# Contents

1. Information Assurance Best Practices ............................................................... 5  
   - Documentation ................................................................. 5  
   - Open Web Application Security Project (OWASP) ................................. 6  
     - Software Development Life Cycle ........................................ 6  
     - Network Infrastructure .................................................. 7  
   - WebFOCUS Settings .......................................................... 7  
   - WebFOCUS ReportCaster Settings ........................................... 9  
   - WebFOCUS Reporting Server Security ...................................... 9  

Customer Connections ............................................................... 11
Information Assurance* refers to measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. In this release, WebFOCUS has been enhanced with a number of new security capabilities that emphasize strategic risk management and defend against malicious hacker attacks. This level of security is critical for externally-facing web-based Business Intelligence applications.

WebFOCUS 8 has achieved a Level 2a validation using Open Web Application Security Project (OWASP) Application Security Verification Standards (ASVS), and a low vulnerability rating against the most important security vulnerabilities and threats in the industry, as defined by OWASP. For more information about Information Assurance and OWASP, go to http://www.owasp.org/index.php/Main_Page.


In this chapter:

- Documentation
- Open Web Application Security Project (OWASP)
- WebFOCUS ReportCaster Settings
- WebFOCUS Reporting Server Security

Documentation

This document is intended to be used as a reference. Settings and controls are fully documented in the following manuals for your specific release:

- WebFOCUS and ReportCaster Installation and Configuration for your platform
- WebFOCUS Security and Administration
- ReportCaster
- Server Installation
Open Web Application Security Project (OWASP)

The Open Web Application Security Project (OWASP) is an open community organization that is dedicated to improving the security of application software. All of the OWASP information, tools, documents, and forums are free to anyone interested in learning about web-based security and how to improve it within their environments.

The OWASP Top Ten (2013) Project provides a list of web vulnerabilities, as well as remediation steps to eliminate them.

These top ten vulnerabilities are listed as:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Unvalidated Redirects and Forwards

OWASP also provides an Application Security Verification Standard (ASVS) document, which outlines a standard that can be implemented to test for web application security vulnerabilities.

For additional information on the Top Ten Project and the ASVS document, visit the OWASP website at www.owasp.org.

Software Development Life Cycle

Information Builders Business Intelligence Products Group has taken information from the OWASP Top Ten list, the Application Security Verification Standard (ASVS) document, and other open source documentation, and has integrated this information utilizing a full Software Development Life Cycle (SDLC) approach that targets these web vulnerabilities within our product.

Our SDLC approach utilizes, but is not limited to:

- Developer code review
单元测试
集成测试
全回归测试
验证测试
全功能规格测试
静态分析软件测试
动态分析软件测试
应用渗透测试使用第三方工具
独立安全漏洞测试

For specific information regarding Application Servers and DBMS support, see the WebFOCUS and ReportCaster Installation and Configuration manual for your specific platform, as well as the Server Installation WebFOCUS Reporting Server DataMigrator Server manual.

Network Infrastructure

External users must connect to Internet servers in order to run applications and retrieve data. Allowing connections is unavoidable so it is really important that connections are secured to prevent malicious attacks. In terms of security, servers are of two types, trusted and untrusted. Trusted servers are typically hosted in the internal or private network behind a firewall. Untrusted servers are typically in the demilitarized zone (DMZ).

Enterprise customers can secure the untrusted servers with a reverse proxy by allowing only the reverse proxy to communicate to the untrusted servers. Customers may choose to isolate Internet servers from trusted servers by hosting only the reverse proxy in the demilitarized zone (DMZ) and hosting trusted servers on their internal network.

This security layer prevents malicious users from communicating directly to web servers. Instead, they can only access the reverse proxy. Reverse proxies also limit exposure to real machine names, providing additional security.

WebFOCUS Settings

The following list includes WebFOCUS specific configuration settings, as well as recommendations to further secure a WebFOCUS application.
Depending on application specific requirements, all of these configuration options may or may not be required or used in the final application security design. As stated in the WebFOCUS Security and Administration manual, customers may need to prototype one or more configuration scenarios before arriving at the optimal solution.

- Use SSL Version 3.0 or TLS to encrypt all sensitive data between the client browser and the web/application servers, using ciphers of 128-bit encryption or higher.

- Use AES encryption for TCP/IP secure communication from the WebFOCUS Client to the WebFOCUS Reporting Server.

- Run the WebFOCUS Client and the WebFOCUS Reporting Server on separate physical machines, with a firewall or RESTRIC_TO_IP in between.

- Implement File Permissions for WebFOCUS and ReportCaster. For more information, see the Protecting Your WebFOCUS Installation chapter of the WebFOCUS Security and Administration manual.

- PROTECT the following variables by adding the following statements to the site.wfs file, which is accessed by the WebFOCUS Administration Console:

  <SET> IBIF_adhocfex(PROTECT)
  <SET> IBIF_raw(PROTECT)
  <SET> IBIF_cmd(PROTECT)
  <SET> IBFS_fexContent(PROTECT)

  The effect of adding these statements will disable any type of ad hoc FOCUS syntax in a production environment. You should contact Customer Support Services for specific information on the implementation and implications of these settings.

- Set WF_proj_list_from_wfrs to YES. This restricts the list of application folders seen in Developer Studio based on the APP PATH setting on the Reporting Server. For more information, see the Using the Administration Console chapter of the WebFOCUS Security and Administration manual.

- Disable Redirection within the mime.wfs file for certain formats.

- Set <session-timeout> in the WebFOCUS web application web deployment descriptor, web.xml.
WebFOCUS ReportCaster Settings

The ReportCaster Distribution Server usually runs within a secured network environment, and encrypting these communication parameters is not usually necessary. If encryption from the Distribution Server to Managed Reporting is needed and encryption of the data to and from the WebFOCUS Reporting Server is needed, follow these steps:

**JSSE Caster**

Set to YES within the ReportCaster configuration. This enables the use of SSL from the ReportCaster Distribution Server communicating to the Managed Reporting Repository to schedule MR procedures.

**JSSE Servlet**

Set to YES within the ReportCaster configuration. This enables the use of SSL for the applet scheduling tools to retrieve MR procedures.

Set 3DES encrypt connection to WFRS, with the following additional parameter on the WebFOCUS Reporting Server JDBC URL:

```
jdbc:eda:\hostname:port;server=;ENCRYPTION=1;
```

WebFOCUS Reporting Server Security

This section addresses WebFOCUS reporting server security. For additional information, see the Server Administration for UNIX, Windows, OpenVMS, IBM i, and z/OS manual. Guidelines include:

- Install the WebFOCUS Reporting Server on a separate physical machine than the WebFOCUS Client.
- RESTRICT_TO_IP restricts incoming communications.
  
  Configure the Reporting Server to accept incoming connections from a restricted list of hosts for the TCP/IP and HTTP connections. Use this and/or set up a firewall in between the WebFOCUS Client and the WebFOCUS Reporting Server.
- Use SSL to encrypt all data between the client browser and the HTTP Listener for the WebFOCUS Reporting Server.
- Use AES encryption for TCP/IP communication from the WebFOCUS Client to the WebFOCUS Reporting Server.
- SET OPSYSCMD=OFF to disable operating system commands.
If applications do not require operating system commands, this should be disabled. In addition, operating system commands can be disabled using Role Based Access control on the Reporting Server by selecting *Disable Operating System Commands* for a particular Role. For more information, see the *Protecting Your WebFOCUS Installation* chapter of the *WebFOCUS Security and Administration* manual.

- **SET DPT=OFF** to disable the Direct Passthru option.

  If application requirements do not require direct SQL Passthru, this should be disabled. In addition, direct SQL Passthru can be disabled using Role Based Access control on the Reporting Server by selecting *Disable Direct Passthru* for a particular Role. For more information, see the *Protecting Your WebFOCUS Installation* chapter of the *WebFOCUS Security and Administration* manual.

- **SET HTMLENCODE=ON** to encode the HTML output that is data.

  This setting will disable the rendering of HTML tags within a browser when these tags are stored within the actual data, or created using a DEFINE or COMPUTE command. In addition, data can be HTML encoded using Role Based Access control on the Reporting Server by selecting *Always Encode HTML Characters for HTML Reports* for a particular Role.

- Encrypt Master Files on the WebFOCUS Reporting Server.

- Encrypt WebFOCUS Reporting Server FOCEXECs.

- **SET DEFECHO=NONE**. This setting will disable echo output, so information regarding WebFOCUS code cannot be returned to the browser.

- Use DBA for Master Files for which you want to restrict access. For more information, see the *Using the Administration Console* chapter of the *WebFOCUS Security and Administration* manual and the *Creating and Rebuilding a Data Source* chapter of the *Describing Data With WebFOCUS Language* manual.
Customer Connections

Where users partner with Information Builders to provide feedback and create quality documentation.

Partner With Us

Information Builders Technical Content Management team is comprised of many talented individuals who work together to design and deliver quality technical documentation products. Your feedback supports our ongoing efforts!

You can also join a usability study to get an early look at new documentation products and services. Your participation helps us create documentation products that meet your needs.

To send us feedback or make a customer connection, contact Michele Brady, Service Director, Technical Content Management at Michele_Brady@ibi.com.

Request Permission to Use Copyright Material

To request permission to repurpose copyrighted material, please contact Frances Gambino, Executive Director, Technical Content Management at Frances_Gambino@ibi.com.

Visit the Information Builders Technical Documentation Library

To visit the Technical Documentation Library, go to http://documentation.informationbuilders.com/.