

Web Plus Security Features and Recommendations

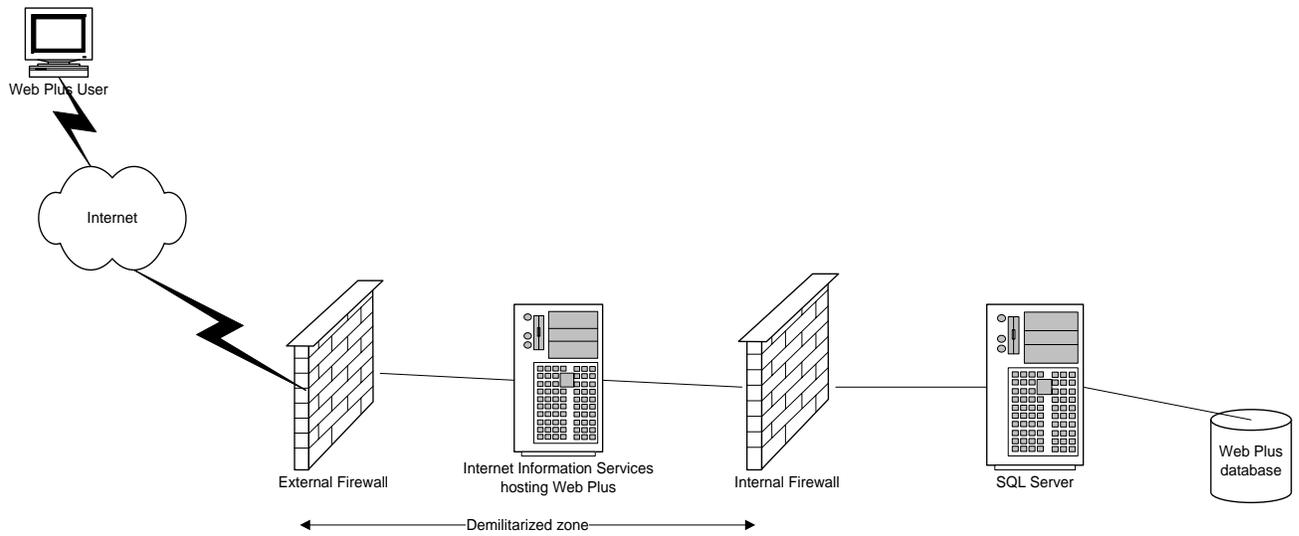
(Based on Web Plus Version 3.x)

**Centers for Disease Control and Prevention
National Center for Chronic Disease Prevention and Health Promotion
Division of Cancer Prevention and Control
National Program of Cancer Registries
Registry Plus™ Software for Cancer Registries**



Web Plus has been designed as a highly secure application that can be used to transmit confidential patient data between reporting locations and a central registry safely over the public Internet. Security is achieved by a combination of software features and network infrastructure. This document outlines the security features of the application and recommendations for the operating environment to ensure a secure installation.

Web Plus is a form-authenticated, ASP.NET application that is hosted on Internet Information Services (IIS) running on Microsoft® Windows® 2000 or later server operating systems. In a typical setting, the Web server sits in the demilitarized zone between the external and internal firewalls while SQL Server, where the Web Plus database is stored, resides inside the internal firewall as part of the trusted network.



The security of Web Plus depends to a large extent on the security of the client computer, the communication channel between the client and the Web server, the Web server, the base operating system, and the configuration of the firewalls on either side of the Web server. It is very important that the hosting agency have a security policy in place and document the users who have access to Web Plus and the database, and their assigned roles. The hosting agency is responsible for encrypting the Web Plus database if required. Security breaches by social engineering attacks are always a consideration; special attention is required in all parts of the system to prevent such attacks. Use of strong passwords is highly recommended, and users should be expressly prohibited from sharing accounts.

Security Features of the Web Plus Application

Authentication

Web Plus uses form-based authentication where users must enter their user ID and password to be authenticated by the application. Multi-factor authentication can be implemented by requiring users to enter a personal identification number (PIN) and/or answer challenge questions in addition to providing their user ID and password.

Passwords

The central registry administrator can configure the following password attributes—

- Enforce password complexity by using a regular expression.
- Keep a password history and require new passwords to be different from the ones used before.
- Set an expiration date to force users to change their password after a specified time interval.

The administrator can reset forgotten passwords. Web Plus then forces the user to change the password after the first login.

Personal Identification Number (PIN)

The PIN is an optional security feature to accommodate two-factor user authentication. When enabled on the systems preference page, the central registry administrator can generate a random and unique Web Plus PIN matrix for every user. At login, in addition to his or her user ID and password, the user must enter the four-digit PIN based on coordinates from their Web Plus PIN matrix.

Note: PIN matrix coordinates are provided on login. The hosting agency must mail the matrices to users.

Challenge Questions

Challenge questions are another optional security feature. When enabled on the systems preference page, the central registry administrator can enter challenge questions to be answered by each user when the feature is enabled initially, and then used upon login to validate the user's identity. The number of challenge questions for initial setup and login can be specified.

Role-Based Access

Web Plus also implements a role-based access, where users are granted different levels of access depending on the role or roles assigned to them. Eight roles are defined in Web Plus:

- **Facility abstractor:** Works in a local facility or doctor's office and handles patients' medical records. When a patient is diagnosed with cancer, the facility abstractor reports the case to the state's central cancer registry. The facility abstractor also completes and submits any follow-back abstracts that the central registry has posted for their facility.
- **Central registry abstractor/reviewer:** Reviews abstracts submitted to the central registry for completeness and accuracy and may abstract additional data items from submitted text; also abstracts new cases.
- **Central registry administrator:** Sets up facilities with access to Web Plus to report their data, manages facility accounts and users at both central registry and facilities, configures display types, edit sets, and system preferences, manages assignment of abstracts to central registry staff, exports data, and views reports.
- **Local administrator:** Locally manages the users who are allowed to access Web Plus at one facility.
- **File uploader:** Uploads either files of abstracts in the appropriate NAACCR format that were not abstracted using Web Plus or non-NAACCR files in any format; views EDITS error reports for uploaded files in NAACCR format; cleans, or works with abstractors to clean, errors on rejected abstracts prior to resubmitting; downloads files posted by the central registry; and views reports.
- **Follow-back supervisor:** Uploads files of partially-filled follow-back abstracts, manually adds follow-back abstracts online, tracks follow-back abstracts by uploaded file or by facility, and generates and views Web Plus follow-back reports.
- **Follow-back monitor:** Tracks follow-back abstracts by assigned facility and generates and views Web Plus follow-back reports.
- **File upload supervisor:** Monitors upload of files to the central registry, tracks file uploads by facility, communicates with facilities to ensure resubmission of rejected files, and views reports.

Prevention of Web Application Vulnerabilities

Web Plus prevents Web application vulnerabilities including SQL injection and cross-site scripting attacks. This security component in Web Plus scans the incoming HTTP requests for malicious

characters. If malicious characters are found in the incoming request, the application page is redirected to a "blocked" page and the user is alerted about suspect input data.

Other Application Security Features

Other security features of the application include—

- Facilities and offices have access only to the abstracts entered at their facility or office.
- Web Plus keeps an extensive log of user logins, data accesses, and updates for auditing purposes.
- User accounts can be locked out if invalid login attempts exceed a threshold value configurable by the central administrator.
- An administrator can deactivate a user account temporarily.
- The central administrator can see users' activities through the Current User Activities page.
- Display types and edit set configurations are controlled centrally.
- Passwords are stored in the database using a one-way hash algorithm.
- The Web Plus configuration file can store the connection string to the SQL Server database in encrypted format.

Security of the Operating Infrastructure

Security on the Client Computer

The client computer should be protected from any kind of Trojan horse or spyware attacks by installing anti-virus and anti-spyware software, and ensuring that these programs are up-to-date.

Secure Communication Channel and Server Certificate

Web Plus relies on a Secure Sockets Layer (SSL) channel between the Web server and client browser for the protection of data exchanged over the Internet. To set up an SSL channel, the Web server needs to have a server certificate installed and the Web site containing the application should have SSL encryption turned on. The certificate for the server can either be created in-house, if a certificate server is available, or can be purchased from a commonly trusted third-party commercial organization called a certificate authority. A certificate of 128-bit cyber strength is the industry standard for secure communication over the Internet and is highly recommended.

Two-Factor Authentication Using Client Certificates

The form-based authentication of Web Plus may be supplemented with a two-factor authentication scheme in which users are authenticated based upon "what they know" and "what they have." The "what they know" part of the scheme is fulfilled by the login page of Web Plus, as users need to know their user ID and password to log into the system. Additionally, you can configure IIS to require users to have certificates to connect to the Web Plus site. When the Web Plus site is configured this way, the hosting agency is responsible for creating and distributing client certificates to users. When installed on users' computers, the client certificates form the "what they have" part of the two-factor authentication scheme.

Note: Multi-factor authentication can be implemented using the personal identification number (PIN) security feature, which requires that users enter a PIN in addition to their user ID and password.

Hardening of the Web Server and Operating System

Windows 2003 Server with IIS6 is highly recommended because of enhanced security over Windows 2000 server. Follow Microsoft's guidelines to harden the Web server and the base operating system. The IISLockdown tool available from Microsoft's download site can be used to automate several security steps to reduce the vulnerability of the Windows 2000 Web server.

Recommendations from Microsoft include—

- Applying the latest patches to the operating system and Internet Information Services (IIS). Use the Microsoft Baseline Security Analyzer to detect patches and updates that may be missing from the current installation.
- Do not install IIS as part of the operating system installation. Rather, install it later, after you have updated and patched the base operating system. Then install IIS, apply patches, and harden the IIS configuration.
- When installing IIS, do not install File Transfer Protocol (FTP) Server, Microsoft FrontPage 2000 server extensions, Internet Service Manager (HTML), NNTP service, or Visual InterDev RAD remote deployment support. However, install SMTP to support Web Plus' e-mail capability.
- Disable NetBIOS and SMB on the Internet-facing network interface card and remove Web Distributed Authoring and Versioning (WebDAV).
- Delete or disable unused accounts: rename the administrator account, disable the guest and IUSR accounts, create a custom anonymous Web account, enforce strong password policies, restrict remote logons, and disable null sessions. The custom anonymous account created to replace the IUSR account should have the least privilege. If you run IISLockdown, add your custom user to the Web Anonymous Users group. IISLockdown denies access to system utilities and the ability to write to Web content directories for the Web Anonymous Users group.
- Use strong access controls to protect sensitive files and directories. Set access at the directory level whenever possible.
- Ensure that only the .NET Framework Redistributable package is installed on the server, and no SDK utilities are installed. Do not install Visual Studio.NET on production servers. Debugging tools should not be available on the Web server. Ensure that access is restricted to powerful system tools and utilities such as those contained in the \Program Files directory. Remove all of the sample files.
- Relocate Web roots and virtual directories to a non-system partition to protect against directory traversal attacks.

Secure Connection to the Database

If SQL server authentication is used, the user ID and password are embedded in the connection string, but the connection string is stored in encrypted form (using DPAPI) in Web.config. If Windows authentication is used, the user's credentials are not included in the connection string; the connection string is still encrypted hiding the database server's IP address and port number.

Windows authentication is the preferred method because it does not transmit the user's credentials over the network. For Windows authentication to work, a mirrored ASPNET process account must be created as a local Windows account with the same name and password on the database server. ASPNET is a least-privileged account created when .NET Framework is installed on the Web server. By default, all ASP.NET applications run under this account's security context. After creating the account in Windows, create a SQL Server login for the account and grant it access to Web Plus database.

It is recommended that the SQL Server listen on a port number different from the default port (1433). This port then should be opened in the internal firewall to allow Web server to access the database.

Configuring ASP.NET for Security

Various security options can be configured in the Web.config and machine.config files. The settings depend on local security requirements and administrative preferences. In most cases, leaving the settings at the default values should provide the required security.