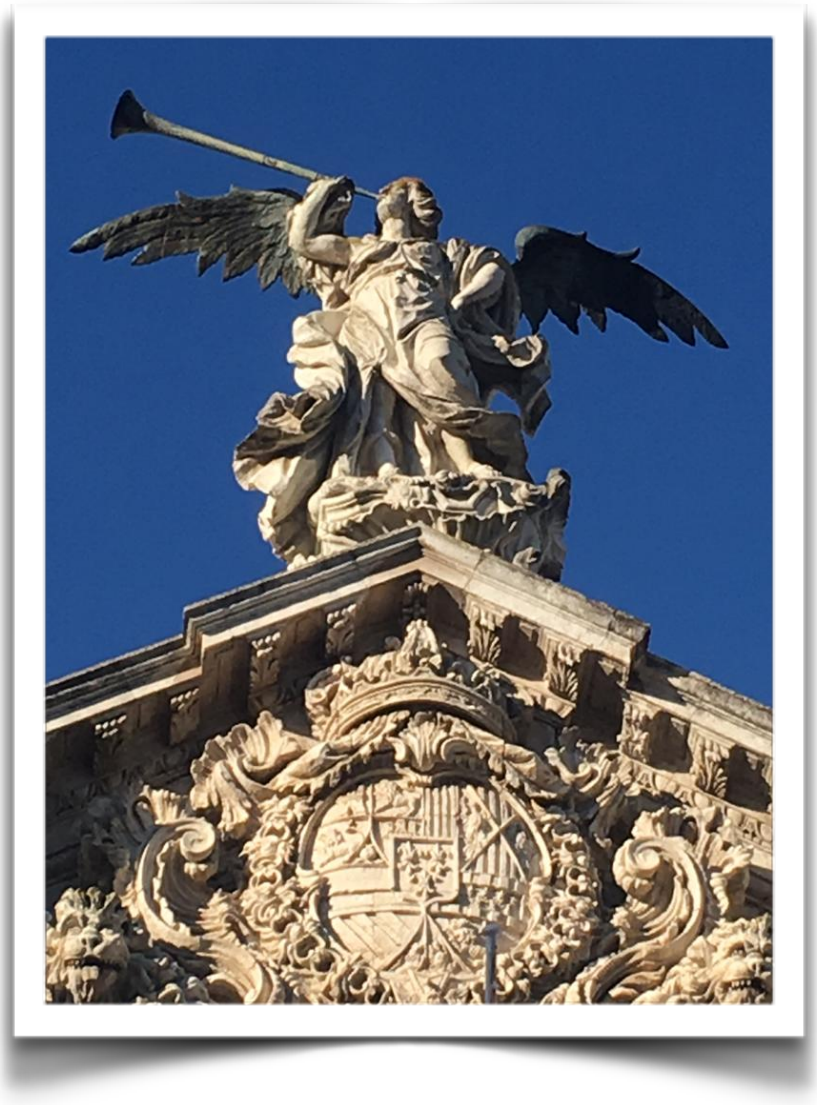
Actualidad SIR2 / eduroam



José Manuel Macías Luna

@lonoak

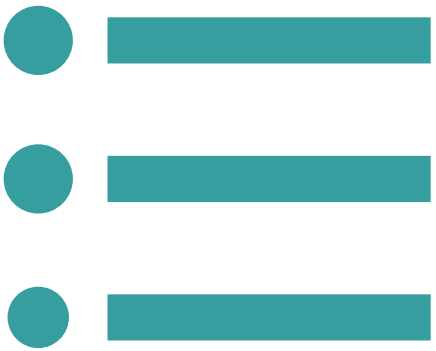
jmanuel.macias@rediris.es

Sevilla, 28 de mayo de 2019

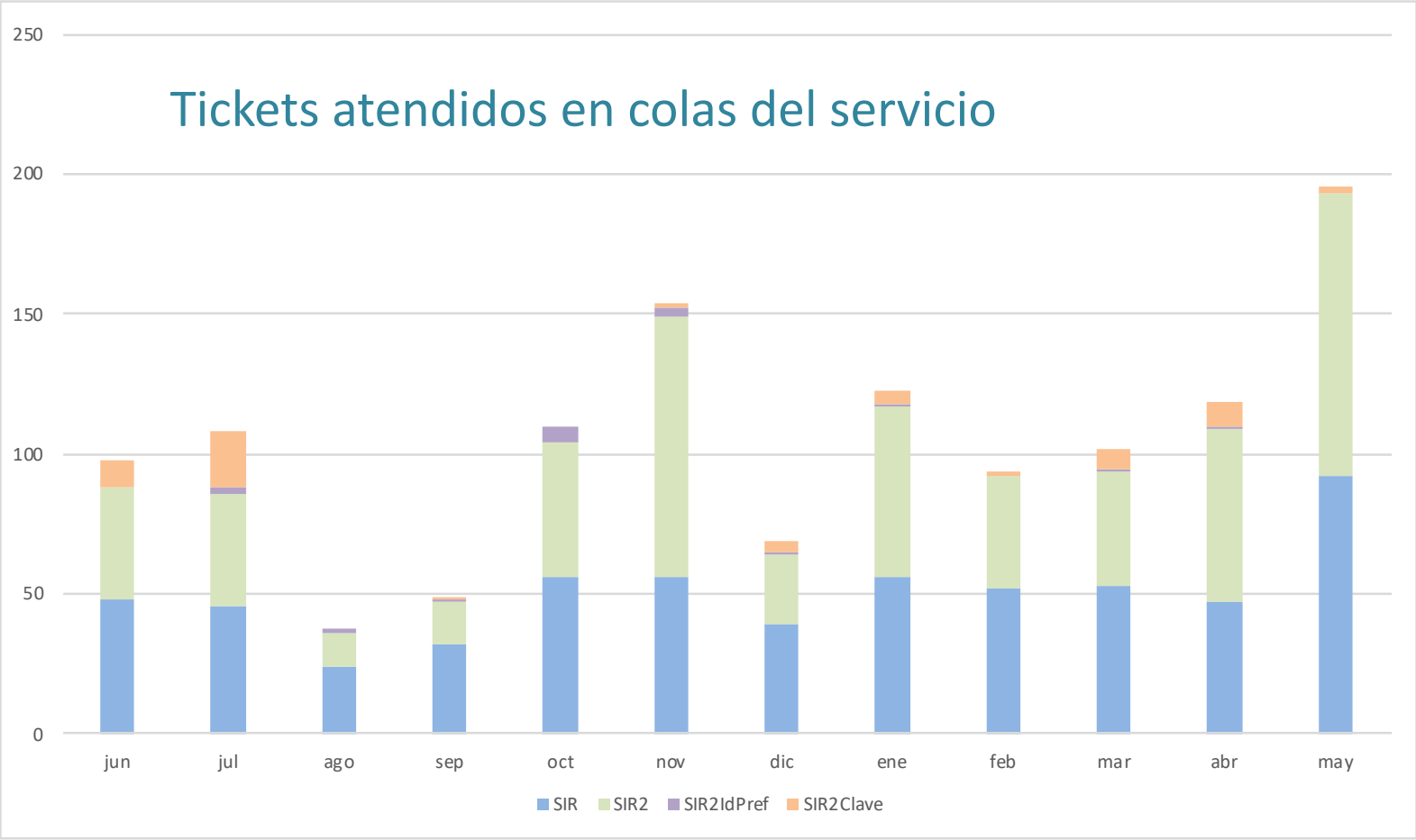
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
Red IRIS
red.es
Infraestructuras Científicas y Técnicas Singulares

Agenda

- Actualidad federación de identidades
  - Operación del servicio / migración
  - Cl@ve / Cl@ve 2
  - eduGAIN
  - IdP en la nube
- Actualidad eduroam
  - eduroam Managed IdP
  - piloto eduroam Visitor Access



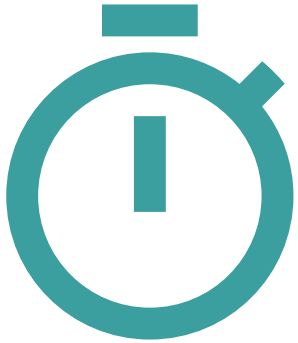
Operación del servicio de federación de identidad



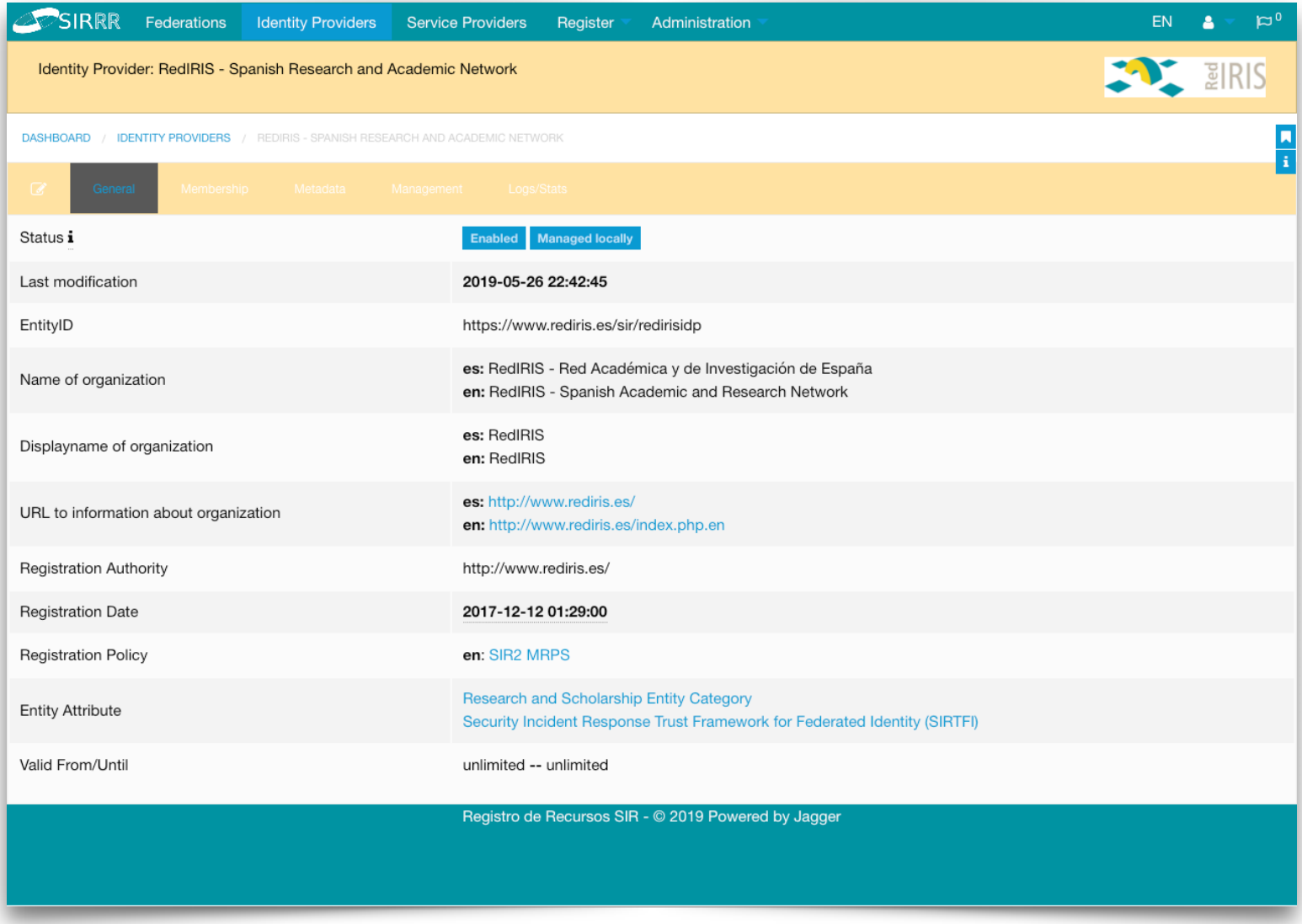
1260 tickets válidos atendidos en el último año

Operación del servicio de federación de identidad

- Menos tickets de migración de IdPs PAPI a SAML2
  - la mayoría ha concluido la migración
- Pasarela SAML de salida (de SIR) ha ocupado buena parte de nuestro tiempo
  - Actualización del software
  - Preparación para “migración de SPs”
- Puesta en marcha paulatina de SIRRR
  - SIRRR = SIR Resource Registry

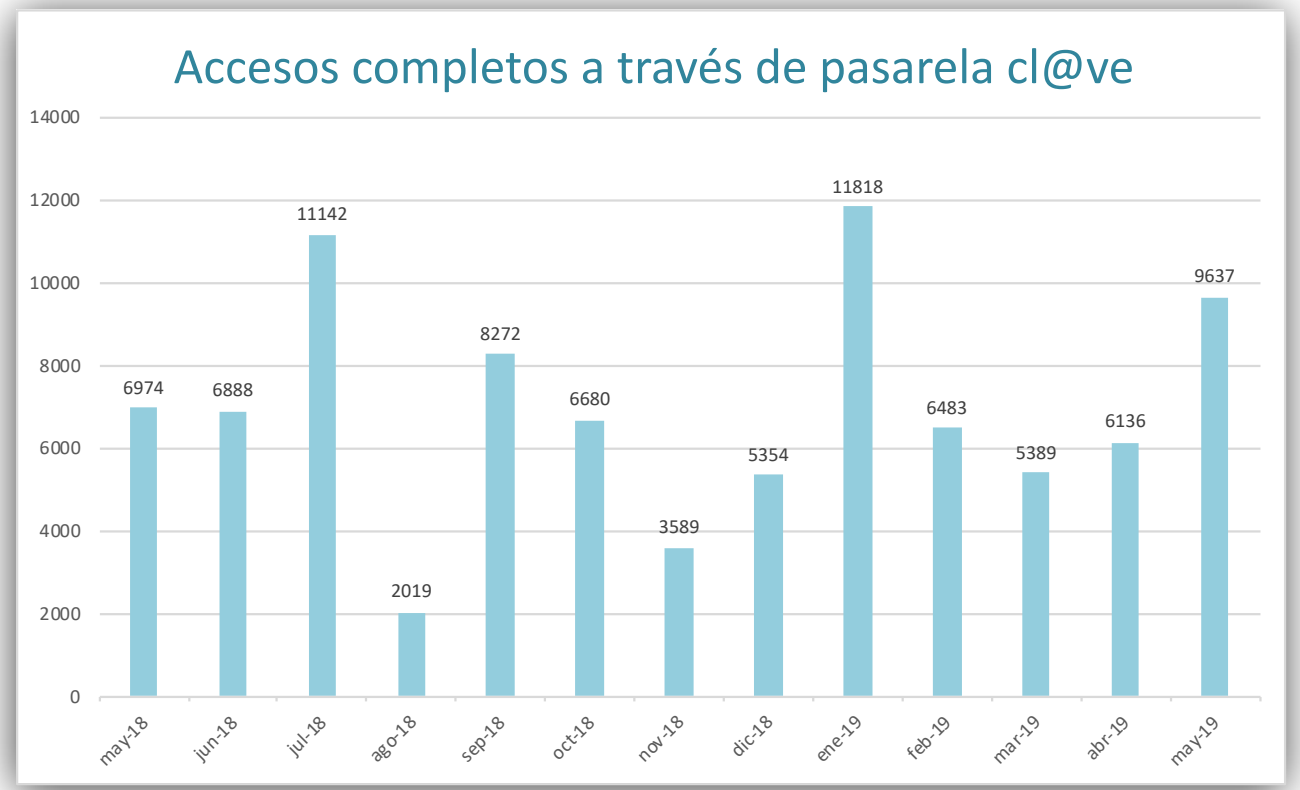


SIR Resource Registry



Cl@ve / Cl@ve 2

- Algunos datos de pasarela cl@ve(producción):
  - Proveedores de servicio: 34
  - Instituciones: 18



Cl@ve / Cl@ve 2

- Cl@ve 2 ya funcionando en pre-producción y producción
- Todo listo para comenzar la transición a cl@ve2:
  - Para SPs SAML2 WebSSO, solamente cambiar end-point y tener en cuenta el nuevo perfil de atributos
  - Para SPs Cl@ve, deberán transicionar a medio plazo (desaparecerá la infraestructura del lado del ministerio) a Cl@ve 2:
    - la pasarela ofrece una interfaz cl@ve a cl@ve2
    - no recomendable: los kits están sin soporte
  - Para SPs Cl@ve2 ofrecemos soporte, pero recomendamos WebSSO
  - Inminentemente se lanzará el nuevo entorno de producción de la pasarela, así como documentación con detalles sobre estos cambios
  - Actualmente podéis ya solicitarlo en el entorno de pre-producción de la pasarela
  - Para niveles de confianza sustancial o alto, es requisito usar Cl@ve 2 en servicios públicos

Cambios en eduGAIN

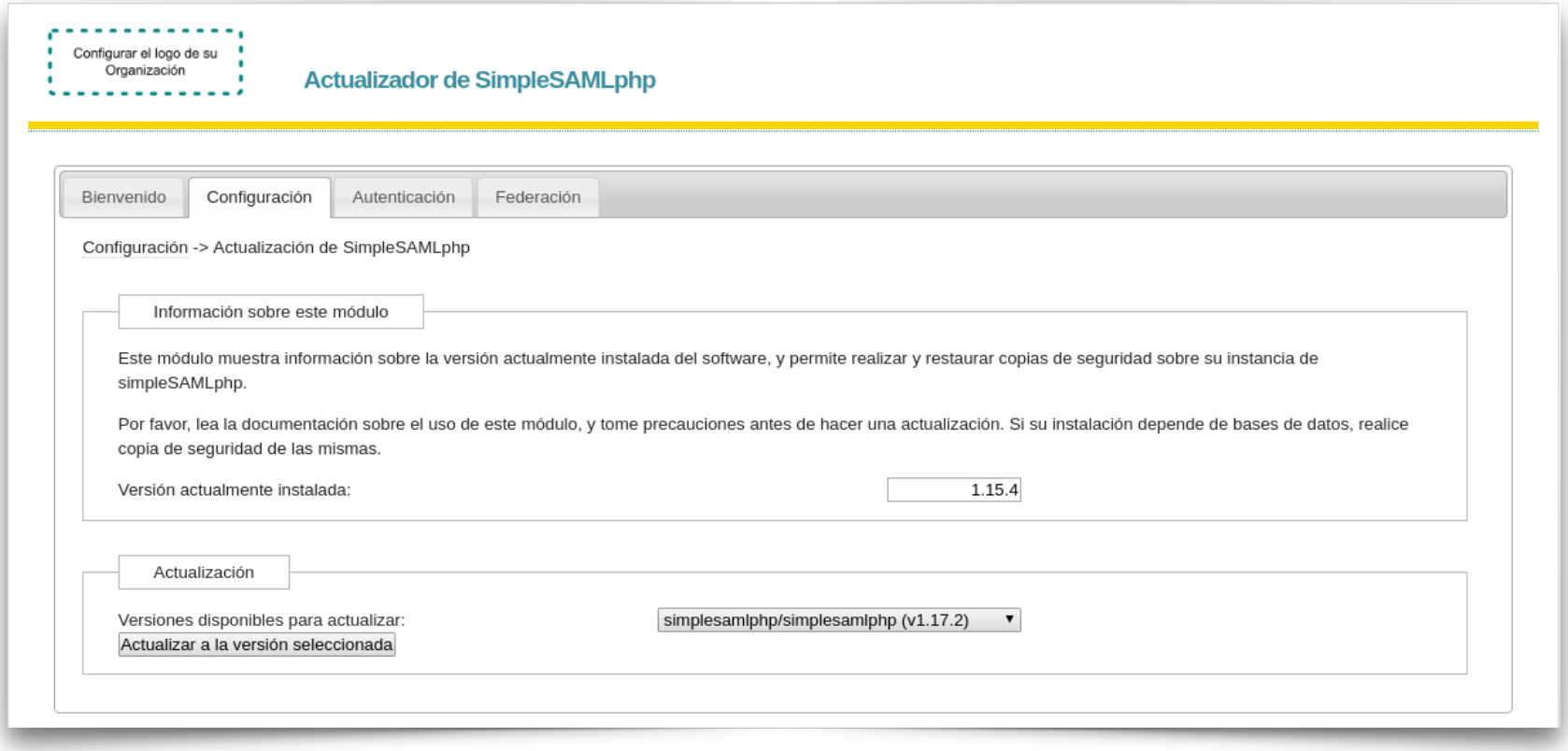
- Actualmente ya hay 77 proveedores de identidad de nuestra federación en eduGAIN
- Se están introduciendo algunos cambios en los metadatos que exportamos:
  - “Research & Scholarship” y “SIRTFI” serán Opt-out
    - Opt-In “CoCo v.1”, pendiente “CoCo v.2”
  - Se incluyen mejoras en extensiones de metadatos de interfaz de usuario
- Cada vez más servicios disponibles a través de eduGAIN
  - Incorporación de servicios InAcademia y eduTeams

Más sobre eduGAIN

- Documentación útil:
  - Herramientas de eduGAIN (wiki de SIR2):
    - https://redir.is/GJAXV
  - Kit de desarrollo de políticas de AARC (Authentication and Authorization for Research and Collaboration):
    - Orientado a infraestructuras científicas que deseen desplegar servicios que necesiten soportar autenticación y autorización
    - Plantillas de políticas, guías de uso, vídeos explicativos, y glosario disponibles
    - https://aarc-project.eu/policies/policy-development-kit/

Soporte IdP de referencia

- Nuevo pre-instalador, basado en composer:
  - https://redir.is/JEDMX
- Nuevo módulo de actualización: https://redir.is/PVTJA



Piloto IdP en la nube

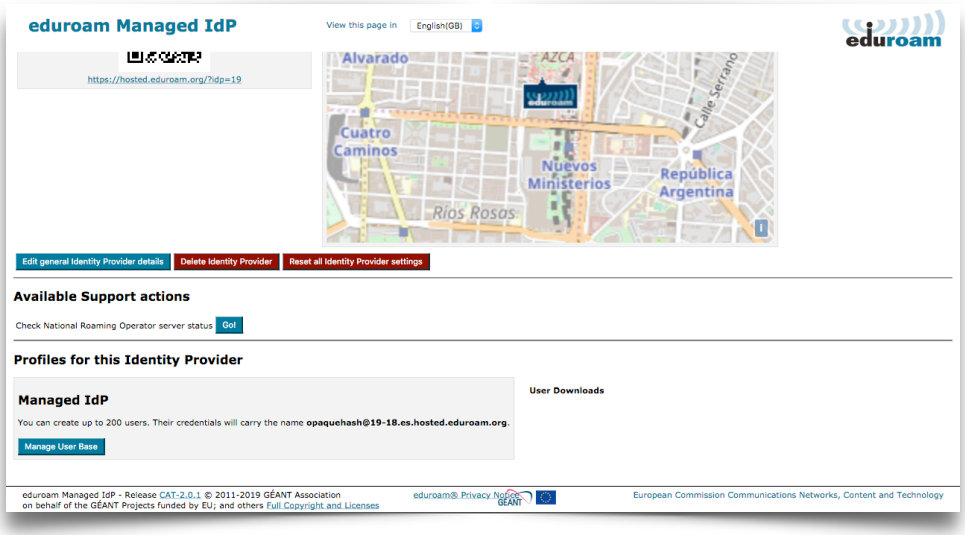
- Retrasos en el comienzo del piloto
  - previsión de comenzar en junio
- Se ha estado trabajando en:
  - Despliegue del *cluster* k8s de producción
  - CVE-2018-1002105 (kube-apiserver) y CVE-2019-5736 (runc)
  - Finalización entorno de integración continua
  - Almacenamiento seguro de contraseñas (Argon2)
  - Funcionalidad de cambio de contraseñas
  - Requisito de acceso con doble factor al panel de administración

SIR2nube

eduroam Managed IdP

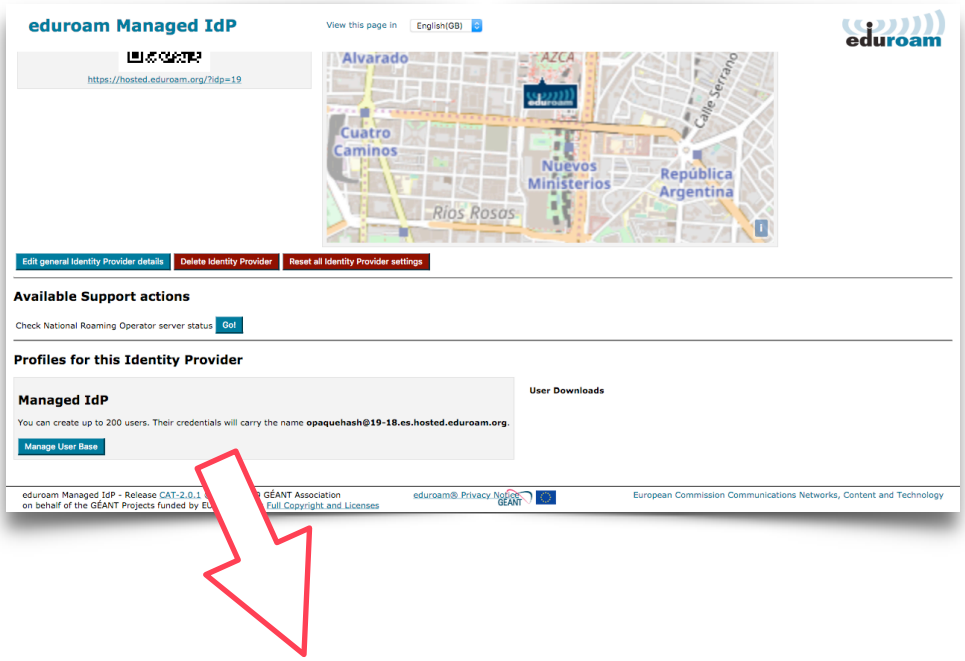
- “IdP eduroam para instituciones pequeñas”
- Gestión de usuarios + Instancia de eduroam CAT
- EAP-TLS como método de autenticación
  - no se utilizan el usuario y contraseña de la institución
- Invitación a los usuarios mediante correo electrónico
- Lo que es:
  - un IdP en eduroam para instituciones de tamaño pequeño
  - una solución cómoda para el administrador
- Lo que **no** es:
  - una solución que escale bien
  - una solución para visitantes

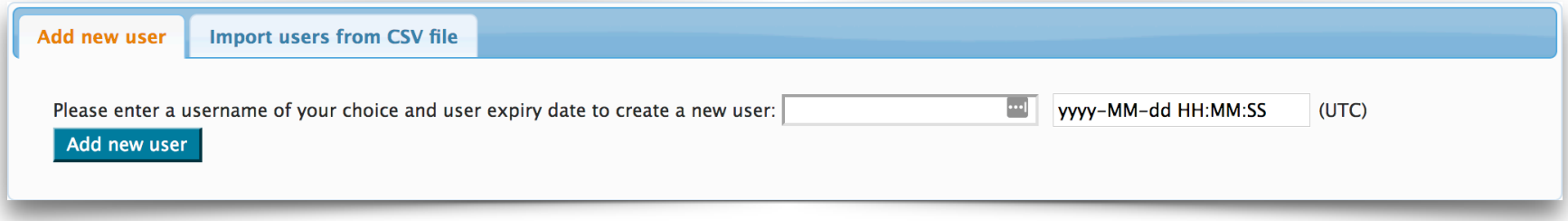
eduroam Managed IdP



GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares
eduroam

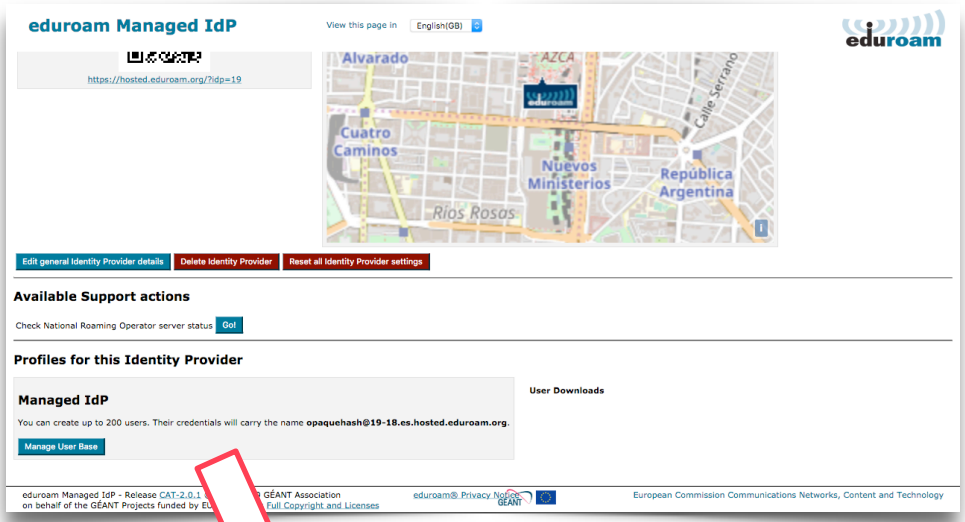
eduroam Managed IdP

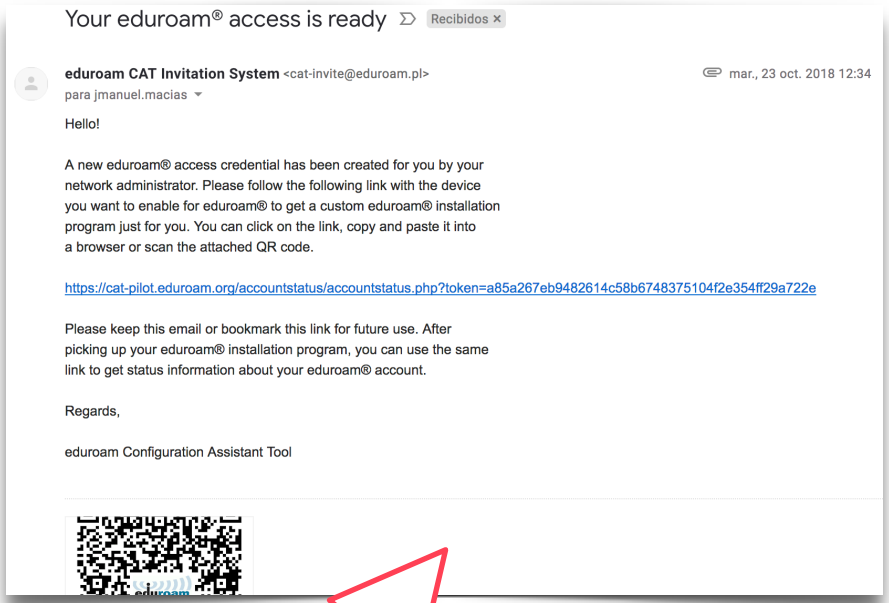


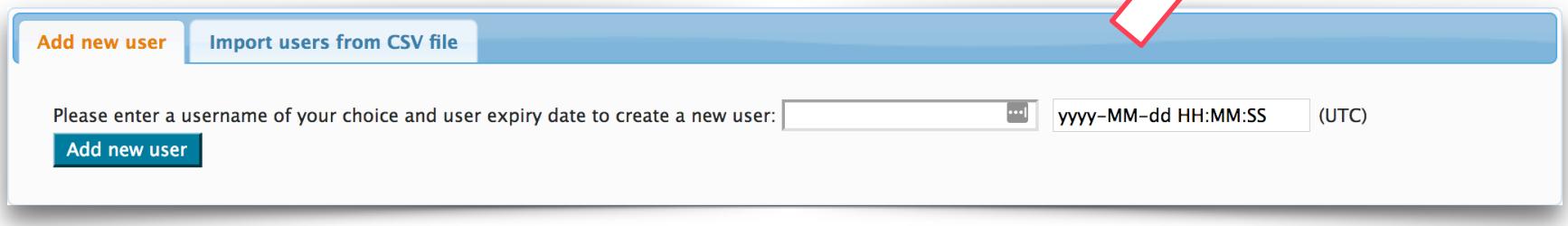


GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares
eduroam

eduroam Managed IdP







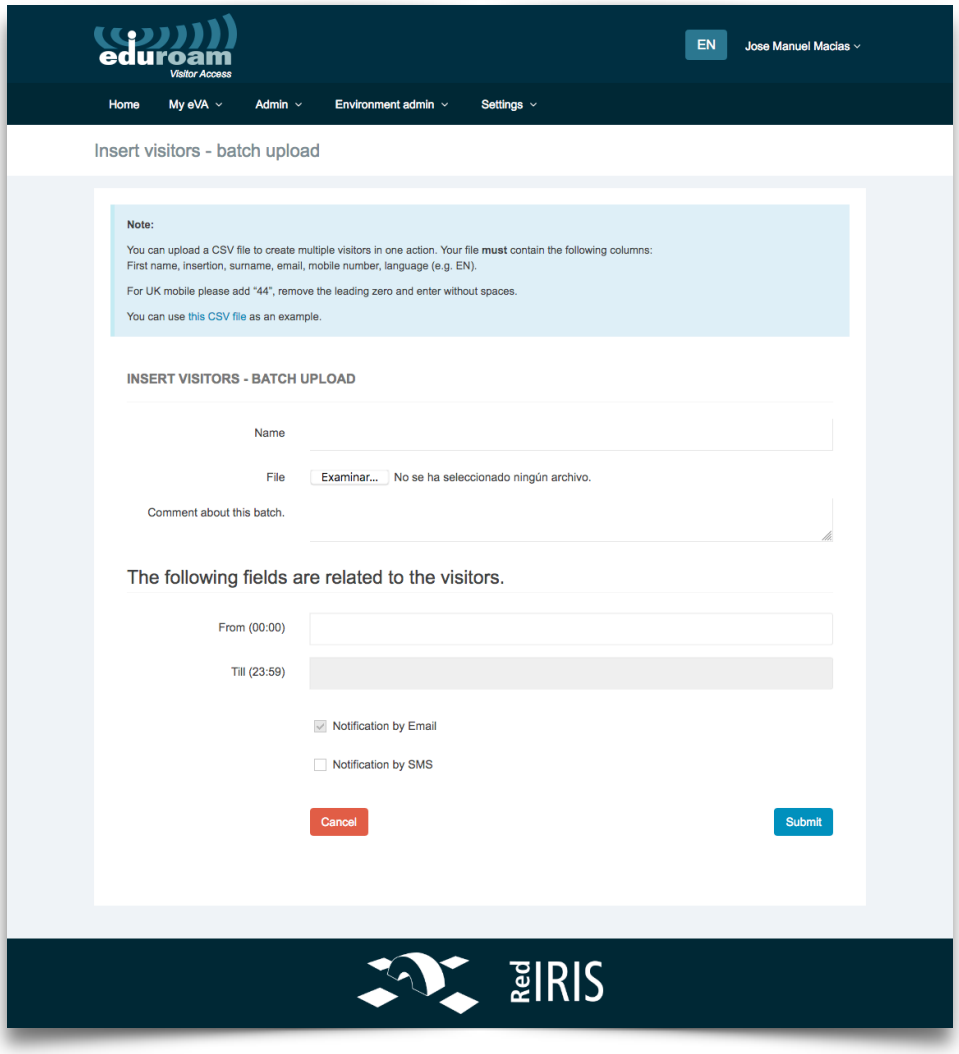
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS
red.es
Infraestructuras Científicas y Técnicas Singulares
eduroam

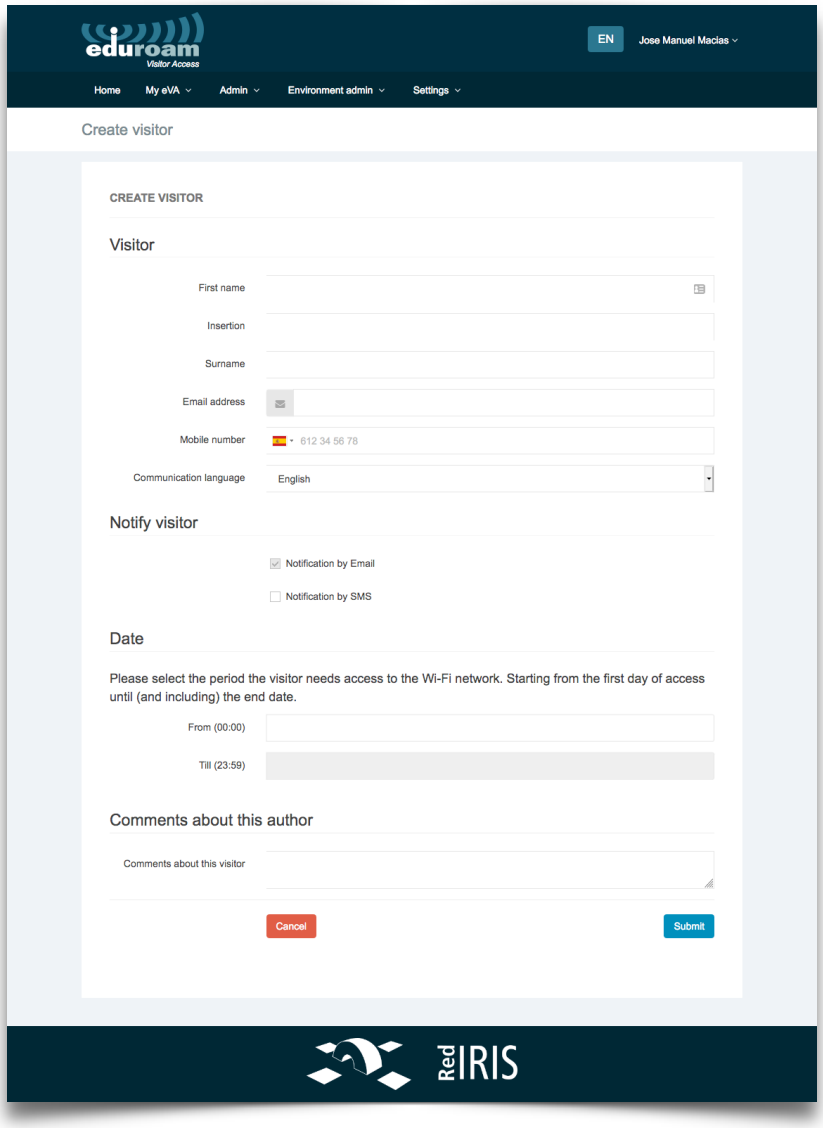
eduroam Visitor Access

- Piloto de eduroam para acceso de visitantes
- Una solución para la gestión de credenciales
- Utiliza una instancia proporcionada a través de acuerdo con eduroam NL (SURFnet)
- Algunas características
  - gestión delegada de invitaciones
  - configuración de la duración de las invitaciones
  - invitaciones por correo y SMS
  - renovación/revocación de invitaciones
  - carga de invitaciones en bloque

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
RedIRIS red.es
Infraestructuras Científicas y Técnicas Singulares
eduroam

eduroam Visitor Access





GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO DE ECONOMÍA Y EMPRESA
Red IRIS
red.es
Infraestructuras Científicas y Técnicas Singulares