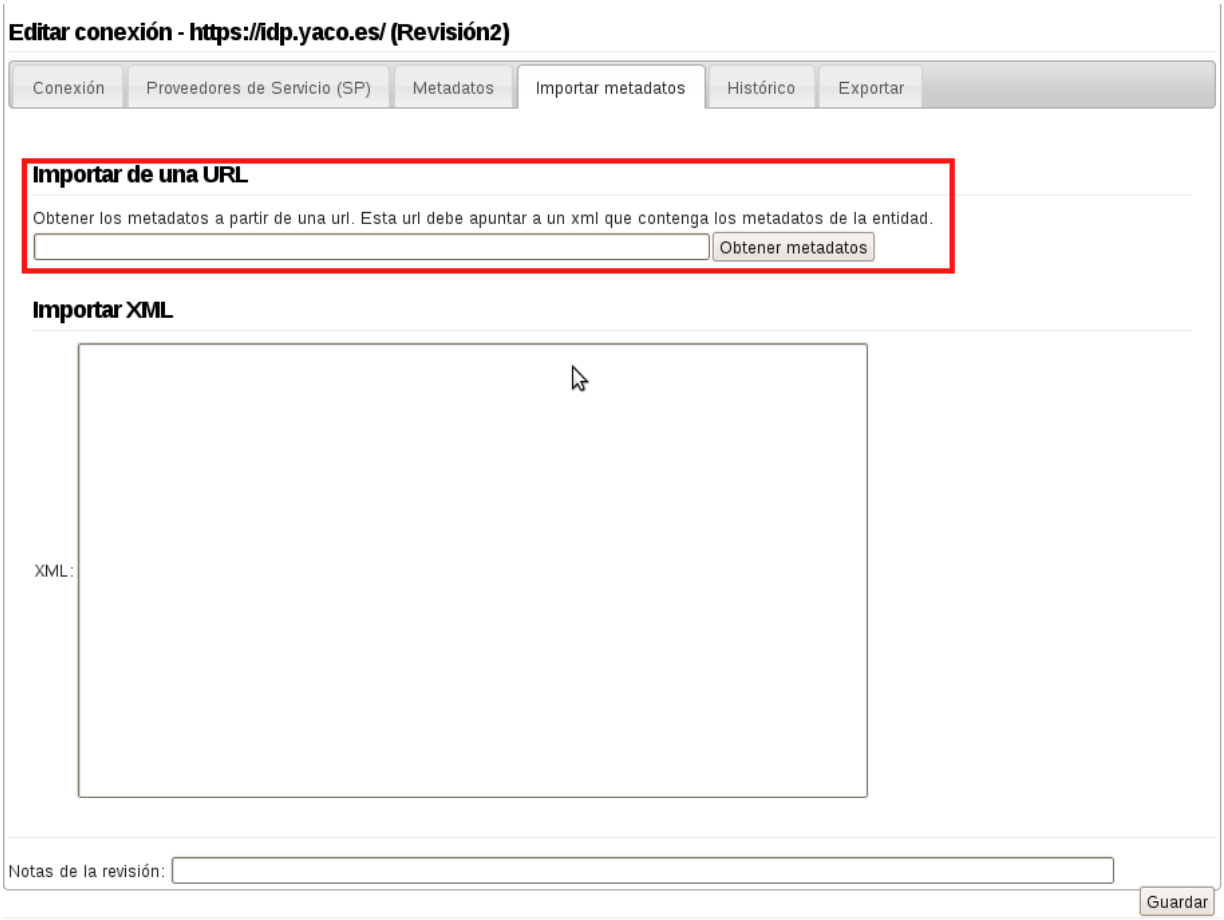
6.3.- Importar metadatos en formato XML

Para importar metadatos en XML en formato SAML o Shibboleth, acceda a la pestaña **Import metadata** en la pantalla de modificación de una conexión, pegue el texto XML en el área de texto con la etiqueta **XML** y pulse en el botón **Save**.



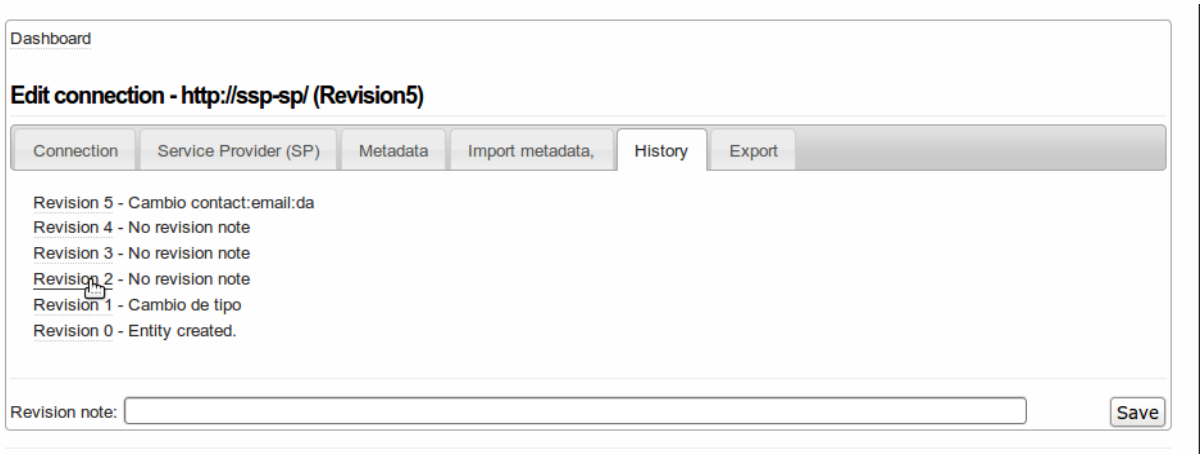
6.4.- Importar metadatos a través de una URL

Para importar metadatos desde una URL, acceda a la pestaña **Import metadata** en la pantalla de modificación de una conexión, e introduzca una URL que contenga metadatos. Para realizar la importación deberá pinchar en el botón **Obtener metadatos.**



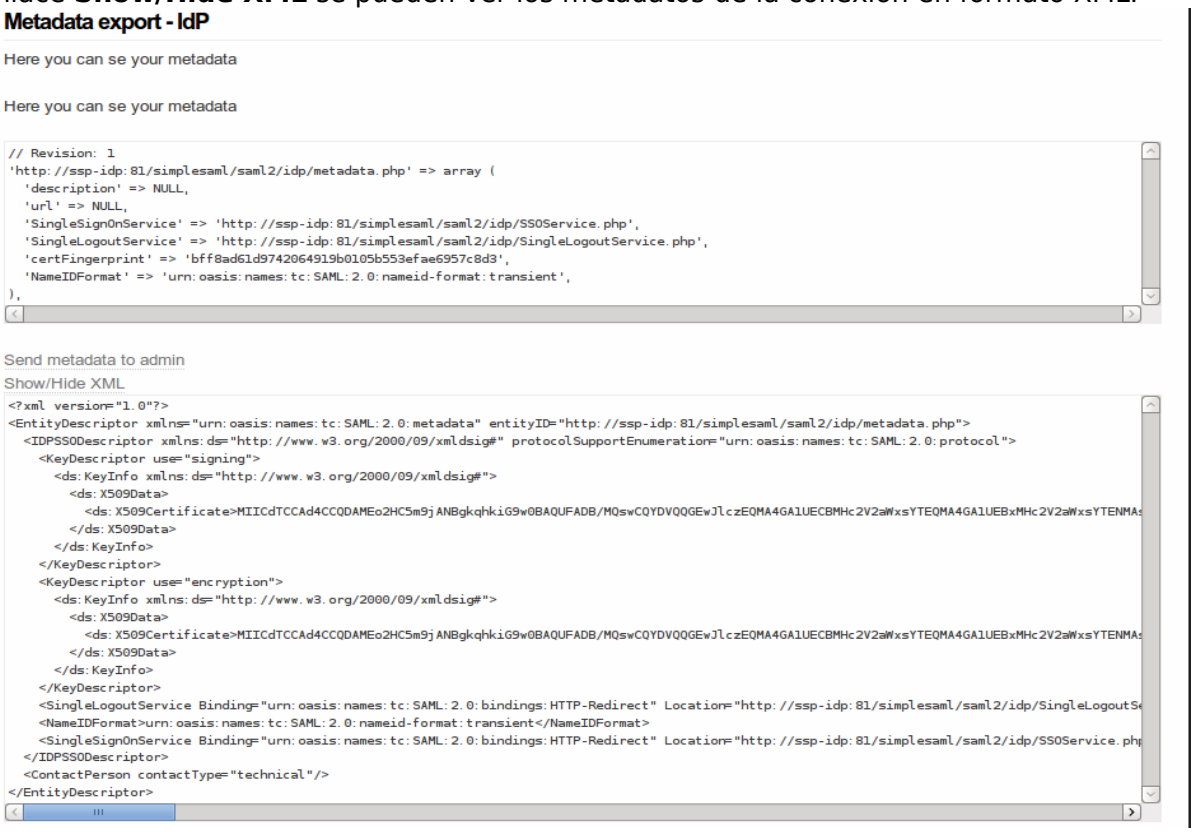
6.5.- Historial de cambios

Todos los cambios de configuración de una conexión quedan registrados mediante un sistema de revisiones. En la pestaña **History** se muestran todas las revisiones que ha tenido una conexión desde su creación, junto con las notas explicativas que acompañan a cada cambio. Es posible pinchar en una revisión para ver la configuración de la conexión en ese punto de su historia.



6.6.- Exportar metadatos

Para exportar metadatos en XML en formato SAML o en formato de configuración de simpleSAMLphp, acceda a la pestaña **Export** en la pantalla de modificación de una conexión y pinche en el enlace **Export metadata**. A continuación se mostrarán los metadatos de la conexión en formato de configuración de simpleSAMLphp. Pulsando en el enlace **Show/Hide XML** se pueden ver los metadatos de la conexión en formato XML.



7.- Acceso como usuario Lector

Un usuario con el rol **Lector** puede autenticarse en el sistema para ver la lista de conexiones SP e IdP y exportar sus metadatos, pero no puede crear conexiones ni editar ninguno de los parámetros de las conexiones creadas: ni su tipo, estado o metadatos.