

Política de movilidad de la iniciativa eduroam ES

Version 1.1

Introducción

La creación de un espacio común de movilidad entre todas las instituciones académicas y de investigación englobadas en las redes europeas de investigación, requiere la adopción de una política común de uso de la tecnología.

Este documento pretende ser una guía de uso de la infraestructura eduroam para España, que está basado y es compatible con la política desarrollada dentro de la actividad JRA5 de GÉANT2.

Objetivo

El objetivo principal de este documento es formalizar la relación entre organizaciones que configuran "**eduroam ES**", aportando procedimientos compatibles con la misma iniciativa a nivel europeo y que faciliten la gestión de la movilidad entre organizaciones a nivel nacional.

La idea

El proyecto eduroam ES consiste en el desarrollo de un espacio de colaboración para facilitar la movilidad en el acceso a la red entre organizaciones de la comunidad RedIRIS, de tal forma que cuando sus usuarios viajen a otras organizaciones, éstos puedan disponer de una manera automática de servicios de conectividad u otros que en un futuro se vayan considerando como necesarios.

Esta política está desarrollada en concordancia con la desarrollada a nivel de las redes de investigación europeas. Es responsabilidad del usuario móvil respetar las políticas de uso tanto de la institución visitada, como de su organización origen.

Servicio de movilidad - Principios generales

- El servicio de movilidad común debe ser prestado únicamente a usuarios que pertenezcan a organizaciones afiliadas a redes de investigación que pertenecen al proyecto de espacio común de movilidad a nivel internacional.
- A todos los usuarios móviles se les requerirá autenticarse frente a su organización origen, con el fin de obtener servicios de acceso en la organización visitada.
- Todos los usuarios móviles son responsables de sus credenciales y deben respetar la política de uso aceptada por su organización origen.
- Las organizaciones visitadas deben ofertar servicios de acceso, y además, los usuarios móviles podrán reconocerlos y hacer uso de ellos.
- La organización visitada debe garantizar la transmisión segura de las credenciales de los usuarios móviles.
- La organización visitada tiene potestad de bloquear el acceso a cualquier usuario móvil, institución o red europea de investigación, si no cumpla con la política de uso de la organización visitada.
- Las organizaciones visitadas establecerán la autorización para el acceso a los servicios prestado a los usuarios móviles.
- La organización origen será responsable de dar soporte a sus usuarios, incluyendo formación en tecnologías de acceso y aceptación de políticas de uso.

Requisitos a cumplir por las organizaciones participantes en eduroam ES

1. Las organizaciones participantes deben responsabilizarse de formar a sus usuarios en el respeto a las políticas de uso de las organizaciones visitadas, y ayudar en cualquier aspecto relacionado con sus usuarios.
2. Las organizaciones participantes deben poseer un servidor de autenticación (NAS) que pueda, de un modo seguro, procesar y transmitir las credenciales de usuario solicitadas, utilizando para ello paquetes Access-Accept de RADIUS, en conformidad con la sección 3.16 de la RFC3580.
3. Las organizaciones participantes deberían disponer de mecanismos para informar a los usuarios visitantes de en qué medida y cómo ofertan sus servicios de movilidad.
4. Es obligatorio el uso del SSID "eduroam" excepto en aquellos casos en los que exista un solapamiento de puntos de acceso de distintas organizaciones físicamente muy cercanas. Para aquellos puntos de acceso en los que se de este solapamiento se recomienda el uso de SSIDs de la forma "eduroam-[INST]", donde [INST] son una sigla descriptiva de la institución a la que pertenece cada uno de los puntos de acceso en cuestión.
5. Las organizaciones participantes deberían disponer de mecanismos para informar a sus usuarios visitantes de los niveles de seguridad ofrecidos en la transmisión de credenciales.
6. Las organizaciones participantes deben informar a sus usuarios del servicio de movilidad, señalando que el soporte técnico recae sobre su organización origen. Sólo cuando la organización origen determina que el problema es responsabilidad de la organización visitada, éste debe ser revisado con la organización visitada.
7. Las organizaciones participantes deben guardar información relativa a sesiones de autenticación y acceso a la red. Asimismo deben ser capaces de capaces de realizar un seguimiento de un usuario por razones de seguridad o gestión de capacidad. En concreto, deberán mantener la correlación de direcciones MAC y direcciones IP dadas a los visitantes mediante DHCP, junto con la hora, establecida a partir de una fuente fiable de tiempo, en la que se produjo la asignación. Las organizaciones participantes deben comunicar problemas de seguridad o uso fraudulento tanto a los responsables de la iniciativa eduroam ES, como a los responsables de seguridad de RedIRIS (IRIS-CERT), para solucionarlo de manera coordinada.
8. Las organizaciones participantes deben disponer de mecanismos de monitorización y seguimiento que permitan conocer el estado de los servidores de autenticación, para poder analizar problemas de conexión.
9. De acuerdo con la política establecida para el servicio a nivel europeo, sólo podrá usarse el SSID "eduroam" para mecanismos de control de acceso basados en el estándar IEEE 802.1x. Aquellas organizaciones que usen otros métodos (notablemente, los basados en redirecciones HTTP) cuentan para su adaptación con una moratoria que expira el **30 de septiembre de 2007**.