



Technical Datasheet

SmartLogin® V1.3 Technical Overview

INDEX

1.Overview.....	3
1.1.On-premises y On-Cloud.....	3
2.¿Por qué SmartLogin?.....	4
2.1.¿Otras razones?.....	5
3.Componentes.....	6
3.1. Single Sign-On.....	6
3.2. Integración con el Directorio central de autenticación.....	7
3.3.Federación de identidad.....	7
3.4.Proxy Federado e inyección de credenciales.....	8
3.5.Gestión de usuarios.....	8
3.6.Informes y análisis.....	9
3.7. Seguridad.....	9
3.8.Autenticación Multi-factor (MFA).....	10
3.9.Envío de notificaciones.....	10
3.10. Gestión de dispositivos móviles.....	11
3.11.Gestión de Desktops y Laptops.....	11
3.12.Restablecimiento seguro de contraseña.....	12
3.13.Auto servicio.....	12
3.14.Gestión de acceso (Perfiles).....	13
3.14.1.Panel de usuario (autoservicio):.....	13
3.14.2.Panel de Administración:.....	14
3.15.Autenticación adaptativa (políticas).....	15
3.16.Políticas sobre aplicaciones.....	15
3.17.Gestión de acceso delegado.....	15
3.18.Multi-zonas.....	16
3.19.Servicios Web.....	16
3.20.Servicio de bloqueo de IPs.....	17
3.21.Actualización de la base de datos GeoIP.....	17
3.22.RESTful.....	17
3.23.Syslog Remoto.....	17
3.24.Integración con HSM.....	18
3.25.Marketplace.....	18
4.Usabilidad e idiomas.....	19
4.1.Visual y diseño.....	19
4.2.Idiomas.....	19
4.3.Imagen corporativa personalizable.....	19
4.4.Plantillas de Email.....	19
5.Copias de seguridad.....	20
6.Monitorización.....	21
6.1.Engeens.....	21
6.2.SNMP.....	22
6.3.SmartLogin Crash Reporter.....	22
7.Arquitecturas.....	23
7.1.Arquitectura 1.....	23
7.2.Arquitectura 2.....	23
7.3.Arquitectura 3.....	24
8.Actualizaciones.....	25
9.Suscripciones y soporte.....	26
9.1.Información sobre la suscripción de soporte.....	27
9.2.Otros servicios de suscripción.....	27

1. Overview

SmartLogin® permite a las organizaciones centralizar la seguridad y el control de acceso a los servicios corporativos en la nube (Software-as-a-Service) y on-premise desde cualquier lugar y dispositivo.

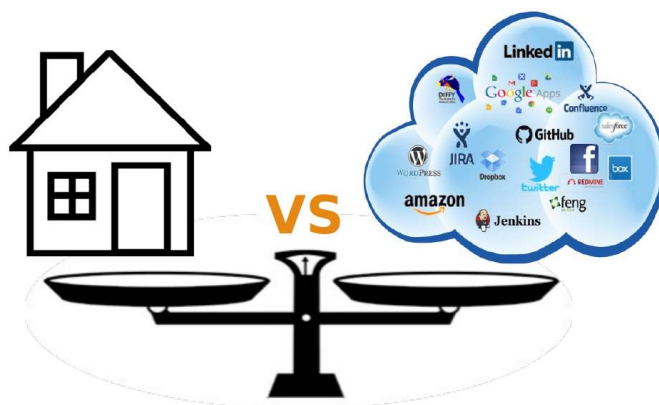


Consiste en una plataforma que refuerza la seguridad a través de: una vigilancia de las sesiones en tiempo real, y un sistema de alertas y políticas de seguridad para los usuarios y dispositivos móviles (BYOD, Bring Your Own Device). Apoyándose en este tipo de dispositivos, es capaz de controlar el inicio de sesión, ofreciendo así una nueva generación de sistemas de control de acceso multiprotocolo (SAML, CAS, etc), federación de identidad y Single-Sign-On (SSO). De esta forma, se elimina la necesidad del uso de

contraseñas, permitiendo incluso la utilización de MFA (Multi-factor Authentication) para todo el entorno corporativo: tanto on-premise, como nube.

1.1. On-premises y On-Cloud

SmartLogin® está basado en una plataforma de tipo Appliance virtual que integra todos los componentes lógicos necesarios en una única plataforma. No requiere la adquisición ni instalación de sistemas operativos ni aplicaciones de terceros para funcionar. Puede adquirirse como un servicio en la nube o como un appliance virtual incluyendo los ficheros estándar necesarios para desplegar una "virtual machine" en las principales plataformas de virtualización.



Esto permite desplegarse tanto en nuestro propio cloud, on-premise en el cliente o en cloud público, ya sea Amazon, Google Cloud, Azure, etc.

2. ¿Por qué SmartLogin?

“....One sign to rule them all”

En la actualidad, las empresas gestionan múltiples servicios de autenticación para proporcionar a sus empleados acceso a servicios empresariales ya sea en la nube o en sus instalaciones internas (incluidos los entornos IaaS alojados en la nube). Al mismo tiempo, los empleados tienen que mantener una larga lista de contraseñas diferentes para acceder a las aplicaciones corporativas que a veces terminan anotadas en una nota bajo su teclado que rompe el requisito de seguridad mínimo.

Los departamentos de TI dedican más recursos para gestionar el ciclo de vida de los empleados, así como los servicios que mantienen diferentes bases de datos de usuarios, no sólo el registro central que da acceso a servicios corporativos internos, sino también servicios descentralizados en nube como Google Apps u Office 365.

SmartLogin® es un servicio de inicio de sesión único gestionado (SSO) y un proveedor de identidad basado en Web Access Management (WAM). SmartLogin® ofrece a los departamentos de TI la capacidad de mantener una base de datos centralizada de usuarios en integración con OpenLdap y Active Directory (AD). Los departamentos de seguridad pueden reforzar las políticas de contraseña ya que el usuario ya no necesita recordar una contraseña por servicio web, así como las auditorías internas a través de reportes de acceso, alarmas en tiempo real y políticas de acceso. Además, SmartLogin® mejora la productividad ya que los empleados sólo necesitan iniciar sesión en una granja de servicios corporativos con una sola identificación y una sola vez. En resumen:

- SmartLogin® proporciona la capacidad de unificar el inicio de sesión al acceder a uno o más sistemas con diferentes directorios de usuario
- SmartLogin® reduce la gestión de autenticación
- SmartLogin® proporciona mecanismos de Identidad federada que permite a varias organizaciones compartir las mismas aplicaciones
- SmartLogin® permite que una sola organización pueda administrar identidades y autenticaciones

¿Con cuántas aplicaciones se pueden conectar SmartLogin®? Cientos...



2.1. ¿Otras razones?

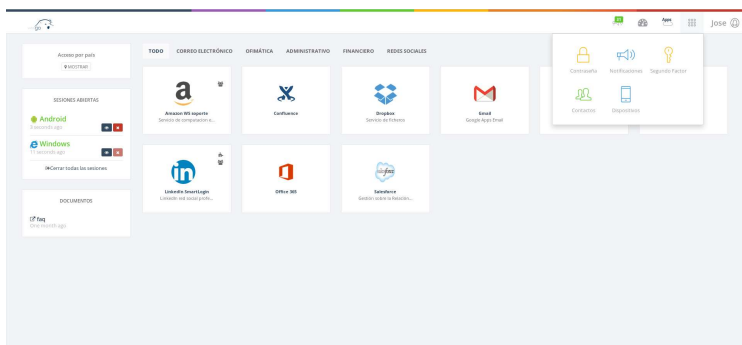
SmartLogin® se presenta como la mejor solución debido a los siguientes factores:

- Plataforma capaz de dar respuesta a la totalidad de los requerimientos de un cliente de una forma óptima en términos de coste económico, de esfuerzos en el despliegue y de su posterior explotación.
- Plataforma basada en modelo de suscripción de soporte, lo que supone un ahorro importante al no existir coste de licencia asociado.
- Plataforma basada en código abierto en su mayor parte y en estándares de mercado, lo cual la convierte en una plataforma altamente interoperable.
- Plataforma basada en Appliance virtual, que incluye todos los componentes lógicos necesarios para su funcionamiento, todos ellos listos para ser utilizados desde el primer momento. Esto supone un ahorro importante de tiempo en el despliegue, y por ello en los costes del proyecto.
- Gran integración de componentes en un único sistema, gestionados desde una interfaz web centralizada e integrada. Esto contribuye de manera significativa a una mayor facilidad de administración.
- Plataforma dotada de diversos mecanismos de gestión que facilitan la evolución y administración de la misma (SNMP, WatchDog, Backup Services, REST Services, Update Services, Remote Support...)
- Gran facilidad a la hora de realizar actualizaciones sobre la plataforma. Todas las actualizaciones del sistema sean al nivel de componente que sean, se realizan desde la propia interfaz gráfica en pocos minutos. Esto no sólo garantiza un despliegue de actualizaciones ágil, sino que dota de estabilidad al sistema al controlar directamente las dependencias entre componentes.
- Soporte pensado para la realidad de las organizaciones. Basado en SLAs y prestado por personal altamente cualificado.

3. Componentes

3.1. Single Sign-On

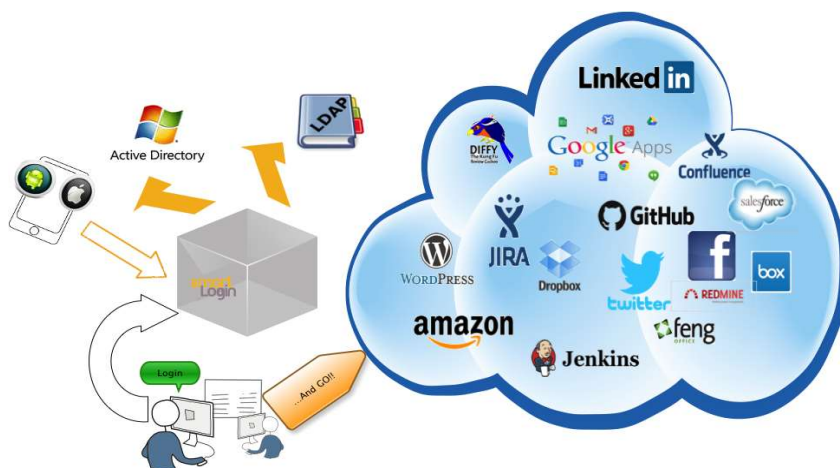
Los usuarios autorizados, podrán autenticar en las herramientas web corporativas a través de SmartLogin® con un solo usuario y contraseña. A su vez los usuarios no necesitarán volver a introducir sus credenciales para acceder a otra aplicaciones ya que SmartLogin® lo gestionará por ellos.



Un ejemplo de esto es cuando un usuario inicia sesión con su cuenta corporativa para posteriormente acceder a todo el entorno de aplicaciones, ya sean Cloud o internas (on-premise) sin que se le solicite de nuevo que se autentique.

En este escenario es muy sencillo conectarse a las aplicaciones SaaS, PaaS e IaaS a través de los protocolos estándar **SAML2**, **CAS**, **Kerberos** y **Oauth**.

Otro ejemplo de este escenario son las organizaciones que desarrollan aplicaciones internas. A estas se les permite mejorar la seguridad al desacoplar la autenticación / autorización de cada aplicación y aprovechar los servicios centralizados de SmartLogin®. En este caso, las aplicaciones internas se desarrollarán como "partes de confianza" que confían en un sistema interno de gestión de identidades corporativas para las decisiones de autenticación / autorización.

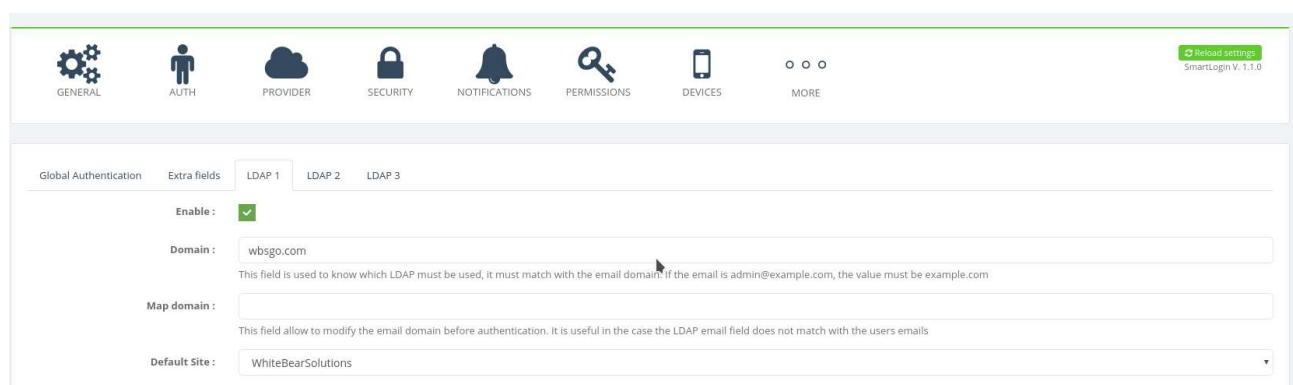


3.2. Integración con el Directorio central de autenticación

SmartLogin® permite conectarse a tantos directorios como sea necesario. Estos pueden ser OpenLdap, Active Directory o WBSVision.

SmartLogin® pueden identificar el directorio contra el que se debe autenticar ya sea por el dominio del email, o bien hacer una búsqueda recursiva hasta que encuentre dicha identidad.

Gracias a la integración nativa con WBSVision hace que de una forma fácil se conecte a su servicio LDAP así como usar sus componentes como el metadirectorio e incluso su módulo de Gestión de Identidad.



The screenshot shows the SmartLogin configuration interface. At the top, there is a navigation bar with icons for GENERAL, AUTH, PROVIDER, SECURITY, NOTIFICATIONS, PERMISSIONS, DEVICES, and MORE. Below this, there is a tabbed interface with tabs for Global Authentication, Extra fields, LDAP 1, LDAP 2, and LDAP 3. The LDAP 1 tab is selected. In this tab, there is a section for configuring LDAP settings. It includes an 'Enable' checkbox which is checked. Below it is a 'Domain' text field containing 'wbsgo.com'. A tooltip explains that this field is used to know which LDAP must be used and must match with the email domain. Below the domain field is a 'Map domain' text field. A tooltip explains that this field allows to modify the email domain before authentication. At the bottom of the section is a 'Default Site' dropdown menu set to 'WhiteBearSolutions'. In the top right corner of the interface, there is a 'Reload settings' button and the version 'SmartLogin V: 1.1.0'.

3.3. Federación de identidad

Las empresas podrán integrar sus empresas asociadas o colaboradoras para autorizar a utilizar sus herramientas corporativas.

Esto posibilita que una empresa pueda tener los mismos usuarios y contraseñas en servicios heterogéneos internos (en aplicaciones locales como ordenadores Windows, Intranets, etc.), externos (terceras organizaciones) e incluso en la nube (como Office 365, GoogleApps, Salesforce, etc). De esta forma evita que los credenciales de acceso a servicios externos o del cloud no cumplan las políticas de contraseñas que por normativa deben cumplir y no representen un agujero de seguridad.

Para ello SmartLogin® utiliza los estándares **SAML2**, **CAS**, **Kerberos** y **Oauth** de forma que se garantice la interoperabilidad a la hora de comunicarse con la gran mayoría de servicios.

SmartLogin® tiene la capacidad de actuar como (Identity provider) IDP y así definir los diferentes proveedores de servicio (SP) que incluirá en el dominio de seguridad gestionado por la plataforma. La configuración de los mismos debe definirse en el producto. SmartLogin® provee un repositorio con las aplicaciones más comunes, pero también permite definir a través de su panel de configuración un SP en base a su configuración.

3.4. Proxy Federado e inyección de credenciales

En el caso de que las aplicaciones finales no soporten ningún protocolo de federación (SAML2, Oauth, CAS o Kerberos), SmartLogin® permite hacer SSO a través de inyección de credenciales. Este sistema es totalmente compatible con el dispositivo móvil (Android e IOs) y con navegadores como Firefox, Edge, Internet Explorer 11 y Chrome.

Para añadir mayor seguridad en este tipo de aplicaciones, SmartLogin® permite añadir un **proxy federado**, el cual obliga al usuario a iniciar sesión en el portal web de SmartLogin® antes de acceder a cualquiera de las aplicaciones On-premise (dentro del mismo dominio) a través de este protocolo.

3.5. Gestión de usuarios

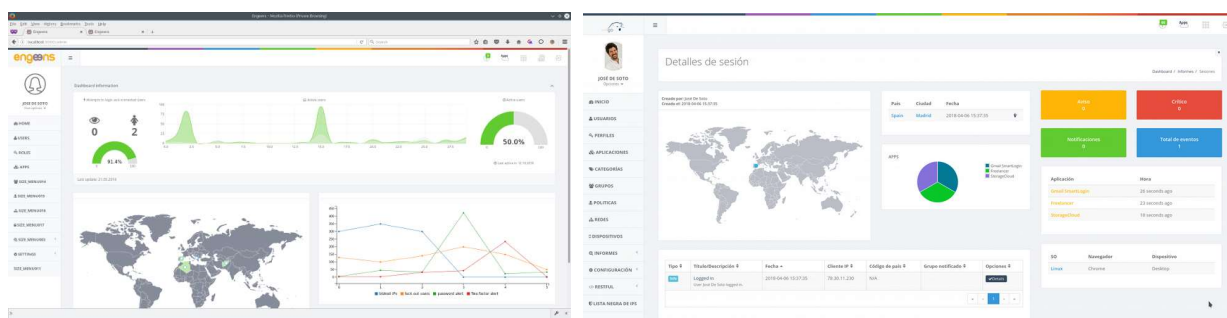
Si se usa la BBDD interna de SmartLogin® como un repositorio central de usuarios, se ofrece una forma sencilla de administrar los mismo a través de su panel. Si esta conectado a un directorio, tendrá la posibilidad de aprovisionamiento.

Las acciones a realizar a través del panel de SmartLogin® son múltiples:

- Restablecimiento de contraseña
- Bloqueo de usuarios
- Configuración de autenticación multifactor (MFA)
- Gestión de aplicaciones y/o grupos
- Gestión de autenticación adaptativa (políticas)
- Gestión de sesiones abiertas
- Gestión de accesos por país

3.6. Informes y análisis

Es una parte muy importante de SmartLogin®. Para dar mayor control, el administrador puede acceder a toda la información de los usuarios relacionada con su accesos (localización, aplicaciones que accede, tiempos, sistema operativo, etc) en tiempo real. Los administradores se verán monitorizados entre si, quedando registrado todas aquellas modificaciones que se realizan y notificándose en tiempo real. Todo ello queda accesible gracias a sus informes y cuadros de mando en linea.



3.7. Seguridad

SmartLogin® combina diferentes mecanismos para cumplir con los estándares de seguridad:

- Multi-factor de autenticación (MFA)
- Lista de acceso por IPs
- Acceso por geolocalización de países
- Políticas de contraseña robusta
- re-CAPTCHA
- Bloqueos de usuarios por intentos fallidos de acceso por contraseña incorrecta
- Auditorias de control de acceso
- Compatibilidad con VPNs
- Autenticación adaptativa o políticas de acceso a nivel global, por usuario o perfil.
- Prevención de intrusión mediante bloqueos de IPs que muestren signos maliciosos
- Información crítica cifrada mediante firma y clave todo ello basado en división de conocimiento

3.8. Autenticación Multi-factor (MFA)

La autenticación Multi-Factor de SmartLogin® proporciona un nivel extra de seguridad en la autenticación, adicional a las credenciales de inicio de sesión del usuario para proteger el acceso.

Por defecto SmartLogin® se integra con:

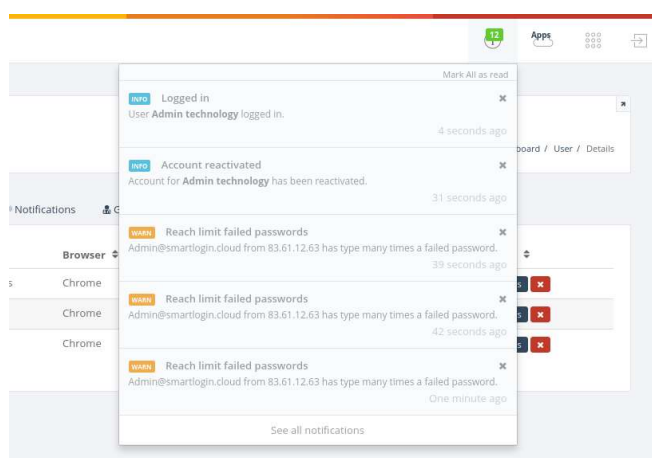
- Google / Microsoft Authenticator
- DroidOTP
- Código de validación por enviado de SMS
- Smart MFA, integrado con la aplicación móvil de SmartLogin®

La flexibilidad del Multi-Factor de SmartLogin® se extiende también a la combinación del uso del segundo factor con el sistema de Servicios Web (apartado 3.19). De tal manera que es posible conectarse o integrar MFA de terceros de una forma muy sencilla.

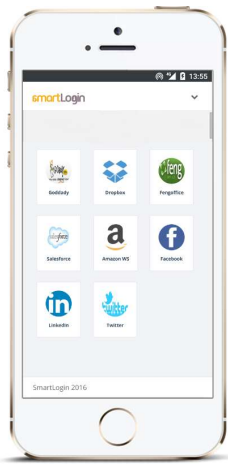
El MFA de SmartLogin® además está integrada con la autenticación adaptativa (apartado 3.15) permitiendo personalizar el método de segundo factor en función de la red, usuario o perfil.

3.9. Envío de notificaciones

La plataforma envía notificaciones tanto a los usuarios como a los administradores. Estas son definidas desde el portal de administración para cada uno de los perfiles. También se puede configurar la forma de notificación, ya sea a través de la aplicación (Live), por email o ambas. Actualmente más de 30 notificaciones son configurables. Entre ellas: Actualización de roles, alerta por intentos fallidos de acceso por contraseña incorrecta, acceso de localización no permitida, etc



3.10. Gestión de dispositivos móviles



SmartLogin® extiende el acceso SSO a las aplicaciones a través de su aplicación móvil, permitiendo incluso acceder a la interfaz web sin uso de credenciales a través del código QR proporcionado por la aplicación móvil combinado con su sistema biométrico.

Gracias a su sistema de gestión de dispositivos se permite definir cuales pueden acceder, así como tener el control de estos pudiéndolos desvincular de la plataforma, denegar el acceso en cualquier momento con un solo paso e incluso geolocalizarlos. Esta funcionalidad no solo la pueden realizar los administradores, sino que se puede extender al autoservicio. Es decir, delegar la responsabilidad de vincular dispositivos,

así como su bloque a los propios usuarios.

Con el uso del dispositivo móvil los propios usuario podrán mejorar la seguridad, ya que se les permite tener un mayor control sobre lo ocurre con respecto a su cuenta e incluso poder controlar las sesiones de forma remota, accediendo a la información de esta en tiempo real o pudiéndolas cerrar desde un menú en caso de dejarlas abiertas por descuidos.

Los administradores por otro lado podrán realizar acciones de administración desde el dispositivo móvil: bloque de usuarios, restablecimiento de contraseñas, limpieza de lista negra de IPs, gestión de políticas, etc. Todo ello controlado con acceso biométrico.



3.11. Gestión de Desktops y Laptops

Con esta nueva funcionalidad SmartLogin® extiende la gestión de dispositivos a los ordenadores de sobremesa y/o portátiles, añadiendo una nueva capa de seguridad a través de claves asimétricas. Un ejemplo de esto, es la capacidad de dar acceso al usuario unicamente desde su ordenador o portátil corporativo. Evitando así el acceso no controlado desde otros dispositivos o incluso el phishing de credenciales, ya que se necesitaría también el dispositivo vinculado de dicho usuario.

3.12. Restablecimiento seguro de contraseña

El restablecimiento de contraseña se puede realizar vía Email o SMS. En el caso de hacerlo por SMS la pasarela de envío de mensajes debe estar configurada. Si se usa el email, es posible que dicho correo electrónico este detrás de SmartLogin®, imposibilitando el uso del email para la recuperación de contraseña. En este caso particular SmartLogin® permite definir un email alternativo.

El restablecimiento de contraseña esta definida como una función crítica de acceso. Por este motivo se puede establecer dentro de las políticas de seguridad. Es decir, se puede definir una regla que defina que el restablecimiento de contraseña se realice sólo desde el centro de trabajo. En este caso si un usuario desde fuera del mencionado centro requiere acceder al restablecimiento de contraseña no podrá. Para esta situación un administrador podrá generar desde el panel de usuario una contraseña temporal (generada de forma aleatoria, y en base la configuración de la contraseña robusta) y de un solo uso. Una vez iniciada la sesión dicho usuario será obligado a modificarla.

3.13. Auto servicio

SmartLogin® tiene la capacidad de delegar ciertas funciones y/o configuraciones a los usuarios. Estas pueden ser configurables a nivel de perfiles, y los servicios que se incluyen son:

- Mostrar lista de contactos
- Editar su perfil
- Configurar el segundo factor
- Gestión de sesiones remotas
- Modificación de contraseña
- Solicitud de accesos por geolocalización
- Gestión de dispositivos
- Acceso delegado

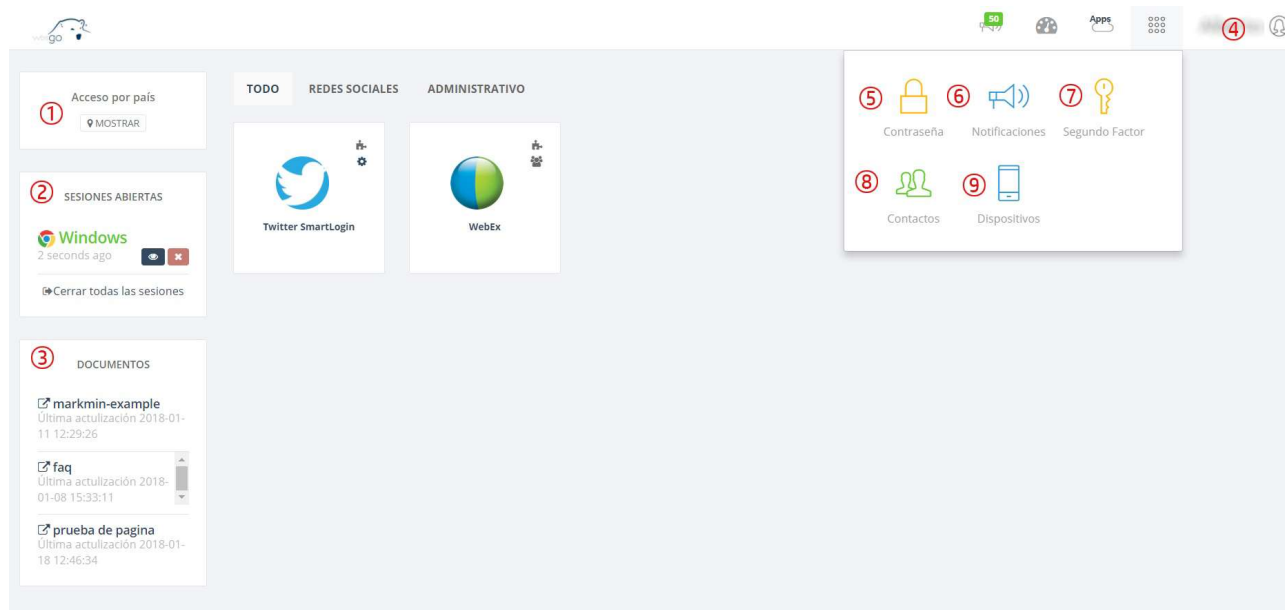
3.14. Gestión de acceso (Perfiles)

Dentro del sistema se pueden diferenciar dos entornos:

3.14.1. Panel de usuario (autoservicio):

Dentro del entorno de usuario no se pueden definir permisos como tal, pero si a qué recursos pueden acceder:

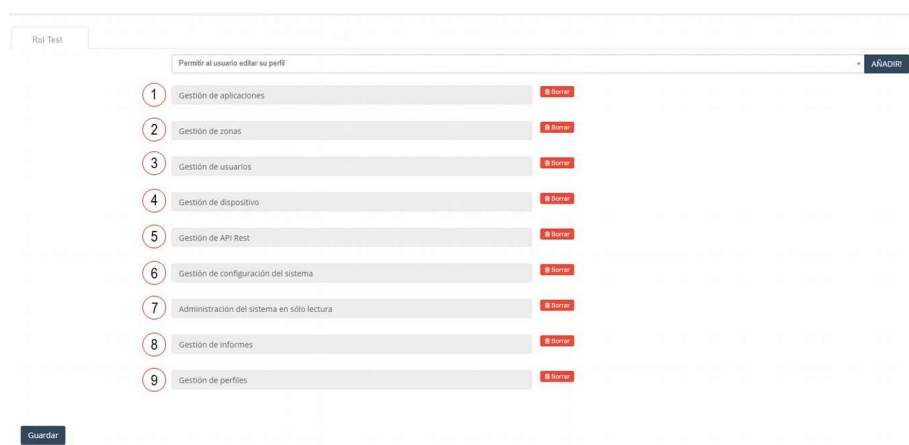
1. Solicitud de accesos por geolocalización (país)
2. Enlaces estáticos de ayuda y/o información
3. Permitir ver sus sesiones abiertas y poder administrarlas
4. Permitir la edición de su propio perfil
5. Gestión de contraseña
6. Permitir ver sus notificaciones
7. Configurar el segundo factor
8. Contactos corporativos en el panel
9. Gestión de dispositivos móviles



3.14.2. *Panel de Administración:*

Dentro del panel de administración se pueden definir diferentes niveles de acceso pudiendo así delegar responsabilidades en diferentes perfiles. Los diferentes permisos que nos podemos encontrar en SmartLogin® son:

1. Administración de entornos multi-zonas
2. Gestión de aplicaciones
3. Gestión de usuarios
4. Gestión de dispositivos móviles
5. Gestión de servicios REST
6. Gestión de configuraciones del sistema
7. Acceso a todo el sistema como lectura
8. Acceso a los informes
9. Gestión de perfiles



3.15. Autenticación adaptativa (políticas)

La autenticación adaptativa permite definir comportamientos o reglas de acceso según la ubicación, el usuario o el perfil que desempeña dicho usuario dentro de la organización o SmartLogin®.

Estas reglas o comportamientos son múltiples. Un ejemplo de estas configuraciones son:

- Definir si se puede acceder o no
- Si se puede restablecer la contraseña
- Si se puede acceder usando un QR desde el dispositivo móvil
- Si es necesario usar un segundo factor
- Definir tiempos de caducidad de sesiones, etc

Con referencia al Multifactor de autenticación (MFA), la autenticación adaptativa permite configurar diferentes métodos de segundo factor dependiendo del usuario, ubicación o perfil.

3.16. Políticas sobre aplicaciones

SmartLogin® extiende las políticas no solo a nivel de acceso sino también a nivel de aplicación. Es decir, permite establecer un segundo factor antes del acceso a una aplicación determinada, e incluso definir si esta aplicación es o no accesible desde el móvil.

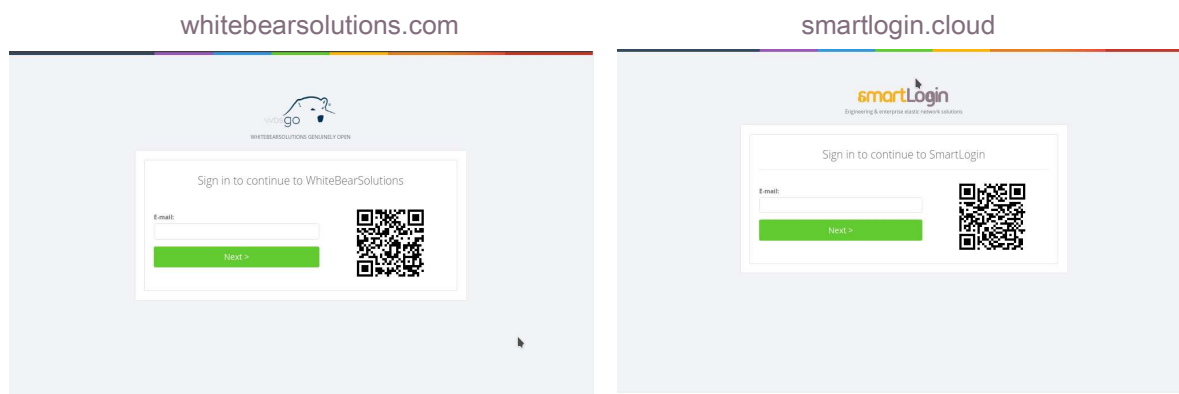
3.17. Gestión de acceso delegado

Desde la versión 1.2, SmartLogin® permite que un usuario pueda compartir su acceso con otro usuario de su misma zona (apartado 3.18). Este permiso es gestionado a través de la propia aplicación e incluso a través de los permisos globales. Esta información queda registrada a través de los eventos y reportes por sesión.



3.18. Multi-zonas

Multi-zonas es una función de SmartLogin® que permite a las empresas crear una red de accesos en una sola instalación. Esto permite poder vincular diferentes dominios y/o subdominios dentro de una instancia y estas ser gestionadas desde un mismo punto.



Es de especial utilidad en varios casos, por ejemplo:

- Empresas dentro de un mismo grupo que comparten recursos pero la imagen corporativa es distinta
- Empresas que venden servicios de terceros, ya que permite centralizar todos los recursos y seguridad en un solo punto con una imagen corporativa para cada cliente
- Si se requiere tener más de un portal de acceso (imagen corporativa) pero compartir los usuarios registrados entre ellos

3.19. Servicios Web

Los Servicios Web de SmartLogin® permiten intercambiar datos entre aplicaciones de terceros facilitando así la integración con estos.

Está integrado con el sistema de directorio, el cual permite a través de servicios web la creación, borrado y actualización de cuentas, así como el restablecimiento de contraseñas, permitiendo así el aprovisionamiento con los diferentes directorios.

Actualmente también está integrado con el core del Multi-factor, permitiendo usar los servicios web con sistemas de segundo factor de terceros, siendo totalmente compatible con la autenticación adaptativa.

3.20. Servicio de bloqueo de IPs

SmartLogin® incorpora un sistema a nivel de capa 3 que permite bloquear IPs de forma automática según ciertos comportamientos, y notificar dichos bloqueos y su motivo al administrador.

Muchas de estas reglas son configuradas por los responsables, por ejemplo el acceso por geolocalización, bloqueos por cambios de IPs, o simplemente por no aportar la información necesaria en las cabeceras. Además SmartLogin® es capaz de forma automática de detectar ataques DoS, boots así como inconsistencias en sesiones.

3.21. Actualización de la base de datos GeoIP

El sistema de GeoIP es una parte importante del core de seguridad de SmartLogin®, así como de los informes. Por este motivo, con frecuencia estará disponible una actualización con respecto a esta información. Dicha BBDD podrá ser actualizada desde el panel de administración.

3.22. RESTful

SmartLogin® posee un Interfaz de programación basado en RESTful que permite utilizar todos sus recursos. Es posible la utilización de esta API gracias a un panel donde los administradores podrán generar sus respectivos *tokens* de acceso para posteriormente acceder a los distintos recursos.

Algunos ejemplos de utilización de la API RESTful podrían ser:

- Reutilización del sistema de MFA para aplicaciones externas
- Reutilización del sistema de bloqueo de IPs a nivel de capa 3 para integrar con SIEMs, SOC, etc
- Generador de informes periódicos sobre un tipo particular de dato

3.23. Syslog Remoto

La herramienta de syslog remoto creada por SmartLogin® permite que todos los logs de acceso al servidor e incluso los eventos del sistema creados por SmartLogin® puedan ser enviados a un servidor remoto. Esto es muy útil si se quiere que esta información sea tratada por un SOC o un SIEM.

Activar : ☒

Servidor de log :

192.168.4.11

Valor de la IP del servidor de log remoto. Usa UDP y 514 por defecto.

Tipo de logs :

Todo

Logs de acceso

Todo

Eventos

Guardar

3.24. Integración con HSM

Desde la versión 1.3 SmartLogin® incorpora la capacidad de integración a través de API REST a sistemas HSM (Módulo de Seguridad Hardware), delegando así la capacidad de cifrado.

3.25. Marketplace

SmartLogin® desde la versión 1.3 pone a disposición de los clientes SmartLogin marketplace. Esta plataforma esta pensada para encontrar fácilmente los nuevos módulos del producto con independencia del Core, así como los desarrollos personalizados (acoplados al producto) que el propio cliente demanda.

4. Usabilidad e idiomas

4.1. Visual y diseño

Tanto el interfaz de usuario como el de administrador tienen un diseño atractivo y muy intuitivo. Gracias a su arquitectura estas interfaces pueden ser personalizadas, e incluso un cliente podría desarrollar su propio diseño web.

4.2. Idiomas

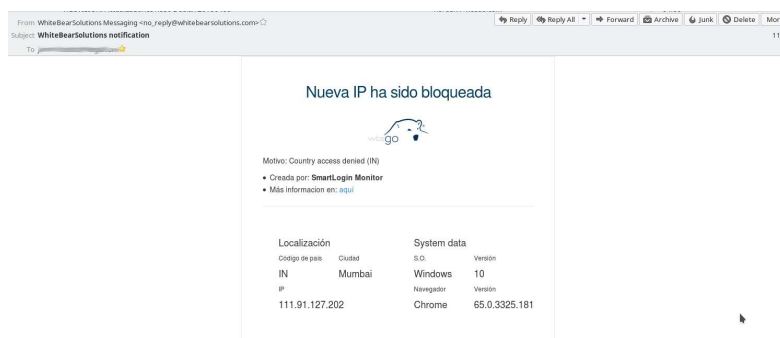
SmartLogin® dispone de una opción que permite seleccionar el idioma en el que trabajar. Este se puede aplicar a nivel global, o incluso permitir que los usuarios personalicen el idioma de su panel. Actualmente está disponible el producto en español e inglés, pero pueden incorporarse nuevos idiomas de forma sencilla a través de ficheros de configuración.

4.3. Imagen corporativa personalizable

SmartLogin® permite personalizar las distintas zonas que los clientes configuran en el sistema. Estas personalizaciones abarcan el idioma por defecto, el logotipo, favicon, páginas de error y eslogan corporativo.

4.4. Plantillas de Email

Los correos electrónicos son otra parte importante de la imagen corporativa. Por este motivo SmartLogin® permite la edición de estos, no solo con respecto al diseño y contenido, sino también respecto a la incorporación de adjuntos, inclusión en copia a otras personas o listas e incluso hacerlos dinámicos según variables del sistema.



5. Copias de seguridad

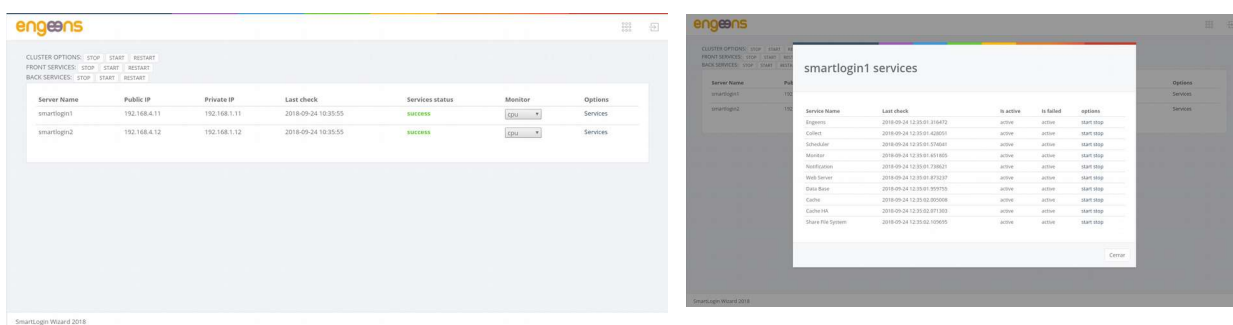
El producto cuenta con un motor interno que realiza instantáneas de la base de datos del directorio y la configuración de los servicios y el sistema. Las instantáneas se pueden lanzar a petición del administrador o de forma automática. El administrador puede realizar en cualquier momento tantas copias como desee, las cuáles se realizan en unos pocos segundos.

La tecnología “bulletproof” permite poder recuperar el estado del producto en segundos aplicando un fichero de instantánea. Esto también se aplica si se desea recuperar dicho estado en un equipo diferente del original.

6. Monitorización

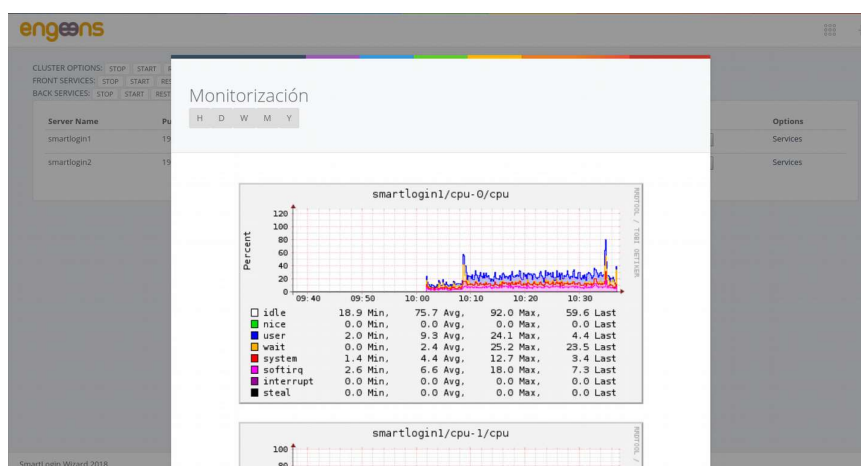
6.1. Engeens

A través de Engeens se puede monitorizar todo el sistema SmartLogin. Este sistema permite administrar el cluster de una forma centralizada así como saber el estado de cada uno de los nodos y de sus servicios.



Este sistema también está en constante vigilancia del sistema y es capaz de activar un reinicio de un servicio determinado u otra acción correctiva si el programa principal, debido a alguna condición de fallo (como un bloqueo) se niega a comunicar con el servicio vigilancia.

A través de sus gráficas es posible monitorizar el estado de la cpu, memoria, swap, discos, interfaces de red, etc. Su vista puede ser configurable por hora, día, semana, mes y año.



6.2. SNMP

SmartLogin® permite la monitorización SNMP a través de cualquier herramienta estándar del mercado.

6.3. SmartLogin Crash Reporter

Es posible que en el caso de que se produzca un error crítico, éste no sea reportado por dicho usuario.

Habilitando *SmartLogin Crash Reporter* el centro de asistencia de SmartLogin® recibirá en tiempo real información sobre el error.

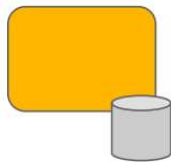
7. Arquitecturas

En el proceso de instalación, SmartLogin® permite de una forma muy sencilla elegir el tipo de arquitectura que quieres montar. Un ejemplo de la pantalla de instalación la podemos ver en la imagen siguiente:



SmartLogin® proporciona las arquitecturas siguientes:

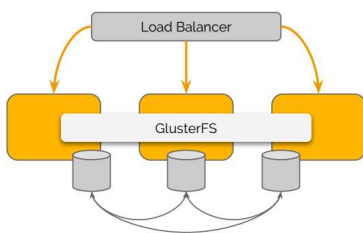
7.1. Arquitectura 1



- Un solo nodo
- Sin alta disponibilidad
- Front-end y Back-end unidos

Pensado para proyectos pequeños y entornos de desarrollo y test

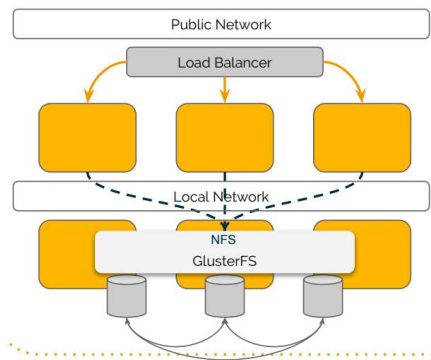
7.2. Arquitectura 2



- Activo-Activo en lectura y escritura
- Mínimo 3 nodos
- Front-end y Back-end en todos los nodos
- Requiere balanceador para el front-end (con persistencia de sesión)
- Base de datos replicada
- Caché replicada
- Caché replicada
- Sistema de ficheros distribuido GlusterFS

Pensado para proyectos de tamaño medio

7.3. Arquitectura 3



- Activo-Activo en lectura y escritura
- Mínimo 3 nodos en back-end y 2 en front-end
- Front-end y Back-end en todos los nodos
- Front-end y Back-end en todos los nodos
- Requiere balanceador para el front-end (con persistencia de sesión)
- Base de datos replicada
- Caché replicada
- Sistema de ficheros distribuido GlusterFS

Pensado para proyectos de tamaño grande o que requieran un acceso público (cloud)

8. Actualizaciones

Todo el sistema está construido en relación a componentes y paquetes. Nuestra compañía pone a disposición de los clientes con suscripción activa un repositorio de paquetes que contienen información de dependencia entre si y permiten que el sistema pueda realizar actualizaciones automáticas a petición del administrador.

Los paquetes realizan automáticamente todo el proceso de actualización sin intervención del administrador, salvo para lanzar el proceso y revisar las actualizaciones disponibles. Dentro del proceso de actualización el producto se conecta automáticamente a nuestro repositorio a través de una conexión directa a internet o un servido proxy y presenta las actualizaciones de paquetes disponibles. Una vez el administrador decide actualizar el producto hace todo de forma automática comunicando únicamente el final del proceso al administrador.

9. Suscripciones y soporte

De cara a proporcionar un soporte orientado a organizaciones que por requerimientos de nivel de servicio, no pueden basar el mismo en las herramientas propias de la comunidad, SmartLogin ha diseñado un conjunto de servicios de soporte basados en suscripciones anuales de servicio de producto. Dichas suscripciones se dividen en diferentes niveles de servicio de manera que cada organización puede seleccionar la que mas se adapte a sus requerimientos. Dicho modelo de contratación se basa en:

- Un único pago: A través de la adquisición de la suscripción obtengo acceso a todas las herramientas necesarias para la adquisición, administración y gestión del producto seleccionado, en base a la dimensión de mi arquitectura. No se paga nunca nada en concepto de licencia, todo el pago está orientado a la percepción de un servicio.
- Soporte basado en SLAs: Cada cliente en base a sus requerimientos de nivel de servicio, selecciona la suscripción más adecuada.
- Soporte global: Nuestros productos están concebidos como una solución completa lista para ser explotada. Nosotros no diferenciamos entre el sistema operativo, aplicación, redes, etc. Aportamos servicios de soporte a la solución completa.
- Soporte reactivo: A través de nuestros diferentes canales de comunicación, y en base al tipo de suscripción contratada podrá dar de alta incidencias relacionadas con problemas de funcionamiento del producto asociado.
- Soporte a consultas: A través de nuestros diferentes canales de comunicación, y en base al tipo de suscripción contratada podrá dar de alta un número restringido de consultas relacionadas con la administración y uso del producto asociado.
- Soporte proactivo: En base a un sistema proactivo de notificaciones, nuestro centro de soporte le mantendrá informado de todas las revisiones y actualizaciones que afecten al producto cuya suscripción haya contratado. Asimismo en aquellas suscripciones en las que esté incluido, nuestro departamento de servicios, concertará con usted el mejor momento para de manera remota o presencial (según se requiera) proceder a instalar la nueva revisión o versión.
- Garantía de vida de versiones: A través de la suscripción obtendrá soporte sobre la versión instalada inicialmente, y salvo caso de fuerza mayor, no estará obligado a migrar dicha versión durante los 2 siguientes años a contar desde la fecha de contratación, quedando garantizado el soporte de la misma en ese periodo.

9.1. Información sobre la suscripción de soporte

El producto genera un identificador único (UUID) por cada máquina virtual dónde se ejecuta. Este identificador se verifica en relación al número de serie hardware del equipo dónde se ejecuta. Cuando se registra, el producto se asocia a una cuenta relacionada con la organización que lo utiliza, lo que permite conocer exactamente los productos con los que cuenta y su estado.

Cuando el producto se encuentra registrado en una cuenta se pueden activar diferentes códigos de servicio.

Este servicio permite contar entre otras cosas con un enlace VPN-SSL automático que puede ser activado en un click por parte del administrador, de forma que un técnico de soporte pueda intervenir en caso de ser necesario. La suscripción permite que el cliente pueda conocer cada caso asociado a cada máquina concreta y su evolución a través de nuestro portal de soporte.

9.2. Otros servicios de suscripción

Tenemos a disposición del cliente otros servicios de suscripción tales como backup remoto y monitorización remota.

Asimismo, a través de nuestro departamento de servicios profesionales se podrán adecuar ciertas características de las suscripciones a las necesidades específicas de nuestros clientes.