WebFOCUS 8 Implementation Guide for PCI Security Standards

This document provides recommendations, information, customizations, and configuration steps for WebFOCUS to meet the Payment Card Industry Data Security Standards outlined within the PCI DSS v2.0 document located at:

https://www.pcisecuritystandards.org

Customers can use this WebFOCUS guide to implement the required steps to be PCI compliant. This guide applies to WebFOCUS Version 8.x.

About the PCI Security Standards

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. The twelve requirements and sub-requirements for PCI DSS compliance apply to all system components around technology and security, particularly that of the protection of cardholder data.

Based on an independent assessment by an information security company, and through an extensive vetting process by the Qualified Security Assessor (QSA), WebFOCUS was evaluated in regard to Payment Card Industry Data Security Standard (PCI DSS) configuration best practices that are applicable to Business Intelligence functionality. PCI requirements for transaction processing are outside the scope of WebFOCUS control and capabilities.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Recommendations and Information for Requirement 1

❑ Install the WebFOCUS Client and the WebFOCUS Reporting Server on an internal (trusted) network segment unexposed to the Internet Demilitarized Zone (DMZ).

❑ TCP/IP listener ports are required for certain WebFOCUS functionality. WebFOCUS also communicates to other non-WebFOCUS servers over TCP/IP, requiring access to those ports.

WebFOCUS TCP/IP Listener Ports

Default TCP/IP Ports	Usage	Remarks
WebFOCUS Reporting Server TCP/IP Listener Ports		
8120	TCP/IP listener	Should only be accessible from the WebFOCUS Client and the ReportCaster Distribution Server.
8121	HTTP or HTTPS listener	Should only be accessible from the internal (trusted) network.
8122	FOCSU listener	Can be disabled if not accessing multi-user FOCUS data sources.
8123	Java Services (JSCOM3) listener	Additional JSCOM3 listeners will require port numbers that increment by one (8124-*nnnn*).
WebFOCUS Client		
1527	Relational Database	Apache™ Derby by default, but can use other Relational Databases.
ReportCaster TCP/IP Ports		
8200	Main listener	Should be accessible from the WebFOCUS Client.

Access Required to Non-WebFOCUS TCP/IP and HTTP Ports

Default TCP/IP Ports	Usage	Remarks
WebFOCUS Reporting Server Access to TCP/IP Ports		
Site dependent	Data Adapters	Used for native and JDBC connections to database servers.
Site dependent	Adapter for Web Services	May need access to the HTTP port.
Site dependent	WebFOCUS Graphics, EXL07, and Magnify for indexing requests	Need access to the HTTP port. If using SSL or any type of single sign on, jscom3 needs to be used.
636	LDAP server	Used for LDAP authentication over TLS/SSL.
ReportCaster Access to TCP/IP Ports		
25	Email server	Used for SMTP connections.
Site dependent	JDBC access to database server	Used for access to the ReportCaster repository.
636	LDAP server	Used for LDAP authentication over TLS/SSL.

The image below illustrates a standard WebFOCUS architecture model and use of TCP/IP listener ports.
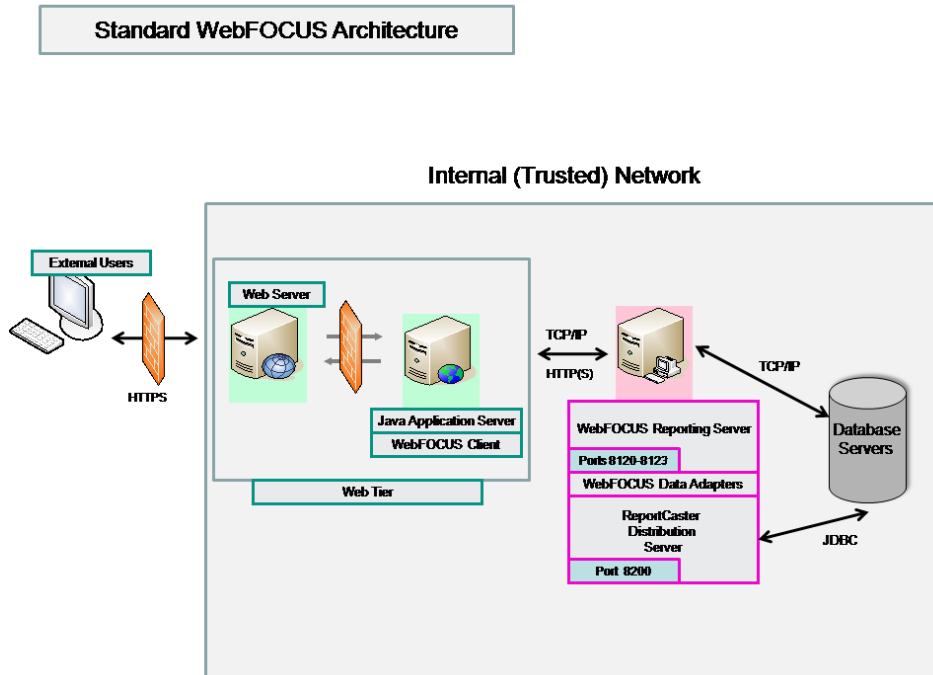
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Recommendations and Information for Requirement Section 2.1

❏ Change the default WebFOCUS Managed Reporting Administration credentials.

Note: Typically within a production environment, WebFOCUS Administration Console access will be disabled, as configuration settings would not be altered.

❏ If installing Apache Tomcat™ from the WebFOCUS media, change the Tomcat administration credentials.

❏ Review and apply, where appropriate, security settings described in the *Information Assurance Best Practices* documentation.

Recommendations and Information for Requirement Section 2.2.1

❏ Install WebFOCUS in at least a three-tier architecture, where the WebFOCUS Client is installed on one machine, the ReportCaster Distribution Server and the WebFOCUS Reporting Server are installed on a second machine, and the Database Server(s) are installed on separate machines.

❏ Firewall rules can be established based on information from Requirement 1. If needed, the WebFOCUS Reporting Server configuration parameter RESTRICT_TO_IP can be used to restrict access to the TCP/IP and HTTP listeners.

Recommendations and Information for Requirement Section 2.2.2

❏ Configure the WebFOCUS Client and the WebFOCUS Reporting Server with the SSL protocol to provide secure HTTPS communication between WebFOCUS components. Refer to the *WebFOCUS Security and Administration* and the *Server Administration for UNIX, Windows, OpenVMS, IBM i, and z/OS* Version 8 manuals.

Recommendations and Information for Requirement Section 2.2.4

Do not install any additional software or functionality that is not required by WebFOCUS.

❏ Minimally, WebFOCUS Client requires:

  ❏ Java Application Server and Java Virtual Machine

  ❏ Relational Database Management System

❏ WebFOCUS Reporting Server requires:

  ❏ Database drivers for database access

  ❏ Java Virtual Machine

❏ ReportCaster requires:

  ❏ Java Virtual Machine

Recommendations and Information for Requirement Section 2.3

❏ The WebFOCUS Reporting Server Console can be configured for HTTPS. Refer to the *Server Administration for UNIX, Windows, OpenVMS, IBM i, and z/OS* Version 8 manual for configuration information.

❏ Communication to the WebFOCUS Client should use SSL to access the web server or application server infrastructure.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Recommendations and Information for Requirement Section 3.3

❏ WebFOCUS developers must ensure that reports written in the WebFOCUS language appropriately mask sensitive data.

❏ The Master File attribute, ACCESS=INTERNAL, should be added to hide columns that contain sensitive data.

Recommendations and Information for Requirement Section 3.4

❏ Limit creation of WebFOCUS extract files containing sensitive data.

❏ Traces should be enabled only for purposes of troubleshooting and gathering diagnostics, and preferably in a non-production WebFOCUS environment. Trace files should be purged immediately after use.

❏ Disable WebFOCUS Redirection for report output types, such as Excel® and PDF output.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Recommendations and Information for Requirement 4

❏ ReportCaster, if distributing content over public networks using FTP, it must be configured to use SFTP.

❏ Configure the WebFOCUS Client to use AES128 or AES256 encryption for communication with the WebFOCUS Reporting Server, using a symmetric key negotiated through RSA PKI. Refer to the *WebFOCUS Encryption Features* chapter in the *WebFOCUS Security and Administration* Version 8 manual for additional details on configuring and implementing encrypted communication to the WebFOCUS Reporting Server.

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Recommendations and Information for Requirement 5

Requirements are not applicable to WebFOCUS.

Requirement 6: Develop and maintain secure systems and applications

Recommendations and Information for Requirement 6

❏ Ensure that the latest WebFOCUS Service Packs and Hot Fixes are applied. Refer to *http://techsupport.ibi.com* for the latest Service Packs and patches.

❏ Third-party software provided by Information Builders, such as Tomcat and Sun Java, should be updated as recommended by those vendors.

Recommendations and Information for Requirement Section 6.3

❏ Adhere to internal Software Development Life Cycle (SDLC) recommendations for application development to ensure that any customizations do not introduce new vulnerabilities.

❏ Remove any test accounts created during development prior to a production rollout.

Recommendations and Information for Requirement Section 6.4

❏ Create separate WebFOCUS environments for development, test, and production.

❏ WebFOCUS applications should not be developed directly on production environments.

❏ WebFOCUS Client and Reporting Server Service Pack installations can be rolled back. Refer to the *WebFOCUS Installation Manual* for your platform for uninstall instructions.

❏ Change Management provides the ability to move content from one environment to another.

Recommendations and Information for Requirement Sections 6.5 and 6.6

❏ Use WebFOCUS Information Assurance Best Practices and coding techniques to eliminate application vulnerabilities. Refer to the *Information Assurance Best Practices* for all security settings that can be applied to public-facing web applications.

❏ For WebFOCUS applications that are public facing, customers must perform regular web application vulnerability assessments and/or install external firewalls.

❏ Information Builders adheres to established Software Development Life Cycle in developing the WebFOCUS product, and has achieved an OWASP Application Security Verification Standard (ASVS) level 3. Additional information is described in the *Information Assurance Best Practices* documentation.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

Recommendations and Information for Requirement 7

❏ WebFOCUS Managed Reporting and Business Intelligence Portal provide role-based security, along with optional privileges, which should be used for access control.

❏ User access control, using Managed Reporting role-based security, can be integrated with the WebFOCUS Reporting Server using a shared authentication scheme. Refer to the *Authentication* chapter in the *WebFOCUS Security and Administration* Version 8 manual for details.

❏ Row-level and column-level security may be included as needed within WebFOCUS. Refer to Information Builders Technical Memo 4694 for details:

http://documentation.informationbuilders.com/masterindex/html/pdf_wf_7703/tm4694.pdf

Requirement 8: Assign a unique ID to each person with computer access

Recommendations and Information for Requirement 8

❏ WebFOCUS should be configured to restrict multiple logins by the same user. This can be done by setting the IBI_Multiple_Logins_Per_User parameter to FALSE in the WebFOCUS Administration Console.

❏ Passwords stored for WebFOCUS Managed Reporting users are stored in a SHA-512 Iterative Salted Hash.

❏ Passwords stored for WebFOCUS service accounts are encrypted using either WebFOCUS encryption, Triple DES, or AES128 through AES256 encryption, using an internally or externally provided key.

❏ Passwords stored for service accounts for the WebFOCUS Reporting Server are encrypted using AES128 through AES256 encryption.

❏ WebFOCUS exits can be used for custom encryption, if the default methods are not sufficient. Refer to the *WebFOCUS Security and Administration* Version 8 manual for additional information.

❏ PCI DSS password policies can be implemented in the following ways:

  ❏ Enabling Account Polices within the WebFOCUS Administration Console.

  ❏ WebFOCUS can be configured to delegate security to third-party authentication providers, such as Microsoft Active Directory, LDAP, Tivoli Access Manager, CA SiteMinder, and others.

❏ Public user access to cardholder data should be restricted.

❏ WebFOCUS can be configured to control session timeouts, which limit the amount of time users can remain active when using the following components:

❏ Global - update the WebFOCUS_HOME\ibi\WebFOCUS80\webapps\webfocus\ WEB-INF\web.xml file as follows:

```
<session-config>
<session-timeout>15</session-timeout>
</session-config>
```

❏ Business Intelligence Dashboard

❏ Update parameters USER_MAX_INACTIVE and PUBLIC_MAX_INACTIVE from the WebFOCUS Administration Console.

❏ Update WebFOCUS_HOME\ibi\WebFOCUS80\worp\conf\bid-config.xml to enforce single login per user credentials, as follows:

```
<internal-var name="allowOnlyOneUserWithSameId" value="true"/>
```

❏ WebFOCUS applications authenticate all access to databases using the following mechanisms:

❏ Password Passthru

❏ Explicit

❏ Trusted

❏ For ad hoc reporting and shared reports, customers must ensure that the appropriate controls and approvals are in place.

Requirement 9: Restrict physical access to cardholder data

Requirements are not applicable to WebFOCUS.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Recommendations and Information for Requirement 10

❏ WebFOCUS Resource Analyzer can be used to audit and monitor application usage, including:

❏ Procedure name, date-time started, execution time, CPU time used, wait time

❏ I/O operations, number of records, number of transactions, number of lines

❏ MR Domain, MR User, connection user ID, APP PATH, network connection

❏ Selection criteria, data source, field

❏ The Resource Analyzer repository should be restricted to user IDs with proper authorization. Refer to the *Resource Analyzer Administrator's and User's Manual*.

❏ WebFOCUS logging is initialized when the application starts and remains active, as long as the application is running.

❏ WebFOCUS provides compensating controls for auditing user and administrative actions.

❏ WebFOCUS Version 8.x includes user access and administrative auditing built into the product.

WebFOCUS Logs

Log File	Usage	Remarks
WebFOCUS Managed Reporting		
audit.log	Tracks all sign in and security-related changes.	Review the *WebFOCUS Security and Administration* manual for specific auditing capabilities.
WebFOCUS Reporting Server		
edaprint.log	Track user connections	Connections made from the WebFOCUS Client and ReportCaster to the WebFOCUS Reporting Server.
Business Intelligence Dashboard		
dashboard.log	Track user connection changes	Uniquely named file backups are created.

Requirement 11: Regularly test security systems and processes

Recommendations and Information for Requirement Section 11.3

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 external-facing web-based Business Intelligence applications. WebFOCUS Version 8.x has achieved Level 3 Application Security Verification Standards low risk security certification against the most important security vulnerabilities and threats, as defined by the Open Web Application Security Project (OWASP).

For more information about Information Assurance and OWASP, visit *http://www.owasp.org*.

Recommendations and Information for Requirement Section 11.5

For each component, directories containing critical WebFOCUS configurations are listed below, where WebFOCUS_HOME refers to the WebFOCUS installation directory.

WebFOCUS Configuration Directories

Directory	Usage	Remarks
WebFOCUS Reporting Server		
WebFOCUS_HOME\ibi\srv80\wfs\etc	TCP/IP communication and profiles	Used to define TCP/IP Listener ports. Host global profile.
WebFOCUS_HOME\ibi\profiles	Profile information	Host and user profiles.
WebFOCUS_HOME\ibi\srv80\wfs\bin	edaserve.cfg	Main Reporting Server configuration file.
ReportCaster		
WebFOCUS_HOME\ibi\ReportCaster\cfg	Configuration information	Used to configure ReportCaster.
WebFOCUS Client		
WebFOCUS_HOME\ibi\WebFOCUS80 \client\wfc\web\cgi	Trace information	Used to define trace levels.
WebFOCUS_HOME\ibi\WebFOCUS80 \client\wfc\etc	Configuration information	Used to configure security, timeouts, and other configuration parameters.
WebFOCUS_HOME\ibi\WebFOCUS80 \config	Configuration information	Used to configure security, timeouts, and other configuration parameters.
WebFOCUS_HOME\ibi\WebFOCUS80 \ibi_html\javaassist	Static content	Used to read and write static content.

Directory	Usage	Remarks
WebFOCUS_HOME\ibi\WebFOCUS80\webapps	Web applications	Used to host web applications packaged with WebFOCUS.
WebFOCUS_HOME\ibi\WebFOCUS80\worp\conf	Business Intelligence Dashboard configuration information	Used to customize Business Intelligence Dashboard parameters.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Requirements are not applicable to WebFOCUS.

Conclusion

Information Builders hopes that the material presented in this document provides an understanding of the WebFOCUS configuration options that will allow customers to be PCI compliant. Information Builders is committed to work in partnership with our customers to further develop the *WebFOCUS Implementation Guide for PCI Security Standards* in anticipation of future WebFOCUS versions and changes in the PCI Security Standards.