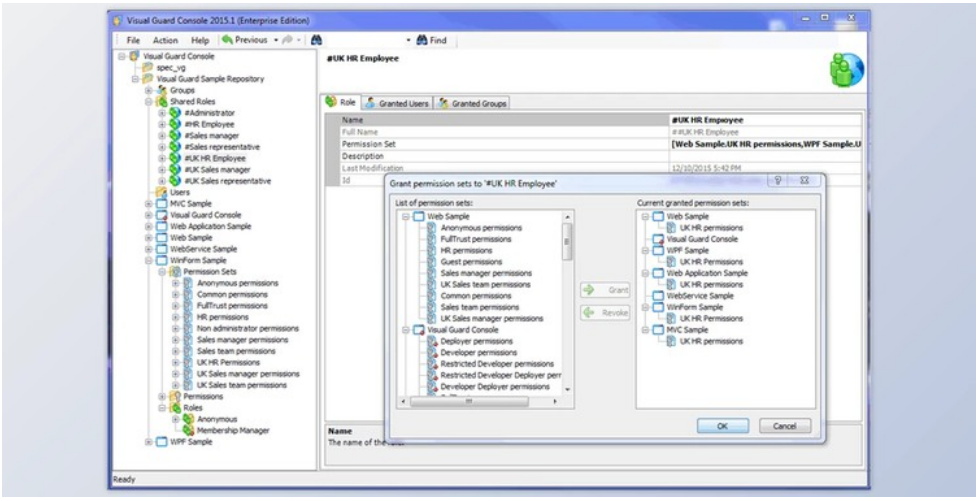
Visual Guard Enterprise v2019.1.0831.19

2025-02-20 15:49:08



Visual Shield is a modular option covering most program security conditions, from application-level safety systems to Corporate Identity and Access Control Solutions.

Visual Guard simplifies your Projects: it handles customers, memberships, and functions. You specify which projects the consumer has access to. Visual Guard facilitates your Programs: Manages users, memberships, roles, and permissions.

Visual Shield is a specific arrangement covering many application security requirements, from application-level safety frameworks to Corporate Identity and Access Control Solutions. For that, the CodeProject 10 Million Members Celebration, Novalys has generated Visual Guard CodeProject Edition (Visual Guard CPE) -- an infrequent rendition of this market-driving response program security. Visual Guard adds safety highlights to your own applications, allowing you to combine customer approval, consents the plank, and inspection at the alone device.

Visual Shield is a ready to-utilize arrangement that communicates a comprehensive organization program. No persuasive reason to modify your app, just a few lines of codes, and you are good to visit go. This unique adaptation is caused available for nothing to Codeproject people. Just click on the link under and adhere to the instructions to Start using Visual Guard.

Visual Guard Enterprise Great Features:

Create, save, manage large volumes (up to millions) of consumer accounts together with the Visual Guard Console. Handle them at a central network, or even set up them to multiple websites.

Produce and handle login/password accounts inside Visual Guard.
Permit them to access specific data and attributes inside your own applications.

Utilize Windows Accounts to authenticate customers accessing your application. Grant rights to Windows Accounts or Windows Groups to get specific application information or attributes.

It's possible to authorize user administrators to add/edit/remove Windows Accounts together with the Visual Guard Console.

Permit users to create an account for themselves. Grant them mechanically default (restricted) access rights. You may opt to need administrator validation before they could access the program.

Establish a hierarchy of classes. Replicate the arrangement of your organization. Place consumers in categories. Grant access rights to user groups.

Users must offer a valid login/password mix before obtaining your program.

Users need to offer legitimate Windows credentials before obtaining your program. Optionally, it is possible to let users input the program without requesting their credentials (see under"Windows SSO").

Highly bonded, yet relatively easy for end-users: they supply their pin password or code through a licensed device (cellular or internet browser). It supports the most complicated security requirements. Read more

Users may log on to your program with their Windows credentials, even though they join a remote location (hotel, airport, people wifi, mobile Internet...).

The identical program can take various kinds of authentication. For example, Windows Accounts for internal customers, login/password for outside users, robust authentication for critical surgeries. Read more

Reuse Windows accounts found in several Lively sites; nothing they belong to the same system or not. Safety is centralized, though users are dispersed over several websites or businesses. Read more

所有软件资源 100%安全 已检测 无病毒 无篡改
去预览

标签

Tools Applications

Windows users can get your program without entering their qualifications: Visual Guard automatically catches the existing Windows accounts and employs the access rights given for this account.

Users may log in once and browse over several sites without login. Whatever the sites are hosted at precisely the identical system or not. They have to communicate with your VG server. Read more

Users can log in and get a desktop program even though they're offline: Visual Guard works locally to authenticate users and apply for their permissions. Supports .NET WPF and Winforms software.

To get login/password accounts, it is possible to customize the rules define, rekindle, unlock, and perish a password. For Windows accounts, the present Active Directory password coverage will apply.

Create right grain permissions, to manage access to particular application data and attributes (buttons, menu, areas...). Group Permissions into Permission Sets and Roles.

Enforce permissions using"dynamic activities": alter objects properties on your program (e.g., disable a menu item, conceal a field...). These activities are entirely independent of the program's code. They're defined and saved within VG and implemented in run-time by Visual Guard. Learn more

Your code frees the user permissions through the Visual Guard API and enables the correct application attributes. E.g., when the user has the permission"Can_Read_Invoice", permit the button"View_Invoice".

Grant functions or permissions to customers through the Visual Guard Console or programming through the VG API.

You can grant Roles to Groups. When placing users in groups, they automatically capture the functions of the classes. Optionally, you may opt to disperse Group functions to sub-groups.

Document important occasions for traceability reasons: user logon, company operations, administrator surgeries, system safety events...

Follow significant tasks in real time within your software for example: access to confidential information, critical trades, security fluctuations. Detect suspicious events - e.g., crucial surgeries at odd times.

Automatically alert administrators, managers or controllers of significant or questionable actions.

Inspection in details the company operations done on your software (who did what, when, from where?). Filter them by program, dates, user, apparatus or occasion. Pinpoint problems or questionable events.

Assess business trends with Graphs. Detect possible problems - for example, odd volumes of trades.

See how each program is utilized. Display time and quantity of powerful or invalid relationships.

Review administrator actions (make customers, grant permissions...). Filter them by program, date, user, apparatus or occasion. Pinpoint problems or questionable events.

Generate reports regarding the access control settings (users, groups, access rights, etc.).

Ready-to-use, Windows-based program, designed for master and developers admins preparing the environment and managing program security. Learn more

Ready-to-use web program, devoted to administrators handling users and granting them access rights, in addition to auditors controlling/reviewing program safety. Learn more

Utility deploying a safety record from dev to check and manufacturing environments. Learn more

Generation server, exposing authentication, access control, logging internet solutions, and procuring any software useful at https or SOAP requests (Java, PHP, Delphi, C++, etc..)

VG APIs expose countless methods for procuring the program in creation (authenticating users, Implementing permissions, logging actions) and restarting safety (managing users, groups, functions...).

Centralize the safety of your software. Get a worldwide overview of users and their access rights throughout the whole IT system. Comprehensive and uniform Control and Audit across all of the programs. 1 Program

Insert a VG .Net run-time on your software to fasten them. Supports Winform, WPF, ASP.NET, WCF, MVC, in Addition to SharePoint Applications.

Insert a VG PowerBuilder run-time on your PowerBuilder Software to fasten them.

Telephone the Internet services exposed from the Visual Guard Server to Authenticate users, apply permissions and log actions. Works with almost any language capable of calling Internet Services.

Get the entire source code of this Web Administration Console and adapt it to your company requirements. Employ your business logic and company presentation standards and telephone the Visual Guard API to handle and audit safety. Our service team will support you each step along the way.

Grow a module which can integrate with a 3rd party authentication provider. Our service staff will guide you each step along the way.

Implement custom safety rules for program security. By way of instance, apply segregation of responsibilities by specifying which functions or user group ought to be mutually exclusive (can not be allowed to the identical user). Our service staff will

guide you each step along the way.

版本列表

Visual Guard Enterprise v2019.1.0831.19