

Expand **SECURITY**

Plataforma de Seguridad para Aplicaciones Web



BASE 100, S.A.

Santa María Magdalena, 10-12

28016 – Madrid

Tel.: 91 353 18 15

www.base100.com

Índice

1.	INTRODUCCIÓN	3
2.	DESCRIPCIÓN DE EXPAND SECURITY	4
2.1	GESTIÓN DE USUARIOS Y CREDENCIALES.....	4
2.2	GESTIÓN DE APLICACIONES, ROLES, RESTRICCIONES Y PERMISOS	5
2.3	IMPORTACIÓN Y EXPORTACIÓN DE DATOS DE SEGURIDAD	6

1. Introducción

Expand **SECURITY** es un gestor horizontal de servicios de seguridad que proporciona de forma automática un conjunto de funcionalidades de autenticación (gestión y comprobación de credenciales de usuario) y autorización (gestión de restricciones, roles y permisos por usuario y aplicación).



La comunicación entre las aplicaciones y el servicio centralizado de seguridad se realiza exclusivamente mediante una infraestructura de servicios SOA. El módulo centralizado gestor de autenticación y autorización delega la persistencia de las credenciales, roles, restricciones y permisos mediante una interfaz específica, en varias implementaciones estándares (tablas de base de datos, infraestructura LDAP, ficheros XML encriptados) y permite escribir un módulo de persistencia adaptado a las necesidades del ambiente de ejecución del cliente.

2. Descripción de Expand SECURITY

La plataforma Expand **SECURITY** permite centralizar, en una única interfaz de programación, todas las funcionalidades de autenticación y autorización necesarias en el desarrollo de aplicaciones Web.

La plataforma de seguridad provee una aplicación Web para la gestión de usuarios, credenciales de acceso, aplicaciones, roles, permisos, etc. De esta forma, es posible centralizar toda la administración de seguridad para diferentes aplicaciones sin necesidad de incluir en cada una de ellas módulos específicos de administración de seguridad. Sin embargo, Expand **SECURITY** provee de una batería de servicios Web mediante los cuales es posible realizar cualquier operación de administración desde las propias aplicaciones integradas.

2.1 Gestión de usuarios y credenciales

Expand **SECURITY** puede almacenar la información de usuarios, roles y credenciales de acceso tanto en tablas de base de datos como en un servidor LDAP. Así mismo, es posible desarrollar un *plugin* específico para almacenar esa misma información en otras infraestructuras de seguridad con las que haya que integrarse.

Editar Usuario por Aplicación

Login: 99-23456789-07
 Usuario: JESÚS VILA GARCÍA

* Campos requeridos

Roles

Nombre	Descripción
MANDAMENTOS	Gestion de Mandamientos con la Oficina de Mandamientos

Añadir Rol Añadir Roles al Usuario

Perfiles de Aplicación

Nombre del perfil	Contexto
Secretario	SECRETARIA_1_014_027

Añadir Perfil de Aplicación Añadir Perfiles al Usuario

Valores definidos

Nombre	Valor
CUIL	27349277390

Añadir Valor

Volver Guardar Borrar

Las claves de acceso se almacenan de forma cifrada (*encrypted*). El sistema de comprobación de credenciales indica la fortaleza de la clave de acceso al introducirla en la aplicación de administración. Además, para evitar que mediante una aplicación se pueda llegar a descubrir la clave de un usuario (probando muchas combinaciones) se ha incluido un sistema de bloqueo al introducir varias veces una clave errónea y de desbloqueo automático al pasar un tiempo.

Mediante un conjunto de roles de seguridad específicos, Expand **SECURITY** ofrece la posibilidad de que diferentes usuarios del sistema puedan realizar tareas de seguridad concretas. Hay tres roles de seguridad globales: *admin*, que puede ejecutar cualquier acción; *development*, que puede definir nuevas aplicaciones, roles por aplicación y permisos; y *securityUser*, que puede añadir nuevos usuarios al sistema y asignarles aplicaciones y roles.

2.2 Gestión de aplicaciones, roles, restricciones y permisos

Para dar soporte a las restricciones de los diferentes elementos funcionales de una aplicación, Expand **SECURITY** permite definir, por cada aplicación incluida en el sistema, un conjunto de objetos restringidos, identificados cada uno de ellos por un nombre. Este conjunto de restricciones se corresponderá, normalmente, con las entidades manejadas por la aplicación. Por cada objeto restringido se pueden definir varias acciones (consulta, alta, modificación, borrado, impresión, etc.), que se corresponderán con cada una de las restricciones funcionales que se comprobarán en cada uno de los componentes de la aplicación.

The screenshot displays the 'Lista de Restricciones por Aplicación' (Restrictions List by Application) interface. It features a sidebar with a tree view of application objects, including 'Abogado', 'AccionModelo', 'ActuacionExp', 'AdEffectumVidendiExp', 'AgendaExp', 'AgendaOficina', 'Alarma', 'AtributoObjetoJuicio', 'Calendario', 'Camara', 'cargaFeria', 'cargaMesaEntrada', 'Causa', 'CedulaExp', 'CedulaExpMasivo', 'ControlInternamiento', 'CodigoPostal', 'CombinarDocumentos', 'CondicionCnx', 'Conexidad', 'ConexidadDeclarada', 'ConfiguracionOficina', 'ConfronteExp', 'CriterioCnx', and 'Cuaderno'. The main area is divided into several sections:

- Editar Restricción (Edit Restriction):** A form for defining a restriction. The 'Nombre del Objeto' (Object Name) is 'AccionModelo' and the 'Descripción' (Description) is 'Accion Modelo'. It includes 'Valer', 'Guardar', and 'Borrar' buttons.
- Acciones (Actions):** A table listing actions for the selected object.

Acción	Descripción	Condición	Permiso requerido
access	Acceso desde el menú		
- Editar Rol (Edit Role):** A form for defining a role. The 'Nombre del Rol' (Role Name) is 'MANDAMIENTOS' and the 'Descripción' (Description) is 'Gestion de Mandamientos con la Oficina de Mandamientos'. It includes 'Campos requeridos' (Required Fields) and 'Permisos' (Permissions) sections.
- Permisos (Permissions):** A table showing the permissions assigned to the role.

Restricción	Descripción	Acción	Descripción
Mandamiento	Gestion de Mandamientos	access	Access from menu
Mandamiento	Gestion de Mandamientos	envio	Envío a la Oficina de Mandamientos
- Roles para conceder (Roles to be granted):** A section indicating 'No tiene Roles definidos' (No roles defined).
- Usuarios (Users):** A table listing users who can be assigned the role.

Id. Usuario	Usuario
99-48051905-06	ANTONIO OROZCO SAN SEGUNDO
99-28763064-05	AURORA PUEYO MARTÍNEZ
99-23456789-07	JESÚS VILA GARCÍA
99-08036974-06	LUIS COLOMER SERRANO
99-54025736-04	MARIO PASCUALIBORRA

La granularidad con la que se definen las acciones (el número de acciones a restringir) se decide para cada objeto restringido, ya que, normalmente, las acciones por objeto restringido dentro de una misma aplicación suelen ser las mismas.

Expand **SECURITY** permite definir una plantilla de permisos para que se creen automáticamente al dar de alta un nuevo objeto restringido.

Por cada aplicación incluida en Expand **SECURITY** se podrán definir unos roles específicos. Dichos roles se pueden asignar a los usuarios de la aplicación de forma aditiva (un usuario puede tener varios roles). Cada uno de los roles puede contener opcionalmente un conjunto de referencias a acciones restringidas, de manera que un usuario, al adquirir un rol, adquiere automáticamente el permiso de cada una de las acciones que contiene dicho rol.

2.3 Importación y exportación de datos de seguridad

Expand **SECURITY** permite exportar e importar en formato XML los datos de configuración de seguridad para una aplicación, de manera que se puedan traspasar fácilmente de un entorno a otro.

Por último, se puede realizar un ajuste muy específico de los permisos utilizando reglas de negocio en notación JBoss Drools. Este *framework* funcional permite establecer reglas de permisos que, combinando *wildcards* y reglas de negocio, se ajusten mucho mejor al modelo de seguridad que necesita la aplicación.