



Control de acceso basado en roles

- **¿Qué es Visual Guard?**
- **Autenticación**
Controle la identidad de los usuarios
- **Autorizaciones**
¿Qué es lo que puede hacer un usuario en su aplicación?
- **Auditoría y reportes**
Herramientas para la realización de auditorías y reportes, listos para su uso
- **Herramientas de seguridad de Visual Guard**
Herramientas de desarrollo, de administración y de auditoría
- **¿Cómo funciona Visual Guard?**
- **Especificaciones técnicas**

■ ¿Qué es Visual Guard?

Novalys ha estado desarrollando soluciones de autenticación y de permisos para aplicaciones corporativas desde hace 15 años. Basados en esta experiencia, nosotros hemos diseñado Visual Guard para .Net, una solución dirigida a cubrir los temas de seguridad de las aplicaciones .Net, no importando lo complejo de su entorno.

Visual Guard es un sistema de control de acceso basado en roles RBAC

Esta herramienta añade elementos de seguridad a sus proyectos, como:

- Gestión de usuarios, membership, roles y política de contraseña;
- Definición de los permisos de los usuarios (¿qué pueden hacer los usuarios finales en la aplicación?);
- Autenticación de los usuarios con el Directorio Activo (Active Directory) o con las cuentas de una base de datos;
- Implementación de un mecanismo de autenticación única (Single Sing-On);
- Registro de un historial de las transacciones sensibles (Implementación de un sistema de registro y de auditoría)

Visual Guard para .Net:

- Ofrece una consola de administración amigable, diseñada para el personal no técnico;
- Centraliza la seguridad de todas sus aplicaciones .Net en una sola herramienta;
- No requiere codificar para definir los permisos
- Se integra fácilmente en una aplicación .Net
- Soporta aplicaciones de tipo Winforms, Webforms y Webservices, así como cualquier componente .Net.

■ Autenticación

La autenticación de un sistema RBAC consiste en verificar la identidad del usuario en un proceso de dos etapas:

- Identificación: el usuario se identifica;
- Autenticación: el usuario prueba su identidad.

Dos tipos de necesidades:

Usted necesita crear una lista de las cuentas de usuario y de sus contraseñas desde la nada.

Usted ya cuenta con un sistema de identificación y desearía utilizar este mismo sistema pero a nivel de la aplicación .

La solución:

Visual Guard.Net soporta la autenticación por medio del registro de usuarios y de sus contraseñas. Una cuenta de usuario creada en Visual Guard podrá ser utilizada para todas sus aplicaciones .Net.

Tipos de autenticación soportados por Visual Guard:

- Cuentas de Windows (cuentas locales o cuentas del Directorio Activo)
- Cuentas de Base de Datos (creadas para que los usuarios tengan acceso a una base de datos)
- Cuentas de Visual Guard (creadas y gestionadas por Visual Guard)

Si usted usa otro sistema de autenticación (tipo smartcard, etc) por favor contáctenos.

Cuentas de Windows / el Directorio Activo

Si usted utiliza el mecanismo de autenticación de Windows, las contraseñas son creadas, almacenadas y administradas en el Directorio Activo.

- La consola de Visual Guard le permite buscar un usuario en el Directorio Activo. Cuando dicho usuario es encontrado, Visual Guard .Net almacenará el identificador de seguridad (SID security identifier) de este usuario en el repositorio. Usted podrá entonces asignar roles y permisos de Visual Guard a este usuario. Usted puede declarar varios usuarios al mismo tiempo (tantos como quiera).
- Usted puede también importar automáticamente algunas o todas las cuentas de windows desde el Directorio Activo hasta el repositorio: Visual Guard lo provee de un API que permite a un programa exterior crear y modificar una nueva cuenta.

Autenticación única (single sing-on)

Si usted utiliza el Directorio Activo para gestionar sus cuentas de usuario, quizás usted esté interesado en implementar un proceso de identificación única: una vez que un usuario entra en una sesión de Windows, él podrá acceder a cualquier otra aplicación sin necesidad de identificarse de nuevo.

Visual Guard soporta las configuraciones de autenticación única para las cuentas de Windows:

- Visual Guard .Net recupera de manera automática el ID de los usuarios que están en la sesión de windows.
- Visual Guard verifica que dicho usuario tenga acceso a la aplicación.
- Visual Guard carga el rol correspondiente y aplica sus permisos a la aplicación.
- Este proceso se repetirá cada vez que un usuario lance la aplicación.
- Por lo tanto, el usuario no se verá en la necesidad de identificarse una vez que entre en la aplicación.

Cuentas de una Base de Datos

Visual Guard. Net soporta la autenticación basada en el sistema de cuentas de bases de datos (DBMS) de Oracle 9 así como de Sql Server 2000.

Visual Guard. Net le permite reutilizar las cuentas y las contraseñas definidas en esta DBMS.

Para mayor información sobre este tema, diríjase a la parte concerniente a la integración de Visual Guard.Net.

Cuentas Username / Password - Cuentas de Visual Guard. Net

Visual Guard .Net posee su propio sistema de membership para gestionar las cuentas de usuario y las contraseñas. Las identificaciones creadas de esta forma, son almacenadas en el repositorio de Visual Guard.

Política de contraseñas

Visual Guard .Net le permite definir una política de contraseñas para las cuentas creadas por Visual Guard.

Por ejemplo, usted puede definir:

- El tamaño mínimo de una contraseña.
- El número mínimo de caracteres no alfanuméricos.
- La imposibilidad de reutilizar sus antiguas contraseñas.
- Cuentas de correo electrónico únicas para cada usuario.
- La modificación de cada una de las contraseñas cada determinado tiempo.
- El número máximo consecutivo de errores al introducir la contraseña. La identificación del usuario estará deshabilitada hasta que se lance un nuevo proceso de autorización.
- El número de entradas de gracia (posibilidad de establecer el número de intentos fallidos antes de que la cuenta sea bloqueada)
- Y muchos más aspectos...

Las expresiones comunes son disponibles para personalizar su política de contraseñas. Usted puede establecer una lista de caracteres obligatorios (por ejemplo: al menos una letra mayúscula, una minúscula, una cifra), una lista de caracteres válidos o inválidos, etc

■ Autorizaciones

Las autorizaciones definen lo que un usuario puede hacer en la aplicación: básicamente, usted define lo que un usuario puede ver, hacer y modificar en la aplicación basándose en su rol. Diversas palabras son usadas para definir una autorización: permisos, derechos, restricciones, privilegios.

Existen dos métodos para definir las autorizaciones:

- La forma más segura es prohibir todo desde un principio, para después crear los permisos. Sin embargo, utilizando este método, usted corre el riesgo de olvidar definir algún permiso, imposibilitando así el trabajo de un usuario final u otorgando permisos a usuarios no indicados.
- La forma más rápida es autorizar toda las acciones, para después asignar restricciones y así prohibir algunas de ellas. Esta forma es más rápida que la anterior puesto que generalmente existen menos restricciones que permisos.

Al termino del proceso de autorizaciones, usted terminará con una solución de seguridad basada en roles demasiado compleja, costosa de mantener y difícil de actualizar.

La necesidad

Generalmente, las aplicaciones contienen el código que define los permisos. Por ende, cada vez que usted define un permiso, usted debe seguir todo el ciclo de desarrollo (especificaciones, codificación, pruebas, despliegue, ...)

Esta situación se torna peligrosa desde el momento que:

- Las aplicaciones son actualizadas cada dos o tres meses, mientras que los permisos son frecuentemente actualizados.
- Tomando en cuenta las limitaciones técnicas de su sistema de seguridad, el cumplir con los requerimientos funcionales de las aplicaciones puede consumir mucho de su tiempo e incluso volverse imposible de realizar.
- Los permisos complejos son generalmente identificados cuando la aplicación está en su fase de producción, requiriendo una modificación inmediata.

La solución: independizar los permisos del código de la aplicación

Con Visual Guard.Net, usted no necesita escribir código en la aplicación para poder definir sus permisos. Su código se modifica dinámicamente en tiempo de ejecución:

- Usted puede crear o modificar permisos sin necesidad de realizar todo el ciclo de desarrollo: codificar, probar, desplegar, esperar la retroalimentación...
- Usted puede definir permisos en cualquier momento, aún cuando la aplicación esté en producción. ¡Los permisos cambian dinámicamente!

¿Qué tipo de permisos puede gestionar Visual Guard?

No existe limitación alguna en lo que concierne el tipo de permiso que usted puede implementar al utilizar Visual Guard. ¡Cualquier cambio o restricción que usted desee hacer en su aplicación .Net es posible!

Usted puede crear los permisos según componentes gráficos u objetos de negocio, así como también según objetos que manejen el acceso a una base de datos.

Por ejemplo, con Visual Guard usted puede:

- Esconder o deshabilitar campos, opciones de menú, tabs, controles;
- Cambiar campos al modo "sólo lectura";
- Filtrar datos en una lista;
- Otorgar acceso a un webservice;
- Modificar las reglas de negocio;

Visual Guard puede asegurar cualquier componente de una aplicación .Net, por ejemplo:

- Objetos de la IHM;
- Objetos no visibles;
- Objetos dinámicos;
- SQL statements...

¿Cómo define los permisos Visual Guard?

Visual Guard utiliza el mecanismo de reflexión (reflection mechanism) brindado por el entorno .Net para modificar la aplicación. Esto le permite gestionar los permisos de manera totalmente independiente del código de la aplicación.

Visual Guard pone a su disposición diferentes soluciones para definir los permisos:

- **Propiedades** de las acciones (property actions): Visual Guard puede listar todos los objetos (gráficos o no gráficos) y sus propiedades. Los desarrolladores usan un asistente para identificar el objeto relacionado con el permiso, para después asignarle un nuevo valor dependiendo de sus propiedades (por ejemplo hacer que la propiedad "visible" cambie de "true" a "false" en caso que usted quiera esconder el control). La definición de dicho permiso será guardada en el repositorio de Visual Guard. El código de la aplicación queda sin cambios. Visual Guard modifica la aplicación en tiempo de ejecución de acuerdo con el permiso.
- **Escritura de una acción (script actions):** la escritura de una acción está compuesta del código que usted escribe. Esta codificación es almacenada en el repositorio de Visual Guard y es aplicada directamente en la aplicación. El código de la aplicación queda, nuevamente, sin cambio alguno.
- **Pruebas de permisos en su aplicación:** usted puede también definir los permisos dentro de su aplicación: puede escribir código en su aplicación con el fin de verificar si el permiso (o el rol) es otorgado a un usuario actual, y ejecutarlo si la prueba del permiso fue exitosa.
- **Limitar el modo de acceso:** usted puede definir para qué rol un determinado modo de acceso será disponible
- **Limitar el acceso a una carpeta:** usted puede definir para qué tipo de roles una carpeta será accesible (para aplicaciones ASP.NET solamente)

En la siguiente página, usted encontrará mayor información de las diferentes soluciones que Visual Guard le provee para adaptar su aplicación a las reglas de negocio.

http://www.visual-guard.com/support/index.php?option=com_content&task=view&id=40&Itemid=43

Cuándo puede definir y otorgar permisos

De manera general , se aconseja un proceso de dos pasos:

- **Paso 1:** el equipo de desarrollo utiliza las herramientas de Visual Guard para definir los permisos. A cada permiso le damos un nombre funcional (permitir crear nuevos clientes, esconder información personal...) con el fin de hacerlo más entendible a los administradores.
- **Paso 2:** los administradores (personas no técnicas) utilizan las herramientas de Visual Guard para gestionar las cuentas de usuario y otorgar roles y permisos

■ Auditoría y reportes

La necesidad

- Guardar un historial de quién hizo qué en su aplicación
- Controlar y registrar las transacciones sensibles o financieras en una aplicación.
- Examinar las cuentas de usuario existentes, sus roles y sus permisos.

Estos elementos le serán necesarios para cumplir con:

- Reglas internas de negocio, específicas a su empresa;
- Requerimientos legales (Sarbanes-Oxley Act...);
- Requerimientos de certificaciones (ISO, CMMI, ITIL...)

La solución

Visual Guard le provee los siguientes elementos listos para usarse:

- **Reportes:** usted puede generar de manera automática reportes detallados de las aplicaciones existentes, cuentas de usuario, roles, permisos, etc;
- **Auditoría:** usted puede registrar cualquier evento de su aplicación y revisar este registro en cualquier momento (LOG). Todos los registros de eventos son centralizados en un documento PDF que usted podrá consultar en cualquier momento. Visual Guard le proporciona diferentes tipos de filtro para enfocarse en los eventos que quiera revisar en un momento dado.
- **Consola de administración y auditoría:** Visual Guard registra automáticamente diferentes acciones que son accesibles mediante esta consola, por ejemplo:
 - ¿Quién entró o no pudo entrar en la consola?;
 - ¿Quién otorgó un permiso en específico?;
 - ¿Quién desbloqueó o bloqueó una cuenta de usuario mediante la consola?

■ Las herramientas de seguridad de Visual Guard

Herramientas para los desarrolladores

Visual Guard provee a los desarrolladores herramientas para:

- Crear y modificar permisos en unos cuantos clics;
- Verificar automáticamente la consistencia entre las aplicaciones .NET y los permisos;
- Lanzar una búsqueda en el repositorio con el fin de encontrar cuentas de usuario existentes, permisos, etc.,
- Desplegar nuevas versiones del repositorio al mismo tiempo que una nueva versión de la aplicación;
- Gestionar diversas versiones del repositorio al momento de desplegar la aplicación

Asistente de acciones de seguridad

La mayoría de los permisos son creados mediante las acciones sobre las propiedades (property actions) o sobre un script (or script actions). El asistente de acciones de seguridad le ayuda a crear los permisos en unos cuantos clics, sin añadir código en la aplicación. Este asistente le ofrece opciones detalladas para implementar los permisos que se ajusten a sus necesidades cambiantes y a su tipo de negocio otorgándole una mayor capacidad de respuesta

La descripción de permisos se almacena en el repositorio de seguridad. Los permisos estarán disponibles de manera inmediata aún cuando la aplicación esté en producción. Usted no necesita realizar todo el ciclo de desarrollo para crear los permisos (cambiar el código, hacer las pruebas, desplegar...)

Coherencia de los permisos

Cuando un permiso está relacionado con un componente, cualquier cambio que se realice en dicho componente puede afectar el permiso y de esta forma generar errores (bugs). Por lo tanto, cada nueva versión de la aplicación exige una verificación exhaustiva de los permisos.

Visual Guard puede verificar automáticamente que los permisos y el código de la aplicación estén en perfecta armonía.

El asistente de despliegue

Cada nueva versión de una aplicación puede implicar nuevos permisos y por consecuencia un nuevo repositorio. Usted necesitará desplegar este nuevo repositorio, sin modificar los datos ya introducidos por los administradores en el repositorio previo.

Visual Guard .Net le ofrece un asistente para desplegar los nuevos permisos en un repositorio de producción. Visual Guard comparará de manera automática, los nuevos y antiguos sets de permisos, sin perder las cuentas de usuario, los roles y los permisos.

Control de versiones de los datos de seguridad

Cuando una aplicación está siendo desplegada, algunos usuarios utilizan la nueva versión mientras que otros siguen utilizando la versión antigua. Ambos repositorios de permisos (el nuevo y el antiguo) deben estar disponibles durante el proceso de migración.

Visual Guard. Net puede gestionar diversas versiones del repositorio de permisos. Él le permite un despliegue progresivo de la nueva aplicación y de su repositorio correspondiente. Los usuarios finales pueden tener acceso a ambos, el nuevo y el antiguo, de acuerdo a la versión de la aplicación que utilicen. Por lo tanto, usted puede cambiar de una a otra versión sin bloquear al usuario final o al proceso de migración.

Búsqueda global

Cuando usted realiza el mantenimiento de los permisos, puede verse en la necesidad de encontrar permisos relacionados a un usuario final específico o a una palabra clave del negocio. Por ejemplo, si usted modifica un control en su proyecto, usted necesita listar todos los permisos relacionados con éste con el fin de adaptarlos.

Visual Guard. Net le ofrece una búsqueda global de elementos que le permiten navegar en el repositorio y encontrar todos los elementos relacionados con dicha palabra clave. Usted ahorrará tiempo en el mantenimiento de los permisos al conseguir de inmediato un resultado completo y confiable.

Herramientas para los Administradores

Los formularios de administración

Usted necesita gestionar las cuentas, los roles y los permisos con exactitud y prontitud de manera cotidiana. Visual Guard. Net le ofrece 2 opciones para la administración de dichas tareas:

- **La consola de administración de Visual Guard:** es una aplicación amigable diseñada para personas no técnicas.
- **El API de Visual Guard:** usted puede diseñar su propia forma de administración para después llamar al API de Visual Guard. El API le ofrece elementos listos para su uso que le permiten gestionar las cuentas de usuario y otorgar roles y permisos. Esta forma se integrará a su aplicación, con el estilo e interfaz de su aplicación, lo que permitirá a las personas teniendo un rol de administrador, una fácil utilización. El API de Visual Guard soporta aplicaciones de tipo Winforms y ASP.Net.

¿Quién puede ser administrador de Visual Guard?

Debido a que la administración de Visual Guard no requiere ninguna habilidad técnica, usted puede delegar su administración a cualquiera que se encuentre en la posición de hacerlo. Los administradores pueden ser el personal de seguridad, los administradores del sistema, los gerentes encargados de un departamento o de un sitio remoto...

Esta decisión ya no estará relacionada con una habilidad técnica. Usted podrá cumplir con la política de seguridad de la empresa y optimizar su proceso interno de negocio.

Usted puede incluso definir diversos niveles de administración, cada uno con más o menos autoridad para el uso de la administración de las cuentas de usuario. Por ejemplo: usted puede tener un administrador general quién puede crear permisos y roles y uno local (en el caso de sitios remotos, filiales, sucursales) quien sólo puede crear cuentas de usuario y otorgar los roles ya existentes, sin la posibilidad de cambiar estos roles.

Como resultado, usted gozará de una mayor flexibilidad:

Los administradores son totalmente independientes. Ellos pueden cambiar permisos, roles y cuentas de usuario en cualquier momento, además estos cambios son efectivos inmediatamente.

Por otra parte, usted libera a su grupo de desarrolladores de esta tarea cotidiana.

Roles compartidos

Existe la posibilidad de que usted tenga que definir roles que estén disponibles a toda la organización, no importando el número de aplicaciones que usted tenga (aplicaciones ya existentes o futuras).

Visual Guard.Net le permite compartir roles en diferentes aplicaciones. Por lo tanto usted no deberá gestionar roles diferentes dependiendo de la aplicación.

Herramientas de auditor

La consola de Visual Guard ofrece el rol de auditor. Este rol restringe las funciones disponibles a la persona que funge como auditor, por ejemplo:

- Explorar el repositorio en modo de sólo lectura;
- Generar reportes detallados sobre los permisos existentes, los roles y las cuentas de usuario;
- Revisar los registros de la aplicación con el fin de monitorear transacciones específicas o delicadas;
- Revisar los registros de administración para encontrar quién dio qué autorizaciones a quién.

■ ¿Cómo funciona?

¿Cómo está conformado Visual Guard?

El Repositorio de Visual Guard

El repositorio de Visual Guard almacena las cuentas de usuario, las contraseñas, los roles y los permisos. Este repositorio centraliza los permisos de todas sus aplicaciones .Net (Winform, Webform, Web services), así como las cuentas de usuario, en un lugar único y seguro.

Nota: Con Visual Guard usted puede crear y gestionar las cuentas de usuario creadas en Visual Guard o las ya existentes en el Directorio Activo o en su Base de Datos.

Visual Guard. Net soporta los siguientes tipos de almacenamiento:

- SQL Server y Oracle para el almacenamiento de los usuarios, los permisos y los roles;
- Archivos encriptados de Visual Guard.Net para almacenar usuarios, permisos y roles;
- En caso de que usted decida reutilizar las cuentas de Windows para la autenticación única, las identificaciones son almacenadas en el Directorio Activo;

Usted no debe cambiar su base de datos cuando integre Visual Guard . Net. Visual Guard le provee un asistente para crear su propio repositorio. Usted puede escoger entre crear las tablas correspondientes de Visual Guard .Net en su base de datos o en una base de datos independiente.

El runtime de Visual Guard

El Visual Guard runtime:

- Se compone de 'assemblies .Net';
- Se integra y se despliega con su aplicación;
- Comunica con el repositorio con el fin de verificar la identidad del usuario y recuperar sus permisos;
- Ajusta dinámicamente su aplicación a los permisos de los usuarios;

Integrando Visual Guard para .Net

La integración es rápida y fácil:

- Añada el runtime de Visual Guard a su proyecto y active los servicios de seguridad de Visual Guard (sólo unas cuantas líneas de código son requeridas);
- Implemente la forma de registro de Visual Guard (o puede usar también su propia forma de login);
- Cree un repositorio de seguridad y declare su proyecto en este repositorio;
- Compile y despliegue la aplicación;
- Con la ayuda de la Consola de Visual Guard defina, para cada aplicación, los permisos relacionados. La lista de permisos inicial es usualmente definida por el equipo de desarrolladores antes de que la aplicación vaya a producción. Sin embargo, los permisos pueden ser creados y modificados en cualquier momento, aún después del despliegue. Los permisos toman efecto de manera inmediata;
- Gestione las cuentas de usuario, otorgueles roles y permisos (tarea hecha generalmente por los administradores). Evidentemente esta tarea también puede ser hecha por el equipo de desarrollo.

Para mayor información acerca del proceso de integración, pulse aquí..

¿Le gustaría probar Visual Guard en su propia aplicación? Pulse aquí..

¿Qué pasa en tiempo de ejecución?

- El usuario final introduce sus datos para identificarse (excepto si el modo de identificación única está activado);
- Visual Guard verifica esta identificación;
- Visual Guard se conecta al repositorio de seguridad y recupera los permisos de dicho usuario;
- El runtime de Visual Guard ajusta la aplicación de acuerdo a los permisos dados.

Por ejemplo: cuando una forma se abre, Visual Guard puede esconder los controles y filtrar una lista (mismas funcionalidades soportadas para aplicaciones de tipo ASP.NET, Winform y Webservices).

Para mayor información, sírvase a leer el manual de inicio de Visual Guard.

■ Especificaciones técnicas de Visual Guard

Aplicaciones soportadas

Visual Guard soporta todas las aplicaciones de .Net:

- Winforms (escritas con VB.NET o C#)
- Webforms (ASP.NET y ASP.NET 2.0)
- Web services (2.0 y 3.0 WCF)

Visual Guard .Net asegura todos sus componentes .Net (gráficos, no gráficos, componentes dinámicos).
Visual Guard .Net soporta los framework .Net 2.0, 3.0 y 3.5

También, Visual Guard soporta PowerBuilder de la versión 5 a la 11.

El repositorio de Visual Guard

Usted puede crear el repositorio en:

- Oracle (9i o versiones posteriores);
- MS SQL Server (2000 o versiones posteriores);
- Archivos encriptados de Visual Guard.Net (para aplicaciones pequeñas);
- Si usted tiene otra Base de Datos, favor de contactarnos...

La autenticación de los usuarios

Visual Guard. Net soporta la autenticación de usuarios basada en:

- Cuentas de Windows (autenticación única [single sing-on] disponible para Winforms, Webforms y Webservice);
- El Directorio Activo (usuarios y grupos del Active Directory);
- Cuentas de una base de datos (nombre de usuario y contraseña almacenados en una DBMS);
- Las cuentas de Visual Guard (nombre de usuario y contraseña definidos con Visual Guard).