

Características técnicas

- **Seguridad aplicativa:** Pitbull KeyHolder™ cuenta con seguridad integrada con Active Directory de Windows, permitiendo acceder a la misma con el usuario y contraseña sistema operativo. Adicionalmente, al poseer perfiles aplicativos permite segregarse adecuadamente los permisos de acceso a lo estrictamente necesario y crear internamente grupos para facilitar la asignación de permisos de solicitud de contraseñas para los usuarios firecalls.
- **Cifrado:** Las contraseñas se almacenan cifradas en la base de datos con el algoritmo RijDAEL, también conocido como AES (Advanced Encryption Standard), el cual fue elegido como estándar de cifrado por el NIST (National Institute of Standards and Technology) y el gobierno de los Estados Unidos. Este algoritmo puede operar con bloques y claves de longitudes que varían entre los 128 y 256 bits. La utilización del motor de base de datos Microsoft SQL Server 2005 permite tomar ventaja de la funcionalidad de cifrado propia de la plataforma, protegiendo la base de datos completa y en forma transparente para la aplicación. La comunicación entre el cliente y el servidor se realiza empleando el protocolo HTTPS (http sobre SSL – Secure Socket Layer), que utiliza certificados digitales y garantiza que la información se transmite en forma cifrada.
- **Cambio claves cifrado:** Mediante una funcionalidad de mantenimiento de la aplicación, se puede efectuar el cambio de las claves de cifrado utilizadas por los algoritmos empleados para cifrar las contraseñas de las cuentas firecalls.
- **Cambio automático de contraseñas:** Cuando un soporte técnico ha solicitado la contraseña de un usuario firecall y luego de transcurrido el tiempo especificado de uso, la aplicación automáticamente efectúa el cambio de dicha contraseña, liberando de esta tarea al administrador de seguridad. Esta funcionalidad sólo es empleada para aquellos usuarios firecalls que tengan activo el atributo de cambio automático de contraseñas.
- **Verificación automática de contraseñas:** Periódicamente la aplicación efectúa una actividad de verificación de contraseñas de los usuarios firecalls que poseen el atributo de verificación de contraseñas activo, de esta forma se garantiza que las contraseñas almacenadas son las correctas y en caso de error se informa al administrador de seguridad para que analice el incidente de seguridad correspondiente.
- **Apertura automática de sesión con usuario firecall:** La aplicación posee conectores tanto con Terminal Server como con SSH que le permiten realizar una conexión en forma automática con el usuario firecall; de esta forma el soporte técnico conoce la contraseña del usuario que está utilizando. Cuando se realiza una solicitud de contraseña de un usuario firecall que posee este atributo activo, Pitbull KeyHolder™ automáticamente establece una sesión remota desde la estación de trabajo del soporte técnico con las credenciales del usuario solicitado.
- **Tablero de control:** Pitbull KeyHolder™ posee un tablero de control (Dashboard), desde el cual se puede realizar un control en línea de las actividades realizadas sobre los usuarios firecalls. El tablero puede mostrar la cantidad de usuarios firecalls que están siendo utilizados, los más solicitados en las últimas 24hs, 48hs, última semana y último mes, la cantidad de aperturas por usuario firecall durante últimas 24hs, 48hs, última semana y último mes, entre otros.
- **Trazabilidad:** Pitbull KeyHolder™ posee un sistema riguroso de auditoría, el cual permite realizar una trazabilidad histórica del ciclo de vida de las cuentas de usuario aplicativos y de los usuarios firecalls, registrando todas las actividades realizadas sobre las mismas.
- **Cambio forzado de contraseña:** El administrador del sistema posee la funcionalidad de efectuar un cambio forzado de contraseña de una cuenta firecall cuando aún no ha caducado el período de tiempo indicado por el soporte técnico para solucionar su incidente.
- **Multi-Idioma:** La aplicación permite el uso de varios idiomas, como ser español, inglés y portugués.

Requisitos del sistema

Servidor:
Microsoft Windows 2003 Server
IIS 6.0 (Internet Information Server 6.0)
Framework 2.0 Enterprise Library 3.1
Microsoft SQL Server 2005

Cliente:
Windows XP/Vista o 2000
(con cliente Remote Desktop)
Internet Explorer 6 / compatibles
Framework 2.0



Pitbull KeyHolder™ es un producto de la línea de soluciones Pitbull®. Windows Vista/2003/XP/2000, Internet Information Server, Microsoft SQL Server 2005 e Internet Explorer son marcas registradas de Microsoft Corporation. Pitbull KeyHolder son marcas registradas de Penta Security Solutions SRL. Todos los productos y nombres de compañías que se encuentran en este folleto pueden ser marcas registradas de sus respectivos propietarios.

www.pitbullsoftware.net

Penta Security Solutions S.R.L. - Av. Rivadavia 717 8° 808 (C1002AAF), Ciudad de Bs. As., Argentina.
Teléfono/Fax: (54-11) 5252-0920 (líneas rotativas). info@pentass.com – www.pentass.com



TECNOLOGÍA DE VANGUARDIA EN ADMINISTRACIÓN DE CONTRASEÑAS DE EMERGENCIA

KeyHolder® es un producto de la familia Pitbull que optimiza y reduce los costos de seguridad informática de su empresa modernizando los procesos y dejando atrás el antiguo sistema de sobre cerrado.

Pitbull KeyHolder® favorece el cumplimiento de leyes, regulaciones y estándares nacionales e internacionales, contando con procesos estandarizados y documentados.

*Sarbanes, Oxley Act (SOX), ISO-IEC 27002, Payment Card Industry (PCI).

Ley de Transferencia y Responsabilidad de Seguros de Salud (HIPAA) y normativas establecidas por el Banco Central de la República Argentina.

Perfiles de usuarios

Administrador del sistema: Es el encargado de efectuar la administración del sistema, puede acceder a todas las funcionalidades de la aplicación.

Soportista: Es la persona autorizada a acceder a las contraseñas de los usuarios firecalls -usuarios de emergencia- que tiene asignadas.

Auditor: Es la persona que tiene acceso a todos los reportes existentes en la aplicación y al módulo de dashboard.

Responsable de usuarios firecalls: Es la persona responsable de los servicios que corren en los sistemas a los que se accede con los usuarios firecalls. Es quien recibe un e-mail cada vez que se accede a la contraseña de uno de estos usuarios. Adicionalmente, puede acceder a la aplicación para extraer reportes de la actividad de sus usuarios firecalls.

Dashboard: Las cuentas de usuarios que tienen asignado este perfil solo pueden visualizar el dashboard. Por ejemplo, se podría utilizar este perfil para monitorear la actividad de los usuarios firecalls, presentándolo en una pantalla gigante a fin de observar los indicadores definidos (ideal para salas de NOC).

Módulos aplicativos

Administración:

Esta opción centraliza el control y lleva adelante la administración general del sistema. Desde aquí el administrador del sistema podrá:

- Crear, modificar y eliminar los usuarios que acceden a la aplicación, los usuarios firecalls y los grupos de usuarios.
- Gestionar los permisos de acceso de los usuarios firecalls.
- Definir las plataformas gestionadas por la compañía (sistemas operativos, bases de datos, equipos de comunicaciones, aplicaciones).
- Administrar los parámetros generales de la aplicación.



- **Gestión de usuario firecall**

Desde esta opción el soportista accede a las contraseñas de los usuarios firecalls.

¿Cómo procede el sistema?

Pitbull KeyHolder®, le permite al soportista solicitar solamente usuarios firecalls que se encuentren habilitados y que no estén siendo utilizados por otro soportista.

Cuando el soportista requiere un usuario firecall, el sistema solicita automáticamente el ingreso de los datos relacionados con el incidente a solucionar, como ser: número de incidente, descripción y lapso de tiempo por el cual va a estar utilizando el usuario firecall. Al completar esta información, el sistema envía un e-mail al responsable del usuario firecall notificándole la utilización de la cuenta.

En función de las características de los usuarios firecalls, existen dos opciones para el acceso con el usuario firecall solicitado:

- Si está activado el inicio de sesión automático, la aplicación se conecta con el usuario firecall sin informar la contraseña al soportista.
- Si está activado el inicio de sesión manual, la aplicación le proporciona al soportista las credenciales para que pueda conectarse y solucionar el incidente asociado.

También desde este módulo, el administrador de seguridad deberá realizar la liberación manual de los usuarios firecalls cuyo tiempo de apertura haya expirado, es decir, cambiar manualmente la contraseña de dichos usuarios.

Reportes

Desde esta opción se pueden obtener distintos tipos de reportes de auditoría que permiten realizar un análisis detallado de la actividad de los usuarios firecalls.

Los reportes poseen amplias posibilidades de filtrado y búsqueda, los cuales pueden ser visualizados desde la aplicación o bien exportados archivos en formato pdf o excel.

Los principales reportes son los siguientes:

- Usuarios firecalls – permisos: Detalle de los permisos asignados a los usuarios puntuales o grupos para cada uno de los usuarios firecalls.
- Usuarios firecalls – responsables: Listado de responsables asociados a cada uno de los usuarios firecalls.
- Usuarios firecalls – abiertos: Listado de usuarios firecalls que han sido solicitados y aún no han sido liberados.
- Usuarios firecalls – administrados: Listado de todos los usuarios firecalls definidos en el software.



- Usuarios de aplicación: Listado de usuarios con acceso a la aplicación.
- Responsables: Listado usuarios de definidos como responsables.
- Grupos de usuarios: Listado de grupos creados y usuarios asignados a los mismos.
- Actividad histórica de usuarios firecalls: Ciclo de vida de los usuarios firecalls.

Esta opción se encuentra disponible para el auditor y administrador de seguridad, quienes pueden acceder a todos los reportes. Adicionalmente, cada responsable de los usuarios firecalls puede acceder a este módulo para extraer reportes de la actividad de los usuarios que tiene asignados, en forma adicional al e-mail que recibieron.

Dashboard

En este módulo de la aplicación se visualiza el tablero de control con varios indicadores que permiten realizar un análisis de la actividad de los usuarios firecalls para identificar aplicaciones o sistemas que requieren soporte continuo. Este módulo se encuentra disponible para los perfiles de administrador del sistema, auditor y dashboard.