

Setting Visual Intercept Web Security

Visual Intercept Web and Web Relay are dependent upon several IIS and directory level configuration settings. Typically these settings will be set by the installer, but in some cases where the IIS server has been locked down or a user manually makes changes to the site these configuration settings may be impacted. This tech-tip describes the basic elements of security as they apply to Visual Intercept Web and Web Relay.

Visual Intercept Web and Web Relay require that the owner of the website, as defined in the VIWebDev Properties| Directory Security Tab, must be granted explicit permissions to several directories to ensure proper operation of the application. By default the owner, or Anonymous User, is IUSR_ *MachineName*.

For purposes of this document we will use IUSR_ *MachineName* to describe owner privileges, but it could just as easily be a specific Domain or Machine account created specifically for the purpose of running the Visual Intercept Web sites.

If proper permissions are not granted to the Anonymous User account the following errors may be encountered:

- Users may not be able to save global queries and/or Notification rules
- Users may not be able to log on
- Users may not be able to attach documents
- Users may not be able to view attached documents
- Users may not be able to access features that are unique to their user profile (i.e.: bookmarks, personal queries and/or notification rules, default queries etc)

Setting Permissions

Setting permissions at the directory level as shown in the table below will insure that Visual Intercept Web sites function properly. To set the permissions, right-click on the appropriate directory, select the Security tab and add the IUSR_ *MachineName* account, applying the security as set forth in the Security Required column.

Security Legend:

Full Control-F

Modify-M

Read & Execute-RE

List Folder Contents-L

Read-R

Write-W

Directory	Security Required	Reason
Inetpub/wwwroot/viWebDev	RE, R, W, L	Site administration and configuration operations
Inetpub/wwwroot/viWebDev/Cache	F	Temporary cache for SCC operations
Inetpub/wwwroot/viWebDev/Profiles	F	User roving profile definitions are stored in this location
Program Files/Visual Intercept Enterprise/Queries	M, RE, L, R, W	Server side queries are stored in this location
Program Files/Visual Intercept Enterprise/Docs	M, RE, L, R, W	Related documents to incidents, projects, and contacts are stored in this location

Program Files/Visual Intercept Enterprise/Temp	M, RE, L, R, W	Temporary cache for document management operations
Program Files/Visual Intercept Enterprise/Rules	M, RE, L, R, W	Server side notification rules are stored in this location

Windows Server 2003 Specific Issues

For Windows 2003 Server, one additional step is needed. Because IIS comes "locked-down" in Windows 2003, you must set IIS to "Allow" the following:

- Server Side Includes
- Active Server Pages
- WebDAV

To do this, launch IIS and select the Web Server Extensions directory. Next, highlight any of the above extensions that are in a "Prohibited" state, right mouse-click, choose "Allowed" and then restart IIS.

If you have other questions about issues not included in or beyond the scope of this Tech Tip, please contact Elsinore Technical Support Services at support@elsitech.com or 866.866.0034, option 2.